Blockbit

Resource Center

Documentação

Blockbit Client

O Blockbit Client é uma aplicação cliente/servidor integrado ao Windows que serve tanta na autenticação do usuário para o serviço de *"Firewall"* como para outros recursos de conexão remota do tipo: *"VPN IPSEC"* ou *"VPN SSL"*.

Ele é a versão melhorada do Blockbit Agent e possui inúmeros novos recursos para facilitar o acesso à VPNs, entre eles:

- Configuração de múltiplos perfis de conexão;
- Importação e exportação destes perfis para facilitar possíveis implementações futuras;
- Exportação de *logs* do perfil de conexão;
- E muito mais, confira todas as novidades, nesta página.

 *O Blockbit Client está homologado para as versões MS-Windows 7+ Superiores.*

Nesta sessão vamos analisar os seguintes tópicos:

- Comparativo das versões anteriores;
- Requisitos mínimos, verificação do ambiente, download e instalação do *Blockbit Client;*
- Configuração do *Blockbit Client*;
- Como efetuar uma conexão usando Blockbit Client;
- Como acessar os logs do Blockbit Client no *event viewer* do *Windows*.

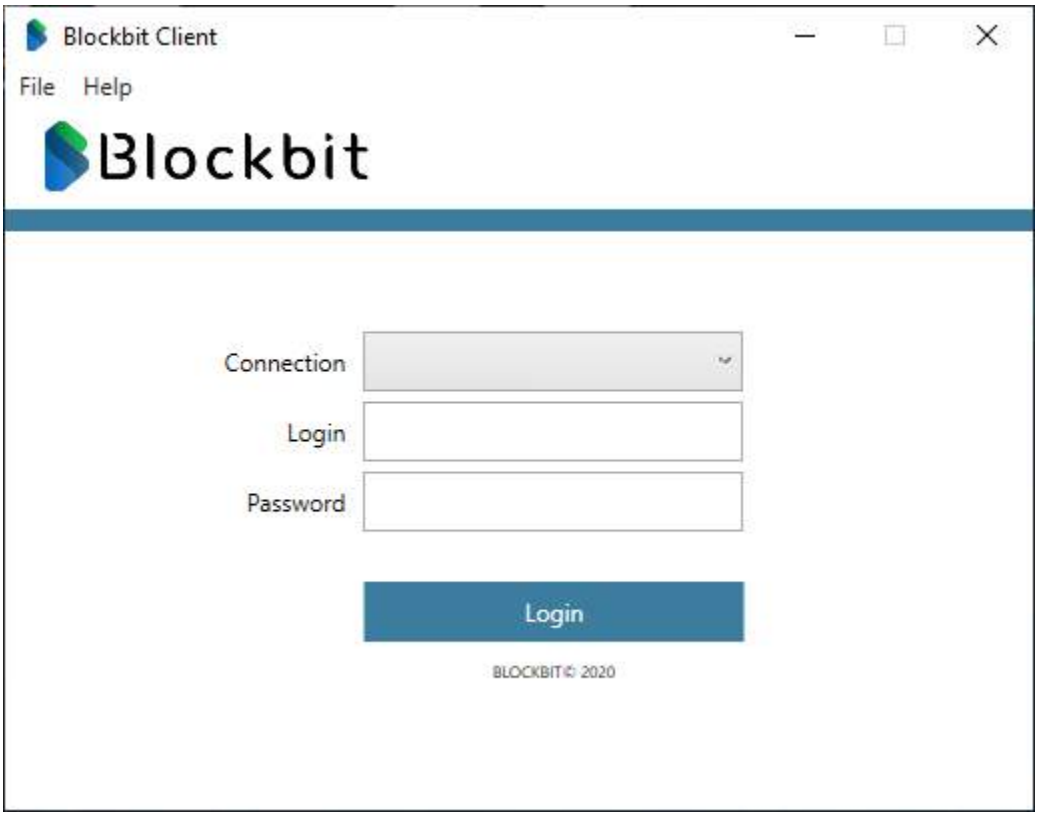
Para fazer *download* do Blockbit Client acesse o portal de autenticação (através do endereço *IP* ou *hostname* do seu UTM através da porta 9803) e clique em **[** 

]. Para mais informações, consulte esta página.

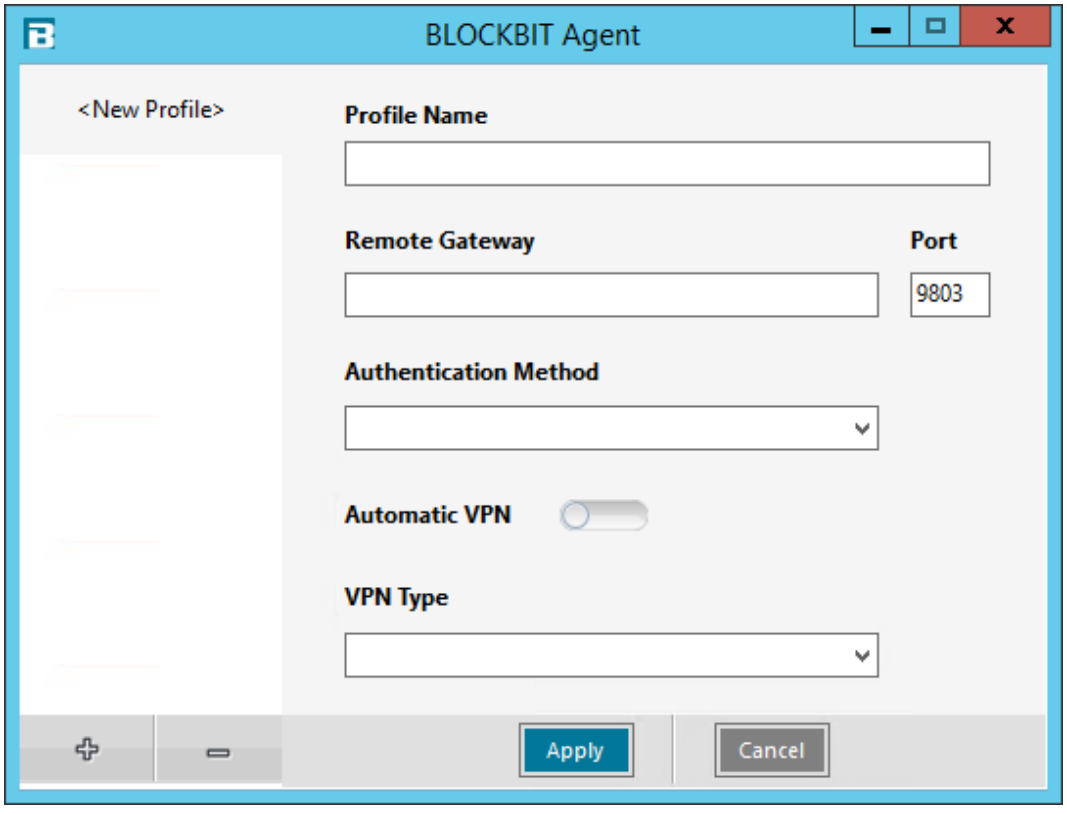
Comparativo das versões anteriores

O Blockbit Client é a versão melhorada do antigo Blockbit Agent, ele possui diversas melhorias que aprimoraram consideravelmente a sua funcionalidade. Segue abaixo uma sequência de screenshots comparativos entre as duas versões para exibir as novas features.

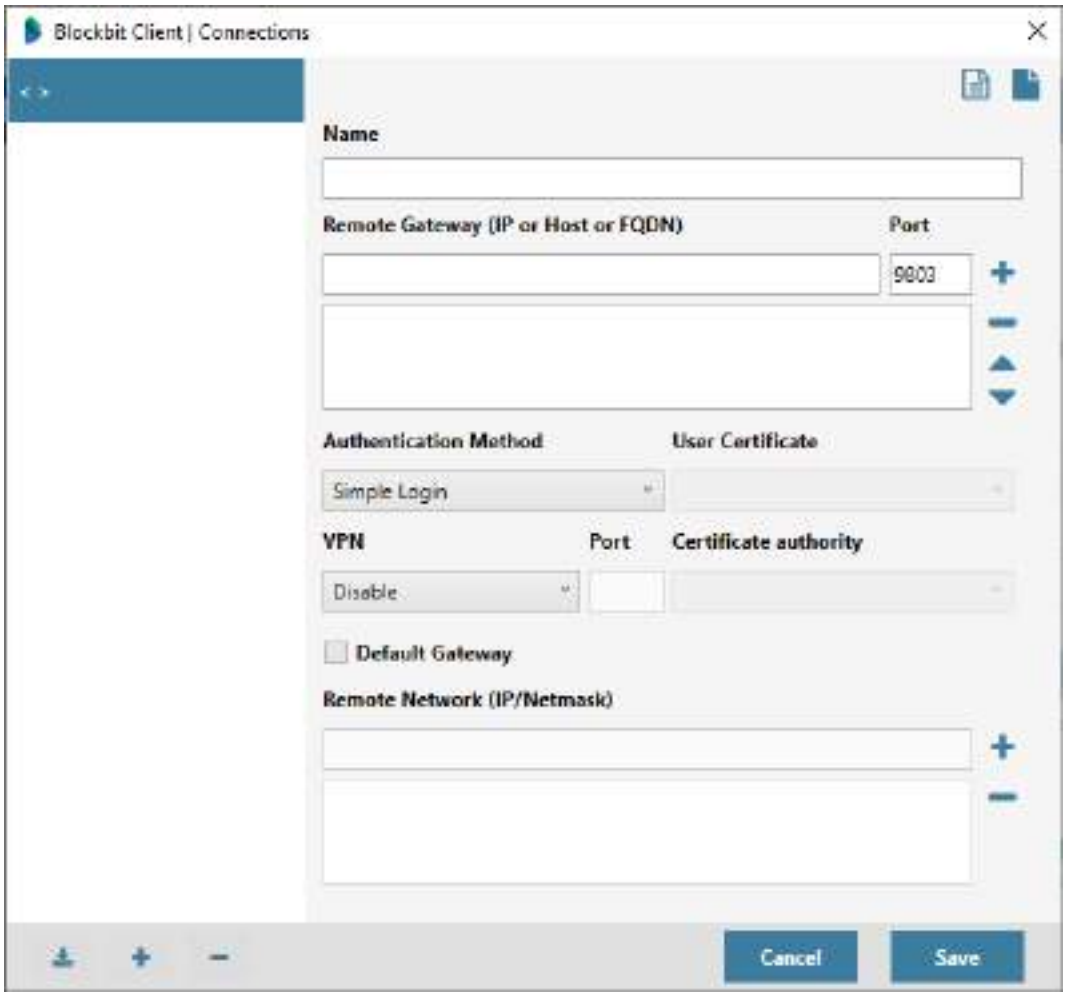
Blockbit Agent - Tela principal



Blockbit Client - Tela principal



Blockbit Agent - *New Profile*



Blockbit Client- *New Profile*

Nesta sessão iremos relacionar as novidades e *features* que foram desenvolvidas nesta versão:

- Esta versão possibilita importar um perfil de conexão automaticamente no momento da instalação (o que permite que o Administrador da Rede distribua o instalador já pré-configurado para os usuários);
- Houve mellhorias no fluxo de conexão, nesta versão, o aplicativo de VPN para estabelece a conexão VPN no endereço público e estabelece a autenticação Firewall no endereço virtual (VPN);
- O Blockbit Client agora possibilita a configuração de endereços de Gateway Remoto secundários, aprimorando a disponibilidade do serviço (o serviço de conexão VPN (IPSEC ou SSL) tenta conectar no endereço secundário caso não consiga estabelecer a conexão pelo Primário);
- Suporta à rotas estáticas configuradas no Client;
- Os menus foram reestruturados e o *design* foi melhorado (atualização no ícone, logotipo e *layout*);
- O serviço de autenticação do Blockbit Client possui suporte a *keepalive*, o que descontinua a dependência ao serviço de notificação do UTM;
- As mensagens de notificações do serviço de conexão *VPN* e autenticação *Firewall* foram revisadas e melhoradas;
- A opção de desabilitar a *VPN* antes ou depois de conectar em um perfil foi removida;
- O gerenciamento de importação de certificados foi removido, nesta versão a importação de certificados digitais é feita diretamente pela ferramenta nativa do *Windows*;
- Suporte à internacionalização, o Blockbit Client adota o idioma utilizado na instalação (Inglês e Português);
- Melhoria na performance ao tentar conectar em um *Gateway* Inacessível;
- Aplicativo e *drive* de interface *TAP* agora é assinado com certificado digital *Authenticode* emitido pela Blockbit;
- O Blockbit Client agora permite estabelecer uma conexão VPN IPSEC utilizando o método de autenticação tanto "*Login* Simples (*Login* e Senha)" como "*Login* Simples com Certificado Digital";
- Em caso de *troubleshooting*, o Blockbit Client agora possibilita exportar *logs* de conexão VPN em arquivo texto, exibindo informações:
    - Eventos de Autenticação *Firewall*;
    - Eventos de *VPN IPSEC*;
    - Eventos de *VPN SSL*.
- O Blockbit Client possui a opção de ativar o recurso *split tunneling* de *VPN*, permitindo que o usuário direcione parte do tráfego de seu dispositivo através da VPN enquanto outros aplicativos mantêm acesso direto à Internet.

Para mais informações a respeito de como fazer *download* e instalação do Blockbit Client, acesse esta página.

Instalação Blockbit Client

Nesta sessão vamos apresentar um passo a passo desde o download até a conclusão da instalação do Blockbit Client.

- *Requisitos Mínimos*;
- *Verificação do Ambiente para Instalação do Blockbit Client*;
- *Processo de Download*;
- *Guia de Instalação;*
- *Configuração da VPN SSL*.

Requisitos mínimos

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

Requisitos mínimos de instalação:

- .NET Framework versão 4.6;
- MS-Windows 7+ Superiores.

O Client está homologado apenas para as versões MS-Windows 7+ Superiores.

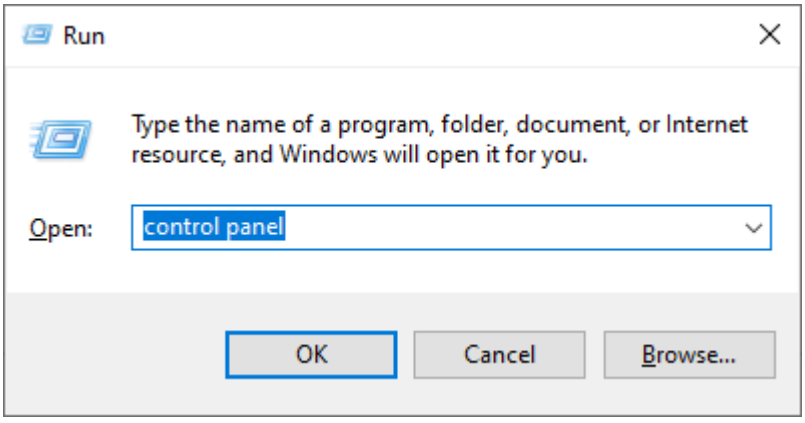
A seguir, vamos confirmar se o ambiente está preparado para instalação do Blockbit *Client*.

Verificação do Ambiente para Instalação do Blockbit Client

Para o funcionamento do Blockbit *Client* e integração com o serviço de notificações e eventos do *Windows*, o sistema requer a instalação e habilitação do aplicativo **.NET *Framework* versão 4.6** nas estações de trabalho *Windows*.

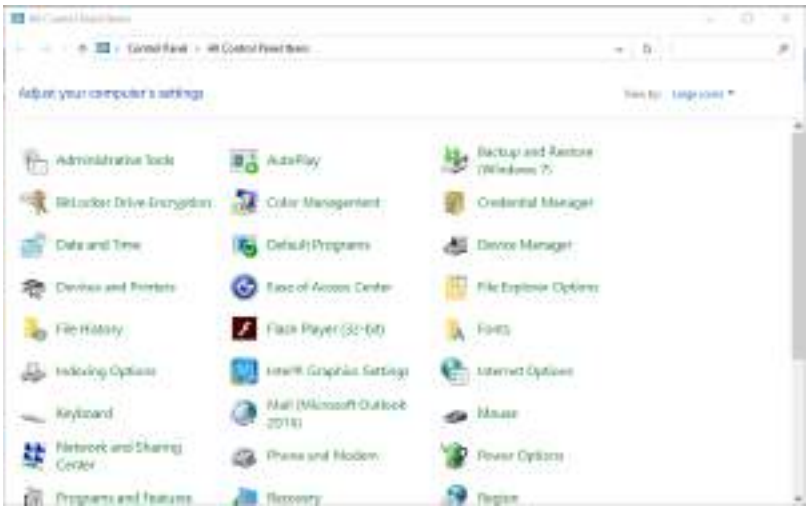
Para instalação do aplicativo **.NET versão 4.6,** siga os passos à seguir:

Digite o comando ***Windows* + *R***, ou selecione "Executar" no seu *Menu* Iniciar, a janela abaixo será exibida, no campo de texto dela, digite "control panel".



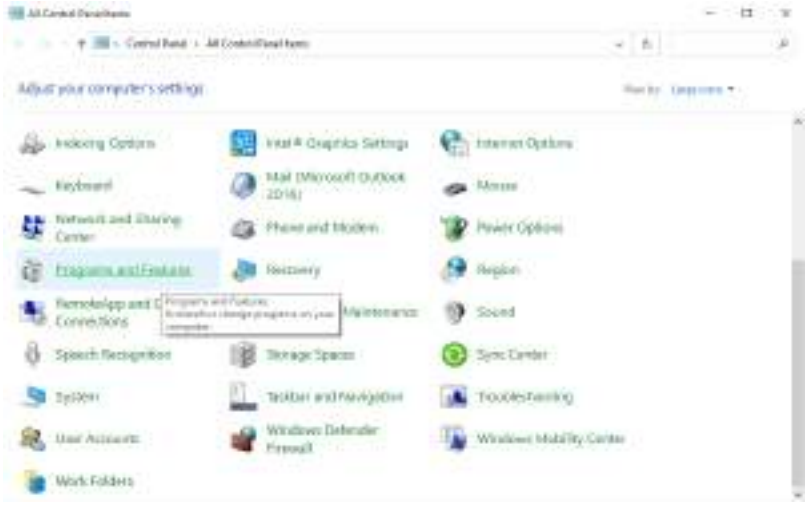
Run - control panel

O painel de controle será exibido, como exemplificado abaixo:



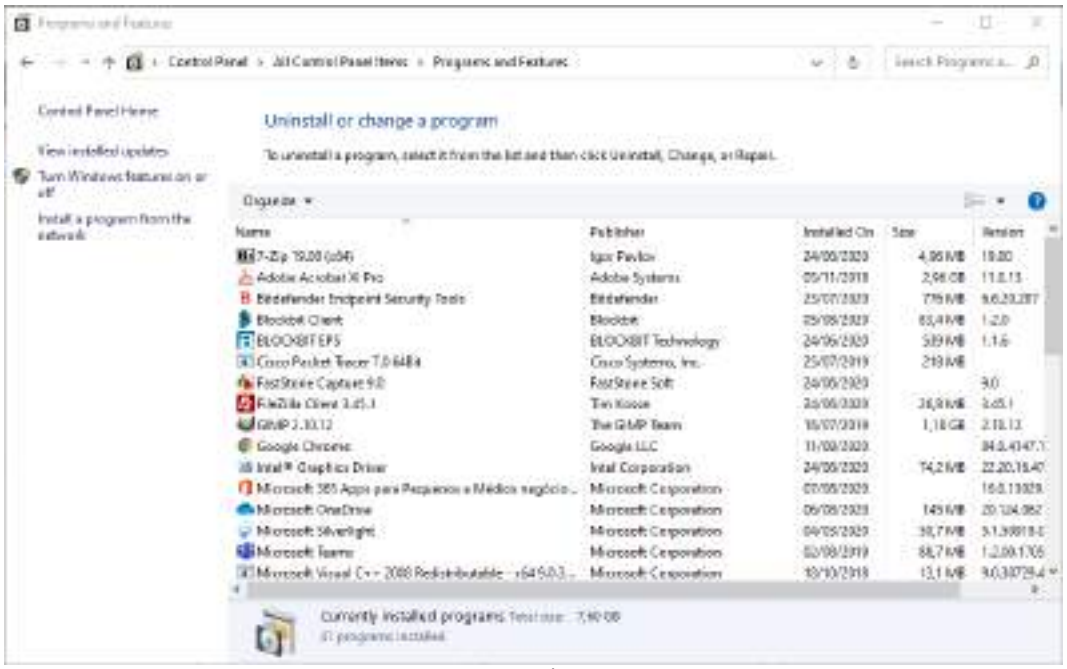
Control Panel

Selecione a opção **[Programas e recursos do Windows]:**



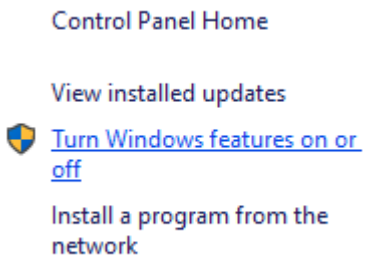
Control Panel - Programs and Features

A janela abaixo será exibida:



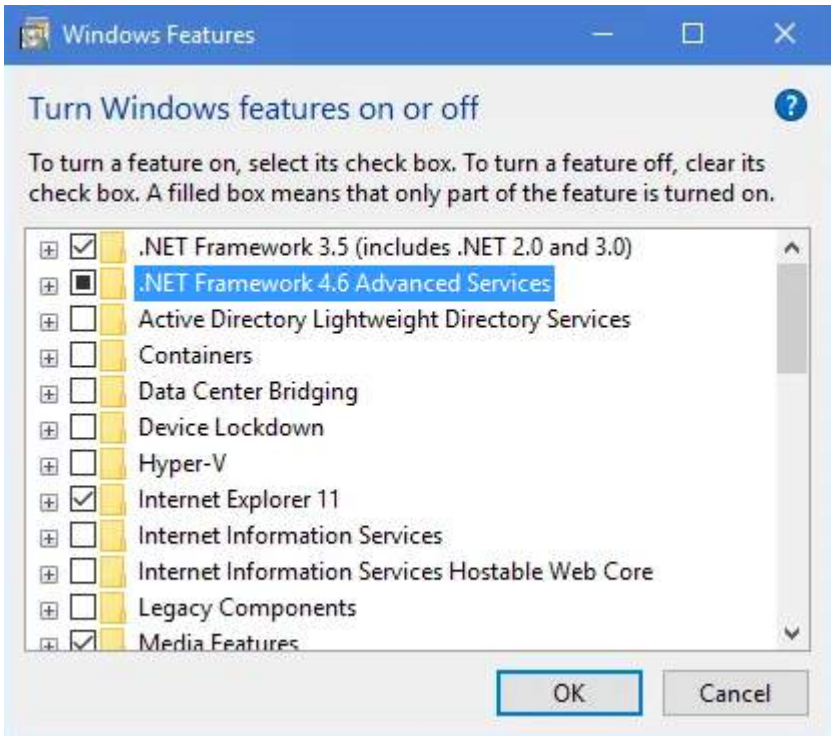
Programs and Features

Selecione a opção **[Ativar/ Desativar recursos do Windows]** localizada no menu à esquerda:



Programs and Features - Turn Windows features on or off

A janela abaixo será exibida:



Windows Features

Para instalar o *.Net Framework 4.6*, basta selecioná-lo nesta janela, apertar [OK] e seguir as instruções do instalador.

Abaixo vamos efetuar o *download* do Blockbit *Client*.

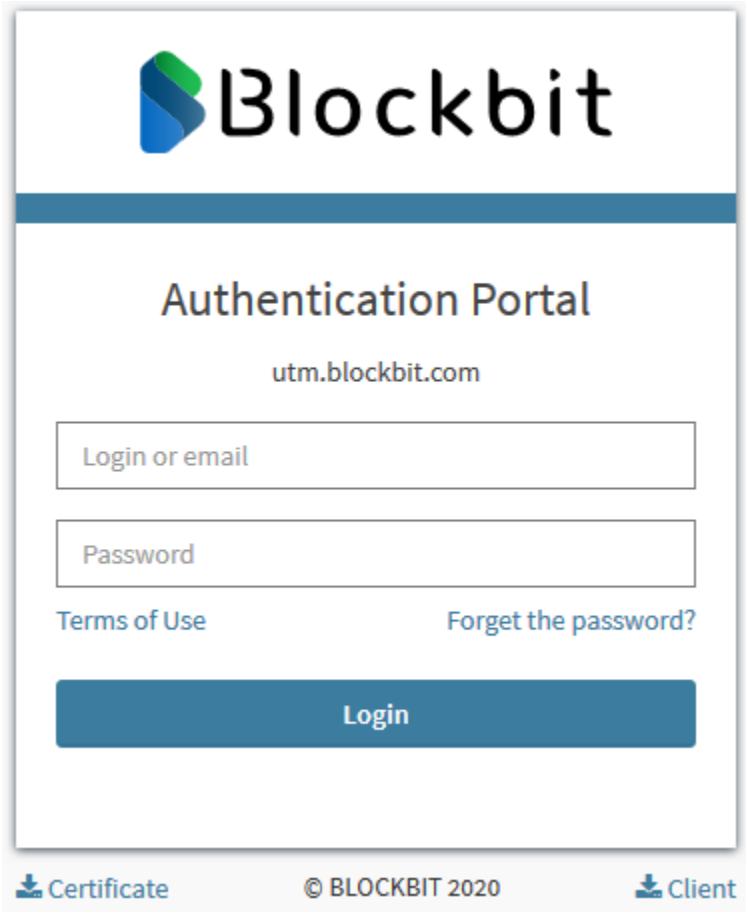
Processo de *Download*

O *link* de *download* do Blockbit *Client* é disponibilizado a partir do portal de autenticação.

Para acessar o portal de autenticação, acesse um navegador (*browser*) e digite o mesmo endereço que foi configurado para acessar o seu UTM, porém utilize a porta 9803, por exemplo:

https://utm.blockbit.com:9803.

