# Enterprise Connect Passwordless Management Console Admin Guide

Version 6.8

## Table of Contents

# Welcome to the Enterprise Connect Passwordless Management Console

This document describes the user interface of the Management Console and how to work with it. Individual topics can be used as an overview of the system for management and non-technical staff.

To get started, refer to the following sections:

- Accessing the Management Console
- Management Console Features Overview

**Solution Overview**

The Authentication Server can be configured to work with various methods of authentication, such as use of a mobile app, FIDO, OTP and more. Once the authentication is verified, the user is authenticated. The Authentication Server can then provide attestations to relying parties for the user's identity.

The Authentication Server is typically deployed on the enterprise domain, where it is configured to access the directory service and to work with relying parties that are either on-premise or SaaS. Connecting to the directory service allows the administrator to assign authentication methods to users and define authentication policies. Connecting with the relying parties can be done by configuring standard interfaces (e.g., RADIUS, SAML, etc.) or by defining a non-standard interface.

In some cases, the Authentication Server authenticates the user and produces the required attestation for the relying party. In other situations, the Authentication Server may need to also facilitate the exchange of a session secret required by the relying party. For example, legacy systems that are still heavily password-dependent may require that a password be produced. In such cases, the Authentication Server provides a temporary session password that is reset at the end of the session.

The administrator configures the system settings from the Management Console.

**Supported System Components and Versions**

The following tables list supported Linux environments, mobile operating systems and browser versions.

**Supported Linux Environments**

| Linux base OS (64-bit) | Supported Versions |
|---|---|
| Red Hat | 8.2 to 8.10 - Minimal image option<br>9.3 to 9.5- Minimal image option |
| Oracle Linux | 8.3 to 8.10<br>9.3 to 9.5 |
| Rocky Linux | 8.4 to 8.10<br>9.3 to 9.5 |

**Important**

If you are using Linux 9 and the tar command is not pre-installed on your machine, please run the following command **before** installing Octopus Authentication Server:

*yum install tar*

**Supported Mobile Devices**

| Device | Supported Versions |
|---|---|
| Android | Android 11 and higher |
| iOS | iOS 15 and higher |

**Supported Browsers: Management Console UI and User Portal**

| Browser | Supported Versions |
|---|---|
| Chrome | 30 and higher |
| Safari | 13.1.2 and higher |
| Firefox | 25 and higher |
| Edge | 41 and higher |

**Supported Browsers for SAML Authentication**

| Browser | Supported Versions |
|---|---|
| Chrome | 30 and higher |
| Edge | 41 and higher |
| Firefox | 25 and higher |
| Internet Explorer | 11.0 |

## Accessing the Management Console

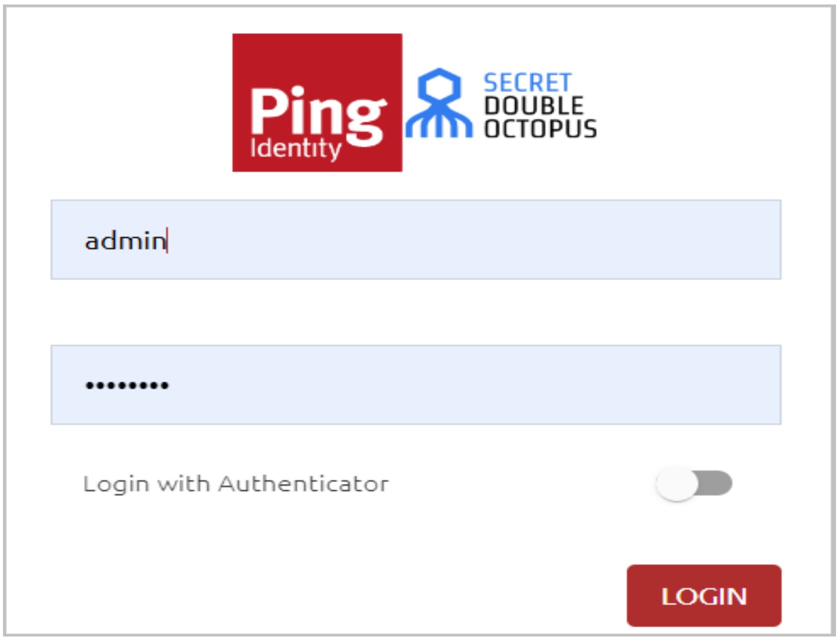
Access the Management Console by entering the base URL and port in your browser (e.g., *https://FQDN:8443*). The first post-installation login must be done using the Super Admin username and password set during installation of the Authentication Server. You can then start to integrate directories, add users and register devices.

**Note**

To access the Management Console, users must be enrolled with the Authentication Server and have a role of **Admin**, **Helpdesk** or **Auditor**.

### Logging In

To access the Management Console, make sure that the **Login with Authenticator** toggle button is inactive. Then, enter your email address and password in the appropriate fields, and click **LOGIN**.

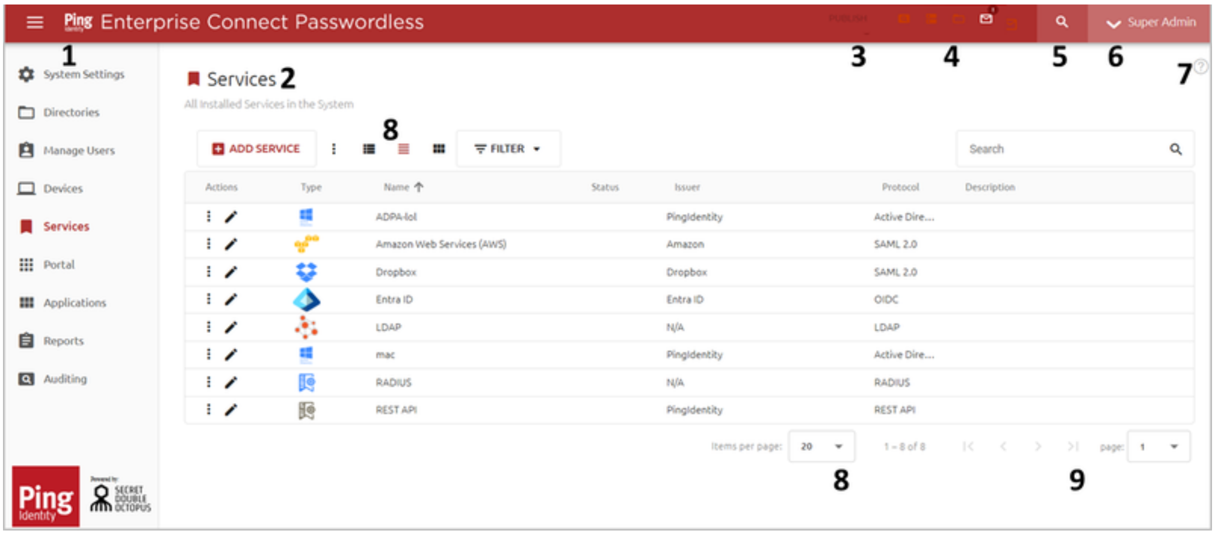


admin

••••••••

## Management Console Features Overview

The main features that appear on most pages of the Management Console are described in the table below the diagram.



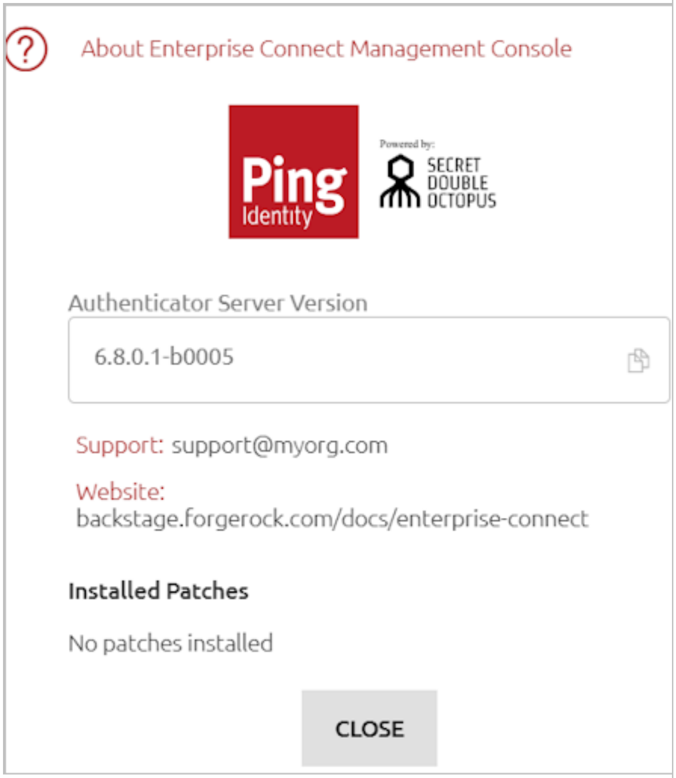
Services

All Installed Services in the System

| Actions | Type | Name | Status | Issuer | Protocol | Description |
|---|---|---|---|---|---|---|
| | | ADPA-lol | | PingIdentity | Active Dire... | |
| | | Amazon Web Services (AWS) | | Amazon | SAML 2.0 | |
| | | Dropbox | | Dropbox | SAML 2.0 | |
| | | Entra ID | | Entra ID | OIDC | |
| | | LDAP | | N/A | LDAP | |
| | | mac | | PingIdentity | Active Dire... | |
| | | RADIUS | | N/A | RADIUS | |
| | | REST API | | PingIdentity | REST API | |

Items per page: 20 1 – 8 of 8 page: 1

| Number | Feature | Description / Notes |
|---|---|---|

| | | |
|---|---|---|
| 1 | Menu bar | Provides access to the various menus of the Management Console. For more information, refer to Menu Bar. |
| 2 | Menu title | Name and description of the currently displayed menu. |
| 3 | Publish button | Shows information about publishing status and provides quick access to the **Publish** dialog. For more details about publishing, refer to Publishing Changes to the Database. |
| 4 | Component Status Information | These icons indicate the connection state and status of various system components. For details, refer to Component Status Icons. |
| 5 | Search by ID tool | Opens the page displaying details about any user, group or workstation in the system. For more information, refer to Using the Search By ID Tool (below). |
| 6 | Username options menu | Click your username to display the following options:<br>- **About:** Opens a popup displaying software version information and support resources. You can copy the current version number to your clipboard by clicking the Copy icon in the **Authentication Server Version** box.<br><br>About Enterprise Connect Management Console<br>Authenticator Server Version<br>6.8.0.1-b0005<br>Support: support@myorg.com<br>Website: backstage.forgerock.com/docs/enterprise-connect<br>Installed Patches<br>No patches installed<br> <br>- **What's New?**: Displays a description of the features introduced in the current version.<br>- **Logout:** Ends your Management Console session. |
| 7 | Help access | Click this icon to open an article describing the current page and how to work with its features. |

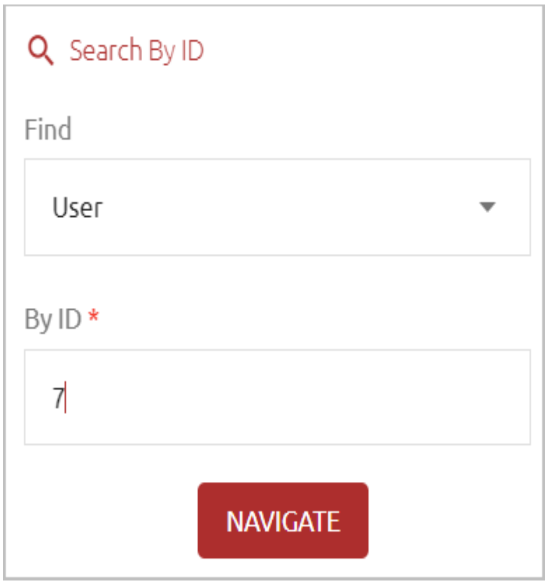
| | | |
|---|---|---|
| 8, 9 | Item presentation and navigation tools | These components, which generally appear on main menu screens, enable you to control the number of items displayed on the page and scroll to other pages of the list. For details, refer to Page Presentation and Navigation Tools. |

### Using the Search By ID Tool

This tool helps administrators easily locate and view details for users or workstations with identified issues, so the issues can be quickly resolved. The unique ID of the user, group or workstation is presented in the Auditing tab as part of the issue summary.

**To use the Search By ID tool:**

1. Click 🔍 to open the **Search by Id** popup.



Search By ID

Find

User

By ID *

7

2. From the **Find** dropdown list, select **User**, **Group** or **Device**.
3. In the **By ID** field, enter the entity's unique ID.
4. Click **Navigate**.

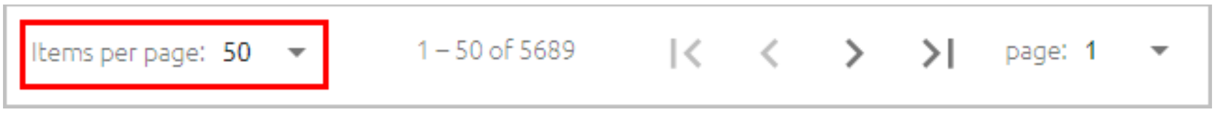
   The Details page for the user, group or workstation is displayed.

### Page Presentation and Navigation Tools

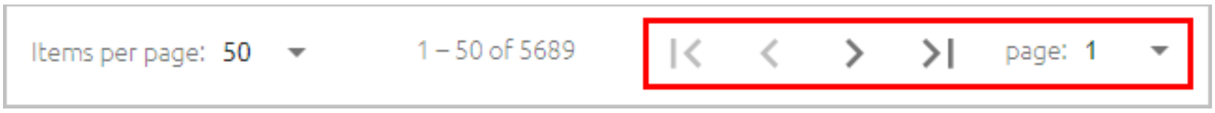
Menus that display lists of many items (such as **Devices**, **Services**, etc.) feature components that allow you to more easily view the list and quickly navigate through multiple-page lists. The icons at the top of these pages enable you to control the display of page content:

- ▦ : Items are presented in separate cards.
- ☰: Items are presented in standard list form, with up to 10 items on a page.
- ≡: Items are presented in compact list form, with up to 20 items on a page.

When items are presented in list view, the **Items per page** feature (at the bottom of the page) allows you to select the number of items displayed on each page of the list (**10**, **20**, **50** or **100**).

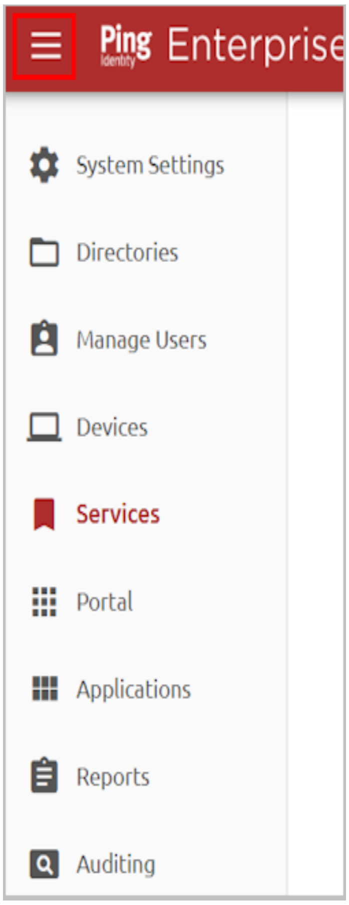


The navigation toolbar at the lower right corner of the page enables you to easily scroll to the next page, previous page, or first / last page of the list. In addition, you can immediately view any page of the list by selecting the page number from the **page** list, at the far right of the navigation toolbar.



**Menu Bar**

The menu bar is located on the left side of the Management Console. It can be collapsed and expanded by clicking the icon at the top of the bar.



The menus are:

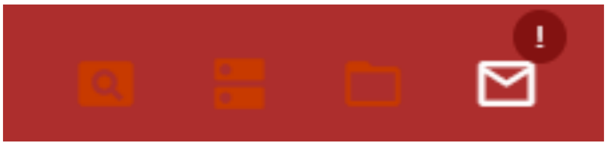
- System Settings: Enable you to view and update system configuration settings, such as authenticators, mail server settings and more.

- Directories: Allows you to integrate corporate directories with the system and configure settings for each directory.
- Manage Users: Lists all users according to their associated directories and enables you to add, remove and perform other administrative actions on users.
- Devices: Lists all workstations in the system, provides detailed information about them and allows you to perform administrative operations on them.
- Services: Lists all services integrated with the Management Console and enables you to add and update services.
- Portal: Allows you to control settings for the User Portal.
- Applications: Enables integration of applications with the Authentication Server and the Windows Agent, so users can access the applications with single sign-on.
- Reports: Provides a variety of out-of-the-box report templates that enable tracking and monitoring of user status, enrollment trends, authentication events, and more.
- Auditing: Displays a log of every administrative action performed by the system or by users.

**Component Status Icons**

The toolbar that appears at the top of every page of the Management Console indicate the current connection and state of important system components. The icons are described in the table below.

When there is an issue involving one of the components that interferes with normal system functioning, the relevant icon is highlighted and a warning icon appears, as shown in the following example.

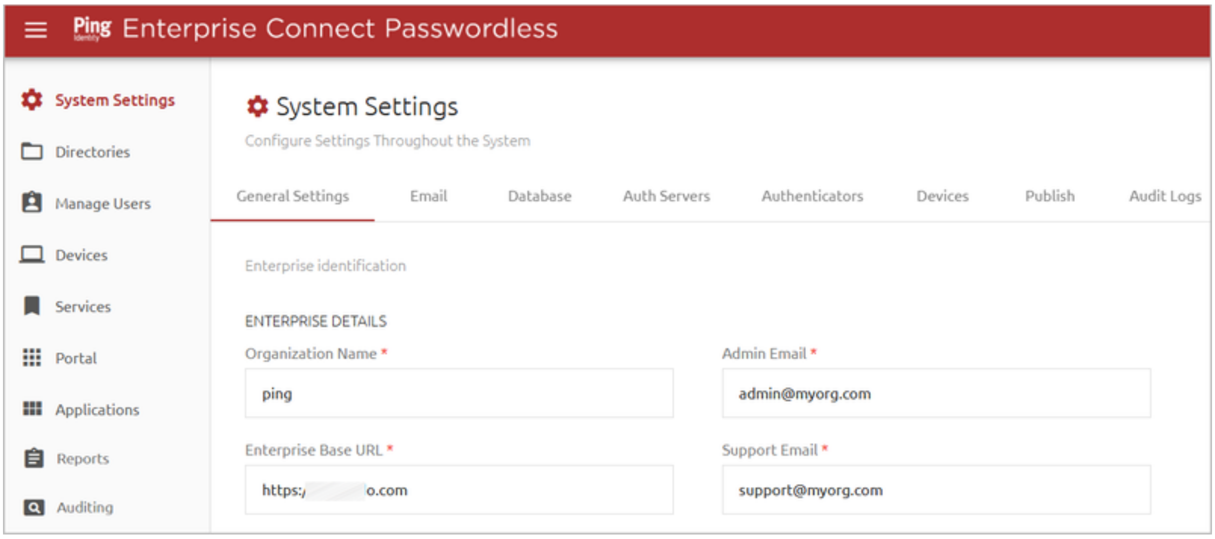


| Icon | Description / Notes |
|---|---|
| 🔍 | Shows the current status of disk usage according to parameters set in the **Audit Logs** tab of the **System Settings** menu. When a warning icon is displayed, click it to view and update log storage settings. For details, refer to Configuring Audit Logs Settings. |
| 🗄 | Indicates connection status of the Authentication Server(s). When a warning icon is displayed, click it to open the Auth Servers tab of the **System Settings** menu, where you can check and verify Server settings. |
| 📁 | Indicates connection status of the integrated directories. When a warning icon is displayed, click it to open the directory settings. |

| Icon | Description / Notes |
|---|---|
| ✉ | Shows connection status of the SMTP server. When a warning icon is displayed, click it to open the Mail Server tab of the **System Settings** menu. |

## Configuring System Settings

The **System Settings** menu contains configuration details for major system components, including authenticators, mail and authentication servers, databases and more. Correct configuration of these settings is essential for successful operation of the platform.



ENTERPRISE DETAILS

Organization Name *: ping

Admin Email *: admin@myorg.com

Enterprise Base URL *: https:/[redacted]o.com

Support Email *: support@myorg.com

The currently selected tab of the **System Settings** menu is indicated by a colored line beneath the tab name. The tabs are:

- General Settings: Contains organization details, license information and timeout parameters for Management Console sessions.
- Email: Sets SMTP server information details and parameters for managing enrollment emails.
- Database: Sets parameters for the database connection to the Management Console.
- Auth Servers: Sets configuration parameters for one or more Authentication Servers.
- Authenticators: Contains a list of integrated authenticators and allows you to add customized third-party authenticators.
- Devices: Contains settings that control handling of communications between the Authentication Server and user workstations.
- Publish: Contains elements and features that manage and control the publishing process.

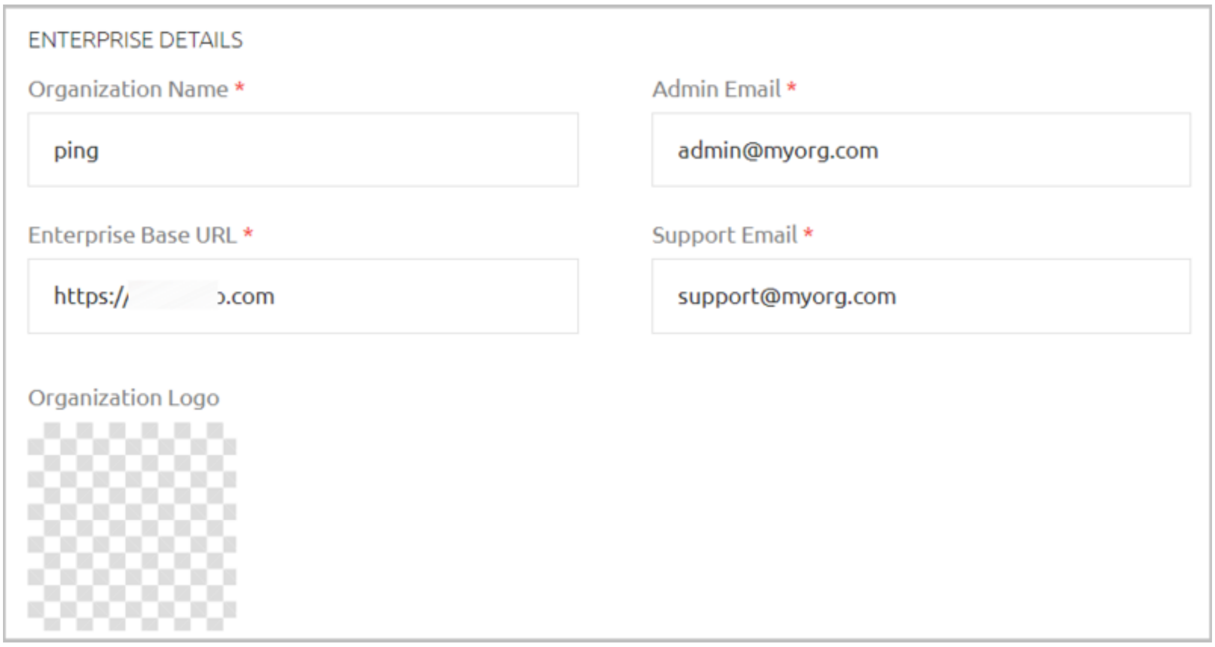
- Audit Logs: Displays data about the amount of accumulated log records and enables configuration of the log retention period.

## General Settings

The **General Settings** tab contains details about your organization and some global parameters related to authentication sessions. To open the tab, select **System Settings > General Settings**.

### Enterprise Details

The settings are described in the table below.



ENTERPRISE DETAILS

Organization Name *
ping

Admin Email *
admin@myorg.com

Enterprise Base URL *
https:/[redacted].com

Support Email *
support@myorg.com

Organization Logo

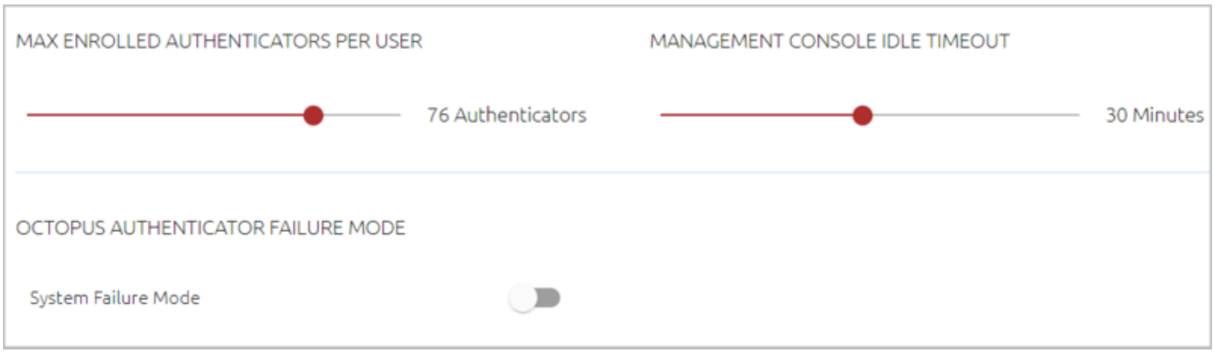
| Setting | Description / Notes |
|---|---|
| Organization Name | The name of your company. By default, the name is the one entered during installation of the Authentication Server.<br>The name specified here is is displayed to users in the authenticator mobile app. |
| Enterprise Base URL | The value should be the address of the Authentication Server or the address of the load balancer (for distributed deployments). This address is used by all services to configure access to the Authentication Server.<br>Note that the field is mandatory - the system cannot function without this value. |
| Organization Logo | This logo is displayed to users in the authenticator mobile app. By default, the setting is empty. To upload a logo, hover over the area, click **Upload File** and select the PNG or JPG file of your choice. Supported image size is 128x128 pixels. |

| Setting | Description / Notes |
|---|---|
| Admin Email | The email address associated with your organization's Admin user. Notifications about network issues (e.g., an offline server) will be sent to this address. |
| Support Email | The email address to which requests for technical assistance should be sent. |

You may update any of the Enterprise Details settings at any time. Always click **Save** (at the bottom of the page) after editing the parameters.

**Authenticator Limit, MC Session Timeout and System Failure Mode**

The lower portion of the **General Settings** tab contains various settings related to authentication sessions.



MAX ENROLLED AUTHENTICATORS PER USER

76 Authenticators

MANAGEMENT CONSOLE IDLE TIMEOUT

30 Minutes

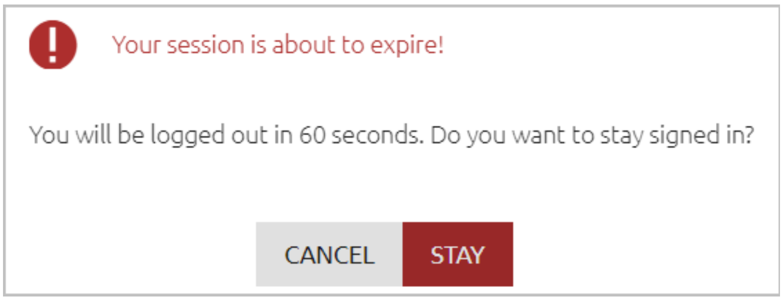
OCTOPUS AUTHENTICATOR FAILURE MODE

System Failure Mode

The settings are:

- **Max Enrolled Authenticators Per User:** The maximum number of authentication devices that can be enrolled in the system for each user. Valid values can range from 1-99. Drag the slider to adjust the value.
- **Management Console Idle Timeout:** The length of time (in minutes) during which no actions are performed in the Management Console before the session is automatically ended. Values can range from 2-60 (default is 10).

  Just before the timeout is reached, a warning popup opens, prompting the user to extend the session. If the user does not respond, the session ends automatically.



Your session is about to expire!

You will be logged out in 60 seconds. Do you want to stay signed in?

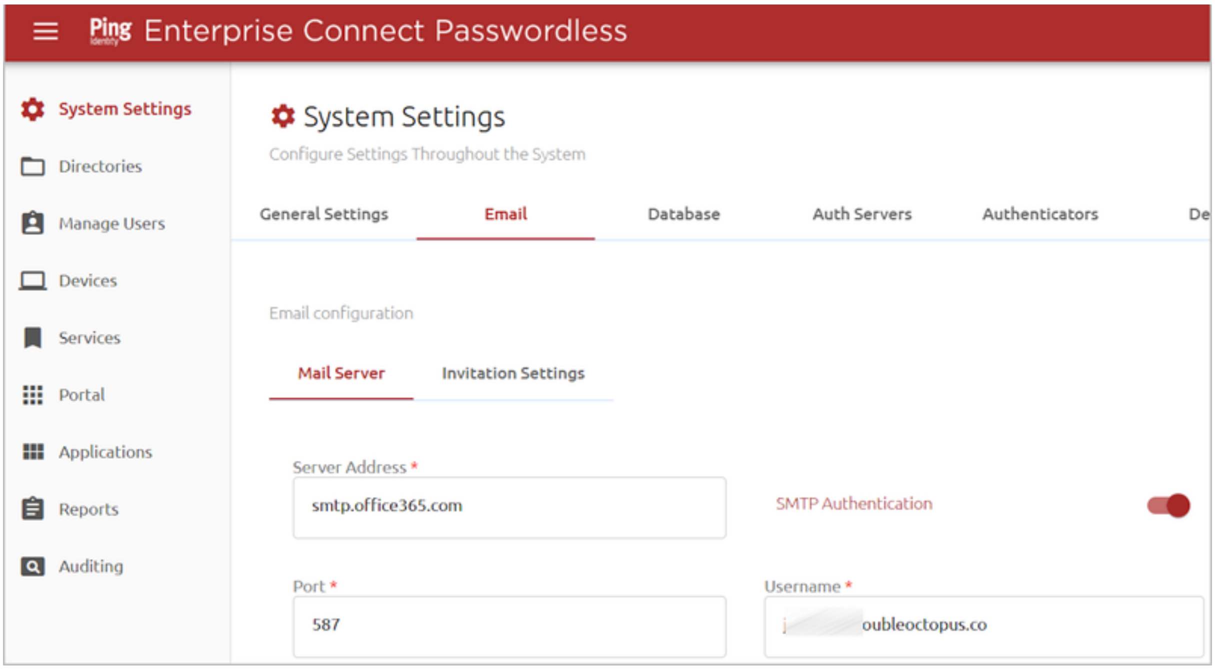
- **Octopus Authenticator Failure Mode:** This setting determines the behavior of the system in situations of network failure or unavailability of the Authentication

Server. When System Failure Mode is enabled, authentication for all services is done with a username and password in the event of system failure.

After updating these settings, click **Save**.

## Email Configuration Settings

The **Email** tab enables you to set up mail server configuration and set the expiration time for invitation (enrollment) emails sent to users. To open the tab, select **System Settings > Email**.



Server Address * smtp.office365.com

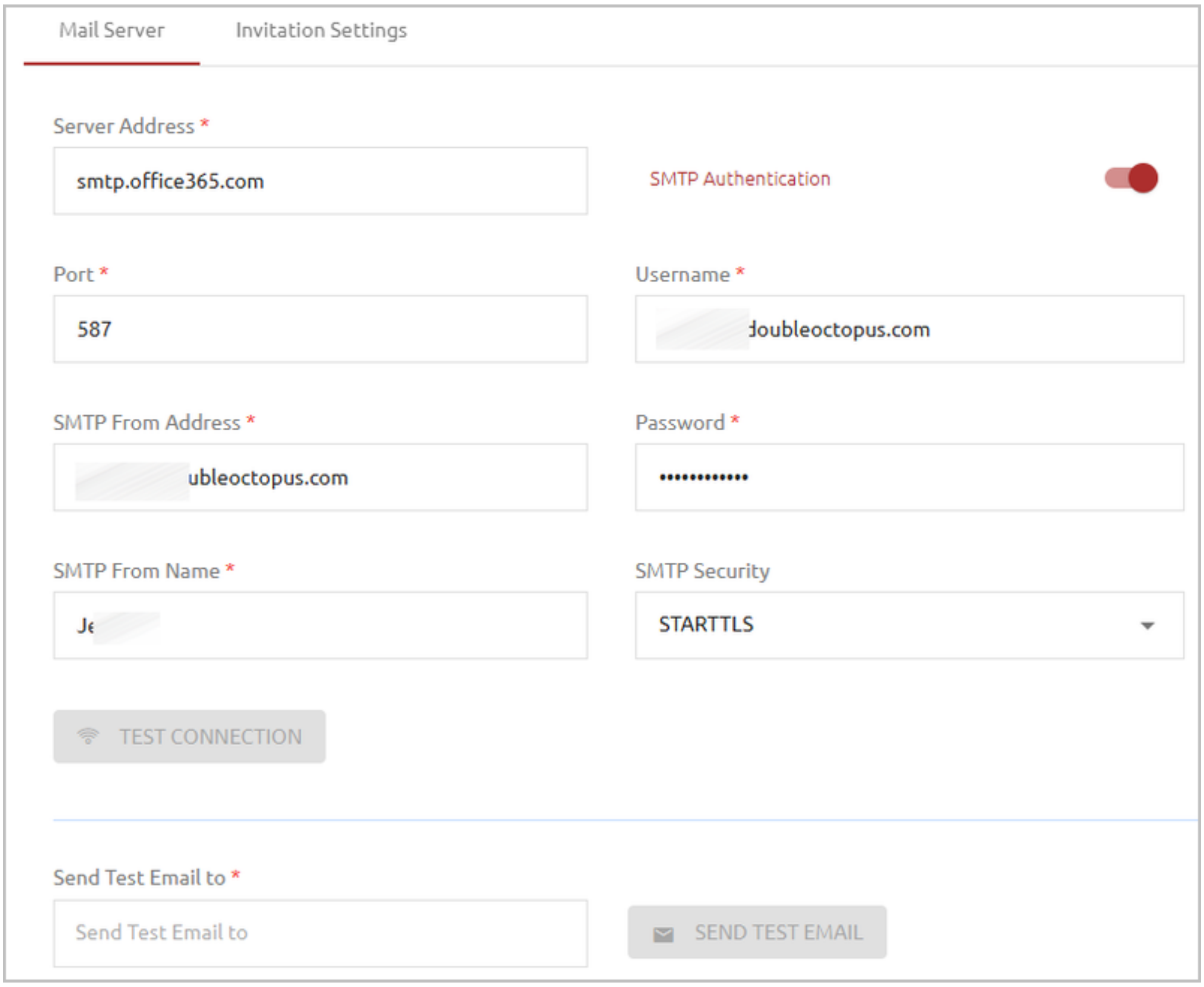
SMTP Authentication ●

Port * 587

Username * j[redacted]oubleoctopus.co

### Configuring Server Details

The **Mail Server** sub-tab contains SMTP server information and other required email parameters.



Server Address * smtp.office365.com

SMTP Authentication

Port * 587

Username * [redacted]doubleoctopus.com

SMTP From Address * [redacted]ubleoctopus.com

Password * ••••••••••••

SMTP From Name * Je[redacted]

SMTP Security STARTTLS

Send Test Email to * Send Test Email to

**To set up SMTP server details:**

1. Enter the following parameters in the appropriate fields:
   - **Server Address:** IP address or hostname of the SMTP server
   - **Port:** Port number for SMTP connection
   - **SMTP From Address:** The From email address that appears in system-generated emails
   - **SMTP From Name:** The name of the sender that appears in system-generated emails
2. Select the appropriate **SMTP Security** method: SSL/TLS or STARTTLS
3. If you want to use SMTP authentication, click the toggle button at the upper right corner of the tab (by default authentication is inactivated), and enter the authentication username and password.
4. Click **Test Connection**.

   Following the test, a confirmation message is displayed at the bottom of the page.

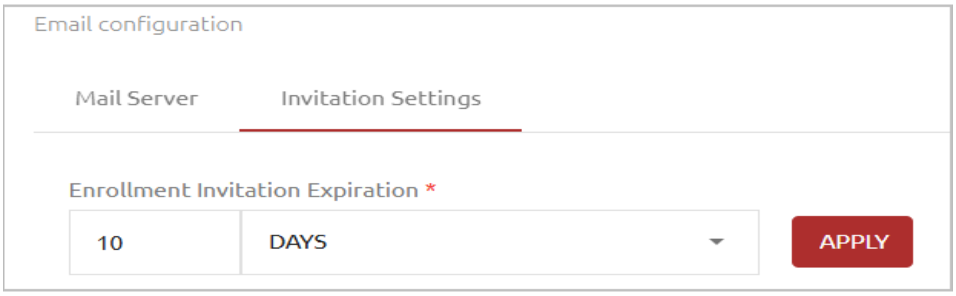
5. In the lower right corner of the page, click **Save**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

6. To verify expected performance, enter a valid email address in the **Send Test Email To** field and click **Send Test Email**. Then, check that an email message was sent and received correctly.

### Setting Enrollment Token Expiration

The **Invitation Settings** sub-tab contains the **Enrollment Invitation Expiration** setting, which determines the maximum period of time for which an invitation email is valid. If a user does not use the invitation to enroll within this time period, the invitation is deleted from the system and a new email needs to be sent.

The **Enrollment Invitation Expiration** can range from 1 hour to 3 weeks (default setting is 3 days). To update the value, specify the desired timeframe and then click **Apply**.



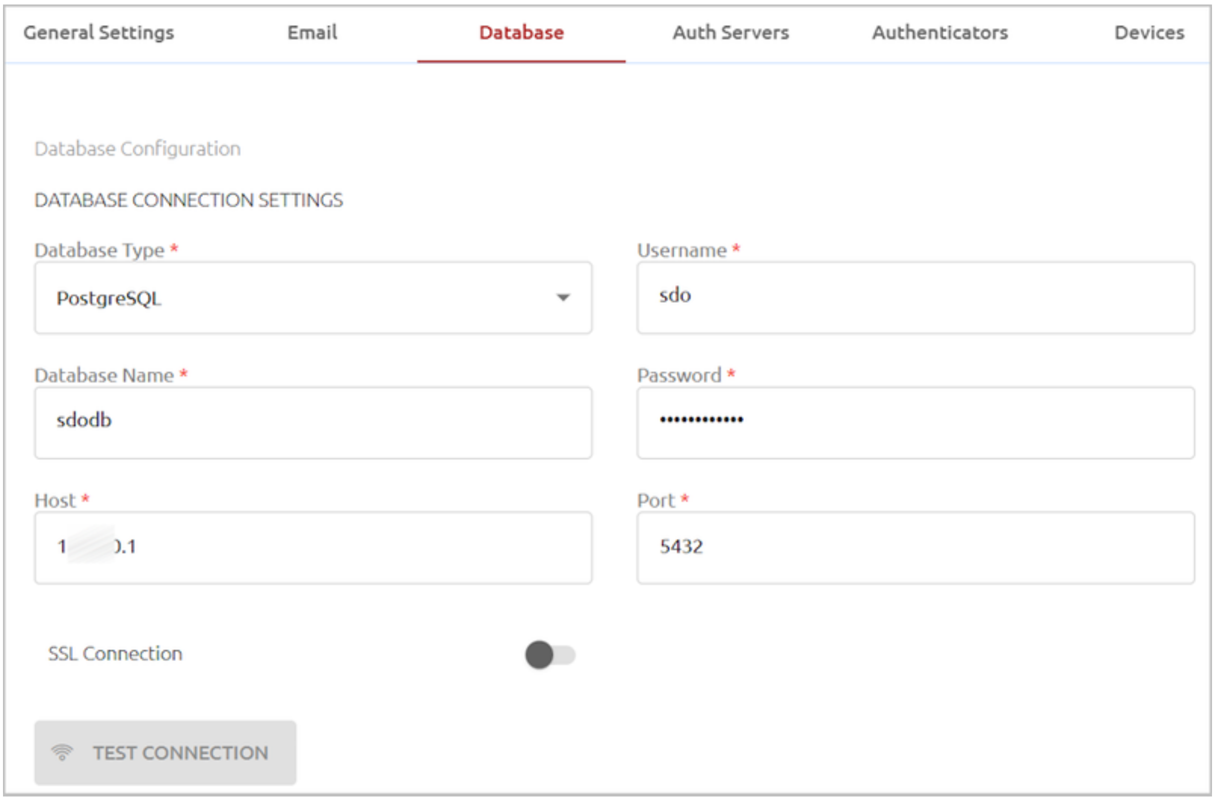
Email configuration

Enrollment Invitation Expiration *: 10 DAYS

## Database Configuration

The database stores all user details and service settings. The **Database** tab of the **System Settings** menu allows you to set and update parameters for the database connection to the Management Console.

When an All-In-One installation is performed, a database is created and initialized as part of the installation. When a different installation type is done, or if the installer chooses not to create the default database, the database connection needs to be created manually from the **Database** tab, as described below.



Database Configuration

DATABASE CONNECTION SETTINGS

Database Type * PostgreSQL

Username * sdo

Database Name * sdodb

Password * ••••••••••••

Host * 1[redacted]).1

Port * 5432

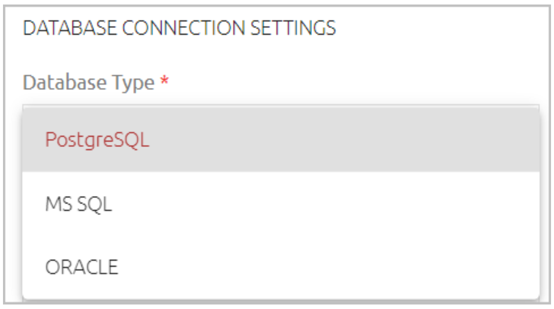
SSL Connection ○

## Configuring Database Settings

The supported database types and versions are listed in the following table. The PostgreSQL type is created automatically as part of the All-In-One installation.

| Database Type | Minimum Version | Maximum Version |
|---|---|---|
| **PostgreSQL** | PostgreSQL 9 | PostgreSQL 15 |
| **MS SQL** | SQL Server 2012 SP4 | SQL Server 2022 |
| **Oracle** | Oracle Database 12c | Oracle Database 19c |

When you set or update database settings, make sure that you specify the database type you are working with by selecting the relevant type from the **Database Type** dropdown list.



**To configure database settings:**

1. At the upper left corner of the **Database** tab, verify that the correct database type (**PostgreSQL**, **MS SQL** or **ORACLE**) is selected from the **Database Type** dropdown list.

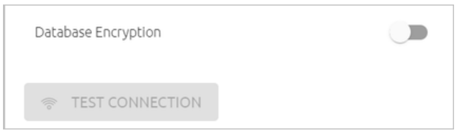
2. Specify the following settings by entering the relevant values in the appropriate fields:

    ○ **Database Name:** Name of the database

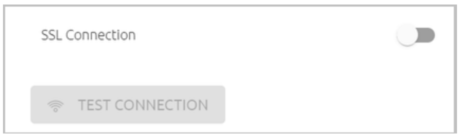
    ○ **Host and Port:** IP address (or URL) and port of the database

    ○ **Username and Password:** Credentials of the database administrator

3. **For MS SQL database types only:** If the connection to the database is encrypted, enable the **Database Encryption** toggle button.



4. **For PostgreSQL database types only:** To enable SSL communication between the Octopus Authentication Server and an external database, enable the **SSL Connection** toggle button.



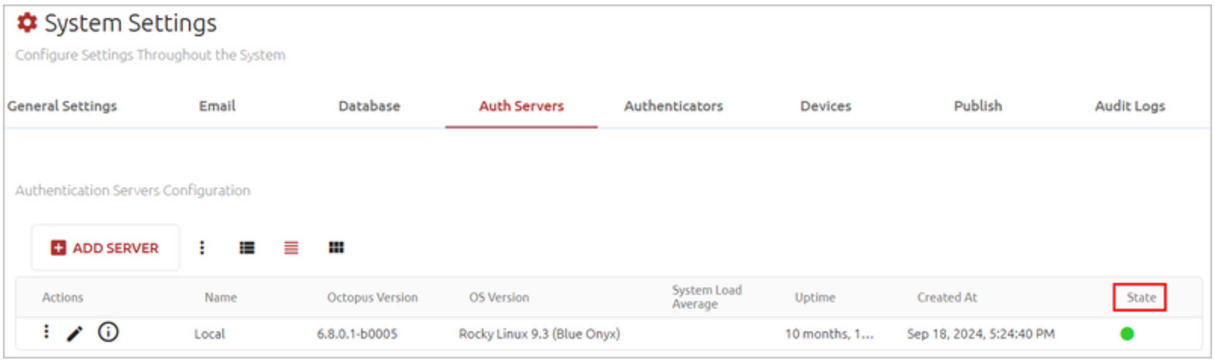
5. To check validity of your settings, click **Test Connection**.

6. To save the settings, click **Save** and then publish your changes.

## Authentication Server Management

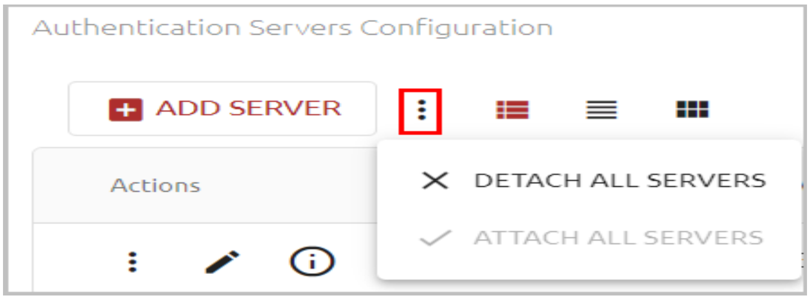
The Management Console can communicate with as many Authentication Servers as your organization requires. To create and maintain the necessary connections, each installed Authentication Server needs to be added to the Management Console.

The **Auth Servers** tab of the **System Settings** menu displays general information about each configured Authentication Server. The **State** indicator (red or green) reflects the Server's current connectivity status.



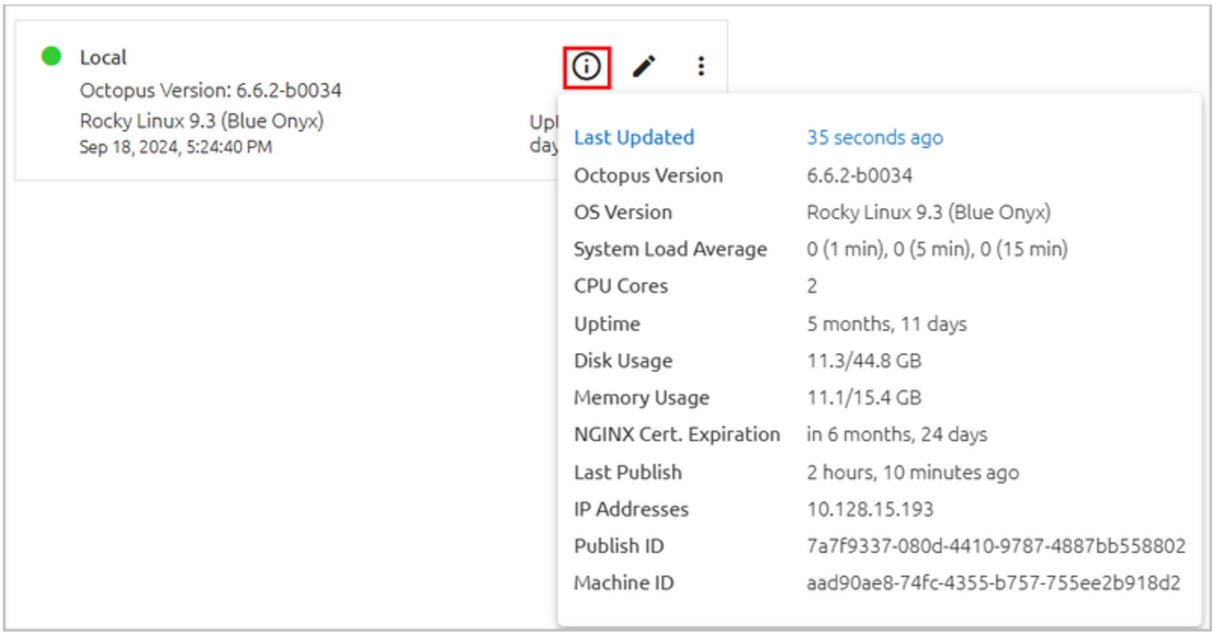
| Actions | Name | Octopus Version | OS Version | System Load Average | Uptime | Created At | State |
|---|---|---|---|---|---|---|---|
| ⋮ ✎ ⓘ | Local | 6.8.0.1-b0005 | Rocky Linux 9.3 (Blue Onyx) | | 10 months, 1... | Sep 18, 2024, 5:24:40 PM | ● |

The Actions icon to the right of the **Add Server** button allows you to detach (and reattach) all Authentication Servers from the Management Console in a single bulk action. This feature lets you easily perform administrative operations, such as system upgrades, without having to delete and recreate each Server.



Clicking ⓘ opens a popup displaying the following additional details about the Authentication Server:

- **Last Updated:** Period of time since the last data update from the server.
- **Octopus Version:** Installed version of the Authentication Server.
- **OS Version:** Server operating system version number.
- **System Load Average:** The average number of tasks waiting to be processed in the run queue. The three values represent averages for the past one, five, and fifteen minutes of system operation.
- **CPU Cores:** Number of CPU cores available on the server.
- **Uptime:** Period of time for which the server has been up and available (since the last restart).
- **Disk Usage:** Amount of disk space used from the total amount of disk space configured for the server.
- **Memory Usage:** Amount of occupied memory from the total amount of memory allocated for the server.
- **NGINX Cert. Expiration:** Period of time remaining until expiration of the certificate. Once the certificate is expired the server will stop working.
- **Last Publish:** Period of time elapsed since the most recent publish on the server.
- **IP Addresses:** IP address of the server.
- **Machine ID:** Random unique identifier for the machine, created during installation.
- **dmz:** If the Authentication Server has a corresponding DMZ Server, data about the DMZ Server is displayed here.



Local

Octopus Version: 6.6.2-b0034

Rocky Linux 9.3 (Blue Onyx)

Sep 18, 2024, 5:24:40 PM

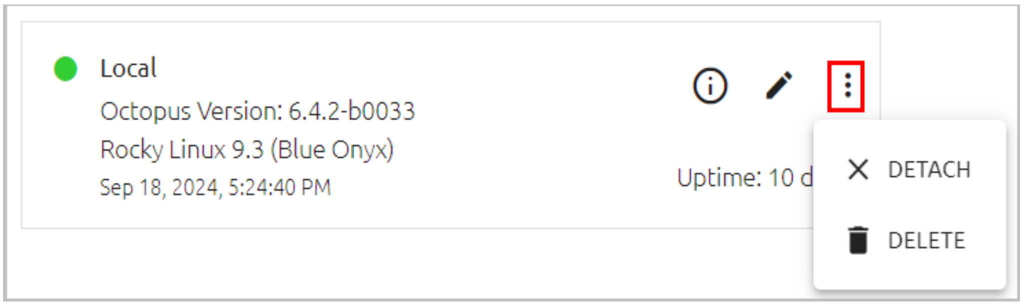
| | |
|---|---|
| Last Updated | 35 seconds ago |
| Octopus Version | 6.6.2-b0034 |
| OS Version | Rocky Linux 9.3 (Blue Onyx) |
| System Load Average | 0 (1 min), 0 (5 min), 0 (15 min) |
| CPU Cores | 2 |
| Uptime | 5 months, 11 days |
| Disk Usage | 11.3/44.8 GB |
| Memory Usage | 11.1/15.4 GB |
| NGINX Cert. Expiration | in 6 months, 24 days |
| Last Publish | 2 hours, 10 minutes ago |
| IP Addresses | 10.128.15.193 |
| Publish ID | 7a7f9337-080d-4410-9787-4887bb558802 |
| Machine ID | aad90ae8-74fc-4355-b757-755ee2b918d2 |

**Important**

It is recommended to regularly monitor the **Disk Usage**, **Memory Usage** and **NGINX Cert. Expiration** values. In the event of full disk space/ memory or certificate expiration, the Authentication Server will stop operating.

Clicking ⋮ in the card or row of an Authentication Server opens an actions menu from which you can perform various operations on the server. The options are:

- **Detach:** Temporarily disconnects the server from the Management Console. While the server is detached, the action changes to **Attach**, allowing you to reconnect the server.
- **Delete:** Allows you to remove an an Authentication Server that is no longer in use.



Local

Octopus Version: 6.4.2-b0033

Rocky Linux 9.3 (Blue Onyx)

Sep 18, 2024, 5:24:40 PM

Uptime: 10 d

### Adding Authentication Servers

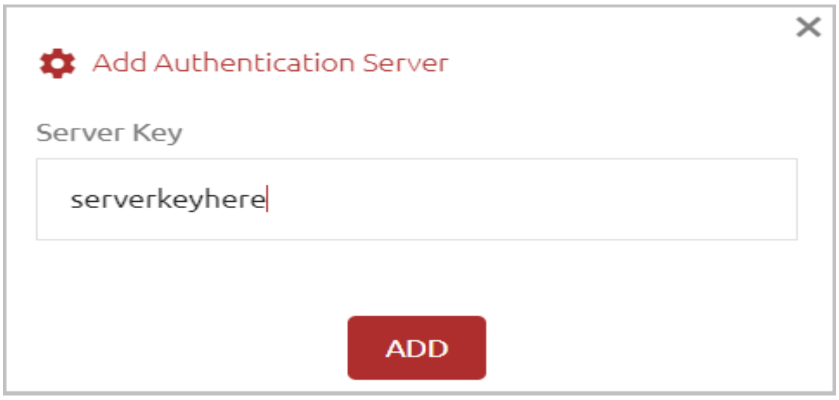
Adding a server to the list of Authentication Servers requires providing the server key to the Management Console.

**To add an Authentication Server:**

1. At the top of the **Auth Servers** tab, click **Add Server**.

The **Add Authentication Server** dialog opens.

2. Paste the server key into the field, and click **Add**.

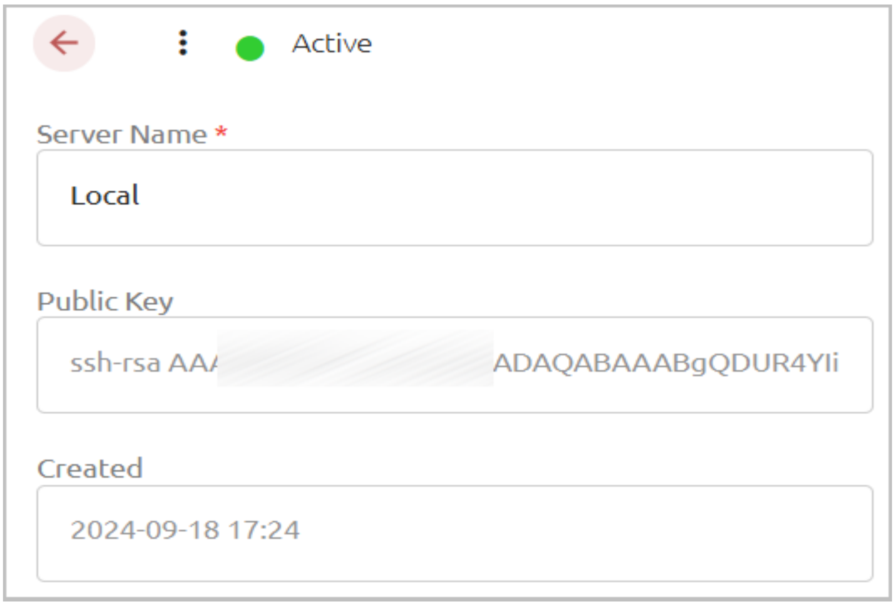


Server Key: serverkeyhere

The server is added to the Authentication Servers list.

### Changing the Name of an Authentication Server

The Details page of an Authentication Server displays the server's public key and allows you to change the server's name. To open this page, click ✎ in the card or row of the relevant server.



Server Name *: Local

Public Key: ssh-rsa AA[redacted]ADAQABAAABgQDUR4YIi

Created: 2024-09-18 17:24

**Server Name** is the only editable parameter on the Details page. After updating the name, click **Save**.

## Authenticator Management

Enterprise Connect Passwordless supports the ability to authenticate to Windows, Mac and the User Portal through multiple authenticators. Third-party authenticators can be added by means of plugins, enabling external developers to expand built-in behavior by adding new plugins or modifying existing ones.

The following sections present details about managing authenticators:

- Authenticator Plugins: Overview
- Viewing the Authenticator List
- Working with Authenticators
- Importing and Managing Hardware OTP Tokens
- Adding Third-party Authenticators
- Managing Authenticator Templates

### Authenticator Plugins: Overview

Authenticator plugins, which determine the authentications method(s) and behavior of third-party authenticators, are made up of two required parts:

- The Authenticator schema, also known as the template, is a JSON file that is uploaded to the Management Console. (For details, refer to Managing Authenticator Templates.)
- The Authenticator code is a JS file that needs to be manually uploaded to each Authentication Server. It is recommended to store the file in a dedicated directory, so system upgrades will not interfere with existing custom authenticators.

The names of the two plugin files (JSON and JS) **must be identical**. In addition, the file name needs to be unique, since it serves as the identifier of the template in the system.

The **Authenticators** tab of the **System Settings** menu allows you to add, update and manage authenticators, as well as upload new templates. Each authenticator you add must be based on one of the uploaded templates.

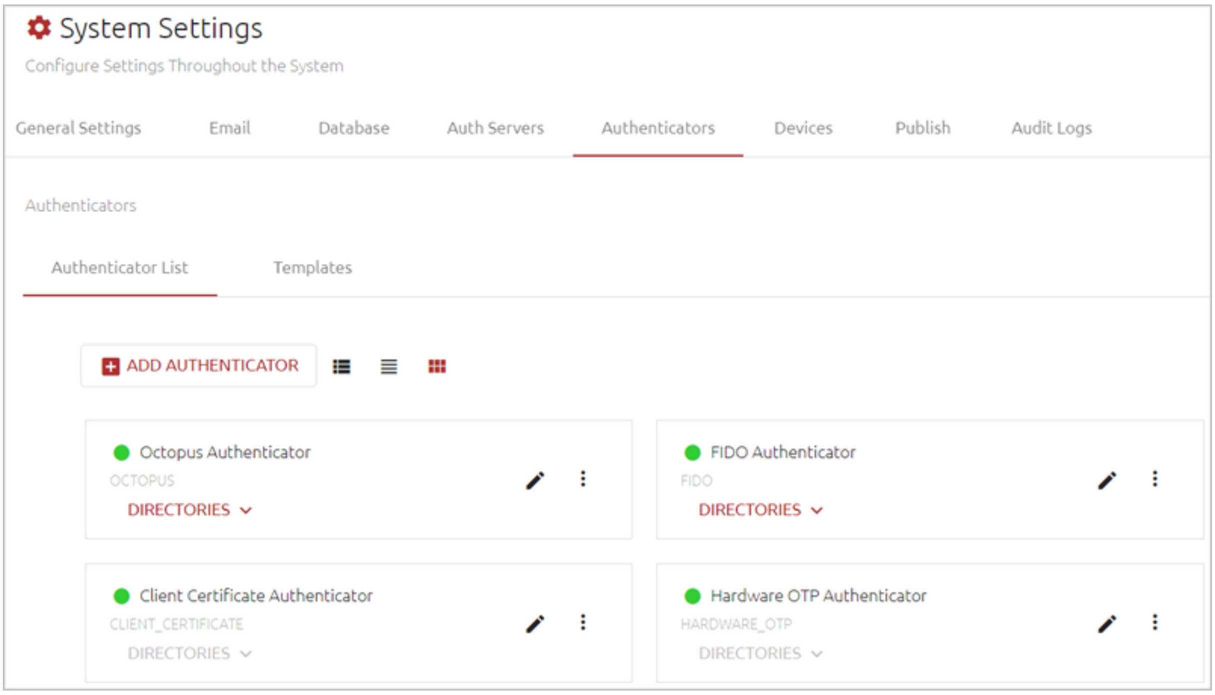
Selection of the primary mobile authenticator is done at the directory level. For more information, refer to Configuring Directory Authentication Options.

The Ping authenticator enables users working in the Ping Identity environment to authenticate by approving an authentication request on the PingID mobile app (delivered by push notification), or by providing the one-time password required by the service, which is validated by the PingFederate server.

A Reporting authenticator is dedicated to receiving workstation authentication event logs, so log reports can be viewed in the third-party platform. To enable third-party event reporting, the relevant Reporting authenticator needs to be specified in the **Authenticators** tab of the directory settings.

### Viewing the Authenticator List

The **Authenticator List** shows all configured authenticators and displays the name, source template, creation time (if relevant) and current connectivity status (red or green indicator) of each one. The Octopus, FIDO, Client Certificate and Hardware OTP Authenticators are preconfigured and automatically available. Other third-party authenticators need to be added, using the templates provided (Adding a New Authenticator).



System Settings

Configure Settings Throughout the System

General Settings | Email | Database | Auth Servers | Authenticators | Devices | Publish | Audit Logs

Authenticators

Authenticator List | Templates

ADD AUTHENTICATOR

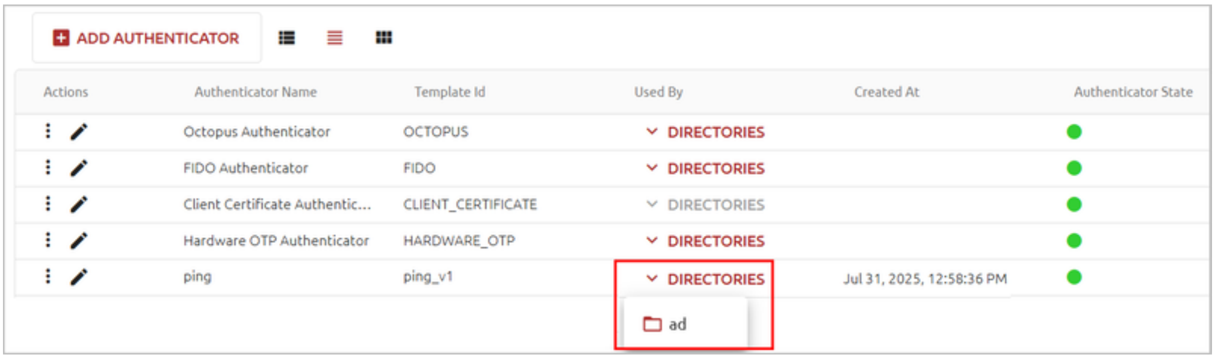
● Octopus Authenticator
OCTOPUS
DIRECTORIES

● FIDO Authenticator
FIDO
DIRECTORIES

● Client Certificate Authenticator
CLIENT_CERTIFICATE
DIRECTORIES

● Hardware OTP Authenticator
HARDWARE_OTP
DIRECTORIES

If an authenticator is used in one or more directories, the **DIRECTORIES** list is enabled. To view the directories to which an authenticator is assigned, click to open the list. Clicking a directory name opens the settings of that directory.



ADD AUTHENTICATOR

| Actions | Authenticator Name | Template Id | Used By | Created At | Authenticator State |
|---|---|---|---|---|---|
| ⋮ ✎ | Octopus Authenticator | OCTOPUS | DIRECTORIES | | ● |
| ⋮ ✎ | FIDO Authenticator | FIDO | DIRECTORIES | | ● |
| ⋮ ✎ | Client Certificate Authentic... | CLIENT_CERTIFICATE | DIRECTORIES | | ● |
| ⋮ ✎ | Hardware OTP Authenticator | HARDWARE_OTP | DIRECTORIES | | ● |
| ⋮ ✎ | ping | ping_v1 | DIRECTORIES<br>ad | Jul 31, 2025, 12:58:36 PM | ● |

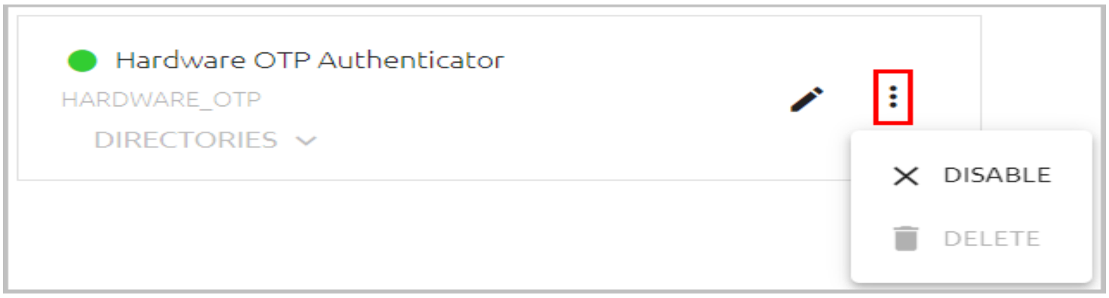
### Working with Authenticators

The options in the **Actions** column allow you to enable/disable the authenticators, update their details, and more. Clicking ⋮ opens a list with the following options:

- **Disable:** Inactivates the authenticator.
- **Delete:** Removes the authenticator from the Management Console. An authenticator can be deleted only if it is NOT currently assigned to any directories.

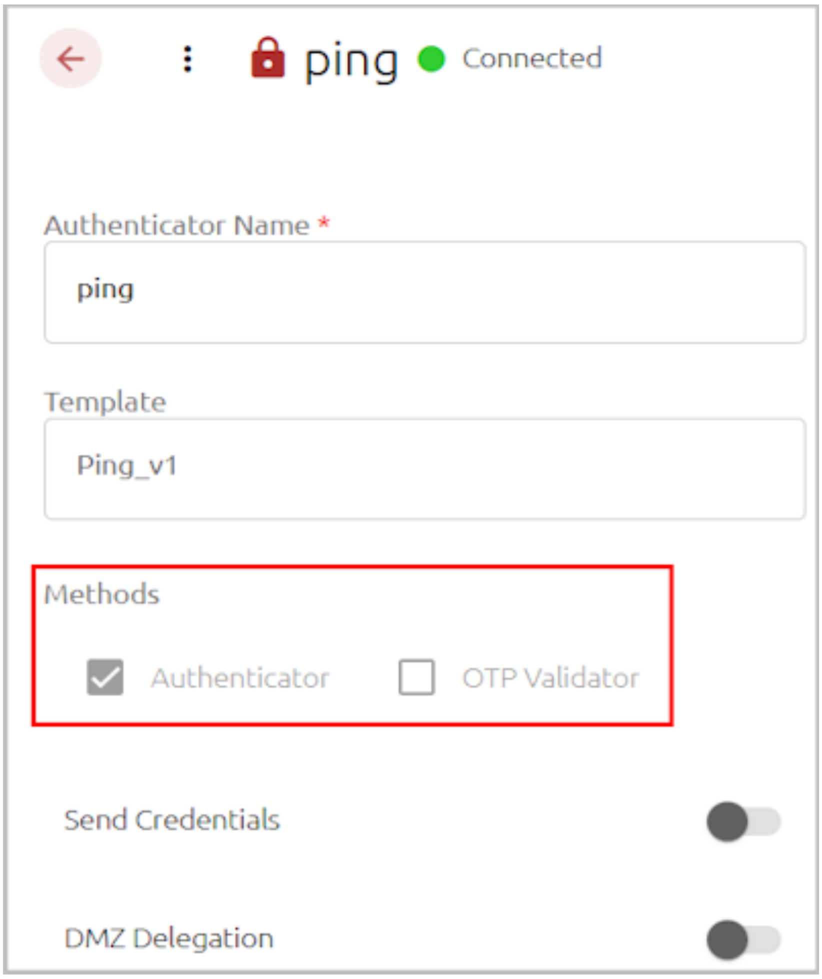
**Important**

Out-of-the-box authenticators cannot be deleted.



Clicking ✏ opens a page on which you can view and update authenticator details. When updating settings for an authenticator, keep the following in mind:

- The template cannot be changed.
- The authentication methods (Authenticator, OTP Validator, etc.) can be updated only if the authenticator is NOT currently assigned to any directories. When an authenticator is assigned, the **Methods** settings are disabled.



Authenticator Name *
ping

Template
Ping_v1

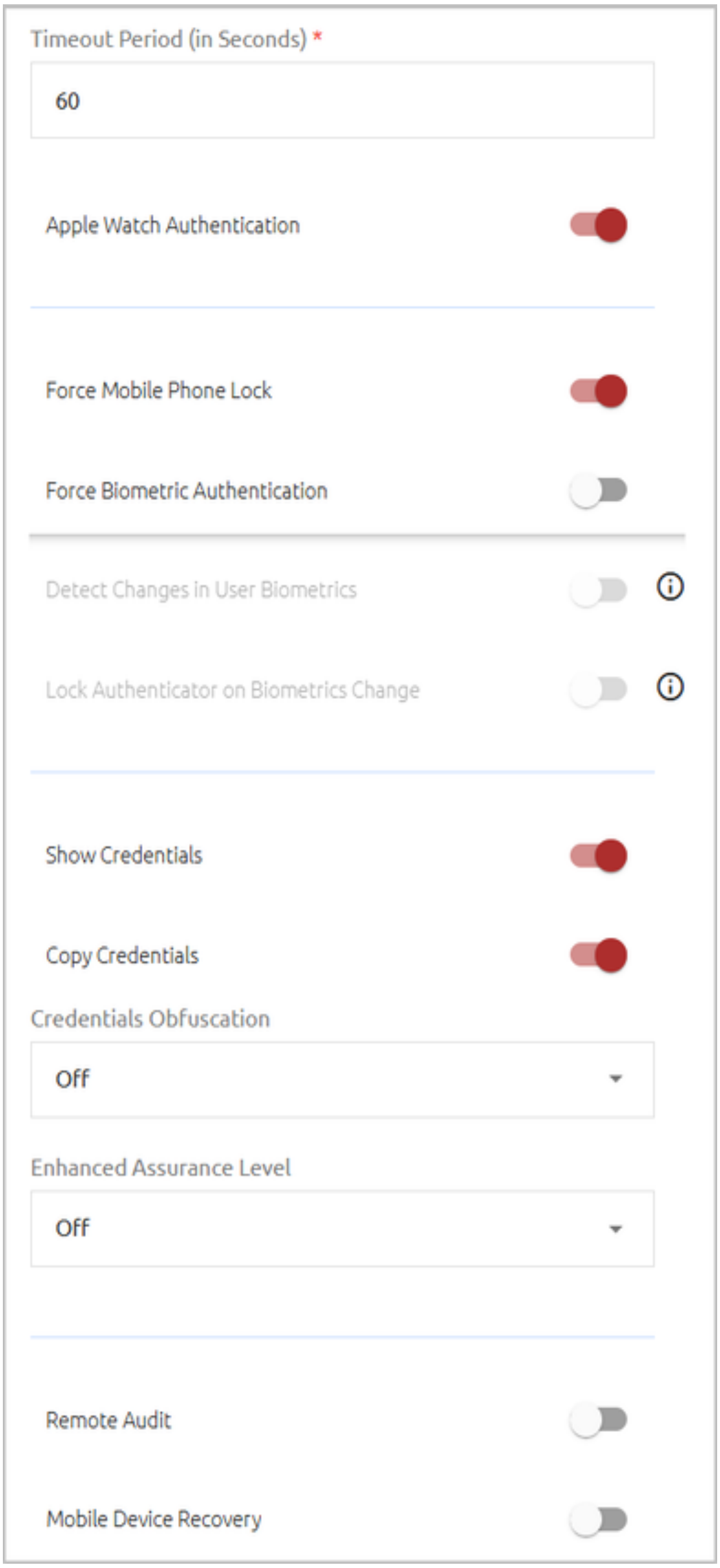
Methods
☑ Authenticator ☐ OTP Validator

Send Credentials

DMZ Delegation

Octopus Authenticator details (name and methods) are not editable, but several settings related to security mechanisms and management of credentials in the mobile app are configurable for this authenticator.

The settings are:



Timeout Period (in Seconds) *

60

Apple Watch Authentication ☑

Force Mobile Phone Lock ☑

Force Biometric Authentication ☐

Detect Changes in User Biometrics ☐ ⓘ

Lock Authenticator on Biometrics Change ☐ ⓘ

Show Credentials ☑

Copy Credentials ☑

Credentials Obfuscation

Off ▾

Enhanced Assurance Level

Off ▾

Remote Audit ☐

Mobile Device Recovery ☐

The settings are:

| Setting | Description | Default |
|---|---|---|
| Timeout Period | The length of time allotted for the mobile device to acknowledge receipt of a push notification from the Octopus Authentication Server. The supported timeout range is 5-60 seconds.<br>If the Server does not receive a confirmation message from the mobile within the specified time period, BLE mode authentication is initiated. If BLE has not been activated for the Octopus Agent, the authentication request fails. | 60 seconds |
| Apple Watch Authentication | When enabled, users are allowed to authenticate on the watch. When disabled, users must authenticate on their mobile devices. | Enabled |
| Force Mobile Phone Lock | When enabled, users are required to use the locking feature on their mobile devices. | Enabled |
| Force Biometric Authentication | When enabled, users must provide a biometric factor (fingerprint, face recognition, etc.) to successfully authenticate. This toggle is available only when the **Force Mobile Phone Lock** setting is enabled. | Disabled |
| Detect Changes in User Biometrics | When enabled, the Octopus mobile app checks for changes in biometric data with every authentication request. If a change is detected (e.g., Face ID added), it is recorded as an auditing event.<br>This toggle is available only when the **Force Biometric Authentication** setting is enabled. | Disabled |
| Lock Authenticator on Biometrics Change | When a change in biometric data is detected and this setting is enabled, the mobile app blocks authentication and sends a message to the Octopus Authentication Server to disable the mobile authenticator. Users are presented with an error message, prompting them to contact their IT team. The phone can be re-enabled by the system admin in the **Authenticators** tab of the user details.<br>This toggle is available only when the **Detect Changes in User Biometrics** setting is enabled. | Disabled |
| Show Credentials | When enabled, the AD password is displayed to users in the Octopus Authenticator mobile app. | Enabled |
| Copy Credentials | When enabled, users are able to copy the password displayed in the Octopus Authenticator app to the clipboard of the mobile device. | Enabled |

| Setting | Description | Default |
|---|---|---|
| Credentials Obfuscation | When this feature is activated, the mobile app is unable to decrypt the AD password, as the Authentication Server sends it to the app encrypted with the workstation's public key. (As a result, the **Show Credentials** and **Copy Credentials** settings must be disabled when using this feature.)<br>**Credentials Obfuscation** can be set to ONE of the following states:<br>• **Off:** Credentials can be decrypted by all versions of the mobile app.<br>• **Enabled:** Credentials can be decrypted by *versions 5.4 and lower* of the mobile app. This setting is useful during rollouts of version 5.5 and higher.<br>• **Enforced:** Credentials can never be decrypted by the mobile app. Authentication will fail for users working with versions of the mobile app lower than 5.5.<br>**Note:** This feature is not currently available for Mac workstations. | Off |

| Setting | Description | Default |
|---|---|---|
| Enhanced Assurance Level | When this feature is activated, an extra layer of security is added to the authentication flow by requiring a BLE challenge between the app and the workstation after the user approves the push request. This challenge ensures that the user's mobile device is in close proximity to the workstation.<br>**Enhanced Assurance Level** can be set to ONE of the following states:<br>• **Off:** A BLE challenge is not required (standard authentication flow).<br>• **Enabled:** A BLE challenge is attempted, but if it fails the user can still successfully authenticate. This setting is useful during rollouts of mobile app version 5.5 and higher and Windows Agent version 3.8.4 and higher.<br>• **Enforced:** A BLE challenge is always required for login. Authentication will fail for users working with versions of the mobile app lower than 5.5 and Agent versions lower than 3.8.4.<br>**Note:** This feature is not currently available for Mac workstations. | Off |
| Remote Audit | When enabled, audit records are sent from the mobile app to the Authentication Server. | Disabled |
| Mobile Device Recovery | When enabled, account recovery after migration to a new mobile device is supported.<br>**Note**<br>Previous configuration of this feature in the **prod.json** file will NOT be saved upon upgrade. The setting needs to be configured in the Management Console after upgrade. | Disabled |

After updating authenticator details or settings, click **Save**.

> **Note**
>
> Details for the FIDO Authenticator and Client Certificate Authenticator are not editable.

### Importing and Managing Hardware OTP Tokens

Enterprise Connect Passwordless supports use of HW OTP tokens to authenticate to Windows and the User Portal. In order for users to successfully login with HW OTP tokens, you need to:

1. Import a list of tokens from a file (as described in the procedure below).

2. Enable support of HW OTP tokens for online and/or offline authentication in the relevant directory (Configuring Directory Authentication Options).

3. Send enrollment invitations to your users.

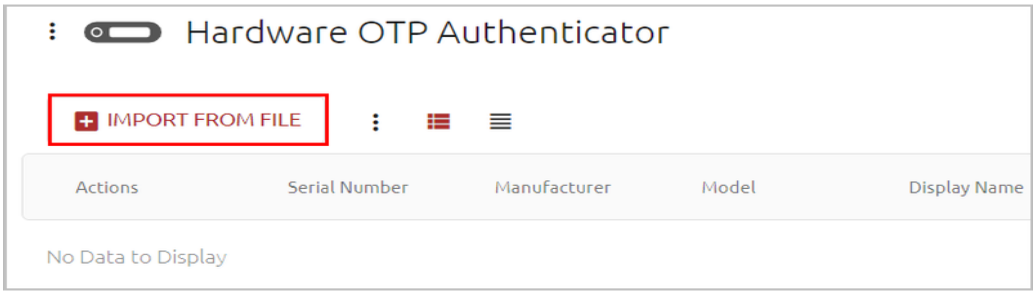
**Important**

Users can enroll with *one* OTP type only (either hardware or software, but not both).

**To import hardware OTP tokens:**

1. From the **Authenticator List**, click ✎ in the card or row of the Hardware OTP Authenticator.

   Then, on the page that opens, click **Import From File**.



Hardware OTP Authenticator

IMPORT FROM FILE

| Actions | Serial Number | Manufacturer | Model | Display Name |
|---|---|---|---|---|

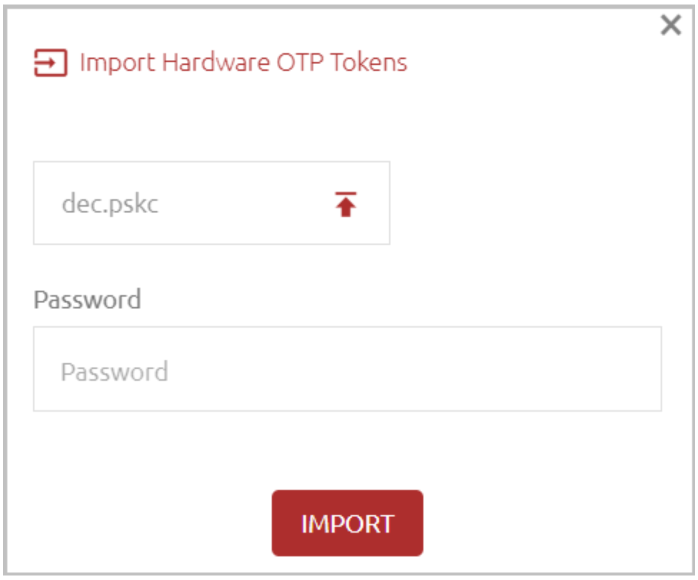
No Data to Display

2. In the popup that opens:

   a. Click **Upload File.** Then, navigate to and select the relevant file.

**Important**

The file must be in **PSKC format**. Maximum supported file size is **20 MB**.



Import Hardware OTP Tokens

dec.pskc

Password

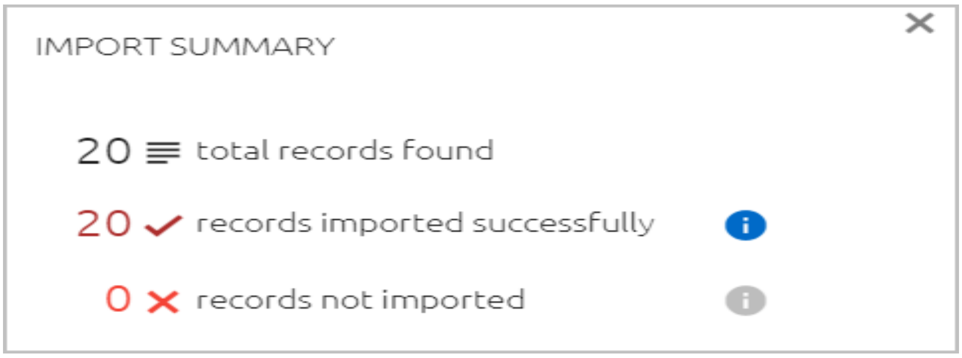
Password

IMPORT

   b. If the selected file is encrypted, enter the password in the **Password** field.

3. Click **Import.**

   Once the import process is complete, an import summary is displayed. For example:



IMPORT SUMMARY

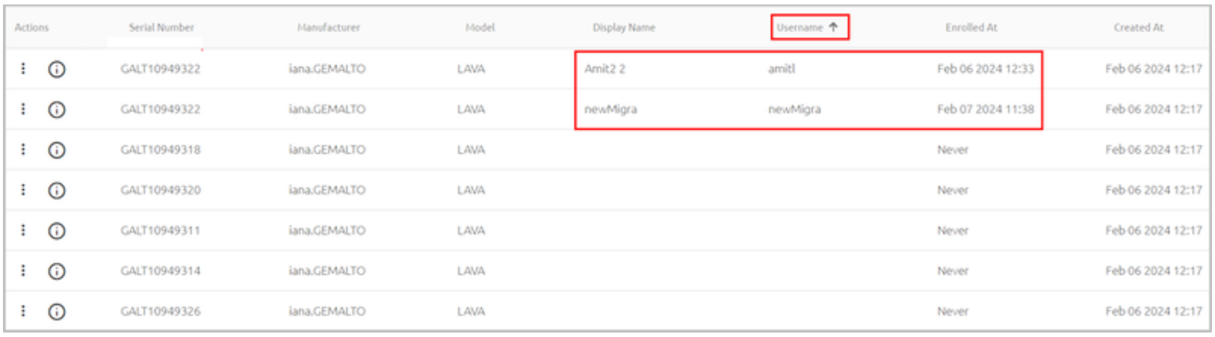
20 ≡ total records found

20 ✓ records imported successfully

0 ✕ records not imported

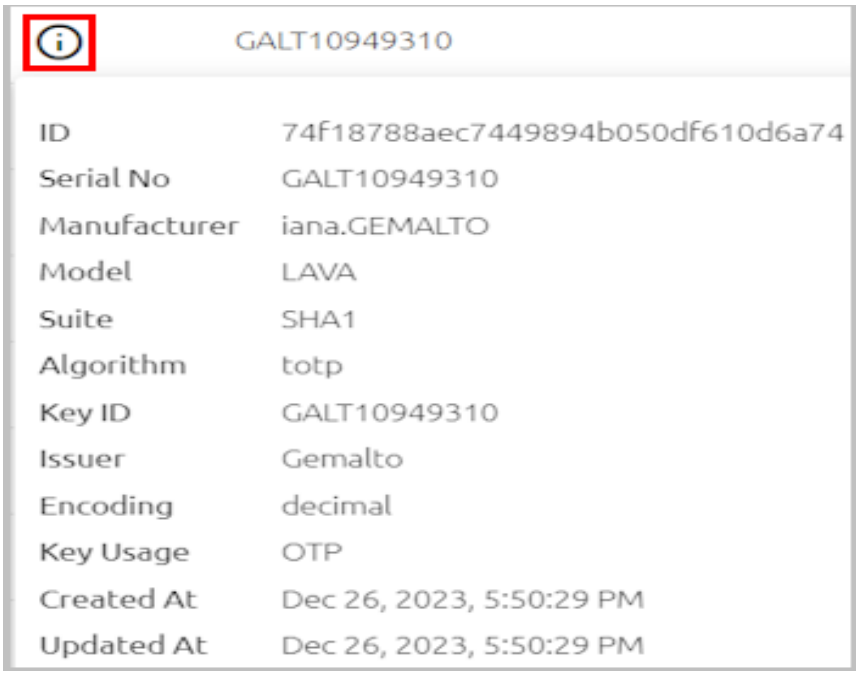
4. Continue by configuring directory settings and inviting users to enroll.

After tokens have been successfully imported, the list of devices appears on the **Hardware OTP Authenticator** page. Once users have registered, enrollment information is displayed in the relevant columns. In addition, you can sort the list according to **Username** and perform searches for a specific username.



| Actions | Serial Number | Manufacturer | Model | Display Name | Username ↑ | Enrolled At | Created At |
|---|---|---|---|---|---|---|---|
| ⋮ ⓘ | GALT10949322 | iana.GEMALTO | LAVA | Amit2 2 | amitl | Feb 06 2024 12:33 | Feb 06 2024 12:17 |
| ⋮ ⓘ | GALT10949322 | iana.GEMALTO | LAVA | newMigra | newMigra | Feb 07 2024 11:38 | Feb 06 2024 12:17 |
| ⋮ ⓘ | GALT10949318 | iana.GEMALTO | LAVA | | | Never | Feb 06 2024 12:17 |
| ⋮ ⓘ | GALT10949320 | iana.GEMALTO | LAVA | | | Never | Feb 06 2024 12:17 |
| ⋮ ⓘ | GALT10949311 | iana.GEMALTO | LAVA | | | Never | Feb 06 2024 12:17 |
| ⋮ ⓘ | GALT10949314 | iana.GEMALTO | LAVA | | | Never | Feb 06 2024 12:17 |
| ⋮ ⓘ | GALT10949326 | iana.GEMALTO | LAVA | | | Never | Feb 06 2024 12:17 |

To view additional details about a given device, click ⓘ in the relevant row or card.



ⓘ GALT10949310

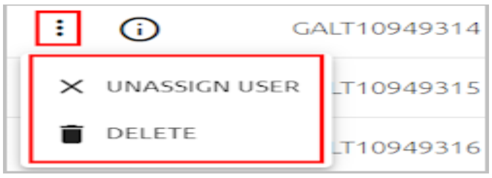
| | |
|---|---|
| ID | 74f18788aec7449894b050df610d6a74 |
| Serial No | GALT10949310 |
| Manufacturer | iana.GEMALTO |
| Model | LAVA |
| Suite | SHA1 |
| Algorithm | totp |
| Key ID | GALT10949310 |
| Issuer | Gemalto |
| Encoding | decimal |
| Key Usage | OTP |
| Created At | Dec 26, 2023, 5:50:29 PM |
| Updated At | Dec 26, 2023, 5:50:29 PM |

Clicking ⋮ in the row of a token enables you to perform the following actions on that token:

- **Unassign User:** Reverses user enrollment. Following this action, the user will need to register again with a new enrollment invitation.
- **Delete:** Removes the token from the system. Following this action, the token will need to be reimported.

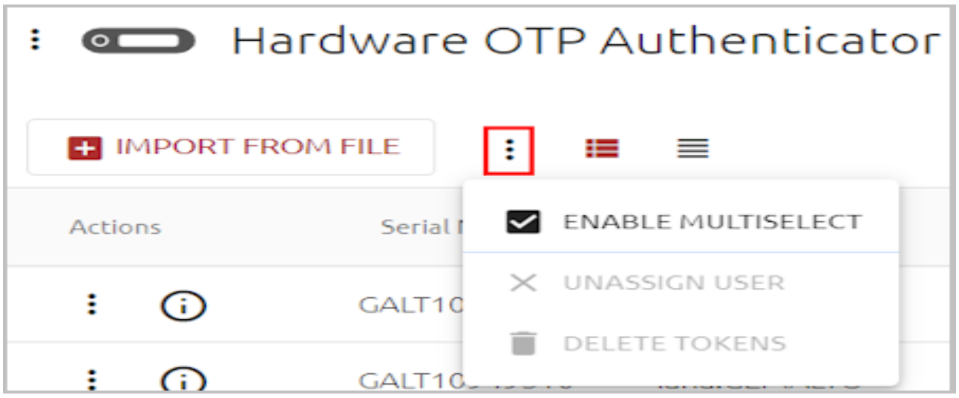
**Note**

Users must be unassigned before tokens can be deleted.



**Performing Bulk Operations on Hardware OTP Tokens**

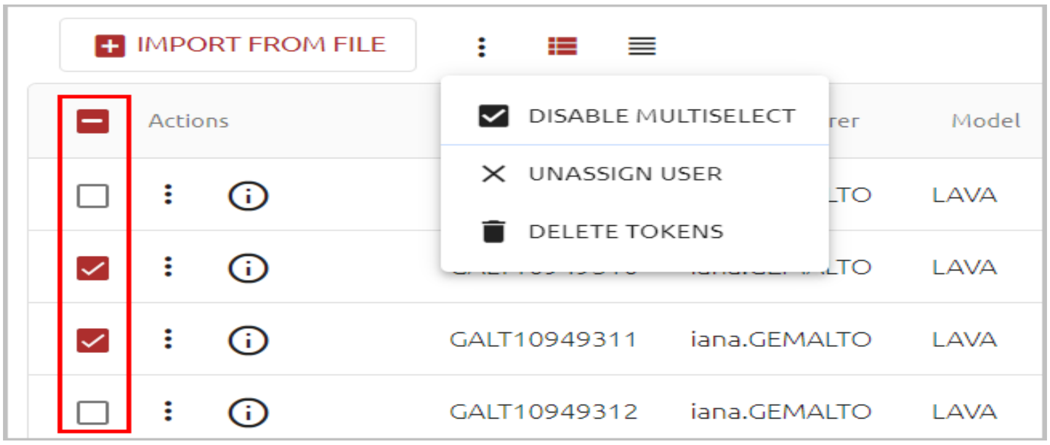
Clicking the ⋮ icon to the right of the **Import From File** button opens an actions menu from which you can enable / disable token selection.



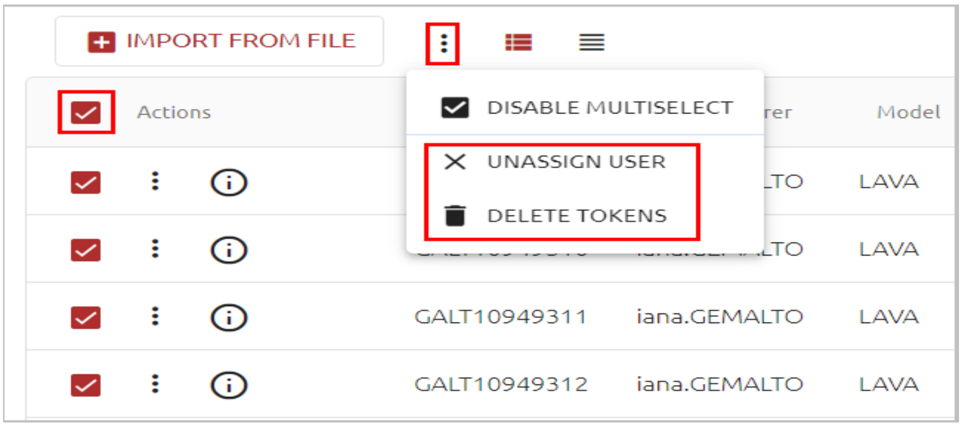
When you click **Enable Multiselect**, checkboxes appear next to the tokens, allowing you to select multiple tokens. Once tokens are selected, you can unassign users from the tokens, or remove the tokens from the system.

**Note**

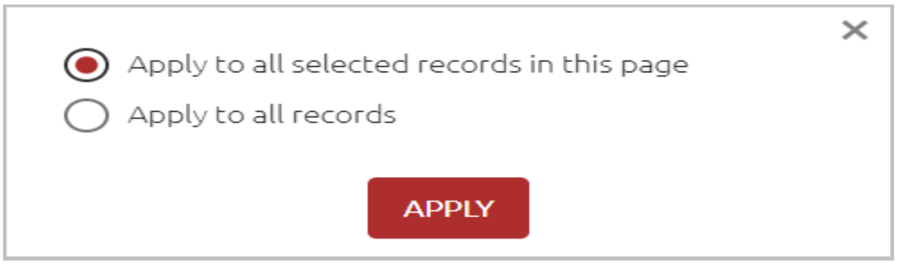
Users must be unassigned before tokens can be deleted.



Selecting the checkbox at the top of the **Actions** column enables you to carry out a bulk action on all tokens on the page, or all tokens on the list.



When you select an action (**Unassign User** or **Delete Tokens**), you will be prompted to specify whether to apply the operation to all tokens, or only the tokens listed on the current page of the list.



● Apply to all selected records in this page

○ Apply to all records

To hide the checkboxes and exit selection mode, click **Disable Multiselect**.

**Adding Third-party Authenticators**

All third-party authenticators must use an installed template. When creating a new authenticator, you will be prompted to select the template on which it is based. The Management Console features several built-in templates and also supports the ability to upload customized templates.

You can create multiple authenticators using the same template, according to your organizational needs. For example, you might want to have a separate authenticator dedicated to OTP authentication.

**To add a Ping authenticator:**

1. In the upper left corner of the **Authenticators** tab, click **Add Authenticator**.

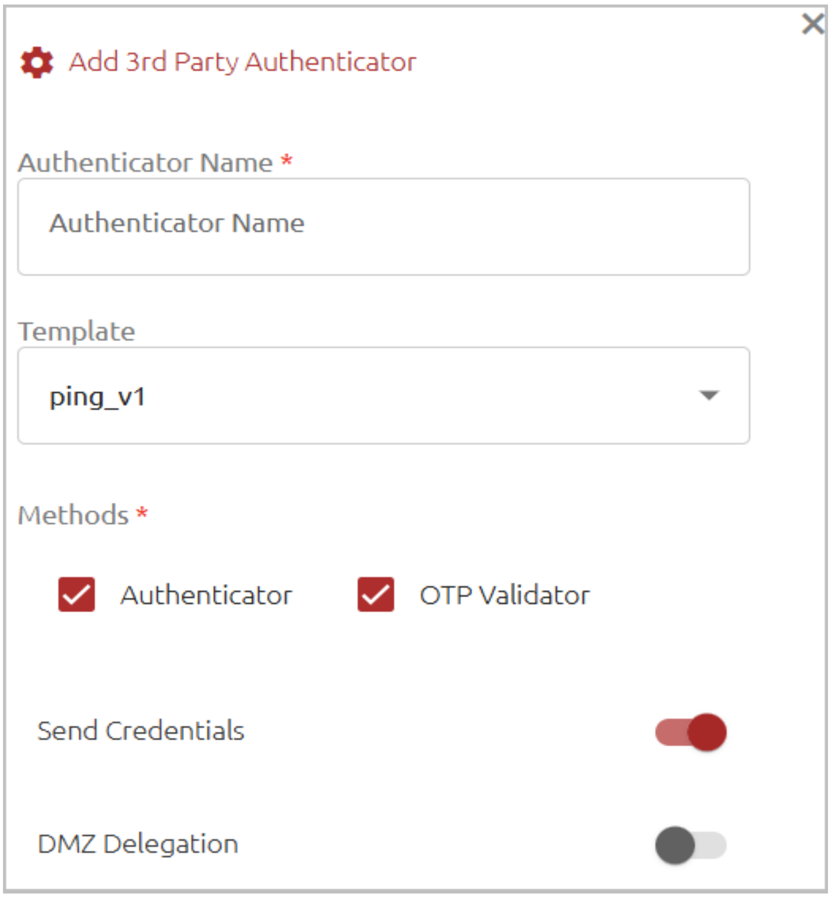
   The **Add 3rd Party Authenticator** dialog opens.

2. In the **Authenticator Name** field, enter a friendly descriptive name for the new authenticator.

3. From the **Template** dropdown list, select the template on which the authenticator will be based.

**Important**

You will not be able to change the template after you create the authenticator.



Add 3rd Party Authenticator

Authenticator Name *: Authenticator Name

Template: ping_v1

Methods *: ☑ Authenticator ☑ OTP Validator

Send Credentials: enabled

DMZ Delegation: disabled

4. Select one or more **Methods** for the new authenticator:

    ○ **Authenticator:** The third party-authenticator can be used as an additional means of authentication (primary and/or secondary).

    ○ **OTP Validator:** The third party-authenticator can be used for one time password authentication (online and/or offline).

    If you do NOT want to use the new authenticator for a method, clear the relevant checkbox.

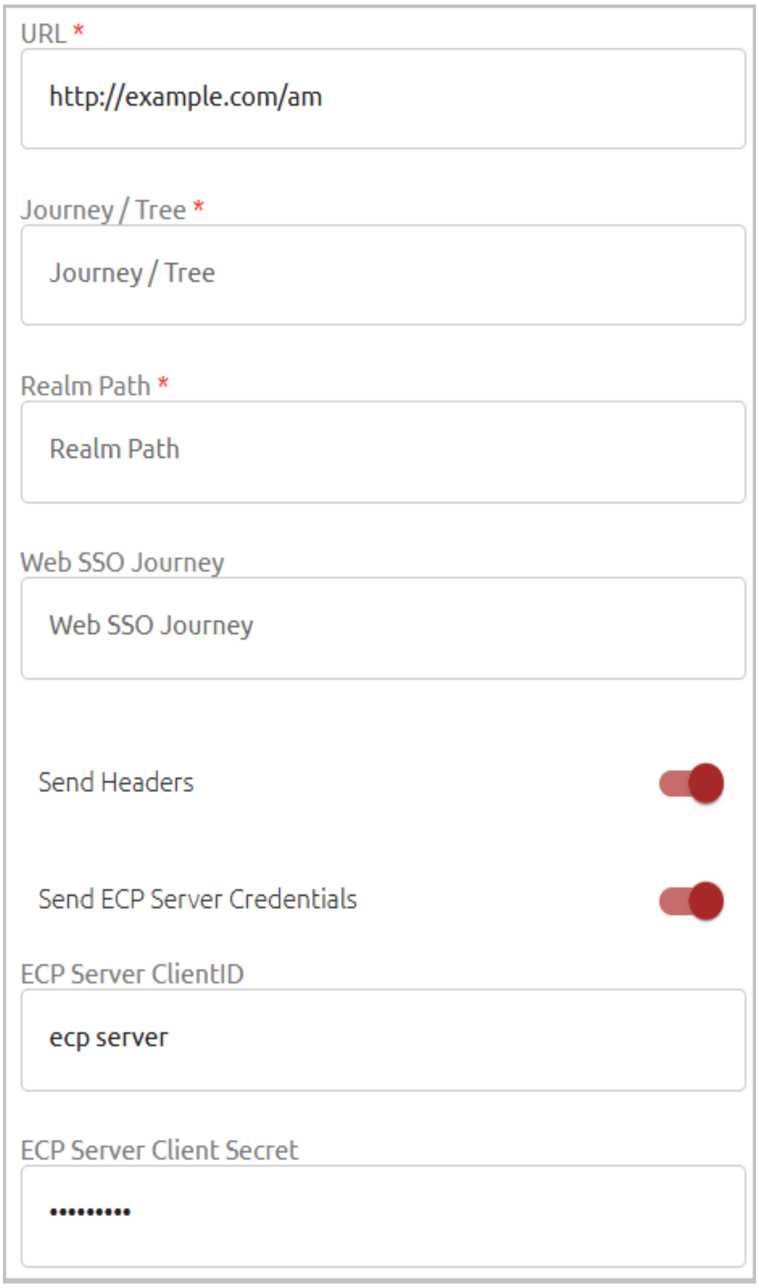
5. Specify whether to send user credentials to the third-party authenticator by enabling or disabling the **Send Credentials** toggle button.

    When credentials are sent (default setting), the third-party authenticator sends back a token for the User Portal, and the Portal opens automatically upon user authentication to Windows or Mac. If credentials are not sent, no token is sent back, and users will need to manually log into the User Portal after being authenticated by the third party.

6. Enable / Disable the **DMZ Delegation** toggle as required. When this setting is enabled, Authentication Servers in the DMZ can communicate directly with a server within the internal network.

7. Specify the following settings:

    - **URL:** The access URL for your Ping Identity Platform
    - **Journey / Tree:** Name of the relevant authentication journey
    - **Realm Path:** Name of the realm in which the journey is located
    - **Web SSO Journey:** URL of the *winsso* journey.
    - **Send Headers:** When the toggle is enabled, HTML headers (*IP*, *User-Agent*, *Primary-Auth-Type*) are sent to Ping Identity.
    - **Send ECP Server Credentials:** When the toggle is enabled, Agent + Token authentication is supported. In the fields below, enter the Agent ID and password defined in your Ping environment.



URL *

http://example.com/am

Journey / Tree *

Journey / Tree

Realm Path *

Realm Path

Web SSO Journey

Web SSO Journey

Send Headers ●

Send ECP Server Credentials ●

ECP Server ClientID

ecp server

ECP Server Client Secret

•••••••••

8. To check the validity of your settings, click **Test Connection**.
9. Click **Add**.

   The dialog closes, and the new authenticator is added to the Authenticator List.

## Managing Authenticator Templates

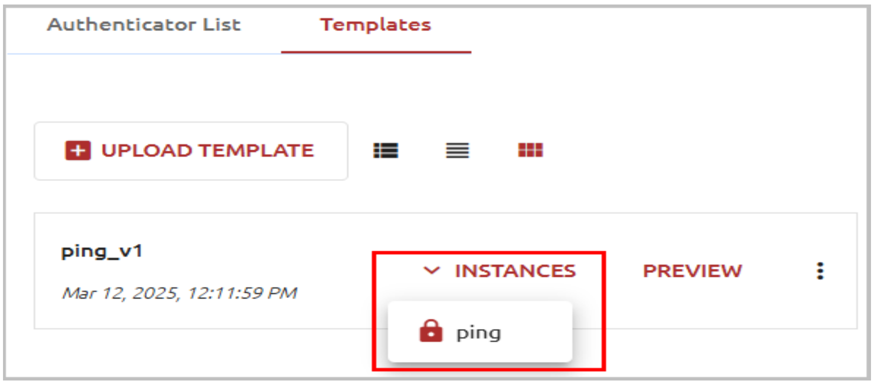
Template files, which are written in JSON format, contain the schema for third-party authenticators used in the system. The Management Console features built-in templates and supports the ability to upload customized template files.

The **Templates** tab allows you to view and manage existing templates and upload new ones.

### Working with the Templates List

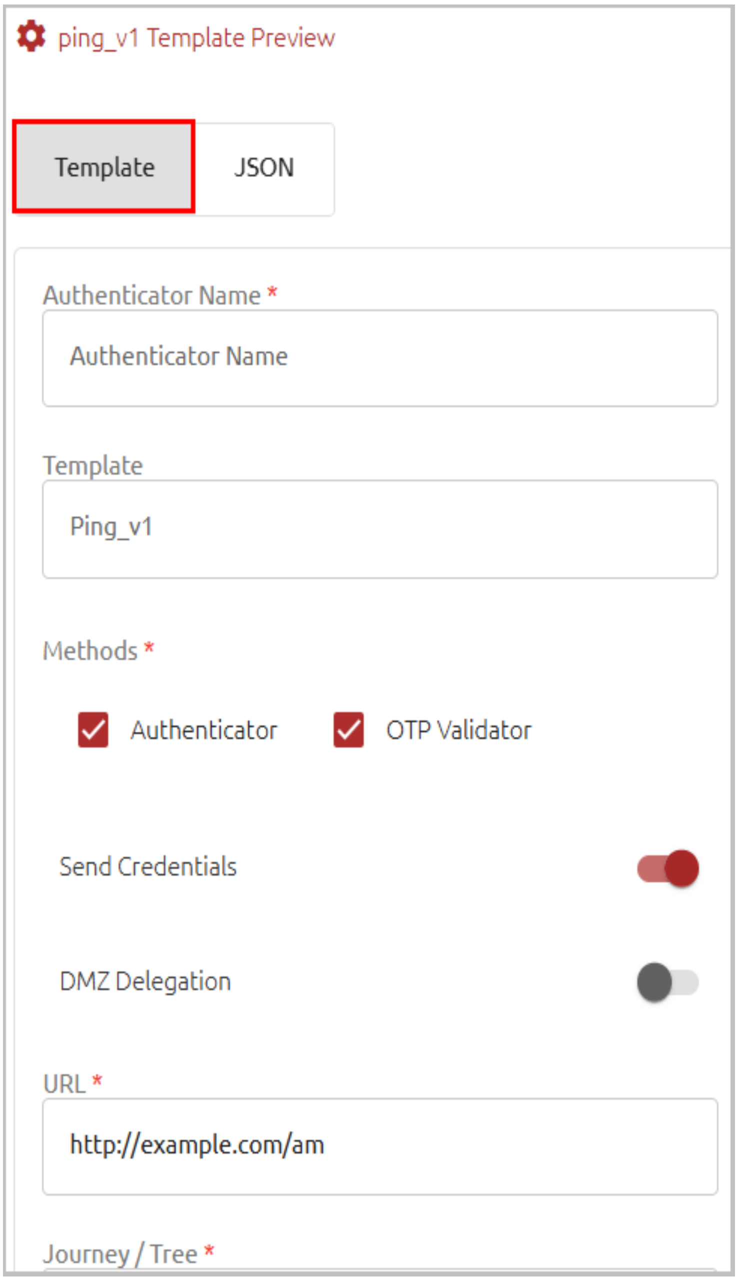
Each card or row in the **Templates** tab shows the file name and creation time of the template. If a template is being used by one or more authenticators, the **INSTANCES** list is enabled.

To view the authenticators currently using the template, click to open the list. Clicking an authenticator in the list opens the settings page for that authenticator.



Clicking **PREVIEW** opens a popup in which you can view the template's fields. The **Template Preview** popup contains two views:

- **Template:** Shows the fields as they will be displayed in the Management Console (e.g., when creating a new authenticator based on the template).



ping_v1 Template Preview

Authenticator Name *

Authenticator Name

Template

Ping_v1

Methods *

☑ Authenticator ☑ OTP Validator

Send Credentials ●

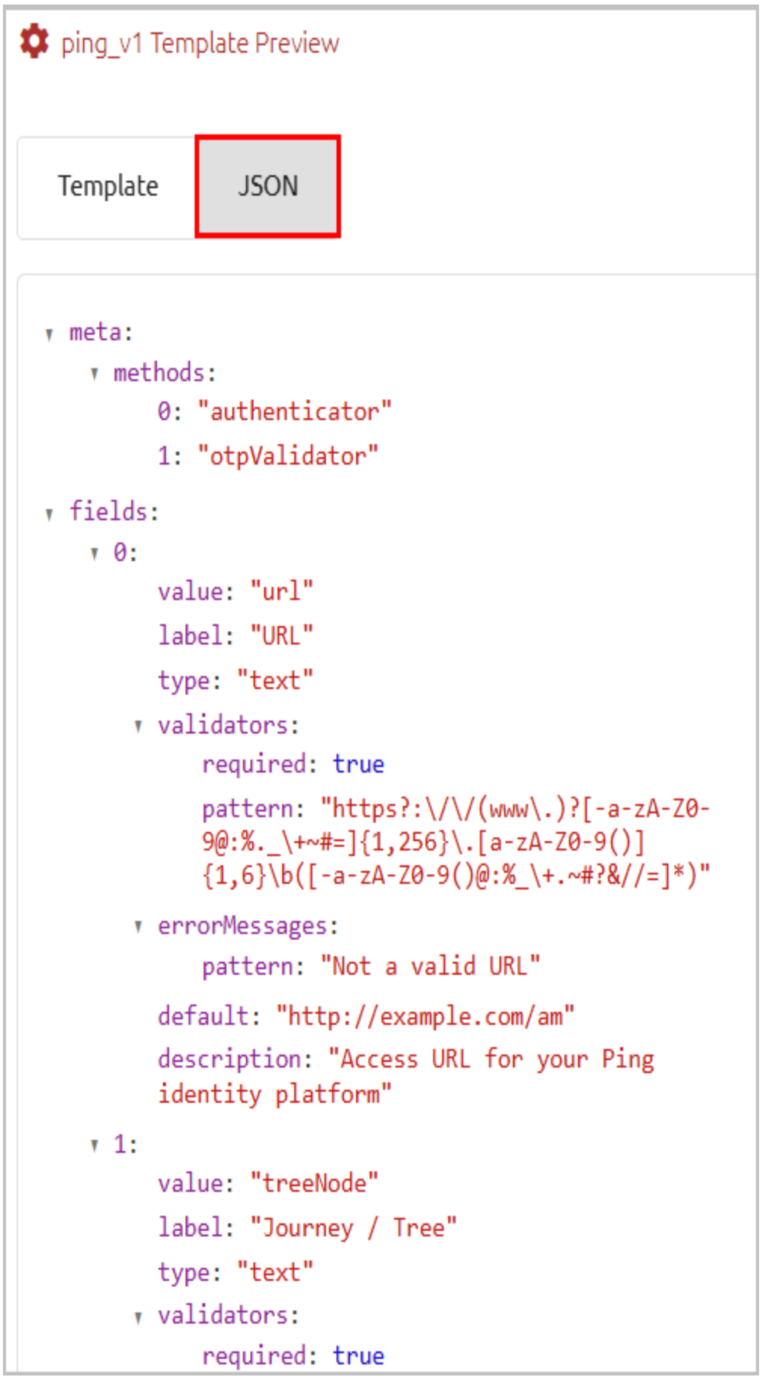
DMZ Delegation ○

URL *

http://example.com/am

Journey / Tree *

- **JSON:** Shows the structure of the JSON file.



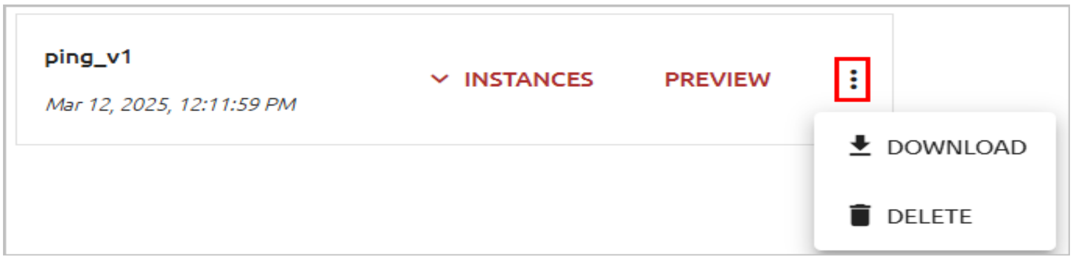
```
▾ meta:
    ▾ methods:
        0: "authenticator"
        1: "otpValidator"
▾ fields:
    ▾ 0:
        value: "url"
        label: "URL"
        type: "text"
      ▾ validators:
            required: true
            pattern: "https?:\/\/(www\.)?[-a-zA-Z0-
            9@:%._\+~#=]{1,256}\.[a-zA-Z0-9()]
            {1,6}\b([-a-zA-Z0-9()@:%_\+.~#?&//=]*)"
      ▾ errorMessages:
            pattern: "Not a valid URL"
        default: "http://example.com/am"
        description: "Access URL for your Ping
        identity platform"
    ▾ 1:
        value: "treeNode"
        label: "Journey / Tree"
        type: "text"
      ▾ validators:
            required: true
```

**Important**

Fields in the **Template Preview** popup are NOT editable.

Clicking ⋮ opens a list with the following actions:

- **Download:** Downloads the JSON file to the user's local machine. Use the Download option for backup and to create new customized files based on a built-in template.
- **Delete:** Removes the template from the Management Console. A template can be deleted only if it is NOT currently being used by an authenticator.



### Uploading a Template File

Custom authenticator templates can be imported to the Management Console by uploading the relevant JSON file.

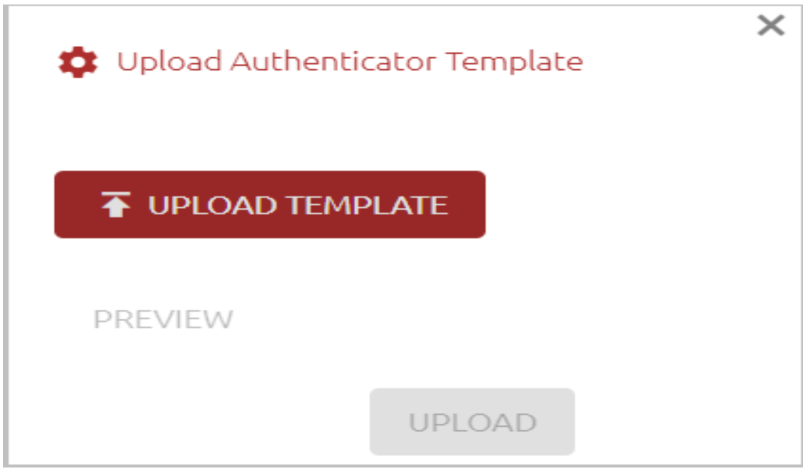
**Important**

Before uploading the file, make sure that the corresponding JS file (containing the authenticator code) has been copied to the **Custom Authenticators** directory on each Authentication Server. The names of the JSON file and the JS file must be identical.

#### To upload a template file:

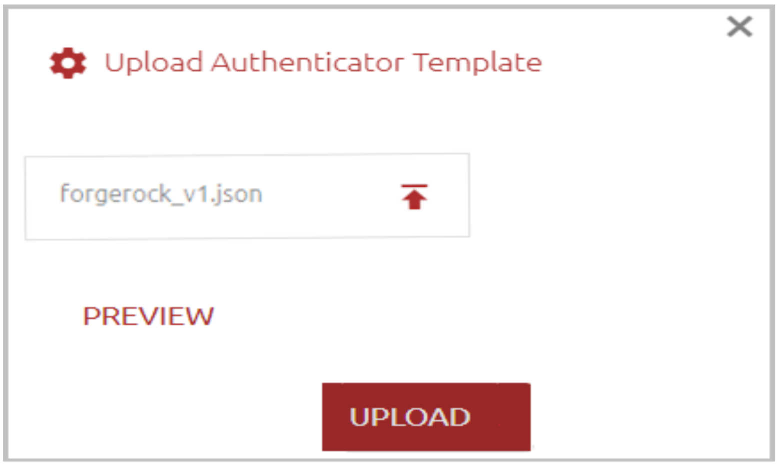
1. In the upper left corner of the **Templates** tab, click **Upload Template**.

   The **Upload Authenticator Template** dialog opens.

2. Click **Upload Template**. Then, navigate to and select the relevant JSON file.

   The name of the selected file is displayed.



3. To view the template's fields before uploading the file, click **Preview**. The **Template Preview** popup allows you to both view the fields as they will appear in the Management Console interface and review the structure of the JSON file.
4. Click **Upload**.

   The template is added to the list in the **Templates** tab.

### Modifying a Built-in Plugin

External developers can expand on built-in behavior by modifying an out-of-the-box plugin.

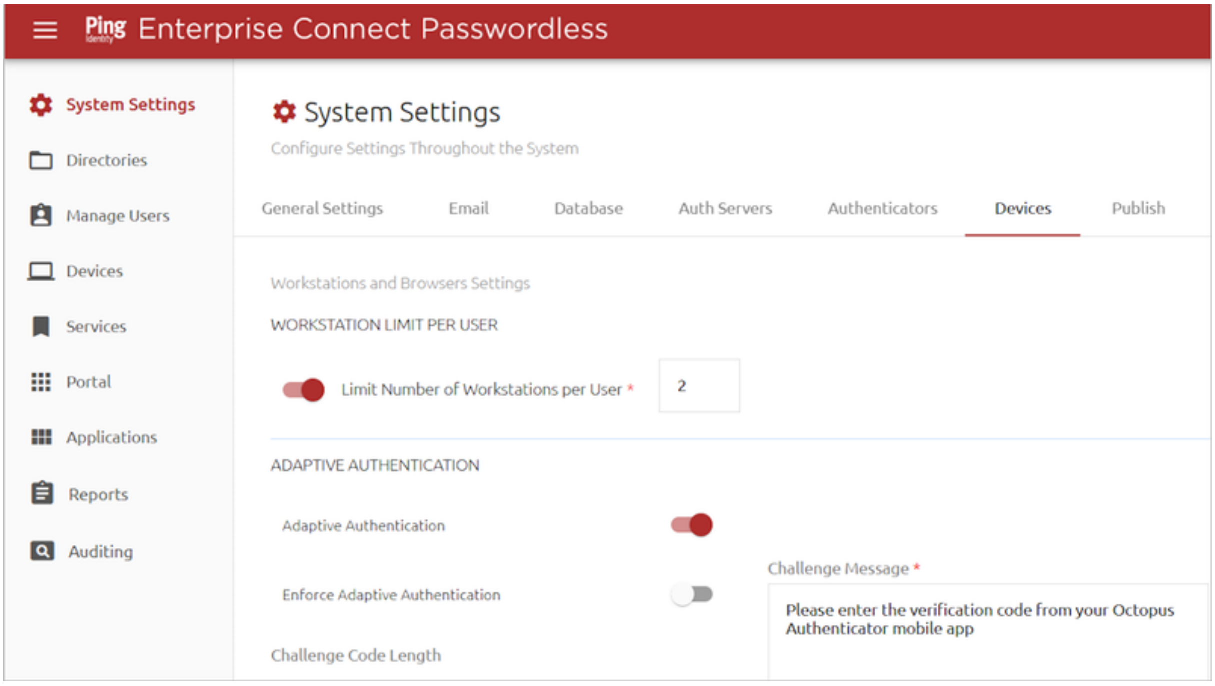
**To modify a built-in plugin:**

1. Access the required files:
   - Export the JSON file from the Management Console.
   - Copy the JS file from the **Custom Authenticators** directory on the Authentication Server.
2. Modify the two files as required. Verify that all variables used in the code are defined in the schema (JSON file).
3. Rename the files with the same file name. The name cannot be one that is being used by one of the built-in templates.
4. Manually upload the modified JS file to the **Custom Authenticators** directory on each Authentication Server. The new file will override any existing authenticator with the same name.
5. Upload the JSON file to the Management Console, using the interface in the **Templates** tab.

## Managing Workstation and Browser Settings

The **Devices** tab of the **System Settings** menu allows you to control the following security settings related to the workstations and browsers that are used for authentication:

- Workstation Limit: When this setting is enabled, you can restrict the number of workstations to which users can successfully authenticate.
- Adaptive Authentication: When this feature is enabled, a stronger authentication mechanism is required for users logging in for the first time via a workstation or browser not previously used for Octopus Authentication.
- Workstation Push Fatigue Protection: When this feature is enabled, automatic protective mechanisms are enforced in the event of a suspected push bombing attack.
- Distributed Workstations Vault settings: Allow you to manage security keys, control support of legacy workstations, and exit Compatibility Mode when you are ready to switch to a decentralized vault configuration.
- macOS FileVault Password settings: Allow you to configure settings related to the Octopus FileVault password (relevant for Octopus for Mac versions 2.6.1 and above).



Workstations and Browsers Settings

WORKSTATION LIMIT PER USER

Limit Number of Workstations per User * 2

ADAPTIVE AUTHENTICATION

Adaptive Authentication

Enforce Adaptive Authentication

Challenge Message *

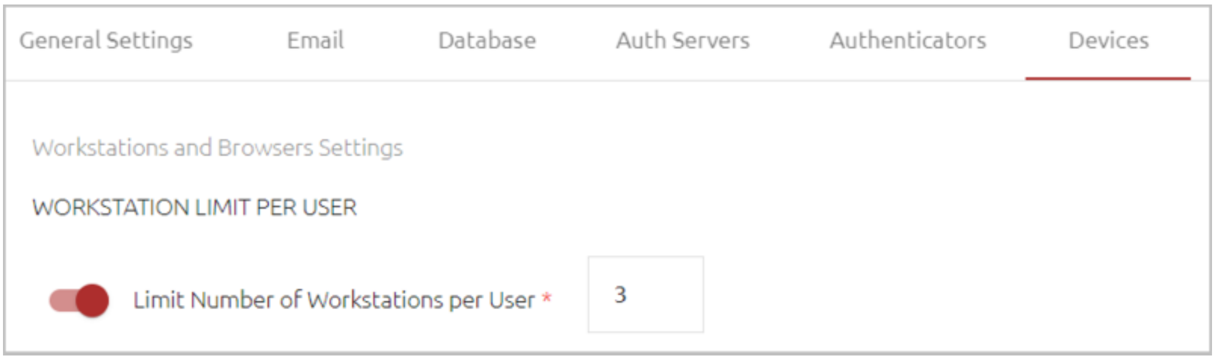
Please enter the verification code from your Octopus Authenticator mobile app

Challenge Code Length

### Workstation Limit Per User

This setting enables you to define a limit on the number of workstations to which users can authenticate. Once the limit is reached, authentication to any other workstation(s) will fail.

To define the limit, click the toggle to enable the setting. Then specify the permitted number of workstations in the field to the right.



Workstations and Browsers Settings

WORKSTATION LIMIT PER USER

Limit Number of Workstations per User * 3

After making your changes, scroll to the bottom of the tab and click **Save**.

**Note**

The global limit set here can be overridden for individual users in the user's details (**Security** tab).

### Adaptive Authentication Settings

Adaptive Authentication provides an extra layer of security when authentication is attempted from a workstation or browser not previously used for Octopus Authentication. When Adaptive Authentication is enabled, users authenticating for the first time from a unrecognized device (browser/workstation) are required to enter the verification code that is generated and displayed in the Octopus Authenticator mobile app. Following the first successful authentication, users are no longer required to enter a code if the browser or workstation is designated as a Trusted device.

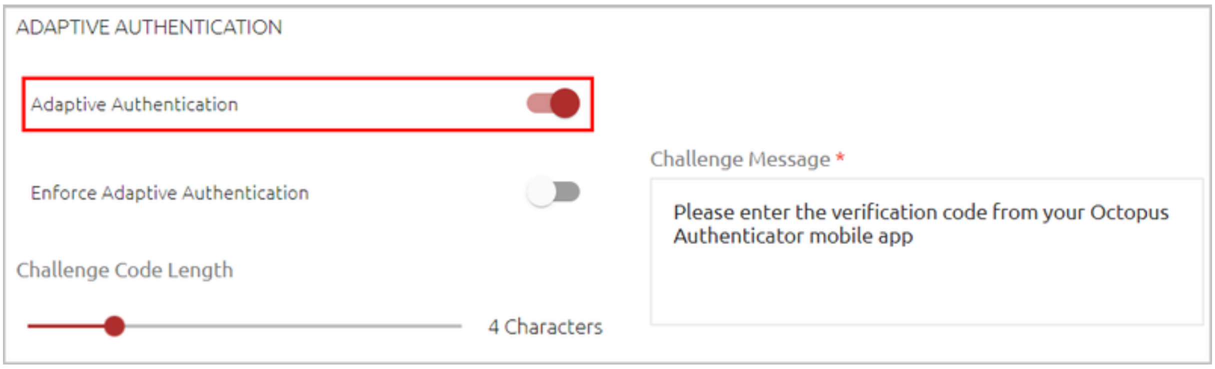
To further enhance security, the Adaptive Authentication mechanism enforces the following limitations on login attempts:

- **Windows login:** Users can enter the verification code only once. If the code is incorrect, authentication will fail and the entire authentication process needs to be restarted.
- **Portal login:** Users are allowed multiple attempts to enter the verification code. However, after three incorrect attempts the system will not permit a user to authenticate (regardless of whether the correct code is provided on later attempts) until a new authentication request is initiated.

**Important**

Adaptive Authentication is relevant to the Octopus Authenticator only.

The feature is activated and inactivated by toggling the **Adaptive Authentication** toggle button.

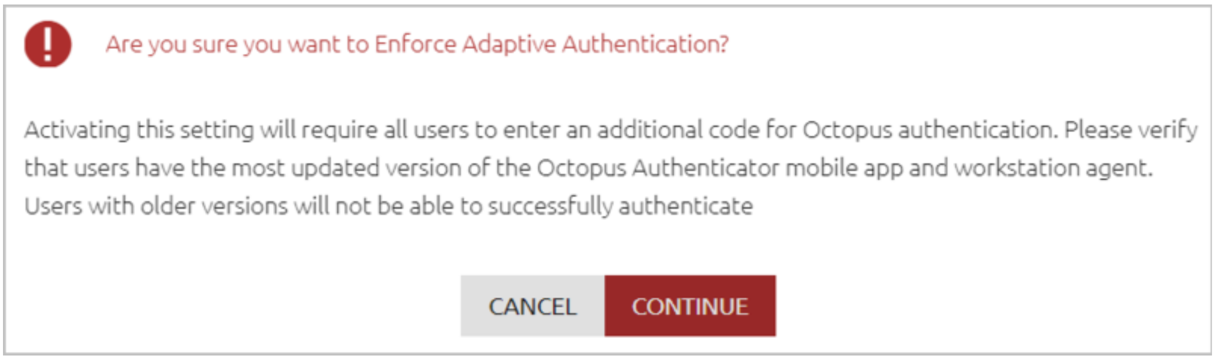


Please enter the verification code from your Octopus Authenticator mobile app

When Adaptive Authentication is active, the following settings are enabled and configurable:

- **Enforce Adaptive Authentication:** This setting determines whether the Adaptive Authentication mechanism will apply to users authenticating with versions of Octopus Authenticator lower than 5.0. When the setting is *off*, users with previous versions of Windows, Mac or Exchange agent will be able to authenticate from an unrecognized device without entering a challenge code. When the setting is *on*, authentication will fail, and these users will need to upgrade to the newest version in order to successfully authenticate.

  To activate Enforce Adaptive Authentication, click the toggle button and then click **Continue** in the confirmation popup.

  Are you sure you want to Enforce Adaptive Authentication?

  Activating this setting will require all users to enter an additional code for Octopus authentication. Please verify that users have the most updated version of the Octopus Authenticator mobile app and workstation agent. Users with older versions will not be able to successfully authenticate

- **Challenge Code Length:** Number of characters in the verification code. Valid values range from 3-8. The default value is 4.

- **Challenge Message:** The message displayed to users prompting them to enter the verification code.

After updated Adaptive Authentication settings, scroll to the bottom of the tab and click **Save**.

**Note**

The global settings defined here can be overridden for individual services, in the Devices tab of the service settings.

**Important**

- In *new* installations of Octopus Authentication Server versions 5.0 and higher, the Adaptive Authentication feature is enabled by default (with the **Enforce** setting off).

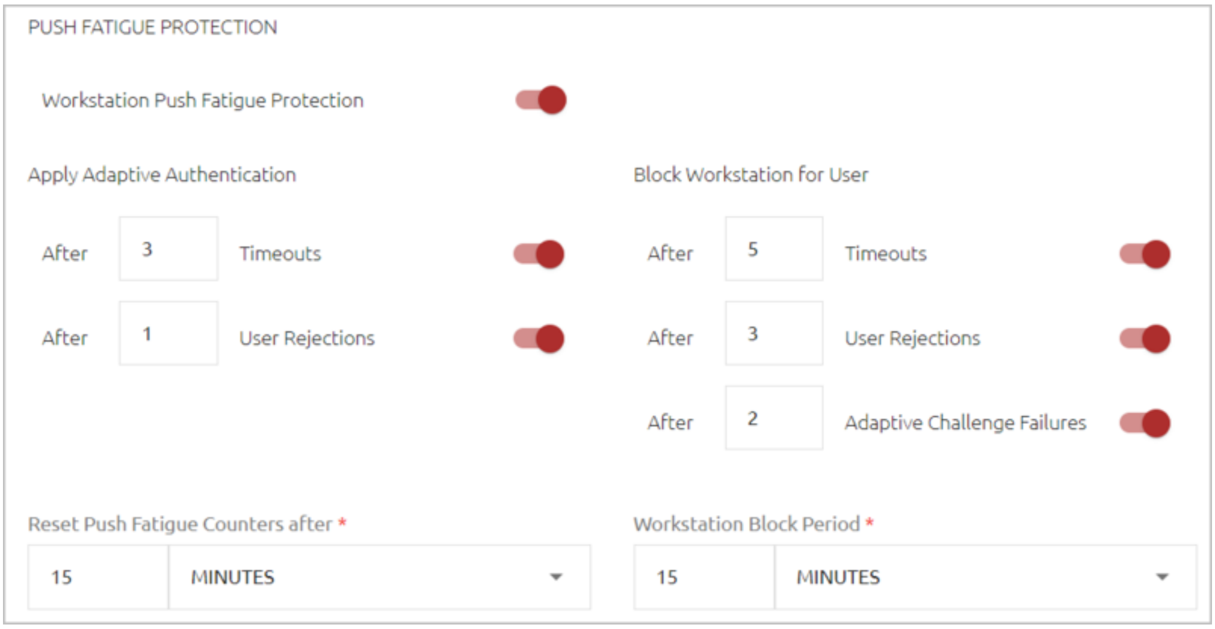
- When *upgrading* the system to these versions, the feature is disabled, to avoid interruptions in login flows. After upgrade, you can configure Adaptive Authentication settings manually, as described above.

  Following a server upgrade, users must perform a hard refresh to the browser (**Ctrl + F5**), or clear the browser cache.

### Push Fatigue Protection Settings

This feature provides an extra layer of protection for workstations targeted for push bombing attacks. When the feature is enabled, mechanisms to protect the workstation are automatically initiated when the system detects a potential push bombing event. These mechanisms become more forceful as the evidence of an attempted attack increases.

Push fatigue protection is activated and disabled by means of the **Workstation Push Fatigue Protection** toggle button.



PUSH FATIGUE PROTECTION

Workstation Push Fatigue Protection ●

Apply Adaptive Authentication

After 3 Timeouts ●

After 1 User Rejections ●

Block Workstation for User

After 5 Timeouts ●

After 3 User Rejections ●

After 2 Adaptive Challenge Failures ●

Reset Push Fatigue Counters after * 15 MINUTES

Workstation Block Period * 15 MINUTES

When push fatigue protection is enabled, you can set up one or both of the following protection mechanisms:

- **Apply Adaptive Authentication:** This mechanism works by requiring the user to provide a verification code for successful login (even when the workstation is a known device). Adaptive Authentication is applied after a specified number of timeouts (the user does not respond to the authentication request) and/or a specified number of user rejections (the user denies the authentication request).

  **IMPORTANT:** To use this mechanism, the **Adaptive Authentication** setting must be enabled.

- **Block Workstation for User:** This mechanism works by preventing the user from accessing the workstation for a configurable period of time. The block is applied after a specified number of timeouts and/or a specified number of user rejections. In addition, if Adaptive Authentication is enabled, workstation access can be denied following a specified number of adaptive challenge failures (the user provides an incorrect verification code).

The following settings are also configurable:

- **Reset Push Fatigue Counters:** The period of time (starting from the last failed / timed out authentication attempt) after which counters for timeouts, rejections and adaptive challenge failures are reset to zero. The counters are automatically reset upon a successful user login. Supported settings range from 1 minute to 48 hours (default is 15 minutes).
- **Workstation Block Period:** The period that must elapse (from the time of user lockout) before the user is authorized to log into the workstation. Supported settings range from 1 minute to 48 hours (default is 15 minutes).

After updating Push Fatigue settings, scroll to the bottom of the tab and click **Save**.

**Important**

- In *new* installations of Octopus Authentication Server versions 5.4 and higher, push fatigue protection is enabled by default.
- When *upgrading* the system to these versions, the feature is disabled, to avoid interruptions in login flows. After upgrade, you can enable the feature manually.

  Following a server upgrade, users must perform a hard refresh to the browser (**Ctrl + F5**), or clear the browser cache.

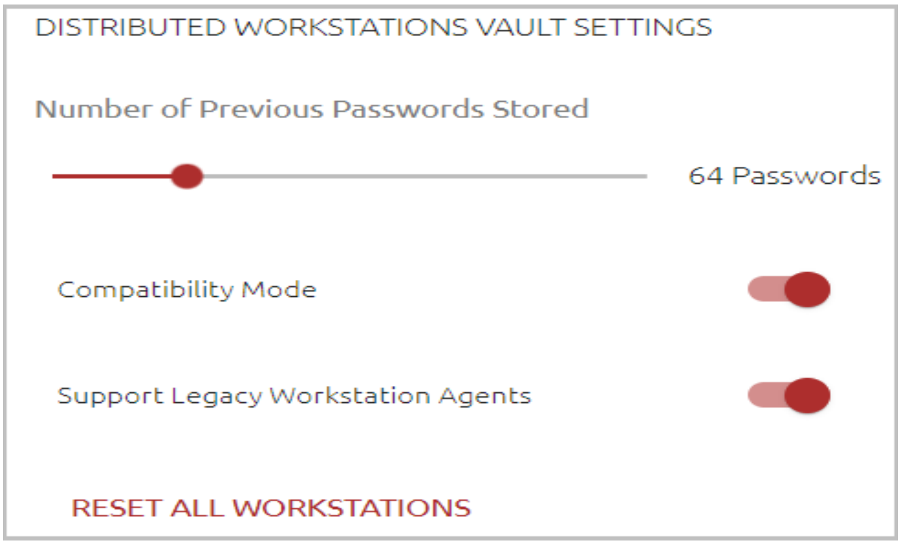
### Distributed Workstations Vault Settings

Workstations running Windows Agent version 3.3 or Mac Agent version 2.3.0 have an extra layer of encryption for communication with the Octopus Authentication Server. Besides credentials encryption, all data passed between the workstation and the Server is encrypted as well. Security keys that were generated by workstations running older versions of the Windows / Mac Agent will therefore be incompatible for workstations running Windows Agent 3.3 or Mac Agent 2.3.0.

