Enterprise Connect Passwordless for Mac Installation Guide

Version 2.6.7

For Enterprise Connect Passwordless Server version 5.4.8 and above

Table of Contents

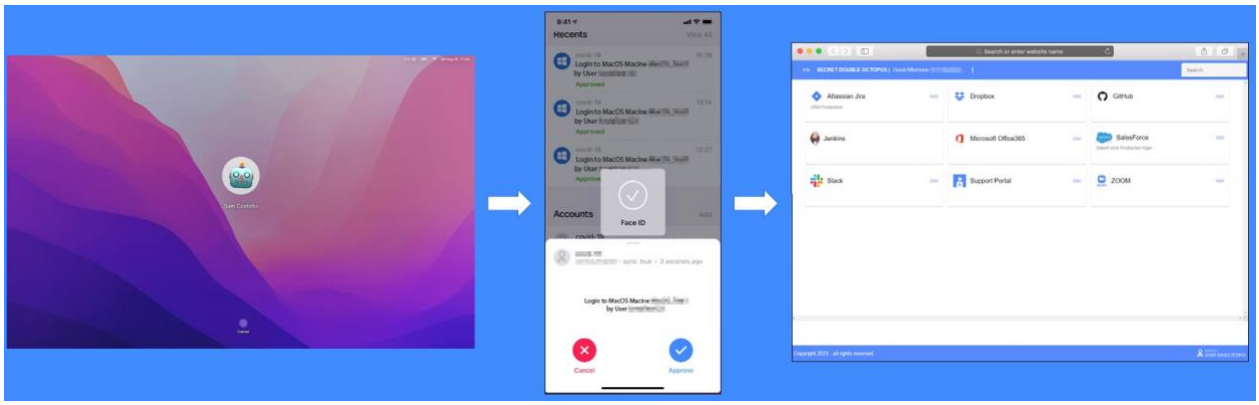
Preface ... 3
Product Overview ... 3
Prerequisites ... 3
Creating the Active Directory Authentication Service ... 4
macOS Client Installation ... 9
Preparing for Installation ... 9
Configuring the XML File ... 9
Installing the Mac Client ... 12
Onboarding Local Users ... 15
Enabling the Octopus Authenticator / ForgeRock Authenticator ... 15
Enabling FIDO Authentication ... 18
Enabling OTP Authentication ... 22
Enabling the Password Free Experience ... 28
XML File Configuration ... 28
Management Console Configuration ... 28
Password-free Mode: User Experience ... 30
Handling FileVault Login ... 31
Enabling FileVault Login (All Configurations) ... 31
Configuring FileVault Login on the Mac (Client Configuration) ... 35
Working with the FileVault Password (Server Configuration) ... 37
Managing the FileVault Password ... 38
Working with Kerberos Tickets ... 40
Renewing the Ticket ... 40
Viewing Kerberos Ticket Status ... 41
Configuring Access Permissions in macOS Monterey ... 43
Uninstalling the Mac Client ... 45
Troubleshooting ... 47
Appendix A: Mac User Experience ... 48
Accessing the User Portal ... 48
Updating System Preferences ... 48
Adding Your Machine to the Active Directory ... 49
Appendix B: Known Issues ... 53

Preface

This document provides step-by-step installation instructions for Enterprise Connect Passwordless for Mac with Active Directory integration.

Product Overview

Secret Double Octopus replaces passwords altogether with a high assurance, password-free authentication paradigm. Using the MAC Authentication Provider in conjunction with standard interfaces to Active Directory, the password-free solution seamlessly replaces AD passwords with a stronger, more secure alternative. As a result, the security posture of the AD domain is enhanced, user experience and productivity improve, and password management costs are dramatically lowered.



Prerequisites

Enterprise Connect Passwordless for Mac supports the following operating systems:

- macOS Big Sur
- macOS Monterey
- macOS Ventura

Before beginning installation, verify that:

- Enterprise Connect Passwordless Authentication Server **version 5.4.8** (or above) is installed and operating with a valid enterprise certificate.
- Your Corporate Directory Server is operating with Admin rights and is integrated with the Enterprise Connect Passwordless Management Console. For more information about directory integration, please refer to the Management Console Admin Guide.
- Enterprise Connect Passwordless for MAC installation and the Configuration XML file are ready to be deployed for all Corporate macOS machines.
- The fingerprint setup is completed (for Mac PCs that support fingerprint).
- Users are enrolled with one or more authenticators on the Authentication Server. These can include the ForgeRock Authenticator or FIDO.

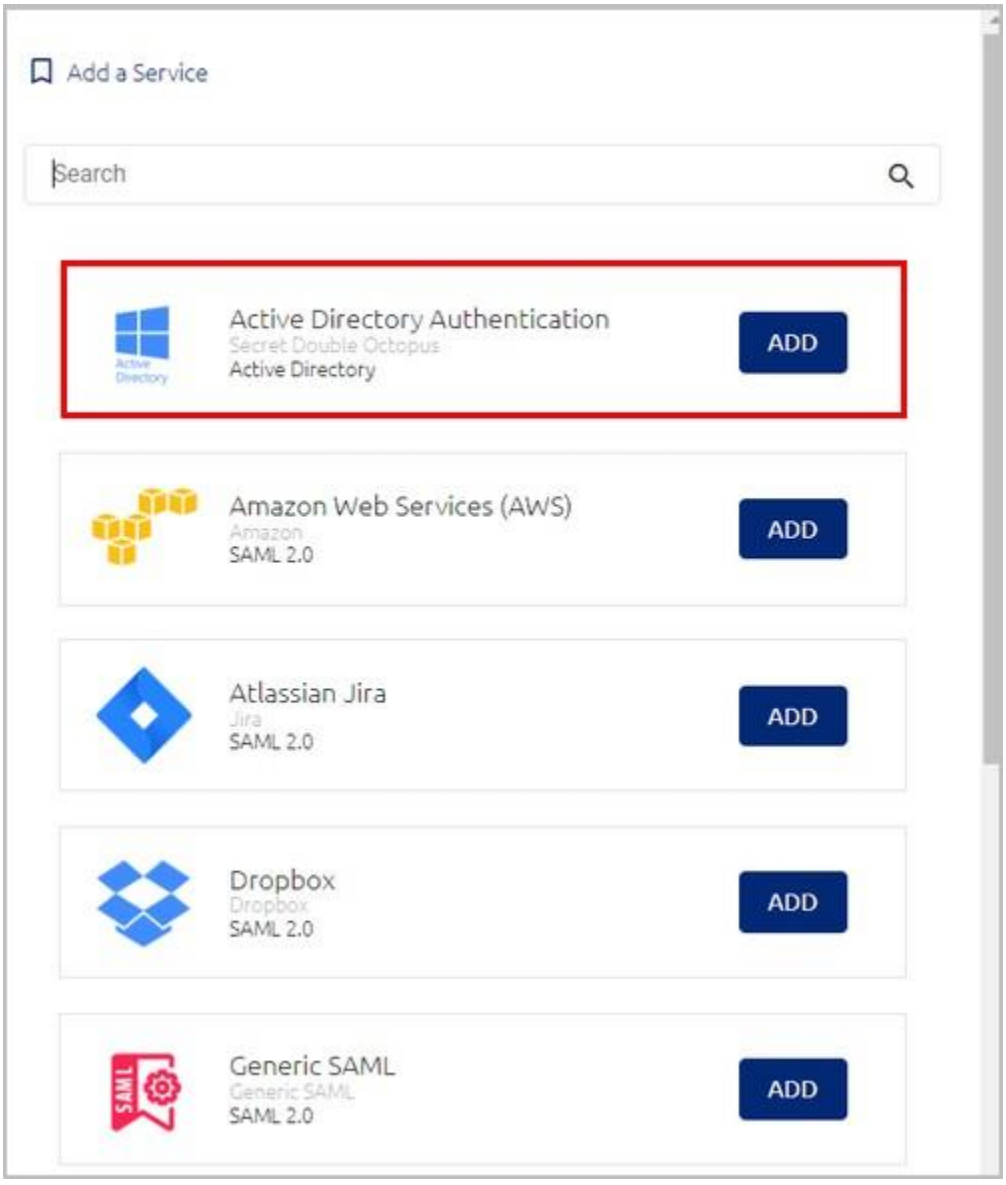
Note: The Enterprise Connect Passwordless for macOS installation and XML template will be provided by the Secret Double Octopus team.

Creating the Active Directory Authentication Service

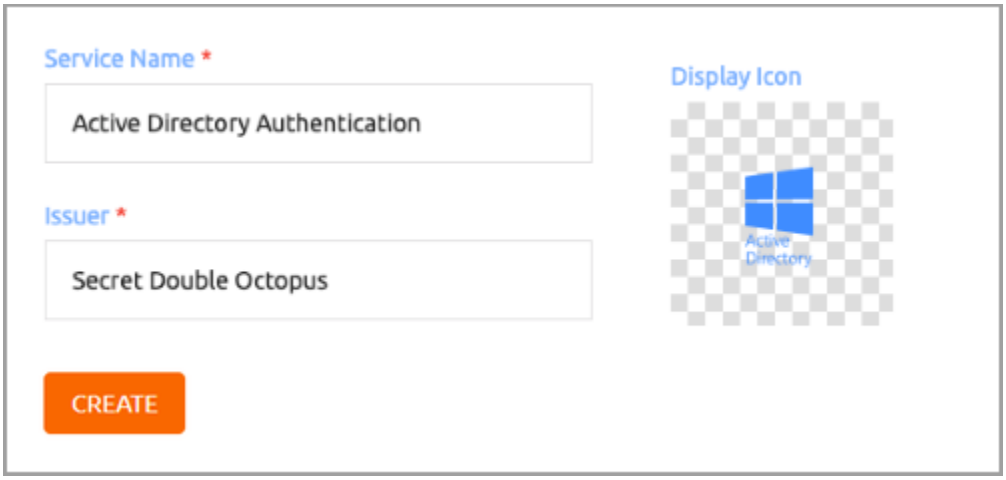
To enable installation of Enterprise Connect Passwordless for Mac, the Active Directory Authentication service needs to be created in the Management Console. Follow the steps below to add the AD service and configure service settings.

To create the Active Directory Authentication service:

1. From the Management Console, open the **Services** menu and click **Add Service**.
2. In the **Active Directory Authentication** tile, click **Add**.

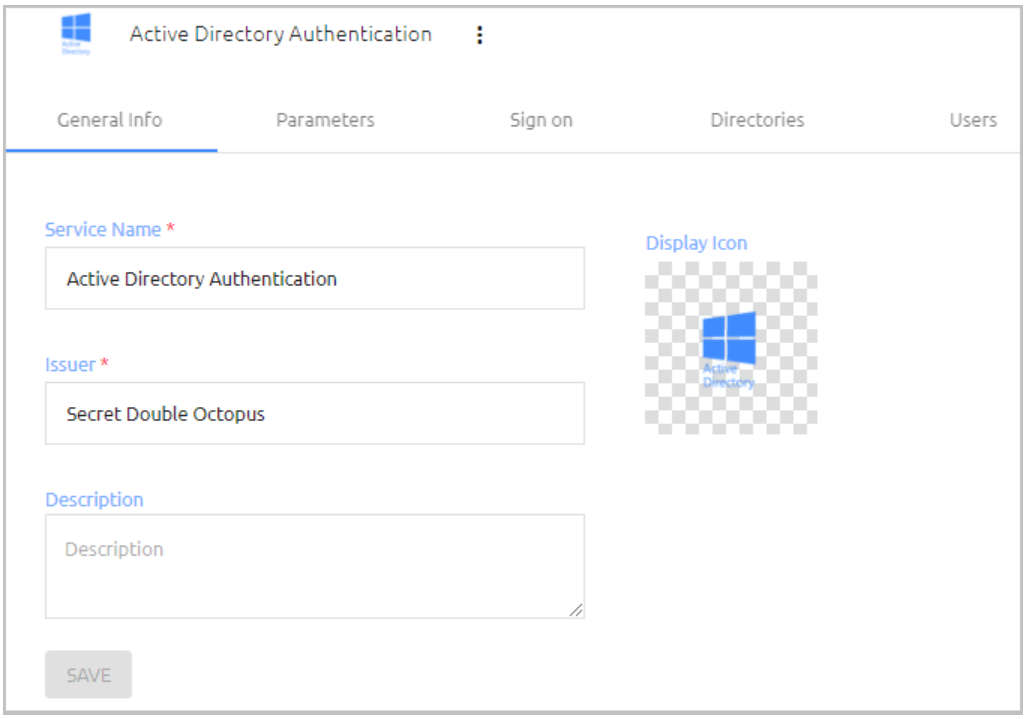


Then, in the dialog that opens, click **Create**.

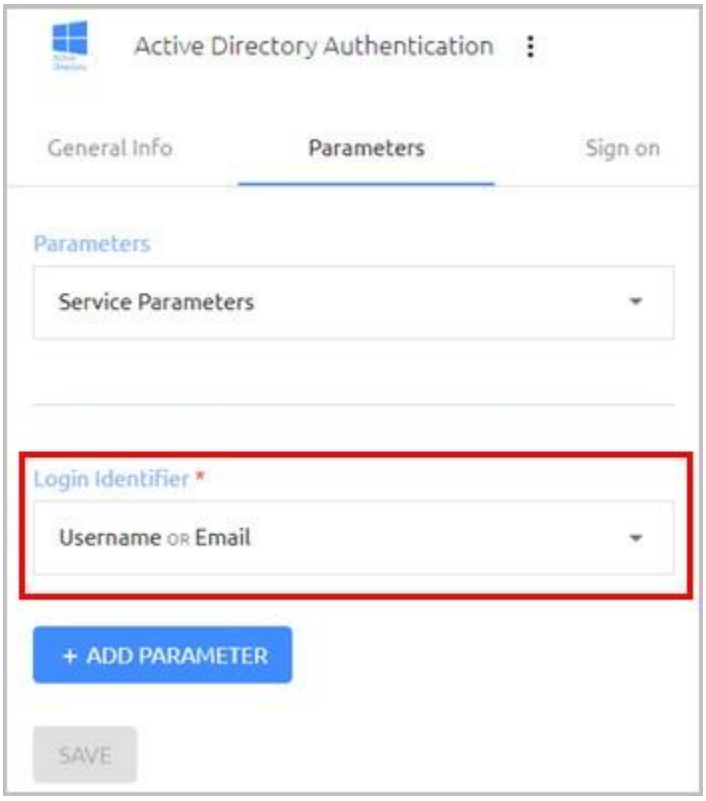


3. Review the settings in the **General Info** tab. If you make any changes, click **Save**.

Setting	Value / Notes
Service Name / Issuer	Change the default values if desired.
Description	Enter a brief note about the service if desired.
Display Icon	This icon will be displayed on the Login page for the service. To change the default icon, click and upload the icon of your choice (JPG or PNG format). Supported image size is 488x488 pixels.



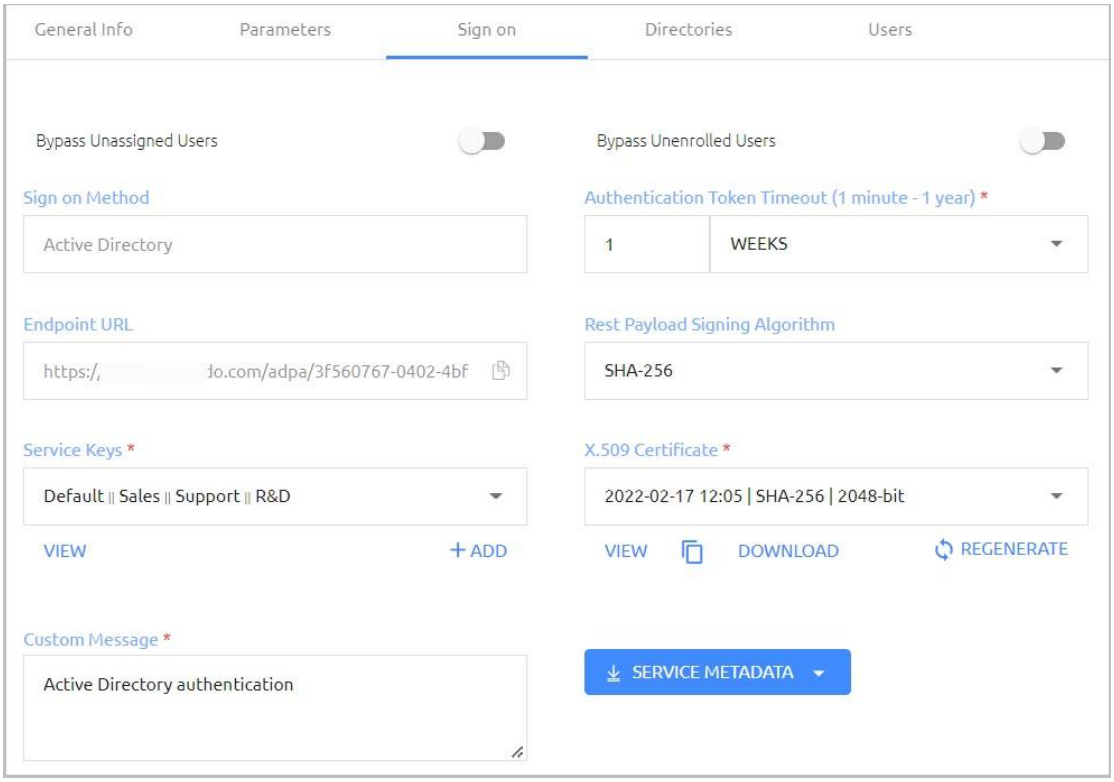
4. Open the **Parameters** tab. From the **Login Identifier** dropdown list, select the credential type that will be sent by the user for the authentication (usually **Username**).



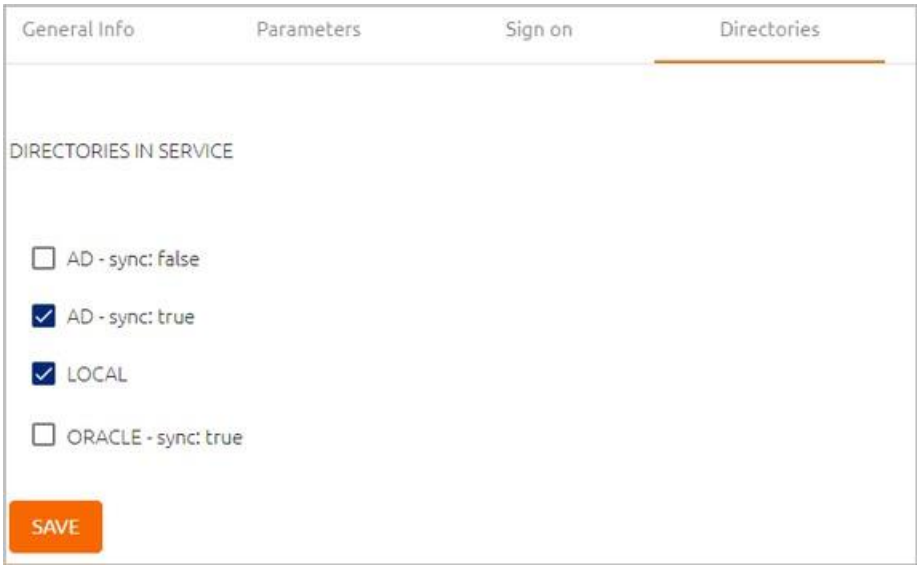
Then, click **Save**.