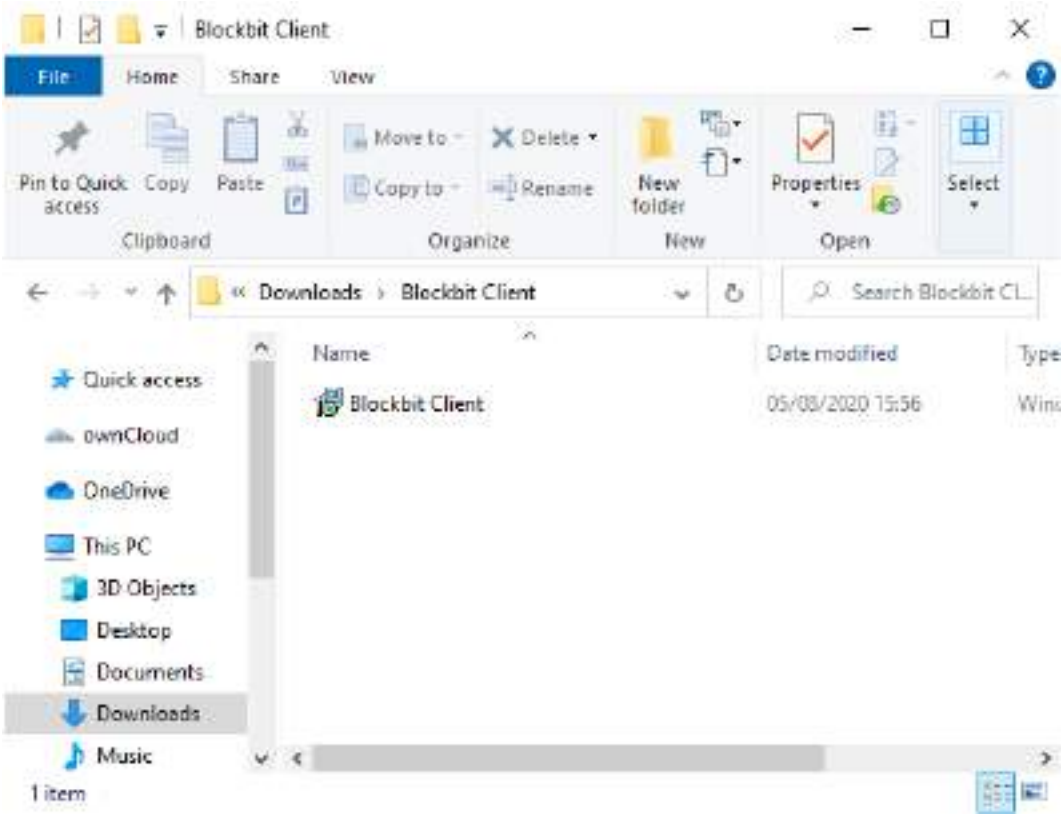
A tela abaixo será exibida:



User's Portal Authentication

Do lado inferior direito, temos um **LINK** para Download do **Client de Autenticação Windows**. Clique em **[**  **]** para o download do agente **[Blockbit_Client.msi]**.

O instalador é um arquivo do tipo *"msi – Microsoft Windows installer"*, basta executar o arquivo com 2(duplo) clique e proceder com a instalação padrão.

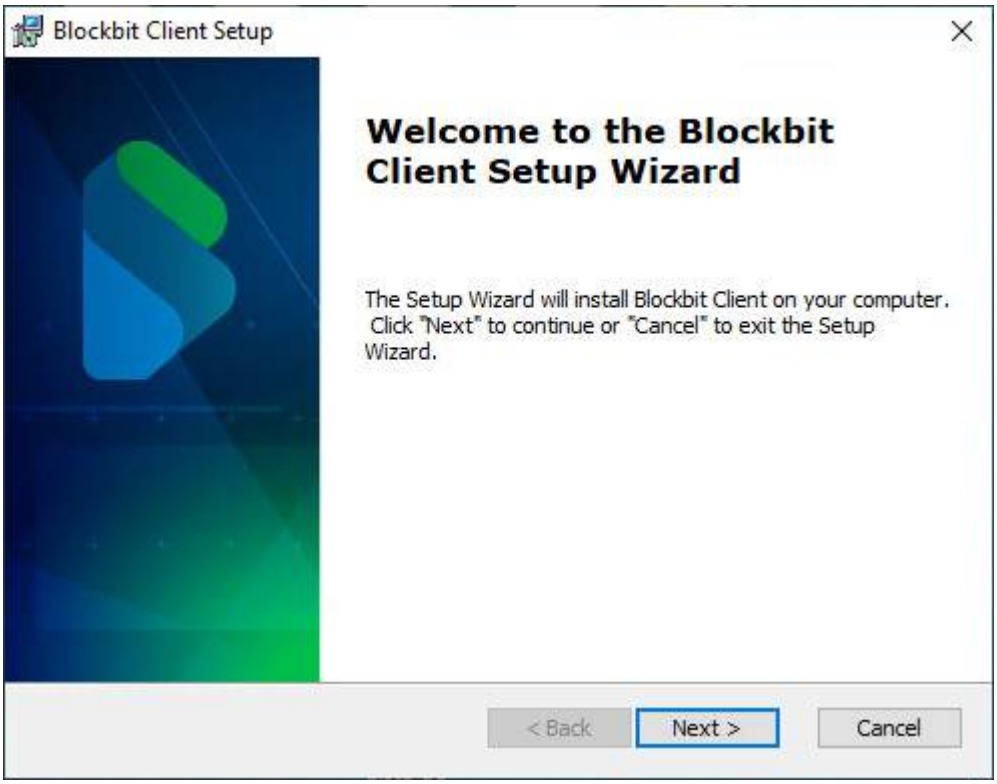


Salve o Blockbit Client

À seguir, analisaremos o processo de instalação do Blockbit Client.

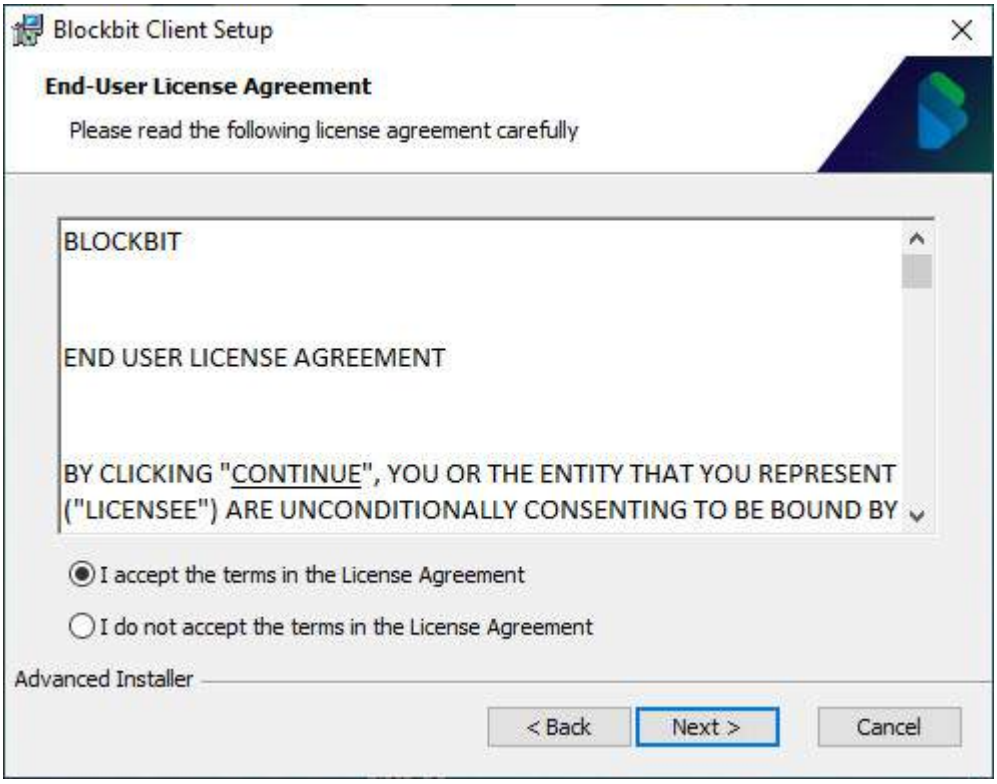
Guia de Instalação

Após dar um duplo clique no instalador do Blockbit Client, a seguinte tela será exibida:



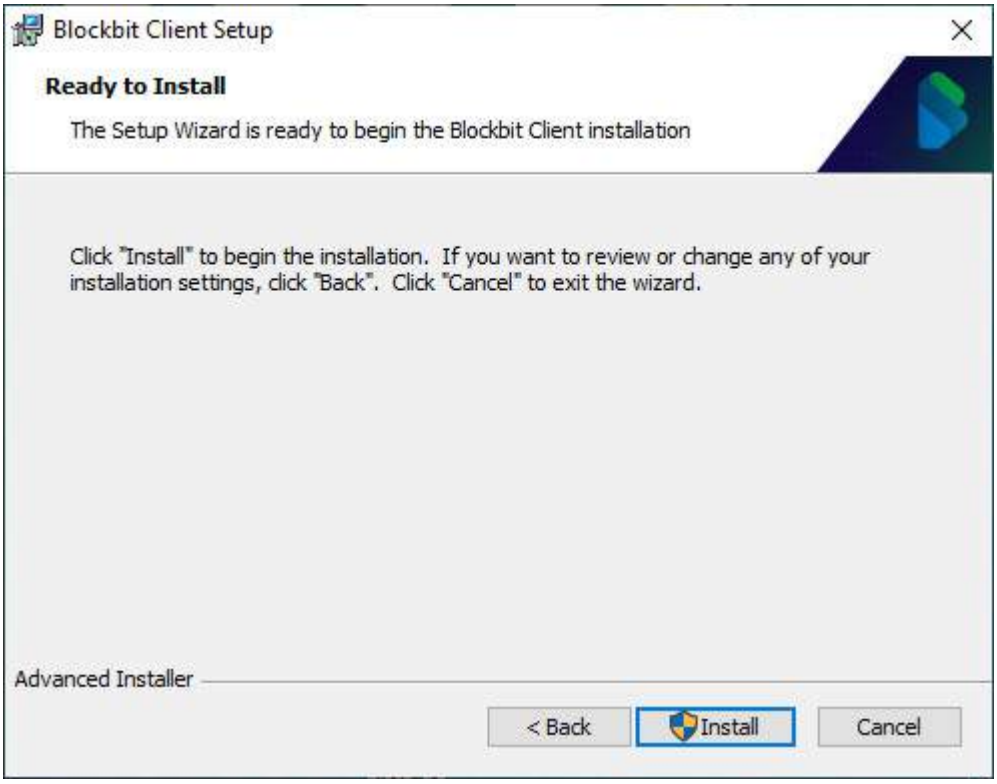
Welcome to the InstallShield Wizard for Blockbit Agent

Clique em [Next >] para prosseguir.



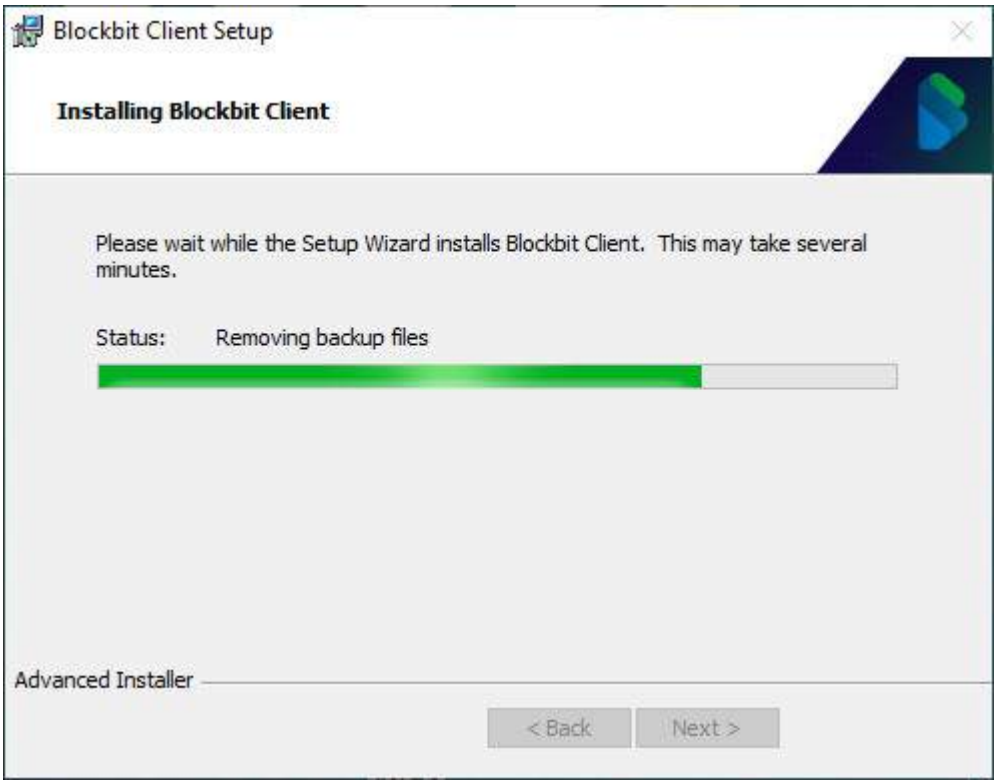
End-User License Agreement

Certifique-se de que [◉] **I accept the terms in this license agreement** está selecionado e aperte [Next >].



Ready to Install

Clique no botão [Install] para iniciar a instalação e aguarde.

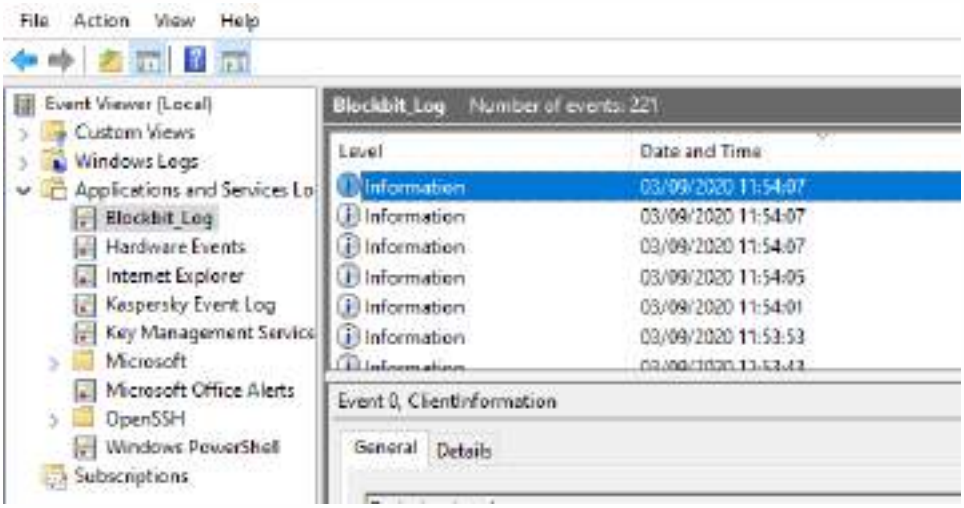

Blockbit Client Setup
Installing Blockbit Client
Please wait while the Setup Wizard installs Blockbit Client. This may take several minutes.
Status: Removing backup files
Advanced Installer
< Back
Next >

Files in Use

Durante a instalação é registrado e iniciado um serviço chamado "Blockbit Service" e um driver de rede *TAP*, esta interface fica desativada em *ba ckground* enquanto estiver fora de uso, sendo ativada automaticamente no momento que uma conexão é efetuada. É possível visualizá-la na janela de conexões de rede, como demonstrado abaixo:

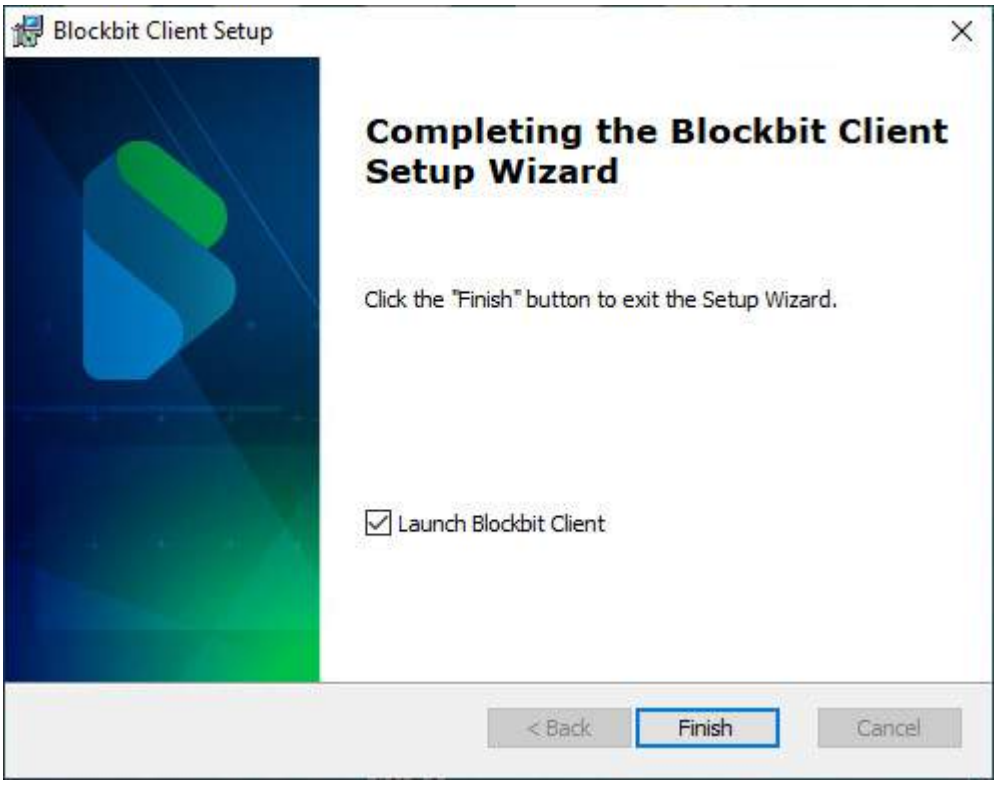
Para mais informações sobre conexão, consulte esta página.

Além disso, o Blockbit Client também registra logs no Gerenciador de Eventos do Windows. Como demonstrado abaixo:



Para mais informações sobre os *logs* nos eventos do *Windows*, consulte esta página.

Após a finalização do processo de instalação, a seguinte tela será exibida:



InstallShield Wizard Completed

Caso essa não seja a sua primeira vez instalando o Blockbit Client ou esteja atualizando ele, os seus perfis de conexão estarão armazenados em uma pasta de sistema do seu *Windows* e serão automaticamente adicionados na sua nova instalação.

Clique em **[** Finish **]**.

Instalação finalizada!

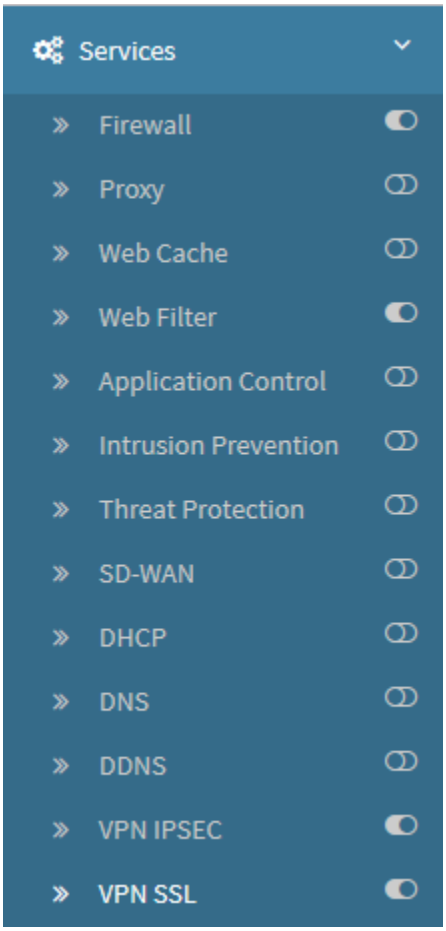
Concluído a instalação o sistema cria um ícone do Agent na área de trabalho.

Atalho na Área de Trabalho

Por fim, será necessário fazer uma configuração no UTM, segue mais informações:

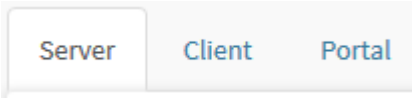
Configuração da *VPN SSL*

Acesse o UTM que será utilizado para fazer a autenticação e no menu Services, clique na opção VPN SSL:



Services - VPN SSL

Caso ela não esteja selecionada, clique na aba *Server*:



VPN SSL - Server

Acesse o painel *Advanced* na parte inferior da tela e expanda ele clicando em **[ ]**;

VPN SSL - Server - Advanced

Neste painel, certifique-se que a opção *compression* está ativada, caso contrário, o Blockbit Client, não funcionará corretamente.

Compression habilitada

Para mais informações sobre VPN SSL, consulte esta página.

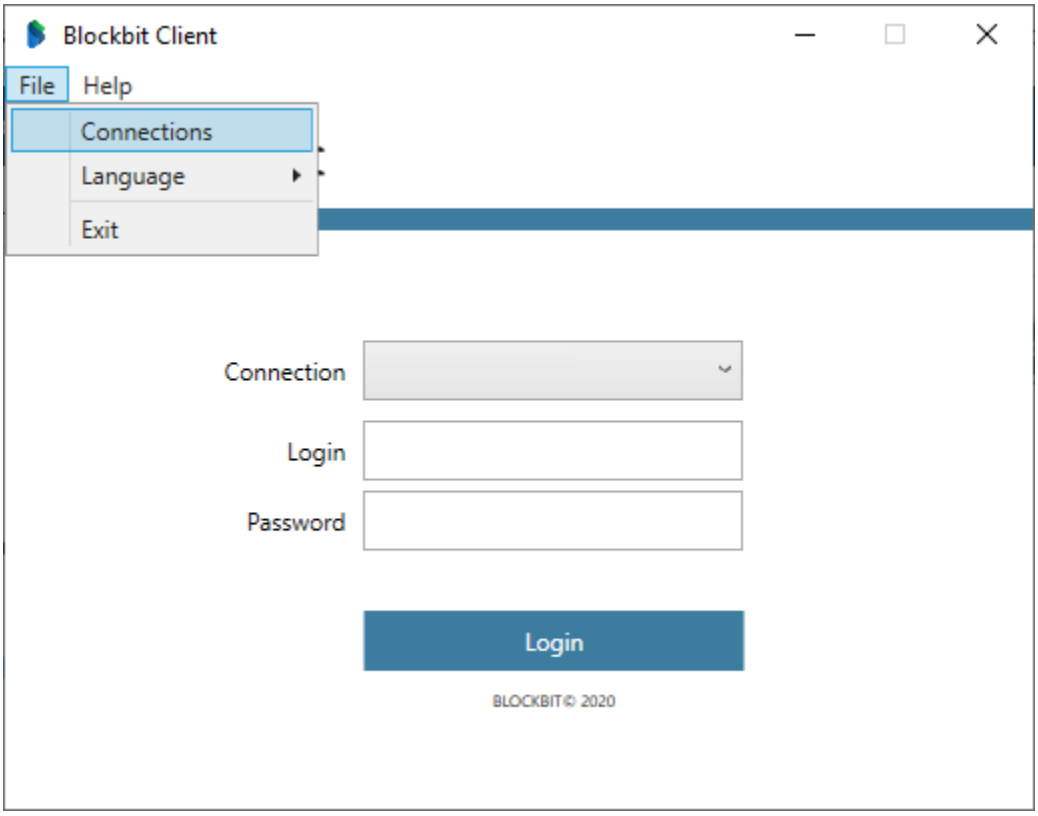
Isso conclui a instalação e preparação do Blockbit Client para seu uso. À seguir, vamos ver mais informações sobre como configurar ele, para tanto acesse esta página.

Configuração do Blockbit Client

O Blockbit Client permite ao administrador criar **[N]** perfis de acesso para a mesma instalação no computador local.

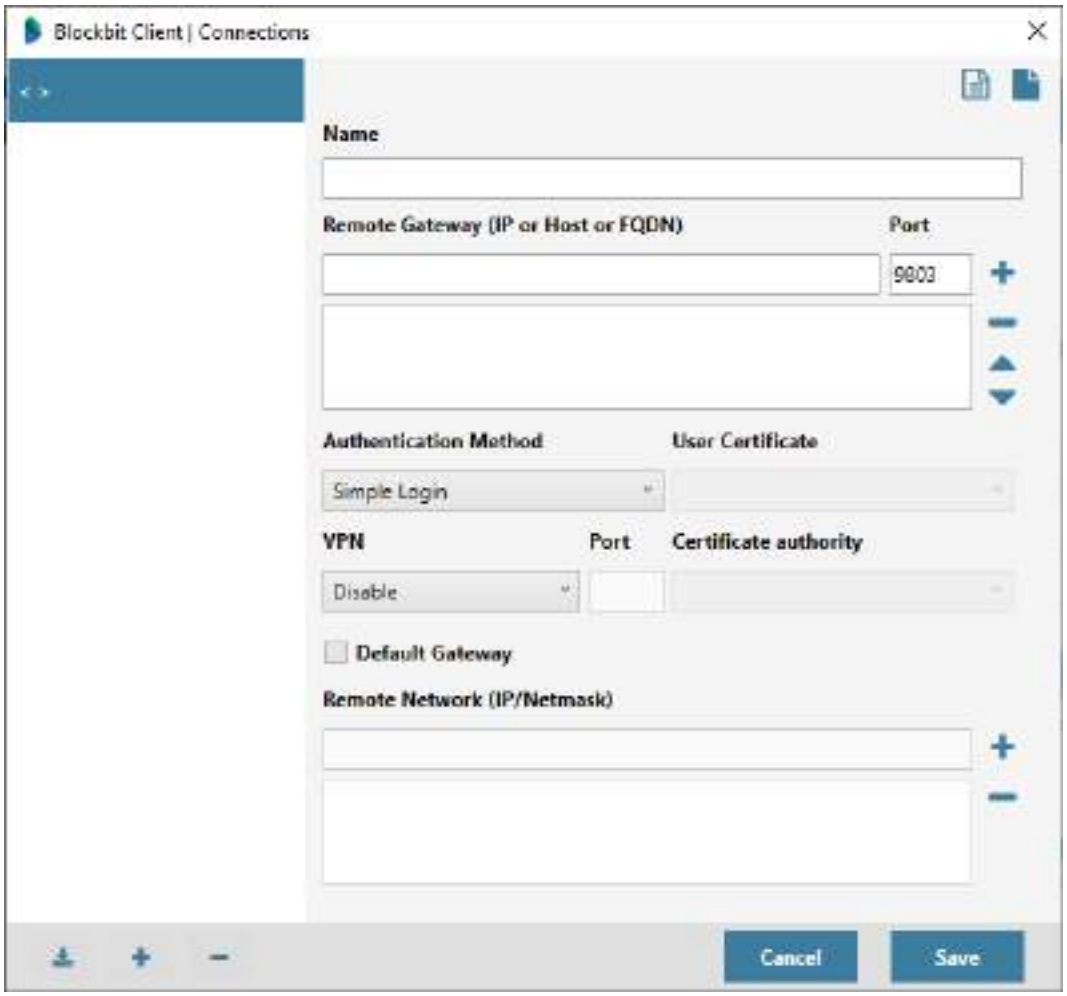
Ao abri-lo pela primeira vez, como nem uma conexão foi configurada a tela "*Connections*" será exibida automaticamente.

