OG | Brasil

SERVIÇO PÚBLICO ESTADUAL **PRODERJ** **APRESENTAÇÃO DE PROPOSTA** **ANEXO III – LOTE I**	**PREGÃO ELETRÔNICO - PE - RP Nº 014/2025** A realizar-se em: **16/01/2025 às 11:00 horas** Processo Nº: SEI-430002/000523/2025
A firma ao lado mencionada propõe fornecer ao PRODERJ - Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro, pelos preços abaixo assinalados, obedecendo rigorosamente as condições estipuladas no **EDITAL PE-RP Nº 014/2025**	CARIMBO DA FIRMA 23.518.044/0001-03 OEG BRASIL LTDA SRTVS N 110 QD 701 BL O SL 423 PARTE K S/N ASA SUL – CEP 70340-000 BRASILIA – DF

	Item	ID-SIGA	Descrição	U.F.	QTDE	VALOR (R$) Com ICMS Unitário	Com ICMS Total	VALOR (R$) Sem ICMS Unitário	Sem ICMS Total
Registro de Preços para contratação de empresa especializada no fornecimento contínuo de Solução de virtualização de desktops e aplicativos, por meio de um gerenciamento centralizado via Streaming Aplicacional, sendo disponibilizado aos usuários de acordo com seu perfil de acesso, com configuração padrão, com controle de acesso limitado, que permita ao Órgão/Autarquia ter o domínio sobre o ambiente computacional, de forma a incorporar regras de alta segurança, disponibilidade, rastreabilidade e governança sobre todas as aplicações e dispositivos assim detalhados, no primeiro lote									
LOTE I	1	192754	Subscrição de licença (Licença Concorrente) de plataforma de virtualização de desktops e aplicativos para o gerenciamento centralizado do ambiente computacional com suporte do fabricante por 12 meses. Marca EO.Workspace - Fabricante: Enterprise Open Workspace (www.enterpriseopen.com)	Licença Concorrente	4.921			680,00	R$ 3.346.280,00
	2	192755	Serviço de consultoria especializada sob demanda para plataforma de virtualização de desktops e aplicativos	Horas	2.380			245,00	R$ 583.100,00
	3	192909	Treinamento em plataforma de virtualização de desktops e aplicativos para o gerenciamento centralizado do ambiente computacional / repasse de conhecimento técnico para equipe técnica	Turma	20			3531,00	R$ 70.620,00
			VALOR TOTAL GLOBAL DO LOTE I			_		_	R$ 4.000.000,00

Valor global por extenso: (Quatro milhões de reais)

Dados do Banco Bradesco do Licitante: BRADESCO / 237 - Agência: 0241 - Conta Corrente N.º 11.702-1

OBSERVAÇÕES

1ª - A PROPOSTA DE PREÇOS:

• Foi preenchida integralmente por processo mecânico ou eletrônico, sem emendas e rasuras;
• contém os preços em algarismos e por extenso, por unidade, já incluídas as despesas de fretes, impostos federais ou estaduais e descontos especiais: e

• Está datada e assinada pelo gerente ou seu procurador.

2ª - O Proponente se obriga, mediante devolução da PROPOSTA DE PREÇOS, a cumprir os termos nela contidos.

3ª - Estamos cientes que a licitação poderá ser anulada no todo, ou em parte, de conformidade com a legislação vigente.

• **Prazo de execução**: Conforme o TR.

• **Validade da PROPOSTA**: Preços válidos por 60 (sessenta) dias.

• **Local de entrega desta Proposta:** Rua da Conceição nº 69/24º andar - Centro - Rio de Janeiro - RJ.

Declaramos inteira submissão ao presente termo e legislação vigente.

Em, 20/03/2026

ELMER ALEXANDRE DE OLIVEIRA:19572332813

Assinado de forma digital por ELMER ALEXANDRE DE OLIVEIRA:19572332813
Dados: 2026.03.20 10:51:10 -03'00'

Elmer Alexandre de Oliveira
Representante Legal
RG 252135404 SSP-SP
OEG BRASIL LTDA

EO.workspace - Operation and Administration

1. Introduction

This guide describes how to operate and administer an installed EO.workspace solution, including how to troubleshoot any problems that might occur.

Before continuing, make sure you are familiar with the components and architecture of EOW by consulting the EO.workspace - Introduction and Architecture guide.

2. Administration

2.1. Administration console

The administration console allows the execution of several high-level administration tasks, such as:

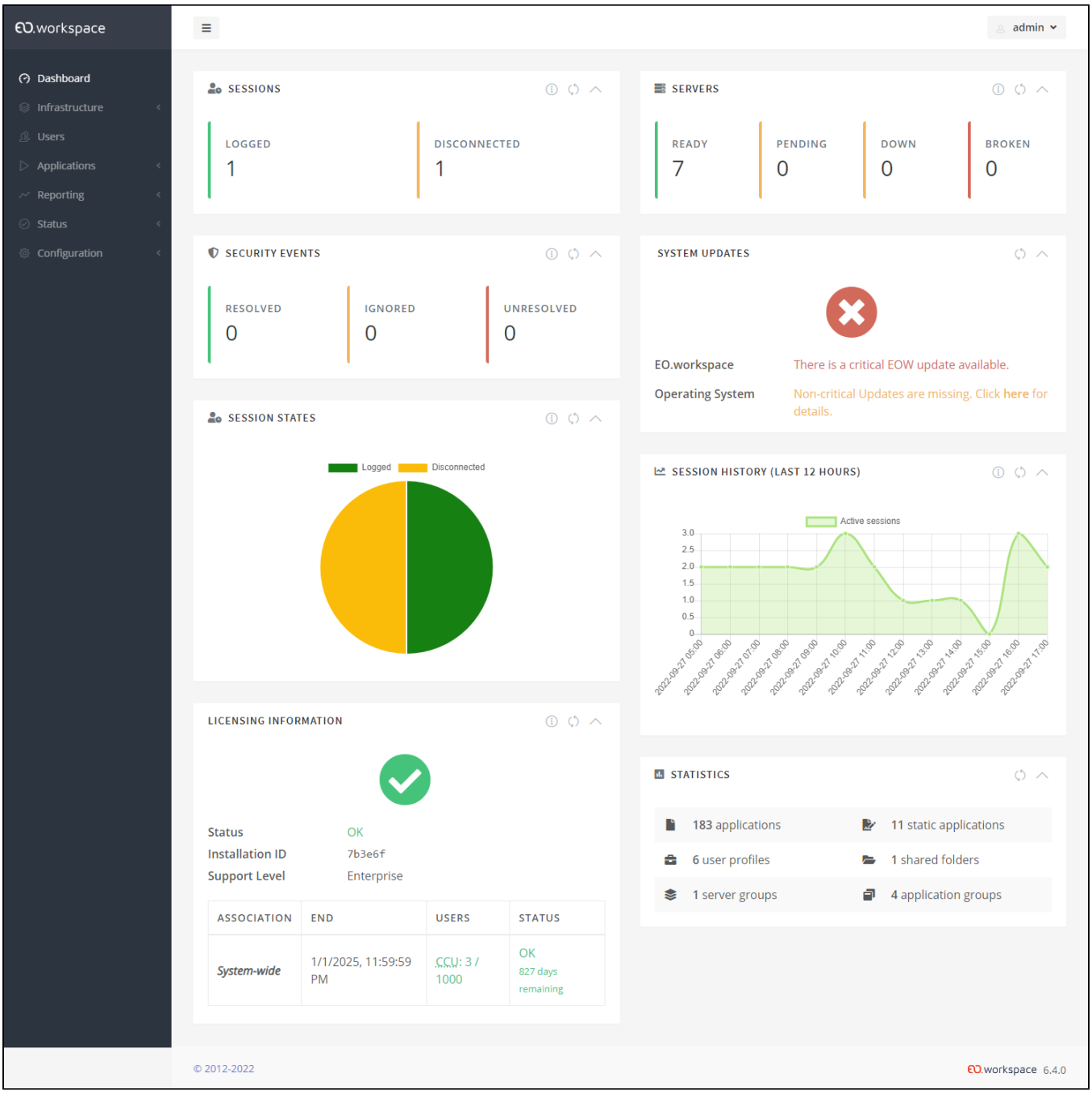
- system maintenance mode management;
- new server registration;
- server and roles configuration;
- server groups configuration;
- scaling configuration (DSM);
- login scripts configuration;

- users and user groups management;
- applications and application groups management;
- mime-types configuration;
- static applications configuration;
- publications management;
- reporting tasks;
- system configuration and tweaking;
- active sessions management;
- accessing the system and component logs;
- news management.

It is available through the following URL:

- `https://<session manager hostname>:8443/`

After logging in with the appropriate administrative credentials, the user is presented with an informative dashboard, which presents links to several administration sections and a quick overview of the status of the infrastructure servers, active sessions, subscription information and other relevant statistics:



The administration console interface is divided into several sections, which are described below.

2.1.1. Infrastructure > Servers

The "Infrastructure > Servers" section contains functionalities related to slave server administration. It's possible to view the status of every slave server, place them on "maintenance mode", configure them, or register new ones. When a new slave server is installed (with any role) and started, it appears on the "Unregistered servers" tab. After selecting the "Register" option, the server will be added to the list of registered servers. When newly added, a server will be in "maintenance mode", in order to be possible to perform the initial configuration.

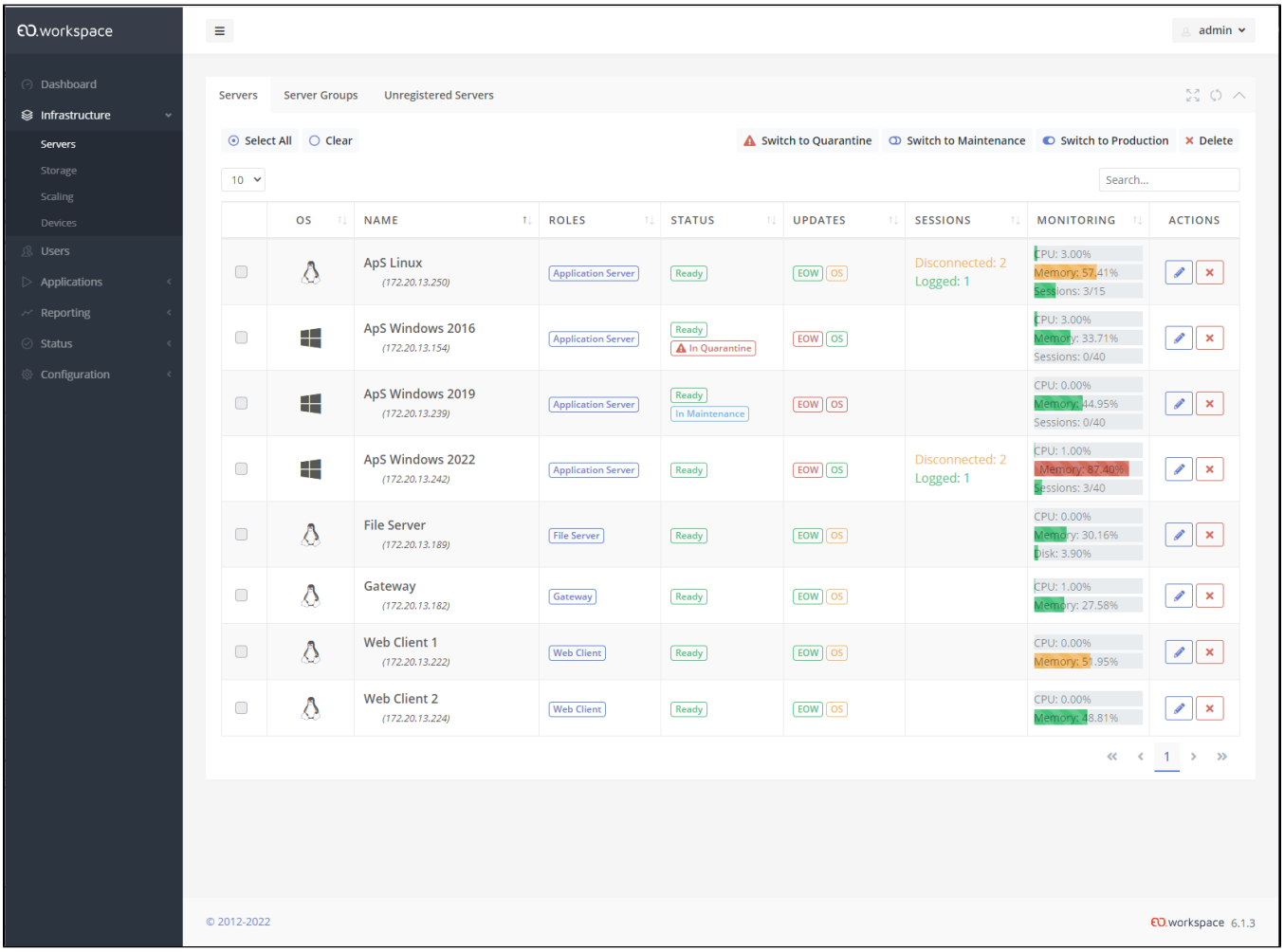
The "maintenance mode" is useful, for instance, to stop new sessions being created on a specific application server. When a server is switched to "maintenance mode":

- Current established sessions are kept logged in;
- News sessions cannot be created in the specified application server;
- It has no effect on slave servers with the gateway or web client roles, new sessions can still be created.

In order to take a server out of "maintenance mode", one has to select the "Switch to production" option.

In this section, it also possible to manually place a slave server or remove it from quarantine. When a server is placed in "quarantine", all the measures of “maintenance mode” are applied and additionally all current active sessions are logged out. To take a server out of "quarantine mode", one must select the “Switch to maintenance” or "Switch to production" option.

Introduced in version 6.4: If the option to check for OS updates is enabled (configure it in '**Configuration > Server**'), this section will also include information regarding available updates in the servers. Each server may be updated or have critical or non-critical updates available. If the option to check for EOW updates ais enabled (configure it in '**Configuration > Server**'), this action will include whether each server have the same version as the Session Manager or not.



Inside each server, it's possible to configure its:

- **Display name**: name displayed on administration console sections.
- **Internal name/FQDN**: server address used by the Session Manager to communicate with the server. Make sure that this address is valid, otherwise communication with the server will fail.
- **Redirection port**: TCP port used for session streaming data. If left empty, the default (3389) is used.

- **Server roles:** enabled or disabled available roles for that server. Depending on the installed roles, the options are: Application Server, Web Client, Gateway and File Server.

Additionally, it's also possible to configure role-specific configurations, depending on the installed roles. For example, for application servers, one can configure the maximum number of sessions on the server.

Still on the "Servers" section, in the "Server Groups" tab, it's also possible to create server groups. This functionality allows the association of certain servers to specific groups of users.

If some server groups are defined:

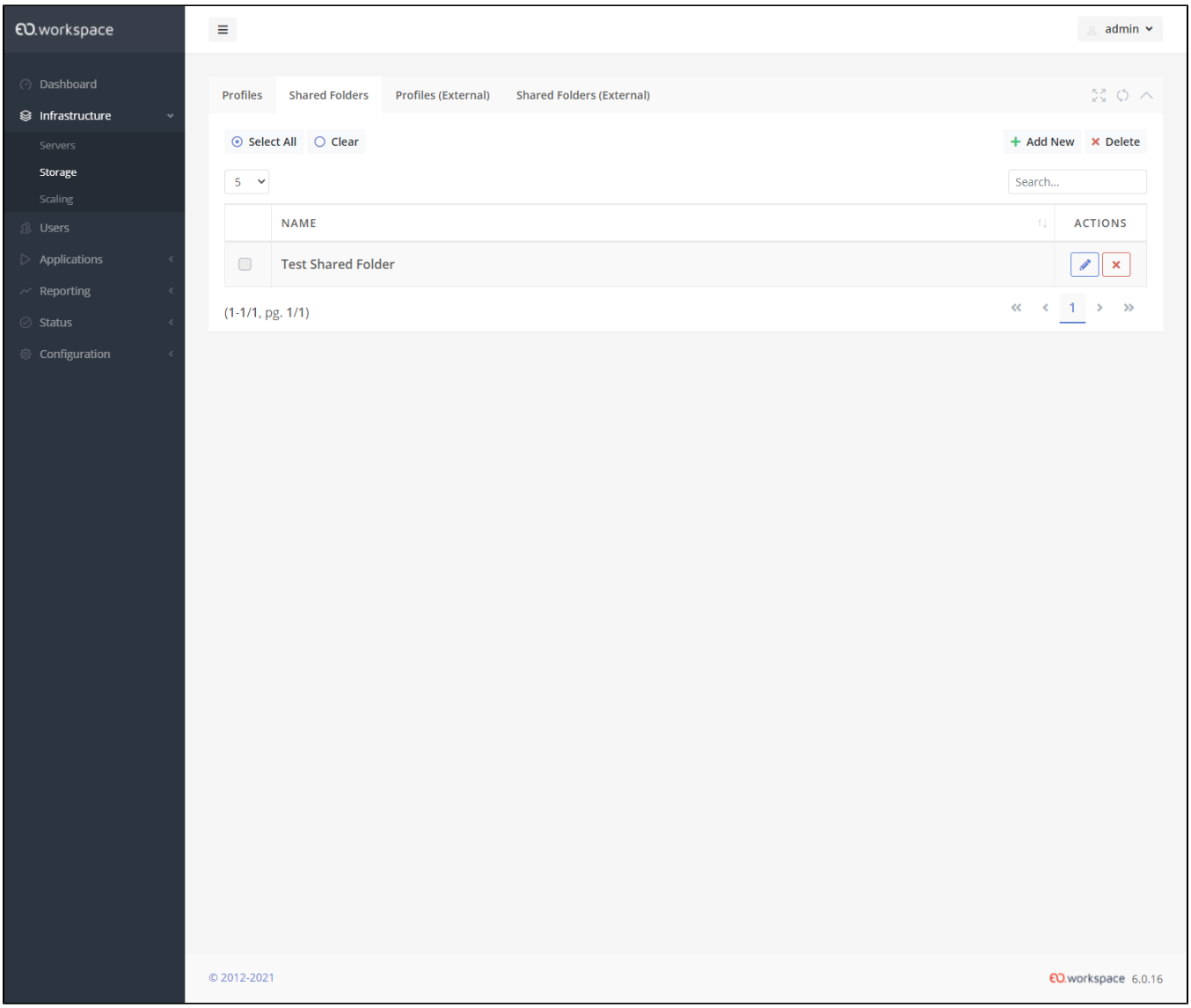
- Users belonging to user groups which are associated with server groups will be distributed among the servers in that groups.
- If the "bypass server groups" option is disabled (configure it in '**Configuration > Sessions**'), if none of the servers on the server groups are available (ie. they are in maintenance, down, broken), the session will not be created.
- If the the "bypass server groups" option is enabled (configure it in '**Configuration > Sessions**'), if none of the servers on the server groups are available (ie. they are in maintenance, down, broken), then:
    1. a server will be selected among other existing server groups;
    2. a server will then be selected among all available servers.
- Users not belonging to any user group associated with server groups will be distributed among all servers which are not in maintenance.
- Other restrictions may apply (eg. per-user or per-user-group desktop server restrictions or "bypass server groups" configuration).

If no server groups are defined:

- All users will be distributed among all servers which are not in maintenance
- Other restrictions may apply (eg. per-user or per-user-group desktop server restrictions).

2.1.2. Infrastructure > Storage

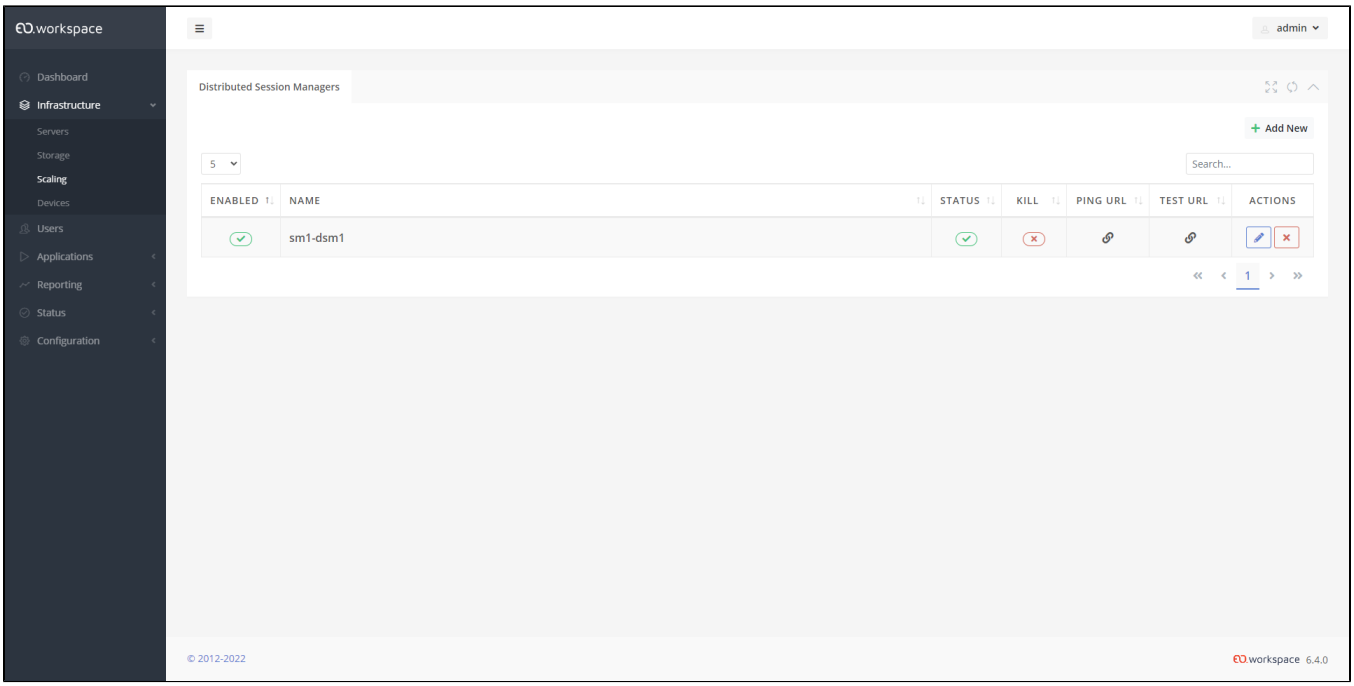
In the "Infrastructure > Storage" section, you can configure everything related to storage, be it internal or external, related to user profiles or shared folders. More information is available in EO.workspace - Configuring External Storage for Persistent User Profiles and Shared Folders.



2.1.3. Infrastructure > Scaling

In the "Infrastructure > Scaling" section, you can configure the connection between this Session Manager (SM) and all intended Distributed Session Managers (DSMs).

This is used when the landscape has multiple locations and requires one or more Distributed Session Managers to distribute users.



When adding a DSM, the following configurations are required:

- **Name:**
  - The DSM/SM name pair.
  - This is only informative, but must match between SM and DSM configurations.
  - Can be any alphanumeric value.
  - Can't be changed after creation (only by deleting and recreating the DSM configuration).
- **Token**:
  - Pre-shared verification token, used to avoid fake heartbeat messages.
  - Must match between SM and DSM configurations.
  - Usually, but not required, a 72 character alphanumeric string or an UUID.
- **Ping URL**:
  - The URL used by the SM to send the heartbeat to the DSM.
  - Must point to "`https://<dsm hostname>/ping`".
- **Test URL:**
  - The URL used by the SM to validate the correct operation of the location.
  - It usually points to the Web Client or Web Client Load Balancer URL.
- **Kill disconnected sessions:**
  - If enabled, when unable to contact the DSM, kill sessions which are in the "disconnected" state.
  - This ensures that a user doesn't have a session in multiple locations.

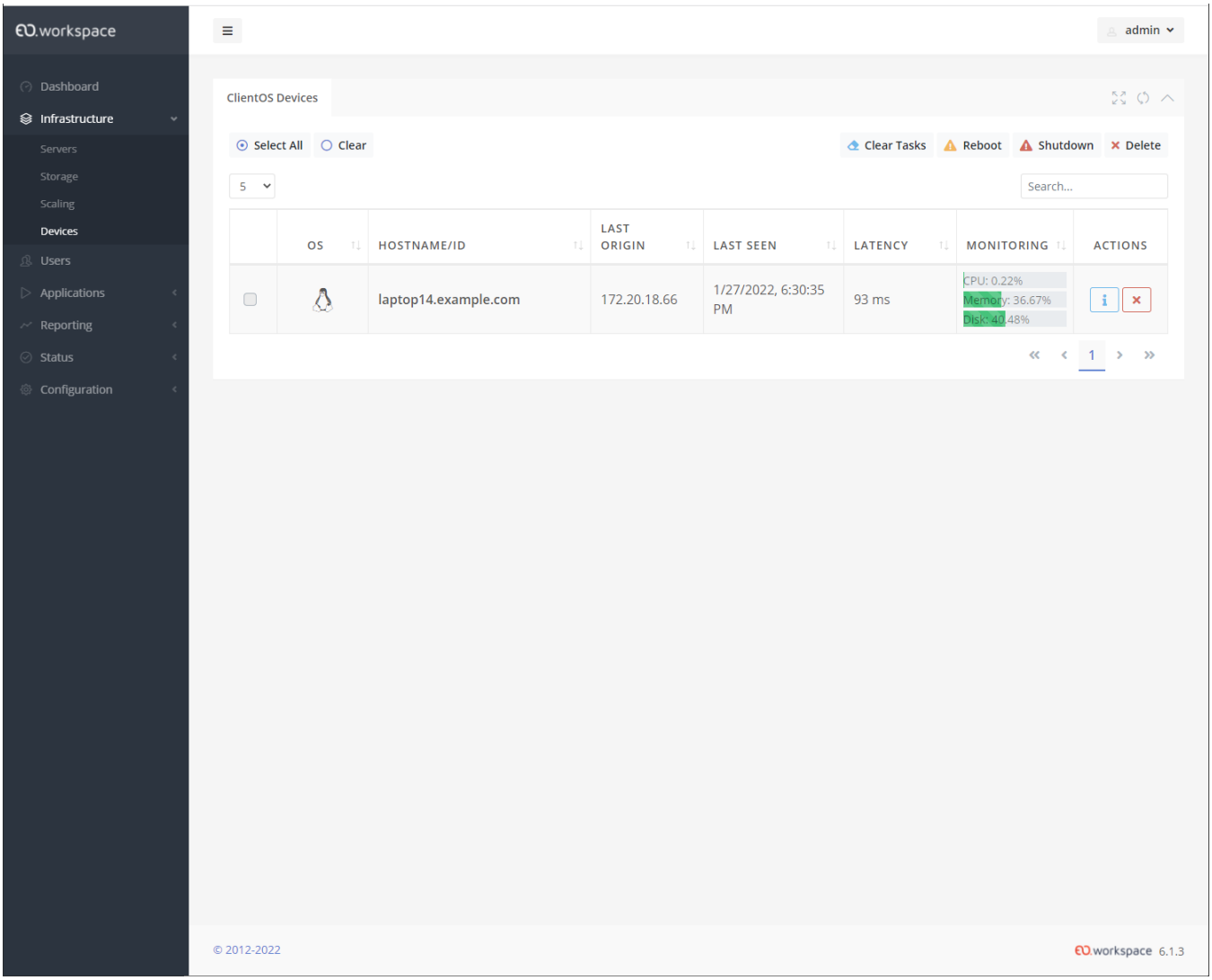
It's also necessary to configure a symmetric entry in the DSM administration console, please see the corresponding documentation section:

- Distributed Session Manager (DSM) Administration Console

2.1.4. Infrastructure > Devices

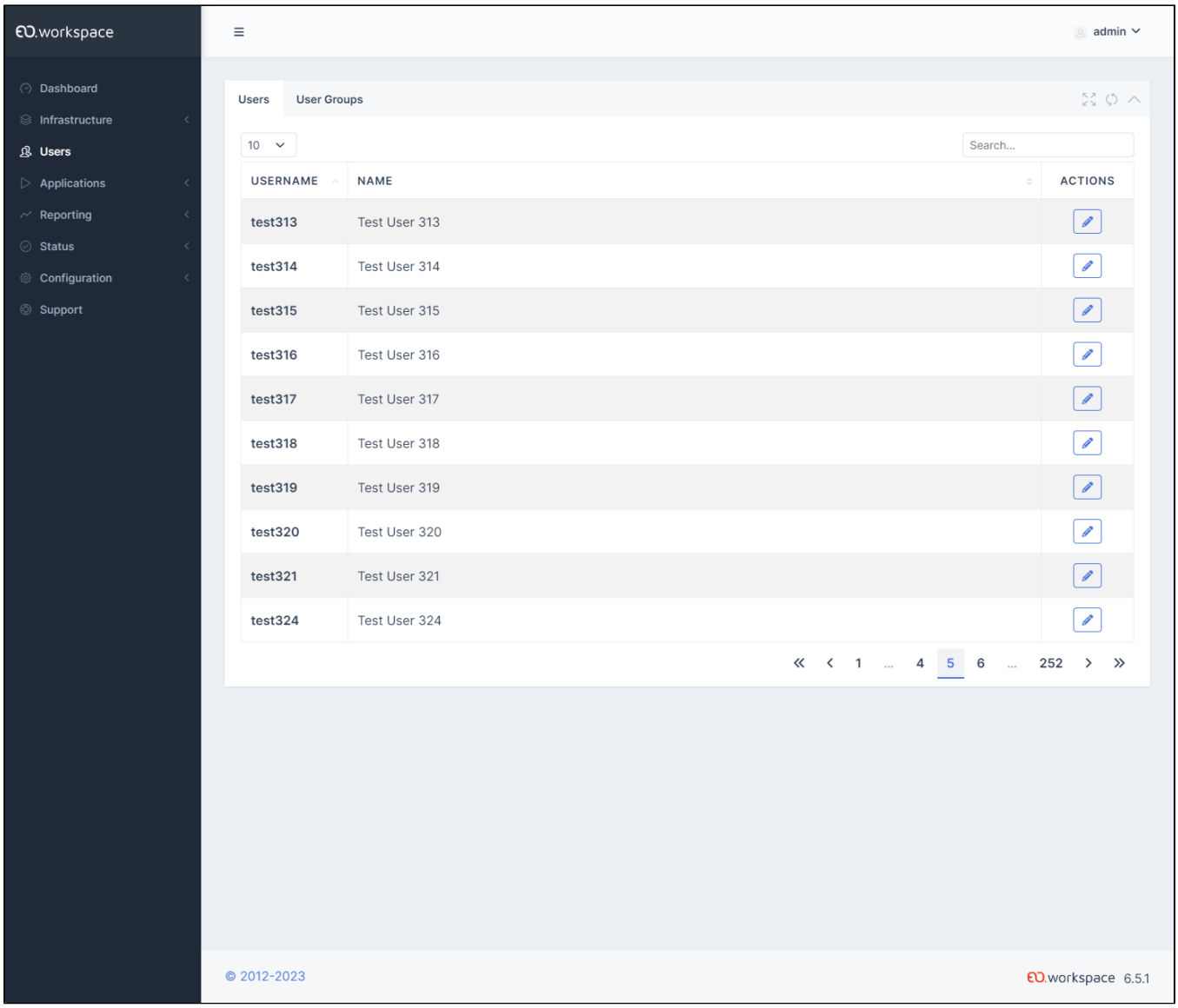
Introduced in version 6.3.

In the "Infrastructure > Devices" section, you can obtain information about ClientOS devices that connected with the Session Manager. It is possible to schedule tasks, such as reboot and shutdown, that will be executed by the device the next time that it contacts the EOW infrastructure.



2.1.5. Users > Users

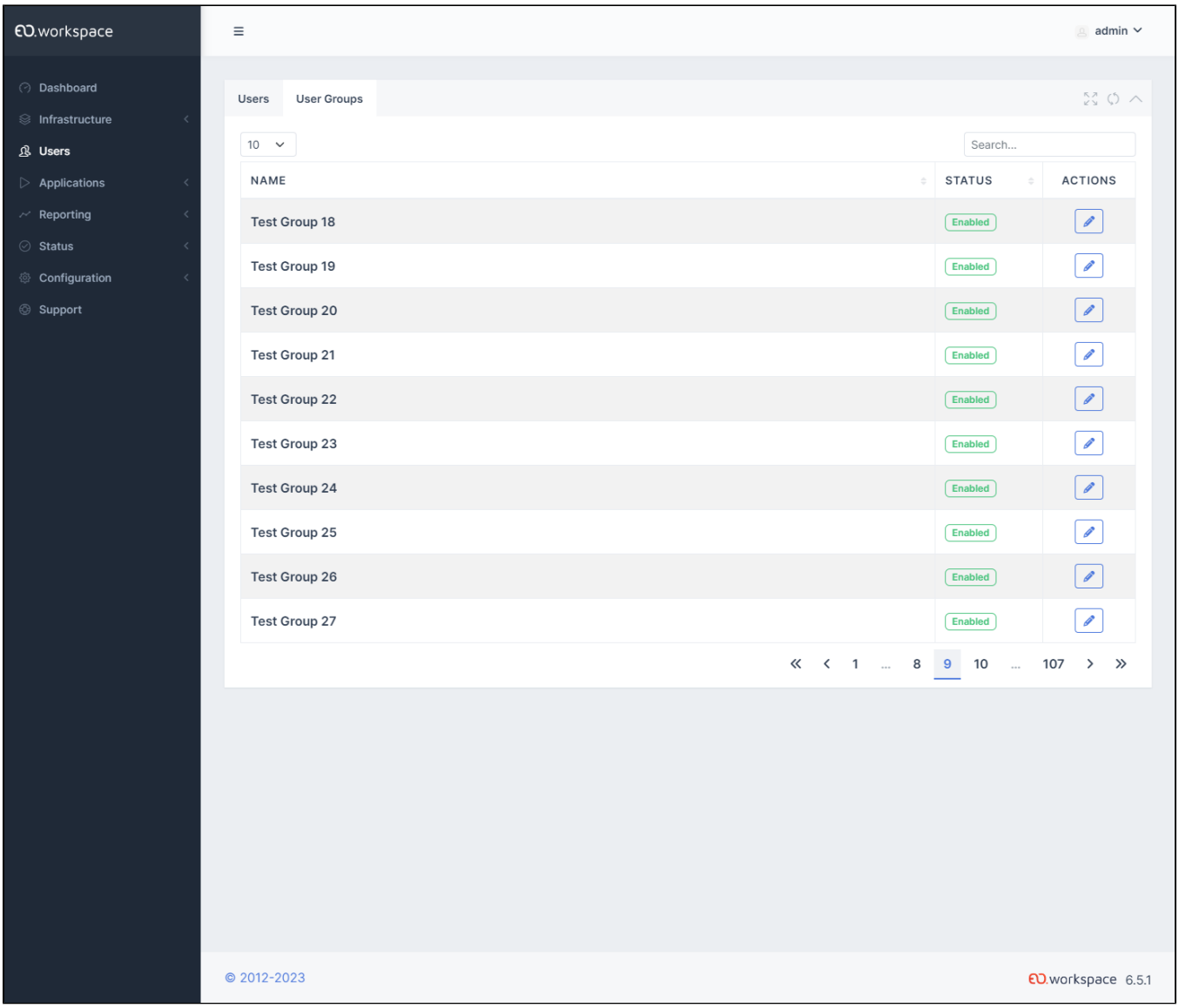
In the "Users > Users" section, it's possible to manage users.



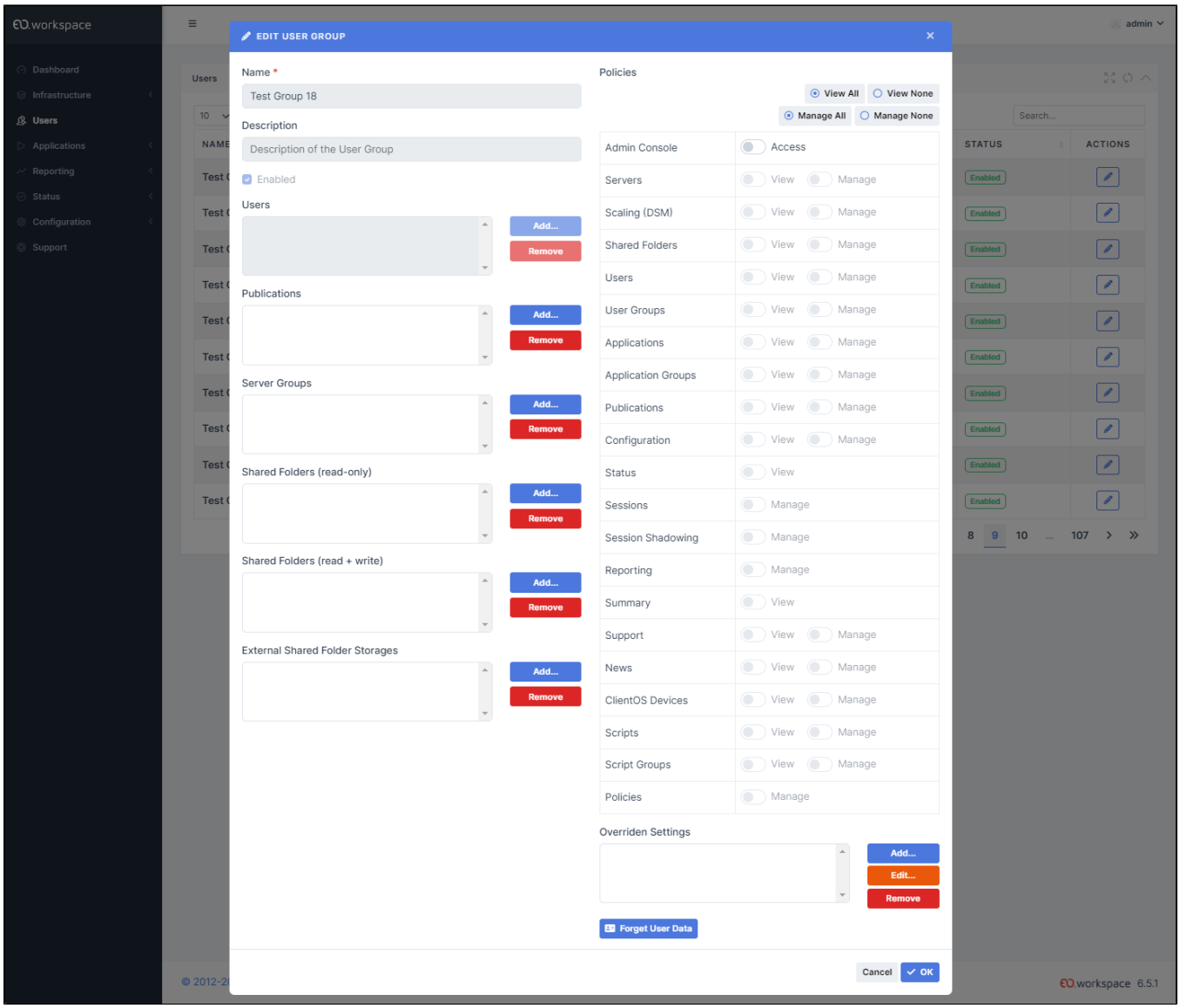
When using EOW's internal user database, this tab is where users are created and managed. When using an external authentication source, such as an LDAP server or Microsoft's Active Directory, this section is automatically filled and users cannot be created nor deleted. This section is useful to verify users' information (eg. to confirm to which groups they belong) and to override individual system-wide configuration parameters.