5. Open the **Sign on** tab and review / configure the following settings:

Setting	Value / Notes
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. The option is usually used on a temporary basis only, during gradual rollouts of the platform.
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).
Sign on Method	The authentication method used for the service (not editable).
Endpoint URL	The access URL from the Mac client to the Authentication Server (not editable). Click the Copy icon to copy the value.
Service Keys	Key(s) used by the service to authenticate with Octopus Authenticator. Click **View** to display the content of the key(s) in a popup window. The Copy icon in the popup lets you easily copy the content.
Custom Message	Message shown to the user on successful authentication.
Authentication Token Timeout	Time period after which the authentication token becomes invalid. The value can range from one minute to one year.
Rest Payload Signing Algorithm	Signature of the generated X.509 certificate. Select **SHA-1** or **SHA-256**.
X.509 Certificate	The public certificate used to authenticate with Octopus Authenticator. • Click View to display the content of the certificate in a popup. • Click Download to download the certificate as a .PEM file. • Click Regenerate to replace the certificate. You will be prompted to select the signature algorithm and size before regenerating.



6. At the bottom of the **Sign on** tab, click **Save** (if the button is enabled).
7. Open the **Directories** tab and select the directories that will be available for the service. Then, click **Save**.



8. Open the **Users** tab and click **Add**.
   A popup opens, with a list of directories displayed on the left.
9. Expand the directories list and select the groups and users to be added to the service. After making your selections, click **Save** (in the upper right corner) to close the dialog.
   The groups and users you selected are listed in the **Users** tab.
10. At the bottom of the **Users** tab, click **Save**. Then, from the toolbar at the top of the page, click

PUBLISH and publish your changes.

macOS Client Installation

The following sections describe the installation process:

- Preparing for Installation [8]
- Installing the Mac Client [10]
- Onboarding Local Users [12]

Preparing for Installation

The following files are required for installation:

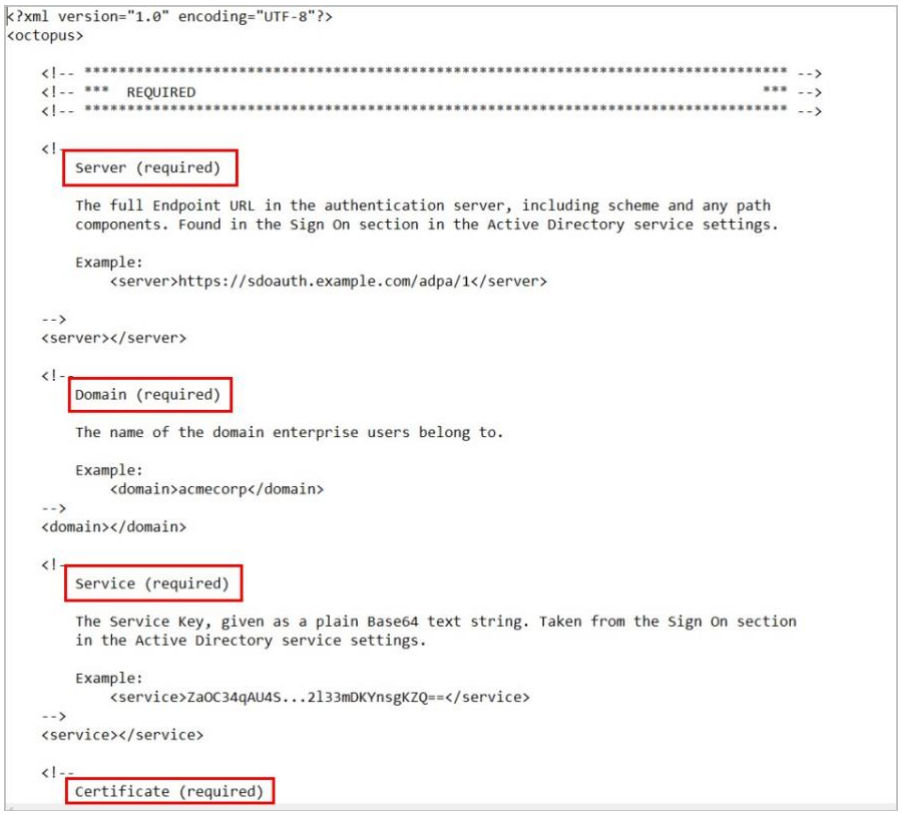
- **enterprise-connect-passwordless.pkg:** The installer file
- **enterprise-connect-passwordless.xml:** The configuration file for the installation

For successful installation, these files must be stored in the same folder and use the same name.

Configuring the XML File

Before beginning installation, open the XML file and set the parameters described below.

Four parameters are required: *server*, *domain*, *service* and *certificate*.

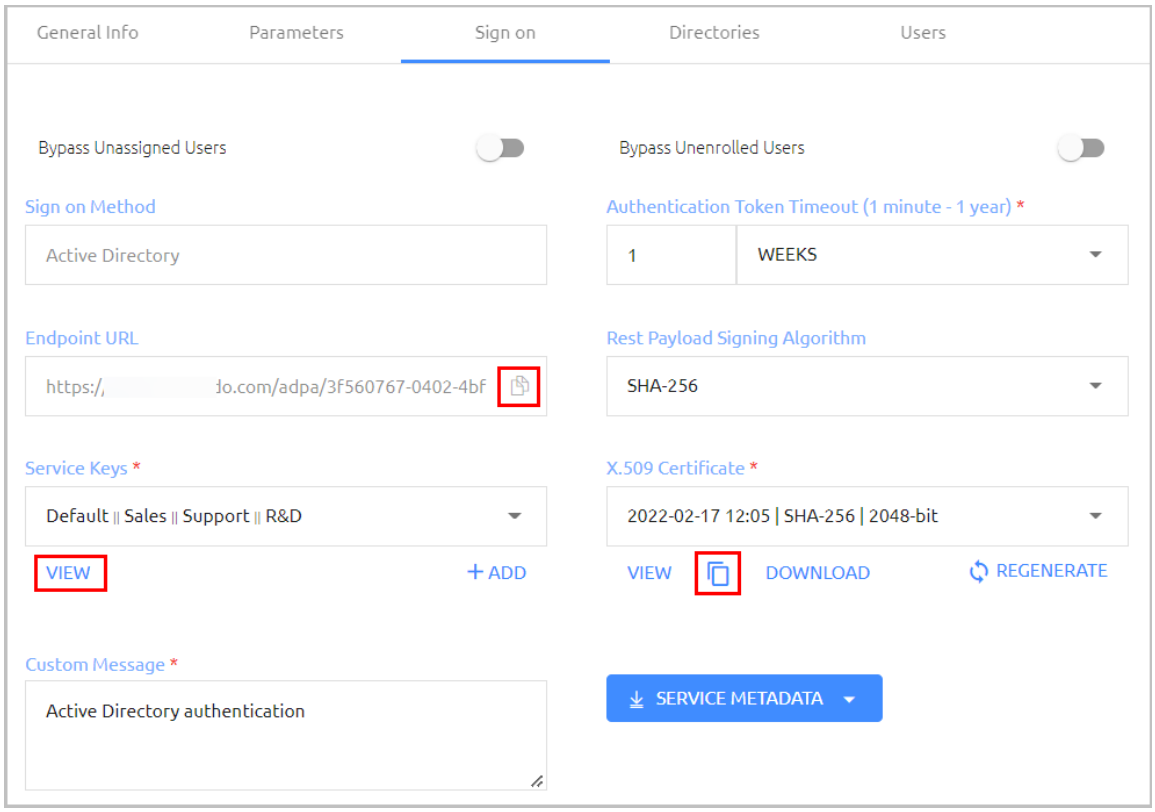



```
<?xml version="1.0" encoding="UTF-8"?>
<octopus>

    <!-- ********************************************************************************** -->
    <!-- ***  REQUIRED                                                                  *** -->
    <!-- ********************************************************************************** -->

    <!--
        Server (required)

        The full Endpoint URL in the authentication server, including scheme and any path
        components. Found in the Sign On section in the Active Directory service settings.

        Example:
            <server>https://sdoauth.example.com/adpa/1</server>

    -->
    <server></server>

    <!--
        Domain (required)

        The name of the domain enterprise users belong to.

        Example:
            <domain>acmecorp</domain>
    -->
    <domain></domain>

    <!--
        Service (required)

        The Service Key, given as a plain Base64 text string. Taken from the Sign On section
        in the Active Directory service settings.

        Example:
            <service>ZaOC34qAU4S...2l33mDKYnsgKZQ==</service>
    -->
    <service></service>

    <!--
        Certificate (required)
```

domain is the name of the domain to which enterprise users belong, for example: *<domain>acmecorp</domain>*

The other required values can be copied from the Management Console. From the **Services** menu, select your Active Directory Authentication service and open the service settings. Then, select the **Sign on** tab.

- **server**: The **Endpoint URL**. Click the Copy icon and paste into the XML file.
- **service**: The **Service Key**. Click **View** and then click the Copy icon of the relevant key. Paste into the XML file.
- **certificate**: The **X.509 Certificate**. Click the Copy icon and paste into the XML file.



The following additional parameters may be updated, as required:

Parameter	Description	Example / Notes

mfa	Enables/Disables MFA. Default value is *false* (disabled).	When MFA is enabled, users are required to enter username + Password, and then the selected MFA authenticator (Octopus or 3rd party will be used). *<mfa>true</mfa>*
passwordfree	Enables/Disables the Password Free Experience [25]. Default value is *false* (disabled).	When the Password Free Experience [25] is enabled, users deploy the Mac agent while maintaining control over the password. After the first login, all authentication is Passwordless. *<passwordfree>true</passwordfree>*
validPasswordIsSufficient	Determines whether users will be able to log in using a valid password even when Passwordless mode is set. Default value is *false*.	*<validPasswordIsSufficient>true</ validPasswordIsSufficient>*
forceLockAfterOfflineLogin	When set to *true* (default value), users who have logged in using offline authentication are required to reauthenticate when the workstation goes back online.	*<forceLockAfterOfflineLogin>true</ forceLockAfterOfflineLogin>*

Parameter	Description	Example / Notes
thirdparty	Determines whether users will have to approve authentication requests using a third party service. Default value is *false* (disabled).	*<thirdparty>true</thirdparty>* The specific third party service used is defined in the Management Console, in the **Authenticators** tab of the Directory settings.
ssourl	If the value is a valid URL, Enterprise Connect Passwordless for Mac automatically opens the SSO portal in a browser window after user login to the Mac.	*<ssourl>https://sso.example.com/webportal </ ssourl>*
ssobrowser	When *ssourl* is defined, this parameter determines which browser is used to open the SSO portal. The default value, *system*, uses the default browser configured for the user.	Valid values are: • system • firefox • safari • chrome
filevaultlogin	Determines mode of operation for the FileVault Login feature. When set to *client* (default value), users can create their own password for FileVault Login. When set to *server,* the password is created and managed by the server.	*<ssobrowser>firefox</ssobrowser>* Valid values are: • client • server *<filevaultlogin>server</filevaultlogin>*
automatickerberossync	When set to *true* (default value), Kerberos tickets renew automatically if the user is logged into the workstation.	*<automatickerberossync>true</ automatickerberossync>*
kerberosrealm	When this parameter is defined, a Kerberos ticket is retrieved automatically upon login / unlock, and the **Kerberos** menu appears in Enterprise Connect Passwordless Preferences. The value should be the organization domain name in all uppercase letters.	*<kerberosrealm>ACMECORP.COM</ kerberosrealm >*
sudo	Enables/Disables authentication on command line sudo. Default value is *false* (disabled).	*<sudo>true</sudo>*
logging	Controls number and detail level of logging messages written by Enterprise Connect Passwordless for Mac.	Valid values are: • none • error • info • debug *<logging>info</logging>*

After updating parameters, save the XML file.

IMPORTANT: For the installation to work properly, **octopus-desk.xml** should have the same name as the installation package file, and both files must be placed in the same folder.

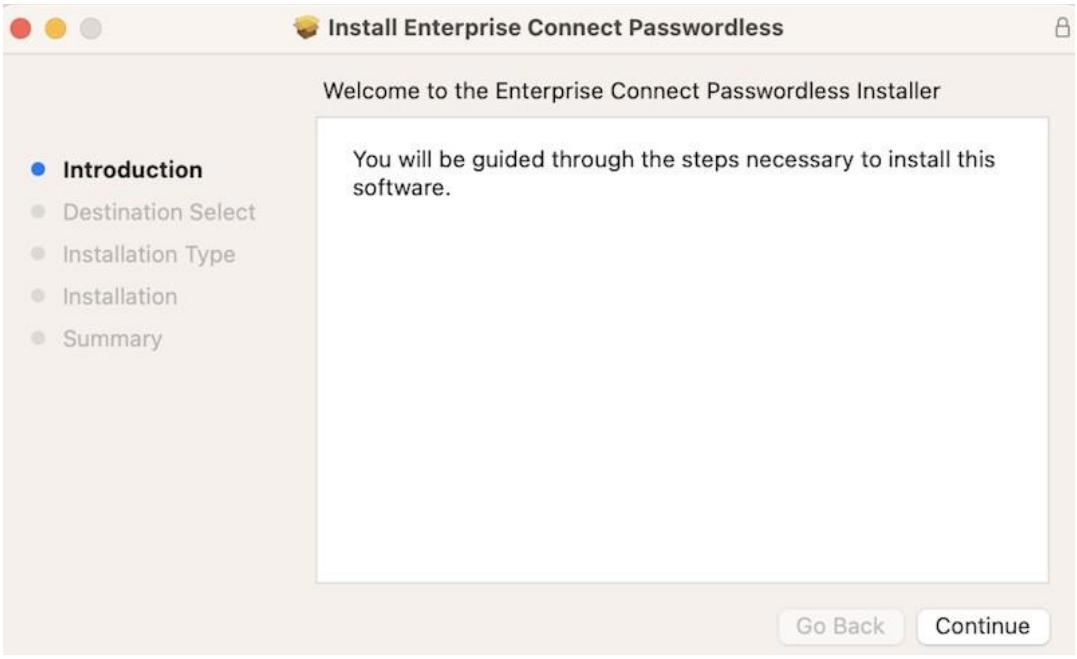
Installing the Mac Client

The following procedure explains how to use the installation wizard to install Enterprise Connect Passwordless for Mac. Before you begin, make sure that you have configured the XML file, as described above.

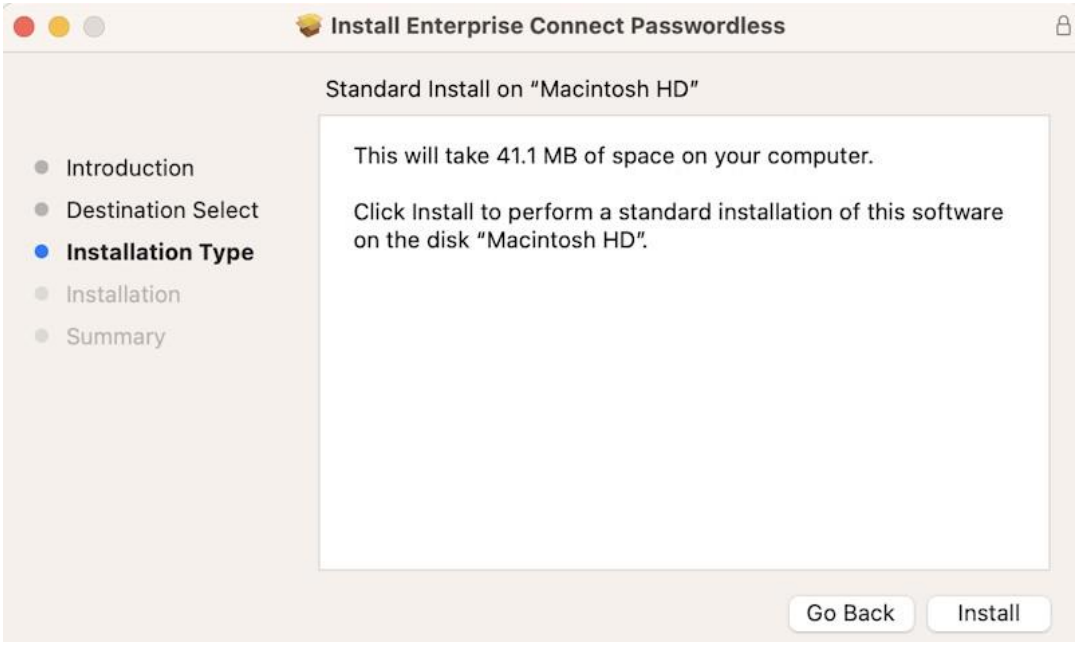
To install Enterprise Connect Passwordless for Mac:

1. As an Administrator, run the **enterprise-connect-passwordless.pkg** file to open the installer.

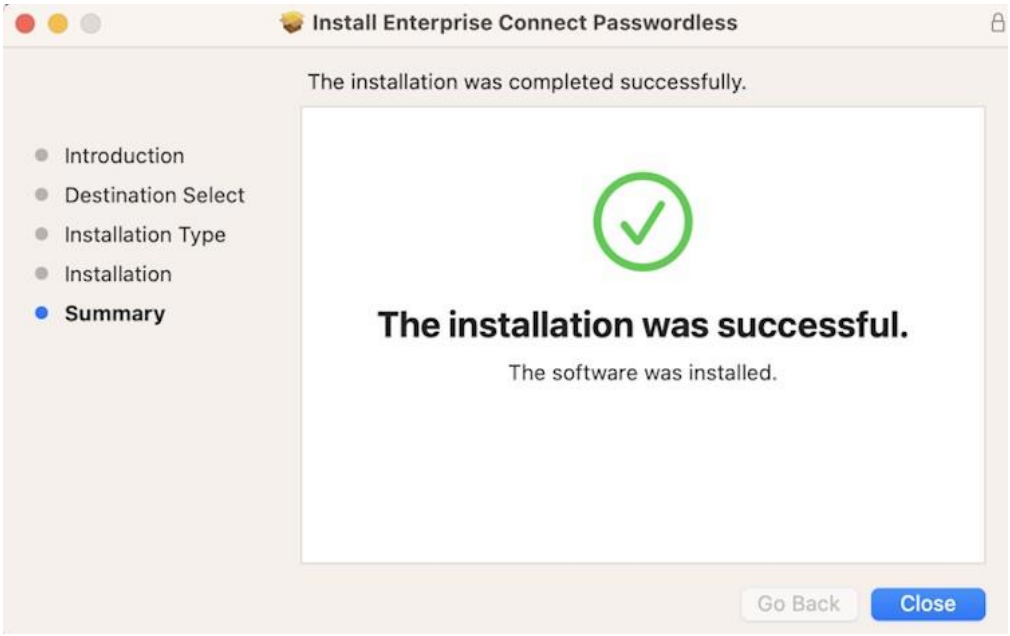
On the **Introduction** page, click **Continue**.