The Distributed Workstations Vault Settings enable you to control how communications and previously used security keys are handled. The settings are:

| Setting | Description |
|---|---|
| Number of Previous Passwords Stored | The number of generated passwords stored by the server for *each* workstation, for authentication when the user is outside of the network. Valid values range from 16-256 (default = **64**). |
| Support Legacy Workstation Agents | Determines whether the system supports workstations running versions below Windows Agent version 3.3 and Mac Agent version 2.3.0. When this setting is enabled (default), these workstations continue to communicate with the server as they did previously (without data encryption).<br>The global setting defined here can be overridden for specific Active Directory Authentication services, in the Devices tab of the service settings. |

| Setting | Description |
|---|---|
| Reset All Workstations | This action deletes the history and security keys on all user workstations. (The workstations will then generate a new public key when the users next log in.)<br>The **Reset All Workstations** option is generally used following a system upgrade to Windows Agent version 3.3 or Mac Agent version 2.3.0. |



DISTRIBUTED WORKSTATIONS VAULT SETTINGS

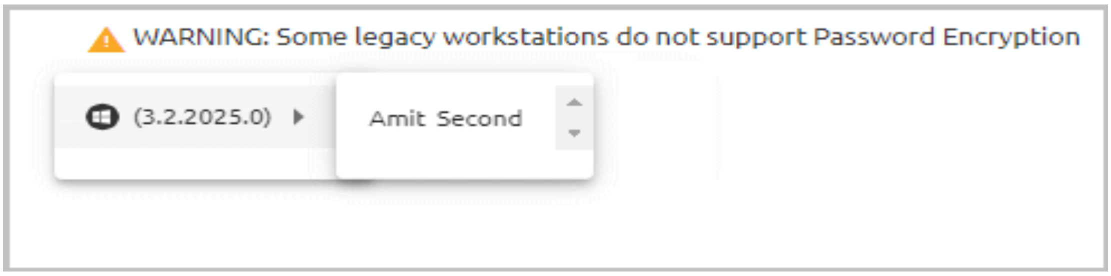
Number of Previous Passwords Stored

64 Passwords

Compatibility Mode

Support Legacy Workstation Agents

If you have legacy workstations in your system, a warning message is displayed. Clicking the warning message opens a list of these workstations. When you hover over a workstation, a list of users associated with that workstation appears.



WARNING: Some legacy workstations do not support Password Encryption

Clicking a name in the list of users opens that user's profile, where you can view detailed information about the user's parameters, devices and more.

### Understanding Compatibility Mode

In the newest versions of the Octopus mobile app and Octopus workstation agents, the Octopus Server operates using the decentralized vault concept. In this configuration, the Server continues to encrypt and store the passwords. However, since the corresponding private key is stored on the device / workstation, the Server is not able to decrypt the password. Decryption can occur only on the endpoint itself.

The decentralized vault model provides an extra layer of security, and it is the best practice method of operation. However, by default, the Server works in Compatibility Mode, to support older versions of the mobile app and workstation agents.

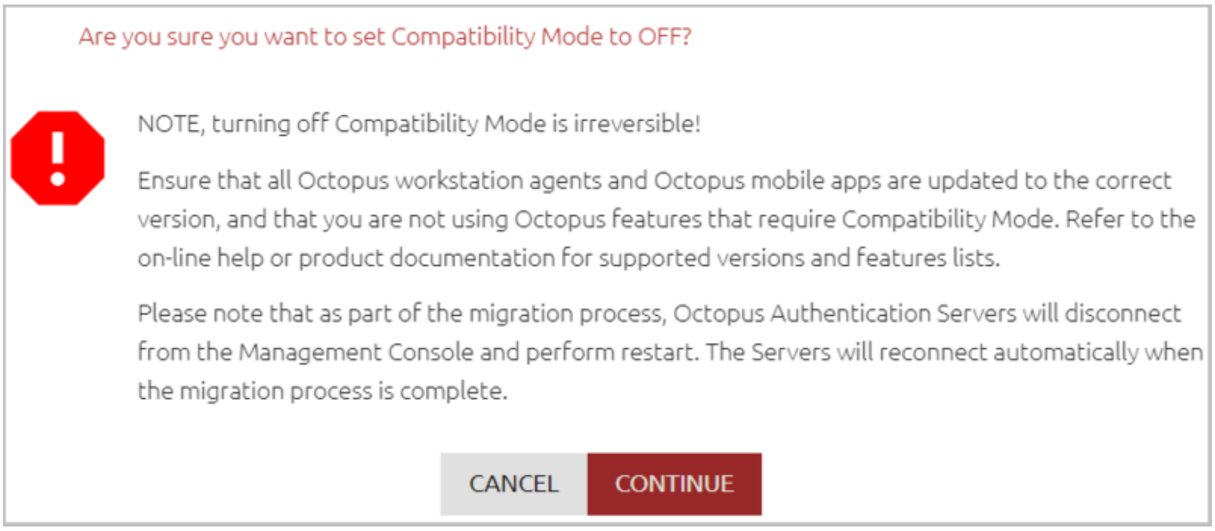
**The action of turning off Compatibility Mode cannot be reversed**. Before exiting Compatibility Mode, it is very important to properly prepare, using the following guidelines:

- Make sure that all clients are updated with these versions:
    - Octopus Desk for Windows 3.6.0 or higher
    - Octopus Desk for Mac 2.6.1 or higher
    - Octopus Authenticator App for iOS / Android 5.0 or higher
- Verify that you are not using Octopus features that require Compatibility Mode, such as:
    - LDAP services
    - Octopus Exchange Agent
    - Components (e.g., third-party authenticators) that are configured with the **Send Credentials** option

**To turn off Compatibility Mode:**

1. After verifying that you have met all requirements described above, click the **Compatibility Mode** toggle to inactivate the feature.

   A warning popup opens.



Are you sure you want to set Compatibility Mode to OFF?

NOTE, turning off Compatibility Mode is irreversible!

Ensure that all Octopus workstation agents and Octopus mobile apps are updated to the correct version, and that you are not using Octopus features that require Compatibility Mode. Refer to the on-line help or product documentation for supported versions and features lists.

Please note that as part of the migration process, Octopus Authentication Servers will disconnect from the Management Console and perform restart. The Servers will reconnect automatically when the migration process is complete.

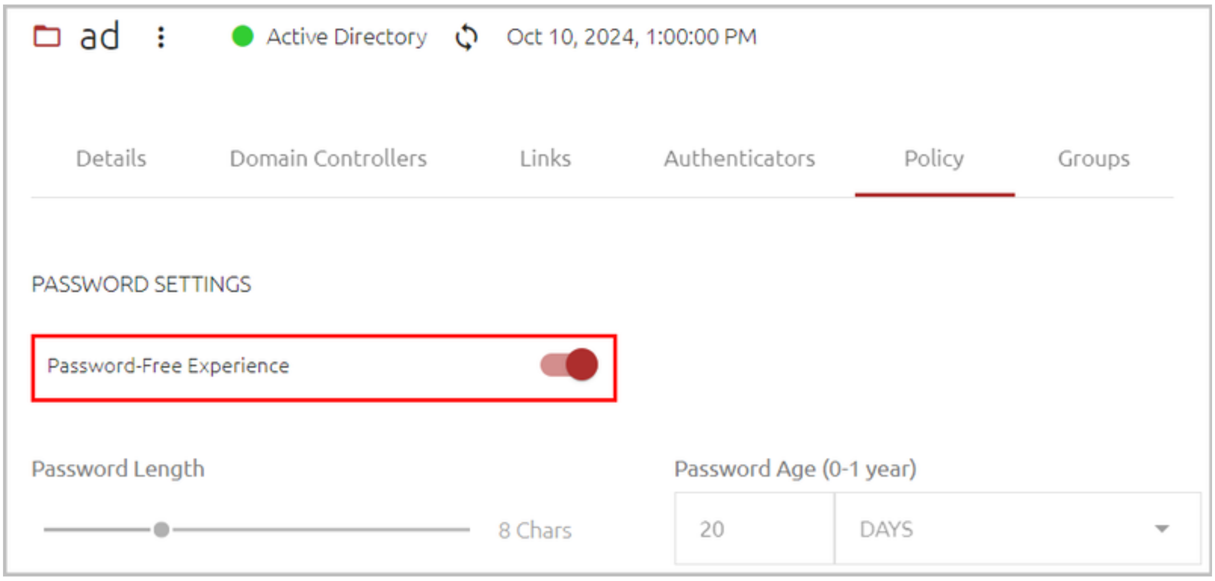
2. Click **Continue**.

   The Authentication Server(s) will temporarily disconnect during the migration process. Once Compatibility Mode is off, the actions for managing workstations are disabled.

3. If you use the Windows Agent and work with the Password Free Experience, follow these steps to enable successful authentication when Compatibility Mode is off:

a. From the **Directories** menu, open the settings of the relevant directory by clicking the Edit icon.

b. Select the **Policy** tab. At the top of the page, enable the **Password-Free Experience** toggle.



ad · Active Directory · Oct 10, 2024, 1:00:00 PM

PASSWORD SETTINGS

Password-Free Experience: on

Password Length: 8 Chars

Password Age (0-1 year): 20 DAYS

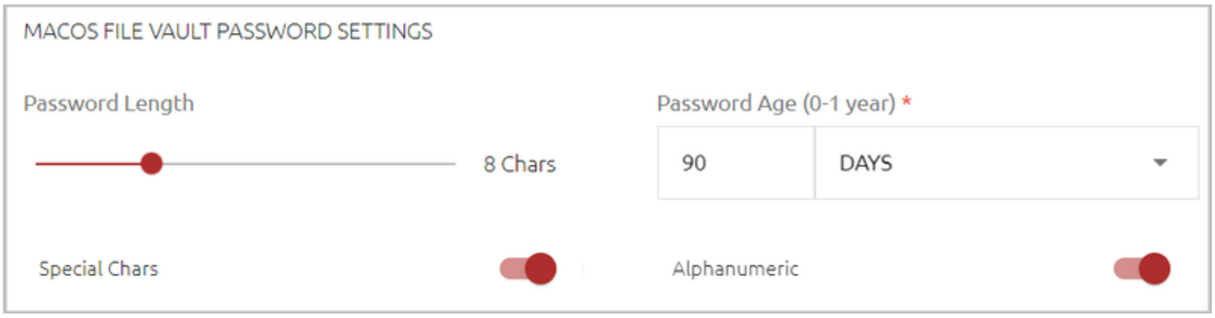
c. At the bottom of the tab, click **Save**.

**Note**

When Compatibility Mode is OFF and the Windows Agent is working in MFA mode, the **Show Credentials** feature of the Octopus mobile app may display password history incorrectly. The last (current) password is still accurate.

### macOS FileVault Password Settings

In the latest versions of Octopus Desk for Mac (2.6.1 and above), the FileVault password (which is required for passwordless authentication) is managed by the Octopus Server, instead of by the endpoint. The FileVault Password Settings enable you to manage settings related to this password.



MACOS FILE VAULT PASSWORD SETTINGS

Password Length: 8 Chars

Password Age (0-1 year) *: 90 DAYS

Special Chars: on

Alphanumeric: on

The settings are:

- **Password Length:** Number of characters in the password (4-20).

- **Password Age:** Period of time before the password expires. The maximum supported value is one year. If you enter a value of **0**, the system will **NOT** rotate the password, and the password will never expire on the Octopus Server.
- **Special Chars:** Determines whether the password must include special characters.
- **Alphanumeric:** Determines whether the password must include both letters and numbers.

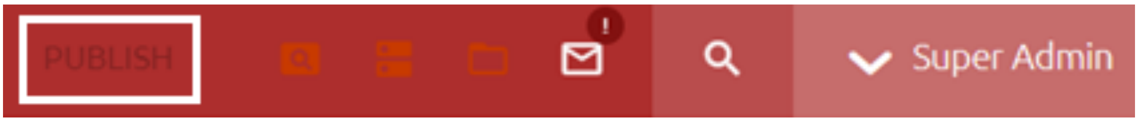
## Publishing Changes to the Database

After updating and saving settings in the Management Console, you need to publish to the database in order to update all servers (in a multiple server setup) with the changes you made. The following sections describe components and features that are available to help you manage and control the publishing process:

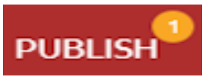
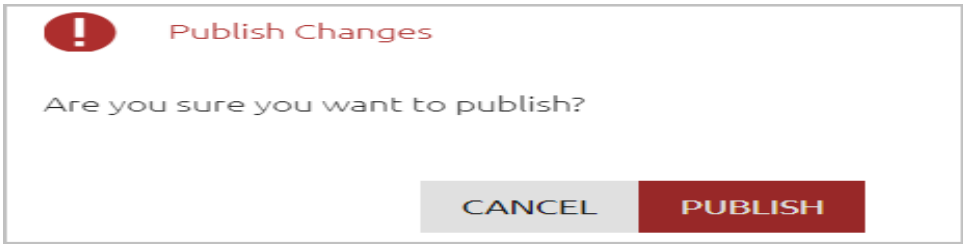
- The Toolbar PUBLISH Element
- Working with Publish Settings
- Setting a Publishing Schedule
- Viewing Your Publishing History
- Managing Publish Optimization

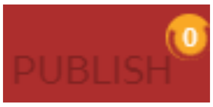
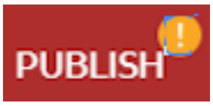
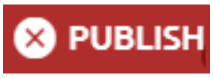
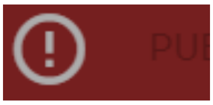
### The Toolbar PUBLISH Element

The **PUBLISH** element at the top of the Management Console shows the current status of database publication. In its default state, when there are no changes to be published, the element appears as follows:



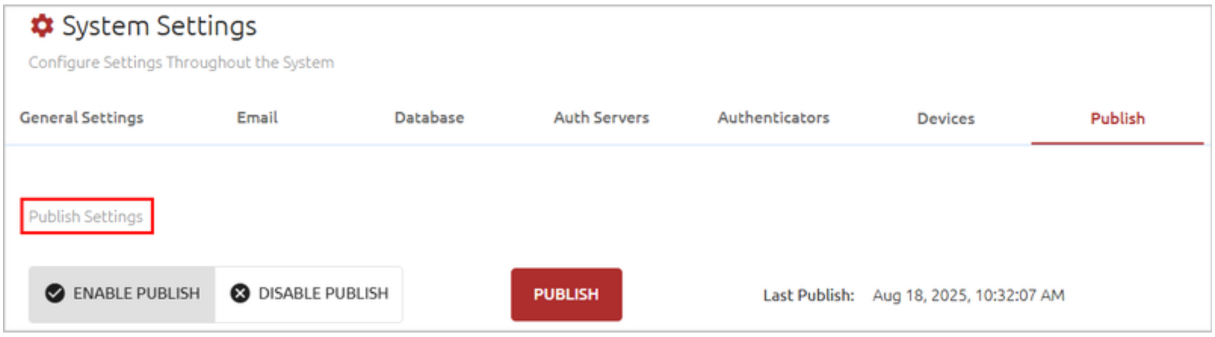
While you are working in the Management Console you may see the following different states of the **PUBLISH** element:

| State | Description |
|---|---|
|  | There are **<n>** unpublished changes. Publishing will update all servers with the changes.  To publish, click the **PUBLISH** element and then, in the confirmation popup, click **Publish**.<br><br>Publish Changes<br>Are you sure you want to publish?<br> |

| State | Description |
|---|---|
|  | Changes are currently being published. Once changes are successfully published, the **PUBLISH** element returns to its default state. |
|  | The publishing process was unsuccessful. Click the warning icon to open a list of issues that were encountered. |
|  | Publishing is disabled. For more information, refer to Working with Publish Settings (below). |
|  | The system is in a restored state. For more information, refer to Restoring the System to a Previous State. |

### Working with Publish Settings

The Publish Settings in the **Publish** tab of the **System Settings** menu allow you to force publish (by clicking the **PUBLISH** button) and disable / enable the publishing operation.



System Settings

Configure Settings Throughout the System

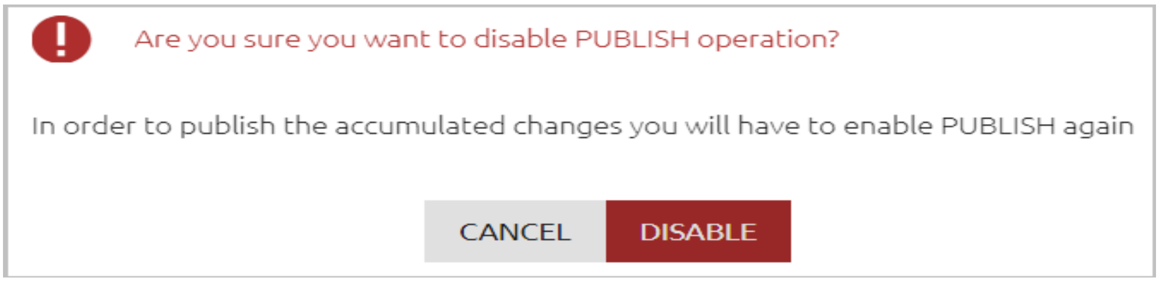
Last Publish: Aug 18, 2025, 10:32:07 AM

When publishing is disabled, you may continue to update settings in the Management Console, but the changes cannot be published until the publishing operation is reactivated.

**To disable publishing:**

1. At the top of the **Publish** tab, click **Disable Publish.**

   A confirmation popup opens.

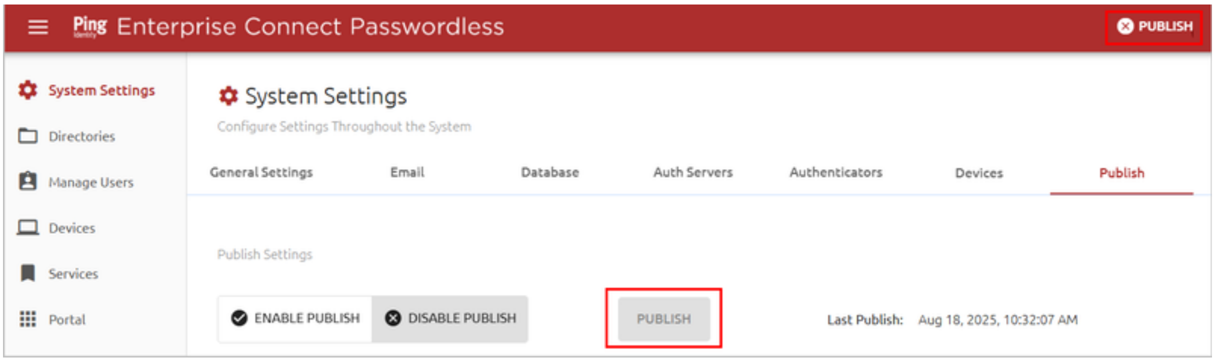
   

   Are you sure you want to disable PUBLISH operation?

   In order to publish the accumulated changes you will have to enable PUBLISH again

2. Click **Disable.**

   The **PUBLISH** button is disabled, and an alert icon appears next to the **PUBLISH** element in the toolbar.



Last Publish: Aug 18, 2025, 10:32:07 AM

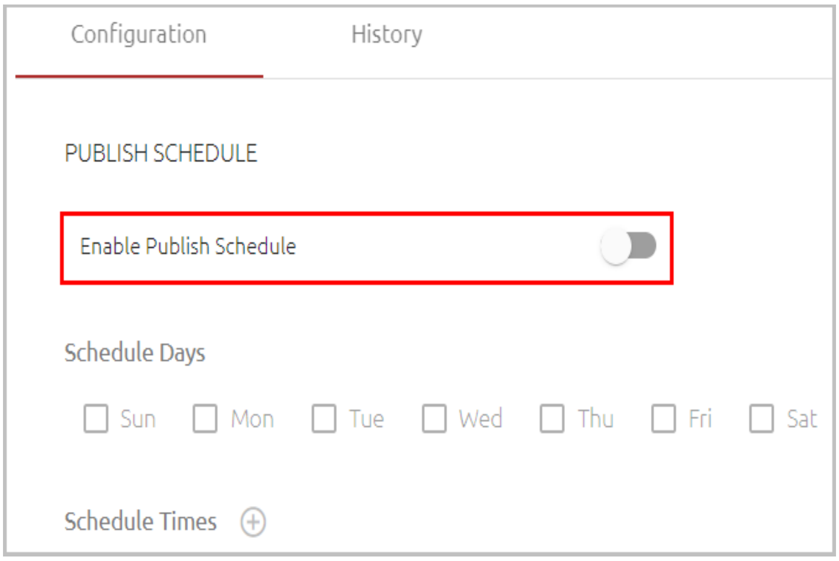
3. To reactivate the publishing operation, click **Enable Publish**. Then, to publish accumulated changes, click **PUBLISH**.

### Setting a Publishing Schedule

The **Configuration** sub-tab allows you to set a schedule specifying days and times when all changes are automatically published to the database.

**To set a publishing schedule:**

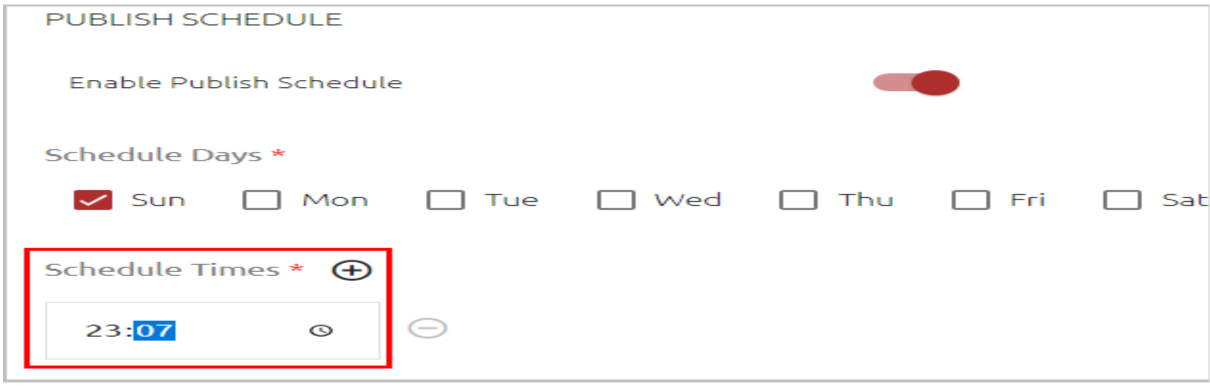
1. From the **Configuration** sub-tab of the **Publish** tab, click the **Enable Publish Schedule** toggle button.



The Schedule options below are enabled.

2. Specify the day(s) on which you want automatic publishing to take place by selecting the relevant checkbox(es).

3. Specify the time(s) at which the publish operation will take place:
   - To add a time, click ⊕.
   - To remove a time, click ⊖.
   - To edit an existing time, click the hour or minute value and enter a new value.



PUBLISH SCHEDULE

Enable Publish Schedule

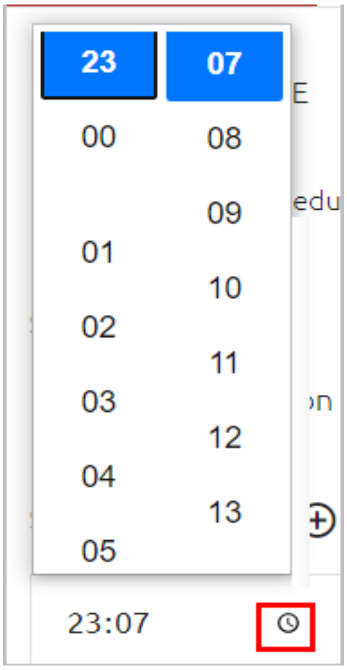
Schedule Days *

☑ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Schedule Times *

23:07

Alternatively, click the Clock icon and then select a new time from the time picker that opens.



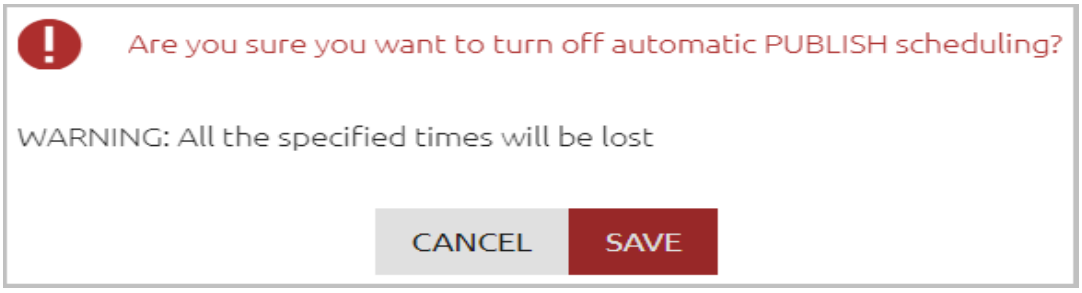
4. When you are finished setting the schedule, click **Save**.

You may discontinue automatic publishing at any time. However, keep in mind that when automatic publishing is stopped, the schedule is not saved and you will need to recreate one if you resume automatic publishing.

**To discontinue automatic publishing:**

1. Click the **Enable Publish Schedule** toggle, and then click **Save**.

   A warning popup opens.



Are you sure you want to turn off automatic PUBLISH scheduling?

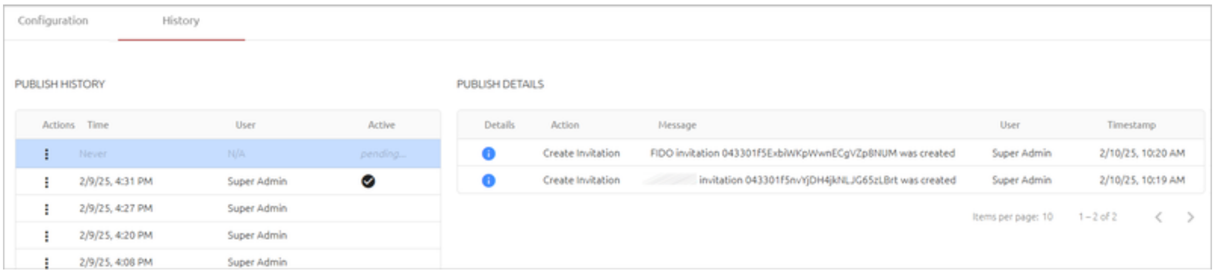
WARNING: All the specified times will be lost

2. From the popup, click **Save**.

**Viewing Your Publishing History**

The **History** sub-tab of the **Publish** tab displays a list of publish operations that have taken place and the initiator of each operation (system, username, etc.). The publish operation that reflects the current state of the database is indicated by a ✓ icon in the **Active** column.

By default, the **Publish Details** pane displays a list of all currently unpublished changes. Clicking a row in the **Publish History** list changes the display to list all changes included in the selected publish operation.



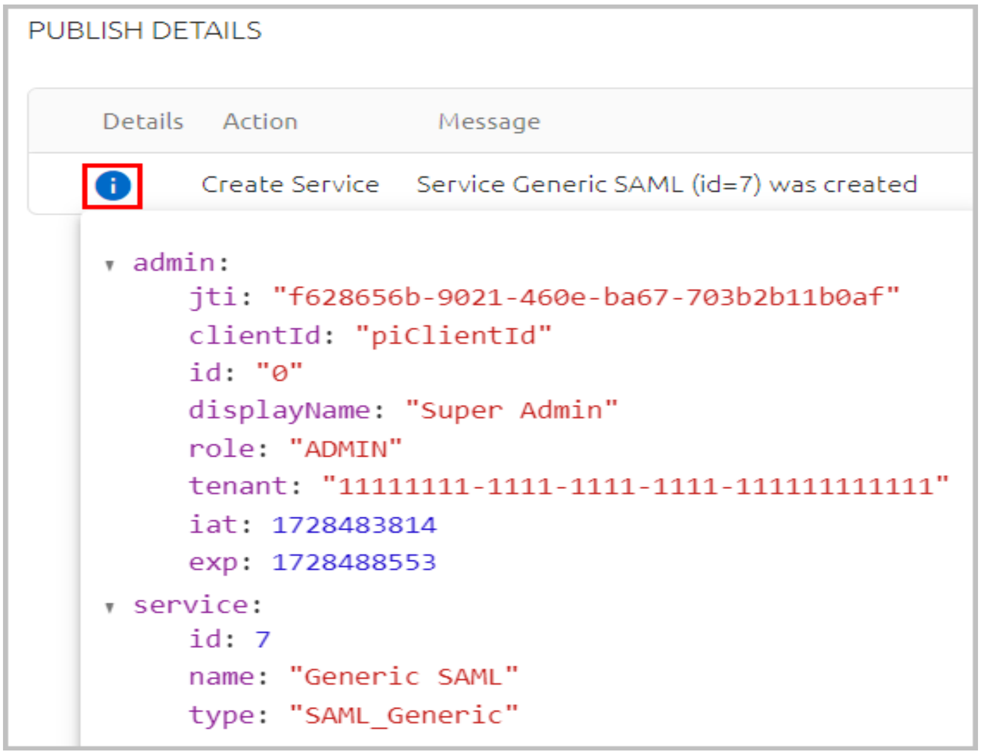
PUBLISH HISTORY

| Actions | Time | User | Active |
|---|---|---|---|
| ⋮ | Never | N/A | pending... |
| ⋮ | 2/9/25, 4:31 PM | Super Admin | ✓ |
| ⋮ | 2/9/25, 4:27 PM | Super Admin | |
| ⋮ | 2/9/25, 4:20 PM | Super Admin | |
| ⋮ | 2/9/25, 4:08 PM | Super Admin | |

PUBLISH DETAILS

| Details | Action | Message | User | Timestamp |
|---|---|---|---|---|
| ⓘ | Create Invitation | FIDO invitation 043301f5ExbiWKpWwnECgVZpBNUM was created | Super Admin | 2/10/25, 10:20 AM |
| ⓘ | Create Invitation | [redacted] invitation 043301f5nvYjDH4jkNLJG65zLBrt was created | Super Admin | 2/10/25, 10:19 AM |

The **Publish Details** list provides a summary of every action that was published in the selected publish operation. To view more details about an action, click ⓘ.



PUBLISH DETAILS

| Details | Action | Message |
|---|---|---|
| ⓘ | Create Service | Service Generic SAML (id=7) was created |

```
▾ admin:
     jti: "f628656b-9021-460e-ba67-703b2b11b0af"
     clientId: "piClientId"
     id: "0"
     displayName: "Super Admin"
     role: "ADMIN"
     tenant: "11111111-1111-1111-1111-111111111111"
     iat: 1728483814
     exp: 1728488553
▾ service:
     id: 7
     name: "Generic SAML"
     type: "SAML_Generic"
```

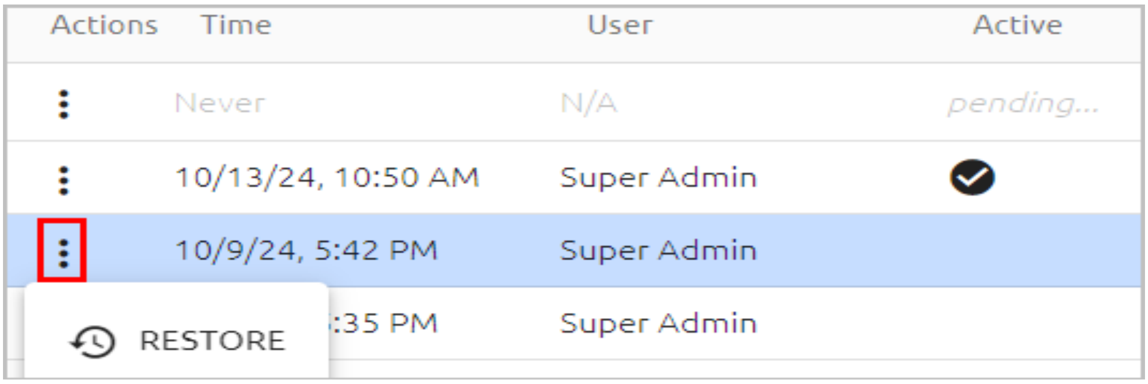
### Restoring the System to a Previous Publish State

Generally, the most recent publish operation is the one that is currently Active. However, if required (e.g., you inadvertently published unsuitable changes) you can restore a previous publish operation, so the system can continue to operate smoothly.

Keep in mind that restoring a previous publish state changes the content in the database, but it does **not** reverse any changes made in the Management Console. Therefore, after performing a Restore operation, you need to manually make relevant changes and updates in the Management Console and then publish those changes.

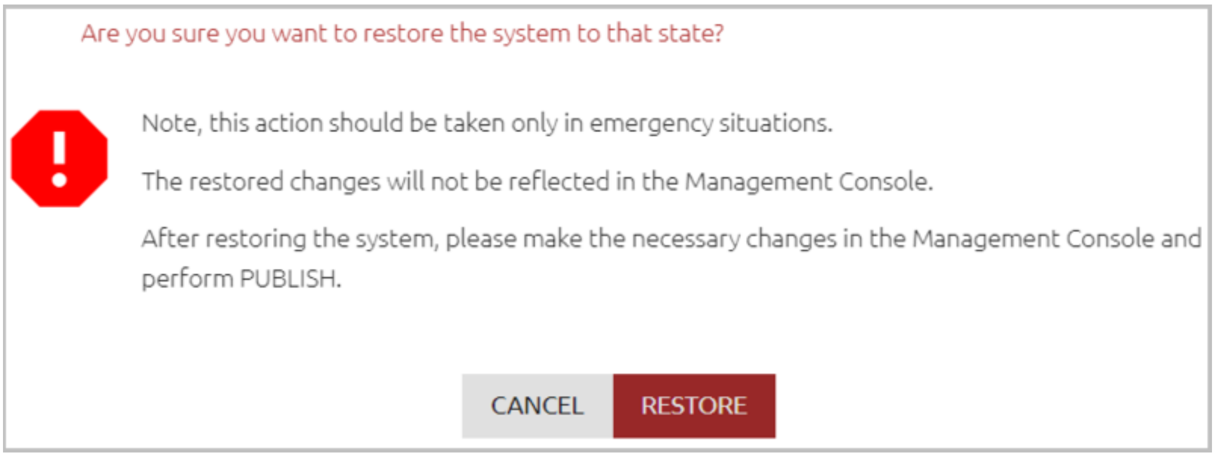
**To restore to a previous publish state:**

1. From the **Publish History** list, in the row of the publish operation that you want to restore, click ⋮ and select **Restore**.



| Actions | Time | User | Active |
|---|---|---|---|
| ⋮ | Never | N/A | *pending...* |
| ⋮ | 10/13/24, 10:50 AM | Super Admin | ✓ |
| ⋮ | 10/9/24, 5:42 PM | Super Admin | |
| | :35 PM | Super Admin | |

A confirmation popup opens.



Are you sure you want to restore the system to that state?

Note, this action should be taken only in emergency situations.

The restored changes will not be reflected in the Management Console.

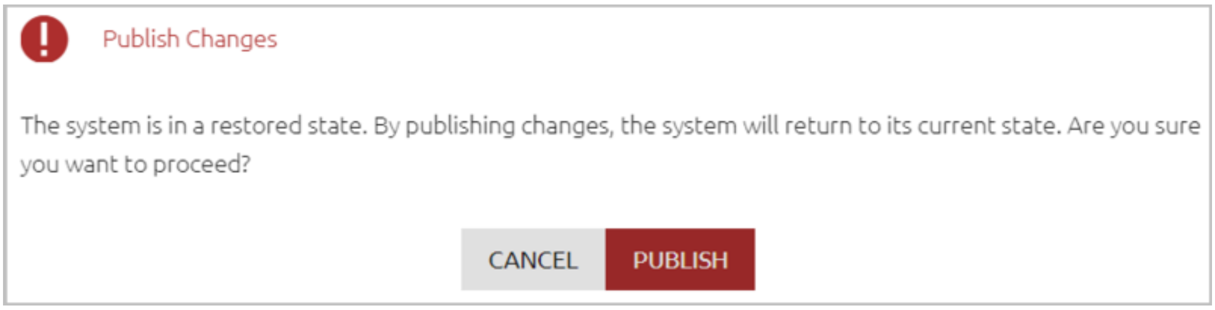
After restoring the system, please make the necessary changes in the Management Console and perform PUBLISH.

2. Click **Restore**.

   The selected publish operation is marked as the Active one, and an alert icon appears next to the toolbar **PUBLISH** element.

3. Make the necessary changes in the Management Console. Then, navigate to **System Settings > Publish** and click the **PUBLISH** button.

   A confirmation popup opens.



Publish Changes

The system is in a restored state. By publishing changes, the system will return to its current state. Are you sure you want to proceed?

4. To publish your changes and exit Restore mode, click **Publish**.

### Managing Publish Optimization

By default, the publish operation updates the database only with changes that affect users who are assigned to at least one service. This behavior, which is called *publish optimization*, significantly reduces publishing time. However, the optimization flow can interfere with smooth enrollment of users who are not yet assigned to any services.

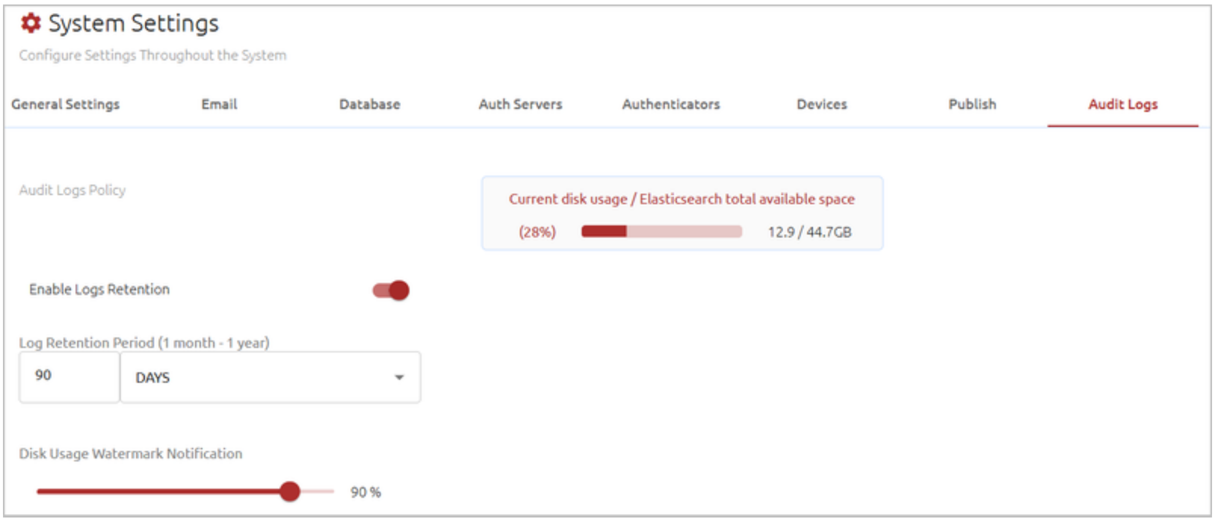
If you prefer not to use publish optimization, you can disable it by editing (or adding) the *disablePublishOptimization* parameter in the following configuration file: **/opt/sdo/mcbackendsql/config/envs/production.json**

Verify that the parameter is set to *True*. The syntax should be as follows:

```
"disablePublishOptimization" : "True",
```

### Configuring Audit Logs Settings

The **Audit Logs** tab provides information about the amount of accumulated records in storage and allows you to set the time period for which logs are retained in the system. To open the tab, select **System Settings > Audit Logs**.



Current disk usage / Elasticsearch total available space
(28%) 12.9 / 44.7GB

Enable Logs Retention ●

Log Retention Period (1 month - 1 year)
90 DAYS

Disk Usage Watermark Notification
90 %

The following features are provided to help you manage storage space on the Elasticsearch disk:

- **Log Retention:** Allows you to specify the period of time (ranging from one month to one year) for which logs are saved. When the time period elapses, older records are automatically deleted to save disk space. For example, if the Log Retention Period is 30 days, only records from the most recent 30 days are saved.

  To use the Log Retention feature, verify that the **Enable Logs Retention** toggle is enabled. Set the **Log Retention Period** in the fields below, and then click **Save**.

- **Disk Usage Watermark Notification:** This setting is the storage limit (in percent disk space) at which a notification is automatically emailed to the system admin. For example, if the value is 80, an email is sent when the disk space is 80% full.

  To configure the setting, drag the slider to the required value and then click **Save**.

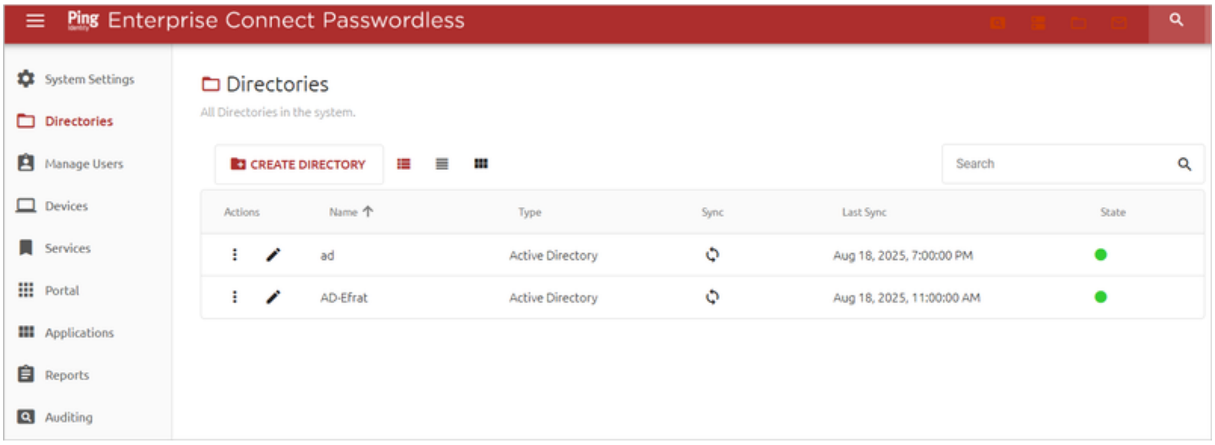
- **Elasticsearch Disk Usage:** This value, which is calculated daily, is the amount of disc space that is currently occupied. The percentage is based on the amount of space being used relative to the amount of space required to contain data for the entire retention period specified (as displayed on the right side of the bar).

## Directory Integration

The Management Console supports integration with Active Directory, Entra ID, ForgeRock, ForgeRock Cloud, Oracle/Open LDAP and Google. You can configure integration with more than one directory type.

Directory integration provides the admin with simple user management capabilities when users are synced directly from one of the selected directory types. For example, when integration is done with an Active Directory (AD), all user and group management can be done directly in the AD, and the changes are then synced to the Authentication Server.

The **Directories** menu of the Management Console lists all integrated corporate directories and displays general information about each one.



Directories

All Directories in the system.

| Actions | Name ↑ | Type | Sync | Last Sync | State |
|---|---|---|---|---|---|
| ⋮ ✎ | ad | Active Directory | ⟳ | Aug 18, 2025, 7:00:00 PM | ● |
| ⋮ ✎ | AD-Efrat | Active Directory | ⟳ | Aug 18, 2025, 11:00:00 AM | ● |

The following topics present details about working with directories:

- Adding a New Directory
- Viewing and Managing Directories
- Creating Directory Links
- Configuring Directory Authentication Options and Settings
- Configuring Directory Policy Settings
- Working with Selective Syncing

## Adding a New Directory

The Management Console supports integration with multiple directory types. When adding directories, keep the following points in mind:

- Upon creating a directory, you will need to decide whether or not to enable automatic directory syncing. When this feature is enabled, Groups and users are synced automatically with the directory, and the users list is updated regularly according to the schedule that you specify as part of the directory's settings. If you add an Active Directory or Azure AD directory type, you can choose only specific Groups for automatic syncing (other Groups will need to be imported manually). For more details, refer to Working with Selective Syncing.

  When automatic directory syncing is NOT enabled, after adding the directory you will need to select users from the folders within the directory and manually import them.

- If you integrate multiple directories that contain one or more identical user objects, the Authentication Server will work with the settings of the user object that is enabled. In the event that a user is enabled in two (or more) directories, the Authentication Server will select the directory that was integrated with Enterprise Connect Passwordless first.

The following sections describe how to add:

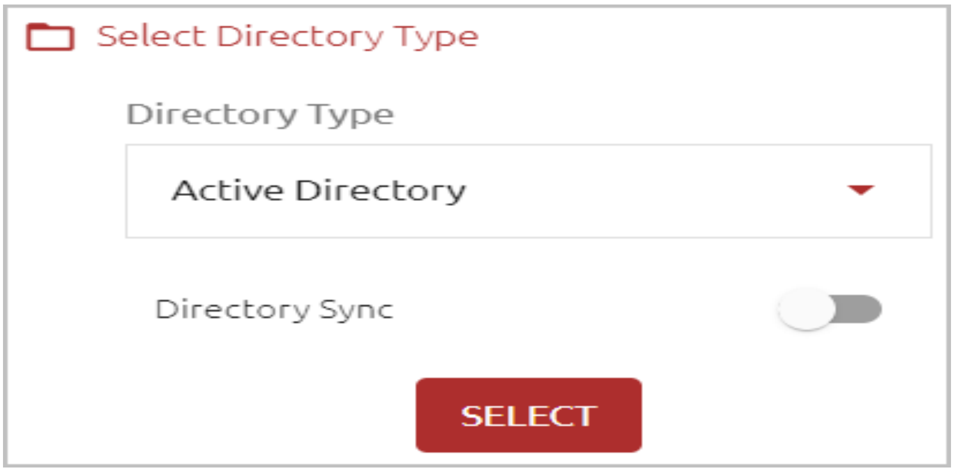
- AD, Oracle/Open LDAP and ForgeRock directories
- ForgeRock Cloud directories
- Entra ID directories
- Google directories

### AD, Oracle/Open LDAP and ForgeRock

**To add a new Active Directory, Oracle/Open LDAP or ForgeRock directory:**

1. At the top of the **Directories** menu, click **Create Directory**.

   The **Select Directory Type** dialog opens.



Select Directory Type

Directory Type

Active Directory

Directory Sync

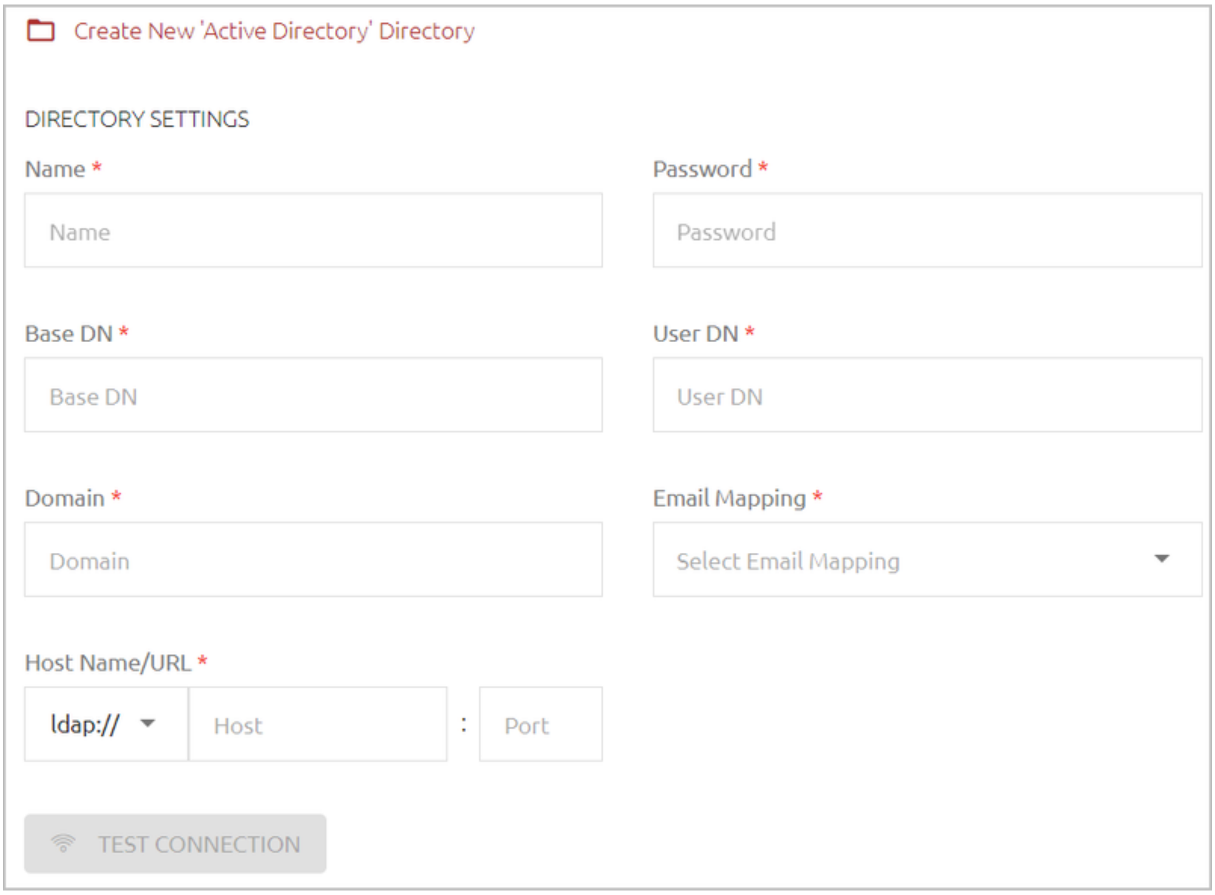
2. Open the **Directory Type** list and select the type of directory that you want to add.
3. Click the **Directory Sync** toggle button to enable and disable automatic syncing.

**Important**

You will NOT be able to change this setting after adding the directory.

4. Click **Select**.

   The **Create New Directory** page opens. For example:



5. Configure the following Directory Settings:

   ○ **Name:** Name by which the directory is known.

   ○ **Password:** The password for the  administrative user account.

   ○ **Base DN:** The distinguished name of the directory from which users will be added to Octopus Authenticator. If you want to add only a specified set of users, enter the relevant node(s) of the directory.

   ○ **User DN:** The username and distinguished name of the administrative user account that allows access to import from the directory.

   ○ **Domain:** The IP address or NetBIOS domain name of the domain.

> **Note**
>
> **For AD only:** A domain value must be entered in order to enable users to authenticate to Windows using a FIDO key.

   ○ **Email Mapping:** The field in the corporate directory used to retrieve the emails of users. Select the mapping source from the list. Keep in mind that you will NOT be able to update the mapping source after directory settings are saved.

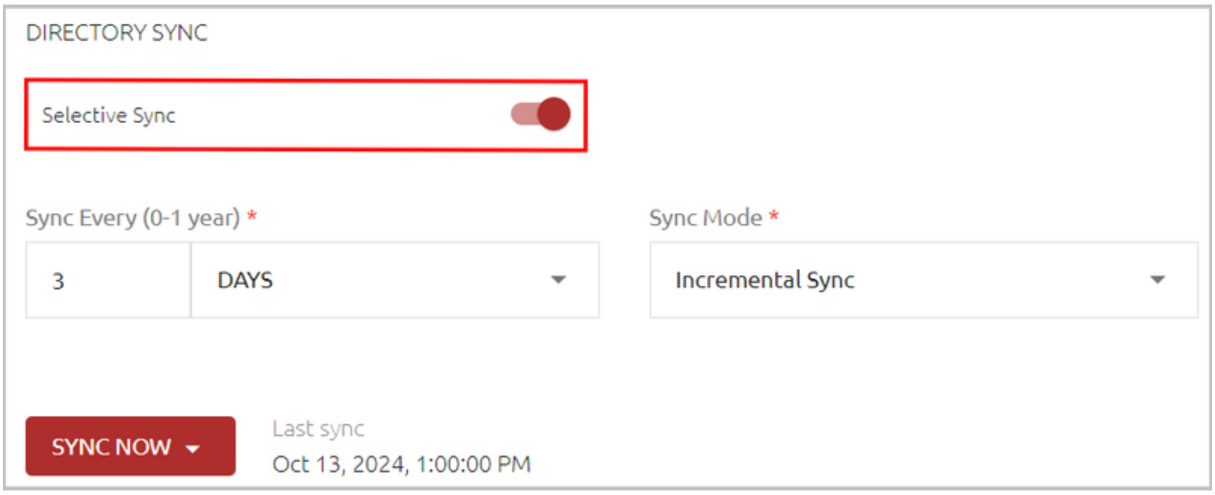
   ○ **Host Name/URL:** Select LDAP or LDAPS. Then, in the **Host** field, enter the FQDN of the domain. In the **Port** field, enter **389** for LDAP or **636** for LDAPS.

- **Certificate:** If you are using LDAPS, click **Upload Certificate** and select the relevant certificate file.

6. Click **Test Connection** to perform a validity check.
7. At the bottom of the page, click **Create**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.
8. **For AD directory types with Automatic Sync**, it is recommended to enable Selective Sync in the directory settings:

   a. From the **Directories** menu, click ✎ in the row or tile of the relevant directory to open the directory settings.

   b. Scroll to the bottom of the **Details** tab. Under **Directory Sync**, enable the **Selective Sync** toggle button.



DIRECTORY SYNC

Selective Sync ●

Sync Every (0-1 year) *: 3 DAYS

Sync Mode *: Incremental Sync

Last sync
Oct 13, 2024, 1:00:00 PM

   c. Click **Save**.

> **Note**
>
> For more information about Selective Sync, refer to Working with Selective Syncing.

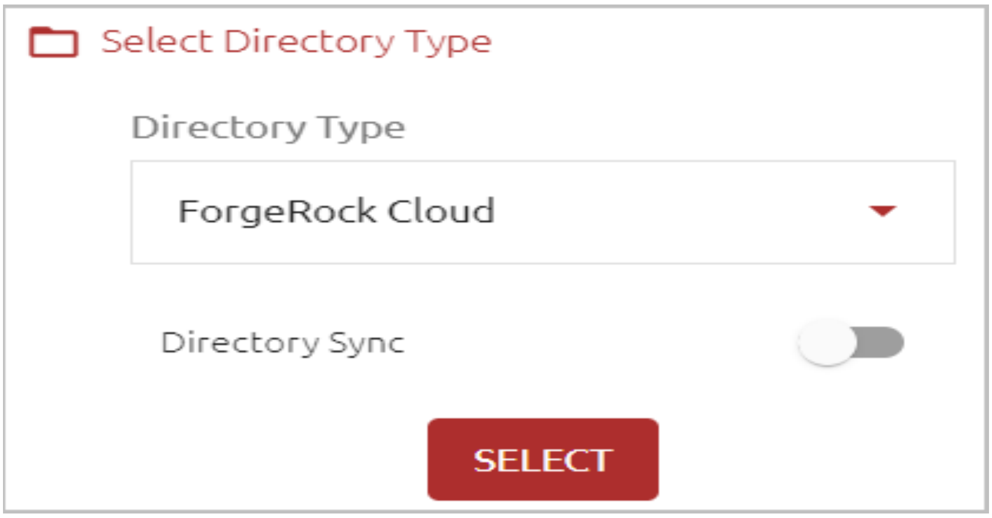
**ForgeRock Cloud**

**To add a new ForgeRock Cloud directory:**

1. At the top of the **Directories** menu. click **Create Directory**.

   The **Select Directory Type** dialog opens.

2. Open the **Directory Type** list and select **ForgeRock Cloud**.



Select Directory Type

Directory Type

ForgeRock Cloud

Directory Sync

3. Click the **Directory Sync** toggle button to enable and disable automatic syncing.

> **Important**
>
> You will NOT be able to change this setting after adding the directory.

4. Click **Select**.

   The **Create New Directory** page opens.

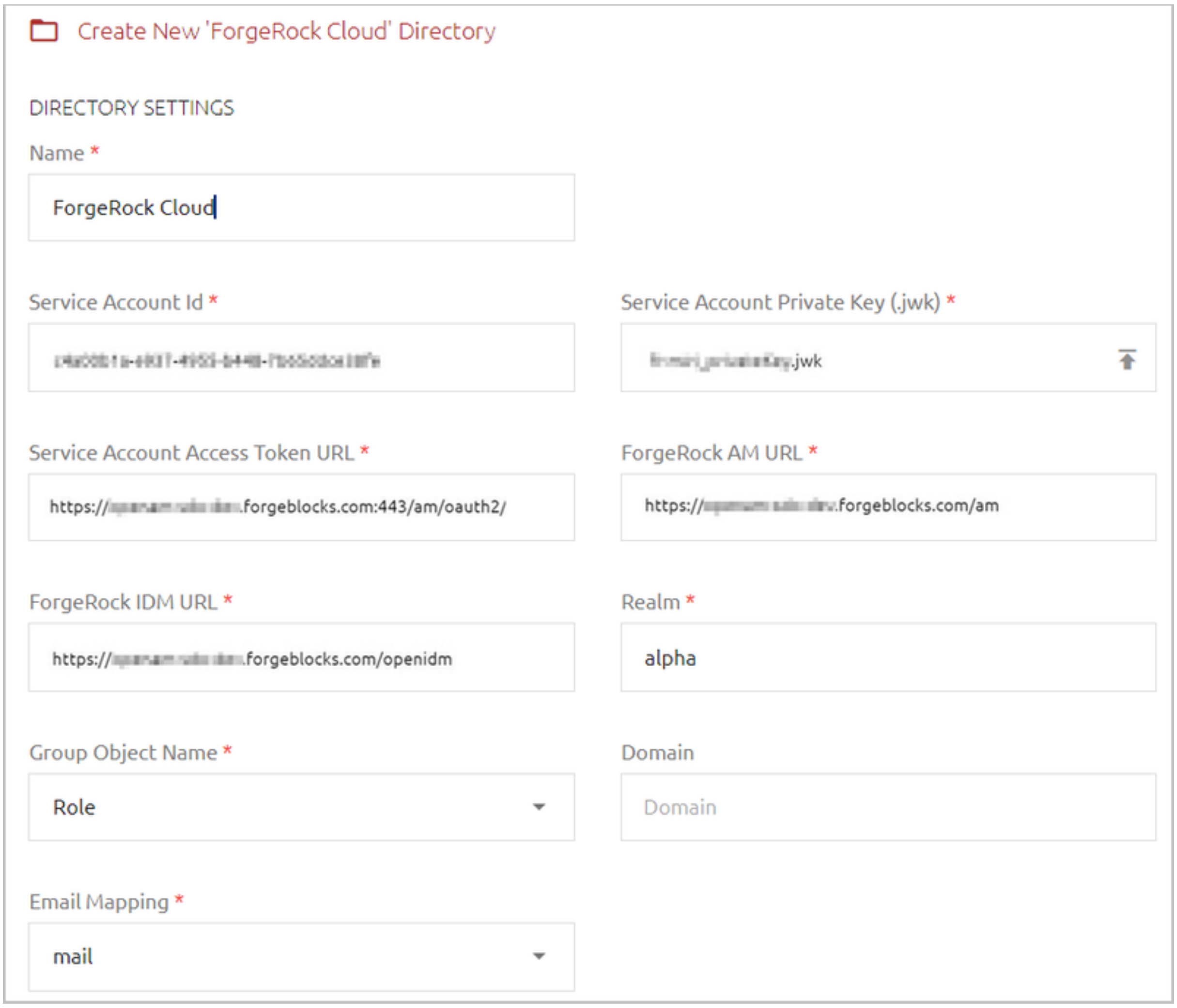
5. Configure the following directory settings:

   - **Name:** Name by which the directory is known.
   - **Service Account Id:** Copy this value from the **Service Accounts** page of the ForgeRock Identity Cloud Admin UI (under **Tenant Settings**).
   - **Service Account Private Key:** Copy this value from the **Service Accounts** page of the ForgeRock Identity Cloud Admin UI (under **Tenant Settings)**.
   - **Service Account Access Token URL:** Enter the Oauth2 access token URL in the following format:

     *https://<tenant-env-fqdn>:443/am/oauth2/access_token*

     For further information please refer to this article.
   - **ForgeRock AM URL:** The public AM URL.
   - **ForgeRock IDM URL:** The public IDM URL.
   - **Realm:** The IDM realm being used.
   - **Group Object Name:** Use the value set in your ForgeRock environment. (The default setting is **Role**.)
   - **Email Mapping:** The field in the corporate directory used to retrieve the emails of users. Select the mapping source from the list. Keep in mind that you will NOT be able to update the mapping source after directory settings are saved.

For example:



Create New 'ForgeRock Cloud' Directory

DIRECTORY SETTINGS

Name * ForgeRock Cloud

Service Account Id * [redacted]

Service Account Private Key (.jwk) * [redacted].jwk

Service Account Access Token URL * https://[redacted].forgeblocks.com:443/am/oauth2/

ForgeRock AM URL * https://[redacted].forgeblocks.com/am

ForgeRock IDM URL * https://[redacted].forgeblocks.com/openidm

Realm * alpha

Group Object Name * Role

Domain

Email Mapping * mail

6. Click **Test Connection** to perform a validity check.
7. At the bottom of the page, click **Create**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

### Entra ID

The platform supports two kinds of Entra ID directory types. Both types enable integration of users in Entra ID directories.

| Directory Type | Description / Requirements |
|---|---|
| Entra ID | Uses the Microsoft Graph API. Does not require LDAP or P1 Entra ID license.<br>This directory type supports O-365 federation with Enterprise Connect Passwordless while using Entra ID. |
| Entra ID (LDAP) | Uses the LDAP API, which requires a P1 Entra ID license. |

**Important**

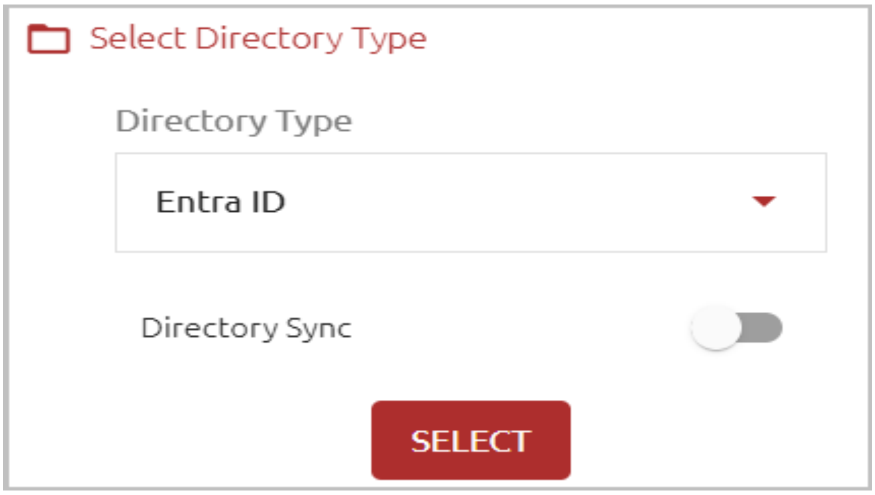
Migration from an Azure AD directory type to an Entra ID directory type is not supported. It is also not possible to migrate from an Entra ID directory type to an Entra ID (LDAP) directory type, or vice versa.

### To add a new Entra ID directory (Graph API):

1. At the top of the **Directories** menu, click **Create Directory**.

   The **Select Directory Type** dialog opens.

2. Open the **Directory Type** list and select **Entra ID**.



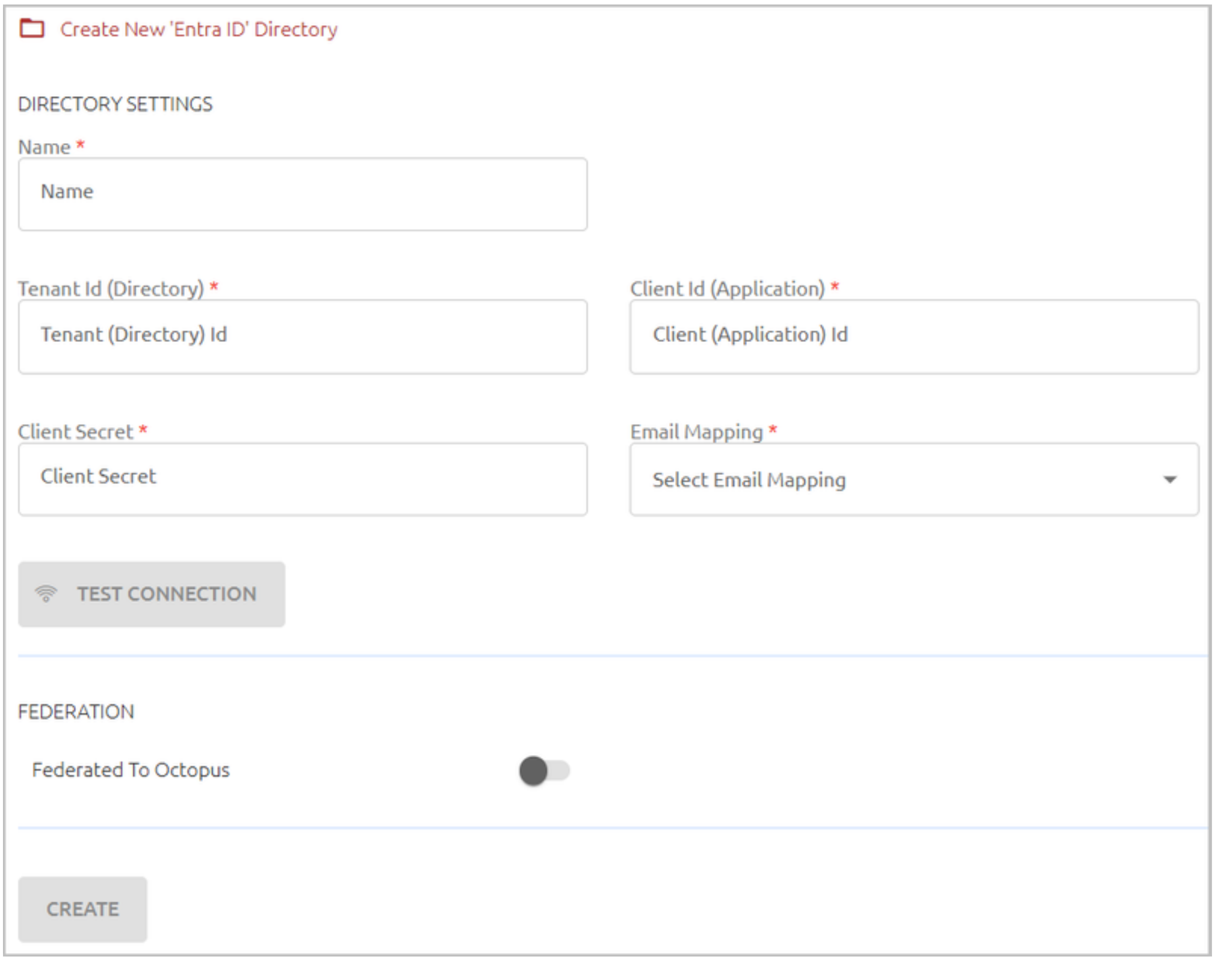
3. Click the **Directory Sync** toggle button to enable and disable automatic syncing.

**Important**

You will NOT be able to change this setting after adding the directory.

4. Click **Select**.

   The **Create New Directory** page opens.



Create New 'Entra ID' Directory

DIRECTORY SETTINGS

Name * : Name

Tenant Id (Directory) * : Tenant (Directory) Id

Client Id (Application) * : Client (Application) Id

Client Secret * : Client Secret

Email Mapping * : Select Email Mapping

FEDERATION

Federated To Octopus

5. Configure the following Directory Settings:
   - **Name:** Name by which the directory is known.
   - **Tenant ID (Directory)** and **Client ID (Application)**: Copy these values from your Entra ID application. (They are displayed in **App Registrations** under the relevant app.)
   - **Client Secret:** Copy the *Secret Value only* (NOT the Secret ID) from your Entra ID application after creating the secret. (To create the secret, navigate to **Certificates and Secrets**, click **New Client Secret** and name the new secret.)
   - **Email Mapping:** The field in the corporate directory used to retrieve the emails of users. Select the mapping source from the list. Keep in mind that you will NOT be able to update the mapping source after directory settings are saved.
6. Click **Test Connection** to perform a validity check.
7. If you have a federated Entra ID domain, select the **Federated To Octopus** toggle button to enable the setting.

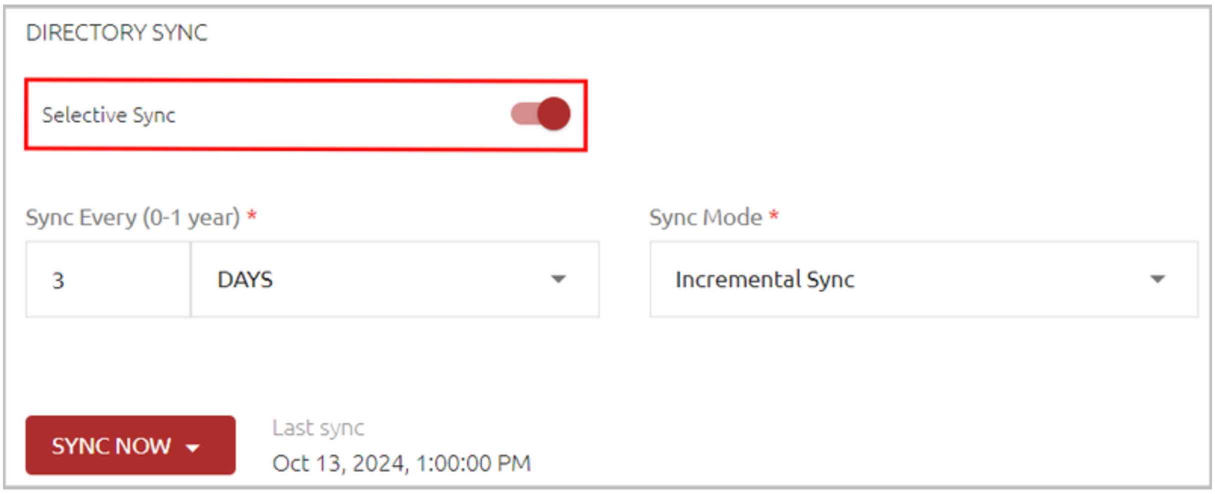
When this setting is enabled, you will be able to add users directly to the remote Entra ID directory, and then import or synchronize them into the Octopus platform.

8. At the bottom of the page, click **Create**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

9. **For directories with Automatic Sync**, it is recommended to enable Selective Sync in the directory settings:

   a. From the **Directories** menu, click ✎ in the row or tile of the relevant directory to open the directory settings.

   b. Scroll to the bottom of the **Details** tab. Under **Directory Sync**, enable the **Selective Sync** toggle button.



DIRECTORY SYNC

Selective Sync ●

Sync Every (0-1 year) * 3 DAYS

Sync Mode * Incremental Sync

Last sync Oct 13, 2024, 1:00:00 PM

   c. Click **Save**.

**Note**

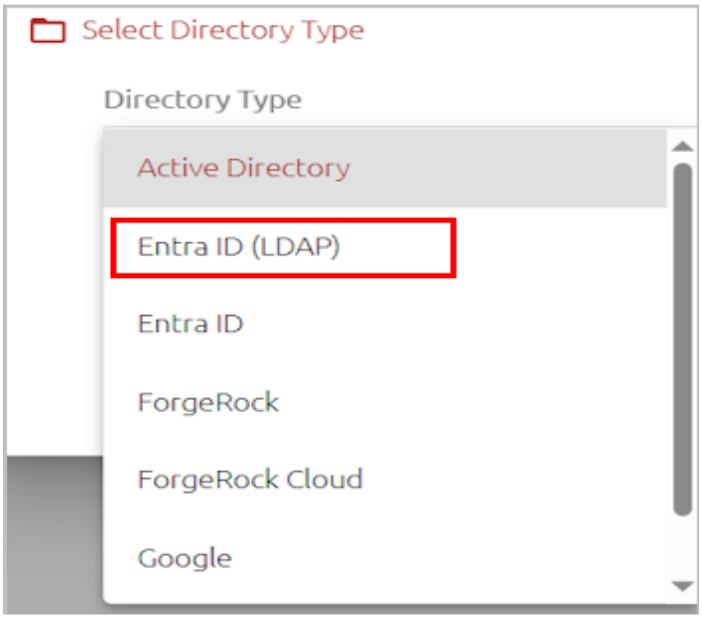
For more information about Selective Sync, refer to Working with Selective Syncing.

### To add a new Entra ID (LDAP) directory:

1. At the top of the **Directories** menu, click **Create Directory**.

   The **Select Directory Type** dialog opens.

2. Open the **Directory Type** list and select **Entra ID (LDAP)**.



Select Directory Type

Directory Type

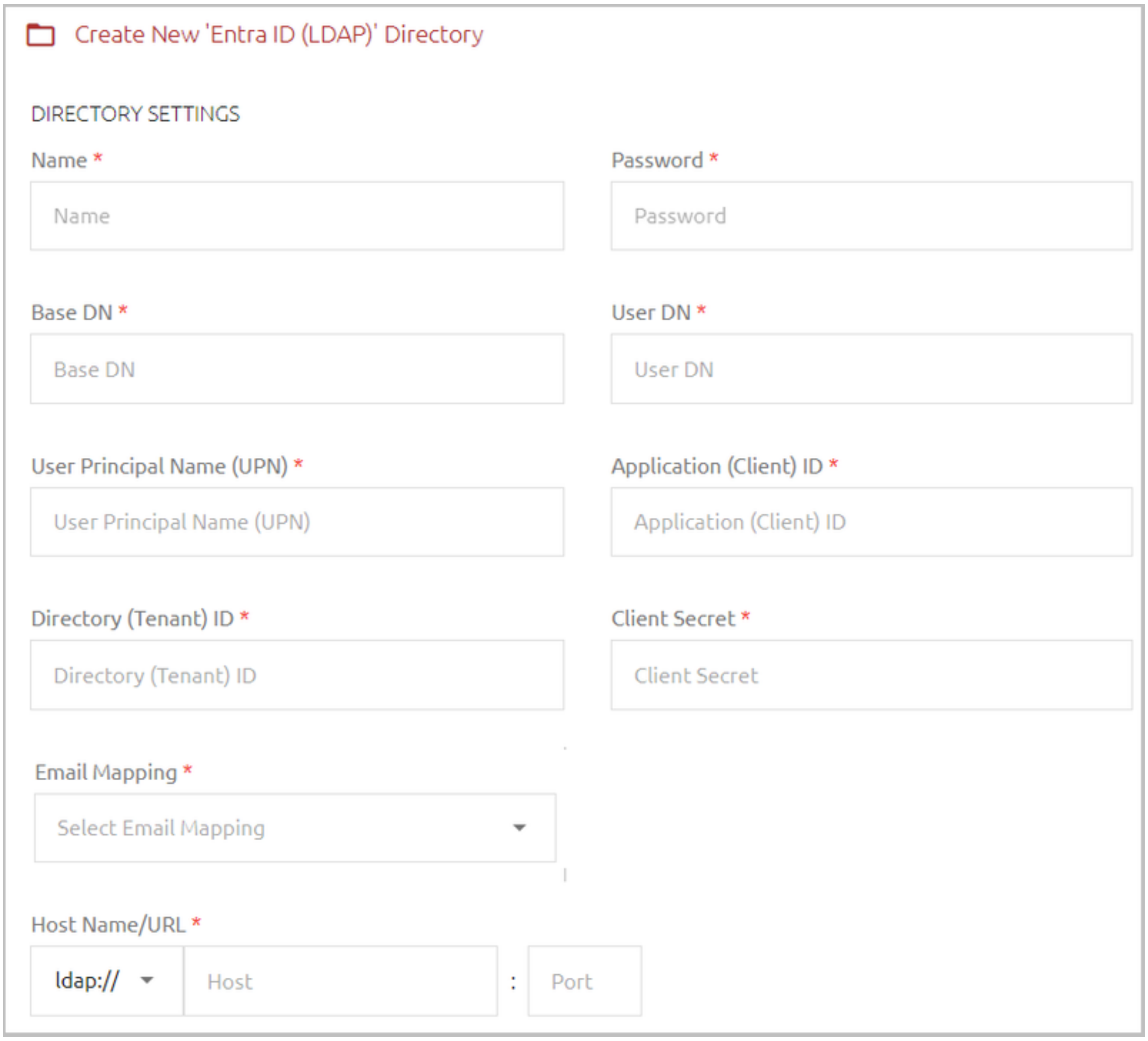
3. Click the **Directory Sync** toggle button to enable and disable automatic syncing.

**Important**

You will NOT be able to change this setting after adding the directory.

4. Click **Select**.

   The **Create New Directory** page opens.



5. Configure the following Directory Settings:

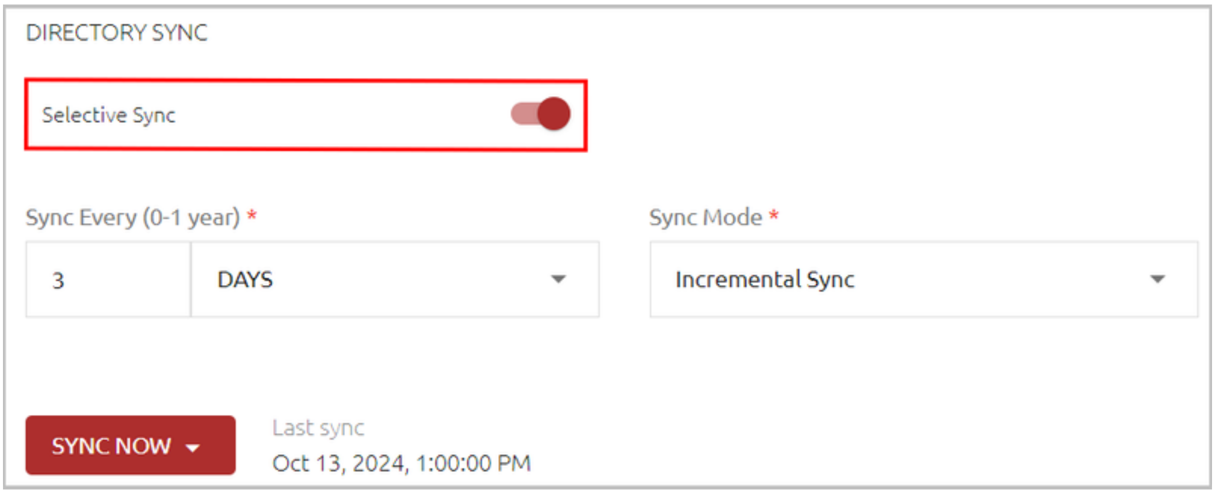
   - **Name:** Name by which the directory is known.
   - **Password:** The password for the  administrative user account.
   - **Base DN:** The distinguished name of the directory from which users will be added to Octopus Authenticator. If you want to add only a specified set of users, enter the relevant node(s) of the directory.
   - **User DN:** The username and distinguished name of the administrative user account that allows access to import from the directory.
   - **User Principal Name (UPN):** The user account used for connecting to the directory.
   - **Application (Client) ID** and **Directory (Tenant) ID:** Copy these values from your Azure AD Portal. (They are displayed in **App registrations**, under the relevant app.)

- **Client Secret:** Copy the *Secret Value only* (NOT the Secret ID) from your Azure AD Portal after creating the secret. (To create the secret, navigate to **Certificates and Secrets**, click **New Client Secret** and name the new secret.)
- **Email Mapping:** The field in the corporate directory used to retrieve the emails of users. Select the mapping source from the list. Keep in mind that you will NOT be able to update the mapping source after directory settings are saved.
- **Host Name/URL:** Select LDAP or LDAPS. Then, in the **Host** field, enter the FQDN of the domain. In the **Port** field, enter **389** for LDAP or **636** for LDAPS.
- **Certificate:** If you are using LDAPS, click **Upload Certificate** and select the relevant certificate file.

6. Click **Test Connection** to perform a validity check.
7. At the bottom of the page, click **Create**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.
8. **For directories with Automatic Sync**, it is recommended to enable Selective Sync in the directory settings:

   a. From the **Directories** menu, click ✎ in the row or tile of the relevant directory to open the directory settings.

   b. Scroll to the bottom of the **Details** tab. Under **Directory Sync**, enable the **Selective Sync** toggle button.


DIRECTORY SYNC

Selective Sync ●

Sync Every (0-1 year) *: 3 DAYS

Sync Mode *: Incremental Sync

Last sync
Oct 13, 2024, 1:00:00 PM

   c. Click **Save**.

**Note**

For more information about Selective Sync, refer to Working with Selective Syncing.

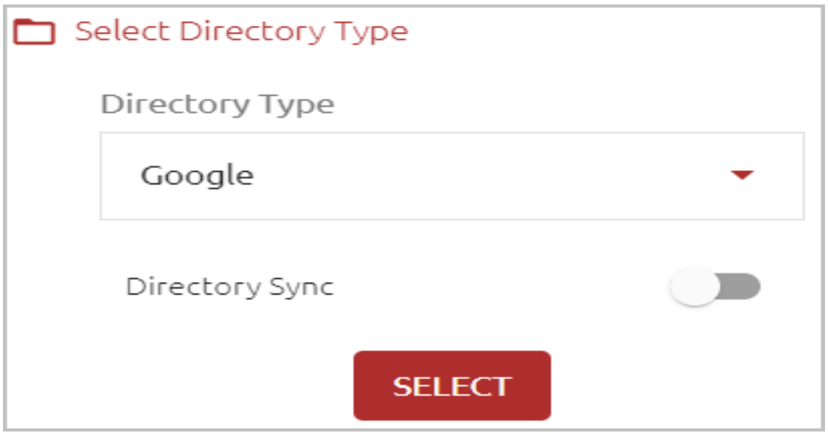
### Google

**To add a new Google directory:**

1. At the top of the **Directories** menu, click **Create Directory**.

   The **Select Directory Type** dialog opens.

2. From the **Directory Type** dropdown list, select **Google Directory**.



Select Directory Type

Directory Type: Google

Directory Sync

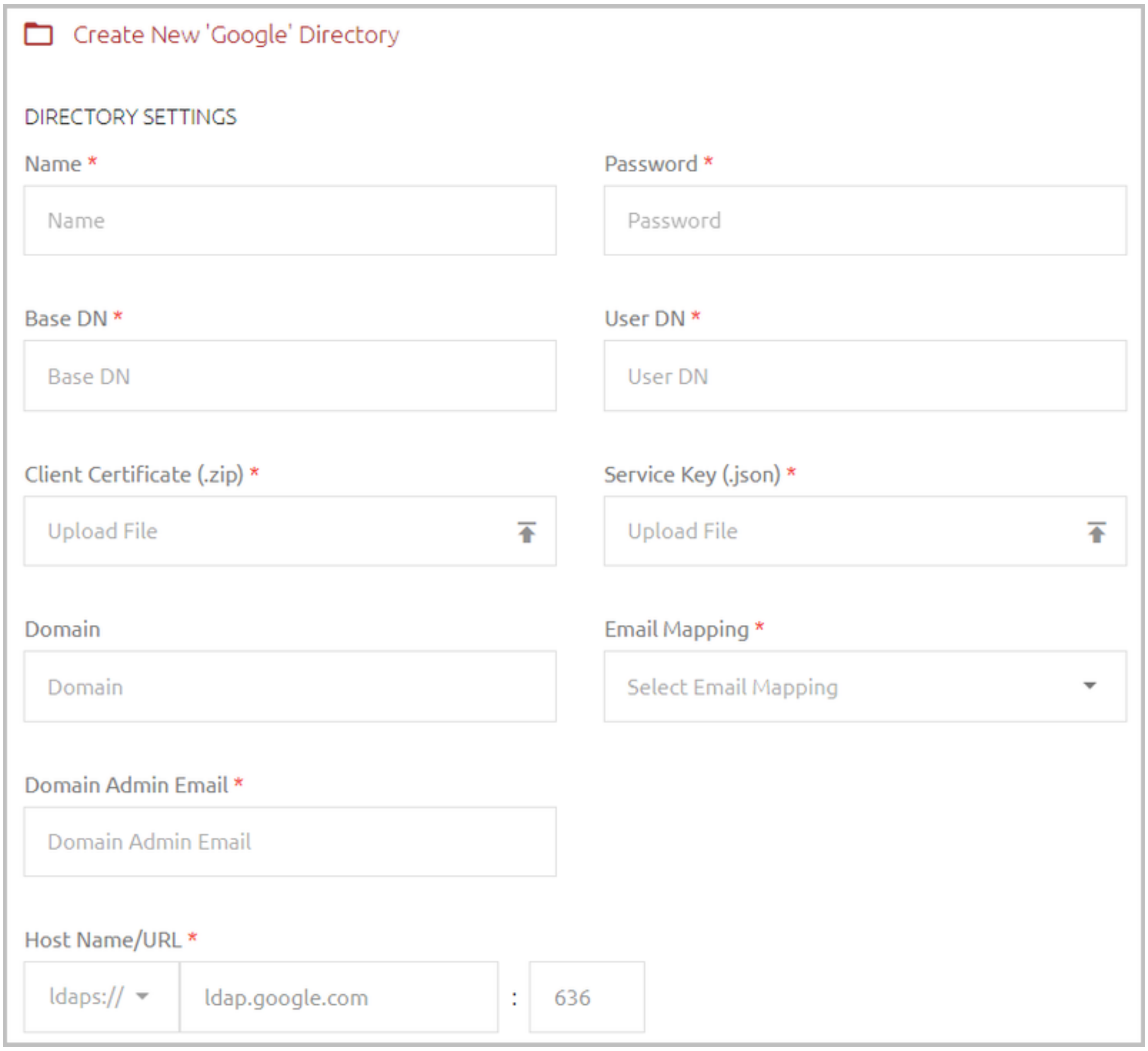
3. Click the **Directory Sync** toggle button to enable and disable automatic syncing.

**Important**

You will NOT be able to change this setting after adding the directory.

4. Click **Select**.

   The **Create New Directory** page opens.



Create New 'Google' Directory

DIRECTORY SETTINGS

Name * : Name

Password * : Password

Base DN * : Base DN

User DN * : User DN

Client Certificate (.zip) * : Upload File

Service Key (.json) * : Upload File

Domain : Domain

Email Mapping * : Select Email Mapping

Domain Admin Email * : Domain Admin Email

Host Name/URL * : ldaps:// ldap.google.com : 636

5. Configure the following Directory Settings:
   - **Name:** Name by which the directory is known.
   - **Password:** The password for the  administrative user account.
   - **Base DN:** The distinguished name of the directory from which users will be added to Octopus Authenticator. If you want to add only a specified set of users, enter the relevant node(s) of the directory.
   - **User DN:** The username and distinguished name of the administrative user account that allows access to import from the directory.
   - **Client Certificate:** Upload the ZIP file from your Google Admin console.
   - **Service Key:** Upload the JSON file from your Google Admin console.
   - **Domain Admin Email:** Email address of the administrative user account that allows access to import from the directory.
   - **Domain:** The IP address or NetBIOS domain name of the domain.

- ○ **Email Mapping:** The field in the corporate directory used to retrieve the emails of users. Select the mapping source from the list. Keep in mind that you will NOT be able to update the mapping source after directory settings are saved.
- ○ **Host Name/URL:** The default setting is prepopulated and is not editable.

6. Click **Test Connection** to perform a validity check.
7. Click **Create**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

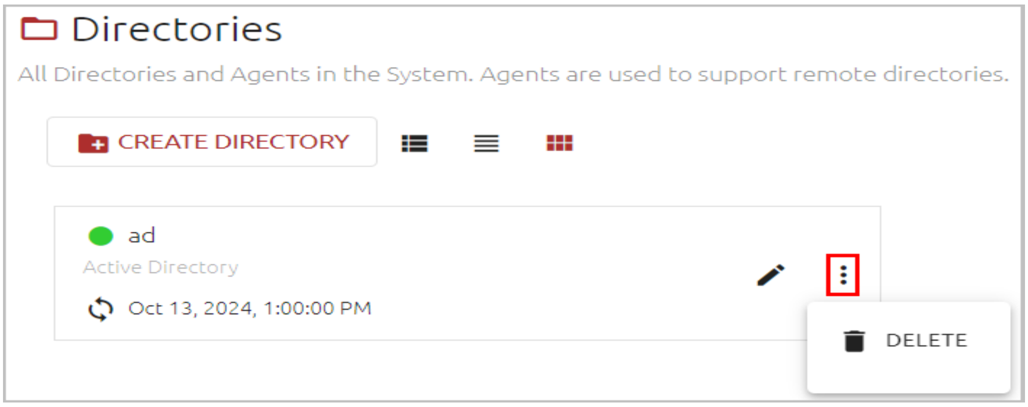
## Viewing and Managing Directories

The **Directories** menu lists all integrated directories and enables you to update their settings. The following information is provided about each directory:

- Name and Type
- Current connectivity status (green or red indicator)
- Automatic Sync indicator icon. Clicking this icon starts a directory sync. If automatic syncing is disabled for the directory, the icon is grayed out.
- Date and time of most recent sync (if automatic syncing is enabled)

Clicking ✎ in the card or row of a directory opens a series of tabs from which you can view and update directory settings. For more information, refer to Updating Directory Details (below).

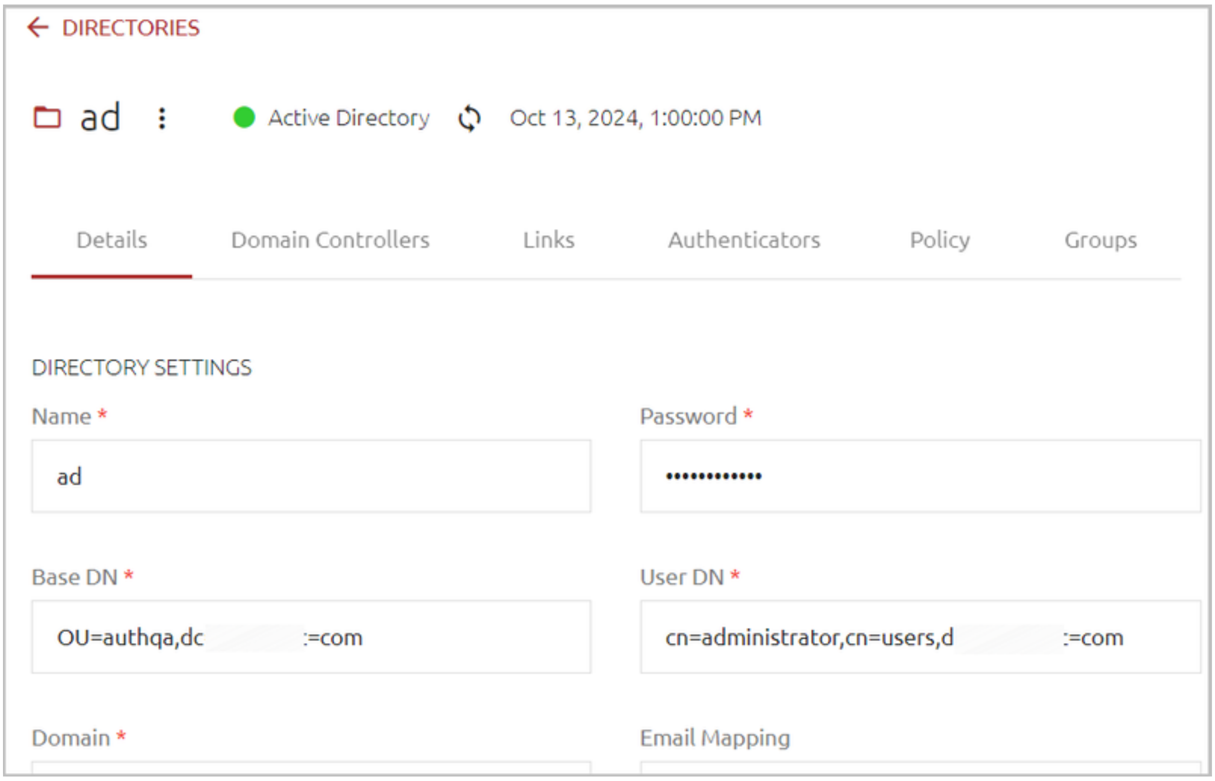
The Delete feature allows you to remove directories that are no longer in use. In the row or card of the relevant directory, click ⋮ and select **Delete**.


Directories
All Directories and Agents in the System. Agents are used to support remote directories.
CREATE DIRECTORY
ad
Active Directory
Oct 13, 2024, 1:00:00 PM
DELETE

Then, click **Delete** in the confirmation popup that opens.

### Updating Directory Details

Clicking ✎ in the tile or row of a directory open another page that displays the settings for that directory in a series of tabs. The name and type of the directory and its current connection state are displayed above the tabs. The Delete and Sync actions (if the directory has automatic sync) are also available from here.



DIRECTORY SETTINGS

Name * ad

Password * ••••••••••••

Base DN * OU=authqa,dc[redacted]:=com

User DN * cn=administrator,cn=users,d[redacted]:=com

Domain *

Email Mapping

The **Details** tab, which is displayed by default when you open the settings page, contains the following sections:

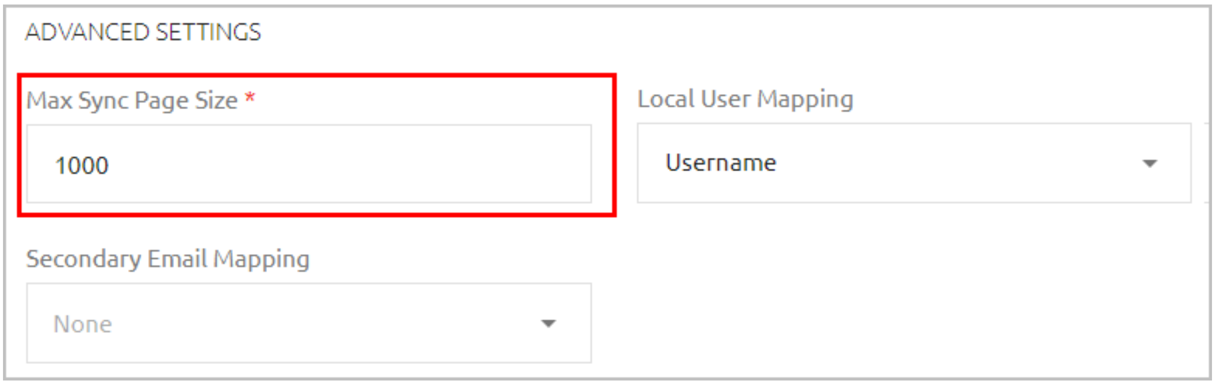
- **Directory Settings:** Displays the directory connection configuration. For details about these settings, refer to Adding a New Directory.
- **Advanced Settings:** Allows you to set maximum number of records and other directory-specific parameters. For details, refer to Configuring Advanced Settings.
- **Directory Sync:** This section appears only in directories for which automatic syncing is enabled. For more information, refer to Configuring Directory Sync Settings.

After updating settings on the **Details** tab, click **Save** (at the bottom of the page). Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

### Configuring Advanced Settings

When relevant, you can update default values for the directory's Advanced Settings. The settings vary slightly depending on whether the directory has automatic syncing enabled.

In directories that do NOT have automatic syncing, you can set the **Max Sync Page Size** value, which controls the number of records added when users are synced from the directory.



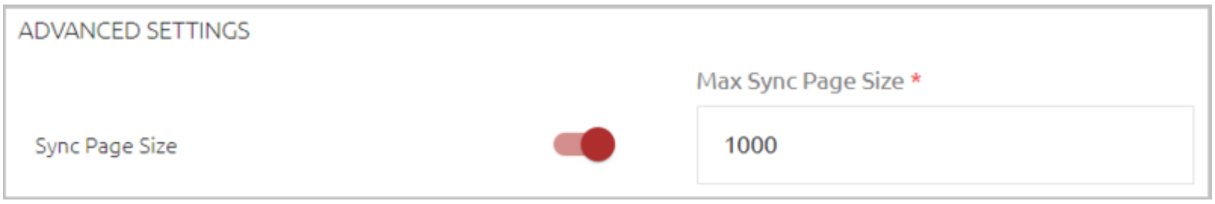
ADVANCED SETTINGS

Max Sync Page Size *
1000

Local User Mapping
Username

Secondary Email Mapping
None

The **Sync Page Size** setting appears in directories with automatic syncing. When the toggle is enabled, pagination is set when adding users from the directory to the authentication platform. If you choose this option, specify the **Max Sync Page Size** in the field to the right.



ADVANCED SETTINGS

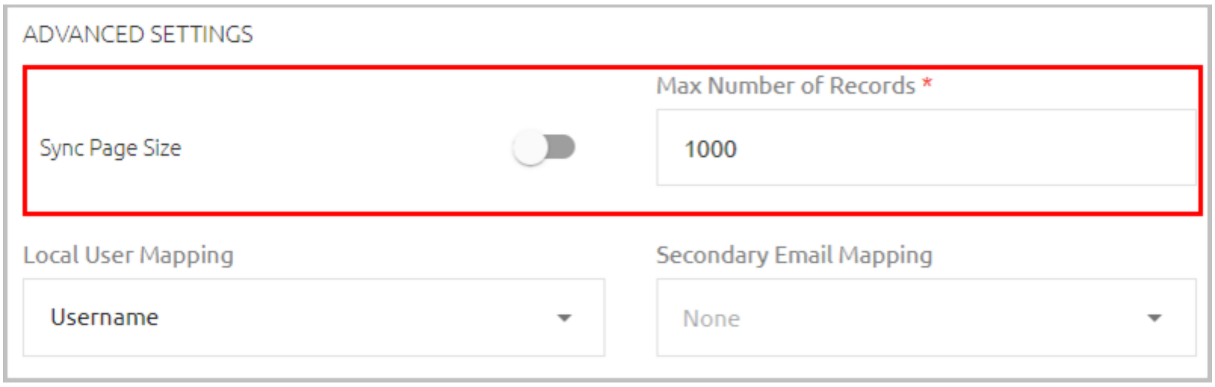
Sync Page Size ●

Max Sync Page Size *
1000

**Note**

Keep in mind that page size affects the number of records that can sync with the Active Directory. A small page size can lead to multiple calls to the AD.

When the **Sync Page Size** setting is disabled, the **Max Number Of Records** setting appears instead. For an unlimited number of records, enter **0**.



ADVANCED SETTINGS

Sync Page Size ○

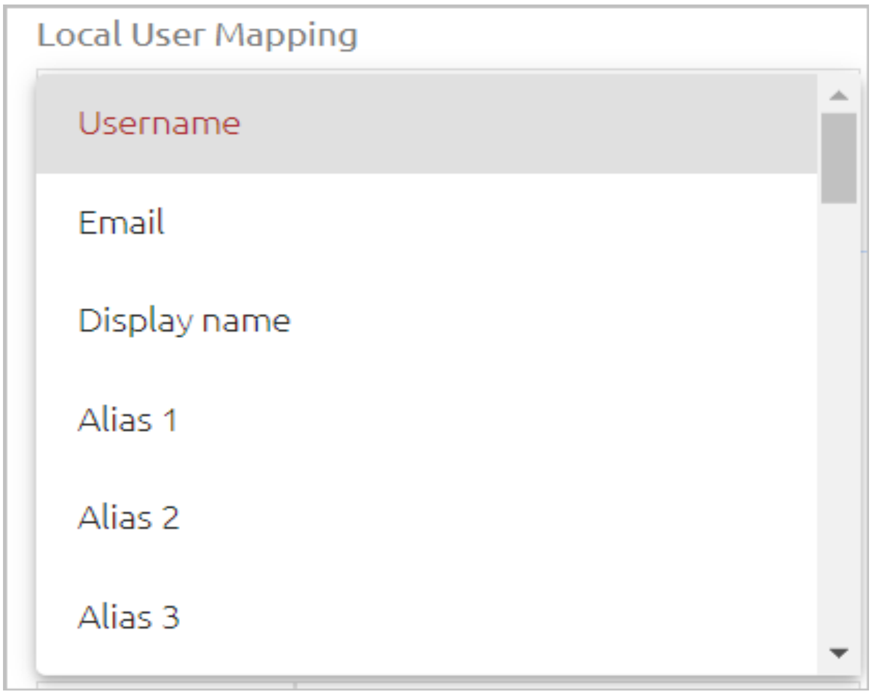
Max Number of Records *
1000

Local User Mapping
Username

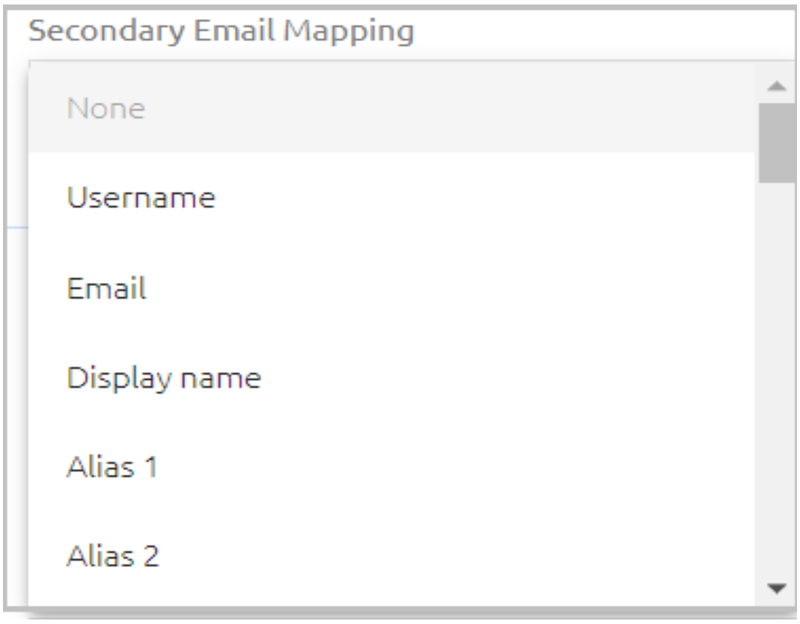
Secondary Email Mapping
None

The following settings are available for all directories, regardless of automatic syncing status:

- **Local User Mapping:** The identifier used for authentication of Local users to Windows.



- **Secondary Email Mapping:** This setting allows enrollment invitations to be automatically sent to two email addresses - the one specified in the **Personal** tab of the user details, and an additional one. When the value is **None**, enrollment emails are sent to only one address (the one listed in the **Personal** tab). The additional email address can be mapped to an attribute added to the directory schema, or to an Alias parameter defined in the **Personal** tab of the user details.



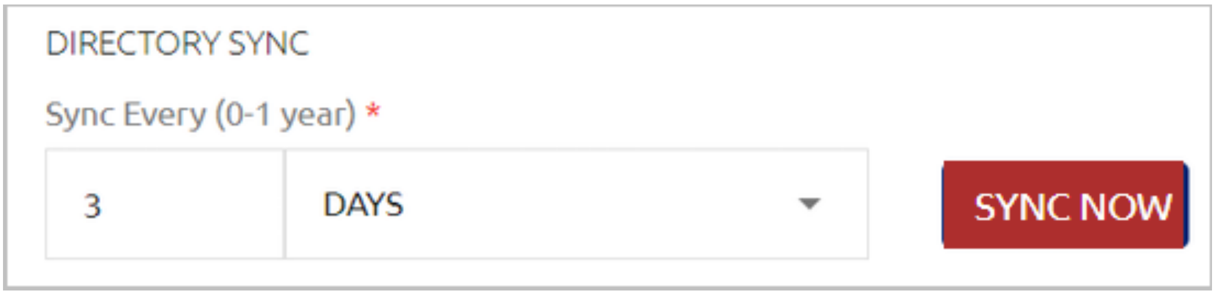
The **Federation** section appears in Entra ID directory types. It is recommended to activate the **Federated To Octopus** setting if you have a federated Entra ID domain.

When this setting is enabled, you will be able to add users directly to the remote Entra ID directory, and then import or synchronize them into the Octopus platform.

After updating Advanced Settings, click **Save**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

### Configuring Directory Sync Settings

The **Directory Sync** settings are available only for directories that have automatic syncing enabled.



DIRECTORY SYNC

Sync Every (0-1 year) *

3 DAYS

The settings are:

- **Sync Every:** Determines the frequency at which automatic syncing occurs. The frequency can range from one hour to one year.

**Note**

To disable automatic syncing, set the value to **0**.

- **Sync Now:** Initiates an immediate sync of the directory.

### Additional Sync Settings for Active Directory

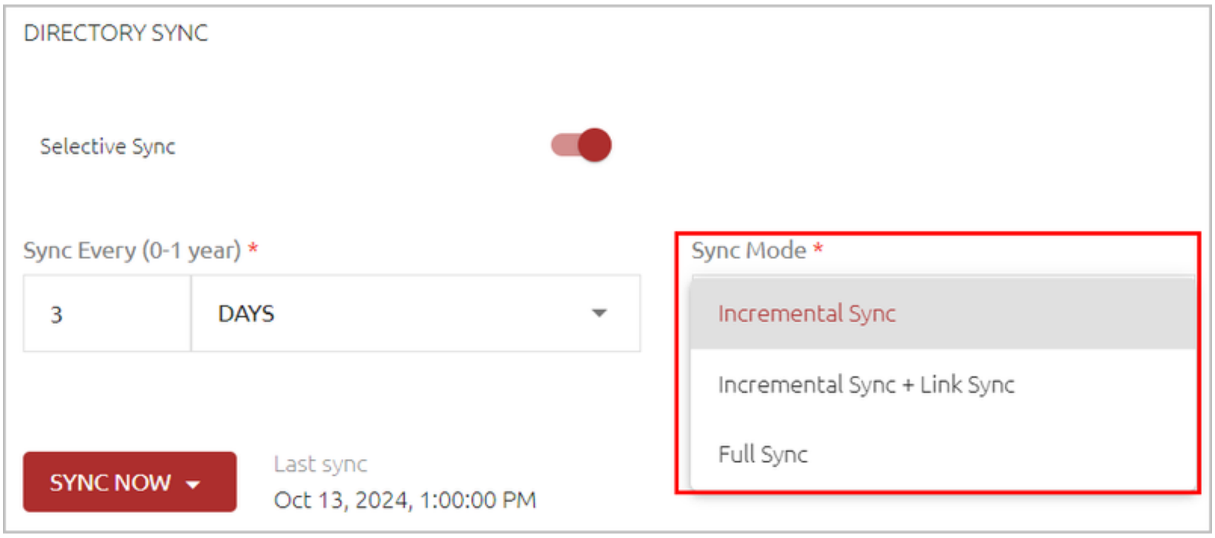
Directory Sync settings for AD type directories include the **Selective Sync** toggle button. Click the toggle button to enable / disable selective syncing. When the feature is enabled, you will be able to choose the Groups that are included in the sync process. For more information, refer to Working with Selective Syncing.

In addition, the settings for AD type directories allow you to choose the extent of the sync. The following sync modes are supported:

- **Incremental Sync:** Checks for changes and updates in the Active Directory and syncs these changes with the Management Console.
- **Incremental Sync + Link Sync:** As part of the incremental sync, user properties in all linked directories are also updated.
- **Full Sync:** Involves a complete sync with the Active Directory (regardless of changes and updates).

The sync mode needs to be selected when configuring the following settings and actions:

- **Scheduling automatic syncing:** After specifying the syncing frequency, select the mode from the **Sync Mode** dropdown list.


DIRECTORY SYNC

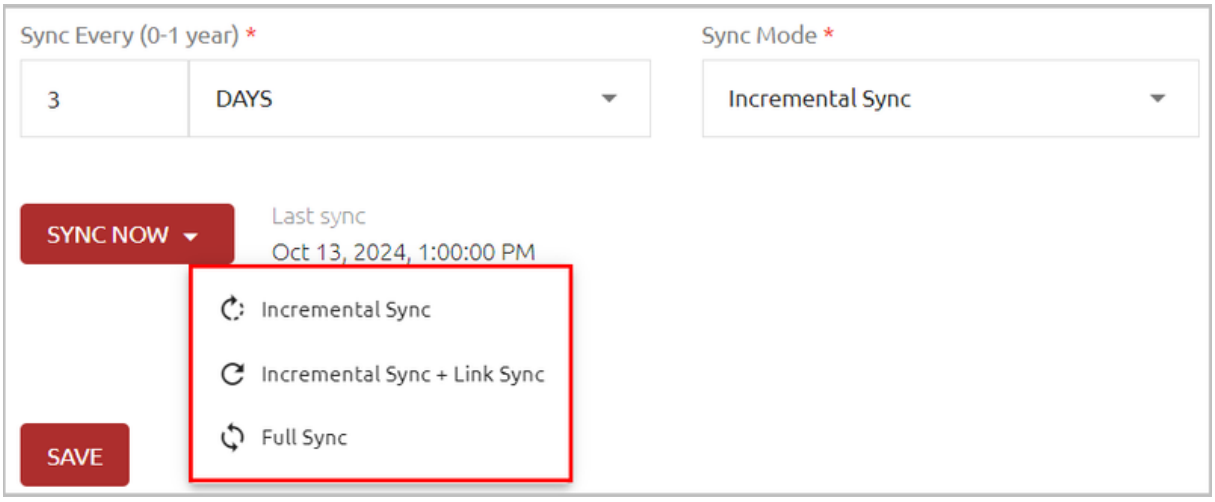
Selective Sync

Sync Every (0-1 year) *: 3 DAYS

Sync Mode *

Last sync
Oct 13, 2024, 1:00:00 PM

- **Initiating an immediate sync:** Click **Sync Now** and then select the sync mode from the options list that opens.


Sync Every (0-1 year) *: 3 DAYS

Sync Mode *: Incremental Sync

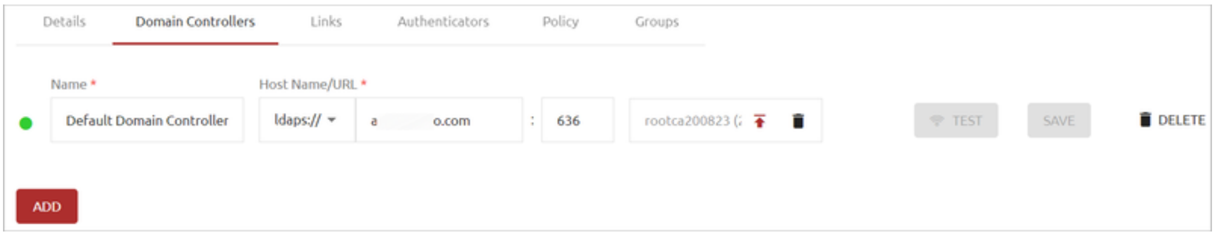
Last sync
Oct 13, 2024, 1:00:00 PM

After updating Directory Sync settings, click **Save** . Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

### Managing Domain Controllers

The **Domain Controllers** tab displays the hostname/URL that was specified for the directory server when the directory was created. The colored indicator (green or red) to the left of the **Name** indicates the current connectivity status of the server. The icons in the certificate field allow you to replace or delete the current certificate.

The **Test** button becomes enabled whenever you make changes to parameters of a domain controller, allowing you to perform a validity check before saving the new settings. The **Delete** button enables you to remove domain controllers that are no longer in use.

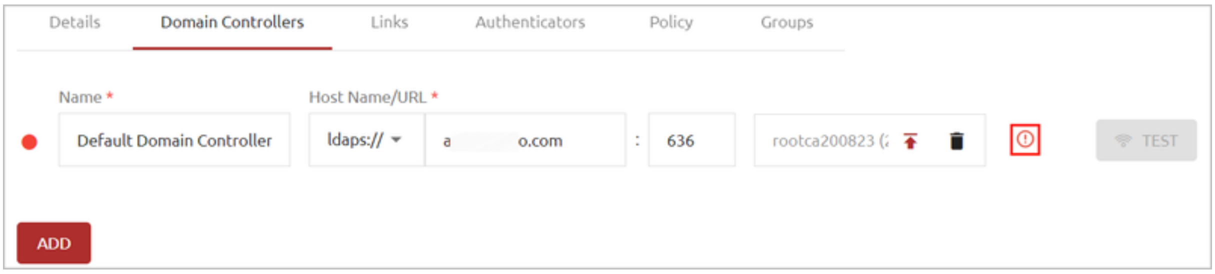


Name * Default Domain Controller

Host Name/URL * ldaps:// a o.com : 636

rootca200823 (

If there are connection problems related to a domain controller, an error icon appears on the right side of the row.

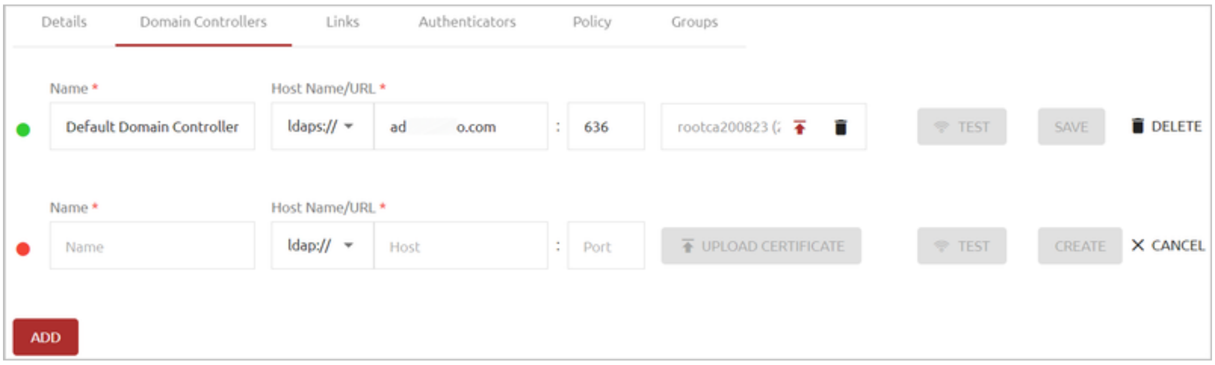


Name * Default Domain Controller

Host Name/URL * ldaps:// a o.com : 636

rootca200823 (

If your environment utilizes multiple servers for the directory, you can configure the additional domain controllers in the Management Console. Click **Add** and enter the details of the domain controller in the relevant fields. Then, click **Create**.



Name * Default Domain Controller

Host Name/URL * ldaps:// ad o.com : 636

rootca200823 (

Name * Name

Host Name/URL * ldap:// Host : Port

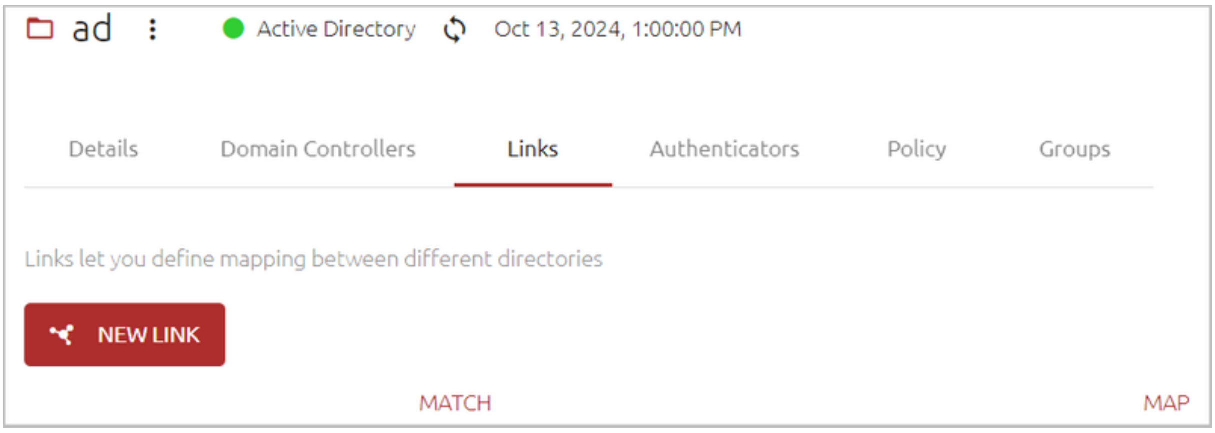
## Creating Directory Links

Some of your users may be members of more than one directory. The **Links** tab of a directory's settings enables you to link specific parameters in different directories. This linking enables the Management Console to map the given parameters, preventing the need for multiple enrollments for the same user.

The directory from which you create the link is called the Local directory. The directory to which you link is known as the Remote directory.

**To add a directory link:**

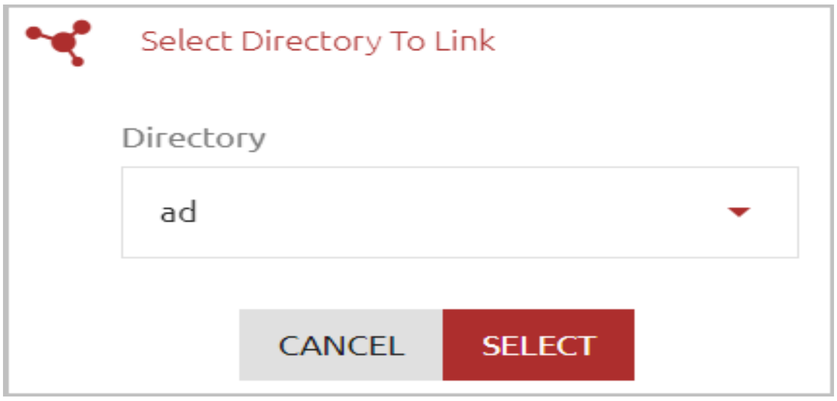
1. From the **Directories** menu, open the settings of the directory in which you want to create a link and select the **Links** tab.



Links let you define mapping between different directories

2. At the top of the tab, click **New Link**.

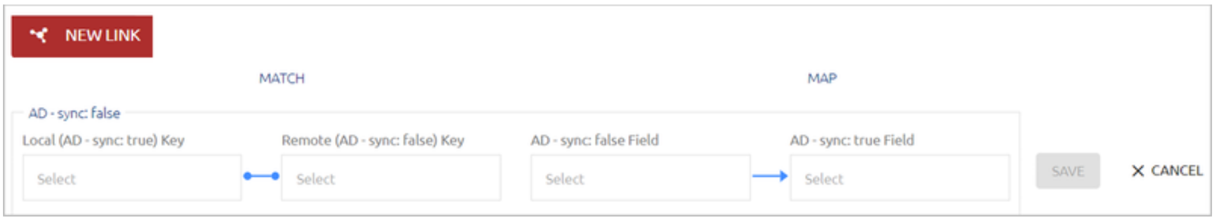
   The **Select Directory To Link** dialog opens.



Directory: ad

3. Open the **Directory** list and select the directory to which you want to link (the Remote directory). Then, click **Select**.

   A new row is added to the **Links** tab.



4. On the left side of the row, click **Select** and choose a parameter in each directory. An exact match of these parameters will indicate that the user in each directory is the same user.

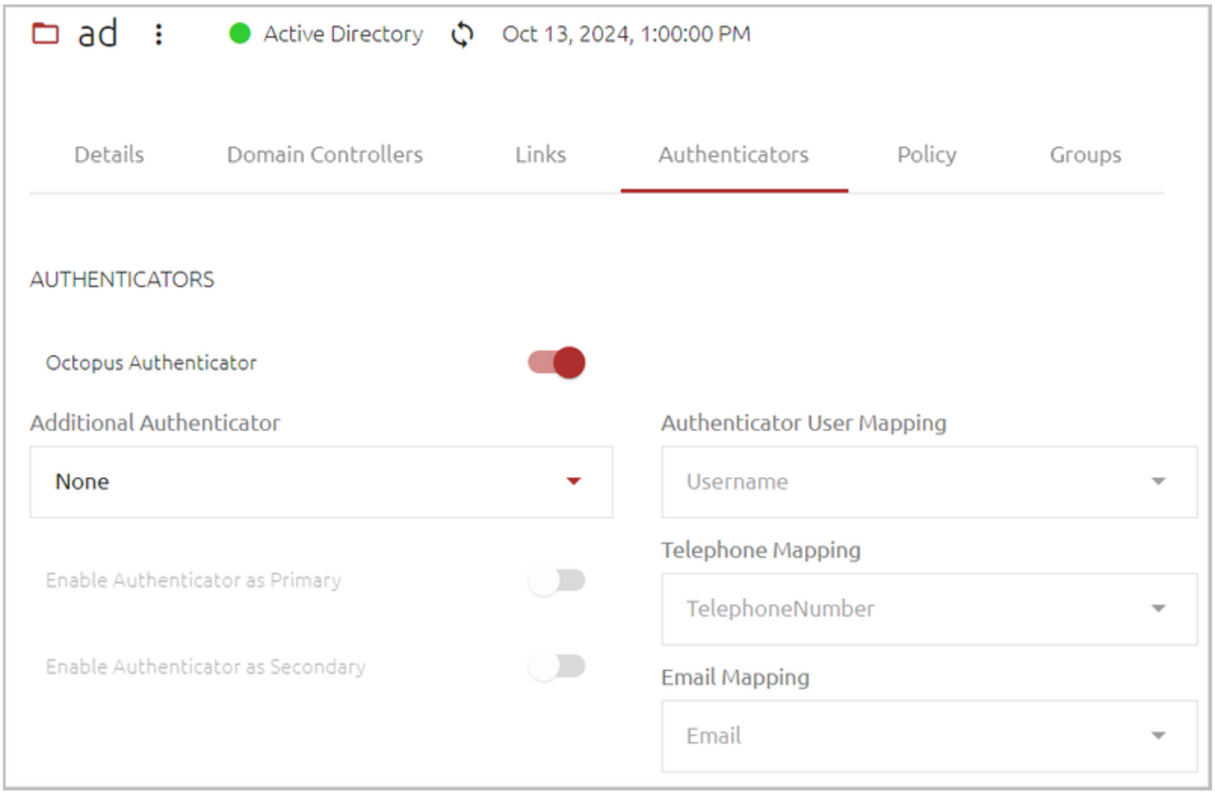
5. On the right side of the row, select a value to be imported from the Remote directory to the Local directory. Then, select the parameter in the user properties of the Local directory to which the value will be imported. (This is generally one of the **Alias** fields.)

6. To save the new link in the system, click **Save** . Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

## Configuring Directory Authentication Options and Settings

Enterprise Connect Passwordless provides the ability to authenticate to Windows, Mac and the User Portal using third-party authenticators that are integrated with the platform by means of Authenticator plugins. Once these plugins are added to the system they can serve as primary or secondary authenticators (or both) and act as OTP validators (for One Time Password authentication) for users in specific directories.

The **Authenticators** tab of a directory's settings enables you to select the authenticator(s) that provide authentication and OTP validation for users. The tab also contains various other settings related to authentication, including FIDO2 Settings and Default Authentication Method.



ad ⋮ ● Active Directory Oct 13, 2024, 1:00:00 PM

Details | Domain Controllers | Links | Authenticators | Policy | Groups

AUTHENTICATORS

Octopus Authenticator ●

Additional Authenticator: None

Enable Authenticator as Primary ○

Enable Authenticator as Secondary ○

Authenticator User Mapping: Username

Telephone Mapping: TelephoneNumber

Email Mapping: Email

After updating settings in the **Authenticators** tab, click **Save**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

### Authenticator Settings

This section of the **Authenticators** tab lets you set the authenticator(s) that provide authentication for users in the directory. When a third-party authenticator is selected as either a Primary or Secondary authenticator, information including user agent, Source IP, etc. is sent to that authenticator for additional policy enforcement or authentication.

**To set the authenticator(s) for the directory:**

1. Enable / Disable Octopus Server authentication by clicking the **Octopus Authenticator** toggle button.

If this setting is disabled, users will not be able to authenticate with Octopus Authenticator, and you need to specify another authenticator. You can also specify an additional authenticator when Octopus Authentication is enabled.

2. To set another authenticator, select the relevant third-party authenticator from the **Additional Authenticator** list. (The list includes all third-party authenticators that have been added to the **Authenticator List** of the **System Settings** menu.)

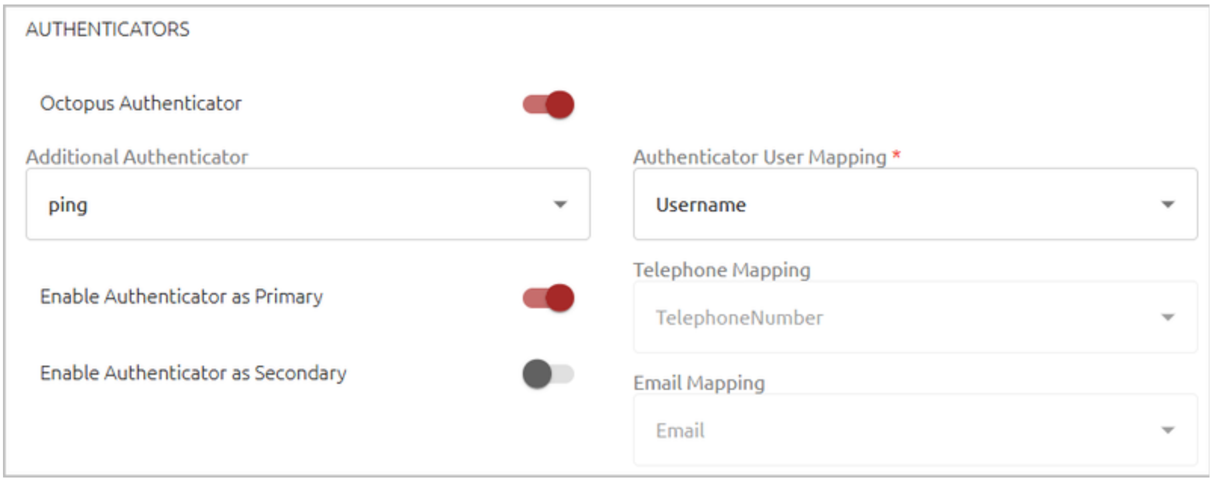
   Once you have selected an authenticator, the settings below the list are enabled.

3. Configure the following settings as required:

   - **Enable Authenticator as Primary:** When enabled, this authenticator will serve as the first line of authentication. If the Octopus Authenticator is enabled, both authenticators will be primary authenticators, and the user will have the option to choose which one to use.

   - **Enable Authenticator as Secondary:** When enabled, this authenticator receives user information from the primary authenticator and then approves or rejects authentication. This information includes the usual headers (user agent, Source IP, etc.) as well as the authentication that was used for the primary authenticator.

   - **Authenticator User Mapping:** Select a parameter to be used for authentication mapping. The options that appear in the dropdown list are the parameters that are defined in the **Personal** tab of your users' accounts. For example, authentication to ForgeRock can be done with **Username**:

     AUTHENTICATORS

     Octopus Authenticator ●

     Additional Authenticator: ping

     Authenticator User Mapping *: Username

     Telephone Mapping: TelephoneNumber

     Enable Authenticator as Primary ●

     Enable Authenticator as Secondary ○

     Email Mapping: Email

   - **Telephone Mapping** and **Email Mapping:** These settings are enabled when Twilio is selected as an additional authenticator. Select the user parameter to be mapped to user phone number and email address.

4. At the bottom of the **Authenticators** tab, click **Save**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

### FIDO2 Authentication Settings

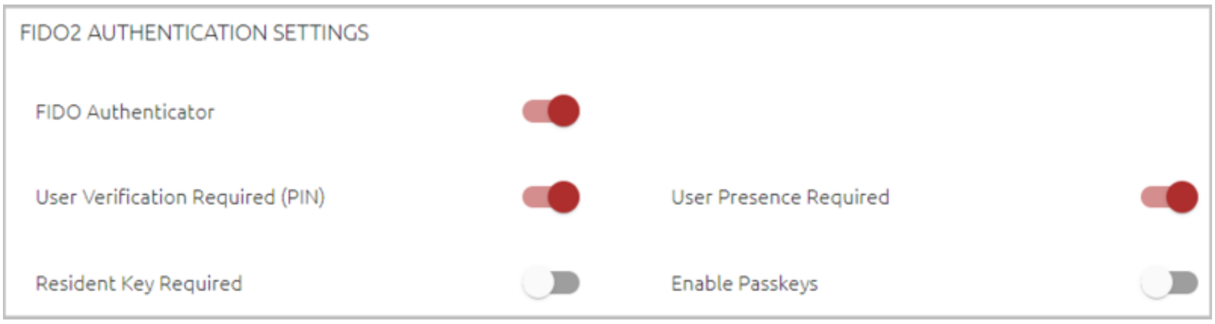
FIDO authentication is supported for:

- Any web application (e.g., SAML with Chrome, Edge, Safari) **that uses WebAuthn or WebView2**
- USB interface authentication
- Windows and Mac login (online /offline)
- Radius login (e.g., VPN)
- Retrieving the user AD password
- Launching the SSO portal

FIDO authentication is NOT currently supported for:

- Embedded browser applications (e.g., the Office365 desktop application)
- NFC and BLE interface authentication
- LDAP services

The **FIDO2 Authentication Settings** allow you to enable / disable FIDO authentication and set other parameters related to the FIDO authenticator.



FIDO2 AUTHENTICATION SETTINGS

| | | | |
|---|---|---|---|
| FIDO Authenticator | ● | | |
| User Verification Required (PIN) | ● | User Presence Required | ● |
| Resident Key Required | ○ | Enable Passkeys | ○ |

The settings are:

- **FIDO Authenticator:** Click the toggle button to enable and disable FIDO authentication for users in the directory.

**Important**

If the FIDO Authenticator is currently disabled globally ( **System Settings > Authenticators**), you will not be able to enable FIDO authentication for the directory.

- **User Verification Required (PIN):** When this setting is enabled, users are asked to choose a new PIN code during the registration process. This feature is used for passwordless authentication in which the FIDO authenticator requires a PIN as the additional authentication factor.
- **User Presence Required:** When this setting is enabled, users are required to touch their token after entering the PIN. The setting is enabled by default.

This setting operates in conjunction with the setting configured in the Windows MSIUpdater (version 3.8.0 and up). For details, refer to the Octopus Desk for Windows Installation Guide.

**Note**

During initial enrollment of a FIDO token, user presence is always required, even when the **User Presence Required** setting is disabled.

- **Enable Passkeys:** When this toggle is selected, users can authenticate to the User Portal and web applications using a passkey that is integrated with their workstation or smartphone. For successful passkey authentication, the following requirements must be fulfilled:
  - The FIDO authenticator needs to be enabled both globally (**System Settings > Authenticators**) and in the directory settings.
  - Users must work with a passkey-supporting phone or a workstation with Windows Hello / Touch ID enabled with fingerprint sensor.
- **Resident Key Required:** When enabled, the identity of the private key used for authentication is required.

### Client Certificate (Smart Card) Authentication Settings

These settings enable users to log into Windows, web apps and other integrated services using a smart card containing a certificate signed by your organization's root Certificate Authority (CA). Users can use their existing smart cards and readers, and authenticate by providing the associated PIN.

Smart card authentication works using the same mechanism as that utilized when users login through the authentication app or by providing a FIDO token. The certificate is NOT meant to be the underlying directory authenticator, but an alternative to the app / FIDO key methods.