2.1.6. Users > User Groups

In the "Users > Users Groups" section, it's possible to manage user groups.



When using EOW's internal user database or when using the Internal user group method, this tab is where user groups are created and managed. When using the groups from an external authentication source, such as an LDAP server or Microsoft's Active Directory, this section is automatically filled and user groups cannot be created nor deleted. This section is useful to verify user groups' information (eg. to confirm to which users belong to a certain group), to configure which applications, servers and shared folders should be available to a certain group, to override system-wide configuration parameters and to define administration permissions for a certain user group.



The Policies for each user group define if the users from that group can access the Admin Console and which sections they have access to. For some sections, it is also possible to define only View or View and Manage permissions. The available policies and a brief description of each one are described below.

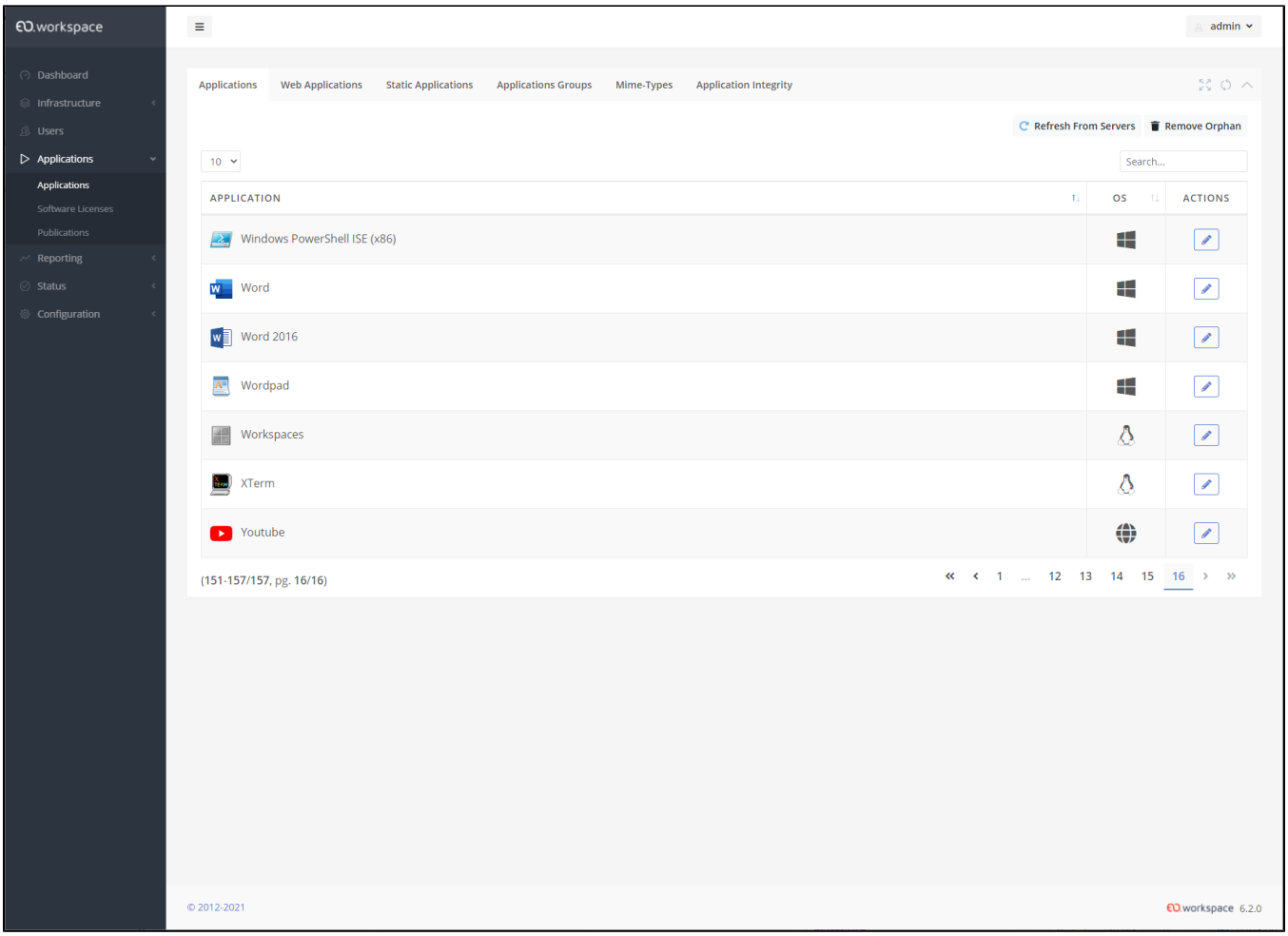
- **Admin Console**
  - Access: users can login and access the dashboard, but cannot view or manage any information without additional permissions. Prerequisite for every other permission
- **Servers**
  - View: users have access to the "Infrastructure > Servers" section
  - Manage: users can change servers' configurations
- **Scaling (DSM)**
  - View: users have access to the "Infrastructure > Scaling" section
  - Manage: users can change scaling configurations
- **Shared Folders**
  - View: users have access to the "Infrastructure > Storage" section
  - Manage: users can change storage configurations
- **Users**
  - View: users have access to the "Users > Users" section
  - Manage: users can manage users when using EOW's internal user database
- **User Groups**
  - View: users have access to the "Users > User Groups" section
  - Manage: users can manage user groups
- **Applications**
  - View: users have access to the "Applications" section
  - Manage: users can manage applications
- **Application Groups**
  - View: users have access to the "Applications > Application Groups" section
  - Manage: users can manage application groups

- **Publications**
  - View: users have access to the "Applications > Publications" section
  - Manage: users can manage publications
- **Configuration**
  - View: users have access to most the "Configuration" section
  - Manage: users can change configurations
- **Status**:
  - View: users can view the current and historical information regarding the system status, such as, sessions, session shadowing, applications, security events, logs and admin audit. This includes the sections "Reporting > General, Sessions, Session Shadowing, Applications, Security Events" and "Status > Sessions, Logs, Admin Audit"
- **Sessions**
  - Manage: users can mange sessions through the sections "Reporting > Sessions" and "Status > Sessions"
- **Introduced in version 6.4: Session Shadowing**
  - Manage: users can shadow sessions.
- **Reporting**
  - Manage: users can perform changes in the "Reporting" section, such as deleting reports
- **Summary**
  - View: users have access to the "Status > Summary" section
- **Support**
  - View: users have access to the "Support" section
  - Manage: users can send support requests
- **News**
  - View: users have access to the "Configuration > News" section
  - Manage: users can manage news
- **Introduced in version 6.3: ClientOS Devices**
  - View: users have access to the "Infrastructure > Devices" section
  - Manage: users can manage ClientOS Devices
- **Scripts**
  - View: users have access to the "Configuration > Login Scripts" section
  - Manage: users can manage Login Scripts
- **Script Groups**
  - View: users can view which Login Scripts are assign to each User Groups
  - Manage: users assign Login Scripts to User Groups
- **Policies**
  - Manage: users can manage these policies

Note that while having access to a section, some of the information usually presented in that section might not appear because it depends on permissions for another section. For example, is a user has permissions to view Publications but does not have permission to view Applications Groups and User Groups, the Publications will not appear.

2.1.7. Applications > Applications

The "Applications > Applications" section is where applications, mime-types and publications are managed.



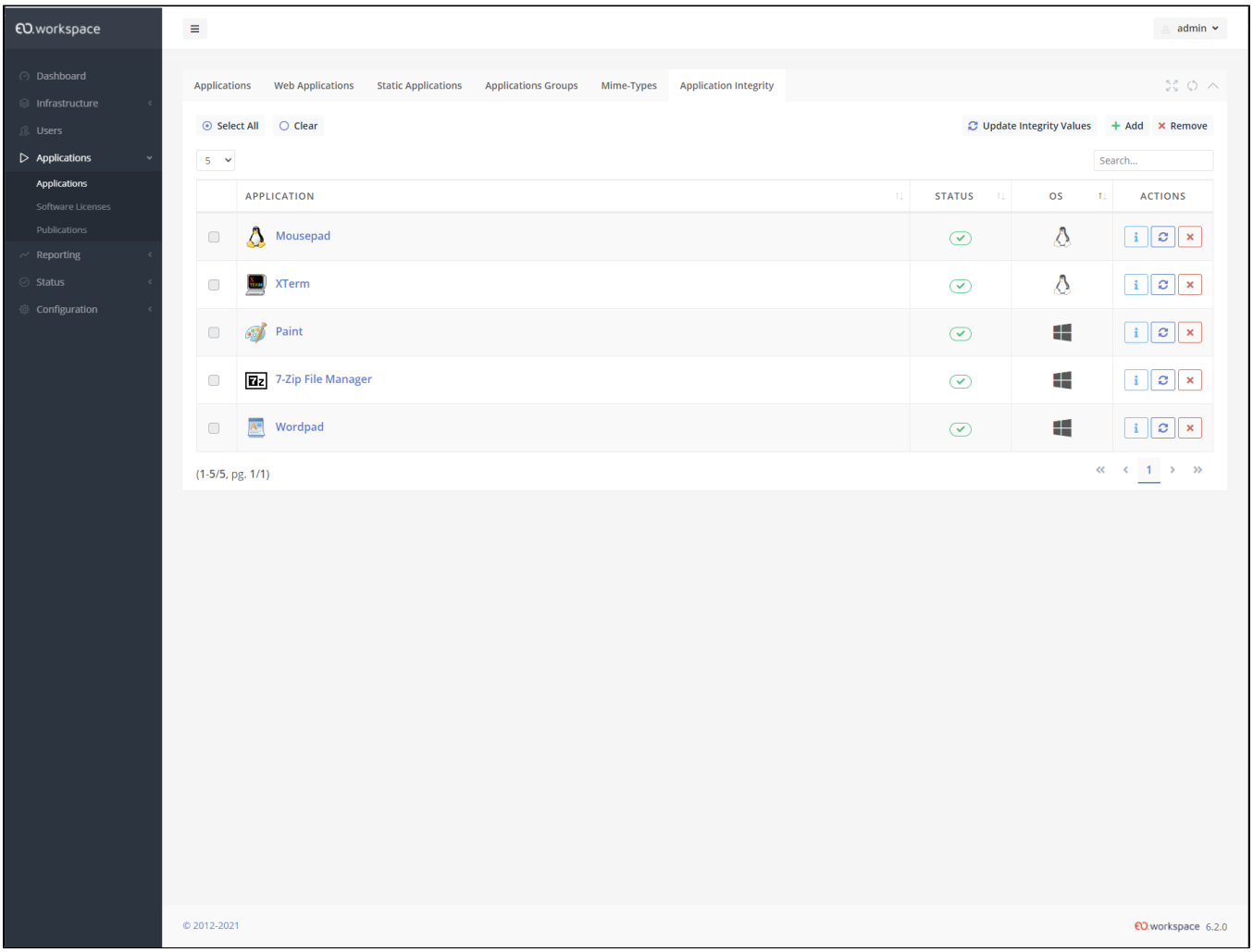
Available applications are automatically populated from the application servers. It's possible, in this section, to see the list of available applications and, for each one of them, to override the displayed icon. It's also possible to create "static applications", which are applications which are not populated automatically, or for which we want to define custom parameters, such as the application name, executable or command line parameters. As a starting point for a static application, one can "clone" one of the automatically populated ones. Also available in this section is the configuration and application groups (which allow to later publish several applications to user groups).

Document file types, or mime-types, can be associated to a specific application, so that when a user opens a certain type of document, it is opened with the correct application. This is configured on the "Mime-Types" box.

Introduced in version 6.1: It is available in this section the configuration of "web applications" (applications which open a website URL on the user's local browser).

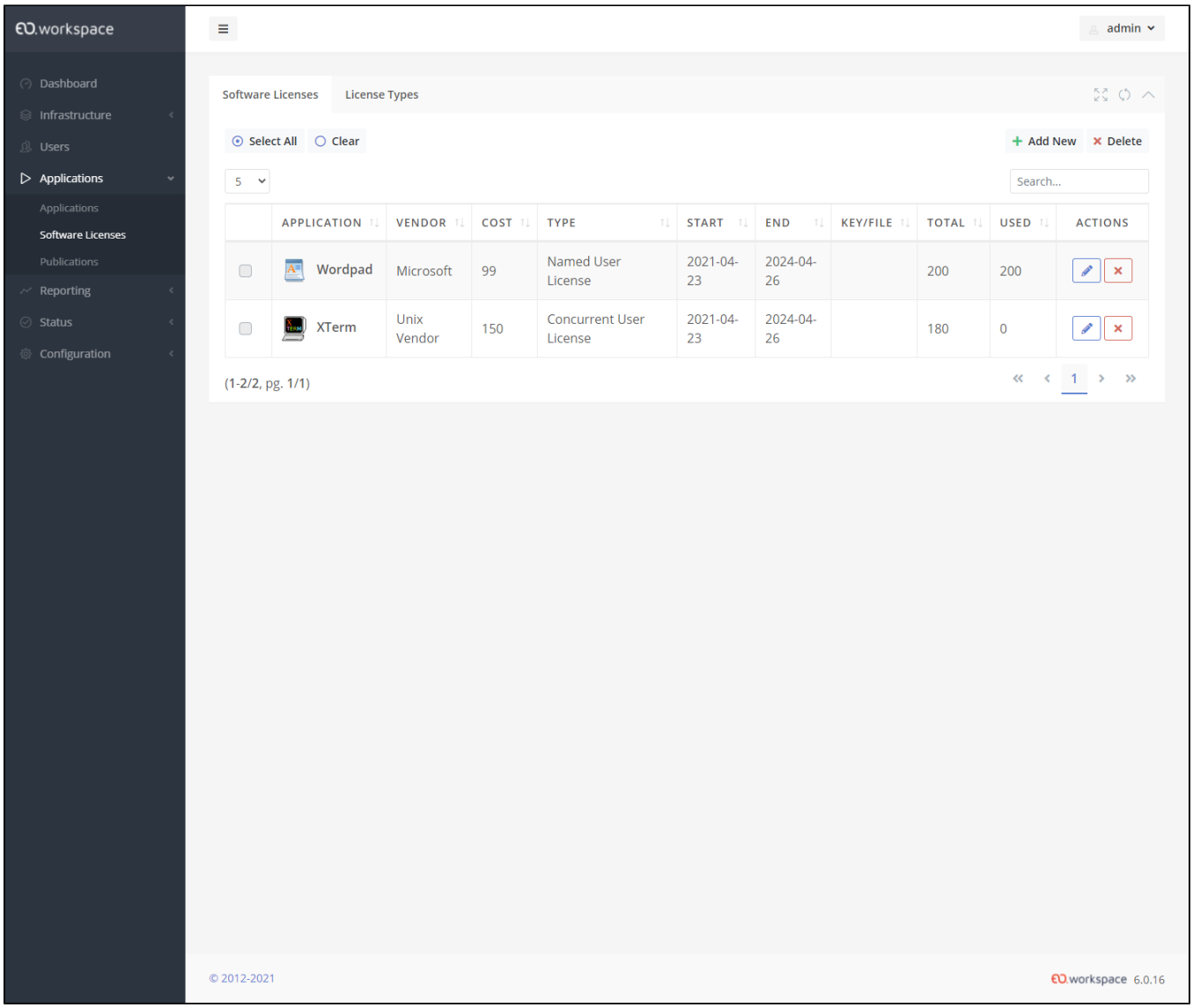
Introduced in version 6.2: Also available in this section is the management of the integrity of selected applications. When an application is added to this table, the session manager communicates with the Application servers to obtain the applications' executable checksum and stores it in the database. At a later time, and if the "Application Integrity" is enabled, the checksum is calculated again and compared with the previous one to verify if the application was compromised in any way.

If the application's executable was purposefully changed, for example due to an update, and the previous checksum is no longer valid, one has to click on "Update integrity value" in this interface to change the checksum saved by the session manager.



2.1.8. Applications > Software Licenses

On the "Applications > Software Licenses" section, you can manage software licenses and license types.



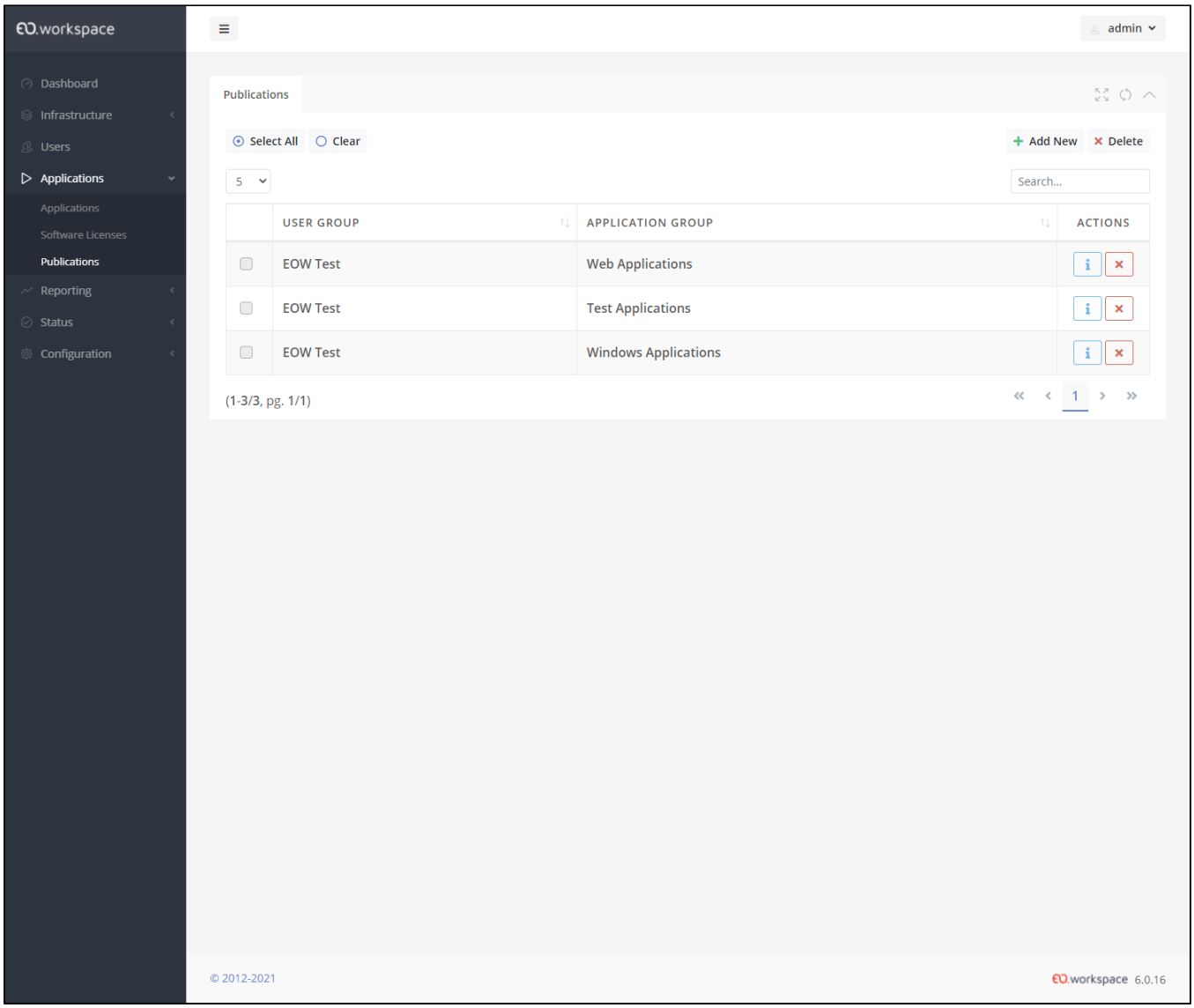
The software licenses do not restrict how many copies of a certain application may run at a certain time, they are only for informational purposes. You can produce reports about application license usage on the "Reporting" section (described below).

Introduced in version 6.6: There are now settings for each license which allow to block applications execution when license limits are reached or when licenses expire. License usage limits can now be enforced for both "Concurrent" and "Named" license types.

2.1.9. Applications > Publications

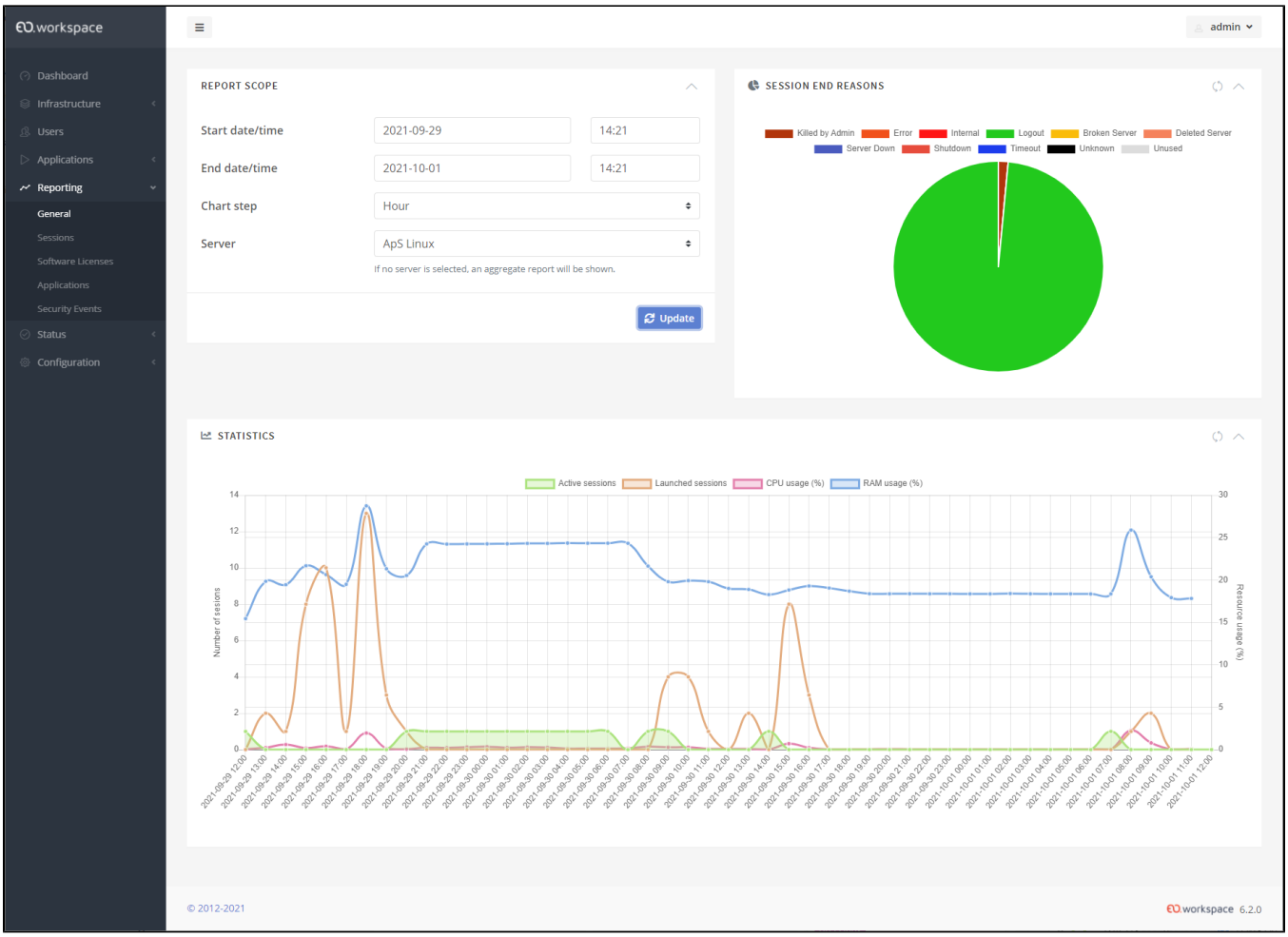
In the "Applications > Publications" section, one can associate application groups with user groups, in order to define which applications are available to which users.

A user group can have multiple application groups associated, and the users of that group will have all those applications published on their sessions. Similarly, an application group can be associated with multiple user groups, and all users of those groups will have access to the applications of that application group.



2.1.10. Reporting

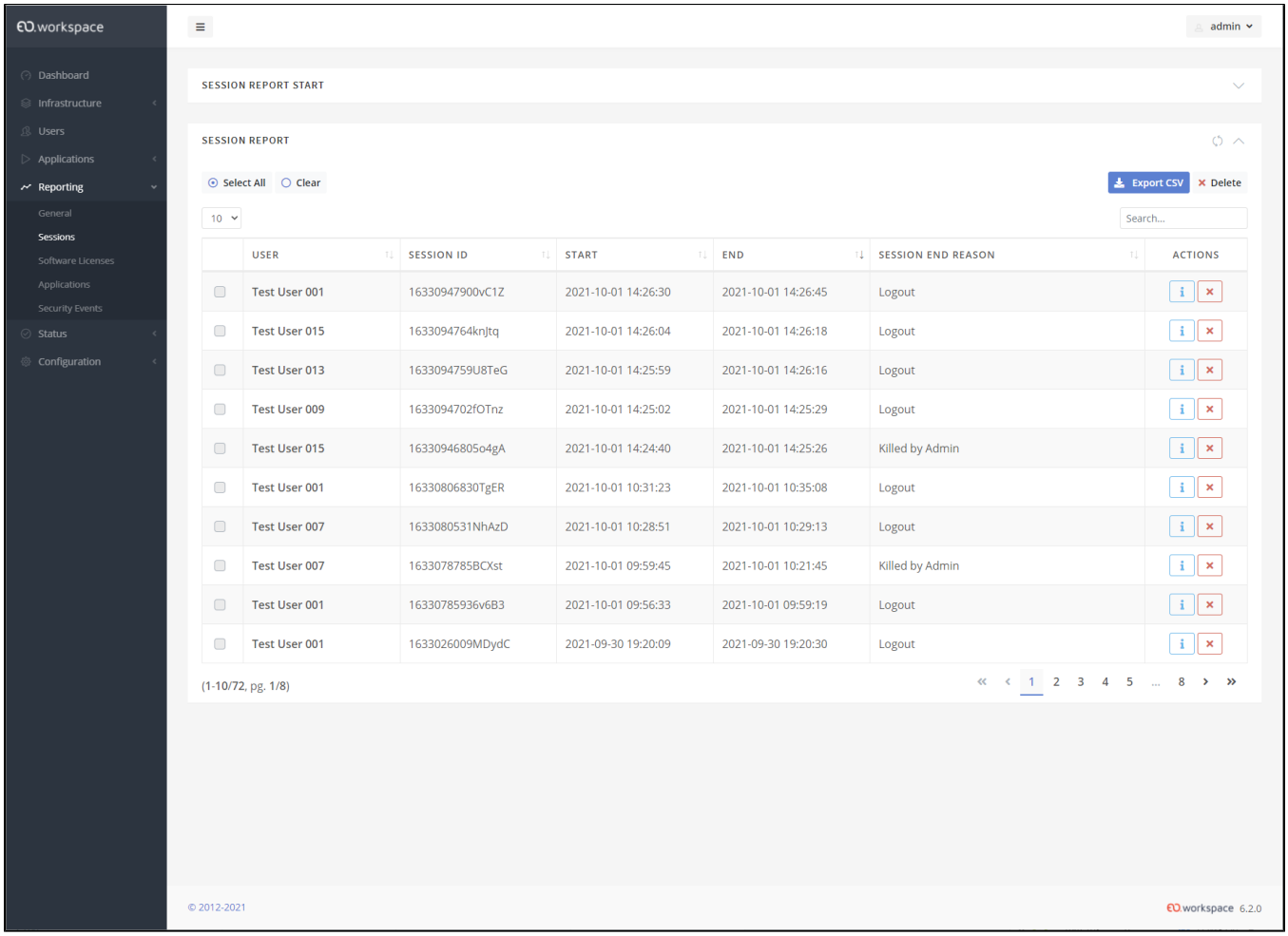
On the "Reporting" section, one can obtain information about the system, for a certain time period, regarding application servers, sessions, application and software license usage.



2.1.10.1. Reporting > Sessions

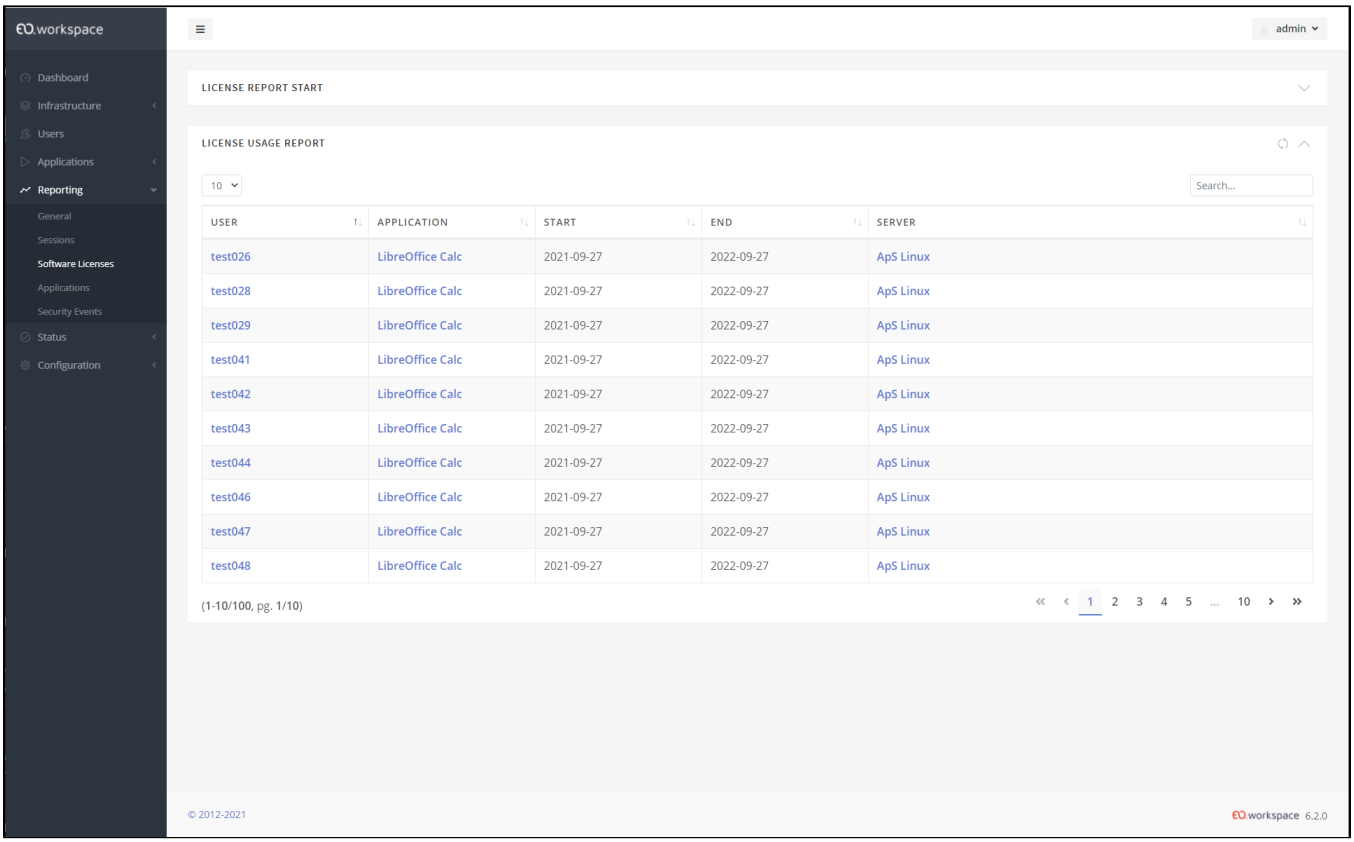
In the "Reporting > Sessions" section, one can obtain information about past sessions over a certain time period. For currently established sessions, go to "Status > Sessions".

By selecting an individual section, it's possible to obtain in-depth information about it, such as the associated user, its session mode, when it was started and when it ended, why it ended, servers used, storage used, client addresses and used and published applications. It is also possible to obtain the session log, the session settings and export all this information into a PDF.



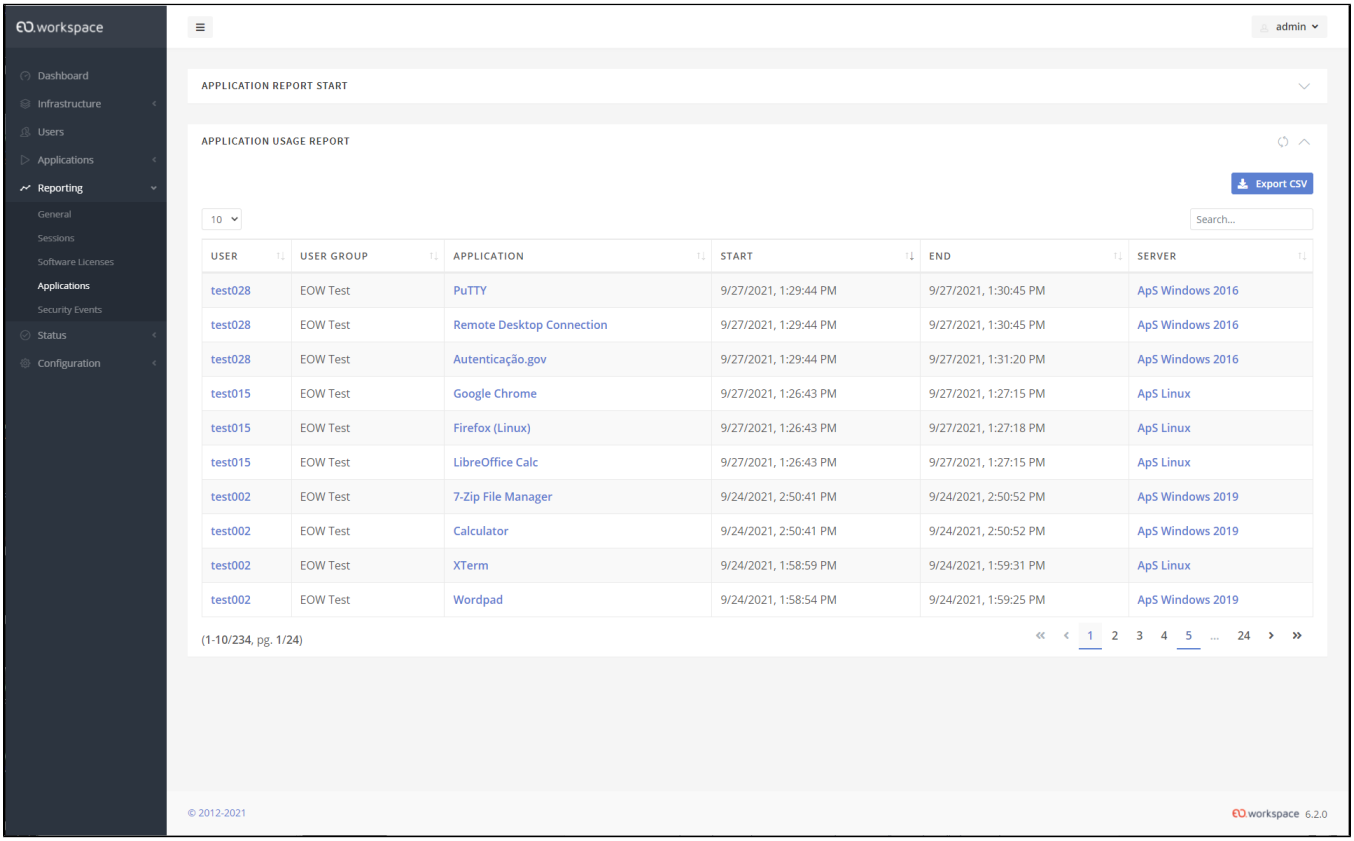
2.1.10.2. Reporting > Software Licenses

In the "Reporting > Software Licenses" section, one can find information about applications that used the software licenses added in the "Applications > Software Licenses" section.



2.1.10.3. Reporting > Applications

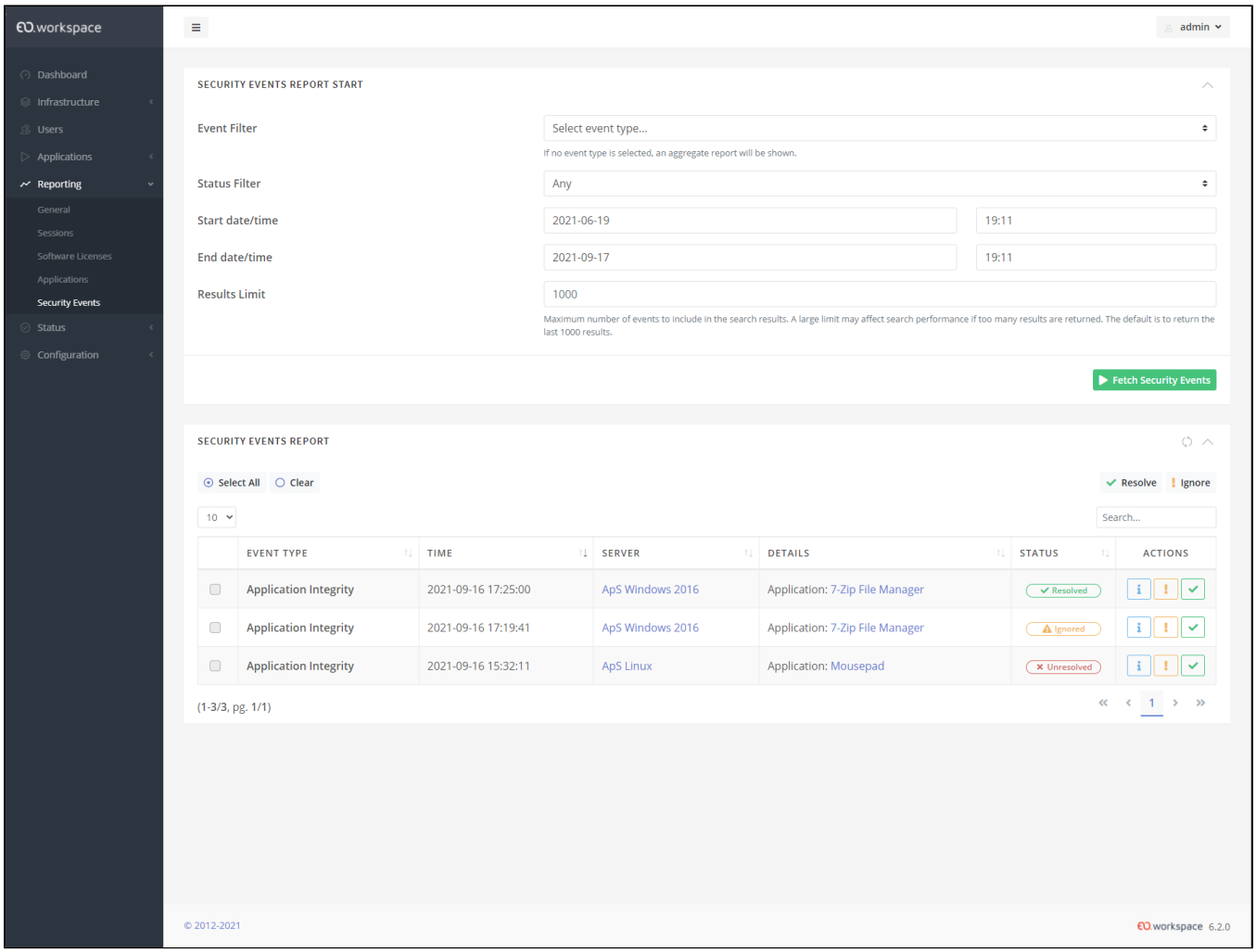
In the "Reporting > Applications" section, one can find information on applications used in a certain time period.



