Enterprise Connect Passwordless Management Console Admin Guide

Version 5.4.4

Table of contents

Overview

This document describes the user interface of the Management Console and how to work with it.

Additionally, 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 Enterprise Connect 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.

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 f Authentication Server (Login with Email and Password). You can then start to integrate directories, add users and register devices.

After users and devices have been enrolled, you will be able to log into the Management Console using the Authenticator app.

Note

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

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 8.7 - Minimal image option
Oracle Linux	8.3 to 8.7
Rocky Linux	8.4 to 8.7

Supported mobile devices

Device	Supported Versions
Android	Android 9 and higher
iOS	iOS 13 and higher

Supported browsers: Management Console UI and User Portal

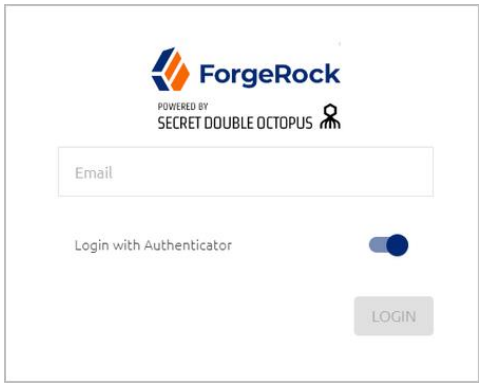
Browser	Supported Versions
Chrome	30 and higher
Safari	13.1.2 and higher
Firefox	25 and higher
Edge	41 and higher

Supported browsers for SAML authentication

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

Login with the authenticator app

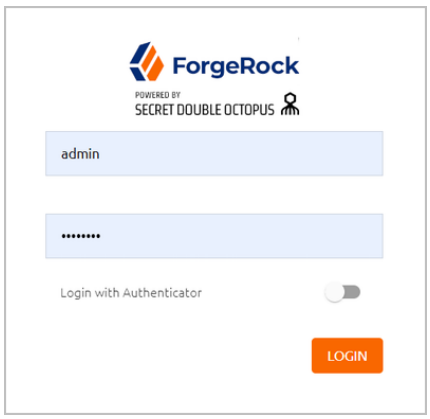
This is the default login method. Enter your email address in the field, and then click **LOGIN**.



After receiving the push notification to your Authenticator mobile app, authenticate as you normally would with any service.

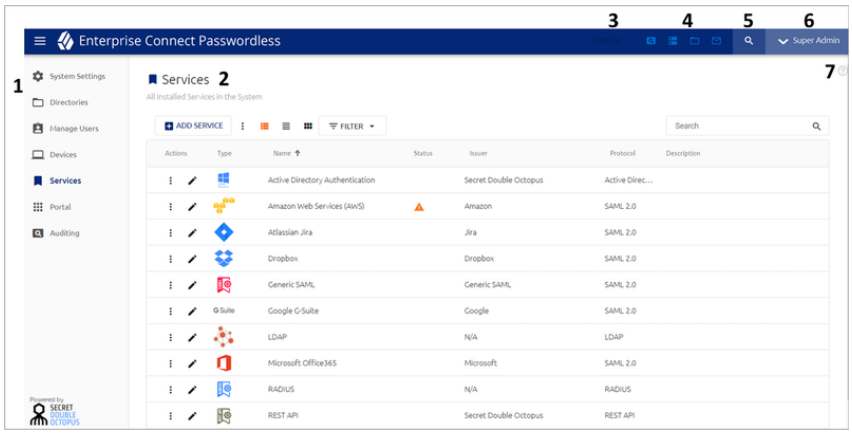
Login with email and password

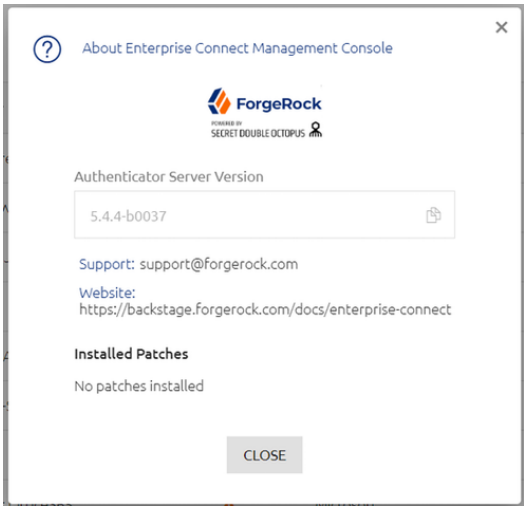
To access the Management Console using your administrative credentials, make sure that the **Login with Authenticator** toggle button is inactive. Then, enter your email address and password in the appropriate fields, and click **LOGIN**.



Management console features overview

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



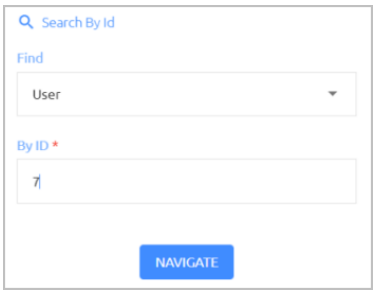
Number	Feature	Description / Notes
1	Menu bar	Provides access to the various menus of the Management Console. For more information, refer to Menu Bar.
2	Menu title	Name and description of the currently displayed menu.
3	Publish button	Shows information about publishing status and provides quick access 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: • **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.  • **What's New?**: Displays a description of the features introduced in the current version. • **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.

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.

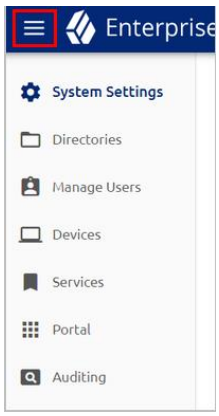


2. From the **Find** dropdown list, select **User**, **Group** or **Device**.
3. In the **By ID** field, enter the entity's unique ID.
4. Click **Navigate**.

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

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.
- Auditing: Displays a log of every administrative action performed by the system or by users.

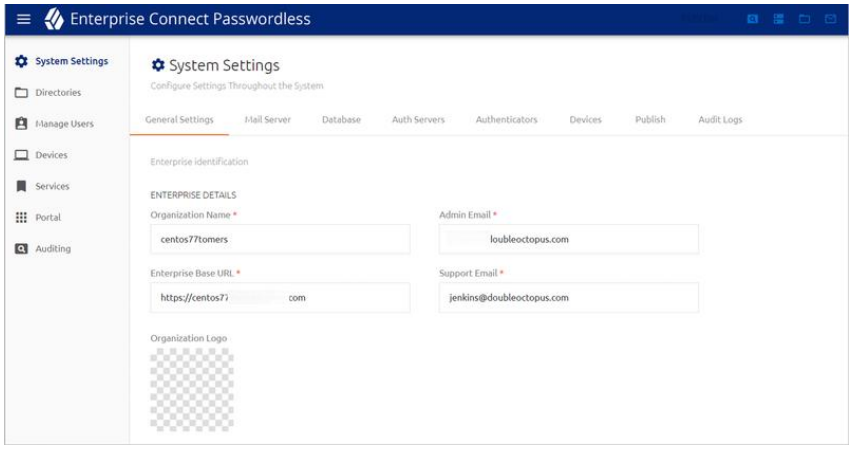
Component status icons

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

Icon	Description / Notes
	Shows the current status of disk usage according to parameters set in the **Audit Logs** tab of the **System Settings** menu. Storage issues are indicated by . Click the warning icon to view and update log storage settings. For details, refer to Configuring Audit Logs Settings.
	Indicates connection status of the Authentication Server(s). Connection issues are indicated by . Click the warning icon 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. Connection issues are indicated by . Click the warning icon to open the directory settings.
	Shows connection status of the SMTP server. Mail server issues are indicated by . Click the warning icon 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.



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

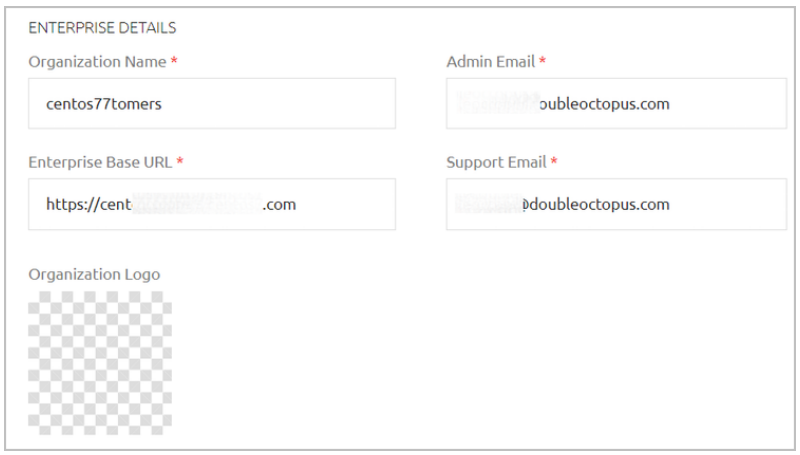
- General Settings: Contains organization details, license information and timeout parameters for Management Console sessions.
- Mail Server: Sets SMTP server information details and other required email parameters.
- Database: Sets parameters for the database connection to the Management Console.
- 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.

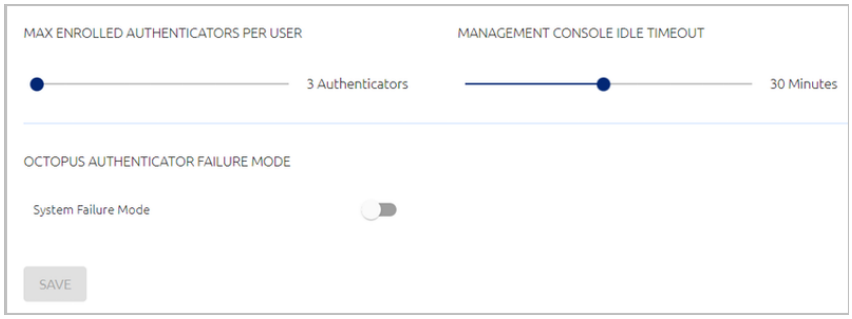


Setting	Description / Notes
Organization Name	The name of your company. By default, the name is the one entered during installation of the Authentication Server. The name specified here is displayed to users in the authenticator mobile app.
Enterprise Base URL	The value should be the address of the Authentication 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. 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 488x488 pixels.
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

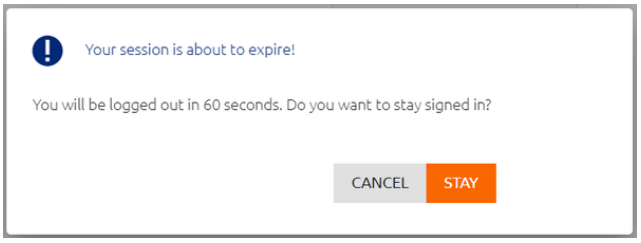
The lower portion of the **General Settings** tab contains various settings related to authentication sessions.



The settings are:

- **Max Enrolled Authenticators Per User:** The maximum number of mobile and FIDO 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.

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

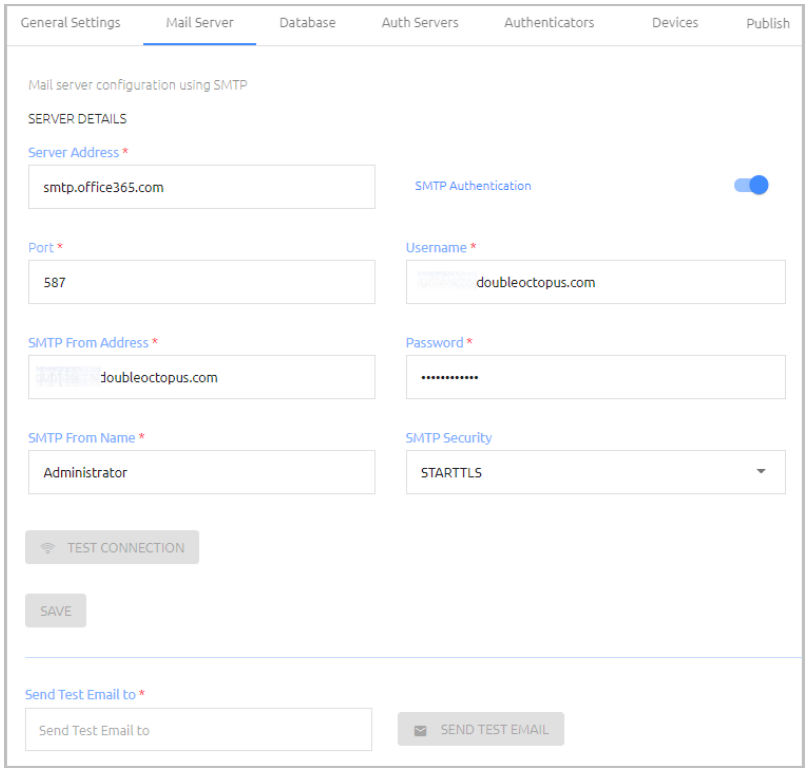
After updating these settings, click **Save**.

Mail server settings

The **Mail Server** tab allows you to set up mail server configuration. Once you have configured these settings, the platform will be able to send invitation (enrollment) emails and other email notifications to users. To open the tab, select **System Settings > Mail Server**.

Configuring server details

The **Server Details** portion of the tab contains SMTP server information and other required email parameters.



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. 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

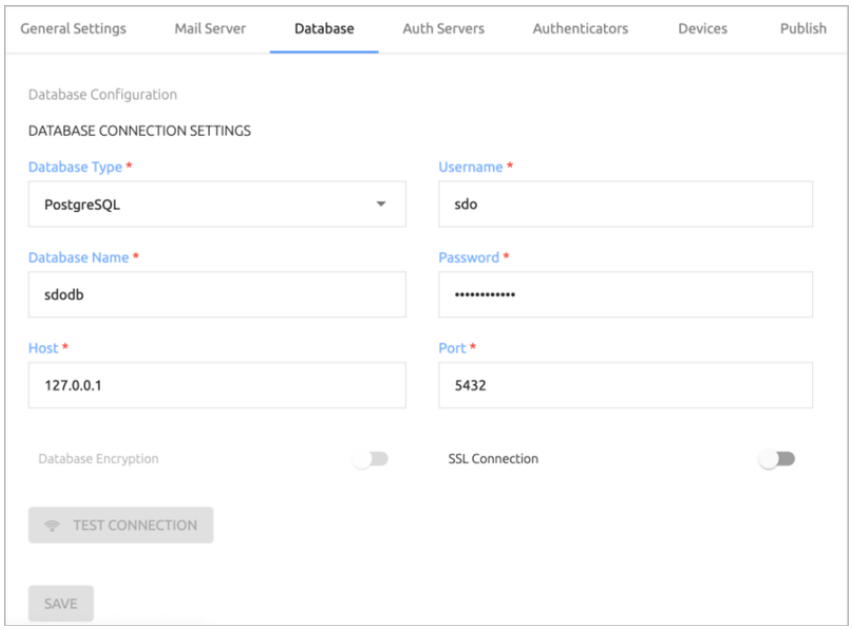
The **Email Settings** section at the bottom of the **Mail Server** tab enables you to set the value for the **Enrollment Token Expiration**. This setting determines the maximum period for which an invitation email is valid. If a user does not use the invitation to enroll within this time period, the invitation is deleted from the system and a new email needs to be sent.

The **Enrollment Token Expiration** can range from 1 minute to 3 weeks (default setting is 10 minutes). To update the setting, specify the desired timeframe and then click **Apply**.

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 (see Configuring Database Settings).

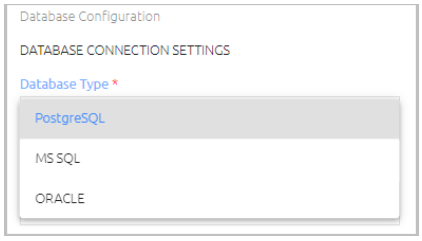


Configuring Database Settings

The following database types are supported:

- PostgreSQL (this type is created automatically as part of the All-In-One installation)
- MS SQL
- Oracle

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.

> **Note**
>
> This toggle button is inactivated for PostgreSQL and Oracle database types.

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.

> **Note**
>
> This toggle button is inactivated for MS SQL and ORACLE database types.

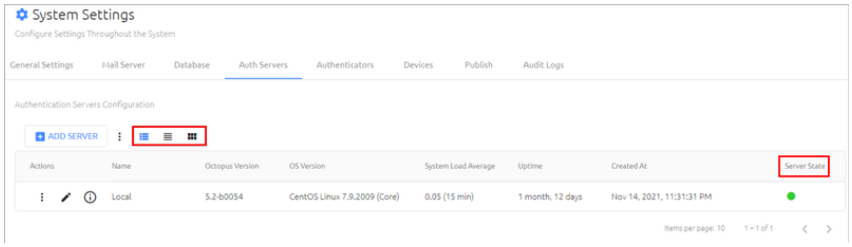
5. To check validity of your settings, click **Test Connection**.

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

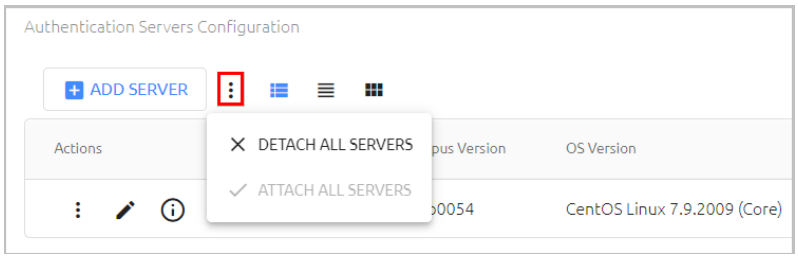
Authentication server management

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

The **Auth Servers** tab of the **System Settings** menu displays general information about each configured Authentication Server. The Server State colored indicator (red or green) reflects the Server's current connectivity status. Clicking the display icons at the top of the page changes the presentation to Cards view List view or Compact List view . List view displays up to 10 items per page, and Compact List view displays up to 20 items per page. When there are multiple Servers, both List views support sorting the list according to any column by clicking the relevant column header.



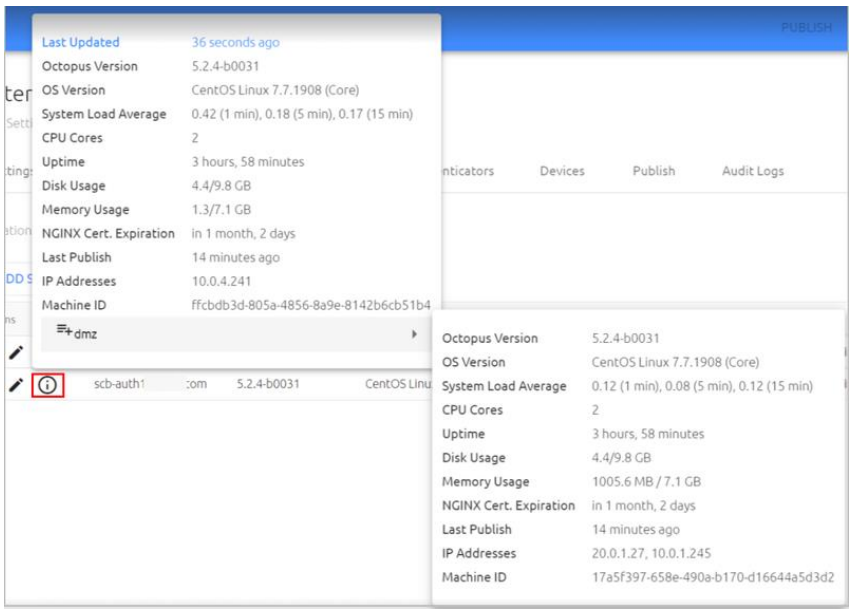
The Actions icon to the right of the **Add Server** button allows you to detach (and reattach) all Authentication Servers from the Management Console in a single bulk action. This feature lets you easily perform administrative operations, such as system upgrades, without having to delete and recreate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



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

- **Last Updated:** Period since the last data update from the Server
- **Octopus Version:** Installed version of Octopus 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 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 remaining until expiration of the certificate. Once the certificate is expired the Server will stop working.
- **Last Publish:** Period 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.



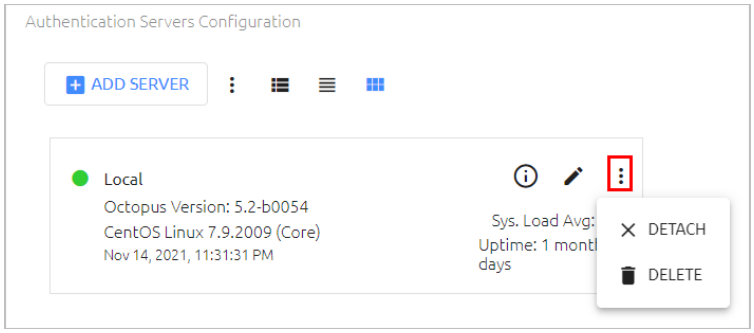
Important

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 tile 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 Authentication Server that is no longer in use.



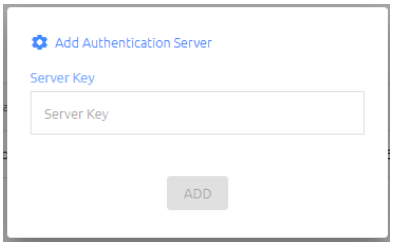
Adding Authentication Servers

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.

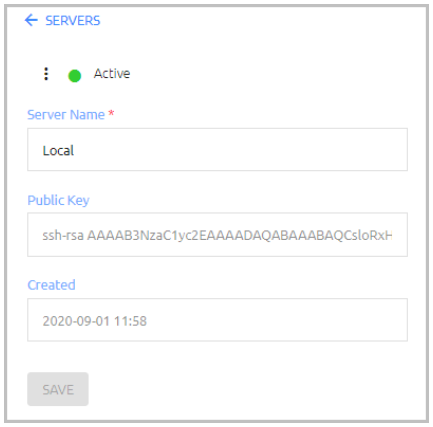


2. Paste the server key into the field and click **Add**.

   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 tile or row of the relevant server.



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

Authenticator management

Secret Double Octopus supports the ability to authenticate to Windows, Mac and the User Portal through multiple authenticators. These authenticators are 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
- Adding a New Authenticator
- Managing Authenticator Templates

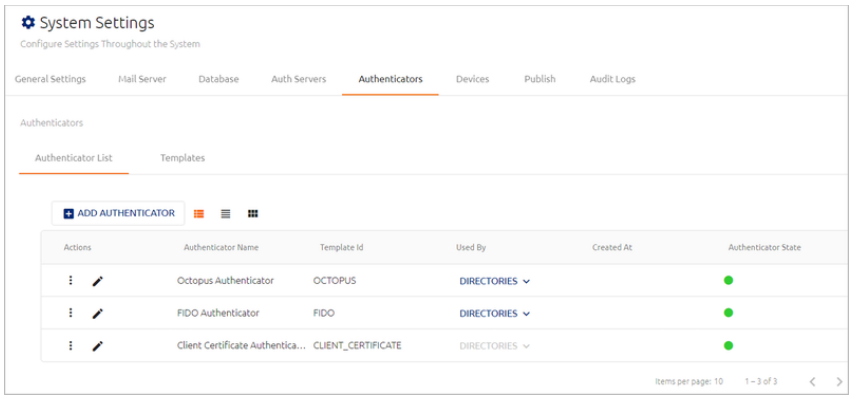
Authenticator Plugins: Overview

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 Octopus 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.

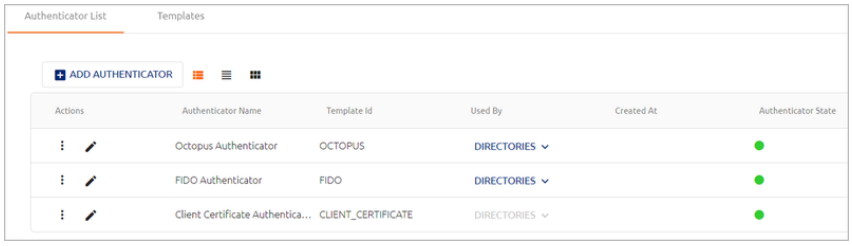


Selection of the primary mobile authenticator is done at the directory level. For more information, refer to Configuring Directory Authentication Options.

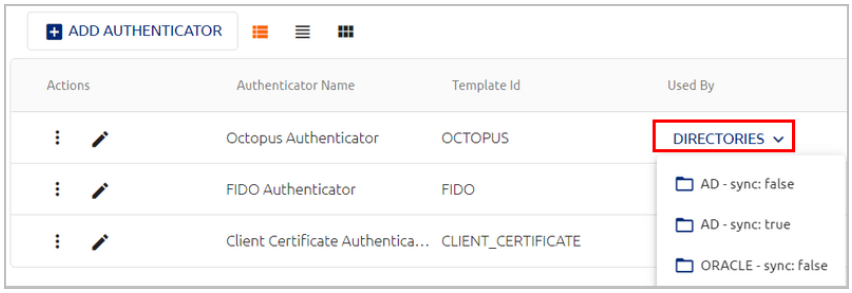
The ForgeRock authenticator enables users working in the ForgeRock environment to authenticate by approving an authentication request on the ForgeRock mobile app (delivered by push notification), or by providing the one-time password required by the service, which is validated by the ForgeRock server.

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 and Client Certificate Authenticators are preconfigured and automatically available. Other third party authenticators need to be added, using the templates provided (Adding a New Authenticator).



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.

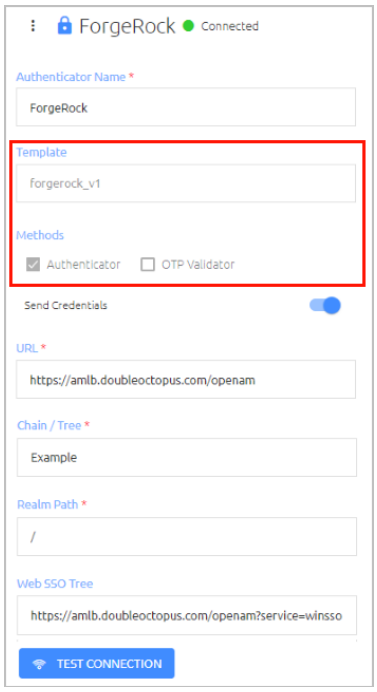


Working with Authenticators

The Actions icons allow you to enable/disable the authenticators, update their details, and more.

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

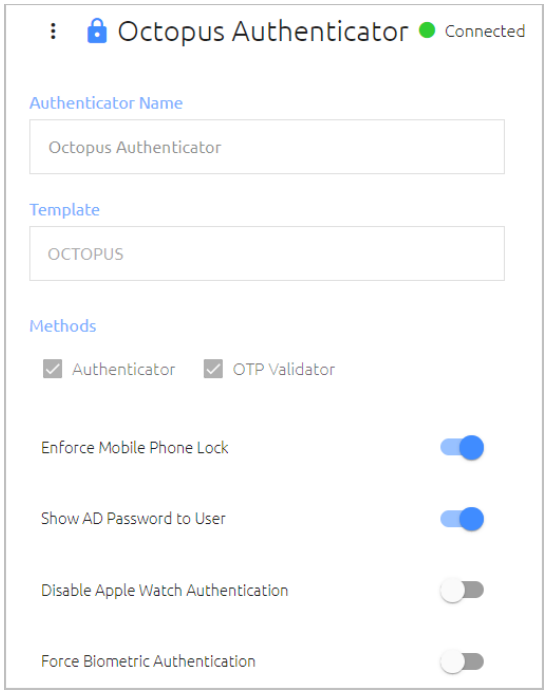
- The template cannot be changed.
- The authentication methods (Authenticator and OTP Validator) can be updated only if the authenticator is NOT currently assigned to any directories. When an authenticator is assigned, the **Methods** settings are disabled.



Octopus Authenticator details are not editable, but the following settings are configurable:

- **Enforce Mobile Phone Lock:** When enabled, users are required to use the locking feature on their mobile devices.
- **Show AD Password to Client:** When enabled, the AD password is displayed to users in the Octopus Authenticator mobile app.

- **Disable Apple Watch Authentication:** When enabled, users cannot use the watch for authentication. (They must authenticate using the smartphone app.)
- **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 **Enforce Mobile Phone Lock** setting is enabled.



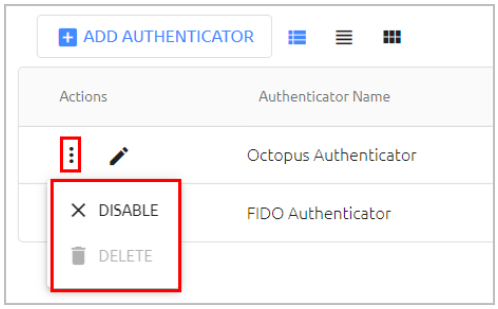
After updating authenticator details, click **Save** (at the bottom of the page).

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

Clicking ⋮ opens a list with the following actions:

- **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**
>
> The Octopus Authenticator and the FIDO Authenticator cannot be deleted.



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 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 ForgeRock authenticator:

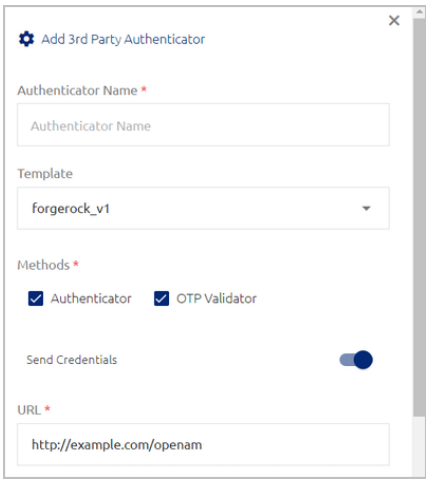
1. In the upper left corner of the **Authenticators** tab, click **Add Authenticator**.

   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.



4. By default, both of the following **Methods** are enabled for a 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).

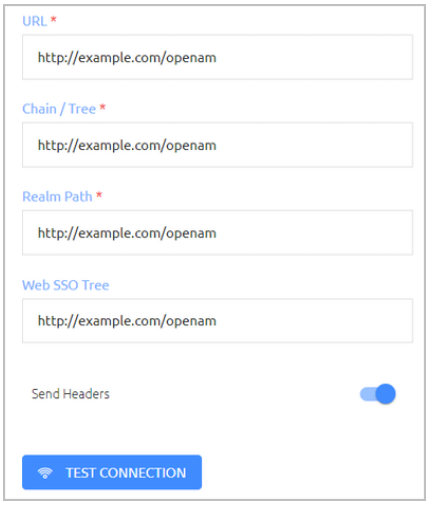
   If you do NOT want to use the new authenticator for a method, clear the relevant checkbox.

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. Specify the following settings for authenticators based on ForgeRock templates:

   - **URL:** The access URL for your ForgeRock environment.
   - **Chain / Tree:** Name of the journey.
   - **Realm Path:** Name of the relevant realm in the AM console
   - **Web SSO Tree:** URL of the *winsso* journey in the ForgeRock environment. This journey enables automatic launching of the user's dashboard upon user login to a Windows or Mac workstation.
   - **Send Headers:** When the toggle is enabled (default setting), HTML headers (*IP*, *User-Agent*, *Primary-Auth-Type*) are sent to the ForgeRock directory.



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

8. Click **Add**.

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

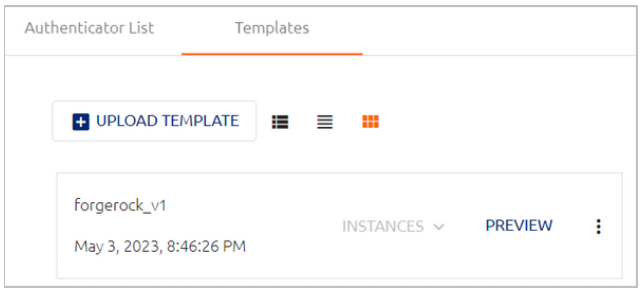
Managing authenticator templates

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.

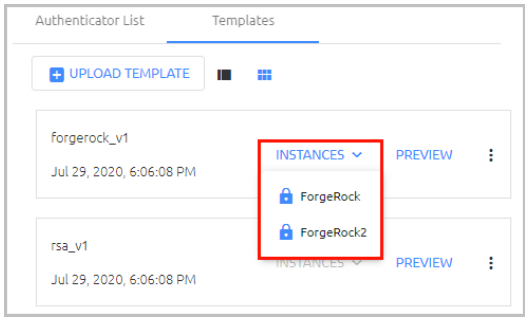
The **Templates** tab allows you to view and manage existing templates and upload new ones.

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.

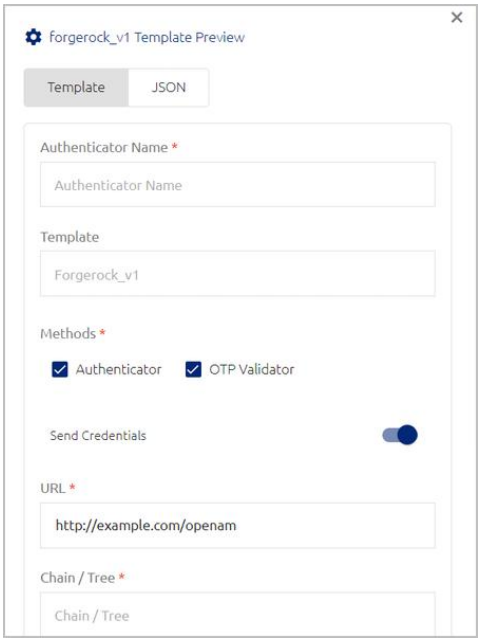


To view the authenticators currently using the template, click to open the list. Clicking an authenticator in the list opens the settings page for that authenticator.

