

Resource Center

Documentação



1. GSM - HISTÓRICO DE REVISÕES	9
2. GSM - INTRODUÇÃO	10
2.1 Recursos - Blockbit GSM	11
2.2 Destaques - Blockbit GSM	12
2.3 Verificação de ambiente para instalação do Blockbit GSM	13
2.3.1 Requisitos de instalação	14
2.4 Sobre o Guia do Administrador	15
3. GSM - ARQUITETURA	16
4. GSM - INSTALAÇÃO	18
4.1 GSM - Importando a Máquina Virtual	19
4.2 Iniciando Máquina Virtual - Primeiro Acesso	24
5. GSM - CONFIGURAÇÃO DE EXCEÇÃO	26
6. GSM - ASSISTENTE DE INSTALAÇÃO	30
7. GSM - AMBIENTE DE REDE	34
8. GSM - NOTIFICATIONS VIA SNMP	36
8.1 GSM - Zabbix	38
8.2 GSM - Geomap	44
8.3 GSM - Geomap hidden for backup	47
9. GSM - INTERFACE WEB	50
10. GSM - OPERAÇÃO BÁSICA	52
11. GSM - MENU DE PERFIL DO USUÁRIO	54
11.1 Profile	55
11.2 Logout	57
12. GSM - DEPLOYS PANEL	58
12.1 Deploys Panel - Busca e Filtros	60
12.2 Deploys Panel - Lista de Deploys	61
12.2.1 Deploys Panel - Coluna Package	63
12.2.2 Deploys Panel - Coluna Auditor	64
12.2.3 Deploys Panel - Coluna Scheduled	65
12.2.4 Deploys Panel - Coluna Progress	66
12.2.5 Deploys Panel - Coluna Status	67
12.2.6 Deploys Panel - Coluna Actions	68
12.2.6.1 Deploys Panel - Botão "Accept"	69
12.2.6.2 Deploys Panel - Botão "Reinstall"	70
12.2.6.3 Deploys Panel - Botão "Cancel"	71
12.2.6.4 Deploys Panel - Botão "Activity"	72
12.2.6.5 Deploys Panel - Botão "Remove"	73
13. GSM - INSTALL PACKAGE	74
13.1 What	75
13.2 Where	76
13.3 When	77
13.4 Who	78
14. GSM - MANAGEMENT	79
14.1 Devices	80
14.1.1 Aba Inventory	81
14.1.1.1 Inventory - Menu de ações	82
14.1.1.1.1 Inventory - Menu de ações - Create Group	83
14.1.1.1.2 Inventory - Menu de ações - Manage Groups	85
14.1.1.1.3 Inventory - Menu de ações - Create Device	92
14.1.1.1.4 Inventory - Menu de ações - Delete Devices	102
14.1.1.1.5 Inventory - Menu de ações - Reload Status	104
14.1.1.1.6 Inventory - Menu de ações - Synchronize Devices	105
14.1.1.1.7 Inventory - Menu de ações - Update Devices	107
14.1.1.2 Inventory - Coluna "Name"	108
14.1.1.3 Inventory - Botões de ações	109
14.1.1.3.1 Inventory - Botão de ações - "Access CLI"	110
14.1.1.3.2 Inventory - Botão de ações - "Access Interface Web"	111
14.1.1.3.3 Inventory - Botão de ações - "Update/Synchronize"	112
14.1.1.4 Inventory - Coluna "Group"	113
14.1.1.5 Inventory - Coluna "Model"	115
14.1.1.6 Inventory - Coluna "License Status"	117
14.1.1.7 Inventory - Coluna "Version"	118
14.1.1.8 Inventory - Coluna "Template"	119
14.1.1.9 Inventory - Coluna "Policy IPv4"	120
14.1.1.10 Inventory - Coluna "Policy IPv6"	121
14.1.1.11 Inventory - Coluna "Actions"	122
14.1.1.11.1 Inventory - Coluna "Actions" - Botão "Delete"	123
14.1.1.11.2 Inventory - Coluna "Actions" - Botão "Edit"	124
14.1.2 Aba Communities	125
14.1.2.1 Communities - Menu de ações	127
14.1.2.1.1 Communities - Menu de ações - Create Community	128
14.1.2.1.2 Communities - Menu de ações - Delete Community	138
14.1.2.2 Communities - Colunas	139
14.1.2.3 Communities - Exemplos de Communities	140
14.1.3 Aba Templates	153
14.1.3.1 Templates - Colunas	154
14.1.3.1.1 Templates - Configurar Template	155
14.1.3.2 Templates - Menu de ações	162
14.1.3.2.1 Templates - Menu de ações - Criar Template	163

14.1.3.2.2 Templates - Menu de ações - Clonar Template	165
14.1.3.2.3 Templates - Menu de ações - Excluir Templates	167
14.1.4 Aba Provisioning	169
14.1.4.1 Provisioning - Menu de ações	170
14.1.4.1.1 Provisioning - Menu de ações - Create Device	171
14.1.4.1.2 Provisioning - Menu de ações - Add Batch Provisioning	179
14.1.4.2 Provisioning - Colunas	198
14.1.5 Aba Backups	199
14.1.5.1 Backups - Menu de Ações	201
14.1.5.1.1 Backup - Menu de ações - Create Backup	202
14.1.5.1.2 Backup - Menu de ações - Delete Backup	205
14.1.5.1.3 Backups - Colunas	207
14.1.5.2 Exemplo - Backup de Devices	210
14.1.5.2.1 Backup de Devices - Inclusão de Devices	211
14.1.5.2.2 Backup de Devices - Criação de Storage	216
14.1.5.2.3 Backup de Devices - Criação das Rotinas de Backup	226
14.1.5.2.4 Backup de Devices - Validação das configurações	233
14.2 Profiles	235
14.2.1 Aba Web Filter	237
14.2.1.1 Web Filter - Menu de ações	238
14.2.1.1.1 Web Filter - Menu de Ações - Create Profile	239
14.2.1.1.2 Web Filter - Menu de Ações - Clone Profile	241
14.2.1.1.3 Web Filter - Menu de ações - Delete Profile	243
14.2.1.2 Web Filter - Colunas	245
14.2.1.2.1 Web Filter - List Profile	246
14.2.2 Aba Application Control	253
14.2.2.1 Application Control - Menu de ações	254
14.2.2.1.1 Application Control - Menu de ações - Create Profile	255
14.2.2.1.2 Application Control - Menu de ações - Clone Profile	257
14.2.2.1.3 Application Control - Menu de ações - Delete Profile	259
14.2.2.2 Application Control - Colunas	261
14.2.2.2.1 Application Control - List Profile	262
14.2.3 Aba Threat Protection	266
14.2.3.1 Threat Protection - Menu de ações	267
14.2.3.1.1 Threat Protection - Menu de ações - Create Profile	268
14.2.3.1.2 Threat Protection - Menu de ações - Clone Profile	270
14.2.3.1.3 Threat Protection - Menu de Ação - Delete Profile	272
14.2.3.2 Threat Protection - Colunas	274
14.2.3.2.1 Threat Protection - List Profile	275
14.2.4 Aba Intrusion Prevention	283
14.2.4.1 Intrusion Prevention - Menu de Ações	284
14.2.4.1.1 Intrusion Prevention - Menu de Ações - Create Profile	285
14.2.4.1.2 Intrusion Prevention - Menu de Ações - Clone Profile	287
14.2.4.1.3 Intrusion Prevention - Menu de Ações - Delete Profile	289
14.2.4.2 Intrusion Prevention - Colunas	291
14.2.4.2.1 Intrusion Prevention - Create Profile	292
14.2.5 Aba SSL Inspection	298
14.2.5.1 SSL Inspection - Menu de ações	299
14.2.5.1.1 SSL Inspection - Menu de Ação - Create Profile	300
14.2.5.1.2 SSL Inspection - Menu de Ação - Clone Profile	302
14.2.5.1.3 SSL Inspection - Menu de Ação - Delete Profile	304
14.2.5.2 SSL Inspection - Colunas	306
14.2.5.2.1 SSL Inspection - SSL Profile	307
14.2.6 Aba SD-WAN	310
14.2.6.1 SD-WAN - Menu de ações	311
14.2.6.1.1 SD-WAN - Menu de ações - Create Profile	313
14.2.6.1.2 SD-WAN - Menu de ações - Clone Profile	315
14.2.6.1.3 SD-WAN - Menu de ações - Delete Profile	317
14.2.6.2 SD-WAN - Colunas	319
14.2.6.2.1 SD-WAN - SDWAN Profile	320
14.3 Objects	325
14.3.1 Objects - Addresses	326
14.3.1.1 Objects - Addresses - Menu de ações	327
14.3.1.1.1 Objects - Addresses - Menu de ações - Create Object	328
14.3.1.1.2 Objects - Addresses - Menu de ações - Create Group	336
14.3.1.1.3 Objects - Addresses - Menu de ações - Delete Object	338
14.3.1.2 Objects - Addresses - Colunas	340
14.3.1.2.1 Objects - Addresses - Object Mapping	341
14.3.2 Objects - Services	342
14.3.2.1 Objects - Services - Menu de ações	344
14.3.2.1.1 Objects - Services - Menu de ações - Create Object	345
14.3.2.1.2 Objects - Services - Menu de ações - Create Group	353
14.3.2.1.3 Objects - Services - Menu de ações - Delete Object	355
14.3.2.2 Objects - Services - Colunas	357
14.3.2.2.1 Objects - Services - Object Mapping	358
14.3.3 Objects - Time	359
14.3.3.1 Objects - Time - Menu de ações	360
14.3.3.1.1 Objects - Time - Menu de ações - Create Object	361
14.3.3.1.2 Objects - Time - Menu de ações - Create Group	363

14.3.3.1.3 Objects - Time - Menu de ações - Delete Object	365
14.3.3.2 Objects - Time - Colunas	367
14.3.3.2.1 Objects - Time - Object Mapping	368
14.3.4 Objects - Schedules	369
14.3.4.1 Objects - Schedules - Menu de ações	370
14.3.4.1.1 Objects - Schedules - Menu de ações - Create Object	371
14.3.4.1.2 Objects - Schedules - Menu de ações - Create Group	373
14.3.4.1.3 Objects - Schedules - Menu de ações - Delete Object	375
14.3.4.2 Objects - Schedules - Colunas	377
14.3.4.2.1 Objects - Schedules - Object Mapping	378
14.3.5 Objects - Dictionaries	379
14.3.5.1 Objects - Dictionaries - Menu de ações	380
14.3.5.1.1 Objects - Dictionaries - Menu de ações - Create Object	381
14.3.5.1.2 Objects - Dictionaries - Menu de ações - Create Group	384
14.3.5.1.3 Objects - Dictionaries - Menu de ações - Delete Object	386
14.3.5.2 Objects - Dictionaries - Colunas	388
14.3.5.2.1 Objects - Dictionaries - Object Mapping	389
14.3.6 Objects - Contents	390
14.3.6.1 Objects - Contents - Menu de ações	391
14.3.6.1.1 Objects - Contents - Menu de ações - Create Object	392
14.3.6.1.2 Objects - Contents - Menu de ações - Create Group	395
14.3.6.1.3 Objects - Contents - Menu de ações - Delete Object	397
14.3.6.2 Objects - Contents - Colunas	399
14.3.6.2.1 Objects - Contents - Object Mapping	400
14.4 Users	401
14.4.1 Aba Users	402
14.4.1.1 Users - Menu de ações	403
14.4.1.1.1 Users - Menu de ações - Add to Group	404
14.4.1.1.2 Users - Menu de ações - Select All e Deselect All	406
14.4.1.2 Users - Colunas	407
14.4.2 Aba Groups	408
14.4.2.1 Groups - Menu de ações	409
14.4.2.1.1 Groups - Menu de ações - Create Group	410
14.4.2.1.2 Groups - Menu de Ações - Delete Group	413
14.4.2.1.3 Groups - Menu ações - Select All e Deselect All	415
14.4.2.2 Groups - Colunas	416
14.4.2.2.1 Groups - Edit Group	417
14.5 Policies	420
14.5.1 Aba Policy Packages	421
14.5.1.1 Policy Packages - Menu de ações	422
14.5.1.1.1 Policy Packages - Menu de ações - Create Package	423
14.5.1.1.2 Policy Packages - Menu de ações - Delete Packages	425
14.5.1.1.3 Policy Packages - Menu de ações - Clone Packages	427
14.5.1.1.4 Policy Packages - Menu de ações - Select All e Deselect All	429
14.5.1.2 Policy Packages - Colunas	430
14.5.1.2.1 Policy Packages - Policy Manager	431
14.5.2 Aba Policy Templates	453
14.5.2.1 Policy Templates - Menu de Ações	454
14.5.2.1.1 Policy Templates - Menu de ações - Create Template	455
14.5.2.1.2 Policy Templates - Menu de ações - Delete Templates	457
14.5.2.1.3 Policy Templates - Menu de ações - Clone Templates	459
14.5.2.1.4 Policy Templates - Menu de ações - Select All e Deselect All	461
14.5.2.2 Policy Templates - Colunas	462
14.5.2.2.1 Policy Templates - Policy Manager	463
15. GSM - ANALYTICS	468
15.1 Analyzer	469
15.1.1 Firewall	471
15.1.1.1 Firewall – Geolocation	475
15.1.1.2 Firewall – Zone Traffic	476
15.1.1.3 Firewall – Top User	478
15.1.1.4 Firewall – Top Service	479
15.1.1.5 Firewall – Top Source	480
15.1.1.6 Firewall – Top Policy	481
15.1.2 Web Filter	483
15.1.2.1 Web Filter - Allowed Sites e History	487
15.1.2.2 Web Filter - Denied Sites e History	488
15.1.2.3 Web Filter - History Categories - Total Traffic e Total Hits	489
15.1.2.4 Web Filter - History Content Types - Total Traffic e Total Hits	491
15.1.2.5 Web Filter - History Domains - Total Traffic e Total Hits	493
15.1.2.6 Web Filter - History Profiles - Total Traffic e Total Hits	495
15.1.2.7 Web Filter - Top Categories	497
15.1.2.8 Web Filter - Top Content Type	498
15.1.2.9 Web Filter - Top Domains	499
15.1.2.10 Web Filter - Top Domains by Time	500
15.1.2.11 Web Filter - Top Profiles	502
15.1.2.12 Web Filter - Top Users	503
15.1.2.13 Web Filter - Total Traffic e History	504
15.1.2.14 Web Filter - Users - Total Traffic e Total Hits	505
15.1.3 Application Control	507

15.1.3.1 Application Control - Allowed Application	511
15.1.3.2 Application Control - Denied Application	512
15.1.3.3 Application Control - History	513
15.1.3.4 Application Control - Top Allowed Categories	515
15.1.3.5 Application Control - Top Denied Categories	516
15.1.3.6 Application Control - Top Allowed Applications	517
15.1.3.7 Application Control - Top Denied Applications	519
15.1.4 Intrusion Prevention	521
15.1.4.1 Intrusion Prevention - Alerted, Blocked e Histórico	525
15.1.4.2 Intrusion Prevention - Alerts by Geolocation	527
15.1.4.3 Intrusion Prevention - Impact - High	528
15.1.4.4 Intrusion Prevention - Impact - Medium	532
15.1.4.5 Intrusion Prevention - Impact - Low	536
15.1.4.6 Intrusion Prevention - Layer 3 Intrusion Protection	540
15.1.4.7 Intrusion Prevention - Intrusion Classification	543
15.1.4.8 Intrusion Prevention - Top Source	545
15.1.4.9 Intrusion Prevention - Top Destination	547
15.1.5 Threat Protection	549
15.1.5.1 Threat Protection - Threats e History	554
15.1.5.2 Threat Protection - Malwares e History	555
15.1.5.3 Threat Protection - Geolocation	556
15.1.5.4 Threat Protection - Impact - High	557
15.1.5.5 Threat Protection - Impact - Medium	559
15.1.5.6 Threat Protection - Impact - Low	561
15.1.5.7 Threat Protection - Malicious IP Classification	563
15.1.5.8 Threat Protection - Top Threat Types	566
15.1.5.9 Threat Protection - Top Users by Threats	568
15.1.5.10 Threat Protection - Top Users by Malware	570
15.1.5.11 Threat Protection - Top Malware	571
15.1.5.12 Threat Protection - Top Infected Domains	572
15.1.5.13 Threat Protection - Top Source	573
15.1.5.14 Threat Protection - Top Destination	575
15.1.6 User Behavior	577
15.1.6.1 User Behavior - History	580
15.1.6.2 User Behavior - Analysis Panel	581
15.1.6.2.1 User Behavior - Analysis Panel - Network Traffic	589
15.1.6.2.2 User Behavior - Analysis Panel - Policy Usage	592
15.1.6.2.3 User Behavior - Analysis Panel - Application Usage	593
15.1.6.2.4 User Behavior - Analysis Panel - Web Usage	594
15.1.6.2.5 User Behavior - Analysis Panel - Threat Protection	597
15.1.6.2.6 User Behavior - Analysis Panel - Intrusion Prevention	600
15.1.6.3 User Behavior - Geolocation Information	603
15.1.7 Dashboard	605
15.2 Reports	618
15.2.1 Reports - Menu de Ações	619
15.2.1.1 Reports - Menu de ações - Create	620
15.2.1.2 Reports - Menu de ações - Delete	624
15.2.2 Reports - Colunas	626
15.3 Events	627
15.3.1 Events - Query Editor	629
15.3.2 Events - Top Hits	632
15.3.3 Events - History	634
15.3.4 Events - Log Events	636
15.3.4.1 Events - Log Events - Event View	637
15.3.4.2 Loggers	638
15.3.4.2.1 Loggers - Loggers	639
15.3.4.2.2 Instalação do Logger	664
15.3.4.2.3 Loggers - Clusters	683
16. GSM - SETTINGS	709
16.1 System	710
16.1.1 System - Aba "General"	711
16.1.2 System - Aba "License"	717
16.1.3 System - Aba "Updates"	720
16.1.4 System - Aba "Backups"	721
16.1.4.1 System - Backups - Settings	722
16.1.4.2 System - Backups - Backups History	725
16.1.4.3 Exemplo - Backup da Manager	727
16.1.4.3.1 Exemplo - Backup da Manager - Inclusão de Storage	728
16.1.4.3.2 Exemplo - Backup da Manager - Criação da Rotina de Backup	733
16.1.4.3.3 Exemplo - Backup da Manager - Validação das Configurações	736
16.1.5 System - Aba "Storages"	738
16.1.5.1 Storages - Menu de Ações	739
16.1.5.1.1 Create Storage - SMB	740
16.1.5.1.2 Create Storage - NFS	742
16.1.5.1.3 Create Storage - SFTP	744
16.1.5.1.4 Create Storage - USB	748
16.1.5.2 Storages - Delete Storages	753
16.1.5.3 Storages - Colunas	755
16.1.6 System - Aba "High Availability"	756

16.1.6.1 High Availability - Cluster Interfaces	758
16.1.6.2 High Availability - Cluster Settings	759
16.1.6.3 High Availability - Cluster Status	761
16.1.6.4 High Availability - Exemplo	763
16.1.6.4.1 High Availability - Configuração do Cluster Primário	765
16.1.6.4.2 High Availability - Configuração do Cluster Secundário	772
16.1.6.4.3 High Availability - Validação das Configurações	786
16.1.7 System - Aba "Certificates"	789
16.1.8 System - Aba "Custom Branding"	792
16.2 Network	795
16.2.1 Network - Aba "General"	796
16.2.2 Network - Aba "Interfaces"	797
16.2.3 Network - Aba "E-mail"	799
16.3 Administration	801
16.3.1 Administration - Aba "Administrators"	802
16.3.1.1 Administration - Administrators - Menu de Ações	803
16.3.1.1.1 Administrators - Menu de Ações - Create User	804
16.3.1.1.2 Administrators - Menu de Ações - Delete User	806
16.3.1.2 Administration - Administrators - Colunas	807
16.3.2 Administration - Aba "Users Profiles"	808
16.3.2.1 Administration - Users Profiles - Menu de Ações	809
16.3.2.1.1 Users Profiles - Menu de Ações - Create Profile	810
16.3.2.1.2 Users Profiles - Menu de Ações - Clone Profile	813
16.3.2.1.3 Users Profiles - Menu de Ações - Delete Profile	815
16.3.2.2 Administration - Users Profiles - Colunas	817
16.3.3 Administration - Aba "Auth Servers"	818
16.3.3.1 Administration - Auth Servers - Menu de Ações	819
16.3.3.1.1 Create Radius	820
16.3.3.1.2 Create LDAP	822
16.3.3.1.3 Delete Server	825
16.3.3.2 Administration - Auth Server - Colunas	826
16.3.3.2.1 Server - Test Authentication	827
16.3.4 Administration - Aba "Identity Provider"	828
16.3.4.1 Identity Provider - Service Provider	830
16.3.4.1.1 Identity Provider - Service Provider - Add Certificate	832
16.3.4.1.2 Identity Provider - Service Provider - Import Certificate	834
16.3.4.2 Identity Provider - Identity Provider	835
16.3.5 Administration - Aba "Audit Log"	837
16.3.5.1 Audit View	838
16.3.6 Administration - Aba "Access Control"	839
17. GSM - CLI - LINHA DE COMANDOS	840
17.1 [arp]	843
17.2 [arping]	844
17.3 [date]	845
17.4 [debug-backup]	847
17.5 [debug-deployer]	849
17.6 [debug-ha]	850
17.7 [debug-rotation]	851
17.8 [debug-sync]	852
17.9 [delete-logger-backup]	853
17.10 [disable-snmp]	854
17.11 [enable-root]	855
17.12 [enable-snmp]	856
17.13 [ethtool]	858
17.14 [exit]	859
17.15 [fdisk]	860
17.16 [free]	862
17.17 [fsck]	863
17.18 [grep]	864
17.19 [help]	865
17.20 [history]	866
17.21 [hostname]	867
17.22 [ifconfig]	868
17.23 [ifstat]	870
17.24 [iotest]	871
17.25 [ip]	872
17.26 [ipcalc]	873
17.27 [less]	874
17.28 [logger-config]	875
17.29 [logger-devices-add]	878
17.30 [logger-devices-list]	879
17.31 [logger-disable]	880
17.32 [logger-enable]	881
17.33 [logger-key]	882
17.34 [lscpu]	883
17.35 [mkfs]	884
17.36 [more]	885
17.37 [netstat]	886
17.38 [ntpdate]	887

17.39 [passwd]	888
17.40 [ping]	889
17.41 [reboot]	890
17.42 [reset]	891
17.43 [reset-admin-blocks]	892
17.44 [reset-admin-password]	893
17.45 [reset-admin-sessions]	894
17.46 [reset-logs]	895
17.47 [rewizard]	896
17.48 [route]	897
17.49 [sar]	899
17.50 [set-network-dns]	900
17.51 [set-network-gateway]	901
17.52 [set-network-hostname]	902
17.53 [set-network-interface]	904
17.54 [set-network-timezone]	905
17.55 [show-devices]	906
17.56 [show-license]	907
17.57 [show-uuid]	908
17.58 [show-version]	909
17.59 [shutdown]	910
17.60 [tcpdump]	911
17.61 [tcpdump]	912
17.62 [telnet]	913
17.63 [tracpath]	915
17.64 [traceroute]	916
17.65 [update-gsm]	919
17.66 [update-license]	921
17.67 [upgrade-blockbit]	922
17.68 [uptime]	923
17.69 [vmstat]	924
17.70 [whois]	925
18. Blockbit GSM versão 2.4.0	928

GSM - HISTÓRICO DE REVISÕES

Controle de Versão do Documento

DATA	DESCRIÇÃO DA ALTERAÇÃO
01/06/2017	Lançamento.
17/10/2018	Revisão e adição de conteúdo.
22/02/2019	Atualização para a versão GSM 1.2.1.
17/01/2020	Atualização para a versão GSM 2.0.
22/06/2020	Atualização para a versão GSM 2.0.4.
04/09/2020	Atualização para a versão GSM 2.0.5.
04/11/2020	Atualização para a versão GSM 2.0.6.
14/12/2020	Atualização para a versão GSM 2.0.7.
14/12/2020	Atualização para a versão GSM 2.0.8.
17/05/2021	Atualização para a versão GSM 2.0.9.
23/08/2021	Atualização para a versão GSM 2.0.10.
24/08/2021	Atualização para a versão GSM 2.0.11.
30/05/2022	Atualização para a versão GSM 2.0.12.
02/08/2022	Atualização para a versão GSM 2.0.13.
25/03/2021	Atualização para a versão GSM 2.1.0.
23/08/2021	Atualização para a versão GSM 2.1.1.
22/09/2021	Atualização para a versão GSM 2.2.0.
30/05/2022	Atualização para a versão GSM 2.2.1.
02/08/2022	Atualização para a versão GSM 2.2.2.
31/10/2022	Atualização para a versão GSM 2.3.0.
27/02/2023	Atualização para a versão GSM 2.4.0.

GSM - INTRODUÇÃO

Obrigado por escolher o Blockbit GSM.

Este Guia do Administrador tem como objetivo auxiliar você e sua empresa a realizar o processo de instalação, configuração e utilização do Blockbit GSM. Ao término deste guia, você estará apto a utilizar todas as funcionalidades e recursos necessários para seu funcionamento.

O Blockbit GSM - Global Security Management, ou Gerenciamento Global de Segurança, foi desenvolvido para gerenciar as múltiplas soluções da Blockbit. Através dele é possível administrar os Perfis de Dispositivos, Gerenciamento e Automação de Inventário, Monitoramento, realizar upgrade remotamente e muitas outras soluções que serão devidamente detalhadas posteriormente.

Os benefícios para sua empresa ao utilizar o Blockbit GSM são diversos: Economia de tempo, redução de custos, diminuição de erros de configuração, padronização das políticas de segurança e consequentemente uma redução drástica de ameaças e ataques cibernéticos, sendo que uma das suas maiores vantagens: É o fato dele não restringir a quantidade de dispositivos gerenciados. Para melhor compreensão, segue um exemplo: Supondo que o João é administrador de uma rede de 1.000 lojas e necessita bloquear o acesso a determinado domínio de rede social para cada loja, sem o Blockbit GSM será necessário configurar o *Firewall* de cada loja para realizar o bloqueio. Porém, com o Blockbit GSM é possível realizar o bloqueio de todas as lojas ao mesmo tempo, basta apenas fazer a configuração adequada no Blockbit GSM e executar o *deploy* para todas as lojas, simples, rápido e prático.

Além disso, o Blockbit GSM fornece maior controle ao administrador graças a permitir a instalação de loggers, o que possibilita uma visualização holística da rede e de seus usuários através de widgets, gráficos, eventos e geração de relatórios, o Blockbit GSM realiza o gerenciamento centralizado de todas as licenças dos seus Dispositivos Blockbit;

O Blockbit GSM oferece flexibilidade, padronização e proteção completa para sua empresa, fazendo tudo isso através de uma plataforma simplificada, rápida, fácil de configurar e de utilização descomplicada, fornecendo ao administrador de rede uma visão completa da gestão de segurança do seu negócio. O Blockbit GSM atende empresas de pequeno, médio e grande porte.

A solução de Gerenciamento Centralizada garante o funcionamento ininterrupto de todos os seus gateways, caso se torne indisponível. Permitindo a administração, operação e total controle sobre cada gateway, mesmo em casos de indisponibilidade da gerência (Stand Alone). A solução também permite a instalação de políticas individuais (apenas para 1 gateway), para um grupo de gateways gerenciados.

Recursos - Blockbit GSM

- **Device Grouping (agrupamento de devices):** Este recurso proporciona a possibilidade de agrupar devices de acordo com as suas necessidades, o que causa uma facilidade considerável no processo de instalação das configurações;
- **Role Based Administration (administração baseada em perfil):** Tem como finalidade principal possibilitar o controle de diversos usuários, monitorar suas permissões por devices e granularidade;
- **Device Template-based Configuration (configuração de devices baseada em Template):** Os Templates são um conjunto de configurações gerais das devices do Blockbit UTM, sendo que este consiste em configurações de: *System, Authentication, Firewall, Web Cache, Web Filter, Anti malware, IPS, ATP, Traffic Shapping, SD-WAN e DNS*, com isso, é possível inicializar os devices utilizando-se das configurações globais de forma rápida, prática e sem erros, diminuindo o TCO (custo total de propriedade), maximizando o desempenho da equipe de TI e evitando eventuais erros nas configurações;
- **Centralized User Management (gerenciamento centralizado de usuários):** Este recurso provê ao administrador a capacidade de elaborar políticas baseada em usuários e grupos autenticados;
- **Policy Template-based Management (gerenciamento de políticas baseada em Templates):** Permite a criação de políticas e grupos de políticas para controlar os acessos das redes protegidas pelas devices, de forma rápida, fácil e sem erros;
- **Workflow for Audit and Deployment Control (auditoria de fluxo de trabalho e controle de implantação):** O Blockbit GSM foi desenvolvido pensando no gerenciamento de mudanças, sendo que todas as configurações realizadas são encaminhadas para aprovação de um auditor previamente selecionado, permitindo: Receber e registrar as solicitações de instalações dos pacotes de configuração, avaliar as implicações, custos, benefícios e riscos das mudanças propostas, justificar e aprovar as mudanças e o agendamento das instalações;
- **VPN Community Management (gerenciamento de comunidades de VPN):** Crie comunidades de VPN – *Virtual Private Network* no Blockbit GSM. Essas configurações permitem que ocorra uma comunicação segura, rápida e criptografada entre as devices.

O Blockbit GSM foi pensando e desenvolvido através de uma arquitetura baseada na facilidade de uso e compreensão, para minimizar erros e dar uma visão completa de gestão aos administradores do sistema.

Destaques - Blockbit GSM

- **Policy Manager:** Em apenas uma interface de configuração, agrupe facilmente políticas de segurança por dispositivo, unidade organizacional, tipos de ameaças ou controles. É possível integrar vários recursos em uma única política, como: Categoria *WEB*, Controle de aplicativo, Controle de banda, Múltiplos serviços, *QoS - Quality of Service*, Cota de tempo e tráfego, Escolha de *link* e Redundância, e controle de vírus e *malware*;
- **Policy Template:** Possibilita a criação de grupos de políticas permitindo o reaproveitamento de outros agrupamentos já criados na tela *Policy Manager*, ganhando em agilidade e praticidade;
- **Device Inventory:** Organize seus dispositivos por versão de "*Firmware*", região geográfica, usuários administrativos, clientes ou unidades organizacionais, facilitando a gestão da rede;
- **Device Communities:** Defina parâmetros de configurações e de segurança dos escopos de *VPN* e distribua facilmente entre os dispositivos;
- **Device Templates:** Defina configurações gerais do sistema de maneira global entre os "*Templates*" de *Device*;
- **Deploys Panel:** Acompanhe e gerencie as instalações dos pacotes de configurações do Blockbit GSM nas *devices* gerenciadas.

Verificação de ambiente para instalação do Blockbit GSM

Para realizar a instalação do Blockbit GSM é necessário que você esteja familiarizado com as soluções Blockbit, este guia tem como principal objetivo o fornecimento de informações a respeito da configuração e realização do gerenciamento do Blockbit GSM.

Antes de prosseguir com a instalação, verifique os requisitos de instalação.

Lembre-se que oferecemos suporte total por meio de nossos parceiros e de nossos canais de atendimento, que terão a maior satisfação em atendê-lo.

Requisitos de instalação

Certifique-se de que a comunicação com a internet está ativa, pois, os processos de licenciamento, atualização do sistema e das bases de dados necessitam de conexão com a internet.

Requisitos mínimos para instalação da Manager:

- **Processamento:** Quad Core (BB 1000);
- **Memória:** 16 GB RAM;
- **Storage:** 128GB;
- **Plataforma de virtualização:** VMware, XenServer ou KVM.

Requisitos mínimos para instalação do Analyzer Remoto:

- **Processamento:** Octa Core (BB 1000);
- **Memória:** 32GB RAM;
- **Storage 1:** 128 GB;
- **Storage 2:** 256 GB (desejável Raid c/ Discos SSD ou SAS);
- **Plataforma de virtualização:** VMware, XenServer ou KVM.

Requisitos mínimos para instalação do GSM + Analyzer Interno:

- **Processamento:** Octa Core (BB 2000);
- **Memória:** 32GB RAM (avaliar aumentar conforme projeto);
- **Storage 1:** 128 GB;
- **Storage 2:** 256 GB (desejável Raid c/ Discos SSD ou SAS);
- **Plataforma de virtualização:** VMware, XenServer ou KVM.

Para executar a instalação e a configuração é necessário um cliente *SSH*, console serial e um navegador *web*. Seguem abaixo as aplicações mínimas recomendadas:

Navegador Web:

- *Mozilla Firefox* versão 45; ou
- *Google Chrome* versão 51; ou
- *Microsoft Internet Explorer* 9.

Acesso remoto (SSH e Console):

- *PUTTY*;
- *CygWin*;
- *Mobaxterm*.

Sobre o Guia do Administrador

Este guia foi desenvolvido especialmente para você administrador, todas as seções foram estruturadas de modo a tornar o processo de instalação fácil e rápido. Todo o passo a passo é apresentado com exemplos, facilitando a compreensão e esclarecendo dúvidas.

No decorrer do guia, você poderá encontrar alguns símbolos seguidos de texto, eles têm o objetivo de alertá-lo sobre uma importante observação ou nota referente àquela seção.

Vamos conhecer esses símbolos:

- **Alerta:** Refere-se a observações ou notas que devem ser seguidas por você com muita cautela durante o processo de instalação do Blockbit UTM:



Exemplo de uma mensagem de Alerta.

Símbolo – "Alerta"

- **CLI - Command Line Interface:** Também conhecido como Shell, refere-se aos comandos que devem ser digitados, ao lado desse símbolo estará disposto o comando a ser digitado:

Linha de Comando

Exemplo de uma Linha de Comando.

Símbolo – CLI – Command Line Interface

- **Dica:** Refere-se a sugestões que tem como função facilitar o processo de instalação do Blockbit UTM:



Exemplo de uma mensagem de dica.

Símbolo – "Dica"

- **Nota:** Refere-se a observações ou notas que tem como função auxiliar o processo de instalação do Blockbit UTM:



Exemplo de uma mensagem de Nota.

Símbolo – "Nota"

- **Informações:** Refere-se a informações adicionais a respeito do Blockbit UTM:



Exemplo de uma mensagem de Informações.

Símbolo – "Informações"

GSM - ARQUITETURA

Esta seção irá apresentar a Arquitetura do Blockbit GSM.

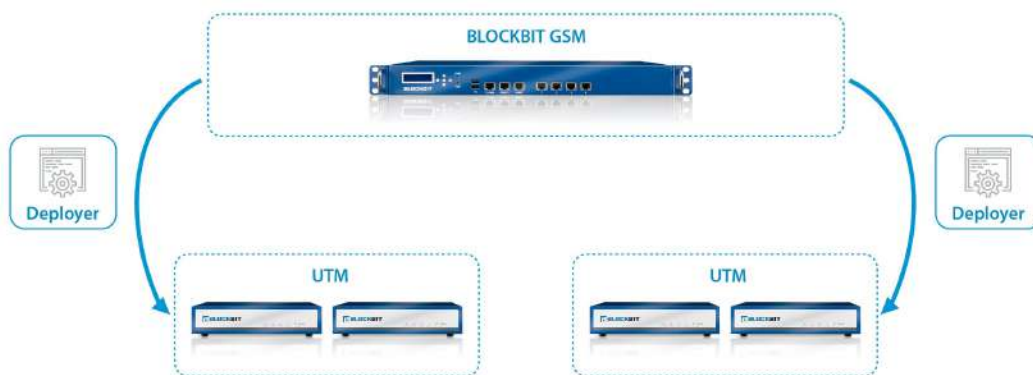
A arquitetura é apresentada por um conjunto de camadas de componentes que, integradas, definem os aspectos técnicos relativos aos serviços oferecidos pelo sistema.

Plataforma

Para compreender a Arquitetura é necessário entender a finalidade do Blockbit GSM e como os dispositivos se comunicam.

O Blockbit GSM - *Global Security Management* - Gerenciamento Global de Segurança foi desenvolvido para gerenciar as múltiplas soluções da Blockbit. Ao conectar um dispositivo Blockbit UTM ao Blockbit GSM é estabelecido um Túnel seguro utilizando comunicação criptografada, possibilitando a aplicação das configurações geradas.

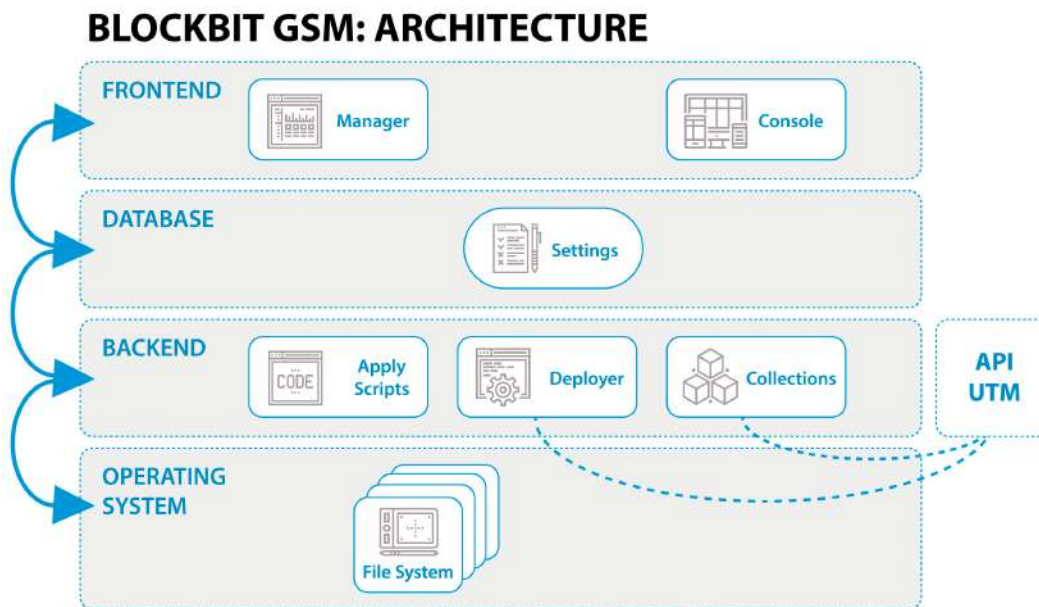
Todas as configurações aplicadas através do Blockbit GSM são geradas em pacotes de arquivos sendo que estes são exportados e implementadas no Blockbit UTM.



Arquitetura – Plataforma Blockbit GSM.

Arquitetura

A arquitetura do Blockbit GSM foi desenvolvida para que o sistema simplifique a gestão centralizada de dispositivos.



Blockbit GSM – Architecture.

A arquitetura é dividida no seguinte modelo de componentes:

- *Frontend*;
- *Backend*;
- Armazenamento de Dados;
- Sistema Operacional.

A seguir explicaremos estes modelos de componentes.

Arquitetura – *Frontend*

Frontend é a camada de desenvolvimento que disponibiliza a interface de apresentação e controles do sistema. Com os recursos de *Frontend* é possível ter acesso a qualquer tipo de informação e executar comandos de configuração nos serviços do Blockbit GSM.

As interfaces da camada de *Frontend* garantem que o usuário final não tenha acesso direto aos demais componentes disponibilizados em outras camadas da arquitetura do sistema.

O sistema foi projetado para oferecer dois tipos de interface na camada de *Frontend*: *Manager* e *Console*:

- **Manager:** É uma aplicação *Web* para administração dos dispositivos. É através dela que o administrador define todos os parâmetros de configurações do sistema e gerencia os pacotes de configurações que serão instalados nos dispositivos remotos;
- **Console:** Interface de linha de comandos administrativos para detecção e solução de problemas no dispositivo Blockbit GSM. Esta interface de *Frontend* pode ser acessada através de conexão por um terminal *SSH*.

Arquitetura – *Backend*

Backend é a camada de desenvolvimento que disponibiliza os comandos e programas que aplicam as configurações solicitadas através das interfaces de *Frontend* aos serviços de gerenciamento centralizado e ao Sistema Operacional.

Como o sistema possui uma característica modular com serviços independentes entre si, as informações entre os recursos da *Frontend* e da *Backend* são transportadas através de dois caminhos criptografados e autenticados por chave: Banco de Dados ou Conexão *SSH*.

- **ApplyScripts:** A principal função dos *ApplyScripts* é ler os parâmetros de configurações armazenados no banco de dados e reescrever essas configurações nos serviços e sistema operacional;
- **Deployer:** É o serviço responsável por instalar os pacotes de configurações gerados através da *Manager* nos dispositivos remotos. O *Deployer* é uma aplicação de *Backend* que utiliza a *API* pública implementada no Blockbit UTM;
- **Collectors:** São serviços de *Backend* que utilizam a *API* do Blockbit UTM para sincronizar informações dos dispositivos. Informações como por exemplo: Licença, Usuários, Placas de Rede, etc.



A solução conta com mecanismo de indexação de logs, permitindo assim uma busca acelerada de eventos, sem a necessidade de abertura de arquivos de logs mais antigos, e também com integração com o SIEM. Suporta também a troca automática de arquivo de Log, de maneira regular ou através do tamanho do arquivo.

Em caso de falha da comunicação entre o appliance de segurança Blockbit e a solução gerenciamento Centralizado e armazenamento de logs (GSM) é realizada uma retenção temporária dos logs no Blockbit até que a comunicação seja restabelecida.

Armazenamento de Dados

A camada de armazenamento de dados é a camada intermediária que oferece os recursos para armazenamento e transferência de informações entre os componentes da *Frontend* e da *Backend*. É através do sistema de banco de dados que a *Frontend* escreve as configurações e parâmetros do sistema para que sejam aplicados nos componentes da *Backend* e Sistema Operacional.

Sistema Operacional

O Sistema Operacional do Blockbit GSM também é mantido pela equipe de pesquisa e desenvolvimento da Blockbit, onde são disponibilizados os pacotes de ferramentas de código aberto utilizadas na implementação dos serviços.

Para simplificar a compatibilidade com os *Appliances* e garantir um bom desempenho na execução dos serviços, o Blockbit GSM é executado em um Sistema Operacional com *Kernel Linux* baseado em arquitetura *Intel x86*.

GSM - INSTALAÇÃO

Esta seção irá apresentar o passo a passo para instalação do Blockbit GSM.

O Blockbit GSM está disponível somente em Máquinas Virtuais compatíveis com as seguintes soluções: *VMware*, *XenServer* e *KVM*.

Para realizar a instalação do Blockbit GSM siga as orientações a seguir.

- [Importando a Máquina Virtual](#);
- [Iniciando Máquina Virtual - Primeiro Acesso](#).

GSM - Importando a Máquina Virtual

Realize o download da OVA - Open Virtual Appliance do Blockbit GSM em nosso site: <http://www.blockbit.com>

Iremos demonstrar a instalação utilizando o software VMware ESXi 6.5.0 como exemplo:

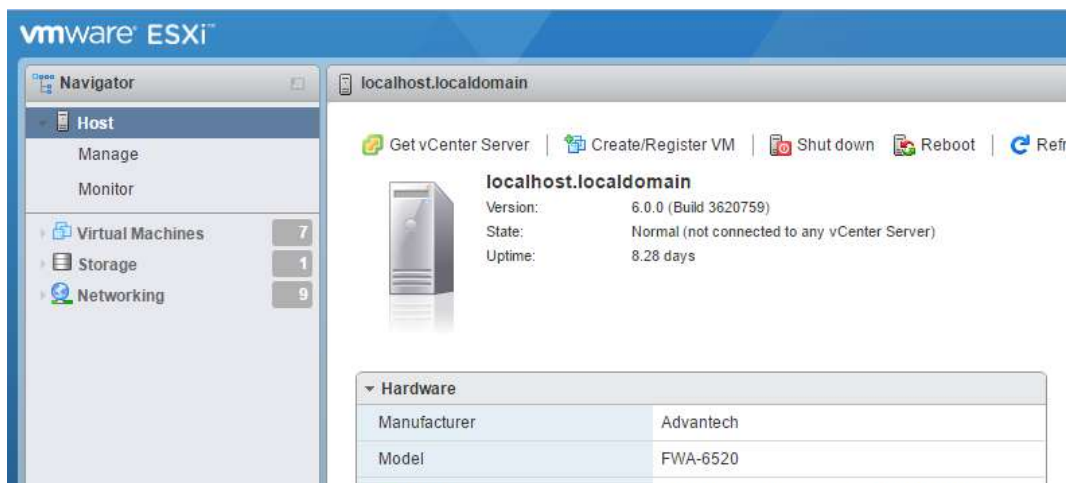
1. Conecte no navegador de internet de sua preferência e acesse a console de gerenciamento do VMware ESXi no VMware Host Client;
2. Preencha os campos com as seguintes informações:
 - **User name:** Usuário cadastrado no VMware;
 - **Password:** Senha do usuário;



Login VMware

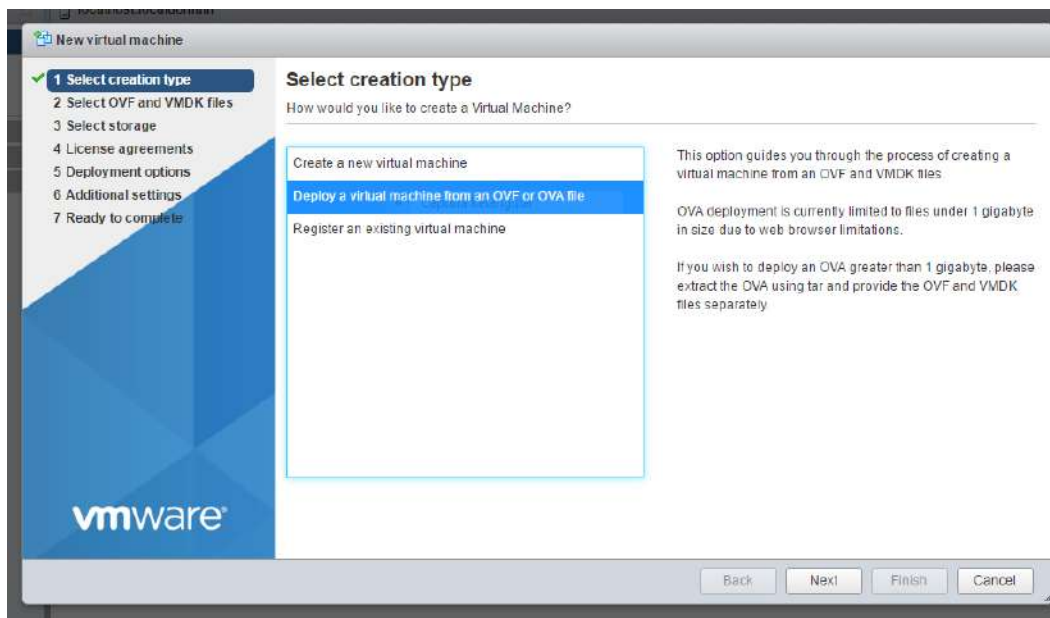
- Clique no botão "Log in".

3. Clique em "Create/Register VM";



Console VMware

4. Selecione a opção “Deploy a virtual machine from an OVF or OVA file”;

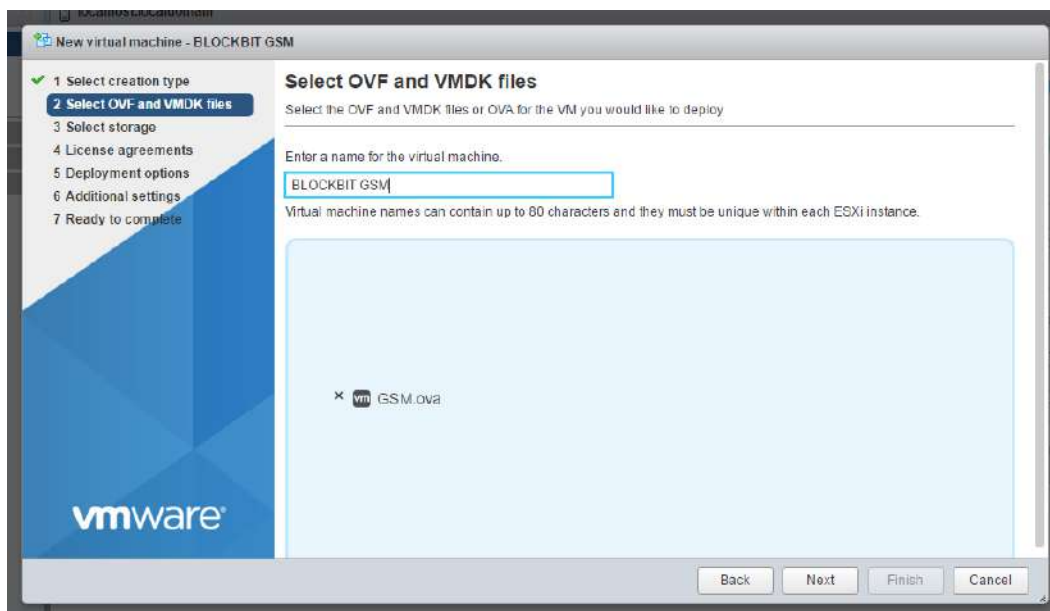


Select creation type

Clique no botão “Next”.

5. Selecione a imagem do Blockbit GSM que foi realizado o *download* no site da Blockbit e digite no campo:

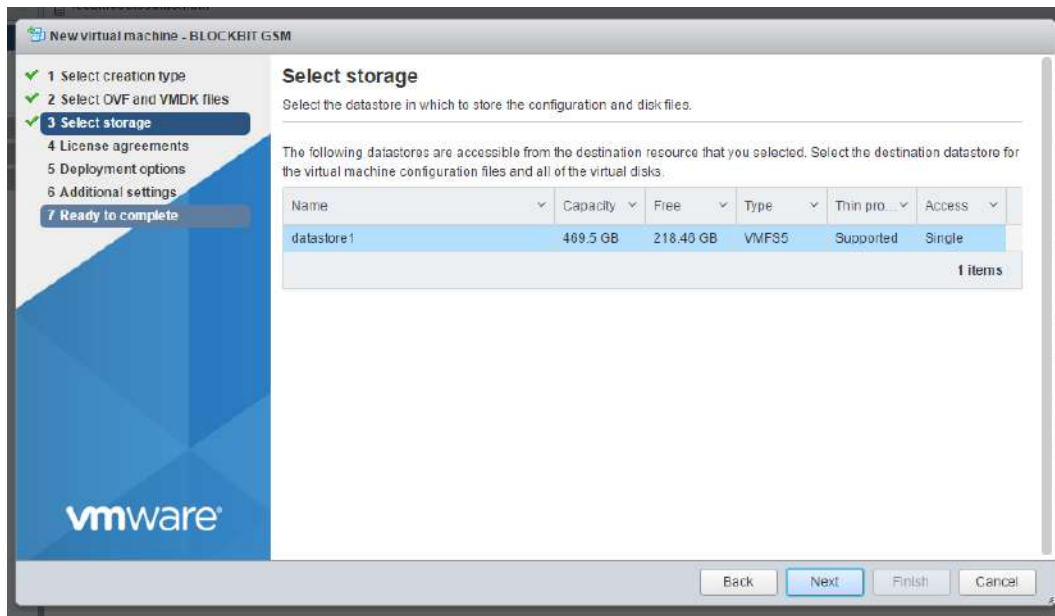
- **Enter a name for the virtual machine:** Inserir o nome da máquina. Ex.: Blockbit GSM;



Select OVF and VMDK files

- Clique no botão "Next".

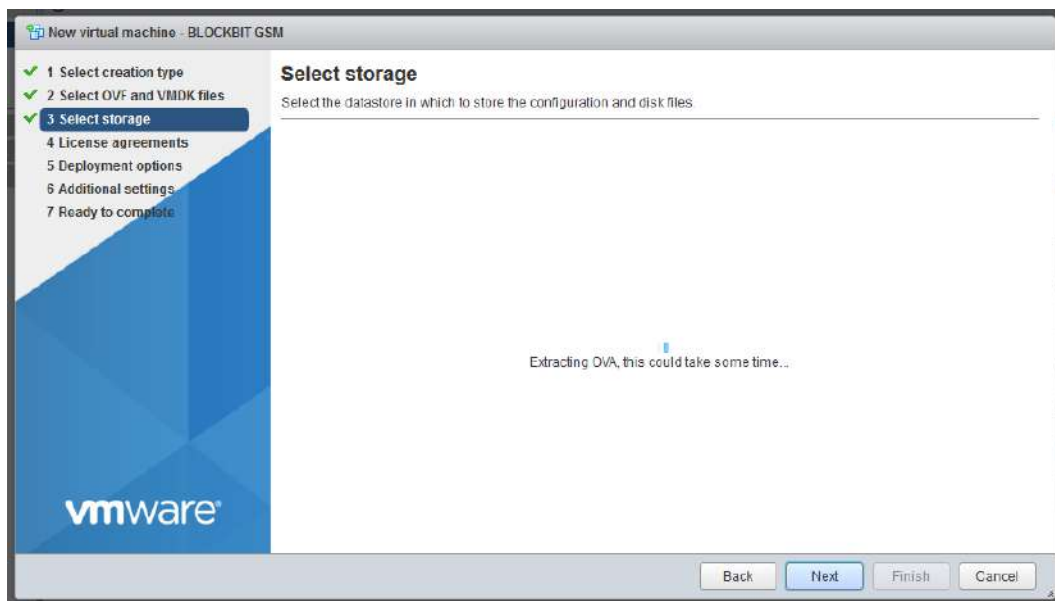
6. Selecione o *storage* desejado. Ex.: *datastore1*;



Select Storage

Clique no botão "Next";

7. Aguarde o *upload* da OVA. Enquanto ocorre o *upload*, aparecerá a seguinte mensagem: "Extracting OVA, this could take some time...";

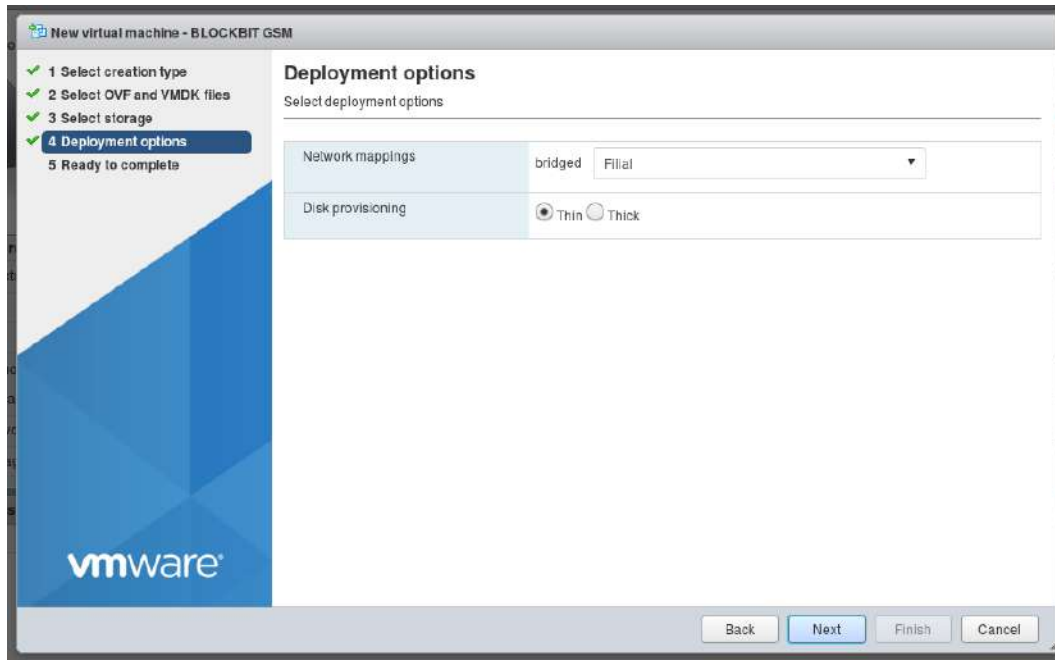


Select storage – "Extracting OVA, this could take some time..."

8. Defina as configurações da máquina virtual:

- **Network mappings:** Define o modo de rede adequado ao seu ambiente. Ex.: *Mode bridged*;
- **Disk provisioning:** Define a opção de sua preferência. Ex.: *Thin*;
- **Disco Thick:** São discos totalmente alocados no *datastore*, ou seja, se você criar um disco *Thick* com 32GB, ele irá ocupar 32GB do seu *datastore* ;
- **Disco Thin:** É um tipo de disco que aloca apenas o espaço que é gravado pelo sistema operacional da máquina virtual, por exemplo, se você criar um disco de 32GB para uma *VM*, inicialmente ele irá ocupar apenas alguns KB/MB no *datastore*, porém, no momento que você começar a gravar dados no mesmo através do sistema operacional, o tamanho dele pode chegar até o limite de 32GB.

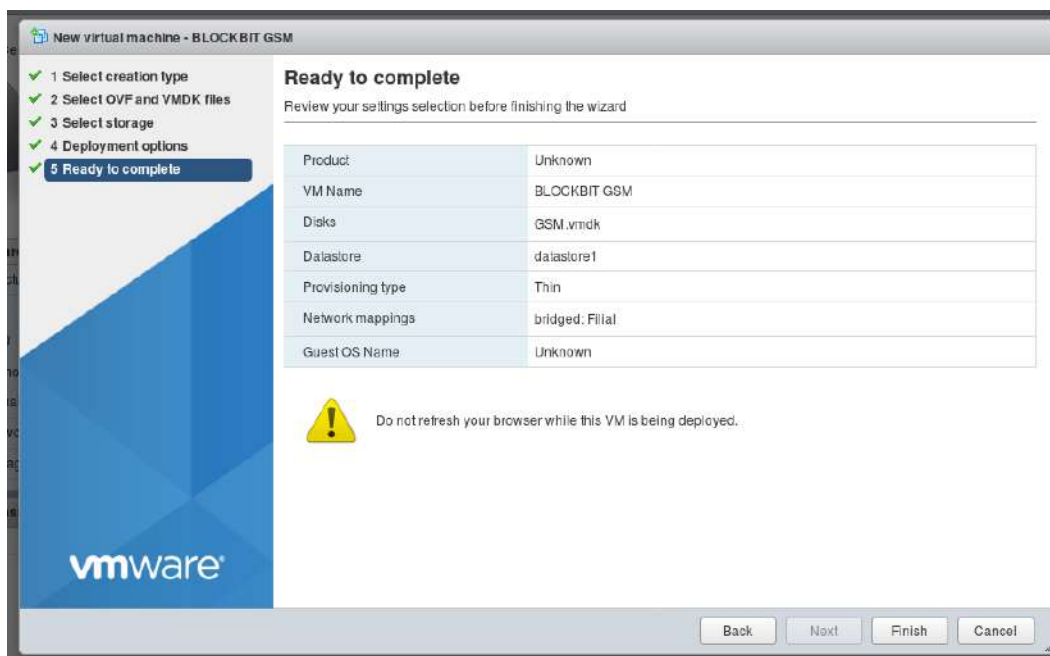
Para maiores informações consulte o manual do *VMware*.



Deployment options

Clique no botão "Next".

9. Revise as configurações definidas antes de finalizar *upload*;



Ready to complete

Clique no botão "Finish".

A importação foi concluída, basta clicar no botão "Power on" para iniciar a máquina virtual e seguir para instalação do Blockbit GSM.

Iniciando Máquina Virtual - Primeiro Acesso

Ao iniciar a máquina virtual pela primeira vez, será exibida a seguinte tela:

```
BLOCKBIT GSM 2.0
.
..
...
Setting up swapspace version 1, size = 1145852 KiB
LABEL=accessdenied, UUID=cc84ebd4-2e08-488a-a2bf-3f497b476c35
Command successful.
Command successful.
Command successful.

Install system. Wait!
_200MiB 0:00:11 [ 799kiB/s] [=====>] 1 27% ETA 0:00:28
```

Iniciando o Blockbit GSM pela primeira vez

Não é necessário realizar nenhum passo, apenas aguardar até a liberação da tela de *login*.

```
BLOCKBIT GSM 2.0

localhost login:
```

Tela de *login* – Blockbit GSM

Agora será necessário configurar o *IP*. Para configurar o *IP*, realize os seguintes passos:

1. **Localhost login:** Efetue o *login* através da console *CLI*, utilizando-se das credenciais padrão, sendo estas: Usuário “admin” e senha “admin”;
2. Altere o endereço *IP* do Blockbit GSM.



O endereço *IP* padrão do Blockbit GSM é 192.168.1.1. Neste guia utilizaremos o endereço *IP* 172.16.102.235 como exemplo. Caso deseje alterar, siga os passos a seguir:

Detalhes da configuração:

IP: 172.16.102.235 **máscaras:** 255.255.254.0

Rota padrão: 172.16.102.1

Digite os comandos:

```
ifconfig eth0 172.16.102.235/23 up
route add default gw 172.16.102.1 dev eth0
```

Após realizar esse procedimento o endereço *IP* foi alterado.

Para garantir a segurança do ambiente iremos realizar a alteração da senha padrão.



É altamente recomendada a alteração da senha padrão do usuário "admin" de console. Para alteração da senha padrão, é necessário criar uma senha segura. Esta senha deve conter no mínimo 8 caracteres com letras maiúsculas e minúsculas, números e caracteres especiais.

Para alterar a senha, digite o comando abaixo:

```
Digite o comando "passwd", e digite "Enter"  
Digite a senha atual, e digite "Enter"  
Digite a nova senha duas vezes.
```

Após realizar esse procedimento a senha foi alterada com sucesso.

GSM - CONFIGURAÇÃO DE EXCEÇÃO

Esta seção irá apresentar como realizar a configuração de exceção nos navegadores web: *Google Chrome*, *Mozilla Firefox* e *Microsoft Internet Explorer*.

Ao realizar o primeiro acesso a Interface Web do Blockbit GSM é normal os *browsers* retornarem a emissão de um alerta de segurança informando um erro de certificado. Isso ocorre porque o *browser* não reconhece nenhuma autoridade certificadora que valide o acesso a esta página como confiável. Portanto, é necessário realizar a configuração de exceção no navegador web. Siga os passos a seguir:

1. Para acessar a interface web, utilize um navegador recomendado;
2. Conecte no navegador de *internet* e acesse o endereço: <https://192.168.1.1>. Caso tenha alterado o endereço IP, utilize o IP alterado.



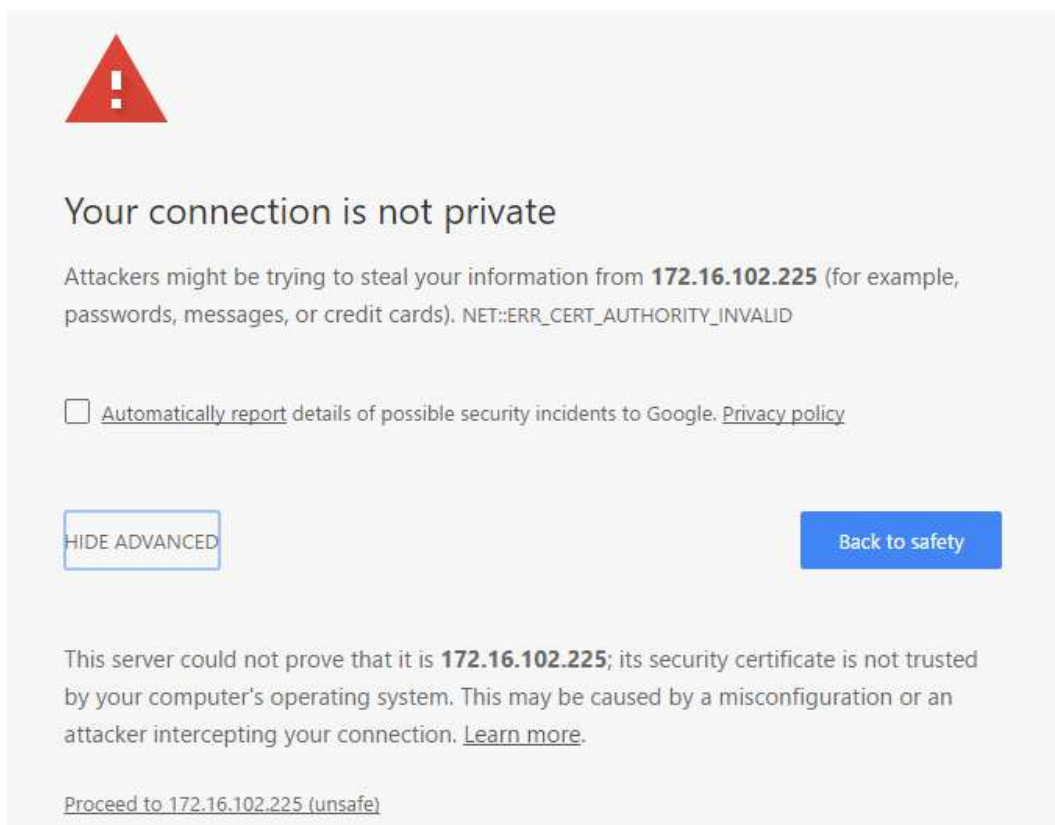
Em caso de o Browser emitir um **ALERTA DE SEGURANÇA**, siga as recomendações abaixo.

Cada *Browser* possui um procedimento para liberar a conexão como confiável. Siga as orientações de como proceder.

Configurando exceção no *Google Chrome*

Para configurar a exceção no *Google Chrome* siga os seguintes passos:

1. Clique no botão "*Hide Advanced*";
2. Clique no botão "*Proceed to 172.16.13.202 (unsafe)*" para aceitar esta página como confiável.



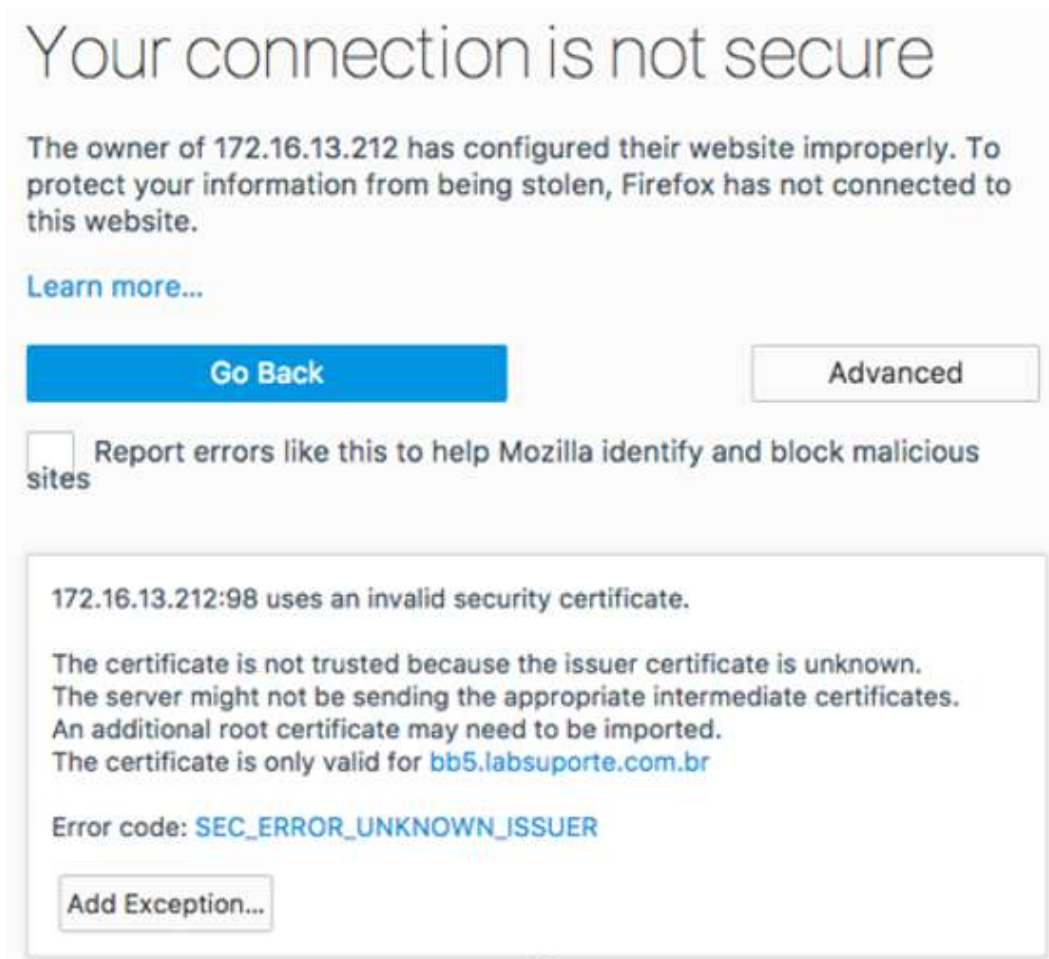
Exceção *Chrome* – "*Proceed to 172.16.32.212 (unsafe)*"

A configuração de exceção no *Google Chrome* foi realizada com sucesso.

Configurando exceção no *Mozilla Firefox*

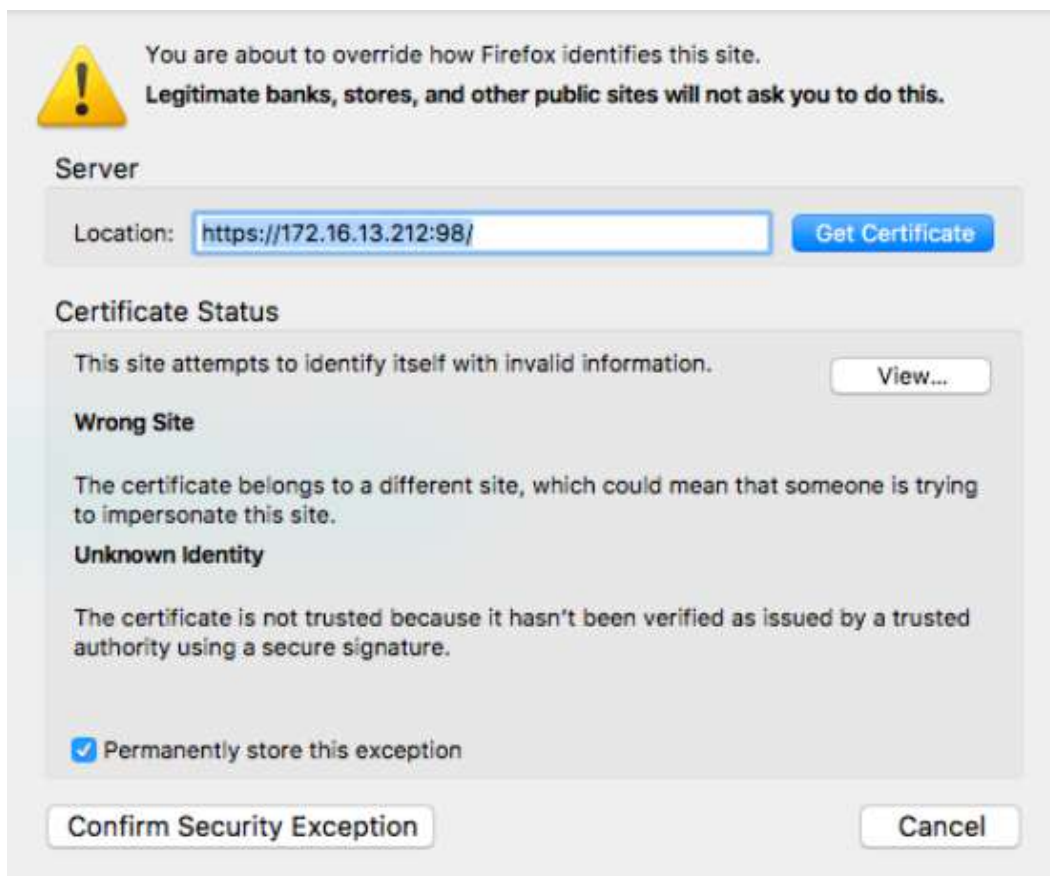
Para configurar a exceção no *Mozilla Firefox* siga os seguintes passos:

1. Clique no botão "Advanced";
2. Clique no botão "Add Exception...";



Exceção Mozilla Firefox – Your connection is not secure

3. Clique no botão "Confirm Security Exception".



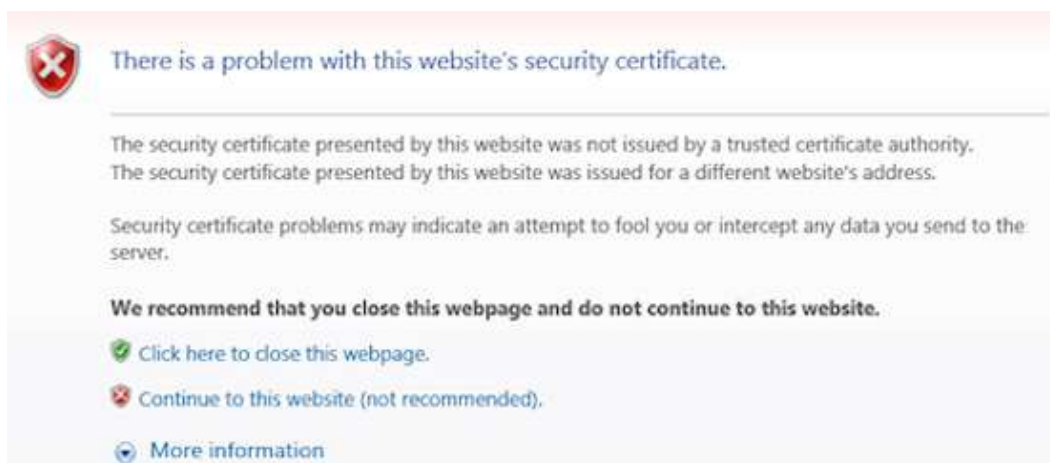
Exceção Mozilla Firefox – Confirm Security Exception

A configuração de exceção no Mozilla Firefox foi realizada com sucesso.

Configurando exceção no Microsoft Internet Explorer

Para configurar a exceção no Microsoft Internet Explorer siga os seguintes passos:

1. Clique no botão "Continue to this web site (not recommended)".



Exceção Microsoft Internet Explorer – There is a problem with this website's security certificate

A configuração de exceção no *Microsoft Internet Explorer* foi realizada com sucesso.

GSM - ASSISTENTE DE INSTALAÇÃO

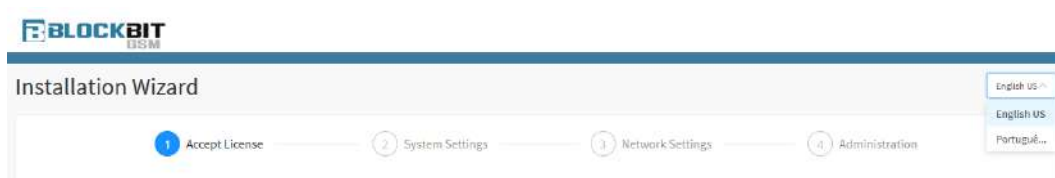
Esta seção irá apresentar como configurar o Assistente de Instalação do Blockbit GSM.

Para realizar a instalação do Assistente de Instalação (*Installation Wizard*), são necessários quatro passos: *Accept License*, *System Settings*, *Network Settings* e *Administration*. Siga as orientações a seguir.

Escolha do idioma

É possível selecionar o idioma de sua preferência (*English US* ou *Português BR*). O idioma padrão é *English US*. Para alterar o idioma:

1. Clique no botão no canto superior direito "*English US*" e escolha o idioma desejado;



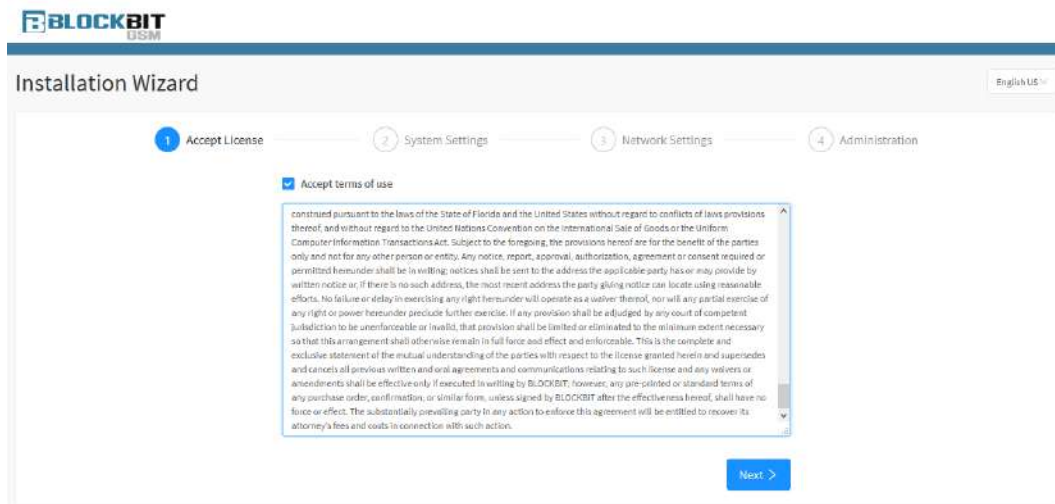
Installation Wizard – Seleção do idioma.

Ao definir o idioma, sua interface será atualizada com o idioma escolhido.

Processo de Instalação

A seguir vamos exemplificar o passo a passo de instalação do assistente:

1. **Accept License:** Apresenta os termos de uso do Blockbit GSM. Leia o termo e selecione o checkbox: "*Accept terms of use*";

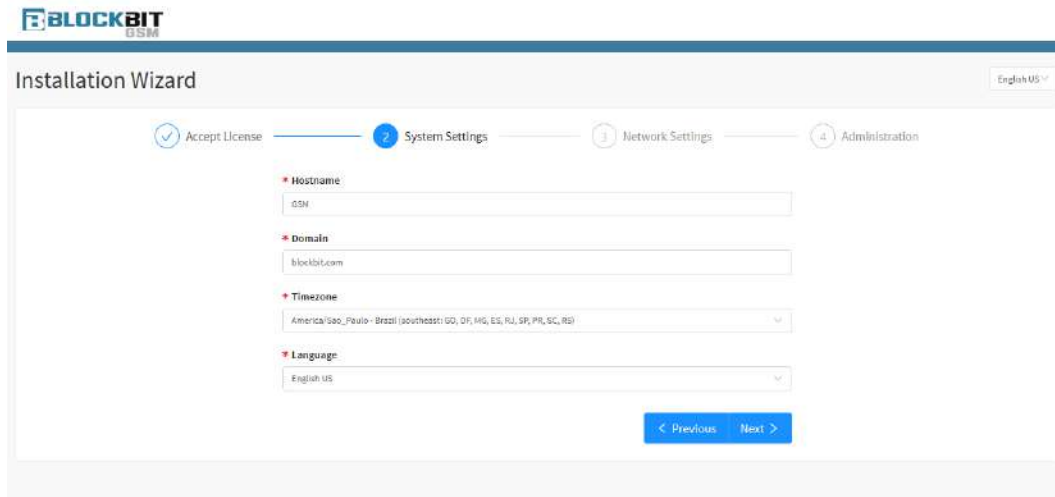


Installation Wizard – Accept License.

Clique no botão **Next** [Next >].

2. **System Settings:** Preencha os campos com as seguintes informações:

- **Hostname:** Nome do *Hostname*. Pode ser qualquer um desde que esteja conforme padrão *FQDN* - *Fully Qualified Domain Name*. Ex.: GSM;
- **Domain:** Domínio da rede. Ex.: blockbit.com;
- **Timezone:** Selecionar o fuso horário no qual sua empresa se encontra. Ex.: America/Sao_Paulo;
- **Language:** Selecionar o idioma padrão. Ex.: *English*;



Installation Wizard – System Settings.

- Clique no botão **Next** [Next >] para prosseguir ou em **Previous** [< Previous] para voltar ao menu anterior.

3. **Network Settings:** Preencher os campos com as seguintes informações:

- **Interface:** Selecione a interface de rede que deseja configurar. Ex.: eth0;
- **IP Address:** Defina o endereço IP adequado a rede. Ex.: 172.16.102.235;
- **Netmask:** Defina a máscara de rede. Ex.: 255.255.0.0;
- **Gateway:** Defina a rota padrão da rede. Ex.: 176.16.102.1;
- **DNS Server 1:** Defina o servidor *DNS* da rede ou da *internet*. Ex.: 172.31.102.184;
- **DNS Server 2:** Defina o *DNS* secundário da sua rede ou da *internet*. Ex.: *DNS* secundário do Google 8.8.4.4;
- **NTP Server 1:** Defina o servidor de sincronização de relógio. Ex.: a.ntp.br;
- **NTP Server 2:** Defina o servidor secundário de sincronização de relógio. Ex.: b.ntp.br.

BLOCKBIT GSM

Installation Wizard

English US

1 Accept License — 2 System Settings — 3 Network Settings — 4 Administration

* Interface
eth0

* IP Address
172.16.102.235

* Netmask
255.255.0.0

* Gateway
172.16.102.1

* DNS Server
172.31.102.104

DNS Server
8.8.4.4

* NTP Server
8-ntp.br

NTP Server
8-ntp.br

< Previous Next >

Installation Wizard – Network Settings.



É imprescindível que o BLOCKBIT GSM e os BLOCKBIT UTM estejam sincronizados pelos mesmos servidores NTP.

Next >

< Previous

- Clique no botão **Next** [Next >] prosseguir ou em **Previous** [< Previous] para voltar ao menu anterior.

4. **Administration:** Preencher os campos com as seguintes informações:

- **Name:** Nome do administrador. Ex.: admin;
- **E-mail:** E-mail do administrador. Este e-mail será utilizado como *login* do Blockbit GSM. Ex.: admin@blockbit.com;
- **Password:** Insira uma senha com no mínimo oito caracteres. A senha deve conter letras maiúsculas, minúsculas e caracteres especiais;
- **Confirm Password:** Confirme a senha inserida acima.

BLOCKBIT GSM

Installation Wizard

English US

1 Accept License — 2 System Settings — 3 Network Settings — 4 Administration

* Name
admin

* E-mail
admin@blockbit.com

* Password

* Confirm Password

< Previous Save



O e-mail do administrador será utilizado como login do Blockbit GSM.

Save

< Previous

Clique no botão **Save** para finalizar o procedimento ou em **Previous** para voltar ao menu anterior.

Ao finalizar esses passos o Assistente de Instalação foi instalado com sucesso.

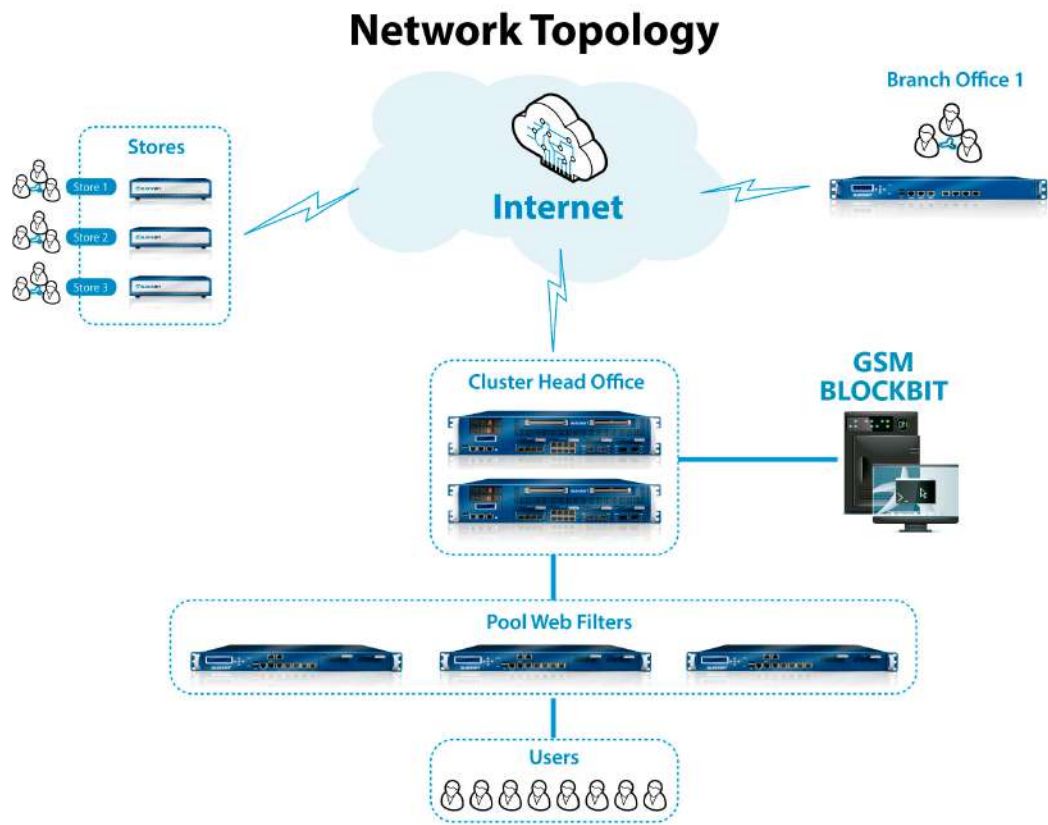
GSM - AMBIENTE DE REDE

Esta seção irá apresentar um exemplo de ambiente de rede utilizando o Blockbit GSM.

Para melhor contextualizar este Guia do Administrador, utilizaremos uma topologia fictícia, porém muito comum entre os prováveis ambientes que devem implantar o Blockbit GSM.

O Blockbit GSM tem foco em ambientes com muitas capilaridades, ou seja, ambientes grandes conectados remotamente, porém, com similaridades entre os pontos remotos, desta forma diminuindo o *TCO - Total Cost of Ownership* de administração da solução e maximizando o *ROI - Return on Investment* da empresa.

A topologia de rede abaixo é uma sugestão de implantação das soluções Blockbit para os produtos Blockbit UTM e o Blockbit GSM:



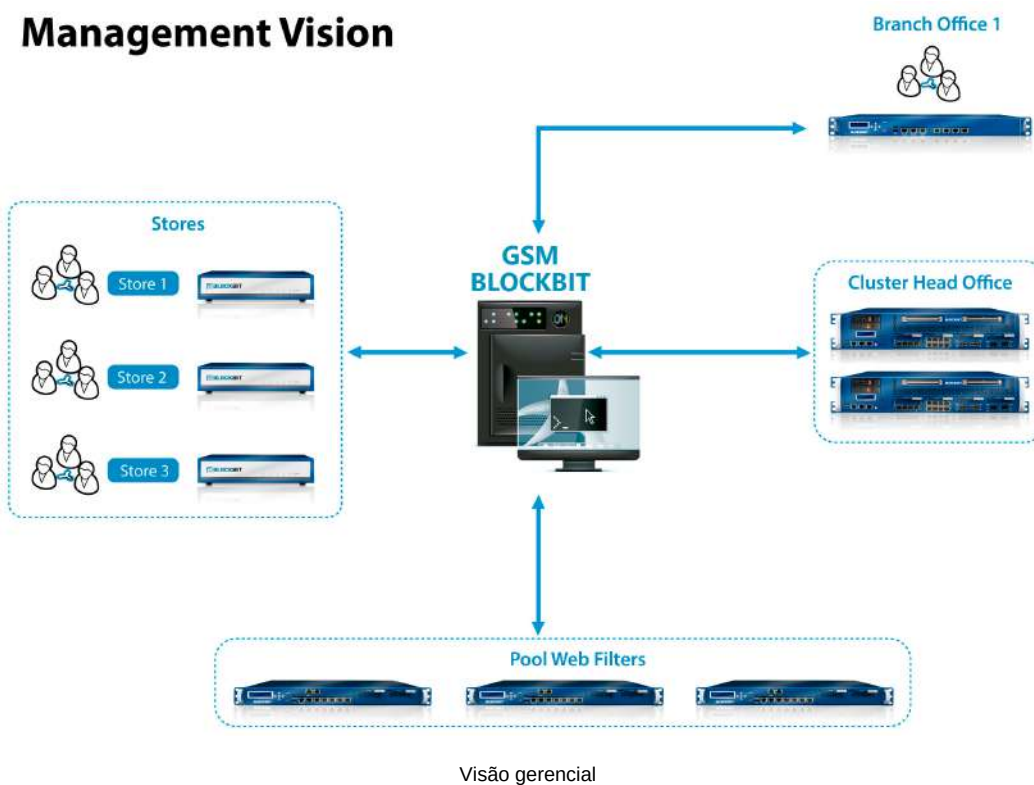
Topologia da rede

Em nosso exemplo, estaremos usando a seguinte tabela de endereços *IP*:

Endereçamento *IP*

Nome	Endereço IP externo	Rede interna/protegida	Grupo Blockbit GSM
Cluster Head Office	172.16.102.220	192.168.220.0/24	Head Office
Branch Office	172.16.102.221	192.168.221.0/24	Branch Office
Store 1	172.16.102.222	192.168.222.0/24	Stores
Store 2	172.16.102.223	192.168.223.0/24	Stores
Store 3	172.16.102.224	192.168.224.0/24	Stores
Webfilter 1	172.16.102.225	192.168.220.0/24	Pool Web Filters
Webfilter 2	172.16.102.226	192.168.220.0/24	Pool Web Filters
Webfilter 3	172.16.102.227	192.168.220.0/24	Pool Web Filters

Na imagem a seguir temos a visão gerencial com o foco no Blockbit GSM, em que ele se comunica com todas as “devices”, Blockbit UTM, que estão agrupados em 4 grupos: *Head Office*, *Branch Office*, *Pool Web Filters* e *Stores*.



Com este agrupamento é possível aplicar as configurações e políticas personalizadas para cada um dos grupos conforme suas necessidades.

GSM - NOTIFICATIONS VIA SNMP

O GSM possui o recurso de configurar o sistema para o envio de notificações por *trap SNMP*. Diferente de um serviço de coleta de dados *SNMP*, uma *Trap* é um serviço de notificações iniciado pelo servidor monitorado, isso inicia a comunicação e entrega dos alertas para o servidor *SNMP* remoto. O serviço suporta a comunicação com os protocolos *SNMP v1*, *SNMP v2* e *SNMP v3*.

No GSM, a configuração do *SNMP* é toda feita através do comando de console [enable-snmp].

Abaixo vamos detalhar um pouco sobre as diferenças das versões do protocolo *SNMP*.

• *SNMP v1*

A primeira versão do *SNMP* possui um esquema de autenticação extremamente frágil, sendo seu único mecanismo de segurança os "nomes de comunidade". Estes, representam um grupo de gerenciamento com permissões específicas, ou seja, a atribuição dos direitos de utilização das instruções *SET* e *GET* sobre um determinado parâmetro a membros desta comunidade. O armazenamento destes nomes é local, ou seja, cada agente que implementa o *SNMP* deve registrar as permissões dadas a cada comunidade de gerenciamento que pode fazer uso de seus parâmetros.

É importante notar que as permissões são dadas à determinada comunidade, e não a estações de gerenciamento específicas, de fato, não há nenhuma listagem dos membros de uma comunidade.

A "autenticação" de uma *NMS* "Network Management Station" é feita através da declaração, enviada em formato texto, do nome da comunidade a qual pertence. A *NMS*, deve, deste modo, manter uma listagem dos nomes de comunidade relevantes para cada agente da rede. Para simplificar a tarefa de gerenciamento, tende-se a manter certa uniformidade nos grupos de gerenciamento cadastrados nas várias entidades da rede, mas isto não é obrigatório.

A principal falha deste modelo de segurança reside no fato de que qualquer um que conheça o nome de comunidade com os privilégios adequados pode enviar um comando do *SNMP* pela rede. Para piorar a situação, como não há privacidade no *SNMPv1*, as informações sobre os nomes de comunidades são enviadas em forma de texto e sem encriptação nas mensagens *UDP* que trafegam na rede, é extremamente simples para um atacante interceptar estes nomes e relacioná-los às estações as quais se destinam.

Dada esta total insegurança gerada pela combinação da falta de privacidade com o modelo simples e descentralizado de autenticação, quase todas as implementações desta versão do *SNMP* em sistemas de produção desabilitam a instrução *SET*, e restringem os parâmetros acessíveis pelas instruções *GET* a informações não confidenciais. Esta atitude limita muito a funcionalidade do protocolo, mas ao mesmo tempo garante segurança nos ambientes onde ela é essencial.

• *SNMP v2*

Originalmente, uma reforma no modelo de segurança do *SNMP* era parte dos objetivos na criação da segunda versão do protocolo. O *SNMPv2* (RFC 1901, 1996) surgiu para suprir algumas das deficiências do *SNMPv1*.

Adicionou pelo menos duas novas funções:

- *Get-bulk-request*: Acesso a grandes blocos de informações em *MIBs*;
- *Inform-request*: Permite que um gerente envie informações relevantes diretamente a outros gerentes;
- Dentre as novidades do *SNMPv2*, destacam-se:
 - Gerenciamento de redes descentralizadas, permitindo a existência de mais de uma estação gerente e, conseqüentemente, a troca de informações entre elas;
 - Possibilidade de transferência de grandes blocos de informação;
 - Introdução de contadores de 64 bits, possibilitando um melhor monitoramento de variáveis que atingem seus limites rapidamente com contadores de 32 bits;
 - Melhoria no tratamento de erros das variáveis, definindo-se o estado de sucesso ou erro da operação para cada variável da *PDU* e não mais para a *PDU*. Assim, se uma variável contiver erro, as demais não serão sacrificadas, sendo o campo da variável em que ocorreu o problema preenchido com um código de erro.

A versão final do protocolo que foi normatizada foi a versão 2c, que apesar de introduzir novas funcionalidades como a instrução *"GetBulkRequest"*, não fez qualquer alteração no modelo de segurança do protocolo e o modelo baseado em nomes de comunidade se manteve.

• *SNMP v3*

Esta versão do protocolo teve como principal foco a melhoria da segurança oferecida pelas versões anteriores do protocolo *SNMP*. Foram desenvolvidos mecanismos para lidar com cada uma das falhas de segurança discutidas até então. Desta forma, se tornou possível utilizar o potencial completo do protocolo, incluindo as instruções *SET*, sem comprometer a segurança da rede. O novo modelo de segurança garante confidencialidade, integridade, autenticação e controle de acesso.

Em termos gerais, o *PDU* efetivo que carrega a instrução do *SNMP* (seja *SNMPv1* ou *SNMPv2*) é encapsulado em um *PDU* do *SNMPv3*. Esta operação provê as funções relacionadas à segurança no nível de processamento de mensagens. Para que esta comunicação seja efetiva, tanto a estação de gerenciamento, quanto os agentes devem estar utilizando a mesma *SNMP engine*.

Os dois módulos principais do modelo de segurança do *SNMPv3* são o Modelo de Segurança Baseado em Usuário (*User-based Security Model - USM*) e o Modelo de Controle de Acesso Baseado em Visões (*View-based Access Control Model - VACM*). O *USM* é encarregado de autenticar, encriptar e deciptar os pacotes *SNMP*, enquanto o *VACM* é encarregado de administrar o acesso aos dados em *MIBs*.

Para o envio das notificações por *SNMP Trap*, acesse o *painel demonstrado abaixo* e configure conforme os campos da interface e dos parâmetros de configuração do servidor *SNMP* remoto e a versão do protocolo em uso.

Para mais informações sobre a configuração, acesse a página [\[enable-snmp\]](#) onde o comando de console é detalhado mais profundamente.

Para mais informações sobre Zabbix, clique [aqui](#).

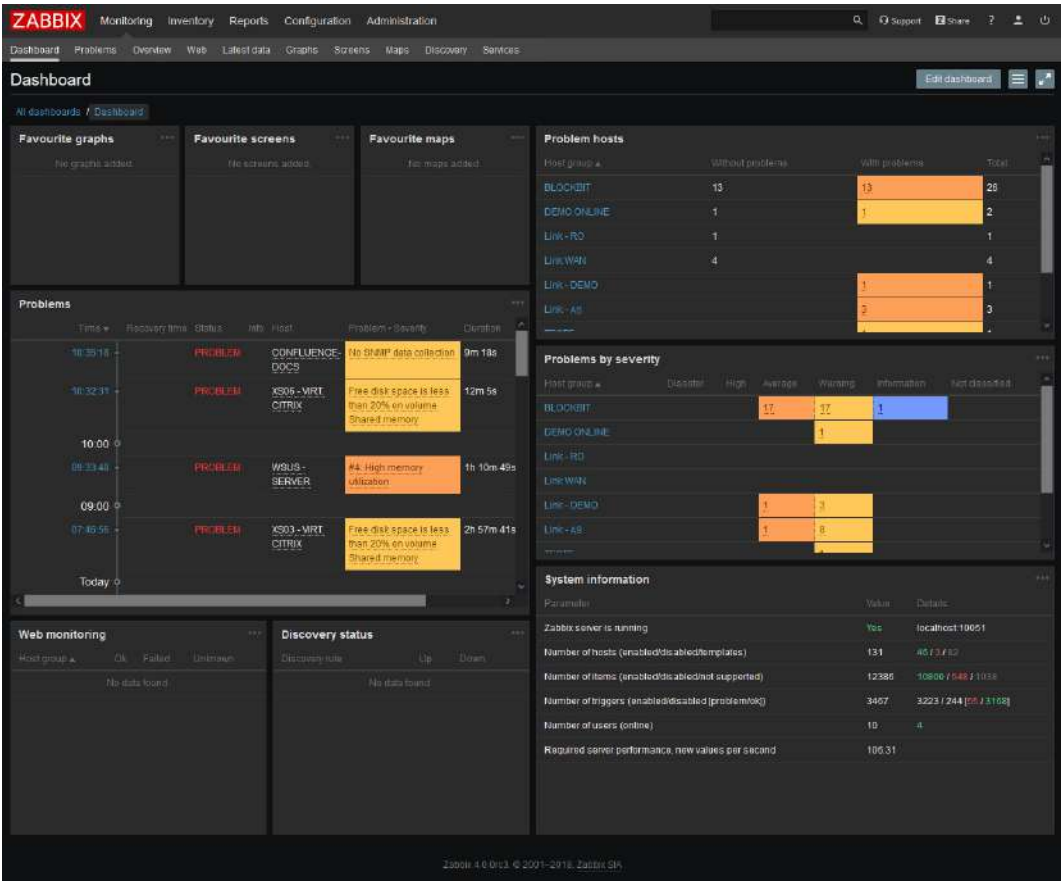
GSM - Zabbix

O *Zabbix* é um sistema open source de monitoramento que permite o acompanhamento em tempo real dos recursos da rede. Ele permite determinar *thresholds* para servir de *trigger* de eventos o que além de possibilitar a criação de uma base de alertas customizados pelo usuário, facilita a visualização e acompanhamento da infraestrutura de rede através do uso de gráficos e diagramas que são construídos em tempo real, possibilitando inclusive a criação de gráficos customizados unindo vários itens em um único diagrama.

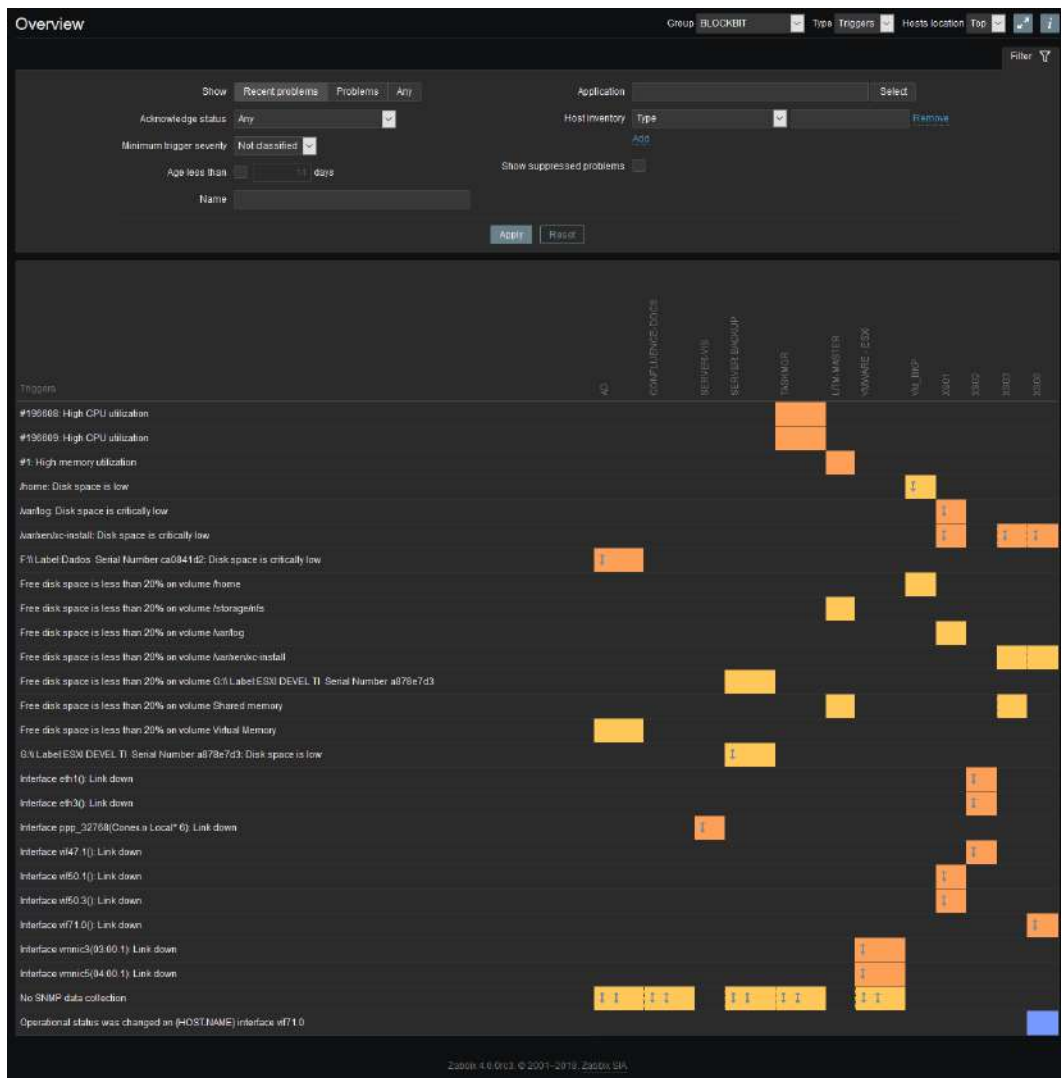
O sistema atua coletando dados de dispositivos monitorados em intervalos configurados através de agentes de proxy ou do servidor e efetua monitoramento da infraestrutura de rede, executando testes de disponibilidade e performance, usando os *triggers* determinados pelo usuário e comparando os resultados com o banco de dados *backend* do sistema.

O Zabbix contém uma gama de visualização gráfica bem extensa gerando relatórios de alto nível, histórico, mapas de rede e diversos tipos de gráficos de monitoramento criados em tempo real com base nas configurações criadas pelo próprio usuário, além de possibilitar a inclusão de diagramas personalizados de acordo com as demandas específicas da infraestrutura do usuário.

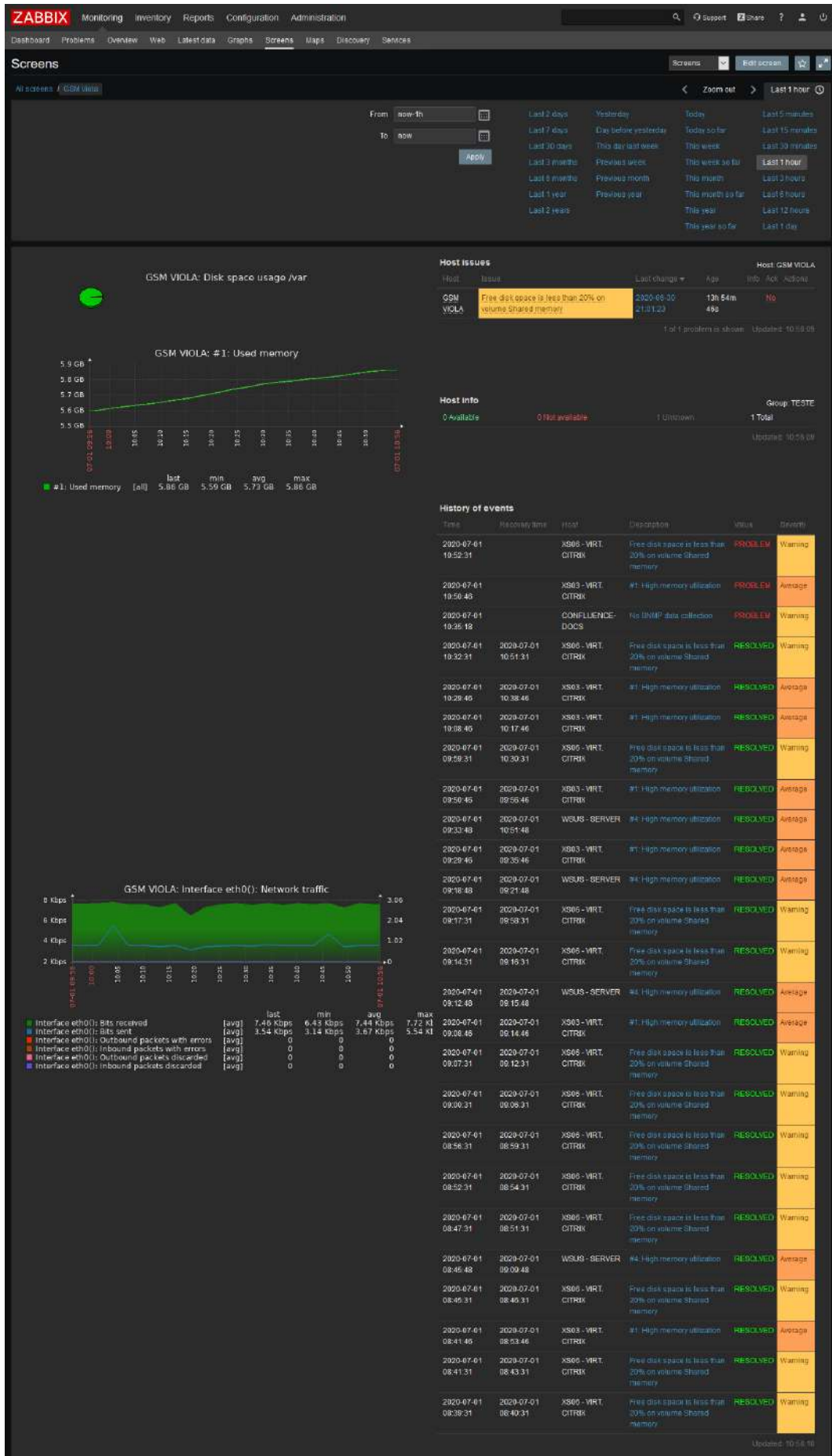
Abaixo, alguns exemplos dos recursos disponíveis no *Zabbix*:

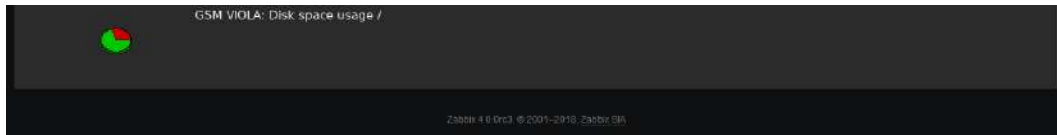


Zabbix - Dashboard

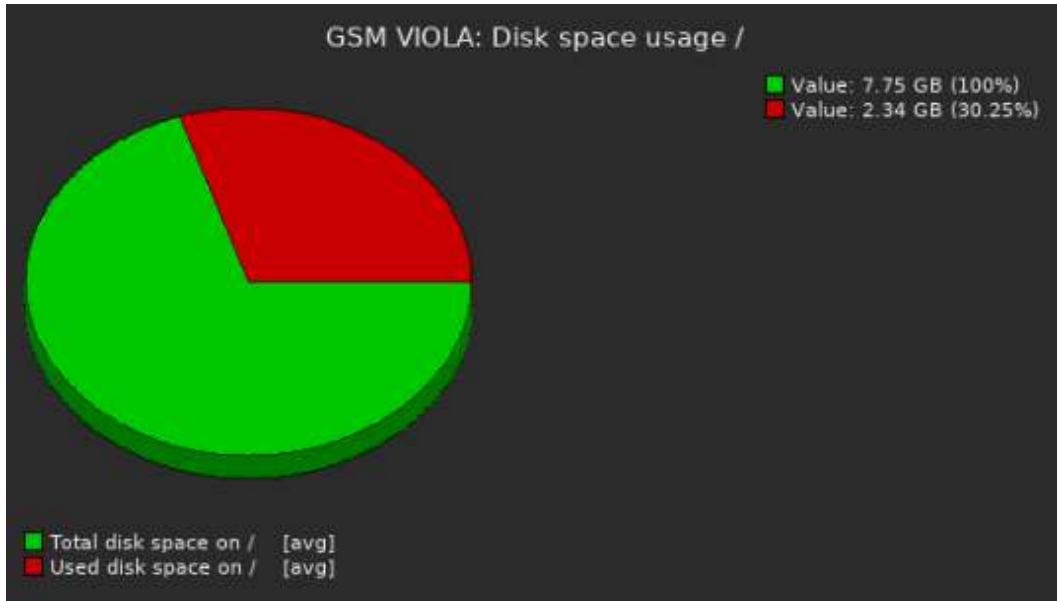


Zabbix - Overview

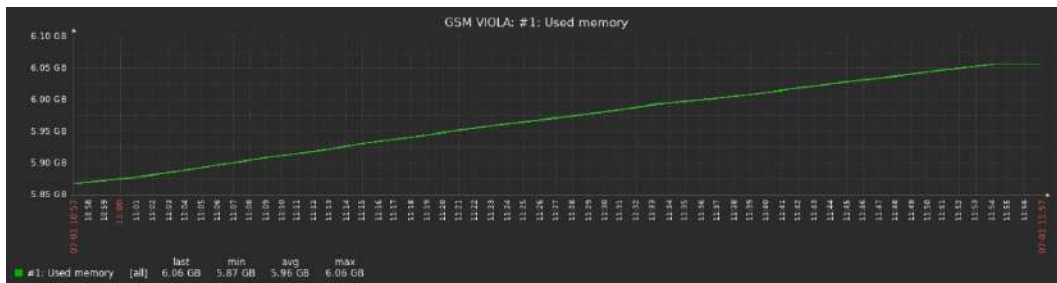




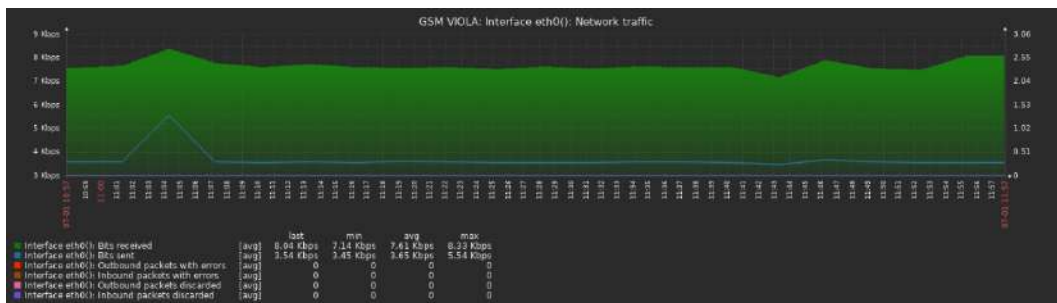
Zabbix - Screens



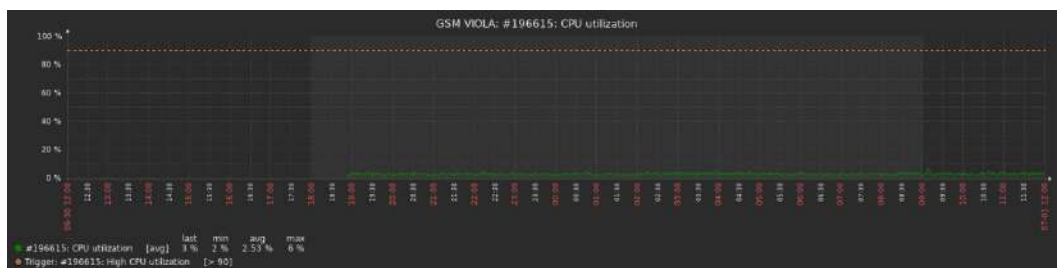
Zabbix - Disk space usage



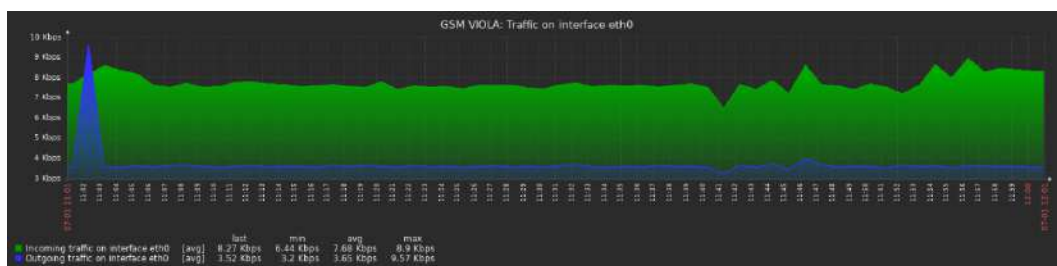
Zabbix - Used memory



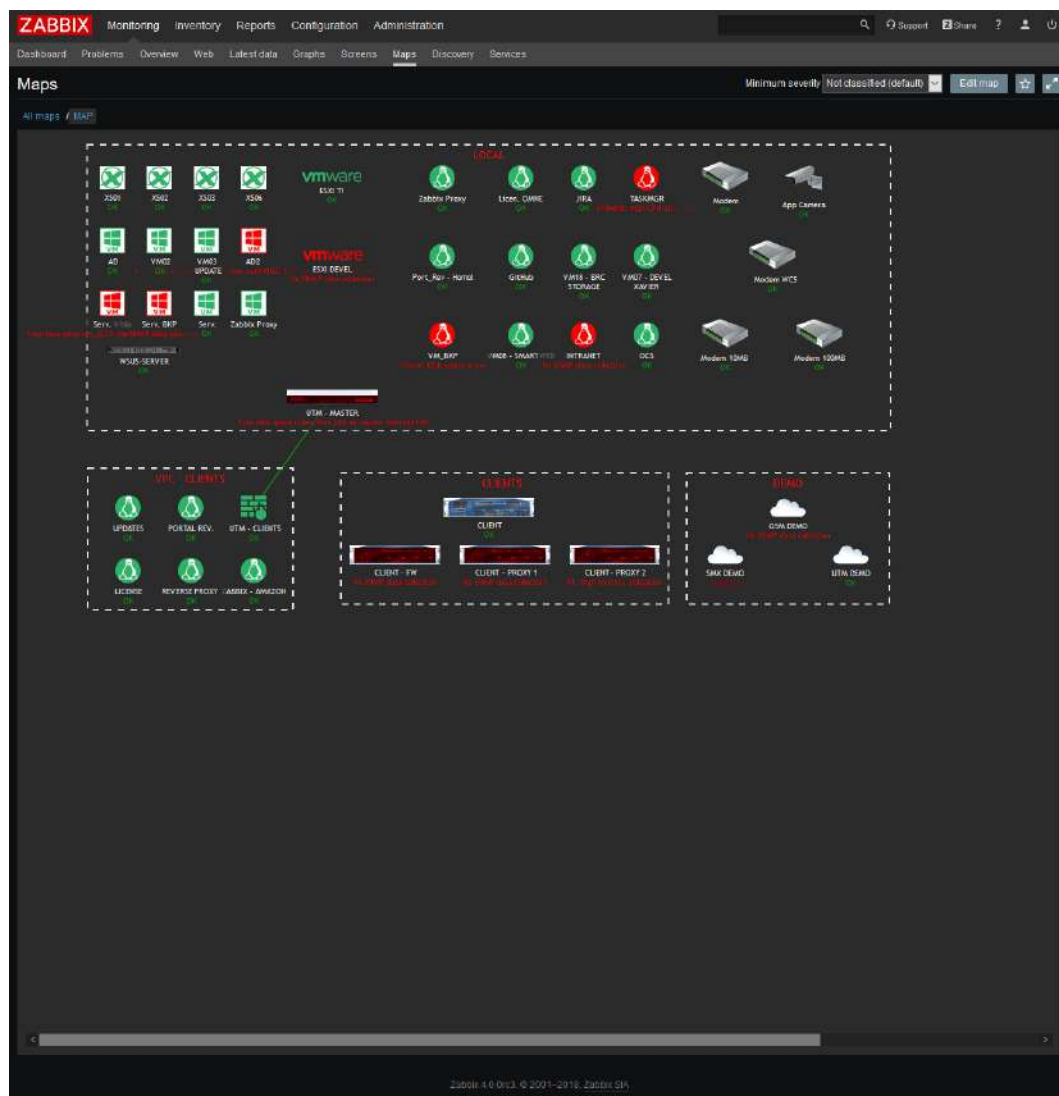
Zabbix - Network Traffic



Zabbix - CPU Utilization



Zabbix - Traffic on interface eth0



Zabbix - Network Map

A seguir, analisaremos a seção [Geomap](#).

GSM - Geomap

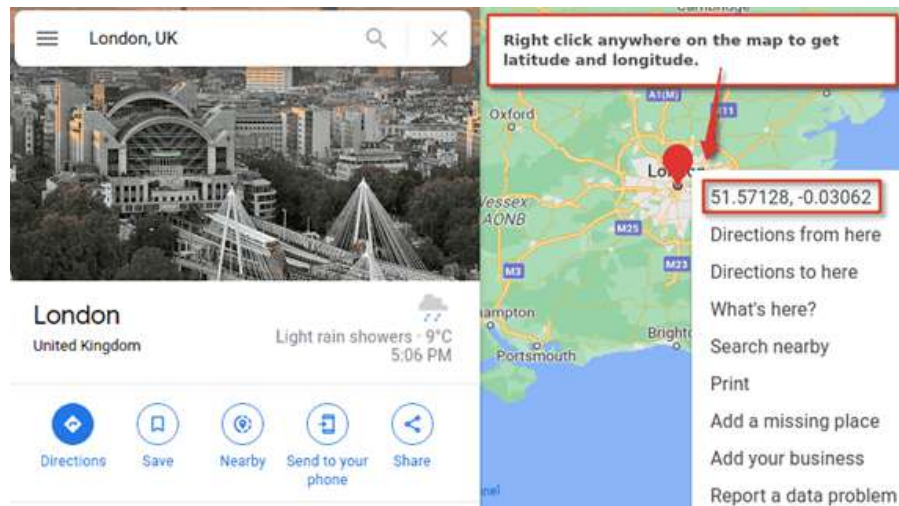
Detalhes da funcionalidade

O GSM possui o recurso chamado "Geomap" que nada mais é que a geolocalização dos ativos dispostos no sistema em tempo real.

Funcionamento

Por padrão, o Geomap exibe todos os hosts com coordenadas geográficas válidas sob o inventário de hosts. Todavia, primeiro precisamos configurar os hosts antes de seguir com a configuração do Geomap.

Por exemplo, temos UTMs em Londres, Amsterdam, Bruxelas e Frankfurt, então copiaremos/colaremos as coordenadas do Google Maps e os hosts no GSM.

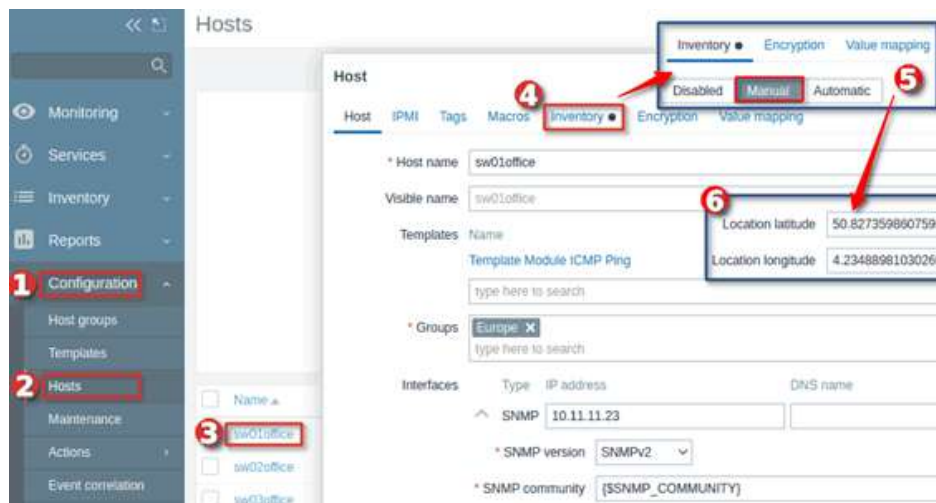


Detalhamento

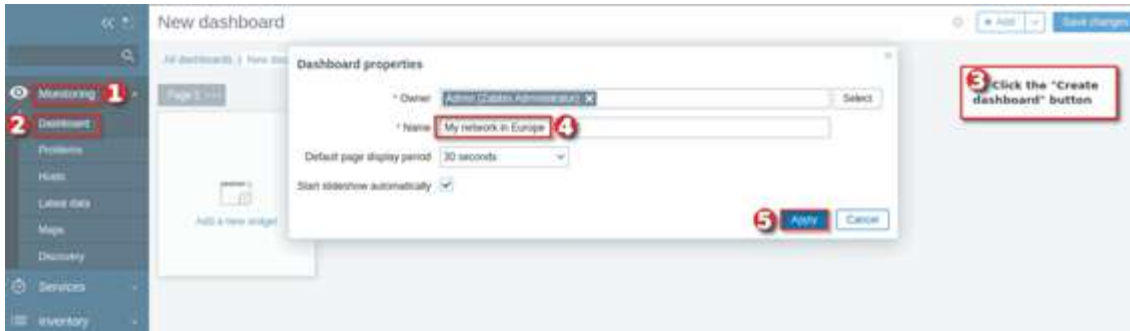
A seguir temos um passo a passo de como configurar o Geomap:

Navegue para Configuration Hosts Selecione seu Host.

Após, mude para Inventory altere o mod para "Manual" Insira as coordenadas nos campos "Location latitude" e "Location longitude", de acordo com a imagem abaixo:



Agora vá para a seção do dashboard e crie um dashboard novo ou utilize um preexistente.

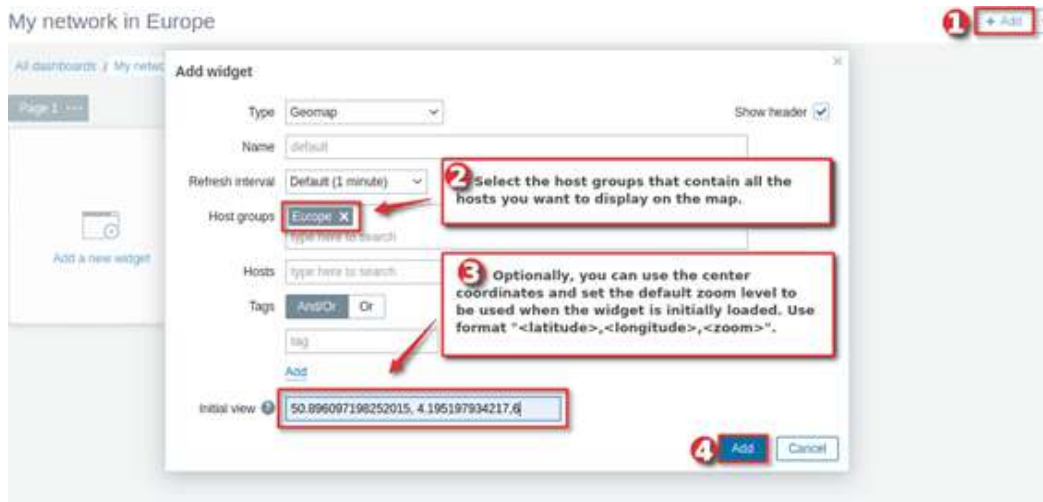


Crie um widget "Geomap" no dashboard recém-criado. Clique no pequeno ícone "Add", depois selecione os grupos de host que contém todos aqueles que deseja que sejam exibidos no mapa.

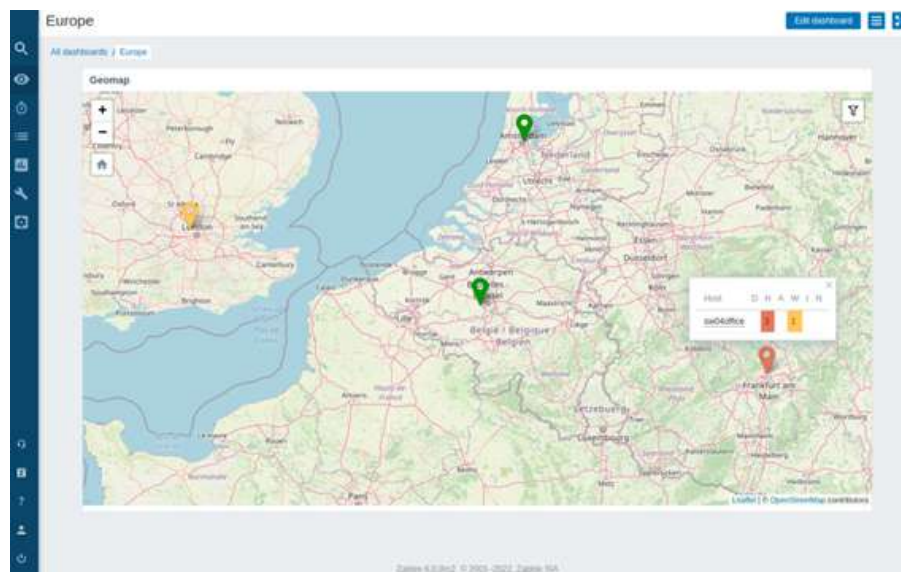
Alternativamente, no campo "Initial view" é possível usar as coordenadas centrais e definir o nível de zoom padrão a ser utilizado quando o widget for inicialmente carregado.

Formato

Utilize o formato "<latitude>, <longitude>, <zoom>", por exemplo 50.896097198252015, 4.195197934217,6. Em nosso exemplo, Utilizarei a latitude e longitude de uma cidade central e o zoom em nível 6.



Se tudo foi feito corretamente, após salvar seu dashboard, deverá ter um Geomap parecido com a imagem abaixo:



Para mais informações sobre Notificações via SNMP, acesse esta [página](#).

Para mais informações sobre a configuração, acesse a página [\[enable-snmp\]](#) onde o comando de console é detalhado mais profundamente.

GSM - Geomap hidden for backup

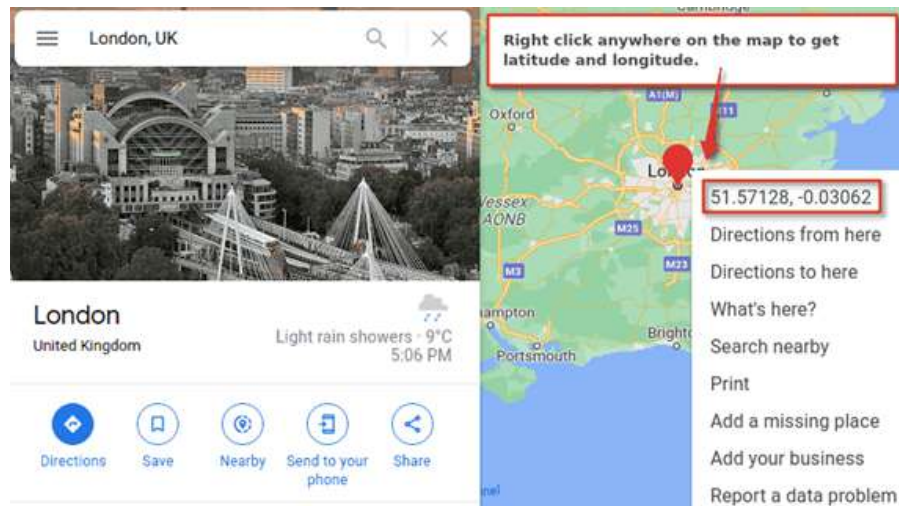
Detalhes da funcionalidade

O GSM possui o recurso chamado "Geomap" que nada mais é que a geolocalização dos ativos dispostos no sistema em tempo real.

Funcionamento

Por padrão, o Geomap exibe todos os hosts com coordenadas geográficas válidas sob o inventário de hosts. Todavia, primeiro precisamos configurar os hosts antes de seguir com a configuração do Geomap.

Por exemplo, temos switches de rede em Londres, Amsterdam, Bruxelas e Frankfurt, então copiaremos/colaremos as coordenadas do Google Maps e os hosts no GSM.

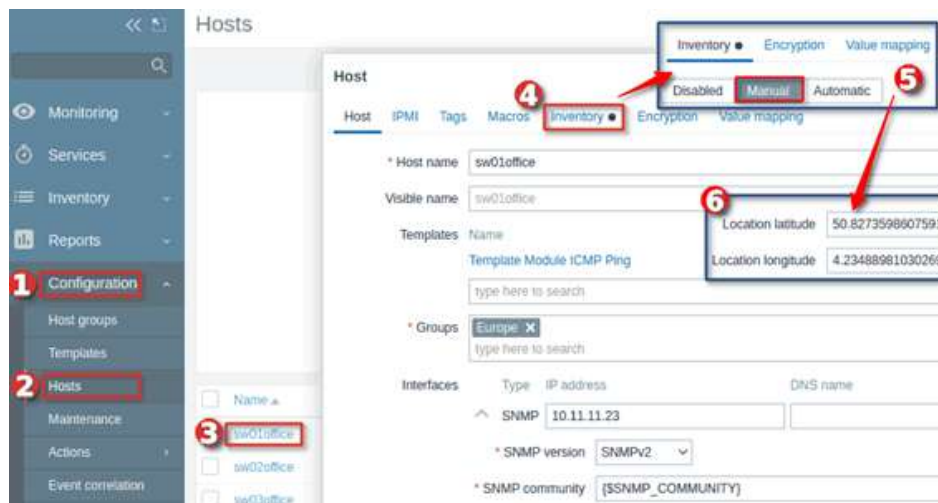


Detalhamento

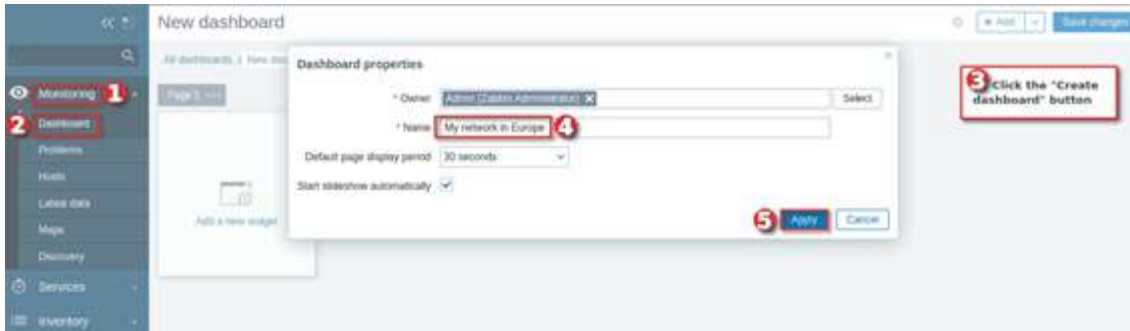
A seguir temos um passo a passo de como configurar o Geomap:

Navegue para Configuration Hosts Selecione seu Host.

Após, mude para Inventory altere o mod para "Manual" Insira as coordenadas nos campos "Location latitude" e "Location longitude", de acordo com a imagem abaixo:



Agora vá para a seção do dashboard e crie um dashboard novo ou utilize um preexistente.

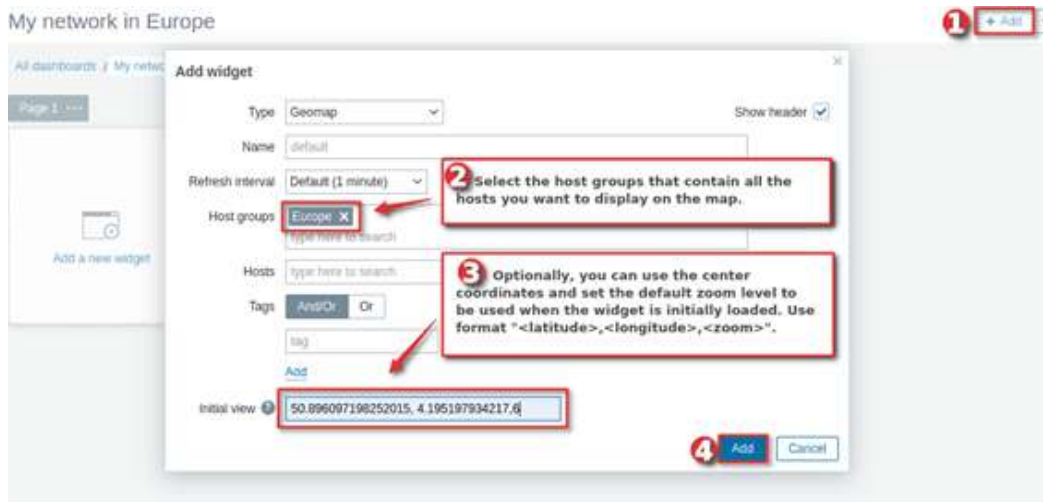


Crie um widget "Geomap" no dashboard recém-criado. Clique no pequeno ícone "Add", depois selecione os grupos de host que contém todos aqueles que deseja que sejam exibidos no mapa.

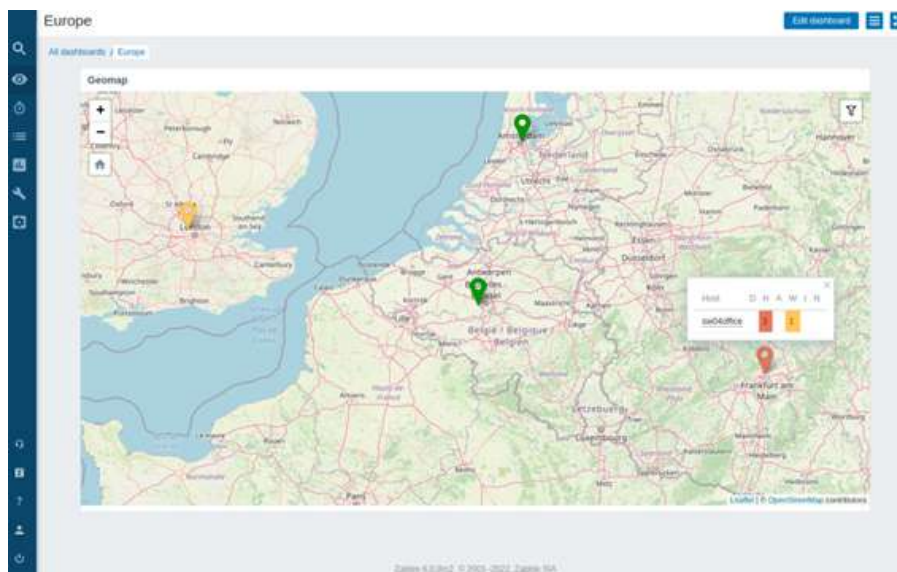
Alternativamente, no campo "Initial view" é possível usar as coordenadas centrais e definir o nível de zoom padrão a ser utilizado quando o widget for inicialmente carregado.

Formato

Utilize o formato "<latitude>, <longitude>, <zoom>", por exemplo 50.896097198252015, 4.195197934217,6. Em nosso exemplo, Utilizarei a latitude e longitude de uma cidade central e o zoom em nível 6.



Se tudo foi feito corretamente, após salvar seu dashboard, deverá ter um Geomap parecido com a imagem abaixo:

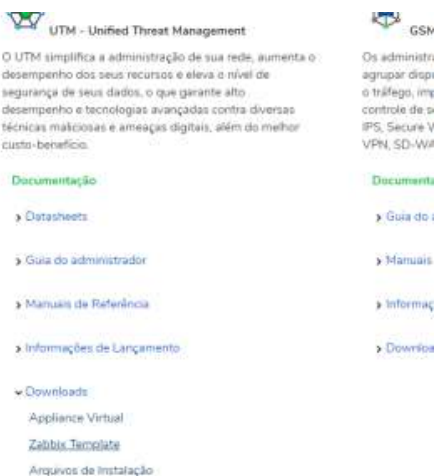


Template

Entre outros recursos também é possível utilizar *templates* para unificar dispositivos que utilizem as mesmas configurações, a Blockbit disponibiliza o *template* em formato XML.

Para efetuar *download* clique neste link: [Template](#).

Também é possível acessar a página inicial do *Resource Center*, clicar em "UTM - Unified Threat Management", entrar em "Downloads" e efetuar o download clicando em "*Zabbix Template*".



Link do Template no Resource Center PT/BR

Caso necessite de mais instruções sobre como utilizar este *template*, consulte a [documentação oficial do Zabbix](#).

Para mais informações sobre Notificações via SNMP, acesse esta [página](#).

Para mais informações sobre a configuração, acesse a página [\[enable-snmp\]](#) onde o comando de console é detalhado mais profundamente.

GSM - INTERFACE WEB

Esta seção irá demonstrar como realizar o acesso a Interface Web do Blockbit GSM.

O Blockbit GSM possui uma interface moderna, de fácil uso e responsiva, ou seja, é capaz se adequar a tela de qualquer dispositivo que seja utilizado para acesso (*tablets, smartphones, notebook, etc.*). Isso garante a sua empresa agilidade e facilidade, podendo ser acessado a qualquer hora e local.

Para realizar o acesso a Interface Web do Blockbit GSM siga as orientações a seguir.

Acessando a Interface Web – Blockbit GSM

Para acessar a interface web, utilize um navegador recomendado.

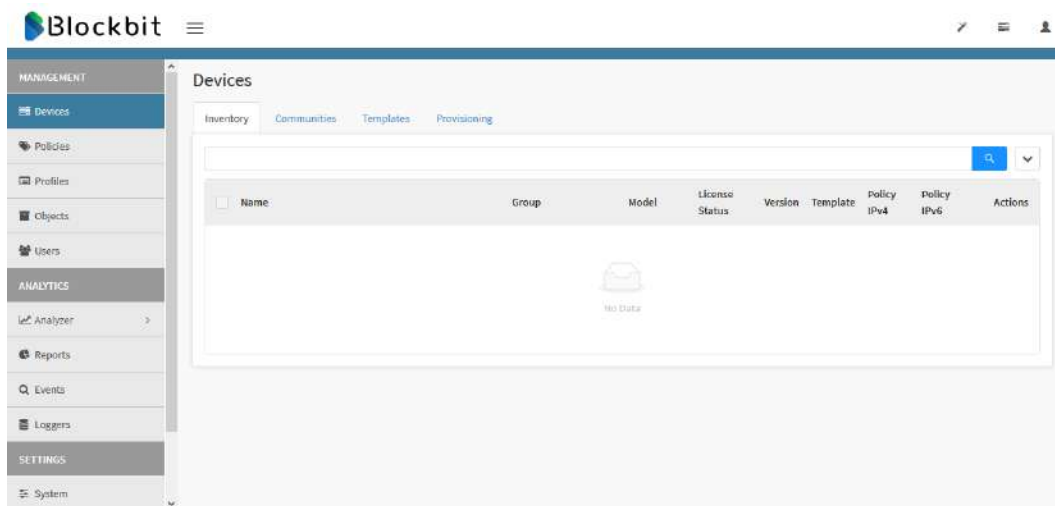
1. Conecte no navegador de *internet* e acesse o endereço: <https://192.168.1.1>. Caso tenha alterado o endereço IP, utilize esse IP alterado;
2. Acesse o IP configurado. Ex.: <https://172.16.102.235>;
3. Digite os seguintes dados:
 - **E-mail address:** E-mail cadastrado. Ex.: admin@blockbit.com;
 - **Password:** Senha cadastrada;
 - **English:** Neste campo define-se o idioma desejado para acessar a Interface Web. O idioma pode ser Inglês ou Português;



Tela de Login – System Administration

- Clique no botão “Login” para acessar a Interface Web.

4. Esta é a tela principal do Blockbit GSM, denominada *Device Manager*.



Device Manager

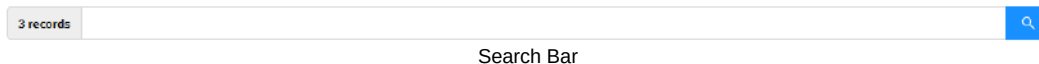
No próximo capítulo, todos os botões e menus serão devidamente explicados.

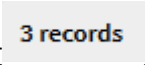
GSM - OPERAÇÃO BÁSICA

O Blockbit GSM é composto de algumas funcionalidades básicas que estão disponíveis em diversos painéis diferentes, de forma a facilitar sua utilização, segue um guia básico de como utilizar esses recursos:

Barra de busca

A barra de busca, fica alocada no topo dos painéis e possibilita localizar itens específicos.



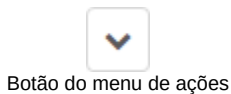
Na **área de registros**  exibido na frente da barra de busca, é exibida a quantia de registros localizados pela busca ou presentes antes de efetuar a busca.

Para remover as palavras chaves digitadas na barra de busca, clique no **botão** , caso a barra de busca esteja em branco, clique no botão **search**  para voltar a tela inicial.

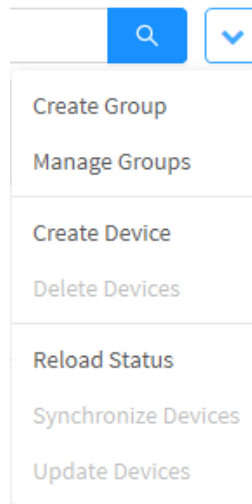
Para executar a busca, adicione a palavra chave desejada e clique no botão **search** .

Menu de ações

O menu de ações fica alocado no topo direito do painel:



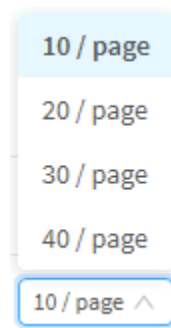
Ao clicar neste botão, um menu com um conjunto de opções contextuais ao painel onde ele estiver localizado será exibido, por exemplo:



Menu de ações

Quantidade de Resultados

Na parte inferior da tela, é possível selecionar quantos resultados serão exibidos por página, sendo o mínimo 10 e o máximo de 40 itens por página.



Quantia de resultados

Por fim, quanto a navegação, os botões de “Alternar Páginas” permite navegar entre as páginas.



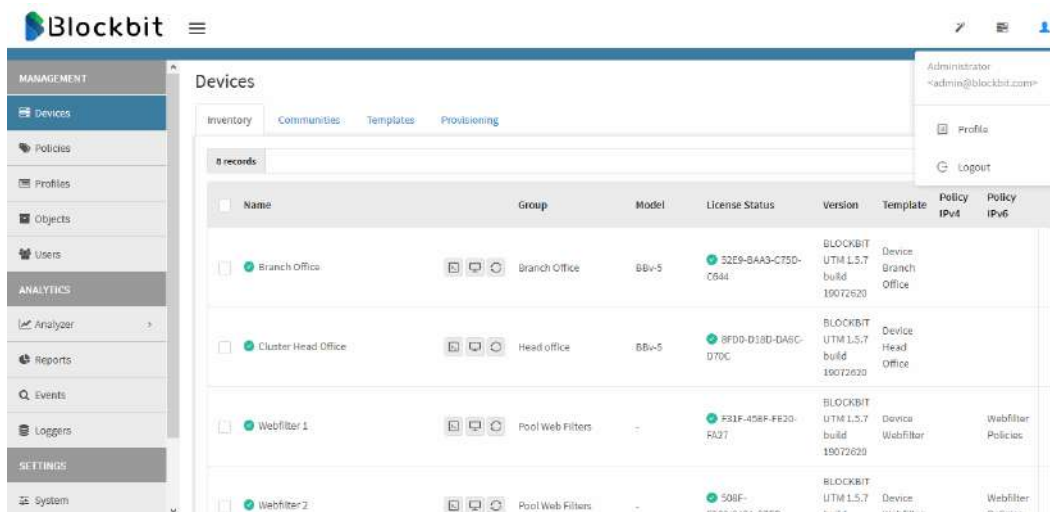
Alternar Página

GSM - MENU DE PERFIL DO USUÁRIO

O menu de perfil do usuário encontra-se localizado no canto superior direito da tela. Para acessar basta clicar no ícone **user** [👤].



Na tela abaixo o menu do usuário aparece com o nome “admin”, isso ocorre pois foi esse o nome cadastrado no item “Name” no capítulo [Assistente de Instalação](#).



Menu de perfil do usuário

O menu de perfil do usuário é composto das opções:

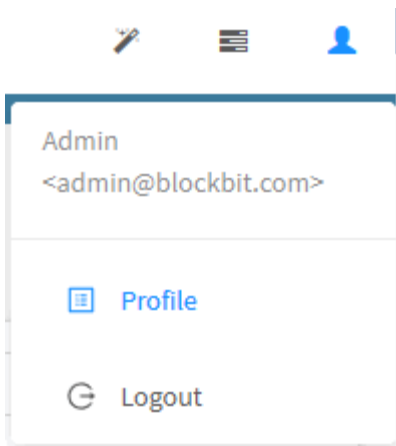
- [Profile](#);
- [Logout](#).

A seguir eles serão explicados detalhadamente.

Profile

Na opção “Profile” é possível editar as informações de perfil do usuário. Para acessá-lo, siga os seguintes passos:

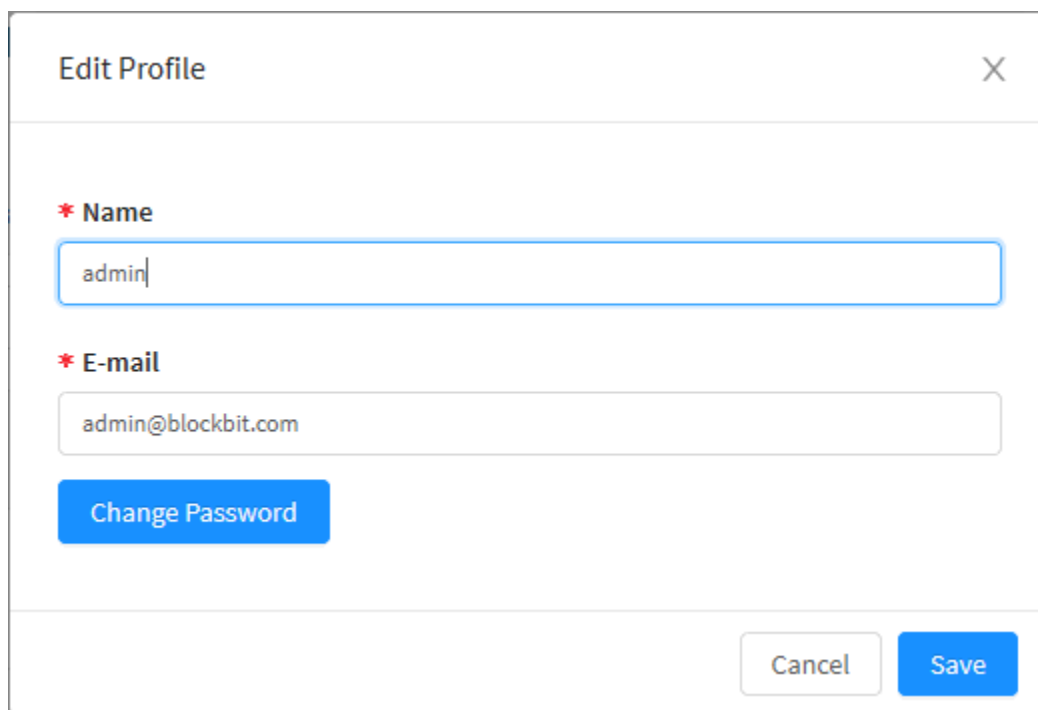
1. No canto superior direito. Clique na opção “Profile”;



Menu do usuário – Botão “Profile”

2. Realize as alterações de edição de perfil desejadas. Esta tela contém as seguintes informações:

- **Name:** O nome do usuário cadastrado;
- **E-mail:** O e-mail do usuário cadastrado. Este campo é utilizado para realizar o *login* no Blockbit GSM;

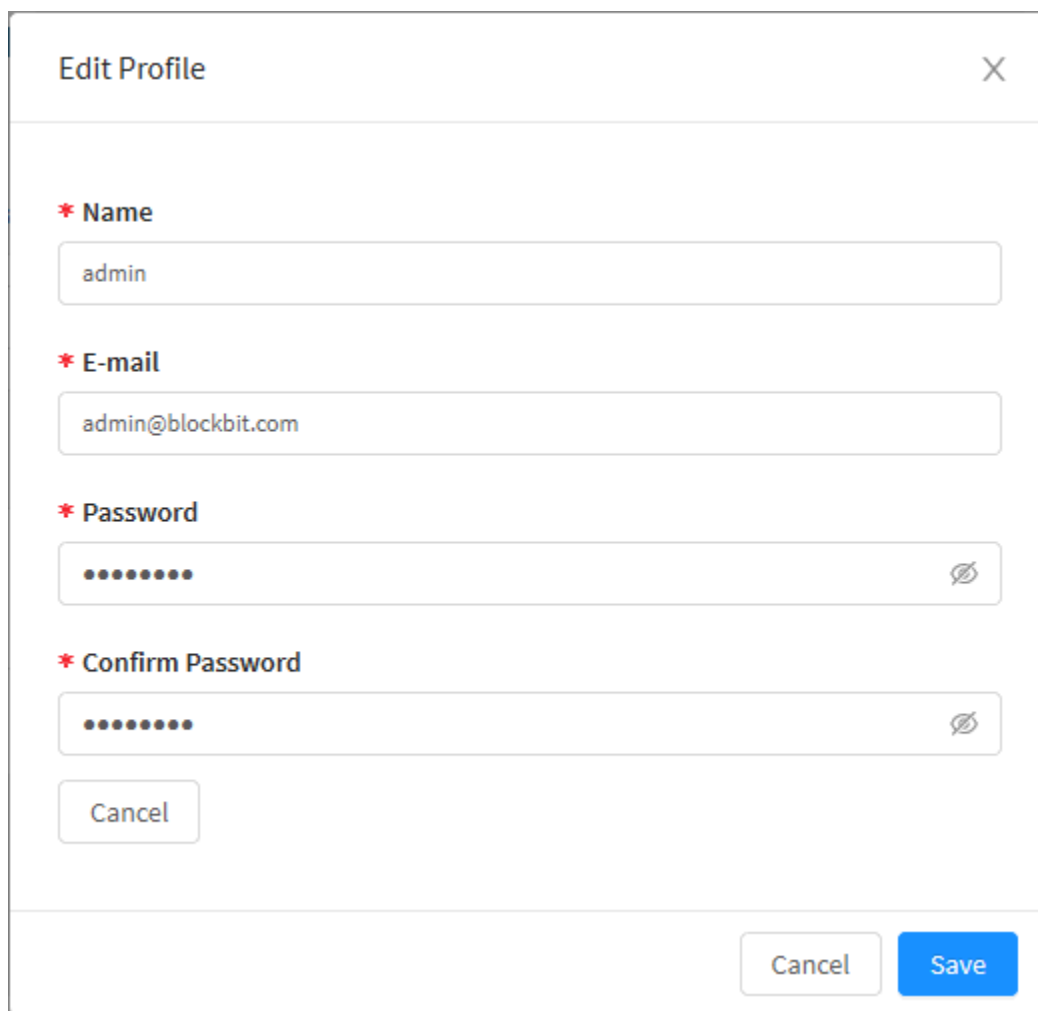


Menu do usuário – Edit Profile

Change Password

3. Para alterar as informações de senha, clique no botão **Change Password** []:

- **Password:** Insira a nova senha desejada;
- **Confirm Password:** Confirme a senha digitada no item anterior.

The image shows a modal dialog box titled "Edit Profile" with a close button (X) in the top right corner. Inside the dialog, there are four required fields, each marked with a red asterisk: "Name" (containing "admin"), "E-mail" (containing "admin@blockbit.com"), "Password" (masked with dots), and "Confirm Password" (masked with dots). Each password field has an eye icon to toggle visibility. At the bottom left of the dialog is a "Cancel" button. At the bottom right, outside the main form area, are two buttons: "Cancel" and "Save".

Edit Profile – Alteração de senha – Password

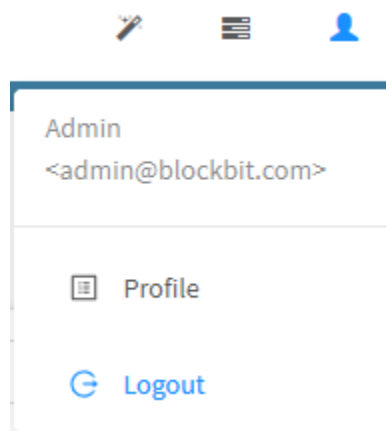
Para sair desta janela, basta clicar em **Cancel** [], ou no [X] do topo direito da tela para voltar à janela anterior.

Save

Clique no botão **Save** [] para salvar as alterações, o sistema irá atualizar e solicitar que o *Login* seja realizado novamente.

Logout

A qualquer momento é possível sair do sistema. Basta clicar no botão “Logout”.



Logout

Isso levará o usuário de volta a página de “Login”.

GSM - DEPLOYS PANEL

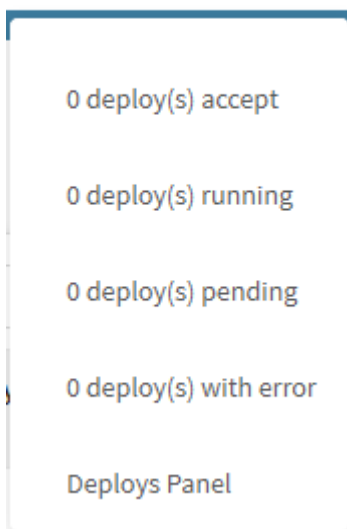
Esta seção irá demonstrar como acompanhar e gerenciar as instalações dos pacotes de configurações do Blockbit GSM nas *devices* gerenciadas. Esses pacotes, quando solicitada a instalação, são nomeados como *DEPLOYS*.

Para acessar o painel *Deploys Panel*, clique no botão localizado no topo direito da tela, do lado do menu do usuário:



Botão “*Deploys Panel*”.

Surgirá uma tela listando os *deploy(s)*. Para acessar a tela com filtros, clique em uma das quatro opções: *deploy(s) accept*, *deploy(s) running*, *deploy(s) pending* e *deploy(s) error*. Será aberta uma nova aba no navegador com o filtro selecionado. Se desejar acessar a tela sem filtro, clique no botão “*Deploys Panel*”.



Deploys Panel – Lista

Para abrir o *Deploys Panel*, selecione a opção [**Deploys Panel**] na lista. A seguinte tela será exibida:

Deploys

Scheduled	Owner	Auditor	Status	Package	
20/10/2019 - 19/11/2019					

Package	Auditor	Scheduled	Progress	Status	Actions
Device Communities	admin Owner: admin	25/09/2019 11:47 Created: 25/09/2019 11:47	0%	Cancelled	
Device Templates	admin Owner: admin	25/09/2019 11:37 Created: 25/09/2019 11:37	0%	Cancelled	
Policy Pack	admin Owner: admin	25/09/2019 11:00 Created: 25/09/2019 11:00	50%	Running	
Device Communities	admin Owner: admin	25/09/2019 09:54 Created: 25/09/2019 09:54	0%	Pending	
Device Templates	admin Owner: admin	25/09/2019 09:37 Created: 25/09/2019 09:37	0%	Error	
Device Communities	admin Owner: admin	25/09/2019 09:16 Created: 25/09/2019 09:16	0%	Error	
Device Templates	admin Owner: admin	25/09/2019 09:15 Created: 25/09/2019 09:15	0%	Cancelled	

Deploys

A tela *Deploys* é composta por um painel de progresso logo no topo da tela, uma barra com ferramentas de busca e a lista de tarefas com seis colunas:

- *Package*;
- *Auditor*;
- *Scheduled*;
- *Progress*;
- *Status*;
- *Action*.

A seguir analisaremos a barra de *Busca* e os *Filtros* deste painel.

Deploys Panel - Busca e Filtros

Para localizar um *Deploy* em específico, há uma barra de busca dividida em: “*Scheduled*”, “*Owner*”, “*Auditor*”, “*Status*”, “*Package*” e o botão de “*Search*”.

Nesta sessão iremos analisar o funcionamento do sistema de busca de *deploys*.

The image shows a search interface for the 'Deploys Panel'. It consists of five input fields labeled 'Scheduled', 'Owner', 'Auditor', 'Status', and 'Package'. The 'Scheduled' field contains a date range from '20/10/2019' to '19/11/2019' with a calendar icon. The 'Owner' and 'Auditor' fields are empty text boxes. The 'Status' field is a dropdown menu with a downward arrow. The 'Package' field is also a dropdown menu with a downward arrow. To the right of these fields is a blue button with a white magnifying glass icon, representing the 'Search' function.

Deploys Panel – Busca de deploys

Da esquerda para a direita temos:

- **Scheduled:** Filtra por data/hora inicial ou final, referindo-se a data para quando o *Deploy* foi agendado;
- **Owner:** Filtra pelo usuário que criou o *Deploy*;
- **Auditor:** Filtra por auditor que aprovou o *Deploy*;
- **Status:** Filtra pelo *status* do *Deploy*, que pode ser dos tipos: *Success*, *Accept*, *Running*, *Pending*, *Error* ou *Cancelled*;
- **Package:** Filtra pelo tipo do *Deploy*, que pode ser: *Policy Pack*, *Device Template* ou *Device Community*.



Para executar a busca, clique no botão de **search**[].

Deploys Panel - Lista de Deploys

Na lista de *deploys* são exibidas todos os *deploys* que foram criados no sistema.

Deploys						
Scheduled		Owner	Auditor	Status	Package	
20/10/2019 - 19/11/2019						
Package	Auditor	Scheduled	Progress	Status	Actions	
Device Communities	admin Owner: admin	25/09/2019 11:47 Created: 25/09/2019 11:47	0%	Cancelled		
Device Templates	admin Owner: admin	25/09/2019 11:37 Created: 25/09/2019 11:37	0%	Cancelled		
Policy Pack	admin Owner: admin	25/09/2019 11:00 Created: 25/09/2019 11:00	50%	Running		
Device Communities	admin Owner: admin	25/09/2019 09:54 Created: 25/09/2019 09:54	0%	Pending		
Device Templates	admin Owner: admin	25/09/2019 09:37 Created: 25/09/2019 09:37	0%	Error		
Device Communities	admin Owner: admin	25/09/2019 09:16 Created: 25/09/2019 09:16	0%	Error		
Device Templates	admin Owner: admin	25/09/2019 09:15 Created: 25/09/2019 09:15	0%	Cancelled		

Deploys Panel – Lista de Deploys

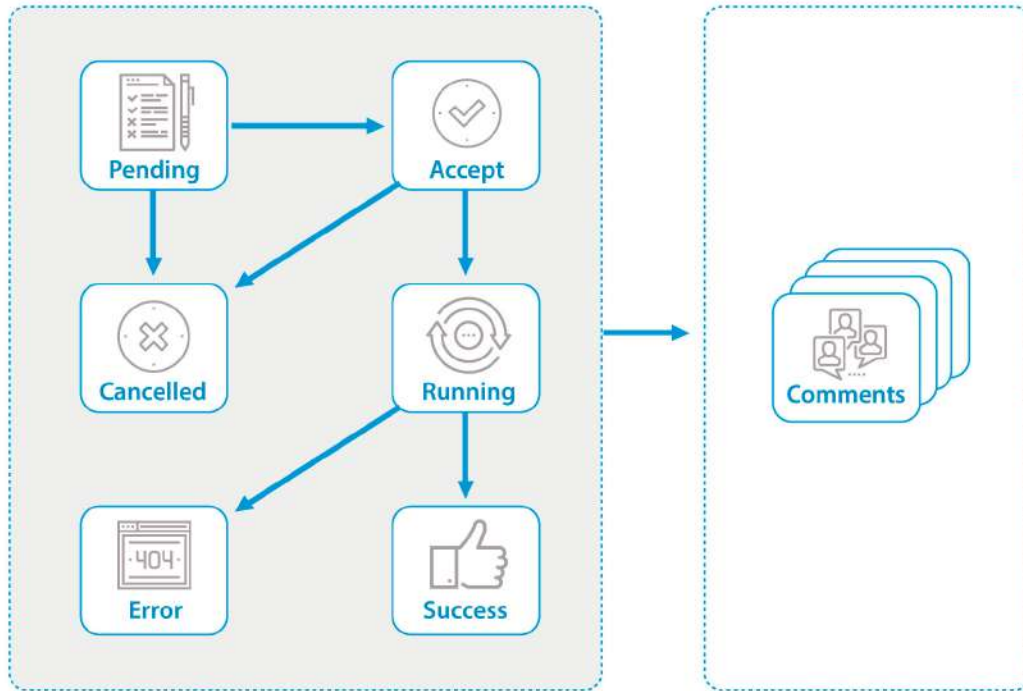
O sistema de *deploys* possui uma regra de negócio que consiste nas seguintes premissas:

- A lista de *deploys* é sempre ordenado por data de criação e ordem decrescente;
- Os status de um *deploy* são classificados em:
 - **Pending** [Pending]: Pacote está aguardando um parecer do auditor;
 - **Accept** [Accept]: Pacote recebeu um aceite e seu *deploy* irá iniciar no prazo determinado;
 - **Running** [Running]: O pacote está sendo implementado;
 - **Success** [Success]: Pacote foi implementado com sucesso;
 - **Cancelled** [Cancelled]: A implementação do pacote foi cancelada;
 - **Error** [Error]: Algo de errado ocorreu (para mais informações basta clicar no próprio ícone de erro).
- Todas as atividades dentro de um *deploy* exigem um comentário. Os comentários são adicionados à lista de "Activity" do *deploy*;
- Caso tenha algum dispositivo com status "Error", esse será o status principal do *deploy*.

! O sistema de validação alerta em caso de ofuscação ou conflito entre Políticas.

Segue o fluxo do processo de aprovação dos *deploys*:

Deploys Panel



Deploys Panel – Processo de aprovação de Deploys

O painel de *deploys* é composto pelas colunas:

- *Package*;
- *Auditor*;
- *Scheduled*;
- *Progress*;
- *Status*;
- *Actions*.

A seguir analisaremos cada coluna desse painel.

Deploys Panel - Coluna Package

A coluna *Package* exibe o nome do pacote aplicada no *deploy*.

Para exibir detalhes do Pacote aplicado no *deploy*, clique no nome do pacote. Surgirá a tela de *Task view*:

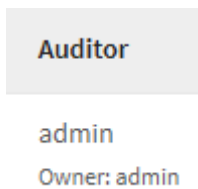


Deploys Panel - Task view

Para fechar a janela, clique no botão **Close**  ou clique em  no topo da janela.

Deploys Panel - Coluna Auditor

A coluna Auditor exibe o nome do *Owner* do *Deploy* e o auditor cadastrado, responsável por aprová-la.



Deploys Panel – Auditor

Deploys Panel - Coluna Scheduled

A coluna "Scheduled" exibe informações referentes ao dia da criação do *deploy* e a data que foi agendada para ser executada.

Scheduled

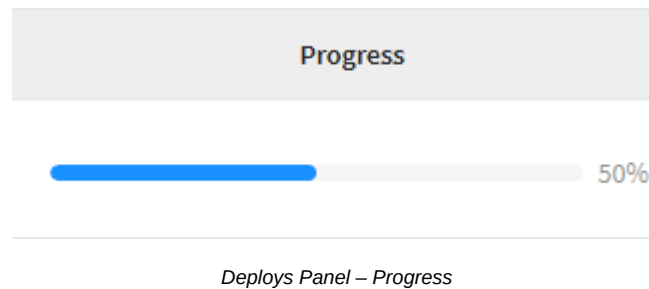
19/11/2019 14:23

Created: 19/11/2019 15:24

Deploys Panel – Scheduled

Deploys Panel - Coluna Progress

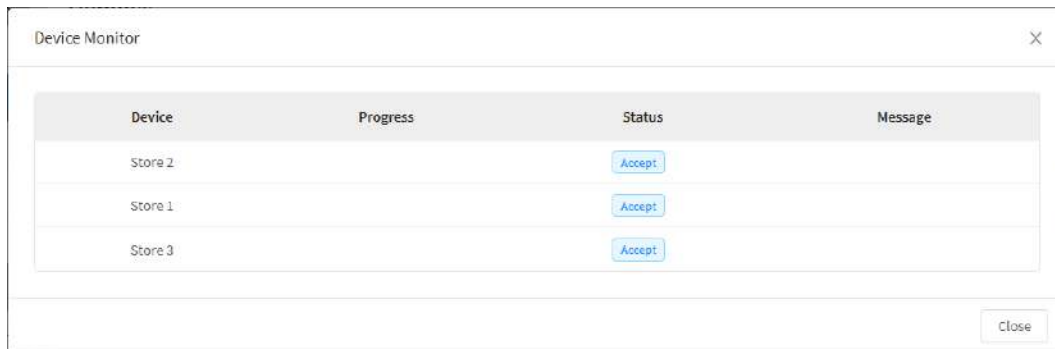
A coluna *Progress* exibe uma barra de progresso que informa a porcentagem de conclusão do *deploy*.



Deploys Panel - Coluna Status

A coluna "Status" exibe o status que um determinado *deploy* se encontra: *Pending*, *Running*, *Cancelled*, *Success* e *Error*.

Para exibir detalhe do Status de cada *device* que será aplicado em um determinado *deploy*, clique no nome do Status e surgirá a tela "Deploy Information":

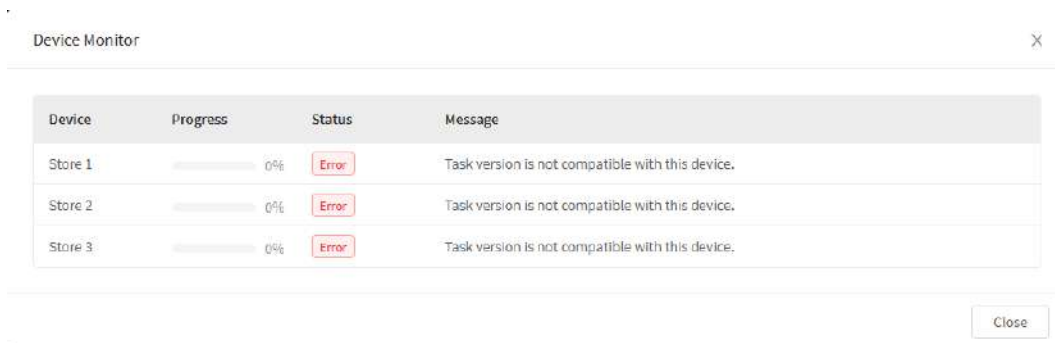


Device	Progress	Status	Message
Store 2		Accept	
Store 1		Accept	
Store 3		Accept	

Deploys Panel – Device Status

Os status exibidos nessa coluna e nessa tela são idênticos aos já citados [anteriormente](#).

Na coluna "Message" são exibidas as mensagens relacionadas a eventuais falhas (caso o status "error" surja), a imagem abaixo exemplifica a função dessa coluna:



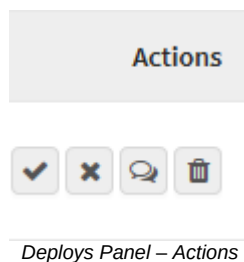
Device	Progress	Status	Message
Store 1	0%	Error	Task version is not compatible with this device.
Store 2	0%	Error	Task version is not compatible with this device.
Store 3	0%	Error	Task version is not compatible with this device.

Deploys Panel – Error Message

A seguir explicaremos os botões e seus respectivos status.

Deploys Panel - Coluna Actions

A coluna de ações disponibiliza alguns botões com funcionalidades essenciais para os *deploys*:



Existem cinco botões de ação:

- [Accept](#);
- [Reinstall](#);
- [Cancel](#);
- [Activity](#);
- [Remove](#).

A seguir, serão apresentadas as funcionalidades de cada botão.

Deploys Panel - Botão "Accept"

Através do botão "Accept" o auditor pode aprovar a instalação do pacote. Com ele também é possível deixar registrado um comentário informando o motivo da aprovação do *Deploy*.

Para acessar, clique no botão "Accept".

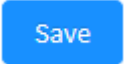
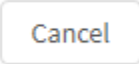


Botão "Accept"

Surgirá a tela Add Justify Action. Escreva o comentário desejado:

A tela "Add Justify Action" é uma caixa de diálogo com um título "Add Justify Action" e um ícone de fechar "X" no canto superior direito. Abaixo do título, há uma seção rotulada "* Comment" com um campo de texto contendo o texto "Authorized". No canto inferior direito da caixa, há dois botões: "Cancel" (branco) e "Save" (azul).

Add Justify Action

Clique no botão **Save** [] para salvar ou **Cancel** [] para fechar a tela.

Deploys Panel - Botão "Reinstall"

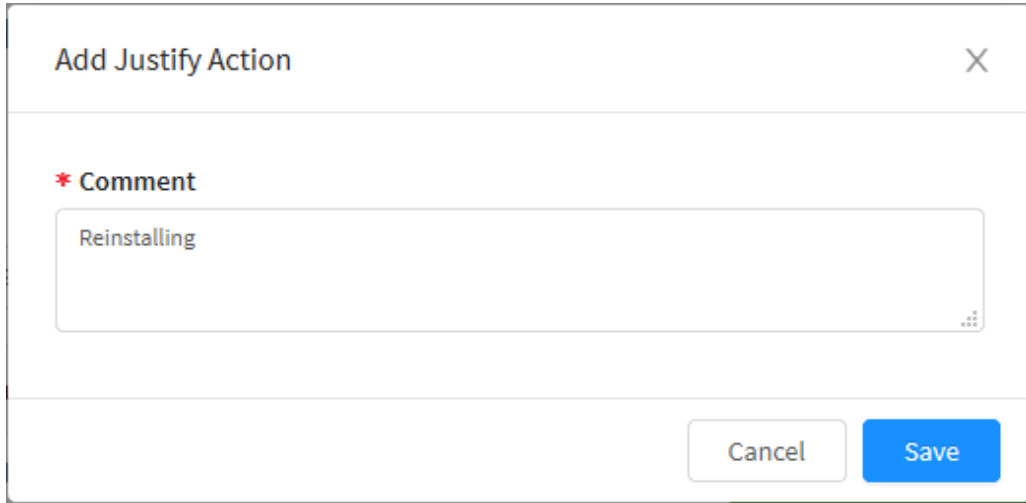
O botão "*Reinstall*" executa a reinstalação dos pacotes.

Para acessar, clique no botão "*Reinstall*".



Botão "*Reinstall*"

Surgirá a tela "*Add Justify Action*", em "*Comment*", escreva o comentário desejado:



Reinstall Deploy

Clique no botão **Save** [] para salvar ou **Cancel** [] para fechar a tela.

Deploys Panel - Botão "Cancel"

Utilizando-se do botão "Cancel" o auditor é capaz de rejeitar a instalação do pacote. Com ele também é possível deixar registrado um comentário informando o motivo da rejeição do *Deploy*.

Para acessar, clique no botão "Cancel".

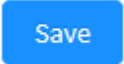
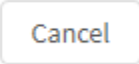


Botão "Cancel"

Surgirá a tela *Justify*.

A tela 'Add Justify Action' é uma caixa de diálogo com um título 'Add Justify Action' e um ícone de 'X' no canto superior direito. Abaixo do título, há uma seção rotulada '* Comment' com um campo de texto contendo o texto 'Canceled'. No canto inferior direito, há dois botões: 'Cancel' (branco com borda cinza) e 'Save' (azul com texto branco).

Justify Action Cancellation

Clique no botão **Save** [] para salvar ou **Cancel** [] para fechar a tela.

Deploys Panel - Botão "Activity"

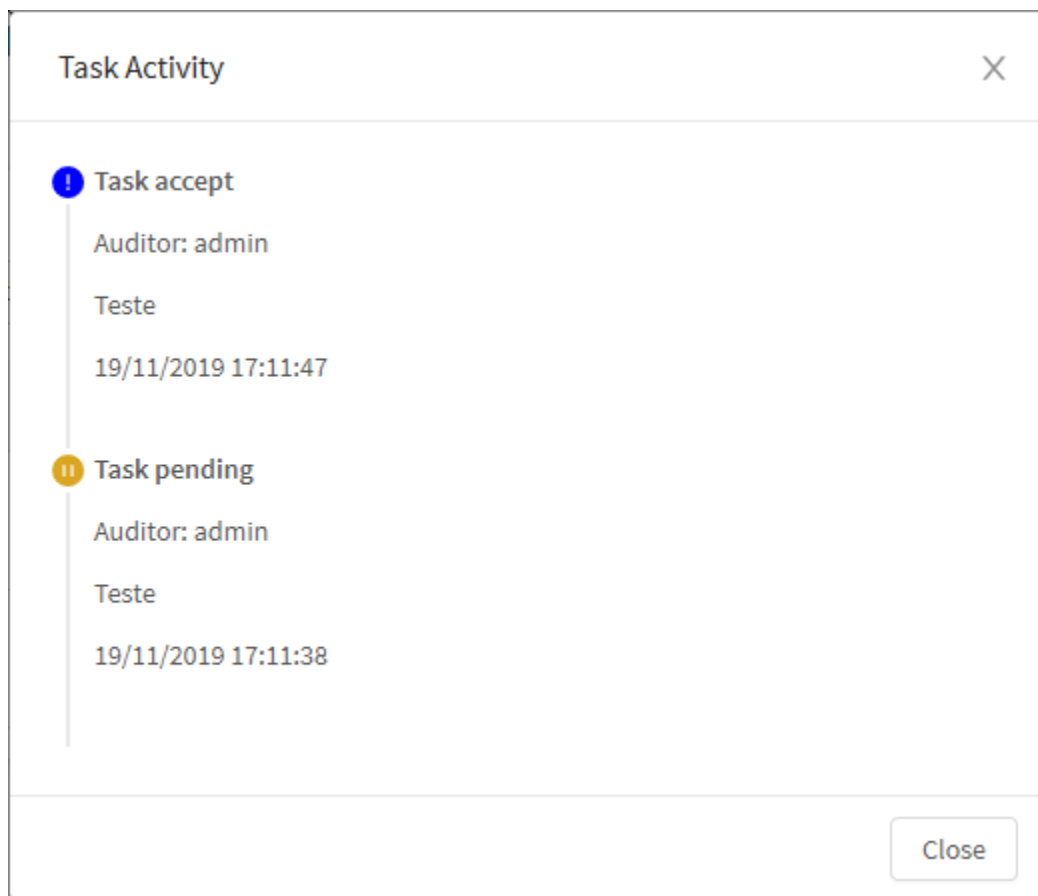
O botão "Activity" exibe o histórico de atividades referentes aos *Deploys*.

Para acessar, clique no botão "Activity".



Botão de Ações *Deploys Panel* – "Activity"

Surgirá a tela *Task Activity*:



Botão "Deploy Activity"

Clique no botão **Close** para fechar a tela.



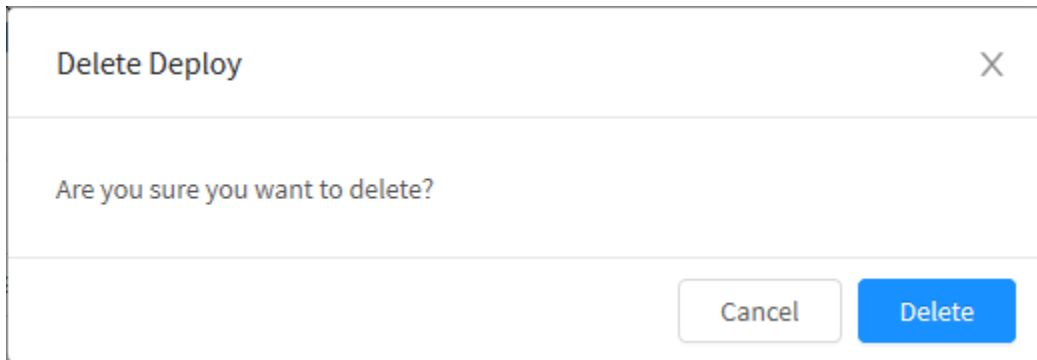
Deploys Panel - Botão "Remove"

O botão "Remove" faz exatamente o que o nome diz: Ele revoga o pacote.

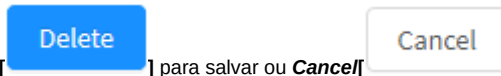
Para acessar, clique no botão "Remove".



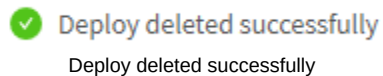
Botão "Remove"



Delete Deploy



Clique no botão **Delete** para salvar ou **Cancel** para fechar a tela.



A exclusão foi efetuada com sucesso.

GSM - INSTALL PACKAGE

Através do botão "Install Package" é possível realizar a instalação do pacote de configurações para as *devices* integradas ao Blockbit GSM.



Botão "Install Package".

Ao clicar no botão surgirá a tela de *Install Package*:

Install Package.

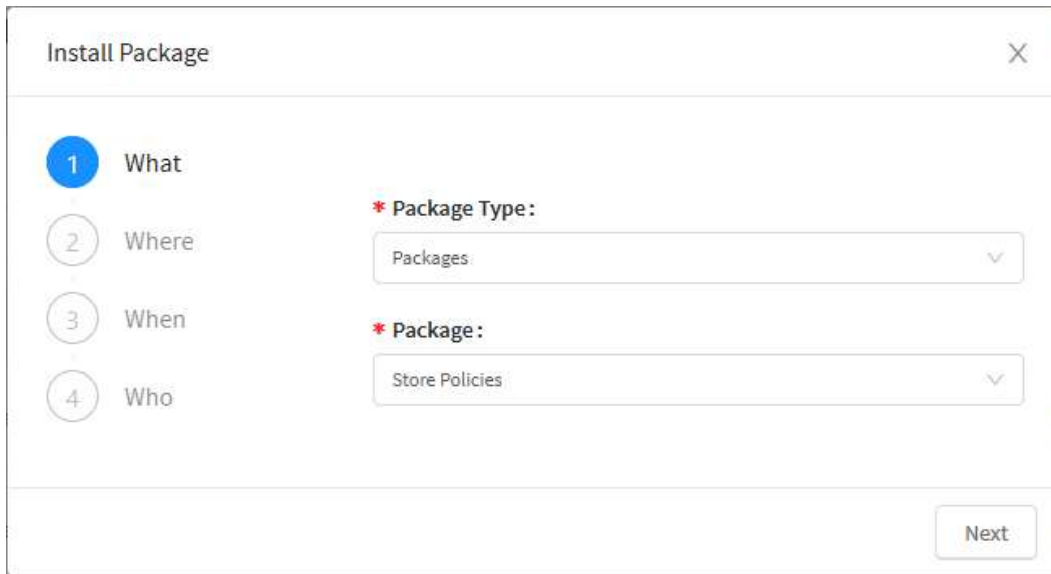
A janela *Install Package* é composta de:

- [What](#);
- [Where](#);
- [When](#);
- [Who](#).

Abaixo analisaremos cada componente do painel "Install Package":

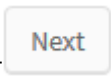
What

Determina qual operação será realizada, consistindo em:



Install Package – What.

- **Tipo de pacote:** Este menu em cascata determina o tipo de pacote que será instalado, o qual pode ser de um dos seguintes tipos:
 - **Policy Package:** Com esta opção é possível instalar Templates criados na aba "[Policy Package](#)";
 - **Device Template:** Com esta opção, é possível instalar Templates criados na aba "[Device Templates](#)";
 - **Device Community:** Através desta opção é possível instalar comunidades em "Device", em "[Device Communities](#)";
- **Pacote:** Este menu em cascata especifica a Política, Device ou Device Community desejada.

The image shows a rectangular button with rounded corners and a light gray border. The word "Next" is centered inside the button in a blue, sans-serif font.

Clique no botão **next** [] para avançar ao painel [Where](#) e continuar os procedimentos

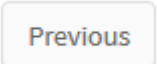
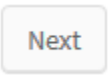
Where

Determina o local onde o pacote será instalado, consiste em:

The screenshot shows a dialog box titled "Install Package" with a close button (X) in the top right corner. On the left side, there is a vertical list of four steps: "What" (with a checkmark icon), "Where" (with a blue circle containing the number 2), "When" (with a circle containing the number 3), and "Who" (with a circle containing the number 4). To the right of the "Where" step, the text "Devices & Device group:" is displayed above a text input field. The input field contains the text "GROUP - Stores" followed by a small "X" icon. At the bottom right of the dialog box, there are two buttons: "Previous" and "Next".

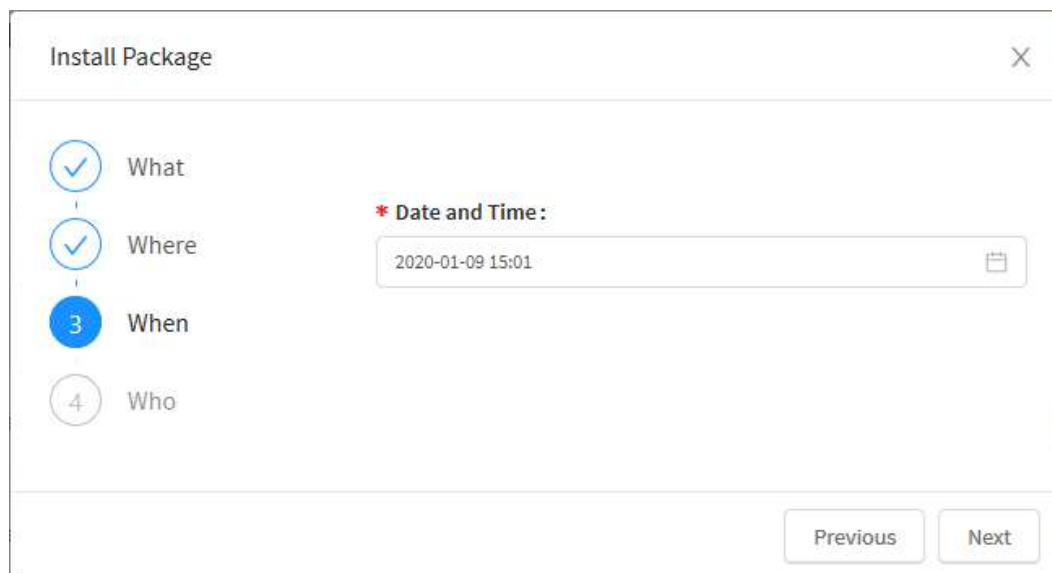
Install Package – Where.

- **Devices & Devices group:** Seleciona o Device ou Device group nos quais os pacotes serão instalados. Selecione a opção desejada para adicionar o item. Caso escolha o item errado, clique no [X] ou selecione o item novamente da lista para desmarcá-lo. É possível selecionar múltiplos grupos ou dispositivos;

Para voltar ao painel [What](#) , clique no botão [], para continuar com os procedimentos e acessar o painel [When](#), clique no botão [].

When

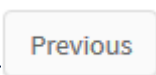
Determina o momento em que o pacote será instalado, consiste em:

The image shows a 'Install Package' dialog box with a close button (X) in the top right corner. On the left, there is a vertical list of four steps: 'What' (with a checkmark icon), 'Where' (with a checkmark icon), 'When' (with a blue circle containing the number 3), and 'Who' (with a circle containing the number 4). To the right of this list, the text '* Date and Time :' is displayed above a text input field containing '2020-01-09 15:01'. A calendar icon is visible on the right side of the input field. At the bottom right of the dialog, there are two buttons: 'Previous' and 'Next'.

Install Package – When.

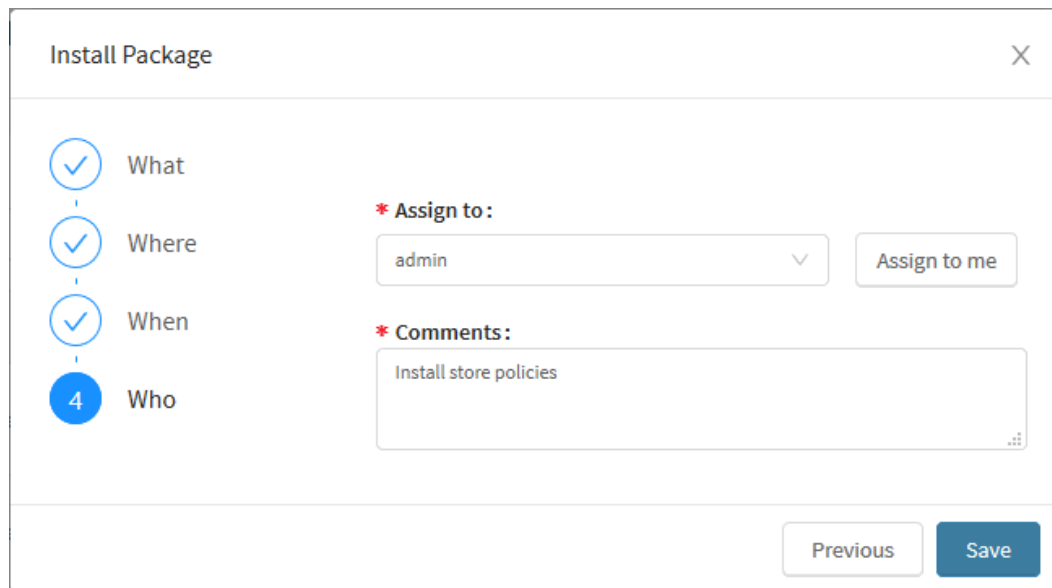
- **Date and Time:** Determina a data e horário desejados. Para selecionar o horário, selecione a data desejada e clique na opção "**select time**" para determinar o horário desejado. Caso queira inserir a data e horário atuais, clique na opção "**Now**", finalmente para salvar suas alterações

clique no botão [].

Para retornar ao painel [Where](#) , clique no botão [], para continuar com os procedimentos e acessar o painel [Who](#), clique no botão [].

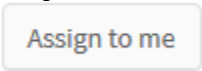
Who

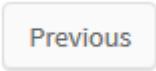
Determina quem será responsável pela instalação do pacote, consiste em:



The screenshot shows a dialog box titled "Install Package" with a close button (X) in the top right corner. On the left side, there is a vertical list of four steps: "What", "Where", "When", and "Who". Each step is preceded by a circular icon. The "What", "Where", and "When" icons contain a checkmark, while the "Who" icon contains the number "4". To the right of this list, under the heading "* Assign to :", there is a dropdown menu showing "admin" and a button labeled "Assign to me". Below this, under the heading "* Comments :", there is a text input field containing the text "Install store policies". At the bottom right of the dialog box, there are two buttons: "Previous" and "Save".

Install Package – Who.

- **Assign To:** Define o auditor responsável por aprovar a configuração da instalação. Caso queira ser o responsável, clique no botão []. Ex.: Admin;
- **Comments:** Insira um comentário para definir a função destas configurações, facilitando assim o entendimento do auditor.

Para voltar ao painel [When](#), clique no botão [], para salvar o prompt de configurações da instalação de pacotes clique no botão [].

Após realizar estes procedimentos, o Template de solicitação de instalação terá sido completado com sucesso.

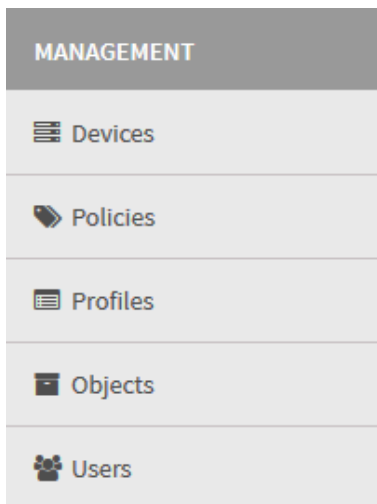
Para aplicar estas configurações, veja o capítulo [Deploys Panel](#).

GSM - MANAGEMENT

O Blockbit GSM viabiliza a administração de vários dispositivos de rede juntos, promovendo uma perspectiva plena da infraestrutura de todas as unidades organizacionais, possui a capacidade de gerar *templates* de configuração e pacotes de políticas de segurança para compartilhamento entre grupos de dispositivos e para determinação dos controles de acesso por função, é apto de estabelecer e catalogar todos os registros de conexão, de acesso a aplicações de *internet*, de dados pessoais e de conteúdo de comunicações privadas em conformidade com as regulamentações do Marco Civil da *Internet*.

Proporciona o monitoramento através de gráficos do status do seu gateway em aspectos gerais, tais como: sistema operacional, utilização de CPU, tuneis ativos, conexões concorrentes e casos de desconexão do gateway com o GSM.

Através do menu "*Management*" é possível administrar os dispositivos, políticas, perfis, objetos e usuários do sistema.



Menu *Management*.

Contém as opções:

- *Devices*;
- *Policies*;
- *Profiles*;
- *Objects*;
- *Users*.

Devices

O painel *Devices* é de vital importância para o Blockbit GSM, sua principal função é a capacidade de, como diz o nome, administrar todos os dispositivos conectados através de um único ponto central, colocando em termos simples: Através deste painel o Blockbit GSM administra os Blockbit UTM e futuramente, outras soluções digitais da Blockbit.

Primeiramente, ao se logar no Blockbit GSM, a aba “*Inventory*” estará automaticamente selecionada. Além disso, é possível acessar os “*Devices*”, clicando no botão localizado no menu vertical lateral, ou selecionando a aba adequada (caso o botão já tenha sido selecionado).



Management – Devices

A tela abaixo será exibida:

Devices

Inventory Communities Templates Provisioning

8 records

Name	Group	Model	License Status	Version	Template	Policy (IPv4)	Policy (IPv6)	Actions
Branch Office	Branch Office	BBW-S	✓ S2E9-BAAB-C75C-C6H	BLOCKBIT UTM 1.5.7 build 19672823	Device Branch Office			
Cluster Head Office	Head office	BBW-S	✓ 6F5D-D15D-DNAC-D79C	BLOCKBIT UTM 1.5.7 build 19672823	Device Head Office			
Webfilter 1	Pool Web Filters	BBW-S	✓ F33F-436F-FE23-7A27	BLOCKBIT UTM 1.5.7 build 19672823	Device Webfilter	Webfilter Policies		
Webfilter 2	Pool Web Filters	BBW-S	✓ 566F-E232-645A-97E8	BLOCKBIT UTM 1.5.7 build 19672823	Device Webfilter	Webfilter Policies		
Webfilter 3	Pool Web Filters	BBW-S	✓ FB47-AF24-257E-4D85	BLOCKBIT UTM 1.5.7 build 19672823	Device Webfilter	Webfilter Policies		
Store 1	Stores	BBW-S	✓ B34D-8ED9-6E7D-943C	BLOCKBIT UTM 1.5.7 build 19672823	Device Store	Store Policies		
Store 2	Stores	BBW-S	✓ 7155-69F2-CC3B-FE0F	BLOCKBIT UTM 1.5.7 build 19672823	Device Store	Store Policies		
Store 3	Stores	BBW-S	✓ D95E-65CA-256B-756A	BLOCKBIT UTM 1.5.7 build 19672823	Device Store	Store Policies		

1 / 8 page

Devices - Inventory

A tela *Devices* comporta as seguintes abas:

- [Inventory](#);
- [Communities](#);
- [Templates](#);
- [Provisioning](#).

A seguir, os componentes da aba [Inventory](#) serão analisadas.

Aba Inventory

No Blockbit GSM é possível realizar inventário de todos os seus dispositivos facilmente, tais como: *Status*, *Licença*, *Versão* e *Atualizações* dos *devices* integrados.

A aba “*Inventory*” é composta por sete colunas: “*Name*”, “*Group*”, “*Model*”, “*License Status*”, “*Version*”, “*Template*”, “*Policy IPV4*”, “*Policy IPV6*” e “*Actions*”. Os dispositivos estão divididos em grupos e além disso, no topo da tela estão localizados a *barra de busca* e no canto superior direito da tela está o *menu de ações*.

Devices

Inventory Communities Templates Provisioning

8 records

Name	Group	Model	License Status	Version	Template	Policy IPV4	Policy IPV6	Actions
Branch Office	Branch Office	BBW-S	52E9-BBAY-C75D-C6H	BLOCKBIT UTM 1.5.7 build 19672820	Device Branch Office			 
Cluster Head Office	Head Office	BBW-S	9F80-D1SD-D9AC-D79C	BLOCKBIT UTM 1.5.7 build 19672820	Device Head Office			 
Webfilter 1	Pool Web Filters	BBW-S	F15F-438F-FE23-4A27	BLOCKBIT UTM 1.5.7 build 19672820	Device Webfilter		Webfilter Policies	 
Webfilter 2	Pool Web Filters	BBW-S	508F-E28D-845A-97EB	BLOCKBIT UTM 1.5.7 build 19672820	Device Webfilter		Webfilter Policies	 
Webfilter 3	Pool Web Filters	BBW-S	F1A7-AF24-251E-4085	BLOCKBIT UTM 1.5.7 build 19672820	Device Webfilter		Webfilter Policies	 
Store 1	Stores	BBW-S	B38D-8E59-6C7D-543C	BLOCKBIT UTM 1.5.7 build 19672820	Device Store	Store Policies		 
Store 2	Stores	BBW-S	745E-69F2-CC3B-FEDF	BLOCKBIT UTM 1.5.7 build 19672820	Device Store	Store Policies		 
Store 3	Stores	BBW-S	D96E-65C4-2583-756A	BLOCKBIT UTM 1.5.7 build 19672820	Device Store	Store Policies		 

1 / 8 page

Aba “*Inventory*”

Esta seção irá demonstrar como:

- *Cadastrar*, *Editar* e *Remover devices*;
- *Administrar grupos de devices*;
- *Sincronizar os devices com o GSM*;
- Etc.

A seguir, analisaremos as funções localizadas no topo deste painel.

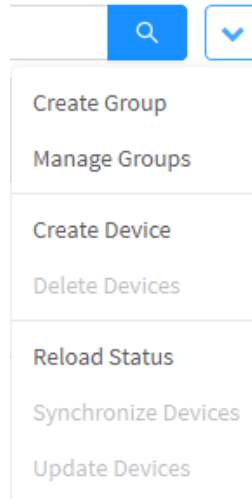
Inventory - Menu de ações

No topo direito da tela temos o menu de ações:



Inventory – Botão do menu de ações.

Ao clicar neste botão o menu abaixo é exibido:



Inventory – Menu de ações.

O menu é composto das seguintes opções:

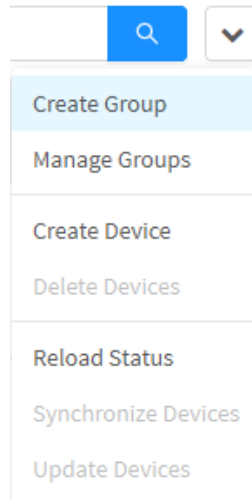
- [Create Group](#);
- [Manage Groups](#);
- [Create Device](#);
- [Delete Devices](#);
- [Reload Status](#);
- [Synchronize Devices](#);
- [Update Devices](#).

A seguir cada opção do menu de ações será detalhada.

Inventory - Menu de ações - Create Group

Os grupos de *devices* ou *Device Manager* têm como objetivo, organizar os *devices* cadastrados. Eles também facilitam a instalação de configurações (*deploy*) para os diversos *devices* em uma única ação, ou seja, não é necessário aplicar configurações em cada um deles, basta apenas selecionar o grupo e este será exibido e no caso de desejar alterar algo, todas as aplicações serão realizadas de uma única vez. Para criar os grupos de *devices*, siga os seguintes passos:

1. Clique no ícone **Menu de ações** ;
2. Selecione a opção "Create Group";



Inventory - Menu de ações - Create Group

3. Uma tela "Add Group" aparecerá, permitindo criar o grupo desejado. Preencha os campos:

Add Group
X

* Name

Description

Devices

Store 1 X
Store 2 X
Store 3 X

Logger

Logger

Cancel
Save

Inventory – Add Group

- **Name:** Nome do Grupo. Ex.: *Stores*;
- **Description:** Descrição do grupo de *devices*. Ex.: *Store Group*;
- **Devices:** Aqui se determina quais *devices* fazem parte do grupo que está sendo criado (pode-se deixar em branco para adicionar os *devices* depois em *Inventory - Menu de ações - Create Device*, ou em *provisioning* na opção *Provisioning - Menu de ações - Create Device*). Os *devices* adicionados neste campo serão inseridos como *tags*;
- **Logger:** Tem como função determinar o *logger* que será utilizado para enviar relatórios (*logs*) para o *analyzer*.

Caso deseje cancelar clique no botão **Cancel** . Para concluir a criação do pacote de política clique no botão **Save** .

✔ Group registered with success!

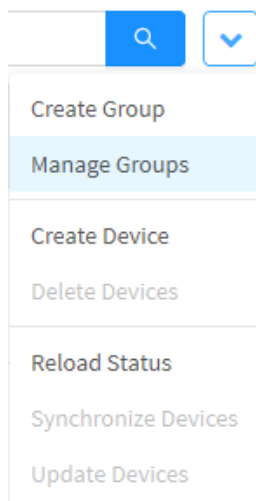
Group registered with success

O grupo foi criado com sucesso. Após a adição do grupo, é possível administrá-los em *Inventory - Menu de ações - Manage Groups*.

Inventory - Menu de ações - Manage Groups

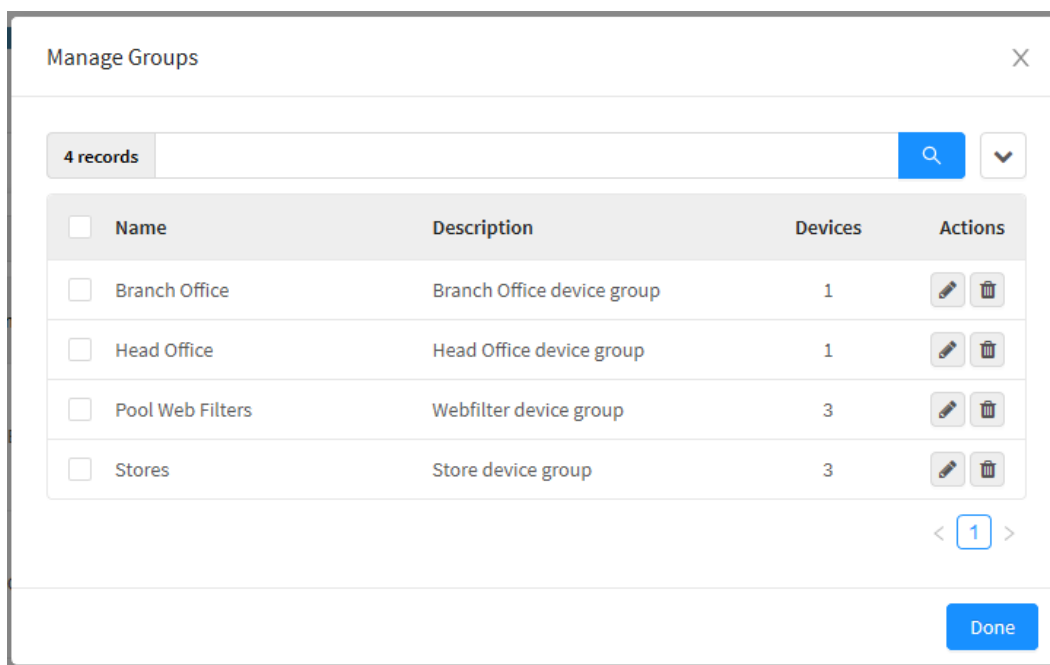
Para gerenciar os grupos de *device*. Siga os seguintes passos:

1. Clique no ícone de **Menu de ações** ;
2. Clique na opção "*Manage Groups*";



Inventory – Menu de ações – Manage Groups

3. A tela de administração dos grupos será exibida:



Inventory – Menu de ações – Manage Groups

A seguir analisaremos cada componente desta janela.

Para mais informações a respeito do menu de ações desta janela, clique nesta [página](#).

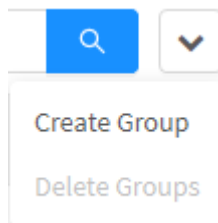
Manage Groups - Menu de ações

No topo direito da tela temos o menu de ações:



Manage Groups – Botão do menu de ações

Ao clicar neste botão o menu abaixo é exibido:



Manage Groups – Menu de ações

O menu é composto das seguintes opções:

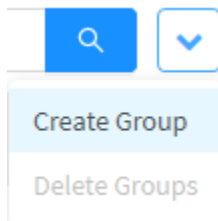
- [Create Group](#);
- [Delete Groups](#).

A seguir cada opção do menu de ações será detalhada.

Manage Groups - Create Group

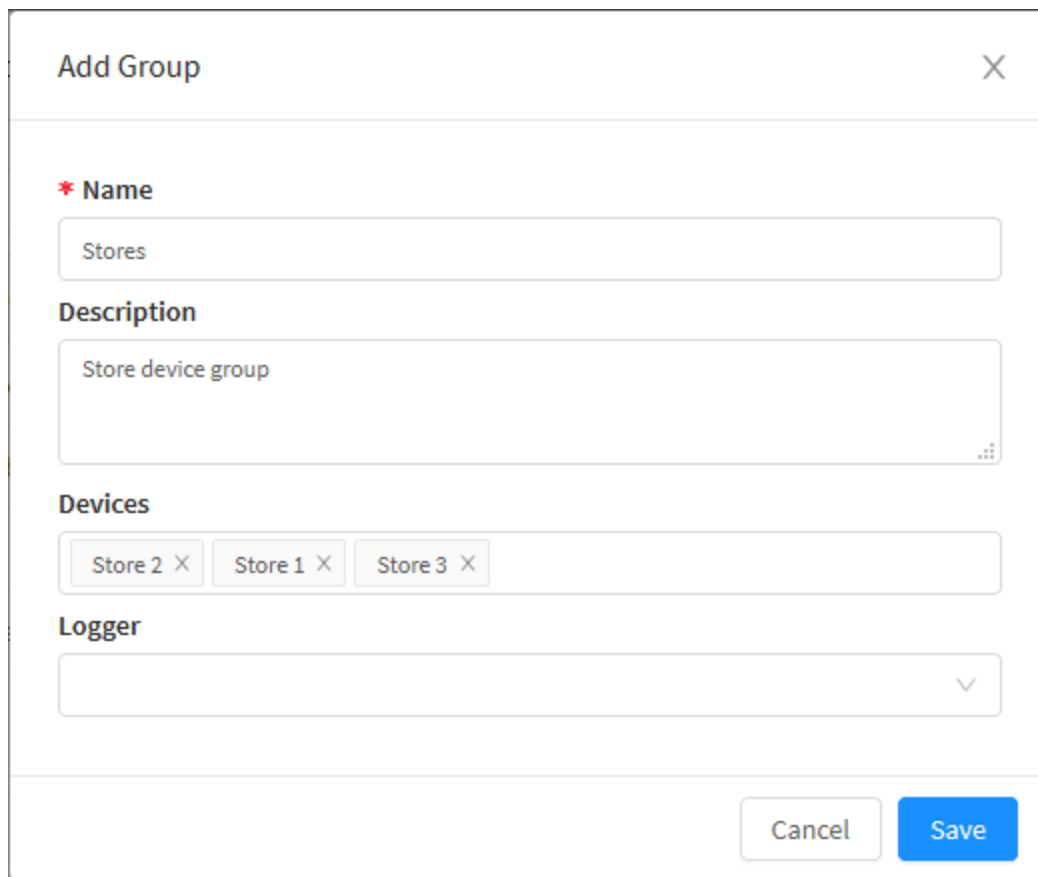
Os grupos de *devices* ou *Device Manager* têm como objetivo, organizar os *devices* cadastrados. Eles também facilitam a instalação de configurações (*deploy*) para os diversos *devices* em uma única ação, ou seja, não é necessário aplicar configurações em cada um deles, basta apenas selecionar o grupo e este será exibido e no caso de desejar alterar algo, todas as aplicações serão realizadas de uma única vez. Para criar os grupos de *devices*, siga os seguintes passos:

1. Clique no ícone **Menu de ações** ;
2. Selecione o botão "Create Group";



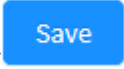
Inventory – Menu de ações - Create Group.