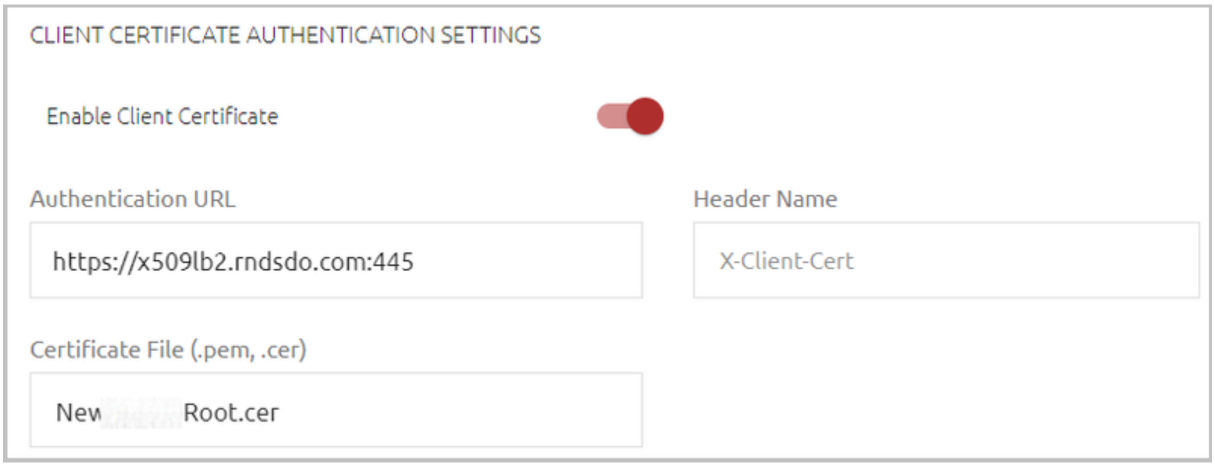
To successfully use smart card authentication, you need to configure the following settings:

- **Enable Client Certificate:** Click the toggle button to enable and disable smart card authentication for users in the directory.

**Important**

If the Client Certificate Authenticator is currently disabled globally ( **System Settings > Authenticators**), you will not be able to enable smart card authentication for the directory.

- **Authentication URL:** Enter the full address of the load balancer where your root certificate is stored, followed by the listening port.
- **Header Name:** The HTTP header used to pass the certificate to the server. If required, change the default value to the header required in your setup.
- **Certificate File:** Click the field to select and upload your root certificate.



CLIENT CERTIFICATE AUTHENTICATION SETTINGS

Enable Client Certificate ●

Authentication URL: https://x509lb2.rndsdo.com:445

Header Name: X-Client-Cert

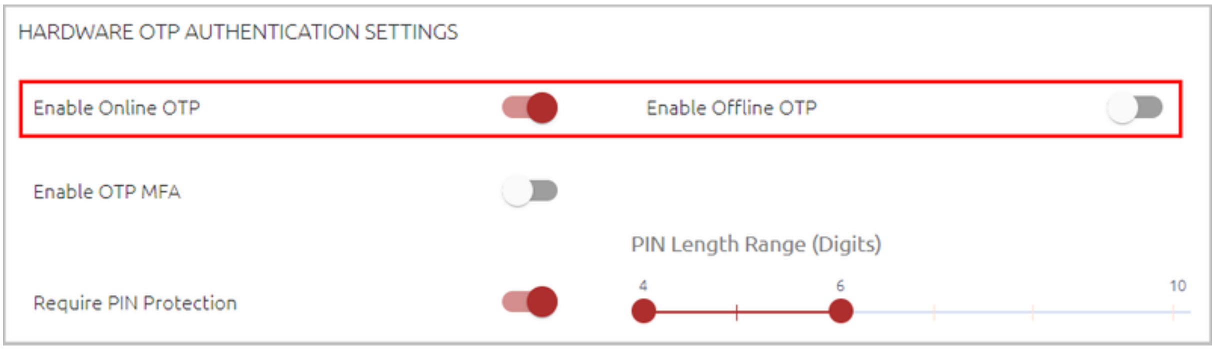
Certificate File (.pem, .cer): New[redacted]Root.cer

**Note**

Smart card authentication requires storing the root certificate on a load balancer. Please refer to the documentation of your setup (Azure AD, AWS, etc.) for guidance on the required configuration.

### Hardware OTP Authentication Settings

Enterprise Connect Passwordless supports use of HW OTP tokens to authenticate to Windows and the User Portal. To allow users to authenticate with these devices, enable the relevant toggle button(s) under **Hardware OTP Authentication Settings**. You can activate Online OTP, Offline OTP, or both.



HARDWARE OTP AUTHENTICATION SETTINGS

Enable Online OTP ●

Enable Offline OTP ○

Enable OTP MFA ○

Require PIN Protection ●

PIN Length Range (Digits): 4 – 6

When the **Require PIN Protection** setting is enabled, users need to enter a PIN together with the OTP code. (Users will select a PIN during the enrollment process.) Under **PIN Length Range**, drag the slider to specify the range for required number of digits in the PIN code. (The maximum supported range is 4-10 digits.) Then, in the confirmation popup, click **Continue**.

**Important**

PIN protection is mandatory for Offline hardware OTP authentication. In addition, TPM must be supported on the Windows workstation.

Online hardware OTP authentication can be configured with or without PIN protection.

The **Enable OTP MFA** toggle determines whether or not users must provide a password when authenticating to the User Portal with a hardware OTP token.

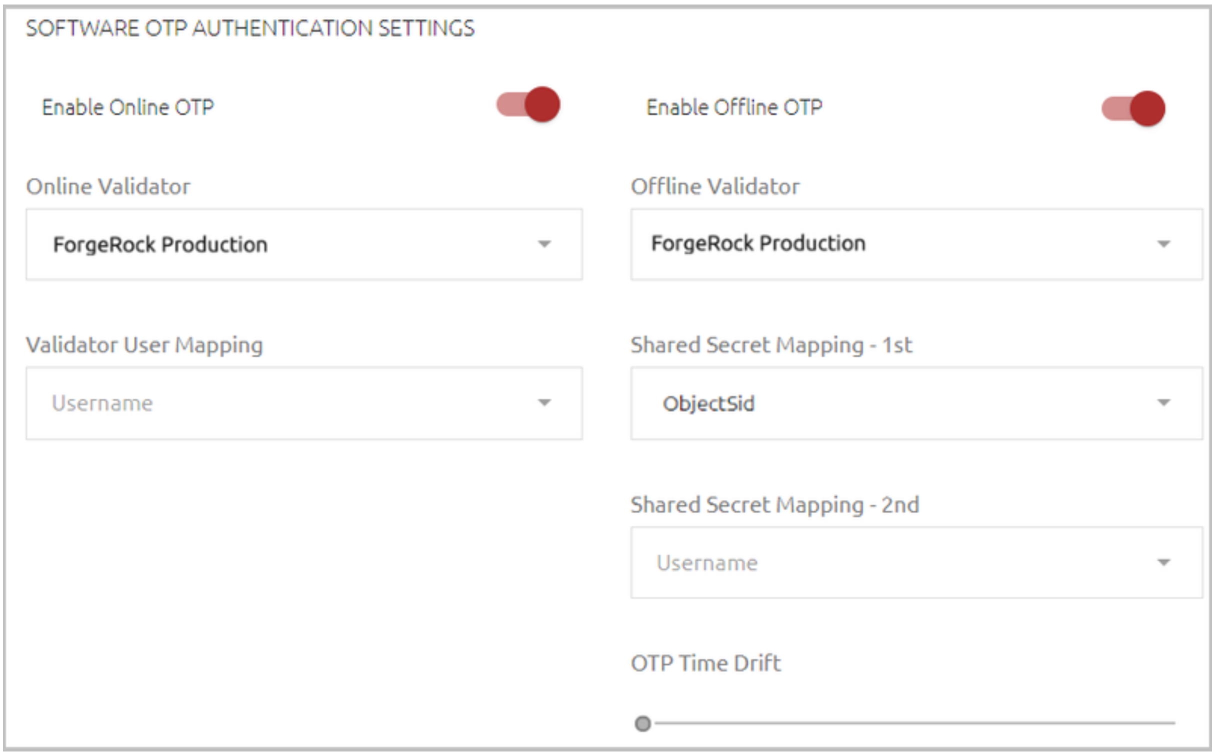
### Software OTP Authentication Settings

To enhance authentication capabilities, Enterprise Connect Passwordless provides the option of issuing a one time password for login. OTP settings are configured per directory, in the **Authenticators** tab of the directory's settings. By default, the OTP feature is disabled.

Enterprise Connect Passwordless offers the following OTP processes. Either or both can be enabled, as required:

- **Online OTP:** When enabled, enrolled users are able to log into Windows, Mac or the User Portal using a one time password issued by either the Octopus Authenticator or by a third-party authenticator.
- **Offline OTP:** When enabled, enrolled users are able to log into Windows / Mac using a one time password that is stored locally. These OTPs are supplied by either the Octopus Authenticator or by a third-party authenticator.

  When offline OTP is activated, a list of OTPs are securely stored on the Windows / Mac workstation to allow users to authenticate to the workstation when not connected to the network. The OTPs are timed-based and use the standard TOTP mechanism. They can therefore be added to any standard authentication mobile app that supports TOTP.



SOFTWARE OTP AUTHENTICATION SETTINGS

Enable Online OTP

Online Validator: ForgeRock Production

Validator User Mapping: Username

Enable Offline OTP

Offline Validator: ForgeRock Production

Shared Secret Mapping - 1st: ObjectSid

Shared Secret Mapping - 2nd: Username

OTP Time Drift

**To enable OTP:**

1. To activate online OTP, click the **Enable Online OTP** toggle button. Then, select the appropriate authenticator from the **Online Validator** list.

**Note**

The **Validator** list is comprised of the Octopus Authentication Server as well as all third-party authenticators that have been added to the **Authenticators List** of the System Settings. For more information, refer to Managing Authenticators.

2. Under **Validator User Mapping**, select the user parameter to be used for OTP authentication.

3. To activate offline OTP, click the **Enable Offline OTP** toggle button. Then, select the appropriate authenticator from the **Offline Validator** list.

4. From the **Shared Secret Mapping**, list(s), select the mapping field(s) to be used to generate the offline tokens. The second Shared Secret Mapping field is optional.

5. If relevant, specify a value (in seconds) for the **OTP Time Drift** by dragging the slider to the required value. The maximum valid value is 600 seconds.

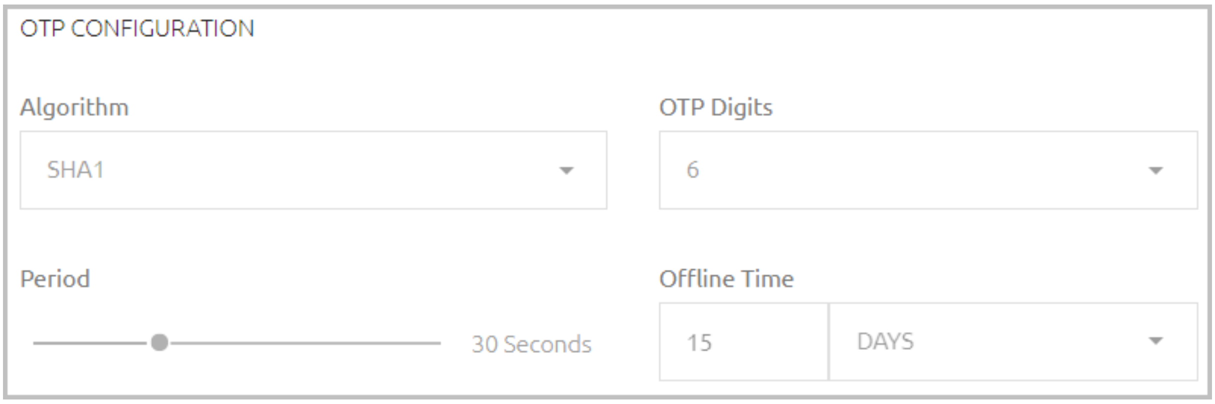
6. Under **OTP Configuration**, specify the following settings:

    - **Algorithm:** Security strength- **SHA1** (default) or **SHA256** .

    - **OTP Digits:** Length of the password - six (default) or eight characters.

    - **Period:** Number of seconds after which each token expires and is replaced by a new one (default = 30).

    - **Offline Time:** The period of time for which the user is allowed to authenticate offline (default = 15 days).



OTP CONFIGURATION

Algorithm: SHA1

OTP Digits: 6

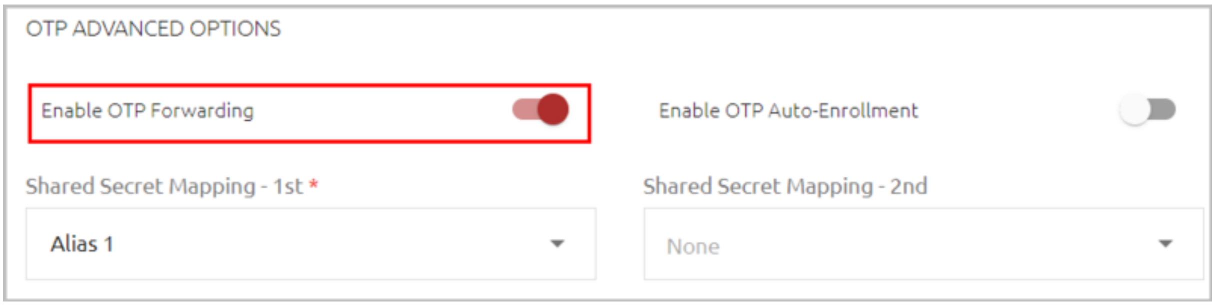
Period: 30 Seconds

Offline Time: 15 DAYS

**Important**

Make sure your settings match the OTP parameters of the authenticator you have chosen to generate the OTP tokens.

7. If you want to provide authorization to pass the OTP to another authentication platform, under **OTP Advanced Options**, click the **Enable OTP Forwarding** toggle button. Then open the **Shared Secret Mapping - 1st** list and select the user identification parameter utilized by the external authenticator. Optionally, you may select an additional parameter from the **Shared Secret Mapping - 2nd** list.



OTP ADVANCED OPTIONS

Enable OTP Forwarding ●

Enable OTP Auto-Enrollment ○

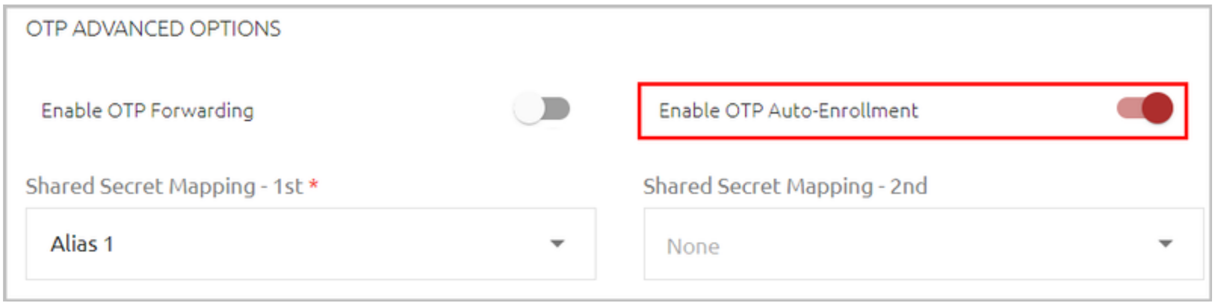
Shared Secret Mapping - 1st *: Alias 1

Shared Secret Mapping - 2nd: None

8. At the bottom of the **Authenticators** tab, click **Save.** Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

### OTP Auto-Enrollment

The Octopus authentication platform supports online authentication using OTP tokens generated by a third-party platform (e.g., ForgeRock), without requiring users to enroll a new account in Octopus Authenticator. To use this feature, in the **OTP Advanced Options** section, activate the **Enable OTP Auto-Enrollment** toggle button. Then, from the **Shared Secret Mapping - 1st** list, select the user attribute populated by the OTP seed (e.g., **Alias 1**).



OTP ADVANCED OPTIONS

Enable OTP Forwarding ○

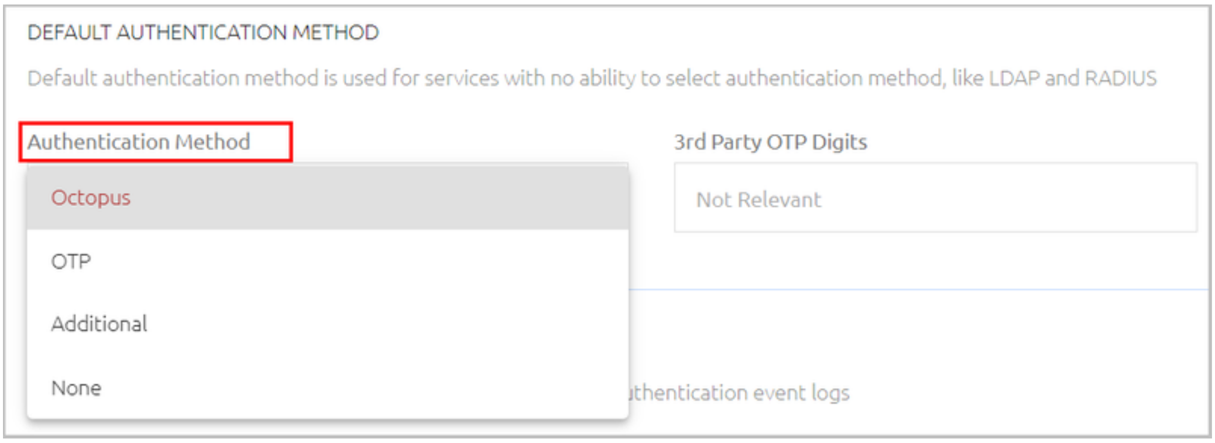
Enable OTP Auto-Enrollment ●

Shared Secret Mapping - 1st *: Alias 1

Shared Secret Mapping - 2nd: None

### Default Authentication Method

The default authentication method is the authenticator used to access services without Login screens that allow users to select an authentication type (e.g., LDAP and RADIUS services). Select the relevant authenticator from the **Authentication Method** dropdown list.



DEFAULT AUTHENTICATION METHOD

Default authentication method is used for services with no ability to select authentication method, like LDAP and RADIUS

Authentication Method

3rd Party OTP Digits: Not Relevant

The options are:

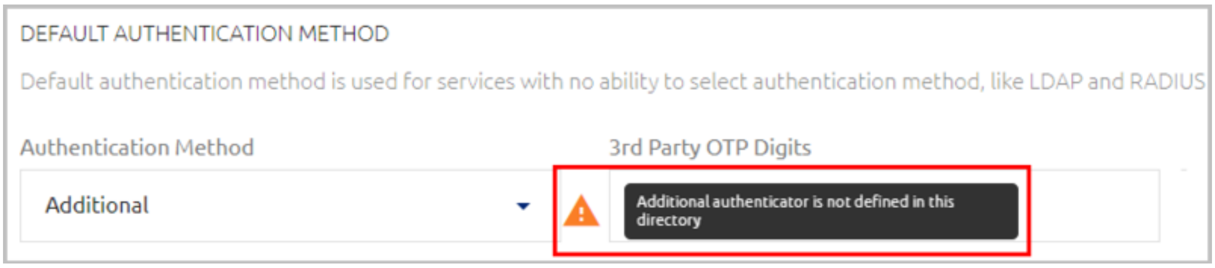
- **Octopus:** The Octopus Authenticator.
- **OTP:** The validator that is specified in the directory's One Time Password (OTP) settings.

**Important**

If you select a third-party OTP validator, enter the length of the validation code in the **3rd Party OTP Digits** field.

- **Additional:** The third-party authenticator that is selected as an Additional Authenticator in the directory's Authenticators settings.
- **None:** Select this option if a default authentication method is not relevant (e.g., RADIUS / LDAP services are not used, or users work with FIDO authentication only and no other authenticator in the system is enabled).

If you select a default authentication method that is currently disabled or not defined in the directory's settings, a warning icon appears next to your selection.


DEFAULT AUTHENTICATION METHOD

Default authentication method is used for services with no ability to select authentication method, like LDAP and RADIUS

Authentication Method: Additional

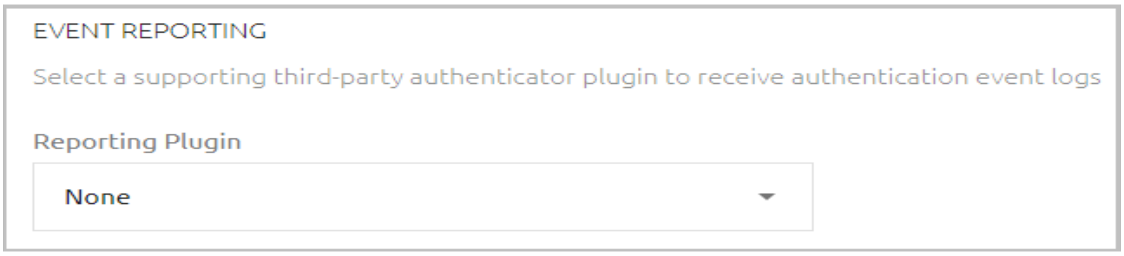
3rd Party OTP Digits

Additional authenticator is not defined in this directory

### Event Reporting

This feature enables you to designate a third-party authenticator that receives authentication event logs. This enables generation of additional log reports that can be viewed in the third-party platform.

To enable third-party event reporting, select the relevant reporting authenticator from the list. All authenticators that have been assigned the **Reporting** method (**System Settings > Authenticators**) are listed.

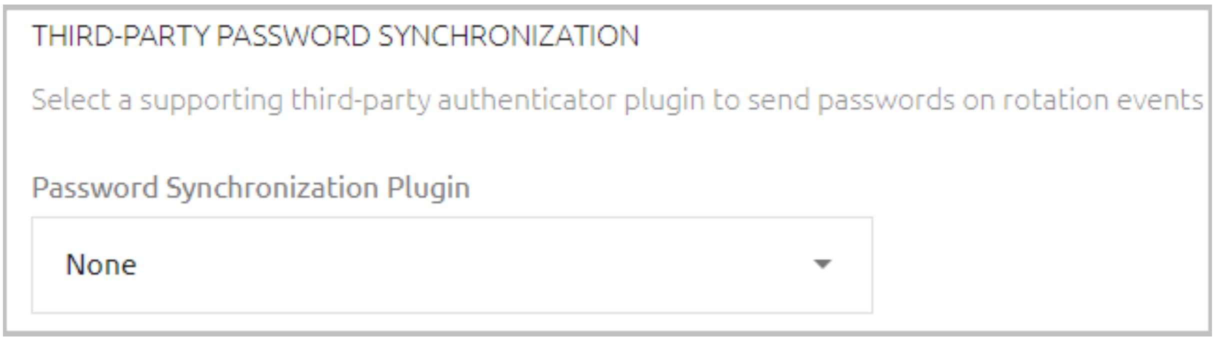

EVENT REPORTING

Select a supporting third-party authenticator plugin to receive authentication event logs

Reporting Plugin: None

### Third-party Password Synchronization

This feature enables you to designate a third-party authenticator that enables update of the AD password in specified external directories every time the Octopus Authentication Server performs password rotation. To enable password sync, select the relevant authenticator from the list. All authenticators that have been assigned the **Password Sync** method (**System Settings > Authenticators**) are listed.



THIRD-PARTY PASSWORD SYNCHRONIZATION

Select a supporting third-party authenticator plugin to send passwords on rotation events

Password Synchronization Plugin

None

## Configuring Directory Policy Settings

The **Policy** tab of a directory's settings contains parameters related to various security options, including:

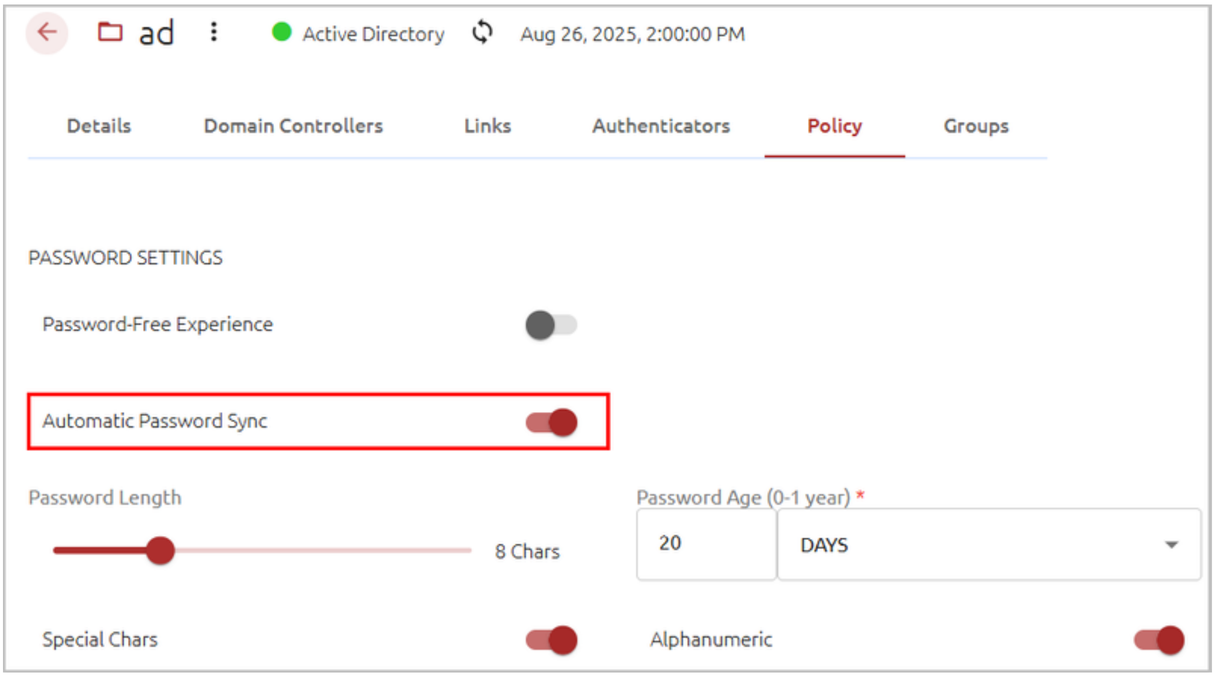
- Password Settings
- Temporary Bypass Token Settings
- Disabled Users Actions (AD)
- User Inactivity Actions
- Enrollment Email Setting
- Auto Enrolled Groups Settings

After updating settings in the **Policy** tab, click **Save** (at the bottom of the page). Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

### Password Settings

These settings include **Password-Free Experience** and **Automatic Password Sync**.

When **Automatic Password Sync** is activated (default setting), users will be able to authenticate using the Octopus mobile app even when the AD password has been changed by an entity outside of Enterprise Connect Passwordless (e.g., the organization's IT team). If there is a mismatch between the current password and the previous one, the Octopus Agent immediately sends a password reset request to the Octopus Authentication Server. The Server then sends an additional authentication request, including a verification code, to the mobile app with the following message to the user:
"**Password change detected. Approve to reset password and unlock machine**." Upon approval of the authentication request, the Server resets the user's AD password and allows login to the workstation.



PASSWORD SETTINGS

Password-Free Experience ○

Automatic Password Sync ●

Password Length 8 Chars

Password Age (0-1 year) * 20 DAYS

Special Chars ●

Alphanumeric ●

**Important**

If the **Automatic Password Sync** toggle is disabled, Octopus authentication will fail in the event of a password mismatch.

The **Password-Free Experience** toggle is related to support of the Password Free Experience on the Windows Agent. By default, this toggle is off, as the feature is not relevant when the system is working in Compatibility Mode. If you turn Compatibility Mode off, make sure to activate the **Password-Free Experience** toggle. When the toggle is on, the password settings below are disabled.

When Compatibility Mode is on, you can configure the following password settings:

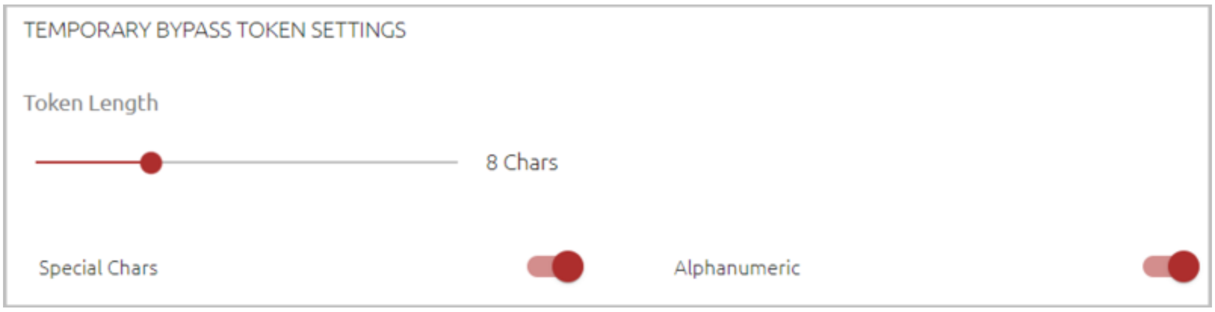
- **Password Length:** Number of characters in the password (4-20).
- **Password Age:** Period of time before the password expires. The maximum supported value is one year. If you enter a value of **0**, the system will **NOT** rotate the AD password, and the password will never expire on the Authentication Server.
- **Special Chars:** Determines whether the password must include special characters.
- **Alphanumeric:** Determines whether the password must include both letters and numbers.

**Important**

The settings you select here must match the applicable password policy in the directory.

### Temporary Bypass Token Settings

These settings determine the requirements for the authentication tokens issued to users who are in Bypass with Temporary Token mode. During the bypass period, these users can authenticate with a username and the token, so they can continue working.



TEMPORARY BYPASS TOKEN SETTINGS

Token Length

8 Chars

Special Chars

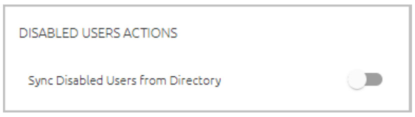
Alphanumeric

The settings are:

- **Token Length:** Drag the slider to the required value. Values range from 4-20 characters.
- **Special Chars:** When the setting is enabled, the token must contain at least one special character.
- **Alphanumeric:** When the setting is enabled, the token must contain both numbers and letters.

### Handling Disabled Users (AD only)

The **Disabled Users Actions** section appears only for Active Directory types that have Automatic Sync. When this setting is enabled, users who are currently disabled in the AD are included in the directory sync.



DISABLED USERS ACTIONS

Sync Disabled Users From Directory

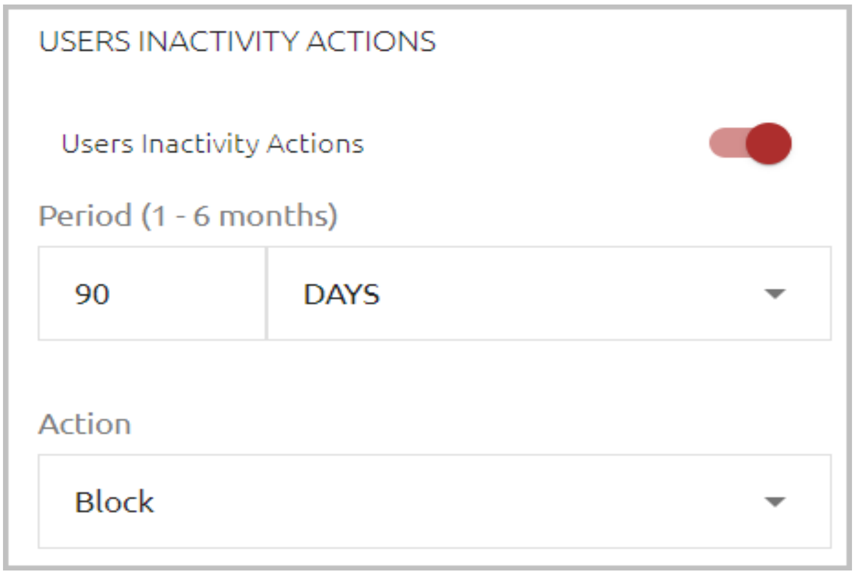
You may continue to send enrollment invitations to disabled users as necessary (e.g., during AD migrations).

### User Inactivity Actions

These settings allow you to block or unenroll users who have not authenticated for a specified period of time. By default, the Inactivity Action feature is off and no action is taken against inactive users.

**To set user inactivity actions:**

1. Activate the feature by clicking the **User Inactivity Actions** toggle button.



USERS INACTIVITY ACTIONS

Users Inactivity Actions ●

Period (1 - 6 months)

90 DAYS

Action

Block

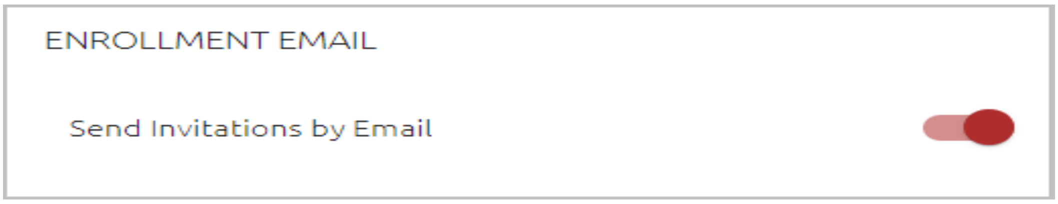
2. Specify the maximum period of time that can elapse from a user's last authentication until the inactivity action is taken. Valid values range from 30 days - 6 months.

3. From the **Action** dropdown list, select the inactivity action (**Block** or **Unenroll**).

4. At the bottom of the tab, click **Save**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

### Enrollment Email Setting

This setting allows you to control how enrollment invitations are delivered. By default, the toggle is enabled and invitations are automatically emailed to users. To support delivery of invitations by other means (e.g., internal organizational workflows), click the toggle to disable the setting, and then click **Save**. When the setting is disabled, invitations continue to be generated in the system but are not emailed to users.



ENROLLMENT EMAIL

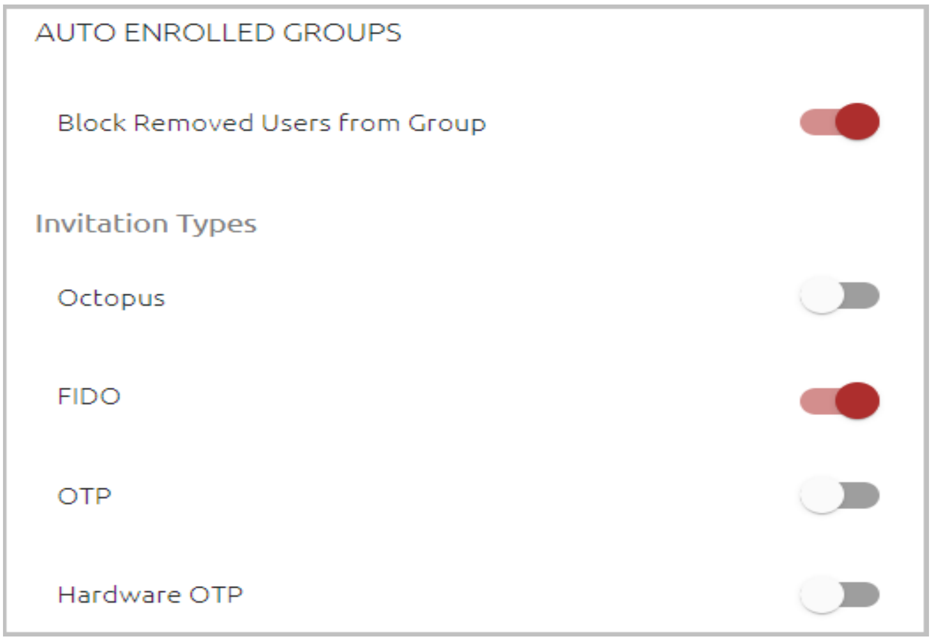
Send Invitations by Email ●

### Auto Enrolled Groups Settings

In Auto Enrolled Groups, enrollment invitations are sent to all Group members automatically. The **Auto Enrolled Groups** settings let you control the types of invitations that are sent and authentication ability for users who have been removed from the Active Directory.

**Note**

Auto Enrolled Groups settings appear only in directories for which automatic syncing is enabled.



AUTO ENROLLED GROUPS

Block Removed Users from Group

Invitation Types

Octopus

FIDO

OTP

Hardware OTP

The settings are:

- **Block Removed Users from Group** (for AD types only): Determines whether users who have been removed from the Active Directory are prevented from authenticating. By default, this setting is enabled (the users are blocked).
- **Invitation types:** Determines the type(s) of Octopus enrollment invitations that can be sent to Group members (Octopus Authenticator, FIDO, software OTP and hardware OTP token). Invitations that have been sent are listed in the **Invitations** tab for the Group and the users.

  If an authentication method is disabled or not currently assigned to the directory, a warning icon and message appear when that method is selected.

## Working with Selective Syncing (AD)

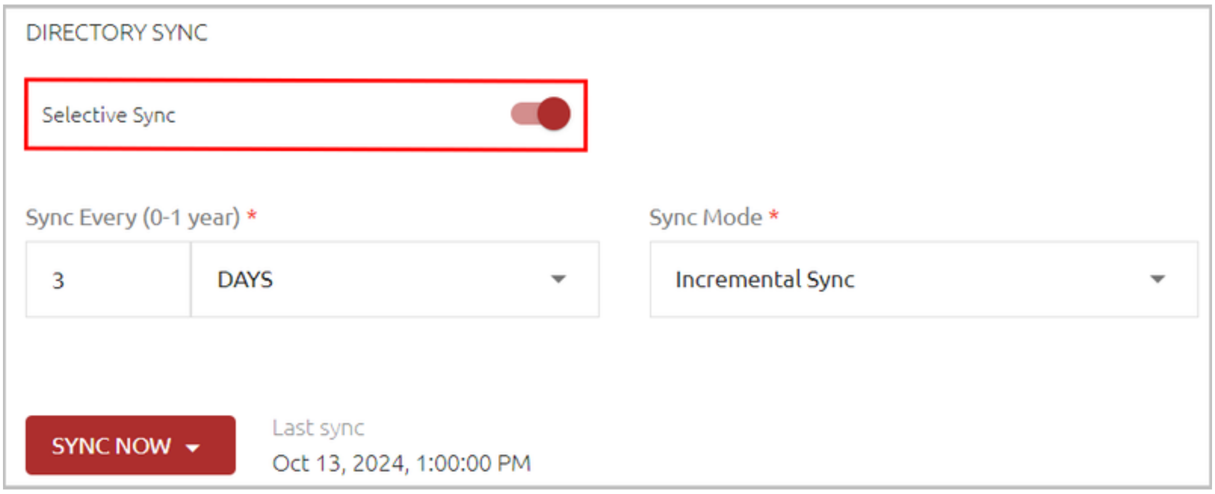
When an Active Directory type directory is created with Directory Sync, you can choose one of the following syncing options:

- **Full Sync:** All Groups in the directory are automatically synced with Enterprise Connect Passwordless.
- **Selective Sync:** Only the Groups specified in the Management Console (in the **Groups** tab of the directory's settings) are automatically synced.

**Important**

It is best practice to enable Selective Sync, for increased efficiency and reduced server load.

Use the **Selective Sync** toggle button to enable and disable selective sync. This toggle is at the bottom of the **Details** tab of the directory's settings.



DIRECTORY SYNC

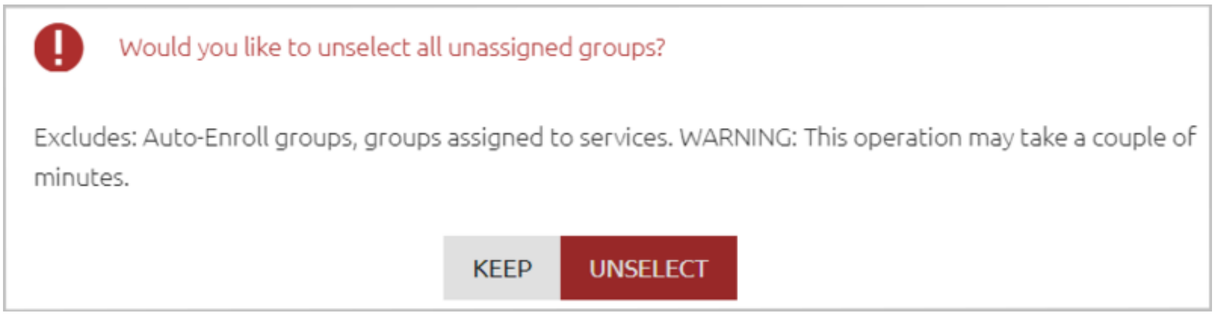
Selective Sync

Sync Every (0-1 year) *: 3 DAYS

Sync Mode *: Incremental Sync

Last sync
Oct 13, 2024, 1:00:00 PM

When you switch from Full Sync to Selective Sync, the following popup opens, prompting you to specify how to handle Groups that are currently *not* assigned to any services. (Groups assigned to services will continue to be synced.)

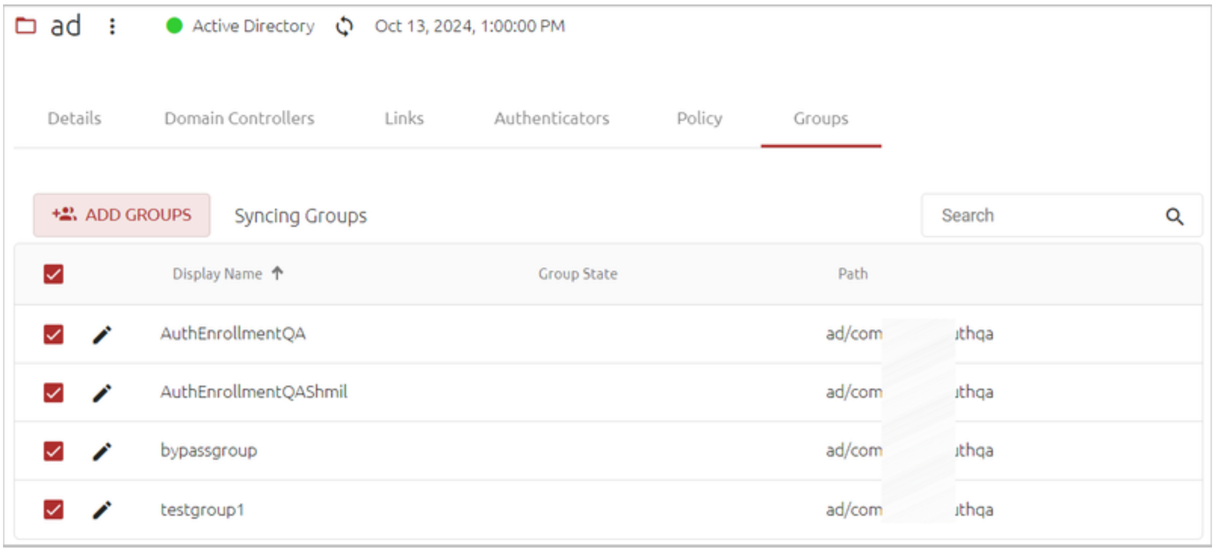


Would you like to unselect all unassigned groups?

Excludes: Auto-Enroll groups, groups assigned to services. WARNING: This operation may take a couple of minutes.

Choose one of the following options, and then click **Save**:

- **Unselect:** No Groups will be selected for syncing. You will need to specify which Groups are synced by adding them to the **Groups** tab (see the next section for details).
- **Keep:** All Groups will be selected for syncing. You will need to specify which Groups should *not* be synced by clearing their checkboxes in the **Groups** tab.



ad ⋮ ● Active Directory Oct 13, 2024, 1:00:00 PM

Syncing Groups

| ☑ | | Display Name ↑ | Group State | Path |
|---|---|---|---|---|
| ☑ | ✎ | AuthEnrollmentQA | | ad/com[redacted]thqa |
| ☑ | ✎ | AuthEnrollmentQAShmil | | ad/com[redacted]thqa |
| ☑ | ✎ | bypassgroup | | ad/com[redacted]thqa |
| ☑ | ✎ | testgroup1 | | ad/com[redacted]thqa |

### Selecting Groups for Automatic Directory Syncing

When Selective Sync is enabled for a directory, the **Groups** tab is enabled. This tab allows you to control which Groups in the Directory are automatically synced with Enterprise Connect Passwordless. You can change your Group selections at any time.

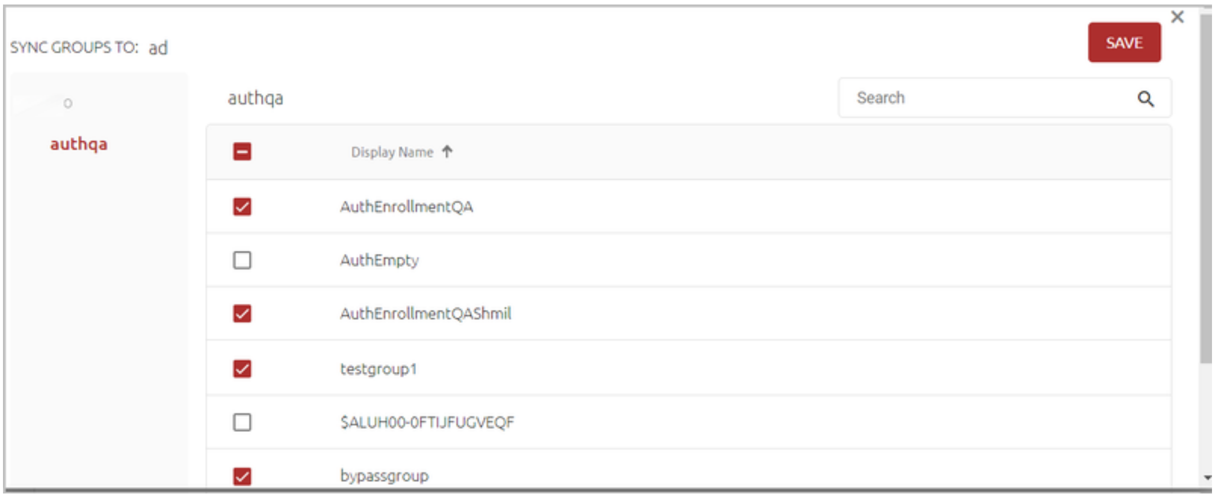
Follow the procedure below to specify Groups to be synced with the directory.

**To select Groups for automatic syncing:**

1. At the top of the **Groups** tab, click **Add Groups**.

   The **Sync Groups To** dialog opens.

2. On the left side of the dialog, expand the directory tree. Then, choose Groups to sync by selecting the relevant checkboxes. (The checkboxes of Groups previously selected for syncing are disabled.)

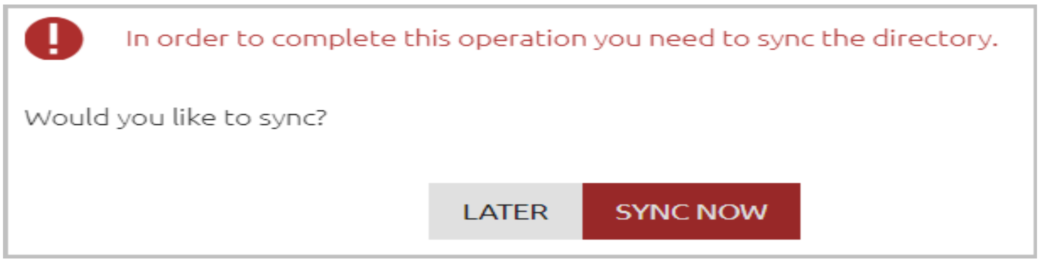


SYNC GROUPS TO: ad

| ☐ | Display Name ↑ |
|---|---|
| ☑ | AuthEnrollmentQA |
| ☐ | AuthEmpty |
| ☑ | AuthEnrollmentQAShmil |
| ☑ | testgroup1 |
| ☐ | $ALUH00-0FTIJFUGVEQF |
| ☑ | bypassgroup |

3. At the upper right corner of the dialog, click **Save**.

   A popup opens, prompting you to sync the directory.



In order to complete this operation you need to sync the directory.

Would you like to sync?

4. Click one of the following options:

   - **Later:** The Groups are added to the list of Groups for automatic syncing, but the users are not added until the next time a sync is done.

   - **Sync Now:** The Groups are added and users are immediately synced with the system.

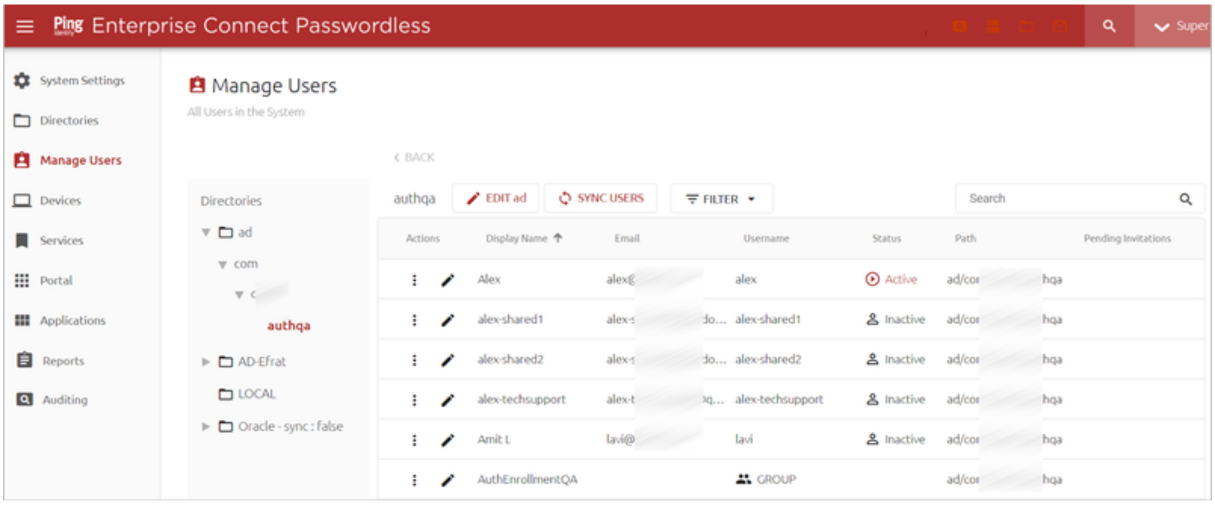
   The popup closes, and the selected Groups are listed in the **Groups** tab.

5. To stop automatic syncing of a selected Group, clear the relevant checkbox, and then click **Save.**

   To add more Groups to the automatic syncing process, repeat Steps 1-3.

## Managing Users

The **Manage Users** menu of the Management Console enables you to add and remove users, as well as perform administrative operations on any user.



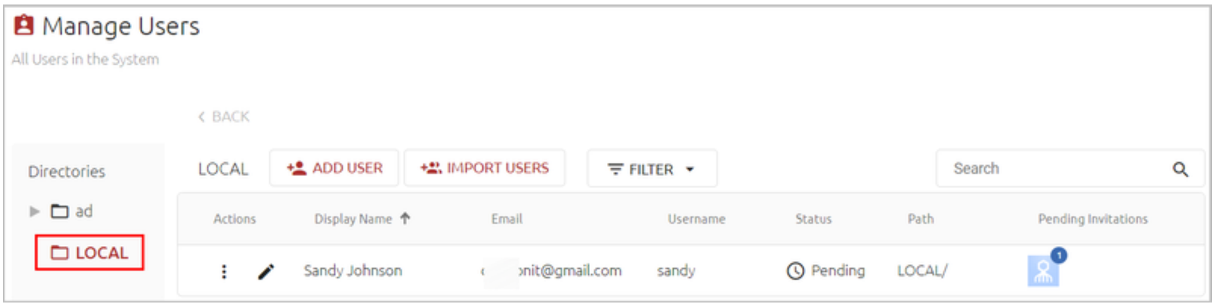
| Actions | Display Name | Email | Username | Status | Path | Pending Invitations |
|---|---|---|---|---|---|---|
| ⋮ ✎ | Alex | alex@[redacted] | alex | Active | ad/co[redacted]hqa | |
| ⋮ ✎ | alex-shared1 | alex-[redacted]do... | alex-shared1 | Inactive | ad/co[redacted]hqa | |
| ⋮ ✎ | alex-shared2 | alex-[redacted]do... | alex-shared2 | Inactive | ad/co[redacted]hqa | |
| ⋮ ✎ | alex-techsupport | alex-t[redacted]q... | alex-techsupport | Inactive | ad/co[redacted]hqa | |
| ⋮ ✎ | Amit L | lavi@[redacted] | lavi | Inactive | ad/co[redacted]hqa | |
| ⋮ ✎ | AuthEnrollmentQA | | GROUP | | ad/co[redacted]hqa | |

The following sections present:

- Understanding the Users List: Explains how to work with the Users List
- Working with Groups: Describes administrative operations that you can take on Groups
- Performing Actions on Users: Explains different administrative actions that you can take on individual users
- Adding Users to the Local Directory: Details methods for creating Local users
- Importing Users from a Directory: Describes how to import users from an integrated corporate directory
- Adding Users to a Federated Entra ID Directory: Describes how to add new users to a remote Entra ID directory

### Understanding the Users List

The Users List enables you to view details of any user by selecting the relevant directory and Group, or by performing a keyword search for the user or Group. By default, the Users List displays all the users in the Local directory.

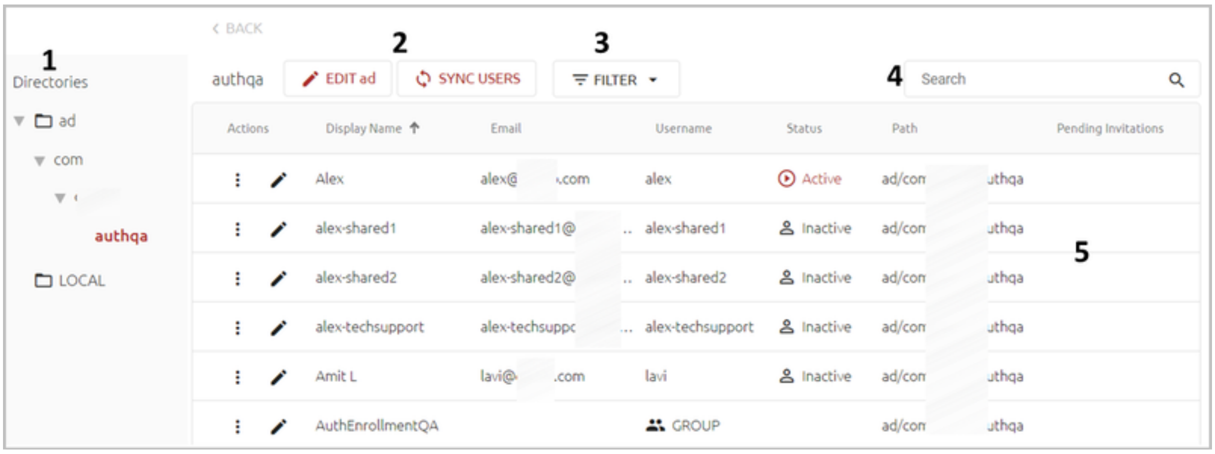


| Actions | Display Name | Email | Username | Status | Path | Pending Invitations |
|---|---|---|---|---|---|---|
| ⋮ ✎ | Sandy Johnson | [redacted]nit@gmail.com | sandy | Pending | LOCAL/ | 1 |

The Local directory is a default, internal directory that cannot be deleted. Users are added to the Local directory by manually creating them or by importing them from a CSV file. The Local directory is useful for organizations that do not manage users through external directories.

Unlike other integrated directories, the Local directory does not have directory settings. Local users therefore cannot utilize options that are configured per directory, such as 3rd party authenticators, OTP authentication and more. Local users can be assigned to SAML, RADIUS and REST API services, to which they can authenticate through the Octopus Authenticator or FIDO authentication only. (They cannot be assigned to LDAP or Active Directory Authentication services.) If services require a password for multifactor authentication, you can set a password for Local users in the **Security** tab of the user's settings. Local users can also use this password to access the Management Console.

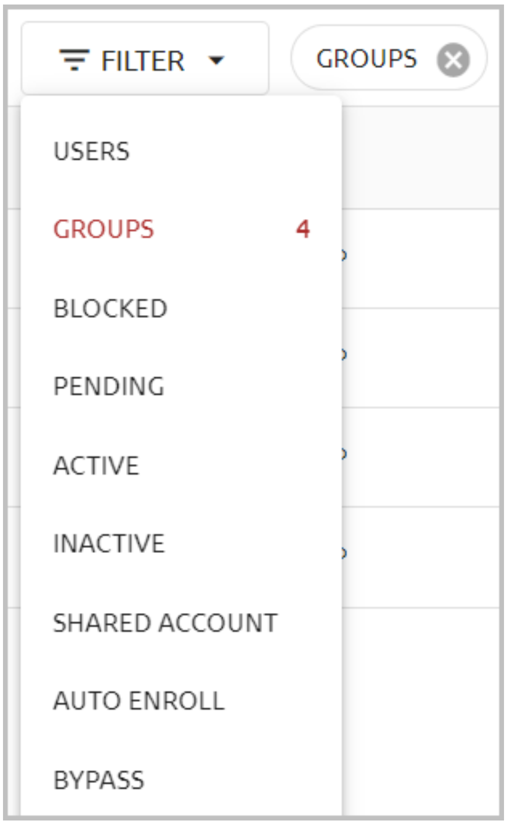
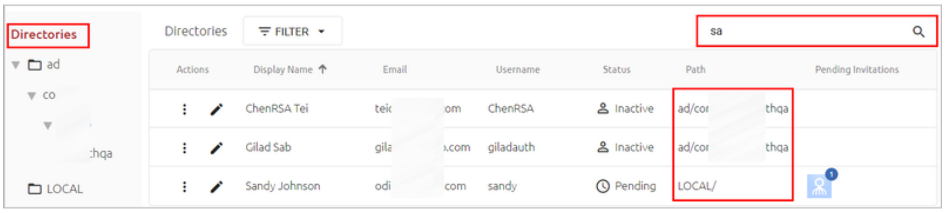
The main portions and features of the Users List are described in the table below the diagram.



| Actions | Display Name | Email | Username | Status | Path | Pending Invitations |
|---|---|---|---|---|---|---|
| ⋮ ✎ | Alex | alex@[redacted].com | alex | Active | ad/con[redacted]uthqa | |
| ⋮ ✎ | alex-shared1 | alex-shared1@[redacted] | alex-shared1 | Inactive | ad/con[redacted]uthqa | |
| ⋮ ✎ | alex-shared2 | alex-shared2@[redacted] | alex-shared2 | Inactive | ad/con[redacted]uthqa | |
| ⋮ ✎ | alex-techsupport | alex-techsuppc[redacted] | alex-techsupport | Inactive | ad/con[redacted]uthqa | |
| ⋮ ✎ | Amit L | lavi@[redacted].com | lavi | Inactive | ad/con[redacted]uthqa | |
| ⋮ ✎ | AuthEnrollmentQA | | GROUP | | ad/con[redacted]uthqa | |

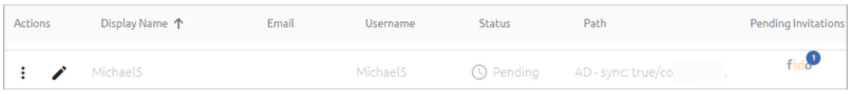
| Number | Feature | Description / Notes |
|---|---|---|
| 1 | Directories tree | Lists all configured directories and their folders. For more information, refer to Working with the Directories Tree. |

| Number | Feature | Description / Notes |
|---|---|---|
| 2 | Directory action buttons | Provide quick access to common directory management actions.<br>The actions for the Local directory are **Add User** (allows you to manually create a Local user) and **Import Users** (allows you to upload Local users from a CSV file). For details, refer to Adding Users to the Local Directory.<br>The actions for integrated corporate directories can include:<br>• **Edit**: Redirects to the directory's settings. This action appears for all directories.<br>• **Sync Users:** This button, which initiates the directory sync process, is available for directories with automatic sync enabled.<br>• **Import Users:** This button is available for directories without automatic sync. Click to import users in a bulk operation.<br>• **Create User** (federated Entra ID directory types only): Click to add a user directly to the remote Entra ID directory. For more information, refer to Adding Users to a Federated Entra ID Directory. |

| Number | Feature | Description / Notes |
|---|---|---|
| 3 | Filtering options | Open the **Filter** list to view statistics about the currently displayed list, such as total number of Groups, total number of users, number of blocked users and so on. (These numbers vary according to the node / folder selected in the Directories tree.)<br>Clicking a filtering option filters the list according to the selected option (e.g., clicking Pending displays only users with a Pending status). The currently selected filter is displayed in a chip next to the **Filter** list. For example:<br> |
| 4 | Search tool | To quickly locate a Group or user, type all or part of the Group name or the user's display name, username or email in the **Search** field. If you are currently viewing a directory, the search returns only Groups and users in the currently selected directory. If the root of the Directories Tree is selected, the search is performed across all directories.<br> |

sa

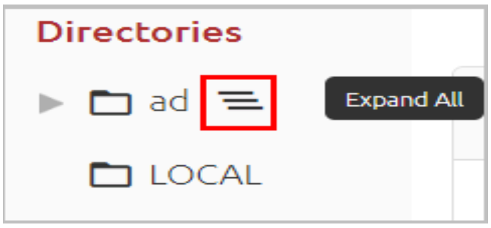
| Actions | Display Name ↑ | Email | Username | Status | Path | Pending Invitations |
|---|---|---|---|---|---|---|
| ⋮ ✎ | ChenRSA Tei | teic [redacted] om | ChenRSA | Inactive | ad/coı [redacted] thqa | |
| ⋮ ✎ | Gilad Sab | gila [redacted] .com | giladauth | Inactive | ad/coı [redacted] thqa | |
| ⋮ ✎ | Sandy Johnson | odi [redacted] com | sandy | Pending | LOCAL/ | 1 |

| Number | Feature | Description / Notes |
|---|---|---|
| 5 | User list | Lists basic details about the Groups and users in the currently selected node of the Directories Tree. You can sort the list according to any column by clicking the column header.<br>In the **Username** column, Groups are indicated by the 👥 icon. The 👥 icon indicates a shared account.<br>A user's **Status** can be one of the following:<br>▶ **Active:** The user has enrolled in an account, created a PIN or verified a FIDO key set, and is authorized to authenticate using the Octopus Authenticator.<br>👤 **Inactive:** The user is not enrolled in the system and has no pending enrollment invitations.<br>🕓 **Pending:** The user has pending invitations but has not yet enrolled in the system.<br>⊘ **Blocked:** The user is currently not authorized to authenticate using the Octopus Authenticator, PIN or FIDO key.<br>If a user is disabled in the Active Directory server, the row of that user in the Users list is disabled. You may continue to send and manage enrollment invitations for disabled users, but no other actions can be performed on them.<br> |

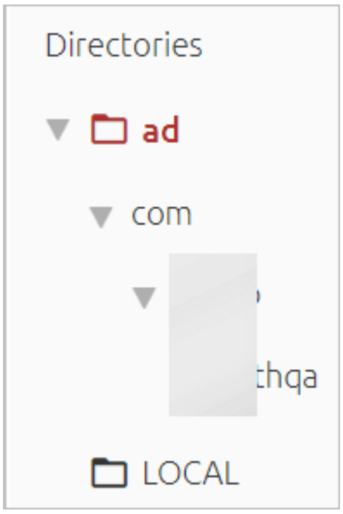
| Actions | Display Name ↑ | Email | Username | Status | Path | Pending Invitations |
|---|---|---|---|---|---|---|
| ⋮ ✎ | Michael5 | | Michael5 | 🕓 Pending | AD - sync: true/co | fido 1 |

## Working with the Directories Tree

The Directories list on the left side of the page lists the Local directory, as well as all other directories that have been integrated with the Management Console. It is organized in a tree format. The Expand All icon appears when you hover over any node that contains sub-nodes. For example:



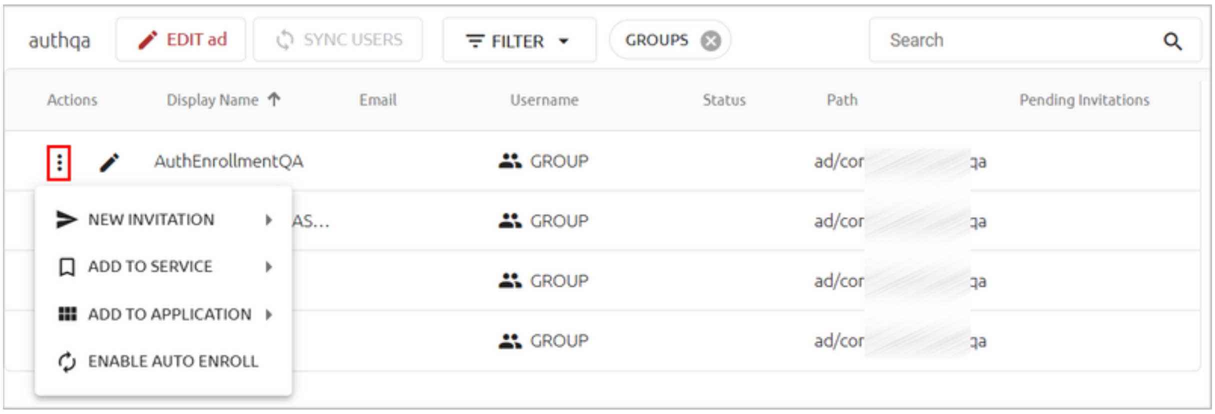
Clicking this icon automatically opens all the sub-nodes beneath the selected node:



You can then select any Group or user and view relevant details. For more information, refer to Working with Groups and Performing Actions on Users.

## Working with Groups

For convenience, you can perform some common administrative actions on Groups directly from the Users list, by clicking ⋮ in the row of the Group and then selecting the relevant action.

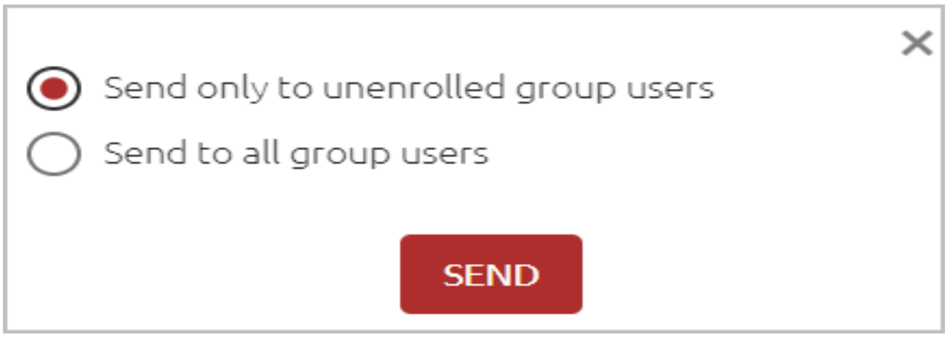


| Actions | Display Name | Email | Username | Status | Path | Pending Invitations |
|---|---|---|---|---|---|---|
| ⋮ | AuthEnrollmentQA | | GROUP | | ad/cor[redacted] | |
| | AS... | | GROUP | | ad/cor[redacted] | |
| | | | GROUP | | ad/cor[redacted] | |
| | | | GROUP | | ad/cor[redacted] | |

The available actions are:

- **New Invitation:** Issues email invitations to all Group members. You can invite the members to enroll in the Octopus Authenticator app, register a FIDO key (FIDO Authenticator), obtain software one-time passwords (OTP Authenticator) or register a hardware OTP token.

  If some Group members are already enrolled, the following popup will open, prompting you to specify whether to send the invitations to the entire Group or only to the members who are not yet enrolled:



● Send only to unenrolled group users

○ Send to all group users

**Important**

In order to enable users to authenticate to Windows using a FIDO key, the corporate directory must have a configured domain. It is recommended to open the directory settings and verify that the **Domain** field is completed.

If the Windows agent is configured with both an internal and external Endpoint URL, users need to enroll their FIDO devices using the internal URL only.

- **Add To Service:** Enables you to control which services are enabled for the Group, by selecting or clearing the checkboxes. The services listed are the ones that are available for directories to which the Group belongs.

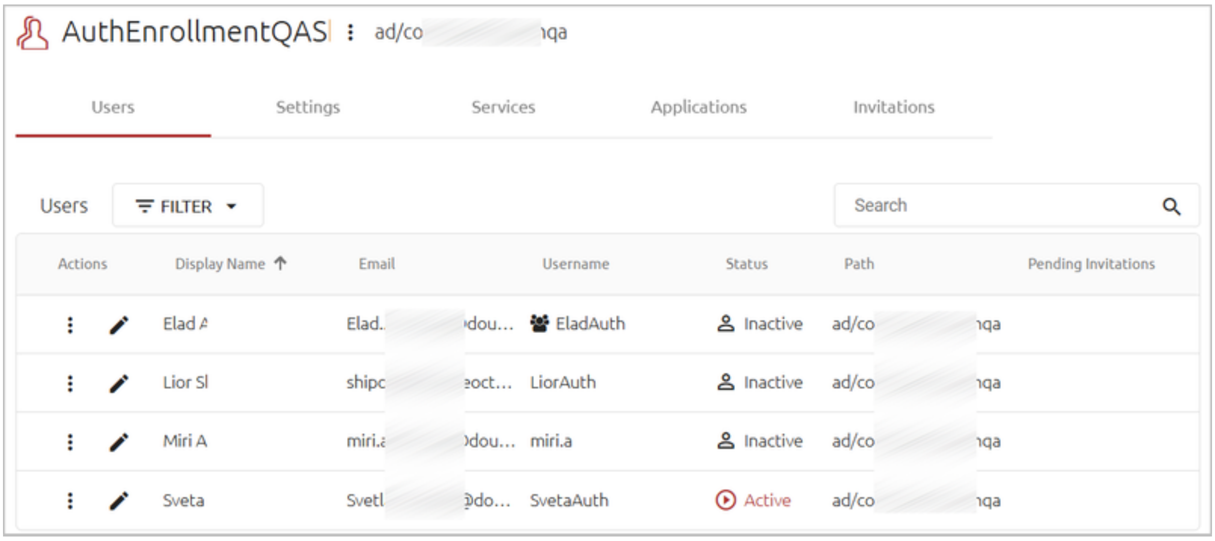
  If a service is not listed, open the settings of the relevant service and verify that the appropriate directory is selected. For more information, refer to Assigning Directories and Users to a Service.

- **Add to Application:** Enables you to control which integrated applications are enabled for the Group, by selecting or clearing the checkboxes. The applications listed are the ones that are available for directories to which the Group belongs.

  If an application is not listed, open the settings of the relevant application and verify that the appropriate directory is selected. For more information, refer to Assigning Directories and Users to Applications.

- **Enable / Disable Auto Enroll:** Sets Auto Enrollment for the Group. In Auto Enrolled Groups, the system automatically sends enrollment emails to all Group members who are not yet enrolled.

Clicking ✎ in the row of a Group opens the **Users** tab. This tab lists the subgroups and users assigned to the Group, and displays general information about each one. Open the **Filter** list to view the number of subgroups and users in the Group, as well as other relevant information about Group entities. You can perform actions on individual users directly from this list. (For more information about user actions, refer to Performing Actions on Users.)



AuthEnrollmentQAS ⋮ ad/co[redacted]ıqa

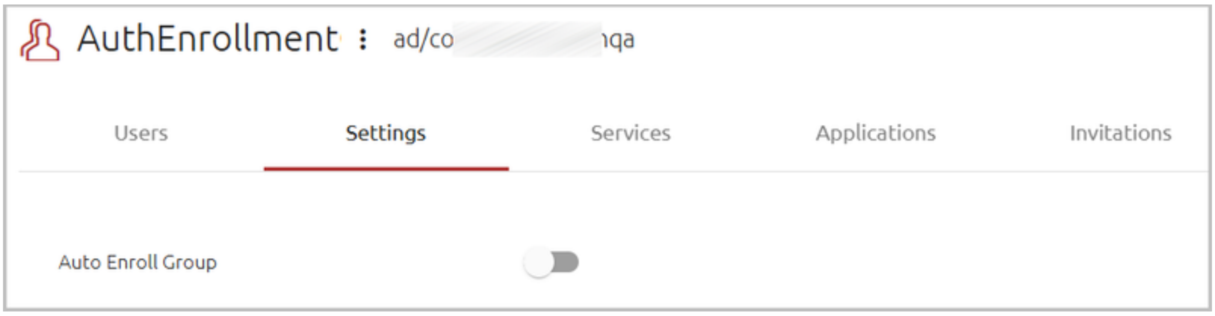
Users

| Actions | Display Name ↑ | Email | Username | Status | Path | Pending Invitations |
|---|---|---|---|---|---|---|
| ⋮ ✎ | Elad A | Elad.[redacted]dou… | EladAuth | Inactive | ad/co[redacted]ıqa | |
| ⋮ ✎ | Lior Sl | shipc[redacted]oct… | LiorAuth | Inactive | ad/co[redacted]ıqa | |
| ⋮ ✎ | Miri A | miri.a[redacted]dou… | miri.a | Inactive | ad/co[redacted]ıqa | |
| ⋮ ✎ | Sveta | Svetl[redacted]@do… | SvetaAuth | Active | ad/co[redacted]ıqa | |

Clicking ⋮ (to the right of the Group name) opens a quick access menu that enables you to perform the actions described above (**New Invitation**, **Add To Service**, etc.). This menu is available from each of the tabs at the Group level.

The following additional tabs are available:

- **Settings:** Enables you to control the **Auto Enroll Group** setting for the Group. When the toggle is enabled, every new user in the Group is sent an automatic invite.

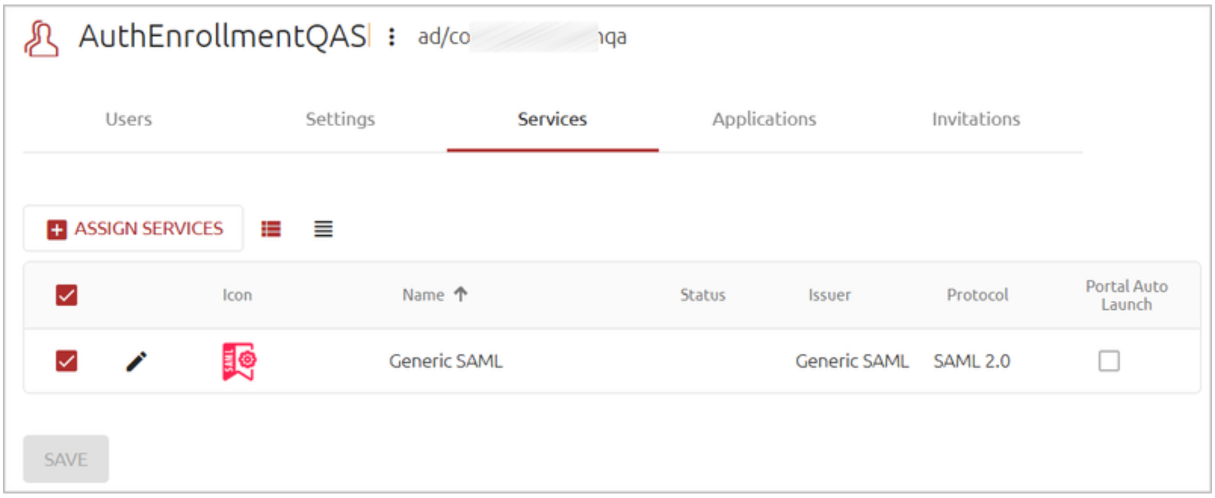


AuthEnrollment ⋮ ad/co[redacted]ıqa

Auto Enroll Group

- **Services:** Displays the services that the Group is currently authorized to access. The checkboxes on the left are toggles that allow you to control whether that service is enabled for the Group. In the example below, the service is enabled.

  Clicking ✎ in the row of a service redirects you to another page where you can update the settings for that service.

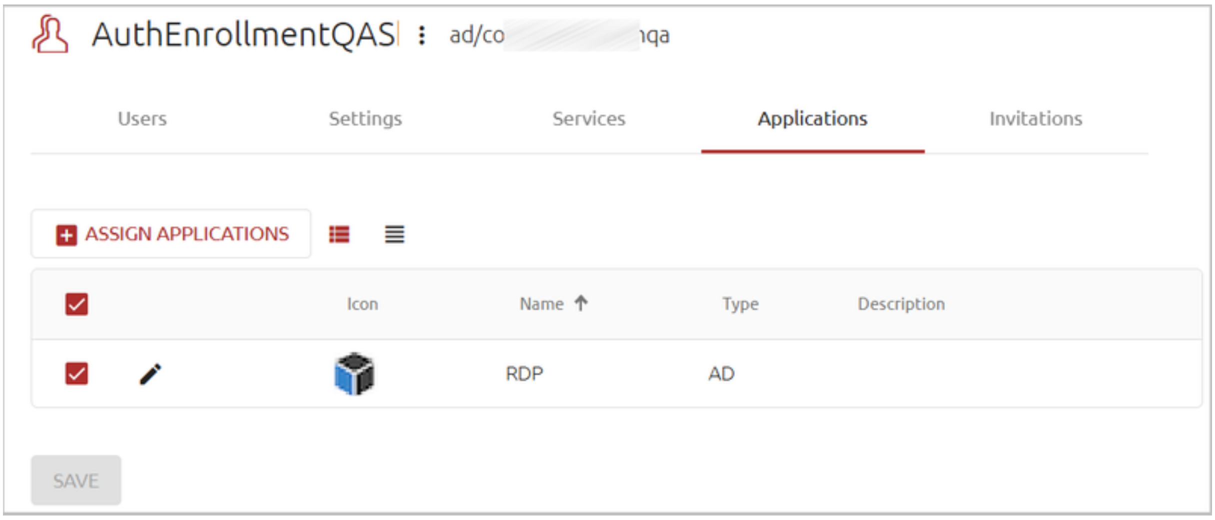


| ☑ | | Icon | Name ↑ | Status | Issuer | Protocol | Portal Auto Launch |
|---|---|---|---|---|---|---|---|
| ☑ | ✏ | | Generic SAML | | Generic SAML | SAML 2.0 | □ |

To assign additional services to the Group, click **Assign Services**. In the dialog that opens, specify the services to add by selecting the relevant checkboxes, and then click **Save**.

The services listed in the **Assign Services** dialog are ones to which the Group is *not* currently assigned AND which may be used by directories to which the Group belongs. If a service is not listed in the dialog, open the settings of the service and verify that the appropriate directory is selected. For more information, refer to Assigning Directories and Users to a Service.

- **Applications:** Displays the integrated applications that the Group is currently authorized to access. The checkboxes on the left are toggles that allow you to control whether that application is enabled for the Group. Clicking ✏ in the row of an application redirects you to another page where you can view and update settings for the application.

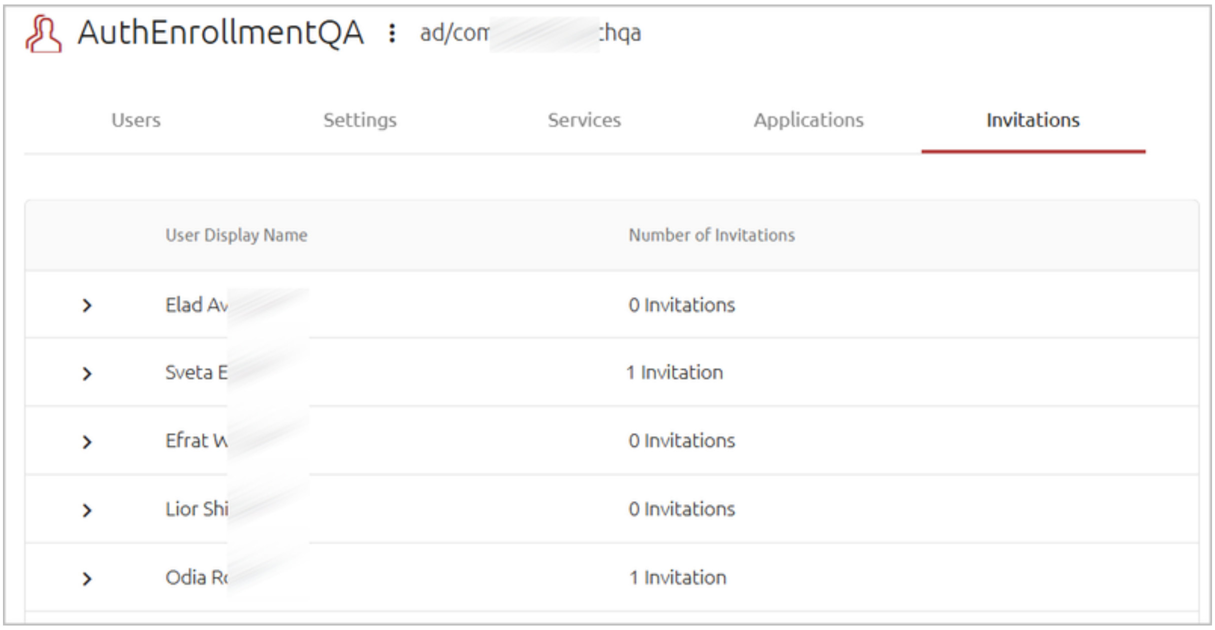


| ☑ | | Icon | Name ↑ | Type | Description |
|---|---|---|---|---|---|
| ☑ | ✏ | | RDP | AD | |

To assign additional applications to the Group, click **Assign Applications**. In the dialog that opens, specify the applications to add by selecting the relevant checkboxes, and then click **Save**.

The applications listed in the **Assign Applications** dialog are ones to which the Group is *not* currently assigned AND which may be used by directories to which the Group belongs. If an application is not listed in the dialog, open the settings of the application and verify that the appropriate directory is selected. For details, refer to Assigning Directories to Applications.

- **Invitations:** Lists the number of pending invitations sent to each member of the Group.

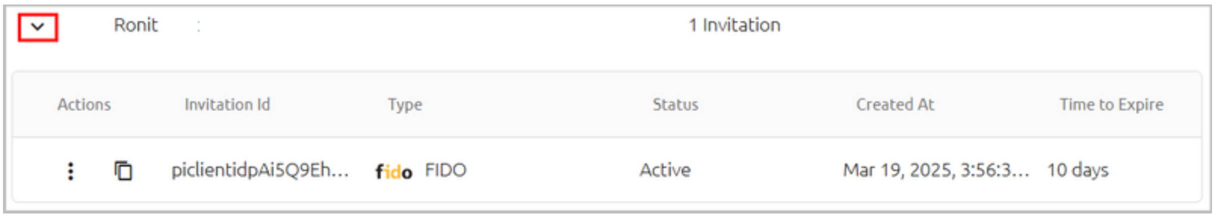


AuthEnrollmentQA ⋮ ad/com[redacted]hqa

| | User Display Name | Number of Invitations |
|---|---|---|
| › | Elad Av[redacted] | 0 Invitations |
| › | Sveta E[redacted] | 1 Invitation |
| › | Efrat W[redacted] | 0 Invitations |
| › | Lior Shi[redacted] | 0 Invitations |
| › | Odia R[redacted] | 1 Invitation |

When a row is expanded, details about each invitation, such as its identifier, authentication type and creation date are displayed. The **Status** column shows the handling workflow for the invitation. This workflow is determined by whether the user is already published in the system or is new. Possible statuses are:

- ○ **Waiting for Publish:** The user has not yet been synced and published in the system. The invitation is being stored as a pending invitation and will be sent to the user as soon as the next Publish process completes successfully.
- ○ **Active:** The user is published in the system and the invitation has been sent.



Ronit 1 Invitation

| Actions | Invitation Id | Type | Status | Created At | Time to Expire |
|---|---|---|---|---|---|
| ⋮ ⧉ | piclientidpAi5Q9Eh... | fido FIDO | Active | Mar 19, 2025, 3:56:3... | 10 days |

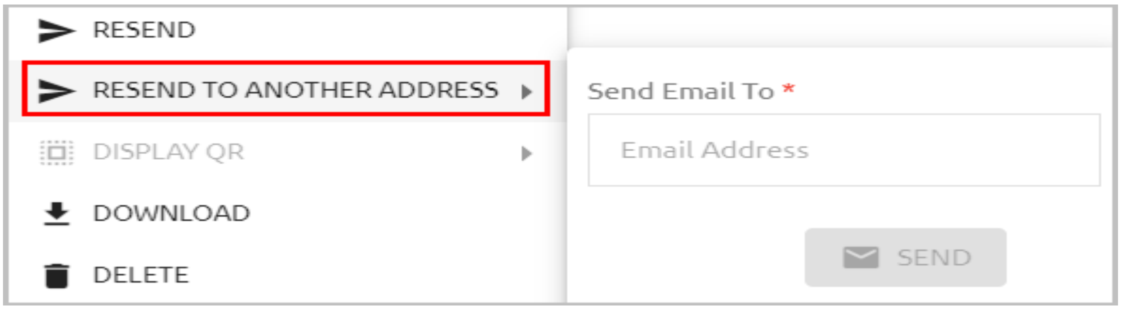
Clicking ⧉ copies the invitation's enrollment link or code, according to invitation type:

- ○ **Octopus type invitations:** The Copy action copies the Invitation ID, which is then converted to the manual enrollment code provided in the invitation.

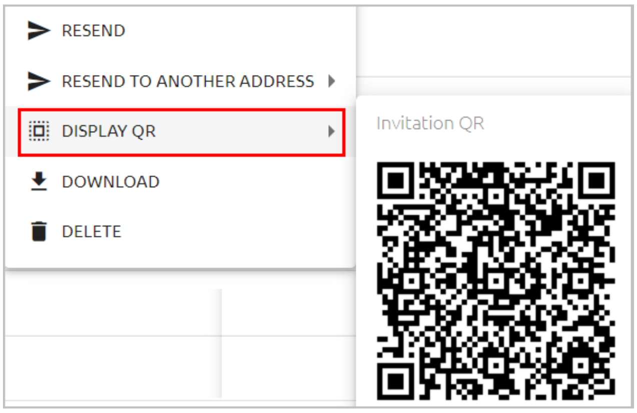
- **FIDO / OTP type invitations:** The Copy action copies the link for registration provided in the invitation.

Clicking ⋮ opens an actions menu for the selected invitation. The actions are:

- **Resend:** Sends the invitation to the email address recorded in the system for the user (in the **Personal** tab of the user details).
- **Resend To Another Address:** Sends the invitation to an email address other than the one recorded in the system. When selecting this option, enter the address in the field that opens, and then click **Send.**



- **Display QR:** Shows the enrollment QR provided with the invitation. This action is relevant for Octopus type invitations only.



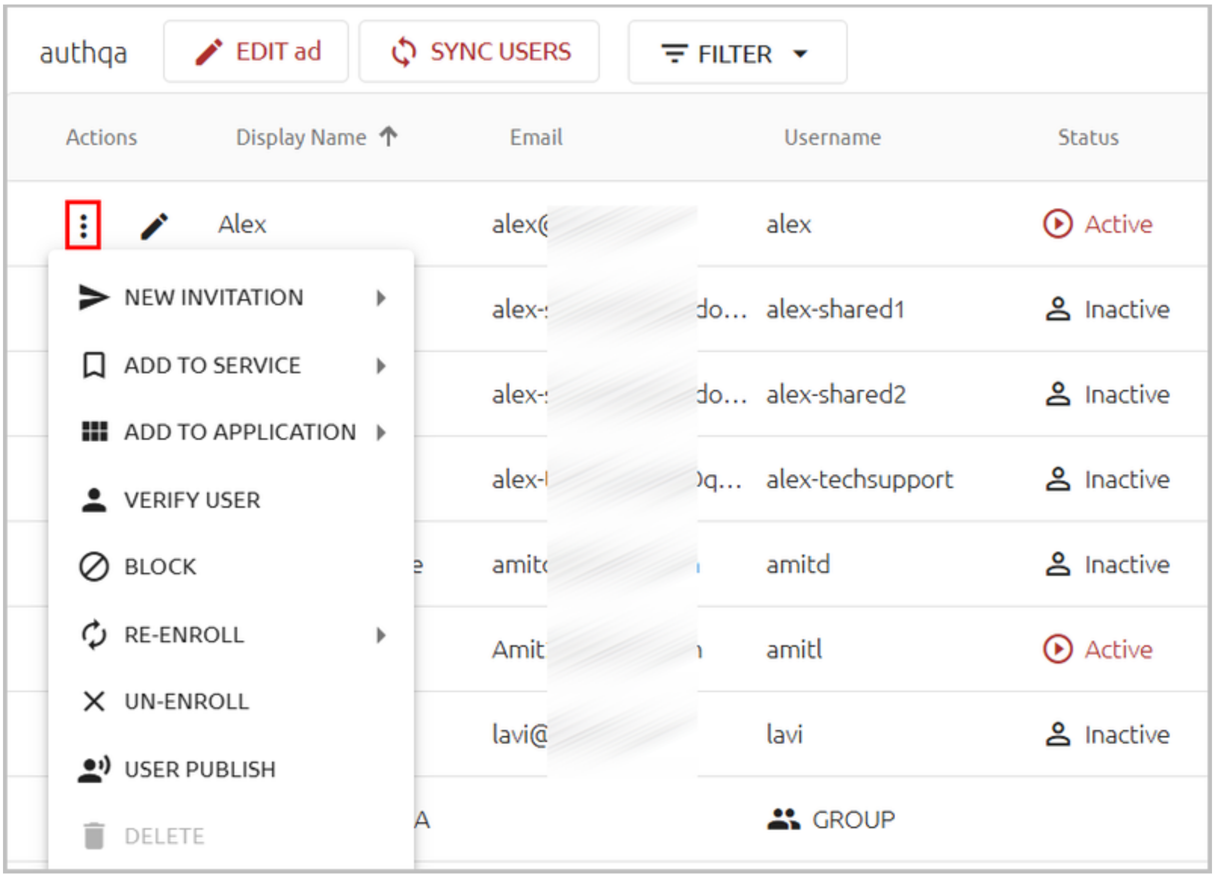
- **Download:** Saves the invitation as an email file and downloads it to your machine.
- **Delete:** Removes the invitation from the system.

**Note**

The Resend and Download actions are not available for invitations with a **Waiting for Publish** status.

## Performing Actions on Users

For convenience, you can perform some common administrative actions on a user directly from the Users list, by clicking ⋮ in the row of the user and then selecting the relevant action.



| Actions | Display Name | Email | Username | Status |
|---|---|---|---|---|
| | Alex | alex@[redacted] | alex | Active |
| | | alex-[redacted]do… | alex-shared1 | Inactive |
| | | alex-[redacted]do… | alex-shared2 | Inactive |
| | | alex-[redacted]0q… | alex-techsupport | Inactive |
| | e | amit[redacted] | amitd | Inactive |
| | | Amit[redacted] | amitl | Active |
| | | lavi@[redacted] | lavi | Inactive |
| | A | | GROUP | |

The available actions are:

- **New Invitation:** Sends the user an invitation via email. You can invite users to enroll in the Octopus Authenticator app, register a FIDO key, obtain software one-time passwords (**OTP Authenticator**) or register a hardware OTP token. For more information about invitation management, refer to Managing User Invitations.

**Important**

In order to enable users to authenticate to Windows using a FIDO key, the corporate directory must have a configured domain. It is recommended to open the directory settings and verify that the **Domain** field is completed.

If the Windows agent is configured with both an internal and external Endpoint URL, users need to enroll their FIDO devices using the internal URL only.

- **Add To Service:** Enables you to control which services are enabled for the user, by selecting or clearing the checkboxes. The services listed are the ones that are available for directories to which the user belongs.

  If a service is not listed, open the settings of the relevant service and verify that the appropriate directory is selected. For more information, refer to Assigning Directories and Users to a Service.

- **Add to Application:** Enables you to control which integrated applications are enabled for the user, by selecting or clearing the checkboxes. The applications listed are the ones that are available for directories to which the user belongs.

If an application is not listed, open the settings of the relevant application and verify that the appropriate directory is selected. For more information, refer to Assigning Directories and Users to Applications.

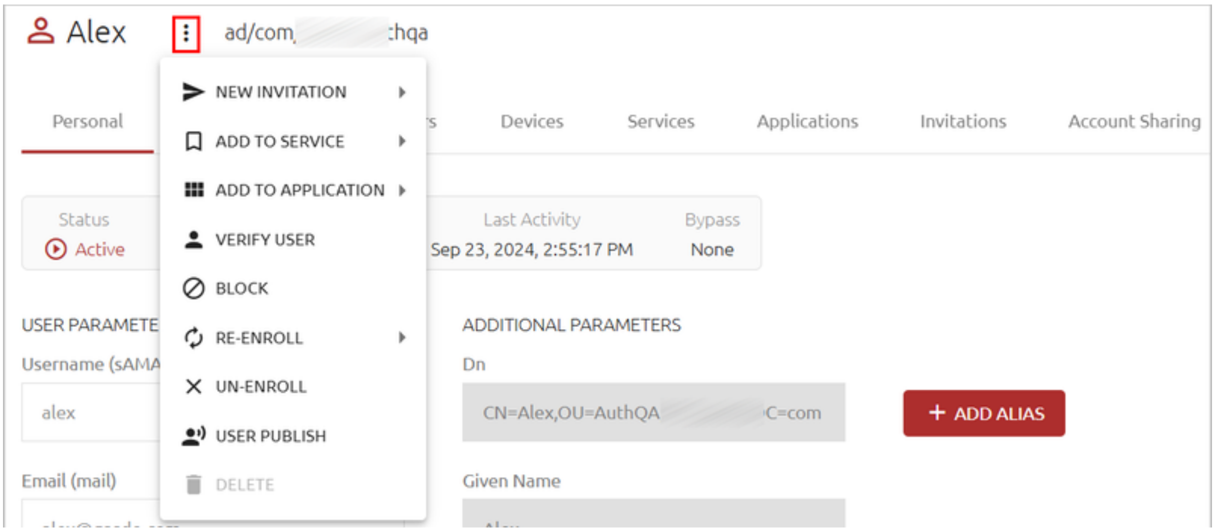
- **Verify User:** Sends an authentication request to the user, in order to verify the user's identity.
- **Block/Unblock:** The Block action prevents the user from authenticating with Octopus Authenticator, PIN or FIDO key. Unblock reverses the Block action.
- **Re-enroll:** Removes user enrollment and sends the user an invitation to enroll again.
- **Un-enroll:** Removes user enrollment without sending a re-enrollment invitation.
- **User Publish:** Generates an immediate publishing process for actions (e.g., enrollment invitations) and updates (e.g., adding a service) affecting the user.

  **Note:** After *removing* a user from a service, a full publish is required.
- **Delete:** Removes the user and all the user's devices from the system. (If the directory has Auto Sync enabled, this option is not available.)

**Note**

**New Invitation** is the only action available for users who are disabled in the Active Directory server.

Clicking ✎ in the the row of a user opens a page from which you can view and manage user details. At the top of the page, the full path of the user's directory appears to the right of the user's name. Clicking ⋮ opens a quick access actions list that enables you to perform common administrative operations on the user (as described above).



ad/com[redacted]hqa

Status: Active

Last Activity: Sep 23, 2024, 2:55:17 PM

Bypass: None

USER PARAMETE

Username (sAMA: alex

Email (mail)

ADDITIONAL PARAMETERS

Dn: CN=Alex,OU=AuthQA[redacted]C=com

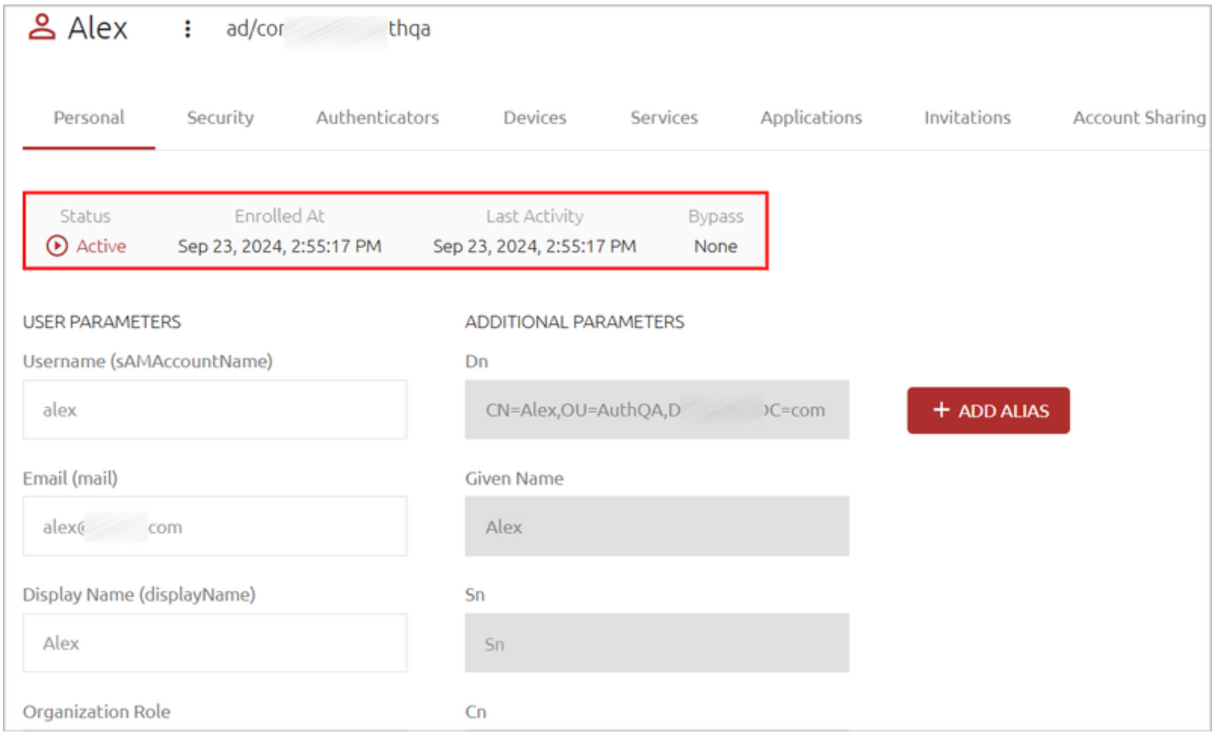
Given Name

The following tabs allow you to view and update settings, parameters and resources related to the user:

- **Personal:** This tab, which is displayed by default when the page opens, lists general information such as username, email, role and aliases. The data in the

**Additional Parameters** column are fields that are imported from the user's directory. (For more information about working with directory fields, refer to Using the Schema Mapping Script.)

The bar at the top of the **Personal** tab shows the user's status (Active, Inactive, Pending or Blocked), date / time of enrollment, date / time of the user's most recent activity, and details related to Octopus Authentication Bypass.



| Status | Enrolled At | Last Activity | Bypass |
|---|---|---|---|
| Active | Sep 23, 2024, 2:55:17 PM | Sep 23, 2024, 2:55:17 PM | None |

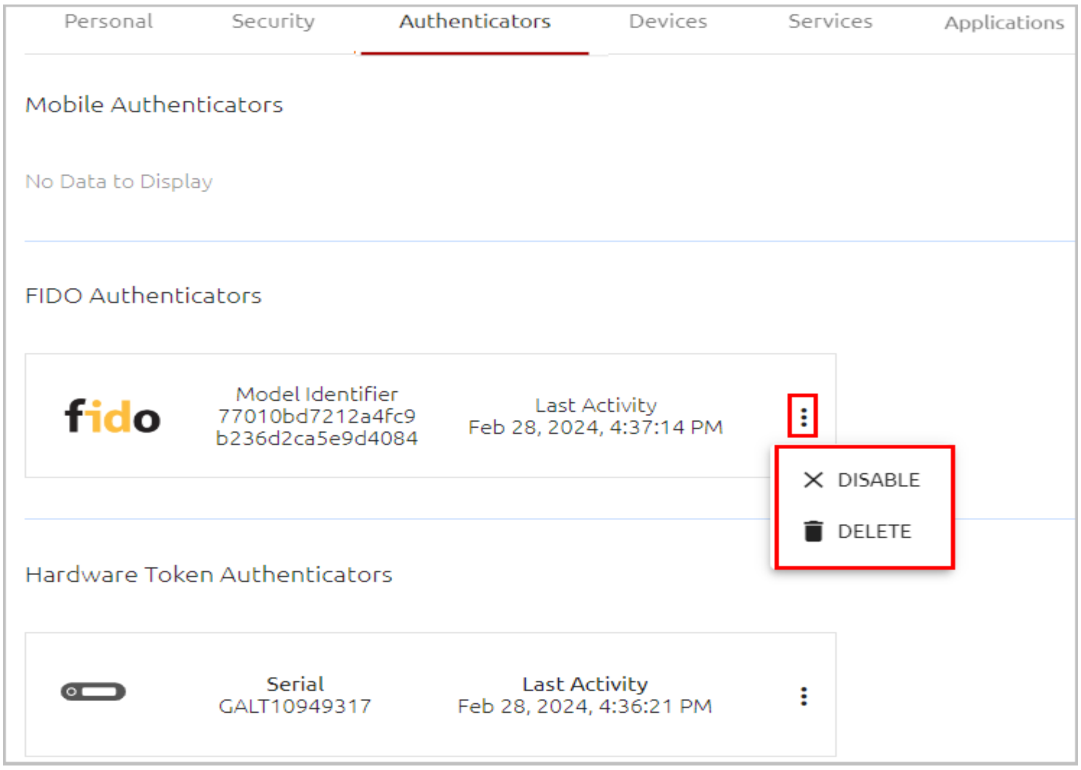
| USER PARAMETERS | ADDITIONAL PARAMETERS |
|---|---|
| Username (sAMAccountName): alex | Dn: CN=Alex,OU=AuthQA,D[redacted]DC=com |
| Email (mail): alex[redacted]com | Given Name: Alex |
| Display Name (displayName): Alex | Sn: Sn |
| Organization Role | Cn |

- **Security:** Allows you to perform various security-related operations, such as setting passwords and PIN codes. For more information, refer to Setting Security Parameters.
- **Authenticators:** Lists all integrated phones, FIDO keys and hardware OTP tokens of the user and provides basic information (e.g., OS version, model identifier, etc.) about each one.

**Note**

This tab does not appear for users who are disabled in the Active Directory server.

Clicking ⋮ opens an actions list that allows you to enable / disable the device, or remove it from the system.



Mobile Authenticators

No Data to Display

FIDO Authenticators

Model Identifier 77010bd7212a4fc9 b236d2ca5e9d4084

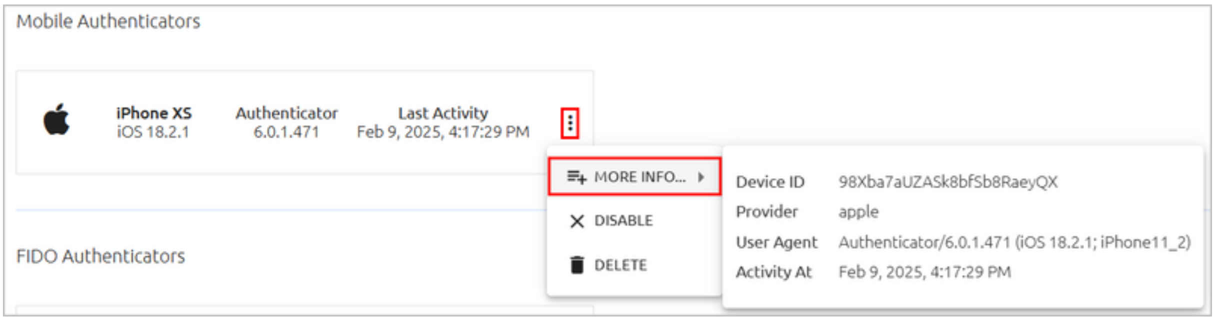
Last Activity Feb 28, 2024, 4:37:14 PM

Hardware Token Authenticators

Serial GALT10949317

Last Activity Feb 28, 2024, 4:36:21 PM

Mobile authenticators also have a **More Info** action. Selecting this action enables you to view additional details, including Device ID.


Mobile Authenticators

iPhone XS iOS 18.2.1

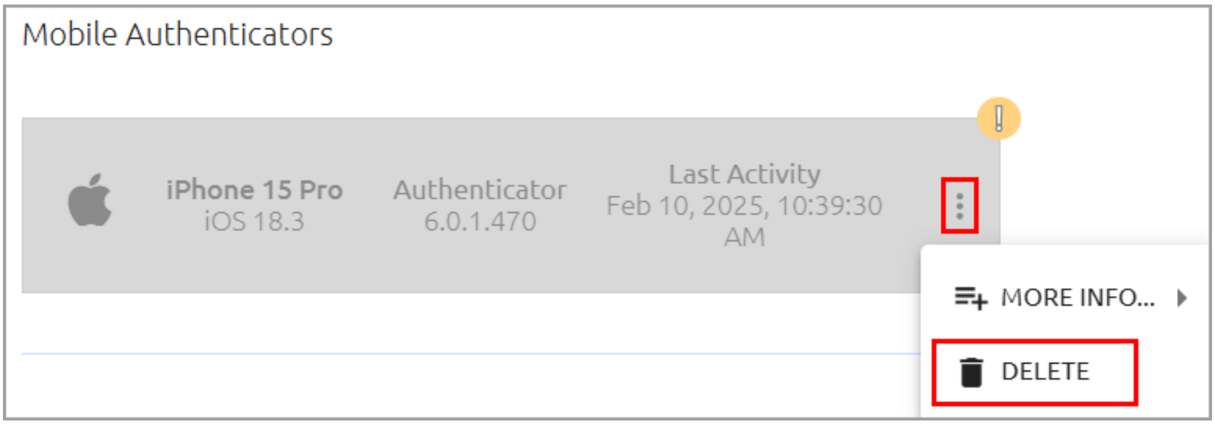
Authenticator 6.0.1.471

Last Activity Feb 9, 2025, 4:17:29 PM

Device ID 98Xba7aUZASk8bfSb8RaeyQX
Provider apple
User Agent Authenticator/6.0.1.471 (iOS 18.2.1; iPhone11_2)
Activity At Feb 9, 2025, 4:17:29 PM

FIDO Authenticators

If the user has deleted the account on the mobile device, the Mobile authenticator is disabled and an alert icon appears in the upper right corner. The authenticator can no longer be used, and it cannot be enabled. To remove the authenticator, click ⋮ and select **Delete**.


Mobile Authenticators

iPhone 15 Pro iOS 18.3

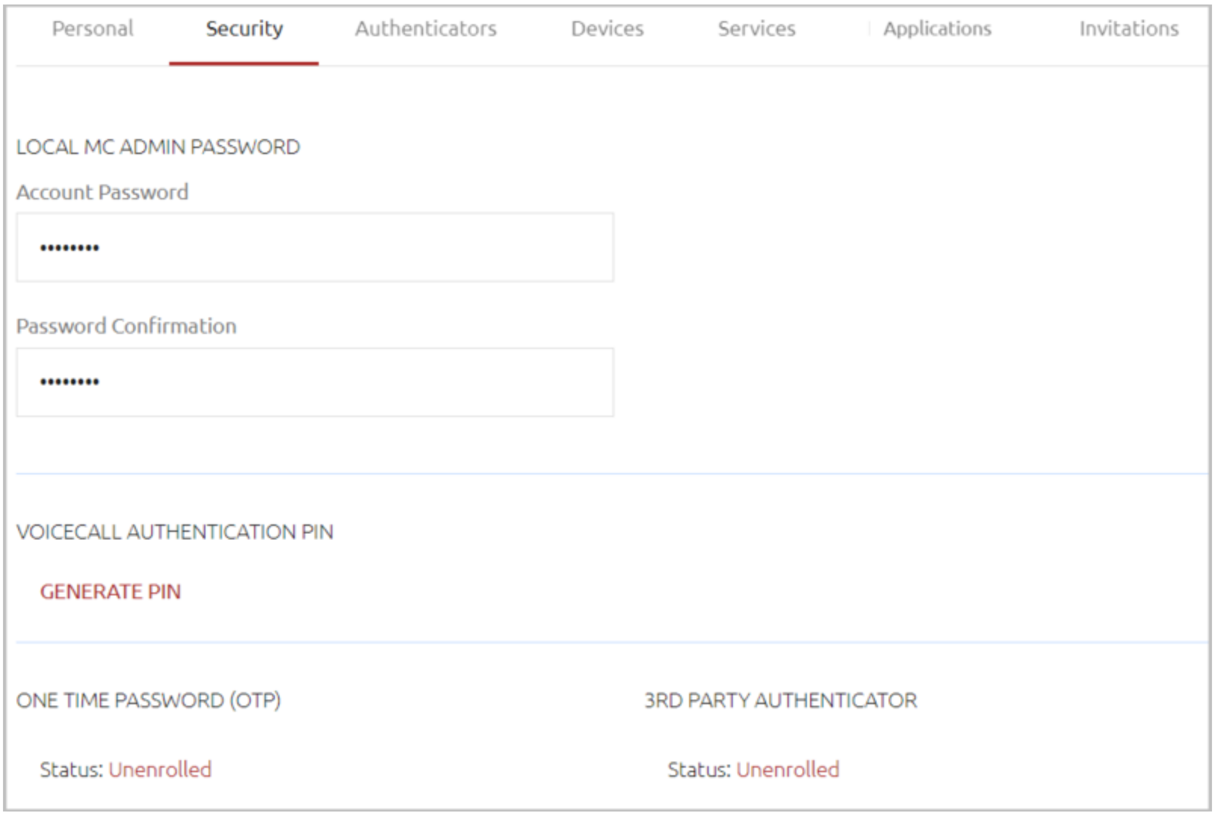
Authenticator 6.0.1.470

Last Activity Feb 10, 2025, 10:39:30 AM

- **Devices:** Lists enrolled workstations on which the user can perform Windows/ MAC authentication and provide details about browsers used for the authentication process. For more information, refer to Managing User Workstations and Browsers.
- **Services:** Displays the services to which the user is assigned. For details, refer to Managing User Services.
- **Applications:** Lists integrated applications to which the user is assigned. For details, refer to Managing User Applications.
- **Invitations:** Lists all active enrollment invitations sent to the user and allows you to manage them. For details, refer to Managing Invitations.
- **Account Sharing:** Allows you to enable account sharing and specify users who are authorized to log into the shared account. For more information, refer to Managing Shared Accounts.

### Setting User Security Parameters

The **Security** tab allows you to perform various password, PIN and other security-related operations. (This tab does not appear for users who are disabled in the Active Directory server.)



LOCAL MC ADMIN PASSWORD

Account Password: ••••••••

Password Confirmation: ••••••••

VOICECALL AUTHENTICATION PIN

ONE TIME PASSWORD (OTP)

Status: Unenrolled

3RD PARTY AUTHENTICATOR

Status: Unenrolled

The following operations are available:

- **Set Local MC Admin Password:** This is the password used for access to the Management Console (MC). The fields in this section are enabled only for Local users who are authorized to access the MC (roles of Admin, Helpdesk or Auditor).

**Important**

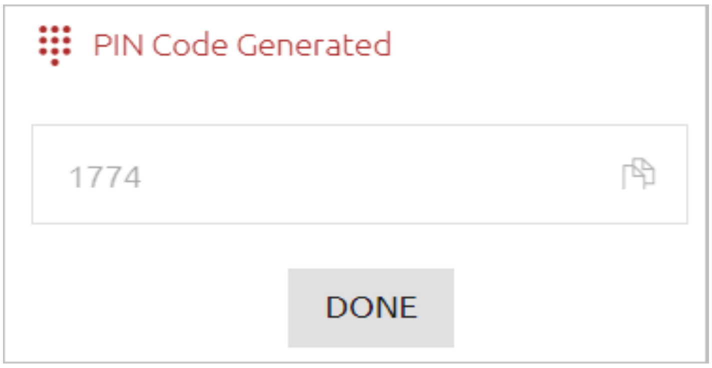
The Local MC Admin Password is used for logging into the MC directly from the browser. When Local users authenticate to the MC via the User Portal, they should use the personal password issued to them for MFA verification.

To set (or update) the password, enter the password in the **Account Password** field. Password requirements are displayed as you type.

Re-enter the password in the **Password Confirmation field**, and then click **Save**.

- **Set Voicecall Authentication PIN:** This operation is useful for users who do not own a smartphone. When these users perform authentication, they receive a voice call that prompts them to enter the PIN code.

  To create a PIN for a user, click **Generate PIN**. The PIN is then displayed in a popup window.



PIN Code Generated

1774

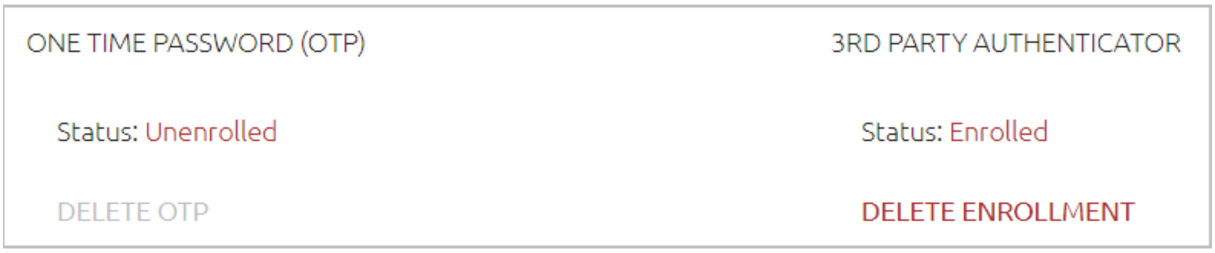
To remove the PIN, in the **PIN Code** section of the **Security** tab, click **Delete PIN**.

**Important**

To use Voicecall Authentication, you need to have a Twilio account. The Twilio service handles the processes of calling the user and managing the verification code.

After you have set up your Twilio account, please send the Account SID, Token, and Phone number to support@doubleoctopus.com and the Support team will complete the integration between Twilio and Enterprise Connect Passwordless.

- **View and manage one-time password (OTP) settings:** The **Status** parameter indicates whether the user is currently enrolled for OTP authentication. If the status is **Enrolled**, you can remove the OTP for the user by clicking **Delete OTP**.



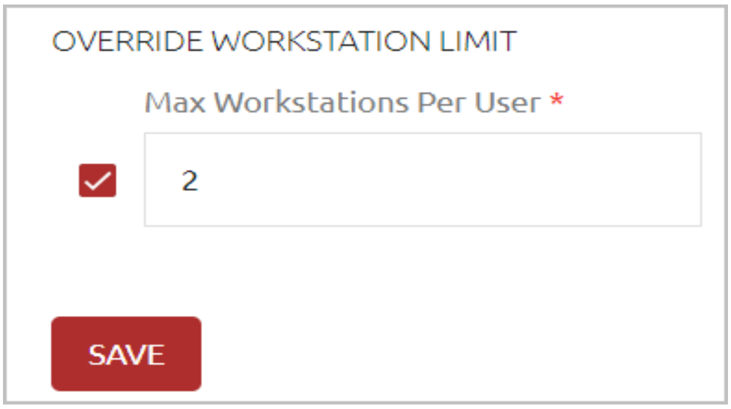
| ONE TIME PASSWORD (OTP) | 3RD PARTY AUTHENTICATOR |
|---|---|
| Status: Unenrolled | Status: Enrolled |
| DELETE OTP | DELETE ENROLLMENT |

- **View and manage 3rd party authenticator settings:** The **Status** parameter indicates whether the user has authenticated using of the defined 3rd party authenticators. (When the user first logs in using one of these authenticators, the status changes from **Unenrolled** to **Active.**) You can changes the status back to

**Unenrolled** by clicking **Delete Enrollment** (e.g., if the user is no longer using that authenticator).

- **Bypass Octopus authentication:** Enables users to authenticate with a username + password or temporary token. For details, refer to Bypassing Authentication.
- **Override Workstation Limit:** This feature enables you to define the number of workstations to which this specific user is allowed to authenticate. The value set here overrides the general value configured for all users (in the **Devices** tab of the **System Settings** menu). The Override feature is useful for accommodating users who need access to large numbers of workstations (e.g., IT personnel).

  To set an override value, select the checkbox and enter the number of workstations allowed in the field to the right. Then, click **Save**.



OVERRIDE WORKSTATION LIMIT

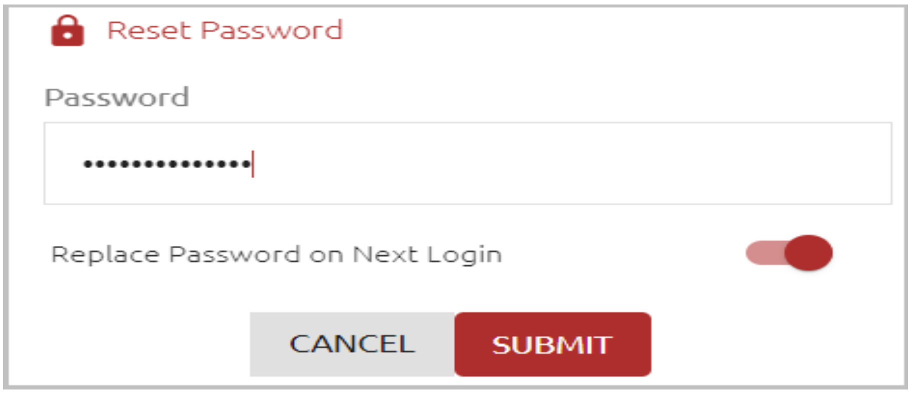
Max Workstations Per User *

☑ 2

The following operations appear in the **Account Password** section:

- **Reset Password:** For users in integrated directories, this option allows you to create a password in the AD for user authentication to Windows/MAC. (The main use case is when a user is temporarily without a mobile device.) The **Reset Password** action will also unlock the user's account (if it had been locked).

  If you enable the **Replace Password on Next Login** toggle when setting the password, the password you create will be a temporary one.



Reset Password

Password

••••••••••••••

Replace Password on Next Login

  For users in the Local directory, **Reset Password** enables you to change the password for user verification in services that utilize multi-factor authentication. The **Replace Password on Next Login** toggle is disabled for Local users.

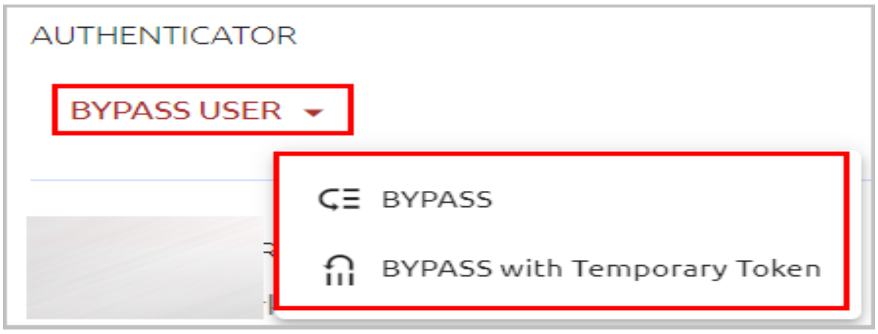
**Note**

Local users can change their own passwords in the User Portal when the **Set Local User Password** option is enabled in Portal Self Service settings.

- **Force Password Change:** Replaces the password with a new one upon the next user login. (This operation is disabled for Local users.)
- **Refresh User Profile:** Restores user details (in the **Personal** tab) to those currently recorded in the AD. (This operation is disabled for Local users.)

### Bypassing Authentication

When the **Bypass User** feature is activated, users authenticate with a username + password or temporary token. The Bypass action is useful for workers who have forgotten their phones, for handling machine-to-machine authentication, and more.

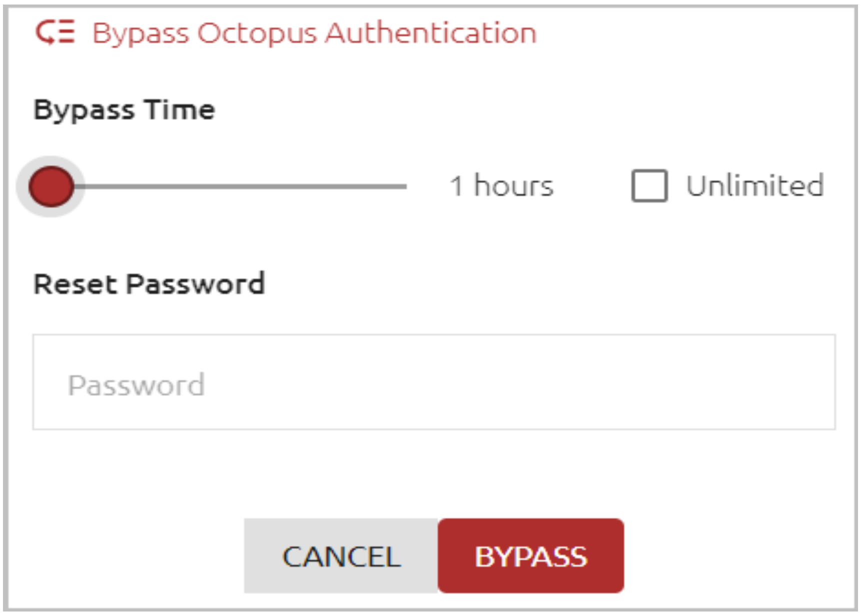


The **BYPASS** option enables you to set a specific or unlimited amount of time for the bypass period. During the bypass period, the user may authenticate with username and password.

**To set a Bypass Authentication time period:**

1. At the bottom of the **Security** tab for the relevant user, in the **Authenticator** section, select **Bypass User > BYPASS.**

   Bypass parameters are displayed in a popup window.

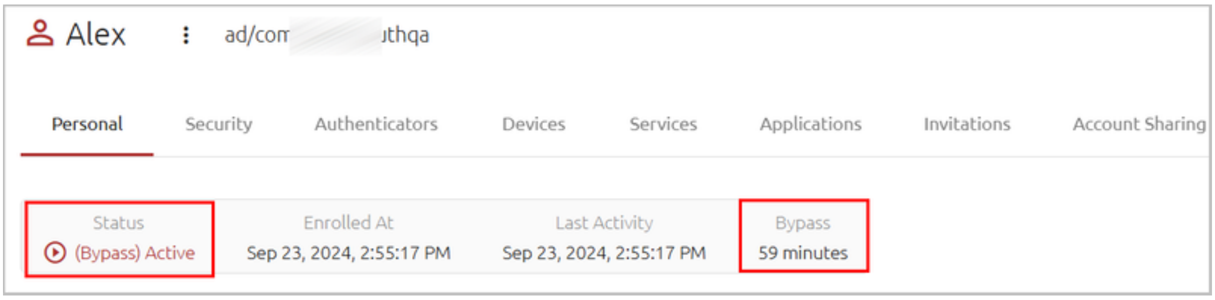


2. Drag the slider until the desired period for the bypass is displayed. (The range is 1 hour- 14 days.) Alternatively, click the **Unlimited** checkbox (recommended for machine-to-machine authentication).

3. If the user is not aware of the current password, in the **Reset Password** field, enter a new password with which the user can authenticate.

4. Click **Bypass.**

   The popup closes. At the top of the **Personal** tab, the Bypass state is indicated in the user's information bar, and the time remaining until the bypass expires is displayed.



| Status | Enrolled At | Last Activity | Bypass |
|---|---|---|---|
| (Bypass) Active | Sep 23, 2024, 2:55:17 PM | Sep 23, 2024, 2:55:17 PM | 59 minutes |

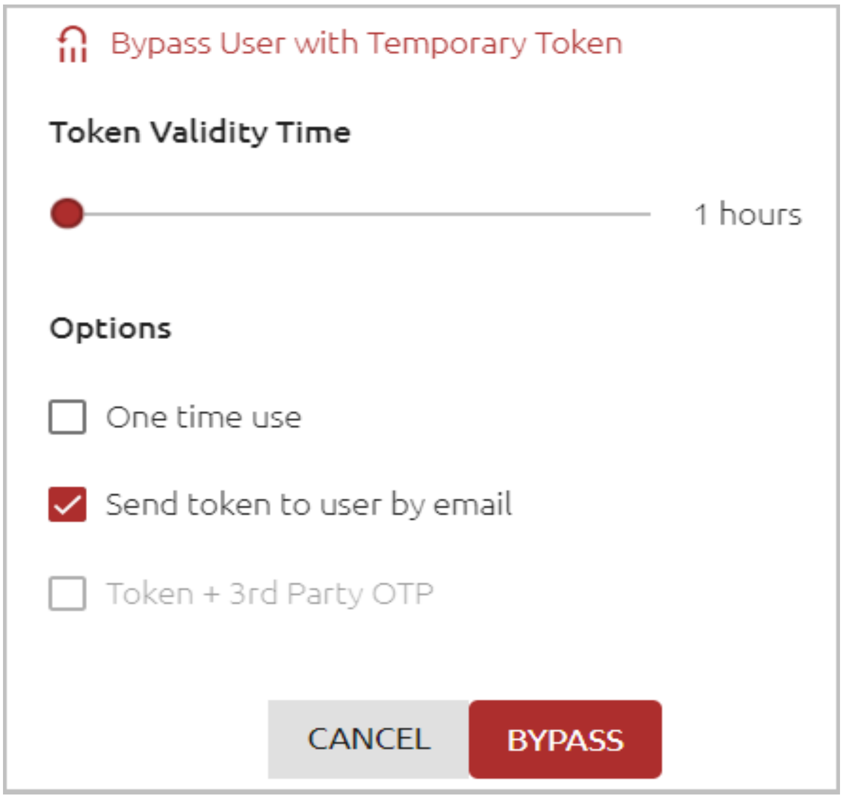
5. To cancel the bypass before the expiration time, at the bottom of the **Security** tab, click **End Bypass.**

The Bypass with Temporary Token option allows you to set a specific period of time for which the token is valid. Token requirements, such as number of characters, are set per directory in the Policy tab of the directory settings.

**To set user bypass with a temporary token:**

1. At the bottom of the **Security** tab for the relevant user, in the **Authenticator** section, select **Bypass User > Bypass with Temporary Token.**

   Bypass parameters are displayed in a popup window.



Bypass User with Temporary Token

Token Validity Time

1 hours

Options

☐ One time use

☑ Send token to user by email

☐ Token + 3rd Party OTP

2. Drag the slider until the desired token validity time is displayed. (The range is 1 hour to 14 days.)

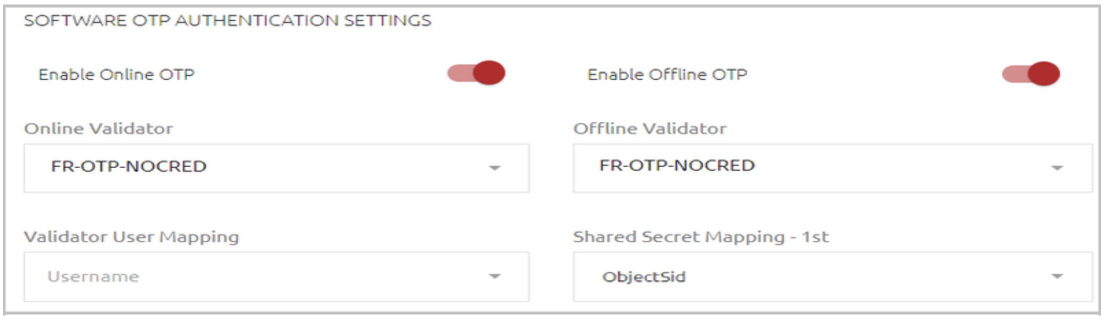
3. Select the following checkboxes as required:

   - **One time use:** When selected, the token may be used for a single time only during the entire validity period. Once the token is used, the bypass ends. This feature is useful for a one-time access, e.g., by IT personnel.

   - **Send token to user by email:** When selected, the user receives the token to the email address displayed in the **Personal** tab of the user details, and the admin is not able to view the token. If the checkbox is NOT selected, the token is copied to the clipboard and the admin needs to forward it to the user.

   - **Token + 3rd Party OTP:** When selected, the user is able to log into Windows and the User Portal with a temporary token + ForgeRock TOTP. For successful authentication, the user needs to enter the token (in the **Passwor**d field) *immediately followed* by the OTP (without spaces or other breaks).

     In order to use this option, a ForgeRock OTP Validator needs to be created (**System Settings > Authenticators**) and assigned as an OTP Validator in the **Authenticators** tab of the directory settings.



SOFTWARE OTP AUTHENTICATION SETTINGS

Enable Online OTP ●

Enable Offline OTP ●

Online Validator: FR-OTP-NOCRED

Offline Validator: FR-OTP-NOCRED

Validator User Mapping: Username

Shared Secret Mapping - 1st: ObjectSid

4. Click **Bypass.**

   The popup closes. At the top of the **Personal** tab, the Bypass state is indicated in the user's information bar, and the time remaining until the bypass expires is displayed.

5. To cancel the bypass before the expiration time, at the bottom of the **Security** tab, click **End Bypass.**

**Important**

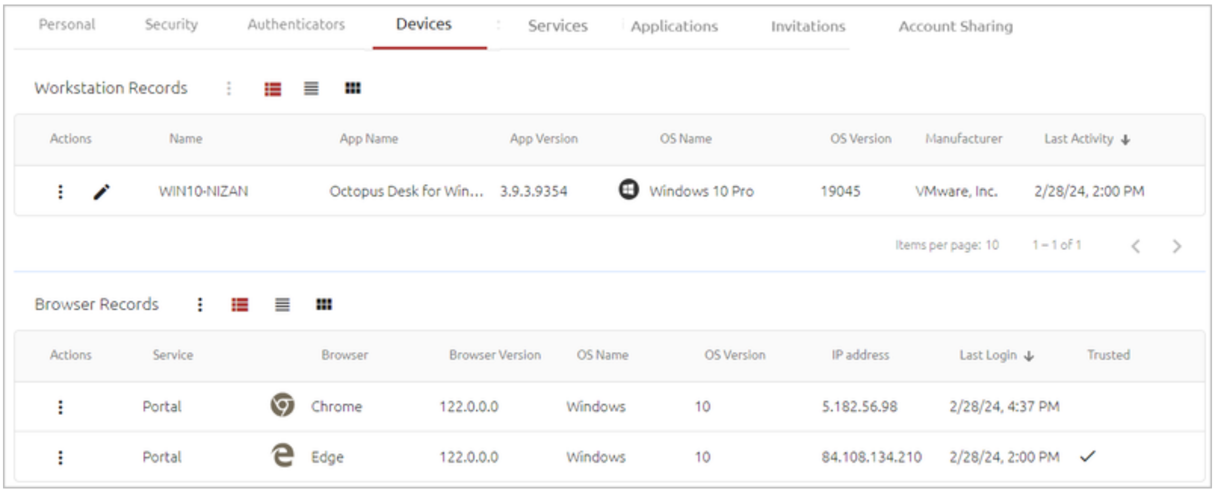
After starting or ending a bypass, publish your changes to the database.

### Managing User Workstations and Browsers

The **Devices** tab lists all devices through which the user has performed authentication. The tab has separate displays for workstation records and browser records.

**Note**

This tab does not appear for users who are disabled in the Active Directory server.



Workstation Records

| Actions | Name | App Name | App Version | OS Name | OS Version | Manufacturer | Last Activity ↓ |
|---|---|---|---|---|---|---|---|
| ⋮ ✎ | WIN10-NIZAN | Octopus Desk for Win... | 3.9.3.9354 | Windows 10 Pro | 19045 | VMware, Inc. | 2/28/24, 2:00 PM |

Items per page: 10   1 – 1 of 1

Browser Records

| Actions | Service | Browser | Browser Version | OS Name | OS Version | IP address | Last Login ↓ | Trusted |
|---|---|---|---|---|---|---|---|---|
| ⋮ | Portal | Chrome | 122.0.0.0 | Windows | 10 | 5.182.56.98 | 2/28/24, 4:37 PM | |
| ⋮ | Portal | Edge | 122.0.0.0 | Windows | 10 | 84.108.134.210 | 2/28/24, 2:00 PM | ✓ |

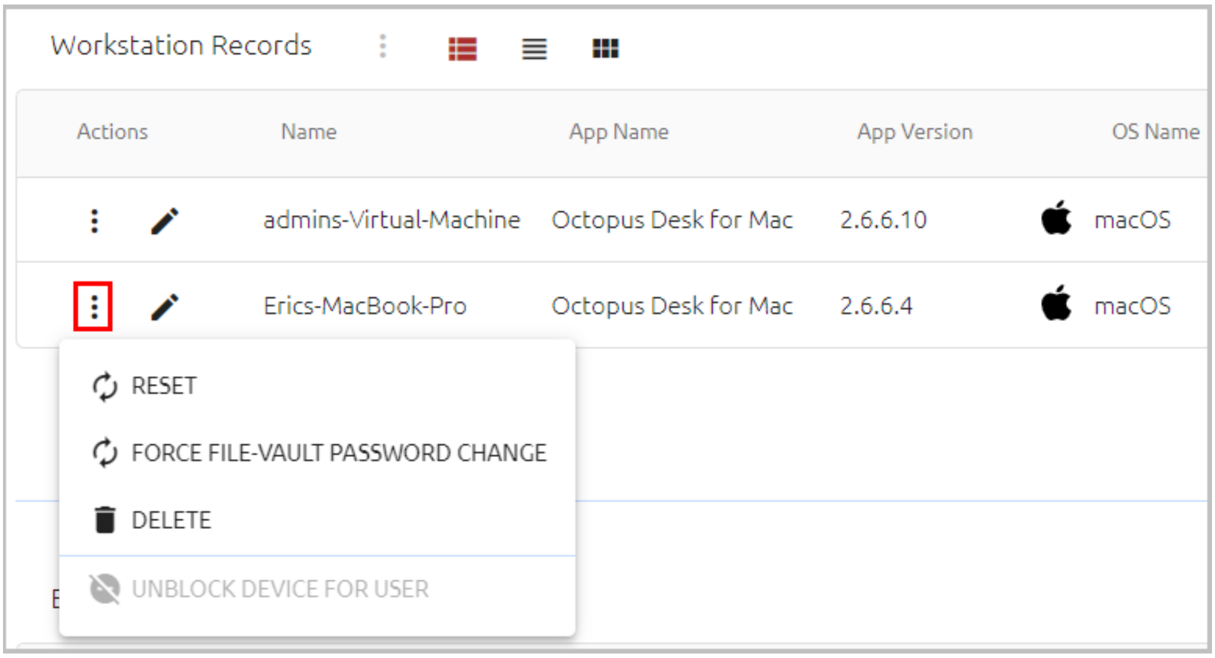
The **Workstation Records** display lists all enrolled workstations on which the user can perform Windows/MAC authentication. Basic information about each workstation, such as OS type, manufacturer, and Octopus application version is provided.