2. On the **Destination Select** page, click **Continue**.
3. On the **Installation Type** page, click **Install**.



4. When installation completes, a confirmation message is displayed. To exit the installer, click **Close**.



5. To verify installation, look for the application icon on the top bar.

Active Directory Domain users are enabled by default and will be able to authenticate immediately after Enterprise Connect Passwordless installation. The system will enforce MFA authentication with the authenticator set in the XML.

Note: If installation was successful but you are unable to use the Enterprise Connect Passwordless client, the machine may not be integrated with the corporate Active Directory. For more information, refer to Adding Your Machine to the Active Directory [46].

Non-domain users need to be onboarded manually. Refer to the next section for details.

Onboarding Local Users

The accounts of Local (non-domain) users need to be manually enabled before those users can log into their machines using Octopus Authenticator, third party authenticators, FIDO authenticators or OTP authentication. Follow the procedures in the sections below to onboard each Local user:

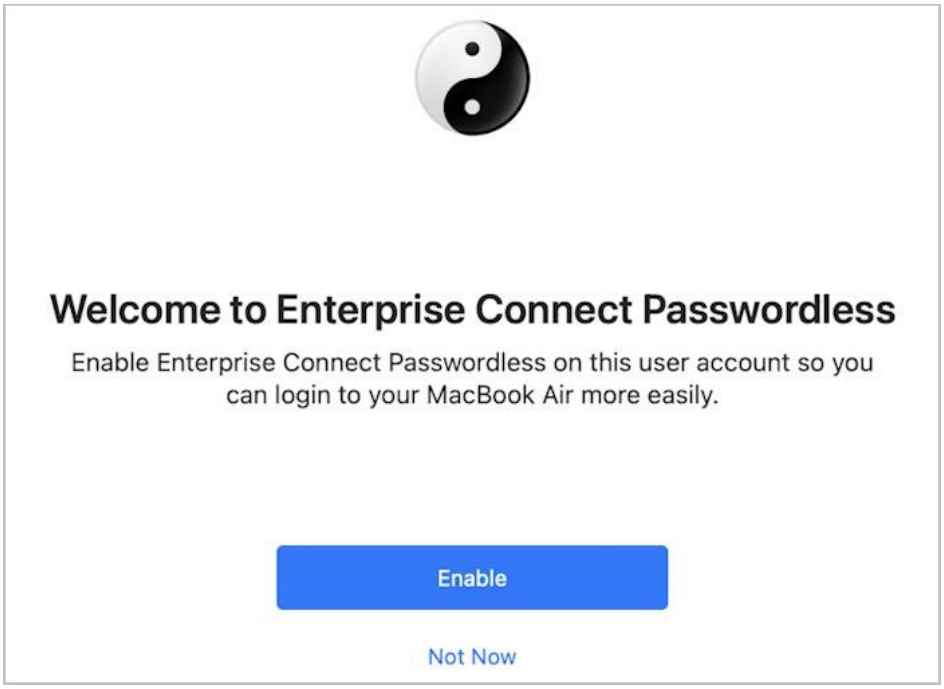
- Enabling the Octopus Authenticator / Third-party Authenticators [12]
- Enabling FIDO Authentication [15]
- Enabling OTP Authentication [19]

Enabling the Octopus Authenticator / ForgeRock Authenticator

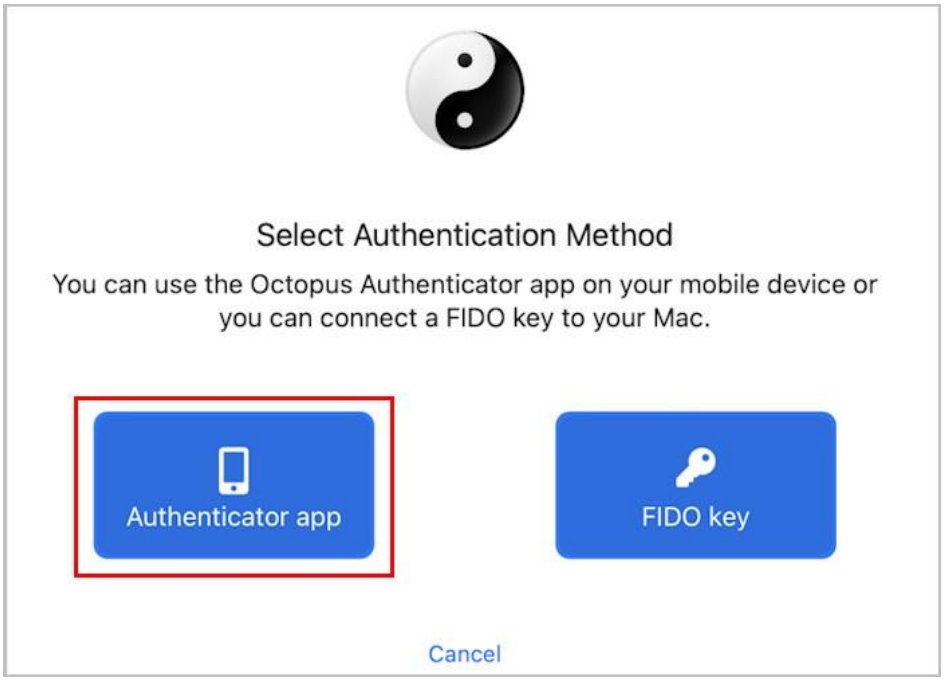
Follow the steps below to enable Local users to log into their machines using the Octopus Authenticator or ForgeRock Authenticator.

To onboard a Local user:

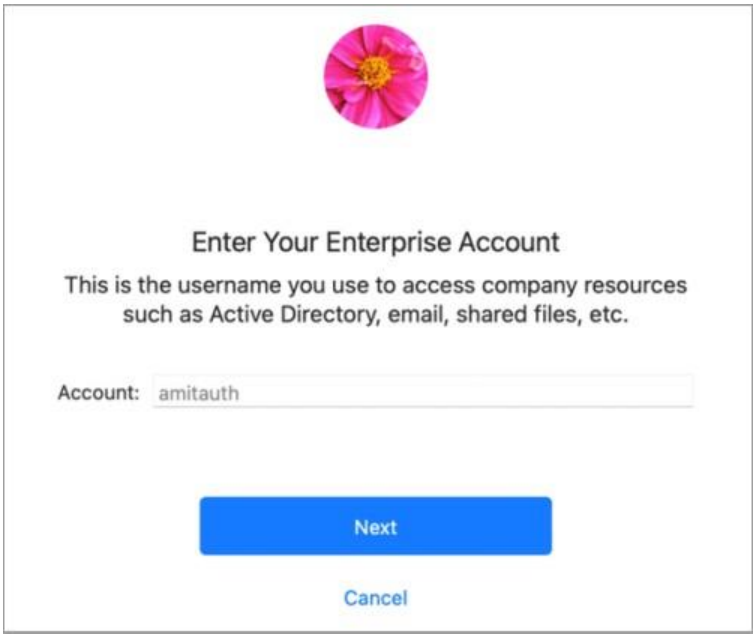
1. From the Welcome dialog, click **Enable**. (This dialog opens automatically after installation completes on machines of Local users.)



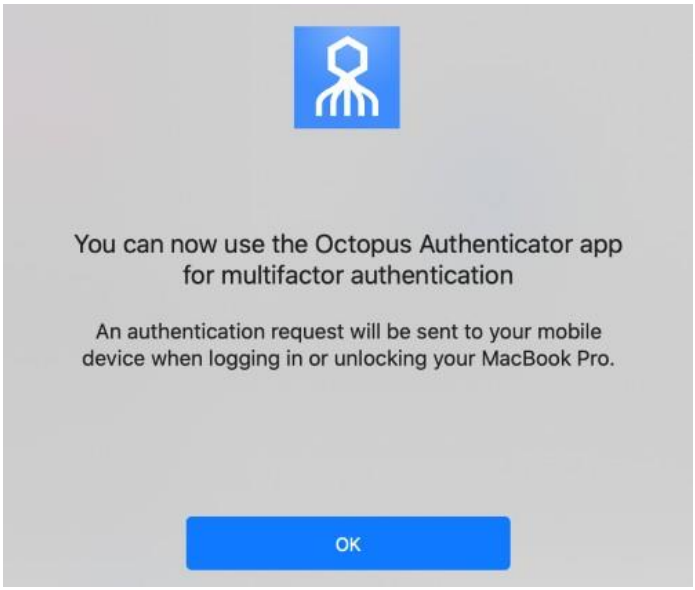
2. From the **Select Authentication Method** dialog, click **Authenticator app**.



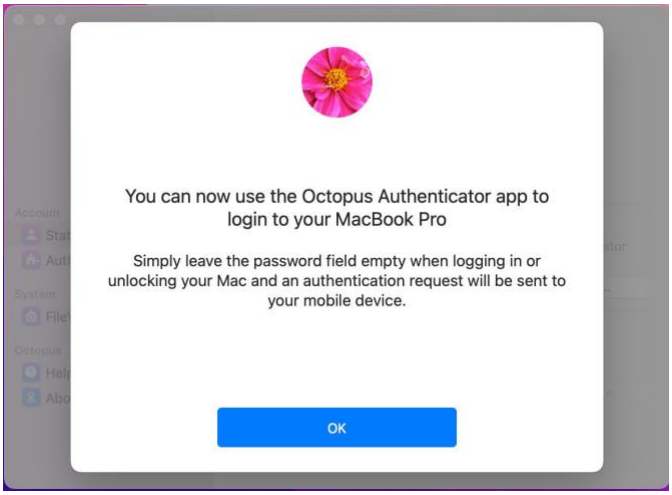
3. To enable Enterprise Connect Passwordless for Mac Authentication, enter the user's credentials in the **Account** field, and click **Next**.



4. When onboarding is complete, a confirmation message is displayed with instructions on how to use Octopus Authenticator.
   Confirmation Message for MFA:



   Confirmation Message for Passwordless:



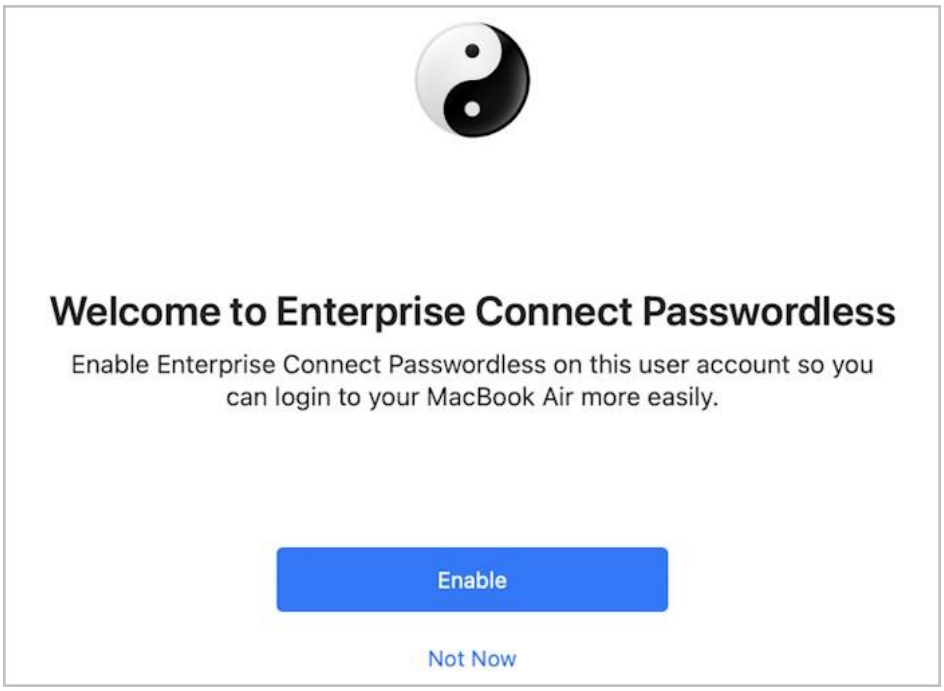
Enabling FIDO Authentication

Follow the steps below to enable Local users to log into their machines using a FIDO Authenticator.

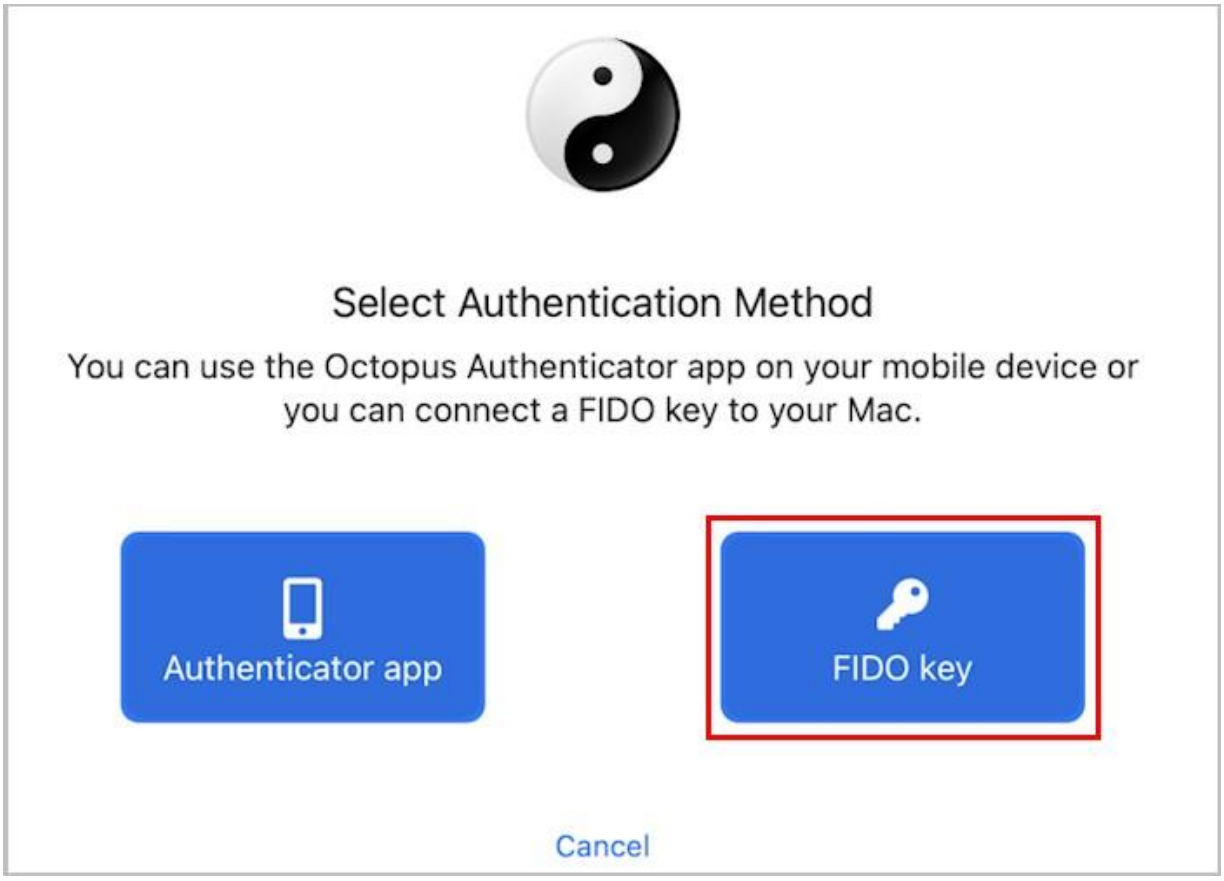
IMPORTANT: Before you begin, make sure that the FIDO key is enrolled with the user on the Authentication Server.

To onboard a Local user:

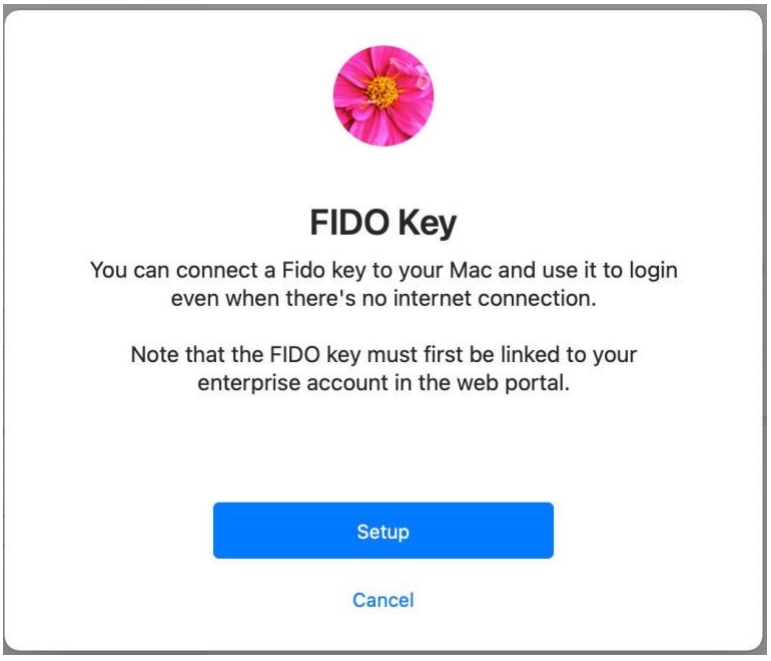
1. From the Welcome dialog, click **Enable**. (This dialog opens automatically after installation completes on machines of Local users.)



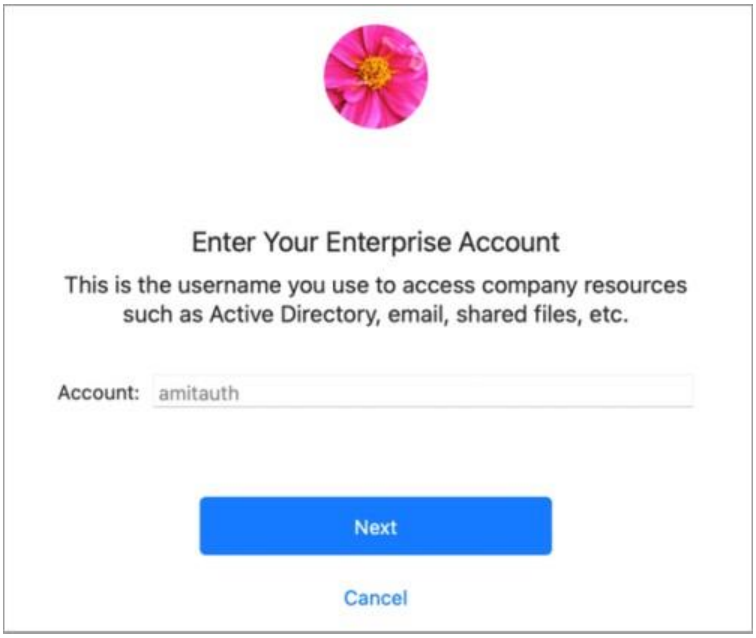
2. On the **Select Authentication Method** dialog, click **FIDO key**.