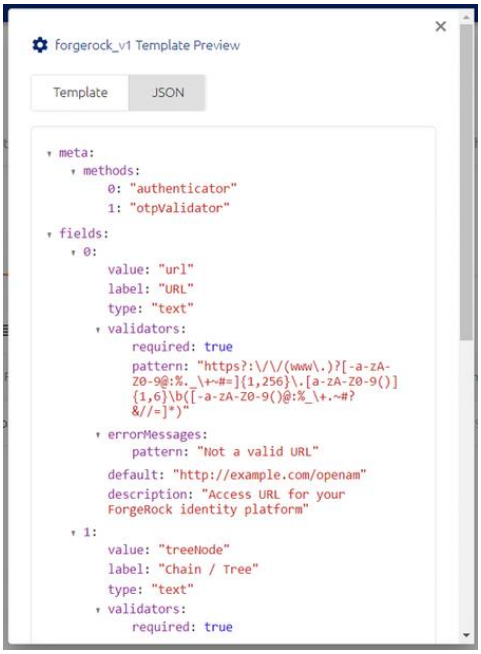


Clicking **PREVIEW** opens a popup in which you can view the template's fields. The **Template Preview** popup contains two views:

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



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



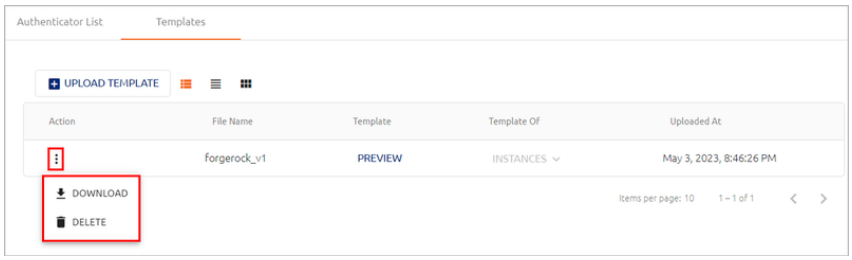
Important

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

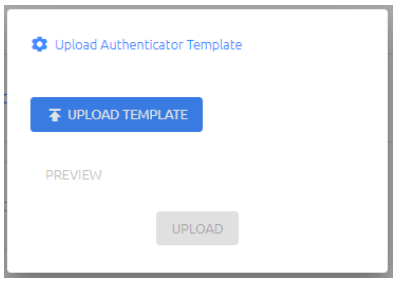
Custom authenticator templates can be imported to the Management Console by uploading the relevant JSON file.

> **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:

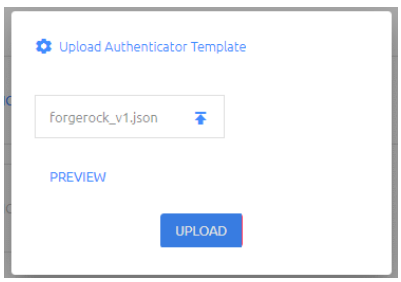
1. In the upper left corner of the **Templates** tab, click **Upload Template**.

   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:

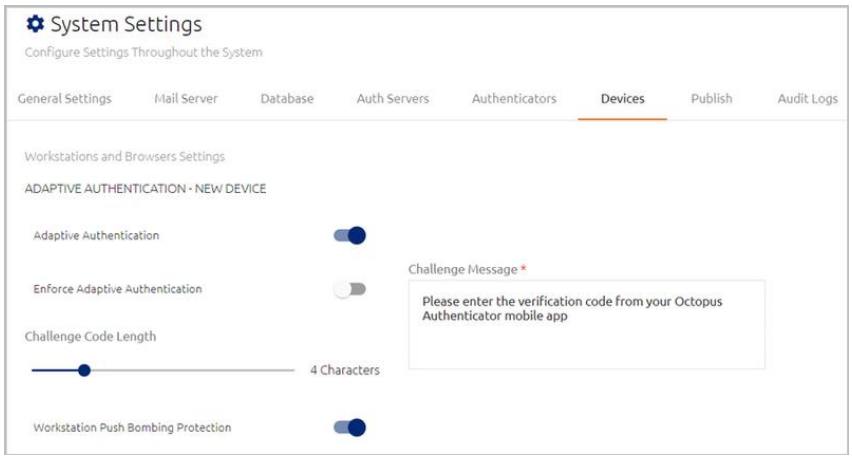
1. Access the required files:
   - Export the JSON file from the Octopus Management Console.
   - Copy the JS file from the **Custom Authenticators** directory on the Authentication Server.
2. Modify the two files as required. Verify that all variables used in the code are defined in the schema (JSON 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 Octopus 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:

- 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 Bombing 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).



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 an 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.

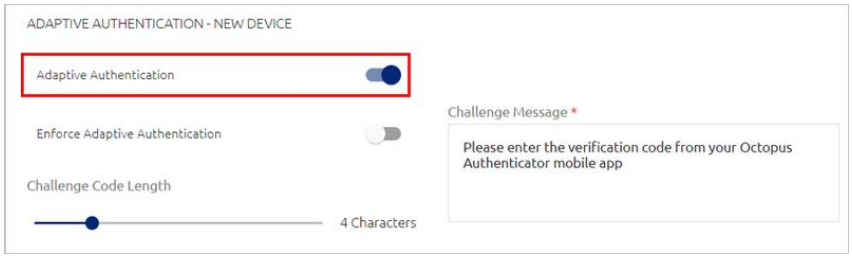
To further enhance security, the Adaptive Authentication mechanism enforces the following limitations on login attempts:

- **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.

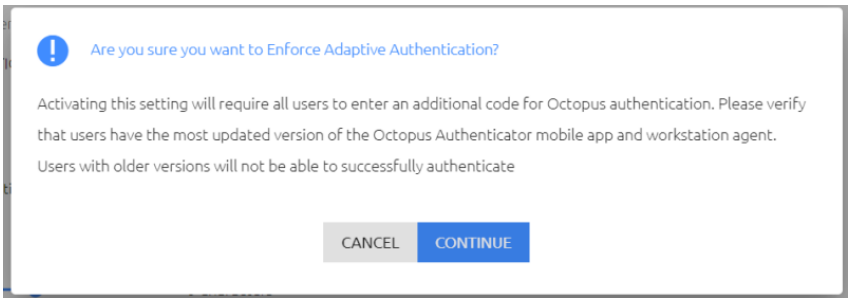
The feature is activated and inactivated by toggling the **Adaptive Authentication** toggle button.



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.



- **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**.

Important

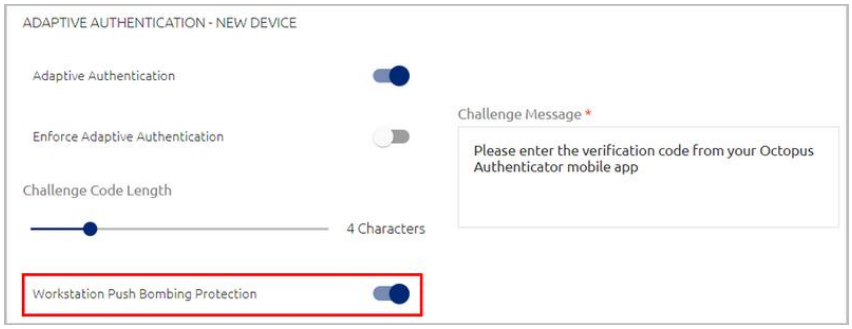
- In *new* installations of Octopus Authentication Server versions 5.0 and higher, the Adaptive Authentication feature is enabled by default (with the **Enforce** setting off).
- When *upgrading* the system to these versions, the feature is disabled, to avoid interruptions in login flows. After upgrade, 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.

Workstation push bombing protection

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



The push bombing protection workflow unfolds in two stages:

- After the user rejects an authentication request, OR after three timeouts (the user does not respond to the authentication request), a verification code is required for successful login (even when the workstation is a known device).

  This initial phase of protection is implemented **only if Adaptive Authentication is enabled**.

- After the user rejects three authentication requests, OR after ten timeouts, the workstation is automatically locked in a period of 15 minutes. This protection mechanism is implemented regardless of whether Adaptive Authentication is enabled.

The initial push bombing protection mechanism (enforcement of Adaptive Authentication) is automatically disabled upon a successful user login. If the machine has been locked, the user must wait for the lockout period to elapse (15 minutes) before successful login can occur.

Important

- In *new* installations of Octopus Authentication Server versions 5.4 and higher, push bombing 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.

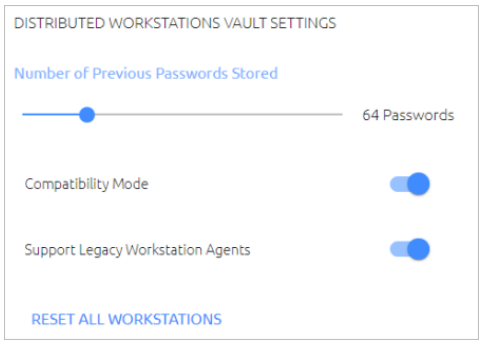
  Following a server upgrade, users must perform a hard refresh to the browser (**Ctrl + F5**) or clear the browser cache.

Distributed workstations vault settings

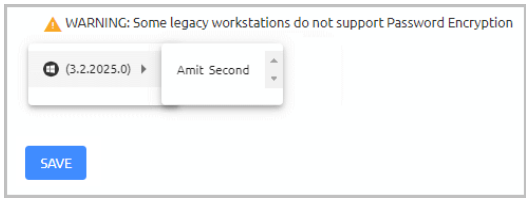
Workstations running Windows Agent version 3.3 or Mac Agent version 2.3.0 have an extra layer of encryption for communication with the Octopus Authentication Server. Besides credentials encryption, all data passed between the workstation and the Server is encrypted as well. Security keys that were generated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



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.



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.

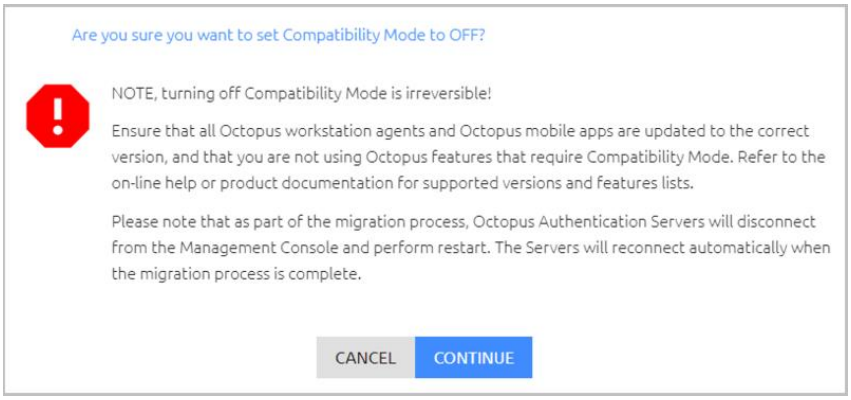
The action of turning off Compatibility Mode cannot be reversed. Before exiting Compatibility Mode, it is very important to properly prepare, using the following guidelines:

- 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:

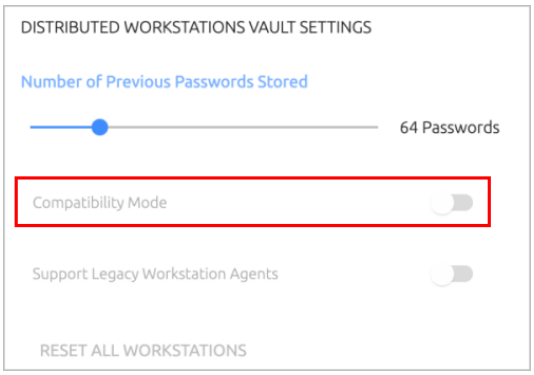
1. After verifying that you have met all requirements described above, click the **Compatibility Mode** toggle to inactivate the feature.

   A warning popup opens.



2. Click **Continue**.

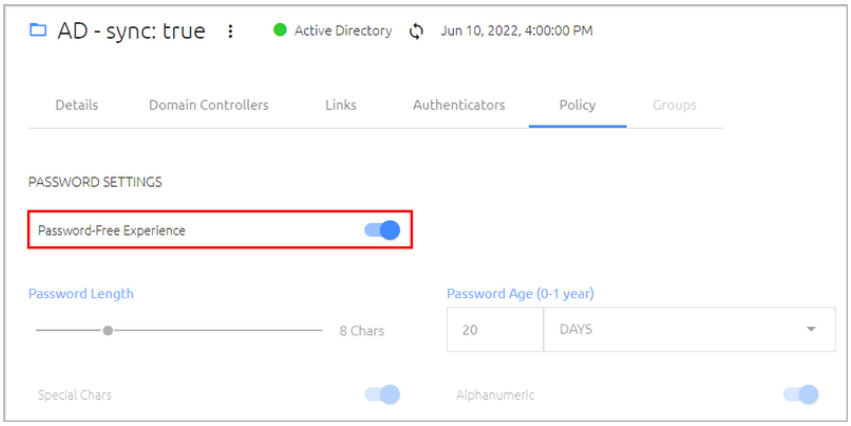
   The Authentication Server(s) will temporarily disconnect during the migration process. Once Compatibility Mode is off, the actions for managing workstations are disabled.



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**.

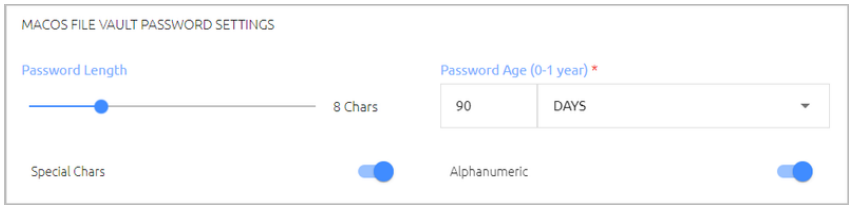


c. At the bottom of the tab, click **Save**.

> **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.



The settings are:

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

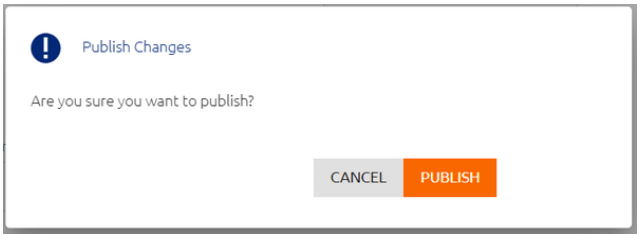
After updating and saving settings in the Management Console, you need to publish to the database in order to update all servers (in a multiple server setup) with the changes you made. The following sections describe components and features that are available to help you manage and control the publishing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

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

The toolbar publish element

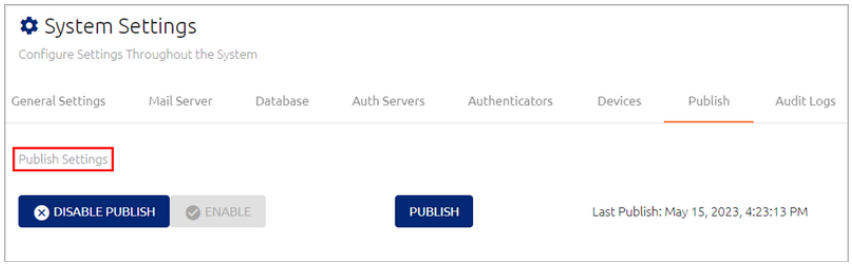
The **PUBLISH** element at the top of the Management Console shows the current status of database publication. In its default state, when there are no changes to be published, the element appears as follows:

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

State	Description
PUBLISH 1	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**. 
PUBLISH	Changes are currently being published. Once changes are successfully published, the **PUBLISH** element returns to its default state.
PUBLISH	The publishing process was unsuccessful. Click the warning icon to open a list of issues that were encountered.
PUBLISH	Publishing is disabled. For more information, refer to Working with Publish Settings (below).
PUBLISH	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.

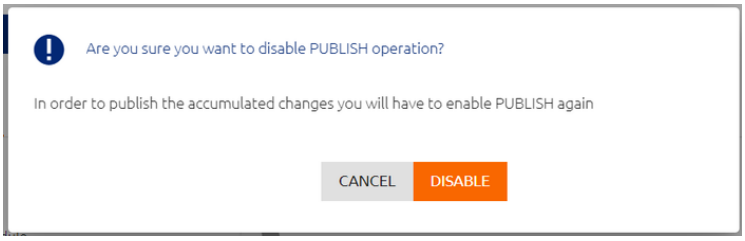


When publishing is disabled, you may continue to update settings in the Management Console, but the changes cannot be published until the publishing operation is reactivated.

To disable publishing:

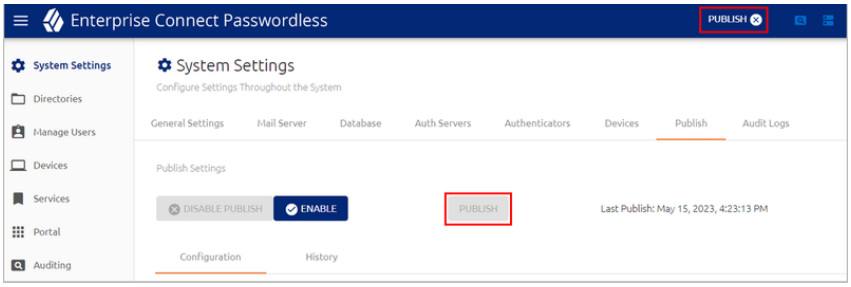
1. At the top of the **Publish** tab, click **Disable Publish**.

   A confirmation popup opens.



2. Click **Disable**.

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



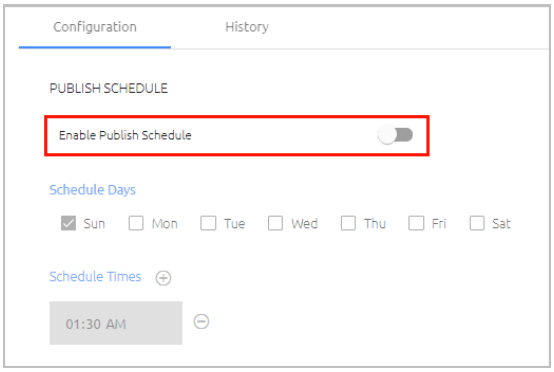
3. To reactivate the publishing operation, click **ENABLE**. Then, to publish accumulated changes, click **PUBLISH**.

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.

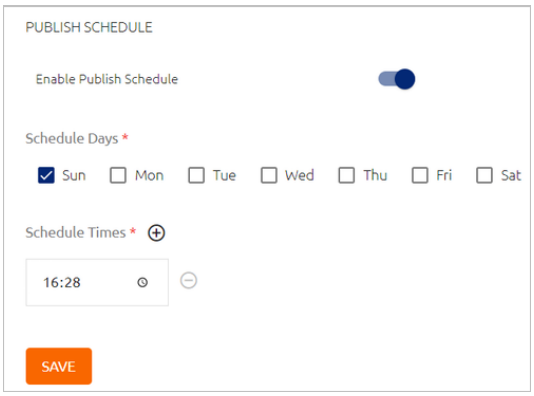


The Schedule options below are enabled.

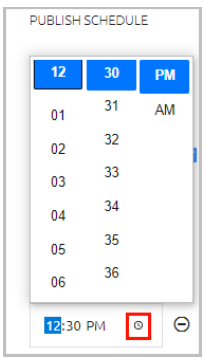
2. Specify the day(s) on which you want automatic publishing to take place by selecting the relevant checkbox(es).

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, minute or AM/PM value and enter a new value.



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



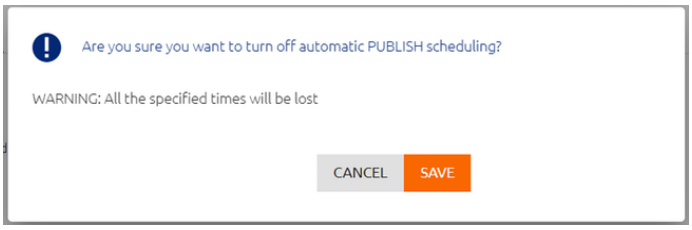
4. When you are finished setting the schedule, click **Save**.

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**.

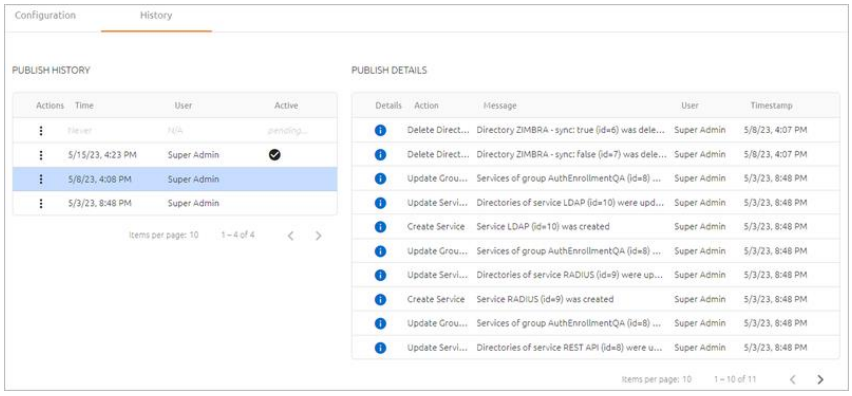
   A warning popup opens.



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. Clicking a row in the **Publish History** list opens the **Publish Details** list.



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 .

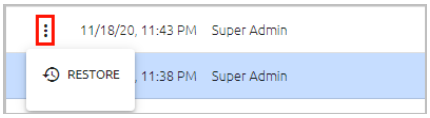
Restoring the System to a Previous Publish State

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.

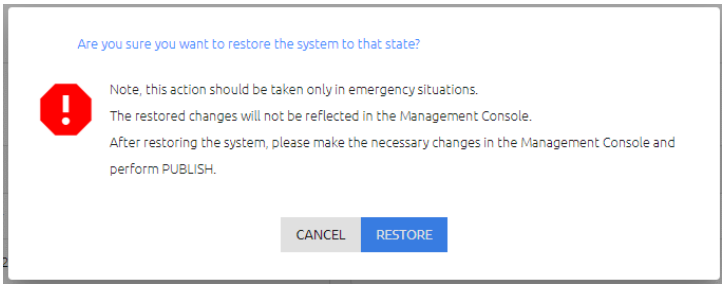
Keep in mind that restoring a previous publish state changes the content in the database, but it does **not** reverse any changes made in the Management Console. Therefore, after performing a Restore operation, you need to manually make relevant changes and updates in the Management Console and then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

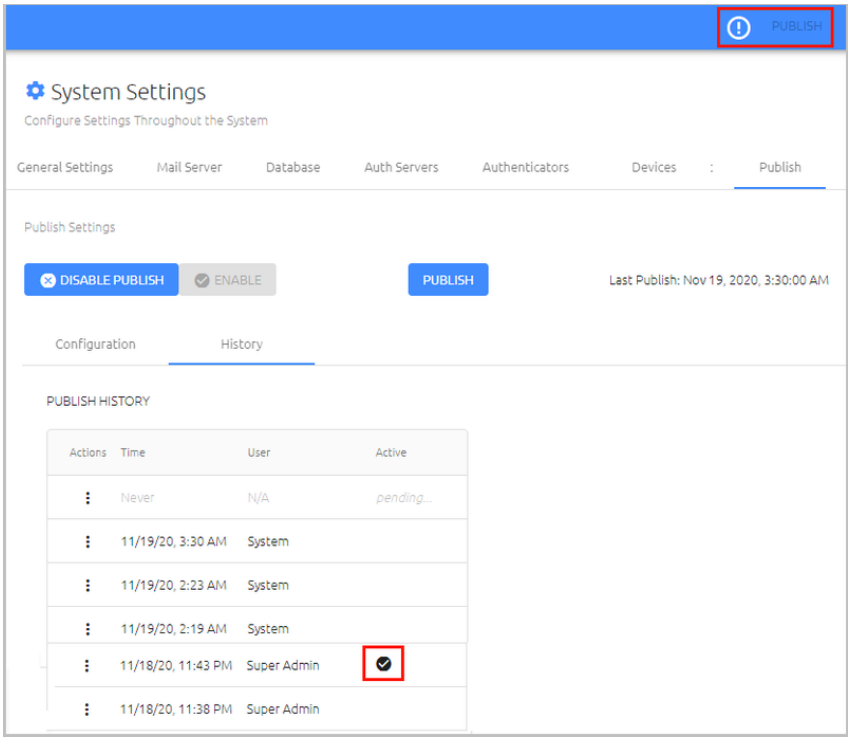


A confirmation popup opens.



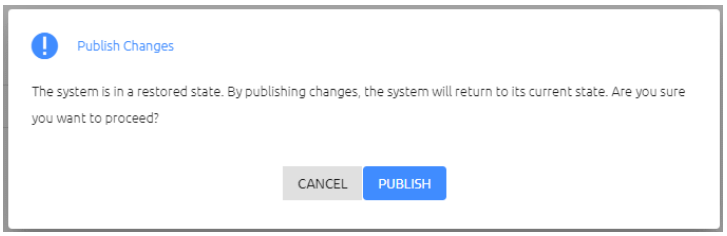
2. Click **Restore**.

   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.



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.

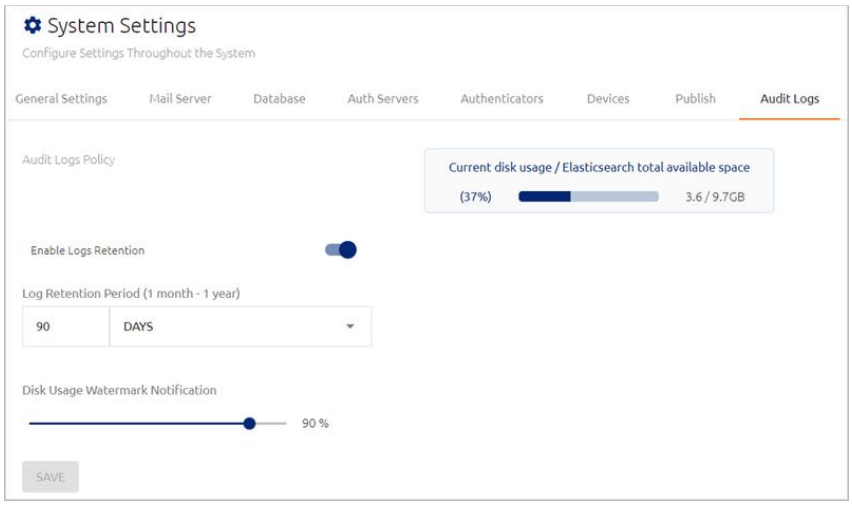
If you prefer not to use publish optimization, you can disable it by editing (or adding) the *disablePublishOptimization* parameter in the following configuration file: **/opt/sdo/mcbackendsql/config/envs/production.json**

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 number 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**.



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

- **Log Retention:** Allows you to specify the period (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**.

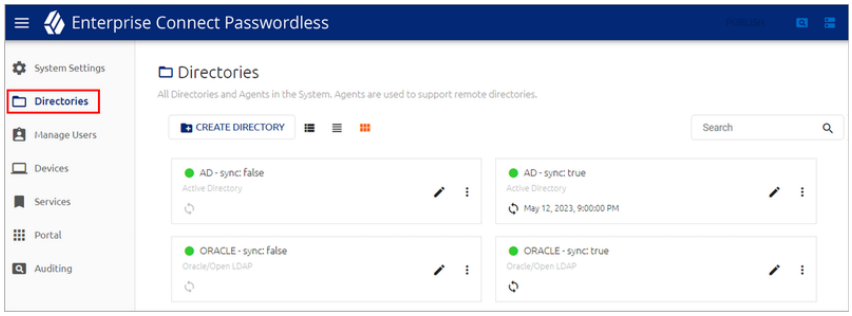
- **Elasticsearch Disk Usage:** This value, which is calculated daily, is the amount of disc space that is currently occupied. The percentage is based on the amount of space being used relative to the amount of space required to contain data for the entire retention period specified (as displayed on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

Directory integration

The Management Console supports integration with Active Directory, Azure AD, ForgeRock LDAP, 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.



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 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. If a user is enabled in two (or more) directories, the Authentication Server will select the directory that was integrated with Secret Double Octopus first.

The following sections describe how to add:

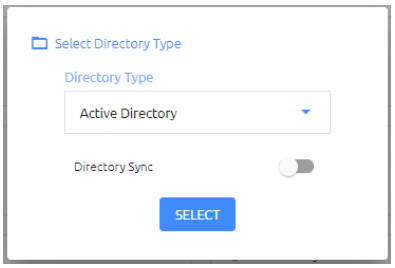
- AD, Oracle/Open LDAP and ForgeRock directories
- ForgeRock Cloud directories
- Azure AD directories
- Google directories

AD, Oracle/Open LDAP, and ForgeRock LDAP

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

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

   The **Select Directory Type** dialog opens.

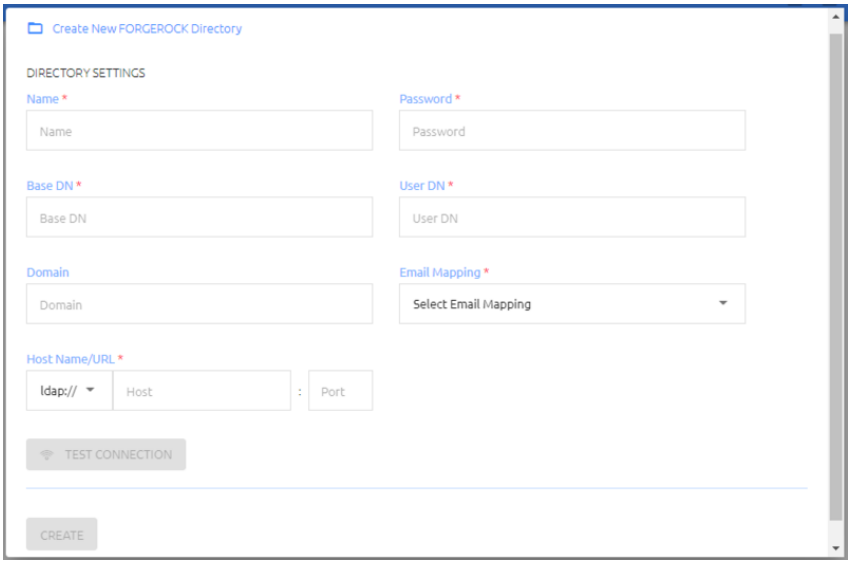


2. Open the **Directory Type** list and select the type of directory that you want to add.
3. Click the **Directory Sync** toggle button to enable and disable automatic syncing.

> **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.

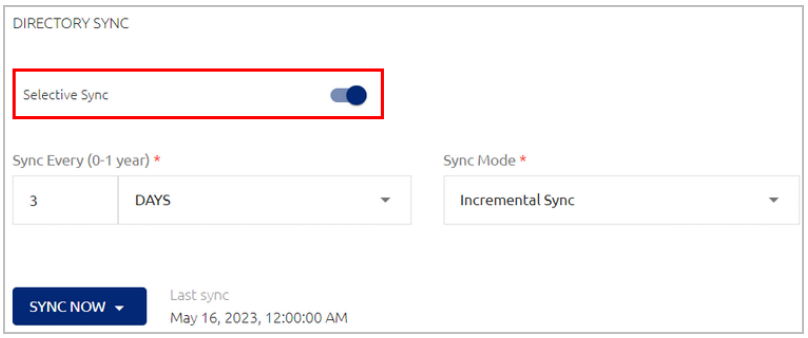
6. Click **Test Connection** to perform a validity check.

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.



   c. Click **Save**.

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

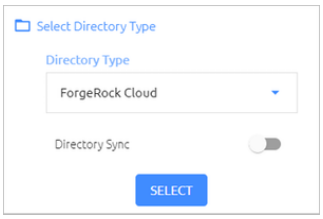
ForgeRock Cloud

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**.



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.

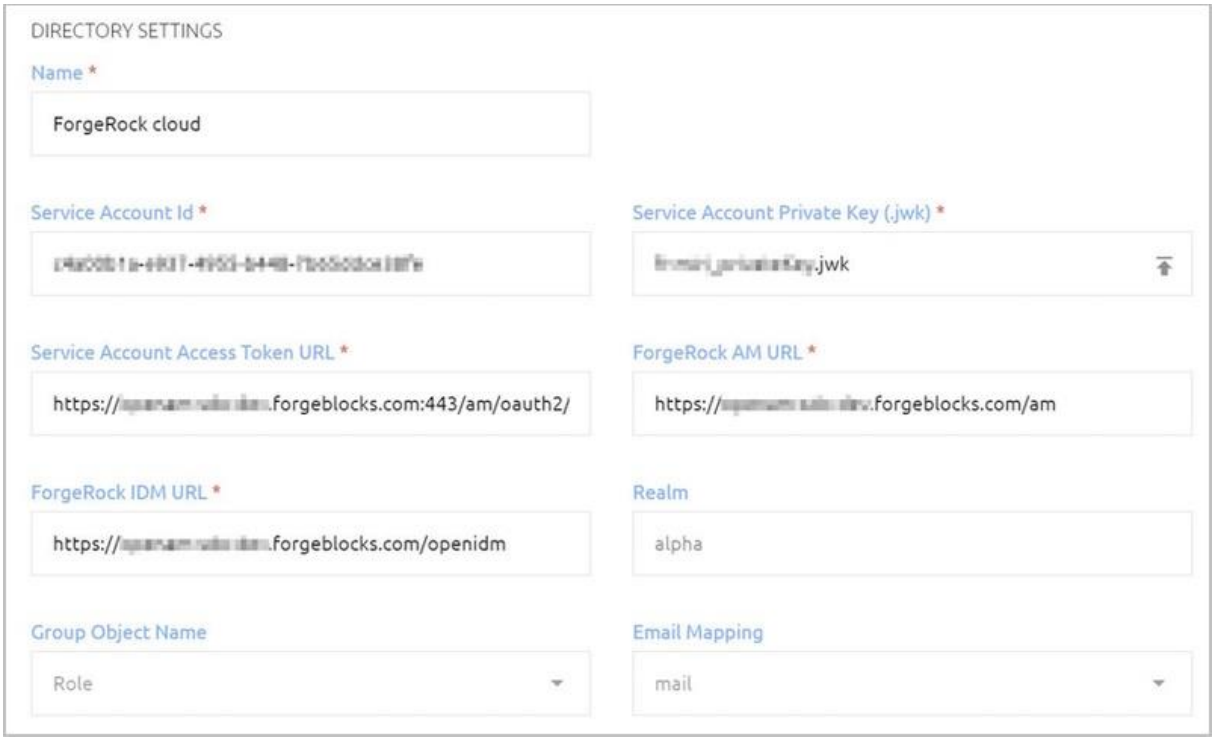
5. Configure the following directory settings:

   - **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:



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.