Clicking ✎ redirects you to another page where you can view more details about the workstation.

Clicking ⋮ opens an actions menu for the selected workstation. The actions are:

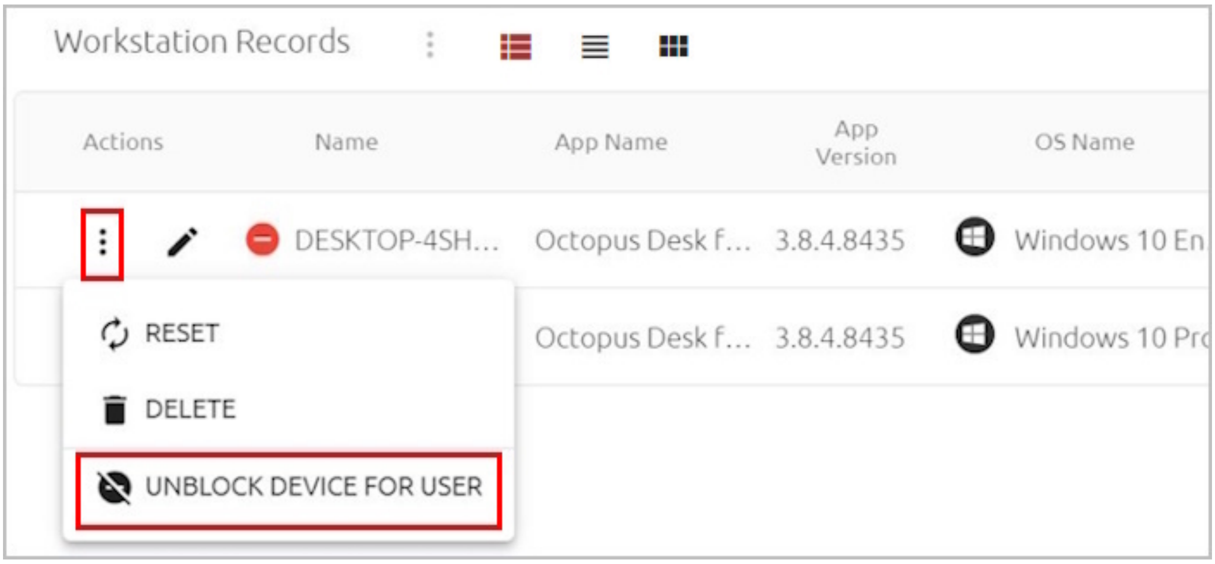
- **Reset:** Deletes the workstation's history and all generated security keys. Use the **Reset** action after upgrading the workstation to Windows Agent 3.3 or Mac Agent 2.3.0. Following a reset, the workstation will generate a new security key with the next authentication.
- **Force FileVault Password Change (Mac workstations only)** : Initiates an immediate rotation of the FileVault password. If the **Password Age** setting is set to 0 (**System Settings > Devices > macOS FileVault Password Settings**), the operation is disabled.
- **Delete:** Deletes the workstation's history and security keys and also removes it from the list of workstations. Keep in mind that deleting a workstation removes it for *all* users.

  The **Delete** action is generally reserved for workstations that are no longer in use. If a user authenticates on a deleted workstation, the workstation will be recreated and will appear in the list again.



| Actions | Name | App Name | App Version | OS Name |
|---|---|---|---|---|
| ⋮ ✎ | admins-Virtual-Machine | Octopus Desk for Mac | 2.6.6.10 | macOS |
| ⋮ ✎ | Erics-MacBook-Pro | Octopus Desk for Mac | 2.6.6.4 | macOS |

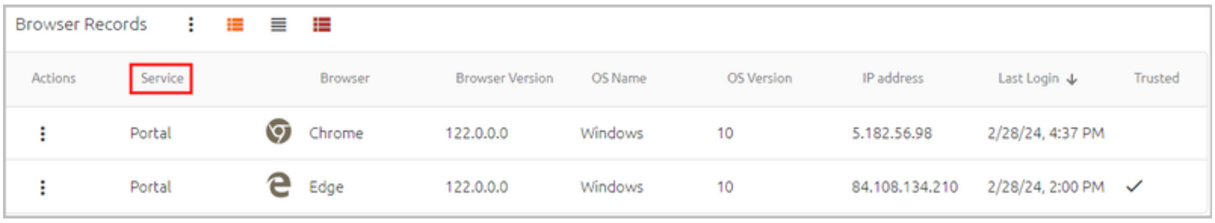
If the user is currently blocked from accessing a workstation due to enforcement of push fatigue protection mechanisms, the ⛔ icon appears in the row of the relevant workstation. To remove the block, click ⋮ and select **Unblock Device For User**.



Workstation Records

| Actions | Name | App Name | App Version | OS Name |
|---|---|---|---|---|
| ⋮ | DESKTOP-4SH… | Octopus Desk f… | 3.8.4.8435 | Windows 10 En |
|  |  | Octopus Desk f… | 3.8.4.8435 | Windows 10 Pr |

The **Browser Records** display lists all browsers through which the user has authenticated to SAML services or the User Portal. The browser version, basic workstation details and last login information are provided. In List view, the **Service** column lists the service to which the user authenticated (User Portal or name of SAML service). A ✓ icon in the **Trusted** column indicates that when Adaptive Authentication is enabled, strong authentication is not required after the first authentication through that browser.

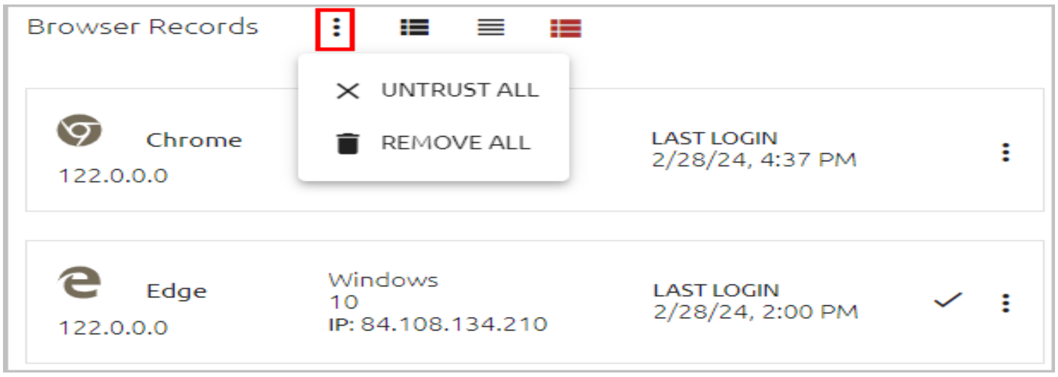


Browser Records

| Actions | Service | Browser | Browser Version | OS Name | OS Version | IP address | Last Login ↓ | Trusted |
|---|---|---|---|---|---|---|---|---|
| ⋮ | Portal | Chrome | 122.0.0.0 | Windows | 10 | 5.182.56.98 | 2/28/24, 4:37 PM |  |
| ⋮ | Portal | Edge | 122.0.0.0 | Windows | 10 | 84.108.134.210 | 2/28/24, 2:00 PM | ✓ |

Clicking ⋮ at the top of the display enables you to perform some bulk operations for managing the browsers. These actions are relevant when Adaptive Authentication is enabled:

- **Untrust All:** Removes the Trusted status of all browsers currently marked as Trusted. (When users authenticate on untrusted browsers, they need to enter a verification code on every authentication.)
- **Remove All:** Clears the browser list and removes the listed browsers from the system. When users next attempt Adaptive Authentication through these browsers, they will be treated as unrecognized devices.



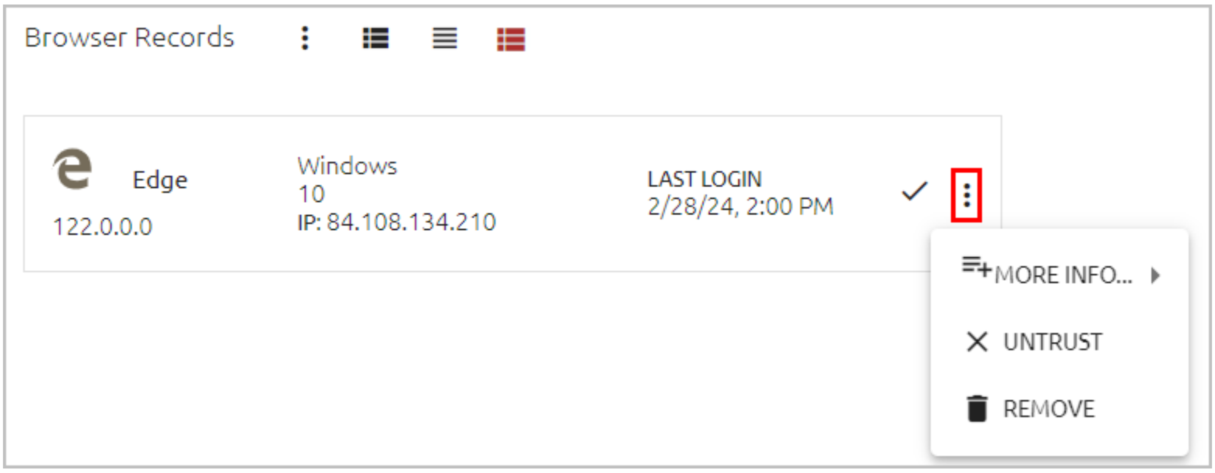
Browser Records

Chrome
122.0.0.0
LAST LOGIN
2/28/24, 4:37 PM

Edge
122.0.0.0
Windows
10
IP: 84.108.134.210
LAST LOGIN
2/28/24, 2:00 PM

Clicking ⋮ in the row or tile of a browser opens an actions menu for that browser. The actions are:

- **More Info:** Displays additional data (such as engine details, CPU architecture and more) in a popup window.
- **Untrust:** Removes the browser's Trusted status (relevant when Adaptive Authentication is enabled).
- **Remove:** Clears the browser from the list and removes it from the system, giving it the status of an unrecognized device (relevant when Adaptive Authentication is enabled).



Browser Records

Edge
122.0.0.0
Windows
10
IP: 84.108.134.210
LAST LOGIN
2/28/24, 2:00 PM

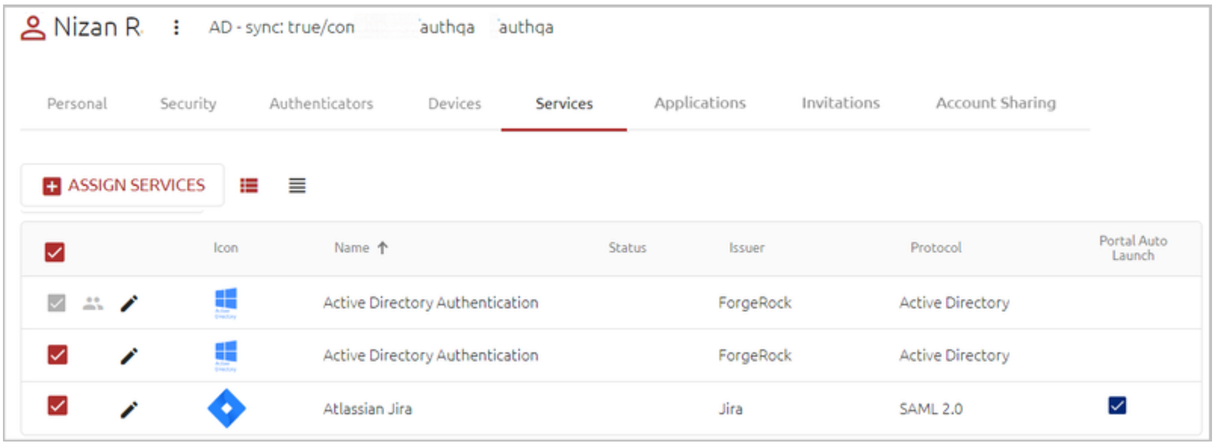
### Managing User Services

This tab lists all services to which the user is assigned. (The tab does not appear for users who are disabled in the Active Directory server.)

Clicking ✎ in the row of a service redirects you to another page where you can update the service settings.

The checkboxes on the left side of each row are toggles that allow you to control whether that service is currently enabled for the user. If the user is part of a Group, services assigned to the Group are automatically assigned to the user, and cannot be enabled / disabled for an individual user. (These services are indicated by a Group icon and disabled Assign checkboxes.) However, in order to enable management of a Group-assigned service for individual members, these services can also be assigned to specific users within the Group, as necessary.

In the example below, the ADPA service is assigned to both a Group to which the user belongs (non-editable settings), and directly to the user (editable settings).



Nizan R ⋮ AD - sync: true/con authqa authqa

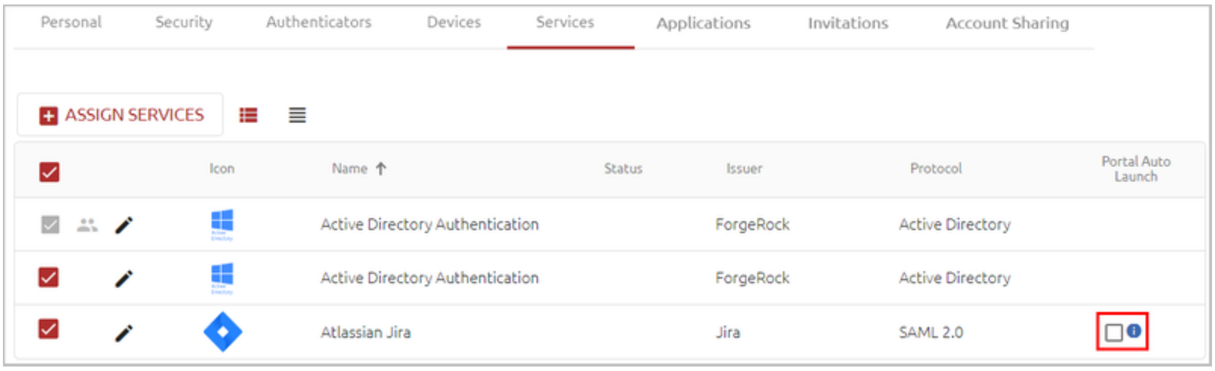
Personal | Security | Authenticators | Devices | **Services** | Applications | Invitations | Account Sharing

ASSIGN SERVICES

| ☑ | | Icon | Name ↑ | Status | Issuer | Protocol | Portal Auto Launch |
|---|---|---|---|---|---|---|---|
| ☑ | ✎ | | Active Directory Authentication | | ForgeRock | Active Directory | |
| ☑ | ✎ | | Active Directory Authentication | | ForgeRock | Active Directory | |
| ☑ | ✎ | | Atlassian Jira | | Jira | SAML 2.0 | ☑ |

The **Portal Auto Launch** column, which is relevant only to SAML services, indicates whether the Auto Launch feature for that service is currently enabled for the user. (When the feature is enabled, the service opens automatically upon login to the User Portal.) You can enable or disable Automatic Launch for a user regardless of whether the **Automatic Launch** toggle is selected for the SAML service (in the **Sign on** tab of the service settings).

If the Auto Launch setting for a user differs from that specified in the service settings, the exception is indicated by an Information icon in the column. In the example below, Auto Launch is disabled for this user, even though it is enabled for the Group and for the SAML service.



Personal | Security | Authenticators | Devices | **Services** | Applications | Invitations | Account Sharing

ASSIGN SERVICES

| ☑ | | Icon | Name ↑ | Status | Issuer | Protocol | Portal Auto Launch |
|---|---|---|---|---|---|---|---|
| ☑ | ✎ | | Active Directory Authentication | | ForgeRock | Active Directory | |
| ☑ | ✎ | | Active Directory Authentication | | ForgeRock | Active Directory | |
| ☑ | ✎ | | Atlassian Jira | | Jira | SAML 2.0 | □ ⓘ |

**Note**

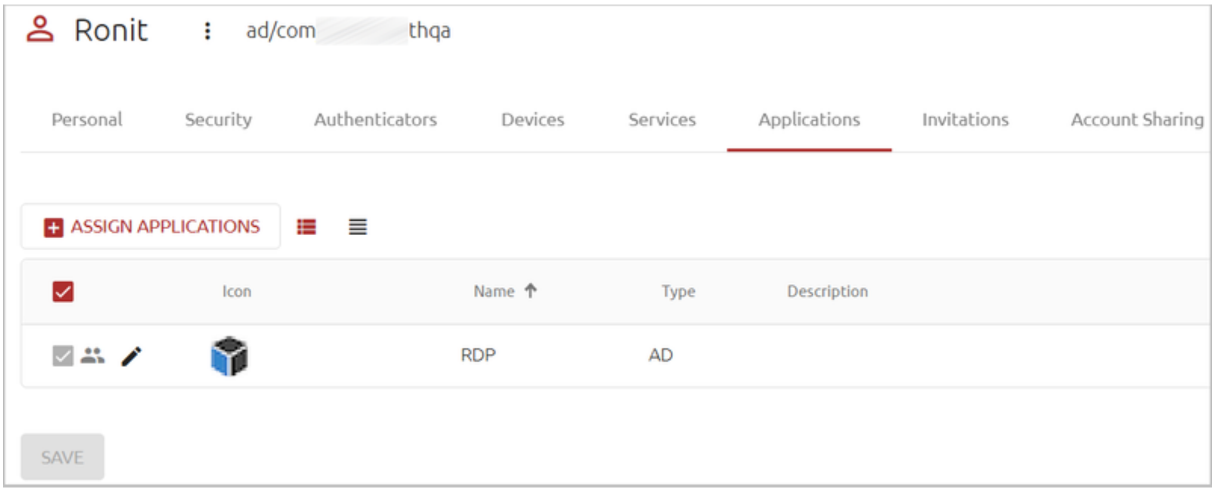
To configure Automatic Launch, **SSO** must be enabled in the SAML service settings. If SSO is not selected in the service settings, the **Portal Auto Launch** checkbox is disabled.

To assign additional services to the user, click **Assign Services**. In the dialog that opens, specify the services to add by selecting the relevant checkboxes, and then click **Save**.

The services listed in the **Assign Services** dialog are ones to which the user is *not* currently assigned AND which may be used by directories to which the user belongs. If a service is not listed in the dialog, open the settings of the service and verify that the appropriate directory is selected. For more information, refer to Assigning Directories and Users to a Service.

**Managing User Applications**

This tab lists integrated applications that the user is currently authorized to work with. The checkboxes on the left are toggles that allow you to control whether that application is enabled for the user. Clicking ✏ in the row of an application redirects you to another page where you can view and update settings for the application.



| ☑ | Icon | Name ↑ | Type | Description |
|---|---|---|---|---|
| ☑ ✏ |  | RDP | AD |  |

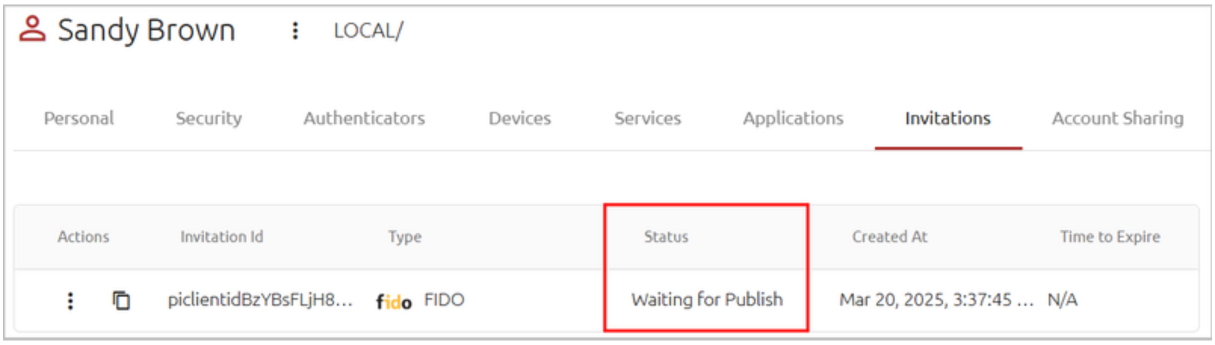
To assign applications to the user, click **Assign Applications**. In the dialog that opens, specify the applications to add by selecting the relevant checkboxes, and then click **Save**.

The applications listed in the **Assign Applications** dialog are ones to which the user is *not* currently assigned AND which may be used by directories to which the user belongs. If an application is not listed in the dialog, open the settings of the application and verify that the appropriate directory is selected. For details, refer to Assigning Directories and Users to Applications.

**Managing User Invitations**

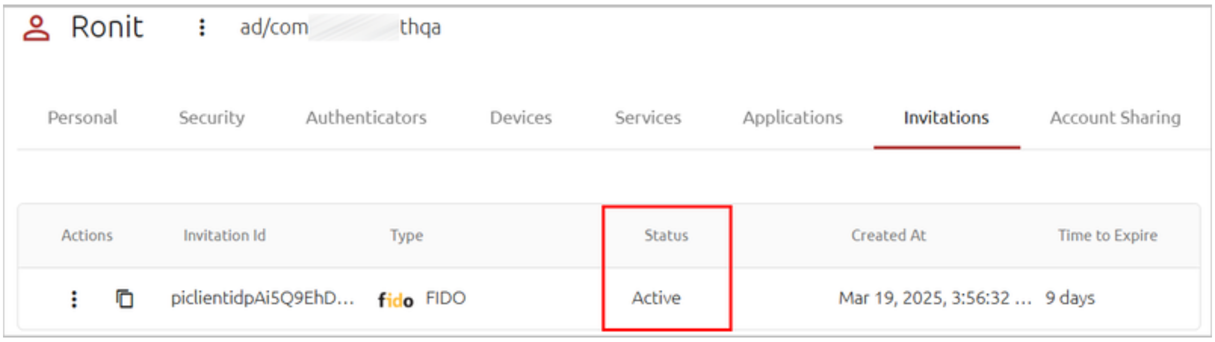
The **Invitations** tab lists all enrollment invitations sent to the user and details about each one, including its unique identifier, invitation type and time until expiration. The **Status** column shows the handling workflow for the invitation. This workflow is determined by whether the user is already published in the system or is new. Possible statuses are:

- **Waiting for Publish:** The user has not yet been synced and published in the system. The invitation is being stored as a pending invitation and will be sent to the user as soon as the next Publish process completes successfully.



| Actions | Invitation Id | Type | Status | Created At | Time to Expire |
|---|---|---|---|---|---|
| ⋮ ⧉ | piclientidBzYBsFLjH8... | fido FIDO | Waiting for Publish | Mar 20, 2025, 3:37:45 ... | N/A |

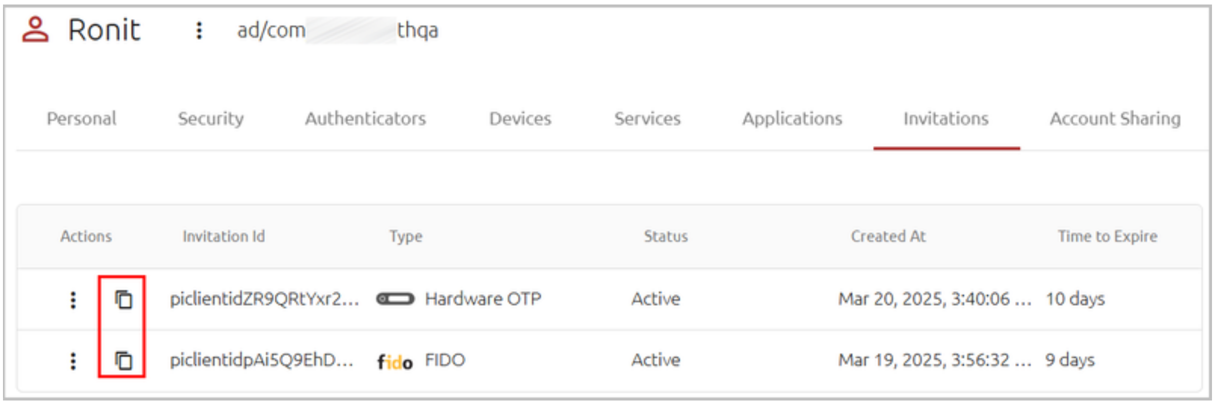
- **Active:** The user is published in the system and the invitation has been sent.



| Actions | Invitation Id | Type | Status | Created At | Time to Expire |
|---|---|---|---|---|---|
| ⋮ ⧉ | piclientidpAi5Q9EhD... | fido FIDO | Active | Mar 19, 2025, 3:56:32 ... | 9 days |

Clicking ⧉ copies the invitation's enrollment link or code, according to invitation type:

- **Octopus type invitations:** The Copy action copies the Invitation ID, which is then converted to the manual enrollment code provided in the invitation.
- **FIDO / OTP type invitations:** The Copy action copies the link for registration provided in the invitation.

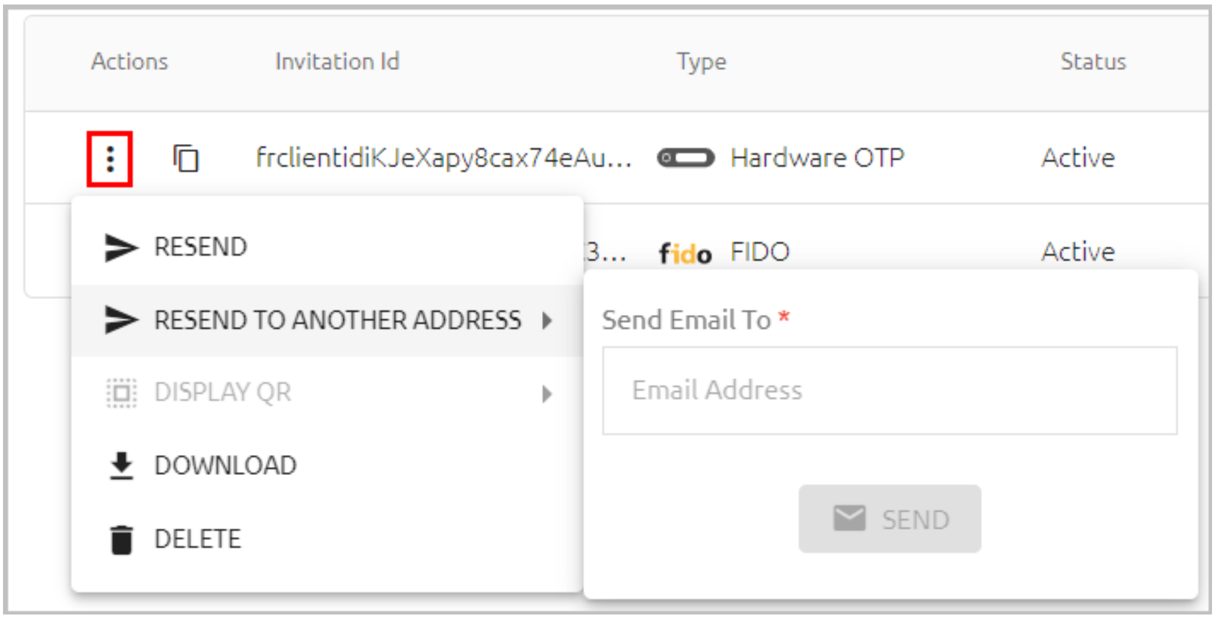


| Actions | Invitation Id | Type | Status | Created At | Time to Expire |
|---|---|---|---|---|---|
| ⋮ ⧉ | piclientidZR9QRtYxr2... | Hardware OTP | Active | Mar 20, 2025, 3:40:06 ... | 10 days |
| ⋮ ⧉ | piclientidpAi5Q9EhD... | fido FIDO | Active | Mar 19, 2025, 3:56:32 ... | 9 days |

Clicking ⋮ opens an actions menu for the selected invitation. The actions are:

- **Resend:** Sends the invitation to the email address recorded in the system for the user (in the **Personal** tab of the user details).
- **Resend To Another Address:** Sends the invitation to an email address other than the one recorded in the system. When selecting this option, enter the address in the field that opens, and then click **Send**.

- **Display QR:** Shows the enrollment QR provided with the invitation. This action is relevant for Octopus type invitations only.
- **Download:** Saves the invitation as an email file and downloads it to your machine.
- **Delete:** Removes the invitation from the system.



| Actions | Invitation Id | Type | Status |
|---|---|---|---|
| ⋮ | frclientidiKJeXapy8cax74eAu… | Hardware OTP | Active |
| | 3… | FIDO | Active |

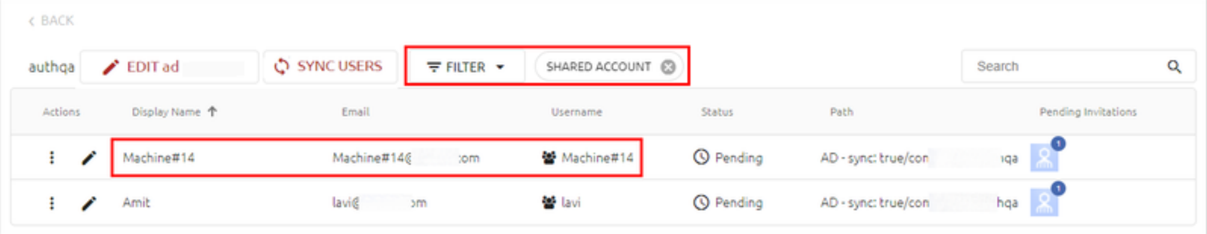
**Note**

The Resend and Download actions are not available for invitations with a **Waiting for Publish** status.

### Managing Shared Accounts

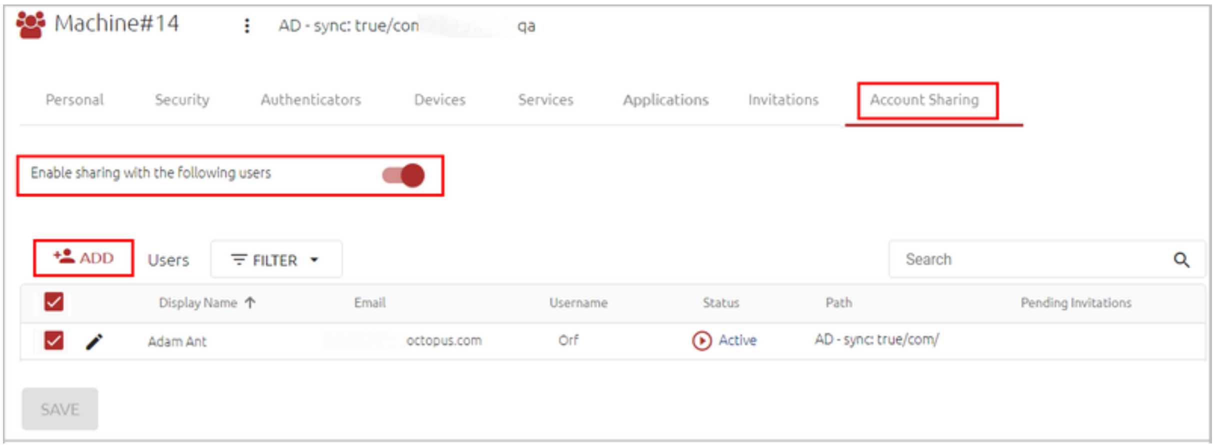
The Shared Account feature enables designated users to log into a generic account on a shared workstation using their personal credentials and devices. Account sharing is particularly useful for specific groups of personnel (such as IT, DevOps, manufacturing floor workers, etc.) who use a shared workstation.

Shared accounts are easily identified on the Users list by a special icon. Alternatively, you can filter the entire list for shared accounts. In addition, we recommend naming the account according to the specific shared use case, e.g., Machine 3, Floor 4, etc.



| Actions | Display Name | Email | Username | Status | Path | Pending Invitations |
|---|---|---|---|---|---|---|
| ⋮ | Machine#14 | Machine#14@[redacted]:om | Machine#14 | Pending | AD - sync: true/con[redacted]ıqa | 1 |
| ⋮ | Amit | lavi@[redacted]ɔm | lavi | Pending | AD - sync: true/con[redacted]hqa | 1 |

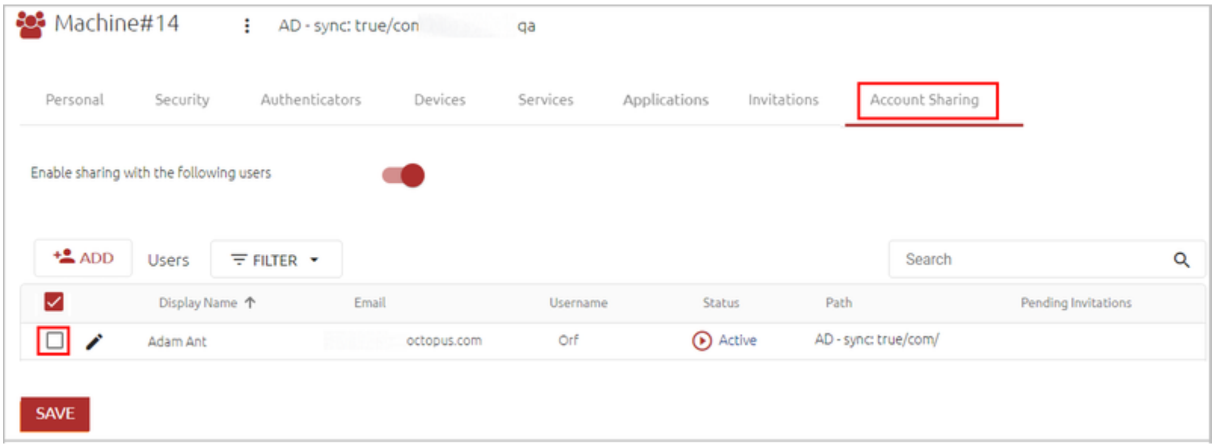
To manage a shared account, click ✎ to open the user details and select the **Account Sharing** tab. The **Enable sharing** toggle button activates and disables account sharing. To allow users to log into the shared account, click **Add** and select the relevant user(s) from the dialog that opens.



Enable sharing with the following users ●

| ☑ | Display Name ↑ | Email | Username | Status | Path | Pending Invitations |
|---|---|---|---|---|---|---|
| ☑ | Adam Ant | [redacted]octopus.com | Orf | Active | AD - sync: true/com/ | |

Once users are added, you can temporarily block their access to the account when required, by clearing the checkbox in the row of the relevant user(s).

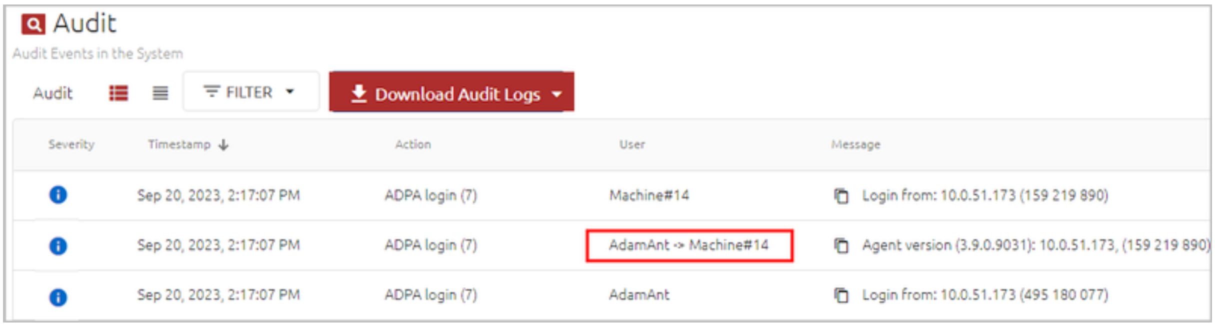


Enable sharing with the following users ●

| ☑ | Display Name ↑ | Email | Username | Status | Path | Pending Invitations |
|---|---|---|---|---|---|---|
| □ | Adam Ant | [redacted]octopus.com | Orf | Active | AD - sync: true/com/ | |

You can also temporarily disable account sharing when necessary by deselecting the **Enable sharing** toggle. The list of approved users will remain intact while sharing is disabled, so you can quickly and easily reactivate account sharing with those users.

In the **Auditing** menu, two users are recorded for the event of login to a shared account - the user who performed the login, and the shared account user. For example:



| Severity | Timestamp ↓ | Action | User | Message |
|---|---|---|---|---|
| ● | Sep 20, 2023, 2:17:07 PM | ADPA login (7) | Machine#14 | Login from: 10.0.51.173 (159 219 890) |
| ● | Sep 20, 2023, 2:17:07 PM | ADPA login (7) | AdamAnt -> Machine#14 | Agent version (3.9.0.9031): 10.0.51.173, (159 219 890) |
| ● | Sep 20, 2023, 2:17:07 PM | ADPA login (7) | AdamAnt | Login from: 10.0.51.173 (495 180 077) |

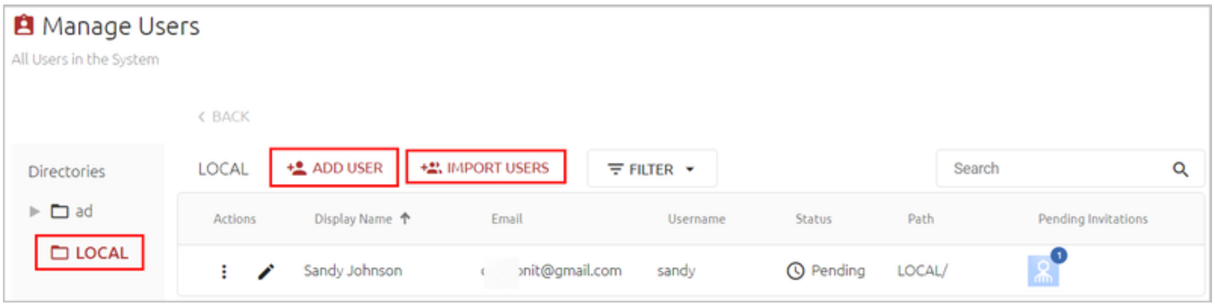
**Important**

The Shared Account feature requires integration with the Windows Agent (version 3.9 or higher) and configuration of some settings in the Windows MSIUpdater client. For details, refer to the Octopus Desk for Windows Installation Guide.

## Adding Users to the Local Directory

The Local directory is a default, internal directory that cannot be deleted. It is useful for organizations that do not manage users through external directories.

You can add users to the Local directory by either creating them manually (by clicking **Add User**), or by uploading them from a CSV file (by clicking **Import Users**).



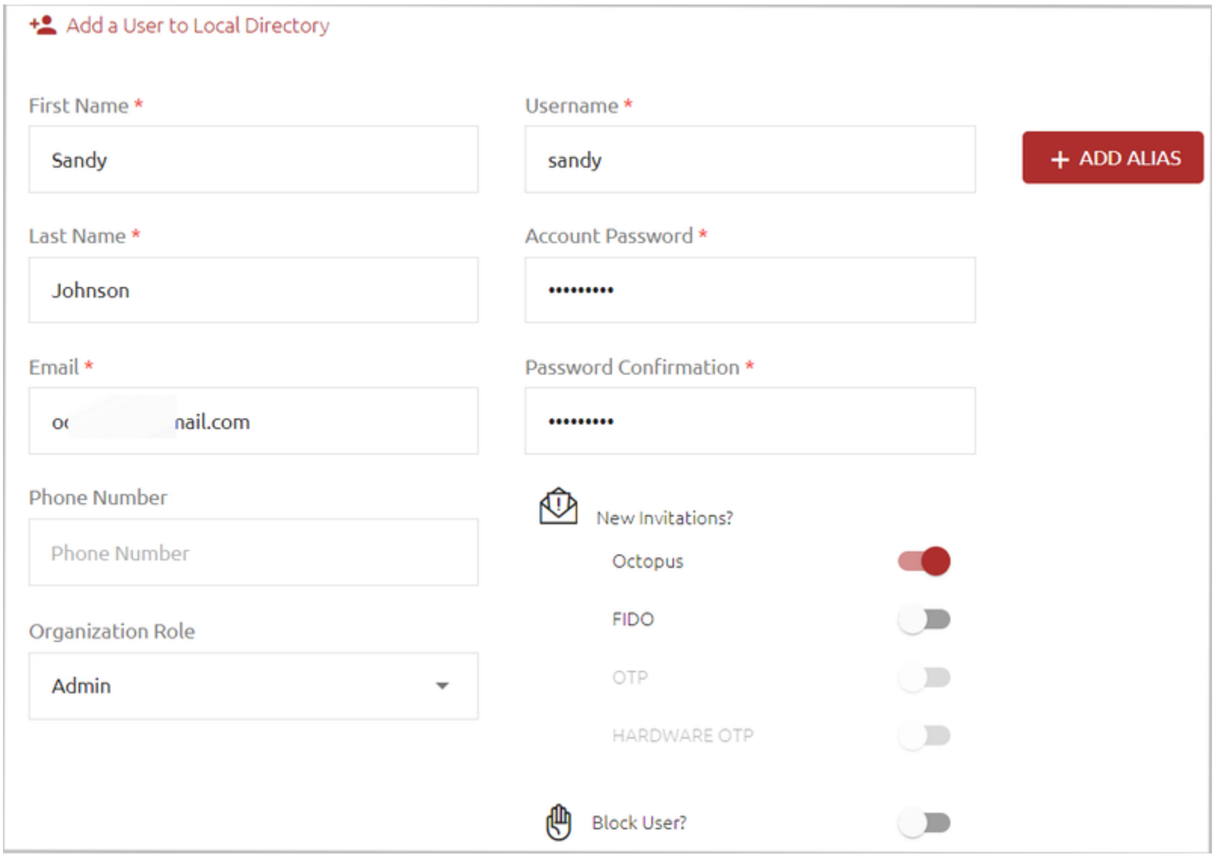
| Actions | Display Name | Email | Username | Status | Path | Pending Invitations |
|---|---|---|---|---|---|---|
| ⋮ ✎ | Sandy Johnson | [redacted]nit@gmail.com | sandy | Pending | LOCAL/ | 1 |

### Adding Local Users Manually

The **Add User** button enables you to create a new Local user.

**To add a Local user manually:**

1. From the **Manage Users** menu, select the **LOCAL** directory from the **Directories** list. Then, click **Add User**.
2. In the dialog that opens, enter the user's first name, last name, email and username in the appropriate fields. If desired, enter the user's mobile number in the **Phone Number** field (this setting is not required).



Add a User to Local Directory

First Name * Sandy

Username * sandy

+ ADD ALIAS

Last Name * Johnson

Account Password * •••••••••

Email * oc[redacted]nail.com

Password Confirmation * •••••••••

Phone Number: Phone Number

Organization Role: Admin

New Invitations?

Octopus ●

FIDO ○

OTP ○

HARDWARE OTP ○

Block User? ○

3. By default, a role of **User** is assigned. To assign a different role, open the **Role in the Organization** list and select one of the following options:

   - **Auditor:** Has read-only permissions in the Management Console.

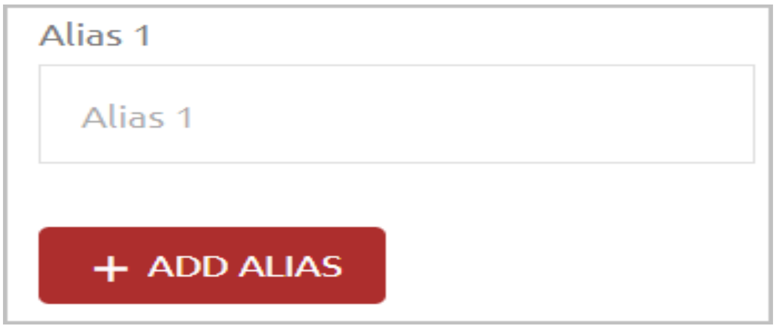
   - **Helpdesk:** Has authorization to update user-related settings, such as setting passwords, generation PIN codes, bypassing Octopus Authentication, etc. All other Management Console settings are read-only.

   - **Admin:** Has authorization to view and update all settings in the Management Console.

4. Set an **Account Password** for the user, and re-enter it in the **Password Confirmation** field.

   The password must contain 8-32 characters and include at least one uppercase letter, one lowercase letter, one number and one special character.

5. If you would like to add other details for the user (e.g., an additional email address), click **Add Alias** and enter the relevant detail in the field. You may add up to 20 **Alias** fields.



Alias 1

Alias 1

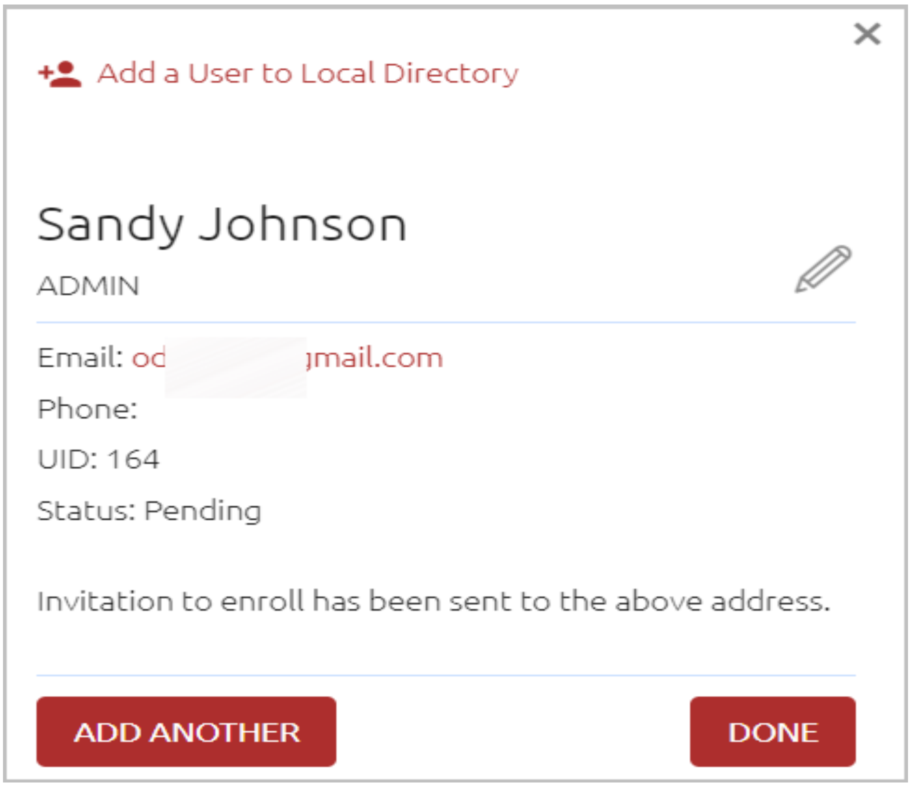
6. Review the following settings:

   - **Send Invitations**: By default, an enrollment email for the Octopus Authenticator is sent, prompting the new user to activate the account. To send invitations for additional authentication types, enable the relevant toggle buttons. If you do not want invitations to be sent, make sure the relevant toggle buttons are disabled. If you block the user (see below), the invitation buttons are automatically disabled.

   - **Block User** : By default, when new users activate an account they will be able to authenticate immediately. To block this behavior, click the toggle button to enable the Block feature.

7. At the bottom of the page, click **Save**.

   The user is added, and a summary of user details is displayed.



Add a User to Local Directory

Sandy Johnson

ADMIN

Email: od[redacted]jmail.com

Phone:

UID: 164

Status: Pending

Invitation to enroll has been sent to the above address.

8. To change user details or perform other actions on the user, click ✎. For more information, refer to [Performing Actions on Users](#).

To create another user, click **Add Another**. To close the dialog and return to the Users list, click **Done**.

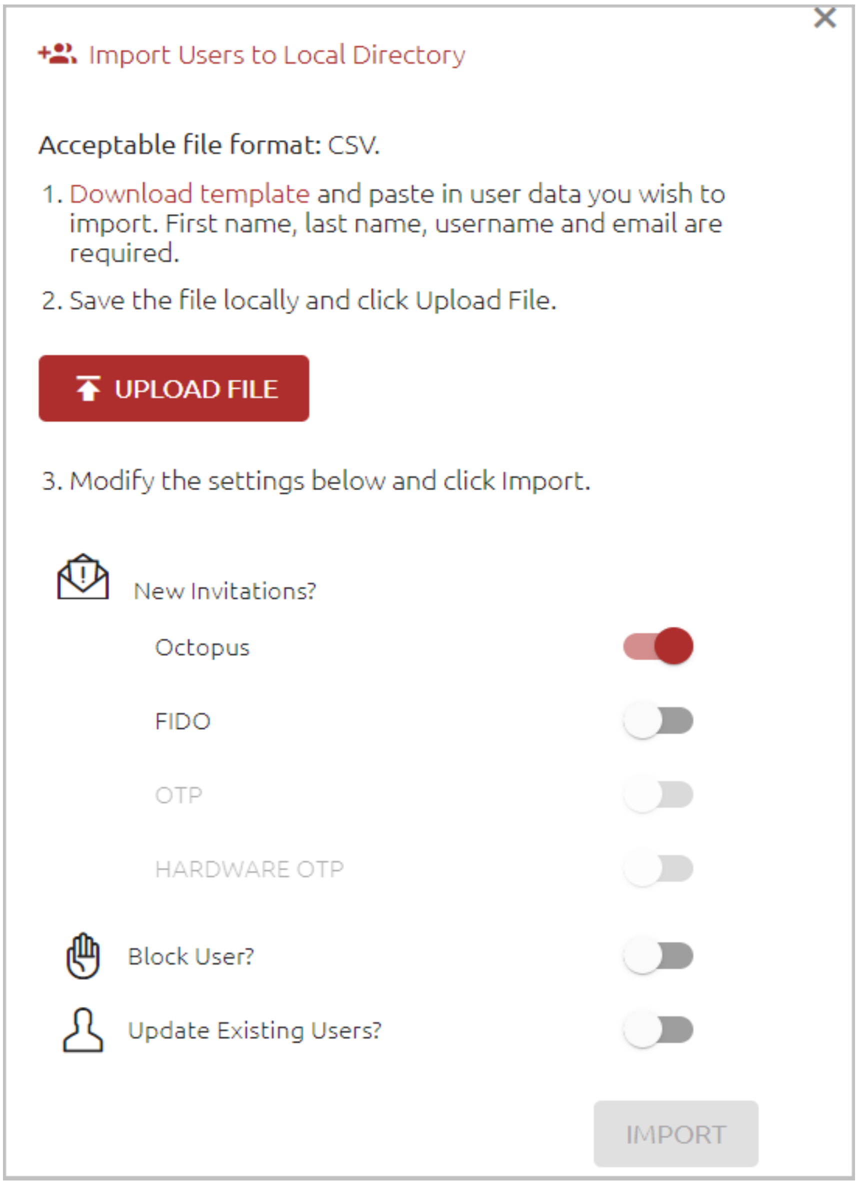
### Importing Local Users from a CSV File

The **Import Users** button enables you to add Local users in a bulk operation by uploading user details from a import file. You can create your own import file based on the template provided, or use a file exported from Microsoft Office 365 or Google G Suite.

**To import Local users from a CSV file:**

1. From the **Manage Users** menu, select the **LOCAL** directory from the **Directories** list. Then, click **Import Users**.

   The **Import Users to Local Directory** dialog opens.



Import Users to Local Directory

Acceptable file format: CSV.

1. Download template and paste in user data you wish to import. First name, last name, username and email are required.

2. Save the file locally and click Upload File.

UPLOAD FILE

3. Modify the settings below and click Import.

New Invitations?

Octopus ●

FIDO ○

OTP ○

HARDWARE OTP ○

Block User? ○

Update Existing Users? ○

IMPORT

If you are using a file exported from Office 365 or G Suite, skip to Step 3.

2. To prepare your import file, click **Download template** and open the file to view the required syntax of the column headers. You may paste user details directly into this file. First and last name, username and email parameters are required for each user. All other details are optional.

   After preparing the file, save it locally.

3. Click **Upload File**. Navigate to the relevant import file and then click **Open**.

4. Review the following settings and enable/disable the toggle buttons as required:

   - **Send Invitations**: Determines whether imported users will receive enrollment invitations by email. The default setting is that users receive an invitation to enroll for the Octopus Authenticator. To send invitations for additional authentication types, enable the relevant toggle buttons. If you do not want invitations to be sent, make sure the relevant toggle buttons are disabled. If you block users (see below), the invitation toggle buttons are automatically disabled.

   - **Block Users**: Determines whether imported users will be prevented from authenticating with Octopus Authenticator, FIDO key or OTP. The default setting is Disabled (users will be able to authenticate).

   - **Update Existing Users**: Determines whether user data is overwritten in the event that imported users are already in the system. The default setting is Disabled (user details are not overwritten).

5. To start the import, click **Import**.

   When the import is complete, the Import Summary is displayed. The summary shows how many users were successfully imported, and how many failed to be imported. Click the information icons to view more details.

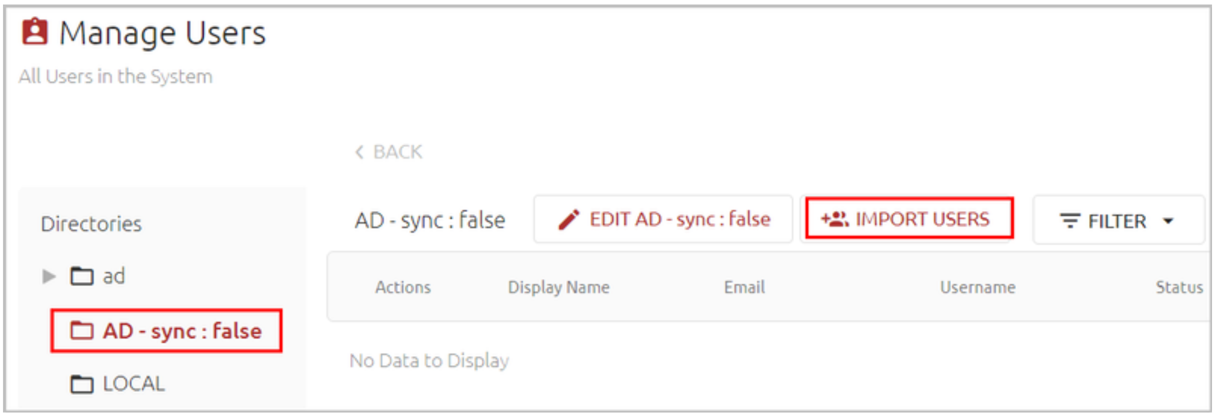
6. To perform an additional import, click **Import More**. To close the dialog and return to the Users list, click **Done**.

## Importing Users from a Directory

The Import Users feature enables you to add users to the Management Console in a bulk operation. Use this feature to import selected users from a directory that is integrated with the Management Console but does NOT have automatic syncing of users.

**To import users from an integrated directory:**

1. From the **Manage Users** menu, select the relevant directory from the **Directories** list. Then, click **Import Users**.



Manage Users

All Users in the System

BACK

Directories

ad

AD - sync : false

LOCAL

AD - sync : false

EDIT AD - sync : false

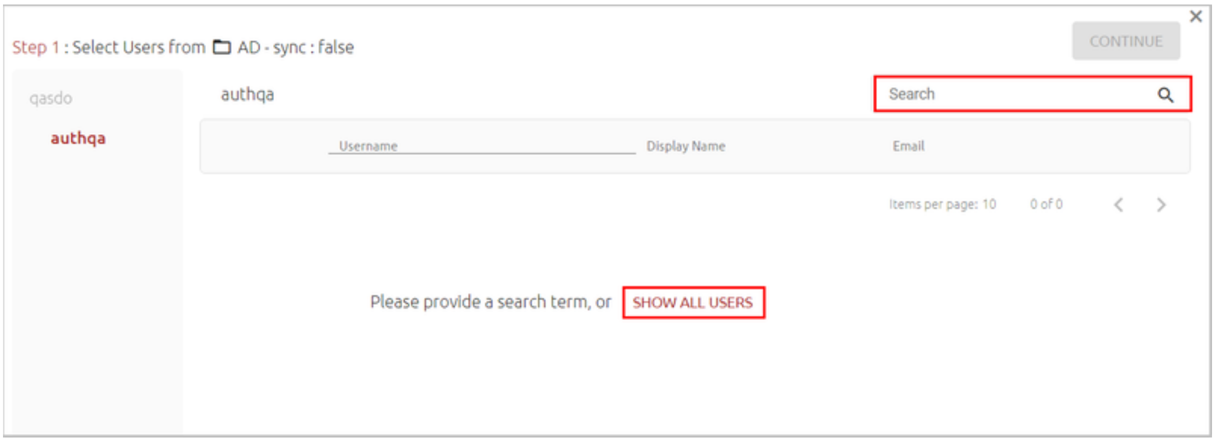
IMPORT USERS

FILTER

| Actions | Display Name | Email | Username | Status |
|---|---|---|---|---|

No Data to Display

2. In the dialog that opens, expand the directory tree and select the node from which you want to import users. You will then be prompted to search for users, or to display all users by clicking **Show All Users**.



Step 1 : Select Users from AD - sync : false

CONTINUE

qasdo

authqa

authqa

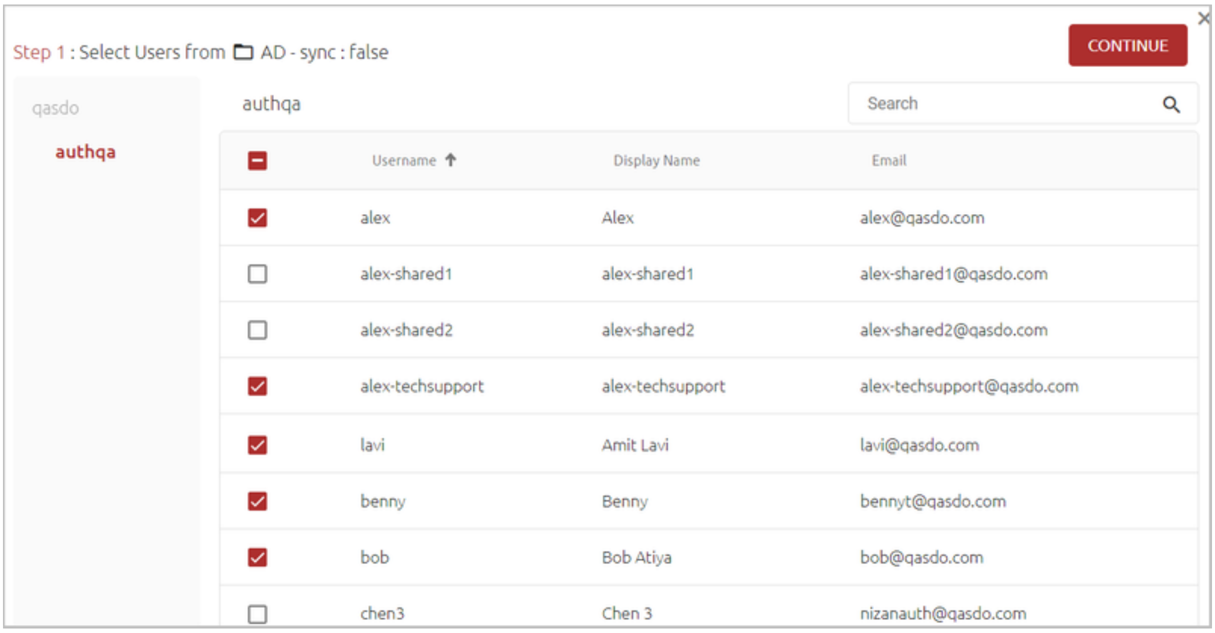
Search

| Username | Display Name | Email |
|---|---|---|

Items per page: 10 0 of 0

Please provide a search term, or SHOW ALL USERS

3. From the list that is displayed, select the checkboxes of the users you want to import.



Step 1 : Select Users from AD - sync : false

CONTINUE

qasdo

authqa

authqa

Search

| ☑ | Username ↑ | Display Name | Email |
|---|---|---|---|
| ☑ | alex | Alex | alex@qasdo.com |
| □ | alex-shared1 | alex-shared1 | alex-shared1@qasdo.com |
| □ | alex-shared2 | alex-shared2 | alex-shared2@qasdo.com |
| ☑ | alex-techsupport | alex-techsupport | alex-techsupport@qasdo.com |
| ☑ | lavi | Amit Lavi | lavi@qasdo.com |
| ☑ | benny | Benny | bennyt@qasdo.com |
| ☑ | bob | Bob Atiya | bob@qasdo.com |
| □ | chen3 | Chen 3 | nizanauth@qasdo.com |

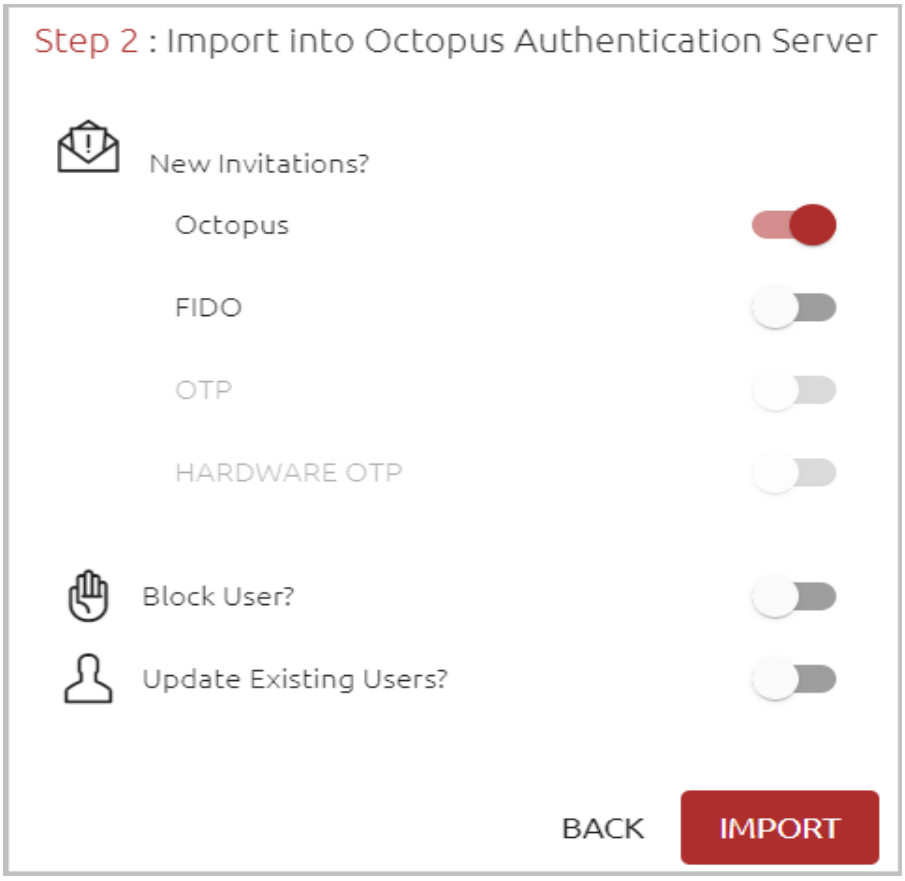
When you have finished selecting users, click **Continue**.

4. Review the following settings and enable/disable the toggle buttons as required:

    ○ **Send Invitations**: Determines whether imported users will receive enrollment invitations by email. The default setting is that users receive an invitation to enroll for Octopus Authenticator. To send invitations for additional authentication types, enable the relevant toggle buttons. If you do not want invitations to be sent, make sure the relevant toggle buttons are disabled. If you block users (see below), the invitation toggle buttons are automatically disabled.

    ○ **Block Users**: Determines whether imported users will be prevented from authenticating with Octopus Authenticator, FIDO key or OTP. The default setting is Disabled (users will be able to authenticate).

    ○ **Update Existing Users**: Determines whether user data is overwritten in the event that imported users are already in the system. The default setting is Disabled (user details are not overwritten).



Step 2 : Import into Octopus Authentication Server

New Invitations?

Octopus ●

FIDO ○

OTP ○

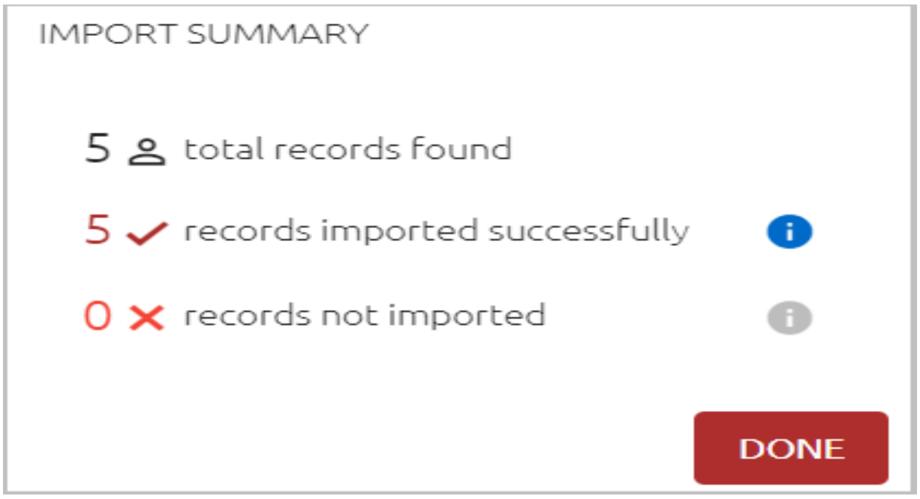
HARDWARE OTP ○

Block User? ○

Update Existing Users? ○

Then, click **Import**.

5. When the import is complete, the Import Summary is displayed. For example:



IMPORT SUMMARY

5 total records found

5 ✓ records imported successfully

0 ✕ records not imported

Click the information icons to view more details.

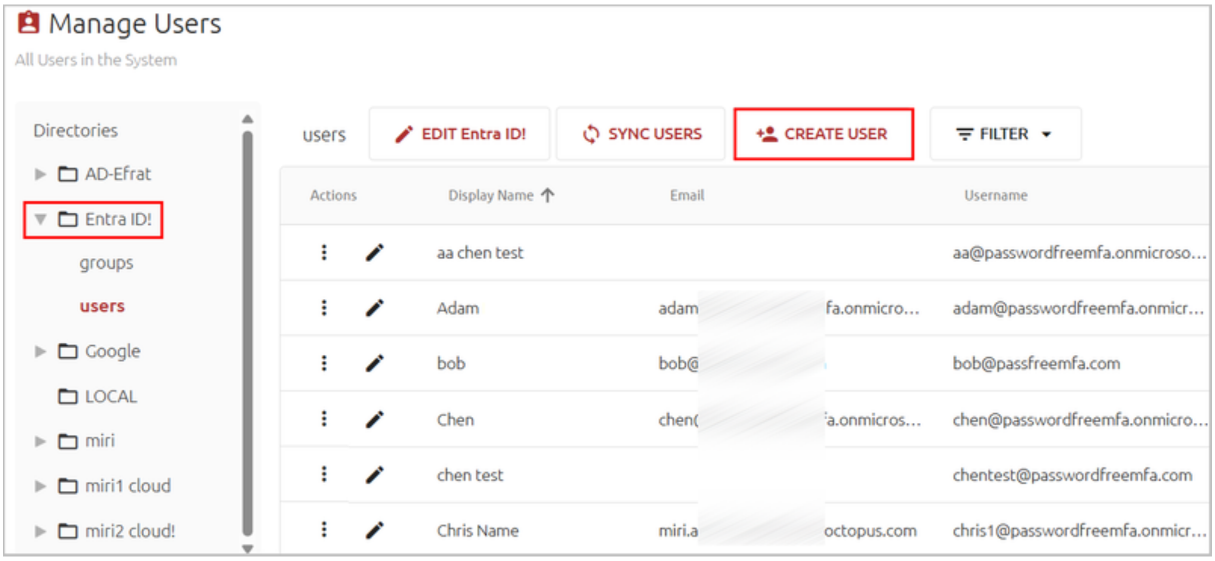
6. To close the dialog and return to the Users list, click **Done**.

## Adding Users to a Federated Entra ID Directory

The Create User action enables you to add a user to an Entra ID directory type that supports O-365 federation. The new user is added directly to the remote Entra ID directory. After creating the user, you will need to perform directory sync or directory import to add the user to the Octopus platform.

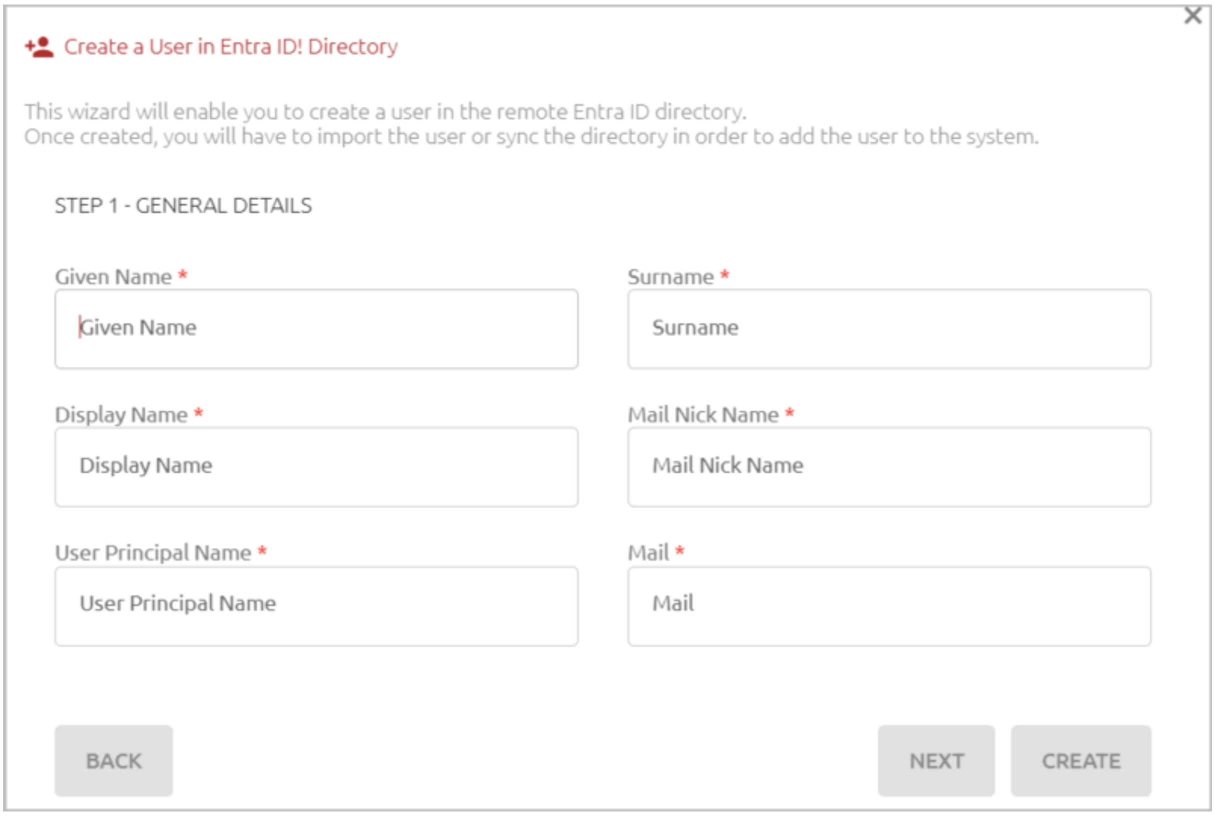
**To add a user to a federated Entra ID directory:**

1. From the **Manage Users** menu, select the relevant Entra ID directory. Then, at the top of the page, click **Create User**.



| Actions | Display Name | Email | Username |
|---|---|---|---|
| ⋮ ✎ | aa chen test | | aa@passwordfreemfa.onmicroso… |
| ⋮ ✎ | Adam | adam[redacted]fa.onmicro… | adam@passwordfreemfa.onmicr… |
| ⋮ ✎ | bob | bob@[redacted] | bob@passfreemfa.com |
| ⋮ ✎ | Chen | chen([redacted]a.onmicros… | chen@passwordfreemfa.onmicro… |
| ⋮ ✎ | chen test | | chentest@passwordfreemfa.com |
| ⋮ ✎ | Chris Name | miri.a[redacted]octopus.com | chris1@passwordfreemfa.onmicr… |

The **Create a User** wizard opens.


Create a User in Entra ID! Directory

This wizard will enable you to create a user in the remote Entra ID directory.
Once created, you will have to import the user or sync the directory in order to add the user to the system.

STEP 1 - GENERAL DETAILS

Given Name *: Given Name

Surname *: Surname

Display Name *: Display Name

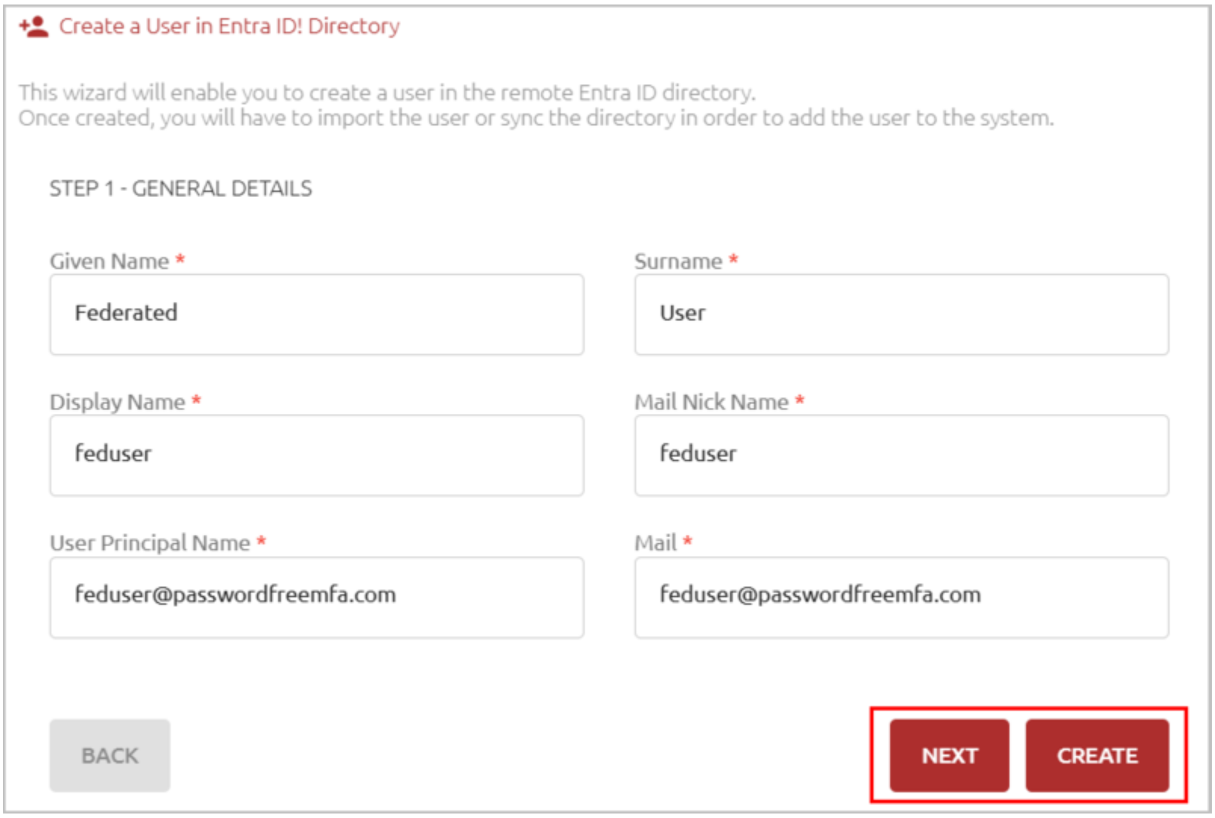
Mail Nick Name *: Mail Nick Name

User Principal Name *: User Principal Name

Mail *: Mail

2. Complete all settings on the first page of the wizard (all are mandatory). When entering the UPN, verify that the federated domain name is used.

   When all settings have been entered, the **Next** and **Create** buttons are enabled.


Create a User in Entra ID! Directory

This wizard will enable you to create a user in the remote Entra ID directory.
Once created, you will have to import the user or sync the directory in order to add the user to the system.

STEP 1 - GENERAL DETAILS

Given Name *: Federated

Surname *: User

Display Name *: feduser

Mail Nick Name *: feduser

User Principal Name *: feduser@passwordfreemfa.com

Mail *: feduser@passwordfreemfa.com

3. To create the user at this point, click **Create** and skip to Step 7 below.

   Alternatively, click **Next** to add more information.

4. On the **Employee Details** page of the wizard, complete optional data such as employee ID, phone number, etc.

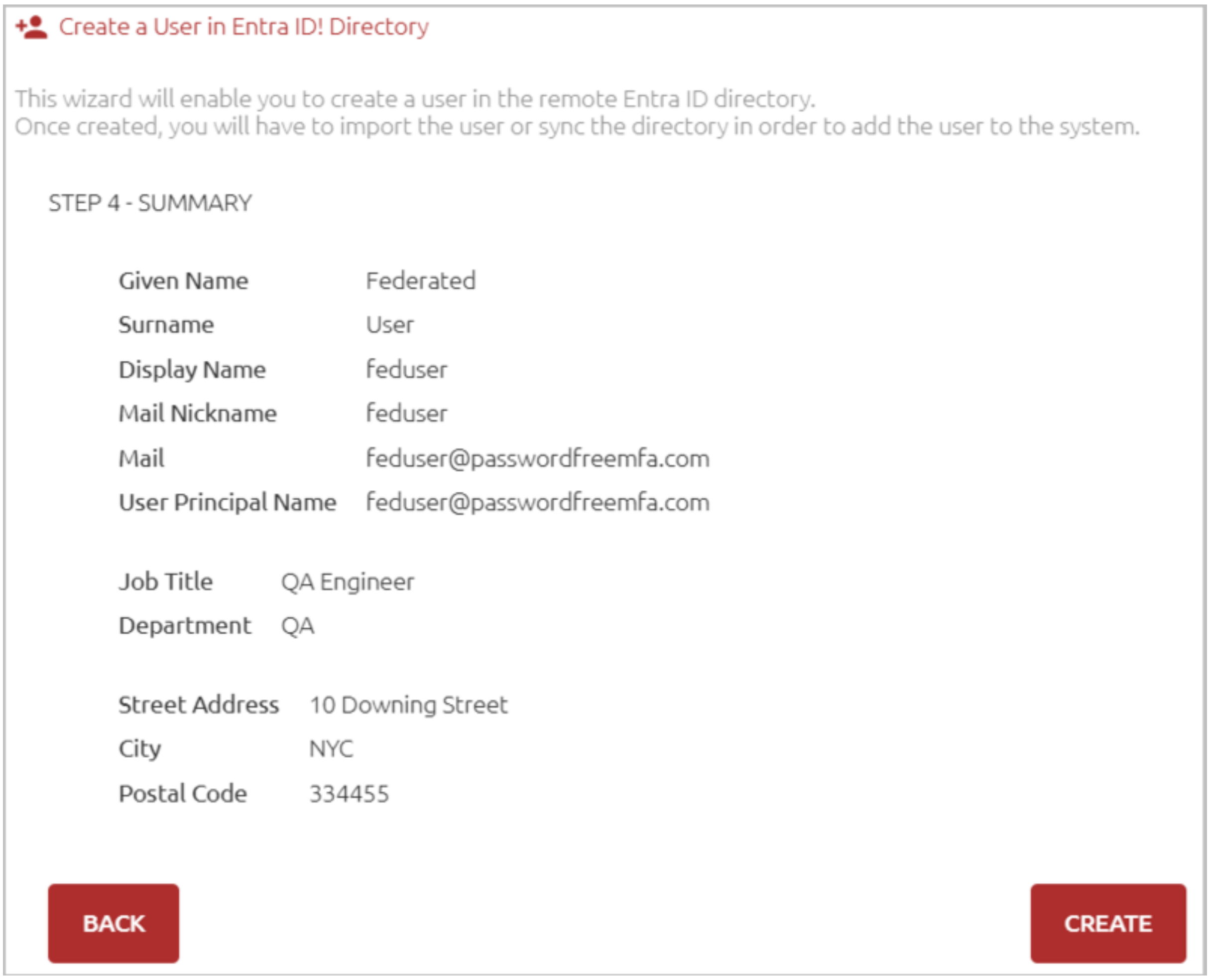
5. To create the user at this point, click **Create** and skip to Step 7 below.

   Alternatively, click **Next** to add more information.

6. One the **Address** page of the wizard, enter street address details for the user. (All settings are optional.)

   Then, click **Next** or **Create**.

7. On the **Summary** page of the wizard, review all configured settings. If you need to correct data, click **Back** to navigate to the relevant page.



Create a User in Entra ID! Directory

This wizard will enable you to create a user in the remote Entra ID directory.
Once created, you will have to import the user or sync the directory in order to add the user to the system.

STEP 4 - SUMMARY

| | |
|---|---|
| Given Name | Federated |
| Surname | User |
| Display Name | feduser |
| Mail Nickname | feduser |
| Mail | feduser@passwordfreemfa.com |
| User Principal Name | feduser@passwordfreemfa.com |

| | |
|---|---|
| Job Title | QA Engineer |
| Department | QA |

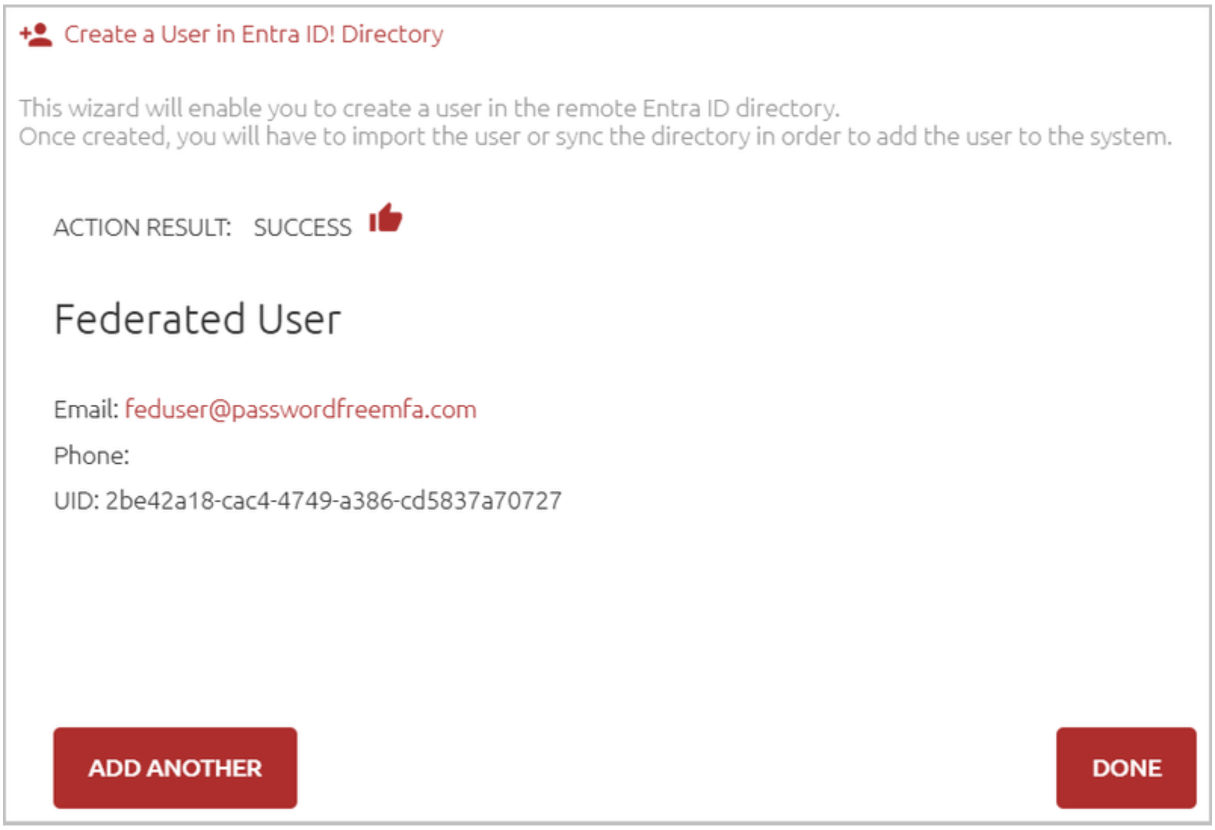
| | |
|---|---|
| Street Address | 10 Downing Street |
| City | NYC |
| Postal Code | 334455 |

**Important**

Check all information carefully. Once the user is created, details can be updated using native Microsoft tools only.

8. Click **Create**.

When the user is successfully added, a confirmation message is displayed with a unique identifier for the new user.



Create a User in Entra ID! Directory

This wizard will enable you to create a user in the remote Entra ID directory.
Once created, you will have to import the user or sync the directory in order to add the user to the system.

ACTION RESULT: SUCCESS

Federated User

Email: feduser@passwordfreemfa.com

Phone:

UID: 2be42a18-cac4-4749-a386-cd5837a70727

9. To create an additional user, click **Add Another**. To close the dialog and return to the Users list, click **Done**.

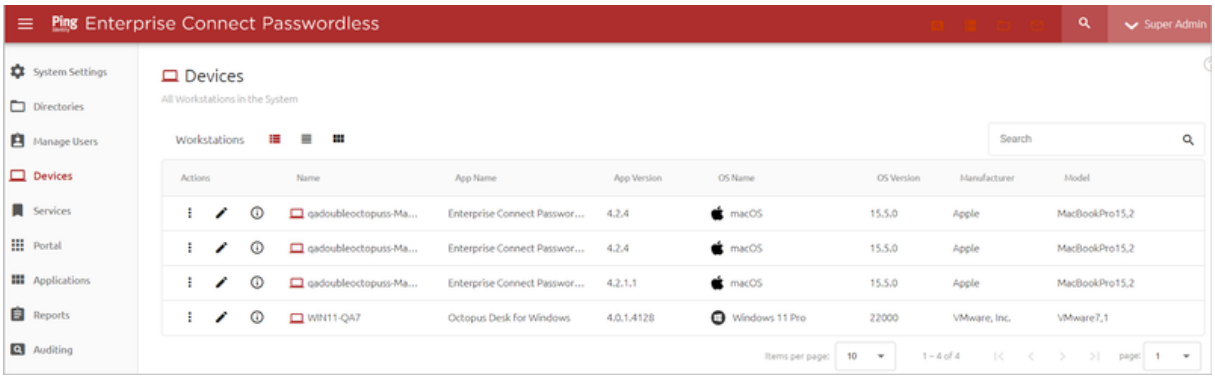
10. When all users have been created, add them to the Octopus platform using the relevant method:

    ○ If the Entra ID integrated directory has automatic syncing enabled, click **Sync Users**.

    ○ If the Entra ID integrated directory does not have automatic syncing, click **Import Users** to add the users manually.

## Managing System Workstations

The **Devices** menu enables you to easily view and manage any workstation that communicates with the Octopus Authentication Server. The Workstations grid lists all machines in the system and provides basic information about each one. You can quickly locate specific workstations using the Search tool, by entering the name or ID of the workstation.



Devices

All Workstations in the System

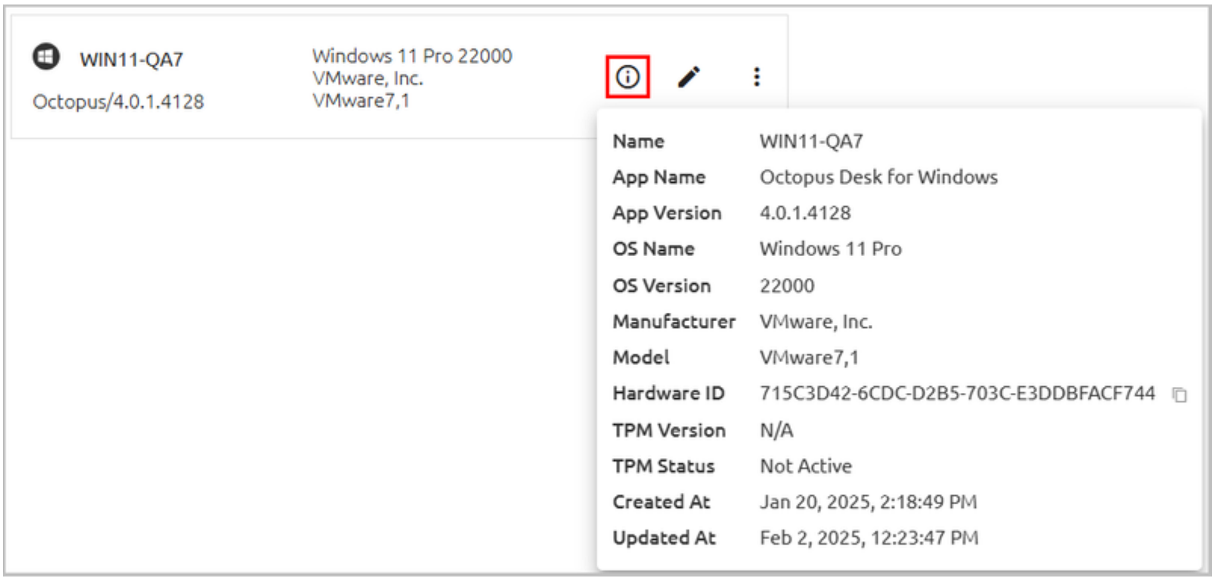
Workstations

Search

| Actions | Name | App Name | App Version | OS Name | OS Version | Manufacturer | Model |
|---|---|---|---|---|---|---|---|
| ⋮ ✎ ⓘ | qadoubleoctopuss-Ma... | Enterprise Connect Passwor... | 4.2.4 | macOS | 15.5.0 | Apple | MacBookPro15,2 |
| ⋮ ✎ ⓘ | qadoubleoctopuss-Ma... | Enterprise Connect Passwor... | 4.2.4 | macOS | 15.5.0 | Apple | MacBookPro15,2 |
| ⋮ ✎ ⓘ | qadoubleoctopuss-Ma... | Enterprise Connect Passwor... | 4.2.1.1 | macOS | 15.5.0 | Apple | MacBookPro15,2 |
| ⋮ ✎ ⓘ | WIN11-QA7 | Octopus Desk for Windows | 4.0.1.4128 | Windows 11 Pro | 22000 | VMware, Inc. | VMware7,1 |

Items per page: 10 1 – 4 of 4 page: 1

Clicking ⓘ in the row of a workstation opens a popup showing additional details, including hardware ID, TPM version, and more.



WIN11-QA7 Octopus/4.0.1.4128

Windows 11 Pro 22000
VMware, Inc.
VMware7,1

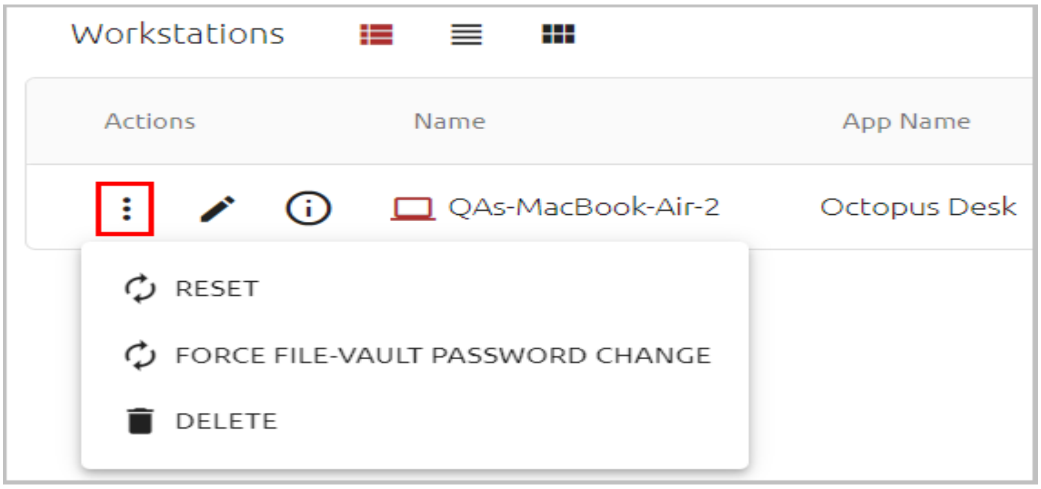
| | |
|---|---|
| Name | WIN11-QA7 |
| App Name | Octopus Desk for Windows |
| App Version | 4.0.1.4128 |
| OS Name | Windows 11 Pro |
| OS Version | 22000 |
| Manufacturer | VMware, Inc. |
| Model | VMware7,1 |
| Hardware ID | 715C3D42-6CDC-D2B5-703C-E3DDBFACF744 |
| TPM Version | N/A |
| TPM Status | Not Active |
| Created At | Jan 20, 2025, 2:18:49 PM |
| Updated At | Feb 2, 2025, 12:23:47 PM |

Clicking ⋮ in the **Actions** column allows you to perform the following operations on the workstation:

- **Reset:** Deletes the workstation's history and all generated security keys. Use the Reset operation following an upgrade to Windows Agent 3.3 or Mac Agent 2.3.0. After a reset, the workstation will generate a new security key with the next authentication.

- **Force FileVault Password Change (Mac workstations only)** : Initiates an immediate rotation of the FileVault password. If the **Password Age** setting is set to 0 (**System Settings > Devices > macOS FileVault Password Settings**), the operation is disabled.

- **Delete:** Deletes the workstation's history and security keys and also removes it from the list of workstations. This operation is generally done for workstations that are no longer in use. If a user authenticates on a deleted workstation, the workstation will be recreated and will reappear in the list.

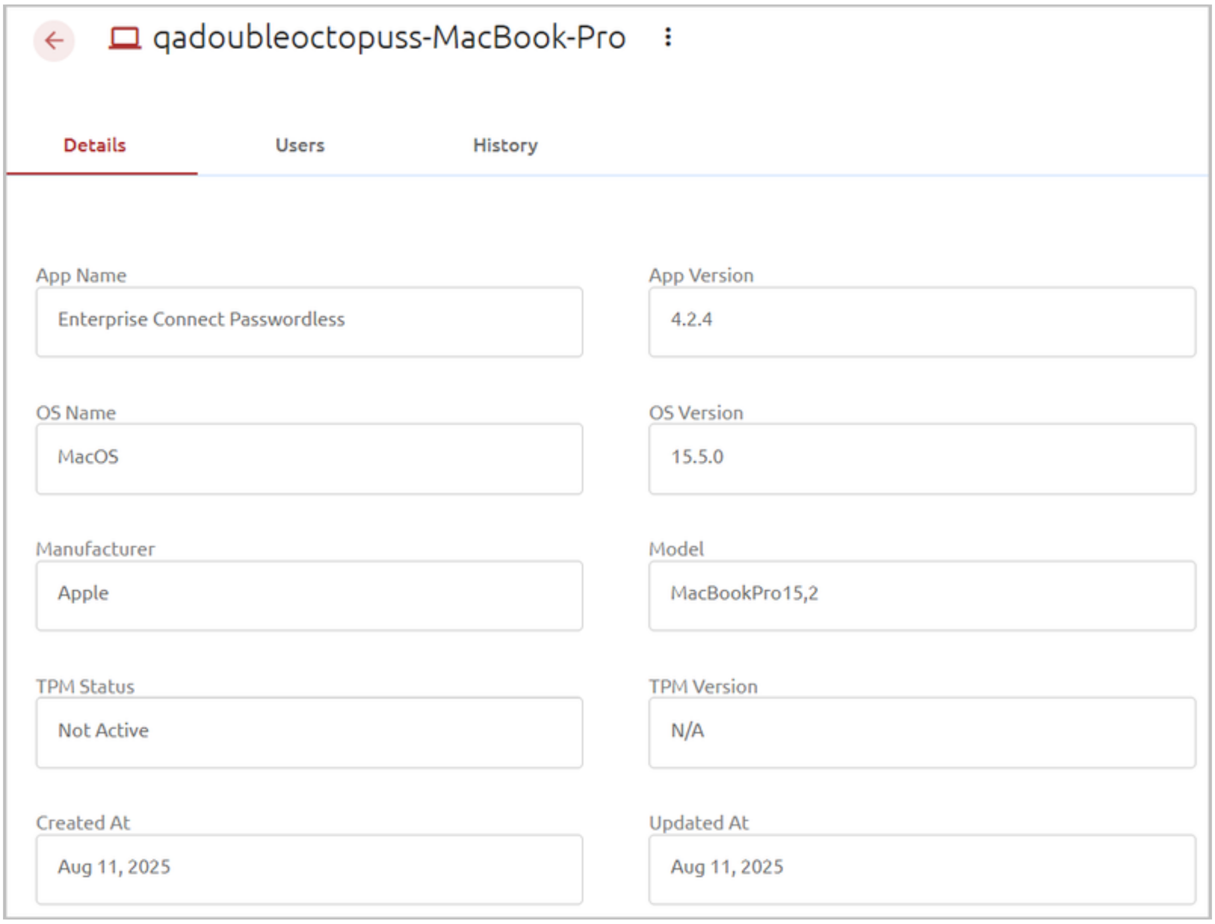


Workstations

| Actions | Name | App Name |
|---|---|---|
| ⋮ ✏ ⓘ | QAs-MacBook-Air-2 | Octopus Desk |

Clicking ✏ opens another page containing the following tabs, each of which provides additional data about the workstation:

- **Details:** Lists general information about the workstation, as well as timestamps for the machine's entry into the system and most recent update.

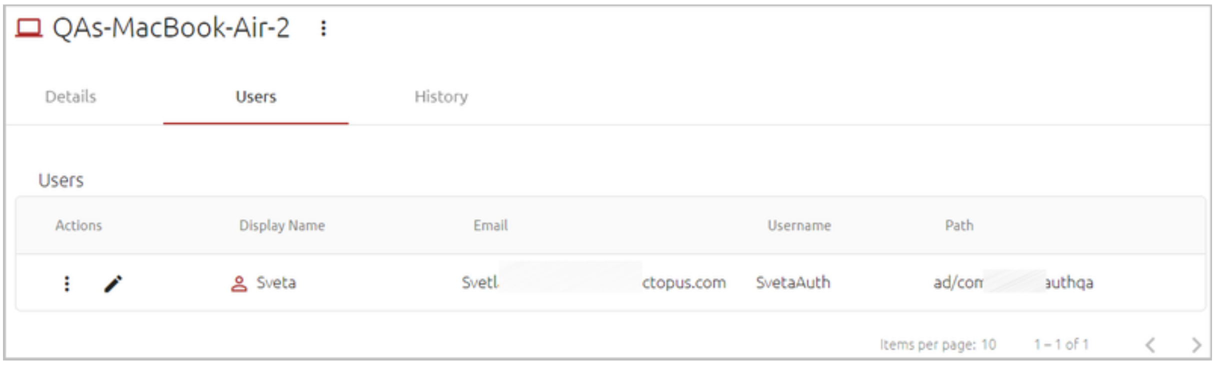


qadoubleoctopuss-MacBook-Pro

| | |
|---|---|
| App Name: Enterprise Connect Passwordless | App Version: 4.2.4 |
| OS Name: MacOS | OS Version: 15.5.0 |
| Manufacturer: Apple | Model: MacBookPro15,2 |
| TPM Status: Not Active | TPM Version: N/A |
| Created At: Aug 11, 2025 | Updated At: Aug 11, 2025 |

- **Users:** List all users who have authenticated through the workstation and provides basic details about each user. Clicking ⋮ in the row of a user enables you to perform some common operations on the user. (For details, refer to Performing

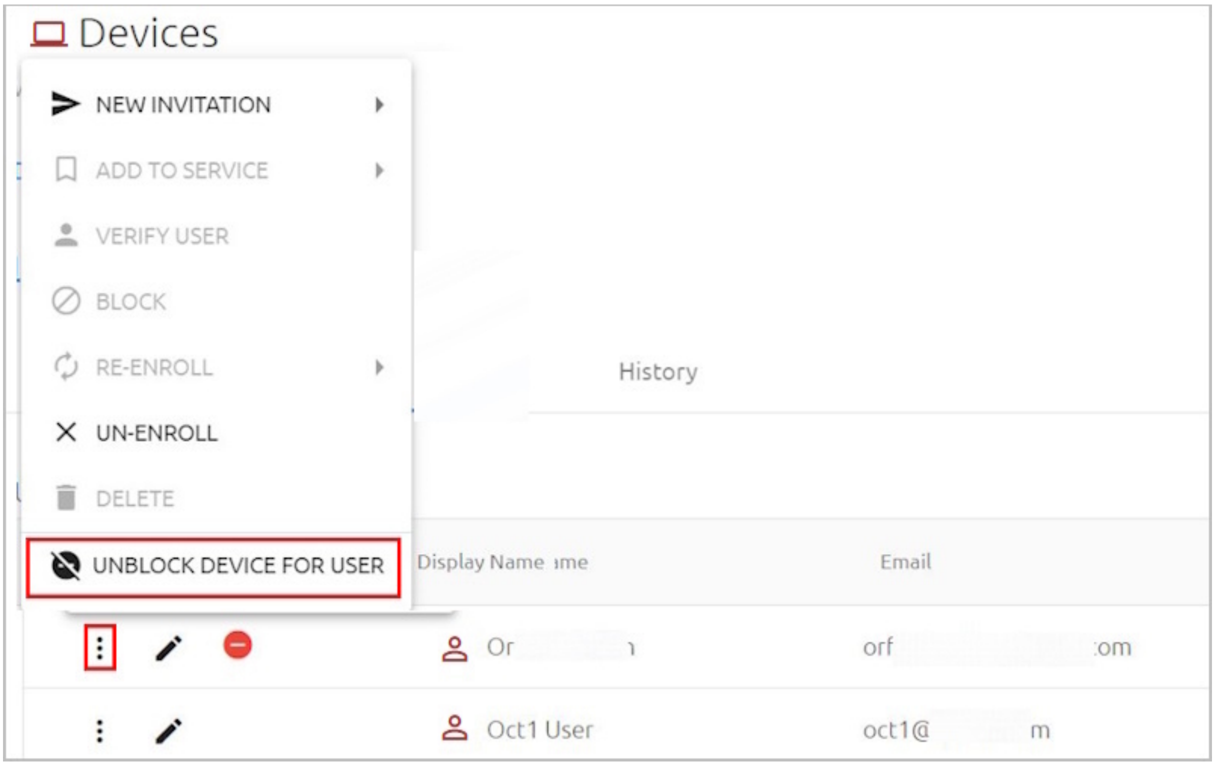
Actions on Users.) Clicking ✎ redirects you to another page where you can view and update user details and settings.



Users

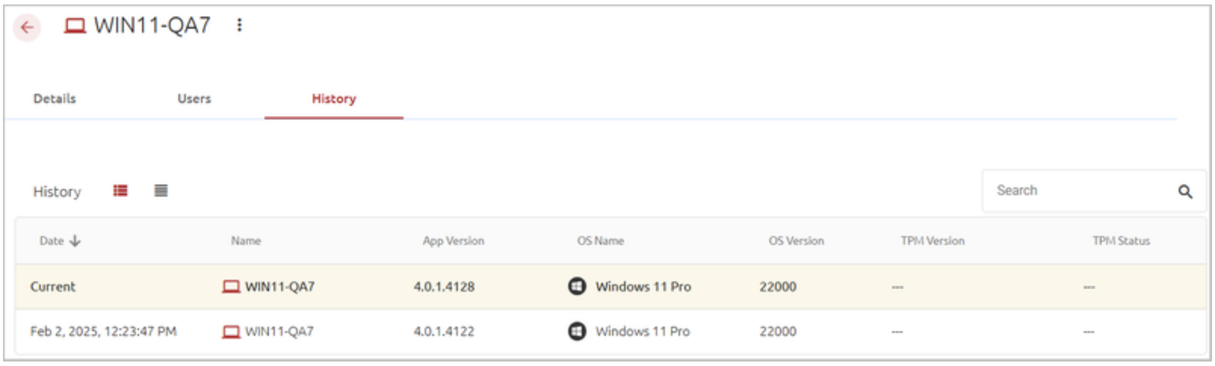
| Actions | Display Name | Email | Username | Path |
|---|---|---|---|---|
| ⋮ ✎ | Sveta | Svetl ctopus.com | SvetaAuth | ad/con authqa |

If a user is currently blocked from accessing the workstation due to enforcement of push fatigue protection mechanisms, the ⛔ icon appears in the row of the user. To manually unblock the user, click ⋮ and select **Unblock Device For User**.



| Display Name | Email |
|---|---|
| Or ı | orf om |
| Oct1 User | oct1@ m |

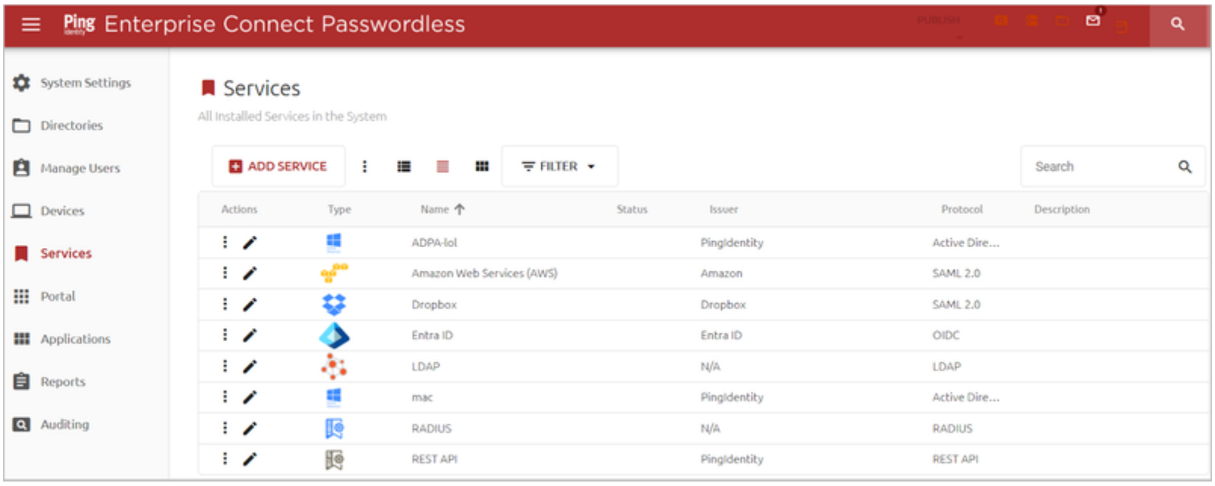
- **History:** Provides information about all updates and upgrades that took place on the workstation.



| Date ↓ | Name | App Version | OS Name | OS Version | TPM Version | TPM Status |
|---|---|---|---|---|---|---|
| Current | WIN11-QA7 | 4.0.1.4128 | Windows 11 Pro | 22000 | --- | --- |
| Feb 2, 2025, 12:23:47 PM | WIN11-QA7 | 4.0.1.4122 | Windows 11 Pro | 22000 | --- | --- |

## Integrating Services

Services are the applications that are integrated to work with the Authentication Server to authenticate users. All services are added, configured and updated from the **Services** menu of the Management Console.



| Actions | Type | Name ↑ | Status | Issuer | Protocol | Description |
|---|---|---|---|---|---|---|
| ⋮ ✎ | | ADPA-lol | | PingIdentity | Active Dire... | |
| ⋮ ✎ | | Amazon Web Services (AWS) | | Amazon | SAML 2.0 | |
| ⋮ ✎ | | Dropbox | | Dropbox | SAML 2.0 | |
| ⋮ ✎ | | Entra ID | | Entra ID | OIDC | |
| ⋮ ✎ | | LDAP | | N/A | LDAP | |
| ⋮ ✎ | | mac | | PingIdentity | Active Dire... | |
| ⋮ ✎ | | RADIUS | | N/A | RADIUS | |
| ⋮ ✎ | | REST API | | PingIdentity | REST API | |

**Note**

Secret Double Octopus provides an extensive collection of guides containing end-to-end instructions on how to configure integration for different services. These How-to guides can be found on the Support Portal or on our website: doubleoctopus.com

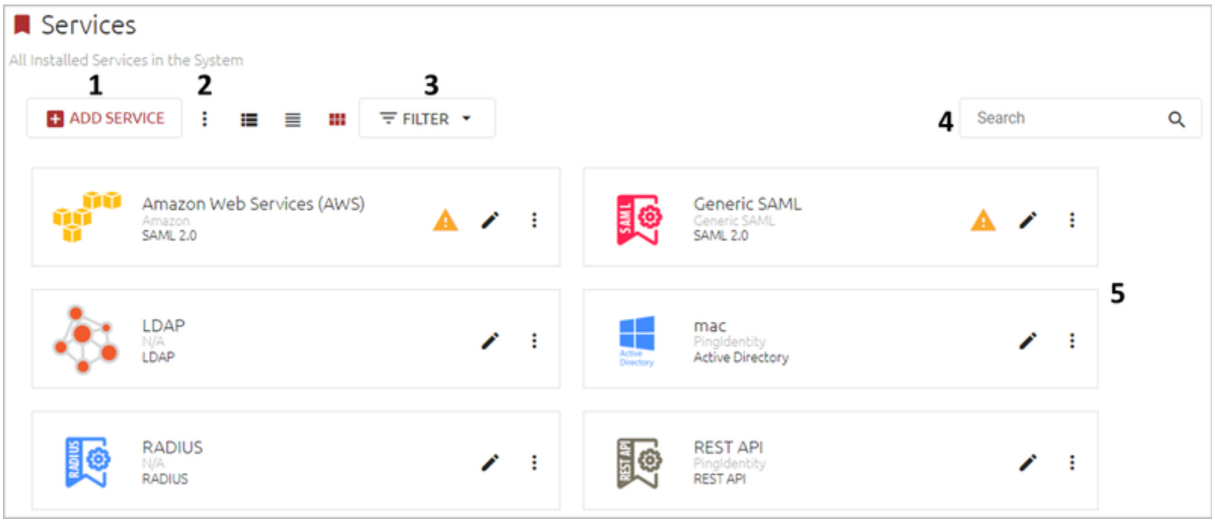
The following sections provide detailed information about working with services:

- Viewing and Managing Installed Services
- Adding Services: Overview and Workflow
- Creating a Service and Assigning Users
- Configuring Service-specific Workstation and Browser Settings
- Configuring Generic SAML Services
- Configuring Generic OpenID Connect Services

- Configuring Radius Services
- Configuring REST API Services
- Configuring LDAP Services
- Configuring Active Directory Authentication Services
- Configuring Amazon Web Service Integration
- Configuring Atlassian Jira Service Integration
- Configuring Dropbox Service Integration
- Configuring Entra ID EAM Service Integration
- Configuring Google G Suite Service Integration
- Configuring Microsoft Office 365 Service Integration
- Configuring WS-Fed Service Integration
- Overriding Default Service Parameters

## Viewing and Managing Installed Services

The **Services** page displays information about all added services and enables you to perform various administrative actions on the services. The main portions and features of the page are described in the table below the diagram.



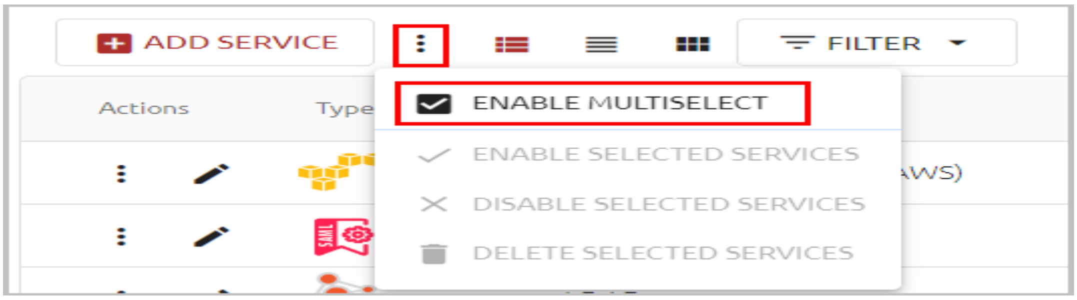
| Number | Feature | Description / Notes |
|---|---|---|
| 1 | Add Service button | Enables you to add a new service. For details, refer to Creating a Service. |
| 2 | Selection mode | Clicking this icon opens the Multiselect feature, which allows you to perform some bulk operations on specific services. For details, refer to Performing Actions on Services. |

| Number | Feature | Description / Notes |
|---|---|---|
| 3 | Filter | This feature shows the total number of enabled, disabled, complete and incomplete (with missing or invalid settings) services, and allows you to filter the Services list according to the option selected. |
| 4 | Search tool | To quickly locate a service, type all or part of the service name in the **Search** field. Keep in mind that the search will be performed only on services that match the current filtering. |
| 5 | Services list | Lists the installed services and provides basic information about each one, including the service name, issuer and type. A ⚠ icon appears in the row or card of services whose settings are incomplete or invalid. Clicking the icon opens a popup listing the invalid settings and a description of the specific error (missing value, incorrect syntax, etc.).<br>You can perform various operations on individual services directly from the Services list. For details, refer to Performing Actions on Services. |

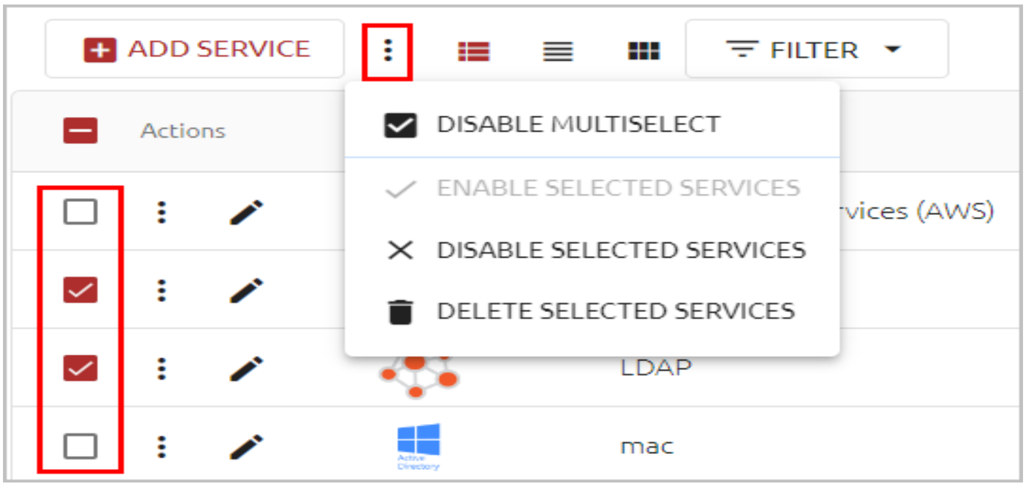
### Performing Actions on Services

The following management operations are available directly from the Services list:

- **Multiselect feature:** Clicking the ⋮ icon at the upper left corner of the Services list opens an actions menu from which you can enable / disable multiple services simultaneously.

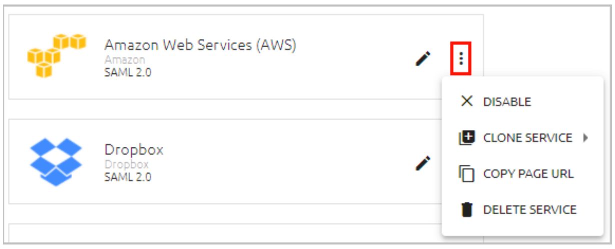


When you click **Enable Multiselect**, checkboxes appear next to each service, allowing you to select one or more services in the Services list. Once services are selected, you can disable them (if they are currently enabled), enable them (if they are currently disabled), or delete them from the system.



To hide the checkboxes and exit selection mode, click **Disable Multiselect**.

- **Edit Service function:** The Edit action allows you to make updates to the settings of a service. To access service settings, click ✎ in the tile or the row of the relevant service.
- **Service actions menu:** To open the actions menu, click ⋮ in the tile or the row of the relevant service.



The actions are:

- **Enable/Disable:** Enables a service that is currently disabled, or disables a service that is currently enabled.
- **Clone Service:** Creates a new instance of the service. All settings of the cloned service are identical to the original service except for certain Sign On settings. For more information, refer to Cloning Services.
- **Copy Page URL:** Provides quick access to the service URL for user authentication. This action is available for SAML services only.
- **Delete Service:** Removes the service from the Management Console.

**Note**

These actions are also available on the settings pages of individual services.

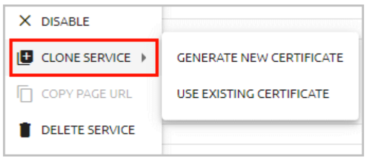
### Cloning Services

The Clone Service action enables you to create a new instance of an existing service. For convenience, all service settings are automatically copied, allowing you to configure only the adjustments that are required for the new service. The following Sign On settings, however, are NOT copied:

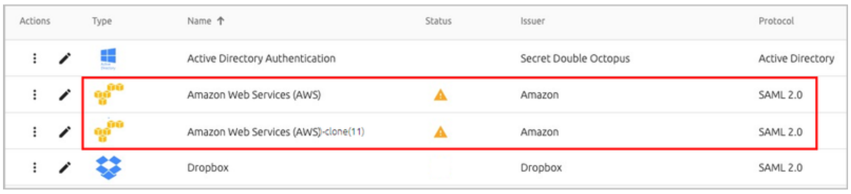
- URLs configured for the service (e.g., Endpoint URL, etc.) are regenerated. The new URLs contain a random UUID instead of the service number. Furthermore, in SAML services, the specific service name no longer appears in the URL path (only *saml* is used).
- In LDAP and RADIUS services, the **Port** field of the cloned service is left blank. The port number needs to be set before the service can be used.

When cloning a service, you will be prompted to select one of the following options:

- **Generate New Certificate:** Choose this option to create and use an additional service with settings similar to the original service.
- **Use Existing Certificate:** Choose this option if you want to continue using the same service but with the newly generated Sign On settings. After cloning the service ,copy the new URLs to the service-side settings.



The name of the cloned service is automatically generated and includes the word *clone* as well as a unique identifier, to avoid cloned service name duplications.



| Actions | Type | Name ↑ | Status | Issuer | Protocol |
|---|---|---|---|---|---|
| ⋮ ✎ | | Active Directory Authentication | | Secret Double Octopus | Active Directory |
| ⋮ ✎ | | Amazon Web Services (AWS) | ⚠ | Amazon | SAML 2.0 |
| ⋮ ✎ | | Amazon Web Services (AWS)-clone(11) | ⚠ | Amazon | SAML 2.0 |
| ⋮ ✎ | | Dropbox | | Dropbox | SAML 2.0 |

## Adding Services: Overview and Workflow

The **Add Service** feature enables you to integrate different types of services with the Management Console. The following categories of services are available for integration:

- **Generic services:** These services include RADIUS, REST API, Generic SAML, and LDAP services. When you add any of these services, the Management Console presents an empty template in which you need to enter all the required parameters.
- **Customized templates:** These include selected services commonly used in enterprises (e.g., Office 365, Jira, etc.) When you add these services, the Management Console presents a template customized for the selected service, in which some of the parameters are pre-populated.
- **Active Directory Authentication services:** This is a service unique to Enterprise Connect Passwordless that enables authentication for Windows, Mac and Microsoft Exchange Server.

### Service Integration Workflow

The general process of integrating a service with the Management Console is the same for all service types. The steps involved are as follows:

1. **Create the service:** Select the service type and specify the service's name, issuer and display icon. The name of the service must be unique.
2. **Configure general details:** Add a description and change the default logo that is displayed to users on the Login screen when they authenticate.
3. **Set parameters:** Parameters are settings of the specific service that the Management Console requires for successful integration. In most cases, the parameters are the configuration received from the service side, and you can copy them to the Management Console.
4. **Set sign on details:** These are the sign-on settings required for the protocol used by the service. After configuring the sign on details, copy them to the Admin Console of the service. Sign on details are generated automatically and need to be copied to the service side.
5. **Select directories and users:** Select the directories that have authorization to authenticate to the service. You can then assign specific Groups and users to the service.

- For more information about creating a service, configuring general details and selecting users, refer to Creating a Service and Assigning Users.
- For information about setting specific parameters and sign on details, refer to the topic describing configuration for the relevant service type.
- For information about creating directory-specific parameters that override default service parameters, refer to Overriding Default Service Parameters.
- For information about defining security mechanisms related to workstations and browsers used to authenticate to a service, refer to Configuring Service-specific Workstation and Browser Settings.

## Creating a Service and Assigning Users

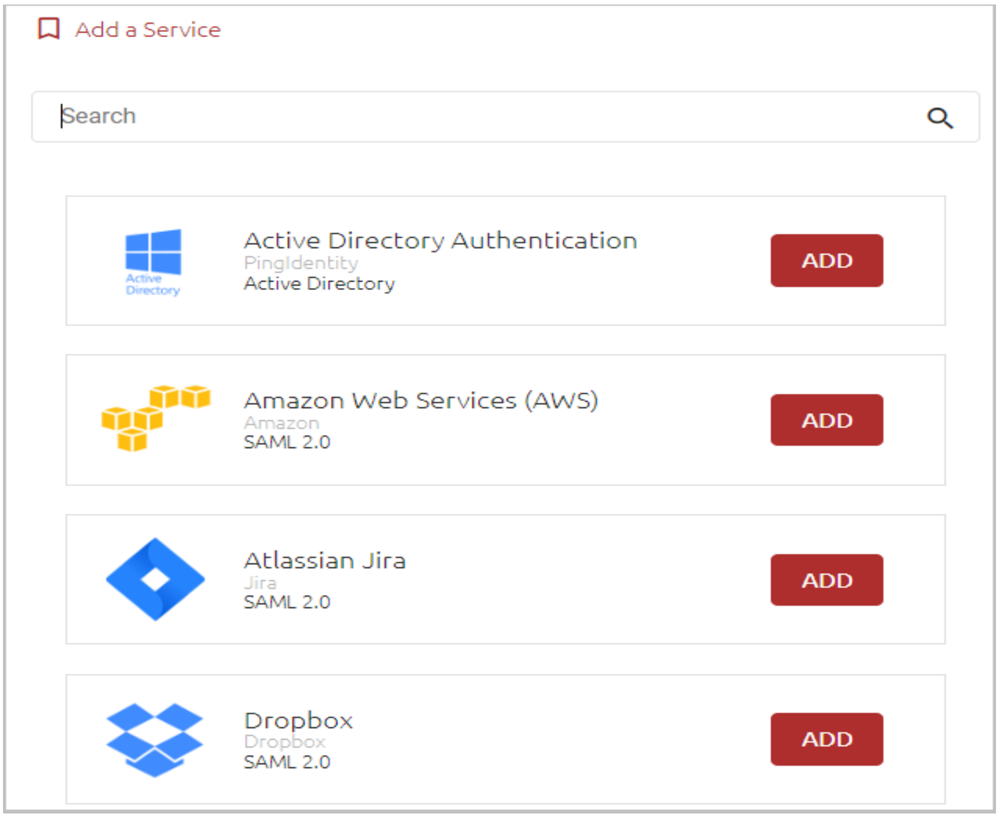
Although each service integrated with the Management Console has its own parameters and sign-on details, the processes of creating a service and assigning users are the same for every service you add. The following sections explain these processes in detail.

### Adding a Service and General Information

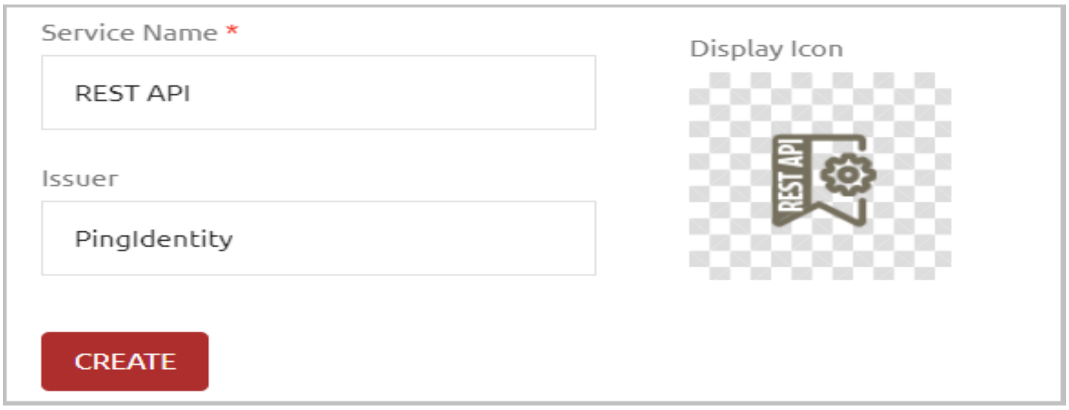
The first step in any service integration is adding the service and specifying its basic details.

**To add a service:**

1. Open the **Services** menu and click **Add Service**.
2. In the tile of the service type that you want to add, click **ADD**.



A dialog opens displaying a default name, issuer and display icon for the service.



Service Name *: REST API

Issuer: PingIdentity

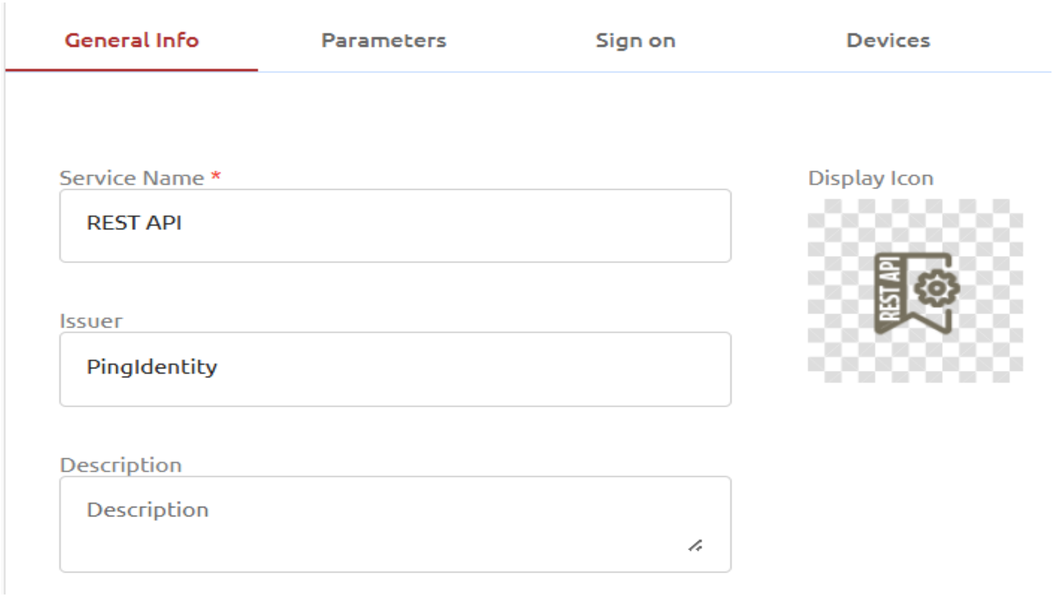
3. If desired, update the default service name and issuer. To change the icon, click the tile and navigate to the file you want to upload. Supported image size is 128x128 pixels.

**Note**

It is not mandatory to update these settings at this point. You will be able to modify the name, issuer and display icon after creating the service.

4. Click **Create**.

   The **General Info** tab for the service opens.



Service Name * REST API

Issuer PingIdentity

Description Description

5. If relevant, configure the following additional settings for the service:
   - **Service activation:** By default, the service is enabled upon creation. If you don't want the service to be active right away, click ⋮ and select **Disable**.
   - **Service description:** You may enter a brief note about the service in the **Description** field.
6. Click **Save.** Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

### Assigning Directories and Users to a Service

In order to be able to access a service using Octopus Authenticator, a user needs to be assigned to the service within the Management Console. Any user who is not specifically assigned to a service will not have authorization to authenticate to the service.

Before assigning users to a service, it is recommended to assign the relevant directory (or directories) to that service.

**Important**

In order to enable users to authenticate to Windows using a FIDO key, the corporate directory must have a configured domain. It is recommended to open the directory settings and verify that the **Domain** field is completed.

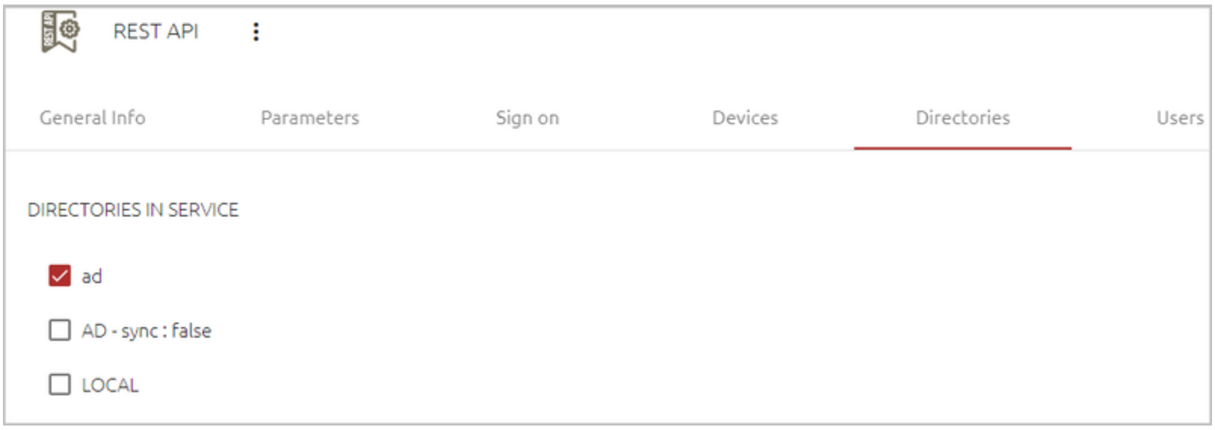
The following procedure explains how to assign directories and users from the service settings.

**Note**

A service can be enabled or disabled for an individual user from the settings of the relevant user. For details, refer to Viewing and Updating User Details.

**To assign directories and users to a service:**

1. Open the settings of the relevant service and select the **Directories** tab. Select the checkboxes of the directories that you want to integrate with the service, and then click **Save.**



DIRECTORIES IN SERVICE

☑ ad

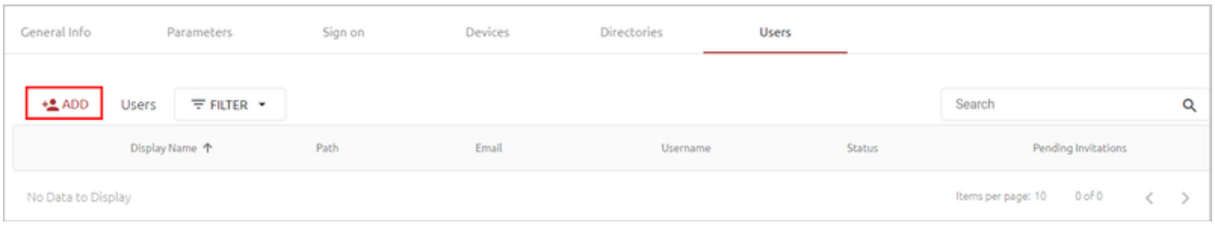
□ AD - sync : false

□ LOCAL

**Important**

Only ONE directory may be selected for integration with LDAP services.