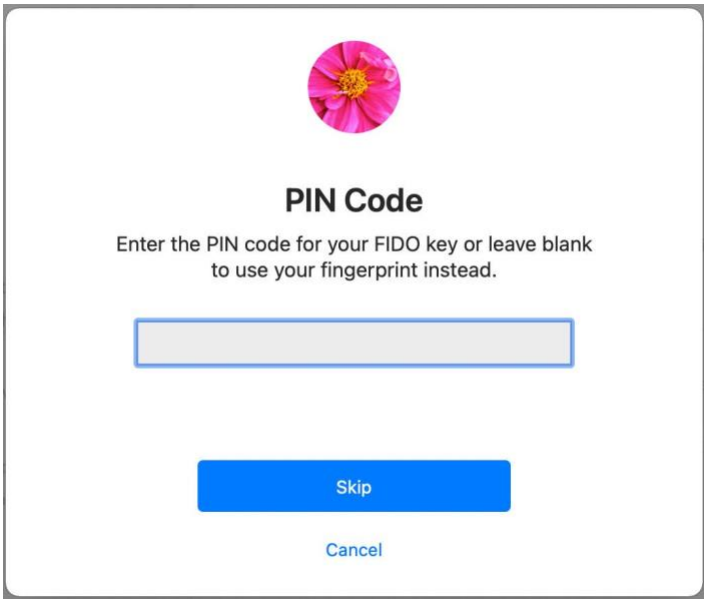
3. Insert the FIDO key into the machine to enable the **Setup** button. Then, click **Setup**.



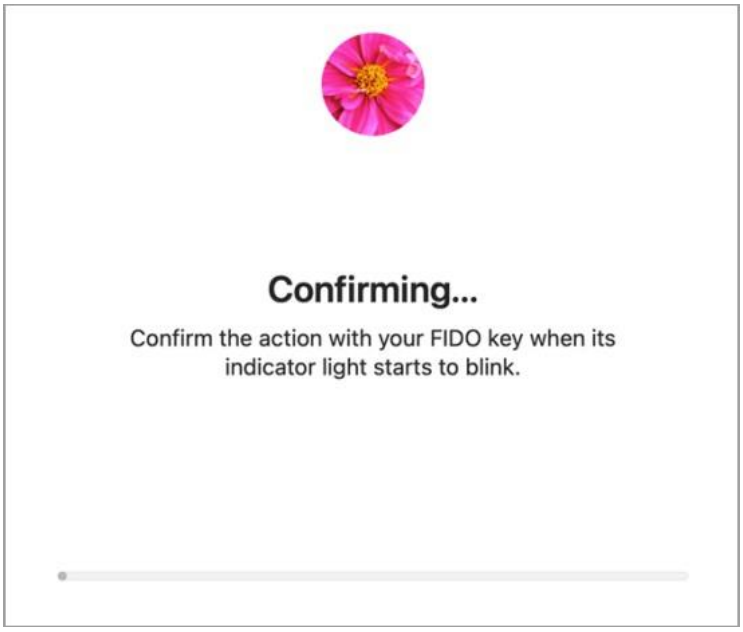
4. To enable Enterprise Connect Passwordless for Mac Authentication, enter the user's credentials in the **Account** field and click **Next**.



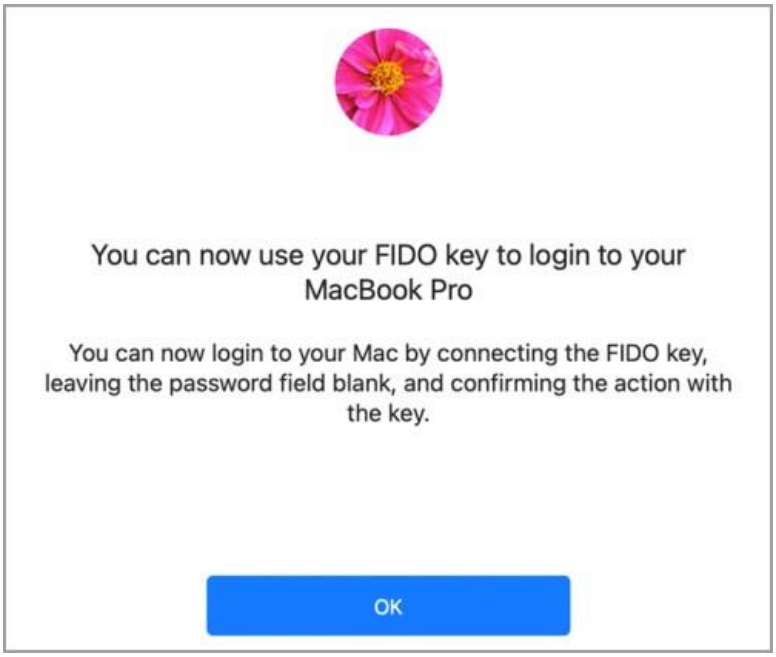
5. If the FIDO key requires a PIN (non-biometric key), enter the PIN code now.
   For biometric keys, leave the field blank and click **Skip**.



6. When the key begins to blink, the user should touch the key (non-biometric) or place the enrolled fingerprint (biometric).



7. When onboarding is complete, a confirmation message is displayed. The user can now use the FIDO key as the main authenticator for login, lock and system preferences (if the user has Admin permissions).



Using the FIDO Key for Authentication

To use FIDO as the default authenticator, the key needs to be inserted into the Mac **before** beginning the authentication process. When users have more than one authenticator enrolled, Enterprise Connect Passwordless will choose the FIDO key as primary only if it is inserted.

If the FIDO key is not inserted before starting authentication, a push notification is sent to the relevant Authenticator mobile app.

Enabling OTP Authentication

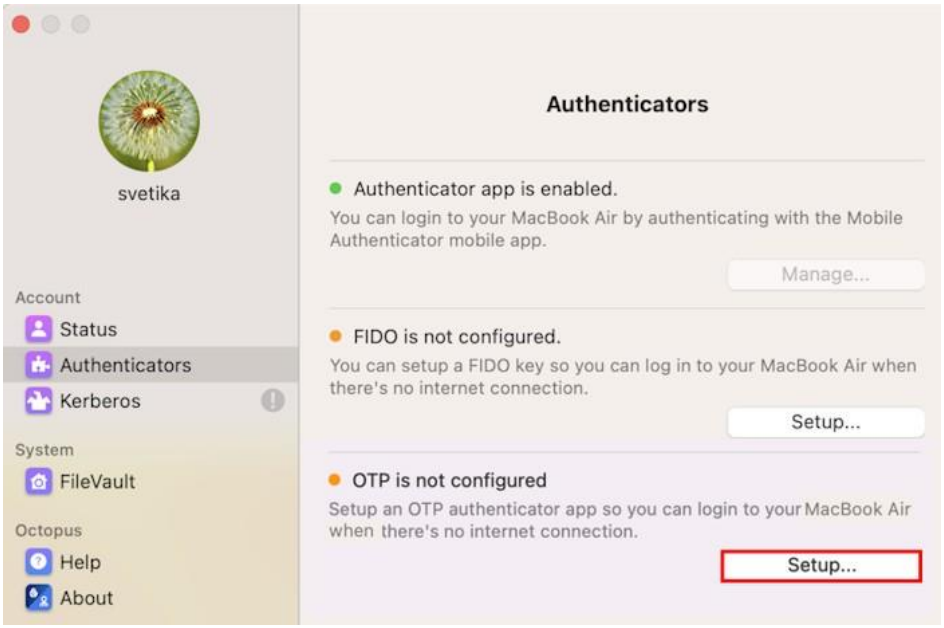
Enterprise Connect Passwordless for Mac supports the ability to use a one-time password as an additional multifactor authentication method. OTP authentication is supported both online and offline, allowing users to be able to authenticate regardless of whether they are currently connected.

IMPORTANT: The OTP option is available only when the Mac client is configured to work in MFA mode (the *mfa* parameter in the installation configuration file is set to *true*). For details, refer to Configuring the XML File [8].

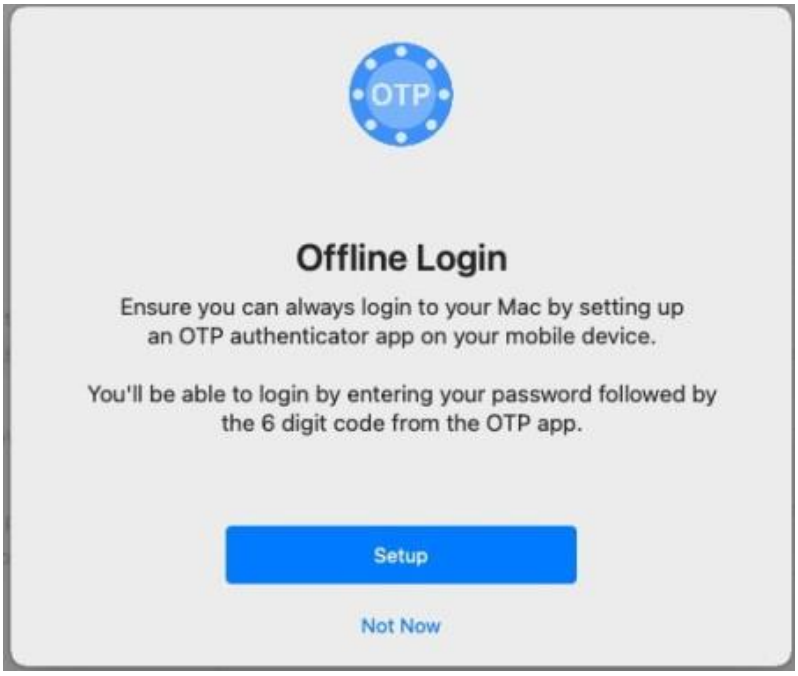
Follow the steps below to configure OTP authentication. Before you begin, open the Authenticator mobile app so you can add the OTP account.

To enable OTP authentication:

1. From the Enterprise Connect Passwordless configuration, select **Authenticators**. Then, in the OTP frame, click **Setup**.

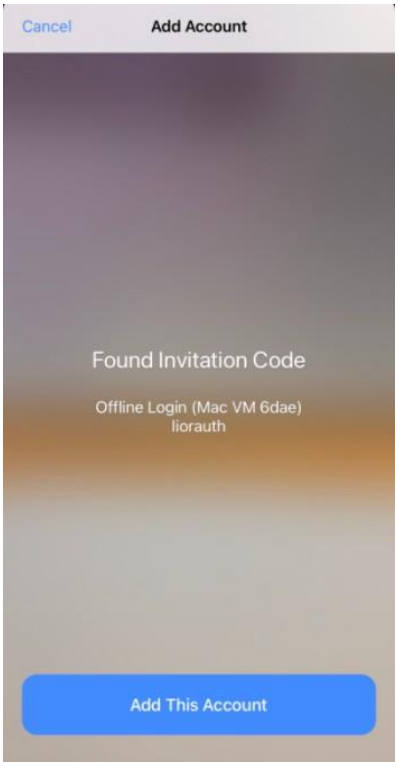


2. On the screen that opens, click **Setup**.

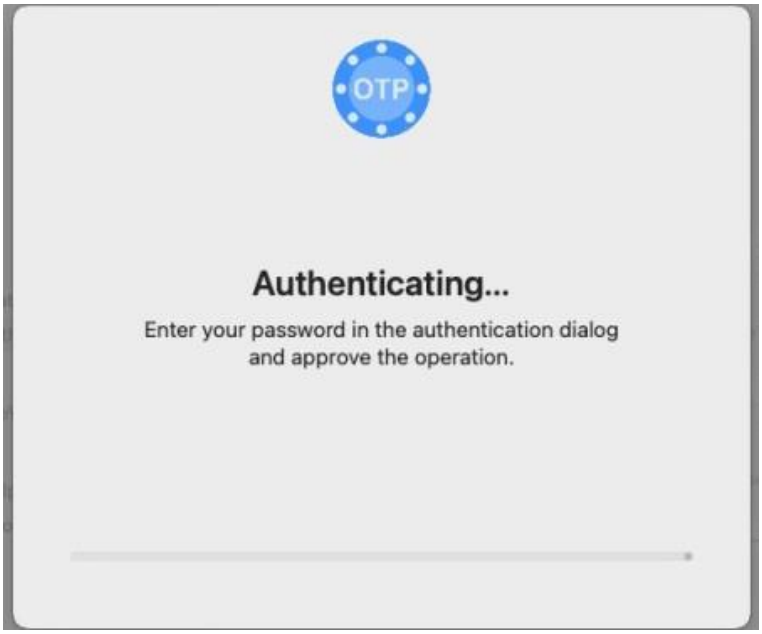


The following screen opens:

3. In the Authenticator mobile app, tap **Add Account**. Then, scan the QR code and click **Next**.
4. After scanning the QR code, tap **Add This Account**.

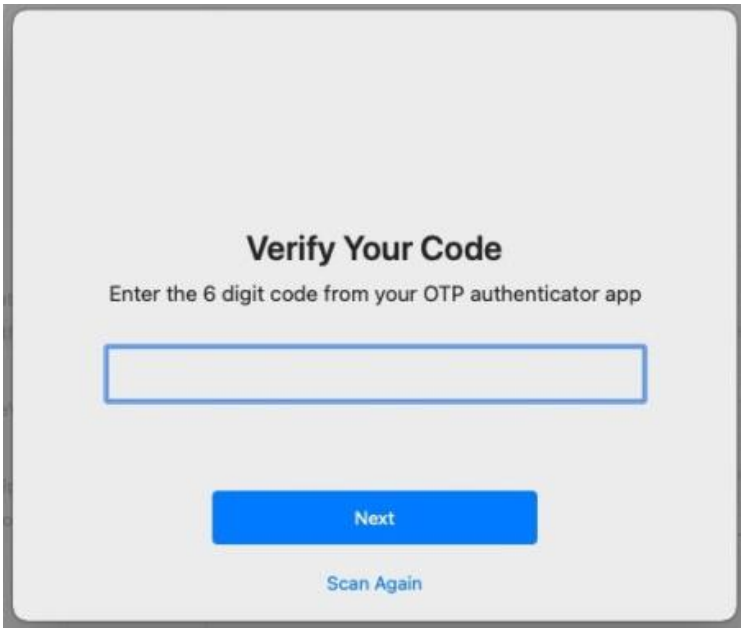


The following screen opens on your Mac:



5. Enter your Mac password and then click **Authenticate**.

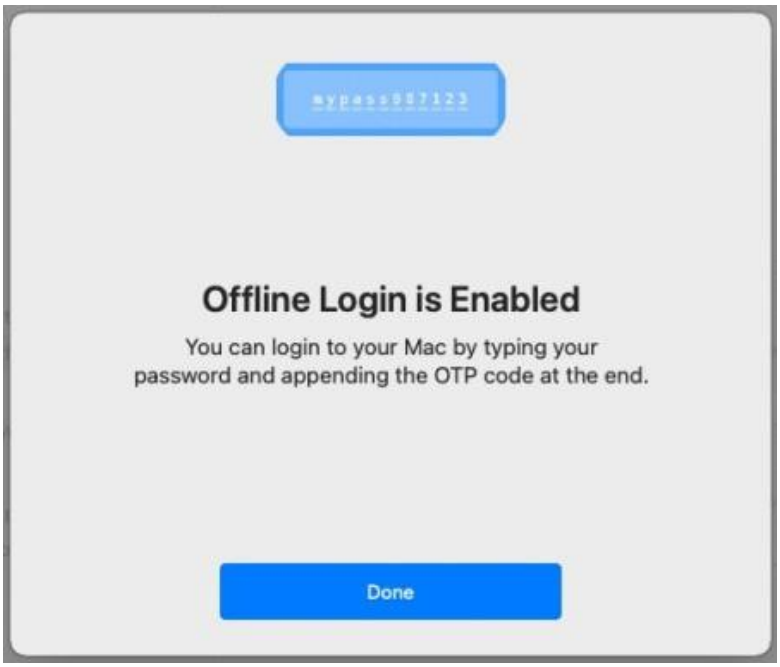
The following screen opens:



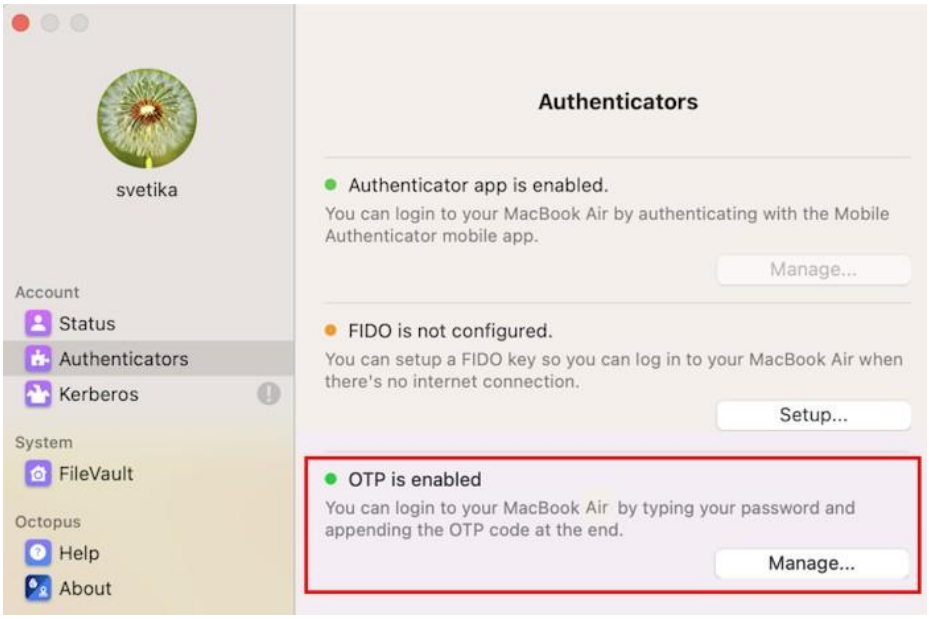
6. Enter the code displayed in the account you added in the Authenticator mobile app.

Then, click **Next**.

7. On the screen that opens, click **Done**.



OTP is now enabled.



Enabling the Password Free Experience

The Password Free Experience enables customers to start deploying the Mac agent while maintaining control over the password, so they can continue to use it for other applications. In the Password Free flow, users will be required to enter the password for the first login. After one successful login, all other authentications will be Passwordless (the user simply selects the Authenticator app or a FIDO security key and does not need to provide a password for each login).

When the Password Free Experience is enabled, Enterprise Connect Passwordless does not manage the password, and users need to replace the password according to enterprise policy. Once users change the password, they will again be required to enter it for the first login only.

The passwords set by users will be captured on the mobile app, and users will be able to view their passwords in the app.

To enable the Password Free Experience, some configuration needs to be done in the **enterprise-connect-passwordless.xml** file and in the Management Console.

XML File Configuration

To enable support for the Password Free Experience in Enterprise Connect Passwordless for Mac, the *passwordfree* parameter needs to be set to *true*.