3. A tela "Add Group" aparecerá, permitindo criar o grupo desejado. Preencha os campos:

A screenshot of a web form titled 'Add Group' with a close button (X) in the top right corner. The form contains several sections: 'Name' with a red asterisk and a text input field containing 'Stores'; 'Description' with a text area containing 'Store device group'; 'Devices' with a horizontal list of three tags: 'Store 2 X', 'Store 1 X', and 'Store 3 X'; and 'Logger' with a dropdown menu showing a downward arrow. At the bottom right, there are two buttons: 'Cancel' and 'Save'.

Inventory – Add Group.

- **Name:** Nome do Grupo. Ex.: *Stores*;
- **Description:** Descrição do grupo de *devices*. Ex.: *Store device group*;
- **Devices:** Aqui se determina quais *devices* fazem parte do grupo que está sendo criado (pode-se deixar em branco para adicionar os *devices* depois em [Inventory - Menu de ações - Create Device](#), ou em *provisioning* na opção [Provisioning - Menu de ações - Create Device](#)). Os *devices* adicionados neste campo serão inseridos como *tags*.
- **Logger:** Tem como função determinar o [logger](#) que será utilizado para enviar relatórios (*logs*) para o [analyzer](#).

Caso deseje cancelar clique no botão **Cancel** . Para concluir o procedimento clique no botão **Save** .

 **Group registered with success!**

Group registered with success

O grupo foi criado com sucesso. Após a adição do grupo, é possível administrá-los em [Inventory - Menu de ações - Manage Groups](#).

Para mais informações a respeito de como deletar os grupos, consulte esta [página](#).

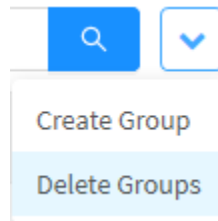
Manage Groups - Delete Groups

No Blockbit GSM é possível deletar grupos de *device*. Siga os seguintes passos:

1. Selecione o grupo que se deseja deletar clicando na **seleção** [];

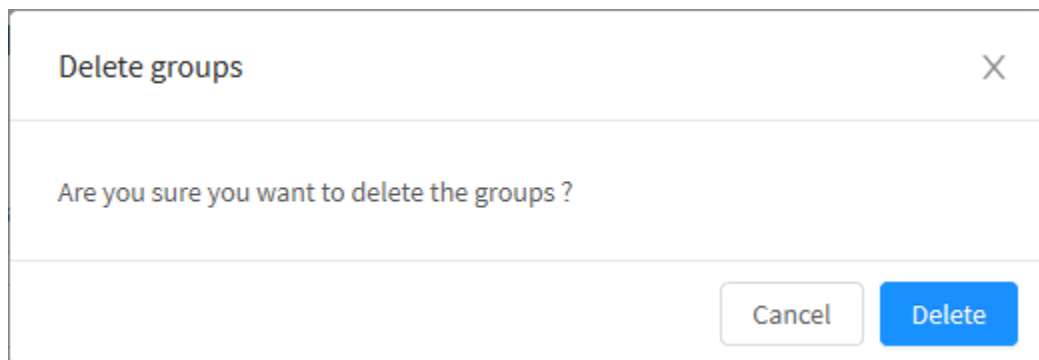
2. Clique no ícone de **Menu de ações** [];

3. Clique na opção "Delete Groups";

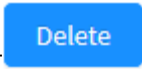
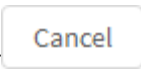


Inventory – Menu de ações – Delete Groups.

4. Surgirá uma mensagem de confirmação verificando se deseja deletar o grupo selecionado:



Inventory - Delete groups message.

Clique no botão **Delete** [] ou clique em **Cancel** [] para voltar ao painel anterior.

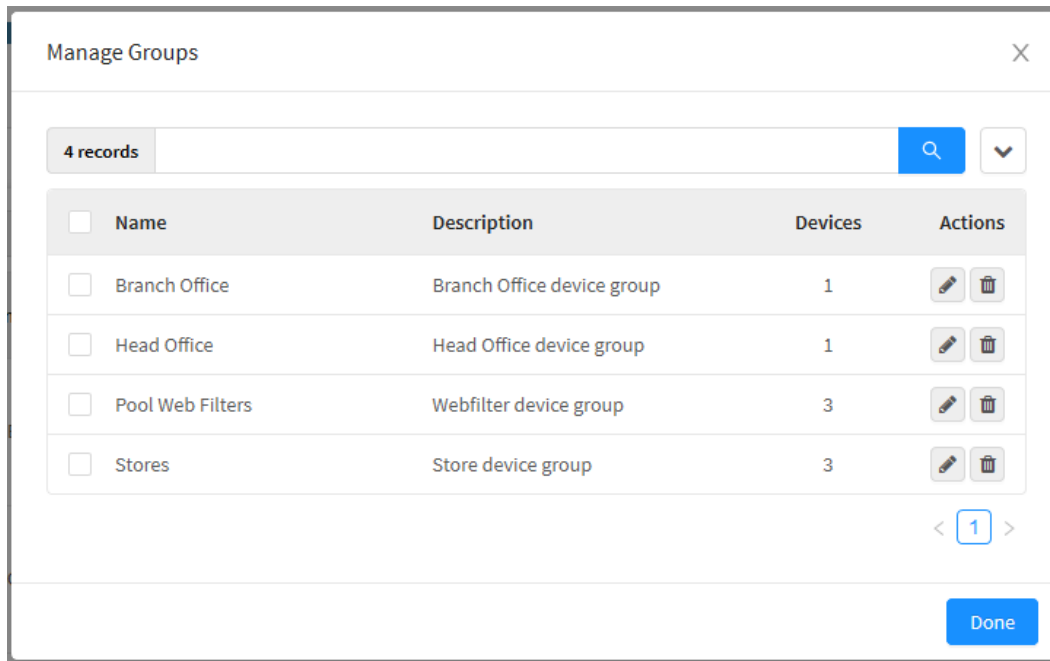
 **Group deleted successfully**
Group deleted successfully

O grupo foi removido com sucesso.

A seguir vamos analisar os componentes das **colunas**.

Manage Groups - Colunas

A seguir explicaremos cada coluna da janela *Manage Groups*:

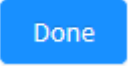


☐	Name	Description	Devices	Actions
☐	Branch Office	Branch Office device group	1	 
☐	Head Office	Head Office device group	1	 
☐	Pool Web Filters	Webfilter device group	3	 
☐	Stores	Store device group	3	 

Manage Groups - Colunas.

A seguir explicaremos cada coluna:

- **Caixa de Seleção** [☐]: Seleciona o grupo.
- **Name**: Apresenta o nome do grupo cadastrado;
- **Description**: Apresenta a descrição do grupo cadastrado;
- **Devices**: Quantia de *devices* cadastrados no grupo;
- **Actions**: A coluna "Actions" é composta por dois botões:
 - **Botão Edit** []: Edita dados do grupo cadastrado;
 - **Botão Delete** []: Remove o grupo.

Clique no **botão** [] no canto superior direito ou em **Done** [] para fechar esta janela.

Para mais informações sobre como Criar um Device, consulte esta [página](#).

Inventory - Menu de ações - Create Device

Para a integração do Blockbit GSM e o Blockbit UTM é necessário realizar os cadastros dos *devices*.

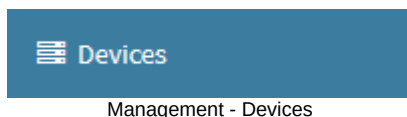


O cadastro dos *devices* deve obrigatoriamente ser realizado na seguinte ordem: primeiro no Blockbit GSM e posteriormente no Blockbit UTM.

Neste momento iremos realizar o cadastro dos *devices*. Para realizar este cadastro é necessário acessar a *Interface Web* do Blockbit GSM e a *Interface Web* do Blockbit UTM. Para facilitar a compreensão será descrito antes do início do passo a passo uma referência em negrito e sublinhado com o nome da interface na qual estamos trabalhando:

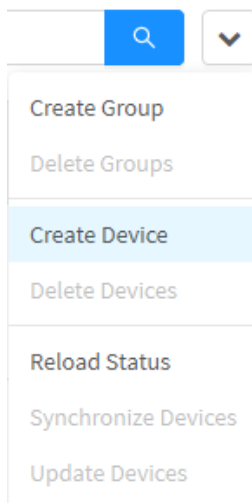
Interface Web Blockbit GSM:

1. Conforme mencionado anteriormente, no menu vertical a esquerda, inicialmente, clique no botão “*Devices*” a aba “*Inventory*” estará aberta automaticamente;



2. Clique no ícone do **Menu de ações** ;

3. Clique na opção “*Create Device*”;



Inventory – Menu de ações – Add Device.

4. A tela de adição de *device* aparecerá, preencha os seguintes campos da tela “*Create device*”:

Add Device
X

* Name

* Company

* Deploy Key

* API Key

* User Admin

Password

Device Group

Logger

Description

Cancel
Save

Inventory – Add Device.

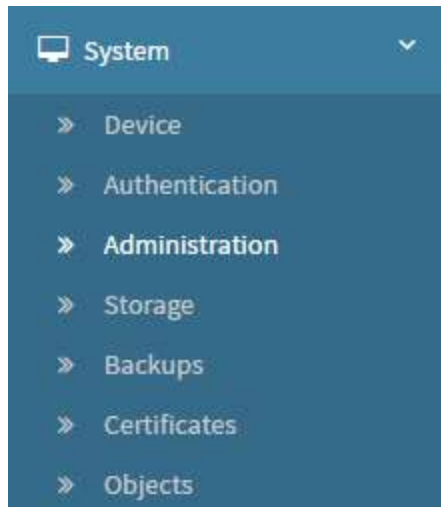
Nesta tela existem duas informações que não foram citadas na sessão anterior, elas devem ser obtidas na *Interface Web* do Blockbit UTM. Essas informações são: *Deploy Key* e *API Key*.

5. Acesse a Interface do Blockbit UTM;

Interface Web Blockbit UTM:

6. Entre no **Menu System** [ System <] localizado a esquerda da interface;

7. Clique no botão **Administration** [];



Menu System – Administration.

8. Clique na aba “Central Management” a seguinte interface será exibida:

Menu System – Administration – Aba “Central Management”.

9. Preencha os campos, conforme exemplificado:

- **Enable Manager** ☒: Habilita o módulo de integração com o Blockbit GSM;
- **Address**: Endereço IP ou *Hostname* do *Blockbit* GSM. Ex.: 172.16.102.235;
- **Deploy Service**: Porta de comunicação com o *Blockbit* GSM, valor padrão: 444;



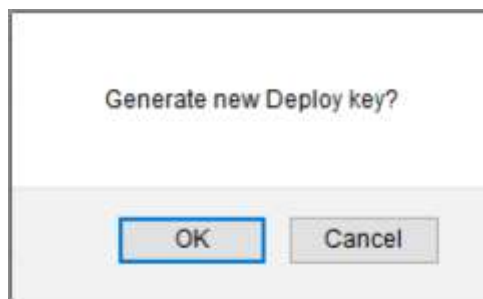
A comunicação é sempre iniciada pelo Blockbit UTM com o destino Blockbit GSM, na porta de comunicação TCP 444 (Porta Deploy, configurável no System Settings do Blockbit GSM).



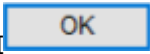
Deve ser criada uma Policy permitindo que as devices se comuniquem com o Blockbit GSM na porta TCP 444.

- **Administrator:** Seleciona o usuário de integração que o Blockbit GSM irá utilizar para administrar o Blockbit UTM. Ex.: admin;
- **Status:** Identifica o status da comunicação com o Blockbit GSM. Ex.: *Offline*;
- **Deploy key:** Chave de criptografia da comunicação entre o Blockbit UTM e o Blockbit GSM. Caso este campo não esteja preenchido, siga os seguintes passos:

- Para gerar a "Deploy key", clique no botão . Surgirá a mensagem se deseja gerar uma Deploy key;



Generate new deploy key.

- Clique no botão **OK** . O sistema irá gerar a Deploy key, conforme demonstrado abaixo:

Deploy key



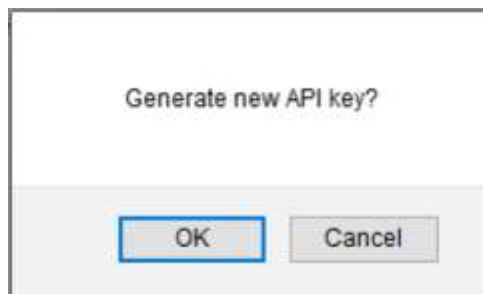
53616c7465645f5fff8659699b473fce0282effb7fdb67c5cdeaccd18b482aa8ef479c83bb49b23!



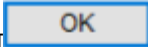
Deploy key.

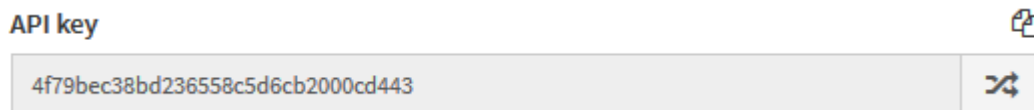
- **API Key:** Chave criptográfica do usuário do Blockbit UTM, com permissões de administração e de uso da API de comunicação com o Blockbit GSM. Caso este campo não esteja preenchido, siga os seguintes passos:

- Para gerar a API key, clique no botão . Surgirá a mensagem se deseja gerar uma API key;



Generate new API key.

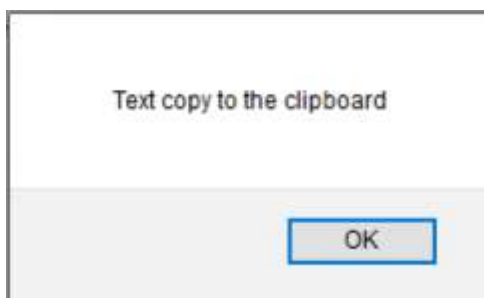
- Clique no botão **OK** . O sistema irá gerar a *API key*, conforme demonstrado abaixo:



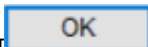
API key.

10. Clique no botão **Save**  localizado no canto superior direito da tela para salvar as configurações;

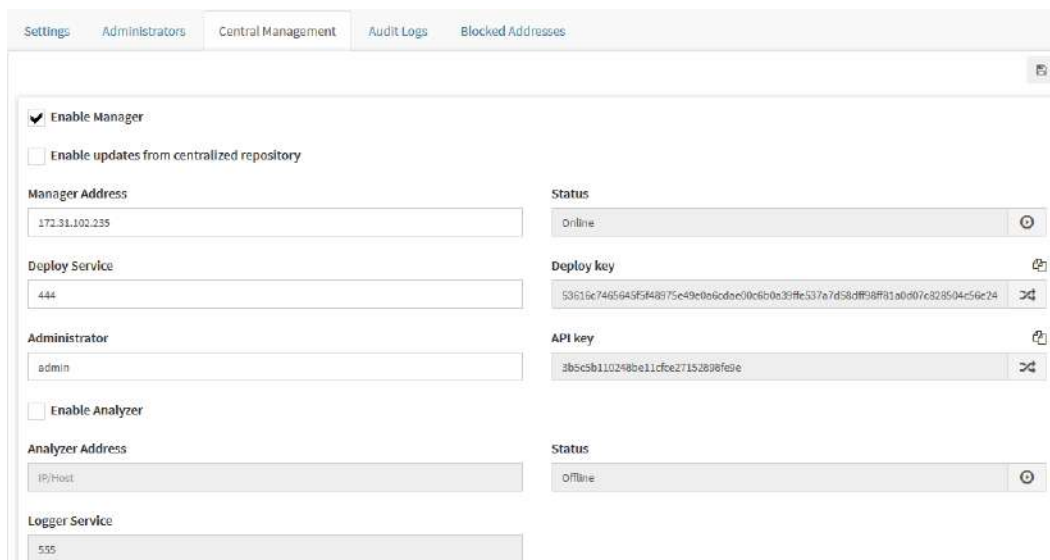
11. Copie a *Deploy key* para inserir no Blockbit GSM. Para copiar a chave, clique no botão **copy**  da *Deploy Key*. Irá aparecer a seguinte mensagem:



Texto copiado para área de transferência – *Deploy Key*.

- Clique no botão **OK** .

Após completar todos os campos, se chegará no seguinte resultado:

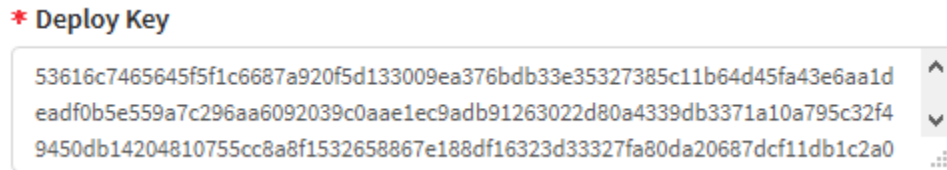


Aba “*Central Management*” completa.

12. Retorne para a *Interface Web* do Blockbit GSM;

Interface Web Blockbit GSM:

13. No painel de “Add Device”, cole a *Deploy Key* na caixa de texto correta;

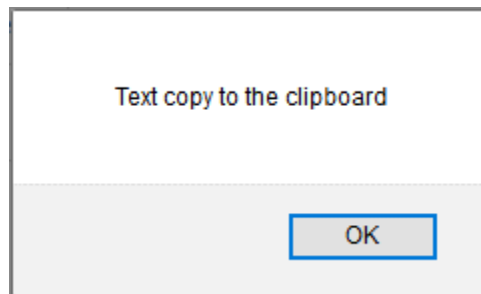


Add Device – Deploy Key.

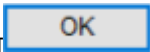
14. Retorne para a *Interface Web* do Blockbit UTM;

Interface Web Blockbit UTM

15. Copie a *API key* para inserir no Blockbit GSM. Para copiar a chave, clique no botão **copy**  da *API key*. Irá aparecer a seguinte mensagem:



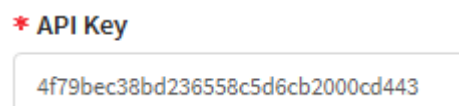
Texto copiado para área de transferência – *API Key*.

Clique no botão **OK** ].

16. Retorne para a *Interface Web* do Blockbit GSM;

Interface Web Blockbit GSM:

17. No painel “Add Device”, cole a *API key* na caixa de texto correta;



18. Preencha os demais dados:

- **Name:** Digite o nome que identifica a *device* no Blockbit GSM. Ex.: *Cluster Head Office*;
- **Company:** Digite o nome da empresa que possui a *Device*. Ex.: Blockbit;
- **Model:** Selecione o modelo do device. Ex.: *BB-10*;
- **User Admin:** Usuário do Blockbit UTM com permissões de administração. Será utilizado quando desejar acessar a *Interface Web* do Blockbit UTM através do Blockbit GSM. Ex.: *admin*;
- **Password:** Senha do usuário do Blockbit UTM com permissões de administração. Caso não seja inserida, será solicitada a senha no momento que realizar o acesso a *device*;
- **Device Group:** Selecione o grupo ao qual deseja adicionar o *device*. Ex.: *Head Office*;
- **Logger:** É um campo opcional, selecione na lista suspensa, qual *Logger* será utilizado para gerar relatórios. Para mais informações, cheque as páginas a respeito de [Loggers](#). Ex.: *Logger1*;



Caso esteja utilizando *Cluster* de *Loggers*, atente que não é possível vincular um *device* a um *logger* que não esteja ativo no *cluster*. Para mais informações a respeito de como efetuar a ativação manualmente, consulte esta [página](#).

- **Description:** É um campo opcional, digite uma descrição caso seja necessário.

Após completar todos os campos, teremos chego em um resultado semelhante ao demonstrado pela imagem abaixo:

Add Device
X

* Name
Cluster Head Office

* Company
Blockbit

* Deploy Key
53616c7465645f5f48975e49e0a6cdae00c6b0a39ffe537a7d58dff98ff81a0d07c828504c56e240bed6ece8fd5c1fbd0466bd27e2d2adc7321385449b0015329299005bd3ed6bb320f20729e4aa6ae15f0f1ed828b9287d1acec4fca0c9a2519077bd18c3888d686118434e5c0c

* API Key
3b5c5b110248be11cfce27152898fe9e

Model
BB-5

* User Admin
admin

Password
••••••••

Device Group
Head Office

Logger

Description
Head Office
IP: 172.31.102.220
Logger

Cancel Save

Inventory – Add Device – exemplo.

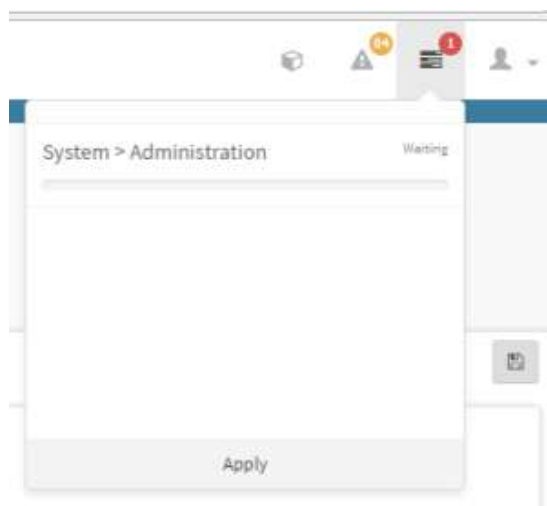
Clique no botão **Save** [Save].

O device foi adicionada com sucesso, a tela *Device Manager* surgirá;

19. Retorne para a *Interface Web* do Blockbit UTM;

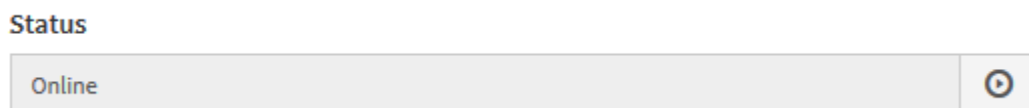
Interface Web Blockbit UTM

20. Clique no ícone **Fila de configurações salvas** [Fila de configurações salvas] para fazer o “Apply” das configurações;



Fila de configurações salvas.

21. Clique no botão "Apply". A comunicação entre o Blockbit UTM e o Blockbit GSM será estabelecida e na tela *Central Manager*, o campo *Status* será alterado de "Offline" para "Online";



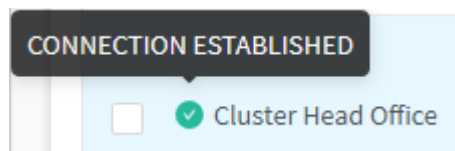
Status - Online.

O cadastro da *device* foi realizado com sucesso no Blockbit UTM.

22. Retorne para a *Interface Web* do Blockbit GSM;

Interface Web Blockbit GSM

23. Na tela *Device Manager* em frente ao campo *Device Name* aparecerá o ícone **online** [] na frente do nome do device criado, informando que a comunicação foi estabelecida com sucesso.



Inventory – Connection Established.

Caso deseje cadastrar outros *devices*, repita os passos demonstrados anteriormente. Em nosso exemplo, ao término de todos os cadastros necessários, teremos um ambiente semelhante a esse:

Devices

Inventory [Communities](#) [Templates](#) [Provisioning](#)

9 records

Name	Group	Model	License Status	Version	Template	Policy (IPv4)	Policy (IPv6)	Actions
☐ Branch Office	Branch Office	BDV-S	S2E9-BAAS-C79D-C94H	BLOCKBRT UTM 1.5.7 Build 19672823	Device Branch Office			
☐ Cluster Head Office	Head office	BDV-S	9F5D-015D-D45C-075C	BLOCKBRT UTM 1.5.7 Build 19672823	Device Head Office			
☐ WebFilter 1	Pool Web Filters	BDV-S	F33F-436F-FF23-FA27	BLOCKBRT UTM 1.5.7 Build 19672823	Device Webfilter		Webfilter Policies	
☐ WebFilter 2	Pool Web Filters	BDV-S	508F-E282-945A-97ED	BLOCKBRT UTM 1.5.7 Build 19672823	Device Webfilter		Webfilter Policies	
☐ WebFilter 3	Pool Web Filters	BDV-S	FB47-AF24-257D-4D55	BLOCKBRT UTM 1.5.7 Build 19672823	Device Webfilter		Webfilter Policies	
☐ Store 1	Stores	BDV-S	B36D-8ED9-6C7D-943C	BLOCKBRT UTM 1.5.7 Build 19672823	Device Store		Store Policies	
☐ Store 2	Stores	BDV-S	715F-69F2-CC3B-7BD7	BLOCKBRT UTM 1.5.7 Build 19672823	Device Store		Store Policies	
☐ Store 3	Stores	BDV-S	D92E-92C4-256B-752A	BLOCKBRT UTM 1.5.7 Build 19672823	Device Store		Store Policies	

1 / 35 / page

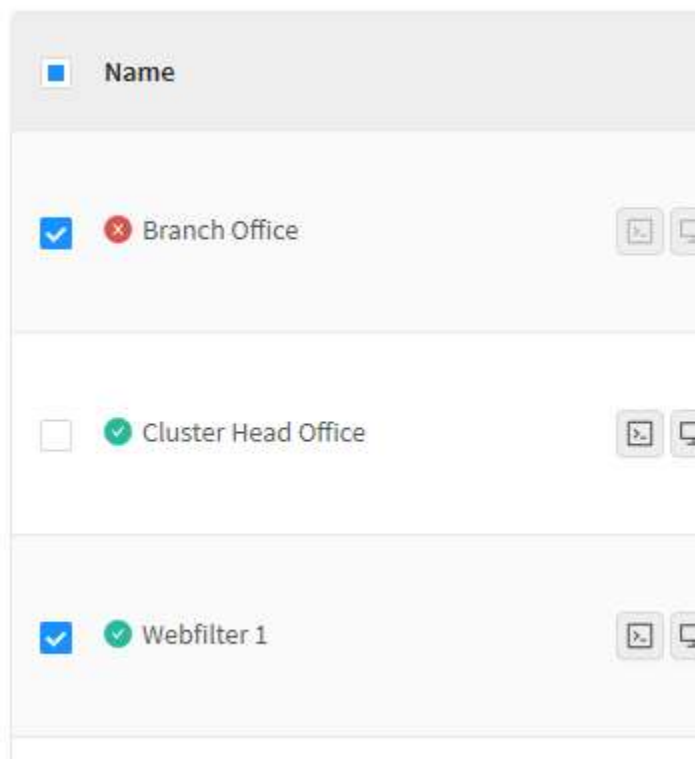
Device Manager – Devices Cadastradas.

À seguir vamos analisar como [remover os devices](#).

Inventory - Menu de ações - Delete Devices

Através do menu de ações é possível deletar vários *devices* ao mesmo tempo. Siga os seguintes passos:

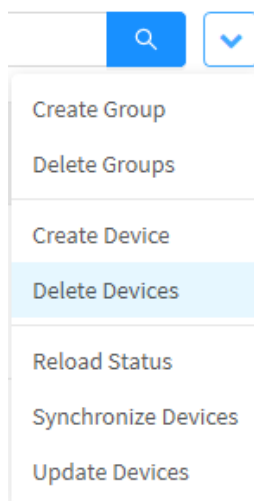
1. Selecione os *devices* que deseja deletar clicando no ícone de **seleção** , localizado na coluna "Actions", do lado direito do ícone de lixeira. Ex.: *Branch office 1*, *Cluster Head Office* e *Store 1*;



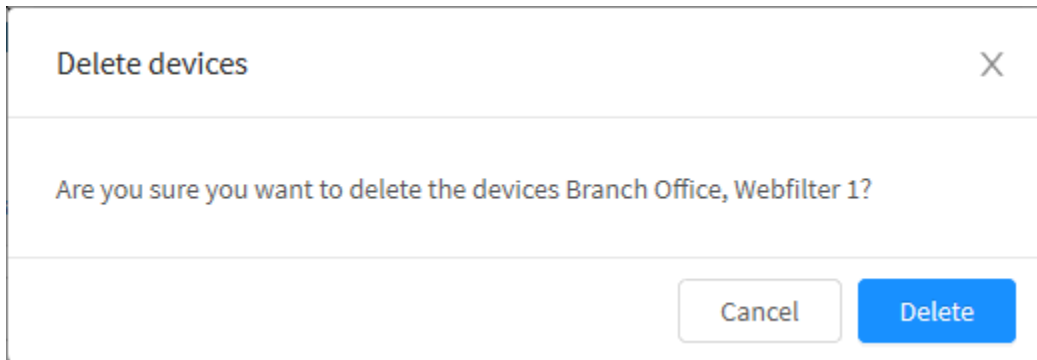
Device Manager – Device selecionadas

2. Clique no **Menu de ações** ;

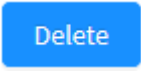
3. Clique na opção "Delete Devices";



4. Surgirá uma tela perguntado se deseja deletar o *device* selecionado:



Inventory – Delete Devices

Clique no botão **Delete** ].

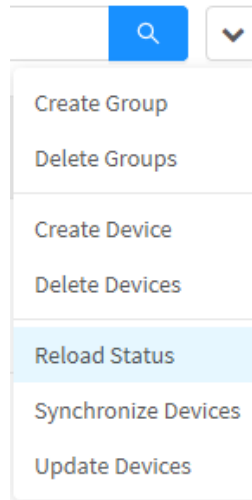
 **Device deleted successfully**
Device deleted successfully

Os *devices* foram deletados com sucesso.

Inventory - Menu de ações - Reload Status

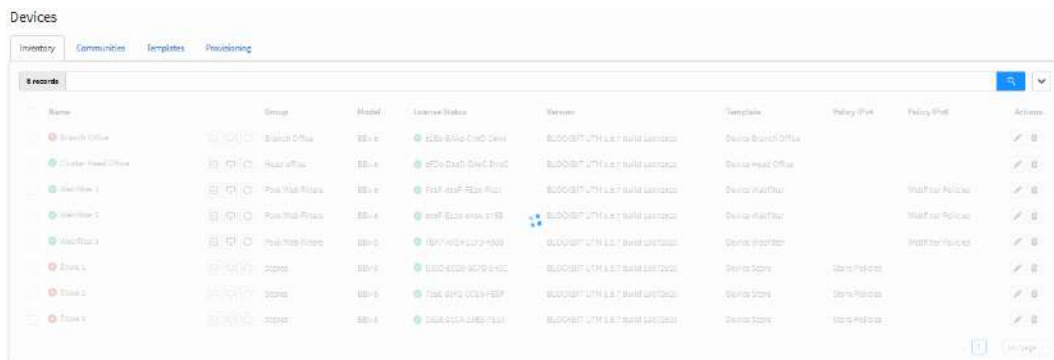
Atualiza o status de todos os dispositivos cadastrados no GSM. Para efetuar essa operação, siga os passos:

1. Clique no **Menu de ações** ;
2. Clique na opção **"Reload Status"**;



Inventory – Menu de ações – Reload Status

3. Aguarde o painel ficar disponível novamente:



Name	Group	Model	License Status	Version	Template	Policy (Pkt)	Policy (Pkt)	Actions
Branch Office	Branch Office	BB-6	BB-6 BB-6 C-100 Dev	8.000.001.07M.8.0.7 build 1000000	Device Branch Office			 
Cluster Head Office	Head Office	BB-6	BB-6 BB-6 C-100 Dev	8.000.001.07M.8.0.7 build 1000000	Device Head Office			 
Head Office 1	Head Office	BB-6	BB-6 BB-6 C-100 Dev	8.000.001.07M.8.0.7 build 1000000	Device Head Office			 
Head Office 2	Head Office	BB-6	BB-6 BB-6 C-100 Dev	8.000.001.07M.8.0.7 build 1000000	Device Head Office			 
Head Office 3	Head Office	BB-6	BB-6 BB-6 C-100 Dev	8.000.001.07M.8.0.7 build 1000000	Device Head Office			 
Head Office 4	Head Office	BB-6	BB-6 BB-6 C-100 Dev	8.000.001.07M.8.0.7 build 1000000	Device Head Office			 
Head Office 5	Head Office	BB-6	BB-6 BB-6 C-100 Dev	8.000.001.07M.8.0.7 build 1000000	Device Head Office			 
Head Office 6	Head Office	BB-6	BB-6 BB-6 C-100 Dev	8.000.001.07M.8.0.7 build 1000000	Device Head Office			 

Inventory – Reload all devices

Após este passo, o **status** terá sido recarregado e exibido no mesmo painel.

Inventory - Menu de ações - Synchronize Devices

Para sincronizar as informações de todos os dispositivos cadastrados no GSM, siga os passos:

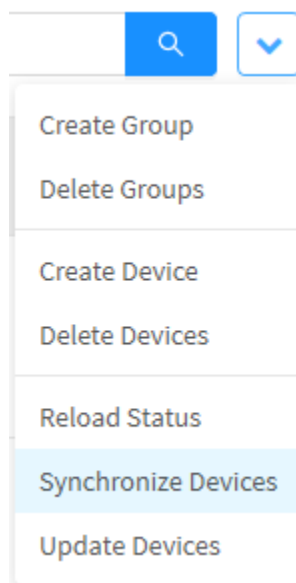
1. Selecione os *devices* que deseja deletar clicando no ícone de **seleção** , localizado na coluna "Actions", do lado direito do ícone de lixeira. Ex.: *Branch office 1*, *Cluster Head Office* e *Store 1*;

	Name	Group
 	Branch Office	   Branch Off
 	Cluster Head Office	   Head Offic
 	Webfilter 1	   Pool Web I

Inventory – Device selecionada.

2. Clique no **Menu de ações** ;

3. Clique na opção "Synchronize Devices";



Inventory – Menu de ações – Synchronize.

Todas as sincronizações serão realizadas com sucesso.



Vale lembrar que ao adicionar um dispositivo UTM ao GSM, a primeira sincronização acontece de maneira automática.

O Blockbit GSM realiza sincronização das informações de TODOS os devices a cada 30 minutos automaticamente.

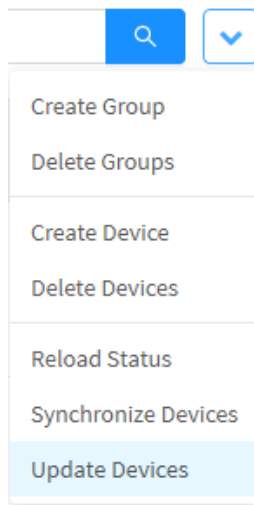
Inventory - Menu de ações- Update Devices

Executa a atualização da versão dos dispositivos cadastrados no GSM. Para efetuar essa operação, siga os passos:

1. Selecione os *devices* desejados clicando na **caixa de seleção** [] desejada;

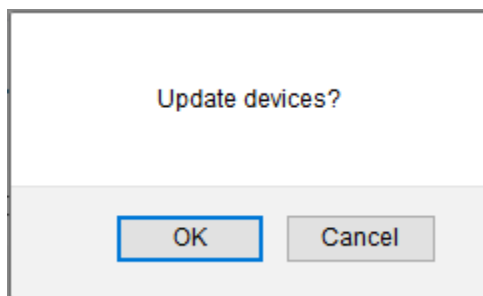
2. Clique no **Menu de ações** [];

3. Clique na opção "*Update Devices*";

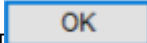
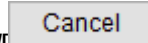


Inventory – Menu de ações – Update Devices

4. Surgirá a mensagem de verificação:



Update devices

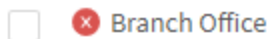
5. Para atualizar os dispositivos selecionados clique em **OK** [], caso contrário clique em **Cancel** [].

Inventory - Coluna "Name"

A coluna "Name" apresenta as devices que foram anteriormente cadastradas, ordenadas em seus respectivos grupos.

Ao lado do nome de cada device cadastrada existe um símbolo que indica o **status da conexão entre o Blockbit GSM e o Blockbit UTM.**

Se o símbolo vermelho estiver sinalizado, significa que aquele device não está conectada:



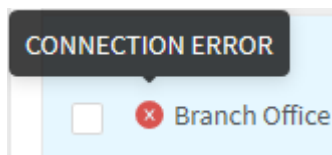
Inventory – Device sem conexão.

Se o símbolo verde estiver sinalizado, significa que aquele device está conectada corretamente:

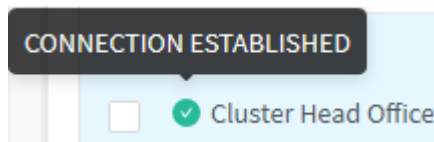


Inventory – Device conectada – Online.

Caso queira verificar o status basta colocar o mouse em cima do botão de status para que uma mensagem seja exibida:



Inventory - Connection error.



Inventory – Connection Established.

Inventory - Botões de ações

Ainda na Coluna *Device Name*, logo a direita do nome do device, existem três botões de ação: **Access CLI (Command Line Interface)** , **Access Interface Web**  e **Synchronize** :



Botões de ação – *Device Name*.

A seguir estaremos apresentando cada um deles.

- [Access CLI](#);
- [Access Interface Web](#);
- [Synchronize](#).

Inventory - Botão de ações - "Access CLI"

O botão de ação "Access CLI" - *Command Line Interface*: acessa a interface texto (*shell*) através da conexão existente com o Blockbit GSM:



Botão "Access CLI" – *Command Line Interface*.



Clique no botão **Access CLI**[]. Ele abrirá uma nova aba no navegador para realizar acesso a interface via *shell*.

Inventory - Botão de ações - "Access Interface Web"

O botão de ação "Access Interface Web" acessa a interface *web* da *device* através da conexão existente com o Blockbit GSM, ou seja, abre uma aba no navegador para acessar diretamente o Blockbit UTM desejado:



Botão "Access Interface Web".



O acesso ao Blockbit UTM também pode ser realizado diretamente no endereço IP da device na porta TCP 98. Ex.: <https://172.16.102.220:98>

Ao clicar no botão "Access Interface Web" pode ocorrer um anti *pop-up* do *browser*. Caso ocorra irá aparecer um símbolo em vermelho avisando que a *pop-up* está bloqueada no canto superior direito da tela do navegador:



Botão "Access Interface Web" – *Pop-up* bloqueada.

É necessário desbloquear. Para isso siga os passos:

1. Clique no botão de bloqueio da *pop-up*, localizado no canto superior direito do navegador;
2. Surgirá a tela para desbloqueio do *pop-up*;
3. Clique no botão "Permitir".

O desbloqueio foi realizado com sucesso. Para prosseguir, clique novamente no botão "Access Interface Web". Ele abrirá uma nova aba no navegador com acesso ao Blockbit UTM.

Inventory - Botão de ações - "Update/Synchronize"

O botão de ação "Update/Synchronize" permite sincronizar ou fazer update da device:



Botão "Update/Synchronize".

Ao clicar no botão **Update/Synchronize** . A seguinte janela será exibida:

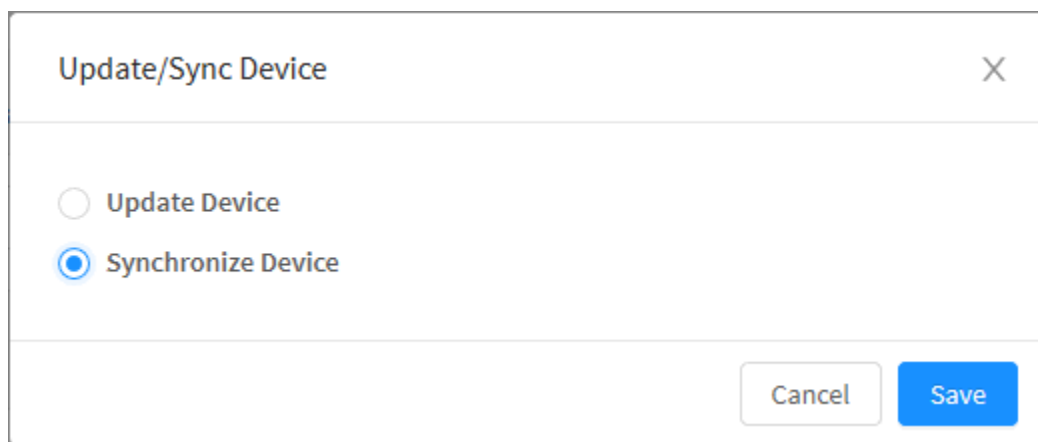
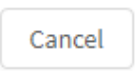
A dialog box titled "Update/Sync Device" with a close button (X) in the top right corner. It contains two radio button options: "Update Device" and "Synchronize Device". The "Synchronize Device" option is selected, indicated by a blue dot. At the bottom right, there are two buttons: "Cancel" and "Save".

Figura 86 – Update/Sync Device.

A seguir analisaremos ambas opções:

- **Update:** Esta opção tem como função, efetuar a atualização da device para a versão mais atual disponível.Ex.: Um UTM 14.6 sendo atualizado para um UTM 1.5.2;
- **Synchronize:** A função desta opção é sincronizar as informações da device em questão com a aba "Device Manager", permitindo a exibição do Status da Licença, a versão e diversas outras informações;

Caso deseje cancelar clique no botão **Cancel** . Ao clicar no botão **save**  a atualização ou sincronização será efetuada.

A sincronização e atualização foram realizadas com sucesso.

Inventory - Coluna "Group"

A coluna "Group" apresenta os grupos de *devices* cadastrados.

Group
Branch Office
Head Office
Pool Web Filters

Inventory – Group.

Ao clicar em um dos grupos, todos os *appliances* categorizados com o grupo clicado serão exibidos, conforme demonstrado abaixo:

3 records		group:"Stores"	
☐	Name	Group	
☐	☒ Store 1	View Edit Refresh	Stores
☐	☒ Store 2	View Edit Refresh	Stores
☐	☒ Store 3	View Edit Refresh	Stores

Inventory – Group - Selected.

Caso o grupo seja clicado novamente, a tela anterior será exibida novamente.

Para mais informações, a respeito de grupos de *device*, cheque [Inventory - Menu de ações - Manage Groups](#).

Inventory - Coluna "Model"

A coluna "*Model*" apresenta os modelos dos *devices* cadastrados.

Model
BBv-1
BBv-5
BBv-10

Inventory – Model.

Ao clicar em um dos modelos, todos os *appliances* do modelo clicado serão exibidos, conforme demonstrado abaixo:

Devices

Inventory					Communities					Templates					Provisioning				
8 records					model:"BBv-5"														
☐ Name					Group					Model									
☐  Branch Office					   Branch Office					BBv-5									
☐  Cluster Head Office					   Head office					BBv-5									
☐  Webfilter 1					   Pool Web Filters					BBv-5									

Inventory – Model - Selected.

Caso o modelo seja clicado novamente, a tela anterior será exibida novamente.

Inventory - Coluna "License Status"

A coluna "License Status" exibe informações referente as licenças tais como: Status da licença e o número de série da licença.

 3F1F-6A54-83AE-F837

License Status – Número da Licença

Os ícones de status possíveis de serem exibidos são:

- **Active**: Exibe caso a licença está ativa ou inativa e sua respectiva data de ativação (*Begin*) e expiração (*End*);
- **Unknown**: Identifica que o estado da licença é desconhecido. Caso uma licença já esteja ativa e este ícone continue aparecendo, é recomendável efetuar um [sincronismo](#);
- **Expired**: Demonstra que a licença expirou. Para reativá-la, entre em contato com a Blockbit;
- **Inactive**: Demonstra que a licença está inativa.

Inventory - Coluna "Version"

A coluna "Version" apresenta as informações de versão e das atualizações do *firmware* instalados no *device*. Ex.: *Blockbit UTM 1.3.0 build 17022114*.

Version
BLOCKBIT UTM 1.5.7 build 19072820
BLOCKBIT UTM 1.5.7 build 19072820
BLOCKBIT UTM 1.5.7 build 19072820

Inventory – Version



O acesso ao Blockbit GSM permite gerenciar devices em versões de *firmware* diferentes, porém, é altamente recomendado sempre utilizar a versão mais recente e mais atualizada disponível.

Para mais informações a respeito do processo de atualização do Blockbit GSM, cheque [System - Aba "Update"](#).

Inventory - Coluna "Template"

A coluna "*Template*" exibe o nome do *Template* de configurações aplicado no *device*.

Template
Device Branch Office
Device Head Office
Device Webfilter
Device Webfilter

Inventory – Devices Template

Para mais informações a respeito de *templates* de *device*, cheque a [Aba Templates](#).

Inventory - Coluna "Policy IPv4"

A coluna "IPv4 Policy" exibe o nome do pacote de política de IP aplicada no device. Ex.: Policies Branch Office.

Policy IPv4
Store Policies
Store Policies
Store Policies

Inventory – Policy IPv4

Para mais informações, cheque a sessão [Policies](#).

Inventory - Coluna "Policy IPv6"

A coluna "IPv6 Policy" exibe o nome do pacote de política aplicada na device.

Policy
IPv6

Webfilter
Policies

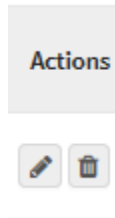
Webfilter
Policies

Inventory – Policies Head Office.

Para mais informações, cheque a sessão [Policies](#).

Inventory - Coluna "Actions"

A coluna *Actions* exibe os botões "*Edit*" e "*Delete*" para cada *device*.



Inventory – Botões "*Edit*" e "*Delete*".

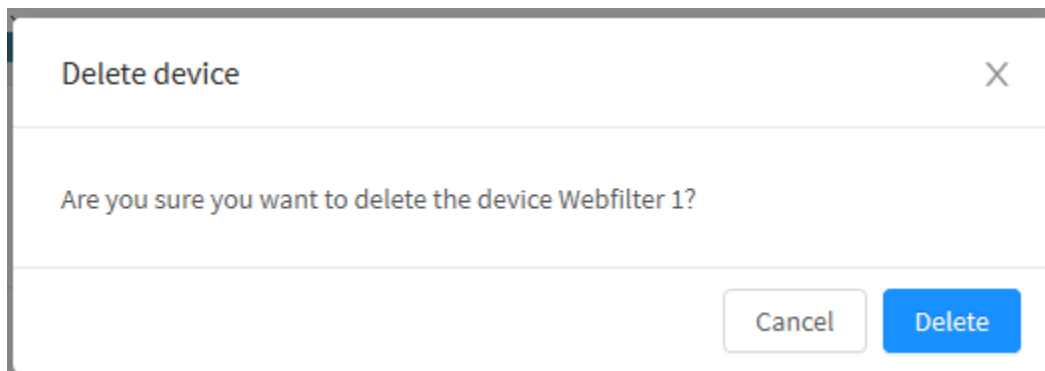
A seguir analisaremos a função de ambos os botões:

- Botão *edit*;
- Botão *delete*.

Inventory - Coluna "Actions" - Botão "Delete"

Através do botão **Delete**  , é possível remover a device ou grupo cadastrado.

1. Determine qual item se deseja deletar;
2. Clique no botão **Delete**  ;
3. Surgirá uma tela perguntando se deseja deletar o item selecionado:



Inventory – Delete device.

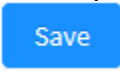
Caso deseje cancelar clique no botão **Cancel**  . Para concluir a remoção, clique no botão **Delete**  .

 **Device deleted successfully**
Device deleted successfully

A remoção foi feita com sucesso.

Inventory - Coluna "Actions" - Botão "Edit"

Através do botão **Edit** ], é possível editar as informações da *device* criados na opção [Inventory - Menu de ações - Create Device](#) ou do grupo selecionado:

1. Determine qual item deseja-se editar;
2. Clique no botão **Edit** ];
3. Edite as informações desejadas;
4. Caso deseje cancelar as alterações feitas clique no botão **Cancel** ]. Para concluir as alterações editadas, clique no botão **Save** ].

As edições foram feitas com sucesso.

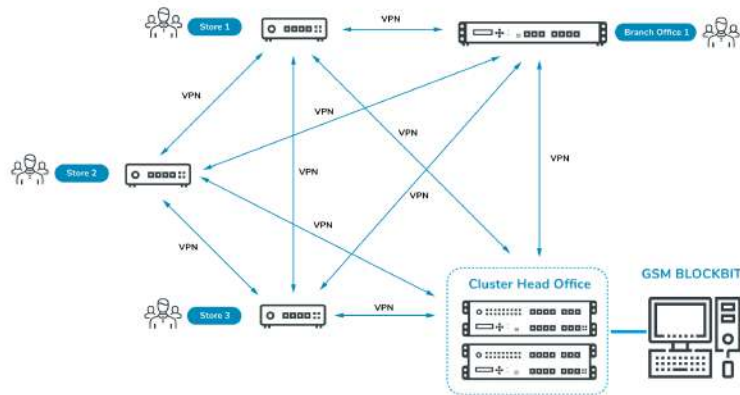
Aba Communities

Esta seção irá demonstrar como criar comunidades de VPN – *Virtual Private Network* no Blockbit GSM. Essas configurações permitem que ocorra uma comunicação segura, rápida e criptografada entre os devices.

O Blockbit GSM permite configurar dois modos de topologia para criar comunidades: *Full Meshed* e *Star*:

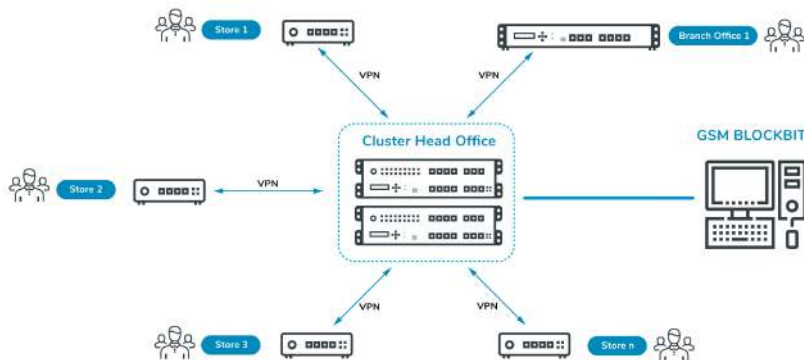
- **Full Meshed:** Todas as *devices* estabelecem comunicação umas com as outras. A seguir, segue o exemplo de Topologia *Full Meshed*:

Device Communities Topology Full Meshed

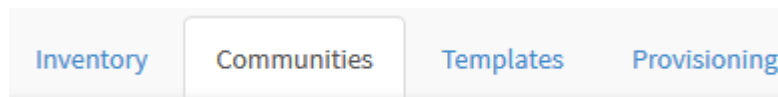


- **Star:** Todas as *devices* estabelecem comunicação com um *HUB* (normalmente é a Matriz da empresa), e esta permite a comunicação entre as *devices*, porém, de forma controlada. A seguir, segue o exemplo de Topologia *Star*.

Device Communities Topology Star



Para acessar a tela *Communities*, clique na aba como demonstrado abaixo.



Aba "Communities"

Surgirá a Tela de *Communities*. Ela é composta por cinco colunas: "Name", "Description", "Topology", "Devices" e "Actions". Além disso, no topo da tela estão localizados a [barra de busca](#) e no canto superior direito da tela está o [menu de ações](#).

Devices

Inventory Communities Templates Provisioning

2 records

☐	Name	Description	Topology	Devices	Actions
☐	VPN - Topology Full Meshed	Topology Full Meshed	full_meshed	2	
☐	VPN - Topology Star	Topology Star	star	3	

< 1 > 10 / page

Devices - Communities

Esta seção irá demonstrar como:

- [Criar](#) e [deletar](#) comunidades de VPN;
- [Adicionar](#) e [remover](#) devices às comunidades de VPN;
- Etc.

A seguir explicaremos cada componente deste painel.

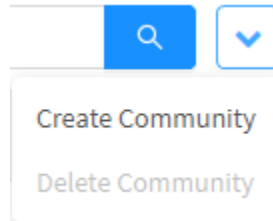
Communities - Menu de ações

No topo direito da tela temos o menu de ações:



Communities – Botão do Menu de ações

Ao clicar neste botão o menu abaixo é exibido:



Communities – Menu de ações

O menu é composto das seguintes opções:

- [Create Community](#);
- [Delete Community](#).

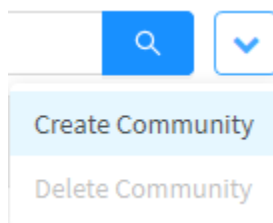
A seguir cada opção do menu de ações será detalhada.

Communities - Menu de ações - Create Community

Para criar *Community*, siga os seguintes passos:

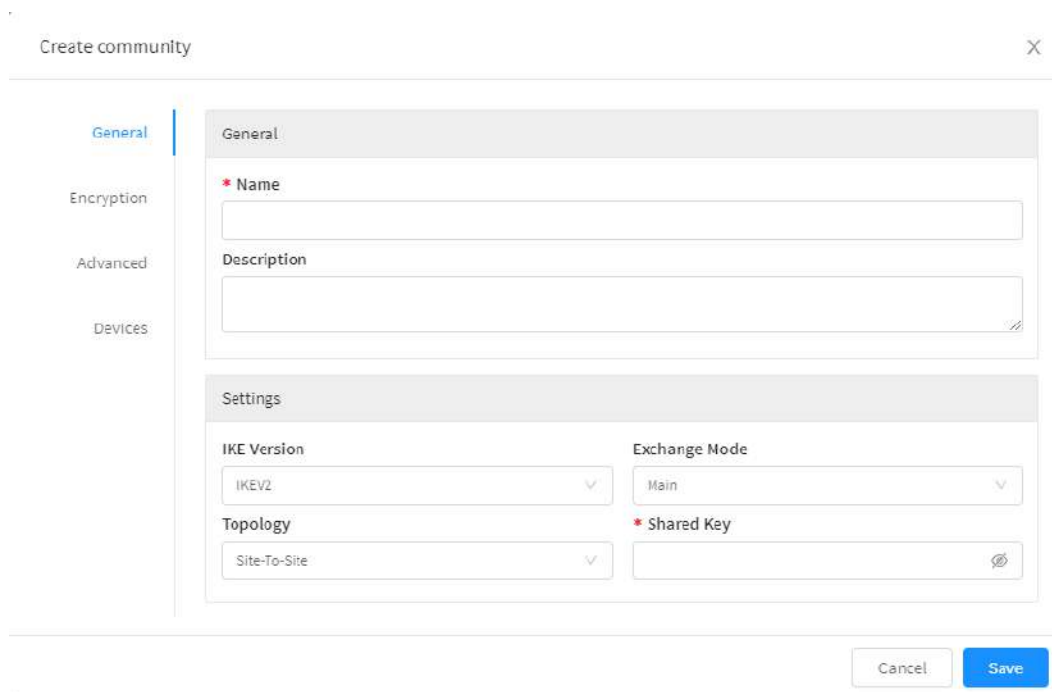


1. Clique no **menu de ações** [];
2. Clique na opção "*Create Community*";



Communities – Menu de ações – Create Community.

3. O painel "*Create Community*" será exibido. Com a aba lateral "*General*" pré-selecionada.



Communities – Create Community - General.

O painel "Create community" é composto pelas abas:

- [General](#);
- [Encryption](#);
- [Advanced](#);
- [Devices](#).

A seguir analisaremos o painel "[Create community](#)" em detalhes.

Communities - Menu de ações - Create Community - General

Na seção "General" há os seguintes campos:

- **Name:** Nome da *Device Community*. Ex.: VPN – Topology Full Meshed;
- **Description:** Descrição da *Device Community*. Ex.: FULL MESHED.

Em Settings são exibidos os campos abaixo:

- **IKE Version:** Determina a versão do *IKE* que será utilizada;
- **Exchange Mode:** Método de negociação da chave *IKE*;
- **Topology:** Define qual a topologia escolhida no campo *Topology*. Ex.: Site-To-Site;
- **Shared Key:** É uma chave compartilhada entre as *devices*. Essa chave é utilizada no processo de autenticação pelo protocolo *IKE*. Ex.: "q1Q!". Para visualizar a chave digitada, clique no ícone **visualizar** [👁].

The screenshot shows a 'Create community' dialog box with a close button (X) in the top right corner. On the left is a sidebar with four tabs: 'General' (selected), 'Encryption', 'Advanced', and 'Devices'. The main area is divided into two sections: 'General' and 'Settings'. The 'General' section contains a red asterisk next to the 'Name' label, a text input field, a 'Description' label, and a larger text input field with a small icon at the bottom right. The 'Settings' section contains four fields: 'IKE Version' (dropdown menu showing 'IKEV2'), 'Exchange Mode' (dropdown menu showing 'Main'), 'Topology' (dropdown menu showing 'Site-To-Site'), and 'Shared Key' (text input field with a red asterisk and a 'visualizar' icon). At the bottom right of the dialog are 'Cancel' and 'Save' buttons.

Communities – Create Community - General.

Communities - Menu de ações - Create Community - Encryption

A aba lateral "Encryption" é dividida em dois painéis: "Phase 1 (IKE)" e "Phase 2 (ESP)".

Em "Phase 1 (IKE)" os seguintes campos são exibidos:

- **Encryption Algorithms:** Determina qual algoritmo de encriptação será utilizado pela comunidade de VPN;
- **Authentication Algorithms:** Determina o algoritmo de autenticação que será utilizado pela comunidade de VPN;
- **Diffie-Hellman (DH) Group:** Determina o nível de complexidade na troca de chaves, quanto maior o valor do Grupo Diffie-Hellman, maior o nível de segurança porém mais tempo para o processamento da chave será necessário.

Em "Phase 2 (IKE)" os seguintes campos são exibidos:

- **ESP Encryption Algorithms:** Determina qual algoritmo de encriptação do protocolo ESP será utilizado pela comunidade de VPN;
- **ESP Authentication Algorithms:** Determina o algoritmo de autenticação do protocolo ESP que será utilizado pela comunidade de VPN;
- **Perfect Forward Secrecy (PFS) Group:** Determina o nível de complexidade na troca de chaves, quanto maior o valor do Grupo Perfect Forward Secrecy, maior o nível de segurança porém mais tempo para o processamento da chave será necessário.

The screenshot shows a 'Create community' dialog box with a sidebar on the left containing 'General', 'Encryption', 'Advanced', and 'Devices'. The 'Encryption' tab is active. The main area is split into two panels: 'Phase 1 (IKE)' and 'Phase 2 (ESP)'. Under 'Phase 1 (IKE)', there are three dropdown menus: 'Encryption Algorithms' (selected: aes256), 'Authentication Algorithms' (selected: sha256), and 'Diffie-Hellman (DH) Group' (selected: DH Group 2: 1024-bit group). Under 'Phase 2 (ESP)', there are three dropdown menus: 'ESP Encryption Algorithms' (selected: aes256), 'ESP Authentication Algorithms' (selected: sha256), and 'Perfect Forward Secrecy (PFS) Group' (selected: PFS Group 2: 1024-bit group). At the bottom right, there are 'Cancel' and 'Save' buttons.

Communities – Create Community - Encryption.

Communities - Menu de ações - Create Community - Advanced

Segue os campos exibidos na aba "Advanced":

- **IKE lifetime (s):** Determina o tempo de vida que o protocolo irá aguardar para renegociar a SA, é determinado em segundos;
- **Key lifetime (s):** Determina o tempo de validade da chave de negociação bem-sucedida, é determinado em segundos;
- **Keying Tries:** Este é o número de vezes que os pontos VPN vão renegociar o túnel ou tentar reautenticar depois que a chave expirar;
- **Rekey margin (s):** Determina quanto tempo antes da conexão expirar os pontos VPN e inicializar a renegociação das chaves do túnel;
- **DPD Action:** Controla o uso do protocolo de detecção dos pontos de VPN perdidos. Segue o funcionamento de cada opção:
 - A ação "Clear" fecha, ou encerra a conexão sem tomadas de medidas prévias;
 - A ação "Hold" configura uma política estratégica que captura o tráfego e tenta renegociar a conexão sob demanda;
 - A ação "Restart" inicia imediatamente uma tentativa de renegociação da conexão;
 - O padrão é "None" ou nenhuma, desativa o envio automático das mensagens DPD.
- **DPD delay (s):** Define o intervalo de tempo ou período, que as mensagens de troca IKE v1 e IKE v2 informativas são enviadas para os pontos VPN. É determinado em segundos;
- **DPD timeout (s):** Define o intervalo de tempo limite para o envio das mensagens, para o IKE v1 após todas as conexões para um ponto VPN serem perdidas em caso de inatividade. É determinado em segundos;
- **Re-Auth []:** Esta caixa de checagem permite habilitar o processo de reautenticação. Este recurso tem como função renegociar as chaves IKE e verificar a validade das credenciais, caso esta caixa de seleção esteja desabilitada, a conexão continuará ativa mesmo caso o certificado tenha expirado. ;
- **Fragmentation []:** Ao habilitar esta caixa de checagem, mensagens IKEv2 muito extensas são fragmentadas em um conjunto de mensagens menores, que por sua vez são encriptadas individualmente;
- **Compression []:** Esta caixa de checagem habilita o uso do protocolo IPComp para a compressão do conteúdo dos pacotes de IP em conjunto com a criptografia IPsec;
- **NAT-T []:** Habilite o item NAT-T (NAT Transversal) caso um dos sites VPN estiver atrás de um servidor de tradução de endereços (NAT) "Firewall".

The screenshot shows a 'Create community' dialog box with a sidebar on the left containing 'General', 'Encryption', 'Advanced' (selected), and 'Devices'. The 'Advanced' tab is active, displaying a 'Settings' section with the following fields:

* IKE lifetime (s)	* Key lifetime (s)	* Keying Tries	* Rekey margin (s)
28800	3600	5	5

* DPD Action	* DPD delay (s)	* DPD timeout (s)
Restart	101	30

Below these tables are four checkboxes, all of which are unchecked:

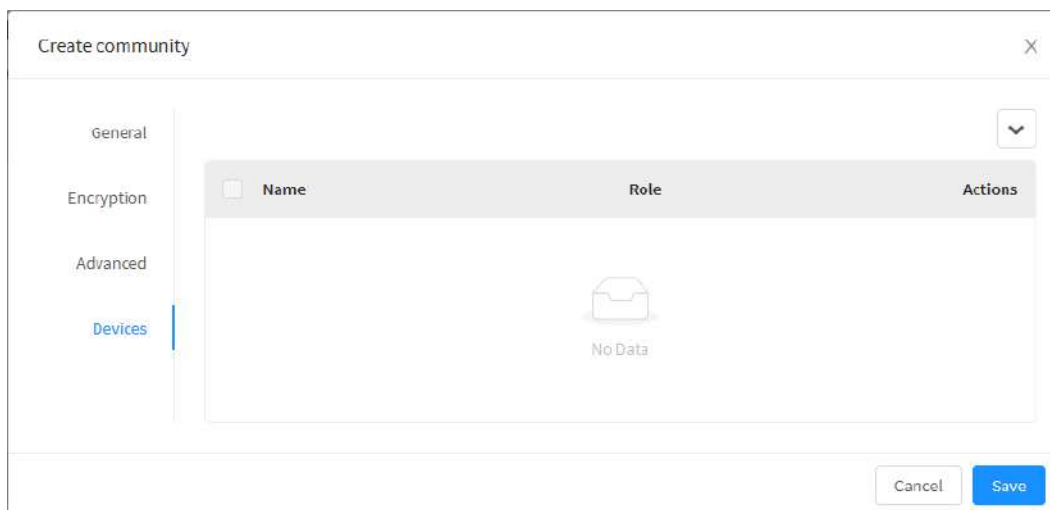
- ☐ Re-Auth
- ☐ Fragmentation
- ☐ Compression
- ☐ NAT-T

At the bottom right of the dialog are 'Cancel' and 'Save' buttons.

Communities – Create Community - Advanced.

Communities - Menu de ações - Create Community - Devices

Na aba "Devices" os seguintes campos são exibidos:



Name	Role	Actions
No Data		

Communities – Create Community - Devices.

- **Name:** Onde é exibido o nome do *device*;
- **Role:** Onde o papel do *device* utilizado pela VPN é exibido, pode ser *Hub* ou *Spoke*;
- **Actions:** Nesta coluna estão presentes dois botões de ação:
 - **Edit** [pencil icon]: Este botão permite editar as configurações dos *devices* adicionados na opção [Add device](#) do menu de ações;
 - **Delete** [trash icon]: Este botão remove o *device*.



ATENÇÃO: Ao adicionar os *devices*, caso um deles for configurado como *hub*, será criado automaticamente uma topologia [site-to-site Star](#). Porém, caso todos os *devices* forem configurados como *spoke* será criado automaticamente uma topologia [site-to-site full-meshed](#).

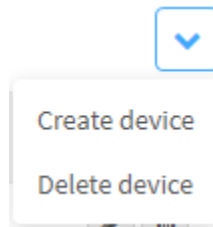
Communities - Menu de ações - Create Community - Devices - Menu de Ações

No topo direito da tela temos o menu de ações:



Devices – Botão do Menu de ações

Ao clicar neste botão o menu abaixo é exibido:



Devices – Menu de ações

O menu é composto das seguintes opções:

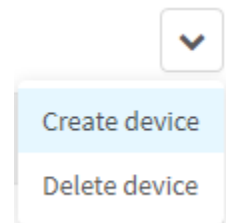
- [Create device](#);
- [Remove devices](#).

A seguir, cada opção do menu de ações será detalhada.

Communities - Menu de ações - Create Community - Devices - Menu de Ações - Create device

Para adicionar um novo *device*. Siga os seguintes passos:

1. Clique no botão de **Menu de ação** []:



Devices - Create Device

2. Clique na opção **Create Device**, a janela a seguir será exibida:

Create Device

X

* Device

▼

* Local Host

* Local ID

Network

+

^

▼

-

Role

Hub

▼

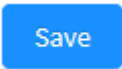
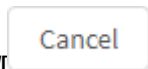
☐ Dynamic

Cancel

Save

Device - Create Device

- **Device:** Selecione o *device* desejado na lista. Ex.: Store 1;
- **Local Host:** Endereço de comunicação do ponto *VPN LOCAL* para estabelecer o túnel. Deve ser identificado por: "Endereço IP" ou "*Hostname (FQDN)*". Ex.: 172.31.102.222;
- **Local ID:** Endereço *IP* da *device* selecionada utilizada para o estabelecimento da *VPN*. Ex.: 172.31.102.222;
- **Networks:** Esse campo de texto permite a adição de redes na lista. Clique em  para adicionar o item selecionado, Caso tenha inserido o item errado, selecione o item e clique em  para retirá-lo da lista. Nesta lista ficam localizadas as redes locais da *device* selecionada que ficará acessível as outras *devices* após o estabelecimento da *VPN*. Ex.: 172.31.102.0/24;
- **Role:** É o papel do *device* utilizado pela *VPN*, ele pode ser *Hub* ou *Spoke*. Ex.: *Hub*;
- **Dynamic** ☐: Ao ativar caixa de checagem os *IPs* das interfaces *eth* dos UTMs membros dessa *community* serão dinâmicos.

Clique em **Save**  para registrar o *device* ou clique em **cancel**  para fechar esse painel.

✔ Device added successfully

Device added successfully

Após estes passos os *devices* terão sido adicionados com sucesso.

Para adicionar os demais *devices*, repita os passos acima. Após adicionar todos os *devices* teremos a seguinte tela:

General

Encryption

Advanced

Devices

Name

Role

Actions

Store 1

hub

Store 2

spoke

Store 3

spoke

Device - Devices adicionados

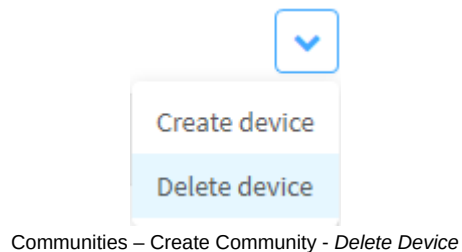
Communities - Menu de ações - Create Community - Devices - Menu de Ações - Delete device

Para deletar *devices*. Siga os seguintes passos:

1. Selecione o *device* que se deseja deletar clicando na **seleção** 

2. Clique no ícone de **Menu de ações** 

3. Clique na opção "*Delete Devices*";



Caso se deseja remover um device basta clicar na caixa de seleção e marcar todos os devices desejados e no menu de ação clicar em "*Delete device*".

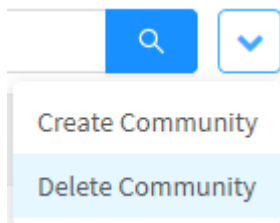
Communities - Menu de ações - Delete Community

Para deletar *communities*. Siga os seguintes passos:

1. Selecione a comunidade que se deseja deletar clicando na **seleção** [];

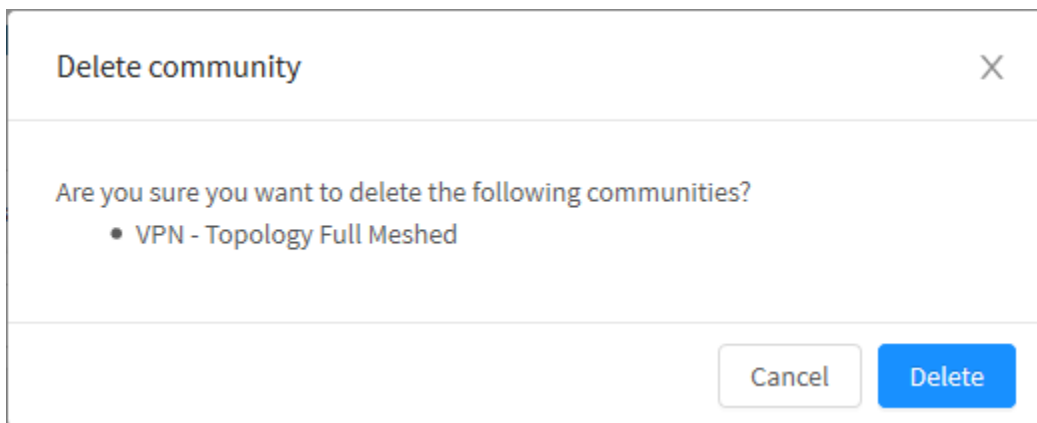
2. Clique no ícone de **Menu de ações** [];

3. Clique na opção "Delete Community";

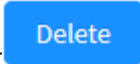
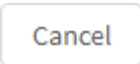


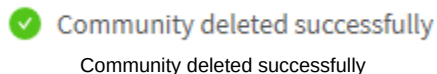
Communities – Menu de ações – Delete Community.

4. Surgirá uma mensagem de confirmação verificando se deseja deletar a comunidade selecionada:



Communities - Delete community.

Clique no botão **Delete** [] ou clique em **Cancel** [] para voltar ao painel anterior.



A comunidade foi removido com sucesso.

Communities - Colunas

A seguir explicaremos cada coluna da aba *Communities*:

Devices

Inventory Communities Templates Provisioning

2 records

☐	Name	Description	Topology	Devices	Actions
☐	VPN - Topology Full Meshed	Topology Full Meshed	full_meshed	2	 
☐	VPN - Topology Star	Topology Star	star	3	 

< 1 > 10 / page

Communities

- **Select** [☐]: Permite selecionar uma *community*.
- **Name**: Apresenta o nome da *Community* cadastrada;
- **Description**: Apresenta a descrição da *Community* cadastrada;
- **Topology**: Apresenta o tipo de topologia cadastrada;
- **Devices**: Exibe a quantidade de *devices* dentro da *Community*;
- **Actions**: Disponibiliza as seguintes ações essenciais:
 - **Botão Edit** []: Permite editar as configurações da *community* adicionada na opção [Create Community](#) do menu de ações;
 - **Botão Delete** []: Permite remover uma *community*.

Communities - Exemplos de Communities

A seguir, vamos exemplificar o cadastro de alguns *device communities* de modo a demonstrar na prática como o GSM cria topologias de VPN automaticamente nos devices:

Efetuaemos a demonstração usando as seguintes topologias:

- [Topology Star](#);
- [Topology Full-Mesh](#).

Iniciaremos os exemplos pela topologia *star*:

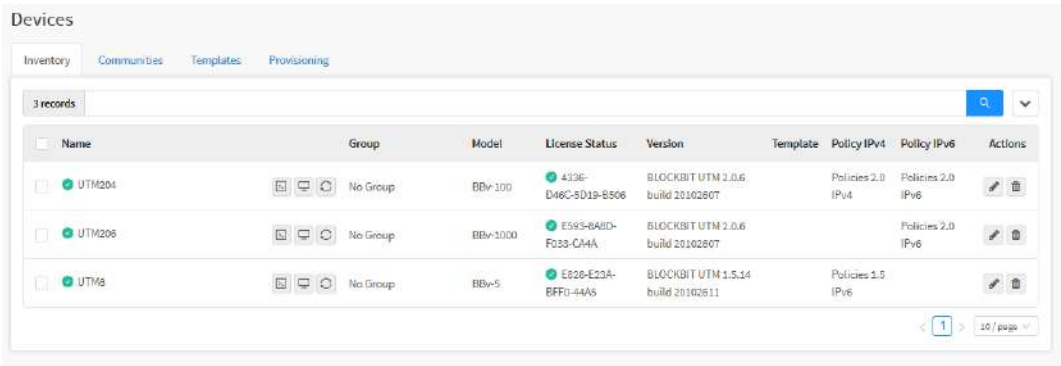
Topology Star

Esta demonstração levará em consideração a seguinte estrutura:

Topology Star - Endereçamento IP

Device	IP	Papel
UTM204	204.204.204.0	Hub
UTM206	206.206.206.0	Spoke
UTM8	108.108.108.0	Spoke

Antes de criar as *communities*, em *Inventory* [adicione os Devices](#) conforme a sua estrutura, neste exemplo usaremos:



Exemplo - Aba Devices

De volta na aba *communities*, [crie uma community](#) nova e configure-a, conforme demonstrado à seguir:

Edit community

X

General

Encryption

Advanced

Devices

General

* Name

Device Community

Description

Device Community

Settings

IKE Version

IKEV2

Exchange Mode

Main

Topology

Site-To-Site

* Shared Key

...

Cancel

Save

Exemplo - Create Community

- **Name:** Device Community;
- **Description:** Device Community;
- **IKE Version:** IKEV2;
- **Exchange Mode:** Main;
- **Topology:** Site-to-site;
- **Shared Key:** q1Q!q1Q!.

As configurações nas abas laterais *Encryption* e *Advanced* permanecerão iguais. Selecione a aba *Devices* e crie os *Hubs* e *Spokes* conforme demonstrado:

UTM204

Configure o *device* UTM204 como um *Hub*, conforme demonstrado a seguir:

Edit Device

X

* Device

UTM204

* Local Host

204.204.204.0

* Local ID

204.204.204.0

Network

+

192.168.204.0/24

^

↓

-

Role

Hub

↓

☐ Dynamic

Cancel

Save

Exemplo - Create Community - Create Device

- **Device:** UTM204;
- **Local Host:** 204.204.204.0;
- **Local ID:** 204.204.204.0;
- **Network:** 192.168.204.0/24;
- **Role:** Hub.

UTM206

Configure o device UTM206 como um *Spoke*, conforme demonstrado a seguir:

Edit Device

X

* Device

UTM206

* Local Host

206.206.206.0

* Local ID

206.206.206.0

Network

+

192.168.206.0/24

^

↓

-

Role

Spoke

↓

☐ Dynamic

Cancel

Save

Exemplo - Create Community - Create Device

- **Device:** UTM206;
- **Local Host:** 206.206.206.0;
- **Local ID:** 206.206.206.0;
- **Network:** 192.168.206.0/24;
- **Role:** Spoke.

UTM8

Configure o device UTM8 como um *Spoke*, conforme demonstrado a seguir:

Edit Device

X

* Device

UTM8

* Local Host

108.108.108.0

* Local ID

108.108.108.0

Network

192.168.108.0/24

+

-

Role

Spoke

☐ Dynamic

Cancel

Save

Exemplo - Create Community - Devices - Create Device

- **Device:** UTM8;
- **Local Host:** 108.108.108.0;
- **Local ID:** 108.108.108.0;
- **Network:** 192.168.108.0/24;
- **Role:** Spoke.

Após estes passos, chegaremos neste resultado:

Edit community

X

General

Encryption

Advanced

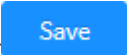
Devices

Name	Role	Actions
UTM204	hub	
UTM206	spoke	
UTM8	spoke	

Cancel

Save

Exemplo - Create Community - Devices

Por fim, clique em , *instale o pacote* e faça o *deploy*. Depois, acesse o *IP* de um dos *Spokes* ou em *Inventory* clique no ícone .

Devices

Inventory

Communities

Templates

Provisioning

4 records

UTM24

UTM204

UTM206

UTM8

No Group

No Group

No Group

No Group

BBv-100

BBv-1000

BBv-5

8F97-48F9-C2D3-7422

4136-D46C-5D19-B508

E593-8A8D-F033-CA4A

E828-E25A-BFFD-44A5

BLOCKBIT UTM 1.5.14 build 20102611

BLOCKBIT UTM 2.0.6 build 20102707

BLOCKBIT UTM 2.0.6 build 20102707

BLOCKBIT UTM 1.5.14 build 20102611

Template 1.5

Template 2.0

Políticas 2.0

Políticas 1.5

Políticas 1.5 IPv4

Políticas 2.0 IPv4

Políticas 2.0 IPv6

Políticas 1.5 IPv4

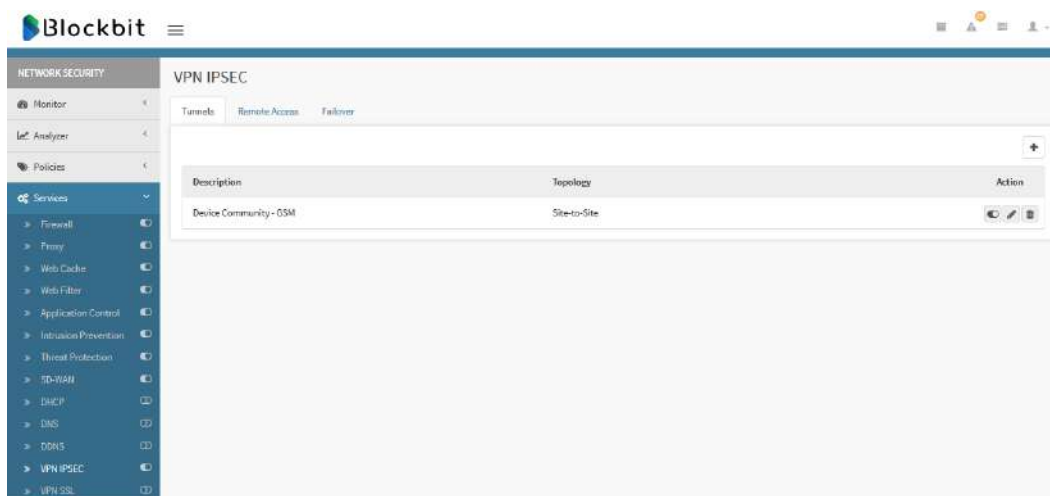
1

10 / page

Exemplo - Inventory - Connect

Já no UTM, acesse o menu *Services*, clique na opção *VPN IPSEC*.

145



Exemplo - UTM - Services - VPN IPSEC - Tunnels - Spokes

Na aba túneis poderemos observar que por termos configurado um *Hub* no *Devices Communities*, automaticamente foi criado apenas um túnel que efetua a comunicação com o centralizador, *gerando* uma topologia *Star*. Caso tivéssemos conectado no Hub, seriam exibidos dois túneis, efetuando a comunicação com os *Spokes*, como demonstrado abaixo:



Exemplo - UTM - Services - VPN IPSEC - Tunnels - Hub

Isso conclui a configuração de uma topologia *Star*. A seguir iremos exemplificar a topologia *Full-Mesh*.

Topology Full-Mesh

Esta demonstração levará em consideração a seguinte estrutura:

Topology Star - Endereçamento IP

Device	IP	Papel
UTM204	204.204.204.0	Spoke
UTM206	206.206.206.0	Spoke
UTM8	108.108.108.0	Spoke

Antes de criar as *communities*, em *Inventory* [adicione os Devices](#) conforme a sua estrutura, neste exemplo usaremos:

Devices

Inventory Communities Templates Provisioning

3 records

Name	Group	Model	License Status	Version	Template	Policy IPv4	Policy IPv6	Actions
UTM204	No Group	BBv-100	4336-D46C-5D19-B506	BLOCKBIT UTM 2.0.6 build 20102807		Policies 2.0 IPv4	Policies 2.0 IPv6	
UTM208	No Group	BBv-1000	E595-6A8D-F033-CA4A	BLOCKBIT UTM 2.0.6 build 20102807		Policies 2.0 IPv4	Policies 2.0 IPv6	
UTM8	No Group	BBv-5	E828-E23A-BFF0-4A4A	BLOCKBIT UTM 1.5.14 build 20102811		Policies 1.5 IPv4		

1 10 / page

Exemplo - Aba Devices

De volta na aba communities, [crie uma community](#) nova e configure-a, conforme demonstrado à seguir:

Edit community

General Encryption Advanced Devices

General

*** Name**
Device Community

Description
Device Community

Settings

IKE Version
IKEV2

Exchange Mode
Main

Topology
Site-To-Site

*** Shared Key**
...

Cancel Save

Exemplo - Create Community

- **Name:** Device Community;
- **Description:** Device Community;
- **IKE Version:** IKEV2;
- **Exchange Mode:** Main;
- **Topology:** Site-to-site;
- **Shared Key:** q1Q!q1Q!.

As configurações nas abas laterais *Encryption* e *Advanced* permanecerão iguais. Selecione a aba [Devices](#) e crie os *Spokes* conforme demonstrado:

UTM204

Configure o device UTM204 como um *Spoke*, conforme demonstrado a seguir:

Edit Device

X

* Device

UTM204

* Local Host

204.204.204.0

* Local ID

204.204.204.0

Network

+

192.168.204.0/24

^

v

-

Role

Spoke

v

☐ Dynamic

Cancel

Save

Exemplo - Create Community - Create Device

- **Device:** UTM204;
- **Local Host:** 204.204.204.0;
- **Local ID:** 204.204.204.0;
- **Network:** 192.168.204.0/24;
- **Role:** Spoke.

UTM206

Configure o *device* UTM206 como um *Spoke*, conforme demonstrado a seguir:

Edit Device

X

* Device

UTM206

* Local Host

206.206.206.0

* Local ID

206.206.206.0

Network

+

192.168.206.0/24

^

↓

-

Role

Spoke

↓

☐ Dynamic

Cancel

Save

Exemplo - Create Community - Create Device

- **Device:** UTM206;
- **Local Host:** 206.206.206.0;
- **Local ID:** 206.206.206.0;
- **Network:** 192.168.206.0/24;
- **Role:** Spoke.

UTM8

Configure o device UTM8 como um *Spoke*, conforme demonstrado a seguir:

Edit Device

X

* Device

UTM8

* Local Host

108.108.108.0

* Local ID

108.108.108.0

Network

+

192.168.108.0/24

^

192.168.108.0/24

▼

-

Role

Spoke

▼

☐ Dynamic

Cancel

Save

Exemplo - Create Community - Devices - Create Device

- **Device:** UTM8;
- **Local Host:** 108.108.108.0;
- **Local ID:** 108.108.108.0;
- **Network:** 192.168.108.0/24;
- **Role:** Spoke.

Após estes passos, chegaremos neste resultado:

Edit community

X

General

Encryption

Advanced

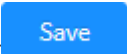
Devices

Name	Role	Actions
UTM204	spoke	
UTM206	spoke	
UTM8	spoke	

Cancel

Save

Exemplo - Create Community - Devices

Por fim, clique em , *instale o pacote* e faça o *deploy*. Depois, acesse o IP de um dos Spokes ou em *Inventory* clique no ícone .

Devices

Inventory

Communities

Templates

Provisioning

4 records

UTM204

UTM204

UTM206

UTM8

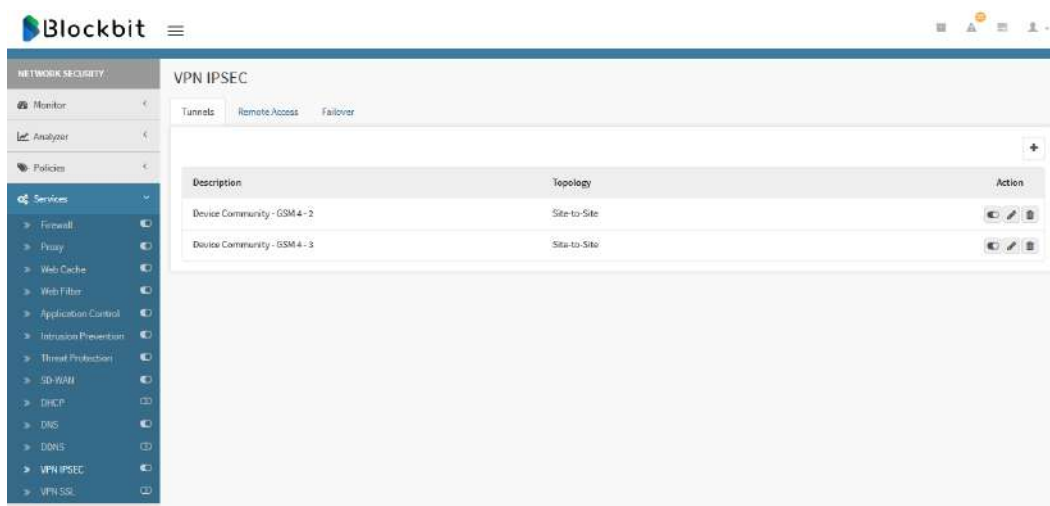
Name	Group	Model	License Status	Version	Template	Policy IPv4	Policy IPv6	Actions
UTM204	No Group	-	BF97-46F9-C2D3-7422	BLOCKBIT UTM 1.5.14 build 20102611	Template 1.5	Políticas 1.5 IPv4		
UTM204	No Group	BBv-100	4335-D46C-5D19-8506	BLOCKBIT UTM 2.0.6 build 20102707	Template 2.0	Políticas 2.0 IPv4	Políticas 2.0 IPv6	
UTM206	No Group	BBv-1000	E593-8ABD-F033-CA4A	BLOCKBIT UTM 2.0.6 build 20102707			Políticas 2.0 IPv6	
UTM8	No Group	BBv-5	E828-E23A-BFF0-44A5	BLOCKBIT UTM 1.5.14 build 20102611		Políticas 1.5 IPv4		

1

19 / page

Exemplo - Inventory - Connect

Já no UTM, acesse o menu *Services*, clique na opção *VPN IPSEC*.



Exemplo - UTM - Services - VPN IPSEC - Tunnels

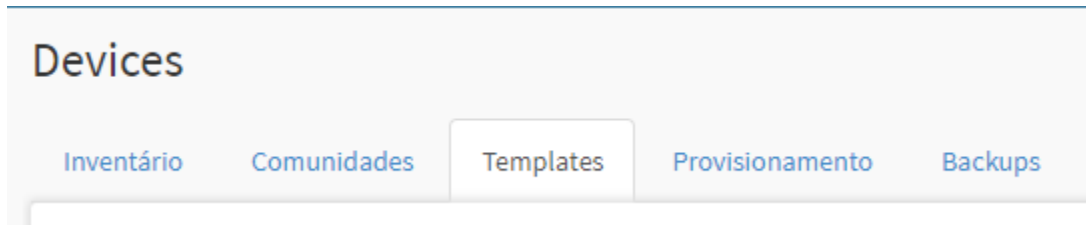
Na aba túneis podemos observar que por termos configurado vários *Spokes* e nenhum *Hub* nos *Device Communities*, automaticamente foi criado um túnel para cada *Spoke* gerando uma topologia *Full Mesh*.

Isso conclui a configuração dos exemplos, para mais informações sobre *device communities*, consulte esta [página](#).

Aba Templates

Os *Templates* são um conjunto de configurações gerais dos *devices* do Blockbit NGFW. Dentro deste conjunto, é possível inicializar os *devices* com as configurações globais de forma rápida, prática e sem erros, diminuindo o TCO, maximizando o desempenho do time de TI e evitando erros de configurações.

Para acessar a tela *Templates*, clique na aba como demonstrado abaixo:

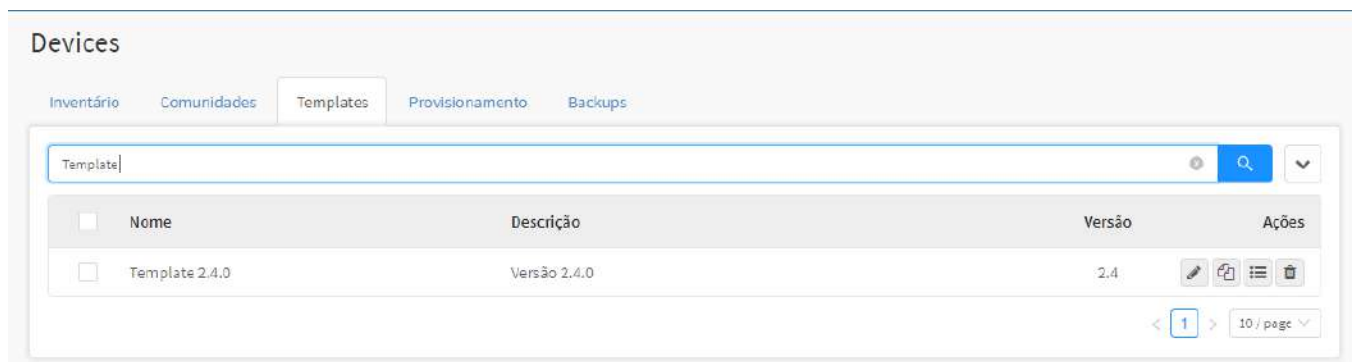


Aba "Templates"

Surgirá a Tela de *Templates*. Ela é composta por quatro colunas: "Nome", "Descrição", "Versão" e "Ações". Além disso, no topo da tela estão localizados

a barra de busca e, no canto superior direito, está o **menu de ações** []

A seguinte tela será exibida:



Devices - Templates

Esta seção irá demonstrar como:

- Criar, clonar e excluir Templates;
- Configurar os Templates criados;
- Etc.

A seguir, analisaremos as funções no topo deste quadro.

Templates - Colunas

A seguir explicaremos cada coluna da aba *Templates*:

Devices

Inventory Communities **Templates** Provisioning

4 records

☐	Name	Description	Version	Actions
☐	Device Branch Office	Template for Branch Office	1.5	  
☐	Device Head Office	Template for Head Office	1.5	  
☐	Device Store	Template for Store Device	1.5	  
☐	Device Webfilter	Template for Webfilter Devices	1.5	  

< 1 > 10 / page

Templates

- **Name:** Apresenta o nome do *Template* cadastrado;
- **Description:** Apresenta a descrição do *Template* cadastrada;
- **Version:** Apresenta a versão na qual o *Template* foi criado;
- **Actions:** O menu "Actions" é composto por vários botões:
 - **Botão Edit** : Permite editar as configurações do *Template* adicionado na opção [Create Template](#) do menu de ações;
 - **Botão Visualizar** : Permite visualizar, editar e adicionar opções mais específicas do *Template*, para mais informações, acesse o capítulo [Templates - Config Template](#);
 - **Botão Delete** : Deleta o *Template*;
 - **Caixa de Seleção** ☐: Seleciona o *Template*.

Templates - Configurar Template

Ao clicar no botão **detalhar**  é possível configurar o template;

Neste painel é possível efetuar as configurações gerais e acionar quais módulos serão utilizados nesse template.

Configurar Template X

Configuration

Firewall

Proxy

Web Cache

Web Filter

Intrusion Prevention

Threat Protection

SD-WAN

DNS

Geral

* Nome

Template 2.4.0

Descrição

Versão 2.4.0

Versão

2.4

Módulos

☐ Custom ☒ UTM ☐ IPS ☐ ATP ☐ SWG

☒ Firewall

☒ Proxy

☒ Web Cache

☒ Web Filter

☒ Intrusion Prevention

☒ Threat Protection

☒ SD-WAN

☒ DNS

Cancelar

Salvar

Configurar Templates – Configurar Template.

Geral

Em "Geral" temos as seguintes caixas de texto:

Geral

*

Nome

Template 2.4.0

Descrição

Versão 2.4.0

Versão

2.4

Configuração - Geral.

- **Name:** O nome do *template*. Ex.: *Device Head Office*;
- **Description:** A descrição do *template*. Ex.: *Template for Head Office*;
- **Version:** A versão utilizada pelo *template*. Pode ser 2.3 ou 2.4. Esta opção é determinada apenas quando o *template* é criado. Para maiores informações, cheque [Templates - Menu de ações - Create Template](#).

Módulos

Em "Módulos" temos as seguintes opções:

Módulos

☐

Custom

☒

UTM

☐

IPS

☐

ATP

☐

SWG

☒

Firewall

☒

Intrusion Prevention

☒

Proxy

☒

Threat Protection

☒

Web Cache

☒

SD-WAN

☒

Web Filter

☒

DNS

Configuração - Módulos.

Os módulos dispostos nas caixas de seleção serão habilitados ou desabilitados de acordo a seleção destas opções:

- **Custom**☐: Caso esta opção seja selecionada, o usuário tem a opção de customizar quais módulos serão habilitados;
- **UTM**☒: Caso esta opção seja selecionada, todos os módulos comumente utilizados pelo *NGFW* serão habilitados;
- **IPS**☐: Caso esta opção seja selecionada, todos os módulos comumente utilizados pelo *IPS* serão habilitados: Os módulos "*Firewall*" e "*Intrusion Prevention*" serão habilitados;
- **ATP**☐: Caso esta opção seja selecionada, todos os módulos comumente utilizados pelo *ATP* serão habilitados: Os módulos "*Firewall*", "*Proxy*", "*Intrusion Prevention*" e "*Threat Protection*" serão habilitados;

- **SWG** ☐: Caso esta opção seja selecionada, todos os módulos comumente utilizados pelo SWG serão habilitados: Os módulos "Firewall", "Proxy", "Web Cache", "Web Filter" e "Threat Protection" serão habilitados.

Ao marcar as caixas de checagem é possível habilitar e desabilitar a configuração dos módulos do NGFW. Os módulos disponíveis são:

- **Firewall** ☐: Neste módulo é possível administrar os serviços, configurações de segurança e *Zone Protection*. Para maiores informações a respeito destas funcionalidades cheque [Firewall](#);
- **Proxy** ☐: Este módulo possibilita administrar as configurações de Certificados, *HTTP*, *FTP*, *SMTP* e *POP3*. Para maiores informações a respeito destas funcionalidades cheque [Proxy](#);
- **Web Cache** ☐: Neste módulo é possível editar as configurações de *Cache*. Para mais informações dessas funcionalidades cheque [Web Cache](#);
- **Web Filter** ☐: Este módulo possibilita customizar a página de bloqueio, os domínios do *Google* e as configurações de *Safe Search*. Para maiores informações a respeito destas funcionalidades cheque [Web Filter](#);
- **Threat Protection** ☐: Neste módulo é possível administrar as configurações gerais de *Threat Protection*. Na versão 1.5 este campo é nomeado "Antimalware". Para maiores informações a respeito destas funcionalidades cheque [Threat Protection](#);
- **Intrusion Prevention** ☐: Este módulo possibilita administrar os *profiles*, *Whitelist* e *Blacklist* do *Intrusion Prevention*. Na versão 1.5 este campo é nomeado "DPI". Para maiores informações a respeito destas funcionalidades cheque [Intrusion Prevention](#);
- **SD-WAN** ☐: Neste módulo é possível administrar os perfis e serviços do SD-WAN. Para maiores informações a respeito destas funcionalidades cheque [SD-WAN](#);
- **DHCP** ☐: Este módulo possibilita gerenciar os *servidores*, *Ranges* e *Relay* do *DHCP*. Para maiores informações a respeito destas funcionalidades cheque [DHCP](#);
- **DNS** ☐: Neste módulo é possível editar as configurações e redirecionamento do *DNS*. Para maiores informações a respeito destas funcionalidades cheque [DNS](#);
- **DDNS** ☐: Este módulo possibilita gerenciar os *host* dinâmicos. Para maiores informações a respeito destas funcionalidades cheque [DDNS \(DynDns\)](#).



Atente que: Quando realizado o *deploy* de *Firewall (Zone Protection)*, com autenticação por usuários/grupos:

Só serão listados os usuários/grupos, caso o NGFW já possua os mesmos, uma vez que o GSM não cria usuários;

Caso o NGFW não possua os usuários/grupos, será criada uma regra somente com a autenticação habilitada (sem considerar os usuários /grupos).



Para maiores informações sobre cada configuração, consulte o manual do *Blockbit* NGFW.

Templates - Config Template - Custom Branding

Através desta aba é possível utilizar o GSM como uma plataforma de customização dos dispositivos de *Firewall*, sendo possível alterar o título do produto, ícone, imagem de fundo, cores de menu etc. Usando estas opções é possível criar *templates* de customização do *firewall* de acordo com a identidade visual utilizada pela própria empresa do usuário. Este *template* por sua vez, pode ser aplicado em múltiplos dispositivos ao fazer o *deploy* de *de vice template* (permitindo selecionar um grupo de dispositivos que selecionem a mesma customização).

A customização de *appliances* é controlada através de licença, assim sendo, essa opção só estará disponível caso o usuário possua uma licença de customização válida ativa. Se a licença do GSM permitir a customização, a aba *custom brand* estará disponível na configuração dos *templates*. Caso a subscrição esteja vencida e o usuário tentar aplicar um *template* já configurado o sistema de *deploy* apresentará um erro de licença.

Esse recurso atua efetuando a customização dos *appliances* antes mesmo deles serem instalados na rede.



Caso deseje customizar o GSM propriamente dito, consulte essa [página](#).

Para habilitar a customização clique em **Enabled** ☒;



Ao ativar o *Custom Branding*, menções à "Blockbit" no *layout* dos UTM serão automaticamente ocultadas, efetivamente tornando os *appliances* um produto *white-label*.

Porém atente que há algumas exceções:

- Janelas e painéis onde é exibido o modelo do appliance;
- O conteúdo do termo de uso;
- Qualquer configuração ou componente que é apenas acessível através de usuário *root*;
- Configurações de *Zero Touch Provisioning*;

Config Template

Configuration

Firewall

Proxy

Web Cache

Web Filter

Intrusion Prevention

Threat Protection

SD-WAN

DNS

Custom Branding

Custom

☒ Enabled Restore Default

* Page Title

BLOCKBIT | UTM

* Favicon

* Logo

* Background

Preview

BLOCKBIT | UTM

https://172.31.240.35/devices/templates

Blockbit

NETWORK SECURITY

Monitor

Dashboard

Live Sessions

Analyzer

* Section

#000000

* Section Font

#FFFFFF

* Selected

#3C7C9F

* Selected Font

#FFFFFF

* Open

#356B89

* Open Font

#CCCCCC

* Open F Hover

#FFFFFF

* Menu

#B9B9B9

* Menu Font

#4E4E4E

* Base

#E9E9E9

Cancel Save

Config Template - Custom Brand

- **Enabled** : É necessário ativar essa caixa de checagem para habilitar a customização do template, caso ela seja desabilitada, a customização do *template* será desabilitada;
- **Page title**: Define o nome que será exibido na barra de título na janela do sistema. Ex.: UTM;
- **Section**: Esta opção customiza a cor das seções do GSM (onde aparece "*Management*", "*Analytics*" e "*Settings*"), este campo aceita o código de cor *HEX*, além disso é possível clicar no quadro ao lado e selecionar a cor desejada em um *color picker* com campo *RGBA*. Ex.: #000000;
- **Section Font**: Nesta opção é customizada a cor das fontes das seções do GSM, este campo aceita o código de cor *HEX*, além disso é possível clicar no quadro ao lado e selecionar a cor desejada em um *color picker* com campo *RGBA*. Ex.: #FFFFFF;
- **Selected**: Nesta opção é customizada a cor dos menus selecionados e da barra superior do GSM, este campo aceita o código de cor *HEX*, além disso é possível clicar no quadro ao lado e selecionar a cor desejada em um *color picker* com campo *RGBA*. Ex.: #ccb516;
- **Selected Font**: Nesta opção é customizada a cor da fonte dos menus selecionados, este campo aceita o código de cor *HEX*, além disso é possível clicar no quadro ao lado e selecionar a cor desejada em um *color picker* com campo *RGBA*. Ex.: #000000;
- **Open**: Nesta opção é customizada a cor dos menus abertos, este campo aceita o código de cor *HEX*, além disso é possível clicar no quadro ao lado e selecionar a cor desejada em um *color picker* com campo *RGBA*. Ex.: #f3dc3a;
- **Open Font**: Nesta opção é customizada a cor da fonte dos menus abertos, este campo aceita o código de cor *HEX*, além disso é possível clicar no quadro ao lado e selecionar a cor desejada em um *color picker* com campo *RGBA*. Ex.: #000000;
- **Open F Hover**: Nesta opção é customizada a cor de destaque da fonte dos menus abertos quando o mouse passa por cima delas, este campo aceita o código de cor *HEX*, além disso é possível clicar no quadro ao lado e selecionar a cor desejada em um *color picker* com campo *RGBA*. Ex.: #ffec6c;
- **Menu**: Nesta opção é customizada a cor dos menus, este campo aceita o código de cor *HEX*, além disso é possível clicar no quadro ao lado e selecionar a cor desejada em um *color picker* com campo *RGBA*. Ex.: #bd9700;
- **Menu Font**: Nesta opção é customizada a cor das fontes dos menus, este campo aceita o código de cor *HEX*, além disso é possível clicar no quadro ao lado e selecionar a cor desejada em um *color picker* com campo *RGBA*. Ex.: #000000;
- **Base**: Nesta opção é customizada a cor base do painel onde ficam os menus, este campo aceita o código de cor *HEX*, além disso é possível clicar no quadro ao lado e selecionar a cor desejada em um *color picker* com campo *RGBA*. Ex.: #000000;

- **Favicon**: Ao clicar no botão  **Click to upload**] permite efetuar o *upload* do *favicon* da página. Caso deseje visualizar a imagem adicionada, clique em , para fazer download clique em , para excluir, clique em . O formato necessita ser *PNG* ou *ICO*, as dimensões mínimas são 24x24, não há tamanho máximo, só é necessário que a imagem possua mesma altura e largura (seja quadrada);
- **Logo**: Ao clicar no botão  **Click to upload**] permite efetuar o *upload* do logo utilizado no topo dos menus. Caso deseje visualizar a imagem adicionada, clique em , para excluir, clique em . O formato necessita ser *SVG* de dimensões 300x65. Não há tamanho máximo, só é necessário que a imagem possua altura e largura diferentes (seja retangular);
- **Background**: Ao clicar no botão  **Click to upload**] permite efetuar o *upload* de uma imagem que é utilizada como background na tela inicial de login. Caso deseje visualizar a imagem adicionada, clique em , para excluir, clique em . O formato necessita ser *PNG* ou *JPG* de dimensões 1920x1080;
- **Preview**: Demonstra as alterações que foram efetuadas nas opções acima em uma pré-visualização para checagem antes de efetivamente aplicá-las.



Para auxiliar na definição das cores:

É possível criar ou consultar uma paleta de cores no site <https://coolors.co/generate> que disponibiliza informações da coloração em: *Color Name*, *HEX*, *RGB*, *HSB*, *HSL*, *CMYK*, *LAB*, *RAL*, *HKS*, *Copic* e *Prismacolor*.

Caso seja necessário converter de *Pantone* para *RGB*, *CMYK* ou *HEX*, consulte o conversor do site oficial neste link: <https://www.pantone.com/color-finder>.

Segue um exemplo de um template com a customização já aplicada:

Config Template

Configuration

Firewall

Proxy

Web Cache

Web Filter

Intrusion Prevention

Threat Protection

SD-WAN

DNS

Custom Branding

Custom

Enabled

Restore Default

Page Title

UTM

Favicon

Logo

Background

Preview

UTM

https://192.168.254.51/devices#

UTM

NETWORK SECURITY

Monitor

Dashboard

Live Sessions

Analyzer

Section

Section Font

Selected

Selected Font

Open

Open Font

Open F Hover

Menu

Menu Font

Base

Cancel

Save

Config Template - Custom Brand - Template editado

Ao aplicar o *custom branding* no UTM pode ser necessário apagar o cache do navegador para visualizar as mudanças.

Para acessar a janela de deleção de *cache* basta utilizar o comando "*ctrl+shift+del*".

A legenda "*Powered by Blockbit*" abaixo do *logo* não é customizável.

Restore Default

Caso não fique satisfeito com as alterações efetuadas clique em [Restore Default] para restaurar às configurações padrões ou desabilite a caixa de seleção **Enabled** [☒] e efetue o *deploy* do template novamente para voltar aos padrões de fábrica.

Save

Cancel

Para salvar as alterações clique em [Save], caso contrário, clique em [Cancel] para fechar a janela.

Saved successfully

Saved successfully

160

Após realizar esses procedimentos a customização do *firewall* foi efetuada com sucesso.

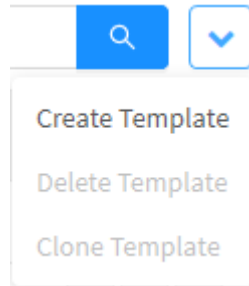
Templates - Menu de ações

No topo direito da tela temos o menu de ações:



Templates – Botão do menu de ações.

Ao clicar neste botão o menu abaixo é exibido:



Templates – Menu de ações.

O menu é composto das seguintes opções:

- [Create Template](#);
- [Delete Templates](#);
- [Clone Template](#).

A seguir cada opção do menu de ações será detalhada.

Templates - Menu de ações - Criar Template

Através do botão "Criar Template" é possível criar um novo *Template*. Para acessar, siga os passos a seguir:

1. Clique na opção "Criar Template";



Templates – Criar Template.

2. Preencha a tela "Criar Templates":

- **Nome:** Nome do *Template*. Ex.: *Devices Store*;
- **Descrição:** Descrição do *Template*. Ex.: *Basic Stores Settings*;
- **Versão:** Selecione a versão correta de acordo com o NGFW que será utilizado. É importante ter em mente que caso selecione uma versão diferente, o *template* não funcionará.

Criar Template

X

* Nome

Descrição

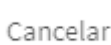
* Versão

2.4

Cancelar

Salvar

Templates – Criar Template.

3. Para salvar as alterações clique em **Salvar** [], caso contrário, clique em **Cancelar** [] para fechar a janela.



Salvo com Sucesso

Após realizar esses procedimentos o "Template" do device foi criada com sucesso.

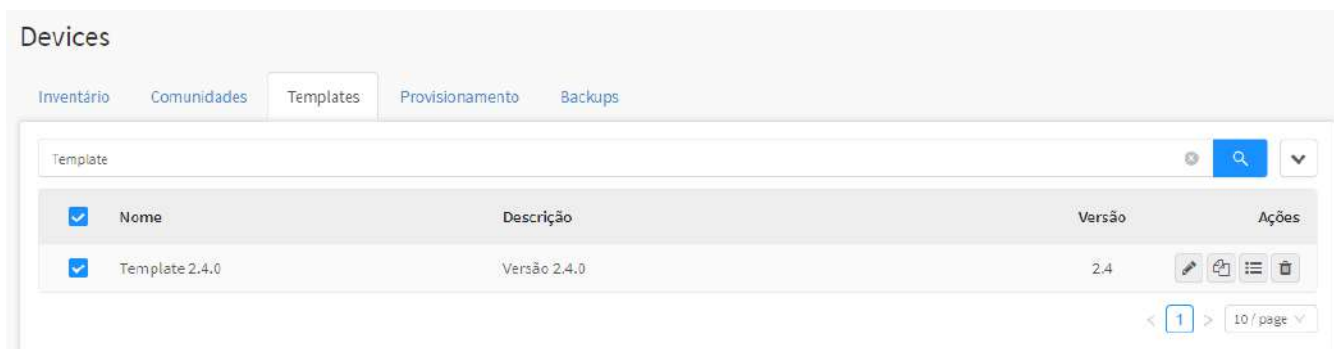
Por fim, depois de cadastrar o nome e a descrição do *Template*, será necessário clicar em **detalhar**  para exibir a tela "Config Template" e finalizar a configuração do template;

Para mais informações acesse o capítulo [Templates - Configurar Template](#);

Templates - Menu de ações - Clonar Template

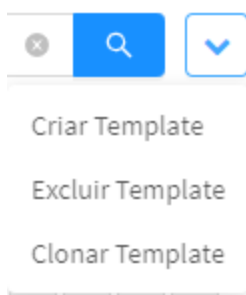
Através do botão "Clonar Template" é possível clonar um Template.

1. Selecione [] qual Template deseja clonar. Ex.: Devices Branch office;



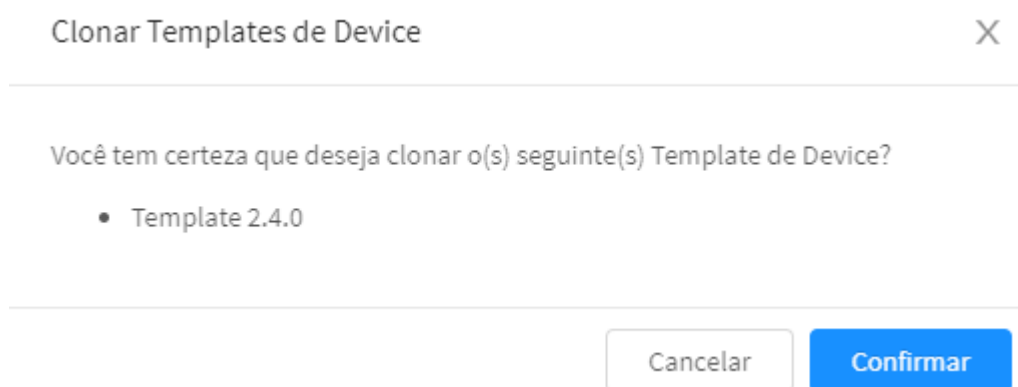
Templates – Seleção dos Templates que serão clonados

2. No Menu de ações [], clique na opção "Clonar Template";

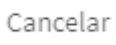


Clonar Template

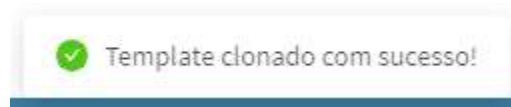
3. Surgirá a mensagem se deseja realmente clonar os itens selecionados;



Templates – Clonar Template.

Caso desejar cancelar clique no botão **Cancelar** []. Para concluir, clique no botão **Confirmar** [].

Também é possível clonar um *Template* clicando no botão Clone [].



Template clonado com sucesso

Os *templates* foram clonados com sucesso.

Templates - Menu de ações - Excluir Templates

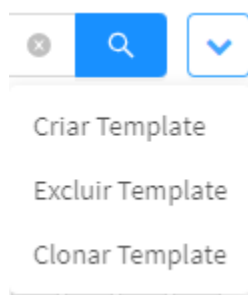
Através do botão "Excluir Templates" é possível deletar vários *Templates* ao mesmo tempo. Para deletar através do menu de ações, siga os seguintes passos:

1. Selecione [] quais *Templates* deseja deletar;



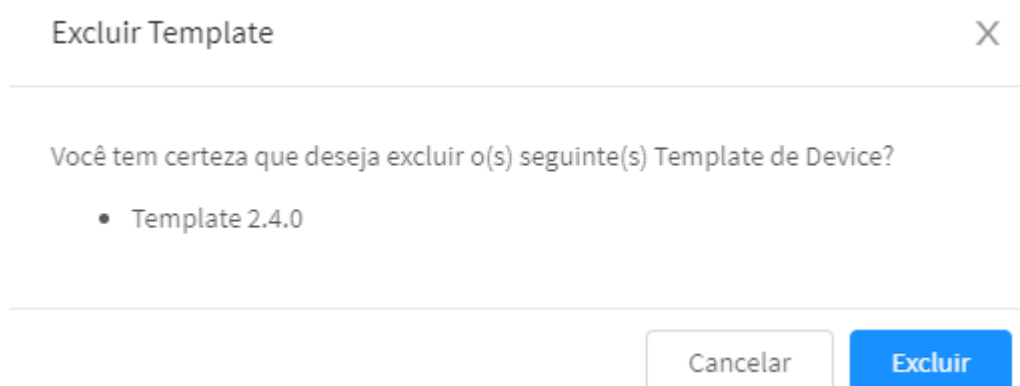
Templates – Seleção dos Templates que serão excluídos.

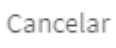
2. Entre no **Menu de ações** [] e clique na opção "Excluir Template";

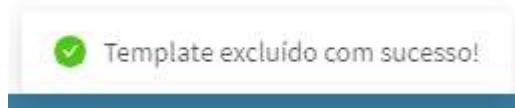


Templates – Excluir Template.

3. Surgirá a mensagem se deseja realmente deletar os itens selecionados;



Caso desejar cancelar clique no botão **Cancelar** []. Para concluir, clique no botão **Excluir** [].



Template excluído com sucesso

Após realizar esses procedimentos os *Templates* serão excluídos com sucesso.

Aba Provisioning

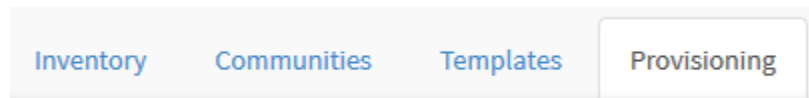
O recurso *Zero Touch Provisioning*, tem como função facilitar e agilizar a implantação de novos Blockbit UTM para serem administrados pelo GSM. Esta funcionalidade automatiza o processo de instalação e configuração de novos *appliances*, sendo apenas necessário disponibilizar uma conexão válida durante o primeiro acesso.

Depois de fazer a [adição](#) e conexão do appliance, ao ligá-lo pela primeira vez, o UTM será instalado, todas as configurações do assistente de instalação do UTM serão detectadas e efetuadas automaticamente, o certificado será validado, qualquer device template que tenha sido configurado será implementado e qualquer policy package que tenha sido pré-configurado será aplicado automaticamente.

Através do *Zero Touch Provisioning* o custo operacional, nível técnico e a possibilidade de erro humano são drasticamente reduzidos, uma vez que no ponto físico da rede não é necessário efetuar nada mais do que apenas conectar o *appliance* e ligá-lo.

É possível fazer provisionamento de um *device* em específico e também de um [lote de vários dispositivos](#).

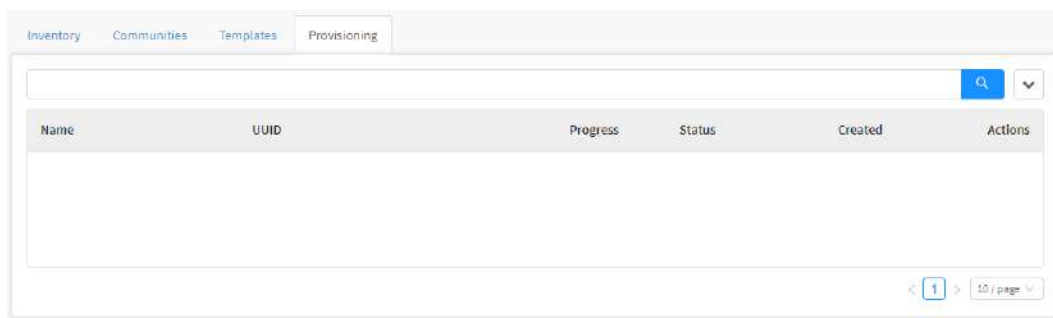
Para acessar a tela *Provisioning*, clique na aba como demonstrado abaixo.



Aba "Provisioning"

A tela *Provisioning* será exibida. Ela é composta pelas colunas: "*Name*", "*Identification*", "*Progress*", "*Status*", "*Connected*" e "*Actions*". Além disso, no topo da tela estão localizados a [barra de busca](#) e no canto superior direito da tela está o [menu de ações](#).

A tela abaixo será exibida:



Devices - Provisioning

Esta seção irá demonstrar:

- Como [Criar devices](#) para provisionamento;
- [Como efetuar provisionamento em lote](#).

A seguir, analisaremos as funções no topo deste quadro.

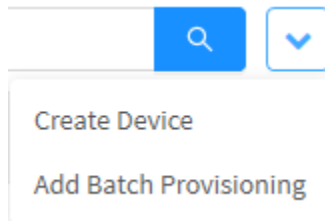
Provisioning - Menu de ações

No topo direito da tela temos o menu de ações:



Provisioning – Botão do menu de ações

Ao clicar neste botão o menu abaixo é exibido:



Provisioning – Menu de ações

O menu possui as opções :

- [Create Device](#),
- [Add Batch Provisioning](#).

A seguir detalharemos cada opção do menu.

Provisioning - Menu de ações - Create Device

Para efetuar o provisionamento *Zero Touch* o device precisa estar corretamente licenciado, a licença é sempre atrelada ao e-mail de uma empresa e a um *UUID*, este passo é fundamental pois a aprovação e confirmação do provisionamento é enviada por e-mail, além disso, pois todo provisionamento é vinculado ao *UUID* de um *appliance*.

Além disso, para que o *Zero Touch provisioning* funcione, é obrigatório possuir um *link* válido configurado de modo a atingir o portal de licenças da Blockbit de forma a validar esse licenciamento.

Antes de você configurar um provisionamento é necessário ter criado um *Device Template* ou um *Policy Package* para adicionar ao *device* durante o provisionamento.



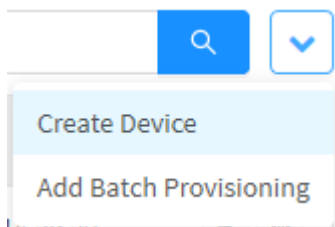
Como as políticas do GSM que estiverem no *header* tem prioridade sob as do UTM, É recomendável que ao criar um *policy package* para ser usada no provisionamento, que elas sejam criadas no *footer* por segurança para que elas não sobrescrevam permissões importantes das políticas do UTM.



Ao efetuar um *deploy* utilizando uma política que use QoS, será necessário ativar a interface WAN em *Network - Traffic Shaping*, caso contrário, a política não funcionará.

Através do botão "Create Device" é possível criar um novo dispositivo para provisionamento. Para acessar, siga os passos a seguir:

1. Clique na opção "Create Device";



Provisioning – Create Device

2. A janela "Device" é composta da aba "General", "Network" e "Certificate". Ao adicionar um device para provisionamento preencha os campos com as configurações do *device*, basicamente como se fosse instalar um UTM normalmente. Complete os campos, conforme demonstrado a seguir:

Device

General

Network

Certificate

* Name

* Company

* User Admin

Password

Device Template

Policy Package

* UUID

Description

Cancel

Save

Create Device – Device - General

- **Name:** Nome do *Device*. Ex.: Provisioned Device;
- **Company:** Define o nome da empresa. Ex.: Blockbit;
- **User Admin:** Insira o mesmo usuário administrador que foi cadastrado durante a instalação do UTM. Ex.: admin;
- **Password:** Insira a senha cadastrada durante a instalação do UTM. Esta senha precisa ter no mínimo oito caracteres, conter letras maiúsculas, minúsculas e caracteres especiais. Ex.: q1W@e3R\$;
- **Device Template:** Através deste campo, é possível adicionar os *template* criados em [Device Template](#) para este *device*;
- **Policy Package:** Através deste campo, é possível adicionar os pacotes de política criados em [Policy Package](#) para este *device*;
- **UUID:** Digitar o código de identificação única do UTM, ele pode ser localizado no *Dashboard - System* no *widget license*;
- **Description:** Descrição do *Device*. Ex.: *Provisioned Device Settings*.

3. Após preencher os campos na guia "Geral", preencha os campos na guia "Rede", conforme mostrado abaixo:

Device

General

Network

Certificate

* Hostname

* Language

* Timezone

* Gateway

* Suffix DNS

* DNS Server

* NTP Server

ETH0

1.1.1.1

255.255.255.255

DHCP Server

ETH1

1.1.1.1

255.255.255.255

DHCP Server

ETH2

1.1.1.1

255.255.255.255

DHCP Server

Cancel

Save

Create Device – Device - Network

- **Hostname:** Define o *Hostname*. Pode ser qualquer um desde que esteja conforme padrão *FQDN - Fully Qualified Domain Name*. Ex.: GSM;
- **Language:** Seleciona o idioma padrão. Ex.: *English*;
- **Timezone:** Seleciona o fuso horário. Ex.: *America/Sao_Paulo*;
- **Gateway:** Define a rota padrão da rede. Ex.: 176.16.102.1;
- **Suffix DNS:** Determina o domínio da rede. Ex.: *blockbit.com*;
- **DNS Server:** Define o servidor *DNS* da rede ou da *internet*. Ex.: 176.16.102.161;
- **NTP Server 1:** Define o servidor de sincronização de relógio. Ex.: *a.ntp.br*;
- **ETH[☒]:** Ative as interfaces de rede desejadas marcando a caixa de checagem;
 - **Endereço IP:** Informar para qual endereço de rede será aplicado as configurações;
 - **Máscara de Rede:** Informar qual será a máscara de rede;
 - **Zona de rede:** Determine qual será a Zona de Rede. Por padrão, as opções padrão são: LAN, WAN e DMZ;
 - **DHCP Server[☒]:** Ative essa caixa de checagem para distribuir os endereços *IP* na medida em que os dispositivos da rede solicitarem conexão;



Caso seja definido um *IP* na porta eth0, ao realizar o provisionamento do UTM, a mudança do IP será aplicada substituindo o DHCP, sendo assim necessário que o usuário acesse o *IP* definido na porta 98.

4. Após completar os campos da aba "Network", complete os campos da aba "Certificate", conforme demonstrado a seguir:

Device

General

Network

Certificate

* Country

Abbreviation of two letters. Ex.: US

* State

Full Ex.: New York

* City

Full Ex.: New York

* Organization

Company name

* E-mail

admin@domain

* Organizational Unit

Ex.: Department

* Expires (years)

Years

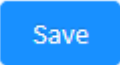
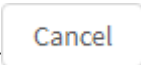
* Hostname

Cancel

Save

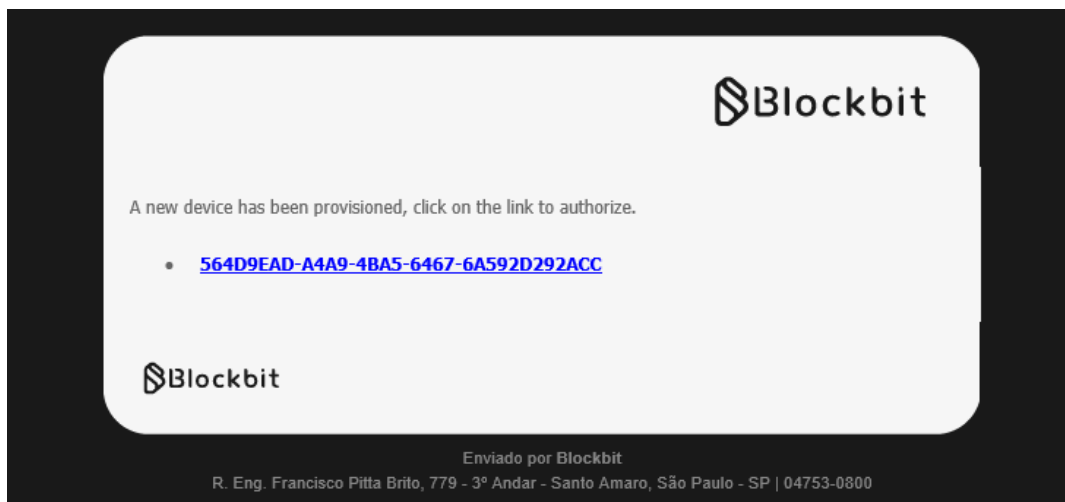
Create Device – Device - Certificate

- **Country:** Define o país. Ex.: *BR*;
- **State:** Define o estado. Ex.: *Sao Paulo*;
- **City:** Define a cidade. Ex.: *Sao Paulo*;
- **Organization:** Define o nome da empresa. Ex.: *Blockbit*;
- **E-mail:** Define o *e-mail* do administrador. Ex.: *user@blockbit*;
- **Organizational Unit:** Define o departamento. Ex.: *QA*;
- **Expires (years):** Define o tempo de validade do certificado. Ex.: *10*;
- **Hostname:** Define o *FQDN* para o certificado. Ex.: *utm.blockbit.com*.

5. Para salvar as alterações clique em **Save** , caso contrário, clique em **Cancel**  para fechar a janela.

 **Saved successfully**
Saved successfully

Ao salvar as configurações, um *e-mail* de confirmação será enviado para o endereço que estiver cadastrado no Portal de Licenças da Blockbit. Será necessário clicar no *link* que aparecerá no corpo do *e-mail* para de fato iniciar o provisionamento propriamente dito.



Provisioning - E-mail de confirmação

Um e-mail de confirmação será enviado ao autorizar o provisionamento, conforme demonstrado abaixo:



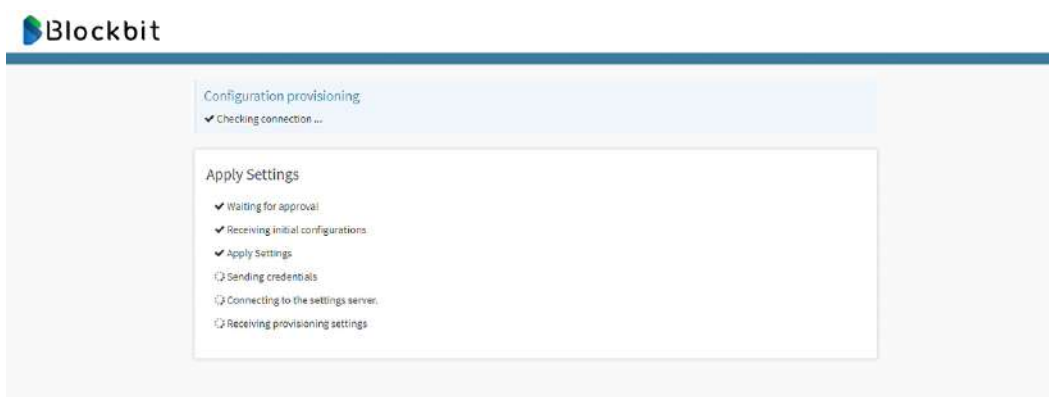
Provisioning - Confirmação do provisionamento

É possível acompanhar o progresso do provisionamento através da coluna *Status* e *Progress* na [aba de Provisioning](#) do GSM, conforme demonstrado abaixo:

Inventory Communities Templates Provisioning						
1 records						
Name	UUID	Progress	Status	Created	Actions	
Provisioned Device	564DD38E-8B9D-7B6F-7754-463B86099040	50%	Sending deploy	August 19th 2020 - 11:31:55		

Provisioning - Progresso do provisionamento

Também é possível ver o andamento do provisionamento pela própria interface do UTM que será provisionado. Conforme demonstrado na imagem a seguir:

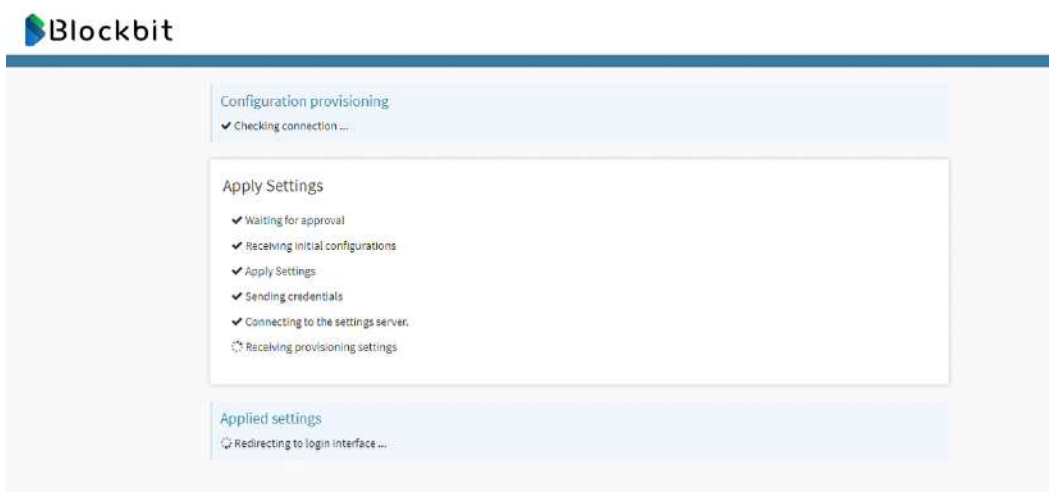


Provisioning - Provisionamento em andamento



Esta tela será exibida em português ou inglês de acordo com as configurações do navegador do usuário.

Caso o provisionamento seja concluído com sucesso, será feito um redirecionamento automático para a tela de login ocorrerá, como demonstrado abaixo:



Provisioning - Redirecionamento

Ao ser direcionado à tela de *Login*, provavelmente não será possível acessar o sistema imediatamente graças a finalização das configurações de provisionamento, aguarde até o acesso ter sido liberado. Durante esta etapa é extremamente importante não desligar o *device*. Caso as configurações ainda estejam sendo efetuadas, uma notificação será exibida bloqueando o acesso ao tentar efetuar *login*. Para ter uma visão mais precisa a respeito do progresso do provisionamento, cheque a coluna *Status* e *Progress* na [aba de Provisioning](#) do GSM.



ATENÇÃO: Ao efetuar o *Zero Touch provisioning*, NÃO desligue o *device* antes de conseguir de fato se logar no UTM. Verifique a coluna *Status* e *Progress* na [aba de Provisioning](#) do GSM para ter uma visão mais precisa do progresso do procedimento. Caso haja uma queda de energia durante qualquer momento do *provisioning*, é recomendável remover o provisionamento que foi feito no GSM, acessar o *CLI* e utilizar o comando [rewizard](#) no *appliance*, de modo que o provisionamento seja reiniciado desde o passo inicial e também para reiniciar todas as configurações de instalação que serão efetuadas no *UTM*.

Caso o provisionamento seja efetuado com sucesso, o *device* será exibido na aba [Inventory](#), da mesma forma que um *device* vinculado manualmente.

Devices

Inventory Communities Templates Provisioning

2 records

☐	Name	Group	Model	License Status	Version	Template	Policy IPv4	Policy IPv6	Actions
☐	NGFW Branch NY	No Group	BBV-10	3AFC-DB25-2434-2F93	BLOCKBIT UTM 2.0.0 build 20030507		Policy 2.0		
☐	UTM23	No Group	BBV-5	09B6-536E-E1B0-5FDE	BLOCKBIT UTM 2.0.0 build 20030216				

< 1 > 10 / page

Provisioning - Device movida para aba Inventory

Ao finalizar o *Zero Touch Provisioning* com sucesso, o UTM estará também automaticamente com a licença validada, sendo administrado pelo GSM em *Central Management*, com o deploy das *Device Templates* e *Policy Packages* definidas no GSM aplicadas.



Após terminar de configurar o *Zero Touch Provisioning*, caso necessite enviar logs para o GSM, acesse no UTM o menu *Settings*, opção *Administration*, aba *Central Management*, marque a caixa de checagem *Enable Manager* ☒ e configure o campo *Manager Address* com o IP do logger do GSM.

Caso o provisionamento não seja concluído com sucesso, surgirá um painel com dois botões:



Provisioning - Configure Provisioning

Caso o provisionamento não ocorra porque o DNS não consegue prover um caminho válido até o Portal de Licenças da Blockbit, clique no botão [

Configure Provisioning

] de modo que o painel ilustrado abaixo seja exibido, nele é possível configurar um IP válido de modo que o UTM consiga efetuar o licenciamento corretamente.

Configuration provisioning

✖ Checking connection ...

Configure Provisioning

Configure Manually

General

IP Address

Mask

255.255.255.255

Gateway

DNS

Save

© BLOCKBIT 2020

Provisioning - Add a valid IP

Configure Manually

Através da opção [] é possível efetuar a configuração manualmente, ao selecionar esta opção você será direcionado para o *Wizard* padrão. Isso também ocorrerá caso a licença tenha vencido ou expirado, o usuário será notificado e direcionado para o *Wizard* normal. Para mais informações a respeito de como configurá-lo, vide a [página](#) de configuração do Wizard do UTM.

Caso seja necessário utilizar o comando *rewizard* em uma máquina que já foi provisionada, primeiramente é necessário remover ela da aba *Inventory* do GSM.

Feito isso, será necessário criar um novo provisionamento para a máquina que passou pelo *rewizard*.

Após estes passos, o processo é o mesmo.

Para mais informações a respeito das colunas da aba *Provisioning* clique neste [link](#) para mais informações a respeito de provisionamento em lote, consulte esta [página](#).

Provisioning - Menu de ações - Add Batch Provisioning

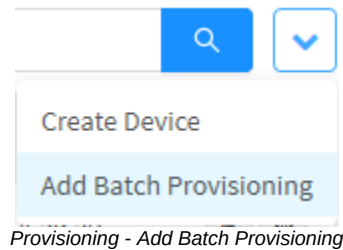
O principal benefício da função de provisionamento em lote é a agilidade com a qual o administrador consegue implementar e configurar *serviços e políticas*, utilizando *configurações* pré-definidas em *device templates* e *pacotes de política*, além de facilitar também o processo de aprovação e checagem de erros neste processo (no caso de eventuais incongruências no código por exemplo). Além de todos estes benefícios, o processo de provisionamento em lote é relativamente simples e transparente, podendo facilmente ser acompanhado pelo painel na aba *Provisioning* através da barra de progresso e dos ícones de *status*.

O provisionamento em lote funciona utilizando um arquivo CSV como modelo, este contém basicamente todos os campos da janela de *Zero Touch Provisioning* e atua da mesma forma: Reunindo todas as informações necessárias para a implementação de um novo *device*.

Após completar o CSV, o usuário simplesmente precisa determinar qual *template* e pacote de políticas será aplicado nesta lista de *devices*, após adicionar os *devices* a serem provisionados, basta aguardar o recebimento do email de provisionamento em lote e clicar no *link* de confirmação.

Caso seja detectada qualquer incongruência, a implementação do lote não é executada, o *e-mail* de confirmação só será recebido caso todo o lote esteja em conformidade no portal de licenciamento da Blockbit e caso o arquivo CSV esteja corretamente configurado.

Para efetuar o provisionamento em lote, clique no menu de ações [] e selecione a opção "Add Batch Provisioning";



A janela abaixo será exibida:

Add Batch Provisioning

* Device Template

* Policy Package

* Import file

Click to upload

Cancel

Download model

Add

Add Batch Provisioning

Download model

Antes de completar o formulário, clique em [] para baixar o modelo em CSV.



O arquivo CSV é disponibilizado conforme o idioma da interface. Por exemplo, caso ao efetuar *login*, tenha selecionado o idioma "Português", todos os campos do CSV estarão neste idioma (pt-BR).

Os dados deste modelo representam os campos do formulário em *Zero Touch Provisioning* por tanto, complete o CSV conforme as necessidades e salve-o, não há obrigatoriedade do arquivo estar com o mesmo nome de quando realizado o *download*, sendo apenas necessário configurá-lo corretamente e utilizar a extensão do arquivo (CSV).



Ao editar o CSV o campo *language*, *ntp server* e *timezone* devem utilizar a informação correta dentre as disponibilizadas pelo GSM (vide [criação de device único](#)). Por exemplo, os únicos idiomas suportados são "pt_BR" ou "en-US", caso um outro valor seja adicionado neste campo, o arquivo será considerado inválido.

Para mais informações a respeito da sintaxe de Fuso-horário no CSV acesse esta [página](#).



Caso esteja usando o *Microsoft Excel* para editar o arquivo CSV, é possível utilizar a função "Obter dados de Text/CSV" para facilitar a interpretação dos dados. Este recurso utiliza os delimitadores como colunas, facilitando a visualização do arquivo.

Click to upload

Ao terminar de completar o CSV, clique em [] para fazer *upload* do lote de *devices*.



Atente que se o CSV for muito extenso é natural que o sistema leve um tempo pra efetuar o *upload* e ler o arquivo.

Após efetuar o upload, faça as seleções no formulário conforme a necessidade:

- **Device Template:** Selecione o *Template de Device* que será aplicado em todos os *appliances* do lote, caso precise de mais informações a respeito de como criar um consulte esta [página](#);
- **Policy Package:** Selecione o Pacote de Política que será aplicado em todos os *appliances* do lote, caso precise de mais informações a respeito de como criar um consulte esta [página](#).



Como o *Custom Branding* é parte do *Device Template*, é possível já personalizar os UTMs durante esse processo.



Não é necessário selecionar um *Template de Device* e um *Policy Package*, é mandatório selecionar ao menos um deles. Caso o usuário prefira selecionar apenas um dos dois, o provisionamento procederá normalmente.

Depois de ter completado o formulário a janela deve estar semelhante ao exemplo abaixo:

Add Batch Provisioning

Device Template

Teste de Device Template 2.x v1

Policy Package

Policy Package

* Import file

Click to upload

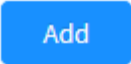
provisioning_model.csv

Cancel

Download model

Add

Add Batch Provisioning - Exemplo

Clique em  para efetuar o provisionamento em lote ou em  para fechar a janela.



Só é possível fazer provisionamento quando os clientes vinculados ao UUID são os mesmos, caso haja divergências será apresentado o erro, informando que tais UUIDs, não pertencem ao mesmo cliente.

Caso um dispositivo no arquivo CSV esteja com algum dado incorreto, é exibida uma janela informando o erro e a linha onde deve ser efetuada a correção.

Error import batch



Invalid fields / Line 1

UUID: as-CF90-4436-D105-0B15CC47F036

Invalid fields / Line 2

UUID: dad-26E5-1213-B4B0-6AC5B4E0C327

Invalid fields / Line 3

UUID: adsadassa-EA0F-D4A9-E500-4FED55BD1E28

Invalid fields / Line 4

UUID: adasd-2E32-3650-3AFA-D9AEA13C9FF7

Duplicate name / Line 5

Name: Lote2

Invalid fields / Line 5

UUID: asdsadas-D46F-0D90-995A-20158F17AF74

Close

Error Import Batch



De forma a assegurar a integridade do lote, caso qualquer erro seja detectado, o lote inteiro será descartado.

Close



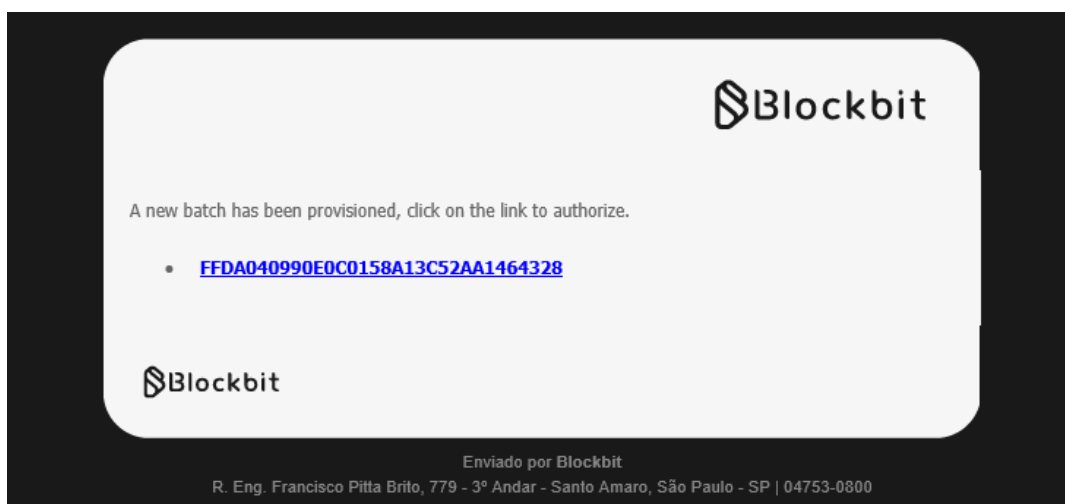
Efetue as correções indicadas e tente novamente. Para fechar essa janela clique no botão [Close] ou em [X].

Além da validação do próprio CSV, o provisionamento em lote também pode ser cancelado por erros no UUID, para mais informações, consulte esta [página](#).

Add

Caso todos os *devices* estejam corretamente configurados, ao clicar em [Add] as configurações serão salvas e um *e-mail* de confirmação será enviado para o endereço que estiver cadastrado no Portal de Licenças da Blockbit. Será necessário clicar no *link* que aparecerá no corpo do *e-mail* para de fato iniciar o provisionamento propriamente dito.

O *e-mail* de confirmação enviado ao autorizar o provisionamento, está demonstrado abaixo:



Batch Provisioning - E-mail de confirmação

Desta etapa em diante, o processo será idêntico ao provisionamento de um único device sendo possível acompanhar o progresso na [aba de Provisioning](#) do GSM, além disso, também é possível ver o andamento pela própria interface do UTM. Para mais informações, consulte esta [página](#).

Após o provisionamento ter sido concluído com sucesso, os devices serão exibidos na [aba Inventory](#), como demonstrado abaixo:

Devices

InventoryCommunitiesTemplatesProvisioning

5 records

No Group

BBv-1000

BBE0-56CC-FFE8-0440

BLOCKBIT UTM 2.0.5
build 20080307

Test

No Group

BBv-100

639D-194F-3158-200F

BLOCKBIT UTM 2.0.5
build 20080307

Test

No Group

BBv-5.000

545F-A663-0918-7C0B

BLOCKBIT UTM 2.0.5
build 20080307

Test

No Group

BBv-100

47D2-96A6-4F28-4246

BLOCKBIT UTM 2.0.5
build 20080307

Test

No Group

BBv-100

15F2-B8B6-0CF3-56C0

BLOCKBIT UTM 2.0.5
build 20080307

Test

1

16 / page

Devices - Inventory - Provisioned Devices

Para mais informações a respeito das colunas da aba *Provisioning* clique neste [link](#), quanto à *Zero Touch Provisioning*, consulte esta [página](#).

Possíveis erros no provisionamento

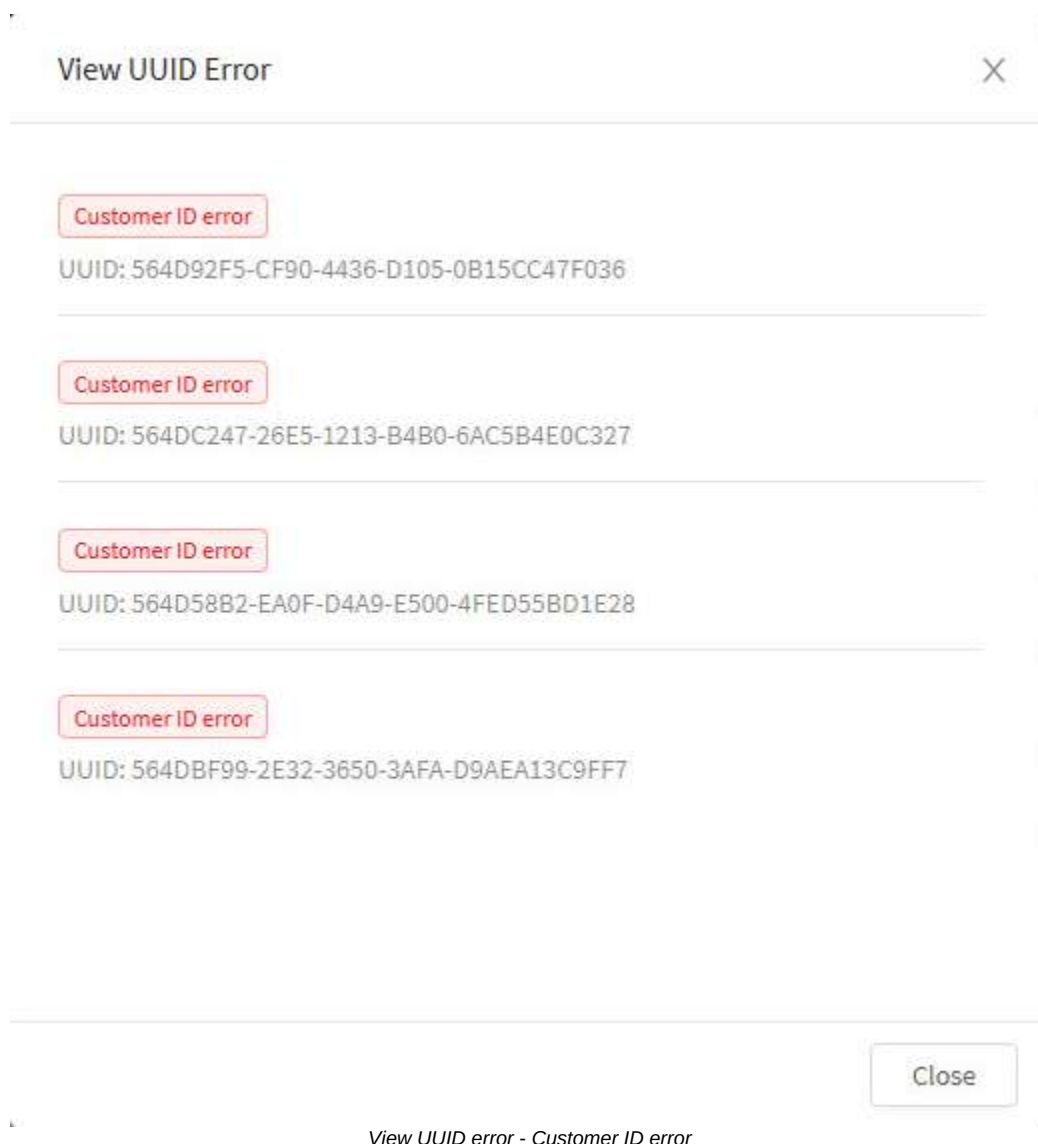
Além da validação do próprio CSV, o provisionamento em lote também pode ser cancelado no casos à seguir:

- [Customer id com erro](#);
- [Licença em uso](#);
- [Licença expirada](#);
- [Licença não encontrada](#);
- [Licença inativa](#).

Para ver mais detalhes a respeito destes erros, basta clicar no ícone [**Error batch**] na coluna de *status*.

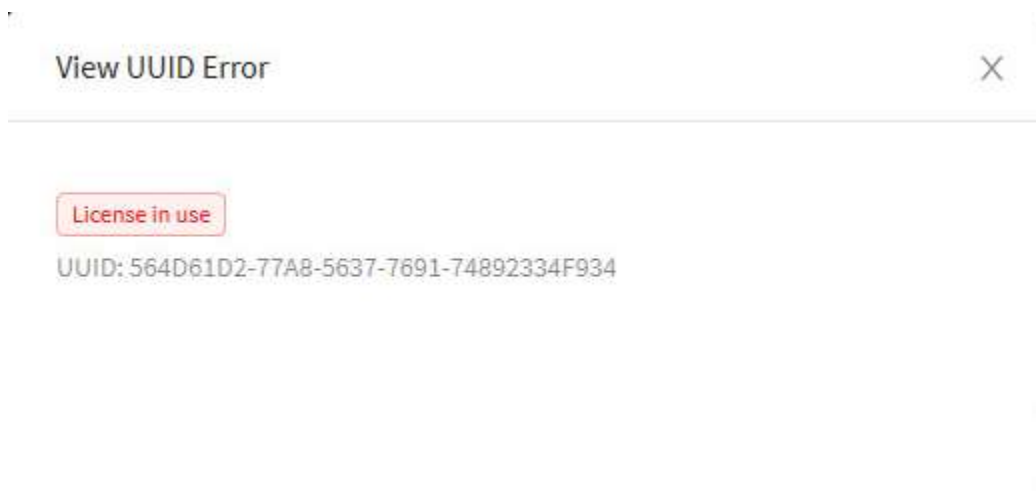
A seguir iremos demonstrar a janela que é exibida ao visualizar estes erros.

Customer ID incorreto



Este erro é exibido caso o *UUID* utilizado no Lote esteja atrelado a outro usuário. Só é possível fazer provisionamento quando o cliente vinculado ao *UUID* é o mesmo, caso haja divergências este erro será apresentado, informando que os *UUIDs* não pertencem ao mesmo cliente.

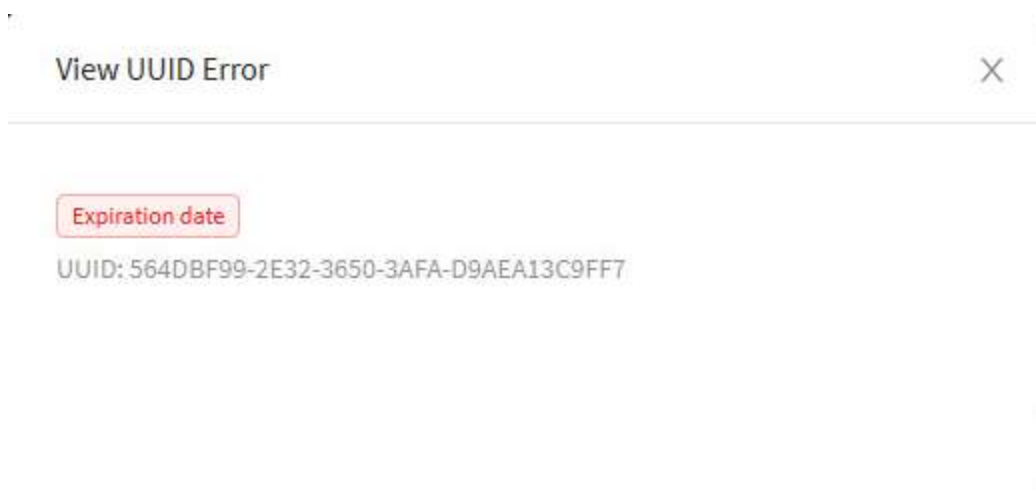
Licença em uso



View UUID error - License in Use

Este erro é exibido caso a licença utilizada no *Lote* já esteja em uso por outro *device*. Caso esse UUID se refira a um *device* provisionado pelo GSM, é recomendável verificar a aba [Inventory](#), onde será possível administrá-lo e removê-lo.

Licença expirada



View UUID error - Expiration Date

Este erro é exibido caso a licença utilizada no *Lote* está expirada. Neste caso, entre em contato com a Blockbit para regularizar a sua situação.

Licença não encontrada



View UUID error - License not found

Este erro é exibido caso a licença não tenha sido localizada no portal. Neste caso, entre em contato com a Blockbit para regularizar a sua situação.

Licença inativa



View UUID error - Inactive License

Este erro é exibido caso a licença esteja inativa. Neste caso, entre em contato com a Blockbit para regularizar a sua situação.

Portanto, assegure-se de que as licenças de todos os dispositivos a serem realizados em provisionamento em lote estão válidas e que os dados do CSV foram completados corretamente antes de efetuar o provisionamento em lote.

Para mais informações sobre provisionamento em lote, consulte esta [página](#).

Sintaxe de Fuso-horário no CSV

De forma a facilitar a edição do CSV, segue uma tabela com o todos os fuso-horários aceitos no UTM e o valor equivalente a ser adicionado no CSV:

Timezone	Valor
Africa/Abidjan	Africa/Abidjan
Africa/Accra	Africa/Accra
Africa/Addis_Ababa	Africa/Addis_Ababa
Africa/Algiers	Africa/Algiers
Africa/Asmara	Africa/Asmara
Africa/Bamako	Africa/Bamako
Africa/Bangui	Africa/Bangui
Africa/Banjul	Africa/Banjul
Africa/Bissau	Africa/Bissau
Africa/Blantyre	Africa/Blantyre
Africa/Brazzaville	Africa/Brazzaville
Africa/Bujumbura	Africa/Bujumbura
Africa/Cairo	Africa/Cairo
Africa/Casablanca	Africa/Casablanca
Africa/Ceuta - Ceuta, Melilla	Africa/Ceuta
Africa/Conakry	Africa/Conakry
Africa/Dakar	Africa/Dakar
Africa/Dar_es_Salaam	Africa/Dar_es_Salaam
Africa/Djibouti	Africa/Djibouti
Africa/Douala	Africa/Douala
Africa/El_Aaiun	Africa/El_Aaiun
Africa/Freetown	Africa/Freetown
Africa/Gaborone	Africa/Gaborone
Africa/Harare	Africa/Harare
Africa/Johannesburg	Africa/Johannesburg
Africa/Juba	Africa/Juba
Africa/Kampala	Africa/Kampala
Africa/Khartoum	Africa/Khartoum
Africa/Kigali	Africa/Kigali
Africa/Kinshasa - Dem. Rep. of Congo (west)	Africa/Kinshasa
Africa/Lagos	Africa/Lagos
Africa/Libreville	Africa/Libreville
Africa/Lome	Africa/Lome
Africa/Luanda	Africa/Luanda
Africa/Lubumbashi - Dem. Rep. of Congo (east)	Africa/Lubumbashi
Africa/Lusaka	Africa/Lusaka
Africa/Malabo	Africa/Malabo

Africa/Maputo	Africa/Maputo
Africa/Maseru	Africa/Maseru
Africa/Mbabane	Africa/Mbabane
Africa/Mogadishu	Africa/Mogadishu
Africa/Monrovia	Africa/Monrovia
Africa/Nairobi	Africa/Nairobi
Africa/Ndjamena	Africa/Ndjamena
Africa/Niamey	Africa/Niamey
Africa/Nouakchott	Africa/Nouakchott
Africa/Ouagadougou	Africa/Ouagadougou
Africa/Porto-Novo	Africa/Porto-Novo
Africa/Sao_Tome	Africa/Sao_Tome
Africa/Tripoli	Africa/Tripoli
Africa/Tunis	Africa/Tunis
Africa/Windhoek	Africa/Windhoek
America/Adak - Aleutian Islands	America/Adak
America/Anchorage - Alaska (most areas)	America/Anchorage
America/Anguilla	America/Anguilla
America/Antigua	America/Antigua
America/Araguaina - Tocantins	America/Araguaina
America/Argentina/Buenos_Aires - Buenos Aires (BA, CF)	America/Argentina/Buenos_Aires
America/Argentina/Catamarca - Catamarca (CT); Chubut (CH)	America/Argentina/Catamarca
America/Argentina/Cordoba - Argentina (most areas: CB, CC, CN, ER, FM, MN, SE, SF)	America/Argentina/Cordoba
America/Argentina/Jujuy - Jujuy (JY)	America/Argentina/Jujuy
America/Argentina/La_Rioja - La Rioja (LR)	America/Argentina/La_Rioja
America/Argentina/Mendoza - Mendoza (MZ)	America/Argentina/Mendoza
America/Argentina/Rio_Gallegos - Santa Cruz (SC)	America/Argentina/Rio_Gallegos
America/Argentina/Salta - Salta (SA, LP, NQ, RN)	America/Argentina/Salta
America/Argentina/San_Juan - San Juan (SJ)	America/Argentina/San_Juan
America/Argentina/San_Luis - San Luis (SL)	America/Argentina/San_Luis
America/Argentina/Tucuman - Tucuman (TM)	America/Argentina/Tucuman
America/Argentina/Ushuaia - Tierra del Fuego (TF)	America/Argentina/Ushuaia
America/Aruba	America/Aruba
America/Asuncion	America/Asuncion
America/Atikokan - EST - ON (Atikokan); NU (Coral H)	America/Atikokan
America/Bahia - Bahia	America/Bahia
America/Bahia_Banderas - Central Time - Bahia de Banderas	America/Bahia_Banderas
America/Barbados	America/Barbados
America/Belem - Para (east); Amapa	America/Belem
America/Belize	America/Belize
America/Blanc-Sablon - AST - QC (Lower North Shore)	America/Blanc-Sablon

America/Boa_Vista - Roraima	America/Boa_Vista
America/Bogota	America/Bogota
America/Boise - Mountain - ID (south); OR (east)	America/Boise
America/Cambridge_Bay - Mountain - NU (west)	America/Cambridge_Bay
America/Campo_Grande - Mato Grosso do Sul	America/Campo_Grande
America/Cancun - Eastern Standard Time - Quintana Roo	America/Cancun
America/Caracas	America/Caracas
America/Cayenne	America/Cayenne
America/Cayman	America/Cayman
America/Chicago - Central (most areas)	America/Chicago
America/Chihuahua - Mountain Time - Chihuahua (most areas)	America/Chihuahua
America/Costa_Rica	America/Costa_Rica
America/Creston - MST - BC (Creston)	America/Creston
America/Cuiaba - Mato Grosso	America/Cuiaba
America/Curacao	America/Curacao
America/Danmarkshavn - National Park (east coast)	America/Danmarkshavn
America/Dawson - Pacific - Yukon (north)	America/Dawson
America/Dawson_Creek - MST - BC (Dawson Cr, Ft St John)	America/Dawson_Creek
America/Denver - Mountain (most areas)	America/Denver
America/Detroit - Eastern - MI (most areas)	America/Detroit
America/Dominica	America/Dominica
America/Edmonton - Mountain - AB; BC (E); SK (W)	America/Edmonton
America/Eirunepe - Amazonas (west)	America/Eirunepe
America/El_Salvador	America/El_Salvador
America/Fort_Nelson - MST - BC (Ft Nelson)	America/Fort_Nelson
America/Fortaleza - Brazil (northeast: MA, PI, CE, RN, PB)	America/Fortaleza
America/Glace_Bay - Atlantic - NS (Cape Breton)	America/Glace_Bay
America/Godthab - Greenland (most areas)	America/Godthab
America/Goose_Bay - Atlantic - Labrador (most areas)	America/Goose_Bay
America/Grand_Turk	America/Grand_Turk
America/Grenada	America/Grenada
America/Guadeloupe	America/Guadeloupe
America/Guatemala	America/Guatemala
America/Guayaquil - Ecuador (mainland)	America/Guayaquil
America/Guyana	America/Guyana
America/Halifax - Atlantic - NS (most areas); PE	America/Halifax
America/Havana	America/Havana
America/Hermosillo - Mountain Standard Time - Sonora	America/Hermosillo
America/Indiana/Indianapolis - Eastern - IN (most areas)	America/Indiana/Indianapolis
America/Indiana/Knox - Central - IN (Starke)	America/Indiana/Knox
America/Indiana/Marengo - Eastern - IN (Crawford)	America/Indiana/Marengo

America/Indiana/Petersburg - Eastern - IN (Pike)	America/Indiana/Petersburg
America/Indiana/Tell_City - Central - IN (Perry)	America/Indiana/Tell_City
America/Indiana/Vevay - Eastern - IN (Switzerland)	America/Indiana/Vevay
America/Indiana/Vincennes - Eastern - IN (Da, Du, K, Mn)	America/Indiana/Vincennes
America/Indiana/Winamac - Eastern - IN (Pulaski)	America/Indiana/Winamac
America/Inuvik - Mountain - NT (west)	America/Inuvik
America/Iqaluit - Eastern - NU (most east areas)	America/Iqaluit
America/Jamaica	America/Jamaica
America/Juneau - Alaska - Juneau area	America/Juneau
America/Kentucky/Louisville - Eastern - KY (Louisville area)	America/Kentucky/Louisville
America/Kentucky/Monticello - Eastern - KY (Wayne)	America/Kentucky/Monticello
America/Kralendijk	America/Kralendijk
America/La_Paz	America/La_Paz
America/Lima	America/Lima
America/Los_Angeles - Pacific	America/Los_Angeles
America/Lower_Princes	America/Lower_Princes
America/Maceio - Alagoas, Sergipe	America/Maceio
America/Managua	America/Managua
America/Manaus - Amazonas (east)	America/Manaus
America/Marigot	America/Marigot
America/Martinique	America/Martinique
America/Matamoros - Central Time US - Coahuila, Nuevo Leon, Tamaulipas (US border)	America/Matamoros
America/Mazatlan - Mountain Time - Baja California Sur, Nayarit, Sinaloa	America/Mazatlan
America/Menominee - Central - MI (Wisconsin border)	America/Menominee
America/Merida - Central Time - Campeche, Yucatan	America/Merida
America/Metlakatla - Alaska - Annette Island	America/Metlakatla
America/Mexico_City - Central Time	America/Mexico_City
America/Miquelon	America/Miquelon
America/Moncton - Atlantic - New Brunswick	America/Moncton
America/Monterrey - Central Time - Durango; Coahuila, Nuevo Leon, Tamaulipas (most areas)	America/Monterrey
America/Montevideo	America/Montevideo
America/Montserrat	America/Montserrat
America/Nassau	America/Nassau
America/New_York - Eastern (most areas)	America/New_York
America/Nipigon - Eastern - ON, QC (no DST 1967-73)	America/Nipigon
America/Nome - Alaska (west)	America/Nome
America/Noronha - Atlantic islands	America/Noronha
America/North_Dakota/Beulah - Central - ND (Mercer)	America/North_Dakota/Beulah
America/North_Dakota/Center - Central - ND (Oliver)	America/North_Dakota/Center
America/North_Dakota/New_Salem - Central - ND (Morton rural)	America/North_Dakota/New_Salem
America/Ojinaga - Mountain Time US - Chihuahua (US border)	America/Ojinaga

America/Panama	America/Panama
America/Pangnirtung - Eastern - NU (Pangnirtung)	America/Pangnirtung
America/Paramaribo	America/Paramaribo
America/Phoenix - MST - Arizona (except Navajo)	America/Phoenix
America/Port_of_Spain	America/Port_of_Spain
America/Port-au-Prince	America/Port-au-Prince
America/Porto_Velho - Rondonia	America/Porto_Velho
America/Puerto_Rico	America/Puerto_Rico
America/Punta_Arenas - Region of Magallanes	America/Punta_Arenas
America/Rainy_River - Central - ON (Rainy R, Ft Frances)	America/Rainy_River
America/Rankin_Inlet - Central - NU (central)	America/Rankin_Inlet
America/Recife - Pernambuco	America/Recife
America/Regina - CST - SK (most areas)	America/Regina
America/Resolute - Central - NU (Resolute)	America/Resolute
America/Rio_Branco - Acre	America/Rio_Branco
America/Santarem - Para (west)	America/Santarem
America/Santiago - Chile (most areas)	America/Santiago
America/Santo_Domingo	America/Santo_Domingo
America/Sao_Paulo - Brazil (southeast: GO, DF, MG, ES, RJ, SP, PR, SC, RS)	America/Sao_Paulo
America/Scoresbysund - Scoresbysund/Itoqqortoormiit	America/Scoresbysund
America/Sitka - Alaska - Sitka area	America/Sitka
America/St_Barthelemy	America/St_Barthelemy
America/St_Johns - Newfoundland; Labrador (southeast)	America/St_Johns
America/St_Kitts	America/St_Kitts
America/St_Lucia	America/St_Lucia
America/St_Thomas	America/St_Thomas
America/St_Vincent	America/St_Vincent
America/Swift_Current - CST - SK (midwest)	America/Swift_Current
America/Tegucigalpa	America/Tegucigalpa
America/Thule - Thule/Pituffik	America/Thule
America/Thunder_Bay - Eastern - ON (Thunder Bay)	America/Thunder_Bay
America/Tijuana - Pacific Time US - Baja California	America/Tijuana
America/Toronto - Eastern - ON, QC (most areas)	America/Toronto
America/Tortola	America/Tortola
America/Vancouver - Pacific - BC (most areas)	America/Vancouver
America/Whitehorse - Pacific - Yukon (south)	America/Whitehorse
America/Winnipeg - Central - ON (west); Manitoba	America/Winnipeg
America/Yakutat - Alaska - Yakutat	America/Yakutat
America/Yellowknife - Mountain - NT (central)	America/Yellowknife
Antarctica/Casey - Casey	Antarctica/Casey
Antarctica/Davis - Davis	Antarctica/Davis

Antarctica/DumontD'Urville - Dumont-d'Urville	Antarctica/DumontD'Urville
Antarctica/Macquarie - Macquarie Island	Antarctica/Macquarie
Antarctica/Mawson - Mawson	Antarctica/Mawson
Antarctica/McMurdo - New Zealand time - McMurdo, South Pole	Antarctica/McMurdo
Antarctica/Palmer - Palmer	Antarctica/Palmer
Antarctica/Rothera - Rothera	Antarctica/Rothera
Antarctica/Syowa - Syowa	Antarctica/Syowa
Antarctica/Troll - Troll	Antarctica/Troll
Antarctica/Vostok - Vostok	Antarctica/Vostok
Arctic/Longyearbyen	Arctic/Longyearbyen
Asia/Aden	Asia/Aden
Asia/Almaty - Kazakhstan (most areas)	Asia/Almaty
Asia/Amman	Asia/Amman
Asia/Anadyr - MSK+09 - Bering Sea	Asia/Anadyr
Asia/Aqtau - Mangghystau/Mankistau	Asia/Aqtau
Asia/Aqtobe - Aqtobe/Aktobe	Asia/Aqtobe
Asia/Ashgabat	Asia/Ashgabat
Asia/Atyrau - Atyrau/Atirau/Gur'yev	Asia/Atyrau
Asia/Baghdad	Asia/Baghdad
Asia/Bahrain	Asia/Bahrain
Asia/Baku	Asia/Baku
Asia/Bangkok	Asia/Bangkok
Asia/Barnaul - MSK+04 - Altai	Asia/Barnaul
Asia/Beirut	Asia/Beirut
Asia/Bishkek	Asia/Bishkek
Asia/Brunei	Asia/Brunei
Asia/Chita - MSK+06 - Zabaykalsky	Asia/Chita
Asia/Choibalsan - Dornod, Sukhbaatar	Asia/Choibalsan
Asia/Colombo	Asia/Colombo
Asia/Damascus	Asia/Damascus
Asia/Dhaka	Asia/Dhaka
Asia/Dili	Asia/Dili
Asia/Dubai	Asia/Dubai
Asia/Dushanbe	Asia/Dushanbe
Asia/Famagusta - Northern Cyprus	Asia/Famagusta
Asia/Gaza - Gaza Strip	Asia/Gaza
Asia/Hebron - West Bank	Asia/Hebron
Asia/Ho_Chi_Minh	Asia/Ho_Chi_Minh
Asia/Hong_Kong	Asia/Hong_Kong
Asia/Hovd - Bayan-Olgii, Govi-Altai, Hovd, Uvs, Zavkhan	Asia/Hovd
Asia/Irkutsk - MSK+05 - Irkutsk, Buryatia	Asia/Irkutsk

Asia/Jakarta - Java, Sumatra	Asia/Jakarta
Asia/Jayapura - New Guinea (West Papua / Irian Jaya); Maluku/Moluccas	Asia/Jayapura
Asia/Jerusalem	Asia/Jerusalem
Asia/Kabul	Asia/Kabul
Asia/Kamchatka - MSK+09 - Kamchatka	Asia/Kamchatka
Asia/Karachi	Asia/Karachi
Asia/Kathmandu	Asia/Kathmandu
Asia/Khandyga - MSK+06 - Tomponsky, Ust-Maysky	Asia/Khandyga
Asia/Kolkata	Asia/Kolkata
Asia/Krasnoyarsk - MSK+04 - Krasnoyarsk area	Asia/Krasnoyarsk
Asia/Kuala_Lumpur - Malaysia (peninsula)	Asia/Kuala_Lumpur
Asia/Kuching - Sabah, Sarawak	Asia/Kuching
Asia/Kuwait	Asia/Kuwait
Asia/Macau	Asia/Macau
Asia/Magadan - MSK+08 - Magadan	Asia/Magadan
Asia/Makassar - Borneo (east, south); Sulawesi/Celebes, Bali, Nusa Tenggara; Timor (west)	Asia/Makassar
Asia/Manila	Asia/Manila
Asia/Muscat	Asia/Muscat
Asia/Nicosia - Cyprus (most areas)	Asia/Nicosia
Asia/Novokuznetsk - MSK+04 - Kemerovo	Asia/Novokuznetsk
Asia/Novosibirsk - MSK+04 - Novosibirsk	Asia/Novosibirsk
Asia/Omsk - MSK+03 - Omsk	Asia/Omsk
Asia/Oral - West Kazakhstan	Asia/Oral
Asia/Phnom_Penh	Asia/Phnom_Penh
Asia/Pontianak - Borneo (west, central)	Asia/Pontianak
Asia/Pyongyang	Asia/Pyongyang
Asia/Qatar	Asia/Qatar
Asia/Qostanay - Qostanay/Kostanay/Kustanay	Asia/Qostanay
Asia/Qyzylorda - Qyzylorda/Kyzylorda/Kzyl-Orda	Asia/Qyzylorda
Asia/Riyadh	Asia/Riyadh
Asia/Sakhalin - MSK+08 - Sakhalin Island	Asia/Sakhalin
Asia/Samarkand - Uzbekistan (west)	Asia/Samarkand
Asia/Seoul	Asia/Seoul
Asia/Shanghai - Beijing Time	Asia/Shanghai
Asia/Singapore	Asia/Singapore
Asia/Srednekolymsk - MSK+08 - Sakha (E); North Kuril Is	Asia/Srednekolymsk
Asia/Taipei	Asia/Taipei
Asia/Tashkent - Uzbekistan (east)	Asia/Tashkent
Asia/Tbilisi	Asia/Tbilisi
Asia/Tehran	Asia/Tehran
Asia/Thimphu	Asia/Thimphu

Asia/Tokyo	Asia/Tokyo
Asia/Tomsk - MSK+04 - Tomsk	Asia/Tomsk
Asia/Ulaanbaatar - Mongolia (most areas)	Asia/Ulaanbaatar
Asia/Urumqi - Xinjiang Time	Asia/Urumqi
Asia/Ust-Nera - MSK+07 - Oymyakonsky	Asia/Ust-Nera
Asia/Vientiane	Asia/Vientiane
Asia/Vladivostok - MSK+07 - Amur River	Asia/Vladivostok
Asia/Yakutsk - MSK+06 - Lena River	Asia/Yakutsk
Asia/Yangon	Asia/Yangon
Asia/Yekaterinburg - MSK+02 - Urals	Asia/Yekaterinburg
Asia/Yerevan	Asia/Yerevan
Atlantic/Azores - Azores	Atlantic/Azores
Atlantic/Bermuda	Atlantic/Bermuda
Atlantic/Canary - Canary Islands	Atlantic/Canary
Atlantic/Cape_Verde	Atlantic/Cape_Verde
Atlantic/Faroe	Atlantic/Faroe
Atlantic/Madeira - Madeira Islands	Atlantic/Madeira
Atlantic/Reykjavik	Atlantic/Reykjavik
Atlantic/South_Georgia	Atlantic/South_Georgia
Atlantic/St_Helena	Atlantic/St_Helena
Atlantic/Stanley	Atlantic/Stanley
Australia/Adelaide - South Australia	Australia/Adelaide
Australia/Brisbane - Queensland (most areas)	Australia/Brisbane
Australia/Broken_Hill - New South Wales (Yancowinna)	Australia/Broken_Hill
Australia/Currie - Tasmania (King Island)	Australia/Currie
Australia/Darwin - Northern Territory	Australia/Darwin
Australia/Eucla - Western Australia (Eucla)	Australia/Eucla
Australia/Hobart - Tasmania (most areas)	Australia/Hobart
Australia/Lindeman - Queensland (Whitsunday Islands)	Australia/Lindeman
Australia/Lord_Howe - Lord Howe Island	Australia/Lord_Howe
Australia/Melbourne - Victoria	Australia/Melbourne
Australia/Perth - Western Australia (most areas)	Australia/Perth
Australia/Sydney - New South Wales (most areas)	Australia/Sydney
Europe/Amsterdam	Europe/Amsterdam
Europe/Andorra	Europe/Andorra
Europe/Astrakhan - MSK+01 - Astrakhan	Europe/Astrakhan
Europe/Athens	Europe/Athens
Europe/Belgrade	Europe/Belgrade
Europe/Berlin - Germany (most areas)	Europe/Berlin
Europe/Bratislava	Europe/Bratislava
Europe/Brussels	Europe/Brussels

Europe/Bucharest	Europe/Bucharest
Europe/Budapest	Europe/Budapest
Europe/Busingen - Busingen	Europe/Busingen
Europe/Chisinau	Europe/Chisinau
Europe/Copenhagen	Europe/Copenhagen
Europe/Dublin	Europe/Dublin
Europe/Gibraltar	Europe/Gibraltar
Europe/Guernsey	Europe/Guernsey
Europe/Helsinki	Europe/Helsinki
Europe/Isle_of_Man	Europe/Isle_of_Man
Europe/Istanbul	Europe/Istanbul
Europe/Jersey	Europe/Jersey
Europe/Kaliningrad - MSK-01 - Kaliningrad	Europe/Kaliningrad
Europe/Kiev - Ukraine (most areas)	Europe/Kiev
Europe/Kirov - MSK+00 - Kirov	Europe/Kirov
Europe/Lisbon - Portugal (mainland)	Europe/Lisbon
Europe/Ljubljana	Europe/Ljubljana
Europe/London	Europe/London
Europe/Luxembourg	Europe/Luxembourg
Europe/Madrid - Spain (mainland)	Europe/Madrid
Europe/Malta	Europe/Malta
Europe/Mariehamn	Europe/Mariehamn
Europe/Minsk	Europe/Minsk
Europe/Monaco	Europe/Monaco
Europe/Moscow - MSK+00 - Moscow area	Europe/Moscow
Europe/Oslo	Europe/Oslo
Europe/Paris	Europe/Paris
Europe/Podgorica	Europe/Podgorica
Europe/Prague	Europe/Prague
Europe/Riga	Europe/Riga
Europe/Rome	Europe/Rome
Europe/Samara - MSK+01 - Samara, Udmurtia	Europe/Samara
Europe/San_Marino	Europe/San_Marino
Europe/Sarajevo	Europe/Sarajevo
Europe/Saratov - MSK+01 - Saratov	Europe/Saratov
Europe/Simferopol - MSK+00 - Crimea	Europe/Simferopol
Europe/Skopje	Europe/Skopje
Europe/Sofia	Europe/Sofia
Europe/Stockholm	Europe/Stockholm
Europe/Tallinn	Europe/Tallinn
Europe/Tirane	Europe/Tirane

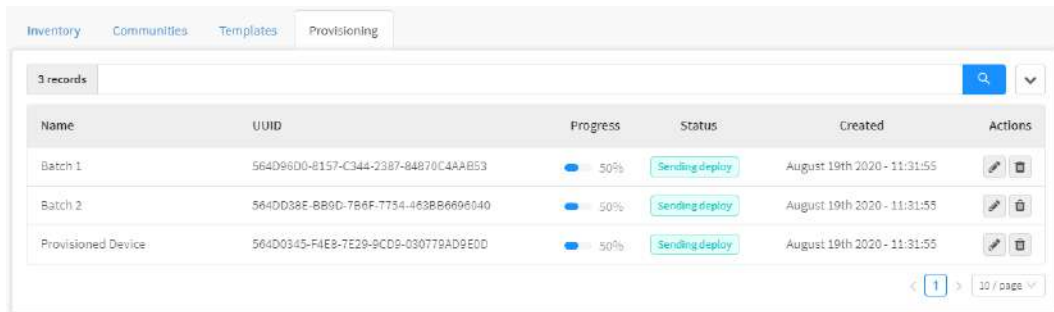
Europe/Ulyanovsk - MSK+01 - Ulyanovsk	Europe/Ulyanovsk
Europe/Uzhgorod - Ruthenia	Europe/Uzhgorod
Europe/Vaduz	Europe/Vaduz
Europe/Vatican	Europe/Vatican
Europe/Vienna	Europe/Vienna
Europe/Vilnius	Europe/Vilnius
Europe/Volgograd - MSK+01 - Volgograd	Europe/Volgograd
Europe/Warsaw	Europe/Warsaw
Europe/Zagreb	Europe/Zagreb
Europe/Zaporozhye - Zaporozh'ye/Zaporizhia; Lugansk/Luhansk (east)	Europe/Zaporozhye
Europe/Zurich	Europe/Zurich
Indian/Antananarivo	Indian/Antananarivo
Indian/Chagos	Indian/Chagos
Indian/Christmas	Indian/Christmas
Indian/Cocos	Indian/Cocos
Indian/Comoro	Indian/Comoro
Indian/Kerguelen	Indian/Kerguelen
Indian/Mahe	Indian/Mahe
Indian/Maldives	Indian/Maldives
Indian/Mauritius	Indian/Mauritius
Indian/Mayotte	Indian/Mayotte
Indian/Reunion	Indian/Reunion
Pacific/Apia	Pacific/Apia
Pacific/Auckland - New Zealand (most areas)	Pacific/Auckland
Pacific/Bougainville - Bougainville	Pacific/Bougainville
Pacific/Chatham - Chatham Islands	Pacific/Chatham
Pacific/Chuuk - Chuuk/Truk, Yap	Pacific/Chuuk
Pacific/Easter - Easter Island	Pacific/Easter
Pacific/Efate	Pacific/Efate
Pacific/Enderbury - Phoenix Islands	Pacific/Enderbury
Pacific/Fakaofu	Pacific/Fakaofu
Pacific/Fiji	Pacific/Fiji
Pacific/Funafuti	Pacific/Funafuti
Pacific/Galapagos - Galapagos Islands	Pacific/Galapagos
Pacific/Gambier - Gambier Islands	Pacific/Gambier
Pacific/Guadalcanal	Pacific/Guadalcanal
Pacific/Guam	Pacific/Guam
Pacific/Honolulu - Hawaii	Pacific/Honolulu
Pacific/Kiritimati - Line Islands	Pacific/Kiritimati
Pacific/Kosrae - Kosrae	Pacific/Kosrae
Pacific/Kwajalein - Kwajalein	Pacific/Kwajalein

Pacific/Majuro - Marshall Islands (most areas)	Pacific/Majuro
Pacific/Marquesas - Marquesas Islands	Pacific/Marquesas
Pacific/Midway - Midway Islands	Pacific/Midway
Pacific/Nauru	Pacific/Nauru
Pacific/Niue	Pacific/Niue
Pacific/Norfolk	Pacific/Norfolk
Pacific/Noumea	Pacific/Noumea
Pacific/Pago_Pago	Pacific/Pago_Pago
Pacific/Palau	Pacific/Palau
Pacific/Pitcairn	Pacific/Pitcairn
Pacific/Pohnpei - Pohnpei/Ponape	Pacific/Pohnpei
Pacific/Port_Moresby - Papua New Guinea (most areas)	Pacific/Port_Moresby
Pacific/Rarotonga	Pacific/Rarotonga
Pacific/Saipan	Pacific/Saipan
Pacific/Tahiti - Society Islands	Pacific/Tahiti
Pacific/Tarawa - Gilbert Islands	Pacific/Tarawa
Pacific/Tongatapu	Pacific/Tongatapu
Pacific/Wake - Wake Island	Pacific/Wake
Pacific/Wallis	Pacific/Wallis

Para mais informações sobre provisionamento em lote, consulte esta [página](#).

Provisioning - Colunas

A seguir explicaremos cada coluna da aba *Provisioning*:



Name	UUID	Progress	Status	Created	Actions
Batch 1	564D96D0-8157-C344-2387-84870C4AAB53	50%	Sending deploy	August 19th 2020 - 11:31:55	 
Batch 2	564D038E-8B9D-7B6F-7754-463B66696040	50%	Sending deploy	August 19th 2020 - 11:31:55	 
Provisioned Device	564D0345-F4E8-7E29-9CD9-030779AD9E0D	50%	Sending deploy	August 19th 2020 - 11:31:55	 

Provisioning

- **Name:** Apresenta o nome do *Device* provisionado cadastrado;
- **UUID:** Apresenta o *UUID* do *Device* cadastrado;
- **Progress:** Exibe uma barra de progresso referente à implantação do *device*;
- **Status:** Exibe o estado atual da implantação do *device*;
- **Created:** Registra a data e o horário de quando o *device* foi adicionado neste painel;
- **Actions:** O menu "Actions" é composto por dois botões:
 - **Botão Edit** : Permite editar as configurações do *device* adicionado na opção [Create Device](#) ou através do Provisionamento em Lote;
 - **Botão Delete** : Deleta o *device*.

Aba Backups

Nesta aba está localizada a ferramenta de gerenciamento dos backups e restores dos UTMs, a função deste recurso é criar rotinas através do GSM e executar remotamente os backups na API dos firewalls.

As rotinas de *backup* são baseadas em *Storages* de *SMB*, *NTS*, *SFTP* e *USB*, além disso, antes de enviar a instrução de criação dos *backups*, o sistema averigua caso haja espaço disponível para o armazenamento e também checa caso outra rotina já esteja sendo executada de modo a garantir que não haja conflitos ou sobrescrição. Embora o diretório de armazenamento e a "ordem" de aplicação do backup seja feita pelo GSM, ele não salva estes arquivos no armazenamento local e sim em um servidor remoto, sendo que as rotinas de *backup* são enviadas de forma criptografada através de um túnel de *VPN*. Após a transferência dos arquivos, de modo a assegurar a confiabilidade na transmissão dos dados, a integridade é verificada através de Checksum (MD5).

Depois de criar as rotinas de backup, o administrador pode remotamente restaurar, fazer download ou remover os arquivos de armazenamento.



Para mais informações sobre rotinas de *backup* automático do próprio GSM, consulte esta [página](#).

Caso queira saber mais sobre criação de *storage devices*, consulte esta [página](#).



O procedimento de *backup* de *devices* está disponível apenas para versão 2.0.1 ou superiores.



É possível consultar os *logs* com mais informações a respeito do procedimento de *backup* através do comando [\[debug-backup\]](#).

Para acessar este recurso, clique na aba *Backups*. Conforme demonstrado abaixo:



Aba Backups

Surgirá a tela de *Backups*. Ela é composta pelas colunas "*Names*", "*Last Backup*", "*Progress*", "*Status*" e "*Actions*". Além disso, no topo da tela estão localizados a [barra de busca](#) e no canto superior direito da tela está o [menu de ações](#).

Nesta janela, todos os itens de cadastro dos pontos de armazenamento do sistema estarão disponíveis.

Devices

Inventory Communities Templates Provisioning Backups

5 records

☐	Name	Last backup	Next backup	Progress	Status	Actions
☐	NFS BACKUP	26/10/2020 12:36	Unscheduled	66%	Running	
☐	SFTP BACKUP	22/10/2020 11:36	22/11/2020 11:30	100%	Success	
☐	ONESHOT SFTP BACKUP	Not done	Unscheduled	0%	Waiting	
☐	MONTHLY USB BACKUP	21/10/2020 11:36	22/11/2020 11:30	100%	Error	
☐	TEST	Not done	Unscheduled	0%	Waiting	

< 1 > 10 / page

Backups

Nesta sessão iremos analisar:

- Como criar *backups* singulares e rotinas de *backup* recorrentes;
- Como editar rotinas de *backup*;
- Componentes das colunas dessa tela.

A seguir, detalharemos o [menu de ações](#).

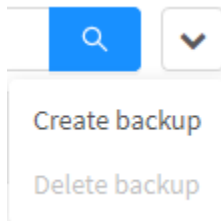
Backups - Menu de Ações

No topo direito da tela temos o menu de ações:



Backups – Botão do menu de ações

Ao clicar neste botão o menu abaixo é exibido:



Backups – Menu de ações

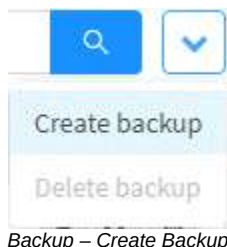
O menu possui as opções :

- [Create Backup;](#)
- [Delete Backup.](#)

A seguir detalharemos cada opção do menu.

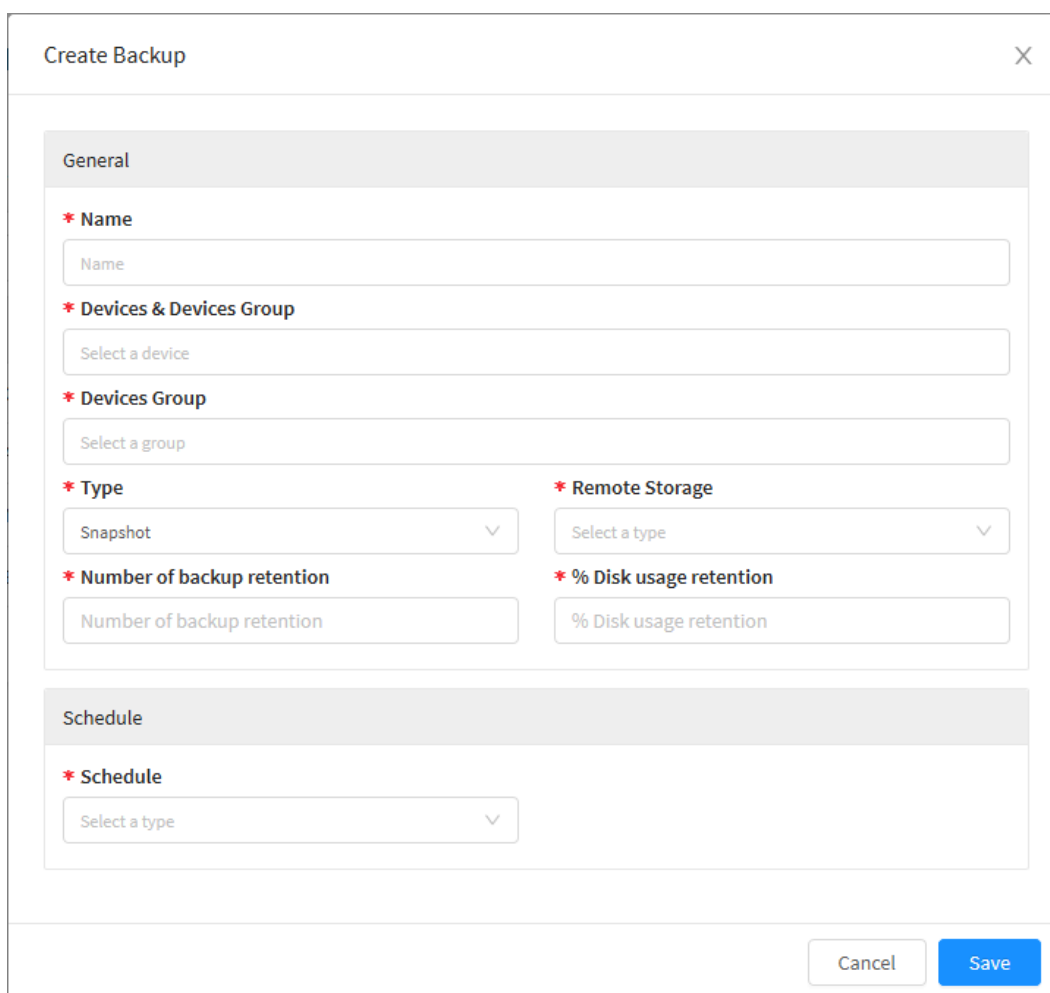
Backup - Menu de ações - Create Backup

Para criar um *backup*, será necessário selecionar o ponto de armazenamento, em quais dispositivos as rotinas de backup serão efetuadas e também se será único ou recorrente. Inicialmente, clique em [] e selecione a opção **Create Backup**, conforme demonstrado abaixo:



Backup – Create Backup

A seguinte janela será exibida:

A screenshot of a 'Create Backup' dialog box. The dialog has a title bar with 'Create Backup' and a close button. It is divided into two main sections: 'General' and 'Schedule'. The 'General' section contains several fields: 'Name' (text input), 'Devices & Devices Group' (text input), 'Devices Group' (text input), 'Type' (dropdown menu with 'Snapshot' selected), 'Remote Storage' (dropdown menu with 'Select a type' selected), 'Number of backup retention' (text input), and '% Disk usage retention' (text input). The 'Schedule' section contains a 'Schedule' dropdown menu with 'Select a type' selected. At the bottom right, there are 'Cancel' and 'Save' buttons.

Backup – Create Backup

Esta janela é dividida em dois painéis:

- [Backup - Menu de ações - Create Backup#General](#);
- [Backup - Menu de ações - Create Backup#Schedule](#).

A seguir iremos detalhar cada painel:

General

O painel *general* é composto pelos seguintes campos:

The screenshot shows the 'General' configuration panel for creating a backup. It contains the following fields:

- * Name:** A text input field with the placeholder 'Name'.
- * Devices & Devices Group:** A dropdown menu with the placeholder 'Select a device'.
- * Devices Group:** A dropdown menu with the placeholder 'Select a group'.
- * Type:** A dropdown menu with 'Snapshot' selected and a downward arrow.
- * Remote Storage:** A dropdown menu with the placeholder 'Select a type' and a downward arrow.
- * Number of backup retention:** A text input field with the placeholder 'Number of backup retention'.
- * Percent usage retention:** A text input field with the placeholder 'Percent usage retention'.

Create Backup - General

- **Name:** Define o nome do *backup*. Ex.: *System Backup - Daily - UTM Devices 2.1 - SMB*;
- **Device & Devices Group:** Determina em qual *Device* ou grupo de *Devices* o *backup* será aplicado. As opções que aparecem neste campo são criados na aba [Inventory](#). Ex.: *UTMDev-2.1*;
- **Type:** Define caso será criado um backup de sistema ou apenas um snapshot das configurações, as opções disponíveis são:
 - **Snapshot** (extensão ".snapshot");
 - **System** (extensão ".system").
- **Remote Storage:** Define a unidade de armazenamento remoto que será utilizada para guardar o *backup*, é criada na aba [Storages](#) em *System*. Ex.: *Storage_SMB*;



ATENÇÃO: É recomendável que o administrador segmente os diretórios onde os *backups* serão armazenados de modo a evitar que os arquivos de *backup* sejam sobrescritos acidentalmente.

- **Number of Backup Retention:** Determina quantos *backups* serão armazenados no diretório. Ao fim deste limite, o *backup* mais antigo é apagado. Por exemplo, caso opte por "3", só serão mantidos os 3 últimos backups, assim sendo, quando um novo *backup* for gerado será executada a rotina para apagar o mais antigo sempre respeitando o valor adicionado neste campo. Ex.: 1;
- **Percent usage retention:** Define a porcentagem de uso que o diretório criado dentro do *storage* usará ao salvar o *backup*. Caso o limite seja atingido, a rotação de *backups* é efetuada, removendo o mais antigo de forma a sempre manter os *backups* mais recentes. Caso um diretório possua 100 GB e seja optado por 30% de retenção, quando os registros ocuparem 30 GB a rotação será ativada, caso contrário, o número de retenção será verificado. Ex.: 100%;



O sistema atua primeiro verificando se a porcentagem de uso foi atingida e depois checando o número de *backups* retidos. Assim sendo:

1. Caso ainda possua espaço livre, o sistema irá verificar o número de *backups* retidos.
2. Caso a quantia máxima de retenção não tenha sido atingida, o armazenamento de *backups* continuará atuando normalmente sem apagar registros anteriores.

Analisando o cenário contrário, a atuação do sistema será conforme explicado abaixo:

1. Caso o limite de espaço seja atingido, a rotação será ativada para manter apenas os *backups* mais recentes;
2. Caso ainda exista espaço em disco, mas o número de *backups* retidos exceda o limite definido pelo administrador, os registros mais antigos serão removidos, respeitando o valor definido no campo, de forma que o diretório possua sempre os *backups* mais recentes.



Se o administrador não quiser que a porcentagem seja considerada, basta adicionar o valor "100" de modo que o espaço seja totalmente utilizado antes de ativar a rotação. Desta forma, só o número de *backups* retidos será considerado.

Schedule

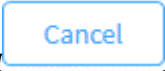
O painel *schedule* é composto pelos seguintes campos:

Create Backup - Schedule

- **Schedule:** Permite determinar a frequência na qual o *backup* será criado. As opções disponíveis são:
 - **Oneshot:** Define que o backup será feito uma única vez. Ao selecionar essa opção, o campo *Date and time* será exibido;
 - **Date and time:** Este campo tem como função agendar quando o *Backup* será executado.
 - **Daily:** Define que o backup será feito uma diariamente. Ao selecionar essa opção, o campo *Hour* será exibido;
 - **Hour:** Este campo tem como função agendar o horário no qual o *Backup* será executado.
 - **Weekly:** Define que o backup será feito uma semanalmente. Ao selecionar essa opção, os campos *Weekday* e *Hour* serão exibidos;
 - **Weekday:** Este campo tem como função agendar o dia da semana no qual o *Backup* será executado;
 - **Hour:** Este campo tem como função agendar o horário no qual o *Backup* será executado.
 - **Monthly:** Define que o backup será feito uma mensalmente. Ao selecionar essa opção, os campos *Month day* e *Hour* serão exibidos;
 - **Month day:** Este campo tem como função agendar o dia do mês no qual o *Backup* será executado;
 - **Hour:** Este campo tem como função agendar o horário no qual o *Backup* será executado.

Cancel

Save

Ao finalizar, clique em [] para cancelar ou em [] para salvar a rotina de *backup*.

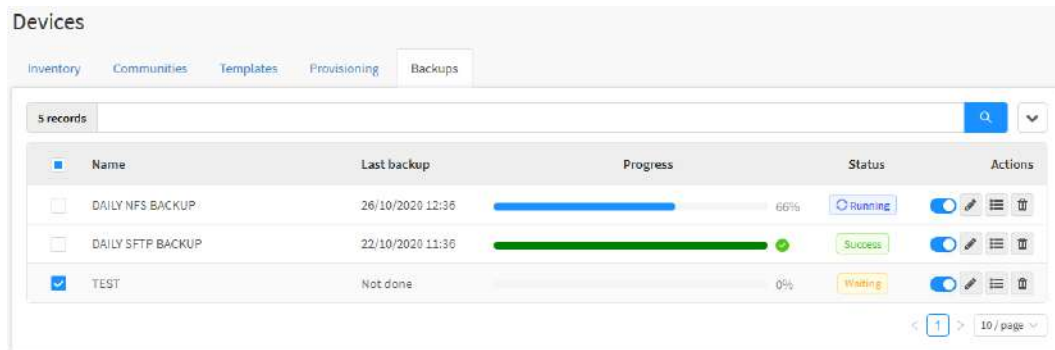
Após efetuar essas configurações, os pontos de armazenamento terão sido definidos no sistema e as rotinas de *backup* para os *devices* serão criadas e listadas nas [colunas](#).

À seguir detalharemos como [remover os backups](#).

Backup - Menu de ações - Delete Backup

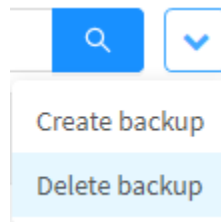
Através do botão "Delete" é possível deletar várias Rotinas de Backup ao mesmo tempo. Para deletar através do menu de ações, siga os seguintes passos:

1. Selecione qual Backup pretende remover, clicando em , como demonstrado abaixo:



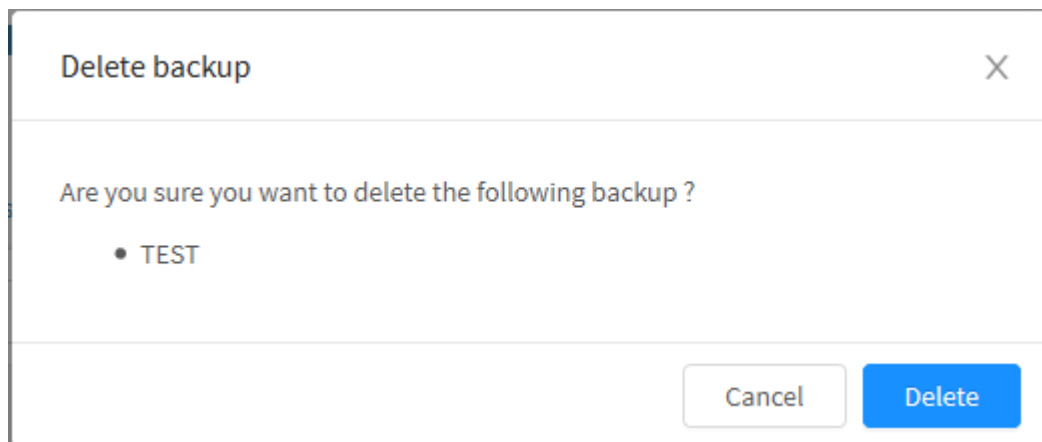
Backups – Seleção das Rotinas de Backup que serão excluídas.

2. Entre no Menu de ações  e clique na opção "Delete Backup";

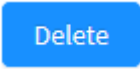


Backups – Delete backup.

3. Surgirá a mensagem se deseja realmente deletar os itens selecionados;



Backups – Delete Backup

A rectangular button with a thin grey border and the word "Cancel" in a light blue font.A solid blue rectangular button with the word "Delete" in white font.

Caso desejar cancelar clique no botão []. Para concluir, clique no botão [].



Backup deleted successfully

Backup deleted successfully

Após realizar esses procedimentos os *Backup* serão excluídos com sucesso.

Backups - Colunas

A seguir explicaremos cada coluna da aba *Backups*:

Devices

InventoryCommunitiesTemplatesProvisioningBackups

5 records

☐	Name	Last backup	Next backup	Progress	Status	Actions
☐	NFS BACKUP	26/10/2020 12:36	Unscheduled	66%	Running	
☐	SFTP BACKUP	22/10/2020 11:36	22/11/2020 11:30	100%	Success	
☐	ONESHOT SFTP BACKUP	Not done	Unscheduled	0%	Waiting	
☐	MONTHLY USB BACKUP	21/10/2020 11:36	22/11/2020 11:30	100%	Error	
☐	TEST	Not done	Unscheduled	0%	Waiting	

<

1

>

10 / page

Backups

- **Name:** Apresenta o nome da rotina de *Backup*;
- **Last backup:** Apresenta quando o último backup foi executado;
- **Next backup:** Seguindo o que foi configurado no agendamento, apresenta quando o próximo backup será executado;
- **Progress:** Exibe uma barra de progresso e uma porcentagem referente à execução do *Backup*;
- **Status:** Exibe o estado atual da execução da rotina de *Backup*, podendo ser:
 - []: A rotina de backup está em execução no momento;
 - []: Aconteceu algo de errado que causou a falha da rotina de *backup*;
 - []: A rotina está em tempo de espera. Isso pode ocorrer quando o sistema detecta um processo que possa interferir no *back up* está em execução no momento (por exemplo, uma outra rotina de *backup*);
 - []: O backup foi executado com sucesso;
- **Actions:** O menu "Actions" é composto pelos botões:
 - **Disable** [] / **Enable Backup** []: Esta opção desabilita ou habilita o agendamento do *backup*. Ao desabilitar o agendamento, os *backups* anteriores não são removidos;
 - **Edit** []: Permite editar as configurações do *backup* adicionado na opção [Create Backup](#);
 - **Backup Details** []: Exibe mais informações a respeito das rotinas de *backup*, consulte esta [página](#) para mais informações;
 - **Delete** []: Deleta a rotina de *backup*, é o equivalente a opção [Delete Backup](#).

Para mais detalhes sobre a aba *backups*, consulte esta [página](#).

Backups - Backup Details

O painel exibido ao clicar no botão **Backup Details** [] tem como função detalhar o progresso da execução das rotinas de *backup* em cada *device* associado à rotina de *backup*.

O painel *Backup details* é composto pelos seguintes campos:

Backups details

System Backup - UTM 2.1 Group - Weekly - NFS

X

2 records

Q

Device	Progress	Status	Actions
UTM 2.1 - 200.1	✓	Success	
UTM 2.1 - 200.41	✓	Success	

< 1 >

10 / page ▾

Close

Backup Details

- **Device:** Apresenta o nome da rotina do *Device*;
- **Progress:** Exibe uma barra de progresso e uma porcentagem referente à execução do *Backup*;
- **Status:** Exibe o estado atual da execução da rotina de *Backup*, podendo ser:
 - []: A rotina de backup está em execução no momento;
 - []: Aconteceu algo de errado que causou a falha da rotina de *backup*;
 - []: A rotina está em tempo de espera. Isso pode ocorrer quando o sistema detecta um processo que possa interferir no *back up* está em execução no momento (por exemplo, uma outra rotina de *backup*);
 - []: O backup foi executado com sucesso;
- **Actions:** O menu “*Actions*” é composto pelo botão:
 - **Backups History**[]: Este botão tem como função detalhar o histórico do *backup*, para mais informações, consulte esta [página](#).

À seguir, detalharemos o botão [Backups History](#);

Para mais informações sobre as colunas, acesse esta [página](#).

Backups - Backups Details - Backup History

O painel exibido ao clicar no botão **Backup History**  tem como função exibir o histórico das rotinas de Backup efetuadas em um determinado *device*. Ele é composto pelos seguintes campos:

Backups history UTM 2.1 - 200.41 X

Name	Size	Last status	Status	Actions
B135-A5AC-A24C-DF29-2.1.0-202103101231.snapshot	18.64 MB	10/03/2021 12:31	Success	  
B135-A5AC-A24C-DF29-2.1.0-202103091231.snapshot	18.64 MB	09/03/2021 12:31	Success	  
B135-A5AC-A24C-DF29-2.1.0-202103091201.snapshot	18.64 MB	09/03/2021 12:01	Success	  
B135-A5AC-A24C-DF29-2.1.0-202103081541.snapshot	18.64 MB	08/03/2021 15:41	Success	  

< 1 > 10 / page

Close

Backup History

- **Name:** Nome do procedimento do *backup*, no exemplo acima, temos snapshots;
- **Size:** Exibe o tamanho do procedimento do *backup*;
- **Last Status:** Define quando a última alteração de *status* ocorreu;
- **Status:** Exibe o estado atual da execução da rotina de *Backup*, podendo ser:
 -  **Running**: A rotina de backup está em execução no momento;
 -  **Error**: Aconteceu algo de errado que causou a falha da rotina de *backup*;
 -  **Waiting**: A rotina está em tempo de espera. Isso pode ocorrer quando o sistema detecta um processo que possa interferir no *back up* está em execução no momento (por exemplo, uma outra rotina de *backup*);
 -  **Success**: O backup foi executado com sucesso;
- **Actions:** O menu “*Actions*” é composto por dois botões:
 -  **Restore**: Ao clicar neste botão o procedimento de *backup* é executado novamente. Caso um backup seja removido do diretório, ele continuará registrado no histórico, porém esta opção estará desabilitada;
 -  **Download**: Ao clicar neste botão, é possível fazer *download* do *snapshot*;
 -  **Delete**: Ao clicar neste botão, o *backup* é removido do histórico.

Para mais informações sobre as colunas, acesse esta [página](#).

Exemplo - Backup de Devices

Esta seção irá apresentar o passo a passo para configuração de Backups de Devices.



Para mais informações a respeito de *Backups* consulte esta [página](#).

Essa demonstração considerará os seguintes cenários:

Backup de Devices - Cenários considerados

Nome das rotinas de Backup	Cenário
System Backup - UTM 2.1 Group - Weekly - NFS-02	Backup de Sistema NFS Semanal
System Backup - UTM 2.1 Group - Daily - NFS-01	Backup de Sistema NFS Diário
Snapshot Backup - UTM 2.1 Group - Daily - NFS-02	Backup de Snapshot NFS Diário
Snapshot Backup - UTM 2.1 Group - Weekly - SFTP-01	Backup de Snapshot SFTP Semanal
Snapshot Backup - UTM 200.41 - Single Time - SFTP-01	Backup de Snapshot SFTP Único

Os seguintes *devices* serão utilizados neste exemplo:

Backup de Devices - Devices utilizados

Nome do Device	Grupo de Device
UTM 2.1 - 200.1	UTM 2.1 Group
UTM 2.1 - 200.41	

Os seguintes Storages serão utilizados neste exemplo:

Backup de Devices - Storages utilizados

Nome	IP
Storage_NFS_01	172.16.102.200
Storage_NFS_02	172.31.160.30
Storage_SFTP_01	172.31.160.31

Os passos que tomaremos nesta demonstração serão:

- [Inclusão de Devices](#);
- [Criação de Storages](#);
- [Criação das Rotinas de Backup](#);
- [Validação das configurações](#).

Iniciaremos a demonstração adicionando os [devices no inventory](#).

Backup de Devices - Inclusão de Devices

Esta seção irá apresentar o passo a passo para configuração de Backups.



Para mais informações a respeito da adição de *Devices*, consulte a [página](#) a respeito da aba *Inventory*.

Os passos que tomaremos nesta demonstração serão:

- [Adição do Device UTM 2.1 - 200.1](#);
- [Adição do Device UTM 2.1 - 200.41](#).

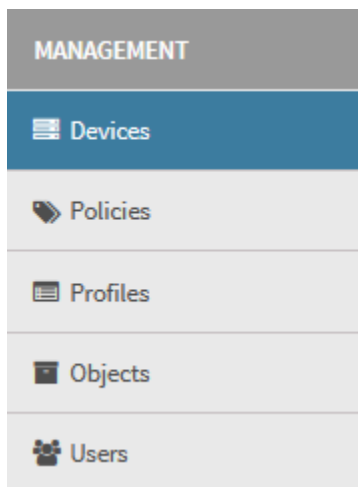
Os seguintes *Devices* serão utilizados neste exemplo:

Backup de Devices - Devices utilizados

Nome	Grupo
UTM 2.1 - 200.1	UTM 2.1 Group
UTM 2.1 - 200.41	

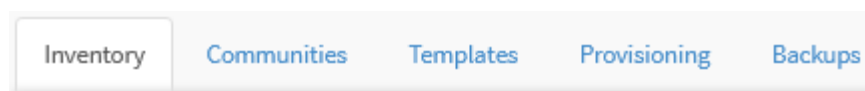
Esta sessão não irá detalhar o processo de instalação e cadastro dos *devices* no GSM, para obter informações mais aprofundadas a respeito destes procedimentos, consulte as instruções presentes nesta [página](#).