2.1.10.4. Reporting > Security Events

Introduced in version 6.2.

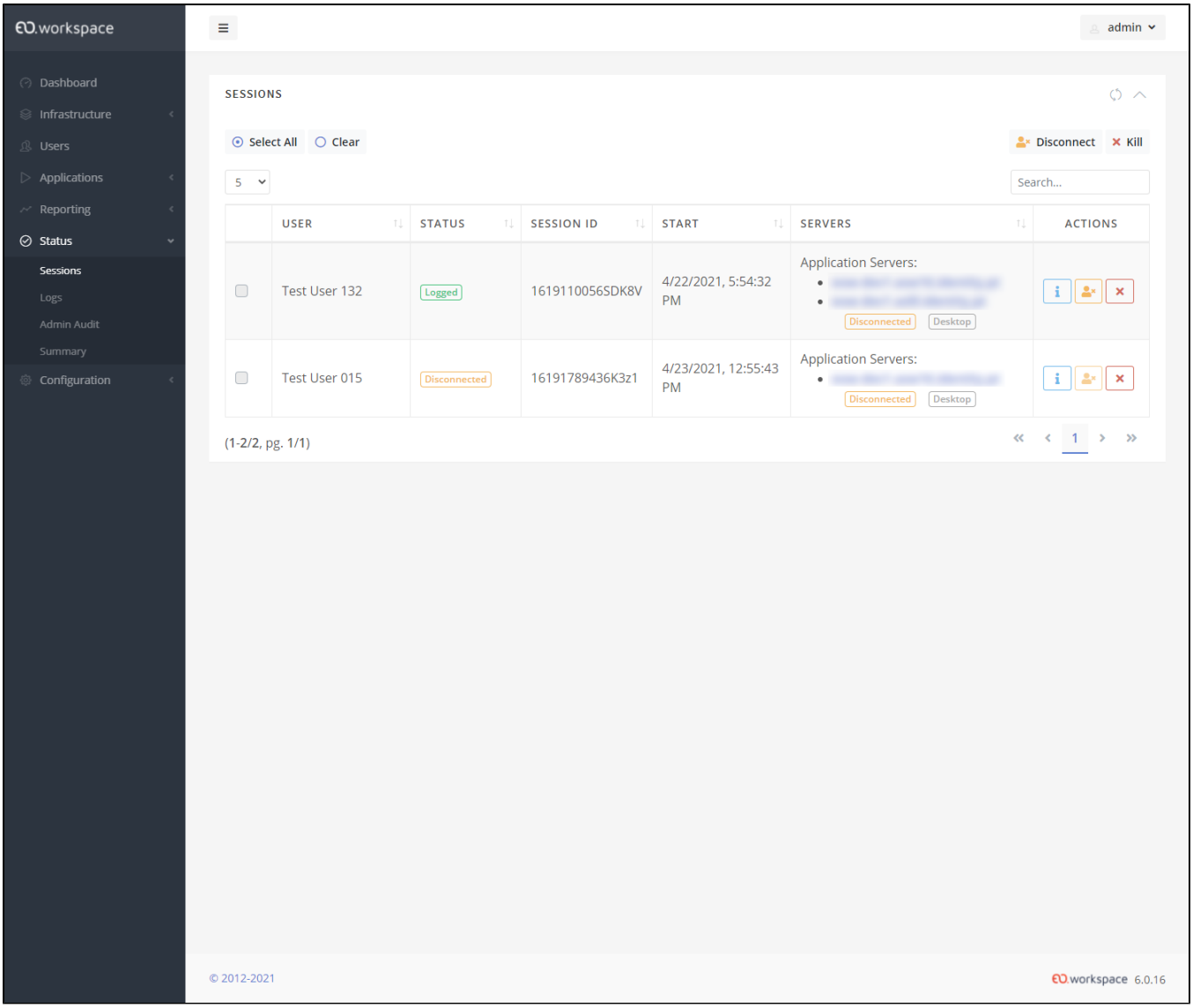
In the "Reporting > Security Events" section, one can obtain information about detected security events, such as security breaches if "Application Integrity" is configured, or screenshot attempts if "Screenshot Protection" is on. One can filter the displayed events by the type of event, its status and date of occurrence. When an event is detected, it is given the status "Unresolved". After analyzing the detected events, one can "Ignore" or "Resolve" the security events by clicking in the respective buttons on this interface.



2.1.11. Status > Sessions

On the "Sessions" sub-section, there's a list of currently active session on all application servers. In this section, it's possible to kill or disconnect any session. By selecting an individual section, it's possible to obtain in-depth information about it, such as its status, the associated user, when it was started and the currently published applications. To obtain information of finished sessions, check out the "Reporting > Sessions" section.

Introduced in version 6.4: When seeing the session details, it's also possible to initiate Shadowing for that session (if enabled).

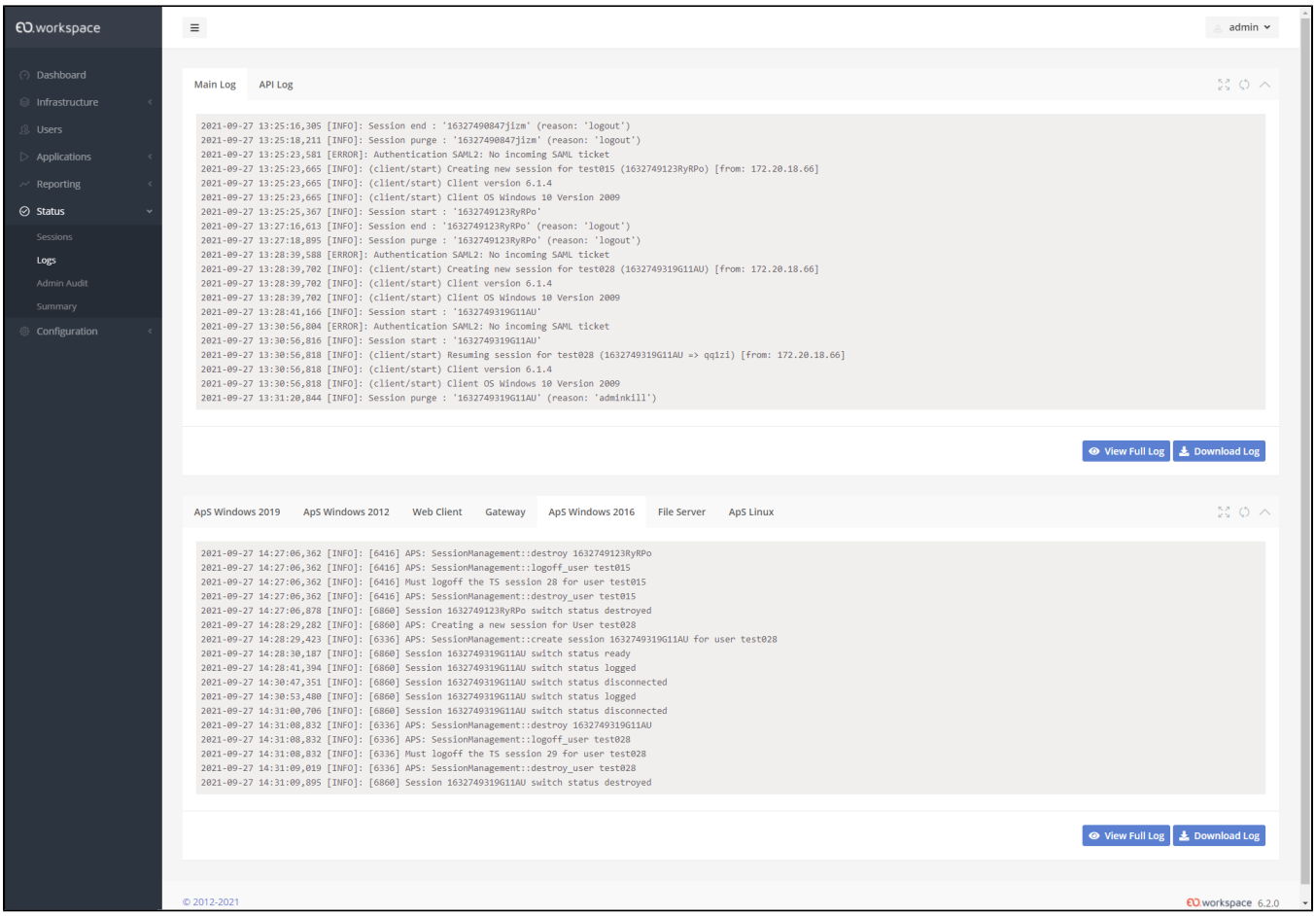


2.1.12. Status > Logs

In the "Logs" sub-section, you can read or download some of the log files described in the section "Log Files" below, without needing operating system access to the corresponding server. Note that this page only shows the most recent entries, click on "View Full Log" or "Download Log" to have access to older entries and verify if there are relevant log messages.

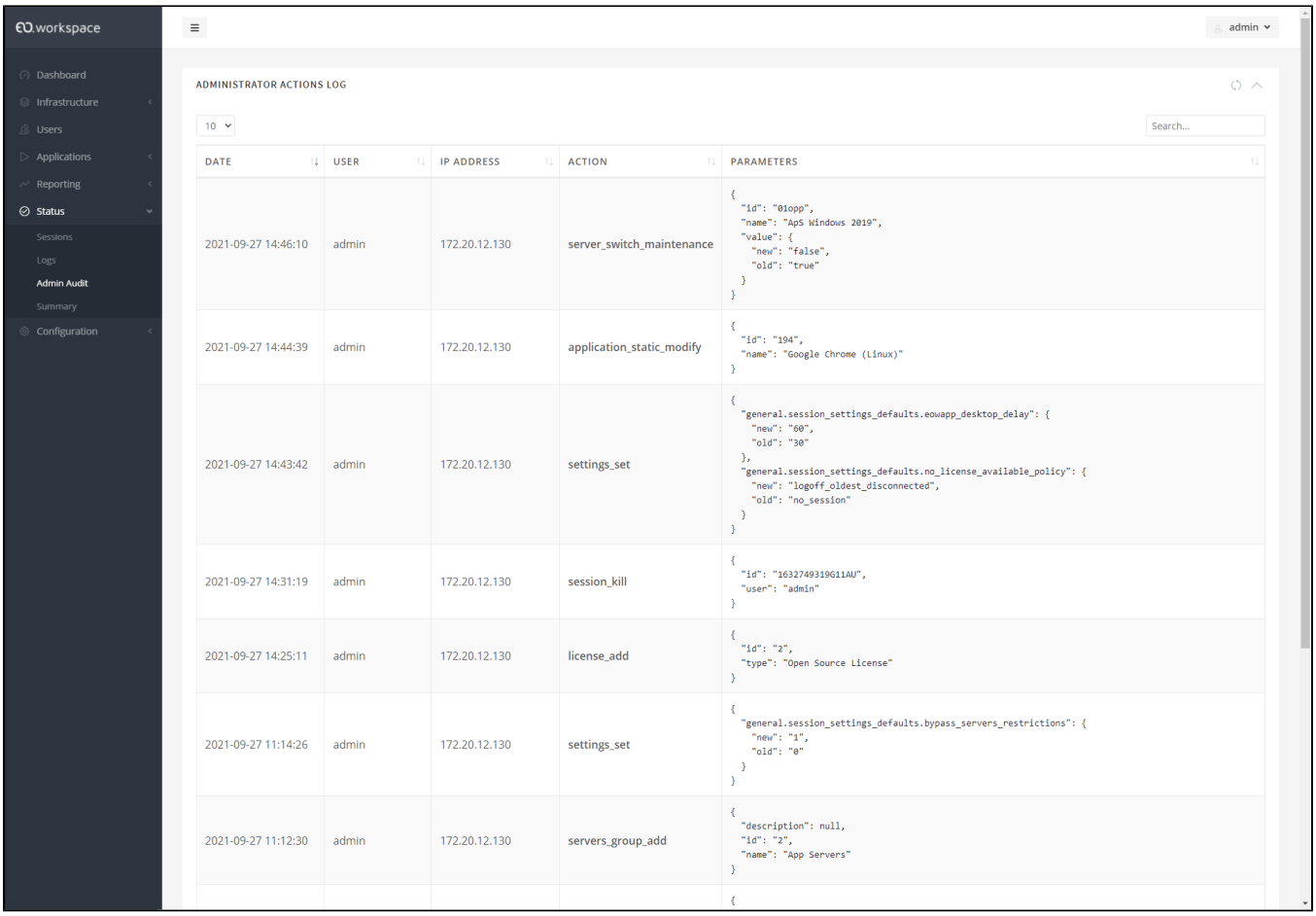
The log files available here are the following:

- Main Log - log pertaining to the Session Manager background tasks and connections.
- API Log - log pertaining to the API calls made by the Administration Console to the Session Manager service.
- Logs pertaining to the Slave Server process on relevant servers.



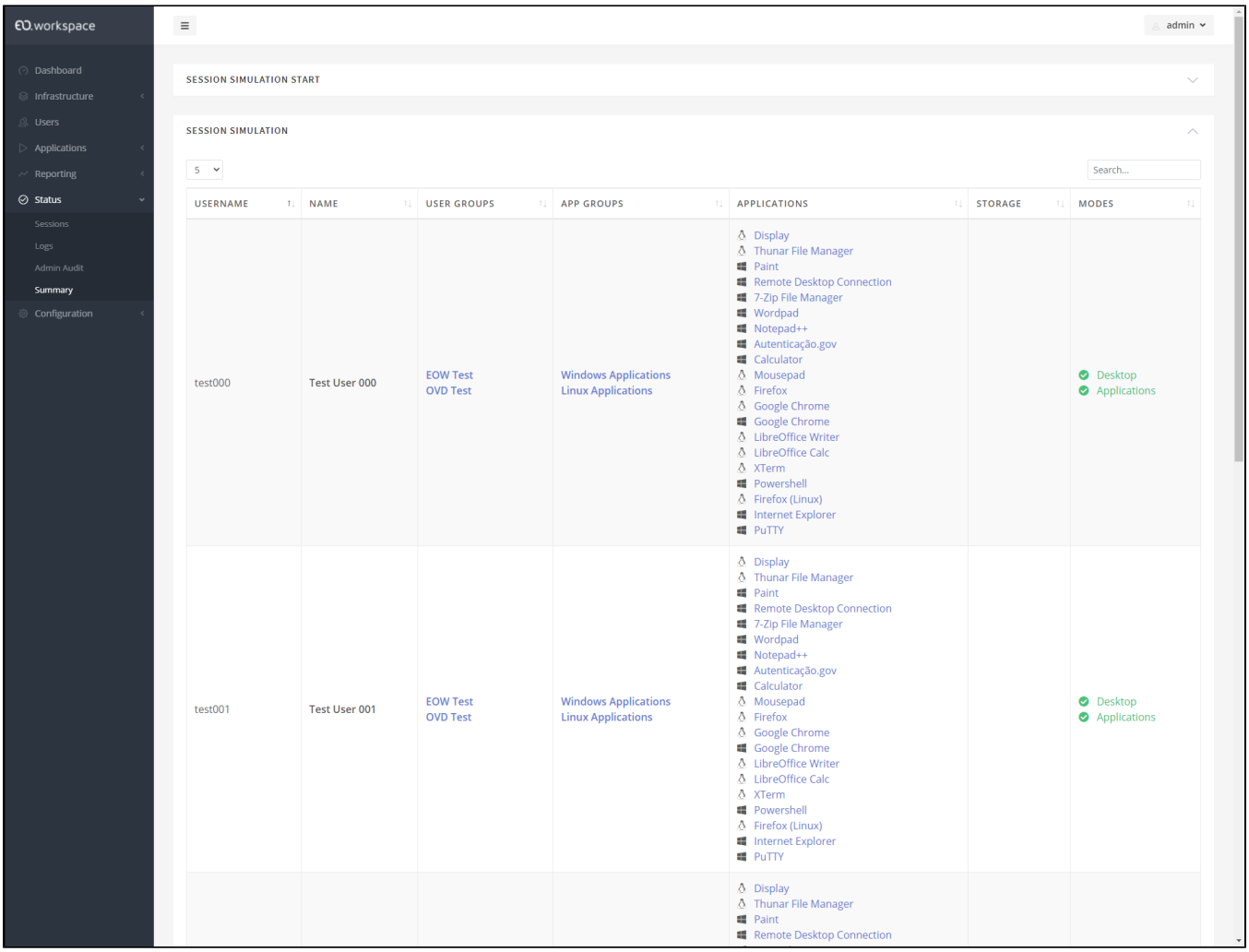
2.1.13. Status > Admin Audit

In the "Admin Audit" sub-section, you can see a list of every administrative and configuration-related action performed by each administrator user in the administration console.



2.1.14. Status > Summary

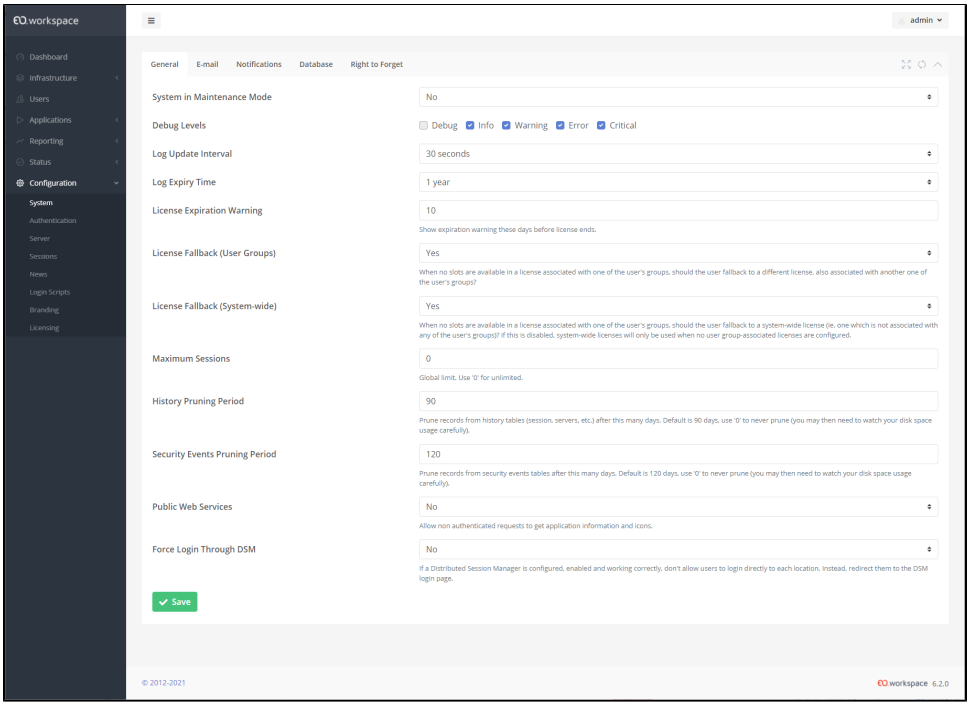
In the "Summary" section, use the "Username Search Term" field to filter for a user or a group of users and then click on the "Simulate Sessions" button. This action will simulate sessions in order to obtain the information on their names, user group membership, published applications and allowed access modes (desktop or application mode). This is useful to verify if the current configuration allow for the selected users to start sessions are to see which applications they have access to.



2.1.15. Configuration > System

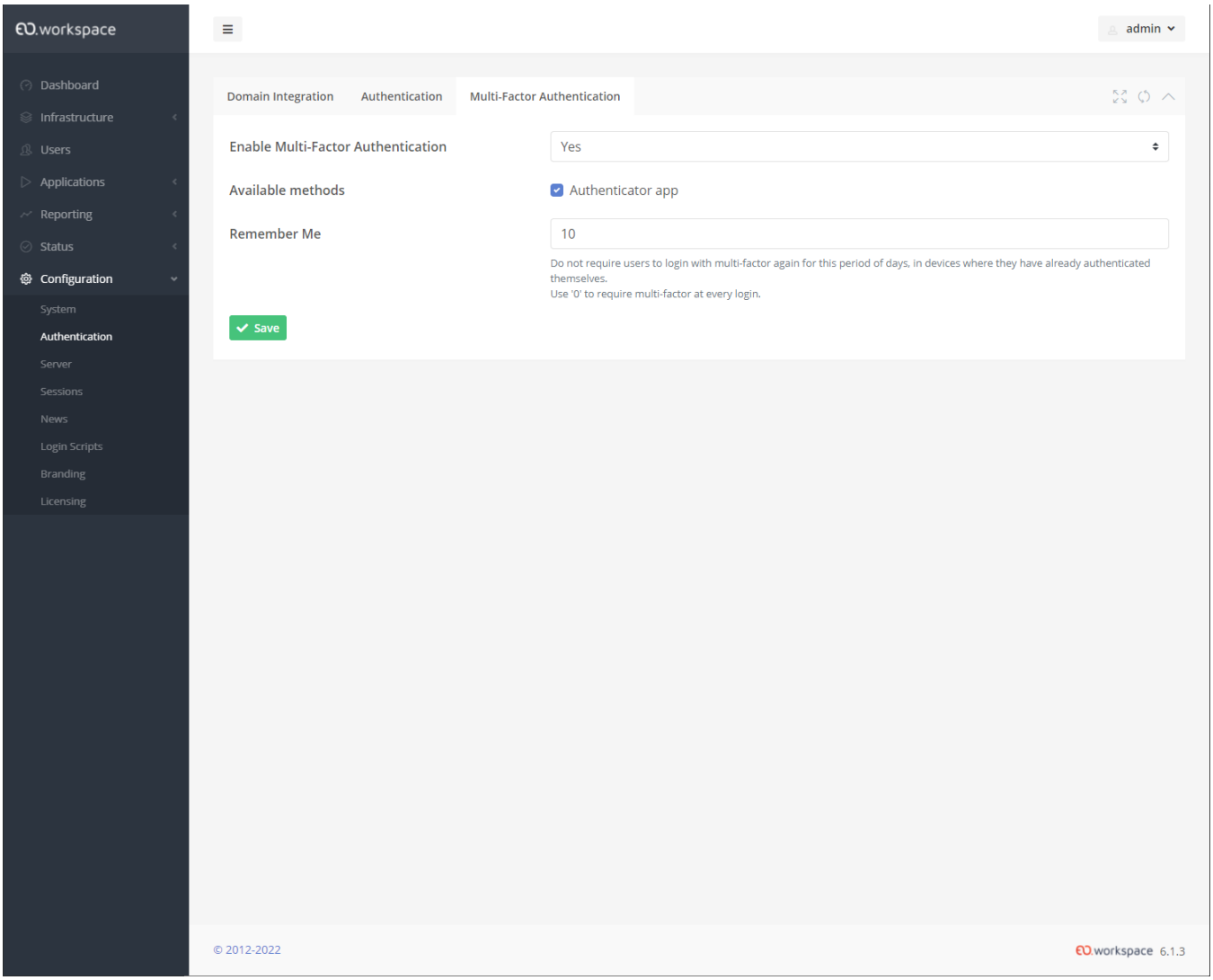
The "Configuration" section is where the system-wide parameters and configurations are made. The following is a short description of each section, which will also link to the relevant documentation for the more advanced configurations:

- General – system-wide configurations (such as logging level, enabled modules, default administration delegation policy, **Introduced in version 6.3:** ClientOS, **Introduced in version 6.4:** Session Shadowing);
- E-mail – e-mail settings (such as SMTP server, authentication details);
- Notifications – recipients and automated notification types to send (for administrators);
- Database – configuration of database parameters (such as database type, hostname, database, user name, table prefix);
- **Introduced in version 6.2:** Right to Forget - configuration of automatic anonymization or deletion of personal data (for more information, go to EO .workspace - Right to Forget).
- **Introduced in version 6.5:** Support - configuration of the automatic support request submission feature, available in the "Support" menu section.



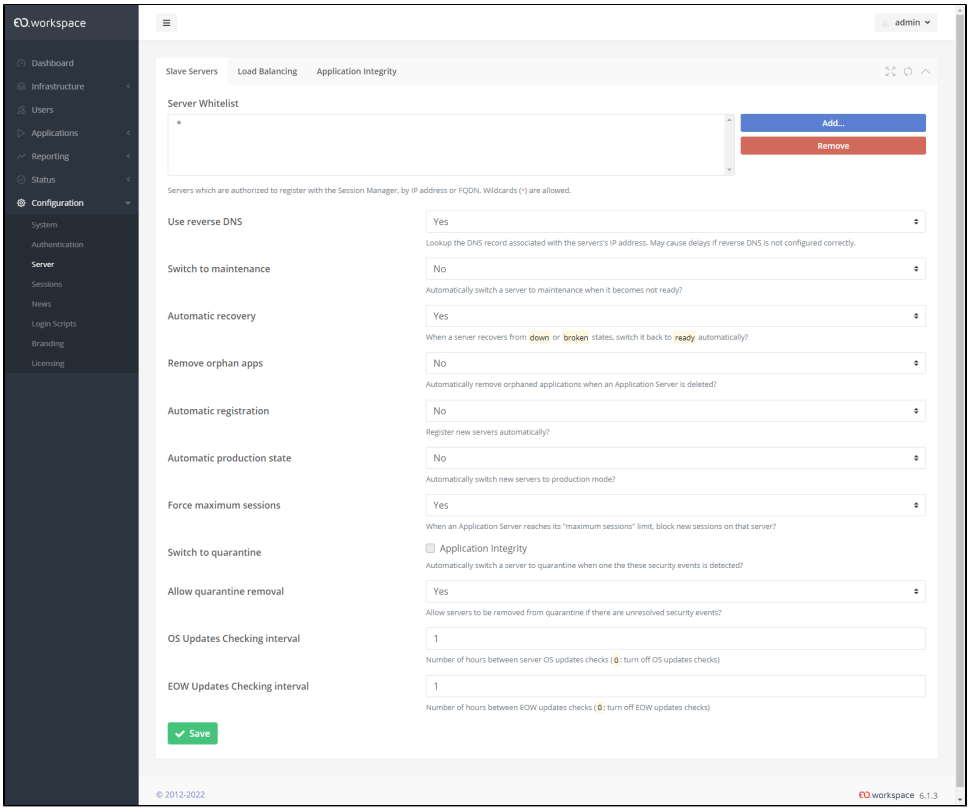
2.1.16. Configuration > Authentication

- Domain Integration – configurations regarding authentication and authorization integration with external sources, such as Microsoft Active Directory or LDAP. To get more details on the available authentication methods, check out EO.workspace - Domain Integration
- Authentication – configuration of single-sign on parameters (SAML2, CAS, etc.); To enable SAML2, check out the following article EO.workspace - SAML2 Configuration.
- **Introduced in version 6.3:** Multi-Factor Authentication – enable the integrated MFA method, which allows the use of an authenticator application (like Google Authenticator) as a second authentication factor for logins. After enabling this option, users will need to use the web or native client the first time that they log in, so that they can access a page that will allow them to setup MFA. If a user loses access to their authenticator application, the MFA configuration can be reset in the section 'Users' by selecting the 'Edit' option for that user. If the 'Remember Me' setting is saved with a number different from '0', the users will have the option to skip the second authentication factor in devices where they have already authenticated themselves.
- **Introduced in version 6.6:** User Assurance – enable the usage of user assurance methods, taking advantage of biometrics and AI. If enabled, allows the configuration of face recognition mechanisms on the EOW login process.



2.1.17. Configuration > Server

- Slave Servers – default slave server parameters;
- Load Balancing – load balancing policy among application servers;
- **Introduced in version 6.2:** Application Integrity - enable or disable the application integrity verification and configure its parameters.



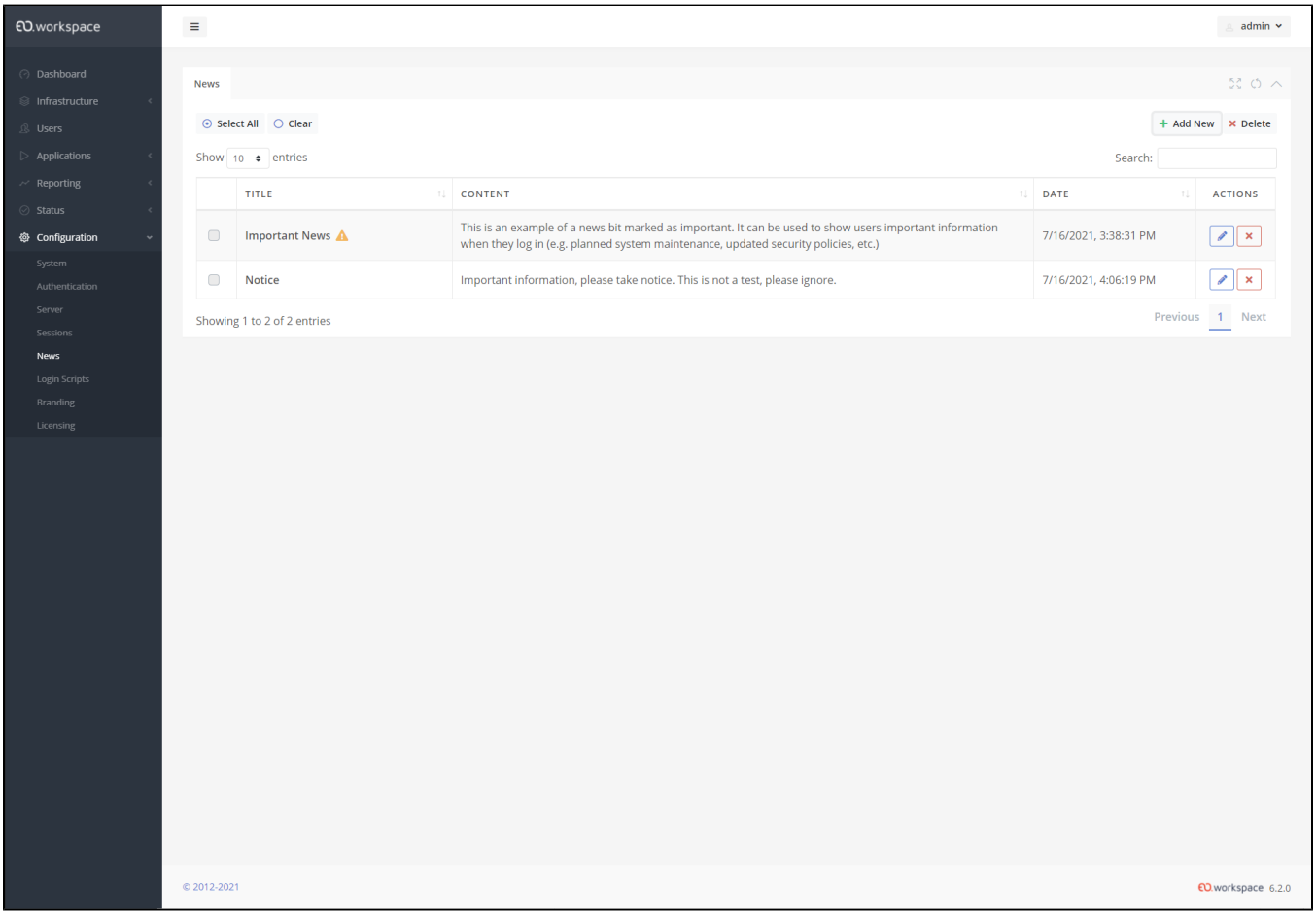
2.1.18. Configuration > Sessions

- Sessions – configurations and default parameters regarding user sessions;
- Desktop Mode – for desktop mode specific settings;
- Application Mode – for application mode specific settings;
- **Introduced in version 6.5:** Screenshot Protection – for configuring detection and/or blocking of screenshots in the Native Clients. Options are separated by OS, since not all OSes offer the same protections. If detection is enabled, you can choose to have security events reported in the admin console if users take a screenshot of the application, and a warning popup displayed in the native client to the users. If blocking is enabled, the application will not be displayed on the screenshot.

2.1.19. Configuration > News

In this section, one can add notifications which are shown once to users when they start new sessions. This can be used for system-related notifications, (e.g. announcing downtime, maintenance periods, updates, etc.) or company-related notifications (e.g. show privacy policy). These messages are shown in a notifications menu for every user in the EOW clients. It is also possible to automatically show them in a pop-up on session start, without user interaction, by selecting one or two of the following attributes:

- **Important**: Show the news item as pop-up which must be dismissed before any further interaction is possible.
- **Persistent**: If the news item is marked as Important and also marked as Persistent, it is shown on every login.

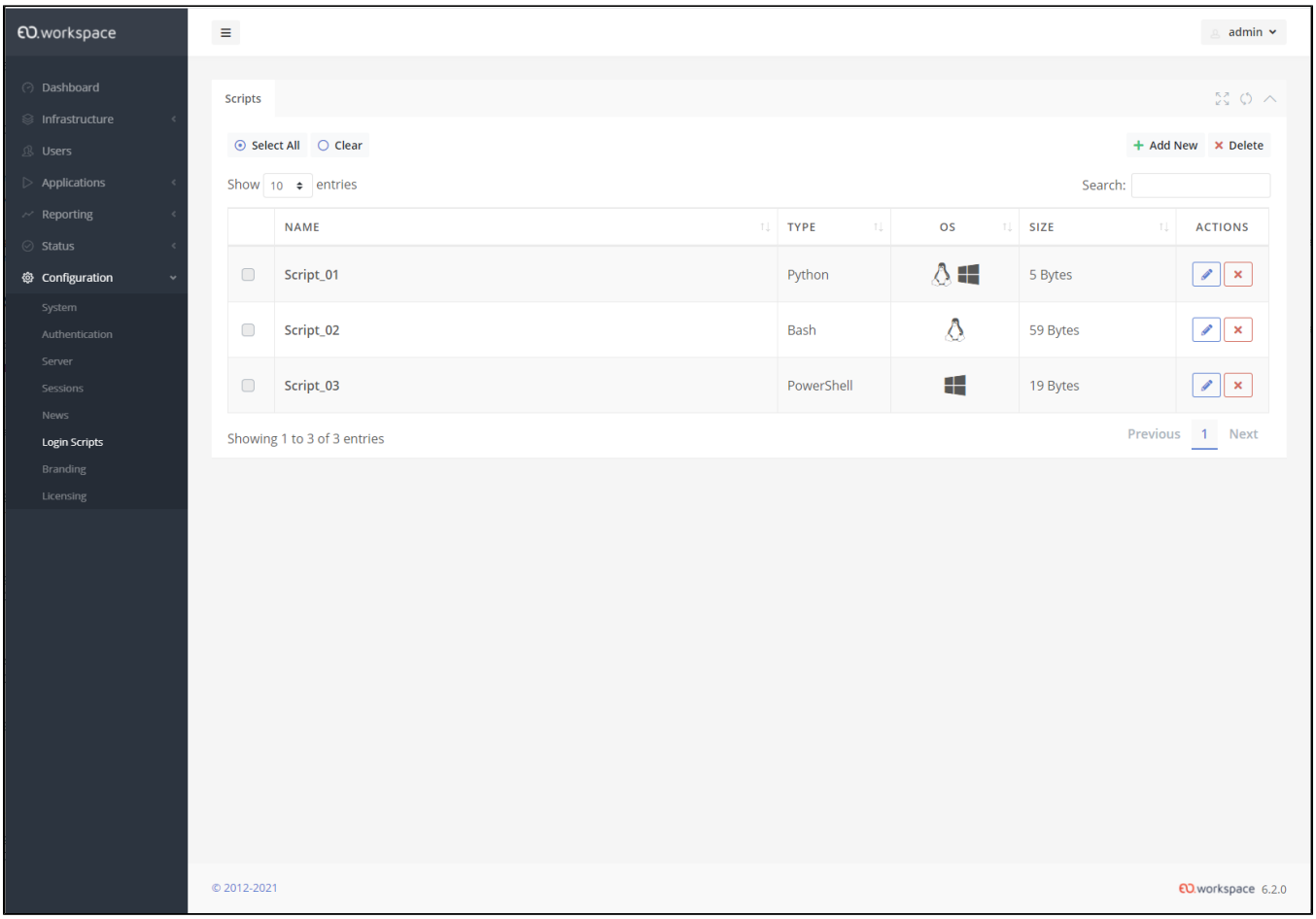


2.1.20. Configuration > Login Scripts

In this section, one can configure scripts to run when a user logs in to a session. Note that these scripts are executed in the user context, not as an administrator user.