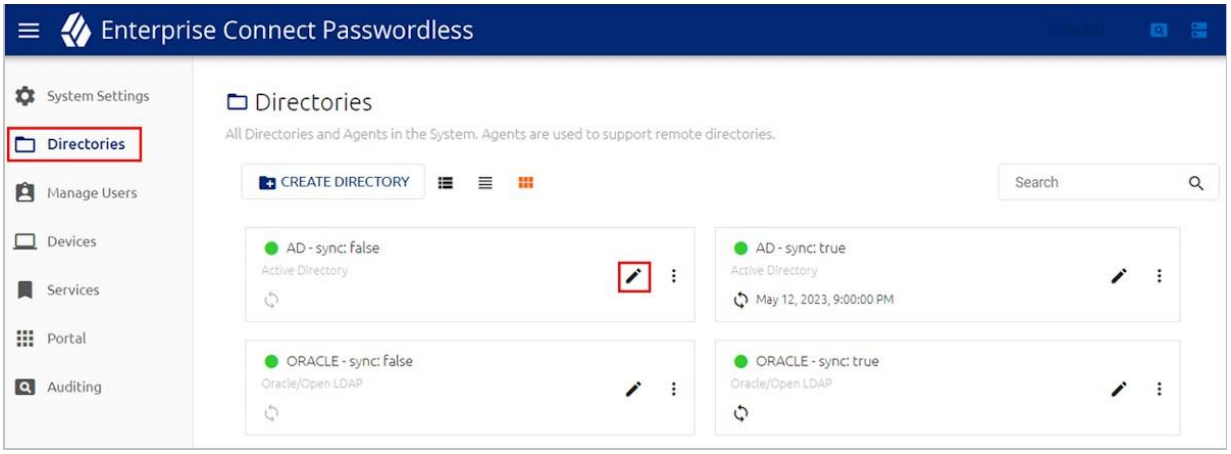
```
<!--
    Password Free Experience (default: 'false')

    The Password Free Experience enables customers to start deploying the Mac agent while maintaining control over the password, so they can continue to use it
    for other applications. In the Password Free flow, users will be required to enter the password for the first during the enable user process.
    After one successful login, all other authentication will be Passwordless until the user changes the password (per policy)

    Example:
        <passwordfree>true</passwordfree>
-->
<passwordfree>true</passwordfree>
```

For more information about configuration file parameters, refer to Configuring the XML File [8].

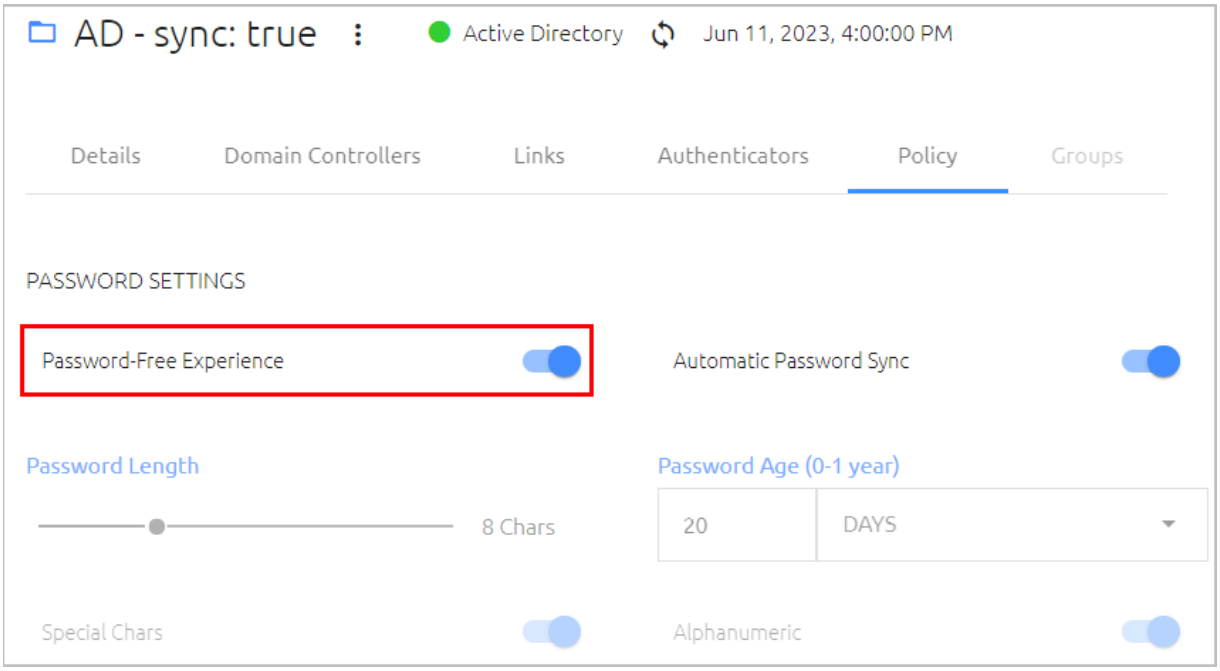
Management Console Configuration

To support the Password Free Experience, the **Password Settings** of the directory need to be configured correctly so the system does NOT rotate the AD password. The configuration required varies depending on whether Compatibility Mode is ON or OFF (as explained in the procedure below). For more information about Compatibility Mode, please refer to the Enterprise Connect Passwordless Management Console Admin Guide.

1. In the Management Console, select the **Directories** menu. Then, open the settings of the relevant directory by clicking  .

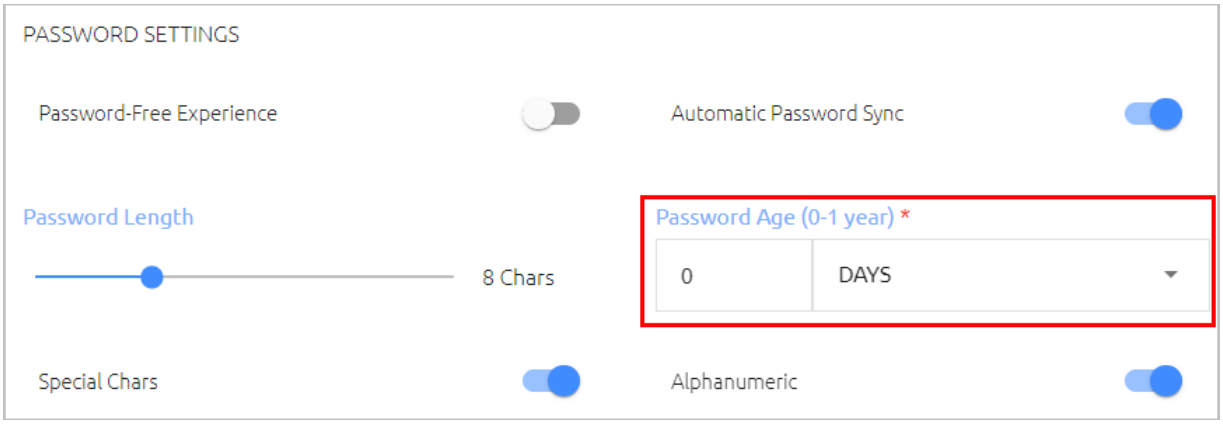


2. Select the **Policy** tab.
3. If Compatibility Mode is OFF, make sure that the **Password-Free Experience** toggle is enabled (blue).



Then, go to Step 5 (below).

4. If Compatibility Mode is ON, set the **Password Age** to **0**.

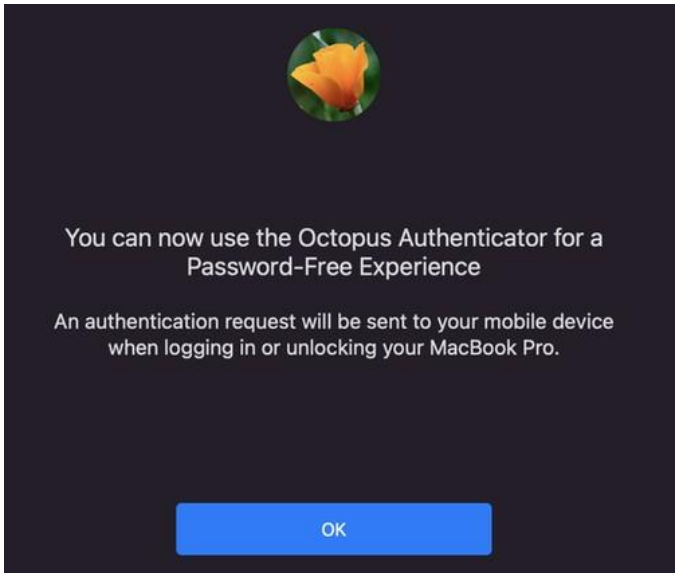


When the value is **0**, the system never rotates the password, and the password is managed directly on the directory or the AD.

5. At the bottom of the **Policy** tab, click **Save** and publish your changes.

Password-free Mode: User Experience

When the Password Free Experience feature is enabled, the following message is displayed upon installation of Enterprise Connect Passwordless:



In addition, the mode of the Agent is shown in the **Status** screen.

The user provides a password for the first login. This password is shared on the vault and sent to the mobile app. Until the next password change, users authenticate with a standard passwordless flow.

Enterprise Connect Passwordless never changes or manages the AD password when set to Password-free mode. Users can always change the password manually or according to AD policy. Once the password changes, users will again be required to enter it for the first login only. FIDO users will need to enter Password + PIN together when the password is changed locally.

Handling FileVault Login

When using Octopus Authentication, it is important that the FileVault Login password is different from passwords set for domain users and Local users. This allows rotation of the AD password (to enable passwordless authentication) without affecting the FileVault Login password.

Enterprise Connect Passwordless for Mac supports the following configurations for FileVault login:

- **Server configuration:** The FileVault Login password is set and automatically managed by the system. The password is rotated when the system rotates the user password (AD password). New passwords are stored on the Server Vault and sent to the user as necessary on an enrolled mobile device.
- **Client configuration:** The FileVault Login password is set and managed by the Mac user.

The configuration is set before installation, in the *filevaultlogin* parameter of the **enterprise-connect-passwordless.xml** file (Configuring the XML File [8]).

```
<!-- ********************************************************************************** -->
<!-- ***  FILEVAULT LOGIN                                                           *** -->
<!-- ********************************************************************************** -->

<!--
    FileVault Login (default: 'client')

    Determines the mode of operation for the FileVault Login feature. When set to the
    default value of 'client' the user can create their own password for FileVault Login.
    When set to 'server' the password will be created and managed by the server.

    The valid values for this setting are:
        * client
        * server

    Example:
        <filevaultlogin>server</filevaultlogin>
-->
<filevaultlogin>client</filevaultlogin>
```

The following sections describe the workflows for setting up and handling FileVault login:

- Enabling FileVault Login [28] (All Configurations)
- Configuring FileVault Login on the Mac [32] (Client Configuration)
- Working with the FileVault Password [34] (Server Configuration)

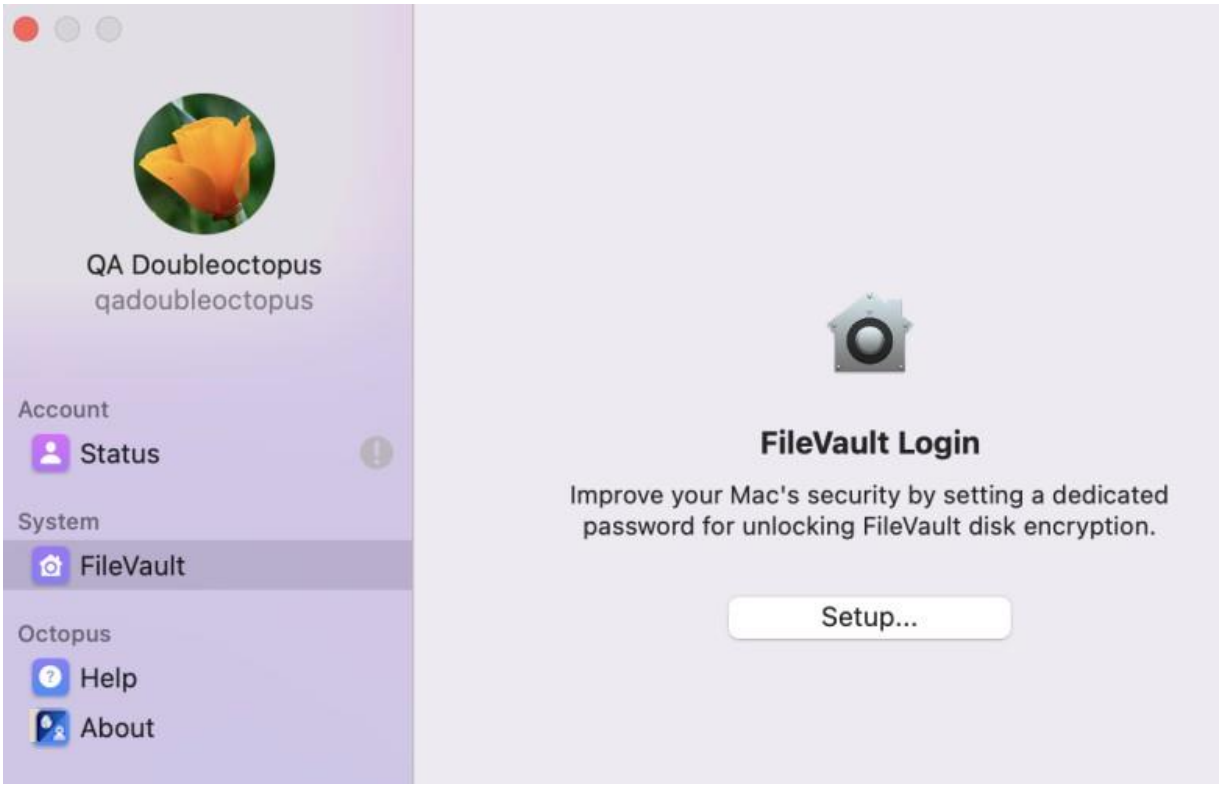
Enabling FileVault Login (All Configurations)

Follow the steps below to enable FileVault Login and set the password.

Important: If you are working with the Server configuration, the procedure needs to be done by a system admin.

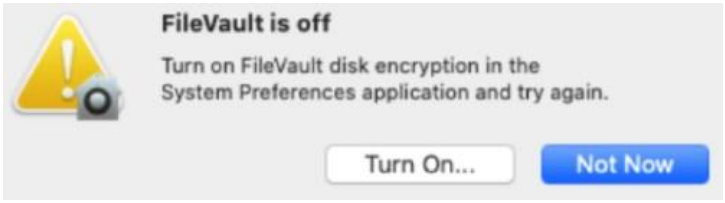
To enable FileVault login:

1. From the app configuration, select **FileVault** and click **Setup**.



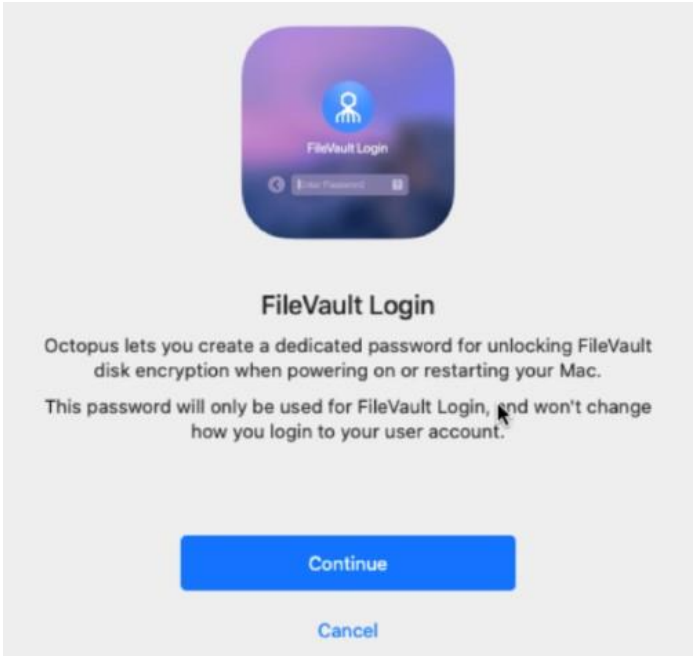
If FileVault is turned on, skip to Step 3.

2. If FileVault is turned off, the following popup opens:



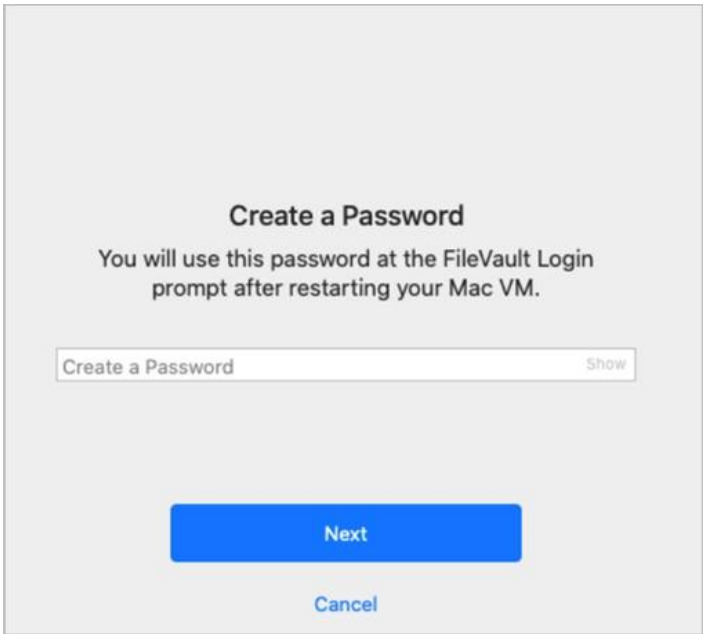
Click **Turn On** and then enable FileVault in the **Security & Privacy** settings.

3. From the **FileVault Login** dialog, click **Continue**.



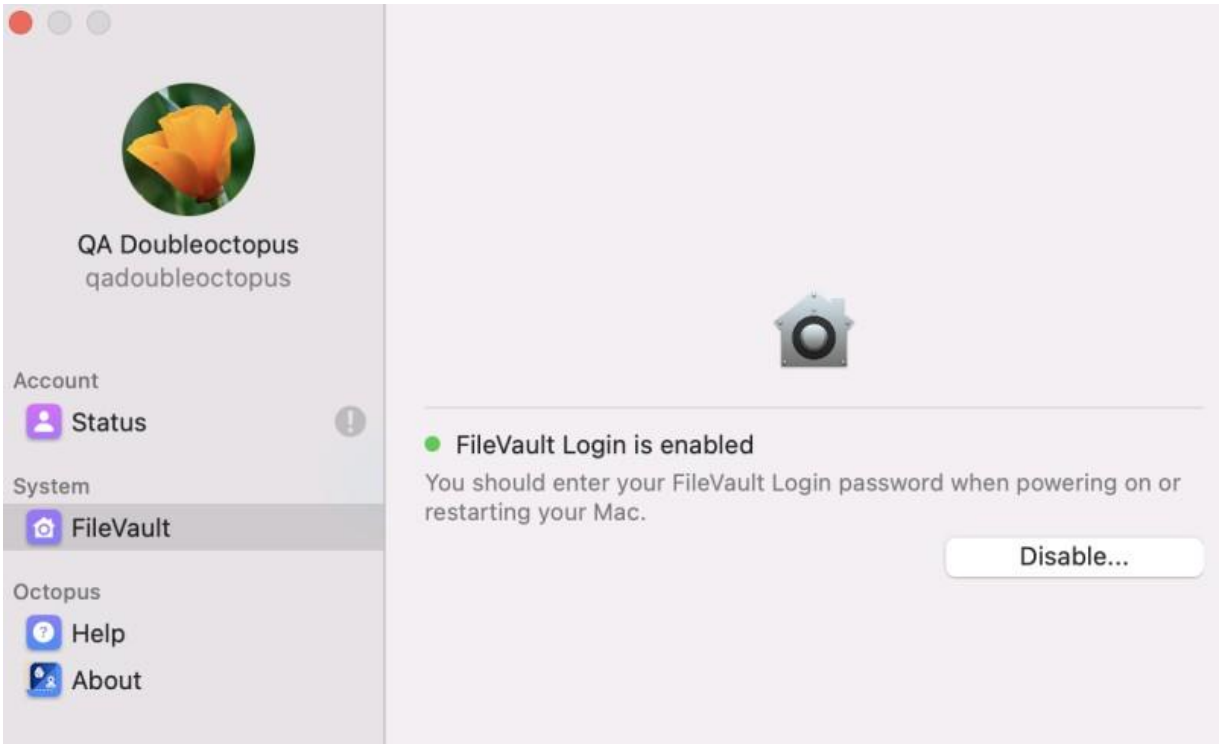
The **Create a Password** dialog opens.