Caso um perfil de conexão já tenha sido instalado, para acessar esta tela, basta clicar em "*File*" no topo da janela e selecionar a opção "*Connections*", como exibido abaixo:



Blockbit Client - File - Connections

Ao selecionar esta opção ou no caso já citado acima (Blockbit Client recém-instalado) a janela abaixo será exibida:



Configuração do Blockbit Client

Para criar um perfil você deve configurar o formulário de acordo com as especificações de conexão com o respectivo servidor Blockbit UTM. A seguir analisaremos cada campo em detalhe:

- ***Name*:** Nome do perfil da conexão. Ex.: Default Auth;
- ***Remote Gateway*:** Digite os endereços *IP, host* ou *FQDN* dos servidores Blockbit UTM e clique em **[ ]** para adicionar na lista, caso deseje removê-lo, clique em **[ ]** e use as setas **[ ]** e **[ ]** para alterar a prioridade. É possível adicionar 3 endereços de *Gateway* remoto. O serviço de conexão *VPN* (*IPSEC* ou *SSL*) tenta conectar no endereço secundário caso não consiga estabelecer a conexão pelo Primário (sendo que o endereço que estiver no topo tem maior prioridade). Ex.: utm.labblockbit.com;
- ***Authentication Method*:** Selecione entre o método de autenticação que será utilizado, podendo ser:

Caso opte por autenticação com certificado, é necessário habilitar no UTM a opção "Verify user certificate" em *Settings - Authentication - Settings*. Depois, importar esse certificado no "Usuário Atual" e selecionar ele na configuração de conexão do Blockbit Client.

O certificado deve possuir o *IP* do UTM ou um *hostname* que resolva o nome para o IP do UTM, de forma que o cliente possua os mesmos dados (*IP* ou *hostname* igual) para efetuar a conexão.

Para autenticação por certificado, é necessário ter a CA do servidor instalada no computador do usuário e usar o gateway assinado no certificado de serviço.

Para utilizar as *VPNs* é necessário instalar os certificados de usuários e *CAs* na estação do usuário. Consulte esta página para mais informações sobre como efetuar as instalações.

- **Windows Login:** Ao selecionar esta opção o Blockbit Client reconhecerá o usuário autenticado localmente no dispositivo ou na rede Windows, como usuário de autenticação para o Blockbit UTM. O sistema utilizará as credenciais do *Active Directory*, não sendo necessário nem utilizar a senha. Para ver um exemplo, consulte esta página;
- **Windows Login + Certificate:** Ao selecionar esta opção, além de reconhecer o usuário autenticado localmente no dispositivo ou na rede Windows, o Blockbit *Client* passará a efetuar a autenticação de dois fatores adicionando o requisito do certificado digital de usuário – SSL durante o login. Ao selecionar este método, o usuário precisará entrar no portal, gerar o certificado e instalá-lo usando a opção Usuário Atual (não máquina local) para que seu certificado seja exibido no campo "*User Certificate*". Para ver um exemplo, consulte esta página;

Pra redes locais, caso use os perfis acima é possível transferir o *Client* com as configurações principais através de uma *GPO* do *Windows*

- **Simple Login:** Caso esta opção for selecionada, o usuário precisará usar o nome do usuário e senha para conexão com o Blockbit UTM. Ex.: Jhonny.muller@ead.labblockbit.com. Este método também utiliza as credenciais do *Active Directory* para efetuar a autenticação. Para ver um exemplo, consulte esta página;
- **Simple Login + Certificate:** Com esta opção selecionada, além de usar o “User Name” e “Password”, o Blockbit *Client* passará a efetuar a autenticação de dois fatores, adicionando o requisito do certificado digital de usuário – SSL durante o login. Para ver um exemplo, consulte esta página;
- ***Login + Certificate* (*IPSEC legacy*):** Esta opção é utilizada especificamente para manter a compatibilidade do Blockbit Client com os UTM 2.0.4 e inferiores, inclusive o 1.5. O Blockbit Client efetua o acesso utilizando certificado digital. Portanto, será necessário completar o campo ***Remote Network*** com informações da *VPN IPSEC* utilizada. Para ver um exemplo, consulte esta página;

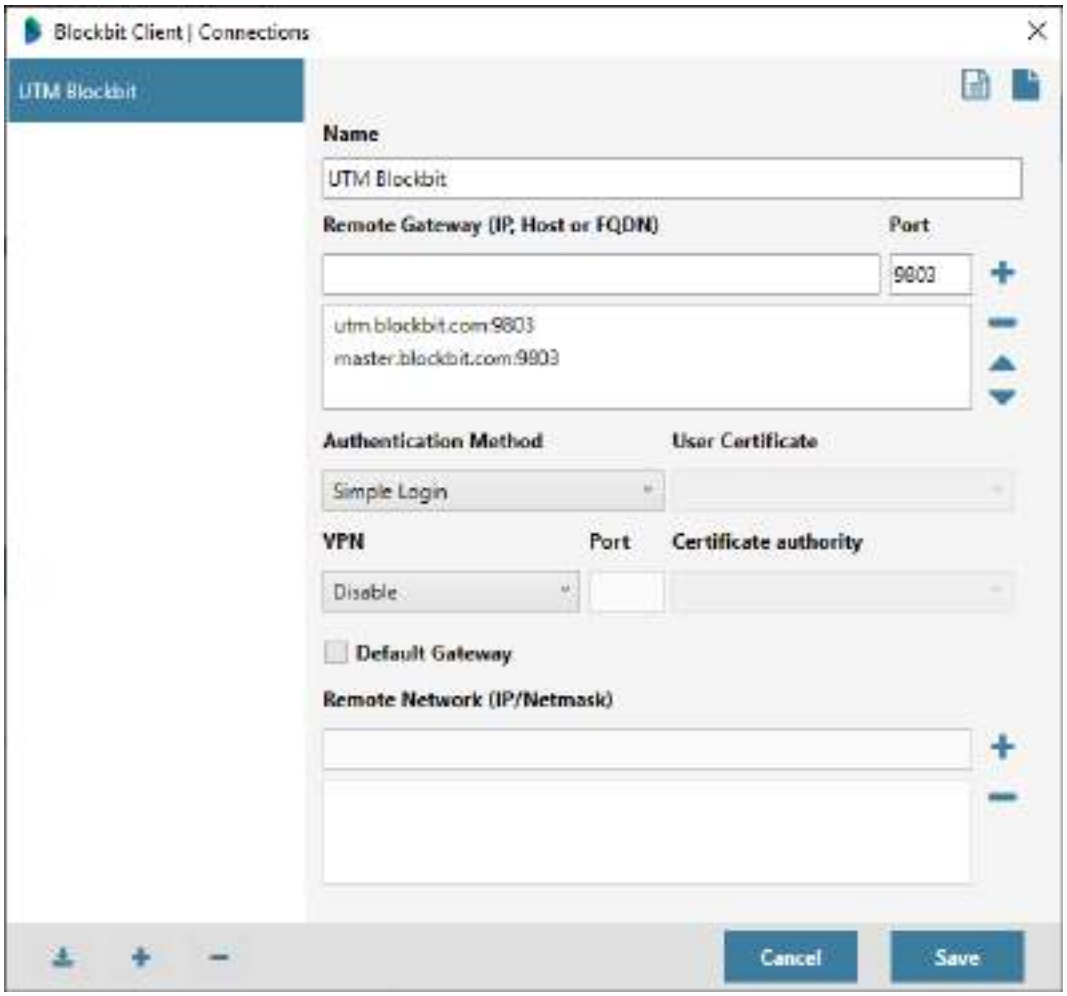
Caso a sua versão for inferior à UTM 2.0.5 e esteja usando o Blockbit Agent com VPN IPSEC, ao migrar para o Blockbit Client, a VPN IPSEC só funcionará caso seja utilizado o modo ***Login + Certificate (IPSEC Legacy)***.

- ***User Certificate:*** Caso tenha selecionado algum método de autenticação que exija certificado, será necessário importá-lo e selecioná-lo neste campo. Caso não tenha selecionado a opção relevante, este campo estará desabilitado. Para exibir ele nesta lista, é necessário instalar no usuário atual (não na máquina local). Para mais informações, consulte esta página;
- **VPN:** Selecione o tipo de VPN que será utilizada para conectar-se automaticamente, há duas opções disponíveis:
  - **Disable:** Nesse caso o acesso será local, portanto o campo **"*Port*"** e a caixa de checagem **"*Default Gateway*"** são desabilitados;
  - **SSL:** Caso esta opção seja selecionada, o campo **"*Port*"** precisará ser preenchido com a porta da SSL (por padrão o sistema usa a porta 9443). À direita, o campo ***Certificate Authority*** será habilitado, informe nele qual *Root CA* será utilizada, consulte esta página para mais informações sobre Instalação de Certificados ou esta página para mais informações sobre como configurar o UTM para utilizar uma VPN SSL;
- ***Port*:** A porta de conexão do serviço de autenticação. A porta padrão é 9443. Ex.: 9803;
- **Certificate Authority:** Quando for selecionada a opção *SSL* no campo *VPN*, este campo será habilitado. Sua função é permitir a seleção de qual *Root CA* será utilizado pela *VPN SSL*. Para exibir a *CA* nesta lista, é necessário instalar o certificado na máquina local (não no usuário local) e salvá-lo na pasta *autoridade de certificaç!ão de raiz confiável*. Para mais informações, consulte esta página;
- **Default Gateway[☑]:** Ao marcar esta caixa de checagem, a *VPN* irá passar a utilizar o *gateway* padrão, isso significa que será fechada uma rota com o UTM e todas as conexões passarão completamente pelo *firewall* (respeitando as políticas dele). Caso esta caixa de checagem não seja selecionada, a conexão sairá completamente pela rede local do computador do usuário, porém fechando rotas com os IPs adicionados na lista *Remote Network (IP/Netmask)*.
- ***Remote Network* (*IP*/*Netmask*):** Caso o caixa de checagem acima seja marcada, este campo estará habilitado para edição. Digite os *IPs* ou *Net masks* que serão utilizados remotamente e clique em **[+]** para adicionar na lista, caso deseje removê-lo, clique em **[−]**.

Em caso de falha de conexão com o *gateway*, é adicionado um registro a respeito no *Log*.

Clique em **[Save]** para criar o perfil e finalizar as configurações ou em **[Cancel]** para voltar à tela anterior.

Após salvar as configurações o perfil terá sido criado com sucesso, como exemplificado pela imagem abaixo:

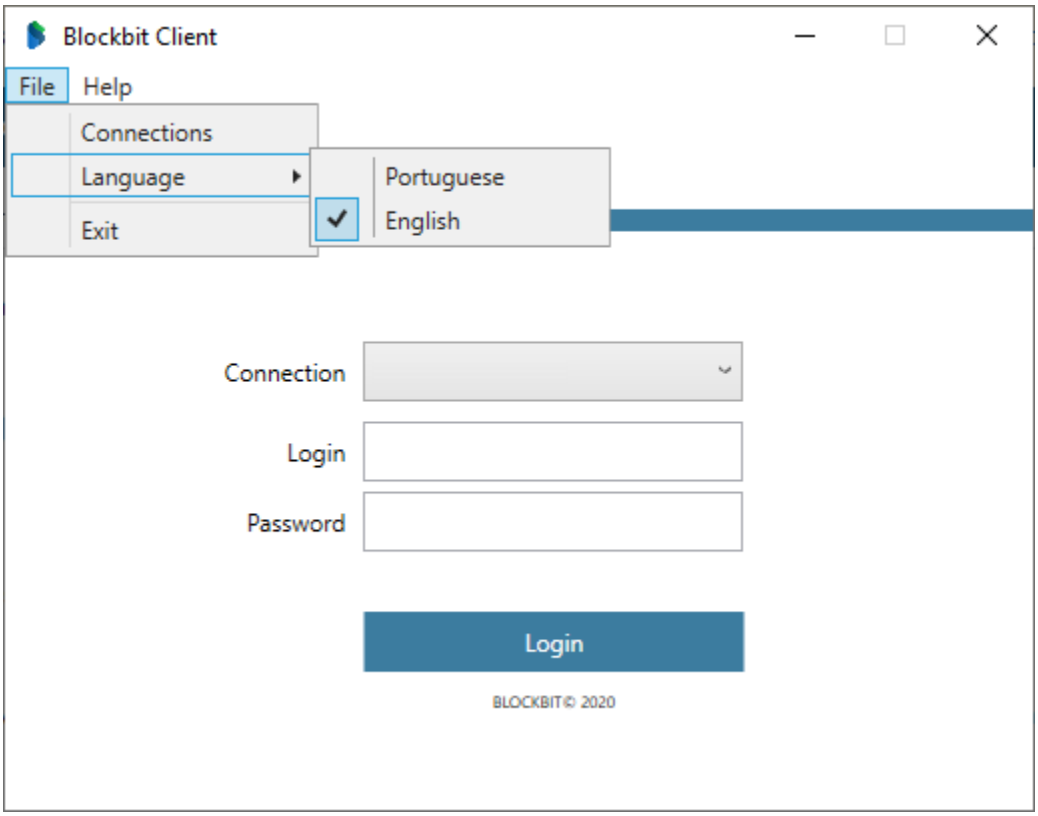


Blockbit Client - Configurado

Após ter configurado um perfil de conexão com sucesso, é possível utilizar as opções à seguir:

- **Adição de um novo Perfil [ ]**;
- **Remoção de Perfil [ ]**;
- **Importação de Perfil [ ]**;
- **Exportação de Perfil [ ]**;
- **Exportação do log de conexões [ ]**.

Por fim, o Blockbit Client está disponível em Português e Inglês. Para alterar o idioma, basta clicar em "*File*" no topo da janela e selecionar a opção "*Langu age*", como exibido abaixo:



Blockbit Client - File - Language

Isso finaliza o processo de configuração dos perfis do Blockbit Client.

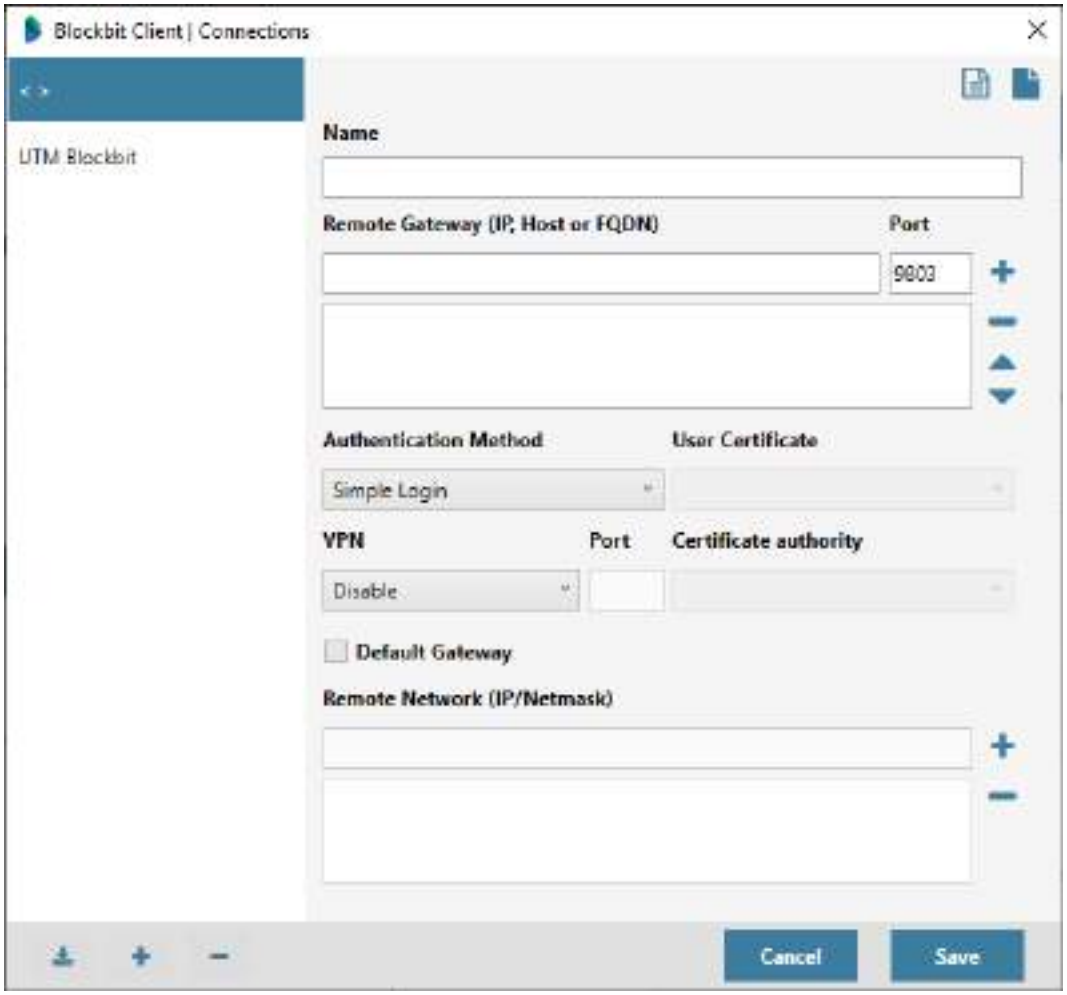
Para visualizar exemplos de configuração de perfis de conexão, consulte esta página.

Para mais informações sobre como utilizar estes perfis para fazer uma conexão, consulte esta página.

Consulte esta página para um passo a passo de como fazer instalação de certificados.

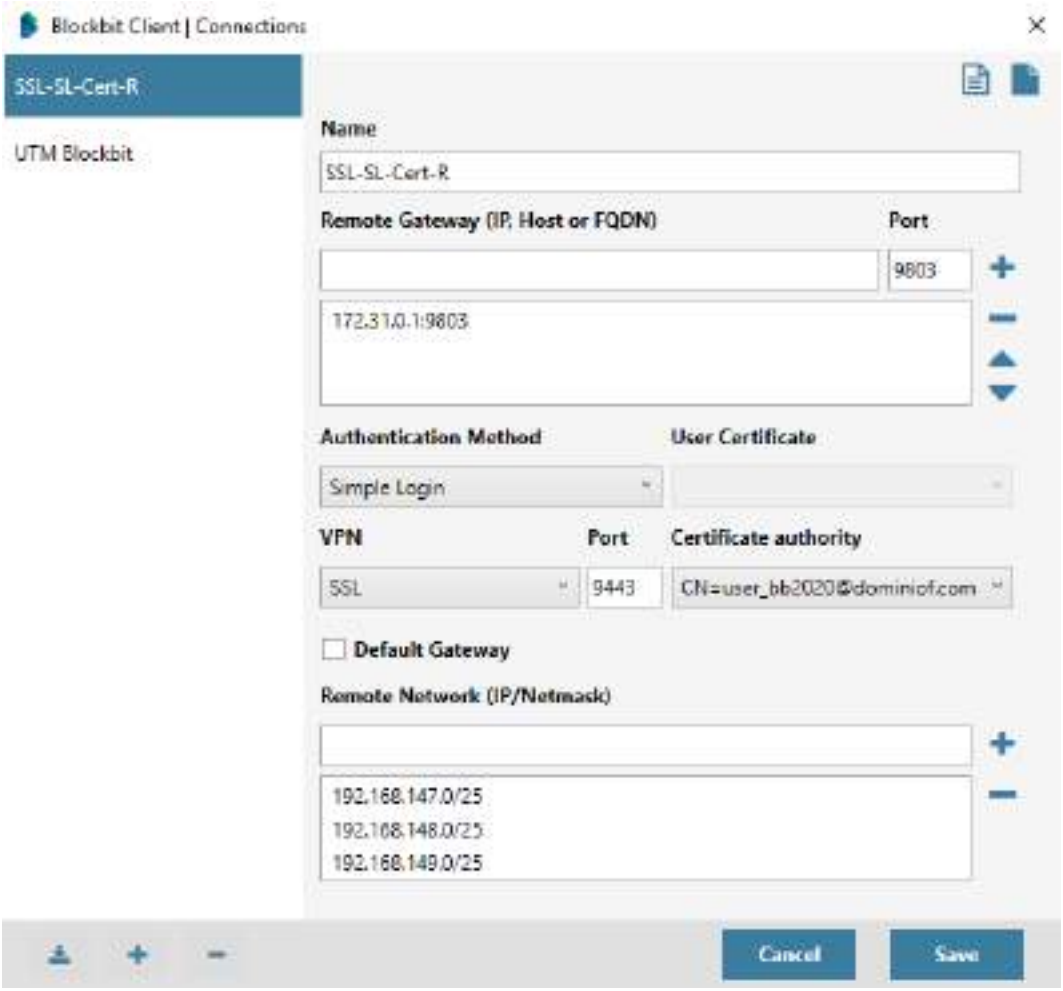
Adição de um novo Perfil

Para adicionar um novo perfil de conexão, clique no botão [+] localizado no canto inferior esquerdo. Um novo formulário de perfil de conexão será exibido:



Blockbit Client - Connections - New Profile

Após clicar neste botão, basta completar o formulário da mesma forma que foi demonstrado nesta página. Por exemplo:



Blockbit Client - Connections - New Profile - Example

Clique em [Save] para criar o perfil e finalizar as configurações ou em [Cancel] para voltar à tela anterior.

Caso o perfil de conexão necessite da instalação de um certificado, consulte esta página para mais informações.

A seguir, vamos analisar como efetuar a Remoção de um Perfil.

Instalação de Certificados

No Blockbit Client em perfis que utilizam certificado para efetuar auteticação ou usem *VPN*, é obrigatório a instalação da CA na máquina local, além disso o certificado deve estar habilitado nas configurações de autenticação no UTM.

Caso a autenticação no Blockbit Client apresente o erro "Falha na conexão", mesmo após instalar a CA do UTM, é necessário habilitar a verificação da CA localizada em Authentication - Aba Settings;

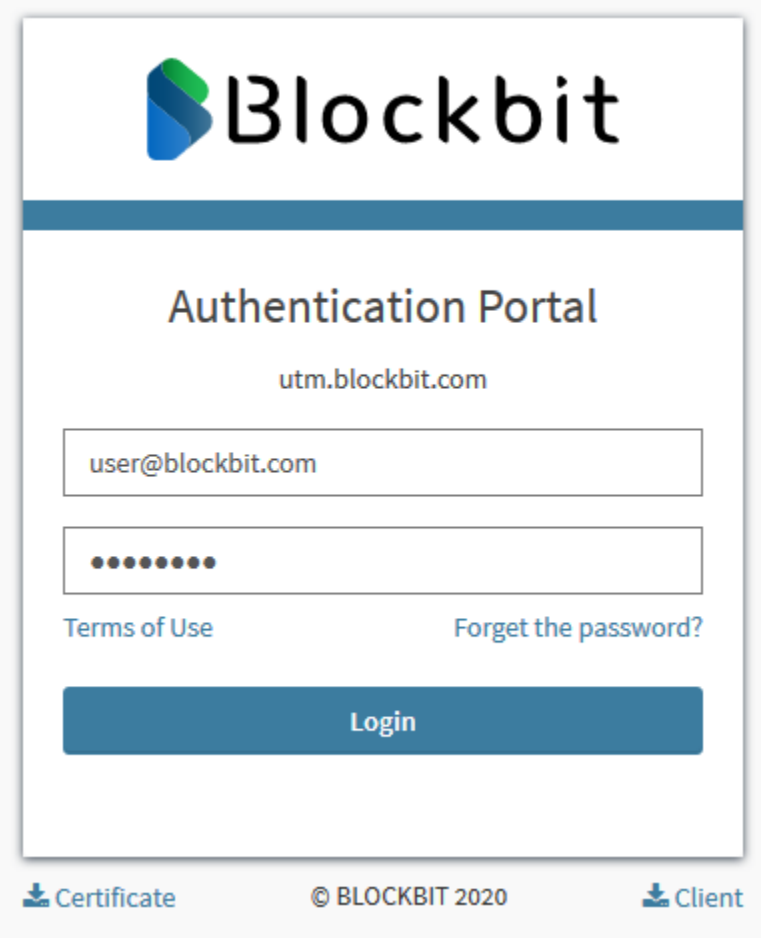
Nesta página iremos demonstrar como efetuar:

- Instalação de Certificados de Usuário;
- Instalação de CAs.

À seguir vamos analisar como fazer a instalação dos certificados.

Instalação de *Certificados de Usuário*

Primeiramente acesse o *captive portal* e efetue o *login* no com o usuário que será utilizado, após preencher o formulário clique no botão **[**Login**]**:



Portal - Certificate

A seguinte janela será exibida:

Portal - Logged

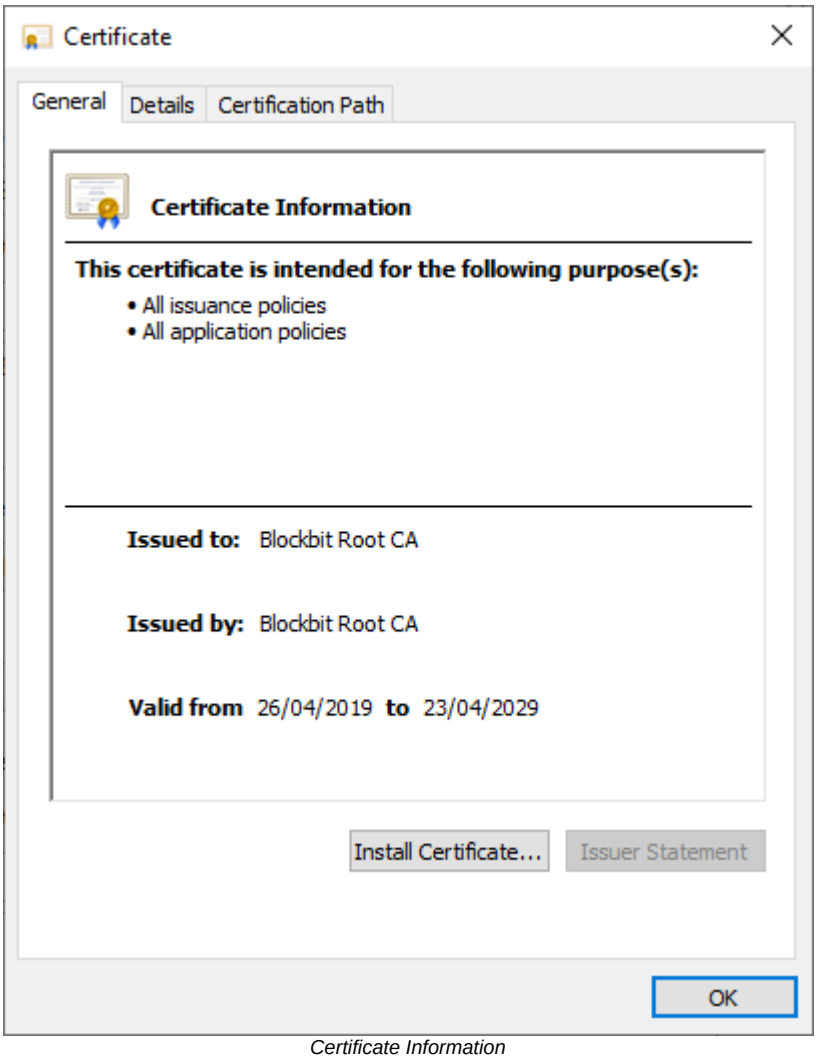
Faça o *download* do certificado do usuário clicando no botão **[** **]** localizado no canto superior direito da tela.