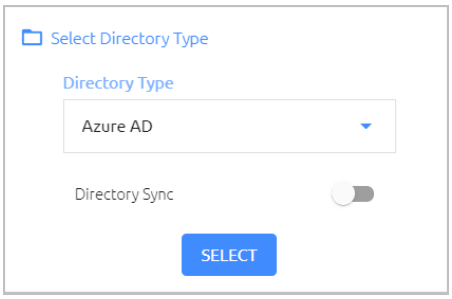
Azure AD

To add a new Azure AD 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 **Azure AD**.

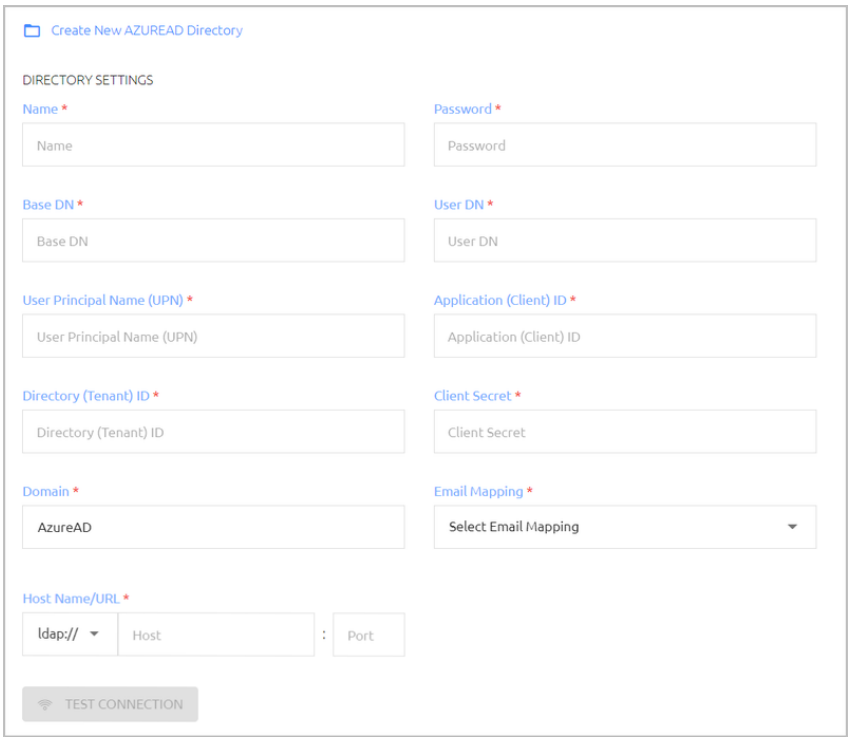


3. Click the **Directory Sync** toggle button to enable and disable automatic syncing.

> **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:

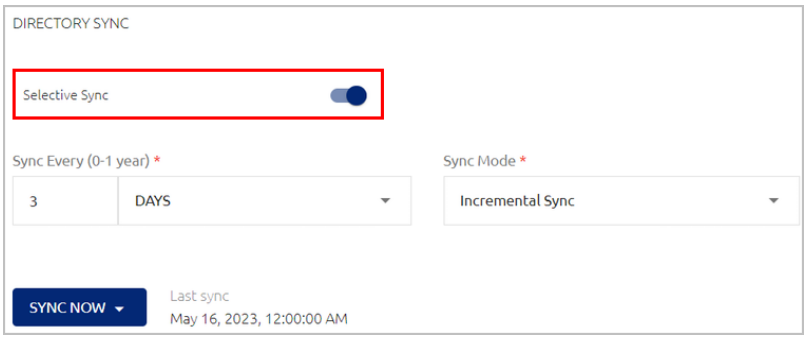
   - **Name:** Name by which the directory is known.
   - **Password:** The password for the administrative user account.
   - **Base DN:** The distinguished name of the directory from which users will be added to Octopus Authenticator. If you want to add only a specified set of users, enter the relevant 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 value from your Azure AD Portal after creating the secret. (To create the secret, navigate to **Certificates and Secrets**, click New Client Secret and enter a value.)
   - **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:** 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.



   c. Click **Save**.

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

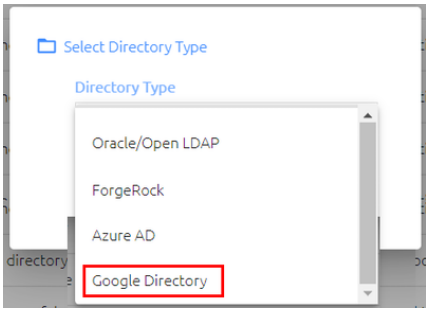
Google

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**.

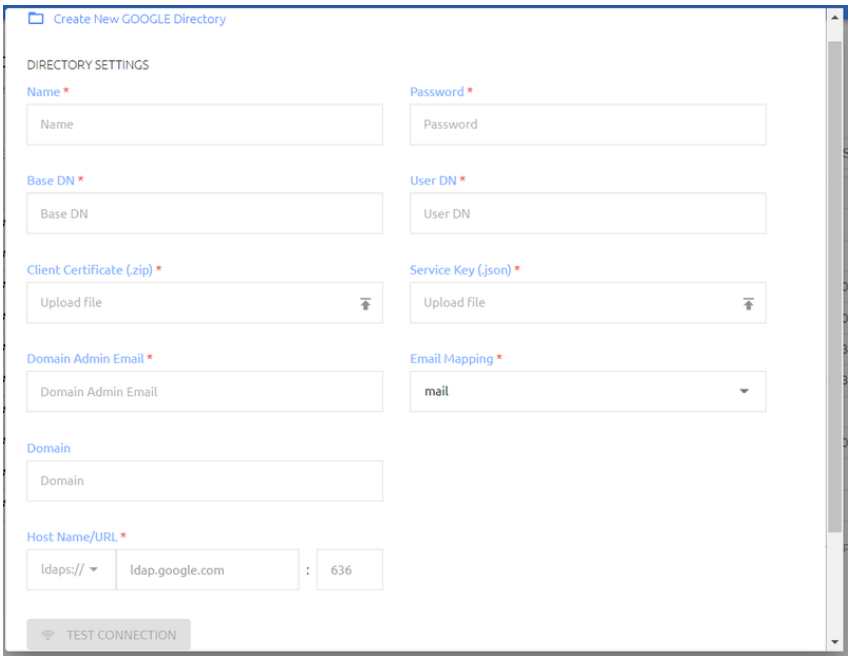


3. Click the **Directory Sync** toggle button to enable and disable automatic syncing.

> **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.

- **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

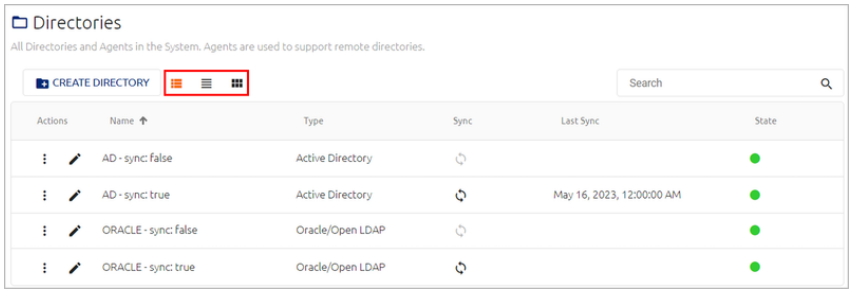
The **Directories** menu lists all integrated directories and enables you to update their settings. The following information is provided about each directory:

- Name
- Type (AD, Oracle/Open LDAP, ForgeRock or Google)
- 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)

The icons next to the **Create Directory** button enable you to control the display of page content:

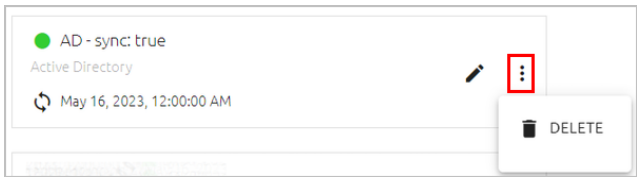
- **Cards view:** Directories are presented in separate frames.
- **List view:** Directories are presented in list form, with up to 10 items on a page.
- **Compact List view:** Directories are presented in list form, with up to 20 items on a page.

Both List views support sorting the list according to name, type, or sync status by clicking on the relevant column header.



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).

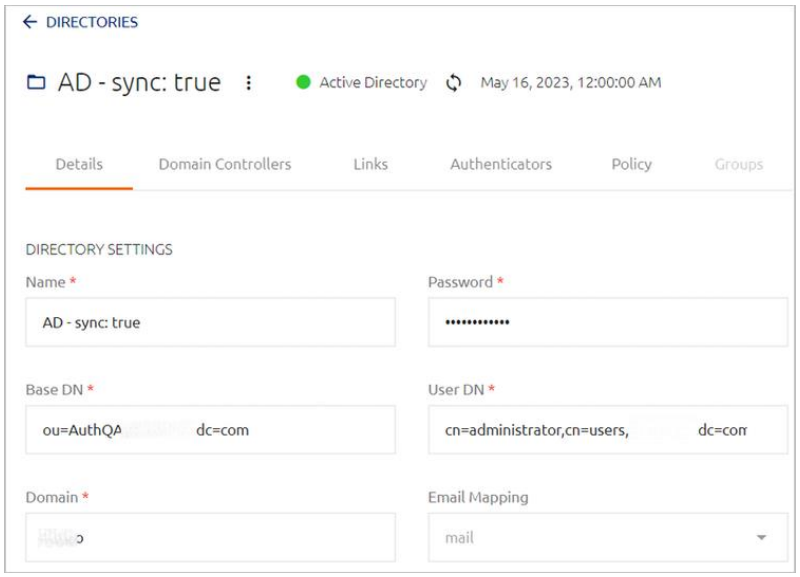
The Delete feature allows you to remove directories that are no longer in use. In the row or tile of the relevant directory, click ⋮ and select **Delete**.



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.



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

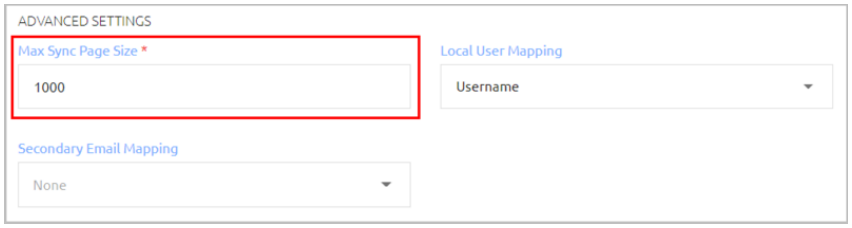
- **Directory Settings:** Displays the directory connection configuration. For details about these settings, refer to Adding a New Directory.
- **Advanced Settings:** Allows you to set maximum number of records and other directory-specific parameters. For details, refer to Configuring Advanced Settings.
- **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.

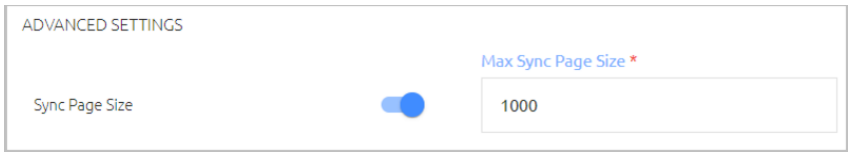
Configuring Advanced Settings

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.



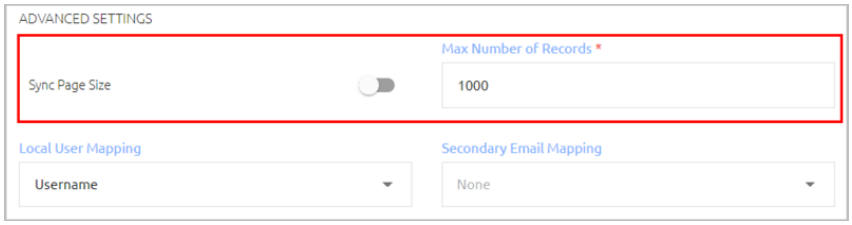
The **Sync Page Size** setting appears in directories with automatic syncing. When the toggle is enabled, pagination is set when adding users from the directory to the authentication platform. If you choose this option, specify the **Max Sync Page Size** in the field to the right.



Note

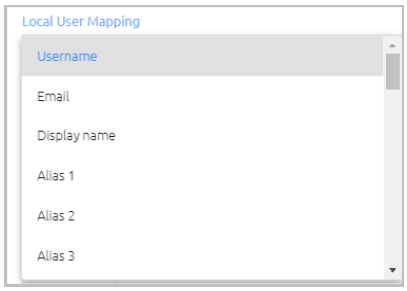
Keep in mind that page size affects the number of records that can sync with the Active Directory. A small page size can lead to multiple calls to the AD.

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

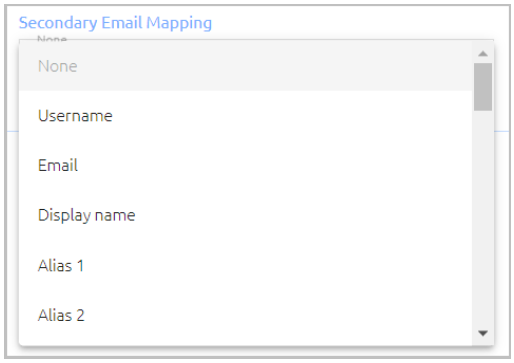


The following settings are available for all directories, regardless of automatic syncing status:

- **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.



After updating Advanced Settings, 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 directory sync settings

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

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

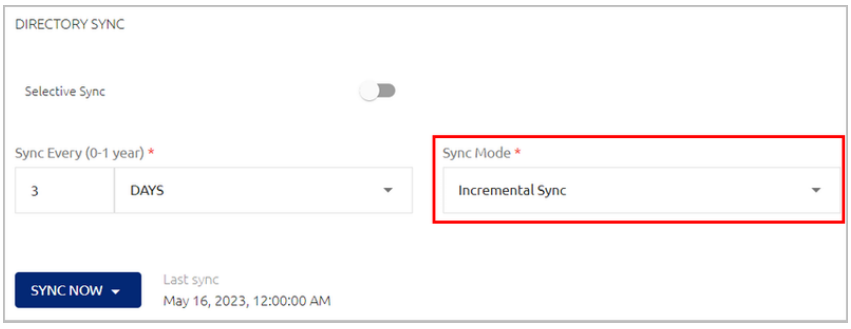
Directory Sync settings for AD type directories include the **Selective Sync** toggle button. Click the toggle button to enable / disable selective syncing. When the feature is enabled, you will be able to choose the Groups that are included in the sync process. For more information, refer to Working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

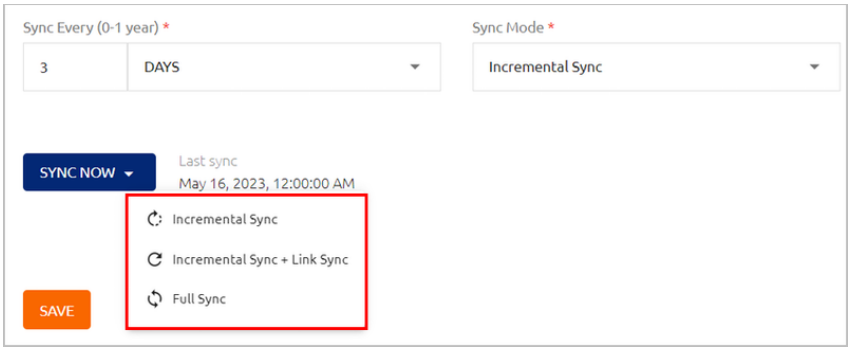
- **Incremental Sync:** Checks for changes and updates in the Active Directory and syncs these changes with the Management Console.
- **Incremental Sync + Link Sync:** As part of the incremental sync, user properties in all linked directories are also updated.
- **Full Sync:** Involves a complete sync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



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

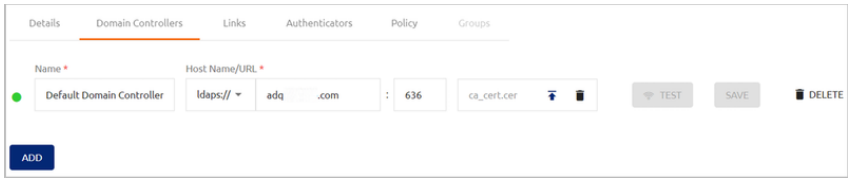


After updating Directory Sync settings, click **Save** . Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

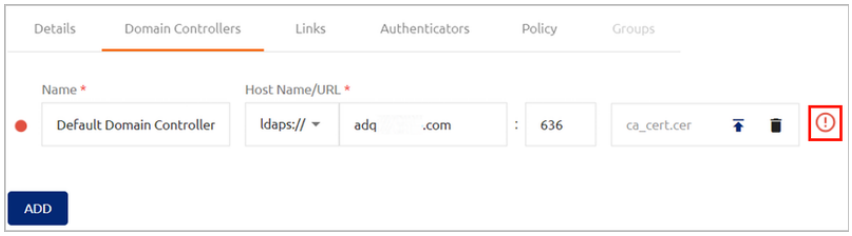
Managing domain controllers

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.

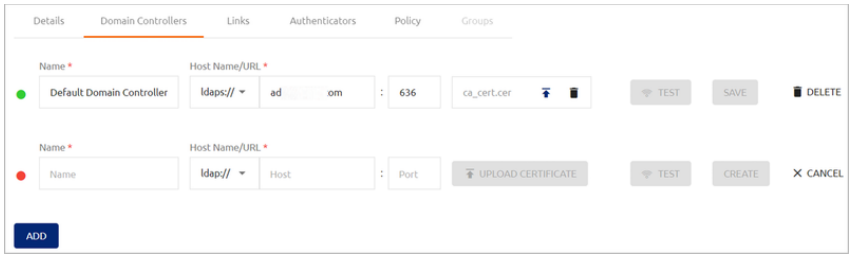
The **Test** button becomes enabled whenever you make changes to parameters of a domain controller, allowing you to perform a validity check before saving the new settings. The **Delete** button enables you to remove domain controllers that are no longer in use.



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



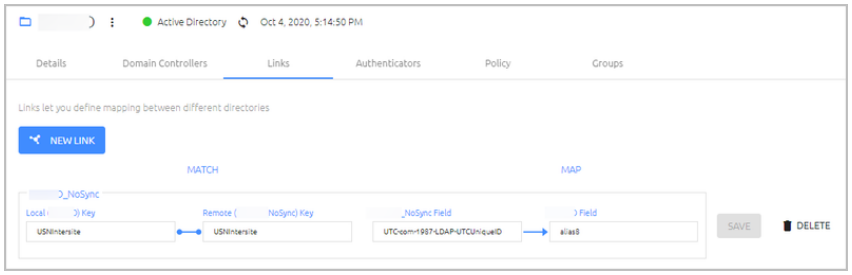
If your environment utilizes multiple servers for the directory, you can configure the additional domain controllers in the Management Console. Click **Add** and enter the details of the domain controller in the relevant fields. Then, click **Create**.



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.

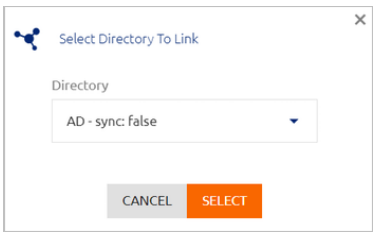
The directory from which you create the link is called the Local directory. The directory to which you link is known as the Remote directory.



To add a directory link:

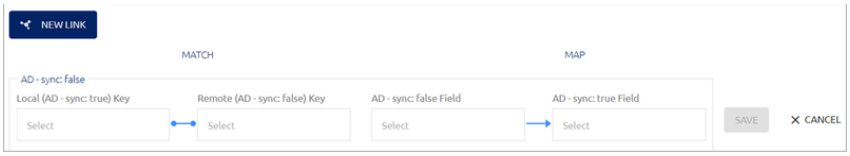
1. From the **Directories** menu, open the settings of the directory in which you want to create a link and select the **Links** tab. At the top of the tab, click **New Link**.

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

2. 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.

3. 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.

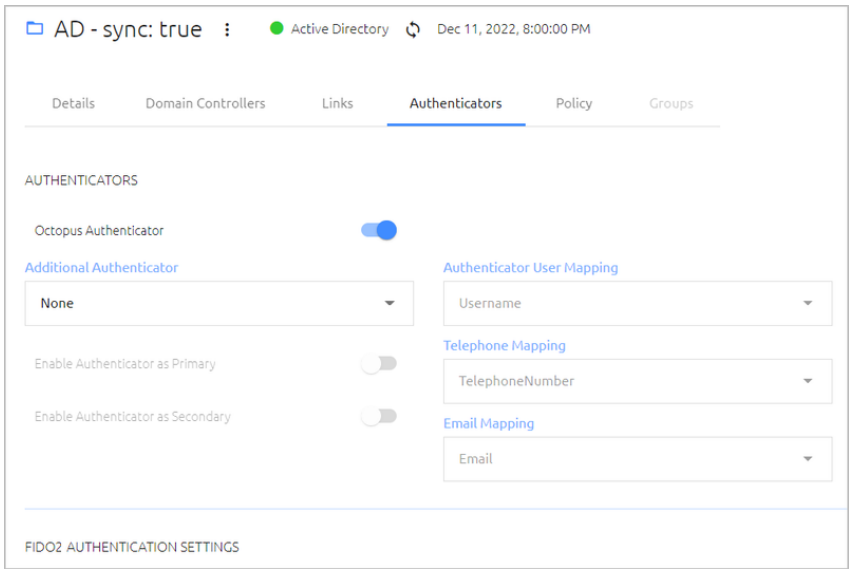
4. On the right side of the row, select a value to be imported from the Remote directory to the Local directory. Then, select the parameter in the user properties of the Local directory to which the value will be imported. (This is generally one of the **Alias** fields.)

5. 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

Secret Double Octopus 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.

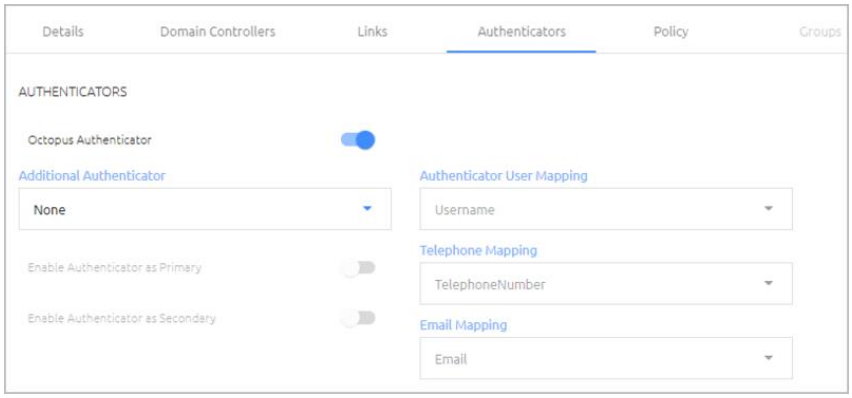


After updating settings in the **Authenticators** tab, click **Save** (at the bottom of the page). Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

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 is comprised of all third party authenticators that have been added to the **Authenticator List** of the **System Settings** menu.)

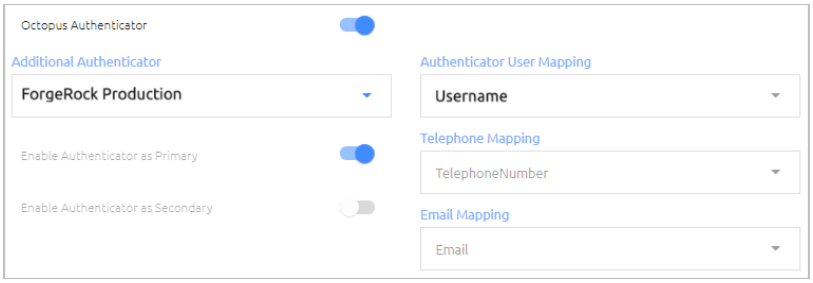
   Once you have selected an authenticator, the settings below the list are enabled.

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**:



- **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

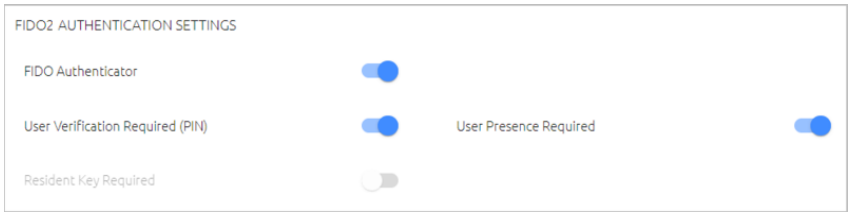
FIDO authentication is supported for:

- 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.



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.

  When using MFA with password, the User Verification setting should remain *disabled* (off), as the Username + Password is the first authentication factor and the FIDO authenticator is used as the second 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).

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

- **Resident Key Required:** When enabled, the identity of the private key used for authentication is required. In the current version, this setting is disabled.

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 user's 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.

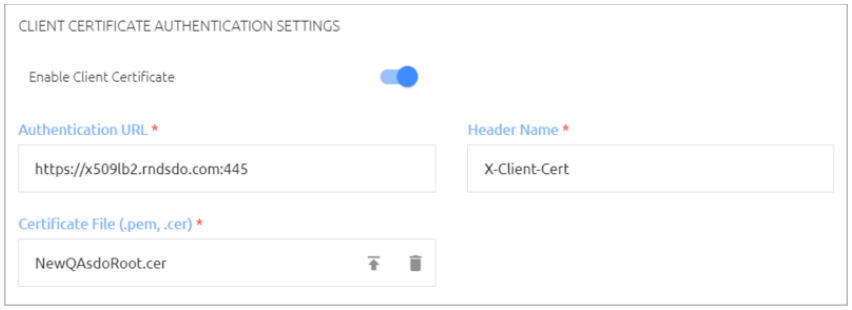
To successfully use smart card authentication, you need to configure the following settings:

- **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.



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.

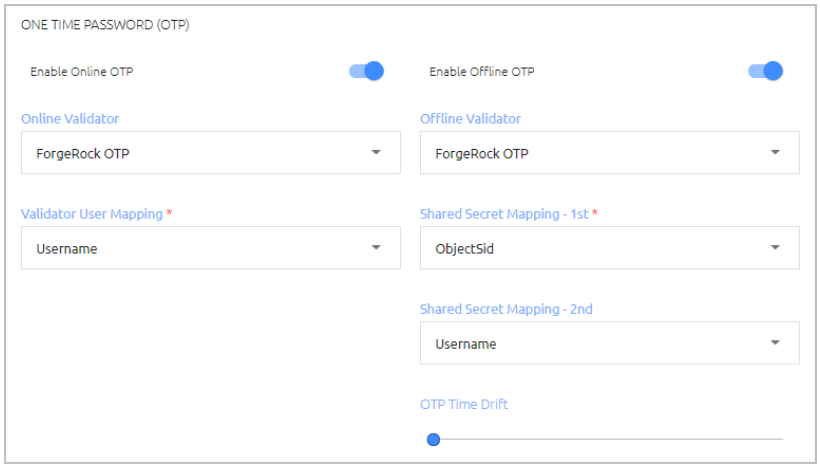
One Time Password (OTP) Settings

To enhance authentication capabilities, Secret Double Octopus 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.

Secret Double Octopus offers the following OTP processes. Either or both can be enabled, as required:

- **Online OTP:** When enabled, enrolled users can 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 can 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 is 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.

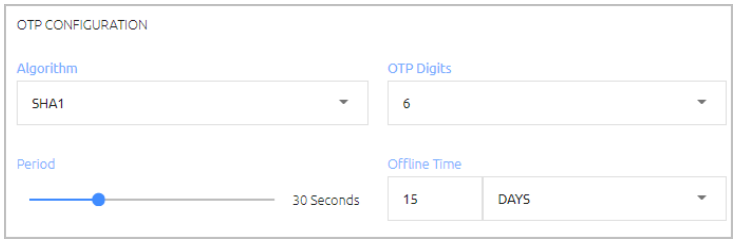


To enable OTP:

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 Third Party Authenticators.

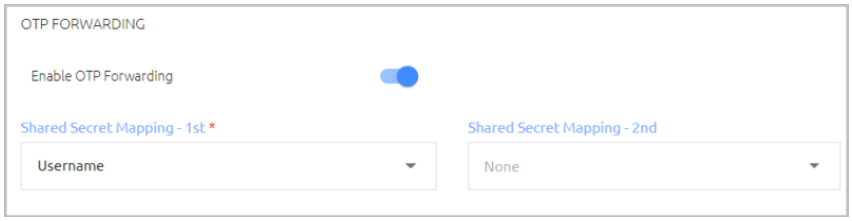
2. Under **Validator User Mapping**, select the user parameter to be used for OTP authentication.
3. To activate offline OTP, click the **Enable Offline OTP** toggle button. Then, select the appropriate authenticator from the **Offline Validator** list.
4. From the **Shared Secret Mapping**, list(s), 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 for which the user is allowed to authenticate offline (default = 15 days).



Important

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

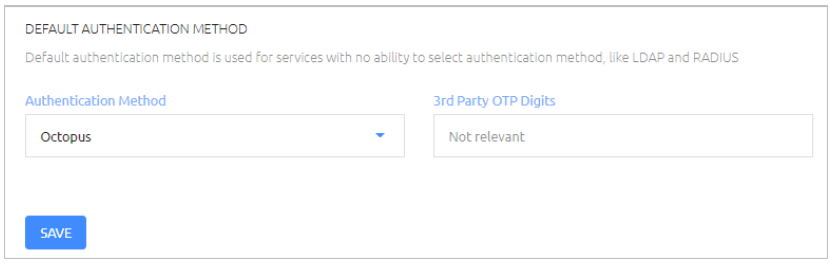
7. If you want to provide authorization to pass the OTP to another authentication platform, click the **Enable OTP Forwarding** toggle button. Then open the **Shared Secret Mapping - 1st** list and select the user identification parameter utilized by the external authenticator. Optionally, you may select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



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.

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.



The options are:

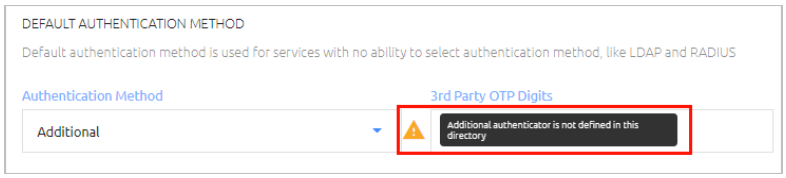
- **Octopus:** The Octopus Authenticator.
- **OTP:** The validator that is specified in the directory's One Time Password (OTP) settings.

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).

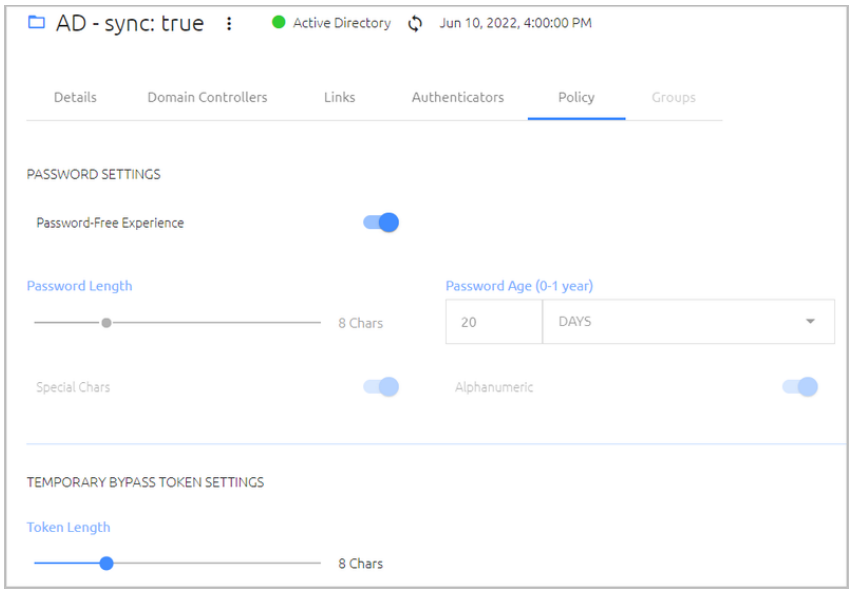
If you select a default authentication method that is currently disabled or not defined in the directory's settings, a warning icon appears next to your selection.



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

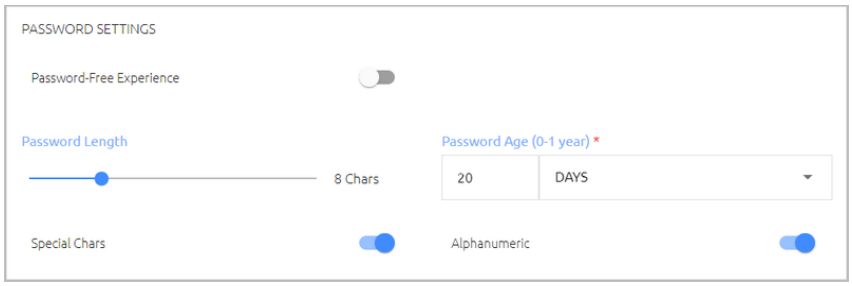


After updating settings in the **Policy** tab, click **Save** (at the bottom of the page). Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

Password Settings

All directory types have configurable settings related to the directory password.