2. After selecting directories, open the **Users** tab and click **Add.**



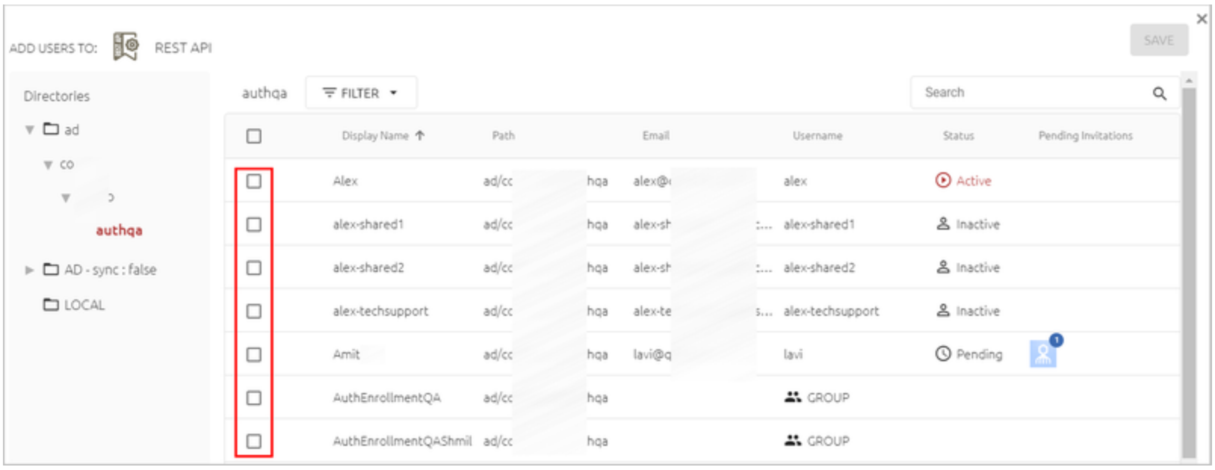
| Display Name ↑ | Path | Email | Username | Status | Pending Invitations |
|---|---|---|---|---|---|

No Data to Display

Items per page: 10 0 of 0

The **Add Users To** popup opens. A list of directories integrated with the Management Console appears on the left side of the popup.

3. Open the directories tree and select the checkboxes of the users and Groups that you want to add to the service.

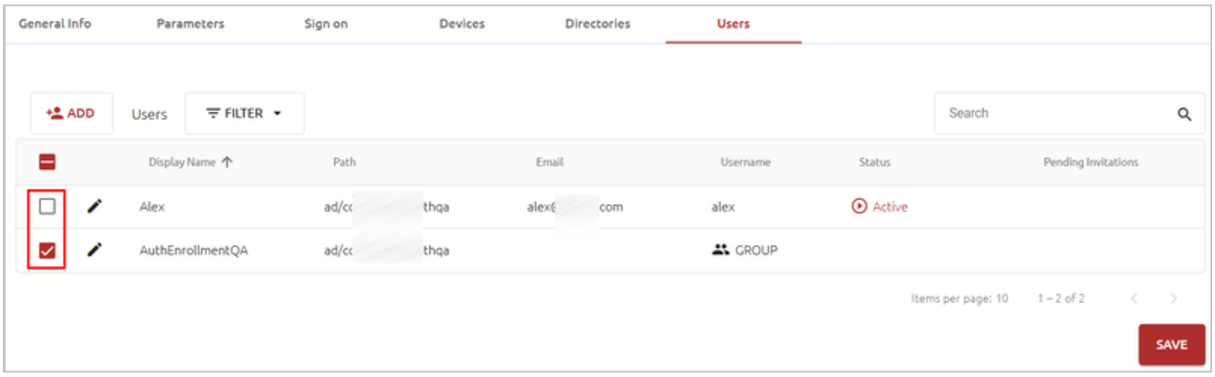


| □ | Display Name ↑ | Path | Email | Username | Status | Pending Invitations |
|---|---|---|---|---|---|---|
| □ | Alex | ad/cc hqa | alex@ | alex | Active | |
| □ | alex-shared1 | ad/cc hqa | alex-sh :... | alex-shared1 | Inactive | |
| □ | alex-shared2 | ad/cc hqa | alex-sh :... | alex-shared2 | Inactive | |
| □ | alex-techsupport | ad/cc hqa | alex-te s... | alex-techsupport | Inactive | |
| □ | Amit | ad/cc hqa | lavi@q | lavi | Pending | 1 |
| □ | AuthEnrollmentQA | ad/cc hqa | | GROUP | | |
| □ | AuthEnrollmentQAShmil | ad/cc hqa | | GROUP | | |

When you have finished making your selections, close the popup by clicking **SAVE**.

4. From the toolbar at the top of the page, click **PUBLISH** and publish your changes.

After assigning users to a service, you can manage them directly from the **Users** tab. To enable or disable the service for a specific user, toggle the checkbox on the left side of the row. Clicking the Edit icon next to the checkbox opens the individual settings for that user (Viewing and Updating User Details).



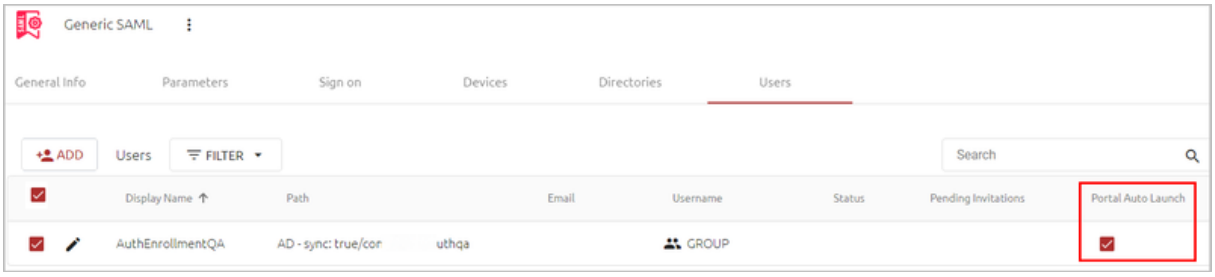
| | | Display Name ↑ | Path | Email | Username | Status | Pending Invitations |
|---|---|---|---|---|---|---|---|
| ☐ | ✎ | Alex | ad/cc thqa | alex com | alex | Active | |
| ☑ | ✎ | AuthEnrollmentQA | ad/cc thqa | | GROUP | | |

Items per page: 10 1 – 2 of 2

### Portal Auto Launch

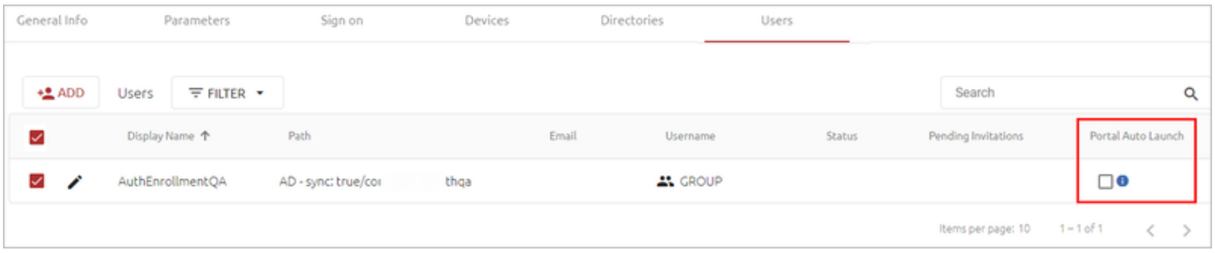
The **Portal Auto Launch** column, which is relevant only to SAML services, indicates whether the Auto Launch feature is currently enabled for that group / user. (When the feature is enabled, the SAML service opens automatically upon login to the User Portal.) You can enable or disable Automatic Launch for any group or user, regardless of whether the **Automatic Launch** toggle is selected for the SAML service (in the **Sign on** tab of the service settings).

In the example below, Automatic Launch is enabled for the group, matching the setting specified in the **Sign on** tab of the SAML service.



| ☑ | | Display Name ↑ | Path | Email | Username | Status | Pending Invitations | Portal Auto Launch |
|---|---|---|---|---|---|---|---|---|
| ☑ | ✎ | AuthEnrollmentQA | AD - sync: true/cor uthqa | | GROUP | | | ☑ |

If the setting for a group or user differs from that specified in the service settings, the exception is indicated by an Information icon in the column. In the following example, Auto Launch is NOT enabled for this particular group, but it is enabled in the service settings.



| ☑ | | Display Name ↑ | Path | Email | Username | Status | Pending Invitations | Portal Auto Launch |
|---|---|---|---|---|---|---|---|---|
| ☑ | ✎ | AuthEnrollmentQA | AD - sync: true/coı thqa | | GROUP | | | ☐ ℹ |

Items per page: 10 1 – 1 of 1

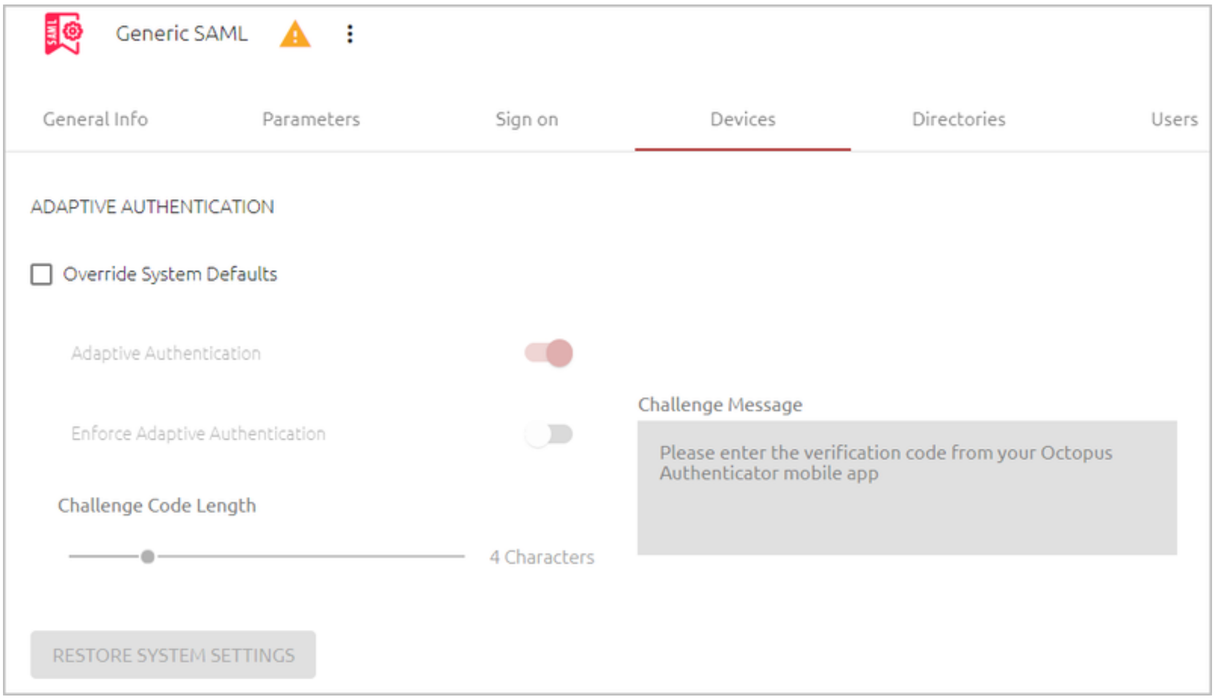
To configure the Automatic Launch setting for a group or user, select or clear the **Portal Auto Launch** checkbox, and then click **Save**.

**Note**

To configure Automatic Launch, **SSO** must be enabled in the SAML service settings. If SSO is not selected in the service settings, the **Portal Auto Launch** checkbox is disabled.

## Configuring Service-specific Workstation and Browser Settings

The **Devices** tab for a service enables you to define various security mechanisms related to workstations and browsers used for authentication to specific services integrated with the platform.



ADAPTIVE AUTHENTICATION

□ Override System Defaults

Adaptive Authentication

Enforce Adaptive Authentication

Challenge Code Length

4 Characters

Challenge Message

Please enter the verification code from your Octopus Authenticator mobile app

### Adaptive Authentication

Adaptive Authentication provides an extra layer of security when authentication is attempted from a workstation or browser not previously used for Octopus Authentication. When the feature is enabled, users authenticating for the first time from a unrecognized device are required to enter the verification code that is generated and displayed in the Octopus Authenticator mobile app. After the first successful authentication, users are no longer required to enter a code if the browser or workstation is designated as a Trusted device.

**Note**

For more information about Adaptive Authentication, refer to Managing Workstation and Browser Settings.

Global settings for Adaptive Authentication are defined in the **Devices** tab of the **System Settings** menu. However, if a specific service requires different handling of Adaptive Authentication, you can configure other settings for that service only, in the **Devices** tab of the service's settings. For example, you may not want to use Adaptive Authentication for a given service, or you might want to change the number of digits in the verification code.

**To define Adaptive Authentication settings for a specific service:**

1. From the **Services** menu, click ✏ to open the service settings. Then, select the **Devices** tab.

2. At the top of the tab, select the **Override System Defaults** checkbox to enable the settings below.

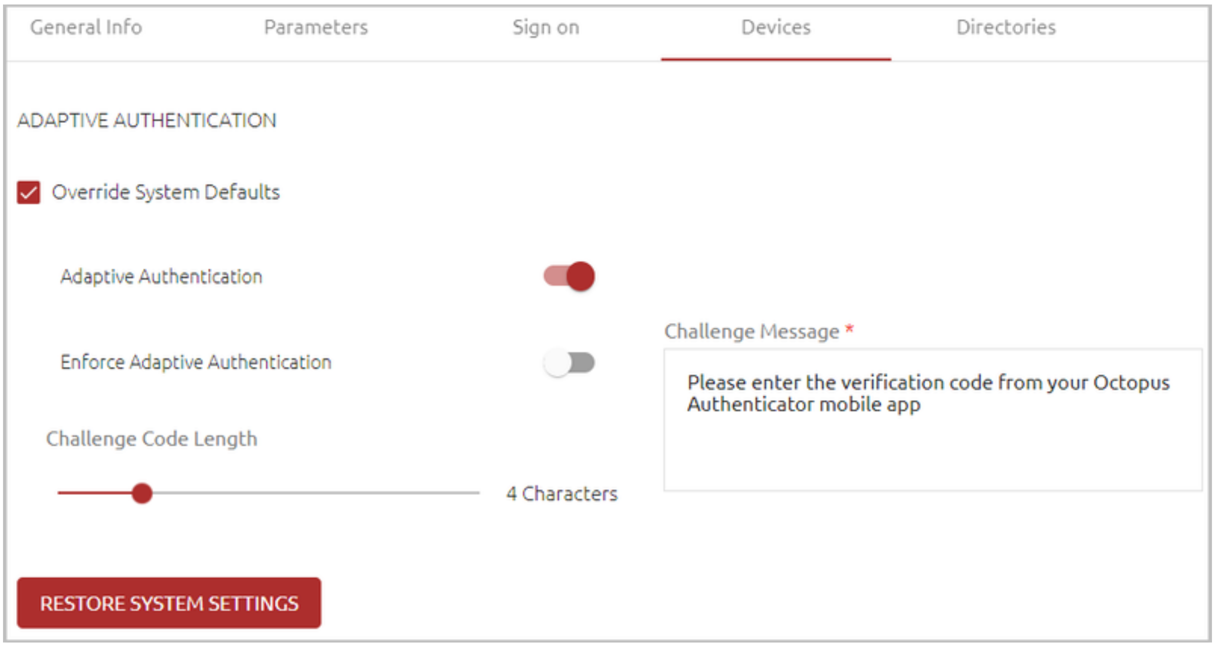
3. Configure the following settings as required:

    - **Adaptive Authentication:** Activates / Disables the Adaptive Authentication mechanism. When the toggle is not selected, the other settings are disabled.

    - **Enforce Adaptive Authentication:** This setting determines whether the Adaptive Authentication mechanism will apply to users authenticating with versions of Octopus Authenticator lower than 5.0. When the setting is *off*, users with previous versions of Windows, Mac or Exchange agent will be able to authenticate from an unrecognized device without entering a challenge code. When the setting is *on*, authentication will fail, and these users will need to upgrade to the newest version in order to successfully authenticate.

    - **Challenge Code Length:** Number of characters in the verification code. Valid values range from 3-8. The default value is 4.

    - **Challenge Message:** The message displayed to users prompting them to enter the verification code.



ADAPTIVE AUTHENTICATION

☑ Override System Defaults

Adaptive Authentication: on

Enforce Adaptive Authentication: off

Challenge Code Length: 4 Characters

Challenge Message *

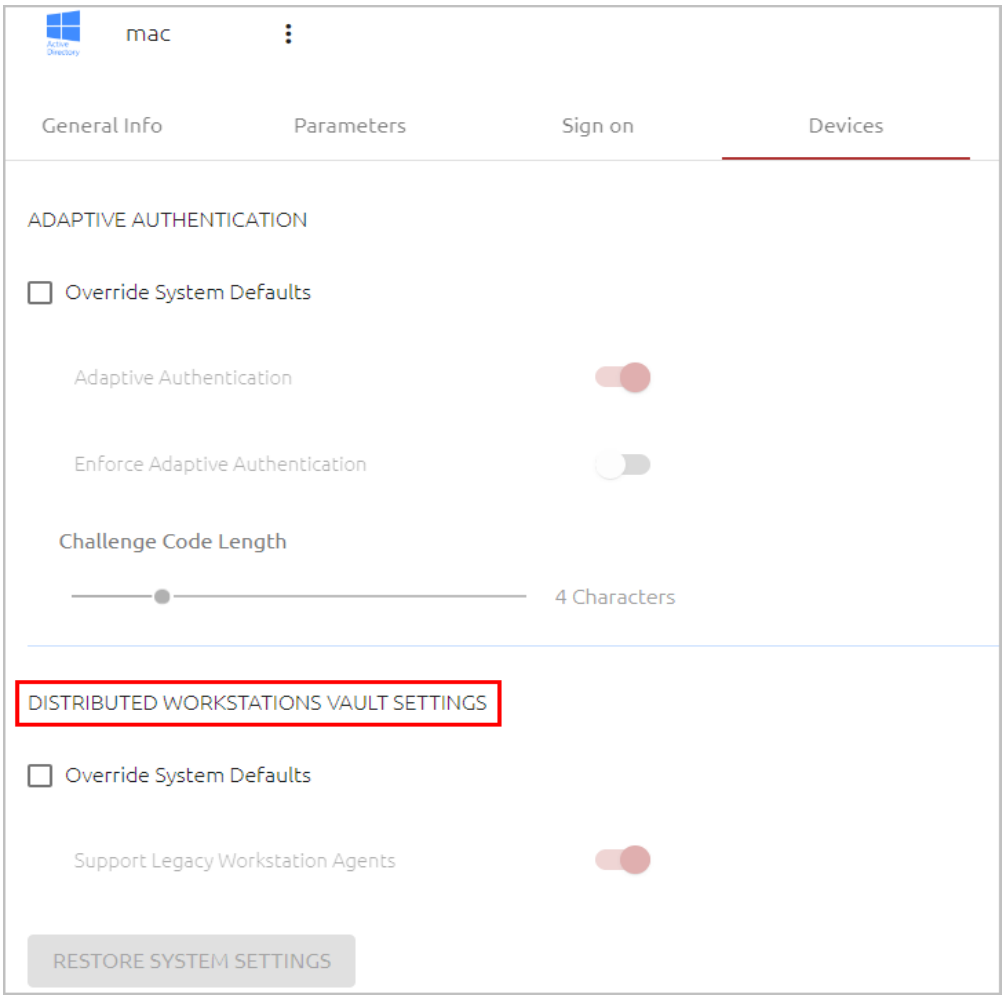
Please enter the verification code from your Octopus Authenticator mobile app

4. Click **Save**.

Clicking **Restore System Settings** resets all settings in the **Devices** tab to the default values defined in the **System Settings** menu. After clicking this button, confirm the action by clicking **Restore** in the verification popup. Then, click **Save**.

### Distributed Workstations Vault Settings (ADPA only)

Active Directory Authentication services feature an additional component in the **Devices** tab which allows you to specify whether the service will support Legacy Workstation Agents. Legacy workstations are those running versions below Windows Agent 3.3 and Mac Agent 2.3.0.



mac

General Info | Parameters | Sign on | Devices

ADAPTIVE AUTHENTICATION

□ Override System Defaults

Adaptive Authentication ●

Enforce Adaptive Authentication ○

Challenge Code Length

4 Characters

DISTRIBUTED WORKSTATIONS VAULT SETTINGS

□ Override System Defaults

Support Legacy Workstation Agents ●

RESTORE SYSTEM SETTINGS

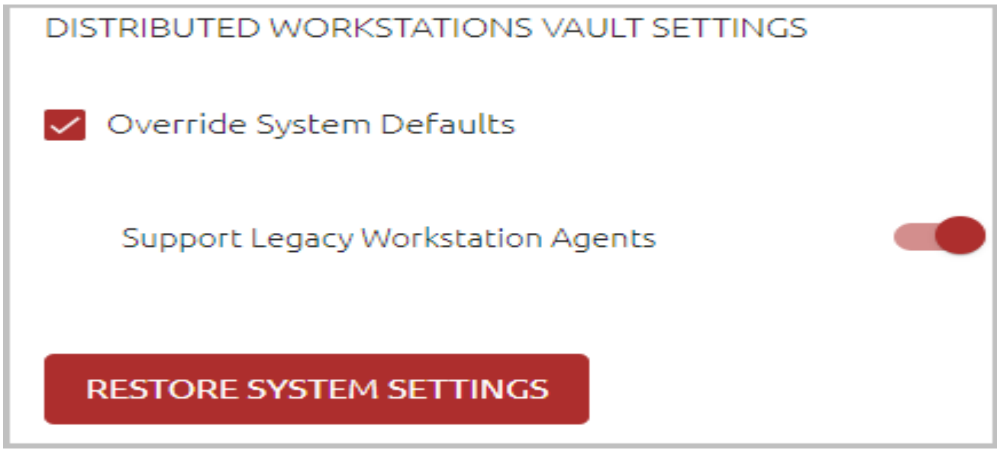
Workstations running Windows Agent version 3.3 (and higher) or Mac Agent version 2.3.0 (and higher) have an extra layer of encryption for communication with the Octopus Authentication Server. Besides credentials encryption, all data passed between the workstation and the Server is encrypted as well. Security keys that were generated by workstations running older versions of the Windows / Mac Agent will therefore be incompatible for workstations running versions Windows Agent 3.3 / Mac Agent 2.3.0 (and above).

When Legacy Workstation Agents are supported, these workstations continue to communicate with the server without complete data encryption. Legacy workstation support is generally implemented when support of the Exchange server is required.

The global setting for Legacy Workstation Agent support is defined in the **Devices** tab of the **System Settings** menu. However, you can override the default setting for your Active Directory Authentication service in the **Devices** tab of the service's settings.

**To set Legacy Workstation Agent support for an AD Authentication service:**

1. From the **Services** menu, in the row or card of the relevant AD Authentication service, click ✎ to open the service settings. Then, select the **Devices** tab.
2. Under **Distributed Workstations Vault Settings**, select the **Override System Defaults** checkbox to enable the settings below.
3. Activate or disable the **Support Legacy Workstation Agents** toggle button, as required.



DISTRIBUTED WORKSTATIONS VAULT SETTINGS

☑ Override System Defaults

Support Legacy Workstation Agents ●

**Important**

If the **Compatibility Mode** toggle in the global Distributed Workstations Vault Settings (**System Settings > Devices**) is OFF, you will not be able to activate the **Support Legacy Workstation Agents** toggle.

4. Click **Save**.

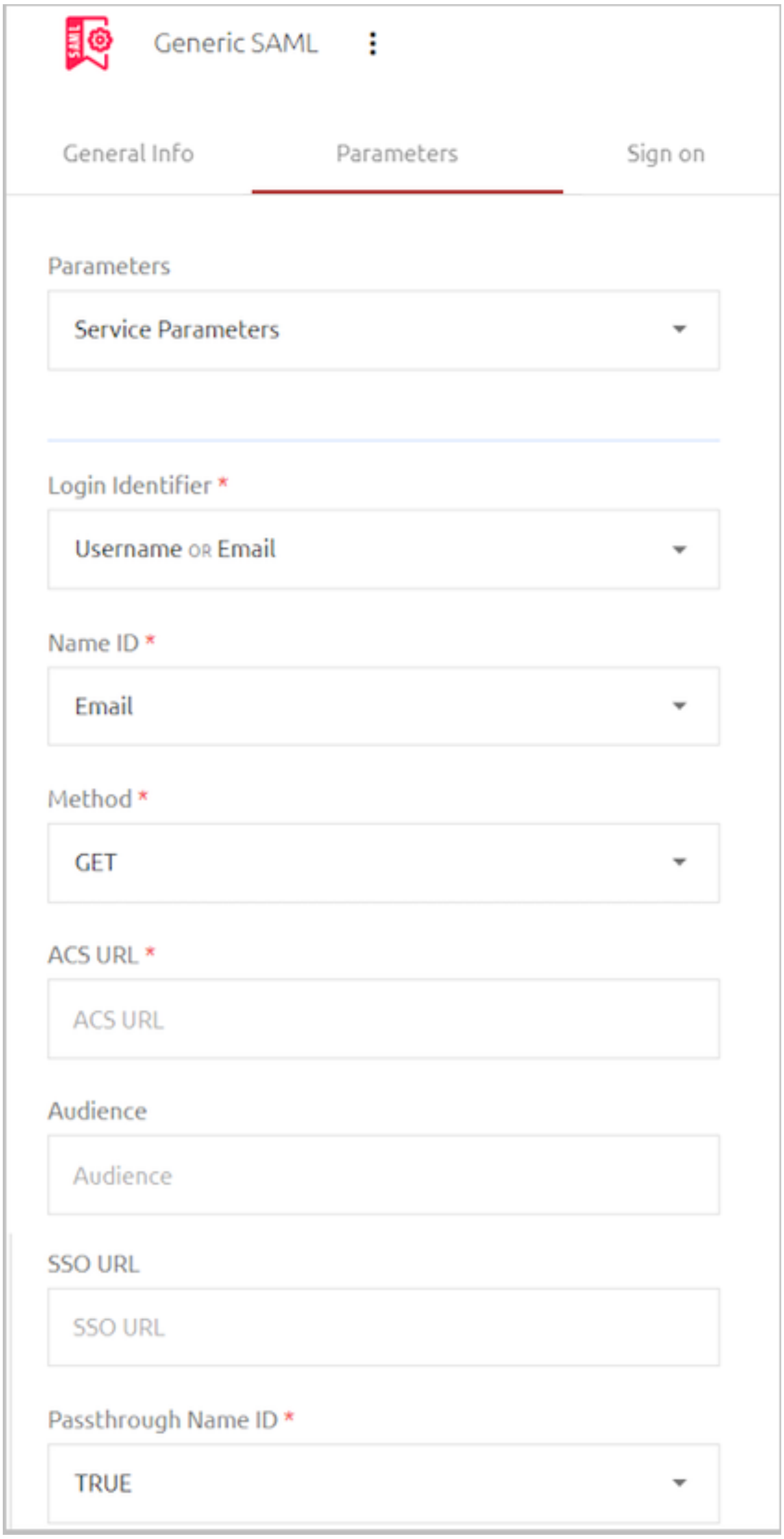
Clicking **Restore System Settings** resets all settings in the **Devices** tab to the default values defined in the **System Settings** menu. After clicking this button, confirm the action by clicking **Restore** in the verification popup. Then, click **Save**.

## Configuring Generic SAML Services

The following sections explain the parameters and sign on settings that you need to configure when adding a generic SAML service.

### Generic SAML Service Parameters

Parameters are settings of the SAML service that the Management Console requires for successful integration. To view and update these values, open the settings for the relevant SAML service and select the **Parameters** tab. Each parameter is described in the table below the figure.



Generic SAML

Parameters: Service Parameters

Login Identifier *: Username OR Email

Name ID *: Email

Method *: GET

ACS URL *: ACS URL

Audience: Audience

SSO URL: SSO URL

Passthrough Name ID *: TRUE

After updating service parameters, click **Save** (at the bottom of the tab). Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

| Parameter | Supported Values | Description / Notes |
|---|---|---|
| Login Identifier | User fields | The identifier that the user needs to enter in order to log into the SAML service (username, email, etc.). You can configure multiple identifier types to support various platforms. To specify the identifier(s), click the field and select the relevant checkbox(es). |
| Name ID | User fields | The identification that is sent to the service to identify the user in the service. When selecting a Name ID, verify that the server accepts this form of identification for user authentication. |
| Method | GET / POST | Sets the service method:<br>• **GET:** Login starts from the Octopus Login page and then authenticates to the service directly.<br>• **POST:** Involves a service redirect. The user logs into the service, and is then redirected to the Octopus Authentication Login page for authentication or MFA. |
| ACS URL | URL | The return address to the service, following successful authentication. |
| Audience | Value | A parameter used for service identification. The value will be sent to the service for additional verification that the authentication is valid and from a valid source. |
| SSO URL | URL | This URL can be set as the authentication address that users utilize to authenticate and receive the authentication request. |
| Passthrough Name ID | TRUE / FALSE | Used for getting the name ID from the SAML request (either from the subject or from the hint) and populating the Login field in our SAML Login page. |

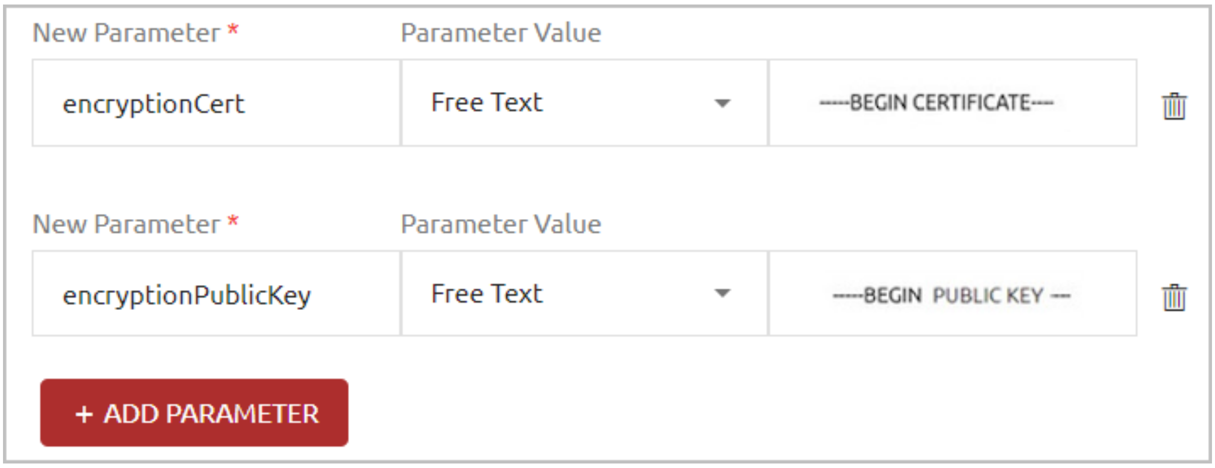
The following are optional parameters that are commonly added for generic SAML services:

| Parameter | Value | Description |
|---|---|---|
| signResponse | TRUE | Signs the SAML response sent back to the service provider. |
| nameIdentifierFormat | Free text value | The name identifier format to be sent to the service provider. |
| nameIdentifierDomain | Free text value | The domain to be used as part of the Name ID *<nameIdentifierDomain>\<nameID>* |

| Parameter | Value | Description |
|---|---|---|
| oldSAML | Free text value | When the value is set to **TRUE**, the login page for the service will be displayed in the format used for older versions. In this format, Octopus Authenticator is the only authentication method offered, and there is no option for users to change their login identifier.<br>Use the *oldSAML* parameter if you want users to authenticate with Octopus Authenticator only, or if the service does not support third party authenticators. |
| samlIssuer | Free text value | Enter the issuer text as required by the SAML service. |
| windowsFidoLogin | Any value (e.g., TRUE) | This parameter enables support of FIDO authentication to services that use older browsers or internal browsers, e.g., Office 365.<br>**Important:** When using this parameter, the **Check Password** and **Force Login Page** options (on the **Sign on** tab) need to be enabled. |
| externalSsoUrl | Free text value | When this parameter exists and users do not possess an SDO SSO token, they are immediately redirected to the URL specified in the parameter's value. The parameter supports any URL, but generally the value used is the SSO URL of an external IdP.<br>**Important:** For this parameter to function as expected, the **SSO** setting for the SAML service (in the **Sign on** tab) must be enabled. |
| altAcsUrl | URL (alternate return address to the service) | Use this parameter to route SAML requests originating from a mobile device to a dedicated ACS URL. When the parameter is set, the User-Agent header of the request is checked. If a mobile User-Agent is detected, the *altAcsUrl* value is used instead of the ACS URL defined in the Generic SAML service settings. |

The following parameters implement whole SAML assertion encryption. The encryption certificate is provided by the SP federated partner holding the private key.

| Parameter | Value |
|---|---|
| encryptionCert | PEM certificate of the SAML service |
| encryptionPublicKey | PEM formatted public key of the SAML service |



| New Parameter * | Parameter Value | |
|---|---|---|
| encryptionCert | Free Text | ----BEGIN CERTIFICATE---- |
| encryptionPublicKey | Free Text | ----BEGIN PUBLIC KEY --- |

The following parameters support sending username and password in the SAML assertion:

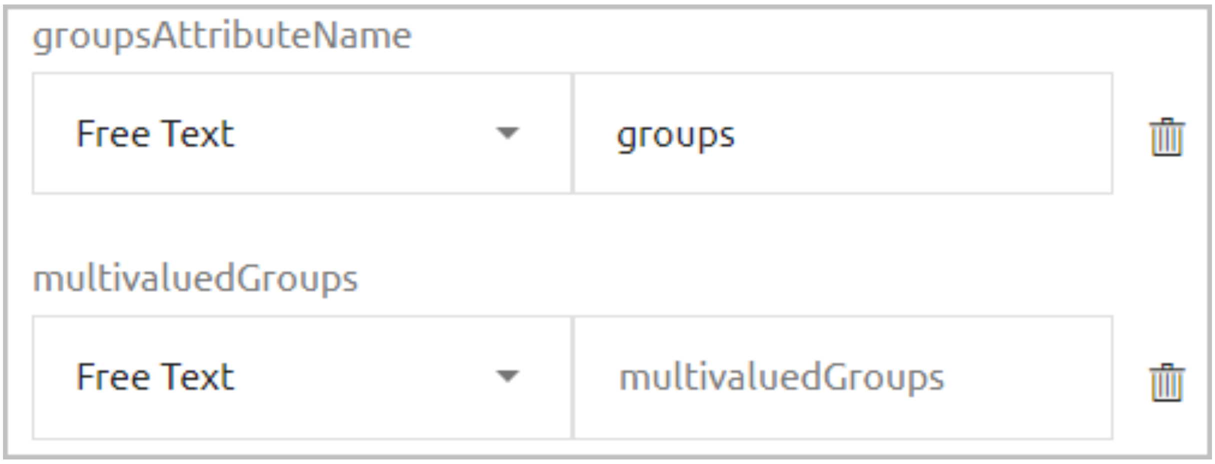
| Parameter | Value | Description |
|---|---|---|
| username | Can point to any value from the user object (username, alias, etc.) | Returns the value in the SAML assertion. |
| password | Any value | When this parameter exists, the password is sent from the vault. |
| encodePassword<br>**Note:** This parameter is relevant only when *password* is set. | Any value | When this parameter exists, the password is Base64 encoded. When the parameter is not set, the password is sent as clear text. |

The parameters below support sending user groups in the SAML assertion. When the *groupsAttributeName* parameter is defined, a list of all groups to which a user belongs is included in the assertion. The assertion contains only groups to which the user is **directly** linked (e.g., defined in the user's *memberof* attribute in LDAP), and not groups inherited recursively. For instance, if a user is a member of group G1, and G1 is a member of G2, the assertion will contain *only* G1.

| Parameter | Value | Description |
|---|---|---|
| groupsAttributeName | *roles*, *memberof*, or *groups* | Name of the attribute in the SAML schema containing a user's groups. When the parameter is set, user groups are sent as part of the SAML response. |
| multivaluedGroups | Empty or any value | This optional parameter sets the format of the SAML when you use the *groupsAttributeName* parameter. If the parameter is not defined, or if the value is empty, the format is a comma-separated string. If any value is defined, the format is multi-line. |

| Parameter | Value | Description |
|---|---|---|
| groupsFullDn | Any value | When this parameter exists, the full DN of groups is sent instead of CN. *groupsFullDn* must be used **together with** *multivaluedGroups*. Otherwise, the response will be invalid. |

The following example shows how these parameters are added to the **Parameters** tab of the relevant SAML service. Since a value is defined for the *multivaluedGroups* parameter, the SAML response will display each value in a separate line.



groupsAttributeName

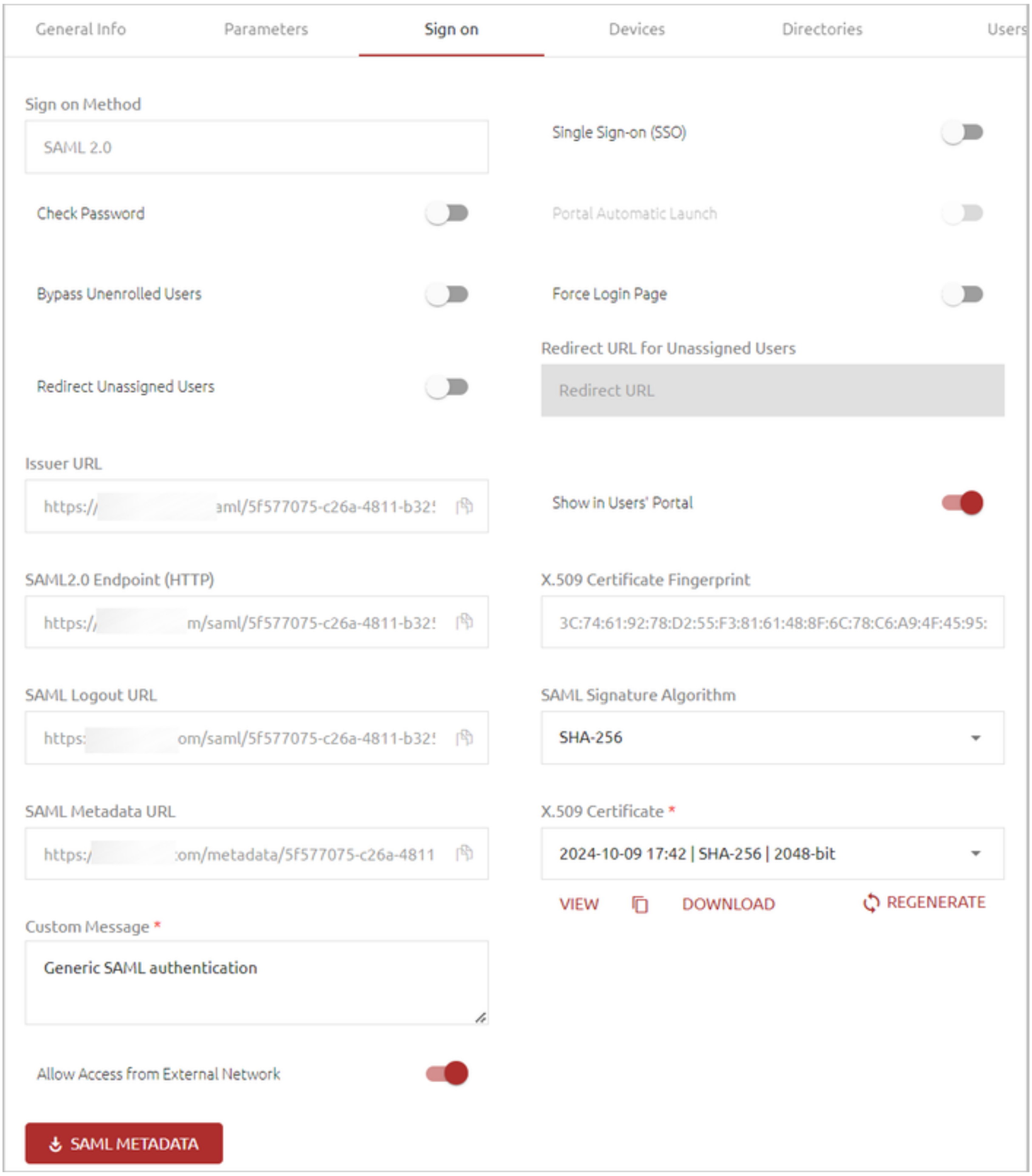
Free Text ▾ groups

multivaluedGroups

Free Text ▾ multivaluedGroups

**Generic SAML Service Sign On Settings**

The sign on settings provide information required by the SAML service protocol. To view and update this information, open the settings for the relevant SAML service and select the **Sign on** tab. The settings are described in the table below the figure.



Sign on Method: SAML 2.0

Single Sign-on (SSO): off

Check Password: off

Portal Automatic Launch: off

Bypass Unenrolled Users: off

Force Login Page: off

Redirect Unassigned Users: off

Redirect URL for Unassigned Users: Redirect URL

Issuer URL: https://[redacted]aml/5f577075-c26a-4811-b32!

Show in Users' Portal: on

SAML2.0 Endpoint (HTTP): https://[redacted]m/saml/5f577075-c26a-4811-b32!

X.509 Certificate Fingerprint: 3C:74:61:92:78:D2:55:F3:81:61:48:8F:6C:78:C6:A9:4F:45:95:

SAML Logout URL: https:[redacted]om/saml/5f577075-c26a-4811-b32!

SAML Signature Algorithm: SHA-256

SAML Metadata URL: https:/[redacted]:om/metadata/5f577075-c26a-4811

X.509 Certificate *: 2024-10-09 17:42 | SHA-256 | 2048-bit

Custom Message *: Generic SAML authentication

Allow Access From External Network: on

| Setting | Description / Notes | Configurable? |
|---|---|---|
| Check Password | When enabled, a password is required for authentication (in addition to the authentication methods used by Octopus Authenticator). | Yes |
| Bypass Unenrolled Users | When enabled, users who are known to the system but have not yet enrolled a mobile device or workstation will be allowed to login with username and password (without MFA). | Yes |

| Setting | Description / Notes | Configurable? |
|---|---|---|
| Single Sign-on (SSO) | When selected, users who are currently logged into another integrated SAML service or logged into the User Portal can log into this service without having to authenticate again. | Yes |
| Portal Automatic Launch | This toggle is enabled when **SSO** is used. When the setting is selected, the SAML service will open immediately upon successful login to the User Portal.<br>The global setting you select here can be overridden for specific groups and users. For example, you can enable Automatic Launch for individual users even though the **Automatic Launch** toggle is not selected in the Sign On settings for the service. | Yes |
| Force Login Page | When selected, users will be presented with the Login page for the service, where they select an authentication method every time they login.<br>When **Force Login Page** is NOT selected (default setting), the Login page is presented on the first login to the service. Afterwards, the system recognizes users who have previously logged in and automatically authenticates them based on information stored in the browser. (Users who want to change their authentication method can clear browser data by selecting the **Clear Authenticator Preferences** self-service option in the User Portal.)<br>**Note:** The **Force Login Page** setting is disabled when **Single Sign-on (SSO)** is selected. | Yes |
| Redirect Unassigned Users | When enabled, users not assigned to the service can access the service via an alternate URL. After enabling the setting, enter the Redirect URL in the field to the right.<br>**Note:** As this feature does not function as expected in legacy services, the setting should not be enabled for services that use the *oldSAML* parameter. | Yes |
| Show in User Portal | When enabled (default status), the service can be accessed from the User Portal. When this setting is disabled, the service does not appear in the Portal and users will be unable to log into the service via the Portal. | Yes |
| Sign On Method | The authentication method used for the service. | No |

| Setting | Description / Notes | Configurable? |
|---|---|---|
| Issuer URL | The URL used by the service to connect to Octopus Authenticator. To copy the URL (e.g., in order to paste it into the Admin Console of the SAML service), click the Copy icon. | No |
| SAML2.0 Endpoint (HTTP) | The URL used by the service for SAML protocol communications. | No |
| SAML Logout URL | The URL to which users are redirected when they log out of the service. | No |
| X.509 Certificate Fingerprint | The calculated fingerprint of the generated X.509 certificate. | No |
| SAML Signature Algorithm | The signature of the generated X.509 certificate. Select **SHA-256** (default) or **SHA-1**.<br>**Note:** SHA-1 is not supported for Red Hat Enterprise Linux 9.3. | Yes |
| X.509 Certificate | The public certificate used by the service to authenticate with Octopus Authenticator. The following options are available:<br>• Click **View** to display the content of the certificate in a popup window. The popup provides both Copy and Download options.<br>• Click **Download** to download the certificate as a .PEM file that can be used by the service.<br>• Click **Regenerate** to replace the certificate. You will be prompted to select the signature algorithm and size (1024 or 2048) before regenerating. | Yes |
| SAML Metadata URL | Provides a link to the XML file containing the metadata for the service. To copy the link, click the Copy icon. | No |
| Custom Message | The message displayed to the user upon successful authentication. Enter the text of your choice in the field.. | Yes |
| Allow access from external network | When enabled (default setting), users may authenticate via networks outside of the organization (e.g., from home).<br>**Note:** An Authentication Server in the DMZ is required for this feature to be supported. For details about adding a DMZ Server to your environment, refer to the Octopus Authentication Server Installation Guide. | Yes |

Clicking **SAML METADATA** opens a new tab displaying all data configured for the service in an XML file format.

After updating settings, click **Save** (at the bottom of the tab). Then, from the toolbar, click **PUBLISH** and publish your changes.

**Important**

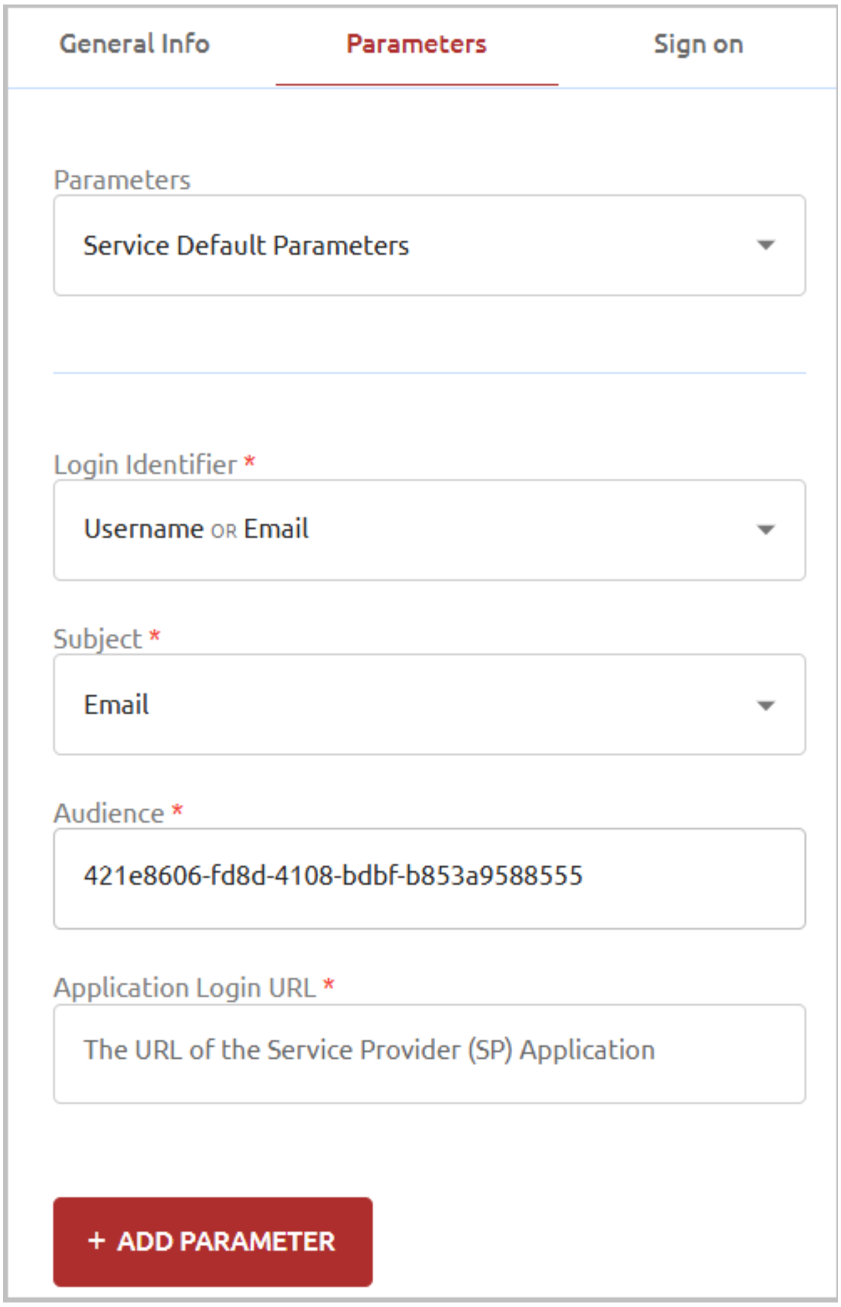
For enhanced security, SAML service URLs (Issuer URL, Endpoint URL, etc.) in Octopus Authentication Server versions 5.0 and higher contain randomly generated UUIDs, instead of the service numbers used in previous versions. Services in new installations of Version 5.0 and higher will automatically use the new URL format. However, upgrades to these versions (from versions lower than 5.0) will preserve the original URL format, to avoid interruptions in workflow. After upgrade, you can use the Clone Service action to upgrade SAML service URLs to the new syntax.

## Configuring Generic OpenID Connect Services

The following sections explain the parameters and sign on settings required for configuring a generic OpenID Connect (OIDC) service. Add this service type to enable integration with any service that supports the standard OpenID Connect protocol.

### Generic OpenID Connect Service Parameters

Parameters are settings of the OIDC service that the Management Console requires for successful integration. To view and update these values, open the settings for the relevant OIDC service and select the **Parameters** tab. Each parameter is described in the table below the figure.



Parameters: Service Default Parameters

Login Identifier *: Username OR Email

Subject *: Email

Audience *: 421e8606-fd8d-4108-bdbf-b853a9588555

Application Login URL *: The URL of the Service Provider (SP) Application

| Parameter | Description |
|---|---|
| Login Identifier | The identifier that the user needs to enter in order to log into the OIDC service (username, email, etc.). You can configure multiple identifier types to support various platforms. To specify the identifier(s), click the field and select the relevant checkbox(es). |
| Subject | The identification that is sent to the service to identify the user in the service. When selecting a Subject, verify that the server accepts this form of identification for user authentication. |
| Audience | A parameter used for service identification. The value will be sent to the service for additional verification that the authentication is valid and from a valid source. |

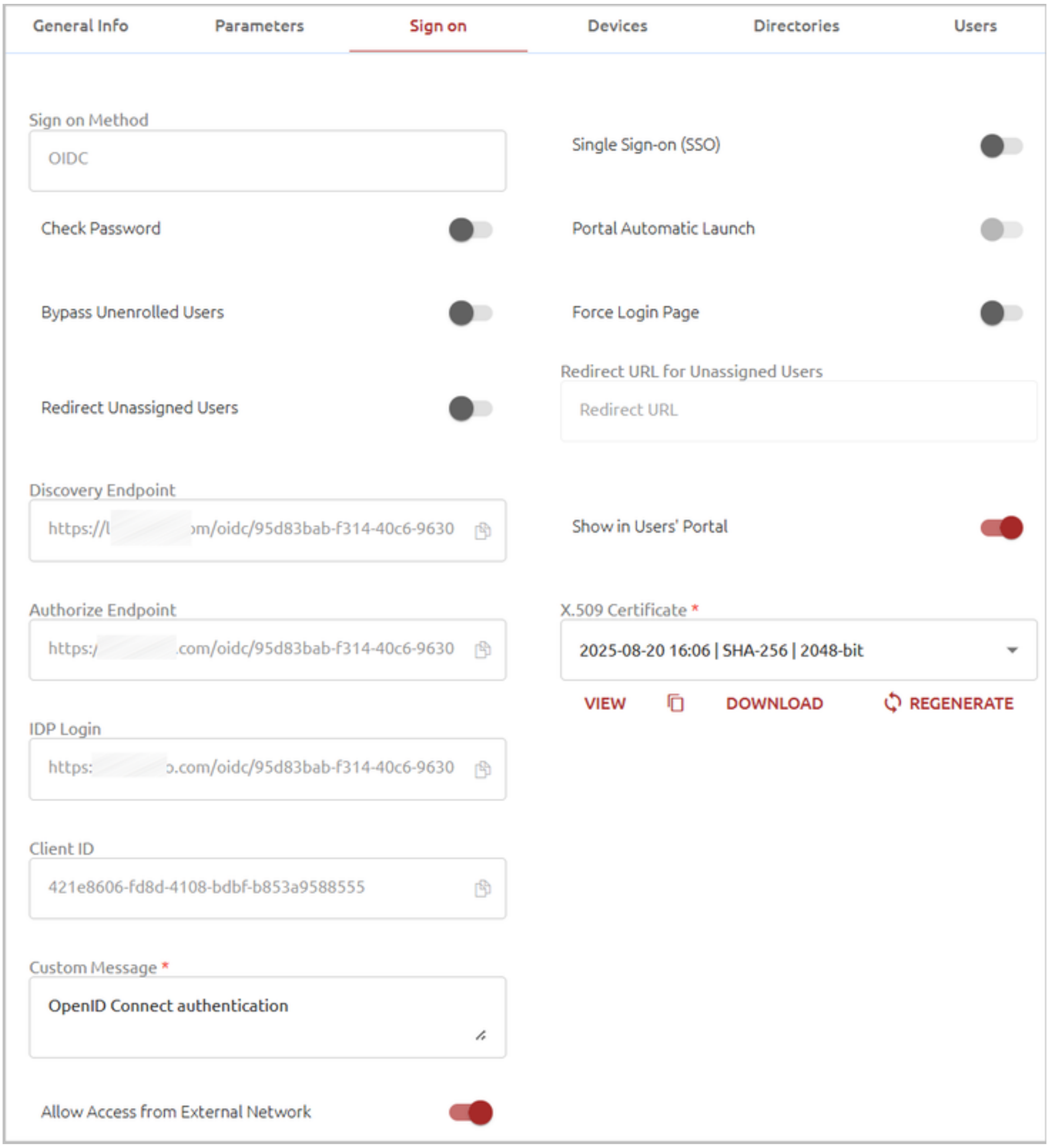
| Parameter | Description |
|---|---|
| Application Login URL | The URL to which users are directed to sign into the application. This is the login page of the Relying Party that redirects to the identity provider for authentication. |

After updating service parameters, click **Save** (at the bottom of the tab). Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

### Generic OpenID Connect Service Sign On Settings

The sign on settings provide information required by the OIDC service protocol. To view and update this information, open the settings for the relevant OIDC service and select the **Sign on** tab. The settings are described in the table below the figure.

After updating settings, click **Save** (at the bottom of the tab). Then, from the toolbar, click **PUBLISH** and publish your changes.



Sign on Method
OIDC

Check Password ○

Bypass Unenrolled Users ○

Redirect Unassigned Users ○

Discovery Endpoint
https://l[redacted]om/oidc/95d83bab-f314-40c6-9630

Authorize Endpoint
https:/[redacted].com/oidc/95d83bab-f314-40c6-9630

IDP Login
https:[redacted]o.com/oidc/95d83bab-f314-40c6-9630

Client ID
421e8606-fd8d-4108-bdbf-b853a9588555

Custom Message *
OpenID Connect authentication

Allow Access from External Network ●

Single Sign-on (SSO) ○

Portal Automatic Launch ○

Force Login Page ○

Redirect URL for Unassigned Users
Redirect URL

Show in Users' Portal ●

X.509 Certificate *
2025-08-20 16:06 | SHA-256 | 2048-bit

| Setting | Description / Notes | Configurable? |
|---|---|---|
| Sign on Method | The authentication method used for the service. | No |
| Check Password | When enabled, a password is required for authentication (in addition to the authentication methods used by Octopus Authenticator). | Yes |
| Bypass Unenrolled Users | When enabled, users who are known to the system but have not yet enrolled a mobile device or workstation will be allowed to login with username and password (without MFA). | Yes |

| Setting | Description / Notes | Configurable? |
|---|---|---|
| Single Sign-on (SSO) | When selected, users who are currently logged into another integrated OIDC service or logged into the User Portal can log into this service without having to authenticate again. | Yes |
| Portal Automatic Launch | This toggle is enabled when **SSO** is used. When the setting is selected, the service will open immediately upon successful login to the User Portal.<br>The global setting you select here can be overridden for specific groups and users. For example, you can enable Automatic Launch for individual users even though the **Automatic Launch** toggle is not selected in the Sign On settings for the service. | Yes |
| Force Login Page | When selected, users will be presented with the Login page for the service, where they select an authentication method every time they login.<br>When **Force Login Page** is NOT selected (default setting), the Login page is presented on the first login to the service. Afterwards, the system recognizes users who have previously logged in and automatically authenticates them based on information stored in the browser. (Users who want to change their authentication method can clear browser data by selecting the **Clear Authenticator Preferences** self-service option in the User Portal.)<br>**Note:** The **Force Login Page** setting is disabled when **Single Sign-on (SSO)** is selected. | Yes |
| Redirect Unassigned Users | When enabled, users not assigned to the service can access the service via an alternate URL. After enabling the setting, enter the Redirect URL in the field to the right. | Yes |
| Show in User Portal | When enabled (default status), the service can be accessed from the User Portal. When this setting is disabled, the service does not appear in the Portal and users will be unable to log into the service via the Portal. | Yes |
| Discovery Endpoint | A URL pointing to a configuration document containing metadata about the OIDC provider, including URLs for authorization, token supply, user data and more. | No |
| Authorize Endpoint | A redirect URL allowing the OIDC service to authorize use of the external identity provider for authentication. | No |

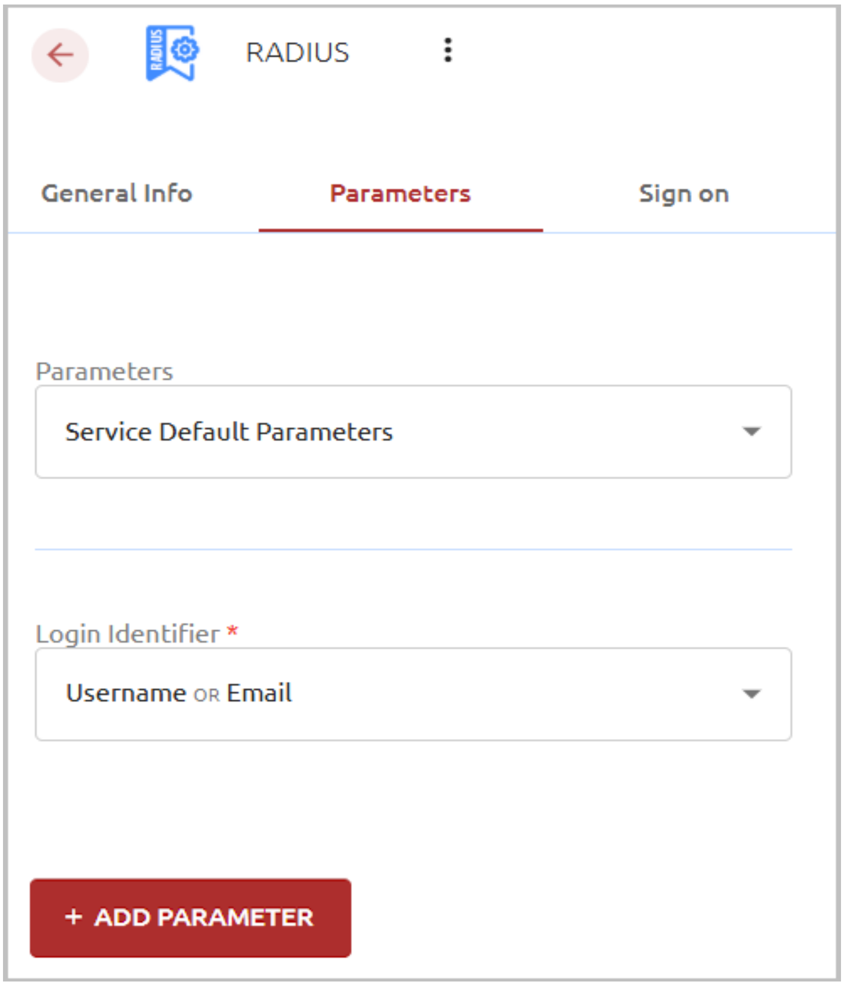
| Setting | Description / Notes | Configurable? |
|---|---|---|
| IDP Login | The URL of the Identity Provider's authentication endpoint. Users will be redirected to the IDP Login to verify identity before accessing the application. | No |
| Client ID | A unique identifier for the service called to handle the authentication request. | No |
| X.509 Certificate | The public certificate used by the service to authenticate with Octopus Authenticator. The following options are available:<br>• Click **View** to display the content of the certificate in a popup window. The popup provides both Copy and Download options.<br>• Click **Download** to download the certificate as a .PEM file that can be used by the service.<br>• Click **Regenerate** to replace the certificate. You will be prompted to select the signature algorithm and size (1024 or 2048) before regenerating. | Yes |
| Custom Message | The message displayed to the user upon successful authentication. Enter the text of your choice in the field.. | Yes |
| Allow Access from External Network | When enabled (default setting), users may authenticate via networks outside of the organization (e.g., from home).<br>**Note:** An Authentication Server in the DMZ is required for this feature to be supported. For details about adding a DMZ Server to your environment, refer to the Octopus Authentication Server Installation Guide. | Yes |

## Configuring RADIUS Services

The following sections explain the parameters and sign on settings that you need to configure when adding a RADIUS service.

### RADIUS Parameters

Parameters are settings of the RADIUS service that the Management Console requires for successful integration. To view and update these values, open the settings for the relevant RADIUS service and select the **Parameters** tab.

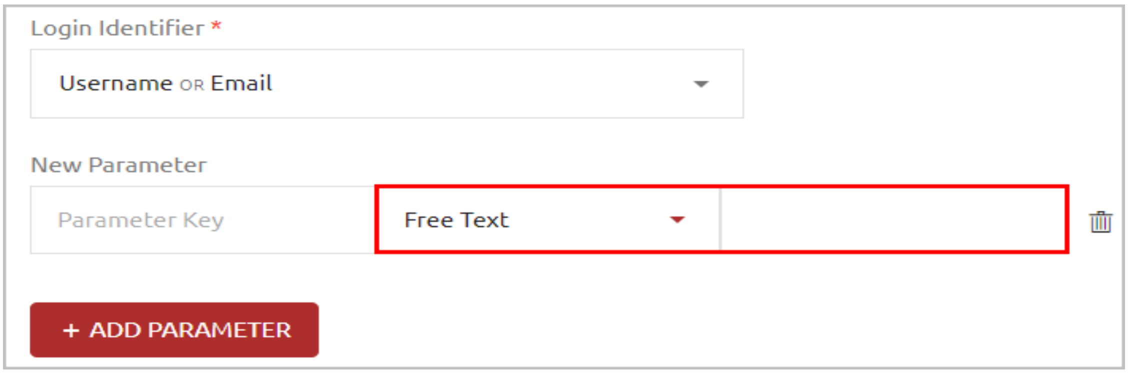


Parameters
Service Default Parameters

Login Identifier *
Username OR Email

The **Login Identifier** is the identifier that the user needs to enter in order to log into the RADIUS service (email, username, etc.). You can configure multiple identifier types to support various platforms. To specify the identifier(s), open the list and select the relevant checkbox(es).

To define additional parameters that are not included in the generic template, click **Add Parameter**. Then, enter the name of the parameter key and select its value from the dropdown list. If you select the **Free Text** option, an additional field opens where you can enter the required value(s).



Login Identifier *
Username OR Email

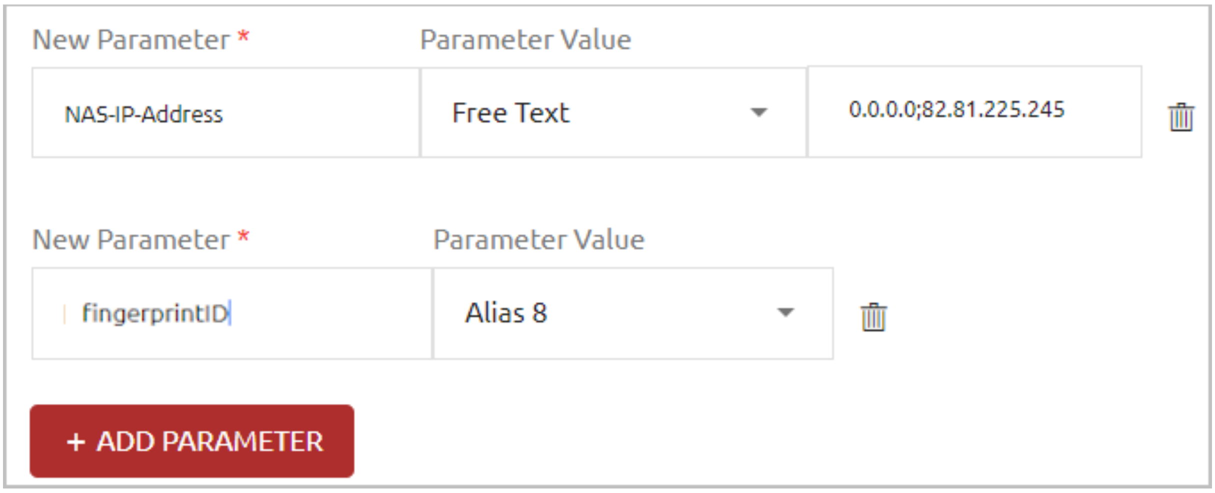
New Parameter
Parameter Key
Free Text

The following additional parameter is commonly configured for RADIUS services:

| Parameter | Value | Description / Notes |
|---|---|---|
| NAS-IP-Address | Free text | The IP of the RADIUS server. To support multiple clients, you can enter several semicolon-separated values, e.g., *0.0.0.0;82.81.225.245* |

**Important**

When multiple values are specified within a single parameter, the values have an *OR* relationship. However, multiple parameters are handled with *AND* logic, so all parameters must be matched for successful authentication. In the example below, the RADIUS client needs to send one of the specified IP addresses as well as a matching fingerprint.

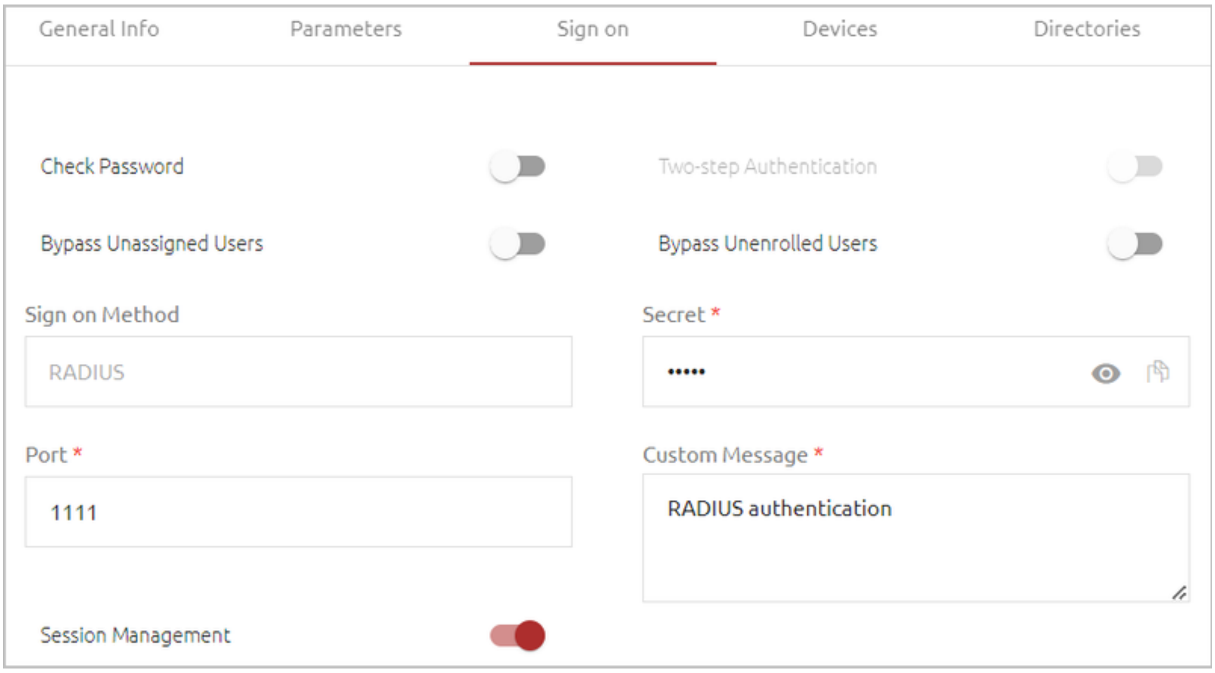


| New Parameter * | Parameter Value | |
|---|---|---|
| NAS-IP-Address | Free Text | 0.0.0.0;82.81.225.245 |
| fingerprintID | Alias 8 | |

After adding or updating parameters, click **Save**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

**RADIUS Sign On Settings**

The sign on settings provide information required by the RADIUS service protocol. To view and update this information, open the settings for the relevant RADIUS service and select the **Sign on** tab. The settings are described in the table below the figure.



Check Password

Two-step Authentication

Bypass Unassigned Users

Bypass Unenrolled Users

Sign on Method: RADIUS

Secret *: •••••

Port *: 1111

Custom Message *: RADIUS authentication

Session Management

| Setting | Description / Notes |
|---|---|
| Check Password | When enabled, users are required to enter a password for MFA authentication. |
| Two-step Authentication | This setting is used to support Adaptive Authentication for login to the RADIUS service. When enabled, users are required to enter the verification code that is generated and displayed in the mobile app after they have approved the push authentication request.<br>**Note:** Adaptive Authentication for RADIUS services is not necessary for FIDO and bypassed users, as they routinely need to provide an accesss token in order to authenticate. Users working with a FIDO key receive the temporary token to enter using the Systray Retrieve Credentials function. Bypassed users should authenticate with the usual bypass token mechanism. |
| Bypass Unassigned Users | When enabled, users who are not assigned to the service will be allowed to login with username and password (without MFA). By default, this option is disabled, and unrecognized users are refused authentication. Bypass Unassigned Users is generally used on a temporary basis only, during gradual rollouts of Octopus Authenticator. |
| Bypass Unenrolled Users | When enabled, users who are known to the system but have not yet enrolled a mobile device or workstation will be allowed to login with username and password (without MFA). |

| Setting | Description / Notes |
|---|---|
| Secret | The RADIUS secret key required for communication between the RADIUS service and Octopus Authenticator.<br>To copy the secret (e.g., in order to paste it in the Admin Console of the RADIUS service), click the Copy icon. Click the Eye icon to unmask and mask the secret. |
| Port | Port used for communication with the RADIUS server. |
| Custom Message | Message displayed to the user upon successful authentication. Enter the text of your choice in the field. |
| Session Management | When enabled, multiple authorization requests for a single authorization are ignored. |

After updating settings, click **Save**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

### External Service Configuration

An Octopus Authentication RADIUS service replaces the direct connection to the RADIUS Server, and performs Octopus Authentication instead of the legacy Username and Password authentication. To redirect authentication requests to the Octopus Server, make the following change in your external RADIUS service configuration:

- Replace the RADIUS Server URL with *<EnterpriseBaseURL>:<port>*
  - **Enterprise Base URL:** The address of the Octopus Authentication Server (or the load balancer in distributed deployments). The URL is displayed in the Management Console under **System Settings > General Settings**.
  - **Port:** The port defined in the **Sign on** tab of the Octopus RADIUS service.

## Configuring REST API Services

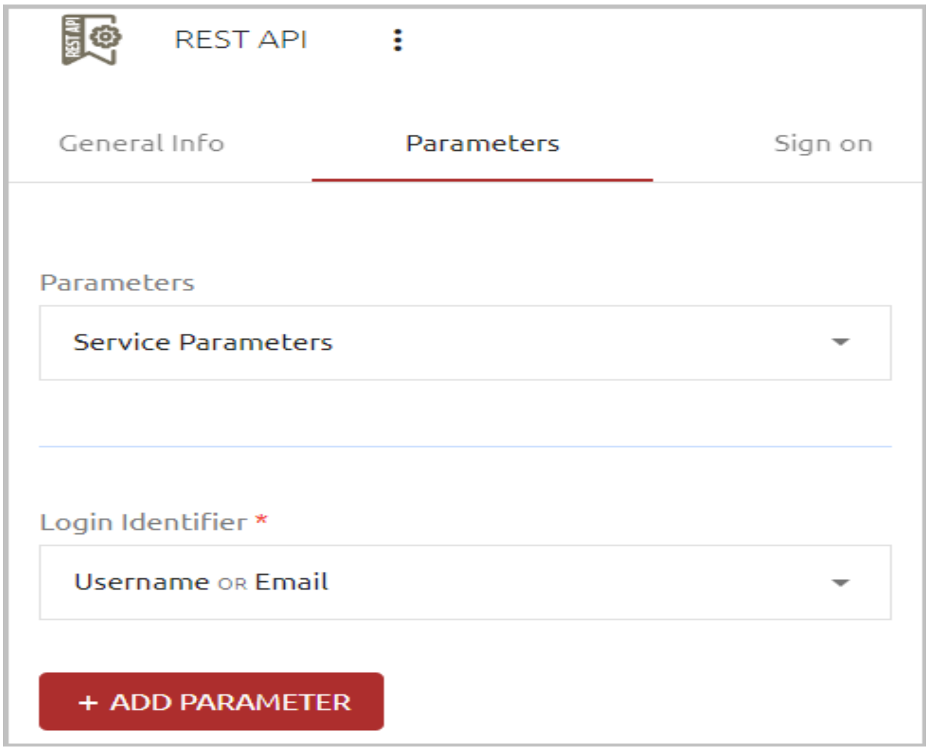
The following sections explain the parameters and sign on settings that you need to configure when adding a REST API service.

### REST API Service Parameters

Parameters are settings of the REST API service that the Management Console requires for successful integration.

**To view and update REST API service parameters:**

1. Open the settings for the relevant REST API service and select the **Parameters** tab.



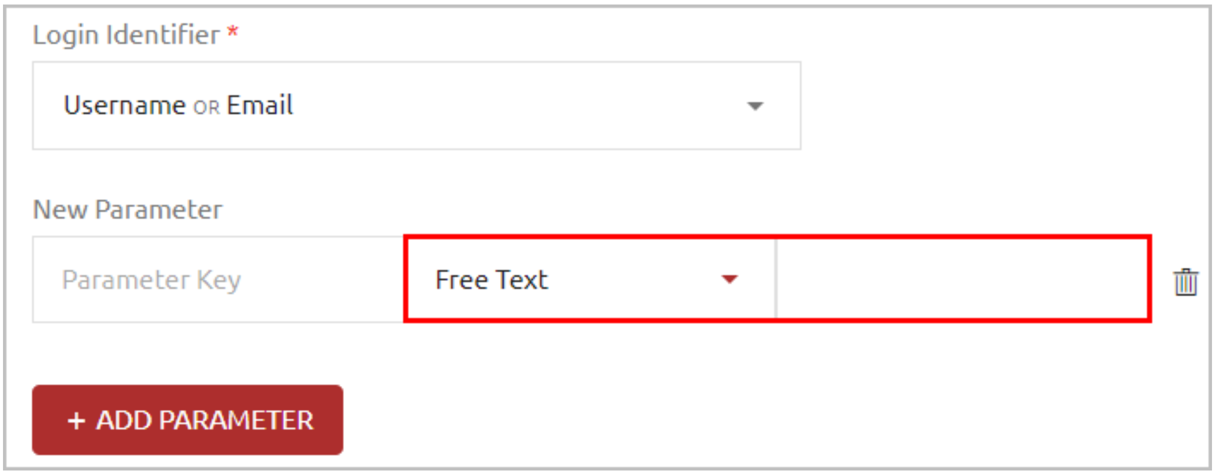
Parameters: Service Parameters

Login Identifier *: Username OR Email

2. The **Login Identifier** is the identifier that the user needs to enter in order to log into the REST API service (username, email, etc.). You can configure multiple identifier types to support various platforms. To specify the identifier(s), open the list and select the relevant checkbox(es).

3. To define additional parameters that are not included in the generic template, click **Add Parameter**. Then, enter the name of the parameter key and select its value from the dropdown list.

   If you select the **Free Text** option, an additional field opens where you can enter the required value(s).



Login Identifier *: Username OR Email

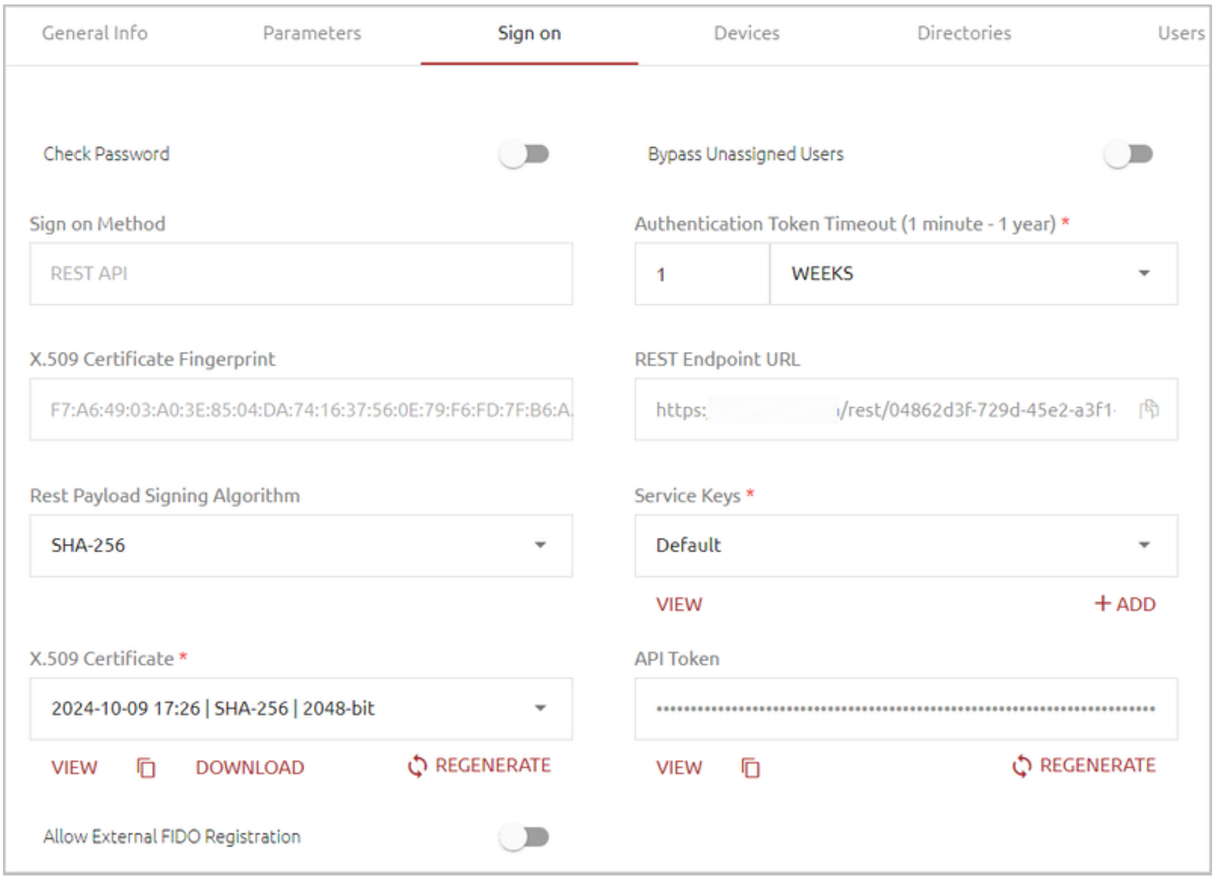
New Parameter: Free Text

4. Click **Save.** Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

### REST API Service Sign On Settings

The Sign On settings provide information required by the REST API service protocol. To view and update this information, open the settings for the relevant REST API service and select the **Sign On** tab. The settings are described in the table below the figure.

After updating settings, scroll to the bottom of the tab and click **Save**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.



Check Password

Bypass Unassigned Users

Sign on Method: REST API

Authentication Token Timeout (1 minute - 1 year) *: 1 WEEKS

X.509 Certificate Fingerprint: F7:A6:49:03:A0:3E:85:04:DA:74:16:37:56:0E:79:F6:FD:7F:B6:A

REST Endpoint URL: https:[redacted]/rest/04862d3f-729d-45e2-a3f1-

Rest Payload Signing Algorithm: SHA-256

Service Keys *: Default

X.509 Certificate *: 2024-10-09 17:26 | SHA-256 | 2048-bit

API Token: ••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••

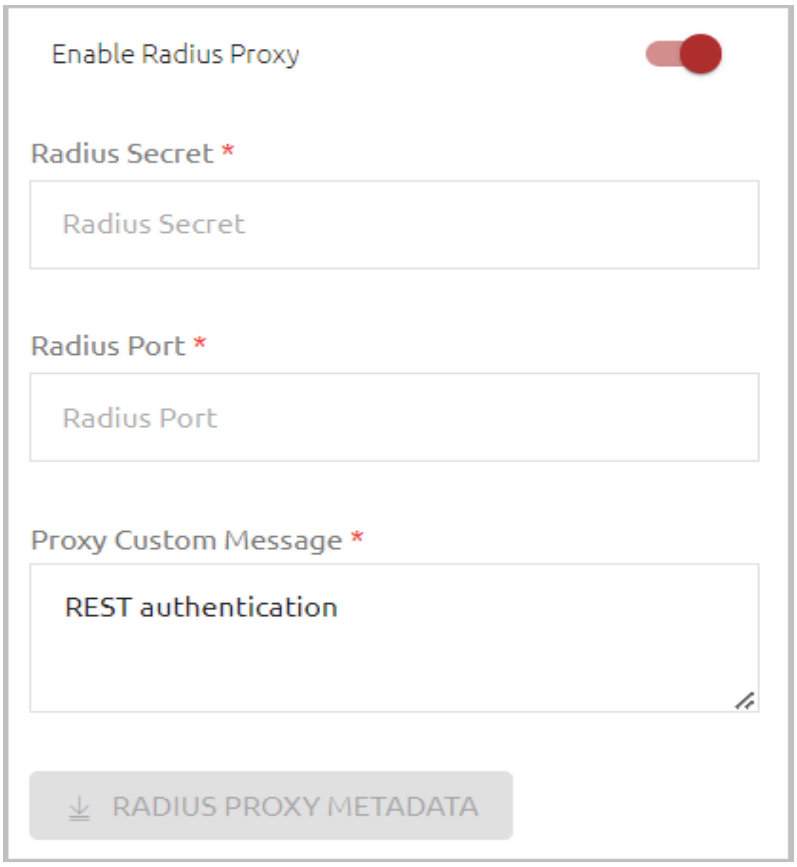
Allow External FIDO Registration

| Setting | Description / Notes | Configurable? |
|---|---|---|
| Check Password | When enabled, a password is required for authentication (in addition to the authentication methods used by Octopus Authenticator) | Yes |
| Bypass Unassigned Users | When this toggle is enabled, users who are not assigned to the service will be allowed to login with username and password (without MFA). By default, this option is disabled, and unrecognized users are refused authentication. Bypass Unassigned Users is generally used on a temporary basis only, during gradual rollouts of Octopus Authenticator. | Yes |
| Sign On Method | The authentication method used for the service. | No |
| X.509 Certificate Fingerprint | The calculated fingerprint of the generated X.509 certificate. | No |

| Setting | Description / Notes | Configurable? |
|---|---|---|
| Rest Payload Signing Algorithm | The signature of the generated X.509 certificate. Select **SHA-1** or **SHA-256**.<br>**Note:** SHA-1 is not supported for Red Hat Enterprise Linux 9.3. | Yes |
| X.509 Certificate | The public certificate used by the service to authenticate with Octopus Authenticator. The following options are available:<br>• Click **View** to display the content of the certificate in a popup window. The popup provides both Copy and Download options.<br>• Click **Download** to download the certificate as a .PEM file that can be used by the service.<br>• Click **Regenerate** to replace the certificate. You will be prompted to select the signature algorithm and size (1024 or 2048) before regenerating. | Yes |
| Authentication token timeout | The time period after which the REST authentication token becomes invalid. The value can range from one minute to one year. | Yes |
| REST Endpoint URL | The URL used by the service for REST protocol communications. To copy the URL (e.g., in order to paste it into the Admin Console of the REST service), click the Copy icon. | No |
| Service Keys | The key(s) used by the service to authenticate with Octopus Authenticator. The following options are available:<br>• Click **View** to open a popup from which you can view and copy all active service keys.<br>• Click **Add** to create a new service key.<br>For more information, refer to Working with Service Keys. | Yes |
| API Token | The token used for an authentication request. The following options are available:<br>• Click **View** to display the content of the token in a popup window. The **Copy** button lets you easily copy the content.<br>• Click **Regenerate** to replace the token. | Yes |

### Using the RADIUS Proxy

Using a RADIUS proxy enables secure transport of a RADIUS service over an untrusted network. If you use the Windows RADIUS Agent, there is no need for any further proxy configuration. For legacy configurations, it is recommended to deploy the Octopus RADIUS proxy by configuring the relevant settings in the **Sign on** tab of the REST API service and installing a RADIUS proxy component.



Enable Radius Proxy

Radius Secret *

Radius Secret

Radius Port *

Radius Port

Proxy Custom Message *

REST authentication

The settings are:

- **Enable Radius Proxy:** Enables/Disables the RADIUS proxy.
- **Radius Secret:** The secret used to connect to the RADIUS proxy.
- **Radius Port:** The port number used for RADIUS proxy communication.
- **Proxy Custom Message:** The message displayed to the user upon successful authentication.

When all the settings have been configured, the **Radius Proxy Metadata** button is enabled. Clicking this button downloads the proxy data in a JSON file format that can be used for installation of the proxy component.

## Configuring LDAP Services

An Octopus Authentication LDAP service replaces the direct connection to the LDAP Repository Server, and performs Octopus Authentication instead of the legacy Username and Password authentication. (Octopus Authentication can also be used as MFA).

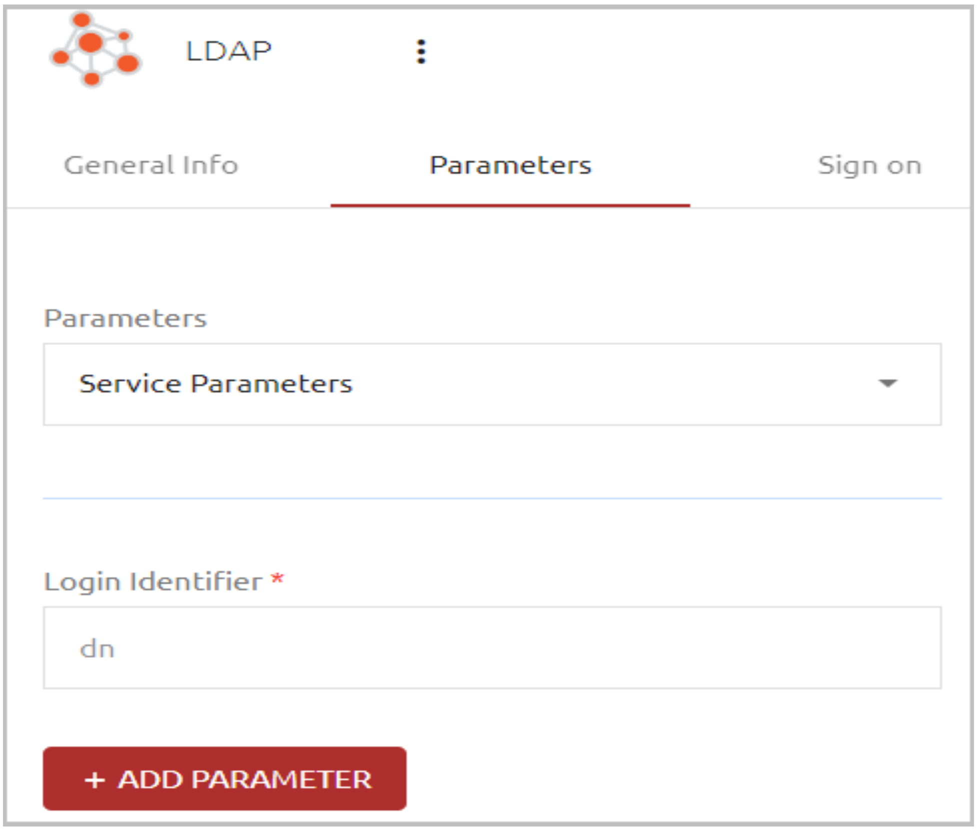
The following sections describe the parameters and sign on settings for the Octopus LDAP service, and explain how to configure your external LDAP service for successful integration with the Octopus Server.

### LDAP Parameters

Parameters are settings of the LDAP service that the Management Console requires for successful integration.

**To view and update LDAP service parameters:**

1. Open the settings for the relevant LDAP service and select the **Parameters** tab.



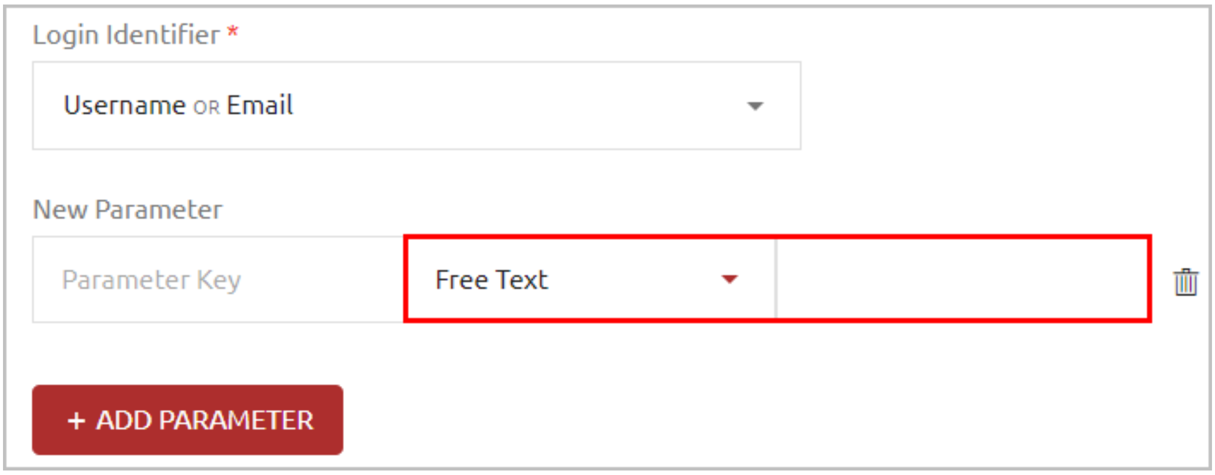
Parameters: Service Parameters

Login Identifier *: dn

2. The **Login Identifier** is the login method to the LDAP Repository (Principle's Username or DN). This parameter is not editable.

3. To define additional parameters, click **Add Parameter**. Then, enter the name of the parameter key and select its value from the dropdown list.

   If you select the **Free Text** option, an additional field opens where you can enter the required value(s).



Login Identifier *

Username OR Email

New Parameter

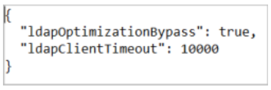
4. Click **Save.** Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

### Configuring Optional Client Connection Parameters

Enterprise Connect Passwordless offers optional parameters that can be manually set in the Authentication Server configuration file to avoid dead or stale LDAP connections and help ensure rapid response times for password operations (e.g., Set Password, Verify Password) over LDAP. Configure these parameters only if you need to reset the LDAP connection timeout or you do not want the same LDAP client to be used for multiple operations. The parameters are:

| Parameter | Default Value | Description | Example |
|---|---|---|---|
| ldapOptimizationBypass | false | When set to *true*, a new LDAP client is created for each password operation. | ldapOptimizationBypass: true |
| ldapClientTimeout<br>**Note:** This parameter is relevant only when ldapOptimizationBypass is set to *false*. | 5000 | Determines the time (in milliseconds) for which the LDAP connection remains open. When the timeout elapses, the connection is closed, a new client is created and the operation is performed again on the new client. | ldapClientTimeout: 5000 |

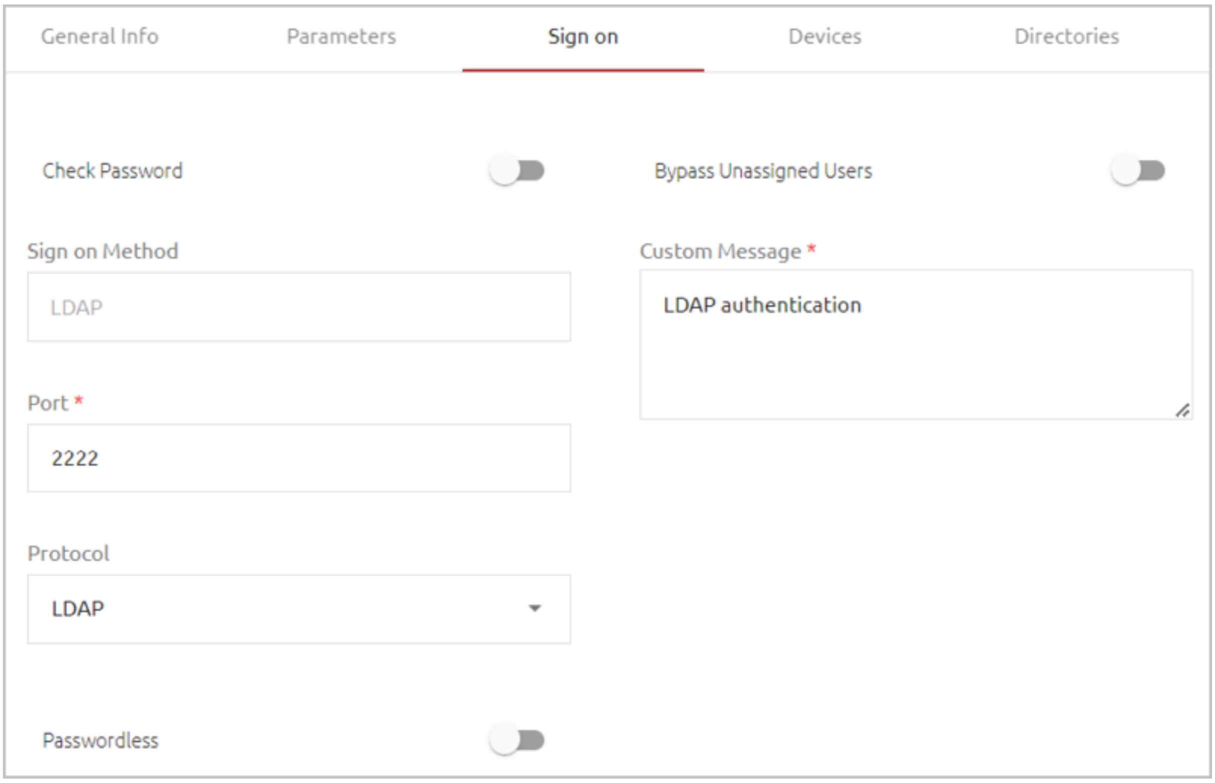
Update the default values by editing the **/opt/sdo/authserver/config/prod.json** file. For example:



```
{
  "ldapOptimizationBypass": true,
  "ldapClientTimeout": 10000
}
```

### LDAP Sign On Settings

The sign on settings provide information required by the LDAP service protocol. To view and update this information, open the settings for the relevant LDAP service and select the **Sign on** tab. The settings are described in the table below the figure.



Check Password

Bypass Unassigned Users

Sign on Method: LDAP

Custom Message *: LDAP authentication

Port *: 2222

Protocol: LDAP

Passwordless

| Setting | Description / Notes |
|---|---|
| Check Password | When enabled, users are required to enter a password for MFA authentication. |
| Bypass Unassigned Users | When enabled, users who are not assigned to the service will be allowed to login with username and password (without MFA). By default, this option is disabled, and unrecognized users are refused authentication. Bypass Unassigned Users is generally used on a temporary basis only, during gradual rollouts of Octopus Authenticator. |
| Port | Enter the port used for communication with the LDAP server. Make sure the port number matches the service provider's LDAP port number. |
| Protocol | Select LDAP or LDAPS. |
| Passwordless | When enabled, the user's password on the AD is rotated transparently, allowing passwordless authentication to all integrated services. |
| Custom Message | The message displayed to users upon successful authentication. |

After updating settings, click **Save**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

### External LDAP Service Configuration

To ensure successful integration with the Octopus LDAP service, you need to configure your corresponding external LDAP service as follows:

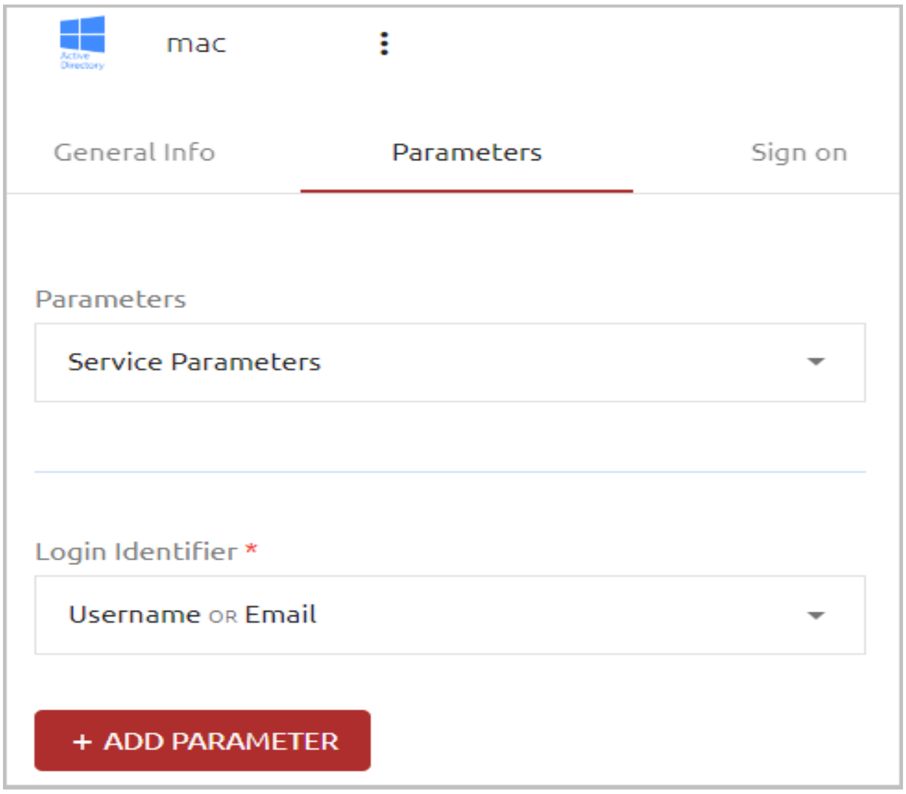
1. To redirect authentication requests to the Octopus Server, replace the LDAP Repository URL with *<EnterpriseBaseURL>:<port>*
   - **Enterprise Base URL:** The address of the Octopus Authentication Server (or the load balancer in distributed deployments). The URL is displayed in the Management Console under **System Settings > General Settings**.
   - **Port:** The port defined in the **Sign on** tab of the Octopus LDAP service.
2. The Admin Name and Password for the service should match the values defined for the integrated directory configured in the Management Console. (These values are displayed in the **Details** tab of the directory settings.)
3. The Base DN for the service should be at the same level (or lower) in the hierarchy defined in the integrated directory, so the search will focus on the same DN.

## Configuring Active Directory Authentication Services

The following sections explain the parameters and sign on settings that you need to configure when adding an Active Directory Authentication service.

### AD Authentication Service Parameters

Parameters are settings of the Active Directory that the Management Console requires for successful integration. To view and update these values, open the settings for the relevant AD Authentication service and select the **Parameters** tab.



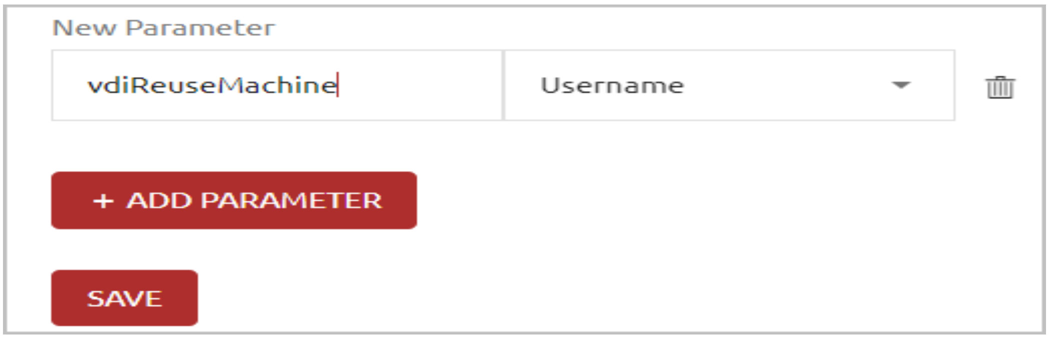
Parameters: Service Parameters

Login Identifier *: Username OR Email

The **Login Identifier** is the identifier that the user needs to enter in order to log into the AD Authentication service (e.g., Username). You can configure multiple identifier types to support various platforms. To specify the identifier(s), open the list and select the relevant checkbox(es).

To define additional parameters, click **Add Parameter**. When working with a temporary virtual machine and Adaptive Authentication is enabled, you can add the following optional parameter:

| Parameter Name | Value | Description |
|---|---|---|
| vdiReuseMachine | Any value, or the value can be blank | When the parameter exists, workstation information (along with the public key) is not saved, and Adaptive Authentication is disabled. |



New Parameter: vdiReuseMachine | Username

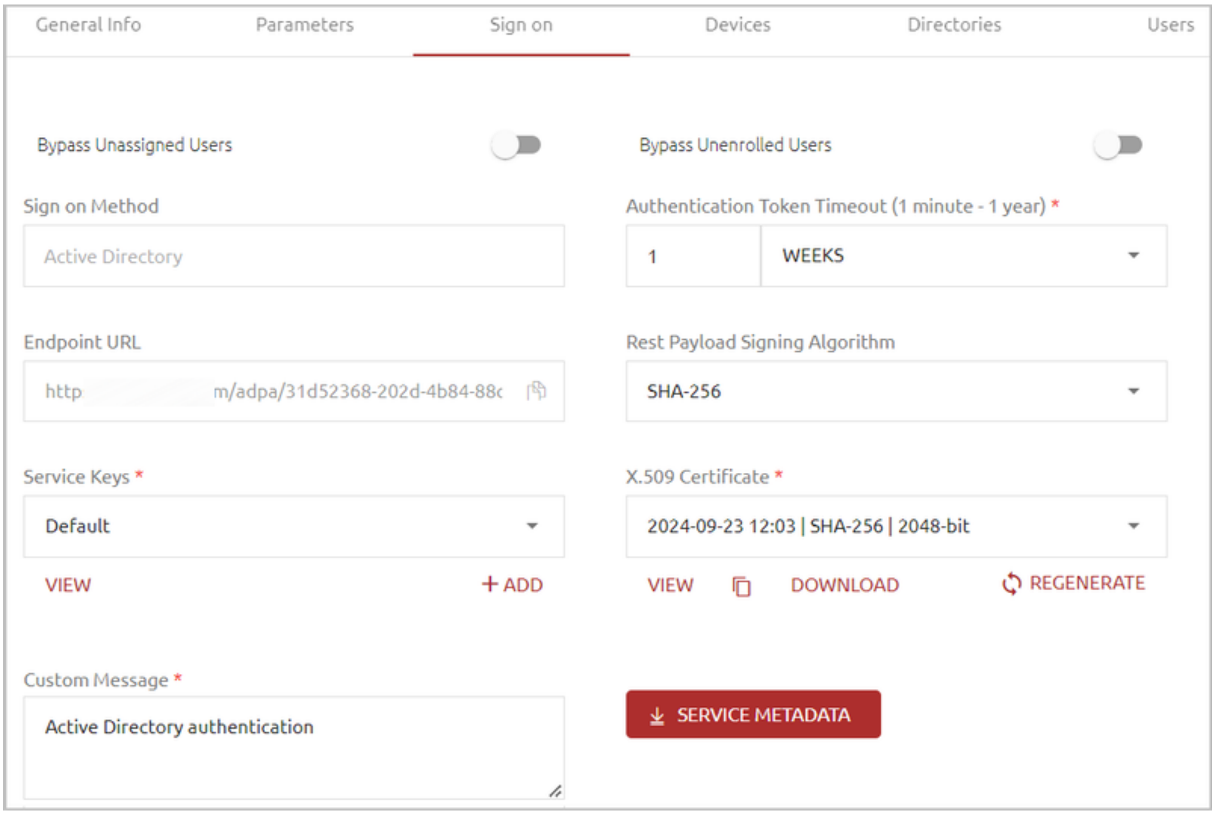
After updating settings or adding parameters, click **Save**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

### AD Authentication Service Sign On Settings

The sign on settings provide data required by the AD Authentication service for user authentication on the workstation. Settings configured in this tab can affect the user experience when authenticating to the workstation. For example, you may decide to allow users who are not enrolled with Octopus to continue to authenticate with Username + Password.

To view and update this type of data, open the settings for the relevant AD Authentication service and select the **Sign on** tab. The settings are described in the table below.

After updating settings, scroll to the bottom of the tab and click **Save**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.



Bypass Unassigned Users

Bypass Unenrolled Users

Sign on Method: Active Directory

Authentication Token Timeout (1 minute - 1 year) *: 1 WEEKS

Endpoint URL: http[redacted]m/adpa/31d52368-202d-4b84-88c

Rest Payload Signing Algorithm: SHA-256

Service Keys *: Default

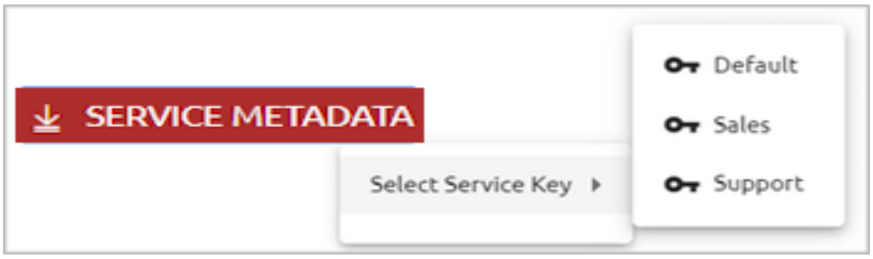
X.509 Certificate *: 2024-09-23 12:03 | SHA-256 | 2048-bit

Custom Message *: Active Directory authentication

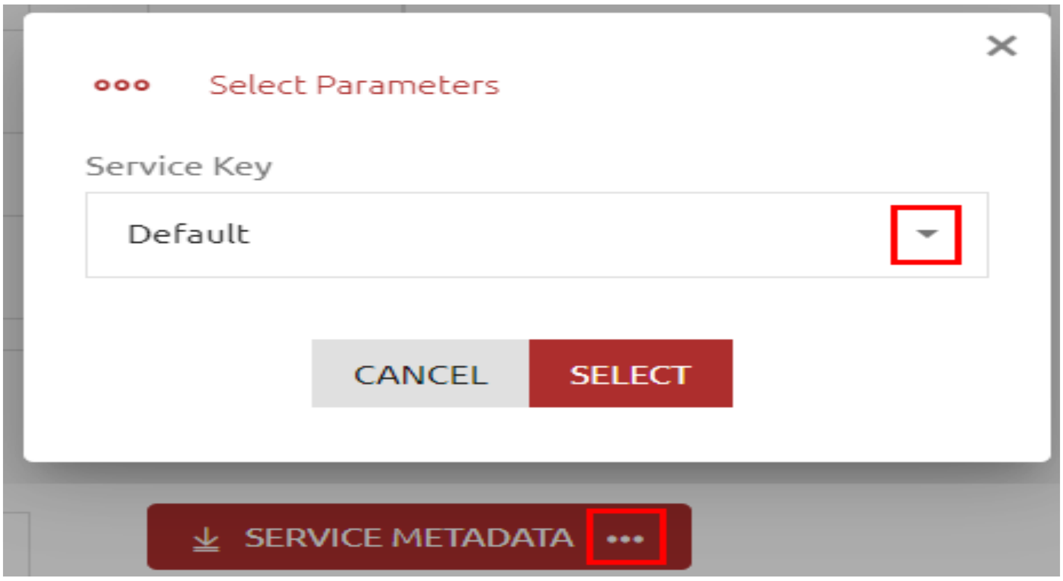
| Setting | Description / Notes | Configurable? |
|---|---|---|
| Bypass Unassigned Users | When this toggle is enabled, users who are not assigned to the service will be allowed to login with username and password (without MFA). By default, this option is disabled, and unrecognized users are refused authentication. Bypass Unassigned Users is generally used on a temporary basis only, during gradual rollouts of Octopus Authenticator. | Yes |
| Bypass Unenrolled Users | When enabled, users who are known to the system but have not yet enrolled a mobile device or workstation will be allowed to login with username and password (without MFA). | Yes |

| Setting | Description / Notes | Configurable? |
|---|---|---|
| Sign On Method | The authentication method used for the service. | No |
| Endpoint URL | The access URL from the AD client to the Octopus Authentication server. To copy the URL (e.g., in order to paste it into the Admin Console of the AD service), click the Copy icon. | No |
| Service Keys | The key(s) used by the service to authenticate with Octopus Authenticator. The following options are available:<br>• Click **View** to open a popup from which you can view and copy all active service keys.<br>• Click **Add** to create a new service key.<br>For more information, refer to Working with Service Keys. | Yes |
| Authentication token timeout | The time period after which the authentication token becomes invalid. The value can range from one minute to one year. | Yes |
| Rest Payload Signing Algorithm | The signature of the generated X.509 certificate. Select **SHA-1** or **SHA-256**.<br>**Note:** SHA-1 is not supported for Red Hat Enterprise Linux 9.3. | Yes |
| X.509 Certificate | The public certificate used by the service to authenticate with Octopus Authenticator. The following options are available:<br>• Click **View** to display the content of the certificate in a popup window. The popup provides both Copy and Download options.<br>• Click **Download** to download the certificate as a .PEM file that can be used by the service.<br>• Click **Regenerate** to replace the certificate. You will be prompted to select the signature algorithm and size (1024 or 2048) before regenerating. | Yes |
| Custom Message | The message shown to users upon successful authentication. | Yes |

Clicking **Service Metadata** downloads all data configured for the service to a file format (XML) that can be used by the Active Directory. If there are multiple active service keys, you will be prompted to select the key to be included in the file.



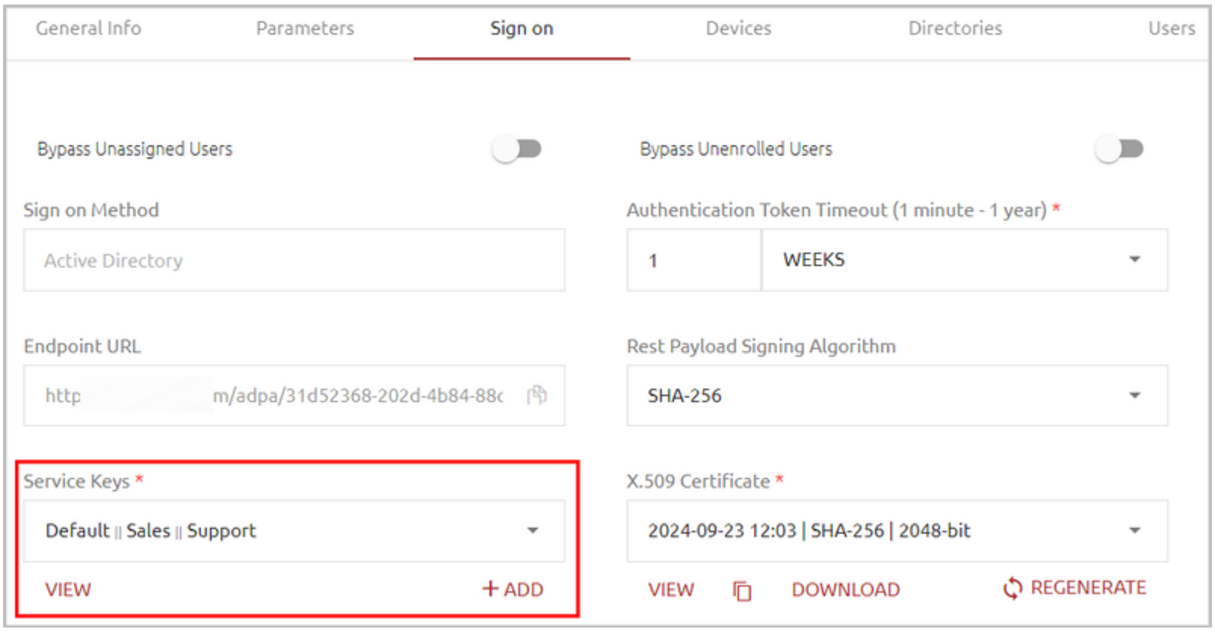
If more than one client certificate has been configured in the system (e.g., there are multiple directories, each with its own certificate), you will see a Browse icon on the **Service Metadata** button. To specify which certificate will be included in the XML file, click the icon, choose the required certificate from the list and then click **SELECT**.



### Working with Service Keys

Active Directory Authentication services and REST API services can support multiple service keys for authentication. You can add as many keys as necessary and use each of them for different Windows / Mac credential provider configurations.

Service keys are managed from the **Sign on** tab of the AD Authentication or REST API service settings. The names of active keys are listed under **Service Keys**.



Bypass Unassigned Users

Bypass Unenrolled Users

Sign on Method: Active Directory

Authentication Token Timeout (1 minute - 1 year) *: 1 WEEKS

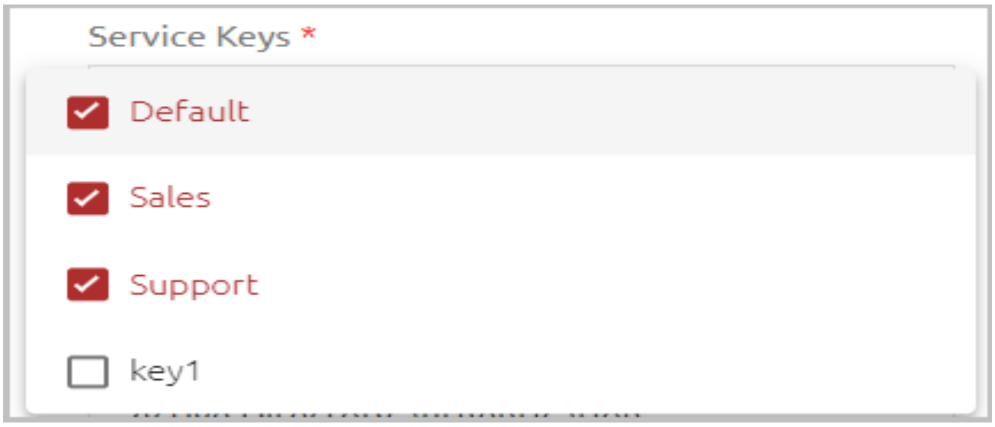
Endpoint URL: http m/adpa/31d52368-202d-4b84-88c

Rest Payload Signing Algorithm: SHA-256

Service Keys *: Default || Sales || Support

X.509 Certificate *: 2024-09-23 12:03 | SHA-256 | 2048-bit

To view all defined service keys, click to open the list. Active service keys are indicated by a selected checkbox. (At least one key must be active at all times.) Inactive keys cannot be included in service metadata and cannot be used for authentication.



Service Keys *

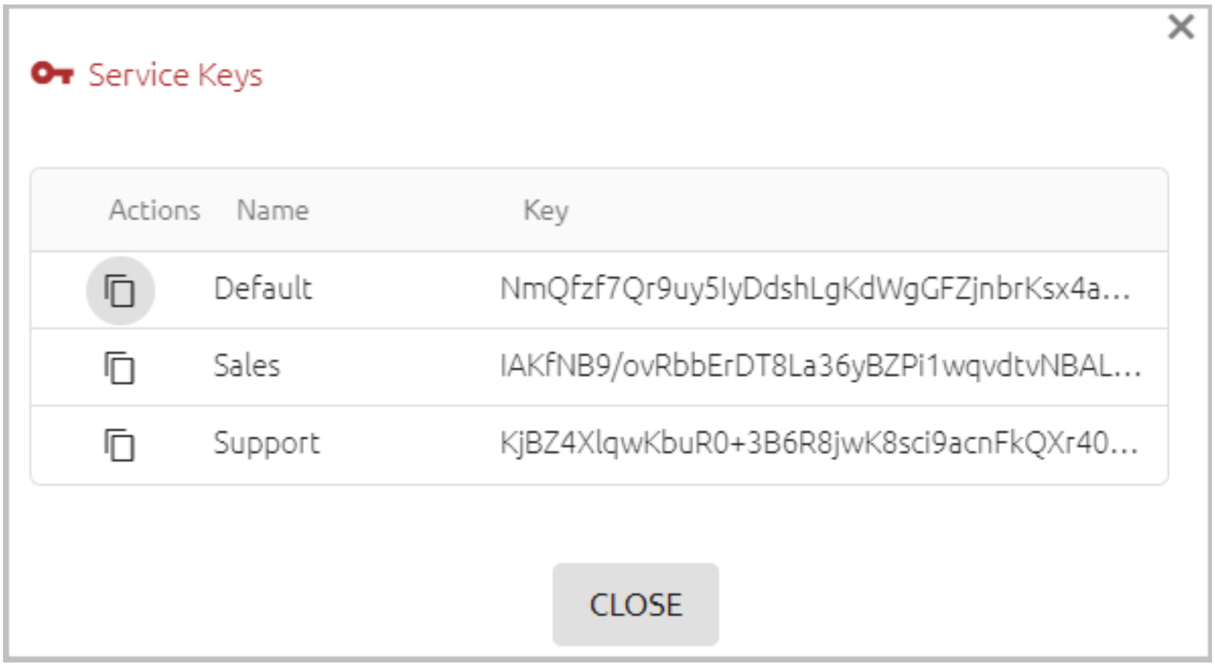
☑ Default

☑ Sales

☑ Support

□ key1

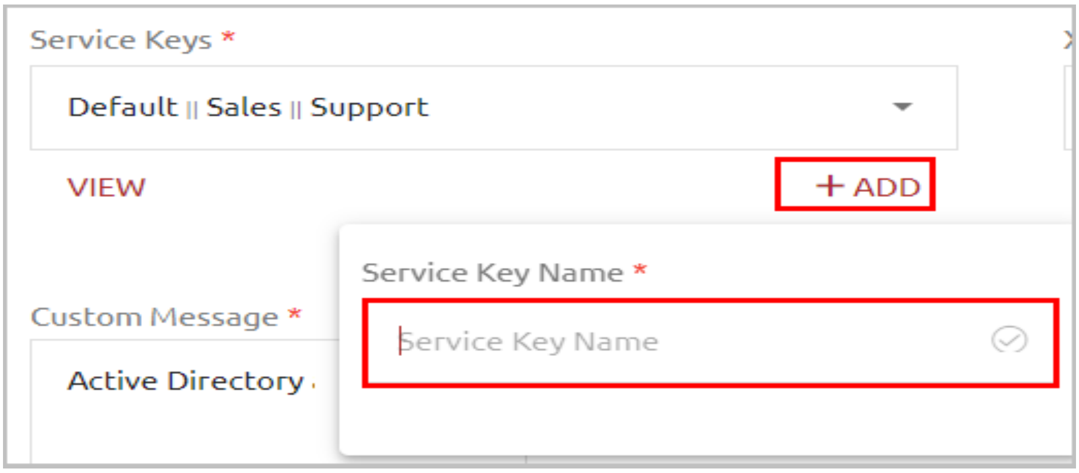
Clicking **VIEW** opens a popup from which you can view and copy all active service keys.



Service Keys

| Actions | Name | Key |
|---|---|---|
| ⧉ | Default | NmQfzf7Qr9uy5lyDdshLgKdWgGFZjnbrKsx4a… |
| ⧉ | Sales | IAKfNB9/ovRbbErDT8La36yBZPi1wqvdtvNBAL… |
| ⧉ | Support | KjBZ4XlqwKbuR0+3B6R8jwK8sci9acnFkQXr40… |

To generate a new service key, click **ADD**. Then, enter a name for the key and press **<Enter>** (or click the confirmation icon). By default, new service keys are active.

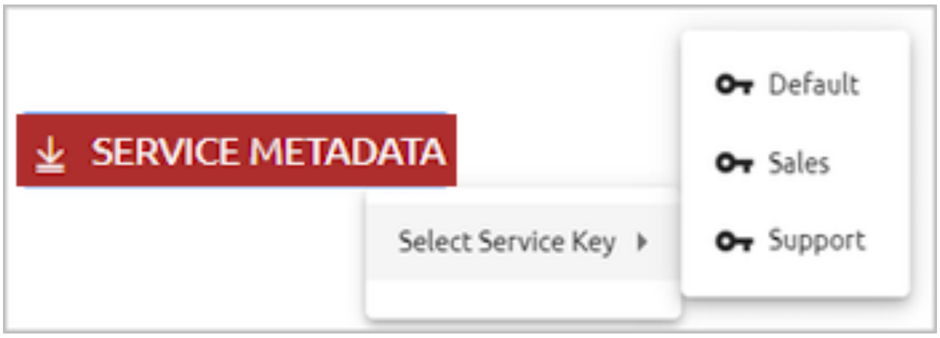


Service Keys *: Default || Sales || Support

Service Key Name *: Service Key Name

Custom Message *: Active Directory .

If there are multiple active service keys, you will be prompted to select the key to be included in the file when downloading service metadata.



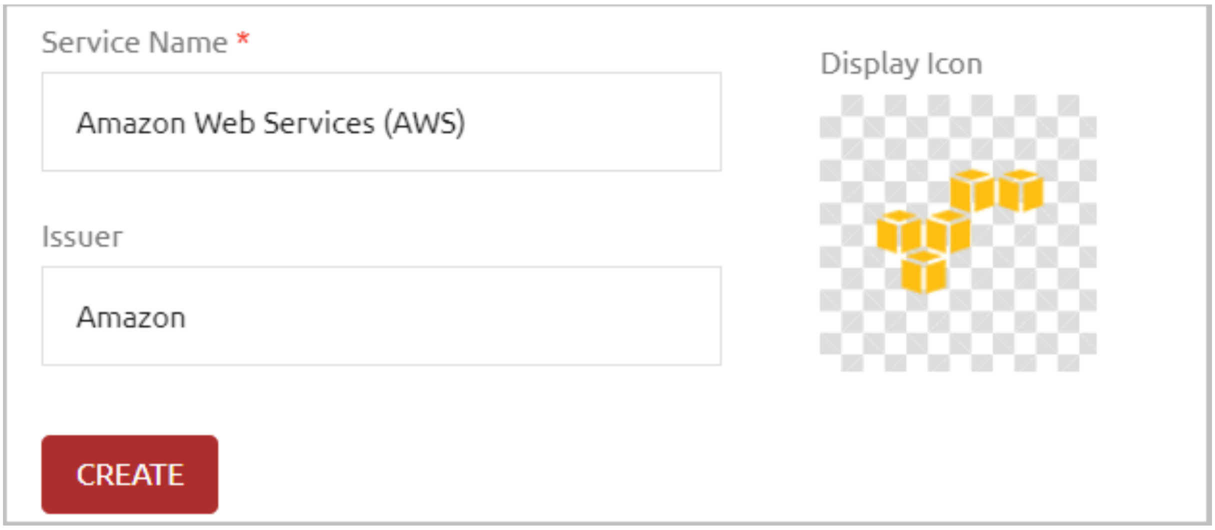
## Configuring Amazon Web Service Integration

The AWS SAML service enables SAML 2.0 integration between the Octopus Authenticator and Amazon Web Services. For successful integration, you need to create the service in the Management Console and configure the appropriate third-party Identity Provider and Role in your AWS account. The following procedure provides a summary of the integration process. For more detailed information, you may refer to the document How to Configure Octopus Authentication for Amazon Web Services.

**To configure AWS integration:**

1. In the Management Console, open the **Services** menu and click **Add Service**. In the **Amazon Web Services (AWS)** tile, click **Add**.

2. In the dialog that opens, update the default service name and issuer if desired. To change the display icon, click the tile and upload the logo of your choice (supported image size is 128x128 pixels). Then, click **Create**.



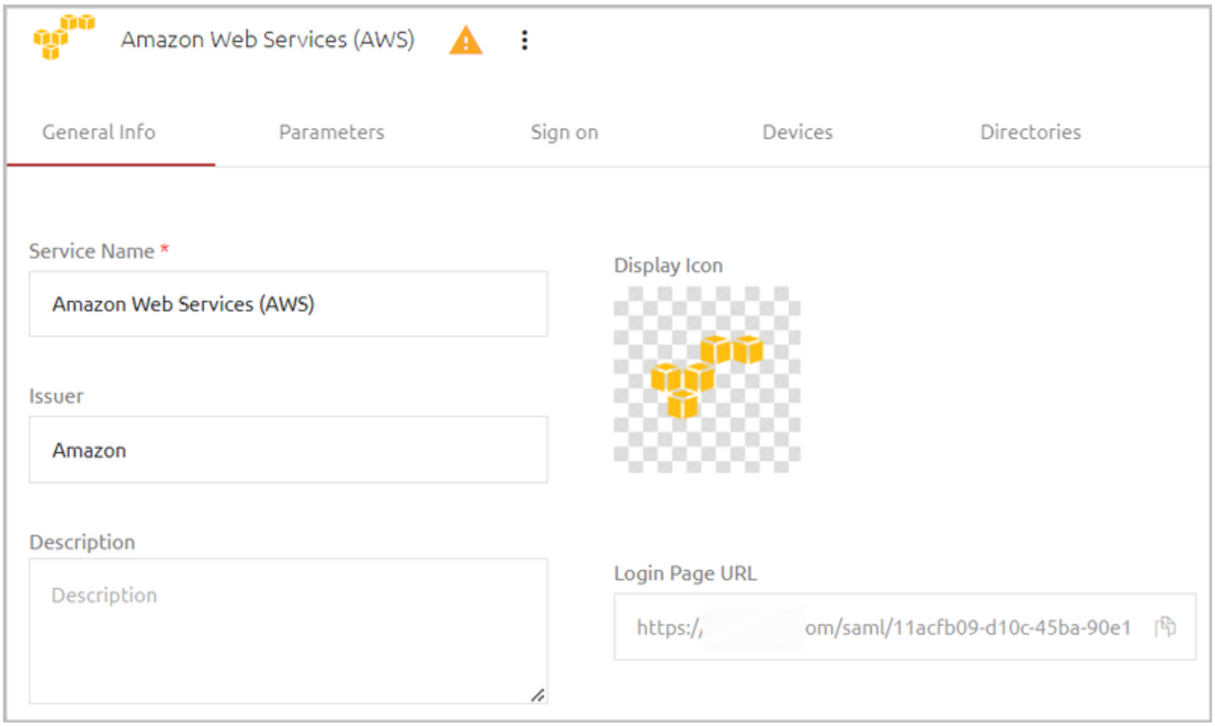
Service Name *

Amazon Web Services (AWS)

Issuer

Amazon

3. Review the settings in the **General Info** tab. If you add a description or update other settings, click **Save**.



Service Name *

Amazon Web Services (AWS)

Issuer

Amazon

Description

Description

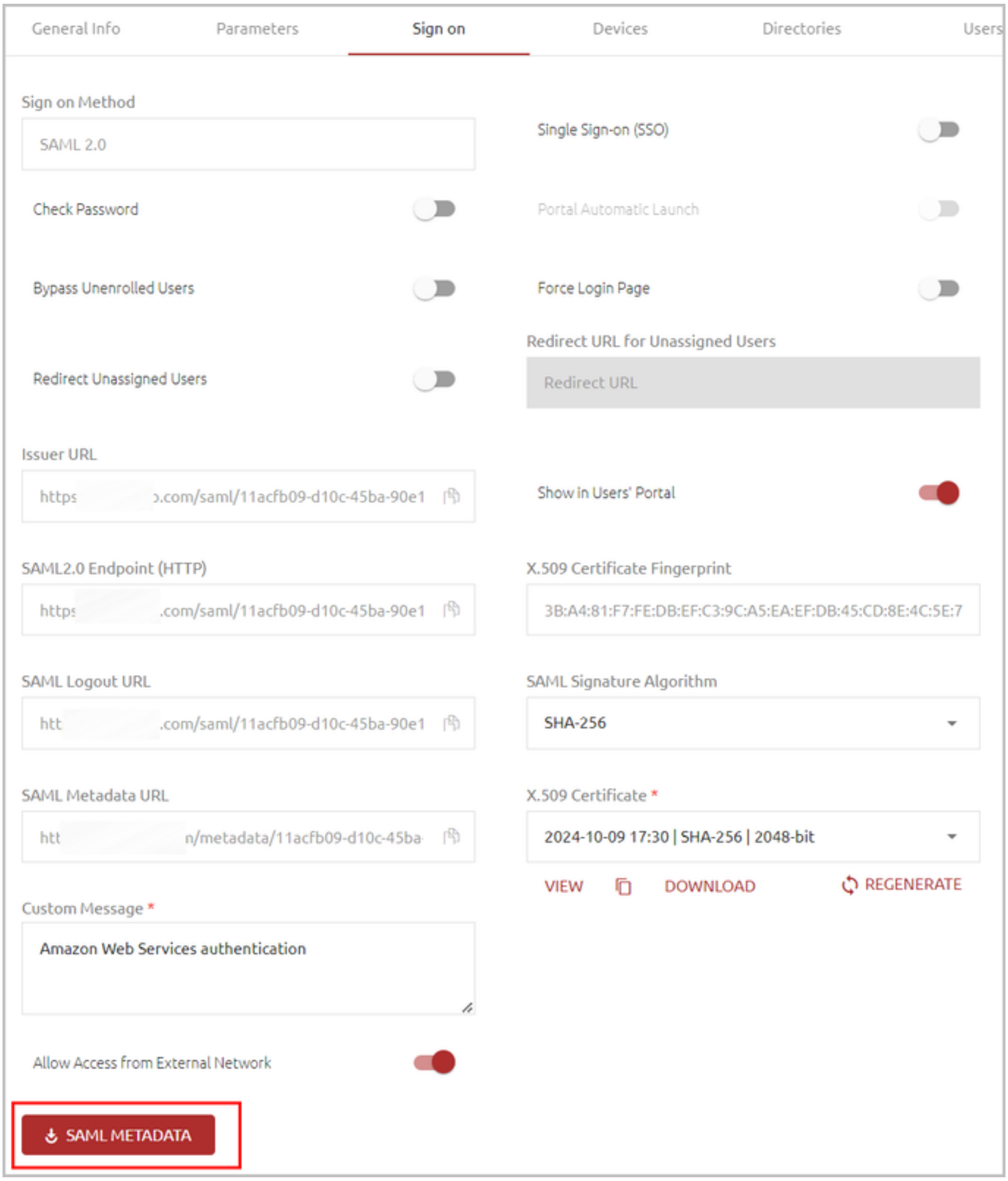
Display Icon

Login Page URL

https:/, om/saml/11acfb09-d10c-45ba-90e1

4. Add directories, users and groups to the service. For details, refer to Creating a Service and Assigning Users.

5. Open the **Sign on** tab. At the bottom of the tab, click **SAML METADATA** to view the **metadata.xml** file. Store this file. You will need it to configure the 3rd party IdP that you will create in your AWS account.