Acesse o menu *Management* e clique na opção *Devices*:



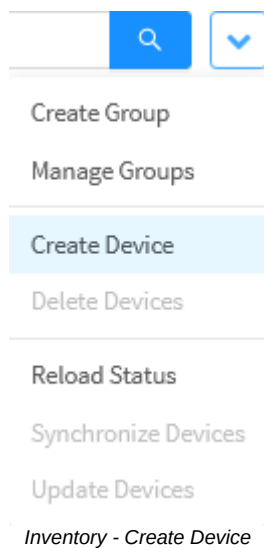
Management - Devices

Clique na aba *Inventory*:



Aba Inventory

Clique no ícone do **Menu de ações**  e selecione a opção "Create Device";



Inicialmente adicionaremos o Device "UTM 2.1 - 200.1":

Adição do Device UTM 2.1 - 200.1

Complete o formulário conforme exemplificado a seguir:

Add Device
X

* Name

UTM 2.1 - 200.1

* Company

Blockbit QA

* Deploy Key

53616c7465645f5fae71eb02a17a5d94c92c040ff40cf8dc43412c6e06e4b4d4a055f258e4
0354841d548f92c6ab29d68dd21f863a59b4f72e16d999e11d90cf6cf6ef66b67d17064fd
deba6705ac64f6e1b04b34237535a2959be5f0dc5709f0799a93c7bccde13d8130eacac

* API Key

870eb285442b834592efbc5d55f4eeb0

* User Admin

admin

Password

.....

Device Group

UTM 2.1 Group

Logger

Remote Logger - 200.30

Description

Cancel
Save

Inventory - Add Device

- **Name:** Nomearemos o *device* como "UTM 2.1 - 200.1";
- **Company:** Neste campo usaremos "Blockbit QA";
- **Deploy Key:** Usaremos a chave de deploy obtida no *Central Management* do UTM em questão;
- **API Key:** Também usaremos a API Key obtida no *Central Management* do UTM;
- **User Admin:** Adicionar o usuário do UTM com permissões de administrativas para efetuar o acesso através do GSM;
- **Password:** Adicionar a senha do usuário do UTM com permissões de administrativas para efetuar o acesso através do GSM;
- **Device Group:** Neste exemplo adicionaremos o *device* ao grupo "UTM 2.1 Group";
- **Logger:** Neste exemplo não lidaremos com Logger, então este campo é opcional;
- **Description:** Não adicionaremos uma descrição.

Clique em  para gravar as configurações.

A seguir, configuraremos o *device* "UTM 2.1 - 200.41":

Adição do Device UTM 2.1 - 200.41

Usaremos as seguintes configurações:

Add Device

X

* Name

UTM 2.1 - 200.41

* Company

Blockbit QA

* Deploy Key

53616c7465645f5d521f743a467c4a6751fc30f77f581100f7be38547c4459f1039bcab4fc
1354fc3f3fd1588d99a2a5a736f2552e653a2f4cd9b3839d2191f32f540e64b0ea5b7f3293
50635b3b947da09b876e0c94e4647f252e56ec7a91eaecaa503e8299f374052862acb4cc

* API Key

9ed9ebc2047978f87471837059c9312f

* User Admin

admin

Password

.....

Device Group

Grupo UTM 2.1

Logger

Logger Remoto - 200.30

Description

Cancel

Save

Inventory - Add Device

- **Name:** Nomearemos o *device* como "UTM 2.1 - 200.41";
- **Company:** Neste campo usaremos "Blockbit QA";
- **Deploy Key:** Usaremos a chave de deploy obtida no *Central Management* do UTM em questão;
- **API Key:** Também usaremos a API Key obtida no *Central Management* do UTM;
- **User Admin:** Adicionar o usuário do UTM com permissões de administrativas para efetuar o acesso através do GSM;
- **Password:** Adicionar a senha do usuário do UTM com permissões de administrativas para efetuar o acesso através do GSM;
- **Device Group:** Neste exemplo adicionaremos o *device* ao grupo "UTM 2.1 Group";
- **Logger:** Neste exemplo não lidaremos com Logger, então este campo é opcional;
- **Description:** Não adicionaremos uma descrição.

Não configuraremos os outros campos, clique em  para gravar as configurações.

Ao finalizar todas as configurações, a tela estará como demonstrado abaixo:

Devices

[Inventory](#)
[Communities](#)
[Templates](#)
[Provisioning](#)
[Backups](#)

5 records

☐
Name

Group

Model

License Status

Version

Template

Policy IPv4

Policy IPv6

Actions

☐	UTM 2.1 - 200.1	Grupo UTM 2.1	BBv-30	E0C4-905A-A41B-4DAA	BLOCKBIT UTM 2.1.0 build 21030815			
☐	UTM 2.1 - 200.41	Grupo UTM 2.1	BBv-30	B135-ASAC-A24C-DF10	BLOCKBIT UTM 2.1.0 build 21030815			

1
10 / page

Loggers - Loggers

Isso finaliza a configuração dos *devices*, a seguir iremos [criar os storages](#).

Bakup de Devices - Criação de Storage

Após ter [adicionado os devices](#), nesta etapa efetuaremos os seguintes passos:

- Criação de Objetos;
 - Criação do Objeto de IP *Storage_NFS_01*;
 - Criação do Objeto de IP *Storage_NFS_02*;
 - Criação do Objeto de IP *Storage_SFTP_02*.
- Configuração dos *Storages*;
 - Criação do *Storage_NFS_01*;
 - Criação do *Storage_NFS_02*;
 - Criação do *Storage_SFTP_01*.

Nesta etapa detalharemos a instalação dos *Storages* utilizados pelo Backup, os seguintes *Storages* serão utilizados neste exemplo:



Este exemplo considerará que o *storage* que será utilizado pelo administrador está instalado e configurado corretamente. Para mais informações a respeito da compatibilidade do Blockbit GSM com *storages* remotos consulte esta [página](#).

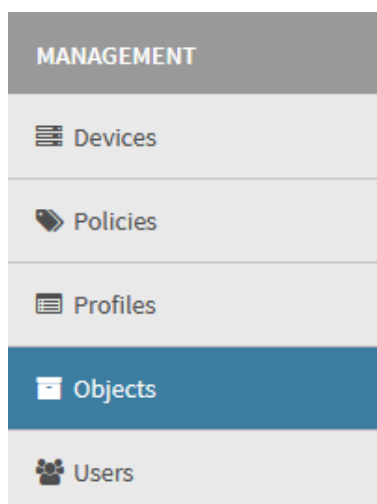
Backup de Devices - Storages utilizados

Nome	IP
Storage_NFS_01	172.16.102.200
Storage_NFS_02	172.31.160.30
Storage_SFTP_01	172.31.160.31

Inicialmente geraremos os IPs que serão utilizados pelos *Storages*.

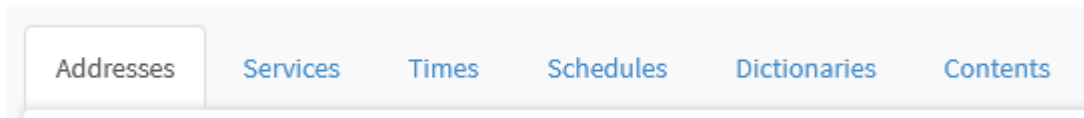
Criação de Objetos

Primeiramente criaremos os Objetos de IP único que serão utilizados para se conectar com os *Storages Remotos*, portanto acesse o menu *Management* e clique na opção *Objects*:



Management - Objects

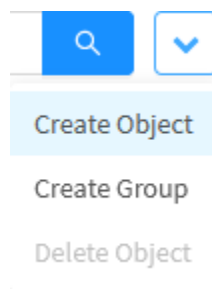
Clique na aba Addresses:



Aba Addresses

Criação do Objeto de IP Storage_NFS_01

Clique no ícone do **Menu de ações**  e selecione a opção "Create Object";



Inventory - Create Device

Inicialmente adicionaremos o IP do Storage_NFS_01, complete o formulário conforme exemplificado a seguir:

Create Addresses Object

X

*

Name

Storage_NFS_01

*

Type

IPv4 Address

▼

✓

Unique

*

Address

172.16.102.200

Mask

255.255.255.255

▼

+

^

▼

-

Description

Cancel

Import Address

Save

Adresses Object - Create Adresses Object

- **Name:** Usaremos o nome "Storage_NFS_01";
- **Type:** Selecione a opção "IPv4 Address";
- **Unique** ☒: Este será um objeto de tipo único, portanto se certifique de marcar esta caixa de seleção;
- **Address:** O endereço do Storage é "172.16.102.200";
- **Mask:** A máscara pode continuar sendo a padrão;
- **Description:** Neste exemplo, não adicionaremos uma descrição.

Clique em  para gravar as configurações.

Criação do Objeto de IP Storage_NFS_02

Além disso, adicionaremos o IP do Storage_NFS_02, complete o formulário conforme exemplificado a seguir:

218

Create Addresses Object

X

* Name

Storage_NFS_02

* Type

IPv4 Address

☒ Unique

* Address

172.31.160.30

Mask

255.255.255.255

+

^

v

-

Description

Cancel

Import Address

Save

Adresses Object - Create Adresses Object

- **Name:** Usaremos o nome "Storage_NFS_02";
- **Type:** Selecione a opção "IPv4 Address";
- **Unique** ☒: Este será um objeto de tipo único, portanto se certifique de marcar esta caixa de seleção;
- **Address:** O endereço do Storage é "172.31.160.30";
- **Mask:** A máscara pode continuar sendo a padrão;
- **Description:** Neste exemplo, não adicionaremos uma descrição.

Save

Clique em [Save] para gravar as configurações.

Criação do Objeto de IP Storage_SFTP_02

Além disso, adicionaremos o IP do Storage_SFTP_02, complete o formulário conforme exemplificado a seguir:

Create Addresses Object

X

*

Name

Storage_SFTP_02

*

Type

IPv4 Address

Unique

*

Address

172.31.160.31

Mask

255.255.255.255

+

-

Description

Cancel

Import Address

Save

Adresses Object - Create Adresses Object

- **Name:** Usaremos o nome "Storage_SFTP_02";
- **Type:** Selecione a opção "IPv4 Address";
- **Unique** ☒: Este será um objeto de tipo único, portanto se certifique de marcar esta caixa de seleção;
- **Address:** O endereço do Storage é "172.31.160.31";
- **Mask:** A máscara pode continuar sendo a padrão;
- **Description:** Neste exemplo, não adicionaremos uma descrição.

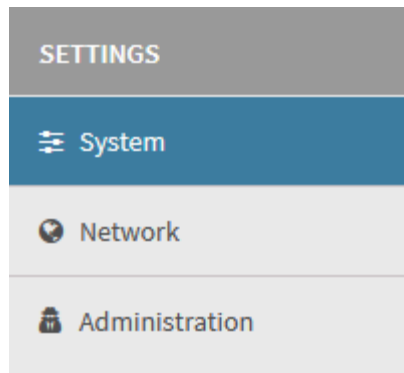
Save

Clique em [] para gravar as configurações.

Após ter criado os objetos de endereço, criaremos os *Storages*.

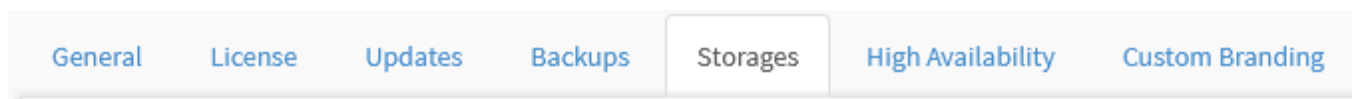
Configuração dos *Storages*

Acesse o menu *Settings* e clique na opção *System*:



Settings - System

Acesse a aba *Storages*:

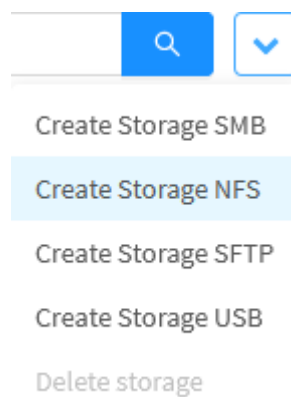


Aba Storages

Criaremos dois *Storages NFS* e um *SFTP*.

Criação do *Storage_NFS_01*

Iniciaremos criando os Storages NFS, clique no ícone do **Menu de ações**  e selecione a opção "*Create Storage NFS*";



Storages - Create Storages NFS

Inicialmente adicionaremos o *Storage_NFS_01*, complete o formulário conforme exemplificado a seguir:

Create Storage NFS

×

* Description

Storage_NFS_01

* IP

Storage_NFS_01

▼

* Directory

/home/bkp-nfs/User/nfs-200.30

Reading Bytes

4096

Writing Bytes

4096

Port

2049

Block sizes Bytes

☐ Protocol TCP

☐ Disable locking

☐ Enable posix

Operation Mode

☒ Hard ☐ Soft

Extra Options

opt=n, opt2=m

Simultaneous transfers

5

☐ Only Logger

Cancel

Save

Storages - Create Storage NFS

Nesta janela iremos apenas configurar os seguintes campos:

- **Description:** Neste exemplo nomearemos o *storage* como "Storage_NFS_01";
- **IP:** Selecione o endereço *IP* do servidor *NFS* configurado no passo anterior, neste caso usaremos o objeto "Storage_NFS_01";
- **Directory:** Usaremos o diretório /home/bkp-nfs/User/nfs-200.30.

Os outros campos podem ser mantidos com a configuração padrão.

Clique em  para gravar as configurações.

Criação do Storage_NFS_02

Novamente, criaremos um Storages NFS, clique no ícone do **Menu de ações**  e selecione a opção "Create Storage NFS";

Create Storage SMB

Create Storage NFS

Create Storage SFTP

Create Storage USB

Delete storage

Storages - Create Storages NFS

Inicialmente adicionaremos o *Storage_NFS_02*, complete o formulário conforme exemplificado a seguir:

Create Storage NFS ✕

* Description

Storage_NFS_02

* IP

Storage_NFS_02 ▼

* Directory

/bkp-blockbit-nfs/user/nfs-200.30

Reading Bytes

4096

Writing Bytes

4096

Port

2049

Block sizes Bytes

☐ Protocol TCP

☐ Disable locking

☐ Enable posix

Operation Mode

☒ Hard ☐ Soft

Extra Options

opt=n, opt2=m

Simultaneous transfers

5

☐ Only Logger

Cancel

Save

Storages - Create Storage NFS

Nesta janela iremos apenas configurar os seguintes campos:

- **Description:** Neste exemplo nomearemos o storage como "Storage_NFS_02";
- **IP:** Selecione o endereço IP do servidor NFS configurado no passo anterior, neste caso usaremos o objeto "Storage_NFS_02";
- **Directory:** Usaremos o diretório "/bkp-blockbit-nfs/user/nfs-200.30".

Os outros campos podem ser mantidos com a configuração padrão.

Clique em para gravar as configurações.

Criação do *Storage_SFTP_01*

Por fim, criaremos um Storage SFTP, clique no ícone do **Menu de ações**  e selecione a opção “*Create Storage SFTP*”;

Menu de ações [] e seleção

- Create Storage SMB
- Create Storage NFS
- Create Storage SFTP
- Create Storage USB
- Delete storage

Storagees - Create Storagees SFTP

Inicialmente adicionaremos o *Storage_SFTP_01*, complete o formulário conforme exemplificado a seguir:

Create Storage SFTP

X

* Description

Storage_SFTP_01

* User

root

* IP

Storage_SFTP_02

* Port

SSH

* Directory

/bkp-blockbit-ssh/user/ssh-200.31

* Simultaneous transfers

5

☐ Compression

☐ Only Logger

Cancel

Save

Storages - Create Storage SFTP

- **Description:** Neste exemplo nomearemos o *storage* como "Storage_SFTP_01";
- **User:** Adicione o usuário administrativo "root";
- **IP:** Selecione o endereço *IP* do servidor *NFS configurado no passo anterior*, neste caso usaremos o objeto "Storage_SFTP_01";
- **Port:** A categoria de acesso será "SSH";
- **Directory:** Usaremos o diretório "/bkp-blockbit-ssh/user/ssh-200.31".
- **Simultaneous transfers:** Podemos deixar como "5";
- **Compression** ☐: Não usaremos esta opção;
- **Only Logger** ☐: Não utilizaremos esta opção.

Save

Clique em [] para gravar as configurações.

Ao finalizar todas as configurações, a tela similar à demonstrada abaixo:

System

General License Updates Backups **Storages** High Availability Custom Branding

4 records

Description	Type	Size	Actions
☐ Storage_NFS_01	NFS	52%	
☐ Storage_NFS_02	NFS	45%	
☐ Storage_SFTP_02	SFTP	45%	

< 1 > 10 / page

System - Storages

No próximo passo, criaremos as [rotinas de Backups](#).

Backup de Devices - Criação das Rotinas de Backup

Criados os [storages](#), iremos nos aprofundar nas rotinas de *backup*:

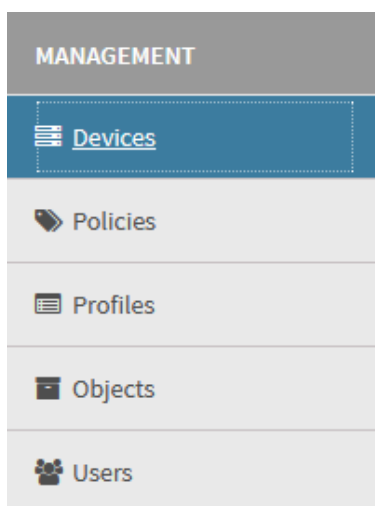
- Criação de Backup de Sistema NFS Semanal;
- Criação de Backup de Sistema NFS Diário;
- Criação de Backup de Snapshot NFS Diário
- Criação de Backup de Snapshot SFTP Semanal;
- Criação de Backup de Snapshot SFTP Único;

As seguintes rotinas de *backup* serão criadas neste exemplo:

Backup de Devices - Backups

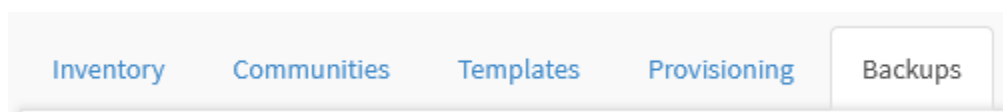
Nome
System Backup - UTM 2.1 Group - Weekly - NFS-02
System Backup - UTM 2.1 Group - Daily - NFS-01
Snapshot Backup - UTM 2.1 Group - Daily - NFS-02
Snapshot Backup - UTM 2.1 Group - Weekly - SFTP-01
Snapshot Backup - UTM 200.41 - Single Time - SFTP-01

Inicialmente, acesse o menu *Management* e clique na opção *Devices*:



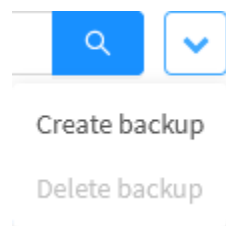
Management - Devices

Clique na aba "*Backups*":



Devices - Aba Backups

Clique no ícone do **Menu de ações**  e selecione a opção “Create Backup”;



Backups - Create Backup

Criação de Backup de Sistema NFS Semanal

Iniciaremos criando um *Backup* Semanal:

Create Backup

General

*

Name

System Backup - UTM 2.1 Group - Weekly - NFS-02

Devices

Select a device

* Devices Group

UTM 2.1 Group X

* Type

System

▼

* Remote Storage

Storage_NFS_02

▼

Number of Backup Retention

1

Percent Usage Retention

100

Schedule

* Schedule

Weekly

▼

* Weekday

Sunday

▼

* Hour

16:00

🕒

Cancel

Save

Backups - Create Backup

227

- **Name:** Neste exemplo nomearemos o *backup* como "System Backup - UTM 2.1 Group - Weekly - NFS-02";
- **Device & Devices Group:** Usaremos o device group "UTM 2.1 Group";
- **Type:** Neste exemplo usaremos o tipo: "System";
- **Remote Storage:** Selecionaremos o "Storage_NFS_02";
- **Number of Backup Retention:** Neste caso configuraremos para que haja retenção de apenas 1 backup;
- **Percent usage retention:** Usaremos 100% do espaço do diretório, de forma que não haja limitação;
- **Schedule:** O agendamento será semanal, portanto selecionaremos a opção "Weekly";
- **Weekday:** Escolha o dia em que o *backup* será feito, neste caso "Sunday";
- **Hour:** Por fim, selecione o horário no qual ele será feito, neste exemplo, será às 16:00.

Save

Clique em [] para gravar as configurações.

Criação de Backup de Sistema NFS Diário

À seguir, criaremos um *Backup* Diário:

Create Backup

General

* Name

System Backup - UTM 2.1 Group - Daily - NFS-01

Devices

UTM Dev - 2.1.0

Devices Group

UTM 2.1 Group

* Type

System

* Remote Storage

Storage_NFS_01

Number of Backup Retention

1

Percent Usage Retention

100

Schedule

* Schedule

Daily

* Hour

18:00

Cancel

Save

Backups - Create Backup

- **Name:** Neste exemplo nomearemos o *backup* como "System Backup - UTM 2.1 Group - Daily - NFS-01";

- **Device & Devices Group:** Usaremos o device group "UTM 2.1 Group";
- **Type:** Neste exemplo usaremos o tipo: "System";
- **Remote Storage:** Seleccionaremos o "Storage_NFS_01";
- **Number of Backup Retention:** Neste caso configuraremos para que haja retenção de apenas 1 backup;
- **Percent usage retention:** Usaremos 100% do espaço do diretório, de forma que não haja limitação;
- **Schedule:** O agendamento será diário, portanto seleccionaremos a opção "Daily";
- **Hour:** Por fim, selecione o horário no qual ele será feito, neste exemplo, será às "18:00".

Save

Clique em [] para gravar as configurações.

Criação de Backup de Snapshot NFS Diário

À seguir, criaremos um *Backup de Snapshot Diário*:

Create Backup

General

* Name

Snapshot Backup - UTM 2.1 Group - Daily - NFS-02

Devices

Select a device

* Devices Group

UTM 2.1 Group X

* Type

Snapshot

* Remote Storage

Storage_NFS_02

Number of Backup Retention

2

Percent Usage Retention

100

Schedule

* Schedule

Daily

* Hour

12:30

Cancel

Save

Backups - Create Backup

- **Name:** Neste exemplo nomearemos o *backup* como "Snapshot Backup - UTM 2.1 Group - Daily - NFS-02";
- **Device & Devices Group:** Usaremos o device group "UTM 2.1 Group";
- **Type:** Neste exemplo usaremos o tipo: "Snapshot";
- **Remote Storage:** Seleccionaremos o "Storage_NFS_02";

- **Number of Backup Retention:** Neste caso configuraremos para que haja retenção de 2 backups;
- **Percent usage retention:** Usaremos 100% do espaço do diretório, de forma que não haja limitação;
- **Schedule:** O agendamento será diário, portanto selecionaremos a opção "Daily";
- **Hour:** Por fim, selecione o horário no qual ele será feito, neste exemplo, será às "12:30".

Save

Clique em [] para gravar as configurações.

Criação de Backup de Snapshot SFTP Semanal

À seguir, criaremos um *Backup* de *Snapshot* Semanal:

Edit Backup
X

General

* Name

* Devices

UTM 2.1 - 200.41 X

3 X

Devices Group

* Type

* Remote Storage

Number of Backup Retention

Percent Usage Retention

Schedule

* Schedule

* Weekday

* Hour

Cancel
Save

Backups - Create Backup

- **Name:** Neste exemplo nomearemos o *backup* como "Snapshot Backup - UTM 2.1 Group - Weekly - SFTP-01";
- **Device & Devices Group:** Usaremos o device "UTM 2.1 - 200.41";
- **Type:** Neste exemplo usaremos o tipo: "Snapshot";
- **Remote Storage:** Selecionaremos o "Storage_SFTP_01";
- **Number of Backup Retention:** Neste caso configuraremos para que haja retenção de 2 backups;
- **Percent usage retention:** Neste caso usaremos 20% do espaço do diretório;

- **Schedule:** O agendamento será diário, portanto selecionaremos a opção "Weekly";
- **Weekday:** Escolha o dia em que o *backup* será feito, neste caso "Monday";
- **Hour:** Por fim, selecione o horário no qual ele será feito, neste exemplo, será às 15:55.

Save

Clique em [] para gravar as configurações.

Criação de Backup de Snapshot SFTP Único

Por fim, criaremos um *Backup de Snapshot* único:

Edit Backup
X

General

* Name

Snapshot Backup - UTM 200.41 - Single Time - SFTP-01

* Devices

UTM 2.1 - 200.41 X

Devices Group

Select a group

* Type

Snapshot

* Remote Storage

Storage_SFTP_01

Number of Backup Retention

1

Percent Usage Retention

100

Schedule

* Schedule

Oneshot

* Date and time

08/03/2021 17:08

Cancel
Save

Backups - Create Backup

- **Name:** Neste exemplo nomearemos o *backup* como "Snapshot Backup - UTM 200.41 - Single Time - SFTP-01";
- **Device & Devices Group:** Usaremos o device "UTM 2.1 - 200.41";
- **Type:** Neste exemplo usaremos o tipo: "Snapshot";
- **Remote Storage:** Selecionaremos o "Storage_SFTP_01";
- **Number of Backup Retention:** Neste caso configuraremos para que haja retenção de 1 backups;
- **Percent usage retention:** Neste caso usaremos 100% do espaço do diretório;
- **Schedule:** Este será um snapshot único, portanto selecionaremos a opção "Oneshot";

- **Date and Time:** Escolha o dia e o horário em que o *backup* será feito, neste caso "08/03/2021 17:08".

Save

Clique em [] para gravar as configurações.

Ao finalizar todas as configurações, a tela estará como demonstrado abaixo:

Devices

Inventory Communities Templates Provisioning Backups

5 records

☐	Name	Last backup	Next backup	Progress	Status	Actions
☐	Snapshot Backup - UTM 2.1 Grou...	10/03/2021 12:31	11/03/2021 12:30	✓	Success	☐ ☐ ☐ ☐
☐	Snapshot Backup - UTM 2.1 Grou...	08/03/2021 15:56	16/03/2021 16:01	✓	Success	☐ ☐ ☐ ☐
☐	Snapshot Backup - UTM 200.41 - ...	08/03/2021 17:09	Unscheduled	✓	Success	☐ ☐ ☐ ☐
☐	System Backup - UTM 2.1 Group ...	10/03/2021 17:15	11/03/2021 16:02	✓	Success	☐ ☐ ☐ ☐
☐	System Backup - UTM 2.1 Group ...	08/03/2021 16:51	08/04/2021 16:00	✓	Success	☐ ☐ ☐ ☐

< 1 > 10 / page

Devices - Backups

Por fim, discutiremos a [validação](#) das configurações que efetuamos.

Backup de Devices - Validação das configurações

Para efetuar a validação do correto funcionamento das configurações de *backup*, basta conferir o *status* e o progresso dos *backups* na própria interface onde eles foram criados, segue um exemplo:

Devices

Inventory Communities Templates Provisioning Backups

5 records

	Name	Last backup	Next backup	Progress	Status	Actions
☐	Snapshot Backup - UTM 2.1 Grou...	11/03/2021 12:31	12/03/2021 12:30		Success	☐ ☐ ☐ ☐
☐	Snapshot Backup - UTM 2.1 Grou...	08/03/2021 15:56	16/03/2021 16:01		Success	☐ ☐ ☐ ☐
☐	Snapshot Backup - UTM 200.41 - ...	08/03/2021 17:09	Unscheduled		Success	☐ ☐ ☐ ☐
☐	System Backup - UTM 2.1 Group ...	11/03/2021 17:18	12/03/2021 16:02		Success	☐ ☐ ☐ ☐
☐	System Backup - UTM 2.1 Group ...	08/03/2021 16:51	08/04/2021 16:00		Success	☐ ☐ ☐ ☐

< 1 > 10 / page

Devices - Backups



Para mais informações sobre os componentes desta tela, consulte esta [página](#).

Além disso, as operações efetuadas pelos backups geram logs de auditoria, como demonstrado na imagem à seguir:

Administration

Administrators Users Profiles Auth Servers Identity Provider Audit Log

142 records

Date	User	Interface	Activity	IP	Actions
2021-03-10 20:58:57	Administrator	backups	Delete	192.168.200.2	☐
2021-03-10 20:58:03	Administrator	backups	Edit	192.168.200.2	☐
2021-03-10 20:16:21	Administrator	device-backups	Edit	192.168.200.2	☐
2021-03-10 19:12:49	Administrator	device-backups	Save	172.31.200.253	☐
2021-03-10 18:53:51	Administrator	device-backups	Delete	172.31.200.253	☐
2021-03-10 18:00:23	Administrator	backups	Edit	172.31.200.253	☐
2021-03-10 16:10:58	Administrator	device-backups	Edit	192.168.112.85	☐
2021-03-10 16:01:42	Administrator	device-backups	Save	192.168.112.21	☐
2021-03-10 16:01:13	Administrator	device-backups	Save	192.168.112.21	☐
2021-03-10 16:01:01	Administrator	device-backups	Save	192.168.112.21	☐

< 1 2 3 4 5 ... 15 > 10 / page

Administration - Audit Log



Para mais informações sobre os relatórios de auditoria, consulte esta [página](#).

Por fim, durante o processo de *backup* também é possível verificar mais detalhes na *CLI* usando o comando de [\[debug-backup\]](#).

```

admin >debug-backup
date="2021-03-10 16:02:03" device_id="4" backup_id="20" backup_name="System Backup - UTM 2.1 Group - Daily - NFS-01" device_type="firewal
l" action="backup" device_name="UTM 2.1 - 200.41" storage_name="Storage_NFS_01" storage_type="nfs" backup_type="system" status="running"
status_message="" service="backup_manager"
date="2021-03-10 16:02:03" device_id="5" backup_id="20" backup_name="System Backup - UTM 2.1 Group - Daily - NFS-01" device_type="firewal
l" action="backup" device_name="UTM Dev - 2.1.0" storage_name="Storage_NFS_01" storage_type="nfs" backup_type="system" status="running" s
tatus_message="" service="backup_manager"
date="2021-03-10 16:02:04" device_id="6" backup_id="20" backup_name="System Backup - UTM 2.1 Group - Daily - NFS-01" device_type="firewal
l" action="backup" device_name="UTM 2.1 - 200.1" storage_name="Storage_NFS_01" storage_type="nfs" backup_type="system" status="running" s
tatus_message="" service="backup_manager"
date="2021-03-10 16:08:10" device_id="5" backup_id="20" backup_name="System Backup - UTM 2.1 Group - Daily - NFS-01" device_type="firewal
l" action="backup" device_name="UTM Dev - 2.1.0" storage_name="Storage_NFS_01" storage_type="nfs" backup_type="system" status="downloadin
g" status_message="" service="backup_manager"

```

CLI - debug-backup

Para mais informações a respeito de backups de device, consulte esta [página](#).

Profiles

Nesta sessão é possível criar perfis para os serviços *Web Filter*, *Application Control*, *Threat Protection*, *Intrusion Prevention*, *SSL Inspection* e *SD-WAN* do s UTM.

A principal função destes perfis é possibilitar a administração dos serviços previamente citados em todos os dispositivos conectados através de um único ponto central.



Para maiores informações sobre cada configuração, consulte o manual do Blockbit UTM.

Para aplicar os perfis criados nesta sessão, acesse o [Device template](#) de um UTM 2.0 e após clicar no botão [], habilite os módulos desejados, feito



isso, acesse o módulo, clique no botão do **menu de ações** [], crie um serviço e no campo "profile" selecione o perfil que foi criado nesta sessão. Para mais informações, acesse [Device template](#).



Os *profiles* criados nesta aba não podem ser aplicados a UTM de versão 1.5 ou anterior.

Nestes casos, durante o processo de criação de um *device template* 1.5 será necessário criar as funções do perfil, diretamente no próprio *template*.

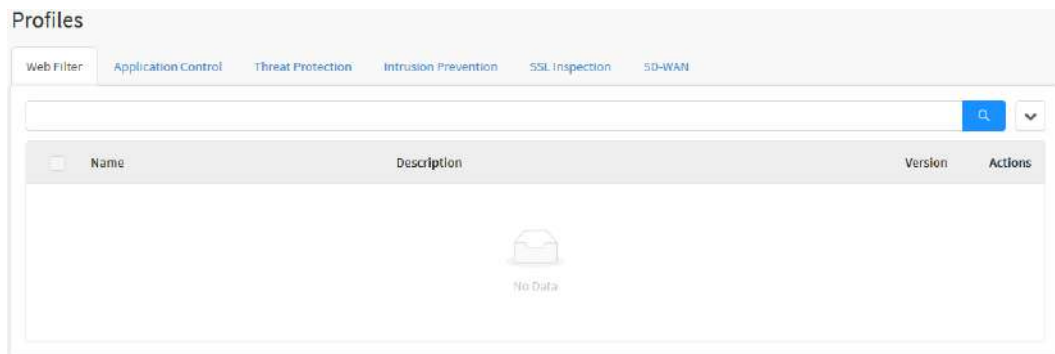
Para mais informações, acesse [Templates - Menu de ações - Create Template](#).

Para acessar a tela, basta selecionar o botão "Profiles".



Management – Profiles

A tela abaixo será exibida:



Profiles – Web Filter

A tela *Profiles* comporta as seguintes abas:

- [Web Filter](#);
- [Application Control](#);

- *Threat Protection*;
- *Intrusion Prevention*;
- *SSL Inspection*;
- *SD-WAN*.

A seguir, os componentes da aba *Web Filter* serão analisadas.

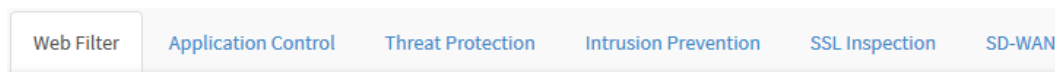
Aba Web Filter

O *Web Filter* funciona como uma segunda camada para filtrar a navegação dos usuários. É o responsável pelo filtro de conteúdo e só pode ser utilizado quando as requisições de acesso *Web HTTP/HTTPS* são repassadas por um servidor *Proxy*, antes de solicitar os dados ao servidor remoto, ele redireciona algumas informações da requisição (*url*, usuário e endereço *IP* do usuário) para o serviço de *Web Filter*.



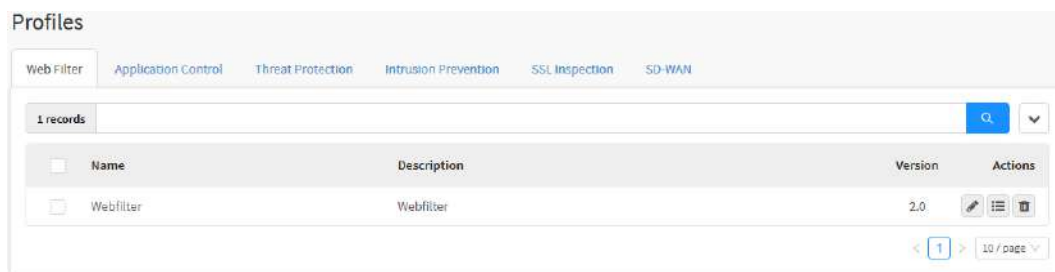
Para maiores informações sobre *Web Filter*, consulte o manual do Blockbit UTM.

Clique na aba "*Web Filter*".



Aba *Web Filter*

Surgirá a Tela de "*Web Filter*". Ela é composta pelas colunas "*Name*", "*Description*", "*Version*" e "*Actions*". Além disso, no topo direito da tela está localizada a [barra de busca](#) e o [menu de ações](#).



Profiles – Web Filter

A seguir, o [menu de ações](#) será analisado e posteriormente nos aprofundaremos no conteúdo das [colunas](#) do painel *Web Filter*.

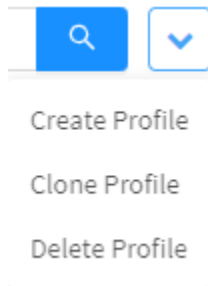
Web Filter - Menu de ações

No topo direito da tela temos o menu de ações:



Web Filter – Botão do Menu de Ações

Ao clicar neste botão o menu abaixo é exibido:



Web Filter – Menu de Ações

O menu é composto das seguintes opções:

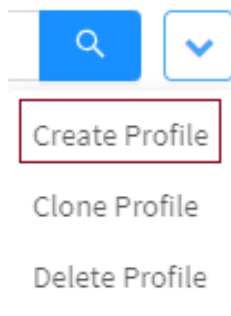
- [Create Profile](#);
- [Clone Profile](#);
- [Delete Profile](#).

A seguir cada opção do menu de ações será detalhada.

Web Filter - Menu de Ações - Create Profile

Através da opção "Create Profile" é possível criar um novo perfil de *Web Filter*. Para acessar, clique no **menu de ações** [].

1. Clique na opção "Create Profile";



Web Filter - Create Profile

2. A tela "Create Profile" será exibida. Preencha-a com os seguintes dados:

Web Filter – Create Profile

- **Name:** Nome do *profile*. Ex.: *Webfilter*;
- **Description:** Descrição do *profile*. Ex.: *Webfilter*;
- **Version:** Define a versão que será utilizada no *profile*. É importante que a versão seja igual a do UTM;



ATENÇÃO: Caso a versão do perfil seja diferente da do UTM, eles não serão compatíveis.

Sempre crie perfis com a mesma versão dos UTMs nos quais eles serão aplicados.

Cancel

Save

Caso deseje cancelar clique no botão **Cancel**[]. Para concluir a criação do pacote de política clique no botão **Save**[].



Profile saved successfully

Profile saved successfully

O perfil foi criado com sucesso.

À seguir iremos analisar como [clonar um perfil de Web Filter](#).

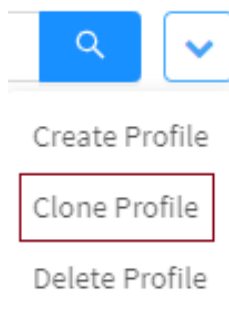
Web Filter - Menu de Ações - Clone Profile

Através da opção "Clone Profile" é possível clonar um novo perfil de Web Filter. Para acessar, clique no **menu de ações** [].



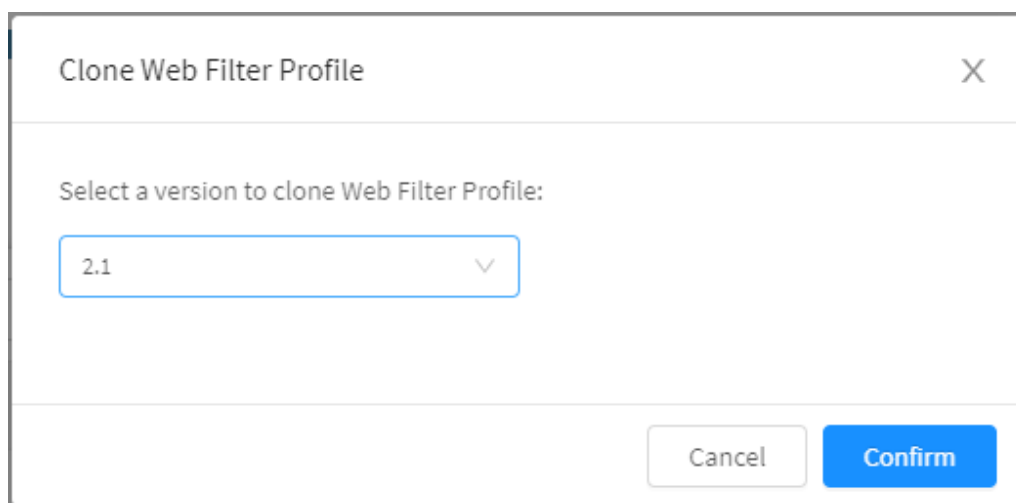
Web Filter - Main Screen

1. Clique na opção "Clone Profile";



Web Filter - Clone Profile

2. A tela "Clone Profile" será exibida. Apenas confirme clique em "Confirm":



Web Filter – Clone Profile

A seguinte tela aparecerá:



Também é possível clonar um perfil de Web Filter clicando no botão Clone[].

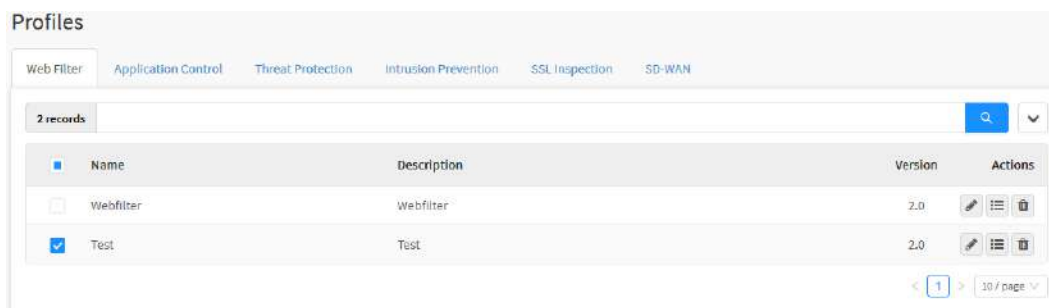
O perfil será clonado com sucesso.

À seguir iremos analisar como [remover um perfil de Web Filter](#).

Web Filter - Menu de ações - Delete Profile

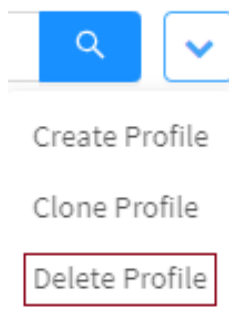
Através do botão "Delete Profile" é possível deletar os *Profiles* selecionados. Para deletar pelo Menu de ações, siga os seguintes passos:

1. Selecione qual(is) *Profile*(s) deseja deletar. Para selecionar, basta clicar com o *mouse* no *checkbox* que fica localizado ao lado do *Name*. Nos *profiles* selecionados o *checkbox* mudará da cor cinza para azul []. Ex.: *Test*;



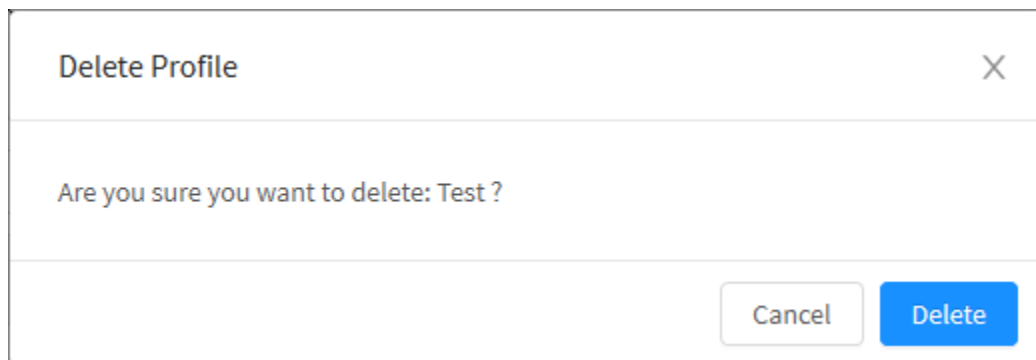
Web Filter – Seleção dos *Profiles* para deletar

2. Entre no **menu de ações** [] e clique na opção "Delete Profile".

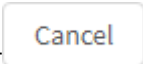
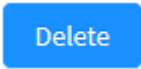


Web Filter – Delete Profiles

3. Surgirá a mensagem de notificação questionando se deseja realmente deletar os *Profiles* selecionados:



Web Filter – Mensagem de deleção do *Profile*

Caso desejar cancelar clique no botão **Cancel**. Para concluir, clique no botão **Delete**.

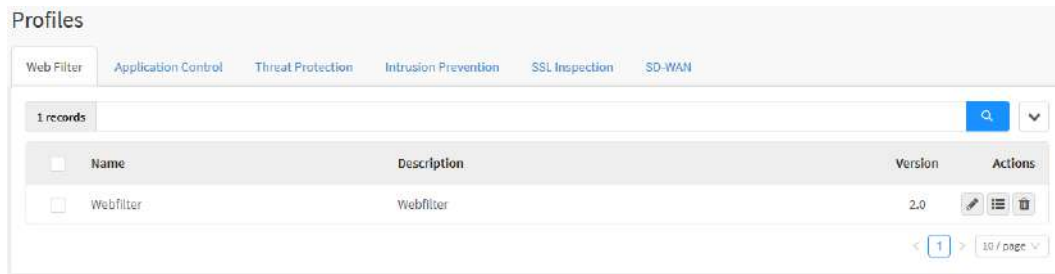
 **Profile deleted successfully!**
Profile deleted successfully

Após realizar esses procedimentos, os *profiles* terão sido deletados com sucesso.

À seguir iremos analisar o conteúdo das [colunas](#).

Web Filter - Colunas

A seguir explicaremos cada coluna da aba *Web Filter*:



Profiles				
Web Filter Application Control Threat Protection Intrusion Prevention SSL Inspection SD-WAN				
1 records				
☐	Name	Description	Version	Actions
☐	Webfilter	Webfilter	2.0	  

Profiles – Web Filter

A seguir explicaremos cada coluna:

- **Caixa de Seleção** [☐]: Seleciona o *profile*;
- **Name**: Apresenta o nome do *profile* cadastrado;
- **Description**: Apresenta a descrição do *profile* cadastrado;
- **Version**: Apresenta a versão na qual o *profile* foi criado. É de extrema importância criar *profiles* da mesma versão que o UTM, caso contrário, o *profile* não será compatível;
- **Actions**: A coluna “Actions” é composta por vários botões:
 - **Botão Edit** []: Permite editar as configurações do *profile* adicionado na opção *Create Profile* do menu de ações;
 - **Botão List Profiles** []: Permite visualizar, editar e adicionar opções mais específicas do *profile*, para mais informações, cheque [Web Filter - List Profile](#);
 - **Botão Delete** []: Deleta o *profile*.

A seguir as funções do botão [List Profiles](#) serão explicadas e exemplificadas.

Web Filter - List Profile

Ao clicar no botão **detalhar**  é possível configurar o *profile*;

Neste painel é possível efetuar as configurações gerais, configurar filtros e quotas que serão utilizados nesse perfil.



Para maiores informações sobre *Web Filter*, consulte o manual do Blockbit UTM.

Edit Profile

General

*

Name

Webfilter

Description

Webfilter

Search

☐ Restrict login domains for Google Apps

☐ Enforce Safe Search for Google, Bing, Yahoo

Filters

☐ Web categories

☐ File Filter

Surfing Quotas

☐ Maximum Time

☐ Maximum Download Size

Hours per day

MB

☐ Maximum Traffic

☐ Maximum Upload Size

MB per day

MB

Cancel

Save

Web Filter - Edit Profile

General

Em "General" temos as seguintes caixas de texto:



General

* Name

Webfilter

Description

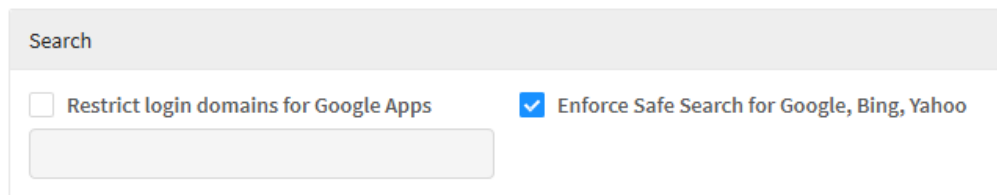
Webfilter

Web Filter – General

- **Name:** Definir um nome para o perfil. Ex.: *Webfilter*;
- **Description:** Definir uma descrição para o perfil. Ex.: *Webfilter*.

Search

Em "Search" é possível gerenciar o acesso aos serviços de busca:



Search

☐ Restrict login domains for Google Apps

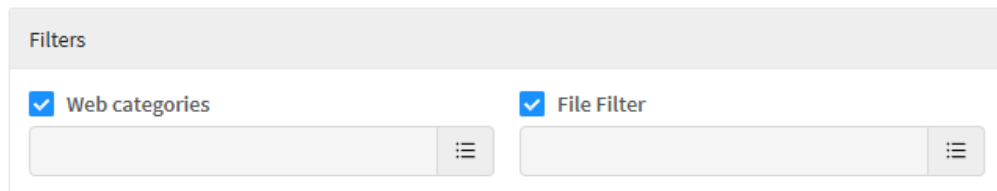
☒ Enforce Safe Search for Google, Bing, Yahoo

Web Filter - Search

- **Restrict login domains for Google Apps** ☒: Esta opção permite controlar quais os domínios efetuarão o acesso aos *Apps* do *Google*;
- **Enforce Safe Search for Google, Bing, Yahoo** ☒: Esta caixa de checagem força a ativação do *Safe Search* nos mecanismos de busca.

Filters

Em "Filters" as seguintes opções estão disponíveis:



Filters

☒ Web categories

☒ File Filter

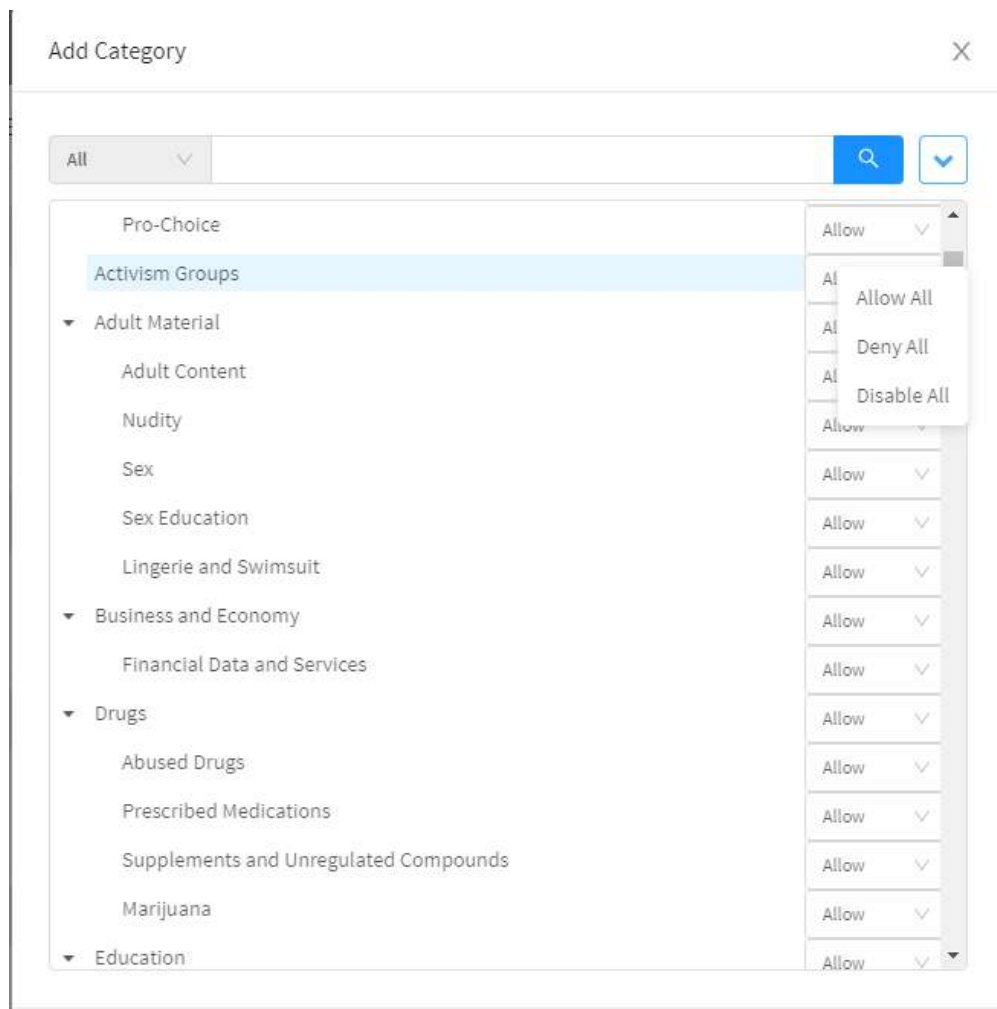
Webfilter - Filters

- **Web categories** []: Permite selecionar as categorias *Web* para aplicar filtros de “Bloqueio” ou “Exceção” ao conjunto de políticas aplicadas.

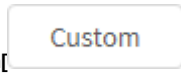
Para selecionar as categorias, clique no botão [], escolha as categorias desejadas e depois selecione **Allow**, **Block** ou **Disable**. No menu

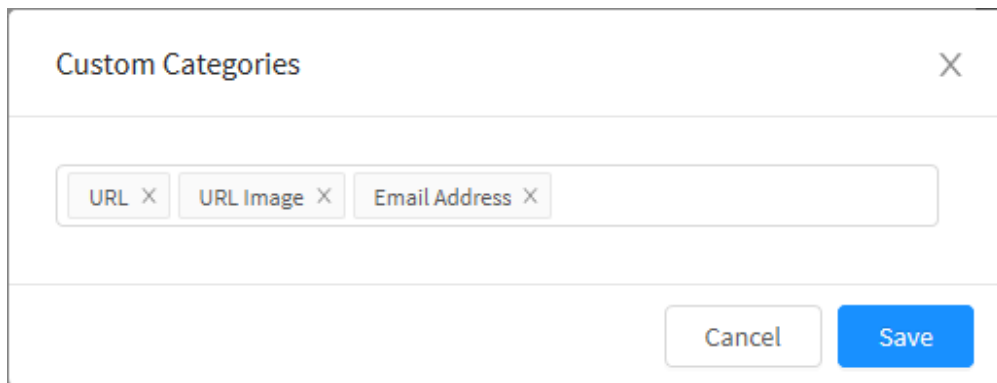
de ações [], também é possível aplicar alguma destas opções em todas as categorias em **Allow All**, **Block All** e **Disable All** para desabilitá-las. Segue uma breve descrição da função de cada ação:

- **Allow:** O acesso a *URLs* classificadas com esta categoria é permitido;
- **Block:** O acesso a *URLs* classificadas com esta categoria é bloqueado;
- **Disable:** Esta categoria é desabilitada, isso significa que o *Web Filter* irá ignorá-la e considerará apenas as *URLs* em categorias permitidas ou bloqueadas.

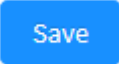


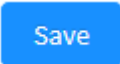
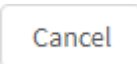
Webfilter - Add Category

Também é possível adicionar categorias customizadas clicando no botão **Custom** [];



Web Filter - Add Category - Custom

Clique no campo e selecione a categoria desejada, neste campo estarão disponíveis os objetos do tipo [dictionaries](#), os objetos selecionados serão adicionados como tags. Por fim, clique no botão **Cancel**  para sair dessa janela ou clique no botão **Save**  para salvar.

Para finalizar a adição das categorias, clique no botão **Save**  para salvar ou clique no botão **Cancel**  para sair desta janela.

- **File Filter** : Permite selecionar os tipos de arquivo adicionados em [Objects - Contents](#) para aplicar filtros ao conjunto de políticas aplicadas. Para selecionar os objetos, clique no botão , e habilite as caixas de checagem desejadas. No menu de ações, também é possível clicar em **Select All** para marcar tudo ou **Deselect All** para desmarcar todas as categorias

Add FileFilter

All

Q

☒ Item

☐ ActiveX

☐ Compressed

☒ Executables

☐ Image group

☐ Images

☐ Javascript

☐ Multimedia

☐ Office

<

1

>

Cancel

Save

Web Filter - Add File Filter

Clique no botão **Cancel** para Cancelar. Clique no botão **Save** para salvar.

Surfing Quotas

Em "Surfing Quotas" o seguinte painel é exibido:

Surfing Quotas

☐ Maximum Time	☐ Maximum Download Size
Hours per day	MB
☐ Maximum Traffic	☐ Maximum Upload Size
MB per day	MB

Web Filter - Surfing Quotas

- ☒ **Maximum Time:** Permite configurar uma quota de tempo em minutos ou horas por dia.

☒ Maximum Time

Hours per day

☐ Maximum Traffic

Minutes per day

Hours per day

Web Filter – Maximum Time

- ☒ **Maximum Traffic:** Permite configurar uma quota de tráfego em MB por dia.

☒ Maximum Traffic

MB per day

MB per day

Web Filter – Maximum Traffic

- ☒ **Max Download Size:** Permite configurar o tamanho máximo para *download*, em MB ou GB.

☒ Maximum Download Size

MB

☐ Maximum Upload Size

MB

GB

Web Filter - Maximum Download Size

- ☒ **Max Upload Size:** Permite configurar o tamanho máximo para *upload*, em MB ou GB.

☒ **Maximum Upload Size**

MB

MB

GB

Web Filter - Maximum Upload Size



As configurações efetuadas podem ser adicionadas a uma [política](#) no menu *Inspection* na opção *Web Filter*.

Cancel

Save

Após finalizar todas as configurações, clique no botão **Cancel** para voltar para o painel *Profiles* ou clique no botão **Save** para salvar.

Para mais informações a respeito da aba *Web Filter*, consulte esta [página](#).

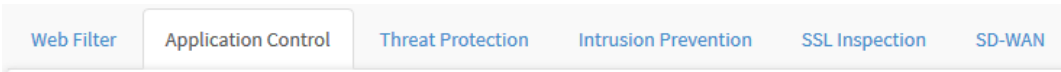
À seguir iremos detalhar o conteúdo da aba [Application Control](#).

Aba Application Control

Através do recurso *Application Control* é possível controlar caso os usuários terão permissão de acesso à determinadas aplicações ou caso não estarão autorizados a utilizar alguma aplicação. As aplicações são divididas entre categorias possibilitando que o administrador determine de forma específica o acesso de cada item.

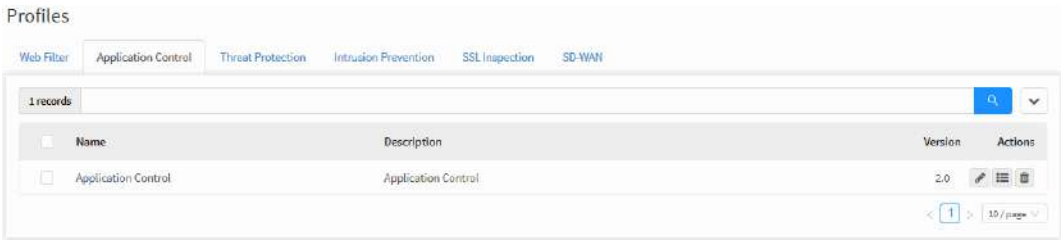
 Para maiores informações sobre *Application Control*, consulte o manual do Blockbit UTM.

Clique na aba “*Application Control*”.



Aba *Application Control*

Surgirá a Tela de “*Application Control*”. Ela é composta pelas colunas “*Name*”, “*Description*”, “*Type*”, “*Version*” e “*Actions*”. Além disso, no topo direito da tela está localizada a [barra de busca](#) e o [menu de ações](#).



Profiles – *Application Control*

A seguir, o [menu de ações](#) será analisado e posteriormente nos aprofundaremos no conteúdo das [colunas](#) do painel *Application Control*.

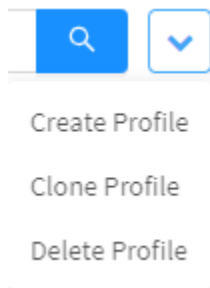
Application Control - Menu de ações

No topo direito da tela temos o menu de ações:



Application Control – Botão do menu de ações.

Ao clicar neste botão o menu abaixo é exibido:



Application Control – Menu de ações.

O menu é composto das seguintes opções:

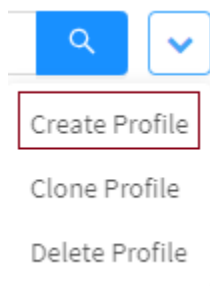
- [Create Profile](#);
- [Clone Profile](#);
- [Delete Profile](#).

A seguir cada opção do menu de ações será detalhada.

Application Control - Menu de ações - Create Profile

Através da opção "Create Profile" é possível criar um novo perfil de *Application Control*. Para acessar, clique no **menu de ações** [].

1. Clique na opção "Create Profile";



Application Control - Criar perfil

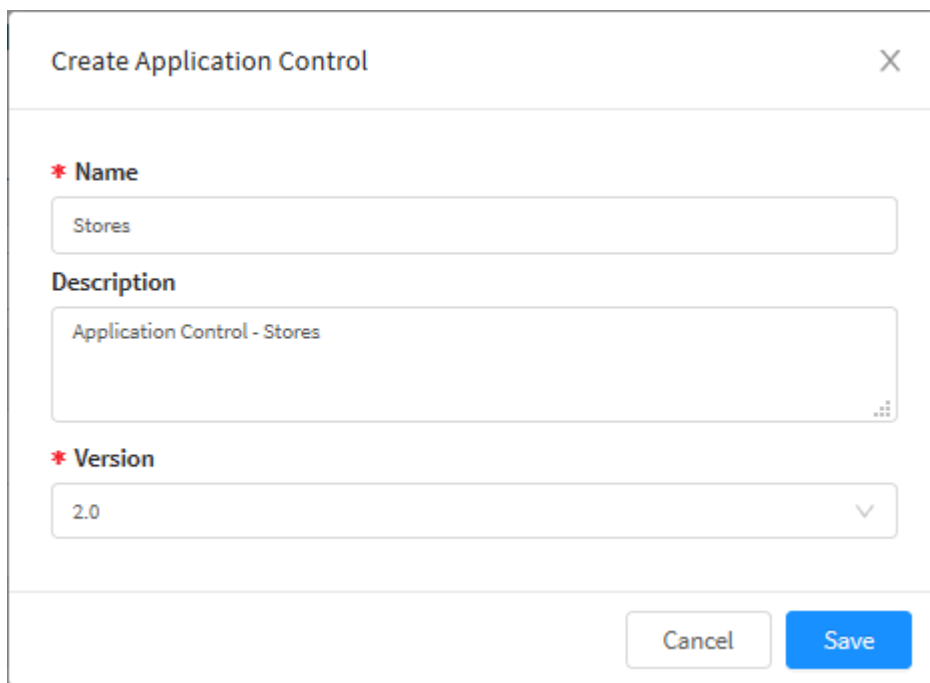
2. A tela "Create Application Control" será exibida. Preencha-a com os seguintes dados:

- **Name:** Nome do *profile*. Ex.: Stores;
- **Description:** Descrição do *profile*. Ex.: Application Control - Stores;
- **Version:** Define a versão que será utilizada no *profile*. É importante que a versão seja igual a do UTM;

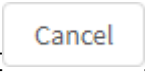
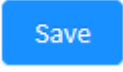


ATENÇÃO: Caso a versão do perfil seja diferente da do UTM, eles não serão compatíveis.

Sempre crie perfis com a mesma versão dos UTMs nos quais eles serão aplicados.

A screenshot of a web form titled "Create Application Control" with a close button (X) in the top right corner. The form contains three main sections: 1. "Name" with a red asterisk, followed by a text input field containing the word "Stores". 2. "Description", followed by a larger text area containing "Application Control - Stores". 3. "Version" with a red asterisk, followed by a dropdown menu showing "2.0". At the bottom right of the form are two buttons: a light gray "Cancel" button and a blue "Save" button.

Application Control – Criar perfil de Application Control.

Caso deseje cancelar clique no botão **Cancel** []. Para concluir a criação do pacote de política clique no botão **Save** [].

 Profile saved successfully

O perfil foi salvo com sucesso.

A seguir, veremos como [Clonar um Perfil](#).

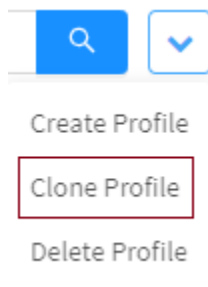
Application Control - Menu de ações - Clone Profile

Através da opção "Clone Profile" é possível criar um novo perfil de *Application Control*. Para acessar, clique no **menu de ações** [].



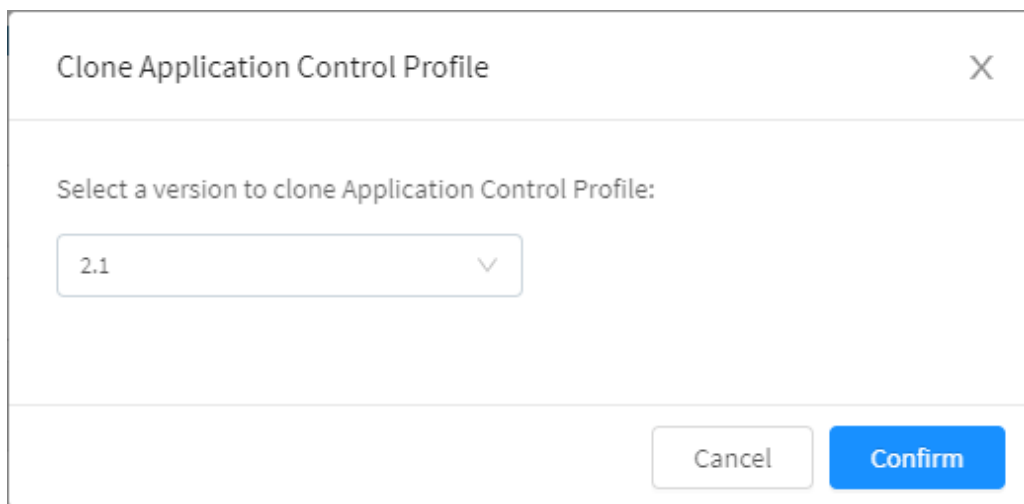
Application Control - Main screen

1. Clique na opção "Clone Profile";



Application Control - Clone Profile

2. Para confirmar, clique em "Confirm":



Application Control – Clone Application Control Profile.



Application Control - Perfil clonado com sucesso.

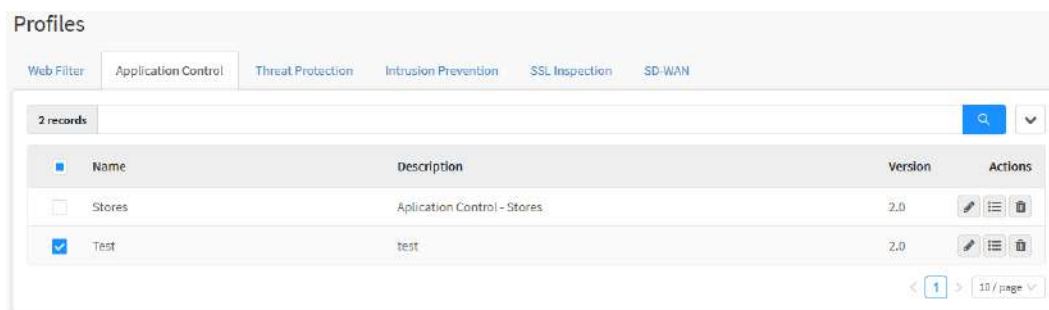
Também é possível clonar um perfil clicando no botão Clone [].

A seguir veremos como [Deletar um Perfil](#).

Application Control - Menu de ações - Delete Profile

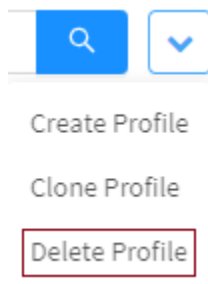
Através do botão "Delete Profile" é possível deletar os *Profiles* selecionados. Para deletar pelo *Menu de Ações*, siga os seguintes passos:

1. Selecione qual(is) *Profile(s)* deseja deletar. Para selecionar, basta clicar com o *mouse* no *checkbox* que fica localizado ao lado do *Name*. Nos *profiles* selecionados o *checkbox* mudará da cor cinza para azul []. Ex.: *Test*;



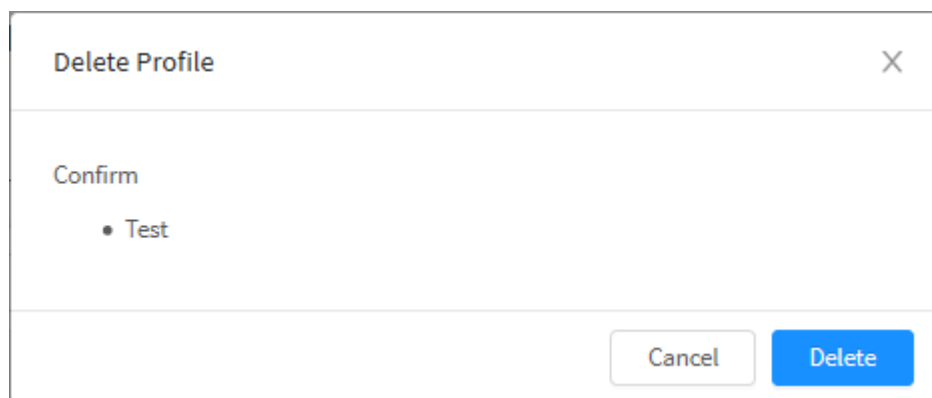
Application Control – Seleção dos *Profiles* para deletar

2. Entre no **menu de ações** [] e clique na opção "Delete Profile".



Application Control – Delete *Profiles*.

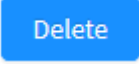
3. Surgirá a mensagem de notificação questionando se deseja realmente deletar os *Profiles* selecionados:



Application Control – Mensagem de confirmação de remoção de perfil

Cancel

Delete

Caso desejar cancelar clique no botão **Cancel**[]. Para concluir, clique no botão **Delete**[].



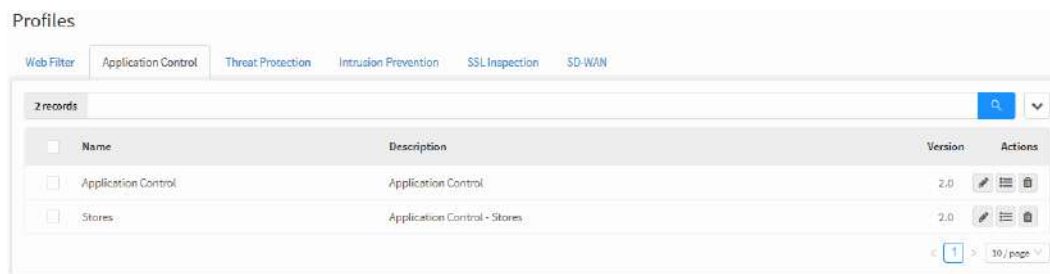
Profile removed successfully

O perfil foi removido com sucesso.

A seguir analisaremos o [menu Colunas](#).

Application Control - Colunas

A seguir explicaremos cada coluna da aba *Application Control*:



The screenshot shows the 'Profiles' section with the 'Application Control' tab selected. It displays a table with 2 records. The table has columns for Name, Description, Version, and Actions. The records are 'Application Control' and 'Stores', both with version 2.0. The Actions column contains icons for Edit, List Profiles, and Delete.

☐	Name	Description	Version	Actions
☐	Application Control	Application Control	2.0	  
☐	Stores	Application Control - Stores	2.0	  

Profiles – Application Control

A seguir explicaremos cada coluna:

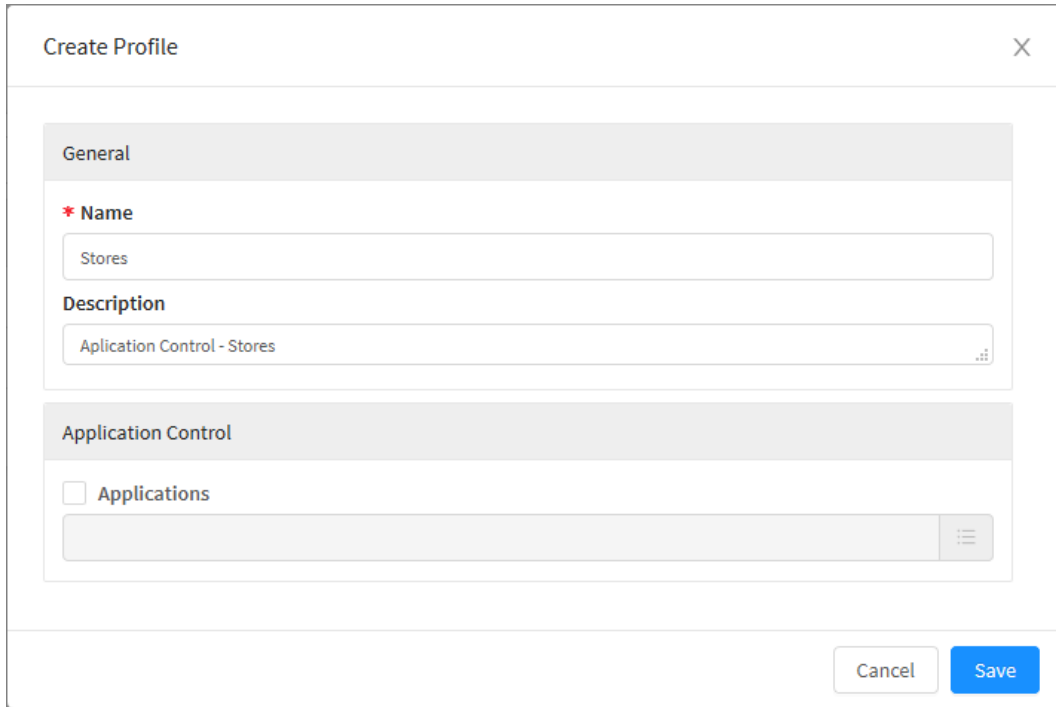
- **Caixa de Seleção** [☐]: Seleciona o *profile*;
- **Name**: Apresenta o nome do *profile* cadastrado;
- **Description**: Apresenta a descrição do *profile* cadastrado;
- **Version**: Apresenta a versão na qual o *profile* foi criado. É de extrema importância criar *profiles* da mesma versão que o UTM, caso contrário, o *profile* não será compatível;
- **Actions**: A coluna "Actions" é composta por vários botões:
 - **Botão Edit** []: Permite editar as configurações do *profile* adicionado na opção *Create Profile* do menu de ações;
 - **Botão List Profiles** []: Permite visualizar, editar e adicionar opções mais específicas do *profile*, para mais informações, cheque [Application Control - Menu de ações - Create Profile](#);
 - **Botão Delete** []: Deleta o *profile*.

A seguir as funções do botão [List Profiles](#) serão explicadas e exemplificadas.

Application Control - List Profile

Ao clicar no botão **detalhar**  é possível configurar o *profile*;

Neste painel é possível efetuar as configurações gerais e definir as permissões das aplicações utilizadas nesse perfil.



Application Control - Create Profile

General

Em "General" temos as seguintes caixas de texto:



Application Control – General

- **Name:** Definir um nome para o perfil. Ex.: *Load Balance*;
- **Description:** Definir uma descrição para o perfil. Ex.: *SD-WAN - Load Balance*.

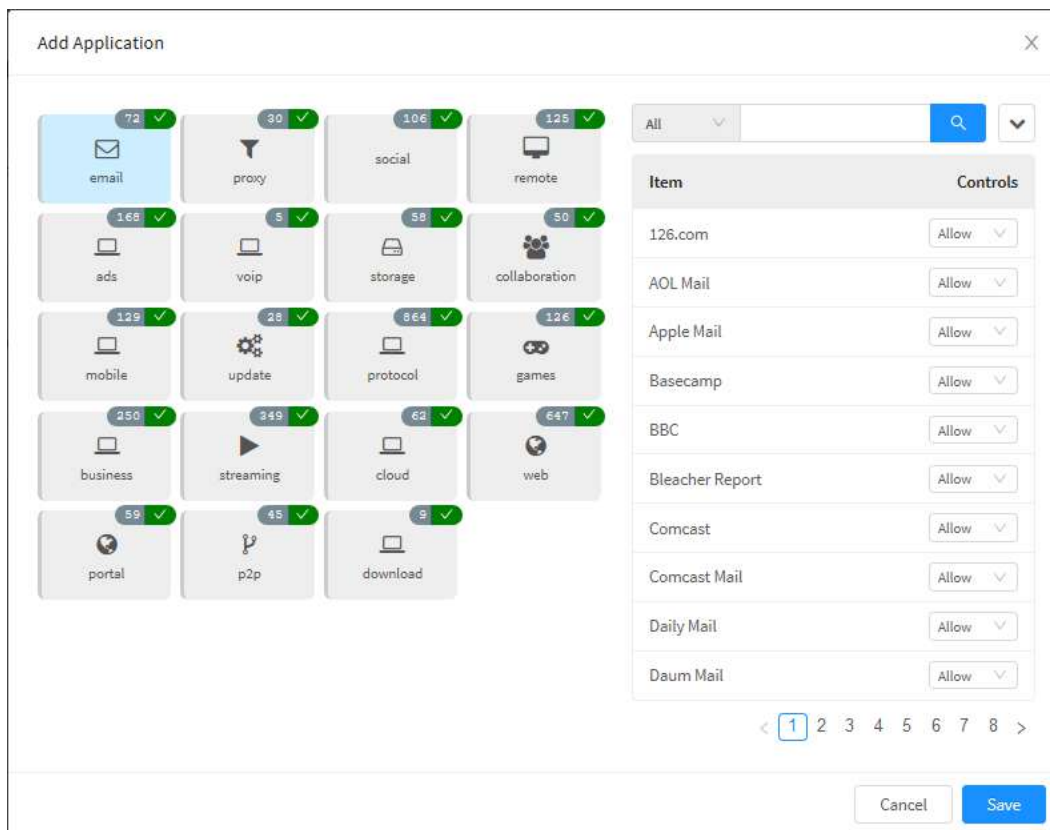
Application Control

Em "Application Control" são determinadas as aplicações cujo acesso será permitido ou negado:



Application Control - Applications

Para editar as aplicações, certifique-se que o **checkbox** ☒ está habilitado, depois clique no botão **list applications**  para administrar as permissões.

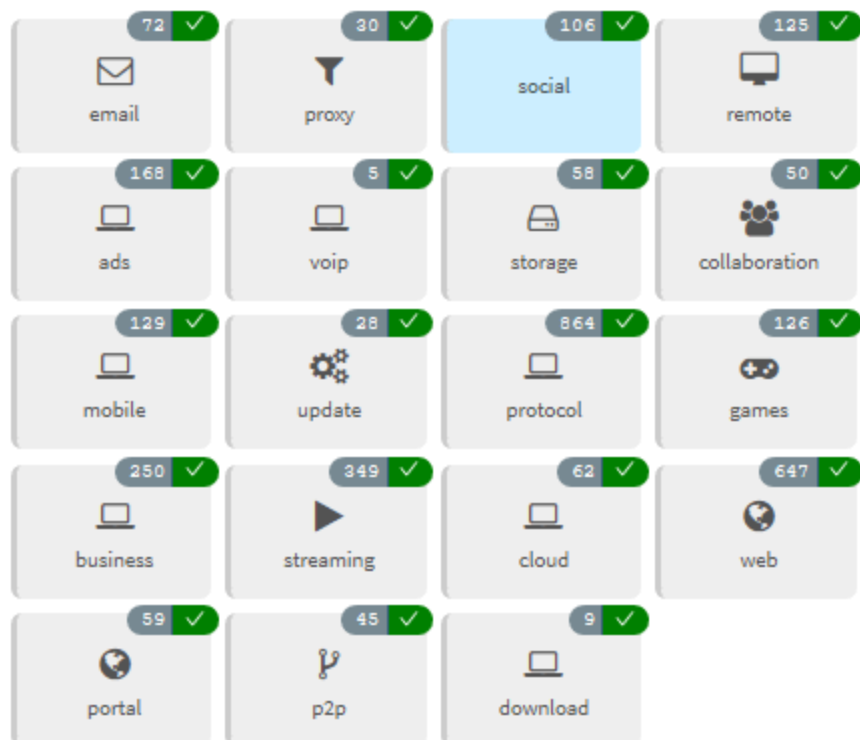


Application Control - Add Application

Ao selecionar um dos ícones à esquerda, as *aplicações* serão exibidos no painel à direita.

No exemplo abaixo, iremos desabilitar o acesso de algumas aplicações de *chat*.

Para tanto, selecione a categoria desejada, neste exemplo, selecionaremos a opção "social":



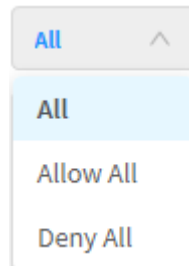
Application Control - Add Application - Opção "social" selecionada

Determine a aplicação desejada e na caixa de seleção, escolha a opção **Deny** [], conforme exemplificado na imagem abaixo:

Item	Controls
Eventbrite	Allow ▾
Facebook Apps	Allow ▲
Facebook Like	Allow
Family Tree	Deny
Fazed	Disable
Facebook Comment	Allow ▾
Facebook event	Allow ▾
Facebook Message	Allow ▾
Facebook Status Update	Allow ▾
Facebook search	Allow ▾

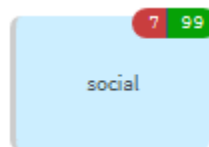
Application Control - Add Application - Itens negados

Caso seja necessário fazer uma configuração em todos os itens de uma categoria, basta selecionar a opção desejada no **menu de ações** [] ou na caixa de seleção demonstrada abaixo:

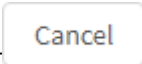


Application Control - Add Application - All, Allow All e Deny All

Ao ter uma aplicação com a permissão negada, a quantia de aplicações negadas e permitidas será exibida sob o ícone da sua respectiva categoria à esquerda, conforme demonstrado abaixo:



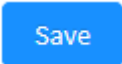
Application Control - Add Application - 7 itens negados e 99 permitidos

Por fim, caso deseje cancelar clique no botão **Cancel** []. Para concluir a edição das aplicações clique no botão **Save** [].

Após, ter efetuado os processos anteriores, um resumo de todas as aplicações permitidas e negadas serão exibidas no campo Applications, conforme exemplificado abaixo:



Application Control - Applications - Applications allowed and denied

Para concluir este processo, basta clicar no botão **Save** [] novamente.

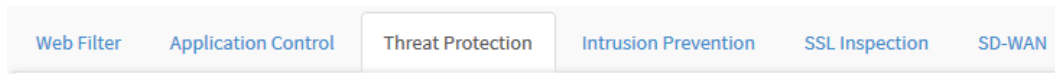
 **Profile updated successfully**
Profile updated successfully

O perfil foi criado com sucesso.

Aba Threat Protection

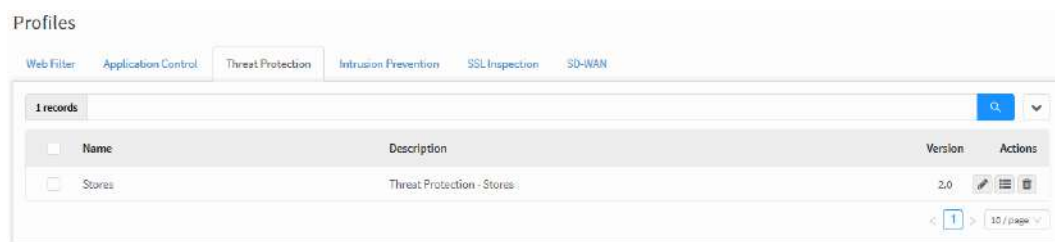
Com os perfis de *Threat Protection*, é possível analisar arquivos para inspeção de *malware* e bloqueio de ameaças. Esta seção irá demonstrar como criar perfis que posteriormente, serão instalados nas políticas.

Clique na aba “*Threat Protection*”.



Aba *Threat Protection*

Surgirá a Tela de “*Threat Protection*”. Ela é composta pelas colunas “*Name*”, “*Description*”, “*Version*” e “*Actions*”. Além disso, no topo direito da tela está localizada a [barra de busca](#) e o [menu de ações](#).



Profiles – *Threat Protection*

A seguir, o [menu de ações](#) será analisado e posteriormente nos aprofundaremos no conteúdo das [colunas](#) do painel *Threat Protection*.

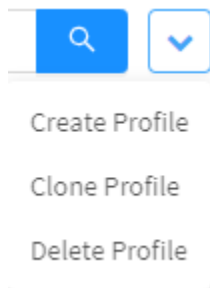
Threat Protection - Menu de ações

No topo direito da tela temos o menu de ações:



Threat Protection – Botão do menu de ações.

Ao clicar neste botão o menu abaixo é exibido:



Threat Protection – Menu de ações

O menu é composto das seguintes opções:

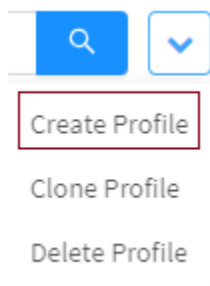
- [Create Profile](#);
- [Clone Profile](#);
- [Delete Profile](#).

A seguir cada opção do menu de ações será detalhada.

Threat Protection - Menu de ações - Create Profile

Através da opção "Create Profile" é possível criar um novo perfil de *Threat Protection*. Para acessar, clique no **menu de ações** [].

1. Clique na opção "Create Profile";



Threat Protection - Create Profile

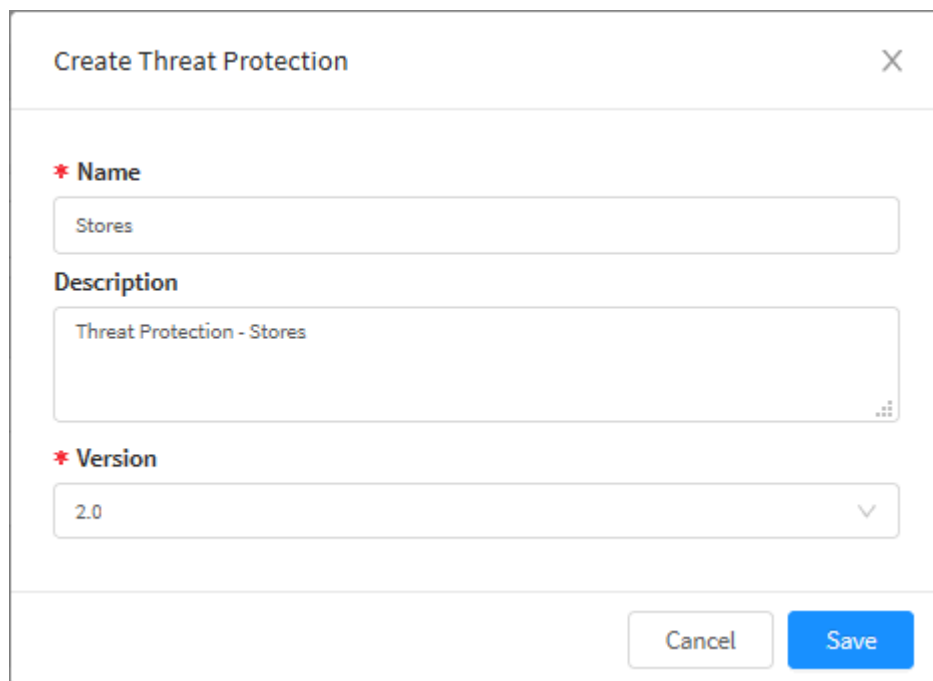
2. A tela "Create Threat Protection" será exibida. Preencha-a com os seguintes dados:

- **Name:** Nome do *profile*. Ex.: Stores;
- **Description:** Descrição do *profile*. Ex.: Application Control - Stores;
- **Version:** Define a versão que será utilizada no *profile*. É importante que a versão seja igual a do UTM;



ATENÇÃO: Caso a versão do perfil seja diferente da do UTM, eles não serão compatíveis.

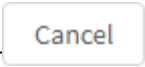
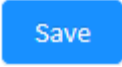
Sempre crie perfis com a mesma versão dos UTMs nos quais eles serão aplicados.

A screenshot of a web form titled 'Create Threat Protection'. The form has three main sections: 'Name' with a text input field containing 'Stores'; 'Description' with a text input field containing 'Threat Protection - Stores'; and 'Version' with a dropdown menu showing '2.0'. At the bottom right, there are two buttons: 'Cancel' and 'Save'. The form is enclosed in a light gray border with a close button (X) in the top right corner.

Threat Protection – Create Threat Protection

Cancel

Save

Caso deseje cancelar clique no botão **Cancel**[]. Para concluir a criação do pacote de política clique no botão **Save**[].



Profile saved successfully

Profile saved successfully

O perfil foi criado com sucesso.

A seguir veremos como [Clonar um Perfil](#).

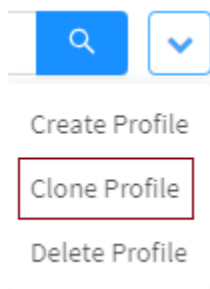
Threat Protection - Menu de ações - Clone Profile

Através da opção "Clone Profile" é possível clonar um perfil de Threat Protection. Para acessar, clique no **menu de ações** [].

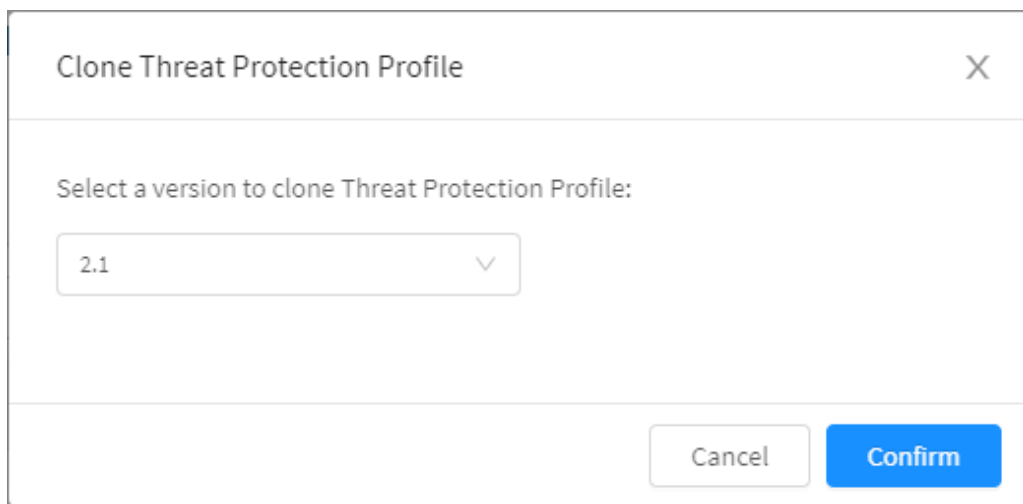


Threat Protection - Main Screen

1. Clique na opção "Clone Profile";



2. Para confirmar clique em "Confirm":



Threat Protection - Clone confirmation screen.



Threat Protection - Perfil clonado com sucesso.

Também é possível clonar um perfil clicando no botão Clone [].

A seguir, veremos como [apagar um Perfil](#).

Threat Protection - Menu de Ação - Delete Profile

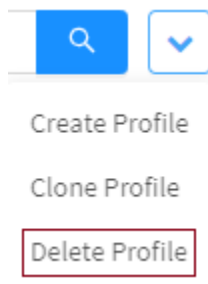
Através do botão "Delete Profile" é possível deletar os *Profiles* selecionados. Para deletar pelo menu de ações, siga os seguintes passos:

1. Selecione qual(is) *Profile*(s) deseja deletar. Para selecionar, basta clicar com o *mouse* no *checkbox* que fica localizado ao lado do *Name*. Nos *profiles* selecionados o *checkbox* mudará da cor cinza para azul []. Ex.: *Test*;



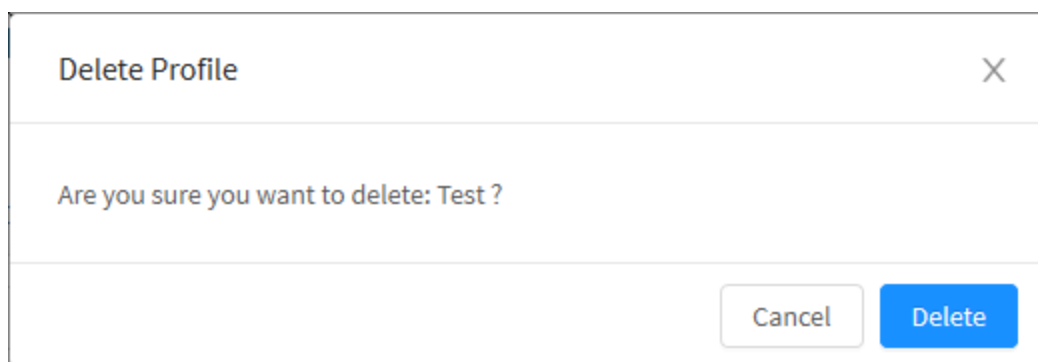
Threat Protection – Seleção dos *Profiles* para deletar

2. Entre no **menu de ações** [] e clique na opção "Delete Profiles".

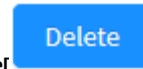
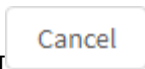


Threat Protection – Delete Profiles.

3. Surgirá a mensagem de notificação questionando se deseja realmente deletar os *Profiles* selecionados:



Threat Protection – Mensagem se deseja deletar os *Profiles*



Caso desejar cancelar clique no botão **Cancel**]. Para concluir, clique no botão **Delete**].



Profile removed successfully

Profile removed successfully

Após realizar esses procedimentos, os *profiles* terão sido deletados com sucesso.

A seguir, analisaremos o [menu Colunas](#).

Threat Protection - Colunas

A seguir explicaremos cada coluna da aba *Threat Protection*:

Profiles

Web Filter

Application Control

Threat Protection

Intrusion Prevention

SSL Inspection

SD-WAN

1 records

☐ Name	Description	Version	Actions
☐ Threat Protection	Threat Protection	2.0	

<

1

>

10 / page

Profiles – Threat Protection

A seguir explicaremos cada coluna:

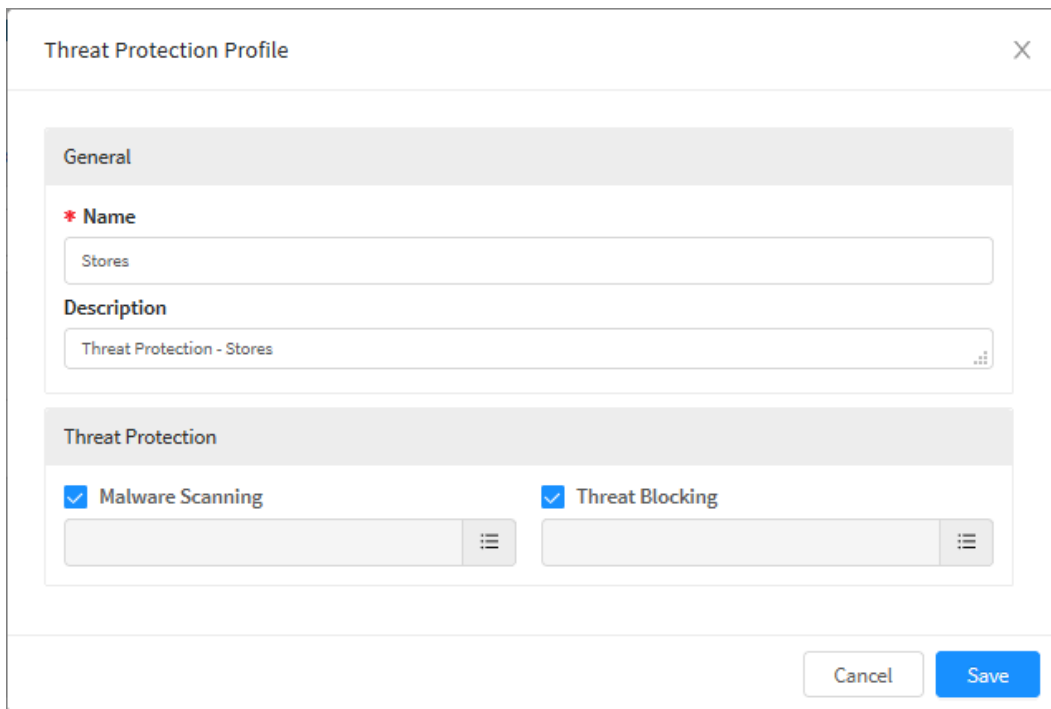
- **Caixa de Seleção** []: Seleciona o *profile*;
- **Name**: Apresenta o nome do *profile* cadastrado;
- **Description**: Apresenta a descrição do *profile* cadastrado;
- **Version**: Apresenta a versão na qual o *profile* foi criado. É de extrema importância criar *profiles* da mesma versão que o UTM, caso contrário, o *profile* não será compatível;
- **Actions**: A coluna “Actions” é composta por vários botões:
 - **Botão Edit** []: Permite editar as configurações do *profile* adicionado na opção *Create Profile* do menu de ações;
 - **Botão List Profiles** []: Permite visualizar, editar e adicionar opções mais específicas do *profile*, para mais informações, cheque [Threat Protection - Menu de ações - Create Profile](#);
 - **Botão Delete** []: Deleta o *profile*.

A seguir as funções do botão [List Profiles](#) serão explicadas e exemplificadas.

Threat Protection - List Profile

Ao clicar no botão **detalhar**  é possível configurar o *profile*;

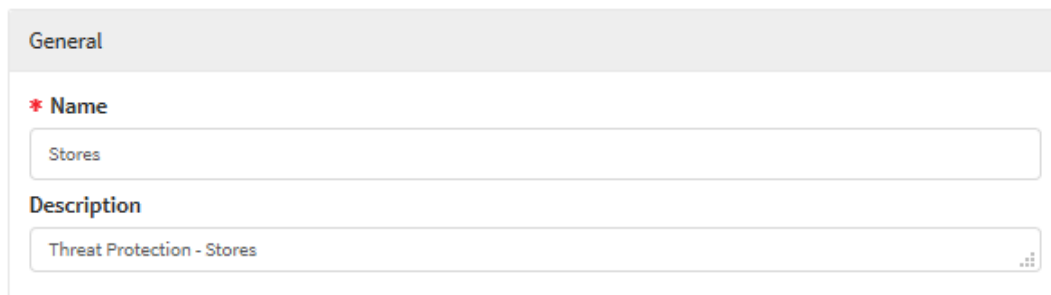
Neste painel é possível efetuar as configurações gerais do perfil, acionar *scan de malwares* e bloqueio de ameaças.



Threat Protection - Profile

General

Em "*General*" temos as seguintes caixas de texto:

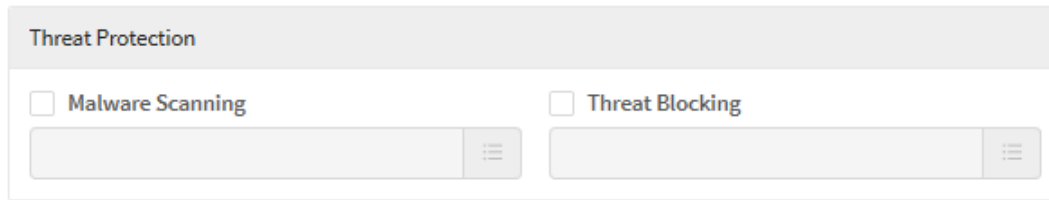


Threat Protection – General

- **Name:** Definir um nome para o perfil. Ex.: *Threat Protection*;
- **Description:** Definir uma descrição para o perfil. Ex.: *Threat Protection*.

Threat Protection

Em "Threat Protection" é determinado o escaneamento de *malware* e o bloqueio de ameaças.



Threat Protection

☒ Malware Scanning

☐ Threat Blocking

Threat Protection - Threat Protection

A seguir, analisaremos em detalhes estes dois campos.

Malware Scanning

Para adicionar o *Malware Scanning*, certifique-se que o **checkbox**  está habilitado, depois clique no botão **list applications**  o seguinte painel, será exibido:

Add Malware Scanning

All

☐

Item

☐

ActiveX

☐

Compressed

☐

Executables

☐

Images

☐

Javascript

☐

Multimedia

☐

Office

<

1

>

Cancel

Save

Threat Protection - Add Malware Scanning

Marque as caixas de checagem para adicionar *malware scanning*, conforme demonstrado abaixo:

Add Malware Scanning

All

☒ Item

☒ ActiveX

☐ Compressed

☐ Executables

☐ Images

☒ Javascript

☐ Multimedia

☐ Office

1

Cancel

Save

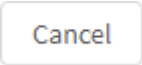
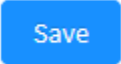
Threat Protection - Caixas de checagem marcadas

Caso seja necessário fazer uma configuração em todos os itens, basta selecionar a opção desejada no **menu de ações** []:

Select All

Deselect All

Threat Protection - Select all e Deselect All

Por fim, caso deseje cancelar clique no botão **Cancel** . Para concluir adição do *Malware Scanning* das aplicações clique no botão **Save** .

Threat Blocking

Para adicionar o *Threat Blocking*, certifique-se que o **checkbox**  está habilitado, depois clique no botão **list applications**  o seguinte painel, será exibido:

Add Threat Blocking

All

☐

Item

☐

Abuse

☐

Anonymizers

☐

Attacks

☐

Malware

☐

Reputation

☐

Spam

<

1

>

Cancel

Save

Threat Protection - Add Threat Blocking

Marque as caixas de checagem para adicionar o bloqueio de ameaças, conforme demonstrado abaixo:

Add Threat Blocking
X

All

☐	Item
☒	Abuse
☒	Anonymizers
☐	Attacks
☐	Malware
☐	Reputation
☒	Spam

<
1
>

Threat Protection - Add Threat Blocking

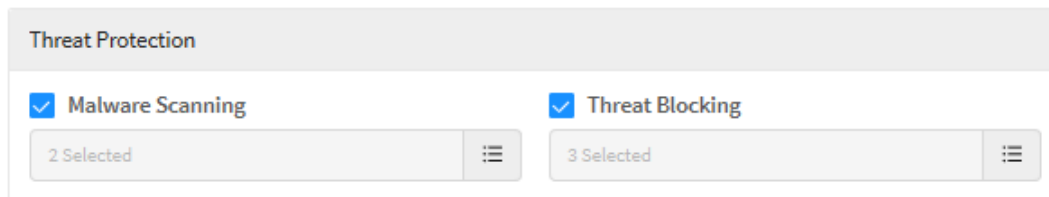
Caso seja necessário fazer uma configuração em todos os itens, basta selecionar a opção desejada no **menu de ações** []:

Select All
Deselect All

Threat Protection - Select all e Deselect All

Por fim, caso deseje cancelar clique no botão **Cancel**. Para concluir adição do *Malware Scanning* das aplicações clique no botão **Save**.

Após, ter efetuado os processos anteriores, um resumo de todos os itens de proteção de ameaças selecionados serão exibidos em ambos os campos, conforme exemplificado abaixo:



The image shows a 'Threat Protection' configuration window. It contains two main sections: 'Malware Scanning' and 'Threat Blocking'. Each section has a blue checkmark icon and a dropdown menu. The 'Malware Scanning' dropdown shows '2 Selected' and the 'Threat Blocking' dropdown shows '3 Selected'. Both dropdowns have a menu icon (three horizontal lines) to their right.

Threat Protection - Itens selecionados

Para concluir, basta clicar no botão **Save** novamente.

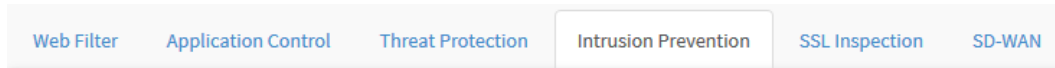
Aba Intrusion Prevention

O *Intrusion Prevention System* (IPS) é um módulos de prevenção de ataques e invasão, ele funciona analisando o fluxo do tráfego de modo a detectar e deter a explorações de vulnerabilidades na rede.



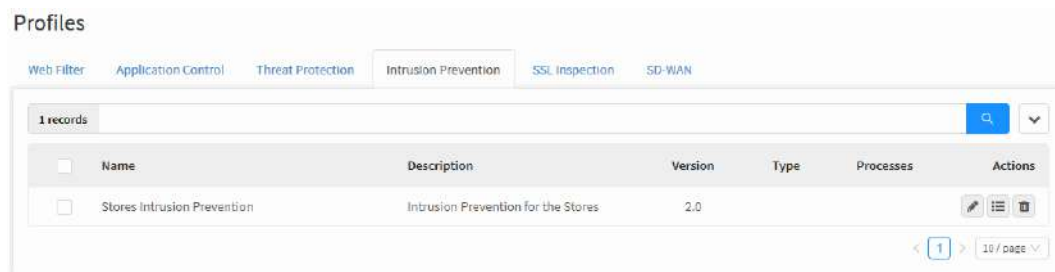
Para maiores informações sobre *Intrusion Prevention*, consulte o manual do Blockbit UTM.

Clique na aba “*Intrusion Prevention*”.



Aba Intrusion Prevention

Surgirá a Tela de “*Intrusion Prevention*”. Ela é composta pelas colunas “*Name*”, “*Description*”, “*Version*”, “*Type*”, “*Processes*” e “*Actions*”. Além disso, no topo direito da tela está localizada a [barra de busca](#) e o [menu de ações](#).



Profiles – Intrusion Prevention

A seguir, o [menu de ações](#) será analisado e posteriormente nos aprofundaremos no conteúdo das [colunas](#) do painel *Intrusion Prevention*.

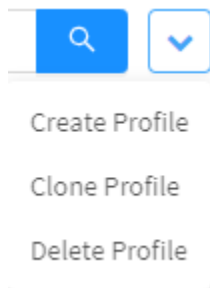
Intrusion Prevention - Menu de Ações

No topo direito da tela temos o menu de ações:



Intrusion Prevention – Botão do Menu de Ações

Ao clicar neste botão o menu abaixo é exibido:



Intrusion Prevention – Menu de Ações

O menu é composto das seguintes opções:

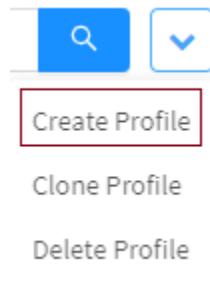
- [Create Profile](#);
- [Clone Profile](#);
- [Delete Profile](#).

A seguir cada opção do menu de ações será detalhada.

Intrusion Prevention - Menu de Ações - Create Profile

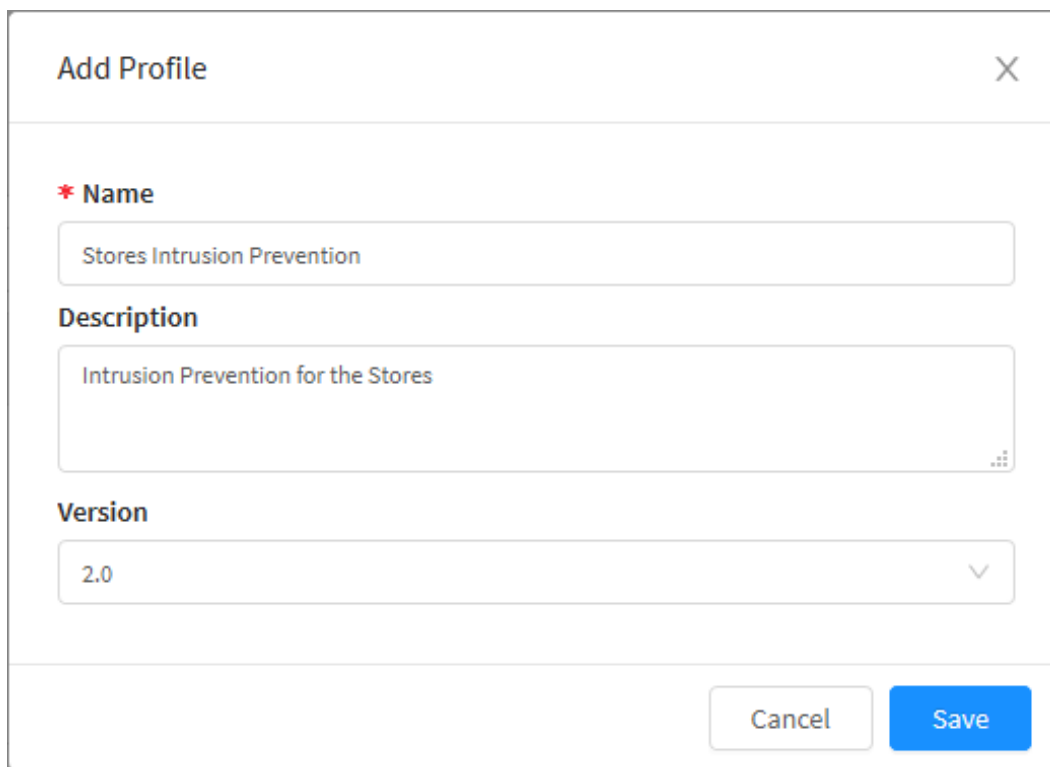
Através da opção "Create Profile" é possível criar um novo perfil de *Intrusion Prevention*. Para acessar, clique no **menu de ações** [].

1. Clique na opção "Create Profile";



Intrusion Prevention - Create Profile

2. A tela "Add Profile" será exibida. Preencha-a com os seguintes dados:

A screenshot of a web form titled 'Add Profile' with a close button (X) in the top right corner. The form contains three main sections: 'Name' with a red asterisk, 'Description', and 'Version'. The 'Name' field contains the text 'Stores Intrusion Prevention'. The 'Description' field contains the text 'Intrusion Prevention for the Stores'. The 'Version' field is a dropdown menu currently showing '2.0'. At the bottom right of the form are two buttons: 'Cancel' and 'Save'.

Intrusion Prevention – Add Profile

- **Name:** Nome do *profile*. Ex.: Intrusion Prevention - Stores;
- **Description:** Descrição do *profile*. Ex.: Intrusion Prevention - Stores;
- **Version:** Define a versão que será utilizada no *profile*. É importante que a versão seja igual a do UTM;



ATENÇÃO: Caso a versão do perfil seja diferente da do UTM, eles não serão compatíveis.

Sempre crie perfis com a mesma versão dos UTMs nos quais eles serão aplicados.

Cancel

Caso deseje cancelar clique no botão **Cancel**[]. Para concluir a criação do pacote de política clique no botão **Save**[].



Profile saved successfully

Profile saved successfully

O perfil foi criado com sucesso.

A seguir, veremos como [Clonar um Perfil](#).

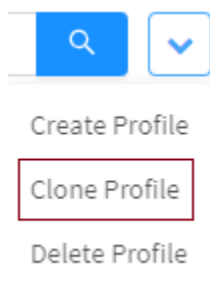
Intrusion Prevention - Menu de Ações - Clone Profile

Através da opção "Clone Profile" é possível clonar um perfil de *Intrusion Prevention*. Para acessar, clique no **menu de ações** [].



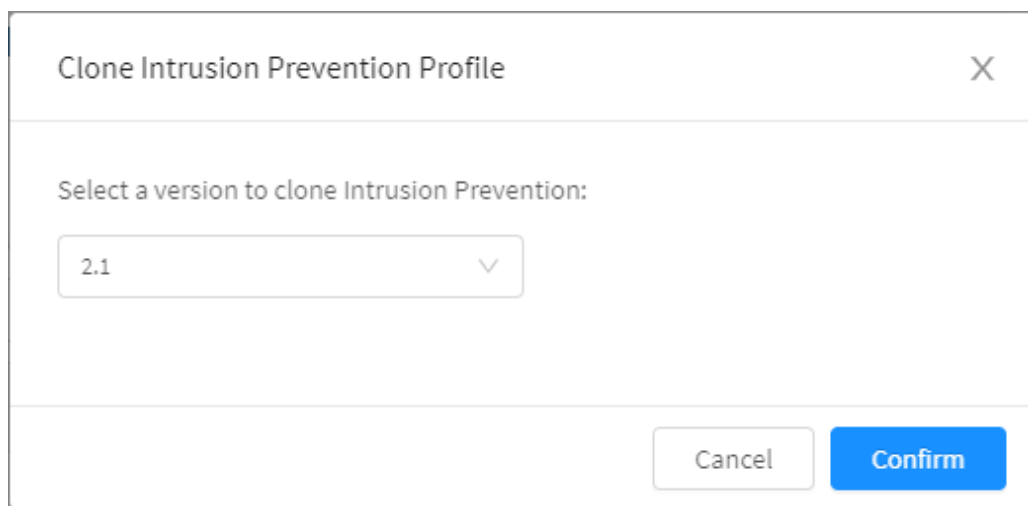
Intrusion Prevention - Main screen.

1. Clique na opção "Clone Profile":



Intrusion Prevention - Clone Profile

2. Para confirmar, clique em "Confirm":



Intrusion Prevention - Tela de Confirmação.



Perfil clonado com sucesso.

Também é possível clonar um perfil clicando no botão Clone [].

A seguir veremos como [Deletar um Perfil](#).

Intrusion Prevention - Menu de Ações - Delete Profile

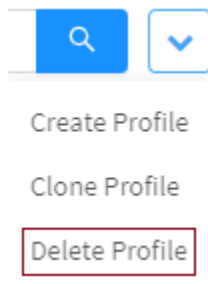
Através do botão "Delete Profile" é possível deletar os *Profiles* selecionados. Para deletar pelo menu de ações, siga os seguintes passos:

1. Selecione qual(is) *Profile(s)* deseja deletar. Para selecionar, basta clicar com o *mouse* no *checkbox* que fica localizado ao lado do *Name*. Nos *profiles* selecionados o *checkbox* mudará da cor cinza para azul []. Ex.: *Test*;



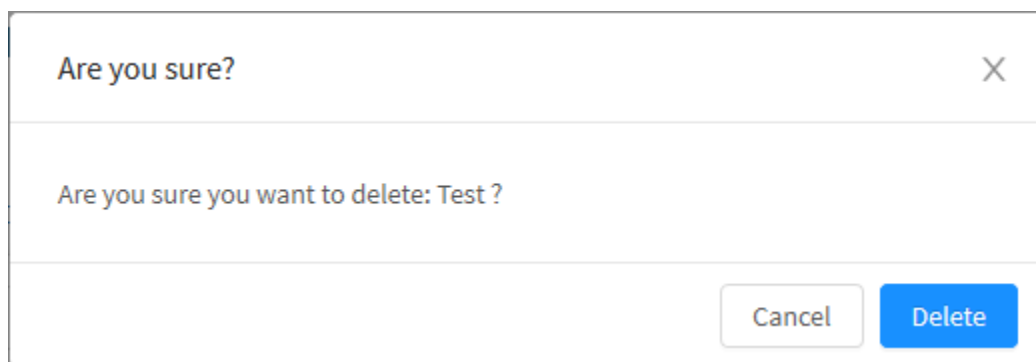
Intrusion Prevention – Seleção dos Profiles para deletar

2. Entre no **menu de ações** [] e clique na opção "Delete Profile".

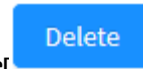
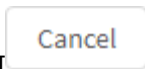


Intrusion Prevention – Delete Profile

3. Surgirá a mensagem de notificação questionando se deseja realmente deletar os *Profiles* selecionados:



Intrusion Prevention – Mensagem se deseja deletar os profiles



Caso desejar cancelar clique no botão **Cancel**]. Para concluir, clique no botão **Delete**].



Profile removed successfully

Profile removed successfully

Após realizar esses procedimentos, os *profiles* terão sido deletados com sucesso.

A seguir, analisaremos o [menu Colunas](#).

Intrusion Prevention - Colunas

A seguir explicaremos cada coluna da aba *Intrusion Prevention*:

Profiles

Web Filter

Application Control

Threat Protection

Intrusion Prevention

SSL Inspection

SD-WAN

1 records

☐	Name	Description	Version	Type	Processes	Actions
☐	Stores Intrusion Prevention	Intrusion Prevention for the Stores	2.0	firewall	1	

<

1

>

10 / page

Profiles – Intrusion Prevention

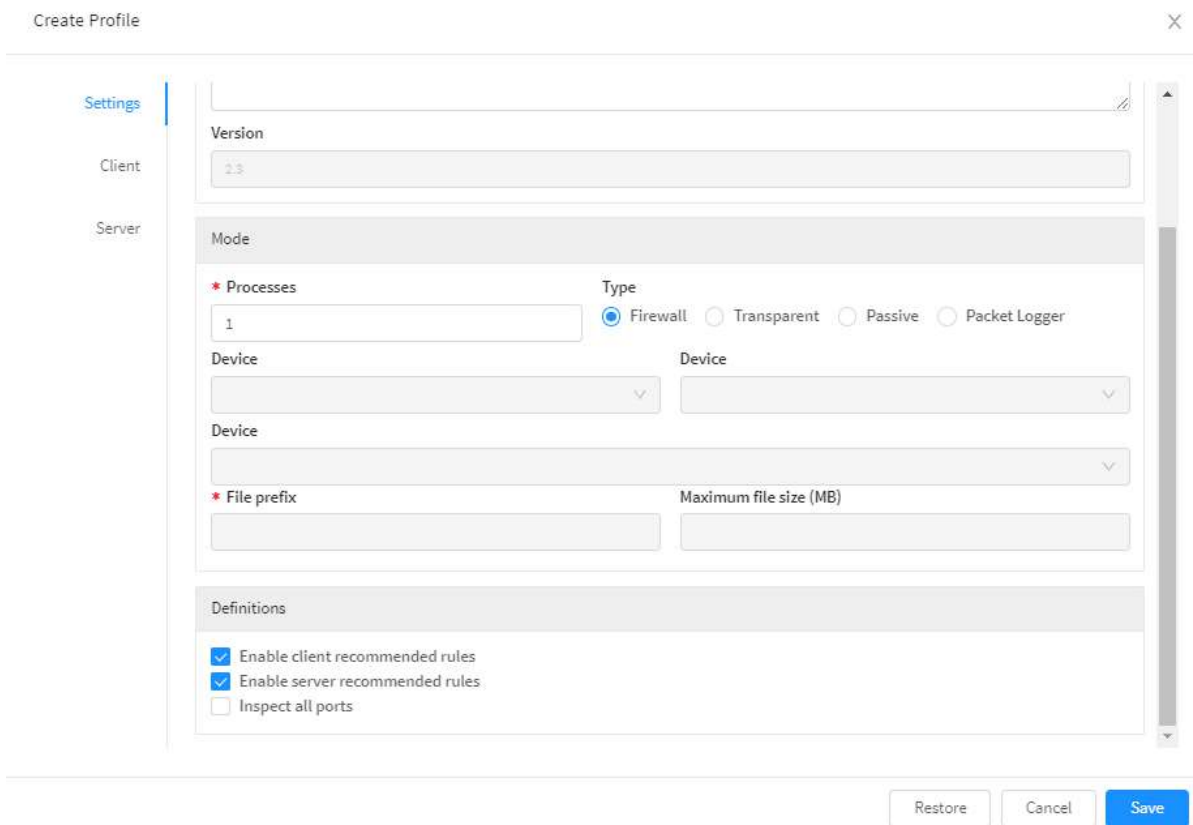
A seguir explicaremos cada coluna:

- **Caixa de Seleção** [☐]: Seleciona o *profile*;
- **Name**: Apresenta o nome do *profile* cadastrado;
- **Description**: Apresenta a descrição do *profile* cadastrado;
- **Version**: Apresenta a versão na qual o *profile* foi criado. É de extrema importância criar *profiles* da mesma versão que o UTM, caso contrário, o *profile* não será compatível;
- **Type**: Determina que tipo de prevenção será aplicada. As opções disponíveis são *Firewall*, *Transparent* e *Passive*;
- **Processes**: Determina o número de processos simultâneos para carregamento do perfil. Cada processo refere-se a um thread. Recomendamos que este valor seja "menor ou igual" ao número de núcleos de processamento do seu *Appliance*;
- **Actions**: A coluna "Actions" é composta por vários botões:
 - **Botão Edit** []: Permite editar as configurações do *profile* adicionado na opção *Create Profile* do menu de ações;
 - **Botão List Profiles** []: Permite visualizar, editar e adicionar opções mais específicas do *profile*, para mais informações, cheque [Intrusion Prevention - Create Profile](#);
 - **Botão Delete** []: Deleta o *profile*.

A seguir as funções do botão [List Profiles](#) serão explicadas e exemplificadas.

Intrusion Prevention - Create Profile

Ao clicar no botão **detalhar**  é possível configurar o *profile*;



Intrusion Prevention - Create Profile

Aba Settings

Nesta aba é possível efetuar as configurações gerais, definições e o modo de atuação do *Intrusion Prevention*.

General

Em "General" temos as seguintes caixas de texto:

General

* Name

Stores Intrusion Prevention

Description

Intrusion Prevention for the Stores

Version

2.0

Intrusion Prevention – General

- **Name:** Definir um nome para o perfil. Ex.: *Intrusion Prevention - Stores*;
- **Description:** Definir uma descrição para o perfil. Ex.: *Intrusion Prevention - Stores*;
- **Version:** Determinar a versão na qual o *profile* foi criado. É de extrema importância criar *profiles* da mesma versão que o UTM, caso contrário, o *profile* não será compatível.

Mode

Em "Mode" são determinadas as aplicações cujo acesso será permitido ou negado:

Mode

* Processes

1

Type

☒ Firewall
 ☐ Transparent
 ☐ Passive
 ☐ Packet Logger

Device

Device

Device

* File prefix

Maximum file size (MB)

Intrusion Prevention - Mode

- **Processes:** Definir um nome para o perfil. Ex.: *Intrusion Prevention - Stores*;
- **Type:** Selecione o Modo de operação do IPS. Os tipos disponíveis são: *Firewall*, *Transparent*, *Passive* e [Packet Logger](#);
- **Flow:** Este item só é requerido para configuração no modo "*Transparent*". Selecione o fluxo de direcionamento do pacote. O fluxo é determinado pelo *device* de entrada do pacote. Ex.: *Eth1* : *Eth2*;
- **Interface:** Este item só é requerido para configuração no modo "*Passive*". Selecione a interface de rede de entrada do fluxo pacote. Ex.: *Eth1*.



Nos campos *Flow* e *Interface*, as interfaces de rede devem estar "habilitadas" e sem endereço IP.

Definitions

Em "Definitions" são determinadas as aplicações cujo acesso será permitido ou negado:

Definitions

☒ Enable client recommended rules

☒ Enable server recommended rules

☐ Inspect all ports

Intrusion Prevention - Definitions

- **Enable client recommended rules**☒: A ativação desta opção habilita a exibição das regras *ATP padrão da Blockbit*. Estas regras serão exibidas aba *client*;
- **Enable server recommended rules**☒: A ativação desta opção habilita a exibição das regras *IPS padrão da Blockbit*. Estas regras serão exibidas na aba *server*;
- **Inspect all ports**☒: Habilita a inspeção independente da porta que o aplicativo esteja rodando.



A ativação da opção *Inspect all Ports* limita o processo do seu tráfego na rede.

Aba Client

Ao habilitar a opção **Enable client recommended rules** na aba *Settings*, a aba *Client* irá exibir as assinaturas *ATP* conforme demonstrado abaixo:



Para maiores informações sobre *ATP*, consulte o manual do Blockbit UTM.

Status	Quarantine	Risk	Category	Name / SID
All	Disabled	All	All	

Status	Block	Quarantine	Risk	Category	Name	SID
☐	☐	Disabled	Low	browser-other	BROWSER-OTHER Adobe Acrobat Pro ...	45043
☐	☐	Disabled	Low	browser-other	BROWSER-OTHER Adobe Acrobat Pro ...	45042
☐	☐	Disabled	Medium	browser-other	BROWSER-OTHER Android browser file ...	40458
☐	☐	Disabled	Medium	browser-other	BROWSER-OTHER Android Browser pot...	40361
☐	☐	Disabled	High	browser-other	BROWSER-OTHER Android WebView sa...	32029
☐	☐	Disabled	Medium	browser-other	BROWSER-OTHER Apple iOS CoreGrap...	38135
☐	☐	Disabled	Low	browser-other	BROWSER-OTHER Apple Safari docume...	44051
☐	☐	Disabled	Low	browser-other	BROWSER-OTHER Apple Safari docume...	44050
☐	☐	Disabled	Medium	browser-other	BROWSER-OTHER Apple Safari javascr...	45355
☐	☐	Disabled	Medium	browser-other	BROWSER-OTHER Apple Safari javascr...	45354

Total items: 3799 < 1 2 3 4 5 ... 380 > 10 / page

Intrusion Prevention - Client

As assinaturas estão divididas da seguinte forma:

- **Status:** Define se a assinatura está “Habilitar/Desabilitar”;
- **Block:** Define se a assinatura está “Habilitar/Desabilitar” para bloqueio;
- **Quarantine:** É possível “Habilitar/Desabilitar” a opção de quarentena informando se será validado por *IP* de origem ou destino. Ao habilitar a opção de quarentena automaticamente o sistema irá habilitar a assinatura com o status de **block** com isso todo tráfego que de *match* na assinatura o sistema irá dinamicamente inserir o endereço na quarentena dessa forma mantendo bloqueado conforme o tempo que foi configurado para quarentena;
- **Risk:** Que determina qual o risco da assinatura baseado na criticidade e complexidade do ataque que pode ser do tipo **Low**, **Medium** e **high**;
- **Category:** São grupos de assinaturas que possui a mesma finalidade;
- **Name:** Determina o nome da assinatura no sistema;
- **SID:** É o identificador único da assinatura.



Ao ativar o checkbox **Enable client recommended rules** ou **Enable server recommended rules** na aba *Definitions*, alguns *SID* serão destacados, o *SID* em azul é o padrão recomendado pela Blockbit (por exemplo, ao editar algum deles, ele passará a ser cinza).

Vide o exemplo abaixo, onde terceiro e quarto *SID* estão destacados:

Status	Block	Quarantine	Risk	Category	Name	SID
☐	☐	Disabled ▾	Low	browser-chrome	BROWSER-CHROME Google Chrome Cr...	46978
☐	☐	Disabled ▾	Low	browser-chrome	BROWSER-CHROME Google Chrome Cr...	46977
☒	☐	Disabled ▾	Low	browser-chrome	BROWSER-CHROME Google Chrome Fil...	49360
☒	☐	Disabled ▾	Low	browser-chrome	BROWSER-CHROME Google Chrome Fil...	49361
☐	☐	Disabled ▾	Low	browser-chrome	BROWSER-CHROME Google Chrome Fil...	21446
☐	☐	Disabled ▾	Low	browser-chrome	BROWSER-CHROME Google Chrome Fil...	21447
☐	☐	Disabled ▾	Low	browser-chrome	BROWSER-CHROME Google Chrome flo...	19710
☐	☐	Disabled ▾	Medium	browser-chrome	BROWSER-CHROME Google Chrome FT...	16795
☐	☐	Disabled ▾	Low	browser-chrome	BROWSER-CHROME Google Chrome GU...	16667
☐	☐	Disabled ▾	Low	browser-chrome	BROWSER-CHROME Google Chrome GU...	16668

Highlighted SID example

Aba Server

Ao habilitar a opção **Enable server recommended rules** na aba *Settings*, a aba *Server* irá exibir as assinaturas *IPS* conforme demonstrado abaixo:



Para maiores informações sobre *IPS*, consulte o manual do Blockbit UTM.

Status	Quarantine	Risk	Category	Name / SID
All	Disabled	All	All	

Status	Block	Quarantine	Risk	Category	Name	SID
☐	☐	Disabled	Low	attack_response	ATTACK_RESPONSE 401TRG Perl DDoS ...	2024977
☐	☐	Disabled	Medium	attack_response	ATTACK_RESPONSE ALBANIA id.php de...	2007656
☐	☐	Disabled	Low	attack_response	ATTACK_RESPONSE Backdoor reDuh ht...	2011667
☐	☐	Disabled	Medium	attack_response	ATTACK_RESPONSE C99 Modified phps...	2007654
☐	☐	Disabled	Medium	attack_response	ATTACK_RESPONSE c99shell phpshell ...	2007652
☐	☐	Disabled	Medium	attack_response	ATTACK_RESPONSE Cisco TclShell TFT...	2009245
☐	☐	Disabled	Medium	attack_response	ATTACK_RESPONSE Cisco TclShell TFT...	2009244
☐	☐	Disabled	Low	attack_response	ATTACK_RESPONSE FTP CWD to windo...	2008556
☐	☐	Disabled	High	attack_response	ATTACK_RESPONSE FTP inaccessible di...	2000507
☐	☐	Disabled	High	attack_response	ATTACK_RESPONSE FTP inaccessible di...	2000499

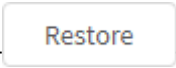
Total items: 24029 < 1 2 3 4 5 ... 2403 > 10 / page

Intrusion Prevention - Server

As assinaturas estão divididas da seguinte forma:

- **Status:** Define se a assinatura está “Habilitar/Desabilitar”;
- **Block:** Define se a assinatura está “Habilitar/Desabilitar” para bloqueio;
- **Quarantine:** É possível “Habilitar/Desabilitar” a opção de quarentena informando se será validado por *IP* de origem ou destino. Ao habilitar a opção de quarentena automaticamente o sistema irá habilitar a assinatura com o status de **block** com isso todo tráfego que de *match* na assinatura o sistema irá dinamicamente inserir o endereço na quarentena dessa forma mantendo bloqueado conforme o tempo que foi configurado para quarentena;
- **Risk:** Que determina qual o risco da assinatura baseado na criticidade e complexidade do ataque que pode ser do tipo **Low**, **Medium** e **high**;
- **Category:** São grupos de assinaturas que possui a mesma finalidade;
- **Name:** Determina o nome da assinatura no sistema;
- **SID:** É o identificador único da assinatura.

Botão Restore

Caso à qualquer momento queira restaurar o perfil e as configurações padrão da Blockbit, clique em **Restore** , a seguinte janela será exibida.

Are you sure?

Do you really want to restore the profile to default?

Cancel Restore

Intrusion Prevention - Do you really want to restore the profile to default?

Cancel

Restore

Clique no botão **Cancel** para sair dessa janela ou no botão **Restore** para restaurar.



Profile restored.

Profile restored

Cancel

Save

Por fim, caso deseje cancelar clique no botão **Cancel**. Para concluir a edição das aplicações clique no botão **Save**.



Saved successfully

Saved successfully

As configurações foram feitas com sucesso.

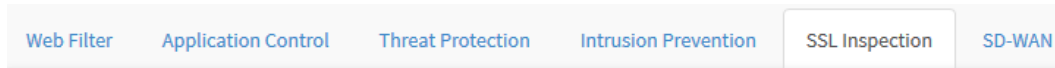
Aba SSL Inspection

O *SSL Inspection* atua interceptando o tráfego SSL e inspecionando conteúdo criptografado, utilizando-se deste recurso é possível selecionar o conteúdo que se deseja inspecionar através de políticas de conformidade.



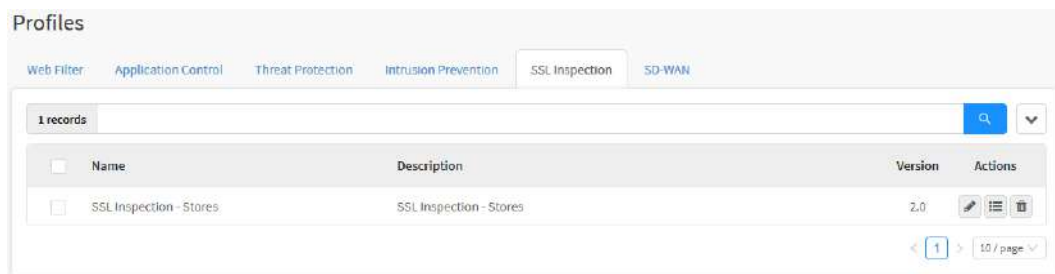
Para maiores informações sobre *SSL Inspection*, consulte esta [página](#) do manual do Blockbit UTM.

Clique na aba "*SSL Inspection*".



Aba *SSL Inspection*

Surgirá a Tela de "*SSL Inspection*". Ela é composta pelas colunas "*Name*", "*Description*", "*Mode*", "*Version*" e "*Actions*". Além disso, no topo direito da tela está localizada a [barra de busca](#) e o [menu de ações](#).



Profiles – *SSL Inspection*

A seguir, o [menu de ações](#) será analisado e posteriormente nos aprofundaremos no conteúdo das [colunas](#) do painel *SSL Inspection*.

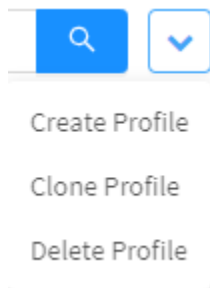
SSL Inspection - Menu de ações

No topo direito da tela temos o menu de ações:



SSL Inspection – Botão do Menu de Ações.

Ao clicar neste botão o menu abaixo é exibido:



SSL Inspection – Menu de Ações.

O menu é composto das seguintes opções:

- [Create Profile](#);
- [Clone Profile](#);
- [Delete Profile](#).

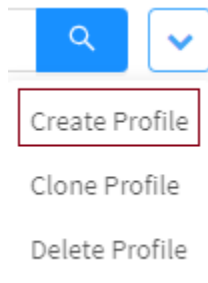
A seguir, cada opção do menu de ações será detalhada.

SSL Inspection - Menu de Ação - Create Profile



Através da opção "Create Profile" é possível criar um novo perfil de *SSL Inspection*. Para acessar, clique no **menu de ações** [

1. Clique na opção "Create Profile";



SSL Inspection - Create Profile

2. A tela "Create SSL Profile" será exibida. Preencha-a com os seguintes dados:

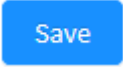
SSL Inspection – Create SSL Profile

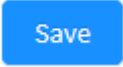
- **Name:** Nome do *profile*. Ex.: *Stores*;
- **Description:** Descrição do *profile*. Ex.: *Aplication Control - Stores*;
- **Version:** Define a versão que será utilizada no *profile*. É importante que a versão seja igual a do UTM;



ATENÇÃO: Caso a versão do perfil seja diferente da do UTM, eles não serão compatíveis.

Sempre crie perfis com a mesma versão dos UTMs nos quais eles serão aplicados.

CancelSave

Caso deseje cancelar clique no botão **Cancel**[]. Para concluir a criação do pacote de política clique no botão **Save**[].

 **Profile saved successfully**

Profile saved successfully

O perfil foi criado com sucesso.

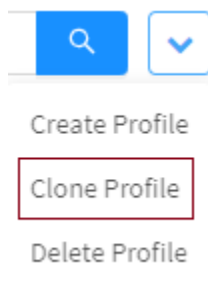
A seguir, veremos como [Clonar um Perfil](#).

SSL Inspection - Menu de Ação - Clone Profile

Através da opção "Clone Profile" é possível clonar um perfil de *SSL Inspection*. Para acessar, clique no **menu de ações** [].

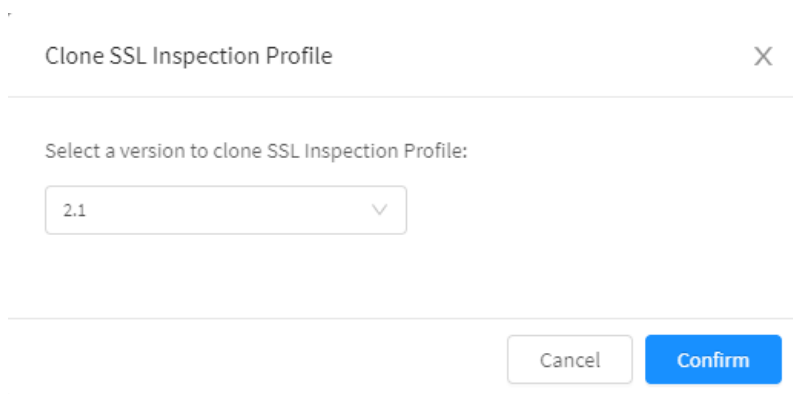


1. Clique na opção "Clone Profile";



SSL Inspection - Clone Profile

2. Para confirmar clique em "Confirm":



SSL Inspection - Clone Profile Confirmation.



SSL Inspection - Perfil clonado com sucesso.

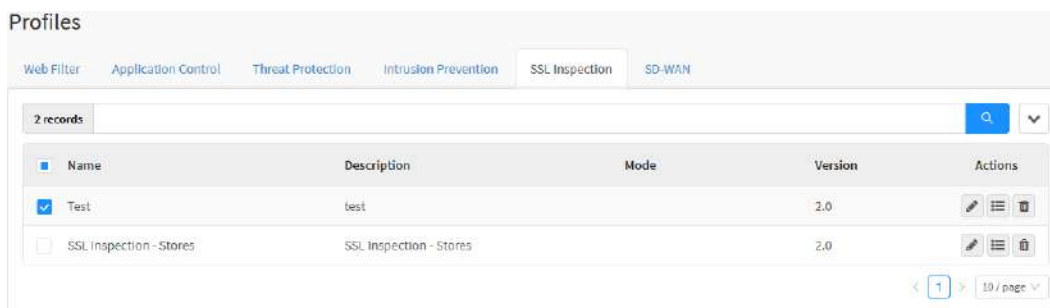
Também é possível clonar um perfil de SSL Inspection clicando no botão Clone [].

A seguir, veremos como [Deletar um Perfil](#).

SSL Inspection - Menu de Ação - Delete Profile

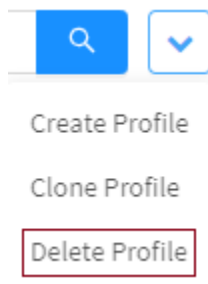
Através do botão "Delete Profile" é possível deletar os *Profiles* selecionados. Para deletar pelo menu de ações, siga os seguintes passos:

1. Selecione qual(is) *Profile*(s) deseja deletar. Para selecionar, basta clicar com o *mouse* no *checkbox* que fica localizado ao lado do *Name*. Nos *profiles* selecionados o *checkbox* mudará da cor cinza para azul []. Ex.: *Test*;



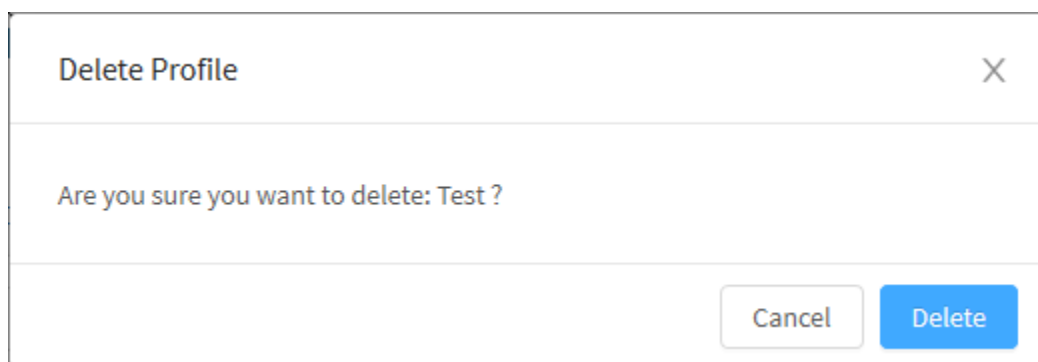
SSL Inspection – Seleção dos *Profiles* para deletar

2. Entre no **menu de ações** [] e clique na opção "Delete Profile".



SSL Inspection – Delete Profile.

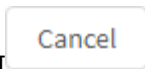
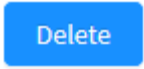
3. Surgirá a mensagem de notificação questionando se deseja realmente deletar os *Profiles* selecionados:



SSL Inspection – Mensagem se deseja deletar os *profiles*

Cancel

Delete

Caso desejar cancelar clique no botão **Cancel**[]. Para concluir, clique no botão **Delete**[].



Profile deleted successfully!

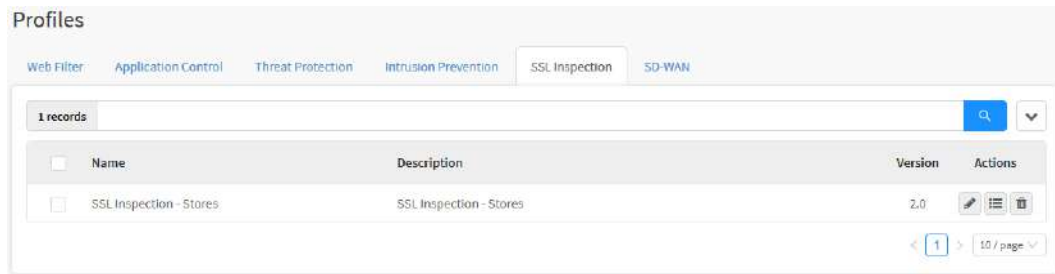
Profile deleted successfully

Após realizar esses procedimentos, os *profiles* terão sido deletados com sucesso.

A seguir analisaremos o [menu Colunas](#).

SSL Inspection - Colunas

A seguir explicaremos cada coluna da aba *SSL Inspection*:



☐	Name	Description	Version	Actions
☐	SSL Inspection - Stores	SSL Inspection - Stores	2.0	  

Profiles – *SSL Inspection*

A seguir explicaremos cada coluna:

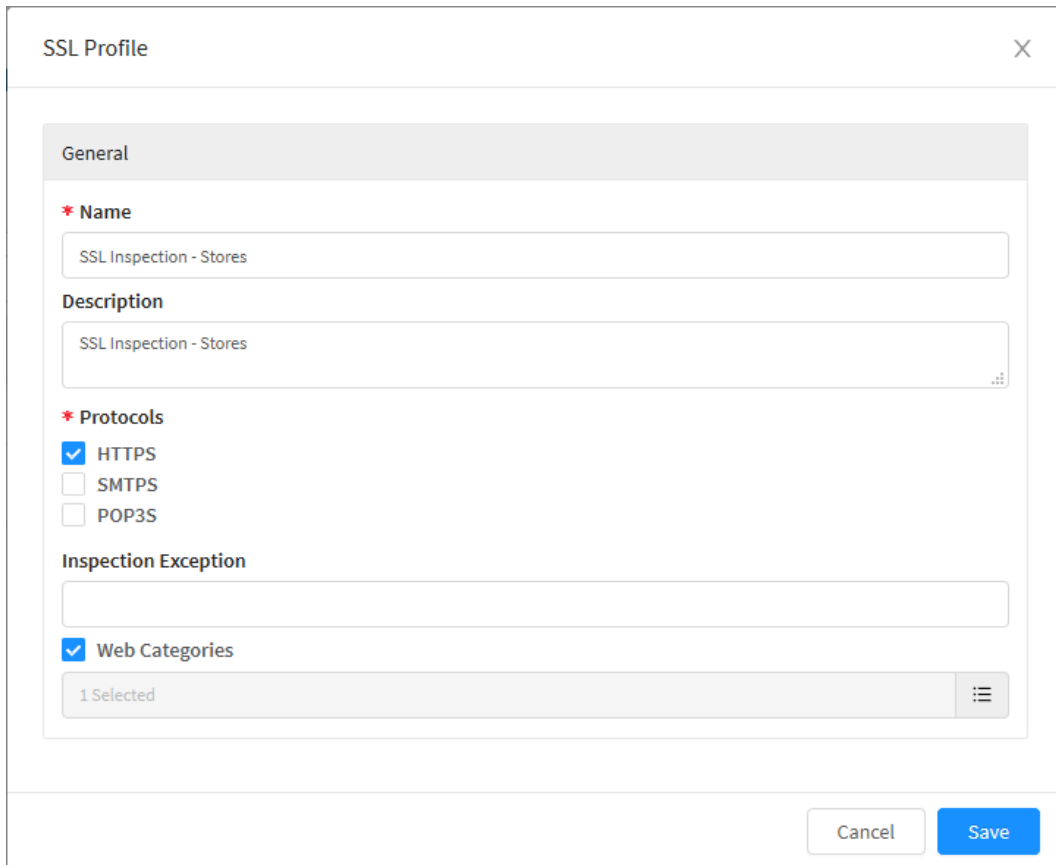
- **Caixa de Seleção** [☐]: Seleciona o *profile*.
- **Name**: Apresenta o nome do *profile* cadastrado;
- **Description**: Apresenta a descrição do *profile* cadastrado;
- **Version**: Apresenta a versão na qual o *profile* foi criado. É de extrema importância criar *profiles* da mesma versão que o UTM, caso contrário, o *profile* não será compatível;
- **Actions**: A coluna “Actions” é composta por vários botões:
 - **Botão Edit** []: Permite editar as configurações do *profile* adicionado na opção [Create Profile](#) do menu de ações;
 - **Botão List Profiles** [] Permite visualizar, editar e adicionar opções mais específicas do *profile*, para mais informações, cheque [SSL Inspection - SSL Profile](#);
 - **Botão Delete** []: Deleta o *profile*.

A seguir as funções do botão [List Profiles](#) serão explicadas e exemplificadas.

SSL Inspection - SSL Profile

Ao clicar no botão  detalhar[] é possível configurar o *profile*;

Neste painel é possível efetuar as configurações gerais, exceções de inspeção e quais protocolos são utilizados nesse perfil.



SSL Inspection - SSL Profile

- **Name:** Definir um nome para o perfil. Ex.: *SSL Inspection - Stores*;
- **Description:** Definir uma descrição para o perfil. Ex.: *SSL Inspection - Stores*;
- **Protocols:** Determina quais protocolos serão utilizados pelo *SSL Inspection*. As opções disponíveis são: *HTTPS*, *SMTPS* e *POP3S*;
- **Inspection Exception:** Determina exceções à inspeção SSL. Os valores inseridos nesse campo serão adicionados como tags;
- **Web Categories:** Permite selecionar as categorias Web para aplicar filtros de "Bloqueio" ou "Exceção" ao conjunto de políticas aplicadas. Para

selecionar as categorias, clique no botão [], escolha as categorias desejadas marcando as **caixas de checagem** [], conforme demonstrado abaixo:

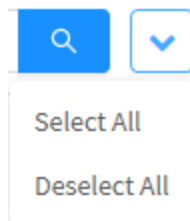
Add Category
X

All

- ☐ Uncategorized Sites
- ▼ ☐ Abortion
 - ☐ Pro-life
 - ☐ Pro-Choice
- ☐ Activism Groups
- ▼ ☒ Adult Material
 - ☒ Adult Content
 - ☒ Nudity
 - ☒ Sex
 - ☒ Sex Education
 - ☐ Lingerie and Swimsuit
- ▼ ☐ Business and Economy
 - ☐ Financial Data and Services
- ▼ ☒ Drugs
 - ☒ Abused Drugs
 - ☐ Prescribed Medications

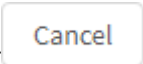
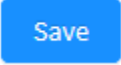
SSL Inspection - Add Category

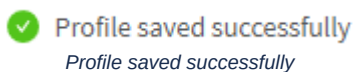
Caso seja necessário fazer uma configuração em todos os itens, basta selecionar a opção desejada no **menu de ações** []:



SSL Inspection - Add Category - Menu de Ações

Para sair deste painel, clique no botão **Cancel**  ou clique no botão **Save**  para concluir a adição das categorias.

Por fim, caso deseje cancelar a configuração clique no botão **Cancel** . Para concluir a edição do perfil clique no botão **Save** .



O perfil foi editado com sucesso.

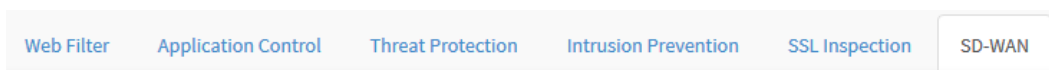
Aba SD-WAN

A função de monitoramento do *SD-WAN* é permitir a supervisão de dados específicos da *WAN*, viabilizando o melhor caminho de rede de acordo com os fatores determinados pelo administrador, isso permite direcionar os recursos mais adequados conforme regras e políticas pré-determinadas ou com base no perfil específico dos usuários.



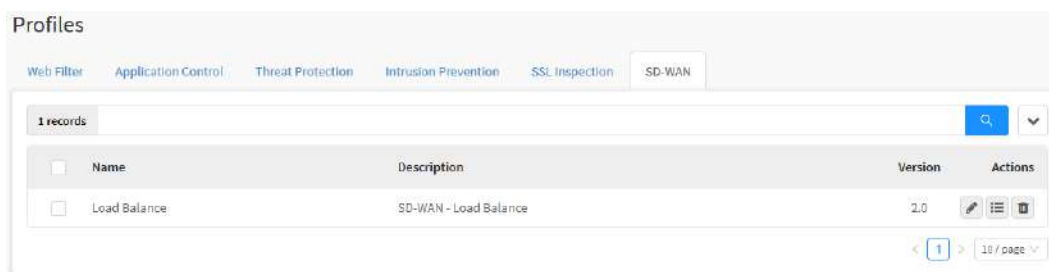
Para maiores informações sobre *SD-WAN*, consulte o manual do Blockbit UTM.

Clique na aba “*SD-WAN*”.



Aba *SD-WAN*

Surgirá a Tela de “*SD-WAN*”. Ela é composta pelas colunas “*Name*”, “*Description*”, “*Version*” e “*Actions*”. Além disso, no topo direito da tela está localizada a [barra de busca](#) e o [menu de ações](#).



Profiles – SD-WAN

A seguir, o [menu de ações](#) será analisado e posteriormente nos aprofundaremos no conteúdo das [colunas](#) do painel *SSL Inspection*.

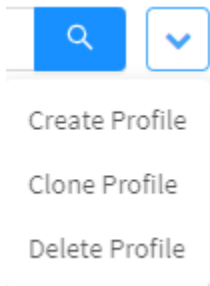
SD-WAN - Menu de ações

No topo direito da tela temos o menu de ações:



SD-WAN – Botão do Menu de ações

Ao clicar neste botão o menu abaixo é exibido:



SD-WAN – Menu de ações

O menu é composto das seguintes opções:

- [Create Profile](#);
- [Clone Profile](#);
- [Delete Profile](#).

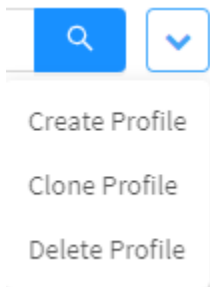
A seguir cada opção do menu de ações será detalhada.

No topo direito da tela temos o menu de ações:



SD-WAN – Botão do Menu de ações

Ao clicar neste botão o menu abaixo é exibido:



SD-WAN – Menu de ações

O menu é composto das seguintes opções:

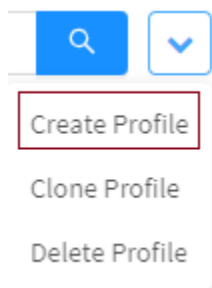
- [Create Profile](#);
- [Clone Profile](#);
- [Delete Profile](#).

A seguir cada opção do menu de ações será detalhada.

SD-WAN - Menu de ações - Create Profile

Através da opção "Create Profile" é possível criar um novo perfil de SD-WAN. Para acessar, clique no **Menu de ações** [].

1. Clique na opção "Create Profile";



SD-WAN - Create Profile

2. A tela "Create Profile SDWAN" será exibida. Preencha-a com os seguintes dados:

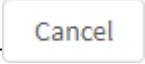
- **Name:** Nome do *profile*. Ex.: *Load Balance*;
- **Description:** Descrição do *profile*. Ex.: *SD-WAN - Load Balance*;
- **Version:** Define a versão que será utilizada no *profile*. É importante que a versão seja igual a do UTM;



ATENÇÃO: Caso a versão do perfil seja diferente da do UTM, eles não serão compatíveis.

Sempre crie perfis com a mesma versão dos UTMs nos quais eles serão aplicados.

SD-WAN – Create Profile SDWAN.

Caso deseje cancelar clique no botão **Cancel**. Para concluir a criação do pacote de política clique no botão **Save**.

 **Profile saved successfully**

Profile saved successfully

O perfil foi criado com sucesso.

A seguir, veremos como [Clonar um Perfil](#).

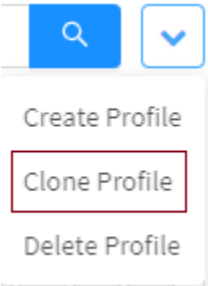
SD-WAN - Menu de ações - Clone Profile

Através da opção "Clone Profile" é possível clonar um perfil de SD-WAN. Para acessar, clique no **Menu de ações** [].



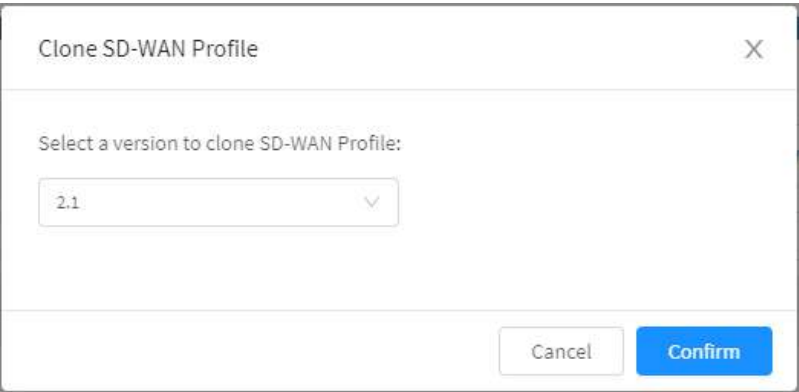
SD-WAN - Main Screen.

1. Clique na opção "Clone Profile":

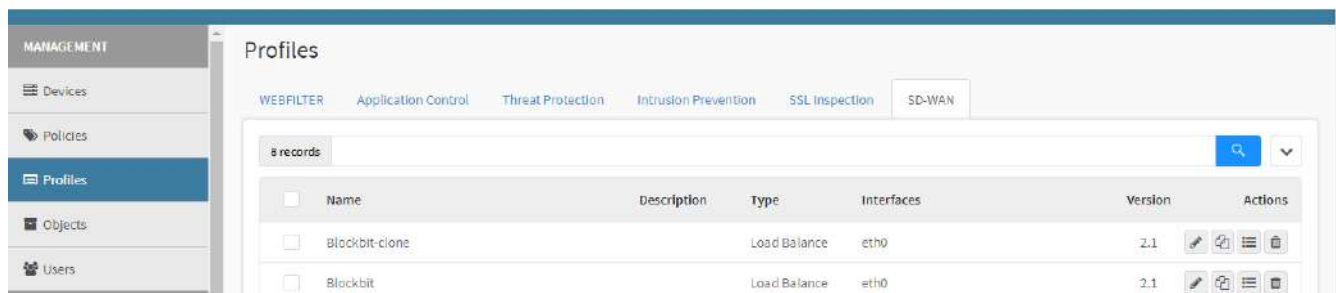


SD-WAN - Clone Profile.

2. Para confirmar clique em "Confirm":



SD-WAN - Clone.



Perfil de SD-WAN clonado com sucesso.

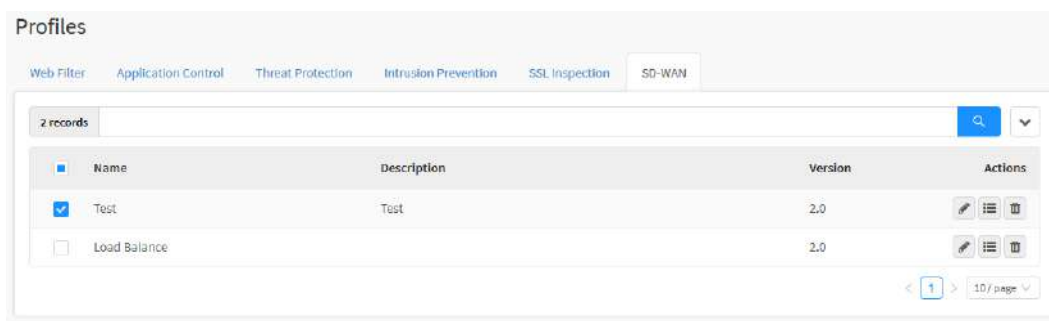
Também é possível clonar um perfil, clicando no botão Clone [].

A seguir, veremos como [Deletar um Perfil](#).

SD-WAN - Menu de ações - Delete Profile

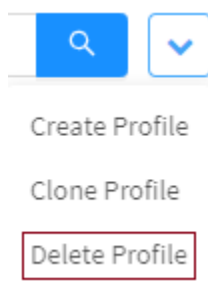
Através do botão "Delete Profile" é possível deletar os *Profiles* selecionados. Para deletar pelo menu de ações, siga os seguintes passos:

1. Selecione qual(is) *Profile(s)* deseja deletar. Para selecionar, basta clicar com o *mouse* no *checkbox* que fica localizado ao lado do *Name*. Nos *profiles* selecionados o *checkbox* mudará da cor cinza para azul [☒]. Ex.: *Test*;



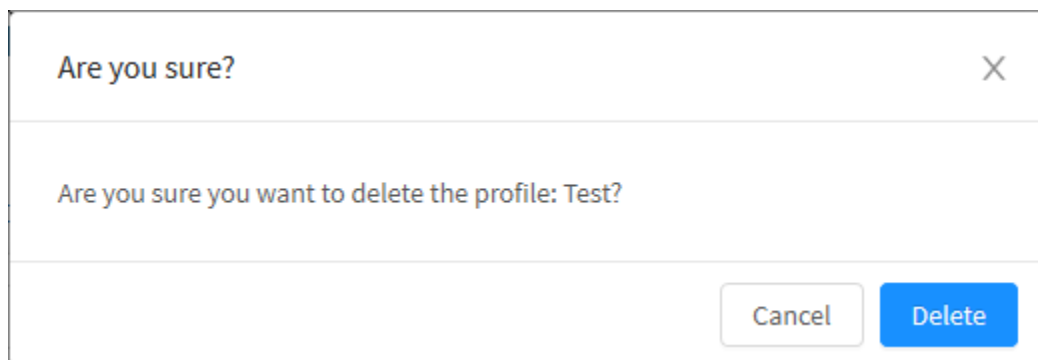
SD-WAN – Seleção dos *Profiles* para deletar.

2. Entre no *Menu Actions* e clique na opção "Delete Templates".

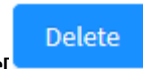
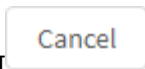


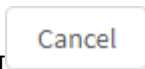
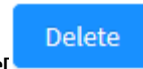
SD-WAN – Delete Profile.

3. Surgirá a mensagem de notificação questionando se deseja realmente deletar os *profiles* selecionados:



SD-WAN – Mensagem se deseja deletar os *Profiles*



Caso desejar cancelar clique no botão **Cancel**[]. Para concluir, clique no botão **Delete**[].



Profile deleted successfully!

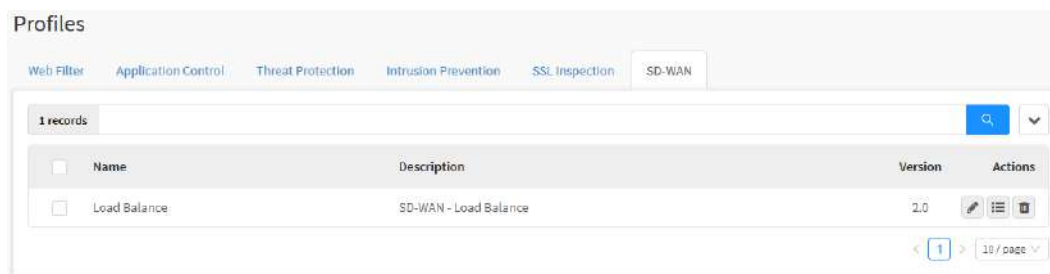
Profile deleted successfully

Após realizar esses procedimentos, os *profiles* terão sido deletados com sucesso.

A seguir, analisaremos o [menu Colunas](#).

SD-WAN - Colunas

A seguir explicaremos cada coluna da aba SD-WAN:



The screenshot shows the 'Profiles' section of a management interface, specifically the 'SD-WAN' tab. It displays a table with one record. The table has columns for Name, Description, Version, and Actions. The record is 'Load Balance' with description 'SD-WAN - Load Balance' and version '2.0'. The Actions column contains three icons: a pencil (Edit), a list (List Profiles), and a trash can (Delete).

Name	Description	Version	Actions
Load Balance	SD-WAN - Load Balance	2.0	  

Profiles – SD-WAN.

A seguir explicaremos cada coluna:

- **Caixa de Seleção** []: Seleciona o *profile*.
- **Name**: Apresenta o nome do *profile* cadastrado;
- **Description**: Apresenta a descrição do *profile* cadastrado;
- **Version**: Apresenta a versão na qual o *profile* foi criado. É de extrema importância criar *profiles* da mesma versão que o UTM, caso contrário, o *p*rofile não será compatível;
- **Actions**: A coluna "Actions" é composta por vários botões:
 - **Botão Edit** []: Permite editar as configurações do *profile* adicionado na opção *Create Profile* do menu de ações;
 - **Botão List Profiles** []: Permite visualizar, editar e adicionar opções mais específicas do profile, para mais informações, cheque [S D-WAN - SDWAN Profile](#);
 - **Botão Delete** []: Deleta o *profile*.

A seguir as funções do botão [List Profiles](#) serão explicadas e exemplificadas.

SD-WAN - SDWAN Profile

Ao clicar no botão **detalhar**  é possível configurar o *profile*;



Para maiores informações sobre cada configuração, consulte esta [página](#) do manual do Blockbit UTM.

Neste painel é possível efetuar todas as configurações referentes à atuação do *SD-WAN*. A seguir demonstraremos configurando o *Load Balance*.

Aba Interfaces

Nesta aba é possível configurar como o *SD-WAN* irá interagir com as interfaces eth.

SDWAN Profile

Interfaces

Monitor

General

* Name

Load Balance

Description

SD-WAN - Load Balance

* Type

Load Balance

* Fail ratio (1 - 100%)

10

* Monitoring Interval (sec)

5

☒ Persistence timeout 1-1440 min

30

Interfaces

:: ETH0	0%	☐
:: ETH1	0%	☐
:: ETH2	0%	☐
:: ETH3	0%	☐

Cancel

Save

General

Em "General" temos as seguintes caixas de texto:

The screenshot shows the 'General' configuration tab for an SD-WAN profile. It includes the following fields and values:

- Name:** Load Balance
- Description:** SD-WAN - Load Balance
- Type:** Load Balance (dropdown menu)
- Fail ratio (1 - 100%):** 10
- Monitoring Interval (sec):** 5
- Persistence timeout 1-1440 min:** ☒ 30

SD-WAN – General

- **Name:** Definir um nome para o perfil. Ex.: *Load Balance*;
- **Description:** Definir uma descrição para o perfil. Ex.: *SD-WAN - Load Balance*;
- **Type:** Neste campo se define como o SD-WAN irá atuar. A seleção destas opções define quais campos de texto serão exibidos no painel *General*. É possível selecionar qualquer tipo, porém nesta demonstração usaremos o "Load Balance". Para mais informações a respeito dos tipos de SD-WAN cheque o capítulo [Tipos de Perfil](#). As opções disponíveis são:
 - Load Balance;
 - Failover;
 - Spillover;
 - Dynamic Selection.
- **Interfaces:** É essencial para o correto funcionamento do SD-WAN definir as interfaces de *link de internet* que serão usadas na composição do perfil. Neste exemplo selecionaremos as *interfaces*: "tun0 – Rede 10" e "tun1 – Rede 11";
- **Monitoring Interval (sec.):** Definir o intervalo de monitoramento entre cada teste. É recomendável deixar como 1 segundo. Ex.: 1 segundo;
- **Fail Ratio 1-100%:** Definir o valor da taxa de falha entre 1 a 100%. É recomendável deixar o padrão de 70%. Ex.: 70%.

Interfaces

Em "Interfaces" temos as seguintes opções:

Interfaces

⋮	ETH0	50%	☒
⋮	ETH1	50%	☒
⋮	ETH2	0%	☐
⋮	ETH3	0%	☐

SD-WAN – Interfaces



Só é possível interagir com as interfaces que tiverem sido **habilitadas** [☒] caso uma interface estiver **desabilitada** [☐], ela ficará esmaecida, não será possível editá-la e será desconsiderada.

- **Mover** []: Clique e arraste para posição desejada, dessa forma o *link* que estiver na primeira posição de cima para baixo será usado para saída do tráfego, caso o *link* estiver desabilitado, o tráfego será redirecionado de forma automática para o *link* subsequente da lista dessa forma garantindo alta disponibilidade no acesso à internet, quando o *link* voltar a ser habilitado o sistema automaticamente irá retornar a saída para o primeiro *link* da lista;
- **Interfaces**: É essencial para o correto funcionamento do SD-WAN definir as interfaces de *link* de *internet* que serão usadas na composição do perfil. Neste exemplo selecionaremos as *interfaces*: "eth0" e "eth1";

Aba Monitor

Nesta aba são configurados os indicadores de performance e alvos de monitoramento, utilizados pelo SD-WAN.

SD-WAN Profile

×

Interfaces

Monitor

* Performance Indicators

☒ Latency (ms)
 ☐ Jitter (ms)

☐ Packet Loss (%)
 ☐ Bandwidth (%)

10

10

10

85

Monitoring Targets

* Address

* Protocol

* Attempts

* Timeout

www.blockbit.com

ICMP

3

3 sec.

+

Cancel

Save

SD-WAN – SDWAN Profile - Aba Monitor

Performance Indicators

Em "Performance Indicators" temos as seguintes caixas de texto:

* Performance Indicators

☒ Latency (ms)
 ☐ Jitter (ms)

☐ Packet Loss (%)
 ☐ Bandwidth (%)

10

10

10

85

SD-WAN – SDWAN Profile - Performance Indicators

- **Latency:** Determina quanto tempo leva para um pacote de dados sair da origem, chegar no destino e voltar. Ex.: 10 ms;
- **Jitter:** Determina a média de quanto tempo leva para um pacote de dados sair da origem, chegar no destino e voltar. Ex.: 30 ms;
- **Packet Loss:** Determina a porcentagem aceitável de perda de pacotes. Ex.: 75%;
- **Bandwidth:** Determina a porcentagem aceitável do consumo de banda. Utiliza como base os valores de download em "Traffic Shaping". Ex.: 70%.



Para maiores informações sobre cada configuração, consulte esta [página](#) do manual do Blockbit UTM.

Monitoring Targets

Em "Monitoring Targets" temos as seguintes caixas de texto:

* Address	* Protocol	* Attempts	* Timeout
www.blockbit.com	ICMP	3	3 sec.

SD-WAN – SDWAN Profile - Monitoring Interfaces

Define os endereços nos quais serão realizados os testes. É recomendável que nos "Monitoring Targets" sejam colocados os IPs virtuais do outro lado do túnel de modo que se a comunicação for feita com sucesso, isso indica que o Túnel está corretamente configurado.

Cancel

Por fim, caso deseje cancelar clique no botão **Cancel**[]. Para concluir a edição das aplicações clique no botão **Save**[].

Save

Objects

Esta seção irá demonstrar como criar, editar e excluir objetos.

O sistema foi desenvolvido orientado a objetos para facilitar o processo de ajuste, manutenção e leitura de regras e configurações.

Os objetos podem ser compartilhados entre *devices* e os serviços do sistema.

Todas as alterações aplicadas em um objeto são automaticamente replicadas e aplicadas a todos os serviços em uso pelo respectivo objeto.

Permite também a detecção do local de origem da base de regras de determinado objeto.

Para acessar a tela, basta selecionar o botão “Objects”;



Management – Objects

A tela abaixo será exibida:

Addresses	Services	Times	Schedules	Dictionaries	Contents
9 records					
☐	Name	Description	Type	Used	Actions
☐	Class A network	Reserved network Class A 10.0.0.0/8	IPv4		
☐	Class B network	Reserved network Class B 172.16.0.0/12	IPv4	-	
☐	Class C network	Reserved network Class C 192.168.0.0/16	IPv4	-	
☐	Localhost	Loopback 127.0.0.1	IPv4	-	
☐	Private class network	Special-use address reserved to private network (A...	IPv4	-	
☐	Skype Servers		IPv4	-	
☐	Teste endereço		IPv4	-	
☐	Webex Servers		IPv4	-	
☐	Whatsapp Servers		IPv4	-	
					< 1 > 10 / page

Objects - Addresses

A tela *objects* comporta as seguintes abas:

- [Addresses](#);
- [Services](#);
- [Times](#);
- [Schedules](#);
- [Dictionaries](#);
- [Contents](#).

A seguir, os componentes da aba [Addresses](#) serão analisadas.

Objects - Addresses

Os objetos do tipo *Address* são utilizados para identificar *hosts* (máquinas) ou *networks* (redes).

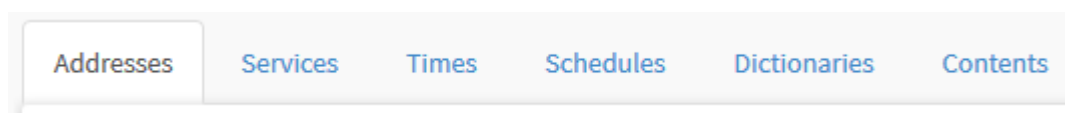
Por padrão, o sistema traz alguns objetos pré-cadastrados, por exemplo, os objetos referentes às classes de rede não válidas: “Classe A reservada”, “Classe B reservada”, “Classe C reservada”.

Todos esses objetos estão disponíveis para serem usados nos processos de configuração e habilitação dos serviços.

O Blockbit GSM permite a definição de três formas de identificação de *Address*:

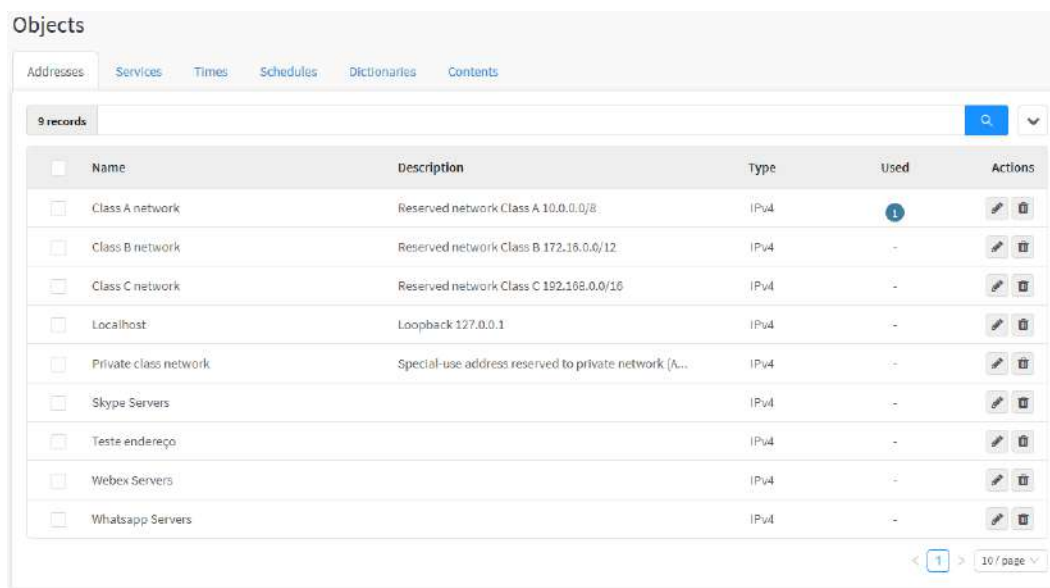
- **IP address / Network address:** São objetos que identificam máquinas e redes através de seus endereços IP. Ex.: 172.16.102.235 ou 172.16.102.0/24;
- **MAC address:** São objetos que identificam as máquinas através dos endereços físicos de suas placas de rede. Ex.: 38:59:F9:1F:4E:16;
- **FQDN address:** São objetos que identificam as máquinas através de seu endereço *DNS*. Ex.: blockbit.com ou www.blockbit.com;

Para acessar, clique na aba “Addresses”:



Aba Addresses

Surgirá a tela “Addresses”. Ela é composta pelas colunas “Select”, “Name”, “Description”, “Type”, “Used” e “Actions”. Além disso, no topo da tela está localizada a [barra de busca](#) e o [menu de ações](#) à direita.



The screenshot shows the 'Objects' page with the 'Addresses' tab selected. At the top, there is a search bar and a dropdown menu. Below this is a table with 9 records. The table has columns for Name, Description, Type, Used, and Actions. The 'Used' column contains a blue circle with a white '1' for the first record. The 'Actions' column contains edit and delete icons for each record.

☐	Name	Description	Type	Used	Actions
☐	Class A network	Reserved network Class A 10.0.0.0/8	IPv4		
☐	Class B network	Reserved network Class B 172.16.0.0/12	IPv4	-	
☐	Class C network	Reserved network Class C 192.168.0.0/16	IPv4	-	
☐	Localhost	Loopback 127.0.0.1	IPv4	-	
☐	Private class network	Special-use address reserved to private network (A...	IPv4	-	
☐	Skype Servers		IPv4	-	
☐	Teste endereço		IPv4	-	
☐	Webex Servers		IPv4	-	
☐	Whatsapp Servers		IPv4	-	

Objects – Addresses

Explicaremos em detalhes o [menu de ações](#) e posteriormente as colunas da aba “Addresses”.

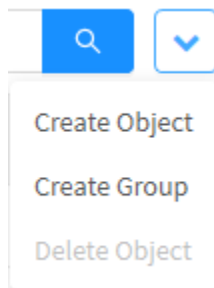
Objects - Addresses - Menu de ações

No topo direito da tela temos o menu de ações:



Objects – Botão do menu de ações

Ao clicar neste botão o menu abaixo é exibido:



Objects – Menu de ações

O menu é composto das seguintes opções:

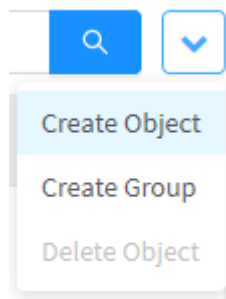
- [Create Object](#);
- [Create Group](#);
- [Delete Object](#).

A seguir cada opção do menu de ações será detalhada.

Objects - Addresses - Menu de ações - Create Object

Através da opção "Create Object" é possível criar um novo *Object Address*. Para acessar, siga os passos:

1. No **menu de ações** [], clique na opção "Create Object";



Objects – Addresses – Create Object

2. Surgirá a tela *Create Addresses Object*. Preencha os campos:

Create Addresses Object

×

* Name

* Type

IPv4 Address

▼

☐ Unique

* Address

Mask

255.255.255.255

▼

+

^

▼

-

Description

Cancel

Import Address

Save

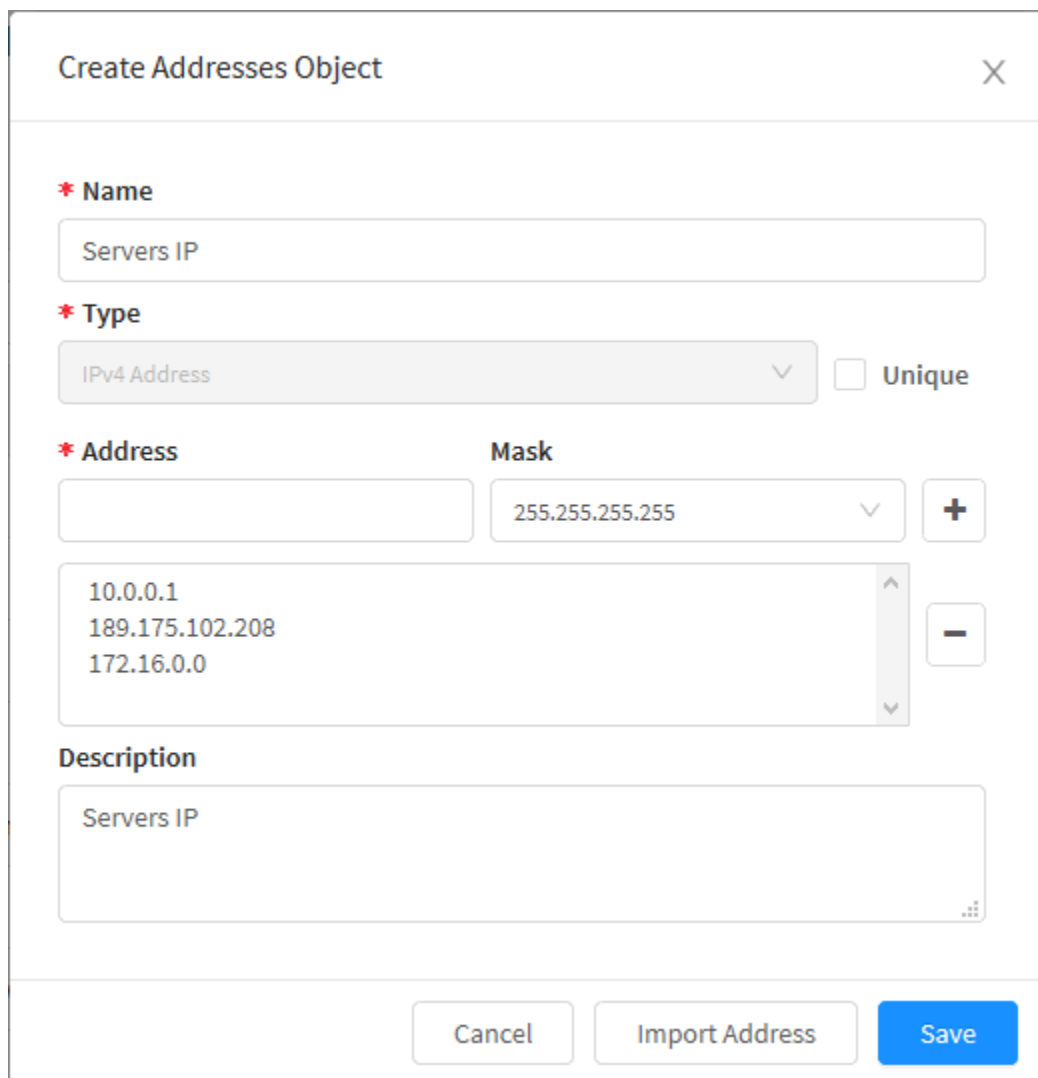
Objects – Create Addresses Object

É possível criar endereços do tipo IPv4, IPv6, Mac e FQDN. Segue alguns exemplos:

- [Exemplo 1 - Criando Objeto de Endereço IPv4;](#)
- [Exemplo 2 - Criando Objeto de Endereço IPv6;](#)
- [Exemplo 3 - Criando Objeto de Endereço Físico.](#)

Objects - Exemplo 1 - Criando Objeto de Endereço IPv4

Segue uma demonstração de como criar um objeto de endereço IPv4:



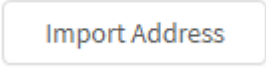
Objects – Create Addresses Object - IPv4



Atenção: Uma vez definido o campo *Type* e depois de salvar o objeto, não é possível alterá-lo durante a edição.

- **Name:** Nome do objeto. Ex.: *Servers IP*;
- **Type:** Tipo do objeto de conexão, podendo optar entre: *IPv4 Address*, *IPv6 Address*, *MAC Address* e *FQDN Address*. Após salvar o objeto, não será mais possível editar este campo;
- **Unique** ☐: Determina se o endereço será único ou não, desabilitando o campo *Mask*;
- **Address:** O endereço do tipo de objeto de conexão selecionado posteriormente. Após digitar um endereço, clique em  para adicioná-lo na lista ou selecione-o e clique em  para remover. Após adicionar um endereço do tipo selecionado, o campo *Type* ficará desabilitado, caso deseje mudar de tipo, remova todos os endereços da lista;
- **Mask:** Este campo estará disponível para adicionar a máscara do endereço IP, caso o *type IPv4 Address* ou *IPv6 Address* seja selecionado no campo "type";

- **Description:** Este campo é destinado para a descrição do objeto. Ex.: Servers IP.

Ao clicar sobre o botão **Import Address**  e selecionar o arquivo que será importado, clicar em  para adicionar o conteúdo do arquivo dentro do objeto, caso queira remover algum endereço cadastrado, selecionar o endereço *IP* e clicar no botão  e o conteúdo será removido.



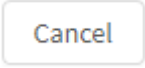
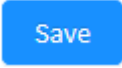
O formato suportado da lista é um endereço IP ou de rede por linha.

Ex.: 10.0.0.1

189.175.102.208

172.16.0.0/16

Cancel

Clique no botão **Cancel**  para Cancelar ou no botão **Save**  para salvar.

Save



Object successfully changed!

Object successfully changed

O *object address* foi criado com sucesso.

Objects - Exemplo 2 - Criando Objeto de Endereço IPv6

Segue uma demonstração de como criar um objeto de endereço IPv6:

Create Addresses Object

*

Name

Server IPs - IPv6

*

Type

IPv6 Address

Unique

*

Address

Prefix

128

+

2001:db8::1

2001:db8::2

2001:db8::3

2001:db8::4

-

Description

Server IPs - IPv6

Cancel

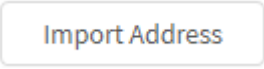
Import Address

Save

Objects – Create Addresses Object - IPv6

Atenção: Uma vez definido o campo *Type* e depois de salvar o objeto, não é possível alterá-lo durante a edição.

- **Name:** Nome do objeto. Ex.: Server IPs - IPv6;
- **Type:** Tipo do objeto de conexão, podendo optar entre: *IPv4 Address*, *IPv6 Address*, *MAC Address* e *FQDN Address*. Após salvar o objeto, não será mais possível editar este campo;
- **Unique**☐: Determina se o endereço será único ou não, desabilitando o campo *Prefix*;
- **Address:** O endereço do tipo de objeto de conexão selecionado posteriormente. Após digitar um endereço, clique em para adicioná-lo na lista ou selecione-o e clique em para remover. Após adicionar um endereço do tipo selecionado, o campo *Type* ficará desabilitado, caso deseje mudar de tipo, remova todos os endereços da lista;
- **Prefix:** Define o prefixo do endereço *IP* que será adicionado no objeto. Ex.: 128;
- **Description:** Este campo é destinado para a descrição do objeto. Ex.: Server IPs - IPv6.

Ao clicar sobre o botão **Import Address**  e selecionar o arquivo que será importado, clicar em  para adicionar o conteúdo do arquivo dentro do objeto, caso queira remover algum endereço cadastrado, selecionar o endereço *IP* e clicar no botão  e o conteúdo será removido.



O formato suportado da lista é um endereço IP ou de rede por linha.

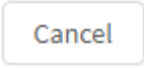
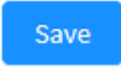
Ex.: 2001::FF:01/68

::FF:0A/128

2001:abcd:172.16.102.0/120

Cancel

Save

Clique no botão **Cancel**  para Cancelar ou no botão **Save**  para salvar.



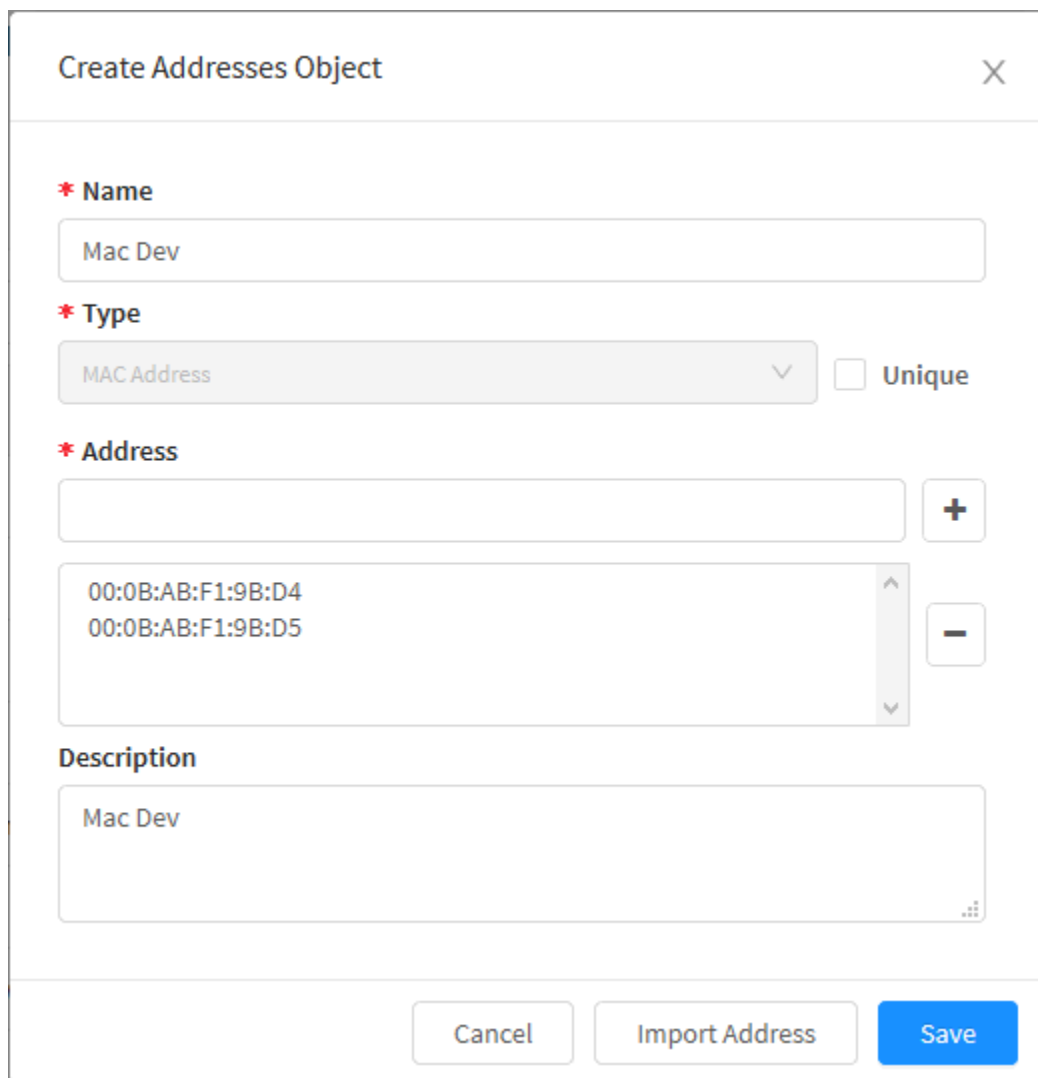
Object successfully changed!

Object successfully changed

O *object address* foi criado com sucesso.

Objects - Exemplo 3 - Criando Objeto de Endereço Físico

Segue uma demonstração de como criar um objeto de MAC Address:



Objects – Create Addresses Object - Mac Address



Atenção: Uma vez definido o campo *Type* e depois de salvar o objeto, não é possível alterá-lo durante a edição.

- **Name:** Nome do objeto. Ex.: Mac Dev;
- **Type:** Tipo do objeto de conexão, podendo optar entre: *IPv4 Address*, *IPv6 Address*, *MAC Address* e *FQDN Address*. Após salvar o objeto, não será mais possível editar este campo;
- **Unique** ☐: Determina se o endereço será único ou não;
- **Address:** O endereço do tipo de objeto de conexão selecionado posteriormente. Após digitar um endereço, clique em  para adicioná-lo na lista ou selecione-o e clique em  para remover. Após adicionar um endereço do tipo selecionado, o campo *Type* ficará desabilitado, caso deseje mudar de tipo, remova todos os endereços da lista;
- **Description:** Este campo é destinado para a descrição do objeto. Ex.: Mac Dev.

Import Address



Ao clicar sobre o botão **Import Address** [] e selecionar o arquivo que será importado, clicar em [] para adicionar o conteúdo do arquivo dentro do objeto, caso queira remover algum endereço cadastrado, selecionar o endereço *IP* e clicar no botão [] e o conteúdo será removido.



A definição do endereço MAC é composta por 48 bits e seu formato é totalmente específico, possui 12 dígitos hexadecimais, agrupados dois a dois separados por dois pontos.

Sintaxe do objeto: 00:01:02:AA:CC:FF

Cancel

Save

Clique no botão **Cancel** [] para Cancelar ou no botão **Save** [] para salvar.



Object successfully changed!

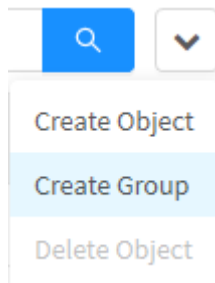
Object successfully changed

O *object address* foi criado com sucesso.

Objects - Addresses - Menu de ações - Create Group

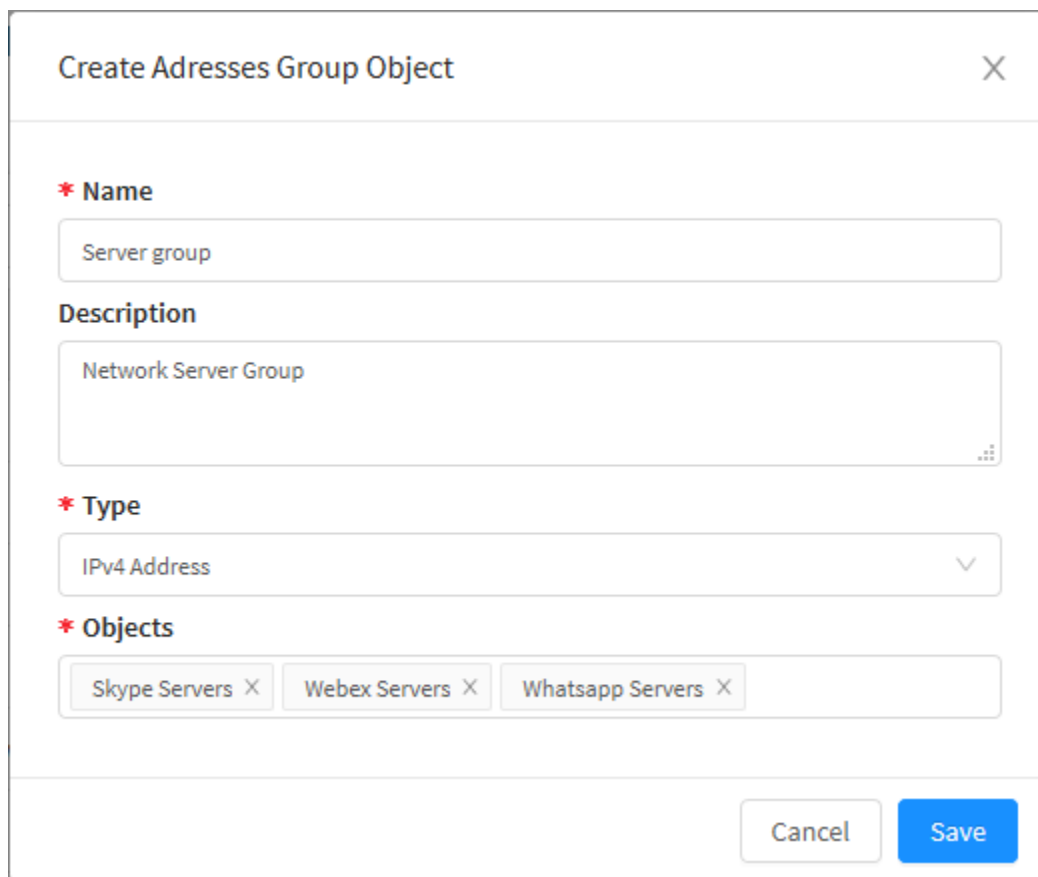
Através do botão "Create Group" é possível criar um novo grupo de objeto. Para acessar, siga os passos:

1. No menu de ações [], clique na opção "Create Group";



Objects – Addresses – Create Group

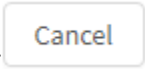
2. Preencha as informações da tela *Create Addresses Group Object*:

A screenshot of a web form titled 'Create Addresses Group Object' with a close button (X) in the top right corner. The form contains four sections: 1. 'Name' with a red asterisk, a text input field containing 'Server group'. 2. 'Description' with a text area containing 'Network Server Group'. 3. 'Type' with a red asterisk, a dropdown menu showing 'IPv4 Address'. 4. 'Objects' with a red asterisk, a container with three tags: 'Skype Servers', 'Webex Servers', and 'Whatsapp Servers', each with a close button (X). At the bottom right are 'Cancel' and 'Save' buttons.

Objects – Create Addresses Group Object

- **Name:** Nome do grupo de objetos. Ex.: *Server group*;
- **Description:** Este campo é destinado para a descrição do grupo. Ex.: *Network Server Group*;
- **Type:** Tipo do objeto de conexão, podendo optar entre: *IPv4 Address*, *IPv6 Address*, *MAC Address* e *FQDN Address*;

- **Objects:** Permite selecionar os objetos que foram adicionados previamente em [Objects - Addresses - Menu de ações - Create Object](#). Os objetos adicionados neste campo serão inseridos como *tags*.

Clique no botão **Cancel**  para Cancelar ou no botão **Save**  para salvar.

 **Settings successfully changed!**
Settings successfully changed

O grupo foi criado com sucesso.

Objects - Addresses - Menu de ações - Delete Object

Através do botão "Delete Object" é possível deletar objetos ou grupos de objetos. Para deletar pelo menu de ações, siga os seguintes passos:

1. Selecione qual(is) pacote(s) deseja deletar clicando no **checkbox** ☐ .Ex.: Test;

Objects

Addresses Services Times Schedules Dictionaries Contents

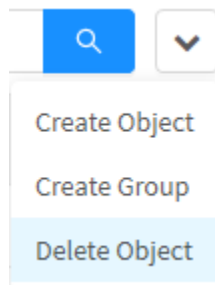
10 records

☐	Name	Description	Type	Used	Actions
☐	Class A network	Reserved network Class A 10.0.0.0/8	IPv4	-	
☐	Class B network	Reserved network Class B 172.16.0.0/12	IPv4	-	
☐	Class C network	Reserved network Class C 192.168.0.0/16	IPv4	-	
☐	Localhost	Loopback 127.0.0.1	IPv4	-	
☐	Private class network	Special-use address reserved to private network (...)	IPv4	-	
☐	Server group	Network Server Group	GROUP IP	-	
☐	Skype Servers		IPv4	-	
☒	Test	Test	IPv4	-	
☐	Webex Servers		IPv4	-	
☐	Whatsapp Servers		IPv4	-	

< 1 > 10 / page

Objects - Objetos selecionados para deleção

2. Entre no **menu de ações** e clique no botão "Delete Object".



Objects - Menu de ações - Delete Object

3. Surgirá a mensagem se deseja realmente deletar os grupos ou objetos selecionados:

Confirm delete

X

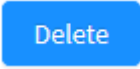
Are you sure you want to delete the following objects address?

- Test

Cancel

Delete

Objects - Are you sure you want to delete the following objects address

Caso deseje cancelar clique no botão **Cancel**. Para concluir, clique no botão **Delete**.

 **Object deleted successfully!**
Object deleted successfully

Após realizar esses procedimentos os pacotes terão sido excluídos com sucesso.

Objects - Addresses - Colunas

Na aba “Addresses” é possível visualizar o menu de ações e seis colunas:

Objects

Addresses Services Times Schedules Dictionaries Contents

9 records

☐	Name	Description	Type	Used	Actions
☐	Class A network	Reserved network Class A 10.0.0.0/8	IPv4	1	
☐	Class B network	Reserved network Class B 172.16.0.0/12	IPv4	-	
☐	Class C network	Reserved network Class C 192.168.0.0/16	IPv4	-	
☐	Localhost	Loopback 127.0.0.1	IPv4	-	
☐	Private class network	Special-use address reserved to private network (A...	IPv4	-	
☐	Skype Servers		IPv4	-	
☐	Teste endereço		IPv4	-	
☐	Webex Servers		IPv4	-	
☐	Whatsapp Servers		IPv4	-	

< 1 > 10 / page

Objects – Aba Addresses.

A seguir explicaremos cada coluna da aba Addresses:

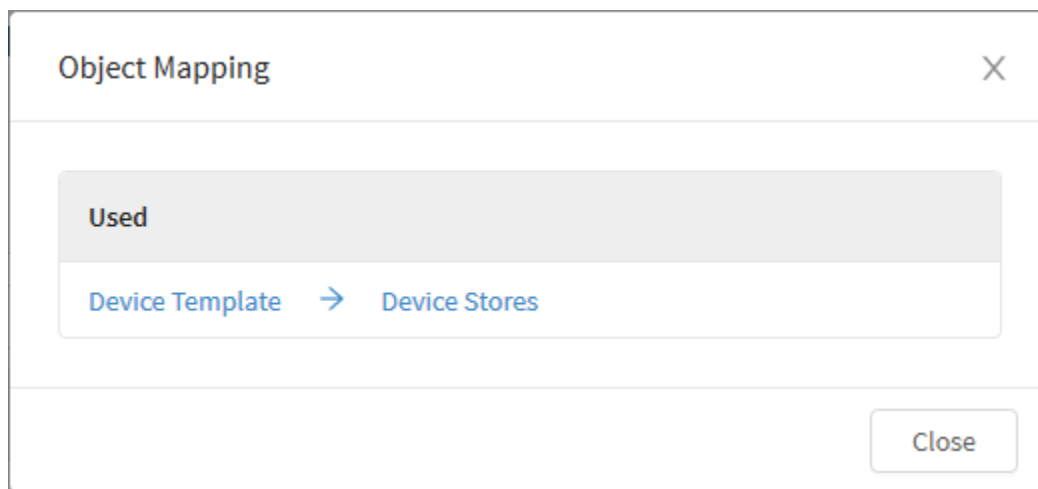
- **Selecionar**: Seleciona os Objetos desejados;
- **Name**: Nome do Objeto;
- **Description**: Apresenta a descrição do Objeto;
- **Type**: Tipo do Objeto;
- **Used**: Enumera o número de vezes que este objeto está sendo utilizado. Ao clicar neste número a janela [Object Mapping](#) é exibida.
- **Actions**: Permite editar, selecionar e deletar o objeto;
 - **Edit**: Permite editar as configurações do Objeto adicionado na opção [Create Object](#) do menu de ações;
 - **Deletar**: Permite remover o Objeto.

Objects - Addresses - Object Mapping

Ao clicar no ícone de quantas vezes um objeto foi utilizado [¹] a janela *Object Mapping* é exibida.

A função da janela *object mapping* é exibir onde o objeto foi utilizado.

No exemplo abaixo, o objeto foi utilizado no *Template* de *device* nomeado *Device Stores*.



Object Mapping

Além disso, ao clicar no *link*, é feito um redirecionamento diretamente para onde o objeto está sendo utilizado.

Objects - Services

Nesta tela temos o painel administrativo dos objetos *Services*, que compõe porta e protocolos.

Em sua configuração inicial, por padrão, o sistema traz alguns objetos (portas/protocolos) pré-cadastrados, os objetos referentes aos protocolos e serviços mais comuns: Exemplo: "*DHCP*", "*DNS*", "*HTTP*", "*HTTPS*".

Todos esses objetos estão disponíveis para serem usados nos processos de configuração e habilitação dos serviços. Os objetos de serviços podem ser compostos por um conjunto de protocolos e serviços diferentes, também é possível criar grupos contendo diversos objetos de serviços como um recurso comum para ser aplicado em qualquer funcionalidade do Blockbit UTM, ex.: "Políticas de *compliance*", "*Services*", entre outras.

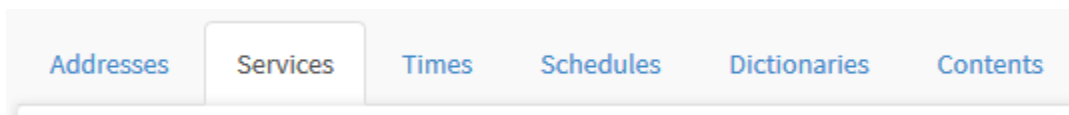
Os objetos do tipo *Services* identificam protocolos e aplicações baseadas em suas portas *TCP*, *UDP*, *IP* e *ICMP*.

Para acessar a tela, selecione o botão "*Objects*".



Botão "*Objects*"

Clique na aba "*Services*".



Aba *Services*

Surgirá a tela "*Services*". Ela é composta pelas colunas "*Select*", "*Name*", "*Description*", "*Type*", "*Used*" e "*Actions*". Além disso, no topo da tela está localizada a **barra de busca** e o **menu de ações** à direita.

Objects					
Addresses Services Times Schedules Dictionaries Contents					
51 records 🔍					
☐	Name	Description	Type	Used	Actions
☐	AH		SERVICE	1	✎ 🗑
☐	AOL		SERVICE	-	✎ 🗑
☐	BGP		SERVICE	-	✎ 🗑
☐	DHCP		SERVICE	-	✎ 🗑
☐	DNS		SERVICE	-	✎ 🗑
☐	ESP		SERVICE	-	✎ 🗑
☐	FTP		SERVICE	-	✎ 🗑
☐	GRE		SERVICE	-	✎ 🗑
☐	H323		SERVICE	-	✎ 🗑
☐	HTTP		SERVICE	-	✎ 🗑
< 1 2 3 4 5 6 > 10 / page					

Objects – Services

Explicaremos em detalhes o [menu de ações](#) e posteriormente as colunas da aba "Services".

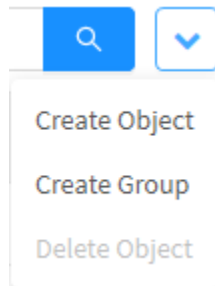
Objects - Services - Menu de ações

No topo direito da tela temos o menu de ações:



Objects – Botão do menu de ações.

Ao clicar neste botão o menu abaixo é exibido:



Objects – Menu de ações.

O menu é composto das seguintes opções:

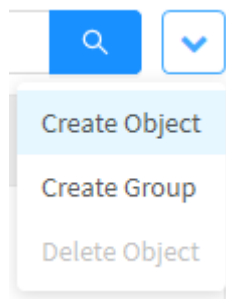
- [Create Object](#);
- [Create Group](#);
- [Delete Object](#).

A seguir cada opção do menu de ações será detalhada.

Objects - Services - Menu de ações - Create Object

Através da opção "Create Object" é possível configurar o objeto de acordo com as definições das políticas que pretende aplicar para os *hosts* específicos. Para criar um novo *Object Services*, siga os passos:

1. No menu de ações [], clique na opção "Create Object";



Objects – Services – Create Object

2. Surgirá a tela *Create Service Objects*.

Create Services Object

X

* Name

* Protocol Type

TCP

▼

* Port Type

Source/Destination

▼

Port

Source port

Destination port

+

▼

-

Description

Cancel

Save

Objects – Services – Create Service Objects

Segue alguns exemplos sobre como criar objetos de endereço:

- [Exemplo 1 - Criando objeto de serviço.](#)
- [Exemplo 2 - Criando objeto de serviço VPN Client utilizando MAC iOS;](#)

Abaixo alguns apontamentos quanto à seleção dos tipos de protocolos em alguns campos do formulário.

Protocol Type

O administrador pode selecionar entre os tipos de protocolo para compor o objeto, esta seleção permite determinar diferentes protocolos e agrupá-los no mesmo objeto:

*** Protocol Type**

TCP

TCP

UDP

IP

ICMP V4

ICMP V6

Objects – Services – Protocol Type

Segue as opções desta caixa de seleção:

- **TCP:** Associa-se a portas e ranges de portas referente aos diversos serviços que executem suas aplicações sob o protocolo *TCP*. Ex.: "Vpn pptp (1723), http (80), https (443), dns (53)";
- **UDP:** Associa-se a portas e ranges de portas referente os diversos serviços que executem suas aplicações sob o protocolo *UDP*. Ex.: "Vpn ike-isakmp (500), Vpn l2tp (1701), Vpn Nat-t (4500), dns (53)";
- **IP:** Associa-se a outros protocolos da camada *IP*. Ex.: "ah, esp, gre, icmp, igmp, sctp, tcp e udp";
- **ICMP v4 e ICMP v6:** Associa-se a tipos de tratamento e/ou resposta esperada referente ao tráfego do protocolo *ICMP v4* ou *ICMP v6*. Ex.: "Echo Request", "Echo Reply", "Destination unreachable", "time exceeded".

Port Type

O administrador pode selecionar entre 2(dois) tipos de portas (serviços) que vai compor o objeto.

*** Port Type**

Source/Destination

Source/Destination

Range

Objects – Services – Port Type

Segue as opções desta caixa de seleção:

- **Source/Destination:** Definição dos campos [Source port] / [Destination port], referente a serviços que normalmente seguem padrões de *RFC's* e executam o serviço uma porta específica (*Destination port*), geralmente em serviços que executam sob o protocolo *TCP*. Ex. "HTTP (80); HTTPS (443), DNS (53)". Existem casos de serviços que também executam sob o protocolo *UDP*. Ex. "DNS (53)";
- **Range:** Definição das portas ou serviços que executam normalmente dentro de uma classe de portas [Initial port] / [End port], geralmente em serviços que executam sob o protocolo *UDP*. Serviços que normalmente executam em ranges de portas. Ex.: "VOIP - porta inicial 4500/UDP; porta final 5500/UDP.; Câmeras – porta inicial 10000/UDP; porta final 20000/UDP".



O campo **[Source port]** é um campo opcional. Geralmente é executada sob uma porta alta [1024:65535] aleatória executa no start do serviço.