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



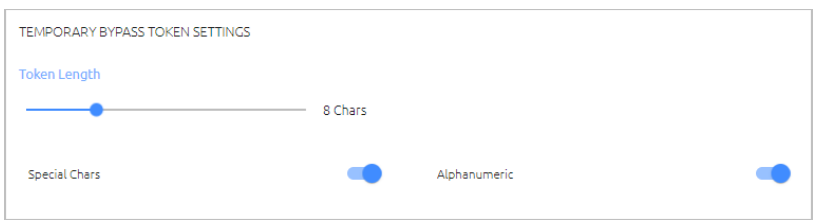
The **Password-Free Experience** toggle is related to support of the Password Free Experience on the Windows Agent. By default, this toggle is off, as the feature is not relevant when the system is working in Compatibility Mode. If you turn Compatibility Mode off, make sure to turn activate the **Password-Free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

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.

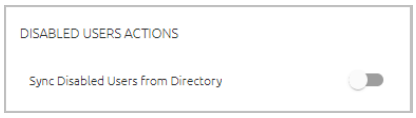


The settings are:

- **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.



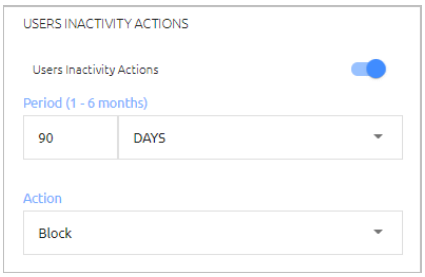
You may continue to send enrollment invitations to disabled users as necessary (e.g., during AD migrations).

User Inactivity Actions

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

To set user inactivity actions:

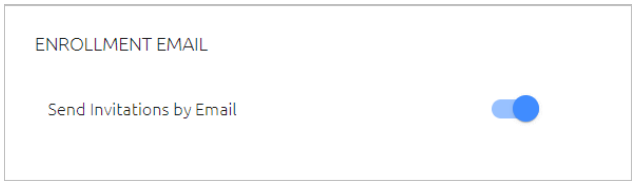
1. Activate the feature by clicking the **User Inactivity Action** toggle button.



2. Specify the maximum period 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

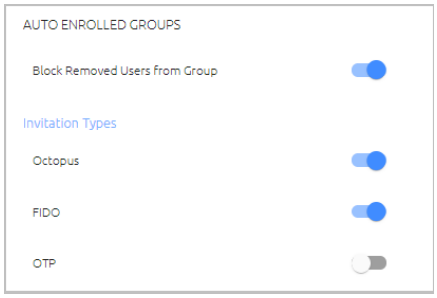
This setting allows you to control how enrollment invitations are delivered. By default, the toggle is enabled, and invitations are automatically emailed to users. To support delivery of invitations by other means (e.g., internal organizational workflows), click the toggle to disable the setting, and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



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.

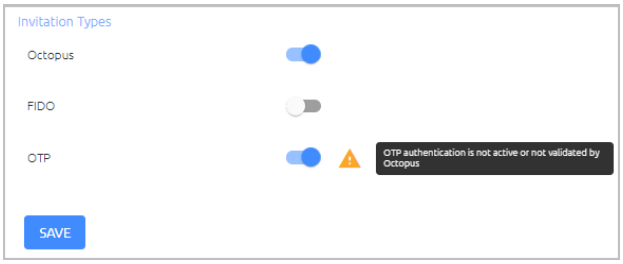
> **Note**
> Auto Enrolled Groups settings appear only in directories for which automatic syncing is enabled.



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 and OTP). 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.



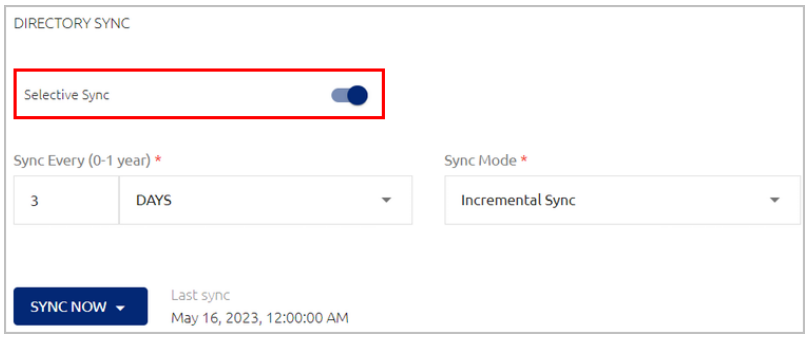
Working with selective syncing (AD)

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

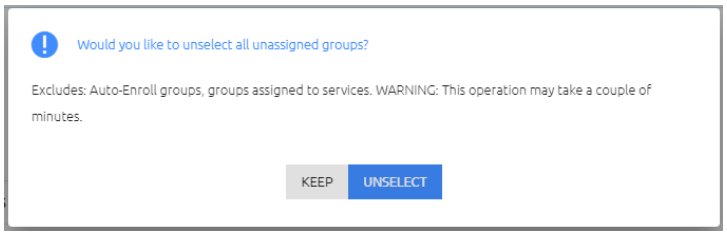
- **Full Sync:** All Groups in the directory are automatically synced with Secret Double Octopus.
- **Selective Sync:** Only the Groups specified in the Management Console (in the **Groups** tab of the directory's settings) are automatically synced.

> **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.

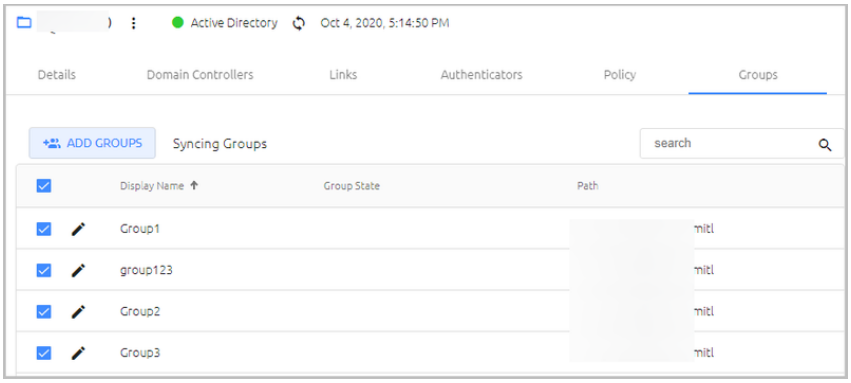


When you switch from Full Sync to Selective Sync, the following popup opens, prompting you to specify how to handle Groups that are currently *not* assigned to any services. (Groups assigned to services will continue to be synced.)



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.



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 Secret Double Octopus. You can change your Group selections at any time.

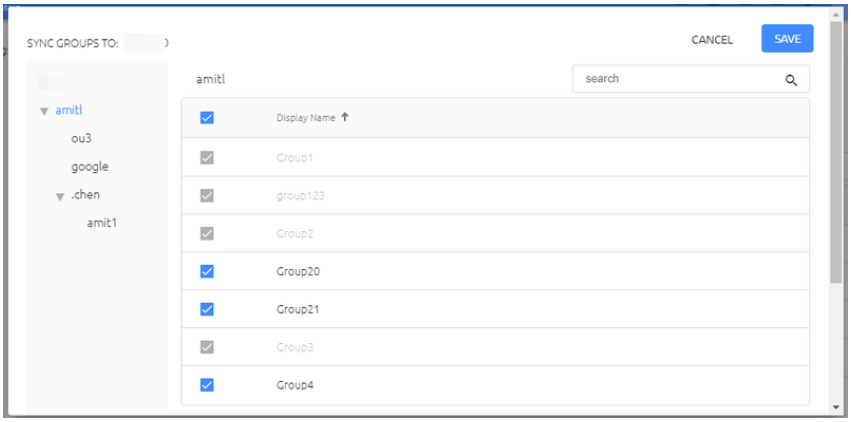
Follow the procedure below to specify Groups to be synced with the directory.

To select Groups for automatic syncing:

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

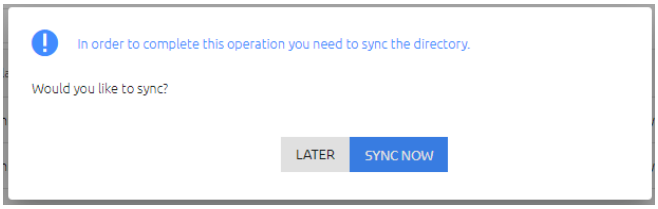
   The **Sync Groups To** dialog opens.

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.)



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

   A popup opens, prompting you to sync the directory.



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.

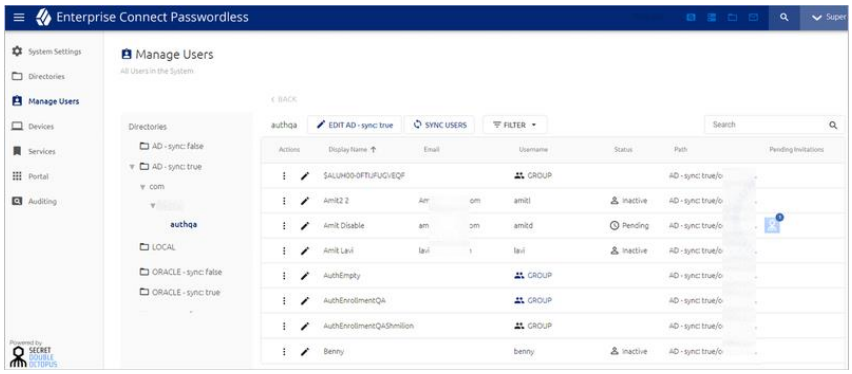
   The popup closes, and the selected Groups are listed in the **Groups** tab.

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.



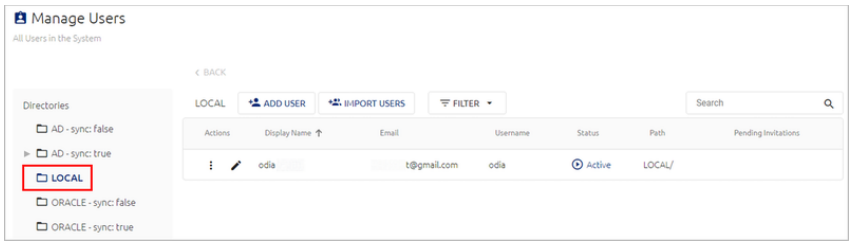
The following sections present:

- 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.

Understanding the users list

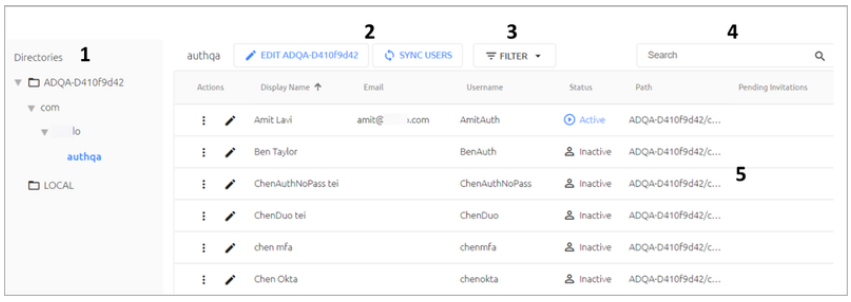
The Users List enables you to view details of any user by selecting the relevant directory and Group, or by performing a keyword search for the user or Group. By default, the Users List displays all the users in the Local directory.



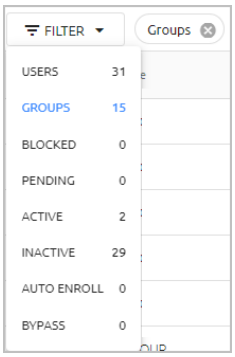
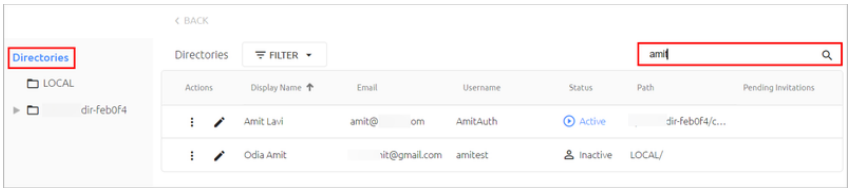
The Local directory is a default, internal directory that cannot be deleted. Users are added to the Local directory by manually creating them or by importing them from a CSV file. The Local directory is useful for organizations that do not manage users through external directories.

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.



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

2	Directory action buttons	Provide quick access to common directory management actions. The actions for integrated corporate directories are **Edit** (redirects to the directory's settings) and **Sync Users** (begins the directory sync process). 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).
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.) 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: 
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. 
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. A user's status can be one of the following:

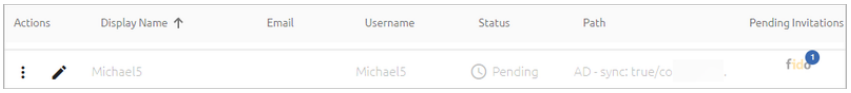
Active: The user has enrolled in an account, created a PIN or verified a FIDO key set, and is authorized to authenticate using the Octopus Authenticator.

Inactive: The user is not enrolled in the system and has no pending enrollment invitations.

Pending: The user has pending invitations but has not yet enrolled in the system.

Blocked: The user is currently not authorized to authenticate using the Octopus Authenticator, PIN or FIDO key.

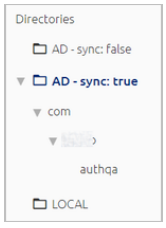
If a user is disabled in the Active Directory server, the row of that user in the Users list is disabled. You may continue to send and manage enrollment invitations for disabled users, but no other actions can be performed on them.



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:

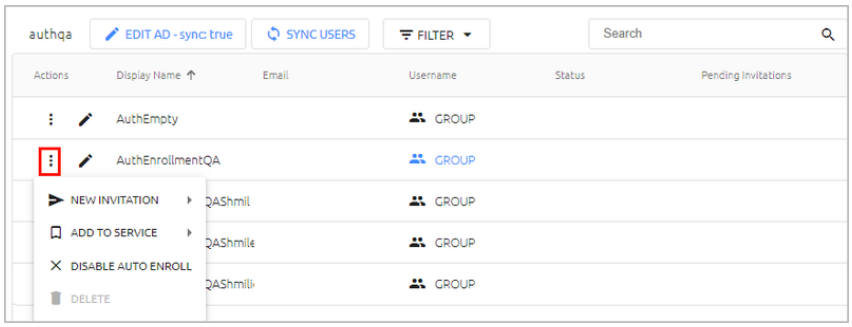
Clicking this icon automatically opens all the sub-nodes beneath the selected node:



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

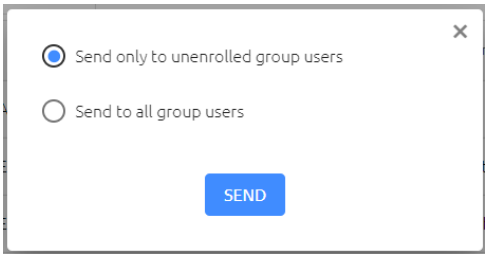
For convenience, you can perform some common administrative actions on Groups directly from the Users list, by clicking ⋮ in the row of the Group and then selecting the relevant action.



The available actions are:

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

  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:



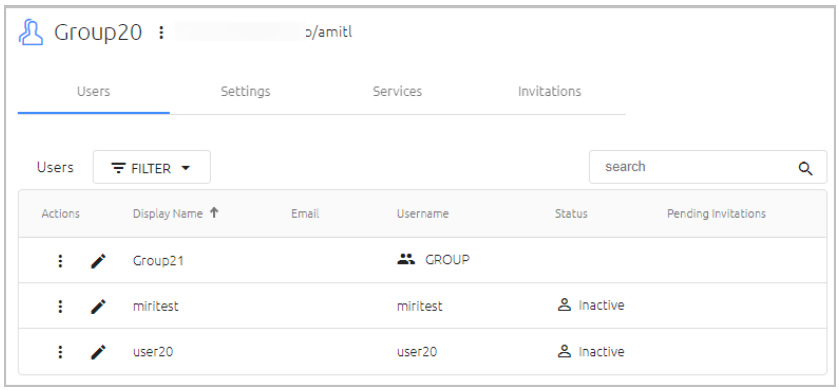
> **Important**
>
> In order to enable users to authenticate to Windows using a FIDO key, the corporate directory must have a configured domain. It is recommended to open the directory settings and verify that the **Domain** field is completed.
>
> If the Windows agent is configured with both an internal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

  Note: 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.

- **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.
- **Delete**: Removes the Group from the Users list. This option is enabled for Groups in Directories without automatic syncing.

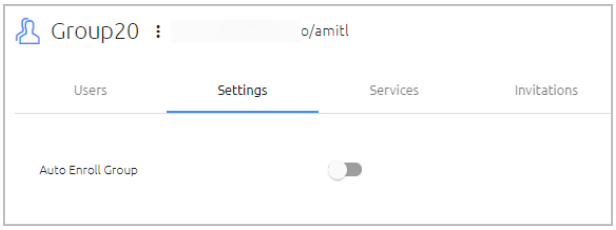
Clicking ✎ in the row of a Group opens the **Users** tab. This tab lists the subgroups and users assigned to the Group and displays general information about each one. Open the **Filter** list to view the number of subgroups and users in the Group, as well as other relevant information about Group entities.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



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.

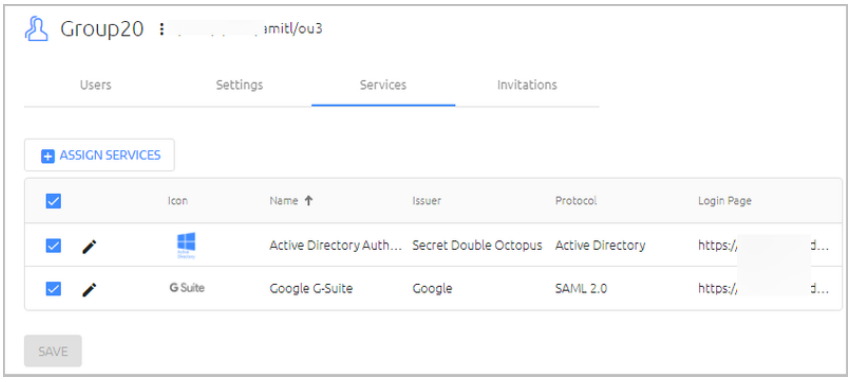
The following additional tabs are available:

- **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.

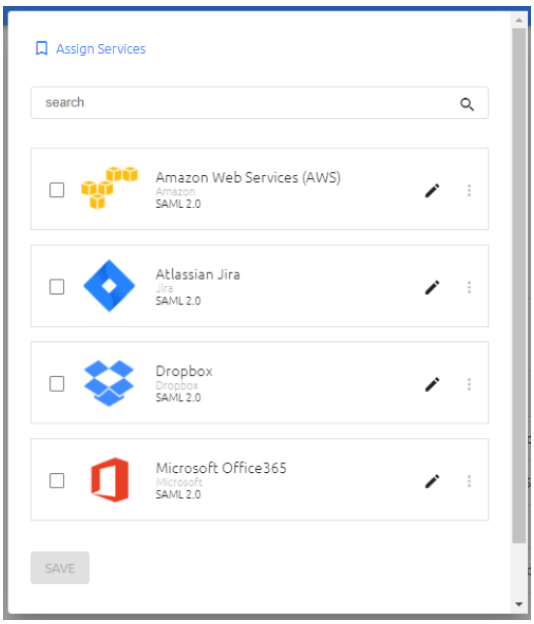


- **Services:** Displays the services that the Group is currently authorized to access. The checkboxes on the left are toggles that allow you to control whether that service is enabled for the Group. In the example below, all the services are enabled.

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

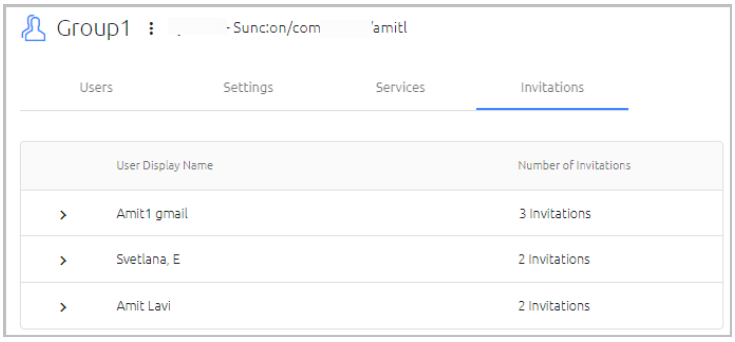


To assign additional services to the Group, click **Assign Services**. In the dialog that opens, specify the services to add by selecting the relevant checkboxes, and then click **Save**.



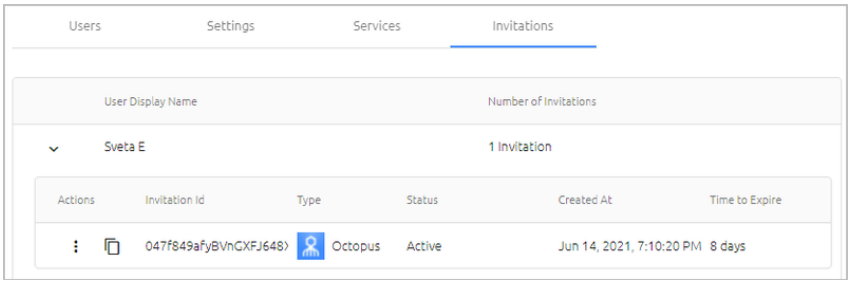
The services listed in the **Assign Services** dialog are ones to which the Group is *not* currently assigned AND which may be used by directories to which the Group belongs. If a service is not listed in the dialog, open the settings of the service and verify that the appropriate directory is selected.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

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



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.

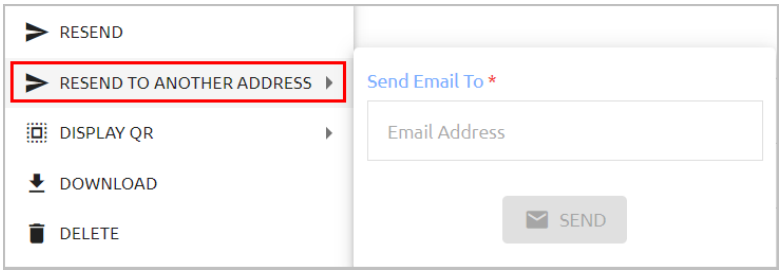


Clicking  copies the invitation's enrollment link or code, according to invitation type:

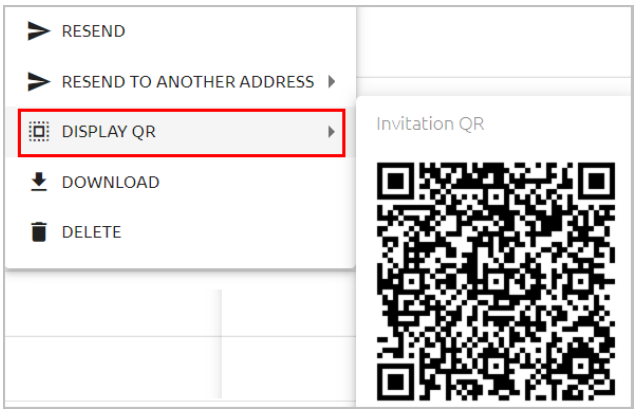
- **Octopus type invitations:** The Copy action copies the Invitation ID, which is then converted to the manual enrollment code provided in the invitation.
- **FIDO / OTP type invitations:** The Copy action copies the link for registration provided in the invitation.

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.

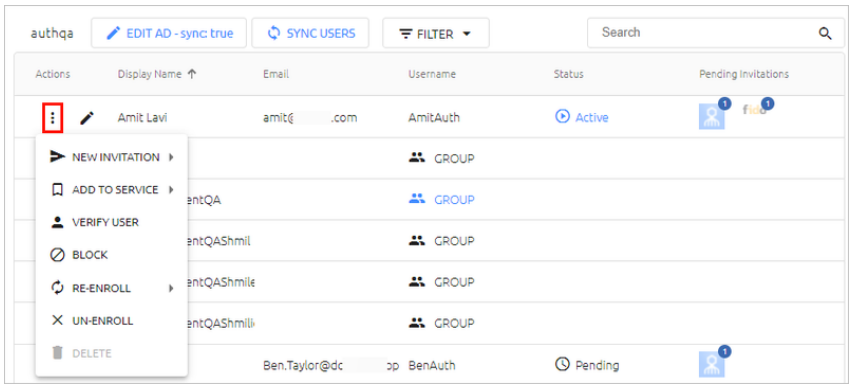


- **Download:** Saves the invitation as an email file and downloads it to your machine.
- **Delete:** Removes the invitation from the system.

> **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.



The available actions are:

- **New Invitation:** Sends the user an invitation via email. You can invite users to enroll in the authenticator app, register a FIDO key, or obtain a one-time password. 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.

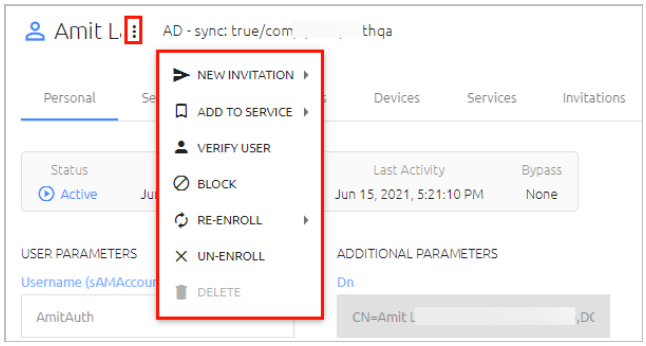
- **Add To Service:** Enables you to control which services are enabled for the user, by selecting or clearing the checkboxes. The services listed are the ones that are available for directories to which the user belongs.

  Note: 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.

- **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.
- **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.

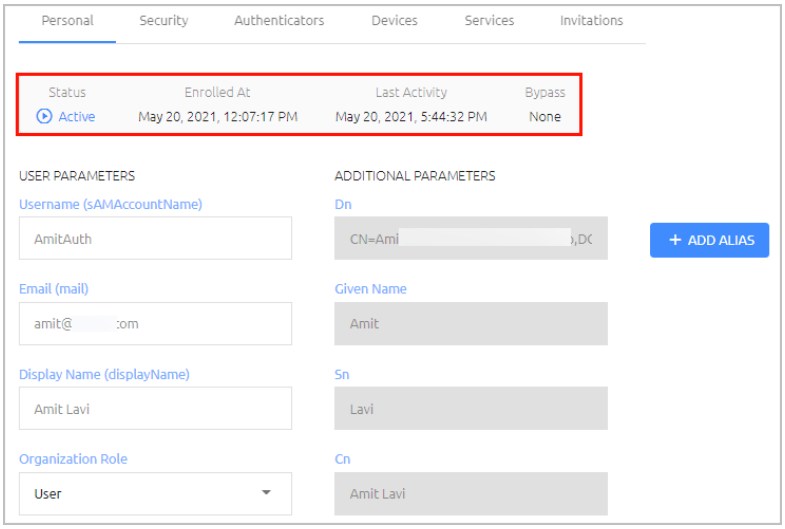
Clicking  in the row of a user opens a page from which you can view and manage user details. At the top of the page, the full path of the user's directory appears to the right of the user's name. Clicking opens a quick access actions list that enables you to perform common administrative operations on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



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.)

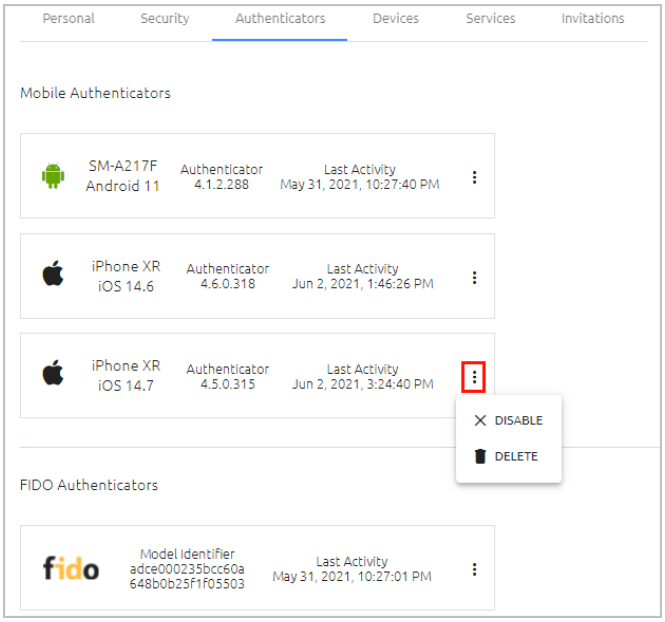
  The bar at the top of the **Personal** tab shows the user's status (Active, Inactive, Pending or Blocked), date / time of enrollment, date / time of the user's most recent activity, and details related to Octopus Authentication Bypass.



- **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 enrolled mobile and FIDO devices of the user and provides basic information (e.g., OS version, model identifier, etc.) about each one.

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



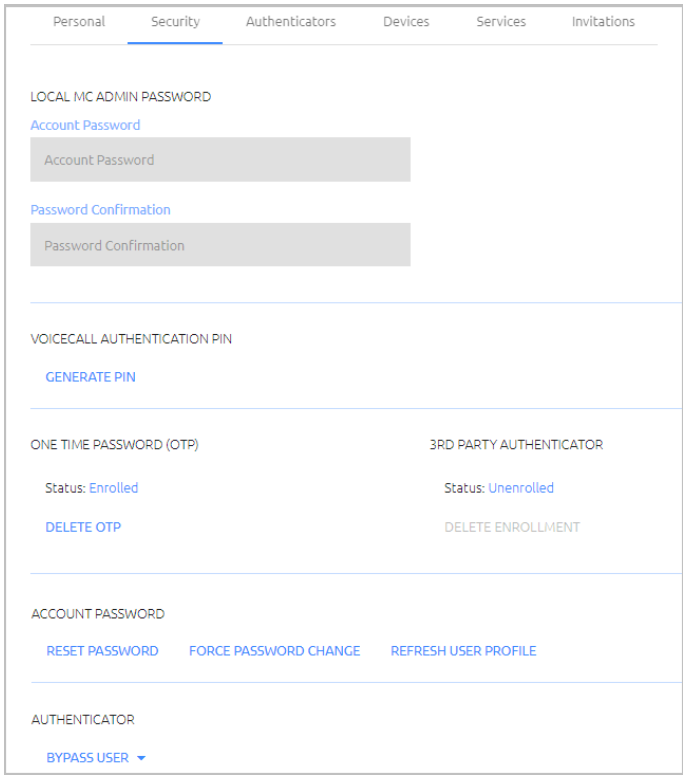
Note

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

- **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.
- **Invitations:** Lists all active enrollment invitations sent to the user and allows you to manage them. For details, refer to Managing Invitations.

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.)

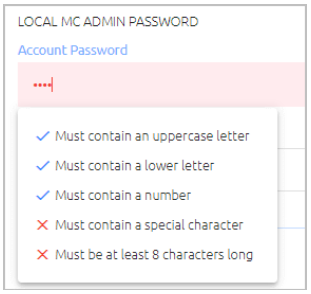


The following operations are available:

- **Set Local MC Admin Password:** This is the password used for access to the Octopus 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.

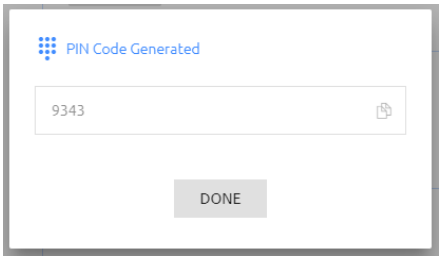
To set (or update) the password, enter the password in the **Account Password** field. Password requirements are displayed as you type.



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.



  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 Secret Double Octopus.

- **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**.

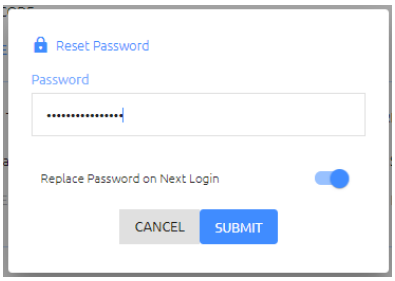
- **View and manage 3rd party authenticator settings:** The **Status** parameter indicates whether the user has authenticated using of the defined 3rd party authenticators. (When the user first logs in using one of these authenticators, the status changes from **Unenrolled** to **Active**.) You can change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

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.



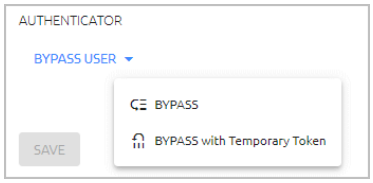
For users in the Local directory, **Reset Password** enables you to change the password for user verification in services that utilize multi-factor authentication. The **Replace Password on Next Login** toggle is disabled for Local users.

> **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.

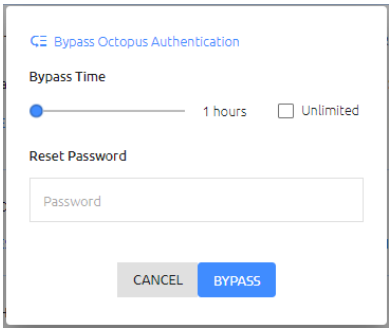


The **BYPASS** option enables you to set a specific or unlimited amount of time for the bypass period. During the bypass period, the user may authenticate with username and password.

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.