Caso seja necessário instalar a CA também, para facilitar, é recomendável renomear o arquivo de forma a distinguí-lo da CA.

Quando o *download* finalizar, clique no certificado pra abrí-lo:

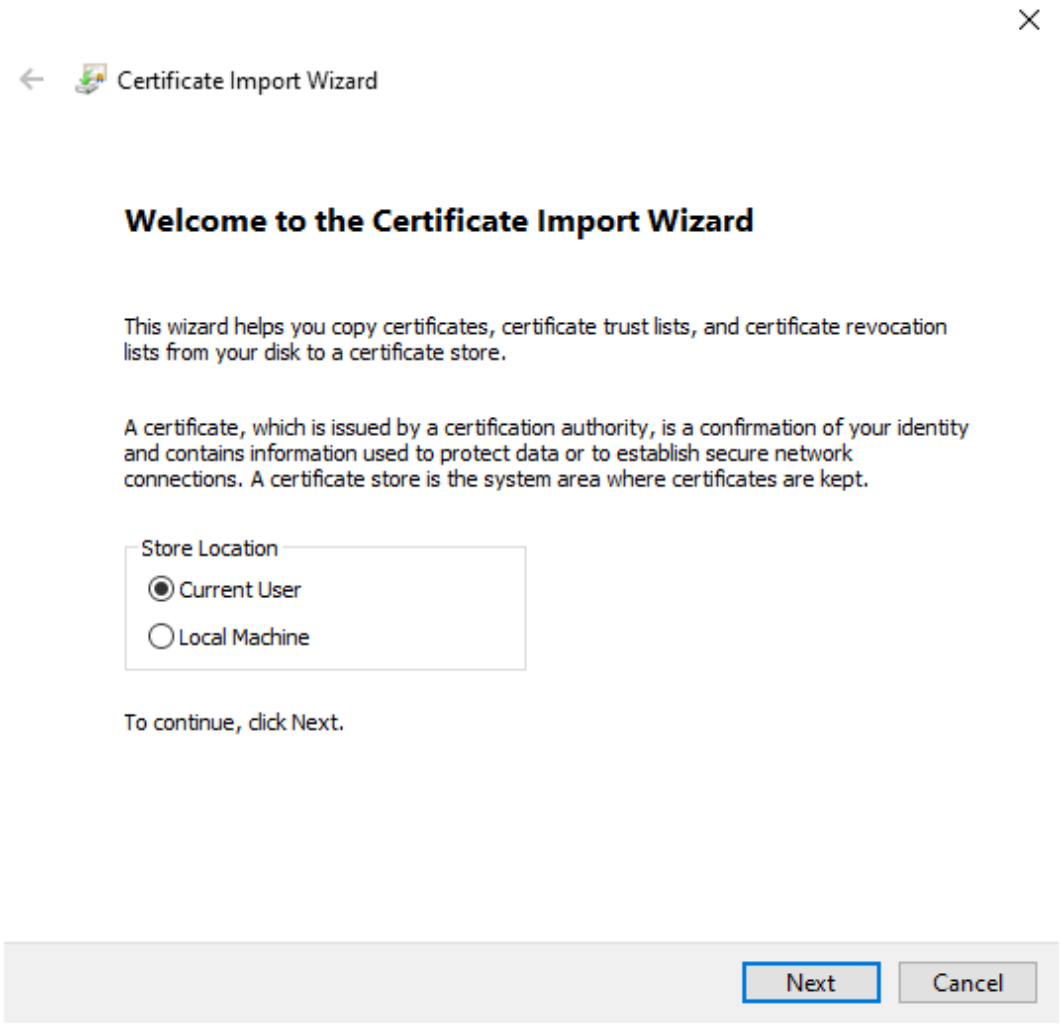
User Certificate

A seguinte janela será exibida:



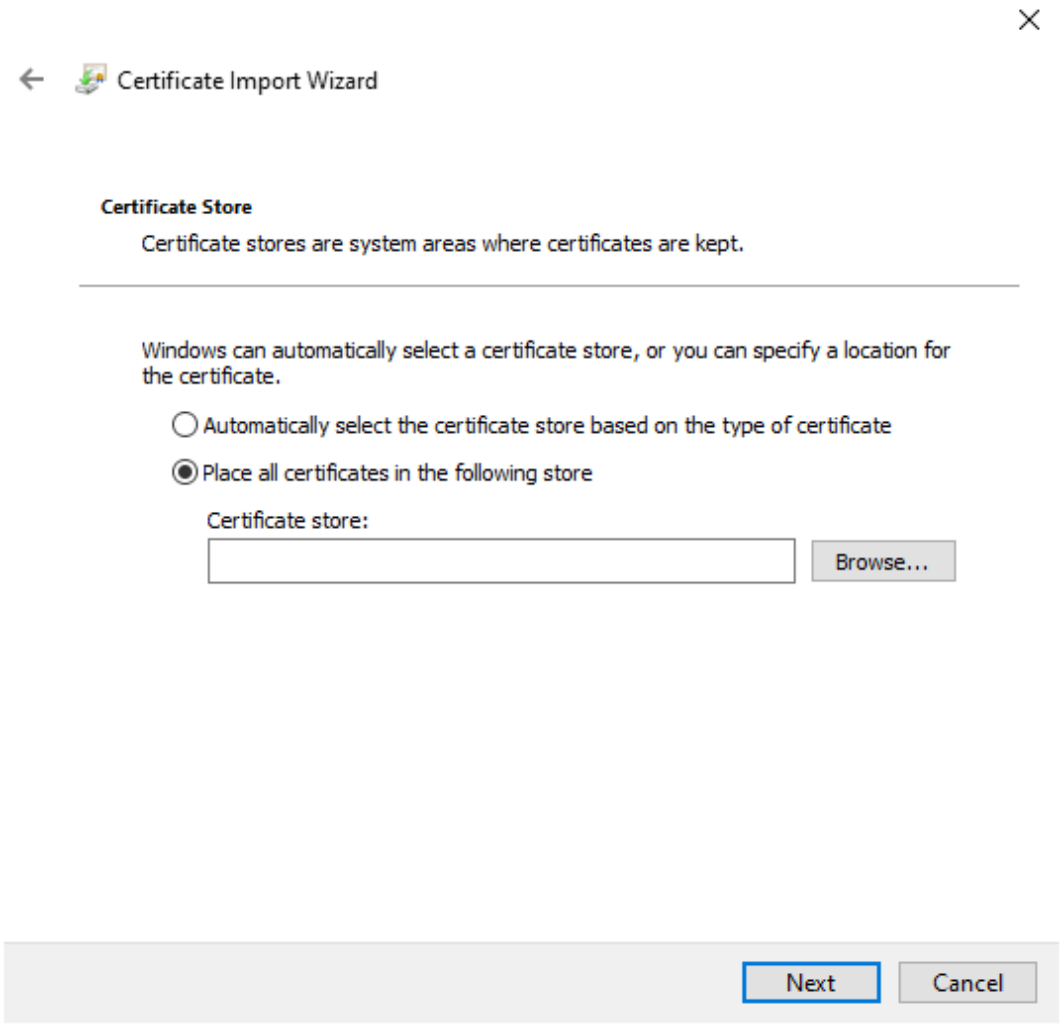
Certificate Information

Clique em [Install Certificate...], a seguinte janela será exibida:



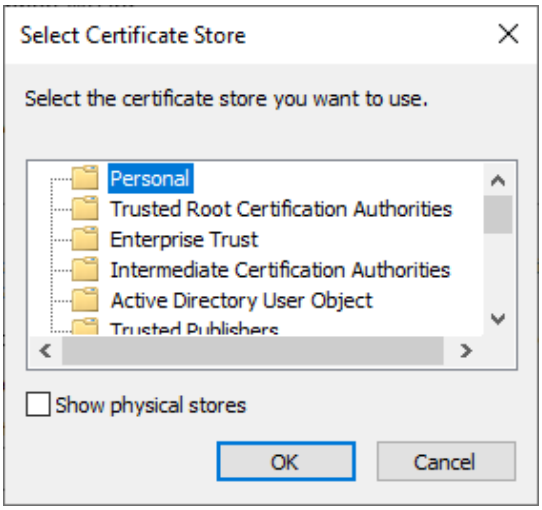
Certificate Import Wizard

Certifique-se que o ***Current User*** [◉] esteja selecionado e clique no botão [Next].



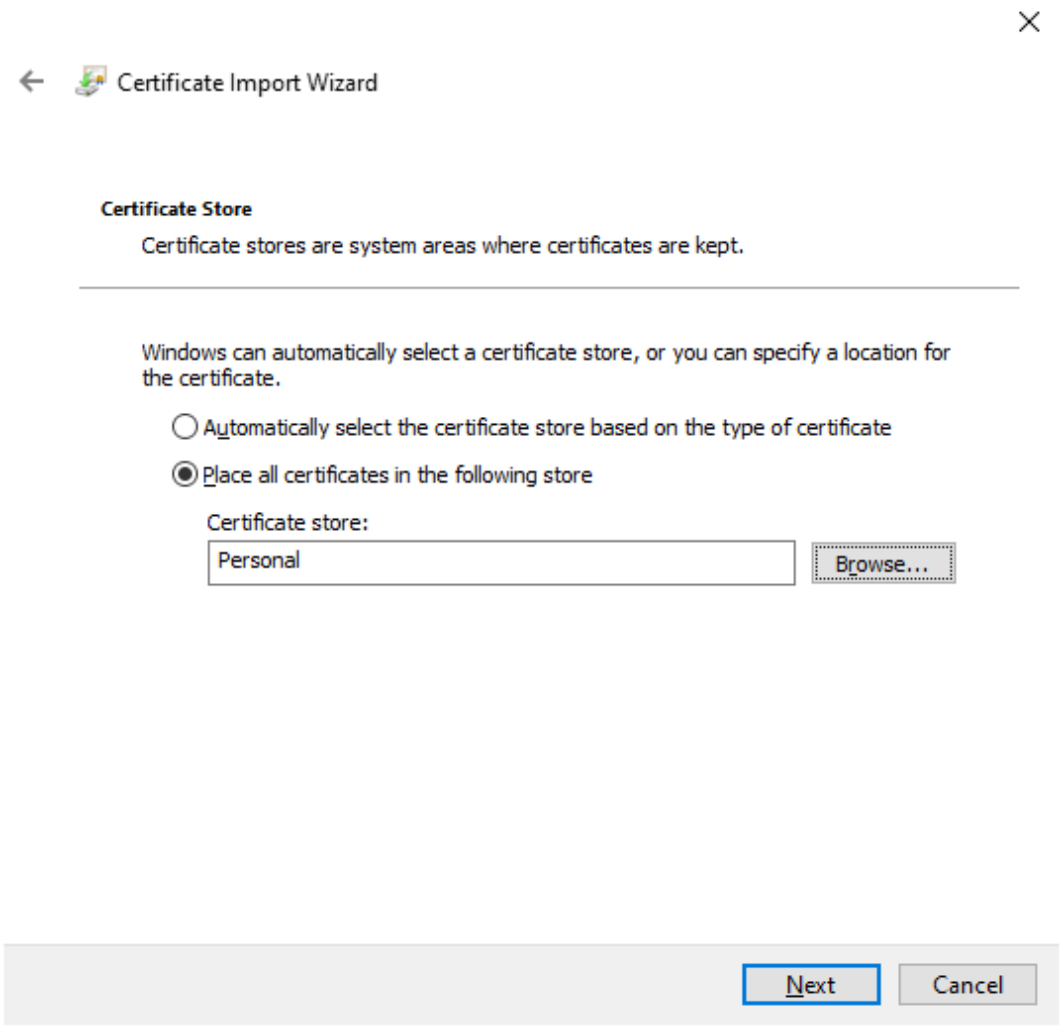
Certificate Store

Selecione a opção ***Place all certificates in the following stores*** **[◉]** e clique no botão **[** Browse... **]** para selecionar onde o certificado será armazenado, a janela a seguir será exibida:



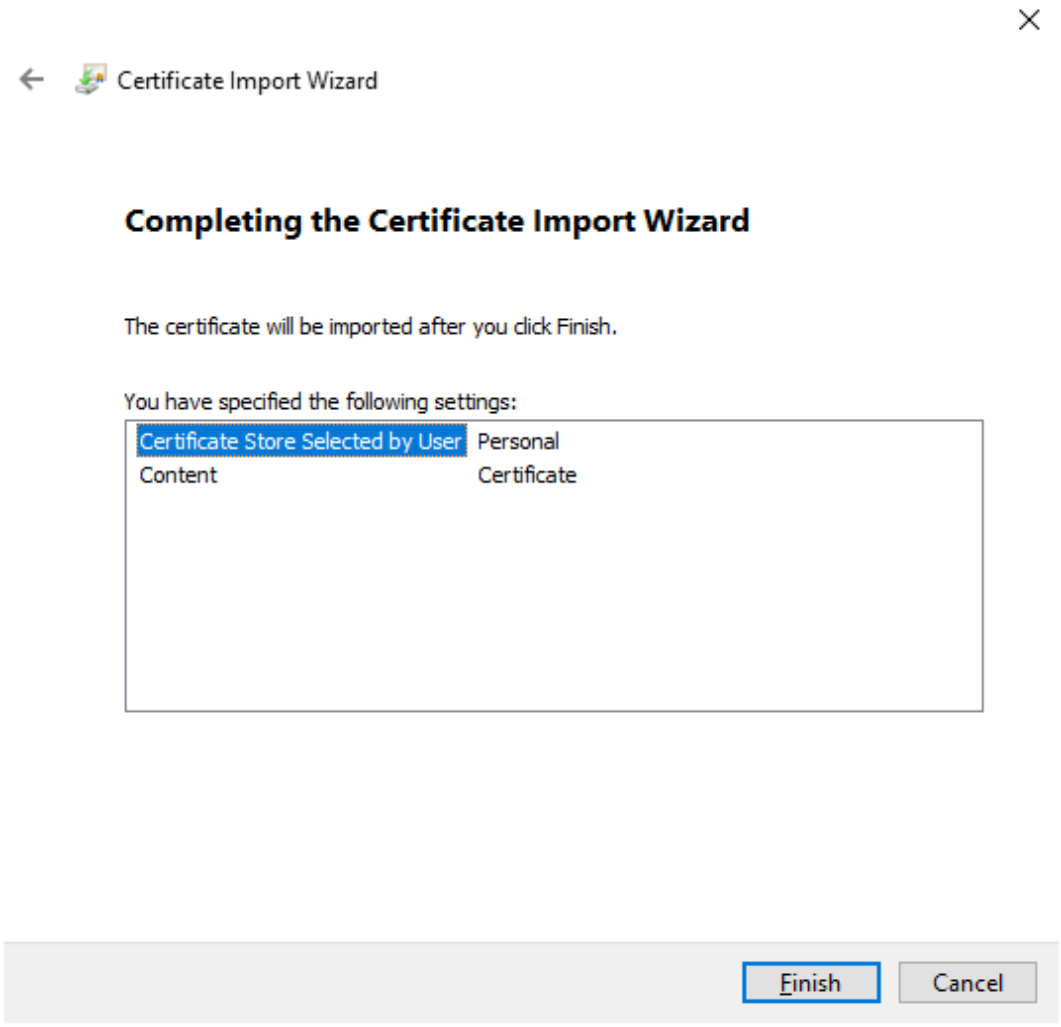
Select Certificate Store

Em *Select Certificate Store,* certifique-se que a opção ***Personal*** está selecionada e clique em **[** OK **]**, a tela à seguir será exibida:



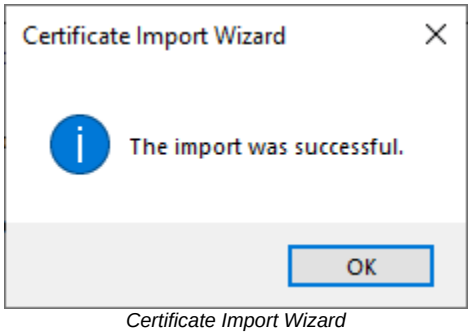
Certificate Store - Selected Store

Clique no botão **[** Next **]** a seguinte tela com um resumo da importação do certificado será exibida:



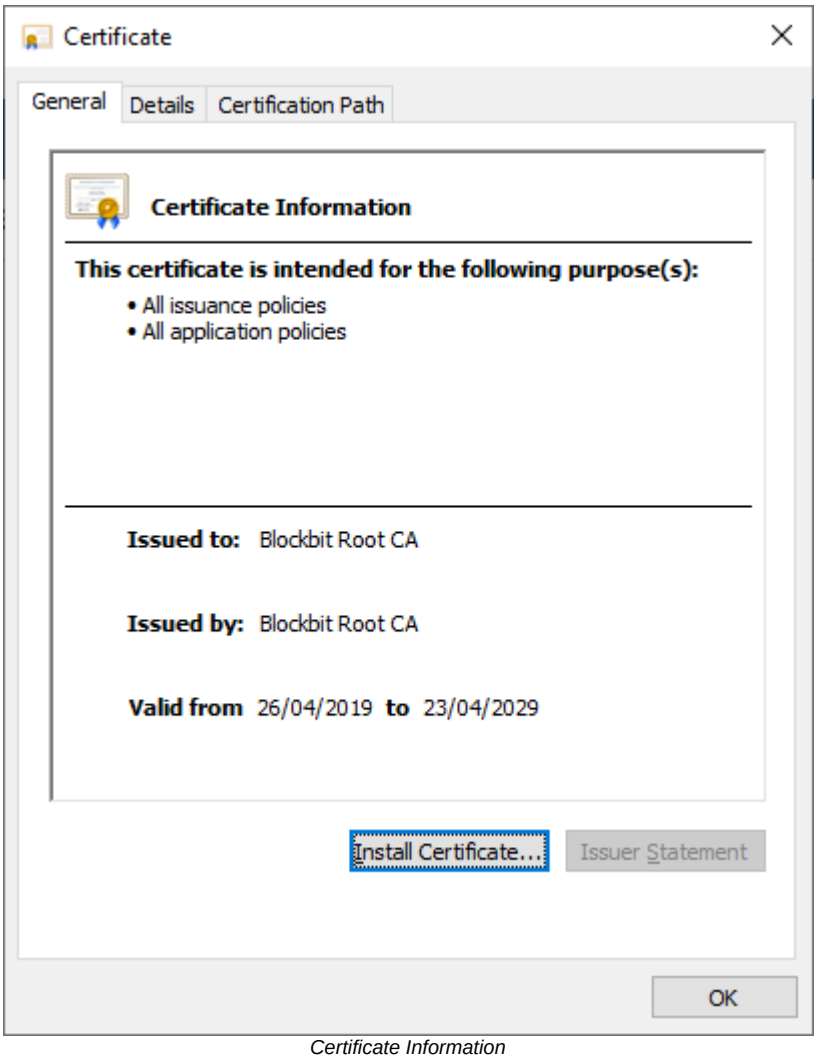
Certificate Import Wizard - Selected Store

Clique no botão **[** Finish **]** para efetuar a importação:



Certificate Import Wizard

Clique no botão **[** OK **]**, a tela de ***certificate information*** será exibida novamente:



Certificate Information

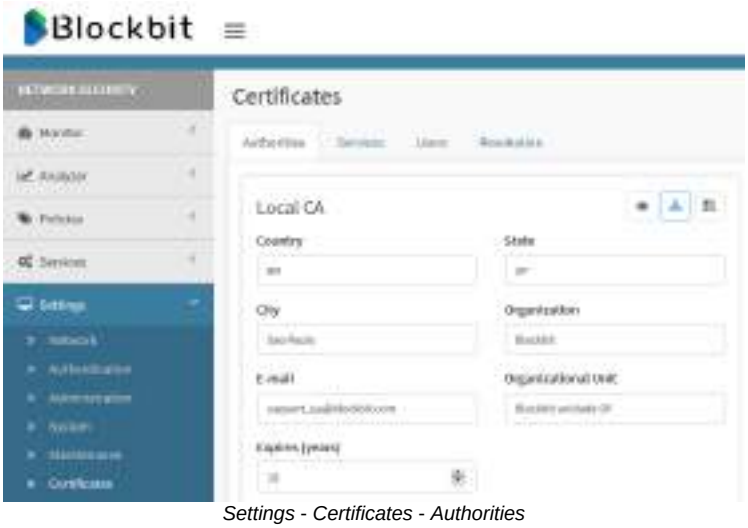
Clique em **[** OK **]** para finalizar a instalação do certificado do usuário.

À seguir vamos detalhar como instalar uma *CA*.

Instalação de *CAs*

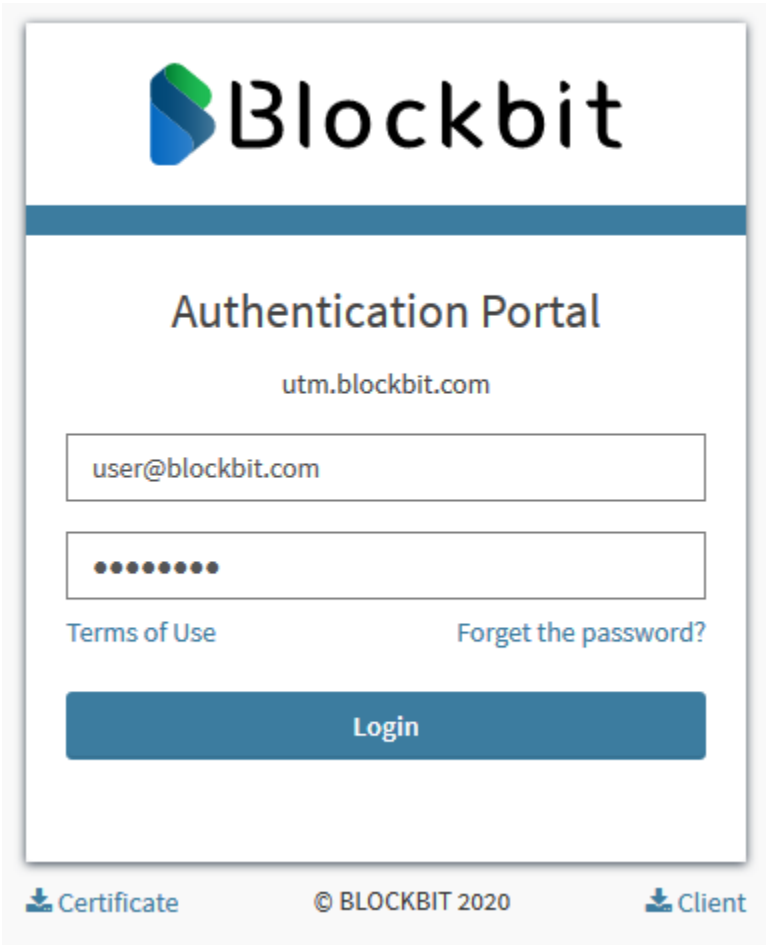
Existem duas formas de baixar a *CA*: Caso seja um administrador, é possível acessar o menu *settings*, opção *certificates,* na aba *authorithies* no UTM (para mais informações, vide esta página).