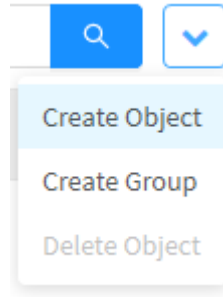
O Range de portas mesmo para aplicações do mesmo tipo pode variar de acordo a especificação de cada aplicativo.

Objects - Exemplo 1 - Criando objeto de serviço

Através da opção “*Create Object*” é possível criar um novo *Object Services*. Para acessar, siga os passos:



1. No menu de ações [], clique na opção “*Create Object*”;



Objects – Services – Create Object

2. Surgirá a tela *Create Service Objects*. Preencha os campos:

Create Services Object

X

* Name

Protocol TCP/UDP

* Protocol Type

IP

* Protocol

tcp

ip/udp

ip/tcp

+

-

Description

Protocol TCP/UDP

Cancel

Save

- **Name:** Nome do objeto. Ex.: *HTTP*;
- **Protocol Type:** Seleciona o protocolo do objeto, entre as opções: "*TCP*", "*UDP*", "*IP*" e "*ICMP*". Ex.: *TCP*;
- **Port Type:** Determina se o tipo da porta será de origem/destino ou dentro um *range* de *IP*. Caso tenha selecionado a opção *range*, será necessário determinar o intervalo nos campos de texto a seguir;
- **Port:** Determina a porta de origem e de destino dos endereços, para serem adicionados na lista dos objetos de serviço;
- **List:** Lista as portas adicionadas. Para excluir algum valor inserido, selecione-o e clique no botão [], caso contrário clique no botão [] para fazer uma adição na lista;
- **Description:** Descrição do objeto. Ex.: *HTTP Protocol*.

Clique no botão **Cancel** [] para Cancelar. Clique no botão **Save** [] para salvar.

 **Object successfully changed!**
Object successfully changed

O objeto de serviço foi criado com sucesso.

Objects - Exemplo 2 - Criando objeto de serviço VPN Client utilizando MAC iOS

Vamos exemplificar o cadastro de um Objeto de serviço para aplicação *VPN Client* utilizando *MAC iOS*. Ex.: “VPN iOS X Server – Portas 500/UDP; 1701 /UDP; 4500/UDP; 1723/TCP”.

Create Services Object

*

Name

VPN iOS X SERVER

*

Protocol Type

TCP

*

Port Type

Source/Destination

Port

Source port

Destination port

+

tcp/1723 Destination

udp/500 Destination

udp/1701 Destination

udp/4500 Destination

−

Description

VPN iOS X SERVER

Cancel

Save

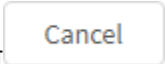
Object Service - VPN iOS X Server

- **Name:** Nome do objeto. Ex.: VPN iOS X SERVER;
- **Protocol Type:** Seleciona o protocolo do objeto, entre as opções: “TCP”, “UDP”, “IP” e “ICMP”. Neste exemplo usaremos o protocolo *TCP* e *UDP*;
- **Port Type:** Determina se o tipo da porta será de origem/destino ou dentre um *range* de *IP*. Caso tenha selecionado a opção *range*, será necessário determinar o intervalo nos campos de texto a seguir. Neste exemplo será utilizado apenas a opção “*Source/Destination*”;
- **Port:** Determina a porta de origem e de destino dos endereços, para serem adicionados na lista dos objetos de serviço. Neste exemplo usaremos especificamente as portas de destino, conforme demonstrado na imagem, adicione:



- **Protocol Type:** TCP; **Destination Port:** 1723 e clique em [+] para adicionar o valor à lista;

- **Protocol Type:** UDP; **Destination Port:** 500 e clique em  para adicionar o valor à lista;
- **Protocol Type:** UDP; **Destination Port:** 1701 e clique em  para adicionar o valor à lista;
- **Protocol Type:** UDP; **Destination Port:** 4500 e clique em  para adicionar o valor à lista.
- **List:** Lista as portas adicionadas. Para excluir algum valor inserido, selecione-o e clique no botão , caso contrário clique no botão  para fazer uma adição na lista. Após o passo anterior, devemos ter 4 inserções já listadas, conforme demonstrado na imagem;
- **Description:** Descrição do objeto. Ex.: VPN IOS X SERVER.

Clique no botão **Cancel**  para Cancelar. Clique no botão **Save**  para salvar.

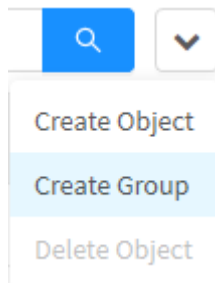
 **Object successfully changed!**
Object successfully changed

O objeto de serviço foi criado com sucesso.

Objects - Services - Menu de ações - Create Group

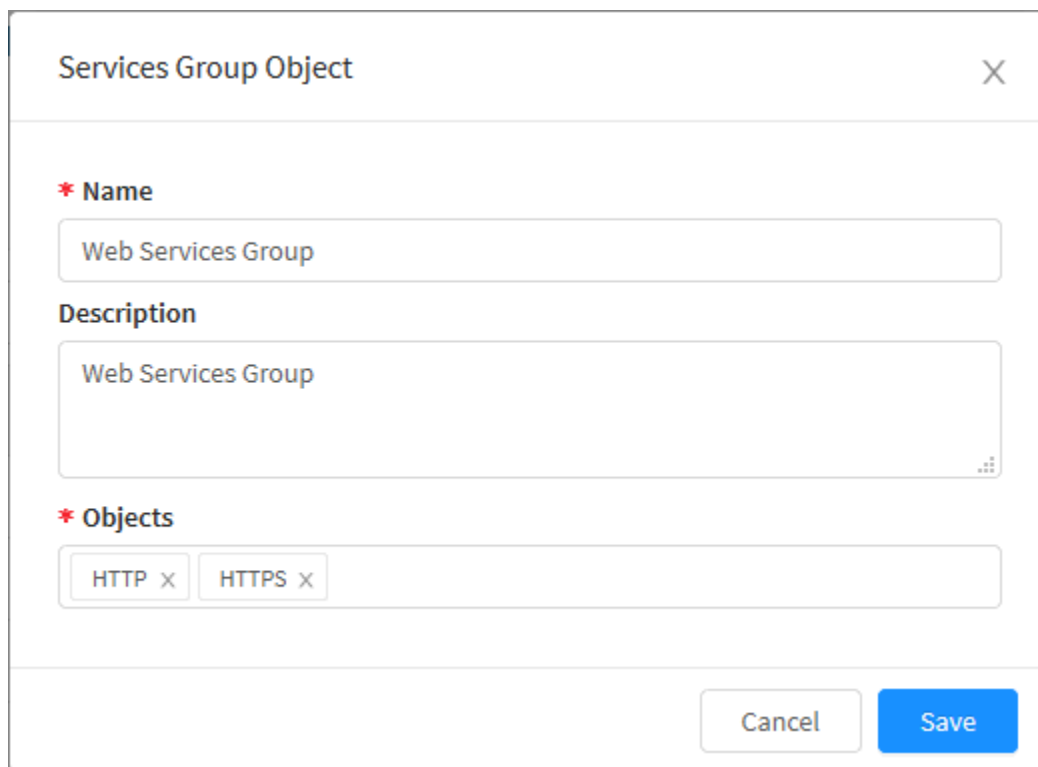
Através do botão "Create Group" é possível criar um novo grupo de objeto. Para acessar, siga os passos:

1. No menu de ações [], clique na opção "Create Group";



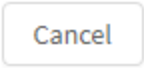
Objects – Services – Create Group

2. Preencha as informações da tela *Services Group Object*:

A screenshot of a web form titled 'Services Group Object' with a close button (X) in the top right corner. The form contains three main sections: 1. 'Name' (required, marked with a red asterisk) with a text input field containing 'Web Services Group'. 2. 'Description' with a larger text area containing 'Web Services Group'. 3. 'Objects' (required, marked with a red asterisk) with a container showing two tags: 'HTTP' and 'HTTPS', each with a close button (X). At the bottom right of the form are two buttons: 'Cancel' and 'Save'.

Objects – Services Group Object

- **Name:** Nome do grupo de objetos. Ex.: *Web Services group*;
- **Description:** Este campo é destinado para a descrição do grupo. Ex.: *Web Services Group*;
- **Objects:** Permite selecionar os objetos que foram adicionados previamente em [Objects - Services - Menu de ações - Create Object](#). Os objetos adicionados neste campo serão inseridos como *tags*.

A rectangular button with a thin grey border and the word "Cancel" in a grey sans-serif font.A solid blue rectangular button with the word "Save" in a white sans-serif font.

Clique no botão **Cancel** para Cancelar ou no botão **Save** para salvar.



Settings successfully changed!

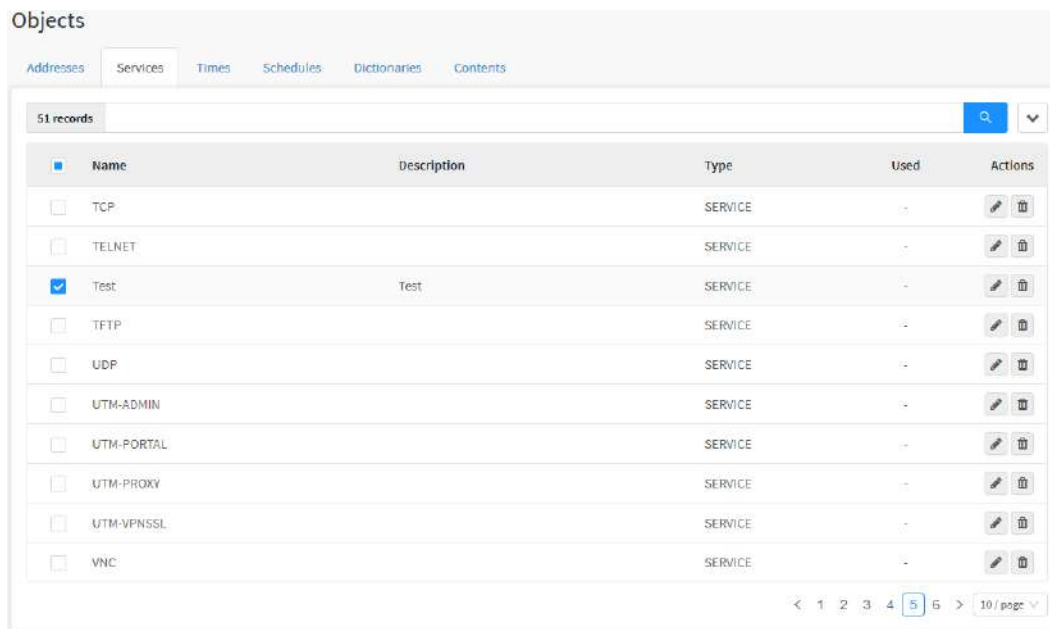
Settings successfully changed

O grupo foi criado com sucesso.

Objects - Services - Menu de ações - Delete Object

Através do botão "Delete Object" é possível deletar objetos ou grupos de objetos. Para deletar pelo menu de ações, siga os seguintes passos:

1. Selecione qual(is) pacote(s) deseja deletar clicando no **checkbox** ☐ .Ex.: Test;

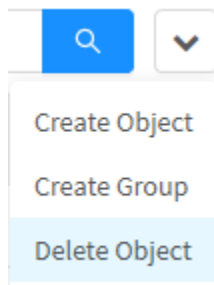


The screenshot shows the 'Objects' management interface. At the top, there are tabs for 'Addresses', 'Services', 'Times', 'Schedules', 'Dictionaries', and 'Contents'. Below the tabs, there is a search bar and a dropdown menu. The main area displays a table with 51 records. The table has columns for 'Name', 'Description', 'Type', 'Used', and 'Actions'. The 'Test' service is selected with a checkbox.

Name	Description	Type	Used	Actions
TCP		SERVICE	-	
TELNET		SERVICE	-	
☒ Test	Test	SERVICE	-	
TFTP		SERVICE	-	
UDP		SERVICE	-	
UTM-ADMIN		SERVICE	-	
UTM-PORTAL		SERVICE	-	
UTM-PROXY		SERVICE	-	
UTM-VPNSSL		SERVICE	-	
VNC		SERVICE	-	

Objects - Objetos selecionados para deleção

2. Entre no **menu de ações**  e clique no botão "Delete Object".



Objects - Menu de ações - Delete Object

3. Surgirá a mensagem se deseja realmente deletar os grupos ou objetos selecionados:

Confirm delete

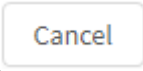
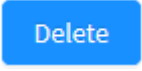
X

Are you sure you want to delete the object service Test?

Cancel

Delete

Objects - Are you sure you want to delete the object service?

Caso deseje cancelar clique no botão **Cancel**. Para concluir, clique no botão **Delete**.

 **Object deleted successfully!**
Object deleted successfully

Após realizar esses procedimentos os pacotes terão sido excluídos com sucesso.

Objects - Services - Colunas

Na aba "Services" é possível visualizar o menu de ações e seis colunas:

☐	Name	Description	Type	Used	Actions
☐	AH		SERVICE	1	
☐	AOL		SERVICE	-	
☐	BGP		SERVICE	-	
☐	DHCP		SERVICE	-	
☐	DNS		SERVICE	-	
☐	ESP		SERVICE	-	
☐	FTP		SERVICE	-	
☐	GRE		SERVICE	-	
☐	H323		SERVICE	-	
☐	HTTP		SERVICE	-	

Objects – Aba Services

A seguir explicaremos cada coluna da aba Services:

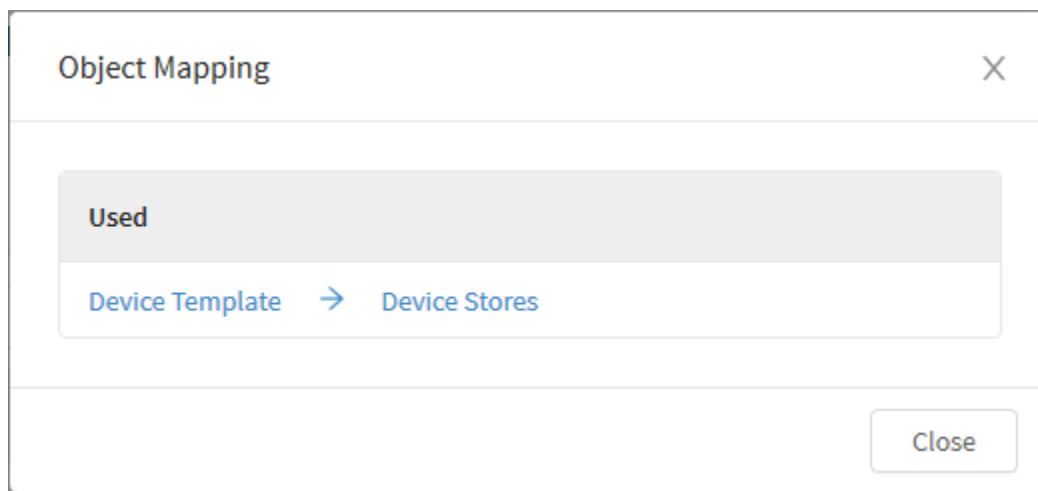
- **Selecionar** : Seleciona os Objetos desejados;
- **Name**: Nome do Objeto;
- **Description**: A descrição do Objeto;
- **Type**: Tipo do Objeto;
- **Used** : Enumera o número de vezes que este objeto está sendo utilizado. Ao clicar neste número a janela [Object Mapping](#) é exibida.
- **Actions**: Permite editar, selecionar e deletar o objeto;
 - **Edit** : Permite editar as configurações do Objeto adicionado na opção [Create Object](#) do menu de ações;
 - **Deletar** : Permite remover o Objeto.

Objects - Services - Object Mapping

Ao clicar no ícone de quantas vezes um objeto foi utilizado [¹] a janela *Object Mapping* é exibida.

A função da janela *object mapping* é exibir onde o objeto foi utilizado.

No exemplo abaixo, o objeto foi utilizado no *Template* de *device* nomeado *Device Stores*.



Object Mapping

Além disso, ao clicar no *link*, é feito um redirecionamento diretamente para onde o objeto está sendo utilizado.

Objects - Time

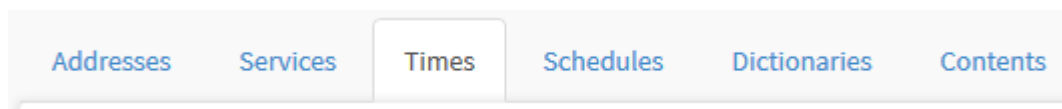
Os objetos do tipo *Time* são compostos pelos “dias da semana” e a “hora inicial e final”. Ex.: “Horário Comercial – início: segunda-feira de 8:00 AM até sexta-feira às 6:00 PM.

Para acessar a tela, basta selecionar o botão “*Objects*”.



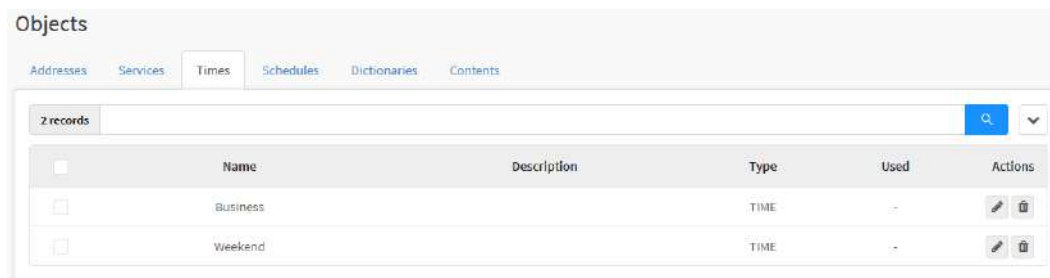
Botão “*Objects*”

Clique na aba “*Time*”.



Aba “*Time*”

Surgirá a tela “*Time*”. Ela é composta pelas colunas “*Select*”, “*Name*”, “*Description*”, “*Type*”, “*Used*” e “*Actions*”. Além disso, no topo da tela está localizada a [barra de busca](#) e o [menu de ações](#) à direita.



	Name	Description	Type	Used	Actions
☐	Business		TIME	-	 
☐	Weekend		TIME	-	 

Objects - Time

Explicaremos em detalhes o [menu de ações](#) e posteriormente as colunas da aba “*Time*”.

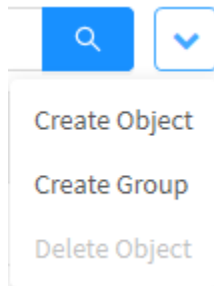
Objects - Time - Menu de ações

No topo direito da tela temos o menu de ações:



Objects – Botão do menu de ações.

Ao clicar neste botão o menu abaixo é exibido:



Objects – Menu de ações.

O menu é composto das seguintes opções:

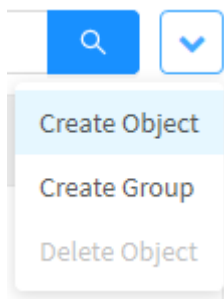
- [Create Object](#);
- [Create Group](#);
- [Delete Object](#).

A seguir cada opção do menu de ações será detalhada.

Objects - Time - Menu de ações - Create Object

Através da opção "Create Object" é possível criar um novo *object Time*. Para acessar, siga os passos:

1. No menu de ações [], clique na opção "Create Object";



Objects – Time – Create Object

2. Surgirá a tela *Create Time Objects*. Preencha os campos:

Create Times Object

*

Name

Working hours

*

Weekday

Monday X Tuesday X Wednesday X Thursday X Friday X

Start / End time

Select time

Select time

+

08:00-23:59

^

↓

-

Description

Business Day/hours

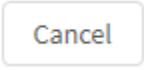
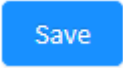
Cancel

Save

- **Name:** Nome do objeto. Ex.: *Working hours*;
- **Weekday:** Permite selecionar os dias da semana. Ex.: *"Monday"*, *"Tuesday"*, *"Wednesday"*, *"Thursday"* e *"Friday"*;
- **Start / End time:** Define as faixas de hora do objeto. O tempo final não pode ser mais cedo do que o tempo inicial e vice versa. Ex.: *"08:00 – 23:59"*;

- **List:** Lista os horários adicionados. Para excluir algum valor inserido, selecione-o e clique no botão [], caso contrário clique no botão [] para fazer uma adição na lista;

- **Description:** Descrição do objeto. Ex.: *HTTP Protocol*.

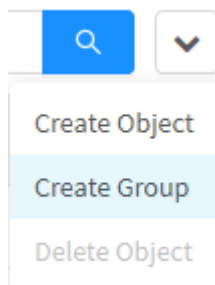
Clique no botão **Cancel** [] para Cancelar. Clique no botão **Save** [] para salvar.

O *object time* foi criado com sucesso.

Objects - Time - Menu de ações - Create Group

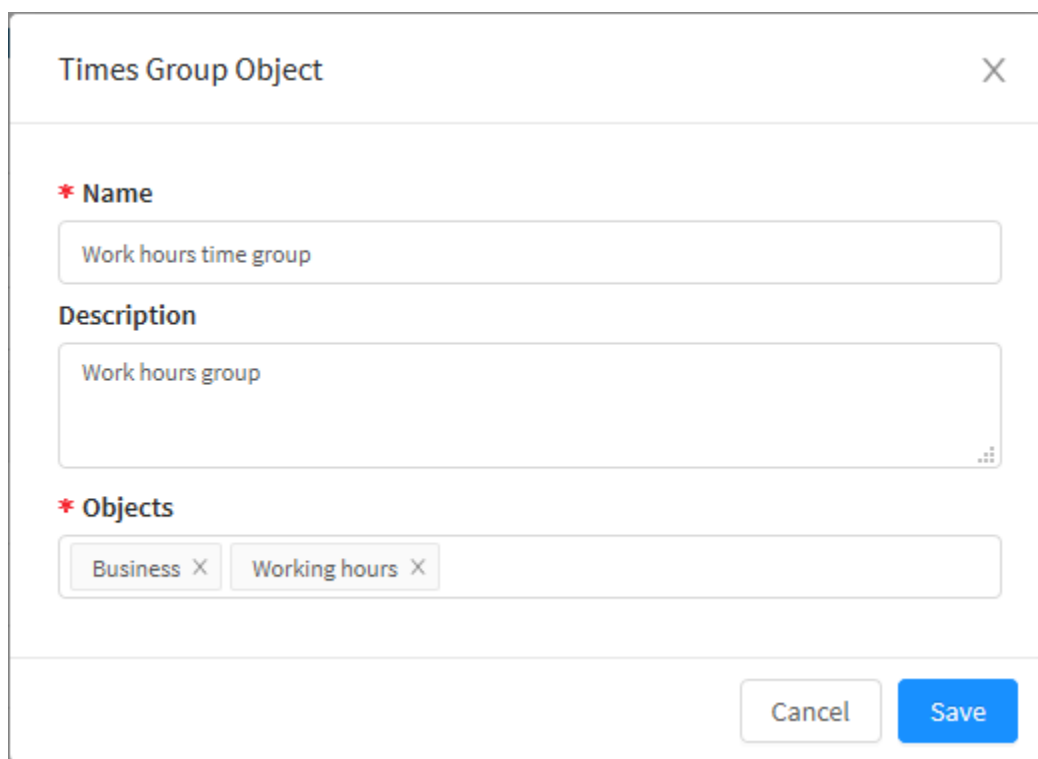
Através do botão "Create Group" é possível criar um novo grupo de objeto. Para acessar, siga os passos:

1. No menu de ações [], clique na opção "Create Group";



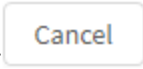
Objects – Time – Create Group

2. Preencha as informações da tela *Time Group Object*:

A screenshot of a web form titled 'Times Group Object' with a close button (X) in the top right corner. The form contains three sections: 1. 'Name' with a red asterisk, a text input field containing 'Work hours time group', and a label 'Name' in bold. 2. 'Description' with a text area containing 'Work hours group' and a label 'Description' in bold. 3. 'Objects' with a red asterisk, a multi-select field containing 'Business' and 'Working hours' (each with a close 'X' button), and a label 'Objects' in bold. At the bottom right are 'Cancel' and 'Save' buttons.

Objects – Time Group Object

- **Name:** Nome do grupo de objetos. Ex.: *Work hours time group*;
- **Description:** Este campo é destinado para a descrição do grupo. Ex.: *Work hours group*;
- **Objects:** Permite selecionar os objetos que foram adicionados previamente em [Objects - Time - Menu de ações - Create Object](#). Os objetos adicionados neste campo serão inseridos como *tags*.



Clique no botão **Cancel** para Cancelar ou no botão **Save** para salvar.



Saved successfully

Saved successfully

O grupo foi criado com sucesso.

Objects - Time - Menu de ações - Delete Object

Através do botão "Delete Object" é possível deletar objetos ou grupos de objetos. Para deletar pelo menu de ações, siga os seguintes passos:

1. Selecione qual(is) pacote(s) deseja deletar clicando no **checkbox** ☐. Ex.: Test;

Objects

[Addresses](#)[Services](#)[Times](#)[Schedules](#)[Dictionaries](#)[Contents](#)

5 records

	Name	Description	Type	Used	Actions
☐	Business		TIME	-	
☒	Test	test	TIME	-	
☐	Weekend		TIME	-	
☐	Work hours time group	Work hours group	GROUP	-	
☐	Working hours	Business Day/hours	TIME	-	

<

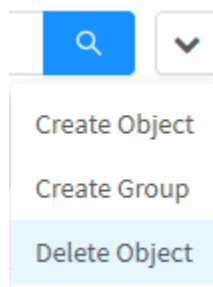
1

>

10 / page

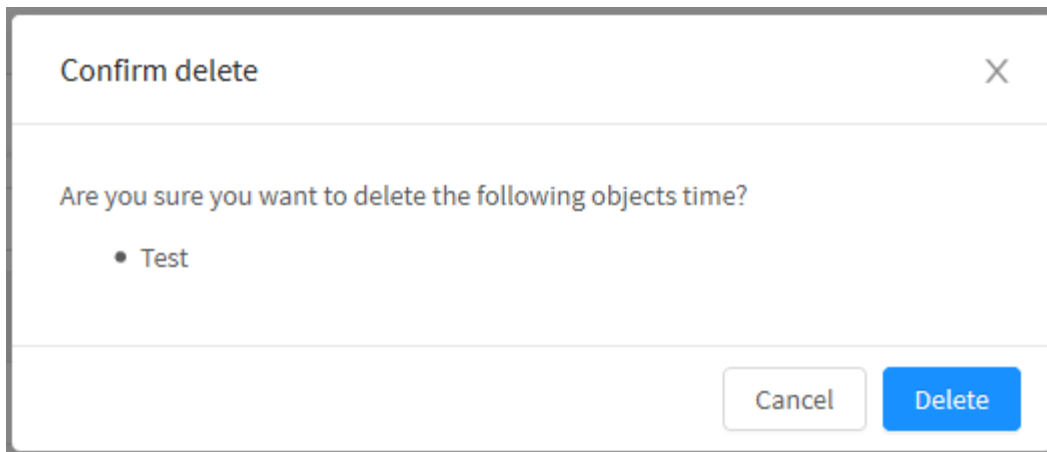
Objects - Objetos selecionados para deleção

2. Entre no **menu de ações**  e clique no botão "Delete Object".

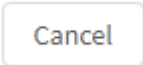
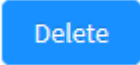


Objects - Menu de ações - Delete Object

3. Surgirá a mensagem se deseja realmente deletar os grupos ou objetos selecionados:



Objects - Are you sure you want to delete the following object time?

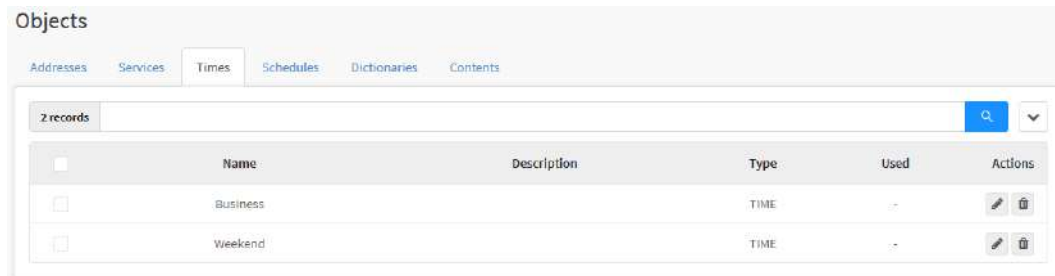
Caso deseje cancelar clique no botão **Cancel** . Para concluir, clique no botão **Delete** .

 **Object deleted successfully!**
Object deleted successfully

Após realizar esses procedimentos os pacotes terão sido excluídos com sucesso.

Objects - Time - Colunas

Na aba "Time" é possível visualizar o menu de ações e seis colunas:



Addresses	Services	Times	Schedules	Dictionaries	Contents
2 records					
☐	Name	Description	Type	Used	Actions
☐	Business		TIME	-	
☐	Weekend		TIME	-	

Objects – Aba Time

A seguir explicaremos cada coluna da aba *Time*:

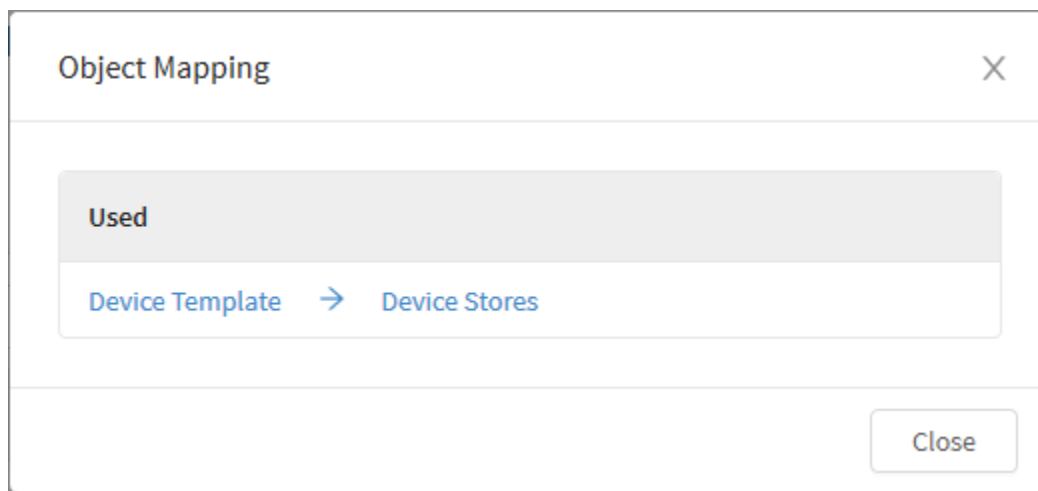
- **Selecionar** : Seleciona os Objetos desejados;
- **Name**: Nome do Objeto;
- **Description**: A descrição do Objeto;
- **Type**: Tipo do Objeto;
- **Used** : Enumera o número de vezes que este objeto está sendo utilizado. Ao clicar neste número a janela [Object Mapping](#) é exibida.
- **Actions**: Permite editar, selecionar e deletar o objeto;
 - **Edit** : Permite editar as configurações do Objeto adicionado na opção [Create Object](#) do menu de ações;
 - **Deletar** : Permite remover o Objeto.

Objects - Time - Object Mapping

Ao clicar no ícone de quantas vezes um objeto foi utilizado [¹] a janela *Object Mapping* é exibida.

A função da janela *object mapping* é exibir onde o objeto foi utilizado.

No exemplo abaixo, o objeto foi utilizado no *Template* de *device* nomeado *Device Stores*.



Object Mapping

Além disso, ao clicar no *link*, é feito um redirecionamento diretamente para onde o objeto está sendo utilizado.

Objects - Schedules

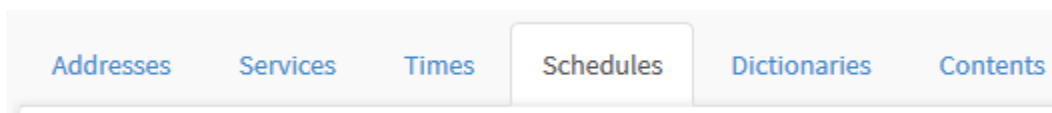
Os objetos do tipo *Schedules* são compostos pelas definições de um período que compete "Data/hora inicial" e "Data/hora final". Ex.: 2017-05-11 8:00 AM até 2017-05-30 5:00 PM.

Para acessar a tela, basta selecionar o botão "*Objects*".



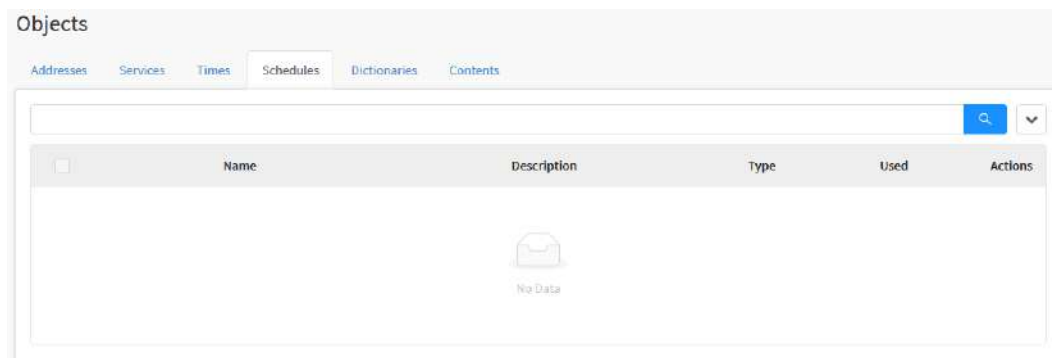
Botão "*Objects*"

Clique na aba "*Schedules*".



Aba *Schedules*

Surgirá a tela "*Schedules*". Ela é composta pelas colunas "*Select*", "*Name*", "*Description*", "*Type*", "*Used*" e "*Actions*". Além disso, no topo da tela está localizada a [barra de busca](#) e o [menu de ações](#) à direita.



Objects - Schedules

Explicaremos em detalhes o [menu de ações](#) e posteriormente as colunas da aba "*Schedules*".

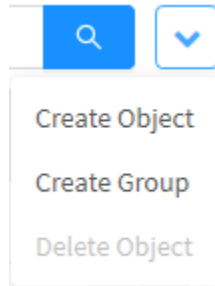
Objects - Schedules - Menu de ações

No topo direito da tela temos o menu de ações:



Objects – Botão do menu de ações.

Ao clicar neste botão o menu abaixo é exibido:



Objects – Menu de ações.

O menu é composto das seguintes opções:

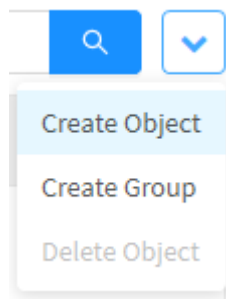
- [Create Object](#);
- [Create Group](#);
- [Delete Object](#).

A seguir cada opção do menu de ações será detalhada.

Objects - Schedules - Menu de ações - Create Object

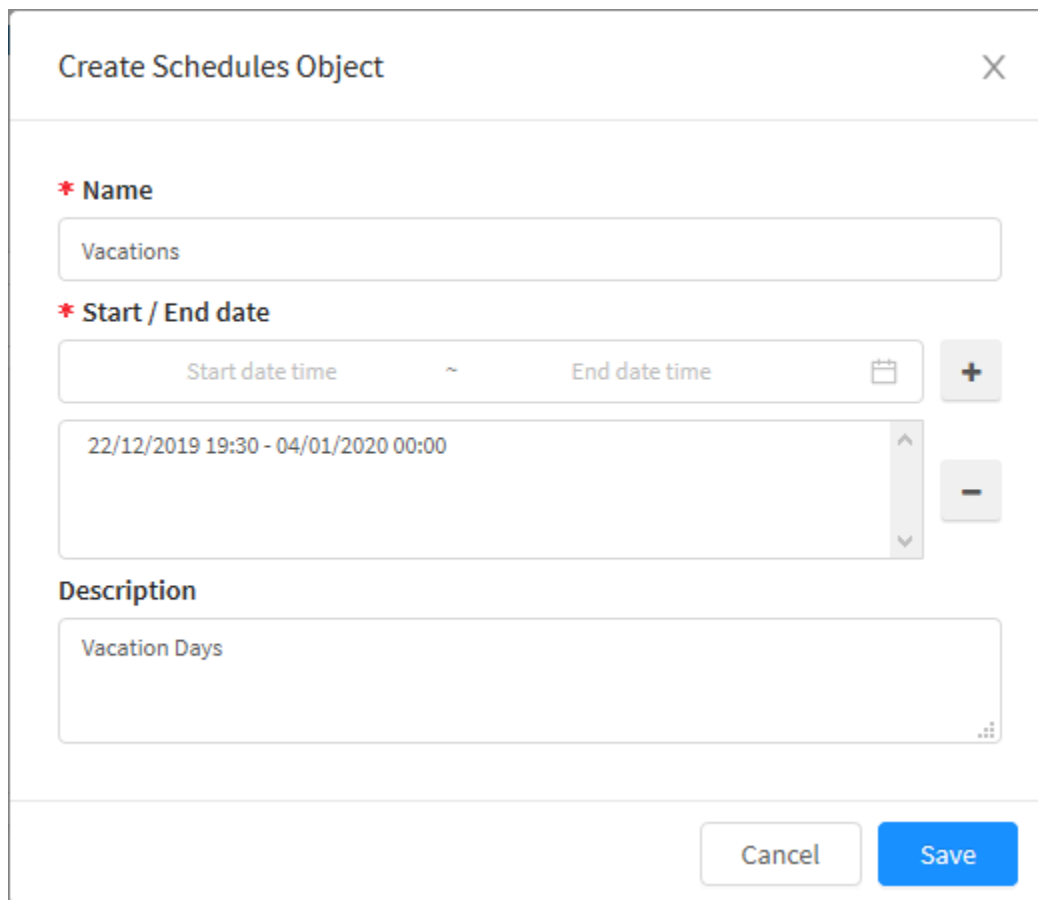
Através da opção "Create Object" é possível criar um novo *object Schedules*. Para acessar, siga os passos:

1. No menu de ações [], clique na opção "Create Object";



Objects – Schedules – Create Object

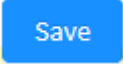
2. Surgirá a tela *Create Schedule Objects*. Preencha os campos:

A screenshot of a web form titled 'Create Schedules Object'. The form has a close button (X) in the top right corner. It contains three main sections: 1. 'Name' with a red asterisk, a text input field containing 'Vacations'. 2. 'Start / End date' with a red asterisk, a date range input field showing '22/12/2019 19:30 - 04/01/2020 00:00', and plus/minus buttons. 3. 'Description' with a text area containing 'Vacation Days'. At the bottom right are 'Cancel' and 'Save' buttons.

Schedules Objects – Create Schedules Object

- **Name:** Nome do objeto. Ex.: *Vacations*;

- **Start / End date:** Define o período que compete a data e hora inicial e a data e hora final, para adicionar clique []. Ex.: 22/12/2019 19:30 - 04/01/2020 00:00;
- **List:** Exibe a lista de períodos adicionados. Para excluir algum valor inserido, selecione-o e clique no botão [];
- **Description:** Descrição do objeto. Ex.: *Vacation Days*.

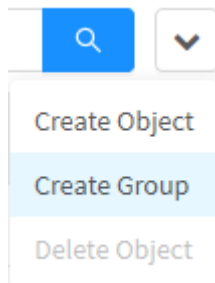
Clique no botão **Cancel** [] para Cancelar. Clique no botão **Save** [] para salvar.

O *schedule object* foi criado com sucesso.

Objects - Schedules - Menu de ações - Create Group

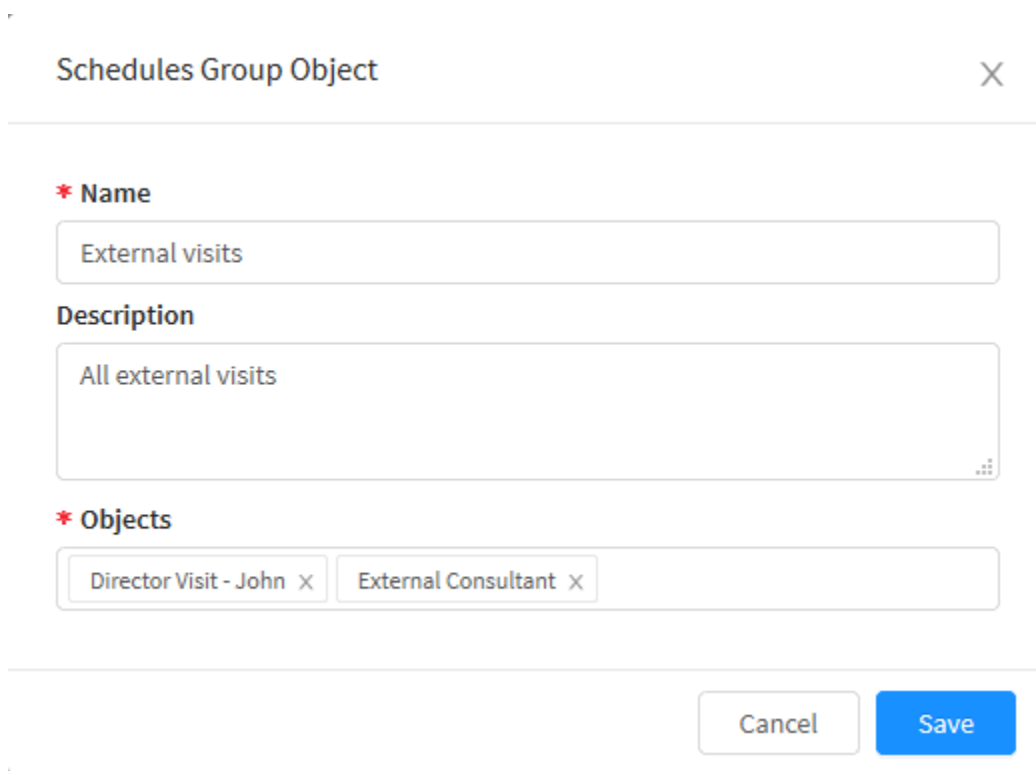
Através do botão "Create Group" é possível criar um novo grupo de objeto. Para acessar, siga os passos:

1. No menu de ações [], clique na opção "Create Group";



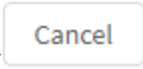
Objects – Schedules – Create Group

2. Preencha as informações da tela *Schedules Group Object*:

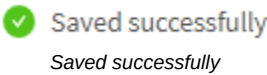
A screenshot of a web form titled 'Schedules Group Object' with a close button (X) in the top right corner. The form has three main sections: 1. 'Name' (required, marked with a red asterisk) with a text input field containing 'External visits'. 2. 'Description' with a larger text area containing 'All external visits'. 3. 'Objects' (required, marked with a red asterisk) with a container holding two tags: 'Director Visit - John' and 'External Consultant', each with a close button (X). At the bottom right of the form are two buttons: 'Cancel' and 'Save'.

Objects – Schedules Group Object

- **Name:** Nome do grupo de objetos. Ex.: *External visits*;
- **Description:** Este campo é destinado para a descrição do grupo. Ex.: *All external visits*;
- **Objects:** Permite selecionar os objetos que foram adicionados previamente em [Objects - Schedules - Menu de ações - Create Object](#). Os objetos adicionados neste campo serão inseridos como *tags*.



Clique no botão **Cancel** para Cancelar ou no botão **Save** para salvar.



O grupo foi criado com sucesso.

Objects - Schedules - Menu de ações - Delete Object

Através do botão "Delete Object" é possível deletar objetos ou grupos de objetos. Para deletar pelo menu de ações, siga os seguintes passos:

1. Selecione qual(is) pacote(s) deseja deletar clicando no **checkbox** ☐. Ex.: Test;

Objects

Addresses Services Times Schedules Dictionaries Contents

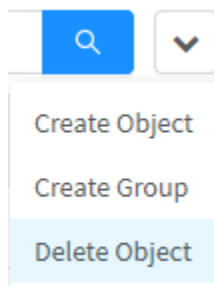
5 records

☐	Name	Description	Type	Used	Actions
☐	Director Visit - John	Director Visit	DATE	1	
☐	External Consultant	External Consultant	DATE	1	
☐	External visits	All external visits	GROUP	-	
☒	Test	Test	DATE	-	
☐	Vacations	Vacation Days	DATE	-	

< 1 > 10 / page

Objects - Objetos selecionados para deleção

2. Entre no **menu de ações** e clique no botão "Delete Object".



Objects - Menu de ações - Delete Object

3. Surgirá a mensagem se deseja realmente deletar os grupos ou objetos selecionados:

Confirm delete

X

Are you sure you want to delete the following objects schedules?

- Test

Cancel

Delete

Objects - Are you sure you want to delete the following object schedules?

Caso deseje cancelar clique no botão **Cancel**

Cancel

. Para concluir, clique no botão **Delete**

Delete

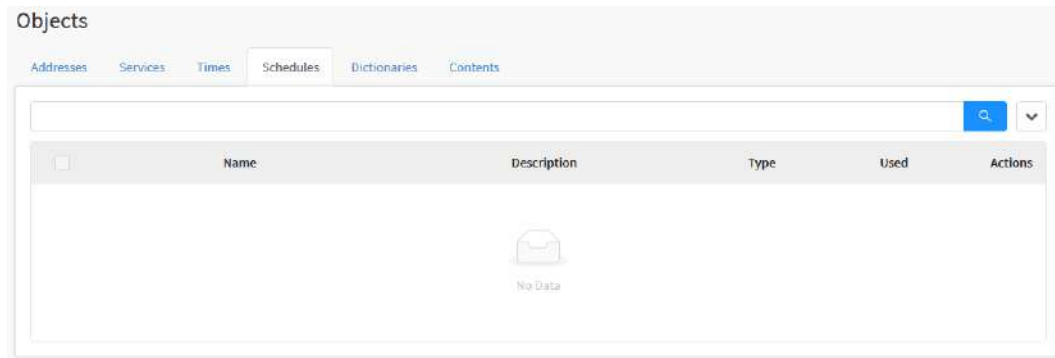
.

 **Object deleted successfully!**
Object deleted successfully

Após realizar esses procedimentos os pacotes terão sido excluídos com sucesso.

Objects - Schedules - Colunas

Na aba “Schedules” é possível visualizar o menu de ações e seis colunas:



Objects – Aba Schedules

A seguir explicaremos cada coluna da aba Schedules:

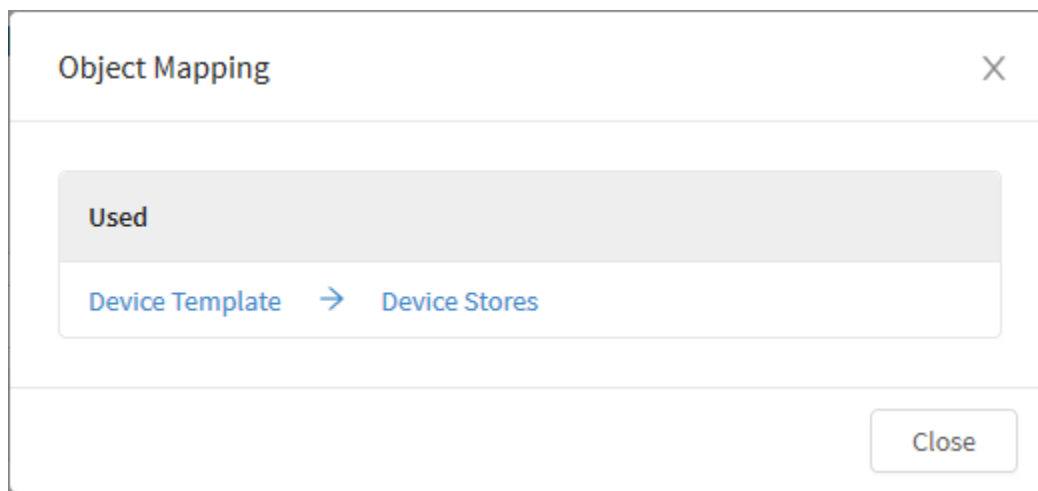
- **Selecionar**[]: Seleciona os Objetos desejados;
- **Name**: Nome do Objeto;
- **Description**: A descrição do Objeto;
- **Type**: Tipo do Objeto;
- **Used**[]: Enumera o número de vezes que este objeto está sendo utilizado. Ao clicar neste número a janela [Object Mapping](#) é exibida.
- **Actions**: Permite editar, selecionar e deletar o objeto;
 - **Edit**[]: Permite editar as configurações do Objeto adicionado na opção [Create Object](#) do menu de ações;
 - **Deletar**[]: Permite remover o Objeto.

Objects - Schedules - Object Mapping

Ao clicar no ícone de quantas vezes um objeto foi utilizado [¹] a janela *Object Mapping* é exibida.

A função da janela *object mapping* é exibir onde o objeto foi utilizado.

No exemplo abaixo, o objeto foi utilizado no *Template* de *device* nomeado *Device Stores*.



Object Mapping

Além disso, ao clicar no *link*, é feito um redirecionamento diretamente para onde o objeto está sendo utilizado.

Objects - Dictionaries

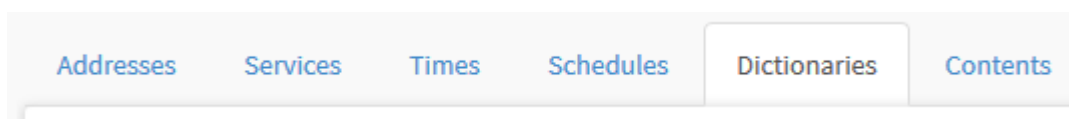
Os objetos do tipo *Dictionaries* são compostos por “listas de palavras” ou conjunto de combinações de “expressões regulares”. Ex.: “Alfanumérico”, “Endereço de E-mail”, “Link HTML”, “URL”, etc.

Para acessar a tela, basta selecionar o botão “Objects”.



Botão “Objects”

Clique na aba “Dictionaries”.



Aba *Dictionaries*

Surgirá a tela “Dictionaries”. Ela é composta pelas colunas “Select”, “Name”, “Description”, “Type”, “Used” e “Actions”. Além disso, no topo da tela está localizada a [barra de busca](#) e o [menu de ações](#) à direita.

Objects

Addresses Services Times Schedules **Dictionaries** Contents

7 records

☐	Name	Description	Type	Used	Actions
☐	Alphanumeric	Regular expression to match alphanumeric (letters...	DICTIONARY	-	
☐	Credit Card	Regular expression to match credit card numbers	DICTIONARY	-	
☐	Email Address	Regular expression to match a email address	DICTIONARY	-	
☐	IP Address	Regular expression to match a IP address	DICTIONARY	-	
☐	Link HTML	Regular expression to match HTML links (a href)	DICTIONARY	-	
☐	URL	Regular expression to match FTP and HTTP URLs	DICTIONARY	-	
☐	URL Image	Regular expression to match image URLs	DICTIONARY	-	

Objects – *Dictionaries*

Explicaremos em detalhes o [menu de ações](#) e posteriormente as colunas da aba “*Dictionaries*”.

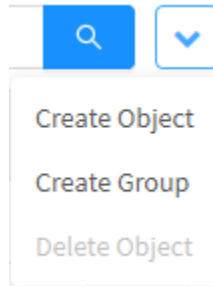
Objects - Dictionaries - Menu de ações

No topo direito da tela temos o menu de ações:



Objects – Botão do menu de ações.

Ao clicar neste botão o menu abaixo é exibido:



Objects – Menu de ações.

O menu é composto das seguintes opções:

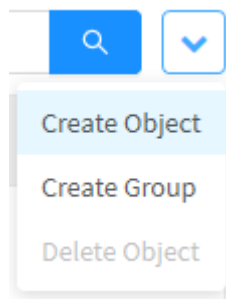
- [Create Object](#);
- [Create Group](#);
- [Delete Object](#).

A seguir cada opção do menu de ações será detalhada.

Objects - Dictionaries - Menu de ações - Create Object

Através da opção "Create Object" é possível criar um novo *object Dictionaries*. Para acessar, siga os passos:

1. No menu de ações [], clique na opção "Create Object";



Objects – Dictionaries – Create Object

2. Surgirá a tela *Create Dictionaries Objects*. Preencha os campos:

Create Dictionaries Object [X]

*** Name**

Alphanumeric

Expressions

.
\.
^
\$

*** Word**

List

[a-zA-Z\s0-9]+

Description

Regular expression to match alphanumeric.

Cancel Import Dictionary Save

Objects – Create Dictionaries Object

- **Name:** Nome do Objeto. Ex.: *Alphanumeric*;
- **Expressions:** Contempla uma lista de “*regex*”, que podemos combinar para construir uma expressão regular e adicionar à lista de palavras-chave. Selecione o código e clique [+] para adicionar no campo *Word*;
- **Word:** Este campo define a expressão regular para identificar o item desejado. Para adicionar clique [+]. Ex.: [a-zA-Z\s0-9]+;
- **List Extensions:** Exibe a lista de expressões regulares. Para excluir algum valor inserido, selecione-o e clique no botão [-];
- **Description:** Descrição do objeto. Ex.: *Regular expression to match alphanumeric*.

Caso prefira importar uma lista de expressões regulares, clique no botão **Import Dictionary** [Import Dictionary], o arquivo precisa conter um item por linha.

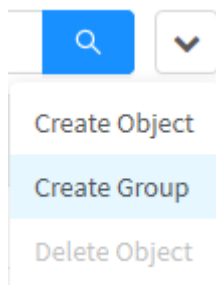
Clique no botão **Cancel** [Cancel] para Cancelar. Clique no botão **Save** [Save] para salvar.

O *dictionaries object* foi criado com sucesso.

Objects - Dictionaries - Menu de ações - Create Group

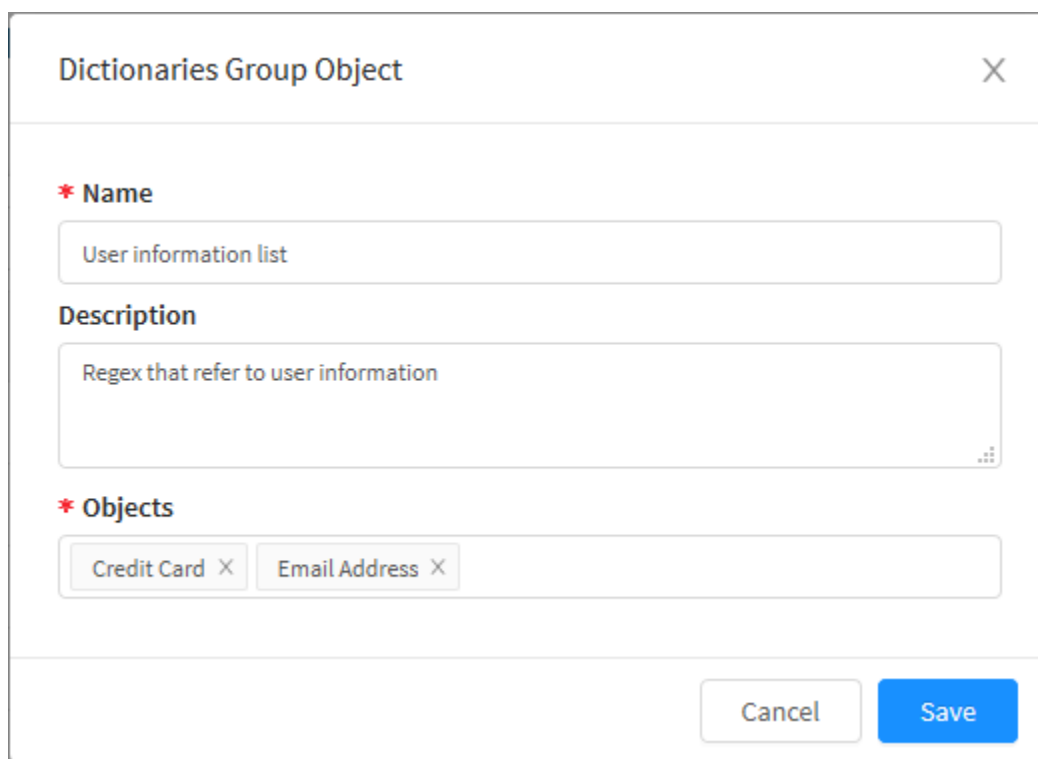
Através do botão "Create Group" é possível criar um novo grupo de objeto. Para acessar, siga os passos:

1. No menu de ações [], clique na opção "Create Group";



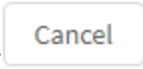
Objects – Dictionaries – Create Group

2. Preencha as informações da tela *Dictionaries Group Object*:

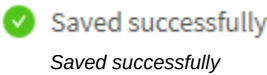
A screenshot of a web form titled 'Dictionaries Group Object' with a close button (X) in the top right corner. The form contains three main sections: 1. 'Name' (required, marked with a red asterisk) with a text input field containing 'User information list'. 2. 'Description' with a larger text area containing 'Regex that refer to user information'. 3. 'Objects' (required, marked with a red asterisk) with a container showing two selected items: 'Credit Card' and 'Email Address', each with a close (X) button. At the bottom right are 'Cancel' and 'Save' buttons.

Objects – Dictionaries Group Object

- **Name:** Nome do grupo de objetos. Ex.: *Dictionaries Group Object*;
- **Description:** Este campo é destinado para a descrição do grupo. Ex.: *Regex that refer to user information*;
- **Objects:** Permite selecionar os objetos que foram adicionados previamente em [Objects - Dictionaries - Menu de ações - Create Object](#). Os objetos adicionados neste campo serão inseridos como *tags*.



Clique no botão **Cancel** para Cancelar ou no botão **Save** para salvar.

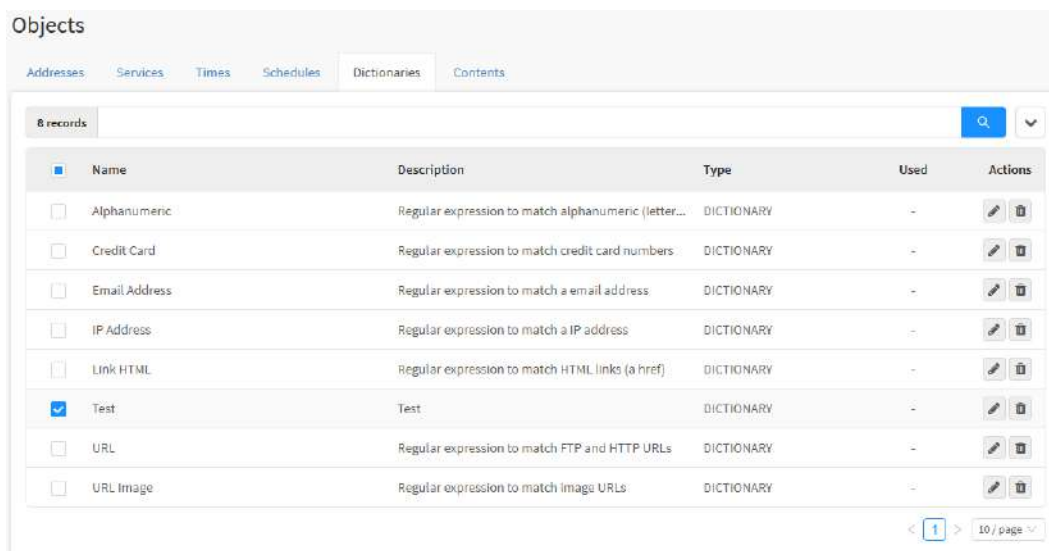


O grupo foi criado com sucesso.

Objects - Dictionaries - Menu de ações - Delete Object

Através do botão "*Delete Object*" é possível deletar objetos ou grupos de objetos. Para deletar pelo menu de ações, siga os seguintes passos:

1. Selecione qual(is) pacote(s) deseja deletar clicando no **checkbox** ☐. Ex.: *Test*;

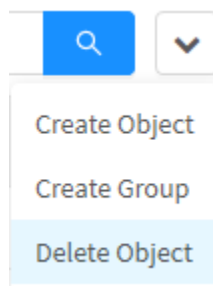


The screenshot shows the 'Objects' management interface. At the top, there are tabs for 'Addresses', 'Services', 'Times', 'Schedules', 'Dictionaries', and 'Contents'. Below the tabs, there is a search bar and a dropdown menu. The main area contains a table with 8 records. The table has columns for 'Name', 'Description', 'Type', 'Used', and 'Actions'. The 'Test' entry is selected, indicated by a checked checkbox in the 'Name' column.

☐	Name	Description	Type	Used	Actions
☐	Alphanumeric	Regular expression to match alphanumeric (letter...	DICTIONARY	-	
☐	Credit Card	Regular expression to match credit card numbers	DICTIONARY	-	
☐	Email Address	Regular expression to match a email address	DICTIONARY	-	
☐	IP Address	Regular expression to match a IP address	DICTIONARY	-	
☐	Link HTML	Regular expression to match HTML links (a href)	DICTIONARY	-	
☒	Test	Test	DICTIONARY	-	
☐	URL	Regular expression to match FTP and HTTP URLs	DICTIONARY	-	
☐	URL Image	Regular expression to match image URLs	DICTIONARY	-	

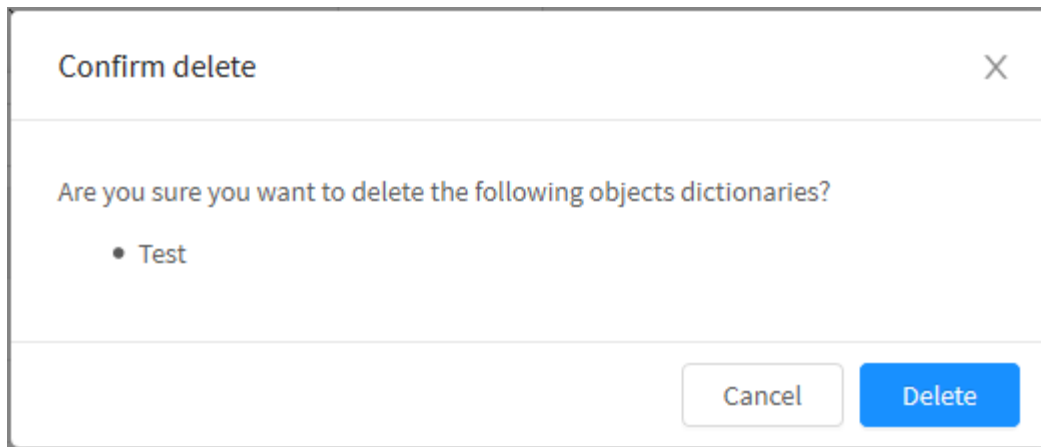
Objects - Objetos selecionados para deleção

2. Entre no **menu de ações**  e clique no botão "*Delete Object*".

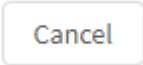
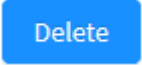


Objects - Menu de ações - Delete Object

3. Surgirá a mensagem se deseja realmente deletar os grupos ou objetos selecionados:



Objects - Are you sure you want to delete the following object dictionaries?

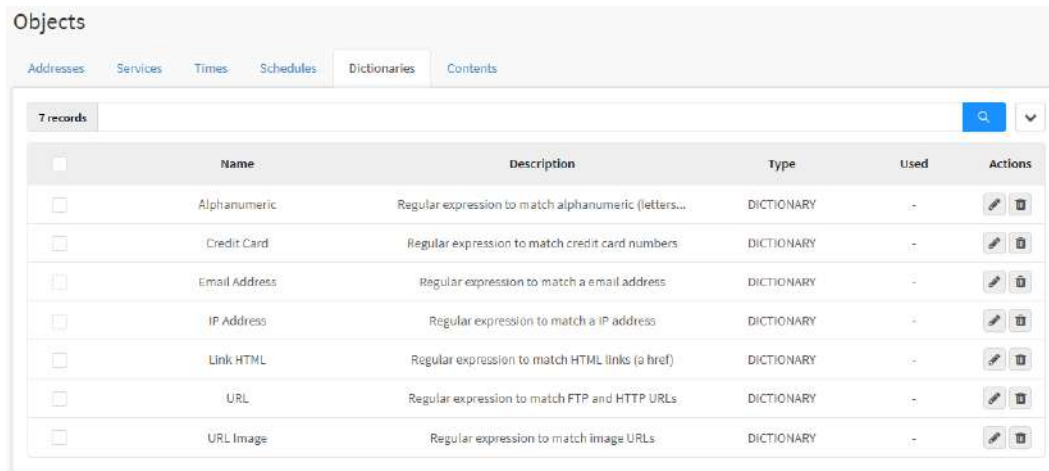
Caso deseje cancelar clique no botão **Cancel** . Para concluir, clique no botão **Delete** .

 **Object deleted successfully!**
Object deleted successfully

Após realizar esses procedimentos os pacotes terão sido excluídos com sucesso.

Objects - Dictionaries - Colunas

Na aba "Dictionaries" é possível visualizar o menu de ações e seis colunas:



	Name	Description	Type	Used	Actions
☐	Alphanumeric	Regular expression to match alphanumeric (letters...	DICTIONARY	-	 
☐	Credit Card	Regular expression to match credit card numbers	DICTIONARY	-	 
☐	Email Address	Regular expression to match a email address	DICTIONARY	-	 
☐	IP Address	Regular expression to match a IP address	DICTIONARY	-	 
☐	Link HTML	Regular expression to match HTML links (a href)	DICTIONARY	-	 
☐	URL	Regular expression to match FTP and HTTP URLs	DICTIONARY	-	 
☐	URL Image	Regular expression to match image URLs	DICTIONARY	-	 

Objects – Aba Dictionaries

A seguir explicaremos cada coluna da aba *Dictionaries*:

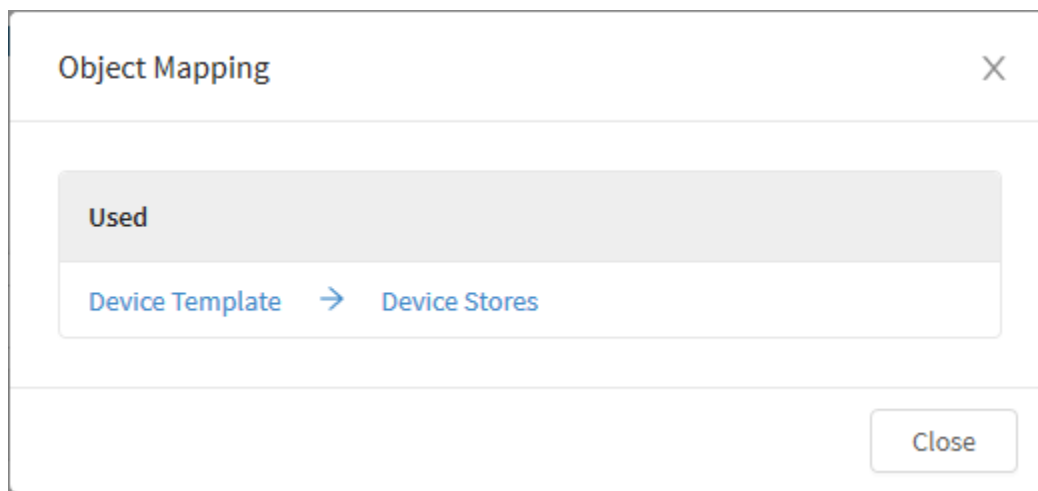
- **Selecionar** : Seleciona os Objetos desejados;
- **Name**: Nome do Objeto;
- **Description**: A descrição do Objeto;
- **Type**: Tipo do Objeto;
- **Used** : Enumera o número de vezes que este objeto está sendo utilizado. Ao clicar neste número a janela *Object Mapping* é exibida.
- **Actions**: Permite editar, selecionar e deletar o objeto;
 - **Edit** : Permite editar as configurações do Objeto adicionado na opção *Create Object* do menu de ações;
 - **Deletar** : Permite remover o Objeto.

Objects - Dictionaries - Object Mapping

Ao clicar no ícone de quantas vezes um objeto foi utilizado [¹] a janela *Object Mapping* é exibida.

A função da janela *object mapping* é exibir onde o objeto foi utilizado.

No exemplo abaixo, o objeto foi utilizado no *Template* de *device* nomeado *Device Stores*.



Object Mapping

Além disso, ao clicar no *link*, é feito um redirecionamento diretamente para onde o objeto está sendo utilizado.

Objects - Contents

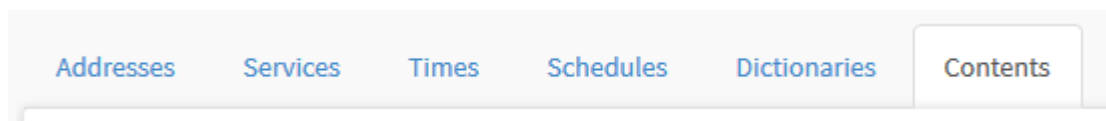
Os objetos do tipo *Contents* são compostos por agrupamentos de tipos de aplicações baseados no tipo de conteúdo que especificam sua característica. Ex.: "ActiveX", "Compactados", "Executáveis", "Imagens", "Javascript", "Multimedia" e "Office".

Para acessar a tela, basta selecionar o botão "Objects".



Botão "Objects"

Clique na aba "Contents".



Objects – Contents

Surgirá a tela "Contents". Ela é composta pelas colunas "Select", "Name", "Description", "Type", "Used" e "Actions". Além disso, no topo da tela está localizada a [barra de busca](#) e o [menu de ações](#) à direita.

Objects					
Addresses Services Times Schedules Dictionaries Contents					
7 records					
☐	Name	Description	Type	Used	Actions
☐	ActiveX	ActiveX Applications	MIME	-	
☐	Compressed	Compressed Files	MIME	-	
☐	Executables	Executable Files	MIME	-	
☐	Images	Bitmaps Images and Vectorial Files	MIME	-	
☐	Javascript	Javascript Files	MIME	-	
☐	Multimedia	Audio and Video Files	MIME	-	
☐	Office	Microsoft Office Files	MIME	-	

Objects - Contents

Explicaremos em detalhes o [menu de ações](#) e posteriormente as colunas da aba "Contents".

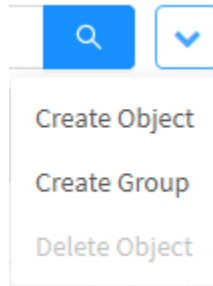
Objects - Contents - Menu de ações

No topo direito da tela temos o menu de ações:



Objects – Botão do menu de ações.

Ao clicar neste botão o menu abaixo é exibido:



Objects – Menu de ações.

O menu é composto das seguintes opções:

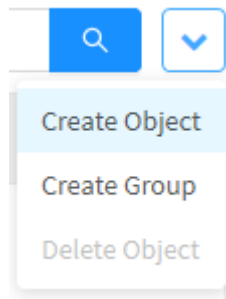
- [Create Object](#);
- [Create Group](#);
- [Delete Object](#).

A seguir cada opção do menu de ações será detalhada.

Objects - Contents - Menu de ações - Create Object

Através da opção "*Create Object*" é possível criar um novo object *Contents*. Para acessar, siga os passos:

1. No **menu de ações** [], clique na opção "*Create Object*";



Objects – Contents – Create Object

2. Surgirá a tela *Create Contents Objects*. Preencha os campos:

Create Contents Object

×

* Name

Image List

* List Mime-Types

▼

+

image/bmp

image/gif

image/jpeg

image/png

^

▼

+

-

* List Extensions

+

bmp

gif

jpeg

png

^

▼

+

-

Description

List of image types

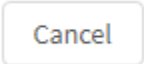
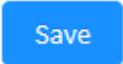
⋮

Cancel

Save

Objects – Create Contents Object

- **Name:** Nome do objeto. Ex.: Images;
- **List Mime-Types:** Exibe a lista de *mime-types* do objeto. Para adicionar, clique [], para excluir algum valor inserido, selecione-o e clique no botão [];
- **List Extensions:** Exibe a lista de extensões do objeto. Para adicionar, clique [], para excluir algum valor inserido, selecione-o e clique no botão [];
- **Description:** Descrição do objeto. Ex.: "Bitmaps Images and Vector Files".

Clique no botão **Cancel**[] para Cancelar. Clique no botão **Save**[] para salvar.

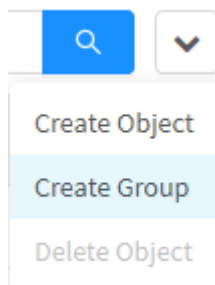
393

O *contents object* foi criado com sucesso.

Objects - Contents - Menu de ações - Create Group

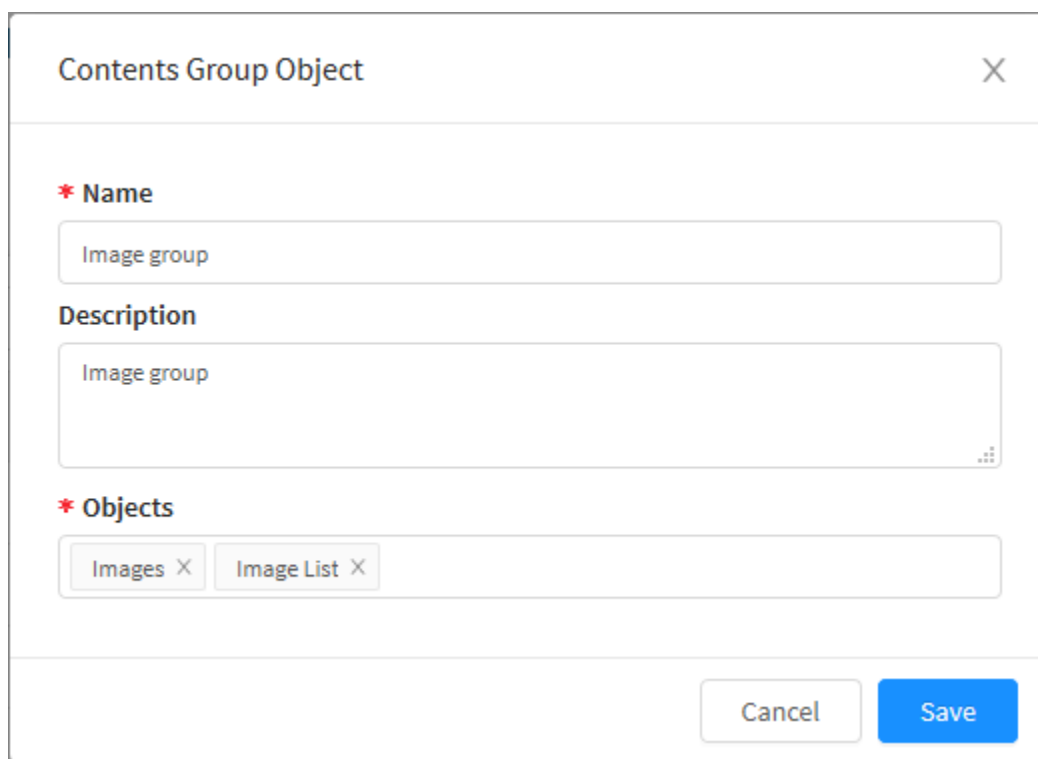
Através do botão "Create Group" é possível criar um novo grupo de objeto. Para acessar, siga os passos:

1. No menu de ações [], clique na opção "Create Group";



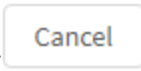
Objects – Contents – Create Group

2. Preencha as informações da tela *Contents Group Object*:

A screenshot of a web form titled 'Contents Group Object' with a close button (X) in the top right corner. The form has three main sections: 1. 'Name' (required, marked with a red asterisk) with a text input field containing 'Image group'. 2. 'Description' with a larger text area containing 'Image group'. 3. 'Objects' (required, marked with a red asterisk) with a container showing two selected items: 'Images' and 'Image List', each with a close (X) button. At the bottom right of the form are 'Cancel' and 'Save' buttons.

Objects – Contents Group Object

- **Name:** Nome do grupo de objetos. Ex.: *Image group*;
- **Description:** Este campo é destinado para a descrição do grupo. Ex.: *Image group*;
- **Objects:** Permite selecionar os objetos que foram adicionados previamente em [Objects - Contents - Menu de ações - Create Object](#). Os objetos adicionados neste campo serão inseridos como *tags*.



Clique no botão **Cancel** para Cancelar ou no botão **Save** para salvar.



Saved successfully

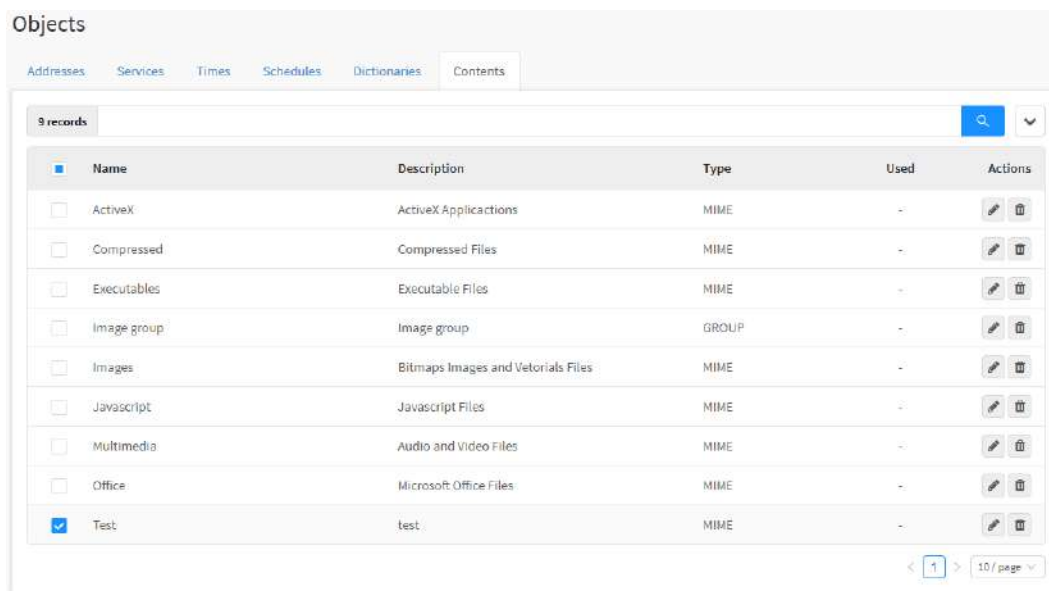
Saved successfully

O grupo foi criado com sucesso.

Objects - Contents - Menu de ações - Delete Object

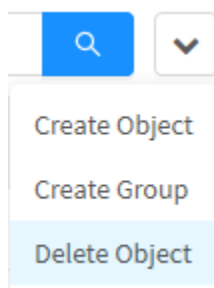
Através do botão "*Delete Object*" é possível deletar objetos ou grupos de objetos. Para deletar pelo menu de ações, siga os seguintes passos:

1. Selecione qual(is) pacote(s) deseja deletar clicando no **checkbox** ☐. Ex.: *Test*;



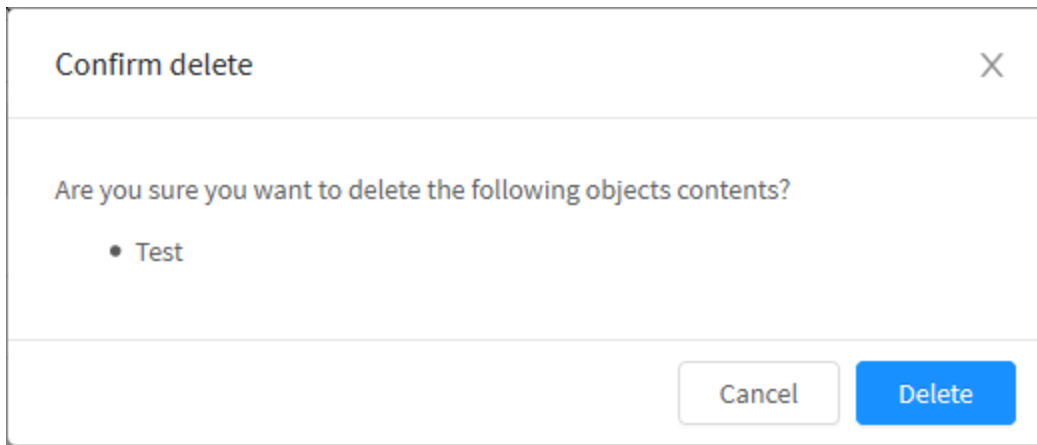
Objects - Objetos selecionados para deleção

2. Entre no **menu de ações** e clique no botão "*Delete Object*".

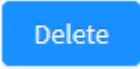


Objects - Menu de ações - Delete Object

3. Surgirá a mensagem se deseja realmente deletar os grupos ou objetos selecionados:



Objects - Are you sure you want to delete the following object contents

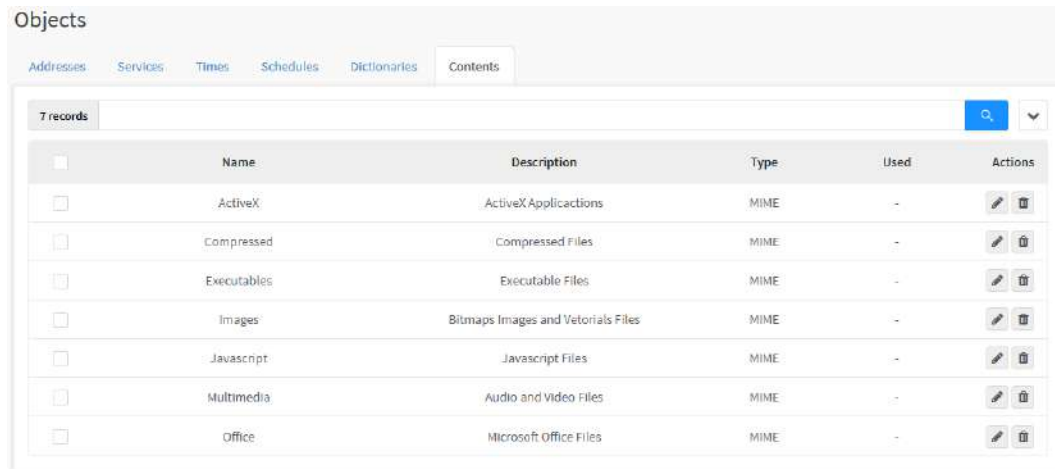
Caso deseje cancelar clique no botão **Cancel** . Para concluir, clique no botão **Delete** .

 **Object deleted successfully!**
Object deleted successfully

Após realizar esses procedimentos os pacotes terão sido excluídos com sucesso.

Objects - Contents - Colunas

Na aba "Contents" é possível visualizar o menu de ações e seis colunas:



	Name	Description	Type	Used	Actions
☐	ActiveX	ActiveX Applications	MIME	-	 
☐	Compressed	Compressed Files	MIME	-	 
☐	Executables	Executable Files	MIME	-	 
☐	Images	Bitmaps Images and Vectorial Files	MIME	-	 
☐	Javascript	Javascript Files	MIME	-	 
☐	Multimedia	Audio and Video Files	MIME	-	 
☐	Office	Microsoft Office Files	MIME	-	 

Objects – Aba Contents

A seguir explicaremos cada coluna da aba Contents:

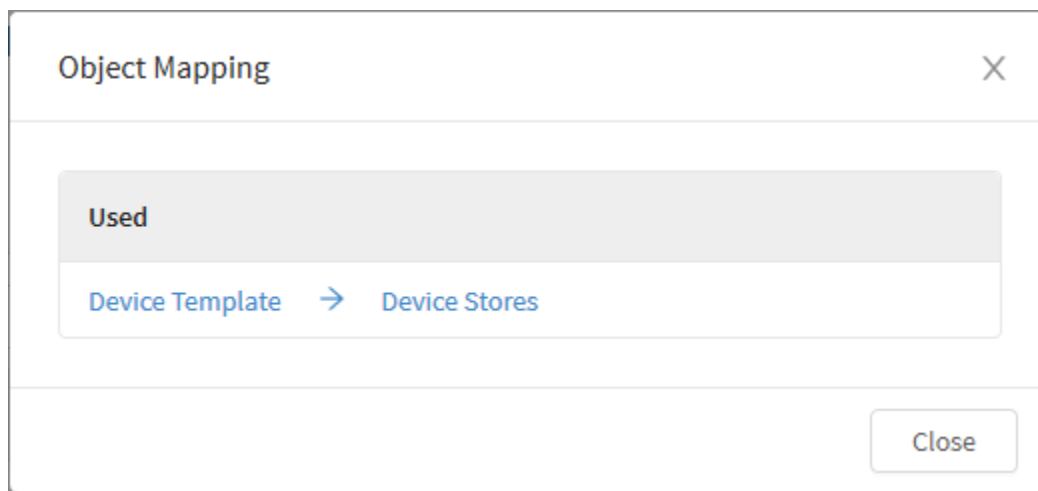
- **Selecionar** : Seleciona os Objetos desejados;
- **Name**: Nome do Objeto;
- **Description**: A descrição do Objeto;
- **Type**: Tipo do Objeto;
- **Used** : Enumera o número de vezes que este objeto está sendo utilizado. Ao clicar neste número a janela [Object Mapping](#) é exibida.
- **Actions**: Permite editar, selecionar e deletar o objeto;
 - **Edit** : Permite editar as configurações do Objeto adicionado na opção [Create Object](#) do menu de ações;
 - **Deletar** : Permite remover o Objeto.

Objects - Contents - Object Mapping

Ao clicar no ícone de quantas vezes um objeto foi utilizado [¹] a janela *Object Mapping* é exibida.

A função da janela *object mapping* é exibir onde o objeto foi utilizado.

No exemplo abaixo, o objeto foi utilizado no *Template* de *device* nomeado *Device Stores*.



Object Mapping

Além disso, ao clicar no *link*, é feito um redirecionamento diretamente para onde o objeto está sendo utilizado.

Users

O menu users permite administrar os usuários dos UTM's conectados ao GSM e ordená-los por grupos de usuários. Este recurso visa facilitar a definição e a administração das políticas de *compliance* que serão aplicadas posteriormente.

Para acessar a tela, basta selecionar o menu "Users";



Management – Users

A tela abaixo será exibida:

Users

Users Groups

24 records

☐	Login	Name	E-mail	Device	Used
☐	user10@blockbit.com	user10	user10@blockbit.com	Branch Office	...
☐	user11@blockbit.com	user11	user11@blockbit.com	Store 1	...
☐	user12@blockbit.com	user12	user12@blockbit.com	Store 1	...
☐	user13@blockbit.com	user13	user13@blockbit.com	Store 1	...
☐	user14@blockbit.com	user14	user14@blockbit.com	Store 1	...
☐	user15@blockbit.com	user15	user15@blockbit.com	Store 1	...
☐	user16@blockbit.com	user16	user16@blockbit.com	Webfilter 1	...
☐	user17@blockbit.com	user17	user17@blockbit.com	Webfilter 1	...
☐	user18@blockbit.com	user18	user18@blockbit.com	Webfilter 1	...
☐	user19@blockbit.com	user19	user19@blockbit.com	Webfilter 2	...

< 1 2 3 > 10 / page

Users - Users

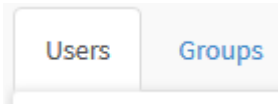
A tela *Users* comporta as seguintes abas:

- [Users](#);
- [Groups](#).

A seguir, os componentes da aba [Users](#) serão analisadas.

Aba Users

Esta aba tem como função administrar os usuários do UTM. A aba "Users" já deve estar selecionada automaticamente, caso contrário, clique nela:



Aba "Users".

Surgirá a Tela de Users. Ela é composta pelas colunas "Login", "Name", "E-mail", "Device" e "Used". Além disso, no topo direito da tela está localizada a barra de busca e o menu de ações.

Users

UsersGroups

24 records

Search

	Login	Name	E-mail	Device	Used
☐	user10@blockbit.com	user10	user10@blockbit.com	Branch Office	
☐	user11@blockbit.com	user11	user11@blockbit.com	Store 1	
☐	user12@blockbit.com	user12	user12@blockbit.com	Store 1	
☐	user13@blockbit.com	user13	user13@blockbit.com	Store 1	
☐	user14@blockbit.com	user14	user14@blockbit.com	Store 1	
☐	user15@blockbit.com	user15	user15@blockbit.com	Store 1	
☐	user16@blockbit.com	user16	user16@blockbit.com	Webfilter 1	
☐	user17@blockbit.com	user17	user17@blockbit.com	Webfilter 1	
☐	user18@blockbit.com	user18	user18@blockbit.com	Webfilter 1	
☐	user19@blockbit.com	user19	user19@blockbit.com	Webfilter 2	

<123>

10 / page

Users – Tela principal Users.

A seguir, o menu de ações será analisado e posteriormente nos aprofundaremos no conteúdo das colunas do painel.

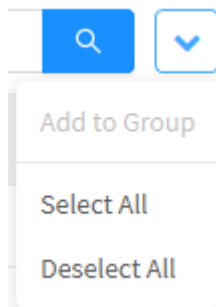
Users - Menu de ações

No topo direito da tela temos o menu de ações:



Users – Botão do Menu de ações.

Ao clicar neste botão o menu abaixo é exibido:



Users – Menu de ações.

O menu é composto das seguintes opções:

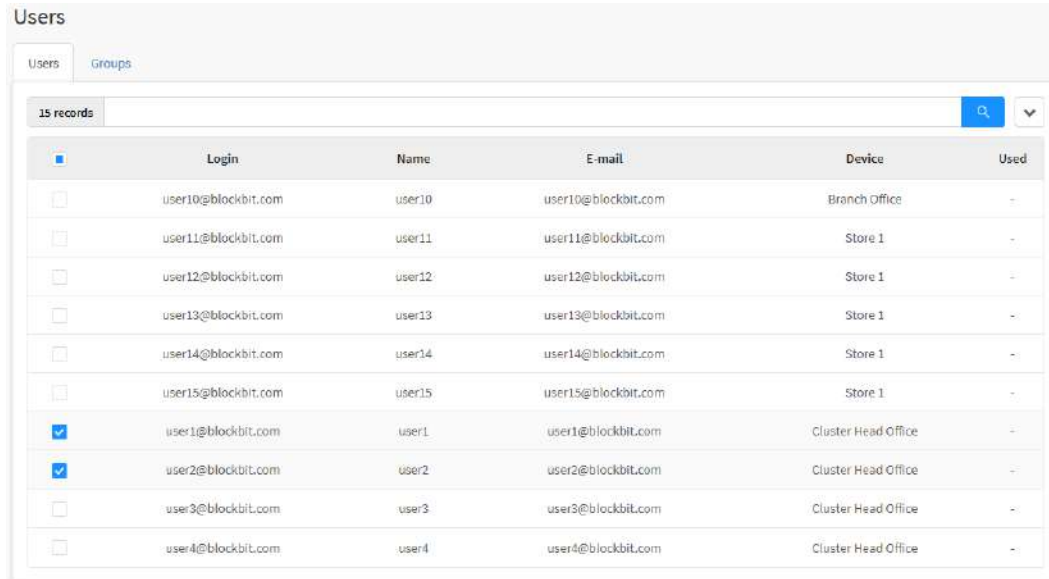
- [Add to Group](#);
- [Select All](#) e [Deselect All](#).

A seguir cada opção do menu de ações será detalhada.

Users - Menu de ações - Add to Group

Através da opção "Add to Group" é possível adicionar um novo usuário ao Grupo. Para acessá-lo, siga os passos:

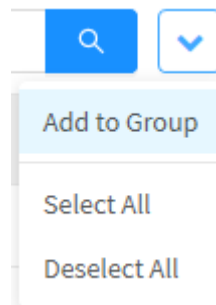
1. Selecione o(s) usuário(s) que deseja adicionar. Para selecionar, clique com o *mouse* no *checkbox* ao lado da coluna "Used". Nos usuários selecionados o *checkbox* mudará para a cor azul []. Ex.: user1@blockbit.com e user2@blockbit.com;



	Login	Name	E-mail	Device	Used
☐	user10@blockbit.com	user10	user10@blockbit.com	Branch Office	-
☐	user11@blockbit.com	user11	user11@blockbit.com	Store 1	-
☐	user12@blockbit.com	user12	user12@blockbit.com	Store 1	-
☐	user13@blockbit.com	user13	user13@blockbit.com	Store 1	-
☐	user14@blockbit.com	user14	user14@blockbit.com	Store 1	-
☐	user15@blockbit.com	user15	user15@blockbit.com	Store 1	-
☒	user1@blockbit.com	user1	user1@blockbit.com	Cluster Head Office	-
☒	user2@blockbit.com	user2	user2@blockbit.com	Cluster Head Office	-
☐	user3@blockbit.com	user3	user3@blockbit.com	Cluster Head Office	-
☐	user4@blockbit.com	user4	user4@blockbit.com	Cluster Head Office	-

Users – Seleção dos usuários para serem adicionados

2. No **menu de ações** [] clique na opção "Add to group";



Users – Add to group.

3. Defina em qual grupo deseja adicionar. É possível selecionar um ou mais grupos para adicionar. Ex.: *Administrators*;

Add users to group

Administrators X

Cancel

Save

Users – Add users to group.

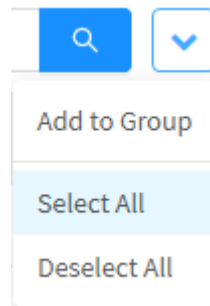
Clique no botão **Save**  para Salvar.

 **Users added successfully to group**
Users added successfully to group

O usuário foi adicionado ao Grupo com sucesso.

Users - Menu de ações - Select All e Deselect All

Ao clicar em "Select All" no menu de ações todos os usuários serão selecionados.



Users – Select All

Isso permite a fácil implementação de uma ação que afete todos os usuários.

A função de "Deselect All" é simplesmente o contrário: Remover todas as seleções feitas previamente.

Users - Colunas

A tela é composta pelo menu de ações e seis colunas. Segue uma breve descrição das colunas:

Users

UsersGroups

15 records

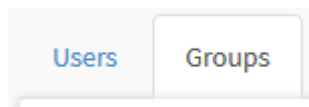
☐	Login	Name	E-mail	Device	Used
☐	user10@blockbit.com	user10	user10@blockbit.com	Branch Office	-
☐	user11@blockbit.com	user11	user11@blockbit.com	Store 1	-
☐	user12@blockbit.com	user12	user12@blockbit.com	Store 1	-
☐	user13@blockbit.com	user13	user13@blockbit.com	Store 1	-
☐	user14@blockbit.com	user14	user14@blockbit.com	Store 1	-
☐	user15@blockbit.com	user15	user15@blockbit.com	Store 1	-
☐	user1@blockbit.com	user1	user1@blockbit.com	Cluster Head Office	-
☐	user2@blockbit.com	user2	user2@blockbit.com	Cluster Head Office	-
☐	user3@blockbit.com	user3	user3@blockbit.com	Cluster Head Office	-
☐	user4@blockbit.com	user4	user4@blockbit.com	Cluster Head Office	-

Users – Users.

- **Select** ☐: Seleciona os usuários desejados;
- **Login**: Login do usuário. Ex.: user1@blockbit.com;
- **Name**: Nome do usuário. Ex.: user1;
- **E-mail**: E-mail do usuário. Ex.: user1@blockbit.com;
- **Device**: Mostra em qual device o User foi cadastrado. Ex.: Branch Office;
- **Used**: Enumera o número de vezes que este grupo foi utilizado nas Policies Manager.

Aba Groups

Esta aba tem como função criar e editar grupos de usuários do UTM. Para acessar a tela, basta selecionar a aba "Groups".



Users – User Groups

Surgirá a Tela de *User Groups*. Ela é composta pelo menu de ações e os *User Groups* já criados, sendo que estes estarão ordenados nas colunas "Name", "Type", "Device Name", "Used" e "Actions". Além disso, no topo direito da tela está localizada a [barra de busca](#) e o [menu de ações](#).



The screenshot shows the 'Users' page with the 'Groups' tab selected. It displays a table with 3 records. The table has columns: Name, Type, Device Name, Used, and Actions. The records are Administrators, Stores, and Webfilter, all of type 'global' and marked as 'Used'.

☐	Name	Type	Device Name	Used	Actions
☐	Administrators	global		-	
☐	Stores	global		-	
☐	Webfilter	global		-	

At the bottom right of the table, there is a pagination control showing '< 1 >' and '10 / page'.

Users - Groups

A seguir, o [menu de ações](#) será analisado e posteriormente nos aprofundaremos no conteúdo das [colunas](#) do painel.

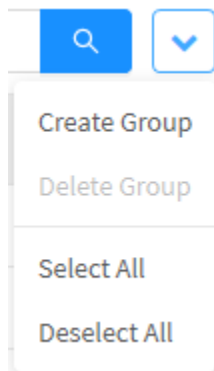
Groups - Menu de ações

No topo direito da tela temos o menu de ações:



Groups – Botão do Menu de ações.

Ao clicar neste botão o menu abaixo é exibido:



Groups – Menu de ações.

O menu é composto das seguintes opções:

- [Create Group](#);
- [Delete Group](#);
- [Select All](#) e [Deselect All](#).

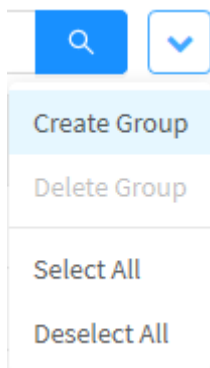
A seguir cada opção do menu de ações será detalhada.

Groups - Menu de ações - Create Group

Esta seção irá demonstrar como criar grupos de usuários. Este recurso facilita a definição e a administração das políticas de *compliance* que serão aplicadas posteriormente.

Através do botão "Create Group" é possível criar um novo Grupo. Para acessar, clique no **menu de ações** [].

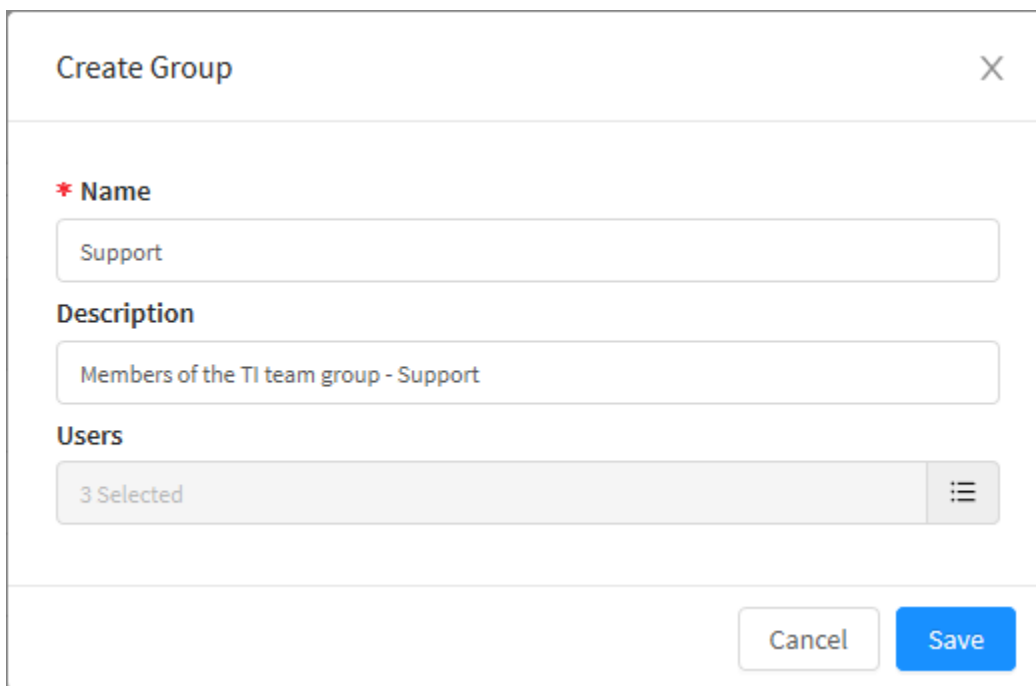
1. Clique na opção "Create Group";



Groups – Menu de ações- Create Group.

2. Preencha a tela *Create Group*;

- **Name:** O nome do Grupo. Ex.: *Support*;
- **Description:** Descrição do Grupo. Ex.: *Members of the TI team group - Support*;
- **Users:** Determina os usuários que farão parte do grupo que está sendo criado.

A screenshot of a 'Create Group' form. The form has a title bar with 'Create Group' and a close button (X). Below the title bar, there are three sections: 'Name' with a red asterisk, 'Description', and 'Users'. The 'Name' field contains the text 'Support'. The 'Description' field contains the text 'Members of the TI team group - Support'. The 'Users' field shows '3 Selected' and a list icon. At the bottom right, there are two buttons: 'Cancel' and 'Save'.

Groups – Create Group.

Para adicionar novos usuários no grupo, clique no **botão de detalhes**  , conforme exemplificado abaixo:

Add Users

All

☒	Users	Device Name
☐	user10@blockbit.com	
☐	user11@blockbit.com	
☐	user12@blockbit.com	
☒	user13@blockbit.com	
☐	user14@blockbit.com	
☒	user15@blockbit.com	
☒	user16@blockbit.com	
☐	user17@blockbit.com	
☐	user18@blockbit.com	
☐	user19@blockbit.com	

<

1

2

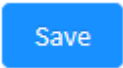
3

>

Cancel

Save

Groups - Create Group - Add Users

Selecione os usuários que se deseja adicionar no grupo e clique no botão **Save**  .

Por fim, clique no botão **Save**  novamente para Salvar.

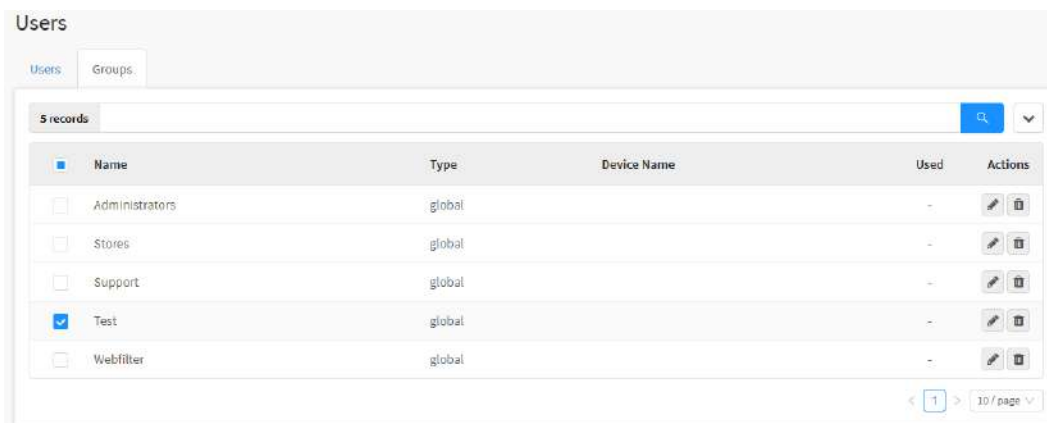
 **Group saved successfully**
Group saved successfully

O grupo foi criado com sucesso.

Groups - Menu de Ações - Delete Group

Através do botão "Delete Group" é possível deletar grupos criados. Para acessar, clique no **Menu de ações** .

1. Selecione o Grupo que deseja deletar. Para selecionar, clique com o mouse no *checkbox* ao lado da coluna *Name*. No grupo selecionado, o *checkbox* mudará da cor cinza para azul . Ex.: *Administrator* e *Store Managers*;

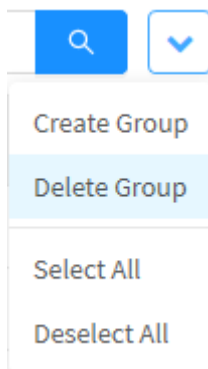


The screenshot shows the 'Users' management interface with the 'Groups' tab active. It displays a table with 5 records. The 'Test' group is selected, indicated by a blue checkbox. The table columns are Name, Type, Device Name, Used, and Actions.

☐	Name	Type	Device Name	Used	Actions
☐	Administrators	global		-	 
☐	Stores	global		-	 
☐	Support	global		-	 
☒	Test	global		-	 
☐	Webfilter	global		-	 

Users - Groups – Grupos que deseja deletar

2. No **menu de ações** , clique na opção "Delete Groups";



Users - Groups – Menu de ações - Delete Groups

3. Surgirá a mensagem se deseja deletar os item(s):

Are you sure?

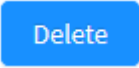
×

Are you sure you want to delete the groups: Test?

Cancel

Delete

User - Groups – Mensagem se deseja deletar os grupos

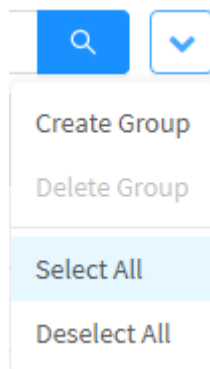
Clique no botão **Cancel** para cancelar. Clique no botão **Delete** para deletar os grupos selecionados.

 **Groups deleted successfully**
Groups deleted successfully

O(s) grupo(s) foram deletados com sucesso.

Groups - Menu ações - Select All e Deselect All

Ao clicar em “*Select All*” no menu de ações todos os grupos de usuários serão selecionados.



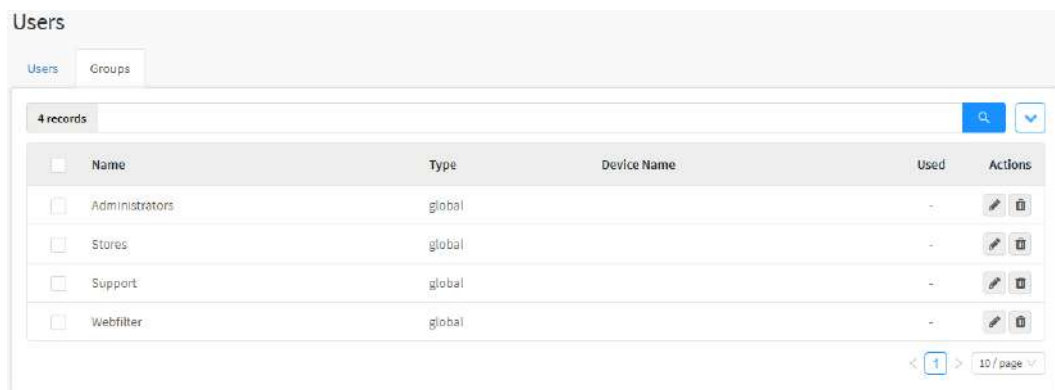
Groups – Select All

Isso permite a fácil implementação de uma ação que afete todos os grupos de usuários.

A função de “*Deselect All*” é simplesmente o contrário: Remover todas as seleções feitas previamente.

Groups - Colunas

Surgirá a Tela de User Groups. Ela é composta pelo Menu Actions e os User Groups já criados no UTM, sendo que estes estarão ordenados pelo Menu *Actions* e seis colunas. Segue uma breve descrição das colunas:



☐	Name	Type	Device Name	Used	Actions
☐	Administrators	global		-	
☐	Stores	global		-	
☐	Support	global		-	
☐	Webfilter	global		-	

Users – Groups

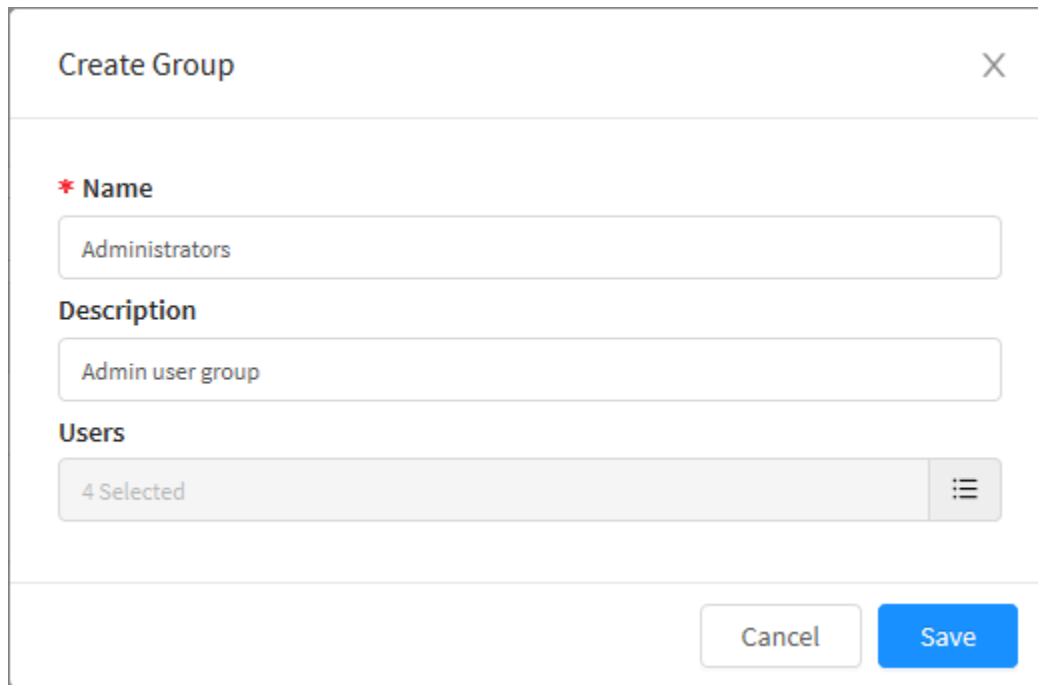
- **Select** : Seleciona os grupos desejados;
- **Name**: Nome do grupo;
- **Type**: Determina o tipo de IP;
- **Device Name**: Mostra em qual *device* o Grupo foi cadastrado;
- **Used**: Enumera o número de vezes que este grupo foi utilizado nas *Policies Manager*.
- **Actions**: *Compõe os botões*:
 - **Edit** : Permite editar as configurações do grupo adicionado na opção [Create Object](#) do menu de ações;
 - **Delete** : Remove o grupo.

Na sessão a frente explicaremos em detalhe o menu *de ações*.

Groups - Edit Group

Através do botão **Edit**  é possível editar um grupo criado.

1. Determine o Grupo que se deseja editar;
2. Na coluna *Actions*, clique no botão **Edit** ;
3. Surgirá a tela *abaixo*. Nesta tela é possível editar as informações *Settings* (de nome do grupo e descrição) e *Users* (usuários do grupo);



The image shows a 'Create Group' dialog box with a title bar containing the text 'Create Group' and a close button 'X'. The dialog has three main sections: 'Name' with a red asterisk, 'Description', and 'Users'. The 'Name' section has a text input field containing 'Administrators'. The 'Description' section has a text input field containing 'Admin user group'. The 'Users' section has a list box showing '4 Selected' and a button with a list icon. At the bottom right, there are 'Cancel' and 'Save' buttons.

Groups – Edit Group

- **Name:** Definir um nome para o grupo. Ex.: *Administrators*;
- **Description:** Definir uma descrição para o grupo. Ex.: *Admin user group*;
- **Users:** Determina os usuários que serão membros deste grupo. Para selecionar as categorias, clique no botão , escolha as categorias desejadas marcando as **caixas de checagem** , conforme demonstrado abaixo:

Add Users
X

All

☐	Users	Device Name
☐	user10@blockbit.com	
☐	user11@blockbit.com	
☐	user12@blockbit.com	
☐	user13@blockbit.com	
☐	user14@blockbit.com	
☒	user15@blockbit.com	
☒	user16@blockbit.com	
☒	user17@blockbit.com	
☐	user18@blockbit.com	
☐	user19@blockbit.com	

<
1
2
3
>

Cancel
Save

Groups – Edit Group

Caso seja necessário fazer uma configuração em todos os itens, basta selecionar a opção desejada no **menu de ações** []:

Select All
Deselect All

SSL Inspection - Add Category - Menu de Ações

Cancel

Save

Para sair deste painel, clique no botão **Cancel**] ou clique no botão **Save**] para concluir a adição das categorias.



Group saved successfully

Group saved successfully

O grupo foi editado com sucesso.

Policies

Esta seção irá demonstrar como criar pacotes de políticas que, posteriormente, serão instalados nos *devices*.

Com os pacotes de políticas, pode-se gerenciar os seguintes serviços no Blockbit UTM: "Filtro de conteúdo *Web*", "Filtro e controle de aplicativos", "Interceptação *SSL*", "Inspeção *IPS*", "Inspeção *ATP*", "Roteamento", "Controle *QoS (Traffic Shaping)*", "Garantia e prioridade de tráfego", "Controle de Cota de tráfego e tempo", "Controle de tamanho de arquivos", "Filtros de cabeçalho e conteúdo", "Balanceamento de *link*", "Múltiplos serviços", "*NAT*" e "*Proxy*",

Possibilitar a execução das seguintes tarefas: criação e administração de políticas de Firewall e controle de aplicação; criação e administração de políticas de IPS, antivírus e anti-spyware; criação e administração de políticas de conteúdo Web e filtro de URL; monitoração e investigação de logs; debugging; troubleshooting; visualização de eventos; dashboards; captura de pacotes por feature (ex:IPS);

Para acessar a tela, basta selecionar o botão "*Policies*".



Management – Policies

A tela abaixo será exibida:

Policies

Policy Packages Policy Templates

4 records

☐	Name	Description	Type	Version	Policies	Actions
☐	Branch Office Policies	Policies and Rules - Branch Office	ipv4	1.5	0	
☐	Head Office Policies	Policies and Rules - Head Office	ipv4	1.5	0	
☐	Store Policies	Policies and Rules - Stores	ipv4	1.5	1	
☐	Webfilter Policies	Webfilter Policies	ipv6	1.5	1	

< 1 > 10 / page

Policies – Policy Packages

A tela *Policies* comporta as seguintes abas:

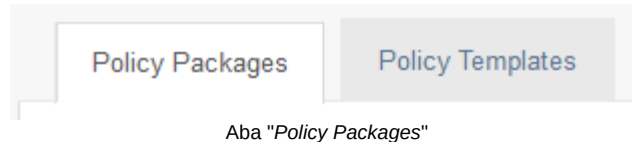
- [Policy Packages](#);
- [Policy Templates](#).

A seguir, os componentes da aba [Policy Package](#) serão analisadas.

Aba Policy Packages

Esta seção irá demonstrar como criar pacotes de políticas que, posteriormente, serão instalados nas *devices*.

Caso não esteja já selecionado, clique na aba "Policy Packages";



Aba "Policy Packages"

Surgirá a Tela de "Policy Packages". Ela é composta pelas colunas "Name", "Description", "Type", "Version", "Policies" e "Actions". Além disso, no topo direito da tela está localizada a [barra de busca](#) e o [menu de ações](#).

Policies

Policy Packages Policy Templates

4 records

☐	Name	Description	Type	Version	Policies	Actions
☐	Branch Office Policies	Policies and Rules - Branch Office	Ipv4	1.5	0	  
☐	Head Office Policies	Policies and Rules - Head Office	Ipv4	1.5	0	  
☐	Store Policies	Policies and Rules - Stores	Ipv4	1.5	1	  
☐	Webfilter Policies	Webfilter Policies	Ipv6	1.5	1	  

< 1 > 10 / page

Policies – Policy Packages

Esta seção irá demonstrar como:

- [Cadastrar e Remover pacotes de política](#);
- [Administrar grupos de políticas](#);
- Etc.

A seguir, vamos analisar cada componente deste painel.

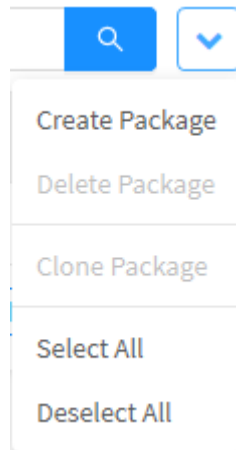
Policy Packages - Menu de ações

No topo direito da tela temos o menu de ações:



Policy Package – Botão do menu de ações.

Ao clicar neste botão o menu abaixo é exibido:



Policy Packages – Menu de ações.

O menu é composto das seguintes opções:

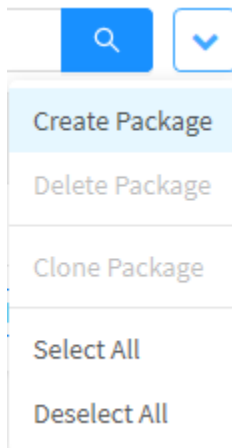
- [Create Package](#);
- [Delete Packages](#);
- [Clone Packages](#);
- [Select All](#) e [Deselect All](#).

A seguir cada opção do menu de ações será detalhada.

Policy Packages - Menu de ações - Create Package

Através da opção "Create Package" é possível criar um novo pacote. Para acessar, clique no menu de ações [].

1. Clique na opção "Create Package";



Policy Packages - Create Package

2. A tela "Create Policy Package" será exibida. Preencha-a com os seguintes dados:

- **Name:** Nome do pacote. Ex.: *Branch Office Policies*;
- **Description:** Descrição do pacote. Ex.: *Policies and Rules - Branch Office*;
- **Version:** Define a versão que será utilizada no pacote. É importante que a versão do pacote seja igual a do UTM;



ATENÇÃO: Caso a versão do pacote seja diferente da do UTM, eles não serão compatíveis.

Sempre crie pacotes com a mesma versão dos UTMs nos quais eles serão aplicados.

- **Type:** Seleciona o tipo de protocolo IP que será utilizado, entre as opções: "IPv4" e "IPv6".

Create Policy Package

X

* Name

Branch Office Policies

Description

Policies and Rules - Branch Office

* Version

1.5

▼

* Type

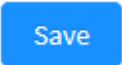
IPv4

▼

Cancel

Save

Policy Packages – Create Policy Package.

Caso deseje cancelar clique no botão **Cancel**. Para concluir a criação do pacote de política clique no botão **Save**.

 **Package created successfully**

Package created successfully

O pacote foi criado com sucesso.

Policy Packages - Menu de ações - Delete Packages

Através do botão "Delete Packages" é possível deletar vários pacotes instalados ao mesmo tempo. Para deletar pelo menu de ações, siga os seguintes passos:

1. Selecione qual(is) pacote(s) deseja deletar clicando no **checkbox** [☐] localizado no *menu action*. Ex.: *Policies Branch office*;

Policies

Policy Packages Policy Templates

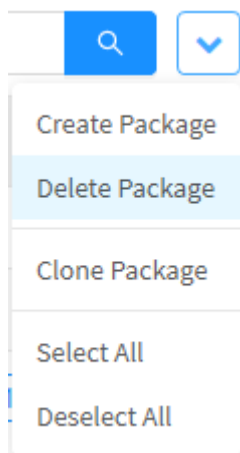
5 records

☐	Name	Description	Type	Version	Policies	Actions
☐	Branch Office Policies	Policies and Rules - Branch Office	ipv4	1.5	0	  
☐	Head Office Policies	Policies and Rules - Head Office	ipv4	1.5	0	  
☐	Store Policies	Policies and Rules - Stores	ipv4	1.5	1	  
☒	Test	Test	ipv6	2.0	0	  
☐	Webfilter Policies	Webfilter Policies	ipv6	1.5	1	  

< 1 > 10 / page

Policy Packages – Delete Packages.

2. Entre no **menu de ações** [] e clique no botão "Delete Packages".



Policy Packages – Menu de ações – Delete Packages.

3. Surgirá a mensagem se deseja realmente deletar os pacotes selecionados:

Delete Policy Package

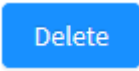
X

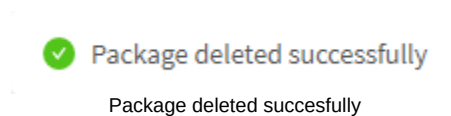
Delete "Test" Policy Package?

Cancel

Delete

Policy Packages – Delete Policy Package?

Caso deseje cancelar clique no botão **Cancel**. Para concluir, clique no botão **Delete**.



Após realizar esses procedimentos os pacotes terão sido excluídos com sucesso.

Policy Packages - Menu de ações - Clone Packages

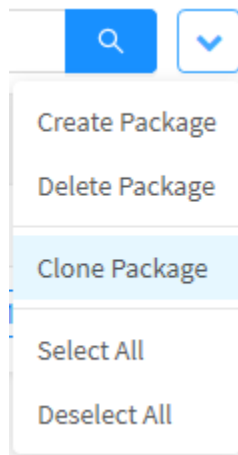
Através do botão "Clone Packages" é possível clonar pacotes existentes. Para clonar pacotes siga os passos:

1. Selecione qual(is) pacote(s) deseja clonar clicando no **checkbox** [] localizado no menu *action*. Ex.: *Policies Branch office*;



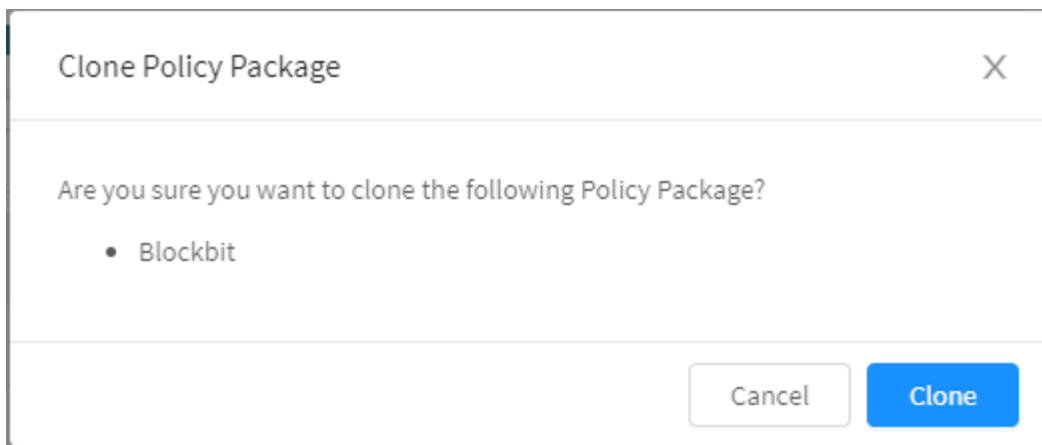
Policy Packages – Seleção dos pacotes que deseja clonar.

2. No menu de ações [], clique na opção "Clone Packages".

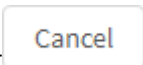
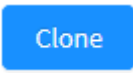


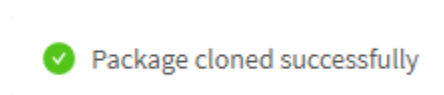
Policy Manager – Menu de ações – Clone Package.

3. Surgirá uma mensagem perguntando se deseja clonar o item selecionado.



Policy Package – Clone Policy Package

Caso desejar cancelar clique no botão **Cancel** []. Para concluir, clique no botão **Clone** [].



Package cloned successfully

Após realizar esses procedimentos os pacotes terão sido duplicados com sucesso. Conforme observado na imagem abaixo:

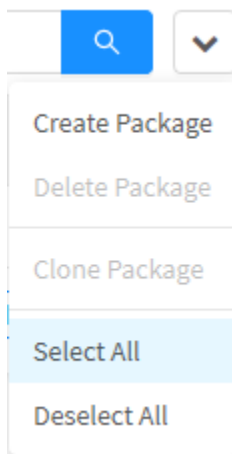


Policy Package - Pacote clonado

Também é possível clonar um Policy Package clicando no botão Clone [].

Policy Packages - Menu de ações - Select All e Deselect All

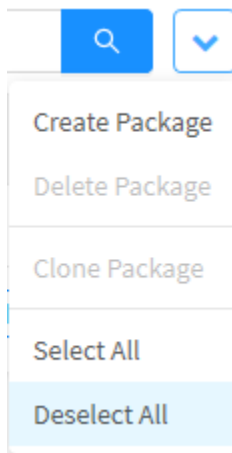
Ao clicar em "Select All" no menu de ações todas as *polícies* serão selecionadas.



Policy Packages – Select All.

Isso permite que alterações que afete todas as *polícies*, sejam facilmente implementadas.

A função de "Deselect All" é simplesmente o contrário: Remover todas as seleções feitas previamente.



Policy Packages - Deselect All.

Policy Packages - Colunas

A seguir explicaremos cada coluna da aba *Policy Packages*:

Policies

Policy Packages

Policy Templates

4 records

☐	Name	Description	Type	Version	Policies	Actions
☐	Branch Office Policies	Policies and Rules - Branch Office	ipv4	1.5	0	  
☐	Head Office Policies	Policies and Rules - Head Office	ipv4	1.5	0	  
☐	Store Policies	Policies and Rules - Stores	ipv4	1.5	1	  
☐	Webfilter Policies	Webfilter Policies	ipv6	1.5	1	  

< 1 >

10 / page

Policies – Policy Packages.

A seguir explicaremos cada coluna:

- **Caixa de Seleção** ☐: Seleciona o Pacote de Políticas;
- **Name**: Apresenta o nome do Pacote de Políticas cadastrado;
- **Description**: Apresenta a descrição do Pacote de Políticas cadastrada;
- **Type**: Representa o tipo de IP. Ex.: "IPv4";
- **Version**: Apresenta a versão na qual o Pacote de Políticas foi criado. É de extrema importância criar Pacotes de Políticas da mesma versão que o UTM, caso contrário, o pacote não será compatível;
- **Policies**: Exibe a quantia de políticas que o pacote possui. Ex.: "100";
- **Actions**: A coluna "Actions" é composta por vários botões:
 - **Botão Edit** : Permite editar as configurações do Pacote de Políticas adicionado na opção *Create Package* do menu de ações;
 - **Botão List Group Policies** : Permite visualizar, editar e adicionar opções mais específicas do Pacote de Políticas. Para mais informações, acesse o capítulo *Policy Packages - Policy Manager*;
 - **Botão Delete** : Deleta o Pacote de Políticas.

A seguir as funções do botão *List Group Policies* serão explicadas e exemplificadas.

Policy Packages - Policy Manager

A tela *Policy Manager* exibe informações mais detalhadas dos *Policy Packages* criados.



Policy packages – Policy Manager

O topo do painel Policy Manager contém:

- **Nome do Pacote:** Apresenta o nome do Pacote de Políticas cadastrado;
- **Versão do Sistema** [🔥]: Apresenta a versão na qual o Pacote de Políticas foi criado. É de extrema importância criar Pacotes de Políticas da mesma versão que o UTM, caso contrário, o pacote não será compatível;
- **IP** [🔑]: Representa o tipo de IP utilizado nos Pacotes de Políticas criados. Ex.: "IPv4";
- **Barra de Busca:** Tem como função possibilitar a localização de itens específicos, é possível clicar em alguns campos das colunas dentro do grupo de política para servir como filtro em uma busca mais específica;
- **Botão Back** [⬅️]: Retorna para o painel anterior;
- **Menu de Ações** [⌵]: Apresenta o seguinte conjunto de opções contextuais:
 - [Create Group](#);
 - [Delete Groups](#);
 - [Import Template](#);
 - [Save Template](#);
 - [Create Policy](#);
 - [Delete Policies](#);
 - [Expand All](#) e [Collapse All](#).
- **Pre Rules:** Representa todos os grupos de políticas que serão criadas antes das outras políticas quando forem instaladas no Blockbit UTM, portanto elas possuem prioridade sobre as regras criadas no próprio UTM;
- **Local Rules:** Representa as regras padrão dos grupos de política já existentes no Blockbit UTM;
- **Post Rules:** Todos os grupos de políticas criadas que serão criadas depois das outras políticas quando forem instaladas no Blockbit UTM, portanto elas terão menor prioridade e serão instaladas abaixo dos grupos de políticas já existente no Blockbit UTM.

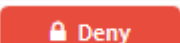
É importante, lembrar que as políticas são ordenadas por "Prioridade", sendo que elas são aplicadas considerando o método "*First Match Wins*" (Que literalmente quer dizer "O 1º entre os concorrentes VENCE"). Logo, as políticas localizadas acima tem prioridade enquanto as abaixo possuem menor prioridade.

Cada grupo de política contém os seguintes botões:

- [⋮] Ao clicar e arrastar, move a ordem do grupo e permite reorganizar a prioridade de acordo com qual grupo está acima (*First Match Wins*);
- [➤] Expande para exibir as políticas criadas no grupo;
- [0] Informa quantas políticas existe no grupo;

-  Permite editar as configurações adicionadas na opção [Create Group](#) do menu de ações;
-  Deleta o grupo;
-  Seleciona o grupo de modo a interagir com o menu de ações.

As colunas de dentro de cada grupo de política são divididas em:

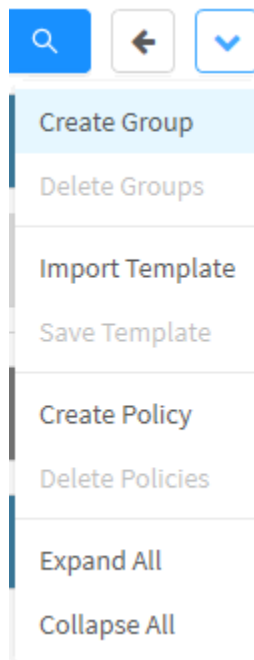
- **Move** : Ao clicar e arrastar, move a ordem da política e permite reorganizar a prioridade de acordo com qual política está acima (*First Match Wins*);
- **Id** : Exibe o número de identificação da política, é possível clicar nele para servir como filtro no campo de busca;
- **Rule**: Exibe o nome da política;
- **Users**: Determina quais usuários são afetados pela política, é possível clicar neste campo para servir como filtro no campo de busca;
- **Source**: Exibe se a origem desta regra será a Zona de rede, endereço IP, interface de rede, Mac Address ou qualquer um destes, é possível clicar neste campo para servir como filtro no campo de busca;
- **Destination**: Determina o destino da regra, o endereço IP ou serviço, é possível clicar neste campo para servir como filtro no campo de busca;
- **Schedule**: Exibe caso a regra depende de um período de tempo ou agendamento, é possível clicar neste campo para servir como filtro no campo de busca;
- **Services**: Exibe os serviços que a regra afeta, é possível clicar neste campo para servir como filtro no campo de busca;
- **Tags**: Exibe as tags que foram adicionadas à essa regra, é possível clicar neste campo para servir como filtro no campo de busca;
- **Modules**: Determina com quais módulos do UTM a regra irá interagir, é possível clicar neste campo para servir como filtro no campo de busca;
- **Action**: Exibe alguns botões contextuais e qual ação a regra executa.
 - **Enabled**  ou **Disabled** : Através deste seletor, ativa ou desativa a regra;
 - **Edit** : Permite editar as configurações adicionadas na opção [Create Policy](#) do menu de ações;
 - **Delete** : Remove a política;
 - **Select** : Permite a seleção das políticas de modo a interagirem com o menu de ações;
 - **Action**: Determina o comportamento da política em questão, tendo como possibilidades:
 - : Como o próprio nome diz, esta opção serve para conceder acesso;
 - : O acesso é negado;
 - : O acesso é negado, porém uma mensagem de rejeição é exibida ao usuário.

Para mais informações a respeito de políticas, consulte o capítulo [12 POLICY](#) do *Manual do UTM*.

Policy Manager - Menu de ações - Create Group

A opção "Create Group" cria grupo de políticas, para tanto, siga os passos:

1. No Menu de ações, clique na opção "Create Group";



Policy Packages – Menu de ações – Create Group

2. Surgirá a tela "Create Group";

A screenshot of a 'Create Group' dialog box. The title bar says 'Create Group' with a close button (X). Inside, there are two required fields marked with a red asterisk: 'Name' with a text input containing 'Administrator Access', and 'Position' with a dropdown menu showing 'Pre Rules'. At the bottom right are 'Cancel' and 'Save' buttons.

Policy Manager – Create a Policy Group – New Group

- **Name:** Determina o nome do grupo de políticas;
- **Position:** Determina a prioridade do grupo de políticas seguindo a regra "First Match wins";
 - **Pre Rules:** Fica acima das outras regras, assim sendo, esse grupo de regras terá maior prioridade;
 - **Post Rules:** Fica abaixo das outras regras, assim sendo, esse grupo de regras terá menor prioridade.

3. Caso desejar cancelar clique no botão **Close** [Close]. Para concluir, clique no botão **Save** [Save];

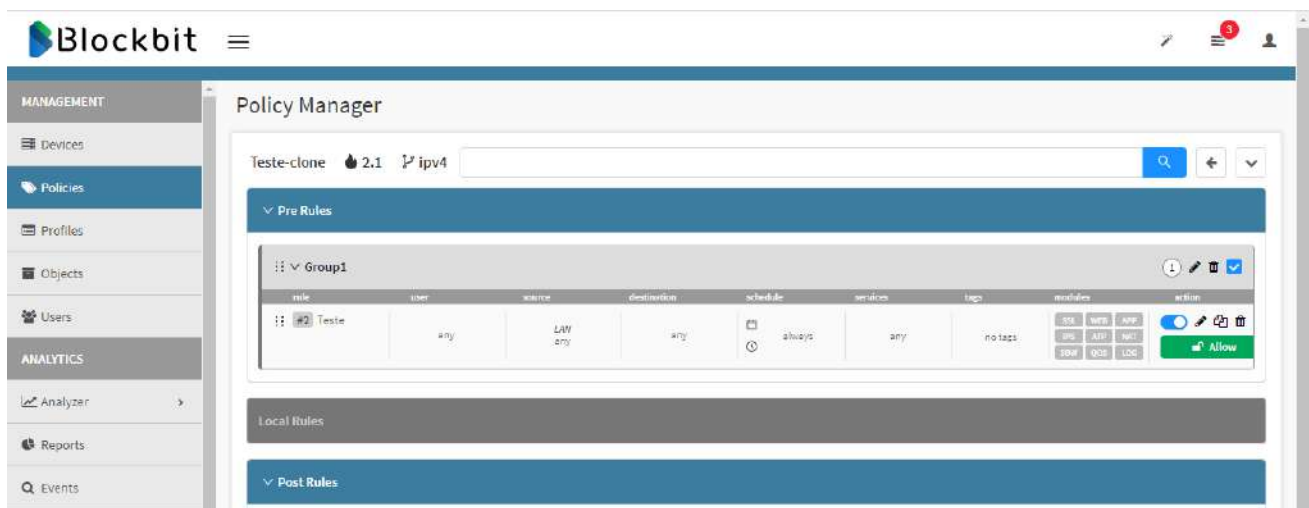
✔ Group created successfully

Group created successfully

4. O grupo foi criado com sucesso.

5. Surgirá na tela *Policy Manager* um novo item em cinza com o nome previamente digitado (no caso do exemplo: "Administrator Access");

6. A barra cinza escura "Local Rules" representa as regras padrão do UTM. O grupo de políticas que foi criado estará posicionado de acordo com o prioridade selecionada previamente, no exemplo, foi selecionado "Pre Rules", assim sendo, estará localizado acima das regras, conforme demonstrado abaixo.



Policy Manager – Rules

A prioridade dos Policy Packages também pode ser editada, basta segurar o botão Drag [⋮] e mover as Pre Rules para baixo ou as Post Rules para cima.

Para mais informações dos componentes deste painel, cheque a página [Policy Packages - Policy Manager](#).

Policy Manager - Menu de ações - Delete Groups

O botão "Delete Policies" deleta os Grupos de Políticas selecionadas.



Atenção: Ao deletar o grupo, todas as políticas que estiverem dentro dele serão deletadas também.

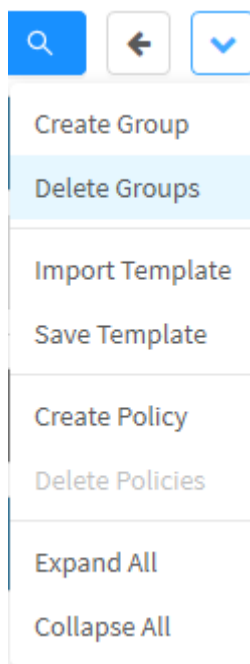
Para deletar, siga os passos:

1. Selecione o(s) grupo(s) de Política(s) que deseja deletar. Para selecionar, clique com o mouse no *checkbox*. Nos grupos selecionados o *checkbox* mudará da cor cinza para azul []. Ex.: *Administrator CLI*;



Política selecionada para ser deletada.

2. No Menu *Actions*, clique na opção "Delete Groups";



Policy Manager – Menu de ações – Delete Policies.

3. Surgirá a tela perguntando se deseja deletar o grupo:

Are you sure?

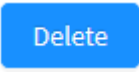
X

Are you sure you want to delete the group Group 1?

Cancel

Delete

Policy Manager – Delete

Caso desejar cancelar, clique no botão **Cancel**. Para concluir, clique no botão **Delete**.

O grupo foi removido com sucesso.

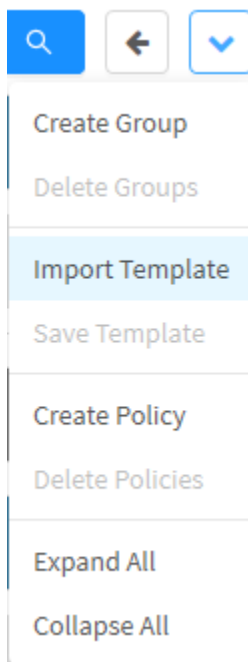
Policy Manager - Menu de ações - Import Template

O botão "Import Template" tem como finalidade importar um *Template* já existente para dentro de um pacote específico, onde ele pode ser importado no "Header" ou "Footer" do pacote selecionado. Para importar um Template, siga os seguintes passos:

1. Selecione o local no qual será importado o Template: "Header" ou "Footer";

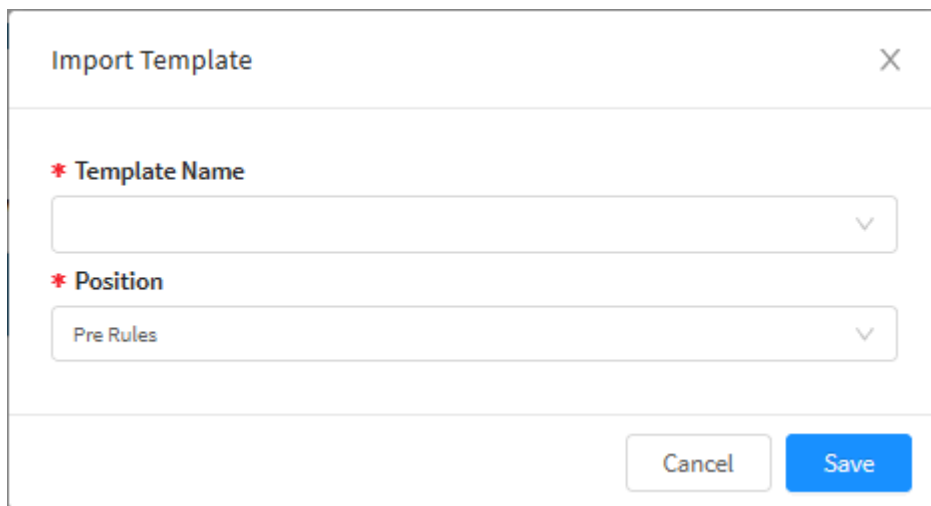


2. No **menu de ações** [], clique na opção "Import Template";



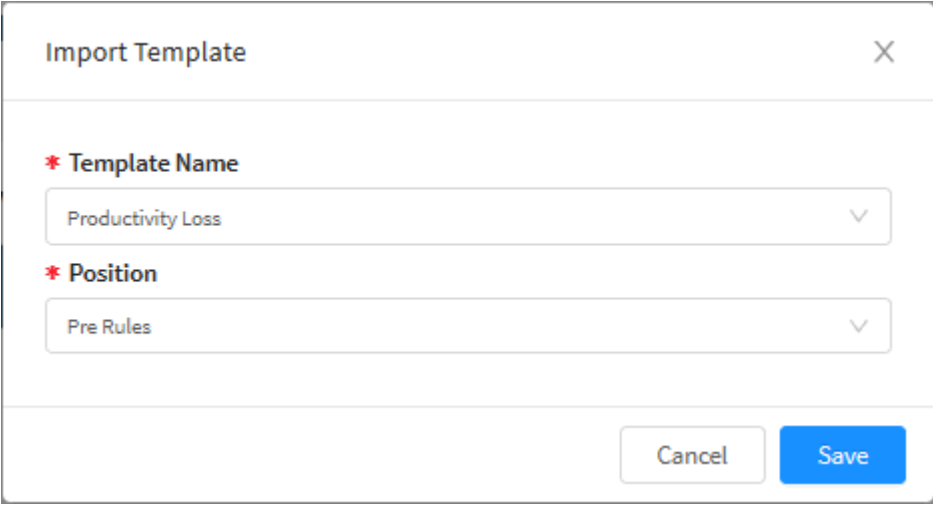
Policy Manager – Menu de ações – Import Template.

3. A tela *Import Template* será exibida;

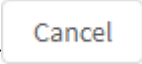
A screenshot of a dialog box titled 'Import Template' with a close button (X) in the top right corner. The dialog contains two required fields, each marked with a red asterisk: 'Template Name' and 'Position'. The 'Template Name' field is an empty text box with a dropdown arrow on the right. The 'Position' field is a dropdown menu currently showing 'Pre Rules' with a dropdown arrow on the right. At the bottom right of the dialog are two buttons: 'Cancel' and 'Save'.

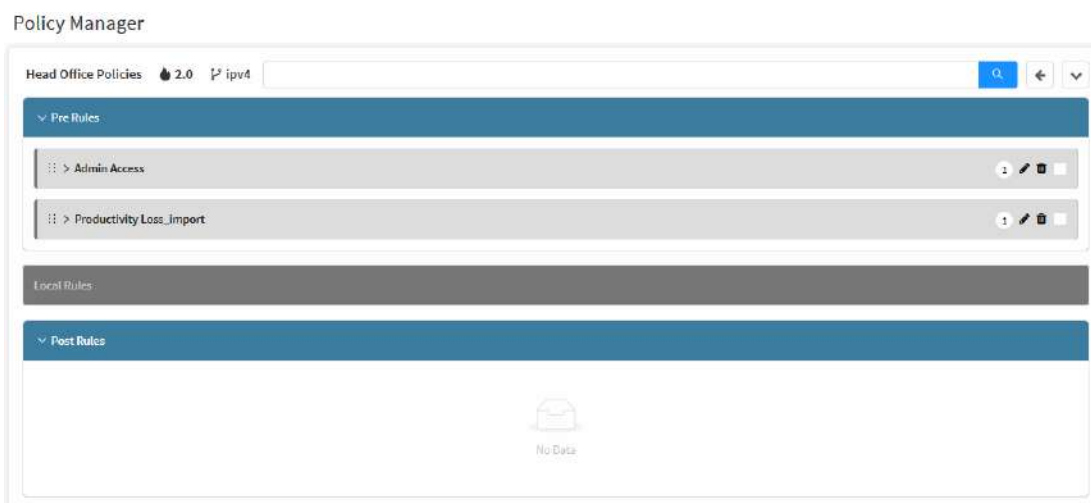
Policy Manager – Template Name

4. Conforme demonstrado abaixo, selecione o *Template Name* desejado e a posição na qual deseja que ele seja importado. Ex.: *Productivity Loss*;

A dialog box titled "Import Template" with a close button (X) in the top right corner. It contains two required fields, each marked with a red asterisk. The first field is "Template Name" with a dropdown menu showing "Productivity Loss". The second field is "Position" with a dropdown menu showing "Pre Rules". At the bottom right, there are two buttons: "Cancel" and "Save".

Policy Manager – Template selecionado

Caso desejar cancelar, clique no botão **Cancel** . Para concluir, clique no botão **Save** . O template importado exibirá "_import" na frente do seu nome, conforme exemplificado pela imagem abaixo.



Policy Manager - Template importado

O *Template* foi importado com sucesso.

Policy Manager - Menu de ações - Save Template

O botão "Save Template" tem como finalidade salvar um determinado grupo de políticas selecionadas e transformá-lo como *Template* para ser reutilizado posteriormente.

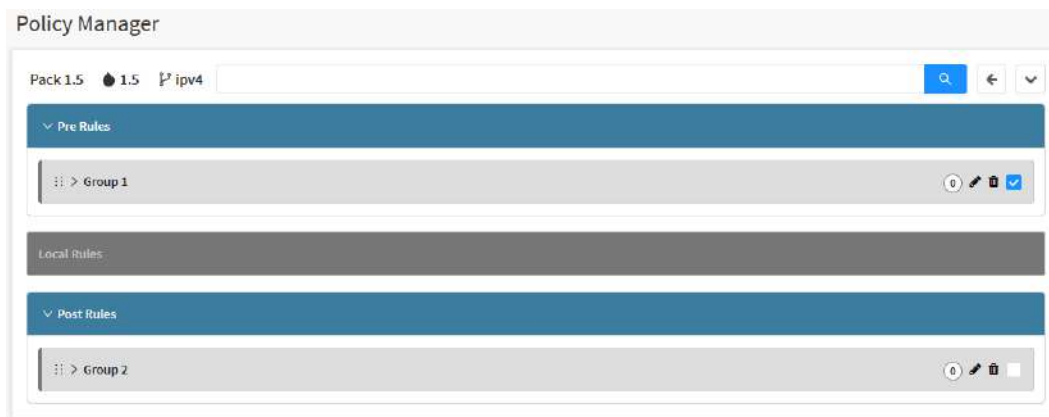


O grupo não pode ter o mesmo nome de um template já criado.

Para salvar um *Template*, siga os seguintes passos:

1. Selecione o grupo que deseja salvar. Para selecionar, clique com o mouse no *checkbox*. Nos pacotes selecionados o *checkbox* mudará da cor cinza

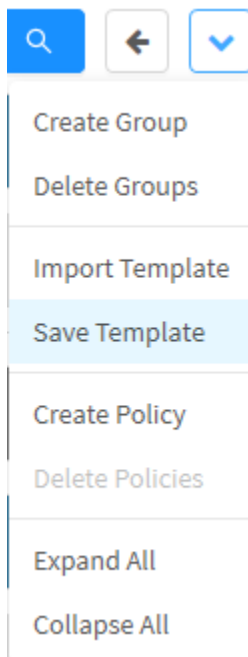
para azul []. Ex.: Access Administrator;



Seleção do grupo – Save Template.

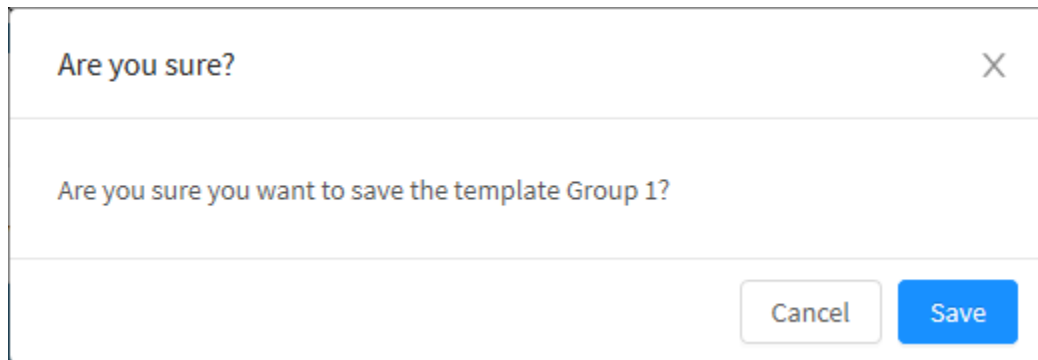


2. No **menu de ações** [], clique na opção "Save Template";

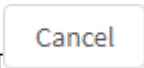


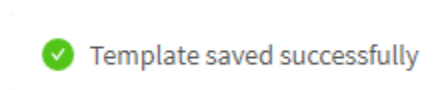
Policy Manager – Menu de ações – Save Template.

3. A mensagem de confirmação será exibida:

A confirmation dialog box with a title bar containing 'Are you sure?' and a close button (X). The main text area contains the question 'Are you sure you want to save the template Group 1?'. At the bottom right, there are two buttons: 'Cancel' and 'Save'.

Policy Manager – Menu de ações – Save Template.

4. Clique no botão  para concluir a operação ou clique no botão  para voltar ao painel anterior:



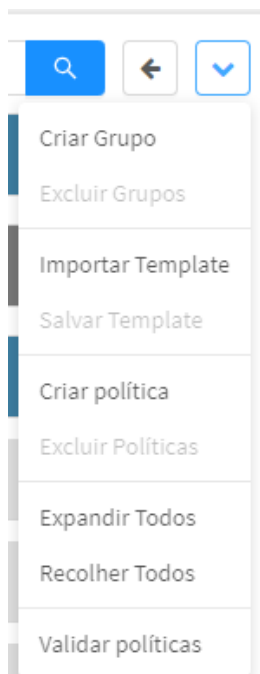
Template saved successfully.

O template foi salvo com sucesso, ele estará disponível na [Aba Policy Templates](#).

Policy Manager - Menu de ações - Create Policy

O botão “*Criar Política*” cria as políticas no grupo de políticas selecionado. Para que ele esteja disponível, é necessário que um grupo tenha sido criado previamente (cheque [Policy Packages - Menu de ações - Create Group](#) para mais informações). A seguir exemplificaremos como criar uma nova política.

1. No **menu de ações** [], clique na opção “*Criar Política*”;



Gerenciador de Políticas – Menu de ações – Criar Política

2. Surgirá a tela ***Criar Política***;

Propriedades

Conexão

Inspeção

Roteamento

Avançado

Geral

* Nome

Descrição

* Ação

Permitir

Tags

* Grupo de política

☐ Traffic Monitor

☐ Traffic Logging

Agendamento

☐ Tempo

☐ Agendamento

Cancelar

Salvar

Gerenciador de Políticas - Nova Política - Propriedades

3. Preencha os campos da aba **Propriedades**:

- **Nome:** Nome da política. Ex.: Admin Access;
- **Descrição:** Descrição da política. Ex.: Full Administrator Access;
- **Tags:** Crie *tags* para facilitar na hora de filtrar a busca da política. Ex.: admin, access, port_98;
- **Ação:** Determina se a ação dessa política será de **"Permitir"**, **"Negar"** ou **"Rejeitar"**.
- **Grupo de Política:** Selecione o grupo no qual será criada a política. Ex.: Administrator Access;
- **Traffic Logging** [☐]: Caso queira ativar o registro de tráfego nesta regra, ative a caixa de checagem;
- **Tempo** []: Caso a caixa de seleção esteja selecionada, determina se a regra se aplicará em dias úteis ("*Business*"), finais de semana ("*Week end*") ou em algum outro objeto do tipo "*Time*" que tenha sido criado;
- **Agendamento** []: Caso a caixa de seleção esteja selecionada, permite determinar se a regra será aplicada em relação a um objeto "*Period/D*ate".

Selecione ☐ os serviços necessários para a configuração

4. Preencha a aba **Conexão** de acordo com a necessidade apresentada:

Propriedades
Conexão
Inspeção
Roteamento
Avançado

* Origem

☐ Zona de rede

☐ Interface de rede

☐ País

☐ Endereço de IP

☐ MAC Address

Destino

☐ Endereço IP

☐ Serviço

☐ País

Identificação

☐ Autenticado

☐ Usuários

☐ Grupos

Cancelar

Salvar

Gerenciador de Políticas - Nova Política - Conexão

- **Origem**
 - **Zona de Rede:** Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar as zonas de rede que podem ser utilizadas. Ex: *WAN, LAN, DMZ*.
 - **Interface de Rede:** Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar interface de rede para serem utilizadas como filtro de origem.
 - **Endereço IP:** Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar *objeto(s)* de Endereço IP (*IPs, redes ou conjuntos*) para serem utilizados como filtro de origem.
 - **MAC Address:** Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar *objeto(s)* de Endereço *MAC Address* para serem utilizados como filtro de origem.
 - **País:** Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar *países* para serem usados como filtro de origem.
- **Destino**
 - **Endereço IP:** Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar *objeto(s)* de Endereço IP (*IPs, redes ou conjuntos*) para serem utilizados como filtro de destino.
 - **Serviços:** Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar *objeto(s)* de serviços (protocolos e portas) utilizados como filtro de destino.
 - **País:** Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar *países* para serem usados como filtro de destino.
- **Identificação**
 - **Autenticado:** Caso habilitada, esta caixa de seleção determina se a política exige autenticação.
 - **Usuários:** Este campo só fica disponível ao marcar a caixa de checagem e a opção *Authenticated*. Permite especificar usuário(s) aos quais a política será aplicada.
 - **Grupos:** Este campo só fica disponível ao marcar a caixa de checagem e a opção *Authenticated*. Permite especificar grupo(s) em que a política se aplica.

Selecione [☐] os serviços necessários para a configuração



Para maiores informações sobre o preenchimento do formulário de política, consulte a Aba "**Conexões**" do Manual do NGFW.

4. Preencha a aba **Inspeção** de acordo com a necessidade apresentada:

Criar política

Propriedades

Conexão

Inspeção

Roteamento

Avançado

Inspeção

☐ Inspeção SSL
▼

☐ Intrusion Prevention
▼

☐ Threat Protection
▼

☐ Application Control
▼

☐ Web Filter
▼

Cancelar

Salvar

Gerenciador de Políticas - Nova Política - Inspeção

- **Inspeção SSL:** Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite interceptar o tráfego SSL permitindo a inspeção do seu conteúdo. As opções que aparecem nesse menu são criadas em [Proxy - SSL Inspection](#);
- **Intrusion Prevention:** Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite aplicar IPS nas políticas. Os perfis exibidos nesse menu são criados em [Services - Intrusion Prevention](#);
- **Threat Protection:** Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite aplicar IPS nas políticas. Os perfis exibidos nesse menu são criados em [Services - Threat Protection](#);
- **Application Control:** Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar um perfil para aplicar controle de acesso à aplicações. Os perfis exibidos nesse menu são criados em [Services - Application Control](#);
- **Web Filter :** Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar um perfil para efetuar a filtragem de conteúdo. Os perfis exibidos nesse menu são criados em [Services - Web Filter](#).

Selecione ☐ os serviços necessários para a configuração e depois o perfil que será utilizado na política que está sendo criada.

5. Preencha a aba **Roteamento** de acordo com a necessidade apresentada:

Criar política

X

Propriedades

Conexão

Inspeção

Roteamento

Avançado

Gateway

☒ NAT
☒ CGNAT

☐ SD-WAN

Roteamento de aplicativos

☐ Aplicativos

Perfil SD-WAN

QoS e Traffic Shaping

☐ Controle de Banda

Very Low

☐ Marcar Pacotes (TOS)

Minimum/Default

Cancelar

Salvar

Gerenciador de Políticas - Nova Política - Roteamento

- Gateway**
 - NAT:** Permite ativar o NAT e a escolha do endereço para tradução de origem, por padrão é configurado o IP do link do Gateway Padrão.
 - CGNAT:** Permite configurar o uso de CGNAT na política, ou seja, uma solução de NAT a nível de provedor, onde o mesmo IP local pode ser atribuído a diferentes hosts ao mesmo tempo, porém com tráfego em portas distintas. As portas disponíveis para o uso de CGNAT devem ser a partir da 2000 (TCP e UDP).
 - SD-WAN:** Permite configurar o uso do SD-WAN na política, podendo escolher perfil que se aplicam a política.
- Roteamento de Aplicativos**
 - Aplicativos:** Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar aplicações para que seja feito o roteamento de solicitações recebidas através do perfil de SD-WAN que for selecionado no campo à seguir, deste modo é possível obter maior controle sobre o consumo e a prioridade de banda consumida pelas aplicações que forem selecionadas. Ao clicar sobre o botão [], a tela abaixo será exibida para selecionar uma ou mais opções que irão compor a regra. Para que serviço funcione, é necessário que a **Inspeção SSL** esteja *ativada*.

Gerenciador de Políticas - Nova Política - Avançado

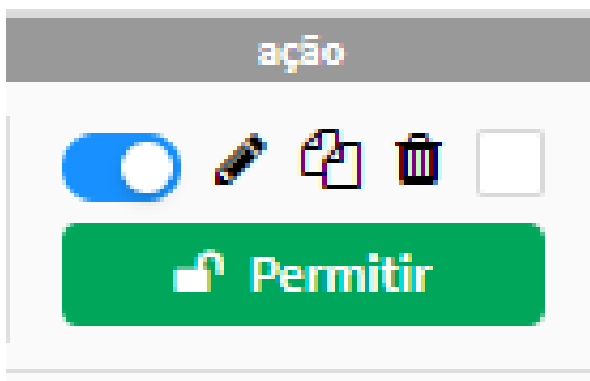
- Selecione [☐] os serviços necessários para a configuração

Salvar

Gerenciador de Políticas

Gerenciador de Política

Após uma "nova política" ser criada no grupo podemos observar que existem seis botões de ações criados, conforme imagem abaixo:



Gerenciador de Política - Ações

Segue a descrição de cada um desses botões da esquerda pra direita:

- **Mover** []: Clique e arraste para mover a política. Caso ela fique abaixo de outra política, ela terá menor prioridade, caso esteja acima, terá maior prioridade;
- **Status da política** []: Determina se a política estará habilitada [] ou desabilitada [];
- **Editar** []: Edita a política criada;
- **Copiar** []: Copia a política criada;
- **Deletar** []: Remove a política criada;
- **Caixa de checagem** []: Seleciona a Política;
- **Ação da Política**: Exibe qual ação a política irá executar, podendo ser: **Permitir**, **Bloquear** ou **Rejeitar**

Policy Manager - Menu de ações - Delete Policies

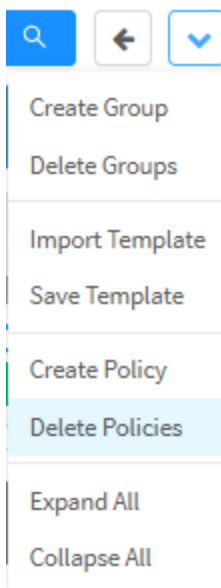
O botão "Delete Policies" deleta as Políticas selecionadas. Para deletar, siga os passos:

1. Selecione a(s) Política(s) que deseja deletar. Para selecionar, clique com o *mouse* no *checkbox*. Nos pacotes selecionados o *checkbox* mudará da cor cinza para azul []. Ex.: *Administrator CLI*;



Política selecionada para ser deletada

2. No menu de ações [], clique na opção "Delete Policies";



Policy Manager – Menu de ações – Delete Policies

3. Surgirá a tela perguntando se deseja deletar os itens:

Are you sure?

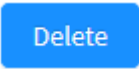
Confirm

- Admin Access

Cancel

Delete

Policy Manager – Delete itens policies

Caso desejar cancelar, clique no botão **Cancel**. Para concluir, clique no botão **Delete**.

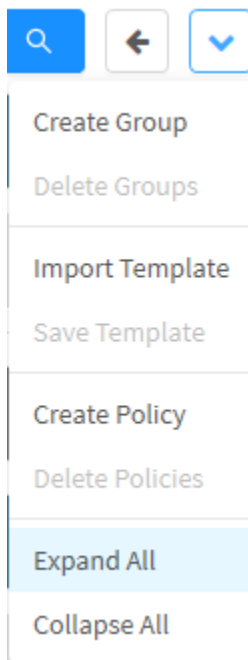
 **Policy deleted successfully**
Policy Deleted successfully

A *Policy* foi removida com sucesso.

Policy Manager - Menu de ações - Expand All e Collapse All

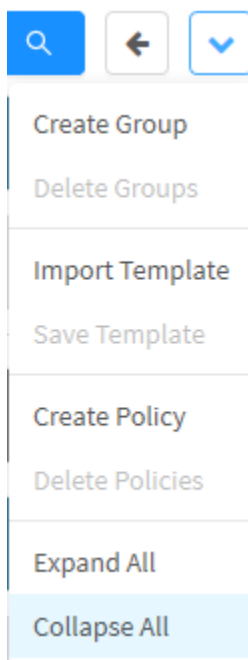
O botão "*Expand All*" tem como finalidade expandir o grupo de políticas. Para expandir o grupo de políticas, siga os seguintes passos:

1. No menu *de ações*, clique na opção "*Expand All*" para expandir os grupos de políticas expandidas;



Policy Manager – Menu de ações – Expand All.

2. Ao clicar em "*Collapse All*" no menu de ações acontece justamente o contrário.

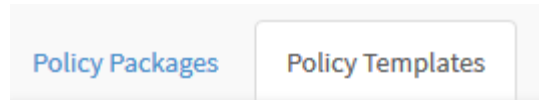


Policy Manager – Menu de ações – Collapse All.

Aba Policy Templates

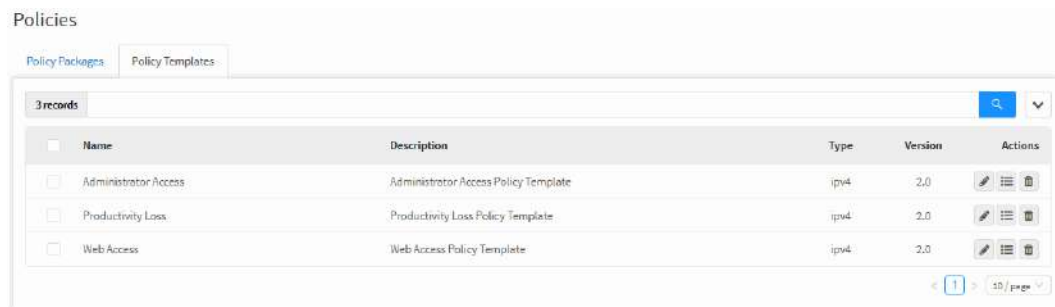
Esta seção irá demonstrar como criar *Policies Templates* que poderão ser reutilizadas posteriormente para um novo pacote de políticas.

Clique na aba “*Policy Templates*”.



Policy Templates

Surgirá a Tela “*Policy Templates*”. Ela é composta pelas colunas “*Name*”, “*Type*”, “*Version*” e “*Actions*”. Além disso, no topo direito da tela está localizada a [barra de busca](#) e o [menu de ações](#).



☐	Name	Description	Type	Version	Actions
☐	Administrator Access	Administrator Access Policy Template	ipv4	2.0	  
☐	Productivity Loss	Productivity Loss Policy Template	ipv4	2.0	  
☐	Web Access	Web Access Policy Template	ipv4	2.0	  

Policies – Policy Templates

Esta seção irá demonstrar como:

- [Cadastrar](#) e [Remover](#) *pacotes de política*;
- [Administrar](#) *grupos de políticas*;
- Etc.

A seguir serão explicadas as colunas de *Policy Template* e posteriormente as ações do menu serão analisadas.

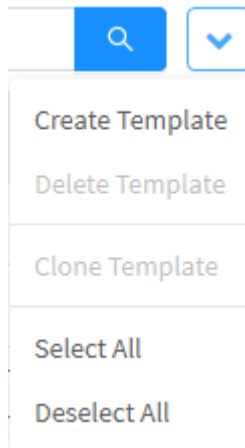
Policy Templates - Menu de Ações

No topo direito da tela temos o menu de ações:



Policy Package – Botão do Menu de Ações.

Ao clicar neste botão o menu abaixo é exibido:



Policy Packages – Menu de Ações.

O menu é composto das seguintes opções:

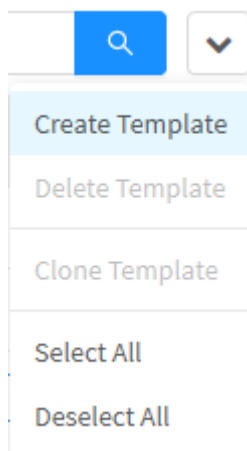
- [Create Template](#);
- [Delete Templates](#);
- [Clone Templates](#);
- [Select All](#) e [Deselect All](#).

A seguir cada opção do menu de ações será detalhada.

Policy Templates - Menu de ações - Create Template

Através da opção "Add Template" é possível criar um novo *Template* de Políticas. Para acessar, clique no **Menu de ações** [].

1. Clique na opção "Add Template";



Policy Templates – Menu de ações.

2. Preencha a tela "New Template":

- **Name:** Nome do template. Ex.: *Productivity Loss*;
- **Type:** Tipo de *IP*;
- **Version:** Define a versão na qual o *template* será feito, é importante que o *template* possua a mesma versão que o UTM;



ATENÇÃO: Caso a versão do template seja diferente da do UTM, eles não serão compatíveis.

Sempre crie templates com a mesma versão dos UTMs nos quais eles serão aplicados.

Create Policy Template

*

Name

Productivity Loss

Description

Productivity Loss Policy Template

*

Version

2.0

*

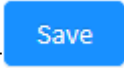
Type

IPv4

Cancel

Save

Policy Template – Create Policy Template.

Clique no botão **Save** .

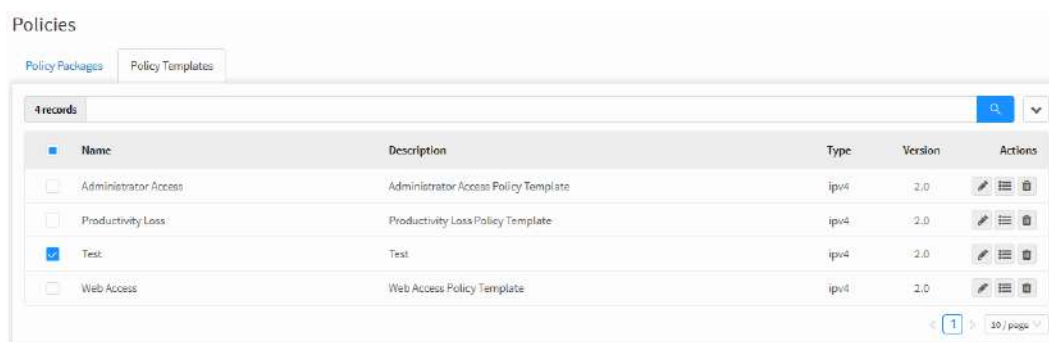
 **Package created successfully**
Package created successfully

O *Template* foi criado com sucesso.

Policy Templates - Menu de ações - Delete Templates

Através do botão “Delete Templates” é possível deletar os *Templates* selecionados. Para deletar através do menu ações, siga os seguintes passos:

1. Selecione qual(is) *Template(s)* deseja deletar. Para selecionar, basta clicar com o *mouse* no *checkbox* que fica localizado ao lado da descrição do *Template Name*. Nos pacotes selecionados o *checkbox* mudará da cor cinza para azul []. Ex.: *Administrator Access*;

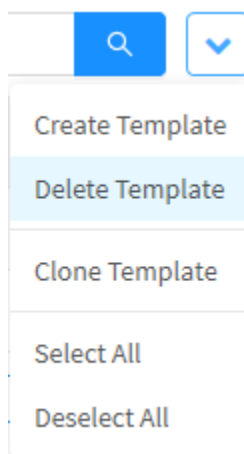


The screenshot shows the 'Policies' interface with a tab for 'Policy Templates'. It displays a table with 4 records. The 'Test' template is selected.

Name	Description	Type	Version	Actions
☐ Administrator Access	Administrator Access Policy Template	ipv4	2.0	  
☐ Productivity Loss	Productivity Loss Policy Template	ipv4	2.0	  
☒ Test	Test	ipv4	2.0	  
☐ Web Access	Web Access Policy Template	ipv4	2.0	  

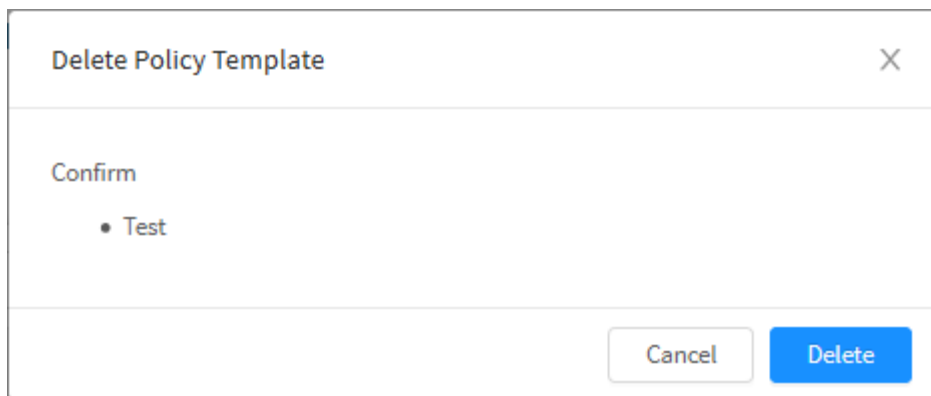
Policy Templates – Seleção dos *Templates* para deletar

2. Entre no menu de ações [] e clique na opção “Delete Templates”.

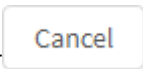
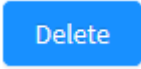


Policy Templates – Delete Templates.

3. Surgirá a mensagem de notificação questionando se deseja realmente deletar os *Templates* selecionados:



Policy Templates – Mensagem se deseja deletar os Templates

Caso desejar cancelar clique no botão **Cancel** . Para concluir, clique no botão **Delete** .

 **Package deleted successfully**
Package deleted successfully

Após realizar esses procedimentos, os *Templates* terão sido deletados com sucesso.

Policy Templates - Menu de ações - Clone Templates

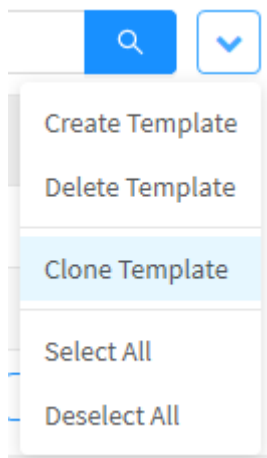
Através do botão “Clone Templates” é possível duplicar um *Template* existente. Para clonar *Templates*, siga os passos:

1. Selecione qual(is) *Template(s)* deseja clonar. Para selecionar, basta clicar com o mouse no *checkbox* que fica localizado ao lado da descrição do *Template Name*. Nos pacotes selecionados o *checkbox* mudará da cor cinza para azul []. Ex.: *Administrator Access*;



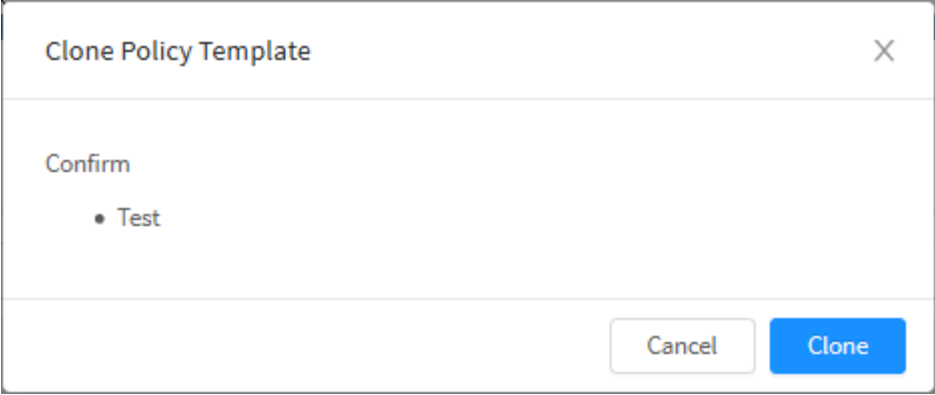
Policy Templates – Seleção dos Templates que deseja clonar.

2. No **menu de ações** [], clique na opção “Clone Templates”;



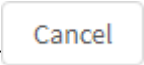
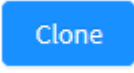
Policy Templates – Clone Templates.

Surgirá uma mensagem perguntando se deseja clonar o item selecionado:



A dialog box titled "Clone Policy Template" with a close button (X) in the top right corner. The main content area is labeled "Confirm" and contains a bulleted list with the item "Test". At the bottom right, there are two buttons: "Cancel" (light gray) and "Clone" (blue).

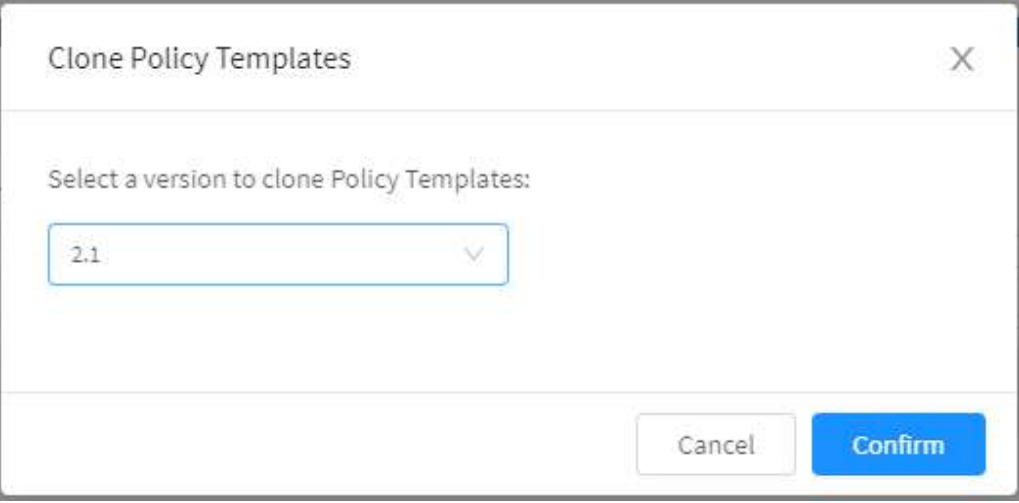
Policy Templates – Mensagem de clonagem do Template

Caso desejar cancelar, clique no botão **Cancel** []. Para concluir, clique no botão **Clone** [].

 **Package cloned successfully**
Package cloned successfully

Surgirá a tela de *Policy Templates novamente* com o pacote clonado.

Também, é possível clonar políticas clicando no botão Clone []. Ao clicar, a seguinte tela aparecerá:

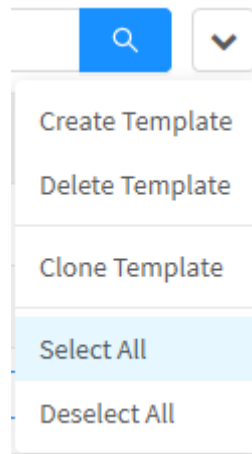


A dialog box titled "Clone Policy Templates" with a close button (X) in the top right corner. The main content area is labeled "Select a version to clone Policy Templates:" and contains a dropdown menu with the value "2.1" and a downward arrow. At the bottom right, there are two buttons: "Cancel" (light gray) and "Confirm" (blue).

Clique em "Confirm" e surgirá a mensagem de confirmação [ **Package cloned successfully**]. O clone terá o mesmo nome, mas com "-clone" ao lado.

Policy Templates - Menu de ações - Select All e Deselect All

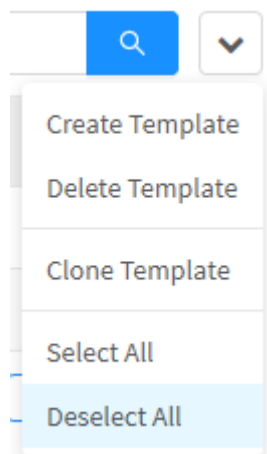
Ao clicar em "Select All" no menu de ações todos os *templates* serão selecionados.



Policy Templates – Select All.

Isso permite a fácil implementação de uma ação que afete todos os templates.

A função de "Deselect All" é simplesmente o contrário: Remover todas as seleções feitas previamente.



Policy Templates – Deselect All.

Policy Templates - Colunas

Na aba “Policy Templates” é possível visualizar o menu de ações e cinco colunas:

Policies

[Policy Packages](#) [Policy Templates](#)

3 records

☐	Name	Description	Type	Version	Actions
☐	Administrator Access	Administrator Access Policy Template	ipv4	2.0	  
☐	Productivity Loss	Productivity Loss Policy Template	ipv4	2.0	  
☐	Web Access	Web Access Policy Template	ipv4	2.0	  

< 1 > 10 / page

Policies – Policy Templates.

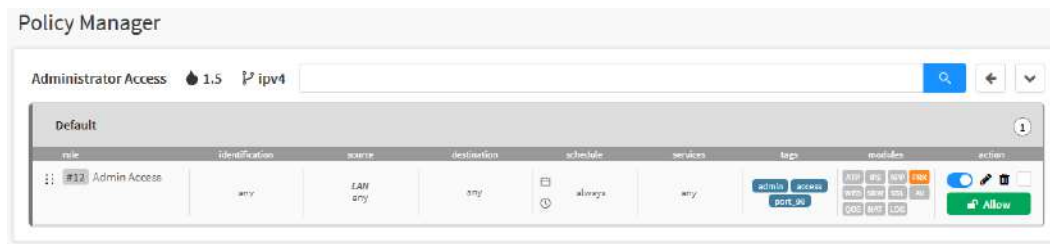
A seguir explicaremos cada coluna da aba Policy Templates:

- **Caixa de Seleção**: Selecciona o Template;
- **Name**: O nome do Template;
- **Description**: Determina a descrição do Template;
- **Type**: O tipo do IP;
- **Version**: A versão do UTM;
- **Actions**: Um conjunto de ações essenciais:
 - **Edit**: Ao clicar nesse ícone é possível renomear o template;
 - **Listar**: Visualiza o conteúdo do template, possibilitando inserir ou remover tags, criar, mover e deletar políticas, validá-las e por fim, efetuar buscas, esta opção oferece possibilidades semelhantes àquelas disponíveis no Policy Manager, com exceção de determinar a sua localização no “Header” ou “Footer”. Para mais informações a respeito, cheque [Policy Templates - Policy Manager](#);
 - **Delete**: Remove o Template.

A seguir analisaremos as funções do botão listar: [Policy Templates - Policy Manager](#).

Policy Templates - Policy Manager

Ao clicar no botão  em Policy Templates a seguinte tela será exibida:



Policy Templates – Policy Manager.

A tela *Policy Manager* exibe informações mais detalhadas dos *Policy Packages* criados.

O painel *Policy Manager* é dividido em:

- **Nome do Pacote:** Apresenta o nome do Pacote de Políticas cadastrado;
- **Versão do Sistema** : Apresenta a versão na qual o Pacote de Políticas foi criado. É de extrema importância criar Pacotes de Políticas da mesma versão que o UTM, caso contrário, o pacote não será compatível;
- **IP** : Representa o tipo de IP utilizado nos Pacotes de Políticas criados. Ex.: "IPv4";
- **Barra de Busca:** Tem como função possibilitar a localização de itens específicos, é possível clicar em alguns campos das colunas dentro do grupo de política para servir como filtro em uma busca mais específica;
- **Botão Back** : Retorna para o painel anterior;
- **Menu de Ações** : Apresenta um conjunto de opções contextuais:
 - [Create Template](#);
 - [Delete Templates](#);
 - [Clone Templates](#);
 - [Select All e Deselect All](#).

É importante, lembrar que as políticas são ordenadas por "Prioridade", sendo que elas são aplicadas considerando o método "*First Match Wins*" (Que literalmente quer dizer "O 1º entre os concorrentes VENCE"). Logo, as políticas localizadas acima tem prioridade enquanto as abaixo possuem menor prioridade.

As colunas do *Policy Manager* são divididas em:

- **Move** : Ao clicar e arrastar, move a ordem da política e permite reorganizar a prioridade de acordo com qual política está acima (*First Match Wins*);
- **Id** : Exibe o número de identificação da política, é possível clicar nele para servir como filtro no campo de busca;
- **Rule:** Exibe o nome da política;
- **Users:** Determina quais usuários são afetados pela política, é possível clicar neste campo para servir como filtro no campo de busca;
- **Source:** Exibe se a origem desta regra será a Zona de rede, endereço IP, interface de rede, Mac Address ou qualquer um destes, é possível clicar neste campo para servir como filtro no campo de busca;
- **Destination:** Determina o destino da regra, o endereço IP ou serviço, é possível clicar neste campo para servir como filtro no campo de busca;
- **Schedule:** Exibe caso a regra depende de um período de tempo ou agendamento, é possível clicar neste campo para servir como filtro no campo de busca;
- **Services:** Exibe os serviços que a regra afeta, é possível clicar neste campo para servir como filtro no campo de busca;
- **Tags:** Exibe as tags que foram adicionadas à essa regra, é possível clicar neste campo para servir como filtro no campo de busca;
- **Modules:** Determina com quais módulos do UTM a regra irá interagir, é possível clicar neste campo para servir como filtro no campo de busca;
- **Action:** Exibe alguns botões contextuais e qual ação a regra executa.
 - **Enabled**  ou **Disabled** : Através deste seletor, ativa ou desativa a regra;
 - **Edit** : Permite editar as configurações adicionadas na opção [Create Policy](#) do menu de ações;
 - **Delete** : Remove a política;

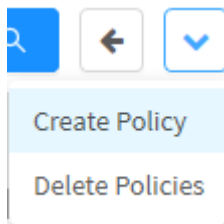
- **Select** : Permite a seleção das políticas de modo a interagirem com o menu de ações;
- **Action**: Determina o comportamento da política em questão, tendo como possibilidades:
 - : Como o próprio nome diz, esta opção serve para conceder acesso;
 - : O acesso é negado;
 - : O acesso é negado, porém uma mensagem de rejeição é exibida ao usuário.

Para mais informações a respeito de políticas, consulte o capítulo [POLICIES](#) do *Manual do UTM*.

Policy Templates - Menu de ações - Create Policy

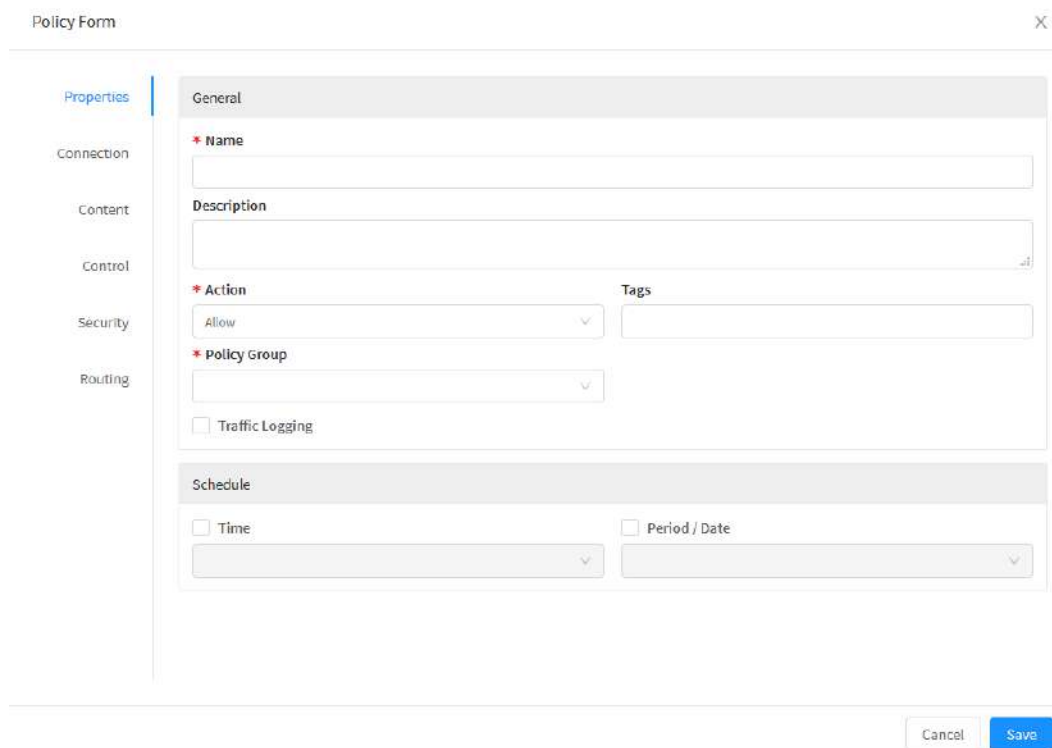
O botão "Create Policy" cria as políticas no grupo de políticas selecionando. Para criar uma *Policy*, siga os passos:

1. No menu de ações [], clique na opção "Create Policy";



Policy Manager – Menu de ações – Create Policy.

2. Surgirá a tela *New Policy*;



Policy Manager – New Policy.

Pra mais informações a respeito de como criar novas políticas, consulte [Policy Manager - Menu de ações - Create Policy](#).

Após concluir a criação da política, ela será adicionada ao pacote de política.

Policy Templates - Menu de ações - Delete Policies

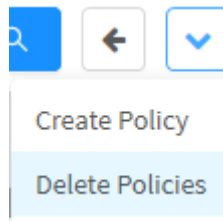
O botão "Delete Policies" deleta as Políticas selecionadas. Para deletar, siga os passos:

1. Selecione a(s) Política(s) que deseja deletar. Para selecionar, clique com o *mouse* no *checkbox*. Nos pacotes selecionados o *checkbox* mudará da cor cinza para azul []. Ex.: *Administrator CLI*;



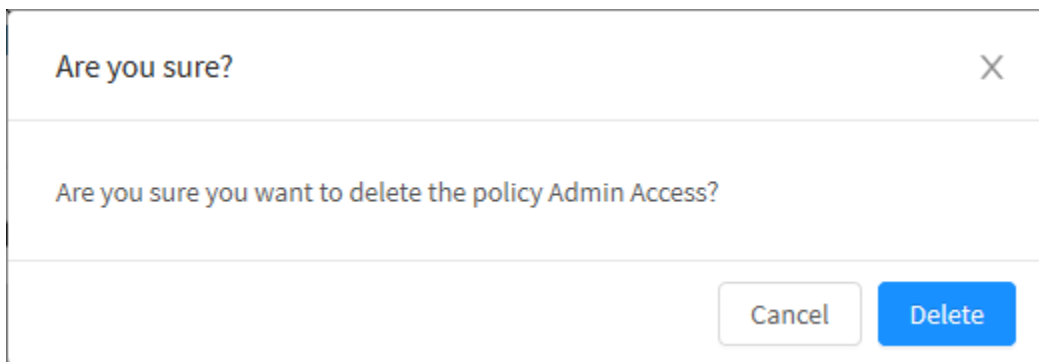
Política selecionada para ser deletada.

2. No **Menu de ações** [], clique na opção "Delete Policies";

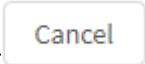


Policy Manager – Menu de ações – Delete Policies.

3. Surgirá a tela perguntando se deseja deletar os itens:



Policy Manager – Are you sure you want to delete the policy

Caso desejar cancelar, clique no botão **Cancel** []. Para concluir, clique no botão **Delete** [].

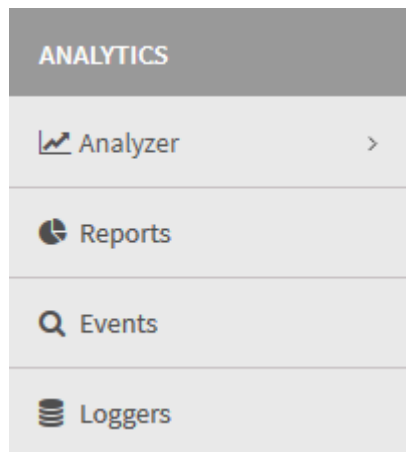
 Package deleted successfully

Package deleted successfully

A *Policy* foi removida com sucesso.

GSM - ANALYTICS

Através do menu "Analytics" é possível analisar relatórios, eventos e gerenciar *loggers*.



Menu *Analytics*.

Contém as opções:

- [Analyzer](#);
- [Reports](#);
- [Events](#);
- [Loggers](#).

Analyzer

O Blockbit GSM – *Analyzer* é um módulo de avaliação e criação de relatórios avançados, proporcionando uma perspectiva holística na detecção, ao executar monitoramento de tráfego de rede em tempo real em múltiplos pontos e segmentos de rede, o *analyzer* possibilita a investigação e execução de ações orientadas no combate a ameaças, tentativas de intrusão e utilização de aplicações não autorizadas.

O Blockbit GSM – *Analyzer* atua recebendo os dados emitidos pelos UTMs, que são administrados nas opções do menu [Blockbit GSM - Management](#), gerando diversos tipos de relatórios e *logs*.

O GSM também prove uma visualização sumarizada de todas as aplicações, ameaças (IPS, anti vírus, anti -malware) e URLs analisadas pelo firewall;

O *analyzer* oferece as seguintes funcionalidades:

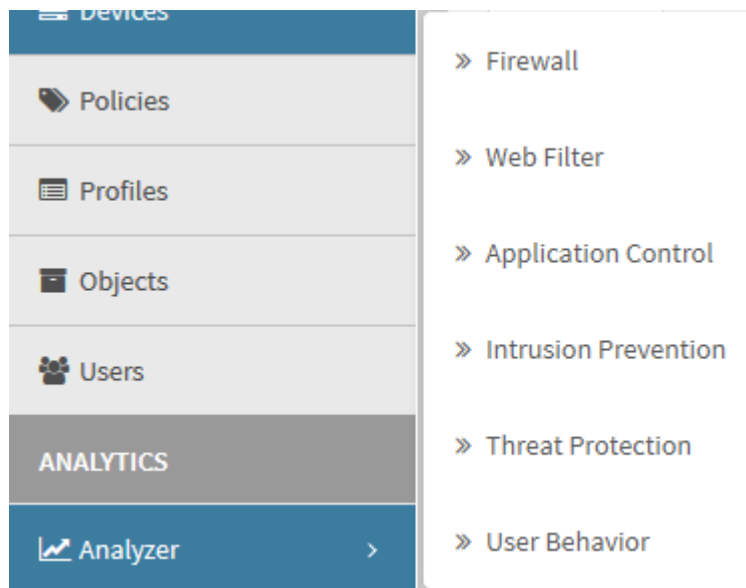
- Ter um registro de todas as atividades executadas pelos seus usuários e também a sua duração;
- Ter resumo da performance dos *appliances* e dos *loggers* utilizados;
- Visualizar eventuais ameaças à segurança e prevenção de intrusões;
- Efetividade de filtros *web* e aplicação de políticas;
- Principais aplicações de alto risco acessadas;
- E mais...

Para acessá-lo, selecione a opção “*Analyzer*”:



Analytics - Analyzer

Ao efetuar essa ação o seguinte menu será exibido:



Analyzer – Submenu

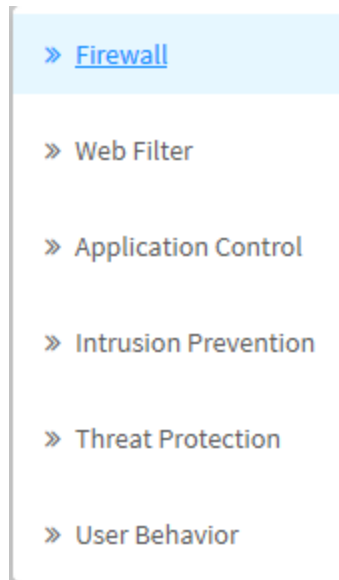
Selecione a opção desejada. As opções disponíveis são:

- [Firewall](#);
- [Web Filter](#);
- [Application Control](#);
- [Intrusion Prevention](#);
- [Threat Protection](#);

- User Behavior.

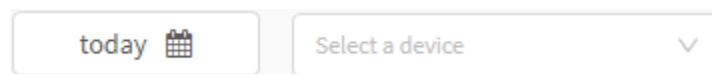
Firewall

Para acessar os relatórios de tráfego de rede, clique no ícone “Analyzer” localizado na lateral esquerda, um menu *dropdown* será exibido, selecione a opção “Firewall”.



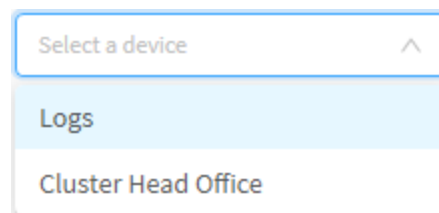
Firewall

Para gerar um relatório, localize a caixa de seleção que está posicionada no topo direito da tela, conforme ilustrado a seguir:



Firewall – Caixa de Seleção.

Nesta caixa de seleção estarão listadas todos os *devices* (ou grupos de *devices*) previamente cadastradas no [Device Manager](#), para criar um relatório, selecione o *device* desejado.

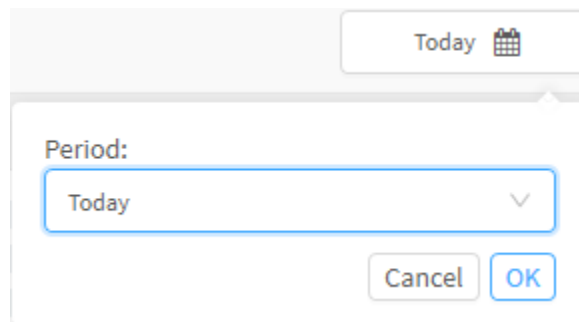


Firewall – Selecionando Device

Logo do lado direito de onde acabamos de selecionar os *devices*, é possível visualizar uma caixa de seleção de datas, o objetivo desta mesma é basicamente permitir uma filtragem de resultados ainda mais precisa, as opções possíveis são:

- **By date:** Determina uma data específica;
- **By period:** Exibe resultados de uma data inicial (“*Start date*”) até uma data final (“*End date*”);
- **Today:** Exibe resultados especificamente para a data de hoje;
- **Yesterday:** Exibe resultados especificamente para ontem;
- **Last 7 days:** Filtra especificamente os resultados dos últimos 7 dias;
- **Last 30 days:** Filtra especificamente os resultados dos últimos 30 dias;
- **This month:** Exibe os resultados deste mês;

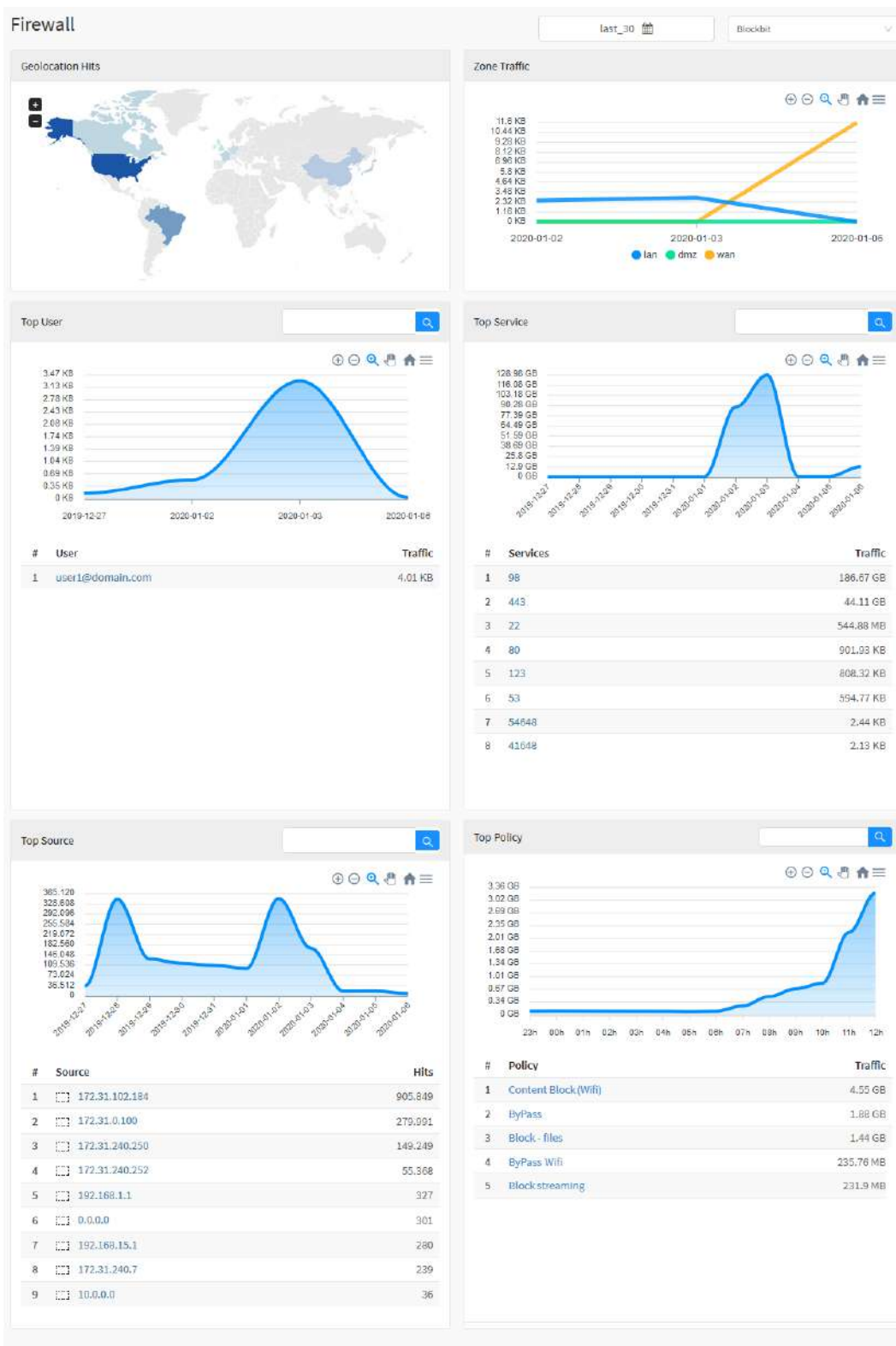
- **Last month:** Exibe os resultados do último mês.



Firewall – Seleção de Data

Selecione a data desejada e clique em **Ok** [];

A tela abaixo será exibida:



Analyzer - Firewall

A maioria dos gráficos desta aba possui um menu de navegação e uma barra de busca.

O menu de navegação possui os seguintes botões:

- : Serve para dar um zoom;

- []: Tem como função remover o zoom;
- []: Serve para fazer um zoom de seleção;
- []: Serve para mover o gráfico;
- []: Reseta o gráfico para a posição inicial;
- []: Permitir baixar este diagrama no formato *svg*, *png* ou *csv*.

A barra de busca permite pesquisar um item específico e modificar os diagramas de acordo com os resultados da pesquisa.

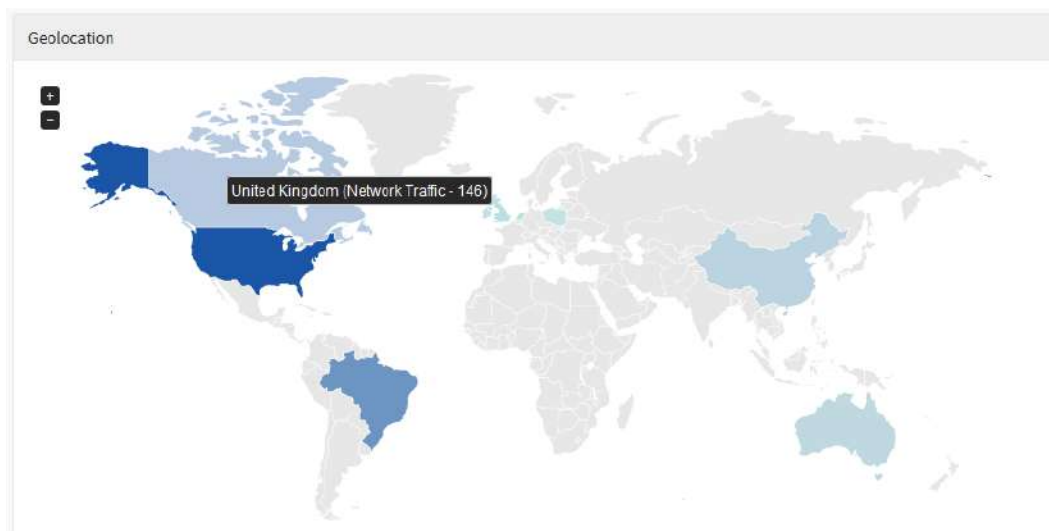
Para efetuar uma pesquisa, digite um termo na barra de busca e clique no **botão de busca** [].

A seguir, analisaremos em detalhes os componentes de “*Firewall*”:

- [Geolocation](#);
- [Zone Traffic](#);
- [Top User](#);
- [Top Service](#);
- [Top Source](#);
- [Top Policy](#).

Firewall – Geolocation

Em "Geolocation" é exibido o destino das conexões dos usuários da rede, o mapa global demonstra através de uma legenda colorida a quantia de acessos feitos pelos usuários. Ao passar o mouse por cima dos países um número total de acessos é exibido, além disso, o país referente a esse valor é destacado no mapa.

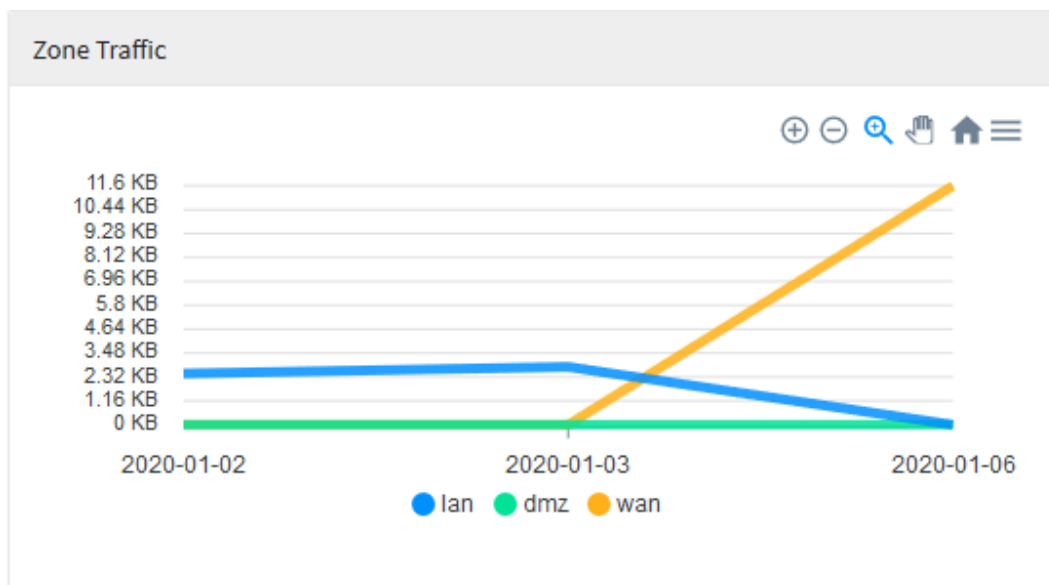


Firewall – Geolocation

Firewall – Zone Traffic

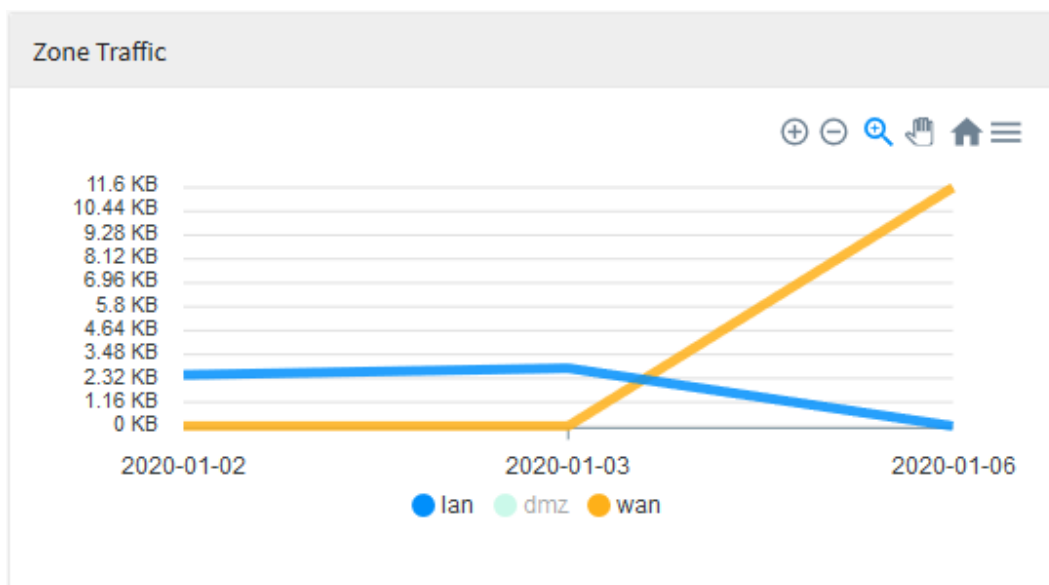
Em "Zone Protection" temos um gráfico demonstrando a quantia de tráfego em determinada zona, através de um gráfico de linha é possível observar esses montantes sendo ilustrados ao longo de um intervalo de tempo. Ao clicar sobre o tipo de rede utilizado (por exemplo: "LAN", "DMZ", "WAN" e etc), o diagrama é alterado de forma a exibir a opção selecionada, o que permite analisar com mais detalhamento o tráfego de acordo com as datas selecionadas.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta [página](#).