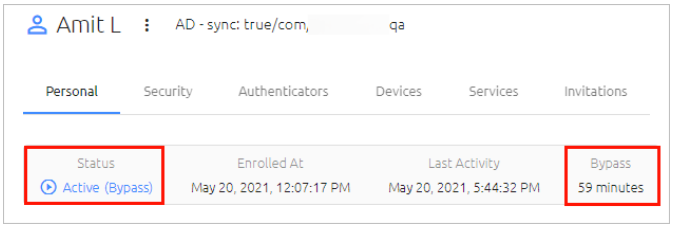


2. Drag the slider until the desired period for the bypass is displayed. (The range is 1 hour- 14 days.) Alternatively, click the **Unlimited** checkbox (recommended for machine-to-machine authentication).

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.



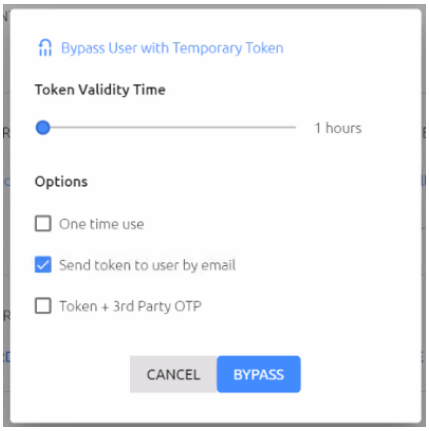
5. To cancel the bypass before the expiration time, at the bottom of the **Security** tab, click **End Bypass**.

The Bypass with Temporary Token option allows you to set a specific period 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.



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

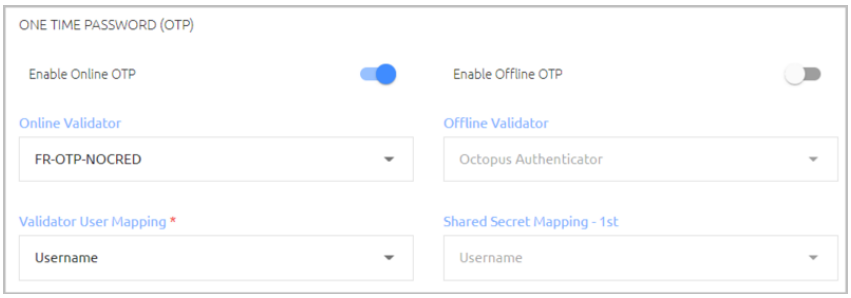
3. Select the following checkboxes as required:

   - **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 can 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 **Password** 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.



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.

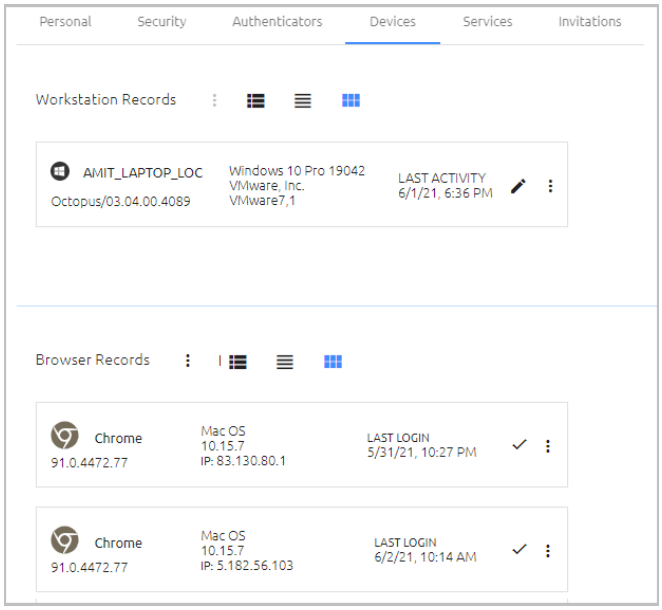
5. To cancel the bypass before the expiration time, at the bottom of the **Security** tab, click **End Bypass**.

> **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.



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.

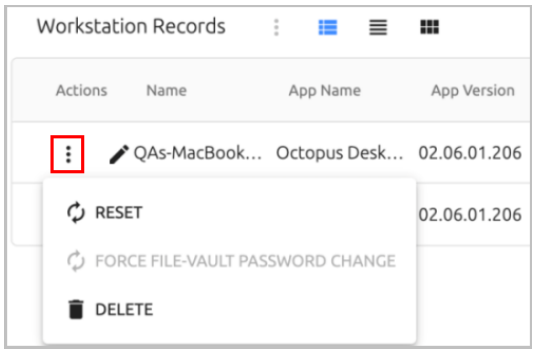
Clicking ✎ redirects you to another page where you can view more details about the workstation.

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

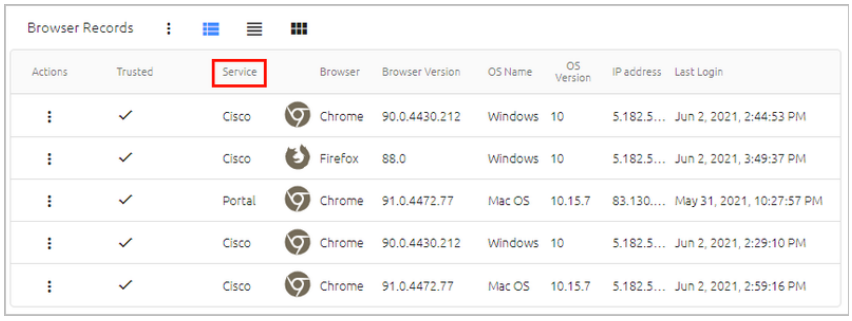
- **Reset:** Deletes the workstation's history and all generated security keys. Use the **Reset** action after upgrading the workstation to Windows Agent 3.3 or Mac Agent 2.3.0. Following a reset, the workstation will generate a new security key with the next authentication.

- **Force FileVault Password Change:** Initiates an immediate rotation of the FileVault password. This operation is available for Mac workstations only. 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 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.



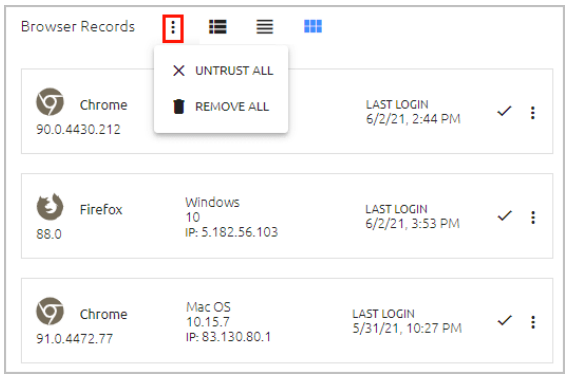
The **Browser Records** display lists all browsers through which the user has authenticated to SAML services or the User Portal. The browser version, basic workstation details and last login information are provided. A ✓ icon indicates that when Adaptive Authentication is enabled, strong authentication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



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:

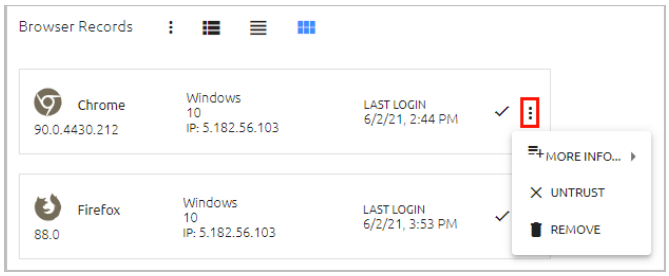
- **Untrust All:** Removes the Trusted status of all browsers currently marked as Trusted. (When users authenticate on untrusted browsers, they need to enter a verification code on every authentication.)

- **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.



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).



Managing User Services

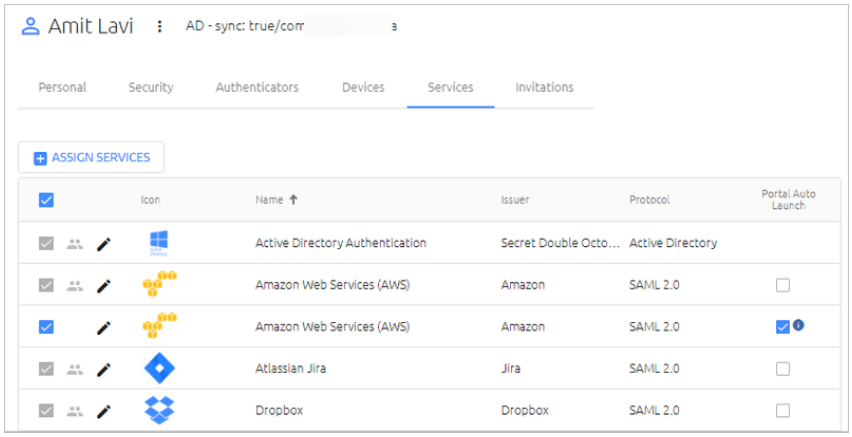
This tab lists all services to which the user is assigned. (The tab does not appear for users who are disabled in the Active Directory server.)

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 AWS service is assigned to both a Group to which the user belongs (non-editable settings), and directly to the user (editable settings). The Jira and Dropbox services are assigned only to Groups of which the user is a member.



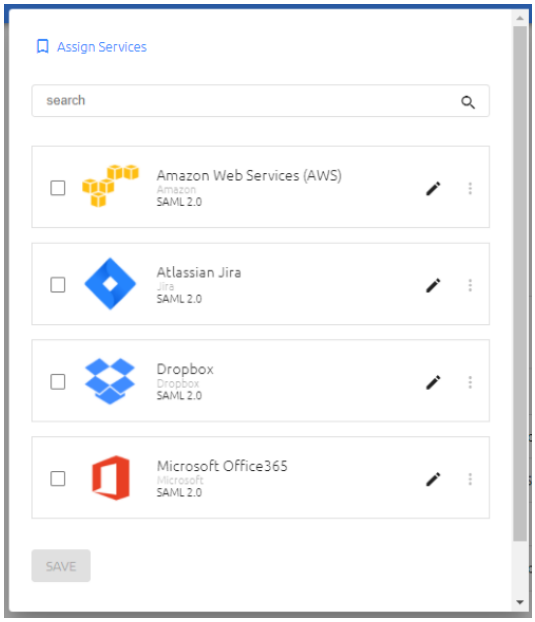
The **Portal Auto Launch** column, which is relevant only to SAML services, indicates whether the Auto Launch feature for that service is currently enabled for the user. (When the feature is enabled, the service opens automatically upon login to the User Portal.) You can enable or disable Automatic Launch 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 shown above, AWS Auto Launch is enabled for this user, even though it is disabled for the Group and for the SAML service.

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**.

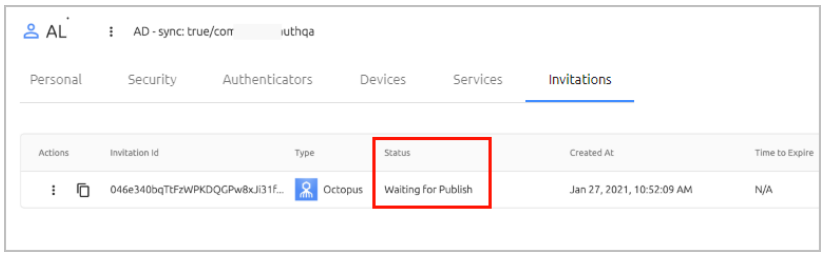


The services listed in the **Assign Services** dialog are ones to which the user is *not* currently assigned AND which may be used by directories to which the user belongs. If a service is not listed in the dialog, open the settings of the service and verify that the appropriate directory is selected.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

Managing User Invitations

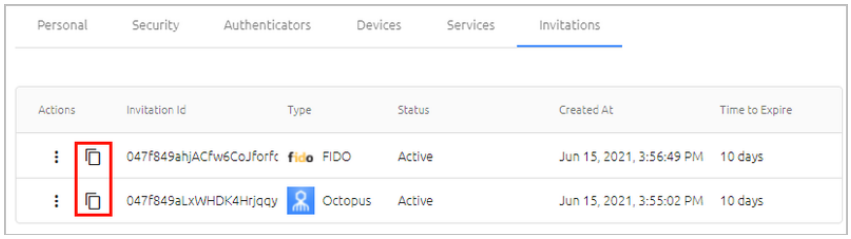
The **Invitations** tab lists all enrollment invitations sent to the user and details about each one, including its unique identifier, invitation type and time until expiration. The **Status** column shows the handling workflow for the invitation. This workflow is determined by whether the user is already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



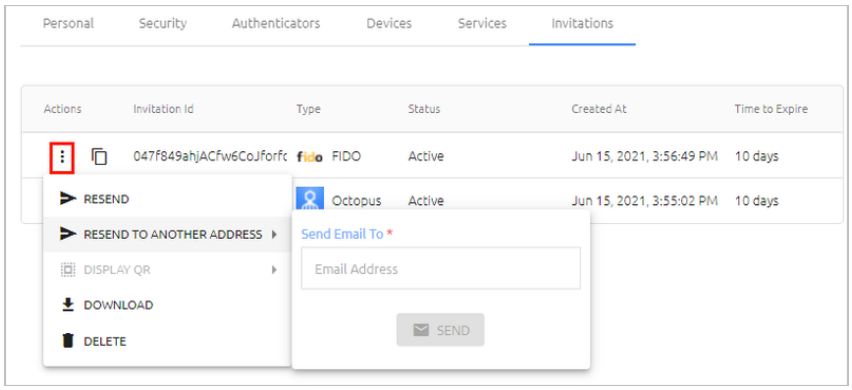
Clicking copies the invitation's enrollment link or code, according to invitation type:

- **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.



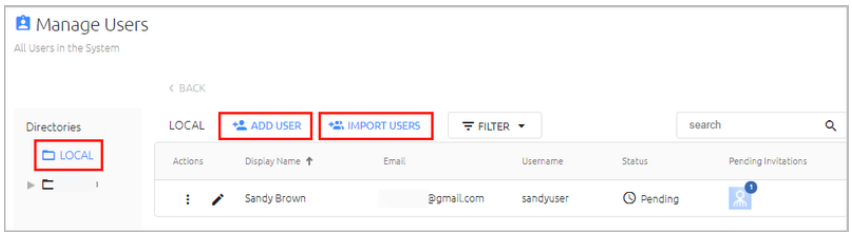
Note

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

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**).



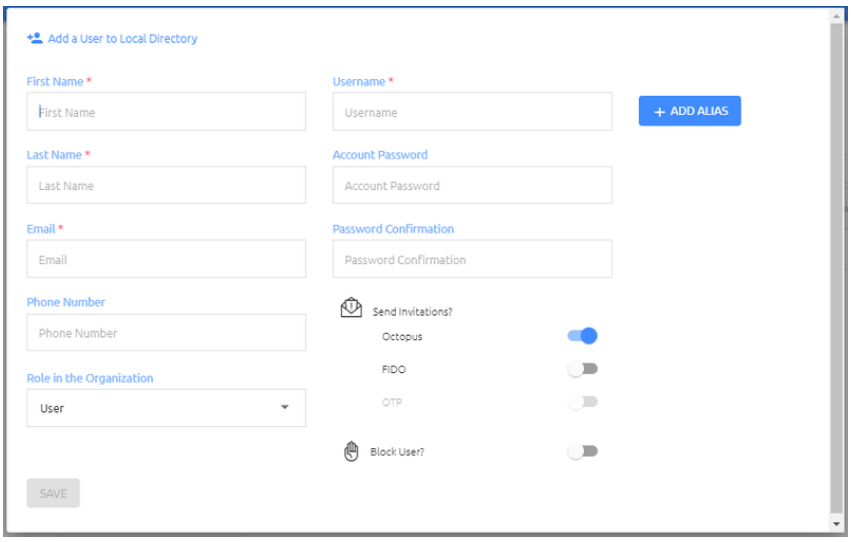
Adding local users manually

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).



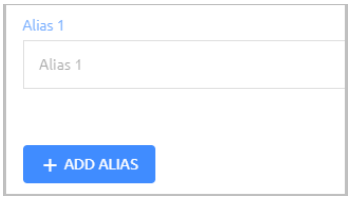
3. By default, a role of **User** is assigned. To assign a different role, open the **Role in the Organization** list and select one of the following options:

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

4. If relevant, 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.



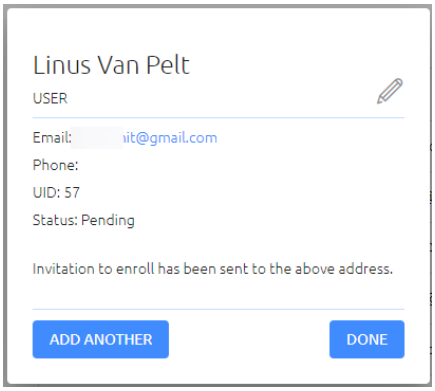
6. Review the following settings:

   - **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.



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**.

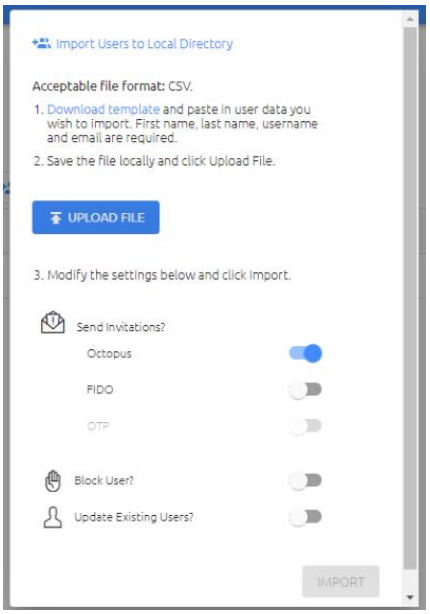
Importing local users from a CSV File

The **Import Users** button enables you to add Local users in a bulk operation by uploading user details from an 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.



   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 if 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.

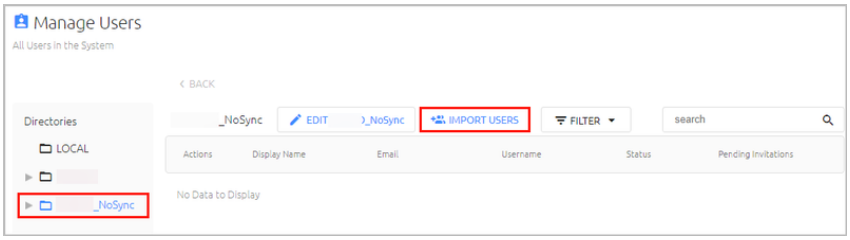
6. To perform an additional import, click **Import More**. To close the dialog and return to the Users list, click **Done**.

Importing users from a directory

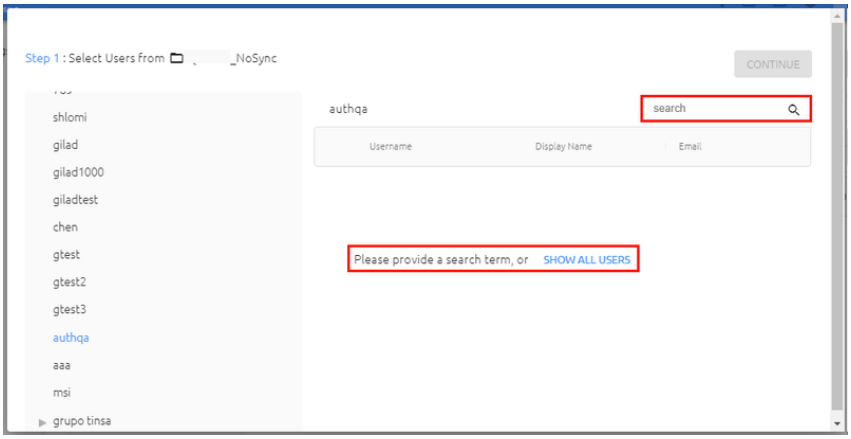
The Import Users feature enables you to add users to the Management Console in a bulk operation. Use this feature to import selected users from a directory that is integrated with the Management Console but does NOT have automatic syncing of users.

To import users from an integrated directory:

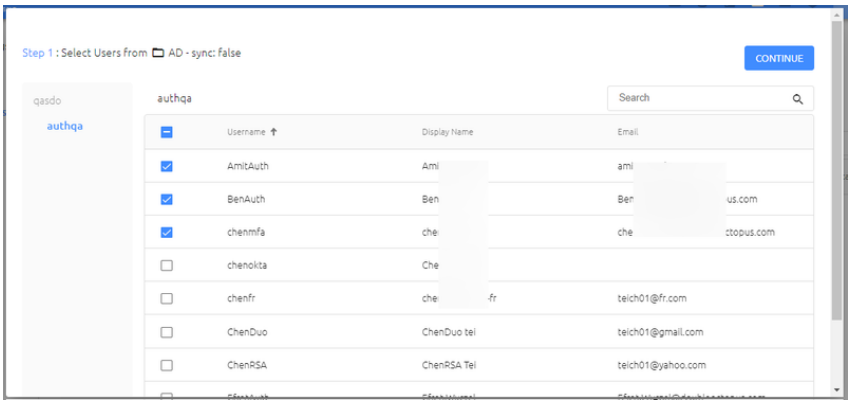
1. From the **Manage Users** menu, select the relevant directory from the **Directories** list. Then, click **Import Users**.



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**.



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



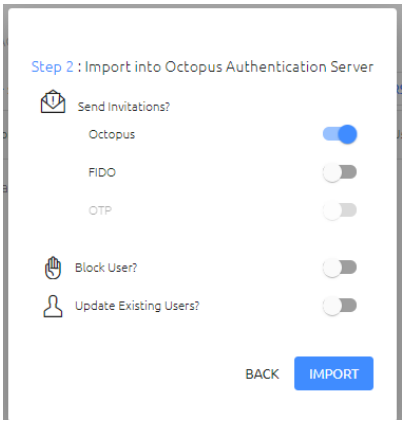
When you have finished selecting users, click **Continue**.

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.

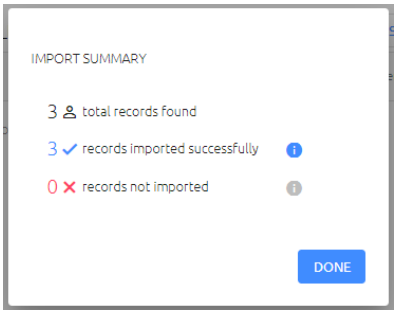
   - **Block Users**: Determines whether imported users will be prevented from authenticating with Octopus Authenticator, FIDO key or OTP. The default setting is Disabled (users will be able to authenticate).

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



Then, click **Import**.

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



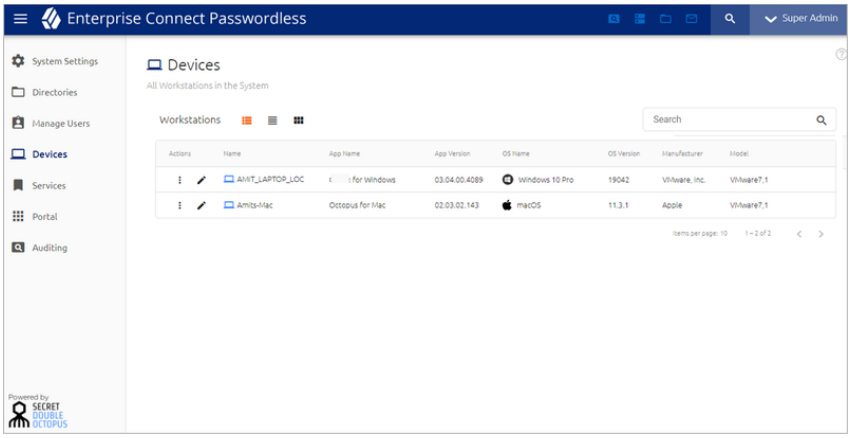
Click the information icons to view more details.

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

Managing system workstations

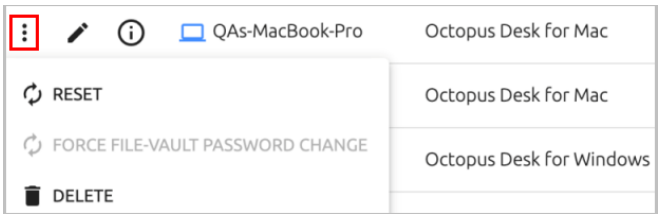
The **Devices** menu enables you to easily view and manage any workstation that communicates with the Octopus Authentication Server. The Workstations grid lists all machines in the system and provides basic information about each one. You can quickly locate specific workstations using the Search tool, by entering the name or ID of the workstation.

Click the display icons at the top of the page to change the presentation to Cards View List View or Compact List View . List View displays up to 10 items per page, and Compact List View displays up to 20 items per page. Both List views support sorting the workstations according to any column by clicking the relevant column header.



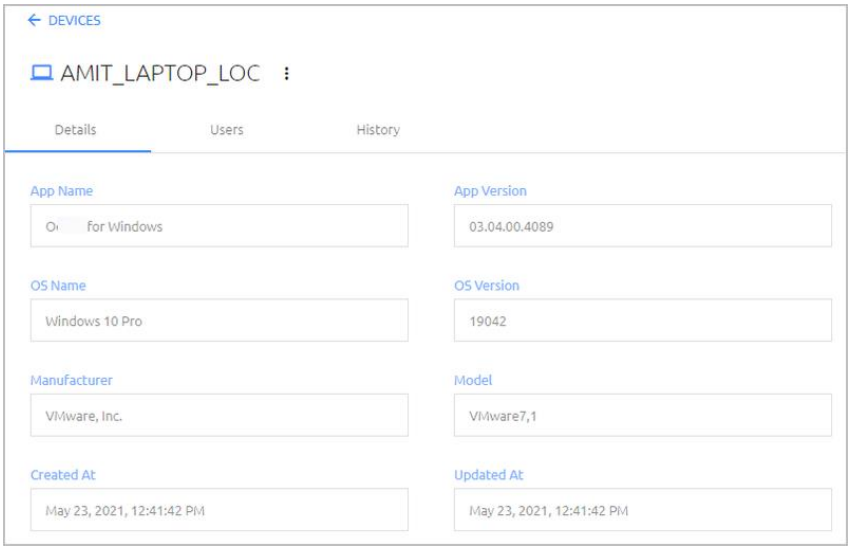
Clicking ⋮ in the **Actions** column allows you to perform the following operations on the workstation:

- **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:** Initiates an immediate rotation of the FileVault password. This operation is available for Mac workstations only. 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 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.

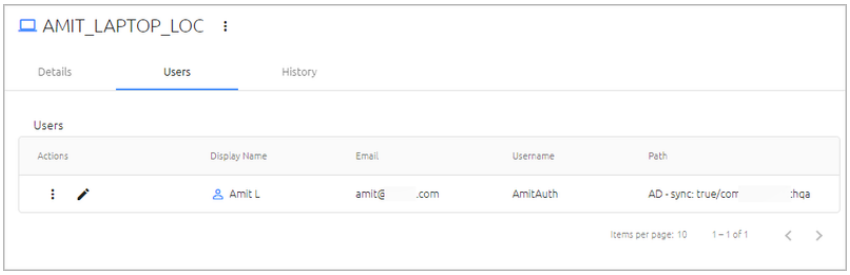


Clicking ✎ opens another page containing the following tabs, each of which provides additional data about the workstation:

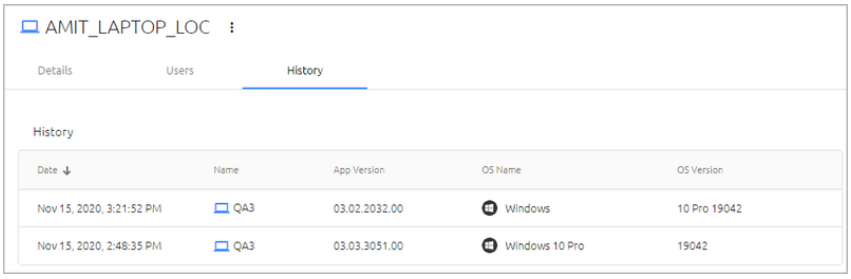
- **Details:** Lists general information about the workstation, as well as timestamps for the machine's entry into the system and most recent update.



- **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.

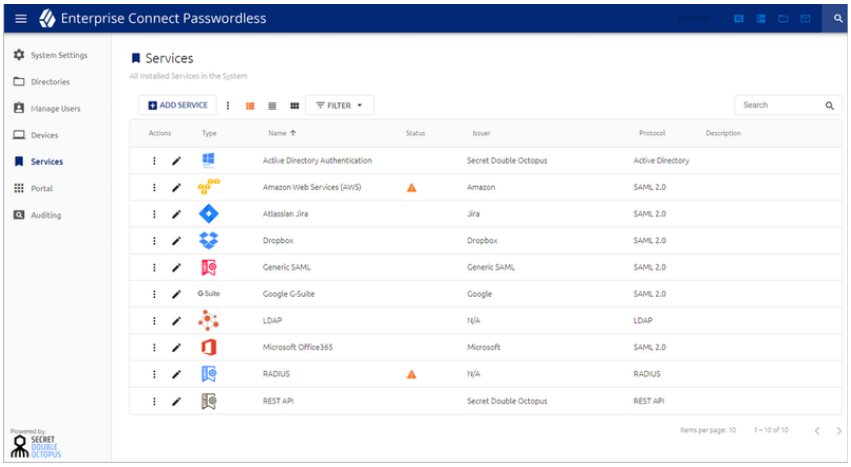


- **History:** Provides information about all updates and upgrades that took place on the workstation.



Integrating services

Services are the applications that are integrated to work with Octopus Authenticator to authenticate users. All services are added, configured and updated from the **Services** menu of the Management Console.



Note

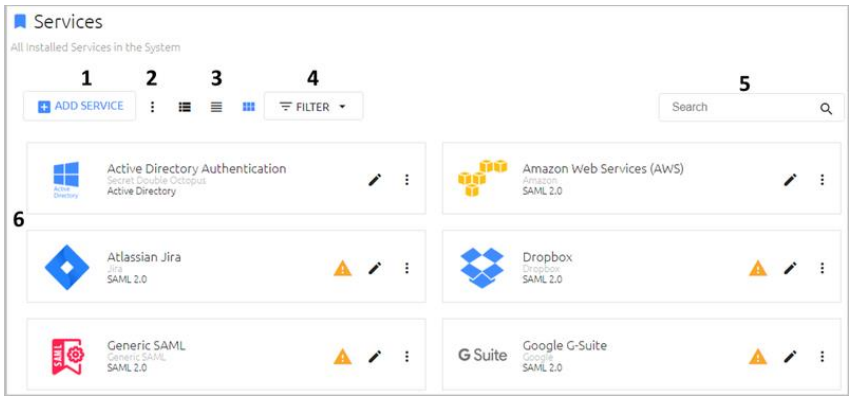
You can collection of guides containing end-to-end instructions on how to configure integration for different services on the Support Portal of Secret Double Octopus's website.

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 Generic SAML 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 Google G Suite Service Integration
- Configuring Microsoft Office 365 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 Select Services feature, which allows you to perform some bulk operations on specific services. For details, refer to Performing Actions on Services.
3	Display icons	Clicking these icons changes the page presentation to Cards view , List view or Compact List view . List view displays up to 10 services per page, and Compact List view displays up to 20 services per page. Both List views support sorting services according to name, issuer or protocol by clicking on the relevant column header.
4	Filter	This feature shows the total number of enabled and disabled services and allows you to filter the Services list according to the selected option (e.g., clicking **Disabled** displays only services that are currently disabled).
5	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.
6	Services list	Lists your installed services and provides basic information about each one, including the service name, issuer and type. A icon appears in the row or tile of services whose settings are incomplete or invalid. Clicking the icon opens a popup

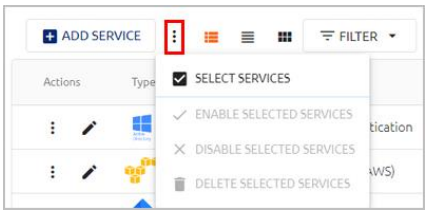
listing the invalid settings and a description of the specific error (missing value, incorrect syntax, etc.).

You can perform various operations on individual services directly from the Services list. For details, refer to Performing Actions on Services.

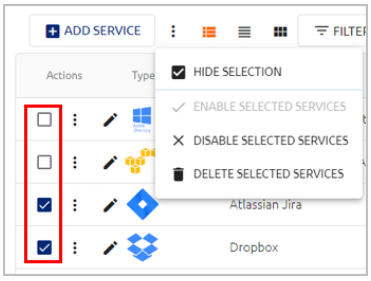
Performing actions on services

The following management operations are available directly from the Services list:

- **Select Services feature:** Clicking the ⋮ icon at the upper left corner of the Services list opens an actions menu from which you can enable / disable service selection.



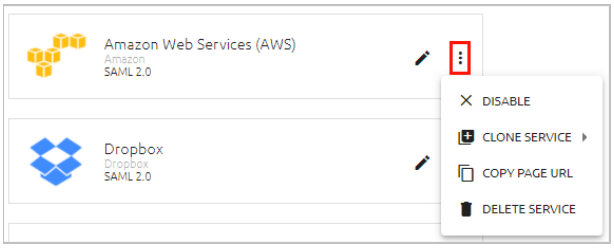
When you click **Select Services**, checkboxes appear next to each service, allowing you to select one or more services in the Services list. Once services are selected, you can disable them (if they are currently enabled), enable them (if they are currently disabled), or delete them from the system.



To hide the checkboxes and exit selection mode, click **Hide Selection**.

- **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.