Sign on Method: SAML 2.0

Single Sign-on (SSO) ○

Check Password ○

Portal Automatic Launch ○

Bypass Unenrolled Users ○

Force Login Page ○

Redirect URL for Unassigned Users: Redirect URL

Redirect Unassigned Users ○

Issuer URL: https[redacted].com/saml/11acfb09-d10c-45ba-90e1

Show in Users' Portal ●

SAML2.0 Endpoint (HTTP): https[redacted].com/saml/11acfb09-d10c-45ba-90e1

X.509 Certificate Fingerprint: 3B:A4:81:F7:FE:DB:EF:C3:9C:A5:EA:EF:DB:45:CD:8E:4C:5E:7

SAML Logout URL: htt[redacted].com/saml/11acfb09-d10c-45ba-90e1

SAML Signature Algorithm: SHA-256

SAML Metadata URL: htt[redacted]n/metadata/11acfb09-d10c-45ba

X.509 Certificate *: 2024-10-09 17:30 | SHA-256 | 2048-bit

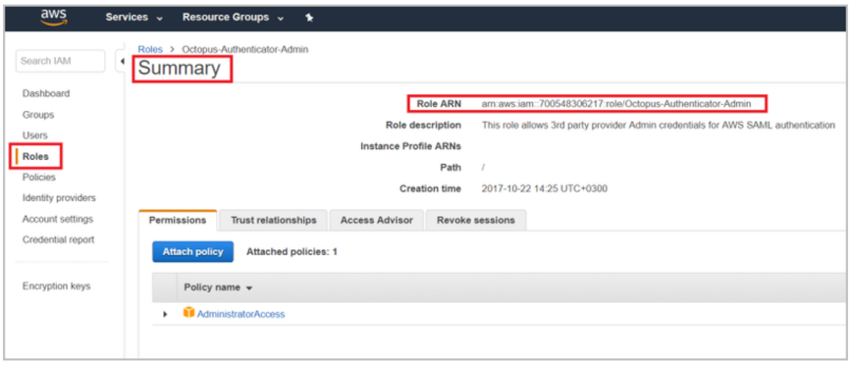
Custom Message *: Amazon Web Services authentication

Allow Access from External Network ●

6. Log into your AWS account and perform these procedures:
   - Create and configure the AWS Identity Provider
   - Create the IAM Role

   For details, refer to the integration document: How to Configure Octopus Authentication for Amazon Web Services.

   After completing the procedures, you will have an **AWS Role ARN** and an **AWS Provider ARN.**



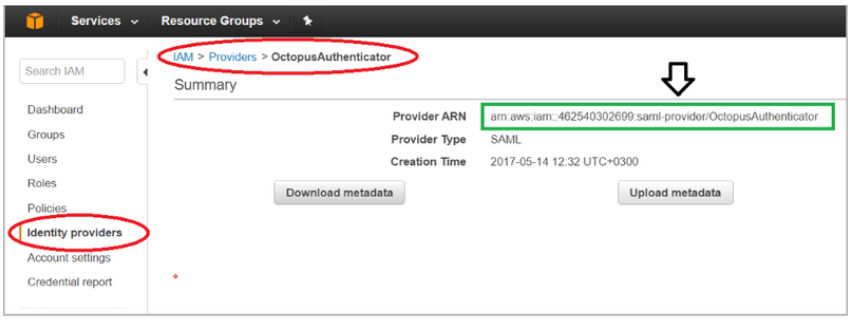
Roles > Octopus-Authenticator-Admin

Summary

Role ARN arn:aws:iam::700548306217:role/Octopus-Authenticator-Admin
Role description This role allows 3rd party provider Admin credentials for AWS SAML authentication
Instance Profile ARNs
Path /
Creation time 2017-10-22 14:25 UTC+0300

Attached policies: 1

| Policy name |
|---|
| AdministratorAccess |



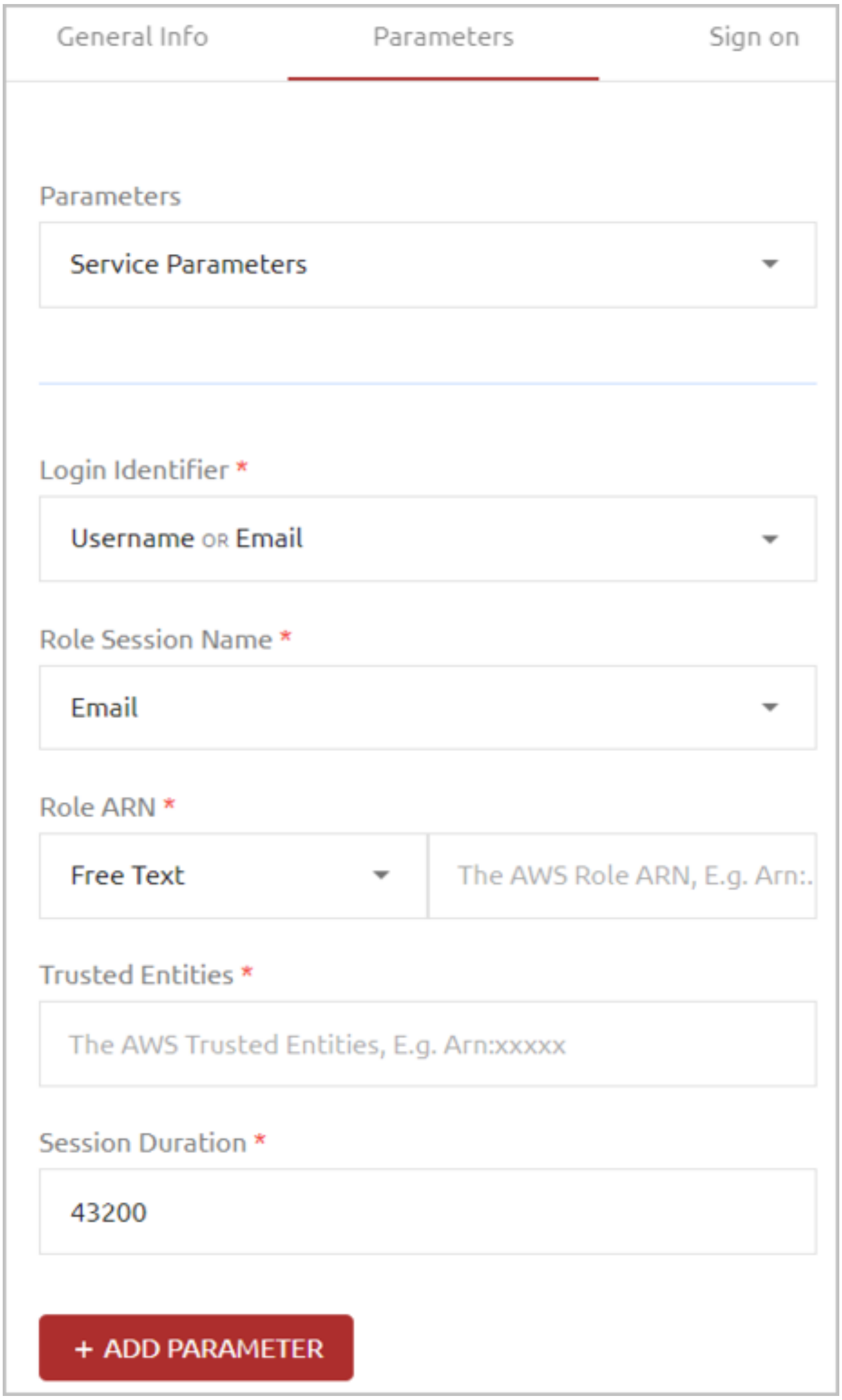
IAM > Providers > OctopusAuthenticator

Summary

Provider ARN arn:aws:iam::462540302699:saml-provider/OctopusAuthenticator
Provider Type SAML
Creation Time 2017-05-14 12:32 UTC+0300

7. In the Management Console, open the service settings for the AWS SAML service you created. Select the **Parameters** tab and configure the following settings:

| Setting | Value / Notes |
|---|---|
| Login Identifier | Select the login method(s) for the Octopus Authentication Server. |
| Role Session Name | Select **Email**. |
| Role ARN | Set the value with the AWS Role ARN string. |
| Trusted Entities | Set the value with the AWS Provider ARN string. |
| Session Duration | Set the period of time (in seconds) for which the console can be open before the session expires. |



Parameters: Service Parameters

Login Identifier *: Username OR Email

Role Session Name *: Email

Role ARN *: Free Text | The AWS Role ARN, E.g. Arn:.

Trusted Entities *: The AWS Trusted Entities, E.g. Arn:xxxxx

Session Duration *: 43200

If you wish, you may click **Add Parameter** to create additional optional parameters that are commonly added to SAML services. For a list of these parameters, refer to Generic SAML Service Parameters.

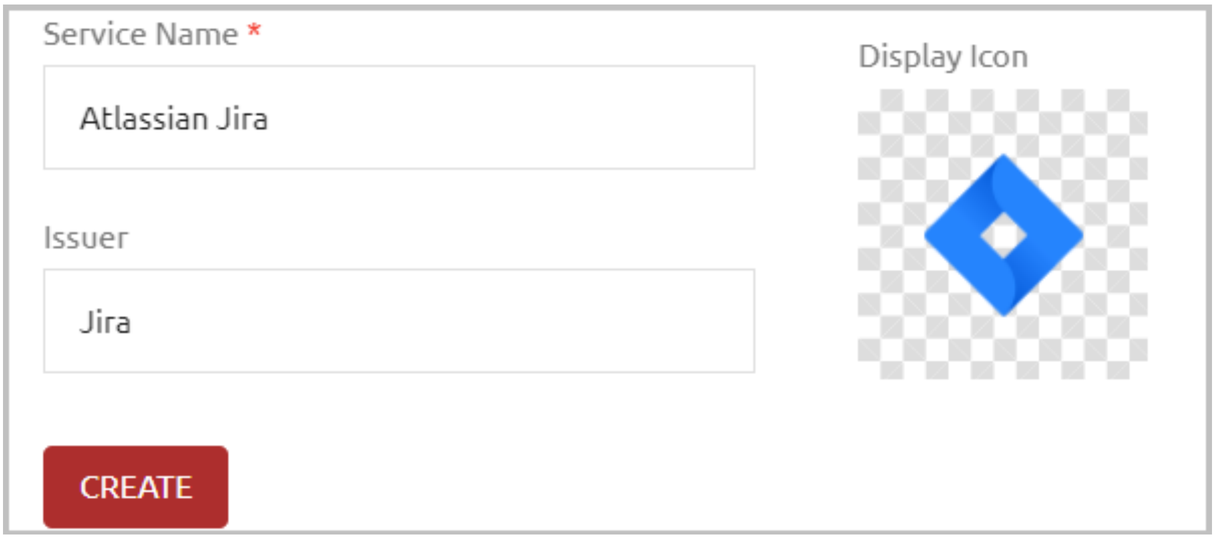
8. At the bottom of the **Parameters** tab, click **Save**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

## Configuring Atlassian Jira Service Integration

The Jira SAML service enables SAML 2.0 integration between the Octopus Authenticator and the Jira software service. For successful integration, you need to create the service in the Management Console and set up the SAML SSO configuration in your Atlassian account. The following procedure provides a summary of the integration process. For more detailed information, you may refer to the document How to Configure Octopus Authentication for Jira Software.

**To configure Jira integration:**

1. In the Management Console, open the **Services** menu and click **Add Service**. In the **Atlassian Jira** tile, click **Add**.
2. In the dialog that opens, update the default service name and issuer if desired. To change the display icon, click the tile and upload the logo of your choice (supported image size is 128x128 pixels). Then, click **Create**.



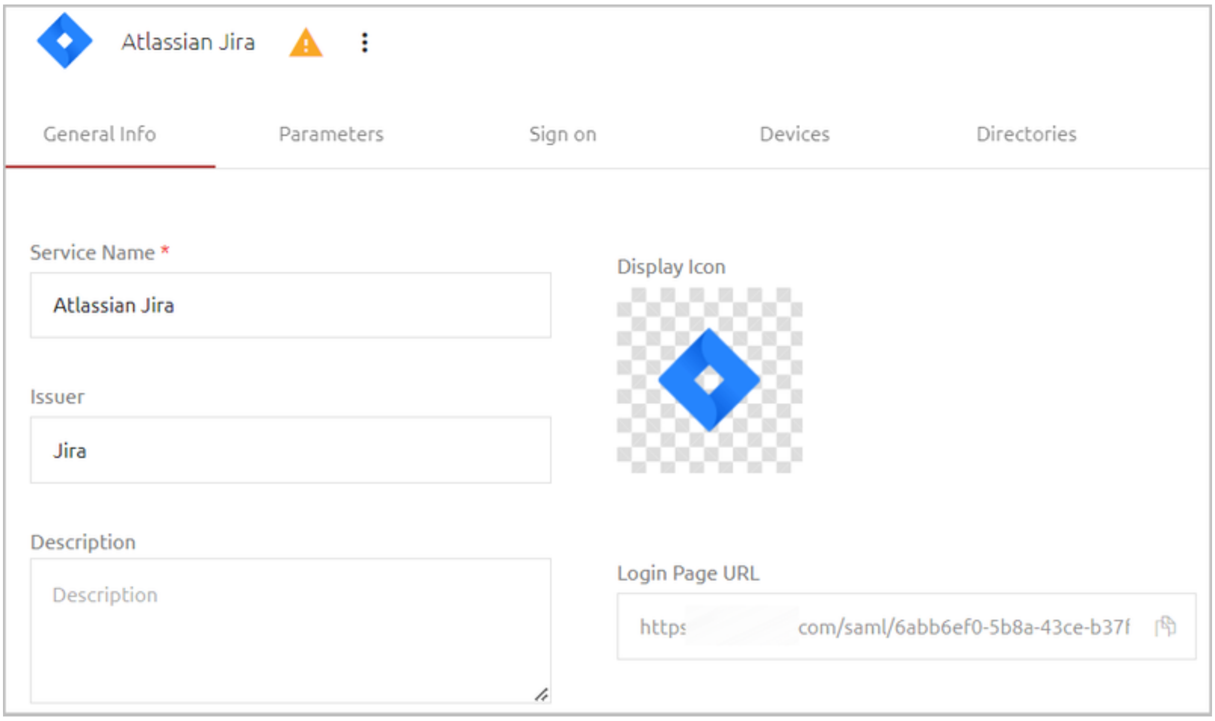
Service Name *

Atlassian Jira

Issuer

Jira

3. Review the settings in the **General Info** tab. If you add a description or update other settings, click **Save**.



Service Name * Atlassian Jira

Issuer Jira

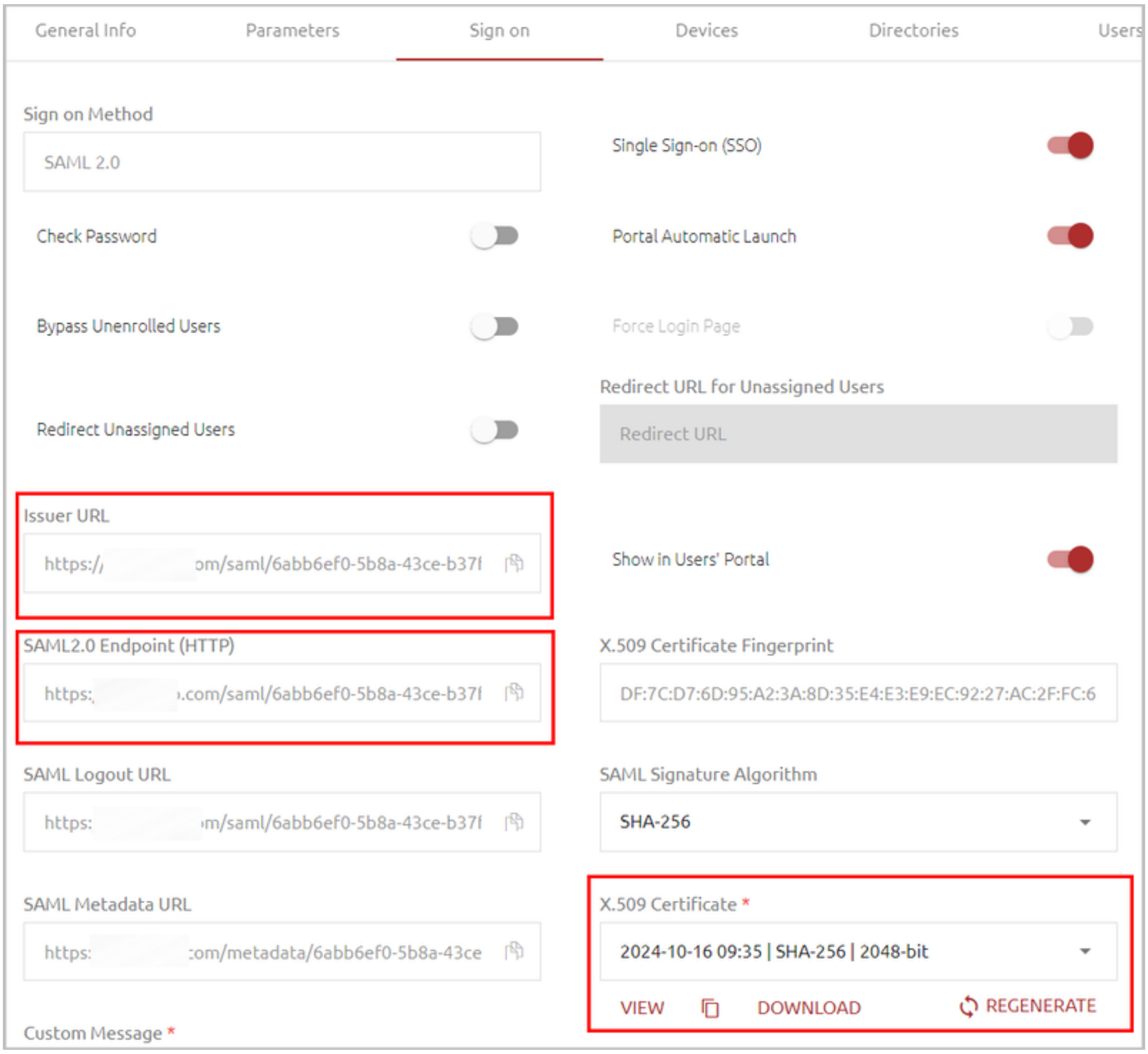
Description Description

Login Page URL https[redacted]com/saml/6abb6ef0-5b8a-43ce-b37f

4. Add directories, users and groups to the service. For details, refer to Creating a Service and Assigning Users.

5. Open the **Sign on** tab. Copy or download the following elements:

   - **Issuer URL:** The URL used by the Jira service to connect to Octopus Authenticator. Click the Copy icon to copy the URL.
   - **SAML2.0 Endpoint (HTTP):** The Octopus Authenticator Login page URL to which the Jira service provider will refer users for Octopus authentication. Click the Copy icon to copy the URL.
   - **X.509 Certificate:** Click **View**. Then, in the popup that opens, click **Copy** to copy the content of the certificate file.



Sign on Method: SAML 2.0

Check Password: off

Bypass Unenrolled Users: off

Redirect Unassigned Users: off

Single Sign-on (SSO): on

Portal Automatic Launch: on

Force Login Page: off

Redirect URL for Unassigned Users: Redirect URL

Issuer URL: https:/[redacted]om/saml/6abb6ef0-5b8a-43ce-b37f

SAML2.0 Endpoint (HTTP): https:[redacted].com/saml/6abb6ef0-5b8a-43ce-b37f

SAML Logout URL: https:[redacted]m/saml/6abb6ef0-5b8a-43ce-b37f

SAML Metadata URL: https:[redacted]com/metadata/6abb6ef0-5b8a-43ce

Custom Message *

Show in Users' Portal: on

X.509 Certificate Fingerprint: DF:7C:D7:6D:95:A2:3A:8D:35:E4:E3:E9:EC:92:27:AC:2F:FC:6

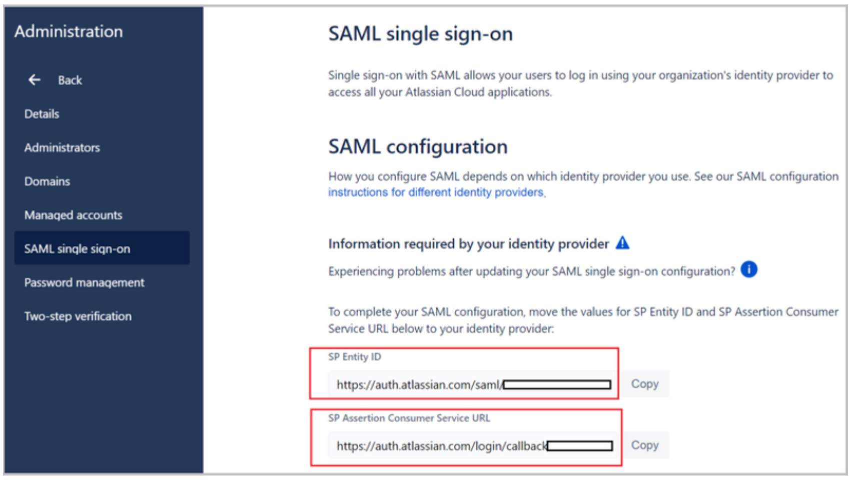
SAML Signature Algorithm: SHA-256

X.509 Certificate *: 2024-10-16 09:35 | SHA-256 | 2048-bit

You will need these elements to set up the SAML SSO configuration in your Atlassian account.

6. Log into your Atlassian account as an administrator and edit the settings of the SAML single sign-on configuration. For details, refer to the integration document: How to Configure Octopus Authentication for Jira Software.

   After completing the configuration, Jira SAML Single Sign-On parameters will be generated and displayed on the **SAML single sign-on** page.



SAML single sign-on

Single sign-on with SAML allows your users to log in using your organization's identity provider to access all your Atlassian Cloud applications.

SAML configuration

How you configure SAML depends on which identity provider you use. See our SAML configuration instructions for different identity providers.

Information required by your identity provider

Experiencing problems after updating your SAML single sign-on configuration?

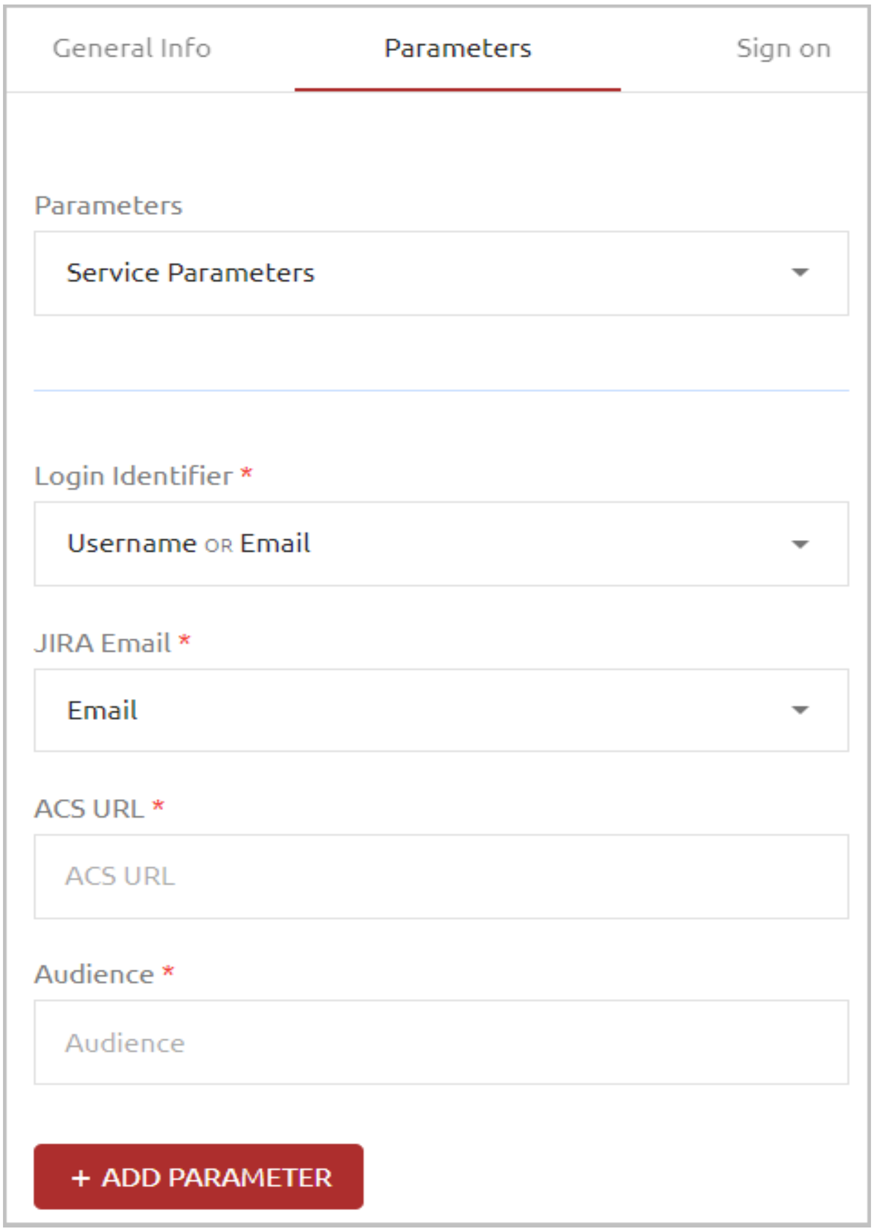
To complete your SAML configuration, move the values for SP Entity ID and SP Assertion Consumer Service URL below to your identity provider:

SP Entity ID: https://auth.atlassian.com/saml/[redacted]

SP Assertion Consumer Service URL: https://auth.atlassian.com/login/callback[redacted]

7. In the Management Console, open the service settings for the Jira SAML service you created. Select the **Parameters** tab and configure the following settings:

| Setting | Value / Notes |
|---|---|
| Login Identifier | Select the login method(s) for the Octopus Authentication Server. |
| JIRA Email | Login method for Jira software (default = **Email**.) |
| ACS URL | Set the value to the **SP Assertion Consumer Service URL**. |
| Audience | Set the value to the **SP Entity ID**. |



Parameters: Service Parameters

Login Identifier *: Username OR Email

JIRA Email *: Email

ACS URL *: ACS URL

Audience *: Audience

If you wish, you may click **Add Parameter** to create additional optional parameters that are commonly added to SAML services. For a list of these parameters, refer to Generic SAML Service Parameters.

8. At the bottom of the **Parameters** tab, click **Save**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

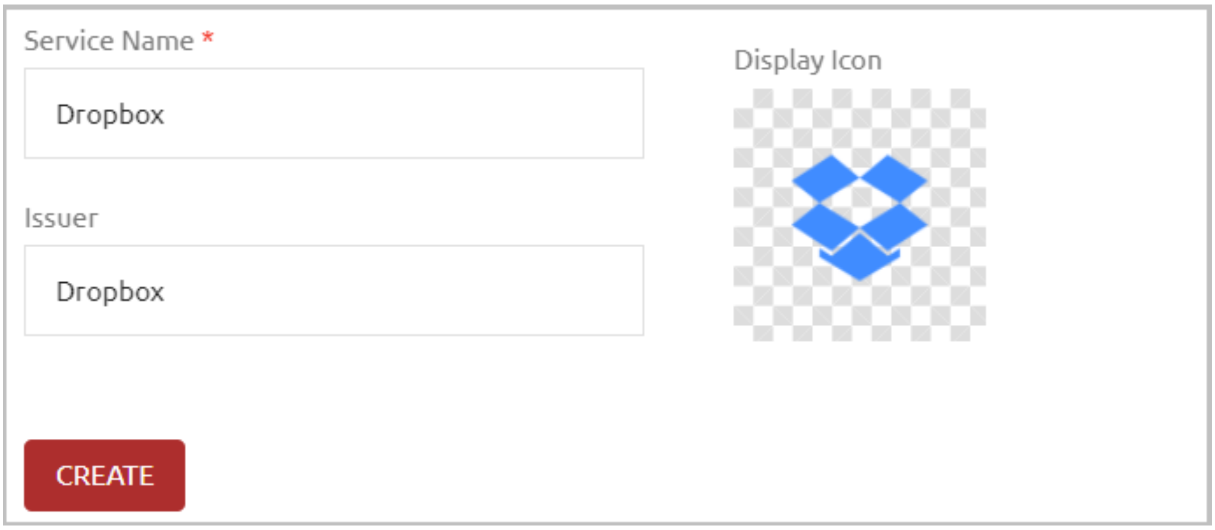
## Configuring Dropbox Service Integration

The Dropbox SAML service enables SAML 2.0 integration between the authentication platform and the Dropbox web service. For successful integration, you need to create the service in the Management Console and set up SSO configuration in your Dropbox admin account. The following procedure provides a summary of the integration process. For more detailed information, you may refer to the document How to Configure Octopus Authentication for Dropbox.

**To configure Dropbox integration:**

1. In the Management Console, open the **Services** menu and click **Add Service**. In the **Dropbox** tile, click **Add**.

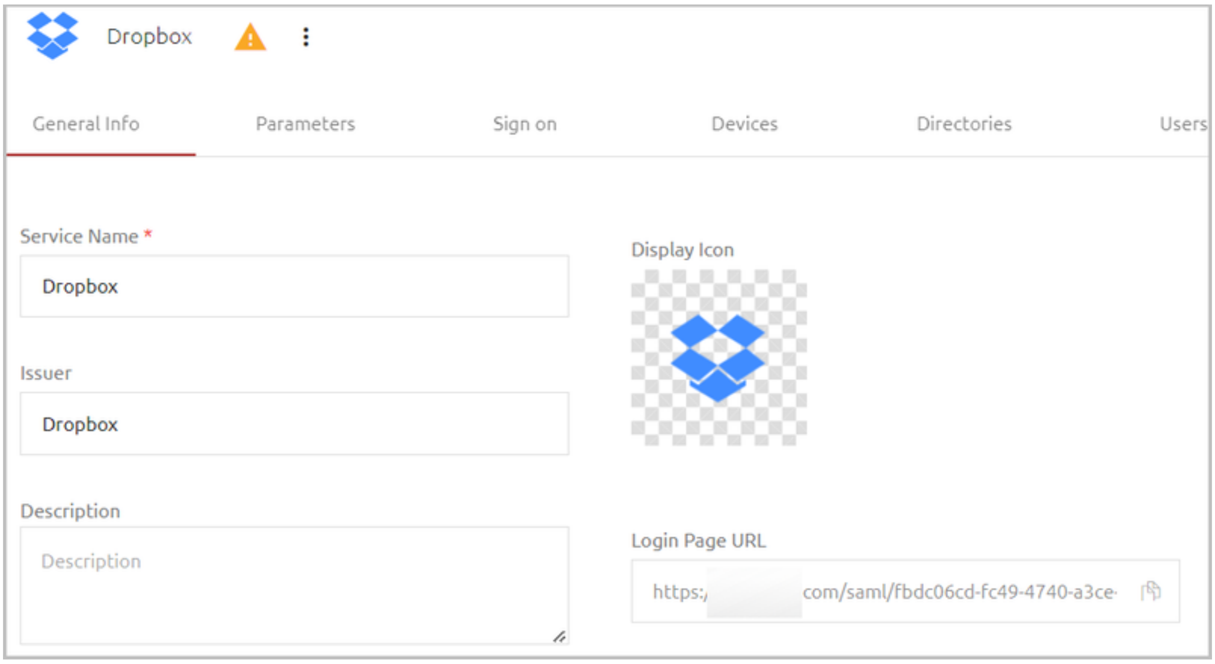
2. In the dialog that opens, update the default service name and issuer if desired. To change the display icon, click the tile and upload the logo of your choice (supported image size is 128x128 pixels). Then, click **Create**.



Service Name * Dropbox

Issuer Dropbox

3. Review the settings in the **General Info** tab. If you add a description or update other settings, click **Save**.



Dropbox

Service Name * Dropbox

Issuer Dropbox

Description Description

Login Page URL https:/[redacted]com/saml/fbdc06cd-fc49-4740-a3ce-

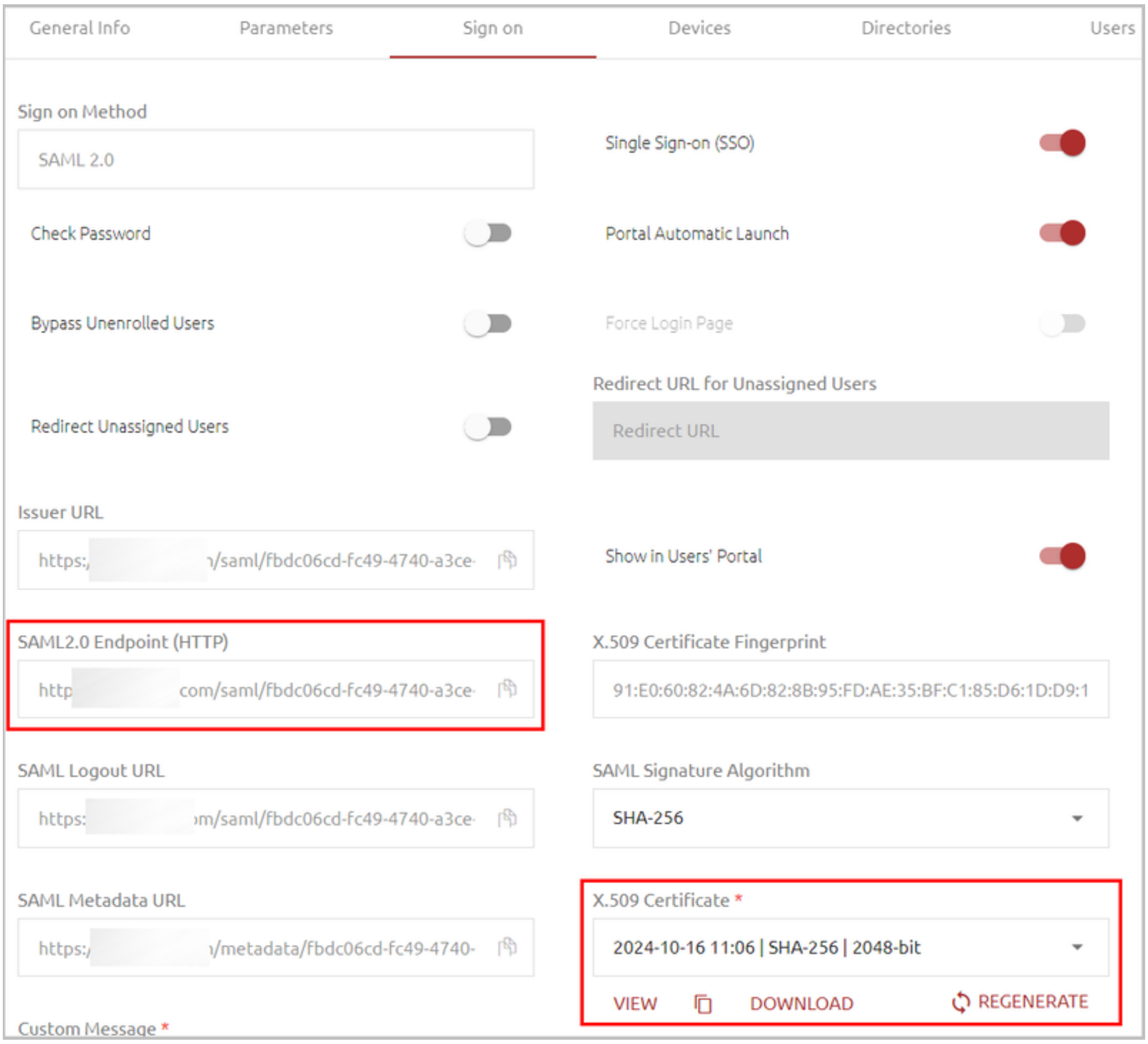
4. Add directories, users and groups to the service. For details, refer to Creating a Service and Assigning Users.

5. Open the **Sign on** tab and do the following:

   ○ Copy the value of the **SAML2.0 Endpoint (HTTP)** URL. This is the Octopus Authenticator Login page URL to which the Dropbox service provider will refer users for Octopus authentication. Click the Copy icon to copy the URL.

- ○ Under **X.509 Certificate**, click **Download** to download the **cert.pem** certificate.

You will use these elements while configuring the 3rd party Identity Provider (IdP)SSO in your Dropbox account.



Sign on Method: SAML 2.0

Single Sign-on (SSO): ●

Check Password: ○

Portal Automatic Launch: ●

Bypass Unenrolled Users: ○

Force Login Page: ○

Redirect URL for Unassigned Users: Redirect URL

Redirect Unassigned Users: ○

Issuer URL: https:/[redacted]ı/saml/fbdc06cd-fc49-4740-a3ce-

Show in Users' Portal: ●

SAML2.0 Endpoint (HTTP): http[redacted]com/saml/fbdc06cd-fc49-4740-a3ce-

X.509 Certificate Fingerprint: 91:E0:60:82:4A:6D:82:8B:95:FD:AE:35:BF:C1:85:D6:1D:D9:1

SAML Logout URL: https:[redacted]ɔm/saml/fbdc06cd-fc49-4740-a3ce-

SAML Signature Algorithm: SHA-256

SAML Metadata URL: https:/[redacted]ı/metadata/fbdc06cd-fc49-4740-

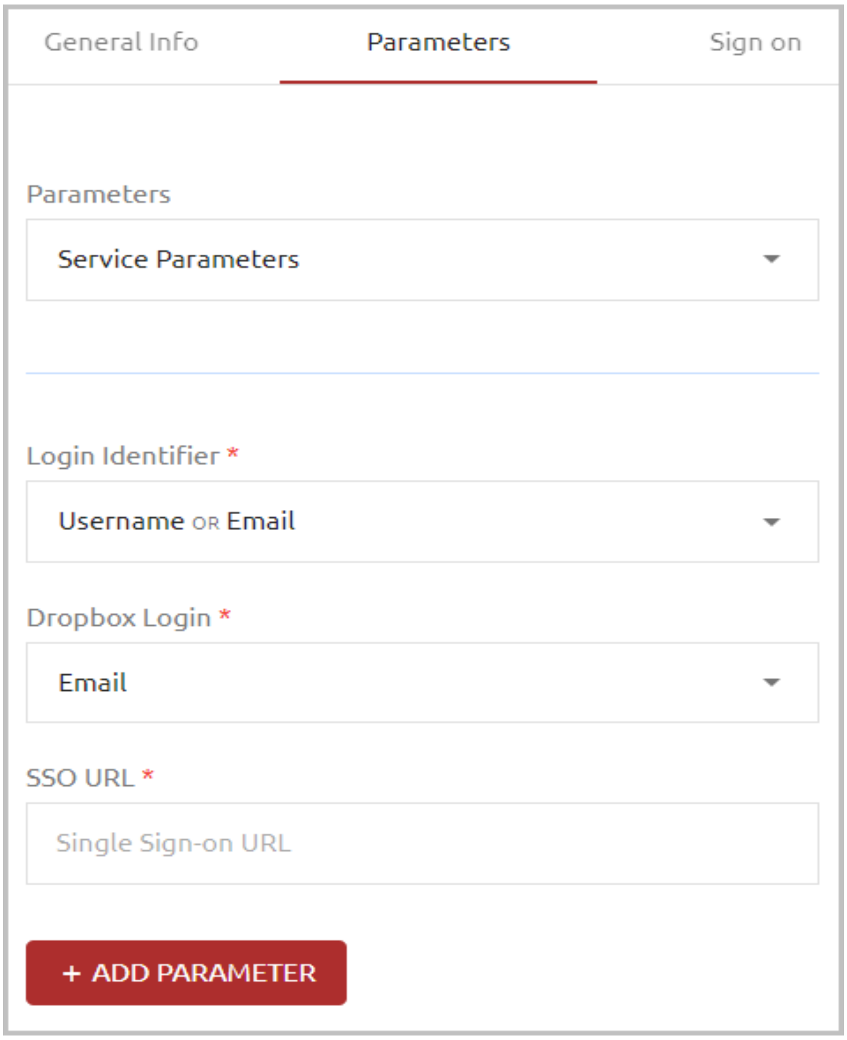
X.509 Certificate *: 2024-10-16 11:06 | SHA-256 | 2048-bit

6. Log into your Dropbox Admin account. From the Admin Console Dashboard, set up the 3rd party IdP SSO.

   For details, refer to the integration document: How to Configure Octopus Authentication for Dropbox.

7. In the Management Console, open the service settings for the Dropbox SAML service you created. Select the **Parameters** tab and configure the following settings:

| Setting | Value / Notes |
|---|---|
| Login Identifier | Select the login method(s) for the Authentication Server. |
| Dropbox Login | Select the login method for Dropbox. |
| SSO URL | Copy the customized link from the SSO settings in your Dropbox account (**SSO sign-in UR**L). |



Parameters: Service Parameters

Login Identifier *: Username OR Email

Dropbox Login *: Email

SSO URL *: Single Sign-on URL

If you wish, you may click **Add Parameter** to create additional optional parameters that are commonly added to SAML services. For a list of these parameters, refer to Generic SAML Service Parameters.

8. Click **Save**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

## Configuring Entra ID EAM Service Integration

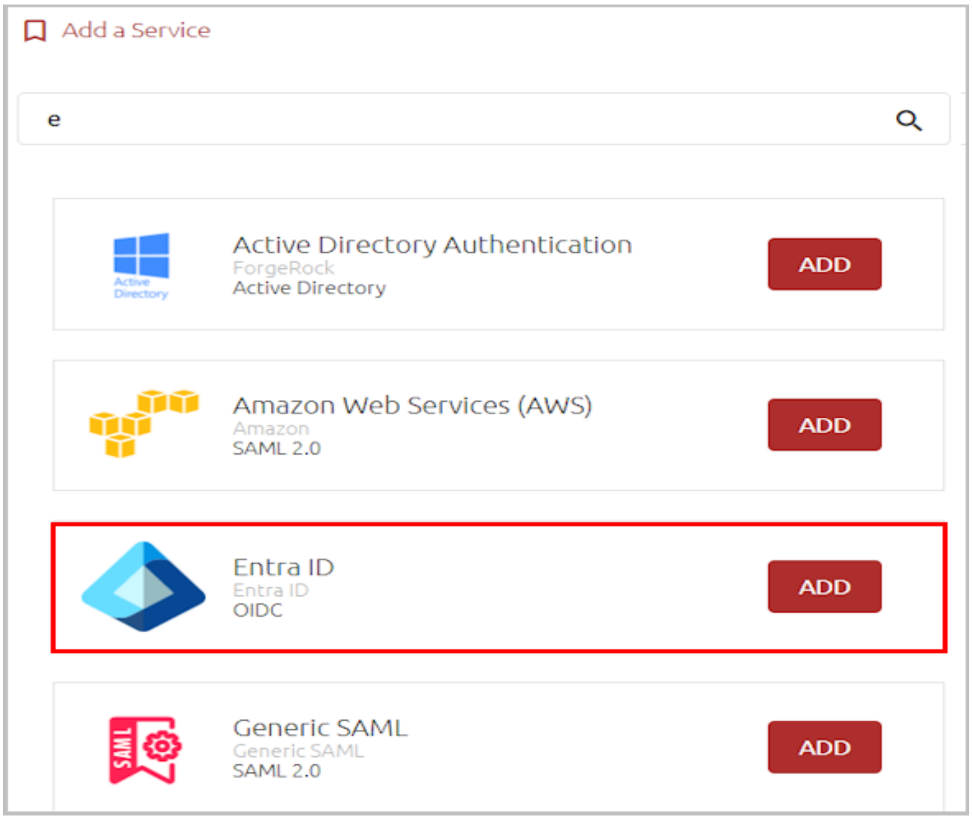
Entra ID EAM service integration enables users to log into the Microsoft Entra admin center using the Enterprise Connect Passwordless platform as a means of two-factor authentication.

For successful integration, you need to create the service in the Management Console, and then perform the required configuration in your Entra ID environment.

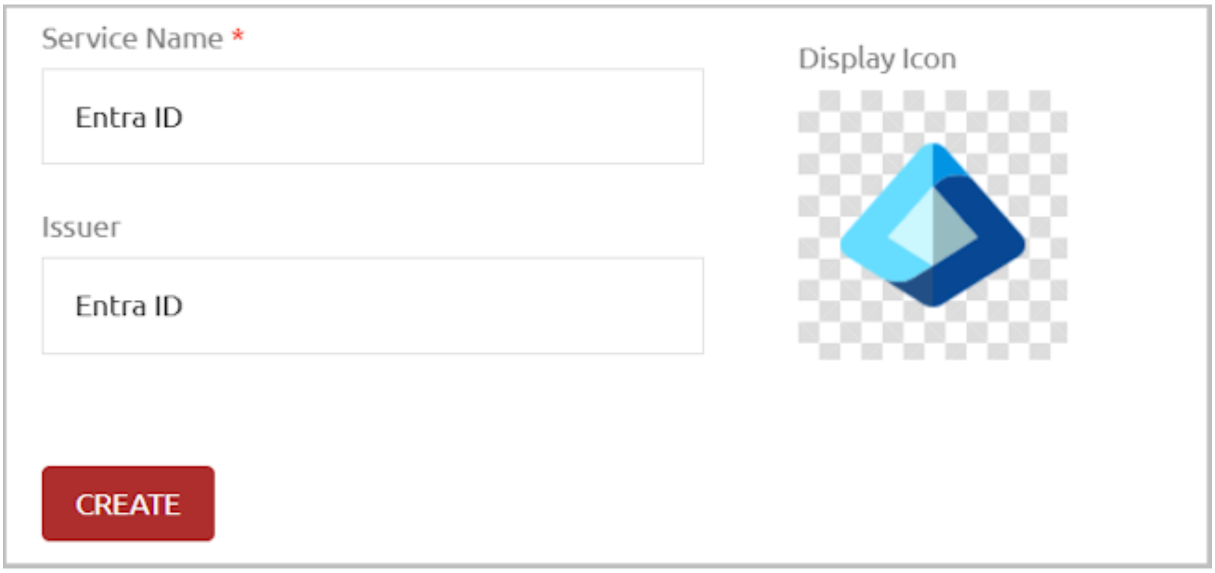
The following procedure provides a summary of the integration process. For full details and instructions, please refer to the document Configuring an External Authentication Method in Microsoft Entra ID with Enterprise Connect Passwordless.

**To configure Entra ID EAM integration:**

1. In the Management Console, open the **Services** menu and click **Add Service**. In the **Entra ID** tile, click **Add**.

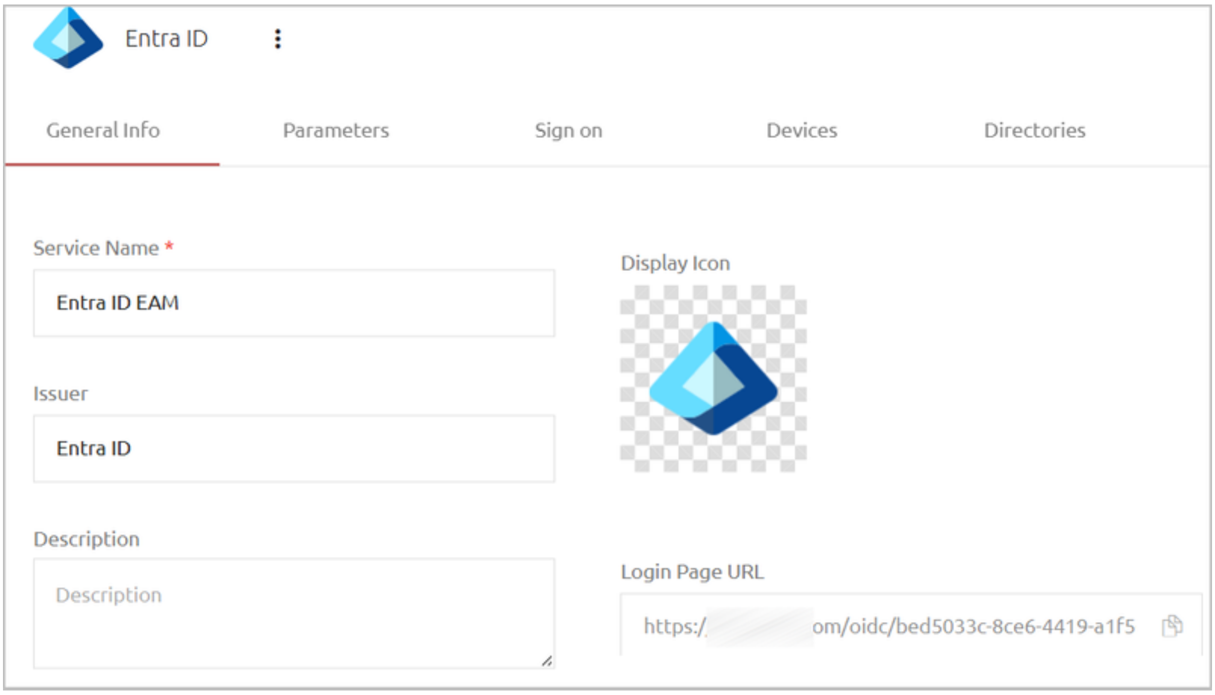


2. In the dialog that opens, update the default service name and issuer if desired. To change the display icon, click the tile and upload the logo of your choice (supported image size is 128x128 pixels). Then, click **Create**.


Service Name *: Entra ID

Issuer: Entra ID

3. Review the settings in the **General Info** tab. If you add a description or update other settings, click **Save**.



Service Name *: Entra ID EAM

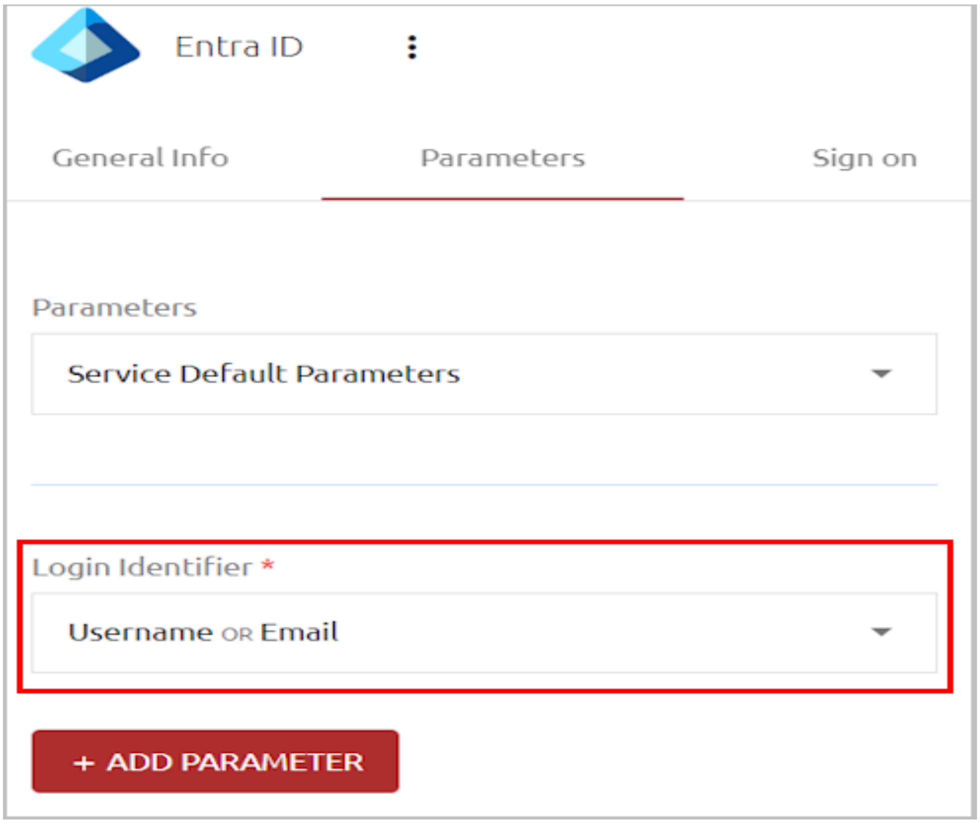
Issuer: Entra ID

Description: Description

Login Page URL: https:/[redacted]om/oidc/bed5033c-8ce6-4419-a1f5

4. Add directories, users and groups to the service. For details, refer to [Creating a Service and Assigning Users](#).

5. Open the **Parameters** tab. From the **Login Identifier** list, verify that **Username** and **Email** are selected.



Parameters

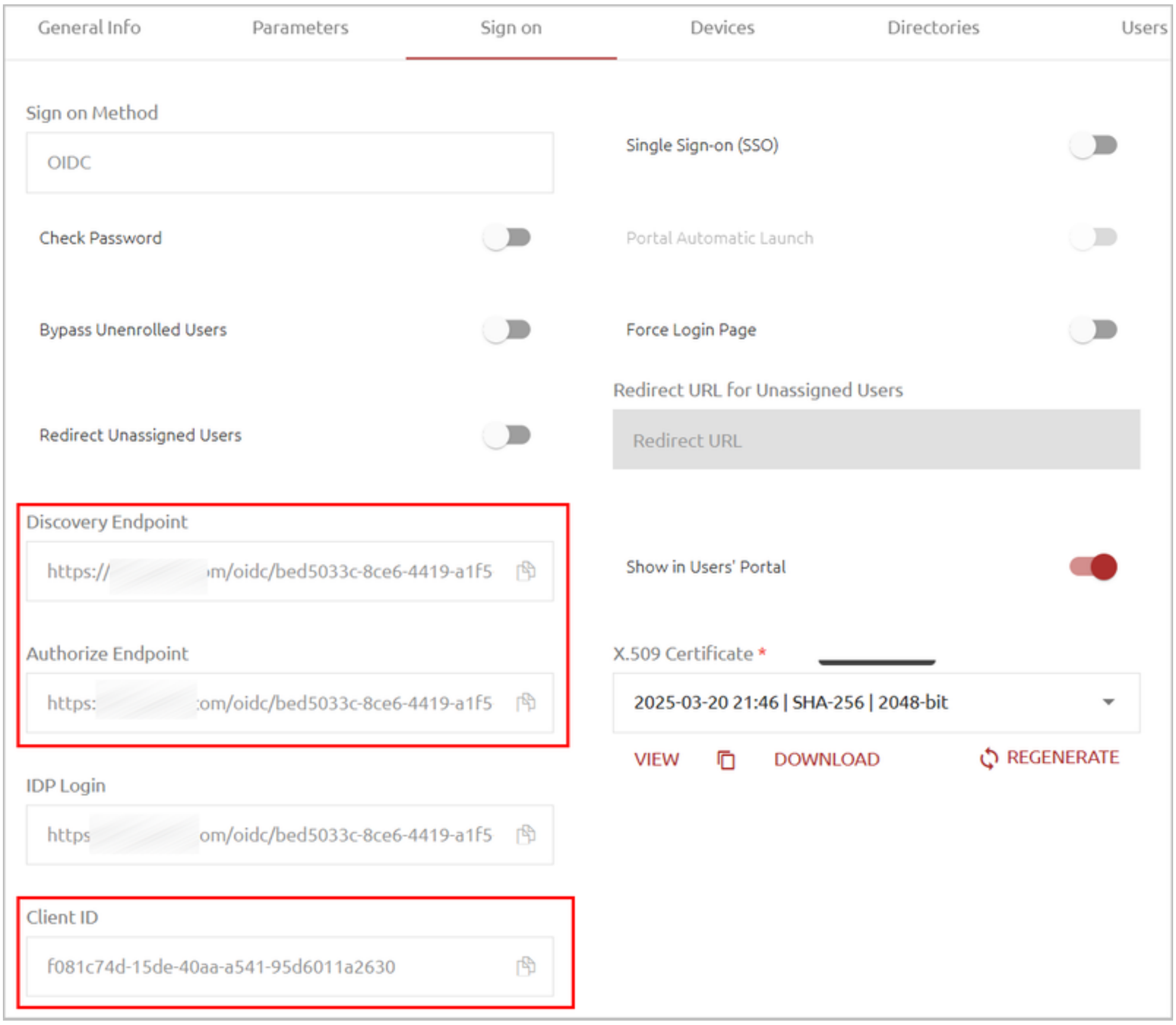
Service Default Parameters

Login Identifier *

Username OR Email

If you update parameters, click **Save**.

6. Open the **Sign on** tab and copy the following elements by clicking the Copy icons:
   - **Discovery Endpoint:** A URL pointing to a configuration document containing metadata about the OIDC provider, including URLs for authorization, token supply, user data and more.
   - **Authorize Endpoint:** A redirect URL allowing Entra ID to authorize use of the external identity provider for authentication.
   - **Client ID:** A unique identifier for the service called to handle the authentication request.



Sign on Method: OIDC

Single Sign-on (SSO)

Check Password

Portal Automatic Launch

Bypass Unenrolled Users

Force Login Page

Redirect URL for Unassigned Users: Redirect URL

Redirect Unassigned Users

Discovery Endpoint: https://[redacted]m/oidc/bed5033c-8ce6-4419-a1f5

Show in Users' Portal

Authorize Endpoint: https:[redacted]om/oidc/bed5033c-8ce6-4419-a1f5

X.509 Certificate *: 2025-03-20 21:46 | SHA-256 | 2048-bit

IDP Login: https[redacted]om/oidc/bed5033c-8ce6-4419-a1f5

Client ID: f081c74d-15de-40aa-a541-95d6011a2630

You will need these elements to configure your Entra ID environment.

7. Configure the Entra ID environment as described in the document Configuring an External Authentication Method in Microsoft Entra ID with Enterprise Connect Passwordless.

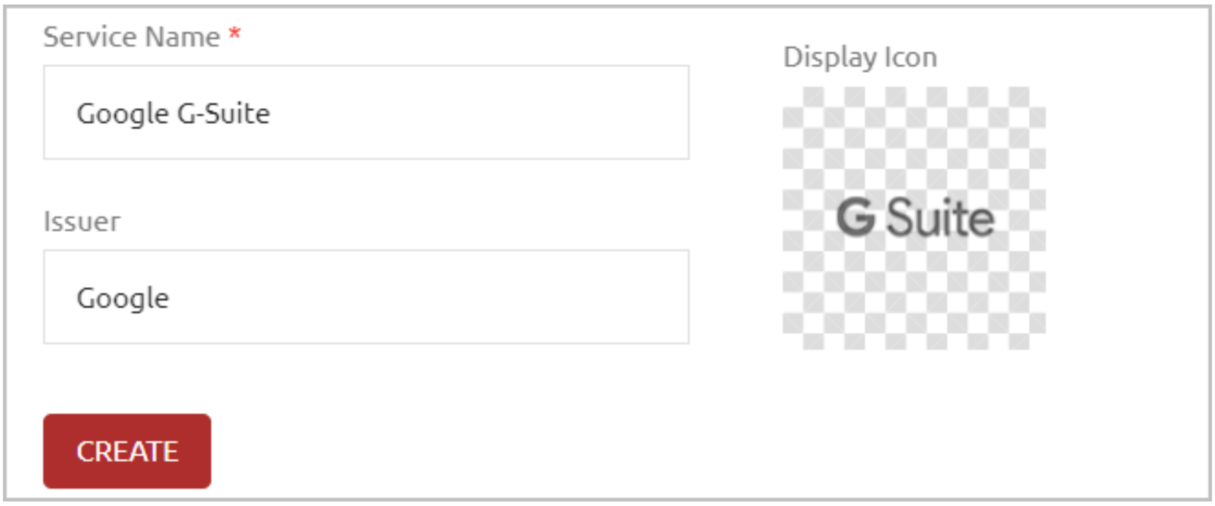
## Configuring Google G Suite Service Integration

The Google G Suite SAML service enables SAML 2.0 integration between the Octopus Authenticator and G Suite web services. For successful integration, you need to create the service in the Management Console and set up the 3rd party identity provider SSO in your Google G Suite Admin account. The following procedure provides a summary of the integration process. For more detailed information, you may refer to the document How to Configure Octopus Authentication for G Suite Web Services.

**To configure Google G Suite integration:**

1. In the Management Console, open the **Services** menu and click **Add Service**. In the **Google G-Suite** tile, click **Add**.

2. In the dialog that opens, update the default service name and issuer if desired. To change the display icon, click the tile and upload the logo of your choice (supported image size is 128x128 pixels). Then, click **Create**.



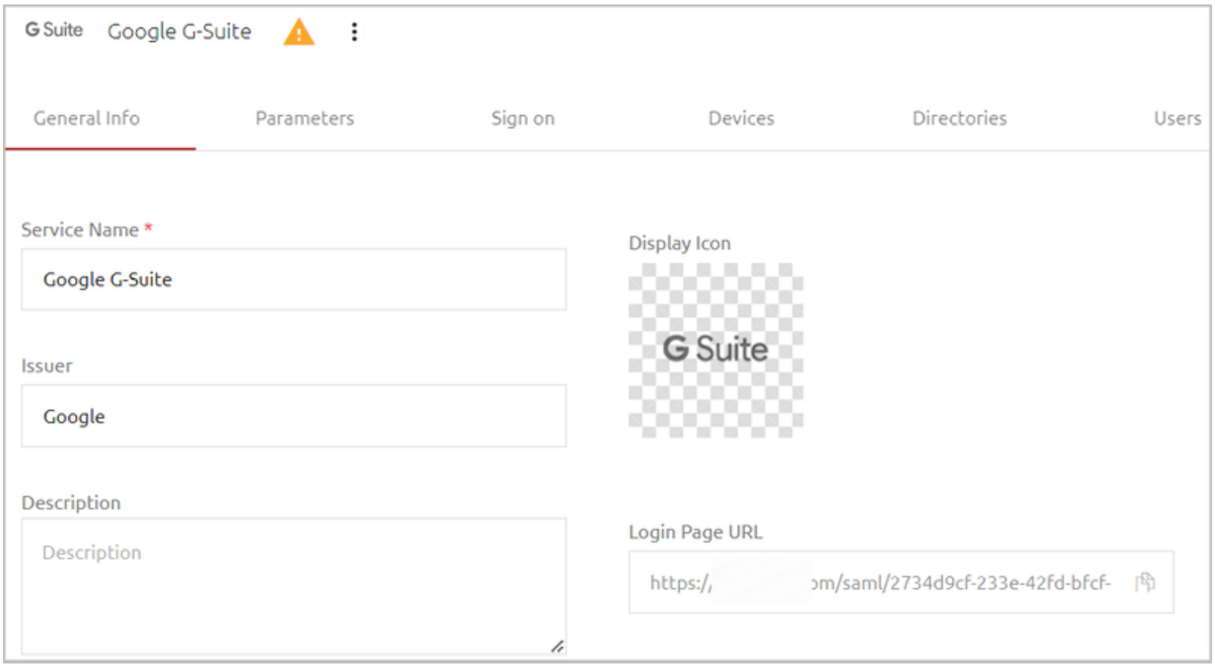
Service Name *

Google G-Suite

Issuer

Google

3. Review the settings in the **General Info** tab. If you add a description or update other settings, click **Save**.



Service Name *

Google G-Suite

Issuer

Google

Description

Description

Login Page URL

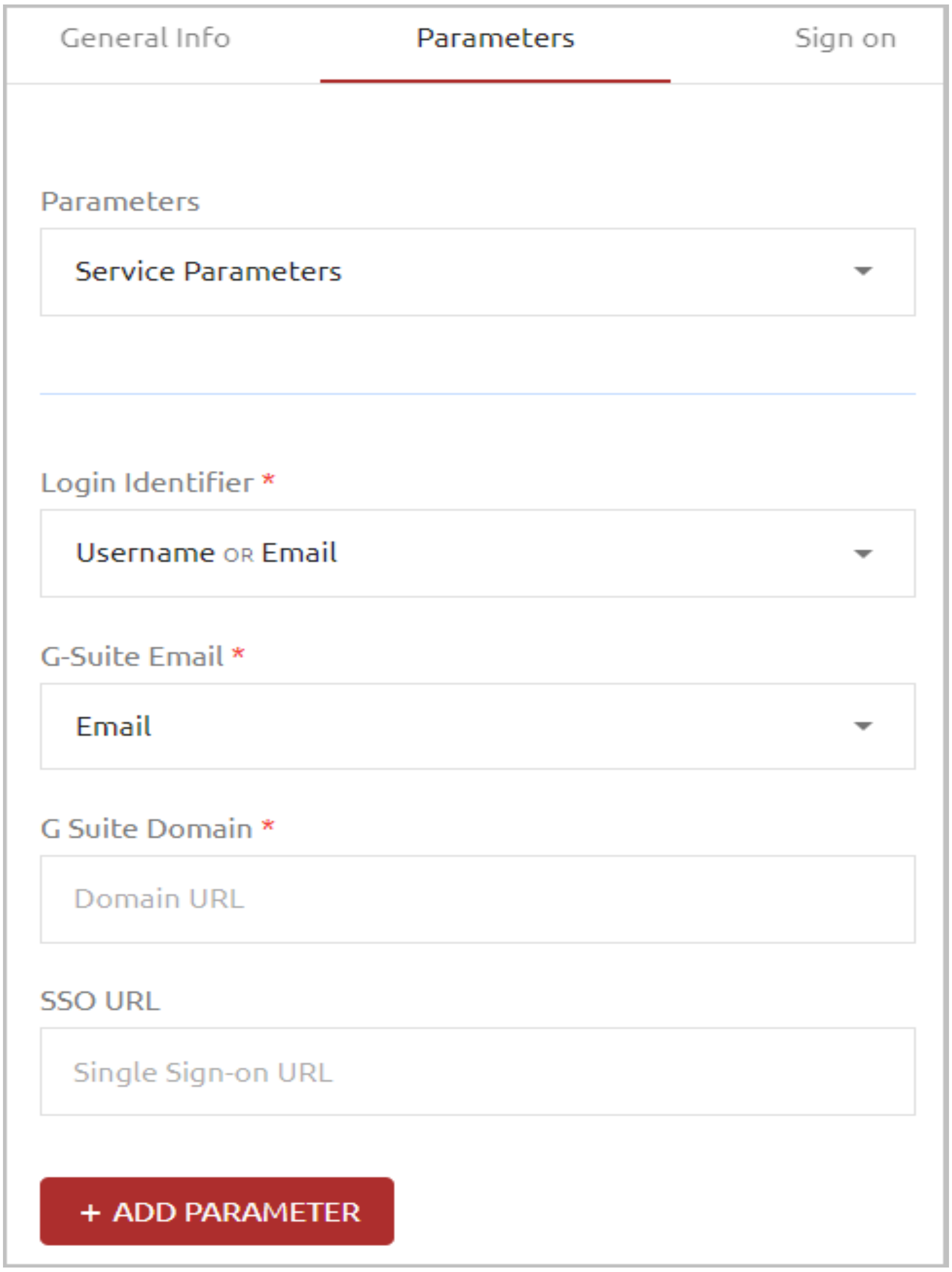
https:/, om/saml/2734d9cf-233e-42fd-bfcf-

4. Add directories, users and groups to the service. For details, refer to Creating a Service and Assigning Users.

5. Open the **Parameters** tab and configure the following settings. Do not configure any additional parameters.

| Setting | Value / Notes |
|---|---|
| Login Identifier | Login method for the Octopus Authentication Server (select **Email**). |

| Setting | Value / Notes |
|---|---|
| G-Suite Email | Select **Email**. |
| G Suite Domain | Enter the domain URL. |



General Info | Parameters | Sign on

Parameters

Service Parameters

Login Identifier *

Username OR Email

G-Suite Email *

Email

G Suite Domain *

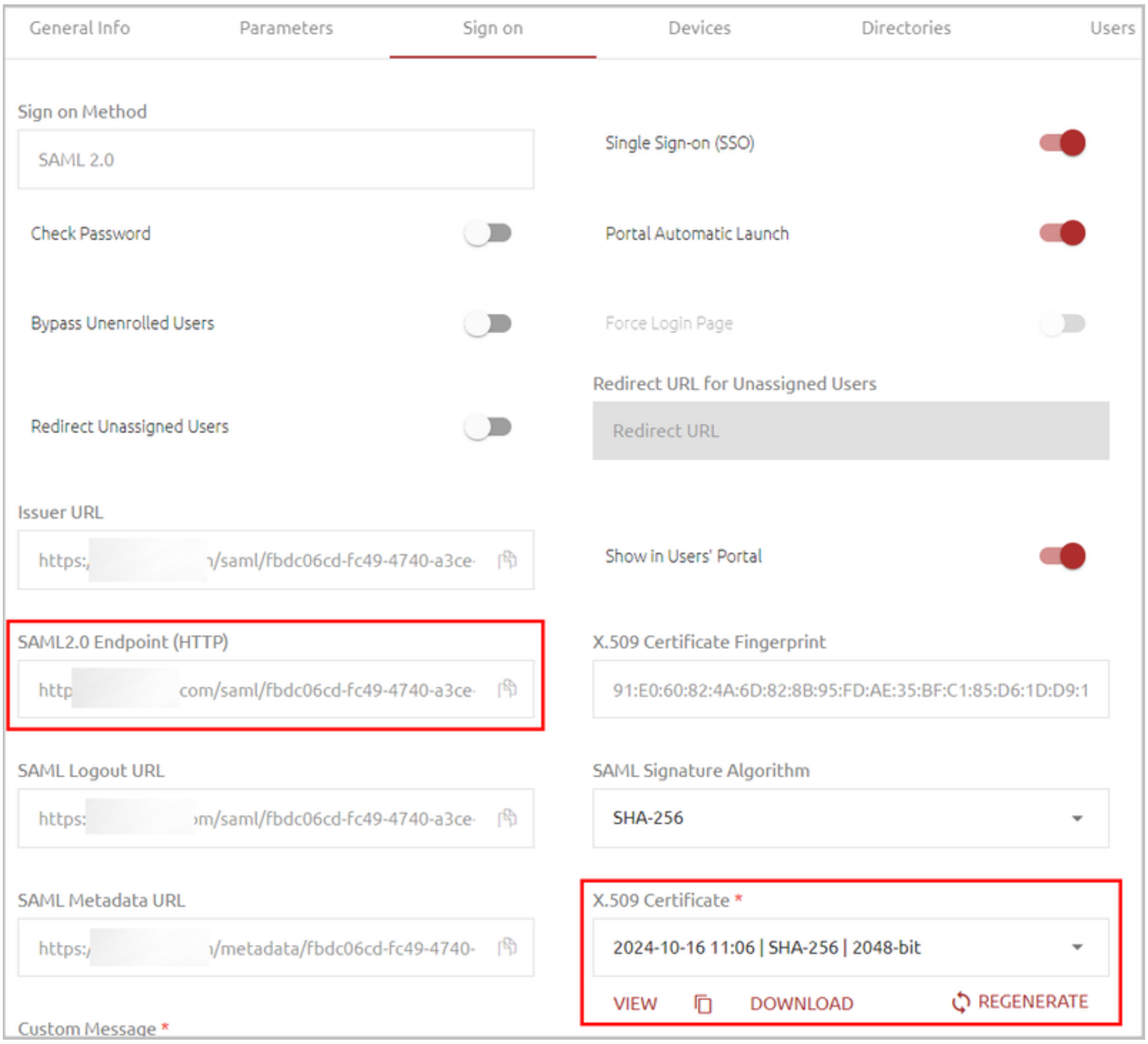
Domain URL

SSO URL

Single Sign-on URL

+ ADD PARAMETER

6. At the bottom of the **Parameters** tab, click **Save**.
7. Open the **Sign on** tab and copy or download the following elements:
    - **SAML2.0 Endpoint (HTTP):** The Octopus Authenticator G Suite Login page URL to which the G Suite service provider will refer users for Octopus authentication. Click the Copy icon to copy the URL.
    - **X.509 Certificate:** Click **Download** to download the **cert.pem** file.



Sign on Method: SAML 2.0

Single Sign-on (SSO): on

Check Password: off

Portal Automatic Launch: on

Bypass Unenrolled Users: off

Force Login Page: off

Redirect URL for Unassigned Users: Redirect URL

Redirect Unassigned Users: off

Issuer URL: https:/[redacted]ı/saml/fbdc06cd-fc49-4740-a3ce-

Show in Users' Portal: on

SAML2.0 Endpoint (HTTP): http[redacted]com/saml/fbdc06cd-fc49-4740-a3ce-

X.509 Certificate Fingerprint: 91:E0:60:82:4A:6D:82:8B:95:FD:AE:35:BF:C1:85:D6:1D:D9:1

SAML Logout URL: https:[redacted]ɔm/saml/fbdc06cd-fc49-4740-a3ce-

SAML Signature Algorithm: SHA-256

SAML Metadata URL: https:/[redacted]ı/metadata/fbdc06cd-fc49-4740-

X.509 Certificate *: 2024-10-16 11:06 | SHA-256 | 2048-bit

Custom Message *

You will need these elements to configure the 3rd party identity provider SSO in your Google G Suite Admin account.

8. Log into your G Suite Admin account. From the Admin Console menu, select **Security** and complete the **Setup SSO with third party identity provider** configuration. For details, refer to the integration document: How to Configure Octopus Authentication for G Suite Web Services.

## Configuring Microsoft Office 365 Service Integration

The Microsoft Office 365 SAML service enables SAML 2.0 integration between the Octopus Authenticator and the Microsoft Office 365 web service. For successful integration, you need to create the service in the Management Console and set up the appropriate configurations in the Office365 Web Service and the Mobile Outlook App. The following procedure provides a summary of the integration process.

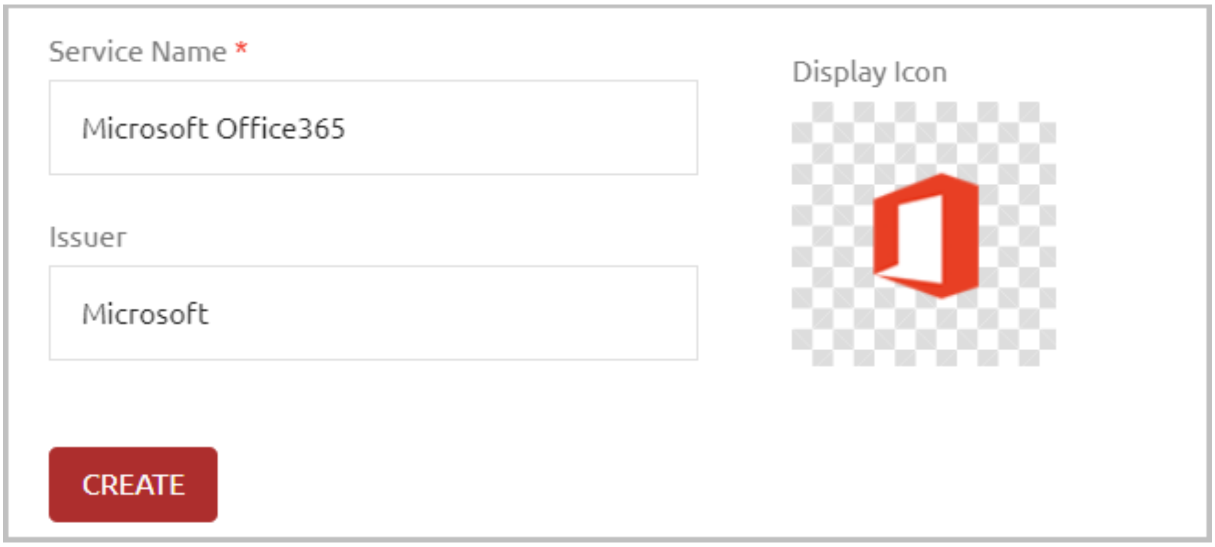
**Important**

For more detailed information, including concept, prerequisites and best practices, it is recommended to refer to the integration document How to Configure Octopus Authentication for Microsoft Office 365.

**To configure Microsoft Office 365 integration:**

1. In the Management Console, open the **Services** menu and click **Add Service**. In the **Microsoft Office 365** tile, click **Add**.

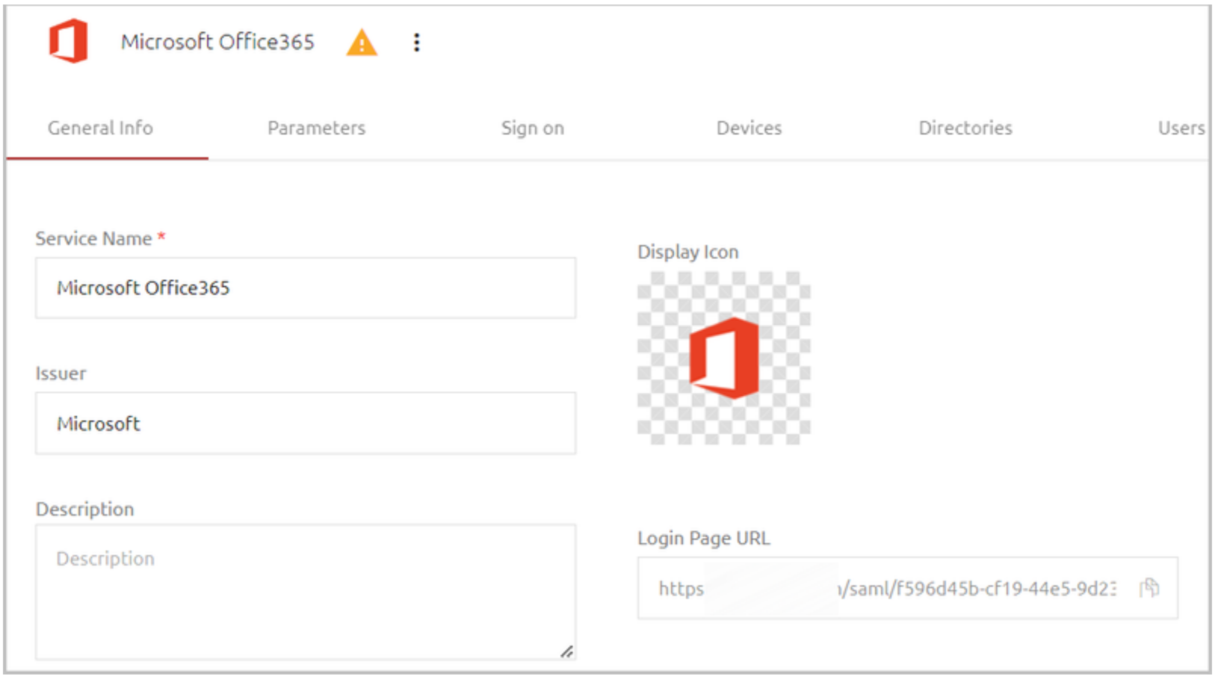
2. In the dialog that opens, update the default service name and issuer if desired. To change the display icon, click the tile and upload the logo of your choice (supported image size is 128x128 pixels). Then, click **Create**.



Service Name *: Microsoft Office365

Issuer: Microsoft

3. Review the settings in the **General Info** tab. If you add a description or update other settings, click **Save**.



Service Name *: Microsoft Office365

Issuer: Microsoft

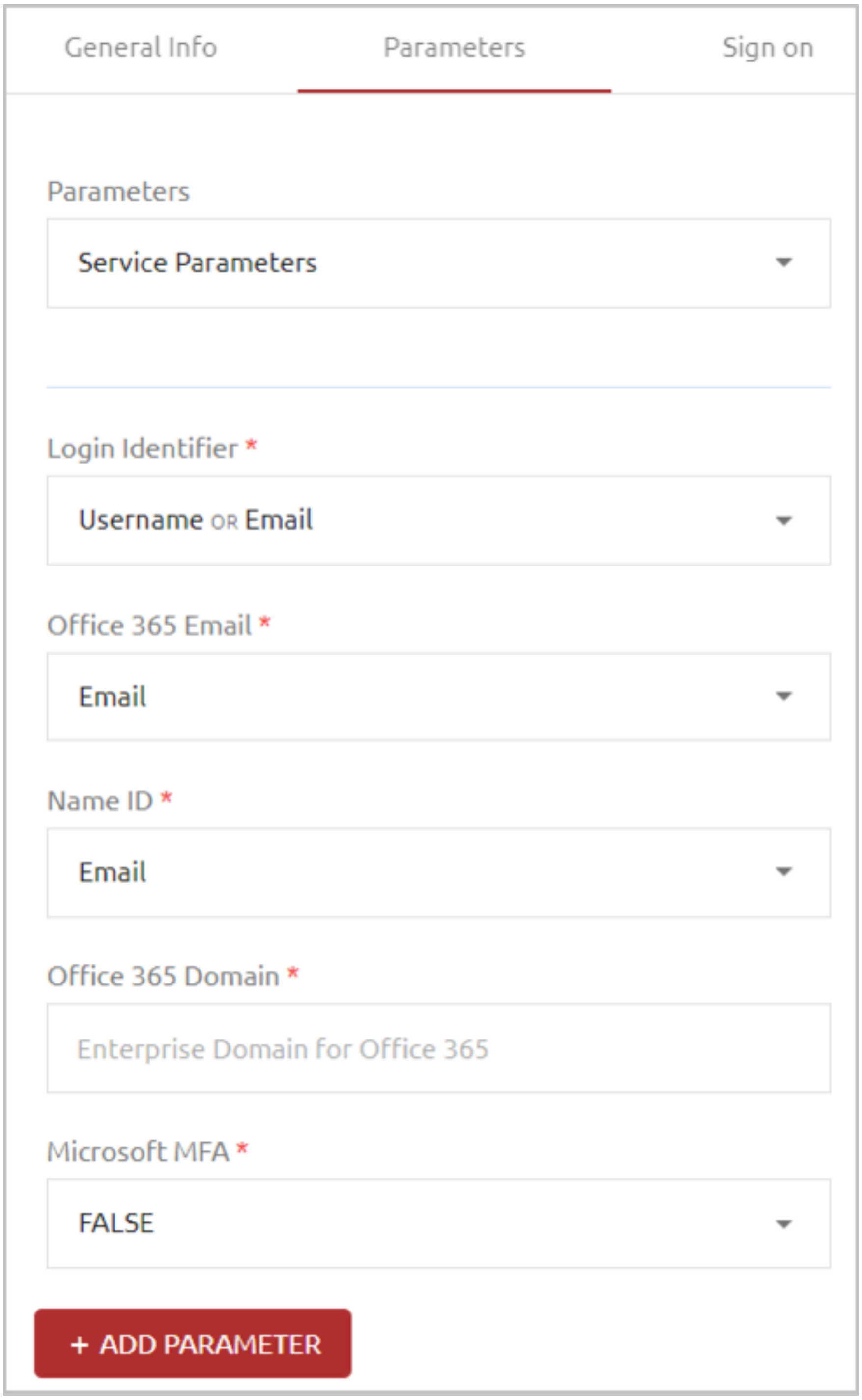
Description: Description

Login Page URL: https /saml/f596d45b-cf19-44e5-9d2

4. Add directories, users and groups to the service. For details, refer to Creating a Service and Assigning Users.

5. Open the **Parameters** tab and configure the following settings.

| Setting | Value / Notes |
|---|---|
| Login Identifier | Login method for the Octopus Authentication Server. Select **Email**. |
| Office 365 Email | Select **Email**. |
| Name ID | Select **Alias 1**. |
| Office 365 Domain | Enter the Office 365 new Intermediary email domain. |
| Microsoft MFA | The default value is FALSE. When set to TRUE, after the user is successfully authenticated by Octopus Authenticator, Microsoft will request additional authentication on the Microsoft authenticator. |



Parameters: Service Parameters

Login Identifier *: Username OR Email

Office 365 Email *: Email

Name ID *: Email

Office 365 Domain *: Enterprise Domain for Office 365

Microsoft MFA *: FALSE

If you wish, you may click **Add Parameter** to create additional optional parameters that are commonly added to SAML services. For a list of these parameters, refer to Generic SAML Service Parameters.

**Important**

To support FIDO authentication, add the *windowsFidoLogin* parameter with any value (e.g., TRUE).

When using this parameter, the **Check Password** and **Force Login Page** options (on the **Sign on** tab) need to be enabled.

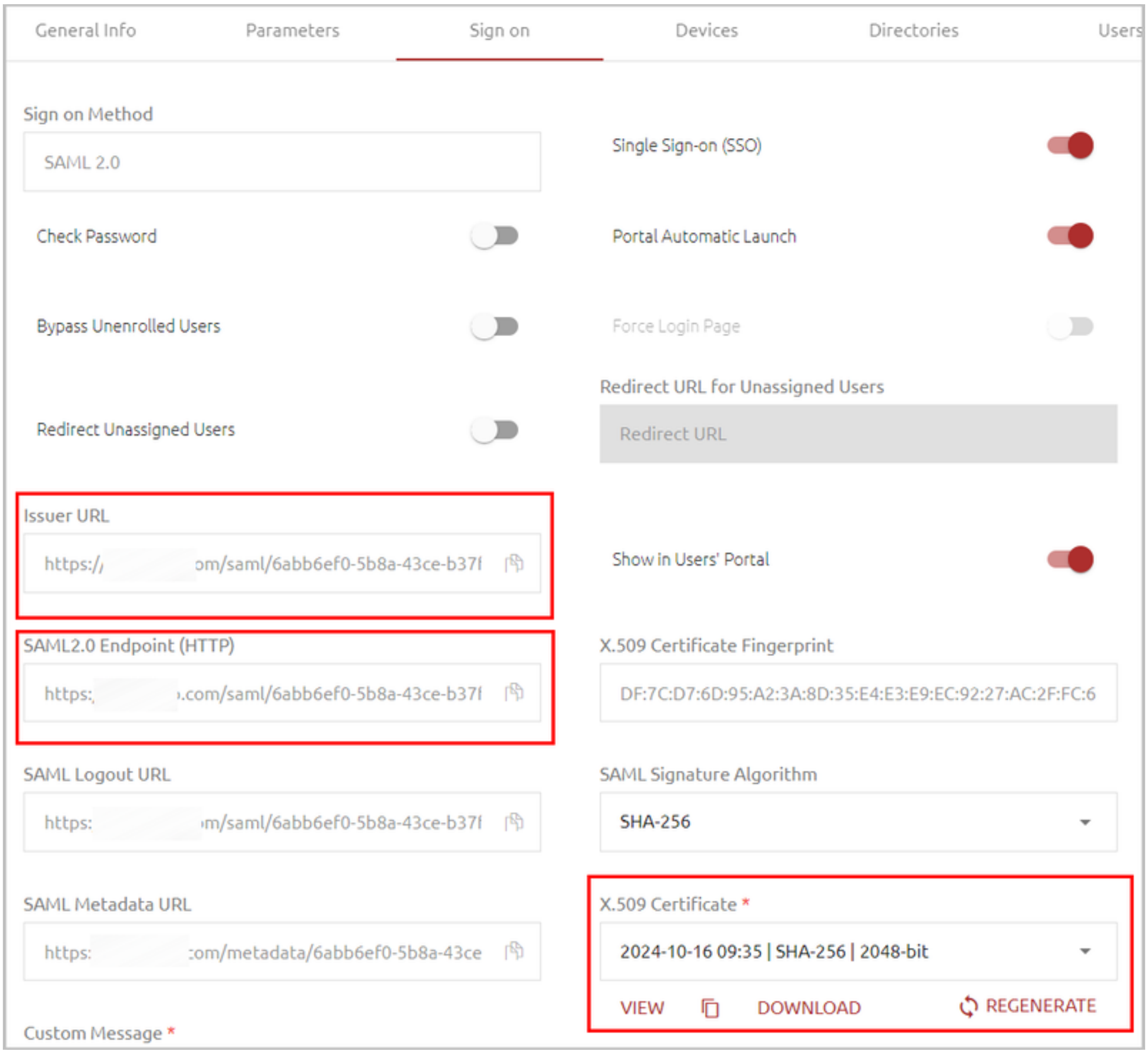
6. At the bottom of the **Parameters** tab, click **Save**.

7. Open the **Sign on** tab and copy or download the following elements:

   ○ **Issuer URL:** The URL used by the Microsoft Office 365 service to connect to Octopus Authenticator. Click the Copy icon to copy the URL.

   ○ **SAML2.0 Endpoint (HTTP):** The Octopus Authenticator Office 365 Login page URL to which the Microsoft Office 365 service provider will refer users for Octopus authentication. Click the Copy icon to copy the URL.

   ○ **X.509 Certificate:** Click **Download** to download the **cert.pem** file.



Sign on Method: SAML 2.0

Single Sign-on (SSO): ●

Check Password: ○

Portal Automatic Launch: ●

Bypass Unenrolled Users: ○

Force Login Page: ○

Redirect URL for Unassigned Users: Redirect URL

Redirect Unassigned Users: ○

Issuer URL: https:/ om/saml/6abb6ef0-5b8a-43ce-b37f

Show in Users' Portal: ●

SAML2.0 Endpoint (HTTP): https: .com/saml/6abb6ef0-5b8a-43ce-b37f

X.509 Certificate Fingerprint: DF:7C:D7:6D:95:A2:3A:8D:35:E4:E3:E9:EC:92:27:AC:2F:FC:6

SAML Logout URL: https: m/saml/6abb6ef0-5b8a-43ce-b37f

SAML Signature Algorithm: SHA-256

SAML Metadata URL: https: com/metadata/6abb6ef0-5b8a-43ce

X.509 Certificate *: 2024-10-16 09:35 | SHA-256 | 2048-bit

Custom Message *

You will need these elements for the configurations in Office 365.

8. Set up SSO for the Office365 Web Service and the Mobile Outlook App using Octopus Authenticator as a third party IDP. For details, refer to the integration document: How to Configure Octopus Authentication for Microsoft Office 365.

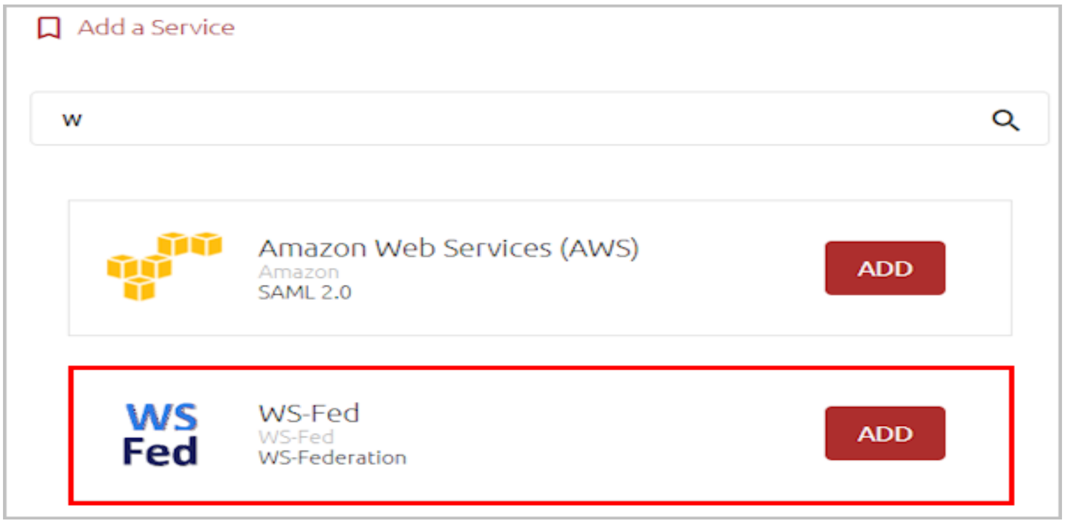
## Configuring WS-Fed Service Integration

WS-Federation provides a general mechanism for allowing authentication across different security boundaries in various security realms, for the purpose of creating a federation of security realms. The WS-Fed service enables integration between the Octopus Authenticator and the WS-Federation mechanism. This process enables full-scale integration with Entra ID, allowing use of the Octopus platform on Entra ID domain-joined machines. It also supports integration with mobile device management systems, such as Microsoft Intune.

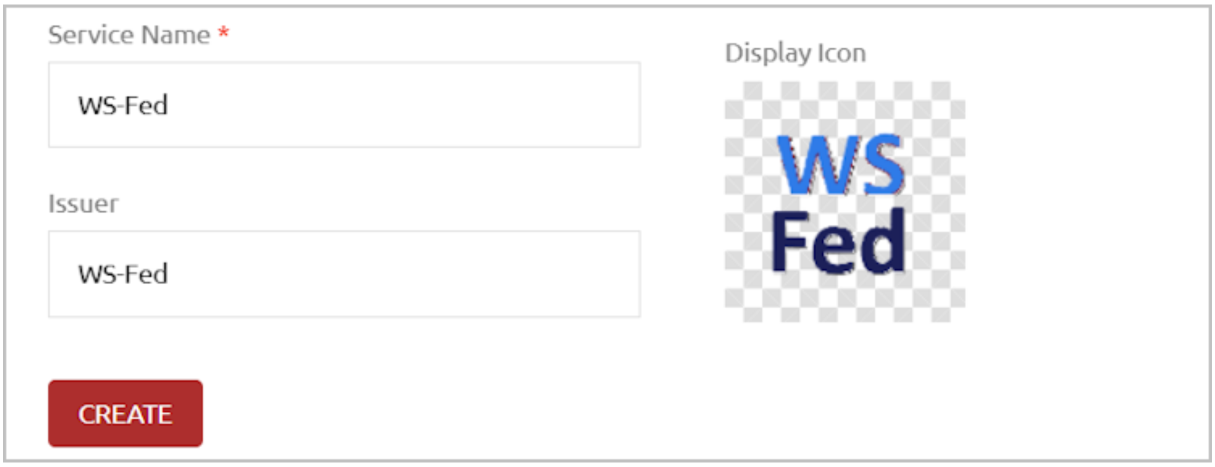
For successful integration, you need to create the service in the Management Console, and then federate the Entra ID domain with WS-Federation to Enterprise Connect Passwordless. The following procedure provides a summary of the integration process. For full details and instructions, please refer to the document How to Configure Octopus Authentication for Microsoft Office 365.

**To configure WS-Federation integration:**

1. In the Management Console, open the **Services** menu and click **Add Service**. In the **WS-Fed** tile, click **Add**.



2. In the dialog that opens, update the default service name and issuer if desired. To change the display icon, click the tile and upload the logo of your choice (supported image size is 128x128 pixels). Then, click **Create**.



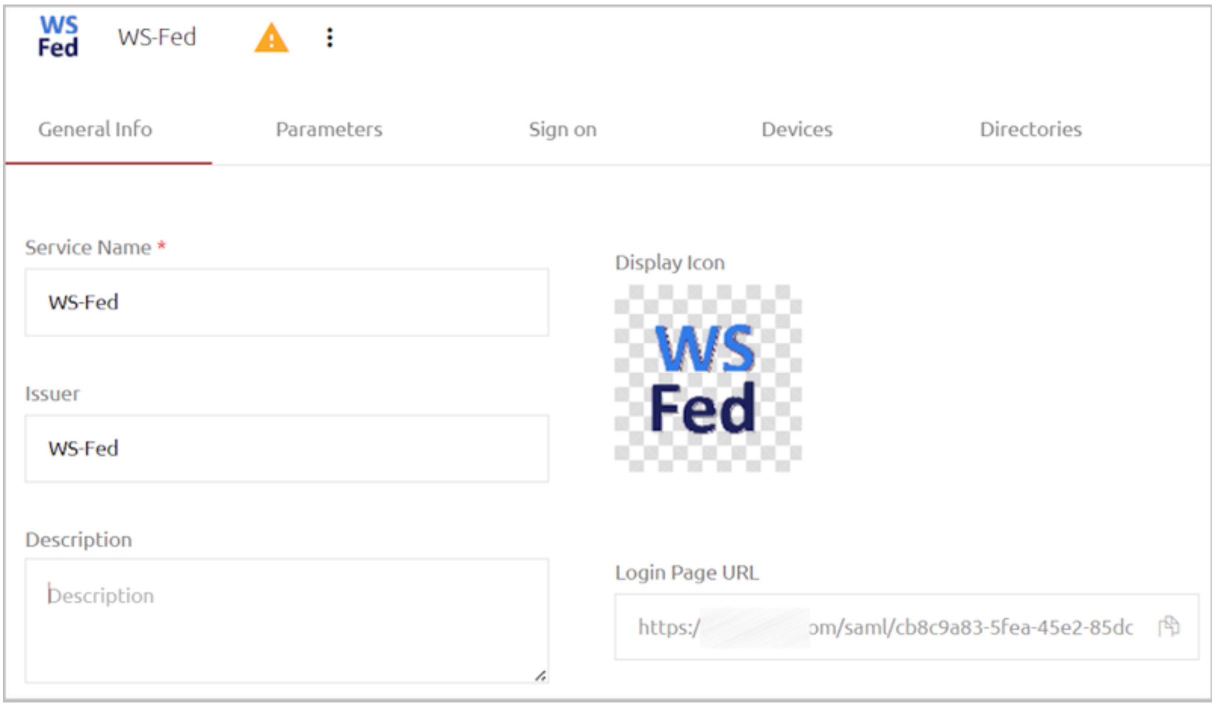
Service Name *

WS-Fed

Issuer

WS-Fed

3. Review the settings in the **General Info** tab. If you add a description or update other settings, click **Save**.



WS-Fed

General Info | Parameters | Sign on | Devices | Directories

Service Name *

WS-Fed

Issuer

WS-Fed

Description

Description

Display Icon

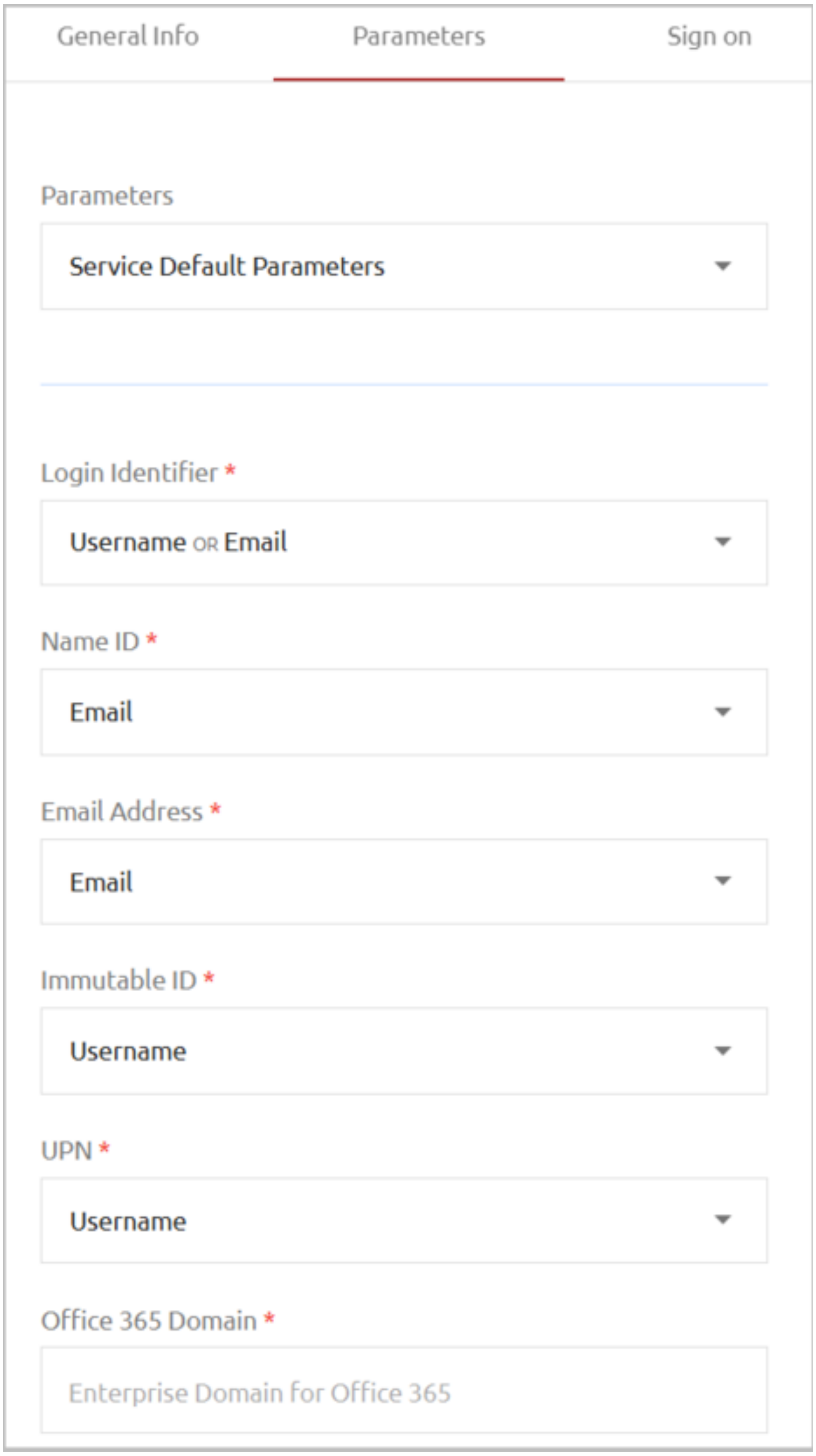
Login Page URL

https:/[redacted]om/saml/cb8c9a83-5fea-45e2-85dc

4. Add directories, users and groups to the service. For details, refer to Creating a Service and Assigning Users.

5. Open the **Parameters** tab and configure the following settings:

| Setting | Value / Notes |
|---|---|
| Login Identifier | Login method for the Octopus Authentication Server. Select **Email**. |
| Name ID | The attribute in the user's profile used for identifying the user. Select **Email**. |
| Email Address | Select **Email**. |
| Immutable ID | A unique attribute for identifying the user in Entra ID. Select **Username**. You will override this parameter with GUID in the next step.) |
| UPN | A unique identifier for the user account. Select **Username**. (You will override this parameter with UPN in the next step.) |
| Office 365 Domain | Enter the Entra ID domain. |



General Info | Parameters | Sign on

Parameters: Service Default Parameters

Login Identifier *: Username OR Email

Name ID *: Email

Email Address *: Email

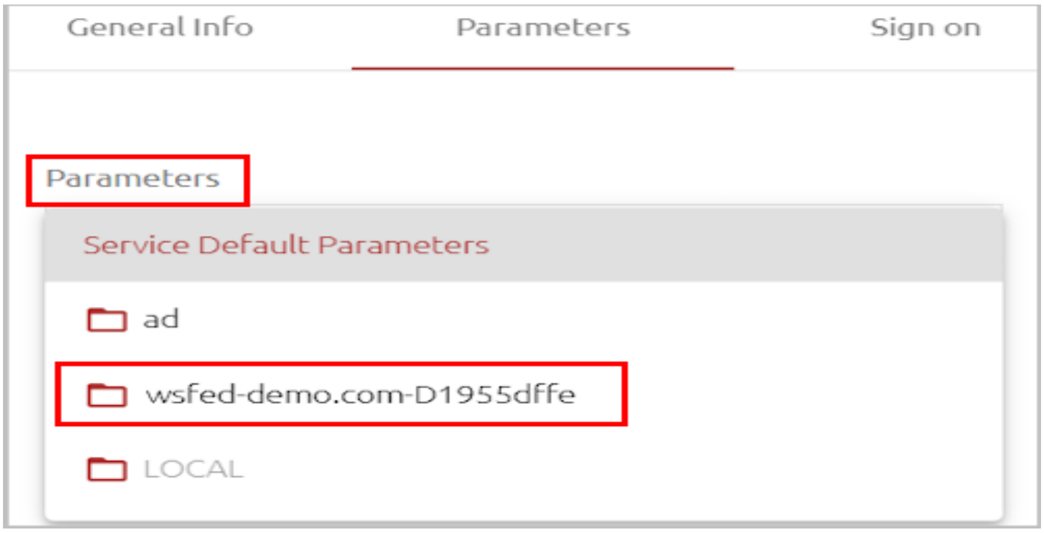
Immutable ID *: Username

UPN *: Username

Office 365 Domain *: Enterprise Domain for Office 365

6. Override the Name ID and UPN parameters:

   a. At the top of the **Parameters** tab, open the **Parameters** list and select the relevant directory.



General Info | Parameters | Sign on

Parameters

Service Default Parameters

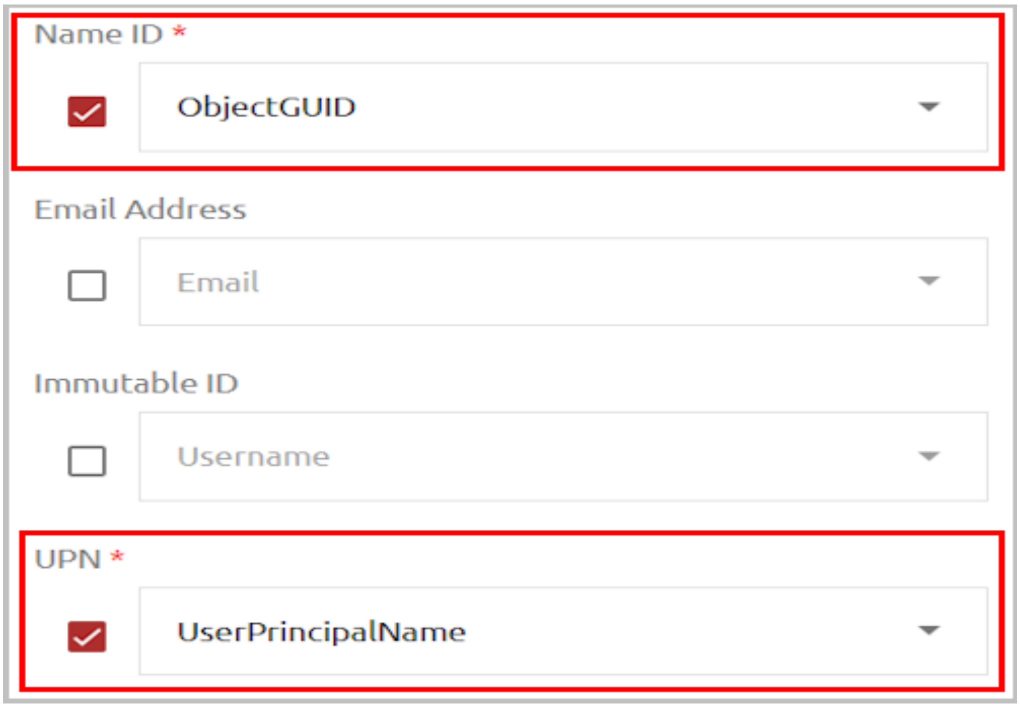
ad

wsfed-demo.com-D1955dffe

LOCAL

b. Select the checkbox next to the **Name ID** parameter. Then, open the dropdown list and select **ObjectGUID**.

c. Select the checkbox next to the **UPN** parameter. Then, open the dropdown list and select **UserPrincipalName**.



Name ID *

☑ ObjectGUID

Email Address

□ Email

Immutable ID

□ Username

UPN *

☑ UserPrincipalName

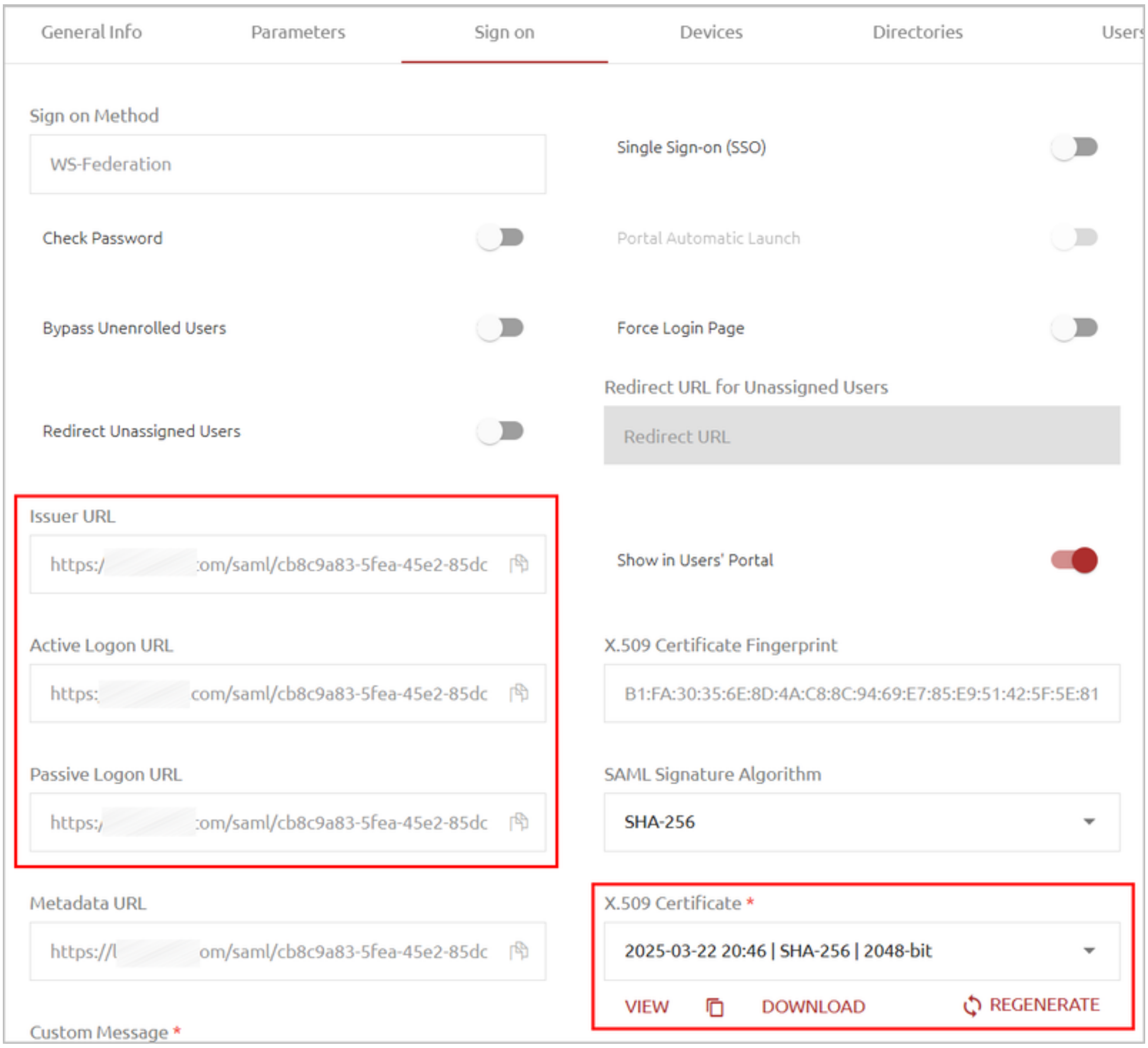
d. Click **Save**.

7. Open the **Sign on** tab and copy or download the following elements:

    ○ **Issuer URL:** The URL used by the WS-Fed service to connect to Octopus Authenticator. Click the Copy icon to copy the URL.

    ○ **Active Logon URL:** The URL used for handling active user authentication traffic. Click the Copy icon to copy the URL.

- ○ **Passive Logon URL:** The URL used for handling authentication traffic in which the requester (e.g., a web browser) is not actively aware of the federation processes taking place. Click the Copy icon to copy the URL.
- ○ **X.509 Certificate:** Click **Download** to download the **cert.pem** file.



Sign on Method: WS-Federation

Single Sign-on (SSO)

Check Password

Portal Automatic Launch

Bypass Unenrolled Users

Force Login Page

Redirect URL for Unassigned Users: Redirect URL

Redirect Unassigned Users

Issuer URL: https:/[redacted]:om/saml/cb8c9a83-5fea-45e2-85dc

Show in Users' Portal

Active Logon URL: https:[redacted]com/saml/cb8c9a83-5fea-45e2-85dc

X.509 Certificate Fingerprint: B1:FA:30:35:6E:8D:4A:C8:8C:94:69:E7:85:E9:51:42:5F:5E:81

Passive Logon URL: https:/[redacted]:om/saml/cb8c9a83-5fea-45e2-85dc

SAML Signature Algorithm: SHA-256

Metadata URL: https://l[redacted]om/saml/cb8c9a83-5fea-45e2-85dc

X.509 Certificate *: 2025-03-22 20:46 | SHA-256 | 2048-bit

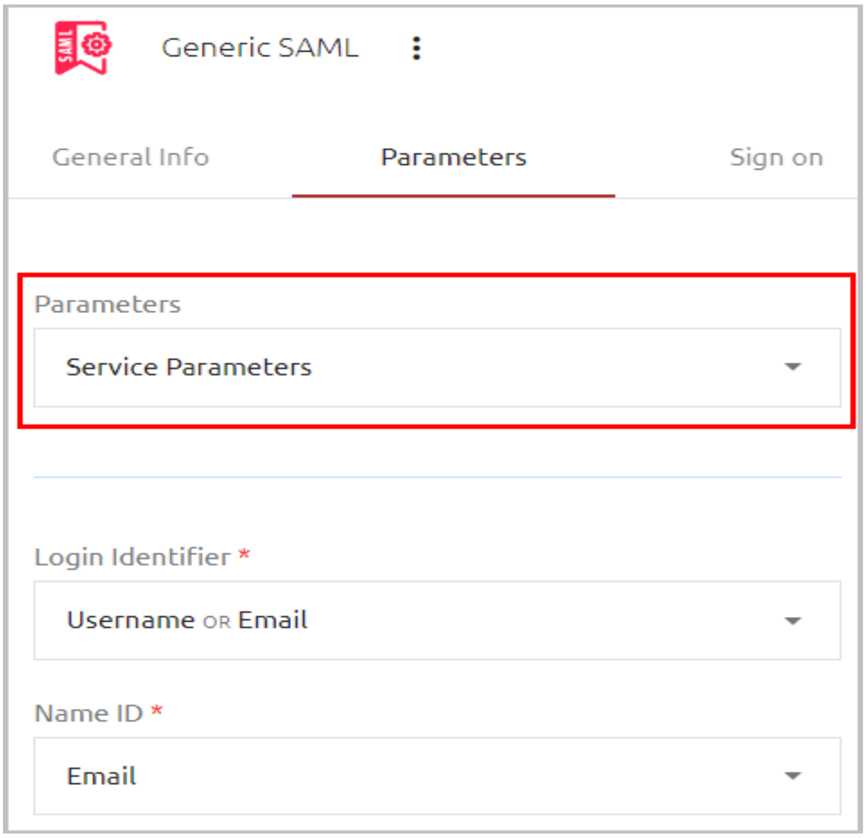
Custom Message *

You will need these elements to federate your Entra ID domain.

8. Federate the Entra ID domain with WS-Federation to Enterprise Connect Passwordless. For details, refer to Appendix B of the document How to Configure Octopus Authentication for Microsoft Office 365.

## Overriding Default Service Parameters

Parameters are service-side settings that the Management Console needs for successful service integration. The set of required parameters are service-specific, and can be viewed in the **Parameters** tab of the service settings.

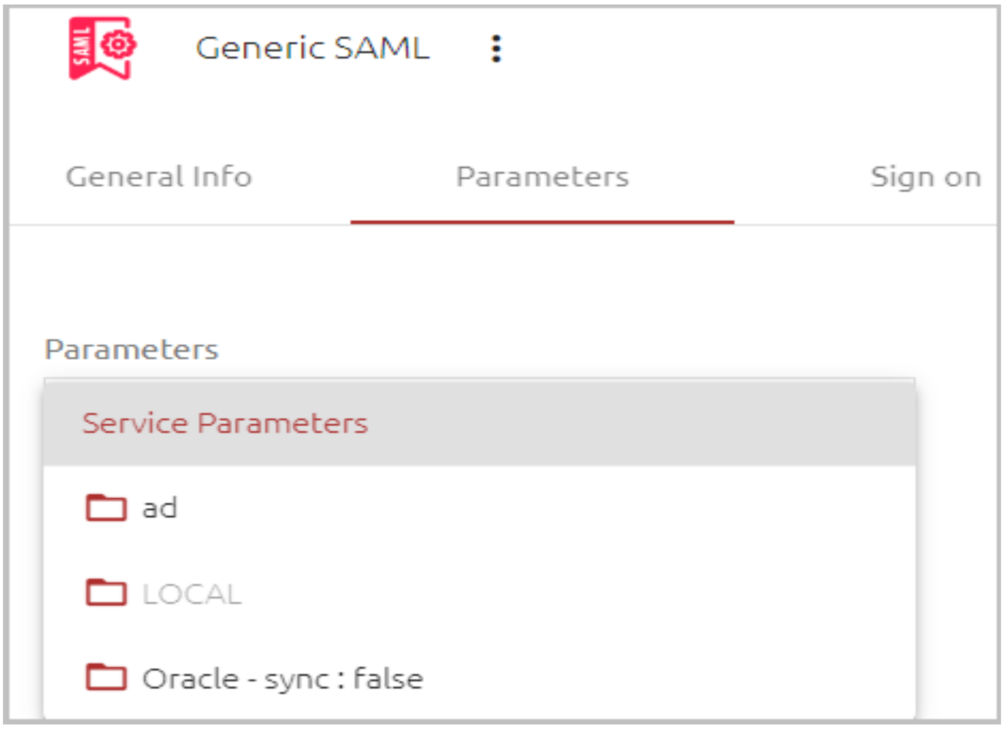


Parameters: Service Parameters

Login Identifier *: Username OR Email

Name ID *: Email

The settings that you specify for **Service Parameters** are the default parameters used for authentication to the service. In addition, the Management Console supports defining directory-specific parameters that override default service parameters.



For example, let's say that in most directories, the user identifier sent to the service (the **Name ID** parameter) is **Email**. However, the identifier recognized for Oracle users is

**Username**. In cases like this, you can define a **Name ID** parameter for the Oracle directory that is different from the default parameter. The procedure below explains how to do it.

**To override default service parameters:**

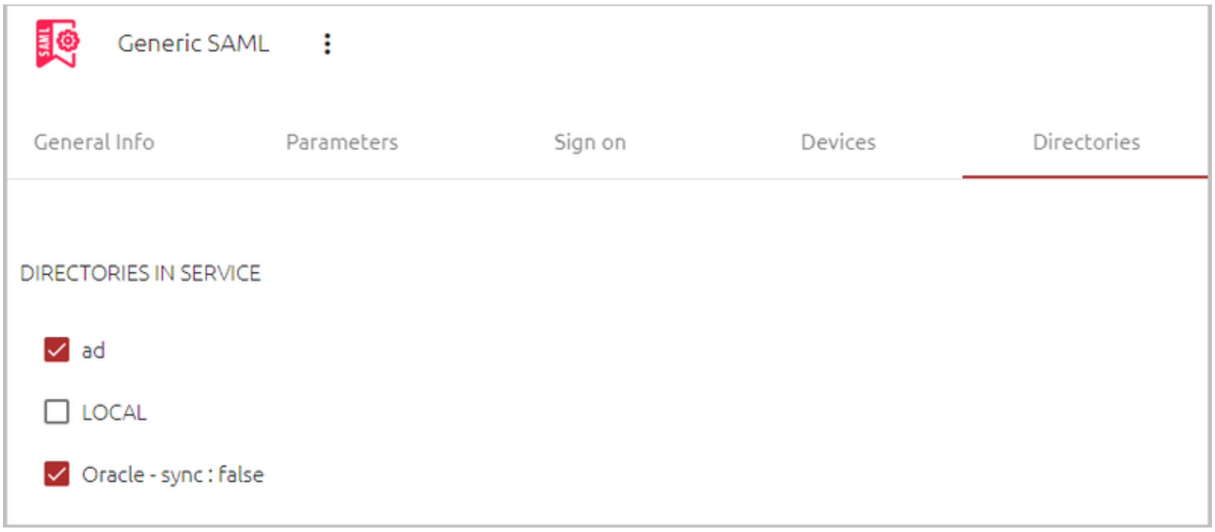
1. Open the settings of the relevant service. From the **Parameters** tab, open the **Service Parameters** dropdown list and check whether the directory for which you want to set override parameters is enabled.

   If the directory is enabled, skip to Step 4.

2. If the directory is disabled in the **Service Parameters** list, select the **Directories** tab.

   All the directories integrated with the Management Console are listed.

3. Select the directories for which you want to set override parameters. Then, click **Save**.



DIRECTORIES IN SERVICE

☑ ad

□ LOCAL

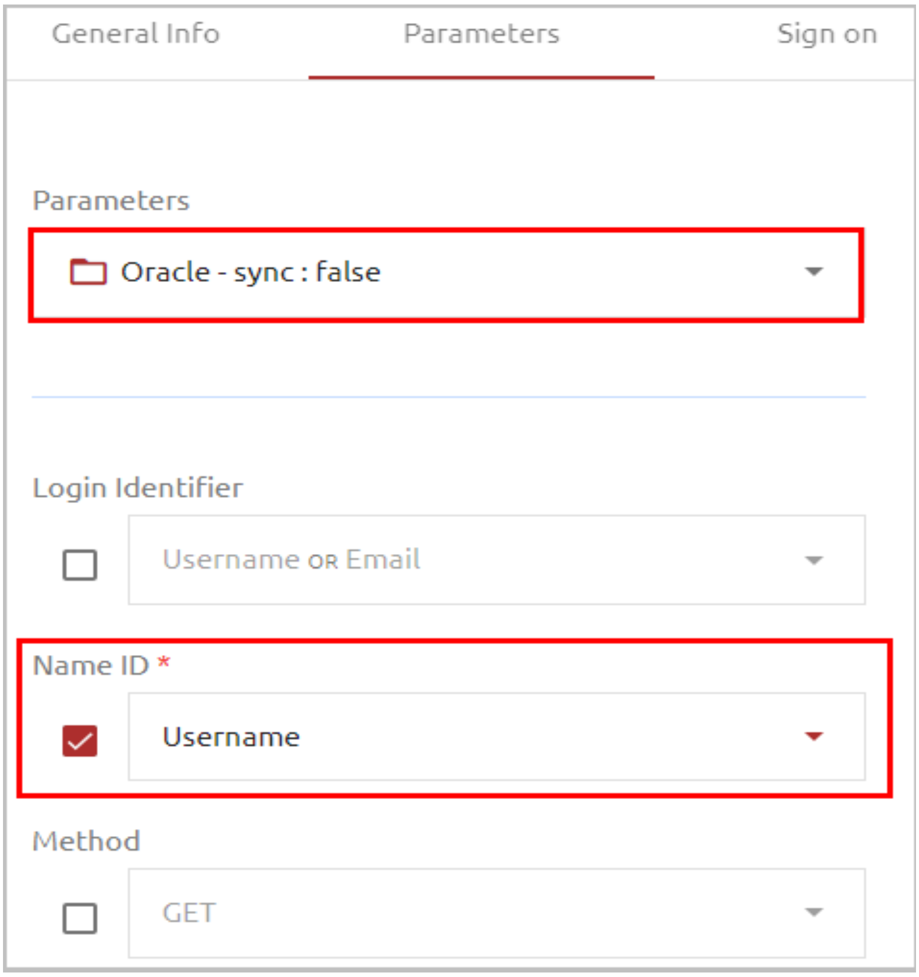
☑ Oracle - sync : false

   In the **Parameters** tab, the selected directories will now be enabled.

4. From the **Service Parameters** list, select the relevant directory.

   A list of parameters is displayed.

5. To override a parameter, select its checkbox and then specify its value.



Parameters

Oracle - sync : false

Login Identifier

□ Username OR Email

Name ID *

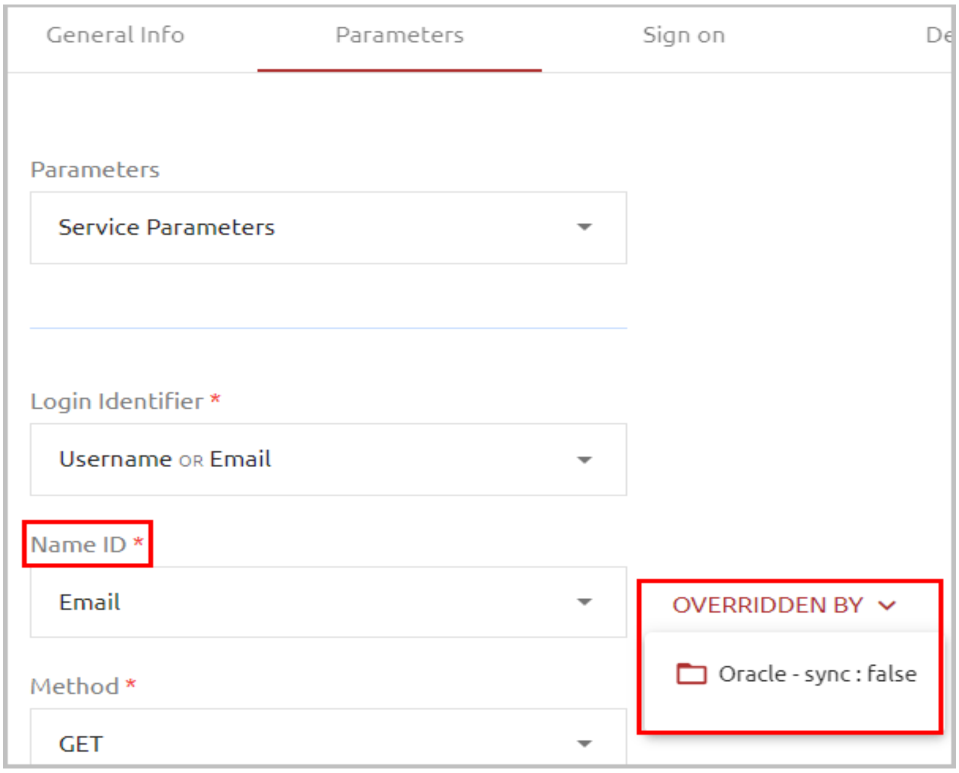
☑ Username

Method

□ GET

6. At the bottom of the tab, click **Save**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

   When default service parameters are displayed, parameters that have override settings are indicated by an **Overridden By** list. To view the override parameters, open the list and select the relevant directory.



Parameters

Service Parameters

Login Identifier *

Username OR Email

Name ID *

Email

OVERRIDDEN BY

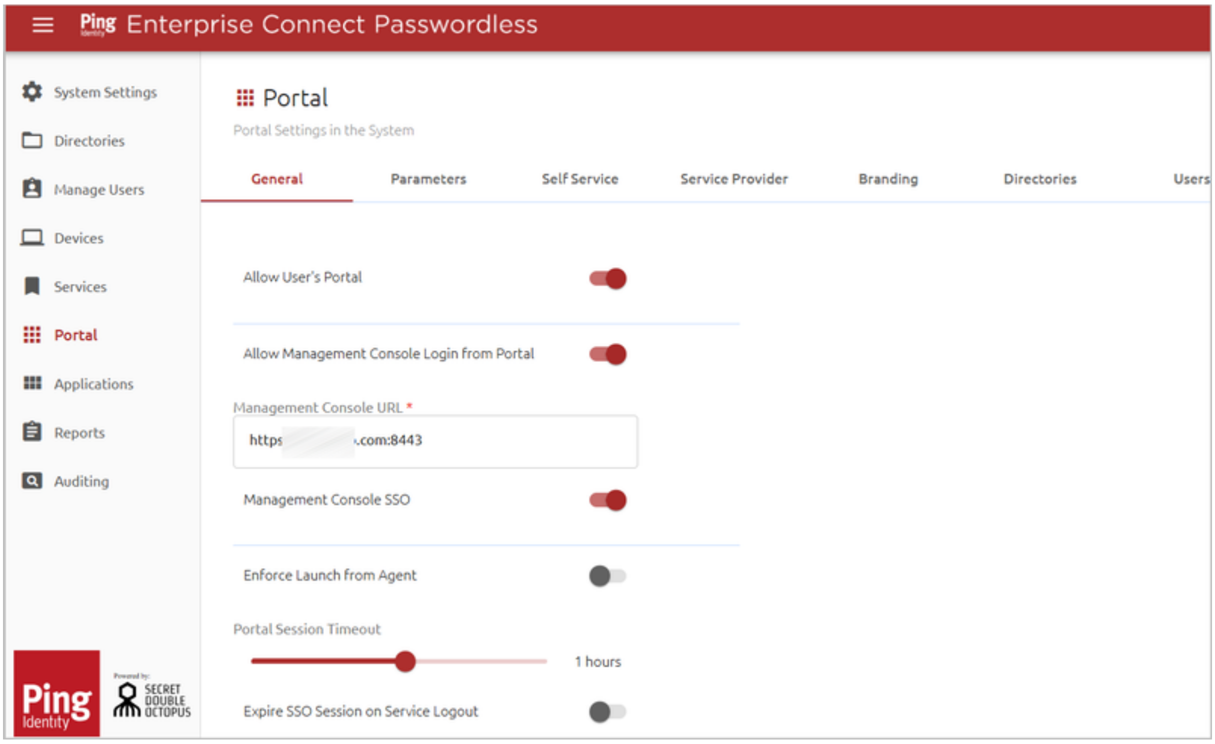
Oracle - sync : false

Method *

GET

## Managing Settings for the User Portal

The User Portal is a platform from which users can access services to which they are assigned and perform various self-service operations. The **Portal** menu of the Management Console enables you to control Portal settings, including the self-service actions that are available, the users who are authorized to access the Portal, and more.



Allow User's Portal ●

Allow Management Console Login from Portal ●

Management Console URL *

https .com:8443

Management Console SSO ●

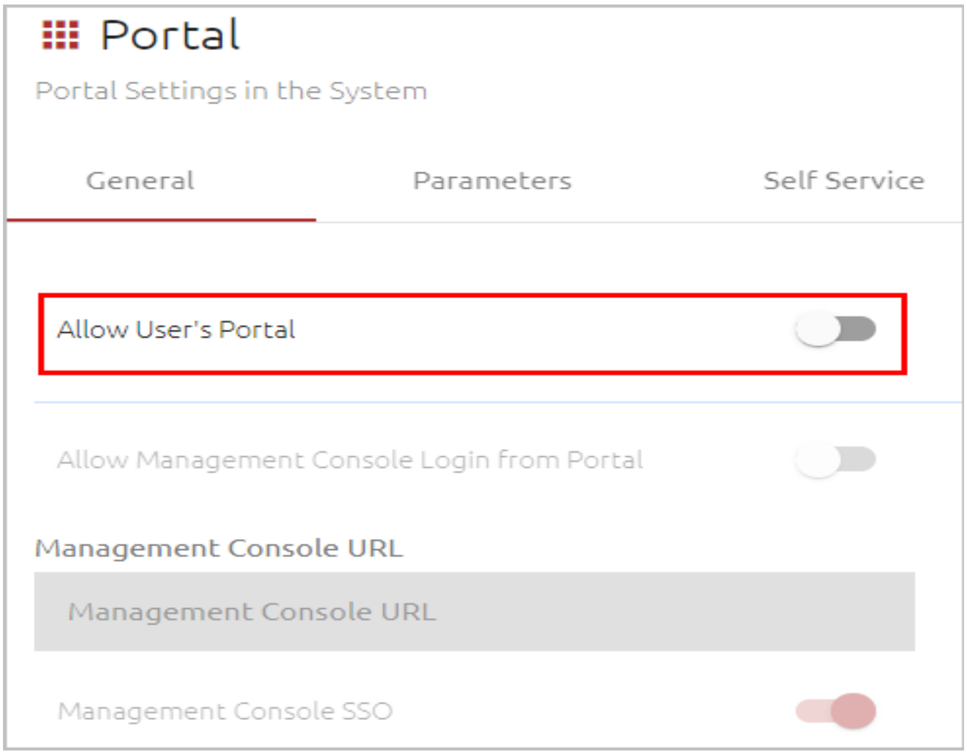
Enforce Launch from Agent ○

Portal Session Timeout

1 hours

Expire SSO Session on Service Logout ○

The **Allow User Portal** toggle is a global setting that determines whether the Portal is currently available to users. When this setting is off, all tabs and settings of the **Portal** menu are disabled.