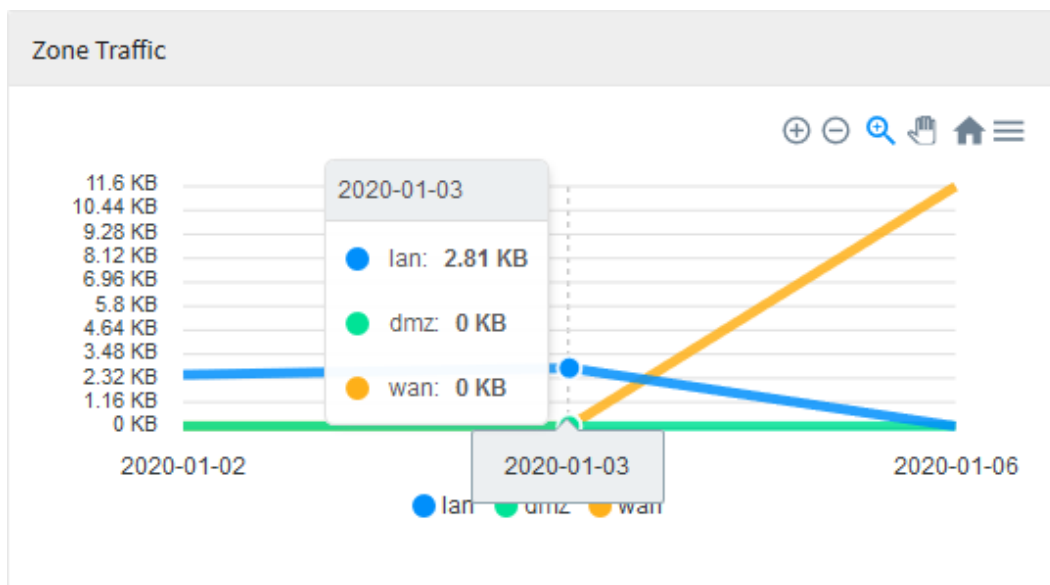
Firewall – Zone Traffic

É possível clicar nas legendas abaixo do gráfico, para ocultar alguma das linhas de forma a ilustrar as informações relevantes, conforme demonstrado abaixo:



Firewall – Zone Traffic - Linha DMZ oculta

Ao passar o mouse por cima do gráfico, um resumo de todo o tráfego do período é exibido, conforme demonstrado na imagem abaixo:

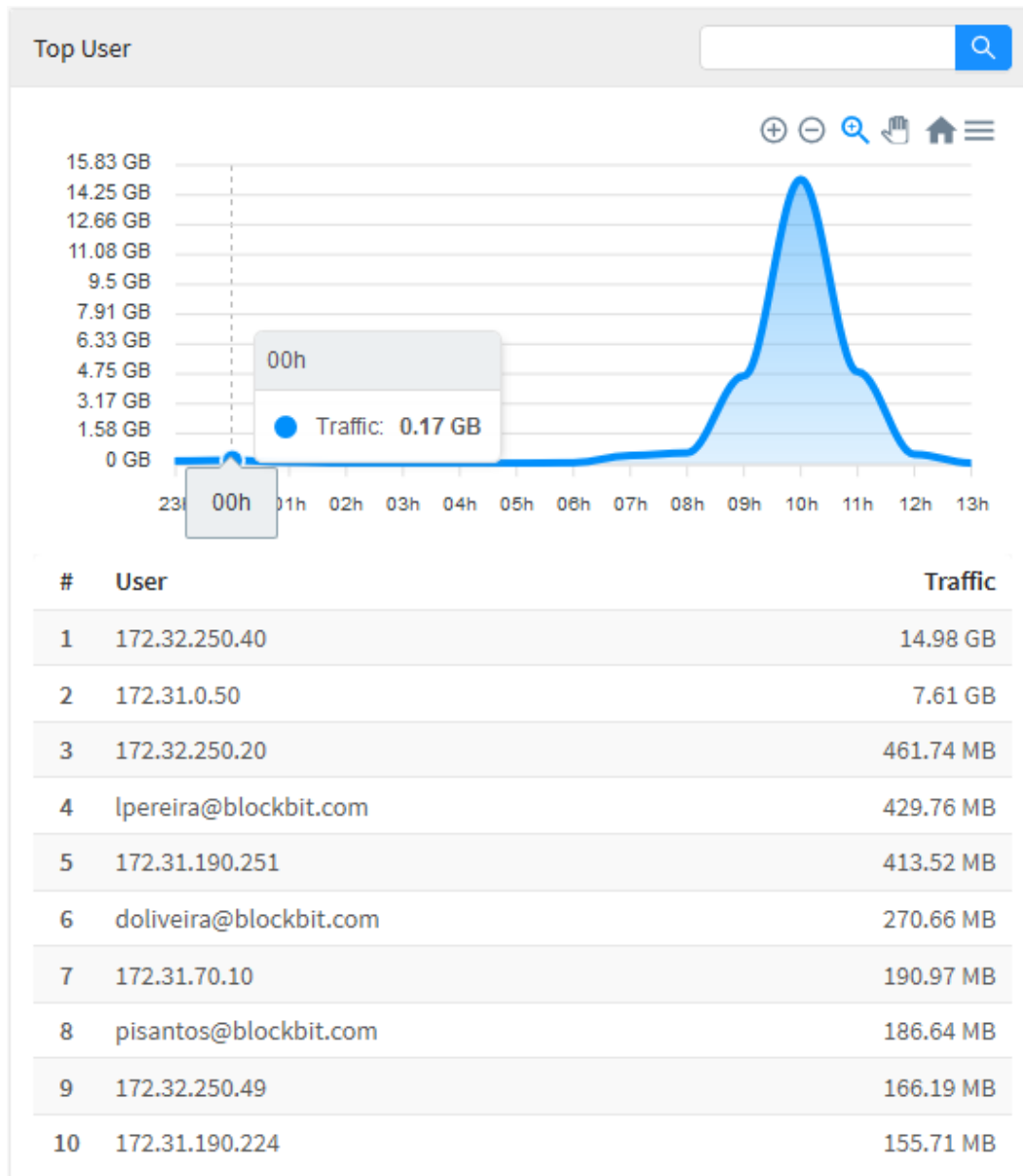


Firewall – Zone Traffic - Resumo dos resultados

Firewall – Top User

Em “*Top User*” tem-se um diagrama demonstrando por data quando houve o maior tráfego de rede e uma lista exibindo dez usuários classificados por ordem de uso de *Gigabytes*. Ao passar o mouse por cima do gráfico, o tráfego de rede em *Gigabytes* de um determinado período é exibido, conforme demonstrado na imagem abaixo. Por fim, ao clicar em um desses usuários ou *IPs*, você será redirecionado para [Events](#) usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito do usuário selecionado.

Para mais informações a respeito do menu de navegação e da barra de busca presente no topo deste gráfico cheque esta [página](#).

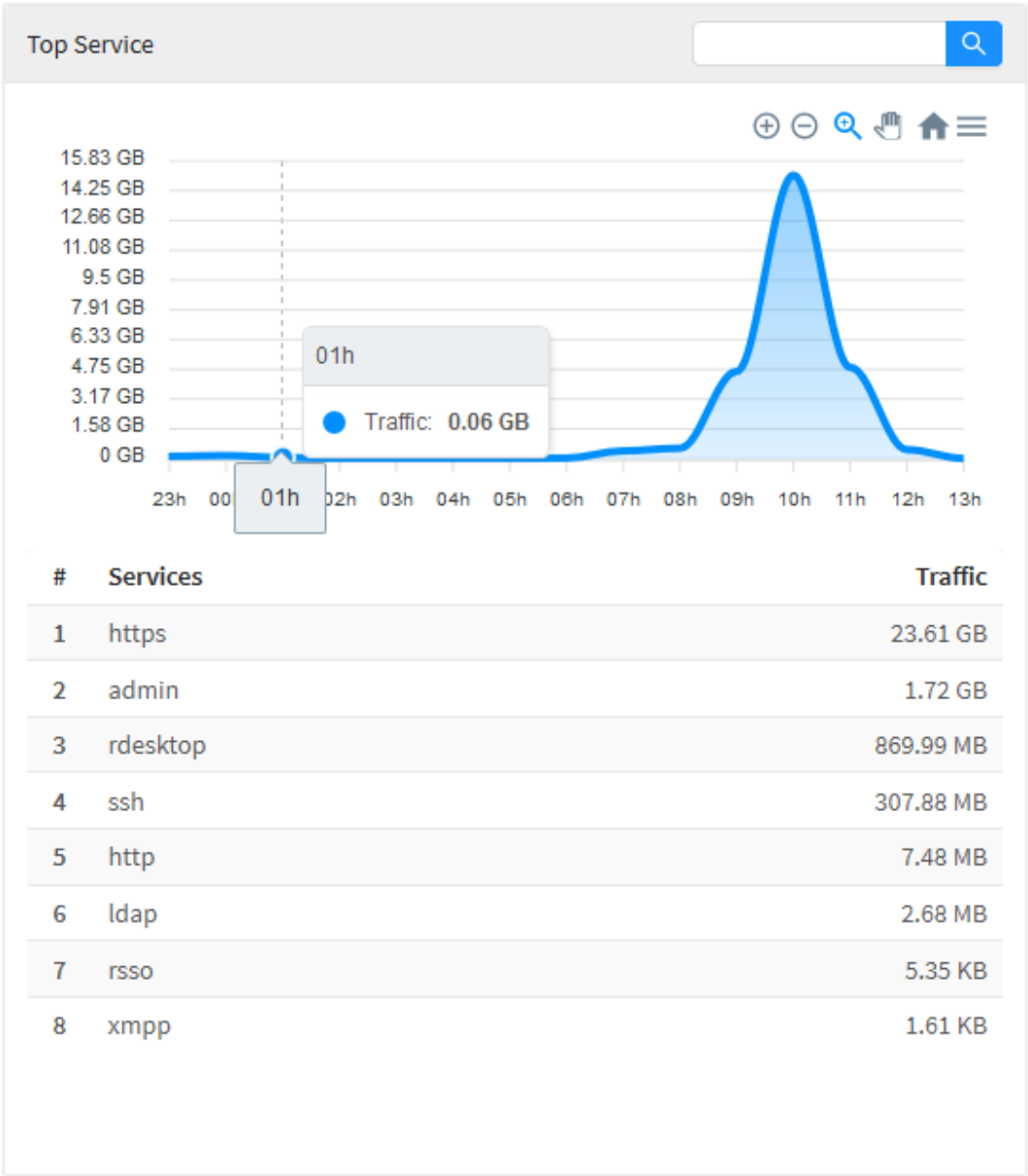


Firewall – Top User

Firewall – Top Service

Em "Top Service" tem-se um diagrama demonstrando por data quando houve maior tráfego de rede e uma lista exibindo os dez tipos de serviços mais usados, sendo estes classificados por ordem de uso de *Gigabytes*. Ao passar o mouse por cima do gráfico, o tráfego de rede em *Gigabytes* de um determinado período é exibido, conforme demonstrado na imagem abaixo.

Para mais informações a respeito do menu de navegação e da barra de busca presente no topo deste gráfico cheque esta [página](#).

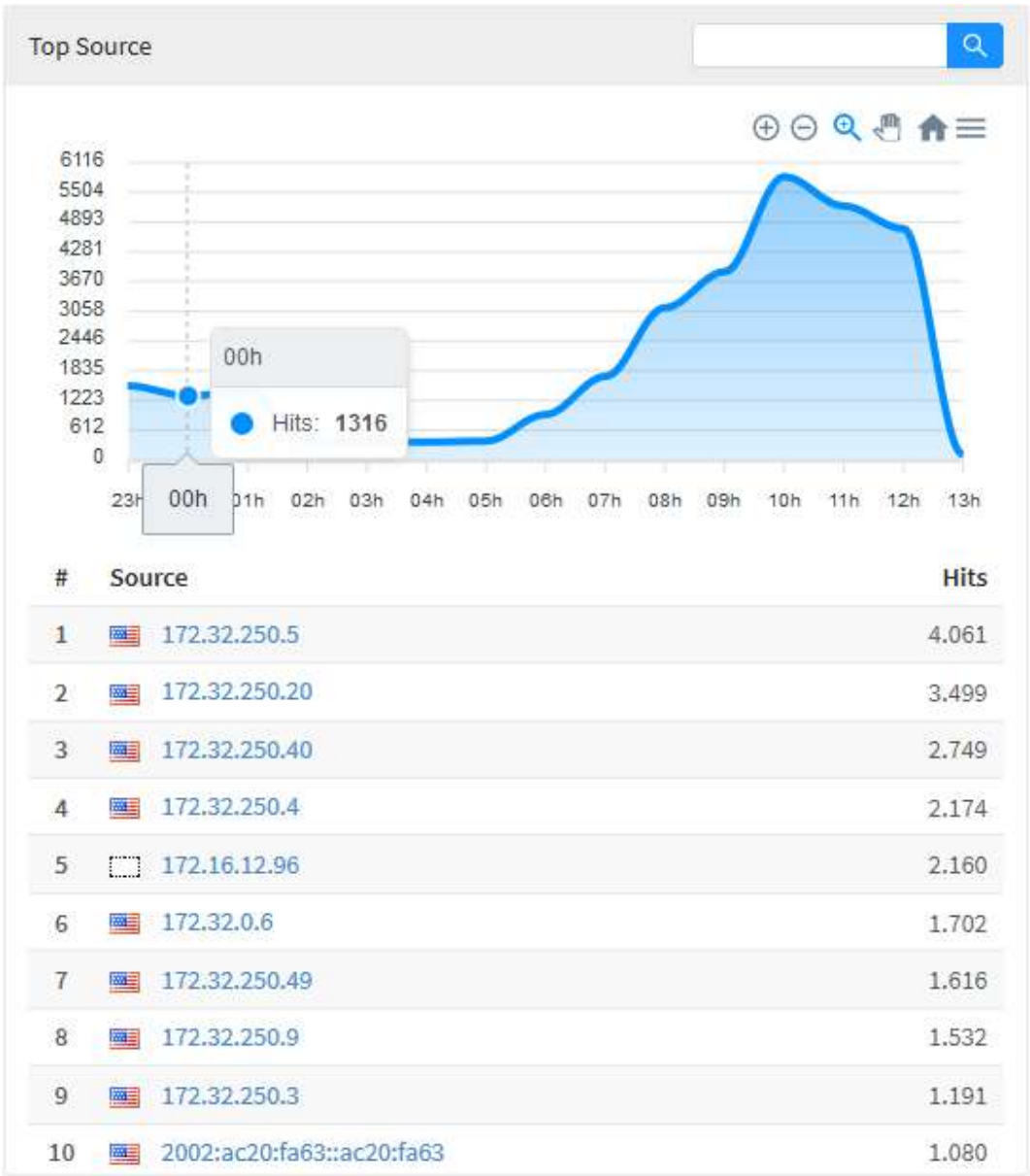


Firewall – Top Service

Firewall – Top Source

Em “Top Source” tem-se um diagrama demonstrando por data quando houve maior tráfego de rede e uma lista exibindo as dez maiores fontes de tráfego de rede classificadas por ordem de uso. Ao passar o mouse por cima do gráfico, o tráfego de rede de um determinado período é exibido, conforme demonstrado na imagem abaixo. Por fim, ao clicar em um desses IPs, você será redirecionado para [Events](#) usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito do IP selecionado.

Para mais informações a respeito do menu de navegação e da barra de busca presente no topo deste gráfico cheque esta [página](#).

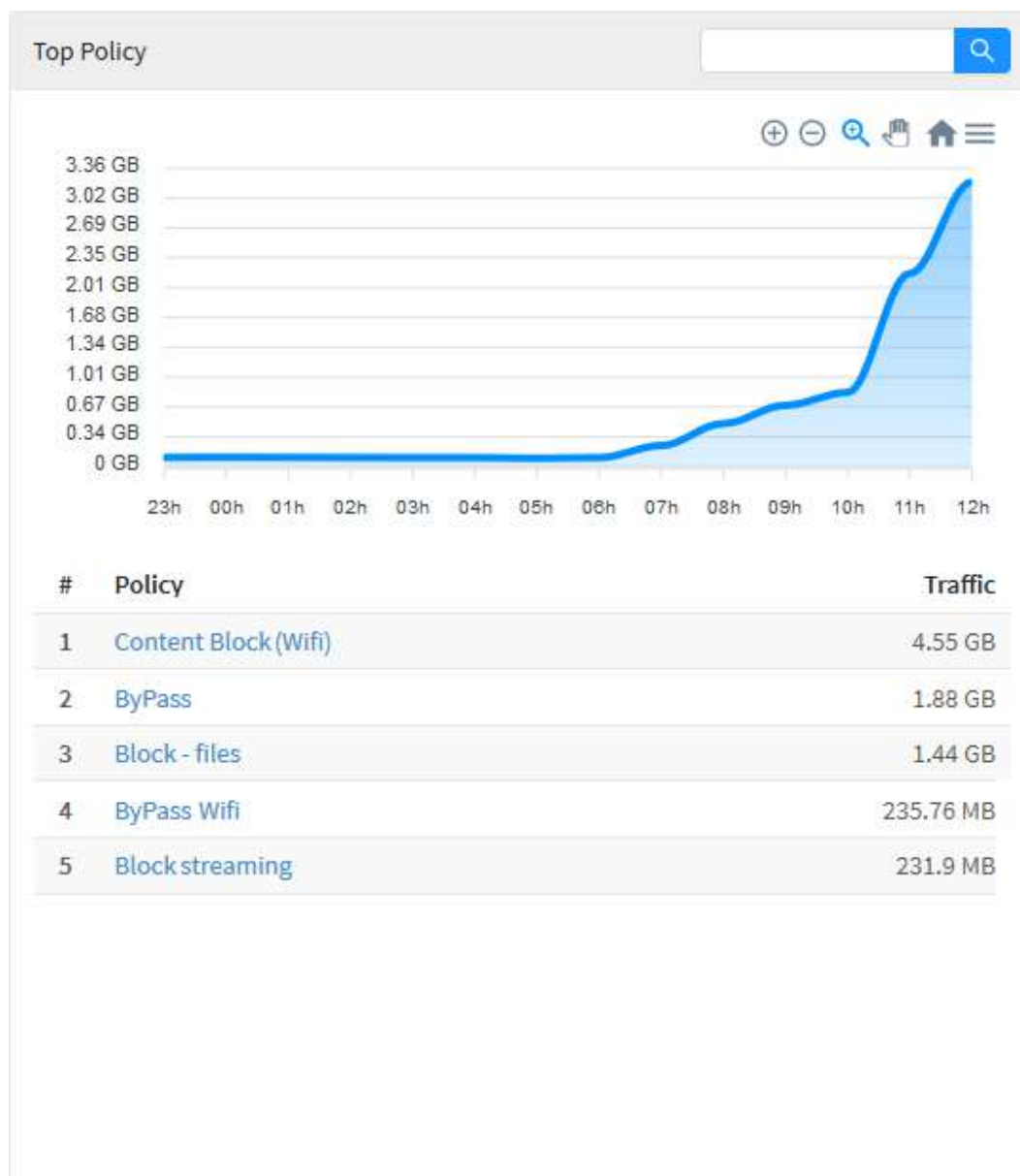


Firewall – Top Source

Firewall – Top Policy

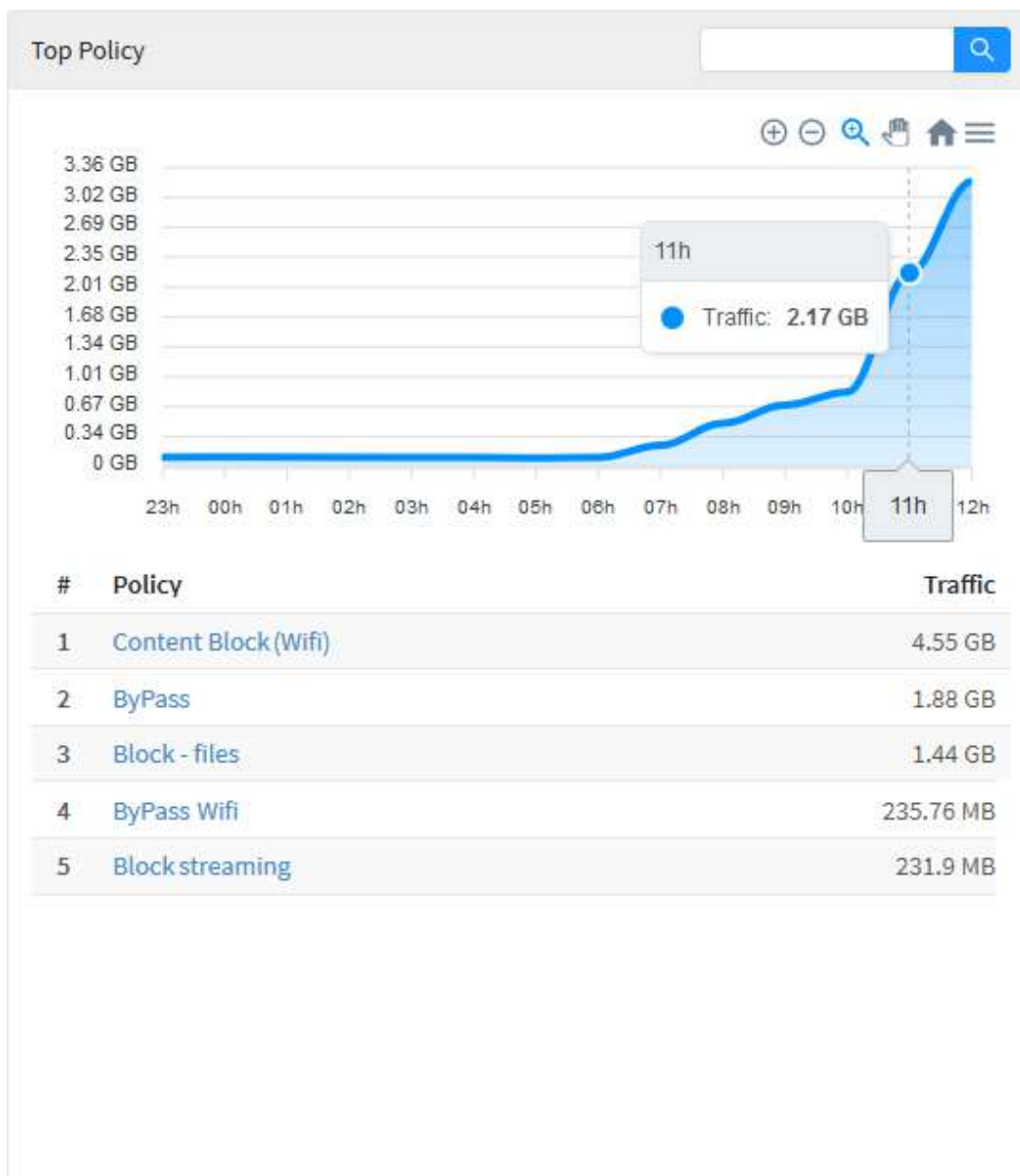
Em “*Top Policy*” tem-se um diagrama demonstrando por data quando houve maior tráfego de rede e uma lista exibindo os dez tipos de políticas mais usadas, sendo estas classificadas por ordem de uso de *Gigabytes*.

Para mais informações a respeito do menu de navegação e da barra de busca presente no topo deste gráfico cheque esta [página](#).



Firewall – Top Policy

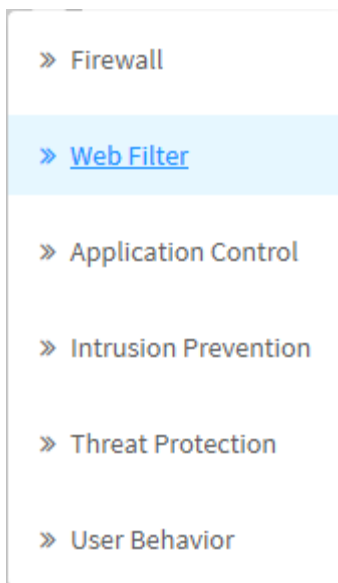
Ao passar o mouse por cima do gráfico, o tráfego de rede em *Gigabytes* de um determinado período é exibido, conforme demonstrado na imagem abaixo.



Firewall – Top Service - Resumo do tráfego de um período

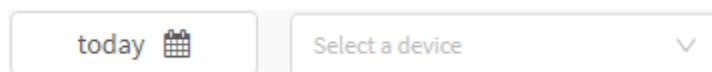
Web Filter

Para acessar os relatórios de *web filter*, clique no ícone “Analyzer” localizado na lateral esquerda, um menu *dropdown* será exibido, selecione a opção “Web Filter”.



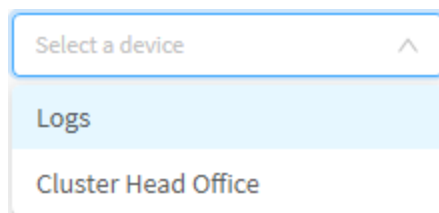
Web Filter

Para gerar um relatório, localize a caixa de seleção que está posicionada no topo direito da tela, conforme ilustrado a seguir:



Caixa de Seleção

Nesta caixa de seleção estarão listadas todos os *devices* (ou grupos de *devices*) previamente cadastradas no [Device Manager](#), para criar um relatório, selecione o *device* desejado.

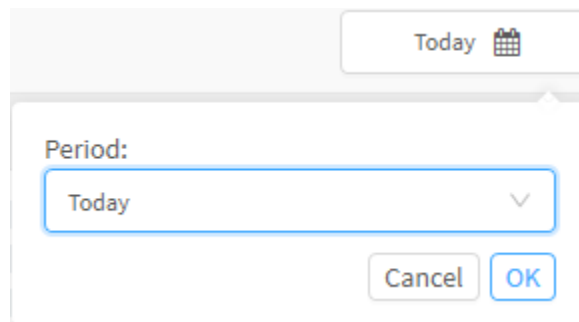


Selecionando Device

Logo do lado de onde acabamos de selecionar os *devices*, é possível visualizar uma caixa de seleção de datas, o objetivo desta mesma é basicamente permitir uma filtragem de resultados ainda mais precisa, as opções possíveis são:

- **By date:** Determina uma data específica;
- **By period:** Exibe resultados de uma data inicial (“*Start date*”) até uma data final (“*End date*”);
- **Today:** Exibe resultados especificamente para a data de hoje;
- **Yesterday:** Exibe resultados especificamente para ontem;
- **Last 7 days:** Filtra especificamente os resultados dos últimos 7 dias;
- **Last 30 days:** Filtra especificamente os resultados dos últimos 30 dias;
- **This month:** Exibe os resultados deste mês;

- **Last month:** Exibe os resultados do último mês.



The image shows a date selection dialog box. At the top right, there is a button labeled "Today" with a calendar icon. Below this, the text "Period:" is followed by a dropdown menu that currently displays "Today" and a downward arrow. At the bottom right of the dialog, there are two buttons: "Cancel" and "OK".

Seleção de Data

Selecione a data desejada e clique em **Ok** [];

Web Filter

today 📅

Blockbit

Total Traffic

📶 544.35 MB

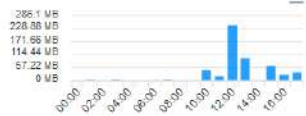
Allowed Sites

✓ 6.528

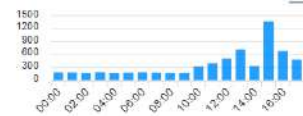
Denied Sites

🚫 87

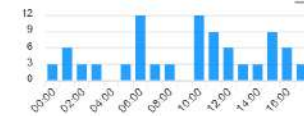
History



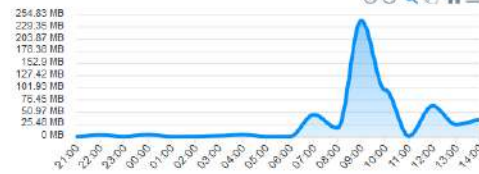
History



History



Users



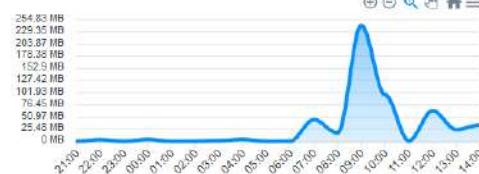
📶 Total Traffic
544.35 MB

📊 Total Hits
6.615

Top Users

#	Name	Hits	Traffic
1	172.32.250.24	84	205.75 MB
2	172.32.250.40	1,353	91.02 MB
3	casantos@blockbit.com	262	80.51 MB
4	172.32.250.41	139	43.23 MB
5	172.32.250.8	46	39.52 MB
6	172.32.250.99	166	39.18 MB
7	172.32.250.46	351	18.15 MB
8	172.32.250.1	80	12.29 MB
9	doliveira@blockbit.com	166	3.02 MB
10	172.32.250.49	506	2.74 MB

History Profiles



📶 Total Traffic
544.35 MB

📊 Total Hits
6.615

Top Profiles

#	Name	Hits	Traffic
1	Content Filtering (Wifi)	3,847	347.06 MB
2	ByPass SSL (Wifi)	2,681	197.29 MB
3	Block - filestreamingservice	87	0 Bytes

History Categories



📶 Total Traffic
497.46 MB

📊 Total Hits
6.296

Top Categories

#	Name	Hits	Traffic
1	Proxy Avoidance	52	276.34 MB
2	Information Technology	4,375	185.8 MB
3	Streaming Media	17	21.13 MB
4	Restaurants and Dining	93	0.80 MB
5	Business and Economy	190	1.53 MB
6	Government	20	1.56 MB
7	Search Engines and Portals	613	1.04 MB
8	News and Media	12	690.83 KB
9	Travel	7	657.2 KB
10	Freeware and Software Download	626	469.41 KB

History Domains

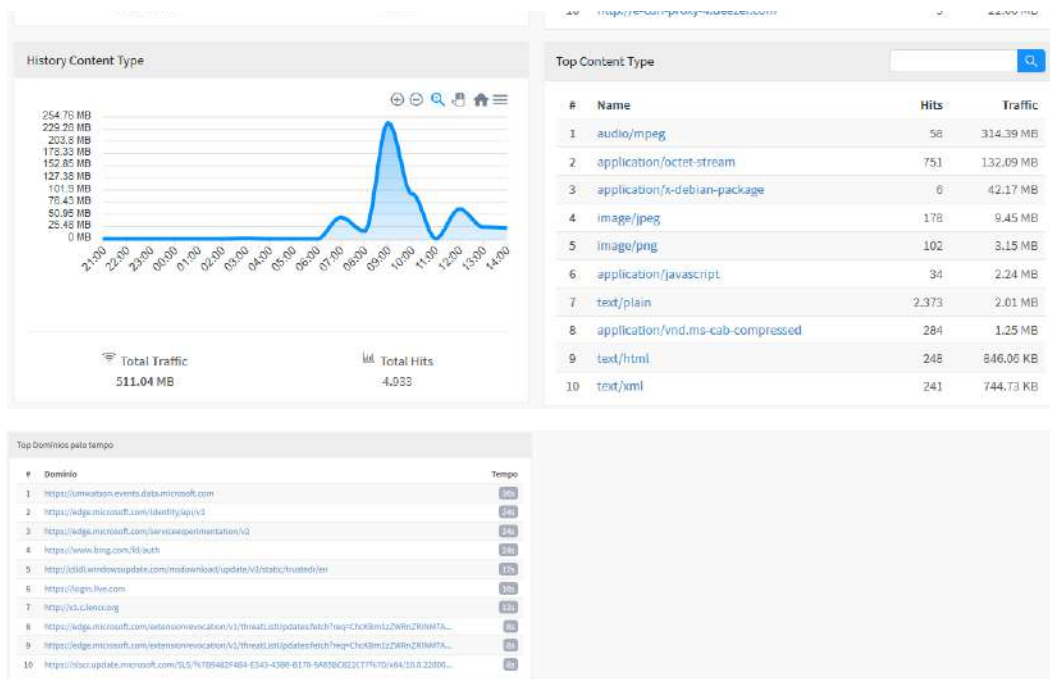


📶 Total Traffic
544.35 MB

📊 Total Hits
6.615

Top Domains

#	Name	Hits	Traffic
1	http://officecdn.microsoft.com.edgesuite.net	526	88.26 MB
2	http://br.archive.ubuntu.com	59	44.11 MB
3	http://e-cdn-proxy-b.deezer.com	7	42.47 MB
4	http://e-cdn-proxy-f.deezer.com	7	40.42 MB
5	http://e-cdn-proxy-a.deezer.com	6	31.51 MB
6	http://e-cdn-proxy-8.deezer.com	4	26.08 MB
7	http://e-cdn-proxy-7.deezer.com	4	25.01 MB
8	http://au.download.windowsupdate.com	63	23.96 MB
9	http://e-cdn-proxy-5.deezer.com	5	22.92 MB
10	http://e-cdn-proxy-3.deezer.com	5	17.68 MB



Analyzer - Web Filter

A maioria dos gráficos desta aba possui um menu de navegação e uma barra de busca.

O menu de navegação possui os seguintes botões:

- : Serve para dar um zoom;
- : Tem como função remover o zoom;
- : Serve para fazer um zoom de seleção;
- : Serve para mover o gráfico;
- : Reseta o gráfico para a posição inicial;
- : Permitir baixar este diagrama no formato *svg*, *png* ou *csv*.

A barra de busca permite pesquisar um item específico e modificar os diagramas de acordo com os resultados da pesquisa.

Para efetuar uma pesquisa, digite um termo na barra de busca e clique no **botão de busca**

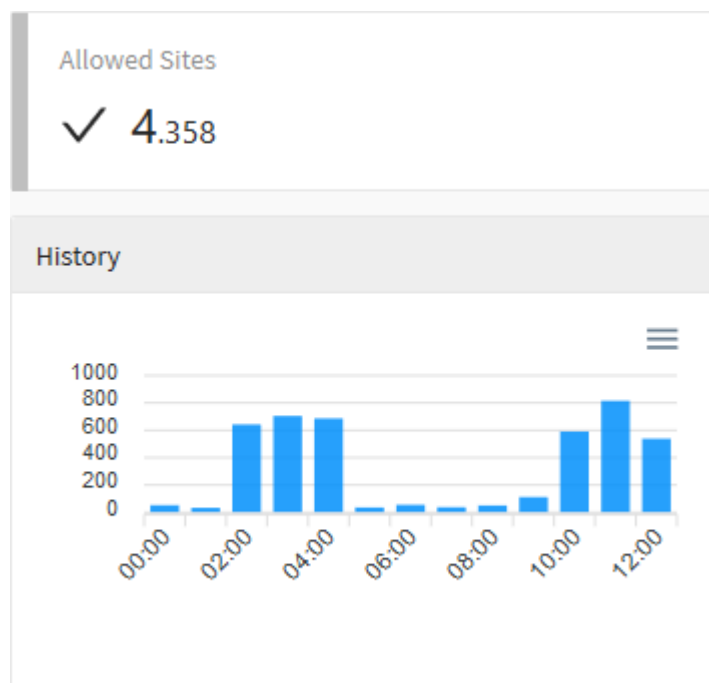
A seguir, analisaremos em detalhes os componentes de “Web Filter”:

- Total Traffic e History;
- Allowed Sites e History;
- Denied Sites e History;
- Total Traffic e Total Hits;
- Top Users;
- History Profiles - Total Traffic e Total Hits;
- Top Profiles;
- History Categories - Total Traffic e Total Hits;
- Top Categories;
- History Domains - Total Traffic e Total Hits;
- Top Domains;
- History Content Types - Total Traffic e Total Hits;
- Top Content Type.
- Top Domains by Time.

Web Filter - Allowed Sites e History

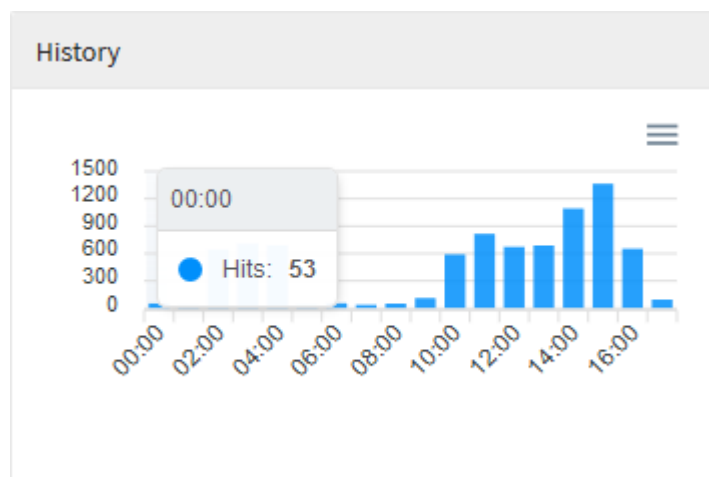
O painel “*Allowed Sites*” exibe um total de páginas que seguindo as políticas tiveram seu acesso autorizado. Logo abaixo, é mostrado o histórico em um gráfico de barras exibindo a quantia de acessos por dia.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta [página](#).



Web Filter – Allowed Sites

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:

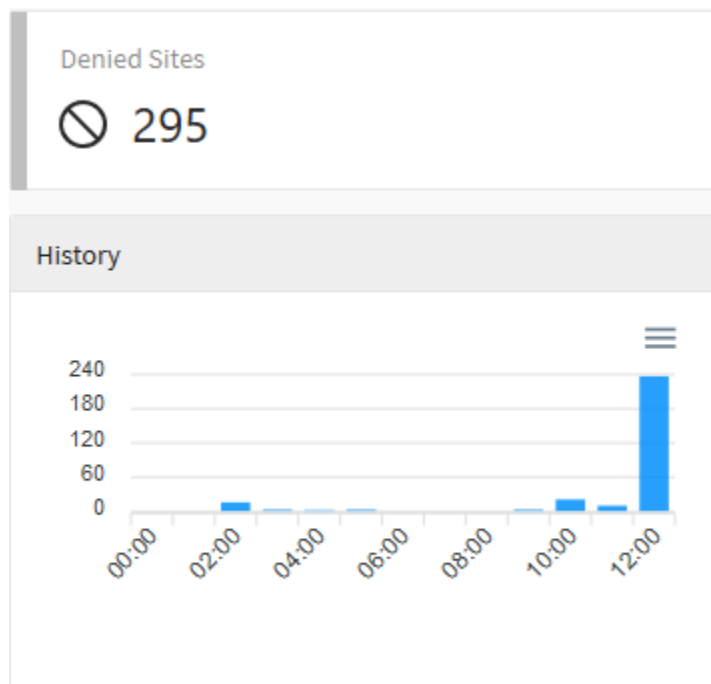


Web Filter – Allowed Sites - Resumo do Período

Web Filter - Denied Sites e History

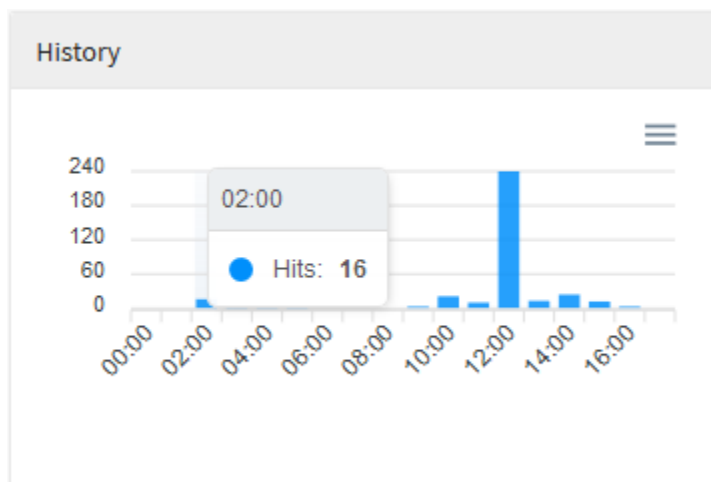
O painel “*Sites Denied*” mostra uma somatória de todas as páginas que seguindo as políticas tiveram seu acesso negado. Logo abaixo, é demonstrado o histórico em um gráfico de barras mostrando a quantia de acessos por dia.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta [página](#).



Web Filter – Denied Sites

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:

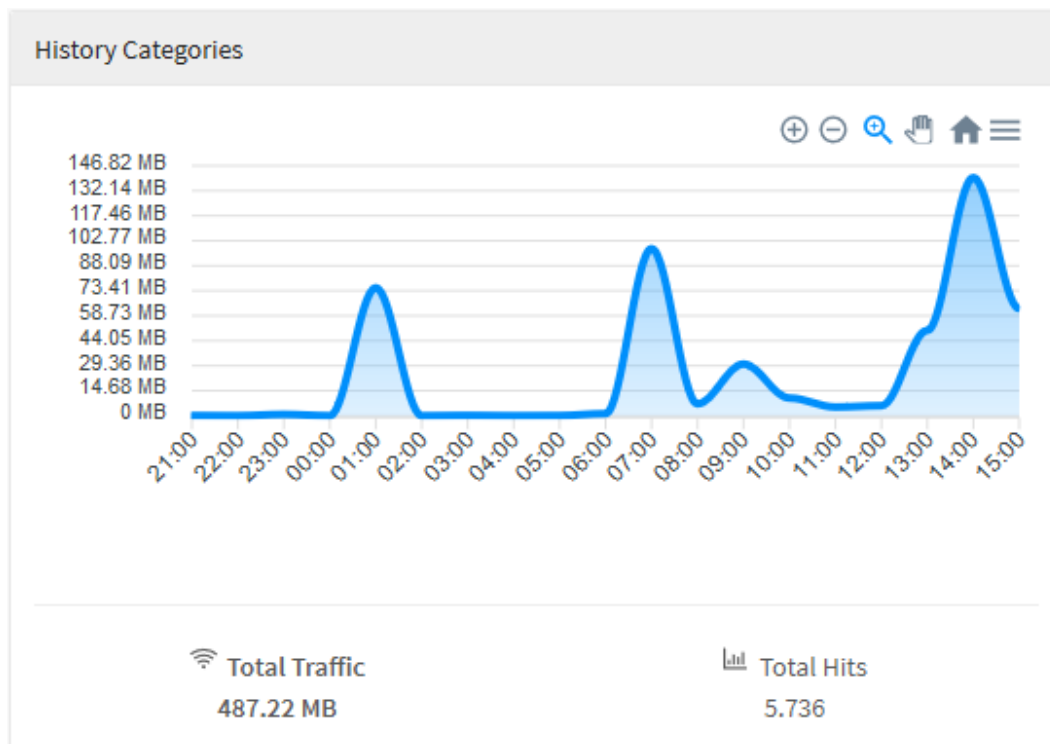


Web Filter – Denied Sites - Resumo do Período

Web Filter - History Categories - Total Traffic e Total Hits

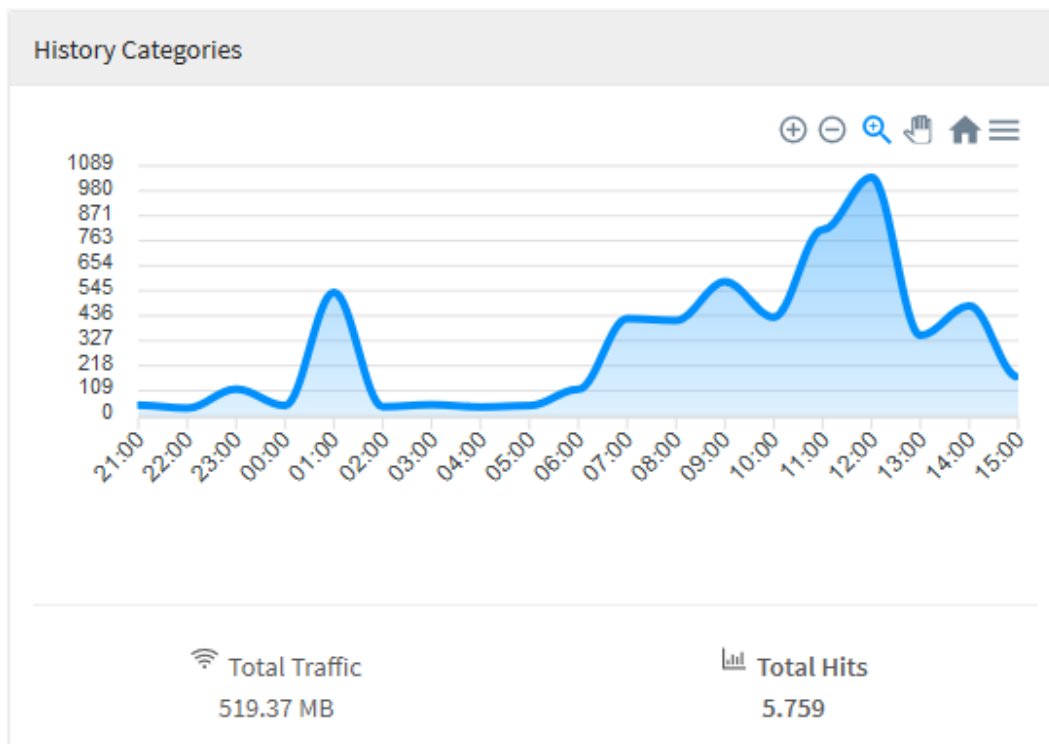
Em "History Categories", temos um gráfico que exibe informações especificamente relacionadas as categorias de rede, sua função é demonstrar quando alguma categoria foi aplicada em um dos acessos. Nessa área temos "Total Traffic" onde é exibido o total de tráfego de rede em *Gigabytes* por dia e "Total Hits" que demonstra o total de acessos para cada um dos dias pesquisados.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta [página](#).



Web Filter – History Categories – Total Traffic

Ao clicar em cada uma dessas legendas, o gráfico será automaticamente modificado para ilustrar as informações relevantes, conforme demonstrado abaixo:



Web Filter – History Categories – Total Hits

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:

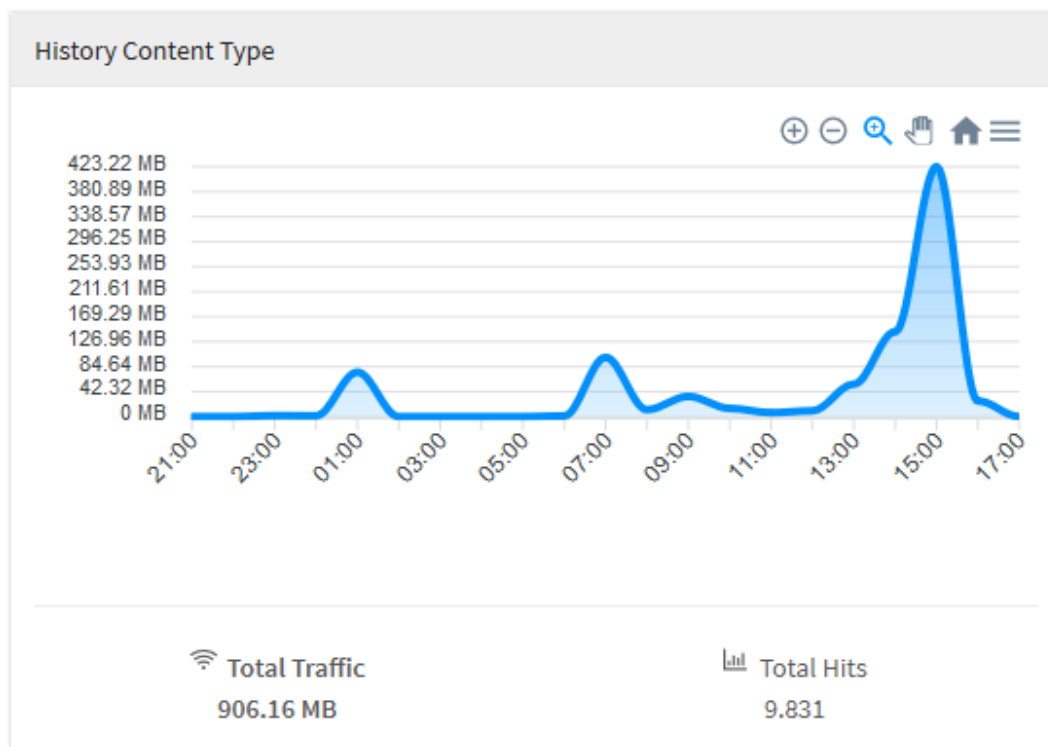


Web Filter – History Categories – Resumo do período

Web Filter - History Content Types - Total Traffic e Total Hits

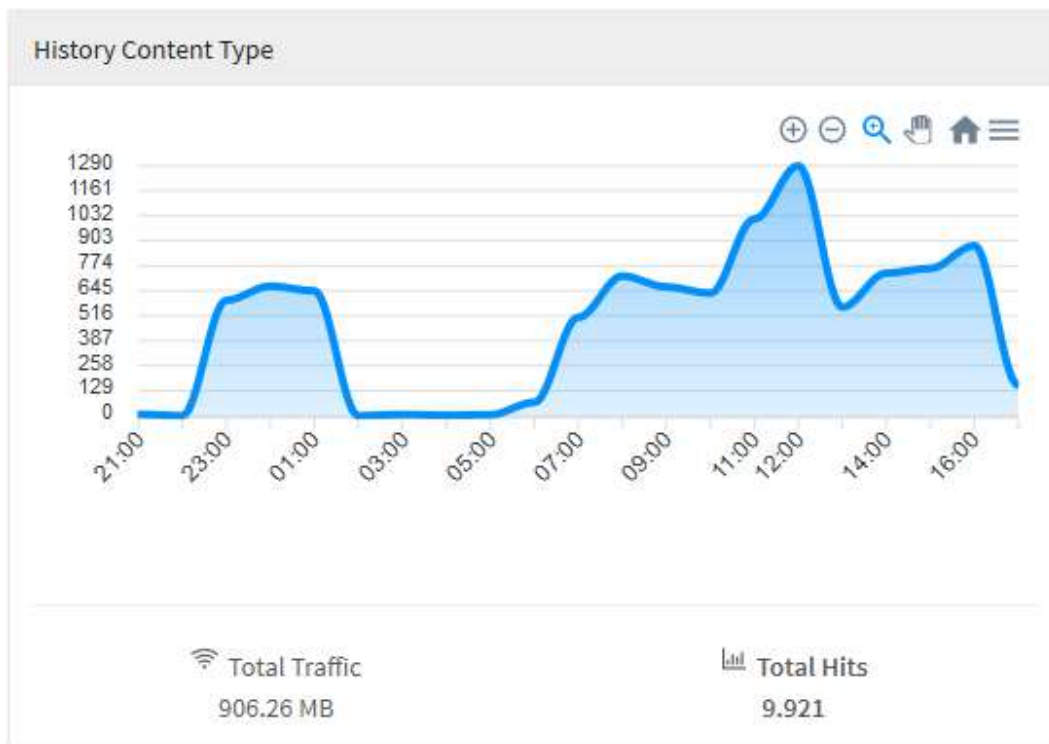
Em "Content Type", temos um gráfico cuja função é demonstrar quando algum tipo de conteúdo foi acessado. Nessa área temos "Total Traffic" onde é exibido o total de tráfego de rede em *Gigabytes* por dia e "Total Hits" que demonstra o total de acessos para cada um dos dias pesquisados.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta [página](#).



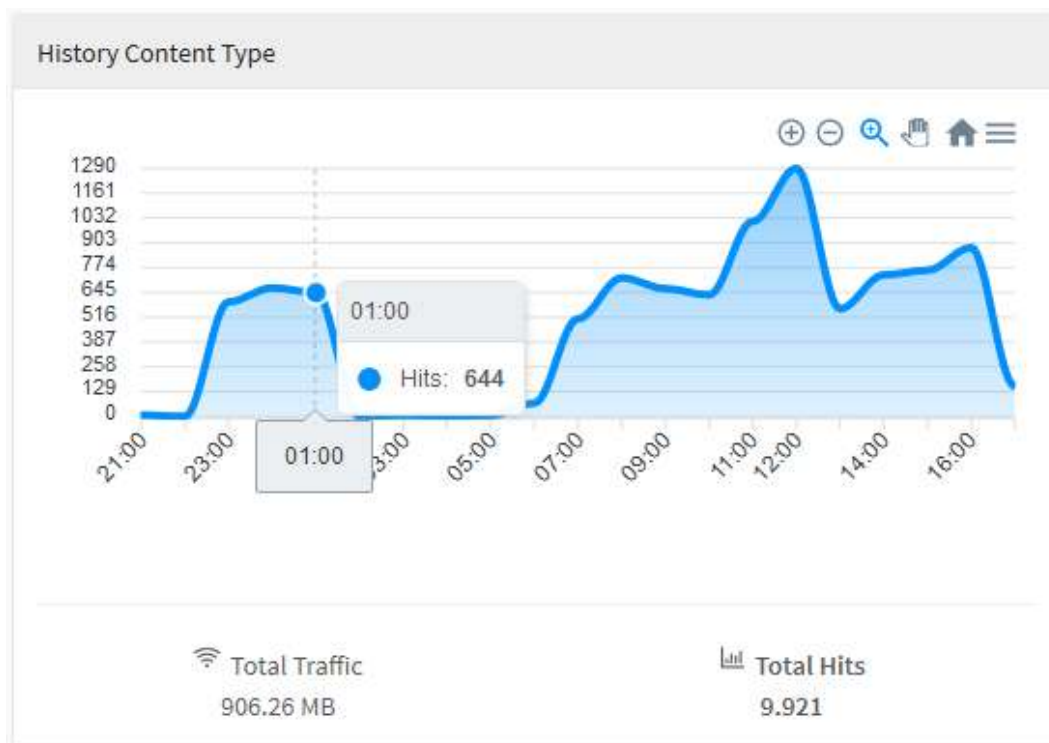
Web Filter – History Content Type – Total Traffic

Ao clicar em cada uma dessas legendas, o gráfico será automaticamente modificado para ilustrar as informações relevantes, conforme demonstrado abaixo:



Web Filter – History Content Type – Total Hits

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:

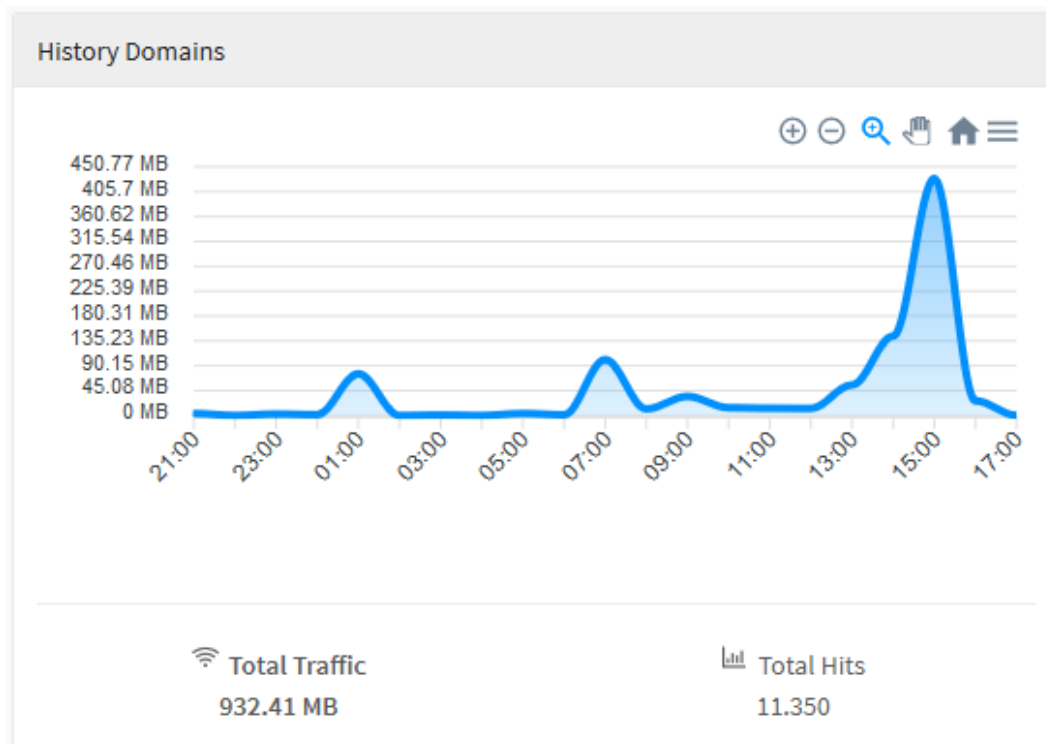


Web Filter – History Content Type - Resumo do Período

Web Filter - History Domains - Total Traffic e Total Hits

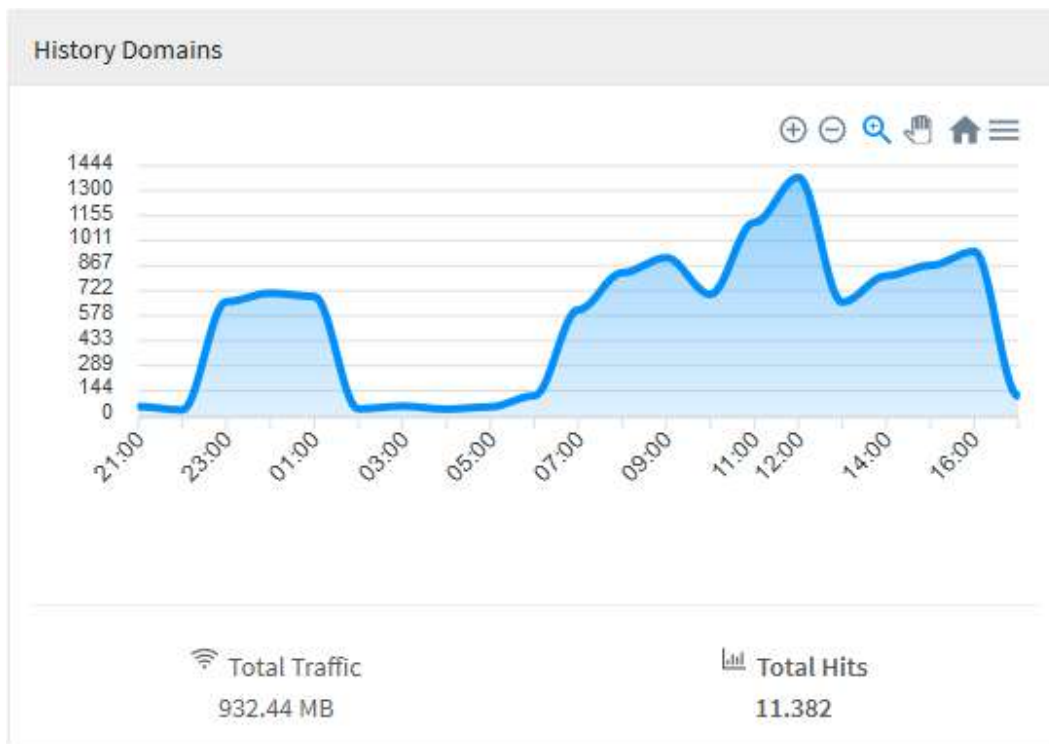
Em "History Domains", temos um gráfico que exibe informações especificamente relacionadas ao acesso de domínios, sua função é demonstrar quando algum domínio foi acessado. Nessa área temos "Total Traffic" onde é exibido o total de tráfego em Gigabytes por dia e "Total Hits" que demonstra o total de acessos para cada um dos dias pesquisados.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta [página](#).



Web Filter - History Domains - Total Traffic

Ao clicar em cada uma dessas legendas, o gráfico será automaticamente modificado para ilustrar as informações relevantes, conforme demonstrado abaixo:



Web Filter - History Domains - Total Hits

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:

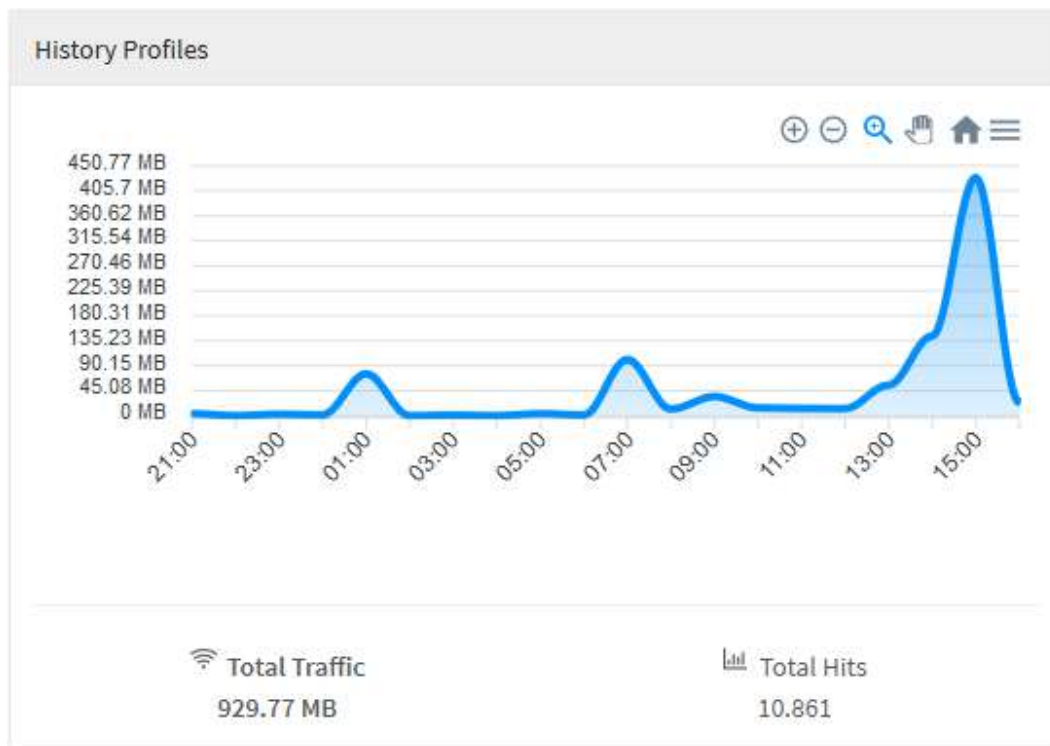


Web Filter - History Domains - Resumo do Período

Web Filter - History Profiles - Total Traffic e Total Hits

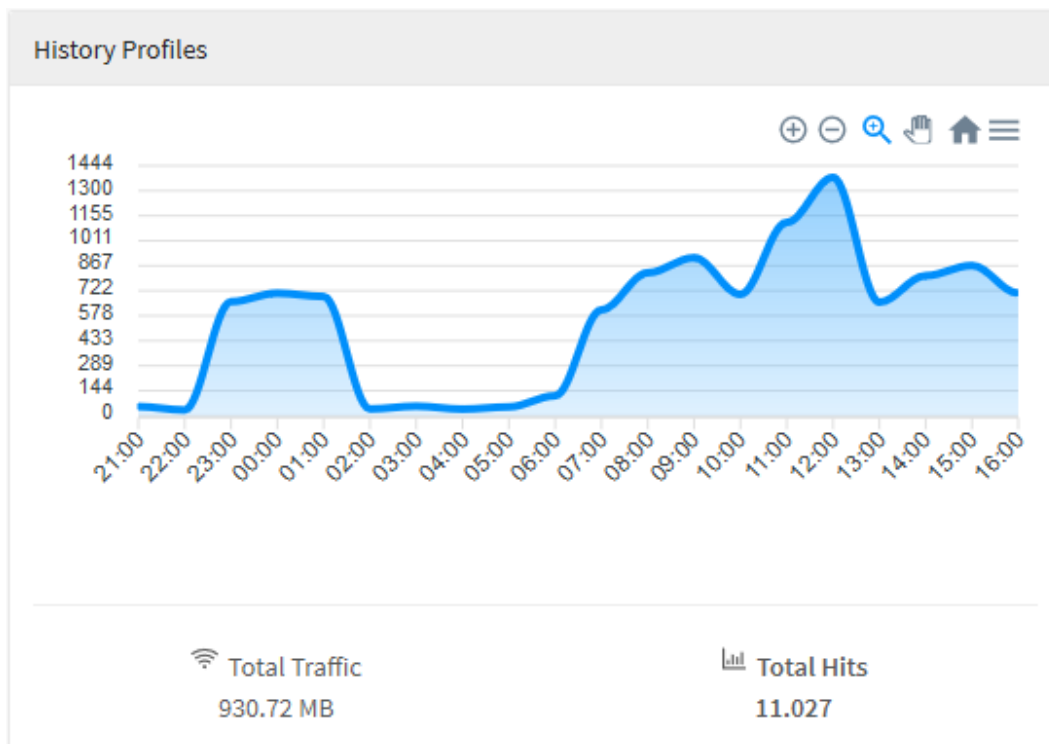
Em "History Profiles", temos um gráfico que exibe informações especificamente relacionadas aos [profiles](#) da rede, sua função é demonstrar quando algum profile foi utilizado em um acesso. Nessa área temos "Total Traffic" onde é exibido o total de tráfego de rede em *Gigabytes* por dia e "Total Hits" que demonstra o total de acessos para cada um dos dias pesquisados.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta [página](#).



Web Filter – History Profiles – Total Traffic

Ao clicar em cada uma dessas legendas, o gráfico será automaticamente modificado para ilustrar as informações relevantes, conforme demonstrado abaixo:



Web Filter – History Profiles – Total Hits

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:



Web Filter – History Profiles – Resumo do Período

Web Filter - Top Categories

Na lista “*Top Categories*”, temos uma listagem dos nomes das dez categorias classificadas por ordem de maior quantia de acessos e seu respectivo uso em *Gigabytes*. Por fim, ao clicar em um desses usuários ou *IPs*, você será redirecionado para [*Events](#) usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito da categoria selecionada.

Para mais informações a respeito da barra de busca presente no topo deste gráfico cheque esta [página](#).

Top Categories			
#	Name	Hits	Traffic
1	Information Technology	3.089	217.74 MB
2	Proxy Avoidance	11	49.65 MB
3	Government	1.162	6.91 MB
4	Travel	24	6.59 MB
5	Restaurants and Dining	101	2.17 MB
6	Search Engines and Portals	443	529.06 KB
7	Web Hosting	51	350.16 KB
8	Freeware and Software Download	83	210.24 KB
9	Computer Security	25	114.67 KB
10	Internet Communication	3	74.58 KB

Web Filter – Top Categories

Web Filter - Top Content Type

Na lista “*Top Content Type*”, temos uma listagem dos nomes dos dez tipos de conteúdo mais acessados classificados por ordem de maior quantia de acessos e seu respectivo uso em *Gigabytes*. Por fim, ao clicar em um desses usuários ou *IPs*, você será redirecionado para [*Events](#) usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito desses tipos de conteúdo.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta [página](#).

Top Content Type			
#	Name	Hits	Traffic
1	application/vnd.ms-cab-compressed	823	109.73 MB
2	application/octet-stream	391	106.39 MB
3	audio/mpeg	4	49.63 MB
4	image/png	1.658	27.34 MB
5	image/jpeg	140	4.42 MB
6	text/css	732	3.52 MB
7	application/json	822	1.96 MB
8	text/xml	451	1.87 MB
9	text/javascript	337	1.53 MB
10	text/html	246	1.34 MB

Top Content Type

Web Filter - Top Domains

Na lista “*Top Domains*”, temos uma listagem dos nomes dos dez domínios classificadas por ordem de maior quantia de acessos e seu respectivo tráfego em *Megabytes*. Por fim, ao clicar em um desses endereços, você será redirecionado para [*Events](#) usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito do domínio selecionado.

Para mais informações a respeito da barra de busca presente no topo deste gráfico cheque esta [página](#).

Top Domains			
#	Name	Hits	Traffic
1	http://au.download.windowsupdate.com	755	195.12 MB
2	http://e-cdn-proxy-e.deezer.com	8	87.59 MB
3	http://e-cdn-proxy-8.deezer.com	6	74.95 MB
4	http://e-cdn-proxy-9.deezer.com	9	73.39 MB
5	http://e-cdn-proxy-1.deezer.com	5	59.74 MB
6	http://e-cdn-proxy-7.deezer.com	5	46.12 MB
7	http://e-cdn-proxy-3.deezer.com	4	41.29 MB
8	http://e-cdn-proxy-a.deezer.com	4	41.05 MB
9	http://rss.utech.com.br	2.742	38.83 MB
10	http://e-cdn-proxy-f.deezer.com	3	33.24 MB

Web Filter – Top Domains

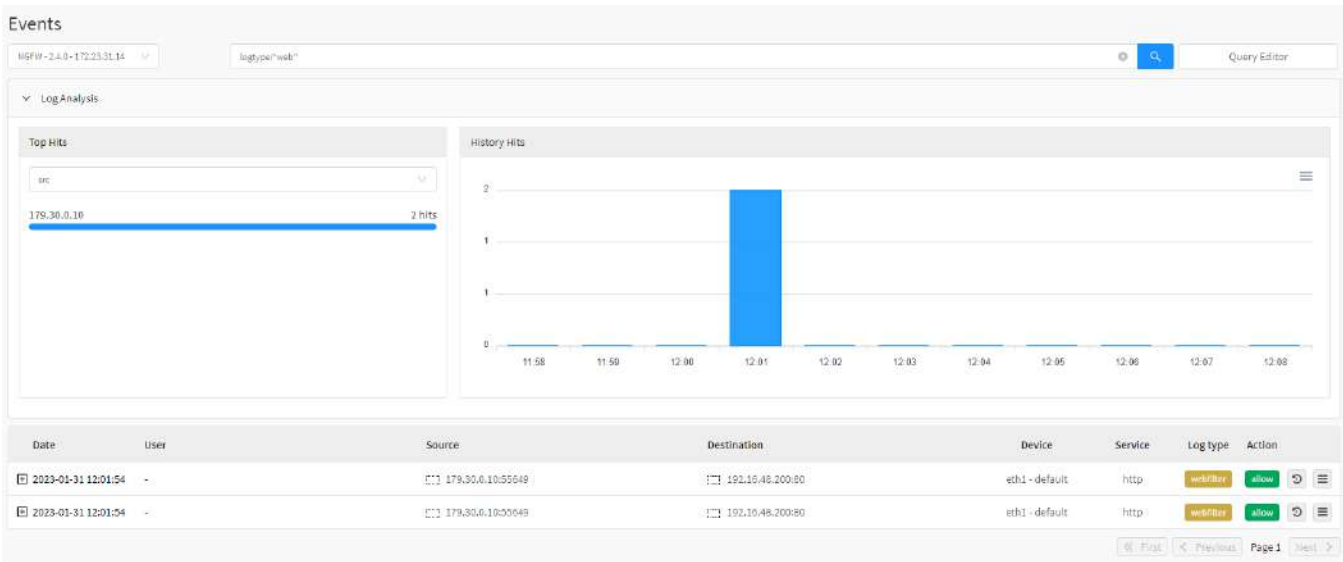
Web Filter - Top Domains by Time

Na lista “Top Domains by Time”, temos uma listagem dos dez domínios mais acessados classificados por ordem de maior tempo de navegação.

Top Domains by time		
#	Domain	Time
1	https://edge.microsoft.com	58s
2	https://umwatson.events.data.microsoft.com	36s
3	https://www.bing.com	18s
4	http://ctldl.windowsupdate.com	14s
5	http://x1.c.lencr.org	10s
6	https://login.live.com	8s
7	https://slscr.update.microsoft.com	8s
8	https://msedge.api.cdp.microsoft.com	6s
9	https://config.edge.skype.com	5s
10	https://update.googleapis.com	4s

Top Domains by Time

Por fim, ao clicar em um desses domínios ou IPs, você será redirecionado para [Events](#) usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito desses tipos de conteúdo.



Events - Sessions

Clicando em [ ou ] é possível verificar informações mais detalhadas nesse filtro. Procure a informação de “surfing time” para verificar o tempo de navegação.

Information					
① date ⊖ 2023-01-31 12:01:54	① client_mac ⊖ 00:0c:29:29:ba:cd	① proto ⊖ tcp	① host ⊖ utmviola23-14	① web_url ⊖ http://ctldl.windowsupdate.com/msdown load/update/v3/static/trustedr/en/pinrule sstl.cab?3d9830fd6545fd8...	① web_site ⊖ http://ctldl.windowsupdate.com/msdown load/update/v3/static/trustedr/en
① logtype ⊖ web	① dst ⊖ 192.16.48.200	① service ⊖ http	① client_ip ⊖ 179.30.0.10	① web_referrer ⊖ -	
① sessid ⊖ 1A0ADF6C286FE0AB30A2683E7B639F38	① dport ⊖ 80	① devout ⊖ default	① web_method ⊖ GET	① web_agent ⊖ Microsoft-CryptoAPI/10.0	
① src ⊖ 179.30.0.10	① devin ⊖ eth1	① rule_action ⊖ allow	① web_profile ⊖ Ética de Segurança	① bytes ⊖ 0	
① sport ⊖ 55649	① zonein ⊖ LAN	① web_mime ⊖ application/octet-stream	① surfing_time ⊖ 1	① web_protocol ⊖ HTTP	



Events - Sessions - [] Information

Event View ✕

▼ "Event Information" : {

```

"date" : "2023-01-31T12:01:54"
"logtype" : "web"
"sessid" : "1A0ADF6C286FE0AB30A2683E7B639F38"
"src" : "179.30.0.10"
"sport" : "55649"
"client_mac" : "00:0c:29:29:ba:cd"
"dst" : "192.16.48.200"
"dport" : "80"
"devin" : "eth1"
"zonein" : "LAN"
"proto" : "tcp"
"service" : "http"
"devout" : "default"
"rule_action" : "allow"
"web_mime" : "application/octet-stream"
"host" : "utmviola23-14"

"client_ip" : "179.30.0.10"
"web_category" : "Search Engines and Portals"
"web_method" : "GET"
"web_profile" : "Ética de Segurança"
"surfing_time" : 1
"web_url" :
"http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?3d9830fd6545fd8"
"web_referrer" : "-"
"web_agent" : "Microsoft-CryptoAPI/10.0"
"bytes" : "0"
"web_protocol" : "HTTP"
"web_site" : "http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en"
}

```

Cancel



Events - Sessions - [] Event View

Web Filter - Top Profiles

Na lista “*Top Profiles*”, temos uma listagem dos dez [profiles](#) mais utilizados classificados por ordem de maior quantia de acessos e seu respectivo uso em *Gigabytes*. Por fim, ao clicar em um desses perfis, você será redirecionado para [*Events](#) usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito do perfil selecionado.

Para mais informações a respeito da barra de busca presente no topo deste gráfico cheque esta [página](#).

Top Profiles			
#	Name	Hits	Traffic
1	Content Filtering (Wifi)	7.894	688.31 MB
2	ByPass SSL (Wifi)	2.590	241.46 MB
3	Block - filestreamingservice	377	0 Bytes

Web Filter – Top Profiles

Web Filter - Top Users

Assim como as outras listas "Top Users", em *Web Filter* temos uma listagem de dez usuários classificados por ordem de maior quantia de acessos e seu respectivo uso em *Gigabytes*. Por fim, ao clicar em um desses usuários ou *IPs*, você será redirecionado para [Events](#) usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito do usuário selecionado.

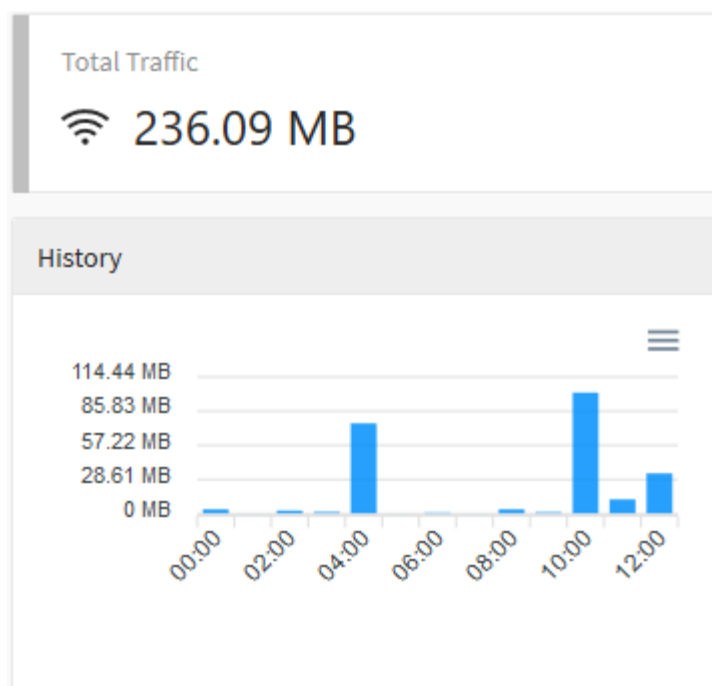
Para mais informações a respeito da barra de busca presente no topo deste gráfico cheque esta [página](#).

Top Users			
#	Name	Hits	Traffic
1	172.32.250.40	762	131.6 MB
2	172.32.250.99	285	98.94 MB
3	doliveira@blockbit.com	1.696	21.28 MB
4	pisantos@blockbit.com	243	20.21 MB
5	172.32.250.46	405	18.68 MB
6	172.32.250.5	553	7.5 MB
7	172.32.250.49	1.461	7.26 MB
8	dsousa@blockbit.com	310	5.43 MB
9	172.32.250.53	67	4.83 MB
10	172.32.250.47	181	4.66 MB

Web Filter – Top Users

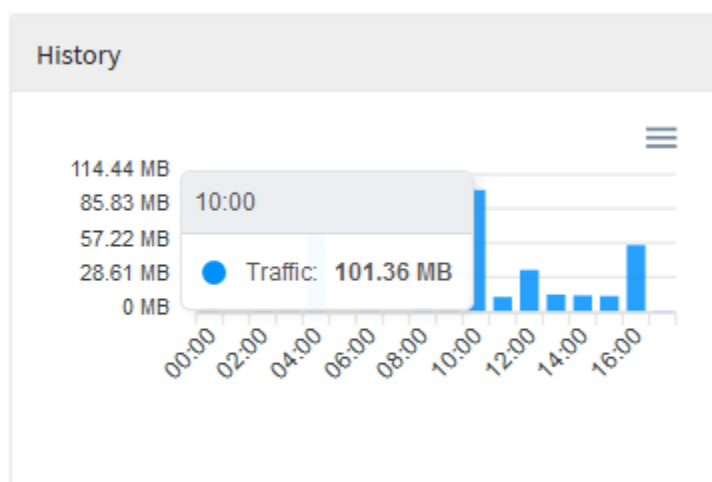
Web Filter - Total Traffic e History

O painel “*Total Traffic*” demonstra o valor total de tráfego em Megabytes. Logo abaixo, é exibido o histórico em um gráfico de barras demonstrando a quantia de *Megabytes* trafegados por dia.



Web Filter – Total Traffic

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:

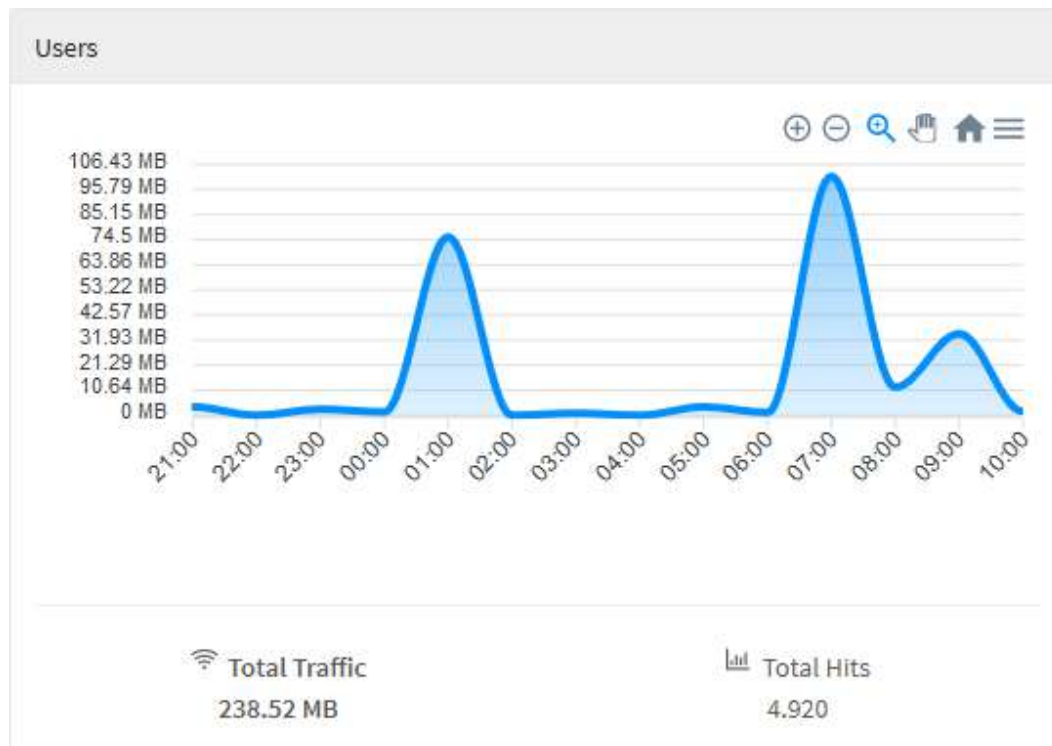


Web Filter – Total Traffic - Resumo do período

Web Filter - Users - Total Traffic e Total Hits

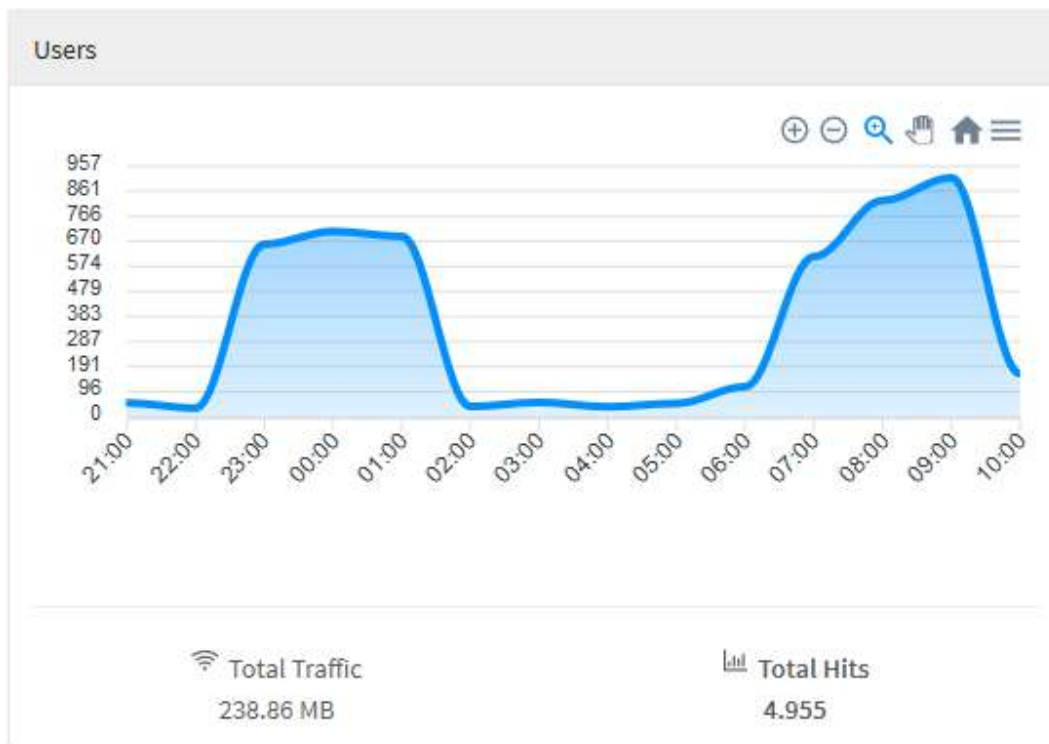
Logo abaixo dos painéis anteriormente descritos, no lado esquerdo da tela temos o gráfico disposto em "Users", que exibe informações especificamente relacionadas ao consumo de rede por parte dos usuários: Nele temos "Total Traffic" onde é exibido o total de tráfego de rede em *Megabytes* por dia e "Total Hits" que demonstra o total de acessos para cada um dos dias pesquisados.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta [página](#).



Web Filter – Users – Total Traffic

Ao clicar em cada uma dessas legendas, o gráfico será automaticamente modificado para ilustrar as informações relevantes, conforme demonstrado abaixo:



Web Filter – Traffic – Total Hits

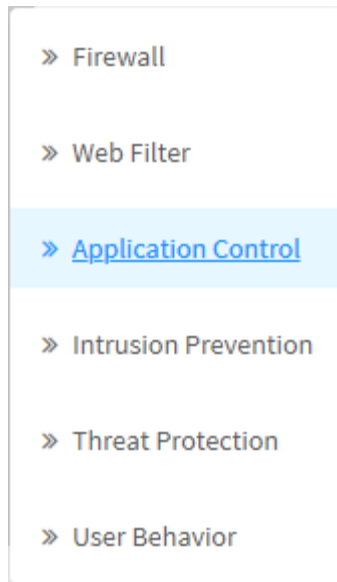
Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:



Web Filter – Users – Total Traffic - Resumo do Período

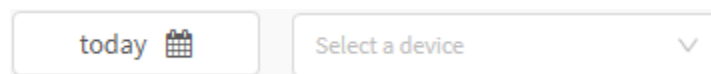
Application Control

Para acessar os relatórios do *Application Control*, clique no ícone “Analyzer” localizado na lateral esquerda, um menu *dropdown* será exibido, selecione a opção “*Application Control*”.



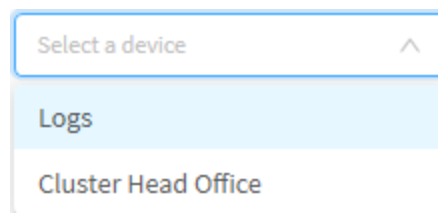
Application Control

Para gerar um relatório, localize a caixa de seleção que está posicionada no topo direito da tela, conforme ilustrado a seguir:



Caixa de Seleção

Nesta caixa de seleção estarão listadas todos os *devices* (ou grupos de *devices*) previamente cadastradas no *Device Manager*, para criar um relatório, selecione o *device* desejado.

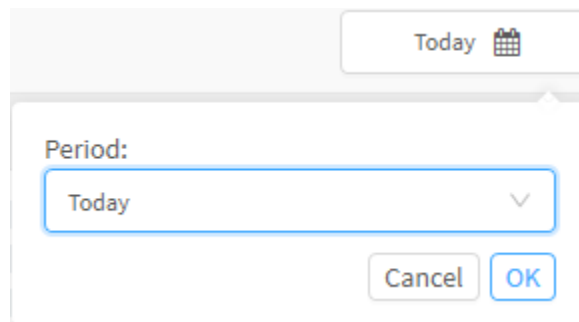


Selecionando *Device*

Logo do lado direito de onde acabamos de selecionar os *devices*, é possível visualizar uma caixa de seleção de datas, o objetivo desta mesma é basicamente permitir uma filtragem de resultados ainda mais precisa, as opções possíveis são:

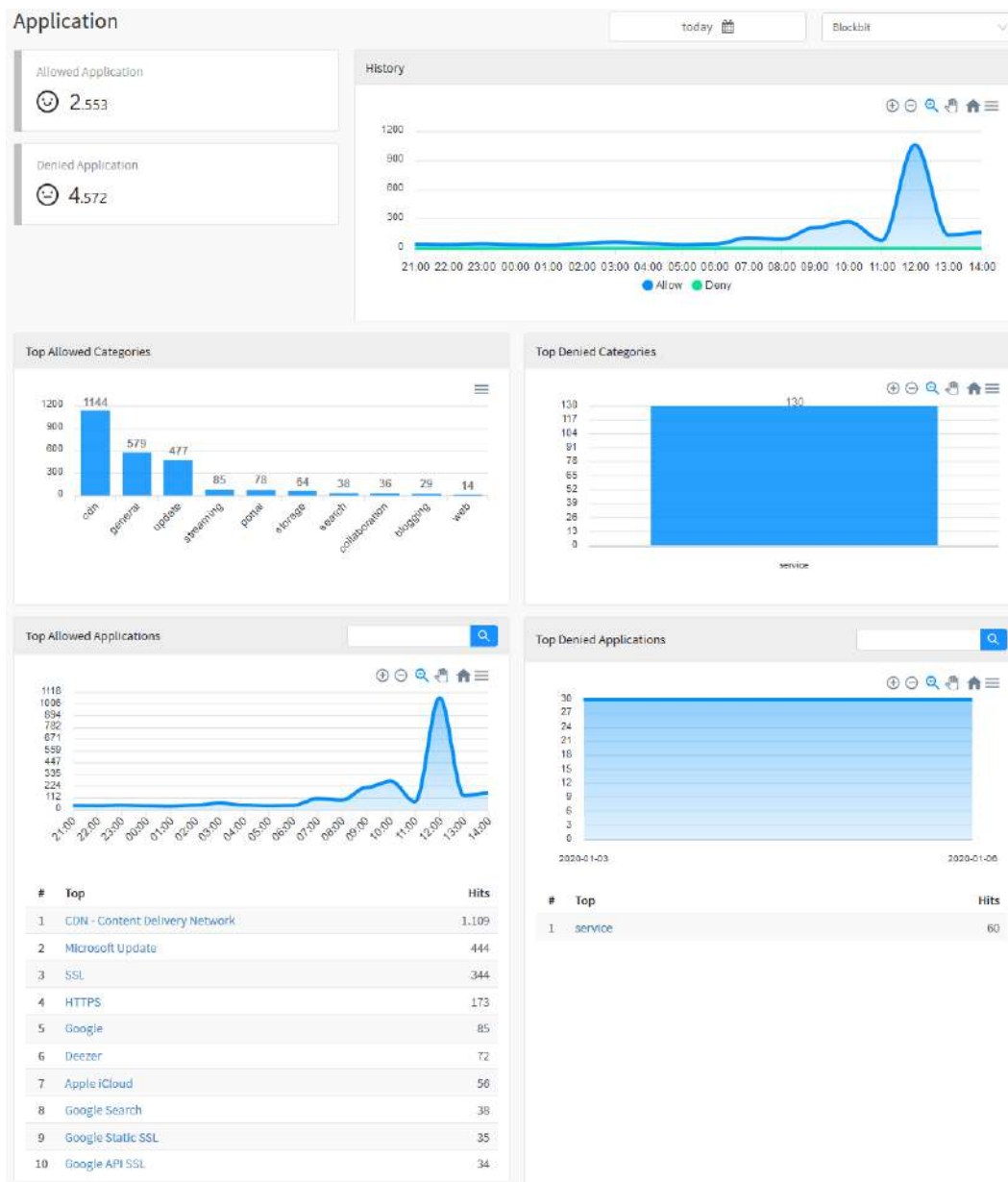
- **By date:** Determina uma data específica;
- **By period:** Exibe resultados de uma data inicial (“*Start date*”) até uma data final (“*End date*”);
- **Today:** Exibe resultados especificamente para a data de hoje;
- **Yesterday:** Exibe resultados especificamente para ontem;
- **Last 7 days:** Filtra especificamente os resultados dos últimos 7 dias;
- **Last 30 days:** Filtra especificamente os resultados dos últimos 30 dias;
- **This month:** Exibe os resultados deste mês;

- **Last month:** Exibe os resultados do último mês.



Seleção de Data

Selecione a data desejada e clique em **Ok** [];



A maioria dos gráficos desta aba possui um menu de navegação e uma barra de busca.

O menu de navegação possui os seguintes botões:

- : Serve para dar um zoom;
- : Tem como função remover o zoom;
- : Serve para fazer um zoom de seleção;
- : Serve para mover o gráfico;
- : Reseta o gráfico para a posição inicial;
- : Permitir baixar este diagrama no formato *svg*, *png* ou *csv*.

A barra de busca permite pesquisar um item específico e modificar os diagramas de acordo com os resultados da pesquisa.

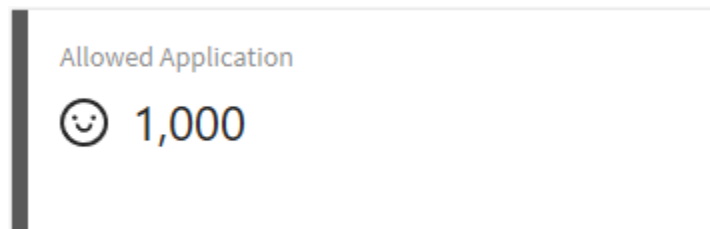
Para efetuar uma pesquisa, digite um termo na barra de busca e clique no **botão de busca**

A seguir, analisaremos em detalhes os componentes de “Application Control”:

- [Allowed Application](#);
- [Denied Application](#);
- [History](#);
- [Top Allowed Categories](#);
- [Top Denied Categories](#);
- [Top Allowed Applications](#);
- [Top Denied Applications](#).

Application Control - Allowed Application

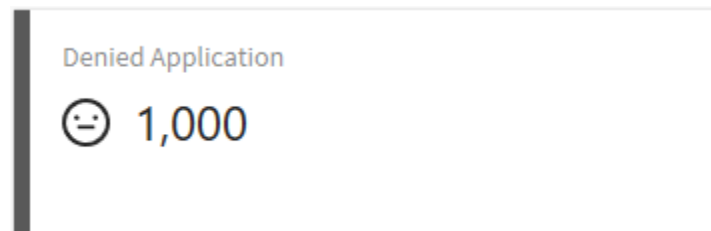
Em "Allowed Application" é exibido um total de aplicações que tiveram seu acesso autorizado.



Application Control – Allowed Application

Application Control - Denied Application

Já em "Application Denied", mostra-se uma somatória das aplicações que tiveram seu acesso negado.

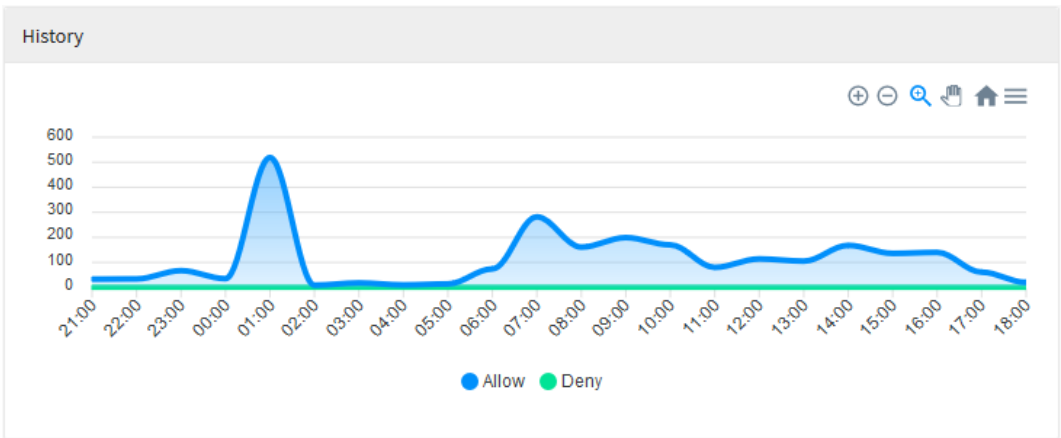


Application Control – Denied Application

Application Control - History

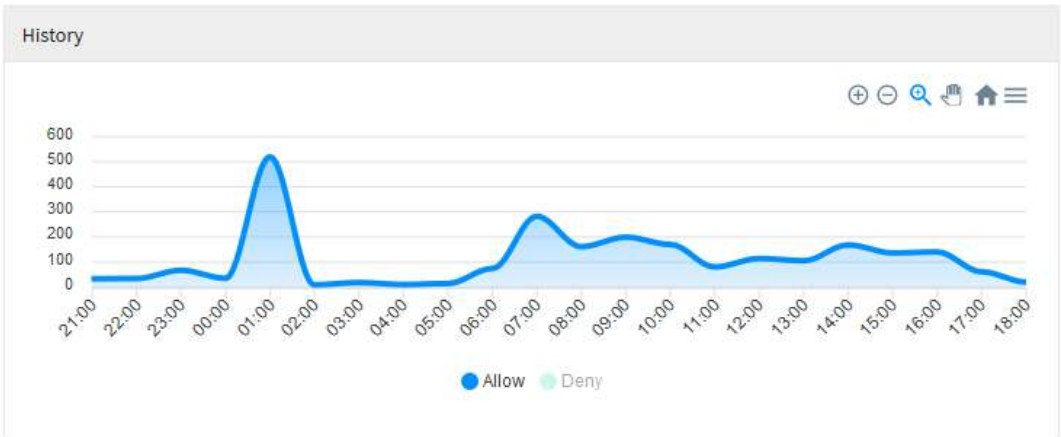
Ao lado direito é possível visualizar o gráfico "History" que exibe um histórico de todas as aplicações que tiveram seu acesso permitido e negado, tendo como referências para seus eixos a quantia de acessos em relação com as datas previamente pesquisadas. Os itens da legenda são interativos sendo possível alterar a exibição do gráfico através deles, de modo a fazer o gráfico exibir os aplicativos que foram permitidos e os que foram negados por data. Neste diagrama temos "Allow" onde são exibidas as aplicações permitidas e "Deny" demonstrando todas as aplicações negadas para cada um dos dias pesquisados.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta [página](#).



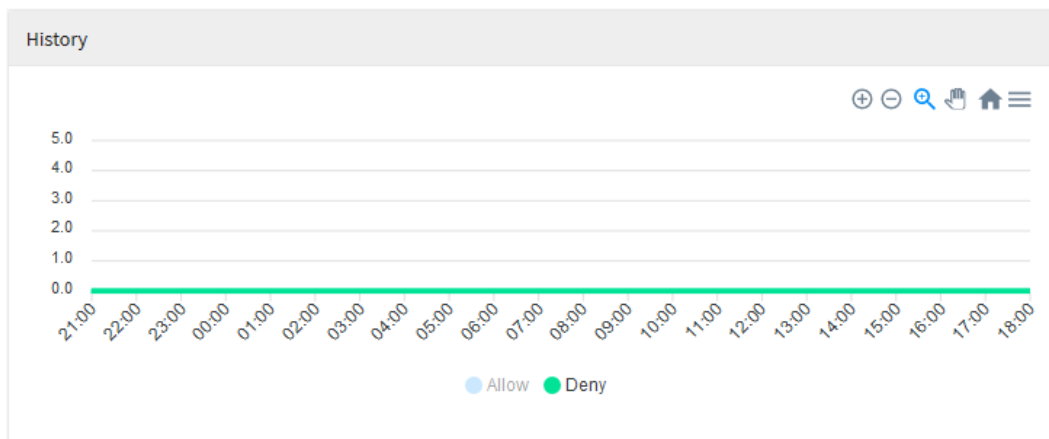
Application Control – History

É possível selecionar "Allow" , para modificar o gráfico e ilustrar as informações relevantes, conforme demonstrado abaixo:



Application Control – History - Allow

Também é possível clicar na legenda "Deny", para modificar o gráfico, conforme demonstrado abaixo:



Application Control – History - Deny

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:

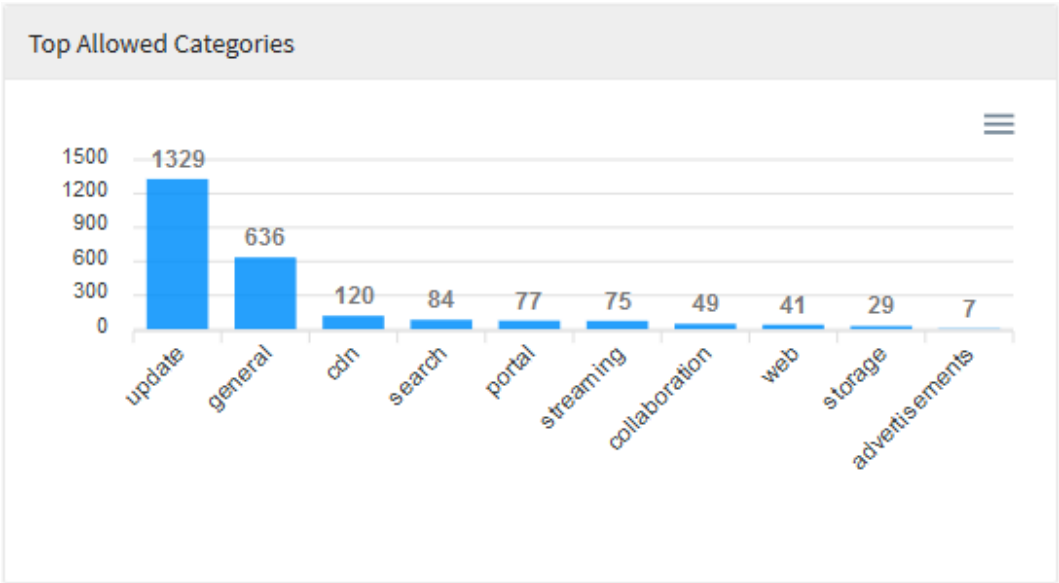


Application Control – History - Resumo do Período

Application Control - Top Allowed Categories

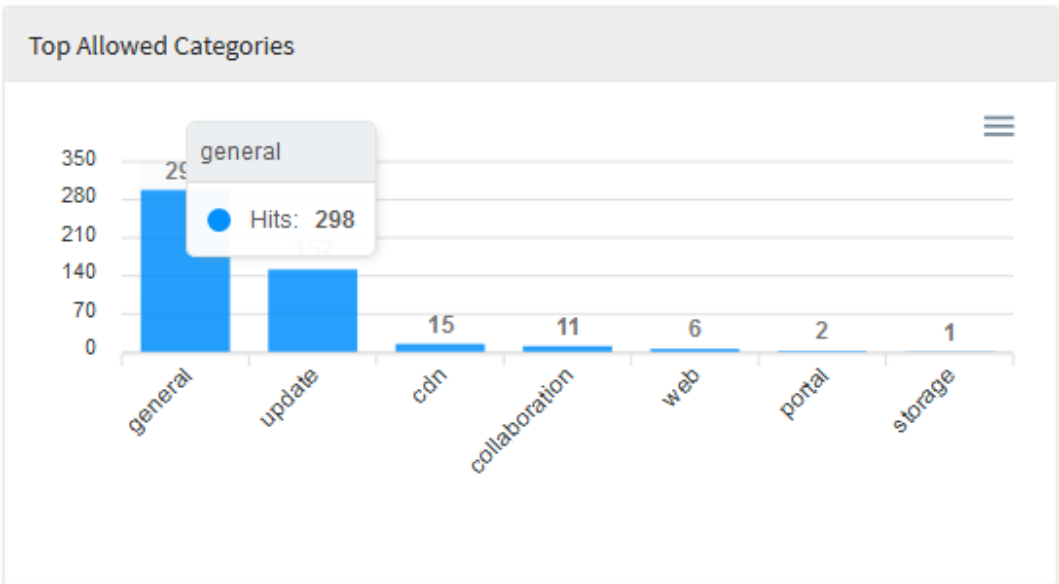
No diagrama “Top Allowed Categories” temos uma representação visual das 10 categorias permitidas mais aplicadas nos acessos dos usuários, essa sessão serve para, representar de forma pragmática, a quantidade de páginas acessadas que se aplicam a cada uma dessas categorizações.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta [página](#).



Application Control – Top Allowed Categories

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:

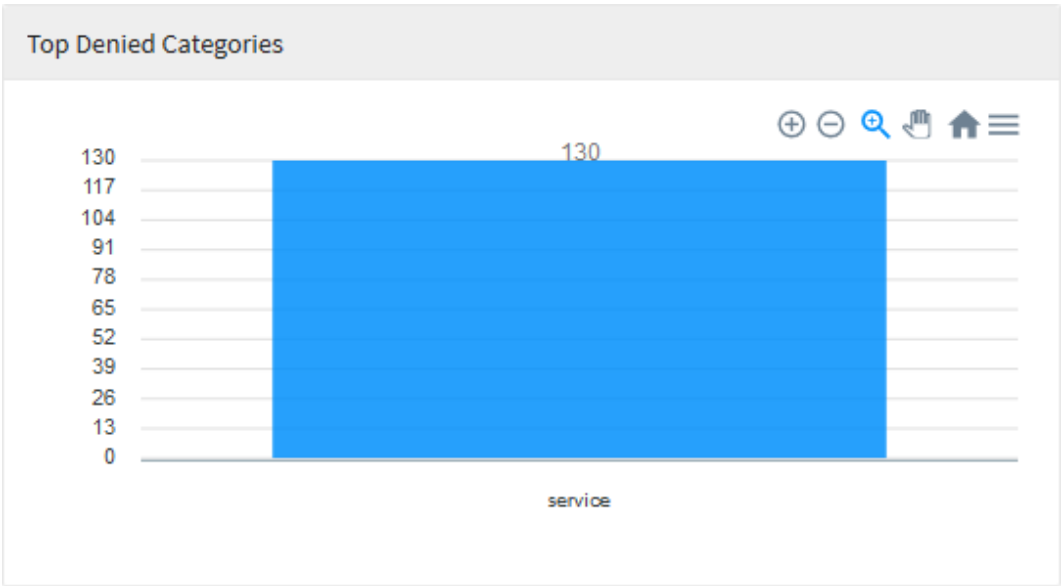


Application Control – Top Allowed Categories - Resumo do Período

Application Control - Top Denied Categories

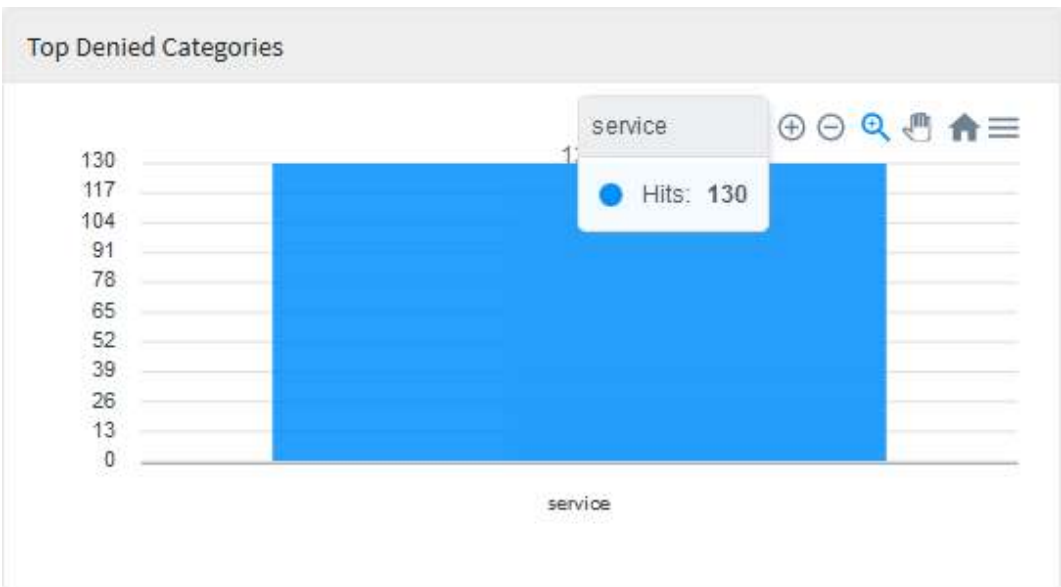
No diagrama “Top Denied Categories” temos uma representação visual das 10 categorias recusadas mais utilizadas nos acessos dos usuários, essa sessão serve para, representar de forma pragmática, a quantidade de páginas acessadas que caíram em cada uma dessas categorias de recusa.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta [página](#).



Application Control – Top Denied Categories

Ao passar o mouse por cima do gráfico, um resumo da quantia de categorias é exibido, conforme demonstrado na imagem abaixo:



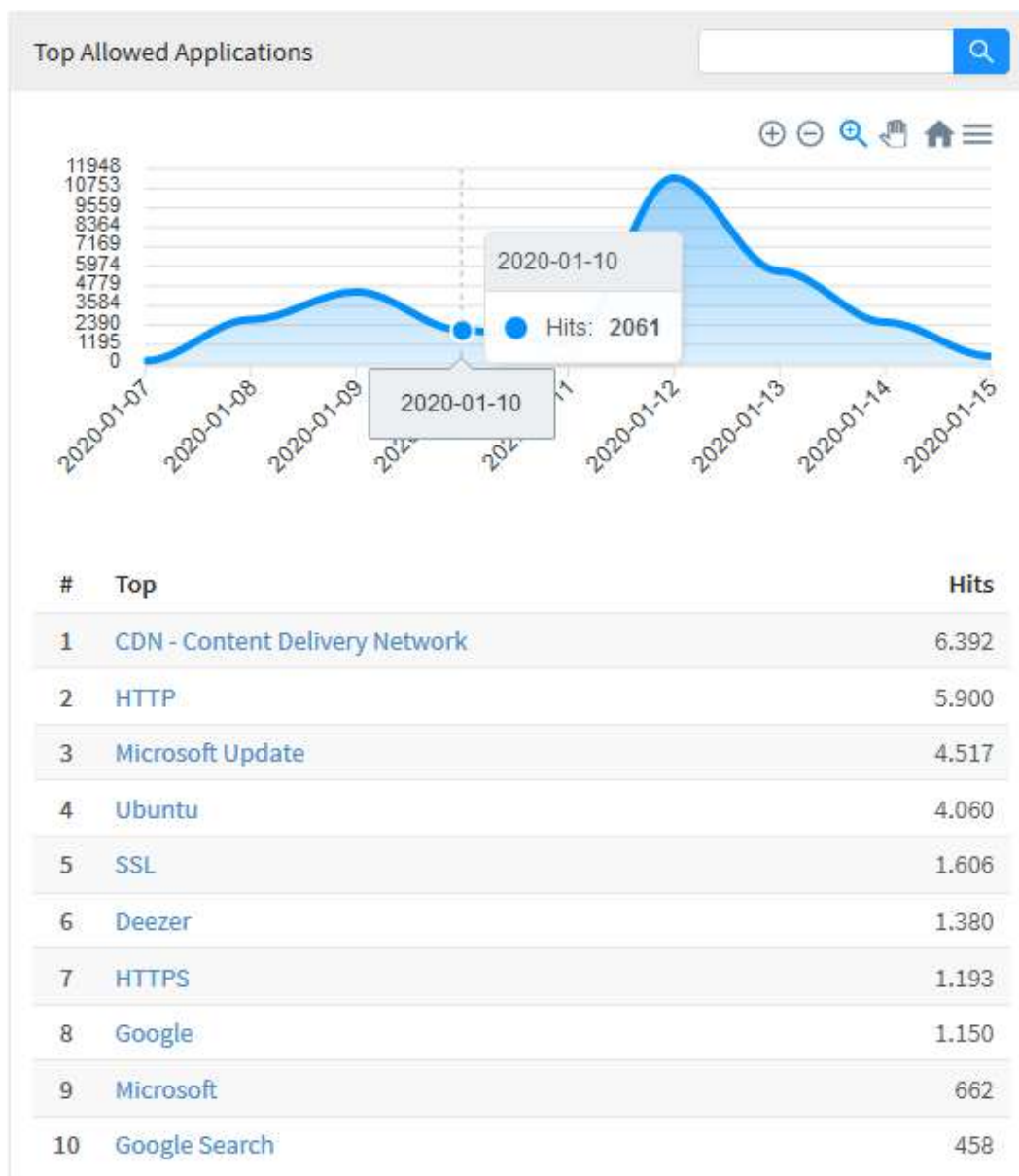
Application Control – Top Denied Categories – Quantia de categorias recusadas

Em “*Top Allowed Applications*” há um gráfico representando as dez aplicações que tiveram seu acesso autorizado em relação ao período de tempo previamente especificado, abaixo desse gráfico, temos uma listagem dos nomes destas dez aplicações classificadas por ordem de maior quantia de acessos e suas respectivas categorias.

Top Allowed Applications

#	Top	Hits
1	CDN - Content Delivery Network	6.392
2	HTTP	5.900
3	Microsoft Update	4.517
4	Ubuntu	4.060
5	SSL	1.606
6	Deezer	1.380
7	HTTPS	1.193
8	Google	1.150
9	Microsoft	662
10	Google Search	458

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:

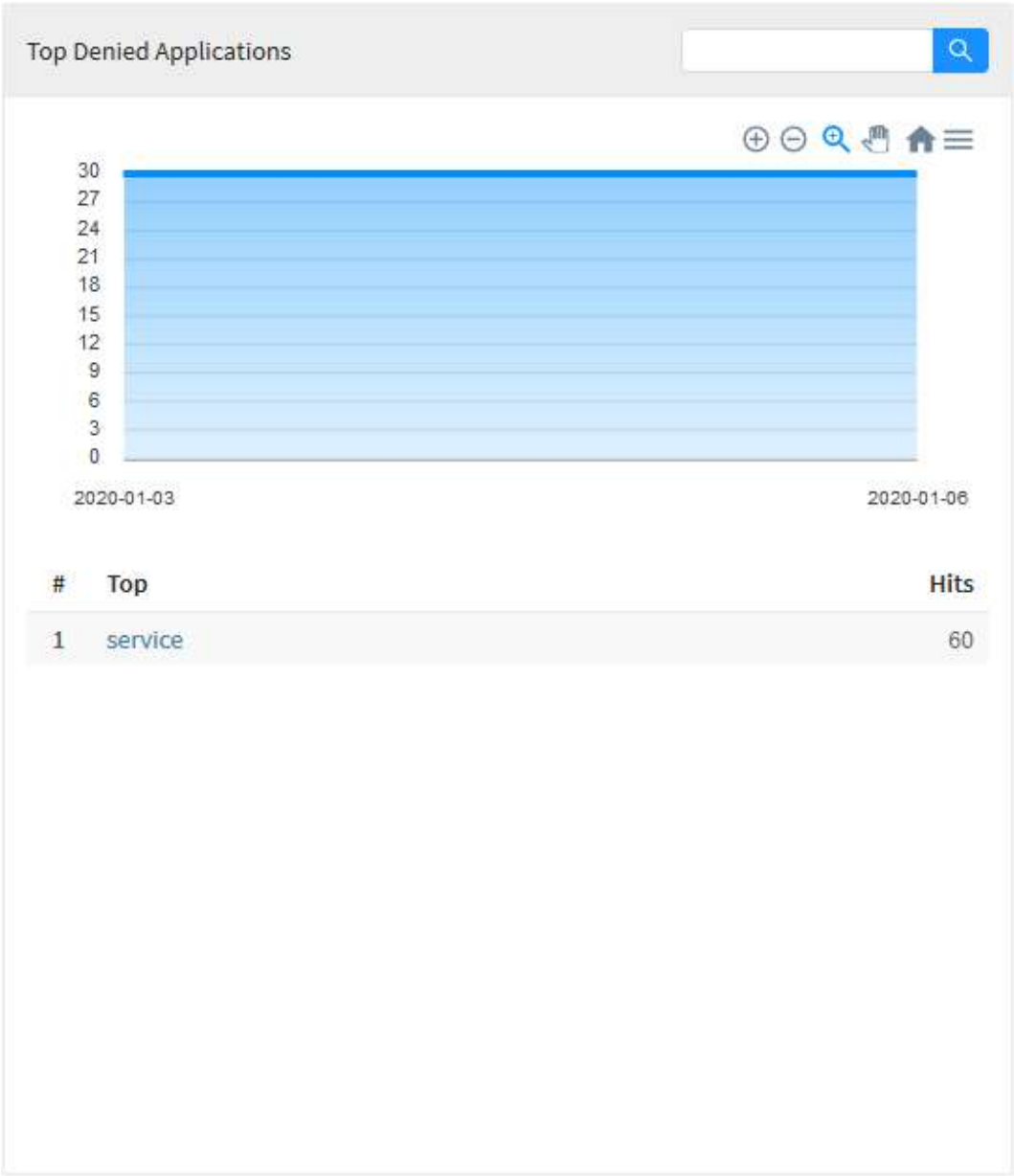


Application Control - Top Allowed Applications - Resumo do Período

Application Control - Top Denied Applications

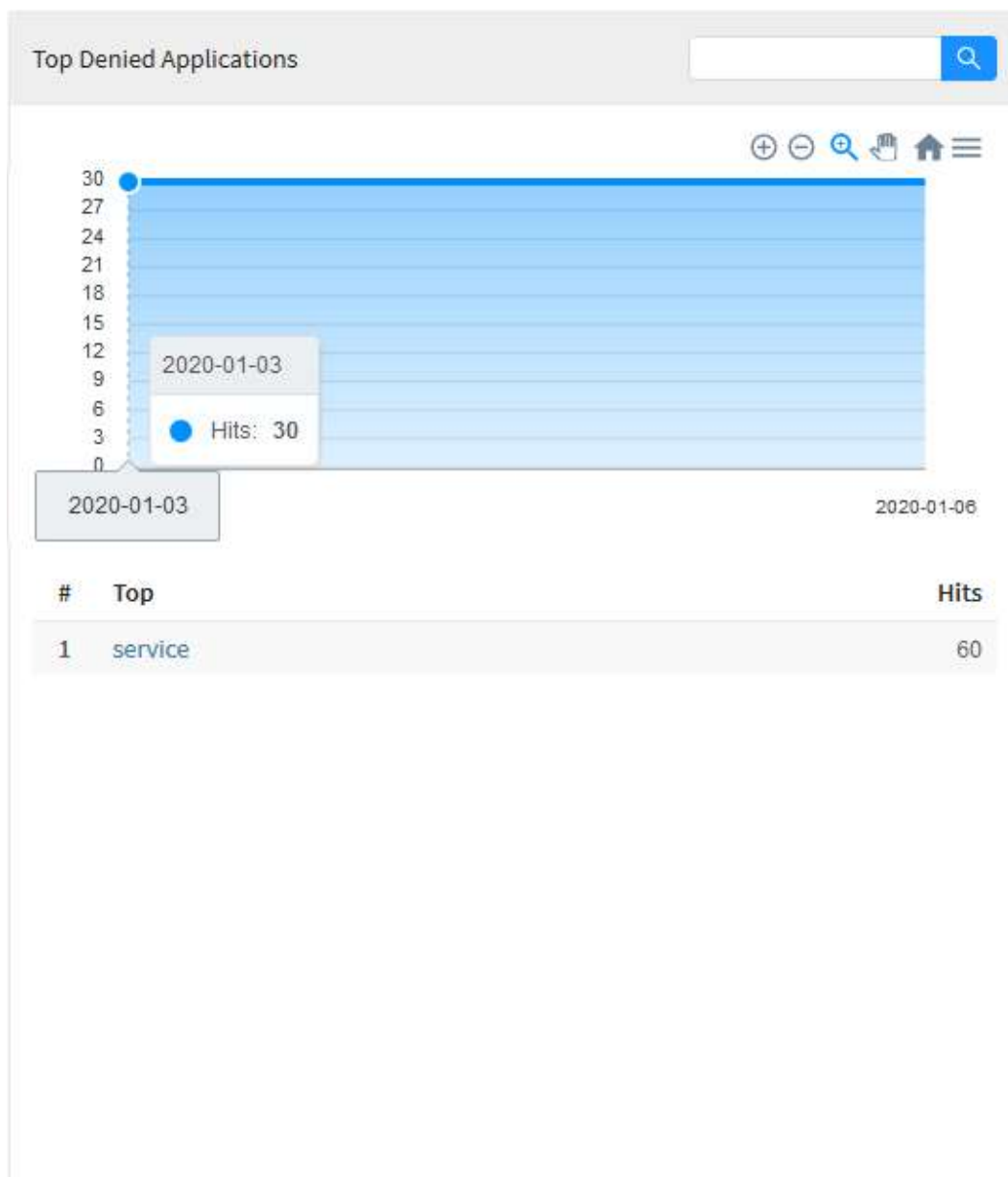
No painel “*Top Denied Applications*” temos o exato oposto da sessão anterior: Um gráfico representando as dez aplicações que tiveram seu acesso negado em relação ao período de tempo previamente especificado, abaixo desse gráfico, temos uma listagem dos nomes destas dez aplicações classificadas por ordem de maior quantia de acessos e suas respectivas categorias.

Para mais informações a respeito do menu de navegação e da barra de busca presente no topo deste gráfico cheque esta [página](#).



Application Control – Top Denied Applications

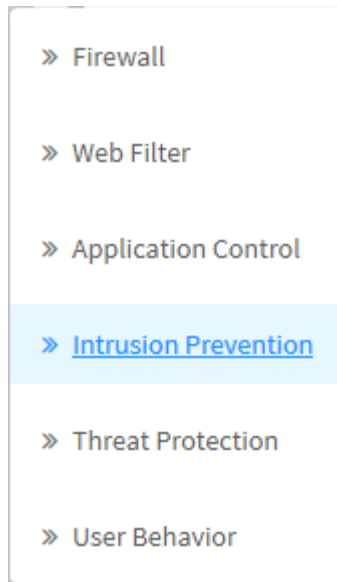
Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:



Application Control – Top Denied Applications - Resumo do período

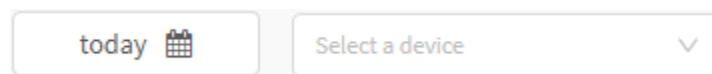
Intrusion Prevention

Para acessar os relatórios de Prevenção de Intrusão, clique no ícone “Analysis” localizado na lateral esquerda, um menu *dropdown* será exibido, selecione a opção “Intrusion Prevention”.



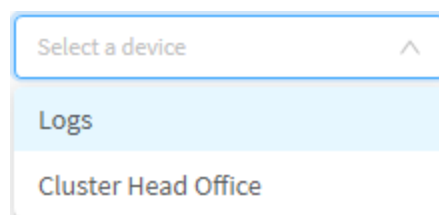
Intrusion Prevention

Para gerar um relatório, localize a caixa de seleção que está posicionada no topo direito da tela, conforme ilustrado a seguir:



Caixa de Seleção

Nesta caixa de seleção estarão listadas todos os *devices* (ou grupos de *devices*) previamente cadastradas no [Device Manager](#), para criar um relatório, selecione o *device* desejado.

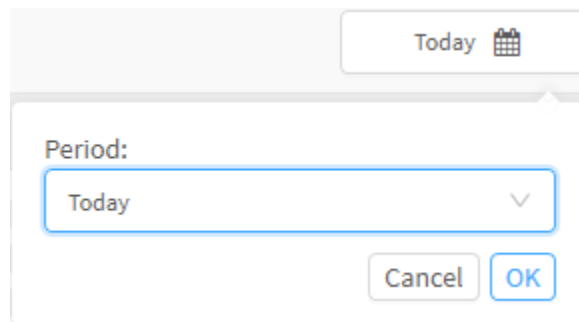


Selecionando Device

Logo do lado direito de onde acabamos de selecionar os *devices*, é possível visualizar uma caixa de seleção de datas, o objetivo desta mesma é basicamente permitir uma filtragem de resultados ainda mais precisa, as opções possíveis são:

- **By date:** Determina uma data específica;
- **By period:** Exibe resultados de uma data inicial (“*Start date*”) até uma data final (“*End date*”);
- **Today:** Exibe resultados especificamente para a data de hoje;
- **Yesterday:** Exibe resultados especificamente para ontem;
- **Last 7 days:** Filtra especificamente os resultados dos últimos 7 dias;
- **Last 30 days:** Filtra especificamente os resultados dos últimos 30 dias;
- **This month:** Exibe os resultados deste mês;

- **Last month:** Exibe os resultados do último mês.



Today 

Period:

Today 

Cancel OK

Seleção de Data

Selecione a data desejada e clique em **Ok** [];

Intrusion Prevention

today

Blockbit

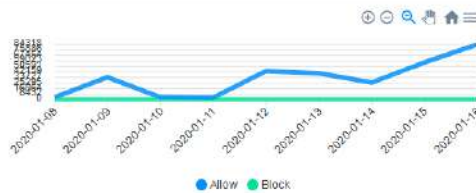
Alerted

✓ 12

Blocked

7,000

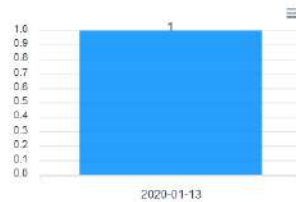
History



Geolocation



Impact - High



#	Threat	Hits
1	SERVER-WEBAPP Checkpoint Firewall-1 HTTP parsing format string vulnerability attempt	1

Impact - Medium



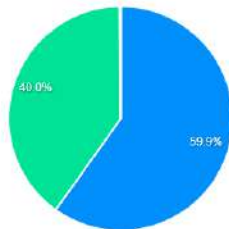
#	Threat	Hits
1	PROTOCOL-ICMP Unusual PING detected	40,993
2	PROTOCOL-DNS SPOOF query response with TTL of 1 min. and no authority	285
3	GPL SNMP request udp	116
4	SERVER-OTHER MRLG fastping echo reply memory corruption attempt	70
5	PROTOCOL-SNMP request udp	65
6	GPL SNMP public access udp	51
7	PROTOCOL-SNMP public access udp	51

Impact - Low



#	Threat	Hits
1	GPL ICMP_INFO Destination Unreachable Port Unreachable	54,896
2	PROTOCOL-ICMP destination unreachable port unreachable packet detected	54,874
3	GPL ICMP_INFO PING	41,115
4	PROTOCOL-ICMP PING	40,964
5	PROTOCOL-ICMP ICMPv6 Echo Request	13,811
6	GPL ICMP_INFO Echo Reply	12,550
7	PROTOCOL-ICMP Echo Reply	12,543

Layer 3 Intrusion Protection



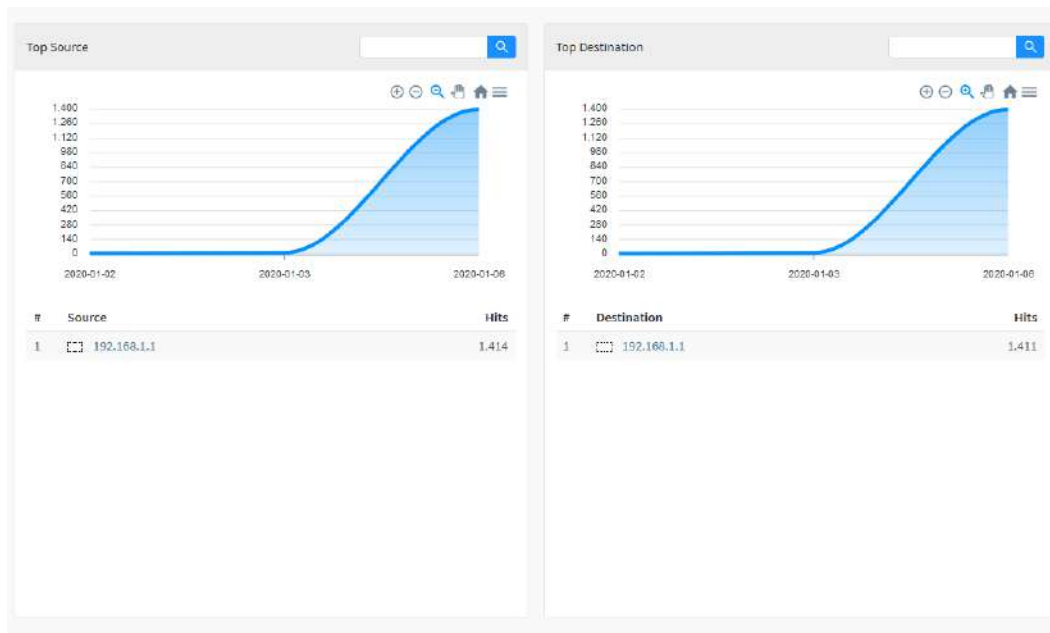
- PROTOCOL-ICMP
- GPL
- PROTOCOL-DNS
- PROTOCOL-SNMP
- SERVER-OTHER
- DNS
- WEB_SERVER
- INDICATOR-COMPROMISE
- SERVER-WEBAPP

#	Malicious IP	Category	Hits
1	172.32.250.20	PROTOCOL-ICMP	59,453
2	172.32.250.20	GPL	57,497
3	172.32.250.24	PROTOCOL-DNS	281
4	172.161.12.129	PROTOCOL-SNMP	116
5	172.32.250.6	SERVER-OTHER	61
6	172.32.250.24	DNS	23
7	192.16.58.8	WEB_SERVER	4
8	8.8.8.8	INDICATOR-COMPROMISE	3
9	34.102.185.99	SERVER-WEBAPP	1

Intrusion Classification



#	Malicious IP	Hits
1	Misc activity	253,481
2	Information Leak	40,993
3	Potentially Bad Traffic	311
4	Attempted Information Leak	310
5	Misc Attack	70
6	Not Suspicious Traffic	24
7	Access to a Potentially Vulnerable Web Application	11
8	Attempted Administrator Privilege Gain	1



Analyzer - Intrusion Prevention

A maioria dos gráficos desta aba possui um menu de navegação e uma barra de busca.

O menu de navegação possui os seguintes botões:

- [+]: Serve para dar um zoom;
- [-]: Tem como função remover o zoom;
- [+]: Serve para fazer um zoom de seleção;
- [🖱️]: Serve para mover o gráfico;
- [🏠]: Reseta o gráfico para a posição inicial;
- [≡]: Permitir baixar este diagrama no formato *svg*, *png* ou *csv*.

A barra de busca permite pesquisar um item específico e modificar os diagramas de acordo com os resultados da pesquisa.

Para efetuar uma pesquisa, digite um termo na barra de busca e clique no **botão de busca** [🔍].

A seguir, analisaremos em detalhes os componentes de "Intrusion Prevention":

- [Alerted, Blocked e Histórico](#);
- [Alerts by Geolocation](#);
- [Impact - High](#);
- [Impact - Medium](#);
- [Impact - Low](#);
- [Layer 3 Intrusion Protection](#);
- [Intrusion Classification](#);
- [Top Source](#);
- [Top Destination](#).

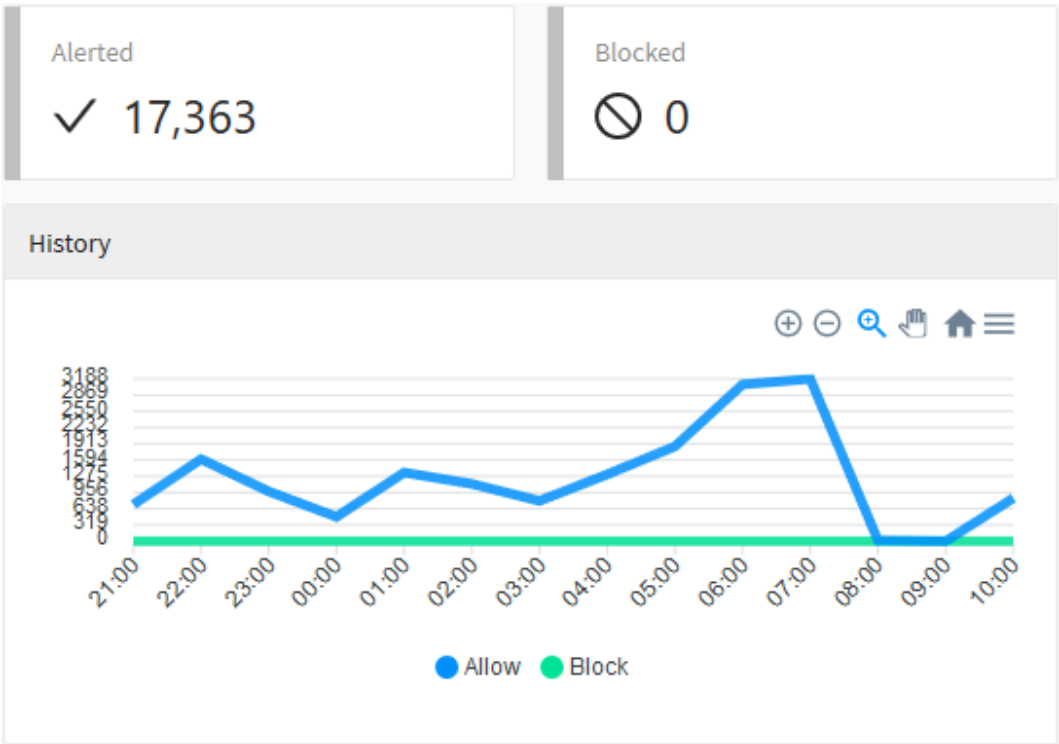
Intrusion Prevention - Alerted, Blocked e Histórico

O painel “Alerted” exibe um total de alertas de intrusão.

Já em “Blocked”, é exibido um número totalizando as tentativas de intrusão bloqueadas.

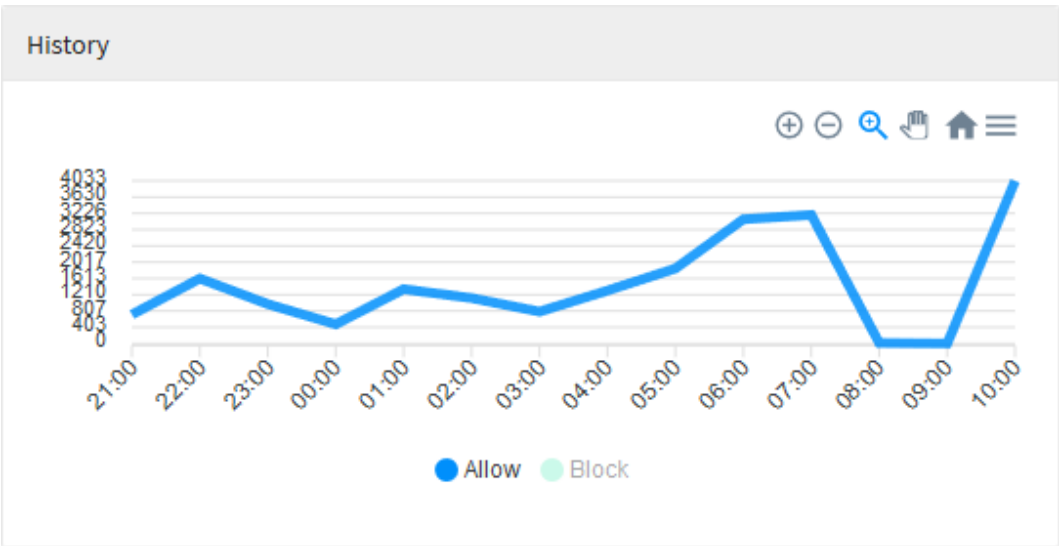
Logo abaixo, é mostrado um resumo dos alertas e bloqueios em um gráfico de linhas exibindo a quantidade de eventos relacionados a intrusão dentro do período de tempo previamente selecionado. Ao selecionar uma das legendas (“Alerted” ou “Blocked”) no topo do gráfico, é possível determinar que apenas uma destas sejam exibidas no gráfico.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta [página](#).



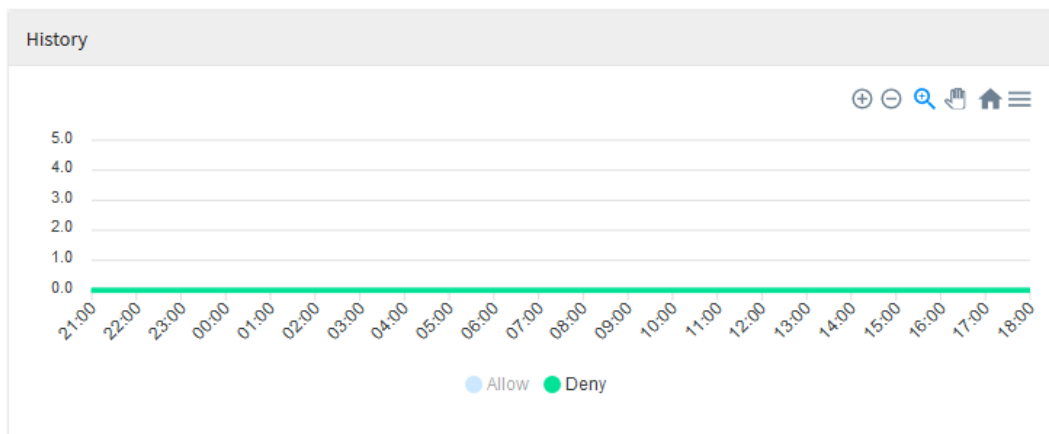
Alerted, Blocked e Histórico

É possível selecionar “Allow”, para modificar o gráfico e ilustrar as informações relevantes, conforme demonstrado abaixo:



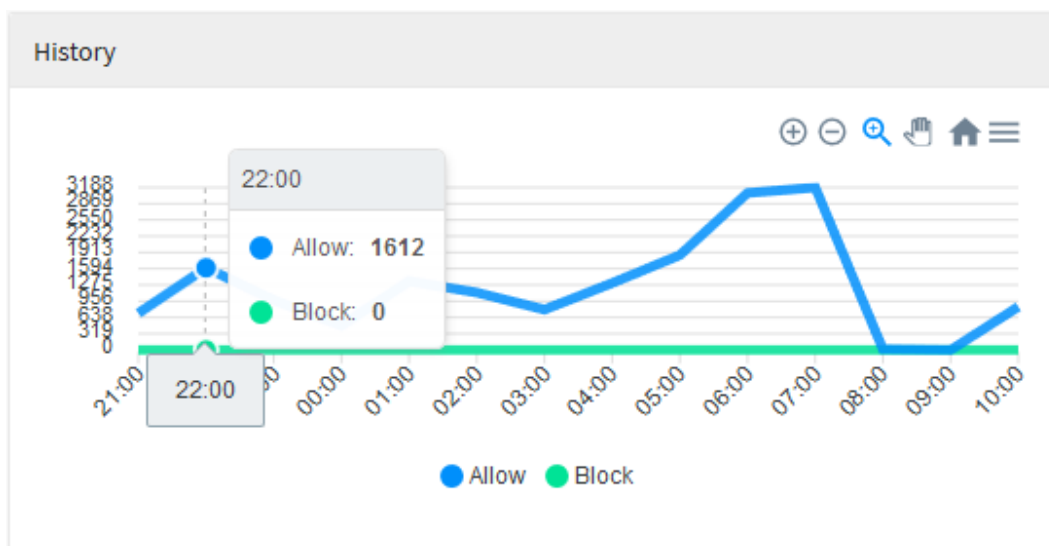
Alerted, Blocked e Histórico - Allow

Também é possível clicar na legenda "Deny", para modificar o gráfico, conforme demonstrado abaixo:



Alerted, Blocked e Histórico - Deny

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:



Alerted, Blocked e Histórico - Resumo do Período

Intrusion Prevention - Alerts by Geolocation

Em "Alerts by Geolocation" é exibida a origem das intrusões por geolocalização, o mapa global demonstra através de uma legenda colorida a quantia de acessos feitos pelos usuários. Ao passar o mouse por cima dos países um número total de alertas é exibido, ao fazer o mesmo com a legenda é possível visualizar uma média, além disso, o país referente a esse valor é destacado no mapa.



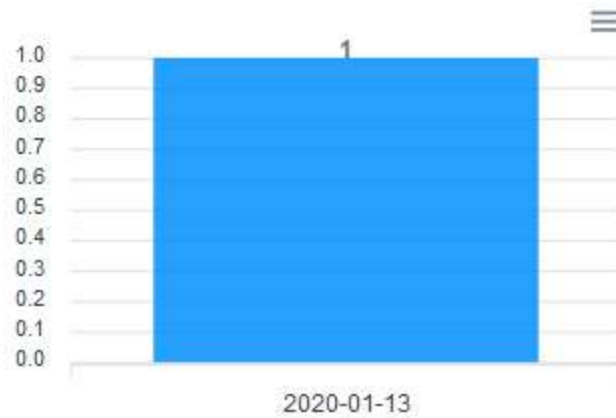
Alerts by Geolocation

Intrusion Prevention - Impact - High

Em "*Impact - High*" temos um gráfico de rosca exibindo a porcentagem de ameaças de intrusão de alto impacto, seguido de um diagrama de colunas exibindo quantas destas mesmas ocorreram dentro do prazo previamente selecionado em comparação com o tráfego de rede do dia. Além disso, uma lista é exibida com as 10 ameaças de alto impacto mais recorrentes, exibindo seu nome e listando-as por quantidade de recorrências.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta [página](#).

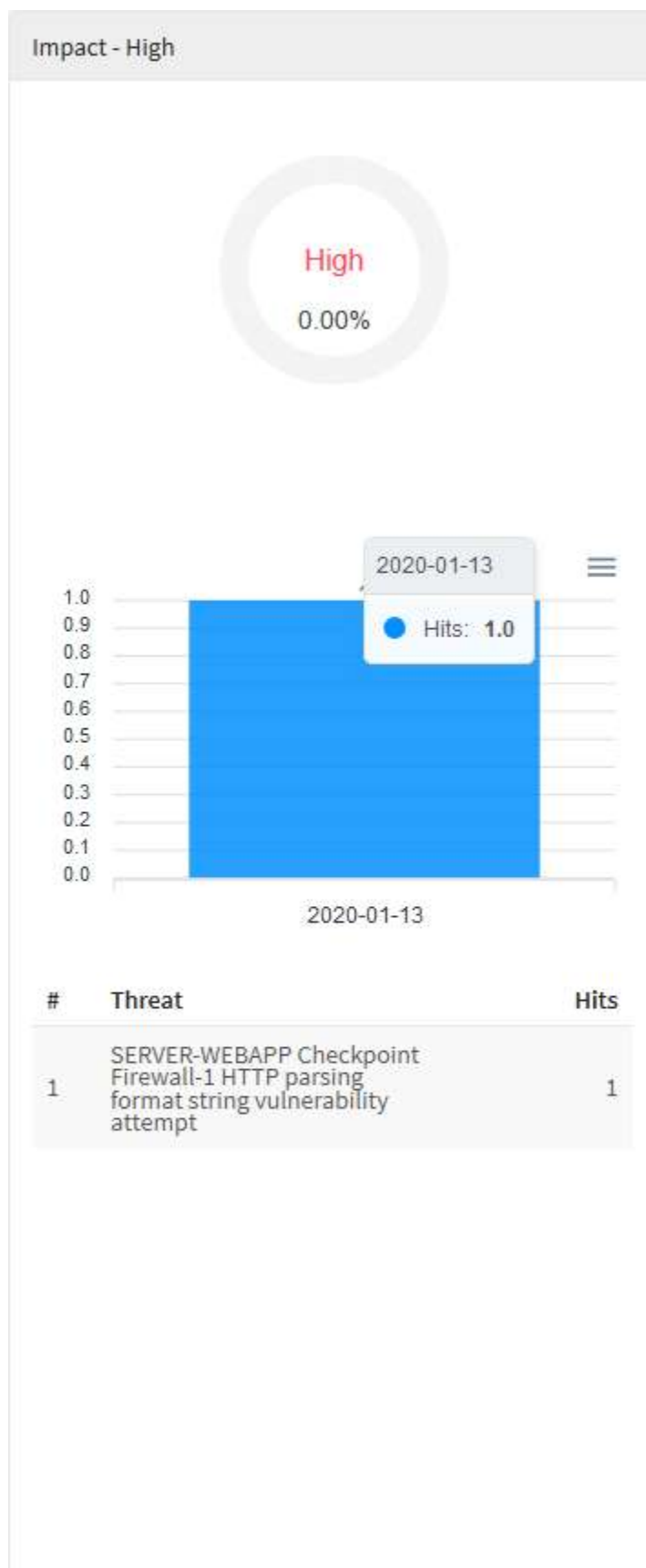
Impact - High



#	Threat	Hits
1	SERVER-WEBAPP Checkpoint Firewall-1 HTTP parsing format string vulnerability attempt	1

Impact - High

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:

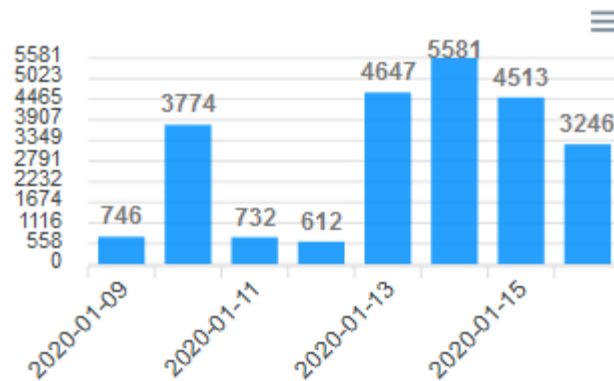
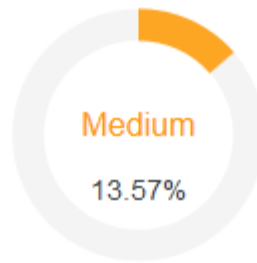


Intrusion Prevention - Impact - Medium

Em "*Impact - Medium*" temos um gráfico de rosca exibindo a porcentagem de ameaças de intrusão de médio impacto, seguido de um diagrama de colunas exibindo quantas destas mesmas ocorreram dentro do prazo previamente selecionado em comparação com o tráfego de rede do dia. Além disso, uma lista é exibida com as 10 ameaças de médio impacto mais recorrentes, exibindo seu nome e listando-as por quantidade de recorrências.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta [página](#).

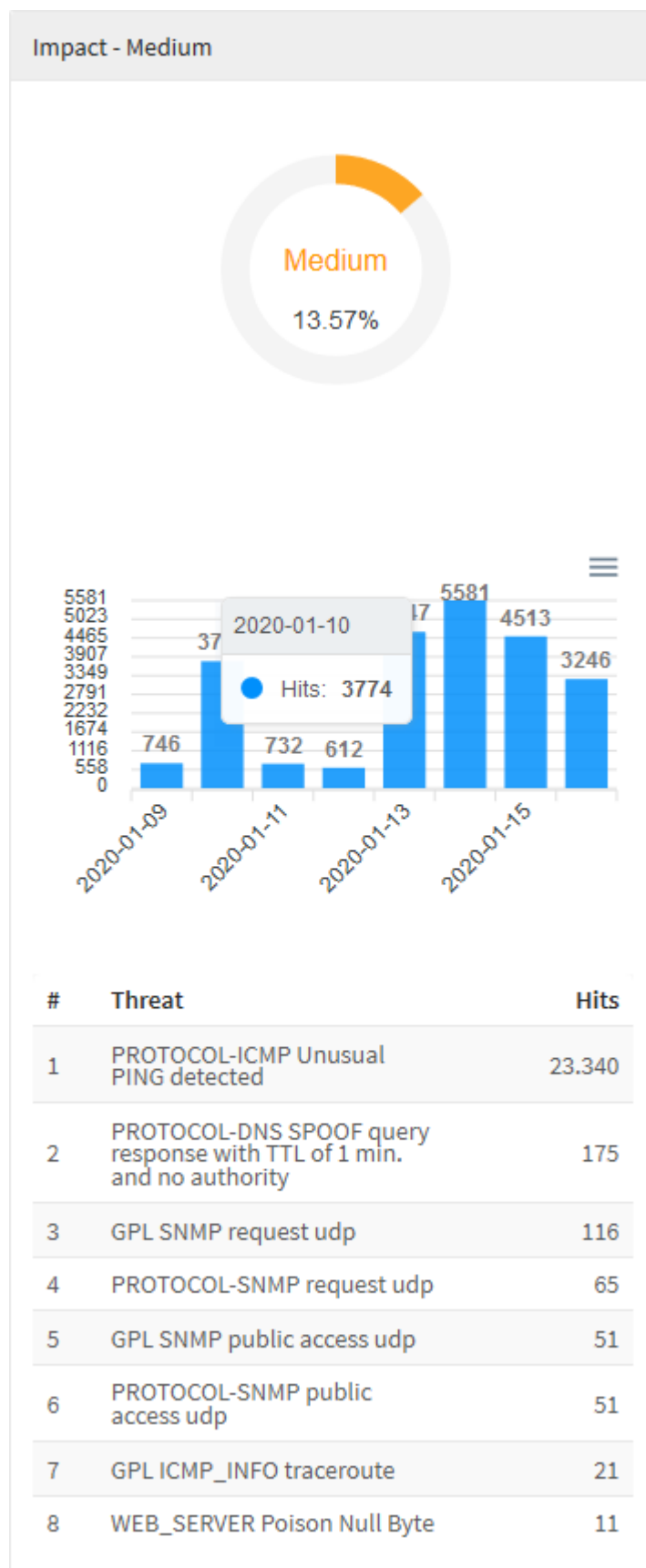
Impact - Medium



#	Threat	Hits
1	PROTOCOL-ICMP Unusual PING detected	23.340
2	PROTOCOL-DNS SPOOF query response with TTL of 1 min. and no authority	175
3	GPL SNMP request udp	116
4	PROTOCOL-SNMP request udp	65
5	GPL SNMP public access udp	51
6	PROTOCOL-SNMP public access udp	51
7	GPL ICMP_INFO traceroute	21
8	WEB_SERVER Poison Null Byte	11

Impact - Medium

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:

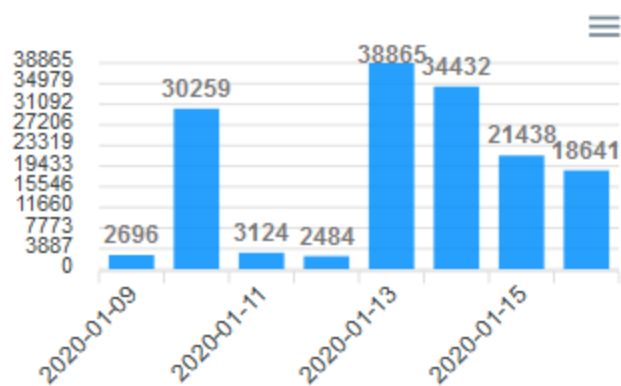
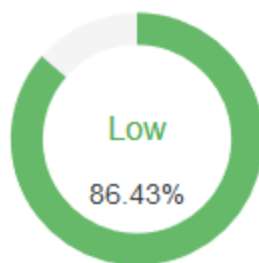


Intrusion Prevention - Impact - Low

Em "*Impact - Low*" temos um gráfico de rosca exibindo a porcentagem de ameaças de intrusão de baixo impacto, seguido de um diagrama de colunas exibindo quantas destas mesmas ocorreram dentro do prazo previamente selecionado em comparação com o tráfego de rede do dia. Além disso, uma lista é exibida com as 10 ameaças de baixo impacto mais recorrentes, exibindo seu nome e listando-as por quantidade de recorrências.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta [página](#).

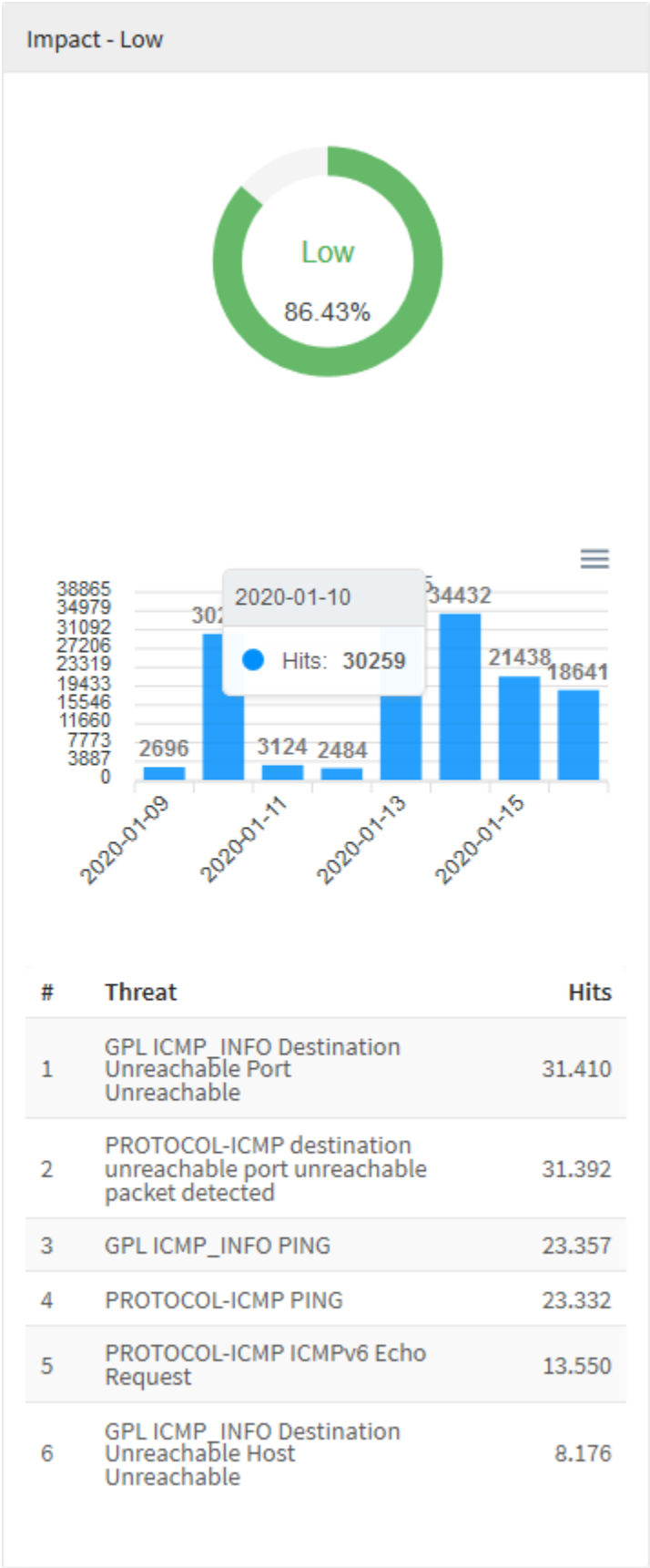
Impact - Low



#	Threat	Hits
1	GPL ICMP_INFO Destination Unreachable Port Unreachable	31.410
2	PROTOCOL-ICMP destination unreachable port unreachable packet detected	31.392
3	GPL ICMP_INFO PING	23.357
4	PROTOCOL-ICMP PING	23.332
5	PROTOCOL-ICMP ICMPv6 Echo Request	13.550
6	GPL ICMP_INFO Destination Unreachable Host Unreachable	8.176

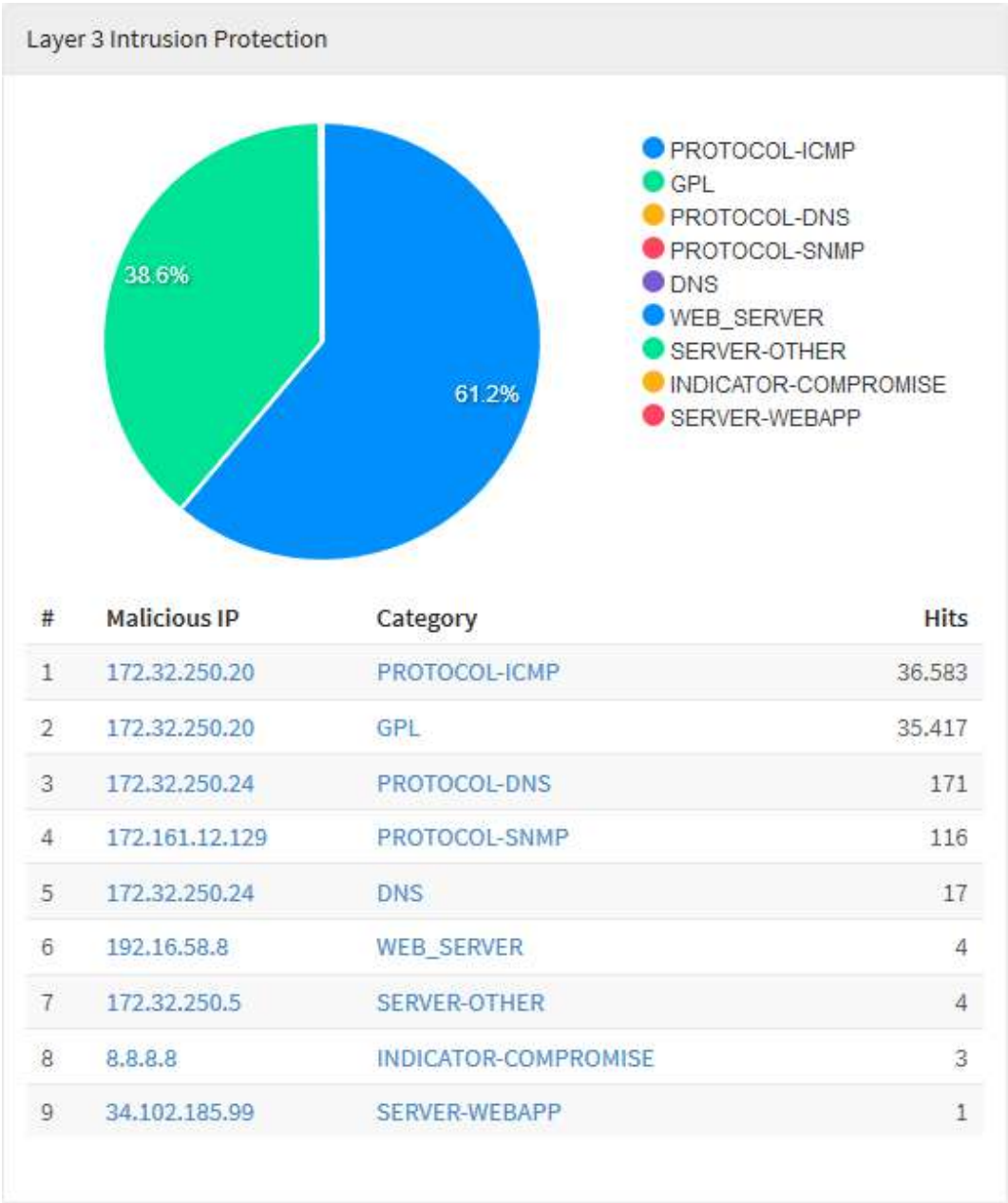
Impact - Low

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:



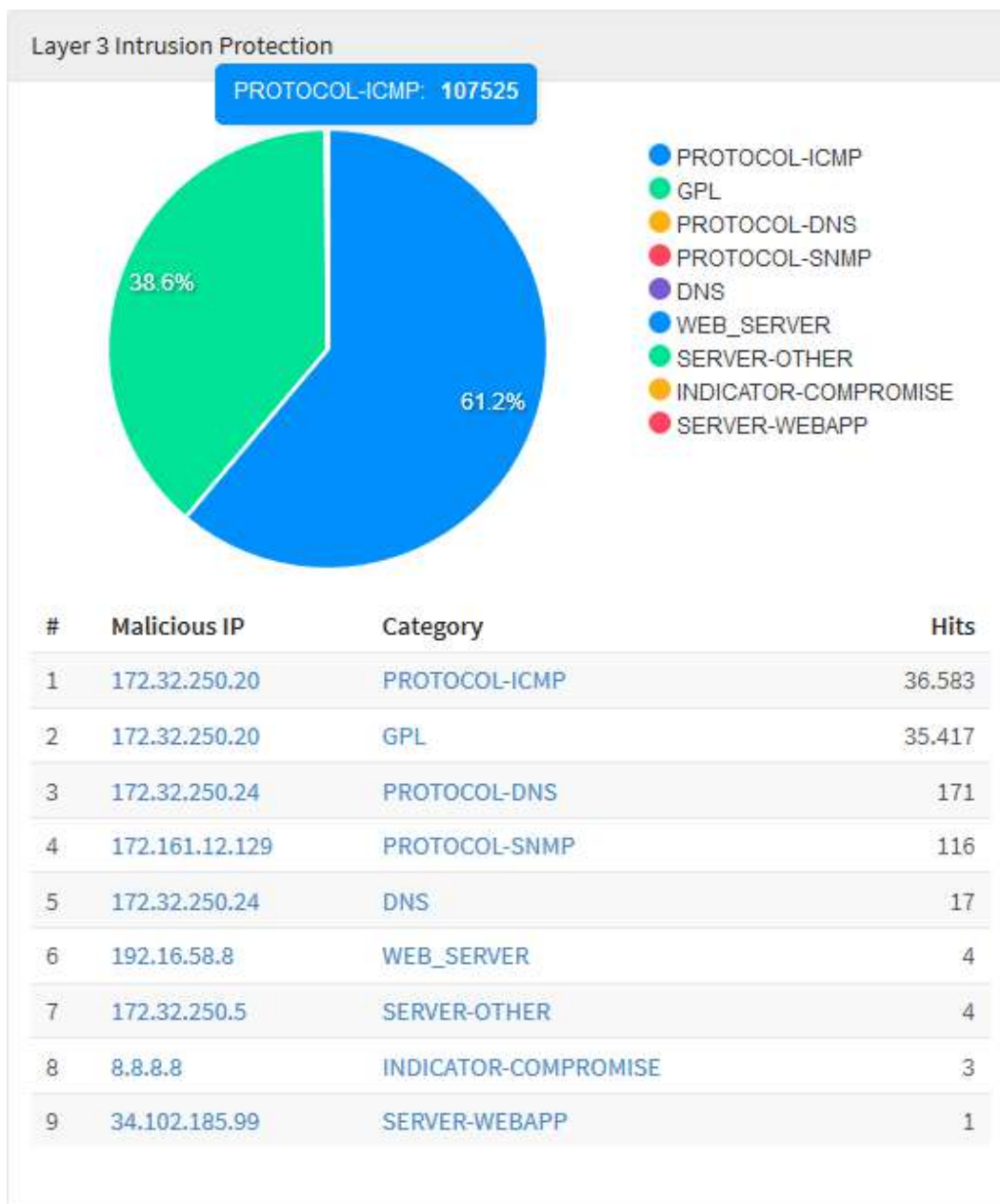
Intrusion Prevention - Layer 3 Intrusion Protection

Em "Layer 3 Intrusion Protection" temos um gráfico exibindo as dez categorias de alertas de intrusão mais detectadas na camada 3 do IPS (Intrusion Prevention System). Ao clicar em um dos IPs ou uma das categorias, você será redirecionado para [*Events](#) usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito do item selecionado. Logo abaixo do gráfico, temos uma listagem dos dez IPs e as categorias mais acessadas em ordem pelo número de acessos.



Layer 3 Intrusion Prevention

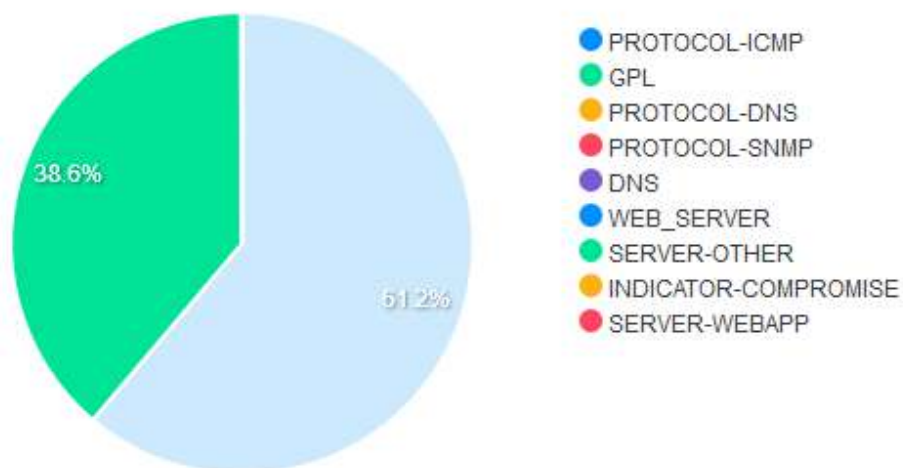
Ao passar o mouse por cima do gráfico, ele exibirá um número com a quantia de alertas de intrusão, conforme demonstrado na imagem abaixo:



Layer 3 Intrusion Prevention - Quantia de alertas de intrusão

Ao passar o mouse sobre a legenda, o gráfico será destacado, conforme demonstrado abaixo:

Layer 3 Intrusion Protection



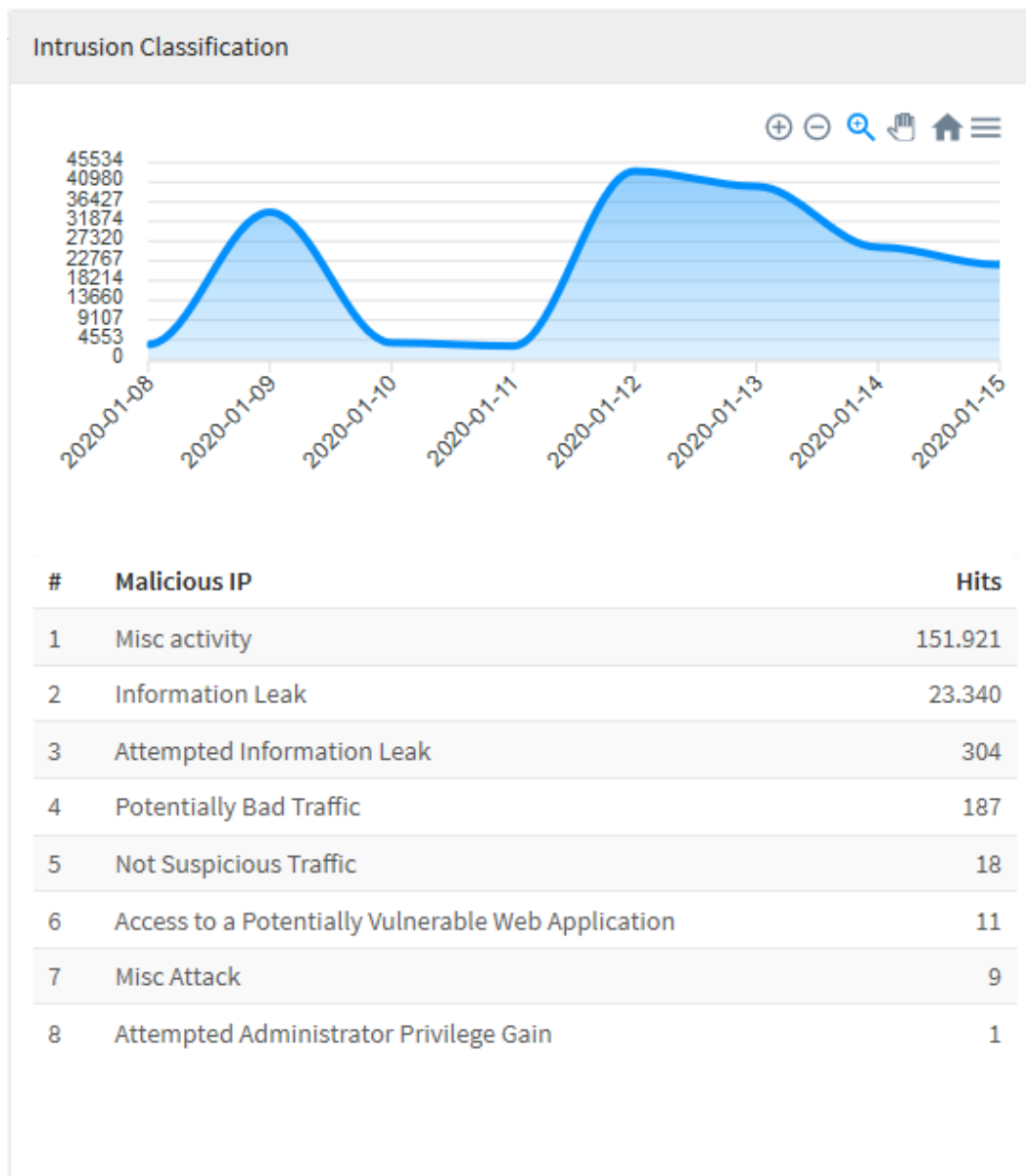
#	Malicious IP	Category	Hits
1	172.32.250.20	PROTOCOL-ICMP	36.583
2	172.32.250.20	GPL	35.417
3	172.32.250.24	PROTOCOL-DNS	171
4	172.161.12.129	PROTOCOL-SNMP	116
5	172.32.250.24	DNS	17
6	192.16.58.8	WEB_SERVER	4
7	172.32.250.5	SERVER-OTHER	4
8	8.8.8.8	INDICATOR-COMPROMISE	3
9	34.102.185.99	SERVER-WEBAPP	1

Layer 3 Intrusion Prevention - Gráfico destacado

Intrusion Prevention - Intrusion Classification

Em "*Intrusion Classification*" temos um gráfico representando as dez classes de alerta de intrusão mais recorrentes em relação ao período de tempo previamente especificado. Abaixo do gráfico, temos uma listagem dos nomes das dez classificações por ordem de maior quantia de acessos.

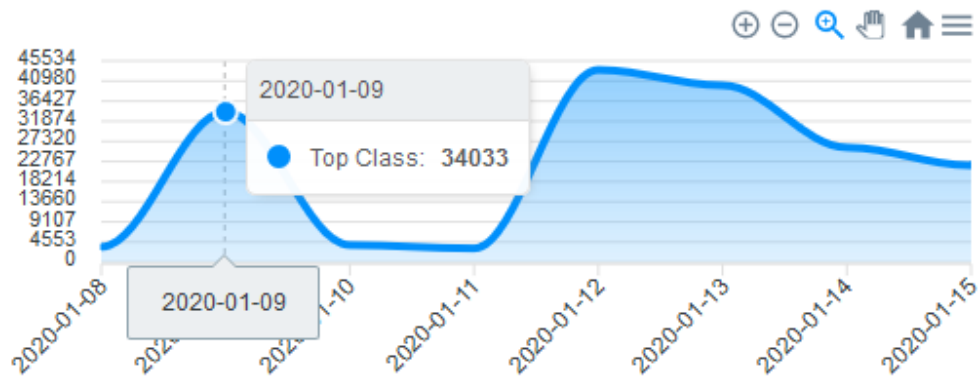
Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta [página](#).



Intrusion Classification

Ao passar o mouse sobre o gráfico, ele evidenciará a data e o número de acessos da classe mais alta deste dia em específico

Intrusion Classification



#	Malicious IP	Hits
1	Misc activity	151.921
2	Information Leak	23.340
3	Attempted Information Leak	304
4	Potentially Bad Traffic	187
5	Not Suspicious Traffic	18
6	Access to a Potentially Vulnerable Web Application	11
7	Misc Attack	9
8	Attempted Administrator Privilege Gain	1

Intrusion Classification - Resumo das classes

Em “*Top Source*” é exibido um gráfico de linha representando as dez fontes de alerta de intrusão mais recorrentes em relação ao período de tempo previamente especificado, ao passar o mouse sobre o gráfico ele mostrará a data e a quantia de acessos a essas fontes em geral. Logo abaixo tem-se uma lista exibindo os *IPs* destas mesmas dez fontes previamente citadas sendo estas classificadas por ordem de maior quantia de acessos. Ao clicar em um dos *IPs* ou uma das categorias, você será redirecionado para **Events* usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito da categoria selecionado

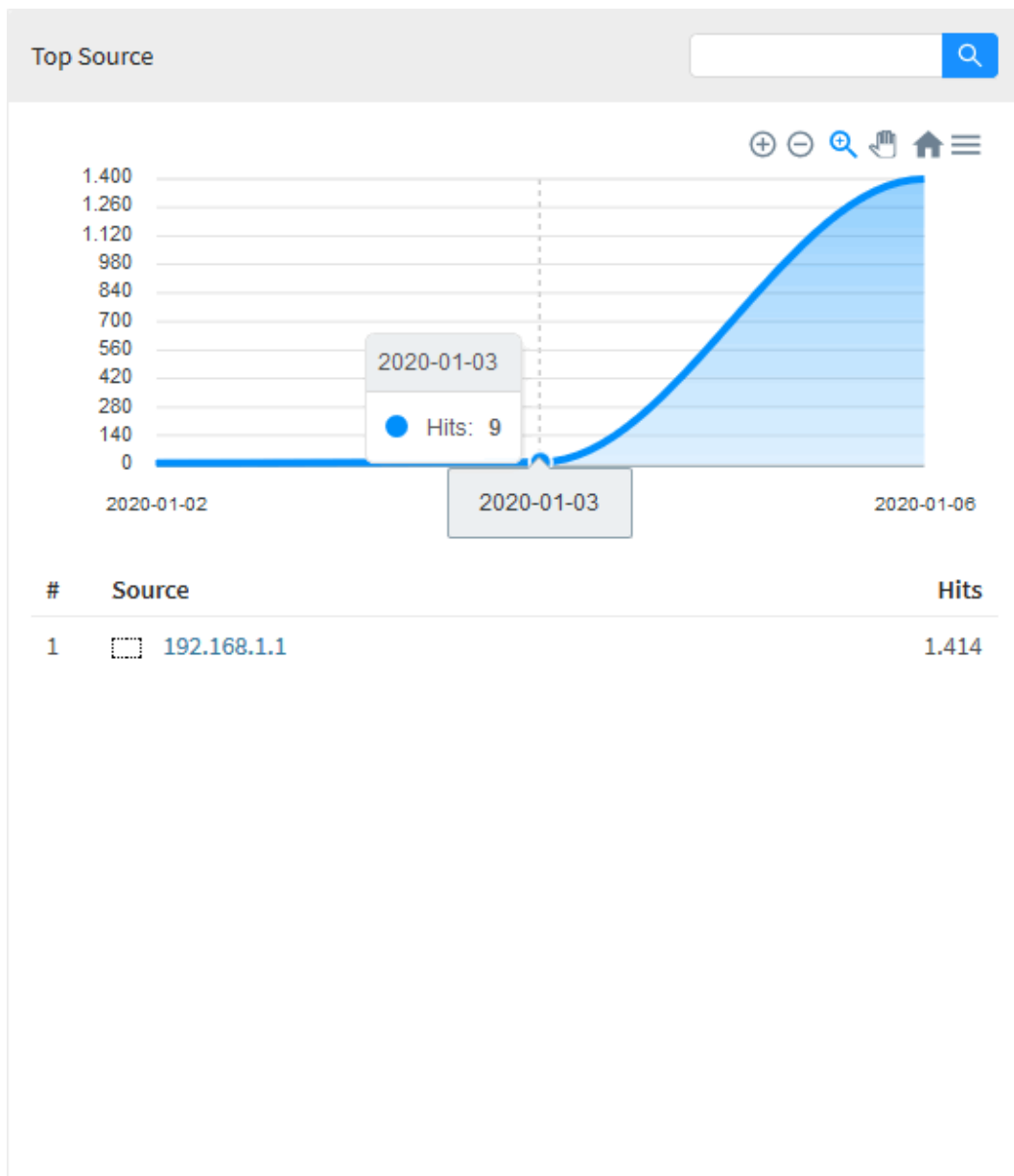
Top Source

1,400
1,260
1,120
980
840
700
560
420
280
140
0

2020-01-02 2020-01-03 2020-01-06

#	Source	Hits
1	192.168.1.1	1,414

Ao passar o mouse sobre o gráfico, ele evidenciará a data e o número de acessos da classe mais alta deste dia em específico:



Top Source - Resumo

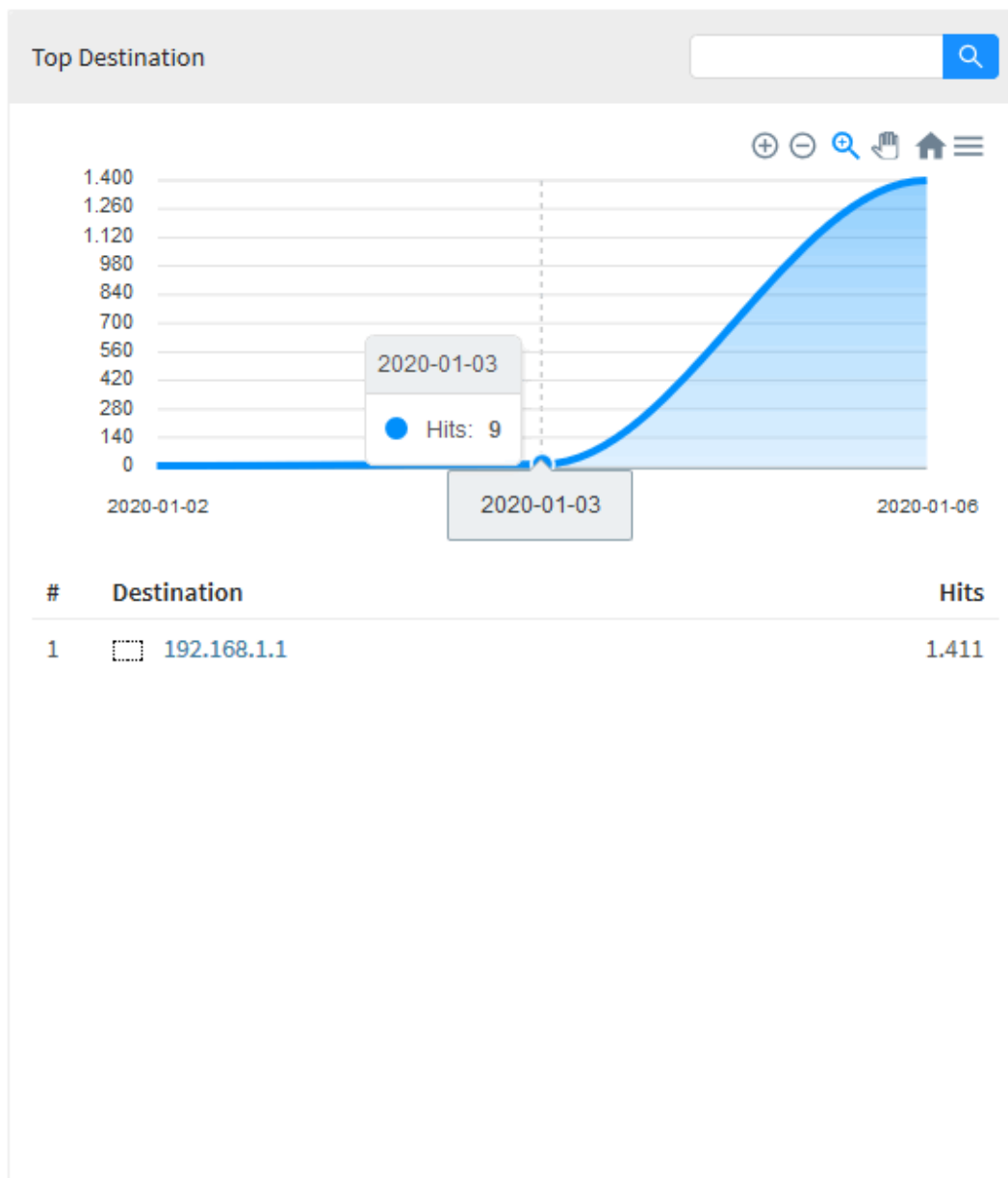
Em “*Top Destination*” tem-se um gráfico de linha exibindo os dez destinos de alerta de intrusão mais recorrentes em relação ao período de tempo previamente especificado, ao passar o mouse sobre o gráfico ele mostrará a data e a quantia de acessos a essas fontes em geral. Logo abaixo tem-se uma lista exibindo os *IPs* dos dez destinos de maior quantia de acessos. Ao clicar em um dos *IPs* ou uma das categorias, você será redirecionado para [*E vents](#) usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito do item selecionado.

Top Destination

The chart displays the number of hits for the top destination, 192.168.1.1, over a five-day period from January 2, 2020, to January 6, 2020. The y-axis represents the number of hits, ranging from 0 to 1,400 in increments of 140. The x-axis shows the dates. The data shows a period of zero hits from January 2 to the early morning of January 3. Starting around 06:00 on January 3, the number of hits begins to rise steadily, reaching a plateau of approximately 1,411 hits by the end of the day on January 6.

#	Destination	Hits
1	192.168.1.1	1,411

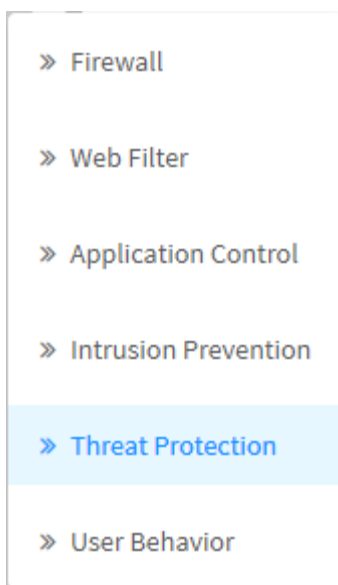
Ao passar o mouse sobre o gráfico, ele evidenciará a data e o número de acessos da classe mais alta deste dia em específico:



Top Destination - Resumo de Acessos

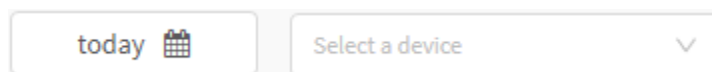
Threat Protection

Para acessar os relatórios de Proteção de Ameaças, clique no ícone "Analysis" localizado na lateral esquerda, um menu *dropdown* será exibido, selecione a opção "Threat Protection".



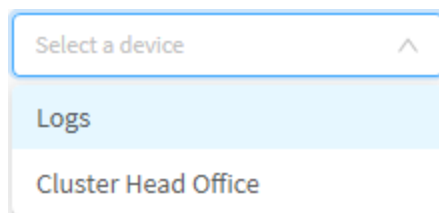
Threat Protection

Para gerar um relatório, localize a caixa de seleção que está posicionada no topo direito da tela, conforme ilustrado a seguir:



Caixa de Seleção

Nesta caixa de seleção estarão listadas todos os *devices* (ou grupos de *devices*) previamente cadastradas no [Device Manager](#), para criar um relatório, selecione o *device* desejado.

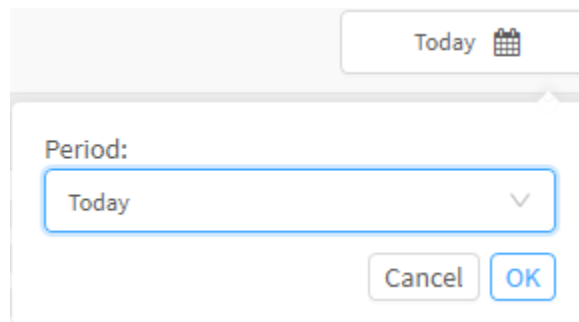


Selecionando Device

Logo do lado direito de onde acabamos de selecionar os *devices*, é possível visualizar uma caixa de seleção de datas, o objetivo desta mesma é basicamente permitir uma filtragem de resultados ainda mais precisa, as opções possíveis são:

- **By date:** Determina uma data específica;
- **By period:** Exibe resultados de uma data inicial ("*Start date*") até uma data final ("*End date*");
- **Today:** Exibe resultados especificamente para a data de hoje;
- **Yesterday:** Exibe resultados especificamente para ontem;
- **Last 7 days:** Filtra especificamente os resultados dos últimos 7 dias;
- **Last 30 days:** Filtra especificamente os resultados dos últimos 30 dias;
- **This month:** Exibe os resultados deste mês;

- **Last month:** Exibe os resultados do último mês.

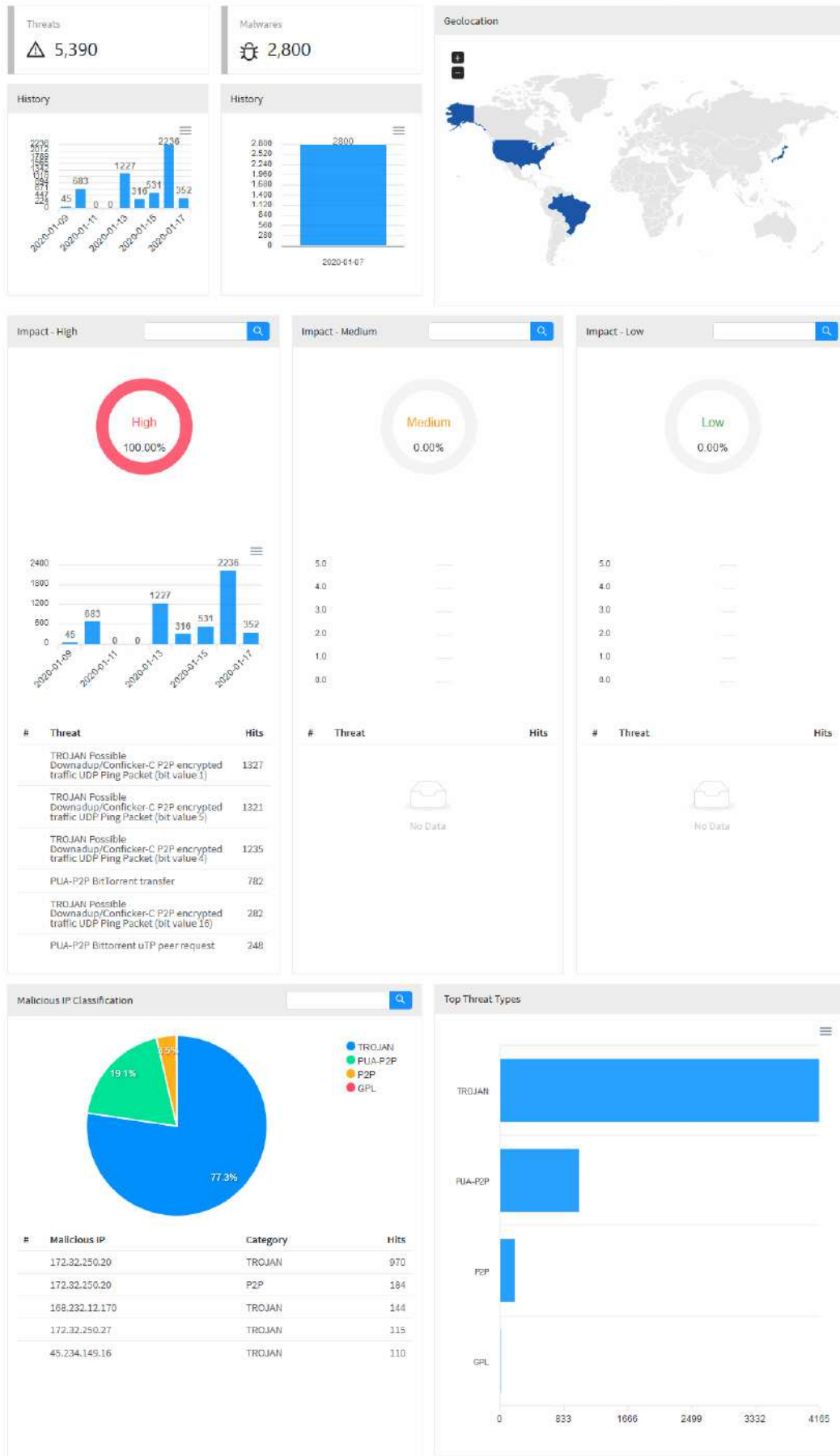


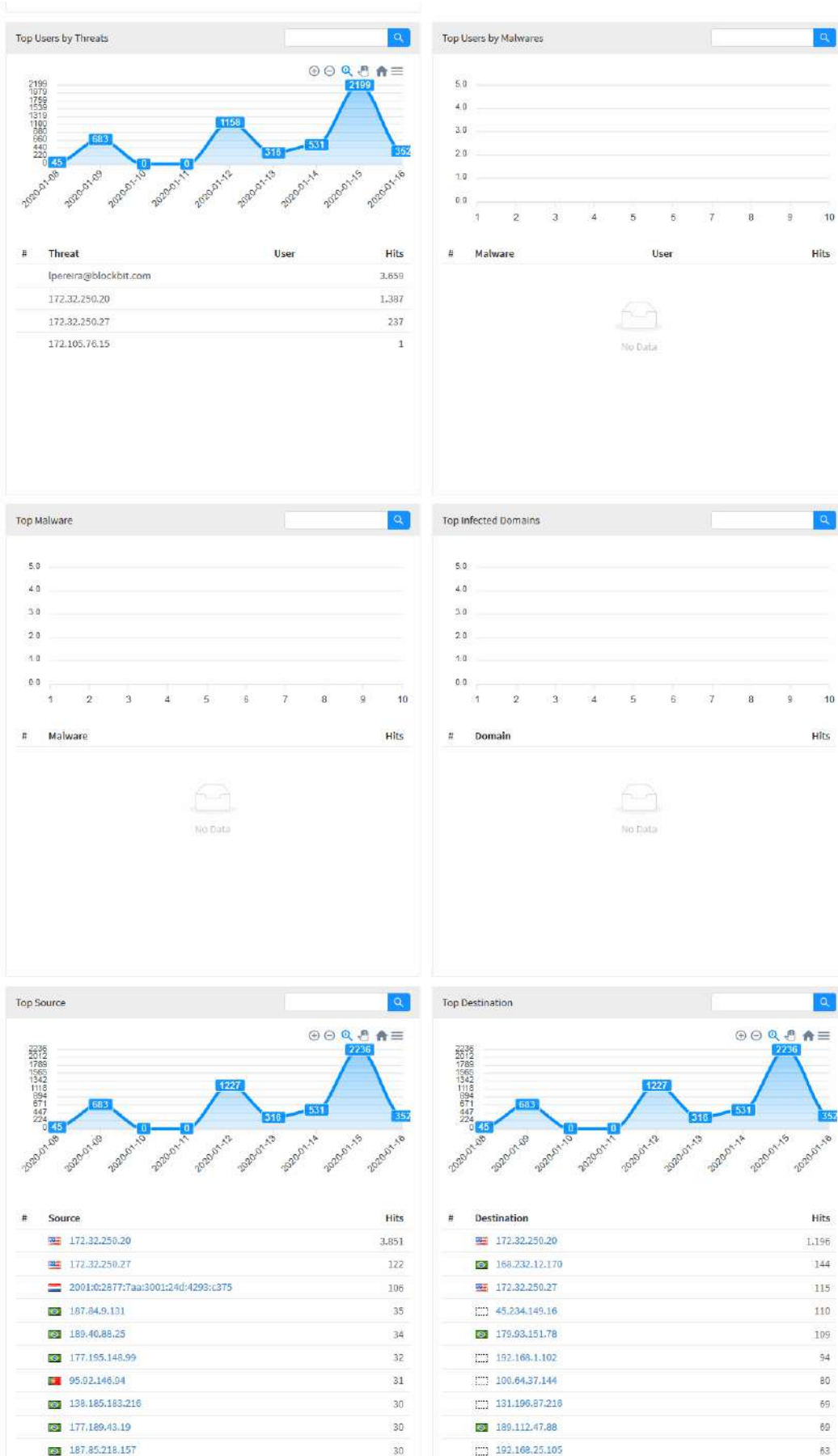
The image shows a date selection dialog box. At the top right, there is a button labeled "Today" with a calendar icon. Below this, the text "Period:" is followed by a dropdown menu that currently displays "Today" with a downward arrow. At the bottom right of the dialog, there are two buttons: "Cancel" and "OK".

Seleção de Data

Selecione a data desejada e clique em **Ok** [];

Threats





A maioria dos gráficos desta aba possui um menu de navegação e uma barra de busca.

O menu de navegação possui os seguintes botões:

- : Serve para dar um zoom;
- : Tem como função remover o zoom;
- : Serve para fazer um zoom de seleção;
- : Serve para mover o gráfico;
- : Reseta o gráfico para a posição inicial;
- : Permitir baixar este diagrama no formato *svg*, *png* ou *csv*.

A barra de busca permite pesquisar um item específico e modificar os diagramas de acordo com os resultados da pesquisa.

Para efetuar uma pesquisa, digite um termo na barra de busca e clique no **botão de busca** .

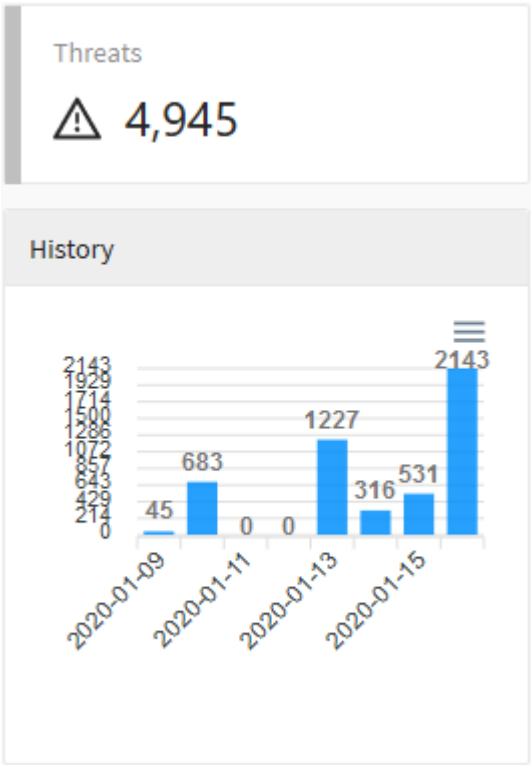
A seguir, analisaremos em detalhes os componentes de “*Threat Protection*”:

- [Threats e History](#);
- [Malwares e History](#);
- [Geolocation](#);
- [Impact - High](#);
- [Impact - Medium](#);
- [Impact - Low](#);
- [Malicious IP Classification](#);
- [Top Threat Types](#);
- [Top Users by Threats](#);
- [Top Users by Malware](#);
- [Top Malware](#);
- [Top Infected Domains](#);
- [Top Source](#);
- [Top Destination](#).

Threat Protection - Threats e History

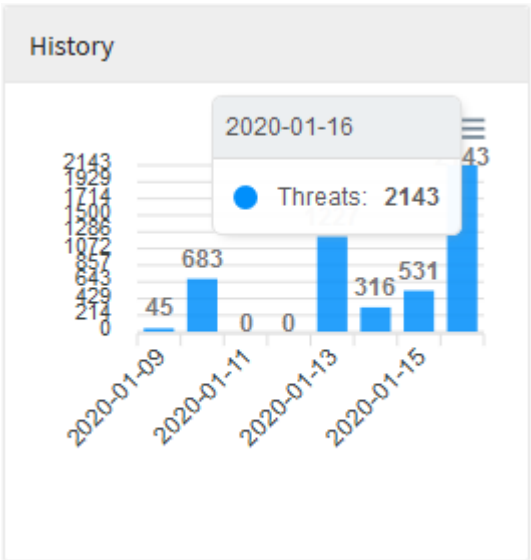
O painel “Threats” exibe um total de ameaças detectadas. Logo abaixo, é exibido o histórico em um gráfico de linhas demonstrando a quantia de ameaças detectadas por dia.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta [página](#).



Threat Protection - Threats e History

Ao passar o mouse por cima do gráfico, um resumo das ameaças do período é exibido, conforme demonstrado na imagem abaixo:

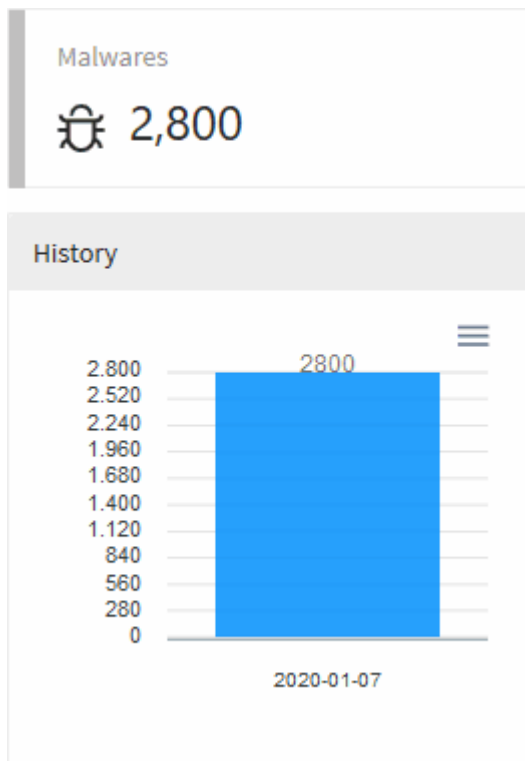


Threat Protection - History - Resumo das ameaças

Threat Protection - Malwares e History

Já em "*Malwares*", é exibido um número totalizando a quantia de *malwares* detectados. Logo abaixo, é exibido o histórico em um gráfico de barras demonstrando a quantia de ameaças detectadas por dia.

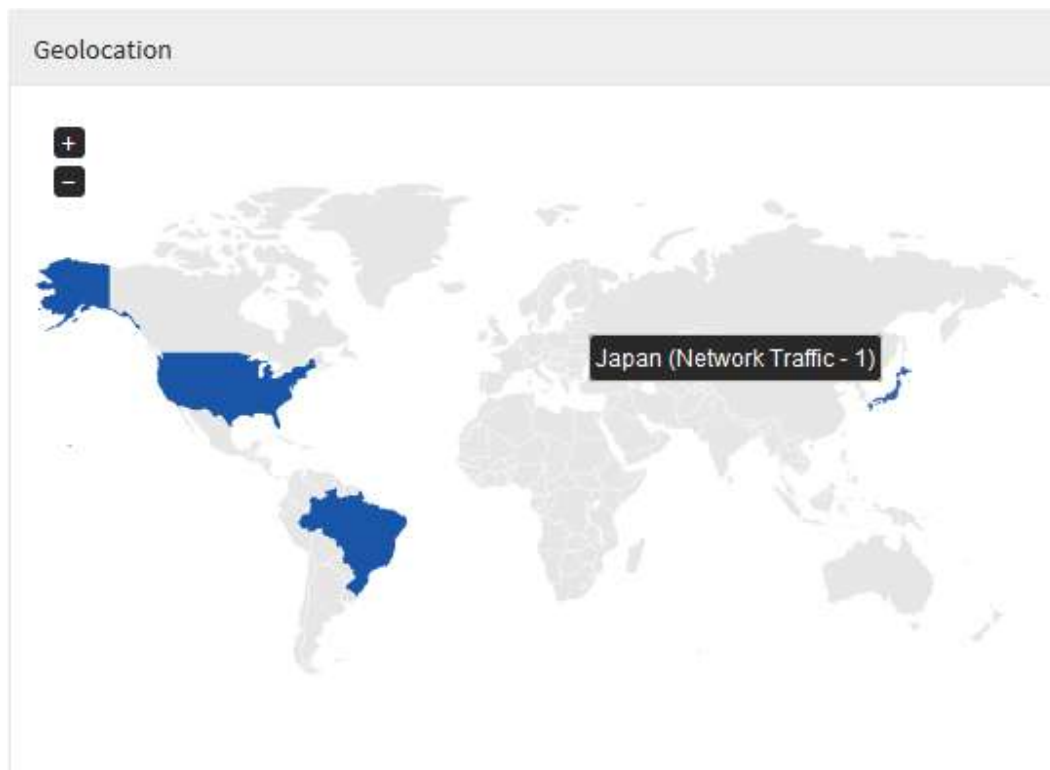
Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta [página](#).



Threat Protection - Malware e History

Threat Protection - Geolocation

Em "Geolocation" é exibida a origem das ameaças por geolocalização, o mapa global demonstra através de uma legenda colorida o nível de risco. Ao passar o mouse por cima dos países um número total de ameaças é exibido, ao fazer o mesmo com a legenda é possível visualizar uma média, além disso, o país referente a esse valor é destacado no mapa.

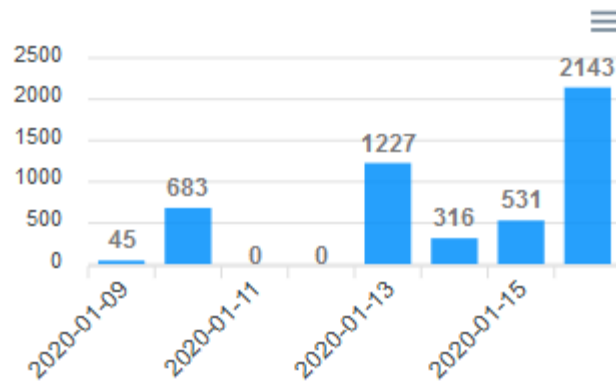


Threat Protection – Geolocation

Threat Protection - Impact - High

Em "*Impact - High*" temos um gráfico de rosca exibindo a porcentagem de ameaças de alto impacto, seguido de um diagrama de colunas exibindo quantas destas mesmas ocorreram dentro do prazo previamente selecionado em comparação com o tráfego de rede do dia. Além disso, uma lista é exibida com as 10 ameaças de alto impacto mais recorrentes, exibindo seu nome e listando-as por quantidade de recorrências.

Para mais informações a respeito da barra de busca presente no topo deste gráfico cheque esta [página](#).

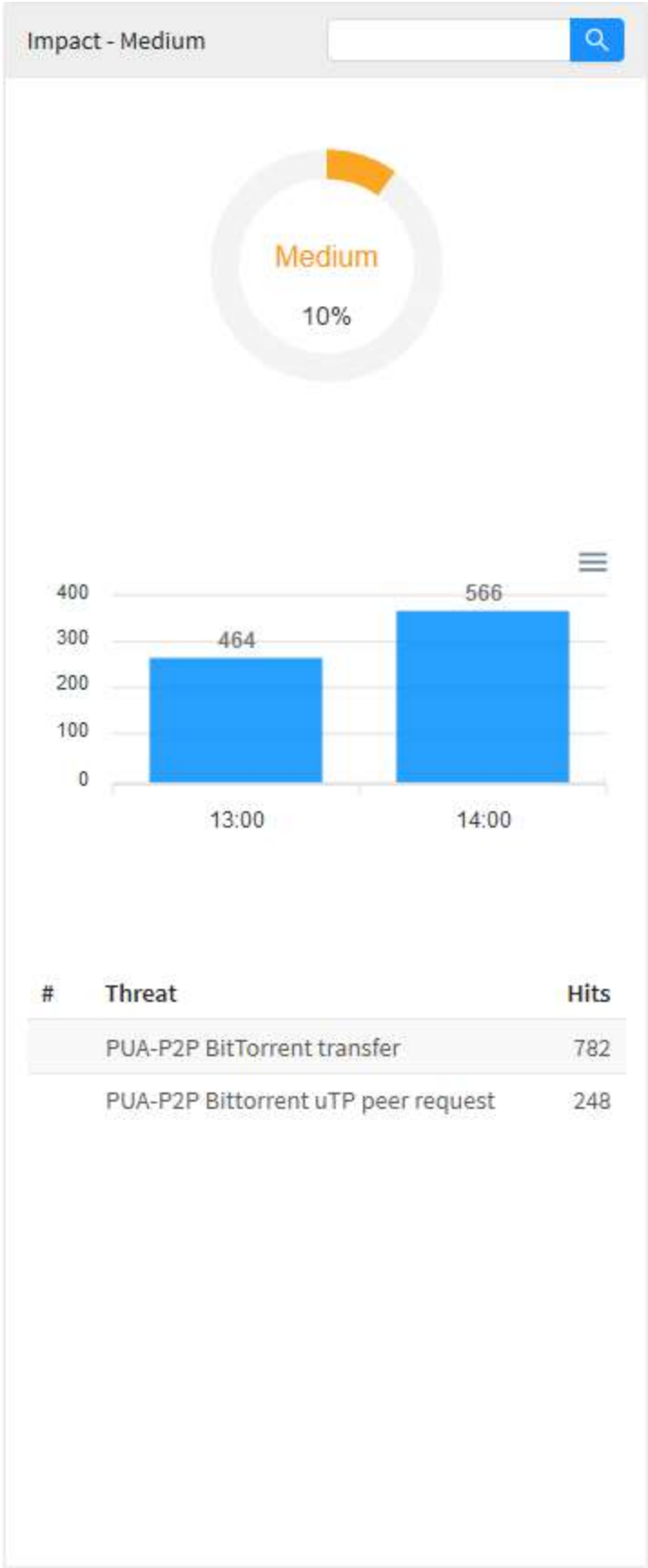


#	Threat	Hits
	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 5)	1191
	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 1)	1150
	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 4)	1109
	PUA-P2P BitTorrent transfer	782
	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 16)	270
	PUA-P2P Bittorrent uTP peer request	248

Threat Protection – Impact - Medium

Em "*Impact - Medium*" temos um gráfico de rosca exibindo a porcentagem de ameaças de médio impacto, seguido de um diagrama de colunas exibindo quantas destas mesmas ocorreram dentro do prazo previamente selecionado em comparação com o tráfego de rede do dia. Além disso, uma lista é exibida com as 10 ameaças de médio impacto mais recorrentes, exibindo seu nome e listando-as por quantidade de recorrências.

Para mais informações a respeito da barra de busca presente no topo deste gráfico cheque esta [página](#).



Threat Protection – Impact Medium

Threat Protection – Impact - Low

Em "*Impact - Low*" temos um gráfico de rosca exibindo a porcentagem de ameaças de baixo impacto, seguido de um diagrama de colunas exibindo quantas destas mesmas ocorreram dentro do prazo previamente selecionado em comparação com o tráfego de rede do dia. Além disso, uma lista é exibida com as 10 ameaças de baixo impacto mais recorrentes, exibindo seu nome e listando-as por quantidade de recorrências.

Para mais informações a respeito da barra de busca presente no topo deste gráfico cheque esta [página](#).