Feito isso, clique no botão **[** **]**, como demonstrado abaixo:



Settings - Certificates - Authorities

A outra forma de baixar a *CA* é através do *captive portal*, clicando em **[** Certificate **]**:

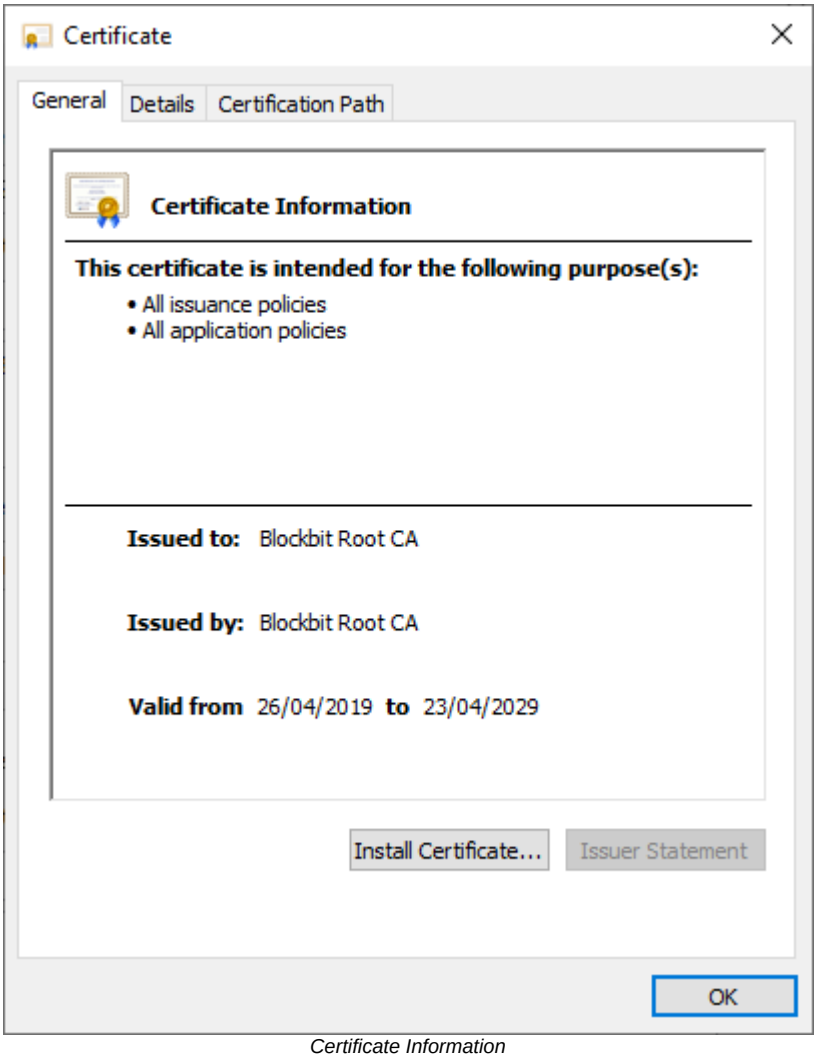


Portal - Certificate

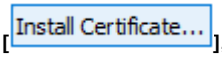
Quando o *download* finalizar, clique no ícone pra abrir o certificado:

Local Root CA

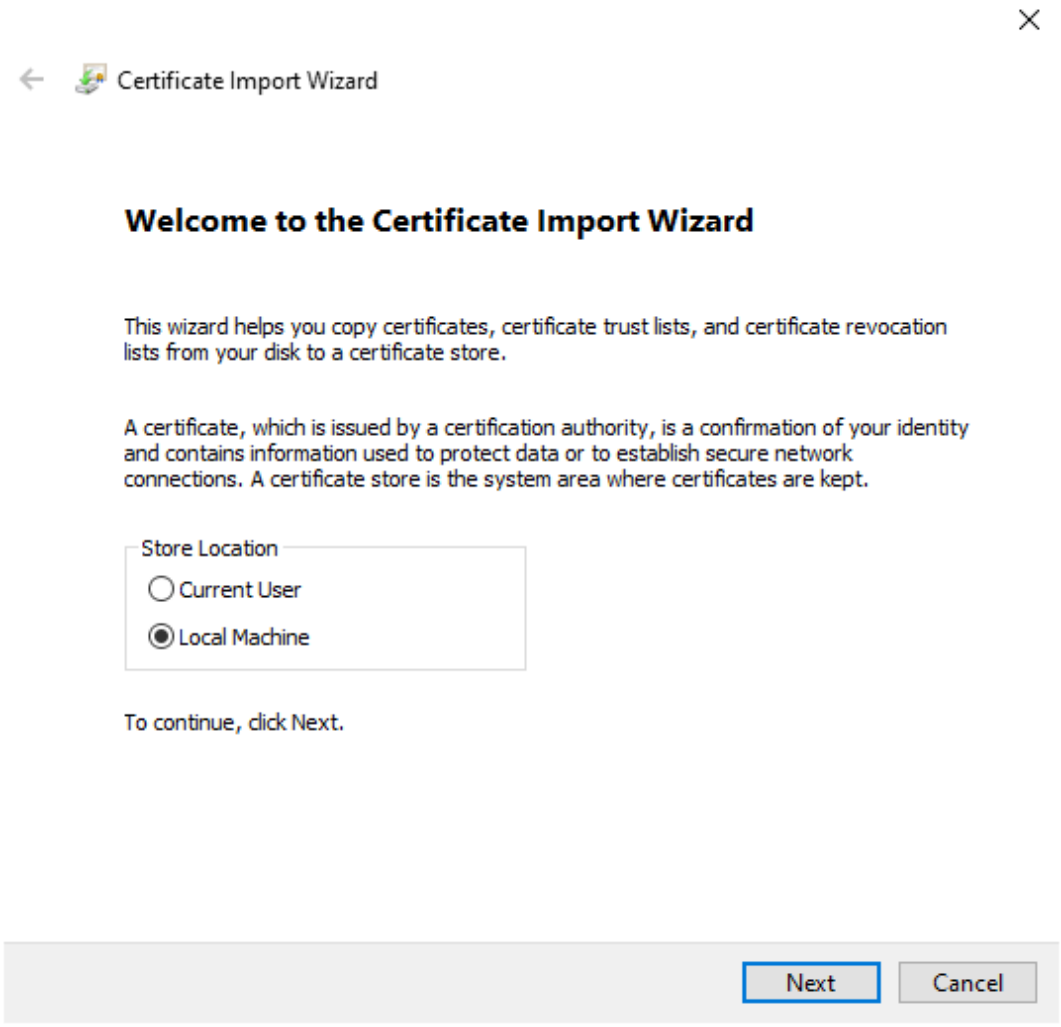
A seguinte janela será exibida:



Certificate Information

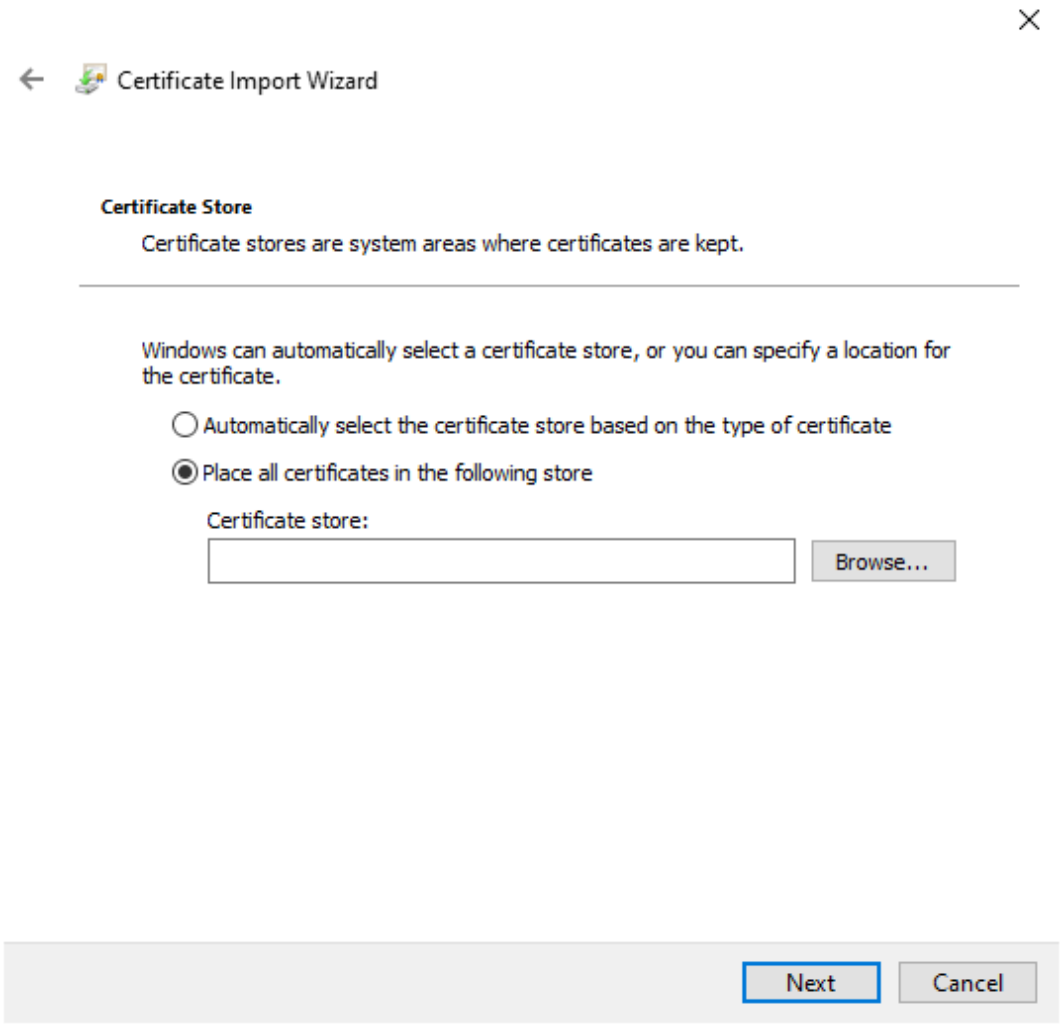
Clique em **[** 

], a seguinte janela será exibida:



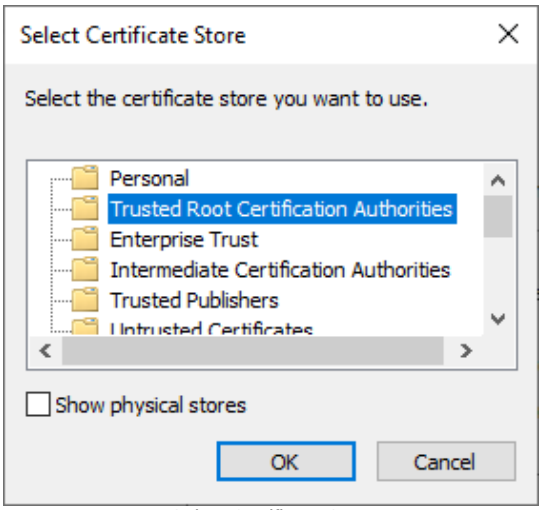
Certificate Import Wizard

Certifique-se que o ***Local Machine*** **[◉]** esteja selecionado e clique no botão **[** Next **]**.



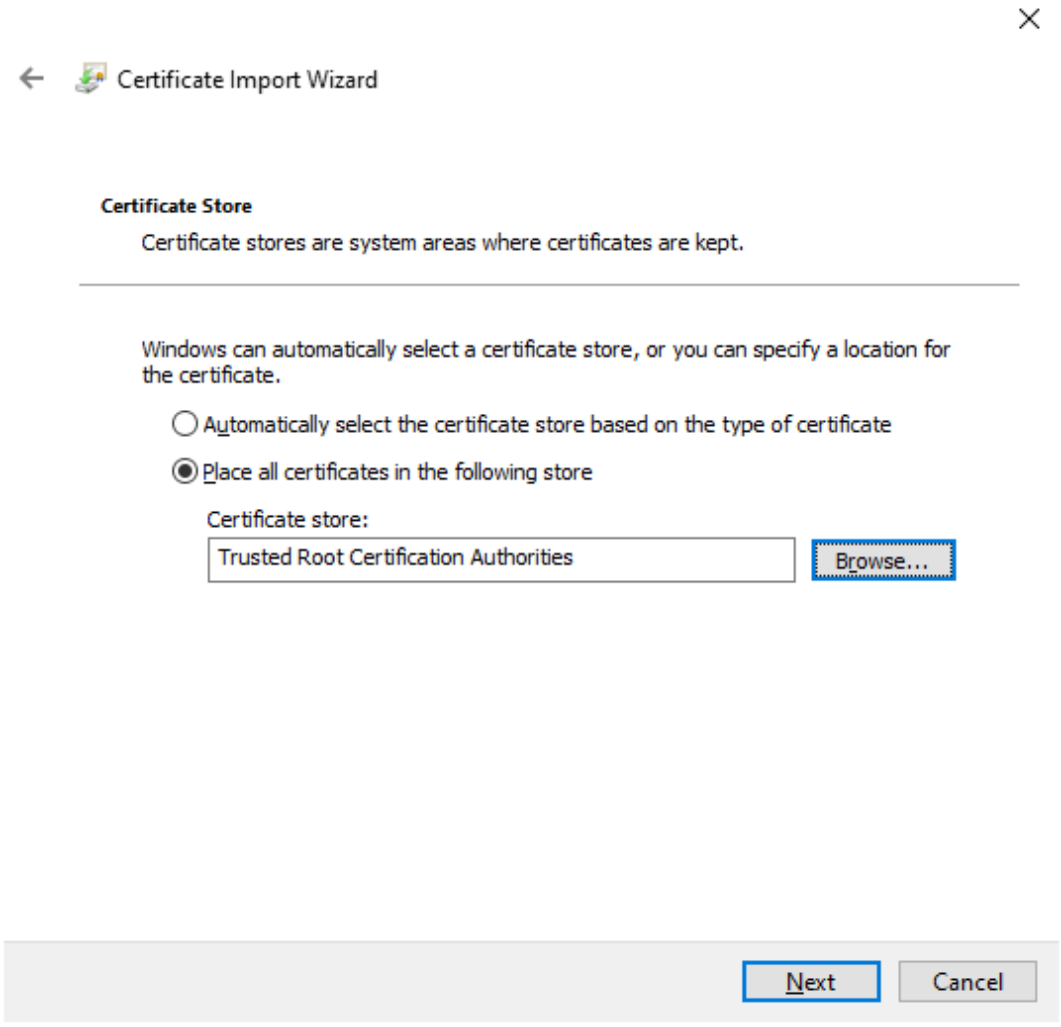
Certificate Store

Selecione a opção ***Place all certificates in the following stores*** **[◉]** e clique no botão **[Browse...]** para selecionar onde o certificado será armazenado, a janela a seguir será exibida:



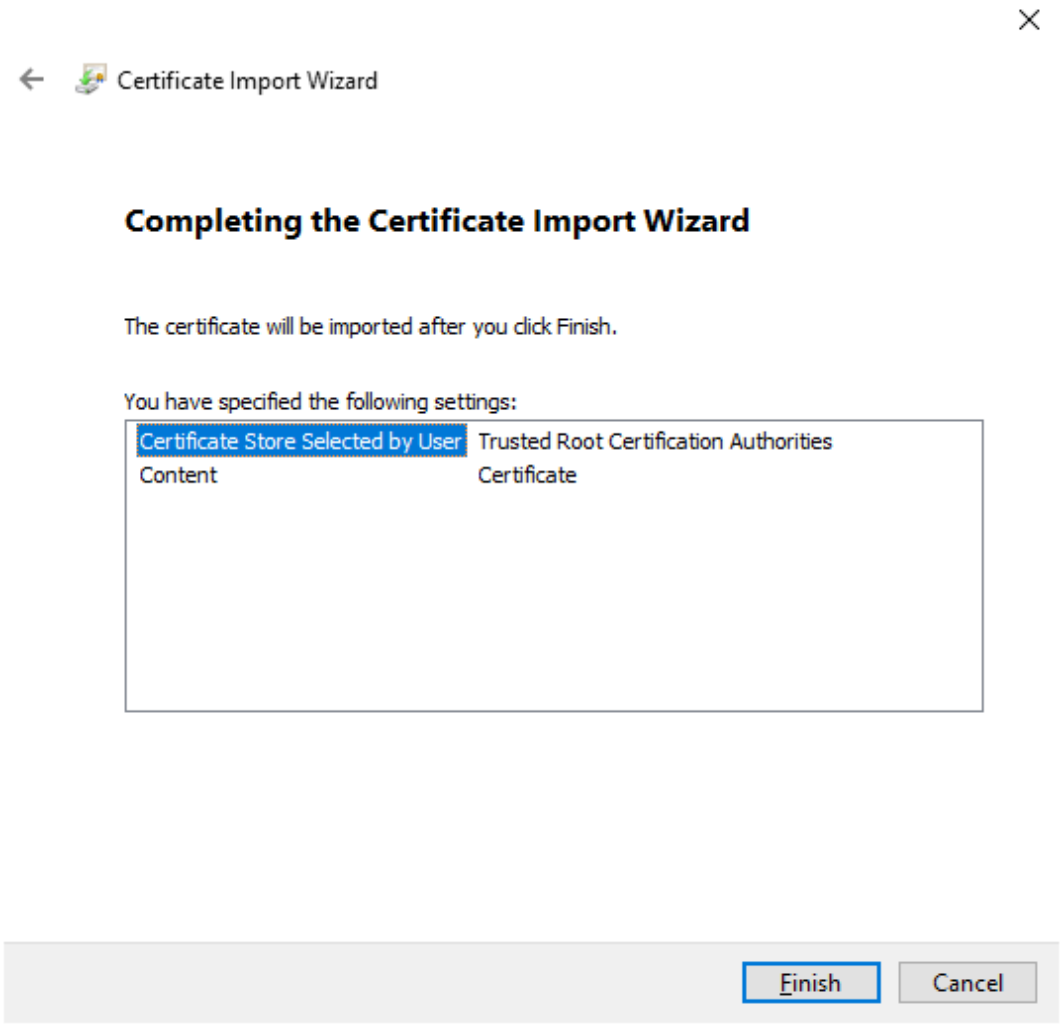
Select Certificate Store

Em *Select Certificate Store,* certifique-se que ***Trusted Root Certification Authorities*** está selecionado e clique em [OK], a tela à seguir será exibida:



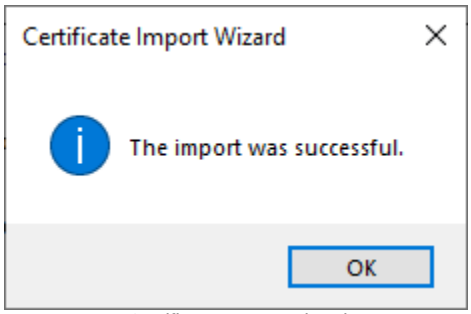
Certificate Store - Selected Store

Clique no botão [Next] a seguinte tela com um resumo da importação do certificado será exibida:



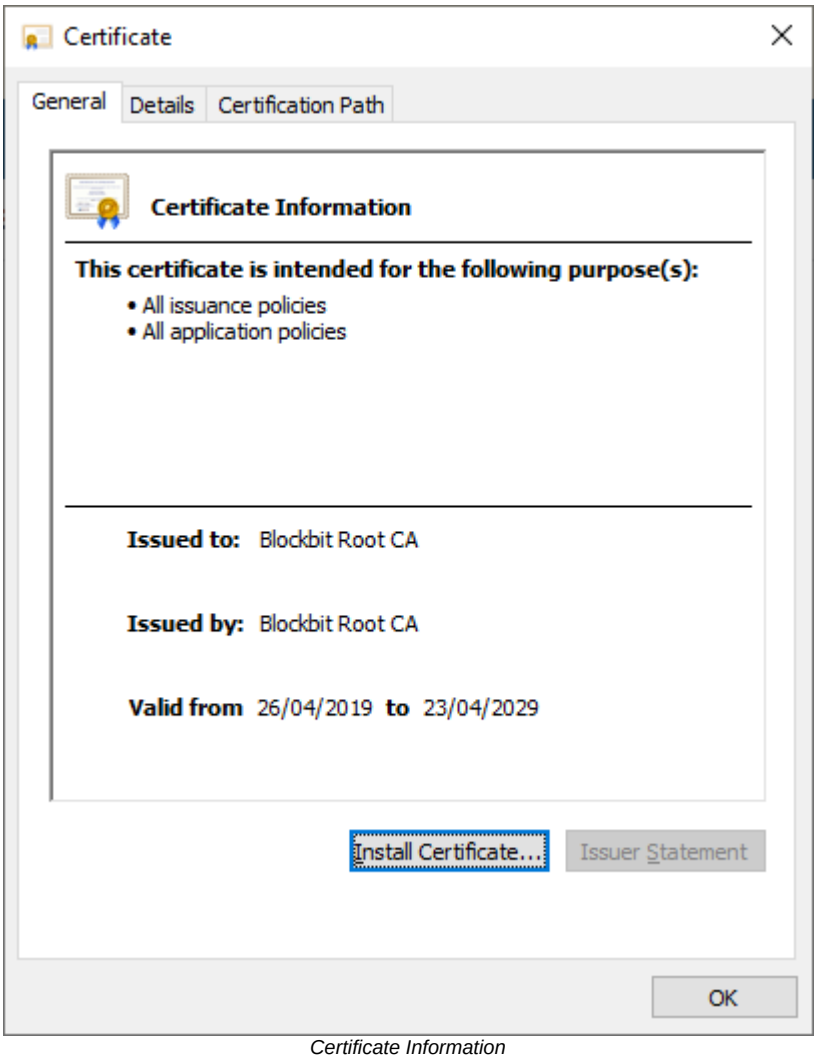
Certificate Import Wizard - Selected Store

Clique no botão **[** Finish **]** para efetuar a importação:



Certificate Import Wizard

Clique no botão **[** OK **]**, a tela de ***certificate information*** será exibida novamente:



Certificate Information

Clique em **[** OK **]** para finalizar a instalação da *CA*.

Isso conclui a instalação dos certificados necessários.

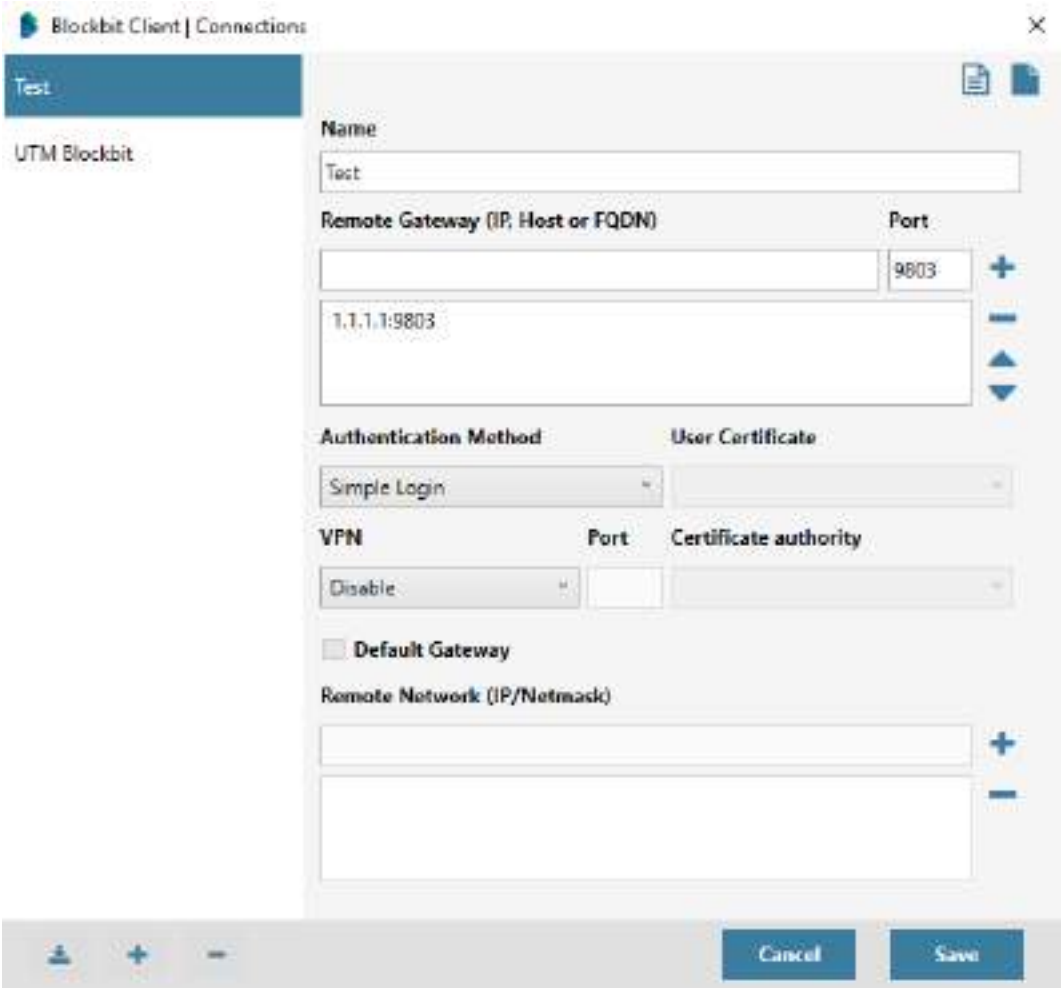
Por fim, de volta no Blockbit Client, basta selecionar no campo *User Certificate* o certificado que foi instalado em ***Personal*** (no passo Instalação de Certificados de Usuário);

E em *Certificate Authority* selecionar o que foi instalado em ***Trusted Root Certification Authorities*** (no passo Instalação de CAs).

Para mais informações a respeito de configuração dos perfis de conexão, consulte esta página.

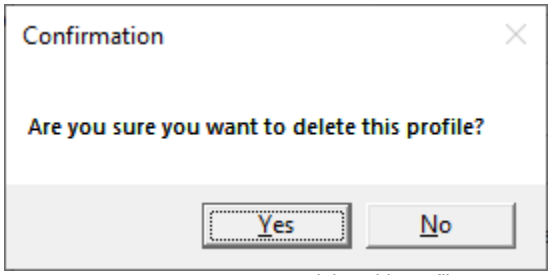
Remoção de Perfil

Para deletar um perfil de conexão, selecione-o no menu à esquerda, conforme demonstrado abaixo:



Blockbit Client - Connections - Selected

Feito isso, clique no botão [ ] localizado no canto inferior esquerdo, a mensagem à seguir será exibida:



Are you sure you want to delete this profile?

Para prosseguir com a deleção, basta clicar em [Yes], caso contrário clique em [No];

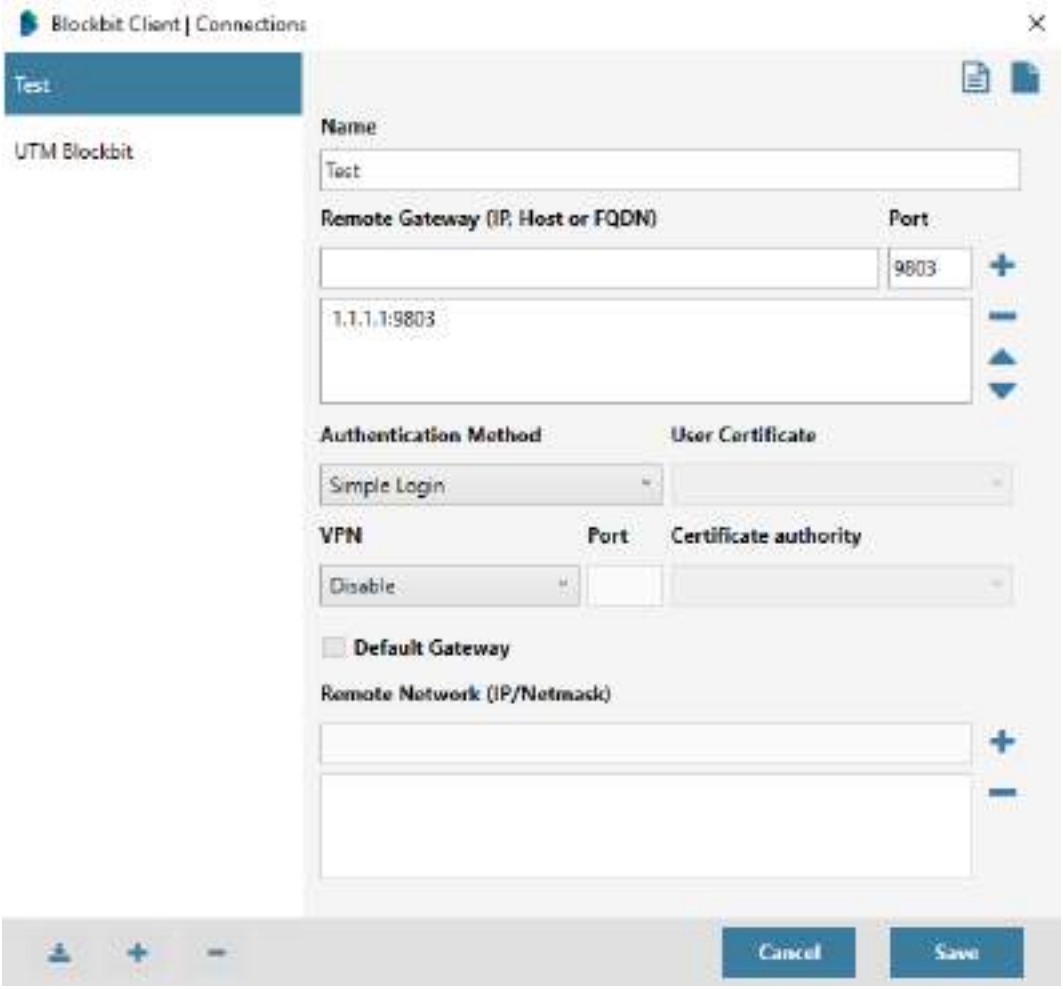
A seguir, vamos analisar como efetuar a Importação e exportação de um Perfil.