4. Enter a password for FileVault Login, and then click **Next**.



A confirmation message is displayed on the Mac.

After successfully enabling FileVault Login, the app configuration will appear as follows:

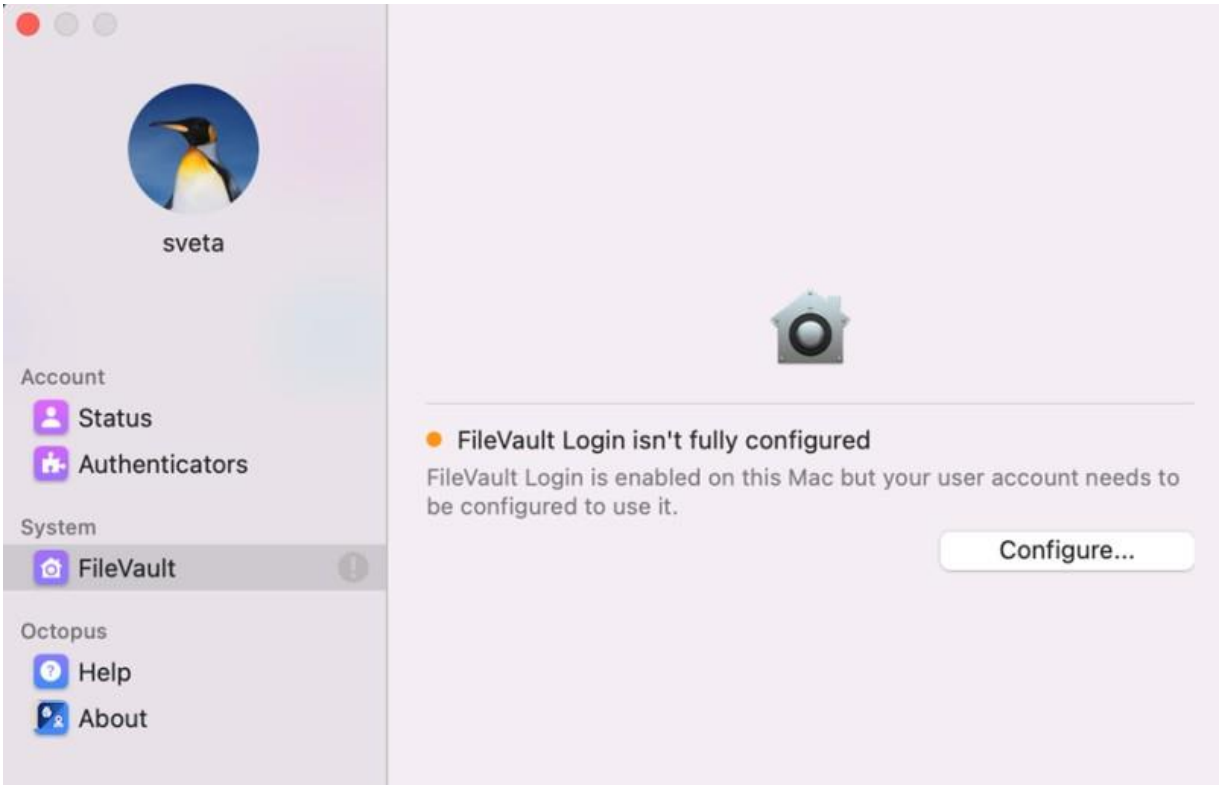


Configuring FileVault Login on the Mac (Client Configuration)

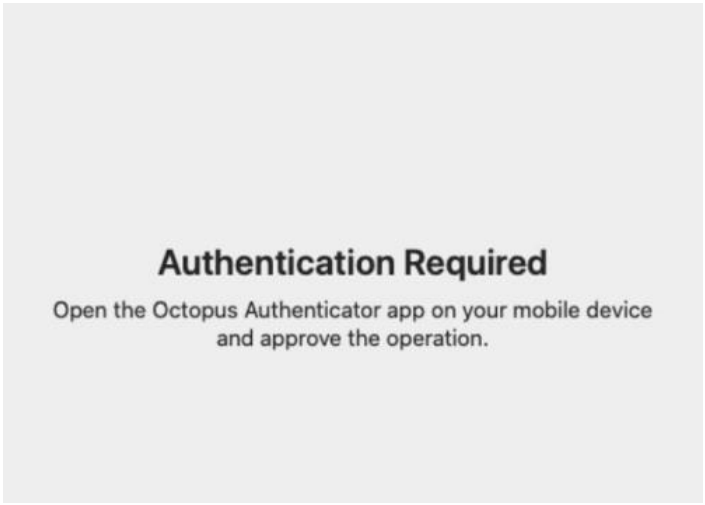
When the Client configuration is used, the user account needs to be configured manually in order to successfully use FileVault Login.

To configure FileVault Login:

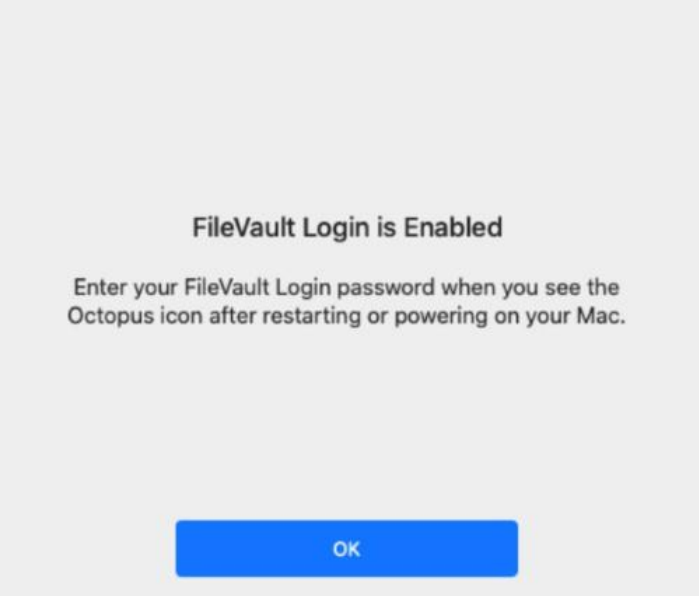
1. From the app configuration, select **FileVault** and click **Configure**.



A message is displayed prompting you to approve the operation on your mobile device.



2. From the Authenticator mobile app, tap **Approve**.
   A confirmation message is displayed on the Mac.



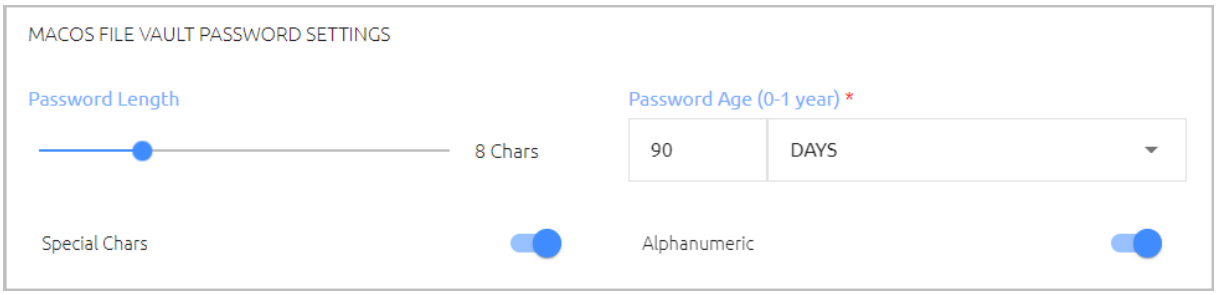
Working with the FileVault Password (Server Configuration)

When the Server configuration is used, FileVault Login is automatically enabled and configured for local users, and no additional setup procedures are necessary. When passwords are rotated by the system, they are sent to the user on an enrolled mobile device. The passwords are displayed in the Octopus Authenticator app on the **Show Credentials** screen (**Account > Show Credentials**).

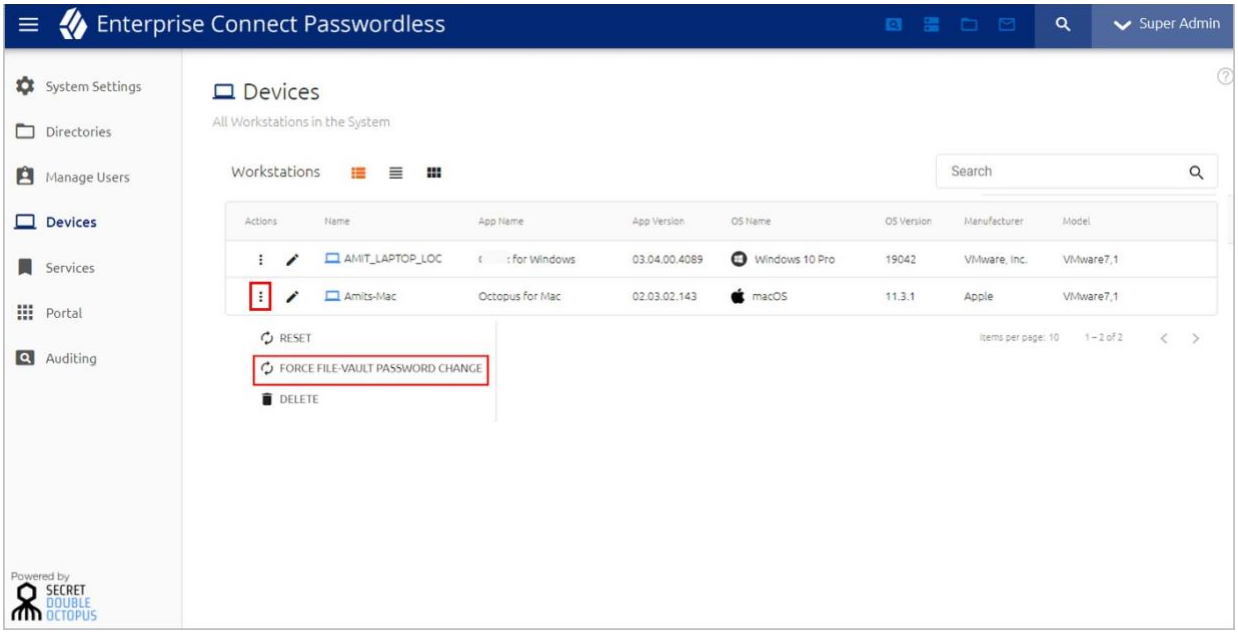
Managing the FileVault Password

The following settings and actions related to the FileVault password are available in the Management Console:

- **macOS FileVault Password Settings:** These settings (in **System Settings > Devices**) allow the admin to set the password's length, expiration time and other requirements.



- **Force FileVault Password Change:** Enables the admin to initiate an immediate password rotation. This setting is found in several locations in the Management Console.



For more information, please refer to the Enterprise Connect Passwordless Management Console Admin Guide.

Working with Kerberos Tickets

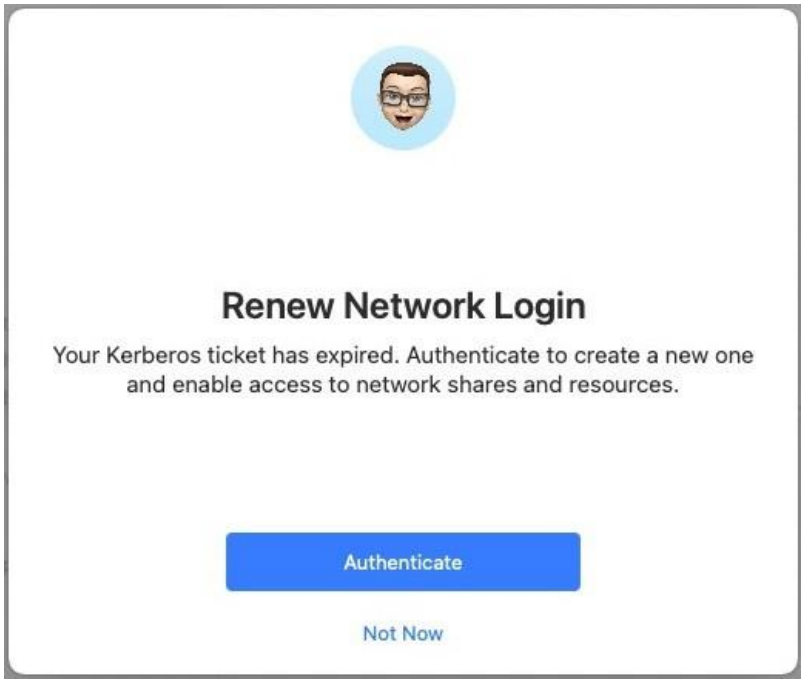
A Kerberos ticket is created when users log into the Mac or perform Lock screen authentication and is renewed automatically. The ticket allows users to authenticate with Kerberos SSO to all internal web applications and shared repositories that require user authentication to Active Directory.

Important: To enable Kerberos authentication, the following conditions are required:

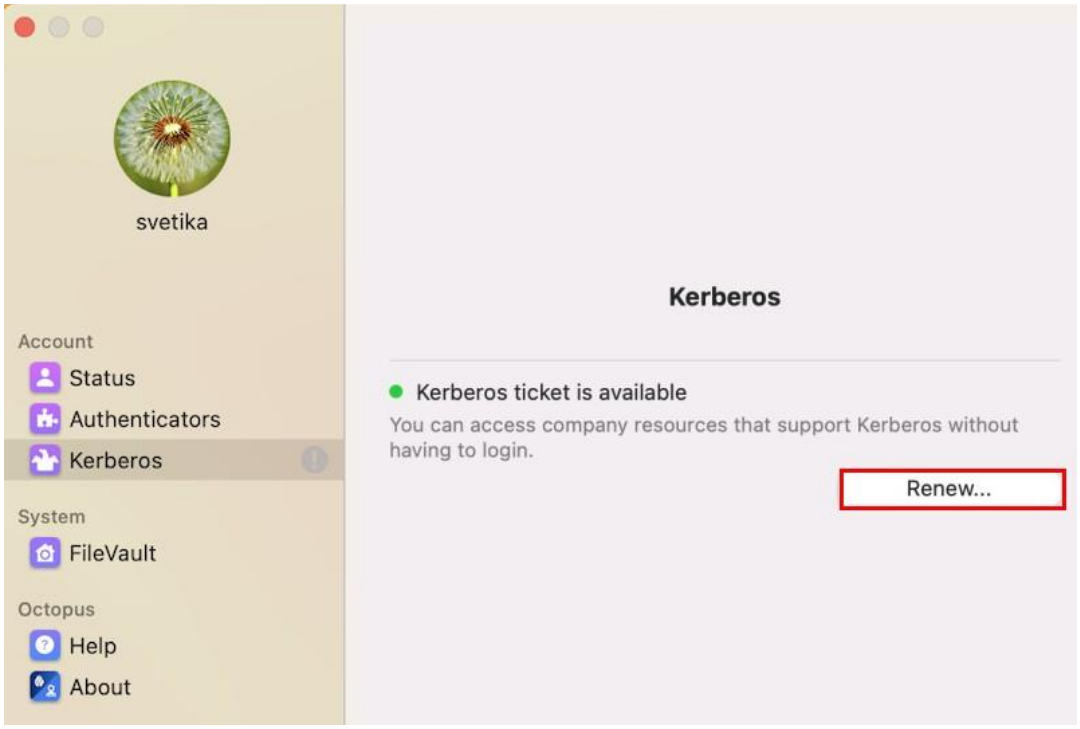
- The *kerberosrealm* parameter must be defined in the **enterprise-connect-passwordless.xml** file. For details, refer to Configuring the XML File [8].
- The workstation must be domain-joined. For details, refer to Adding Your Machine to the Active Directory [46].

Renewing the Ticket

If the Kerberos ticket is expired, the following popup opens, allowing users to renew it:



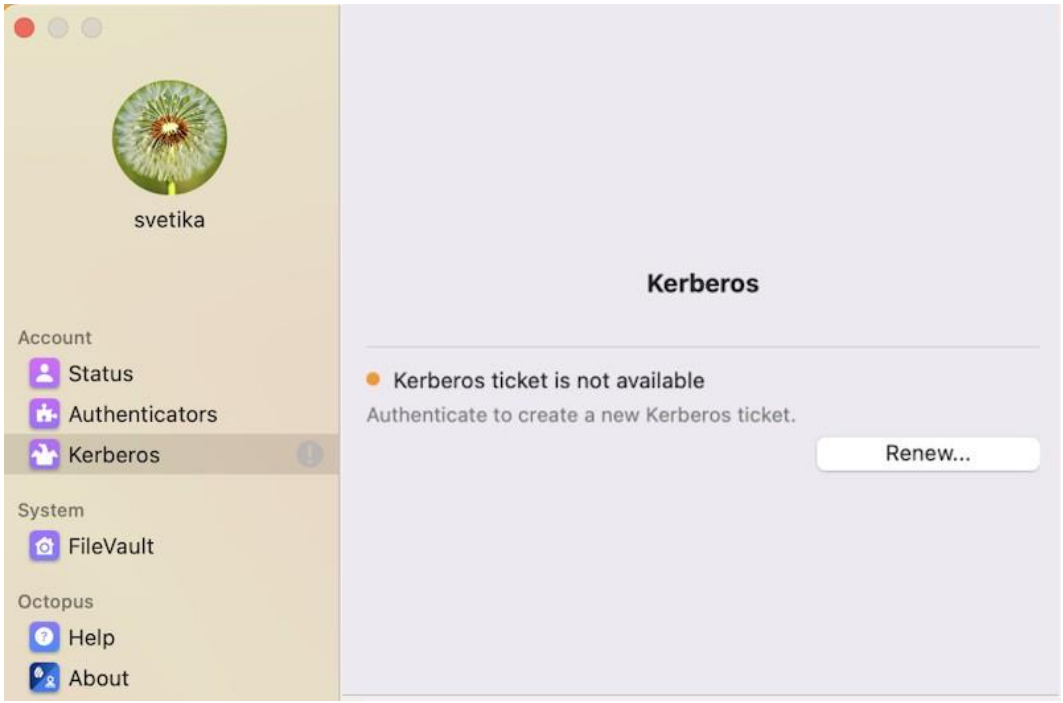
Users can also renew the ticket manually at any time, either from the app options menu or from the Enterprise Connect Passwordless Preferences.