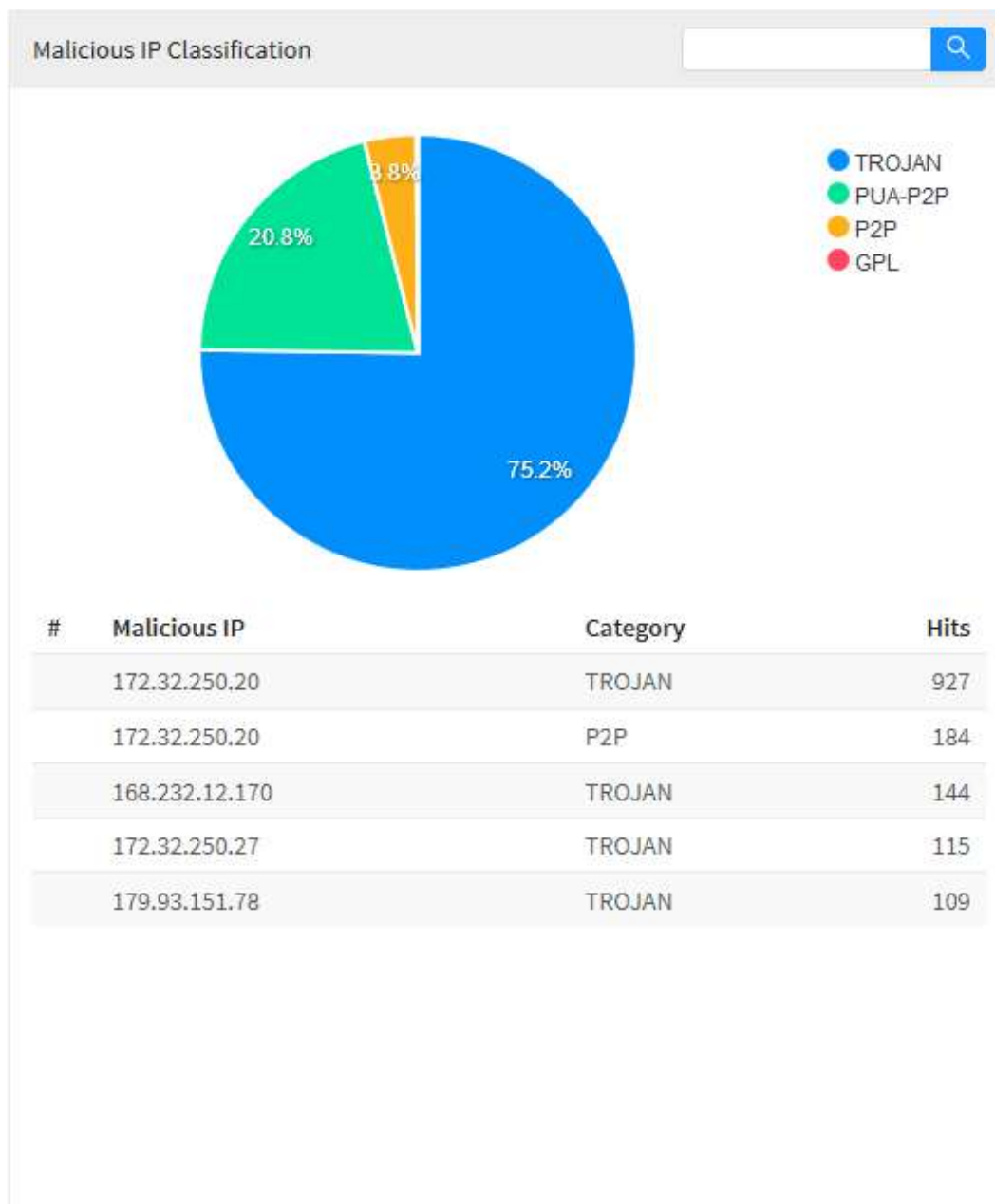


Threat Protection – Impact Low

Threat Protection – Malicious IP Classification

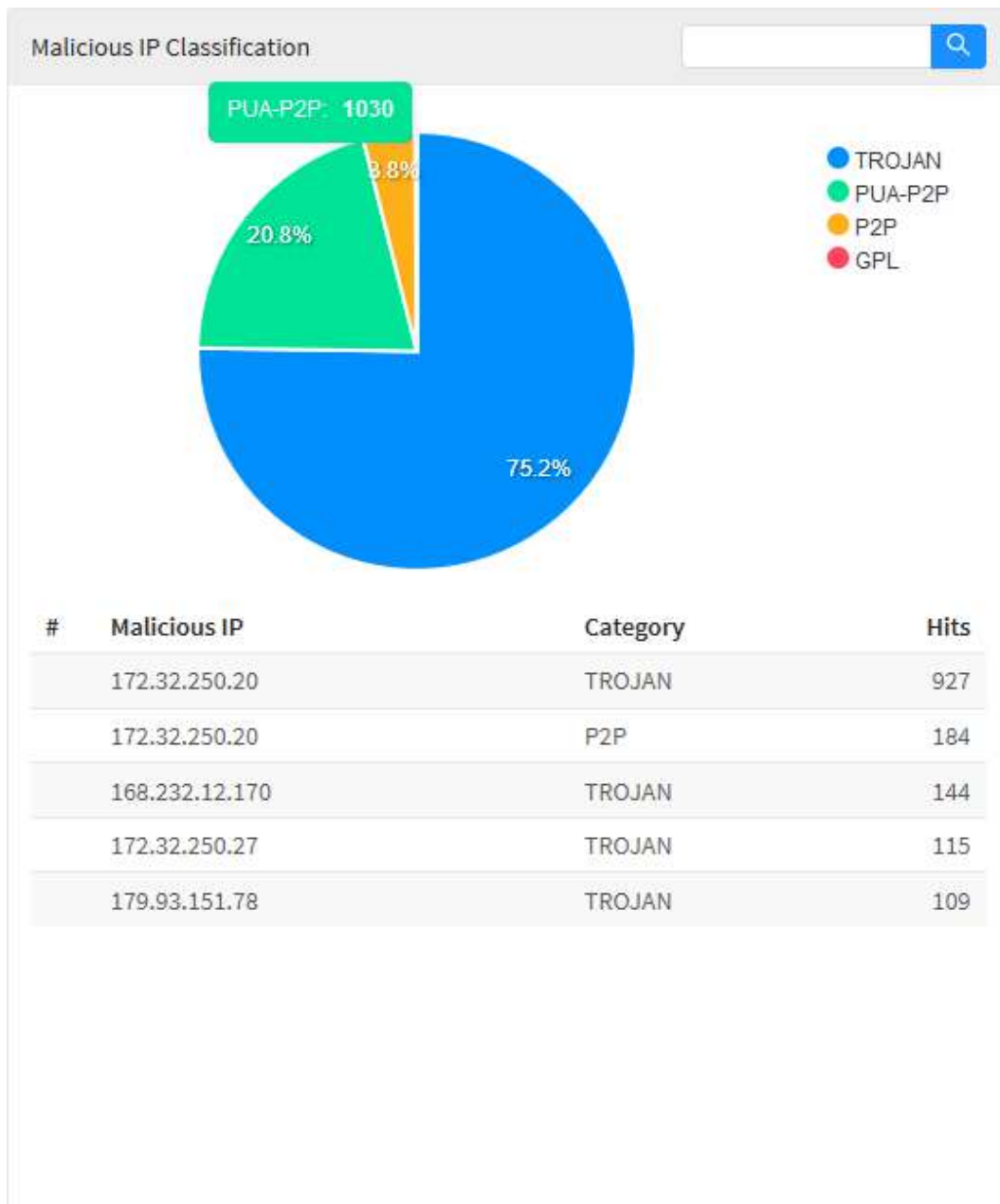
Em "*Malicious IP Classification*" temos um gráfico de rosca exibindo as dez categorias de alertas de *IP* Malicioso mais detectadas na rede, ao passar o mouse sobre cada parte do gráfico ou seu texto correspondente, ele o destacará e exibirá um número com a quantia de acessos a essa categoria de *IP* e sua porcentagem correspondente em relação com as outras categorias. Logo abaixo do gráfico, temos uma listagem dos dez *IPs* que mais acessaram essas categorias ordenados por número de acessos.

Para mais informações a respeito do menu de navegação e da barra de busca presente no topo deste gráfico cheque esta [página](#).



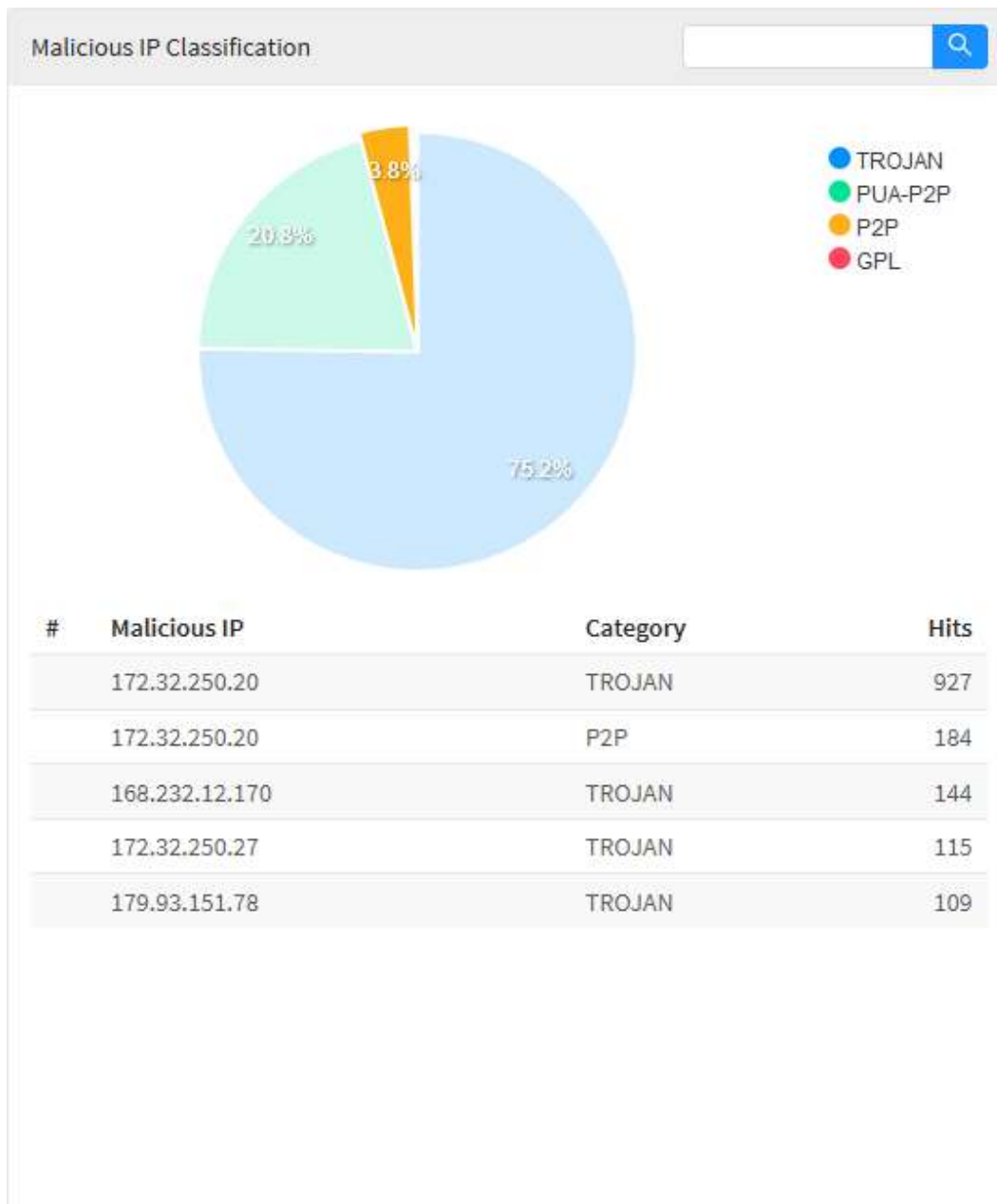
Threat Protection – Malicious IP Classification

Ao passar o mouse por cima do gráfico, ele exibirá um número com a quantia de *IPs* maliciosos, conforme demonstrado na imagem abaixo:



Threat Protection – Malicious IP Classification - Resumo

Ao passar o mouse sobre a legenda, o gráfico será destacado, conforme demonstrado abaixo:

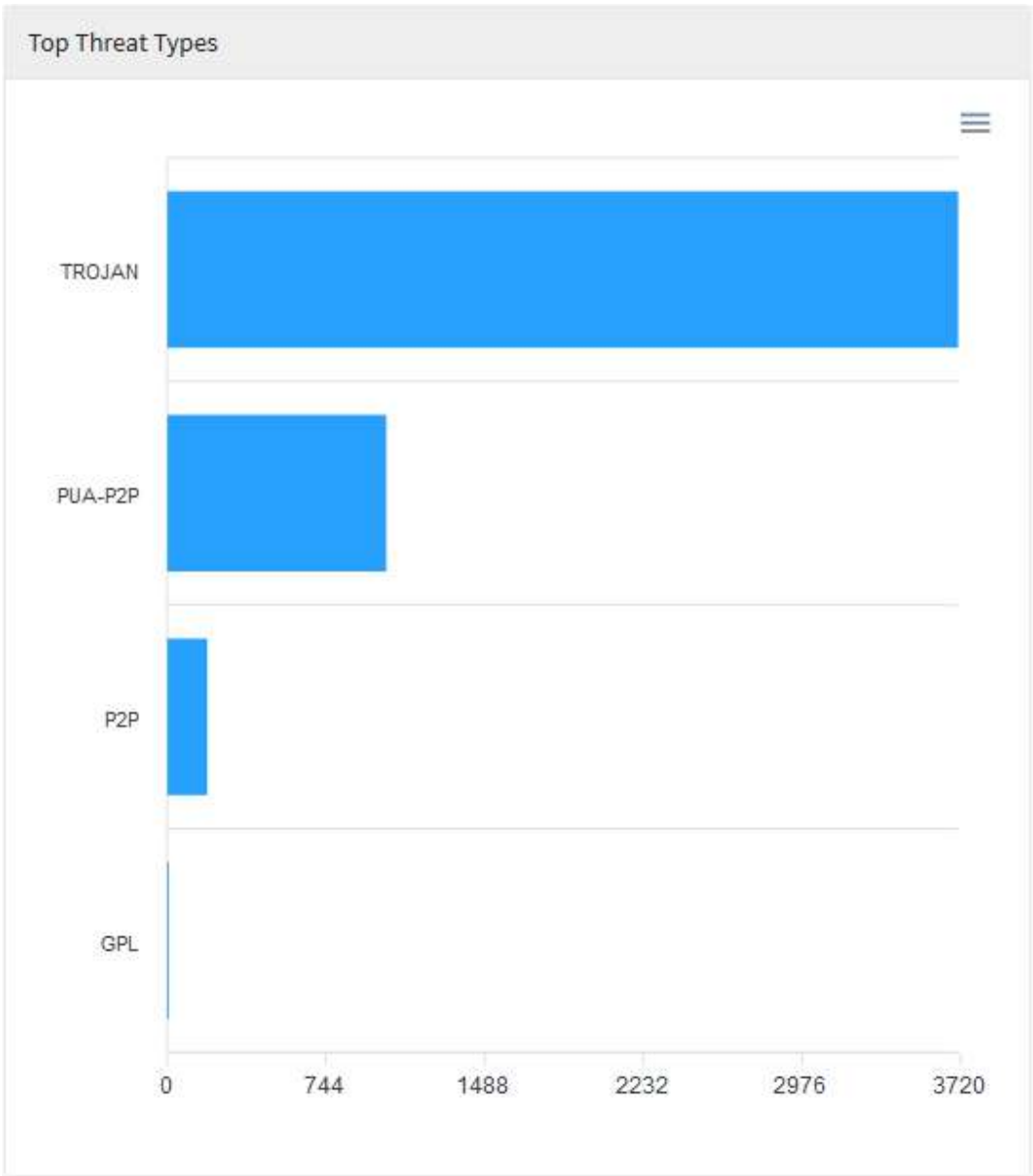


Threat Protection – Malicious IP Classification - Resumo

Threat Protection – Top Threat Types

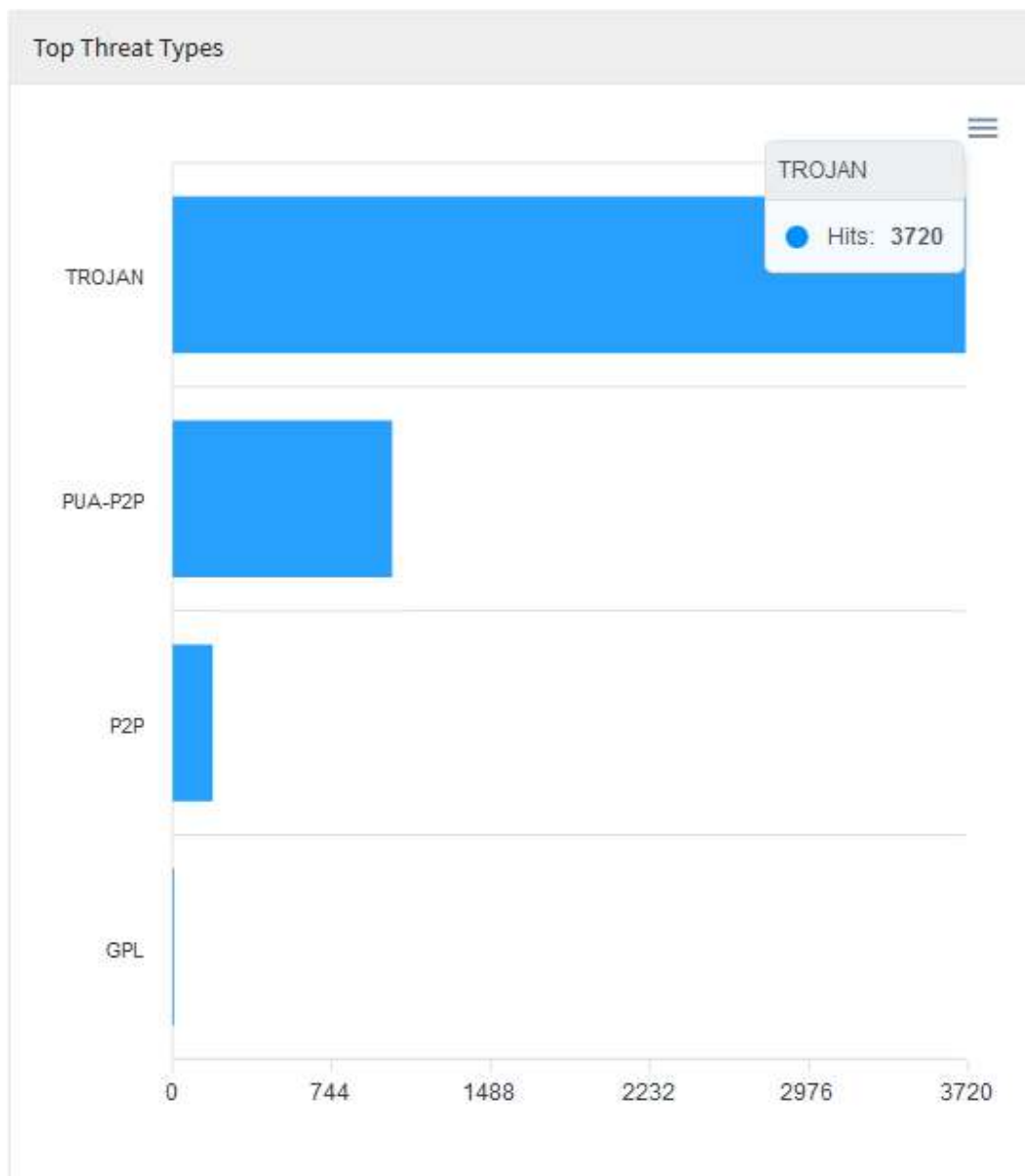
Em "Top Threat Types" é exibido um gráfico de barras representando os tipos de ameaça mais recorrentes em relação a quantia de vezes que elas foram detectadas

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta [página](#).



Threat Protection – Top Threat Types

Ao passar o mouse sobre o gráfico ele mostrará a quantia exata de detecções:

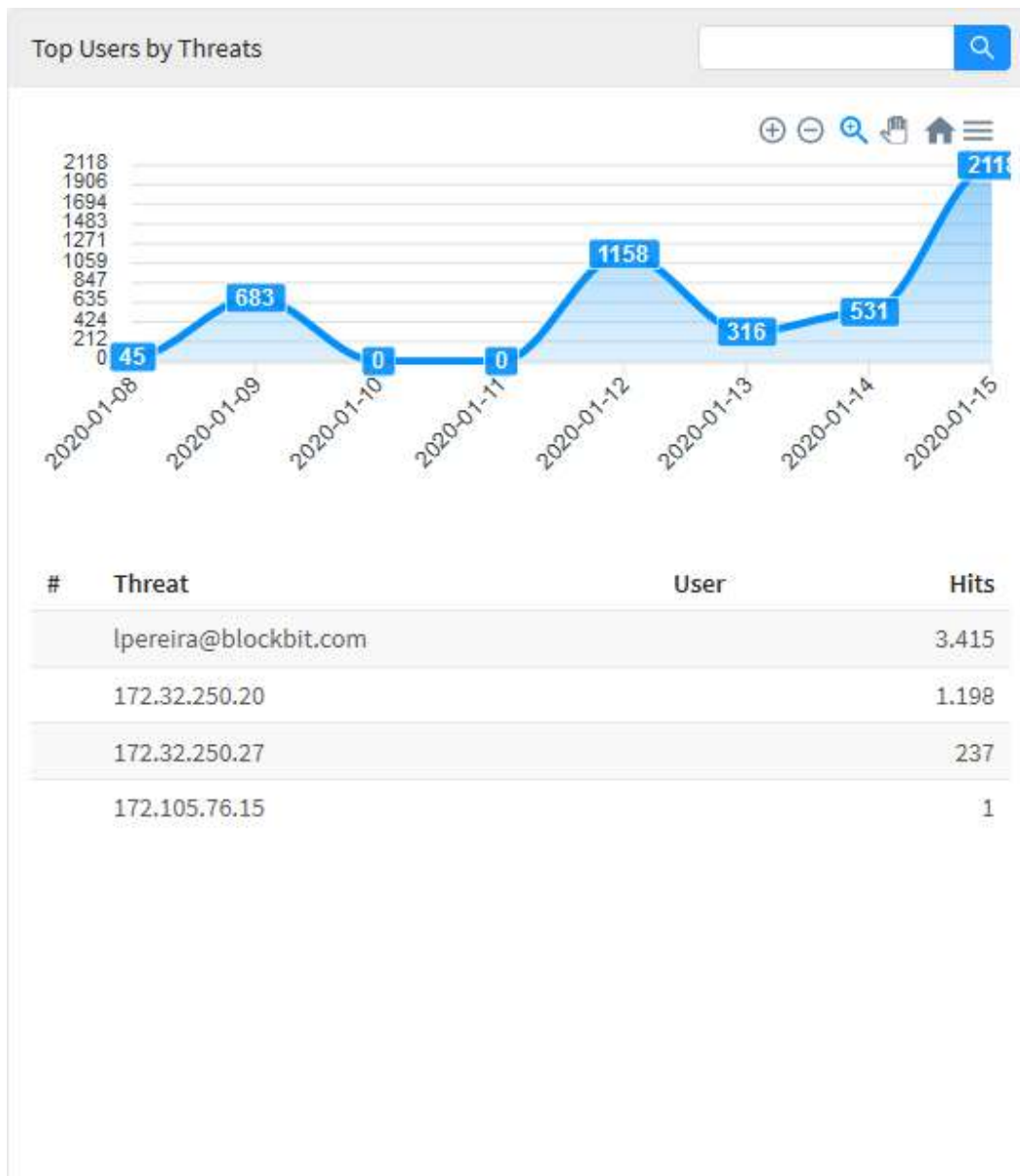


Threat Protection – Top Threat Types - Resumo

Threat Protection – Top Users by Threats

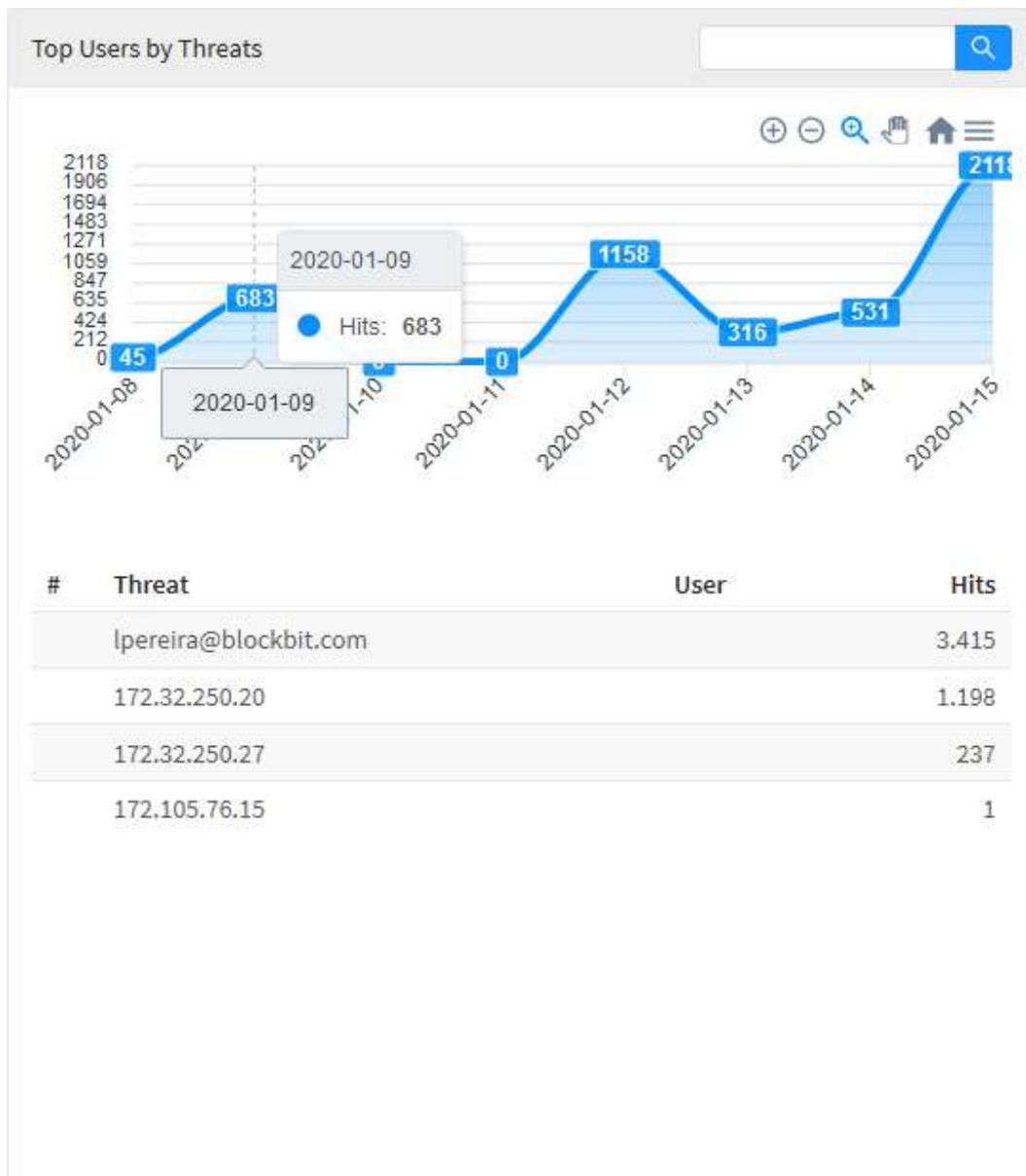
Em "Top Users by Threats" temos um gráfico de linha exibindo a quantia de ameaças por dia, ao passar o mouse sobre cada parte do gráfico, ele o destacará e exibirá um número com a quantia de ameaças do dia selecionado. Logo abaixo do gráfico, temos uma listagem dos dez usuários que mais foram afetados por essas ameaças ordenados por quantia de acessos.

Para mais informações a respeito do menu de navegação e da barra de busca presente no topo deste gráfico cheque esta [página](#).



Threat Protection – Top Users by Threats

Ao passar o mouse por cima do gráfico, é exibido um resumo dos resultados dentro do período selecionado, conforme demonstrado na imagem abaixo:

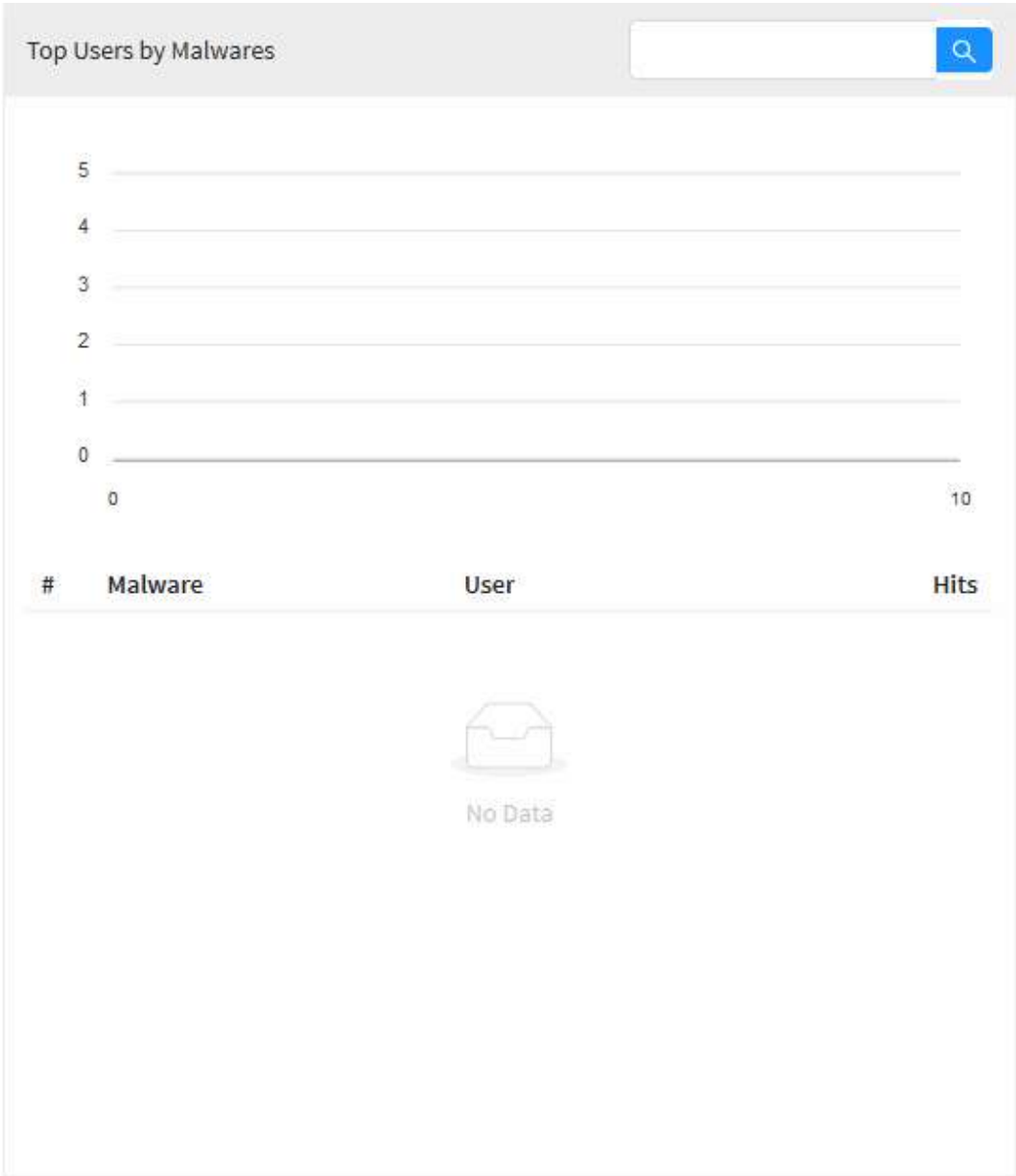


Threat Protection – Top Users by Threats - Resumo

Threat Protection – Top Users by Malware

Em “*Top Users by Malware*” temos um gráfico de linha exibindo a quantia de alerta de *malware* por dia, ao passar o *mouse* sobre cada parte do gráfico, ele o destacará e exibirá um número com a quantia de ameaças do dia selecionado. Logo abaixo do gráfico, temos uma listagem dos dez usuários que mais foram afetados por *malware* ordenados por quantia de detecções. Logo abaixo do gráfico, temos uma listagem dos dez usuários que mais foram afetados por essas ameaças ordenados por quantia de acessos. Por fim, ao clicar em um desses usuários ou *IPs*, você será redirecionado para [Events](#) usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito do usuário selecionado.

Para mais informações a respeito da barra de busca presente no topo deste gráfico cheque esta [página](#).

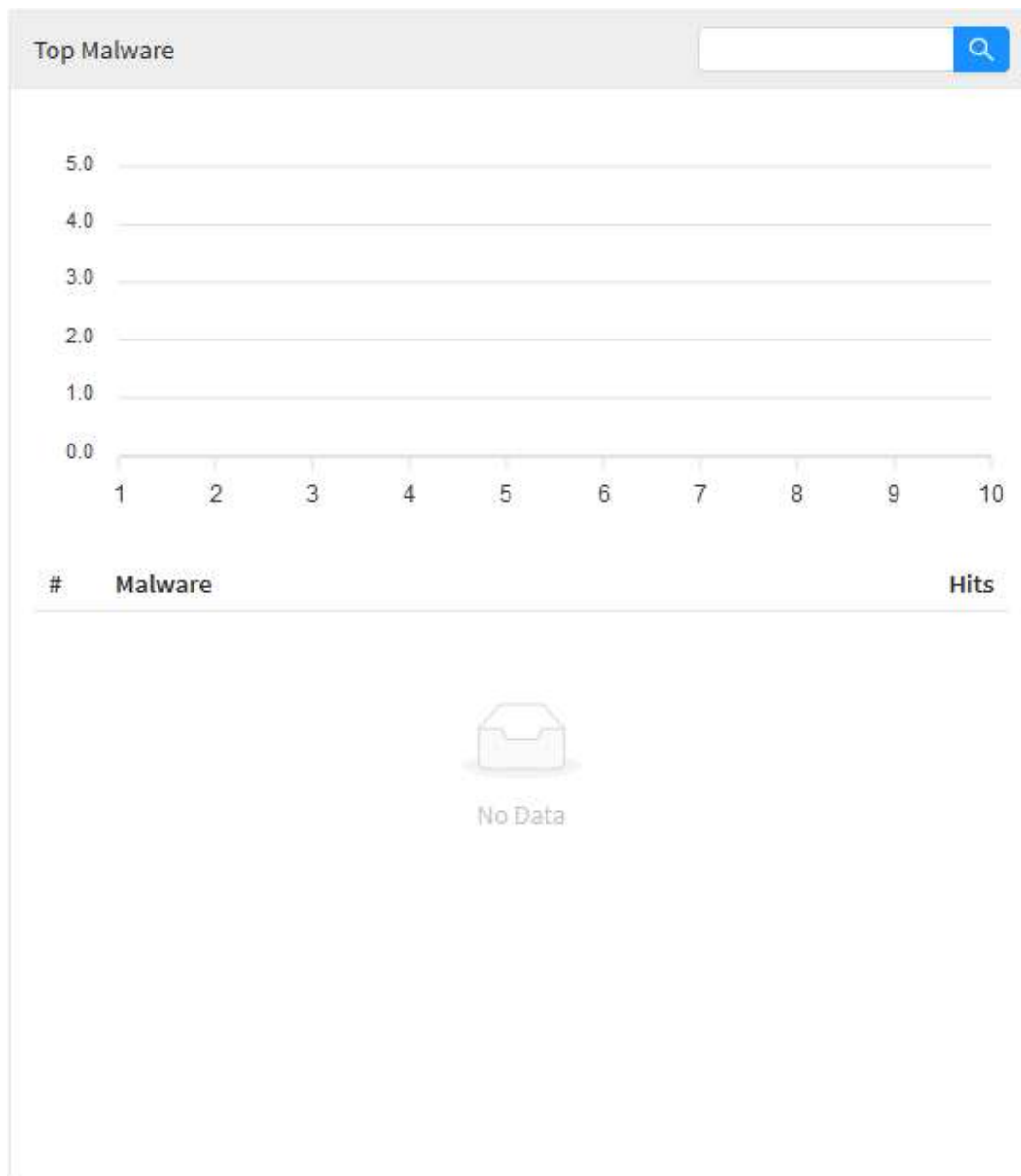


Threat Protection – Top Users by Malware

Threat Protection – Top Malware

Em “*Top Malware*” temos um gráfico de linha exibindo a quantia de *malwares* detectados por dia, ao passar o mouse sobre cada parte do gráfico, ele o destacará e exibirá um número com a quantia de detecções do dia selecionado. Logo abaixo do gráfico, temos uma listagem dos dez *malwares* mais recorrentes ordenados por quantia de detecções.

Para mais informações a respeito da barra de busca presente no topo deste gráfico cheque esta [página](#).



Threat Protection – Top Malware

Threat Protection – Top Infected Domains

Em "Top Infected Domains" temos um gráfico de linha exibindo a quantia de domínios infectados detectados por dia, ao passar o *mouse* sobre cada parte do gráfico, ele o destacará e exibirá um número com a quantia de detecções do dia selecionado. Logo abaixo do gráfico, temos uma listagem dos dez domínios mais recorrentes ordenados por quantia de detecções.

Para mais informações a respeito da barra de busca presente no topo deste gráfico cheque esta [página](#).



Threat Protection – Top Infected Sites

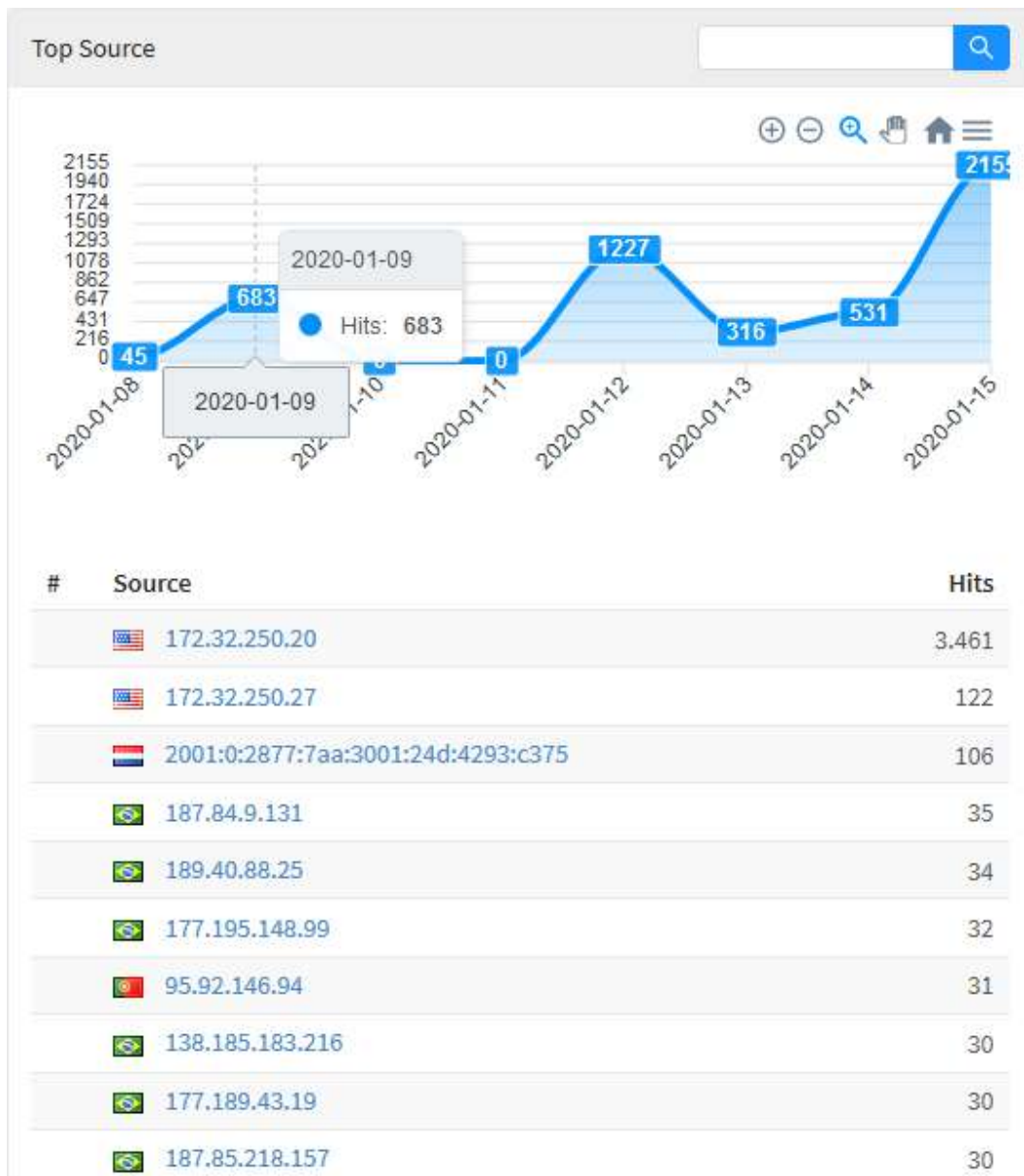
Em “*Top Source*” é exibido um gráfico de linha representando as dez fontes de ameaça mais recorrentes em relação ao período de tempo previamente especificado, ao passar o *mouse* sobre o gráfico ele mostrará a data e a quantia de acessos a essas fontes em geral. Logo abaixo tem-se uma lista exibindo os *IPs* destas mesmas dez fontes previamente citadas sendo estas classificadas por ordem de maior quantia de acessos. Ao clicar em um dos *IPs* ou uma das categorias, você será redirecionado para ***Events** usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito da fonte de ameaça selecionada.

Top Source

Date	Hits
2020-01-08	45
2020-01-09	683
2020-01-10	0
2020-01-11	0
2020-01-12	1227
2020-01-13	316
2020-01-14	531
2020-01-15	2155

#	Source	Hits
1	172.32.250.20	3,461
2	172.32.250.27	122
3	2001:0:2877:7aa:3001:24d:4293:c375	106
4	187.84.9.131	35
5	189.40.88.25	34
6	177.195.148.99	32
7	95.92.146.94	31
8	138.185.183.216	30
9	177.189.43.19	30
10	187.85.218.157	30

Ao passar o mouse por cima do gráfico, é exibido um resumo dos resultados dentro do período selecionado, conforme demonstrado na imagem abaixo:



Threat Protection – Top Source - Resumo

Em “*Top Destination*” é exibido um gráfico representando os dez destinos de ameaça mais recorrentes em relação ao período de tempo previamente especificado, ao passar o mouse sobre o gráfico ele mostrará a data e a quantia de acessos a essas fontes em geral. Logo abaixo tem-se uma lista exibindo os IPs destes mesmos dez destinos previamente citadas sendo estes classificados por ordem de maior quantia de acessos. Ao clicar em um dos IPs, você será redirecionado para [*Events](#) usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito da fonte de ameaça selecionada.

Top Destination

Hour	Hits
21h	57
22h	12
23h	33
00h	0
01h	5
02h	0
03h	0
04h	12
05h	8
06h	43
07h	5
08h	0
09h	0
10h	1133
11h	749
12h	86
13h	0
14h	5
15h	7

#	Destination	Hits
1	172.32.250.20	749
2	131.196.87.216	69
3	10.1.1.96	49
4	192.168.1.30	37
5	187.123.93.192	25
6	189.71.197.252	24
7	191.19.55.153	24
8	179.254.160.196	21
9	189.34.216.61	19
10	201.34.70.97	18

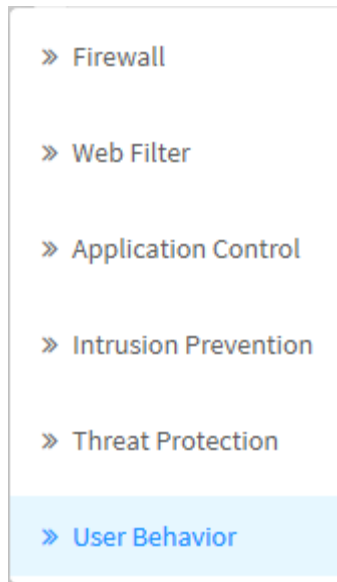
Ao passar o mouse por cima do gráfico, é exibido um resumo dos resultados dentro do período selecionado, conforme demonstrado na imagem abaixo:



Threat Protection – Top Destination - Resumo

User Behavior

Para acessar os relatórios disponíveis em "User Behavior", clique no ícone "Analysis" localizado na lateral esquerda, um menu *dropdown* será exibido, selecione a opção "User Behavior".



User Behavior

O relatório "User Behavior" é um resumo do comportamento de determinado usuário de um dispositivo, dentro de um período de tempo específico. Os relatórios dispostos são um resumo das informações já anteriormente citadas, porém sendo aplicadas especificamente a esse usuário.

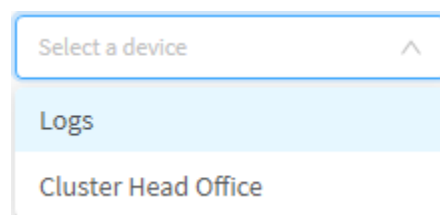
Para gerar um novo relatório, será necessário selecionar o *device* desejado, depois o usuário que se deseja analisar e por fim, determinar uma data. Feita a seleção desses três dados, os relatórios serão gerados.

Localize a caixa de seleção que está posicionada no topo direito da tela, conforme ilustrado a seguir:



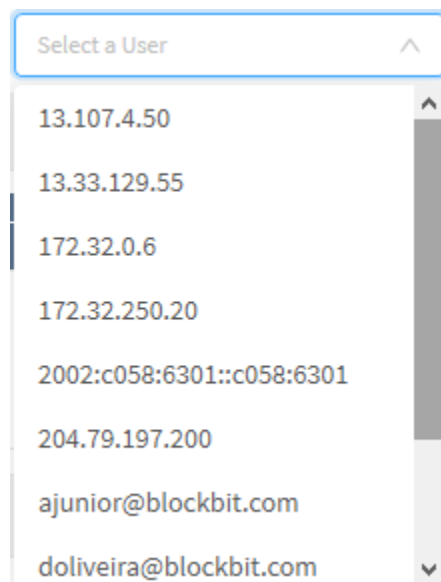
Caixa de Seleção

Na caixa de seleção "Select a device" estarão listados todos os *devices* (ou grupos de *devices*) previamente cadastradas no [Device Manager](#), para criar um relatório, selecione o *device* desejado.



Selecionando Device

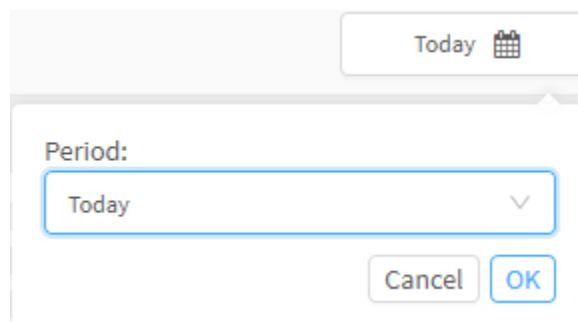
Na caixa de seleção "Select a User" estarão listados todos os usuários do *device* previamente selecionado, selecione o usuário desejado.



Selecionando o usuário.

Por fim, a caixa de seleção de datas tem como objetivo permitir uma filtragem mais precisa de resultados, as opções possíveis são:

- **By date:** Determina uma data específica;
- **By period:** Exibe resultados de uma data inicial ("Start date") até uma data final ("End date");
- **Today:** Exibe resultados especificamente para a data de hoje;
- **Yesterday:** Exibe resultados especificamente para ontem;
- **Last 7 days:** Filtra especificamente os resultados dos últimos 7 dias;
- **Last 30 days:** Filtra especificamente os resultados dos últimos 30 dias;
- **This month:** Exibe os resultados deste mês;
- **Last month:** Exibe os resultados do último mês.



Seleção de Data

Selecione a data desejada e clique em **Ok** [];

A maioria dos gráficos desta aba possui um menu de navegação e uma barra de busca.

O menu de navegação possui os seguintes botões:

- []: Serve para dar um zoom;
- []: Tem como função remover o zoom;
- []: Serve para fazer um zoom de seleção;
- []: Serve para mover o gráfico;

- []: Reseta o gráfico para a posição inicial;
- []: Permitir baixar este diagrama no formato *svg*, *png* ou *csv*.

A barra de busca permite pesquisar um item específico e modificar os diagramas de acordo com os resultados da pesquisa.

Para efetuar uma pesquisa, digite um termo na barra de busca e clique no **botão de busca** [].

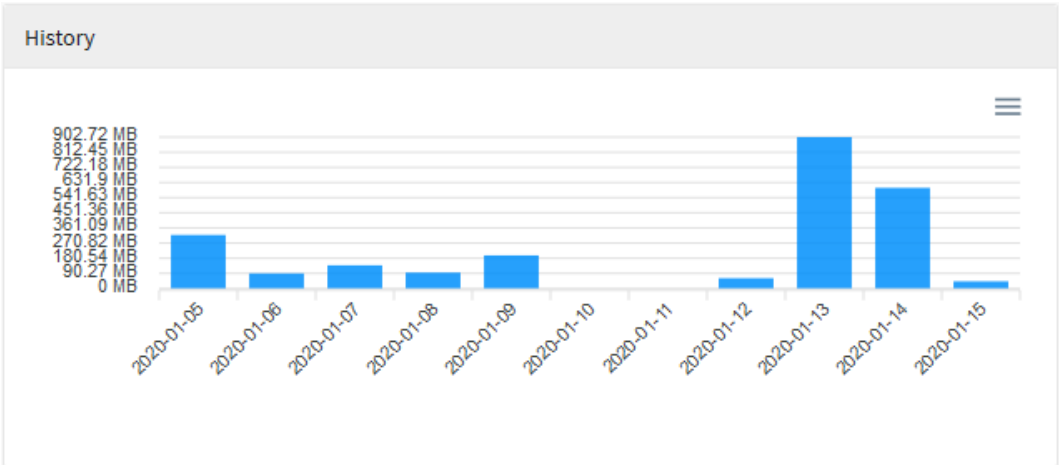
A seguir, analisaremos cada um desses relatórios em detalhe:

- [History](#);
- [Analysis Panel](#);
- [Geolocation Information](#).

User Behavior - History

Em "History" um gráfico de barras verticais é exibido demonstrando o consumo de tráfego em *Megabytes* em relação com os dias pré-selecionados, a flecha no meio do gráfico representa a média de consumo dos usuários em geral. Ao passar o mouse por cima de uma das colunas do gráfico é exibido a quantia exata de tráfego em *Megabytes* para cada dia.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta [página](#).



User Behavior - History

User Behavior - Analysis Panel

Em "*Analysis Panel*" temos um resumo de várias informações citadas nos relatórios previamente analisados, porém desta vez, aplicados especificamente ao usuário em questão.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta [página](#).

Network Traffic

Total Traffic

 2.37 GB

Top Services



#	Services	Traffic
1	https	1.08 GB
2	admin	548.79 MB
3	ssh	548.9 MB
4	http	4.06 MB
5	rdesktop	221.56 MB

Top Source



#	Source	Traffic
1	 172.32.250.20	48.74 KB
2	 172.16.13.246	123 Bytes
3	 172.16.102.130	81 Bytes
4	 192.168.254.252	43 Bytes
5	 172.16.12.27	30 Bytes

Top Destination



#	Destination	Hits
1	 172.16.13.245	2.916
2	 172.16.13.246	2.502
3	 172.16.12.171	1.063
4	 172.31.0.50	558
5	 172.16.13.57	485

Policy Usage

Policy Tags

w SSL

Top Profiles



#	Policies	Hits
1	Default (Allow) (Wifi)	24.647
2	Default (Allow) (Wifi) (Copy)	12.246
3	SMB	5.412
4	FORWARD LOCAL	3.962
5	Content Filtering (Wifi)	3.138

Application Usage

Total Application

 1.74 KB

Top Applications



#	Applications	Hits
1	CDN - Content Delivery Network	1.043
2	Microsoft Update	547
3	HTTP	50
4	Google API SSL	48
5	MSN	18

Web Usage

Total Traffic

 0

Allowed Sites

 0

Denied Sites

 0

Top Categories



#	Categories	Hits
1	Information Technology	1,628
2	Search Engines and Portals	763
3	Freeware and Software Download	527
4	Business and Economy	145
5	Web Hosting	91

Top Destination



#	Ip	Hits
1	2.23.98.145	476
2	201.0.217.42	449
3	13.107.4.50	273
4	52.114.142.2	117
5	191.252.51.215	111

THREAT PROTECTION

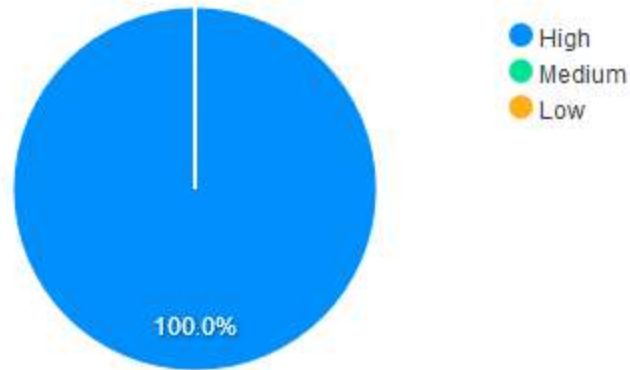
Total Threats

 1,198

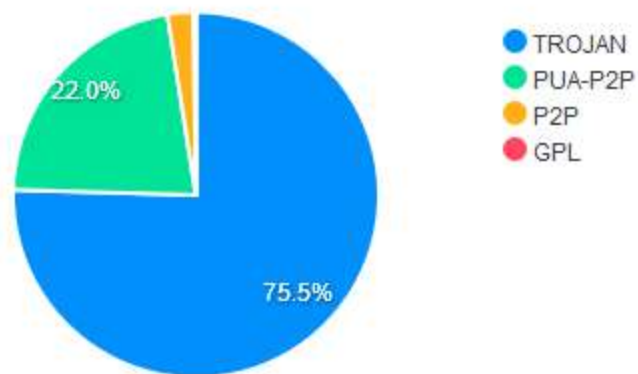
Total Malwares

0

Impacts



Malicious IP Classification



Top Threats

#	Threats	Hits
1	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 1)	308
2	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 5)	298
3	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 4)	275

4	PUA-P2P BitTorrent transfer	176
5	PUA-P2P Bittorrent uTP peer request	88

Top Malwares



#	Malwares	Hits



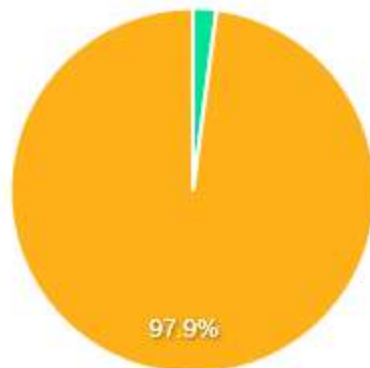
No Data

INTRUSION PREVENTION

Total Alerts

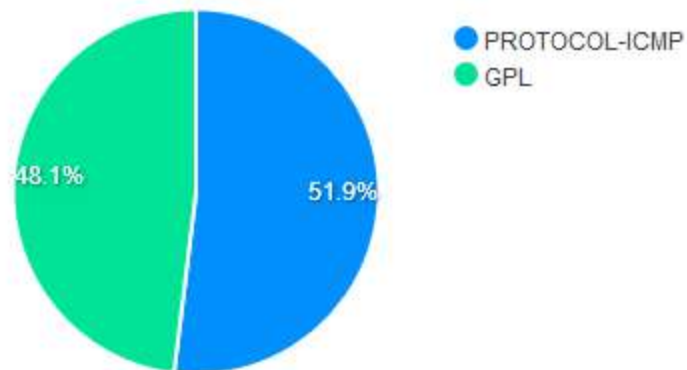
100,666

Impacts



- High
- Medium
- Low

Intrusion Protection



Top Alerts

#	Alerts	Hits
1	GPL ICMP_INFO Destination Unreachable Port Unreachable	37.678
2	PROTOCOL-ICMP destination unreachable port unreachable packet detected	37.659
3	GPL ICMP_INFO Destination Unreachable Host Unreachable	8.511
4	PROTOCOL-ICMP Destination Unreachable Host Unreachable	8.511
5	GPL ICMP_INFO PING	2.081

User Behavior - Analysis Panel

User Behavior - Analysis Panel - Network Traffic

Abaixo de "Network Traffic" temos:

"Total Traffic", exibindo o total de tráfego do usuário em *Gigabytes*, em "Top Services" é exibida uma listagem com os 10 serviços mais utilizados pelo usuário em questão, "Top source" demonstra as maiores fontes de acesso do utilizador e "Top Destination" uma listagem de *IPs* dos destinos mais acessados pelo usuário.

Network Traffic

Total Traffic

 2.37 GB

Top Services



#	Services	Traffic
1	https	1.08 GB
2	admin	548.79 MB
3	ssh	548.9 MB
4	http	4.06 MB
5	rdesktop	221.56 MB

Top Source



#	Source	Traffic
1	 172.32.250.20	48.74 KB
2	 172.16.13.246	123 Bytes
3	 172.16.102.130	81 Bytes
4	 192.168.254.252	43 Bytes
5	 172.16.12.27	30 Bytes

Top Destination			
#	Destination	Hits	
1	☐ 172.16.13.245	2.916	
2	☐ 172.16.13.246	2.502	
3	☐ 172.16.12.171	1.063	
4	☐ 172.31.0.50	558	
5	☐ 172.16.13.57	485	

User Behavior - Analysis Panel - Network Traffic

User Behavior - Analysis Panel - Policy Usage

Em "Policy Usage" temos:

"Policy Tags" que demonstra quais as Tags de política que foram mais aplicadas a esse usuário, em "Top Policies" temos as políticas mais aplicadas a esse usuário em específico.

Policy Usage

Policy Tags

w

SSL

Top Profiles

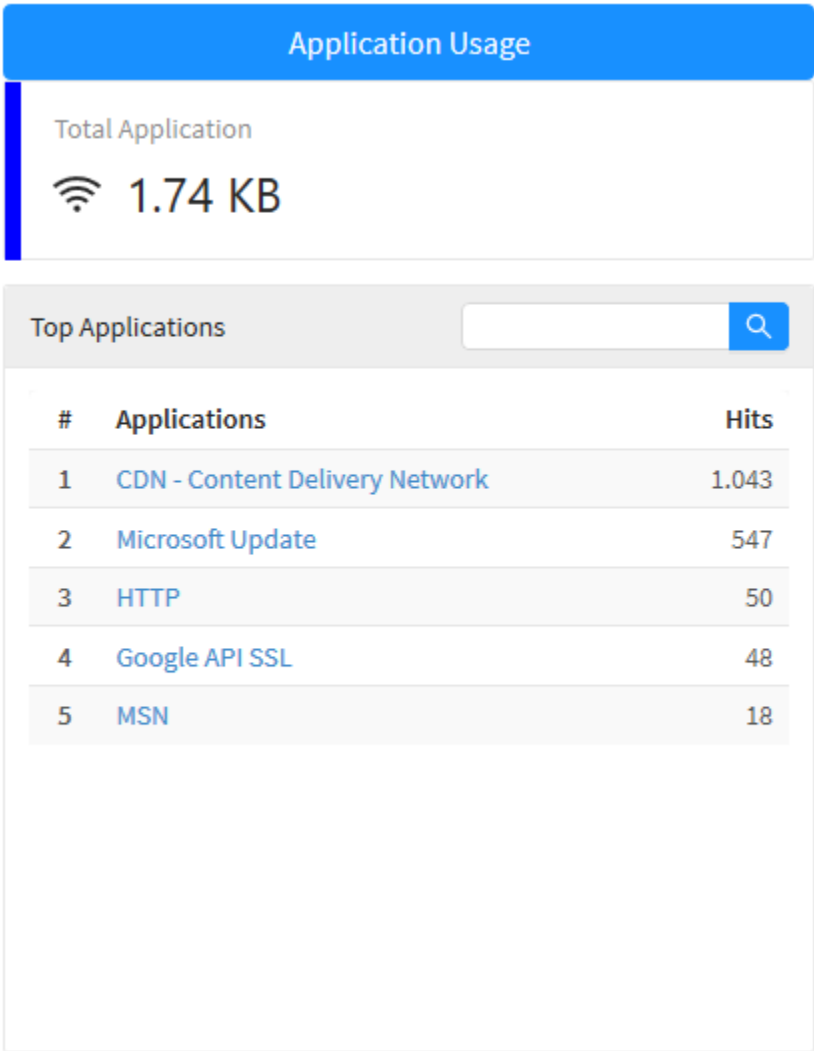
#	Policies	Hits
1	Default (Allow) (Wifi)	24.647
2	Default (Allow) (Wifi) (Copy)	12.246
3	SMB	5.412
4	FORWARD LOCAL	3.962
5	Content Filtering (Wifi)	3.138

Analysis Panel - Policy Usage

User Behavior - Analysis Panel - Application Usage

Em "Application Usage" temos:

"Total Applications" menciona o total de aplicações utilizadas pelo usuário e "Total Application" que serve para demonstrar as aplicações mais utilizadas pelo usuário e a quantia de acessos efetuados a estas mesmas.



Analysis Panel - Application Usage

User Behavior - Analysis Panel - Web Usage

Em "*Web Usage*" temos:

"*Total Traffic*" demonstrando um total do tráfego de rede do usuário, "*Sites Allowed*" mostrando o total de acessos a sites permitidos efetuados pelo usuário, "*Sites Denied*" mostrando o total de acessos a sites recusados efetuados pelo usuário, "*Top Categories*" uma lista de acessos do usuário por categoria e por fim, em "*Top destination*" uma lista de acessos do usuário por destino exibindo o *IP* e quantia de acessos a esse mesmo.

Web Usage

Total Traffic

 0

Allowed Sites

 0

Denied Sites

 0

Top Categories



#	Categories	Hits
1	Information Technology	1,628
2	Search Engines and Portals	763
3	Freeware and Software Download	527
4	Business and Economy	145
5	Web Hosting	91

Top Destination



#	Ip	Hits
1	2.23.98.145	476
2	201.0.217.42	449
3	13.107.4.50	273
4	52.111.140.2	117

4	52.114.142.2	111
5	191.252.51.215	111

Analysis Panel - Web Usage

User Behavior - Analysis Panel - Threat Protection

Em "*Threat Protection*" temos:

"*Total Threats*" exibindo o total de ameaças, "*Total Malwares*" exibe o número total de *malwares* detectados nesse usuário, no gráfico "*Impacts*" são exibidos os níveis de impactos das ameaças previamente citadas, "*Malicious IP Classification*" exibe um gráfico demonstrando um resumo da classificação dos *IPs* mal-intencionados acessados pelo usuário, na listagem "*Top Threats*" são exibidas as 5 ameaças mais recorrentes a esse usuário e a quantia de acessos feitos e em "*Top Malware*" é exibida uma lista com os 5 *malwares* mais detectados no usuário em questão.

THREAT PROTECTION

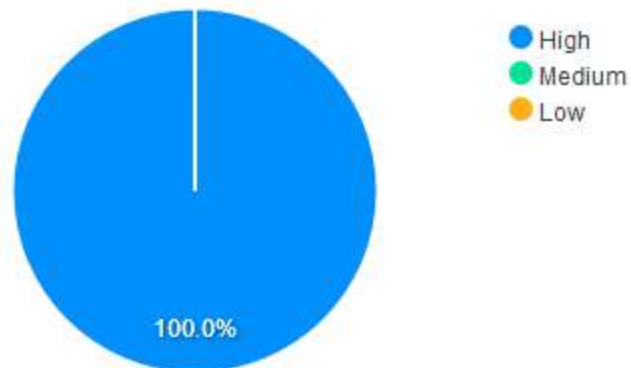
Total Threats

📶 1,198

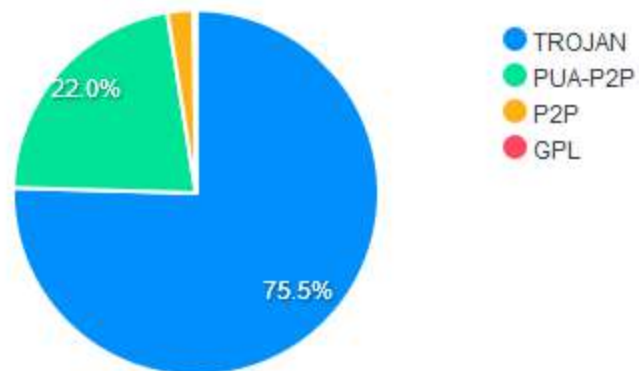
Total Malwares

📶 0

Impacts



Malicious IP Classification



Top Threats



#	Threats	Hits
	TROJAN Possible	

1	Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 1)	308
2	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 5)	298
3	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 4)	275
4	PUA-P2P BitTorrent transfer	176
5	PUA-P2P Bittorrent uTP peer request	88

Top Malwares

#	Malwares	Hits
 No Data		

Analysis Panel - Threat Protection

User Behavior - Analysis Panel - Intrusion Prevention

Em "*Intrusion Prevention*" temos:

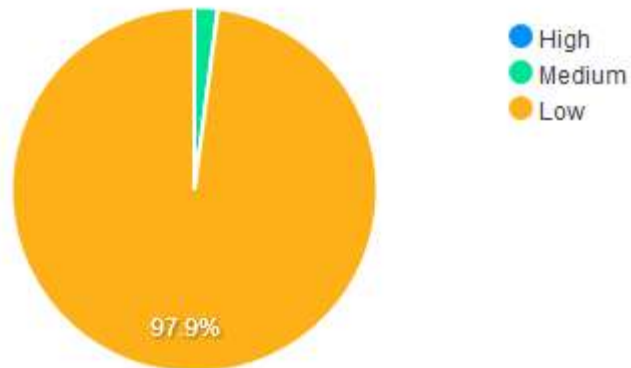
"*Total Alerts*" exibindo o total de alertas referentes a esse usuário, em "*Impacts*" temos os níveis de impacto dos alertas previamente citados, "*Intrusion Protection*" exibe um gráfico de rosca onde é possível de se ver os tipos de invasão detectados pelo sistema e por fim, em "*Top Alerts*" temos uma listagem dos 5 alertas referentes a esse usuário e quantas vezes eles ocorreram.

INTRUSION PREVENTION

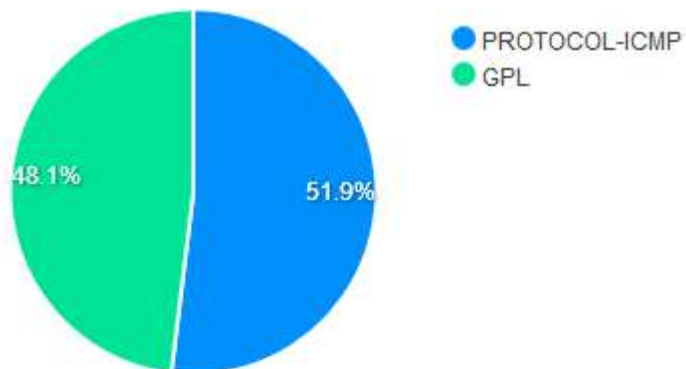
Total Alerts

📶 100,666

Impacts



Intrusion Protection



Top Alerts

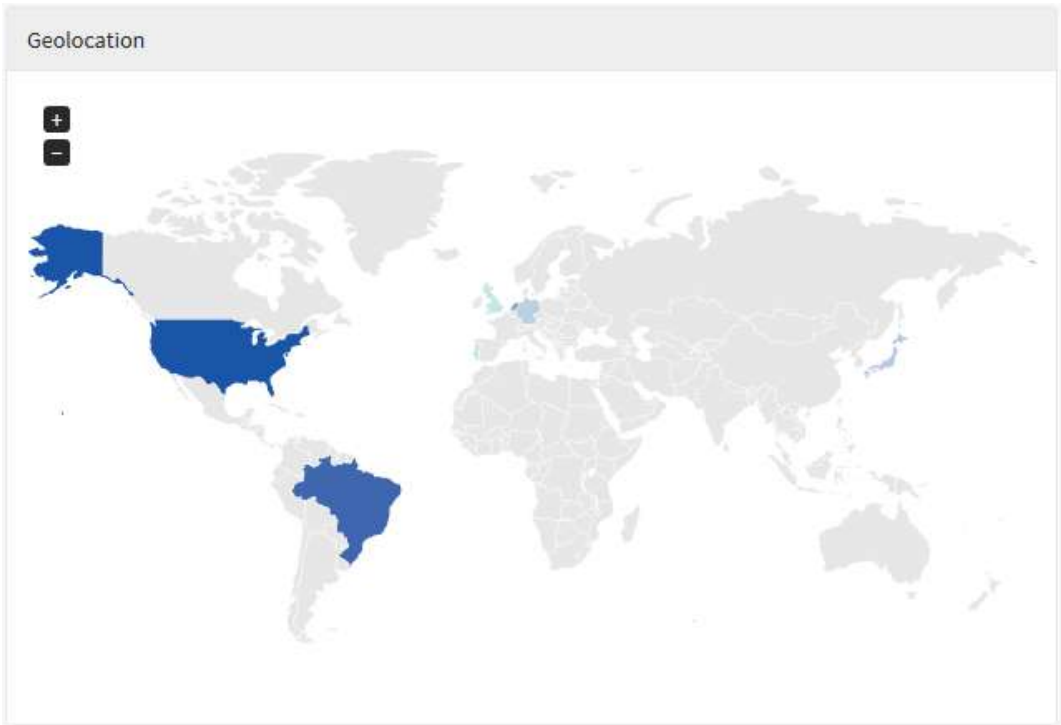
#	Alerts	Hits
1	GPL ICMP_INFO Destination Unreachable Port Unreachable	37,678
2	PROTOCOL-ICMP destination unreachable port unreachable packet detected	37,659
3	GPL ICMP_INFO Destination Unreachable Port Unreachable	8,511

Unreachable Host Unreachable		
4	PROTOCOL-ICMP Destination Unreachable Host Unreachable	8.511
5	GPL ICMP_INFO PING	2.081

Analysis Panel - Intrusion Prevention

User Behavior - Geolocation Information

Em "Hits by Geolocation" é exibido o destino das conexões desse usuário em específico, o mapa global demonstra através de uma legenda colorida a quantia de acessos feitos pelos usuários para cada país.



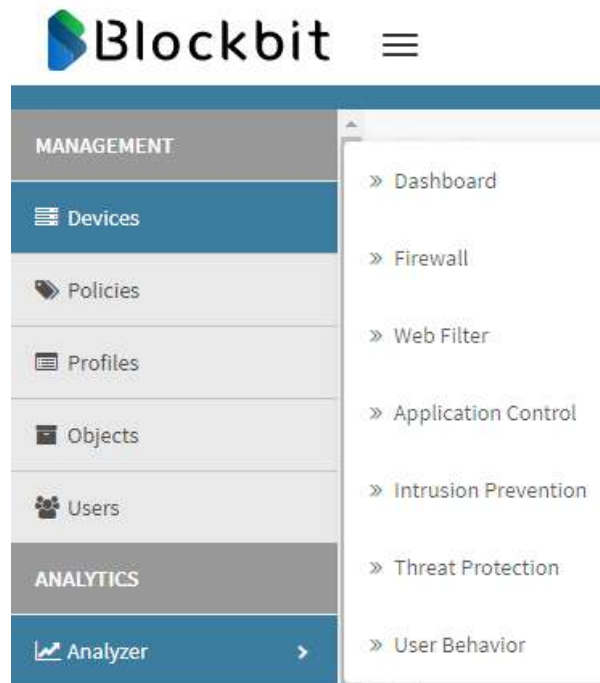
User Behavior - Geolocation

Ao passar o mouse por cima dos países um número total de acessos é exibido, ao fazer o mesmo com a legenda é possível visualizar uma média, além disso, o país referente a esse valor é destacado no mapa.



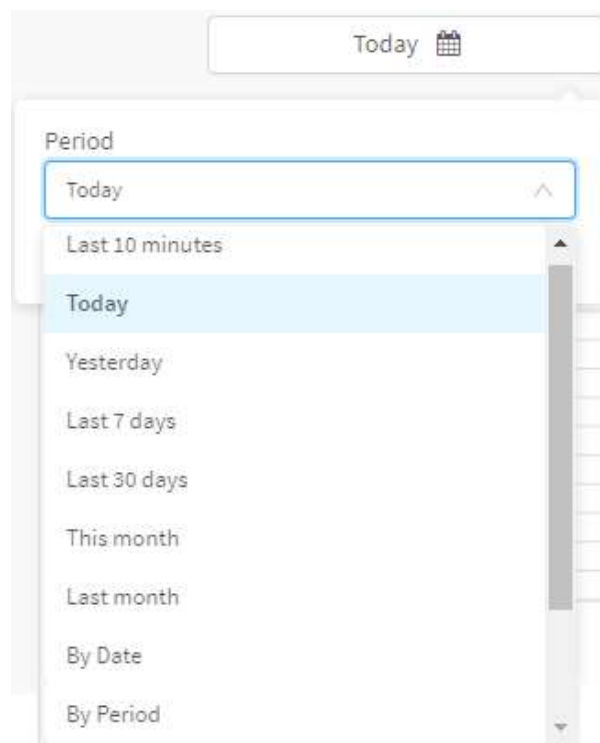
Dashboard

O Dashboard exibe as informações consolidadas dos logs gerados por um Device ou grupo de Devices no GSM. As seções exibidas são: Firewall, Web Filter, Application Control, Intrusion Prevention, Threat Protection e User Behavior.



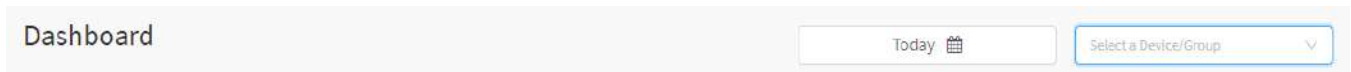
Analyzer menu - Dashboard

Para visualizar estas informações no Dashboard temos que, antes de tudo, selecionar o período de tempo a ser coberto e um Device (ou todos), para tê-los apresentados na interface ao usuário:



Dashboard - Time period selection

1. Esta opção permite filtrar pelos seguintes períodos de tempo:
 - a. Hoje
 - b. Últimos 10 minutos;
 - c. Ontem;
 - d. Últimos 7 dias;
 - e. Últimos 30 dias;
 - f. Este Mês;
 - g. Último Mês;
 - h. Por Data;
 - i. Por Período;



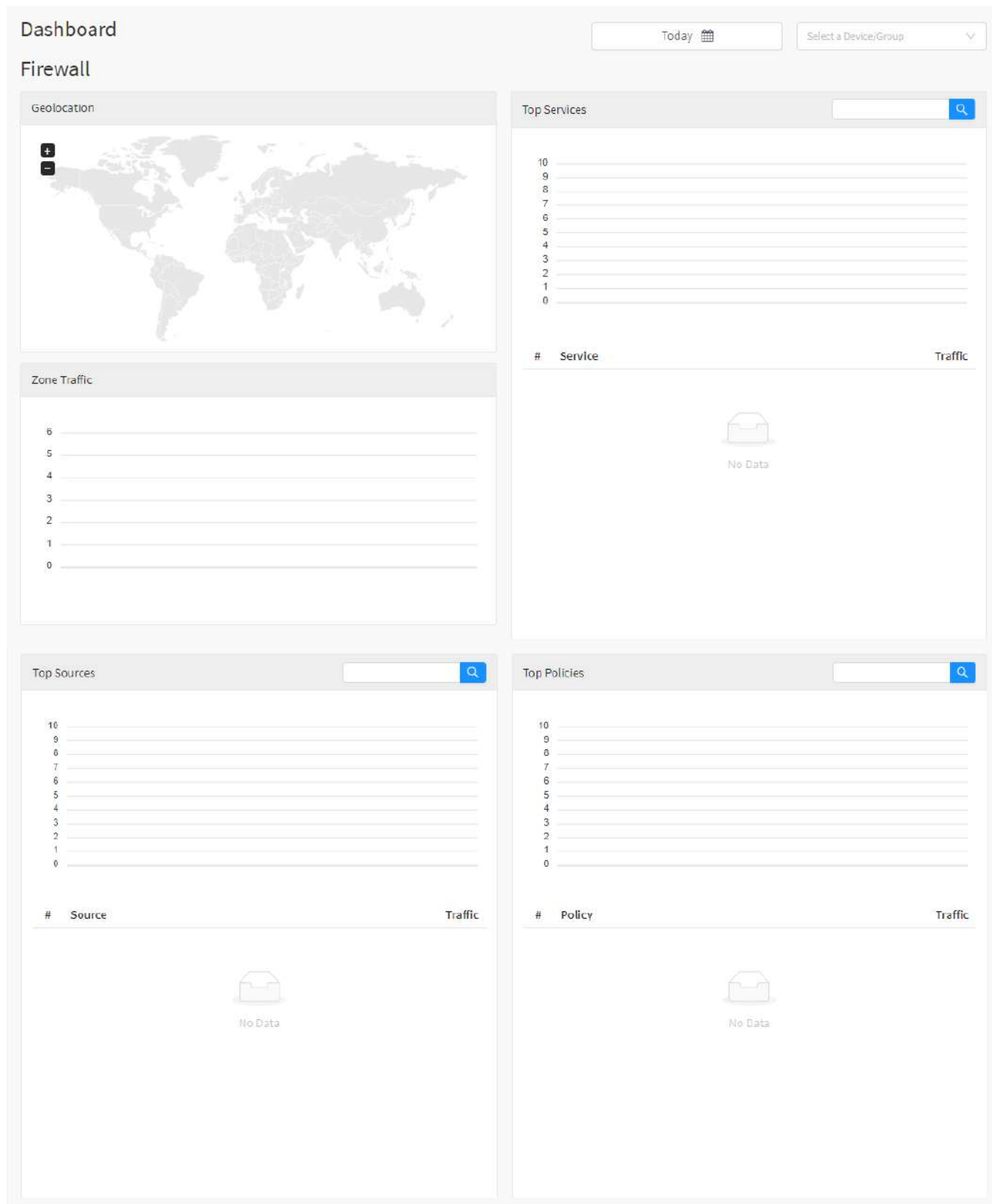
Dashboard - Device group selection

A seguir veremos mais seções exibidas em Dashboard.

Firewall

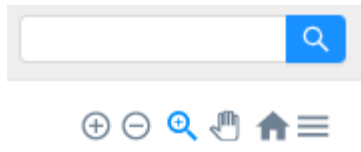
Em Firewall, são exibidos os dados dos seguintes Logs:

- Geolocalização
- Top 10 Serviços
- Top 10 Tráfego de zona
- Top 10 Origens
- Top 10 Políticas



Firewall - Dashboard

Ao seleccionar o Device, ou grupo de Devices, as seguintes ferramentas ficarão disponíveis para a exploração das informações exibidas:



Dashboard - Exploring tools

Barra de Pesquisa [] : Permite o filtro de itens específicos, pesquisados por palavras-chave.

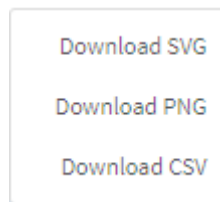
Zoom In/Out [ ] : Botões de aumento e redução de zoom respectivamente.

Zoom [] : Permite a seleção do modo zoom.

Arrastar [] : Seleciona para mover o visualizador e acessar os dados exibidos.

Home [] : Zera o zoom e reseta a posição do visualizador.

Download [] : Permite realizar o download deste relatório nos formatos SVG, PNG e CSV.



Download options

Geolocation

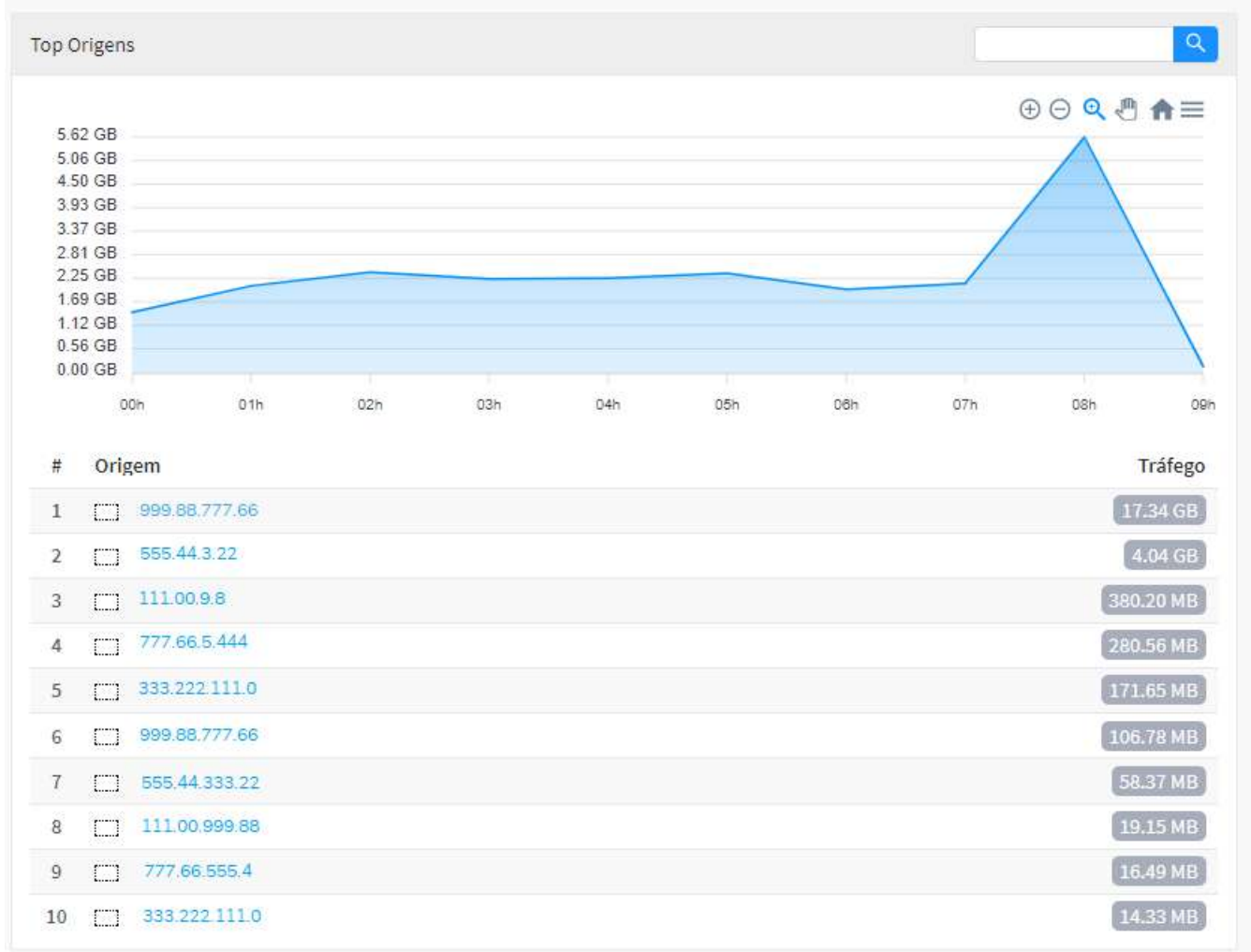
Verifica todos os IPs e exibe o desenho da Geolocalização, somando os IPs dos Devices (ou todos) em tempo real. Basta passar o mouse pelas regiões em azul para verificar os dados:

Top 10 Origens (Firewall)

O serviço realiza a validação de todos os logs, faz a soma dos logs por IP, e exibe o Top 10, sendo eles do mesmo Device ou não.

Ao clicar sobre as informações, o usuário é redirecionado para a tela dos Logs, que contém maiores detalhes.

O tráfego total utilizado pelo IP também é informado.

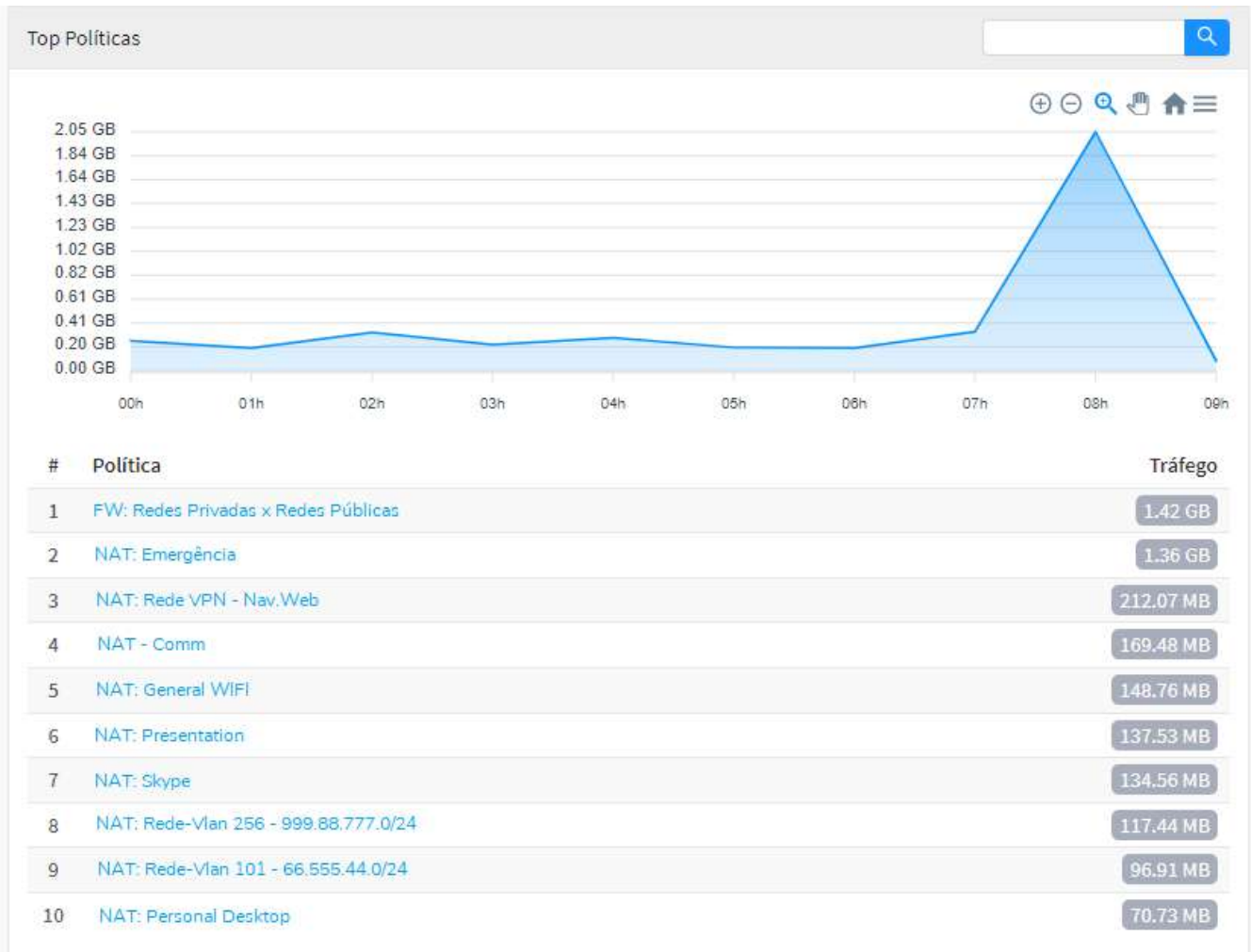


Top 10 Serviços (Firewall)

O serviço realiza a validação de todos os logs, faz a soma dos logs por serviço, e exibe o Top 10, sendo eles do mesmo Device ou não. Também é possível acessar a tela dos Logs detalhados ao clicar sobre as informações e exibe o tráfego total utilizado no serviço:

Top 10 Políticas (Firewall)

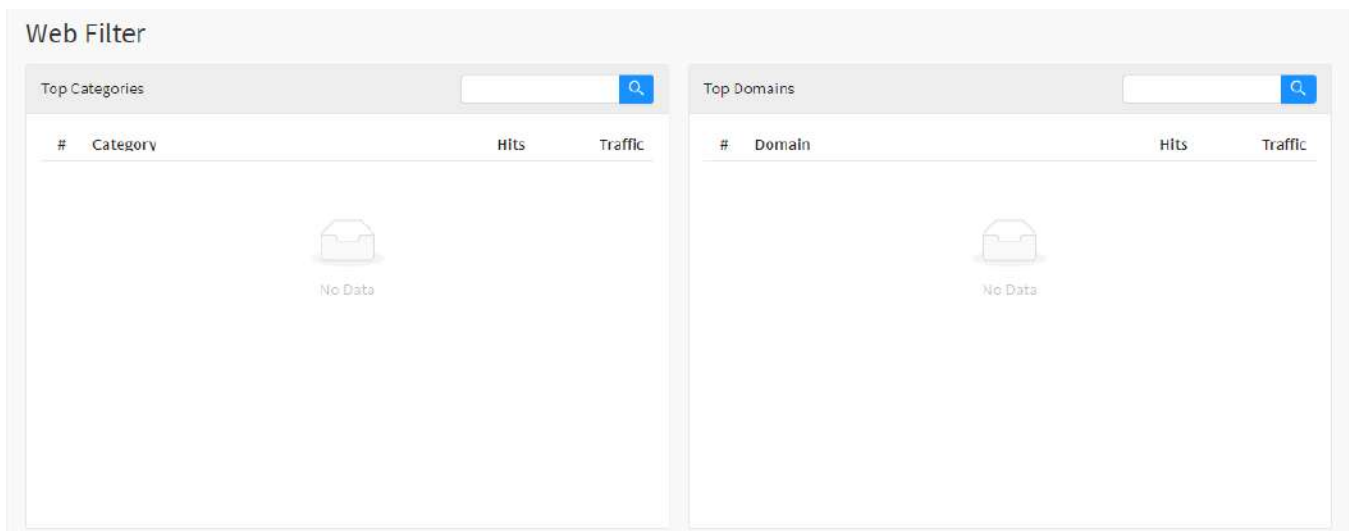
O serviço realiza a validação de todos os logs, faz a soma daqueles utilizados nas Políticas do Device, e exibe o Top 10. O serviço permite ao usuário o redirecionamento para a tela dos Logs detalhados (basta clicar sobre os dados) e também exibe o tráfego total utilizado pela Política, conforme demonstrado na imagem abaixo:



Web Filter

Em Web Filter, são exibidos os dados dos seguintes Logs:

- Top 10 Domínios
- Top 10 Categorias



Web Filter - Dashboard

Top 10 Domínios (Web Filter)

O serviço valida todos os logs, somando-os pelo tipo de Domínio, e exibe o Top 10, sendo eles do mesmo Device (ou não). O serviço permite o redirecionamento para a tela dos Logs detalhados, com um clique sobre as informações. Exibe também a quantidade de Hits do domínio exibido no Top 10, bem como o tráfego total utilizado pelo Domínio;

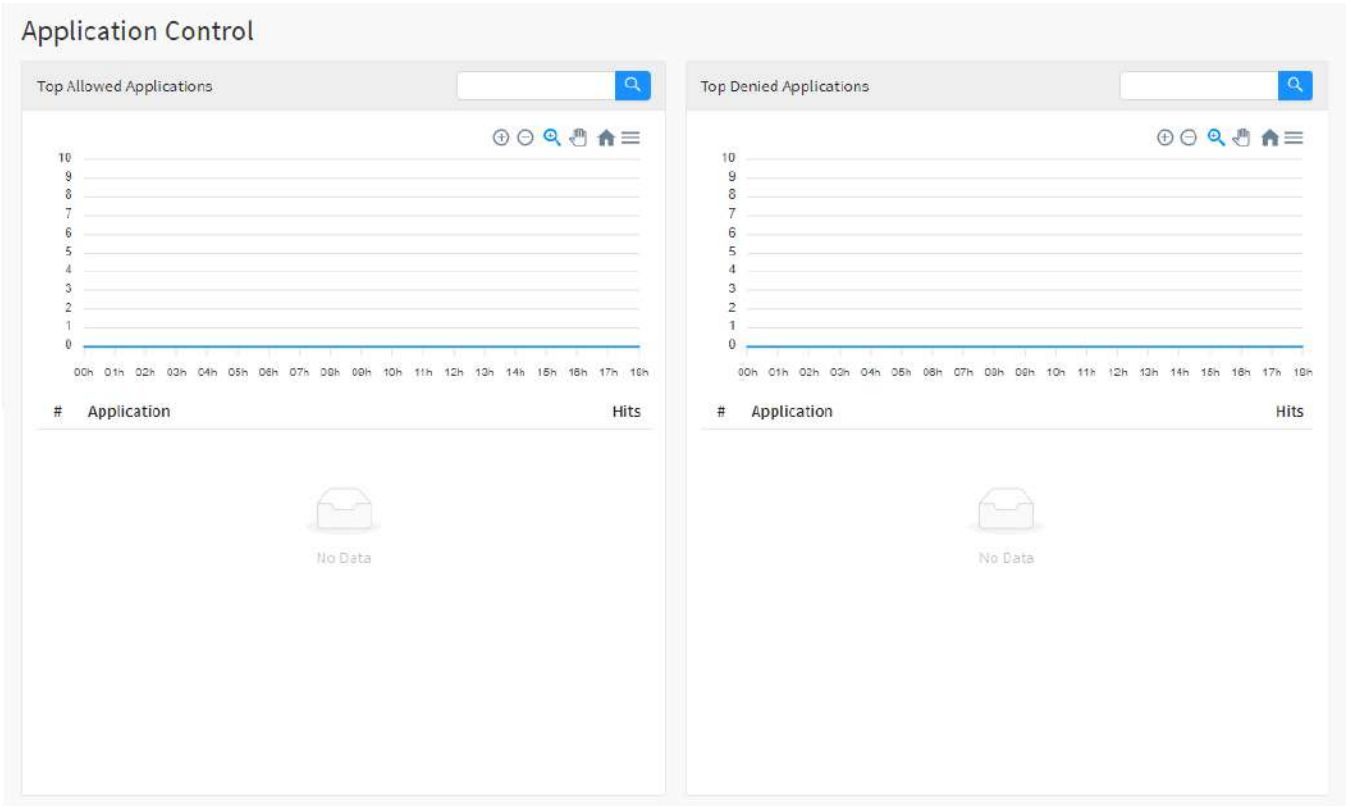
Top 10 Categorias (Web Filter)

O serviço realiza a validação de todos os logs, faz a soma dos logs das Categorias, e exibe o Top 10, sendo eles do mesmo Device (ou não). O serviço permite ao usuário ser redirecionado para a tela dos Logs detalhados, ao clicar sobre as informações. Exibe a quantidade Hits da categoria exibida no Top 10 e a quantidade de tráfego utilizado pela Categoria.

Application Control

Em Application Control são exibidos os dados dos seguintes Logs:

- Top 10 Aplicações Permitidas
- Top 10 Aplicações Negadas



Dashboard - Application Control

Top 10 Aplicações Permitidas (Application Control)

O serviço realiza a validação de todos os logs, faz a soma dos logs das Aplicações, e exibe o Top 10, sendo eles do mesmo Device (ou não). O serviço permite ao usuário ser redirecionado para a tela dos Logs detalhados ao clicar sobre as informações, exibe também a quantidade de Hits da aplicação exibida no Top 10:

Top 10 Aplicações Negadas (Application Control)

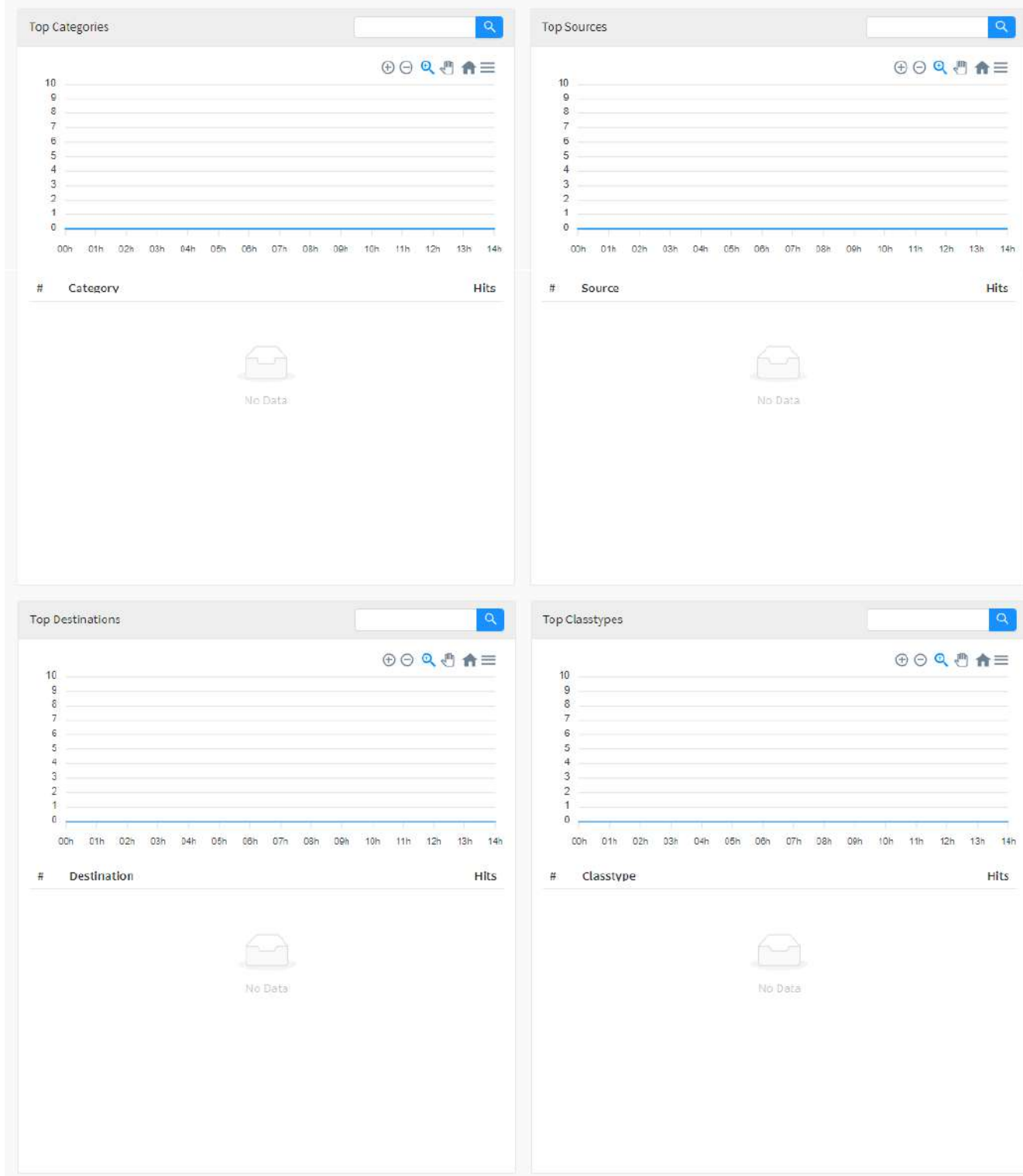
O serviço realiza a validação de todos os logs, faz a soma dos logs das Aplicações e exibe o Top 10. O serviço permite ao usuário ser redirecionada para a tela dos Logs detalhados, da mesma maneira que os anteriores. Exibe a quantidade de Hits da aplicação no Top 10:

Intrusion Prevention

Em Intrusion Prevention são exibidas as informações dos seguintes Logs:

- Top 10 Categorias
- Top 10 Origens
- Top 10 Destinos
- Top 10 Tipos de classe

Intrusion Prevention



Top 10 Categorias (Intrusion Prevention)

O serviço realiza a validação de todos os logs, faz a soma dos logs das categorias e exibe o Top 10 do mesmo Device (ou não). O serviço permite ao usuário ser redirecionada para a tela dos Logs detalhados ao clicar sobre as informações. Exibe também a quantidade de Hits da categoria no Top 10:

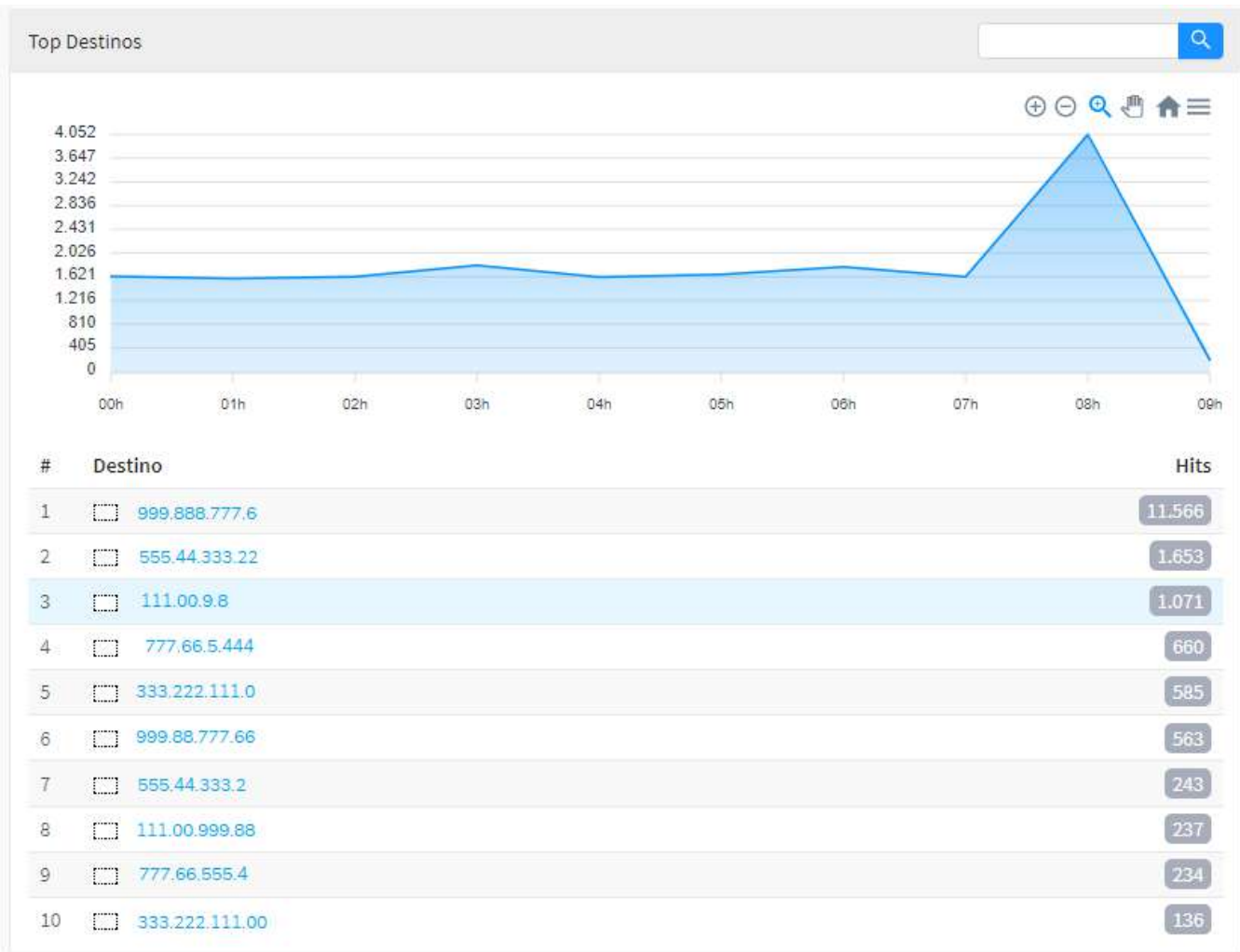
Top 10 Origens (Intrusion Prevention)

O serviço realiza a validação de todos os logs, faz a soma dos logs das Origens, e exibe o Top 10, sendo eles do mesmo Device ou não. O serviço também permite ao usuário redirecionamento para a tela dos Logs detalhados, bem como exibe a quantidade de Hits do IP de origem no Top 10:



Top 10 Destinos (Intrusion Prevention)

O serviço realiza a validação de todos os logs, faz a soma dos logs dos IPs de Destino, e exibe o Top 10. O serviço permite ao usuário o redirecionamento para a tela dos Logs detalhados e exibe a quantidade de Hits dos IPs de Destino exibida no Top 10:



Top 10 Tipos de classe (Intrusion Prevention)

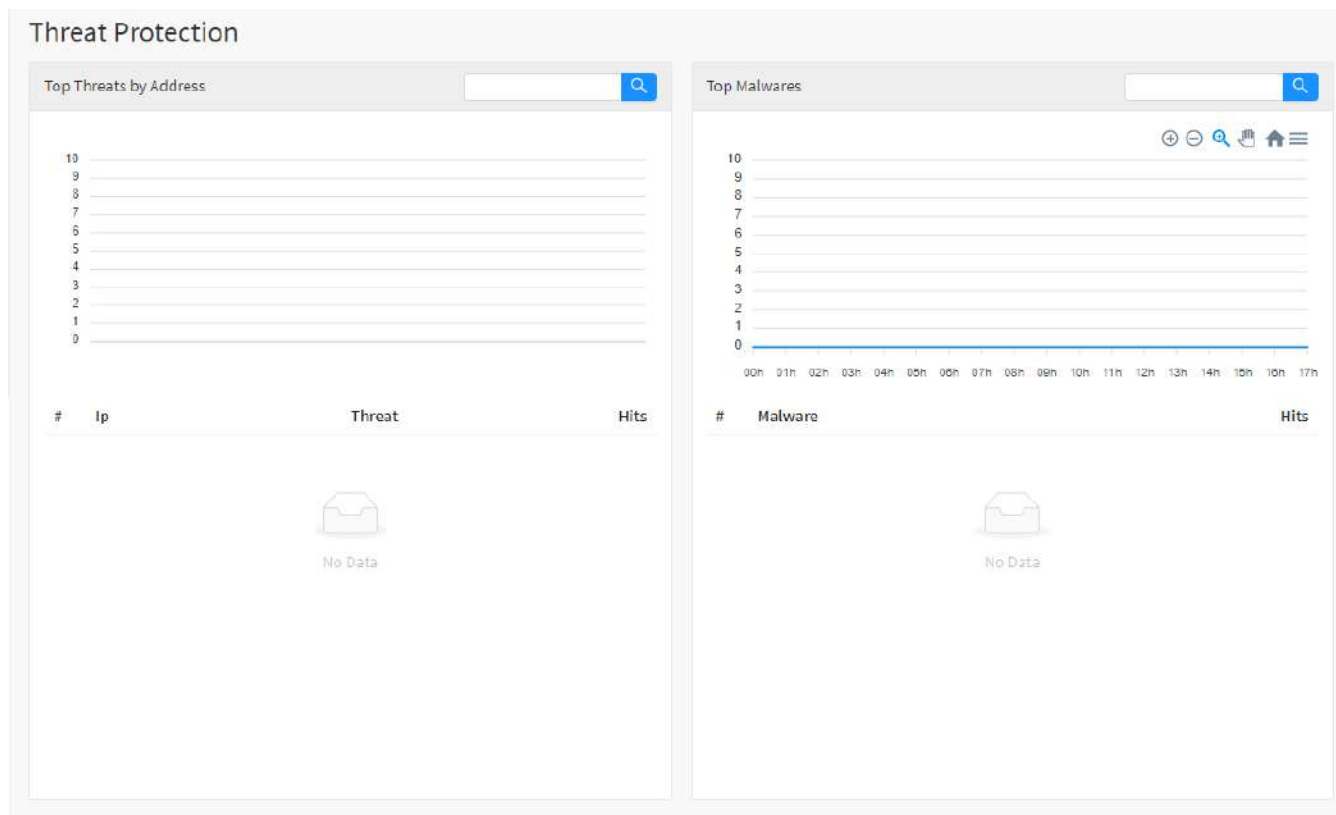
O serviço realiza a validação de todos os logs, faz a soma dos logs dos tipos de malware , e exibe o Top 10. O serviço permite ao usuário o redirecionamento para a tela dos Logs detalhados e exibe a quantidade de Hits exibida no Top 10:



Threat Protection

Em Threat Protection, são apresentados os dados das seguintes Logs:

- Top 10 Ameaças por Endereço
- Top 10 Malwares



Top 10 Ameaças por Endereço (Threat Protection)

O serviço realiza a validação de todos os logs, faz a soma das ameaças e exibe o Top 10, sendo eles do mesmo Device ou não.

O serviço permite ao usuário clicar sobre a ameaça, e ser redirecionado para a tela dos Logs detalhados. Exibe a quantidade de Hits das ameaçadas exibidas no Top 10

Top 10 Malwares (Threat Protection)

O serviço realiza a validação de todos os logs, faz a soma dos Malwares e exibe o Top 10, sendo eles do mesmo Device ou não.

O serviço permite ao usuário clicar sobre o Malware, e ser redirecionado para a tela dos Logs detalhados. Exibe a quantidade de Hits dos malwares no Top 10.

Reports

A função desta opção é administrar a criação automática e periódica de relatórios personalizados, permitindo seleção de característica específica dos *devs* selecionados. Suporta também a distribuição automática de relatórios por e-mail através de agenda pré-determinada;

Para acessar e administrar a criação automática de relatórios, clique no ícone "Reports" localizado na lateral esquerda:



Analytics - Reports

A tela de *reports* será exibida.

Reports

3 records

☐	Name	Scheduled	Owner	Period	Status	Actions
☐	Store 1 report Network traffic analysis on Store 1	09/12/2019 18:37:08 Created: 09/12/2019 18:36:35	admin	from: December 09, 2019 to: December 09, 2019	Pending	
☐	Intrusion Report Intrusion report on the stores	09/12/2019 18:33:19 Created: 09/12/2019 18:35:14	admin	from: December 06, 2019 to: December 08, 2019	Download Visualize	
☐	Store 1 report Network traffic analysis on Store 1	09/12/2019 18:32:06 Created: 09/12/2019 18:32:17	admin	from: December 04, 2019 to: December 09, 2019	Download Visualize	

< 1 >

10 / page

Reports

A seguir analisaremos a função de cada componente desta tela.

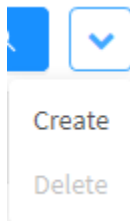
Reports - Menu de Ações

No topo direito da tela temos o menu de ações:



Reports – Botão do Menu de Ações

Ao clicar neste botão o menu abaixo é exibido:



Reports – Menu de Ações

O menu é composto das seguintes opções:

- [Create](#);
- [Delete](#).

A seguir cada opção do menu de ações será detalhada.

Reports - Menu de ações - Create

Para criar um relatório automático clique em "Create", a seguinte tela será exibida, com a aba lateral "Settings" pré-selecionada:

Aba Settings

Create Report

X

Settings

Datasets

Custom

* Name

* Description

Type

Analyzer

* Scheduled

Select date

Recurrence

Unique

* Period

Start date

End date

* Device/Logger

Select Device/Logger

☐ Send Report by Email

Cancel

Create

Reports – Create Report - Settings

A seguir analisaremos cada campo deste painel:

- **Name:** O nome do relatório. Ex.: *Store 1 report*;
- **Description:** A descrição do relatório. Ex.: *Network traffic analysis on Store 1*;
- **Type:** Este menu suspenso determina as opções que estarão disponíveis na aba "Datasets", temos as seguintes opções:
 - **Analysis:** Permite a criação dos seguintes relatórios na aba *Datasets*:
 - **Network Traffic**;
 - **Policy Usage**;
 - **Web Filter**;
 - **Application Control**;
 - **Intrusion Prevention**;

- **Threat Protection;**
- **User Behavior.**
- **Top Hits:** Gera um relatório de *Top Hits*, sendo que na aba *Datasets* é determinado a quantia de *hits* a ser amostrado e os filtros a serem utilizados;
- **Top Bytes:** Gera um relatório de *Top Bytes*, sendo que na aba *Datasets* é determinado a quantia de *bytes* a ser amostrado e os filtros a serem utilizados;
- **Log:** Permite a criação de um relatório personalizado, em *Datasets* é possível utilizar-se de *Queries* personalizadas e determinar os filtros a serem utilizados.
- **Scheduled:** Exibe a data de agendamento para quando esse relatório será executado;
- **Period:** Determina o período de quando os dados serão analisados pelo *logger* nos UTMs Ex.: Ao selecionar de 1 de setembro de 2018 a 24 de outubro de 2018, todos os dados que existirem fora desse período, não serão exibidos no "*Report*";
- **Device/Logger:** É selecionado o device de onde os dados serão analisados para gerar o relatório.
- **Send report by e-mail:** Marque esta opção [☒ **Send Report by Email**] para receber os relatórios gerados em analytics por e-mail, na periodicidade determinada para que os mesmos sejam gerados.

É importante salientar que para receber os relatórios é necessário fazer as configurações de [e-mail](#).

Aba *Datasets*

A aba "*Datasets*" determina o tipo de gráfico que será gerado, conforme mencionado anteriormente, os componentes dela são determinados pela caixa de seleção "*Type*" da aba "*Settings*".

The screenshot shows a 'Create Report' dialog box with a close button (X) in the top right corner. On the left, there is a vertical sidebar with three tabs: 'Settings', 'Datasets' (which is selected and highlighted with a blue vertical bar), and 'Custom'. The main area of the dialog is titled 'Analysis' and contains a dropdown menu with 'Network Traffic' selected. At the bottom right, there are two buttons: 'Cancel' and 'Create'.

Reports – Create Report - Datasets

Aba Custom

Na aba “Custom” é possível determinar o texto que ficará de rodapé em “Footer” e customizar o “Logo” que aparecerá no relatório.

Create Report

Settings

Datasets

Custom

Footer Text

Customize Logo



Cancel

Create

Reports – Create Report - Custom

Clique no botão **Cancel** para sair dessa janela ou clique em **Create** para agendar o relatório. Caso queira emití-lo imediatamente configure-o para ser executado na data de hoje.

Reports - Menu de ações - Delete

Através do botão “Delete” é possível deletar os *Reports* selecionados. Para deletar através do Menu de ações, siga os seguintes passos:

1. Selecione qual(is) *Report(s)* deseja deletar. Para selecionar, basta clicar com o *mouse* no *checkbox* que fica localizado ao lado do *Name*. Nos *reports* selecionados o *checkbox* mudará da cor cinza para azul []. Ex.: *Test*;

Reports

4 records

	Name	Scheduled	Owner	Period	Status	Actions
	Test test	09/12/2019 19:08:02 Created: 09/12/2019 19:08:25	admin	from: December 09, 2019 to: December 09, 2019	Pending	
	Store 1 report Network traffic analysis on Store 1	09/12/2019 18:37:08 Created: 09/12/2019 18:36:35	admin	from: December 09, 2019 to: December 09, 2019	Pending	
	Intrusion Report Intrusion report on the stores	09/12/2019 18:33:19 Created: 09/12/2019 18:35:14	admin	from: December 06, 2019 to: December 08, 2019	Pending	
	Store 1 report Network traffic analysis on Store 1	09/12/2019 18:32:06 Created: 09/12/2019 18:32:17	admin	from: December 04, 2019 to: December 09, 2019	Pending	

<

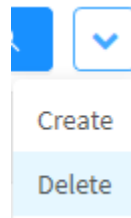
1

>

10 / page

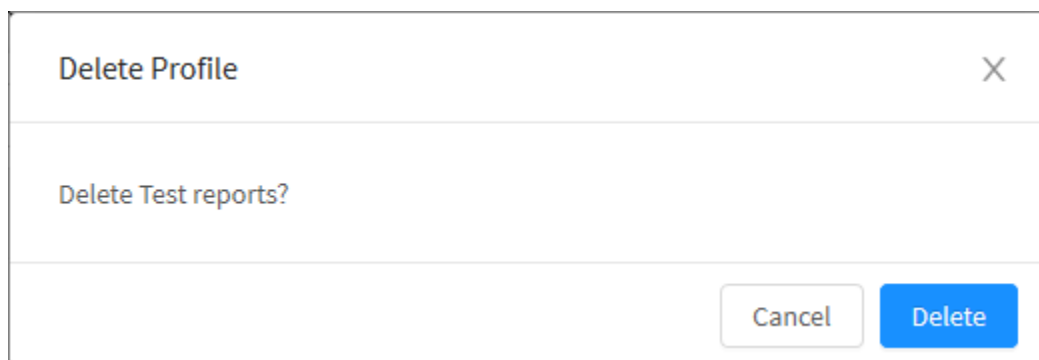
Reports – Seleção dos Reports para deletar

2. Entre no **menu de ações** [] e clique na opção “Delete”.



Reports – Delete

3. Surgirá a mensagem de notificação questionando se deseja realmente deletar os *Reports* selecionados:



The image shows a dialog box titled 'Delete Profile' with a close button (X) in the top right corner. The main text inside the dialog is 'Delete Test reports?'. At the bottom right, there are two buttons: 'Cancel' and 'Delete'.

Cancel

Delete

Caso desejar cancelar clique no botão **Cancel**[]. Para concluir, clique no botão **Delete**[].



Profile deleted successfully!

Profile deleted successfully

Após realizar esses procedimentos, os *reports* terão sido deletados com sucesso.

Reports - Colunas

A seguir explicaremos cada coluna da aba *Reports*:

Reports

3 records

☐	Name	Scheduled	Owner	Period	Status	Actions
☐	 Store 1 report Network traffic analysis on Store 1	09/12/2019 18:37:08 Created: 09/12/2019 18:36:35	admin	from: December 09, 2019 to: December 09, 2019	Pending	 
☐	 Intrusion Report Intrusion report on the stores	09/12/2019 18:33:19 Created: 09/12/2019 18:35:14	admin	from: December 06, 2019 to: December 08, 2019	Download Visualize	 
☐	 Store 1 report Network traffic analysis on Store 1	09/12/2019 18:32:06 Created: 09/12/2019 18:32:17	admin	from: December 04, 2019 to: December 09, 2019	Download Visualize	 

< 1 > 10 / page

Reports

- **Select** [☐]: Permite selecionar um *report*;
- **Name**: Exibe o nome do relatório cadastrado na opção *Create* do menu de ações. Logo abaixo do nome está a descrição cadastrada no mesmo menu;
- **Scheduled**: Exibe o agendamento para quando o relatório será executado, logo abaixo dessa data está marcada a data de quando esse processo foi criado. Suportando a geração de relatórios diários, semanais e mensais;
- **Owner**: O nome do usuário responsável por criar esse agendamento;
- **Period**: É onde está registrado o período de quando os dados serão extraídos do sistema;
- **Status**: É exibido o estado atual da produção do relatório. Nesta coluna também é possível visualizá-lo clicando no botão *Visualize* ou baixa-lo em formato PDF clicando em *Download* após o relatório ter sido gerado. Ex.: *Pending*;
- **Actions**: Botões com funções essenciais para interação com os relatórios:
 - **Botão Visualizar** []: Permite editar as configurações do *Report* adicionado na opção *Create* do menu de ações;
 - **Botão Excluir** []: Exclui o relatório selecionado.

Events

O painel *Events* tem como função principal exibir todas as ocorrências de um determinado *logger* ou grupo de *devices* próximos ao tempo real.

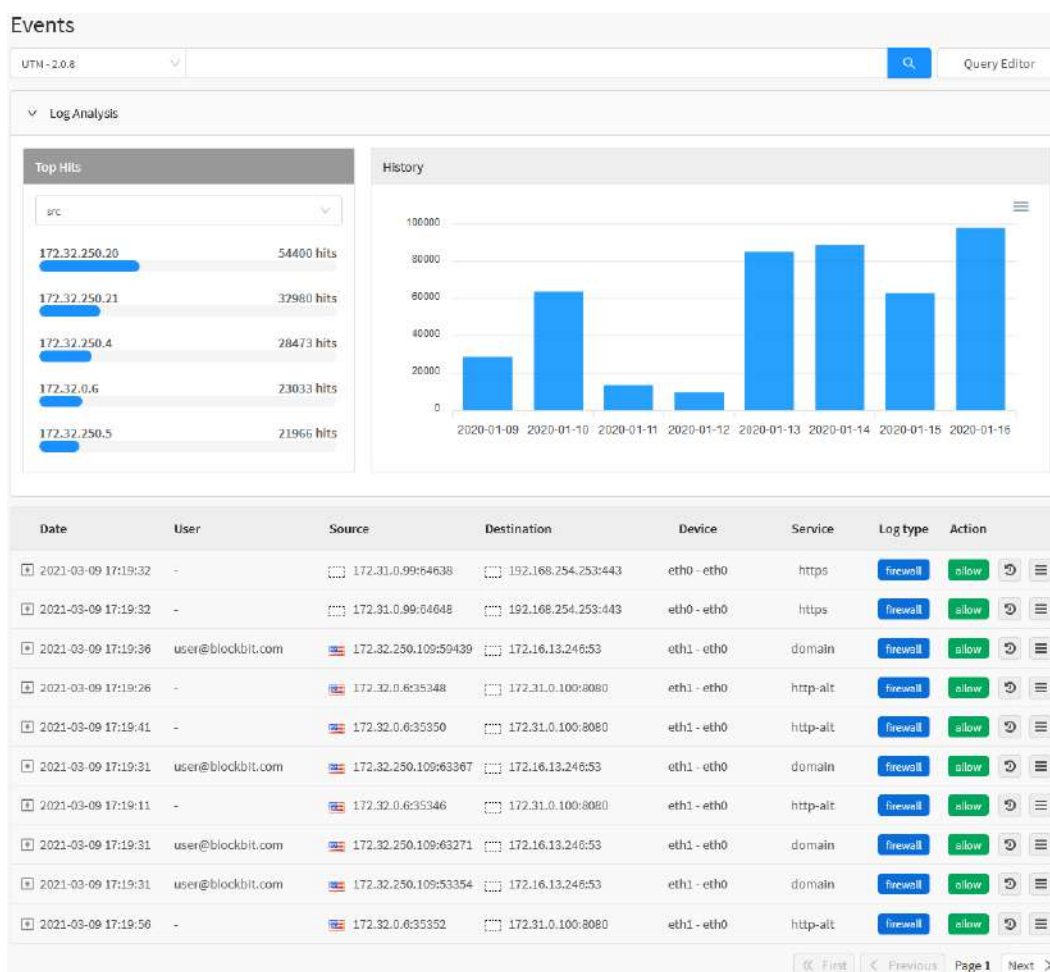
Este painel possui alguns recursos que permitem uma análise profunda mais detalhada: Através deste painel é possível efetuar uma busca de acordo com *queries* personalizadas, analisar incidentes e eventualidades específicas, permitindo uma administração muito mais precisa e eficiente.

Para acessar a tela de eventos, clique no ícone “Events” localizado na lateral esquerda:



Analytics - Events

Surgirá a Tela de “Events”. Ela é composta pelos quadros internos “Top Hits”, “History” e “Log Events”. Além disso, no topo direito da tela está localizada a barra de busca e o “query editor”.



Events

Assim que se efetua o acesso a “Events” uma caixa de seleção é apresentada no canto direito da tela, para visualizar os Eventos é necessário selecionar o *logger* ou grupo de *devices* desejado nesse painel de seleção. Conforme demonstrado abaixo:

Blockbit



Events - Seleção do logger

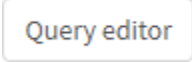
Após selecionar a opção desejada, os eventos relevantes serão automaticamente exibidos.

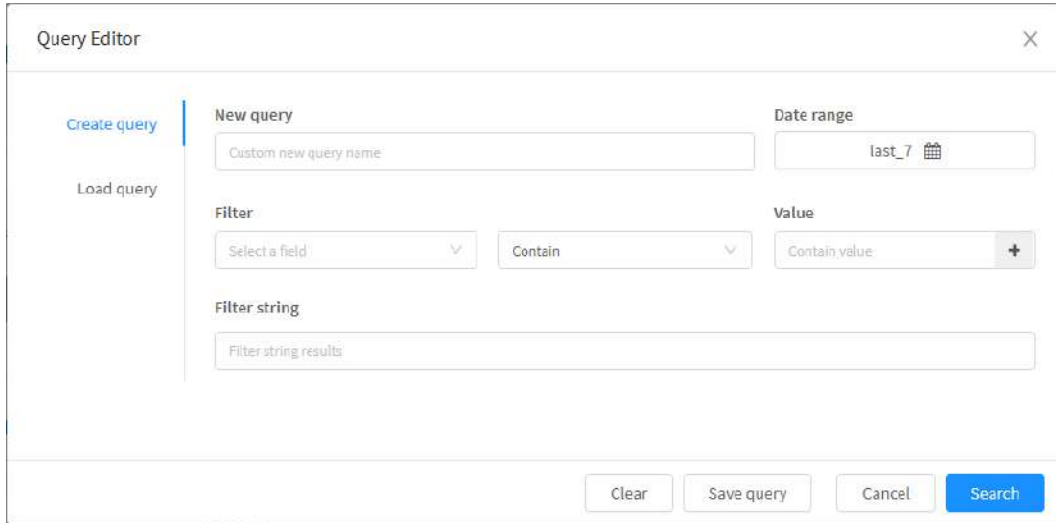
Nesta sessão, analisaremos os componentes do painel *events*.

- [Query Editor](#);
- [Top Hits](#);
- [History](#);
- [Log Events](#).

Inicialmente nos aprofundaremos no [Query Editor](#).

Events - Query Editor

Através do editor de queries, é possível criar, editar e salvar uma *queries* para efetuar uma busca aprofundada nos eventos, ao clicar no **Query Editor** [] a seguinte janela será exibida:

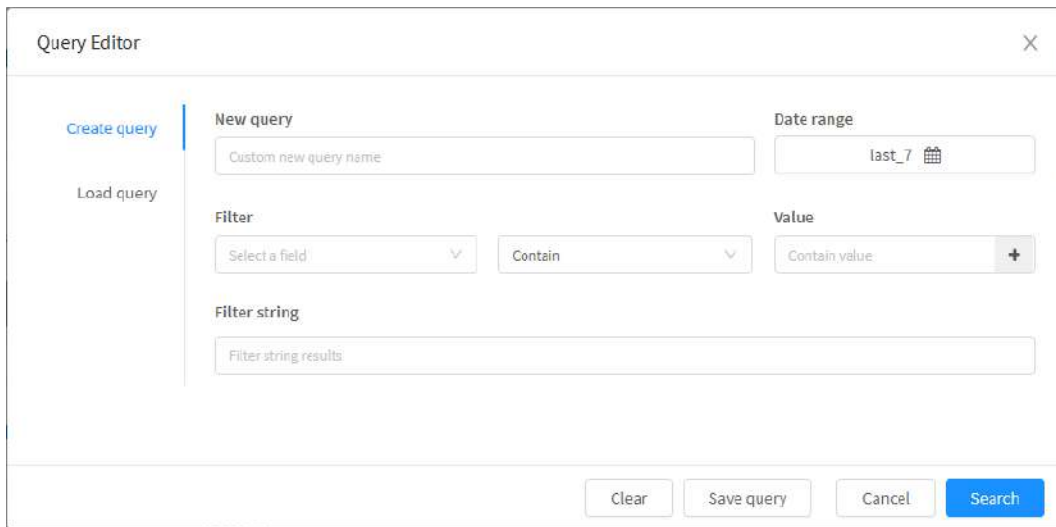


Events - Query Editor

A seguir analisaremos cada campo desta janela:

Events - Query Editor - Create query

Na aba "Create query" é possível configurar como a *query* irá atuar:



Events - Query Editor - Create query

- **New query:** Determina qual será o nome da *query*. Ex.: *Last 7 days*;
- **Date range:** Permite determinar um período para filtrar os resultados de forma mais precisa, as opções possíveis são:
 - **By date:** Determina uma data específica;
 - **By period:** Exibe resultados de uma data inicial ("*Start date*") até uma data final ("*End date*");

- **Today:** Exibe resultados especificamente para a data de hoje;
 - **Yesterday:** Exibe resultados especificamente para ontem;
 - **Last 7 days:** Filtra especificamente os resultados dos últimos 7 dias;
 - **Last 30 days:** Filtra especificamente os resultados dos últimos 30 dias;
 - **This month:** Exibe os resultados deste mês;
 - **Last month:** Exibe os resultados do último mês.
- **Filter:** Esta campo permite selecionar o tipo de filtro que será utilizado pela *query* para selecionar os resultados que serão exibidos. As opções possíveis são:
 - **logtype:** Faz a seleção pelo tipo de *log*, para este filtro as opções disponíveis são: webfilter, firewall, dpi, ips, atp;
 - **src:** Efetua a seleção pelo IP de origem, este filtro aceita endereços IPv4 ou Ipv6 como *valor*. Ex.: 172.16.12.171;
 - **dst:** Faz a seleção pelo IP de destino, este filtro aceita endereços IPv4 ou Ipv6 como *valor*. Ex.: 172.16.12.171;
 - **sport:** Este filtro possibilita a seleção por uma porta de origem. Ex.: 1 a 65535;
 - **dport:** Este filtro possibilita a seleção por uma porta de destino. Ex.: 1 a 65535;
 - **protocol:** Este filtro permite a seleção por protocolo, as opções disponíveis são: tcp, udp, icmp, ip;
 - **service:** No caso deste filtro, é feita a seleção por serviço, os valores aceitos são baseados na tabela do IANA, para mais informações consulte esta [página](#);
 - **devin:** Faz a seleção pelo Device de entrada, este filtro aceita interfaces, para mais informações sobre como criá-las, consulte esta [página](#). Ex.: eth0, eth1, eth2, etc;
 - **devout:** No caso deste filtro, a seleção é feita pelo Device de saída, os valores aceitos são as interfaces criadas pelo usuário, para mais informações sobre como criá-las, consulte esta [página](#). Ex.: eth0, eth1, eth2, etc;
 - **zonein:** Este filtro possibilita a seleção pela zona de entrada, os valores aceitos são as zonas configuradas nas *interfaces do UTM*, para mais informações consulte esta [página](#). Ex.: LAN, WAN, DMZ, etc;
 - **zoneout:** Este filtro possibilita a seleção pela zona de saída, os valores aceitos são as zonas configuradas nas *interfaces do UTM*, para mais informações consulte esta [página](#). Ex.: LAN, WAN, DMZ, etc;
 - **client_mac:** Faz a seleção por endereço MAC, portanto, este filtro aceita endereços físicos. Ex.: 84:d5:f7:57:5b:db;
 - **client_user:** Este filtro efetua a seleção por usuário, ele aceita e-mails como valores. Ex.: user@blockbit.com;
 - **client_ip:** Este filtro efetua a seleção pelo IP do cliente, os valores aceitos são endereços IPv4 ou Ipv6. Ex.: 172.16.9.153;
 - **geoip_src:** No caso deste filtro, a seleção é feita pela origem do GeoIP (Geolocalização de endereço IP), os valores aceitos são siglas de país. Ex.: BR, US, CA, CN, etc;
 - **geoip_dst:** Efetua a seleção pelo destino do GeoIP (Geolocalização de endereço IP), os valores aceitos são siglas de país. Ex.: BR, US, CA, CN, etc;
 - **rule_name:** Este filtro efetua seleções pelo nome da regra, sendo que o nome das regras criadas no UTM são utilizadas como *valor*, para mais informações consulte esta [página](#);
 - **rule_action:** Faz a seleção baseada na ação que a regra toma, este filtro aceita como valor as opções: Allow, Alert ou Deny. Ex.: Deny;
 - **web_category:** Este filtro possibilita a seleção por categoria *web*, sendo estas mesmas aceitas como valor. Ex.: Information Technology, Web Mail, Personal Network Storage and Backup, etc.
 - **web_site:** Faz a seleção por sites, este filtro aceita URLs como *valor*. Ex.: https://www.blockbit.com;
 - **web_method:** Efetua a seleção pelo métodos HTTP, este filtro aceita como valores os métodos POST e GET. Ex.: POST;
 - **web_mime:** Este filtro permite a seleção por MIME-Type, sendo exatamente este mesmo o valor aceito. Ex.: "application/octet-stream";
 - **ips_profile:** Efetua a seleção pelo Perfil de Intrusion Prevention System, o valor aceito é o nome do perfil, para mais informações consulte esta [página](#);
 - **app_name:** Este filtro permite efetuar a seleção por nome do aplicativo. Ex.: Google APIs;
 - **app_category:** Efetua a seleção pela categoria do aplicativo, sendo exatamente este mesmo o valor aceito. Ex.: web;
 - **malware_file:** Faz a seleção nome do arquivo do *malware*. Ex.: malwarefile.com;
 - **malware_md5:** Seleciona através do MD5 dos *malwares*. Ex.: c69e30152b6aa805b23ba26ca1bfa866
 - **malware_status:** Seleção pelo *status* dos *malwares*. Ex.: INFECTED;
 - **malware_name:** Seleção pelo nome dos *malwares*. Ex.: Malware;
 - **threat_class:** Este filtro faz a seleção pela classe da ameaça. Ex.: Potentially Bad Traffic;
 - **threat_category:** Efetua a seleção pela categoria da ameaça. Ex.: USER_AGENTS;
 - **threat_sid:** Seleciona pelo SID da ameaça. Este filtro utiliza o SID da ameaça. Ex.: 2027916;
 - **threat_name:** Este filtro faz a seleção pelo nome da ameaça. Ex.: Poison Null Byte;
 - **threat_impact:** Este filtro faz a seleção baseada no nível de impacto da ameaça. Ex.: High, Medium, Low;
 - **threat_dump:** Seleção pelo dump da ameaça. Este filtro aceita o *dump* da ameaça;
 - **threat_payload:** Faz a seleção pelo payload da ameaça. Esse filtro exige como *value* a sequência de *payload* da ameaça.
 - **flow:** Mostra juntamente com o endereço IP, a NAT aplicada e qual o endereço atribuído.
- **Contain/Not Contain:** Esta caixa de seleção atua basicamente como um operador lógico do filtro da *query*;
 - **Contain:** Irá exibir todos os resultados que contêm o valor do próximo campo (*Value*);
 - **Not Contain:** Irá exibir todos os resultados que NÃO contêm o valor do próximo campo (*Value*).
 - **Equals:** Irá exibir todos os resultados que são EXATAMENTE iguais ao que for adicionado no próximo campo (*Value*);
 - **Not Equals:** Irá exibir todos os resultados que NÃO são iguais ao que for adicionado no próximo campo (*Value*);
- **Value:** Esta caixa determina o valor que será utilizado para filtrar a *query*, após definir o valor, clique em [+] para adicionar a *string* no campo *Filter string*;
- **Filter string:** Após editar os campos anteriores, este campo exibirá a *string* que será utilizada pela busca. Além de usar as opções anteriores, é possível editar manualmente essa linha de código.



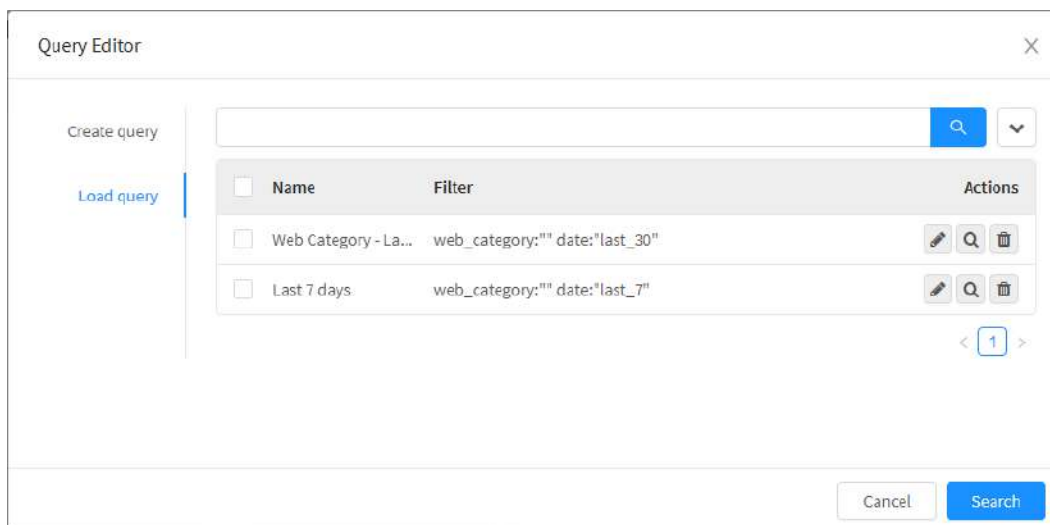
Para limpar a *query* configurada, clique no botão **Clear** [Clear]. Caso deseje cancelar clique no botão **Cancel** [Cancel]. Para efetuar uma busca utilizando a *query* clique no botão **Search** [Search].

Save query

Para salvar a *query*, clique no botão **Save Query** [

Events - Query Editor - Load query

Na aba "Query Editor" é possível administrar as *queries* salvas, este painel é composto de uma [barra de busca](#) e um botão de ação com função de deletar todos os campos selecionados, a seguir analisaremos cada componente deste painel:



Events - Query Editor - Load Query

- **Select** [☐]: Permite selecionar a *query* desejada;
- **Name**: Exibe o nome da *query*;
- **Filter**: Exibe a *string* utilizada pela busca;
- **Actions**: Exibe um conjunto de botões contextuais;
 - **Edit** []: Editar as configurações da *query*;
 - **Search** []: Efetua uma busca utilizando a *query*;
 - **Delete** []: Remove a *query*.

Cancel

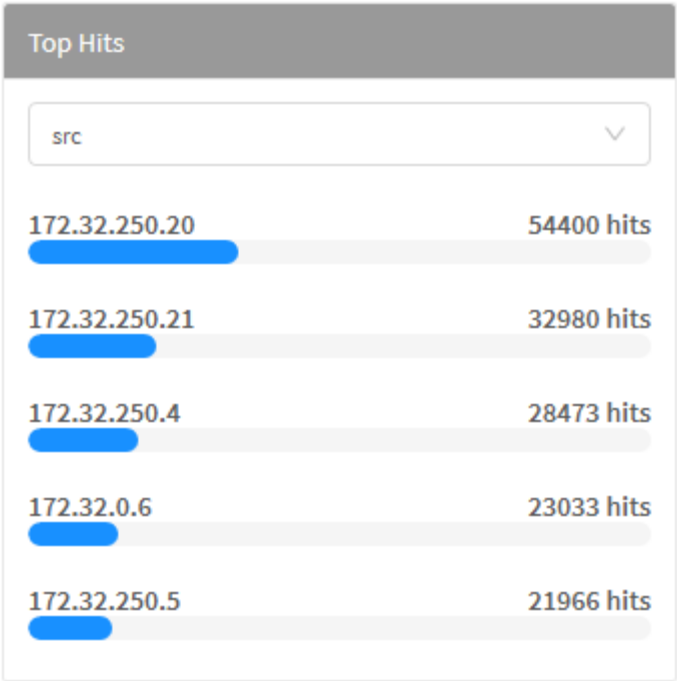
Caso deseje cancelar clique no botão **Cancel** [

Search

].

Events - Top Hits

Em "Top Hits" temos uma caixa de seleção composta de várias opções, ao selecionar alguma delas, é exibido um gráfico destrinchando ainda mais a opção selecionada e exibindo os 5 maiores itens divididos por quantia de acessos relacionados a opção selecionada, conforme demonstrado abaixo:



Events - Top hits

As opções disponíveis são:

Opções da Caixa de Seleção Top hits

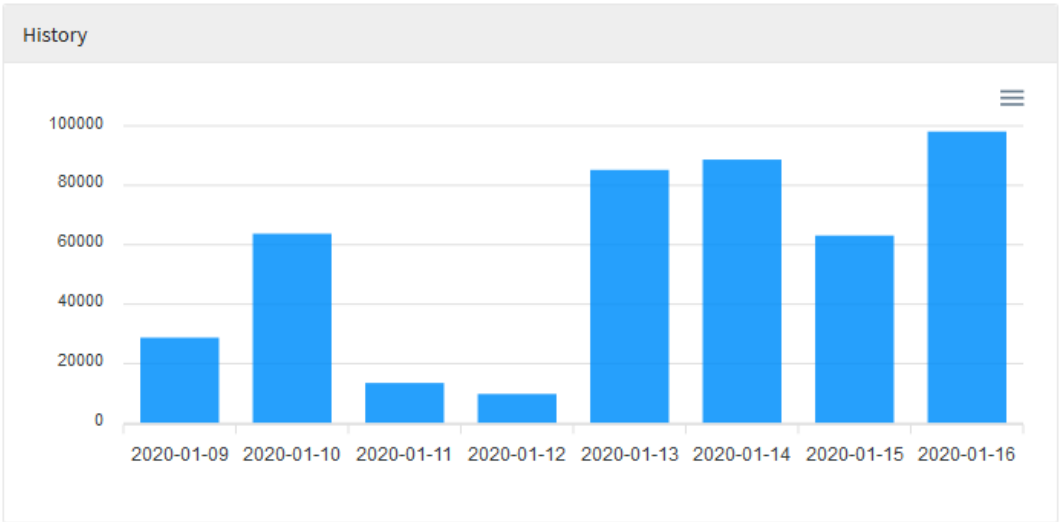
Seleção	Detalhamento
app_category	Categorias de aplicativos mais usadas.
app_name	Nomes dos aplicativos mais usados.
client_ip	IPs dos clientes com maior número de acessos.
client_user	Usuários com maior número de acessos.
client_mac	Endereço MAC com maior número de acessos.
dport	Números das portas de destino mais ativas e a quantia de acessos a cada uma delas.
dst	Porta de destino com maior número de acessos.
devin	Device de entrada com maior número de acessos.
devout	Device de saída com maior número de acessos.
geoup_dst	Os destinos dos GeoIP com maior número de acessos.
geoup_src	As origens dos GeoIP com maior número de acessos.
logtype	Tipos de log mais gerados de acordo com o maior número de acessos.
malware_file	Tipo dos arquivos de malware mais detectados de acordo com o maior número de acessos.
malware_name	Nome dos malwares mais detectados de acordo com o maior número de acessos.
malware_md5	MD5 dos malwares mais detectados de acordo com o maior número de acessos.

<i>malware_status</i>	Os <i>status</i> dos <i>malwares</i> mais detectados de acordo com o maior número de acessos.
<i>protocol</i>	Os protocolos com maior número de acessos.
<i>rule_name</i>	O nome das regras com maior número de acessos.
<i>service</i>	Os serviços com maior número de acessos.
<i>sport</i>	A porta de origem com maior número de acessos.
<i>src</i>	Os <i>IPs</i> de origem com maior número de acessos.
<i>threat_impact</i>	O impacto das ameaças de acordo com maior número de acessos.
<i>threat_sid</i>	O <i>SID</i> com maior número de acessos.
<i>threat_dump</i>	O <i>dump</i> das ameaças com maior número de acessos.
<i>threat_name</i>	O nome das ameaças com maior número de acessos.
<i>threat_classification</i>	As classificações das ameaças com maior número de acessos.
<i>threat_category</i>	As categorias das ameaças com maior número de acessos.
<i>web_category</i>	As categorias <i>web</i> com maior número de acessos.
<i>web_mime</i>	Os <i>MIME-Types</i> com maior número de acessos.
<i>web_browser</i>	Os navegadores com maior número de acessos.
<i>web_site</i>	Os sites com maior número de acessos.
<i>web_method</i>	Os métodos <i>HTTP</i> com maior número de acessos.
<i>zonein</i>	As zonas de entrada com maior número de acessos.
<i>zoneout</i>	As zonas de saída com maior número de acessos.

Events - History

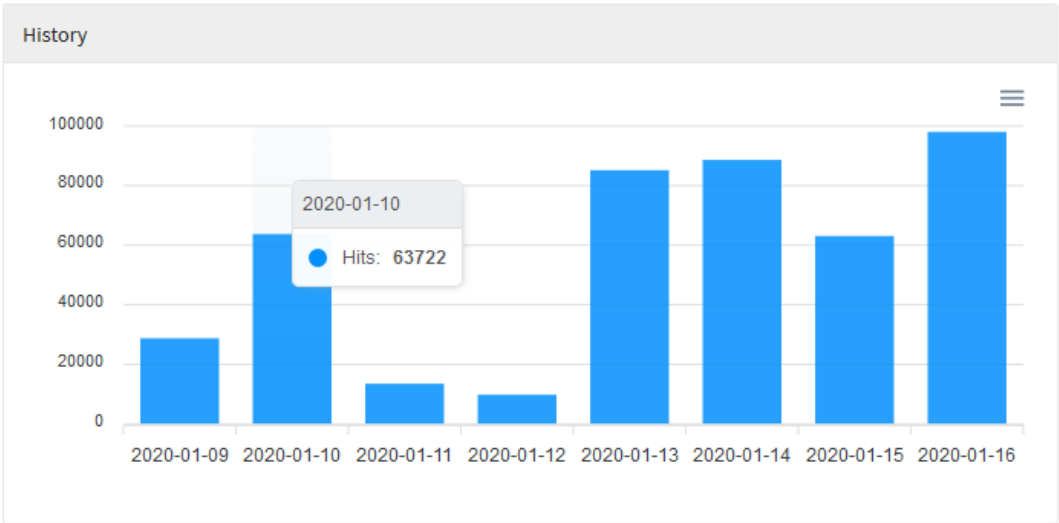
Em "history" temos um gráfico de colunas verticais exibindo o histórico total de acessos por data, o eixo vertical do gráfico exibe a média dos acessos e o horizontal os dias onde eles aconteceram.

O gráfico *History*, NÃO representa os *Top Hits* mas sim o histórico total de acessos.



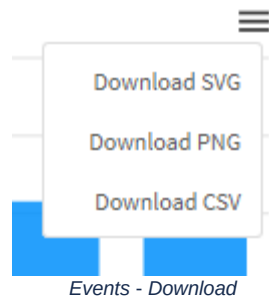
Events - History

Ao passar o *mouse* por cima do gráfico é exibido o valor exato dos acessos representados pela coluna selecionada.



Events - History - Valor exato dos acessos

Ao clicar no botão de **menu** ], é possível baixar este diagrama no formato *svg*, *png* ou *csv*.



Events - Log Events

Por fim, em "Log Events" temos um registro de todos os eventos detectados no *device* selecionado.

Date	User	Source	Destination	Device	Service	Log type	Action
2021-03-09 17:19:32	-	172.31.0.99:64638	192.168.254.253:443	eth0 - eth0	https	firewall	allow
2021-03-09 17:19:32	-	172.31.0.99:64648	192.168.254.253:443	eth0 - eth0	https	firewall	allow
2021-03-09 17:19:36	user@blockbit.com	172.32.250.100:59439	172.16.13.246:53	eth1 - eth0	domain	firewall	allow
2021-03-09 17:19:26	-	172.32.0.6:35348	172.31.0.100:8080	eth1 - eth0	http-alt	firewall	allow
2021-03-09 17:19:41	-	172.32.0.6:35350	172.31.0.100:8080	eth1 - eth0	http-alt	firewall	allow
2021-03-09 17:19:31	user@blockbit.com	172.32.250.109:63367	172.16.13.246:53	eth1 - eth0	domain	firewall	allow
2021-03-09 17:19:11	-	172.32.0.6:35346	172.31.0.100:8080	eth1 - eth0	http-alt	firewall	allow
2021-03-09 17:19:31	user@blockbit.com	172.32.250.109:63271	172.16.13.246:53	eth1 - eth0	domain	firewall	allow
2021-03-09 17:19:31	user@blockbit.com	172.32.250.109:53354	172.16.13.246:53	eth1 - eth0	domain	firewall	allow
2021-03-09 17:19:56	-	172.32.0.6:35352	172.31.0.100:8080	eth1 - eth0	http-alt	firewall	allow

Events – Log Events

Esse painel é composto por 4 colunas:

- **Date:** Temos a data e o horário exato desse evento;
 - **User:** Exibe a identificação do usuário que gerou o evento;
 - **Source:** Temos a fonte desse evento, um endereço *IP*;
 - **Destination:** Temos o destino desse evento, outro endereço *IP*;
 - **Device:** Define em quais *interfaces* o acesso que gerou o evento;
 - **Service:** Temos o serviço atrelado a esse evento;
 - **Log Type:** Determina a categoria de registro deste evento;
 - **Action:** Define qual ação foi efetuada pelo evento;
- **Sessid** [🔄]: Ao clicar neste botão é efetuada uma busca utilizando o *Id* da Sessão do evento selecionado;
- **Event View** [☰]: Este botão permite acessar a janela "event view";

Logo do lado da data do evento temos um ícone [⊕] que ao ser selecionado irá expandir a seleção e exibir mais informações a respeito desse evento específico.

Information					
data	client_mac	proto	host	web_url	web_site
2023-01-31 12:01:54	00:0c:29:d5:ba:cd	tcp	utmviole23-14	http://ctldl.windowsupdate.com/msdown	http://ctldl.windowsupdate.com/msdown
logtype	dst	service	client_ip	load/update/v3/static/trusted/en/pinnule	load/update/v3/static/trusted/en
web	192.16.48.200	http	179.30.0.10	ssl.cab73d5830f1d6545...	
sessid	rport	devout	web_method	web_referrer	
1A0ADF6C296FEDAB30A2683E7B639F39	80	default	GET	-	
src	devin	rule_action	web_profile	web_agent	
179.30.0.10	eth1	allow	Ética de Segurança	Microsoft-CryptoAPI/10.0	
sport	zonein	web_mime	surfing_time	bytes	
55649	LAN	application/octet-stream	1	0	
				web_protocol	
				HTTP	

Events – Log Events – Information

À seguir, nos aprofundaremos nos componentes da janela *event view*.

Events - Log Events - Event View

O botão **Event View**  exibe detalhes mais aprofundados do evento em questão, conforme exibido na imagem abaixo:



Events - Log Events - Event View

Loggers

Os *loggers* tem como função efetuar a captação de informações dos Blockbit UTM administrados pelo sistema e utilizando estes dados, efetuar a criação dos relatórios no Blockbit GSM.

Além disso, este recurso também centraliza o gerenciamento das rotinas automáticas de *backup* desta *feature*, ela atua armazenando os eventos de log gerados remotamente para cada um dos dispositivos de *Logger*.

As rotinas de backup são administradas e enviadas ao servidor de *backup* pelo próprio *Logger*, podendo ser armazenadas em servidores *SMB*, *NFS* e *SFTP*.



Para mais informações a respeito de backup dos *Loggers*, consulte esta [página](#).

Para gerir os *loggers*, clique no ícone localizado na lateral esquerda:



Analytics - *Loggers*.

A seguinte tela será exibida:

Name	CPU Usage	Memory Usage	Disk Usage	Storage Usage	Actions
Logger 3 - 2.0.8	0%	7.8 GB	7.7 GB	Storage unavailable	
Logger 4 - 2.1	1%	15.6 GB	7.7 GB	Storage unavailable	
Logger 5 - 2.1	0%	15.6 GB	7.7 GB	Storage unavailable	
Logger1	0%	15.6 GB	7.7 GB	Storage unavailable	
Logger2	0%	15.6 GB	7.7 GB	Storage unavailable	

Analytics - *Loggers*

Esta tela é composta pelas abas:

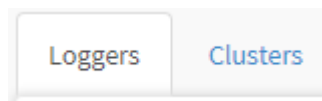
- [Loggers](#);
- [Clusters](#);

Inicialmente vamos analisar o passo a passo de como efetuar a [instalação de um Logger](#).

Loggers - Loggers

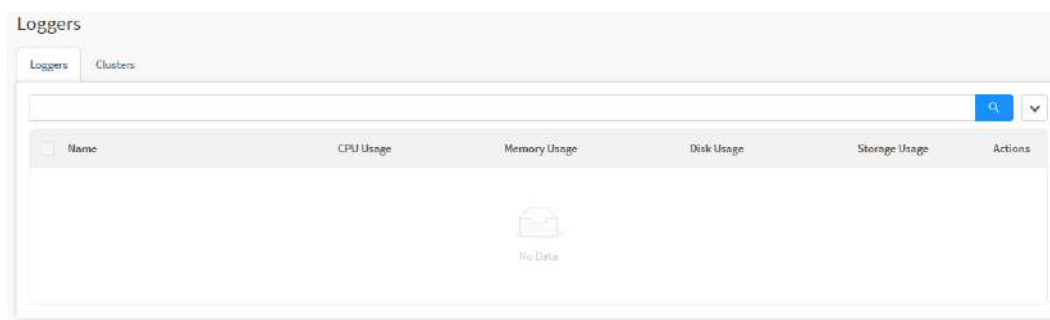
Nesta aba temos acesso aos recursos para criação de *loggers* e de rotinas automáticas de *backup*, possuindo também ferramentas para visualizar o desempenho e estado atual dos dispositivos de *log* e de possibilidade de visualizar o histórico dos *backups*.

Para acessar estas funções, selecione a aba "Loggers":



Aba Loggers

A tela à seguir será exibida:



Loggers - Loggers

Nesta sessão analisaremos:

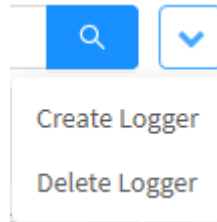
- Como [criar](#), editar e [remover](#) um logger e uma rotina de *backup*;
- [Detalhes do histórico de backups](#);
- [Os componentes das colunas desta tela](#).

A seguir detalharemos as opções do [menu de ações](#).

Loggers - Menu de ações



Ao clicar no botão **menu de ações**] no topo direito é possível adicionar o *logger* ou removê-lo.



Loggers – Menu de ações do Logger.

O menu é composto das seguintes opções:

- [Create Logger](#);
- [Delete Logger](#).

A seguir cada opção do menu de ações será detalhada.

Create Logger

Para cadastrar um *logger* clique na opção "Create Logger" no canto superior direito da tela, a seguinte janela será exibida:

The screenshot shows a web application window titled "Create Logger Device". On the left side, there is a sidebar with two tabs: "Settings" (which is active and highlighted in blue) and "Storage". The main content area is divided into a "General" section. This section contains several form fields, each marked with a red asterisk to indicate they are required: "Name", "Mode" (a dropdown menu currently showing "Integrated"), "Description" (a large text area), "Interface", "Address", "Secret Key" (a text area), and "Devices & Devices Group" (a dropdown menu showing "Select a type" with a list area below it containing up and down arrow buttons and plus/minus buttons). At the bottom right of the window, there are two buttons: "Cancel" and "Save".

Loggers – Create Logger Device



Para mais informações sobre como instalar um *logger device*, acesse esta [página](#).

Esta janela é dividida em duas abas que podem ser acessadas na lateral esquerda:

- [Settings](#);
- [Storage](#).

Além disso, a aba [Archiving](#) possui os painéis:

- [Backups](#);
- [Log Rotation](#).

À seguir vamos analisar os componentes da aba [Settings](#):

Settings

Este painel tem como função determinar as configurações do *Logger*. Para tanto, configure o formulário conforme as instruções a seguir:



Atente que o processo de *upgrade* interfere com as interfaces configuradas em *loggers* do tipo *standalone*. Para mais informações sobre o comando *upgrade-blockbit*, consulte esta [página](#).

Create Logger Device - Settings

- **Name:** Determina o nome do *Logger* a ser cadastrado. Ex.: *Logger 1*;
- **Mode:** Define qual será o modo de atuação do *Logger*. Podendo ser:
 - Standalone;
 - Integrated.
- **Description:** A descrição do *logger*, possui basicamente caráter organizacional;
- **Interface:** Define a *interface* que será utilizada para configurar o *logger*, ela terá sido determinada no *wizard* de configuração do *logger*. Deve-se utilizar a mesma onde foi cadastrado o *IP* da *logger*, para mais informações, consulte esta [página](#).
- **Address:** Determina o endereço *IP* que será utilizado para acessar esse *logger*. Além disso, caso o *H.A.* de *logger* tenha sido configurado, o endereço definido neste campo será usado no *heartbeat*, para mais informações, consulte esta [página](#). Ex.: 10.0.0.1;
- **Secret Key:** É a chave secreta emitida pelo *wizard* de instalação do *logger*. Ela precisa ser colada na íntegra para o *Logger* funcionar, caso necessário, é possível copiá-la através da CLI usando o comando [\[logger-key\]](#). Além disso, caso o *H.A.* de *logger* tenha sido configurado, a chave (ssh) definida neste campo será usada no *heartbeat*, para mais informações, consulte esta [página](#);
- **Devices & Devices Group:** É uma caixa de seleção que permite a localização dos *devices* ou grupos de *device* que o *logger* usará para criação

de relatórios. Clique em [] para adicioná-los ou em [] para removê-los.



O device UTM deverá estar previamente cadastrado no menu *Administration*, em *Devices*, na aba *Inventory* para ser exibido em *Devices & Device Groups*



Caso esteja utilizando *Cluster de Loggers*, atente que não é possível vincular um *device* a um *logger* que não esteja ativo no *cluster*. Para mais informações a respeito de como efetuar a ativação manualmente, consulte esta [página](#).

Isso conclui a configuração do *logger*.

À seguir vamos analisar como configurar *Backups* do *Loggers*:

Storage

Nesta interface o administrador tem os recursos necessários para gerenciar as rotinas de *backups* automáticas para cada dispositivo de *Logger* que for criado e para configurar a retenção destes mesmos.

Create Logger Device

Settings

Storage

Backups

☐ Enable

Remote Storage

Select a type

Number of backup retention

100

% Disk usage retention

70

Log Rotation

☐ Enable

% Log Retention by Disk Space

70

Log Retention by Period

Unlimited

Maintenance Interval

5

Minutes

Cancel

Save

Create Logger Device - Backups

Esta tela é dividida em dois painéis:

- [Backups](#);
- [Log Rotation](#).

À seguir, iremos analisar cada um dos componentes dessa janela:

Backups

Neste painel estão as configurações que permitem criar uma rotina de *backup* automatizada para cada *Logger*.

Archiving - Backups

- **Enable** []: Habilita o *backup* de *Loggers*;
- **Remote Storage**: Define o local onde será armazenado os *backups*, os itens que aparecem nesta lista são criados na *Aba Storages* no menu *System*, porém, o *Storage* deve possuir a opção "Only Logger" habilitada. Para mais informações a respeito, consulte esta [página](#). Ex.: *Backup*;
- **Number of Backup Retention**: Determina quantos *backups* serão armazenados no diretório. Ao fim deste limite, o *backup* mais antigo é apagado. Por exemplo, caso opte por "3", só serão mantidos os 3 últimos *backups*, assim sendo, quando um novo *backup* for gerado será executada a rotina para apagar o mais antigo sempre respeitando o valor adicionado neste campo. Ex.: 1;
- **% Disk usage retention**: Define a porcentagem de uso que o diretório criado dentro do *storage* usará ao salvar o *backup*. Caso o limite seja atingido, a rotação de *backups* é efetuada, removendo o mais antigo de forma a sempre manter os *backups* mais recentes. Caso um diretório possua 100 GB e seja optado por 30% de retenção, quando os registros ocuparem 30 GB a rotação será ativada, caso contrário, o número de retenção será verificado. Ex.: 100;



O sistema atua primeiro verificando se a porcentagem de uso foi atingida e depois checando o número de *backups* retidos. Assim sendo:

1. Caso ainda possua espaço livre, o sistema irá verificar o número de *backups* retidos.
2. Caso a quantia máxima de retenção não tenha sido atingida, o armazenamento de *backups* continuará atuando normalmente sem apagar registros anteriores.

Analisando o cenário contrário, a atuação do sistema será conforme explicado abaixo:

1. Caso o limite de espaço seja atingido, a rotação será ativada para manter apenas os *backups* mais recentes;
2. Caso ainda exista espaço em disco, mas o número de *backups* retidos exceda o limite definido pelo administrador, os registros mais antigos serão removidos, respeitando o valor definido no campo, de forma que o diretório possua sempre os *backups* mais recentes.



Se o administrador não quiser que a porcentagem seja considerada, basta adicionar o valor "100" de modo que o espaço seja totalmente utilizado antes de ativar a rotação. Desta forma, só o número de *backups* retidos será considerado.

Isso finaliza a configuração do painel de *backups* do *logger*.

À seguir vamos analisar como configurar o painel *Log Rotation*.

Log Rotation

Neste painel estão as configurações que determinam a retenção dos *logs* armazenados pelo *Analyzer* para cada *Logger*.



Atente que o *Log Rotation* não é dependente do *Backup*. Cada recurso pode ser utilizado separadamente, bastando apenas ativá-los conforme a necessidade pelas suas respectivas caixas de checagem.

Log Rotation

☐ Enable

% Log Retention by Disk Space

70

Log Retention by Period

Maintenance Interval

Unlimited

5

Minutes

Archiving - Log Rotation



- **Enable** [☒]: Habilita a retenção dos *logs*;
- **% Log retention by disk space**: Determina o limite de retenção de *logs* por porcentagem de espaço em disco. O valor padrão é: 70%; O máximo é: 90%.
- **Log retention by period**: Define o período de retenção dos *logs*, o primeiro campo determina o número de dias, meses e anos, já o segundo campo define o período propriamente dito, as opções disponíveis são:
 - **Unlimited**: Desabilita o primeiro campo e define que a retenção dos *logs* será ilimitada.
 - **Days**: Define que a retenção dos *logs* será feita em determinados dias;
 - **Months**: Define que a retenção dos *logs* será feita em determinados meses;
 - **Years**: Define que a retenção dos *logs* será feita anualmente.
- **Maintenance Interval**: Define o tempo de manutenção dos *logs*, o primeiro campo determina o número de minutos e horas, já o segundo campo define o período propriamente dito, as opções disponíveis são:
 - **Minutos**: Desabilita o primeiro campo e define que a retenção dos *logs* será ilimitada.
 - **Horas**: Define que a retenção dos *logs* será feita em determinados dias.

Isso conclui a configuração do painel *Log Rotation*.

Save

Cancel

Para finalizar a criação do *logger*, clique em [Save]. Caso queira cancelar o processo, clique em [Cancel].

A seguir analisaremos como [remover um logger](#).

Delete Logger

Para deletar os *loggers*, siga os seguintes passos:



Só é possível deletar *Loggers* que não estejam vinculados a um [cluster](#).

1. Selecione o grupo que se deseja deletar clicando na **seleção**[];

☒	Name	CPU Usage	Memory Usage	Disk Usage	Actions
☒	Logger	0 core(s) 0%	0 GB 0%	0 GB 0%	 

Loggers - Selected Logger.

2. Clique no ícone de **menu de ações**[];

3. Clique na opção "*Delete Logger*";





Create Logger

Delete Logger

Loggers – Menu Actions – Delete Logger.

4. Surgirá uma mensagem de confirmação verificando se deseja deletar o *logger* selecionado:

Are you sure?

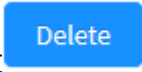
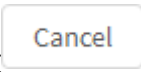
X

Are you sure you want to delete the logger Logger?

Cancel

Delete

Inventory - Delete logger message.

Clique no botão **Delete**[] ou clique em **Cancel**[] para voltar ao painel anterior.

 **Loggers deleted successfully**
Loggers deleted successfully

O *logger* foi removido com sucesso.

À seguir vamos analisar os componentes das [colunas](#).

Loggers - Colunas

A seguir explicaremos cada coluna do painel *Loggers*:

Loggers

Loggers

Clusters

3 records

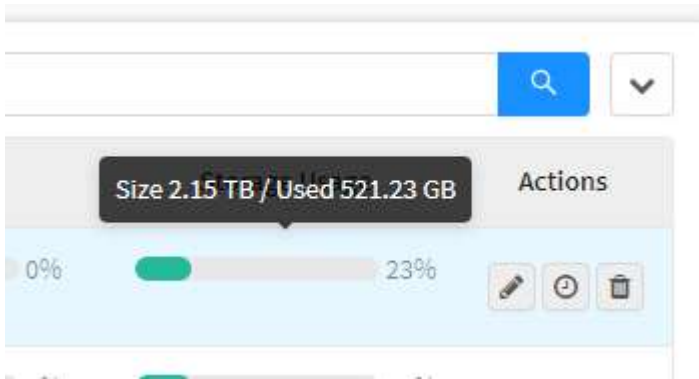
☐	Name	CPU Usage	Memory Usage	Disk Usage	Storage Usage	Actions
☐	LOGGER	0% 4 core(s)	76% 7.8 GB	5% 14.64 GB	23%	
☐	LOGGER BLOCKBIT	0% 0 core(s)	0% 0 GB	0% 0 GB	Storage unavailable	
☐	LOGGER TEST	0% 0 core(s)	0% 0 GB	0% 0 GB	Storage unavailable	

< 1 >

10 / page

Painel Loggers.

- **Select** [☐]: Permite selecionar um *logger*;
- **Status**: Exibe o estado atual do *logger*. Caso o ícone esteja verde [], o *Logger* está funcionando normalmente, porém, caso o ícone esteja vermelho [], tem algum erro no *Logger*.
- **Name**: Apresenta o nome do *logger* cadastrado;
- **CPU Usage**: Representa o uso de *CPU*, sua porcentagem de consumo e a capacidade total. É demonstrado em quantia de *cores* e *GigaBytes*;
- **Memory Usage**: Representa o uso de memória, sua porcentagem de consumo e a capacidade total. É demonstrado em *GigaBytes*;
- **Disk Usage**: Representa o uso de disco, sua porcentagem de consumo e a capacidade total. Exibido em *GigaBytes*;
- **Storage Usage**: Representa a porcentagem de uso do espaço de armazenamento total do *logger*. Para mais informações, passe o mouse em cima desta barra para exibir uma *tooltip*, conforme demonstrado na imagem à seguir:



Storage Usage - Tooltip

- **Actions**: Disponibiliza as seguintes ações essenciais:
 - **Edit** []: Caso o *logger* não esteja vinculado a um *cluster*, permite editar as configurações do *Logger* adicionado na opção *Create Logger* do menu de ações;
 - **Backups History** []: Exibe um painel com o histórico centralizado dos *backups* do *Logger*, incluindo informações sobre os que estão sendo efetuados no momento, para mais informações, consulte esta [página](#);
 - **Delete** []: Caso o *logger* não esteja vinculado a um *cluster*, permite remover o *logger*, é o equivalente à opção *Delete Logger*.

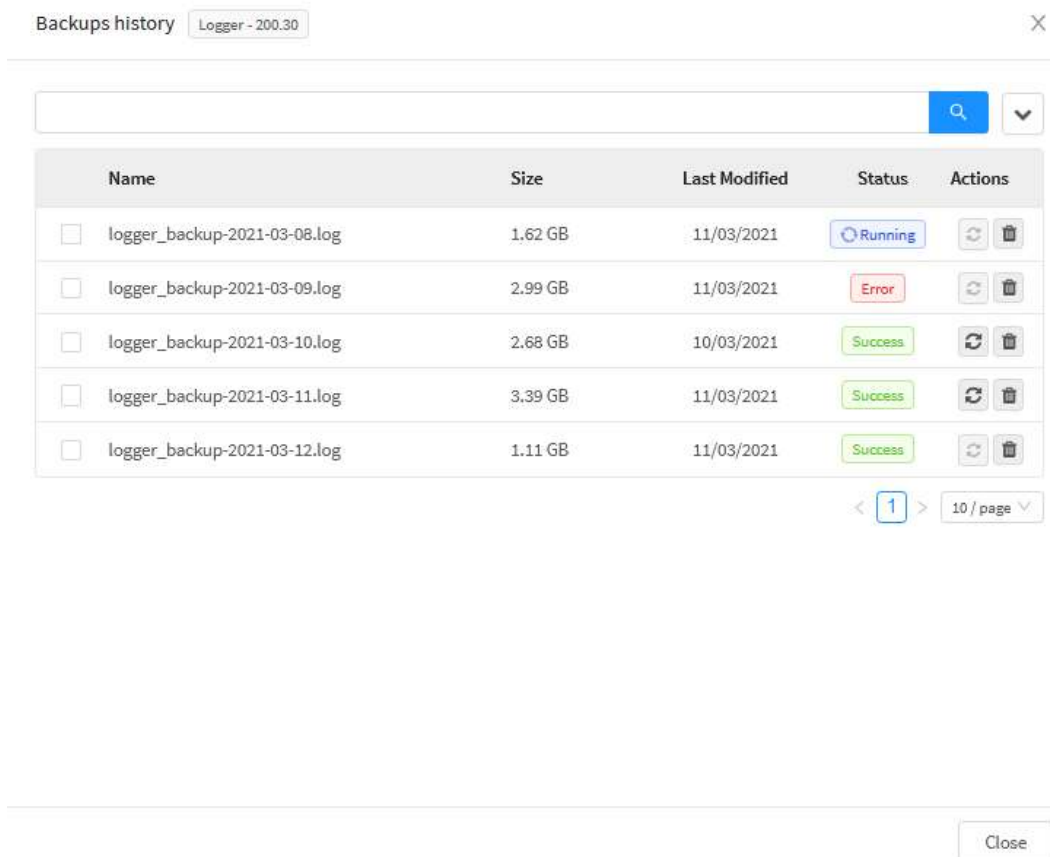


A remoção e edição de um *logger* só poderá ser realizada caso ele não esteja vinculada a um *cluster*.

À seguir, vamos nos aprofundar nos componentes da janela [Backups History](#).

Loggers - Backups History

Através da janela *Backups History*, é possível ter acesso a uma lista com todos os *bakups* já efetuados ou em curso. Abaixo, detalharemos cada componente desta janela:



Loggers - Backups History

- **Name:** Exibe o nome arquivo de *backup*;
- **Size:** Apresenta o tamanho do *backup*;
- **Last Modified:** Apresenta a data referente à quando o *backup* teve uma última alteração no seu estado;
- **Status:** Exibe o estado atual da execução da rotina de *Backup*, podendo ser:
 - []: A rotina de backup está em execução no momento;
 - []: Aconteceu algo de errado que causou a falha da rotina de *backup*;
 - []: A rotina está em tempo de espera. Isso pode ocorrer quando o sistema detecta um processo que possa interferir no *back up* está em execução no momento (por exemplo, uma outra rotina de *backup*);
 - []: O *backup* foi executado com sucesso.
- **Actions:** É composto por um conjunto de botões com ações úteis, sendo eles:
 - **Restore** []: Ao clicar neste botão o sistema avalia se o espaço em disco possibilita restaurar o *backup*, caso seja possível o procedimento de *backup* é executado no *Device* novamente. Porém, se não houver espaço o suficiente, a restauração será rejeitada e o usuário é informado na interface gráfica;
 - **Delete** []: Ao clicar neste botão, o *backup* é removido do histórico.

Para fechar esta janela basta clicar no [] localizado no topo da tela ou em [].

Para mais informações sobre as colunas, acesse esta [página](#).

À seguir detalharemos o conteúdo da aba [Clusters](#).

Exemplo - Backups de Logger

Esta seção irá apresentar o passo a passo para configuração de Backups da *Logger*.



Para mais informações a respeito de *Backups de Logger* consulte esta [página](#).

Os passos que tomaremos nesta demonstração serão:

- [Inclusão de Storage](#);
- [Criação da Rotina de Backup](#);
- [Validação das Configurações](#).

Iniciaremos a demonstração configurando um [Storage](#).

Exemplo - Backups de Logger - Inclusão de Storage

Após ter [adicionado os devices](#), nesta etapa efetuaremos os seguintes passos:

- Criação de Objeto;
- Configuração do *Storage*;

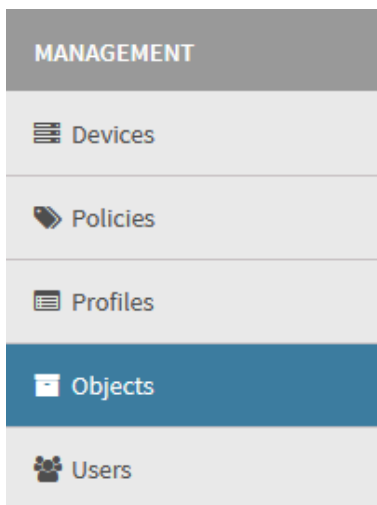


Este exemplo considerará que o *storage* que será utilizado pelo administrador está instalado e configurado corretamente. Para mais informações a respeito da compatibilidade do Blockbit GSM com *storages* remotos consulte esta [página](#).

Inicialmente geraremos os IPs que serão utilizados pelos Storages.

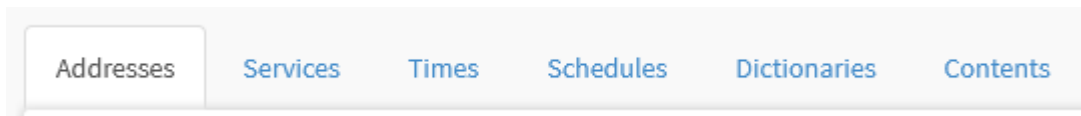
Criação de Objetos

Primeiramente criaremos o objetos de IP único que será utilizado para se conectar com o *Storage Remoto*, portanto acesse o menu Management e clique na opção *Objects*:



Management - Objects

Clique na aba *Addresses*:



Aba *Addresses*



Clique no ícone do **Menu de ações** [] e selecione a opção “*Create Object*”;

Inventory - Create Device

Adicionaremos o objeto de IP "Storage_SMB", complete o formulário conforme exemplificado a seguir:

Create Addresses Object

×

* Name

Storage_SMB

* Type

IPv4 Address

☒ Unique

* Address

Mask

255.255.255.255

+

172.31.0.180

^

▼

-

Description

Cancel

Import Address

Save

Adresses Object - Create Adresses Object

- **Name:** Usaremos o nome "Storage_SMB";
- **Type:** Selecione a opção "IPv4 Address";
- **Unique** ☒: Este será um objeto de tipo único, portanto se certifique de marcar esta caixa de seleção;
- **Address:** O endereço do Storage é "172.31.0.180";
- **Mask:** A máscara pode continuar sendo a padrão;

- **Description:** Neste exemplo, não adicionaremos uma descrição.

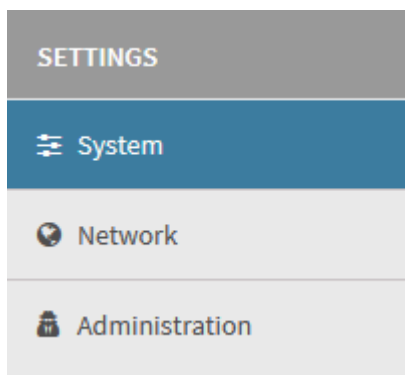
Save

Clique em [] para gravar as configurações.

Após ter criado os objetos de endereço, criaremos os *Storages*.

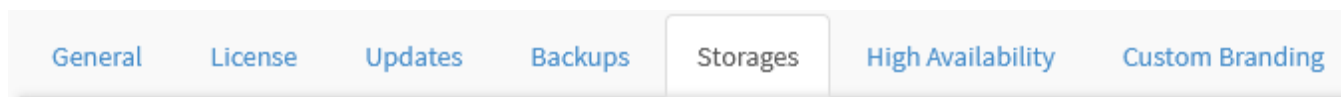
Configuração dos *Storages*

Acesse o menu *Settings* e clique na opção *System*:



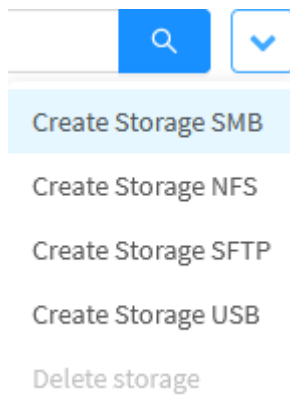
Settings - System

Acesse a aba *Storages*:



Aba Storages

Clique no ícone do **Menu de ações** [] e selecione a opção "Create Storage NFS";



Storages - Create Storages SMB

Adicionaremos o Storage_SMB_Logger, complete o formulário conforme exemplificado a seguir:

Create Storage SMB

X

* Description

Storage_SMB_Logger

* IP

Storage_SMB

Login

administrator@dominiof.com

Password

.....

* Share

SMB

* Simultaneous transfers

5

☒ Only Logger

Cancel

Save

Storages - Create Storage SMB

Complete o formulário como exemplificado abaixo:

- **Description:** Nomearemos este storage como "Storage_SMG_Logger";
- **IP:** Selecionaremos o objeto de IP que criamos anteriormente, o "Storage_SMB";
- **Login:** Adicione o usuário do servidor de arquivos, neste exemplo será "administrator@dominiof.com";
- **Password:** Insira a senha do usuário do servidor de arquivos;
- **Share:** Adicione o diretório que será utilizado para o compartilhamento no servidor de arquivos, neste exemplo será "SMB";
- **Simultaneous transfers:** Defina o limite de Transferências simultâneas deixaremos como 5 mesmo;
- **Only Logger** ☒: Por fim, certifique-se de marcar esta caixa de checagem.

Clique em  para gravar as configurações.

Ao finalizar todas as configurações, o storage terá sido configurado com sucesso:

System

[General](#)
[License](#)
[Updates](#)
[Backups](#)
[Storages](#)
[High Availability](#)
[Custom Branding](#)

4 records

Storage_NFS_01

NFS

54%

Storage_NFS_02

NFS

45%

Storage_SFTP_02

SFTP

45%

Storage_SMB_Logger

SMB

This Storage is mounted on the logger

<

1

>

10 / page

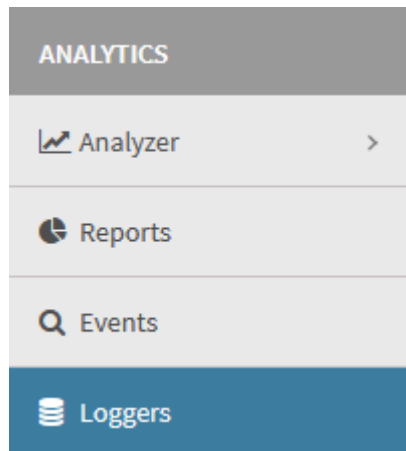
System - Storages

No próximo passo, criaremos as [rotinas de Backups](#) no *Logger*.

Exemplo - Backups de Logger - Criação da Rotina de Backup

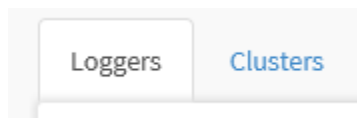
Este exemplo não irá detalhar o processo completo de instalação do Logger, para mais informações a respeito, consulte esta [página](#).

Após criar o [storage](#), criaremos um *Logger* com rotina de *backup*, inicialmente, acesse o menu *Analytics* e clique na opção *Loggers*:



Analytics - Loggers

Clique na aba "Backups":



Loggers - Aba Loggers

Criaremos um *Logger* com uma rotina diária de backup:



Para detalhes mais aprofundados sobre a criação de *Loggers*, consulte esta [página](#).

Create Logger Device

Settings

Storage

General

* Name

Remote Logger - 200.30

* Mode

Standalone

* Description

Remote Logger - 200.30

* Interface

eth0

* Address

172.31.200.30

* Secret Key

53616c7465645f5fe07b0287b0b6696955f243f6639117cafee982605c7e01f863d49ee42ebd1234c463c32e0a5c5fa296c6e48e4ba48d04dd3ca797ad68911c0b4c0355dded3483312b6e4b787fd20f825301ef9bcd6277b34702a5f001928b3881594f80f05730e07bf4

Devices & Devices Group

Select a type

+

UTM - 2.0.8

UTM 2.1 - 200.41

UTM Dev - 2.1.0

UTM Wifi - 2.0.8

-

Cancel

Save

Loggers - Create Logger Device - Settings

- **Name:** Usaremos o nome "Remote Logger - 200.30";
- **Mode:** Selecione "Standalone".
- **Description:** Como descrição simplesmente usaremos "Remote Logger - 200.30";
- **Interface:** Use a mesma interface que foi utilizada ao criar o *logger*, neste exemplo será a "eth0", para mais informações, consulte esta [página](#);
- **Address:** Digite o endereço IP que será utilizado para acessar o *logger*, neste exemplo será "172.31.200.30", para mais informações, consulte esta [página](#);
- **Secret Key:** Cole a chave secreta emitida pelo *wizard* durante instalação do *logger* na CLI;
- **Devices & Devices Group:** Adicione os Devices que serão utilizados neste logger, neste exemplo simplesmente foram adicionados todos os UTM's cadastrados no GSM.

Clique na aba "Storage" à esquerda e configure os campos como exemplificado abaixo:

Create Logger Device

X

Settings

Storage

Backups

☒ Enable

* Remote Storage

Storage_SMB_Logger

Number of backup retention

6

% Disk usage retention

80

Log Rotation

☒ Enable

* % Log Retention by Disk Space

65

Log Retention by Period

Unlimited

Maintenance Interval

30

Minutes

Cancel

Save

Loggers - Create Logger Device - Storage

- ☒
Enable [☒]: Marque esta caixa de checagem para habilitar o *backup de Loggers*;
- Remote Storage**: Selecione o Storage que foi criado no passo anterior: "Storage_SMB_Logger";
- Number of Backup Retention**: Neste exemplo iremos definir uma retenção de 6 backups;
- Percent usage retention**: Permitiremos um uso de 80% do diretório de armazenamento;
- ☒
Enable [☒]: Marque a caixa de checagem para habilitar o *Log Rotation*;
- % Log retention by disk space**: Neste exemplo, definiremos uma retenção de 65% de espaço em disco;
- Log retention by period**: Usaremos a opção "Unlimited" para que a retenção dos *logs* seja ilimitada;
- Maintenance Interval**: Para este exemplo usaremos um intervalo de manutenção de 30 minutos.

Save

Clique em [Save] para gravar as configurações.

Ao finalizar todas as configurações, a tela estará como demonstrado abaixo:

Loggers

Loggers Clusters

1 record

Q

☐	Name	CPU Usage	Memory Usage	Disk Usage	Storage Usage	Actions
☐	Remote Logger - 200.39	0% 8 core(s)	88% 23.5 GB	51% 19.6 GB	10%	

<

1

>

10 / page

Loggers - Loggers

Por fim, discutiremos a [validação](#) das configurações que efetuamos.

Exemplo - Backups de Logger - Validação das Configurações

Para validar o funcionamento dos *backups*, basta verificar se o histórico está disponível através do botão **Backups History** [🕒], como exibido abaixo:

Backups history Remote Logger - 200.30

🔍

▼

Name	Size	Last Modified	Status	Actions
☐ logger_backup-2021-03-10.log	6 Bytes	15/03/2021		
☐ logger_backup-2021-03-11.log	3.39 GB	11/03/2021		
☐ logger_backup-2021-03-12.log	1.71 GB	12/03/2021		
☐ logger_backup-2021-03-13.log	2.05 GB	13/03/2021		
☐ logger_backup-2021-03-14.log	1.53 GB	14/03/2021		
☐ logger_backup-2021-03-15.log	647.09 MB	15/03/2021		

< 1 >

10 / page ▼

Close

Loggers - Backups History

Esta janela estar disponível indica que o serviço irá efetuar o *backup* e criar o arquivo ".log" do dia.

Para mais informações sobre os componentes desta tela, consulte esta [página](#).

Além disso, as operações efetuadas pelos backups geram logs de auditoria, como demonstrado na imagem à seguir:

Administration

Administrators Users Profiles Auth Servers Identity Provider Audit Log

142 records

Date	User	Interface	Activity	IP	Actions
2021-03-10 20:58:57	Administrator	backups	Delete	192.168.200.2	
2021-03-10 20:58:03	Administrator	backups	Edit	192.168.200.2	
2021-03-10 20:16:21	Administrator	device-backups	Edit	192.168.200.2	
2021-03-10 19:12:49	Administrator	device-backups	Save	172.31.200.253	
2021-03-10 18:53:51	Administrator	device-backups	Delete	172.31.200.253	
2021-03-10 18:00:23	Administrator	backups	Edit	172.31.200.253	
2021-03-10 16:10:58	Administrator	device-backups	Edit	192.168.112.85	
2021-03-10 16:01:42	Administrator	device-backups	Save	192.168.112.21	
2021-03-10 16:01:13	Administrator	device-backups	Save	192.168.112.21	
2021-03-10 16:01:01	Administrator	device-backups	Save	192.168.112.21	

< 1 2 3 4 5 ... 15 > 10 / page

Administration - Audit Log

Clique em [] para obter mais informações a respeito do registro:

Audit View

```

{
  "Audit Information": {
    "settings_system-download-file": "5CA7-B928-5C8E-1B1C2.1.0-202103121619.conf"
    "settings_system-download-size": "1.05 MB"
  }
}

```

Close

Devices - Backups - Audit View



Para mais informações sobre os relatórios de auditoria, consulte esta [página](#).

Por fim, durante o processo de *rotate* do *log* também é possível verificar mais detalhes na *CLI* usando o comando de [\[debug-rotation\]](#).

```

admin >debug-rotation
date="2021-03-14 18:56" device_id="1" device_name="Logger Remoto - 200.30" deleted_date_ini="2021.03.09" deleted_date_end="2021.03.09" cu
rrent_total_index="4" total_space_disk="206" total_free_space_disk="8.86"
admin >

```

CLI - debug-rotation

Para mais informações a respeito de backups de *loggers*, consulte esta [página](#).

Instalação do Logger

Esta seção irá apresentar o passo a passo para instalação de um *logger* no Blockbit GSM.

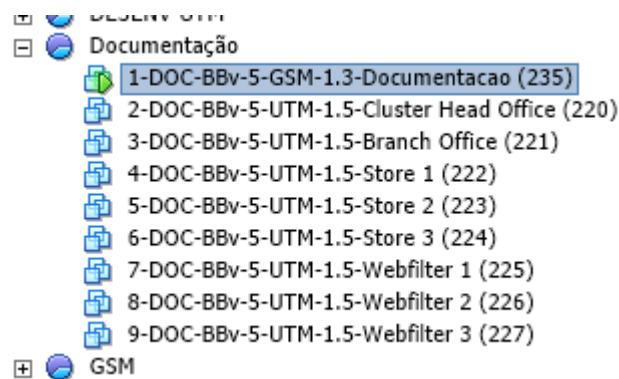
- [Instalação da Máquina Virtual](#);
- [Instalação do Logger Integrated](#);
- [Instalação do Logger Standalone](#);
- [Configuração da Logger na interface administrativa/manager do GSM](#).

Iremos demonstrar a instalação utilizando o software *VMware vSphere Client* como exemplo, procedimentos já executados no passo a passo citado no capítulo a respeito da [Instalação do GSM](#) não serão refeitos, caso haja alguma dúvida verifique a [sessão adequada](#).

Para realizar a instalação do *logger* no Blockbit GSM siga as orientações a seguir.

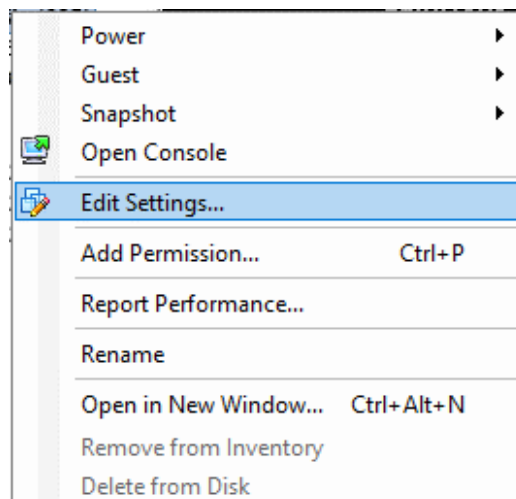
Instalação da Máquina Virtual

Primeiramente, inicie o *VMware* e navegue na sua estrutura de diretórios até a máquina virtual desejada, conforme exemplificado a seguir:

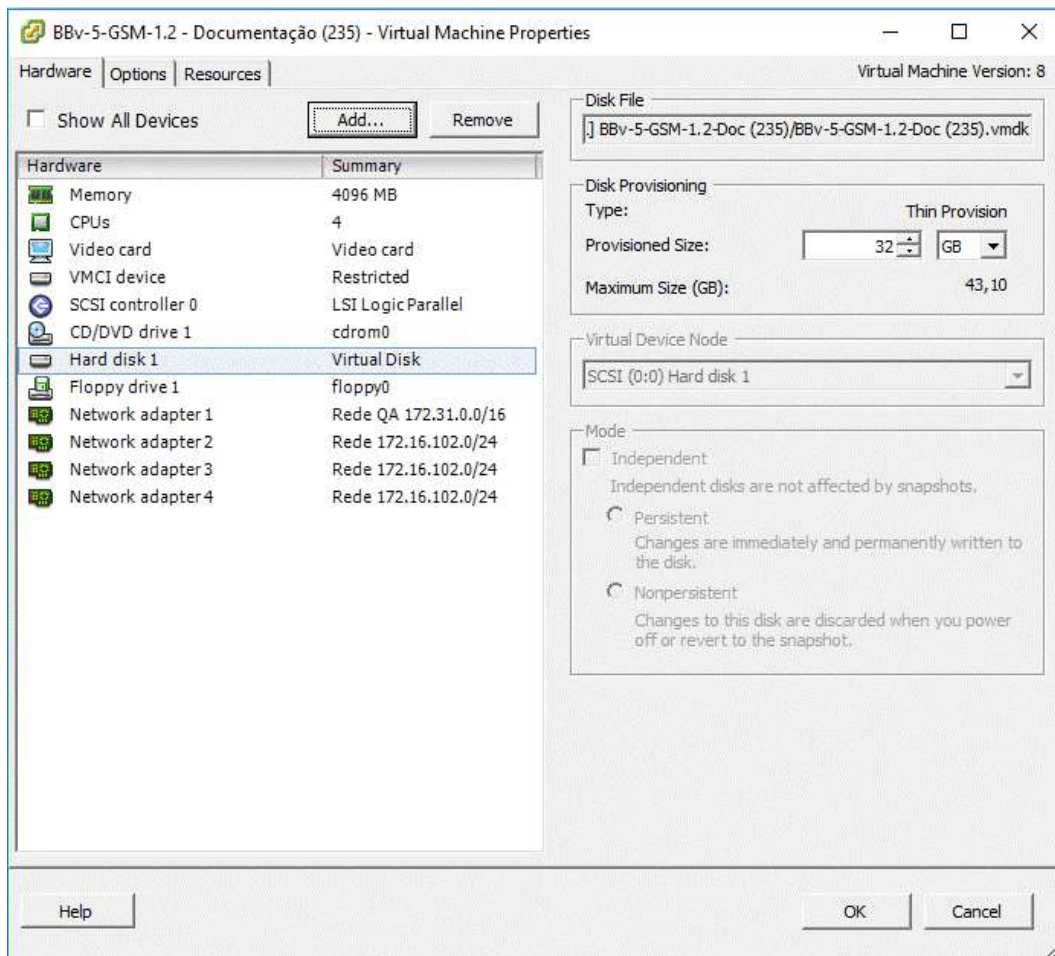


Instalação do *Logger* – Máquina Virtual

De forma a ter espaço de armazenamento em disco para a instalação do *Logger*, faremos a inserção de um *HD* na interface virtual. Clique com botão direito na máquina desejada e selecione a opção “*Edit Settings...*” conforme ilustrado pela imagem abaixo:



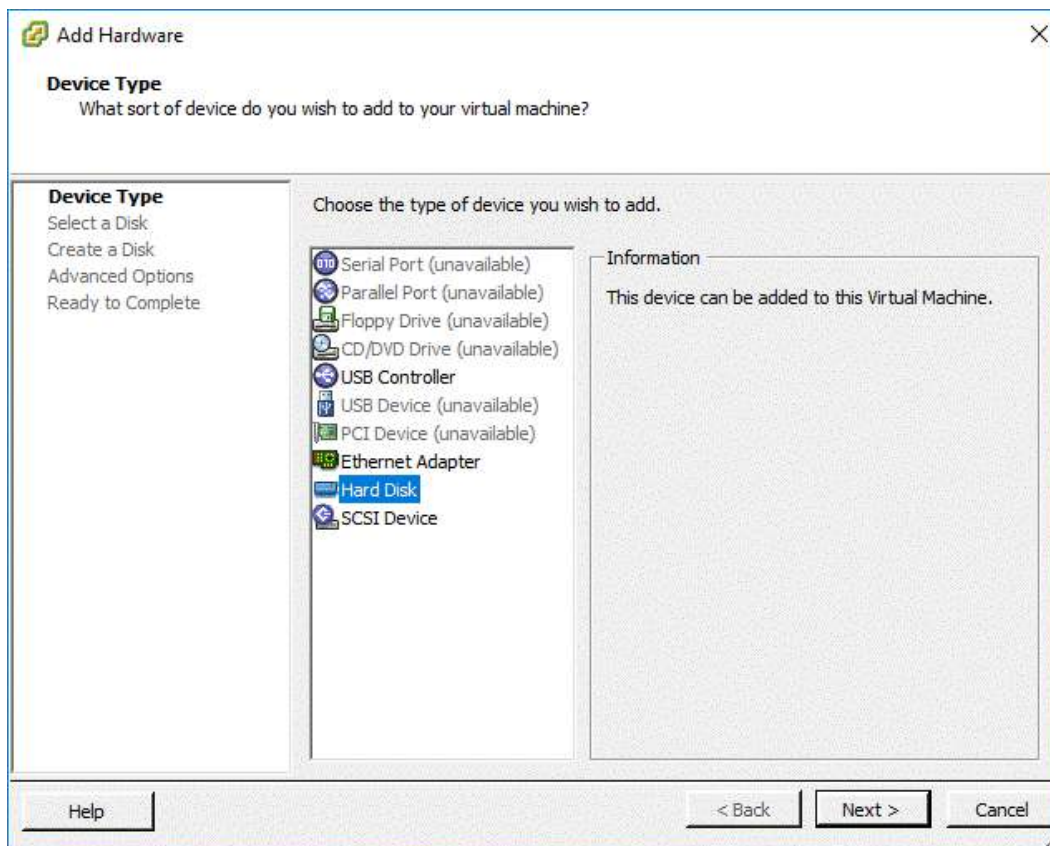
Uma tela exibindo as configurações de hardware da sua máquina virtual será exibida, conforme demonstrado pela imagem abaixo:



Máquina Virtual – *Add*.

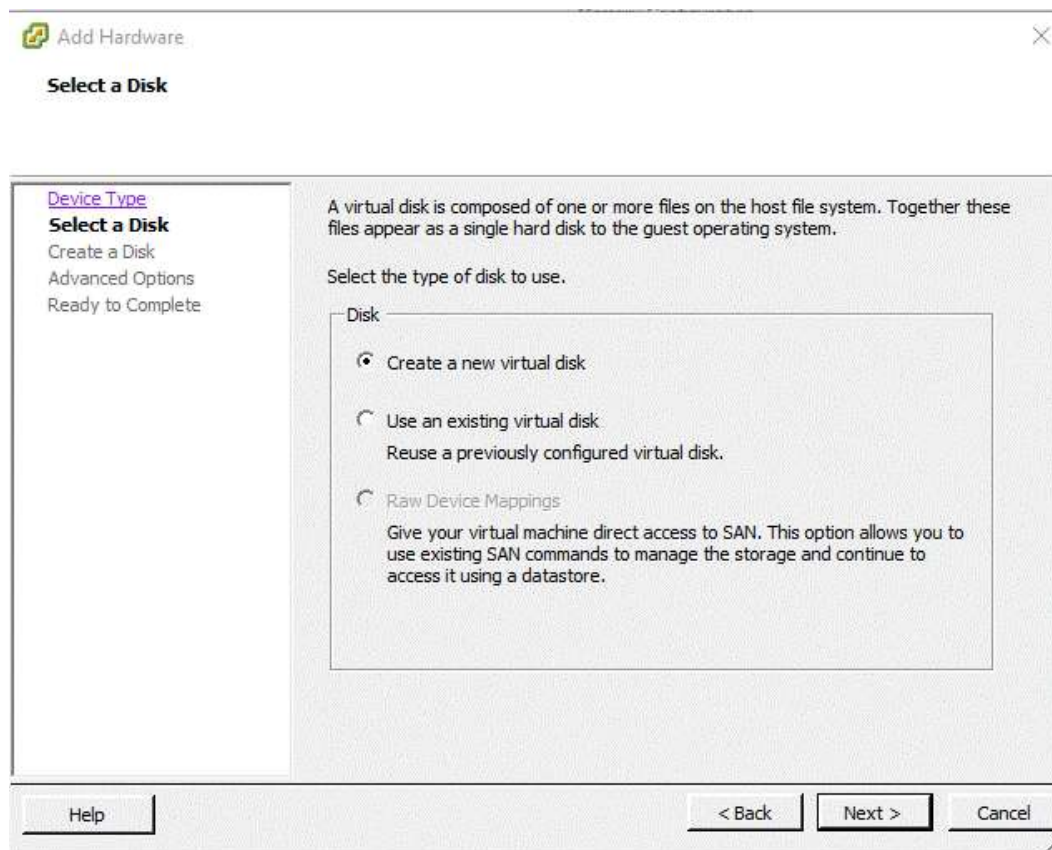
Clique no botão “Add...” localizado na parte superior da tela, do lado direito da caixa de checagem “Show All Devices”.

Uma tela requisitando o tipo de device desejado aparecerá:



Máquina Virtual – Device Type.

Selecione a opção "Hard Disk" clicando sobre o ícone na listagem no meio da tela, feito isso, clique no botão "Next" para prosseguir para a próxima etapa. Conforme demonstrado pela imagem abaixo, na próxima janela será requisitado que tipo de disco se pretende criar:



Máquina Virtual – Select Disk.

Selecione "Create a new virtual disk" caso esta opção não esteja previamente selecionada. Clique no botão "Next".

Add Hardware

Create a Disk
Specify the virtual disk size and provisioning policy

[Device Type](#)
[Select a Disk](#)
Create a Disk
[Advanced Options](#)
[Ready to Complete](#)

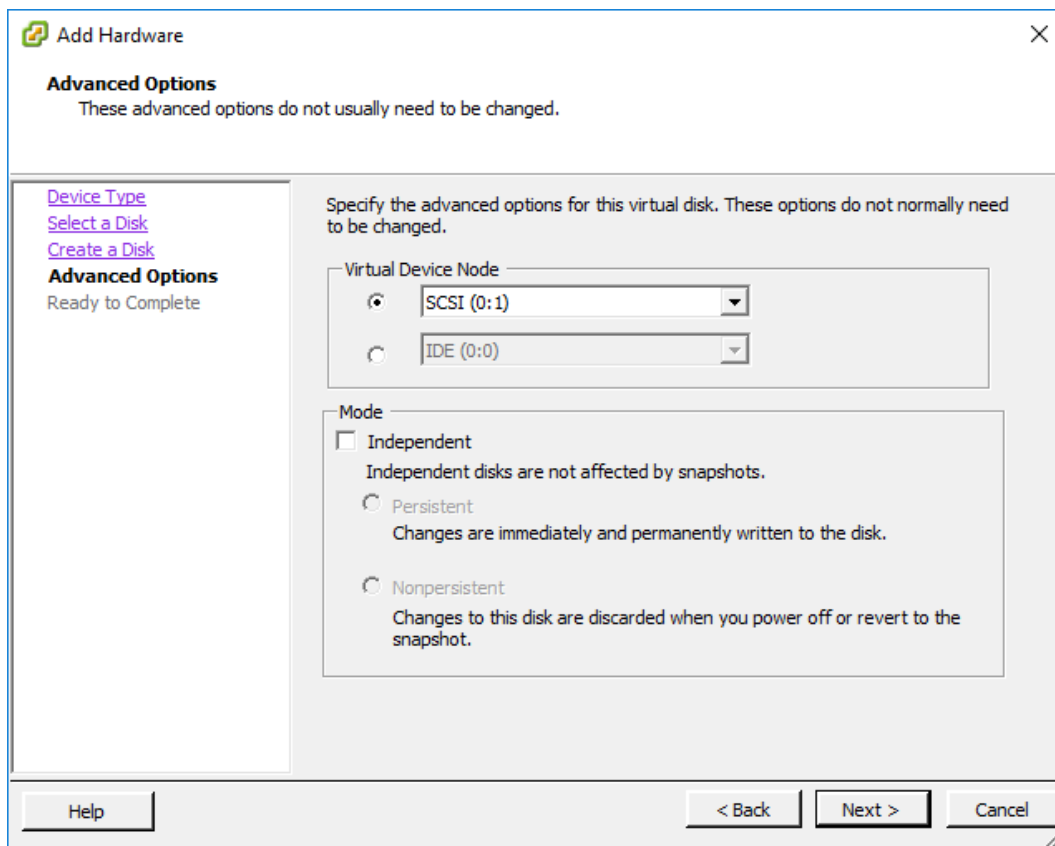
Capacity
Disk Size:

Disk Provisioning
☐ Thick Provision Lazy Zeroed
☐ Thick Provision Eager Zeroed
☒ Thin Provision

Location
☒ Store with the virtual machine
☐ Specify a datastore or datastore cluster:

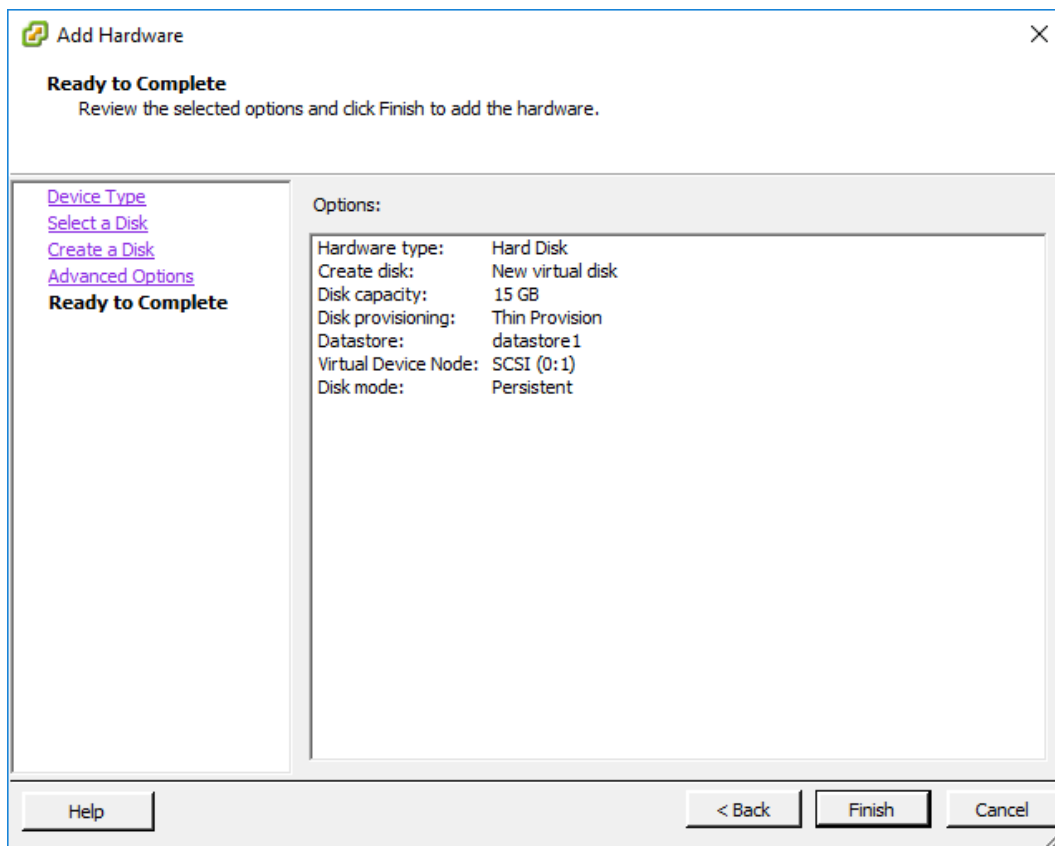
Máquina Virtual – Create a Disk.

Nesta nova janela, determine o tamanho do disco desejado em “Disk Size” e selecione a opção “Thin Provision” em “Disk Provision”. Feito isso, clique em “Next”, ignore as opções que surgirão na próxima janela (“Advanced Options”) e clique em “Next”.