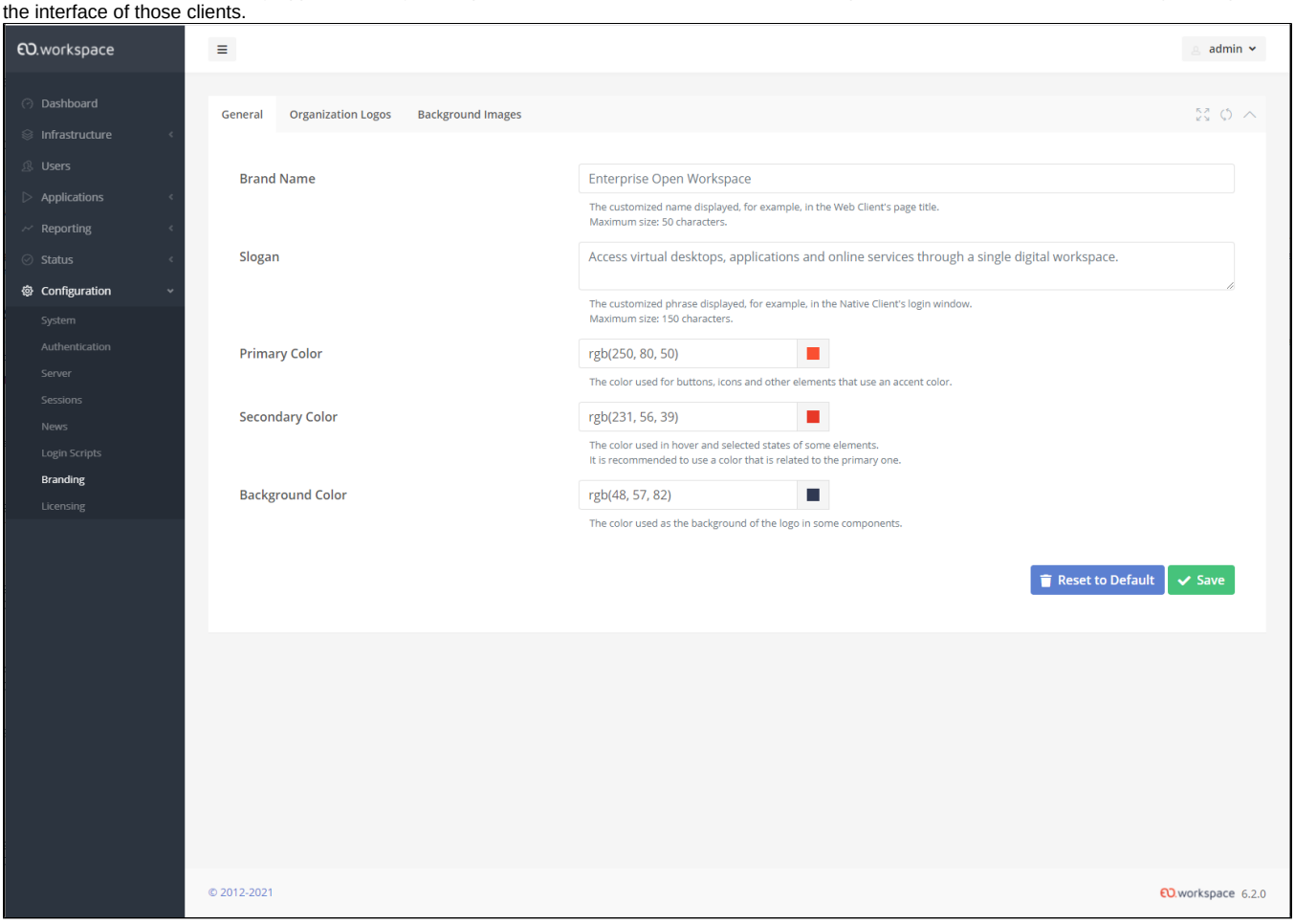
The following script types are supported for the different Operating Systems:

- **Windows and Linux**: Python
- **Linux**: Python, Bash
- **Windows**: Python, Batch (.bat), PowerShell, VBScript



2.1.21. Configuration > Branding

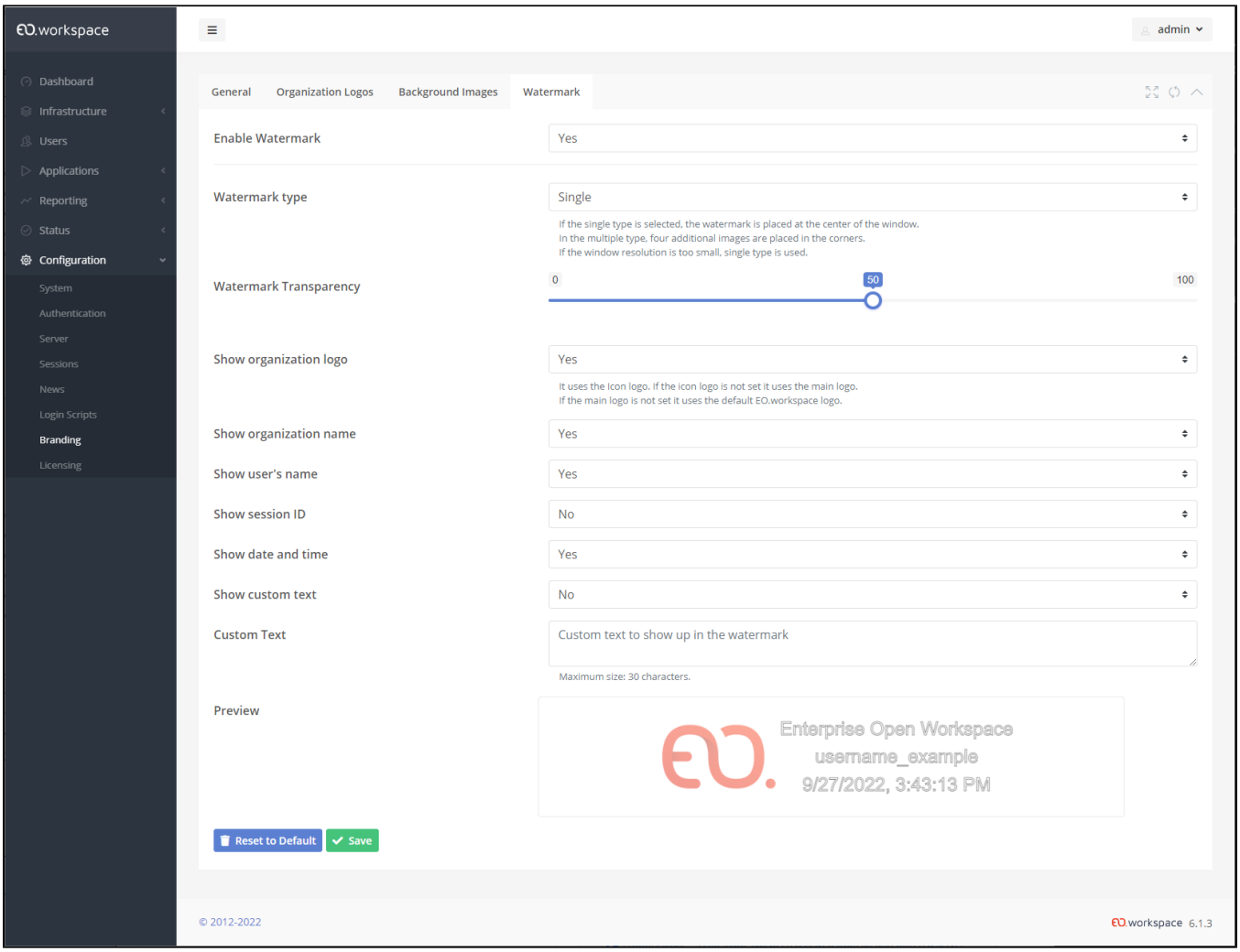
Allows the configuration of branding elements on the EOW solution (organization, slogan, colors, logos, background images, etc.). These branding elements are then automatically applied to every client (Web Client, Native Client and Mobile Clients) that connects to this Session Manager, adapted to the interface of those clients.



2.1.21.1. Configuration > Branding > Watermark

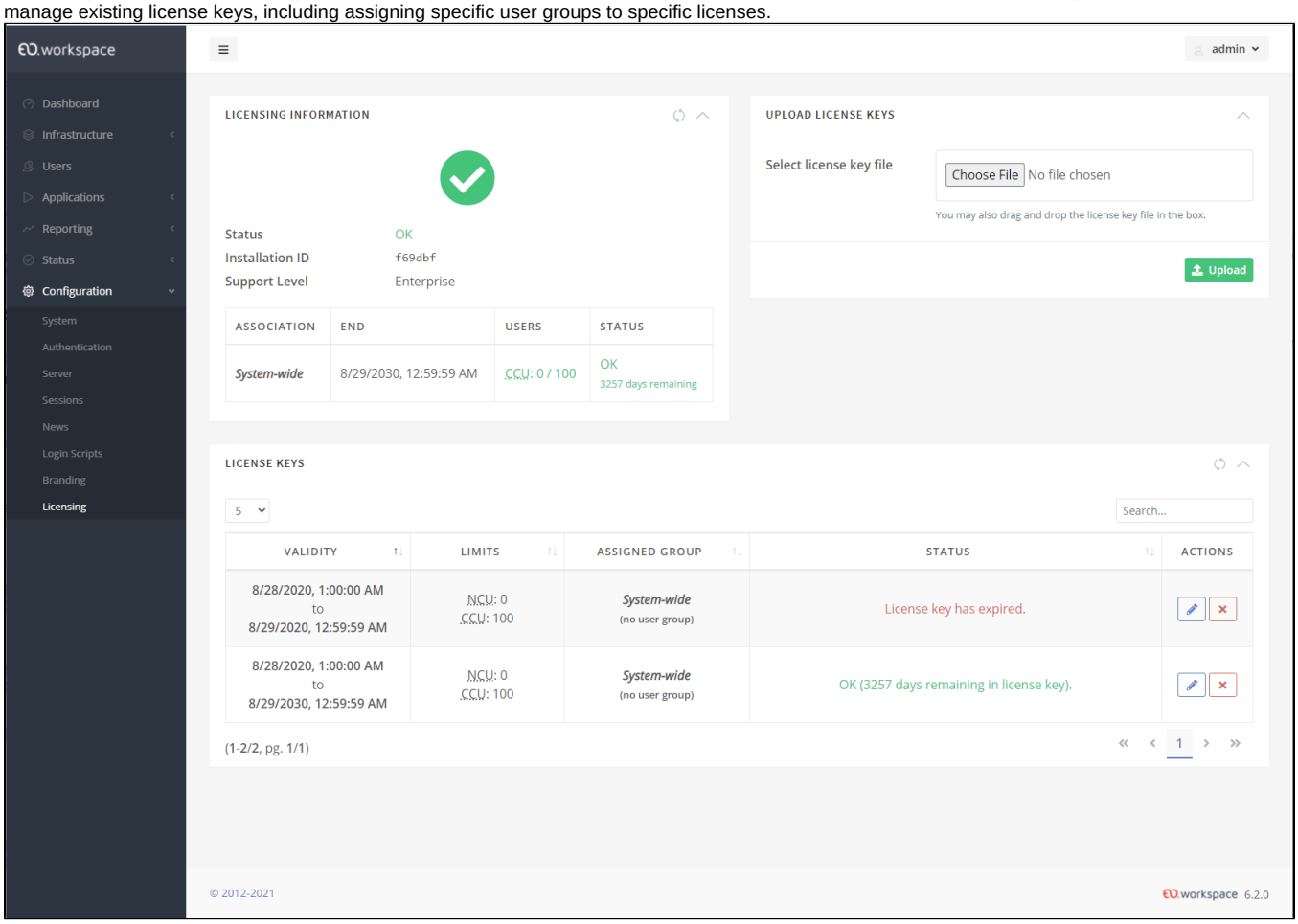
Introduced in version 6.4.

Enable a watermark that is drawn over the user's session and configure its elements (logo, organization name, username, date, etc). If there is a custom logo and brand name defined, these are also used in the watermark. The watermark is applied to every session, regardless of client or session mode.



2.1.22. Configuration > Licensing

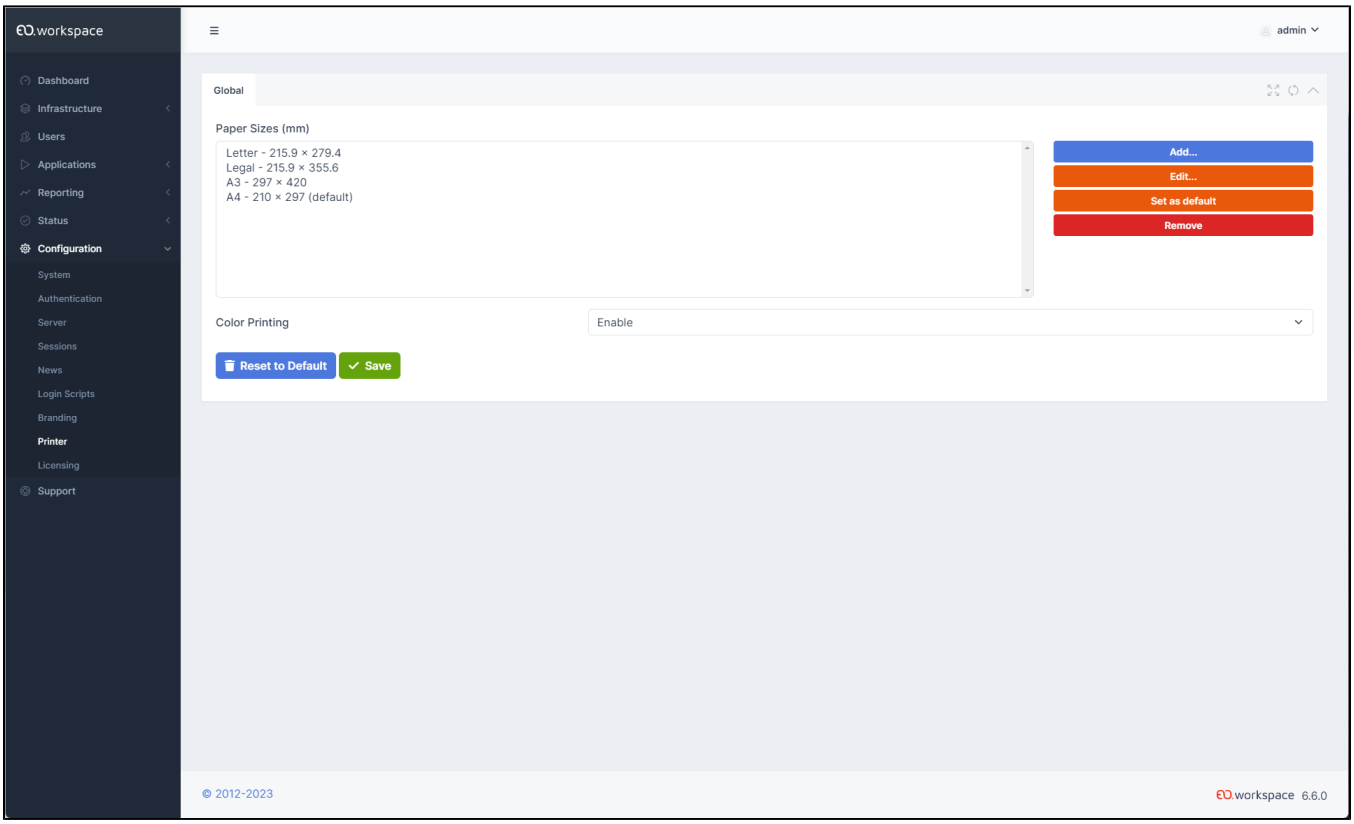
EO.workspace license and subscription key management. In this section, it is possible to consult the current licensing status, upload new license keys, and manage existing license keys, including assigning specific user groups to specific licenses.



2.1.23. Configuration > Printer

Introduced in version 6.6.

In this section, it is possible manage printing settings that are available to users when they use printers during an EOW session.



There are the following options:

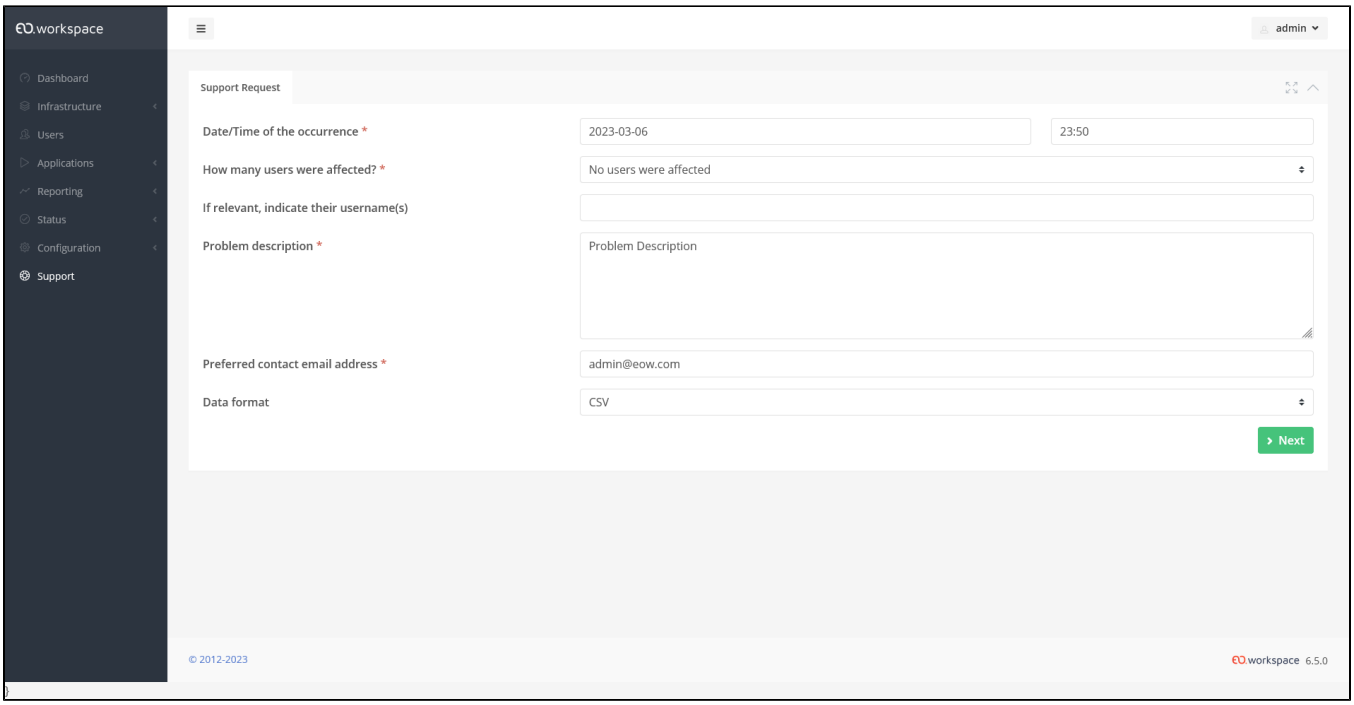
- **Paper Size**: Add a custom paper size by assigning it a Name, Width, and Height. Alternatively, you can simply select a standard size and add it to the list of available paper sizes. Paper sizes can also be edited and deleted.
- **Default Paper Size**: Define a paper size as the default. For Windows applications, please note that if the Letter paper size is available, that will always appear as the default.
- **Color Printing**: Enabling this option allows users to print in color. In Windows applications, users can select to print in black and white or in color and in Linux applications, it will always print in color. When disabled, it restricts printing to black and white only for both Windows and Linux applications.
- **Reset to Default**: By clicking on this, all Paper Sizes in the table will be removed, and Letter, Legal, A3 and A4 will be added, with A4 as the default.

If any modifications are made to these configurations, restart the EOW session for the changes to take effect.

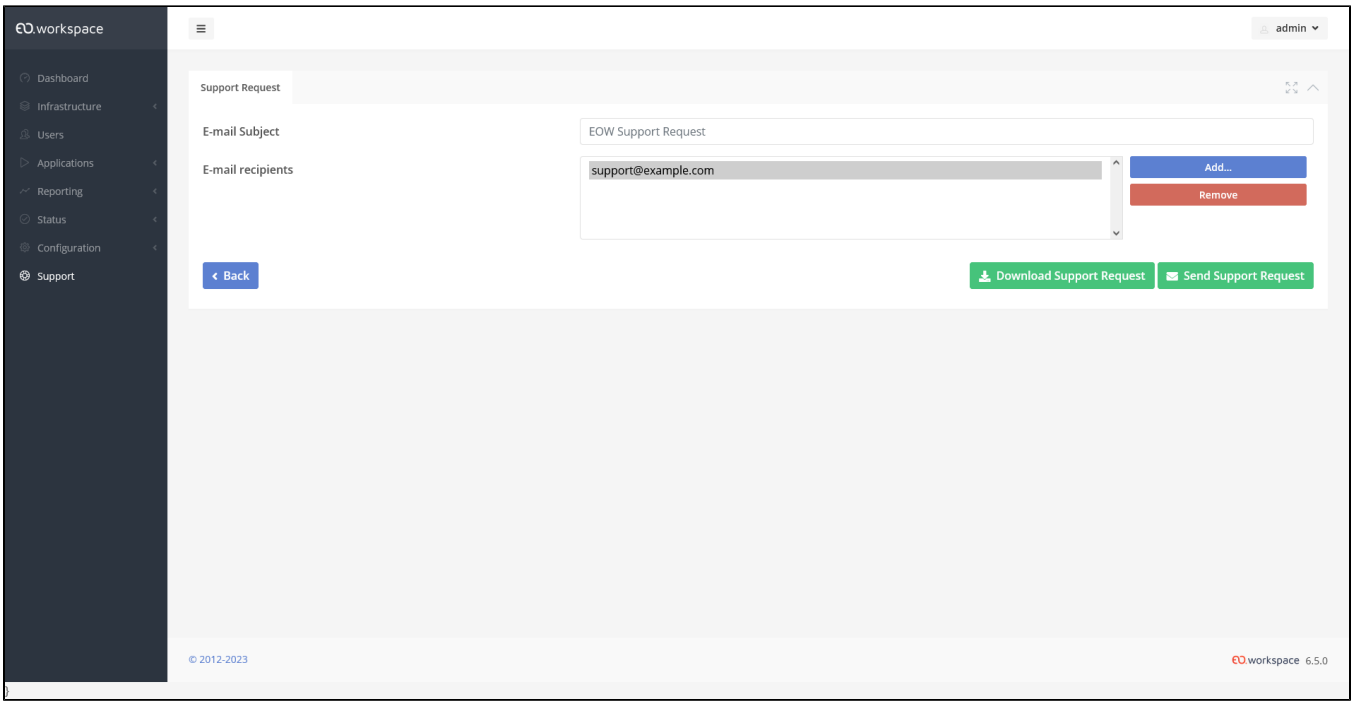
2.1.24. Support

Introduced in version 6.5.

The "Support" section contains a wizard for creating support requests using data present in the Administration Console, including server logs and the admin audit. The first section contains a series fields which are used to detail an ongoing issue or problem in the existing EOW infrastructure. After filling these fields, the Administration Console will automatically retrieve the necessary information and prepare the support request in the chosen format.



On the second section, it is possible to download the created support request as a zip, or directly e-mail the support request to one or more e-mail addresses. Note that in order to use the e-mail option, the Administration Console E-mail Delivery must be configured in **Configuration > System > E-mail**, and the available E-mail recipients are retrieved from the **Configuration > System > Notifications** section.

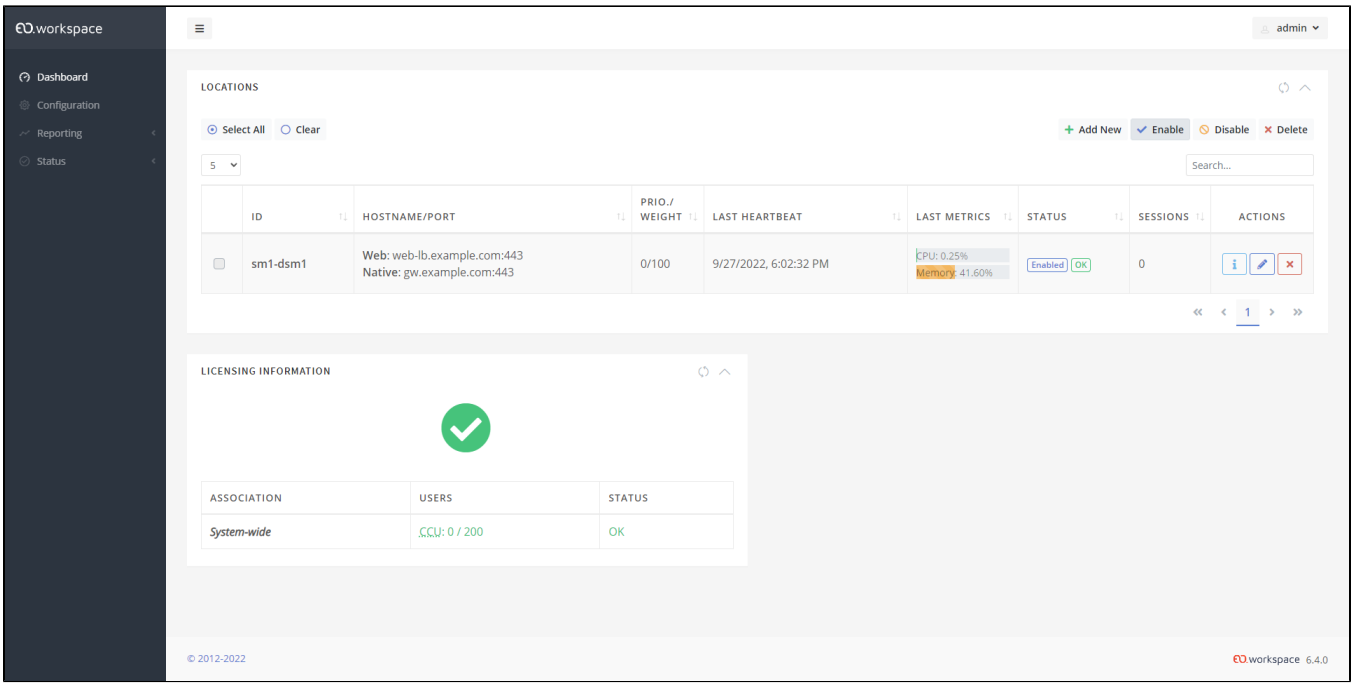


2.2. Distributed Session Manager (DSM) Administration Console

The Distributed Session Manager (DSM) Administration Console allows you to configure a specific DSM server.

It's through the following URL:

- `https://<dsm hostname>/admin`



When you configure an EOW landscape which uses DSM server, it's not only necessary to configure the directly (as described in this section), but also configure the connected Session Manager servers, as described in the corresponding section:

- Infrastructure > Scaling

The configuration is performed in the DSM administration console "Dashboard" section, and the following configurations are required on the DSM side:

- **ID:**
  - The same ID (name) defined in the Session Manager side.
  - Can't be changed after creation (only by deleting and recreating the location configuration).
- **Hostname** :
  - Redirection hostname for web clients
  - It normally is the Web Client or Web Client Load Balancer hostname.
- **Port**:
  - Optional redirection port for web clients.
  - The default value is 443, as its the default port for HTTPS connections.
- **Application Hostname**:
  - Redirection hostname for native clients.
  - It normally is the Gateway hostname.
- **Application Port**:
  - Optional redirection port for native clients.
  - The default value is 443, as its the default port for HTTPS connections.
- **Priority**:
  - The priority of this location.
  - Use the default "0" value if you don't need to configure priorities.
- **Weight**:
  - The weight of this location.
  - Use the default "100" value if you don't need to configure priorities.
- **Token**:
  - The same token defined in the Session Manager side.

If the Session Manager is able to test the Test URL and send the heartbeat message to the Ping URL:

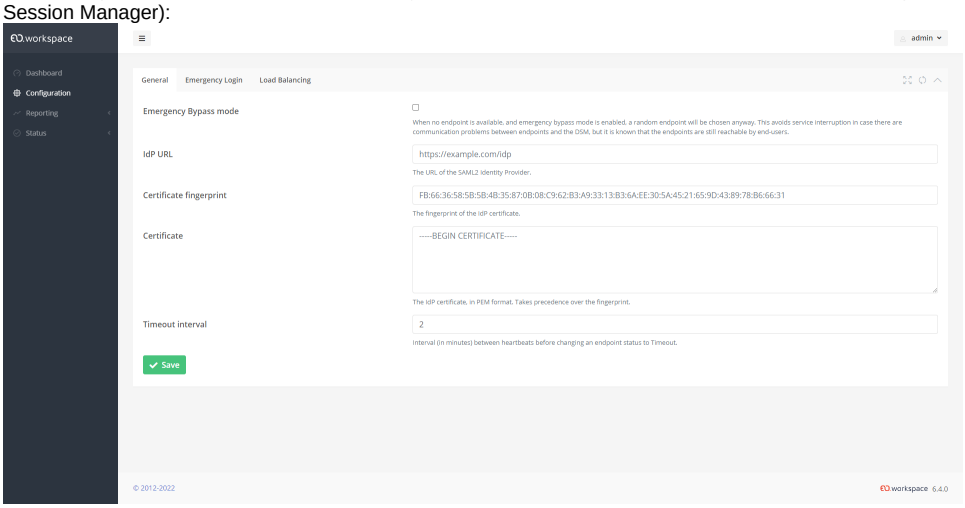
- A **green check mark** will appear on the "Status" column of the Session Manager DSM configuration.
- A **green "OK" badge** will appear on the DSM configuration console.

If the status indicator on the Session Manager DSM configuration is a **red cross**, hovering over it will reveal the error cause. This should also be available on the Session Manager "Main Log".

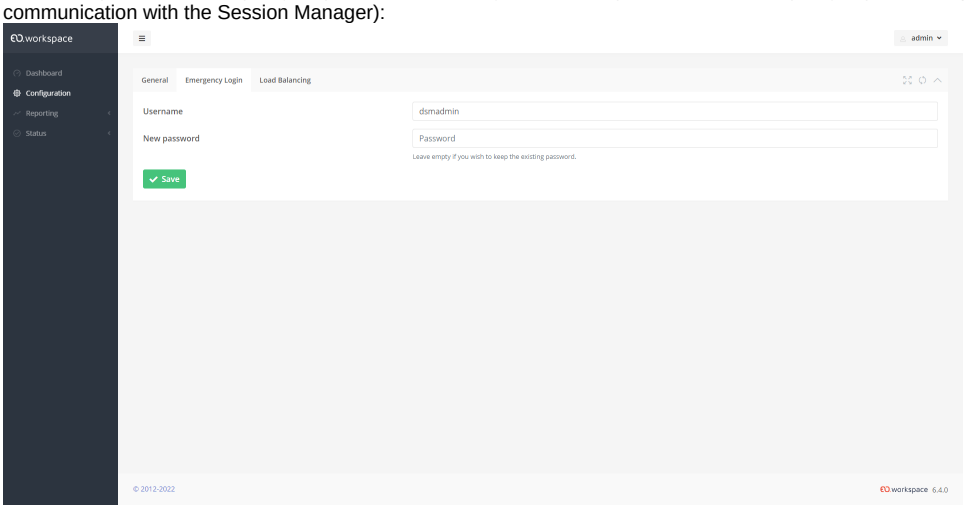
Additional DSM-related configurations on the Session Manager are available in the "Configuration" section of the Administration Console, and are described in the appropriate section.

On the DSM administration console, you also have some additional sections, namely:

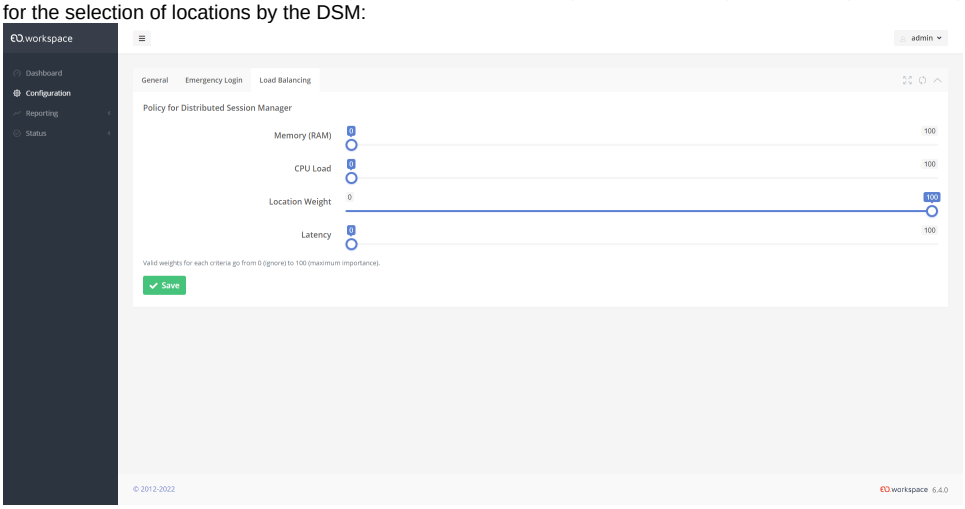
- The "Configuration > General" section, where you can find some DSM and SAML authentication configurations (which should match those on the Session Manager):



- The "Configuration > Emergency Login" section, where you can configure the DSM emergency login details (which will work even if there's no communication with the Session Manager):



- **Introduced in version 6.4:** The "Configuration > Load Balancing" section, where you can configure the weight of each available metric/indicator for the selection of locations by the DSM:



There are also the "Reporting" and "Status" sections of the DSM administration console, where you can see reports on DSM usage, as well as the current status (established sessions, logs, etc.).

3. Operation

3.1. Configuration files

There are several configuration files which can be edited for more advanced configurations.

These files do not need to be edited in the majority of the cases, but they're documented here if the need arises.

Please be careful when changing these configurations, only do it when fully aware of all the implications. Editing these files with incorrect values may cause service unavailability and inability to receive proper support.

3.1.1. Session Manager configuration files

The configuration files for the Session manager are located in `/etc/eow/session-manager/ .` There are various Apache configuration files for different modules of the Session Manager module (`apache2.4.conf`, `apache2.4-admin.conf` , `apache2.4-vhost-server.conf` *)*, one *cron* file defining the session manager *cron* tasks to be run, `sessionmanager.cron`, and one settings file, `config.inc.php`:

```
<?php
define('SESSIONMANAGER_SPOOL', '/var/spool/eow/sessionmanager');
define('SESSIONMANAGER_LOGS', '/var/log/eow/sessionmanager');

define('SESSIONMANAGER_CONFFILE_SERIALIZED', SESSIONMANAGER_SPOOL.'/config');

//...

// Emergency administration account. Password is SHA256 hashed with salt.
define('SESSIONMANAGER_ADMIN_LOGIN', 'admin');
define('SESSIONMANAGER_ADMIN_PASSWORD', '40ee285b86554a814a5817a0b7f216b0');
define('SESSIONMANAGER_ADMIN_SALT', 'zerUMwLZg3pcFE8q');
//define('SESSIONMANAGER_ADMIN_DEBUG', true);
```

This file is used to define the locations of the session manager spool, logs and serialized configuration file and to define the session manager admin login.

If one needs to change configurations after the initial setup of the session manager, the following command can be used:

```
# eow-session-manager-config
```

3.1.2. Administration Console configuration files

The configuration files for the Administration Console are located in `/etc/eow-admin/`. There is one configuration file, `config.json`, one TLS private key (`key.pem`) and one TLS certificate (`cert.pem`):

```
{
    "sessionmanager": {
        "host": "localhost"
    },
    "keys": {
        "sign": "4pb2jbHVDV3kl5w7NLnLjQIqmu/yKGF6RclTU+2nnyuD9UM2nevCpnKBbiH8k+2bUKfrIt0FGdp54Rtqq+vniZkA==",
        "encrypt": "Q9Gzsq2jTGeGl/Ilgz70dq2LYg7bfdfsd443HqnOtA="
    }
}
```

If one needs to change configurations after the initial setup of the administration console, the following command can be used:

```
# eow-admin-config
```

3.1.3. Web Client configuration files

The configuration files for the Web Client are located in `/etc/eow/web-access/`. There are two Apache configuration file, `apache2.4.conf` and `apache2.4-html5.conf`. There are two separate files for configuration specific to the Web Access component:

- `config.client.ini` is used to hardcode certain network settings for sessions established through the web client, like for example using packet compression or TLS or defining socket timeout;
- `config.inc.php` is used to configure other settings related to the web interface login screen, like forcing fullscreen mode or SSO, defining the default language and keymap, and establishing whether the HTML5 web client is available or not.

These files contain configuration which affect the specific Web Client server in which they are stored. For system-wide branding or customization options, please use the administration console.

If one needs to change configurations after the initial setup of the web client, the following command can be used:

```
# eow-web-access-config
```

3.1.4. Slave Server configuration files

All Slave Servers, independent of their role, use one main configuration file which is divided into different sections for each role, located at `/etc/eow/slaveserver/slaveserver.conf`. The first section is used by all slave servers, and defines the IP of the Session Manager, the Slave Server role, and the log level:

```
[main]
session_manager = session-manager-server.example.com
# stop_timeout define the time in second granted to the service to stop
# for infinit, use 0
# default is 600 (10 minutes)
# stop_timeout = 20
roles = Gateway

# server_allow_reuse_address = true|false
# On Windows, if we authorize this parameter, two servers can bind on the same ip
# default is true for linux and false for Windows
# server_allow_reuse_address =

[log]
# level =
# can be error, warn, info, debug
# multi occurence of 'debug' are allowed to enable deeper debug messages
# "*" pattern is an alias to error, warn, info and debug
level = error warn info
# file =
# the log file to use. Default is autodetect
#
# thread = 1
# use a dedicated thread for logger or not
# default is yes
```

Further sections in the log file are specific to a certain role and only used by slave servers fulfilling that role (eg. `ApplicationServer`, `Gateway`, `FileServer`, etc.).

If one needs to change configurations after the initial setup of the slaveserver, the following command can be used:

```
# eow-slaveserver-config
```

3.1.5. Distributed Session Manager configuration files

The configuration files for the Distributed Session Manager are located in `/etc/eow-dsm/`. There is one configuration file, `config.json`, one TLS private key (`key.pem`) and one TLS certificate (`cert.pem`):

```
{
  "sessionmanager": {
    "host": "sm.example.com"
  },
  "database": {
    "type": "mysql",
    "server": "localhost",
    "name": "eow_dsm",
    "user": "eow",
    "password": "password"
  },
  "keys": {
    "sign": "ba8cMtjBHUDUTeRiEAMJS9aQt20PWHTGPNBdxBsLfWqktL72iZrSqtI8uJGdeh4qiop1FDHRdsCz3zre58ZKsQ==",
    "encrypt": "MHkR8c6tED/Wnlvkuk+y2kpzznDm2Y8cVh2jEI+Y6UQ="
  }
}
```

If one needs to change configurations after the initial setup of the administration console, the following command can be used:

```
# eow-dsm-config
```

3.1.6. Native Client configuration files

The current Native Client configuration is saved in different places depending on the system in use:

- Linux: `~/.config/Enterprise Open/EO.workspace Client.conf`
- macOS: `~/Library/Preferences/com.enterpriseopen.EO.workspace Client.plist`
- Windows: Stored in the Microsoft registry. The Native Client reads the `HKEY_CURRENT_USER` tree. The path to the registry data is `Software\Enterprise Open\EO.workspace Client`.

3.2. Log files

Most important EOW log files are available to read or export from the Administration Console.

However, for additional log resources, as well if you want in some way copy or process the log files directly, here is a list of relevant log files for each server type or component.

3.2.1. Session Manager/Administration Console Logs

Log locations on the Session Manager server:

- `/var/log/eow/session-manager/main.log` (log pertaining to the Session Manager background tasks and connections);
- `/var/log/eow/session-manager/api.log` (log pertaining to the API calls made by the Administration Console to the Session Manager service);
- `/var/log/httpd/ssl_access_log` (log with requests made to the services hosted on the Session Manager server: Administration Console and the Session Manager itself);
- `/var/log/httpd/ssl_error_log` (log with errors related to the services hosted on the Session Manager server: Administration Console and the Session Manager itself).
- `/var/spool/eow/session-manager/cache/logs/` (local cache of the Slave Server logs received from all Slave servers).
- `/var/log/php-fpm/` (PHP logs).

When debugging web services errors (such as "HTTP Error 500" reported by the client), the most useful log is the Apache `error_log`, which usually reports the cause of the internal server error. This is usually caused by failing PHP code, and the details can be seen here. When debugging session-related errors (such as sessions being disconnected on purpose, or login failures), the Session Manager `main.log` is the one that contains more information related to it. The `api.log` file usually contains useful information about errors related to the Administration Console. The Apache `ssl_access_log` contains useful information about the requests being made by the clients and Administration Console, as well as the corresponding HTTP return codes. The `main.log`, `api.log` and Application Server log files are accessible (with some limitations) through the Administration Console.