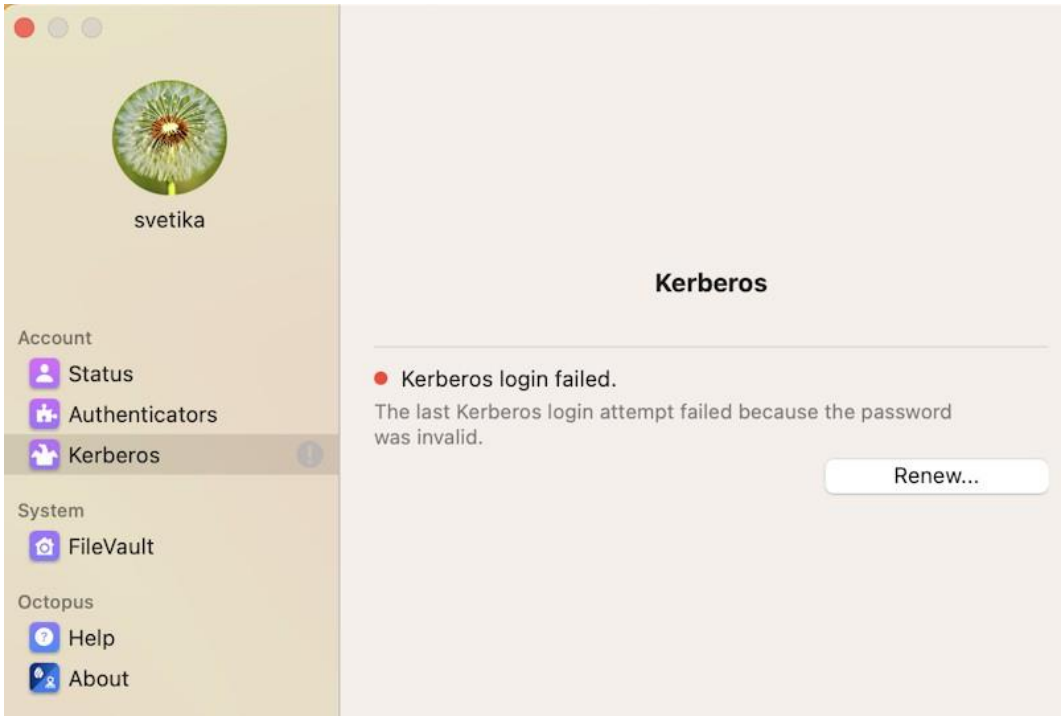
Viewing Kerberos Ticket Status

The current status of the Kerberos ticket is displayed in the Kerberos menu of the Enterprise Connect Passwordless Preferences. An active ticket is indicated by a green icon, as shown in the example above.

If the ticket needs to be renewed, the icon is orange.



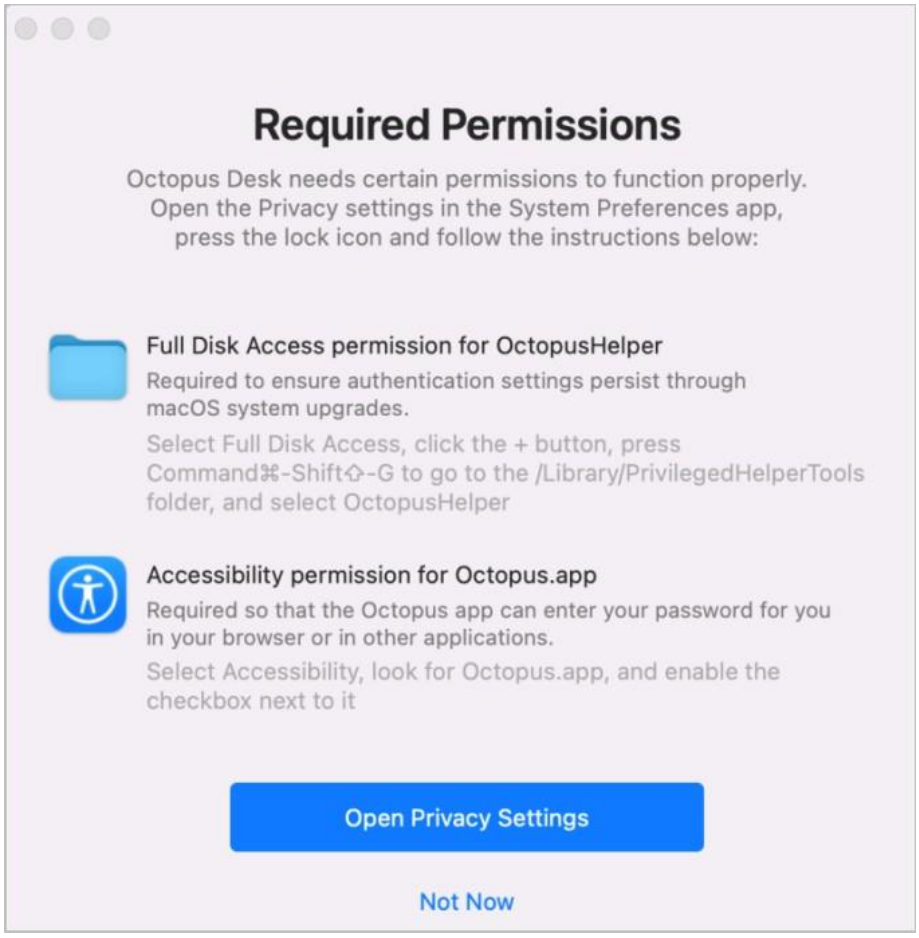
A red icon indicates that the most recent Kerberos login failed. The cause of the login failure is described below the status.



Configuring Access Permissions in macOS Monterey

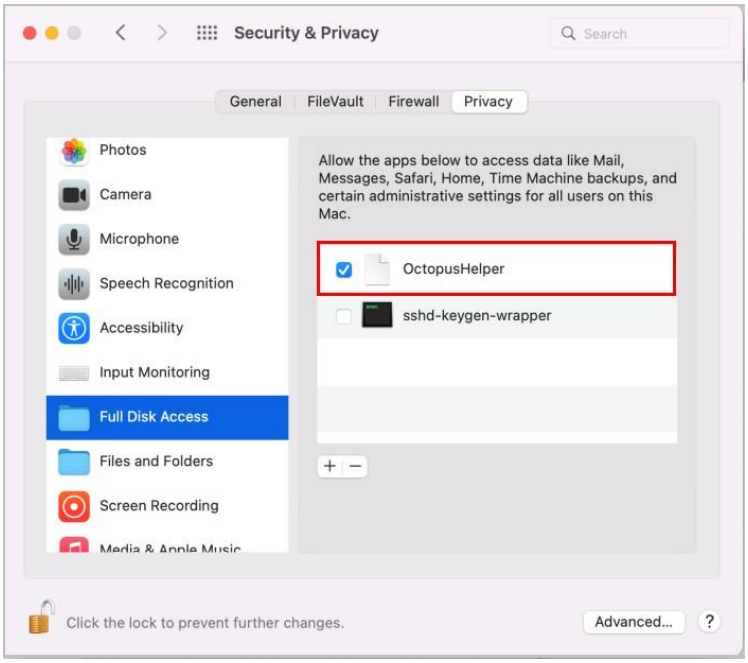
When installing or upgrading Octopus Desk for Mac on macOS Monterey, or when the Mac is upgraded to Monterey from another operating system, required permissions need to be configured manually to enable successful installation / upgrade of Octopus Desk.

When this issue occurs, the following popup will open:

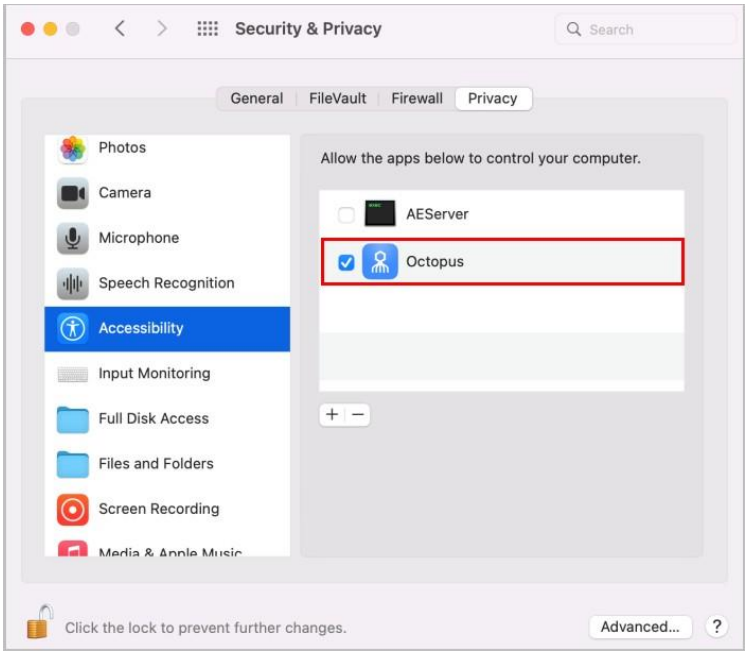


To enable successful completion of the installation / upgrade process, configure the following permissions:

- Enable **Full Disk Access** permissions for OctopusHelper, as shown in the figure below.

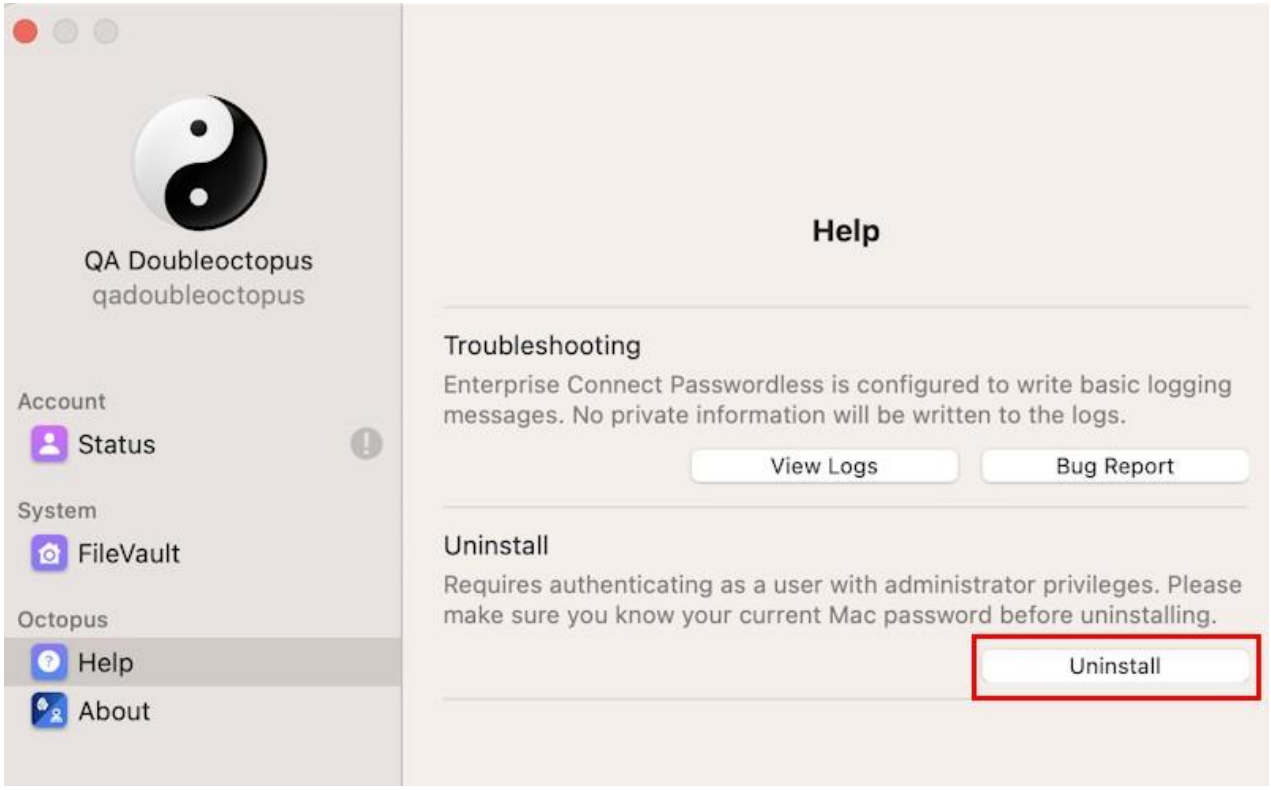


- Enable **Accessibility** permissions for Octopus.app, as shown in the figure below.



Uninstalling the Mac Client

If it becomes necessary to uninstall the client, you can remove it directly from the Enterprise Connect Passwordless Preferences. Click the app icon on the top bar and select the **Help** menu. Then click **Uninstall**.



If the FileVault Login feature is enabled, you will be prompted to disable it before continuing the uninstallation process.

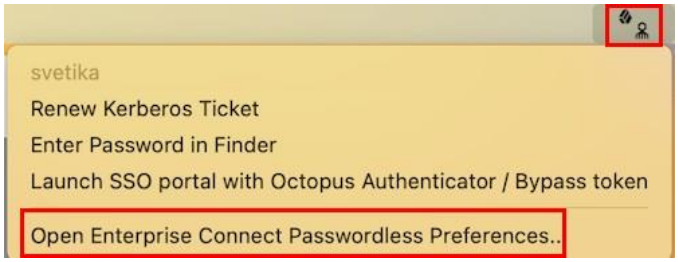
To disable FileVault Login:

1. From the **Status** menu, disable Enterprise Connect Passwordless.
2. Open the **FileVault** menu and click **Disable**.
   If you haven't yet disabled Enterprise Connect Passwordless, you will be prompted to do so now.
   If the app is currently being used by another user, follow the instructions in the warning popup:

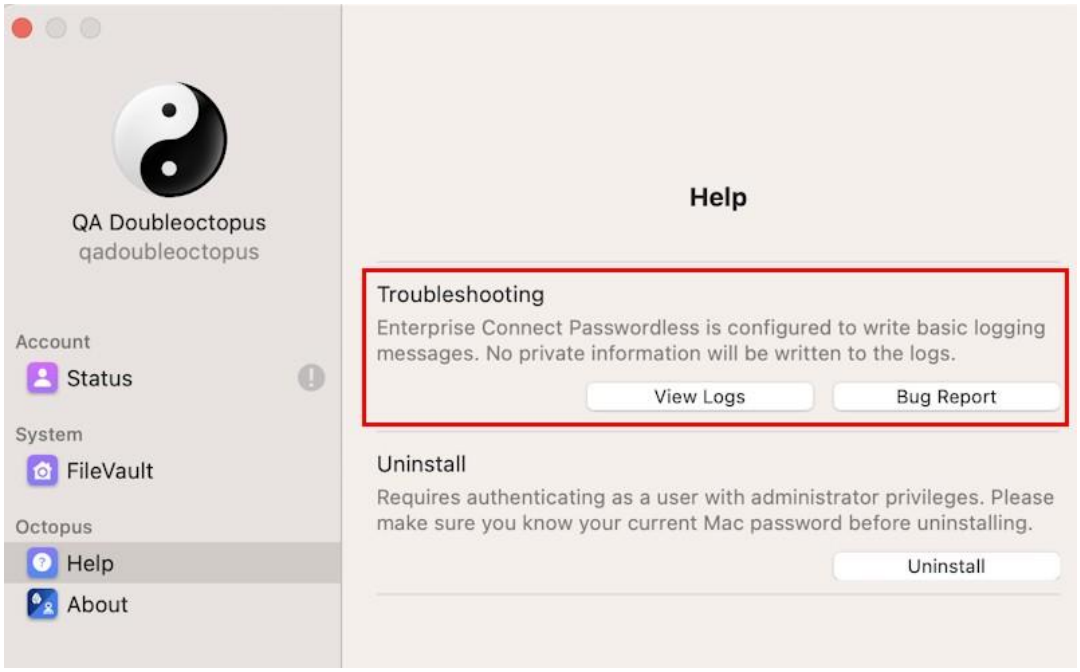
After both Enterprise Connect Passwordless and FileVault Login have been disabled, you will be able to proceed with uninstallation.

Troubleshooting

When Enterprise Connect Passwordless is not operating as expected and assistance is required, users can utilize the built-in troubleshooting options. To access these options, click the app icon and select **Open Enterprise Connect Passwordless Preferences**.



Then, select the **Help** menu.



The following troubleshooting options are offered:

- **View Logs:** Displays the Octopus Desk logs in a new window
- **Bug Report:** Opens a new email message with the log files automatically attached. By default, the message is sent to <feedback@doubleoctopus.com>

Appendix A: Mac User Experience

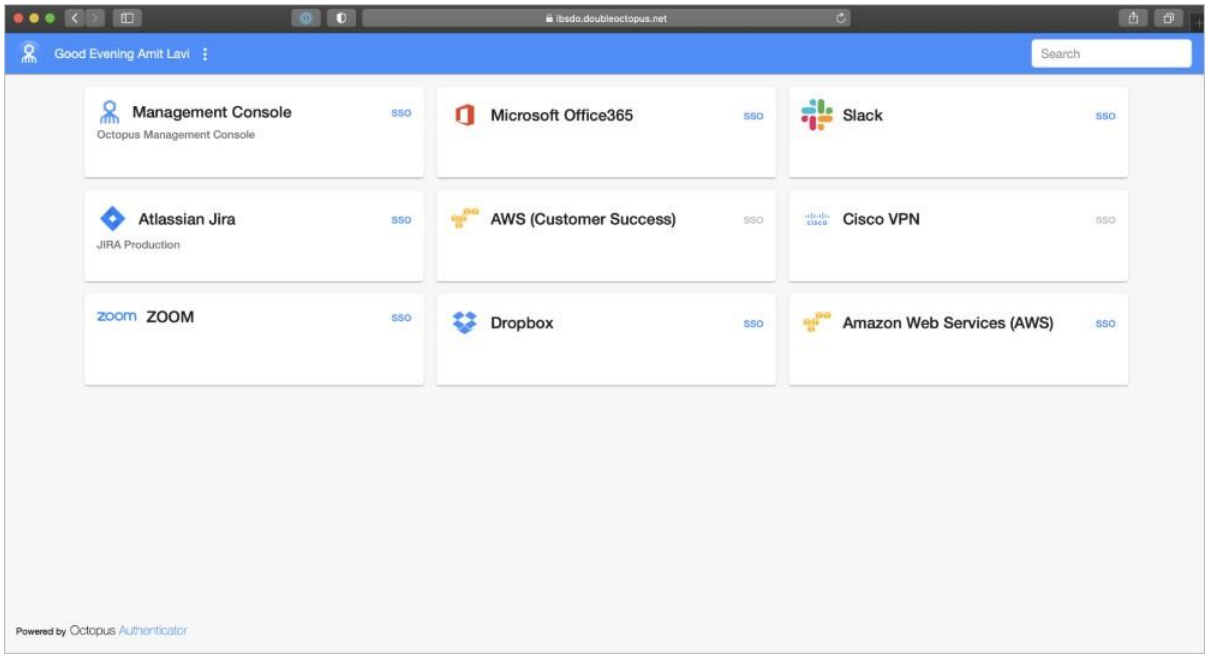
The following sections present various scenarios related to user experience:

- Accessing the User Portal [45]
- Updating System Preferences [45]
- Adding Your Machine to the Active Directory [46]

Accessing the User Portal

Enterprise Connect Passwordless for Mac supports automatic launch of the SSO portal in a browser window after user login to the machine.