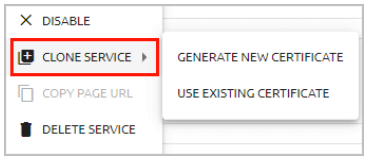
Cloning Services

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:

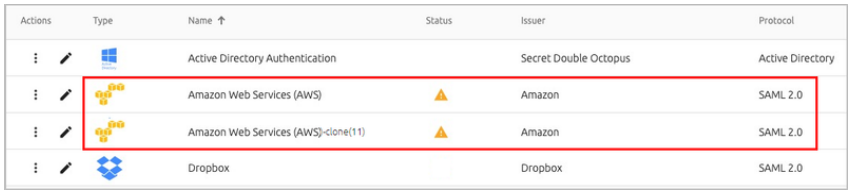
- URLs configured for the service (e.g., Endpoint URL, etc.) are regenerated. The new URLs contain a random UUID instead of the service number. Furthermore, in SAML services, the specific service name no longer appears in the URL path (only *saml* is used).
- In LDAP and RADIUS services, the **Port** 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 like 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.



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 Secret Double Octopus 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 is 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.

Creating a service and assigning users

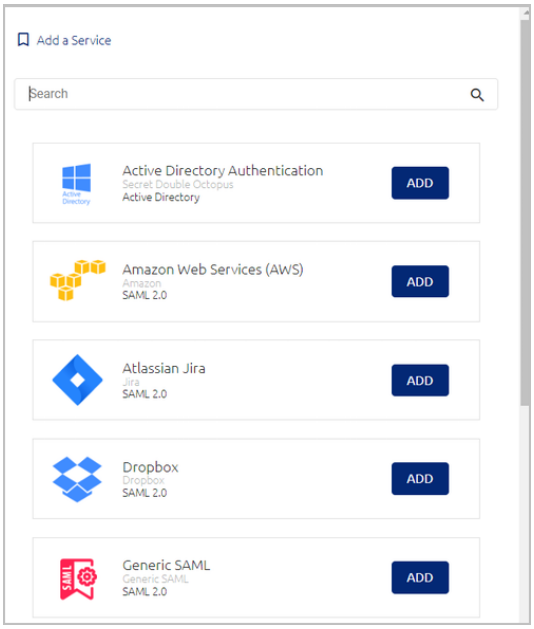
Although each service integrated with the Management Console has its own parameters and sign-on details, the processes of creating a service and assigning users are the same for every service you add. The following sections explain these processes in detail.

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**.



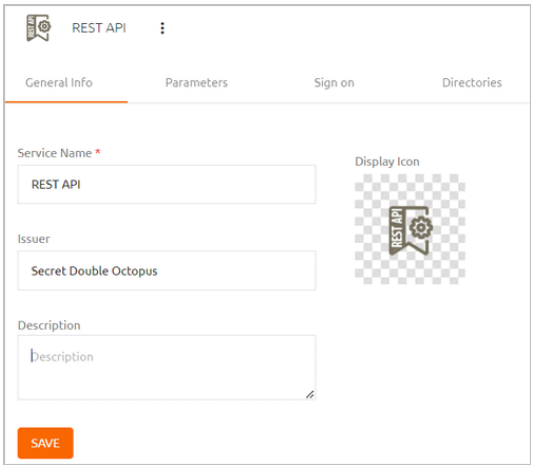
A dialog opens displaying a default name, issuer and display icon for the service.

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 488x488 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.



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.

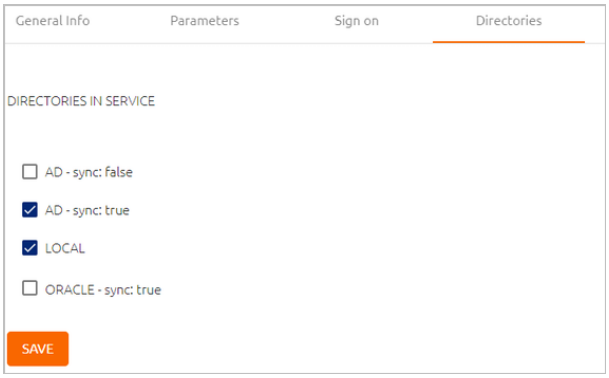
The following procedure explains how to assign directories and users from the service settings.

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:

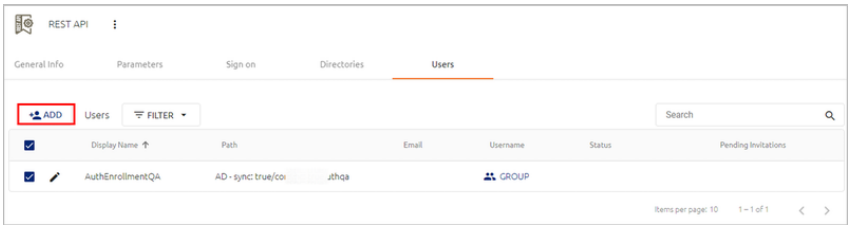
1. Open the settings of the relevant service and select the **Directories** tab. Select the checkboxes of the directories that you want to integrate with the service, and then click **Save**.



Important

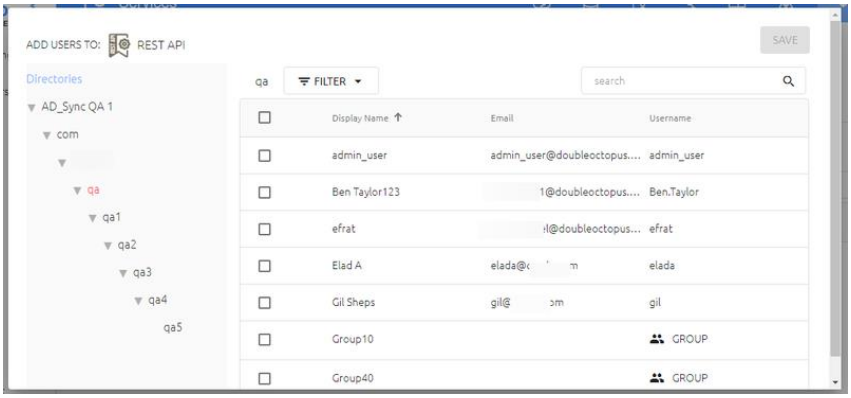
Only ONE directory may be selected for integration with LDAP services.

2. After selecting directories, open the **Users** tab and click **Add**.



The **Add Users To** popup opens. A list of directories integrated with the Management Console appears on the left side of the popup.

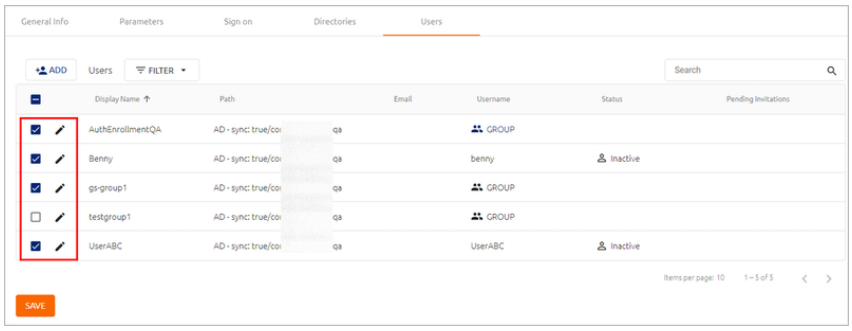
3. Open the directories tree and select the checkboxes of the users and Groups that you want to add to the service.



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.

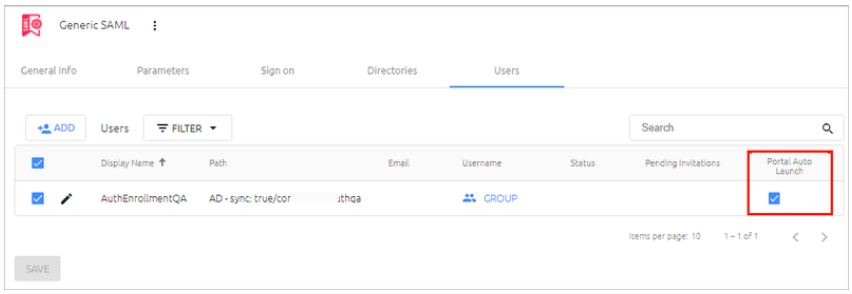
After assigning users to a service, you can manage them directly from the **Users** tab. To enable or disable the service for a specific user, toggle the checkbox on the left side of the row. Clicking the Edit icon next to the checkbox opens the individual settings for that user (Viewing and Updating User Details).



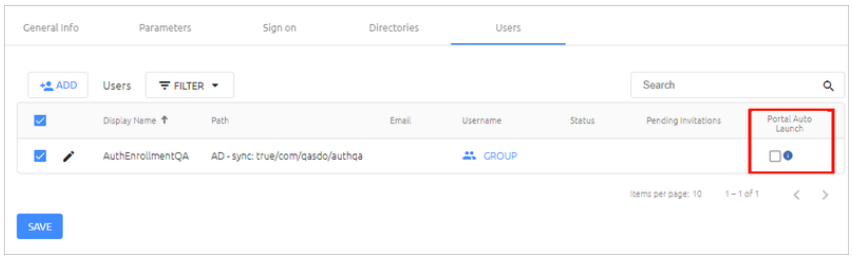
Portal Auto Launch

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.



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 group, but it is enabled in the service settings.



To configure the Automatic Launch setting for a group or user, select or clear the **Portal Auto Launch** checkbox, and then click **Save**.

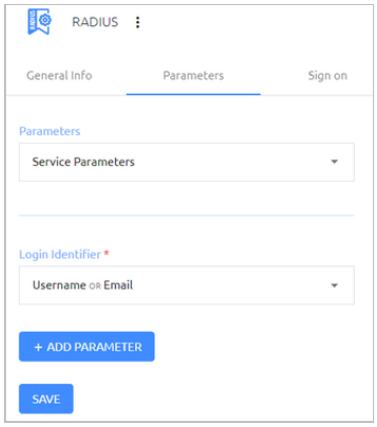
> **Note**
>
> To configure Automatic Launch, **SSO** must be enabled in the SAML service settings. If SSO is not selected in the service settings, the **Portal Auto Launch** checkbox is disabled.

Configuring RADIUS services

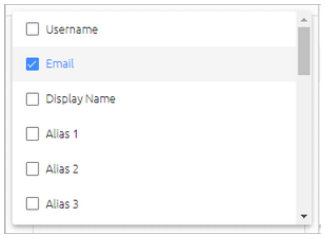
The following sections explain the parameters and sign on settings that you need to configure when adding a RADIUS service.

RADIUS Parameters

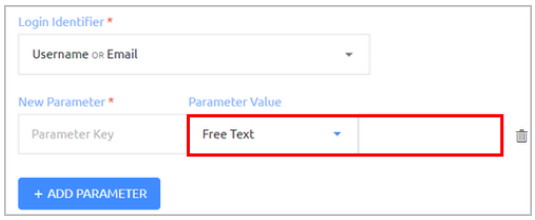
Parameters are settings of the RADIUS service that the Management Console requires for successful integration. To view and update these values, open the settings for the relevant RADIUS service and select the **Parameters** tab.



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), click the field 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).

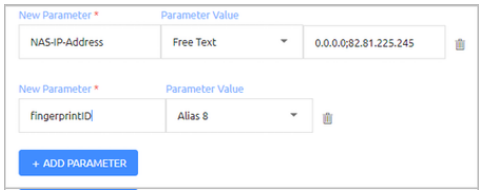


The following additional parameter is commonly configured for RADIUS services:

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

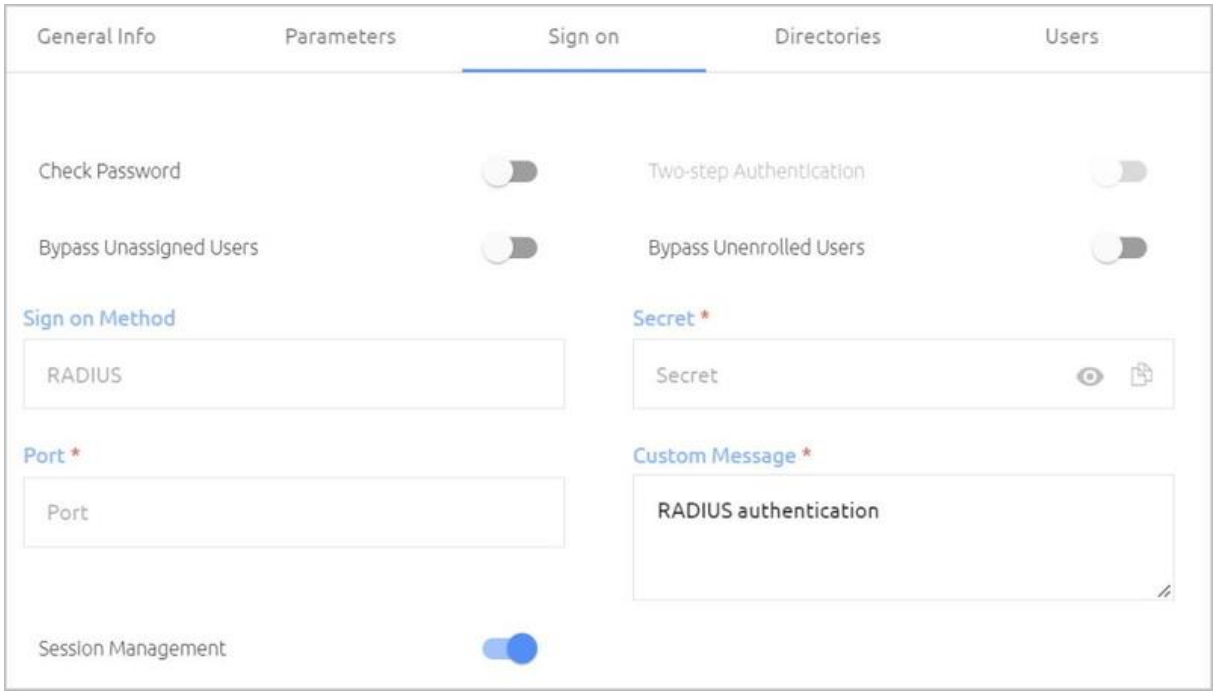
When multiple values are specified within a single parameter, the values have an *OR* relationship. However, multiple parameters are handled with *AND* logic, so all parameters must be matched for successful authentication. In the example below, the RADIUS client needs to send one of the specified IP addresses as well as a matching fingerprint.



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 provides 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.



Setting	Description / Notes
Check Password	When enabled, users are required to enter a password for MFA authentication.
Two-step Authentication	This option is available when the **Check Password** setting is active. When two-step authentication is enabled, users first enter their credentials, and then enter the one-time code in a separate step. By default, two-step authentication is not enabled, and users enter both credentials and the code in the same field.
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).
Secret	The RADIUS secret key required for communication between the RADIUS service and Octopus Authenticator. 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:

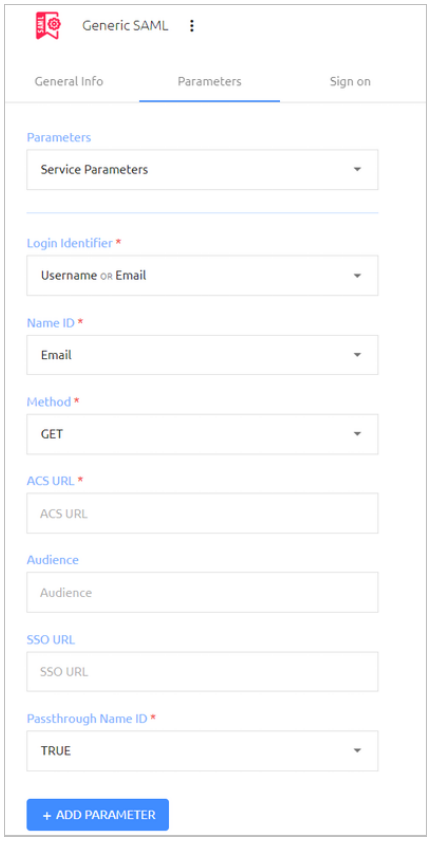
- Replace the RADIUS Server URL with *<EnterpriseBaseURL>:<port>*
  - **Enterprise Base URL:** The address of the Octopus Authentication Server (or the load balancer in distributed deployments). The URL is displayed in the Management Console under **System Settings > General Settings**.
  - **Port:** The port defined in the **Sign on** tab of the Octopus RADIUS service.

Configuring 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.



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: • **GET:** Login starts from the Octopus Login page and then authenticates to the service directly. • **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.

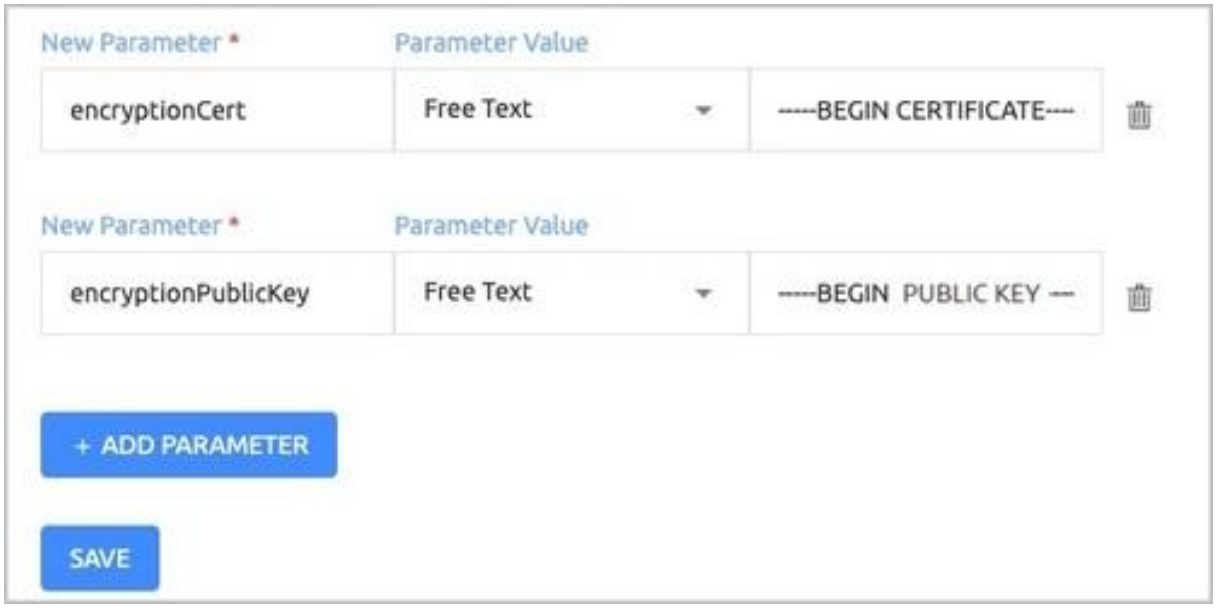
The following are optional parameters that are commonly added for generic SAML services:

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>*
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. 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. **Important:** When using this parameter, the **Check Password** and **Force Login Page** options (on the **Sign on** tab) need to be enabled.

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



The following parameters support sending username and password in the SAML assertion:

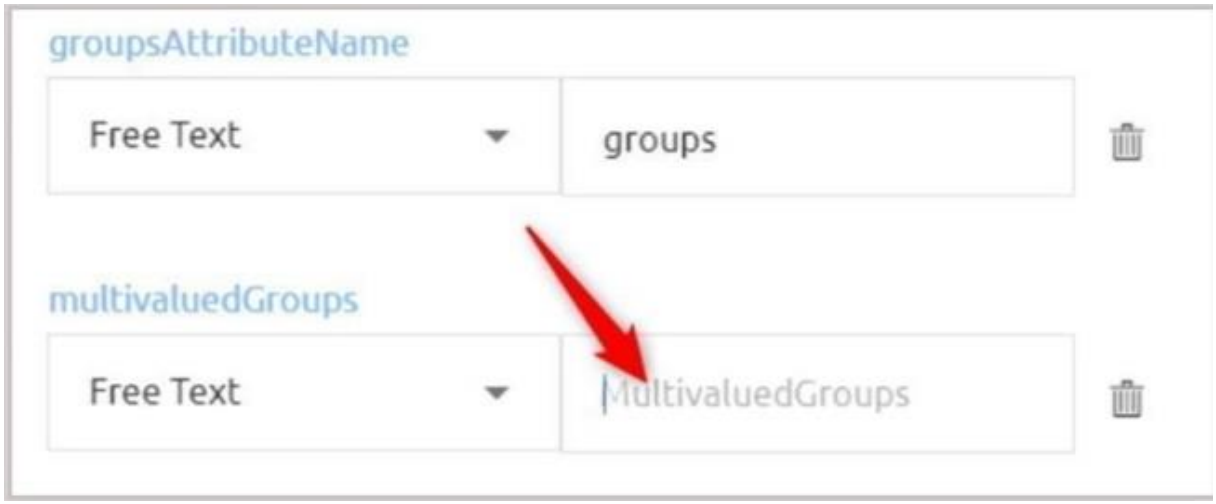
Parameter	Value	Description
username	Can point to any value from the user object (username, alias, etc.)	Returns the value in the SAML assertion.
password	Any value	When this parameter exists, the password is sent from the vault.
encodePassword	Any value	When this parameter exists, the password is Base64 encoded.

Note: This parameter is relevant only when *password* is set.	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.

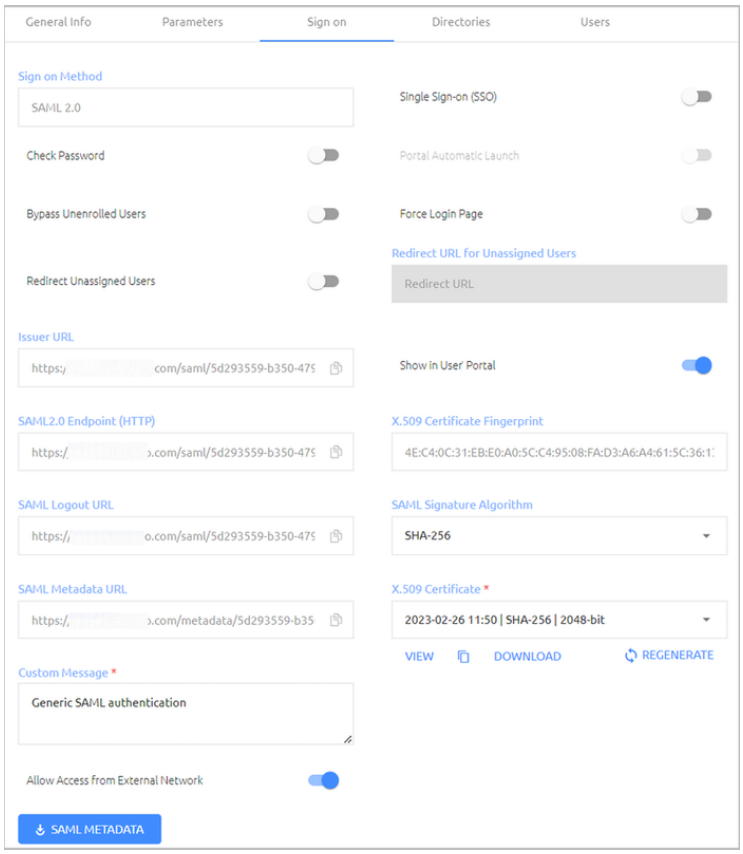
Parameter	Value	Description
groupsAttributeName	*roles*, *memberof*, or *groups*	Name of the attribute in the SAML schema containing a user's groups. When the parameter is set, user groups are sent as part of the SAML response.
multivaluedGroups	Empty or any value	This optional parameter sets the format 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.
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.



Generic SAML service sign on settings

The sign on settings provides 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.



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
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.	Yes

	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.	
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. 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.) **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. **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
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**.	Yes
X.509 Certificate	The public certificate used by the service to authenticate with Octopus Authenticator. The following options are available: • Click **View** to display the content of the certificate in a popup window. The popup provides both Copy and Download options. • Click **Download** to download the certificate as a .PEM file that can be used by the service. • 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). **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 REST API services

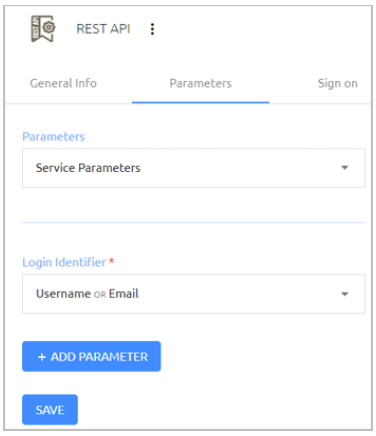
The following sections explain the parameters and sign on settings that you need to configure when adding a REST API service.

REST API Service Parameters

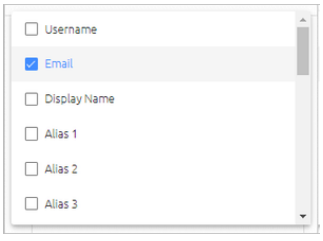
Parameters are settings of the REST API service that the Management Console requires for successful integration.

To view and update REST API service parameters:

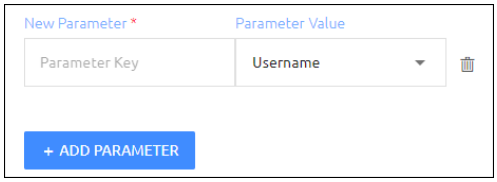
1. Open the settings for the relevant REST API service and select the **Parameters** tab.



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), click the field 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.

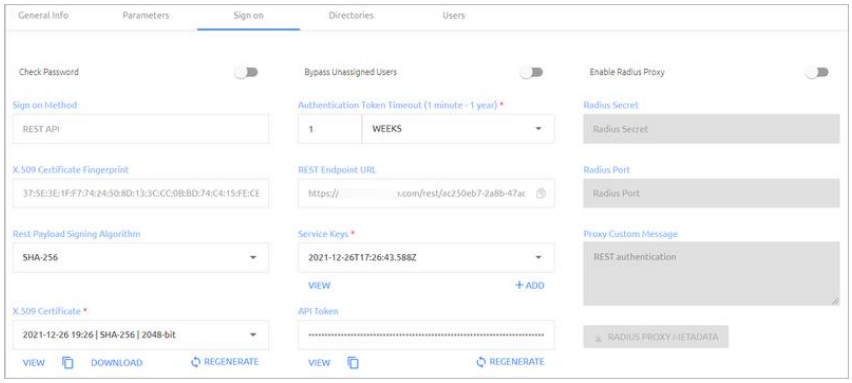


4. Click **Save**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

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.

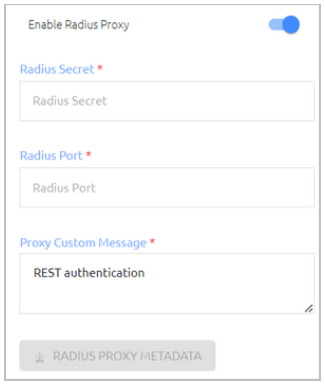


Setting	Description / Notes	Configurable?
Check Password	When enabled, a password is required for authentication (in addition to the authentication methods used by Octopus Authenticator)	Yes
Bypass Unassigned Users	When this toggle is enabled, users who are not assigned to the service will be allowed 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

Rest Payload Signing Algorithm	The signature of the generated X.509 certificate. Select **SHA-1** or **SHA-256**.	Yes
X.509 Certificate	The public certificate used by the service to authenticate with Octopus Authenticator. The following options are available: • Click **View** to display the content of the certificate in a popup window. The popup provides both Copy and Download options. • Click **Download** to download the certificate as a .PEM file that can be used by the service. • 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: • Click **View** to open a popup from which you can view and copy all active service keys. • Click **Add** to create a new service key. For more information, refer to Working with Service Keys.	Yes
API Token	The token used for an authentication request. The following options are available: • Click **View** to display the content of the token in a popup window. The **Copy** button lets you easily copy the content. • 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.



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).

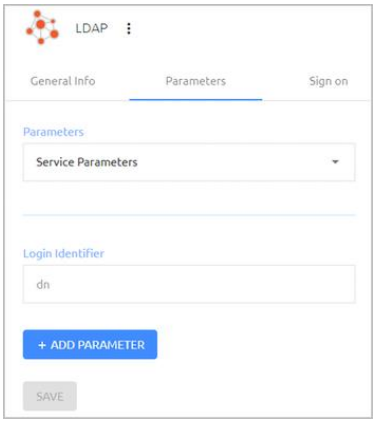
The following sections describe the parameters and sign on settings for the Octopus LDAP service and explain how to configure your external LDAP service for successful integration with the Octopus Server.

LDAP Parameters

Parameters are settings of the LDAP service that the Management Console requires for successful integration.

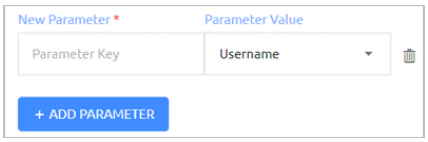
To view and update LDAP service parameters:

1. Open the settings for the relevant LDAP service and select the **Parameters** tab.



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.



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

Configuring Optional Client Connection Parameters

Secret Double Octopus 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 **Note:** This parameter is relevant only when	5000	Determines the time (in milliseconds) for which the LDAP connection remains open. When the	ldapClientTimeout: 5000

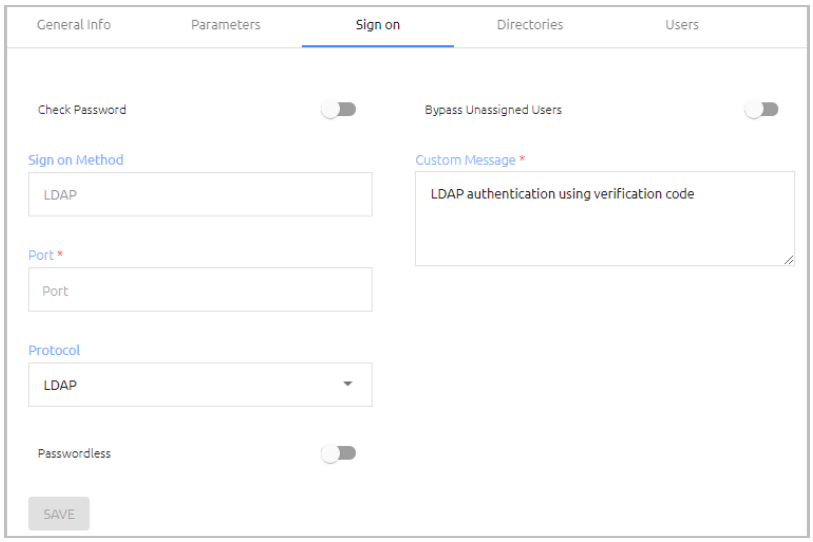
ldapOptimizationBypass is set to *false*.	timeout elapses, the connection is closed, a new client is created, and the operation is performed again on the new client.

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 provides 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.



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:

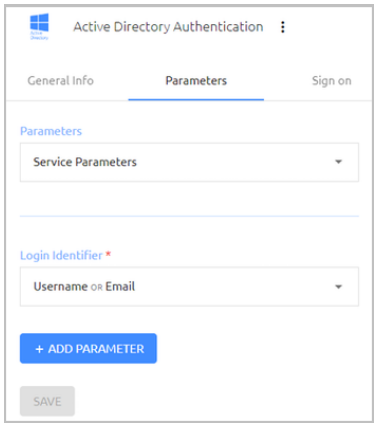
1. To redirect authentication requests to the Octopus Server, replace the LDAP Repository URL with *<EnterpriseBaseURL>:<port>*
   - **Enterprise Base URL:** The address of the Octopus Authentication Server (or the load balancer in distributed deployments). The URL is displayed in the Management Console 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

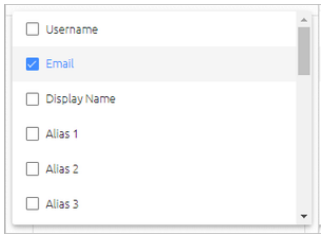
The following sections explain the parameters and sign on settings that you need to configure when adding an Active Directory Authentication service.

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.

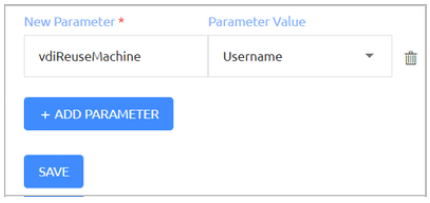


The **Login Identifier** is the identifier that the user needs to enter in order to log into the AD Authentication service (e.g., Username). You can configure multiple identifier types to support various platforms. To specify the identifier(s), click the field and select the relevant checkbox(es).



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.



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

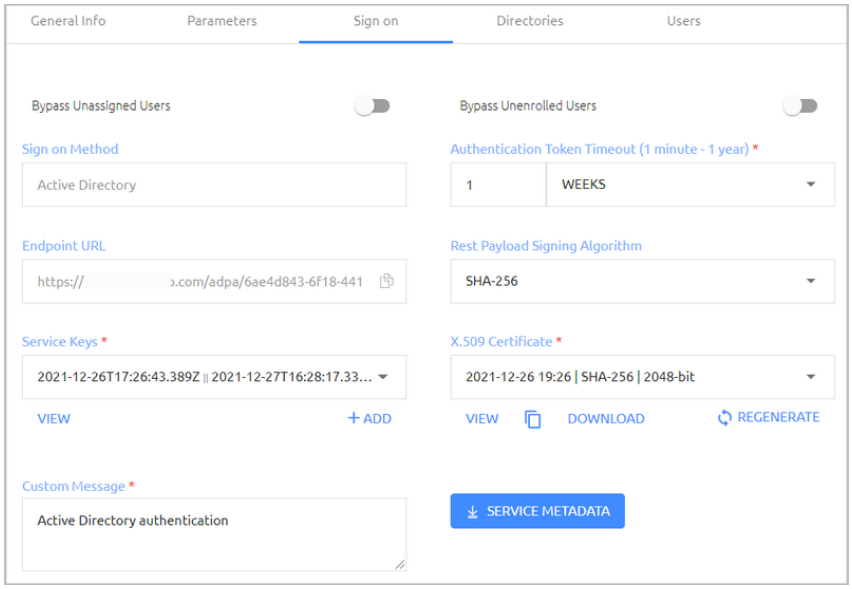
AD Authentication Service sign on settings

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.