You can also view the Administration Console startup, error and access log by using the following command:

```
journalctl -ru eow-admin
```

3.2.2. File Server logs

Log locations on the File Server:

- `/var/log/eow/slaveserver.log` (log pertaining to the File Server Slave Server process);
- `/var/log/samba/log.smbd` (logs pertaining to Samba and CIFS shares);
- `/var/log/httpd/access_log` and `ssl_access_log` (log with requests made to the File Server Slave Server role);
- `/var/log/httpd/error_log` and `ssl_error_log` (log with errors related to the File Server Slave Server role).

3.2.3. Application Server logs

Log locations on the Application Server (Windows):

- `%PROGRAMDATA%\EOW\slaveserver\log\slaveserver.log` (log pertaining to the Application Server Slave Server process);
- `%PROGRAMDATA%\EOW\slaveserver\sessions\` (logs pertaining to currently active sessions);
- `%PROGRAMDATA%\EOW\slaveserver\spool\sessions dump archive\` (logs pertaining to past sessions).

Some useful information is also registered on the Windows Event Log, on the "Applications" section.

Log locations on the Application Server (Linux):

- `/var/log/eow/slaveserver.log` (log pertaining to the Application Server Slave Server process);
- `/var/log/xrdp*.log` (log pertaining to the xrdp process);
- `/var/spool/eow/slaveserver/sessions/` (logs pertaining to currently active sessions);
- `/var/spool/eow/slaveserver/sessions dump archive/` (logs pertaining to past sessions).

3.2.4. Web Client logs

Log locations on the Gateway server:

- `/var/log/eow/slaveserver.log` (log pertaining to the Web Client Slave Server process);
- `/var/log/httpd/ ssl_access_log` (log with requests made to the Web Client Slave Server role);
- `/var/log/httpd/ ssl_error_log` (log with errors related to the Web Client Slave Server role);
- `/var/log/messages` (lines starting with `guacd`: logs of the Guacamole server-side component);
- Enterprise Linux 8: `/var/log/tomcat9/*` (logs from the Tomcat application server, which executes some of the Guacamole server-side components).
- Enterprise Linux 9: `/var/log/tomcat/*` (logs from the Tomcat application server, which executes some of the Guacamole server-side components).

3.2.5. Gateway logs

Log locations on the Gateway server:

- `/var/log/eow/slaveserver.log` (log pertaining to the Gateway Slave Server process).

Some log entries that must be present in order to indicate that the service is functioning correctly:

```
2021-04-20 13:17:00,847 [INFO]: [907] Delaying startup for 5 seconds...
2021-04-20 13:17:06,040 [INFO]: [907] Gateway init
2021-04-20 13:17:06,043 [INFO]: [907] Gateway:: running on (0.0.0.0, 443)
2021-04-20 13:17:07,184 [INFO]: [907] SlaveServer started
2021-04-20 13:17:07,184 [INFO]: [907] Version 6.1.4
```

This entry indicates that the Gateway service is listening on port 443 (HTTPS), on every IP address, and that it initialized correctly, being able to contact the Session Manager.

3.2.6. Distributed Session Manager logs

You can also view the DSM startup and error log by using the following command:

```
journalctl -ru eow-dsm
```

3.2.7. Native Client logs

Log locations on clients running the EOW Native Client:

- Microsoft Windows:
  - `%LOCALAPPDATA%\Enterprise Open\EO.workspace Client\`
- Linux:
  - `~/.local/share/Enterprise Open/EO.workspace Client/`
- macOS:
  - `~/Library/Application Support/Enterprise Open/EO.workspace Client/`

The log file itself usually has a name corresponding to the current date, or the date when the program was executed (ex: `client-20200112.log`).

When a session is successfully established, the client should write the following line to the log file::

```
15:25:03 [INFO] session status switch from ready to logged
```

The client performs a query to the Session Manager, asking for the session status every 60 seconds. It's crucial that this request is answered correctly, or the client disconnects.

3.3. Services

For maintenance, update or reconfiguration reasons, there's occasionally the need to start, stop or restart services related to individual components of the EOW landscape. In this section we describe the recommended procedures for those tasks.

3.3.1. Session Manager (SM)

There are two services relevant to the Session Manager component:

- Apache web server (`httpd`);
- MySQL database (`mariadb`).

Those services should be configured to start automatically on operating system start-up.

In order to start all the services:

1. Start the MySQL server;
2. Start the Apache web server;

In order to stop all the services:

1. Stop the Apache web server;
2. Stop the MySQL server.

In order to restart all the services:

1. Stop all the services;
2. Start all the services.

Command examples:

- Check status on all services:
  - `systemctl status mariadb httpd`
- Start all services:
  - `systemctl start mariadb httpd`
- Stop all services:
  - `systemctl stop mariadb httpd`
- Restart all services:
  - `systemctl restart mariadb httpd`

3.3.2. Administration Console (AC)

There is only one service relevant to the Administration Console component:

- EO.workspace Administration Console (`eow-admin` service);

That service should be configured to start automatically on operating system start-up.

In order to start, stop or restart the component, simply use the appropriate start, stop or restart command for the service.

Take notice that the Administration Console component is usually installed on the same server as the Session Manager component.

Command examples:

- Check status on all services:
  - `systemctl status eow-admin`
- Start all services:
  - `systemctl start eow-admin`
- Stop all services:
  - `systemctl stop eow-admin`
- Restart all services:
  - `systemctl restart eow-admin`

3.3.3. Slave Server (SS) - Linux

On Linux, there is only one service relevant to any Slave Server component:

- EO.workspace Slave Server (`eow-slaveserver` service).

That service should be configured to start automatically on operating system start-up.

In order to start, stop or restart the component, simply use the appropriate start, stop or restart command for the service.

Each Slave Server role may have more services which support the execution of the platform.

Command examples:

- Check status on all services:
  - `systemctl status eow-slaveserver`
- Start all services:
  - `systemctl start eow-slaveserver`
- Stop all services:
  - `systemctl stop eow-slaveserver`
- Restart all services:
  - `systemctl restart eow-slaveserver`

3.3.3.1. File Server role (SS-FS)

There are two additional services relevant to the Slave Server component File Server role:

- Apache web server (`httpd`);
- Samba (`smb` service).

Those services should be configured to start automatically on operating system start-up.

In order to start, stop or restart the component, simply use the appropriate start, stop or restart command for the service.

After restarting one of the supporting services, it may be necessary to also restart the EOW Slave Server service.

Command examples:

- Check status on all services:
  - `systemctl status smb httpd eow-slaveserver`
- Start all services:
  - `systemctl start smb httpd eow-slaveserver`
- Stop all services:
  - `systemctl stop smb httpd eow-slaveserver`
- Restart all services:
  - `systemctl restart smb httpd eow-slaveserver`

3.3.3.2. Application Server role (SS-AS) - Linux

On Linux, there are two additional services relevant to the Slave Server component application server role:

- XRDP (`xrdp` service);
- CUPS (`cups` service).

Those services should be configured to start automatically on operating system start-up.

In order to start, stop or restart the component, simply use the appropriate start, stop or restart command for the service.

After restarting one of the supporting services, it may be necessary to also restart the EOW Slave Server service.

Command examples:

- Check status on all services:
  - `systemctl status cups xrdp eow-slaveserver`
- Start all services:
  - `systemctl start cups xrdp eow-slaveserver`
- Stop all services:
  - `systemctl stop cups xrdp eow-slaveserver`
- Restart all services:
  - `systemctl restart cups xrdp eow-slaveserver`

3.3.3.3. Web Client role (SS-WC)

There are three services relevant to the session manager component:

- Apache web server (`httpd`);
- Tomcat application server (`tomcat9` on Enterprise Linux 8, `tomcat` service on Enterprise Linux 9)
- Guacamole server (`guacd` service);

Those services should be configured to start automatically on operating system start-up.

In order to start, stop or restart the component, simply use the appropriate start, stop or restart command for the services, in any order.

Command examples:

- Enterprise Linux 8:
  - Check status on all services:
    - `systemctl status httpd tomcat9 guacd eow-slaveserver`
  - Start all services:
    - `systemctl start httpd tomcat9 guacd eow-slaveserver`
  - Stop all services:
    - `systemctl stop httpd tomcat9 guacd eow-slaveserver`
  - Restart all services:
    - `systemctl restart httpd tomcat9 guacd eow-slaveserver`
- Enterprise Linux 9:
  - Check status on all services:
    - `systemctl status httpd tomcat guacd eow-slaveserver`
  - Start all services:
    - `systemctl start httpd tomcat guacd eow-slaveserver`
  - Stop all services:
    - `systemctl stop httpd tomcat guacd eow-slaveserver`
  - Restart all services:
    - `systemctl restart httpd tomcat guacd eow-slaveserver`

3.3.3.4. Gateway role (SS-GW)

There are no additional services for the slave server component gateway role.

Command examples:

- Check status on all services:
  - `systemctl status eow-slaveserver`
- Start all services:
  - `systemctl start eow-slaveserver`
- Stop all services:
  - `systemctl stop eow-slaveserver`
- Restart all services:
  - `systemctl restart eow-slaveserver`

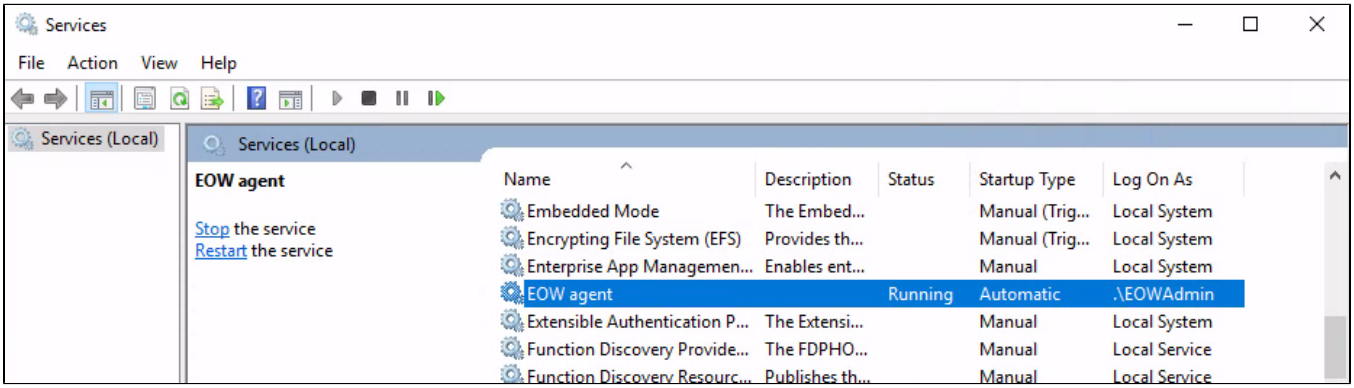
3.3.4. Slave server (SS) - Windows

On Windows, there is only one service relevant to any slave server component:

- EOW slave server (`"EOW agent"` service).

That service should be configured to start automatically on operating system start-up.

In order to start, stop or restart the component, simply use the appropriate start, stop or restart command for the service, through the "Services" MMC snap-in or through the `sc.exe` command-line tool.



Make sure the "Remote Desktop Services" windows service is running correctly.

3.3.5. Distributed Session Manager (DSM)

There is only one service relevant to the DSM component:

- EO.workspace DSM (`eow-dsm` service);

That service should be configured to start automatically on operating system start-up.

In order to start, stop or restart the component, simply use the appropriate start, stop or restart command for the service.

Command examples:

- Check status on all services:
  - `systemctl status eow-dsm`
- Start all services:
  - `systemctl start eow-dsm`
- Stop all services:
  - `systemctl stop eow-dsm`
- Restart all services:
  - `systemctl restart eow-dsm`

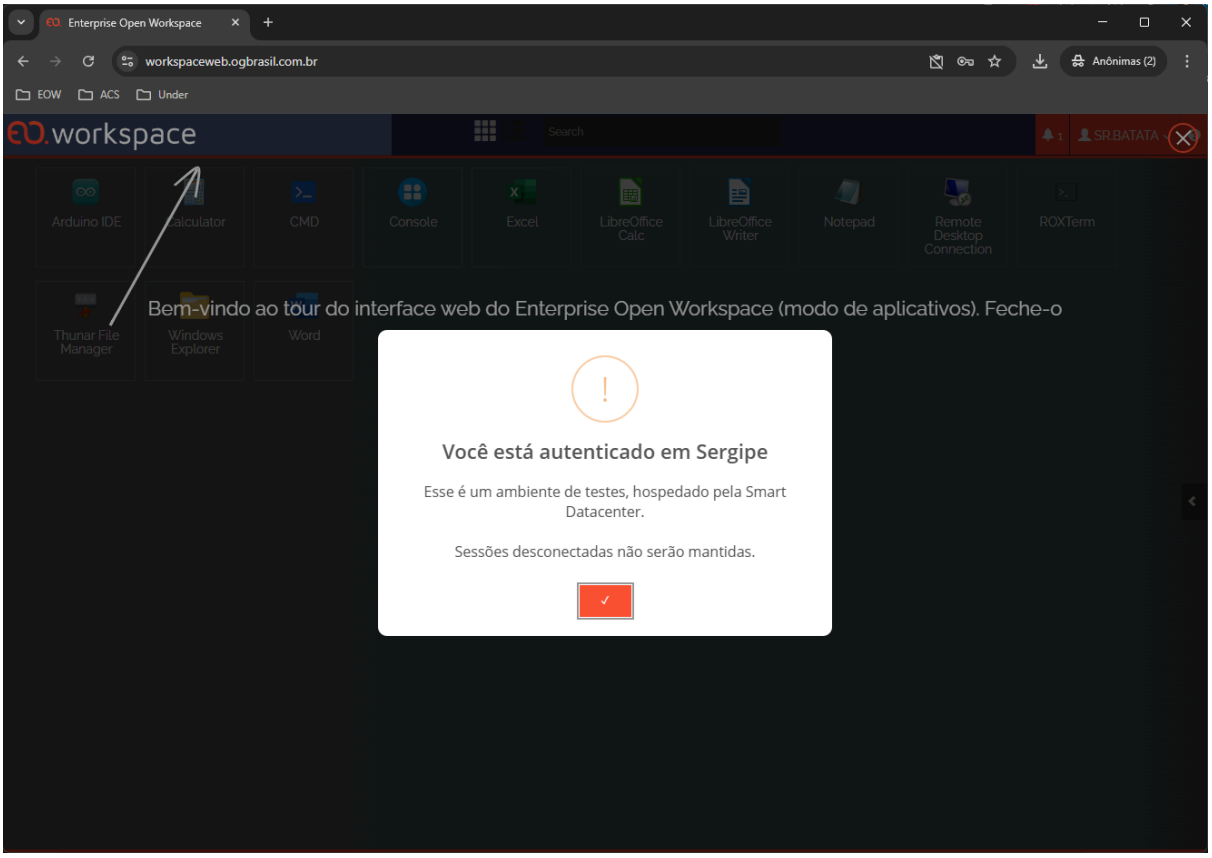
Evidências complementares

O presente documento tem como objetivo complementar as evidências de atendimento aos requisitos técnicos estabelecidos no Termo de Referência deste pregão, especificamente no que se refere às funcionalidades da solução de virtualização de desktops e aplicativos (streaming aplicacional) ofertada.

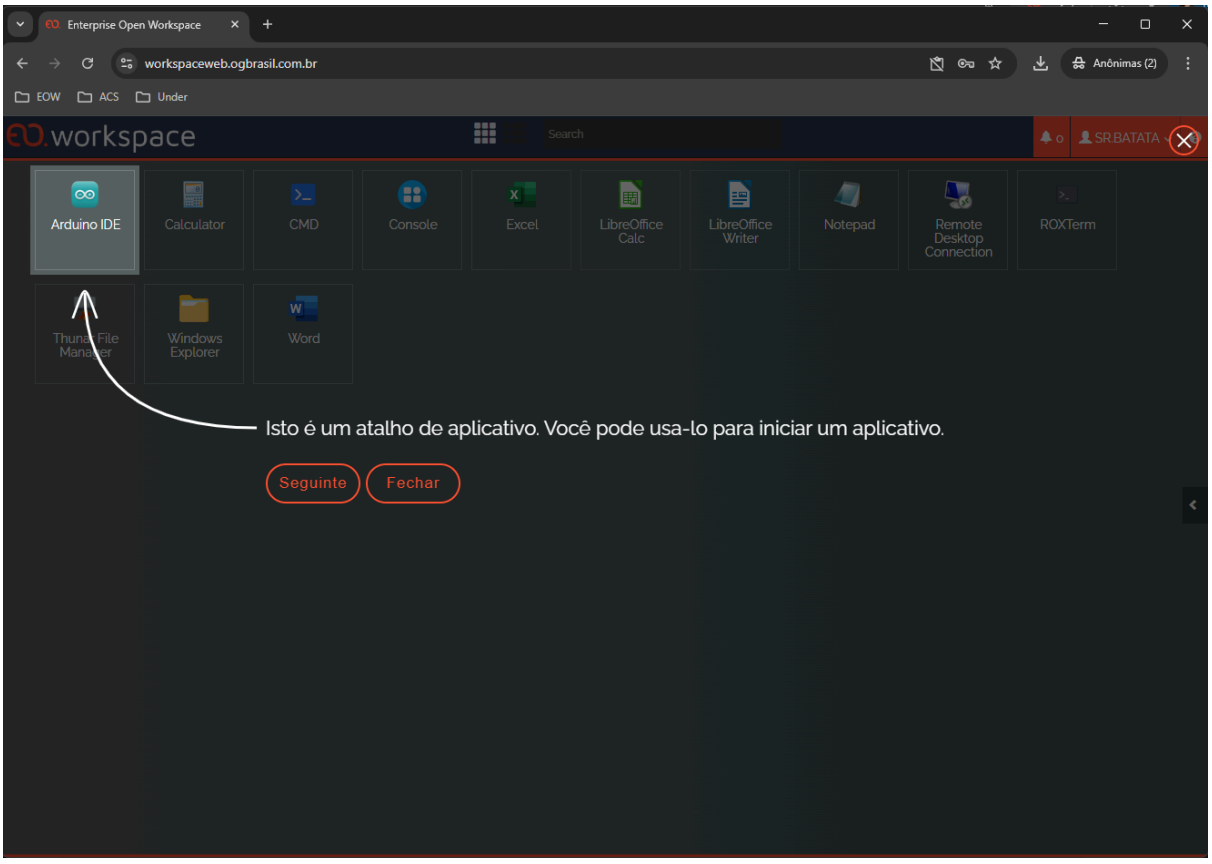
Seu propósito é demonstrar, por meio de capturas de tela (prints) e descrições contextualizadas, o efetivo funcionamento de recursos que, embora presentes e operacionais na plataforma, **não estejam explicitamente descritos ou ilustrados na documentação técnica oficial do fabricante disponível publicamente**.

As evidências aqui apresentadas foram obtidas em ambiente controlado/homologado, reproduzindo uma implementação típica da solução, e visam exclusivamente esclarecer e reforçar a conformidade com os itens do edital, sem alterar ou substituir qualquer declaração ou informação originalmente apresentada na proposta.

1. Aviso pop-up



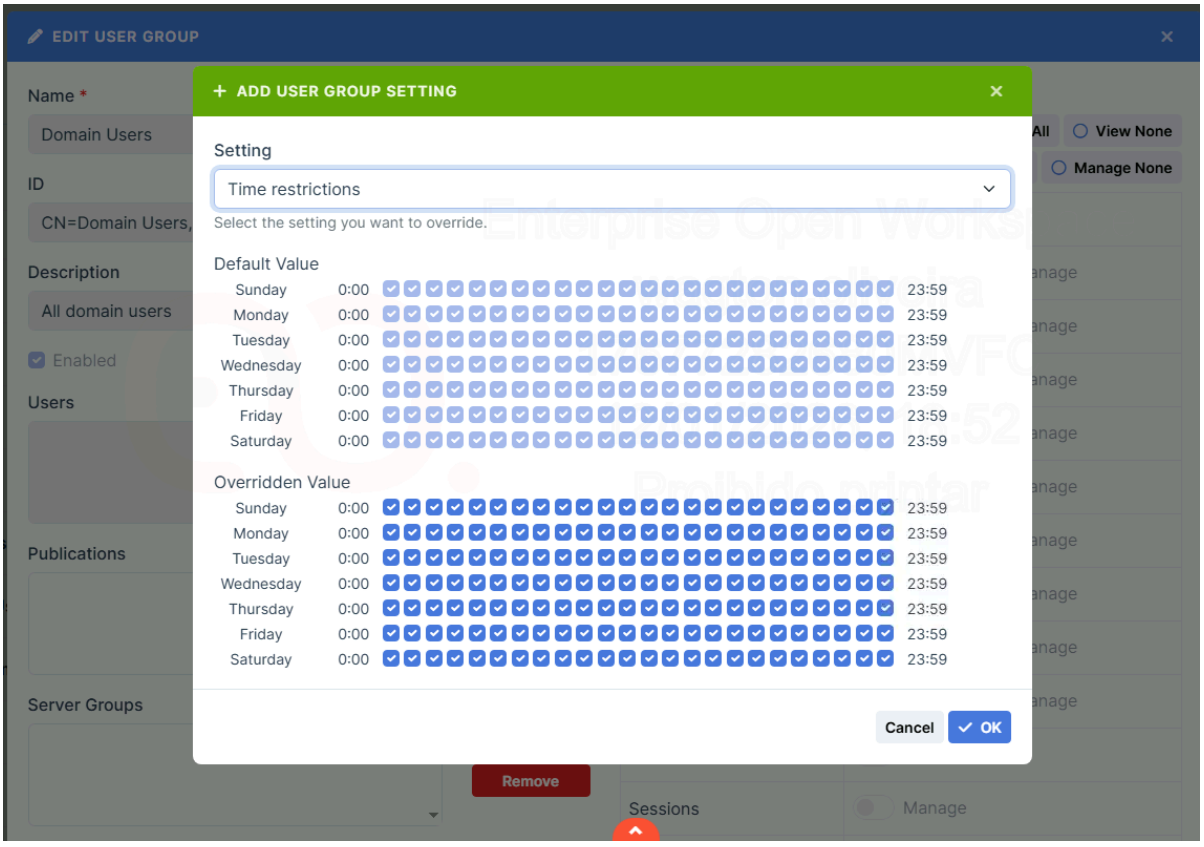
2. Tutorial interativo



3. Restrições de horário

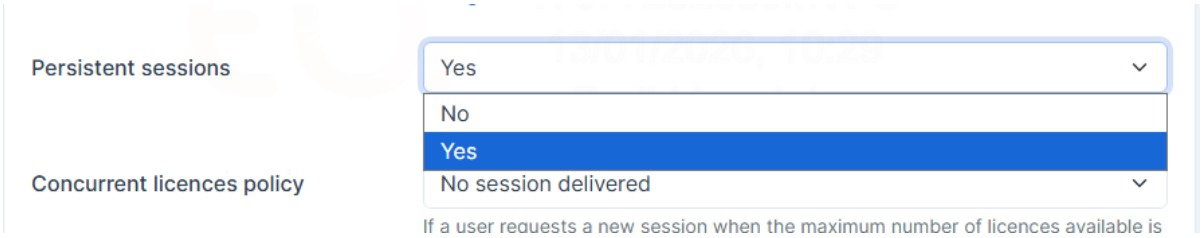
As restrições de horário podem ser aplicadas de forma global, por usuário ou grupo.

Cada caixa de seleção representa um intervalo de uma hora, iniciando à meia-noite e indo até 23:00 (11h da noite). As caixas marcadas indicam os horários em que os usuários podem realizar login. Passe o cursor sobre cada caixa para ver a descrição do intervalo de tempo.



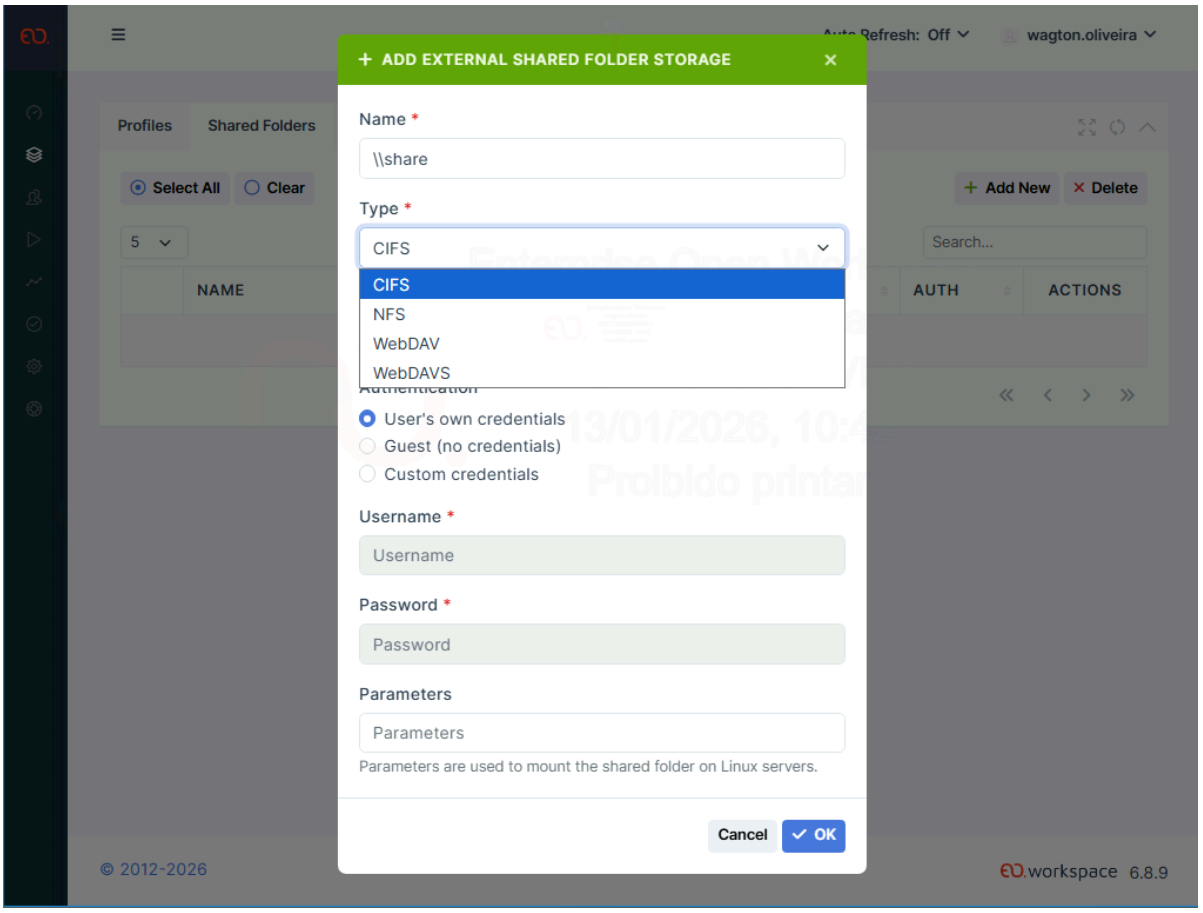
4. Persistência de sessão

Esta configuração permite que os usuários retomem uma sessão desconectada.



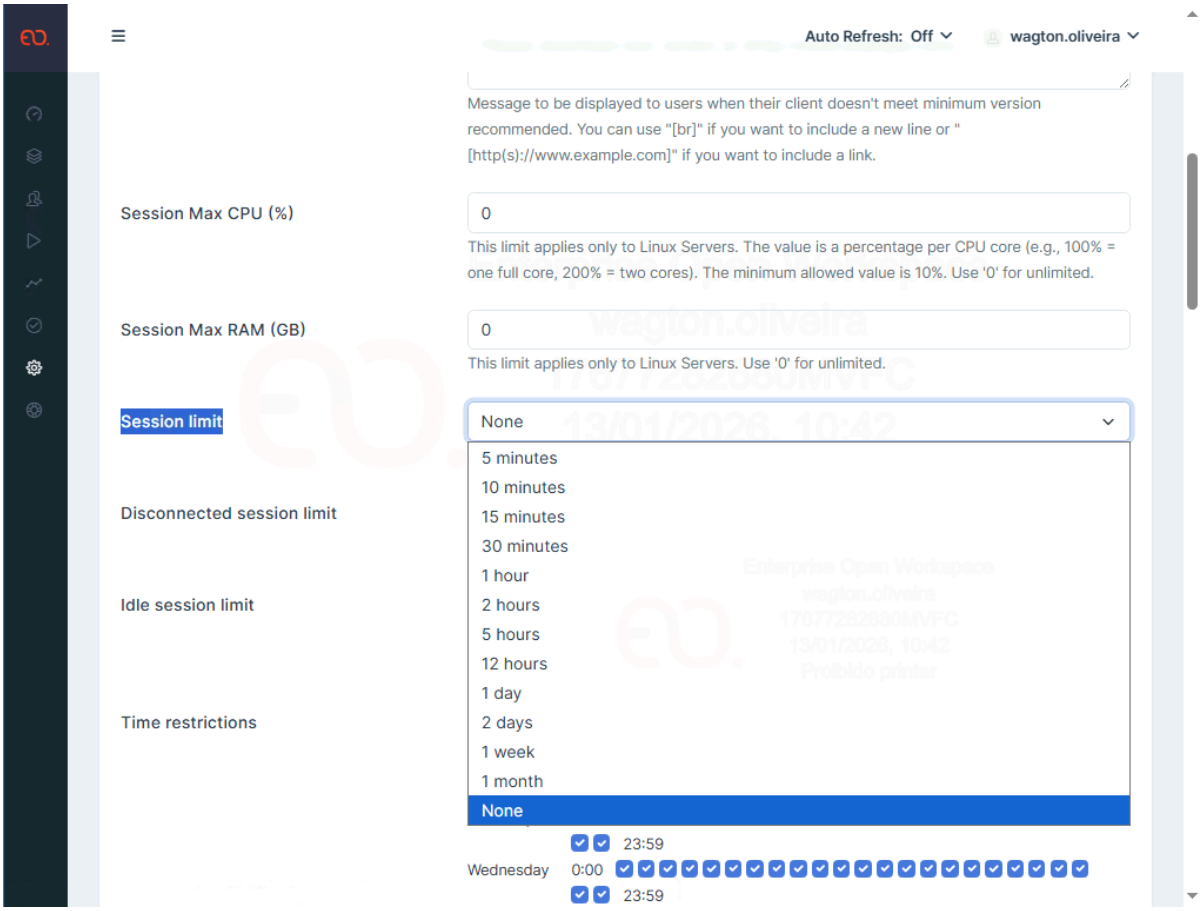
5. Compartilhamento de diretórios externos

Na seção **“Infrastructure > Storage”**, é possível configurar tudo o que está relacionado ao armazenamento, seja ele interno ou externo, relacionado a perfis de usuários ou a pastas compartilhadas.



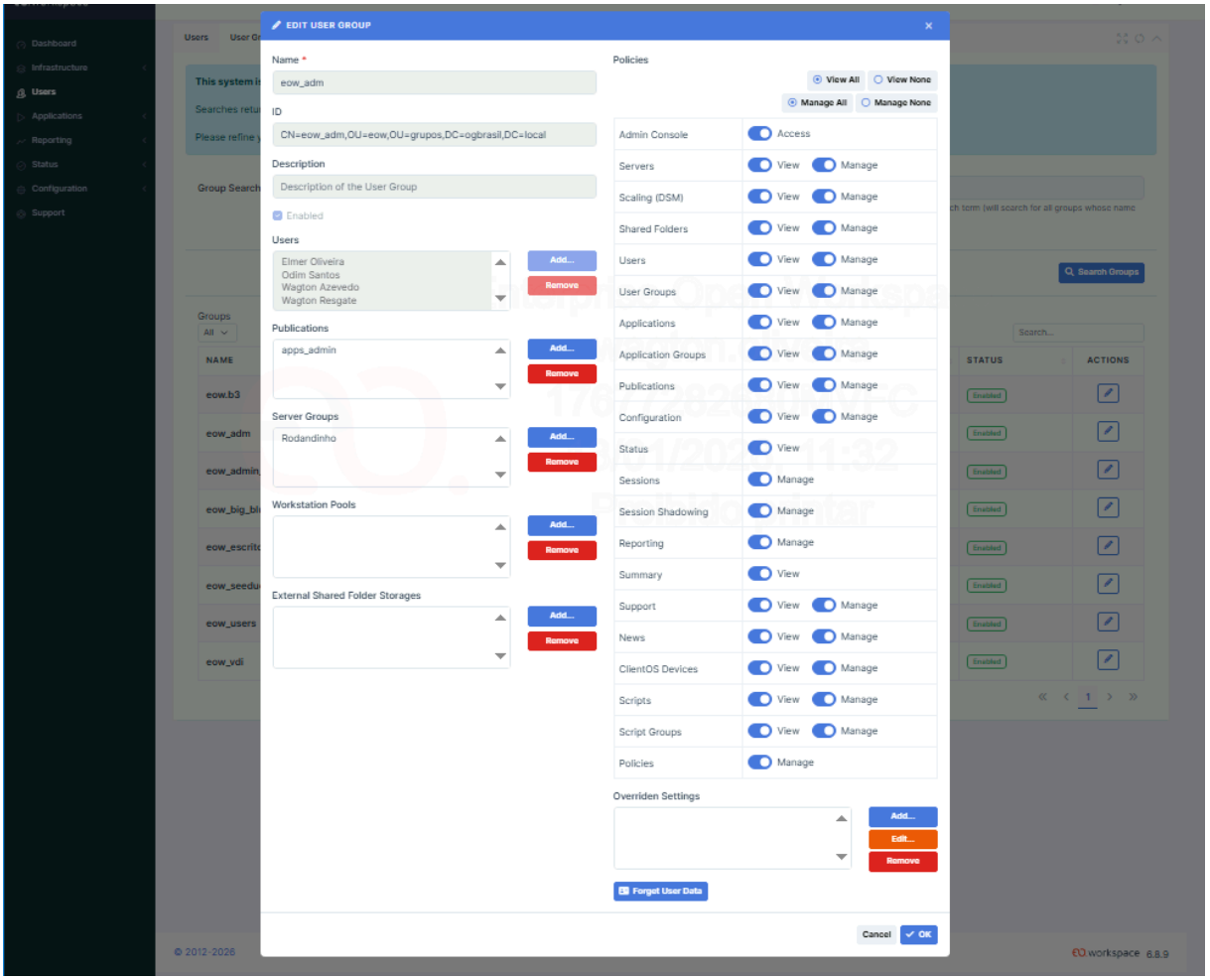
6. Tempo limite de sessão

Tempo após o qual uma sessão ativa é desconectada ou encerrada (logout).



7. Grupos do Active Directory

O grupo de usuários do AD "CN=eow_adm,OU=eow,OU=grupos,DC=ogbrasil,DC=local" está associado ao grupo de aplicações publicadas "apps_admin".



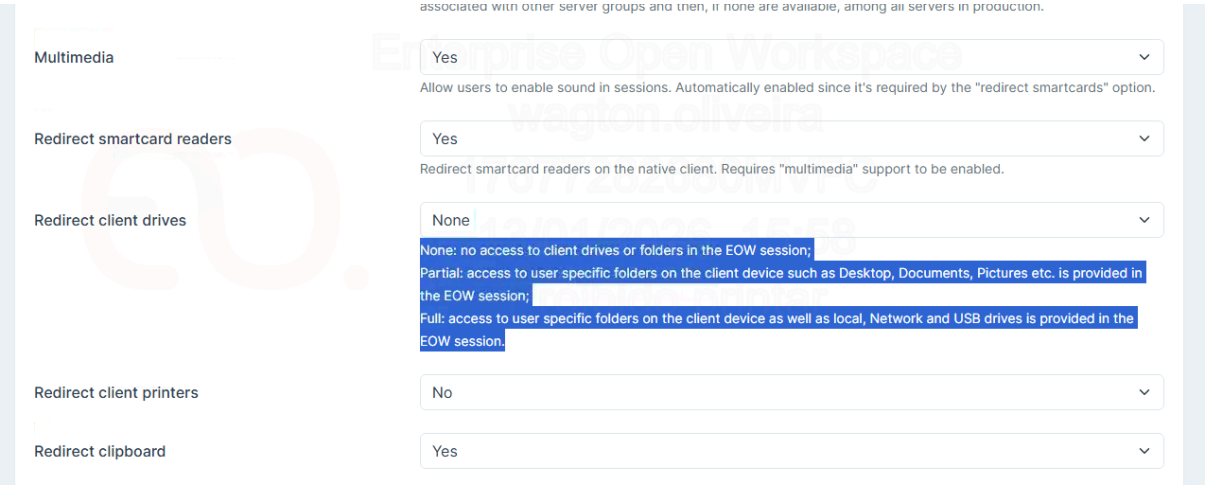
8. Balanceamento de carga

Política de balanceamento de carga entre servidores de aplicações.

- Pesos válidos para cada critério variam de 0 (ignorar) a 100 (importância máxima).
- "Random” adiciona um certo grau de aleatoriedade à escolha do servidor.

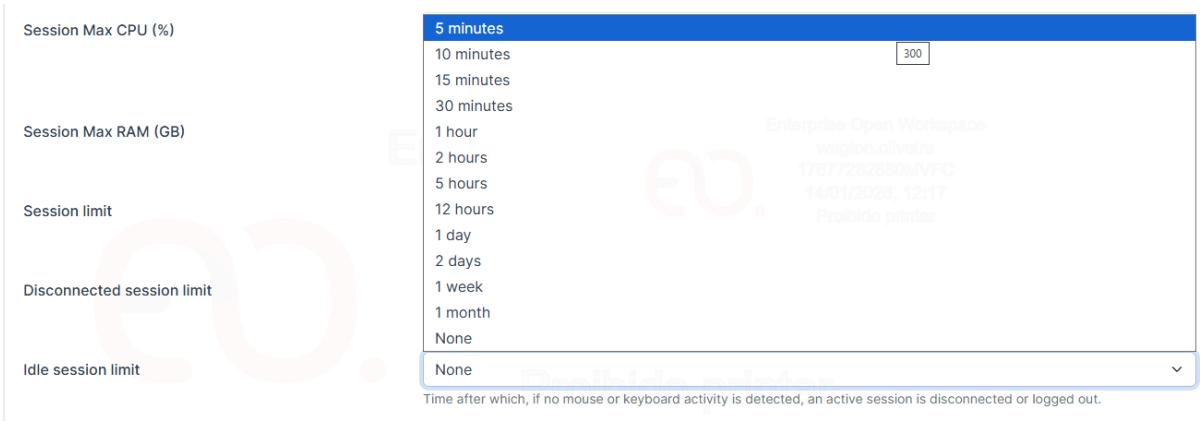
9. Redirecionamento de drives, diretórios e multimídia

None: nenhum acesso a unidades ou pastas do cliente na sessão EOW;
Partial: acesso a pastas específicas do usuário no dispositivo cliente, como Área de Trabalho, Documentos, Imagens etc., é disponibilizado na sessão EOW;
Full: acesso às pastas específicas do usuário no dispositivo cliente, bem como a unidades locais, de rede e USB, é disponibilizado na sessão EOW.