Exportação e Importação de Perfil

Nesta página iremos demonstrar o processo de exportação e importação de um perfil de conexão.

Exportação de Perfil

Inicialmente, antes de efetuar a exportação de um perfil, selecione-o no menu lateral à esquerda, conforme demonstrado abaixo:



Blockbit Client - Connections - Selected

Feito isso, ao clicar no ícone **[**  **]** localizado no canto superior direito da janela, um arquivo XML será gerado, salve-o em um local seguro.

O perfil é um arquivo XML contendo as informações adicionadas ao criar o perfil selecionado, segue um exemplo:

Isso conclui o processo de exportação.

À seguir demonstraremos como efetuar a importação deste perfil de conexão.

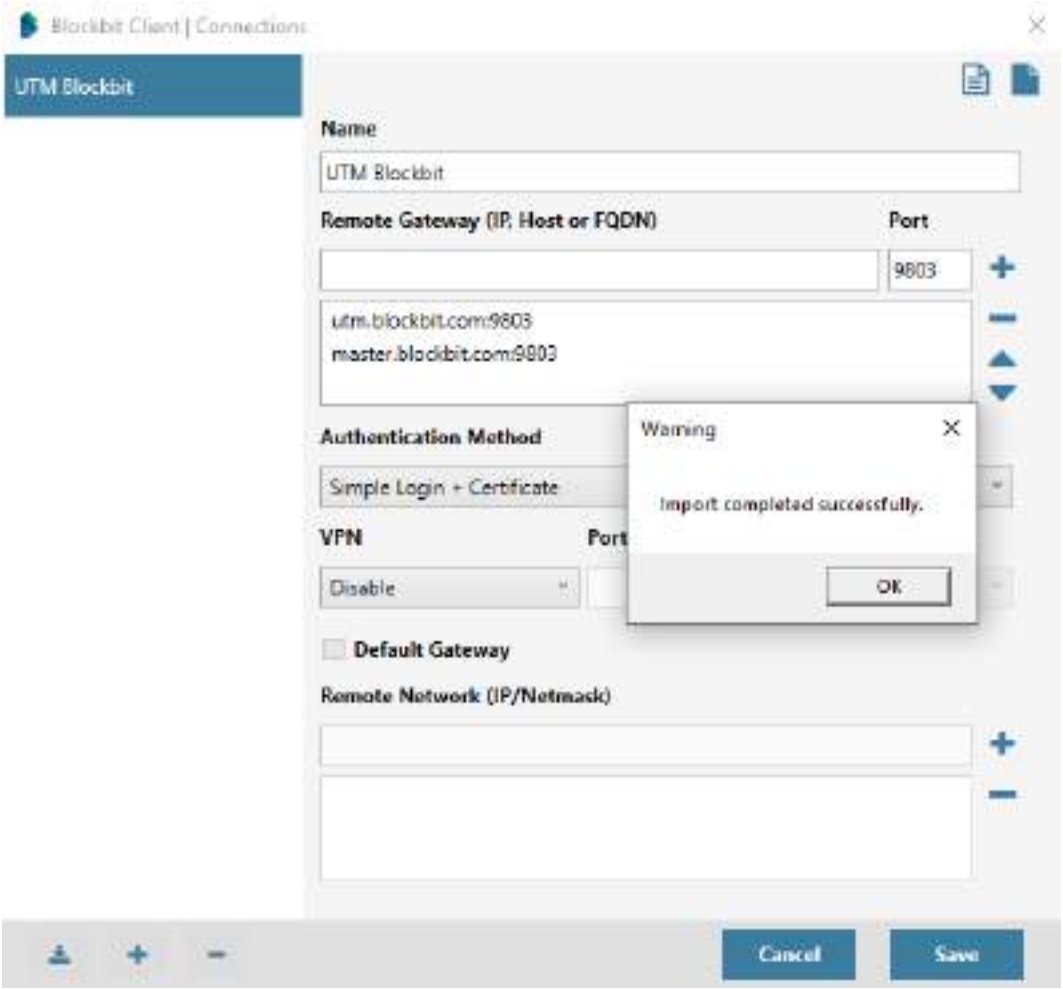
Importação de Perfil

Como faremos a demonstração no mesmo Blockbit Client, iremos remover o perfil "Test" para possibilitar a importação. Para mais informações sobre a remoção de perfis, consulte esta página.

A importação de arquivo XML, contendo certificados, seja de CA ou de usuário (ou ambos), só será possível se os mesmos certificados estiverem instalados na maquina que está realizando a importação, caso contrário a mensagem de erro "Arquivo XML inválido" será exibida.

Para efetuar a importação, clique no ícone **[ ]** localizado no canto inferior esquerdo da janela e basta selecionar o perfil XML que será importado.

Caso o XML tenha A mensagem abaixo será exibida:

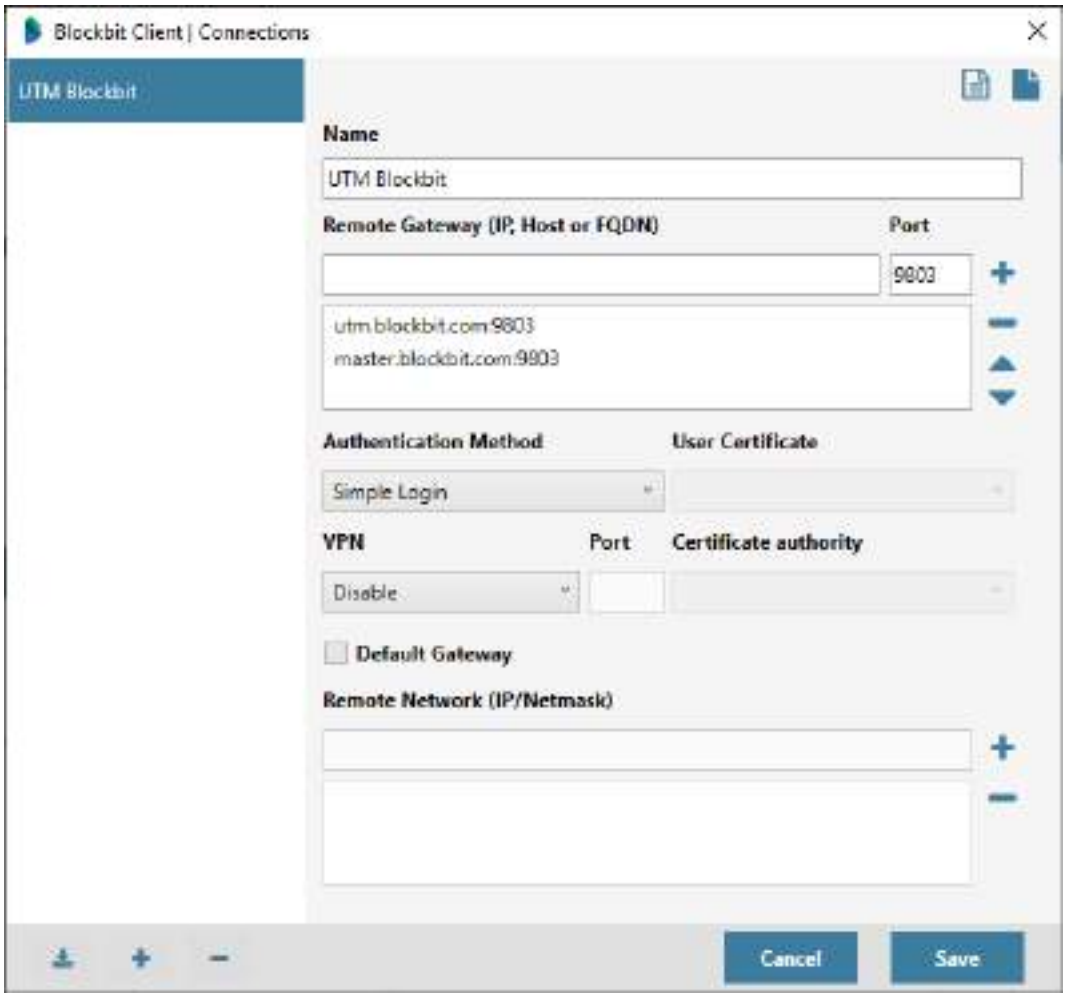


Blockbit Client - Connections - Import Completed Successfully

A seguir, vamos analisar como efetuar a Exportação do log de conexões.

Exportação do log de conexões

Para exportar um log de conexão, selecione o perfil de conexão que se deseja exportar, como exemplificado:



Blockbit Client - Connections - Export Log

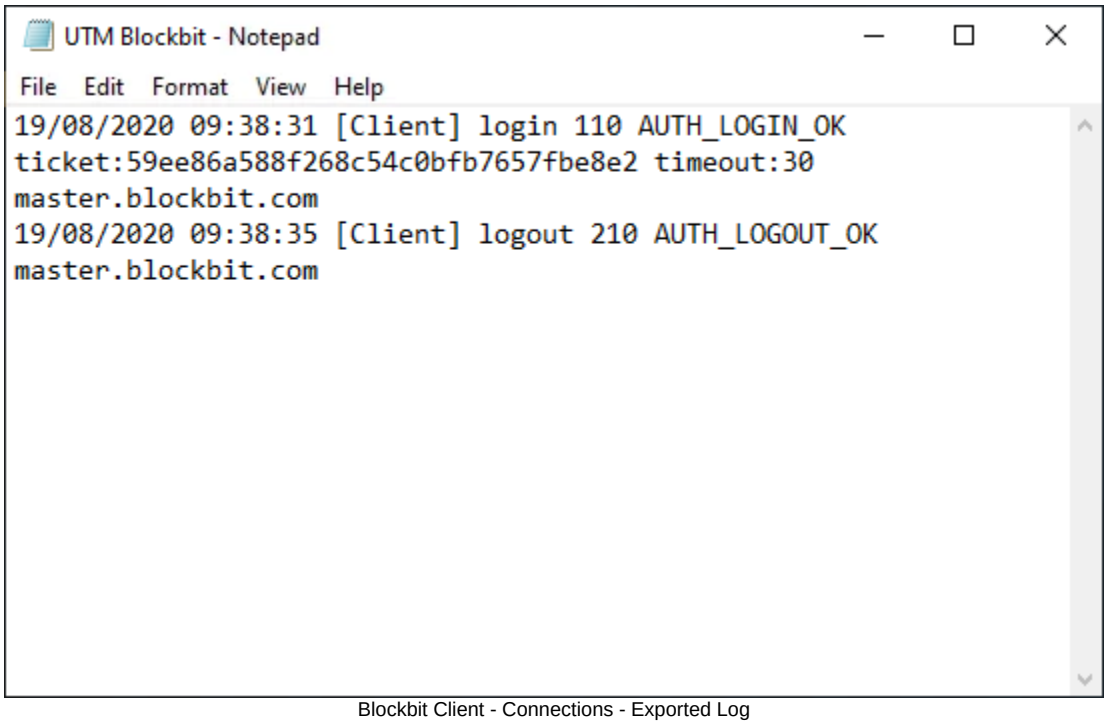
Feito isso, clique no botão **[**  **]** localizado no canto superior direito e salve o *log* em um local seguro.

O *log* é um arquivo de texto com informações referentes aos eventos de conexão do perfil selecionado, em caso de falha de conexão com o gateway, um registro é efetuado no *log*, porém caso a conexão ocorra normalmente, será registrado quando a conexão ocorreu, o *status* da conexão, o evento de autenticação de login (com sucesso) e etc.

Além disso, a cada 30 segundos, o Client faz um *keepalive* enviando uma solicitação para o UTM que foi configurado no perfil de conexão, de modo a checar: A autenticação, o tráfego de dados e caso o usuário continua autenticado. Se o administrador derrubar a autenticação do usuário ou algo ocorrer para que esta conexão seja interrompida, o *keepalive* fazer 5 tentativas para ter certerza que a autenticação está no ar. Caso falhe, o Client derrubará a *vp* . Porém, caso nada de anormal ocorra, o *keepalive* será executado novamente à cada 30 segundos.

ATENÇÃO: Somente o *Client* salva o log apenas da última conexão que foi feita com o perfil selecionado. Isso significa que caso mais de uma tentativa de conexão seja efetuada, o *log* anterior ao da conexão atual será sobrescito.

Segue um exemplo de *Log*:



Blockbit Client - Connections - Exported Log

Além deste recurso, o Blockbit Client também exibe *Logs* no Gerenciador de Eventos do *Windows*.

A seguir, vamos analisar como efetuar uma Conexão usando Blockbit Client.

Exemplos de Configuração

Como forma de demonstrar a gama variada de possibilidades de configuração no Blockbit Client, nesta sessão iremos exibir vários perfis de conexão do Blockbit Client.

Os tipos de perfil de conexão que serão mostrados são:

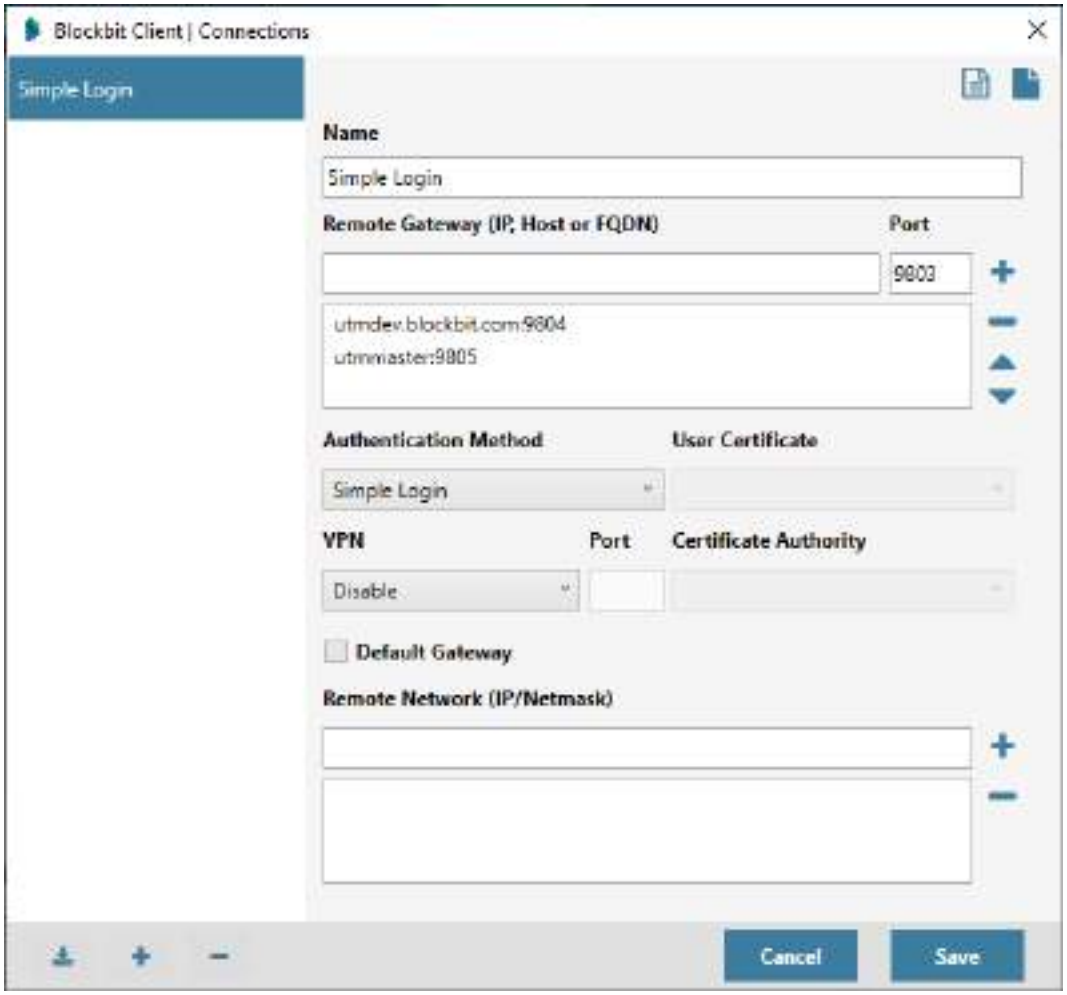
- *Simple Login*;
- Simple Login + Certificate;
- *Windows Login*;
- *Windows Login* + Certificate;
- Simple Login com *VPN SSL*;
- Simple Login + Certificate com *VPN SSL*;
- Simples Login + Certificate com VPN SSL e Remote Network;
- *Login* + Certificate *IPSEC Legacy*;
- *Login* + Certificate *IPSEC Legacy* com *Remote Network*.

Para mais informações a respeito da adição de perfis, consulte esta página.

Simple Login

No método de autenticação *Login Simples*, a autenticação é feita na máquina local (usando o usuário configurado no AD), diferente do *Windows Login*, neste método o usuário deve digitar seu *login* e senha manualmente.

Para configurar um perfil com método de autenticação Login Simples, complete o formulário como indicado abaixo:



Blockbit Client - Login Simples

- ***Name*:** Digite o nome que será utilizado no perfil. Ex.: Simple Login;
- ***Remote Gateway/Port*:** Adicione os gateways remotos e suas respectivas portas. Ex.: utmmaster:9805 e utmdev.blockbit.com:9804;
- ***Authentication Method*:** No método de autenticação, basta selecionar a opção "*Simple Login*".

Para concluir, clique em [Save] caso contrário, clique em [Cancel] desfazer essas configurações.

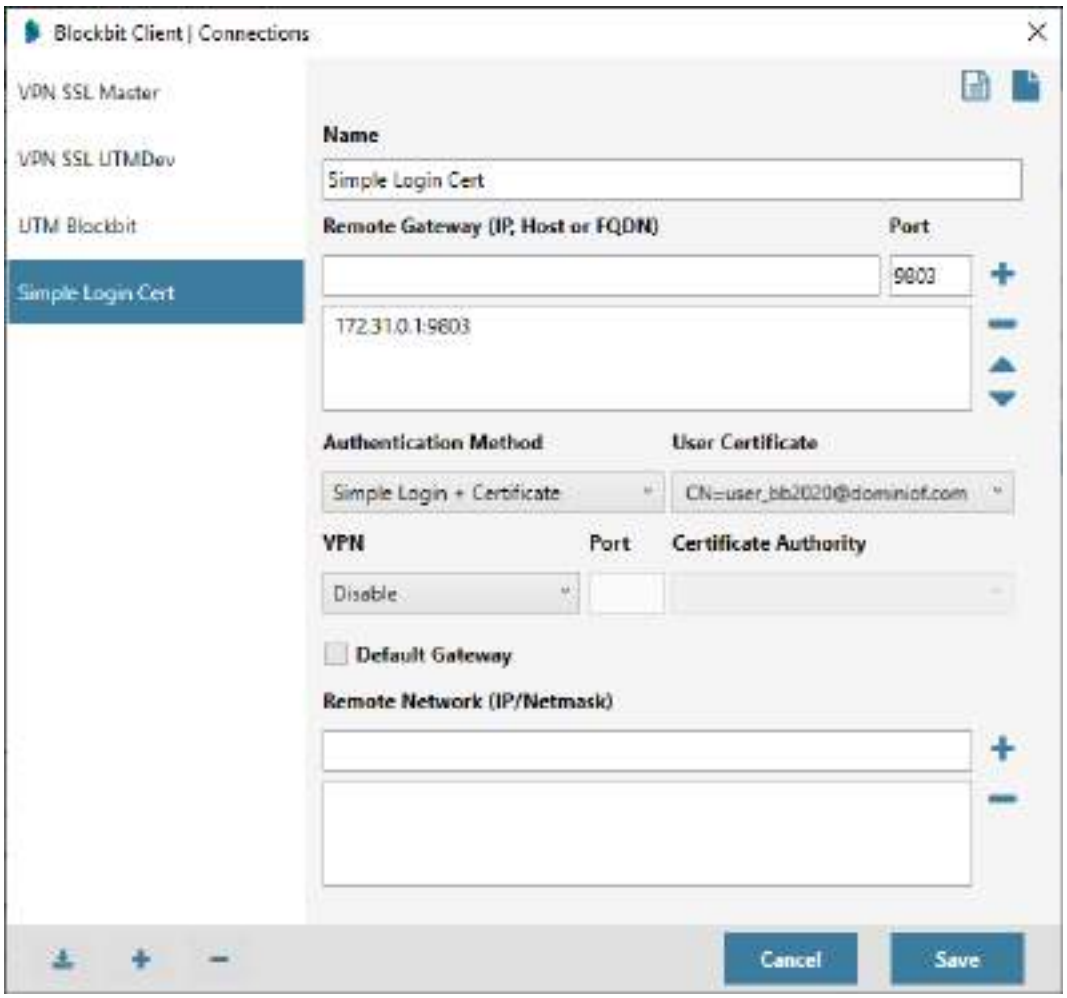
Para visualizar outros exemplos de configuração, consulte esta página.

Simple Login + Certificate

O método de autenticação *Login Simples* + Certificado atua como o método *Windows Login*, porém para que o certificado seja exibido no campo, o usuário precisará entrar no portal, gerar seu certificado e instalá-lo como Usuário Atual (não na máquina local).

Para que o UTM passe a exigir o certificado na autenticação é necessário acessar o menu *Settings,* clicar na opção *Authentication* e na aba *Settings* marcar a caixa de seleção *Verify user certificate*. Após habilitar esta opção, basta dar um *Apply* para que todas as vezes que o *Client* tentar fazer autenticação com o UTM o certificado seja exigido.

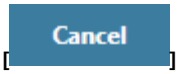
Para configurar um perfil com método de autenticação *Login* Simples + Certificado, complete o formulário como indicado abaixo:



Blockbit Client - Login Simples+Certificado

Para mais informações a respeito de como efetuar a instalação de certificados, consulte esta página.

- ***Name*:** Digite o nome que será utilizado no perfil. Ex.: Simple Login Cert;
- ***Remote Gateway/Port*:** Adicione os gateways remotos e suas respectivas portas. Ex.: 172.31.0.1:9803;
- ***Authentication Method*:** No método de autenticação, basta selecionar a opção "*Simple Login + Certificate*";
- **User Certificate:** Selecione o certificado que o usuário utilizará neste perfil de conexão.

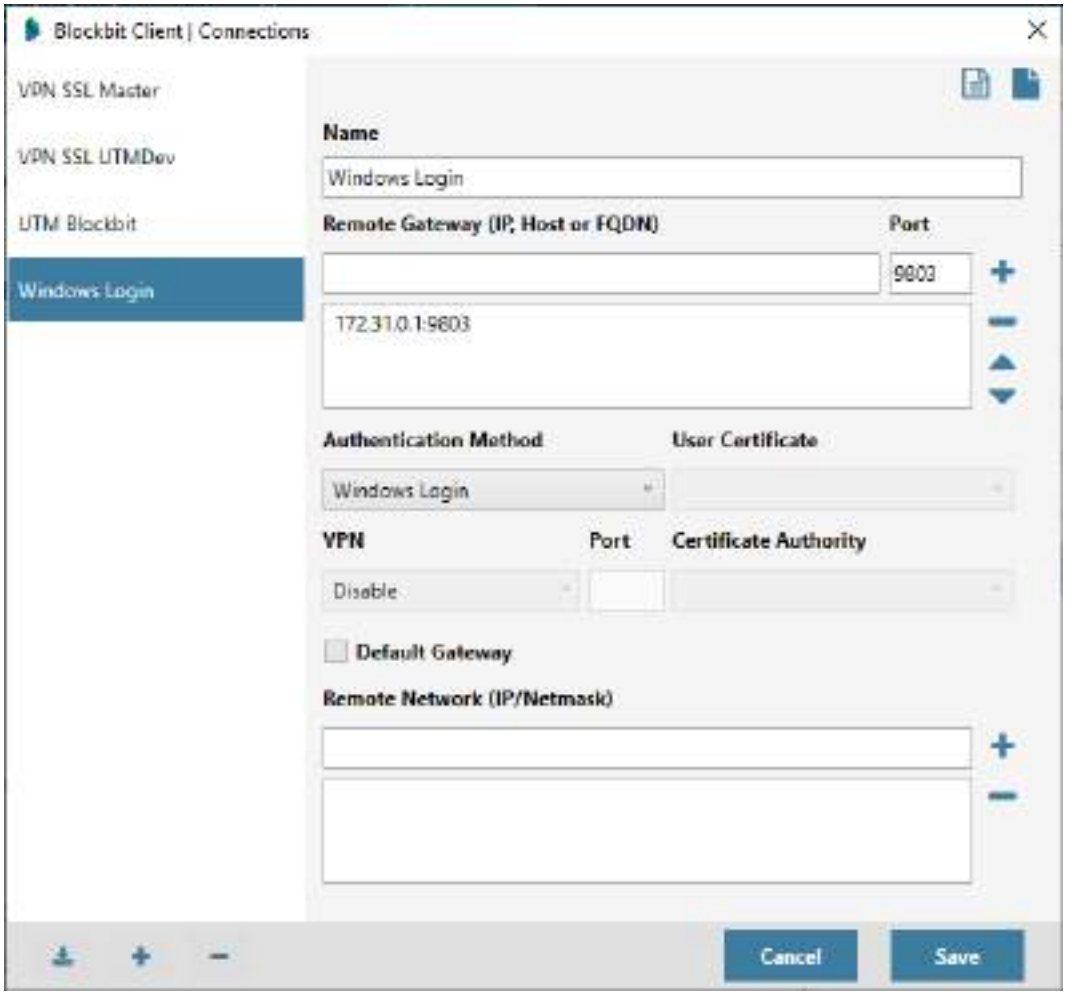
Para concluir, clique em **[**  **]** caso contrário, clique em **[**  **]** desfazer essas configurações.