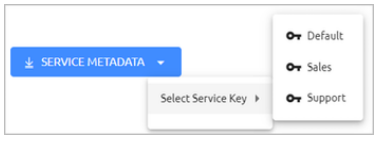
After updating settings, scroll to the bottom of the tab and click **Save**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.



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
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

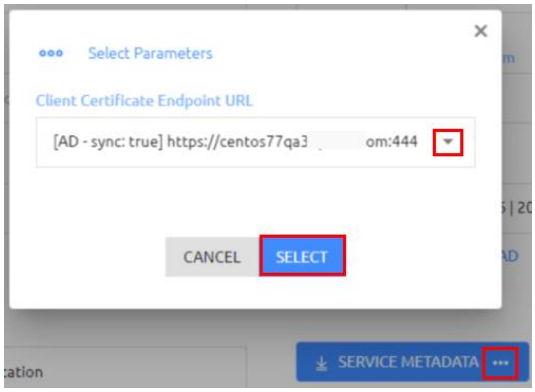
Service Keys	The key(s) used by the service to authenticate with Octopus Authenticator. The following options are available: • Click **View** to open a popup from which you can view and copy all active service keys. • Click **Add** to create a new service key. For more information, refer to Working with 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**.	Yes
X.509 Certificate	The public certificate used by the service to authenticate with Octopus Authenticator. The following options are available: • Click **View** to display the content of the certificate in a popup window. The popup provides both Copy and Download options. • Click **Download** to download the certificate as a .PEM file that can be used by the service. • 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

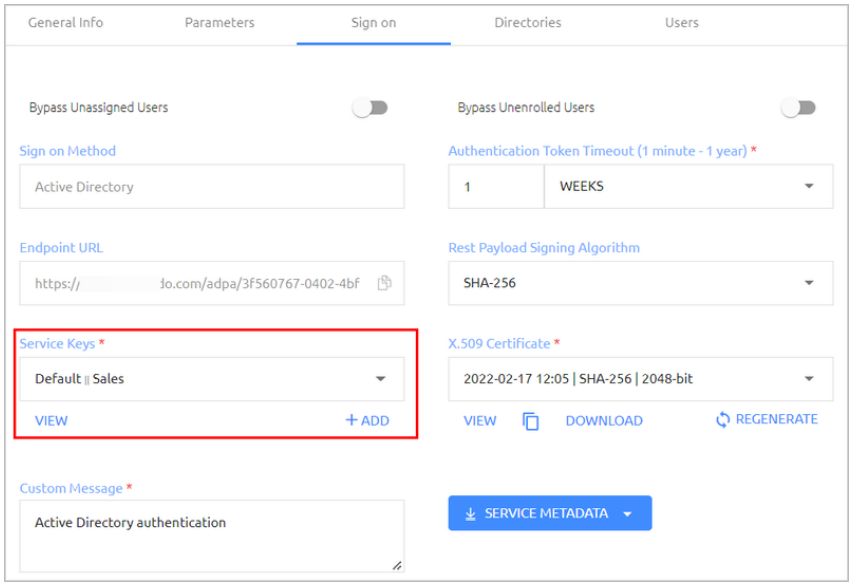
Service Metadata button. To specify which certificate will be included in the XML file, click the icon, choose the required certificate from the list and then click **SELECT**.



Working with service keys

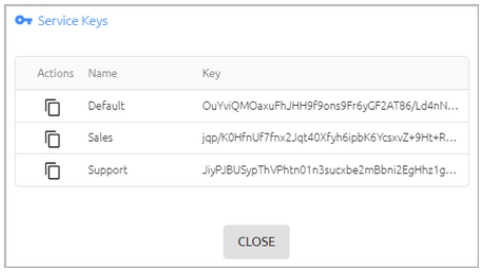
Active Directory Authentication services and REST API services can support multiple service keys for authentication. You can add as many keys as necessary and use each of them for different Windows / Mac credential provider configurations.

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**.

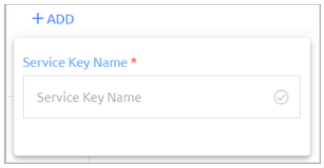


To view all defined service keys, click to open the list. Active service keys are indicated by a selected checkbox. (At least one key must be active.) Inactive keys cannot be included in service metadata and cannot be used for authentication.

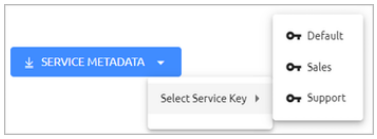
Clicking **VIEW** opens a popup from which you can view and copy all active service keys.



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.



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.

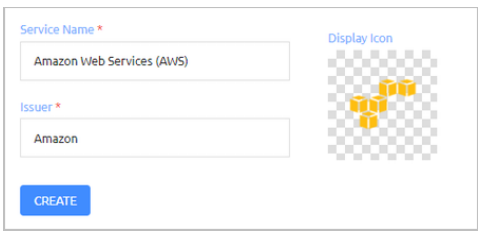


Configuring Amazon Web Service integration

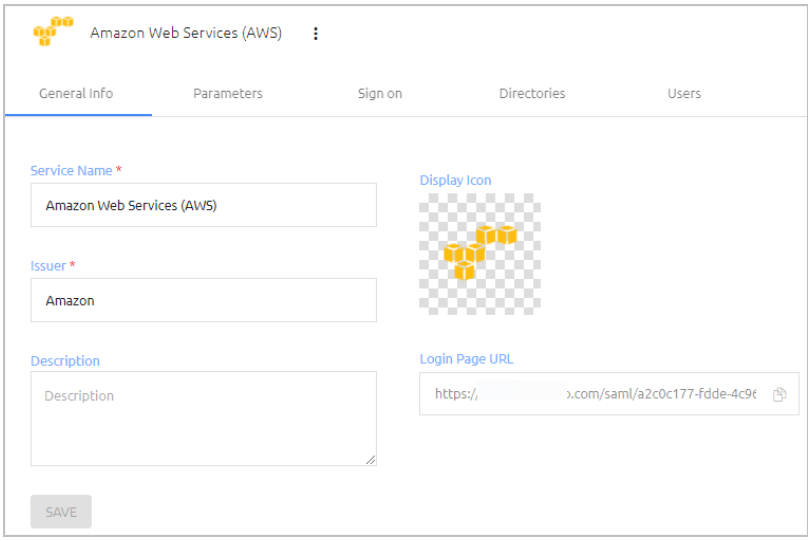
The AWS SAML service enables SAML 2.0 integration between the Octopus Authenticator and Amazon Web Services. For successful integration, you need to create the service in the Management Console and configure the appropriate third-party Identity Provider and Role in your AWS account. The following procedure 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 488x488 pixels). Then, click **Create**.

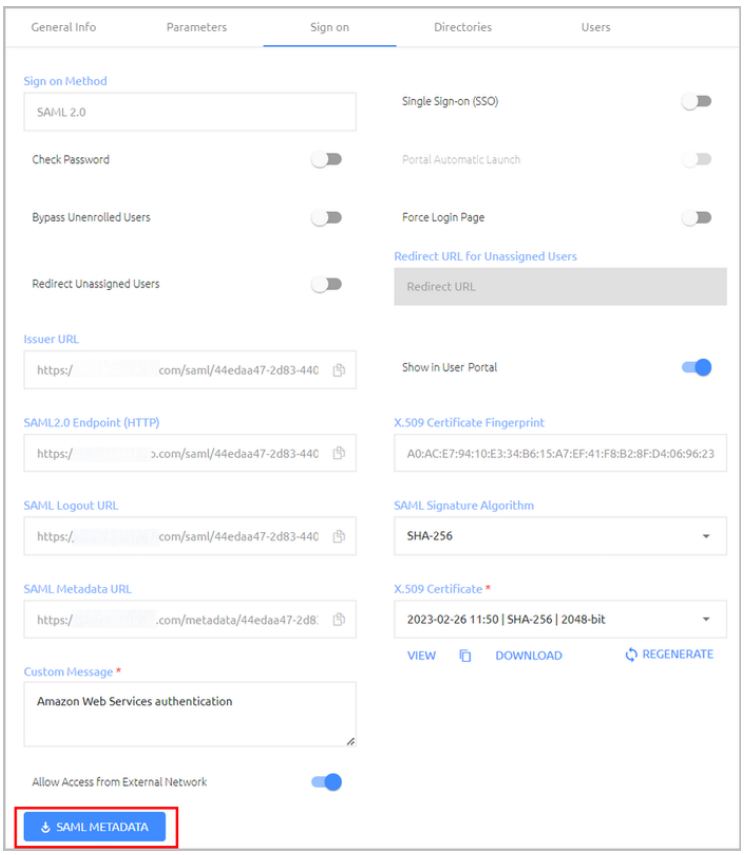


3. Review the settings in the **General Info** tab. If you add a description or update other settings, click **Save**.



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.

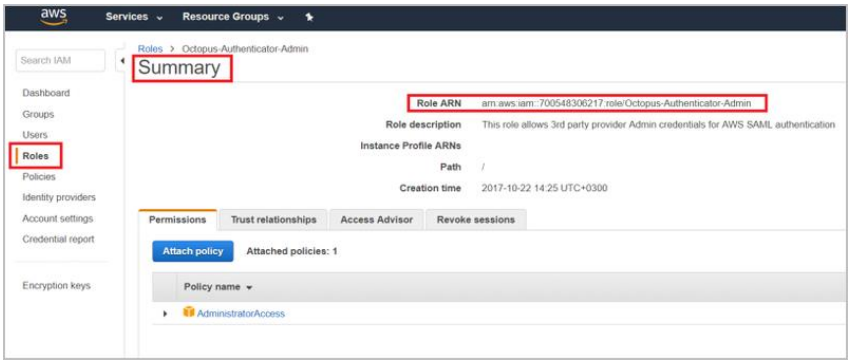


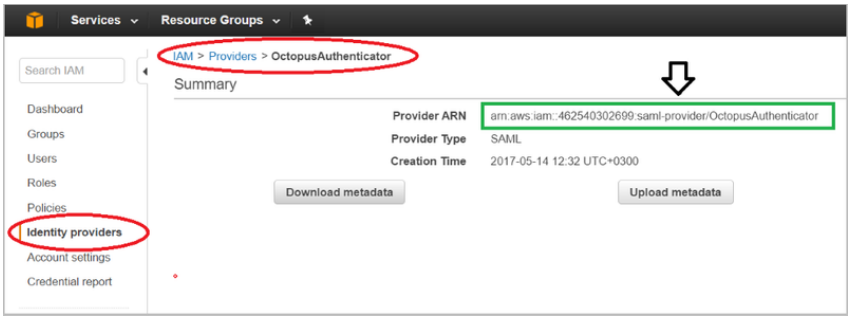
6. Log into your AWS account and perform these procedures:

   - 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.

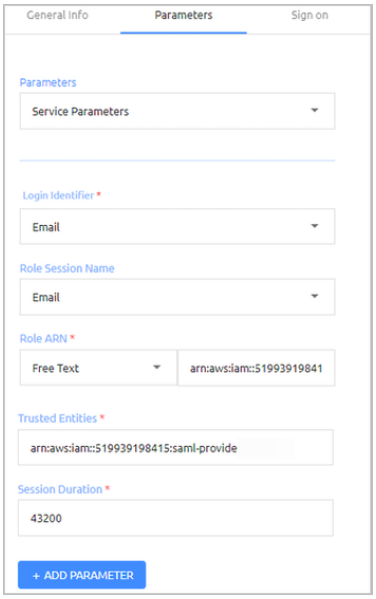
   After completing the procedures, you will have an **AWS Role ARN** and an **AWS Provider ARN**.





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 (in seconds) for which the console can be open before the session expires.



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.

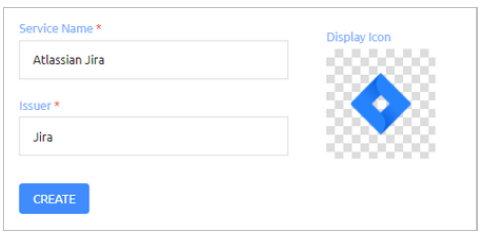
Configuring Atlassian Jira service integration

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.

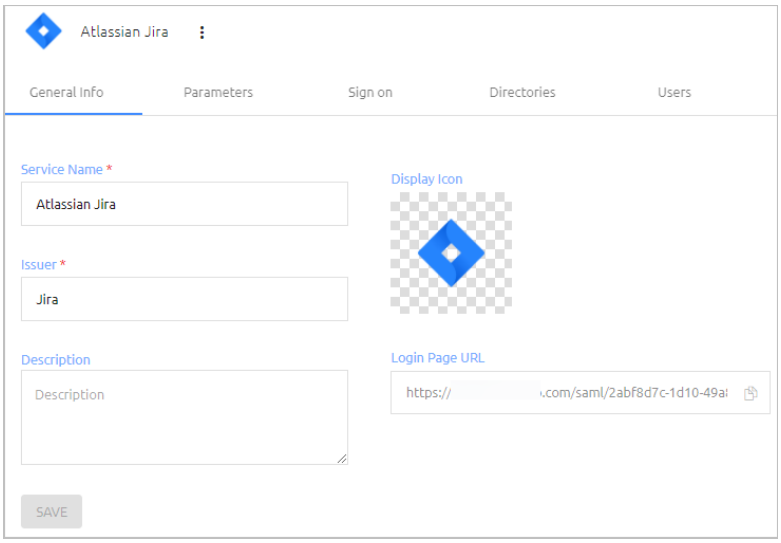
To configure Jira integration:

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 488x488 pixels). Then, click **Create**.



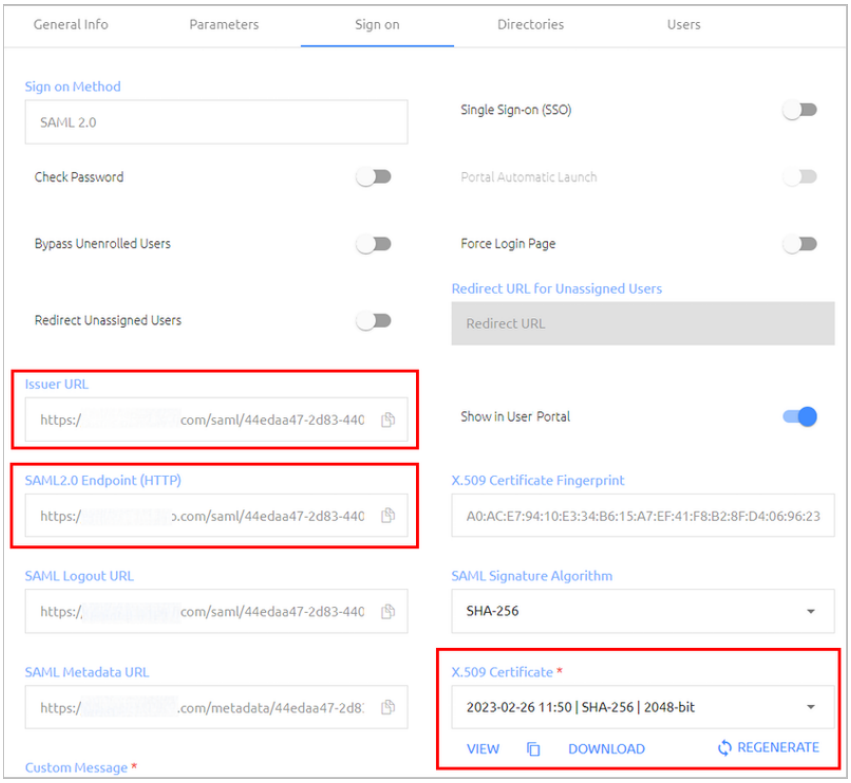
3. Review the settings in the **General Info** tab. If you add a description or update other settings, click **Save**.



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:

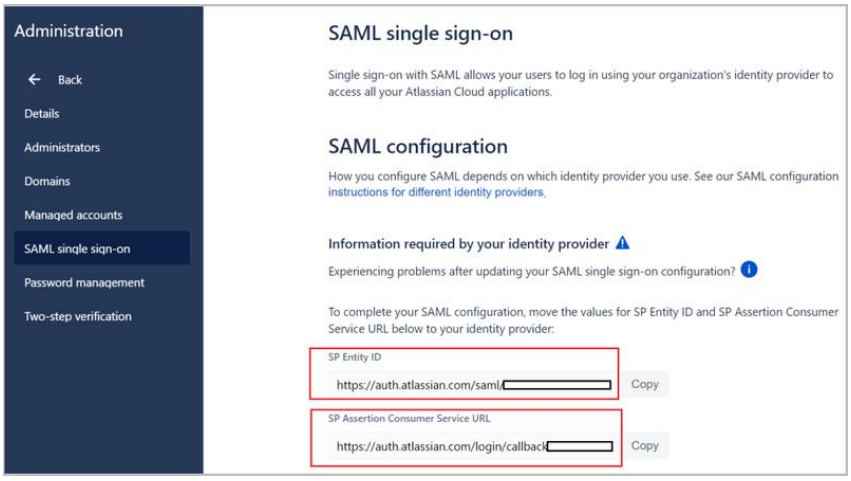
   - **Issuer URL:** The URL used by the Jira service to connect to Octopus Authenticator. Click the Copy icon to copy the URL.
   - **SAML2.0 Endpoint (HTTP):** The Octopus Authenticator Login page URL to which the Jira service provider will refer users for Octopus authentication. Click the Copy icon to copy the URL.
   - **X.509 Certificate:** Click **View**. Then, in the popup that opens, click **Copy** to copy the content of the certificate file.



You will need these elements to set up the SAML SSO configuration in your Atlassian account.

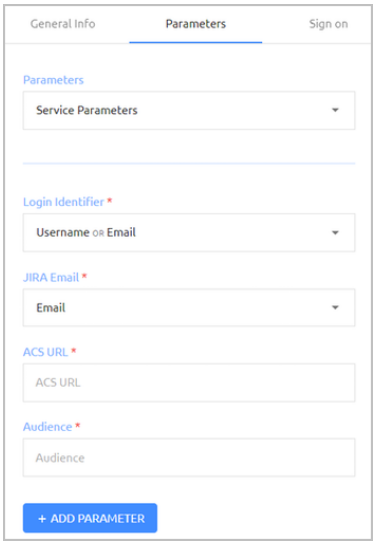
6. Log into your Atlassian account as an administrator and edit the settings of the SAML single sign-on configuration. For details, refer to the integration document: How to Configure Octopus Authentication for Jira Software.

   After completing the configuration, Jira SAML Single Sign-On parameters will be generated and displayed on the **SAML single sign-on** page.



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**.



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.

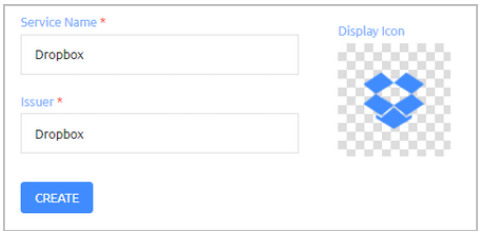
Configuring Dropbox service integration

The Dropbox SAML service enables SAML 2.0 integration between the Octopus Authenticator and the Dropbox web service. For successful integration, you need to create the service in the Octopus 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.

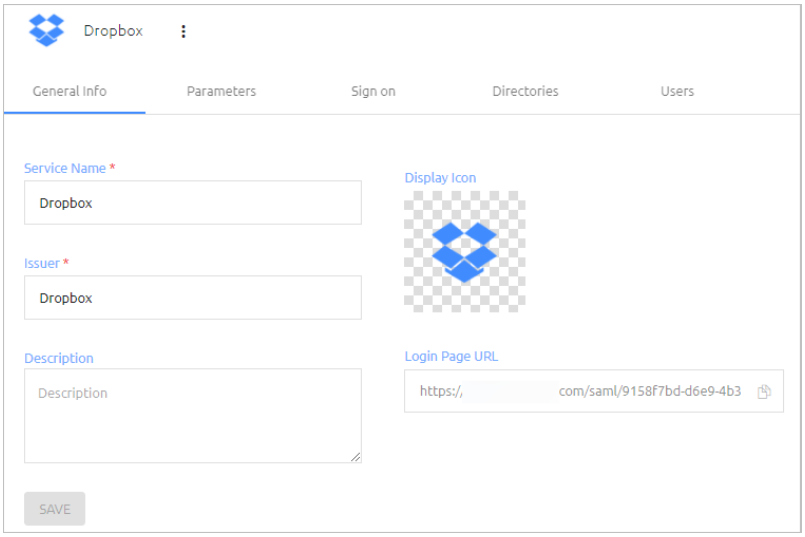
To configure Dropbox integration:

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 488x488 pixels). Then, click **Create**.



3. Review the settings in the **General Info** tab. If you add a description or update other settings, click **Save**.

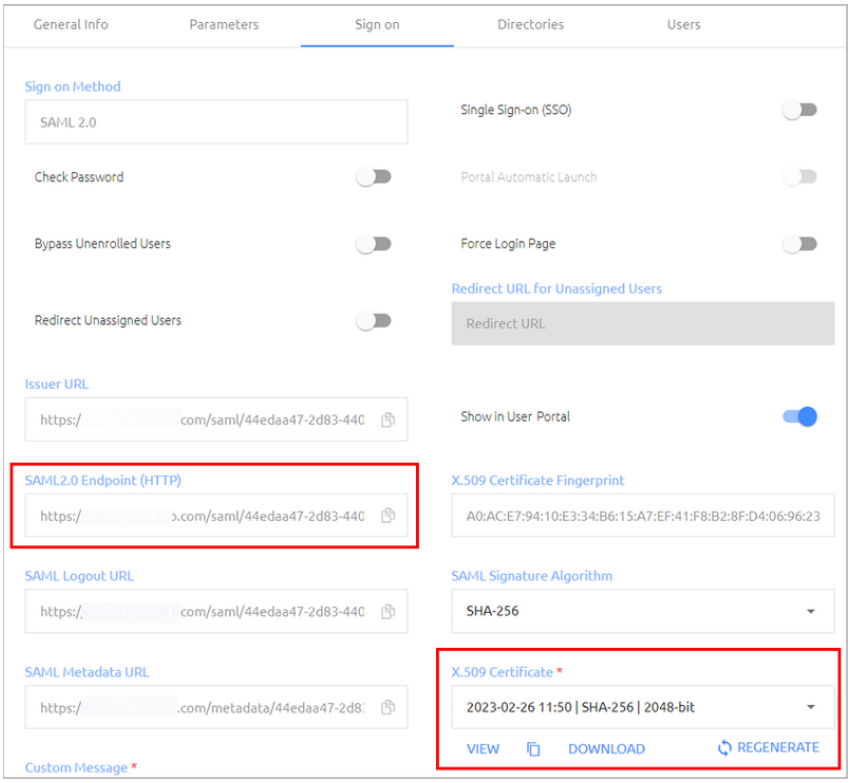


4. Add directories, users and groups to the service. For details, refer to Creating a Service and Assigning Users.

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.

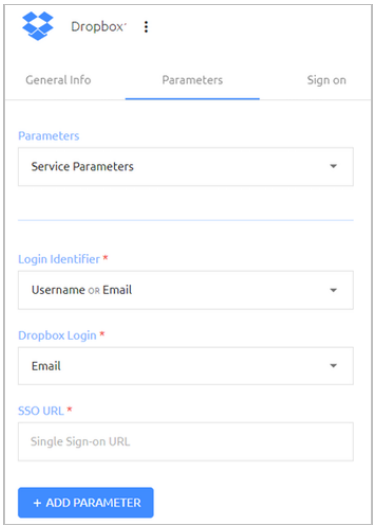


6. Log into your Dropbox Admin account. From the Admin Console Dashboard, set up the 3rd party IdP SSO.

   For details, refer to the integration document: How to Configure Octopus Authentication for Dropbox.

7. In the Octopus 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 Octopus 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 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. 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.

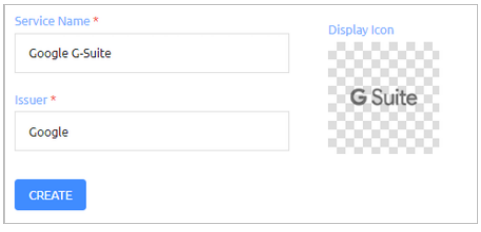
Configuring Google G Suite service integration

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 Octopus 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.

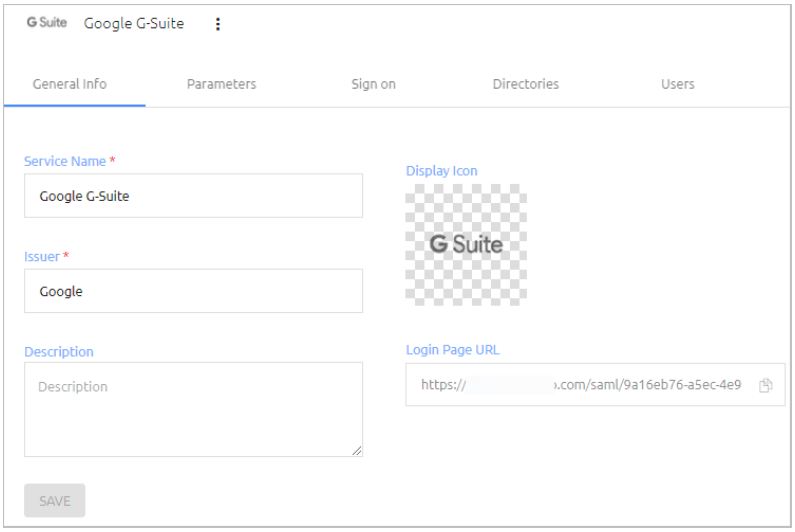
To configure Google G Suite integration:

1. In the Octopus 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 488x488 pixels). Then, click **Create**.



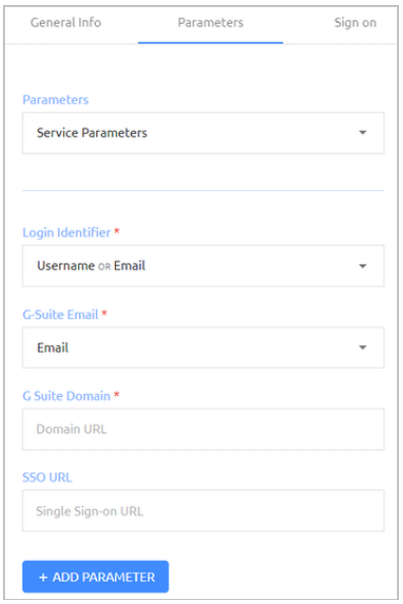
3. Review the settings in the **General Info** tab. If you add a description or update other settings, click **Save**.



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.

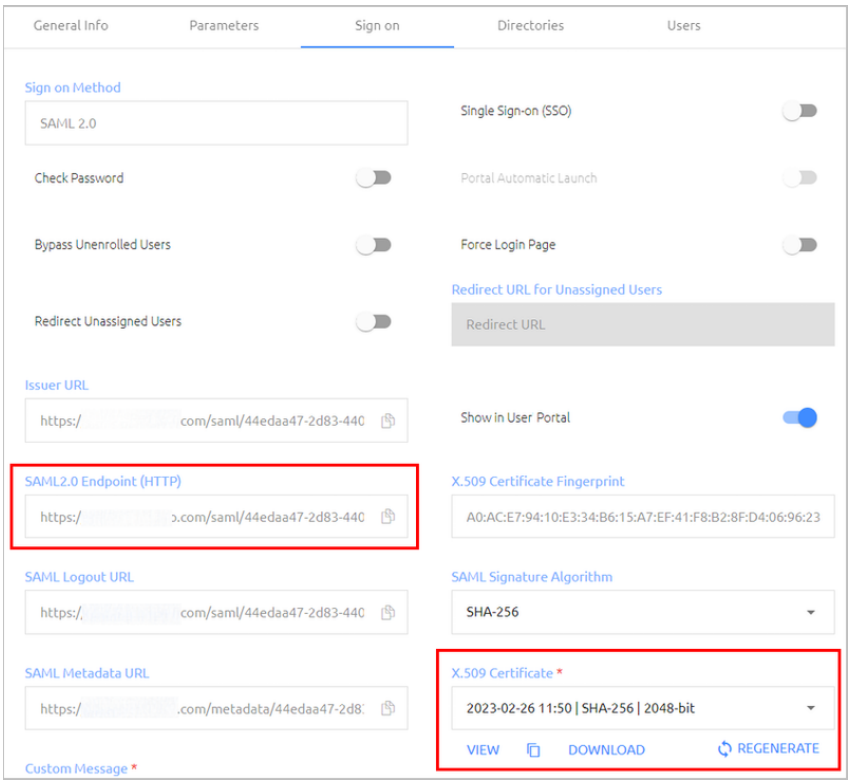
Setting	Value / Notes
Login Identifier	Login method for the Octopus Authentication Server (select **Email**).
G-Suite Email	Select **Email**.
G Suite Domain	Enter the domain URL.



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.



   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 Octopus 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.

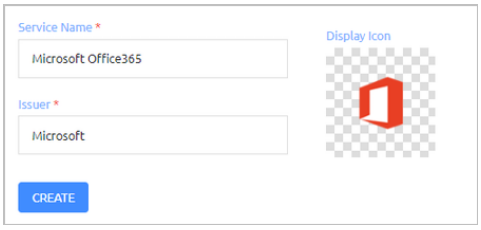
Important

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.

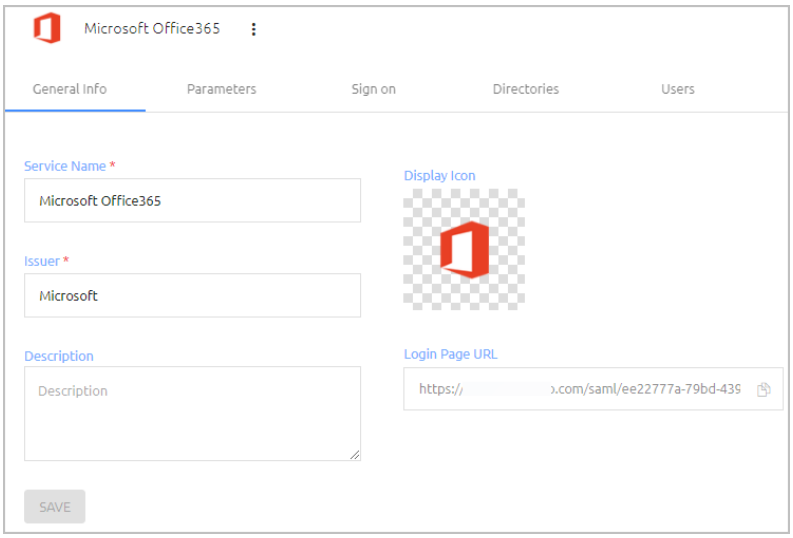
To configure Microsoft Office 365 integration:

1. In the Octopus 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 488x488 pixels). Then, click **Create**.



3. Review the settings in the **General Info** tab. If you add a description or update other settings, click **Save**.

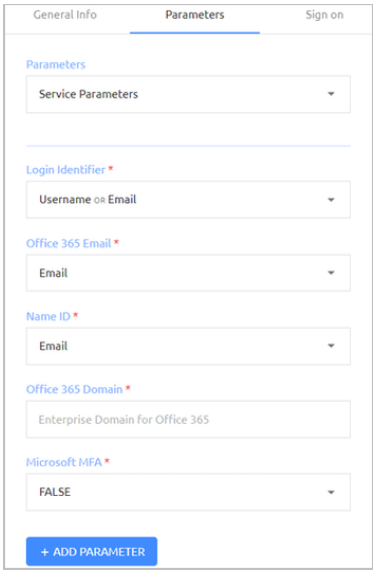


4. Add directories, users and groups to the service. For details, refer to Creating a Service and Assigning Users.

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**.

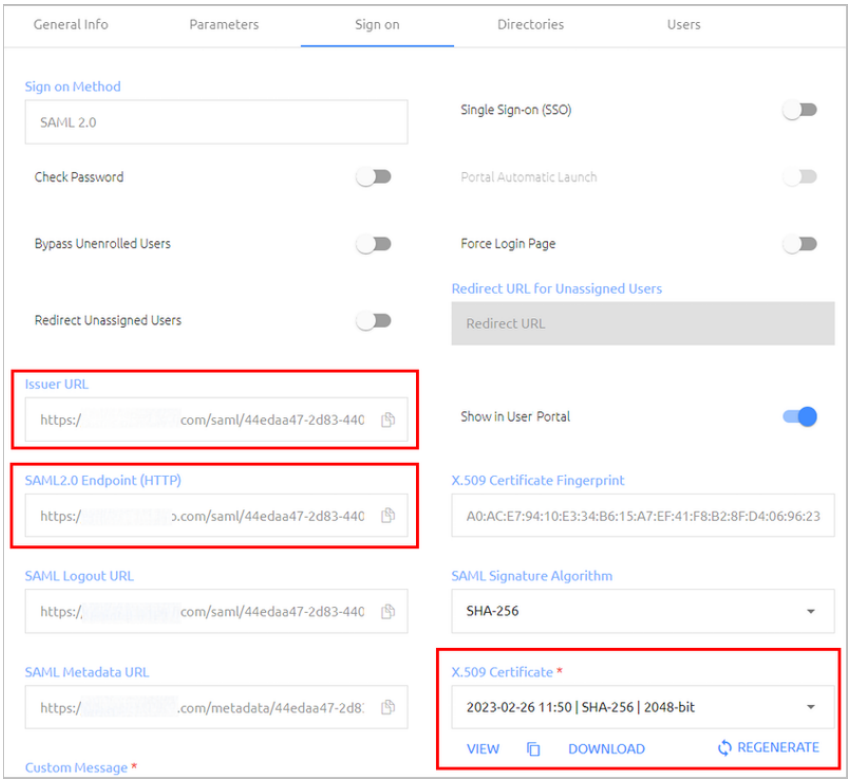
Name ID	Select **Alias 1**.
Office 365 Domain	Enter the Office 365 new Intermediary email domain.
Microsoft MFA	The default value is FALSE. When set to TRUE, after the user is successfully authenticated by Octopus Authenticator, Microsoft will request additional authentication on the Microsoft authenticator.