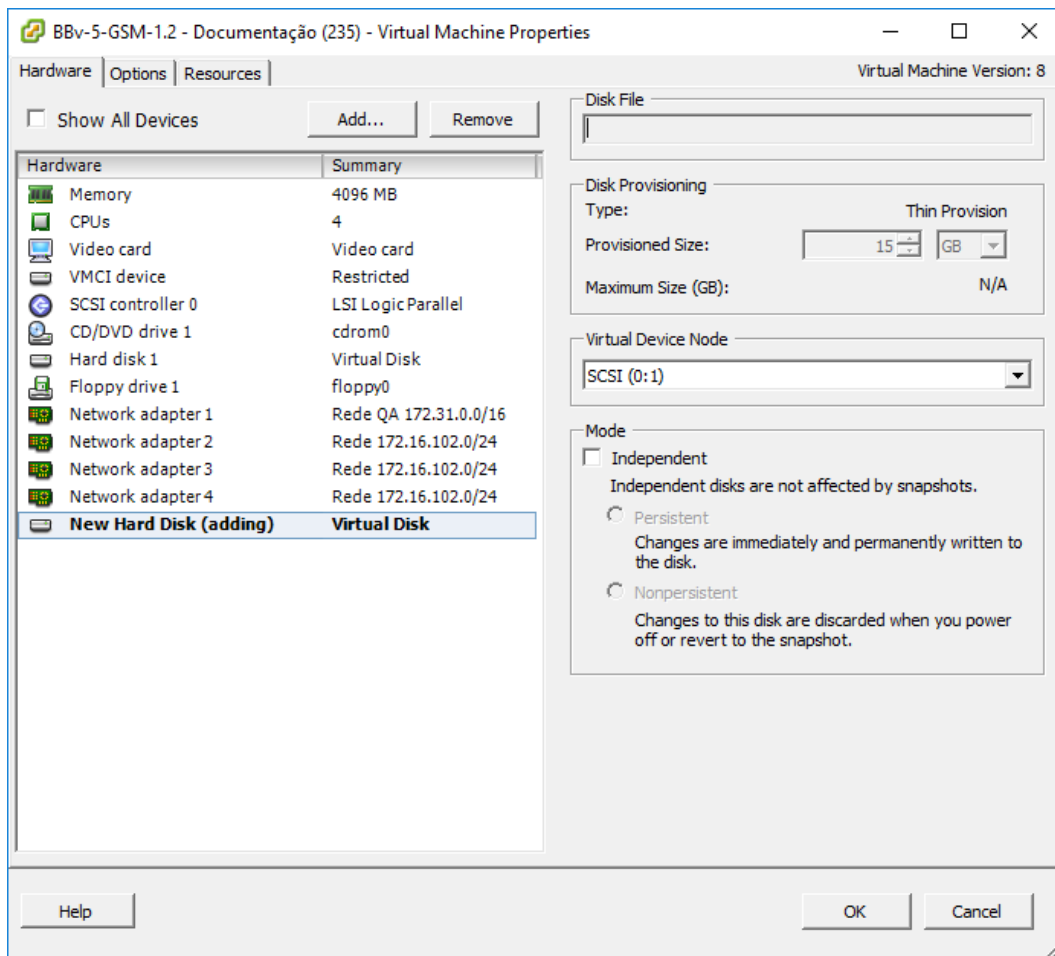
Máquina Virtual – *Advanced Options*.

Por fim a tela de finalização surgirá:



Máquina Virtual – Ready to Complete.

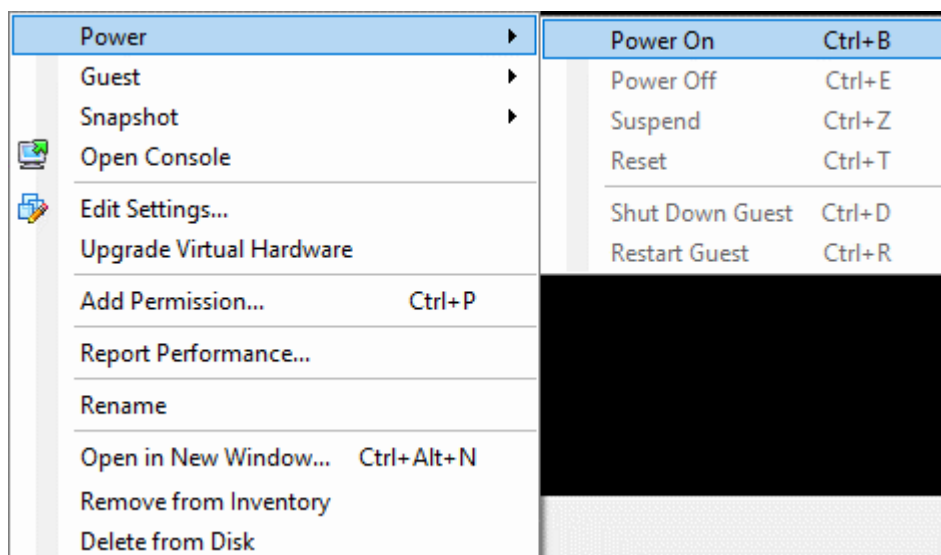
Caso todas as configurações estejam de acordo com o pretendido, clique em “Finish”, caso contrário clique em “Cancel” para cancelar o processo.



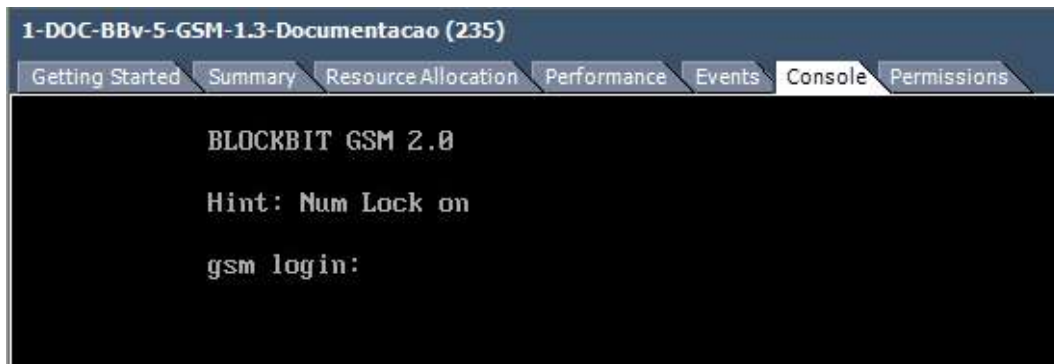
Máquina Virtual – Adding virtual Disk.

A máquina começará o processo de adicionar o disco, clique em "OK" para sair dessa tela.

Caso a máquina virtual não esteja ligada, clique com o botão direito sobre ela e selecione a opção "Power" e "Power On", a seleção desta mesma pode ser visualizada na imagem abaixo:



Após este passo, quando a máquina terminar de ser ligada clique na aba “Console” (que pode ser visualizada na imagem abaixo) ou acesse o IP da máquina através de SSH.



Máquina Virtual – Aba console.

Após efetuado o login, digite o comando CLI `"logger-config"` para iniciar o wizard de instalação do logger. Há dois modos de operação para o logger, *Standalone* e *Integrado*.



Atente que caso o usuário opte que uma chave não seja gerada quando o prompt exibir "Generate Key?", ele poderá usar o comando `"logger-key -c"` ou efetuar o `"logger-config"` mais uma vez.

O exemplo de instalação de loggers será focado no logger integrado e não no standalone, porém abaixo detalharemos rapidamente a instalação neste modo de operação:

Standalone

Neste modo de operação, o servidor é exclusivo para logger remoto, sua utilização para qualquer outra função não é possível, desta forma se fazendo necessário o uso do *firmware* da Blockbit.



É recomendável executar esse comando diretamente no console da máquina, pois durante a sua configuração a conexão SSH poderá ser perdida.



Atente que o processo de *upgrade* interfere com as interfaces configuradas em loggers do tipo *standalone*. Para mais informações sobre o comando `upgrade-blockbit`, consulte esta [página](#).

Segue um exemplo rápido de sua instalação:


```

admin >logger-config
Enter the logger operating mode: [ standalone / integrated ]: standalone
Interface (ex: eth0): eth0
IP address (ex: 1.1.1.10): 172.31.200.80
Mask (ex: 255.255.255.0): 255.255.0.0
Gateway (ex: 1.1.1.1): 172.31.0.1
Hostname (ex: logger): gsmlogger
DNS (ex: 1.1.1.2): 172.31.0.100
Timezone (ex: America/Sao_Paulo): America/Sao_Paulo

Disk /dev/sda: 128.8 GB  SYSTEM
Disk /dev/sdb: 16.1 GB  EXT4
Disk (ex: /dev/sdb): /dev/sdb
mkfs2fs 1.42.9 (28-Dec-2013)
/dev/sdb is entire device, not just one partition!
Proceed anyway? (y,n) y
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
983040 inodes, 3932160 blocks
196608 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
120 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

Generate key? [y/N]: y
Key:
53616c7465645f5f1fd31d110bfa221ae5e812311b838210546609b76aa5600820d1652f3dd95becb35ef5df77ece59527
7c3979b16741098b2329bdd5b39e0057aca51725c4c74a7ec30e34142fca78300b428fe551a89f465d73ef628dff2f910b-
3ea33e4f09f3146feb57a9fb23d2ac0e2e274acff2d6d70ba6cfef41f4e3e5499c9290ca6cf41c2b8b8eb7cc0ebd7dcfe9f
2fdefca61d98a28882b8c915d9f7e16745f4968c28ce6e030114163042744d0c1dd9000310c9f6c2ed7378f25c7592444e
84bc3a0301d6ee2a8a27cf732a938311da3cd05ebf54675fd2f5719fdbc8ec14e33d3d5e265b56806f8860d6c30e398fbc7
9b4b0c3caf417ae7fef536014aff35554d9cfe81149b819b0659730b29740b6a8d38f2daf9d85716ba1fc1f1b468732ac6f
9b23f113ac1925a38fa79e8f39f98dd8f9357774842c0bfff5a93f69c0346240b03f7cc930604634fc8a1c51af8de1248fd
7ad25b8a828e0480bee015860d75b5b4829f05f984dff115d0c8d3d66451e327ab00f67dc8f3b29475e55d25657026ac2e
f3ca8275b3eb42d2744f0c15c14bd09ff1e54078c6b3cb0bff3b8a9ce904e2b81b861da2f62b0b35b8f869505e2c9b127c
56aed9c9999ad3f180f9834c9eca59a3517708d6e2ed39515aeb87f46c635d45a3e73fcffe36ad00568d8c5f1964ce1e36f
5a2ba9f59f3b319a00a35c13f031df14cd98e0322d93adc4cae29a1ed4b362da5fe0f171d724d68449c59a99bf6d00b0f8f
22e8e3709f5ae1562948b12e3f5be5c716b0d9cd4f51b331143819c6d6e345bc10cc1bf2a9d95f40b75a1fc8eccebf94e1f
0983396d70a88596d6276234289b46bc427af1f158e25ceb39807ed37a9238d939031f2cfca4fc8a9d3a448b612ccabf54f
b8398b70e0e3c71c961c27572832024ff32e32960a3e929dcf18980f0f10ab35d8fcf399057b

Completed

Now configure the logger in administrative interface

```

Logger – logger-config - Standalone



Para mais informações a respeito de como configurar um Logger standalone, consulte esta [página](#).

Após esta etapa, basta efetuar os mesmos procedimentos na [instalação do GSM](#).

Integrated

Neste modo de operação é possível utilizar o próprio GSM local onde o *manager* estiver instalado como servidor de *logger*. Porém, é necessário dedicar um disco inteiro apenas para esta função, sendo indiferente se este mesmo será virtual ou físico.

Como exemplo, este guia executará a instalação de um *logger* integrado, como pode ser observado na imagem abaixo:

```
admin >logger-config
Enter the logger operating mode: [ standalone / integrated ]: integrated
```

Logger – logger-config.

Após selecionar a opção “*integrated*”, o sistema reconhecerá todos os discos instalados na máquina (física ou virtual) e requisitará que um deles seja selecionado para a instalação do *logger*, porém, é importante ressaltar que o disco inteiro será utilizado para tanto, assim sendo, qualquer dado que esteja armazenado nele será removido durante a instalação. Tal fato pode ser constatado pela imagem abaixo:

```
Disk /dev/sda: 34.4 GB SYSTEM
Disk /dev/sdb: 16.1 GB AVAILABLE
Disk (ex: /dev/sdb): /dev/sdb
mke2fs 1.42.9 (28-Dec-2013)
/dev/sdb is entire device, not just one partition!
Proceed anyway? (y,n) y
```

Logger – Entire device, not just one partition.

Para dar continuidade é necessário confirmar digitando “y” e dando “enter”. Feito este procedimento, o *wizard* começará a criar o *logger*, conforme demonstrado pela imagem abaixo:

```
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
983040 inodes, 3932160 blocks
196608 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
120 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

Logger – Criando Logger.

Após estes passos, o sistema questionará se deseja que a chave secreta seja gerada, é recomendável confirmar com “y”, copiar essa informação e guardá-la em um local seguro. A única forma de reaver esta chave é utilizando o comando “*logger-key*” na CLI (para mais informações acesse este [link](#)), a imagem abaixo demonstra o processo de criação de uma chave secreta:

```
Generate key? [y/N]: y
Key:
53616c7465645f5f07f0a3aef40c61f07096ce46f9a00e2547017356a39f0db0c10aead6f64100110dcb9ddf5d49d90504f02252db75d20da5f751b273d90c3a196a353
2c55f8a41bbf4608c6330a0fcbb4c73cfac72bacbf5d67f85b27a888c9d33da3cd8854f7b45f249c84f54daa4bbdfeffc1fe2babc75818c919ddcb4d5bf09c158e97aac
d5cb485accd0a9c0d0d3374bab8e5e5ad65c08c8758788c7c75d0a23ddc0a0b7f1f844f63234620ddd447b402b4db79887a5e2bca15b76c2280fc7d2daa84bb78d1
5c58dfb7e4f012a04bb523c962b7038d55d2afc3c24126b6e1ddfd02e9e325d9bb9e0c222edd91be2f02738324475cc19cafff4ed24325808d41360ff1ca5b57f275bebb
0827f116428f9ab1ac4dd77a60a5397f5fea906c4702cddb93a8c661b4f7ea6473fafb66dcf04ea4f1159f097234b62feada09efe2375ea3841f01aca37a7b4a04e77ec
b4956b555b51356d0f1b1f198e772dde47da4f318706fcf7122f0e80651e32761f0e6b3c853e9d93beaeb7b5cc0cbfb57c44b6ccasb38e4b79a26f9de9379ef4ead81401
5b8ad768a826118980e0d9f6583fb7d2b6c0d0a1d3a49dc0a57ed33115a0b506e3d75836ba2c0b3a3e7a2242225d702e0df01c0ea367d5048c7863d085abf8d6bedccf23
f4cca62c90ab90574b3d98b7988ec2881d4055c37b0738771dc080208c64e9eb0c8c484039a9e7a72b08c90902f094983f2f8206228c05654128ae7f901e718f35163daf5
bf45ed074f92ca3e25a12c29f94da9a8ac83b2a80aa9276c836835915fe78617a4be0cd04f1bda1c0f7cb9bd2791ede465967283865cc73f0bf3d7b8c65af31c3a8a3d6
fc762dacc09bc767736946f334e94ec758d126f476e713b3e4f368f234be3357ef1b190d3f8febd50f15764b5c703012ad7aaeebbcb62bb23db0f5d10b3ac0cd996029b951
0e7d5b
```

Logger – Secret Key.

Após este passo, conforme pode ser observado graças a mensagem do próprio *wizard* o *Logger* já está instalado no GSM.

```
Completed  
Now configure the logger in administrative interface  
admin >|
```

Logger – Completed

A etapa utilizando a *CLI* foi completada com sucesso. O próximo passo será na interface administrativa do GSM:

Configuração da Logger na interface administrativa/manager do GSM

Efetue o *login* através do navegador.



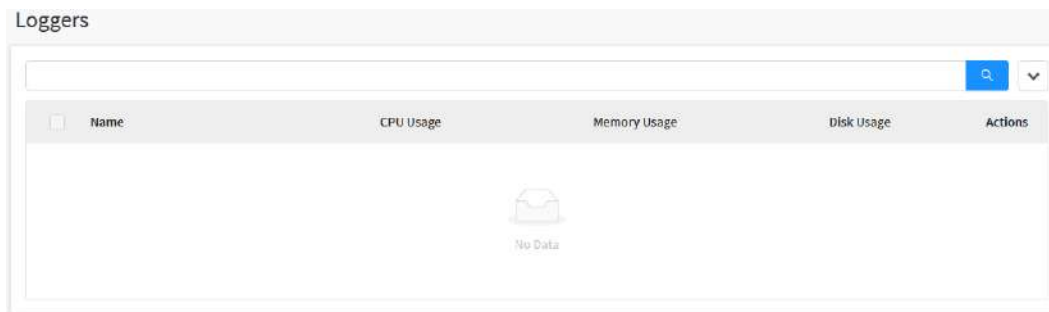
GSM – Login.

Clique no botão "*Loggers*" no menu vertical a esquerda.



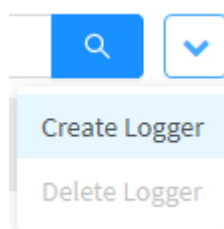
Loggers

A seguinte tela será exibida:



Loggers – Loggers

Adicione um *logger* selecionando o **menu de ações** [] e clicando na opção "Create Logger":



Loggers - Actions Menu - Create Logger

O seguinte formulário será exibido:

Loggers – Create Logger Device

Complete os campos conforme o padrão (para mais informações acesse este [link](#)):



Esta tela levará em torno de 40 segundos para exibir os *status* das *loggers*.

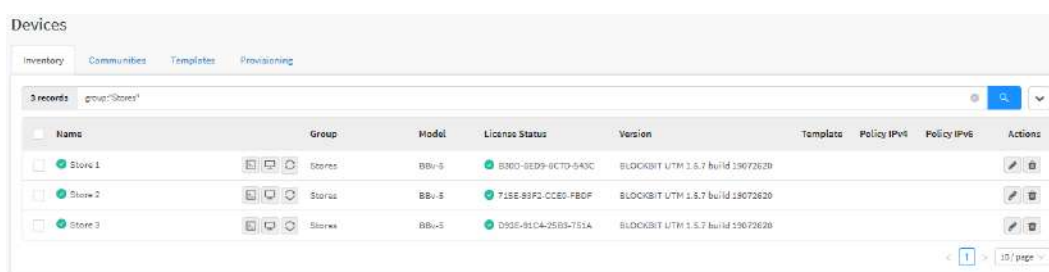
Durante este intervalo de tempo são criadas as configurações essenciais do *logger*.

O próximo passo é conectar o *Logger* aos dispositivos. Para tanto, acesse a opção **Devices** localizada no menu lateral à esquerda.



GSM – Devices

Neste exemplo, o *Logger* será aplicado aos UTM's das *Store* 1, 2 e 3. Clique ou busca o nome do grupo, neste caso "Stores"

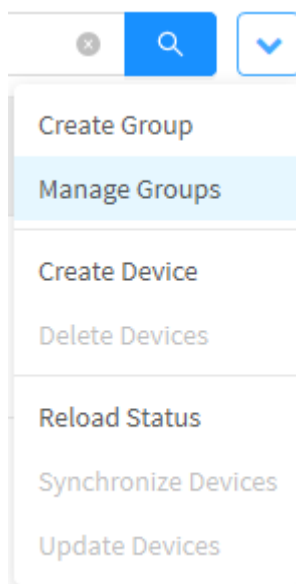


Name	Group	Model	License Status	Version	Template	Policy IPv4	Policy IPv6	Actions
Store 1	Stores	BBu-S	B300-8ED9-8C7D-843C	BLOCKBIT UTM 1.5.7 build 19072620				[Edit] [Delete]
Store 2	Stores	BBu-S	715E-93F2-CC60-FB0F	BLOCKBIT UTM 1.5.7 build 19072620				[Edit] [Delete]
Store 3	Stores	BBu-S	D93E-91C4-25B3-7514	BLOCKBIT UTM 1.5.7 build 19072620				[Edit] [Delete]

GSM – Stores



No **menu actions** [], selecione a opção "Manage Groups".



Menu Actions - Manage Groups

A seguinte tela será exibida:

Manage Groups

4 records

☐	Name	Description	Devices	Actions
☐	Branch Office	Branch Office device group	1	
☐	Head Office	Head Office device group	1	
☐	Pool Web Filters	Webfilter device group	3	
☐	Stores	Store device group	3	

<

1

>

Done

Manage groups

Selecione o grupo desejado e clique no botão **edit**  a seguinte janela aparecerá:

Edit Group

*

Name

Stores

Description

Store device Group

Devices

Store 1 X

Store 2 X

Store 3 X

Logger

Cancel

Save

Manage Groups – Edit Group

Selecione o *logger* adequado, conforme exemplificado abaixo:

Edit Group
X

* Name

Stores

Description

Store device Group

Devices

Store 1 X Store 2 X Store 3 X

Logger

Logger

Cancel
Save

Manage Groups – Edit Group - Logger selecionado.

Clique no botão **save**  para finalizar a edição.

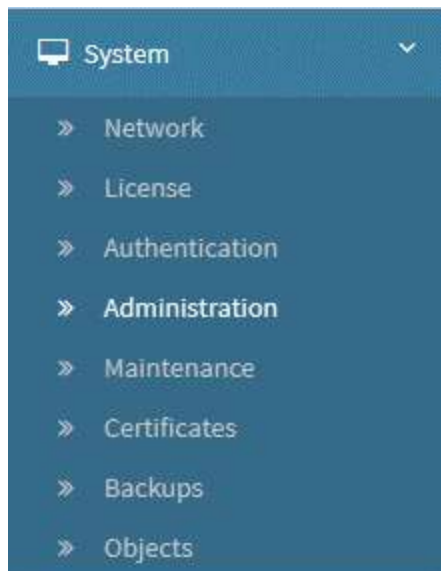
 **Group updated with success!**
Group updated with success

Com isso, todos os dispositivos do grupo se utilizarão do *logger* selecionado.

Após efetuar este processo, clique no ícone **Access Interface Web**  para acessar o UTM desejado.

Caso seja necessário, efetue o login.

Vá em “System” e clique na opção “Administration” conforme exemplificado pela imagem abaixo:



UTM – System - Administration

Acesse a aba “Central Management”:

UTM – Central Management

Marque a caixa de checagem “Enable Analyzer”, em “Analyzer Address” digite o IP do GSM (ou o IP do Analyzer caso este seja Standalone), em “Logger Service”, digite o serviço do logger. Feito isso, clique no ícone **save**  e acesse a fila de tasks clicando no ícone de **Fila de configurações**  **salvas**  e dê o *apply* das configurações. Caso tudo ocorra corretamente, o “Status” (do lado direito de “Analyzer Address”) será alterado para “Online”.

Retornando ao GSM, novamente volte a acessar os “Loggers”. Agora é possível observá-los atuando normalmente, conforme demonstrado abaixo.

Loggers

1 records

Name	CPU Usage	Memory Usage	Disk Usage	Actions
☐ Logger	4 core(s) 0%	7.8 GB 76%	14.64 GB 5%	  

< 1 > 10 / page

Logger Devices

O *Logger* foi conectado aos dispositivos com sucesso.

Par mais informações a respeito das colunas deste painel, consulte esta [página](#).

À seguir vamos analisar os componentes do [Menu de Ações](#), para demonstrar como [criar](#) e [remover](#) um *Logger*;

Loggers - Clusters

A aba "Clusters" permite a configuração do serviço de Alta Disponibilidade dos servidores de armazenamento de logs, possibilitando que o administrador defina servidores de logger redundantes, sendo que estes possuem também a funcionalidade de replicar automaticamente e em tempo real os logs do cluster primário para o secundário. A importância deste recurso é garantir a disponibilidade do serviço e efetuar *failover*, caso seja detectada alguma discrepância na rede o servidor secundário é ativado, substituindo o primário e garantindo que a coleta de *logs* dos devices vinculados continuem funcionais.



ATENÇÃO: Para configurar o H.A. os seguintes requisitos devem ser observados:

É obrigatório que os dois servidores tenham as mesmas capacidades computacionais (Memória, Processador, Armazenamento e etc), os mesmos modelos e mesmas versões, independente de ser um appliance físico ou virtual.

A funcionalidade de H.A. nas configurações da Manager só poderá ser habilitada quando não houver um Logger local integrado.

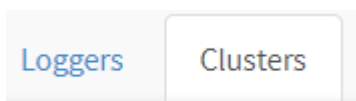


Caso o *logger* esteja em *standby*, o armazenamento externo é interrompido, os *backups* só voltarão a ocorrer quando o *logger* estiver ativo.



O GSM suporta um máximo de 125 clusters configurados.

Para configurar este recurso, clique na aba "Clusters":



Aba Clusters

Surgirá a tela à seguir, conforme demonstrado pela imagem abaixo:

Loggers - Clusters



Atente que em sistemas com versão inferior à 2.1.0, não é possível utilizar *cluster* de *loggers* no modo standalone.

Para utilizar Cluster de loggers será necessário utilizar loggers com a versão 2.1.0 e posteriores.

Nesta sessão iremos analisar:

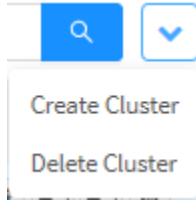
- Como [criar](#), editar e [remover](#) um cluster;
- [Os componentes da coluna](#);

A seguir analisaremos o [menu de ações](#).

Clusters - Menu de Ações



Ao clicar no botão **menu de ações**] no topo direito é possível adicionar um *Cluster* ou removê-lo.



Clusters – Menu de ações

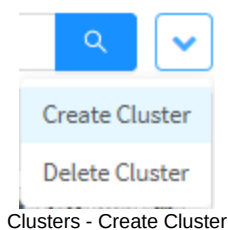
O menu é composto das seguintes opções:

- [Create Cluster](#);
- [Delete Cluster](#).

A seguir cada opção do menu de ações será detalhada.

Clusters - Menu de Ações - Create Cluster

Atente que o sistema não permitirá cadastrar logger já utilizadas em outro cluster, loggers integradas ou com versões anteriores à 2.1.0. Para criar um Cluster para o Logger, clique na opção "Create Cluster" do menu de opções, como demonstrado abaixo:



Neste painel estão todas as configurações do *Cluster* utilizado pelos recursos de alta disponibilidade do *Logger*, a seguir iremos nos aprofundar em como configurar cada campo.

Create Cluster

X

* Name

* Secret Key

* Primary Logger

* Replica Logger

* Virtual IP

* Netmask

* Heartbeat Interval (seconds)

5

* Failover Threshold

5

☐ Notifications to e-mail ⓘ

☐ Auto Activation Replica

Cancel

Save

Clusters - Create Cluster

Ao criar um cluster de H.A. de Logger o administrador deverá informar os seguintes parâmetros de configuração:

- **Name:** Define o Nome que será utilizado para identificar o cluster. Campo obrigatório;
- **Secret Key:** Define a chave secreta do *cluster* de alta disponibilidade. A definição desta senha é obrigatória, de forma a garantir a relação de confiabilidade entre ambos os dispositivos;
- **Primary Logger:** Define o *logger* que será utilizado como *cluster* primário. Os itens que aparecem neste campo são configurados na aba *Logger*, consulte esta [página](#) para mais informações. Este campo é obrigatório;

- **Replica Logger:** Define o *logger* que será utilizado como *cluster* secundário. Os itens que aparecem neste campo são configurados na aba *Logger*, consulte esta [página](#) para mais informações. Evidentemente a réplica não poderá usar a mesma *logger* selecionada para o *cluster* primário. Este campo é obrigatório;



Nos campos *Primary* e *Replica logger*, só serão listados os *loggers* que não estejam sendo utilizados como *cluster* no momento, além disso, o sistema não permitirá cadastrar *loggers* do tipo *integrated* ou que utilizem versão anterior à 2.1.0.

- **Virtual IP:** Define o endereço IP virtual que será associado ao *cluster* de Alta disponibilidade. A configuração do endereço IP usado pelo cluster do serviço de alta disponibilidade suporta apenas *IPv4*. Este campo é obrigatório. IP Virtual deverá ser adicionado aos Blockbit Next Generation Firewall como endereço de *analyzer* para o uso de redundância de *Loggers*, para mais informações, consulte esta [página](#);



Atenção: Mesmo que o *firewall* esteja configurado para usar um *IP* real, caso ele esteja em *cluster*, ainda assim ele será replicado para servidor secundário. Porém, ainda considerando esta situação, caso o servidor falhe, ele não irá transmitir *logs* para o servidor secundário.

- **Netmask:** Determina a máscara de rede que será utilizada pelo endereço *IP* virtual. Este campo é obrigatório;
- **Heartbeat Interval:** Determina o intervalo de monitoramento, definindo quando serão feitos os testes de conexão e sincronismo entre os dispositivos. Este campo é obrigatório;
- **Failover Threshold:** Determina o limite de falhas nos testes de *Heartbeat*, caso o valor máximo de erros gerados pelos testes de *Heartbeat* seja alcançado, o *Logger* secundário será ativado e o primário entrará em *standby* efetuando o *failover* automaticamente. Este campo é obrigatório;
- **Notifications to E-mail** ☐: Caso a caixa de checagem esteja habilitada, o administrador poderá cadastrar um endereço para recebimento de e-mails de notificações, as mensagens serão enviadas em tempo real em eventos de *Failover* e sincronismo. Além disso, o idioma utilizado pelo e-mail, não é o mesmo que estiver sendo utilizado na interface e sim o que for configurado no sistema, para mais informações, consulte esta [página](#). Para que o envio das notificações seja efetuado, é necessário configurar a aba *e-mail* em *Network*, para mais informações, consulte esta [página](#);



Ao alterar o idioma, mantenha os dois *Loggers* ligados, caso contrário, a configuração não será sincronizada para o *Logger* que estiver desligado.

Caso tenha alterado o idioma no menu *System*, aba *General*, opção *Settings* no campo *Language*, será necessário salvar novamente o cluster para passar a receber e-mails no novo idioma selecionado.

- **Auto Activation Replica** ☐: Caso a caixa de checagem estiver habilitada, o *failover* do *logger* primário pelo secundário será feita automaticamente. A ativação da *Logger* Primária é feita manualmente através do botão *Active Primary Logger*, para mais informações consulte esta [página](#).



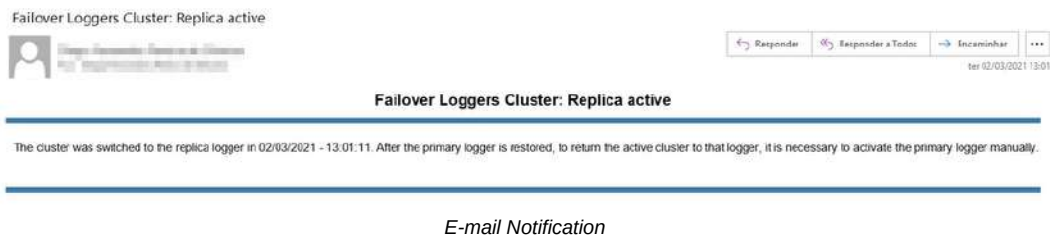
Atenção: Para garantir a gravação do *backup* quando o servidor secundário estiver Ativo, é recomendável certificar-se de que a rotina de *backup* automática no servidor secundário está ativa. Para mais informações, consulte esta [página](#). O servidor Secundário não gravará os *backups* no armazenamento externo enquanto estiver em *standby*.

Save

Cancel

Para finalizar a criação do *cluster*, clique em [Save]. Caso queira cancelar, clique em [Cancel].

Ao ter criado o *Cluster* corretamente e tendo o campo *Notifications to E-mail* corretamente configurado, o administrador será notificado todas as vezes que o servidor de *logger* secundário for ativado, conforme demonstrado abaixo:



À seguir iremos detalhar a opção [Delete Cluster](#).

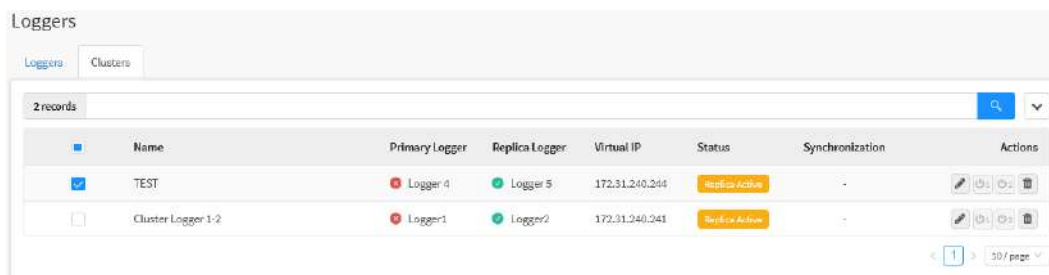
Clusters - Menu de Ações - Delete Cluster

Através do botão "Delete Cluster" é possível deletar os *Clusters* selecionados. Para deletar pelo *Menu de Ações*, siga os seguintes passos:



Após a exclusão do *Cluster*, o *Blockbit Next Generation Firewall* irá interromper o envios de *logs*, pois o IP virtual cadastrado, passou a não existir, entrando assim no status de "STOPPED".

1. Selecione qual(is) *Cluster(s)* deseja deletar. Para selecionar, basta clicar com o *mouse* no *checkbox* que fica localizado ao lado do *Name*. Nos *clusters* selecionados o *checkbox* mudará da cor branca para azul [];

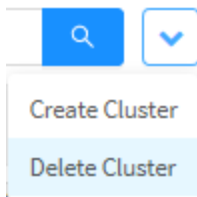


☒	Name	Primary Logger	Replica Logger	Virtual IP	Status	Synchronization	Actions
☒	TEST	Logger 4	Logger 5	172.31.240.244	Active/Active	-	  
☐	Cluster Logger 1-2	Logger1	Logger2	172.31.240.243	Active/Active	-	  

Clusters – Seleção dos *Clusters* para deletar

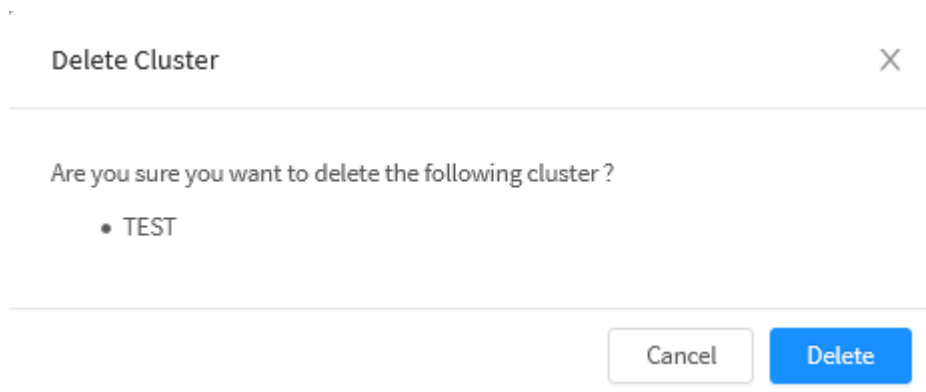


2. Entre no **menu de ações** [] e clique na opção "Delete Profile".



Clusters - Delete Cluster

3. Surgirá a mensagem de notificação questionando se deseja realmente deletar os *Clusters* selecionados:



Clusters - Delete Cluster

Cancel

Delete

Caso desejar cancelar clique no botão []. Para concluir, clique no botão [].



Cluster deleted successfully

Cluster deleted successfully

Após realizar esses procedimentos, os *Clusters* terão sido deletados com sucesso.



Após deletar o *cluster*, as *loggers* vinculadas voltarão a ficar disponíveis para edição e uso como um *logger normal*.

À seguir, detalharemos os componentes das [colunas](#).

Clusters - Colunas

A seguir detalharemos cada coluna da aba *Clusters*:

	Name	Primary Logger	Replica Logger	Virtual IP	Status	Synchronization	Actions
☐	Cluster Logger 4-5	Logger 4	Logger 5	172.31.240.244	Replica Active	61%	
☐	Cluster Logger 1-2	Logger1	Logger2	172.31.240.241	Primary Active	-	

Loggers - Aba Clusters

- **Select**: Permite selecionar um ou mais *clusters*;
- **Name**: Exibe o nome do *Cluster* de *Loggers*;
- **Primary Logger**: Exibe o nome e o status da conexão do servidor Primário, podendo ser:
 - : Representa que o *logger* está *online*;
 - : Representa que o *logger* está *offline*;
- **Logger Replica**: Exibe o nome e o status da conexão do servidor Secundário, podendo ser:
 - : Representa que o *logger* está *online*;
 - : Representa que o *logger* está *offline*;
- **Virtual IP**: Exibe o IP Virtual adicionado em [Create Cluster](#);
- **Status**: Esta coluna exibe o estado atual dos *Loggers*, podendo ser:
 - : Representa que o *logger* primário está *ativo*;
 - : Representa que o *logger* secundário está *ativo*;
- **Sync Progress**: Exibe a barra de progresso do sincronismo entre os *clusters*;
- **Actions**: Disponibiliza as seguintes funções essenciais:
 - **Edit**: Permite editar um dos servidores criados na opção [Create Cluster](#) no menu de ações;
 - **Active Primary Logger**: Este botão permite ativar manualmente o *cluster* primário;
 - **Active Replica Logger**: Este botão permite ativar manualmente o *cluster* secundário;
 - **Delete**: Permite deletar um *cluster*, é o equivalente a opção [Delete Cluster](#) do menu de ações.



Após um ativamento manual ou após a detecção do *Failover*, a *interface* secundária leva no mínimo 30 segundos para ser ativada.

Apesar disso, o sincronismo pode demorar um tempo muito maior dependendo da quantia de informações e da estrutura da rede do administrador.

Para informações mais detalhadas sobre o processo de sincronismo, é possível acompanhar o progresso através do comando de CLI [\[debug-ha\]](#).

Além do *status* e da barra *sync progress* é possível consultar o estado do sincronismo e ativamento do *clusters* de *Loggers* acessando a CLI e utilizando o comando de [\[debug-ha\]](#);

```
admin >debug-ha
date="2021-03-02 17:20:50" status="threshold" status_message="peer error 4/5"
date="2021-03-02 17:20:57" status="threshold" status_message="peer error 5/5"
date="2021-03-02 17:21:00" status="failover" status_message="can't connect to primary logger"
date="2021-03-02 17:21:01" status="error" status_message="Sync peer connection error, progress: 0%"
date="2021-03-02 17:21:05" status="failover" status_message="secondary server, new status: active"
```

CLI - *debug-ha*

Ao fazer a ativação dos Loggers manualmente, é gerado um log de auditoria, que pode ser analisado no menu Settings, opção Administration, na aba [Audit Log](#), conforme demonstrado na imagem à seguir:

Administration

Administrators Users Profiles Auth Servers Identity Provider **Audit Log**

137 records

Date	User	Interface	Activity	IP	Actions
2021-03-05 09:50:13	admin	loggers-clusters	Update	192.168.200.5	
2021-03-05 09:50:11	admin	loggers-clusters	Update	192.168.200.5	
2021-03-05 09:29:13	admin	loggers-clusters	Update	192.168.200.5	
2021-03-04 15:37:48	admin	loggers-clusters	Update	192.168.111.77	
2021-03-04 15:05:30	admin	loggers-clusters	Edit	192.168.111.77	
2021-03-04 15:03:48	admin	loggers-clusters	Edit	192.168.111.77	
2021-03-04 15:02:34	admin	loggers-clusters	Edit	192.168.111.77	
2021-03-04 12:34:02	admin	loggers	Delete	192.168.111.77	
2021-03-04 12:33:58	admin	loggers	Delete	192.168.111.77	
2021-03-04 12:31:53	admin	loggers-clusters	Delete	192.168.111.77	

< 1 2 3 4 5 ... 14 > 10 / page

Administration - Audit Log

Quando a ativação de um dos *loggers* é realizada, o evento de atividade é listado como *update*. É possível consultar mais informações sobre clicando no botão .

Audit View ×

```

{
  "Audit Information": {
    "logger_id": "4"
    "logger_name": "Logger 5"
    "activate-logger": true
  }
}

```

Close

Audit Log - Audit view

Como demonstrado na imagem acima, ao efetuar a ativação manual, a linha *"activate-logger"*, ficará marcada como *"true"*;

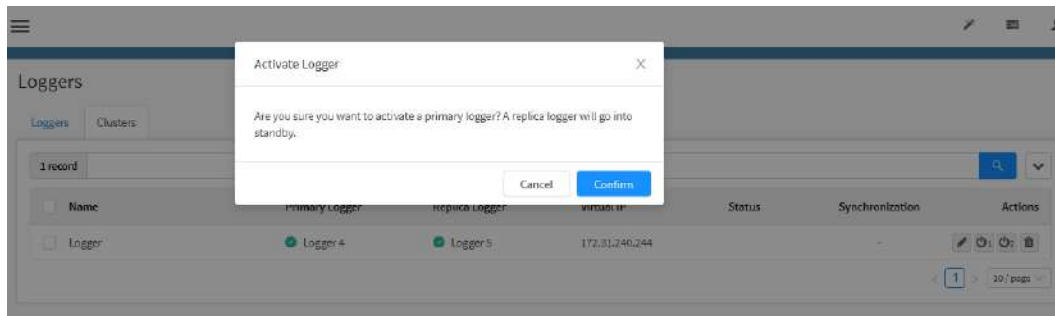
Para mais informações sobre os *loggers* consulte esta [página](#).

Clusters - Active Primary Logger

Ao clicar no botão **Active Primary Logger**  uma mensagem de confirmação será exibida na tela, conforme demonstrado abaixo:



Como mencionado no *e-mail* recebido em um evento de *failover*, a *logger* primária deverá ser ativada manualmente quando houver garantia de que a mesma está estável, evitando assim a perda de *logs* durante a instabilidade.



Clusters - Activate Logger

Clique em  para ativar o *Logger* Primário manualmente e deixar o *Logger* secundário em *Standby*. Caso contrário, clique em  para fechar esta janela.

Ao ativar o *logger*, a seguinte confirmação será exibida:

 **Logger activated successfully. Wait the synchronization to finish in a few minutes.**

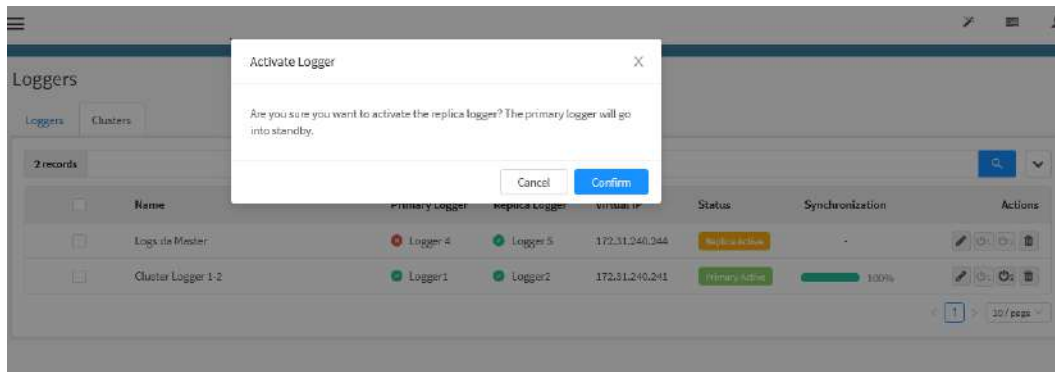
Mensagem de ativação do *Logger*

O procedimento descrito nesta página é muito similar ao efetuado no botão [Active Replica Logger](#).

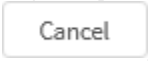
Para mais informações sobre as outras opções exibidas nas colunas em *Clusters*, consulte esta [página](#).

Clusters - Active Replica Logger

Ao clicar no botão **Active Replica Logger**  uma mensagem de confirmação será exibida na tela, conforme demonstrado abaixo:



Clusters - Activate Replica Logger

Clique em  para ativar o *Logger* secundário manualmente e deixar o *Logger* primário em *Standby*. Caso contrário, clique em  para fechar esta janela.

Ao ativar o *logger*, a seguinte confirmação será exibida:

 **Logger activated successfully. Wait the synchronization to finish in a few minutes.**

Mensagem de ativação do *Logger*

O procedimento descrito nesta página é muito similar ao efetuado no botão [Active Primary Logger](#).

Para mais informações sobre as outras opções exibidas nas colunas em *Clusters*, consulte esta [página](#).

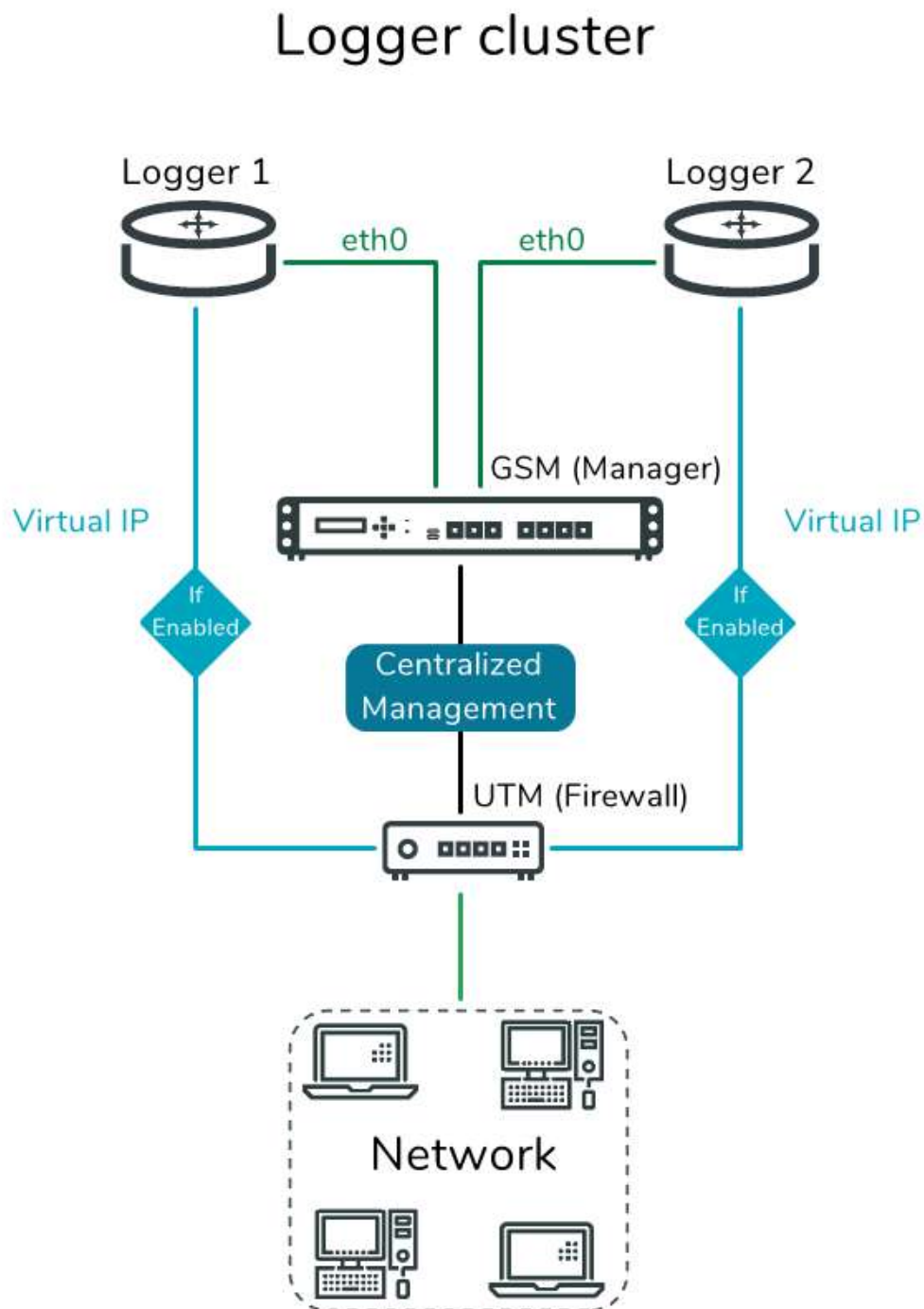
Clusters - Exemplo

Esta seção irá apresentar o passo a passo para configuração de um Logger primário e secundário em Cluster.



Para mais informações a respeito de *Clusters de Logger* consulte esta [página](#).

Essa demonstração considerará a seguinte estrutura:



Cluster de Logger - Estrutura

Os seguintes *IPs* serão utilizados neste exemplo:

Cluster de Logger - Endereçamento IP

Nome	Endereço <i>IP</i>	IP Virtual
Primary Cluster	172.31.240.1	172.31.240.241
Secondary Cluster	172.31.240.2	

Os passos que tomaremos nesta demonstração serão:

- [Configuração das Interfaces e Loggers](#);
- [Configuração dos Clusters](#);
- [Validação das Configurações](#).

Iniciaremos a demonstração configurando as [Interfaces e Loggers](#).

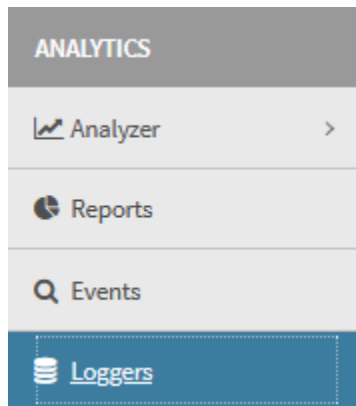
Clusters - Configuração das Interfaces e Loggers

Neste exemplo efetuaremos as seguintes configurações:

- Primeiramente, é necessário Instalar os *loggers* que serão utilizados, siga as orientações desta [página](#) e armazene a chave secreta em um lugar seguro;
- Configuração dos *loggers*.

Configurações dos Loggers

Acesse o menu Analytics e clique na opção *Loggers*:



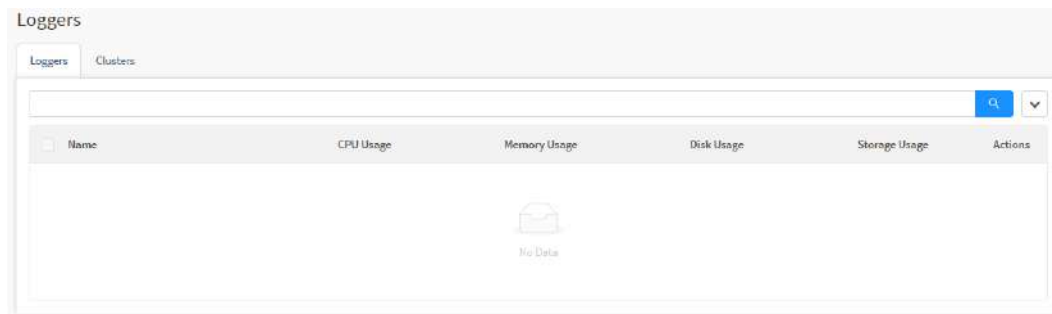
Analytics - Loggers

Clique na aba *Loggers*:



Aba Loggers

A seguinte tela será exibida:



Loggers - Loggers

À seguir detalharemos os painéis que serão configurados.

Logger Device

Complete o formulário conforme exemplificado a seguir:

Create Logger Device

Settings

Storage

General

* Name

Logger 1

* Mode

Standalone

* Description

Logger 1

* Interface

eth0

* Address

172.31.240.1

* Secret Key

53616c7465645f5f4acdb42d25e6c954fb6629ebed20d33fa393d37661d56d7aea665beb18045ed40e1f04c4007a3fecb9b5ab6ee20ebc0de9f86845797e25fe0df00ff40984613fdb94dd8985eea409ca2ee4526e3d9516d879f1b0b08aa91bab28249e9cdf29f7d7212a072cd0ff

Devices & Devices Group

Select a type

Cancel

Save

Loggers - Create Logger Device

- **Name:** Nomearemos o *logger* como "Logger 1";
- **Mode:** Utilizaremos um logger "*Standalone*";
- **Description:** Como descrição simplesmente digitaremos "Logger 1";
- **Interface:** Neste campo é adicionada a mesma interface que foi configurada no processo de instalação da *logger*;
- **Address:** Neste campo é adicionado o *IP* que foi configurado ao instalar o *Logger*, neste exemplo usaremos o IP 172.31.240.1;
- **Secret Key:** Neste campo deve-se colar a chave secreta que foi gerado ao instalar o *Logger*;
- **Devices & Devices Group:** Adicione os *devices* do *inventory* que deseje utilizar com o *logger*. Este exemplo não irá considerar essa etapa.

Não configuraremos os outros campos, clique em

Save

 para gravar as configurações.

A seguir, iremos configurar a *Logger* secundária, usaremos as seguintes configurações:

697

Edit Logger Device

X

Settings

Storage

General

* Name

Logger2

* Mode

Standalone

* Description

Logger 2

* Interface

eth0

* Address

172.31.240.2

* Secret Key

53616c7465645f5f40eae74aa339f6937fa8dc535c63931cf9a7d4dd1e78b122330e94
b6d2ab42a90061be740b04ead3e786c8db8efb6bd58ff4d0fa8680d228027e37512585
c6c0380e997dd4f8002c081ba35341bf5e992bd327e051c66c3c09f280d59eb46472610

Devices & Devices Group

Select a type

+

UTM211

-

Cancel

Save

Loggers - Create Logger Device

- **Name:** Nomearemos o *logger* como "Logger 2";
- **Mode:** Utilizaremos um logger "*Standalone*";
- **Description:** Como descrição simplesmente digitaremos "Logger 2";
- **Interface:** Neste campo é adicionada a mesma interface que foi configurada no processo de instalação da *logger*;
- **Address:** Neste campo é adicionado o *IP* que foi configurado ao instalar o *Logger*, neste exemplo usaremos o IP 172.31.240.2;
- **Secret Key:** Neste campo deve-se colar a chave secreta que foi gerado ao instalar o *Logger*;
- **Devices & Devices Group:** Adicione os *devices* do *inventory* que deseje utilizar com o logger. Este exemplo não irá considerar essa etapa.

Não configuraremos os outros campos, clique em

Save

 para gravar as configurações.

Ao finalizar todas as configurações, a tela estará como demonstrado abaixo:

Loggers

Loggers Clusters

2 records

Q

☐	Name	CPU Usage	Memory Usage	Disk Usage	Storage Usage	Actions
☐	Logger1	0% 8 core(s)	62% 15.6 GB	6% 7.7 GB	Storage unavailable	
☐	Logger2	0% 8 core(s)	62% 15.6 GB	6% 7.7 GB	Storage unavailable	

< 1 >

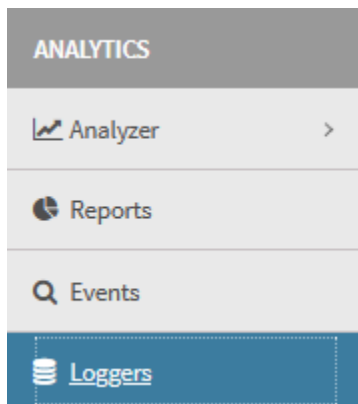
10 / page

Loggers - Loggers

Isso finaliza a configuração dos *loggers*, à seguir iremos [configurar o cluster de Loggers](#).

Clusters - Configuração do Cluster de Loggers

Após ter configurado os [Loggers](#), configuraremos o *Cluster*, acesse o menu Analytics e clique na opção *Loggers*:



Analytics - Loggers

Clique na aba Clusters:

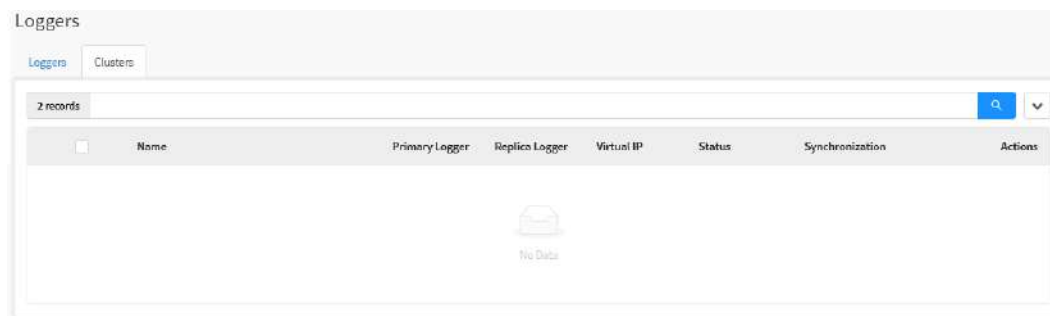


Aba Clusters



Alguns detalhes da aba Clusters não serão considerados neste exemplo, caso deseje mais informações, consulte esta [página](#).

A seguinte tela será exibida:



Loggers - Clusters

Configuremos o *Cluster* de *Logger* conforme demonstrado a seguir:

X

Save

Loggers

Loggers Clusters

2 records

	Name	Primary Logger	Replica Logger	Virtual IP	Status	Synchronization	Actions
☐	Cluster Logger 1-2	Logger1	Logger2	172.31.240.241	Primary Active	-	

< 1 > 10 / page

Network Settings - Interfaces

Isso finaliza a configuração do *Cluster de Logger*, à seguir iremos [validar as configurações](#).

Clusters - Validação das Configurações

Para efetuar a validação, iremos acessar a CLI do Logger Primário e Secundário e rodar alguns comandos, caso necessite de mais informações a respeito, consulte esta [página](#).

Um dos testes mais simples para validar a comunicação entre os *Loggers* é efetuar um [ping](#) do Primário (172.31.240.1) para o Secundário (172.31.240.2) e verificar se há resposta, conforme demonstrado pela imagem a seguir:

```
admin >ping 172.31.240.2
PING 172.31.240.2 (172.31.240.2) 56(84) bytes of data.
64 bytes from 172.31.240.2: icmp_seq=1 ttl=64 time=2.04 ms
64 bytes from 172.31.240.2: icmp_seq=2 ttl=64 time=0.454 ms
64 bytes from 172.31.240.2: icmp_seq=3 ttl=64 time=1.27 ms
64 bytes from 172.31.240.2: icmp_seq=4 ttl=64 time=0.533 ms
64 bytes from 172.31.240.2: icmp_seq=5 ttl=64 time=0.483 ms

--- 172.31.240.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4065ms
rtt min/avg/max/mdev = 0.454/0.957/2.041/0.622 ms
admin >
```

CLI - Validação da comunicação do Logger Primário para o Secundário

Também é possível efetuarmos estes mesmos passos na outra ponta, segue uma demonstração usando o comando [ping](#) para verificar a comunicação do Logger Secundário (172.31.240.2) para o Primário (172.31.240.1):

```
admin >ping 172.31.240.1
PING 172.31.240.1 (172.31.240.1) 56(84) bytes of data.
64 bytes from 172.31.240.1: icmp_seq=1 ttl=64 time=0.754 ms
64 bytes from 172.31.240.1: icmp_seq=2 ttl=64 time=0.291 ms
64 bytes from 172.31.240.1: icmp_seq=3 ttl=64 time=0.281 ms
64 bytes from 172.31.240.1: icmp_seq=4 ttl=64 time=0.298 ms
64 bytes from 172.31.240.1: icmp_seq=5 ttl=64 time=0.246 ms
64 bytes from 172.31.240.1: icmp_seq=6 ttl=64 time=0.241 ms

--- 172.31.240.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5078ms
rtt min/avg/max/mdev = 0.241/0.351/0.754/0.182 ms
admin >
```

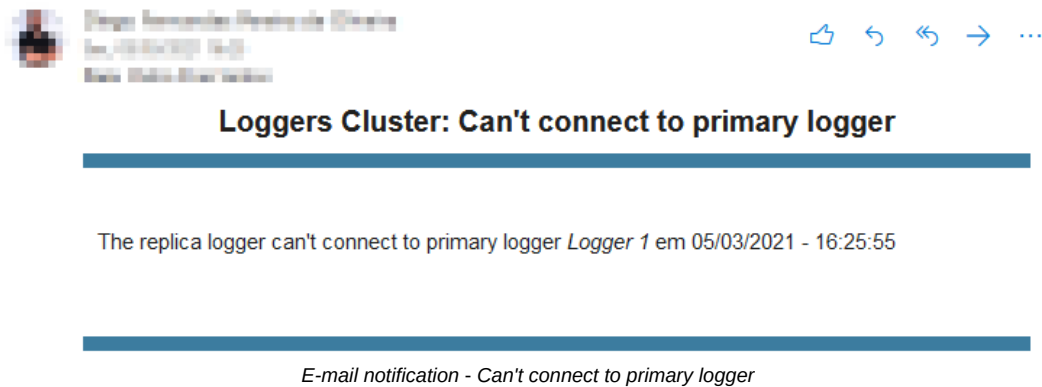
CLI - Validação da comunicação do Logger Secundário para Primário através do comando *Ping*

Outro teste que podemos executar é: Usar o comando [\[shutdown\]](#) na *Logger* primária ativa para verificar através do [\[debug-ha\]](#) se a secundária efetuará o *failover* e será ativada automaticamente, segue o que deve ser exibido na CLI do *Logger* secundário:

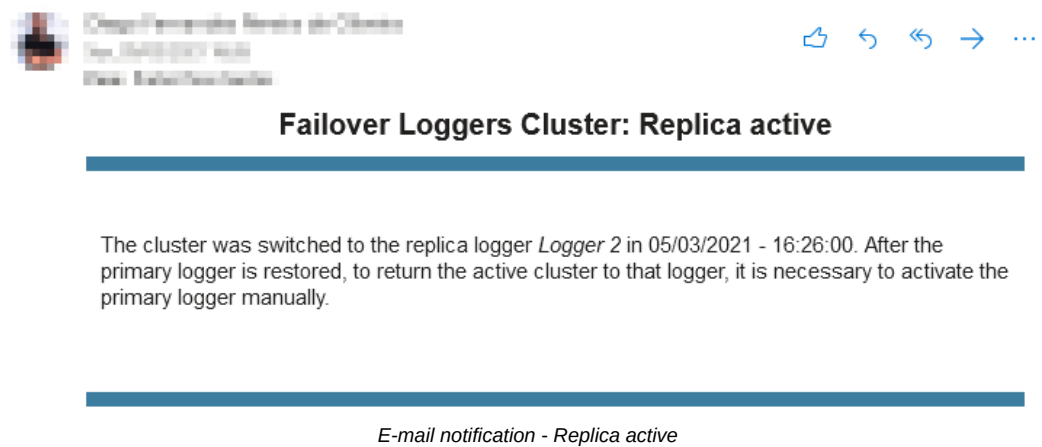
```
admin >debug-ha
date="2021-03-05 16:25:09" status="threshold" status_message="peer error 1/5"
date="2021-03-05 16:25:19" status="threshold" status_message="peer error 2/5"
date="2021-03-05 16:25:29" status="threshold" status_message="peer error 3/5"
date="2021-03-05 16:25:39" status="threshold" status_message="peer error 4/5"
date="2021-03-05 16:25:49" status="threshold" status_message="peer error 5/5"
date="2021-03-05 16:25:55" status="failover" status_message="can't connect to Primary logger"
date="2021-03-05 16:25:57" status="error" status_message="Sync peer connection error, progress: 0%"
date="2021-03-05 16:26:00" status="failover" status_message="secondary server, new status: active"
```

CLI - debug da H.A. no *Logger* Secundário exibindo *failover*

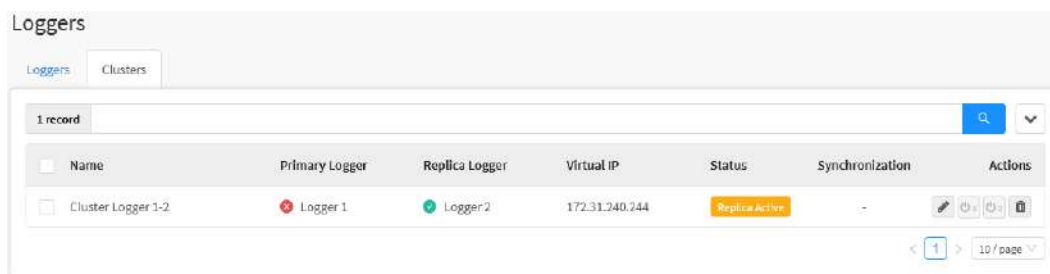
Caso um e-mail tenha sido cadastrado, como exemplificado ao [Configurar o Cluster](#), uma notificação será enviada todas notificando que o *logger* primário está *offline*:



E após a execução com sucesso do failover, uma notificação de que o *logger* secundário assumiu a prioridade no *cluster*:



Além disso, estas alterações são representadas na *interface*, conforme demonstrado na imagem abaixo (Para mais informações consulte esta [página](#)):



Clusters - Loggers

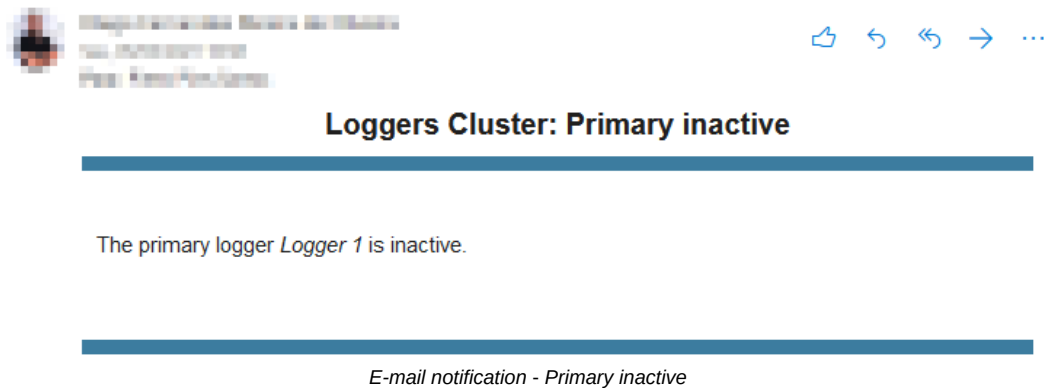
Ao religar o *Logger* Primário, o [\[debug-ha\]](#) irá reconhecer que ele foi ligado, porém, não efetuará a ativação automaticamente, este comportamento é normal. Para ativar o primário de fato, será necessário acessar a interface do sistema e efetuar esse processo manualmente através do botão **Activate**

Primary Logger [], segue o que é exibido na CLI:

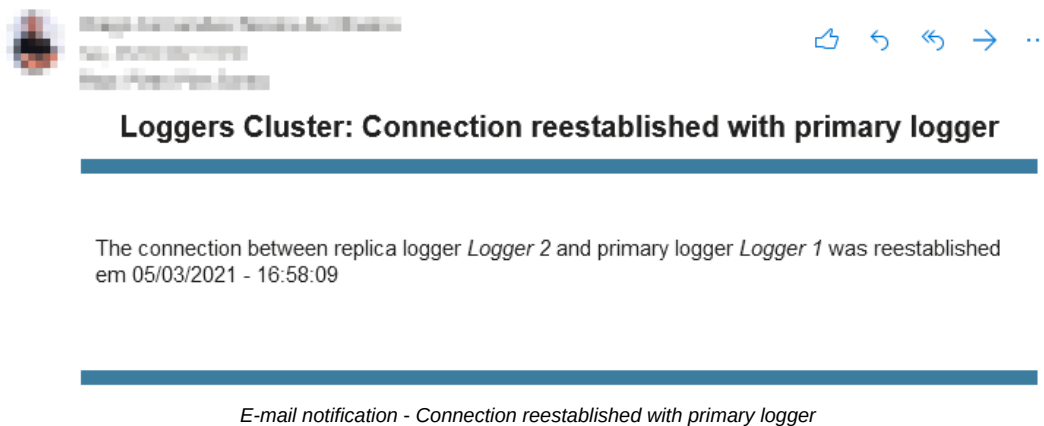

```
admin >debug-ha
date="2021-03-05 16:58:09" status="failover" status_message="connection reestablished with Primary logger"
```

CLI - debug da H.A. no Logger Secundário detectando ativação do *Logger* Primário

Quando o *Logger* Primário ficar online novamente, será enviado um e-mail reconhecendo este evento porém detectando que ela está inativa, afinal, a *Logger* secundária está ativa:



E após a execução do sincronismo, mais uma notificação será enviada:



A interface representará esta situação com o ícone ao lado do *Logger* Primário demonstrando que ele está online, porém o status denotando que a secundária está ativa

Loggers

Loggers

Clusters

1 record

☐

Name

Primary Logger

Replica Logger

Virtual IP

Status

Synchronization

Actions

☐

Cluster Logger 1-2

Logger 1

Logger 2

172.31.240.244

Replica Active

-

<

1

>

10 / page

Clusters - Loggers



Para ativar o *Logger* primário quando o secundário está *online*, devemos clicar no botão **Activate Primary Logger** []. Novamente, é possível observar o comportamento dos *Loggers* através do comando `[debug-ha]`, no *Logger* Primário, todo o processo de sincronismo e ativação será detalhado:

```
date="2021-03-05 17:21:38" status="" status_message="Sync , progress: 99%"
date="2021-03-05 17:21:38" status="" status_message="Sync , progress: 99%"
date="2021-03-05 17:21:38" status="" status_message="Sync , progress: 99%"
date="2021-03-05 17:21:38" status="" status_message="Sync , progress: 99%"
date="2021-03-05 17:21:38" status="" status_message="Sync , progress: 99%"
date="2021-03-05 17:21:38" status="" status_message="Sync , progress: 99%"
date="2021-03-05 17:21:38" status="" status_message="Sync , progress: 99%"
date="2021-03-05 17:21:38" status="" status_message="Sync , progress: 99%"
date="2021-03-05 17:21:38" status="" status_message="Sync , progress: 99%"
date="2021-03-05 17:21:38" status="" status_message="Sync , progress: 100%"
date="2021-03-05 17:21:38" status="done" status_message="Sync , progress: 100%"
date="2021-03-05 17:22:57" status="done" status_message="Sync , progress: 100%"
date="2021-03-05 17:22:59" status="failover" status_message="primary server, new status: active"
```

CLI - debug da H.A. no *Logger* Primário detectando ativação e sincronismo do *Logger* Primário

A seguir as informações que são exibidas considerando o mesmo cenário citado acima, porém ao aplicar o comando `[debug-ha]` no *Logger* Secundário:

```
admin >debug-ha
date="2021-03-05 17:23:00" status="failover" status_message="secondary server, new status: inactive"
```

CLI - debug da H.A. no *Logger* Secundário

Quando o sincronismo do *Logger* Primário for finalizado, será enviado um e-mail reconhecendo este evento:



Rogério R. de Almeida
Instituto de Física
UFPA



Failover Loggers Cluster - Sync Status: done

Logger Name: Logger 1. Sync Status: done on 05/03/2021 - 17:22:55. Progress: 100%

E-mail - Sync status: done

Um outro e-mail apontará a ativação da *Logger* Primária:



The cluster was switched to the primary logger *Logger 1* in 05/03/2021 - 17:22:59.

E-mail - Primary Active

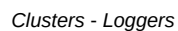
E por fim, um último e-mail reconhecerá que *Logger* Secundária foi inativada:



The replica logger *Logger 2* is inactive.

E-mail - Replica Inactive

A interface representará esta situação com o ícone ao lado do *Logger* Primário demonstrando que ele está online, e o status denotando que a Primária está ativa:



Por fim, ao fazer qualquer ativação manual dos Loggers, um log de auditoria é criado em **Audit Log**, detalhando mais informações sobre a atividade executada, conforme demonstrado na imagem a seguir:

Administration					
Administrators	Users Profiles	Auth Servers	Identity Provider	Audit Log	
134 records					
Date	User	Interface	Activity	IP	Actions
2021-03-04 15:37:48	admin	loggers-clusters	Updates	192.168.111.77	
2021-03-04 15:05:30	admin	loggers-clusters	Edit	192.168.111.77	
2021-03-04 15:03:48	admin	loggers-clusters	Edit	192.168.111.77	
2021-03-04 15:02:34	admin	loggers-clusters	Edit	192.168.111.77	
2021-03-04 12:34:02	admin	loggers	Delete	192.168.111.77	
2021-03-04 12:33:59	admin	loggers	Delete	192.168.111.77	
2021-03-04 12:31:53	admin	loggers-clusters	Delete	192.168.111.77	
2021-03-04 12:22:52	admin	analyzer-reports	Save	192.168.111.77	
2021-03-04 12:19:20	admin	loggers-clusters	Edit	192.168.111.77	
2021-03-04 12:14:30	admin	analyzer-reports	Save	192.168.111.77	

Administration - Audit Log

Quando a ativação de um dos *loggers* é realizada, o evento de atividade é listado como *update*. É possível consultar mais informações sobre clicando no botão [].

Audit View

▼

"Audit Information" : {

"logger_id" : "4"

"logger_name" : "Logger 5"

"activate-logger" : true

}

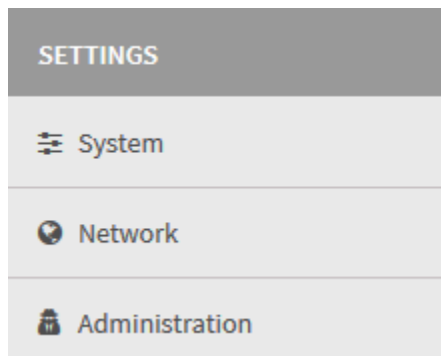
Close

Audit Log - Audit view

Isso finaliza a demonstração, para mais informações a respeito de *Cluster de Loggers*, consulte esta [página](#).

GSM - SETTINGS

Através do menu "*Settings*" é possível alterar e verificar as configurações administrativas, do sistema e da rede.



Menu *Settings*

Contém as opções:

- [System](#);
- [Network](#);
- [Administration](#).

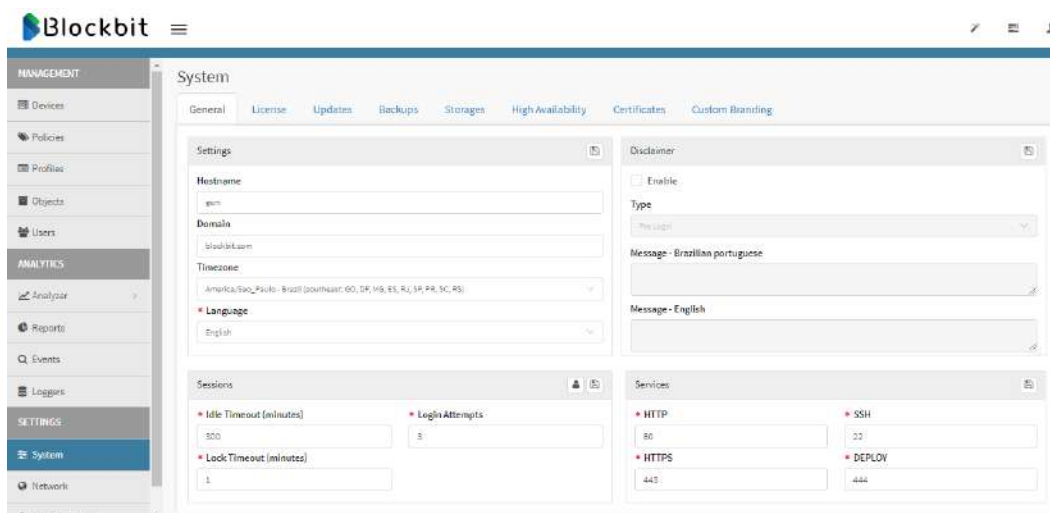
System

Através do botão "System" é possível alterar as configurações do sistema.



Settings – System

Surgirá a tela *System* com a aba "General" pré-selecionada, conforme demonstrado abaixo:



Settings – System - Aba "General".

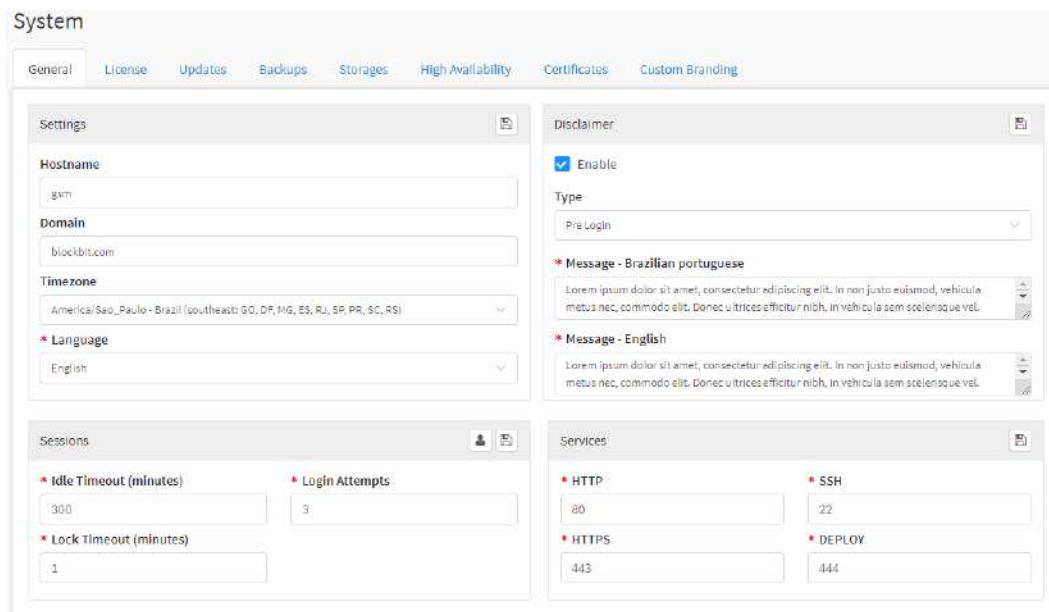
A tela *System* comporta as seguintes abas:

- [General](#);
- [License](#);
- [Update](#);
- [Backups](#);
- [Storages](#);
- [High Availability](#);
- [Certificates](#);
- [Custom Branding](#).

Descreveremos a seguir as funcionalidades disponíveis nesta tela.

System - Aba "General"

Esta aba tem como principal função, realizar alterações nas configurações gerais do Blockbit GSM:



System Settings – General

Ela é composta pelos painéis:

- [Settings](#);
- [Login Disclaimer](#);
- [Sessions](#);
- [Services](#).

A seguir iremos analisar cada um deles.

Settings

No painel *settings* podemos configurar as seguintes opções:

Settings

Hostname

gsm

Domain

blockbit.com

Timezone

America/Sao_Paulo - Brazil (southeast: GO, DF, MG, ES, RJ, SP, PR, SC, RS) ▾

* Language

English ▾

General - Settings

- **Hostname:** O nome escolhido. Pode ser qualquer um desde que esteja conforme padrão FQDN - *Fully Qualified Domain Name*. Ex.: GSM;
- **Domain:** Domínio da rede. Ex.: blockbit.com;
- **Timezone:** Selecionar o fuso horário no qual sua empresa se encontra. Ex.: America/Sao_Paulo;
- **Language:** Selecionar o idioma desejado. Ex.: *English*;

Após realizar as alterações desejadas, deve-se clicar no botão “Salvar”, localizado no canto superior direito da tela.



Botão “Salvar”

Suas alterações terão sido salvas com sucesso.

A seguir analisaremos o painel Disclaimer.

Login Disclaimer

O GSM permite habilitar uma mensagem de *Disclaimer* que é exibida na página de login da Interface de Administração. Ela pode ser configurada para aparecer, ao entrar no sistema ou depois de efetuar o processo de *login*. Nesta mensagem é possível adicionar as políticas de uso da empresa e compliance do sistema.

No painel *Disclaimer*, temos as seguintes opções:

Disclaimer

☒ Enable

Type

Pre Login

* Message - Brazilian portuguese

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut rhoncus, leo in lacinia sodales, odio augue gravida mauris, sed pretium risus erat cursus nisi. Etiam libero arcu, interdum a aliquet ac, malesuada vitae lorem. Proin at erat pharetra, dignissim enim porta, gravida

* Message - English

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut rhoncus, leo in lacinia sodales, odio augue gravida mauris, sed pretium risus erat cursus nisi. Etiam libero arcu, interdum a aliquet ac, malesuada vitae lorem. Proin at erat pharetra, dignissim enim porta, gravida

- **Enable:** Ao marcar este *checkbox* a exibição do *disclaimer* será habilitada;
- **Type:** Define como a mensagem será exibida. Podendo selecionar entre as seguintes opções:
 - **Pre Login:** A mensagem de *Disclaimer* será exibida assim que acessar o sistema, antes de efetuar o *Login*. Caso o sistema detecte o pacote de Idiomas "português" instalado no navegador, o *Disclaimer* exibido será o escrito no campo *Message - Brazilian* português, caso contrário, por padrão será utilizado o disclaimer registrado em *Message - English*;
 - **Post Login:** A mensagem de *Disclaimer* será exibida ao usuário após efetuar o *Login*.
- **Message - Brazilian portuguese:** Neste campo é possível escrever a mensagem que será exibida caso o idioma selecionado seja Português;
- **Message - English:** Neste campo é possível escrever a mensagem que será exibida caso o idioma selecionado seja Inglês.



Os campos *Messsage - Brazilian portuguese* e *Message - English* aceitam somente texto simples (puro), não sendo possível utilizar formatação.

Após realizar as alterações desejadas, deve-se clicar no botão “Salvar”, localizado no canto superior direito da tela.



Botão “Salvar”

Suas alterações terão sido salvas com sucesso.

A mensagem de *Disclaimer* será exibida conforme configurado, segue um exemplo:

Login Disclaimer

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras vel placerat ipsum, sit amet sollicitudin tellus. Fusce feugiat vehicula lectus sit amet hendrerit. Proin et arcu ut quam molestie maximus. Phasellus ut feugiat justo. Morbi elementum vitae diam non aliquam. Etiam ut ultrices dui. Sed varius, urna in commodo facilisis, magna massa volutpat quam, id interdum lorem lacus id augue. Fusce ipsum lorem, malesuada eu nulla convallis, vestibulum finibus nibh. Nullam id urna sit amet justo pretium scelerisque et commodo ante. Aliquam velit metus, convallis tempor quam at, viverra convallis metus. Curabitur sollicitudin ipsum elit, ac congue tellus consectetur at. Fusce tincidunt leo non tincidunt pellentesque.

Refuse

Accept

Login Disclaimer - Exemplo

Caso o usuário clique no botão 

Isso conclui a customização da mensagem de *Disclaimer*.

Sessions

Nesta tela é possível configurar parâmetros de autenticação e visualizar a sessão dos administradores logados no Blockbit GSM, além de encerrar suas sessões.

1. Para configurar os parâmetros de autenticação, basta alterar os campos com os valores desejados:

Sessions

* Idle Timeout (minutes)

300

* Login Attempts

3

* Lock Timeout (minutes)

1

System Settings – Sessions

- **Idle timeout:** Tempo ocioso antes da sessão expirar, o valor está em minutos. Ex.: 30;
- **Login attempts:** Número de tentativas máximas de falha de *Login* antes de bloquear o acesso, o valor está em minutos. Ex.: 3;
- **Lock timeout:** Tempo que o usuário ficará bloqueado ao realizar o número máximo de tentativas erradas no *login*, o valor está em minutos. Ex.: 3.



Clique em **save** [] localizado no canto superior direito da tela para salvar as alterações feitas nas configurações.



2. Para visualizar as sessões ativas dos administradores logados, clique no botão **Active Sessions** [] localizado no canto superior direito da tela:

Active Sessions ×				
Start	Name	Address	Status	Action
2019-10-04 13:19:14	admin	172.16.100.144	✓	
2019-10-04 14:18:34	admin	172.16.100.144	✓	
				Close

Sessões ativas

- **Start:** Data e hora que o administrador efetuou ou *login* no BLOCKBIT GSM. Ex.: 2017-04-21 19:42:42;
- **Name:** Nome do administrador. Ex.: admin;
- **Address:** Endereço *IP* do administrador. Ex.: 192.168.111.14;
- **Status:** Status do *login*. Ex.: Active;
- **Action:** Permite remover a sessão do administrador. Ao clicar no botão **Remove** [] o administrador será removido da sessão e a tela de *login* será exibida para quem quer que tenha sido removido.



Clique no botão **Close** [] para fechar a tela.



Clique em **save** [] localizado no canto superior direito da tela para salvar as alterações feitas nas configurações.

A seguir vamos analisar o painel **Services**.

Services

Nesta tela é possível alterar as portas de comunicação e administração do *Blockbit* GSM:



Caso as portas sejam alteradas no Blockbit GSM, elas também devem ser alteradas nos demais dispositivos Blockbit gerenciados.



Caso as portas HTTP e/ou HTTPS forem alteradas o acesso à Interface Web devem ser realizados com as novas portas configuradas.

Services	
* HTTP	* SSH
80	22
* HTTPS	* DEPLOY
443	444

System Settings – Services

- **HTTP:** Porta de acesso a Interface Web do Blockbit GSM. Ex.: 80;
- **HTTPS:** Porta de acesso a Interface Web do Blockbit GSM. Ex.: 443;
- **SSH:** Porta de acesso ao console CLI do Blockbit GSM e de comunicação com os devices gerenciados. Ex.: 22;
- **DEPLOY:** Porta de comunicação com os devices gerenciadas. Ex.: 444.



Clique em **save** [] localizado no canto superior direito da tela para salvar as alterações feitas nas configurações.

À seguir iremos analisar o conteúdo da aba [License](#).

System - Aba "License"

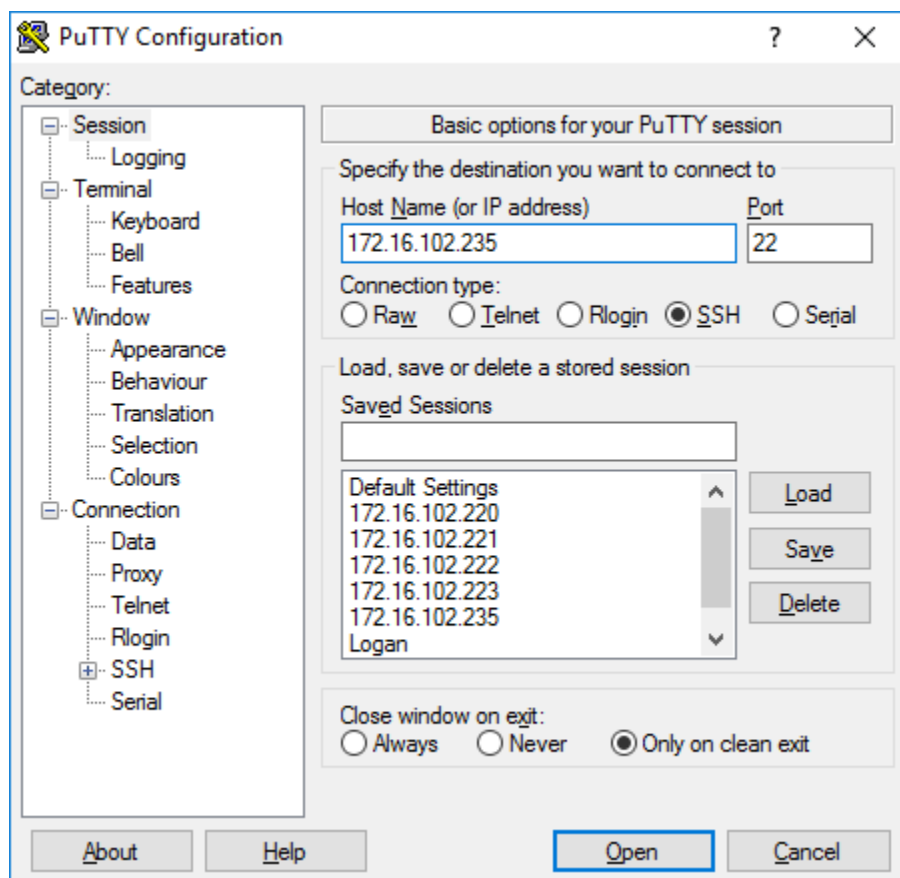
Nesta tela é possível aplicar ou renovar a licença de ativação do *Blockbit* GSM. Para realizar o licenciamento, é necessário fornecer o *UUID* (Indicador Único Universal do *Blockbit* GSM) para o seu canal de atendimento, que irá lhe fornecer o número da licença.



Antes de efetuar o licenciamento, verifique se o *Blockbit* GSM está conectado a internet.

A seguir, iremos apresentar o passo a passo para licenciar seu *Blockbit* GSM:

1. Verifique se o dispositivo de acesso possui um cliente *SSH* recomendado já instalado. Vamos exemplificar o processo utilizando o aplicativo "*PUTTY*";
2. Acesse a console *SSH*. Preencha os campos:
 - **Host Name (or IP Address):** Inserir o endereço *IP* do *Blockbit* GSM. Ex.: 172.16.102.235;



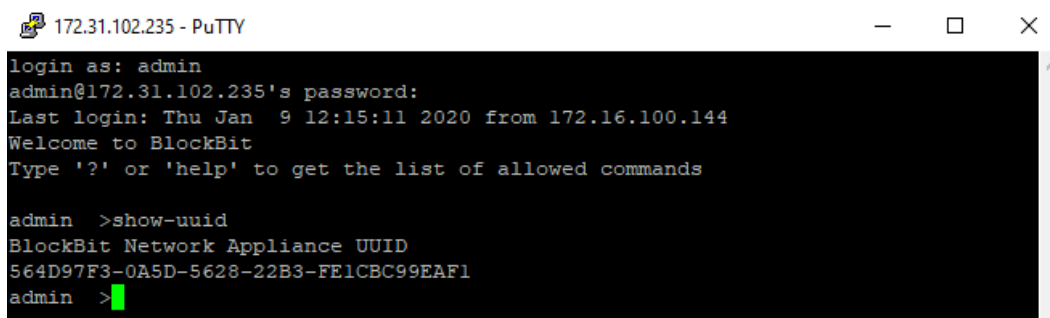
Licenciamento – *PuTTY*

- Clique no botão "*Open*".

3. A console será exibida solicitando usuário e senha;

Em "login as:" digite o usuário "admin" e pressione "Enter".
Após "password:" entre com a senha "admin" e pressione "Enter".

4. Execute o comando *show-uuid*;



```
172.31.102.235 - PuTTY
login as: admin
admin@172.31.102.235's password:
Last login: Thu Jan  9 12:15:11 2020 from 172.16.100.144
Welcome to BlockBit
Type '?' or 'help' to get the list of allowed commands

admin >show-uuid
BlockBit Network Appliance UUID
564D97F3-0A5D-5628-22B3-FE1CBC99EAF1
admin >
```

Comando *show-uuid*

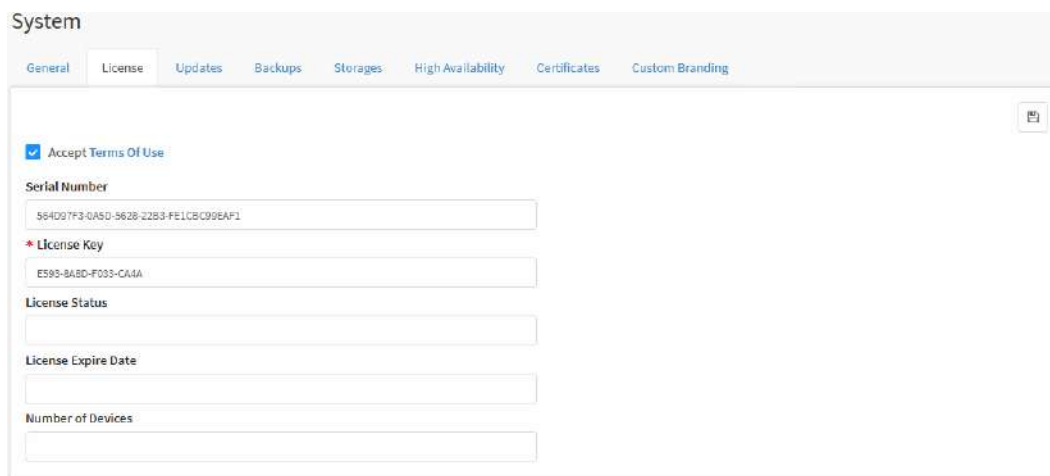
5. Encaminhe para o seu canal de atendimento *Blockbit* o código "*Blockbit Network Appliance UUID*" para a liberação da licença. Ex.: 564D97F3-0A5D-5628-22B3-FE1CBC99EAF1;

6. Você receberá o código *License number*, do seu canal de atendimento. Ex.: 8FD0-D18D-DA6C-D70C;

7. Retorne a *Interface Web* do *Blockbit* GSM na tela de Licença;

8. Certifique-se de que a Caixa de seleção "*Accept Terms of Use*" está checada, caso esteja desmarcada, clique para marcá-la;

9. Na caixa de texto "*License Key*" digite o seu número de licença, conforme exemplificado pela imagem abaixo;



System

General License Updates Backups Storages High Availability Certificates Custom Branding

☒ Accept Terms Of Use

Serial Number
564D97F3-0A5D-5628-22B3-FE1CBC99EAF1

* License Key
E593-BA8D-F033-CA1A

License Status

License Expire Date

Number of Devices

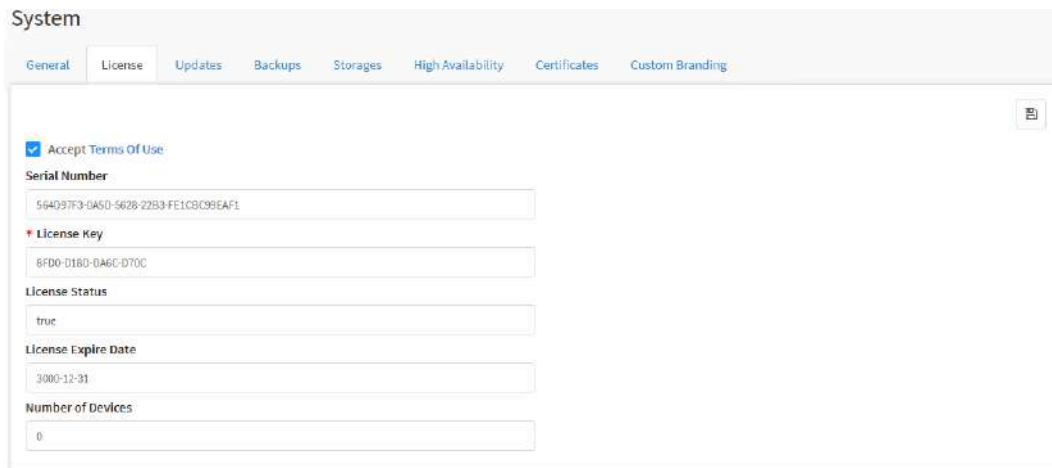
License key

10. Após realizar as alterações desejadas, deve-se clicar no botão **Save** , localizado no canto superior direito da tela;

✔ Settings successfully changed!

Settings successfully changed!

11. As informações na tela serão atualizadas e passarão a exibir as seguintes informações: “Serial Number”, “License Key”, “License Status”, “License Expiration Date” e “Number of Devices”, porém, com seus dados representando o estado atual do sistema.



The screenshot shows the 'System' settings page with the 'License' tab selected. The page has a header with tabs: General, License, Updates, Backups, Storages, High Availability, Certificates, and Custom Branding. The 'License' tab is active. Below the tabs, there is a section for license information. It starts with a checkbox labeled 'Accept Terms Of Use' which is checked. Below this, there are several input fields: 'Serial Number' with the value '564937F3-0A5D-5628-22B3-FE1C8C99EAF1', 'License Key' with the value '8FDD-D18D-0A6C-D70C', 'License Status' with the value 'true', 'License Expiration Date' with the value '3000-12-31', and 'Number of Devices' with the value '0'. There is a small icon in the top right corner of the license section.

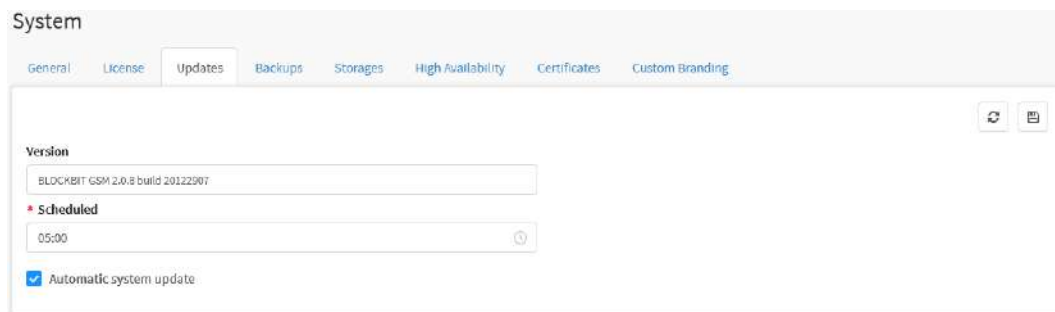
Field	Value
Serial Number	564937F3-0A5D-5628-22B3-FE1C8C99EAF1
License Key	8FDD-D18D-0A6C-D70C
License Status	true
License Expiration Date	3000-12-31
Number of Devices	0

System Settings – License

À seguir iremos analisar o conteúdo da aba [Update](#).

System - Aba "Updates"

Esta tela tem como função, efetuar a atualização do seu GSM. Este painel é composto de três opções: "Version", "Scheduled" e "Automatic System Update".



System Settings – Updates

- **Version:** Exibe a versão e o *build* atual do seu *Blockbit* GSM. Ex.: *Blockbit* GSM 1.3.0 build 19092518;
- **Scheduled:** Clicando sobre a caixa de texto um menu aparecerá, nele é possível alterar o horário agendado para executar a atualização desejada, para tanto basta clicar sobre as setas para alterar as horas e os minutos, feito isso, clique fora do menu de modo a finalizar a seleção. Ex.: 14:41;
- **Automatic System Update:** Essa caixa de seleção permite que a atualização automática de sistema seja executada. Caso ela esteja selecionada a atualização ocorrerá no horário agendado na opção acima "Scheduled".

1. No canto direito superior da tela é possível de se localizar dois botões contextuais: "Update Now" e o botão "Save" (cuja função é autoexplicativa);



2. Ao clicar no botão **update now** [], o sistema será atualizado imediatamente ao invés de aguardar o agendamento mencionado em "scheduled".



Clique em **save** [] localizado no canto superior direito da tela para salvar as alterações feitas nas configurações.

À seguir iremos analisar o conteúdo da aba [Backups](#).

System - Aba "Backups"

Através das opções disponíveis nesta aba, o administrador pode configurar uma rotina de *backup* automática das configurações do sistema, além disso, sendo possível visualizar um registro do *status* da implementação dos *backups* no painel à direita com a possibilidade de efetuar uma nova implementação, baixar o arquivo de *backup*, remover ou interromper um *backup* que esteja sendo efetuado.



Para mais informações sobre como configurar *backup* nos UTMs administrados pelo GSM, consulte esta [página](#).

Caso queira saber mais sobre criação de *storage devices*, consulte esta [página](#).



É possível consultar os *logs* com mais informações a respeito do procedimento de *backup* através do comando [\[debug-backup\]](#).

Name	Size	Last status	Status	Actions
5CA7-B928-5C8E-1B1C2-1.0-2021030920...	1.05 MB	09/03/2021 20:00	Success	[Refresh] [Download] [Delete]
5CA7-B928-5C8E-1B1C2-1.0-2021030820...	400 KB	04/03/2021 20:00	Success	[Refresh] [Download] [Delete]
5CA7-B928-5C8E-1B1C2-1.0-2021030815...	380 KB	04/03/2021 15:55	Success	[Refresh] [Download] [Delete]

System - Backups

Esta aba é composta pelos painéis:

- [Settings](#);
- [Backups History](#).

A seguir, iremos analisar cada um deles começando pelo painel [Settings](#).

System - Backups - Settings

Neste painel é possível configurar o serviço automático de *backup*, garantindo uma cópia íntegra do sistema e garantindo a sua restauração de maneira muito mais rápida e eficiente, para tanto é necessário definir o local de armazenamento, sendo que este precisa ser previamente cadastrado em [Storages](#).



Ao efetuar um *backup*, o GSM cria uma "imagem" completa do sistema, o arquivo gerado possuirá a extensão ".conf" e nele será incluso:

- O Sistema Operacional;
- O banco de dados de configuração.

A seguir, analisaremos o conteúdo deste painel:

Backups - Settings

- **Remote Storage:** Define o local onde será armazenado os *backups*. Os itens que aparecem nesta caixa são criados na aba [Storages](#). Ex.: *Storage_NFS_02*;
- **Number of Backup Retention:** Determina quantos *backups* serão armazenados no diretório. Ao fim deste limite, o *backup* mais antigo é apagado. Por exemplo, caso opte por "3", só serão mantidos os 3 últimos backups, assim sendo, quando um novo *backup* for gerado será executada a rotina para apagar o mais antigo sempre respeitando o valor adicionado neste campo. Ex.: 3;
- **Percent usage retention:** Define a porcentagem de uso que o diretório criado dentro do *storage* usará ao salvar o *backup*. Caso o limite seja atingido, a rotação de *backups* é efetuada, removendo o mais antigo de forma a sempre manter os *backups* mais recentes. Caso um diretório possua 1000 GB e seja optado por 30% de retenção, quando os registros ocuparem 30 GB a rotação será ativada, caso contrário, o número de retenção será verificado. Ex.: 100%;



O sistema atua primeiro verificando se a porcentagem de uso foi atingida e depois checando o número de *backups* retidos. Assim sendo:

1. Caso ainda possua espaço livre, o sistema irá verificar o número de *backups* retidos.
2. Caso a quantia máxima de retenção não tenha sido atingida, o armazenamento de *backups* continuará atuando normalmente sem apagar registros anteriores.

Analisando o cenário contrário, a atuação do sistema será conforme explicado abaixo:

1. Caso o limite de espaço seja atingido, a rotação será ativada para manter apenas os *backups* mais recentes;
2. Caso ainda exista espaço em disco, mas o número de *backups* retidos exceda o limite definido pelo administrador, os registros mais antigos serão removidos, respeitando o valor definido no campo, de forma que o diretório possua sempre os *backups* mais recentes.



Se o administrador não quiser que a porcentagem seja considerada, basta adicionar o valor "100" de modo que o espaço seja totalmente utilizado antes de ativar a rotação. Desta forma, só o número de *backups* retidos será considerado.

- **Secret:** Inserir a chave segura, ela deve conter no mínimo oito caracteres com letras maiúsculas e minúsculas, números e caracteres especiais. Sem esta chave não é possível realizar o *restore* do *backup*. Ex.: q1Q!q1Q!;
- **Schedule:** Define o período que o *backup* de sistema será realizado, o mesmo pode ser:
 - **Disabled:** Desabilita o *backup* automático;
 - **Daily:** Define que o *backup* será efetuado diariamente;
 - **Weekly:** Define que o *backup* será efetuado semanalmente;
 - **Monthly:** Define que o *backup* será efetuado mensalmente.
- **Hour:** Define o horário que será realizado o *backup*. Ex.: 20:00;



Você ainda pode baixar um arquivo de backup ao clicar no botão [] localizado no topo do painel.

System Backup

* Key

* Confirm Key

Cancel

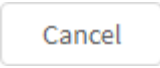
Save

Backups - System Backup

- **Key:** Cadastre uma chave segura para o arquivo de backup. Ex.: q1Q!q1Q!;
- **Confirm Key:** Efetue a confirmação da chave digitando-a novamente.

Save

Cancel

Clique em [] para salvar e baixar o arquivo de *backup* ou em [] para fechar essa janela.



Para restaurar um arquivo de backup da *Manager*, basta clicar em [], a janela abaixo será exibida:



Caso o ambiente esteja em H.A. é recomendável efetuar a restauração do *Backup* da *Manager* através do IP da *interface* física e não pelo IP virtual.

System Restore

X

* Key

* Backup File

Backup File

Cancel

Restore

Backups - System restore

- **Key:** Digite a chave que foi adicionada ao criar o arquivo de *backup*;
- **Backup File:** Selecione o arquivo de *backup* que será restaurado.

Clique em  para restaurar o arquivo de *backup* ou em  para fechar essa janela.

Por fim, para salvar as configurações de *backup* deste painel clique no botão .

 **Backup saved successfully**
Backup saved successfully

A seguir iremos analisar o painel [Backups History](#).

System - Backups - Backups History

Nesta área o sistema registra em uma lista a implementação dos *backups* configurados no painel [Settings](#) possuindo a possibilidade de efetuar algumas ações como reimplementação de rotinas de backup concluídas, *download* do arquivo de *backup*, remoção de *backups* e etc. A seguir iremos, analisar os recursos deste painel:

Backups history				
3 records				
Name	Size	Last status	Status	Actions
5CA7-B928-5C8E-1B1C2.1.0-2021030920...	1.05 MB	09/03/2021 20:00	Success	  
5CA7-B928-5C8E-1B1C2.1.0-2021030820...	400 KB	08/03/2021 20:00	Success	  
5CA7-B928-5C8E-1B1C2.1.0-2021030815...	380 KB	08/03/2021 15:55	Success	  
< 1 > 10 / page				

Backups - Backups

- **Name:** Identificação do *backup*, apresenta o nome do snapshot efetuado. Ex.: 4B4F-BB06-3B2D-D3BB-UTM-2.0.4-140820.snap;
- **Size:** Exibe o tamanho do arquivo de *backup*. Ex.: 1.05 MB
- **Date:** Nesta coluna, exibe a data e hora do sistema no momento da realização do *backup*;
- **Status:** Exibe o estado atual da execução da rotina de *Backup*, podendo ser:
 -  **Running**: A rotina de backup está em execução no momento;
 -  **Error**: Aconteceu algo de errado que causou a falha da rotina de *backup*;
 -  **Waiting**: A rotina está em tempo de espera. Isso pode ocorrer quando o sistema detecta um processo que possa interferir no *back up* está em execução no momento (por exemplo, uma outra rotina de *backup*);
 -  **Success**: O backup foi executado com sucesso.
- **Actions:** O menu "Actions" é composto pelos botões:
 -  **Restore**: Este botão serve para executar o procedimento de *backup* no *Device* novamente. Para tanto é necessário adicionar a chave criada no campo *Secret* no painel [Settings](#). Caso um *backup* seja removido do diretório, ele continuará registrado no histórico, porém esta opção estará desabilitada;



Caso o ambiente esteja em H.A. é recomendável efetuar a restauração do *Backup* da *Manager* através do IP da *interface* física e não pelo IP virtual.

-  **Download**: Este botão não é exibido caso o tipo de *backup* seja "System". Ao clicar nele, é possível fazer *download* do *snapshot*.
-  **Delete**: Ao clicar neste botão, o *backup* é removido do histórico.

Para mais informações sobre *backups*, consulte esta [página](#).

A seguir vamos analisar a aba [Storages](#).

Exemplo - Backup da Manager

Esta seção irá apresentar o passo a passo para configuração de Backups da *Manager*.



Para mais informações a respeito de *Backups* consulte esta [página](#).

Os passos que tomaremos nesta demonstração serão:

- [Inclusão de *Storage*](#);
- [Criação da Rotina de *Backup*](#);
- [Validação das Configurações](#).

Iniciaremos a demonstração configurando um [Storage](#).

Exemplo - Backup da Manager - Inclusão de Storage

Após ter [adicionado os devices](#), nesta etapa efetuaremos os seguintes passos:

- Criação de Objeto;
- Configuração do *Storage*;

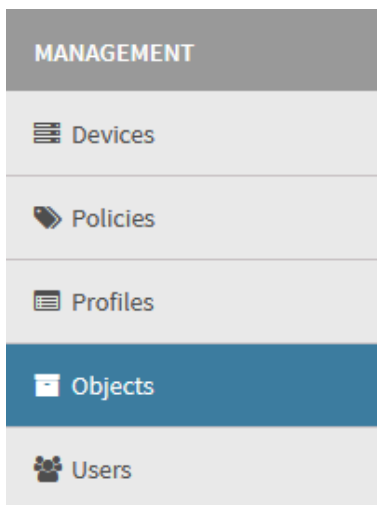


Este exemplo considerará que o *storage* que será utilizado pelo administrador está instalado e configurado corretamente. Para mais informações a respeito da compatibilidade do Blockbit GSM com *storages* remotos consulte esta [página](#).

Inicialmente geraremos os IPs que serão utilizados pelos Storages.

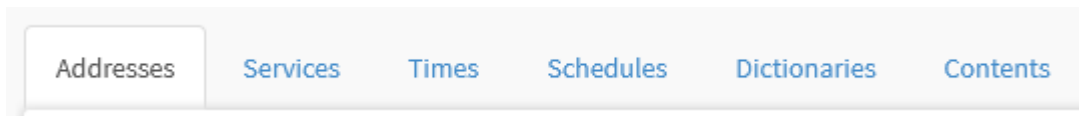
Criação de Objetos

Primeiramente criaremos o objetos de IP único que será utilizado para se conectar com o *Storage Remoto*, portanto acesse o menu Management e clique na opção *Objects*:



Management - Objects

Clique na aba Addresses:



Aba Addresses



Clique no ícone do **Menu de ações** [] e selecione a opção “Create Object”;

Inventory - Create Device

Adicionaremos o objeto de IP "Storage_NFS_02", complete o formulário conforme exemplificado a seguir:

Create Addresses Object

×

* Name

Storage_NFS_02

* Type

IPv4 Address

▼

☒ Unique

* Address

172.31.160.30

Mask

255.255.255.255

▼

+

^

▼

-

Description

Cancel

Import Address

Save

Adresses Object - Create Adresses Object

- **Name:** Usaremos o nome "Storage_NFS_02";
- **Type:** Selecione a opção "IPv4 Address";
- **Unique** ☒: Este será um objeto de tipo único, portanto se certifique de marcar esta caixa de seleção;
- **Address:** O endereço do Storage é "172.31.160.30";
- **Mask:** A máscara pode continuar sendo a padrão;
- **Description:** Neste exemplo, não adicionaremos uma descrição.

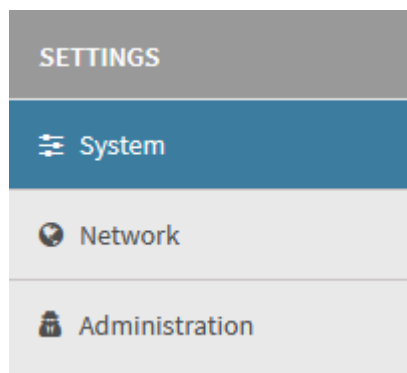
Save

Clique em [] para gravar as configurações.

Após ter criado os objetos de endereço, criaremos os *Storages*.

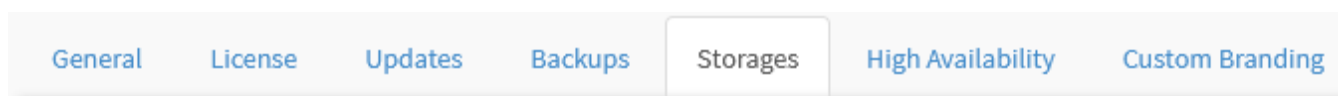
Configuração dos *Storages*

Acesse o menu *Settings* e clique na opção *System*:



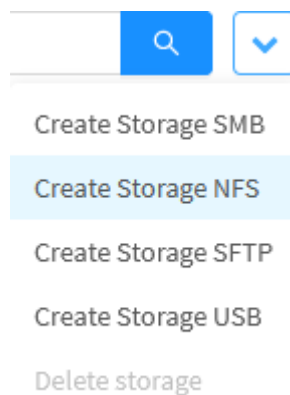
Settings - System

Acesse a aba *Storages*:



Aba Storages

Clique no ícone do **Menu de ações** [] e selecione a opção "Create Storage NFS";



Storages - Create Storages NFS

Adicionaremos o *Storage_NFS_02*, complete o formulário conforme exemplificado a seguir:

Create Storage NFS

X

Description

Storage_NFS_02

IP

Storage_NFS_02

Directory

/bkp-blockbit-nfs/user/nfs-200.30

Reading Bytes

4096

Writing Bytes

4096

Port

2049

Block sizes Bytes

☐ Protocol TCP

☐ Disable locking

☐ Enable posix

Operation Mode

☒ Hard ☐ Soft

Extra Options

opt=n, opt2=m

Simultaneous transfers

5

☐ Only Logger

Cancel

Save

Storages - Create Storage NFS

Nesta janela iremos apenas configurar os seguintes campos:

- **Description:** Neste exemplo nomearemos o *storage* como "Storage_NFS_02";
- **IP:** Selecione o endereço *IP* do servidor *NFS* configurado no passo anterior, neste caso usaremos o objeto "Storage_NFS_02";
- **Directory:** Usaremos o diretório "/bkp-blockbit-nfs/user/nfs-200.30".

Os outros campos podem ser mantidos com a configuração padrão.

Clique em  para gravar as configurações.

Ao finalizar todas as configurações, o *storage* terá sido configurado com sucesso:

System

GeneralLicenseUpdatesBackupsStoragesHigh AvailabilityCustom Branding

4 records

Description	Type	Size	Actions
☐ Storage_NFS_01	NFS	52%	
☐ Storage_NFS_02	NFS	45%	
☐ Storage_SFTP_02	SFTP	45%	

< 1 >

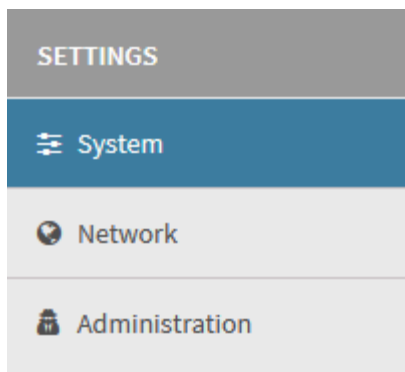
10 / page

System - Storages

No próximo passo, criaremos as [rotinas de Backups](#).

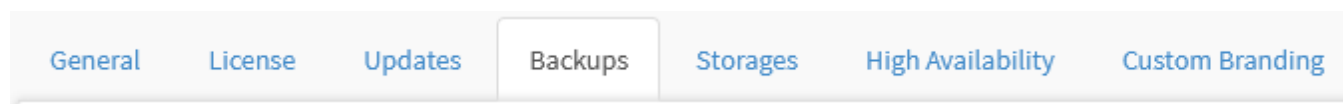
Exemplo - Backup da Manager - Criação da Rotina de Backup

Após criar o [storage](#), basta criar a rotina de *backup*, inicialmente, acesse o menu *Settings* e clique na opção *System*:



Settings - System

Clique na aba "Backups":



System - Aba Backups

Criaremos uma rotina diária de backup:

Settings





Remote Storage

Storage_NFS_02

* Number of Backup Retention

3

* Percent Usage Retention

100

* Secret

.....

* Schedule

Daily

* Hour

20:00

Backups - Create Backup

- **Remote Storage:** Selecionaremos o "Storage_NFS_02";
- **Number of Backup Retention:** Neste caso configuraremos para que haja retenção de 3 backups;
- **Percent usage retention:** Usaremos 100% do espaço do diretório, de forma que não haja limitação;
- **Secret:** Digite a chave secreta desejada;
- **Schedule:** O agendamento será diário, portanto selecionaremos a opção "Daily";
- **Hour:** Por fim, selecione o horário no qual ele será feito, neste exemplo, será às 20:00.

Clique em [] para gravar as configurações.

Ao finalizar todas as configurações, a tela estará como demonstrado abaixo:

System

General License Updates Backups Storages High Availability Custom Branding

Settings

Remote Storage

Storage: NFS_02

Number of Backup Retention: 3

Percent Usage Retention: 100

Secret: *****

Schedule: Daily

Hour: 20:00

Backups history

5 records

Name	Size	Last status	Status	Actions
SCAT-B92B-5C8E-1B1C2.1.0-2021031120...	1.05 MB	11/03/2021 20:00	Success	  
SCAT-B92B-5C8E-1B1C2.1.0-2021031020...	1.05 MB	10/03/2021 20:00	Success	  
SCAT-B92B-5C8E-1B1C2.1.0-2021030920...	1.05 MB	09/03/2021 20:00	Success	  
SCAT-B92B-5C8E-1B1C2.1.0-2021030820...	400 KB	08/03/2021 20:00	Success	  
SCAT-B92B-5C8E-1B1C2.1.0-2021030815...	380 KB	08/03/2021 15:55	Success	  

< 1 > 10 / page

Devices - Backups

Por fim, discutiremos a [validação](#) das configurações que efetuamos.

Exemplo - Backup da Manager - Validação das Configurações

Para efetuar a validação do correto funcionamento das configurações de *backup*, é possível forçar o backup manual através do botão **Run System**

Backup Now [].

System Backup

* Key

.....

* Confirm Key

.....

Cancel

Save

Backups - System Backups

Após adicionar a chave secreta, basta clicar em [] e conferir o status e o progresso dos *backups* na própria *interface* onde eles foram criados, segue um exemplo:

System

General

License

Updates

Backups

Storages

High Availability

Custom Branding

Settings

Remote Storage

Storage_NFS_02

* Number of Backup Retention

3

* Percent Usage Retention

100

* Secret

.....

* Schedule

Daily

* Hour

20:00

Backups history

5 records

Name	Size	Last status	Status	Actions
SCA7-B928-9C8E-1B1C2.L0-2021031120...	1.05 MB	11/03/2021 20:00	Success	
SCA7-B928-9C8E-1B1C2.L0-2021031020...	1.05 MB	10/03/2021 20:00	Success	
SCA7-B928-9C8E-1B1C2.L0-2021030920...	1.05 MB	09/03/2021 20:00	Success	
SCA7-B928-9C8E-1B1C2.L0-2021030820...	400 KB	08/03/2021 20:00	Success	
SCA7-B928-9C8E-1B1C2.L0-2021030815...	380 KB	08/03/2021 15:55	Success	

1

10 / page

Devices - Backups



Para mais informações sobre os componentes desta tela, consulte esta [página](#).

Além disso, as operações efetuadas pelos backups geram logs de auditoria, como demonstrado na imagem à seguir:

Administration

Administrators Users Profiles Auth Servers Identity Provider Audit Log

142 records

Date	User	Interface	Activity	IP	Actions
2021-03-10 20:58:57	Administrator	backups	Delete	192.168.200.2	
2021-03-10 20:58:03	Administrator	backups	Edit	192.168.200.2	
2021-03-10 20:16:21	Administrator	device-backups	Edit	192.168.200.2	
2021-03-10 19:12:49	Administrator	device-backups	Save	172.31.200.253	
2021-03-10 18:53:51	Administrator	device-backups	Delete	172.31.200.253	
2021-03-10 18:00:23	Administrator	backups	Edit	172.31.200.253	
2021-03-10 16:10:58	Administrator	device-backups	Edit	192.168.111.85	
2021-03-10 16:01:42	Administrator	device-backups	Save	192.168.112.21	
2021-03-10 16:01:13	Administrator	device-backups	Save	192.168.112.21	
2021-03-10 16:01:01	Administrator	device-backups	Save	192.168.112.21	

< 1 2 3 4 5 ... 15 > 10/page

Administration - Audit Log

Clique em  para obter mais informações a respeito do registro:

Audit View

```

{
  "Audit Information": {
    "settings_system-download-file": "5CA7-B928-5C8E-1B1C2.1.0-202103121619.conf"
    "settings_system-download-size": "1.05 MB"
  }
}

```

Close

Devices - Backups - Audit View



Para mais informações sobre os relatórios de auditoria, consulte esta [página](#).

Por fim, durante o processo de *backup* também é possível verificar mais detalhes na *CLI* usando o comando de [\[debug-backup\]](#).

```

admin >debug backup
date="2021-03-12 16:23:02" backup_id="4" device_type="manager" action="backup" storage_name="Storage_NFS_02" storage_type="nfs" backup_type="conf" status="running" status_message="" service="backup_manager"
date="2021-3-12 16:23" backup_id="4" device_type="manager" action="backup" storage_name="Storage_NFS_02" storage_type="nfs" backup_type="Conf" status="Done" service="Backup_manager"

```

CLI - debug-backup

Para mais informações a respeito de backups de device, consulte esta [página](#).

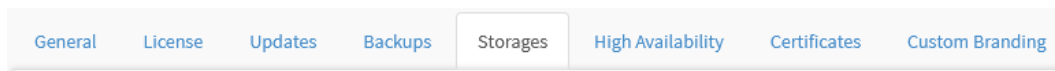
System - Aba "Storages"

Nesta aba estão localizados os recursos que permitem a administração das interfaces de armazenamento do GSM. Este painel permite que o administrador efetue o cadastro dos dispositivos de armazenamento que serão utilizados pelos serviços de *backup*.



Os storage devices criados nesta aba são utilizados principalmente no serviço de [backup do GSM](#) e nos [backups dos UTMs](#) administrados pelo sistema.

Para acessar a interface de gerenciamento dos Armazenamentos, clique na aba "Storages":



Aba Storages

Surgirá a tela, conforme demonstrado pela imagem abaixo:

Description	Type	Size	Actions
SFTP Storage	SFTP	0%	
SMB Storage	SMB	20%	
USB Storage 1	USB	99%	
USB Storage 2	USB	0%	

System - Backup Storages



ATENÇÃO: Independente de qual categoria de diretório tenha sido criado pelo administrador, cada GSM necessita ter o seu próprio diretório.

Nessa seção iremos expor os tipos de armazenamentos suportados pelo sistema e suas aplicações:

- [SMB](#);
- [NFS](#);
- [SFTP](#);
- [USB](#).

Esta seção irá demonstrar:

- [Cadastrar cada tipo de Storages](#);
- [Deletar os Storages](#);
- [Componentes da coluna dessa tela](#).

A seguir analisaremos o botão [Create Storage](#).

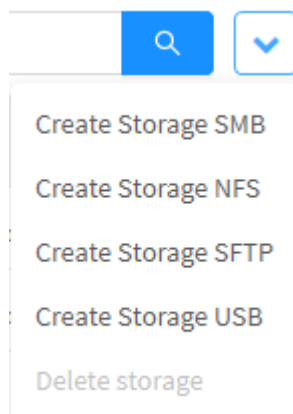
Storages - Menu de Ações

O menu de ações contém opções para a criação das unidades de armazenamento no GSM, sendo que estas serão utilizadas na criação de *Backups* (cheque esta [página](#) para mais informações).

E também possui a opção de removê-las.



Clique em [], a seguinte janela será exibida:



Storages - Create Storage

As opções disponíveis são:

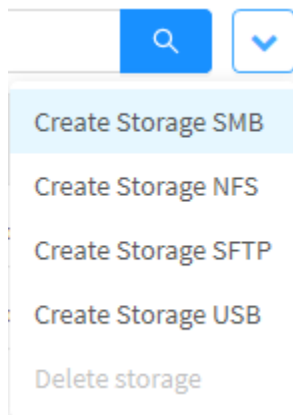
- [Create Storage SMB](#);
- [Create Storage NFS](#);
- [Create Storage SFTP](#);
- [Create Storage USB](#);
- [Delete Storage](#).

A seguir explicaremos cada opção deste menu.

Create Storage - SMB

O armazenamento "Server Message Block" é comumente utilizado em compartilhamento de pasta pelo *Windows*. Esse modelo de armazenamento é disponibilizado pelo sistema para as aplicações de "Backup/Restore".

Para adicionar um armazenamento *SMB*, clique em [] e selecione a opção "Create Storage SMB" conforme demonstrado abaixo:



Create Storage SMB

A janela abaixo será exibida, configure o formulário de acordo com as especificações para conexão com respectivo servidor *SMB*:

Create Storage SMB

X

* Description

* IP

Select

Login

Password

* Share

* Simultaneous transfers

5

☐ Only Logger

Cancel

Save

Storage - Add SMB storage

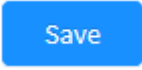
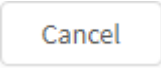
- **Description:** Nome do storage. Ex.: *SMB Storage*;
- **IP:** Selecione o endereço *IP* do servidor de arquivos. Este campo apresentará os objetos de *IP* existentes, portanto é recomendável criar um Objeto de endereço *IPv4* único para o *storage* que será utilizado. Ex.: 172.16.102.52;
- **Login:** Usuário do servidor de arquivos. Ex.: blockbit1;
- **Password:** Senha do usuário do servidor de arquivos;
- **Share:** Nome da pasta que foi compartilhada no servidor de arquivos. Ex.: *storage*;
- **Simultaneous transfers:** Define o limite de Transferências simultâneas que o Sistema pode fazer utilizando este storage em particular. Ex.: 5;
- **Only Logger** ☐: Caso esta caixa de checagem seja habilitada, a unidade será utilizado exclusivamente para fazer *armazenamento dos loggers*.



Para mais informações a respeito de como criar um Objeto de IP único, consulte esta [página](#).

Save

Cancel

Depois de preencher todos os campos clique em [] para concluir ou clique em [] para fechar a janela sem efetuar nenhuma alteração;

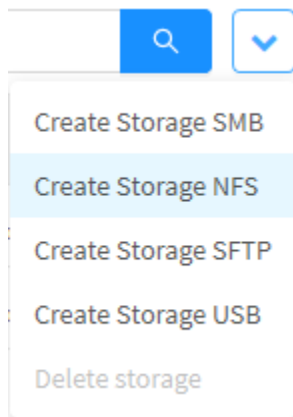
Após salvar, para que as configurações entrem em vigor, será necessário acessar a **fila de comandos** [] e aplicar as alterações efetuadas. Para mais informações a respeito da fila de comandos acesse a página: [UTM - Fila de comandos](#).

À seguir vamos analisar como criar um *storage NFS*.

Create Storage - NFS

O "Network File System" é comumente utilizado em compartilhamento de pastas em servidores *UNIX*. Esse modelo de armazenamento é disponibilizado pelo sistema para as aplicações de "Backup/Restore".

Para adicionar um armazenamento *NFS*, clique em [] e selecione a opção "Create Storage NFS", conforme demonstrado:



Create Storage NFS

A janela abaixo será exibida, configure o formulário especificando os campos "Description", "IP" e "Directory" do servidor *NFS* para o armazenamento do recurso de *backup/restore*.

Create Storage NFS

Description

IP

Select

Directory

Reading Bytes

4096

Writing Bytes

4096

Port

2049

Block sizes Bytes

Protocol TCP

Disable locking

Enable posix

Operation Mode

Hard

Soft

Extra Options

opt=n, opt2=m

Simultaneous transfers

5

Only Logger

Cancel

Save

Storage - Add NFS storage

- **Description:** Nome do armazenamento *NFS*. Ex.: *NFS Backup*;

- **IP:** Selecione o endereço *IP* do servidor *NFS*. Este campo apresentará os objetos de *IP* existentes, portanto é recomendável criar um Objeto de endereço *IPv4* único para o *storage* que será utilizado. Ex.: 172.16.102.53;
- **Directory:** Diretório de armazenamento no servidor *NFS*. Ex.: */storage/backup*;
- **Reading Bytes:** Define a velocidade de leitura dos *bytes* do servidor;
- **Writing Bytes:** Define a velocidade de escrita dos *bytes* do servidor;
- **Port:** Define a porta utilizada pelo servidor;
- **Block sizes Bytes:** Determina o tamanho dos blocos de armazenamento do *NFS*;
- **Protocol TCP** ☐: Caso esta caixa de checagem seja habilitada, o protocolo TCP será utilizado pelo servidor *NFS*;
- **Disable locking** ☐: Caso esta caixa de checagem estiver habilitada, os arquivos armazenados não poderão ser bloqueados;
- **Enable posix** ☐: Ao ativar esta caixa de checagem, este *storage* será habilitado para ser acessado por sistemas que usem os requerimentos *POSIX* (*Portable Operating System Interface*);
- **Operation Mode:** Define o modo de operação do *Storage NFS*, podendo ser:
 - **Hard**;
 - **Soft**.
- **Extra Options:** A configuração deste item pode ser definida com base nas configurações e especificações do servidor *NFS*;
- **Only Logger** ☐: Caso esta caixa de checagem seja habilitada, a unidade será utilizado exclusivamente para fazer *armazenamento dos loggers*.



Para mais informações a respeito de como criar um Objeto de IP único, consulte esta [página](#).



Caso o administrador não conheça detalhes da configuração do servidor *NFS*, pode manter os valores padrões de configuração da interface.

Save

Cancel

Depois de preencher todos os campos clique em para concluir ou clique em para fechar a janela sem efetuar nenhuma alteração;



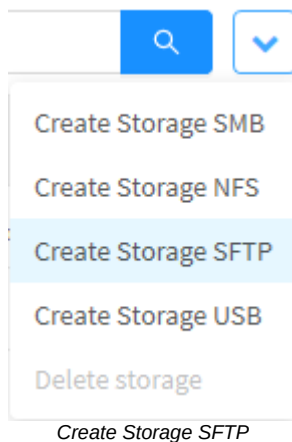
Após salvar, para que as configurações entrem em vigor, será necessário acessar a **fila de comandos**  e aplicar as alterações efetuadas. Para mais informações a respeito da fila de comandos acesse a página: [UTM - Fila de comandos](#).

À seguir vamos analisar como criar um *storage SFTP*.

Create Storage - SFTP

O "Secure Shell" é um protocolo de rede criptográfico comumente utilizado para conexão de serviços de rede de forma segura, o "SSH File Transfer Protocol" utiliza esses recursos para transferência e gerenciamento de dados. Esse modelo de armazenamento é disponibilizado pelo sistema para as aplicações de "Backup/Restore";

Para adicionar um armazenamento *SFTP*, clique em [] e selecione a opção "Create Storage SFTP", conforme demonstrado:



Configure o formulário do servidor *SFTP* para o armazenamento do recurso de *backup/restore*.

Create Storage SFTP

X

* Description

* User

* IP

Select

* Port

Select

* Directory

Ex./mnt/sftp/

* Simultaneous transfers

5

☐ Compression

☐ Only Logger

Cancel

Save

Storage - Add SFTP storage

- **Description:** Nome do armazenamento *SFTP*. Ex.: *SFTP Backup*;
- **User:** Usuário responsável pela conexão *SFTP*. Ex: *user1*;
- **IP:** Endereço *IP* do servidor *SFTP*. Este campo apresentará os objetos de *IP* existentes, portanto é recomendável criar um Objeto de endereço *IPv4* único para o *storage* que será utilizado. Ex.: *Storage_SFTP*;
- **Port:** Porta do serviço *SFTP*. Ex.: 22;
- **Directory:** Diretório de armazenamento no servidor *SFTP*. Ex.: */home/user1/backup*;
- **Simultaneous transfers:** Define o limite de Transferências simultâneas que o Sistema pode fazer utilizando este storage em particular. Ex.: 5;
- **Compression** ☐: Ao ativar essa caixa de seleção os dados deste *storage* serão compactados;
- **Only Logger** ☐: Caso esta caixa de checagem seja habilitada, a unidade será utilizado exclusivamente para fazer *armazenamento dos loggers*.



Para mais informações a respeito de como criar um Objeto de IP único, consulte esta [página](#).

Save

Cancel

Depois de preencher todos os campos clique em [] para concluir ou clique em [] para fechar a janela sem efetuar nenhuma alteração;

1

Após salvar, para que as configurações entrem em vigor, será necessário acessar a **fila de comandos** [] e aplicar as alterações efetuadas. Para mais informações a respeito da fila de comandos acesse a página: [UTM - Fila de comandos](#).



Após isso, vamos editar o *storage* "*SFTP*" clicando no botão [] que fica na coluna *Action*, a tela abaixo será exibida.

Edit Storage SFTP
X

* Description

Backup SSH

* User

root

* IP

Storage_SFTP_IP

* Port

SSH

* Directory

/home/user1/backup

* Simultaneous transfers

5

☐ Compression
☐ Only Logger

Public Key

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDcYlgoUdjFAadl3b3QqssJE7bDkth5mi6jfrjHPw
Tp7wX3CJCRxLLc+i8J6B9I+Qrr9Z9fyf6ztg8O8UwxHXKYcggUfuZS586ecXf8vowUJ7Kjgn

Cancel Save

SSH - Edit storage SSH.

O sistema irá gerar uma chave pública para ser exportada para o servidor SSH, ao clicar sobre o ícone , após copiar a chave iremos ao servidor remoto onde será configurado o SSH.

No diretório `.ssh` do usuário onde será feito o armazenamento do *backup* como, por exemplo: `/home/user1/.ssh`, a chave que foi copiada no diretório `authorized_keys` será salva, conforme imagem abaixo.

```
[root@nfsfwm .ssh]# pwd
/home/user1/.ssh
[root@nfsfwm .ssh]# ls -alh
total 20K
drwx-----. 2 user1 user1 4,0K Dez 22 15:09 .
drwx-----. 5 user1 user1 4,0K Set 14 11:00 ..
-rw-r--r--. 1 user1 user1 1,2K Set 14 11:05 authorized_keys
-rw-----. 1 user1 user1 1,7K Jun 12 2017 id_rsa
-rw-r--r--. 1 user1 user1 394 Jun 12 2017 id_rsa.pub
[root@nfsfwm .ssh]#
```

SSH - SSH *authorized_keys*

Ao editar o arquivo vamos colar a chave e salvar as alterações.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDAIhycBz51qhz481DCM0W9aU/T91wN0ZTYK1W29T1nr4pc0vBA+K4vaNP1CgmF74WC1L+ngYARZ3HUxeVgPy2a31nz288ay88zPVSvQb/2n0-xNu8H0j3MUk0Vux  
Vw5Vsb7wPSFY68m0b0InF/srdcjzF14DjhPaDmT00Y6NmpXrbWkq+ck3mULwHEj1hyeqs6YLX2ro1S(C9TAKN5PN5RhjyyavcdLIPg5xs4QEDypR5d8qQ26FB03RL3BkOTT/7309SLudp1j91R/FBpeaUEahG0h+T91bQ  
TKJMTS+N7D3EV0EOLpnKd/QM244d3UwKMEM2j521/+NLhh-root@utw-blockbit.com
```

SSH - Edit SSH authorized_keys

Isso conclui as configurações do *Device Storage SFTP*.

À seguir vamos analisar como criar um *storage USB*.

Create Storage - USB

Trata-se de um dispositivo físico de armazenamento de dados. São suportados dispositivos do tipo (*USB-HDD*; *USB-SSD*). Esse modelo de "Storage" é disponibilizado pelo sistema para as aplicações de "Backup/Restore".

Para identificar um dispositivo do tipo "USB", será necessário certificar-se de que ele está conectado, e efetuar algumas configurações na *CLI* para que seja feita a montagem, reconhecimento do tipo de dispositivo e configuração da unidade de acesso de acordo com sua identificação.

Para preparar o dispositivo de modo que ele seja reconhecido pelo sistema, siga os passos abaixo:

Configuração de Storage USB na CLI

Inicialmente certifique-se que o dispositivo está conectado e que não há nenhum dado importante armazenado nele.



ATENÇÃO: Ao seguir este passo à passo, em alguns passos da configuração alguns comandos irão limpar todos os dados do dispositivo de armazenamento.

Certifique-se de que está usando um dispositivo limpo ou que os dados dentro dele não serão necessários.

Acesse o console do Blockbit UTM via [Terminal](#), faça *login* utilizando o usuário *admin* e a senha personalizada.



A senha padrão é:

Login: admin

Password: admin



É altamente recomendada a alteração da senha padrão do usuário "admin" de console. Para alteração da senha padrão, é necessário criar uma senha segura. Esta senha deve conter no mínimo 8 caracteres com letras maiúsculas e minúsculas, números e caracteres especiais. Para alterar a senha, use o comando de *CLI* "*passwd*", cheque esta [página](#) para mais informações.

O acesso ao terminal é restrito, para listar os comandos disponíveis, digite: **?** ou **help**.

```

admin >help
arp                ip                reset-admin-sessions  uptime
arping            ipcalc           reset-logs           vmstat
date              less            restore-logger-backup whois
debug-backup      logger-backup    rewizard
debug-deployer    logger-certificate-sync
debug-ha          logger-config    route
debug-rotation    logger-config-sync
debug-sync        logger-connect   sar
delete-logger-backup
logger-devices-add  set-network-dns
disable-snmpp      logger-devices-list
enable-root        logger-disable   set-network-gateway
enable-snmpp       logger-enable    set-network-hostname
ethtool           logger-key       set-network-interface
exit              logger-storage   set-network-timezone
fdisk             logger-update-schedule
free              lscpu            show-devices
fsck              mkfs             show-license
grep             more             show-logger-backups
ha-failover       netstat          show-uuid
ha-up             ntpdate          show-version
help             passwd           shutdown
history          ping             snapshot
hostname         reboot           tcpdump
ifconfig         reset            tcptop
ifstat          reset-admin-block telnet
iotest          reset-admin-password
admin >

```

Terminal

1. Para listar o novo disco, digite: **fdisk -l**

```

admin > fdisk -l
Disk /dev/sda: 320.1 GB, 320072933376 bytes, 625142448 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000b93f6

Dispositivo Boot      Start          End      Blocks   Id  System
/dev/sda1  *           2048       1026047    512000   83   Linux
/dev/sda2              1026048    625141759   312057856   8e   Linux LVM

Disk /dev/mapper/root: 21.5 GB, 21474836480 bytes, 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/swap: 4177 MB, 4177526784 bytes, 8159232 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/data: 293.9 GB, 293890686976 bytes, 574005248 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/sdb: 8000 MB, 8000110592 bytes, 15625216 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

admin >

```

Antes de formatar o disco, pode ser necessário proceder com o particionamento do disco.

Particionando o disco, execute o comando: ex.: **fdisk /dev/sdb**

```
admin >fdisk /dev/sdb
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Command (m for help):
```

Digite “m” para listar a base de parâmetros/comandos do utilitário “fdisk” para o particionamento do disco.

```
Command (m for help): m
Command action
  a   toggle a bootable flag
  b   edit bsd disklabel
  c   toggle the dos compatibility flag
  d   delete a partition
  g   create a new empty GPT partition table
  G   create an IRIX (SGI) partition table
  l   list known partition types
  m   print this menu
  n   add a new partition
  o   create a new empty DOS partition table
  p   print the partition table
  q   quit without saving changes
  s   create a new empty Sun disklabel
  t   change a partition's system id
  u   change display/entry units
  v   verify the partition table
  w   write table to disk and exit
  x   extra functionality (experts only)

Command (m for help):
```

Delete a partição atual. “d – delete a partition”

```
Command (m for help): d
Selected partition 1
Partition 1 is deleted

Command (m for help):
```

Adicione uma nova partição. “n – add new partition”

```
Command (m for help): n
Partition type:
  p   primary (0 primary, 0 extended, 4 free)
  e   extended
```

```
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-31299583, default 2048): 2048
Last sector, +sectors or +size{K,M,G} (2048-31299583, default 31299583):
Using default value 31299583
Partition 1 of type Linux and of size 14.9 GiB is set

Command (m for help):
```

Salvar a nova tabela de partições no disco. “w – write table to disk and exit”

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```



O sistema requer que dispositivos do tipo “Disco” estejam formatados de acordo com o sistema de arquivos de registro *EXT4*.

Para formatar o disco identificado já particionado, digite: **mkfs -t ext4 /dev/sdb1**

```
admin >mkfs -t ext4 /dev/sdb1
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
979200 inodes, 3912192 blocks
195609 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
120 block groups
32768 blocks per group, 32768 fragments per group
8160 inodes per group
Superblock backups stored on blocks:
32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208

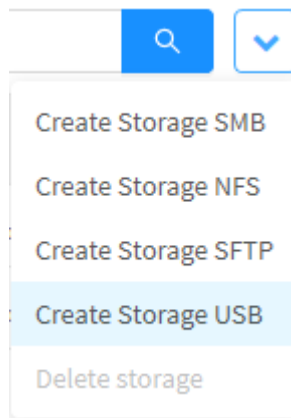
Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

Uma vez conectado ao servidor e formatado no padrão *EXT4*, o dispositivo estará pronto para ser listado. Para tanto, precisaremos adicionar o dispositivo de armazenamento na interface gráfica do GSM.

Configuração de *Storage USB* na *Interface*



Clique em [] e selecione a opção “*Create Storage USB*”.



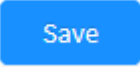
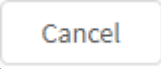
Create Storage USB

O formulário abaixo será exibido:

A form titled 'Create Storage USB' with a close button (X) in the top right corner. It contains three required fields, each marked with a red asterisk: 'Description' (a single-line text box), 'USB Device' (a single-line text box), and 'Simultaneous transfers' (a single-line text box containing the number '5'). At the bottom right of the form are two buttons: 'Cancel' and 'Save'.

Storage - Add SMB storage

- **Description:** Digite o nome da conexão. Ex.: *SMB*;
- **USB Device:** Selecione o dispositivo de armazenamento USB que será utilizado, caso a lista não exiba nada, consulte os passos descritos [acima](#).
- **Simultaneous transfers:** Define o limite de Transferências simultâneas que o Sistema pode fazer utilizando este storage em particular. Ex.: 5.

Depois de preencher todos os campos clique em [] para concluir ou clique em [] para fechar a janela sem efetuar nenhuma alteração;

Após salvar, para que as configurações entrem em vigor, será necessário acessar a **fila de comandos** [] e aplicar as alterações efetuadas. Para mais informações a respeito da fila de comandos acesse a página: [UTM - Fila de comandos](#).

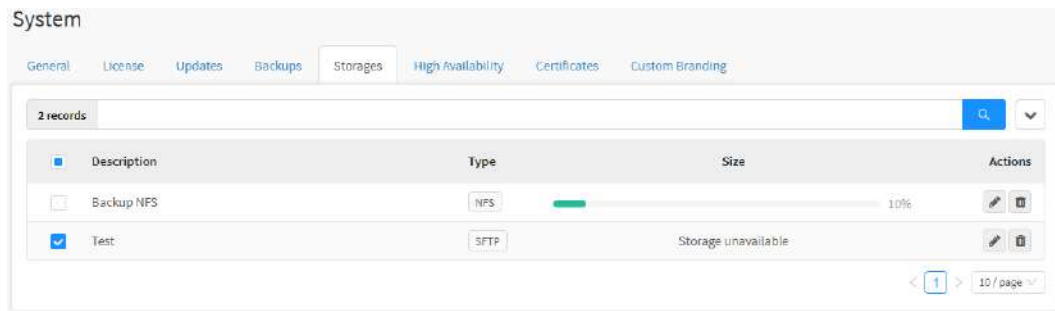
À seguir iremos detalhar como [deletar storages](#).

Storages - Delete Storages

Através do botão "Delete Storages" é possível deletar os Storages selecionados. Para deletar pelo Menu de ações, siga os seguintes passos:

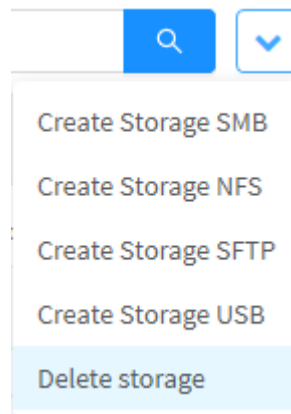
1. Selecione qual(is) Device(s) de Storage(s) deseja deletar. Para selecionar, basta clicar com o *mouse* no *checkbox* que fica localizado ao lado do *Name*.

Nos *devices* de *storage* selecionados o *checkbox* mudará da cor cinza para azul []. Ex.: *Test*;



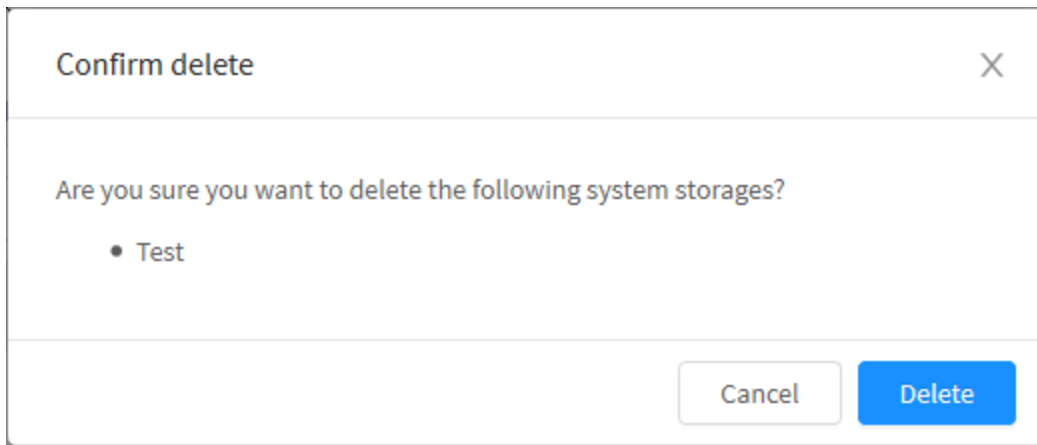
Storages – Seleção dos Devices de Storages para deletar

2. Entre no **menu de ações** [] e clique na opção "Delete Profile".

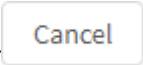


Storages – Delete Storage

3. Surgirá a mensagem de notificação questionando se deseja realmente deletar os *Profiles* selecionados:



Storages – Mensagem de deleção do Storages

Caso desejar cancelar clique no botão . Para concluir, clique no botão .

 **System storage deleted successfully!**

System storage deleted successfully!

Após realizar esses procedimentos, os *profiles* terão sido deletados com sucesso.

À seguir iremos detalhar os componentes das [colunas](#).

Storages - Colunas

A seguir explicaremos o conteúdo de cada coluna da aba *Storages*:

☐	Description	Type	Size	Actions
☐	SFTP Storage	SFTP	0%	
☐	SMB Storage	SMB	20%	
☐	USB Storage	USB	99%	
☐	NFS Storage	NFS	52%	
☐	SMB Storage (Logger)	SMB	This Storage is mounted on the logger	

Profiles – Storages

A seguir explicaremos cada coluna:

- **Caixa de Seleção** : Ao clicar nesta caixa de checagem o *Storage Device* é selecionado para efetuar outras operações;
- **Description**: Apresenta a descrição do *Storage Device* cadastrado;
- **Type**: Exibe o tipo de storage, as possíveis opções a serem exibidas são:
 - [SMB](#);
 - [NFS](#);
 - [SFTP](#);
 - [USB](#).
- **Size**: Exibe a porcentagem de uso do armazenamento do *device* em questão ou indica que o *Storage* está sendo usado especificamente para *logger*;
- **Actions**: A coluna “Actions” é composta pelos botões:
 - **Edit** : Permite editar as configurações do *Storage Device* adicionado na opção do [menu de ações](#);
 - **Delete** : Deleta o *profile*, é equivalente a opção [Delete Storage](#) do menu de ações.

Para mais informações a respeito de *device storages* consulte esta [página](#).

Caso queira mais informações a respeito da aba *High Availability*, acesse esta [página](#).

System - Aba "High Availability"

A aba "High Availability" possibilita que o administrador configure um servidor de gerenciamento do GSM primário ativo e um secundário passivo (*standby*) para ser utilizado em caso de falha. Este recurso garante que o sistema seja mais resiliente reduzindo consideravelmente a sua indisponibilidade e garantindo sua operação normal independente de componentes do servidor primário não estarem operacionais.

O servidor secundário atua em redundância do principal, sendo ativado e assumindo as funções operacionais caso ocorra algum tipo de falha no servidor primário, durante este evento, o servidor principal ficará em *standby* até a situação ter sido normalizada. Quando a conexão voltar ao normal, o servidor principal voltará à ativa e o secundário ficará novamente em *standby* para novas falhas eventuais que possam vir a ocorrer.

O sincronismo do H.A. é resiliente, ele atua sincronizando todos os dados em um ambiente temporário, efetua uma validação da integridade dos dados e depois de fato os replica no servidor propriamente dito. Além disso, todos os deploys que não foram concluídos graças a um evento de falha do servidor, serão reiniciados e os pacotes reaplicados garantindo que nenhum dado ou processo seja corrompido por causa de algum evento com os *clusters*.

Por padrão, o servidor é instalado no modo *Standalone*, ou seja, o recurso de *High Availability* vem desabilitado. Caso deseje habilitá-lo altere a caixa de seleção *Operation Mode* em *Cluster Settings* de acordo com qual appliance estiver configurando, caso pretenda configurar o appliance principal, selecione a opção "Primary", caso contrário opte por "Secondary" de modo a configurar o *appliance* que ficará em *standby*.



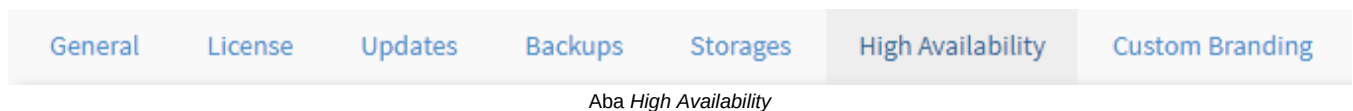
ATENÇÃO: Para configurar o H.A. os seguintes requisitos devem ser observados:

É obrigatório que os dois servidores tenham as mesmas capacidades computacionais (Memória, Processador, Armazenamento e etc), os mesmos modelos e mesmas versões, independente de ser um appliance físico ou virtual.

A funcionalidade de H.A. nas configurações da Manager só poderá ser habilitada quando não houver um Logger local integrado. É obrigatório o uso de *logger standalone*.

O servidor primário precisa estar devidamente licenciado e a licença precisa estar com os dois appliances que serão utilizados vinculados.

Para configurar este recurso, clique na aba "High Availability":



Surgirá a tela à seguir, conforme demonstrado pela imagem abaixo:

System

General

License

Updates

Backups

Storages

High Availability

Custom Branding

Cluster Settings

* Operation Mode

Standalone

Secret Key

Local Key

Peer Interface #1

Select

Peer IP #1

Peer Interface #2

Select

Peer IP #2

Peer Interface #3

Select

Peer IP #3

Peer Key

* Heartbeat Interval (seconds)

3

* Sync Interval (minutes)

5

* Failover Threshold

10

E-mail Notifications

☐ Auto Activation

Cluster Interfaces

Interface

Virtual IP

Netmask

Virtual Mac

☐ ETH0

Select

Cluster Status

Local State

Active Uptime

Peer Connection

Peer State

Synchronization Date

Synchronization Status

System - High Availability

Esta tela é composta pelos painéis:

- [Cluster Settings](#);
- [Cluster Interfaces](#);
- [Cluster Status](#).

Além disso, também exemplificaremos [como configurar appliances com o H.A. habilitado](#).

A seguir analisaremos o painel [Cluster Settings](#).

High Availability - Cluster Interfaces

Este painel exibe todas as interfaces de rede redundantes em um Cluster de alta disponibilidade. À seguir vamos detalhar os componentes deste painel:



A configuração das interfaces usadas pelo cluster do serviço de alta disponibilidade suporta apenas redes IPv4.

Cluster Interfaces

Interface	Virtual IP	Netmask	Virtual MAC
☐ ETH1			
☐ ETH2			
☐ ETH3			

High Availability - Cluster Interfaces

- **Eth** ☐: Ao habilitar esta caixa de checagem, os campos para configurar a interface são habilitados e a interface é ativada para ser usada pelo Cluster;
- **Virtual IP**: Trata-se do IP ao qual os UTMs usam para se comunicar com a *manager*. Define o endereço IP virtual que será iniciado dinamicamente no dispositivo ativo. Este campo é obrigatório;



O IP virtual é o endereço ao qual os UTMs irão se comunicar com a Manager e também é o IP que é utilizado pelo cluster que estiver com prioridade, isso significa que:

Se o servidor primário parar de funcionar, o secundário assumirá o IP virtual que foi configurado neste campo.

Da mesma forma, caso o servidor secundário não seja mais necessário, o primário ativará e assumirá o IP virtual configurado.

- **Netmask**: Determina a máscara de rede que será utilizada pelo endereço IP virtual. Este campo é obrigatório;
- **Virtual MAC**: Define o endereço MAC do IP virtual. Este campo não é obrigatório porém, caso seja deixado em branco, o endereço MAC do próprio *appliance* será utilizado estando passível a conflitos com tabela ARP.



É recomendado adicionar um Virtual MAC, esta configuração é importante para evitar conflitos na rede ou com a tabela *arp*.

À seguir iremos detalhar o painel [Cluster Status](#).

High Availability - Cluster Settings

Neste painel estão todas as configurações básicas do *Cluster* utilizado pelos recursos de alta disponibilidade do GSM, à seguir iremos nos aprofundar em como configurar cada campo.

Cluster Settings

* Operation Mode

Standalone

Secret Key

Local Key

Peer Interface #1

Select

Peer IP #1

Peer Interface #2

Select

Peer IP #2

Peer Interface #3

Select

Peer IP #3

Peer Key

* Heartbeat Interval (seconds)

3

* Sync Interval (minutes)

5

* Failover Threshold

5

E-mail Notifications

☐ Auto Activation

High Availability - Cluster Settings

- **Operation Mode:** Por padrão o recurso de *High Availability* vem desabilitado (*Standalone*), para habilitá-lo altere esta caixa de seleção de acordo com qual appliance estiver configurando. As opções disponíveis são:
 - **Standalone:** Esta é a opção padrão, caso já tenha feito outra configuração, ao selecionar "*Standalone*" novamente o H.A. será desabilitado e o sistema irá operar sem um servidor secundário em redundância;
 - **Primary:** Selecione esta opção, caso pretenda configurar o cluster principal;
 - **Secondary:** Selecione esta opção, caso pretenda configurar o *appliance* que ficará em *standby*.

- **Secret Key:** Define a chave de segurança do *cluster* de alta disponibilidade. A definição desta senha é obrigatória, de forma a garantir que não ocorrerá sincronismo não autorizado nos *clusters*, garantindo a relação de confiabilidade entre ambos os dispositivos. Este campo é obrigatório. É necessário que ambos os *clusters* possuam a mesma *secret key*;
- **Local Key:** Define a chave *do túnel*, trata-se de uma chave local que será utilizada para efetuar a conexão de monitoramento e para sincronismo de dados com o servidor remoto. Este campo é obrigatório. A chave é gerada automaticamente pelo sistema e ela deve ser inserida no *peer key* na outra ponta. Este campo possui os botões:
 - **Copy** [ícone]: Tem como função copiar a chave secreta, de modo a evitar erros de digitação na configuração dos clusters;
 - **Change Key** [ícone]: Este botão permite a criação automática de uma chave secreta aleatória.
- **Peer IP #1:** Neste campo é definido o endereço *IP* de um servidor redundante com função de monitorar o *heartbeat* e efetuar sincronismo de dados. É um campo obrigatório;
- **Peer IP #2:** Assim como no campo acima, é configurado opcionalmente um endereço *IP* redundante para monitoramento e sincronismo. O *Peer IP #2* é ativado em caso de falhas do *Peer IP #1*. Este campo é opcional;
- **Peer IP #3:** Da mesma maneira que os anteriores, é configurado como um endereço *IP* redundante para monitoramento e sincronismo. É ativado em caso de falhas dos *Peers IP #1* e *#2*. Trata-se de um campo opcional.



Nas opções de *Peer IP* é possível configurar 1 ou 2 servidores de *heartbeat*.

No servidor primário deve-se apontar o *Peer IP* do *cluster* secundário.

No servidor secundário deve-se apontar o *Peer IP* do *cluster* primário.



Para configuração dos campos *Peer IP #1*, *#2* e *#3* será necessário configurar as interfaces anteriormente nas configurações de rede, consulte esta [página](#).

- **Peer Key:** Neste campo deve-se adicionar a "*Local Key*" do servidor secundário (ou a do primário, caso esteja configurando o servidor secundário). Ela é utilizada para autorizar a conexão entre os dispositivos. É um campo obrigatório;
- **Heartbeat Interval:** Determina o intervalo de monitoramento, definindo quando serão feitos os testes de conexão e sincronismo entre as interfaces *Heartbeat* dos servidores. O valor neste campo é definido em segundos. Este campo é obrigatório;
- **Sync Interval:** Define o intervalo do sincronismo de todas as configurações do servidor primário para o secundário. Este campo é determinado em minutos. Este campo é obrigatório;
- **Failover Threshold:** Determina o limite de falhas nos testes de *Heartbeat*, caso o valor máximo de erros gerados pelos testes de *Heartbeat* seja alcançado, o servidor secundário será ativado e o primário entrará em *standby* efetuando o *failover* automaticamente. Este campo é determinado em segundos. Este campo é obrigatório;
- **E-mail Notifications:** Neste campo, o administrador pode cadastrar um endereço para recebimento de e-mails de notificações, as mensagens serão enviadas tempo real em eventos de *Failover* e sincronismo. Para que o envio das notificações seja efetuado, é necessário configurar a aba *e-mail* em *Network*, para mais informações, consulte esta [página](#);
- **Auto Activation** [ícone]: Caso esta opção estiver habilitada, a ativação automática entre o dispositivo Secundário e o Primário será efetuada. Assim sendo, caso a máquina primária esteja desativada e esta opção estiver marcada, ele ativará a máquina secundária.

À seguir iremos detalhar o conteúdo do painel [Cluster Interfaces](#).

High Availability - Cluster Status

Os recursos exibidos neste painel possibilitam ter acesso ao estado atual do *Cluster*, além de permitir o sincronismo e ativação manual do servidor secundário. À seguir vamos detalhar as funcionalidades disponíveis nesta tela:

Cluster Status

Local State

SECONDARY ACTIVE

Active Uptime

22:49:56

Peer Connection

DOWN

Peer State

PRIMARY STANDBY

Sincronization Date

09/01/2021 15:30

Sincronization Status

DONE

High Availability - Cluster Status

No topo deste painel temos as seguintes opções:

- **Sync Now** []: Este botão tem como função executar o sincronismo manualmente;
- **Active Now** []: Este botão efetua o *failover* manual do *clusters*, em um cenário normal, por exemplo, ao clicar neste botão a interface secundária será ativada e a primária ficará em *standby*.

Além disso, este painel é composto pelos campos:

- **Local State:** Exibe o estado atual do dispositivo local podendo ser:
 - **Primary Active:** Demonstra que o *Cluster* primário está ativo;
 - **Primary Standby:** Demonstra que o *Cluster* primário está em *Standby*;
 - **Secondary Active:** Demonstra que o *Cluster* secundário está ativo;
 - **Secondary Standby:** Demonstra que o *Cluster* secundário está em *Standby*.
- **Active Uptime:** Exibe por quanto tempo o Cluster alterou o seu status dele para Active. Este campo não exibirá nenhuma informação caso o *cluster* entre em *Standby*. Ex.: 10 days -21:42:07;



Atente que o campo Active Uptime não se refere à quanto tempo o servidor está ligado e sim à quando o status foi alterado para "Active".

- **Peer Connection:** Exibe o estado da conexão do túnel com o dispositivo remoto, podendo ser:
 - **Up:** Demonstra que a conexão está funcionando normalmente;

- **Down:** Demonstra que a conexão caiu.
- **Peer State:** Exibe o estado atual do dispositivo remoto podendo ser:
 - **Primary Active:** Demonstra que o *Cluster* primário está ativo;
 - **Primary Standby:** Demonstra que o *Cluster* primário está em *Standby*;
 - **Secondary Active:** Demonstra que o *Cluster* secundário está ativo;
 - **Secondary Standby:** Demonstra que o *Cluster* secundário está em *Standby*.
- **Synchronization Date:** Exibe a data do último sincronismo. Ex.: 04/12/2020 -21:42:07;
- **Synchronization Status:** Exibe caso o estado do último sincronismo, podendo ser:
 - **Success:** Demonstra que o sincronismo foi efetuado com sucesso;
 - **Error:** Demonstra que ocorreu algum erro no sincronismo.
- **Error Message:** No caso de algum erro, este campo exibe uma mensagem especificando o ocorrido, podendo ser:
 - **Conexão:** Neste caso, a mensagem demonstra que houve um erro na conexão entre os *clusters*;
 - **Integridade:** Esta mensagem demonstra uma falha na integridade de um dos *clusters*.

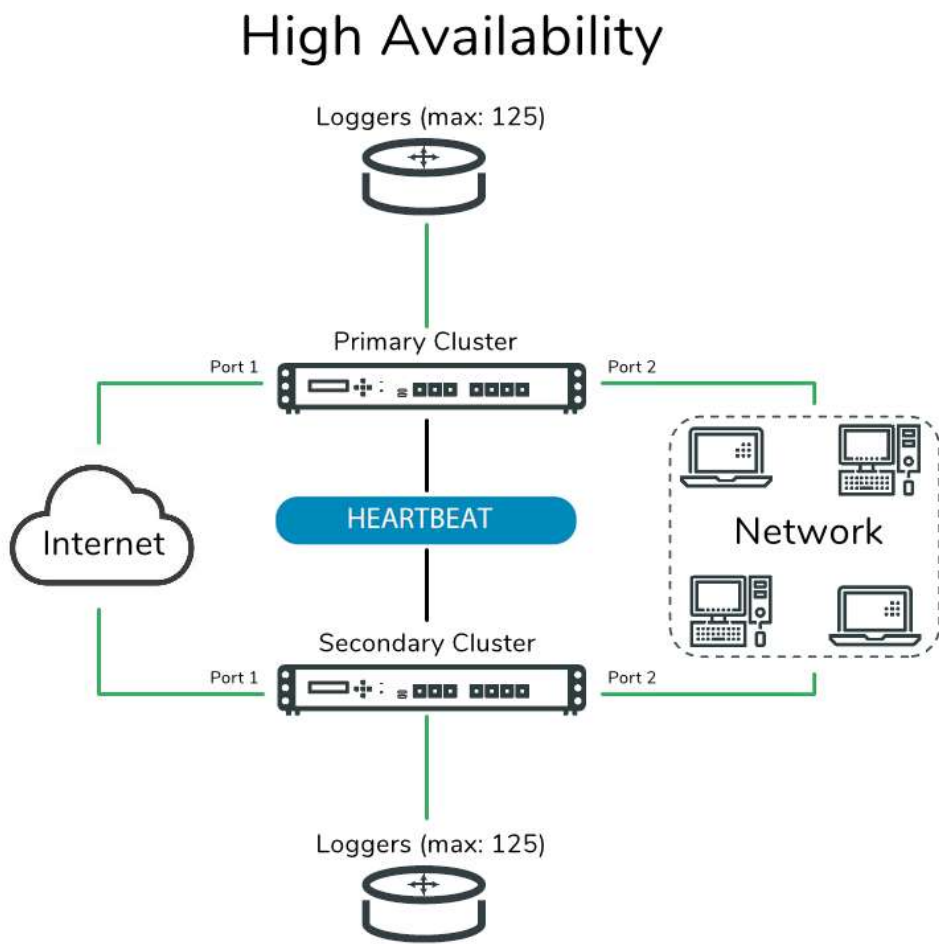
À seguir iremos analisar uma [demonstração de como configurar o H.A. no GSM](#).

High Availability - Exemplo

Esta seção irá apresentar o passo a passo para configuração de um servidor primário e secundário H.A.

 Para mais informações a respeito de H.A. consulte esta [página](#).

Essa demonstração levará em consideração a seguinte estrutura:



High Availability - Estrutura

Os seguintes IPs serão utilizados neste exemplo:

High Availability - Endereçamento IP

Nome	Endereço IP	IP Virtual
Primary Cluster	172.31.207.81	172.31.207.80
Secondary Cluster	172.31.207.82	

Os passos que tomaremos nesta demonstração serão:

1. Configuração do Cluster Primário;
2. Configuração do Cluster Secundário;
3. Validação das Configurações de H.A.

Iniciaremos a demonstração configurando as interfaces do [Cluster Primário](#).

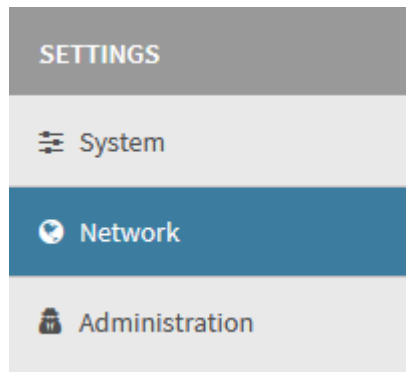
High Availability - Configuração do Cluster Primário

Neste exemplo efetuaremos as seguintes configurações:

- Configuração das interfaces de *heartbeat* pois a comunicação com o *IP* do *cluster* secundário precisa estar funcional para que o *heartbeat* seja efetivo;
- Configuração do *cluster* primário.

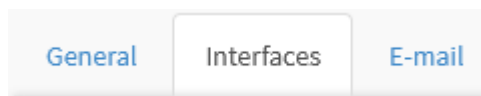
Configuração da Interface

Inicialmente, acesse o menu *Settings* e clique em *Network*:



Settings - Network

Clique na aba *Interfaces*:



Aba Interfaces



Alguns detalhes da aba interfaces não serão considerados neste exemplo, caso deseje mais informações, consulte esta [página](#).

Configure a sua rede conforme o necessário, neste exemplo usaremos a *eth0*:

Add Edit Interface

* IP Address

172.31.207.81

* Mask Address

255.255.0.0

☒ Enable

Cancel

Save

Configurações da *eth0*

- **IP Address:** O endereço IP utilizado pela interface. Seguindo a topologia, o *IP* será 172.31.207.81;
- **Mask Address:** A máscara utilizada por esse endereço *IP*;
- **Enable** ☒: Marque esta caixa de seleção para habilitar a interface.

Clique em  para finalizar as configurações:

Além disso, configuraremos a *eth1* para utilizar no heartbeat com o *Cluster* secundário.

Add Edit Interface

* IP Address

10.10.10.1

* Mask Address

255.255.255.252

☒ Enable

Cancel

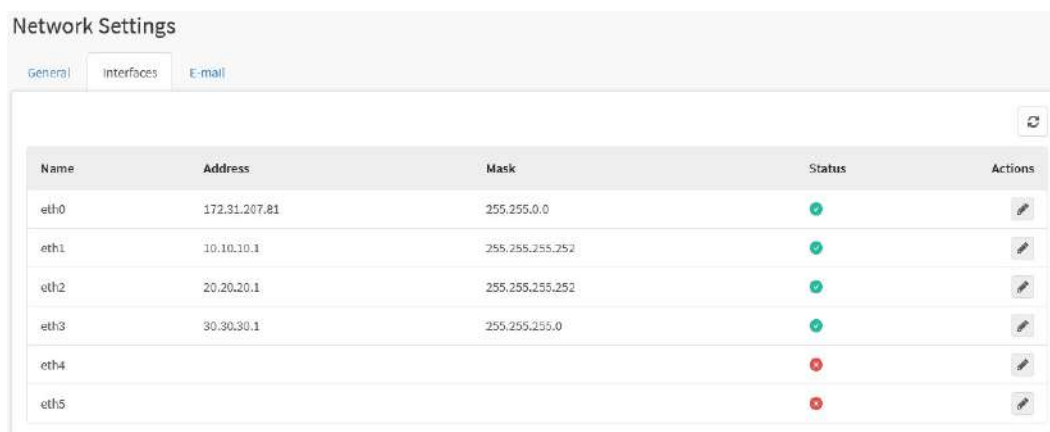
Save

Configurações da *eth1*

- **IP Address:** O endereço IP utilizado pela interface, neste caso usaremos o *IP* 10.10.10.1;
- **Mask Address:** A máscara utilizada por esse endereço *IP*;
- **Enable** ☒: Marque esta caixa de seleção para habilitar a interface.

Clique em  para finalizar as configurações:

O screenshot abaixo exibe as interfaces do *Cluster Primário* já configuradas e habilitadas corretamente:



The screenshot shows the 'Network Settings' window with the 'Interfaces' tab selected. It displays a table of network interfaces with their names, addresses, masks, and status. The status column shows green checkmarks for interfaces eth0 through eth3, and red X marks for eth4 and eth5. Each row has an edit icon in the 'Actions' column.

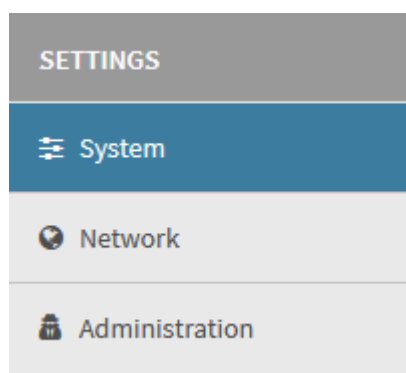
Name	Address	Mask	Status	Actions
eth0	172.31.207.81	255.255.0.0	✓	
eth1	10.10.10.1	255.255.255.252	✓	
eth2	20.20.20.1	255.255.255.252	✓	
eth3	30.30.30.1	255.255.255.0	✓	
eth4			✗	
eth5			✗	

Network Settings - Interfaces

À seguir trataremos das configurações de H.A. do cluster:

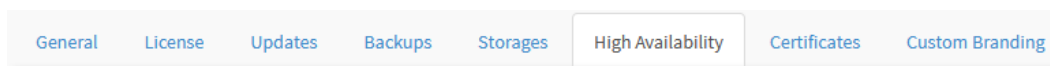
Configurações de H.A.

Acesse o menu Settings e clique na opção *System*:



Settings - System

Clique na aba *High Availability*:



Aba High Availability

A seguinte tela será exibida:

System
General
License
Updates
Backups
Storages
High Availability
Certificates
Custom Branding

Cluster Settings

* Operation Mode

Standalone

Secret Key

Local Key

Peer Interface #1

Select

Peer IP #1

Peer Interface #2

Select

Peer IP #2

Peer Key

* Heartbeat Interval (seconds)

3

* Sync Interval (seconds)

5

* Failover Threshold (seconds)

5

E-mail Notifications

☐ Auto Activation

Cluster Interfaces

Interface	Virtual IP	Netmask	Virtual Mac
☐ ETH0		Select	
☐ ETH1		Select	

Cluster Status

Local State

Active Uptime

Peer Connection

Peer State

Synchronization Date

Synchronization Status

System - High Availability

À seguir vamos detalhar os painéis que precisaremos configurar.

Cluster Settings

Complete o formulário conforme exemplificado a seguir:

Cluster Settings

* Operation Mode

Primary

* Secret Key

.....

* Local Key

53616c7465645f5f8fc2755ad99bb7121060b3c0610ffa71b73be4c6a5d9221b4ebc744432e19008a620832b53b3c5bd3c42f119ce296f2fe02c039dc55f7295c675acae96f1d7b7305bd685cfdbb06f104a4ea6f5cb54d2e43725de74c7e3e322951c829dbc4539ab1381210733c29db8e73

* Peer Interface #1

eth1

* Peer IP #1

10.10.10.2

Peer Interface #2

Select

Peer IP #2

* Peer Key

53616c7465645f5f63fbfe70e19299bbcb1338592a632daa14dba80ba136d49c23a1700b3db6fc492f8767052c6ecb172a0ed5e22ecba3e4ba334a643a2db3c0814512b8857711e9412bc7ef23449eb775980bcef656a1faf191997c30282674460cdb2852fac1008c62b518354b112c4a017

* Heartbeat Interval (seconds)

3

* Sync Interval (seconds)

5

* Failover Threshold (seconds)

5

E-mail Notifications

admin@blockbit.com

☒ Auto Activation

High Availability - Cluster Settings

- **Operation Mode:** Como este será o *Cluster* primário, selecione a opção "Primary";
- **Secret Key:** Define a chave de segurança para a relação de confiança entre os *clusters*, eles precisarão utilizar a mesma chave. Ex.: q1Q!q1Q!;
- **Local Key:** Para gerar um certificado para sincronismo de dados, clique no botão .
- **Peer Interface #1:** Neste campo é adicionada a interface que será utilizada para efetuar o *heartbeat* com *Cluster* Secundário, no caso usaremos a eth1;
- **Peer IP #1:** Neste campo é adicionado o IP da interface que efetuará *heartbeat* com o *Cluster* Secundário, para tanto, usaremos o IP da eth1 do *Cluster* Secundário: 10.10.10.2;
- **Peer Key:** Neste campo deve-se colar o "Local Key" do *Cluster* Secundário;
- **Heartbeat Interval:** Configuraremos o intervalo do *heartbeat* para 3 segundos;
- **Sync Interval:** Configuraremos o intervalo de sincronismo para 5 minutos;
- **Failover threshold:** Configuraremos o limite para 5 falhas;
- **E-mail Notifications:** Adicione o e-mail que será utilizado para receber as notificações do serviço de H.A., no caso usaremos: admin@blockbit.com;

- **Auto Activation** ☒: Por fim, iremos habilitar a auto-ativação para que o cluster seja ativado automaticamente em caso de falha.

À seguir, iremos configurar os IPs virtuais.

Cluster Interfaces

Complete o formulário conforme exemplificado a seguir:

Cluster Interfaces			
Interface	Virtual IP	Netmask	Virtual Mac
☒ ETH0	172.31.207.80	255.255.0.0 ▼	00:0c:29:f4:f1:ff
☐ ETH1		Select ▼	
☐ ETH2		Select ▼	

High Availability - Cluster Interfaces

- **ETH0** ☒: Neste exemplo utilizaremos apenas a interface ETH0, portanto, habilite-a marcando a caixa de checagem;
- **Virtual IP**: Adicione a o IP virtual que o *cluster* irá assumir quando estiverem com prioridade, no exemplo utilizaremos o IP: 172.31.207.80;
- **Netmask**: Adicione a máscara do endereço IP, no caso: 255.255.0.0;
- **Virtual Mac**: O Mac Virtual é opcional, no caso iremos usá-lo para evitar conflitos na tabela ARP. No exemplo usaremos o MAC: 00:0c:29:f4:f1:ff.

Ao finalizar todas as configurações, a tela estará como demonstrado abaixo:

System
General
License
Updates
Backups
Storages
High Availability
Certificates
Custom Branding

Cluster Settings

* Operation Mode

Primary

* Secret Key

* Local Key

S3615c7460d45f5bfc2755ad295b7111040b3c0010fa71b73be4c0e5d9221b4ec344423c13
000a030632155bdc3bc3c42f118e29823e00c0296c59729e0875eaa83f147b7305b095c1
d5b0ef104e4eae8f8cb54d2e43725d674c7e9e523951c825db0f5399b1981210733c25d99c73

* Peer Interface #1

eth1

* Peer IP #1

10.10.10.2

Peer Interface #2

Select

Peer IP #2

* Peer Key

53615c7460d45f5bfc2755ad295b7111040b3c0010fa71b73be4c0e5d9221b4ec344423c13
fc49218767052cfecb172a0e05e2ecba5e4ba334a643a2db3c0814512b857711e9412bc7ef
23440e3775980b0cf656a1faf191937c3028267460c0b2852fac1006c52b518354b112e4e017

* Heartbeat Interval (seconds)

3

* Sync Interval (seconds)

5

* Fallover Threshold (seconds)

5

E-mail Notifications

admin@blockbit.com

☒ Auto Activation

Cluster Interfaces

Interface	Virtual IP	Netmask	Virtual Mac
☒ ETH0	172.31.207.80	255.255.0.0	00:0c:29:f4:f1:ff
☐ ETH1		Select	
☐ ETH2		Select	

Cluster Status

Local State

Active Uptime

Peer Connection

Peer State

Synchronization Date

Synchronization Status

High Availability - Cluster Primário



Para salvar, clique em [].

Isso finaliza a configuração do cluster primário, à seguir iremos [configurar o cluster secundário](#).

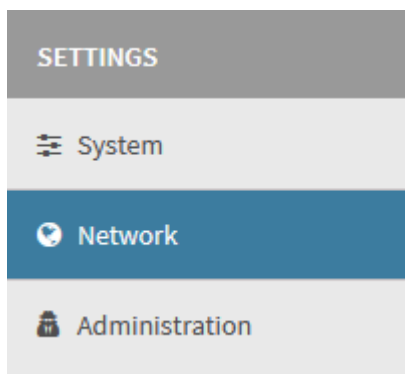
High Availability - Configuração do Cluster Secundário

Após ter feito as configurações no [Cluster Primário](#), efetuaremos as seguintes configurações no Secundário:

- É necessário realizar o *Wizard* de Instalação da máquina secundária, conforme orientações desta [página](#).
- Configuração das interfaces de *heartbeat* pois a comunicação com o *IP* do *cluster* primário precisa estar funcional para que o *heartbeat* seja efetivo;
- Configuração do *cluster* secundário.

Configuração da Interface

Acesse o menu *Settings* e clique em *Network*:



Settings - Network

Clique na aba *Interfaces*:



Aba Interfaces



Alguns detalhes da aba interfaces não serão considerados neste exemplo, caso deseje mais informações, consulte esta [página](#).

Configure a sua rede conforme o necessário, neste exemplo usaremos a *eth0*:

Add Edit Interface

* IP Address

172.31.207.82

* Mask Address

255.255.0.0

☒ Enable

Cancel

Save

Configurações da *eth0*

- **IP Address:** O endereço IP utilizado pela interface. Seguindo a topologia, o *IP* será 172.31.207.82;
- **Mask Address:** A máscara utilizada por esse endereço *IP*;
- **Enable** ☒: Marque esta caixa de seleção para habilitar a interface.

Clique em  para finalizar as configurações:

Além disso, configuraremos a *eth1* para utilizar no heartbeat com o *Cluster* Primário.

Add Edit Interface

* IP Address

10.10.10.2

* Mask Address

255.255.255.252

☒ Enable

Cancel

Save

Configurações da *eth1*

- **IP Address:** O endereço IP utilizado pela interface, neste caso usaremos o *IP* 10.10.10.2;
- **Mask Address:** A máscara utilizada por esse endereço *IP*;
- **Enable** ☒: Marque esta caixa de seleção para habilitar a interface.

Save

Clique em [] para finalizar as configurações:

O screenshot abaixo exhibe as interfaces do *Cluster Primário* já configuradas e habilitadas corretamente:

Network Settings

General Interfaces E-mail

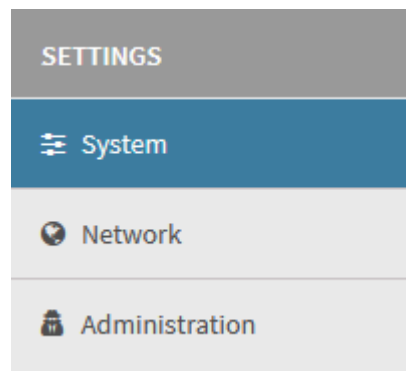
Name	Address	Mask	Status	Actions
eth0	172.31.207.82	255.255.0.0	✓	
eth0	172.31.207.82	255.255.0.0	✓	
eth1	10.10.10.2	255.255.255.252	✓	
eth2	20.20.20.2	255.255.255.252	✓	
eth3	30.30.30.2	255.255.255.0	✓	
eth4			✗	
eth5			✗	

Network Settings - Interfaces

À seguir trataremos das configurações de H.A. do cluster:

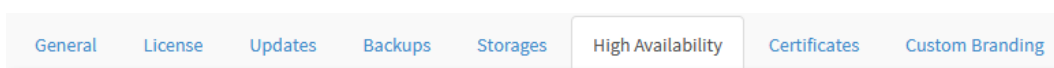
Configurações de H.A.

Acesse o menu Settings e clique na opção System:



Settings - System

Clique na aba High Availability:



Aba High Availability

A seguinte tela será exibida:

System

General License Updates Backups Storages **High Availability** Certificates Custom Branding

Cluster Settings

* **Operation Mode**
Standalone

Secret Key
[password field]

Local Key
[password field]

Peer Interface #1
Select

Peer IP #1
[text field]

Peer Interface #2
Select

Peer IP #2
[text field]

Peer Key
[password field]

* **Heartbeat Interval (seconds)**
3

* **Sync Interval (seconds)**
5

* **Failover Threshold (seconds)**
5

E-mail Notifications
[text field]

☐ Auto Activation

Cluster Interfaces

Interface	Virtual IP	Netmask	Virtual Mac
☐ ETH0	[text field]	Select	[text field]
☐ ETH1	[text field]	Select	[text field]

Cluster Status

Local State
[text field]

Active Uptime
[text field]

Peer Connection
[text field]

Peer State
[text field]

Synchronization Date
[text field]

Synchronization Status
[text field]

System - High Availability

À seguir vamos detalhar os painéis que precisaremos configurar.

Cluster Settings

Complete o formulário conforme exemplificado a seguir:

Cluster Settings

* Operation Mode

Secondary

* Secret Key

.....

* Local Key

53616c7465645f5f63fbfe70e19299bbcb1338592a632daa14dba80ba136d49c23a1700b3db6fc492f8767052c6ecb172a0ed5e22ecba3e4ba334a643a2db3c0814512b8857711e9412bc7ef23449eb775980bcef656a1faf191997c30282674460cdb2852fac1008c62b518354b112c4a017

* Peer Interface #1

eth1

* Peer IP #1

10.10.10.1

Peer Interface #2

Select

Peer IP #2

* Peer Key

53616c7465645f5f8fc2755ad99bb7121060b3c0610ffa71b73be4c6a5d9221b4ebc744432e19008a620832b53b3c5bd3c42f119ce296f2fe02c039dc55f7295c675acae96f1d7b7305bd685cfdbb06f104a4ea6f5cb54d2e43725de74c7e3e322951c829dbc4539ab1381210733c29db8e73

* Heartbeat Interval (seconds)

3

* Sync Interval (seconds)

5

* Failover Threshold (seconds)

5

E-mail Notifications

admin@blockbit.com

☒ Auto Activation

High Availability - Cluster Settings

- **Operation Mode:** Como este será o Cluster Secundário, selecione a opção "Secondary";
- **Secret Key:** Define a chave de segurança para a relação de confiança entre os clusters, eles precisarão utilizar a mesma chave. Ex.: q1Q!q1Q!;
- **Local Key:** Para gerar um certificado para sincronismo de dados, clique no botão [🔄];
- **Peer Interface #1:** Neste campo é adicionada a interface que será utilizada para efetuar o heartbeat com Cluster Primário, no caso usaremos a eth1;
- **Peer IP #1:** Neste campo é adicionado o IP da interface que efetuará heartbeat com o Cluster Primário, para tanto, usaremos o IP da eth1 do cluster Primário: 10.10.10.1;
- **Peer Key:** Neste campo deve-se colar o "Local Key" do Cluster Primário;
- **Heartbeat Interval:** Configuraremos o intervalo do heartbeat para 3 segundos;
- **Sync Interval:** Configuraremos o intervalo de sincronismo para 5 minutos;
- **Failover threshold:** Configuraremos o limite para 5 falhas;
- **E-mail Notifications:** Adicione o e-mail que será utilizado para receber as notificações do serviço de H.A., no caso usaremos: admin@blockbit.com;

- **Auto Activation** ☒: Por fim, iremos habilitar a auto-ativação para que o cluster seja ativado automaticamente em caso de falha.

À seguir, iremos configurar os IPs virtuais.

Cluster Interfaces

Complete o formulário conforme exemplificado a seguir:

Cluster Interfaces			
Interface	Virtual IP	Netmask	Virtual Mac
☒ ETH0	172.31.207.80	255.255.0.0 ▼	00:0c:29:f4:f1:ff
☐ ETH1		Select ▼	
☐ ETH2		Select ▼	

High Availability - Cluster Interfaces

- **ETH0** ☒: Neste exemplo utilizaremos apenas a interface ETH0, portanto, habilite-a marcando a caixa de checagem;
- **Virtual IP**: Adicione a o IP virtual que o *cluster* irá assumir quando estiverem com prioridade, no exemplo utilizaremos o IP: 172.31.207.80;
- **Netmask**: Adicione a máscara do endereço IP, no caso: 255.255.0.0;
- **Virtual Mac**: O Mac Virtual é opcional, no caso iremos usá-lo para evitar conflitos na tabela ARP. No exemplo usaremos o MAC: 00:0c:29:f4:f1:ff.

Ao finalizar todas as configurações, a tela estará como demonstrado abaixo:

System
General
License
Updates
Backups
Storages
High Availability
Certificates

Cluster Settings

* Operation Mode
Secondary

* Secret Key

* Local Key
50616c7465645f5f6c2735ad98b7111090b3c0410f7a71b73ben1c5a5d9221b4ebc74432e19008a62632b53b3c5b3c42f113cc23692fe02c039dc5f7295c675ecce9f9d7b7305b0605cfdbb09f104a4ea8f5cb54d2e43725de74c7e9e922951c829d0c4539ab1381210733c29d0b6e73

* Peer Interface #1
eth1

* Peer IP #1
10.10.10.1

Peer Interface #2
Select

Peer IP #2

* Peer Key
50616c7465645f5f6c2735ad98b7111090b3c0410f7a71b73ben1c5a5d9221b4ebc74432e19008a62632b53b3c5b3c42f113cc23692fe02c039dc5f7295c675ecce9f9d7b7305b0605cfdbb09f104a4ea8f5cb54d2e43725de74c7e9e922951c829d0c4539ab1381210733c29d0b6e73

* Heartbeat Interval (seconds)
3

* Sync Interval (seconds)
5

* Failover Threshold (seconds)
5

E-mail Notifications
admin@blockbit.com

☒ Auto Activation

Cluster Interfaces

Interface	Virtual IP	Netmask	Virtual Mac
☒ ETH0	172.31.207.80	255.255.0.0	00:0c:29:44:1f:1f
☐ ETH1		Select	
☐ ETH2		Select	

Cluster Status

Local State

Active Uptime

Peer Connection

Peer State

Synchronization Date

Synchronization Status

High Availability - Cluster Secundário



Para salvar, clique em [].

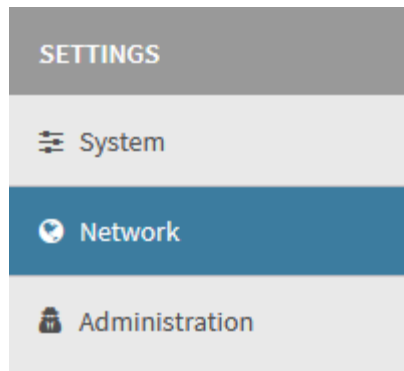
Isso finaliza a configuração no cluster secundário, à seguir iremos [validar as configurações](#).

Após ter feito as configurações no [Cluster Primário](#), efetuaremos as seguintes configurações no Secundário:

- Configuração das interfaces de *heartbeat* pois a comunicação com o *IP* do *cluster* primário precisa estar funcional para que o *heartbeat* seja efetivo;
- Configuração do *cluster* secundário.

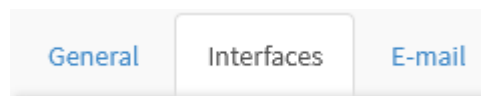
Configuração da Interface

Acesse o menu *Settings* e clique em *Network*:



Settings - Network

Clique na aba *Interfaces*:



Aba *Interfaces*



Alguns detalhes da aba interfaces não serão considerados neste exemplo, caso deseje mais informações, consulte esta [página](#).

Configure a sua rede conforme o necessário, neste exemplo usaremos a eth0:

Add Edit Interface

* IP Address

172.31.207.82

* Mask Address

255.255.0.0

☒ Enable

Cancel

Save

Configurações da *eth0*

- **IP Address:** O endereço IP utilizado pela interface. Seguindo a topologia, o IP será 172.31.207.82;
- **Mask Address:** A máscara utilizada por esse endereço IP;

- **Enable** ☒: Marque esta caixa de seleção para habilitar a interface.

Save

Clique em [] para finalizar as configurações:

Além disso, configuraremos a eth1 para utilizar no heartbeat com o *Cluster* Primário.

Add Edit Interface

* IP Address

10.10.10.2

* Mask Address

255.255.255.252

☒ Enable

Cancel
Save

Configurações da *eth1*

- **IP Address:** O endereço IP utilizado pela interface, neste caso usaremos o *IP* 10.10.10.2;
- **Mask Address:** A máscara utilizada por esse endereço *IP*;
- **Enable** ☒: Marque esta caixa de seleção para habilitar a interface.

Save

Clique em [] para finalizar as configurações:

O *screenshot* abaixo exhibe as interfaces do *Cluster Primário* já configuradas e habilitadas corretamente:

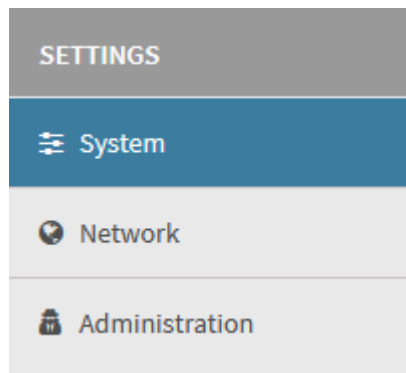
General Interfaces E-mail				
Name	Address	Mask	Status	Actions
eth0	172.31.207.82	255.255.0.0	✓	
eth0	172.31.207.82	255.255.0.0	✓	
eth1	10.10.10.2	255.255.255.252	✓	
eth2	20.20.20.2	255.255.255.252	✓	
eth3	30.30.30.2	255.255.255.0	✓	
eth4			✗	
eth5			✗	

Network Settings - Interfaces

À seguir trataremos das configurações de H.A. do cluster:

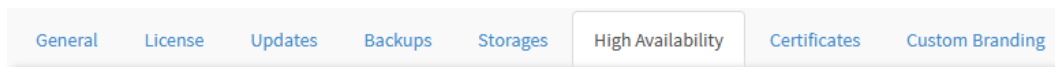
Configurações de H.A.

Acesse o menu Settings e clique na opção *System*:



Settings - System

Clique na aba *High Availability*:



Aba High Availability

A seguinte tela será exibida:

System
General
License
Updates
Backups
Storages
High Availability
Certificates
Custom Branding

Cluster Settings

* Operation Mode

Standalone

Secret Key

Local Key

Peer Interface #1

Select

Peer IP #1

Peer Interface #2

Select

Peer IP #2

Peer Key

* Heartbeat Interval (seconds)

3

* Sync Interval (seconds)

5

* Failover Threshold (seconds)

5

E-mail Notifications

☐ Auto Activation

Cluster Interfaces

Interface	Virtual IP	Netmask	Virtual Mac
☐ ETH0		Select	
☐ ETH1		Select	

Cluster Status

Local State

Active Uptime

Peer Connection

Peer State

Synchronization Date

Synchronization Status

System - High Availability

À seguir vamos detalhar os painéis que precisaremos configurar.

Cluster Settings

Complete o formulário conforme exemplificado a seguir:

Cluster Settings

* Operation Mode

Secondary

* Secret Key

.....

* Local Key

53616c7465645f5f63fbfe70e19299bbcb1338592a632daa14dba80ba136d49c23a1700b3db6fc492f8767052c6ecb172a0ed5e22ecba3e4ba334a643a2db3c0814512b8857711e9412bc7ef23449eb775980bcef656a1faf191997c30282674460cdb2852fac1008c62b518354b112c4a017

* Peer Interface #1

eth1

* Peer IP #1

10.10.10.1

Peer Interface #2

Select

Peer IP #2

* Peer Key

53616c7465645f5f8fc2755ad99bb7121060b3c0610ffa71b73be4c6a5d9221b4ebc744432e19008a620832b53b3c5bd3c42f119ce296f2fe02c039dc55f7295c675acae96f1d7b7305bd685cfdbb06f104a4ea6f5cb54d2e43725de74c7e3e322951c829dbc4539ab1381210733c29db8e73

* Heartbeat Interval (seconds)

3

* Sync Interval (seconds)

5

* Failover Threshold (seconds)

5

E-mail Notifications

admin@blockbit.com

☒ Auto Activation

High Availability - Cluster Settings

- **Operation Mode:** Como este será o Cluster Secundário, selecione a opção "Secondary";
- **Secret Key:** Define a chave de segurança para a relação de confiança entre os clusters, eles precisarão utilizar a mesma chave. Ex.: q1Q!q1Q!;
- **Local Key:** Para gerar um certificado para sincronismo de dados, clique no botão [🔄];
- **Peer Interface #1:** Neste campo é adicionada a interface que será utilizada para efetuar o heartbeat com Cluster Primário, no caso usaremos a eth1;
- **Peer IP #1:** Neste campo é adicionado o IP da interface que efetuará heartbeat com o Cluster Primário, para tanto, usaremos o IP da eth1 do cluster Primário: 10.10.10.1;
- **Peer Key:** Neste campo deve-se colar o "Local Key" do Cluster Primário;
- **Heartbeat Interval:** Configuraremos o intervalo do heartbeat para 3 minutos;
- **Sync Interval:** Configuraremos o intervalo de sincronismo para 5 segundos;
- **Failover threshold:** Configuraremos o limite para 5 falhas;
- **E-mail Notifications:** Adicione o e-mail que será utilizado para receber as notificações do serviço de H.A., no caso usaremos: admin@blockbit.com;

- **Auto Activation** ☒: Por fim, iremos habilitar a auto-ativação para que o cluster seja ativado automaticamente em caso de falha.

À seguir, iremos configurar os IPs virtuais.

Cluster Interfaces

Complete o formulário conforme exemplificado a seguir:

Cluster Interfaces			
Interface	Virtual IP	Netmask	Virtual Mac
☒ ETH0	172.31.207.80	255.255.0.0 ▼	00:0c:29:f4:f1:ff
☐ ETH1		Select ▼	
☐ ETH2		Select ▼	

High Availability - Cluster Interfaces

- **ETH0** ☒: Neste exemplo utilizaremos apenas a interface ETH0, portanto, habilite-a marcando a caixa de checagem;
- **Virtual IP**: Adicione a o IP virtual que o *cluster* irá assumir quando estiverem com prioridade, no exemplo utilizaremos o IP: 172.31.207.80;
- **Netmask**: Adicione a máscara do endereço IP, no caso: 255.255.0.0;
- **Virtual Mac**: O Mac Virtual é opcional, no caso iremos usá-lo para evitar conflitos na tabela ARP. No exemplo usaremos o MAC: 00:0c:29:f4:f1:ff.

Ao finalizar todas as configurações, a tela estará como demonstrado abaixo:

System
General
License
Updates
Backups
Storages
High Availability
Certificates

Cluster Settings

* Operation Mode
Secondary

* Secret Key

* Local Key
50616c7465645f5f6c2795ad98bb7110c90b3c0410fa71b73benca5d9221b4ebc74432e19008a62032b53b3c5b3c42f113cc2362fe02c039dc5c77295c975ec9e9f9d7b7305b0605cfdbb09f104afea8f5cb54d2e43725de74c7e9e922951c829dbca4539ab1381210733c29db0e73

* Peer Interface #1
eth1

* Peer IP #1
10.10.10.1

Peer Interface #2
Select

Peer IP #2

* Peer Key
50616c7465645f5f6c2795ad98bb7110c90b3c0410fa71b73benca5d9221b4ebc74432e19008a62032b53b3c5b3c42f113cc2362fe02c039dc5c77295c975ec9e9f9d7b7305b0605cfdbb09f104afea8f5cb54d2e43725de74c7e9e922951c829dbca4539ab1381210733c29db0e73

* Heartbeat Interval (seconds)
3

* Sync Interval (seconds)
5

* Failover Threshold (seconds)
5

E-mail Notifications
admin@bblockbit.com

☒ Auto Activation

Cluster Interfaces

Interface	Virtual IP	Netmask	Virtual Mac
☒ ETH0	172.31.207.80	255.255.0.0	00:0c:29:44:11:11
☐ ETH1		Select	
☐ ETH2		Select	

Cluster Status

Local State

Active Uptime

Peer Connection

Peer State

Synchronization Date

Synchronization Status

High Availability - Cluster Secundário



Para salvar, clique em [].

Isso finaliza a configuração no cluster secundário, à seguir iremos [validar as configurações](#).

High Availability - Validação das Configurações

Para efetuar a validação, iremos acessar a CLI do Cluster Primário e rodar alguns comandos, caso necessite de mais informações a respeito, consulte esta [página](#).

Um dos testes mais simples para validar o funcionamento do H.A. é efetuar um [ping](#) do Cluster Primário (172.31.207.81) para o Secundário (172.31.207.82) e verificar se há resposta, conforme demonstrado pela imagem a seguir:

```
admin >ping 172.31.207.82
PING 172.31.207.82 (172.31.207.82) 56(84) bytes of data.
64 bytes from 172.31.207.82: icmp_seq=1 ttl=64 time=0.179 ms
64 bytes from 172.31.207.82: icmp_seq=2 ttl=64 time=0.257 ms
64 bytes from 172.31.207.82: icmp_seq=3 ttl=64 time=0.173 ms
64 bytes from 172.31.207.82: icmp_seq=4 ttl=64 time=0.169 ms
64 bytes from 172.31.207.82: icmp_seq=5 ttl=64 time=0.109 ms

--- 172.31.207.82 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4107ms
rtt min/avg/max/mdev = 0.109/0.177/0.257/0.048 ms
admin >
```

CLI - Validação da comunicação do Cluster Primário para o Secundário

Também é possível efetuarmos estes mesmos passos na outra pontas, segue uma demonstração usando o comando [ping](#) para verificar a comunicação do Cluster Secundário (172.31.207.82) para o Primário (172.31.207.81):

```
admin >ping 172.31.207.81
PING 172.31.207.81 (172.31.207.81) 56(84) bytes of data.
64 bytes from 172.31.207.81: icmp_seq=1 ttl=64 time=0.233 ms
64 bytes from 172.31.207.81: icmp_seq=2 ttl=64 time=0.211 ms
64 bytes from 172.31.207.81: icmp_seq=3 ttl=64 time=0.246 ms
64 bytes from 172.31.207.81: icmp_seq=4 ttl=64 time=0.182 ms
64 bytes from 172.31.207.81: icmp_seq=5 ttl=64 time=0.267 ms
64 bytes from 172.31.207.81: icmp_seq=6 ttl=64 time=0.305 ms