10. Desconexão por inatividade

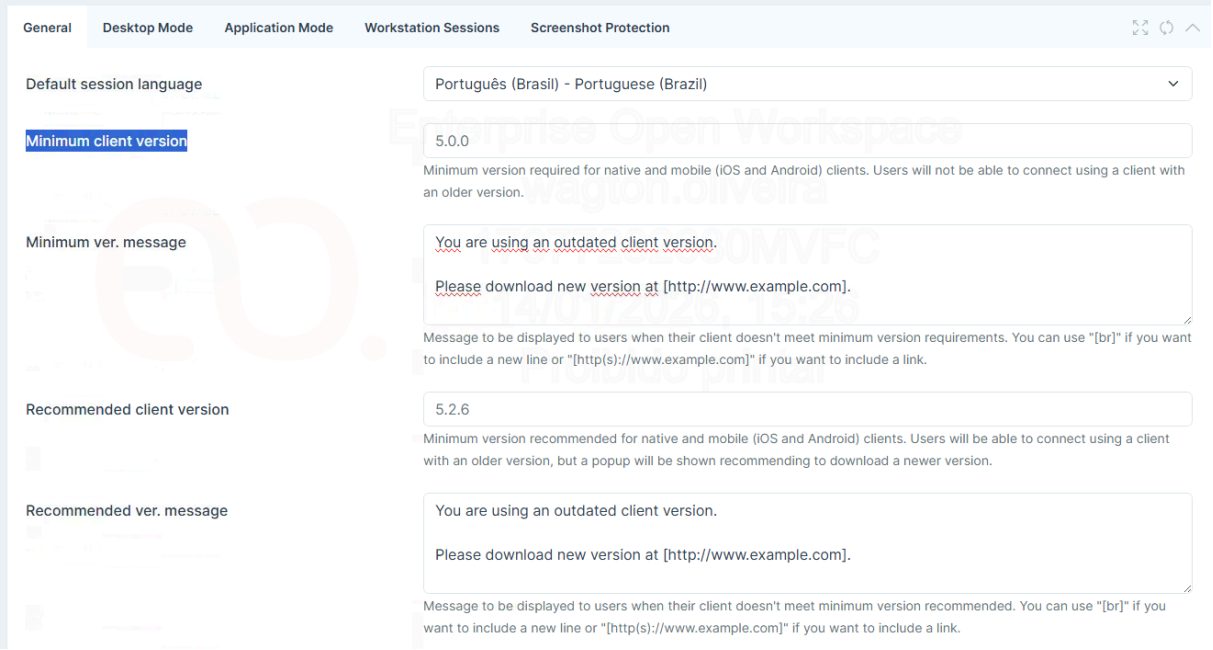
Tempo após o qual, caso nenhuma atividade de mouse ou teclado seja detectada, uma sessão ativa é desconectada ou encerrada (logout).



11. Controle de versão

Versão mínima exigida para clientes nativos e móveis (iOS e Android). Usuários não poderão se conectar utilizando um cliente com versão anterior.

Uma mensagem é exibida aos usuários quando o cliente não atender aos requisitos de versão mínima.



EO.workspace - Native Client Command-Line Interface (CLI) Options

1. Introduction

The following instructions show how to control the Native Client by using its Command Line Interface (CLI) options.

Some options are only available from a specific EOW Native Client version. When this is the case, it should be noted on the specific option documentation.

The following command line options are usable, unless specifically specified, on all available target platforms (Windows, Linux and macOS).

> ⚠ The SAML-related command line options described in the next session are only available on **EOW version 6.0.12 or later**.

2. Command-Line Options

The command line usage for the Native Client is:

```
eowclient [options]
```

The following command line options are available (in short, single letter or keyword format):

- `-?, -h, --help`
  - Displays a help message with a list of these options.
- `-v, --version`
  - Displays version information.
- `-c, --config <file>`
  - Load configuration options from '<file>'.
- `-s, --server <server[:port]>`
  - The Session Manager or Gateway server address (and optional port).
- `-u, --username <username>`
  - The username.
- `-p, --password <password>`
  - The password.
- `-m, --mode <D|A>`
  - The session mode (D> Desktop or A> Applications).
- `-g, --geometry <WxH>`
  - In desktop mode, the window dimensions.
- `-f, --full-screen`
  - In desktop mode, enable full-screen mode.
- `-l, --language <xx_YY>`
  - The language for the user interface (format includes language and country (eg. en_US, en_GB, pt_PT).
- `-r, --reset-existing`
  - Reset any established (disconnected) session.
- `-t, --use-all-monitors`
  - Use all available monitors (for full screen desktop or applications mode).
- `-o, --enable-sound`
  - Enable sound for this session.
- `-x, --shortcuts`
  - Publish shortcuts to the applications on the host OS.
- `-a, --auto-login`
  - Auto-login, using the (required) username, password and server.
- `-b, --saml-auto-login`
  - Auto-login, using SAML/Organization login.
- `-q, --auto-quit`
  - When using auto-login, exit when the session is logged out or disconnected.
- `-z, --simple-mode`
  - Enable simple mode, where certain fields (such as settings, session mode and server name) and the applications window is hidden in applications mode.
- `-n, --no-save`
  - Don't remember values for credential fields (username and password) between connections.
- `-e, --eac <token>`
  - Enable External Apps Client (EAC) mode, using the specified token to authenticate. Assumes enabling applications mode, shortcut publishing, auto-login, auto-quit and simple mode.

- `-i, --profile <low|medium|high>`
  - Image quality. High profile may impact performance, depending on available bandwidth.
- `--usb <usb_config>`
  - Enable USB device redirection, when supported. Accepts a mandatory USB configuration string.
- `-d, --disable-crash-reports`
  - Disable automated sending of anonymous crash reports.

The configuration file specified in the "`-c, --config`" option is a simple text file, which can contain any of the long command line options, followed by an '=' sign and the intended value. If the option doesn't have a value (ie. it's on/off), you must specify 'true' or 'false'.

See the next section for some configuration file examples.

3. Examples

Here are some examples of command line options usage.

To auto-fill a certain server name on the server field:

```
eowclient -s eow.example.com
```

To auto-fill the server and username fields, and preselect the Applications mode:

```
eowclient -s eow.example.com -u johndoe -m A
```

The command line can also typically take advantage of command line variables. For instance, in Windows operating systems, if you want to reuse the current OS username for EOW, auto-fill the server name and select Applications mode:

```
eowclient -s eow.example.com -u %USERNAME% -m A
```

The same in Linux (Bash) based operating systems:

```
eowclient -s eow.example.com -u $USER -m A
```

For a more complicated command line usage, here's an example providing server name, username, password, selecting the Desktop mode, logging in automatically, using the full screen, and quitting when the session ends (quite common in Kiosk mode):

```
eowclient -s eow.example.com -u kioskuser -p kioskpassword54364 -m D -a -f -q
```

Using the last command line example, but specifying a configuration file instead:

```
eowclient -c kiosk.cfg
```

The configuration file would have the following contents:

```
[configuration]
server=eow.example.com
username=kioskuser
password=kioskpassword54364
mode=D
auto-login=true
full-screen=true
auto-quit=true
```

Another configuration file example, the same as above, but this time performing auto-login using SAML, and not quitting at the end of the session:

```
[configuration]
server=eow.example.com
mode=D
saml-auto-login=true
full-screen=true
```

EO.workspace - Installation and Configuration (Enterprise Linux 8)

1. Introduction

This guide describes how to install and configure an EO.workspace landscape. Before continuing, make sure you are familiar with the components and architecture of EO.workspace by consulting the Introduction and Architecture Guide.

These installation instructions apply and should be used only for EOW version 6.1.3 or later.

2. Prerequisites

2.1. Supported Linux Distributions

Warning!

CentOS Linux 8 has reached End-Of-Life on December 31st, 2021.

It no longer receives any updates (security or otherwise) and the software repositories have been archived.

This makes it impossible to either install new CentOS 8 systems or install any package from the official repositories in existing systems.

We highly recommend that you migrate as soon as possible to a supported Linux Distribution, as listed below.

If you are looking for a free, open-source Linux Distribution, comparable to CentOS 8, we recommend Rocky Linux 8. There's a simple migration process, which should cover most use cases and environments, described here:

- https://docs.rockylinux.org/guides/migrate2rocky/

This documentation describes the installation of Enterprise Open Workspace server components on any Enterprise Linux 8 or binary-compatible Linux Distribution.

Currently supported distributions are:

- Red Hat Enterprise Linux 8

- Oracle Linux 8
- Rocky Linux 8

If installing EO.workspace on an Enterprise Linux 7 or binary-compatible Linux Distribution, please refer to this document:

- EO.workspace - Installation and Configuration (Enterprise Linux 7)

2.2. Linux Installation

When installing the Linux systems for EO.workspace components, always choose the available Server minimal software install option, and not the Desktop version.

Desktop-related packages installed by the "Gnome", "KDE" or other desktop environments are incompatible with certain EO.workspace components.

Also note that EO.workspace does not support SELinux natively. You have two options when using Enterprise Linux:

1. Disable SELinux on the solution machines, by editing the `/etc/selinux/config` file and rebooting;
2. Configure SELinux appropriately.

2.3. Firewall

If using a firewall, rules must be created to open certain ports for incoming and outgoing traffic, in order for EO.workspace components to be able to communicate with each other, as described in the "Component interactions" section of the Introduction and Architecture Guide.

The following communications should be allowed, and any necessary firewall rules or routing ACL should be properly configured.

Communications between the solution servers:

Source(s)	Destination(s)	Port(s)	Description
Session Manager	Gateway	1112 (TCP)	Session Manager communications to Slave Servers
	Web Access		
	Application Server		
Session Manager	Distributed Session Manager	443 (TCP)	Availability heartbeat from Session Manager to DSM
Session Manager	*All Servers*	10050	Server and service monitoring
All Servers	Session Manager	10051	
Web Access	Session Manager	80 (TCP) 443 (TCP) 1111 (TCP)	Slave Servers communications to Session Manager
Application Server			
Gateway			
Application Server	Application Server	3389 (TCP)	Application Servers RDP connection to other Application Servers
Gateway	Application Server	3389 (TCP)	Gateway RDP connection to Application Servers
Gateway	Web Access Load Balancer	443 (TCP)	Gateway HTTPS connection to Web Load Balancer
Web Access	Application Server	3389 (TCP)	Web Client RDP connection to Application Servers
Web Access Load Balancer	Web Access	443 (TCP)	Web Load Balancer communications to Web Client servers

Communications between the solution servers and external resources:

Source(s)	Destination(s)	Port(s)	Description
Session Manager	Domain Controllers/LDAP Servers (LDAP or LDAPS)	389 (TCP) or 636 (TCP)	Directory user/group listing and user authentication
Application Server			
Application Server	*Any networks, servers and ports required by the installed applications.* *This can include resources on the organization's internal networks or on external networks (Internet).*		
All Servers	Organization DNS Server(s)	53 (TCP+UDP)	DNS resolution
	Organization NTP Server(s)	123 (UDP)	Time and date synchronization
	Unrestricted internet access for operating system updates (Enterprise Linux and Windows), as well as necessary package downloads for the solution implementation.		

Additionally, the following accesses to the servers must be allowed:

Source	Destination	Port(s)	Description
Administrator Users	*All Servers*	ICMP	Server availability checks
	All Linux Servers	22 (TCP)	Administrative access via SSH
	All Windows Servers	3389 (TCP)	Administrative access via RDP
	Session Manager	443 (TCP) 8443 (TCP)	Access to monitoring and administration consoles
Users on external networks *(Internet)*	Web Load Balancer	443 (TCP)	Solution access (using the web client)
	Gateway	443 (TCP)	Solution access (using the native clients)
	Distributed Session Manager	443 (TCP)	Solution access (all clients)
Users on internal networks *(Intranet)*	Web Load Balancer	443 (TCP)	Solution access (using the web client)
	Session Manager	80 (TCP) 443 (TCP)	Solution access (using the native clients)
	Application Servers (Linux/Windows)	3389 (TCP)	Solution access (using the native clients)
	Distributed Session Manager	443 (TCP)	Solution access (all clients)

3. Pre-installation checklist

Not following the pre-installation checklist may result in errors during or after EOW installation that may be hard to diagnose.

Before contacting Enterprise Open Support for any issue relating to an EOW landscape, please ensure every item in the pre-installation checklist is done.

Before starting installation, copy the table below and check that all the items have been done:

Item	Done	Not Done
All machines have the latest OS updates		
All machines have access to their software repositories		
Reverse and forward DNS is configured so that all machines are reachable		
Firewall rules described in the Prerequisites section are implemented		
Linux servers have SELinux disabled or configured as described in the Prerequisites section		
Windows servers do not have any installed role or other configuration that may restrict remote access to the machine		

4. Installation

4.1. Session Manager

4.1.1. Minimum System Requirements

- CPU: 4 Cores
- Memory: 4 GiB
- Storage: 50 GiB
- Network: 1 Gbps NIC (2 for failover)
- OS: Enterprise Linux 8 (RedHat, Oracle, Rocky, Alma)

4.1.2. Instructions

In order to install the Session Manager component (and the Administration Console, which will be deployed on the same server), one should execute the following tasks.

First, we need to configure the Apache/PHP environment on the server, so that PHP 7.4 is used:

```
# dnf -y module reset php
# dnf -y module enable php:7.4
```

We need to install the EPEL repository for dependencies:

```
# dnf -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

On **Red Hat Enterprise Linux**, some additional repositories must be enabled, because the installation of some packages (from EPEL or EOW) depend on them:

```
# subscription-manager repos --enable "codeready-builder-for-rhel-8-$(arch)-rpms"
```

On **Rocky Linux** and **AlmaLinux**, we need to enable the "powertools" repository, since some packages (from EPEL or EOW) depend on it:

```
# dnf config-manager --set-enabled powertools
```

On **Oracle Linux**, some additional repositories must be enabled, because the installation of some packages (from EPEL or EOW) depend on them:

```
# dnf config-manager --set-enabled ol8_codeready_builder
```

Next, install the MariaDB database server (a drop-in replacement for the MySQL database). Also enable it to start on boot and start it:

```
# dnf -y install mariadb-server
# systemctl enable --now mariadb
```

Next, the `mysql_secure_installation` command should be run, in order to secure the MariaDB installation (eg. define the 'root' user password, remove test databases and users, etc.):

```
# mysql_secure_installation
```

Following the MySQL/MariaDB optimization instructions, although optional, is recommended. They are available here:

- EO.workspace - MySQL/MariaDB optimization

Finally, we need to create the database for EOW, and create a user which will have full access to this database:

```
# mysql -u root -p
...
MariaDB[(none)]> CREATE DATABASE eow;
MariaDB[(none)]> CREATE USER 'eow'@'localhost' IDENTIFIED BY '<password>';
MariaDB[(none)]> GRANT ALL PRIVILEGES ON eow.* TO 'eow'@'localhost';
MariaDB[(none)]> FLUSH PRIVILEGES;
MariaDB[(none)]> quit
```

We now install the EO.workspace Session Manager and Administration Console packages, which should have been previously downloaded to the server:

```
# dnf -y install \
eow-session-manager-*.rpm \
eow-admin-*.rpm \
php-libchart-*.rpm \
php-pecl-imagick-*.rpm \
php-pecl-mcrypt-*.rpm
```

On **Oracle Linux**, we need to install some additional PHP-related packages, which are not installed automatically, as in other distributions:

```
# dnf -y install php-fpm php-json php-opcache
```

Next, we need to configure the EO.workspace Session Manager. On the Session Manager configuration, we need to define the super-administrator username and password:

```
# eow-session-manager-config
```

We then need to edit the PHP configuration file (`/etc/php.ini`) and configure the appropriate time zone, by changing the following line:

```
date.timezone = ...
```

One can either use "UTC" for the time zone or, if preferred, use one of the time zones described in the PHP documentation (eg. "Europe/Lisbon"):

- https://secure.php.net/manual/en/timezones.php

Finally, we need to enable and start the web server (and PHP-FPM) services:

```
# systemctl enable --now httpd
```

On the Administration Console configuration, we need to define the Session Manager address (which, in this specific case will be 'localhost' or the FQDN of the server) and generate temporary self-signed TLS certificates:

```
# eow-admin-config
...
# eow-admin-gen-tls --host $(hostname -f)
```

These temporary certificates should be replaced by proper ones as soon as possible.

Finally, we need to enable and start the admin console daemon:

```
# systemctl enable --now eow-admin
```

You can now bootstrap the Session Manager, by accessing the Administration console on the server, via HTTPS on TCP port 8443.

4.2. File Server

4.2.1. Minimum System Requirements

- CPU: 4 cores
- Memory: 4 GiB
- Storage: 50+ GiB (depending on number of user profiles/shared folders)
- Network: 1 Gbps NIC
- OS: Enterprise Linux 8 (RedHat, Oracle, Rocky, Alma)

4.2.2. Instructions

In order to install the File Server component, one should execute the following tasks.

We now install the EO.workspace File Server packages, which should have been previously downloaded to the server:

```
# dnf -y install \
eow-slaveserver-[0-9]*.rpm \
eow-slaveserver-role-fs-*.rpm \
eow-regular-union-fs-*.rpm
```

We now need to configure the EO.workspace Slave Server. To do this, we need to define the Session Manager address:

```
# eow-slaveserver-config
```

Important

If you need to accept connections from old versions of Windows (pre-Windows NT 4.0 SP4) or Linux, or if your Windows Application Servers are configured to use NTLMv1 (eg. via domain policies, for some reason), you must enable NTLMv1 support on the Samba configuration file `/etc/samba/smb.conf`, by adding the following line:

```
ntlm auth = yes
```

And restarting Samba (which is done in the following step).

Note that this is an insecure setting, and NTLMv1 is an insecure and vulnerable protocol. You should really change your environment in order not to use NTLMv1.

Then restart the Samba CIFS server, the web server, and the EO.workspace Slave Server service, and configure them to start on boot:

```
# systemctl restart smb httpd eow-slaveserver
# systemctl enable smb httpd eow-slaveserver
```

The File Servers should now appear on the administration console, in the "Unregistered Servers" tab of the servers list on the "Infrastructure > Servers" section.

In order to enable them on the platform, the following steps should be executed:

- In the "Unregistered Servers" table, select the "+" button for each server; or select all the servers you want to add and use the "+ Register" button;
- In the "Servers" tab, check that all the servers were added correctly;
- If the server name doesn't correspond to its fully qualified domain name (FQDN), edit the server configuration, fill the "Internal name" input box with the correct FQDN;
- Click the "Switch to production" button in the server edit dialog, in order to activate them; or select all the servers you want to switch to production and use the "Switch to production" button on the servers table.

After this procedure, the File Servers are ready to be used.

4.3. Application Server (Linux)

4.3.1. Minimum System Requirements

- CPU: 4 cores
- Memory: 8 GiB
- Storage: 50+ GiB. High speed disks with RAID-1 (15krpm, SSDs or SAN disks).
- Network: 1 Gbps NIC
- OS: Enterprise Linux 8 (RedHat, Oracle, Rocky, Alma)

4.3.2. Instructions

In order to install the Linux Application Server component, one should execute the following tasks.

We need to install the EPEL repository for dependencies:

```
# dnf -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

We now install the EO.workspace packages, which should have been previously downloaded to the server:

```
# dnf -y install \
fdk-aac-*.rpm \
eow-slaveserver-[0-9]*.rpm \
eow-slaveserver-role-aps-*.rpm \
eow-desktop-*.rpm \
eow-xrdp-*.rpm \
eow-xrdp-printer-*.rpm \
eow-xrdp-seamrdp-*.rpm \
eow-xrdp-python-*.rpm \
eow-shells-*.rpm \
eow-regular-union-fs-*.rpm \
eow-logout-dialog-*.rpm \
eow-desktop-gtk-theme-*.rpm \
eow-externalapps-client-*.rpm \
eow-xfce4-whiskermenu-plugin-*.rpm \
ghostscript-*.rpm
```

We now need to configure the EO.workspace Slave Server. To do this, we need to define the Session Manager address:

```
# eow-slaveserver-config
```

Finally, we need to restart the CUPS printing server, the XRDP daemon and the EO.workspace Slave Server and configure the CUPS server and the EO.workspace Slave Server to start automatically on boot:

```
# systemctl restart cups xrdp eow-slaveserver
# systemctl enable cups xrdp eow-slaveserver
```

The application servers should now appear on the administration console, in the "Unregistered Servers" tab of the servers list on the "Infrastructure > Servers" section.

In order to enable them on the platform, the following steps should be executed:

- In the "Unregistered Servers" table, select the "+" button for each server; or select all the servers you want to add and use the "+ Register" button;
- In the "Servers" tab, check that all the servers were added correctly;
- If the server name doesn't correspond to its fully qualified domain name (FQDN), edit the server configuration, fill the "Internal name" input box with the correct FQDN;
- Click the "Switch to production" button in the server edit dialog, in order to activate them; or select all the servers you want to switch to production and use the "Switch to production" button on the servers table.

After this procedure, the application servers are ready to be used.

4.4. Application Server (Windows)

4.4.1. Minimum System Requirements

- CPU: 4 cores
- Memory: 8 GiB
- Storage: 50+ GiB. High speed disks with RAID-1 (15krpm, SSDs or SAN disks).
- Network: 1 Gbps NIC
- OS: Windows Server 2012 R2 / 2016 / 2019 / 2022

4.4.2. Instructions

In order to install the Windows Application Server component, one should execute the following tasks.

Before installing the EO.workspace software, the "Remote Desktop Services" Windows Role should be added to the servers, by using "Server Manager - Roles - Add Roles".

During the setup of the Remote Desktop Services role, the following considerations should be taken into account:

- Only the "Remote Desktop Session Host" role service is required;
- **The "Do not require Network Level Authentication" option must be selected;**
- The "Audio and video playback" and "Audio recording redirection" options should be enabled;
- The "Desktop composition" option should be disabled.

Important

If you want to use the **Session Shadowing** feature, you must install the "Remote assistance" feature through Server Manager (*Add roles and features* > *Features* > *Remote Assistance*).

If you want to **support audio** on your Windows applications, you should **start and enable the "Windows Audio" service** on Windows Server.

When using **Windows Server 2016 or later**, support for the AVC444 codec on remote desktop session should be activated, in order to improve session performance and reduce bandwidth usage. To do this, we should edit the Local Group Policy (using the `gpedit.msc` command), and define the following policies:

- *Computer Configuration* > *Administrative Templates* > *Windows Components* > *Remote Desktop Services* > *Remote Desktop Session Host* > *Remote Session Environment:*
  - Prioritize H.264/AVC 444 Graphics mode for Remote Desktop connections – Enabled;
  - Configure H.264/AVC hardware encoding for Remote Desktop connections – Enabled.

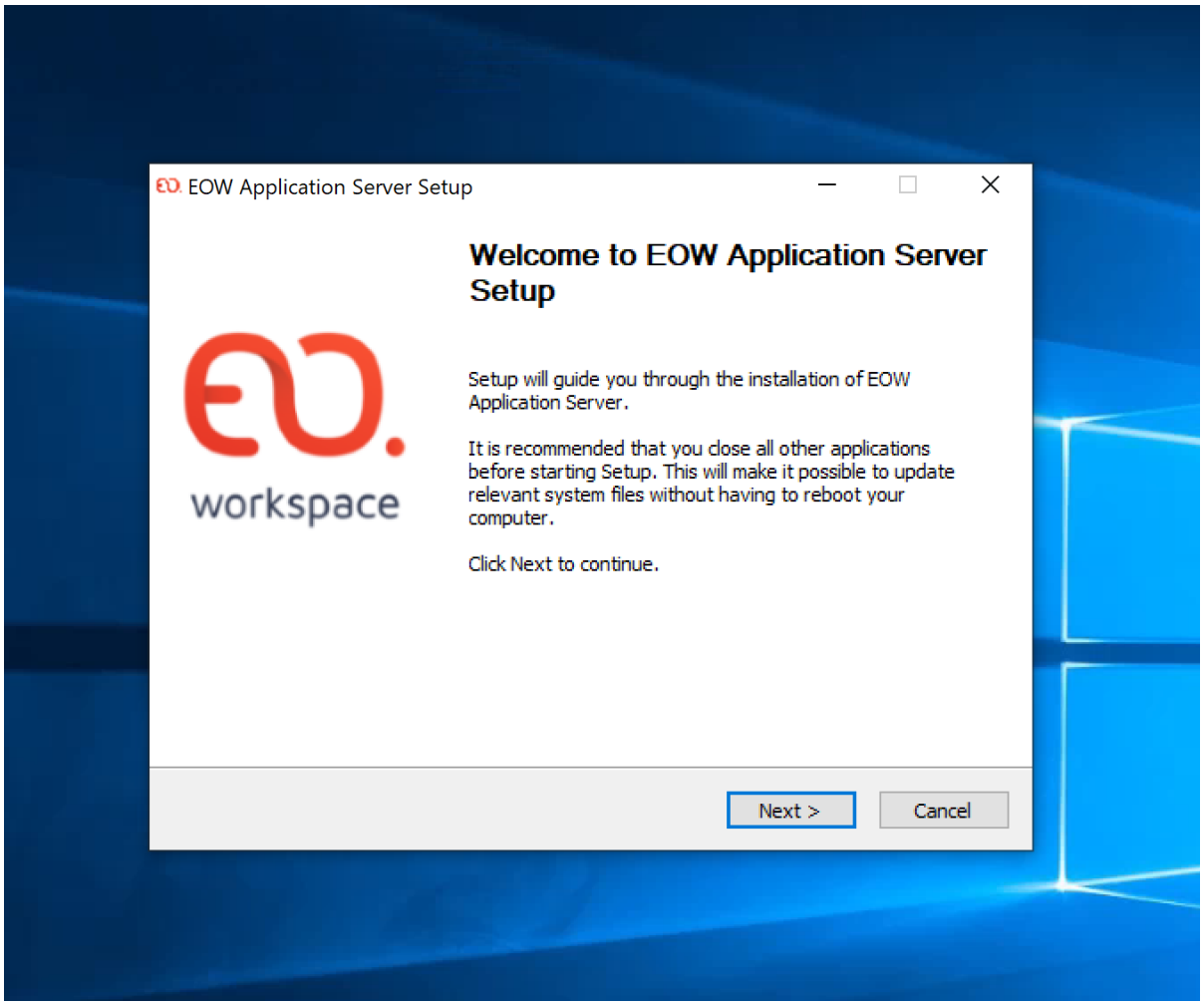
Also, on **any Windows Server version**, in order to make sure that regular users don't see update notifications or start menu options, activate the following policies:

- *Computer Configuration* > *Administrative Templates* > *Windows Components* > *Windows Update:*
  - Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box – Enabled;
  - Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box – Enabled;
  - Allow non-administrators to receive update notifications – Disabled;
- *User Configuration* > *Administrative Templates* > *Windows Components* > *Windows Update:*
  - Remove access to use all Windows Update features – Enabled (0: Do not show any notifications).

Finally, take notice that after the Remote Desktop Services role is installed, it will have a 120 days grace period before a proper license is required. Make sure you **license your Remote Desktop Services installation properly, or it will stop working after the grace period**. Refer to Microsoft's documentation for more information:

- License your RDS deployment with client access licenses (CALs)

After installing the role, the system should reboot. We can now install the EO.workspace Windows Application Server software from the installation executable:



In the installation wizard, you should specify the Session Manager server address. After completing the installation, the system will reboot.

The application servers should now appear on the administration console, in the "Unregistered Servers" tab of the servers list on the "Infrastructure > Servers" section.

In order to enable them on the platform, the following steps should be executed:

- In the "Unregistered Servers" table, select the "+" button for each server; or select all the servers you want to add and use the "+ Register" button;
- In the "Servers" tab, check that all the servers were added correctly;
- If the server name doesn't correspond to its fully qualified domain name (FQDN), edit the server configuration, fill the "Internal name" input box with the correct FQDN;
- Click the "Switch to production" button in the server edit dialog, in order to activate them; or select all the servers you want to switch to production and use the "Switch to production" button on the servers table.

After this procedure, the application servers are ready to be used.

4.5. Web Client

4.5.1. Minimum System Requirements

- CPU: 4 cores recommended as a minimum
- Memory: 4 GiB recommended as a minimum
- Storage: 50 GiB
- Network: 1 Gbps NIC (2 for failover)
- OS: Enterprise Linux 8 (RedHat, Oracle, Rocky, Alma)

4.5.2. Instructions

In order to install the Web Client component, one should execute the following tasks.

First, we need to configure the Apache/PHP environment on the server, so that PHP 7.4 is used:

```
# dnf -y module reset php
# dnf -y module enable php:7.4
```

We need to install the EPEL repository for dependencies:

```
# dnf -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

On **Red Hat Enterprise Linux**, some additional repositories must be enabled, because the installation of some packages (from EPEL or EOW) depend on them:

```
# subscription-manager repos --enable "codeready-builder-for-rhel-8-$(arch)-rpms"
```

On **Rocky Linux** and **AlmaLinux**, we need to enable the "powertools" repository, since some packages (from EPEL or EOW) depend on it:

```
# dnf config-manager --set-enabled powertools
```

On **Oracle Linux**, some additional repositories must be enabled, because the installation of some packages (from EPEL or EOW) depend on them:

```
# dnf config-manager --set-enabled ol8_codeready_builder
```

We also need to install Tomcat, which is not provided natively by Enterprise Linux 8, and it will be done through the "harbottle-main" repository (as described here):

```
# dnf -y install https://harbottle.gitlab.io/harbottle-main/8/x86_64/harbottle-main-release.rpm
# dnf -y install tomcat9 tomcat9-native
# sed -i 's#JAVA_HOME=/usr/lib/jvm/jre$#JAVA_HOME=/usr/lib/jvm/jre-openjdk#' /etc/tomcat9/tomcat9.conf
```

We now install the EO.workspace packages, which should have been previously downloaded to the server:

```
# dnf -y install -y \
eow-web-access-*.rpm \
eow-guacamole-*.rpm \
eow-l10n-*.rpm \
eow-slaveserver-[0-9]*.rpm \
eow-slaveserver-role-wc-*.rpm \
ghostscript-*.rpm \
php-pecl-mcrypt-*.rpm
```

On **Oracle Linux**, we need to install some additional PHP-related packages, which are not installed automatically, as in other distributions:

```
# dnf -y install php-fpm php-json php-opcache
```

We now need to configure the Web Client component. To do this, we need to define the Session Manager address:

```
# eow-web-access-config
```

We then need to run the Slave Server configuration utility:

```
# eow-slaveserver-config
```

We then need to edit the PHP configuration file (`/etc/php.ini`) and configure the appropriate time zone, by changing the following line:

```
date.timezone = ...
```

One can either use "UTC" for the time zone or, if preferred, use one of the time zones described in the PHP documentation (eg. "Europe/Lisbon"):

- https://secure.php.net/manual/en/timezones.php

Finally, we need to enable and restart the web server (and PHP-FPM) services:

```
# systemctl enable httpd
# systemctl restart httpd php-fpm
```

Finally, we need to restart and configure the Tomcat service, the `guacd` daemon and the EOW Slave Server service to start automatically on boot:

```
# systemctl enable tomcat9 guacd eow-slaveserver
# systemctl restart tomcat9 guacd eow-slaveserver
```

The Web Client servers should now appear on the administration console, in the "Unregistered Servers" tab of the servers list on the "Infrastructure > Servers" section.

In order to enable them on the platform, the following steps should be executed:

- In the "Unregistered Servers" table, select the "+" button for each server; or select all the servers you want to add and use the "+ Register" button;
- In the "Servers" tab, check that all the servers were added correctly;
- If the server name doesn't correspond to its fully qualified domain name (FQDN), edit the server configuration, fill the "Internal name" input box with the correct FQDN;
- Click the "Switch to production" button in the server edit dialog, in order to activate them; or select all the servers you want to switch to production and use the "Switch to production" button on the servers table.

After this procedure, the Web Client servers are ready to be used.

4.5.3. Branding

Up to EOW version 6.0, in order to customize the branding of the user interface (replacing the product logos with the organization's), it's necessary to read the "EOW - Branding" article.

From EOW version 6.1 and later, the branding customization is performed through the Administration Console, in the "Configuration > Branding" section.

4.6. Gateway

The Gateway must be installed in a separate server from other EOW components.

4.6.1. Minimum System Requirements

- CPU: 4 cores
- Memory: 2 GiB
- Storage: 50 GiB
- Network: 1 Gbps NIC (2 for failover)
- OS: Enterprise Linux 8 (RedHat, Oracle, Rocky, Alma)

4.6.2. Instructions

In order to install the Gateway component, one should execute the following tasks.

We now install the EO.workspace packages, which should have been previously downloaded to the server:

```
# dnf -y install \
eow-slaveserver-[0-9]*.rpm \
eow-slaveserver-role-gateway-*.rpm \
eow-l10n-*.rpm
```

Next, we need to configure the EO.workspace Slave Server. On the Slave Server configuration, we need to define Session Manager address (which is described on the "Server - Virtual Servers" mechanism):

```
# eow-slaveserver-config
```

Finally, enable and restart the Slave Server service:

```
# systemctl enable eow-slaveserver
# systemctl restart eow-slaveserver
```

The Gateway servers should now appear on the administration console, in the "Unregistered Servers" tab of the servers list on the "Infrastructure > Servers" section.

In order to enable them on the platform, the following steps should be executed:

- In the "Unregistered Servers" table, select the "+" button for each server; or select all the servers you want to add and use the "+ Register" button;
- In the "Servers" tab, check that all the servers were added correctly;
- If the server name doesn't correspond to its fully qualified domain name (FQDN), edit the server configuration, fill the "Internal name" input box with the correct FQDN;
- Click the "Switch to production" button in the server edit dialog, in order to activate them; or select all the servers you want to switch to production and use the "Switch to production" button on the servers table.

From this moment on, you should be able to access the web client and administration console through the Gateway.

4.7. Distributed Session Manager

4.7.1. Minimum System Requirements

- CPU: 4 Cores
- Memory: 4 GiB
- Storage: 50 GiB
- Network: 1 Gbps NIC (2 for failover)
- OS: Enterprise Linux 8 (RedHat, Oracle, Rocky, Alma)

4.7.2. Instructions

In order to install the Distributed Session Manager component, one should execute the following tasks.

First, install the MariaDB database server (a drop-in replacement for the MySQL database). Also enable it to start on boot and start it:

```
# dnf -y install mariadb-server
# systemctl enable --now mariadb
```

Next, the `mysql_secure_installation` command should be run, in order to secure the MariaDB installation (eg. define the 'root' user password, remove test databases and users, etc.):

```
# mysql_secure_installation
```

Following the MySQL/MariaDB optimization instructions, although optional, is recommended. They are available here:

- EO.workspace - MySQL/MariaDB optimization

Finally, we need to create the database for the DSM, and create a user which will have full access to this database:

```
# mysql -u root -p
...
MariaDB[(none)]> CREATE DATABASE eow_dsm;
MariaDB[(none)]> CREATE USER 'eow'@'localhost' IDENTIFIED BY '<password>';
MariaDB[(none)]> GRANT ALL PRIVILEGES ON eow_dsm.* TO 'eow'@'localhost';
MariaDB[(none)]> FLUSH PRIVILEGES;
MariaDB[(none)]> quit
```

We now install the EO.workspace Distributed Session Manager and required packages, which should have been previously downloaded to the server:

```
# dnf install -y \
eow-dsm-*.rpm \
eow-gen-tls-*.rpm
```

Next, we need to configure the EO.workspace Distributed Session Manager. On the DSM configuration, we need to define the master Session Manager server (which will be used for initial authentication), as well as information regarding the database we previously configured:

```
# eow-dsm-config
```

Before we start the DSM for the first time, we need to either get a TLS key and certificate signed by a trusted CA, or generate a self-signed one:

Finally, simply enable and start the DSM service:

```
# eow-gen-tls -host $(hostname -f)
# mv cert.pem key.pem /etc/eow-dsm/
```

Finally, we need to enable and start the DSM daemon:

```
# systemctl enable --now eow-dsm
```

You can now access the DSM administration section by accessing the following URL and logging in with some credentials which are also valid for login on the configured Session Manager's Administration Console:

- https://<hostname>/admin

And perform the initial configuration.

5. Post-installation checklist

Not following the post-installation checklist may result in errors during EOW configuration and operation that may be hard to diagnose.

Before contacting Enterprise Open Support for any issue relating to an EOW landscape, please ensure every item in the post-installation checklist is done.

After installation, copy the table below and check that all the items have been done:

Item	Done	Not Done
All EOW and dependent services are running		
User-facing components (Web Client, Gateway) are accessible and have valid certificates installed		
Windows Application Servers do not require Network Level Authentication (NLA) to be used		
Application servers have security policies in place to restrict remote users' permissions in accordance with company guidelines		
If using domain integration for authentication, like AD or LDAP, ensure that users can login to all application servers with domain accounts		

6. Conclusion

After installation, you may consult the Quick Start Guide for a brief introduction to configuring and testing your EO.Workspace landscape, or consult the Operation and Administration Guide for a complete reference on how to administer and configure every part of the EO.Workspace environment.

O&G | Brasil

Enterprise Open workspace

A O&G BRASIL LTDA
CNPJ 23.518.044/0001-03
Endereço Setor SRTVS QD 701 BL O
Ed. Multiempresarial – Sala 423 parte K, Asa Sul
Distrito Federal, Brasília, Brasil – CEP: 70340-000
contato@ogbrasil.com.br | dpo@ogbrasil.com.br

REF	REQUISITO	*OBSERVAÇÕES*
1.	**introdução da especificação detalhada do objeto**	
1.1.	A presente especificação detalhada tem como objetivo descrever as especificações técnicas referentes a contratação de empresa especializada na implementação de soluções de área de trabalho virtual para aplicações corporativas. Além disso, a contratação inclui a prestação de serviços de treinamento, suporte técnico especializado sob demanda e Licença perpétua CAL (Client Access License) Microsoft RDS (Remote Desktop Services).	
1.2.	**Características Gerais**	
1.2.1.	Licenciamento (Licença Concorrente) da solução de gerenciamento centralizado de ferramentas e soluções do PRODERJ com suporte do fabricante: A empresa contratada irá fornecer, instalar e configurar licenças concorrentes para a solução de gerenciamento centralizado de ferramentas e soluções do PRODERJ. Essas licenças serão adquiridas diretamente do fabricante, com seu suporte técnico.	
2.	**Requisitos Gerais da Contratação**	
2.1.	Este processo de contratação prevê a aquisição de uma solução de área de trabalho virtual para aplicações corporativas que permita o PRODERJ oferecer uma nova modalidade de serviço de entrega de seus sistemas e aplicativos aos clientes finais por meio de um portal do cliente, sem a necessidade de instalação e configuração dos dispositivos locais, atendendo as mais altas práticas de segurança e rastreabilidade, além de permitir o uso de múltiplos dispositivos, como tablet's e smartphones.	• *Área de trabalho virtual: https://br.enterpriseopen.com/workspace/features/unified-application-environment/* • *Entrega ágil: https://br.enterpriseopen.com/workspace/features/user-zero-configuration/* • *Segurança: https://br.enterpriseopen.com/workspace/project-type/seguranca-e-privacidade-pt-br/*
2.2.	**A solução pretendida será composta, no mínimo, por:**	
2.2.1.	A solução deve prover tecnologia adaptável de alto desempenho, possibilitando que os aplicativos da CONTRATANTE sejam transmitidos dos servidores para diversos tipos de dispositivos dos usuários, usando tecnologias de codec modernas, adaptadas às condições de rede entre os usuários e a infraestrutura, bem como aos requisitos de negócios do PRODERJ.	• *Codecs modernos: https://br.enterpriseopen.com/workspace/features/high-performance-streaming/*
2.2.2.	A solução deve entregar o acesso aos aplicativos, arquivos, sites e rede, não sendo necessário que do lado da infraestrutura de servidores do PRODERJ, seja necessário possuir uma máquina virtual para cada usuário.	• *Servidores centralizados: https://br.enterpriseopen.com/workspace/features/consolidation-and-optimization/* • *Arquitetura baseada em sessões: https://br.enterpriseopen.com/workspace/features/modular-architecture/* • *Streaming de aplicações: https://br.enterpriseopen.com/workspace/features/seamless-applications/*
2.2.3.	A solução deve permitir seções de tutorial e ou ajuda específicas de aplicativos/telas (por exemplo, detectando títulos de janelas, nomes de executáveis etc.), fornecendo instruções detalhadas sobre aplicativos específicos ou funcionalidades.	• *2. Tutorial Interativo: Evidencias complementares.pdf* • *Publicação customizável de aplicações estáticas e Web: https://enterpriseopen.com/workspace/wp-content/uploads/EOW-Showcase-Web-Applications-01-Fast-Recode.mp4*
2.2.4.	A solução deve permitir a utilização e o reaproveitamento dos recursos computacionais disponíveis no parque computacional da CONTRATANTE: servidores, microcomputadores (desktops), tablets e notebooks.	• *Consolidação de recursos: https://br.enterpriseopen.com/workspace/features/consolidation-and-optimization/* • *Otimização do uso de recursos: https://br.enterpriseopen.com/workspace/features/lean-server-components/* • *Eficiência com uso de dispositivos obsoletos ou de baixo custo: https://br.enterpriseopen.com/workspace/features/plug-forget-and-disposable-clients/* • *Eficiência com uso de dispositivos externos: https://br.enterpriseopen.com/workspace/features/bring-your-own-device/* • *Eficiência com uso de softwares alternativos: https://br.enterpriseopen.com/workspace/features/supplier-choice* • *Multiplataforma: https://br.enterpriseopen.com/workspace/features/cross-platform-and-cross-generation/* • *Suporte integral: https://br.enterpriseopen.com/workspace/descarregar/*

2.2.5.	Permitir a mesma experiência do usuário e a disponibilidade de funcionalidades presentes nas plataformas Windows e Linux, para qualquer tipo de suporte tecnológico descrito no item 4.2.14 deste documento.	• *Ambiente cirtual unificado: https://br.enterpriseopen.com/workspace/features/unified-application-environment/*
2.2.6.	A solução deve autenticar seus usuários de forma centralizada, estruturada por perfis e grupos de usuários.	• *Single Sign-On (SSO): https://br.enterpriseopen.com/workspace/features/advanced-authentication/* • *Autenticação Multi Fator: https://br.enterpriseopen.com/workspace/features/integrated-multi-factor-authentication/* • *Autenticação Centralizada (AD/LADAP/INTERNAL): https://br.enterpriseopen.com/workspace/features/multiple-domains-and-directories/*
2.2.7.	A solução deve permitir a configuração de restrição de login, por meio de uma agenda com limite de horas e dias da semana em que os usuários podem acessar os aplicativos (por grupo de usuários ou usuários específicos).	• *3. Restrições de horário: Evidencias complementares.pdf*
2.2.8.	Cada usuário deve possuir sua própria área de trabalho, sendo que os acesso aos aplicativos e os links de acesso devem ser previamente definidos pelo Gestor da CONTRATANTE. Nenhuma configuração precisa ser realizada pelo usuário, apenas o nome do servidor e as credenciais precisam ser fornecidas.	• *Entrega ágil: https://br.enterpriseopen.com/workspace/features/user-zero-configuration/* • *Controle administrativo granular: https://br.enterpriseopen.com/workspace/features/delegated-administration/*
2.2.9.	A solução deve permitir a persistência de sessão, ou seja, o usuário poderá iniciar uma atividade dentro da solução / plataforma em um determinado período e/ou equipamento e concluí-lo em um tempo posterior e/ou em outro equipamento, garantindo que a sua sessão com as informações e sistemas em operação serão mantidos.	• *4 - Persistência de sessão: Evidencias complementares.pdf* • *Persistência de sessão: https://enterpriseopen.com/workspace/wp-content/uploads/EOW-Showcase-High-Performance-Streaming-01-Fast.mp4-Recode.mp4*
2.2.10.	A solução deve prever o redimensionamento dinâmico de tela, permitindo que os aplicativos publicados possam corresponder à resolução local do usuário ou à janela do navegador.	• *Interface dinâmica: https://br.enterpriseopen.com/workspace/features/multi-monitor/*
2.2.11.	A solução deve possuir um acesso simplificado ao ambiente computacional da CONTRATANTE através de um navegador Web de mercado, suportado a partir da tecnologia HTML5, compatível minimamente com os navegadores Google Chrome e Microsoft EDGE.	• *Cliente Web: https://br.enterpriseopen.com/workspace/features/advanced-web-client/*
2.2.12.	A solução deve possuir, alternativamente, aplicativo cliente próprio, que permita a utilização de portas USB, com o acesso rápido ao ambiente da CONTRATANTE, disponível minimamente para as seguintes plataformas de mercado:	• *Redirecionamento de recursos: https://br.enterpriseopen.com/workspace/features/advanced-customizable-redirection/* • *Cliente Nativo: https://br.enterpriseopen.com/workspace/features/seamless-applications/* • *ClientOS: https://br.enterpriseopen.com/workspace/features/clientos/*
2.2.12. a)	Windows	• *Cliente Nativo: https://br.enterpriseopen.com/workspace/descarregar/*
2.2.12. b)	Linux	• *Cliente Nativo: https://br.enterpriseopen.com/workspace/descarregar/*
2.2.12. c)	MacOS	• *Cliente Nativo: https://br.enterpriseopen.com/workspace/descarregar/*
2.2.12. d)	IOS	• *Cliente Nativo: https://br.enterpriseopen.com/workspace/descarregar/*
2.2.12. e)	ANDROID	• *Cliente Nativo: https://br.enterpriseopen.com/workspace/descarregar/*
2.2.13.	**A solução deve apresentar, em todas as suas formas de acesso, uma interface homogênea, intuitiva e unificada, similar a um Desktop, onde:**	
2.2.13. a)	Seja possível buscar e a utilizar simultaneamente diferentes aplicações;	• *Ambinetente unificado: https://br.enterpriseopen.com/workspace/features/unified-application-environment/*
2.2.13. b)	Seja possível minimizar, maximizar, redimensionar as janelas das aplicações;	• *Interface dinâmica: https://br.enterpriseopen.com/workspace/features/multi-monitor/*
2.2.13. c)	Permita o uso de tela cheia e múltiplos monitores;	• *Interface dinâmica: https://br.enterpriseopen.com/workspace/features/multi-monitor/*
2.2.13. d)	Haja pelo menos uma forma de apresentação alternativa, simplificada que permita a utilização dos aplicativos.	• *Cliente Web: https://br.enterpriseopen.com/workspace/features/advanced-web-client/*
2.2.14.	**A solução deve apresentar em todas as suas formas de acesso as seguintes funcionalidades:**	
2.2.14. a)	Suportar operações de copiar e colar, transitando a área de transferência entre as diferentes aplicações, servidores e sistemas operacionais envolvidos, incluindo o dispositivo local do usuário, simulando um ambiente unificado e sem complicações aos usuários.	• *Ambinetente unificado: https://enterpriseopen.com/workspace/wp-content/uploads/EOW-Showcase-Seamless-Applications-01-Fast-Recode.mp4*

2.2.14. b)	Permitir abrir aplicações remotas, no dispositivo do usuário, em janelas individuais, lado a lado, independentemente se elas estão instaladas em ambientes operacionais Linux ou Windows, garantindo uma experiência fluída com diversos sistemas operacionais.	• *Multiplataforma: https://br.enterpriseopen.com/workspace/features/linux-application-streaming/* • *Integração local: https://br.enterpriseopen.com/workspace/features/local-environment-integration/* • *Cliente Nativo: https://br.enterpriseopen.com/workspace/descarregar/* • *Ambinetente unificado: https://enterpriseopen.com/workspace/wp-content/uploads/EOW-Showcase-Seamless-Applications-01-Fast-Recode.mp4*
2.2.14. c)	Permitir exibir notificações de informações importantes para todos os usuários em sua sessão, com a possibilidade de configurar mensagens, mostradas no formato pop-up, no momento do login do usuário.	• *1. Aviso pop-up: Evidencias complementares.pdf* • *2.1.19. Configuration > News: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.2.14. d)	Possibilitar o uso do navegador da própria estação de trabalho para carregar aplicações WEB configuradas no ambiente de trabalho centralizado que invoquem uma chamada externa, possibilitando a passagem de parâmetros de autenticação.	• *Web Applications: https://br.enterpriseopen.com/workspace/features/web-applications/*
2.2.15.	**O software cliente deve possuir, minimamente, as seguintes funcionalidades:**	
2.2.15. a)	A solução deve impedir que versões de Cliente desatualizadas efetuem login no ambiente, com a capacidade de exibir avisos customizados aos usuários. Poder ser configurado no console de administração da solução - para ser iniciado com uma interface de usuário simplificada, incluindo apenas o processo de autenticação definido.	• *11. Controle de versão: Evidencias complementares.pdf*
2.2.15. b)	Poder definir diferentes formas de autenticação, de maneira simplificada.	• *Single Sign-On (SSO): https://br.enterpriseopen.com/workspace/features/advanced-authentication/* • *Autenticação Multi Fator: https://br.enterpriseopen.com/workspace/features/integrated-multi-factor-authentication/* • *Autenticação Centralizada (AD/LADAP/INTERNAL): https://br.enterpriseopen.com/workspace/features/multiple-domains-and-directories/*
2.2.15. c)	Deve suportar recurso de assistência remota nativa do sistema operacional para permitir que o suporte técnico e os administradores de sistema forneçam assistência aos clientes e usuários com sessões ativas na solução sem a necessidade de softwares adicionais.	• *Diagnóstico de sessão: https://br.enterpriseopen.com/workspace/features/session-diagnostics/* • *Assistência remota: https://br.enterpriseopen.com/workspace/features/session-shadowing/* • *Suporte ágil: https://br.enterpriseopen.com/workspace/features/agile-support/*
2.2.15. d)	Deve suportar o uso de múltiplos monitores em microcomputadores pessoais (desktops) e notebooks.	• *Interface dinâmica: https://br.enterpriseopen.com/workspace/features/multi-monitor/*
2.2.15. e)	Deve permitir a execução de comandos através de linha de comando, permitindo que os administradores configurem e distribuam lançadores personalizados ou atalhos que simplificam o processo de login dos usuários;	• *EO.workspace - Native Client Command-Line Interface.pdf* • *Publicação customizável de aplicações estáticas e Web: https://enterpriseopen.com/workspace/wp-content/uploads/EOW-Showcase-Web-Applications-01-Fast-Recode.mp4* • *SDK: https://br.enterpriseopen.com/workspace/features/sdk-de-integracao/*
2.2.16.	A solução deve permitir o uso dispositivos periféricos de entrada (teclado e mouse) ao acessar aplicativos publicados por meio de um dispositivo móvel (smartphone ou tablet).	• *Multiplataforma: https://br.enterpriseopen.com/workspace/features/linux-application-streaming/* • *Integração local: https://br.enterpriseopen.com/workspace/features/local-environment-integration/* • *Cliente Nativo: https://br.enterpriseopen.com/workspace/descarregar/*
2.2.17.	A solução deve permitir a utilização da porta USB do dispositivo local para o ambiente remoto, possibilitando o uso de Smartcard, tokens, impressoras locais, etc, independente do sistema operacional (Windows e Linux).	• *Redirecionamento de recursos: https://br.enterpriseopen.com/workspace/features/advanced-customizable-redirection/* • *Cliente Nativo: https://br.enterpriseopen.com/workspace/features/seamless-applications/* • *ClientOS: https://br.enterpriseopen.com/workspace/features/clientos/*
2.2.18.	A solução deve possuir a capacidade de entregar, no ambiente de trabalho centralizado do Usuário, aplicações legadas, geralmente, desenvolvidas no modelo Cliente/Servidor, e devem ser entregues de forma transparente e integrada.	• *Suporte à aplicações legadas: https://br.enterpriseopen.com/workspace/features/legacy-application-support/*
2.2.19.	A solução deve permitir a passagem de parâmetros na publicação de aplicações locais e WEB, gerando links personalizados pelo console de administração no ambiente de trabalho centralizado do usuário.	• *Publicação customizável de aplicações estáticas e Web: https://enterpriseopen.com/workspace/wp-content/uploads/EOW-Showcase-Web-Applications-01-Fast-Recode.mp4*
2.2.20.	A solução deve possuir a capacidade de agrupar um conjunto de aplicações e definir políticas de acesso baseadas em grupos ou perfis de usuários, gerenciadas pelo console de administração.	• *Controle administrativo granular: https://br.enterpriseopen.com/workspace/features/delegated-administration/* • *2.1.9. Applications > Publications: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.2.21.	A solução deve permitir que os usuários mantenham arquivos e configurações de forma persistente entre as sessões, em diferentes servidores de aplicativos com diferentes sistemas operacionais.	• *4 - Persistência de sessão: Evidencias complementares.pdf* • *Persistência de sessão: https://enterpriseopen.com/workspace/wp-content/uploads/EOW-Showcase-High-Performance-Streaming-01-Fast.mp4-Recode.mp4*

2.2.22.	A solução deve permitir a inicialização de aplicativos de forma intuitiva para os usuários, a partir de atalhos em sua área de trabalho local.	• *Ambinetente unificado: https://br.enterpriseopen.com/workspace/features/unified-application-environment/*
2.2.23.	A solução deve permitir que os usuários ou administradores organizem os ícones do aplicativo em pastas ou usando tags.	• *Ambinetente unificado: https://br.enterpriseopen.com/workspace/features/unified-application-environment/*
2.2.24.	A solução deve suportar a execução de aplicativos portáteis, que são baixados e executados no dispositivo do usuário final.	• *Publicação customizável de aplicações estáticas e Web: https://enterpriseopen.com/workspace/wp-content/uploads/EOW-Showcase-Web-Applications-01-Fast-Recode.mp4*
2.2.25.	A solução deve permitir a instalação de aplicativos e o provisionamento de recursos (por exemplo, armazenamento etc.) na infraestrutura da solução.	• *2.1.7. Applications > Applications: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf* • *Consolidação de recursos: https://br.enterpriseopen.com/workspace/features/consolidation-and-optimization/* • *5 - Compartilhamento de diretórios externos: Evidencias complementares.pdf* • *2.1.2. Infrastructure > Storage: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.2.26.	A solução deve permitir a orquestração de todos os componentes por meio do uso de estratégias modernas, como conteinerização e tecnologias equivalentes em sistemas operacionais baseados em Windows.	• *Agnóstico à virtualização: https://br.enterpriseopen.com/workspace/features/infrastructure-and-cloud-agnostic/* • *EO.workspace - Native Client Command-Line Interface.pdf* • *EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.2.27.	A solução deve permitir seções de tutorial/ajuda específicas de aplicativos/telas, detectando títulos de janelas, nomes de executáveis, etc.	• *Agnóstico à virtualização: https://br.enterpriseopen.com/workspace/features/infrastructure-and-cloud-agnostic/* • *1 - Tutorial: Evidencias complementares.pdf*
2.2.28.	A solução deve permitir integrar (configurar, gerenciar e controlar) recursos de isolamento de aplicativos do sistema operacional, como o Windows AppLocker ou o SELinux.	• *Isolamento de aplicações: https://br.enterpriseopen.com/workspace/features/application-bubble/*
2.2.29.	A solução deve permitir monitorar o estado de atualização do produto de cada sistema operacional dos servidores e dos aplicativos publicados.	• *Gerenciamento de atualizações: https://br.enterpriseopen.com/workspace/features/update-management/* • *Dashboard: https://enterpriseopen.com/workspace/wp-content/uploads/EOW-Showcase-Quarentine-01-Fast-Recode.mp4*
2.2.30.	A solução deve permitir a ativação de uma funcionalidade de marca d'agua que será inserida em diversos pontos durante a sessão do usuário.	• *Marca d'agua: https://br.enterpriseopen.com/workspace/features/session-watermark/*
2.2.31.	A solução deve impedir que os usuários façam capturas de tela dos aplicativos em execução ou notificar os administradores caso um usuário tente realizar essa ação.	• *Proteção contra captura de tela: https://br.enterpriseopen.com/workspace/features/screenshot-protection/*
2.2.32.	A solução deve permitir que os usuários acessem diretamente os arquivos armazenados nos servidores da solução usando algum tipo de navegador de arquivos no Web Client.	• *Cliente Web: https://br.enterpriseopen.com/workspace/features/advanced-web-client/*
2.3.	**Requisitos de Negócio**	
2.3.1.	A solução a ser adotada deverá ser capaz de:	
2.3.1.1.	Fortalecer a segurança da informação nos sistemas da CONTRATANTE.	• *Recursos de segurança: https://br.enterpriseopen.com/workspace/project-type/seguranca-e-privacidade-pt-br/*
2.3.1.2.	Permitir, com maior eficiência, o rastreamento de acesso e utilização de recursos por cada usuário/login.	• *Trilha de auditoria: https://br.enterpriseopen.com/workspace/features/audit-trail/*
2.3.1.3.	Possibilidade de prover soluções tecnológicas adequadas ao ambiente centralizado de trabalho da CONTRATANTE, seja no seu ambiente on-premisse ou em nuvem pública.	• *Agnóstico à virtualização: https://br.enterpriseopen.com/workspace/features/infrastructure-and-cloud-agnostic/* • *Consolidação de recursos: https://br.enterpriseopen.com/workspace/features/consolidation-and-optimization/* • *Otimização do uso de recursos: https://br.enterpriseopen.com/workspace/features/lean-server-components/* • *Eficiência com uso de dispositivos obsoletos ou de baixo custo: https://br.enterpriseopen.com/workspace/features/plug-forget-and-disposable-clients/* • *Eficiência com uso de dispositivos externos: https://br.enterpriseopen.com/workspace/features/bring-your-own-device/* • *Eficiência com uso de softwares alternativos: https://br.enterpriseopen.com/workspace/features/supplier-choice* • *Multiplataforma: https://br.enterpriseopen.com/workspace/features/cross-platform-and-cross-generation/* • *Suporte integral: https://br.enterpriseopen.com/workspace/descarregar/*
2.3.1.4.	Permitir a migração gradual para o ambiente centralizado da CONTRANTE, de forma a permitir a execução do projeto em fases, não impactando no processo de migração para o novo ambiente.	• *Arquitetura modular: https://br.enterpriseopen.com/workspace/features/modular-architecture/*
2.3.1.5.	Garantir uma interface unificada, padronizada e centralizada para todos os dispositivos suportados.	• *Ambinetente unificado: https://br.enterpriseopen.com/workspace/features/unified-application-environment/* • *Integração local: https://br.enterpriseopen.com/workspace/features/local-environment-integration/* • *Múltiplataforma: https://br.enterpriseopen.com/workspace/features/linux-application-streaming/* • *Múltigeracional: https://br.enterpriseopen.com/workspace/features/cross-platform-and-cross-generation/* • *Interoperável: https://br.enterpriseopen.com/workspace/descarregar/*

2.3.1.6.	Permitir a otimização de gestão e disponibilidade doe ambiente de trabalho da CONTRANTE, viabilizando o acesso somente às ferramentas tecnológicas homologadas e autorizadas.	• *Admnistração Centralizada: https://br.enterpriseopen.com/workspace/features/delegated-administration/* • *Dashboard: https://enterpriseopen.com/workspace/wp-content/uploads/EOW-Showcase-Quarentine-01-Fast-Recode.mp4*
2.3.1.7.	Permitir a gestão e monitoramento de recursos oferecidos aos usuários.	• *Administração Centralizada: https://br.enterpriseopen.com/workspace/features/delegated-administration/* • *Controle centralizado de dispositivos: https://br.enterpriseopen.com/workspace/features/clientos/* • *Autenticação centralizada: https://br.enterpriseopen.com/workspace/features/advanced-authentication/* • *Autorização centralizada: https://br.enterpriseopen.com/workspace/features/robust-authorization/* • *Processamento centralizado: https://br.enterpriseopen.com/workspace/features/seamless-applications/* • *Isolamento físico: https://br.enterpriseopen.com/workspace/features/untrusted-end-device/*
2.3.1.8.	Disponibilizar mecanismos que viabilizem o acesso a conteúdos digitais por diversos canais: navegadores web, aplicativos de texto, planilhas, apresentações, gestão de arquivos de todos os usuários, dentre outras modalidades que possam surgir com a evolução tecnológica..	• *Ambinetente unificado: https://br.enterpriseopen.com/workspace/features/unified-application-environment/* • *Integração local: https://br.enterpriseopen.com/workspace/features/local-environment-integration/* • *Múltiplataforma: https://br.enterpriseopen.com/workspace/features/linux-application-streaming/* • *Múltigeracional: https://br.enterpriseopen.com/workspace/features/cross-platform-and-cross-generation/* • *Interoperável: https://br.enterpriseopen.com/workspace/descarregar/*
2.3.1.9.	Permitir a gestão e gerenciamento computacionais fornecidos aos usuários de forma centralizada, considerando a otimização de infraestrutura.	• *Administração Centralizada: https://br.enterpriseopen.com/workspace/features/delegated-administration/* • *Controle centralizado de dispositivos: https://br.enterpriseopen.com/workspace/features/clientos/* • *Autenticação centralizada: https://br.enterpriseopen.com/workspace/features/advanced-authentication/* • *Autorização centralizada: https://br.enterpriseopen.com/workspace/features/robust-authorization/* • *Processamento centralizado: https://br.enterpriseopen.com/workspace/features/seamless-applications/* • *Isolamento físico: https://br.enterpriseopen.com/workspace/features/untrusted-end-device/*
2.3.1.10.	Assegurar e responsabilizar-se pela continuidade do negócio implementado pelos ambientes gerenciados sob sua responsabilidade técnica.	*Requisito de prestação de serviço*
2.3.1.11.	Assegurar o adequado tratamento de dados pessoais e informações classificadas, dos quais venha a ter conhecimento, ou manusear em razão da execução do objeto do contrato, nos termos da Lei n° 13.709/2018 (Lei Geral de Proteção de Dados) e em aderência aos requisitos de segurança da informação vigentes no ambiente da CONTRANTANTE.	*Requisito de prestação de serviço*
2.3.1.12.	Assegurar a gestão e o tratamento de incidentes de forma sistematizada, em estrita harmonia aos requisitos vigentes no ambiente da CONTRATANTE.	*Requisito de prestação de serviço*
2.3.1.13.	Promover recursos de segurança da Informação visando a proteção dos recursos computacionais gerenciados pela solução, além de suporte para apurar falhas e/ou atestar a conformidade da utilização destes recursos pelos usuários.	• *Diagnóstico de sessão: https://br.enterpriseopen.com/workspace/features/session-diagnostics/* • *Assistência remota: https://br.enterpriseopen.com/workspace/features/session-shadowing/* • *Suporte ágil: https://br.enterpriseopen.com/workspace/features/agile-support/*
2.3.1.14.	Promover a alta disponibilidade em ambientes geograficamente distintos, permitindo a disponibilidade do serviço e a operação, mesmo em casos de sinistros, relacionados a um local específico do datacenter.	• *Balanceador de carga geográfico: https://br.enterpriseopen.com/workspace/features/dsm-advanced-load-balancing/*
2.3.1.15.	Permitir um acesso unificado a todas as aplicações através de uma única interface, possibilitando uma melhor compreensão de todos os recursos disponíveis aos usuários.	• *Ambinetente unificado: https://br.enterpriseopen.com/workspace/features/unified-application-environment/* • *Integração local: https://br.enterpriseopen.com/workspace/features/local-environment-integration/* • *Múltiplataforma: https://br.enterpriseopen.com/workspace/features/linux-application-streaming/* • *Múltigeracional: https://br.enterpriseopen.com/workspace/features/cross-platform-and-cross-generation/* • *Interoperável: https://br.enterpriseopen.com/workspace/descarregar/*
2.3.1.16.	Assegurar que as aplicações do PRODERJ executem com requisitos computacionais extremamente baixos, melhorando a eficácia e eficiência dos recursos já empregados no ambiente computacional existente.	• *Consolidação de recursos: https://br.enterpriseopen.com/workspace/features/consolidation-and-optimization/* • *Otimização do uso de recursos: https://br.enterpriseopen.com/workspace/features/lean-server-components/* • *Eficiência com uso de dispositivos obsoletos ou de baixo custo: https://br.enterpriseopen.com/workspace/features/plug-forget-and-disposable-clients/* • *Eficiência com uso de dispositivos externos: https://br.enterpriseopen.com/workspace/features/bring-your-own-device/* • *Eficiência com uso de softwares alternativos: https://br.enterpriseopen.com/workspace/features/supplier-choice* • *Multiplataforma: https://br.enterpriseopen.com/workspace/features/cross-platform-and-cross-generation/* • *Suporte integral: https://br.enterpriseopen.com/workspace/descarregar/*
2.3.1.17.	A solução deve permitir a personalização da marca em diversos aspectos fundamentais, incluindo nome, logótipos, cores, imagens de fundo, legendas e outros elementos.	• *Customização de identidade visual: https://br.enterpriseopen.com/workspace/features/pervasive-branding/*

2.3.1.18.	A solução deve permitir que os usuários mantenham arquivos e configurações entre as sessões, em diferentes servidores de aplicativos com diferentes sistemas operacionais.	• *5 - Compartilhamento de diretórios externos: Evidencias complementares.pdf* • *2.1.2. Infrastructure > Storage: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.3.1.19.	A solução deve possuir recurso que permita o compartilhamento de diretórios de rede ou grupos ou perfis sem a necessidade da aplicação de políticas de grupo ou login scripts.	• *5 - Compartilhamento de diretórios externos: Evidencias complementares.pdf* • *2.1.2. Infrastructure > Storage: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.3.1.20.	A solução deve permitir que os usuários acessem aplicativos de qualquer dispositivo e em qualquer local, tanto internamente ao PRODERJ quanto remotamente pela Internet.	• *Bring Your Own Device (BYOD): https://br.enterpriseopen.com/workspace/features/bring-your-own-device/*
2.3.1.21.	A solução deve permitir a reutilização de hardware antigo ou dispositivos simples de baixo consumo de energia.	• *Eficiência com uso de dispositivos obsoletos ou de baixo custo: https://br.enterpriseopen.com/workspace/features/plug-forget-and-disposable-clients/*
2.3.1.22.	A solução deve permitir que milhares de usuários trabalhem a partir de um pequeno número de servidores.	• *Consolidação de recursos: https://br.enterpriseopen.com/workspace/features/consolidation-and-optimization/* • *Otimização do uso de recursos: https://br.enterpriseopen.com/workspace/features/lean-server-components/* • *Eficiência com uso de dispositivos obsoletos ou de baixo custo: https://br.enterpriseopen.com/workspace/features/plug-forget-and-disposable-clients/* • *Eficiência com uso de dispositivos externos: https://br.enterpriseopen.com/workspace/features/bring-your-own-device/* • *Eficiência com uso de softwares alternativos: https://br.enterpriseopen.com/workspace/features/supplier-choice*
2.3.1.23.	A solução deve utilizar a infraestrutura de virtualização existente do PRODERJ, sem comprometer o desempenho ou a estabilidade.	• *Agnóstico à virtualização: https://br.enterpriseopen.com/workspace/features/infrastructure-and-cloud-agnostic/*
2.3.1.24.	A solução deve permitir a configuração do limite de tempo para as sessões do usuário.	• *6. Tempo limite de sessão: Evidencias complementares.pdf*
2.3.1.25.	A solução deve possuir funcionalidade que permita a utilização das soluções de armazenamento externo existentes para perfil de usuário ou dados do usuário.	• *5 - Compartilhamento de diretórios externos: Evidencias complementares.pdf* • *2.1.2. Infrastructure > Storage: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.3.1.26.	A solução deve permitir a simplificação da publicação de aplicativos, permitindo a definição de conjuntos de aplicativos relacionados.	• *2.1.9. Applications > Publications: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.3.1.27.	A solução deve aproveitar os grupos de usuários novos ou existentes em seu domínio do Active Directory para regras de publicação de aplicativos.	• *7. Grupos do Active Directory: Evidencias complementares.pdf* • *Autenticação Centralizada (AD/LADAP/INTERNAL): https://br.enterpriseopen.com/workspace/features/multiple-domains-and-directories/* • *Autorização robusta: https://br.enterpriseopen.com/workspace/features/robust-authorization/* • *Redirecionamento de recursos: https://br.enterpriseopen.com/workspace/features/advanced-customizable-redirection/* • *Gestão de impressão avançada: https://br.enterpriseopen.com/workspace/features/advanced-printing/*
2.3.1.28.	A solução deve permitir a integração com um domínio LDAP como fonte de recursos.	• *7. Grupos do Active Directory: Evidencias complementares.pdf* • *Autenticação Centralizada (AD/LADAP/INTERNAL): https://br.enterpriseopen.com/workspace/features/multiple-domains-and-directories/* • *Autorização robusta: https://br.enterpriseopen.com/workspace/features/robust-authorization/* • *Redirecionamento de recursos: https://br.enterpriseopen.com/workspace/features/advanced-customizable-redirection/* • *Gestão de impressão avançada: https://br.enterpriseopen.com/workspace/features/advanced-printing/*
2.4.	**Requisitos tecnológicos de Segurança e Autenticação**	
2.4.1.	A solução deve prover uma tecnologia em que os usuários acessem aplicativos e dados com segurança, mesmo via Internet, sem a necessidade de uma VPN, reduzindo a complexidade e diminuindo as possíveis superfícies de ataque. Todo o tráfego deve ser criptografado, reduzindo o número de portas que precisam ser abertas no Firewall do PRODERJ.	• *VPN Integrada: https://br.enterpriseopen.com/workspace/features/integrated-tls-vpn/*
2.4.2.	A solução deve possuir recursos de verificação de integridade das aplicações publicadas de forma automática e permitindo o agendamento dessas verificações.	• *Verificação de integridade de aplicações: https://br.enterpriseopen.com/workspace/features/application-integrity/*
2.4.3.	A solução deve, ainda, permitir colocar em quarentena, de forma automática, aplicações e/ou servidores da solução se algum evento de segurança for acionado (falha na validação da integridade do aplicativo, alerta de antivírus e atualizações críticas de segurança disponíveis.	• *Quarentena automática: https://br.enterpriseopen.com/workspace/features/quarantine/*
2.4.4.	A solução deve permitir habilitar uma marca d'água que será desenhada em vários locais ao longo da sessão do usuário, independentemente do cliente e método de acesso utilizado. Essa marca d'água deve permitir que a capturas de tela sejam identificáveis.	• *Marca d'agua: https://br.enterpriseopen.com/workspace/features/session-watermark/*

2.4.5.	A solução deve garantir acesso seguro aos aplicativos em todas as suas formas de acesso, com o uso de criptografia SSL/TLS integrada.	• VPN TLS Integrada: https://br.enterpriseopen.com/workspace/features/integrated-tls-vpn/
2.4.6.	A solução deve possuir funcionalidade de detecção e mitigação de capturas de tela dos aplicativos em execução na plataforma.	• *Proteção contra captura de tela: https://br.enterpriseopen.com/workspace/features/screenshot-protection/*
2.4.7.	A solução deve permitir a configuração de ambientes sandbox (isolado)de aplicações, de forma isolada do restante do ambiente.	• *Sandbox: https://br.enterpriseopen.com/workspace/features/application-bubble/*
2.4.8.	A solução deve permitir a integração com balanceadores, proxy reversos e outros recursos de infraestrutura de forma a permitir o acesso a aplicações web internas, através do browser do ambiente de trabalho publicado e, eventualmente do dispositivo local do cliente, sem necessidade de utilização de VPN.	• *VPN TLS Integrada: https://br.enterpriseopen.com/workspace/features/integrated-tls-vpn/*
2.4.9.	**A solução deve proporcionar funcionalidades de Autenticação, Autorização e Auditoria, observando:**	
2.4.9. a)	Autenticação- Suportar diversos fatores de autenticação podendo ser baseada em Credenciais padrão (nome e senha), com suporte a tecnologia de Múltiplo Fator de Autenticação (MFA) e permitindo a integração com as bases Open LDAP e Microsoft Active Directory, além do suporte à provedores de identidade externos (IDP) como Google, Azure etc.	• *Single Sign-On (SSO): https://br.enterpriseopen.com/workspace/features/advanced-authentication/* • *Autenticação Multi Fator: https://br.enterpriseopen.com/workspace/features/integrated-multi-factor-authentication/* • *Autenticação Centralizada (AD/LADAP/INTERNAL): https://br.enterpriseopen.com/workspace/features/multiple-domains-and-directories/*
2.4.9. b)	Autorização– Permitir a liberação do acesso às aplicações publicadas no ambiente computacional a partir de grupos ou permissão direta, sem que haja a necessidade de instalar uma aplicação para cada usuário.	• *7. Grupos do Active Directory: Evidencias complementares.pdf*
2.4.9. c)	Auditoria– Permitir, minimamente, o acesso das seguintes informações para fins de auditoria: data e hora de autenticação, nome do usuário, identificador (ID) da sessão, forma de acesso às aplicações, identificação dos servidores que sustentam as aplicações, das quais o usuário tem permissão de acesso, todas as aplicações que o usuário tem permissão de acesso, data e hora que o usuário acessou cada aplicação, data e hora que o usuário saiu de cada aplicação, data e hora que o usuário saiu da solução de sua área de trabalho, Forma de desconexão e encerramento da sessão.	• *Trilha de auditoria: https://br.enterpriseopen.com/workspace/features/audit-trail/*
2.4.10.	A solução deve disponibilizar mecanismos de Controle de Autenticação, Acesso e Segurança que permita integrar com Provedores de Identidade (IdP) baseados em SAML para delegação segura de autenticação de usuário e Federação de Identidade.	• *Single Sign-On (SSO): https://br.enterpriseopen.com/workspace/features/advanced-authentication/* • *Autenticação Multi Fator: https://br.enterpriseopen.com/workspace/features/integrated-multi-factor-authentication/* • *Autenticação Centralizada (AD/LADAP/INTERNAL): https://br.enterpriseopen.com/workspace/features/multiple-domains-and-directories/*
2.4.11.	A solução deve permitir que os ne aplicativos nela publicados autentiquem-se diretamente com seus respectivos IDPs através da tecnologia de Single Sign-On (SSO).	• *Single Sign-On (SSO): https://br.enterpriseopen.com/workspace/features/advanced-authentication/* • *Autenticação Multi Fator: https://br.enterpriseopen.com/workspace/features/integrated-multi-factor-authentication/* • *Autenticação Centralizada (AD/LADAP/INTERNAL): https://br.enterpriseopen.com/workspace/features/multiple-domains-and-directories/*
2.4.12.	A solução deve permitir o mapeamento e a conexão a diretórios existentes (LDAP/AD) com gerenciamento de controle de acesso de usuário granular tais como aplicativos, servidores, redirecionamento de impressoras/unidades e permissões de gerenciamento.	• *7. Grupos do Active Directory: Evidencias complementares.pdf* • *Autenticação Centralizada (AD/LADAP/INTERNAL): https://br.enterpriseopen.com/workspace/features/multiple-domains-and-directories/* • *Autorização robusta: https://br.enterpriseopen.com/workspace/features/robust-authorization/* • *Redirecionamento de recursos: https://br.enterpriseopen.com/workspace/features/advanced-customizable-redirection/* • *Gestão de impressão avançada: https://br.enterpriseopen.com/workspace/features/advanced-printing/*
2.4.13.	A solução deve permitir o uso de subsistemas de segurança fornecidos por fornecedores de sistemas operacionais, minimamente o AppLocker e o SELinux para aumentar o controle sobre o que os usuários podem fazer.	• *Suporte a subsistemas de segurança: https://enterpriseopen.com/workspace/wp-content/uploads/EOW-Showcase-Integrated-TLS-VPN-01-Fast-Recode.mp4* • *Consolidação de recursos: https://br.enterpriseopen.com/workspace/features/consolidation-and-optimization/*
2.4.14.	A solução deve permitir a imposição de privilégio mínimo a aplicativos e usuários, reduzindo ou eliminando possíveis problemas de segurança.	• *Autorização robusta: https://br.enterpriseopen.com/workspace/features/robust-authorization/*

2.4.15.	A solução deve permitir o controle completo e granular sobre quais recursos de redirecionamento (entrada/saída de áudio, unidades e arquivos, área de transferência, impressoras, cartão inteligente) os usuários podem usar em seus dispositivos locais.	• *7. Grupos do Active Directory: Evidencias complementares.pdf* • *Autenticação Centralizada (AD/LADAP/INTERNAL): https://br.enterpriseopen.com/workspace/features/multiple-domains-and-directories/* • *Autorização robusta: https://br.enterpriseopen.com/workspace/features/robust-authorization/* • *Redirecionamento de recursos: https://br.enterpriseopen.com/workspace/features/advanced-customizable-redirection/* • *Gestão de impressão avançada: https://br.enterpriseopen.com/workspace/features/advanced-printing/*