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.

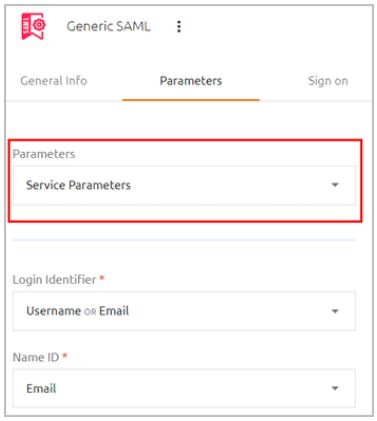


You will need these elements for the configurations in Office 365.

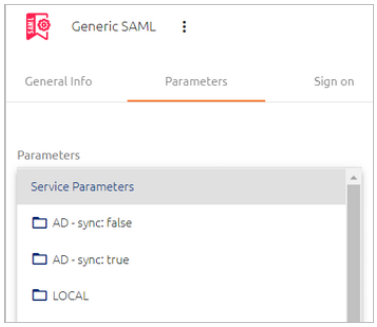
8. Set up SSO for the Office365 Web Service and the Mobile Outlook App using Octopus Authenticator as a third party IDP. For details, refer to the integration document: How to Configure Octopus Authentication for Microsoft Office 365.

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.



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:

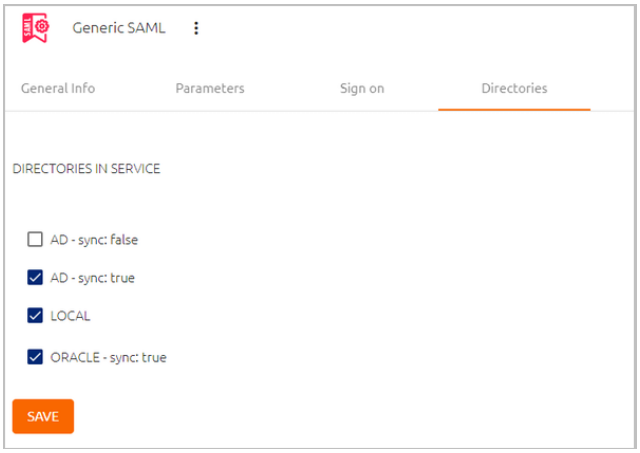
1. Open the settings of the relevant service. From the **Parameters** tab, open the **Service Parameters** dropdown list and check whether the directory for which you want to set override parameters is enabled.

   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**.

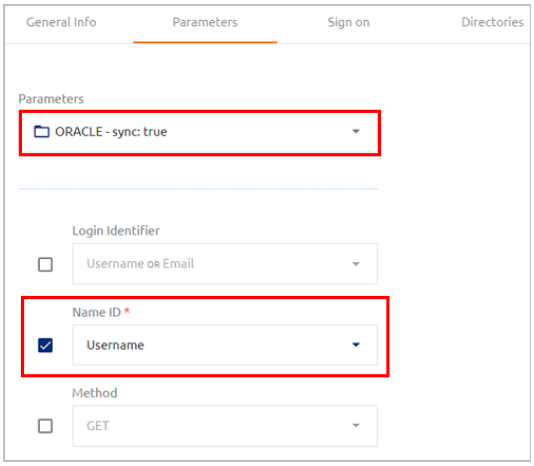
   

   In the **Parameters** tab, the selected directories will now be enabled.

4. From the **Service Parameters** list, select the relevant directory.

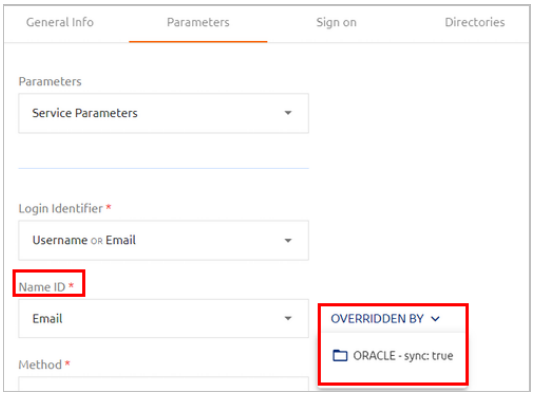
   A list of parameters is displayed.

5. To override a parameter, select its checkbox and then specify its value.



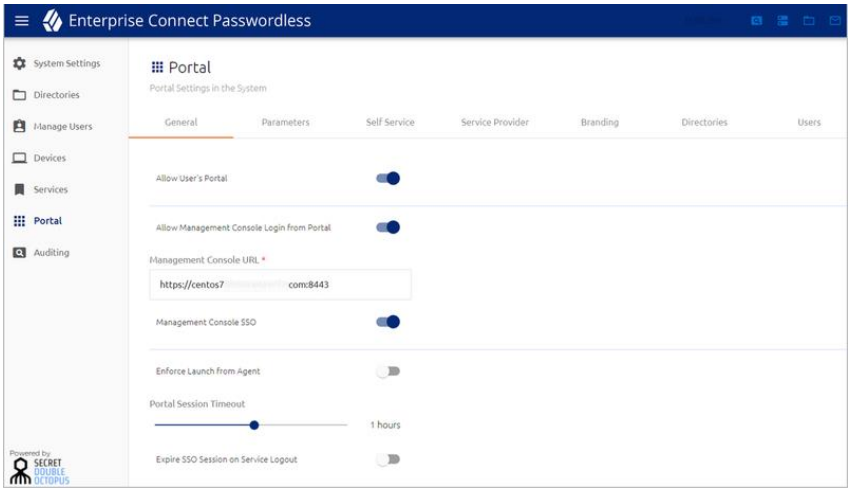
6. At the bottom of the tab, click **Save**. Then, from the toolbar at the top of the page, click **PUBLISH** and publish your changes.

   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.

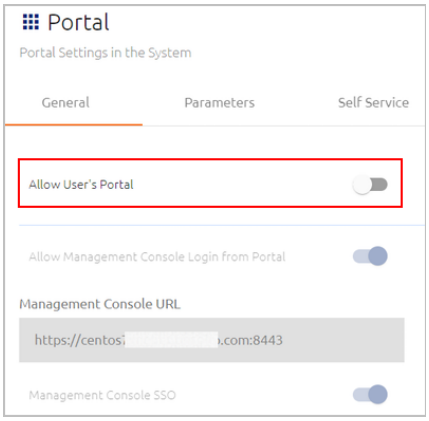


Managing settings for the user portal

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.



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.



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

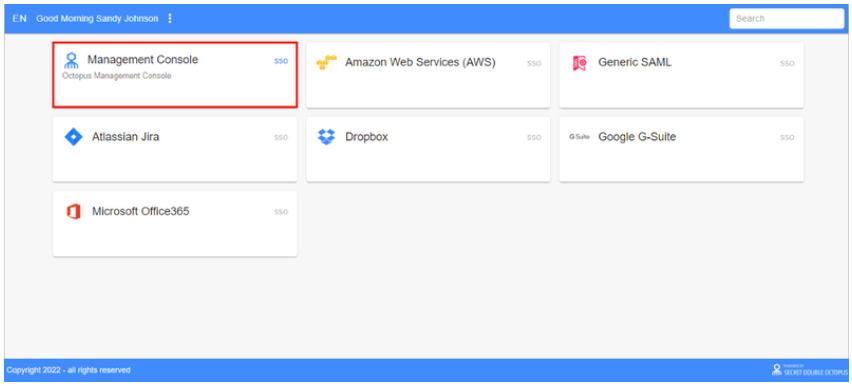
User portal general settings

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.

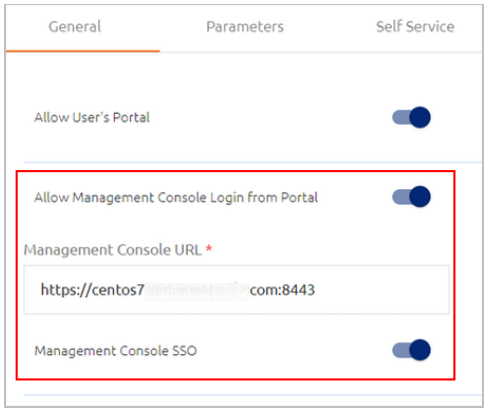
Management Console Access Settings

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.



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.

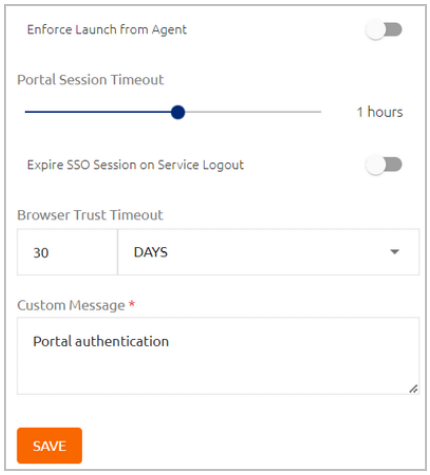


Portal Security and Authentication Settings

The following settings appear at the bottom of the **General** tab:

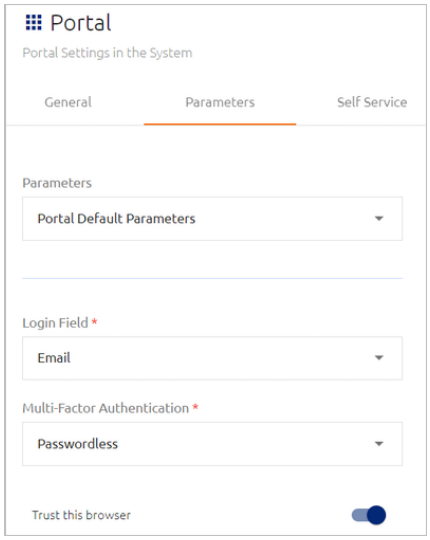
- **Enforce Launch from Agent:** When this setting is enabled, the Portal can be accessed only from the user's workstation, via the Windows / Mac Agent. (Manual Portal login through a browser is disabled.)
- **Portal Session Timeout:** Determines the maximum length of a User Portal session. The session 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.



Setting user portal parameters

The **Parameters** tab contains settings related to the process of authenticating to the User Portal.



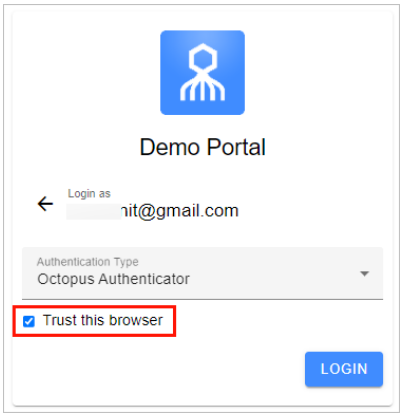
The settings are:

- **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.

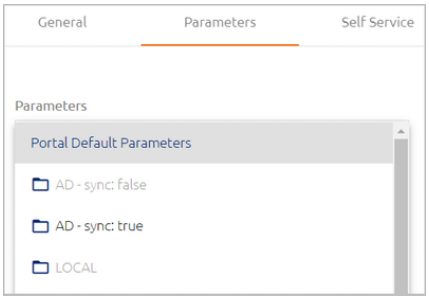
Note

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 this browser:** 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.)



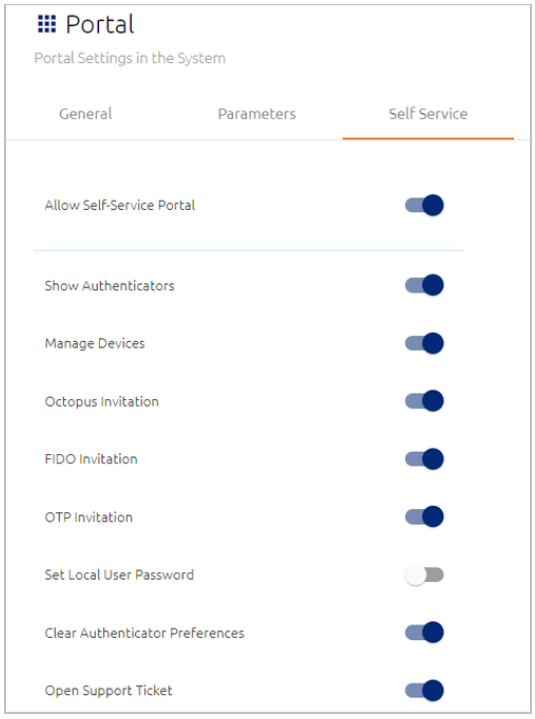
The **Parameters** dropdown list at the top of the tab enables you to define directory-specific parameters that override the Portal default parameters.



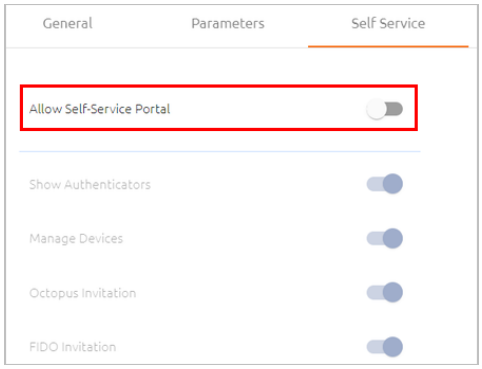
For more details and instructions for overriding parameters, refer to Overriding Default Service Parameters.

Managing user portal self-service settings

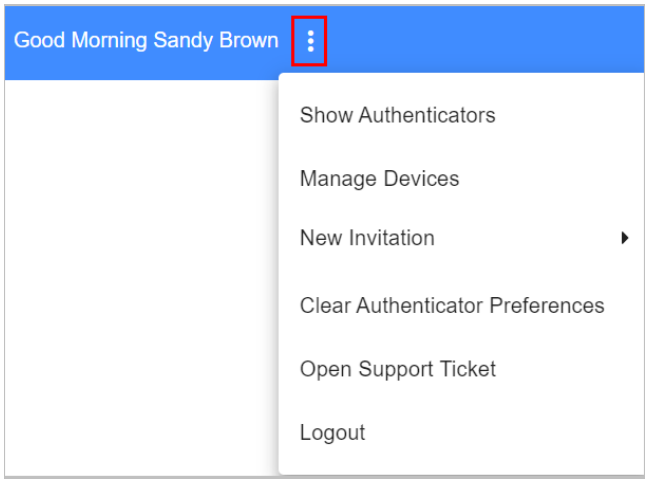
The **Self Service** tab contains settings that determine which self-service actions are available in the User Portal. Actions are enabled and disabled by clicking the relevant toggle buttons.



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.

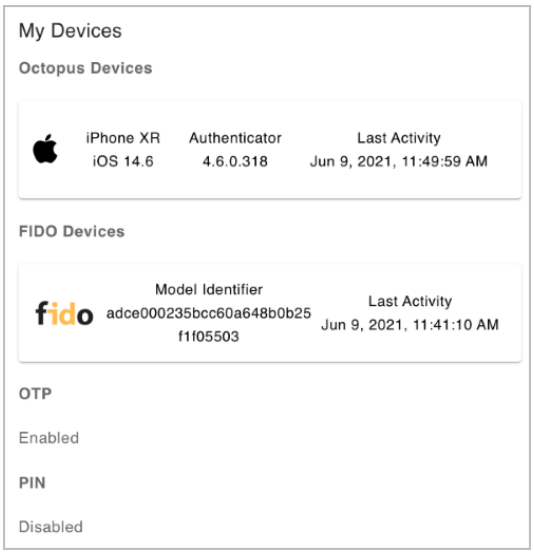


When the **Allow Self-Service Portal** setting is on, the actions that are currently activated in the **Self Service** tab are displayed to users when they click the Actions icon of the User Portal.

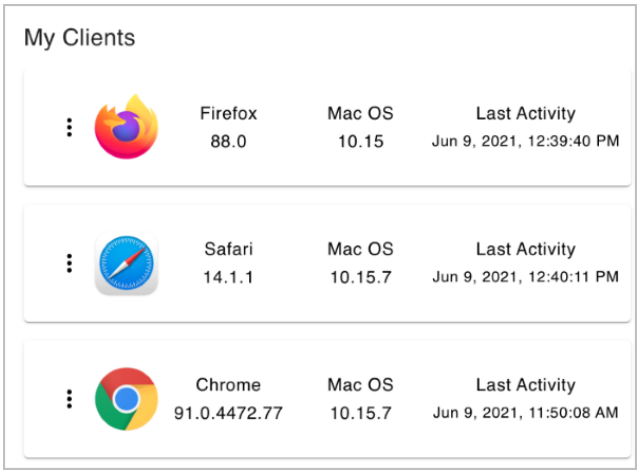


The self-service actions are:

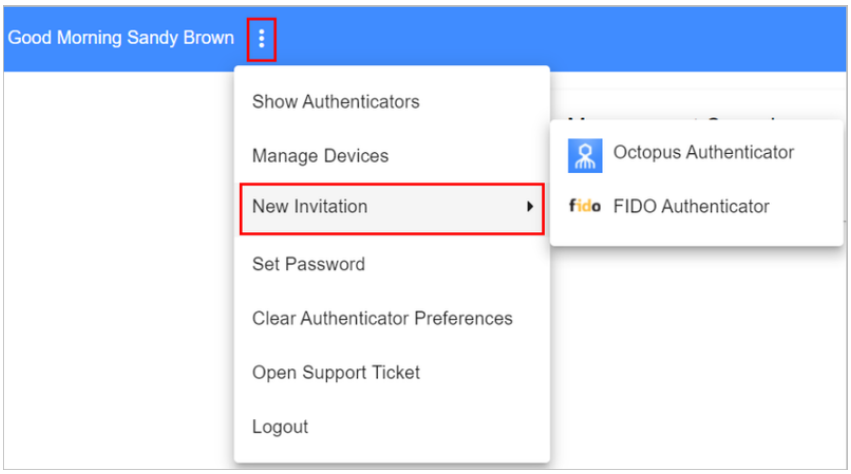
- **Show Authenticators:** When this setting is enabled, users can open a popup displaying basic information about all the devices they have used for authentication.



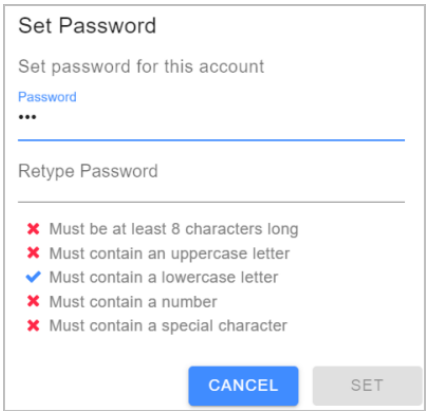
- **Manage Devices:** When this setting is enabled, users can view a popup displaying basic information about all the browsers they have used for authentication. Users can remove the browser from the list by clicking the Actions icon and selecting **Delete**.



- **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 OTP).

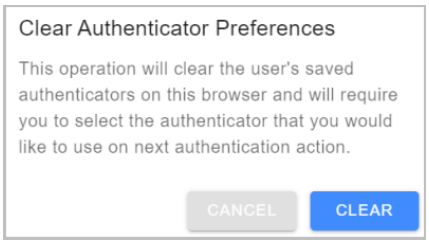


- **Set Password:** When this setting is enabled, users in the LOCAL directory have the option to reset the password required for user verification in services that utilize multi-factor authentication. To reset the password, users select the **Set Password** self-service option and enter the new password 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.

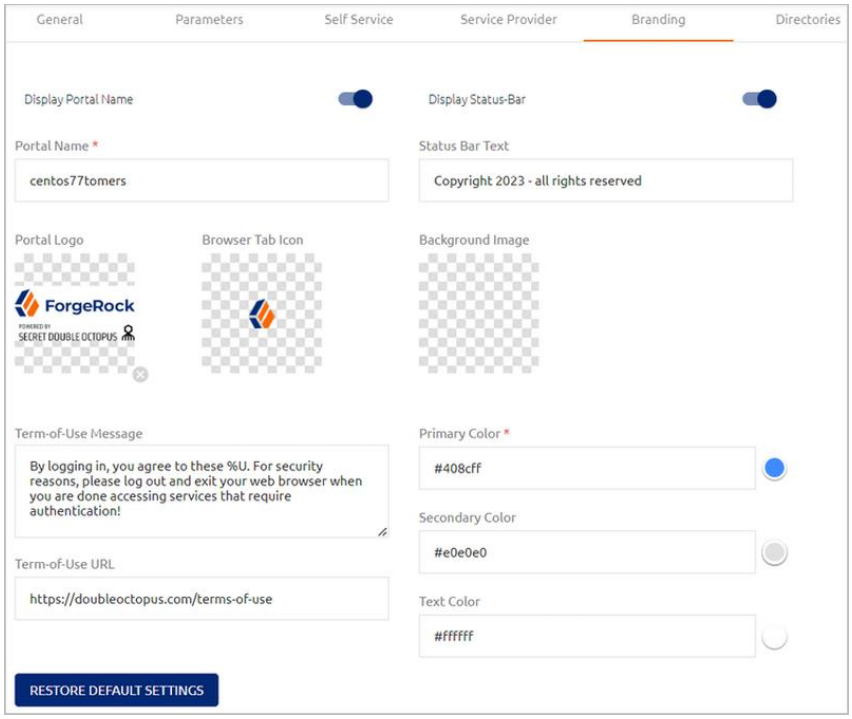
  To clear stored data, users select the **Clear Authenticator Preferences** self-service option and then click **Clear** in the confirmation popup.



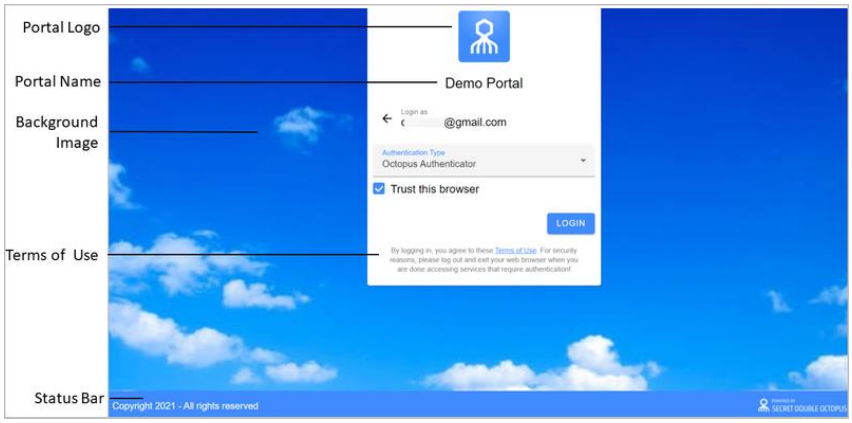
- **Open Support Ticket:** When users select this action, an email message to the **Support Email** address (specified in **System Settings > General Settings**) is automatically created in the user's default email client.

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.



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.



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 488x488 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.

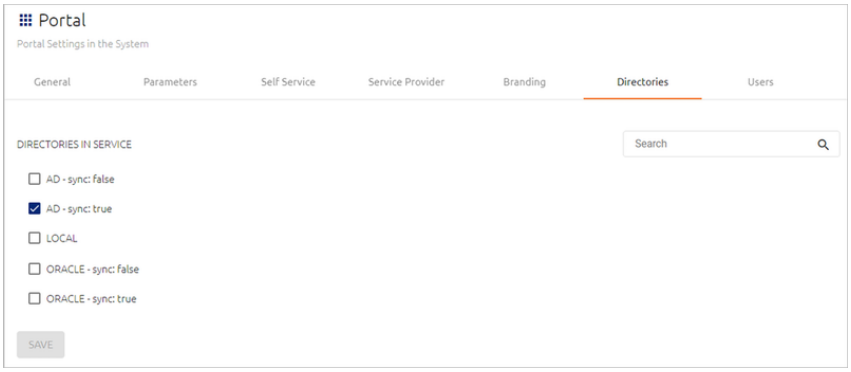
Assigning access privileges to the user portal

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.

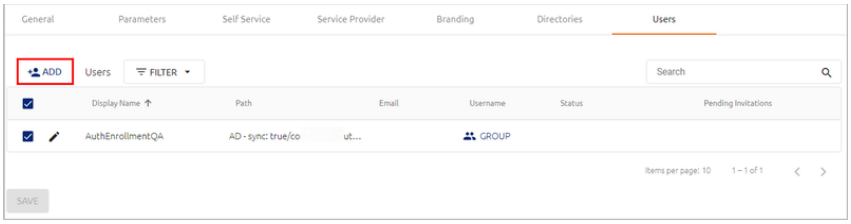
The following procedure explains how to grant Portal access by selecting the appropriate directories, groups and users.

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.

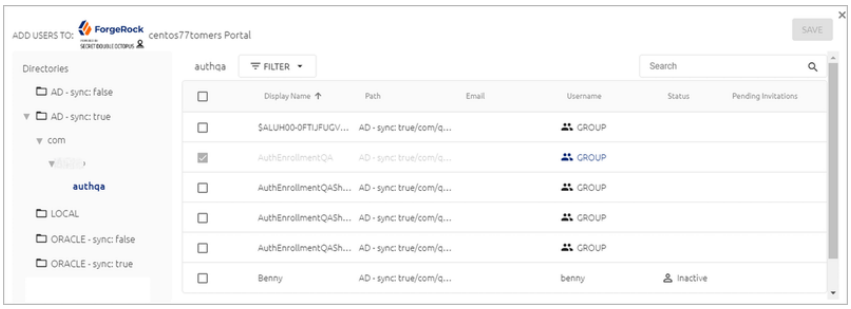


2. After selecting directories, open the **Users** tab and click **Add**.



   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.

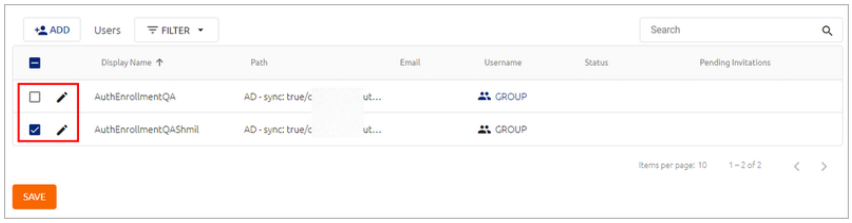


4. When you have finished making your selections, click **SAVE** (in the upper right corner of the popup).

   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.

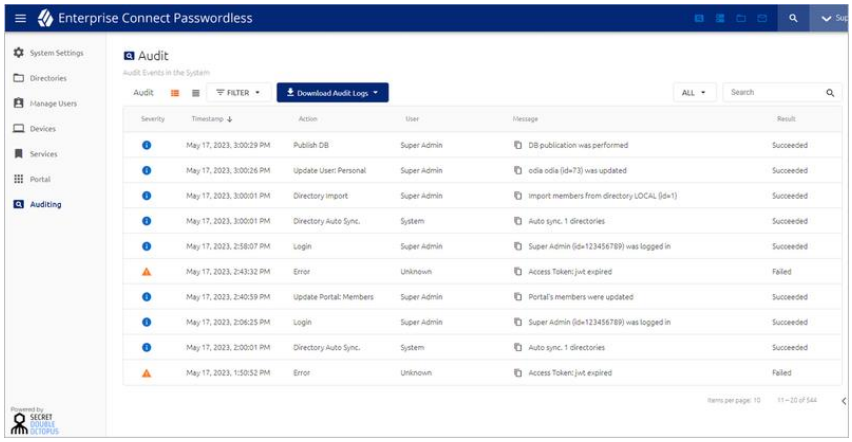
After adding users to the list, you can manage them directly from the **Users** tab. To enable or disable Portal access for a specific user, toggle the checkbox on the left side of the row. Clicking the Edit icon next to the checkbox opens the individual settings for that user.



Auditing events

The Management Console records and logs every administrative action performed by the system or by users. You can use these records for auditing purposes and for fulfilling regulatory requirements.

To view the list of auditing events, select **Auditing** from the menu bar of the console. By default, all recorded events are listed. You can filter the list according to event severity and keywords, as described in the sections below.

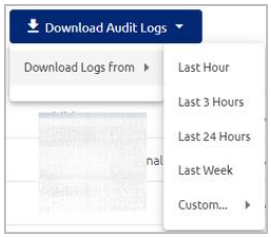


The grid on the **Auditing** page provides the following information about each event:

Column	Description / Notes
Severity Level	• **Critical:** Events that interfere with system functioning, such as LDAP service errors, enrollment failures, etc. • **Warning:** Events that interrupt a user's workflow (e.g., failed authentication), or that involve unsuccessful administrative operations (e.g., creating a user who already exists). • **Info:** Events involving routine administrative operations.
Timestamp	Date and time of event occurrence.
Action	Type of event.
User	Name or username of the entity performing the action.
Message	A brief summary of the event. You can view more information by clicking the icon in the **Severity** column (Viewing Event Details).
Result	Status of the event (succeeded, failed, etc.).

Click the icons at the top of the page to toggle presentation of the list between standard List view and Compact List view. The standard List view displays up to 10 items per page, and Compact List view displays up to 20 items per page. In either view, you can sort the list according to any column (except **Message**) by clicking on the column header.

To download auditing events in CSV format, click **Download Audit Logs** and select a timeframe.



Then, in the confirmation popup, click **Download**.

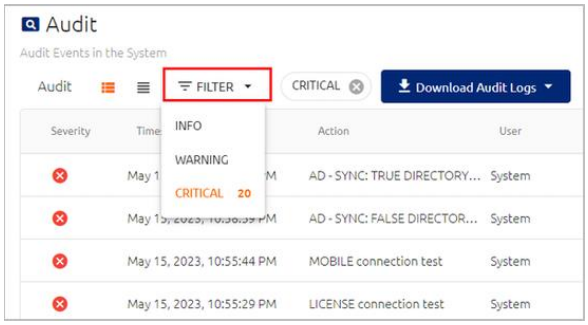
> **Note**
>
> When auditing filters are selected, the filtered Audit list is downloaded.

Filtering the events list

The filtering options at the top of the Events list allow you to filter displayed events according to event severity and according to keyword search. You may use both filtering techniques simultaneously.

Filtering by Event Severity

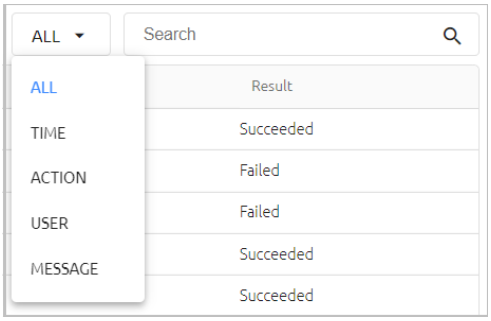
The Filter feature shows how many events occurred of each severity and enables you to filter the Events list according to a specified severity. To view all events of a given severity, click the relevant option. To restore the default view, close the filtering chip to the right of the Filter list.



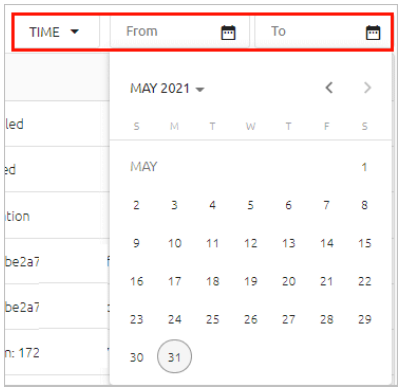
Filtering by Category and Keyword

The Search tool on the upper right side of the Events 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 further target the scope of your search, you can select a category from the list to the left of the Search tool before performing your keyword search. You may select any ONE category.



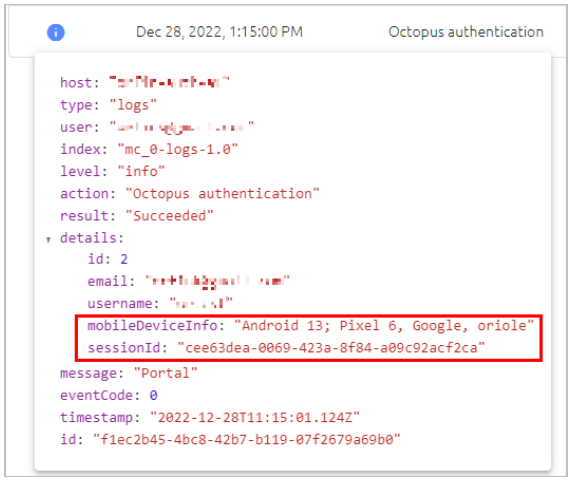
When using the **Time** category, specify the start and end dates by selecting them from the Calendar popups. The Events list is filtered automatically after you select the dates.



After selecting other categories, enter a keyword in the **Search term** field, and then press **<Enter>**.

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 unique session ID and data about the mobile device are provided for each authentication event, to help track and debug authentication sessions.



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.
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 currently. Please contact your administrator.
3016	3rd party authenticator not available	Alternate BLE, Allow offline	Authentication failed. Current 3rd party authentication method is not available currently. 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.
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 currently. Please contact your administrator.
3028	Error writing agent data	None	Authentication failed. Current 3rd party authentication method is not available currently. Please contact your administrator.
3021	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	
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.

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. Make a copy of 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
   ```

4. Open the new JSON file for editing:

   ```
   vi <AAGUID of new key>.json
   ```

   Replace the existing AAGUID value with that of the new FIDO key.

5. Navigate to the directory containing the scripts:

```
cd ../../mcbackendsql
```

6. Run the following script:

```
node scripts/fidoMetadata.js add ../etc/fido/<AAGUID of new key>.json
```

7. On all Authentication Servers and Authentication Servers in the DMZ, run the following command to restart the service:

```
systemctl restart sdoweba
```