Portal

Portal Settings in the System

Allow User's Portal

Allow Management Console Login from Portal

Management Console URL

Management Console URL

Management Console SSO

The following sections describe how to work with the **Portal** menu:

- User Portal General Settings
- Setting User Portal Parameters
- Managing User Portal Self Service Settings
- Customizing the User Portal
- Assigning Directories and Users to the Portal

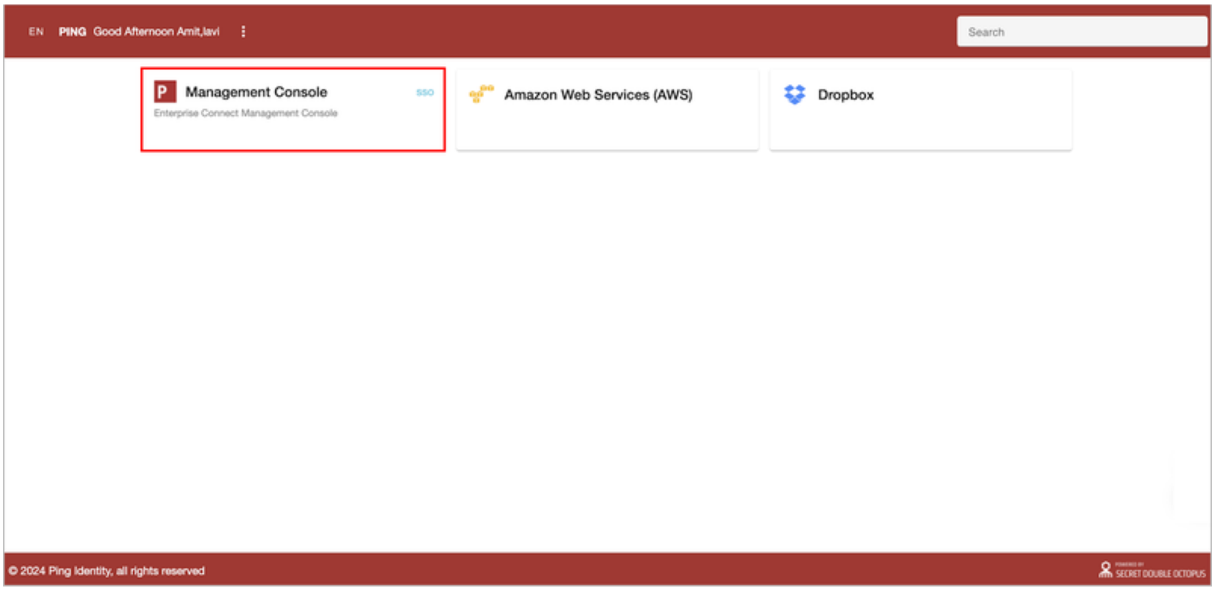
## User Portal General Settings

The **General** tab, which is displayed by default when you open the **Portal** menu, contains settings related to Portal access, session timeout and Management Console access details.

After updating settings in the **General** tab, click **Save**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

### Management Console Access Settings

The **Allow Management Console Login from Portal** setting determines whether the User Portal provides quick access to the Management Console (MC) for users who are authorized to access the MC (roles of Auditor, Helpdesk and Admin). When the setting is enabled, a Management Console tile is displayed in the User Portal.



EN PING Good Afternoon Amit,lavi

Search

Management Console SSO
Enterprise Connect Management Console

Amazon Web Services (AWS)

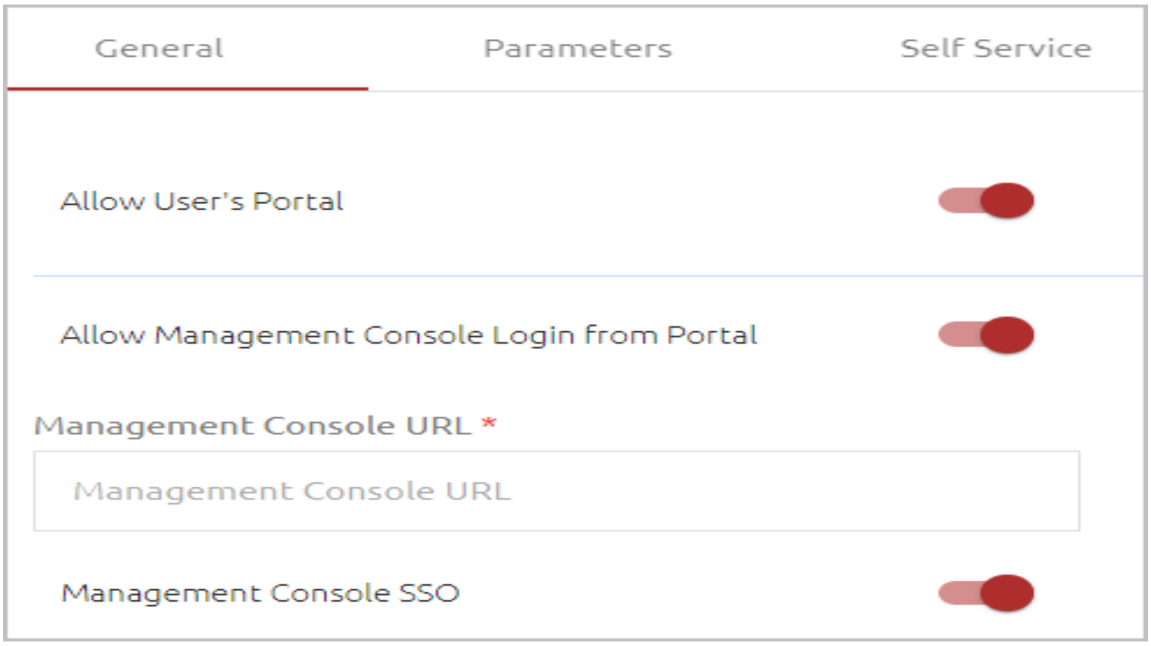
Dropbox

© 2024 Ping Identity, all rights reserved

POWERED BY SECRET DOUBLE OCTOPUS

When **Allow MC Login from Portal** is enabled, the following settings are also enabled:

- **Management Console URL:** This setting is required.
- **Management Console SSO:** When this setting is enabled, users logging into the MC from the Portal do not need to reauthenticate to access the MC.



General | Parameters | Self Service

Allow User's Portal

Allow Management Console Login from Portal

Management Console URL *

Management Console URL

Management Console SSO

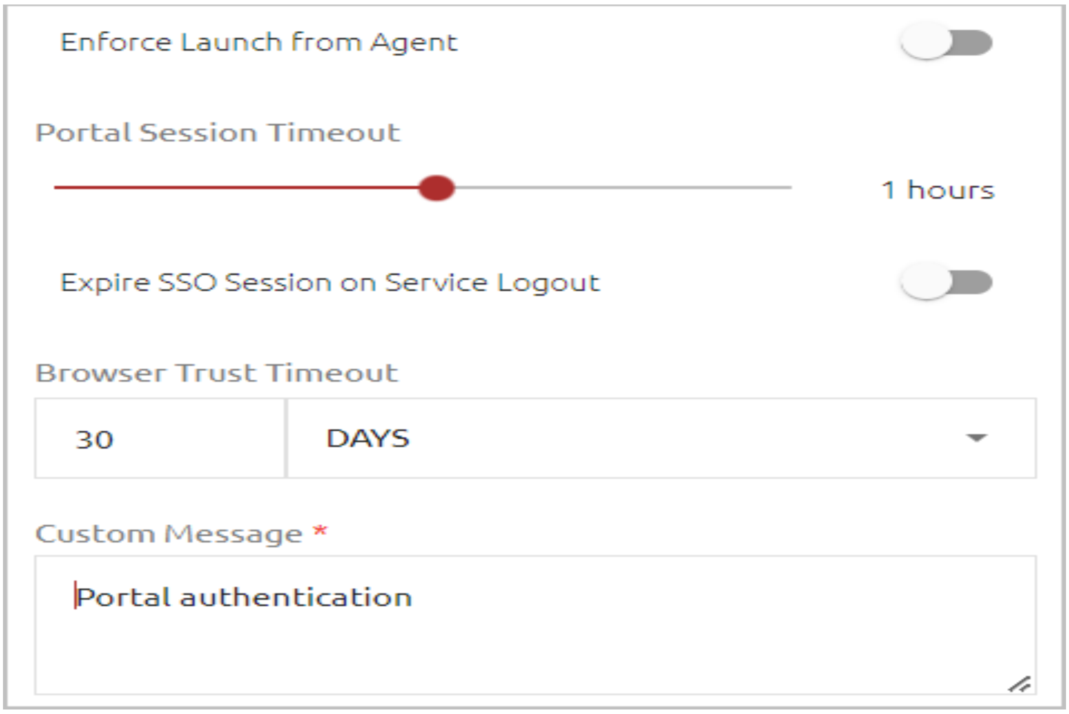
### Portal Security and Authentication Settings

The following settings appear at the bottom of the **General** tab:

- **Enforce Launch from Agent:** When this setting is enabled, the Portal can be accessed only from the user's workstation, via the Windows / Mac Agent. (Manual Portal login through a browser is disabled.)
- **Portal Session Timeout:** Determines the maximum length of a User Portal session. The session timeout can range from 1 minute to 24 hours (default is 1

hour). To update the setting, drag the slider to specify the desired value and then click **Save**.

- **Expire SSO Session on Service Logout:** When this setting is enabled, the entire SSO session ends automatically when the user logs out of an SSO service.
- **Browser Trust Timeout:** This setting, which is relevant when Adaptive Authentication is enabled, determines the period of time for which strong authentication is not required on browsers that are designated as Trusted devices. When the specified timeout elapses, users will be prompted to enter a verification code when authenticating from these browsers. Valid timeout periods range from 1 hour to 12 months (default is 30 days).
- **Custom Message:** The message displayed to users on successful authentication to the Portal. Enter the text of your choice in the field.



Enforce Launch from Agent

Portal Session Timeout

1 hours

Expire SSO Session on Service Logout

Browser Trust Timeout

30

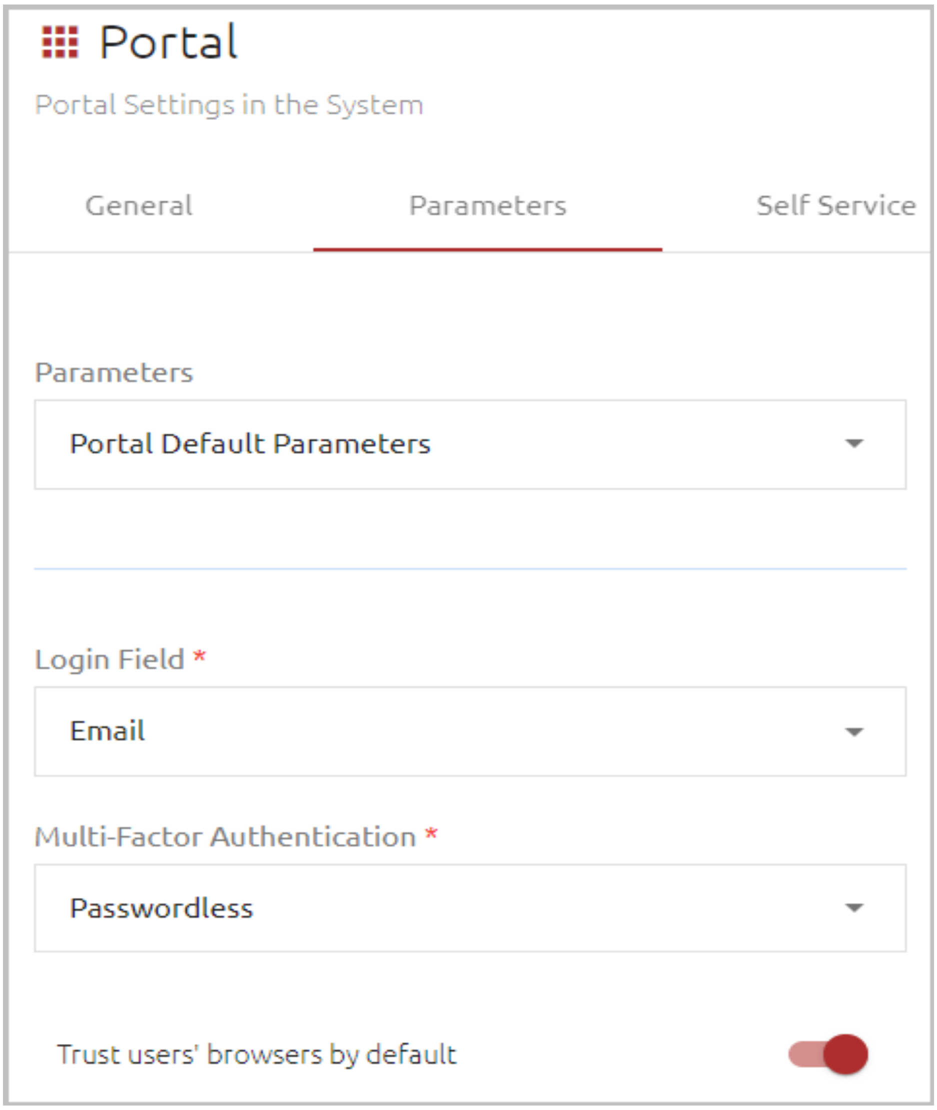
DAYS

Custom Message *

Portal authentication

## Setting User Portal Parameters

The **Parameters** tab contains settings related to the process of authenticating to the User Portal.



Portal

Portal Settings in the System

Parameters: Portal Default Parameters

Login Field *: Email

Multi-Factor Authentication *: Passwordless

Trust users' browsers by default: ●

The settings are:

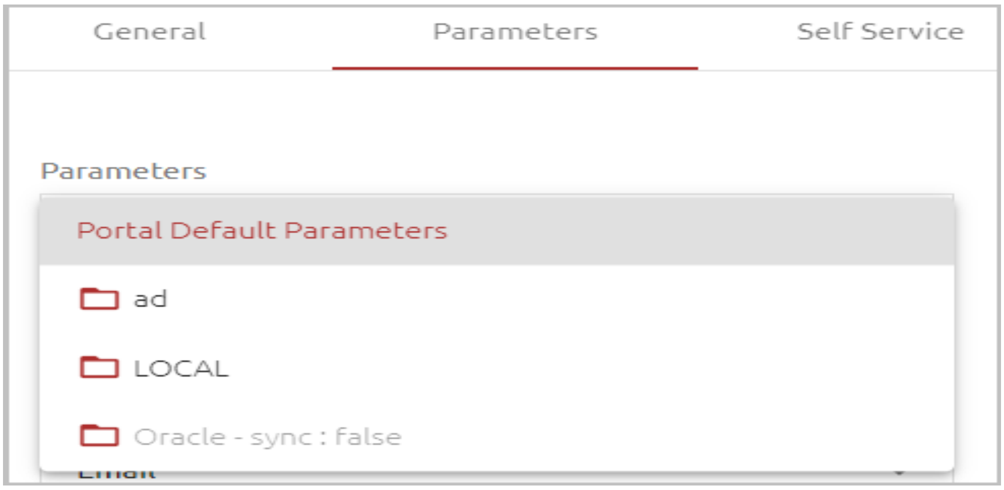
- **Login Field:** The identifier that the user enters on the Login screen of the User Portal (email, username, etc.). You may select more than one identifier type.

> **Note**
>
> If you select a field that is not unique (e.g., a user may have the same username in multiple directories), users need to enter *<domain>**<username>* on the Login screen.

- **Multi-Factor Authentication:** The MFA method used for Portal authentication:
  - **Passwordless:** Users enter only the Login parameter and MFA is done in the background.
  - **Username + Password (MFA):** Users provide the Login parameter as well as a password.
- **Trust users' browsers by default:** This setting is relevant when Adaptive Authentication is enabled. When the toggle is selected, the **Trust this browser** checkbox on Login screens of the User Portal and SAML services will be selected

by default. (When this checkbox is selected, the browser will be marked as a Trusted device after the first successful strong authentication.)

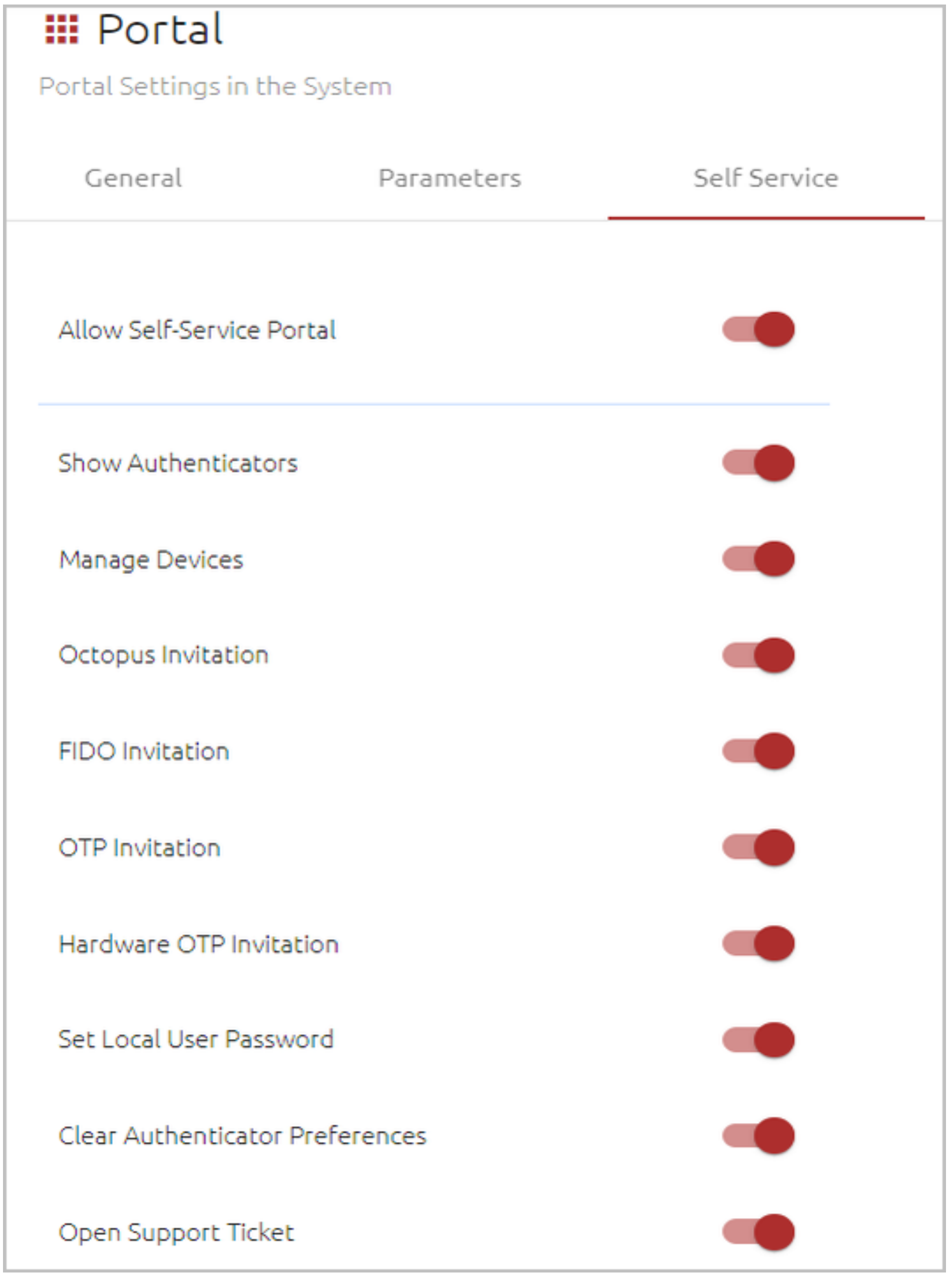
The **Parameters** dropdown list at the top of the tab enables you to define directory-specific parameters that override the Portal default parameters.



For more details and instructions for overriding parameters, refer to Overriding Default Service Parameters.

## Managing User Portal Self Service Settings

The **Self Service** tab contains settings that determine which self-service actions are available in the User Portal. Actions are enabled and disabled by clicking the relevant toggle buttons.



Portal

Portal Settings in the System

Allow Self-Service Portal ●

Show Authenticators ●

Manage Devices ●

Octopus Invitation ●

FIDO Invitation ●

OTP Invitation ●

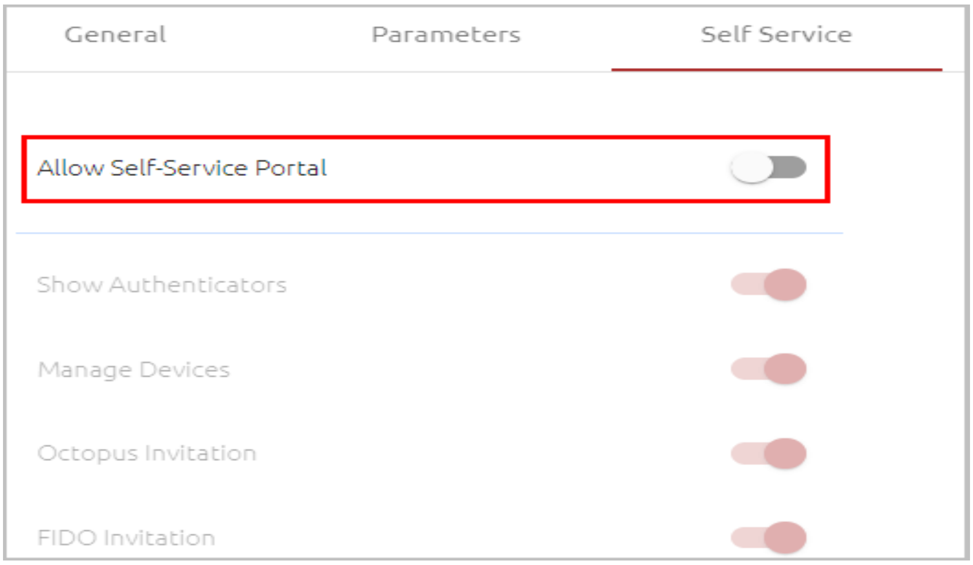
Hardware OTP Invitation ●

Set Local User Password ●

Clear Authenticator Preferences ●

Open Support Ticket ●

The **Allow Self-Service Portal** toggle is a global setting that determines whether any self-service actions appear in the Portal. When this setting is off, all other toggles in the tab are disabled.



Allow Self-Service Portal ○

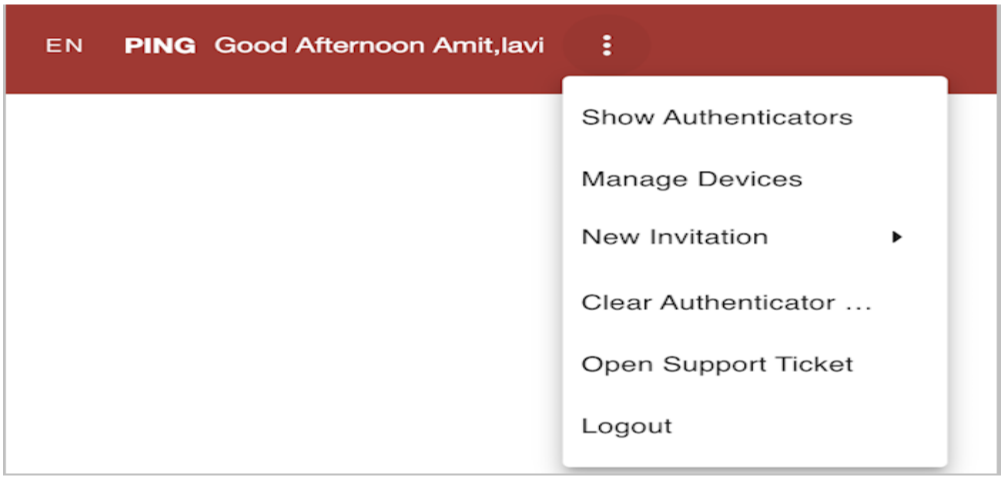
Show Authenticators ●

Manage Devices ●

Octopus Invitation ●

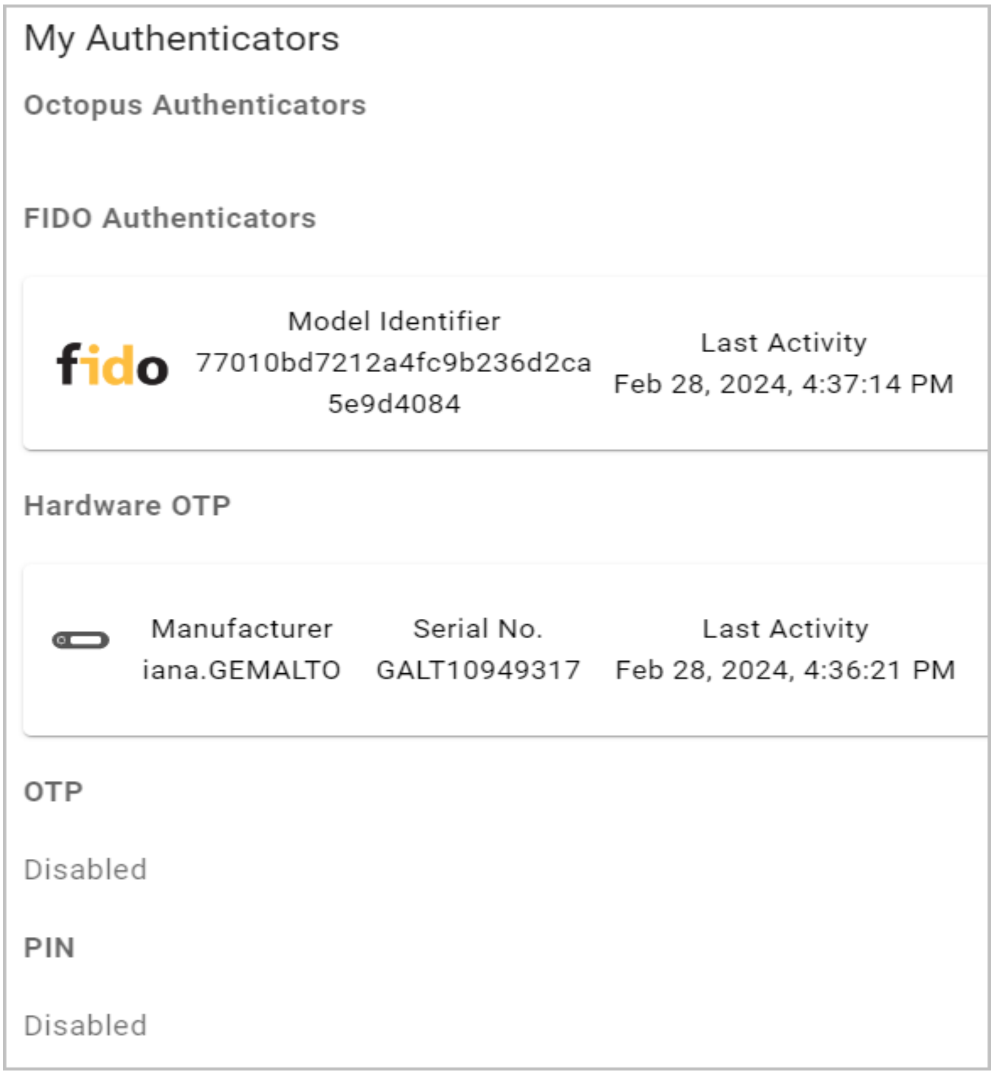
FIDO Invitation ●

When the **Allow Self-Service Portal** setting is on, the actions that are currently activated in the **Self Service** tab are displayed to users when they click the Actions icon of the User Portal.



The self-service actions are:

- **Show Authenticators:** When this setting is enabled, users are able to open a popup displaying basic information about all the devices they have used for authentication.



My Authenticators

Octopus Authenticators

FIDO Authenticators

| Model Identifier | Last Activity |
|---|---|
| 77010bd7212a4fc9b236d2ca5e9d4084 | Feb 28, 2024, 4:37:14 PM |

Hardware OTP

| Manufacturer | Serial No. | Last Activity |
|---|---|---|
| iana.GEMALTO | GALT10949317 | Feb 28, 2024, 4:36:21 PM |

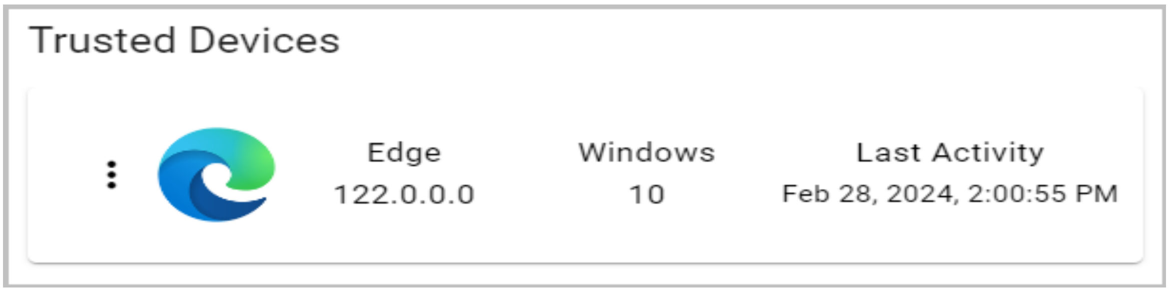
OTP

Disabled

PIN

Disabled

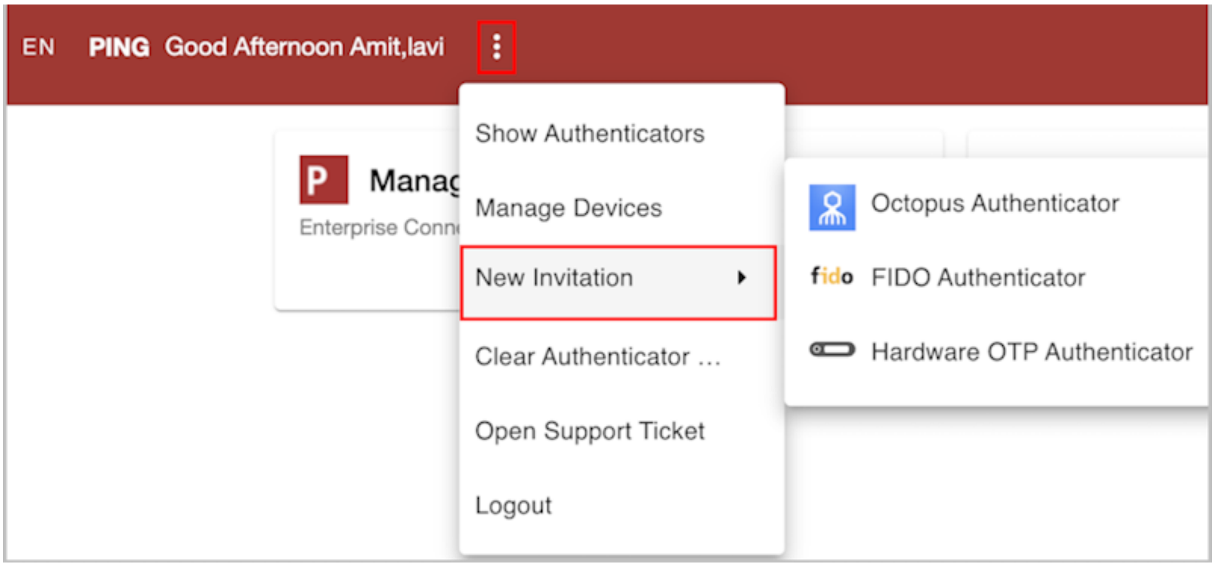
- **Manage Devices:** When this setting is enabled, users are able to view a popup displaying basic information about all the browsers they have used for authentication. Users are able to remove the browser from the list by clicking the Actions icon and selecting **Delete.**



Trusted Devices

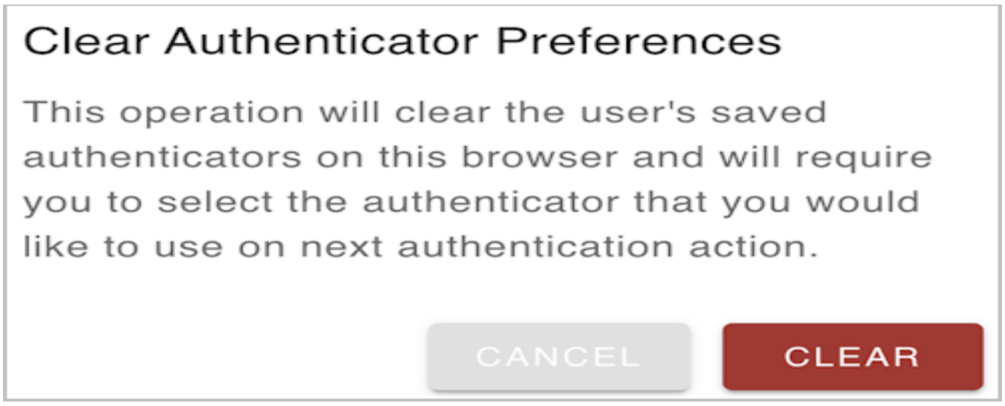
| Edge | Windows | Last Activity |
|---|---|---|
| 122.0.0.0 | 10 | Feb 28, 2024, 2:00:55 PM |

- **New Invitation:** This action enables users to send enrollment invitations to themselves so they can enroll additional devices in the system. The invitation types that are available in the User Portal are determined by the **Invitation** settings that are enabled in the **Self Service** tab (Octopus, FIDO and software / hardware OTP).



- **Set Password:** When this setting is enabled, users in the LOCAL directory have the option to reset the password required for user verification in services that utilize multi-factor authentication. To reset the password, users select the **Set Password** self-service option and enter the new password in the **Set Password** popup.
- **Clear Authenticator Preferences:** This action enables users to remove data stored on the browser, such as the previously selected authentication method for accessing SAML services. After clearing preferences, users will need to specify an authentication method when they next access the service.

  To clear stored data, users select the **Clear Authenticator Preferences** self-service option and then click **Clear** in the confirmation popup.



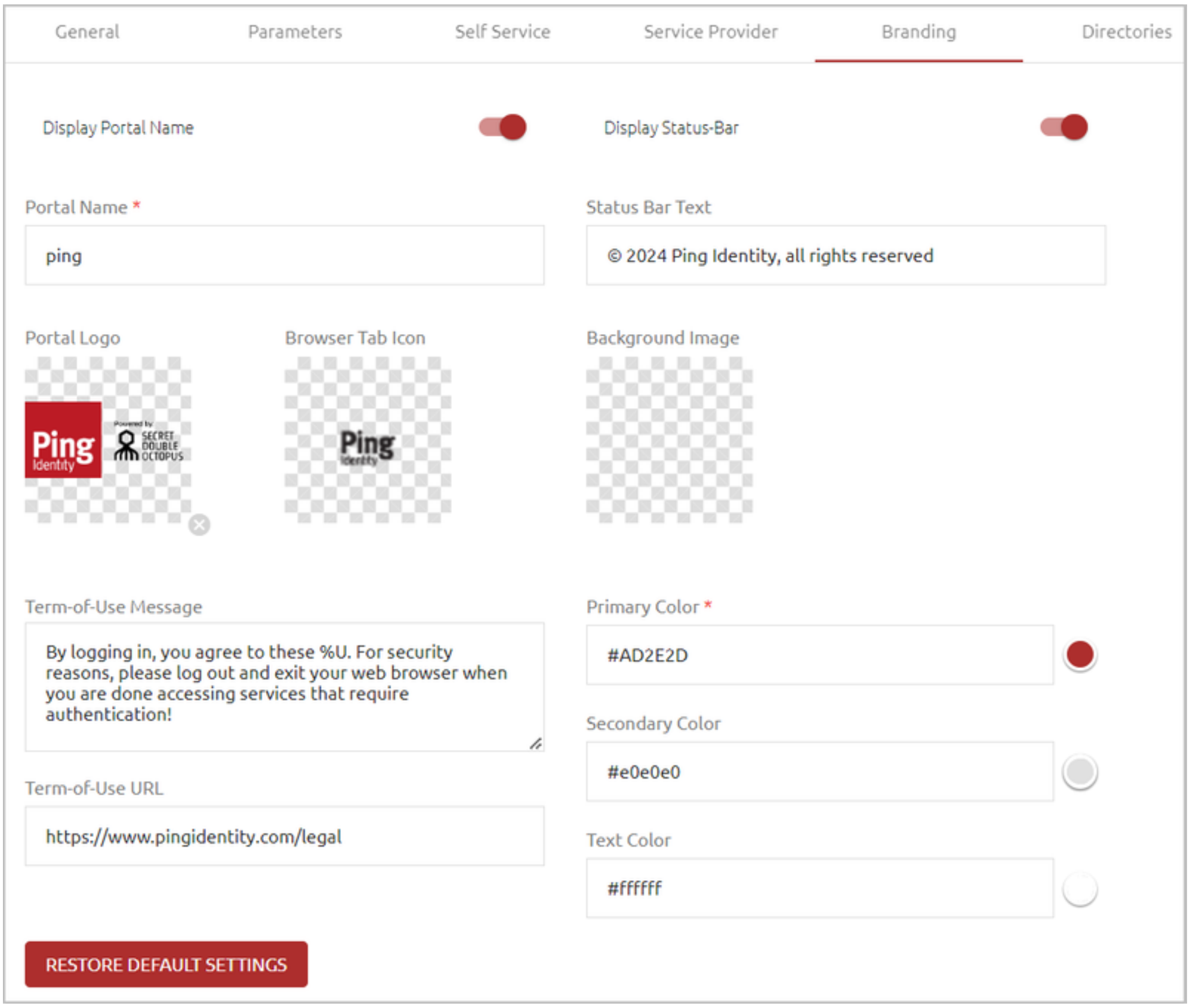
Clear Authenticator Preferences

This operation will clear the user's saved authenticators on this browser and will require you to select the authenticator that you would like to use on next authentication action.

- **Open Support Ticket:** When users select this action, an email message to the **Support Email** address (specified in **System Settings > General Settings**) is automatically created in the user's default email client.

### Customizing the User Portal

The **Branding** tab allows you to create a customized look and feel for the Portal using colors, images and texts that are specific to your organization.



Display Portal Name ●

Display Status-Bar ●

Portal Name *

ping

Status Bar Text

© 2024 Ping Identity, all rights reserved

Portal Logo

Browser Tab Icon

Background Image

Term-of-Use Message

By logging in, you agree to these %U. For security reasons, please log out and exit your web browser when you are done accessing services that require authentication!

Term-of-Use URL

https://www.pingidentity.com/legal

Primary Color *

#AD2E2D ●

Secondary Color

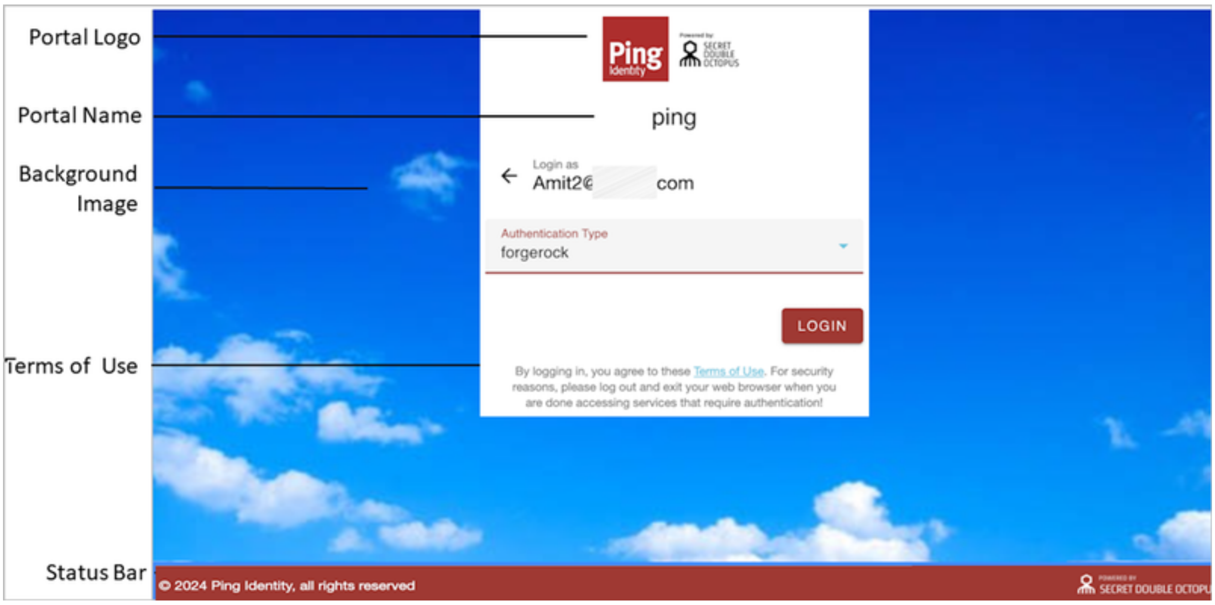
#e0e0e0 ●

Text Color

#ffffff ○

RESTORE DEFAULT SETTINGS

The following figure shows an example of how you can use branding to design your User Portal. All available branding settings are described in the table below the diagram.



By logging in, you agree to these Terms of Use. For security reasons, please log out and exit your web browser when you are done accessing services that require authentication!

© 2024 Ping Identity, all rights reserved

| Setting | Description / Notes |
|---|---|
| Display Portal Name / Portal Name | When the toggle is enabled, the name entered in the **Portal Name** field appears on the Login screen and in the upper left corner of the User Portal. |
| Display Status Bar / Status Bar Text | When the toggle is enabled, the text in the **Status Bar Text** field appears on the bottom of both the Login screen and the User Portal. |
| Portal Logo | This image appears at the top of the Login screen for the Portal. To update the logo, hover over the area, click **Upload Image** and select the JPG or PNG file of your choice. Supported image size is 128x128 pixels. |
| Browser Tab Icon | The favicon for the browser tab in which the Portal is displayed. To update the image, hover over the area, click **Upload Image** and select the icon of your choice. Supported image formats are PNG, GIF, and ICO. Image size should be 16x16 or 32x32 pixels, using either 8-bit or 24-bit colors. |
| Background Image | This image is displayed across the Login screen. To update it, hover over the area, click **Upload Image** and select the image of your choice. |
| Term-of-Use Message / URL | This text appears on the Login screen for the Portal. **%U** is a link to the **Term-of-Use URL**. |
| Primary Color | Color of the status bar, the **Login** button, and other major components. To change the color, enter the code in the field or click the circle on the right to open the color picker. |
| Secondary Color | Color of non-primary components, such as **Cancel** buttons. To change the color, enter the code in the field or click the circle on the right to open the color picker. |
| Text Color | Color of the text in the header and the status bar. To change the color, enter the code in the field or click the circle on the right to open the color picker. |
| Restore Default Settings | Click to revert all branding settings to the default values. |

After updating branding settings, click **Save**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

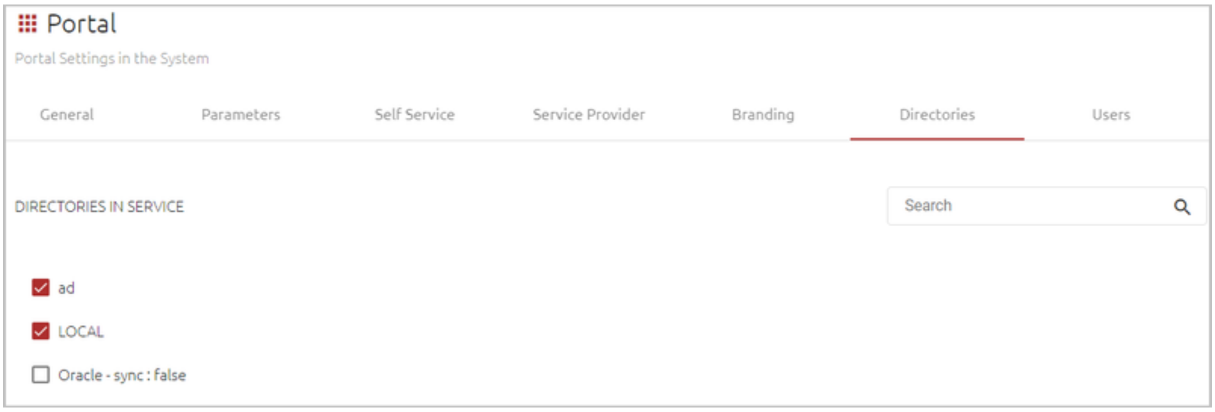
### Assigning Access Privileges to the User Portal

In order to work with the User Portal, users need to be assigned access privileges to the Portal. This is done in the **Directories** and **Users** tabs of the Management Console's **Portal** menu. Any user who is not assigned Portal access will not be able to successfully log into the Portal.

The following procedure explains how to grant Portal access by selecting the appropriate directories, groups and users.

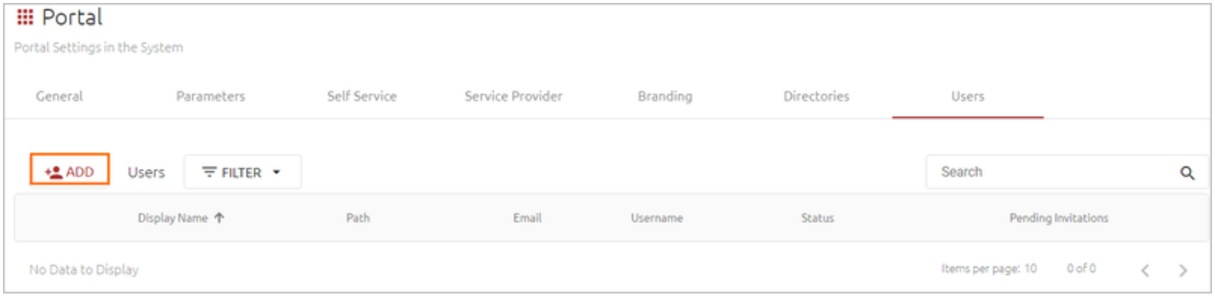
**To assign access privileges to the Portal:**

1. From the **Portal** menu, open the **Directories** tab. Select the checkboxes of the directories that you want to integrate with the User Portal, and then click **Save**. You can filter the Directories list by entering a keyword in the Search field.



☑ ad
☑ LOCAL
☐ Oracle - sync : false

2. After selecting directories, open the **Users** tab and click **Add**.



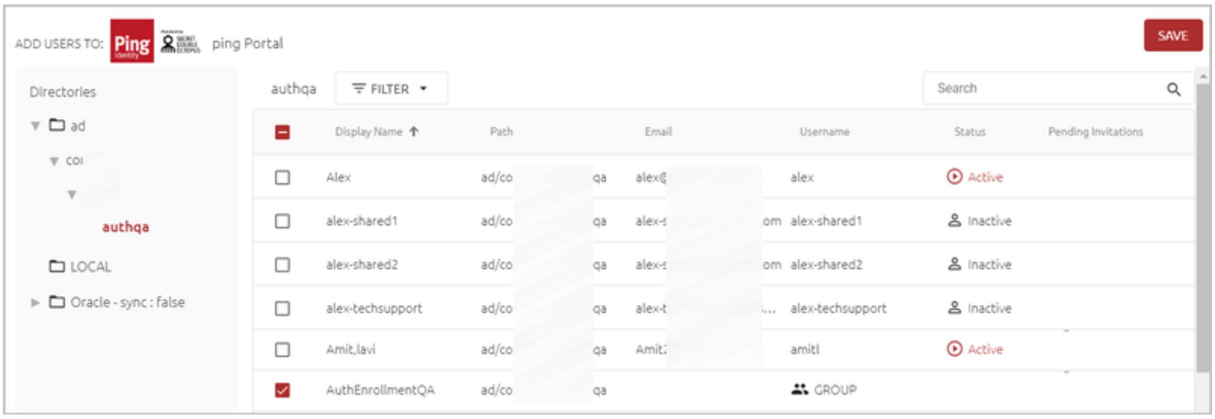
| Display Name ↑ | Path | Email | Username | Status | Pending Invitations |
|---|---|---|---|---|---|

No Data to Display

Items per page: 10 0 of 0

The **Add Users To** popup opens. A list of directories integrated with the Management Console appears on the left side of the popup.

3. Expand the directories tree and select the checkboxes of the users and Groups to which you want to grant Portal access. If a user or Group already has Portal access, the checkbox is disabled.



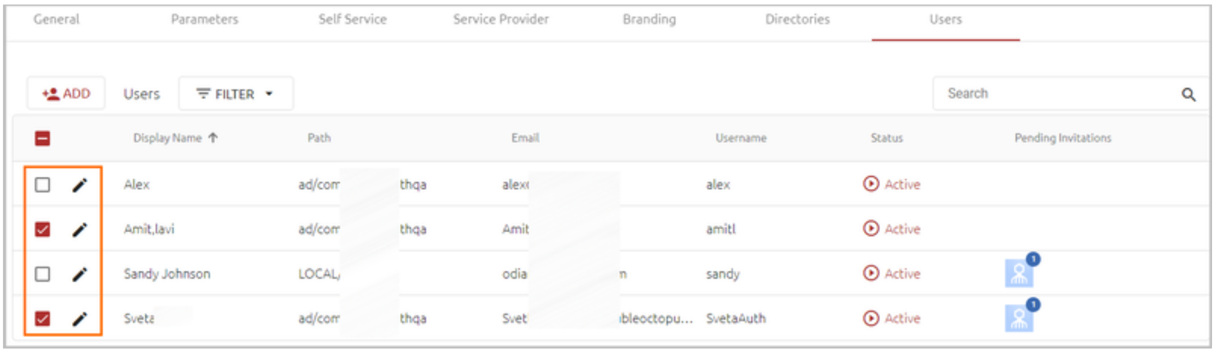
| | Display Name ↑ | Path | Email | Username | Status | Pending Invitations |
|---|---|---|---|---|---|---|
| ☐ | Alex | ad/co qa | alex@ | alex | Active | |
| ☐ | alex-shared1 | ad/co qa | alex-s om | alex-shared1 | Inactive | |
| ☐ | alex-shared2 | ad/co qa | alex-s om | alex-shared2 | Inactive | |
| ☐ | alex-techsupport | ad/co qa | alex-t ... | alex-techsupport | Inactive | |
| ☐ | Amit,lavi | ad/co qa | Amit | amitl | Active | |
| ☑ | AuthEnrollmentQA | ad/co qa | | GROUP | | |

4. When you have finished making your selections, click **SAVE** (in the upper right corner of the popup).

The popup closes, and the selected groups and users are listed in the **Users** tab.

5. From the toolbar at the top of the page, click **PUBLISH** and publish your changes.

After adding users to the list, you can manage them directly from the **Users** tab. To enable or disable Portal access for a specific user, toggle the checkbox on the left side of the row. Clicking the Edit icon next to the checkbox opens the individual settings for that user.



|  | Display Name ↑ | Path | Email | Username | Status | Pending Invitations |
|---|---|---|---|---|---|---|
| □ | Alex | ad/com thqa | alex | alex | Active |  |
| ☑ | Amit,lavi | ad/com thqa | Amit | amitl | Active |  |
| □ | Sandy Johnson | LOCAL, | odia n | sandy | Active | 1 |
| ☑ | Sveta | ad/com thqa | Svet ibleoctopu... | SvetaAuth | Active | 1 |

## Configuring Integrated Applications

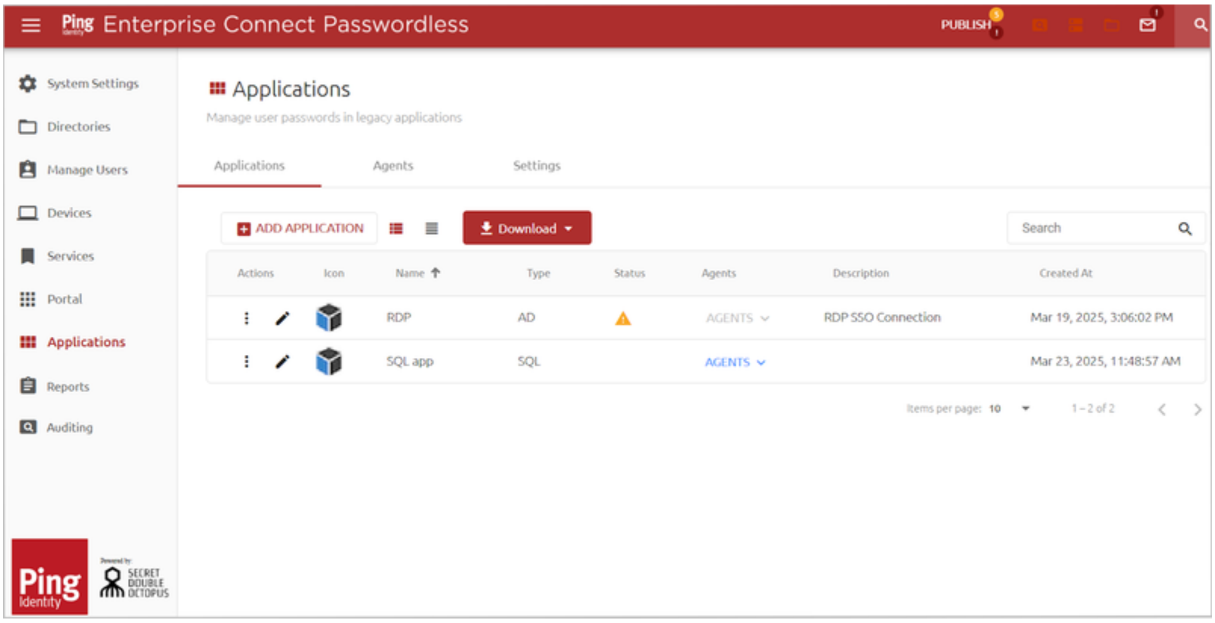
The Enterprise Connect Passwordless platform supports integration of a wide variety of applications with the Authentication Server and the Enterprise Connect Passwordless Windows Agent (version 4.0 and higher). This integration provides Windows users with seamless access to these applications, without the need to manually enter login credentials. When an integrated application is launched, the Windows Agent retrieves the user's credentials and populates the fields of the Login screen, thus enabling successful login.

All integrated applications fall into one of three Credential Type categories, according to where the password is stored. Credential Types are:

- **AD:** The password for the application is synced with the Active Directory.
- **Vault:** The password for the application is stored locally (e.g., on the workstation).
- **SQL:** The password for the application is stored in the application's database. Applications of this type manage password handling via the Octopus SQL Agent, which is installed on an on-premise Windows server or workstation.

Automatic population of the fields of the Login screen is accomplished through defining Desktop SSO elements for the integrated application in the Management Console. The **Desktop SSO** tab (in the application's settings) enables the system admin to specify properties and parameters of the Login screen's fields. These parameters are then saved to a configuration file which is deployed to the workstations, allowing the Windows Agent to identify the fields and set user credentials in the appropriate fields.

Most procedures related to setup and configuration of integrated applications are performed from the **Applications** menu of the Management Console.



Applications

Manage user passwords in legacy applications

| Actions | Icon | Name ↑ | Type | Status | Agents | Description | Created At |
|---|---|---|---|---|---|---|---|
| ⋮ ✎ | | RDP | AD | ⚠ | AGENTS ⌄ | RDP SSO Connection | Mar 19, 2025, 3:06:02 PM |
| ⋮ ✎ | | SQL app | SQL | | AGENTS ⌄ | | Mar 23, 2025, 11:48:57 AM |

Items per page: 10 1 – 2 of 2

The following topics describe how to create and work with integration applications:

- Adding Integrated Applications: Workflow
- Adding, Viewing and Managing Applications
- Viewing and Updating Application General Details
- Configuring Single Sign-on Settings for Applications
- Selecting Application Login Parameters
- Configuring Desktop SSO Elements
- Assigning Directories and Users to Applications
- Working with Octopus SQL Agents
- Selecting Application Database Configuration Settings

## Adding Integrated Applications: Workflow

The process for creating and configuring integrated **AD** and **Vault** type applications involves the following stages:

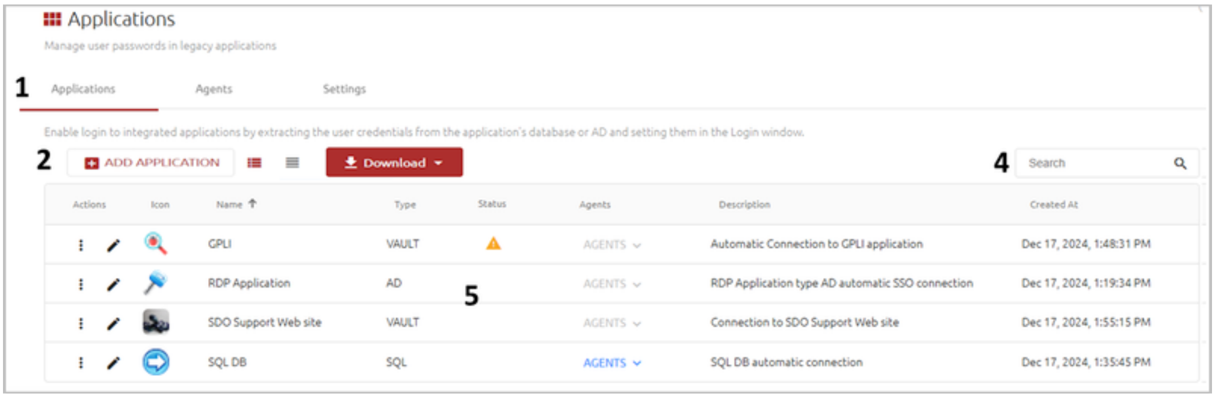
1. Add a new application to the Management Console and specify the relevant Credential Type (Adding Applications).
2. Specify general details and parameters for the application.
3. Select the groups and users who are authorized to use the application.
4. Configure Desktop SSO elements for identifying the application's Login screen, download the generated JSON file and install it on Windows workstations.

The workflow for creating **SQL** type applications includes the following additional requirements:

- Add an Octopus SQL Agent and install it on an on-premise Windows server or workstation. The Agent must be created **BEFORE** adding the new application. For more information, refer to the Octopus SQL Agent Installation Guide.
- After adding the integrated application, review database details in the **Config** tab of the application's settings, and update them if necessary.

## Adding, Viewing and Managing Applications

The **Applications** page lists all added applications and enables you to perform various administrative actions on them. The main portions and features of the page are described in the table below the diagram.



Enable login to integrated applications by extracting the user credentials from the application's database or AD and setting them in the Login window.

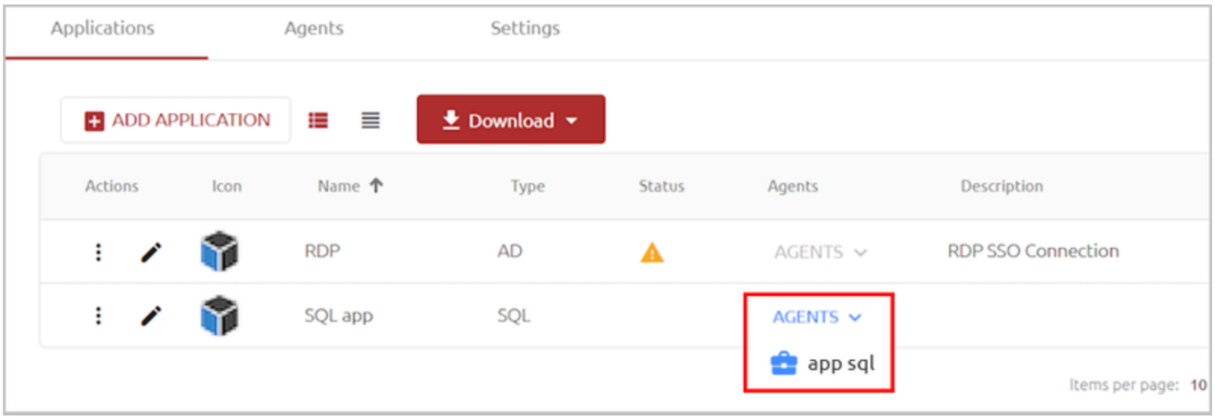
| Actions | Icon | Name | Type | Status | Agents | Description | Created At |
|---|---|---|---|---|---|---|---|
| ⋮ ✎ | | GPLI | VAULT | ⚠ | AGENTS | Automatic Connection to GPLI application | Dec 17, 2024, 1:48:31 PM |
| ⋮ ✎ | | RDP Application | AD | | AGENTS | RDP Application type AD automatic SSO connection | Dec 17, 2024, 1:19:34 PM |
| ⋮ ✎ | | SDO Support Web site | VAULT | | AGENTS | Connection to SDO Support Web site | Dec 17, 2024, 1:55:15 PM |
| ⋮ ✎ | | SQL DB | SQL | | AGENTS | SQL DB automatic connection | Dec 17, 2024, 1:35:45 PM |

| Number | Feature | Description / Notes |
|---|---|---|
| 1 | Tab selection | • **Applications:** Lists all integrated applications and provides access to administrative operations.<br>• **Agents:** Lists all added Octopus SQL Agents and enables you to create and edit Agents. This tab is relevant to SQL type applications only. For more information, refer to Working with Octopus SQL Agents.<br>• **Settings:** Enables you to set the SSO Session Timeout. For details, refer to Managing Application Details and Parameters. |
| 2 | Add Application button | Enables you to create a new application. For details, refer to Adding Applications. |
| 3 | Download button | Downloads the JSON file that is generated in the background when Desktop SSO elements are added or updated. For more information, refer to Configuring Desktop SSO Elements. |
| 4 | Search tool | To quickly locate a service, type all or part of the service name in the **Search** field, and click **<Enter>**. The Applications list is filtered according to your entry. |

| Number | Feature | Description / Notes |
|---|---|---|
| 5 | Applications list | Displays information about each added application, allows management operations and provides access to application settings. A ⚠ icon appears in the row of applications whose settings are incomplete or invalid. Clicking the icon opens a popup listing the invalid settings and a description of the specific error. |

### Viewing and Handling Applications

The Applications list provides basic information about each added application, including type, description (if any) and creation date. If an Agent is assigned to an SQL type application, the **AGENTS** list is enabled. To view the Agent to which the application is assigned, click to open the list. Clicking the Agent name opens the settings of that Agent.

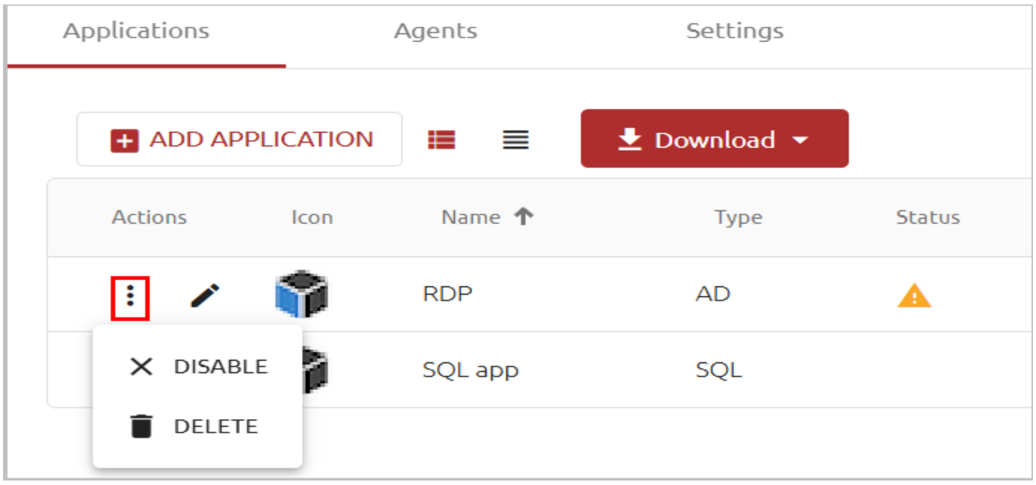


**Note**

The **AGENTS** list is always disabled for AD and Vault type applications.

The **Actions** column provides access to the following administrative operations:

- **Disable / Enable:** Inactivates an application / Reactivates a disabled application.
- **Delete:** Removes an application from the Management Console.



Clicking ✎ in the row of an application enables you to view and update the application's settings.

### Adding Applications

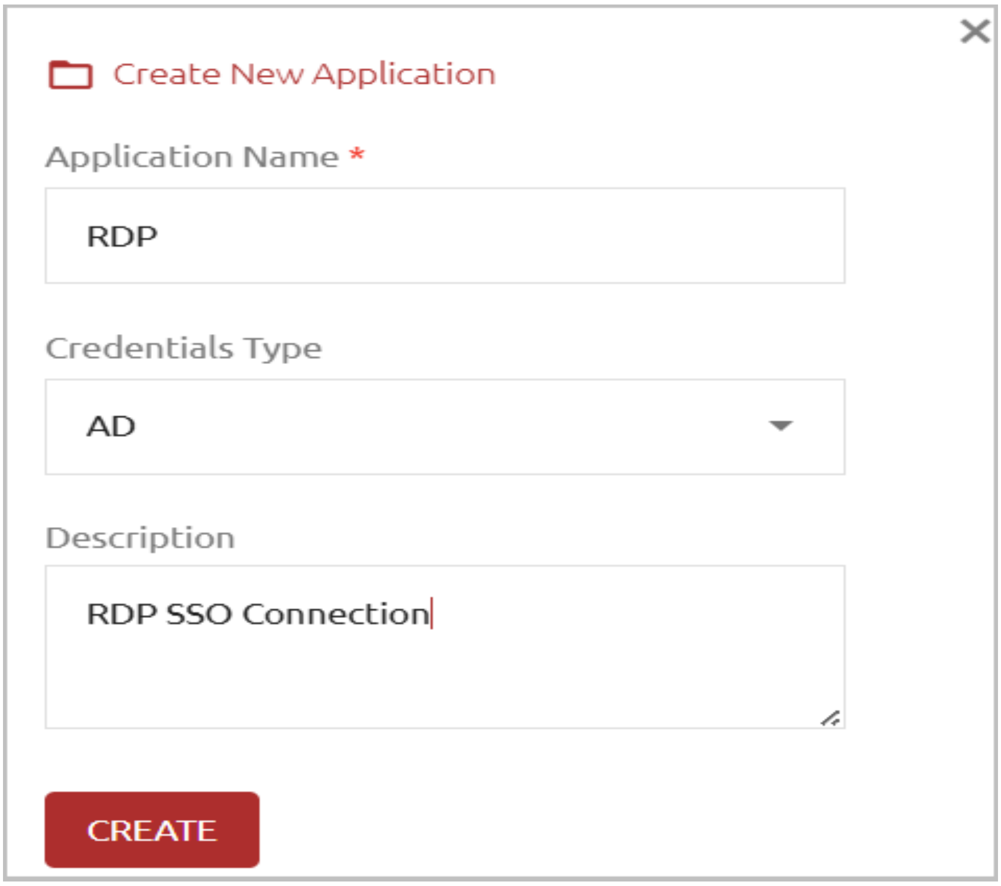
Adding a new application involves specifying the application's name and Credentials Type.

**To add an application:**

1. At the top of the **Applications** tab, click **Add Application**.

   The **Create New Application** dialog opens.

2. At the top of the dialog, enter a name for the application.
3. From the **Credentials Type** dropdown list, select **AD**, **SQL** or **Vault**.
4. If desired, in the **Description** field, enter notes or comments about the application.



Create New Application

Application Name *

RDP

Credentials Type

AD

Description

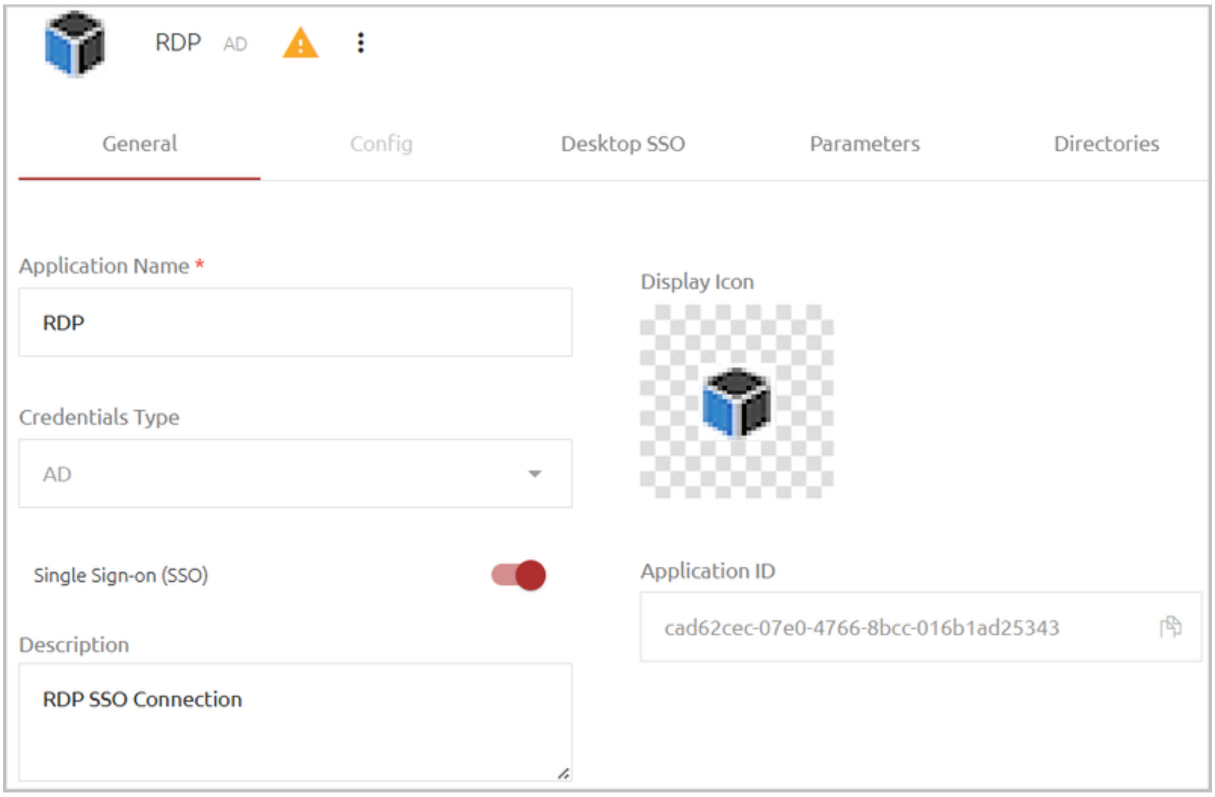
RDP SSO Connection

5. Click **Create.**

   The application is added, and the **General** tab of the application's settings opens.

## Viewing and Updating Application General Details

The **General** tab is displayed by default when the application's settings are opened.



Application Name *: RDP

Credentials Type: AD

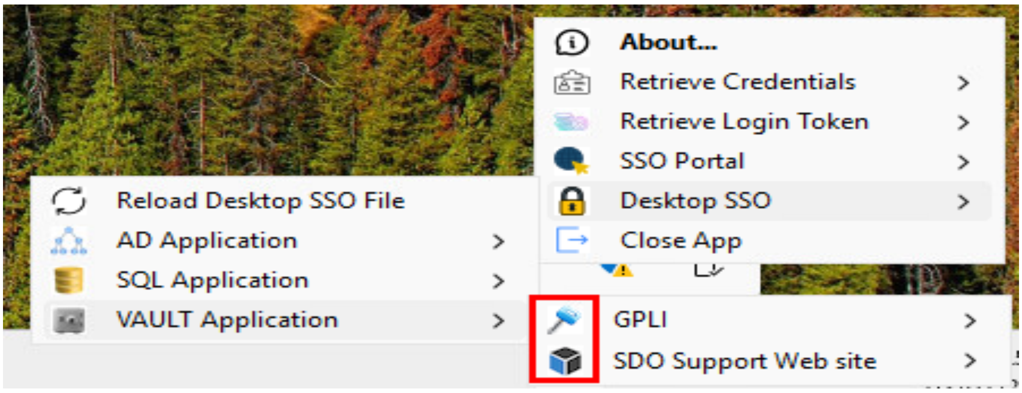
Single Sign-on (SSO): ●

Description: RDP SSO Connection

Application ID: cad62cec-07e0-4766-8bcc-016b1ad25343

This tab contains the following components:

| Component / Setting | Description / Notes |
|---|---|
| Application Name | The user-assigned name for the application. |
| Credentials Type | **AD**, **SQL** or **Vault**. This setting is not editable. |
| Single Sign-on (SSO) | This toggle determines whether an authentication request is generated when users access the integrated application. When the **SSO** setting is enabled, users do NOT receive push notifications when logging into the application.<br>For more information about single sign-on, refer to Configuring Application SSO Settings. |
| Description | Notes or comments about the application. |

| Component / Setting | Description / Notes |
|---|---|
| Display Icon | This logo is displayed in the Windows systray. For example:<br><br> About...<br>Retrieve Credentials<br>Retrieve Login Token<br>SSO Portal<br>Desktop SSO<br>Close App<br>Reload Desktop SSO File<br>AD Application<br>SQL Application<br>VAULT Application<br>GPLI<br>SDO Support Web site<br>To change the default logo, click it and upload the image of your choice. Recommended logo size is 16x16 pixels. |
| Application ID | A system-generated unique identifier for the application. Click the Copy icon to copy the ID. |

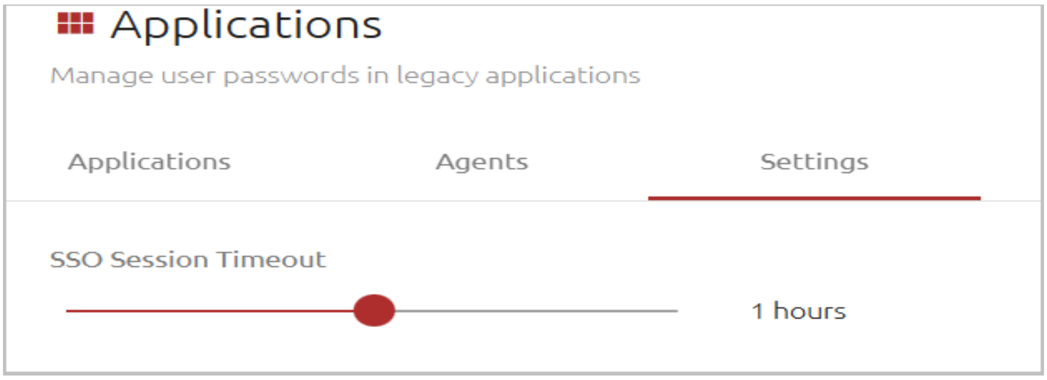
After editing settings in the **General** tab, click **Save**.

## Configuring Single Sign-on Settings for Applications

The **SSO Session Timeout** value, on the **Settings** tab of the **Applications** menu, determines the maximum length of an integrated application session. The session timeout can range from 1 minute to 24 hours (default is 1 hour). To update the setting, drag the slider to specify the desired value and then click **Save**.

**Note**

The **SSO Session Timeout** is a global setting for ALL integrated applications.



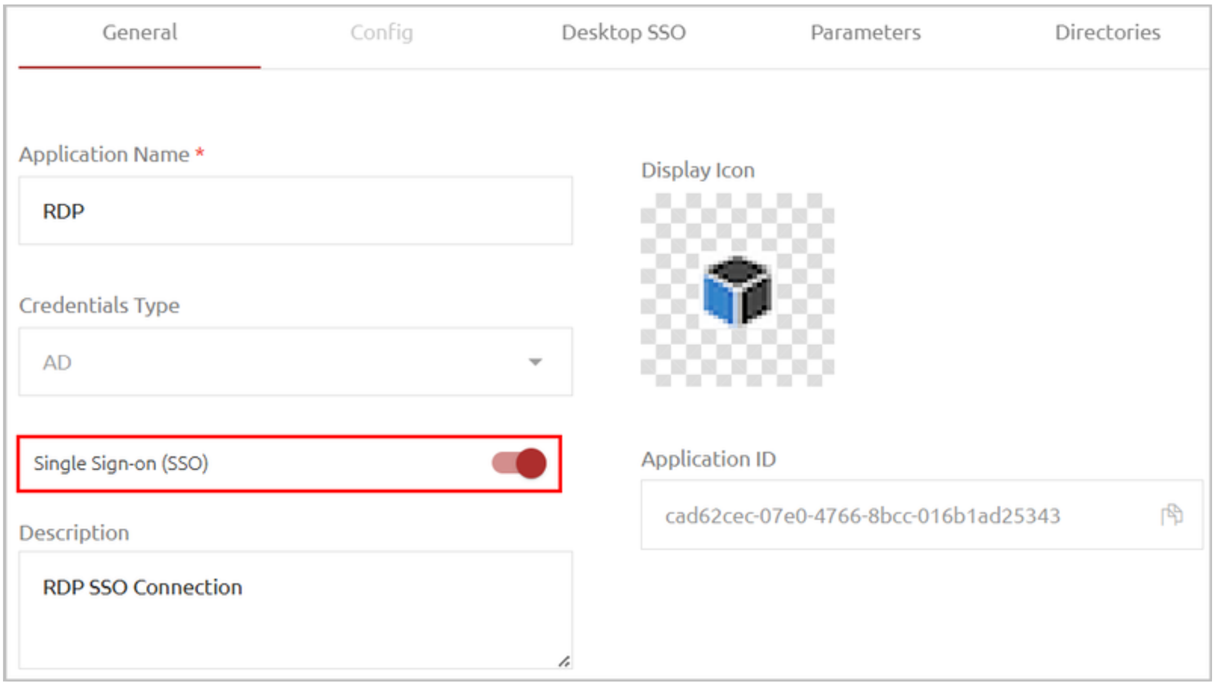
Applications

Manage user passwords in legacy applications

SSO Session Timeout

1 hours

To support SSO for a specific application, access the **General** tab of the application's settings, and verify that the **Single Sign-on (SSO)** toggle is enabled. When SSO is enabled, users are immediately logged into the application, without receiving an authentication request via push notification.



Application Name *

RDP

Credentials Type

AD

Single Sign-on (SSO)

Description

RDP SSO Connection

Display Icon

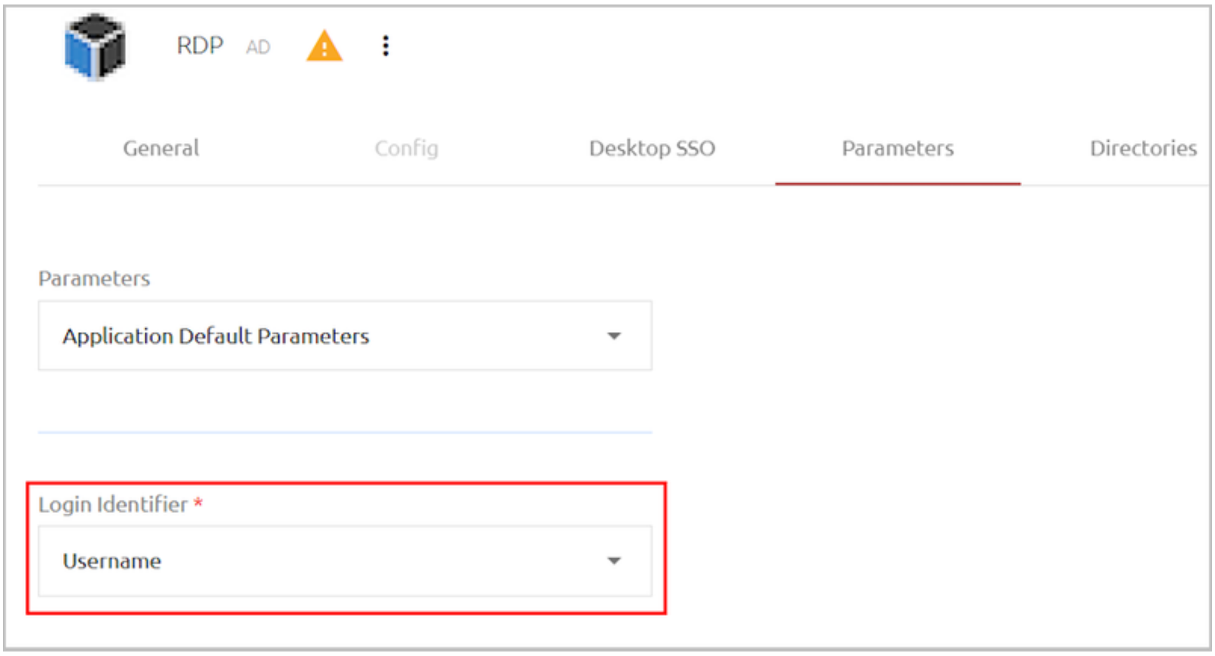
Application ID

cad62cec-07e0-4766-8bcc-016b1ad25343

## Selecting Application Login Parameters

The **Parameters** tab of an application's settings specifies the user identifier required for authenticating to the application.

For AD and Vault application types, select the **Login Identifier**. This is the identifier that the user would need to provide (email, username, etc.) in order to authenticate to the application.



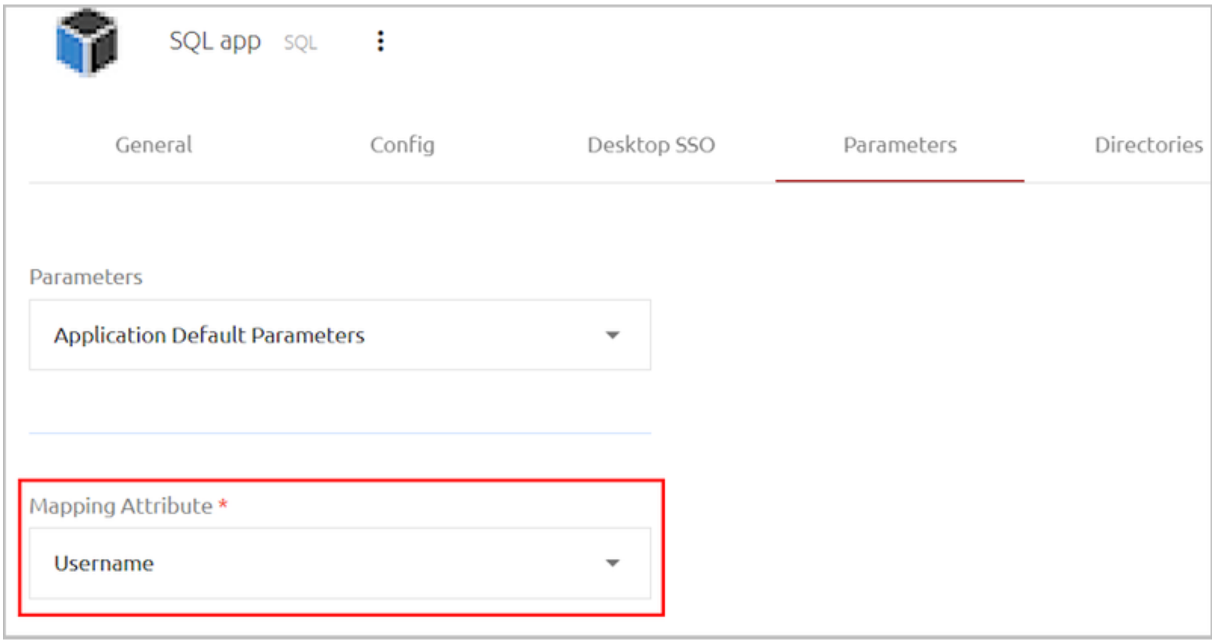
Parameters

Application Default Parameters

Login Identifier *

Username

For SQL application types, select the **Mapping Attribute**. This is the parameter used to identify the user in the application's database. The parameter selected should correspond to the **ID Field name** specified in the **Config** tab of the application's settings (Selecting Application Database Configuration Settings).



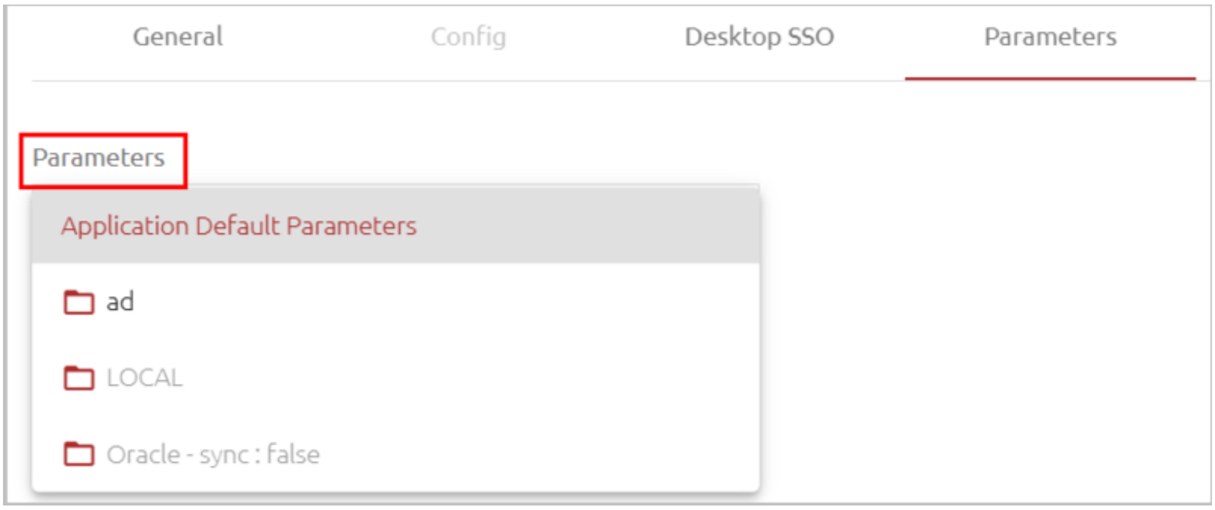
Parameters

Application Default Parameters

Mapping Attribute *

Username

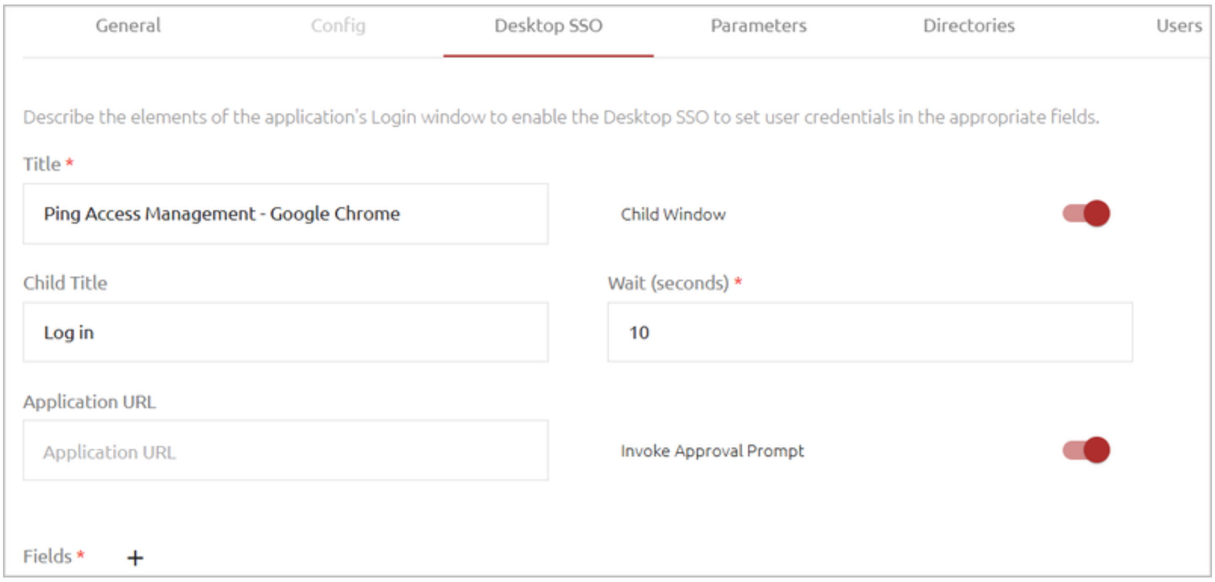
The **Parameters** dropdown list at the top of the tab enables you to define a directory-specific parameter that overrides the default identifier configured for the application.



For more details and instructions for overriding parameters, refer to Overriding Default Service Parameters.

## Configuring Desktop SSO Elements

The **Desktop SSO** tab allows you to define unique elements of the application's Login window, thus enabling the Windows Agent to identify the correct window and set user credentials in the appropriate fields. Each time you update elements in the **Desktop SSO** tab, your changes are automatically saved to a configuration file that can be downloaded and deployed to all Windows workstations in your organization.



Describe the elements of the application's Login window to enable the Desktop SSO to set user credentials in the appropriate fields.

Title *: Ping Access Management - Google Chrome

Child Window: ●

Child Title: Log in

Wait (seconds) *: 10

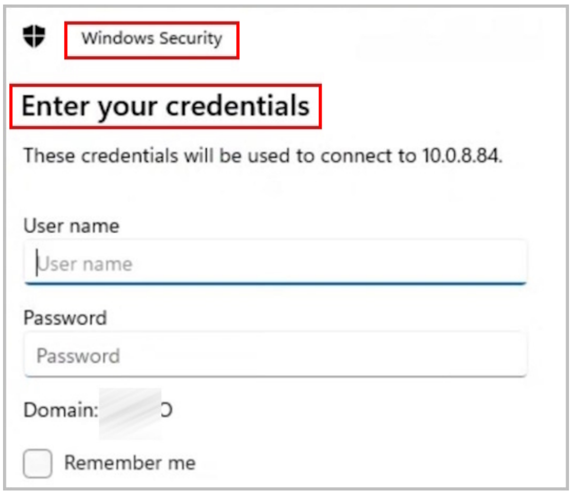
Application URL: Application URL

Invoke Approval Prompt: ●

Fields * +

## Specifying Login Window Title and Desktop SSO Behaviors

The upper portion of the **Desktop SSO** tab contains the following settings:

| Setting | Description / Notes |
|---|---|
| Title | Enter the title of the application's Login window. If the Login window is a child window, enter the title of the parent window. |
| Child Window | Enable this setting if the application's Login window is a child of another window. |
| Child Title | This setting is relevant when the Login window has a child with a unique title that identifies the window. A common use case is Login screens that have a generic title for multiple applications, as in the example below. In this case, **Windows Security** is the Title, and **Enter your credentials** is the Child Title.<br> |
| Application URL | This optional setting can be used to enhance the security of Desktop SSO authentication to web applications. When the setting is present, the Windows Agent checks the target website to avoid accessing incorrect or malicious sites. |

Windows Security

Enter your credentials

These credentials will be used to connect to 10.0.8.84.

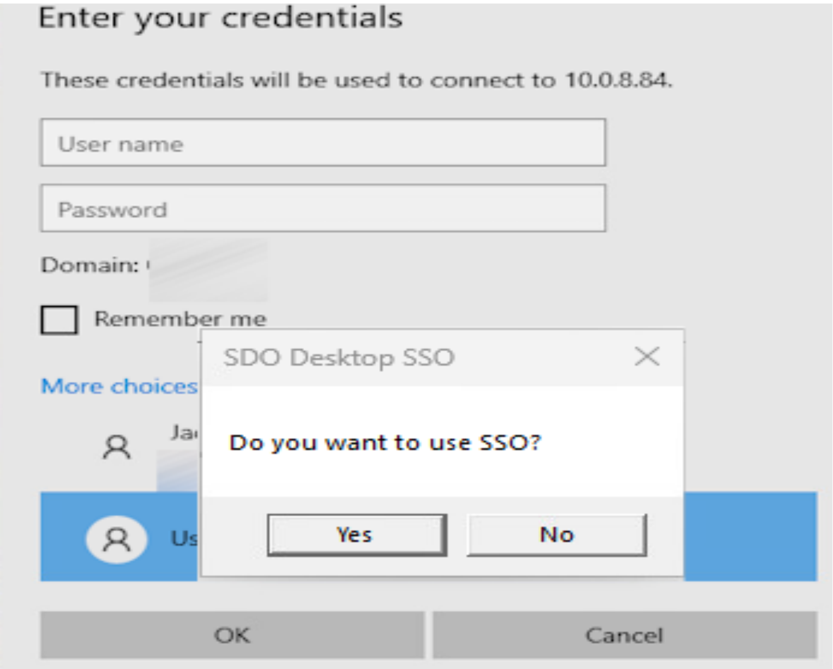
User name: User name

Password: Password

Domain: D

□ Remember me

| Setting | Description / Notes |
|---|---|
| Wait | If the value is greater than zero, the Desktop SSO mechanism will wait the specified number of seconds between populating the credentials fields and clicking the **OK** / **Submit** button. |
| Invoke Approval Prompt | When this setting is enabled, users are presented with a message box prompting them to confirm or reject use of Desktop SSO for the login flow to the application. |



Enter your credentials

These credentials will be used to connect to 10.0.8.84.

Domain: [redacted]

SDO Desktop SSO

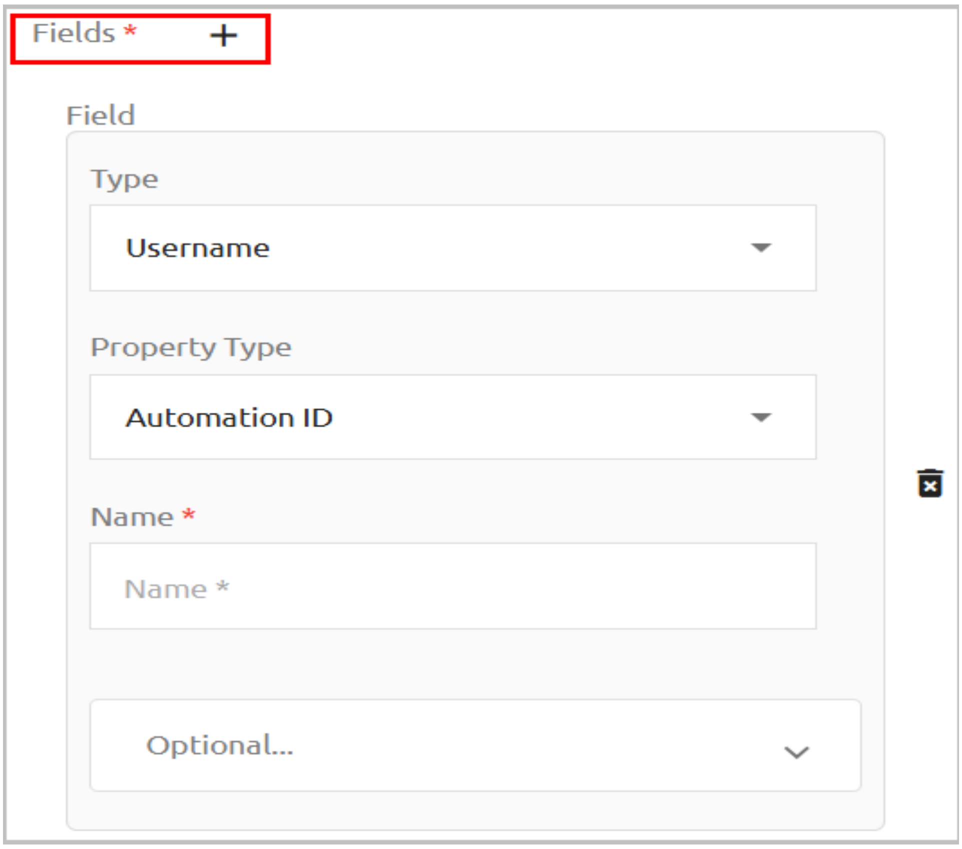
Do you want to use SSO?

### Defining Fields in the Login Window

The lower portion of the **Desktop SSO** tab enables you to describe fields of the application's Login window by specifying their unique attributes. Generally you will need to define only the fields that are required for authentication (usually **Username**, **Password**, and **OK** / **Submit**).

**To define Login window fields:**

1. In the **Fields** portion of the **Desktop SSO** tab, click **+** to add a new field.

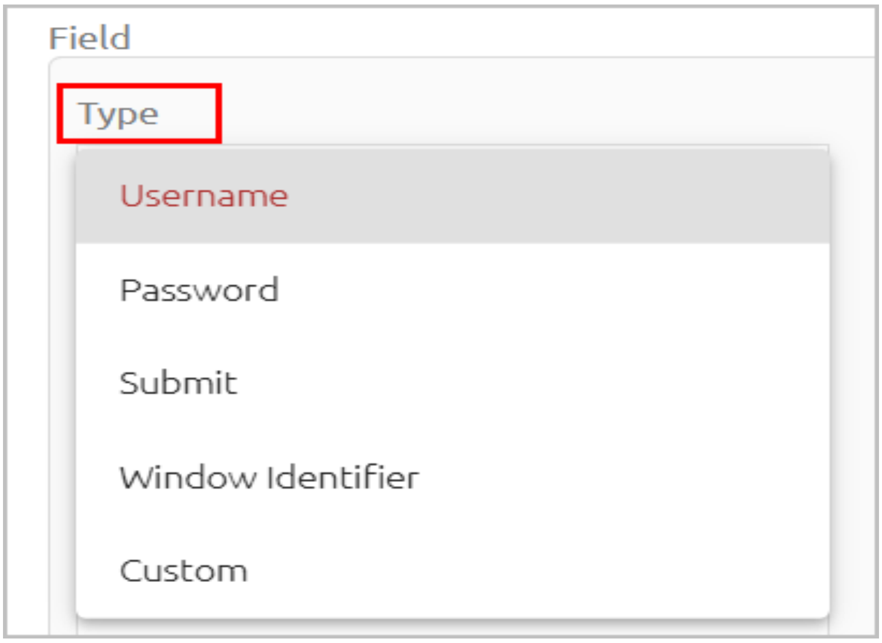


Type
Username

Property Type
Automation ID

Name *
Name *

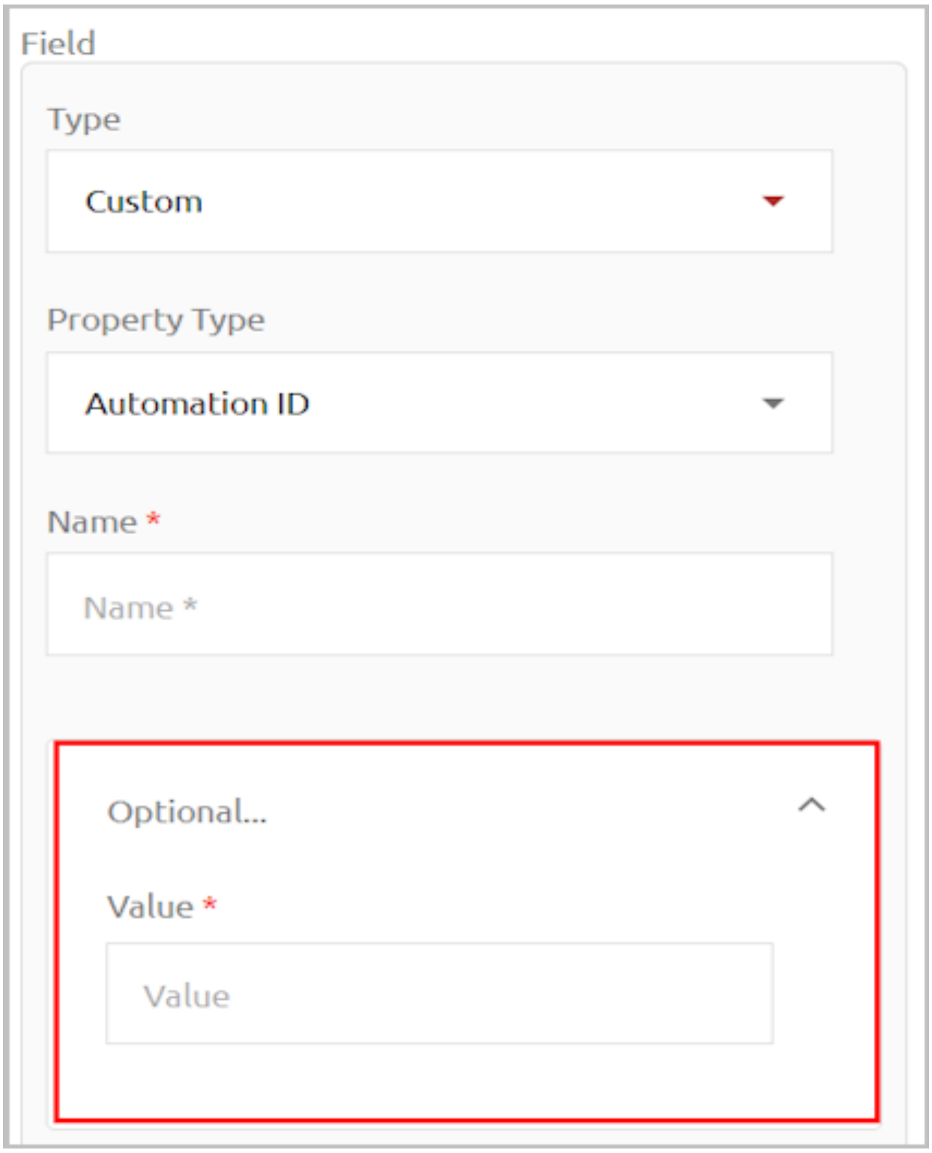
2. From the **Type** dropdown list, select the relevant field type.



The options are:

- **Username:** A field in which to set the username.
- **Password:** A field in which to set the password.
- **Submit:** The **OK** or **Submit** button.

- **Window Identifier:** A field that can be used to positively identify the Login window. The field must be specific to the Login window of this particular application.
- **Custom:** A field in which to set a hard-coded text value. To specify the text to be set in the field, expand the **Optional** frame and enter the required text in the **Value** field.



Field

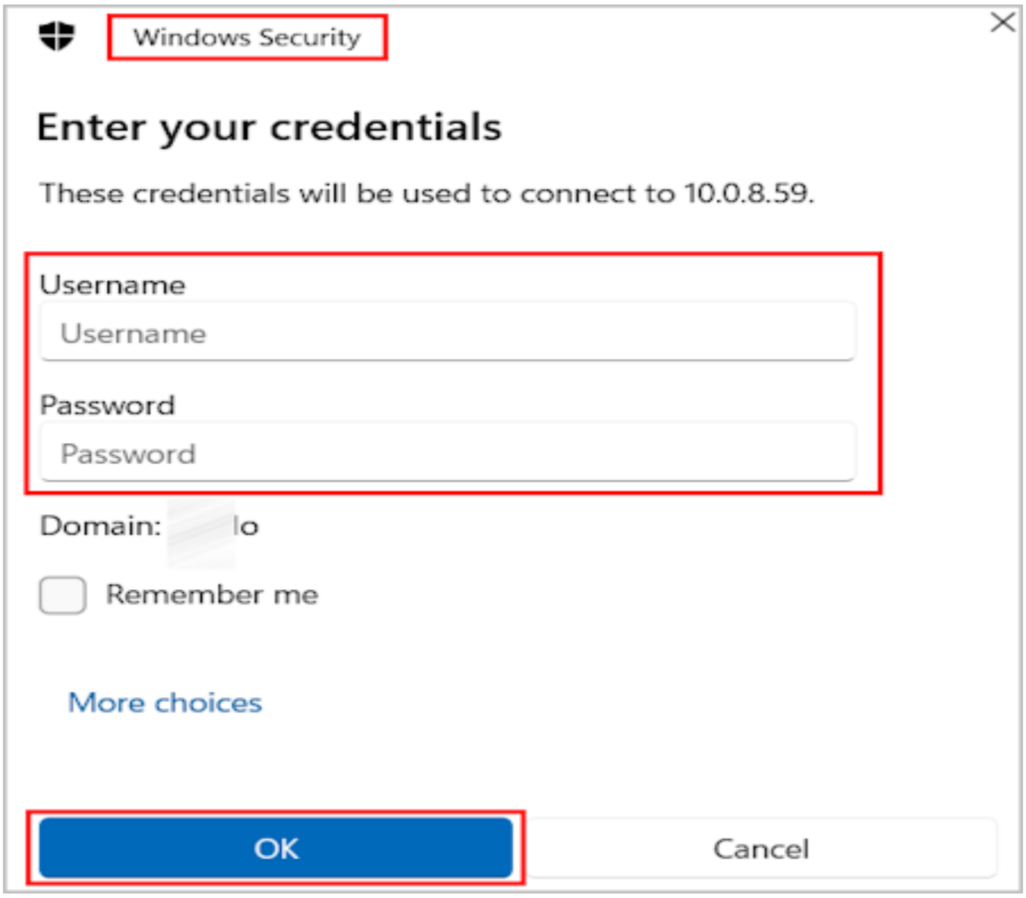
Type: Custom

Property Type: Automation ID

3. Select the relevant **Property Type** for the field (**Automation ID, Class Name**, **Name**, **Control Type** or **Localized Control Type**.
4. Using the helper tool of your choice, identify the field's name and enter it in the **Name** field.
5. Repeat Steps 1-4 for additional target fields.
6. At the bottom of the **Desktop SSO** tab, click **Save**.

### Describing Desktop SSO Fields: Example

This section shows an example of defining required elements for Desktop SSO login to a remote workstation. The application's Login screen is shown below.



Windows Security

Enter your credentials

These credentials will be used to connect to 10.0.8.59.

Username

Username

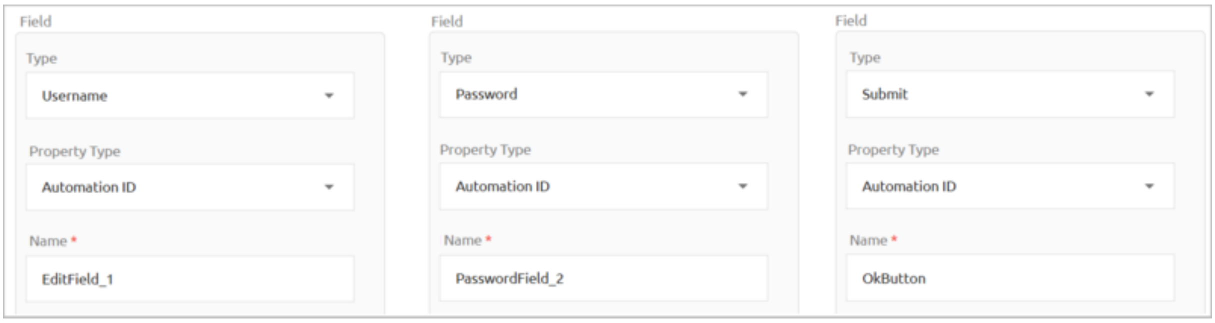
Password

Password

Domain: [redacted]lo

□ Remember me

**Windows Security** should be entered in the **Title** field at the top of the **Desktop SSO** tab, and **Enter your credentials** should be entered in the **Child Title** field. The three required fields (**Username**, **Password**, and the **OK** button), should then be described as follows:



Field
Type: Username
Property Type: Automation ID
Name *: EditField_1

Field
Type: Password
Property Type: Automation ID
Name *: PasswordField_2

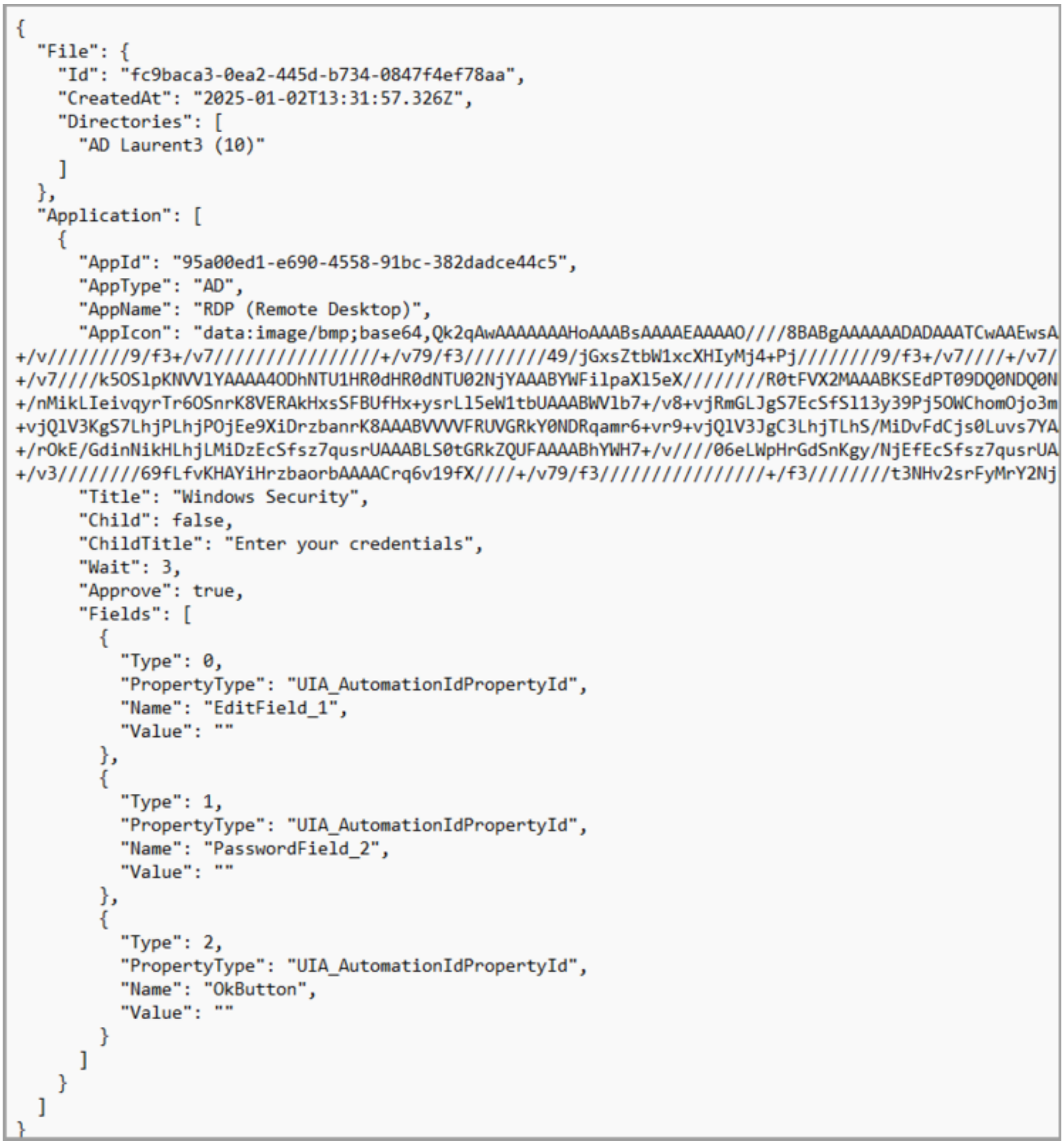
Field
Type: Submit
Property Type: Automation ID
Name *: OkButton

### Downloading and Deploying the Configuration File

All updates made in the **Desktop SSO** settings of your integrated applications are automatically added to a configuration file named **applications-desktop-sso.json**. Each application you add is stored as a separate object in the file. The example below shows the RDP application presented in the section above.

Each time the configuration file is downloaded (as described below), a unique ID and timestamp are automatically generated. This metadata appears at the beginning of the file.

The name(s) and unique ID(s) of the directory or directories selected for the download are also listed.

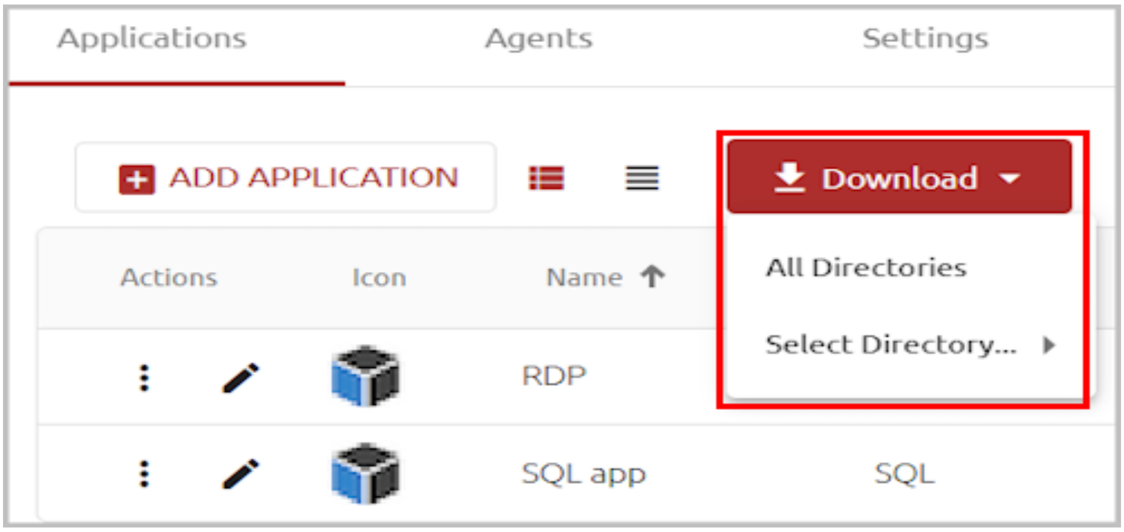


```
{
  "File": {
    "Id": "fc9baca3-0ea2-445d-b734-0847f4ef78aa",
    "CreatedAt": "2025-01-02T13:31:57.326Z",
    "Directories": [
      "AD Laurent3 (10)"
    ]
  },
  "Application": [
    {
      "AppId": "95a00ed1-e690-4558-91bc-382dadce44c5",
      "AppType": "AD",
      "AppName": "RDP (Remote Desktop)",
      "AppIcon": "data:image/bmp;base64,Qk2qAwAAAAAAAHoAAABsAAAAEAAAAO////8BABgAAAAAADADAAATCwAAEwsA
+/v////////9/f3+/v7/////////////////+/v79/f3////////49/jGxsZtbW1xcXHIyMj4+Pj////////9/f3+/v7////+/v7/
+/v7////k5OSlpKNVV1YAAAA4ODhNTU1HR0dHR0dNTU02NjYAAABYWFilpaXl5eX////////R0tFVX2MAAABKSEdPT09DQ0NDQ0N
+/nMikLIeivqyrTr6OSnrK8VERAkHxsSFBUfHx+ysrLl5eW1tbUAAABWVlb7+/v8+vjRmGLJgS7EcSfSl13y39Pj5OWChomOjo3m
+vjQlV3KgS7LhjPLhjPOjEe9XiDrzbanrK8AAABVVVVFRUVGRkY0NDRqamr6+vr9+vjQlV3JgC3LhjTLhS/MiDvFdCjs0Luvs7YA
+/rOkE/GdinNikHLhjLMiDzEcSfsz7qusrUAAABLS0tGRkZQUFAAAABhYWH7+/v////06eLWpHrGdSnKgy/NjEfEcSfsz7qusrUA
+/v3////////69fLfvKHAYiHrzbaorbAAAACrq6v19fX////+/v79/f3/////////////////+/f3////////t3NHv2srFyMrY2Nj
      "Title": "Windows Security",
      "Child": false,
      "ChildTitle": "Enter your credentials",
      "Wait": 3,
      "Approve": true,
      "Fields": [
        {
          "Type": 0,
          "PropertyType": "UIA_AutomationIdPropertyId",
          "Name": "EditField_1",
          "Value": ""
        },
        {
          "Type": 1,
          "PropertyType": "UIA_AutomationIdPropertyId",
          "Name": "PasswordField_2",
          "Value": ""
        },
        {
          "Type": 2,
          "PropertyType": "UIA_AutomationIdPropertyId",
          "Name": "OkButton",
          "Value": ""
        }
      ]
    }
  ]
}
```

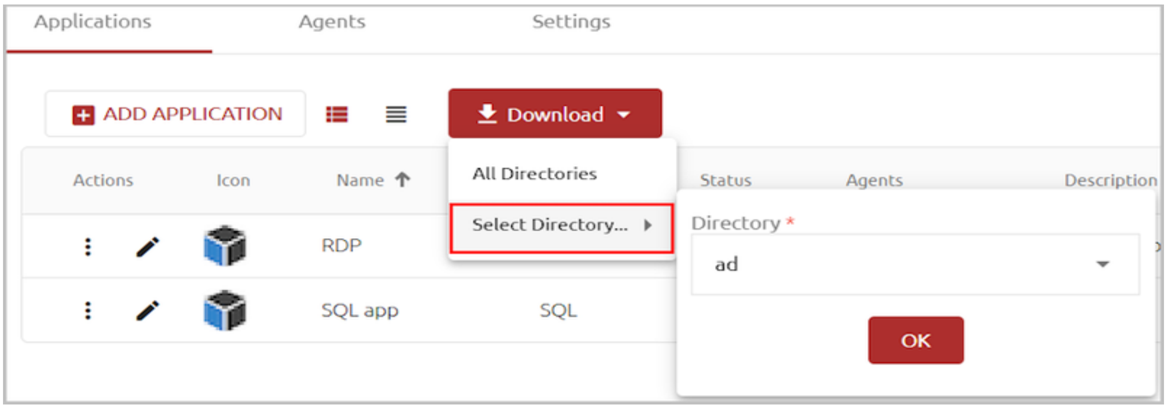
To enable Windows users to work with Desktop SSO, the configuration file needs to be downloaded, copied and deployed to the workstations.

**To download and deploy the configuration file:**

1. At the top of the **Applications** tab, click **Download**.

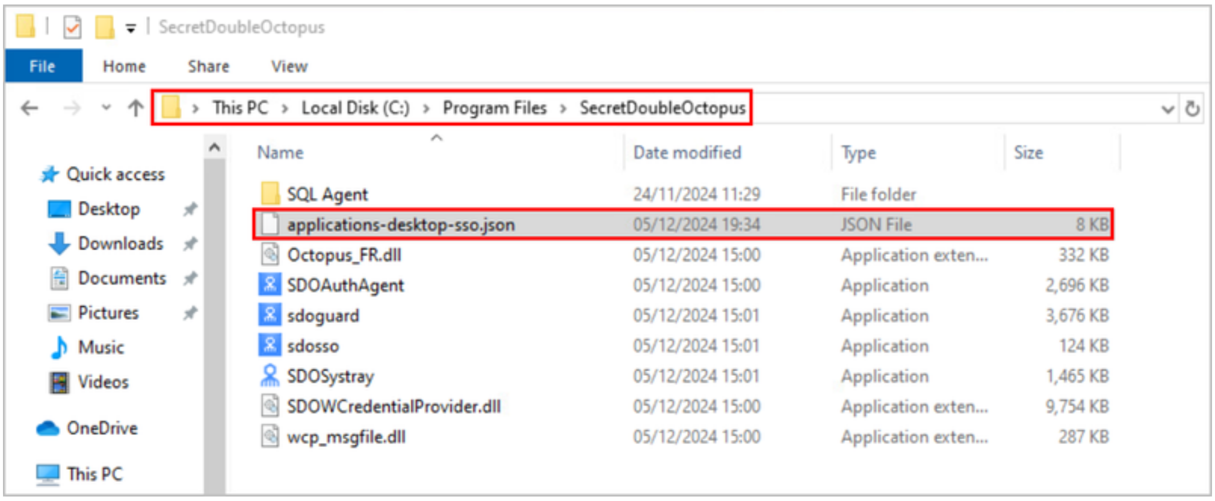


2. To start the download, select one of the following options:
   - **All Directories:** All defined applications are included in the configuration file.
   - **Select Directory:** Only applications assigned to a specified directory are included in the configuration file. Choose the relevant directory from the list, and then click **OK**.



Directory: ad

3. Copy the downloaded file to the **SecretDoubleOctopus** folder. For example:

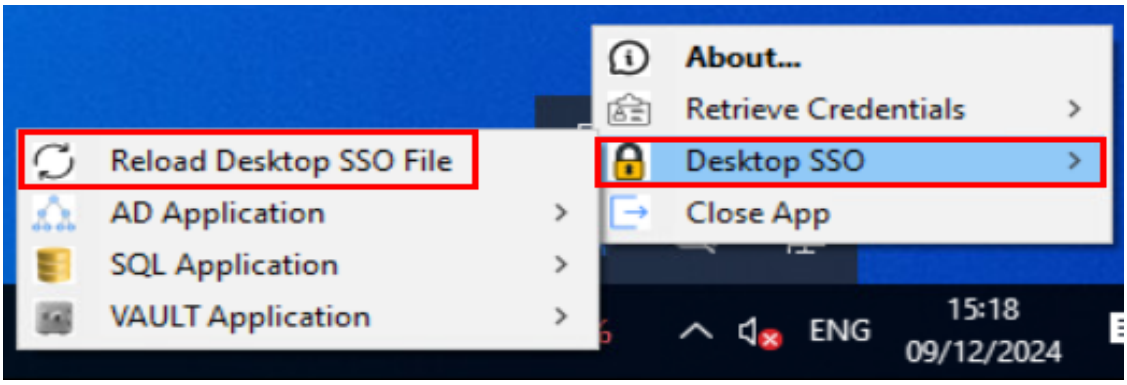


| Name | Date modified | Type | Size |
|---|---|---|---|
| SQL Agent | 24/11/2024 11:29 | File folder | |
| applications-desktop-sso.json | 05/12/2024 19:34 | JSON File | 8 KB |
| Octopus_FR.dll | 05/12/2024 15:00 | Application exten... | 332 KB |
| SDOAuthAgent | 05/12/2024 15:00 | Application | 2,696 KB |
| sdoguard | 05/12/2024 15:01 | Application | 3,676 KB |
| sdosso | 05/12/2024 15:01 | Application | 124 KB |
| SDOSystray | 05/12/2024 15:01 | Application | 1,465 KB |
| SDOWCredentialProvider.dll | 05/12/2024 15:00 | Application exten... | 9,754 KB |
| wcp_msgfile.dll | 05/12/2024 15:00 | Application exten... | 287 KB |

4. Deploy the file to the relevant Windows workstations in your organization.

> **Important**
>
> Do NOT change the name of the file.

It is recommended to download the configuration file each time you add a new application or update an existing one (instead of editing the file manually). Windows users can obtain the latest changes using the systray options, by selecting
**Desktop SSO > Reload Desktop SSO File**.



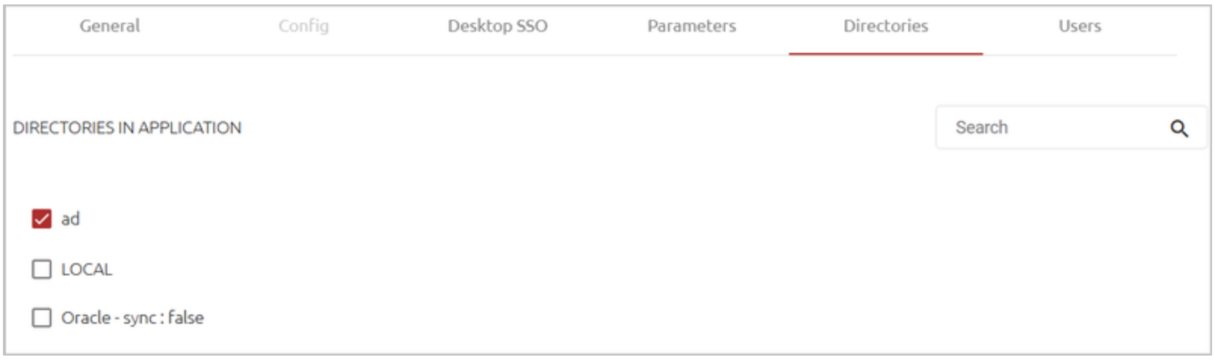
## Assigning Directories and Users to Applications

In order to work with an integrated application, users need to be assigned access privileges to the application. This is done in the **Directories** and **Users** tabs of the application's settings. Any user who is not assigned access privileges will not be able to log into the application through the Octopus Desktop SSO mechanism.

The following procedure explains how to grant access to an application by selecting the appropriate directories, groups and users.

**To assign access privileges to an integrated application:**

1. From the **Applications** tab of the **Applications** menu, click ✎ in the row of the relevant application to open the settings.
2. From the **Directories** tab, select the checkboxes of the directories that you want to integrate with the application, and then click **Save.** You can filter the Directories list by entering a keyword in the Search field.



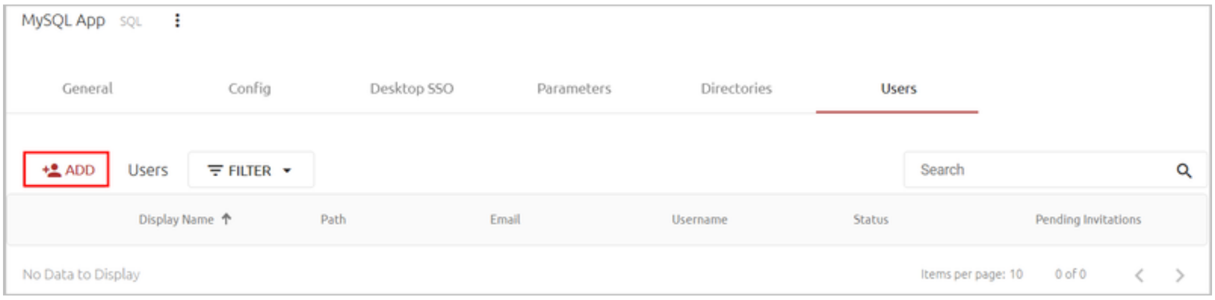
DIRECTORIES IN APPLICATION

☑ ad

☐ LOCAL

☐ Oracle - sync : false

3. In the upper left corner of the **Users** tab, click **Add**.



| Display Name | Path | Email | Username | Status | Pending Invitations |
|---|---|---|---|---|---|

No Data to Display

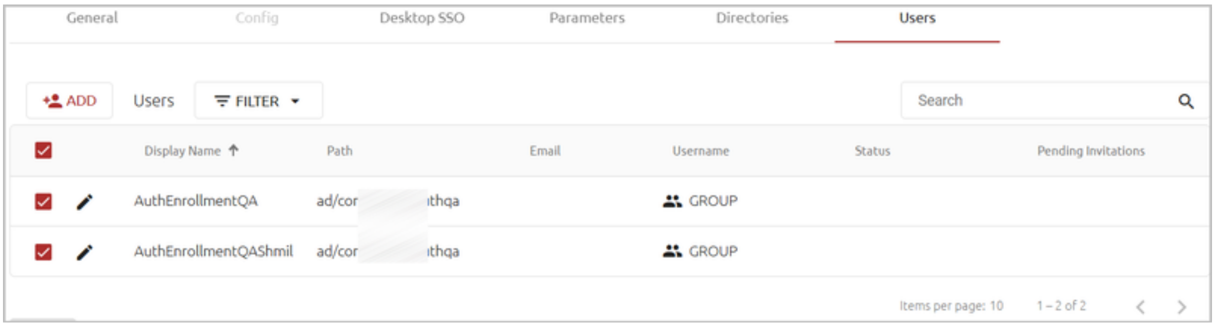
Items per page: 10 0 of 0

The **Add Users To** popup opens. A list of directories integrated with the Management Console appears on the left side of the popup.

4. Expand the directories tree and select the checkboxes of the users and groups to which you want to grant application access. If a user or group already has access, the checkbox is disabled.

5. When you have finished making your selections, click **SAVE** (in the upper right corner of the popup).

The popup closes, and the selected groups and users are listed in the **Users** tab.



| ☑ | Display Name | Path | Email | Username | Status | Pending Invitations |
|---|---|---|---|---|---|---|
| ☑ | AuthEnrollmentQA | ad/cor[redacted]ithqa | | GROUP | | |
| ☑ | AuthEnrollmentQAShmil | ad/cor[redacted]ithqa | | GROUP | | |

Items per page: 10 1 – 2 of 2

6. From the toolbar at the top of the page, click **PUBLISH** and publish your changes.

After adding users to the list, you can manage them directly from the **Users** tab. To enable or disable application access for a specific user or group, toggle the checkbox on the left side of the row. Clicking the Edit icon next to the checkbox opens the individual settings for that user/group.

## Working with Octopus SQL Agents

The Octopus SQL Agent is an independent component required for integration of SQL type applications. The SQL Agent acts as an intermediary element between the Authentication Server and the application that stores the password. The Agent is responsible for setting the password generated by the Authentication Server in the application's database, and retrieving username details from the database. These credentials are then sent to the Windows Agent, via the Authentication Server, so Desktop SSO can be performed. To enable this workflow, the Octopus SQL Agent needs to be installed on a domain-joined Windows server or workstation.

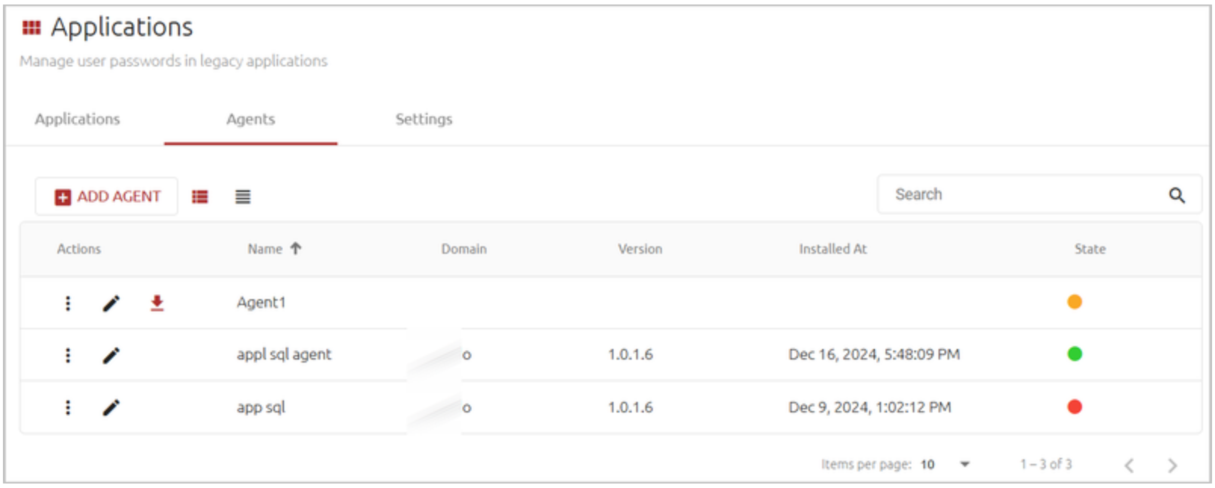
**Note**

For detailed information about the SQL Agent and the installation process, please refer to the Octopus SQL Agent Installation Guide.

### Viewing and Managing SQL Agents

The **Agents** tab of the **Applications** menu lists all added SQL Agents (installed and uninstalled) and enables you to perform some administrative operations on them. Basic information, including name, domain, version and installation date (if relevant) is provided about each Agent. The **State** column indicates the current connectivity status of each Agent:

- **Green indicator:** Agent is installed and connected.
- **Red indicator:** Agent is installed but not currently connected.
- **Orange indicator:** Agent has been created / downloaded but has not yet been installed.