Para visualizar outros exemplos de configuração, consulte esta página.

Windows Login

No método de autenticação *Windows Login*, a autenticação é feita na máquina local (usa-se o usuário configurado no AD), este método de autenticação não exige a senha durante o *login*.

Para configurar, complete o formulário como indicado abaixo:



Blockbit Client - Windows Login

- ***Name*:** Digite o nome que será utilizado no perfil. Ex.: Windows Login;
- ***Remote Gateway/Port*:** Adicione os gateways remotos e suas respectivas portas. Ex.: 172.31.0.1:9803;
- ***Authentication Method*:** No método de autenticação, basta selecionar a opção "*Windows Login*".

Para concluir, clique em **[** Save **]** caso contrário, clique em **[** Cancel **]** desfazer essas configurações.

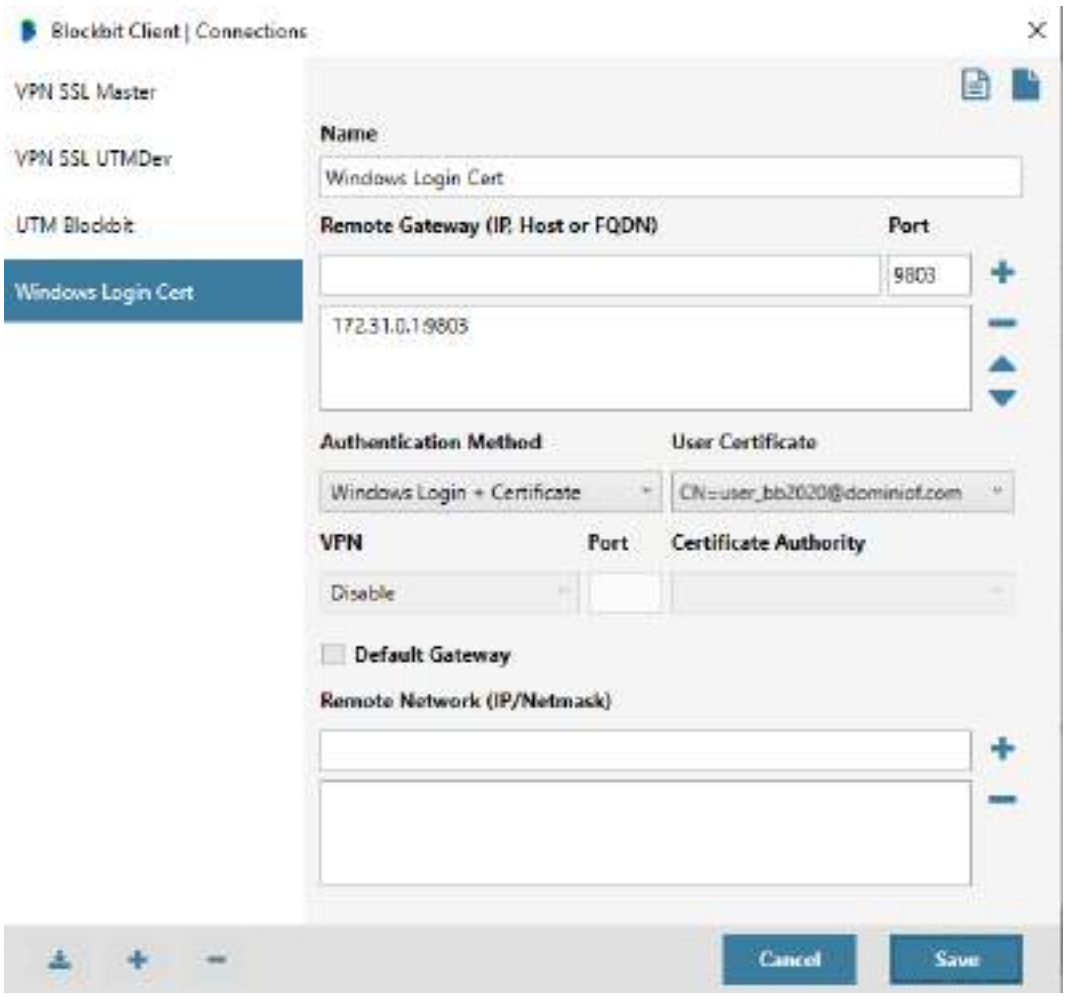
Para visualizar outros exemplos de configuração, consulte esta página.

Windows Login + Certificate

O método de autenticação *Windows Login* + Certificado atua como o método *Windows Login*, porém para que o certificado seja exibido no campo, o usuário precisará entrar no portal, gerar seu certificado e instalá-lo como Usuário Atual (não na máquina local).

Para que o UTM passe a exigir o certificado na autenticação é necessário acessar o menu *Settings,* clicar na opção *Authentication* e na aba *Settings* marcar a caixa de seleção *Verify user certificate*. Após habilitar esta opção, basta dar um *Apply* para que todas as vezes que o *Client* tentar fazer autenticação com o UTM o certificado seja exigido.

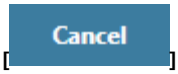
Para configurar um perfil com método de autenticação *Windows Login* + Certificado , complete o formulário como indicado abaixo:



Blockbit Client - Windows Login + Certificado

Para mais informações a respeito de como efetuar a instalação de certificados, consulte esta página.

- ***Name*:** Digite o nome que será utilizado no perfil. Ex.: Windows Login Cert;
- ***Remote Gateway/Port*:** Adicione os gateways remotos e suas respectivas portas. Ex.: 172.31.0.1:9803;
- ***Authentication Method*:** No método de autenticação, basta selecionar a opção "*Windows Login + Certificate*";
- **User Certificate:** Selecione o certificado que o usuário utilizará neste perfil de conexão.

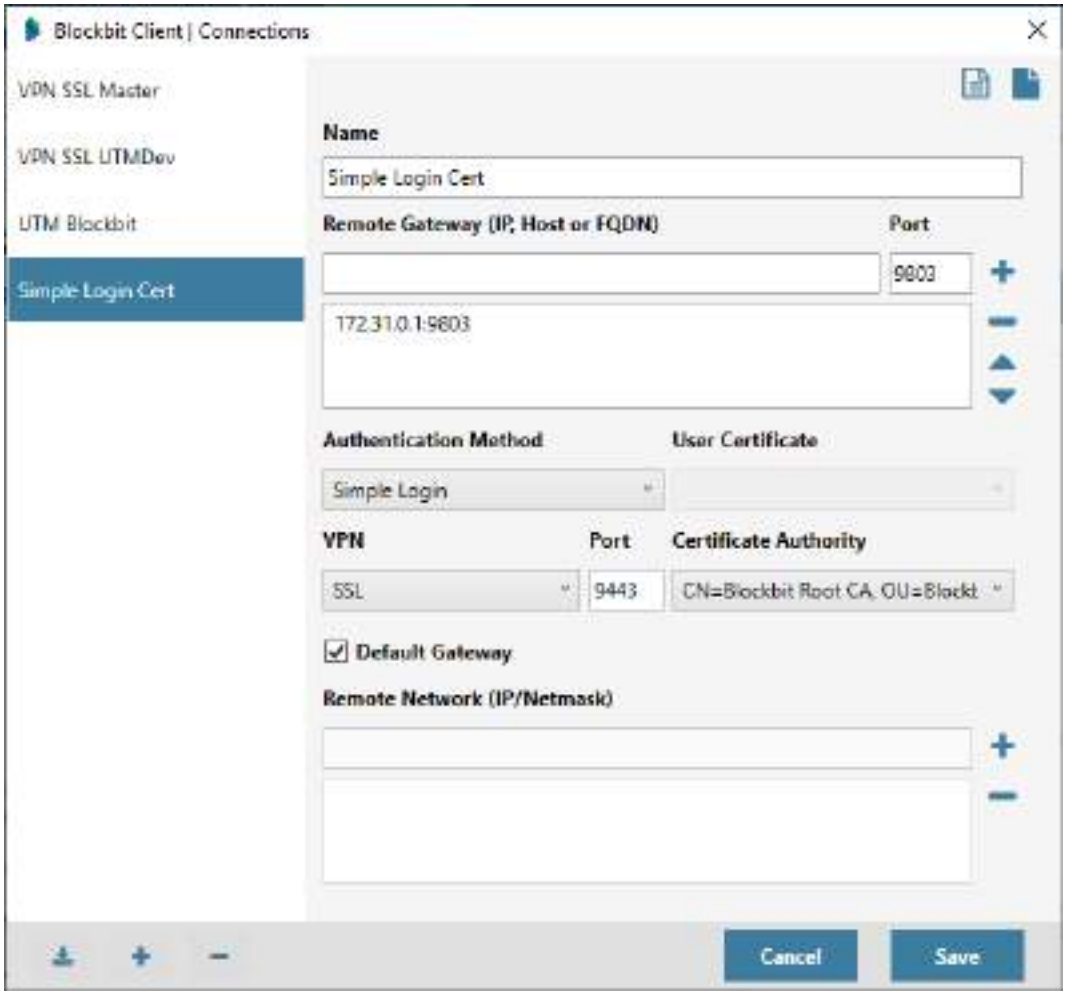
Para concluir, clique em **[**  **]** caso contrário, clique em **[**  **]** desfazer essas configurações.

Para visualizar outros exemplos de configuração, consulte esta página.

Simple Login com VPN SSL

Para mais informações a respeito de como o *Login* Simples funciona, consulte esta página. Ao utilizar esse método de autenticação, é possível configurar a *VPN SSL*, a porta padrão a ser utilizada é a 9443 (que pode ser alterada) e para usar o SSL será necessário instalar a *CA* como Autoridade Confiável, para mais informações, consulte esta página.

Para configurar um perfil com método de autenticação "Login Simples com VPN SSL", complete o formulário como indicado abaixo:

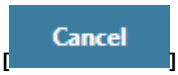


Blockbit Client - Login Simples com VPN SSL

Para mais informações a respeito de como efetuar a instalação de certificados, consulte esta página.

- ***Name*:** Digite o nome que será utilizado no perfil. Ex.: Simple Login Cert;
- ***Remote Gateway/Port*:** Adicione os gateways remotos e suas respectivas portas. Ex.: 172.31.0.1:9803;
- ***Authentication Method*:** No método de autenticação, basta selecionar a opção "*Simple Login*";
- ***VPN*:** Selecione a opção "SSL";
- ***Port*:** Adicionar a porta que será utilizada. Neste caso usaremos a porta padrão. Ex.: 9443;
- ***Certificate Authority*:** Selecionar a *CA* que será utilizada. Ele precisa estar instalado na máquina do usuário;
- ***Default Gateway* [☑]:** Habilite esta caixa de seleção para que somente 172.31.0.1:9803 seja roteado pela *VPN*.

Para concluir, clique em [

] caso contrário, clique em [

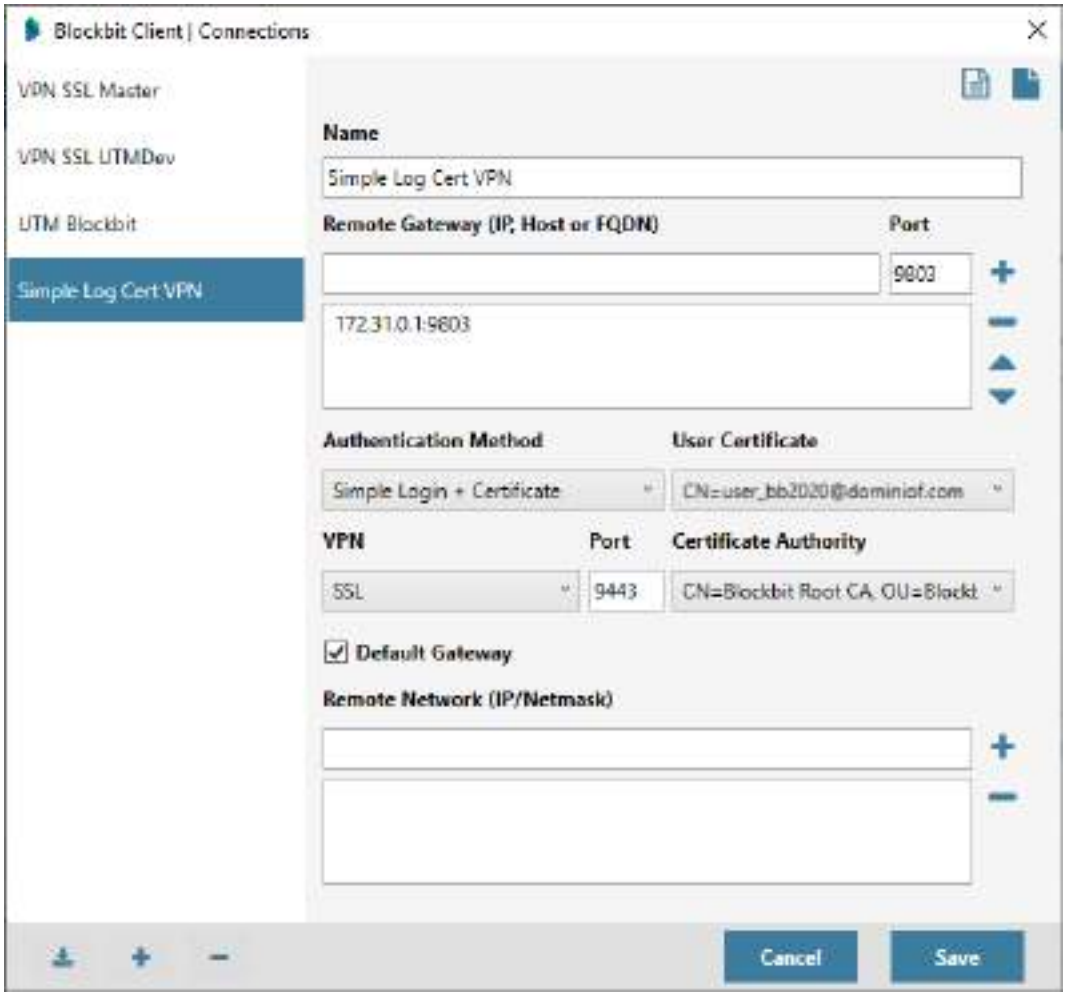
] desfazer essas configurações.

Para visualizar outros exemplos de configuração, consulte esta página.

Simple Login + Certificate com VPN SSL

Para mais informações a respeito de como o *Login* Simples com Certificado funciona, consulte esta página. Ao utilizar esse método de autenticação, é possível configurar a *VPN SSL*, a porta padrão a ser utilizada é a 9443 (que pode ser alterada) e para usar o SSL será necessário instalar a *CA* como Autoridade Confiável, para mais informações, consulte esta página.

Para configurar um perfil com método de autenticação "Login Simples + Certificado com VPN SSL", complete o formulário como indicado abaixo:



Blockbit Client - Login Simples + Certificado com VPN SSL

Para mais informações a respeito de como efetuar a instalação de certificados, consulte esta página.

- ***Name*:** Digite o nome que será utilizado no perfil. Ex.: Simple Log Cert VPN;
- ***Remote Gateway/Port*:** Adicione os gateways remotos e suas respectivas portas. Ex.: 172.31.0.1:9803;
- ***Authentication Method*:** No método de autenticação, basta selecionar a opção "*Simple Login + Certificate*";
- **User Certificate:** Selecione o certificado que o usuário utilizará neste perfil de conexão;
- ***Certificate Authority*:** Selecionar a *CA* que será utilizada. Ele precisa estar instalado na máquina do usuário;
- **VPN:** Selecione a opção "SSL";
- ***Port*:** Adicionar a porta que será utilizada. Neste caso usaremos a porta padrão. Ex.: 9443;
- **Default Gateway [☑]:** Habilite esta caixa de seleção para que somente 172.31.0.1:9803 seja roteado pela *VPN*.

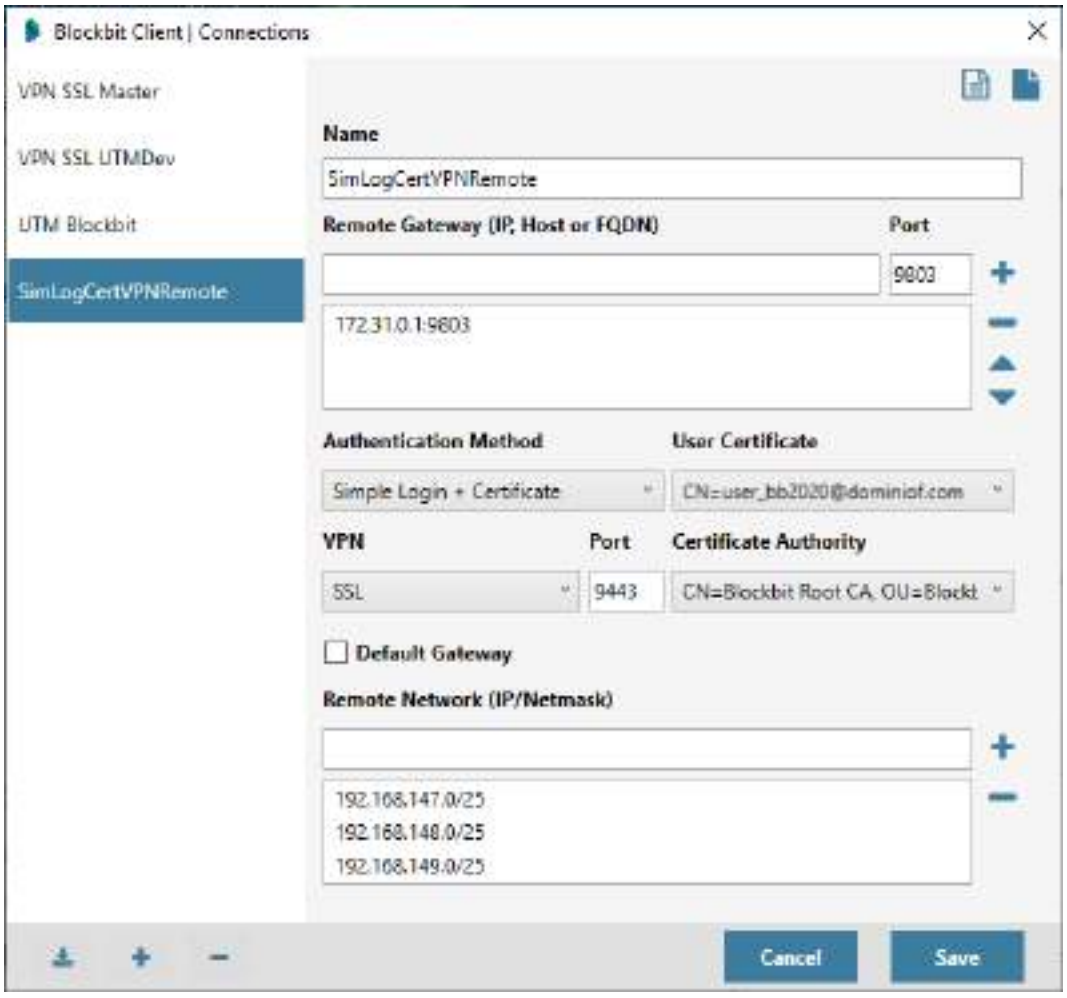
Para concluir, clique em [Save] caso contrário, clique em [Cancel] desfazer essas configurações.

Para visualizar outros exemplos de configuração, consulte esta página.

Simples Login + Certificate com VPN SSL e Remote Network

Para mais informações a respeito de como o *Login* Simples com Certificado funciona, consulte esta página. Ao utilizar esse método de autenticação, é possível configurar a *VPN SSL*, a porta padrão a ser utilizada é a 9443 (que pode ser alterada) e para usar o SSL será necessário instalar a *CA* como Autoridade Confiável, para mais informações, consulte esta página.

Para configurar um perfil com método de autenticação "Login Simples + Certificado com VPN SSL e Remote Network", complete o formulário como indicado abaixo:

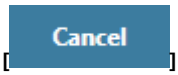


Blockbit Client - Login Simples + Certificado com VPN SSL e Remote Network

Para mais informações a respeito de como efetuar a instalação de certificados, consulte esta página.

- ***Name*:** Digite o nome que será utilizado no perfil. Ex.: SimLogCertVPNRemote;
- ***Remote Gateway/Port*:** Adicione os gateways remotos e suas respectivas portas. Ex.: 172.31.0.1:9803;
- ***Authentication Method*:** No método de autenticação, basta selecionar a opção "*Simple Login + Certificate*";
- **User Certificate:** Selecione o certificado que o usuário utilizará neste perfil de conexão;
- ***Certificate Authority*:** Selecionar a *CA* que será utilizada. Ele precisa estar instalado na máquina do usuário;
- **VPN:** Selecione a opção "SSL";
- ***Port*:** Adicionar a porta que será utilizada. Neste caso usaremos a porta padrão. Ex.: 9443;
- **Remote Network:** Adicione as redes remotas que serão utilizadas. Ex.: 192.168.149.0/25, 192.168.148.0/25 e 192.168.147.0/25.

Para concluir, clique em [

] caso contrário, clique em [

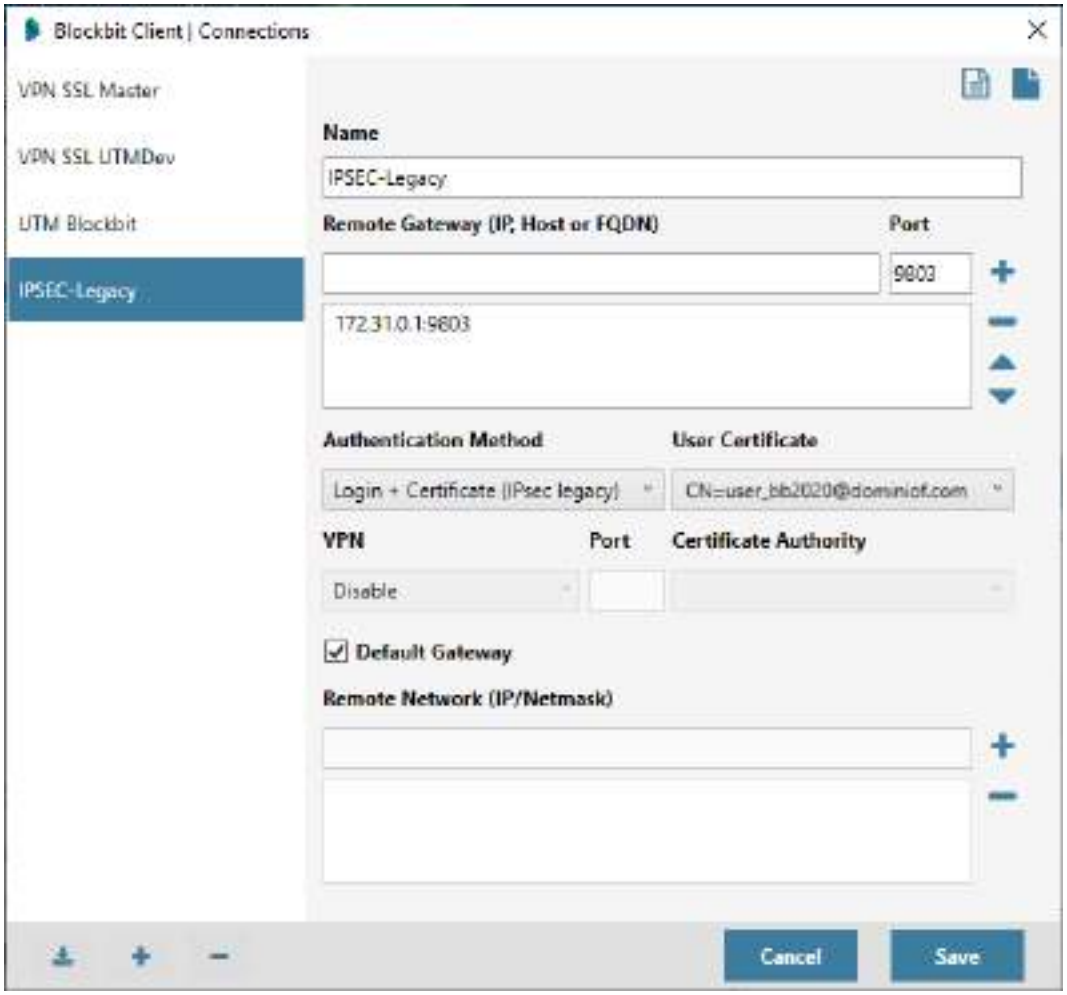
] desfazer essas configurações.

Para visualizar outros exemplos de configuração, consulte esta página.

Login + Certificate IPSEC Legacy

O método de autenticação *Login* com Certificado *IPSEC Legacy* efetua basicamente o mesmo processo que foi feito no *SSL*, porém para que o certificado seja exibido no campo, o usuário precisará entrar no portal, gerar sua CA e instalá-la como Máquina Local (não como Usuário Atual).

Para configurar um perfil com método de autenticação "Login + Certificado IPSEC Legacy", complete o formulário como indicado abaixo:



Blockbit Client - Login + Certificado IPSEC Legacy

Para mais informações a respeito de como efetuar a instalação de certificados, consulte esta página.

- ***Name*:** Digite o nome que será utilizado no perfil. Ex.: IPSEC-Legacy;
- ***Remote Gateway/Port*:** Adicione os gateways remotos e suas respectivas portas. Ex.: 172.31.0.1:9803;
- ***Authentication Method*:** No método de autenticação, basta selecionar a opção "*Login + Certificate (IPSEC Legacy)*";
- **User Certificate:** Selecione o certificado que o usuário utilizará neste perfil de conexão.