--- 172.31.207.81 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5123ms
rtt min/avg/max/mdev = 0.182/0.240/0.305/0.043 ms
admin >
```

CLI - Validação da comunicação do Cluster Secundário para Primário através do comando Ping

Além disso, após efetuar a configuração a própria interface exibe o estado atual de ambos os Clusters, em Local State é exibido o estado atual da máquina que se logado no momento e Peer State exibe o estado da máquina na outra ponta. No exemplo abaixo estamos observando o painel do Cluster Primário que está ativo, enquanto o Cluster Secundário está em Standby:

Cluster Status

Local State

PRIMARY ACTIVE

Active Uptime

00:43:13

Peer Connection

UP

Peer State

SECONDARY STANDBY

Sincronization Date

13/01/2021 15:59

Sincronization Status

DONE

Cluster Status do Cluster Primário

Segue o mesmo painel, porém observado pela ponta do Cluster secundário:

Cluster Status

Local State

SECONDARY STANDBY

Active Uptime

01:09:53

Peer Connection

UP

Peer State

PRIMARY ACTIVE

Sincronization Date

13/01/2021 17:05

Cluster Status do Cluster Secundário

Por fim, para garantir que o H.A. está funcionando corretamente, podemos desligar o Cluster Primário, para isso iremos dar o comando `[shutdown]` na *CLI* do Cluster primário. Graças a ele não estar mais disponível, o secundário assumirá a prioridade e subirá no IP 172.31.207.80 definido anteriormente nas interfaces do cluster. O painel de status refletirá essas mudanças, conforme demonstrado abaixo:

Cluster Status



Local State	SECONDARY ACTIVE
Active Uptime	
Peer Connection	DOWN
Peer State	PRIMARY STANDBY
Synchronization Date	13/01/2021 17:35
Synchronization Status	DONE

Cluster Status do Cluster Secundário após o Primário ter sido desligado

Isso conclui a demonstração, para mais informações a respeito de *High Availability*, consulte esta [página](#).

Para mais informações sobre os status de *High Availability*, consulte esta [página](#).

System - Aba "Certificates"

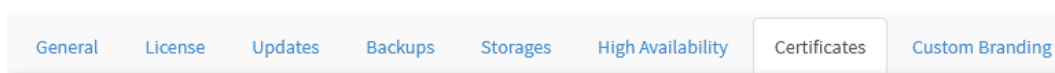
Os recursos desta aba, permitem que o administrador configure sua própria autoridade certificadora, sendo esta uma maneira simples e prática de se obter o certificado que será utilizado para garantir confiabilidade no acesso aos recursos da solução.

O propósito de uma autoridade certificadora é confirmar a titularidade dos certificados, confirmando que o certificado recebido ao acessar determinado *site* ou endereço pertence realmente à entidade que o está fornecendo. É isso que garante que você está mesmo acessando os sites e endereços *SSL/HTTPS* de forma segura.



É necessário configurar uma CA nesta aba poder criar um provedor de identidade SAML, para mais informações consulte esta [página](#).

Para acessar a interface de gerenciamento de certificados, acesse a aba *Certificates*.



Aba *Certificates*

System - Backups

A seguir iremos detalhar os campos deste formulário.

- **Country:** Determina o país. Ex.: *US*;
- **State:** Define o estado. Ex.: *New York*;
- **City:** Determina a cidade. Ex.: *New York*;
- **Organization:** Define o nome da empresa. Ex.: *Blockbit*;
- **E-mail:** Determina o e-mail do administrador. Ex.: *admin@blockbit.com*;
- **Organizational Unit:** Define o departamento. Ex.: *QA*;
- **Expires (years):** Determina o tempo de validade do certificado. Ex.: 10 anos;
- **Hostname:** Define o Hostname da CA. Ex.: *admin@blockbit.com*;
- **Key Size:** Define o tamanho que a chave da CA possuirá. Ex.: 2048.



Ao finalizar a configuração, clique em [] para salvar.



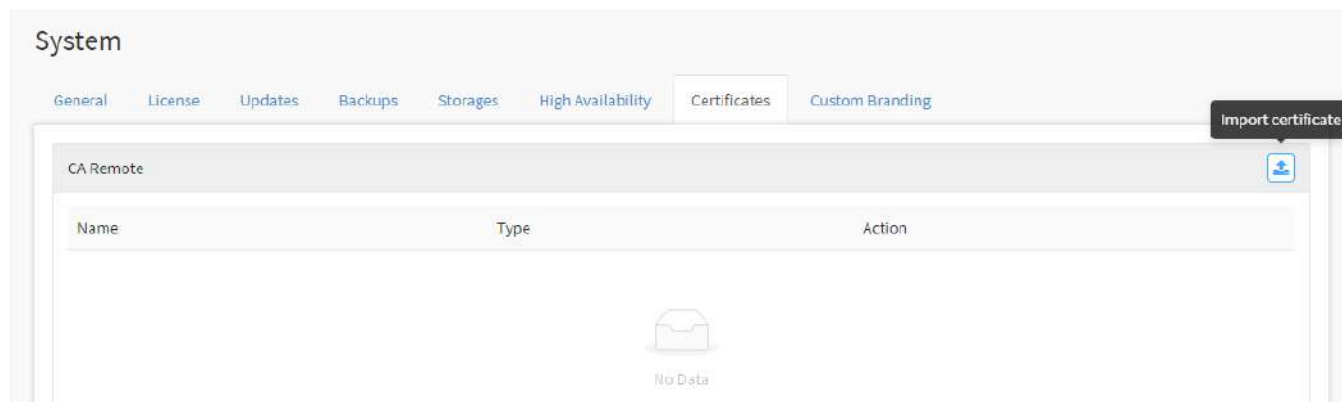
Salvar uma CA requer que o servidor gere uma nova entidade certificadora. Esta ação exige a reinstalação da nova CA em todos os dispositivos da rede.



Caso deseje recriar a CA, você também deve refazer o Certificado do Servidor, este procedimento requer a instalação da nova CA em todos os dispositivos da rede. Faça o download da CA e reinstale em todas as estações de trabalho. Lembrando que para validação da nova CA você deve REINICIAR o servidor.

Import Certificates

Esta opção permite fazer o upload de certificados em formato `.CRT` ou `.PEM`:



Certificates - Import Certificate

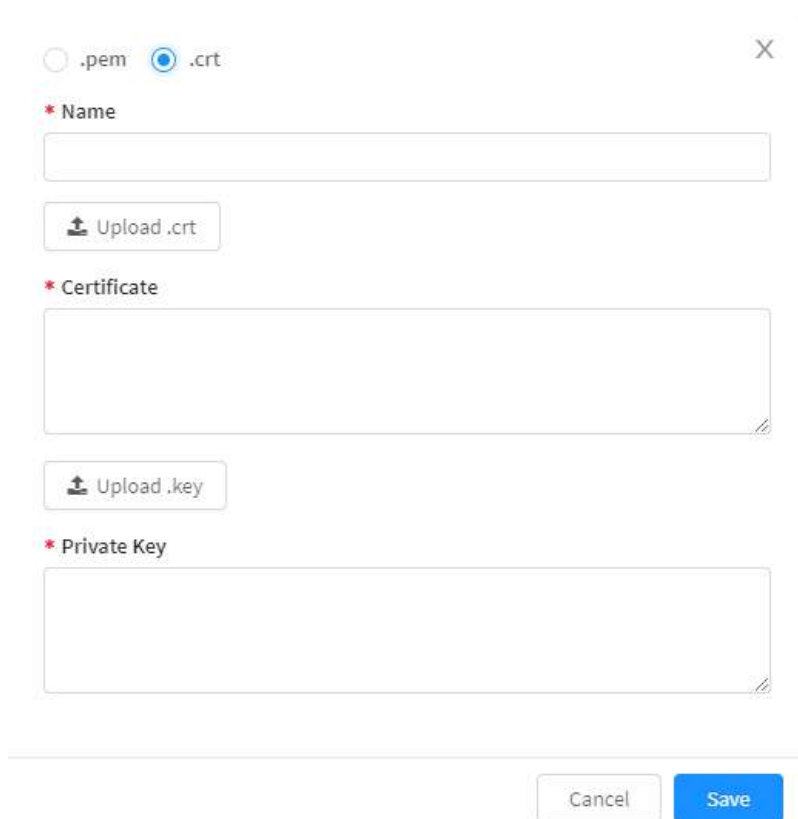
Ao clicar em *Import certificate*, a tela de upload aparecerá:

Import certificates - .PEM files

- **Name:** Insira um nome customizado para o certificado;
- **Upload .PEM:** Selecione o certificado `.PEM` a ser utilizado;

- **Certificate:** Insira o nome do certificado;
- **Private Key:** Campo para a inserção da chave de validação do certificado.

Ao selecionar a opção .CRT o campo *upload key* surgirá:



☐ .pem
 ☒ .crt
 X

*** Name**

 Upload .crt

*** Certificate**

 Upload .key

*** Private Key**

Import Certificates - .CRT files

- **Name:** Insira um nome customizado para o certificado.
- **Upload .CRT:** Selecione o certificado .CRT a ser utilizado.
- **Certificate:** Insira o nome do certificado.
- **Upload .KEY:** Campo para selecionar o arquivo .KEY.
- **Private Key:** Campo para a inserção da chave de validação do certificado.

Isso conclui a configuração da aba *certificates*.

A seguir vamos analisar a aba [Custom Branding](#).

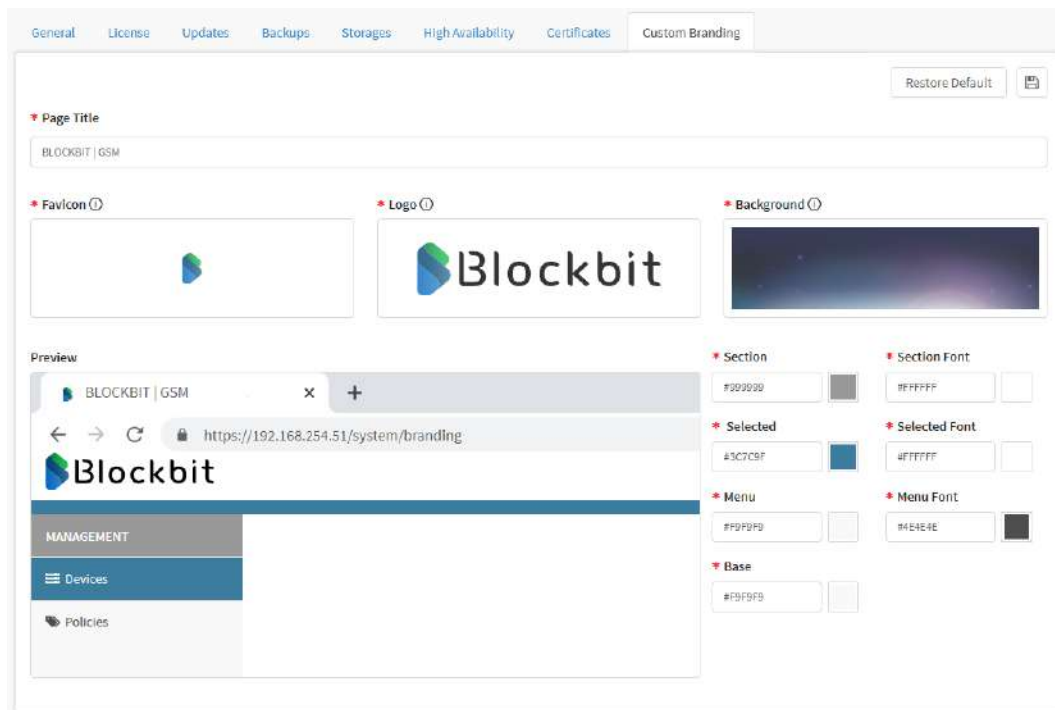
System - Aba "Custom Branding"

Nesta aba o GSM pode ser customizado, sendo possível alterar o título do produto, ícone, imagem de fundo, cores de menu etc. Usando estas opções é possível personalizar o GSM de acordo com a identidade visual utilizada pela empresa do usuário.

A customização de *appliances* é controlada através de licença, assim sendo, essa opção só estará disponível caso o usuário possua uma licença de customização válida ativa. Se a licença do GSM permitir a customização, a aba *custom branding* estará disponível.

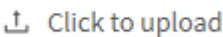
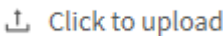


Para mais informações a respeito de como customizar UTMs, consulte essa [página](#).



System Settings - Custom Branding

- **Page title:** Define o nome que será exibido na barra de título na janela do sistema. Ex.: UTM;
- **Section:** Esta opção customiza a cor das seções do GSM (onde aparece "Management", "Analytics" e "Settings"), este campo aceita o código de cor HEX, além disso é possível clicar no quadro ao lado e selecionar a cor desejada em um *color picker* com campo RGBA. Ex.: #89968e;
- **Section Font:** Nesta opção é customizada a cor das fontes das seções do GSM, este campo aceita o código de cor HEX, além disso é possível clicar no quadro ao lado e selecionar a cor desejada em um *color picker* com campo RGBA. Ex.: #000000;
- **Selected:** Nesta opção é customizada a cor dos menus selecionados e da barra superior do GSM, este campo aceita o código de cor HEX, além disso é possível clicar no quadro ao lado e selecionar a cor desejada em um *color picker* com campo RGBA. Ex.: #466452;
- **Selected Font:** Nesta opção é customizada a cor da fonte dos menus selecionados, este campo aceita o código de cor HEX, além disso é possível clicar no quadro ao lado e selecionar a cor desejada em um *color picker* com campo RGBA. Ex.: #f9f9f9;
- **Menu:** Nesta opção é customizada a cor dos menus, este campo aceita o código de cor HEX, além disso é possível clicar no quadro ao lado e selecionar a cor desejada em um *color picker* com campo RGBA. Ex.: #81d47a;
- **Menu Font:** Nesta opção é customizada a cor das fontes dos menus, este campo aceita o código de cor HEX, além disso é possível clicar no quadro ao lado e selecionar a cor desejada em um *color picker* com campo RGBA. Ex.: #000000;
- **Base:** Nesta opção é customizada a cor base do painel onde ficam os menus, este campo aceita o código de cor HEX, além disso é possível clicar no quadro ao lado e selecionar a cor desejada em um *color picker* com campo RGBA. Ex.: #b4daaa;

- **Favicon:** Ao clicar no botão  permite efetuar o *upload* do *favicon* da página. Caso deseje visualizar a imagem adicionada, clique em , para fazer download clique em , para excluir, clique em . O formato necessita ser PNG ou ICO, as dimensões mínimas são 24x24, não há tamanho máximo, só é necessário que a imagem possua mesma altura e largura (seja quadrada);
- **Logo:** Ao clicar no botão  permite efetuar o *upload* do logo utilizado no topo dos menus. Caso deseje visualizar a imagem adicionada, clique em , para excluir, clique em . O formato necessita ser SVG de dimensões 300x65. Não há tamanho máximo, só é necessário que a imagem possua altura e largura diferentes (seja retangular);

 Click to upload

- **Background:** Ao clicar no botão  permite efetuar o *upload* de uma imagem que é utilizada como background na tela inicial de login. Caso deseje visualizar a imagem adicionada, clique em , para excluir, clique em . O formato necessita ser *PNG* ou *JPG* de dimensões 1920x1080;
- **Preview:** Demonstra as alterações que foram efetuadas nas opções acima em uma pré-visualização para checagem antes de efetivamente aplicá-las.

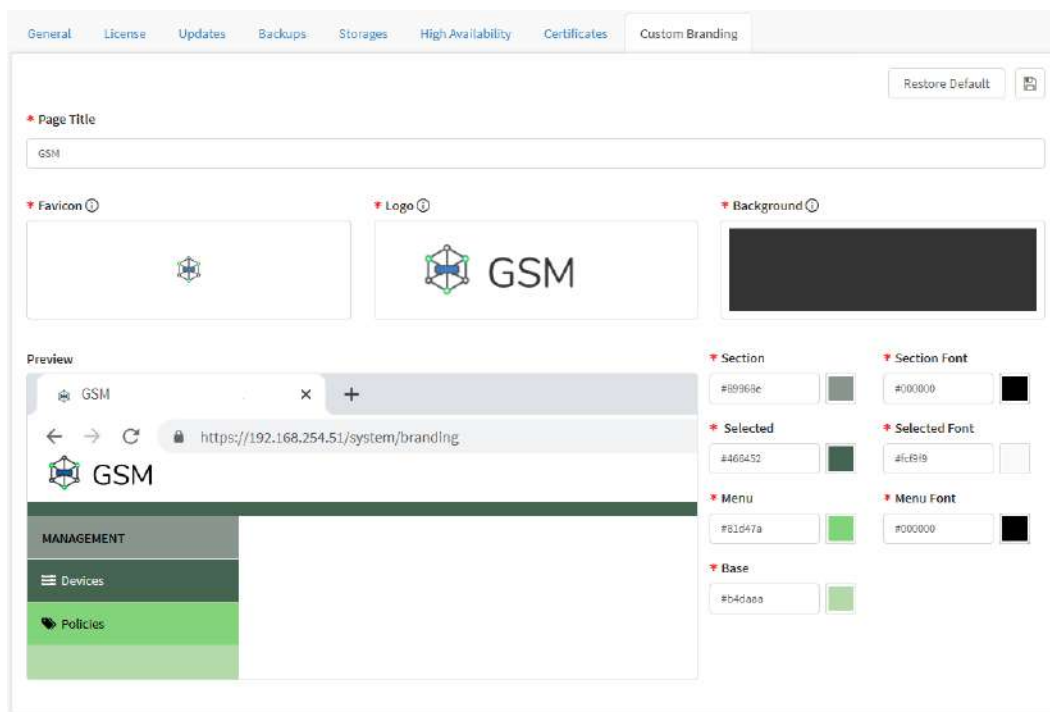


Para auxiliar na definição das cores:

É possível criar ou consultar uma paleta de cores no site <https://coolors.co/generate> que disponibiliza informações da coloração em: *Color Name*, *HEX*, *RGB*, *HSB*, *HSL*, *CMYK*, *LAB*, *RAL*, *HKS*, *Copic* e *Prismacolor*.

Caso seja necessário converter de *Pantone* para *RGB*, *CMYK* ou *HEX*, consulte o conversor do site oficial neste link: <https://www.pantone.com/color-finder>.

Segue um exemplo de um template com a customização já aplicada:



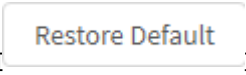
Config Template - Custom Branding - Template editado



Ao aplicar o *custom branding* no UTM pode ser necessário apagar o cache do navegador para visualizar as mudanças.

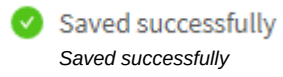
Para acessar a janela de deleção de *cache* basta utilizar o comando "*ctrl+shift+del*".

Restore Default

Caso não fique satisfeito com as alterações efetuadas clique em  para restaurar às configurações padrões.



Para salvar as alterações clique em .



Após realizar esses procedimentos a customização do *firewall* foi efetuada com sucesso.

Para mais informações sobre as abas em *System*, consulte esta [página](#).

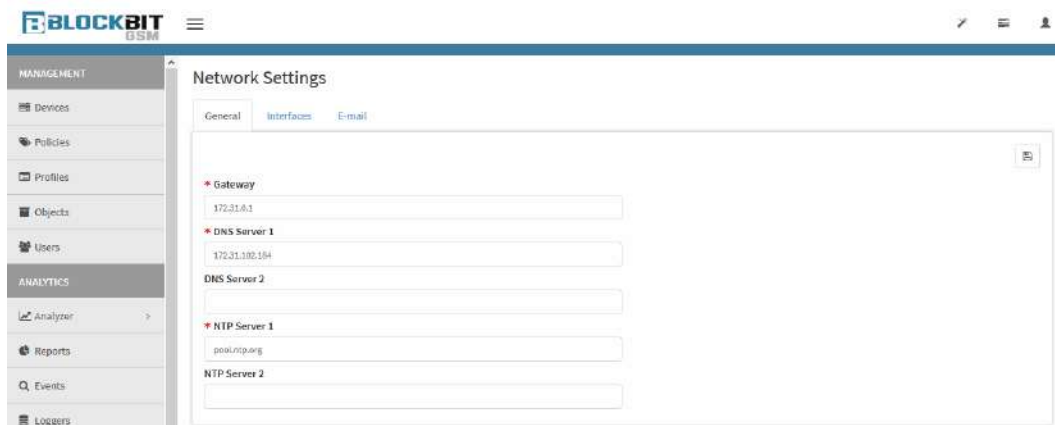
Network

Através do botão "Network" é possível alterar as configurações de rede.



Settings – Network.

Surgirá a tela *System* com a aba "General" pré-selecionada., conforme demonstrado abaixo:



Settings – Network - Aba "General".

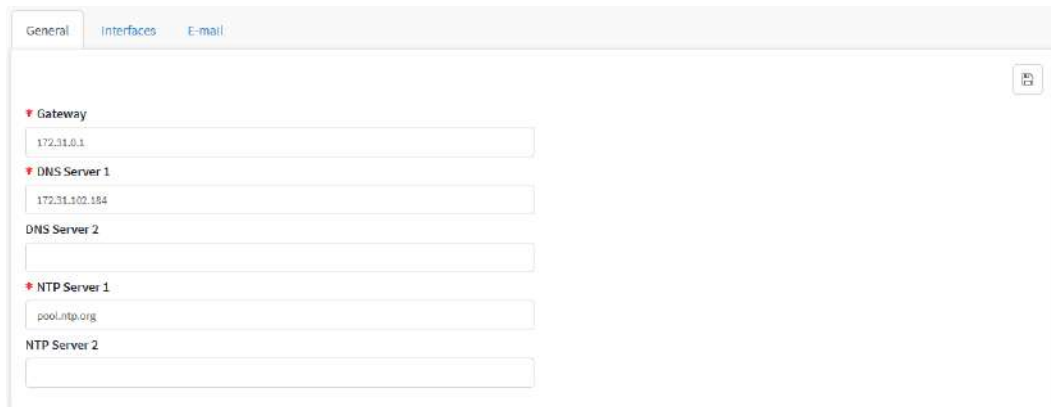
A tela *Network Settings* comporta as seguintes abas:

- [General](#);
- [Interfaces](#);
- [E-mail](#).

Descreveremos a seguir as funcionalidades.

Network - Aba "General"

Esta tela permite alterar as configurações de servidores:



Network Settings

- **Gateway:** Endereço da rota padrão da rede. Ex.: 172.16.102.1;
- **DNS Server 1:** Defina o servidor *DNS* da rede ou da *internet*. Ex.: 176.16.102.161;
- **DNS Server 2:** Defina o *DNS* secundário da sua rede ou da *internet*. Ex.: *DNS* secundário do *Google* 8.8.4.4;
- **NTP Server 1:** Defina o servidor de sincronização de relógio. Ex.: a.ntp.br;
- **NTP Server 2:** Defina o servidor secundário de sincronização de relógio. Ex.: b.ntp.br.

Clique em **save**  localizado no canto superior direito da tela para salvar as alterações feitas nas configurações.

Network - Aba "Interfaces"

Esta tela permite alterar as configurações de interface de rede.

General Interfaces E-mail				
Name	Address	Mask	Status	Actions
eth0	172.31.240.245	255.255.0.0		
eth1				
eth2				
eth3				

Network Interfaces

- **Name:** O nome das interfaces de rede. Ex.: eth0;
- **Address:** Endereço IP do Blockbit GSM. Ex.: 172.16.102.235;
- **Mask:** Máscara de rede. Ex.: 255.255.254.0;
- **Status:** Determina se a interface de rede está **habilitada** ou **desabilitada** , para ativar o status, edite a interface;
- **Action:** Ao clicar no botão **edit** , permite editar as configurações de rede;
- **Botão Reload Interfaces:** Ao clicar no botão **refresh** atualiza o número de interfaces de rede existentes no Blockbit GSM.

Para editar as configurações de rede de uma interface siga os passos abaixo:

1. Na coluna Action clique no botão **Edit** . Preencha os dados que deseja editar:

- **Address:** Endereço IP do Blockbit GSM. Ex.: 10.0.0.1;
- **Mask:** Máscara de rede. Ex.: 255.255.255.0.

Add Edit Interface

* IP Address

172.31.240.245

* Mask Address

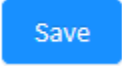
255.255.0.0

☒ Enable

Cancel

Save

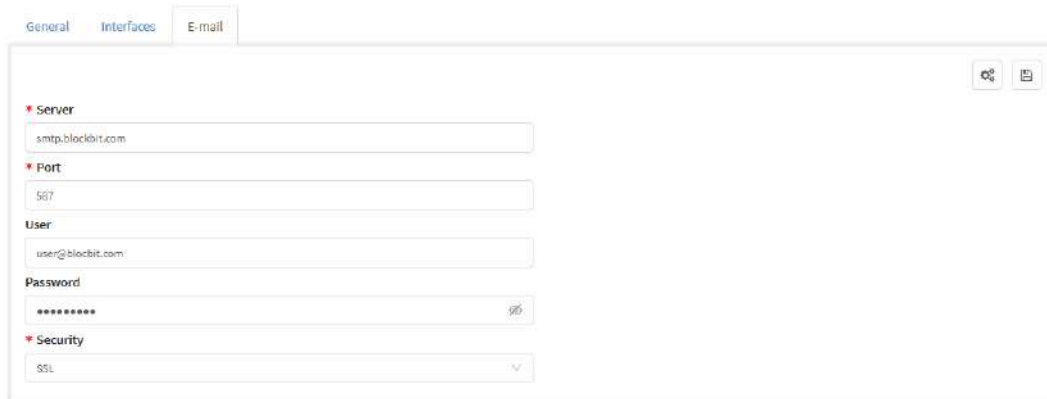
Edit Interface.

2. Para salvar as alterações clique em **Save** ], caso contrário, clique em **Cancel** ] para fechar a janela.

Clique em **synchronize** ] localizado no canto superior direito da tela para salvar as alterações feitas nas configurações.

Network - Aba "E-mail"

Esta tela permite alterar as configurações de envio e recebimento de notificações via *e-mail*.



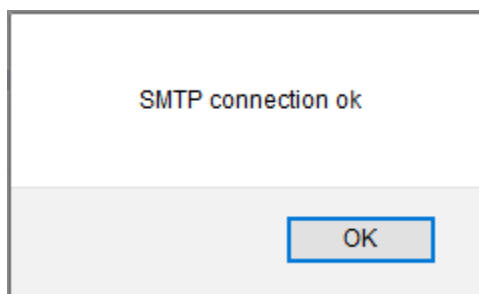
E-mail

A seguir analisaremos cada campo do formulário:

- **Server:** Determina o servidor de *e-mail*. Ex.: smtp.blockbit.com;
- **Port:** Determina a porta a ser utilizada. Ex.: 587;
- **User:** O *e-mail* do usuário. Ex.: user@blockbit.com;
- **Password:** A senha a ser utilizada;
- **Security:** O tipo de criptografia tendo três opções: "SSL", "TLS" e "none" (nenhuma criptografia).

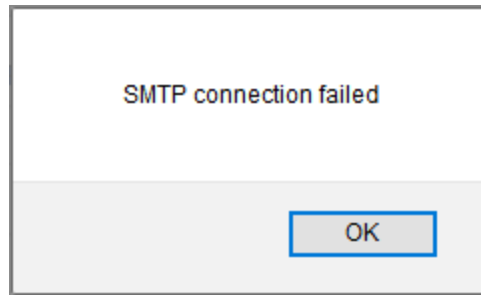
Após completar os campos, é recomendável executar uma verificação clicando no botão **configurations** , a seguir analisaremos esse procedimento:

- **Botão Configurações:** Ao clicar no botão **configurations**  é feita uma verificação no servidor para detectar se ele está funcionando corretamente. Uma validação nas credenciais de acesso é executada e por fim, é feita uma checagem no serviço da porta, podendo exibir três mensagens:
 - **SMTP connection ok:** Caso as configurações estejam funcionando corretamente, conforme exemplificado pela imagem abaixo;



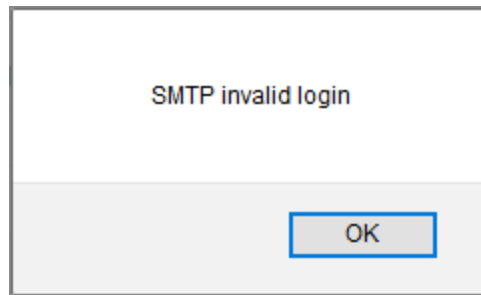
SMTP connection ok

- **SMTP connection failed:** Caso exista algum erro nas configurações do servidor, conforme exemplificado pela imagem abaixo;



SMTP connection failed

- **SMTP invalid login:** Caso as credenciais estejam incorretas, conforme exemplificado pela imagem abaixo.



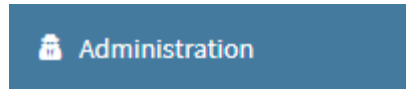
SMTP invalid login

Clique em **save**  localizado no canto superior direito da tela para salvar as alterações feitas nas configurações.

Administration

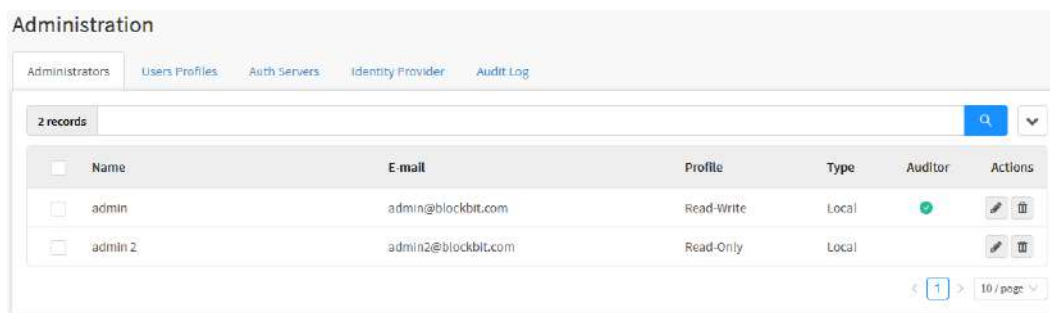
Através do botão “Administration” é possível alterar as configurações administrativas do GSM.

Para tanto, clique na opção adequada como demonstrado abaixo:



Settings – Administration

Surgirá a tela *Administration* com a aba “Administrators” pré-selecionada, conforme demonstrado abaixo:



Settings – Administration

A tela *Administration* comporta as seguintes abas:

- [Administrators](#);
- [Users Profiles](#);
- [Auth Servers](#);
- [Identity Provider](#);
- [Audit Log](#).

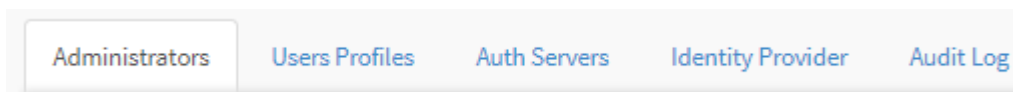
Descreveremos a seguir todas funcionalidades desta tela.

Administration - Aba "Administrators"

Na aba "Administrators" é possível cadastrar usuários de perfil administrativo no Blockbit GSM.

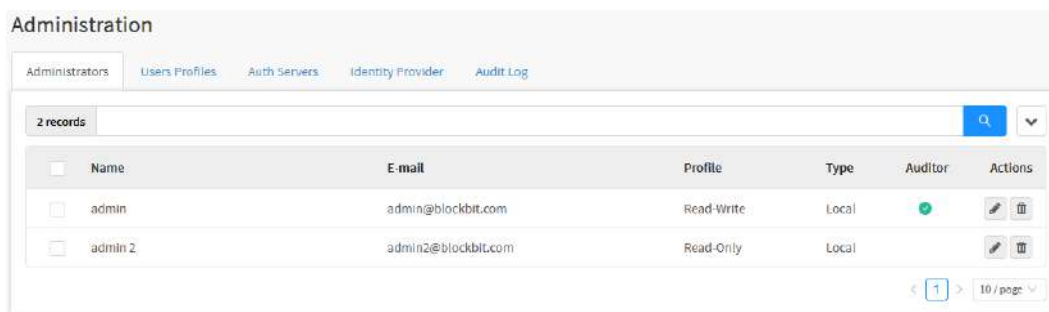
A aba "Administrators" é composta por seis colunas: "Name", "E-mail", "Profile", "Type", "Auditor" e "Actions" e além disso, no topo da tela estão localizados a barra de busca e o menu de ações.

Caso já não esteja selecionada, clique na aba "Administrators".



Aba Administrators

Surgirá a tela demonstrada pela imagem abaixo:



Administration - Administrators

Esta seção irá abordar o [Cadastro](#), Edição e [Remoção](#) dos usuários administradores;

A seguir, analisaremos cada componente deste painel.

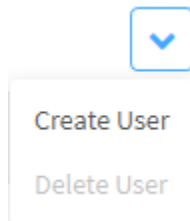
Administration - Administrators - Menu de Ações

No topo direito da tela temos o menu de ações:



Users – Botão do menu de ações

Ao clicar neste botão o menu abaixo é exibido:



Users – Menu de ações

O menu é composto das seguintes opções:

- [Create User](#);
- [Delete User](#).

A seguir cada opção do menu de ações será detalhada.

Administrators - Menu de Ações - Create User



Ao acessar o **menu de ações** [] e clicar no botão "Create User", aparecerá o formulário "Create Admin User", conforme ilustrado pela imagem abaixo.

Administration – Create Admin User.

Neste formulário é possível criar um novo usuário com seu respectivo perfil de acesso, conforme os campos abaixo:

- **Name:** Nome do usuário. Ex.: "Admin";
- **E-mail:** O e-mail de acesso do usuário. Ex.: "admin@blockbit.com";
- **Profile:** Nessa sessão é possível determinar o perfil de acesso do usuário que está sendo cadastrado. Selecione o perfil previamente cadastrado na aba "Profiles" na lista suspensa. Ex.: "WebFilter - Admins";
- **Type:** Define se o usuário administrador fará login local ou efetuará acesso remoto ao sistema. Caso tenha selecionado "Remote" o formulário exibirá o campo para seleção do tipo de servidor ao invés da senha e confirmação desta mesma. Consulte a imagem abaixo para mais informações;
- **Server:** Caso em "Type" a opção "Remote" tenha sido selecionada, este campo será exibido ao invés de "Password" e "Confirm Password". Selecione o servidor remoto que será utilizado na autenticação remota, os itens presentes nesta caixa de seleção são adicionados na aba [Server](#);
- **Password:** Caso em "Type" a opção "Local" tenha sido selecionada, este campo será exibido ao invés de "Server". Digite a senha de acesso do usuário;

- **Confirm Password:** Assim como "Password" este campo está disponível apenas no acesso local, sua função é efetuar a confirmação de segurança da senha, digite-a novamente;
- **Auditor:** Essa caixa de seleção, determina se o usuário possui acesso como "Auditor".

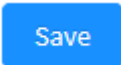
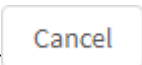
Como mencionado anteriormente, caso o no campo "Type" seja selecionado a opção "Remote", o campo "Server" será exibido, conforme demonstrado pela imagem abaixo:

The image shows a 'Create Admin User' dialog box. It has a title bar with the text 'Create Admin User' and a close button (X) on the right. The dialog contains the following fields:

- * Name**: A text input field.
- * User**: A text input field.
- * Profile**: A dropdown menu.
- * Type**: A dropdown menu with 'Remote' selected.
- * Server**: A dropdown menu with 'LDAP Server' selected.
- Auditor**: A checkbox.

At the bottom right of the dialog, there are two buttons: 'Cancel' and 'Save'.

Administration – Create Admin User

Clique no botão  para gravar todas as alterações, caso contrário, clique em , ou no  do topo direito da tela, para fechar a janela.

Administrators - Menu de Ações - Delete User

O botão "Delete User" do menu de ações serve para remover usuários que foram previamente selecionados ao clicar na caixa de seleção. Como demonstrado abaixo:

Administration

Administrators Users Profiles Auth Servers Identity Provider Audit Log

2 records

☐	Name	E-mail	Profile	Type	Auditor	Actions
☐	admin	admin@blockbit.com	Read-Write	Local		
☒	test	test@blockbit.com	Read-Only	Local		

< 1 > 10 / page

Administration - Seleção para remoção

Depois de selecionar essa opção, uma mensagem de verificação aparecerá requisitando a confirmação.

Delete User X

Are you sure you want to delete the following User ?

- Test

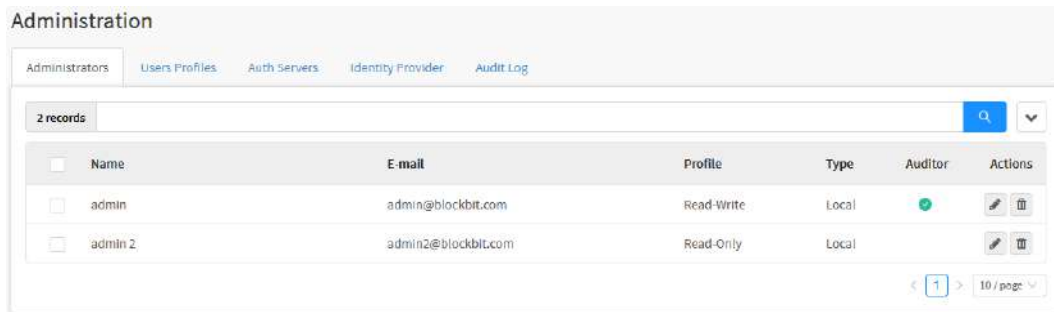
Cancel Delete

Delete User

Ao clicar em , os usuários selecionados serão removidos. Caso clique em , essa mensagem de verificação será dispensada sem efetuar nenhuma remoção.

Administration - Administrators - Colunas

A seguir explicaremos cada coluna da aba Administrators:



The screenshot shows the 'Administration' interface with the 'Administrators' tab selected. It displays a table with 2 records. The table has columns: Name, E-mail, Profile, Type, Auditor, and Actions. The records are 'admin' and 'admin 2'.

☐	Name	E-mail	Profile	Type	Auditor	Actions
☐	admin	admin@blockbit.com	Read-Write	Local		
☐	admin 2	admin2@blockbit.com	Read-Only	Local		

Administration - Users

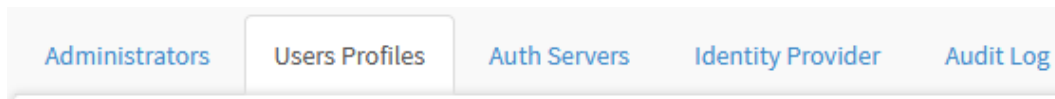
- **Select** ☐: Permite selecionar um ou mais *users*;
- **Name**: Exibe o nome do usuário administrador do Blockbit GSM;
- **E-mail**: Exibe o *E-mail* do usuário cadastrado;
- **Profile**: Determina o perfil de usuário, este perfil é configurado na aba [Users Profiles](#);
- **Type**: Exibe se o usuário administrador fará *login* local ou efetuará acesso remoto ao sistema. Esta opção é configurada ao [criar o usuário](#);
- **Auditor**: Caso o usuário possua permissão de auditor o ícone será exibido. Esta opção é configurada ao [criar o usuário](#);
- **Actions**: Disponibiliza as seguintes funções essenciais:
 - **Edit** : Permite editar um *user* dos usuários [adicionados](#);
 - **Delete** : Permite [deletar](#) um *user*.

Administration - Aba "Users Profiles"

Na aba "Users Profiles" visualizamos os Perfis de administradores do *Blockbit* GSM, a sua função é determinar o nível de acesso e restrição que usuários configurados com determinado perfil passarão a ter dentro do sistema. Este recurso garante mais especificidade na gestão de permissões dos usuários administrativos.

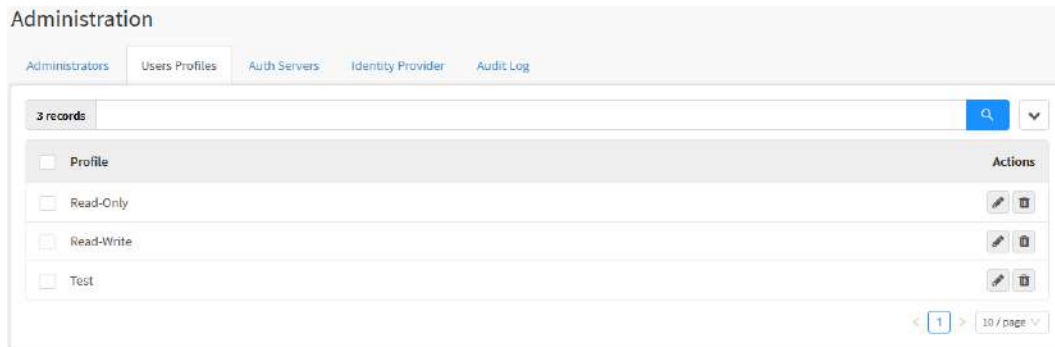
A aba "Users Profiles" é composta pelas colunas: "Profile" e "Actions" e além disso, no topo da tela estão localizados a barra de busca e o menu de ações.

Clique na aba "Users Profiles".



Aba Users Profiles

Surgirá a tela demonstrada pela imagem abaixo:



Administration - Users Profiles

Esta seção irá abordar o [Cadastro](#), Edição e [Remoção](#) dos perfis de administradores do GSM;

A seguir, analisaremos cada componente deste painel.

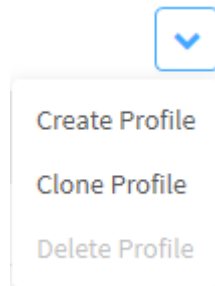
Administration - Users Profiles - Menu de Ações

No topo direito da tela temos o menu de ações:



Users Profiles – Botão do menu de ações

Ao clicar neste botão o menu abaixo é exibido:



Users Profiles – Menu de ações.

O menu é composto das seguintes opções:

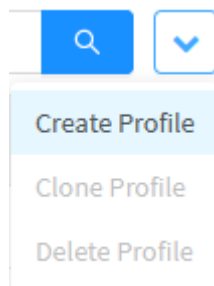
- [Create Profile](#);
- [Clone Profile](#);
- [Delete Profile](#).

A seguir cada opção do menu de ações será detalhada.

Users Profiles - Menu de Ações - Create Profile

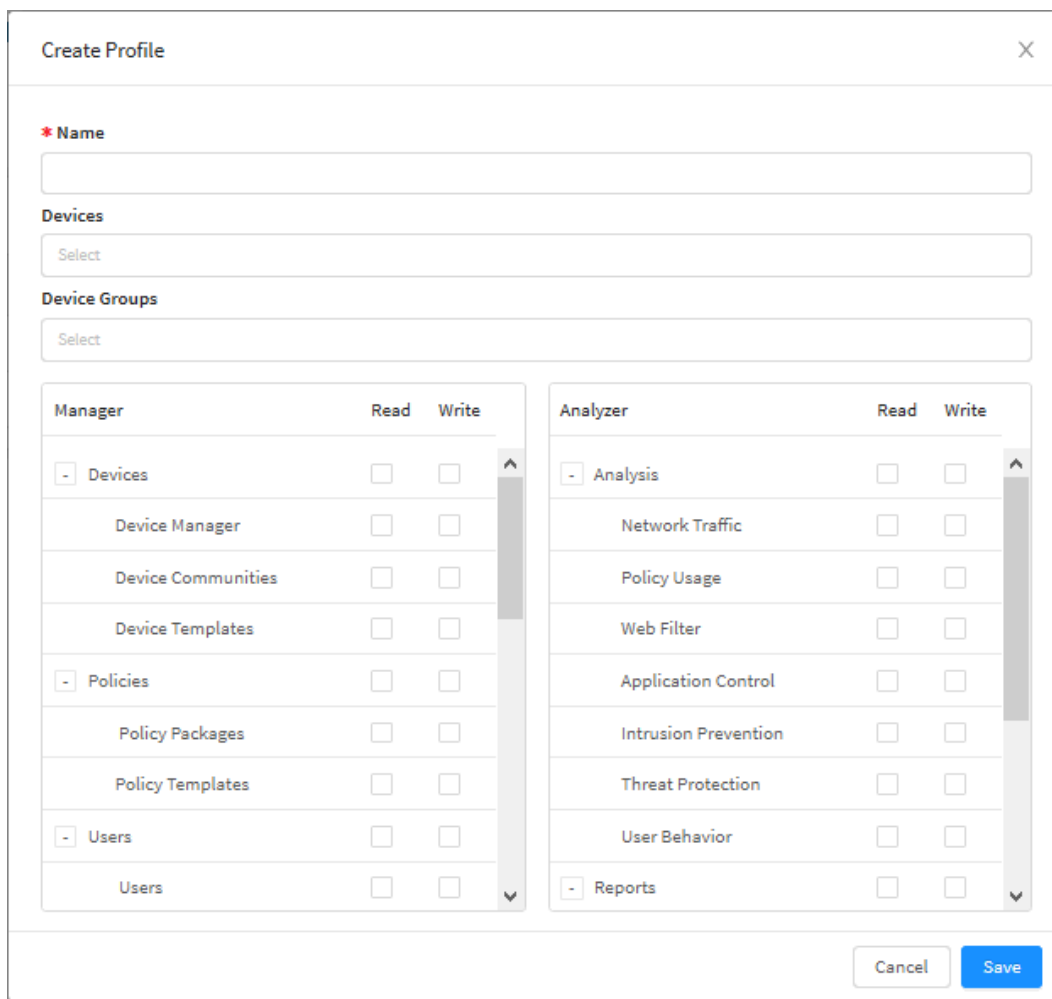
Nesta opção é possível criar um perfil de usuário e configurar as permissões de acesso que ele terá dentro do sistema. Ao criar um usuário e atrelar este perfil, todas as configurações efetuadas nesta sessão entrarão em vigor.

Para criar um novo perfil, acessar o **menu de ações** [] e clique no botão "Create Profile"



Menu de Ações - Create Profile

Aparecerá a tela de configuração dos perfis de administração, como demonstrado abaixo:



Create Profile [Close]

*** Name**

Devices

Device Groups

Manager	Read	Write
☐ Devices	☐	☐
Device Manager	☐	☐
Device Communities	☐	☐
Device Templates	☐	☐
☐ Policies	☐	☐
Policy Packages	☐	☐
Policy Templates	☐	☐
☐ Users	☐	☐
Users	☐	☐

Analyzer	Read	Write
☐ Analysis	☐	☐
Network Traffic	☐	☐
Policy Usage	☐	☐
Web Filter	☐	☐
Application Control	☐	☐
Intrusion Prevention	☐	☐
Threat Protection	☐	☐
User Behavior	☐	☐
☐ Reports	☐	☐

Create Profile

A seção "Profile" permite definir as permissões que o perfil irá controlar, à seguir vamos detalhar todos os campos desta tela:

- **Name:** Nome do perfil de administração. Ex.: "WebFilter - Admins";
- **Devices:** Permite selecionar à quais devices estas opções serão aplicadas;
- **Device Groups:** Permite selecionar quais grupos de devices onde estas opções serão aplicadas. Ex.: "Pool Web Filters";
- **Manager:** Exibe vários menus expansivos com conjuntos de módulos e configurações do Manager do Blockbit GSM, é possível controlar o acesso através das caixas de seleção, tendo as seguintes permissões: "None" (nenhuma), "Read Only" (somente leitura) e por fim, "Read" e "Write" (leitura e escrita). Os conjuntos são:
 - **Devices:** Device Manager, Device Communities, e Device Template;
 - **Policies:** Policy Manager e Policy Templates;
 - **Users:** Users e Users Groups;
 - **Objects:** Tratam-se dos tipos de objeto, Addresses, Services, Times, Schedules, Dictionaries e Content Types;
 - **Settings:** Telas do menu do usuário, System, Network e Admin;
 - **Deploys:** Tela do Deploys Panel.
- **Analyzer:** Exibe vários menus expansivos com conjuntos de módulos e configurações do Analyzer do Blockbit GSM, é possível controlar o acesso através das caixas de seleção, tendo as seguintes permissões: "None" (nenhuma), "Read Only" (somente leitura) e por fim, "Read" e "Write" (leitura e escrita). Os conjuntos são:
 - **Analysis:** Network Traffic, Police Usage, Web Filter, Application Control, Intrusion Prevention, Threat Protection e User Behavior;
 - **Reports:** Trata-se do painel de relatórios, sua única opção é "Reports";
 - **Events:** Se refere ao painel de eventos, sua única opção é "Events";
 - **Loggers:** Determina o acesso ao painel de "Loggers", sendo esta mesma sua única opção.

Para definir as permissões desejadas, selecione o item, expanda a opção através do botão mais [+] (caso seja necessário) e clique com o mouse no ícone de seleção [], conforme exemplo abaixo:

Create Profile

×

* Name

Test

Devices

Select

Device Groups

Select

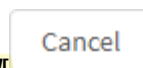
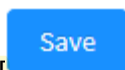
Manager	Read	Write
- Devices	☐	☐
Inventory	☒	☒
Communities	☒	☒
Templates	☒	☒
Provisioning	☒	☒
Backups	☐	☐
- Policies	☐	☐
Packages	☐	☐
Templates	☐	☐

Analyzer	Read	Write
- Analyzer	☐	☐
Network Traffic	☐	☐
Web Filter	☐	☐
Application Control	☐	☐
Intrusion Prevention	☐	☐
Threat Protection	☐	☐
User Behavior	☐	☐
- Reports	☐	☐
Reports	☐	☐

Cancel

Save

Create Profile - Exemplo



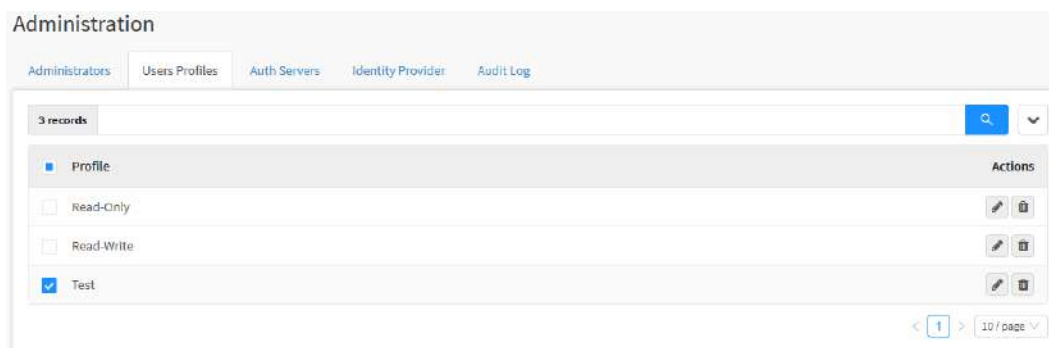
Clique no botão **save** para gravar o perfil, caso contrário, clique em **cancel**, ou no [X] do topo direito da tela, para voltar à aba "Profiles".

Os perfis de administração foram criados com sucesso.

Após criar este perfil, é possível atrelá-lo a um usuário específico para que suas configurações sejam aplicadas, para mais informações, consulte esta [página](#).

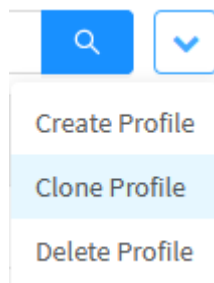
Users Profiles - Menu de Ações - Clone Profile

O botão "Clone Profile" do menu de ações serve para duplicar perfis que foram previamente selecionados ao clicar na caixa de seleção. Como demonstrado abaixo:



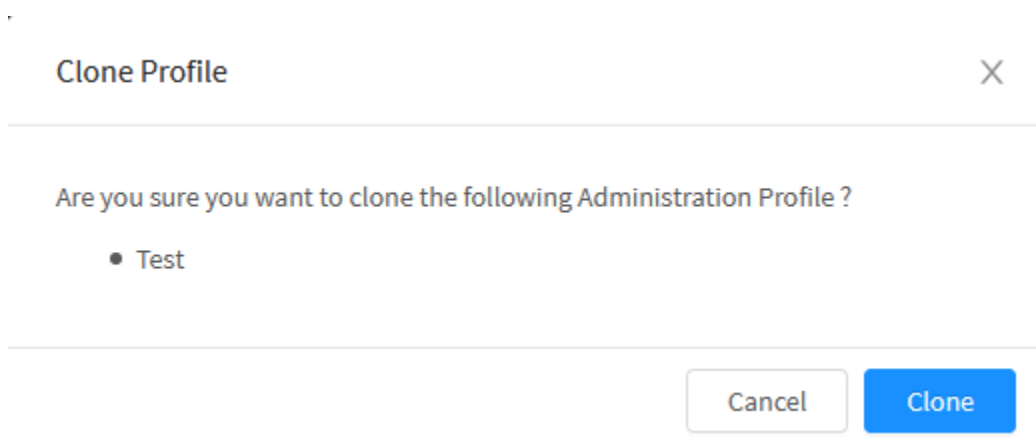
Administration - Users Profiles - Item selecionado

Depois de selecionar os itens que se deseja clonar, selecione a opção no menu de ações []:

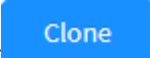
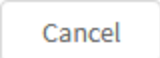


Actions Menu - Clone Profile

Uma mensagem de verificação aparecerá requisitando a confirmação:



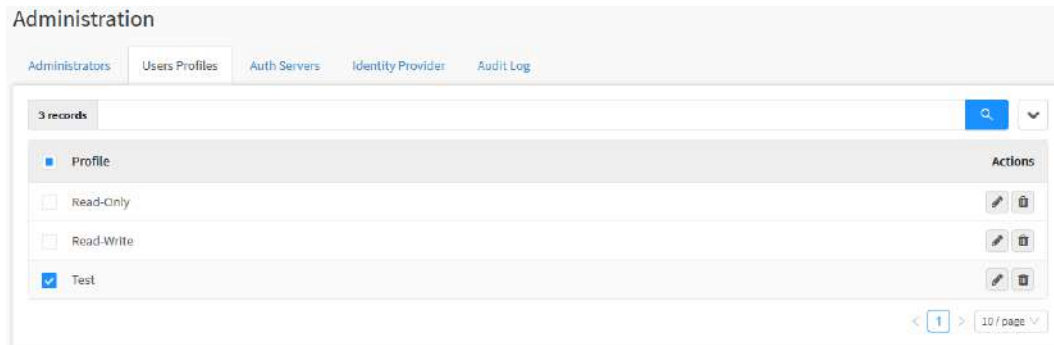
Clone Profile - Mensagem de confirmação

A blue rectangular button with the word "Clone" in white text.A light gray rectangular button with the word "Cancel" in gray text.

Ao clicar em [Clone], os perfis selecionados serão duplicados. Caso clique em [Cancel] essa mensagem de verificação será dispensada sem efetuar nenhuma remoção.

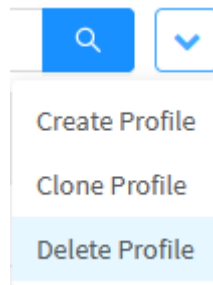
Users Profiles - Menu de Ações - Delete Profile

O botão "Delete Profile" do menu de ações serve para remover perfis que foram previamente selecionados ao clicar na caixa de seleção. Como demonstrado abaixo:



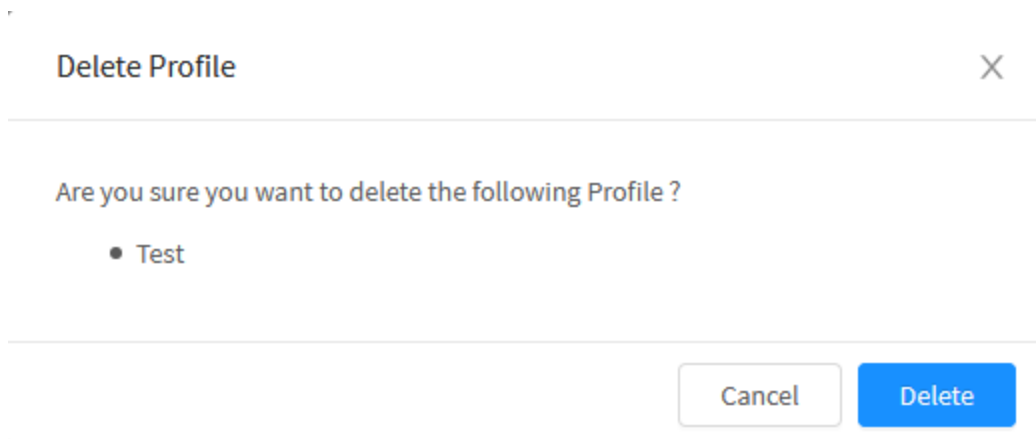
Administration - Users Profiles - Item selecionado

Depois de selecionar os itens que se deseja deletar, selecione a opção no meu de ações []:

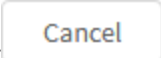


Actions Menu - Delete Profile

Uma mensagem de verificação aparecerá requisitando a confirmação:



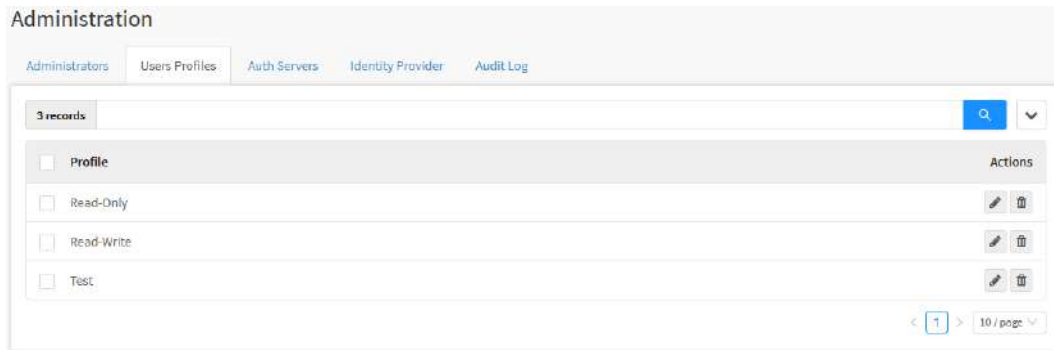
Delete Profile - Mensagem de confirmação

A blue rectangular button with rounded corners and the word "Delete" in white text.A light gray rectangular button with rounded corners and a thin border, containing the word "Cancel" in gray text.

Ao clicar em [Delete], os perfis seleccionados serão duplicados. Caso clique em [Cancel] essa mensagem de verificação será dispensada sem efetuar nenhuma remoção.

Administration - Users Profiles - Colunas

A seguir explicaremos cada coluna da aba Users Profiles:



The screenshot shows the 'Administration' interface with the 'Users Profiles' tab selected. It displays a table with 3 records. The table has two main columns: 'Profile' and 'Actions'. The 'Profile' column lists 'Read-Only', 'Read-Write', and 'Test'. The 'Actions' column contains edit and delete icons for each profile. A search bar and a dropdown menu are at the top right. A pagination bar at the bottom shows page 1 of 10.

Profile	Actions
Read-Only	 
Read-Write	 
Test	 

Profiles

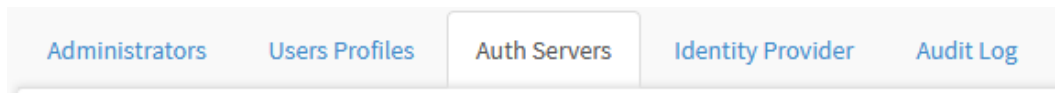
- **Select** : Permite selecionar um ou mais *profiles*;
- **Profile**: Exibe o nome dos *profiles* de administradores criado em [Create Profile](#);
- **Actions**: Disponibiliza as seguintes ações essenciais:
 - **Edit** : Permite editar um dos *profiles* criados na opção [Create Profile](#);
 - **Delete** : Permite deletar um *profile*, é o equivalente à opção [Delete Profile](#).

Administration - Aba "Auth Servers"

Na aba "Auth Servers" é possível efetuar o cadastro de servidores com função de permitir a autenticação de usuários de perfil administrador com *login* remoto.

A aba "Auth Servers" é composta por cinco colunas: "Server Name", "Primary Server", "Secondary Server", "Authentication Type" e "Actions" e além disso, no topo da tela estão localizados a barra de busca e o menu de ações.

Clique na aba "Servers".



Aba Auth Servers

Surgirá a tela demonstrada pela imagem abaixo:

☐	Name	Primary	Secondary	Type	Actions
☐	Radius Linux	172.16.102.200:1812		PAP	   
☐	Radius Windows	172.31.0.180:3268		MSCHAP	   
☐	test	100.100.100.100:1812	100.100.100.100:1812	PAP	   

Administration - Aba Auth Servers

Esta seção irá abordar:

- Cadastro e Edição de servidores Radius e Ldap;
- Remoção dos servidores;
- Como testar se a autenticação de um usuário no servidor está funcionando.

A seguir, analisaremos cada componente deste painel.

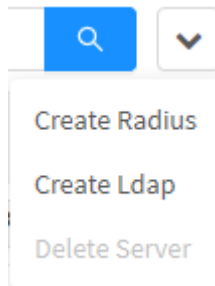
Administration - Auth Servers - Menu de Ações

No topo direito da tela temos o menu de ações:



Users – Botão do menu de ações

Ao clicar neste botão o menu abaixo é exibido:



Administration – Menu de ações.

O menu é composto das seguintes opções:

- [Create Radius](#);
- [Create Ldap](#);
- [Delete Server](#).

A seguir cada opção do menu de ações será detalhada.

Create Radius

Neste formulário é possível criar um novo servidor remoto RADIUS.



Para informações mais aprofundadas a respeito das características de um servidor RADIUS consulte esta [página](#) do manual do UTM.



Ao acessar o **menu de ações** [] e clicar na opção “*Create Radius*”, aparecerá o formulário “*Create Server*”, conforme ilustrado pela imagem abaixo.

Administration – Create Radius

À seguir detalharemos cada campo deste formulário:

- **Server Name:** Define o nome do servidor para identificação, este nome será exibido nas [colunas](#). Ex.: “Radius Server”;
- **Primary Server:** Determina o Endereço IP do servidor de autenticação *Radius* primário;
- **Port:** Define a porta utilizada pelo servidor primário. Ex.: 10;
- **Secret:** Determina a chave pré-compartilhada (*Pre-Shared Key* ou *PSK*). Trata-se do segredo compartilhado entre o servidor de autenticação “*Radius*” e o servidor de contas “*Blockbit UTM*”. Ex.: *blockbit.utm*;
- **Secondary Server:** Define o Endereço IP do servidor de autenticação *Radius* secundário;
- **Port:** Determina a porta utilizada pelo servidor secundário;
- **Secret:** Define a chave pré-compartilhada (*Pre-Shared Key* ou *PSK*). Segredo compartilhado entre o servidor de autenticação “*Radius*” e o servidor de contas “*Blockbit UTM*”. Ex.: *blockbit.utm*;
- **Authentication Type:** Determina qual tipo de protocolo de autenticação será utilizado, as opções disponíveis são:
 - **MSCHAP**;
 - **CHAP**;
 - **PAP**.
- **NAS IP Address:** Trata-se do endereço IP dos dispositivos capazes de receber as solicitações de clientes de autenticação e repassar o pedido ao servidor *Radius* da rede, podendo ser: Roteadores *Wireless*, *Switches* ou seu próprio Dispositivo *UTM*.

Save

Cancel



Clique no botão **save** [] para gravar todas as alterações, caso contrário, clique em **Cancel** [], ou no [X] do topo direito da tela, para fechar a janela.



Server saved successfully

Atente que apesar de ter criado o servidor RADIUS, não há auto-cadastro dos usuários administradores, para tanto é necessário acessar a tela de usuário administradores e criar este usuário, apontando qual é o servidor que ele pertence.

Create LDAP



Ao acessar o **menu de ações** [] e clicar na opção "Create LDAP", aparecerá o formulário "Create Server LDAP", conforme ilustrado pela imagem abaixo.

Administration – Create Server LDAP

Esta janela é composta pelas abas:

- [Settings;](#)
- [User Filter.](#)

À seguir analisaremos todos os componentes de cada uma destas abas laterais.

Settings

A aba settings é composta pelos seguintes campos:

Administration – Create Server LDAP

- **Name:** Define um nome para a conexão de sincronismo, este nome será exibido nas [colunas](#). Ex.: *Primary DC*;
- **SSL** ☒: Caso o serviço esteja rodando em SSL habilite este *checkbox*;
- **Primary Server:** Define o endereço *IP* primário do controlador de domínio. Ex.: 172.16.102.191;
- **Port:** Determina a porta para conexão ao controlador de domínio. Ex.: 389;
- **Login:** Define um usuário do servidor *Windows* com direitos de fazer pesquisa na base *LDAP*, geralmente usuário membro do grupo administradores. Ex.: "administrador@dominioc.com";
- **Password:** Determina a senha do usuário;
- **Secondary Server:** Define o endereço *IP* secundário do controlador de domínio. Ex.: 172.16.102.192;
- **Port:** Determina a porta para conexão ao controlador de domínio. Ex.: 389;
- **Login:** Define um usuário do servidor *Windows* com direitos de fazer pesquisa na base *LDAP*, geralmente usuário membro do grupo administradores. Ex.: "administrador@dominioc.com";
- **Password:** Determina a senha do usuário.

Para continuar configurando, acesse a próxima aba lateral: [User Filter](#).

User Filter

Nesta aba configura-se os campos que se referem à base de pesquisa de usuários e os seus respectivos filtros na base *LDAP* do servidor *Windows AD*.

The screenshot shows a dialog box titled "Create Server Ldap" with a close button (X) in the top right corner. On the left, there are two tabs: "Settings" and "User Filter", with "User Filter" being the active tab. The main area contains three input fields: "Base" with the value "DC=dominiof,DC=com", "Filter" with the value "(&(objectclass=user)(objectclass=person)(!(objectclass=computer)))", and "Login Attribute" with the value "sAMAccountName". At the bottom right, there are two buttons: "Cancel" and "Save".

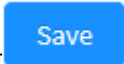
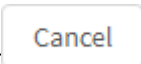
Authentication – Add Windows Server – User filter

Configure os campos "Base", "Filter" e "Login Attribute", de acordo com os dados da base *LDAP* do respectivo servidor *Windows*.



Para a configuração de um servidor *Windows AD* com *LDAP*, é necessário alterar manualmente os campos para possuírem os valores abaixo:

- **Filter:** (&(objectclass=user)(objectclass=person)(!(objectclass=computer)))
- **Attribute login:** userPrincipalName

Clique no botão **save**  para gravar todas as alterações, caso contrário, clique em **Cancel** , ou no  do topo direito da tela, para fechar a janela.

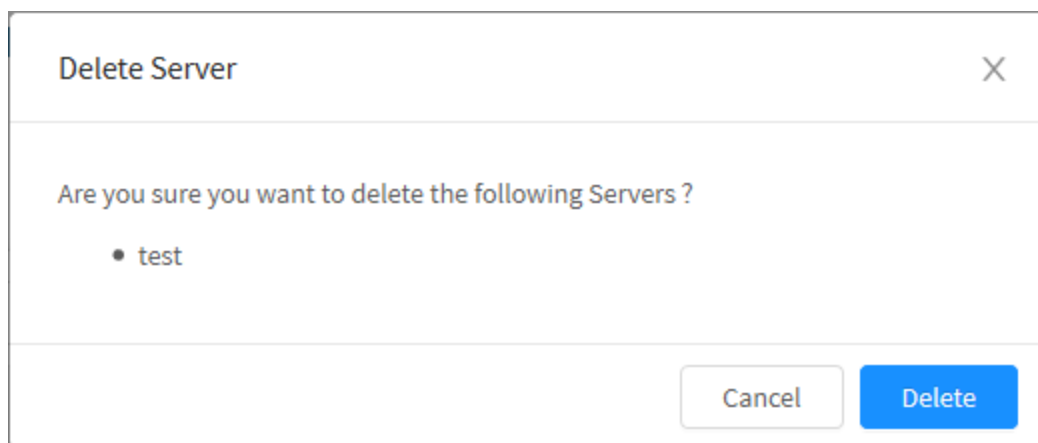


Server saved successfully

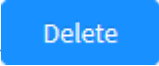
Atente que apesar de ter criado o servidor *LDAP*, não há auto-cadastro dos usuários administradores, para tanto é necessário acessar [Administration - Aba "Users"](#) e criar este usuário, apontando qual é o servidor que ele pertence.

Delete Server

O botão "Delete Server" do menu de ações serve para remover servidores que foram previamente selecionados ao clicar na caixa de seleção. Depois de selecionar essa opção, uma mensagem de verificação aparecerá requisitando a confirmação.



Delete Server

Ao clicar [], os servidores selecionados serão removidos. Caso clique em [] essa mensagem de verificação será dispensada sem efetuar nenhuma remoção.

Administration - Auth Server - Colunas

A seguir detalharemos cada coluna da aba *Servers*:

Administrators

Users Profiles

Auth Servers

Identity Provider

Audit Log

1 records

☐	Name	Primary	Secondary	Type	Actions
☐	Server LDAP	172.31.0.180:3268		LDAP	
☐	Radius Linux	172.16.102.200:1812		RADIUS	
☐	Radius Windows	172.31.0.180:3268		RADIUS	
☐	test	100.100.100.100:1812	100.100.100.100:1812	LDAP	

<

1

>

10 / page

Administration - Aba Auth Servers

- **Select** : Permite selecionar um ou mais *servidores*;
- **Primary**: Define o endereço *IP* do servidor primário;
- **Secondary**: Define o endereço *IP* do servidor secundário;
- **Type**: Exibe o tipo escolhido ao criar o servidor, podendo ser LDAP ou RADIUS;
- **Actions**: Disponibiliza as seguintes funções essenciais:
 - **Edit** : Permite editar um dos servidores criados na opção [Create Radius](#) ou [Create LDAP](#) no menu de ações;
 - **Test Connection** : Permite testar a conectividade de um servidor;
 - **Test Authentication** : Permite testar caso a autenticação de um usuário no servidor está ocorrendo corretamente, cheque esta [página](#) para mais informações;
 - **Delete** : Permite [deletar](#) um *servidor*.

Server - Test Authentication

Esta tela serve para testar se a autenticação está funcionando corretamente.

Ao clicar no botão **Test Authentication** [] a tela abaixo será exibida:

Test Authentication

* User

* Password

Cancel

Confirm

Test Authentication

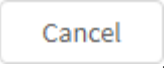
- **User:** Digite o usuário desejado;
- **Password:** Digite a senha do usuário.



O usuário que pode ser utilizado neste painel precisa ter sido adicionado na aba *User* com o tipo "Remoto", para mais informações cheque esta [página](#).

Confirm

Cancel

Para testar a autenticação, clique em [] para testar a autenticação ou clique em [] para fechar a janela.

Administration - Aba "Identity Provider"

Esta aba contém os recursos necessários para configurar a integração com o provedor de identidade *SAML* (*Security Assertion Markup Language*), trata-se de um protocolo de autenticação *opensource* baseado em *XML* para autenticação entre um *identity provider* (provedor de identidade) e um *service provider* (provedor de serviços). Este recurso é um padrão *single sign on* usado para integrar múltiplas aplicações de autenticação *web* (*http*) com o *GSM*. Ele atua permitindo que o usuário informe seu *login* e senha para um *identity provider* externo ao invés de efetuar o login padrão através do *GSM*.

Quando um usuário acessa uma aplicação do provedor de serviços (no caso, o *GSM*), o *identity provider* requisita o *login* e senha do usuário para confirmar sua identidade, caso as credenciais estejam corretas, ele envia uma asserção de autenticação (sendo esta predeterminada pelo *SAML*) para o *service provider* de forma que ele possa definir o controle de acesso do usuário que efetuou a requisição.

O *identity provider* é uma aplicação terceirizada confiável que gera, armazena e administra dados de identificação dos usuários, ele transmite uma asserção de autenticidade baseada no *SAML* quando a credencial deste usuário é validada, além disso, ele é capaz de fornecer serviços de autenticação a múltiplos *service provider*, permitindo que seus usuários efetuem *login* em qualquer aplicação que seja compatível com essa tecnologia.

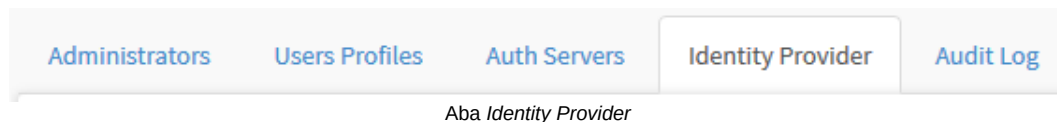
Ao habilitar essa opção, o *GSM* passará a atuar como *service provider*, permitindo que o usuário utilize o *identity provider* para efetuar login e também oferecendo os mecanismos necessários para a integração com o *identity provider* selecionado.

O *SAML* não especifica qual método de autenticação será utilizado no *identity provider* sendo possível utilizar autenticação de multifator, *RADIUS*, *LDAP*, *Active Directory* e etc, de acordo com o provedor selecionado.

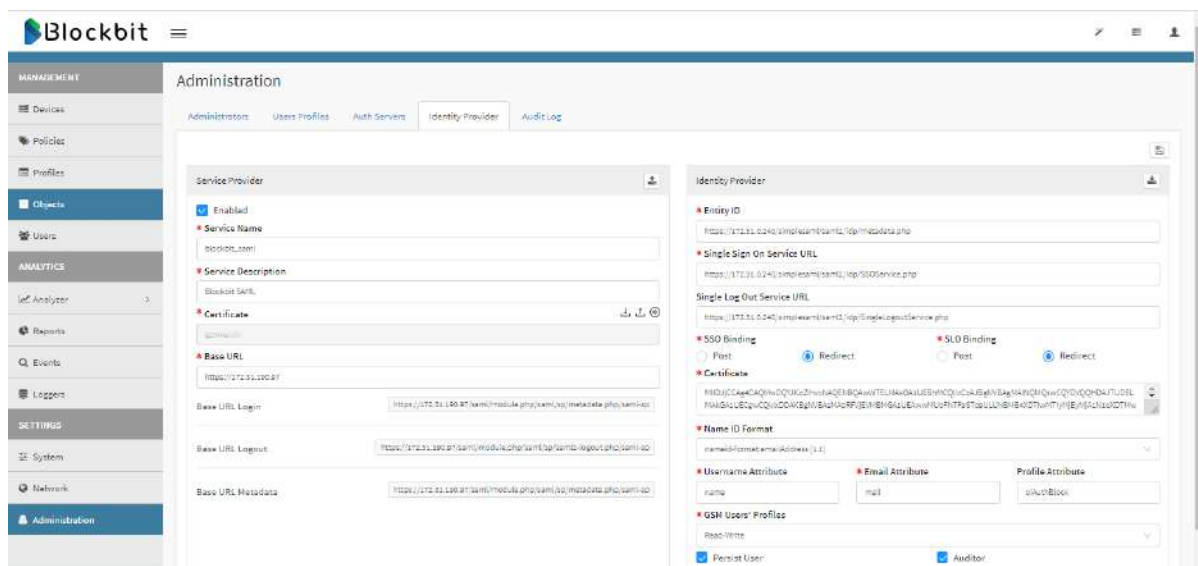
As vantagens deste recurso são:

- Evita que o usuário tenha que se lembrar de múltiplas senhas para acessar diversas aplicações;
- Graças ao sistema ser terceirizado e baseado em um servidor de confiança, a segurança no processo de *login* é aprimorada;
- Por depender de menos acessos reduz os vetores de ataque por onde um *exploit* possa ser aplicado.

Para acessar essas funcionalidades, clique na aba "Identity Provider":



A seguinte tela será exibida:



Administration - Identity Provider

Essa tela é composta pelos painéis:

- *Service Provider*;
- *Identity Provider*.

À seguir iremos analisar os componentes de cada um destes painéis.

Identity Provider - Service Provider

Neste painel estão os recursos necessários para configurar o GSM como *Service Provider*. À seguir iremos detalhar como configurar este formulário:

Service Provider

☒ SAML SSO Enabled

* Service Name

gsm23

* Service Description

Service Provider GSM23

* Certificate

gsm23.blockbit.com

* Base URL

https://172.31.240.23

Base URL Login

https://172.31.240.23/saml/module.php/saml/sp/metadata.php/saml-sp

Base URL Logout

https://172.31.240.23/saml/module.php/saml/sp/saml2-logout.php/saml-sp

Base URL Metadata

https://172.31.240.23/saml/module.php/saml/sp/metadata.php/saml-sp

Identity Provider - Service Provider

- **SAML SSO Enabled** ☒: Ao marcar esta caixa de seleção o sistema habilita o *Single Sign On* baseado em SAML;
- **Service Name**: Define o nome do Serviço que será passado para o *Identity Provider*;



O *service name* será utilizado nas requisições do *identity provider* e será enviado pela *URL*, e portanto será necessário seguir a sintaxe, segue os caracteres aceitos:

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-._~!/?#[]@!\$&'()*+,:=

Para mais informações, consulte o [RFC 3986](#).

- **Service Description**: Determina uma descrição para facilitar a identificação do serviço;

- **Certificate:** Esta opção permite que o usuário gere um certificado auto-assinado ou importe um certificado externo do *Identity Provider*, podendo ser público ou privado. Este campo contém as seguintes opções:
 - **Add Certificate** : Este botão permite adicionar um novo certificado automaticamente, para mais informações sobre a janela de certificados, consulte esta [página](#);
 - **Import Certificate** : O botão possibilita que certificados gerados pelo *Identity Provider* sejam importados, para mais informações sobre a janela de importação, consulte esta [página](#);
 - **Export Certificate** : Este botão permite fazer download do certificado.
- **Base URL:** Determina o URL base do serviço que será redirecionado pelo *Identity Provider*, este campo aceita IP ou FQDN. Ao alterar as informações de URL base, todos os campos abaixo receberão as informações referentes ao provedor de serviço;
- **Base URL Login:** Neste campo, é adicionado o URL do serviço de *Login* do *Identity Provider*, ele é utilizado para retornar as mensagens, esse URL é gerado automaticamente usando como referência as informações em Base URL;
- **Base URL Logout:** Neste campo, é determinado o URL do serviço de *Logout* que o *Identity Provider* utilizará para retornar as mensagens, esse URL é gerado automaticamente usando como referência as informações em Base URL;
- **Base URL Metadata:** Este campo define o URL do serviço de *Metadata* que o *Identity Provider* usará caso seja necessário importar as informações acima sobre o *Service Provider*, esse URL é gerado automaticamente usando como referência as informações em Base URL.



Clique no botão  para exportar todos os metadados em formato XML, possibilitando e importar este arquivo na interface do *Identity Provider*, essas informações são necessárias para federar o servidor de serviços (GSM) e fechar a comunicação com o *Identity Provider*.

Para mais informações sobre a janela de importação de certificados, consulte esta [página](#).

Para detalhes a respeito da configuração do painel *Identity Provider*, consulte esta [página](#).

Identity Provider - Service Provider - Add Certificate

Os recursos desta janela, permitem que o administrador configure sua própria autoridade certificadora, sendo esta uma maneira simples e prática de se obter o certificado que será utilizado para garantir confiabilidade no acesso aos recursos da solução.

O propósito de uma autoridade certificadora é confirmar a titularidade dos certificados, confirmando que o certificado recebido ao acessar determinado *site* ou endereço pertence realmente à entidade que o está fornecendo. É isso que garante que você está mesmo acessando os sites e endereços *SSL/HTTPS* de forma segura.



É necessário configurar uma CA nesta aba poder criar um provedor de identidade SAML, para mais informações consulte esta [página](#).

Add Certificate

X

* Country

BR

* State

SP

* City

Sao Paulo

* Organization

gsm24 Blockbit

* E-mail

admin@blockbit.com

* Organizational Unit

QA Blockbit

* Expires in (years)

10

* Hostname

gsm24.blockbit.com

* Key Size

2048

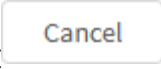
Cancel

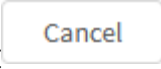
Save

System - Backups

A seguir iremos detalhar os campos deste formulário.

- **Country:** Determina o país. Ex.: *US*;
- **State:** Define o estado. Ex.: *New York*;
- **City:** Determina a cidade. Ex.: *New York*;
- **Organization:** Define o nome da empresa. Ex.: *Blockbit*;
- **E-mail:** Determina o *e-mail* do administrador. Ex.: *admin@blockbit.com*;
- **Organizational Unit:** Define o departamento. Ex.: *QA*;
- **Expires (years):** Determina o tempo de validade do certificado. Ex.: *10 anos*;
- **Hostname:** Define o Hostname da CA. Ex.: *admin@blockbit.com*;
- **Keysize:** Define o tamanho que a chave da CA possuirá. Ex.: *2048*.

SaveCancel

Ao finalizar a configuração, clique em [] para salvar ou em [] para fechar esta janela.



Salvar uma CA requer que o servidor gere uma nova entidade certificadora. Esta ação exige a reinstalação da nova CA em todos os dispositivos da rede.



Caso deseje recriar a CA, você também deve refazer o Certificado do Servidor, este procedimento requer a instalação da nova CA em todos os dispositivos da rede. Faça o download da CA e reinstale em todas as estações de trabalho. Lembrando que para validação da nova CA você deve REINICIAR o servidor.

A seguir vamos analisar o botão [Import Certificate](#).

Identity Provider - Service Provider - Import Certificate

Esta janela permite a adição de um certificado auto-assinado, podendo ser chave pública ou privada, à seguir analisaremos os componentes do formulário:

Add Certificate

* Certificate Type

☒ (.crt/key) ☐ (.pem)

* Certificate - Public Key (.crt)

Paste Here

* Certificate - Private Key (.key)

Paste Here

Cancel

OK

Identity Provider - Add Certificate

- **Certificate Type:** Esta opção determina o tipo de certificado que será utilizado. A seleção determina quais campos serão exibidos no formulário, as opções são:
 - **(.crt/key)**☒: Caso a opção (.crt/key) esteja habilitada os campos Certificate - Public Key (.crt) e Certificate - Private Key (.key) serão exibidos;
 - **(.pem)**☐: Caso a opção (.pem) esteja habilitada o campo Certificate (.pem) será exibido.
- **Certificate - Public Key (.crt):** Este campo permite a adição da chave pública do certificado (.crt);
- **Certificate - Private Key (.key):** Este campo permite a adição da chave privada do certificado (.key);
- **Certificate (.pem):** Caso tenha selecionado a opção (.pem), basta adicionar o certificado neste campo.

Para mais informações a respeito do formulário do painel Service Provider, consulte esta [página](#);

Para ter acesso a informações a respeito do painel Identity Provider, consulte esta [página](#).

Identity Provider - Identity Provider

Neste painel estão os recursos necessários para configurar o sincronismo do GSM com o *Identity Provider*. À seguir iremos detalhar como configurar este formulário:

Identity Provider

* Entity ID

* Single Sign On Service URL

Single Log Out Service URL

* SSO Binding
☐ Post ☒ Redirect

* SLO Binding
☐ Post ☒ Redirect

* Certificate

* Name ID Format

* Username Attribute

* Email Attribute

Profile Attribute

* GSM Users' Profiles

☒ Persist User ☒ Auditor

Identity Provider

- **Entity ID:** Define a *URL* que será utilizado para fazer a comunicação e configurar o *Identity Provider*. Este campo é obrigatório;
- **Single Sign On Service URL:** Determina o *URL* de Single Sign On que será utilizado no *login* do GSM pelo *Identity Provider*. Este campo é obrigatório;
- **Single Log Out Service URL:** Define o *URL* de Single Log Out do GSM pelo *Identity Provider*. Este campo não é obrigatório. Ao adicionar alguma informação neste campo, a opção *SLO Binding* é habilitada;



Atente que alguns provedores de identidade não obrigam a configuração do serviço de *Logout*.

- **SSO Binding:** Define qual método de *bind* será utilizado pelas requisições *HTTP* do serviço de *Login*, podendo ser:
 - **Post** : Ao selecionar esta opção, será utilizado o método *POST*, transferindo a requisição de *Login* através do corpo do *HTTP*;

- **Redirect** ☐: Ao selecionar esta opção, será utilizado o método *GET*, transferindo a requisição de *Login* por URL.
- **SLO Binding**: Para que esta opção seja habilitada, é necessário completar o campo *Single Log Out Service URL*. Esta opção define qual método de *bind* será utilizado pelas requisições *HTTP* do serviço de *Logout*, podendo ser:
 - **Post** ☐: Ao selecionar esta opção, será utilizado o método *POST*, transferindo a requisição de *Login* através do corpo do *HTTP*;
 - **Redirect** ☒: Ao selecionar esta opção, será utilizado o método *GET*, transferindo a requisição de *Login* por URL.



ATENÇÃO: Os campos a respeito de *Binding* precisam estar condizentes com os requerimentos do *Identity Provider*, caso contrário, o serviço não funcionará. Para tanto, analise o XML que está sendo importado, para verificar qual o método de *Binding* é necessário, caso não esteja sendo possível acessar o *Identity Provider*, é aconselhável reavaliar se a seleção na configuração de *SSO Binding* está correta.

- **Certificate**: Neste campo, deve-se colar o certificado gerado pelo *Identity Provider*. A sua função é efetuar a validação das asserções do *Identity Provider*;
- **Named ID Format**: Esta caixa de seleção define qual será a formatação de Name ID que será usada pelo SAML. O Name ID determina qual informação é prioritária no processo de login, isso é alterado de acordo com a importação do XML, cada *Identity Provider* possui suporte a uma versão de Name ID Format, portanto, selecione a versão indicada para o seu provedor;



ATENÇÃO: O *Name ID Format* precisa estar condizentes com os requerimentos do *Identity Provider*, caso contrário, o serviço não funcionará. Para tanto, selecione a opção requerida pelo seu provedor.

- **Username Attribute**: Define o Atributo do documento XML que representará o Nome do usuário, este dado é utilizado para criar a sessão do usuário no GSM quando for efetuado o *login* via SAML. Este atributo deve ser copiado do *Identity Provider*;
- **Email Attribute**: Determina o Atributo do documento XML que representará o Email do usuário, este dado é utilizado para criar a sessão do usuário no GSM quando for efetuado o *login* via SAML. Este atributo deve ser copiado do *Identity Provider*;
- **Profile Attribute**: Determina o Atributo do documento XML que representará o Perfil do usuário, este dado é utilizado para criar a sessão do usuário no GSM quando for efetuado o *login* via SAML. Este atributo deve ser copiado do *Identity Provider*;
- **GSM Users' Profiles**: Este campo define qual perfil de permissões padrão será utilizado quando o usuário autenticado acessar o GSM, os itens desta caixa de seleção são criados na aba User Profiles, para mais informações, consulte esta [página](#);
- **Persist User** ☐: Ao habilitar esta opção, a persistência da sessão do usuário no sistema será ativada, esta opção define se quando o usuário faz o *logout* ele será removido da aba [Administrators](#), se estiver desabilitada, ao fazer o *logout* o usuário também é removido do GSM, caso esteja habilitada o usuário continuará gravado no GSM mesmo após o *Logout*. Por padrão, esta opção é desabilitada;
- **Audit User** ☐: Caso esta opção seja habilitada, ao se autenticar o usuário possuirá permissão de auditor, um usuário com essa permissão poderá fazer *deploys*, caso contrário, só poderá visualizá-los. Por padrão, esta opção é desabilitada.



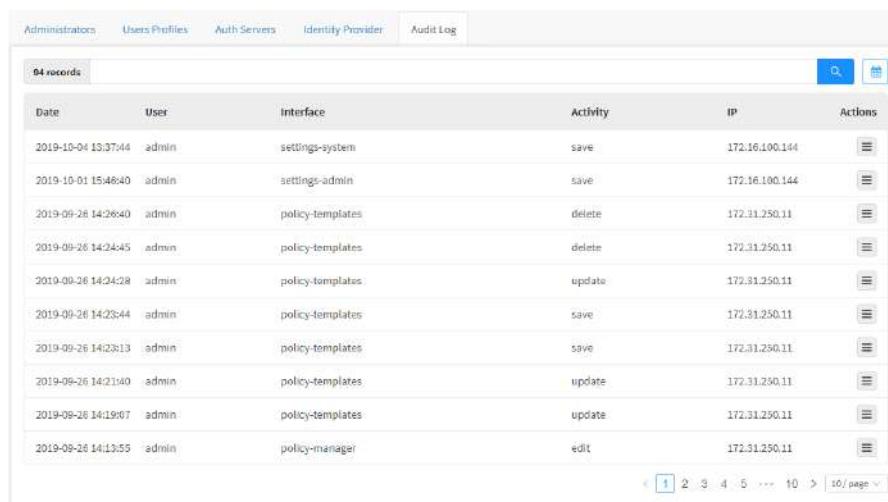
Clique no botão para importar os metadados em formato XML, possibilitando utilizar as configurações fornecidas na interface do *Identity Provider*. Ao importar o XML através deste botão, por padrão são auto-completadas as informações dos campos *Entity ID*, o *Single Sign On Service URL*, *Single Log Out Service URL* (quando suportado pelo *Identity Provider*), *SSO* e *SLO Binding*, *Certificate* e *Name ID Format*.

Para mais informações a respeito do formulário do painel Service Provider, consulte esta [página](#);

Para outras informações a respeito de SAML, consulte esta [página](#).

Administration - Aba "Audit Log"

Na aba "Audit Log" visualizamos a tela de Auditoria de Atividades:



The screenshot shows the 'Audit Log' tab in a web application. At the top, there are navigation tabs: Administrators, Users Profiles, Auth Servers, Identity Provider, and Audit Log. Below the tabs, there is a search bar and a calendar icon. The main content is a table with the following columns: Date, User, Interface, Activity, IP, and Actions. The table contains 10 records. At the bottom right of the table, there is a pagination control showing '10 / page'.

Date	User	Interface	Activity	IP	Actions
2019-10-04 13:37:44	admin	settings-system	save	172.16.100.144	[icon]
2019-10-01 15:46:40	admin	settings-admin	save	172.16.100.144	[icon]
2019-09-26 14:26:40	admin	policy-templates	delete	172.31.250.11	[icon]
2019-09-26 14:24:45	admin	policy-templates	delete	172.31.250.11	[icon]
2019-09-26 14:24:28	admin	policy-templates	update	172.31.250.11	[icon]
2019-09-26 14:23:44	admin	policy-templates	save	172.31.250.11	[icon]
2019-09-26 14:23:13	admin	policy-templates	save	172.31.250.11	[icon]
2019-09-26 14:21:40	admin	policy-templates	update	172.31.250.11	[icon]
2019-09-26 14:19:07	admin	policy-templates	update	172.31.250.11	[icon]
2019-09-26 14:13:55	admin	policy-manager	edit	172.31.250.11	[icon]

Audit Log

No topo da tela temos os campos a seguir:

- **Barra de busca:** Nesta barra é possível digitar *palavras chaves* e executar uma busca. Para executar uma busca clique no botão **buscar** ;
- **Calendário** : O calendário permite fazer buscas mais precisas levando em consideração requisitos temporais, as opções permitidas são: *All* (Considera todas as opções), *By Date* (Faz a busca especificamente em uma data), *By Period* (Faz a busca especificamente entre um período), *Today* (Hoje), *Yesterday* (Ontem), *Last 7 Days* (Últimos 7 dias), *Last 30 Days* (Últimos 30 dias), *This Month* (Esse mês) e *Last Month* (Último mês). Em algumas opções, um calendário surgirá permitindo a seleção das datas desejadas;

Abaixo dos campos de busca, as seguintes informações são exibidas:

- **Date:** Demonstra a data e o horário em que as atividades foram realizadas. Ex.: "08/10/2018 18:22:26";
- **User:** Determina qual usuário foi responsável por executar a ação que será listada posteriormente. Ex.: "admin";
- **Interface:** Exibe qual interface foi acessada pelo usuário previamente mencionado. Ex.: "Settings-System";
- **Activity:** Determina qual foi a atividade que o usuário executou no sistema. Ex.: "update";
- **IP:** Trata-se do endereço IP do usuário que executou a ação registrada; Ex.: "172.16.100.144";
- **Actions:** É o registro de qual atividade foi executada na interface previamente mencionada. Ao clicar no botão **Audit View** , são exibidas mais informações a respeito das ações tomadas pelo usuário, consulte esta [página](#) para mais informações.

No canto inferior da tela o botão **Exibição de resultados** : Permite determinar quantos resultados serão exibidos por página, as possibilidades são: 10, 20, 30, 40, 50, 100, 500;



É importante ressaltar que com a opção de Domínios Virtuais ligada, as informações exibidas serão referentes somente ao próprio domínio, sem acesso a informações de outros Domínios Virtuais.

Para mais informações sobre Domínios Virtuais (VDOMs) acesse esta [página](#).

A seguir analisaremos o botão **Audit View** .

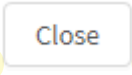
Audit View

Esta tela tem como função exibir todas as ações tomadas pelo usuário.

Ao clicar no botão **Audit View**  a tela abaixo será exibida:

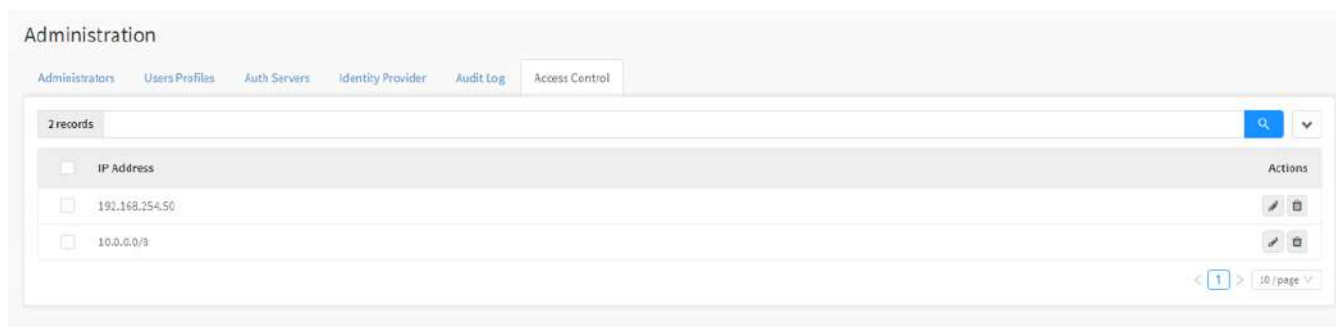


Audit View

Para sair desta janela, basta clicar em **Close** , ou no  do topo direito da tela para voltar à janela anterior.

Administration - Aba "Access Control"

Em Access Control é possível criar políticas que restringem o acesso a interface gerencial do GSM, de modo a garantir apenas que IPs específicos possam ter acesso a tal interface



Access Control

Nesta seção é possível controlar por meio de atribuição de IP ou whitelist os usuários que terão acesso ao controle do GSM.

GSM - CLI - LINHA DE COMANDOS

O Blockbit GSM disponibiliza um recurso de console *Command Line Interface - CLI*, que possibilita ao administrador executar comandos de administração e *troubleshooting* dos principais serviços do sistema.

Para executar a configuração é necessário um cliente *SSH* e *Console*. As aplicações mínimas recomendadas são:

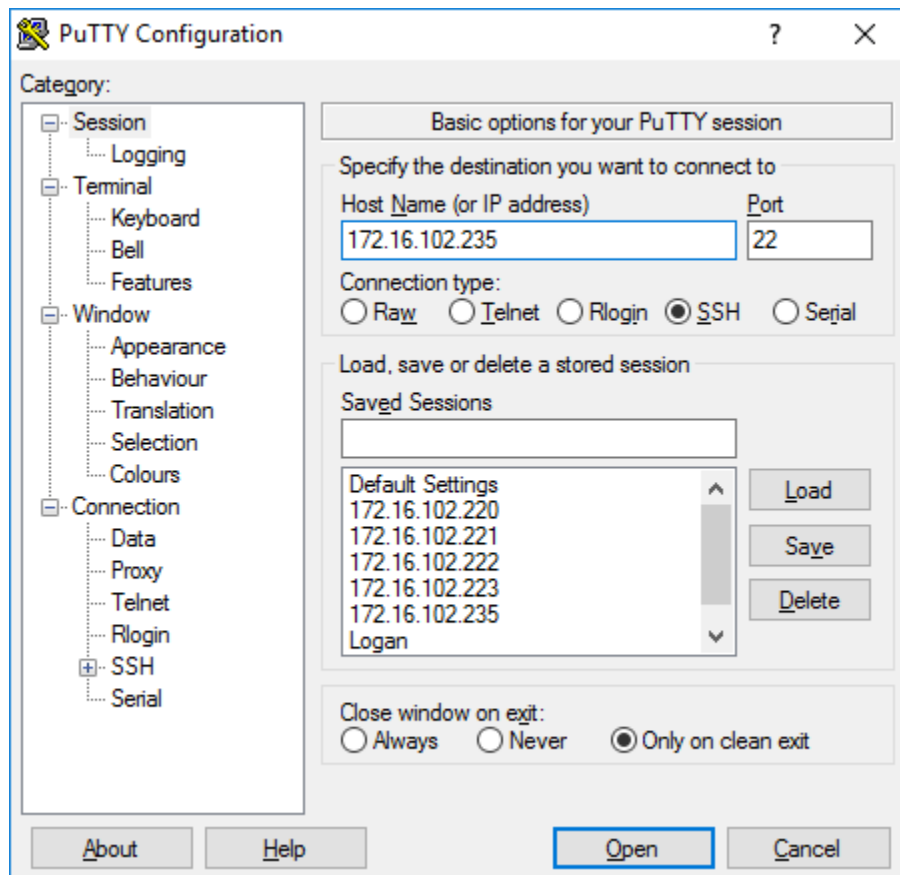
- *PUTTY*; ou
- *CygWin*; ou
- *Mobaxterm*.

A seguir apresentaremos passo a passo como acessar o console *CLI* do Blockbit GSM:

1. Verifique se o dispositivo de acesso possui um cliente *SSH* recomendado já instalado. Vamos exemplificar o processo utilizando o aplicativo "*PUTTY*";

2. Acesse o console *SSH*. Preencha os campos:

- **Host Name (or IP Address):** Inserir o endereço *IP* do Blockbit GSM. Ex.: 172.16.102.235;
- Clique no botão "*Open*".



PuTTY Configuration

3. O console será exibido solicitando usuário e senha;

Em "login as:" Digite o usuário admin e pressione "Enter".
Após "password:" Entre com a senha admin e pressione "Enter".

A imagem abaixo apresenta os comandos dos principais serviços do sistema.

```
admin >help
arp
arping
date
debug-backup
debug-deployer
debug-ha
debug-rotation
debug-sync
delete-logger-backup
disable-snmp
enable-root
enable-snmp
ethtool
exit
fdisk
free
fsck
grep
ha-failover
ha-up
help
history
hostname
ifconfig
ifstat
iotest
admin >

ip
ipcalc
less
logger-backup
logger-certificate-sync
logger-config
logger-config-sync
logger-connect
logger-devices-add
logger-devices-list
logger-disable
logger-enable
logger-key
logger-storage
logger-update-schedule
lscpu
mkfs
more
netstat
ntpdate
passwd
ping
reboot
reset
reset-admin-block
reset-admin-password

reset-admin-sessions
reset-logs
restore-logger-backup
rewizard
route
sar
set-network-dns
set-network-gateway
set-network-hostname
set-network-interface
set-network-timezone
show-devices
show-license
show-logger-backups
show-uuid
show-version
shutdown
snapshot
tcpdump
tcptop
telnet
tracepath
tracert
update-gsm
update-license
upgrade-kernel
uptime
vmstat
whois
```

Blockbit GSM – Command Line Interface.

A seguir, apresentaremos cada comando.

- [arp];
- [arping];
- [date];
- [debug-backup];
- [debug-deployer];
- [debug-ha];
- [debug-rotation];
- [debug-sync];
- [delete-logger-backup];
- [disable-snmp];
- [enable-root];
- [enable-snmp];
- [ethtool];
- [exit];
- [fdisk];
- [free];
- [fsck];
- [grep];
- [help];
- [history];
- [hostname];
- [ifconfig];
- [ifstat];
- [iotest];
- [ip];
- [ipcalc];
- [less];
- [logger-config];
- [logger-devices-add];
- [logger-devices-list];
- [logger-disable];
- [logger-enable];
- [logger-key];
- [lscpu];
- [mkfs];

- [more];
- [netstat];
- [ntpddate];
- [passwd];
- [ping];
- [reboot];
- [reset];
- [reset-admin-blocks];
- [reset-admin-password];
- [reset-admin-sessions];
- [reset-logs];
- [rewizard];
- [route];
- [sar];
- [set-network-dns];
- [set-network-gateway];
- [set-network-interface];
- [set-network-timezone];
- [show-devices];
- [show-license];
- [show-uuid];
- [shutdown];
- [tcpdump];
- [tcpdump];
- [telnet];
- [tracepath];
- [traceroute];
- [update-gsm];
- [update-license];
- [uptime];
- [vmstat];
- [whois].

[arp]

Utilizado para mapear o endereço de rede (por exemplo, um endereço *IPv4*) para um endereço físico (também chamado endereço *MAC*), como um endereço *Ethernet*. Exibe e modifica esta tabela de relação de endereços da *Internet* para endereços *Ethernet*. O *ARP* foi implementado com muitas combinações de tecnologias de rede e camada de enlace de dados. O *IPv4* é o caso mais comum.

Utilize este comando para identificar um problema de comunicação de rede ou identificar eventos e status de *IP* conectados.

Modo de uso:

```
Modo de uso
admin >arp -h
Usage:
  arp [-vn]  [<HW>] [-i <if>] [-a] [<hostname>] <-Display ARP cache
  arp [-v]   [-i <if>] -d <host> [pub] <-Delete ARP entry
  arp [-vnD] [<HW>] [-i <if>] -f [<filename>] <-Add entry from file
  arp [-v]   [<HW>] [-i <if>] -s <host> <hwaddr> [temp] <-Add entry
  arp [-v]   [<HW>] [-i <if>] -Ds <host> <if> [netmask <nm>] pub <-'''-

      -a display (all) hosts in alternative (BSD) style
      -e display (all) hosts in default (Linux) style
      -s, --set          set a new ARP entry
      -d, --delete      delete a specified entry
      -v, --verbose      be verbose
      -n, --numeric      don't resolve names
      -i, --device       specify network interface (e.g. eth0)
      -D, --use-device   read <hwaddr> from given device
      -A, -p, --protocol specify protocol family
      -f, --file         read new entries from file or from /etc/ethers

<HW>=Use '-H <hw>' to specify hardware address type. Default: ether
List of possible hardware types (which support ARP):
  ash (Ash) ether (Ethernet) ax25 (AMPR AX.25)
  netrom (AMPR NET/ROM) rose (AMPR ROSE) arcnet (ARCnet)
  dlci (Frame Relay DLCI) fddi (Fiber Distributed Data Interface) hippi (HIPPI)
  irda (IrLAP) x25 (generic X.25) infiniband (InfiniBand)
  eui64 (Generic EUI-64)
admin >
```

Figura 511 – Command Line Interface – arp.

Exemplo: Apresentar a tabela de endereços *IP* e endereços de *hosts* físicos (dispositivos) na rede:

```
admin >arp -a
? (172.16.12.85) at 00:26:8b:04:eb:bd [ether] on eth0
? (192.168.254.15) at 00:30:48:c2:02:a4 [ether] on eth2.254
? (172.16.13.248) at 0c:c4:7a:11:0f:96 [ether] on eth0
? (172.16.12.81) at 00:30:48:de:78:ae [ether] on eth0
? (192.168.254.4) at e6:9c:1f:89:11:32 [ether] on eth2.254
? (192.168.253.34) at 7e:49:6f:55:42:00 [ether] on eth2.253
? (172.16.12.92) at <incomplete> on eth0
? (172.16.12.90) at 10:98:36:fb:c9:1b [ether] on eth0
? (172.16.20.22) at 00:0b:ab:f1:9b:bc [ether] on eth3
? (172.16.12.71) at <incomplete> on eth0
? (172.16.20.20) at 00:0c:29:b7:34:cf [ether] on eth3
? (172.16.20.19) at 04:7d:7b:fd:53:d7 [ether] on eth3
? (172.16.12.65) at 78:2b:cb:c4:e7:12 [ether] on eth0
? (172.16.12.64) at <incomplete> on eth0
? (172.16.12.77) at 90:b1:1c:f6:2f:e2 [ether] on eth0
? (192.168.254.22) at 00:e0:4c:68:19:bf [ether] on eth2.254
admin >
```

Figura 512 – Command Line Interface – arp – Exemplo.

[arping]

Utilizado para descobrir e identificar os *hosts* conectados utilizando a associação da tabela *ARP* com a resposta análoga ao *ping* que utiliza o protocolo *ICMP*.

Modo de uso:

```
admin >arping -h
Usage: arping [-fqbdUAV] [-c count] [-w timeout] [-I device] [-s source] destination
  -f : quit on first reply
  -q : be quiet
  -b : keep broadcasting, don't go unicast
  -D : duplicate address detection mode
  -U : Unsolicited ARP mode, update your neighbours
  -A : ARP answer mode, update your neighbours
  -V : print version and exit
  -c count : how many packets to send
  -w timeout : how long to wait for a reply
  -I device : which ethernet device to use
  -s source : source ip address
  destination : ask for what ip address
admin >
```

Figura 513 – Command Line Interface – arping.

Exemplo: Descobrir o endereço *MAC* de um determinado *IP*:

```
admin >arping -c 5 -I eth0 172.16.12.85
ARPING 172.16.12.85 from 172.16.12.1 eth0
Unicast reply from 172.16.12.85 [00:26:8B:04:EB:BD] 6.465ms
Unicast reply from 172.16.12.85 [00:26:8B:04:EB:BD] 2.099ms
Unicast reply from 172.16.12.85 [00:26:8B:04:EB:BD] 0.773ms
Unicast reply from 172.16.12.85 [00:26:8B:04:EB:BD] 0.761ms
^CSent 4 probes (1 broadcast(s))
Received 4 response(s)
admin >
```

Figura 514 – Command Line Interface – arping - Exemplo.

[date]

Utilizado para listar e permitir alterar a data e hora atual.

Modo de uso:

```
admin >date --help
Usage: date [OPTION]... [+FORMAT]
or: date [-u|--utc|--universal] [MMDDhhmm[[CC]YY][.ss]]
Display the current time in the given FORMAT, or set the system date.
...
Mandatory arguments to long options are mandatory for short options too.
-d, --date=STRING      display time described by STRING, not 'now'
-f, --file=DATEFILE    like --date once for each line of DATEFILE
-I[TIMESPEC], --iso-8601[=TIMESPEC] output date/time in ISO 8601 format.
                        TIMESPEC='date' for date only (the default),
                        'hours', 'minutes', 'seconds', or 'ns' for date
                        and time to the indicated precision.
-r, --reference=FILE    display the last modification time of FILE
-R, --rfc-2822          output date and time in RFC 2822 format.
                        Example: Mon, 07 Aug 2006 12:34:56 -0600
```

Figura 515 – Command Line Interface – date.

```
--rfc-3339=TIMESPEC    output date and time in RFC 3339 format.
                        TIMESPEC='date', 'seconds', or 'ns' for
                        date and time to the indicated precision.
                        Date and time components are separated by
                        a single space: 2006-08-07 12:34:56-06:00
-s, --set=STRING        set time described by STRING
-u, --utc, --universal  print or set Coordinated Universal Time (UTC)
--help                  display this help and exit
--version               output version information and exit

admin >
```

Figura 515 – Command Line Interface – date 2.

Exemplo 1: Listar a data e hora atual:

```
admin >date
Thu Sep  1 09:59:08 BRT 2016
admin >
```

Figura 516 – Command Line Interface – date – Exemplo 1.

Exemplo 2: Atualizar data e hora baseado no fuso horário América/São Paulo:

```
admin > date --date='TZ="America/Sao_Paulo" 11:00'  
Thu Sep 1 11:00:00 BRT 2016  
admin >  
_OK ticket:57ddcb336098c149eebca22604e3a01a
```

Figura 517 – *Command Line Interface* – *date* – Exemplo 2.

[debug-backup]

Este comando exibe os logs das rotinas de *backups* e *restore* da Manager, Loggers e Firewalls (Snapshots e Imagens)

```
admin >debug-backup -h
Usage: [OPTIONS] [TYPE] Pattern
       debug-backup Show debug logs for Targets

Optional Arguments
  -p, --profile      Set the profile name
  -s, --specific     Search for specific text on log
  -h, --help         Display this help message and exit

Examples:
  debug-backup -p PROFILE_NAME -s "2019-02-20 19:47"

Copyright BLOCKBIT® (http://www.blockbit.com/)
All rights reserved <info@blockbit.com>
```

Command Line Interface – debug-backup

Modo de uso:

```
admin >debug-backup
date="2021-01-14 15:37:01" device_id="4" backup_id="59" backup_name="Douglas Sistema" device_type="firewall" action="backup" device_name="UTM 2.1 - 200.31" storage_name="Storage_SMB" storage_type="smb" backup_type="system" status="running" status_message="" service="backup_manager"
date="2021-01-14 15:37:05" device_id="4" backup_id="59" backup_name="Douglas Sistema" device_type="firewall" action="backup" device_name="UTM 2.1 - 200.31" storage_name="Storage_SMB" storage_type="smb" backup_type="system" status="error" status_message="" service="backup_manager"
date="2021-01-14 15:39:02" device_id="5" backup_id="62" backup_name="Backup_200.32" device_type="firewall" action="backup" device_name="UTM 2.1 - 200.32" storage_name="Storage_SMB" storage_type="smb" backup_type="snapshot" status="running" status_message="" service="backup_manager"
date="2021-01-14 15:40:02" device_id="5" backup_id="62" backup_name="Backup_200.32" device_type="firewall" action="backup" device_name="UTM 2.1 - 200.32" storage_name="Storage_SMB" storage_type="smb" backup_type="snapshot" status="downloading" status_message="" service="backup_manager"
date="2021-01-14 15:40:03" device_id="5" backup_id="62" backup_name="Backup_200.32" device_type="firewall" action="backup" device_name="UTM 2.1 - 200.32" storage_name="Storage_SMB" storage_type="smb" backup_type="snapshot" status="done" status_message="" service="backup_manager"
date="2021-01-14 15:41:03" device_id="4" backup_id="59" backup_name="Douglas Sistema" device_type="firewall" action="backup" device_name="UTM 2.1 - 200.31" storage_name="Storage_SMB" storage_type="smb" backup_type="system" status="running" status_message="" service="backup_manager"
date="2021-01-14 15:41:07" device_id="4" backup_id="59" backup_name="Douglas Sistema" device_type="firewall" action="backup" device_name="UTM 2.1 - 200.31" storage_name="Storage_SMB" storage_type="smb" backup_type="system" status="error" status_message="" service="backup_manager"
date="2021-01-14 15:45:02" device_id="4" backup_id="59" backup_name="Douglas Sistema" device_type="firewall" action="backup" device_name="UTM 2.1 - 200.31" storage_name="Storage_SMB" storage_type="smb" backup_type="system" status="running" status_message="" service="backup_manager"
date="2021-01-14 15:45:05" device_id="4" backup_id="59" backup_name="Douglas Sistema" device_type="firewall" action="backup" device_name="UTM 2.1 - 200.31" storage_name="Storage_SMB" storage_type="smb" backup_type="system" status="error" status_message="No available space disk" service="backup_manager"
date="2021-01-14 15:49:04" device_id="4" backup_id="59" backup_name="Douglas Sistema" device_type="firewall" action="backup" device_name="UTM 2.1 - 200.31" storage_name="Storage_SMB" storage_type="smb" backup_type="system" status="running" status_message="" service="backup_manager"
admin >
```

Command Line Interface – debug-backup

Exibe as informações à seguir:

- **Date:** Define a data e hora;
- **Device_id:** Determina o ID do dispositivo;
- **Device_type:** Define o tipo do dispositivo, podendo ser:
 - manager;
 - firewall;
 - analyzer.
- **Action:** Determina qual ação a rotina tomará:
 - backup;
 - restore.
- **Device_name:** Exibe o nome do dispositivo;
- **backup_name:** Mostra o nome do arquivo de backup;
- **storage_name:** Exibe o nome do armazenamento remoto;
- **storage_type:** Define o tipo do armazenamento remoto;
- **backup_type:** Determina o tipo do backup, podendo ser:

- snapshot;
 - image;
 - logger.
- **Status:** Exibe a mensagem do status, podendo ser:
 - waiting;
 - running;
 - error;
 - success.
- **Status_message:** Caso o status tenha exibido uma mensagem (mais comum no caso de erros), esta linha exibe a mensagem do status.

[debug-deployer]

Utilizado para monitorar o *deployer* das configurações e instalação de pacote nas devices.

Modo de uso:

```
admin >debug-deployer
2017-05-15 17:57:50: (Task:sync-device - Dev:6) Finish sync-device
2017-05-15 17:57:51: (Task:sync-device - Dev:8) Finish sync-device
2017-05-15 17:57:51: (Task:sync-device - Dev:9) Finish sync-device
2017-05-15 17:57:51: (Task:sync-device - Dev:7) Finish sync-device
2017-05-15 17:57:51: (Task:sync-device - Dev:8) Finish sync-device
2017-05-15 17:57:52: (Task:sync-device - Dev:6) Finish sync-device
2017-05-15 17:57:52: (Task:sync-device - Dev:2) Finish sync-device
2017-05-15 17:57:52: (Task:sync-device - Dev:4) Finish sync-device
2017-05-15 17:57:52: (Task:sync-device - Dev:5) Finish sync-device
2017-05-15 17:57:52: (Task:sync-device - Dev:3) Finish sync-device
```

Figura 518 – *Command Line Interface – debug-deployer.*

[debug-ha]

Este comando tem como função exibir os *logs* de *debug* dos serviços de Alta Disponibilidade (H.A.).

Modo de uso:

```
admin ~>debug-ha
type=ha date=2018-03-17 11:54:49 Mar 1 11:54:49 master.blockbit.com blockbit-apply-cluster-master-notifyVI_2: conntrack primary
type=ha date=2018-03-17 11:54:50 Mar 1 11:54:50 master.blockbit.com blockbit-apply-cluster-master-notifyVI_1: reconfigure macaddr: eth7 (00:90:28:01:2f:48)
type=ha date=2018-03-17 11:54:50 Mar 1 11:54:50 master.blockbit.com blockbit-apply-cluster-master-notifyVI_1: conntrack primary
```

Command Line Interface – debug-ha

[debug-rotation]

Este comando é utilizado para consultar os logs de manutenção via CLI armazenado.

```
admin >debug-rotation -h
Usage: [OPTIONS] Pattern
       debug-rotation Show debug logs for log rotation

Optional Arguments
  -dev, --device      Search for specific device
  -s, --specific      Search for specific text on log
  -h, --help          Display this help message and exit

Examples:
  debug-logrotate -dev d1 -s "2019-02-20 19:47"

Copyright BLOCKBIT® (http://www.blockbit.com/)
All rights reserved <info@blockbit.com>

admin >|
```

Command Line Interface – debug-rotation -h

Modo de uso:

```
admin >debug-rotation -h
Feb 19 10:02:37 logserver21-80 gsm-apply-rotate: total_space_disk="150" total_used_disk_ini="4.30%" device_id="5" device_name="Logon Remoto" date="2021-2-19 10:12" deleted_date_ini="logstash-2021-02-17" de
leted_date="2021-02-18" deleted_date="2021-02-17" deleted_date="2021-02-18" deleted_date="2021-02-19" deleted_date_end="" Total_used_disk_end="40%" total_free_space_disk="146" current_total_index="0" service
="log-rotation"
```

Command Line Interface – debug-rotation -h

O comando exibe as informações à seguir:

- **Date:** Exibe a Data e hora;
- **Device_id:** Mostra o ID do dispositivo;
- **Device_name:** Exibe o nome do dispositivo;
- **Deleted_date_ini:** Exibe a data inicial do período de logs apagados;
- **Deleted_date_end:** Exibe a data final do período de logs apagados;
- **Current_total_index:** Mostra o total atual de índices de logs;
- **Total_space_disk:** Exibe o total de espaço utilizado pelo armazenamento;
- **Total_free_space_disk:** Mostra o espaço disponível total.

[debug-sync]

Utilizado para monitorar a comunicação do *Blockbit* GSM com as *devices*. Exibe as atualizações e o *status* das *devices*.

Modo de uso:

```
admin >debug-sync
2017-05-15 19:30:24: (Task:status-device - Dev:7) Authentication OK
2017-05-15 19:30:24: (Task:status-device - Dev:7) Finish status-device
2017-05-15 19:30:24: (Task:status-device - Dev:6) Authentication OK
2017-05-15 19:30:24: (Task:status-device - Dev:6) Finish status-device
2017-05-15 19:30:24: (Task:status-device - Dev:4) Authentication OK
2017-05-15 19:30:24: (Task:status-device - Dev:4) Finish status-device
2017-05-15 19:30:24: (Task:status-device - Dev:3) Authentication OK
2017-05-15 19:30:24: (Task:status-device - Dev:3) Finish status-device
2017-05-15 19:30:24: (Task:status-device - Dev:9) Authentication OK
2017-05-15 19:30:24: (Task:status-device - Dev:9) Finish status-device
admin >
```

Figura 519 – *Command Line Interface – debug-sync*.

[delete-logger-backup]

Esse comando tem como função apagar o *storage* da *Logger*.

Modo de Uso:

```
admin >delete-logger-backup -h
Usage: delete-logger-backup [OPTIONS] [TYPE] Pattern
Get files backup logger

Optional Arguments
  -p, --file      Backup file
  -h, --help      Display this help message and exit

Copyright BLOCKBIT® (http://www.blockbit.com/)
All rights reserved <info@blockbit.com>

admin >█
```

Command Line Interface - delete-logger-backup

[disable-snmp]

Desabilita o serviço de *SNMP*.

Modo de uso:

```
admin >disable-snmp
snmpd is disabled!
admin >
```

Command Line Interface – disable-snmp



Desabilita apenas o serviço, as configurações permanecerão.

[enable-root]

Habilita o acesso *root* ao sistema, será necessário entrar com a senha compatível a chave que aparecerá na tela.

Modo de uso:

```
admin >enable-root  
Challenge: 7bad30ac339b94cc259d756a02b62ff7  
Type the password: █
```

Figura 520 – *Command Line Interface – enable-root.*

[enable-snmp]

Habilita e configura o *SNMP* (*SNMPv1*, *SNMPv2* ou *SNMPv3*).

Modo de uso:

```
admin >enable-snmp
Location: Sao Paulo
Organization: BLOCKBIT
E-mail: admin@blockbit.com
Enable SNMPv1 (Y/N)? Y
Enable SNMPv2 (Y/N)? Y
Community name: BLOCKBIT
Network Access (Leave blank to default 0.0.0.0/0): 172.16.102.0/24
Enable SNMPv3 (Y/N)? Y
Auth Protocol (MD5 or SHA): MD5
Username: blockbit
User password (minimum of 8 characters): password
Encryption Protocol (3DES or DES): 3DES
Encryption Password: password
Enable SNMPv1
Enable SNMPv2
Community: BLOCKBIT
Network Access: 172.16.102.0/24
Enable SNMPv3
Auth Protocol: MD5
Username: blockbit
Encryption Protocol: 3DES

Confirm (Y/N)? Y
```

Command Line Interface – enable-snmp

Após confirmar a configuração acima, é exibido as configurações abaixo:


```

snmp is enabled!

syslocation "Sao Paulo"

syscontact "admin@blockbit.com"
syscontact "BLOCKBIT"

com2sec local localhost BLOCKBIT
com2sec mynetwork 172.16.102.0/24 BLOCKBIT

group MyRWGroup v1 local
group MyRWGroup v2c local
group MyRWGroup usm local

group MyROGroup v1 mynetwork
group MyROGroup v2c mynetwork
group MyROGroup usm mynetwork

view all included .1.3.6.1.2.1.1
view all included .1.3.6.1.2.1.2
view all included .1.3.6.1.4.1.2021
view all included .iso.org.dod.internet.mgmt.mib-2.system
view all included .iso.org.dod.internet.mgmt.mib-2.host.hrSystem.hrSystemUptime
view all included .iso.org.dod.internet.mgmt.mib-2.host.hrDevice
view all included .iso.org.dod.internet.mgmt.mib-2.host.hrSWRunPerf
view all included .iso.org.dod.internet.mgmt.mib-2.host.hrStorage
view all included .iso.org.dod.internet.private.enterprises.ucdavis.laTable.laEntry
view all included .1.3.6.1.4.1.8072.1.3.2.4.1.2
view all included .1.3.6.1.2.1.31

pass .1.3.6.1.2.1.31.1.1.1.18 /bin/bash /opt/omne/conf/mibs/net-ifalias

access MyROGroup "" any noauth exact all none none
access MyRWGroup "" any noauth exact all none none
rouser blockbit
admin >

```

Command Line Interface – enable-snmp – Exemplo de configurações

As informações obtidas através do *SNMP* podem ser melhor visualizadas através do *Zabbix*, para mais informações a respeito acesse esta [página](#). Atente que caso deseje utilizar o *Zabbix* o nome da sua comunidade não pode possuir espaços. Ex.: *Community Name: Blockbit Community*.



Para mais informações sobre notificações via *SNMP*, consulte esta [página](#).



Caso deseje usar um *community name* com espaços no *Zabbix*, será necessário nomeá-la entre aspas. Ex.: *Community Name: "Blockbit Community"*

[ethtool]

Utilizado para apresentar e detalhar informações referente às interfaces de rede, verificar as interfaces *online*, *offline*, alterar velocidade, alterar forma de negociação e verificar qual interface está localizada fisicamente.

Modo de uso:

```
admin >ethtool -h
ethtool version 3.15
Usage:
    ethtool DEVNAME Display standard information about device
    ethtool -s|--change DEVNAME      Change generic options
    [ speed %d ]
    [ duplex half|full ]
    [ port tp|au|bnc|mii|fibre ]
    [ mdix auto|on|off ]
    [ autoneg on|off ]
    [ advertise %x ]
    [ phyad %d ]
    [ xcvr internal|external ]
    [ wol p|u|m|b|a|g|s|d... ]
    [ sopass %x:%x:%x:%x:%x:%x ]
    [ msglvl %d | msglvl type on|off ... ]
```

Figura 521 – Command Line Interface – ethtool.

Exemplo: Identificar uma interface de rede específica:

```
admin >ethtool eth0
Settings for eth0:
    Supported ports: [ TP ]
    Supported link modes:   10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Full
    Supported pause frame use: Symmetric
    Supports auto-negotiation: Yes
    Advertised link modes:  10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Full
    Advertised pause frame use: Symmetric
    Advertised auto-negotiation: Yes
    Speed: 1000Mb/s
    Duplex: Full
    Port: Twisted Pair
    PHYAD: 1
    Transceiver: internal
    Auto-negotiation: on
    MDI-X: off (auto)
    Supports Wake-on: pumbg
    Wake-on: g
    Current message level: 0x00000007 (7)
                           drv probe link
    Link detected: yes
Admin >
```

Figura 522 – Command Line Interface – ethtool - Exemplo.

[exit]

Utilizado para abandonar a sessão.

Modo de uso:

A screenshot of a Command Line Interface (CLI) with a black background and white text. The prompt 'Modo de uso' is displayed on the first line. The second line shows 'admin >exit' followed by a vertical cursor bar. The word 'exit' is highlighted in red.

```
Modo de uso  
admin >exit |
```

Figura 523 – *Command Line Interface* – exit.

[fdisk]

Utilizado para gerenciamento de partições de discos rígidos. É possível listar e identificar dispositivos de armazenamento do tipo *HDD-SSD*, criar partições físicas, lógicas, excluir, exibir informações e etc.

Modo de uso:

```
admin >fdisk -h
Usage:
fdisk [options] <disk>    change partition table
fdisk [options] -l <disk> list partition table(s)
fdisk -s <partition>      give partition size(s) in blocks
Options:
-b <size>                  sector size (512, 1024, 2048 or 4096)
-c[=<mode>]                compatible mode: 'dos' or 'nondos' (default)
-h                          print this help text
-u[=<unit>]                display units: 'cylinders' or 'sectors' (default)
-v                          print program version
-C <number>                specify the number of cylinders
-H <number>                specify the number of heads
-S <number>                specify the number of sectors per track
admin >
```

Figura 524 – *Command Line Interface – fdisk.*

Exemplo: Listar os discos e partições existentes:

```

admin >fdisk -l
WARNING: fdisk GPT support is currently new, and therefore in an experimental phase.
Use at your own discretion.

Disk /dev/sda: 128.0 GB, 128035676160 bytes, 250069680 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: gpt

#          Start          End          Size Type          Name
1          2048           4095          1M BIOS boot parti
2          4096          1052671         512M Microsoft basic
3         1052672         42049535         19.6G Microsoft basic
4         42049536         70758399         13.7G Microsoft basic
5         70758400         74891263          2G Linux swap
6         74891264         79024127          2G Microsoft basic
7         79024128         250069646         81.6G Microsoft basic

Disk /dev/napper/luks-ba8b8ea1-522e-49c2-9c48-02e8db50ec5d: 21.0 GB, 20988297216
bytes, 40992768 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/napper/luks-049e58a3-626a-46bf-8019-3db9fd8b6241: 87.6 GB, 87573208576
bytes, 171041423 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/napper/luks-999d4257-849e-4a76-9bbf-6a0ae186ac98: 2113 MB, 2113929216
bytes, 4128768 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/napper/luks-92f58453-e018-4e1f-a014-2489dfb715e1: 14.7 GB, 14696841216
bytes, 28704768 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/napper/cryptoswap: 2116 MB, 2116026368 bytes, 4132864 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

admin >

```

Figura 525 – Command Line Interface – fdisk – Exemplo.

[free]

Utilizado para verificar o tamanho e uso da memória no servidor.

Modo de uso:

```
admin >free --h
free: option '--h' is ambiguous; possibilities: '--human' '--help'

Usage:
  free [options]

Options:
  -b, --bytes          show output in bytes
  -k, --kilo           show output in kilobytes
  -m, --mega           show output in megabytes
  -g, --giga           show output in gigabytes
  --tera              show output in terabytes
  -h, --human          show human-readable output
  --si                use powers of 1000 not 1024
  -l, --lohi           show detailed low and high memory statistics
  -t, --total          show total for RAM + swap
  -s N, --seconds N   repeat printing every N seconds
  -c N, --count N     repeat printing N times, then exit
  -w, --wide           wide output

  --help              display this help and exit
  -V, --version        output version information and exit

For more details see free(1).
admin >
```

Figura 526 – Command Line Interface – free.

Exemplo: Verificar o consumo de memória:

```
admin >free -m
              total        used        free      shared  buff/cache   available
Mem:          3952          172          186         216       3593       3324
Swap:          1995           80         1915
admin >
```

Figura 527 – Command Line Interface – free – Exemplo.

[fsck]

Utilizado para verificar e corrigir erros em discos e sistemas de arquivos.

Modo de uso:

```
admin >fsck -h
/usr/sbin/fsck.ext4: invalid option -- 'h'
Usage: /usr/sbin/fsck.ext4 [-panyrcdfvtDFV] [-b superblock] [-B blocksiz]
      [-I inode_buffer_blocks] [-P process_inode_size]
      [-l|-L bad_blocks_file] [-C fd] [-j external_journal]
      [-E extended-options] device

Emergency help:
-p          Automatic repair (no questions)
-n          Make no changes to the filesystem
-y          Assume "yes" to all questions
-c          Check for bad blocks and add them to the badblock list
-f          Force checking even if filesystem is marked clean
-v          Be verbose
-b superblock Use alternative superblock
-B blocksiz  Force blocksiz when looking for superblock
-j external_journal Set location of the external journal
-l bad_blocks_file Add to badblocks list
-L bad_blocks_file Set badblocks list
admin >
```

Figura 528 – Command Line Interface – fsck.

Exemplo: Verificar se existem possíveis erros em determinada partição:

```
Admin >fsck /dev/sda3
fsck from util-linux-ng 2.17.2
e2fsck 1.41.12 (17-May-2010)
/dev/sda3: clean, 702/192000 files, 52661/768000 blocks
...
reloading firewall chains
reloading firewall zones
reloading firewall input
iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
reloading firewall redirects
reloading firewall security rules
reloading firewall multilink rules
reloading firewall vpn rules
reloading firewall atp rules
admin >
```

Figura 529 – Command Line Interface – fsck - Exemplo.

[grep]

Este comando tem como função executar uma busca pela ocorrência de expressões regulares que correspondam com o padrão pesquisado. Ele é utilizado em conjunto com outros comandos para filtrar os resultados de saída.

Exemplo: Filtrar a saída do *debug-web* para visualizar apenas as requisições com destino a uma *URL* específica:

```
admin >debug-web|grep blockbit.com
type=web date=2018-03-14 10:51:43 bytes=745 nrc=00:00:00:00:00:00 src=172.16.12.82:15958 dst=104.108.108.7:443 code=TCP_TUNNEL/ method=CONNECT rule=WEB: Navegação Permitida user= site=ww
w.blockbit.com url=www.blockbit.com agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.166 Safari/537.36]
type=web date=2018-03-14 10:52:18 bytes=1011 mac=08:09:90:80:00:00 src=172.16.12.82:16962 dst=104.108.203.7:443 code=TCP_TUNNEL/ method=CONNECT rule=WEB: Navegação Permitida user= site=ww
w.blockbit.com url=www.blockbit.com agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.166 Safari/537.36]
type=web date=2018-03-14 10:53:10 bytes=1011 mac=00:00:00:00:00:00 src=172.16.12.82:16968 dst=104.108.203.7:443 code=TCP_TUNNEL/ method=CONNECT rule=WEB: Navegação Permitida user= site=ww
w.blockbit.com url=www.blockbit.com agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.166 Safari/537.36]
```

Figura 880 - Command Line Interface – *grep* - exemplo.

Exemplo 2: Filtrar a saída do comando *ethtool* utilizando *regex*:

```
admin >ethtool eth0|grep -ie "speed\|detected"
Speed: 10000Mb/s
Link detected: yes
```

Figura 881 - Command Line Interface – *grep* – exemplo 2.

[help]

Utilizado para exibir uma lista de todos os comandos disponíveis na interface.

Modo de uso:

```
admin >help
arp                ifconfig            ntpdate            show-devices
arping             ifstat              passwd             show-license
date               iotest              ping               show-uuid
debug-deployer    ip                  reboot             show-version
debug-sync         ipcalc              reset              shutdown
enable-root        less                reset-admin-block  tcpdump
ethtool            logger-config        reset-admin-password  tcptop
exit               logger-devices-add   reset-admin-sessions  telnet
fdisk              logger-devices-list reset-logs           tracepath
free               logger-disable        rewizard            traceroute
fsck               logger-enable         route                update-gsm
grep               logger-key            sar                  update-license
help               lscpu                 set-network-dns       uptime
history            mkfs                  set-network-gateway   vmstat
hostname           more                   set-network-interface whois
hystory            netstat                set-network-timezone
admin >|
```

Figura 530 – Command Line Interface – help.

[history]

Ao utilizar-se desse comando, é exibido um histórico de todos os últimos comandos utilizados.

Modo de uso:

```
admin >history
1:  aa
2:  help
3:  ifconfig eth0 172.31.102.235
4:  route add default gw 172.31.0.1
5:  ifconfig
6:  hrlp
7:  help
8:  route -n
9:  ifconfig eth0 172.31.102.236
10: route add default gw 172.31.0.1
11: route -n
12: ifconfig
13: route -n
14: ifconfig
15: ifconfig eth0 172.31.102.236/16
16: route add default gw 172.31.0.1
17: ifconfig
18: grep
19: grep log myfile
20: ls
21: fgrep log myfile
22: grep
23: ?
24: debug-deployer
25: debug-sync
26: debug-sync | grep log
27: history
admin >
```

Figura 531 – *Command Line Interface – history.*

[hostname]

Utilizado para exibir ou alterar o nome de *host* do seu dispositivo *Blockbit* UTM.

Modo de uso:

```
Modo de uso
admin >hostname -h
Usage: hostname [-b] {hostname|-F file}      set host name (from file)
        hostname [-a|-A|-d|-f|-i|-I|-s|-y]    display formatted name
        hostname                               display host name

        {yp,nis,}domainname {nisdomain|-F file} set NIS domain name (from file)
        {yp,nis,}domainname                  display NIS domain name

        dnsdomainname                        display dns domain name

        hostname -V|--version|-h|--help      print info and exit

Program name:
        {yp,nis,}domainname=hostname -y
        dnsdomainname=hostname -d

Program options:
        -a, --alias                alias names
        -A, --all-fqdns            all long host names (FQDNs)
        -b, --boot                 set default hostname if none available
        -d, --domain               DNS domain name
        -f, --fqdn, --long         long host name (FQDN)
        -F, --file                 read host name or NIS domain name from given file
        -i, --ip-address           addresses for the host name

        -I, --all-ip-addresses     all addresses for the host
        -s, --short                short host name
        -y, --yp, --nis            NIS/YP domain name

Description:
        This command can get or set the host name or the NIS domain name. You can
        also get the DNS domain or the FQDN (fully qualified domain name).
        Unless you are using bind or NIS for host lookups you can change the
        FQDN (Fully Qualified Domain Name) and the DNS domain name (which is
        part of the FQDN) in the /etc/hosts file.
admin >
```

Figura 532 – Command Line Interface – *hostname*.

Exemplo: Utilizar o comando para exibir o nome atual do seu dispositivo *Blockbit* UTM:

```
admin >hostname
gsm.blockbit.com
admin >
```

Figura 533 – Command Line Interface – *hostname* - Exemplo.

[ifconfig]

Utilizado para configurar e manter as configurações da interface. Pode ativar, desativar e listar o status de cada uma das interfaces. Também pode ser utilizado para otimizar a configuração do sistema.

Modo de uso:

```
admin >ifconfig -h
Usage:
  ifconfig [-a] [-v] [-s] <interface> [[<AF>] <address>]
  [add <address>[/<prefixlen>]]
  [del <address>[/<prefixlen>]]
  [[-]broadcast <address>] [[-]pointopoint <address>]
  [netmask <address>] [dstaddr <address>] [tunnel <address>]
  [outfill <NN>] [keepalive <NN>]
  [hw <HW> <address>] [mtu <NN>]
  [[-]trailers] [[-]arp] [[-]allmulti]
  [multicast] [[-]promisc]
  [mem_start <NN>] [io_addr <NN>] [irq <NN>] [media <type>]
  [txqueuelen <NN>]
  [[-]dynamic]
  [up|down] ...
  <HW>=Hardware Type.
  List of possible hardware types:
    loop (Local Loopback) slip (Serial Line IP) cslip (VJ Serial Line IP)
    slip6 (6-bit Serial Line IP) cslip6 (VJ 6-bit Serial Line IP) adaptive (Adaptive
Serial Line IP)
    ash (Ash) ether (Ethernet) ax25 (AMPR AX.25)
    netrom (AMPR NET/ROM) rose (AMPR ROSE) tunnel (IPIP Tunnel)
    ppp (Point-to-Point Protocol) hdlc ((Cisco)-HDLC) lapb (LAPB)
    arcnet (ARCnet) dlci (Frame Relay DLCI) frad (Frame Relay Access Device)
    sit (IPv6-in-IPv4) fddi (Fiber Distributed Data Interface) hippi (HIPPI)
    irda (IrLAP) ec (Econet) x25 (generic X.25)
    infiniband (InfiniBand) eui64 (Generic EUI-64)
  <AF>=Address family. Default: inet
  List of possible address families:
    unix (UNIX Domain) inet (DARPA Internet) inet6 (IPv6)
    ax25 (AMPR AX.25) netrom (AMPR NET/ROM) rose (AMPR ROSE)
    ipx (Novell IPX) ddp (Appletalk DDP) ec (Econet)
    ash (Ash) x25 (CCITT X.25)
admin >
```

Figura 534 – Command Line Interface – ifconfig.

Exemplo: Exibir as informações sobre todas as interfaces de rede, ativas e desabilitadas:

```

admin >ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.102.235 netmask 255.255.254.0 broadcast 172.16.103.255
    inet6 fd29:2e81:cb18:0:20c:29ff:fe57:b1e7 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::20c:29ff:fe57:b1e7 prefixlen 64 scopeid 0x20<link>
    inet6 2002:db5:db5:0:20c:29ff:fe57:b1e7 prefixlen 64 scopeid 0x0<global>
    ether 00:0c:29:57:b1:e7 txqueuelen 1000 (Ethernet)
    RX packets 23001360 bytes 5108284564 (4.7 GiB)
    RX errors 0 dropped 1210 overruns 0 frame 0
    TX packets 28303075 bytes 4079603075 (3.7 GiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 10.0.0.1 netmask 255.255.255.0 broadcast 10.0.0.255
    ether 00:0c:29:57:b1:f1 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth2: flags=4098<BROADCAST,MULTICAST> mtu 1500
    ether 00:0c:29:57:b1:fb txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth3: flags=4098<BROADCAST,MULTICAST> mtu 1500
    ether 00:0c:29:57:b1:05 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 0 (Local loopback)
    RX packets 123895270 bytes 37387210708 (34.8 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 123895270 bytes 37387210708 (34.8 GiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

admin >

```

Figura 535 – Command Line Interface – ifconfig - Exemplo.

[ifstat]

Utilizado para exibir a estatística do tráfego de rede.

Modo de uso:

```
admin >ifstat -h
Usage: ifstat [OPTION] [ PATTERN [ PATTERN ] ]
-h, --help                this message
-a, --ignore ignore history
-d, --scan=SECS           sample every statistics every SECS
-e, --errors show errors
-n, --nooutput            do history only
-r, --reset               reset history
-s, --noupdate            don't update history
-t, --interval=SECS      report average over the last SECS
-V, --version             output version information
-z, --zeros               show entries with zero activity
admin >
```

Figura 536 – Command Line Interface – ifstat.

Exemplo: Listar relatório estatístico geral do tráfego de todas as interfaces da rede:

```
admin >ifstat
#kernel
Interface      RX Pkts/Rate  TX Pkts/Rate  RX Data/Rate  TX Data/Rate
RX Errs/Drop  TX Errs/Drop  RX Over/Rate  TX Coll/Rate
lo             19982K 0      19982K 0      425601K 0     425601K 0
              0 0      0 0      0 0      0 0
eth0           896411 0      789041 0      676523K 0     687826K 0
              0 0      0 0      0 0      0 0
eth1           829588 0      821426 0      229273K 0     646217K 0
              0 1476 0 0      0 0      0 0
eth3           302159 0      19735 0      24840K 0      1616K 0
              0 30 0 0      0 0      0 0
ifb0           537040 0      537040 0      107390K 0     107390K 0
              0 0      0 0      0 0      0 0
ipsec0         0 0      0 0      0 0      0 0
              0 0      0 0      0 0      0 0
admin >
```

Figura 537 – Command Line Interface – ifstat - Exemplo.

[iotest]

Utilizado para executar um teste de escrita de entrada e saída (I/O) na estrutura de partições “file system” do disco do *Blockbit* UTM.

Modo de uso:

```
admin >iotest
Testing root filesystem
1000000+0 registros de entrada
1000000+0 registros de saída
2048000000 bytes (2,0 GB) copiados, 89,0756 s, 23,0 MB/s
Cleaning
admin >
```

Figura 538 – *Command Line Interface* – *iotest* - Exemplo.

[ip]

Através desse comando é possível executar a exibição, manipulação e roteamento de dispositivos, interfaces e túneis de rede.

Modo de uso:

```
admin >ip
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
where  OBJECT := { link | addr | addrlabel | route | rule | neigh | ntable |
                  tunnel | tuntap | maddr | mroute | mrule | monitor | xfrm |
                  netns | l2tp | tcp_metrics | token }
       OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
                    -f[amily] { inet | inet6 | ipx | dnet | bridge | link } |
                    -4 | -6 | -I | -D | -B | -O |
                    -l[oops] { maximum-addr-flush-attempts } |
                    -o[neline] | -t[imestamp] | -b[atch] [filename] |
                    -rc[vbuf] [size]}
```

Figura 539 – Command Line Interface – ip.

[ipcalc]

Utilizado para cálculo de máscara de rede/sub-redes IPv4 e IPv6. Possui opções para identificar o prefixo (máscara), o endereço de rede e de broadcast.

Modo de uso:

```
admin >ipcalc -h
ipcalc: ip address expected
Usage: ipcalc [OPTION...]
  -c, --check           Validate IP address for specified address family
  -4, --ipv4            IPv4 address family (default)
  -6, --ipv6            IPv6 address family
  -b, --broadcast       Display calculated broadcast address
  -h, --hostname        Show hostname determined via DNS
  -m, --netmask         Display default netmask for IP (class A, B, or C)
  -n, --network         Display network address
  -p, --prefix          Display network prefix
  -s, --silent          Don't ever display error messages

Help options:
  -?, --help           Show this help message
  --usage              Display brief usage message
admin >
```

Figura 540 – Command Line Interface – ipcalc.

Exemplo: Calcular uma *subnet*, seu endereço de rede e *broadcast*:

```
admin >ipcalc -n -b -p 192.168.7.0/23
PREFIX=23
BROADCAST=192.168.7.255
NETWORK=192.168.6.0
admin >
```

Figura 541 – Command Line Interface – ipcalc – Exemplo.

[less]

Utilizado para fazer a paginação de arquivos ou de uma entrada padrão. É possível direcionar a saída de outro comando usando o *pipe* “|”.

Modo de uso: Utilizar o comando *less* como saída de outro comando que devolve uma quantidade de informações muito extensa.

```
admin >iplist | less
admin >

ZONE LAN (1) 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 00:0c:29:71:fe:66 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.1/24 brd 192.168.1.255 scope global eth0
        valid_lft forever preferred_lft forever
eth0: negotiated 1000baseT-FD flow-control, link ok

ZONE WAN (3) 3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc htb state UP
qlen 1000
    link/ether 00:0c:29:71:fe:70 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.11/24 brd 192.168.0.255 scope global eth1
        valid_lft forever preferred_lft forever
eth1: negotiated 1000baseT-FD flow-control, link ok
ZONE (WAN) eth2: negotiated 1000baseT-FD flow-control, link ok
ZONE DMZ (2) 5: eth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 00:0c:29:71:fe:84 brd ff:ff:ff:ff:ff:ff
    inet 172.16.102.11/24 brd 172.16.102.255 scope global eth3
        valid_lft forever preferred_lft forever
eth3: negotiated 1000baseT-FD flow-control, link ok
(END)
```

Figura 542 – *Command Line Interface – less.*

[logger-config]

Este comando serve para habilitar um *Wizard* de configuração para a instalação de um servidor *logger*.



Para mais informações a respeito do processo de instalação de *loggers*, consulte esta [página](#).



É recomendável executar esse comando diretamente no *console* da máquina, pois durante a sua configuração a conexão SSH é derrubada.

Há dois modos de operação disponíveis: *Standalone* ou *Integrated*, a diferença entre estes é:

Standalone

Neste modo de operação, o servidor é exclusivo para *logger* remoto, não sendo possível utilizá-lo para qualquer outra função, sendo obrigatório utilizar-se do *firmware* da *Blockbit*.

Integrated

Este modo de operação permite utilizar-se do próprio GSM local onde o *manager* estiver instalado como servidor de *logger*. Porém, é necessário dedicar um disco inteiro apenas para esta função, sendo indiferente se este mesmo será virtual ou físico.

Modo de uso:

Exemplo 1: Para a instalação de um *logger standalone* é necessário optar por este modo de operação quando requisitado em “Enter the logger operating mode”, a seguir analisaremos cada uma das opções que aparecerem no *wizard*:

```
admin >logger-config
Enter the logger operating mode: [ standalone / integrated ]: standalone
Interface (ex: eth0): eth0
IP address (ex: 1.1.1.10): 172.31.200.80
Mask (ex: 255.255.255.0): 255.255.0.0
Gateway (ex: 1.1.1.1): 172.31.0.1
Hostname (ex: logger): gsmlogger
DNS (ex: 1.1.1.2): 172.31.0.180
Timezone (ex: America/Sao_Paulo): America/Sao_Paulo

Disk /dev/sda: 128.8 GB  SYSTEM
Disk /dev/sdb: 16.1 GB  EXT4
Disk (ex: /dev/sdb): /dev/sdb
mke2fs 1.42.9 (28-Dec-2013)
/dev/sdb is entire device, not just one partition!
Proceed anyway? (y,n) y
```

Command Line Interface – logger-config – Exemplo 1

- **Interface:** Tipo de interface do GSM. Ex.: eth0;
- **IP address:** Endereço IP do GSM. Ex.: 172.31.102.236;
- **Mask:** Máscara de rede do GSM. Ex.: 255.255.0.0;
- **Gateway:** Determina o *gateway* do GSM. Ex.:172.31.0.1;
- **Hostname:** Define o *Hostname* que será utilizado pelo *Logger*. Ex.: gsmlogger;
- **DNS:** Determina o *DNS* do GSM. Ex.:172.16.102.148;
- **Timezone:** Determina a zona temporal com a qual o GSM foi configurado. Ex.: America/Sao_Paulo;
- **Disk:** Determina o disco no qual o *logger* será instalado. Será exibido um resumo dos discos que integram a *appliance*, e o *status* deles (por exemplo, “Available” representa um disco disponível e “System” um disco utilizado pelo sistema). Deve-se digitar o diretório do disco que será utilizado. Após esse passo, uma mensagem alertando o fato de que será utilizado o disco inteiro e não apenas uma partição surgirá, para proceder, digite “y” e tecla “enter”. Ex.: /dev/sdb;

- **Generate Key:** Para gerar a chave secreta digite “y” e tecla “enter”, é importante guardar essa sequência pois ela será utilizada durante a criação do *Logger* na interface visual do *Analyzer* no GSM (para mais informações consulte esta [página](#)).



Atente que caso o usuário opte que uma chave não seja gerada quando o *prompt* exibir “Generate Key?”, ele poderá usar o comando “logger-key -c” ou efetuar o “logger-config” mais uma vez.

No final do *wizard* deve-se chegar em resultados semelhantes aos exibidos pela imagem abaixo:

```
admin >logger-config
Enter the logger operating mode: [ standalone / integrated ]: standalone
Interface (ex: eth0): eth0
IP address (ex: 1.1.1.10): 172.31.200.80
Mask (ex: 255.255.255.0): 255.255.0.0
Gateway (ex: 1.1.1.1): 172.31.0.1
Hostname (ex: logger): gsmlogger
DNS (ex: 1.1.1.2): 172.31.0.100
Timezone (ex: America/Sao_Paulo): America/Sao_Paulo

Disk /dev/sda: 128.8 GB  SYSTEM
Disk /dev/sdb: 16.1 GB  EXT4
Disk (ex: /dev/sdb): /dev/sdb
mkfs2fs 1.42.9 (28-Dec-2013)
/dev/sdb is entire device, not just one partition!
Proceed anyway? (y,n) y
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
983040 inodes, 3932160 blocks
196608 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
120 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

Generate key? [y/N]: y
Key:
53616c7465645f5f1fd31d110bfa221ae5e812311b838210546609b76aa5600820d1652f3dd95becb35ef5df77ece59527
7c3979b16741098b2329bdd5b39e8057aca51725c4c74a7ec30e34142fca78308b428fe551a89f465d73ef628dff2f910b-
3ea33e4f09f3146feb57a9fb23d2ac0e2e274acff2d6d70ba6cf e641f4e3e5499c9290ca6cf41c2b8b8eb7cc0ebd7dcfe9f
2fdefca61d98a28882b8c915d9f7e16745f4968c28ce6e030114163042744d0c1dd9000310c9f6c2ed7378f25c7592444e
84bc3a0301d6ee2a8a27cf732a930311da3cd05ebf54675fd2f5719fdbc8ec14e33d3d5e265b56806f8060d6c30e398fbc7
9b4b0c3caf417ae7fef536014aff35554d9cfe81149b819b0659730b29740b6a8d38f2daf9d85716ba1fc1f1b468732ac6f
9b23f113ac1925a38fa79e8f39f98dd8f9357774842c0bffa5a93f69c0346240b03f7cc930604634fc8a1c51af8de1248fd
7ad25b8a828e0480bee015860d75b5b4829f05f984dff115d0c8d3d66451e327ab00f67dc8f3b29475e55d25657026ac2e
f3ca8275b3eb42d2744f0c15c14bd09ff1e54078c6b3cb0bff3b8a9ce904e2b81b861da2f62b0b35b8f869505e2c9b127c
56aed9c9999ad3f180f9834c9eca59a3517708d6e2ed39515aeb87f46c635d45a3e73fcffe36ad00568d8c5f1964ce1e36f
5a2ba9f59f3b319a00a35c13f031df14cd98e0322d93adc4cae29a1ed4b362da5fe0f171d724d68449c59a99bf6d00b0f8f
22e8e3709f5ae1562948b12e3f5be5c716b0d9cd4f51b331143819c6d6e345bc10cc1bf2a9d95f40b75a1fc8eccebf94e1f
0983396d70a88596d6276234289b46bc427af1f158e25ceb39807ed37a9238d939031f2cfc4fc8a9d3a448b612ccabf54f
b8398b70e0e3c71c961c27572832024ff32e32960a3e929dcf18980f0f10ab35d8f9cf399057b

Completed

Now configure the logger in administrative interface
```

Command Line Interface – logger-config – Standalone

Exemplo 2: Para a instalação de um *logger* integrado é necessário optar por este modo de operação quando requisitado em “Enter the logger operating mode”, a seguir analisaremos cada uma das opções que aparecerem no *wizard*:

```

admin >logger-config
Enter the logger operating mode: [ standalone / integrated ]: integrated

Disk /dev/sda: 34.4 GB  SYSTEM
Disk /dev/sdb: 2147 MB  AVAILABLE
Disk (ex: /dev/sdb): /dev/sdb
mke2fs 1.42.9 (28-Dec-2013)
/dev/sdb is entire device, not just one partition!
Proceed anyway? (y,n) y

```

Command Line Interface – logger-config – Exemplo 2

- **Disk:** Determina o disco no qual o *logger* será instalado. Será exibido um resumo dos discos que integram a *appliance*, e o *status* deles (por exemplo, “Available” representa um disco disponível e “System” um disco utilizado pelo sistema). Deve-se digitar o diretório do disco que será utilizado. Após esse passo, uma mensagem alertando o fato de que será utilizado o disco inteiro e não apenas uma partição surgirá, para proceder, digite “y” e tecla “enter”. Ex.: /dev/sdb;
- **Generate Key:** Para gerar a chave secreta digite “y” e tecla “enter”, é importante guardar essa sequência pois ela será utilizada durante a criação do *Logger* na interface visual do *Analyzer* no *GSM* (para mais informações consulte esta [página](#)).



Atente que caso o usuário opte que uma chave não seja gerada quando o *prompt* exibir “Generate Key?”, ele poderá usar o comando “*logger-key -c*” ou efetuar o “*logger-config*” mais uma vez.

No final do *wizard* deve-se chegar em resultados semelhantes aos exibidos pela imagem abaixo:

```

admin >
admin >logger-config
Enter the logger operating mode: [ standalone / integrated ]: integrated

Disk /dev/sda: 34.4 GB  SYSTEM
Disk /dev/sdb: 2147 MB  AVAILABLE
Disk (ex: /dev/sdb): /dev/sdb
mke2fs 1.42.9 (28-Dec-2013)
/dev/sdb is entire device, not just one partition!
Proceed anyway? (y,n) y
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Strides=0 blocks, Stripe width=0 blocks
131072 inodes, 524288 blocks
26214 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=536870912
16 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912

Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done

Generate key? [y/N]: y
Key:
53616c7465645f5fd6c4e9d919bc6daa94284d36b752d877f48cae914e5dda22a39c3a867ed26dfbfa105efbbb93635fd754f8f00b6b4bd96fd0f4f117db265c00088
6e64b863375ad73647143f4b38fa4c9dab14036baeabb9fa03e8ddf7db5e845849a7b6f8ea3e91e15d47dd7989a087d60460bce90d225cf9827b8c5bef0fca306b6862859
7219486dfb0e58cd3bab365d051198a0592ef05aebf7f012d02f429e9c8a8b6da95c6595890797d232e3a3704b9ba0119f422fb0b71a247c9a77225a979a1b59ab1d5356
02d39e0c8ab83c3d41430556fabba5dc090b199b24f0b7b887c33a313bc649c107447afdb8fd5e6c2872cfe801d5c17eed15698ed886519744fb31811cbf3d5a841597
2132dfa21e0f0e8fc35671ce94293be5bcfe329c6bc5be6a39fe4658d2ec4c9c7392782bfc4ccf5ac17813ce0fab8ace325a9f5d57df666aad9ba501ade152716a8d7927
f9d3aff1887a047a33045b0904df8b1a8bffa90ff4110f9da23b5a4a89f2804feabd455e810b21a984d6fea129dc8c09882c54b7a89a30c115c2fb29171c259feee1a377
918fe8fcb0a843351a56fb72968459ad595d8f0f3e676eec4de95af5f3d61852b1caf76ff076f3503a1ddf7f3eb1d8618855b68d29bd333eb7d2311ff2d522c197207a63
fdeb5a7489fcbcd6e21ce4d6f1f169afaa7fc0a1a3ea4b4cad1b40655c1d8d25f586f368ac629d4826fcaa99033adde5474e577501a95ce7fc01ec7bcfd5a0f614c3429
2867c8b03487769919c95e7d4695469befee193df003487584d75bd2640c2810715781c4a8a5a78dac3a01d4c4c07762f025a8a9e35292e3d10e2cc60966e035bf85ef07b
b1d7966b41e4a2c1b27721cd6098d3a1a4fd4315603e426f0539bc64e3369bb27fe78b912b9ef4df40c9150737132b8b9b8f11556ea0cd97a2aa55a82bcb5c0aaf1439ab9
ffd9c9

Completed

Now configure the logger in administrative interface

admin >

```

Command Line Interface – logger-config – Integrated

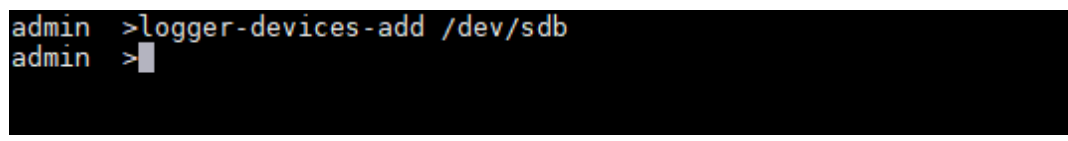


Caso necessite de mais informações a respeito dos Loggers, consulte esta [página](#).

[logger-devices-add]

Utilizado para adicionar *devices* no *logger*, é necessário passar o caminho da device para poder executar a adição.

Modo de uso:



```
admin >logger-devices-add /dev/sdb
admin >
```

Figura 547 – *Command Line Interface – logger-devices-add.*

[logger-devices-list]

Este comando serve para exibir uma lista de *devices* utilizados pelo *logger*.

Modo de uso:

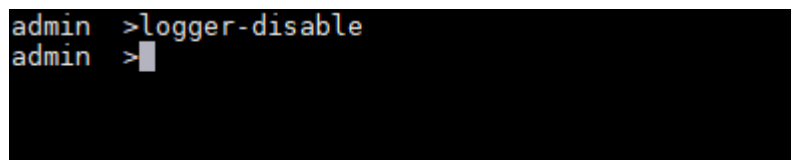
```
admin >logger-devices-list  
Disk /dev/sdb: 34.4 GB  P00L  
Disk /dev/sda: 34.4 GB  SYSTEM  
admin >
```

Figura 548 – *Command Line Interface – logger-devices-list*.

[logger-disable]

Comando para desabilitar o *logger* no *pool*.

Modo de uso:



```
admin >logger-disable  
admin >
```

Figura 549 – *Command Line Interface* – *logger-disable*.

[logger-enable]

Comando para habilitar o *logger* no *pool*.

Modo de uso:



```
admin >logger-enable  
admin >█
```

Figura 550 – *Command Line Interface* – *logger-enable*.

[logger-key]

Este comando é utilizado para exibir a chave secreta do *logger*, ela é utilizada durante a criação do *Logger* na interface visual do *Analyzer* no GSM.

Além disso, ao passar o parâmetro “-c” o comando irá gerar uma nova chave.

Modo de uso:

```
admin ->logger-key
53616c7465645f5fd6dc4e9d919bc6deaa94284d30b752d877f48cae914e5dda322aa39c3a867ed26dfbfa105efbbb93635fd754f8f00b6b4bd96fd0f4f117db265c00088
6e64b863375ad73647143f4b38fa4c9dab14036bacabb9fa03e8ddf7db5e845849a7b6f8ea3e91e15d47dd7989a087d60460bce90d225cf9827b8c5bef0fca396b6862859
7219486dfb9e58cd3bab365d051198a0592ef05a6bf7f012d02f429e9cba8b6dea95c6595890797d232e3a3704b9ba0119f422fb9b71a247c9a77225a979a1b59ab1d5356
02d39e0c8abd83cd41430556fabba5dc090b199b24f0b7b887c33a313bc649c107447afdb8fd5e6c2872cfed801d5c17eed15698ed886519744fb31811cbf3d5a841597
2132dfa21e6f0e8fcc35671ce94293be5bcfe329c6bc5be6a39fe4658d2ec4c9c7392782bfc4ccf5ac17813ce0fab8ace325a9f5d57df66d6ad9ba501ade152716a8d7927
f9d3aff1887a047a33045b0904df8b1a8bff490ff4110f9da23b5a4a89f2804fefabd455e810b21a984d6fea129dc8c09882c54b7a89a30c115c2fb29171c259feee1a377
918fe8fcb0a843351a56fb72968459ad595d8f0f3e678e6c4de95af5f3d61852b1caf76ff076f3503a1ddf7ff3eb1d8618855b68d29bd333eb7d2311ff2d522c197207a63
f0eb5a7489fcbcd6621ce4d6f1f109efaa77c0a1a3ea4b4cad1b49655c1d8d25f586f388ac629d4826fcaa99033adde5474e577501a95ce77f0c1ec7b0cfdaa5a0fe14c3429
2867c8b03487769919c05e7d4695489befee193df003487584d75b82640c2810715781c4a8a5a78d4c3a01d4c4c07762f025a8a9e35292e3d10e2cc6096e035bf05ef07b
b1d7966b41e4a2c1b27721cd6098d3a1a4fd4315603e426f0539bc64e3369bb27fe78b912b9ef4df40c9150737132b8b9b8f11556ea0cd97a2aa55a82bc5c0aaf1439ab9
ffd9c9
admin ->
```

Command Line Interface – logger-key

[lscpu]

Utilizado para exibir informações sobre a arquitetura da CPU.

Modo de uso:

```
admin >lscpu
Architecture:      x86_64
CPU op-mode(s):    32-bit, 64-bit
Byte Order:        Little Endian
CPU(s):            4
On-line CPU(s) list: 0-3
Thread(s) per core: 1
Core(s) per socket: 4
Socket(s):         1
NUMA node(s):      1
Vendor ID:         GenuineIntel
CPU family:        6
Model:             55
Model name:        Intel(R) Celeron(R) CPU J1900 @ 1.99GHz
Stepping:          8
CPU MHz:           2400.093
BogoMIPS:          4000.16
Virtualization:    VT-x
L1d cache:         24K
L1i cache:         32K
L2 cache:          1024K
NUMA node0 CPU(s): 0-3
admin >
```

Figura 552 – Command Line Interface – lscpu.

[mkfs]

Utilizado para executar uma formatação. Será necessário determinar o *device* que será formatado. Ex.: `mkfs -t ext4 /dev/sdb`;

Modo de uso:

```
admin >mkfs
Usage: mkfs.ext4 [-c|-l filename] [-b block-size] [-C cluster-size]
        [-i bytes-per-inode] [-I inode-size] [-J journal-options]
        [-G flex-group-size] [-N number-of-inodes]
        [-m reserved-blocks-percentage] [-o creator-os]
        [-g blocks-per-group] [-L volume-label] [-M last-mounted-directory]
        [-O feature[,...]] [-r fs-revision] [-E extended-option[,...]]
        [-t fs-type] [-T usage-type ] [-U UUID] [-jnqvDFKSV] device [blocks-count]
admin >
```

Figura 553 – *Command Line Interface – mkfs.*

[more]

Utilizado para fazer a paginação de arquivos ou de uma entrada padrão. É possível direcionar a saída de outro comando usando o *pipe* "|".

Modo de uso: Utilizar o comando `more` como saída de outro comando que devolve uma quantidade de informações muito extensa.

```
admin >iplist | more
ZONE LAN (1) 5: eth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
qlen 1000
    link/ether 00:0b:ab:ac:a3:b7 brd ff:ff:ff:ff:ff:ff
    inet 172.16.20.1/24 brd 172.16.20.255 scope global eth3
        valid_lft forever preferred_lft forever
eth3: negotiated 1000baseT-FD flow-control, link ok

ZONE DMZ (2) 8: eth0.102@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
noqueue state UP
    link/ether 00:0b:ab:ac:a3:b4 brd ff:ff:ff:ff:ff:ff
    inet 172.16.102.1/24 brd 172.16.102.255 scope global eth0.102
        valid_lft forever preferred_lft forever
eth0.102: negotiated 1000baseT-FD flow-control, link ok

ZONE DMZ (2) 7: eth0.101@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
noqueue state UP
    link/ether 00:0b:ab:ac:a3:b4 brd ff:ff:ff:ff:ff:ff
    inet 172.16.101.1/24 brd 172.16.101.255 scope global eth0.101
        valid_lft forever preferred_lft forever
eth0.101: negotiated 1000baseT-FD flow-control, link ok
ZONE LAN (1)
ZONE LAN (1) 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
qlen 1000
    link/ether 00:0b:ab:ac:a3:b4 brd ff:ff:ff:ff:ff:ff
    inet 172.16.12.1/23 brd 172.16.13.255 scope global eth0
        valid_lft forever preferred_lft forever
eth0: negotiated 1000baseT-FD flow-control, link ok
[--csv|-C] [--raw] [--xml] [--split] [--mpls] [--no-dns]
    [--show-ips] [--address interface] [--filename=FILE|-F]
    [--ipinfo=item_no|-y item_no] [--aslookup|-z]
    [--psize=bytes/-s bytes] [--order fields]
    [--report-wide|-w] [--inet] [--inet6] [--max-ttl=NUM] [--first-
ttl=NUM]
    [--bitpattern=NUM] [--tos=NUM] [--udp] [--tcp] [--port=PORT] [--
timeout=SECONDS]
    [--interval=SECONDS] HOSTNAME
admin >
```

Figura 554 – Command Line Interface – *more*.

[netstat]

Utilizado para exibir as portas em escuta no servidor.

Modo de uso:

```
admin >netstat
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address      Foreign Address    State
tcp      0      0 127.0.0.1:20518    0.0.0.0:*          LISTEN
tcp      0      0 0.0.0.0:4200      0.0.0.0:*          LISTEN
tcp      0      0 0.0.0.0:22        0.0.0.0:*          LISTEN
tcp      0      0 127.0.0.1:10519    0.0.0.0:*          LISTEN
tcp      0      0 127.0.0.1:1464     0.0.0.0:*          LISTEN
tcp      0      0 127.0.0.1:5432     0.0.0.0:*          LISTEN
tcp      0      0 127.0.0.1:9497     0.0.0.0:*          LISTEN
tcp      0      0 127.0.0.1:42971    0.0.0.0:*          LISTEN
tcp      0      0 127.0.0.1:64668    0.0.0.0:*          LISTEN
tcp      0      0 0.0.0.0:444       0.0.0.0:*          LISTEN
tcp      0      0 127.0.0.1:63551    0.0.0.0:*          LISTEN
tcp      0      0 127.0.0.1:49571    0.0.0.0:*          LISTEN
tcp6     0      0 :::80             :::*               LISTEN
tcp6     0      0 :::443            :::*               LISTEN
udp      0      0 0.0.0.0:123       0.0.0.0:*          LISTEN
udp      0      0 127.0.0.1:323     0.0.0.0:*          LISTEN
udp6     0      0 :::123            :::*               LISTEN
udp6     0      0 :::1:323          :::*               LISTEN
admin >
```

Figura 555 – Command Line Interface – netstat.

[ntpdate]

Utilizado para ajustar a data e a hora local do seu dispositivo consultando servidores *NTP* (*Network Time Protocol*) disponíveis na rede.

Modo de uso:

```
admin >ntpdate -h

/sbin/ntpdate: unknown option -h
usage: /sbin/ntpdate [-46bBdqsu] [-a key#] [-e delay] [-k file] [-p samples] [-o
version#] [-t timeo] [-U username] server ...
admin >
```

Figura 556 – *Command Line Interface* – *ntpdate*.

Exemplo: Atualizar a data e a hora com os servidores *NTP* público:

```
admin >ntpdate a.ntp.br
1 Sep 18:06:33 ntpdate[8569]: adjust time server 200.160.0.8 offset -0.000371 sec
admin >
```

Figura 557 – *Command Line Interface* – *ntpdate* – Exemplo.

[passwd]

Utilizado para definição ou alteração da senha do usuário “admin” padrão do console.

Modo de uso:

```
admin >passwd
Mudando senha para o usuário admin.
Mudando senha para admin.
Senha UNIX (atual):
Nova senha:
Redigite a nova senha:
passwd: todos os tokens de autenticações foram atualizados com sucesso.
admin >
```

Figura 558 – *Command Line Interface* – passwd.

[ping]

Utilizado para testar a conectividade entre dispositivos na rede. Utiliza o datagrama do protocolo *ICMP*.

Modo de uso:

```
admin >ping 192.168.1.99
PING 192.168.1.99 (192.168.1.99) 56(84) bytes of data.
64 bytes from 192.168.1.99: icmp_seq=1 ttl=128 time=2.65 ms
64 bytes from 192.168.1.99: icmp_seq=2 ttl=128 time=1.55 ms
64 bytes from 192.168.1.99: icmp_seq=3 ttl=128 time=6.86 ms
64 bytes from 192.168.1.99: icmp_seq=4 ttl=128 time=4.16 ms
64 bytes from 192.168.1.99: icmp_seq=5 ttl=128 time=16.5 ms
64 bytes from 192.168.1.99: icmp_seq=6 ttl=128 time=1.87 ms
64 bytes from 192.168.1.99: icmp_seq=7 ttl=128 time=4.58 ms
64 bytes from 192.168.1.99: icmp_seq=8 ttl=128 time=2.20 ms
64 bytes from 192.168.1.99: icmp_seq=9 ttl=128 time=1.61 ms
64 bytes from 192.168.1.99: icmp_seq=10 ttl=128 time=3.89 ms
^C
--- 192.168.1.99 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 1.553/4.598/16.589/4.298 ms
admin >
```

Figura 559 – *Command Line Interface – ping.*

[reboot]

Utilizado para reinicializar o sistema.

Modo de uso: [Saída padrão do comando]:

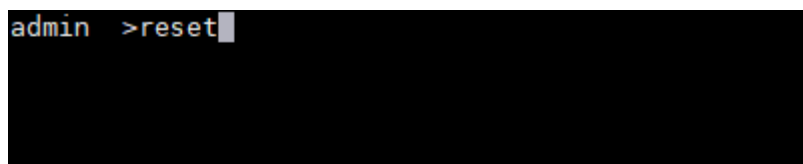
```
admin >reboot  
Connection to 192.168.1.1 closed by remote host.  
Connection to 192.168.1.1 closed.
```

Figura 560 – *Command Line Interface – reboot.*

[reset]

Utilizado para reresetar o sistema.

Modo de uso:



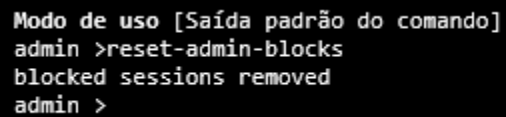
```
admin >reset
```

Figura 561 – *Command Line Interface – reset.*

[reset-admin-blocks]

Utilizado para liberar sessões bloqueadas do usuário “*admin*” da interface *WEB*.

Modo de uso [Saída padrão do comando]:



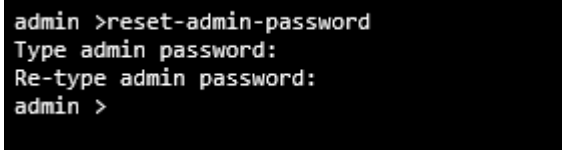
```
Modo de uso [Saída padrão do comando]  
admin >reset-admin-blocks  
blocked sessions removed  
admin >
```

Figura 562 – *Command Line Interface* – *reset-admin-blocks* – Exemplo.

[reset-admin-password]

Utilizado para aplicar um *reset* (anular) na senha do usuário “*admin*” da interface *WEB*. Automaticamente, é solicitada criação de uma nova senha.

Modo de uso: [Saída padrão do comando]:



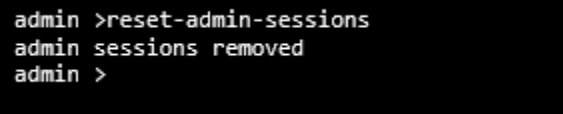
```
admin >reset-admin-password
Type admin password:
Re-type admin password:
admin >
```

Figura 563 – *Command Line Interface* – *reset-admin-password*.

[reset-admin-sessions]

Utilizado para remover as sessões “Ativas” do usuário “admin” da interface *WEB*.

Modo de uso: [Saída padrão do comando]:



```
admin >reset-admin-sessions  
admin sessions removed  
admin >
```

Figura 564 – *Command Line Interface* – *reset-admin-sessions*.

[reset-logs]

Deleta todos os logs do *analyzer*.

Modo de uso:

```
admin >ethtool -h
ethtool version 3.15
Usage:
    ethtool DEVNAME Display standard information about device
    ethtool -s|--change DEVNAME      Change generic options
        [ speed %d ]
        [ duplex half|full ]
        [ port tp|aur|bnc|mii|fibre ]
        [ mdix auto|on|off ]
        [ autoneg on|off ]
        [ advertise %x ]
        [ phyad %d ]
        [ xcvr internal|external ]
        [ wol p|u|m|b|a|g|s|d... ]
        [ sopass %x:%x:%x:%x:%x:%x ]
        [ msglvl %d | msglvl type on|off ... ]
```

Figura 565 – Command Line Interface – *ethtool*.

[rewizard]

Utilizado para aplicar um *reset* (anular) nas configurações do dispositivo BLOCKBIT GSM. Este comando só deve ser usado em casos de real necessidade de reconfiguração total do sistema.

Modo de uso [Saída padrão do comando]:

```
admin >rewizard -d
Do you want to reset this device (y/n)?y
omne-apply-cluster-reset: running
omne-apply-cluster-reset: stop postgres
omne-apply-cluster-reset: remove wizard flag
omne-apply-cluster-reset: remove databases
omne-apply-cluster-reset: remove sessions
omne-apply-cluster-reset: remove known_hosts
omne-apply-cluster-reset: finish
admin >
```

Figura 566 – *Command Line Interface – rewizard.*

[route]

Utilizado para exibir e manipular a tabela de roteamento de endereços IP.

Modo de uso:

```
admin >route -h
Uso: route [-nNvee] [-FC] [famílias_de_endereços] Lista as tabelas de roteamento do kernel
route [-v] [-FC] {add|del|flush} ... Modifica tabela de roteamento da família.

route {-h|--help} [família_de_endereços] Sintaxe para a AF (Família de endereços) especificada.
route {-V|--version} Mostra a versão do comando e sai.

-v, --verbose listagem detalhada
-n, --numeric don't resolve names
-e, --extend mostra outras/mais informações
-F, --fib mostra a Base de Informações de Repasse (default)
-C, --cache mostra cache de roteamento no lugar da FIB

<AF>=Use -4, -6, '-A <af>' or '--<af>'; default: inet
Lista das famílias de endereços possíveis (que suportam roteamento):
inet (DARPA Internet) inet6 (IPv6) ax25 (AX.25 AMPR)
netrom (NET/ROM AMPR) ipx (Novell IPX) ddp (Appletalk DDP)
x25 (CCITT X.25)
admin >
```

Figura 567 – Command Line Interface – route.



Rotas estáticas adicionadas através da console CLI (linha de comando) não são salvas e não são carregadas após o boot.

Exemplo 1.: [Saída padrão do comando]:

```
admin >route -n
Tabela de Roteamento IP do Kernel
Destino      Roteador      MáscaraGen.    Opções Métrica Ref  Uso Iface
0.0.0.0      192.168.0.1   0.0.0.0        UG      0      0      0 eth1
192.168.0.0  0.0.0.0       255.255.255.0  U      0      0      0 eth1
192.168.1.0  0.0.0.0       255.255.255.0  U      0      0      0 eth0
admin >
```

Figura 568 – Command Line Interface – route – Exemplo 1.

Exemplo 2: Configurando um roteamento estático para uma rede estendida:

```
admin >route add -net 192.168.254.0/24 gw 172.16.102.1 dev eth3
admin >
admin >route -n
Tabela de Roteamento IP do Kernel
Destino      Roteador      MáscaraGen.    Opções Métrica Ref  Uso Iface
0.0.0.0      192.168.0.1   0.0.0.0        UG      0      0      0 eth1
172.16.102.0 0.0.0.0       255.255.255.0  U      0      0      0 eth3
192.168.0.0   0.0.0.0       255.255.255.0  U      0      0      0 eth1
192.168.1.0   0.0.0.0       255.255.255.0  U      0      0      0 eth0
192.168.254.0 172.16.102.1  255.255.255.0  UG      0      0      0 eth3
admin >
```

Figura 569 – Command Line Interface – route – Exemplo 2.

[sar]

Utilizado para exibir os relatórios de atividades do sistema.

Modo de uso:

```
admin >sar
Linux 3.10.0-229.20.1.el7.x86_64 (host.blockbit.com) 11/22/18 _x86_64_ (4 CPU)

00:00:01      CPU      %user      %nice      %system      %iowait      %steal      %idle
00:10:01      all        1.45        0.00        0.98        0.06        0.00      97.51
00:20:01      all        1.44        0.00        0.97        0.01        0.00      97.58
00:30:01      all        1.44        0.00        0.99        0.11        0.00      97.46
00:40:01      all        1.41        0.00        1.01        0.03        0.00      97.55
00:50:01      all        1.39        0.00        0.96        0.01        0.00      97.65
01:00:01      all        1.41        0.00        0.96        0.01        0.00      97.63
01:10:01      all        1.12        0.00        0.77        0.01        0.00      98.10
01:20:01      all        1.44        0.00        1.04        0.01        0.00      97.51
01:30:01      all        1.42        0.00        1.01        0.01        0.00      97.56
01:40:01      all        1.49        0.00        1.03        0.01        0.00      97.47
01:50:01      all        1.50        0.00        1.03        0.01        0.00      97.47
02:00:01      all        1.39        0.00        0.98        0.15        0.00      97.48
02:10:01      all        1.40        0.00        0.98        0.04        0.00      97.58
02:20:01      all        1.43        0.00        0.97        0.01        0.00      97.60
02:30:01      all        1.36        0.00        0.94        0.01        0.00      97.70
02:40:01      all        1.39        0.00        0.95        0.01        0.00      97.65
02:50:02      all        1.39        0.00        0.97        0.01        0.00      97.64
03:00:01      all        1.43        0.00        0.99        0.01        0.00      97.58
03:10:01      all        1.43        0.00        1.00        0.01        0.00      97.56
03:20:01      all        1.49        0.00        1.07        0.01        0.00      97.43
03:30:01      all        1.45        0.00        1.02        0.01        0.00      97.52
03:40:01      all        1.37        0.00        0.95        0.01        0.00      97.66
03:50:01      all        1.32        0.00        0.94        0.03        0.00      97.71
04:00:01      all        1.49        0.00        1.09        0.02        0.00      97.39
04:10:01      all        1.46        0.00        1.02        0.01        0.00      97.51
04:20:01      all        1.45        0.00        1.04        0.02        0.00      97.49
04:30:01      all        1.42        0.00        0.97        0.03        0.00      97.58
04:40:01      all        1.42        0.00        0.98        0.01        0.00      97.59
04:50:01      all        1.39        0.00        0.97        0.01        0.00      97.63
05:00:01      all        1.43        0.00        1.00        0.01        0.00      97.57
05:10:01      all        1.47        0.00        1.05        0.01        0.00      97.47
05:20:01      all        1.49        0.00        1.10        0.01        0.00      97.40
05:30:01      all        1.49        0.00        1.06        0.09        0.00      97.35
05:40:01      all        1.46        0.00        1.05        0.04        0.00      97.44
05:50:01      all        1.46        0.00        1.03        0.01        0.00      97.51
06:00:01      all        1.46        0.00        1.03        0.01        0.00      97.50

06:00:01      CPU      %user      %nice      %system      %iowait      %steal      %idle
06:10:01      all        1.43        0.00        1.03        0.01        0.00      97.53
06:20:01      all        1.43        0.00        0.98        0.01        0.00      97.59
06:30:02      all        1.45        0.00        1.01        0.01        0.00      97.53
06:40:01      all        1.38        0.00        0.94        0.01        0.00      97.68
06:50:01      all        1.21        0.00        0.85        0.01        0.00      97.93
07:00:01      all        1.41        0.00        1.02        0.01        0.00      97.57
07:10:01      all        0.98        0.00        0.68        0.01        0.00      98.33
07:20:01      all        1.41        0.00        1.03        0.01        0.00      97.55
07:30:01      all        1.44        0.00        0.97        0.01        0.00      97.59
07:40:01      all        1.42        0.00        0.98        0.01        0.00      97.59
07:50:01      all        1.38        0.00        0.94        0.01        0.00      97.66
08:00:01      all        1.41        0.00        0.95        0.01        0.00      97.63
08:10:01      all        1.40        0.00        0.95        0.01        0.00      97.64
08:20:01      all        1.42        0.00        0.97        0.01        0.00      97.60
08:30:01      all        1.42        0.00        0.98        0.07        0.00      97.53
08:40:01      all        1.43        0.00        1.00        0.07        0.00      97.50
08:50:01      all        1.43        0.00        0.98        0.01        0.00      97.58
09:00:01      all        1.45        0.00        1.00        0.01        0.00      97.55
09:10:01      all        1.45        0.00        1.03        0.01        0.00      97.52
09:20:01      all        1.48        0.00        1.03        0.01        0.00      97.48
09:30:01      all        1.49        0.00        1.07        0.01        0.00      97.43
09:40:01      all        1.49        0.00        1.03        0.01        0.00      97.47
Average:      all        1.41        0.00        0.99        0.02        0.00      97.58
admin >
```

Figura 570 – Command Line Interface – sar.

[set-network-dns]

Configura o endereço *DNS* no servidor.

Modo de uso:

```
admin >ethtool -h
ethtool version 3.15
Usage:
    ethtool DEVNAME Display standard information about device
    ethtool -s|--change DEVNAME      Change generic options
        [ speed %d ]
        [ duplex half|full ]
        [ port tp|aur|bnc|mii|fibre ]
        [ mdix auto|on|off ]
        [ autoneg on|off ]
        [ advertise %x ]
        [ phyad %d ]
        [ xcvr internal|external ]
        [ wol p|u|m|b|a|g|s|d... ]
        [ sopass %x:%x:%x:%x:%x:%x ]
        [ msglvl %d | msglvl type on|off ... ]
```

Figura 571 – Command Line Interface – *ethtool*.

[set-network-gateway]

Utilizado para definir o *gateway* da rede.

Modo de uso:

```
admin >set-network-gateway 172.31.0.1  
admin >
```

Figura 572 – *Command Line Interface – set-network-gateway.*

[set-network-hostname]

Este comando tem como função, permitir que o usuário administrador defina o *hostname* do sistema através da CLI.

```
admin >set-network-hostname -h
hostnamectl [OPTIONS...] COMMAND ...

Query or change system hostname.

-h --help                Show this help
--version                Show package version
--no-ask-password        Do not prompt for password
-H --host=[USER@]HOST    Operate on remote host
-M --machine=CONTAINER  Operate on local container
--transient               Only set transient hostname
--static                 Only set static hostname
--pretty                 Only set pretty hostname

Commands:
status                  Show current hostname settings
set-hostname NAME       Set system hostname
set-icon-name NAME       Set icon name for host
set-chassis NAME         Set chassis type for host
set-deployment NAME     Set deployment environment for host
set-location NAME        Set location for host
admin >
```

Command Line Interface – set-network-hostname

Modo de uso:

Para definir o hostname, basta digitar o comando e adicionar o nome desejado, conforme demonstrado à seguir:

```
admin >set-network-hostname test
admin >
```

Command Line Interface – set-network-hostname - Exemplo

Caso o dispositivo seja do tipo Manager, o comando irá aplicar as informações de hostname de modo que ela apareça ao acessar a interface localizada no campo Hostname em [System na aba "General"](#). Segue um exemplo abaixo:

System

[General](#) [License](#) [Updates](#) [Backups](#) [Storages](#) [High Availability](#)

Settings 

Hostname

test

Domain

blockbit.com

Timezone

America/Sao_Paulo - Brazil (southeast: GO, DF, MG, ES, RJ, SP, PR, SC, RS) 

*** Language**

Portuguese 

Settings - System - General

Além disso, é possível rodar o comando `hostname`, como demonstrado abaixo:

```
admin >hostname  
test
```

Command Line Interface – hostname

Caso o dispositivo seja do tipo Logger, o comando aplicará as informações de hostname somente no Sistema Operacional.

[set-network-interface]

Configura a interface de rede do *logger*.

Modo de uso:

```
admin >ethtool -h
ethtool version 3.15
Usage:
    ethtool DEVNAME Display standard information about device
    ethtool -s|--change DEVNAME      Change generic options
        [ speed %d ]
        [ duplex half|full ]
        [ port tp|aur|bnc|mii|fibre ]
        [ mdix auto|on|off ]
        [ autoneg on|off ]
        [ advertise %x ]
        [ phyad %d ]
        [ xcvr internal|external ]
        [ wol p|u|m|b|a|g|s|d... ]
        [ sopass %x:%x:%x:%x:%x:%x ]
        [ msglvl %d | msglvl type on|off ... ]
```

Figura 573 – Command Line Interface – *ethtool*.

[set-network-timezone]

Utilizado para determinar o *timezone* da rede.

Modo de uso:

```
admin >set-network-timezone America/Sao_Paulo  
admin >
```

Figura 574 – *Command Line Interface* – *set-network-timezone*.

[show-devices]

Exibe uma listagem com o nome e *ID* de todas as devices cadastradas no GSM.

Modo de uso:

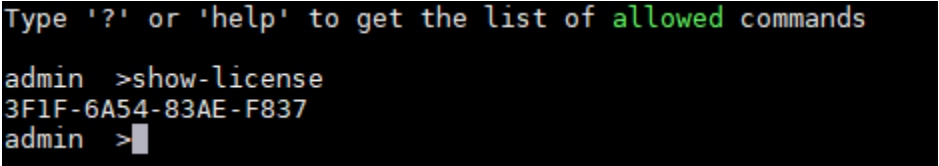
```
admin >show-devices
Device Name: '172.31.208.13'; Device ID: '6384'
Device Name: '172.31.208.14'; Device ID: '18655'
Device Name: '172.31.208.66'; Device ID: '1940'
Device Name: '172.31.208.12'; Device ID: '55754'
Device Name: '172.31.208.140'; Device ID: '54942'
Device Name: '172.31.208.80'; Device ID: '25916'
Device Name: 'UTM QA - 172.16.100.5'; Device ID: '64403'
Device Name: 'UTM MASTER'; Device ID: '6704'
admin >
```

Figura 575 – *Command Line Interface – show-devices.*

[show-license]

Exibe informações a respeito da licença.

Modo de uso:



```
Type '?' or 'help' to get the list of allowed commands  
admin >show-license  
3F1F-6A54-83AE-F837  
admin >
```

Figura 943 - *Command Line Interface – show-license.*

[show-uuid]

Utilizado para exibir o número de identificação do Blockbit GSM. Esse *ID* é utilizado na identificação do *hardware* para validação da licença de uso.

Modo de uso: [Saída padrão do comando]:

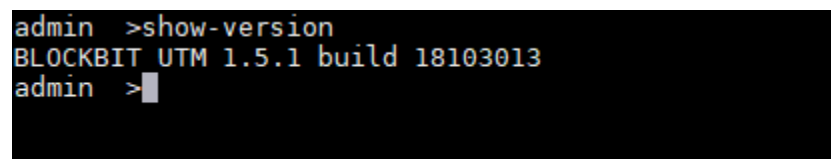
```
admin >show-uuid  
BlockBit Network Appliance UUID  
94248368-3E53-11E6-AE26-EDD8677A1442  
admin >
```

Figura 576 – *Command Line Interface – show-uuid.*

[show-version]

Comando para obter informações da versão.

Modo de uso:



```
admin >show-version  
BLOCKBIT UTM 1.5.1 build 18103013  
admin >
```

Figura 946 - *Command Line Interface – show-version.*

[shutdown]

Utilizado para desligar o sistema.

Modo de uso [Saída padrão do comando]:

```
admin >shutdown -h  
Connection to 192.168.1.1 closed by remote host.  
Connection to 192.168.1.1 closed.
```

Figura 577 – *Command Line Interface – shutdown.*

[tcpdump]

Utilizado para monitorar, capturar e analisar pacotes que estão sendo transmitidos através da rede. Assim, ela permite ao administrador analisar o comportamento da rede, auxiliando na identificação de problemas, estações infectadas, tráfego malicioso, gargalos, etc.

Modo de uso:

```
admin >tcpdump -h
tcpdump version 4.5.1
libpcap version 1.5.3
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqRStuUvxxX] [-B size] [-c count]
               [-C file_size] [-E algo:secret] [-F file] [-G seconds]
               [-i interface] [-j timestamp] [-M secret]
               [-P in|out|inout]
               [-r file] [-s snaplen] [-T type] [-V file] [-w file]
               [-W filecount] [-y datalinktype] [-z command]
               [-Z user] [expression]

admin >
```

Figura 578 – Command Line Interface – tcpdump.

Exemplo: Monitorar todo o tráfego da interface da rede local – interface *Eth0*:

```
admin >tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
20:35:53.129859 IP 172.16.12.80.58139 > utm.ssh: Flags [.], ack 220346669, win 53006,
length 0
20:35:53.133304 IP 172.16.12.144.36793 > 13.68.106.67.26886: UDP, length 182
20:35:53.142155 IP utm.ssh > 172.16.12.80.58139: Flags [P.], seq 1:189, ack 0, win
21, length 188
20:35:53.142216 IP utm.ssh > 172.16.12.80.58139: Flags [P.], seq 189:225, ack 0, win
21, length 36
20:35:53.142419 IP 172.16.12.80.58139 > utm.ssh: Flags [.], ack 225, win 52950,
length 0
20:35:53.144878 IP utm.28489 > 172.16.13.245.domain: 49669+ PTR? 80.12.16.172.in-
addr.arpa. (43)
20:35:53.145312 IP 172.16.13.245.58067 > google-public-dns-a.google.com.domain:
12406+ [1au] PTR? 80.12.16.172.in-addr.arpa. (54)
20:35:53.151967 IP 172.16.12.144.36793 > 13.68.106.67.26886: UDP, length 182
20:35:53.158607 IP google-public-dns-a.google.com.domain > 172.16.13.245.58067: 12406
NXDomain 0/0/1 (54)
20:35:53.158889 IP 172.16.13.245.domain > utm.28489: 49669 NXDomain 0/0/0 (43)
Admin >
```

Figura 579 – Command Line Interface – tcpdump – Exemplo.

[tcptop]

Utilizado para extrair e exibir informações de tráfego das interfaces de rede, tais como: total de pacotes capturados, total de pacotes recebidos, total de pacotes bloqueados pelo *kernel* e o total de pacotes trafegados pelo TOP 10 endereços *IP*.

Modo de uso:

```
Modo de uso
admin >tcptop
you must specify the interface: [eth0,eth1 ...]
admin >
```

Figura 580 – Command Line Interface – *tcptop*.

Exemplo: Exibir informações de tráfego top 10 da interface *eth1*:

```
admin >tcptop eth1
Wait capturing frames ...
tcpdump: WARNING: eth1: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
10000 packets captured
10070 packets received by filter
21 packets dropped by kernel
 3268 IP 177.185.5.137
 3090 IP 192.168.0.2
 1626 IP 192.168.3.2
  481 IP 201.86.139.109
  290 IP 8.8.8.8 > 192
  288 IP 192.168.3.2 > 8
  246 IP 201.31.172.3
admin >
```

Figura 581 – Command Line Interface – *tcptop* – Exemplo.

[telnet]

Utilizado para acesso remoto e testes de simulação de um terminal. Pode ser utilizado para teste de resposta de conexão de um serviço e até testes de envio de uma mensagem de *e-mail*.

Modo de uso:

```
admin >telnet -h
telnet: invalid option -- 'h'
Usage: telnet [-8] [-E] [-L] [-S tos] [-a] [-c] [-d] [-e char] [-l user]
        [-n tracefile] [-b hostalias ] [-r]
        [host-name [port]]
admin >
```

Figura 582 – Command Line Interface – telnet.

Exemplo: [Saída padrão do comando]:

```
admin >telnet
telnet> ?
Commands may be abbreviated.  Commands are:

close          close current connection
logout         forcibly logout remote user and close the connection
display        display operating parameters
mode           try to enter line or character mode ('mode ?' for more)
open           connect to a site
quit           exit telnet
send           transmit special characters ('send ?' for more)
set            set operating parameters ('set ?' for more)
unset          unset operating parameters ('unset ?' for more)
status         print status information
toggle         toggle operating parameters ('toggle ?' for more)
slc            change state of special charaters ('slc ?' for more)
z             suspend telnet
!             invoke a subshell
environ        change environment variables ('environ ?' for more)
?             print help information
telnet>
```

Figura 583 – Command Line Interface – telnet – Exemplo.

Exemplo 1: Testes de conexão com um serviço remoto *Ts* (*terminal Service*) em uma porta específica:

```
admin >telnet 172.16.13.245 3389
Trying 172.16.13.245...
Connected to 172.16.13.245.
Escape character is '^['.
```

Figura 584 – Command Line Interface – telnet – Exemplo 1.

Exemplo 2: Testes de conexão com um serviço remoto em uma porta específica com a resposta de falha na conexão:

```
admin >telnet 172.16.102.11 22
Trying 172.16.102.11...
telnet: connect to address 172.16.102.11: Connection timed out
admin >
```

Figura 585 – *Command Line Interface – telnet* – Exemplo 2.

[tracpath]

Utilizado para traçar um caminho para um endereço de rede designado, informando sobre o “tempo de vida ” ou *lag TTL* e a unidade de transmissão máxima (*MTU*) ao longo do caminho.

Modo de uso:

```
admin >tracpath -h
Usage: tracpath [-n] [-b] [-l <len>] [-p port] <destination>
admin >
Exemplo: Testes para traçar o roteamento ou caminho até o end. www.google.com.br
especificando a porta TCP/80 (http).
admin >tracpath -p 3389 172.16.13.245
1?: [LOCALHOST] pmtu 1500
1: 172.16.13.245 0.555ms reached
Resume: pmtu 1500 hops 1 back 128
admin >tracpath -n -b -p 80 www.google.com
1?: [LOCALHOST] pmtu 1500
1: 10.70.64.1 (10.70.64.1) 13.510ms
1: 10.70.64.1 (10.70.64.1) 12.625ms
2: 201.6.37.65 (c9062541.virtua.com.br) 12.592ms
3: 201.6.40.37 (c9062825.virtua.com.br) 11.712ms
4: 201.6.42.93 (c9062a5d.virtua.com.br) 11.800ms
5: no reply
6: no reply
7: no reply
8: no reply
9: no reply
10: no reply
11: no reply
12: no reply
13: no reply
14: no reply
15: no reply
16: no reply
17: no reply
18: no reply
19: no reply
20: no reply
21: no reply
22: no reply
23: no reply
24: no reply
25: no reply
26: no reply
27: no reply
28: no reply
29: no reply
30: no reply
31: no reply
Too many hops: pmtu 1500
Resume: pmtu 1500
admin >
```

Figura 586 – Command Line Interface – tracpath.

Exemplo: Teste para traçar o roteamento ou caminho até o endereço www.google.com.br especificando a porta TCP/80 (http).

[traceroute]

Utilizado para traçar um caminho para um endereço de rede designado. O comando "traceroute" suporta alguns parâmetros avançados que o diferencia do "tracepath", incluindo a seleção de protocolos, como: TCP, UDP, ICMP ou outros.

Modo de uso:

```
admin >traceroute --help
Usage:
  traceroute [ -4dFITnreAUDV ] [ -f first_ttl ] [ -g gate,... ] [ -i device ] [ -m
max_ttl ] [ -N squeries ] [ -p port ] [ -t tos ] [ -l flow_label ] [ -w waittime ] [
-q nqueries ] [ -s src_addr ] [ -z sendwait ] [ --fwmark=num ] host [ packetlen ]

Options:
  -4                      Use IPv4
  -6                      Use IPv6
  -d --debug              Enable socket level debugging
  -F --dont-fragment      Do not fragment packets
  -f first_ttl --first=first_ttl
                          Start from the first_ttl hop (instead from 1)
  -g gate,... --gateway=gate,...
                          Route packets through the specified gateway
                          (maximum 8 for IPv4 and 127 for IPv6)
  -I --icmp               Use ICMP ECHO for tracerouting
  -T --tcp                Use TCP SYN for tracerouting (default port is 80)
  -i device --interface=device
                          Specify a network interface to operate with
  -m max_ttl --max-hops=max_ttl
                          Set the max number of hops (max TTL to be
                          reached). Default is 30
  -N squeries --sim-queries=squeries
                          Set the number of probes to be tried
                          simultaneously (default is 16)
  -n                      Do not resolve IP addresses to their domain names
  -p port --port=port
                          Set the destination port to use. It is either
                          initial udp port value for "default" method
                          (incremented by each probe, default is
                          33434), or initial seq for "icmp" incremented
                          as well, default from 1), or some constant
                          destination port for other methods (with default of 80
                          for "tcp", 53 for "udp", etc.)
```

Figura 587 – Command Line Interface – traceroute_1.

```

-t tos --tos=tos          Set the TOS (IPv4 type of service) or TC (IPv6
                           traffic class) value for outgoing packets
-l flow_label --flowlabel=flow_label
                           Use specified flow_label for IPv6 packets
-w waittime --wait=waittime
                           Set the number of seconds to wait for response
                           to a probe (default is 5.0). Non-integer (float
                           point) values allowed too
-q nqueries --queries=nqueries
                           Set the number of probes per each hop. Default is 3
-r                          Bypass the normal routing and send directly to a
                           host on an attached network
-s src_addr --source=src_addr
                           Use source src_addr for outgoing packets
-z sendwait --sendwait=sendwait
                           Minimal time interval between probes (default 0).
                           If the value is more than 10, then it specifies a
                           number in milliseconds, else it is a number of
                           seconds (float point values allowed too)
-e --extensions           how ICMP extensions (if present), including MPLS
-A --as-path-lookups      Perform AS path lookups in routing registries and
                           print results directly after the corresponding
                           addresses
-M name --module=name     Use specified module (either builtin or external)
                           for traceroute operations. Most methods have
                           their shortcuts (`-I' means `-M icmp' etc.)

-O OPTS,... --options=OPTS,...
                           Use module-specific option OPTS for the

```

Figura 588 – Command Line Interface – traceroute_2.

```

tracert module. Several OPTS allowed,
separated by comma. If OPTS is "help", print
info about available options
--sport=num               Use source port num for outgoing packets.
                           Implies '-N 1'
--fwmark=num              Set firewall mark for outgoing packets
-U --udp                  Use UDP to particular port for tracerouting
                           (instead of increasing the port per each probe),
                           default port is 53
-UL                       Use UDPLITE for tracerouting (default dest port
                           is 53)
-D --dccp                 Use DCCP Request for tracerouting (default port
                           is 33434)
-P prot --protocol=prot   Use raw packet of protocol prot for tracerouting
--mtu                     Discover MTU along the path being traced. Implies
                           '-F -N 1'
--back                    Guess the number of hops in the backward path and
                           print if it differs
-V --version              Print version info and exit
--help                    Read this help and exit

Arguments:
+   host                  The host to traceroute to
    packetlen             The full packet length (default is the length of an IP
                           header plus 40). Can be ignored or increased to a minimal
                           allowed value

admin >

```

Figura 589 – Command Line Interface – traceroute_3.

Exemplo: Testes para traçar o roteamento ou caminho até o endereço IP de DNS do Google, IP 8.8.8.8 no protocolo UDP (17):

```
admin >tracert -n -p 53 -t 17 8.8.8.8
tracert to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  10.70.64.1  15.412 ms  15.242 ms  15.152 ms
 2  201.6.37.65  15.607 ms  15.618 ms  15.566 ms
 3  201.6.40.37  15.511 ms  16.380 ms  21.774 ms
 4  201.6.42.93  22.970 ms  22.917 ms  22.697 ms
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
...
27  * * *
28  * * *
29  * * *
30  * * *
admin >
```

Figura 590 – Command Line Interface – tracert – Exemplo 1.

[update-gsm]

Utilizado para verificação, *download* e instalação dos pacotes de atualização do Blockbit GSM.

Modo de uso [Saída padrão do comando]:

```
admin >update-gsm
Loaded plugins: fastestmirror
Determining fastest mirrors
gsm-apply-update: running
gsm-apply-update: >/etc/yum.repos.d//BlockBit-centos.repo
gsm-apply-update: >/etc/yum.repos.d//BlockBit-epel.repo
gsm-apply-update: >/etc/yum.repos.d//BlockBit-gsm.repo
gsm-apply-update: >/etc/yum.repos.d//BlockBit-bases.repo
gsm-apply-update: >/etc/yum.repos.d//BlockBit-elastic.repo
gsm-apply-update: update system packages
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
bases-local | 2.9 kB 00:00:00
centos-local | 2.9 kB 00:00:00
elastic-local | 2.9 kB 00:00:00
epel-local | 2.9 kB 00:00:00
gsm-local | 2.9 kB 00:00:00
(1/15): bases-local/2.0/x86_64/filelists_db | 24 kB 00:00:01
(2/15): bases-local/2.0/x86_64/primary_db | 43 kB 00:00:01
(3/15): bases-local/2.0/x86_64/other_db | 19 kB 00:00:00
(4/15): centos-local/2.0/x86_64/filelists_db | 370 kB 00:00:04
(5/15): elastic-local/2.0/x86_64/primary_db | 13 kB 00:00:01
(6/15): elastic-local/2.0/x86_64/other_db | 1.1 kB 00:00:00
(7/15): centos-local/2.0/x86_64/primary_db | 857 kB 00:00:06
(8/15): centos-local/2.0/x86_64/other_db | 211 kB 00:00:02
(9/15): elastic-local/2.0/x86_64/filelists_db | 202 kB 00:00:02
(10/15): epel-local/2.0/x86_64/primary_db | 6.9 kB 00:00:00
(11/15): epel-local/2.0/x86_64/filelists_db | 2.9 kB 00:00:01
(12/15): epel-local/2.0/x86_64/other_db | 5.1 kB 00:00:00
(13/15): gsm-local/2.0/x86_64/primary_db | 44 kB 00:00:01
(14/15): gsm-local/2.0/x86_64/other_db | 3.3 kB 00:00:00
(15/15): gsm-local/2.0/x86_64/filelists_db | 1.7 MB 00:00:07
Metadata Cache Created
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
Resolving Dependencies
--> Running transaction check
--> Package atp-blacklist.x86_64 0:202011020812-0.el7.centos will be updated
--> Package atp-blacklist.x86_64 0:202102150811-0.el7.centos will be an update
--> Package atp-geoip.x86_64 0:202011020901-0.el7.centos will be updated
--> Package atp-geoip.x86_64 0:202102150901-0.el7.centos will be an update
--> Package atp-threats.x86_64 0:202011030809-0.el7.centos will be updated
--> Package atp-threats.x86_64 0:202102160809-0.el7.centos will be an update
--> Package bbos-scripts.x86_64 0:2.0.6-80 will be updated
--> Package bbos-scripts.x86_64 0:2.0.7-69 will be an update
--> Package gsm-apply.x86_64 0:2.0.6-80 will be updated
--> Package gsm-apply.x86_64 0:2.0.7-69 will be an update
--> Package gsm-backend.x86_64 0:2.0.6-80 will be updated
--> Package gsm-backend.x86_64 0:2.0.7-69 will be an update
--> Package gsm-console.x86_64 0:2.0.6-80 will be updated
--> Package gsm-console.x86_64 0:2.0.7-69 will be an update
--> Package gsm-manager.x86_64 0:2.0.6-80 will be updated
--> Package gsm-manager.x86_64 0:2.0.7-69 will be an update
--> Package gsm-repos.x86_64 0:2.0.6-80 will be updated
--> Package gsm-repos.x86_64 0:2.0.7-69 will be an update
--> Package gsm-schema.x86_64 0:2.0.6-80 will be updated
--> Package gsm-schema.x86_64 0:2.0.7-69 will be an update
--> Package ips-threats.x86_64 0:202011030809-0.el7.centos will be updated
--> Package ips-threats.x86_64 0:202102160809-0.el7.centos will be an update
--> Package wgs-class.x86_64 0:202010300800-0.el7.centos will be updated
--> Package wgs-class.x86_64 0:202102120800-0.el7.centos will be an update
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package Arch Version Repository Size
=====
Updating:
atp-blacklist x86_64 202102150811-0.el7.centos bases-local 1.2 M
atp-geoip x86_64 202102150901-0.el7.centos bases-local 12 M
atp-threats x86_64 202102160809-0.el7.centos bases-local 2.7 M
bbos-scripts x86_64 2.0.7-69 gsm-local 14 k
gsm-apply x86_64 2.0.7-69 gsm-local 43 k
gsm-backend x86_64 2.0.7-69 gsm-local 65 k
gsm-console x86_64 2.0.7-69 gsm-local 20 k
gsm-manager x86_64 2.0.7-69 gsm-local 76 M
gsm-repos x86_64 2.0.7-69 gsm-local 11 k
gsm-schema x86_64 2.0.7-69 gsm-local 25 k
ips-threats x86_64 202102160809-0.el7.centos bases-local 1.4 M
wgs-class x86_64 202102120800-0.el7.centos bases-local 285 M
=====

Transaction Summary
=====
Upgrade 12 Packages

Total download size: 378 M
Downloading packages:
Delta RPMs disabled because /usr/bin/applydelta.rpm not installed.
warning: /var/cache/yum/x86_64/2.0/bases-local/packages/atp-blacklist-202102150811-0.el7.centos.x86_64.rpm: Header V4 RSA/SHA1 Signature,
key ID b08c6759: NOKEY
Public key for atp-blacklist-202102150811-0.el7.centos.x86_64.rpm is not installed
(1/12): atp-blacklist-202102150811-0.el7.centos.x86_64.rpm | 1.2 MB 00:00:06
Public key for bbos-scripts-2.0.7-69.x86_64.rpm is not installed ] 647 kB/s | 4.0 MB 00:09:52 ETA
(2/12): bbos-scripts-2.0.7-69.x86_64.rpm | 14 kB 00:00:01
(3/12): gsm-apply-2.0.7-69.x86_64.rpm | 43 kB 00:00:01
(4/12): gsm-console-2.0.7-69.x86_64.rpm | 20 kB 00:00:00
(5/12): gsm-backend-2.0.7-69.x86_64.rpm | 65 kB 00:00:01
(6/12): gsm-repos-2.0.7-69.x86_64.rpm | 11 kB 00:00:00
(7/12): gsm-schema-2.0.7-69.x86_64.rpm | 25 kB 00:00:00
(8/12): atp-threats-202102160809-0.el7.centos.x86_64.rpm | 2.7 MB 00:00:05
(9/12): atp-geoip-202102150901-0.el7.centos.x86_64.rpm | 12 MB 00:00:12
(10/12): ips-threats-202102160809-0.el7.centos.x86_64.rpm | 1.4 MB 00:00:03
(11/12): gsm-manager-2.0.7-69.x86_64.rpm | 76 MB 00:00:25
(12/12): wgs-class-202102120800-0.el7.centos.x86_64.rpm | 285 MB 00:01:05
-----
Total | 4.9 MB/s | 378 MB 00:01:17
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-BlockBit
Importing GPG key 0XB08C6759:
```



O screenshot acima não representa a saída do comando em sua totalidade. O comando irá liberar o console ao finalizar e exibirá a mensagem "gsm-apply-update: finish", para validar se a atualização foi feita corretamente, utilize o comando [show-version](#).

[update-license]

Utilizado para efetuar o registro do Blockbit UTM através da CLI. A licença precisa ser digitada na frente do comando. O **[update-license]** deve ser utilizado apenas caso a licença estiver desativada e liberada pela Blockbit para ativação, é extremamente importante ter em mente que: Caso esse comando seja executado quando a licença já estiver devidamente ativada ela irá ser DESATIVADA.

Modo de uso:

```
admin >update-license 3F1F-6A54-83AE-F837
status:true
admin >
```

Figura 967 - Command Line Interface – update-license.



Atenção para a utilização adequada do comando [update-license]: Se o comando for efetuado duas vezes, ou caso ele seja executado quando a licença estiver ativa, ela será DESATIVADA. Além disso, para a utilização correta deste comando é necessário que esta mesma esteja liberada para poder registrá-la corretamente.

[upgrade-blockbit]

Este comando é utilizado para efetuar verificação, download e upgrade do Blockbit UTM para a versão mais atual.



ATENÇÃO: Recomendamos SEMPRE que seja feito um BACKUP COMPLETO da última versão sistema e dos relatórios antes da execução de qualquer procedimento de *update* ou *upgrade* e que os arquivos sejam salvos em um lugar seguro.



O processo de *upgrade* interfere com as interfaces configuradas em *loggers* do tipo *standalone*. Portanto, caso o ambiente do usuário possua um logger *standalone* usando uma interface diferente da *eth0*, após o processo de upgrade, será necessário fazer a edição e alterar a interface de modo que não haja nenhum tipo de problema de redirecionamento futuro.

Ao rodar o comando, o sistema requisitará que usuário confirme que todos os relatórios foram exportados e que um backup do sistema foi gerado. Para que o comando seja executado, será necessário essa confirmação dupla do usuário.



ATENÇÃO: Ao finalizar a execução deste comando, será necessário reiniciar o seu GSM.

Modo de uso:

```
admin >upgrade-blockbit
Are you sure do you want upgrade version 2.0 to 2.1 (restart system is required)? [y/N]y
Have you export all reports? [y/N]y
Have you made a full system backup? [y/N]y

Testing connection to update server:
Connection succeeded

will restart when the upgrade is complete
Upgrading...

- No SSL mode enabled
- Downloading packages
Checking for license...
Checking for available upgrade...
Downloading kernel upgrade...
##### 100.0%
Kernel upgrade downloaded
Kernel upgrade downloaded. Installing...
Checking environment...
Preparing environment...
Environment ok.
Testing installer integrity...
Installer integrity ok.
Unpacking installer...
Installer unpacked.
Running installer...
Finding installation disk...
Mounting installation disk
Installing new kernel files. It will take a while...
Installing new initramfs...
Setting new kernel as bootable...
Cleaning up old entries...
New kernel installed!
Kernel upgraded from 3.10.0-957.10.1 to 5.8.8-1
A reboot is required.
```

Command Line Interface – upgrade-blockbit

[uptime]

Exibe durante quanto tempo que o servidor está em operação.

Modo de uso:

```
admin >uptime
09:57:34 up 16:43, 1 user, load average: 0.00, 0.01, 0.05
admin >█
```

Figura 592 – *Command Line Interface – uptime.*

[vmstat]

Utilizado para relatar informações sobre processos, memória, paginação, I/O de blocos e atividades da CPU.

Modo de uso:

```
admin >vmstat --help

Usage:
  vmstat [options] [delay [count]]

Options:
  -a, --active           active/inactive memory
  -f, --forks            number of forks since boot
  -m, --slabs            slabinfo
  -n, --one-header       do not redisplay header
  -s, --stats            event counter statistics
  -d, --disk             disk statistics
  -D, --disk-sum         summarize disk statistics
  -p, --partition <dev> partition specific statistics
  -S, --unit <char>     define display unit
  -w, --wide             wide output
  -t, --timestamp        show timestamp

  -h, --help             display this help and exit
  -V, --version          output version information and exit

For more details see vmstat(8).
admin >
```

Figura 593 – Command Line Interface – vmstat.

Exemplo: Saída padrão do comando:

```
admin >vmstat
procs -----memory----- ---swap-- -----io----- -system-- -----cpu-----
r b  swpd  free  buff  cache  si  so   bi   bo   in  cs us sy id wa st
1 0   86316 178524 7820 3685772 0 0    1    9    5   7 1 1 98 0 0
```

Figura 594 – Command Line Interface – vmstat - Exemplo.

[whois]

Utilizado para consultar a informação sobre um domínio de *Internet*.

Modo de uso:

```
admin >whois
Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST    connect to server HOST
-p PORT, --port PORT    connect to PORT
-H                      hide legal disclaimers
                        --verbose    explain what is being done
                        --help      display this help and exit
                        --version    output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-l          find the one level less specific match
-L          find all levels less specific matches
-m          find all one level more specific matches
-M          find all levels of more specific matches
-c          find the smallest match containing a mnt-irt attribute
-x          exact match
-b          return brief IP address ranges with abuse contact
-B          turn off object filtering (show email addresses)
-G          turn off grouping of associated objects
-d          return DNS reverse delegation objects too
-i ATTR[,ATTR]...    do an inverse look-up for specified ATTRIBUTES
-T TYPE[,TYPE]...    only look for objects of TYPE
-K          only primary keys are returned
-r          turn off recursive look-ups for contact information
-R          force to show local copy of the domain object even
              if it contains referral
-a          also search all the mirrored databases
-s SOURCE[,SOURCE]... search the database mirrored from SOURCE
-g SOURCE:FIRST-LAST find updates from SOURCE from serial FIRST to LAST
-t TYPE      request template for object of TYPE
-v TYPE      request verbose template for object of TYPE
-q [version|sources|types] query specified server info
admin >
```

Figura 595 – Command Line Interface – whois.

Exemplo: Saída padrão do comando:



 www.blockbit.com

Blockbit GSM versão 2.4.0

Release Notes

27/02/2023

Implementações realizadas no GSM 2.4.0:

- O envio de [relatórios](#) gerados pelo analyzer por e-mail foi implementado.
- Implementado suporte a [CGNAT](#) (Carrier Grade Network Address Translator).
- Implementado [Filtro Anti-Spam](#).
- Implementada a exibição de Top 10 usuários por aplicação na forma de [Dashboard](#) em Monitor > Dashboard.

A tabela a seguir lista as melhorias realizadas no lançamento do Blockbit GSM 2.4.0:

Código	Descrição
20509	Correção feita na busca de Top Categorias no Web Filter (Analyzer e Dashboard).
20730	
20732	
18153	Correção feita no Firewall ao salvar um Template.
18223	Correção feita no Firewall ao alterar um Template.
18224	Correção feita na tela de configuração de Templates.
18225	Correção feita na clonagem de Templates.
18286	Correção feita no ícone "monitor" que acessa o NGFW.
18287	Correção feita no acesso remoto a um NGFW.
18449	Correção feita na exibição das opções clone e delete, disponível mesmo sem a seleção do item, em Device Templates.
20732	Correção feita na caixa de pesquisa do Web Filter Top Categorias.
20734	Melhoria feita nas configurações de geração de relatórios em horários pré-determinados.
24125	Correção feita nas Permissões ACL.
24270	Melhoria feita na exibição de logs, em grupos contendo um Device, em Devices > Inventory.
24955	Melhoria feita na aplicação de Políticas a um NGFW.
25841	Correção feita no acesso da tela "Dashboard".
26863	Melhoria feita na gravação de configurações em Device Templates.
29325	Correção feita na validação de políticas em "Gerenciador de Políticas".
29584	Correção feita na criação de perfil SD-WAN em Device Template.
29587	Correção feita ao criar perfil de Intrusion Prevention (IPS) em Device Template.
29675	Correção feita ao criar Query em Eventos.
29852	Correção feita ao realizar deploy de Device Template clonado.
33769	Correção feita nos relatórios CSV.
34815	Correção feita no timestamp de relatórios (.csv) do tipo <i>log sessions</i> .
34853	Correção feita no disparo de e-mails sem marcação de checkbox.