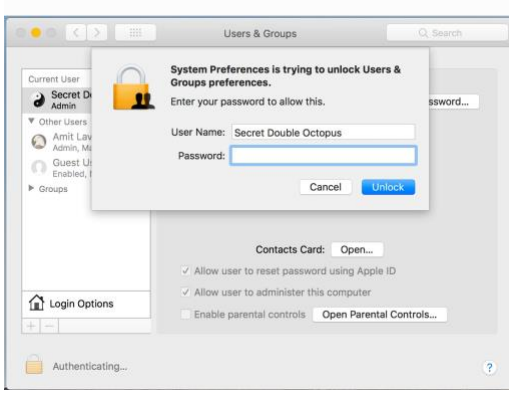
If the *ssourl* parameter of the configuration XML file is defined, that URL is used. (Configuring the XML File [8].) If that parameter is empty, the target URL is taken from the Authentication Server.



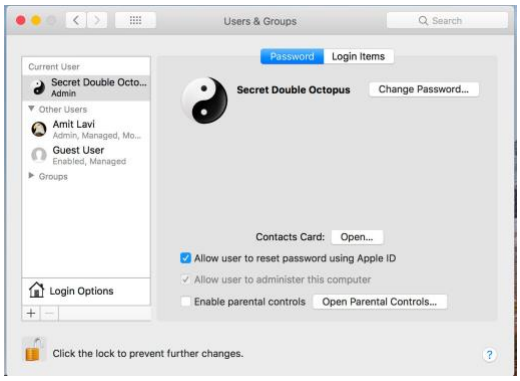
Updating System Preferences

Octopus Authentication is enabled on all System Preferences settings for which authentication is required.

To unlock the preferences, the user press the Lock icon, enters the password and approves the authentication operation on the Octopus Authenticator mobile app.



After successful authentication, the Lock icon opens and the user may update System Preferences.

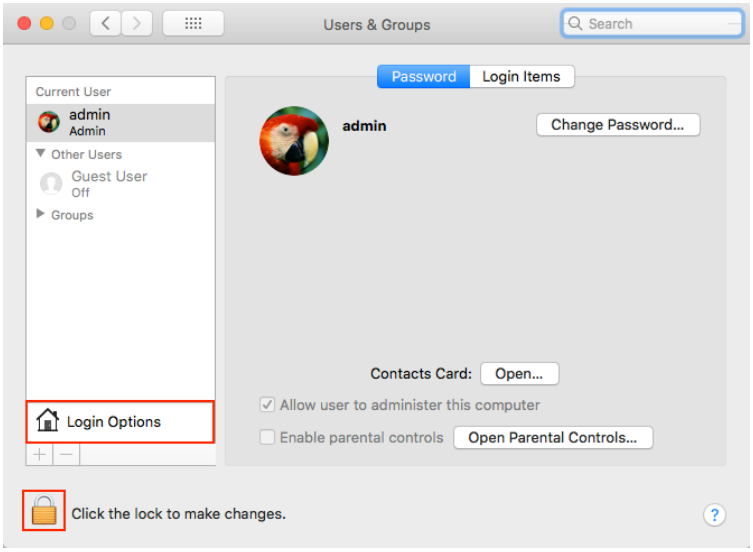


Adding Your Machine to the Active Directory

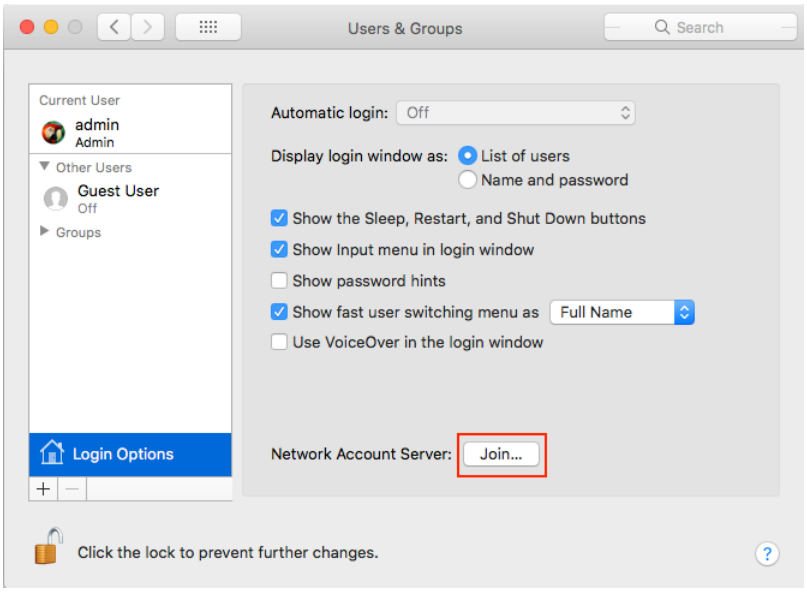
The following procedure describes how to add your Mac to the corporate Active Directory.

To add your machine to the AD:

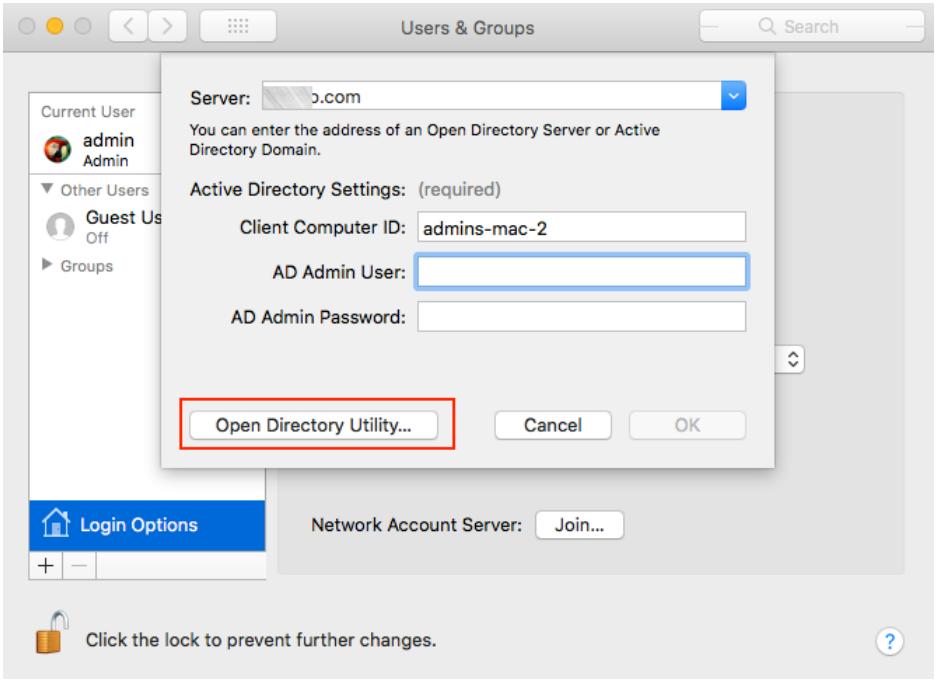
1. Open **System Preferences** and select **Users & Preferences**.
   The **Users & Preferences** dialog opens.
2. Click the Lock icon to enable editing mode. Then, click **Login Options**.



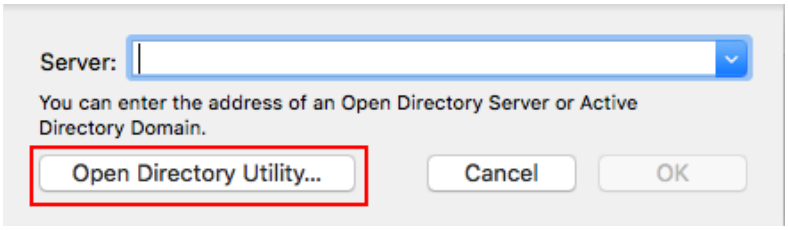
3. Next to **Network Account Server**, click **Join**.



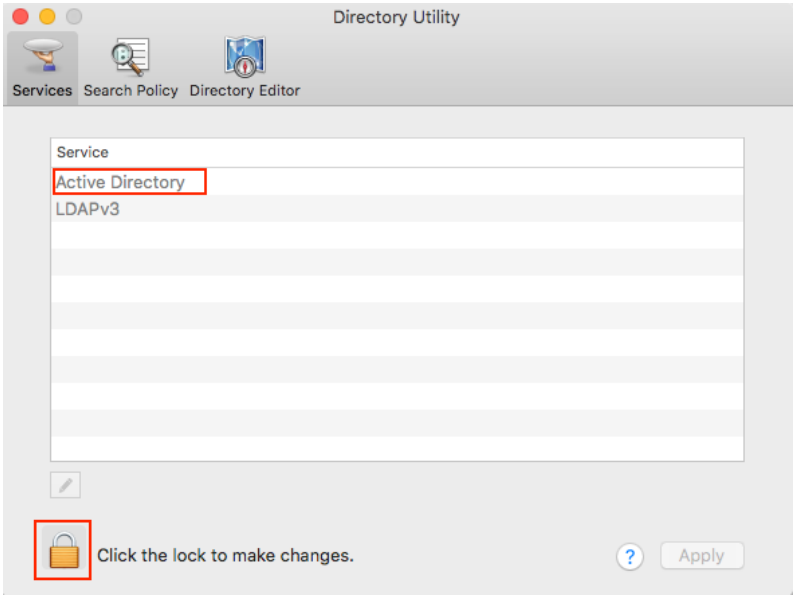
4. In the popup that opens, enter the address of the AD server and the credentials of the AD Admin. Then, click **Open Directory Utility**.



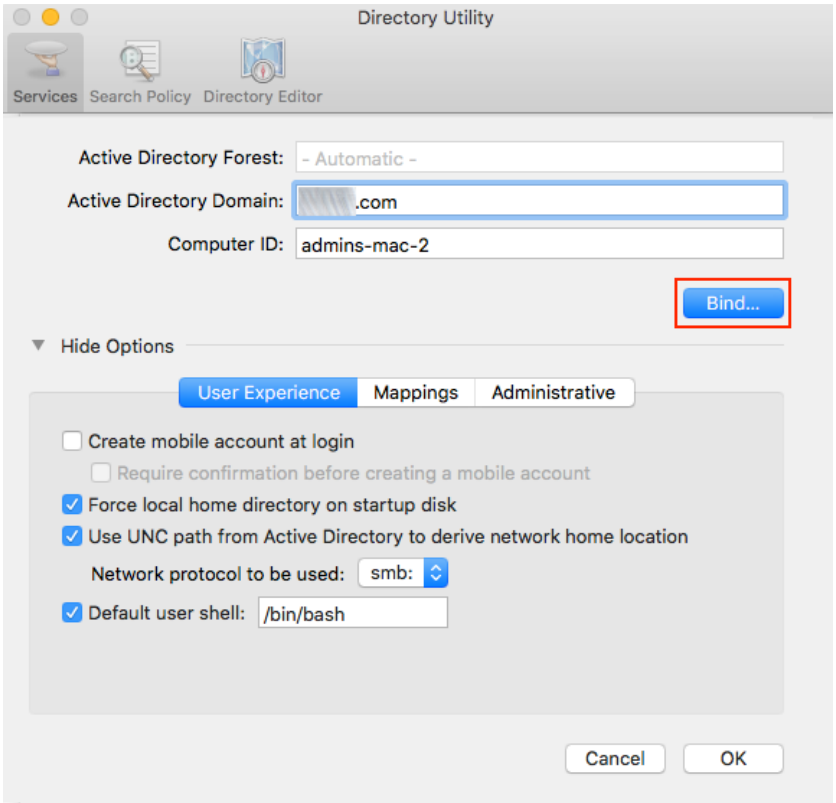
5. In the second popup that opens, re-enter the address of the server and then click **Open Directory Utility**.to open the **Directory Utility** dialog.



6. From the **Directory Utility** dialog, click the Lock icon to enable editing mode. Then, select **Active Directory**.

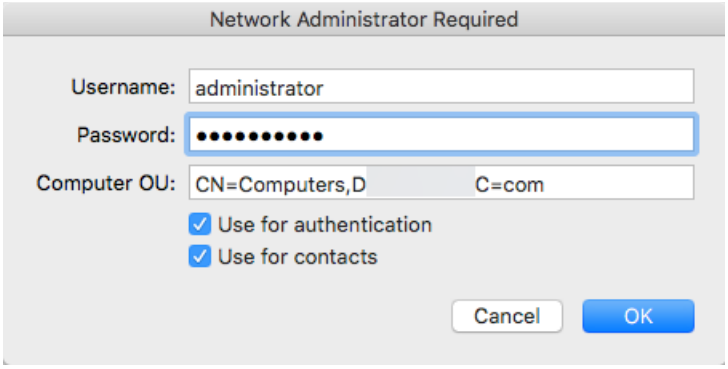


7. In the dialog that opens, click **Bind**.



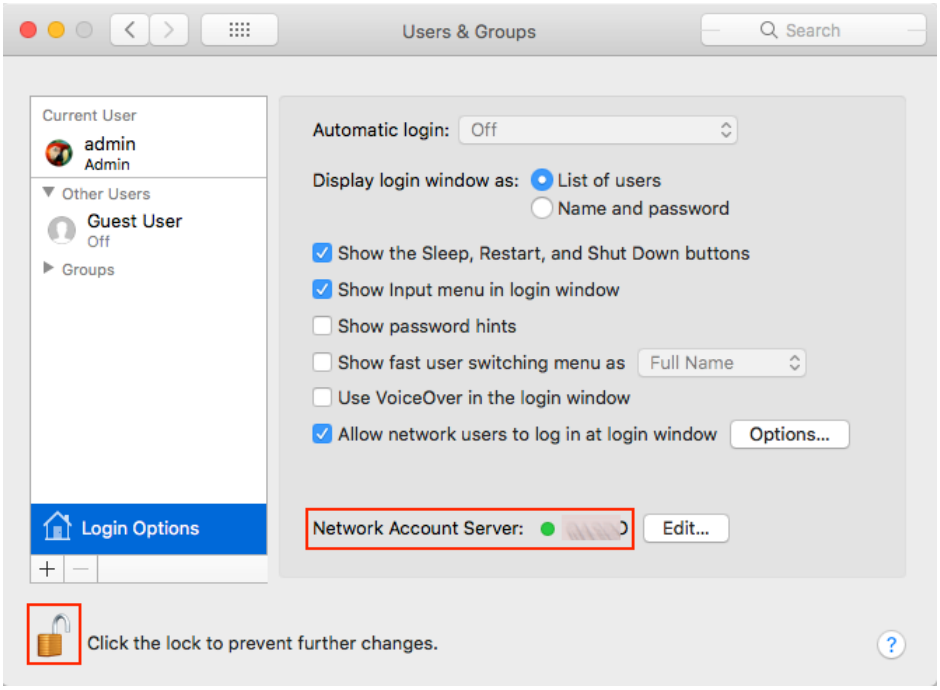
The **Network Administrator Required** popup opens.

8. Enter the credentials of the AD Admin and then click **OK**.



The popup closes. In the **Users & Groups** dialog, the name of the AD server is displayed as the Network Account Server, and a green LED indicates a successful connection.

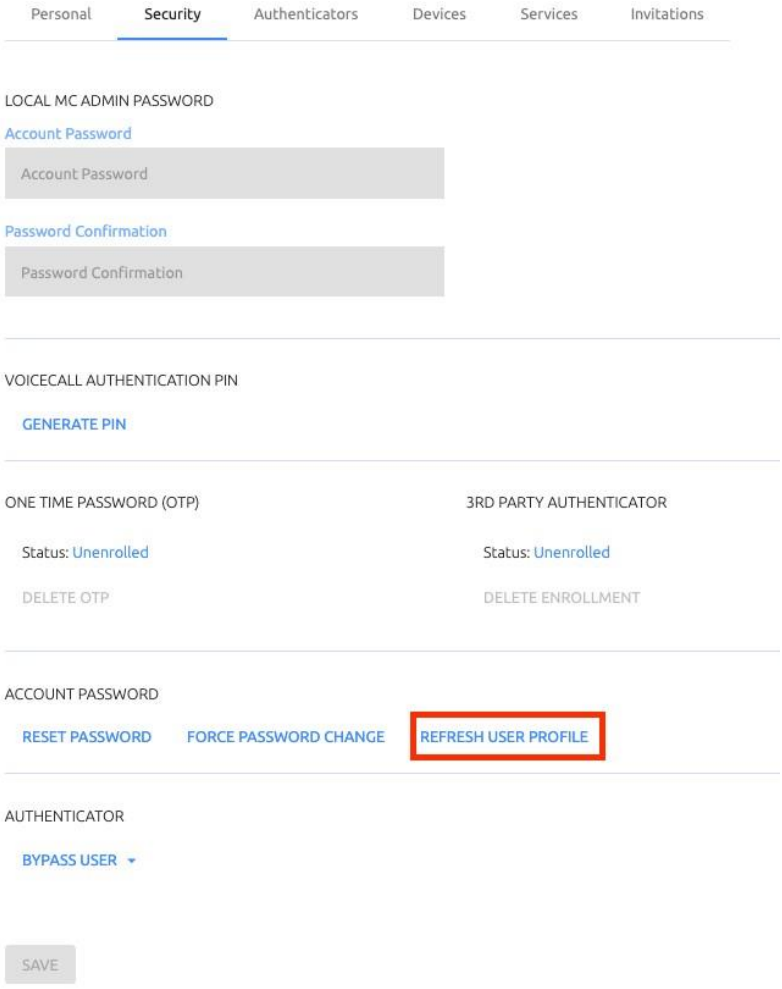
9. Click the Lock icon to disable Edit mode.



Appendix B: Known Issues

The following issues, discovered during software testing, will not be resolved in version 2.6.7:

- **Refresh User Profile** does not work for Local users: This option, in the **Security** tab of the user details in the Management Console, does not work properly on the Mac. Clicking **Refresh User Profile** deletes the password history, and the correct local password will not be successfully retrieved to the Mac.
  Mac users are advised not to use this option.



- **Jamf policy issues:** In some cases when Jamf is installed on the Mac, Enterprise Connect Passwordless for Mac is unable to sync the password. Users may need to disable Jamf password policies in order to resolve this issue.
- **BLE issues:** BLE authentication can be used to unlock the Mac but does not work as expected for login.
- **sudo for Bypass users:** A password is currently required for users in Bypass mode to run sudo.