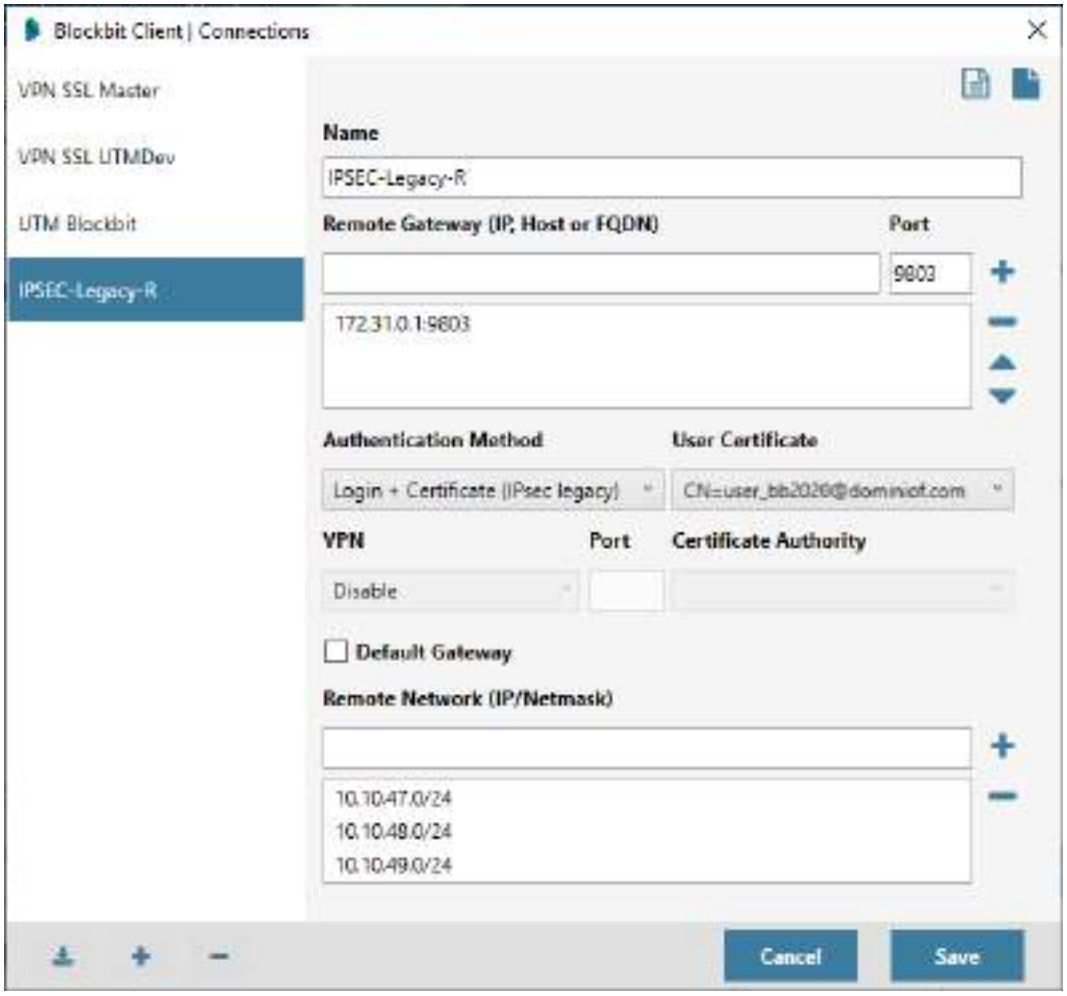
Para concluir, clique em [Save] caso contrário, clique em [Cancel] desfazer essas configurações.

Para visualizar outros exemplos de configuração, consulte esta página.

Login + Certificate IPSEC Legacy com Remote Network

O método de autenticação *Login* com Certificado *IPSEC Legacy* efetua basicamente o mesmo processo que foi feito no *SSL*, porém para que o certificado seja exibido no campo, o usuário precisará entrar no portal, gerar sua CA e instalá-la como Máquina Local (não como Usuário Atual).

Para configurar um perfil com método de autenticação "Login + Certificado IPSEC Legacy com Remote Network", complete o formulário como indicado abaixo:



Blockbit Client - Login + Certificado IPSEC Legacy com Remote Network

Para mais informações a respeito de como efetuar a instalação de certificados, consulte esta página.

- ***Name*:** Digite o nome que será utilizado no perfil. Ex.: IPSEC-Legacy-R;
- ***Remote Gateway/Port*:** Adicione os gateways remotos e suas respectivas portas. Ex.: 172.31.0.1:9803;
- ***Authentication Method*:** No método de autenticação, basta selecionar a opção "*Login + Certificate (IPSEC Legacy)*";
- **User Certificate:** Selecione o certificado que o usuário utilizará neste perfil de conexão;
- **VPN:** Selecione a opção "IPSEC";
- **Remote Network:** Adicione as redes remotas que serão utilizadas. Ex.: 10.10.49.0/32, 10.10.48.0/32 e 10.10.47.0/32.

Para concluir, clique em [Save] caso contrário, clique em [Cancel] desfazer essas configurações.

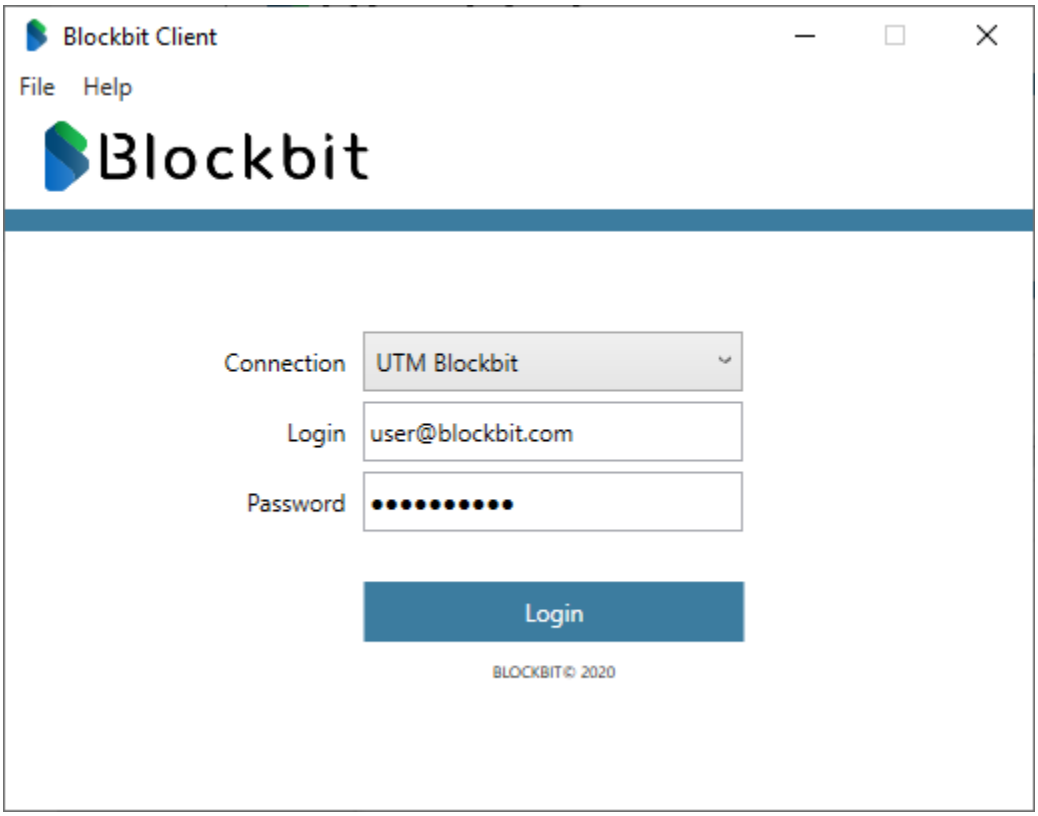
Para visualizar outros exemplos de configuração, consulte esta página.

Conexão usando Blockbit Client

Após criar e salvar o perfil de conexão, o usuário será automaticamente redirecionado para a tela inicial, conforme demonstrado abaixo:

Tela de *Login*

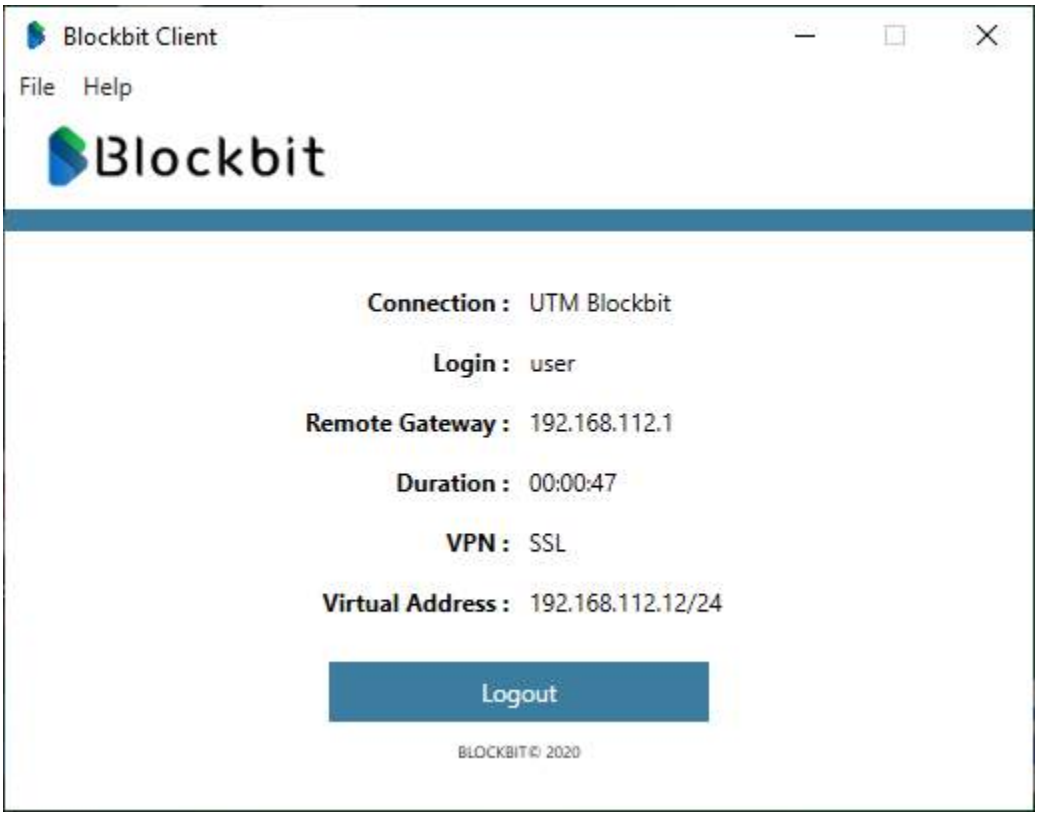
Complete os campos como exemplificado:



Tela de *Login* - Completa

- ***Connection*:** Selecione o perfil de conexão desejado. Por exemplo, o perfil criado na sessão anterior. Ex.: *UTM Blockbit*;
- ***Login*:** Digite o *login* que será utilizado na conexão. Ex.: user@blockbit.com;
- ***Password*:** Digite o *password* que será utilizado na conexão. Ex.: q1Q!q1Q!.

Para efetuar a conexão, clique em [Login], caso a autenticação tenha sido efetuada com sucesso, a tela abaixo será exibida.

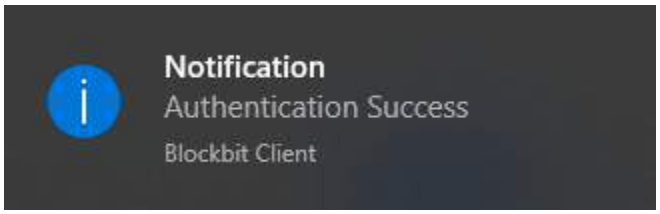


Blockbit Client - Conectado

As informações exibidas nesta tela são:

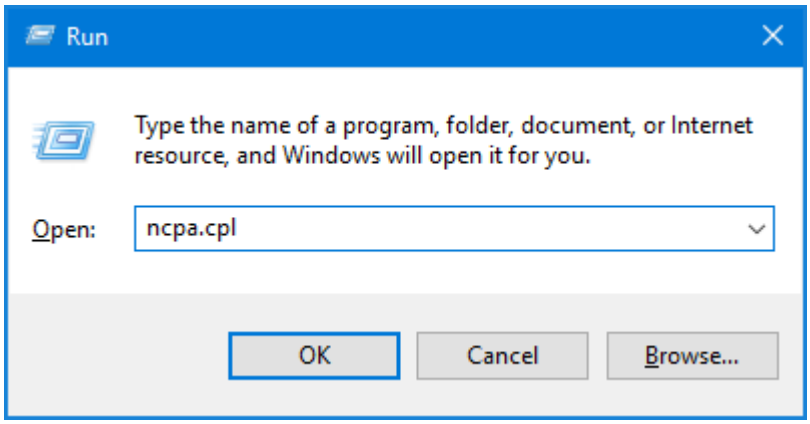
- ***Connection*:** Exibe o nome do perfil de conexão;
- ***Login*:** Exibe qual usuário está logado;
- ***Remote Gateway*:** Exibe o *IP* do endereço remoto que foi utilizado para efetuar a conexão;
- ***Duration*:** Mostra por quanto tempo o usuário está conectado;
- ***VPN*:** Mostra qual tipo de *VPN* está sendo utilizada;
- ***Virtual Address*:** Exibe o *IP* virtual que foi associado ao usuário nesta conexão.

Além disso, uma mensagem confirmando a conexão aparecerá no canto inferior direito da sua tela.



Mensagem de confirmação de conexão

Durante o processo de instalação do Blockbit Client a interface *TAP* é criada, ela fica desativada em *background* quando não tem nenhuma ligação entre túneis *VPN* sendo ativada no momento da conexão. Para visualizá-la, digite o comando ***Windows + R***, ou selecione "Executar" no seu *Menu* Iniciar, a janela abaixo será exibida, no campo de texto dela, digite "ncpa.cpl" e clique em **[** OK **]** (ou "tecle Enter"):

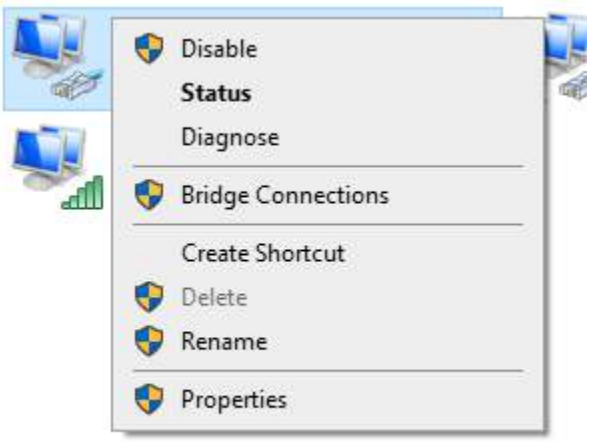


Run - control panel

A janela "Conexões de Rede" será exibida, como exemplificado abaixo, nela é possível visualizar a interface *TAP*:

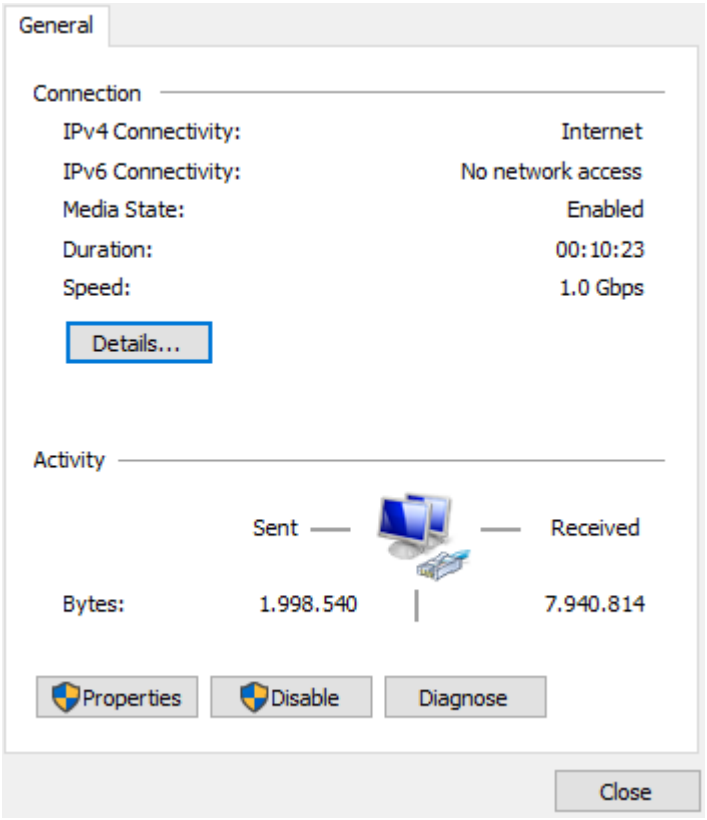
Network Connections

Quando uma *VPN* está estabelecida, a interface é automaticamente ativada, como exibido acima. O Blockbit Client utiliza esta interface para a comunicação entre os túneis. Para mais informações, clique em *Status*, como demonstrado abaixo:

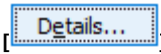


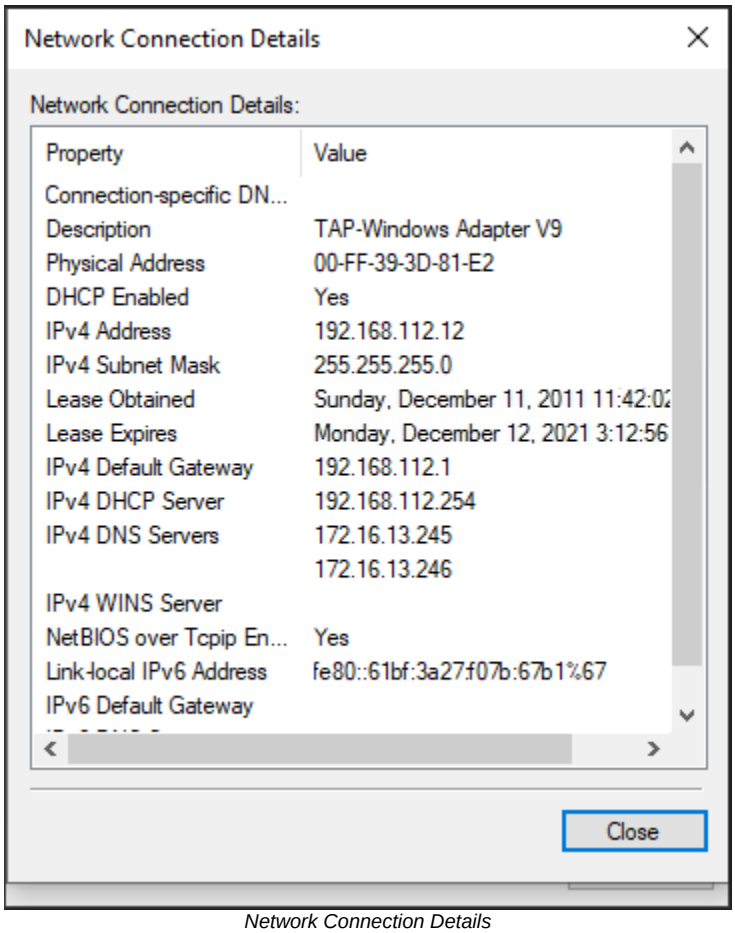
Local Area Connections - Status

O painel abaixo será exibido:



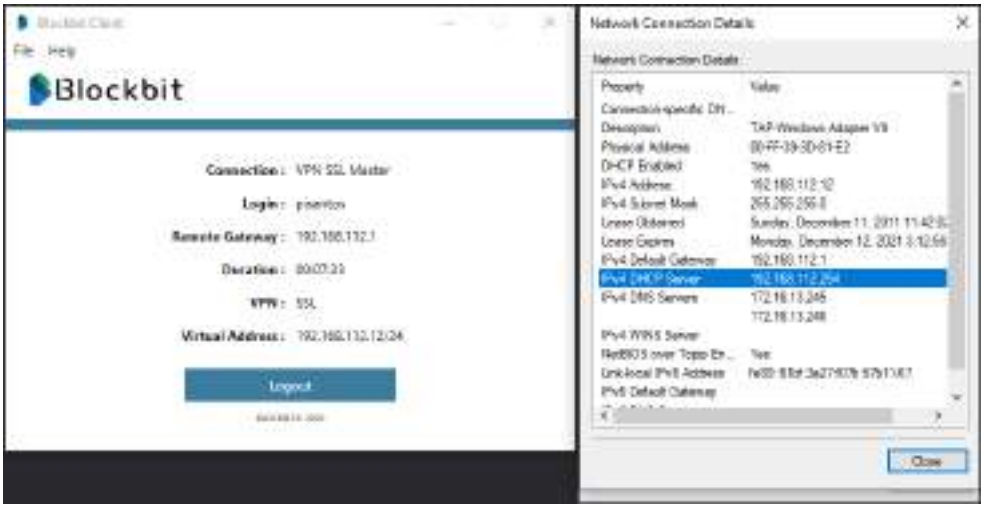
Local Area Connections

Clique no botão **[**  **]**, os detalhes de conexão serão exibidos:



Network Connection Details

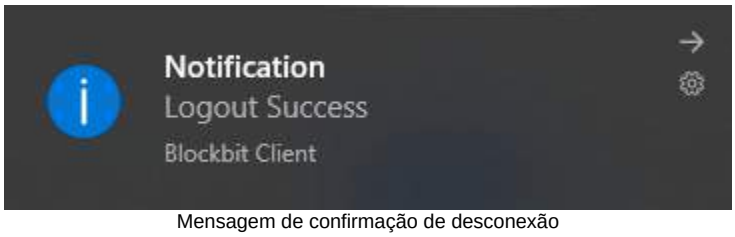
Na janela *Network Connection Details* é possível ver algumas informações úteis sobre a conexão, como por exemplo, o *IP* na interface é o mesmo que foi associado ao endereço virtual:



Network Connection Details - Example

Por fim, para se desconectar basta clicar no botão [

].



Mensagem de confirmação de desconexão

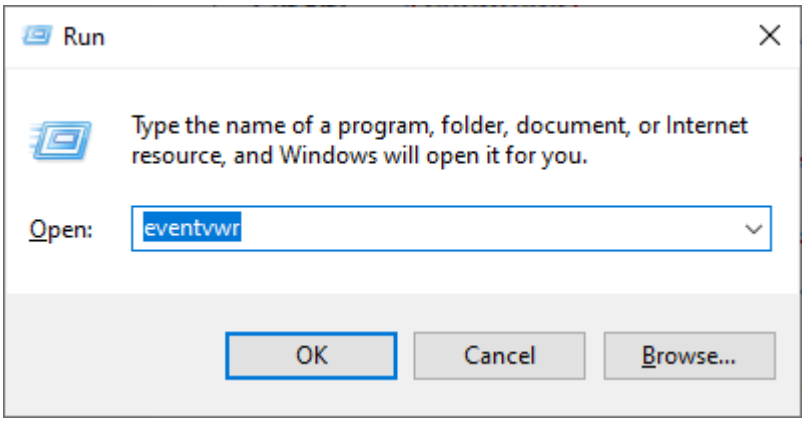
Isso conclui a conexão e desconexão utilizando o Blockbit Client.

Para mais informações sobre como efetuar a configuração, consulte essa página.

Logs no Gerenciador de Eventos do Windows

Ao instalar o Blockbit Client, o ***Blockbit_Log*** é adicionado automaticamente no Gerenciador de Eventos do *Windows*, registrando dados sobre as sessões e permitindo que o administrador efetue análises ou *troubleshooting* dos acessos.

Para acessar o Blockbit_Log, basta seguir os passos abaixo, digite o comando ***Windows + R***, ou selecione "Executar" no seu *Menu* Iniciar, a janela abaixo será exibida, no campo de texto dela, digite "ncpa.cpl" e clique em **[OK]** (ou "tecle Enter"):

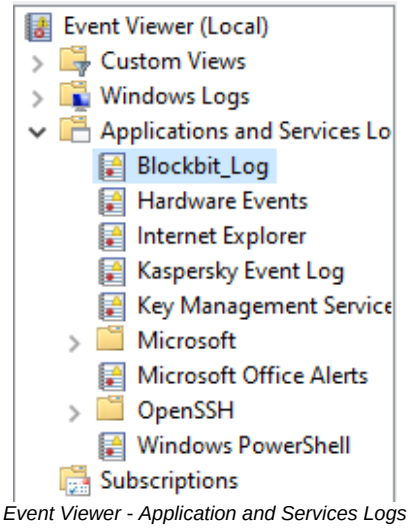


Run - Event Viewer

A janela do Gerenciador de Eventos do *Windows* será exibida, como exemplificado abaixo:

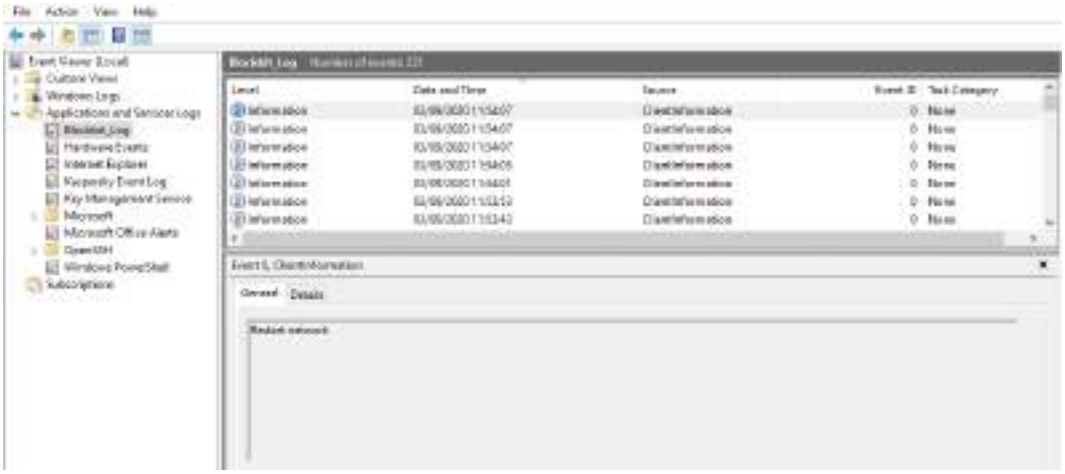
Event Viewer

À esquerda, expanda ***Application and Services Logs*** e clique em **Blockbit_Log**:



Event Viewer - Application and Services Logs

Ao acessar o ***Blockbit_Log*** o administrador tem acesso a todos os eventos registrados pelo sistema, conforme demonstrado abaixo:



Event Viewer - Application and Services Logs - Blockbit_Log

Além deste recurso, o Blockbit Client também conta com a sua própria opção de exportação de *logs* de conexão, para mais informações consulte esta pág ina.

Isso conclui a configuração e instalação do Blockbit Client.

Blockbit

it's easy to be secure

www.blockbit.com