2.4.16.	A solução deve fornecer, minimamente, mecanismos de controle do ambiente de execução do aplicativo, para impedir que os usuários executem tarefas que alterem configurações sensíveis do ambiente, a fim de reduzir o número de chamadas de suporte.	• *Autorização robusta: https://br.enterpriseopen.com/workspace/features/robust-authorization/*
2.4.17.	**A solução deve possuir suporte a mecanismos de controle como Política de Segurança de Conteúdo ou Content Security Policy (CSP) contra vulnerabilidades que possam levar ao**	
2.4.18.	comprometimento de dados ou da experiência do usuário, incluindo bloqueio de ataques de injeção de dados, Cross-Site Scripting (XSS).	• *Content Security Policy: https://br.enterpriseopen.com/workspace/features/content-security-policy/*
2.4.19.	A solução deve permitir a utilização em servidores de plataformas SIEM (Informações de segurança e gerenciamento de eventos).	• *Recursos avançados de integração: https://br.enterpriseopen.com/workspace/features/sdk-de-integracao/*
2.4.20.	A solução deve possibilitar o balanceamento de carga em diversos locais geograficamente distintos, em vários data centers, para usuários e configurações variadas.	• *Balanceador de carga geográfico: https://br.enterpriseopen.com/workspace/features/dsm-advanced-load-balancing/*
2.4.21.	A solução deve permitir o redirecionamento das unidades locais no dispositivo do usuário para serem utilizadas pelos aplicativos publicados, evitando assim etapas intermediárias para operações de cópia de arquivos ou configuração de serviços ou infraestrutura adicionais.	• *Redirecionamento de recursos: https://br.enterpriseopen.com/workspace/features/advanced-customizable-redirection/* • *Gestão de impressão avançada: https://br.enterpriseopen.com/workspace/features/advanced-printing/*
2.4.22.	A solução deve garantir a capacidade de configurar scripts para serem executados no momento do login do usuário, independentemente dos aplicativos publicados, e com suporte a vários sistemas operacionais.	• *2.1.20. Configuration > Login Scripts: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.4.23.	A solução deve ser capaz de montar automaticamente compartilhamentos de arquivos nos servidores de aplicativos, baseando-se nos compartilhamentos configurados no dispositivo do usuário.	• *5 - Compartilhamento de diretórios externos: Evidencias complementares.pdf* • *2.1.2. Infrastructure > Storage: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.4.24.	A solução deve permitir que os usuários mantenham arquivos e configurações entre as sessões, em diferentes servidores de aplicativos com diferentes sistemas operacionais.	• *5 - Compartilhamento de diretórios externos: Evidencias complementares.pdf* • *2.1.2. Infrastructure > Storage: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.4.25.	A solução deve permitir a criação de pastas compartilhadas, possibilitando que os usuários compartilhem arquivos entre diferentes servidores de aplicativos com diferentes sistemas operacionais.	• *5 - Compartilhamento de diretórios externos: Evidencias complementares.pdf* • *2.1.2. Infrastructure > Storage: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.4.26.	A solução deve permitir a personalização de vários aspectos da aplicação cliente por meio do uso de opções de linha de comando.	• *Publicação customizável de aplicações estáticas e Web: https://enterpriseopen.com/workspace/wp-content/uploads/EOW-Showcase-Web-Applications-01-Fast-Recode.mp4*
2.4.27.	A solução deve garantir que o fluxo de trabalho, a experiência do usuário e a aparência sejam uniformes entre diferentes clientes (Web, Nativo, Mobile) e plataformas (Linux, macOS, Windows, iOS, Android).	• *Ambinetente unificado: https://br.enterpriseopen.com/workspace/features/unified-application-environment/* • *Integração local: https://br.enterpriseopen.com/workspace/features/local-environment-integration/* • *Múltiplataforma: https://br.enterpriseopen.com/workspace/features/linux-application-streaming/* • *Múltigeracional: https://br.enterpriseopen.com/workspace/features/cross-platform-and-cross-generation/* • *Interoperável: https://br.enterpriseopen.com/workspace/descarregar/*
2.4.28.	A solução deve permitir uma fácil configuração da distribuição de aplicativos e recursos de computação para os usuários finais, baseando-se em regras (publicações) simples.	• *2.1.9. Applications > Publications: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.4.29.	A solução deve prover uma configuração na qual nenhum ajuste é necessário pelo usuário; somente o nome do servidor e as credenciais são necessários.	• *Entrega ágil: https://br.enterpriseopen.com/workspace/features/user-zero-configuration/*
2.4.30.	A solução deve permitir que os usuários acessem aplicativos de qualquer dispositivo e em qualquer local, tanto internamente ao PRODERJ quanto remotamente pela Internet.	• *Bring Your Own Device (BYOD): https://br.enterpriseopen.com/workspace/features/bring-your-own-device/*
2.4.31.	A solução deve permitir o uso de atalhos/lançadores locais para as aplicações remotas.	• *Integração local: https://br.enterpriseopen.com/workspace/features/local-environment-integration/*

2.4.32.	A solução deve permitir a execução de aplicativos em diferentes plataformas e sistemas operacionais (Windows e Linux), bem como em várias versões de sistema operacional (Windows Server 2012R2, 2016, 2019, Windows 10 ENT Multi-Session ou RHEL/CentOS 7, 8).	• *Ambinetente unificado: https://br.enterpriseopen.com/workspace/features/unified-application-environment/* • *Integração local: https://br.enterpriseopen.com/workspace/features/local-environment-integration/* • *Múltiplataforma: https://br.enterpriseopen.com/workspace/features/linux-application-streaming/* • *Múltigeracional: https://br.enterpriseopen.com/workspace/features/cross-platform-and-cross-generation/* • *Interoperável: https://br.enterpriseopen.com/workspace/descarregar/*
2.4.33.	A solução deve entregar todos os aplicativos publicados (sejam eles para Windows ou Linux) por meio de uma mesma interface unificada.	• *Ambinetente unificado: https://br.enterpriseopen.com/workspace/features/unified-application-environment/* • *Integração local: https://br.enterpriseopen.com/workspace/features/local-environment-integration/* • *Múltiplataforma: https://br.enterpriseopen.com/workspace/features/linux-application-streaming/* • *Múltigeracional: https://br.enterpriseopen.com/workspace/features/cross-platform-and-cross-generation/* • *Interoperável: https://br.enterpriseopen.com/workspace/descarregar/*
2.4.34.	A solução deve permitir o redirecionamento do áudio de aplicativos publicados para o dispositivo do usuário e redirecionar os dispositivos de entrada de áudio (microfones) para os aplicativos remotos.	• *Redirecionamento de recursos: https://br.enterpriseopen.com/workspace/features/advanced-customizable-redirection/* • *Gestão de impressão avançada: https://br.enterpriseopen.com/workspace/features/advanced-printing/*
2.4.35.	A solução deve prover o redirecionamento das impressoras locais acessíveis pelo dispositivo do usuário para serem utilizadas pelos aplicativos publicados remotamente.	• Redirecionamento de recursos: https://br.enterpriseopen.com/workspace/features/advanced-customizable-redirection/ • Gestão de impressão avançada: https://br.enterpriseopen.com/workspace/features/advanced-printing/
2.4.36.	A solução deve prover o redirecionamento dos leitores de smartcard conectados ao dispositivo do usuário para serem utilizados pelos aplicativos remotos publicados.	• *Redirecionamento de recursos: https://br.enterpriseopen.com/workspace/features/advanced-customizable-redirection/* • *Gestão de impressão avançada: https://br.enterpriseopen.com/workspace/features/advanced-printing/*
2.4.37.	A solução deve prover a integração da área de transferência local no dispositivo do usuário com os aplicativos publicados.	• *Ambinetente unificado: https://br.enterpriseopen.com/workspace/features/unified-application-environment/* • *Integração local: https://br.enterpriseopen.com/workspace/features/local-environment-integration/* • *Múltiplataforma: https://br.enterpriseopen.com/workspace/features/linux-application-streaming/* • *Múltigeracional: https://br.enterpriseopen.com/workspace/features/cross-platform-and-cross-generation/* • *Interoperável: https://br.enterpriseopen.com/workspace/descarregar/*
2.4.38.	A solução deve prover a apresentação de aplicativos publicados em um ambiente de desktop remoto virtual.	• *Ambinetente unificado: https://br.enterpriseopen.com/workspace/features/unified-application-environment/* • *Integração local: https://br.enterpriseopen.com/workspace/features/local-environment-integration/* • *Múltiplataforma: https://br.enterpriseopen.com/workspace/features/linux-application-streaming/* • *Múltigeracional: https://br.enterpriseopen.com/workspace/features/cross-platform-and-cross-generation/* • *Interoperável: https://br.enterpriseopen.com/workspace/descarregar/*
2.4.39.	**A solução deve prover a apresentação de aplicativos publicados em uma lista, utilizando**	
2.4.40.	uma interface gráfica de usuário mínima.	• *Seamless Applications: https://br.enterpriseopen.com/workspace/features/seamless-applications/*
2.4.41.	A solução deve prover uma aplicação cliente que utilize pouquíssimos recursos no dispositivo do usuário, com baixa sobrecarga de processamento.	• *Eficiência com uso de dispositivos obsoletos ou de baixo custo: https://br.enterpriseopen.com/workspace/features/plug-forget-and-disposable-clients/*
2.4.42.	A solução deve prover clientes resilientes a problemas de conectividade, mantendo uma sessão aberta durante interrupções.	• *4 - Persistência de sessão: Evidencias complementares.pdf*
2.4.43.	A solução deve permitir o acesso aos aplicativos publicados a partir de dispositivos baseados em iOS, como iPhones ou tablets iPad.	• *Ambinetente unificado: https://br.enterpriseopen.com/workspace/features/unified-application-environment/* • *Integração local: https://br.enterpriseopen.com/workspace/features/local-environment-integration/* • *Múltiplataforma: https://br.enterpriseopen.com/workspace/features/linux-application-streaming/* • *Múltigeracional: https://br.enterpriseopen.com/workspace/features/cross-platform-and-cross-generation/* • *Interoperável: https://br.enterpriseopen.com/workspace/descarregar/*
2.4.44.	A solução deve permitir o acesso aos aplicativos publicados a partir de dispositivos baseados no Android, como telefones, phablets ou tablets.	• *Ambinetente unificado: https://br.enterpriseopen.com/workspace/features/unified-application-environment/* • *Integração local: https://br.enterpriseopen.com/workspace/features/local-environment-integration/* • *Múltiplataforma: https://br.enterpriseopen.com/workspace/features/linux-application-streaming/* • *Múltigeracional: https://br.enterpriseopen.com/workspace/features/cross-platform-and-cross-generation/* • *Interoperável: https://br.enterpriseopen.com/workspace/descarregar/*
2.4.45.	A solução deve prover o acesso aos aplicativos publicados utilizando qualquer um dos navegadores da Web suportados (Chrome, Firefox, Edge, Opera).	• *Cliente Web: https://br.enterpriseopen.com/workspace/features/advanced-web-client/*
2.4.46.	A solução deve prover o Cliente Nativo, permitindo que os usuários acessem os aplicativos publicados enquanto desfrutam do mais alto nível de integração com o sistema operacional no dispositivo local.	• *Redirecionamento de recursos: https://br.enterpriseopen.com/workspace/features/advanced-customizable-redirection/* • *Cliente Nativo: https://br.enterpriseopen.com/workspace/features/seamless-applications/* • *ClientOS: https://br.enterpriseopen.com/workspace/features/clientos/*

2.4.47.	A solução deve prover o Cliente Nativo, possibilitando que os usuários acessem os aplicativos publicados enquanto desfrutam do mais alto nível de integração com o sistema operacional no dispositivo local.	• *Redirecionamento de recursos: https://br.enterpriseopen.com/workspace/features/advanced-customizable-redirection/* • *Cliente Nativo: https://br.enterpriseopen.com/workspace/features/seamless-applications/* • *ClientOS: https://br.enterpriseopen.com/workspace/features/clientos/*
2.4.48.	O Cliente Nativo permite que os usuários acessem os aplicativos publicados enquanto aproveitam o mais alto nível de integração com o sistema operacional no dispositivo local.	• *Redirecionamento de recursos: https://br.enterpriseopen.com/workspace/features/advanced-customizable-redirection/* • *Cliente Nativo: https://br.enterpriseopen.com/workspace/features/seamless-applications/* • *ClientOS: https://br.enterpriseopen.com/workspace/features/clientos/*
2.4.49.	A solução deve aproveitar a capacidade de executar aplicativos em dispositivos ChromeOS e integrar essa funcionalidade na variante personalizada do Cliente Nativo.	• *ChromeOS Client: https://br.enterpriseopen.com/workspace/features/chromeos-client/* • *Redirecionamento de recursos: https://br.enterpriseopen.com/workspace/features/advanced-customizable-redirection/* • *Cliente Nativo: https://br.enterpriseopen.com/workspace/features/seamless-applications/* • *ClientOS: https://br.enterpriseopen.com/workspace/features/clientos/*
2.4.50.	A solução deve prover a transmissão dos aplicativos publicados para os dispositivos dos usuários utilizando tecnologias de codec modernas.	• *Codecs modernos: https://br.enterpriseopen.com/workspace/features/high-performance-streaming/*
2.4.51.	A tela da sessão remota e as janelas dos aplicativos publicados são automaticamente redimensionadas para corresponder à resolução local do usuário ou à janela do navegador.	• *Interface dinâmica: https://br.enterpriseopen.com/workspace/features/multi-monitor/*
2.4.52.	A solução deve permitir a publicação dos aplicativos da Web e do PRODERJ lado a lado com todos os outros aplicativos Linux e Windows.	• *Ambinetente unificado: https://br.enterpriseopen.com/workspace/features/unified-application-environment/* • *Integração local: https://br.enterpriseopen.com/workspace/features/local-environment-integration/* • *Múltiplataforma: https://br.enterpriseopen.com/workspace/features/linux-application-streaming/* • *Múltigeracional: https://br.enterpriseopen.com/workspace/features/cross-platform-and-cross-generation/* • *Interoperável: https://br.enterpriseopen.com/workspace/descarregar/*
2.4.53.	A solução deve oferecer implantação flexível, permitindo a escolha do local de hospedagem conforme as necessidades específicas da instituição.	• *Agnóstico à virtualização: https://br.enterpriseopen.com/workspace/features/infrastructure-and-cloud-agnostic/*
2.4.54.	A solução deve permitir habilitar a compatibilidade total de aplicativos e certificação independente do ambiente de execução do usuário final.	• *Redirecionamento de recursos: https://br.enterpriseopen.com/workspace/features/advanced-customizable-redirection/* • *Cliente Nativo: https://br.enterpriseopen.com/workspace/features/seamless-applications/* • *ClientOS: https://br.enterpriseopen.com/workspace/features/clientos/*
2.4.55.	A solução deve permitir a reutilização de hardware antigo ou dispositivos simples de baixo consumo de energia.	• *Eficiência com uso de dispositivos obsoletos ou de baixo custo: https://br.enterpriseopen.com/workspace/features/plug-forget-and-disposable-clients/*
2.4.56.	A solução deve permitir que milhares de usuários trabalhem a partir de um pequeno número de servidores.	• *Consolidação de recursos: https://br.enterpriseopen.com/workspace/features/consolidation-and-optimization/* • *Otimização do uso de recursos: https://br.enterpriseopen.com/workspace/features/lean-server-components/* • *Eficiência com uso de dispositivos obsoletos ou de baixo custo: https://br.enterpriseopen.com/workspace/features/plug-forget-and-disposable-clients/* • *Eficiência com uso de dispositivos externos: https://br.enterpriseopen.com/workspace/features/bring-your-own-device/* • *Eficiência com uso de softwares alternativos: https://br.enterpriseopen.com/workspace/features/supplier-choice*
2.4.57.	A solução deve utilizar a infraestrutura de virtualização existente do PRODERJ, sem comprometer o desempenho ou a estabilidade.	• *Agnóstico à virtualização: https://br.enterpriseopen.com/workspace/features/infrastructure-and-cloud-agnostic/*
2.4.58.	A solução deve permitir a configuração do limite de tempo para as sessões do usuário.	• *6. Tempo limite de sessão: Evidencias complementares.pdf*
2.4.59.	A solução deve permitir saber quais aplicativos são executados, quem tem acesso a eles, bem como quando estão sendo usados ativamente.	• *2.1.11. Status > Sessions - 2.1.14. Status > Summary - EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.4.60.	A solução deve prover a utilização das soluções de armazenamento externo existentes para perfil de usuário ou dados do usuário.	• *5 - Compartilhamento de diretórios externos: Evidencias complementares.pdf* • *2.1.2. Infrastructure > Storage: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.4.61.	A solução deve permitir a simplificação da publicação de aplicativos, permitindo a definição de conjunto de aplicativos relacionados.	• *2.1.9. Applications > Publications: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.4.62.	A solução deve aproveitar os grupos de usuários novos ou existentes em seu domínio do Active Directory para regras de publicação de aplicativos.	• *7. Grupos do Active Directory: Evidencias complementares.pdf* • *Autenticação Centralizada (AD/LADAP/INTERNAL): https://br.enterpriseopen.com/workspace/features/multiple-domains-and-directories/* • *Autorização robusta: https://br.enterpriseopen.com/workspace/features/robust-authorization/* • *Redirecionamento de recursos: https://br.enterpriseopen.com/workspace/features/advanced-customizable-redirection/* • *Gestão de impressão avançada: https://br.enterpriseopen.com/workspace/features/advanced-printing/*

2.4.63.	A solução deve permitir a integração com um domínio LDAP como fonte de recursos.	• 7. Grupos do Active Directory: Evidencias complementares.pdf • Autenticação Centralizada (AD/LADAP/INTERNAL): https://br.enterpriseopen.com/workspace/features/multiple-domains-and-directories/ • Autorização robusta: https://br.enterpriseopen.com/workspace/features/robust-authorization/ • Redirecionamento de recursos: https://br.enterpriseopen.com/workspace/features/advanced-customizable-redirection/ • Gestão de impressão avançada: https://br.enterpriseopen.com/workspace/features/advanced-printing/
2.4.64.	A solução deve prover um painel único para o gerenciamento e controle, permitindo a gestão de todos os aspectos da solução.	• *Admnistração Centralizada: https://br.enterpriseopen.com/workspace/features/delegated-administration/* • *Controle centralizado de dispositivos: https://br.enterpriseopen.com/workspace/features/clientos/* • *Autenticação centralizada: https://br.enterpriseopen.com/workspace/features/advanced-authentication/* • *Controle centralizado: https://br.enterpriseopen.com/workspace/features/robust-authorization/* • *Processamento centralizado: https://br.enterpriseopen.com/workspace/features/seamless-applications/* • *Isolamento físico: https://br.enterpriseopen.com/workspace/features/untrusted-end-device/*
2.4.65.	A solução deve permitir a automação da implantação, instanciação, manutenção e operação de servidores de aplicativos Windows e Linux.	• *Agnóstico à virtualização: https://br.enterpriseopen.com/workspace/features/infrastructure-and-cloud-agnostic/* • *Multpataforma: https://br.enterpriseopen.com/workspace/features/cross-platform-and-cross-generation/* • *Suporte Linux avançado: https://br.enterpriseopen.com/workspace/features/linux-application-streaming/* • *Containerização e encapsulamento: https://br.enterpriseopen.com/workspace/features/application-bubble/*
2.4.66.	A solução deve permitir a definição de regras de balanceamento de carga de sessão entre servidores de aplicativos.	• *8. Balanceamento de carga - Evidencias complementares.pdf*
2.5.	**Requisitos tecnológicos de Arquitetura e Plataforma Tecnológica**	
2.5.1.	A solução a ser implantada deverá suportar os seguintes ambientes computacionais do lado dos servidores de aplicação:	
2.5.2.	Suporte ao sistema operacional Windows, no mínimo, nas versões:	
2.5.2. a)	Windows Server 2016;	• *Suporte Windows Server, Enterprise Linux 8/9 (Red Hat/Rocky/Oracle/Alma) - https://br.enterpriseopen.com/workspace/especificacoes/*
2.5.2. b)	Windows Server 2019;	• *Suporte Windows Server, Enterprise Linux 8/9 (Red Hat/Rocky/Oracle/Alma) - https://br.enterpriseopen.com/workspace/especificacoes/*
2.5.2. c)	Windows Server 2022.	• *Suporte Windows Server, Enterprise Linux 8/9 (Red Hat/Rocky/Oracle/Alma) - https://br.enterpriseopen.com/workspace/especificacoes/*
2.5.3.	Suporte ao Sistema Operacional Linux:	• *Suporte Windows Server, Enterprise Linux 8/9 (Red Hat/Rocky/Oracle/Alma) - https://br.enterpriseopen.com/workspace/especificacoes/*
2.5.3. a)	Red Hat Enterprise 8 ou superior;	• *Suporte Windows Server, Enterprise Linux 8/9 (Red Hat/Rocky/Oracle/Alma) - https://br.enterpriseopen.com/workspace/especificacoes/*
2.5.4.	Os componentes da solução devem poder ser implementados em plataforma de Infraestrutura de Virtualização de mercado ou em servidores físicos, tanto em ambiente on-premises, nuvem ou híbrido.	• *Agnóstico à virtualização: https://br.enterpriseopen.com/workspace/features/infrastructure-and-cloud-agnostic/*
2.5.5.	Caso utilize streaming a solução deve prover o suporte à aceleração por hardware.	• *Streaming de alta performance: https://br.enterpriseopen.com/workspace/features/high-performance-streaming/*
2.5.6.	A solução deve permitir o uso de Servidores de Aplicações baseado no sistema operacional Windows que não estejam, necessariamente, associados a um domínio do Microsoft Active Directory.	• *Multidiretório: https://br.enterpriseopen.com/workspace/features/non-ad-domain-joined/*
2.5.7.	A solução deve possuir recurso de gerenciamento dos seus elementos de forma a possibilitar a manutenção parcial do ambiente sem que haja indisponibilidade dos serviços..	• *Arquitetura modular: https://br.enterpriseopen.com/workspace/features/modular-architecture/* • *Administração Centralizada: https://br.enterpriseopen.com/workspace/features/delegated-administration/* • *Controle centralizado de dispositivos: https://br.enterpriseopen.com/workspace/features/clientos/* • *Controle centralizado: https://br.enterpriseopen.com/workspace/features/robust-authorization/* • *Isolamento físico: https://br.enterpriseopen.com/workspace/features/untrusted-end-device/* • *EO.workspace - Native Client Command-Line Interface.pdf* • *EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.5.8.	A solução possuir funcionalidade de "Scripts de Login", que permita a configuração personalizada de algumas aplicações e regras de segurança, independentemente dos aplicativos por ela publicados, e com suporte, minimamente aos sistemas operacionais Windows e Linux.	• *2.1.20. Configuration > Login Scripts: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.5.9.	A solução deve permitir a publicação de aplicativos por meio do console de administração.	• *2.1.9. Applications > Publications: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.5.10.	O software cliente, desenvolvido pelo fabricante da solução deve permitir que usuários externos possam acessar os conteúdos a partir das seguintes plataformas de mercado:	
2.5.11.	Sistemas operacionais para computadores:	
2.5.11. a)	Microsoft Windows: versão 7 ou superior;	• *Interoperável: https://br.enterpriseopen.com/workspace/descarregar/*
2.5.11. b)	Linux: Red Hat Linux (RHEL) 7 ou superior e Ubuntu 18.04 ou superior;	• *Interoperável: https://br.enterpriseopen.com/workspace/descarregar/*

2.5.11. c)	Ubuntu 18.04 ou superior;	• *Interoperável: https://br.enterpriseopen.com/workspace/descarregar/*
2.5.11. d)	Mac OS: 10.14 ou superior.	• Interoperável: https://br.enterpriseopen.com/workspace/descarregar/
2.5.12.	Aplicativos nativos para tablets e Smartphones:	
2.5.12. a)	Android: versões 7 ou superior;	• *Interoperável: https://br.enterpriseopen.com/workspace/descarregar/*
2.5.12. b)	IOS: versões 13 ou superior.	• *Interoperável: https://br.enterpriseopen.com/workspace/descarregar/*
2.5.13.	O acesso a solução através de Navegadores Web deve ser, minimamente, compatível com os seguintes softwares de mercado:	
2.5.13. a)	Microsoft Edge;	• *Cliente Web: https://br.enterpriseopen.com/workspace/features/advanced-web-client/*
2.5.13. b)	Google Chrome.	• *Cliente Web: https://br.enterpriseopen.com/workspace/features/advanced-web-client/*
2.5.14.	A solução deve permitir o acesso otimizado à compartilhamento de Arquivos, permitindo o compartilhamento de unidades de rede por meio da própria aplicação, sem necessidade de políticas de grupo ou configuração de domínio, bem como oferecer o suporte ao uso de unidades de nuvem (interna ou externa) de armazenamento.	• *5 - Compartilhamento de diretórios externos: Evidencias complementares.pdf* • *2.1.2. Infrastructure > Storage: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.5.15.	A solução deve permitir o envio de alertas por e-mail para realizar notificações de eventos do sistema.	• *2.1.15. Configuration > System: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.5.16.	A solução deve permitir o uso modular, possibilitando habilitar somente os servidores e serviços que efetivamente serão necessários para o ambiente do PRODERJ..	• *Arquitetura modular: https://br.enterpriseopen.com/workspace/features/modular-architecture/*
2.5.17.	A solução deve possuir, minimamente, uma API que permita integração e utilização de ferramentas e mecanismos externos ou dispositivos remotos, permitindo que a PRODERJ possa ampliar o escopo de utilização do seu ambiente computacional..	• *Recursos avançados de integração: https://br.enterpriseopen.com/workspace/features/sdk-de-integracao/*
2.5.18.	A solução possuir funcionalidade de Integração Avançada da Infraestrutura de Desktop Virtual (VDI).	• *Advanced VDI: https://br.enterpriseopen.com/workspace/features/advanced-vdi/*
2.6.	**Requisitos tecnológicos de alta disponibilidade**	
2.6.1.	A solução deve ser capaz de distribuir a carga de trabalho baseada em recurso computacional como memória RAM, utilização de CPU, número de sessões, disponibilidade de aplicações, além de balanceamento randômico e entrega arbitrária de um servidor específico para um usuário ou grupo de usuários.	• *8. Balanceamento de carga - Evidencias complementares.pdf*
2.6.2.	A solução deve obrigatoriamente ser capaz de permitir a redundância de ambientes computacionais (sítios), independente da sua localização, nuvem, on-premisses, de forma ativo-ativo, sem a necessidade de ferramentas de terceiros.	• *Balenceador geográfico: https://br.enterpriseopen.com/workspace/features/dsm-advanced-load-balancing/*
2.6.3.	A solução deve possuir capacidade de tolerância a falhas (HA – High Availability ou Alta- Disponibilidade), permitindo a reconexão dos usuários às suas sessões e do acesso do administrador à Console de Administração da solução em caso de falha de algum servidor individual ou dos dispositivos de acesso dos usuários.	• 2.1.1. Infrastructure > Servers: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf
2.6.4.	A solução deve permitir a Autenticação Federada, com o uso de protocolos (Oauth2 ou OpenID connect) para delegar autenticação de usuário administrativos.	• *Single Sign-On (SSO): https://br.enterpriseopen.com/workspace/features/advanced-authentication/* • *Autenticação Multi Fator: https://br.enterpriseopen.com/workspace/features/integrated-multi-factor-authentication/* • *Autenticação Centralizada (AD/LADAP/INTERNAL): https://br.enterpriseopen.com/workspace/features/multiple-domains-and-directories/*
2.7.	**Requisitos tecnológicos de Atendimento a Conformidades Legais**	
2.7.1.	A solução, respeitando as diretrizes da LGPD, deve proporcionar Direito ao Esquecimento (Eliminação de Dados de usuário) e a emissão de relatórios respeitando a Anonimização dos Dados dos usuários que utilizam a plataforma.	• *Recursos de proteção de dados (GDPR/LGPD): https://br.enterpriseopen.com/workspace/features/right-to-forget/*
2.7.2.	**Requisitos tecnológicos de Administração e Console da Solução**	
2.7.3.	A solução deve prover um console de administração gráfico que permita o gerenciamento da solução e seus componentes, de forma segura, através de computadores convencionais, sem a necessidade de equipamentos específicos, instaladores, plugins ou extensões adicionais que possam gerar dependência ou obsolescência prematura da solução.	• *Admnistração Centralizada: https://br.enterpriseopen.com/workspace/features/delegated-administration/* • *Controle centralizado de dispositivos: https://br.enterpriseopen.com/workspace/features/clientos/* • *Autenticação centralizada: https://br.enterpriseopen.com/workspace/features/advanced-authentication/* • *Controle centralizado: https://br.enterpriseopen.com/workspace/features/robust-authorization/* • *Processamento centralizado: https://br.enterpriseopen.com/workspace/features/seamless-applications/* • *Isolamento físico: https://br.enterpriseopen.com/workspace/features/untrusted-end-device/*

2.7.4.	A solução deve possuir um console administrativo deve ser centralizado, com delegação administrativa granular, que permita a criação de diferentes perfis administrativos, contemplando relatórios de históricos (de uso, estatísticas de sistema, estatísticas de acesso, permissão, autorização dentre outros), com exibição de informações em tempo real.	• *Entrega ágil: https://br.enterpriseopen.com/workspace/features/user-zero-configuration/* • *Controle administrativo granular: https://br.enterpriseopen.com/workspace/features/delegated-administration/*
2.7.5.	A solução deve permitir, via Console Administrativo, que o controle de entrada e saída (download e upload) de arquivos seja configurado dentro das políticas de segurança estabelecidas pelo PRODERJ.	• *9. Redirecionamento de drives, diretórios e multimídia - Evidencias complementares.pdf*
2.7.6.	A solução permitir a utilização de recursos de assistência remota nos sistemas operacionais envolvidos.	• *Assistência remota: https://br.enterpriseopen.com/workspace/features/session-shadowing/*
2.7.7.	A solução deve permitir delegar funções administrativas específicas a usuários ou grupos específicos, como agentes de “service desk” ou equipes de TI específicas. A solução deve permitir a configuração de equipes com acesso somente leitura.	• *Controle administrativo granular: https://br.enterpriseopen.com/workspace/features/delegated-administration/*
2.7.8.	A solução deve por meio do seu console de administração, customizar a personalização do uso de imagem do PRODERJ em seus diversos aspectos fundamentais:	
2.7.8.1.	Nome, logotipos, cores (primárias, secundária) e legendas, propagadas automaticamente para todas as interfaces do ambiente de trabalho centralizado sem a necessidade de intervenção local compilação de pacotes ou qualquer outra atividade que não possa ser gerenciada diretamente pela solução.	• *Customização de identidade visual: https://br.enterpriseopen.com/workspace/features/pervasive-branding/*
2.7.9.	A solução deve, via Console Administrativo, permitir que as aplicações sejam disponibilizadas aos usuários e grupos de usuários, em dias e horas específicos através de uma agenda configurável pelos gestores do PRODERJ.	• *3. Restrições de horário - Evidencias complementares.pdf*
2.7.10.	A solução possuir a funcionalidade de monitoramento do estado de atualização do produto, e de seus componentes, sinalizando aos administradores que há atualizações disponíveis, incluindo atualizações dos sistemas operacionais envolvidos.	• *Gerenciamento de atualizações: https://br.enterpriseopen.com/workspace/features/update-management/*
2.7.11.	A solução deve permitir o controle centralizado com funcionalidades de Administração e Gestão, possuindo minimamente as seguintes funcionalidades:	
2.7.11. a)	Dashboard informativo do status dos servidores, sessões e recursos em tempo real, sendo minimamente: número de sessões registradas e desconectadas, motivo da desconexão, eventos de segurança, estatísticas (aplicações, usuários, servidores, grupos e outros) e histórico de sessões, incluindo ajustes de período;	• *2.1. Administration console > 2.1.10. Reporting - EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.7.11. b)	Gestão dos servidores virtualizados, provendo informações do sistema operacional e sua versão, recurso computacional, percentual de uso (memória e processador), status (online, offline, manutenção);	• *Console administrativo: https://enterpriseopen.com/workspace/wp-content/uploads/EOW-Showcase-Modular-Architecture-01-Fast-Recode.mp4*
2.7.11. c)	Gerenciamento de usuários, grupos de usuários e perfis;	• *7. Grupos do Active Directory: Evidencias complementares.pdf* • *Autenticação Centralizada (AD/LADAP/INTERNAL): https://br.enterpriseopen.com/workspace/features/multiple-domains-and-directories/* • *Autorização robusta: https://br.enterpriseopen.com/workspace/features/robust-authorization/* • *Redirecionamento de recursos: https://br.enterpriseopen.com/workspace/features/advanced-customizable-redirection/* • *Gestão de impressão avançada: https://br.enterpriseopen.com/workspace/features/advanced-printing/*
2.7.11. d)	Agrupamento de servidores (pools) com associação de usuários e usuários;	• *2.1.1. Infrastructure > Servers: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.7.11. e)	Configuração de scripts de login, para serem executados no momento da autenticação do usuário;	• *2.1.20. Configuration > Login Scripts: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.7.11. f)	Configuração de tipos MIME que associa um tipo de documento a uma aplicação específica;	• *2.1.7. Applications > Applications: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.7.11. g)	Gerenciamento de sessões ativas;	• *2.1.11. Status > Sessions - 2.1.14. Status > Summary - EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.7.11. h)	Acesso aos logs do sistema e seus componentes;	• *2.1.12. Status > Logs: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*
2.7.11. i)	Gerenciamento de notificações;	• *1. Aviso pop-up: Evidencias complementares.pdf* • *2.1.19. Configuration > News: EOKB-EO.workspace-OperationandAdministration-170724-1939-94.pdf*

2.8.	Requisitos de Segurança e Privacidade	
2.8.1.	**São requisitos exigidos para CONTRATADA com relação a sigilo e segurança da informação:**	
2.8.1. a)	Obedecer aos critérios, padrões, normas e procedimentos operacionais adotados pelo PRODERJ;	*Requisito de prestação de serviço*
2.8.1. b)	Manter sigilo, sob pena de responsabilidades civis, penais e administrativas, sobre todo e qualquer assunto de interesse do PRODERJ ou de terceiros de que tomar conhecimento em razão da execução do objeto deste Contrato devendo orientar seus empregados nesse sentido;	*Requisito de prestação de serviço*
2.8.1. c)	Promover o afastamento, no prazo máximo de 24 (vinte e quatro) horas após o recebimento da notificação, de qualquer dos seus funcionários que não correspondam aos critérios de confiança ou que perturbe a ação da equipe de fiscalização do PRODERJ;	*Requisito de prestação de serviço*
2.8.1. d)	Não veicular publicidade acerca dos serviços contratados, sem prévia autorização, por escrito, do PRODERJ;	*Requisito de prestação de serviço*
2.28.6. a)	O aceite (recebimento definitivo) da instalação dos softwares ou codigos convertidos serão dados após a confirmação de operação estável por 30 (trinta) dias corridos. Considera-se “operação estável”, a visualização pela equipe técnica do CONTRATANTE de “status” normal por meio de canal a ser definido;	*Requisito de prestação de serviço*
2.28.6. b)	A CONTRATADA deverá informar tão logo seja assinado o contrato, todos os pré- requisitos de servidores e sistemas operacionais necessários para o pleno funcionamento da solução;	*Requisito de prestação de serviço*
2.28.6. c)	A CONTRATADA deverá emitir parecer validando que os ambientes solicitados estão de acordo com os requerimentos para início dos trabalhos de instalação e configuração;	*Requisito de prestação de serviço*
2.28.6. d)	Dinâmica de capacitação; e	*Requisito de prestação de serviço*
2.28.6. e)	Definição de prazos de atendimento para as atividades previstas no Catálogo de Serviços.	*Requisito de prestação de serviço*
2.28.7.	A licitante vencedora deverá informar todas as necessidades de adequação do ambiente computacional para a implantação da solução dentro do plano de implementação, conforme descrito;	*Requisito de prestação de serviço*
2.28.8.	A execução do objeto será iniciada a partir da assinatura do contrato, o qual autoriza a licitante vencedora a seguir e cumprir o cronograma de atividades;	*Requisito de prestação de serviço*
2.28.9.	A licitante vencedora deverá garantir a qualidade e a estabilidade do objeto em todas as etapas utilizando as melhores práticas de mercado, de tal forma que a CONTRATANTE tenha uma solução viável do ponto de vista técnico com alto grau de segurança, escalabilidade, usabilidade e desempenho;	*Requisito de prestação de serviço*
2.28.10.	Para a execução da solução a licitante vencedora entregará, para validação da CONTRATANTE, Plano de Implementação Inicial contendo:	*Requisito de prestação de serviço*
2.28.10. a)	Levantamento de Dados: coleta dos dados necessários à elaboração do Planejamento e execução do processo, através de reuniões entre profissionais e especialistas da CONTRATANTE e da CONTRATADA	*Requisito de prestação de serviço*
2.28.10. b)	Plano de Integração: neste documento deverá constar, no mínimo, a arquitetura desenhada pela contratada para a integração na estrutura existente da CONTRATANTE, relativamente aos itens que forem pertinentes	*Requisito de prestação de serviço*
2.28.10. c)	Projeto de Configuração e Parametrização: elaboração da documentação necessária à correta configuração e parametrização do sistema de gerenciamento para garantir a correta operação e funcionalidade da solução no ambiente tecnológico	*Requisito de prestação de serviço*

2.28.10. d)	Plano de Teste: tem como finalidade estabelecer os procedimentos para aceitação em campo das implantações, customizações e parametrizações efetuadas pela CONTRATADA, verificando o correto funcionamento da solução implantada.	*Requisito de prestação de serviço*
2.28.10. I -	A forma de atuação das áreas de implantação e de operações;	*Requisito de prestação de serviço*
2.28.10. II -	Descrição dos testes a serem realizados e respectivos procedimentos de execução;	*Requisito de prestação de serviço*
2.28.10. III -	Critérios para a avaliação dos resultados.	*Requisito de prestação de serviço*
2.28.11.	A equipe técnica da licitante vencedora que irá executar a instalação deverá trabalhar sob a orientação e supervisão direta do profissional responsável pela coordenação das atividades de implantação (Gerente de Projeto) e com acompanhamento do profissional técnico indicado pela CONTRATANTE;	*Requisito de prestação de serviço*
2.28.12.	Caberá ao Gerente de Projeto coordenar e orientar todo o processo de planejamento, fornecimento, instalação, configuração, integração, conversão e testes dos produtos, acompanhando o cumprimento dos prazos e atestando a qualidade dos entregáveis;	*Requisito de prestação de serviço*
2.28.13.	Os Manuais deverão ser apresentadas em meio digital (por opção do CONTRATANTE pode ser por meio impresso em folha A4). Este será considerado como efetivamente entregue e aceito somente após a validação pela Comissão de Fiscalização do CONTRATANTE;	*Requisito de prestação de serviço*
2.28.14.	Os Manuais, digitais ou impressos, deverão ser emitidos utilizando a logomarca da licitante vencedora;	*Requisito de prestação de serviço*
2.28.15.	Qualquer alteração no corpo técnico ou gerencial da licitante vencedora não poderá afetar o cronograma de entrega nem a execução do Plano de Trabalho.	*Requisito de prestação de serviço*
2.28.16.	O pagamento estará condicionado à entrega das licenças dos softwares e a prestação do serviços, que deverá ser precedido de um Plano de trabalho para abertura de Ordem de Serviço (OS) contendo ao menos: nome do software/serviço, descrição detalhada do serviço, atividades e entregáveis, esforço aplicado na execução, complexidade da atividade, perfil profissional adequado para a execução, quantidade unitária de UST, prazo e quantitativo estimado de UST para a execução do serviço e valor monetário de cada serviço.	*Requisito de prestação de serviço*
2.28.17.	A especificação completa dos Serviços Técnico Especializado foi abordada via – Anexo III Catálogo de Serviços.	*Requisito de prestação de serviço*
2.29.	Requisitos de Experiência Profissional e Formação da Equipe	*Requisito de prestação de serviço*
2.29.1.	Caberá à CONTRATADA indicar e comprovar a capacitação, realizada junto aos fabricantes, ou por entidade devidamente registrada junto ao fabricante, dos membros das equipes envolvidas no projeto.	*Requisito de prestação de serviço*