Applications

Manage user passwords in legacy applications

Applications | Agents | Settings

ADD AGENT

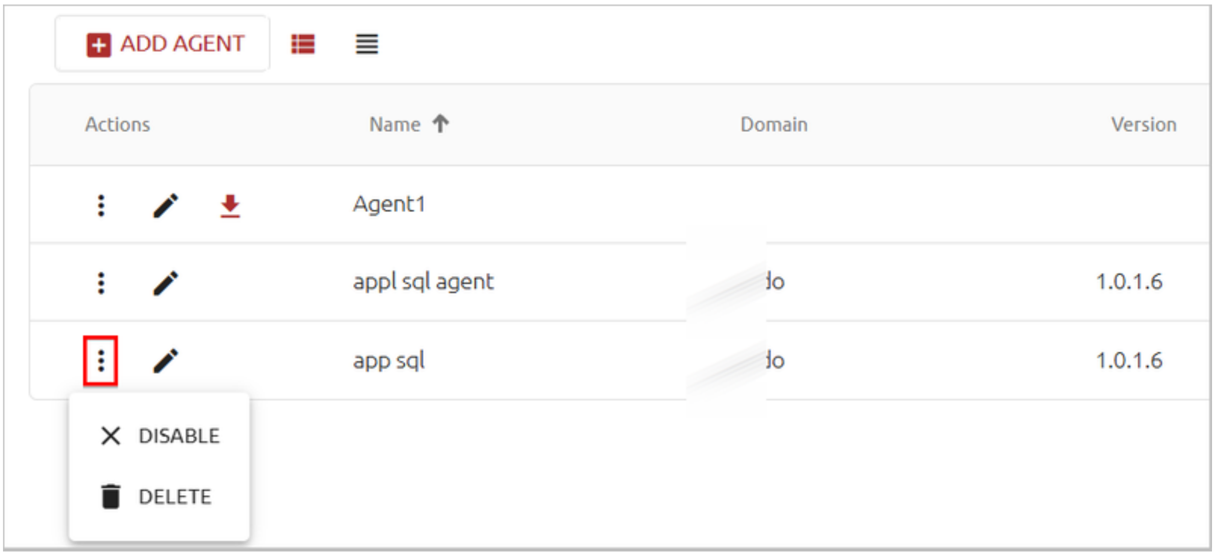
Search

| Actions | Name ↑ | Domain | Version | Installed At | State |
|---|---|---|---|---|---|
| ⋮ ✎ ⬇ | Agent1 | | | | 🟠 |
| ⋮ ✎ | appl sql agent | [redacted] | 1.0.1.6 | Dec 16, 2024, 5:48:09 PM | 🟢 |
| ⋮ ✎ | app sql | [redacted] | 1.0.1.6 | Dec 9, 2024, 1:02:12 PM | 🔴 |

Items per page: 10 ▾ 1 – 3 of 3 ‹ ›

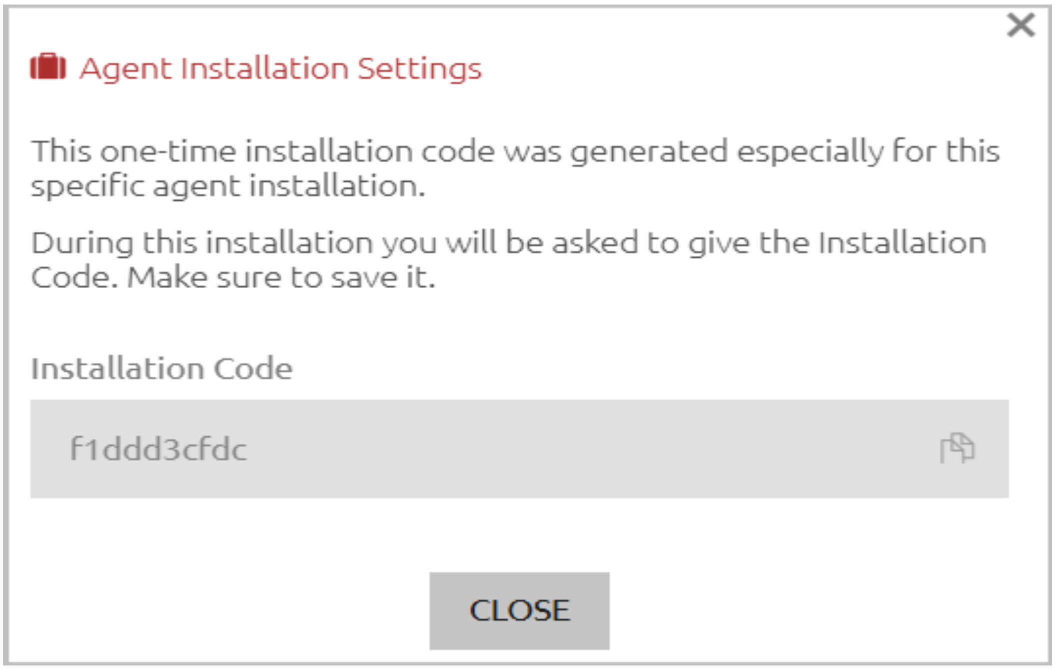
Clicking ⋮ in the row of an Agent enables you to perform the following actions:

- **Disable / Enable:** Inactivates / Reactivates an installed Agent. (This action is not available for uninstalled Agents.) When disabling an Agent that is used by one or more applications, you need to confirm the action from a popup warning.
- **Delete:** Removes the Agent from the system. Agents that are being used by applications cannot be deleted.



| Actions | Name | Domain | Version |
|---|---|---|---|
| | Agent1 | | |
| | appl sql agent | do | 1.0.1.6 |
| | app sql | do | 1.0.1.6 |

Clicking ⤓ in the row of an uninstalled Agent opens the **Agent Installation Settings** popup, from which you can copy the code required for Agent installation.



Agent Installation Settings

This one-time installation code was generated especially for this specific agent installation.

During this installation you will be asked to give the Installation Code. Make sure to save it.

Installation Code

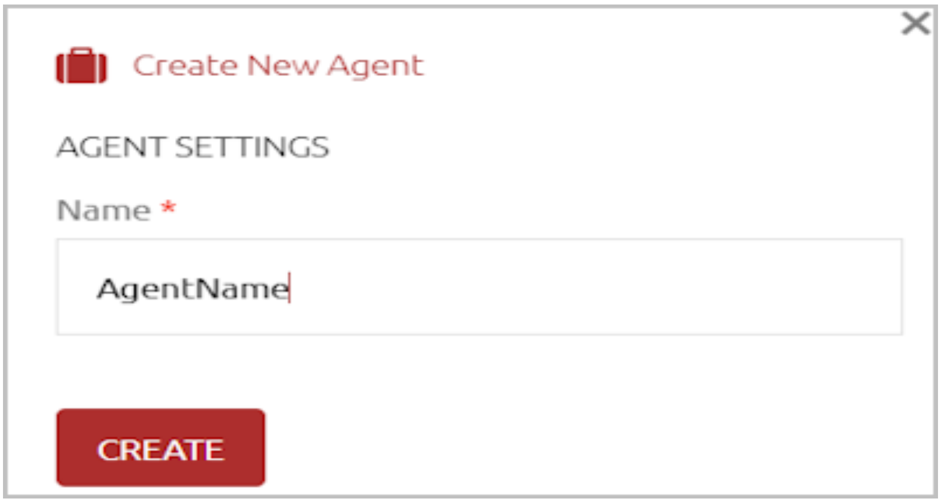
f1ddd3cfdc

### Adding SQL Agents

You can add multiple Octopus SQL Agents to the system. Every Agent added must be assigned a unique name.

**To add an Octopus SQL Agent:**

1. In the upper left corner of the **Agents** tab, click **Add Agent**.
2. In the popup that opens, enter a unique name for the new Agent. Then, click **Create**.



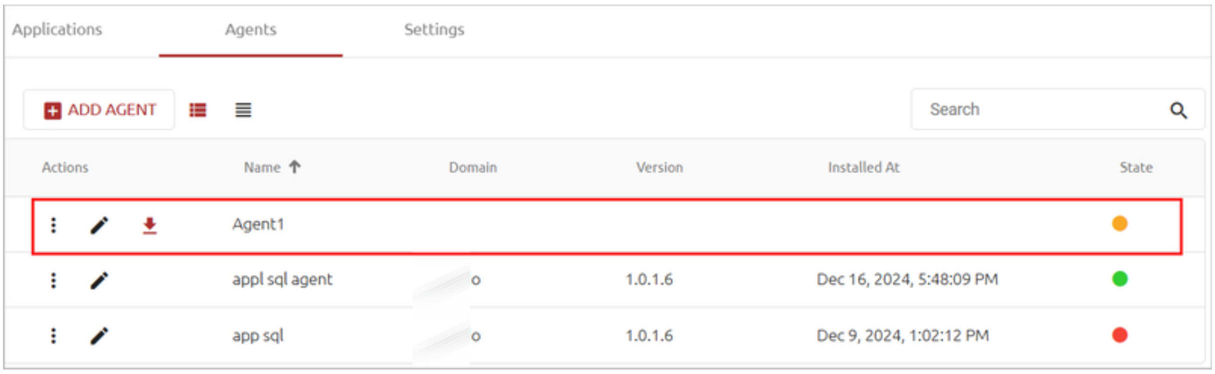
Create New Agent

AGENT SETTINGS

Name *

AgentName

The **Create New Agent** popup closes, and a row for the new Agent is added to the **Agents** tab.



| Actions | Name ↑ | Domain | Version | Installed At | State |
|---|---|---|---|---|---|
| ⋮ ✎ ⬇ | Agent1 | | | | ● |
| ⋮ ✎ | appl sql agent | o | 1.0.1.6 | Dec 16, 2024, 5:48:09 PM | ● |
| ⋮ ✎ | app sql | o | 1.0.1.6 | Dec 9, 2024, 1:02:12 PM | ● |

3. Continue by installing the new Agent. For details and instructions, refer to the Octopus SQL Agent Installation Guide.

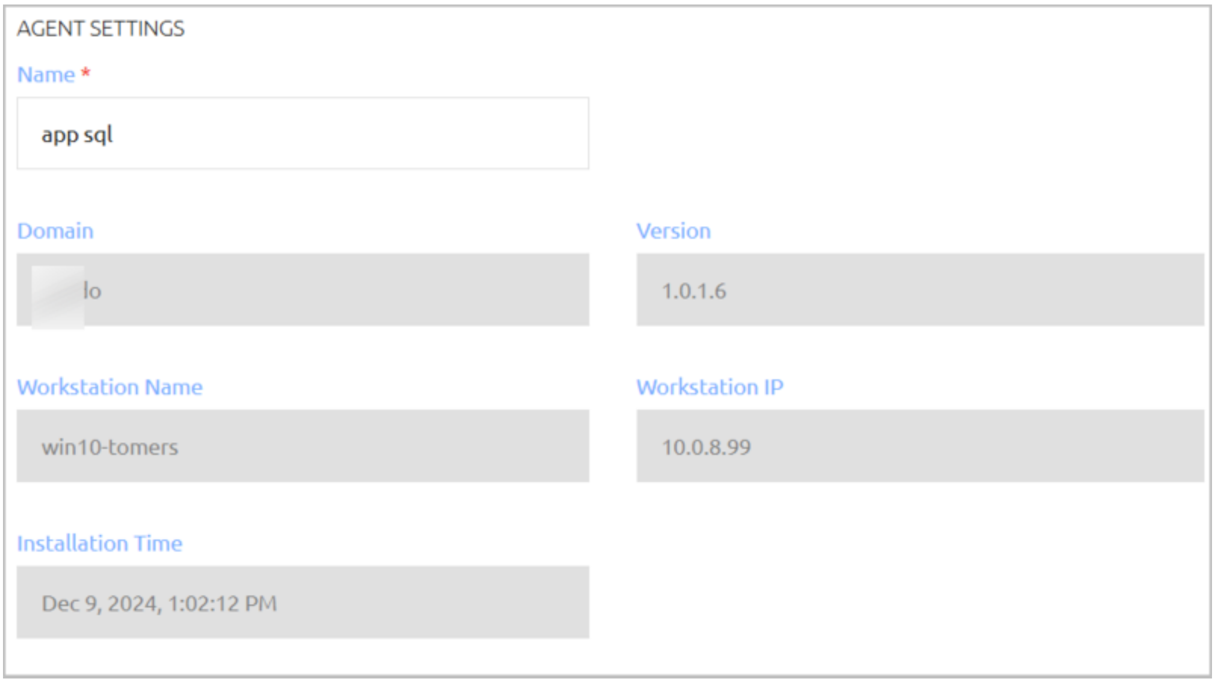
**Important**

The Octopus SQL Agent should be installed *before* adding an SQL type integrated application to the Management Console.

### Viewing SQL Agent Settings

Clicking ✎ in the row of an Agent opens the **Agent Settings** page, where you can change the name of the Agent. Enter the new name in the **Name** field, and then click **Save**.

The other settings for installed Agents cannot be updated. The settings displayed include the name and IP of the machine on which the Agent is installed, as well as domain, version and installation time.



AGENT SETTINGS

Name *: app sql

Domain: [redacted]lo

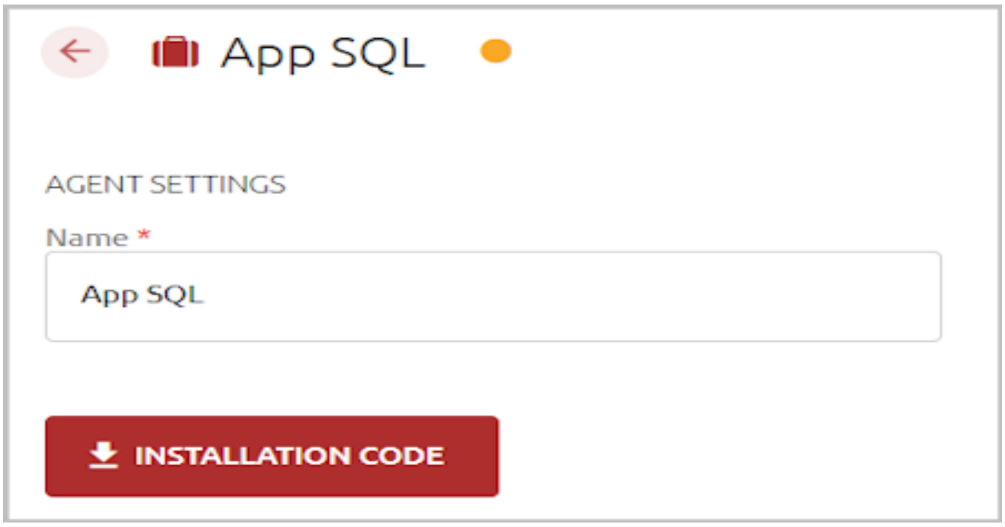
Version: 1.0.1.6

Workstation Name: win10-tomers

Workstation IP: 10.0.8.99

Installation Time: Dec 9, 2024, 1:02:12 PM

If the Agent has not yet been installed, the **Agent Settings** page has an **Installation Code** button. Clicking this button opens a popup from which you can copy the one-time code required for installing the Agent.



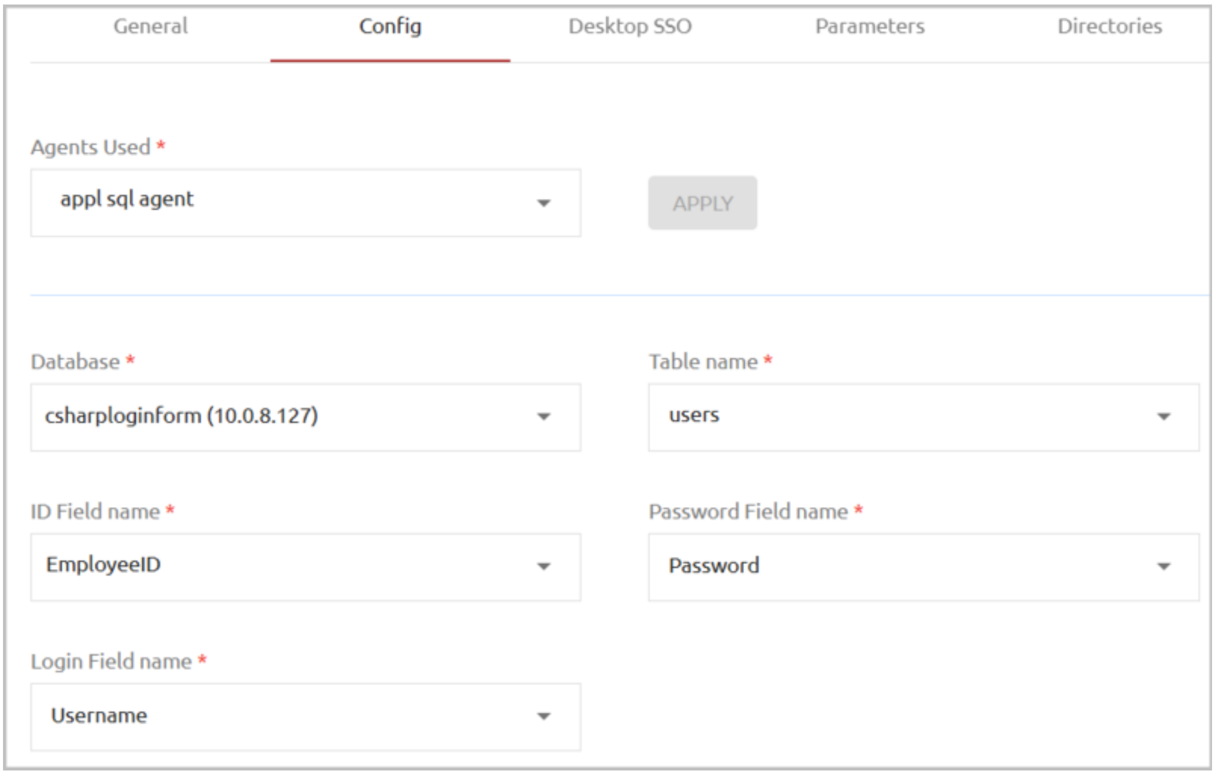
App SQL

AGENT SETTINGS

Name *: App SQL

## Selecting Application Database Configuration Settings

The **Config** tab of an integrated application's settings displays data related to the Octopus SQL Agent and the database with which it communicates. This tab is therefore enabled for SQL type applications only.



Agents Used *: appl sql agent

Database *: csharploginform (10.0.8.127)

Table name *: users

ID Field name *: EmployeeID

Password Field name *: Password

Login Field name *: Username

The upper portion of the tab displays the SQL Agent currently being used by the application, and allows you to assign a different one when required. To change the Agent being used, select the relevant Agent from the **Agents Used** list, and then click **Apply**.

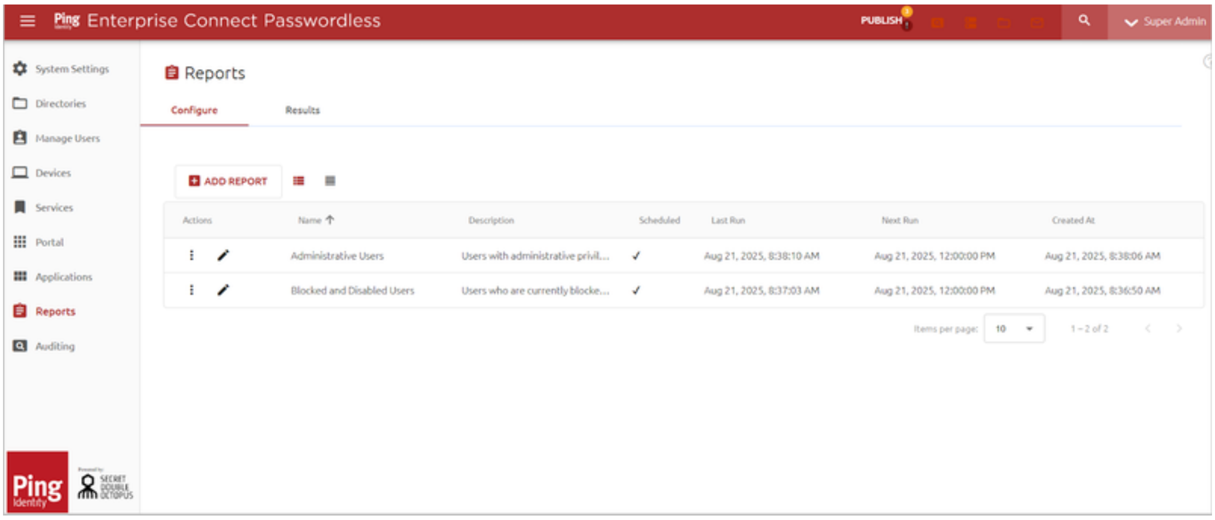
The lower portion of the tab shows the currently selected settings for directing the Octopus SQL Agent to locate user credentials in the application's database. By default, the settings shown are the ones that were configured upon installation of the SQL Agent. After installation, all settings except for **Database** may be updated by selecting a different option from the dropdown lists. The editable settings are:

| Setting | Description |
|---|---|
| Table name | Name of the database table storing user authentication credentials. |
| ID Field name | The attribute used by the SQL Agent to identify the user in the database. |
| Login Field Name | Name of the column holding the user credential to be entered in the Login field of the application. |
| Password Field Name | Name of the column holding the user credential to be entered in the Password field of the application. |

## Generating Reports

The **Reports** menu of the Management Console offers a variety of out-of-the-box report templates that enable you to easily track and monitor user status, enrollment trends, authentication events, and much more. A simple and intuitive report creation wizard is provided for each different report type, allowing you to add reports that are relevant for your needs and receive them in the format and at the frequency of your choice.

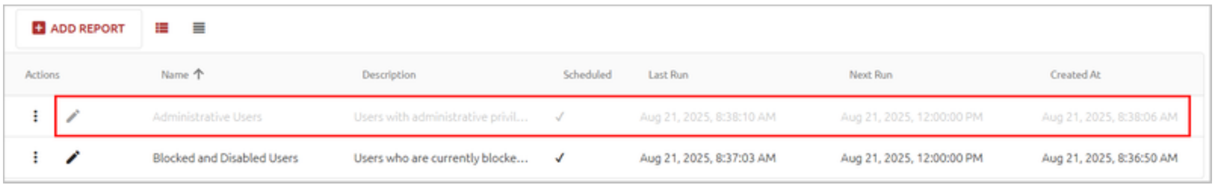
The **Configure** tab of the **Reports** menu lists all reports that have been added and displays basic scheduling information about each one.



| Actions | Name ↑ | Description | Scheduled | Last Run | Next Run | Created At |
|---|---|---|---|---|---|---|
| ⋮ ✎ | Administrative Users | Users with administrative privil... | ✓ | Aug 21, 2025, 8:38:10 AM | Aug 21, 2025, 12:00:00 PM | Aug 21, 2025, 8:38:06 AM |
| ⋮ ✎ | Blocked and Disabled Users | Users who are currently blocke... | ✓ | Aug 21, 2025, 8:37:03 AM | Aug 21, 2025, 12:00:00 PM | Aug 21, 2025, 8:36:50 AM |

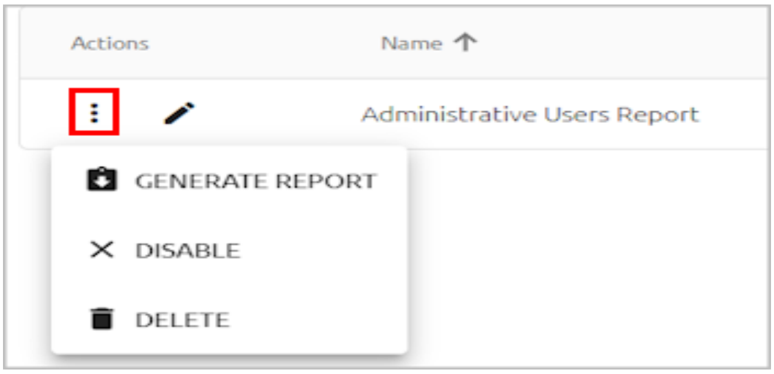
Clicking ⋮ in the **Actions** column enables you to perform the following operations on a report:

- **Generate Report:** Initiates immediate report generation.
- **Disable / Enable:** Inactivates / Reactivates the report generation schedule. The row of a disabled report is grayed out.



| Actions | Name ↑ | Description | Scheduled | Last Run | Next Run | Created At |
|---|---|---|---|---|---|---|
| ⋮ ✎ | Administrative Users | Users with administrative privil... | ✓ | Aug 21, 2025, 8:38:10 AM | Aug 21, 2025, 12:00:00 PM | Aug 21, 2025, 8:38:06 AM |
| ⋮ ✎ | Blocked and Disabled Users | Users who are currently blocke... | ✓ | Aug 21, 2025, 8:37:03 AM | Aug 21, 2025, 12:00:00 PM | Aug 21, 2025, 8:36:50 AM |

- **Delete:** Removes the report from the system.



Clicking ✎ in the row of a report opens the **Edit Report Definition** wizard, where you can review and update report parameters and settings.

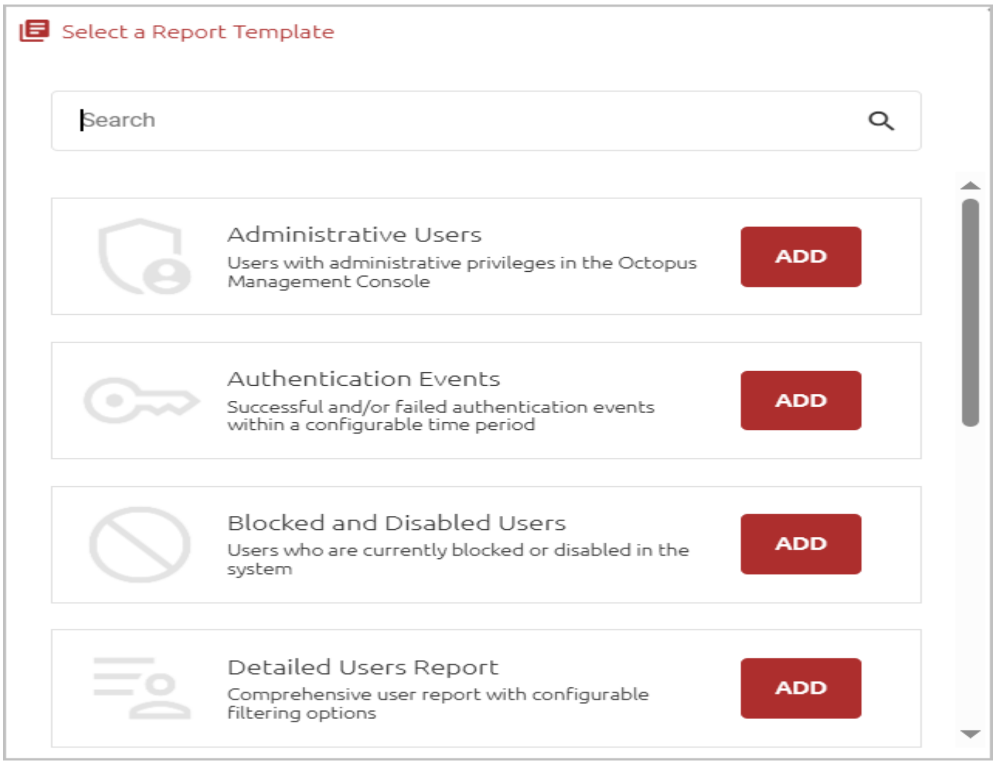
## Adding a New Report

Adding a report involves choosing a report template and then specifying parameters and settings in the relevant Report Definition wizard. Although some parameters can vary, depending on the type of report, the basic creation workflow is the same for all reports. The main steps for adding a new report are summarized in the procedure below.

**To add a new report:**

1. **Select the template:** At the top of the **Configure** tab, click **Add Report** to open the **Select a Report Template** dialog.

   Then, in the frame of the relevant report type, click **Add.**

   Select a Report Template

   Search

   Administrative Users
   Users with administrative privileges in the Octopus Management Console
   ADD

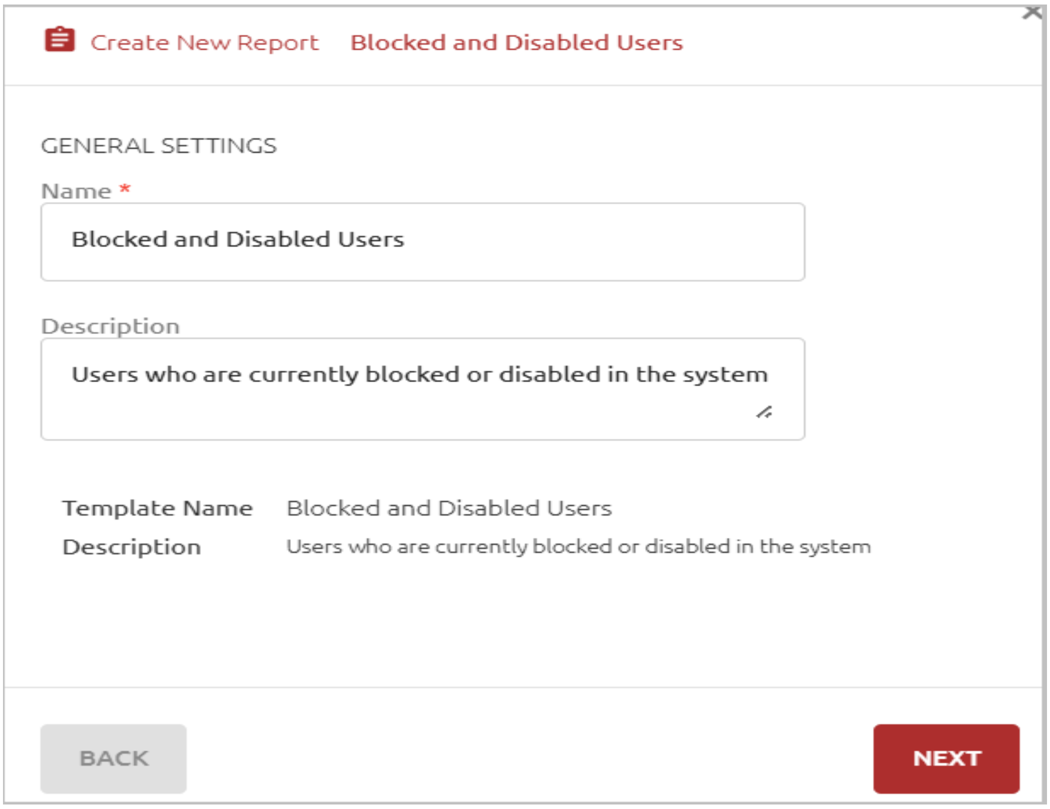
   Authentication Events
   Successful and/or failed authentication events within a configurable time period
   ADD

   Blocked and Disabled Users
   Users who are currently blocked or disabled in the system
   ADD

   Detailed Users Report
   Comprehensive user report with configurable filtering options
   ADD

2. **Name your report:** On the **General Settings** page of the **Create New Report Definition** wizard, give the report a name (required) and a description (optional).

   Then, click **Next.**



Create New Report Blocked and Disabled Users

GENERAL SETTINGS

Name *

Blocked and Disabled Users

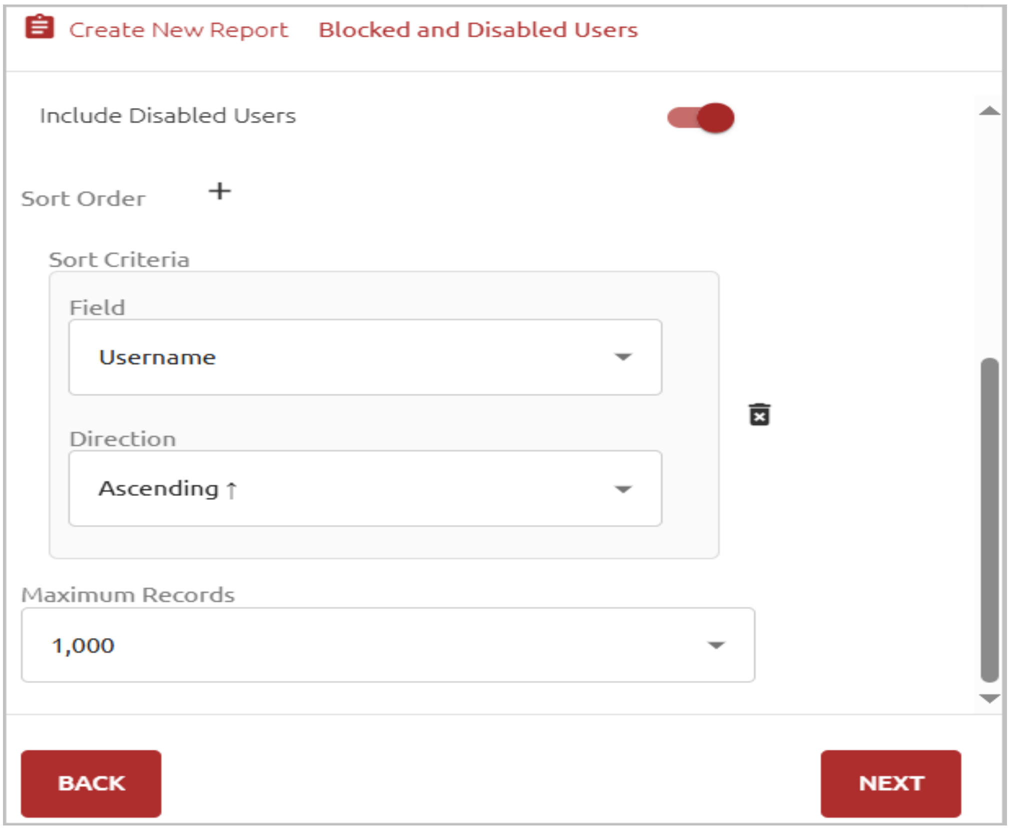
Description

Users who are currently blocked or disabled in the system

Template Name Blocked and Disabled Users

Description Users who are currently blocked or disabled in the system

3. **Specify report parameters:** Parameters vary according to report type, but some common settings are:
   - **Fields to Include** in the report, such as username, role, invitation type, authentication method, etc.
   - **Sort Criteria:** This section enables you to add fields according to which the report can be sorted and specify sorting order (ascending or descending).
   - **Maximum Records:** Select **100**, **500**, **1000**, **5000** or **All records**.



Create New Report Blocked and Disabled Users

Include Disabled Users: on

Sort Order +

Sort Criteria

Field: Username

Direction: Ascending ↑

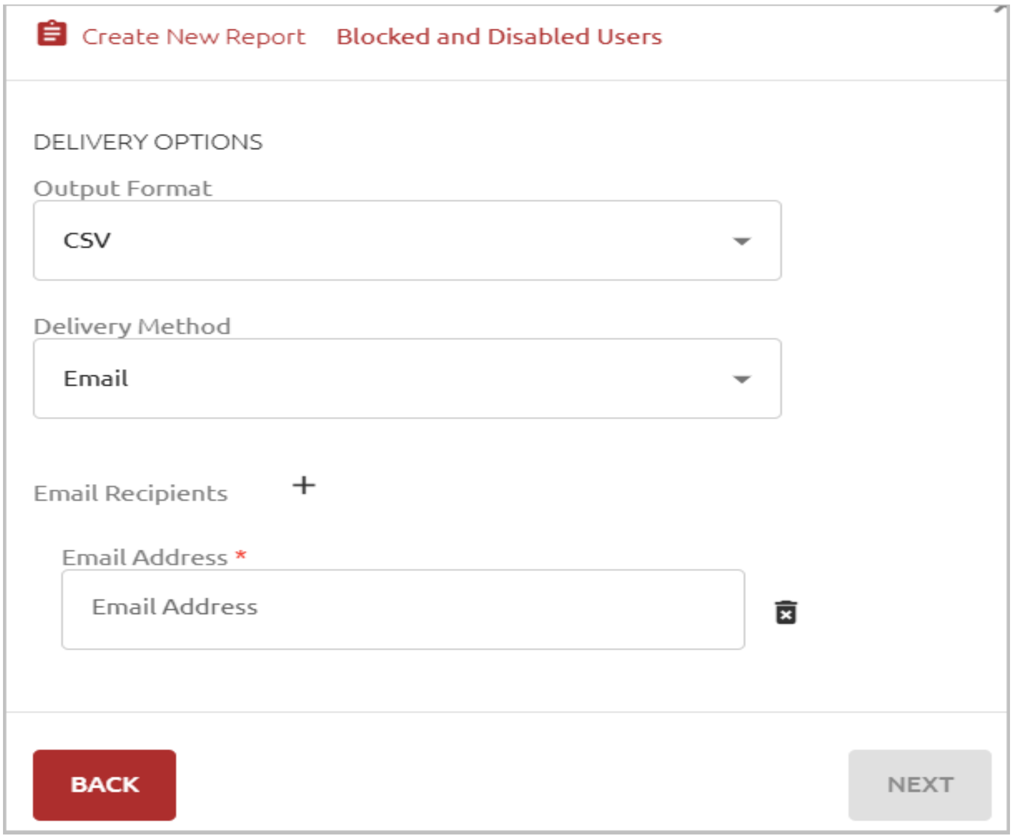
Maximum Records: 1,000

4. Set **Delivery Options**:

   ○ **Output Format:** Choose **CSV**, **Excel**, **PDF** or **JSON**.

   ○ **Delivery Method:** Select **Email** or **Download**.

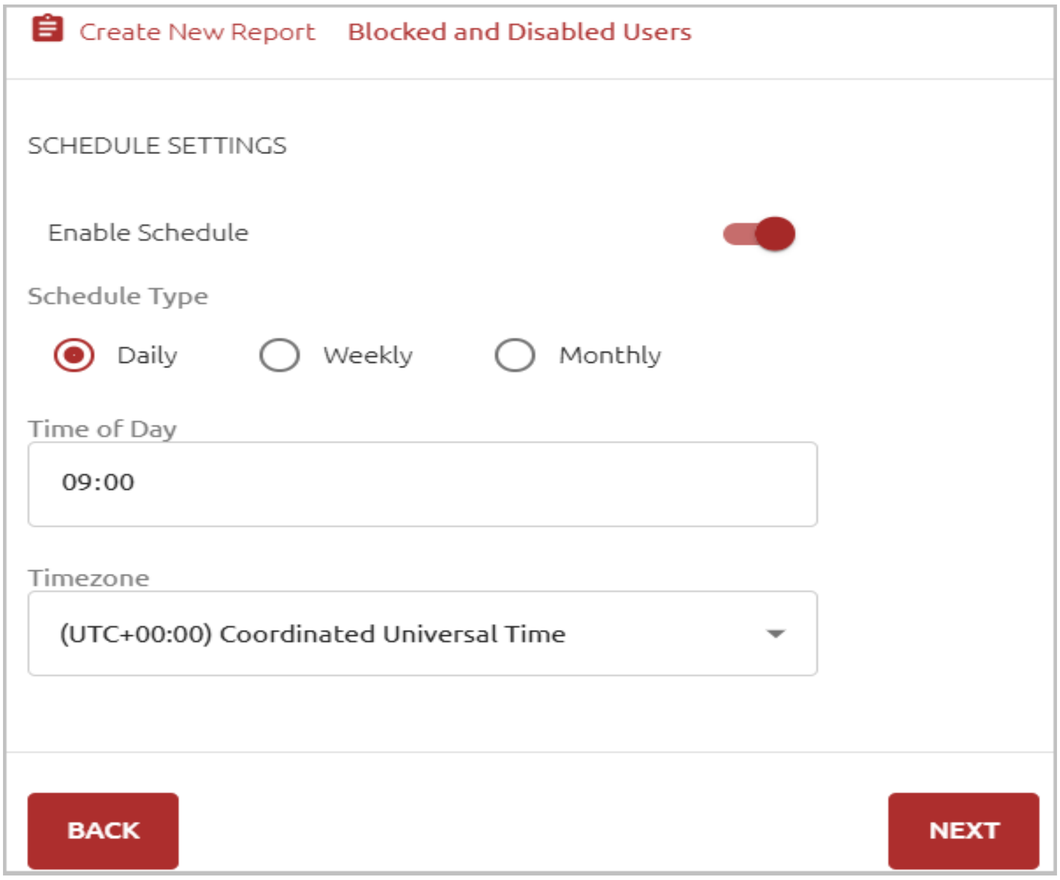
     If you choose **Email**, at least one email address needs to be provided.



Output Format: CSV

Delivery Method: Email

5. Configure **Schedule Settings**: Choose daily, weekly or monthly delivery. Then, specify time of delivery and choose a timezone.



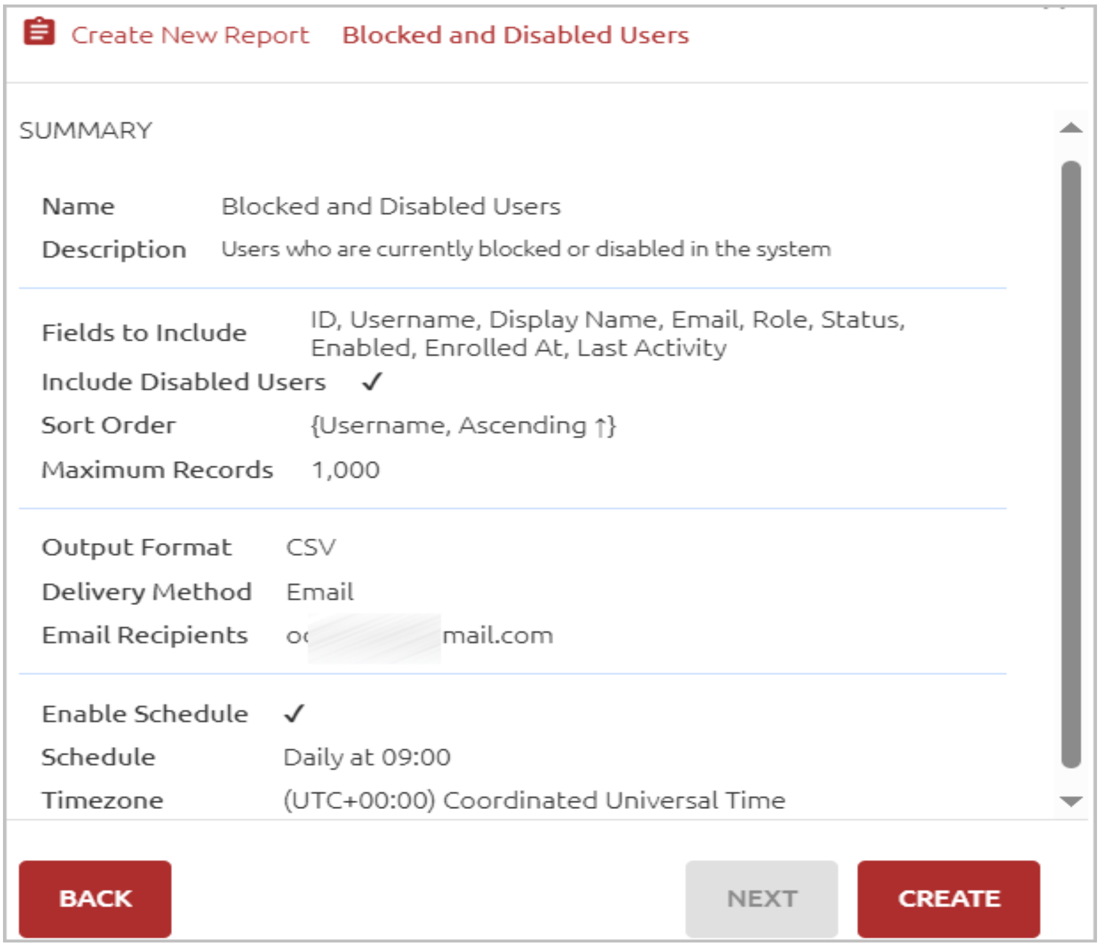
Enable Schedule: on

Schedule Type: ● Daily ○ Weekly ○ Monthly

Time of Day: 09:00

Timezone: (UTC+00:00) Coordinated Universal Time

6. **Review and save:** Check the information displayed on the **Summary** page. To add the report, click **Create**.

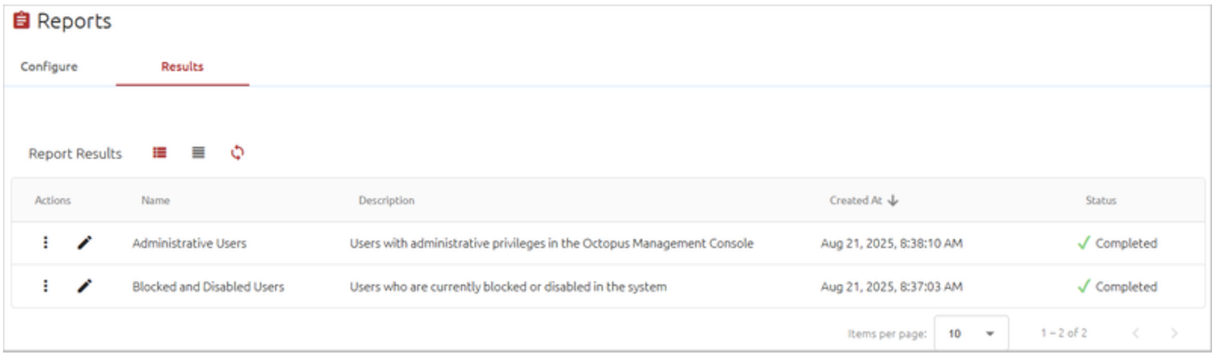


SUMMARY

| | |
|---|---|
| Name | Blocked and Disabled Users |
| Description | Users who are currently blocked or disabled in the system |
| Fields to Include | ID, Username, Display Name, Email, Role, Status, Enabled, Enrolled At, Last Activity |
| Include Disabled Users | ✓ |
| Sort Order | {Username, Ascending ↑} |
| Maximum Records | 1,000 |
| Output Format | CSV |
| Delivery Method | Email |
| Email Recipients | o[redacted]mail.com |
| Enable Schedule | ✓ |
| Schedule | Daily at 09:00 |
| Timezone | (UTC+00:00) Coordinated Universal Time |

## Viewing and Managing Report Results

The **Results** tab of the **Reports** menu lists all report execution results. The grid on this page displays the name, description, generation timestamp and status (**Completed** or **Failed**) of each result. Clicking the Refresh icon at the top of the grid updates the list with the latest results from the database.

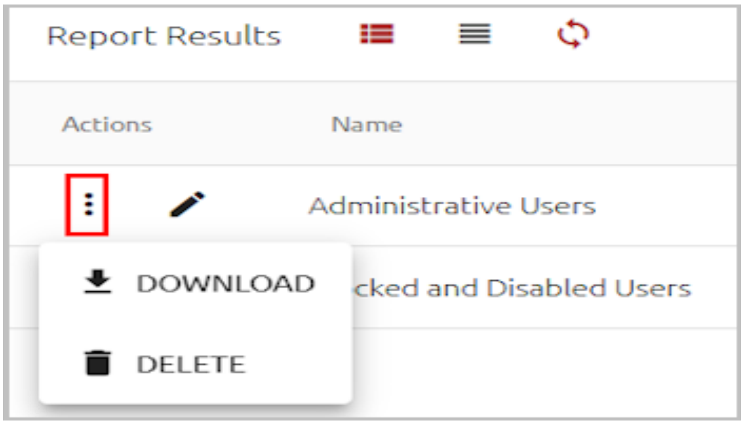


Report Results

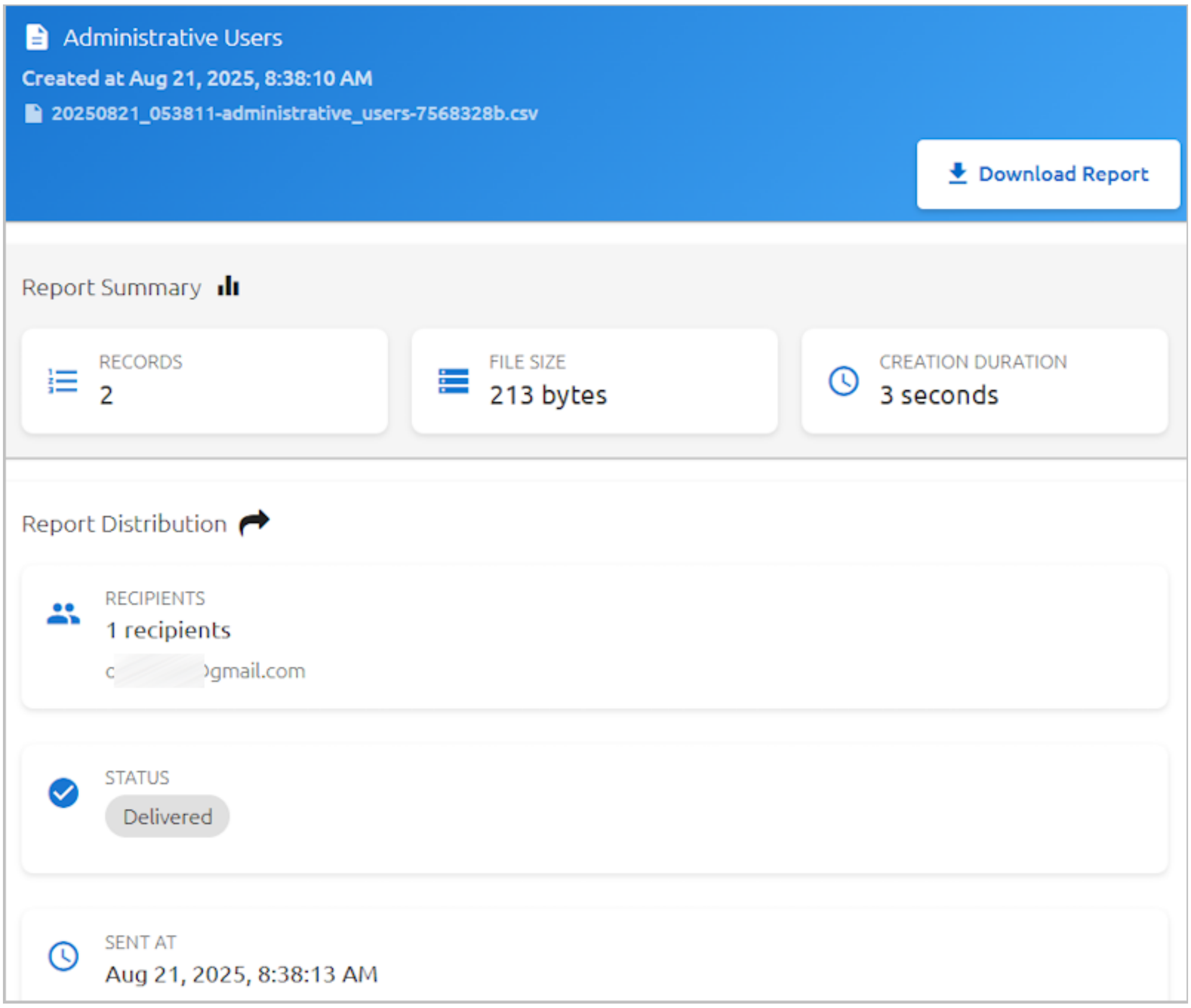
| Actions | Name | Description | Created At ↓ | Status |
|---|---|---|---|---|
| ⋮ ✎ | Administrative Users | Users with administrative privileges in the Octopus Management Console | Aug 21, 2025, 8:38:10 AM | ✓ Completed |
| ⋮ ✎ | Blocked and Disabled Users | Users who are currently blocked or disabled in the system | Aug 21, 2025, 8:37:03 AM | ✓ Completed |

Clicking ⋮ in the **Actions** column enables you to perform the following operations on a report output:

- **Download:** Saves the report output locally.
- **Delete:** Removes the report output from the list.



Clicking ✎ in the row of a report output allows you to preview some report highlights, such as number of records in the report, file size, the list of recipients (if relevant), and more. You can also download the report from this page.



Administrative Users

Created at Aug 21, 2025, 8:38:10 AM

20250821_053811-administrative_users-7568328b.csv

Report Summary

RECORDS
2

FILE SIZE
213 bytes

CREATION DURATION
3 seconds

Report Distribution

RECIPIENTS
1 recipients
c[redacted])gmail.com

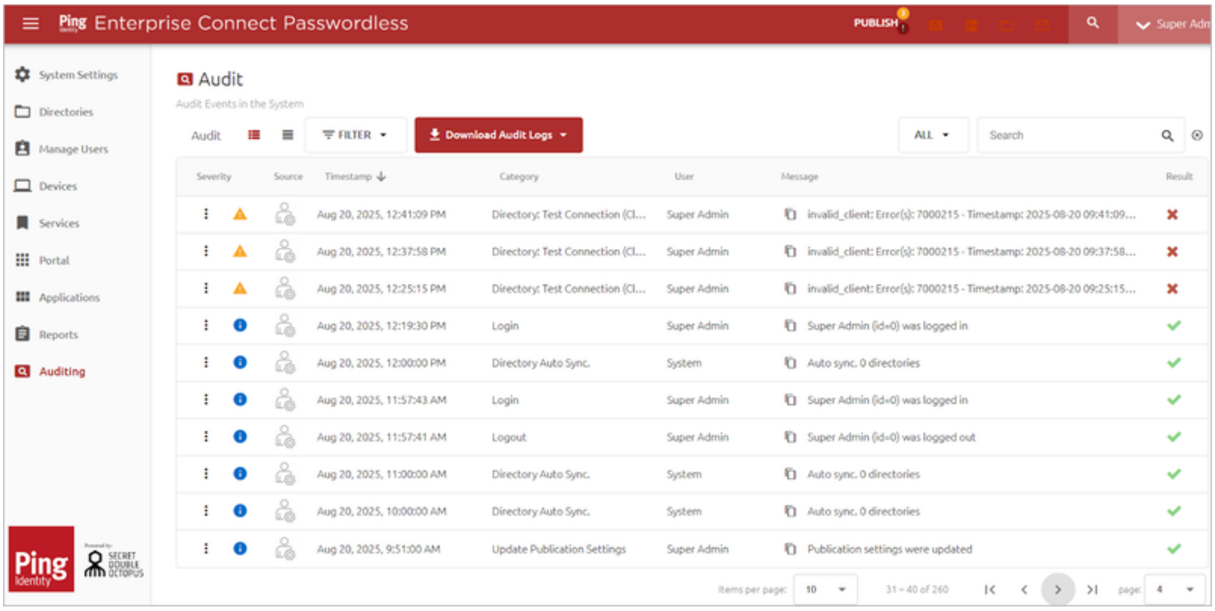
STATUS
Delivered

SENT AT
Aug 21, 2025, 8:38:13 AM

## Auditing Events

The Management Console records and logs all actions completed or attempted by users and other system components (e.g., servers).  You can use these records for troubleshooting, auditing, and fulfilling regulatory requirements.

To view the list of auditing events, select **Auditing** from the menu bar. By default, all recorded events are listed. You can filter the list according to event severity, source, session ID and more, as described in the sections below.



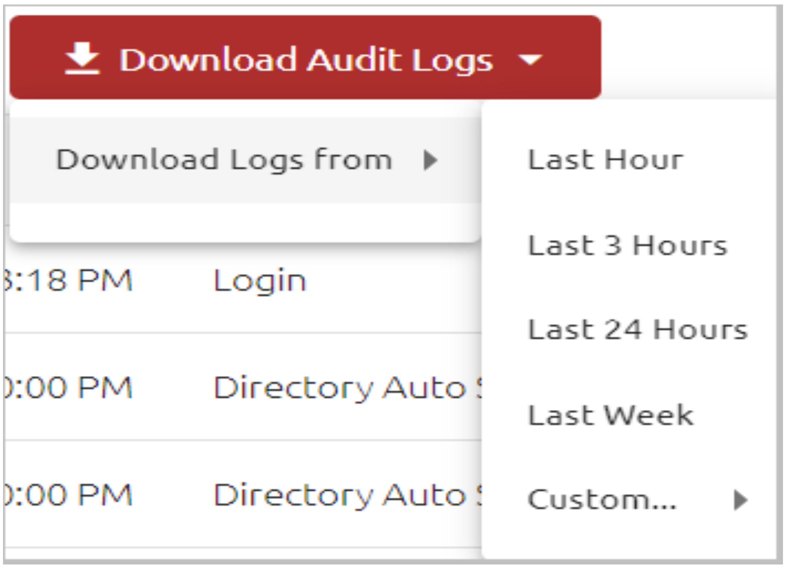
| Severity | Source | Timestamp | Category | User | Message | Result |
|---|---|---|---|---|---|---|
| ⚠ | | Aug 20, 2025, 12:41:09 PM | Directory: Test Connection (Cl... | Super Admin | invalid_client: Error(s): 7000215 - Timestamp: 2025-08-20 09:41:09... | ✗ |
| ⚠ | | Aug 20, 2025, 12:37:58 PM | Directory: Test Connection (Cl... | Super Admin | invalid_client: Error(s): 7000215 - Timestamp: 2025-08-20 09:37:58... | ✗ |
| ⚠ | | Aug 20, 2025, 12:25:15 PM | Directory: Test Connection (Cl... | Super Admin | invalid_client: Error(s): 7000215 - Timestamp: 2025-08-20 09:25:15... | ✗ |
| ℹ | | Aug 20, 2025, 12:19:30 PM | Login | Super Admin | Super Admin (id=0) was logged in | ✓ |
| ℹ | | Aug 20, 2025, 12:00:00 PM | Directory Auto Sync. | System | Auto sync. 0 directories | ✓ |
| ℹ | | Aug 20, 2025, 11:57:43 AM | Login | Super Admin | Super Admin (id=0) was logged in | ✓ |
| ℹ | | Aug 20, 2025, 11:57:41 AM | Logout | Super Admin | Super Admin (id=0) was logged out | ✓ |
| ℹ | | Aug 20, 2025, 11:00:00 AM | Directory Auto Sync. | System | Auto sync. 0 directories | ✓ |
| ℹ | | Aug 20, 2025, 10:00:00 AM | Directory Auto Sync. | System | Auto sync. 0 directories | ✓ |
| ℹ | | Aug 20, 2025, 9:51:00 AM | Update Publication Settings | Super Admin | Publication settings were updated | ✓ |

Items per page: 10 31 – 40 of 260 page: 4

The grid on the **Auditing** page provides the following information about each event:

| Column | Description / Notes |
|---|---|
| Severity | The extent to which the event affects normal system functioning. For details, refer to Understanding Severity, Sources and Results of Events. |
| Source | The system component or element where the event took place. For more information, refer to Understanding Severity, Sources and Results of Events. |
| Timestamp | Date and time of event occurrence. |
| Category | Type of event. |
| User | Name or username of the entity performing the event. |
| Message | A brief summary of the event. You can view additional data by clicking the icon in the **Severity** column (Viewing Event Details). |
| Result | Icons indicating the status of the event. For details, refer to Understanding Severity, Sources and Results of Events. |

To download auditing events in CSV format, click **Download Audit Logs** and select a timeframe.



Then, in the confirmation popup, click **Download**.

**Note**

When auditing filters are selected, the filtered Audit list is downloaded.

## Understanding Severity, Sources and Results of Events

Event *severity* reflects the degree of impact (or potential impact) of the event on normal system operation and end user experience. The severity levels are:

- ⊗ **Critical:** Events that interfere with system functioning, such as LDAP service errors, system component connectivity issues, etc.
- ⚠ **Warning:** Events that interfere with management and administrative operations (e.g., unsuccessful Admin login to the Management Console).
- ℹ **Info:** Events involving routine flows, actions and operations.

**Important**

All events related to user authentication have a severity level of **Info**, regardless of whether authentication succeeded.

The *source* is the system component that generated the event or that served as the event venue. Possible sources are:

| Icon | Source Name | Description | Sample Event |
|---|---|---|---|
| 🪪 | Authentication Server | The component responsible for processing authentication requests | Push delivery acknowledgment received from mobile device |
| 👤 | Management Console | The component responsible for administration and management of the product | Admin user logged in |

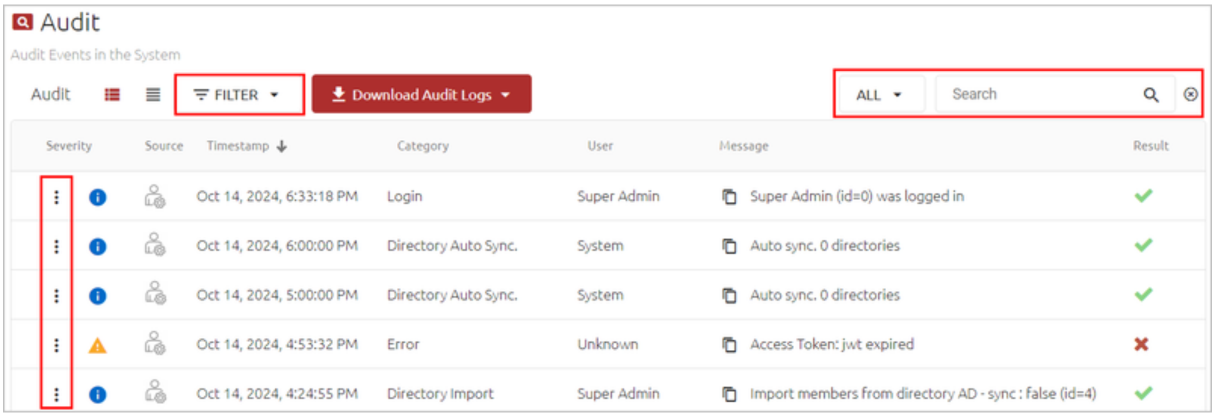
| Icon | Source Name | Description | Sample Event |
|---|---|---|---|
| 📱 | Octopus Mobile App | The Octopus Authenticator mobile application<br>**Important:** To receive events from this source, the **Enable Remote Audit** toggle in the Octopus Authenticator settings (**System Settings > Authenticators**) needs to be enabled. | Authentication request approved by user |
| 🖥 | Portal Server | The component responsible for user enrollment, access to supported web applications, and user self-service actions | Sending login request to Authentication Server |
| fido | FIDO Server | The component responsible for processing FIDO-specific authentication requests | Logged in from FIDO Server |

The icons in the **Result** column show the event's status. Possible results include:

| Icon | Status | Event Description |
|---|---|---|
| ✓ | Succeeded | Events that were executed and completed as expected. |
| ✗ | Failed | Events involving unsuccessful authentication, system errors, and system performance or connection issues. |
| ℹ | Challenged | Login events involving the Adaptive Authentication flow. |
| ⊂≡ | Bypassed | Login events involving authentication with username + password. This result is relevant only for events related to the ADPA service. |
| ℹ | Deferred | Login events in which the authentication push request is not received by the mobile app, and the Authentication Server then defers to the Octopus Agent to allow or prevent offline (e.g., BLE) authentication. Deferred events generally occur in scenarios involving insufficient mobile network coverage. |

## Filtering the Events List

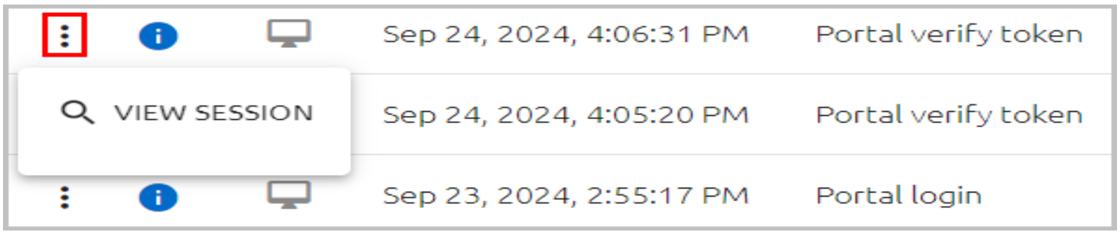
The filtering features at the top of the **Auditing** menu enable you to filter displayed events according to session ID, severity, source, result, and/or a specific search term, such as a user. Multiple filtering methods can be used simultaneously.



| | Severity | Source | Timestamp | Category | User | Message | Result |
|---|---|---|---|---|---|---|---|
| ⋮ | ⓘ | | Oct 14, 2024, 6:33:18 PM | Login | Super Admin | Super Admin (id=0) was logged in | ✓ |
| ⋮ | ⓘ | | Oct 14, 2024, 6:00:00 PM | Directory Auto Sync. | System | Auto sync. 0 directories | ✓ |
| ⋮ | ⓘ | | Oct 14, 2024, 5:00:00 PM | Directory Auto Sync. | System | Auto sync. 0 directories | ✓ |
| ⋮ | ⚠ | | Oct 14, 2024, 4:53:32 PM | Error | Unknown | Access Token: jwt expired | ✗ |
| ⋮ | ⓘ | | Oct 14, 2024, 4:24:55 PM | Directory Import | Super Admin | Import members from directory AD - sync : false (id=4) | ✓ |

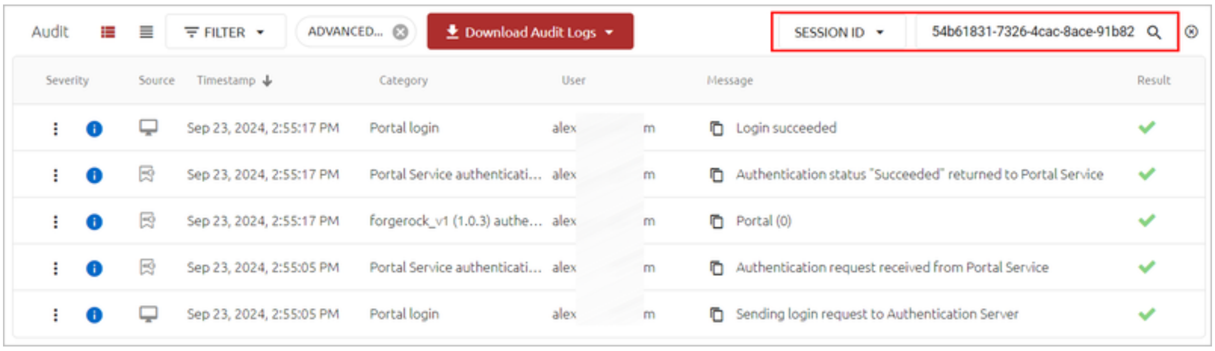
### Filtering by Session ID

The View Session feature allows you to quickly filter the **Auditing** list for all events related to a specific authentication session. In the row of a relevant event, click ⋮ and then select **View Session**.



| | | | | |
|---|---|---|---|---|
| ⋮ | ⓘ | | Sep 24, 2024, 4:06:31 PM | Portal verify token |
| | | | Sep 24, 2024, 4:05:20 PM | Portal verify token |
| ⋮ | ⓘ | | Sep 23, 2024, 2:55:17 PM | Portal login |

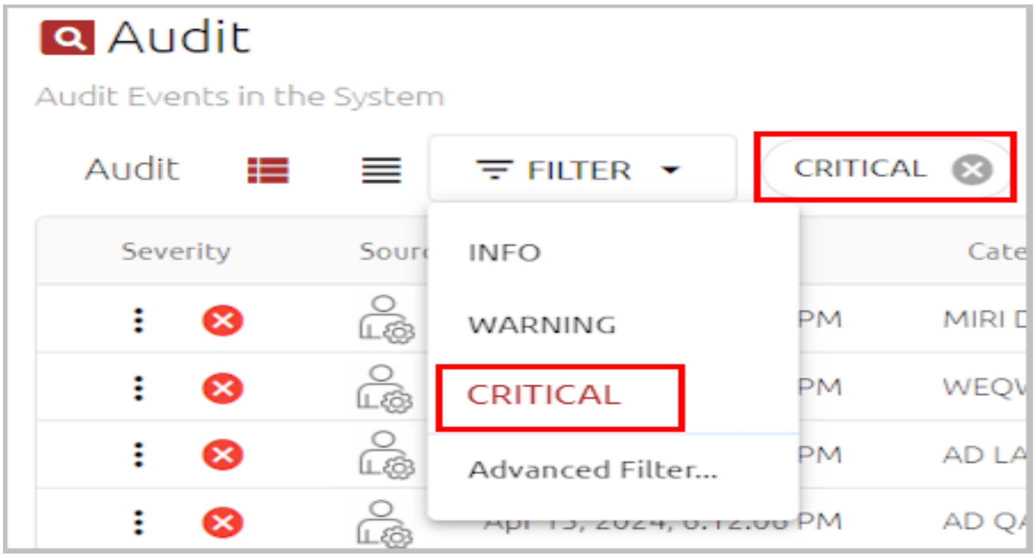
The **Auditing** list immediately displays only events that share the same Session ID as the selected event. The following example shows the complete sequence of events involved in authentication to the User Portal.



| | Severity | Source | Timestamp | Category | User | Message | Result |
|---|---|---|---|---|---|---|---|
| ⋮ | ⓘ | | Sep 23, 2024, 2:55:17 PM | Portal login | alex[redacted]m | Login succeeded | ✓ |
| ⋮ | ⓘ | | Sep 23, 2024, 2:55:17 PM | Portal Service authenticati... | alex[redacted]m | Authentication status "Succeeded" returned to Portal Service | ✓ |
| ⋮ | ⓘ | | Sep 23, 2024, 2:55:17 PM | forgerock_v1 (1.0.3) authe... | alex[redacted]m | Portal (0) | ✓ |
| ⋮ | ⓘ | | Sep 23, 2024, 2:55:05 PM | Portal Service authenticati... | alex[redacted]m | Authentication request received from Portal Service | ✓ |
| ⋮ | ⓘ | | Sep 23, 2024, 2:55:05 PM | Portal login | alex[redacted]m | Sending login request to Authentication Server | ✓ |

### Filtering by Event Severity, Source and Result

The Filter feature on the upper left side of the **Audit** list enables you to display events matching specified severity levels, sources and/or results. To view all events of a given severity, click the relevant option. To restore the default view, close the filtering chip to the right of the **Filter** list.

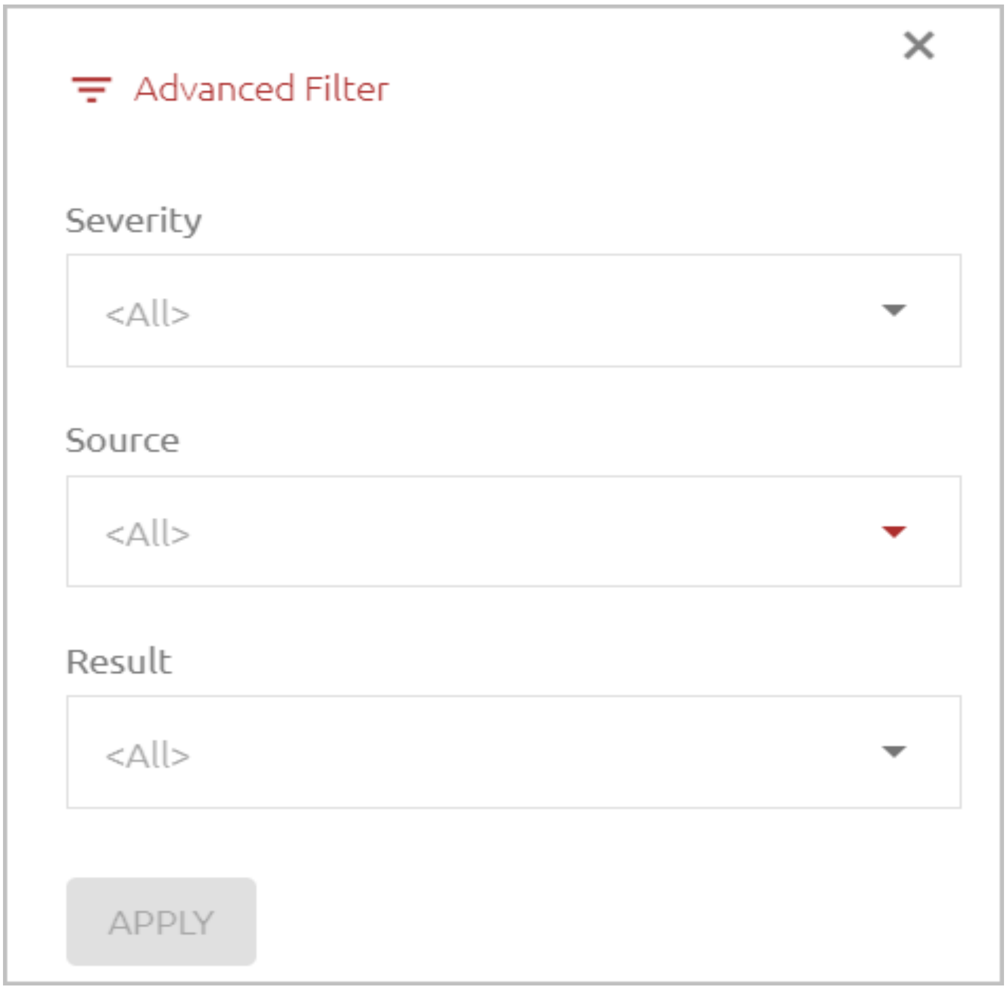


The **Advanced Filter** option supports multi-factor filtering, including combinations of different severity levels, sources and results.

**To use the Advanced Filter feature:**

1. From the **Filter** list, select **Advanced Filter**.

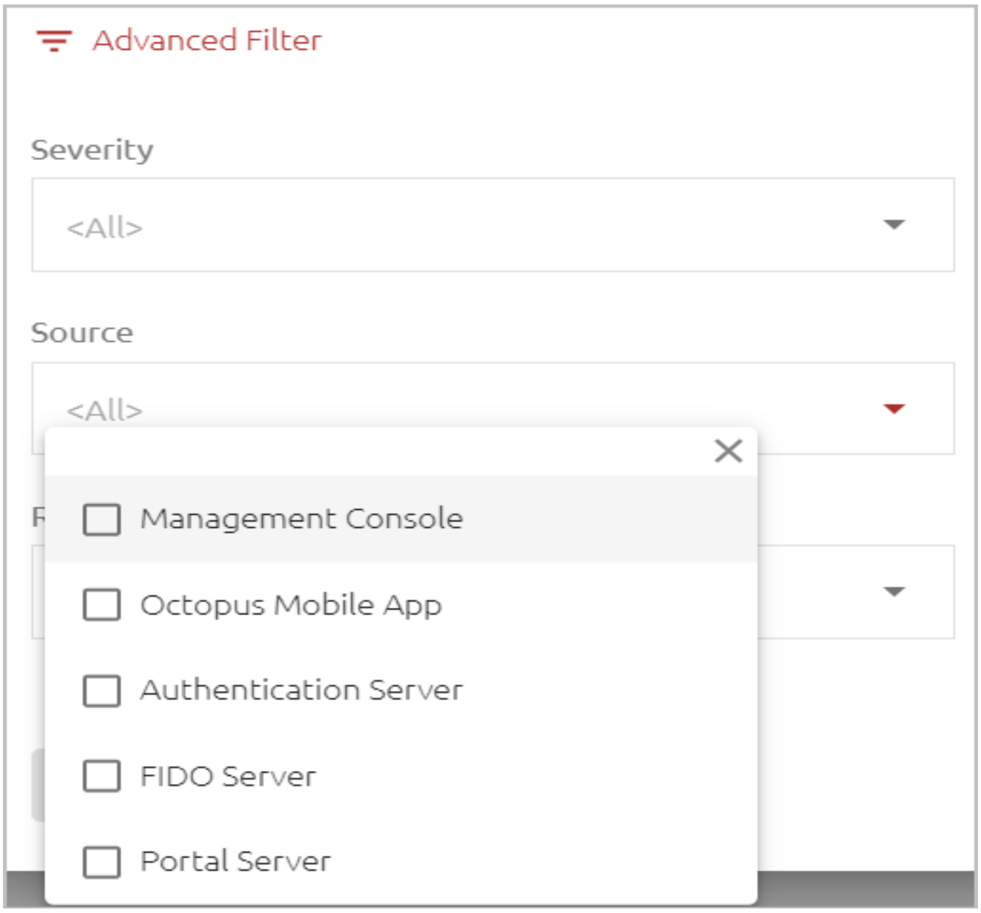
   The **Advanced Filter** dialog opens.



2. Open each list and select the checkboxes of the required severities, sources and results. Note that only elements and components included in the current **Auditing** list are displayed as selection options. For example, if there are no events in the list whose source is the mobile app, **Octopus Mobile App** will not appear in the Advanced Search **Source** list.

**Note**

To receive events from the Mobile App, verify that the **Enable Remote Audit** toggle in the Octopus Authenticator settings (**System Settings > Authenticators**) is enabled.



Advanced Filter

Severity

<All>

Source

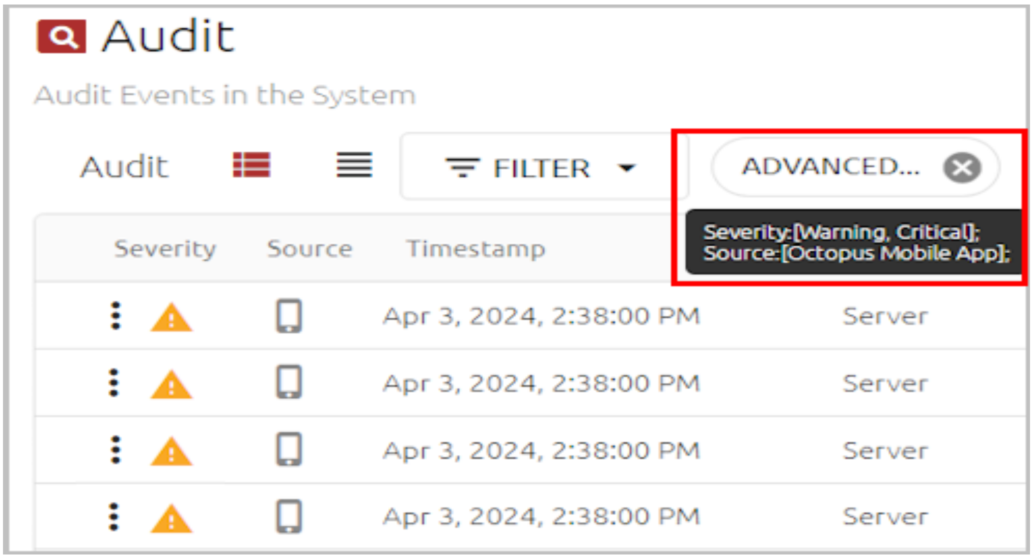
<All>

- □ Management Console
- □ Octopus Mobile App
- □ Authentication Server
- □ FIDO Server
- □ Portal Server

After making your selection(s), close the list by clicking **X** or clicking anywhere outside the list.

3. Click **Apply**.

   The **Audit** list is filtered according to your selections. To view the current filters, hover over the filtering chip to display the tooltip. For example:



Audit

Audit Events in the System

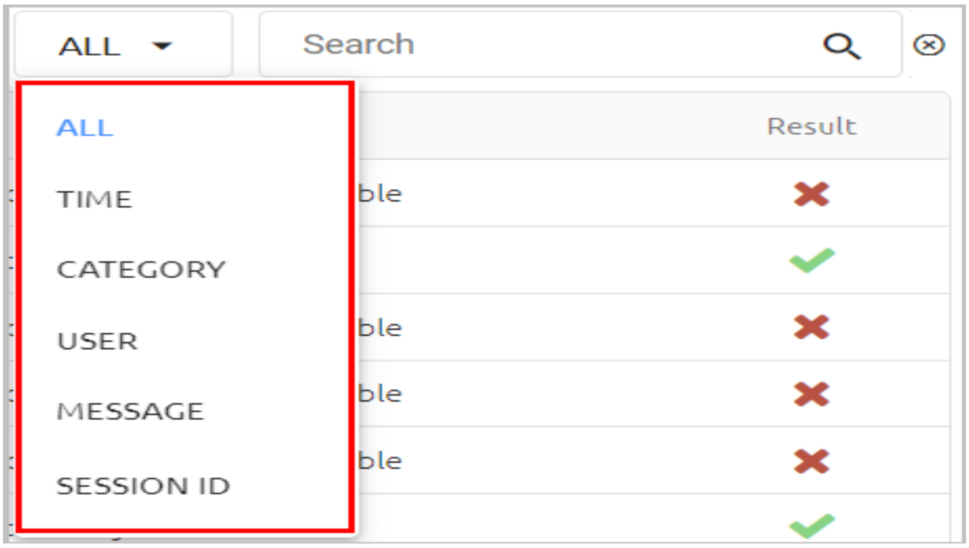
Severity:[Warning, Critical]; Source:[Octopus Mobile App];

|   | Severity | Source | Timestamp |   |
|---|---|---|---|---|
| ⋮ | ⚠ | 📱 | Apr 3, 2024, 2:38:00 PM | Server |
| ⋮ | ⚠ | 📱 | Apr 3, 2024, 2:38:00 PM | Server |
| ⋮ | ⚠ | 📱 | Apr 3, 2024, 2:38:00 PM | Server |
| ⋮ | ⚠ | 📱 | Apr 3, 2024, 2:38:00 PM | Server |

### Searching for Event Attributes and Keywords

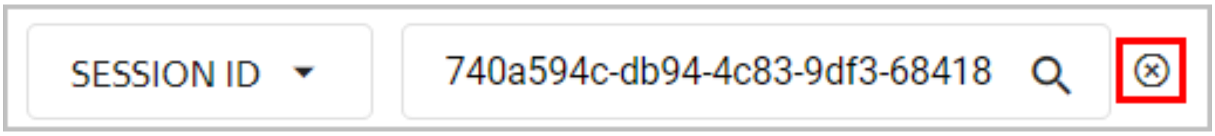
The Search tool in the upper right corner of the **Audit** list lets you filter the list according to a free text keyword. Enter the keyword in the **Search term** field, and then click the Search icon or press **<Enter>**.

To narrow the scope of your search, you can select an attribute from the list to the left of the Search tool before performing your keyword search. You may select any ONE attribute.



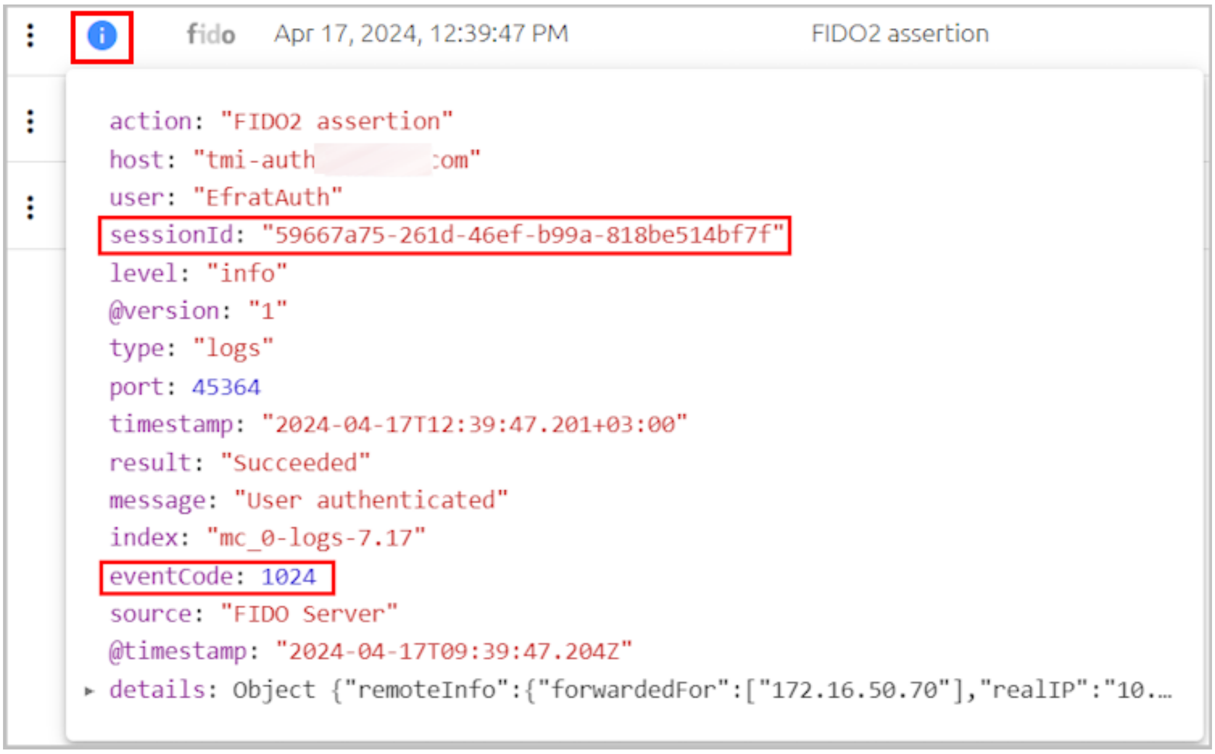
When using the **Time** attribute, specify the start and end dates by selecting them from the Calendar popup. The Events list is filtered automatically upon selecting the dates. After selecting other attributes, enter a relevant term in the **Search** field (such as a username, etc.), and then press **<Enter>**.

To quickly undo keyword filtering, click the Clear Search icon to the right of the **Search** field. (Any severity, source and/or result filtering will be maintained.)



## Viewing Event Details

To view more detailed data about an event, click the icon in the **Severity** column, in the row of the relevant event. Additional information about the event appears in a popup. The event code, unique session ID, data about the device used for authentication (if relevant) and other attributes are provided for each event, to help track and debug authentication sessions.



```
fido    Apr 17, 2024, 12:39:47 PM                FIDO2 assertion

  action: "FIDO2 assertion"
  host: "tmi-auth[redacted]om"
  user: "EfratAuth"
  sessionId: "59667a75-261d-46ef-b99a-818be514bf7f"
  level: "info"
  @version: "1"
  type: "logs"
  port: 45364
  timestamp: "2024-04-17T12:39:47.201+03:00"
  result: "Succeeded"
  message: "User authenticated"
  index: "mc_0-logs-7.17"
  eventCode: 1024
  source: "FIDO Server"
  @timestamp: "2024-04-17T09:39:47.204Z"
▸ details: Object {"remoteInfo":{"forwardedFor":["172.16.50.70"],"realIP":"10.…
```

To close the popup, click the icon again.

### Configuring the Logstash Address and Port

The Logstash address is user configurable. To customize the Logstash address and port, open **/opt/sdo/authserver/config/prod.json** and, within the top level, add the configuration shown in the following example.

```
"logstash": {
     "host": "127.0.0.1",
     "port": 10001
  }
```

When editing the file, be sure to maintain the correct JSON syntax. You can use the **/opt/sdo/authserver/config/base.json** file for reference as you work. (The prod.json will override the base.json configuration.)

## Appendix A: Using the Schema Mapping Script

The script *schema_mapping.sh* can be used to add fields to the schema of a directory. The fields you add will be brought from the Active Directory to the Octopus Authentication Server and will appear in the user profiles.

The following sections describe different parameters you can use with this script.

**list**

To display a list of all your Active Directories, run:

```
./schema_mapping.sh list
```

**add-to-schema**

Use this parameter to add an attribute to the directory schema. Follow these steps:

1. In the Active Directory VM, right-click on an object and select **Properties > Attribute Editor**.

   Then, choose the relevant attribute.

2. In your VM, run:

   ```
   ./schema-mapping.sh add-to-schema <id of the relevant
   directory> <Name of the attribute to appear in the Octopus MC>
   <Name of the attribute in the AD> <Type of attribute (text,
   bin, sid)>
   ```

**reset-schema**

To return the schema to its original structure, run:

```
./schema_mapping.sh reset-schema
```

## Appendix B: Authentication Error Codes and Reject Reasons

The following table lists the different error codes related to rejection of authentication requests. It also explains the reasons for the rejections and provides possible workaround actions.

This information will help you to identify and correct conditions that result in 400 Bad Request errors.

| Error Code | Reject Reason | Workaround Action(s) | Message to User |
|---|---|---|---|
| 3001 | Local user mismatch | Allow offline | We cannot verify your identity. Please contact your administrator. |
| 3002 | No enrollments | Allow offline | We cannot verify your identity. Please contact your administrator. |
| 3003 | General error | Alternate BLE, Allow offline | We cannot verify your identity. Please try again later or contact your administrator. |
| 3004 | User not assigned to service | Allow offline | We cannot verify your identity. Please contact your administrator. |
| 3005 | User disabled | None | Authentication failed. Please contact your administrator. |
| 3006 | User blocked | None | Authentication failed. Please contact your administrator. |

| Error Code | Reject Reason | Workaround Action(s) | Message to User |
|---|---|---|---|
| 3007 | Service bypass enabled, direct bind failed (REST only) | None | Authentication failed. Please try again later or contact your administrator. |
| 3009 | Bypass, MFA failed | None | Authentication failed. Please try again later or contact your administrator. |
| 3010 | MFA failed | None | Authentication failed. Please try again later or contact your administrator. |
| 3011 | FIDO UUID mismatch | Alternate BLE, Allow offline | Authentication failed. Please try again later or contact your administrator. |
| 3012 | FIDO token not found | Alternate BLE, Allow offline | Authentication failed. Please try again later or contact your administrator. |
| 3013 | OTP fail | Alternate BLE, Allow offline | Authentication failed. Please check your OTP token and try again. |
| 3014 | Octopus Auth disabled | Alternate BLE, Allow offline | Authentication failed. Octopus Authenticator is not allowed. Please contact your administrator. |
| 3015 | Online OTP disabled | Alternate BLE, Allow offline | Authentication failed. Authentication using OTP is not available at this time. Please contact your administrator. |
| 3016 | 3rd party authenticator not available | Alternate BLE, Allow offline | Authentication failed. Current 3rd party authentication method is not available at this time. Please contact your administrator. |
| 3017 | No password in vault | N/A | Login Fail |
| 3018 | Login key not found | N/A | Login Fail |
| 3019 | Public key mismatch | None | Authentication failed. Security methods do not match. Please contact your administrator. |
| 3022 | Public key is missing from the request | None | Authentication failed. Security methods do not match. Please contact your administrator. |
| 3023 | Not a remote directory user | None | Authentication failed. Security methods do not match. Please contact your administrator. |

| Error Code | Reject Reason | Workaround Action(s) | Message to User |
|---|---|---|---|
| 3024 | Missing public key in storage | None | Authentication failed. Security methods do not match. Please contact your administrator. |
| 3025 | No password in vault | None | Authentication failed. We cannot verify your identity. Please contact your administrator. |
| 3026 | No 3rd party authenticator | Alternate BLE, Allow offline | Authentication failed. We cannot verify your identity. Please contact your administrator. |
| 3027 | Agent data unavailable | None | Authentication failed. Current 3rd party authentication method is not available at this time. Please contact your administrator. |
| 3028 | Error writing agent data | None | Authentication failed. Current 3rd party authentication method is not available at this time. Please contact your administrator. |
| 3021, 3040 | Unsupported agent version | N/A | Authentication failed. Security methods are not supported for this version. Please contact your administrator. |
| 3101, 3102, 3103, 3104, 3109 | ForgeRock OTP error | Alternate BLE, Allow offline | Authentication failed. Please check your ForgeRock OTP token and try again. |
| 3111, 3112, 3113, 3114, 3115, 3116, 3119 | ForgeRock push error | Alternate BLE, Allow offline | Authentication to ForgeRock failed. Please try again later or contact your administrator. |
| 3020 | OTP Octopus Authenticator disabled | Alternate BLE, Allow offline | Authentication failed. Octopus Authenticator is disabled. |
| 3031, 3132 | Auth delegation error | Alternate BLE, Allow offline | Authentication failed. Please contact your administrator. |

## Appendix C: List of Required Ports

The following table lists all ports that the Octopus Server requires for normal operation. These ports need to be available for successful installation and system operation.

| Port Number | Applicable Role | Service | Notes |
|---|---|---|---|
| 443 | AIO/AUTH/DMZ | nginx | portal/rest/adpa |
| 2222 | MC/AIO | sdomcbe/sshd | default/user configurable |
| 4444 | MC/AIO | sdomcbe | auth → mc comm |
| 5555 | AIO/AUTH/DMZ | reverse proxy (nginx) for the portal (local) | |
| 5432 | MC/AIO | postgresql | if configured and running |
| 6379 | MC/AIO/AUTH | redis | |
| 9600/10000 | MC/AIO | logstash | |
| 8008 | MC/AIO | nginx | /api and /doc when ssl is disabled |
| 8080 | AIO/AUTH/DMZ | reverse proxy (nginx) for webauthn (local) | |
| 8443 | MC/AIO | nginx | /api and /doc when ssl is enabled |
| 3000 | MC/AIO | reverse proxy (nginx) for sdomcbe | /api and /doc on 8443 or 8008 |
| 3331 | AIO/AUTH/DMZ | reverse proxy (nginx) for sdomon/rest (local) | mc → auth comm |
| 3332 | AIO/AUTH/DMZ | reverse proxy (nginx) for sdomon/adpa | |
| 3333 | AIO/AUTH/DMZ | reverse proxy (nginx) for sdomon/rest | |
| 3334 | AIO/AUTH/DMZ | reverse proxy (nginx) for sdomon/saml | |
| 3340 | AIO/AUTH/DMZ | reverse proxy (nginx) for sdomon/saml (metadata) | |
| 9200/9300 | AIO/MC | elasticsearch | |

| Port Number | Applicable Role | Service | Notes |
|---|---|---|---|
| 13700 + slot_id | MC/AIO | sdotun | mc → auth comm. Allocated for each connected authserver. The slot_id can be found in /opt/sdo/.conf of the authserver. |
| 14444 | AIO/AUTH/DMZ | sdotun | auth → mc comm tunneling |
| 16379 | AUTH/DMZ/secondaryMC | sdotun | redis tunneling |
| 10001 | AUTH/DMZ/AIO | sdotun | logstash tunneling |
| 12000 + dir_id | AUTH/AIO | ldap-proxy | |

## Appendix D: Adding FIDO Metadata to the System

The following procedure explains how to enable support for a new FIDO key using the JSON file from the FIDO Alliance repository.

**To add a new FIDO key to the system:**

1. Establish a secure connection (SSH) to the **Management Console** Server.
2. Navigate to the directory where the FIDO metadata is stored:

   ```
   cd /opt/sdo/etc/fido
   ```

3. Place the JSON file for an existing FIDO key. The copy should be named according to the AAGUID value of the new key. For example:

   ```
   cp fa2b99dc-9e39-4257-8f92-4a30d23c4118.json <AAGUID of new
   key>.json
   ```

**Note**

Verify that enable support for a new FIDO key using the JSON file from the FIDO Alliance repository.

4. Navigate to the directory containing the scripts:

   ```
   cd ../../mcbackendsql
   ```

5. Usage: *node./scripts/fidoMetadata.js add <file path> <tenantId>*

   Tenant ID is constant, as specified in Step 6.

6. Run the following script:

   ```
   node scripts/fidoMetadata.js add ../etc/fido/<AAGUID of new
   key>.json 11111111-1111-1111-1111-111111111111
   ```

7. On all Authentication Servers and Authentication Servers in the DMZ, run the following command to restart the service:

```
systemctl restart sdoweba
```

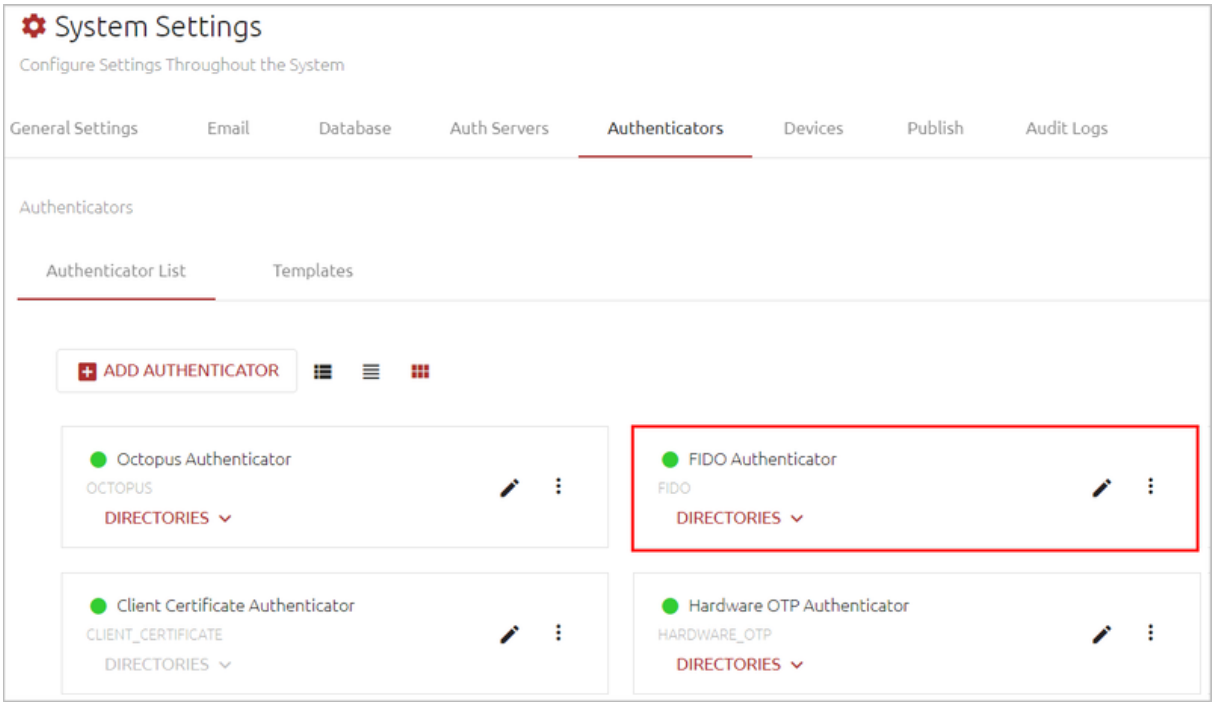
# Appendix E: Passkey Enrollment and Authentication

The Enterprise Connect Passwordless solution supports authentication to the User Portal and web applications using a passkey that is integrated with the user's workstation or smartphone. This appendix describes the prerequisites for successful passkey authentication and presents the flow for login to the User Portal.

## Requirements for Passkey Authentication

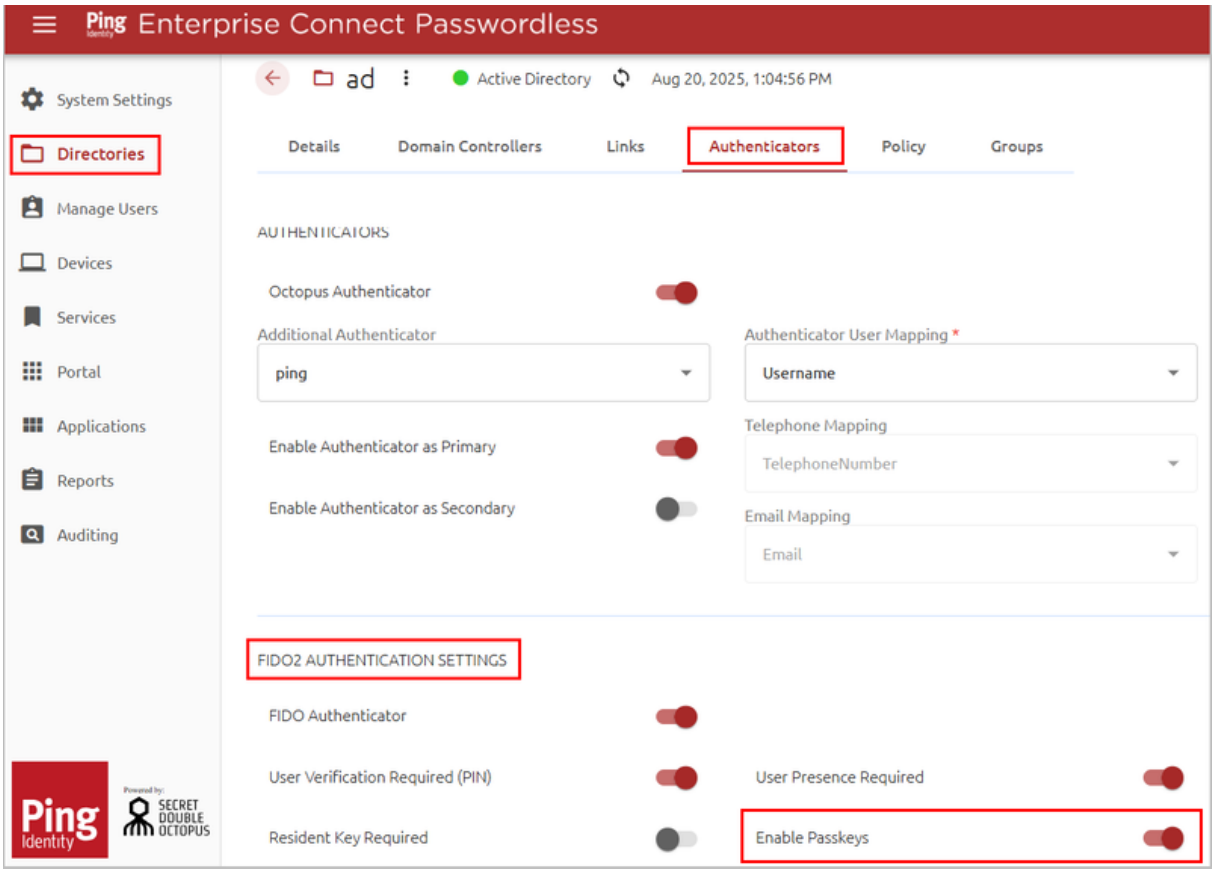
To enable passkey authentication, the following configuration needs to be done in the Enterprise Connect Management Console:

- From the **System Settings** menu, select the **Authenticators** tab and verify that the FIDO Authenticator is enabled and connected.



- From the **Directories** menu, click the Edit icon of the relevant directory to open the directory settings. Then, select the **Authenticators** tab.

  Under **FIDO2 Authentication Settings**, select the **Enable Passkeys** toggle to activate the setting.



AUTHENTICATORS

Octopus Authenticator: ●

Additional Authenticator: ping

Authenticator User Mapping *: Username

Telephone Mapping: TelephoneNumber

Email Mapping: Email

Enable Authenticator as Primary: ●

Enable Authenticator as Secondary: ○

FIDO2 AUTHENTICATION SETTINGS

FIDO Authenticator: ●

User Verification Required (PIN): ●

User Presence Required: ●

Resident Key Required: ○

Enable Passkeys: ●

In addition, users need to work with a passkey-supporting phone or a workstation with Windows Hello / Touch ID enabled with fingerprint sensor.

## Passkey Registration

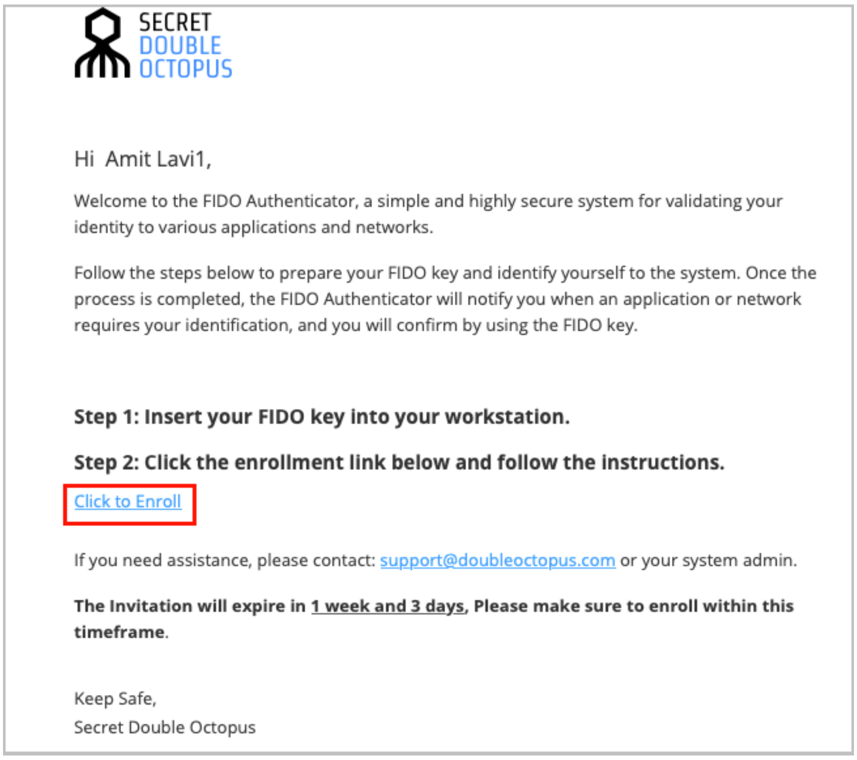
In order to authenticate to web applications using a passkey, users must first register (enroll) the passkey in the system. Users can perform registration after receiving an enrollment invitation email (for the FIDO Authenticator). Every passkey requires its own enrollment invitation.

**IMPORTANT:** Keys need to be enrolled from within the organization's network, or while connected to a network VPN. After enrollment, users will be able to use the passkey for authentication from both inside and outside the network.

The following procedure presents user instructions for passkey enrollment. Keep in mind that the registration process is controlled by the browser, so the exact flow and screenshots presented may vary for different browsers. The example in the procedure shows enrollment of a passkey stored on a mobile device, using the Chrome browser.

**To enroll a passkey:**

1. Open the invitation email from Enterprise Connect Passwordless and click the **Click to Enroll** link. (Disregard the instruction about inserting a FIDO key.)



SECRET DOUBLE OCTOPUS

Hi  Amit Lavi1,

Welcome to the FIDO Authenticator, a simple and highly secure system for validating your identity to various applications and networks.

Follow the steps below to prepare your FIDO key and identify yourself to the system. Once the process is completed, the FIDO Authenticator will notify you when an application or network requires your identification, and you will confirm by using the FIDO key.

**Step 1: Insert your FIDO key into your workstation.**

**Step 2: Click the enrollment link below and follow the instructions.**

Click to Enroll

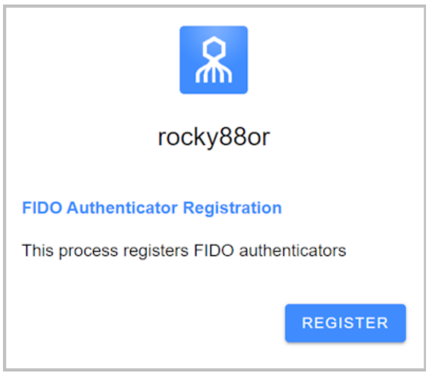
If you need assistance, please contact: support@doubleoctopus.com or your system admin.

**The Invitation will expire in 1 week and 3 days, Please make sure to enroll within this timeframe**.

Keep Safe,
Secret Double Octopus

You will be redirected to FIDO Authentication Registration in the User Portal.

2. Click **Register**.

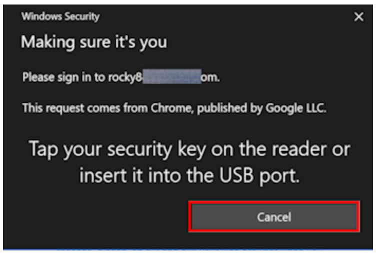


rocky88or

FIDO Authenticator Registration

This process registers FIDO authenticators

3. If the following popup opens, click **Cancel**.



Windows Security

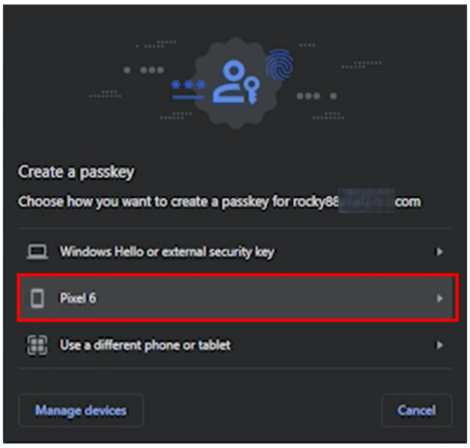
Making sure it's you

Please sign in to rocky8[redacted]om.

This request comes from Chrome, published by Google LLC.

Tap your security key on the reader or insert it into the USB port.

4. Select the device on which the passkey is stored. Any devices that are already connected with your computer will appear in the list of options. For example:



Create a passkey

Choose how you want to create a passkey for rocky88[redacted]com

Windows Hello or external security key

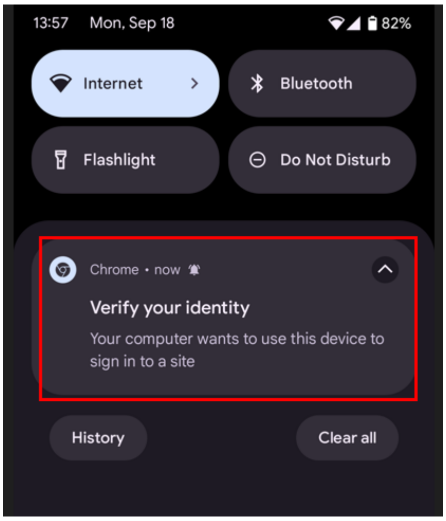
Pixel 6

Use a different phone or tablet

Manage devices

Cancel

A notification is sent to the selected device.



13:57 Mon, Sep 18 82%

Internet

Bluetooth

Flashlight

Do Not Disturb

Chrome • now

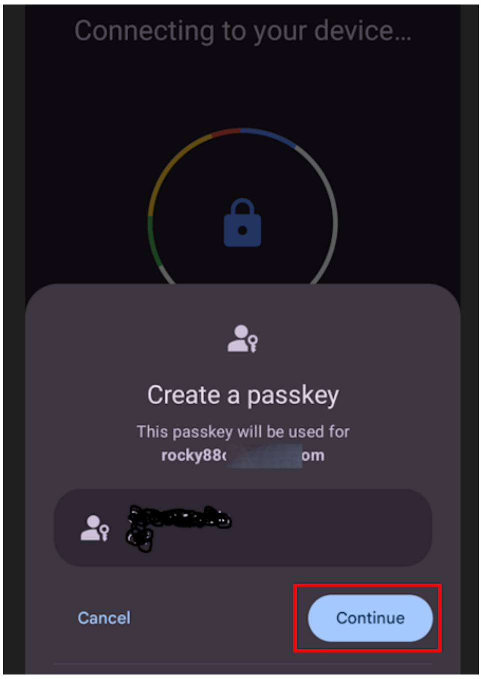
Verify your identity

Your computer wants to use this device to sign in to a site

History

Clear all

5. Follow the instructions shown in your browser and on the device. For example:



Connecting to your device...

Create a passkey

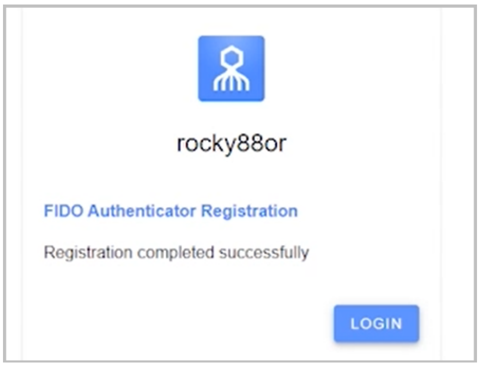
This passkey will be used for rocky88[redacted]om

[redacted]

Cancel

Continue

After the passkey is successfully enrolled, a confirmation message is displayed and the **Login** button appears.



rocky88or

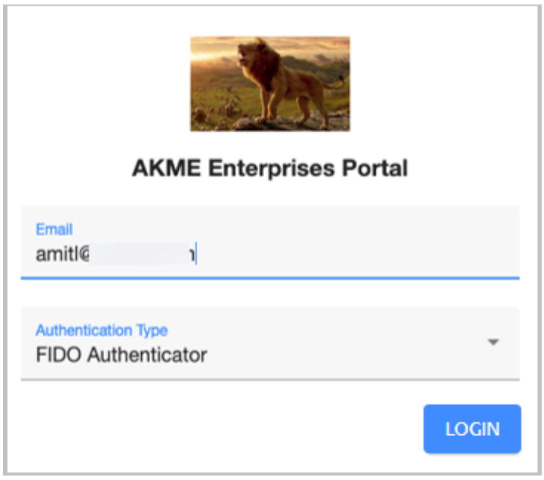
FIDO Authenticator Registration

Registration completed successfully

## Passkey Authentication Flow

The user authentication flow once a passkey is enrolled is presented below. The example used is login to the User Portal from a Chrome browser.

1. The user opens the User Portal in the browser of choice.
2. The user enters an email address / username, chooses **FIDO Authenticator** as the authentication type and clicks **LOGIN**. For example:

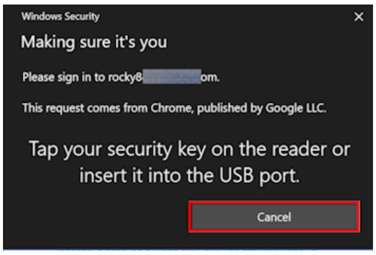


AKME Enterprises Portal

Email: amitl@[redacted]n

Authentication Type: FIDO Authenticator

3. In the popup that opens, the user clicks **Cancel**.



Windows Security

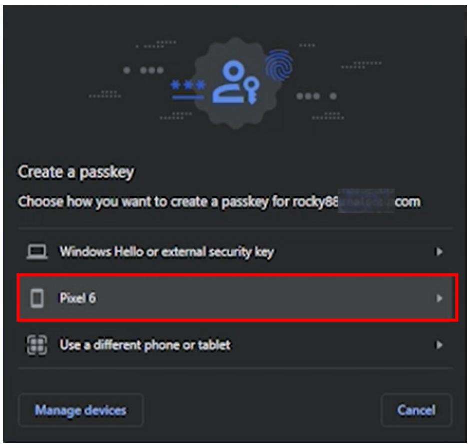
Making sure it's you

Please sign in to rocky8[redacted]om.

This request comes from Chrome, published by Google LLC.

Tap your security key on the reader or insert it into the USB port.

4. The user selects the device on which the passkey is stored.

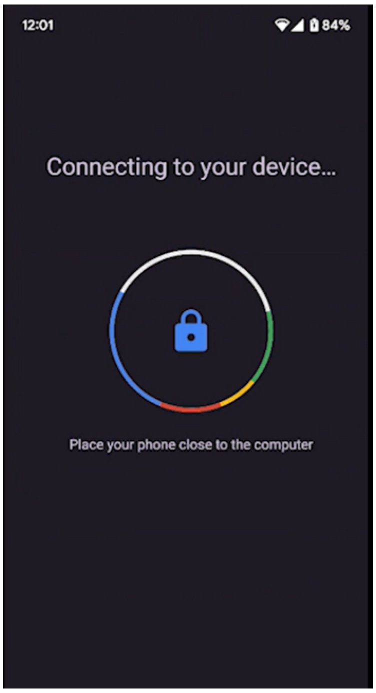


Create a passkey

Choose how you want to create a passkey for rocky88[redacted]com

Windows Hello or external security key
Pixel 6
Use a different phone or tablet
Manage devices
Cancel

The browser then initiates a connection with the selected device.



Connecting to your device...

Place your phone close to the computer

5. Following successful authentication, a confirmation message is displayed on the mobile device, and the User Portal is launched.

## Appendix F: HW OTP Token Enrollment and Authentication

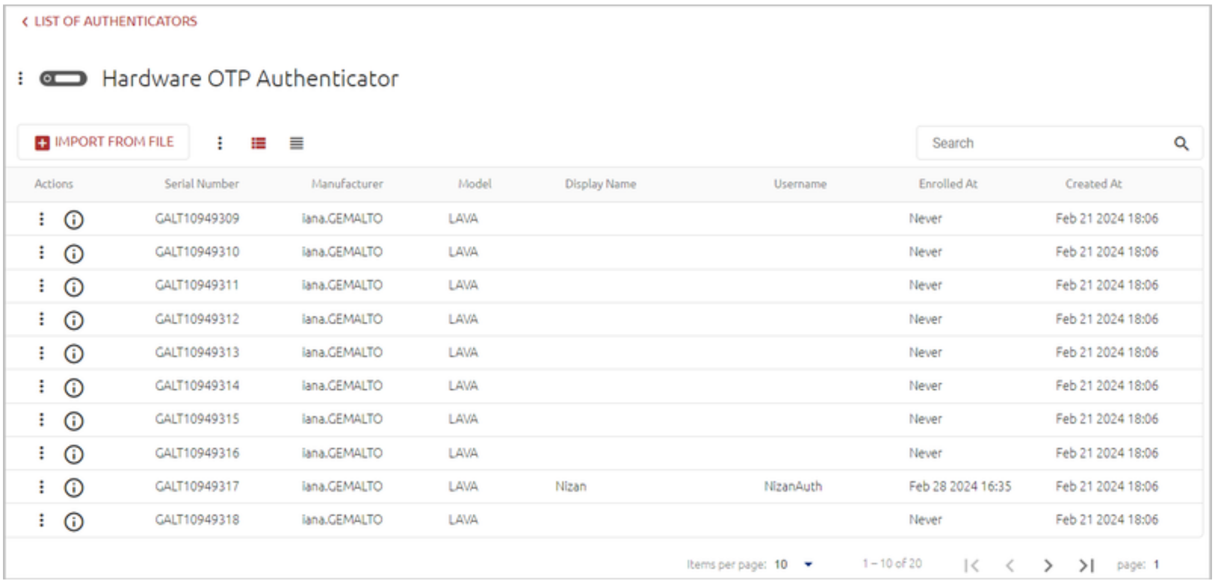
The Enterprise Connect Passwordless solution supports use of hardware OTP tokens to authenticate to Windows and the User Portal. This appendix presents the prerequisites for successful authentication with HW OTP tokens and describes the enrollment process.

### Requirements for HW OTP Token Authentication

Before sending enrollment invitations to your users, verify that the following configuration has been done in the Management Console:

- The Hardware OTP Authenticator is enabled and connected (**System Settings > Authenticators**).

- A list of hardware OTP tokens has been imported. For example:



| Actions | Serial Number | Manufacturer | Model | Display Name | Username | Enrolled At | Created At |
|---|---|---|---|---|---|---|---|
| ⋮ ⓘ | GALT10949309 | iana.GEMALTO | LAVA | | | Never | Feb 21 2024 18:06 |
| ⋮ ⓘ | GALT10949310 | iana.GEMALTO | LAVA | | | Never | Feb 21 2024 18:06 |
| ⋮ ⓘ | GALT10949311 | iana.GEMALTO | LAVA | | | Never | Feb 21 2024 18:06 |
| ⋮ ⓘ | GALT10949312 | iana.GEMALTO | LAVA | | | Never | Feb 21 2024 18:06 |
| ⋮ ⓘ | GALT10949313 | iana.GEMALTO | LAVA | | | Never | Feb 21 2024 18:06 |
| ⋮ ⓘ | GALT10949314 | iana.GEMALTO | LAVA | | | Never | Feb 21 2024 18:06 |
| ⋮ ⓘ | GALT10949315 | iana.GEMALTO | LAVA | | | Never | Feb 21 2024 18:06 |
| ⋮ ⓘ | GALT10949316 | iana.GEMALTO | LAVA | | | Never | Feb 21 2024 18:06 |
| ⋮ ⓘ | GALT10949317 | iana.GEMALTO | LAVA | Nizan | NizanAuth | Feb 28 2024 16:35 | Feb 21 2024 18:06 |
| ⋮ ⓘ | GALT10949318 | iana.GEMALTO | LAVA | | | Never | Feb 21 2024 18:06 |

- The relevant **Hardware OTP Authentication Settings** have been selected in the **Authenticators** tab of the required directory.

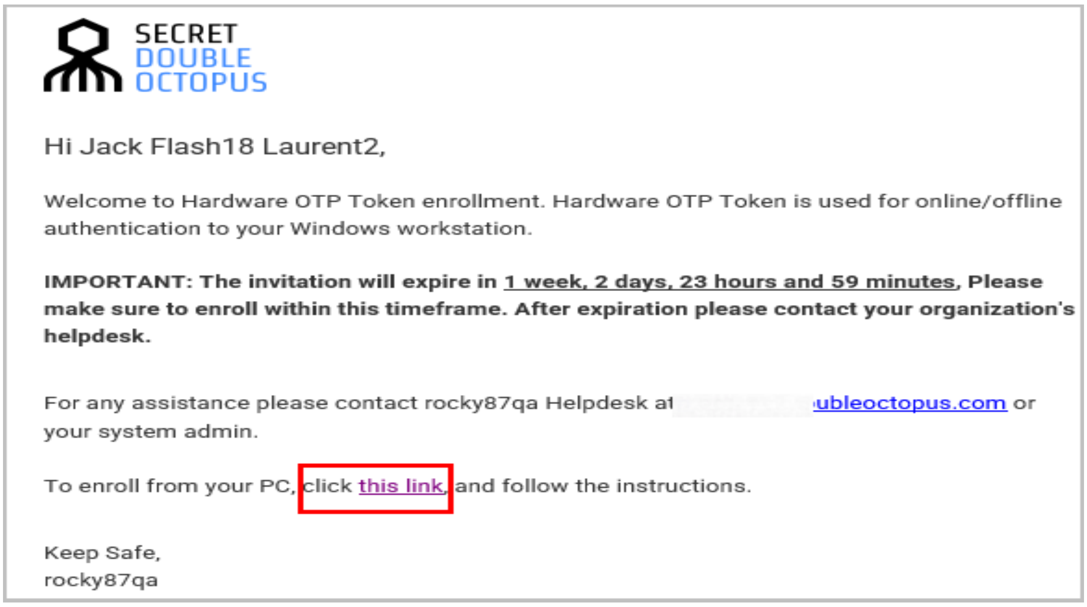
## Hardware OTP Token Registration

In order to login using a HW OTP token, users must first register (enroll) the device in the system. Users can perform registration after receiving an enrollment invitation email.

The following procedure presents user instructions for HW OTP token enrollment.

**To enroll a hardware OTP token:**

1. Open the invitation email from Enterprise Connect Passwordless and click the enrollment link.



Hi Jack Flash18 Laurent2,

Welcome to Hardware OTP Token enrollment. Hardware OTP Token is used for online/offline authentication to your Windows workstation.

**IMPORTANT: The invitation will expire in <u>1 week, 2 days, 23 hours and 59 minutes</u>, Please make sure to enroll within this timeframe. After expiration please contact your organization's helpdesk.**

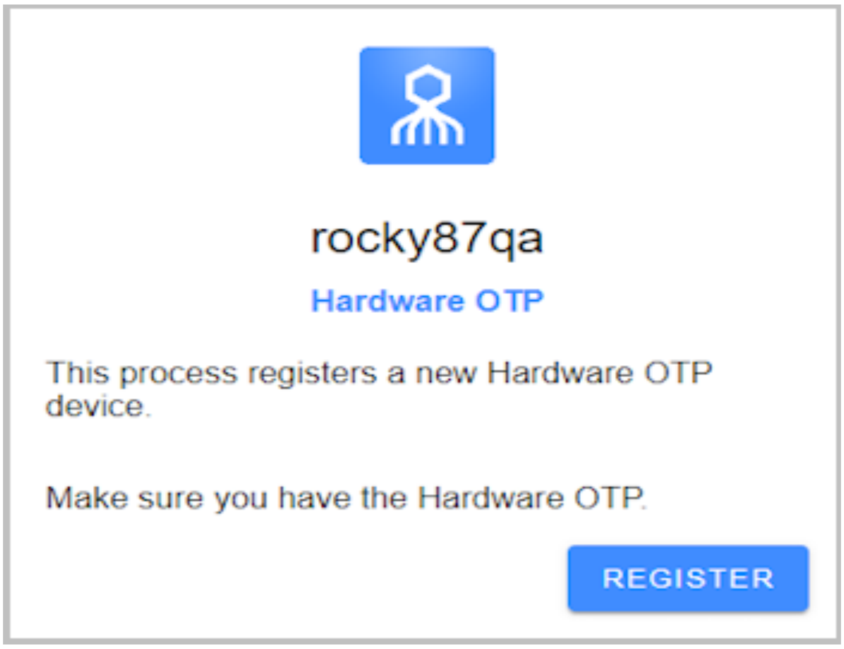
For any assistance please contact rocky87qa Helpdesk at [redacted]ubleoctopus.com or your system admin.

To enroll from your PC, click this link, and follow the instructions.

Keep Safe,
rocky87qa

You will be redirected to Hardware OTP Registration in the User Portal.

2. Click **Register**.



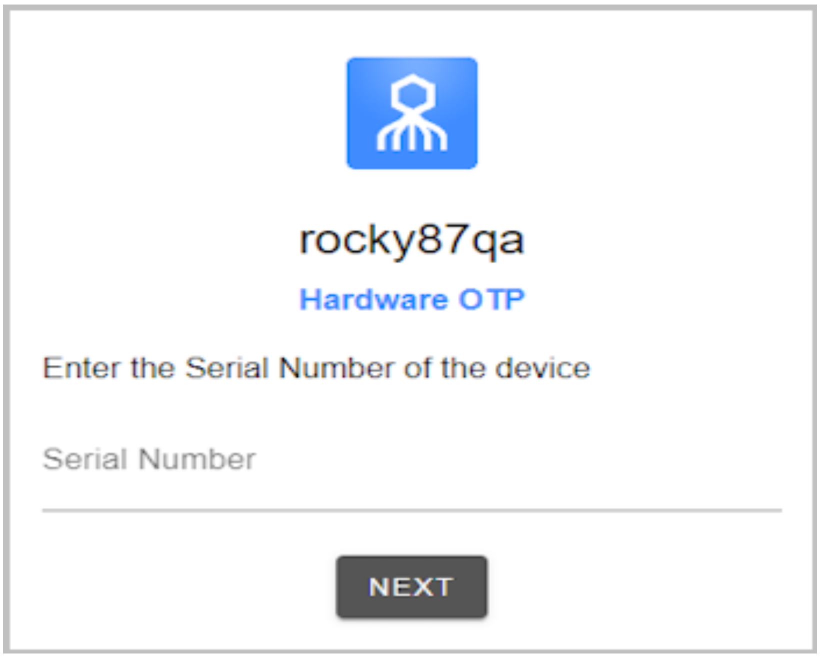
rocky87qa

Hardware OTP

This process registers a new Hardware OTP device.

Make sure you have the Hardware OTP.

3. Enter the serial number of your token, and then click **Next**.



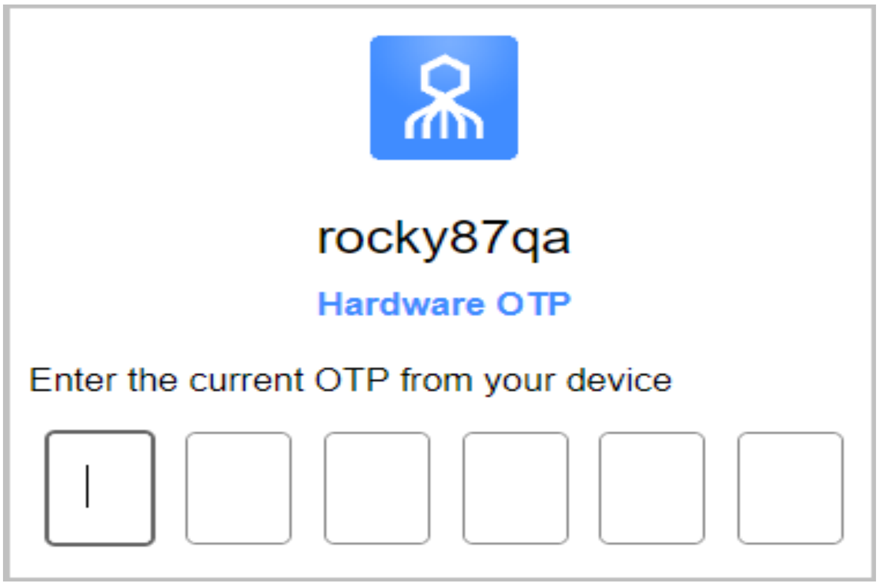
rocky87qa

Hardware OTP

Enter the Serial Number of the device

Serial Number

4. Type the OTP code displayed on your hardware token.

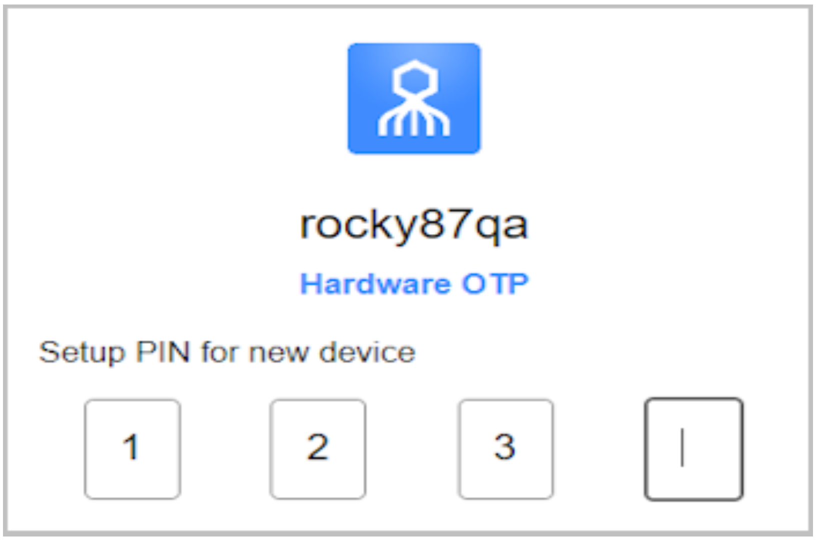


rocky87qa

Hardware OTP

Enter the current OTP from your device

5. If you are prompted to choose a PIN, enter a code of your choice.



rocky87qa

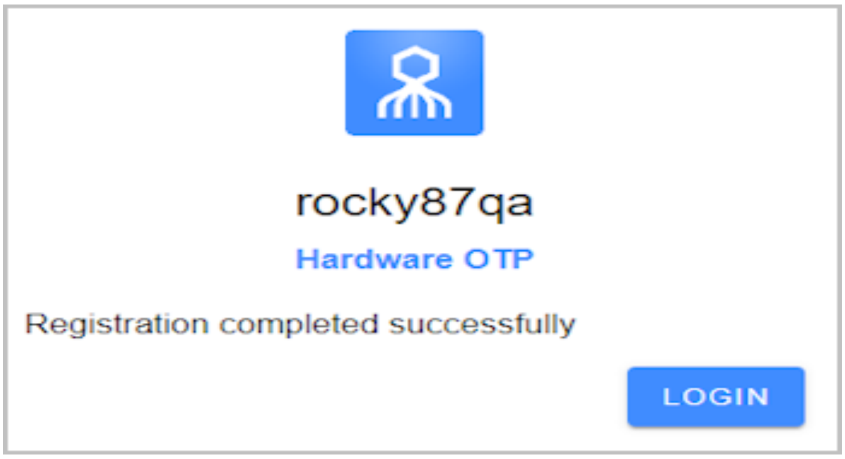
Hardware OTP

Setup PIN for new device

1 2 3

After entering the PIN, you will be asked to retype it.

6. When your token has been successfully enrolled, a confirmation message is displayed and the **Login** button appears.



rocky87qa

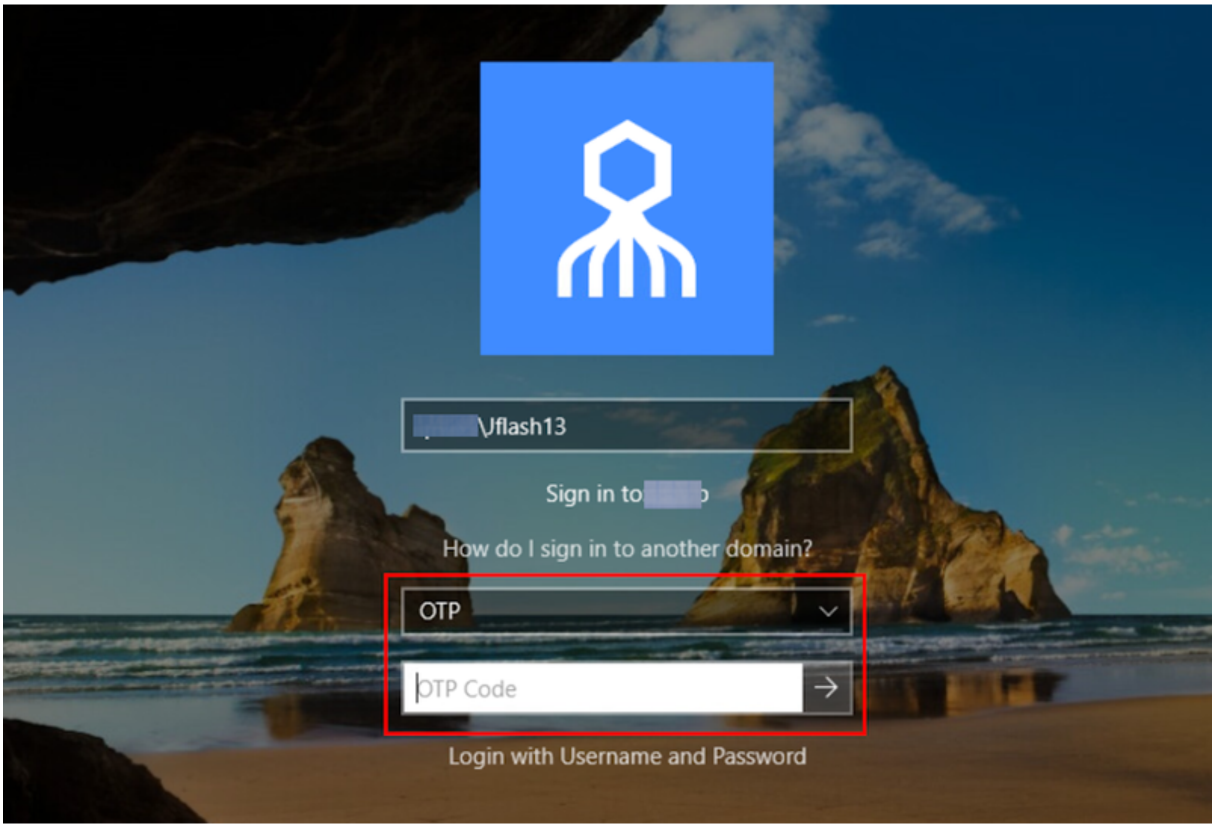
Hardware OTP

Registration completed successfully

## Login Flow with Hardware OTP Tokens

The user authentication flow once a HW OTP token is enrolled is presented below. The example used is login to Windows.

1. The user enters a username and selects **OTP** as the authentication method.
2. The user types the code displayed on the hardware token and presses **<Enter>**.



[redacted]\flash13

Sign in to [redacted]

OTP

How do I sign in to another domain?
OTP Code
Login with Username and Password

**Important**

If a PIN has been configured for the token, the user enters the PIN followed by the OTP code, with no space between them.