Enterprise Connect Passwordless for Mac Installation Guide

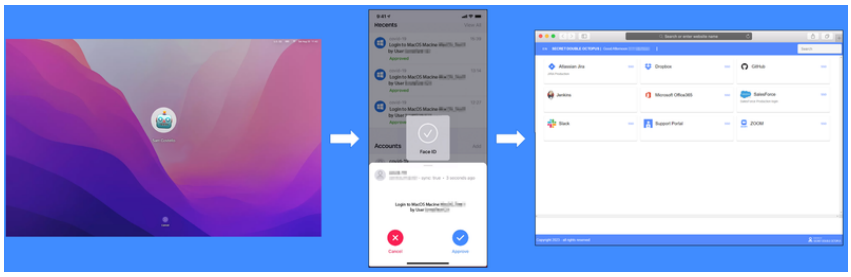
Version 4.3

Preface

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

Product Overview

Enterprise Connect Passwordless 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 Sonoma
- macOS Sequoia
- macOS Ventura

Before beginning installation, verify that:

- Enterprise Connect Passwordless Authentication Server **version 6.4.2** (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 PingID authenticator or FIDO.

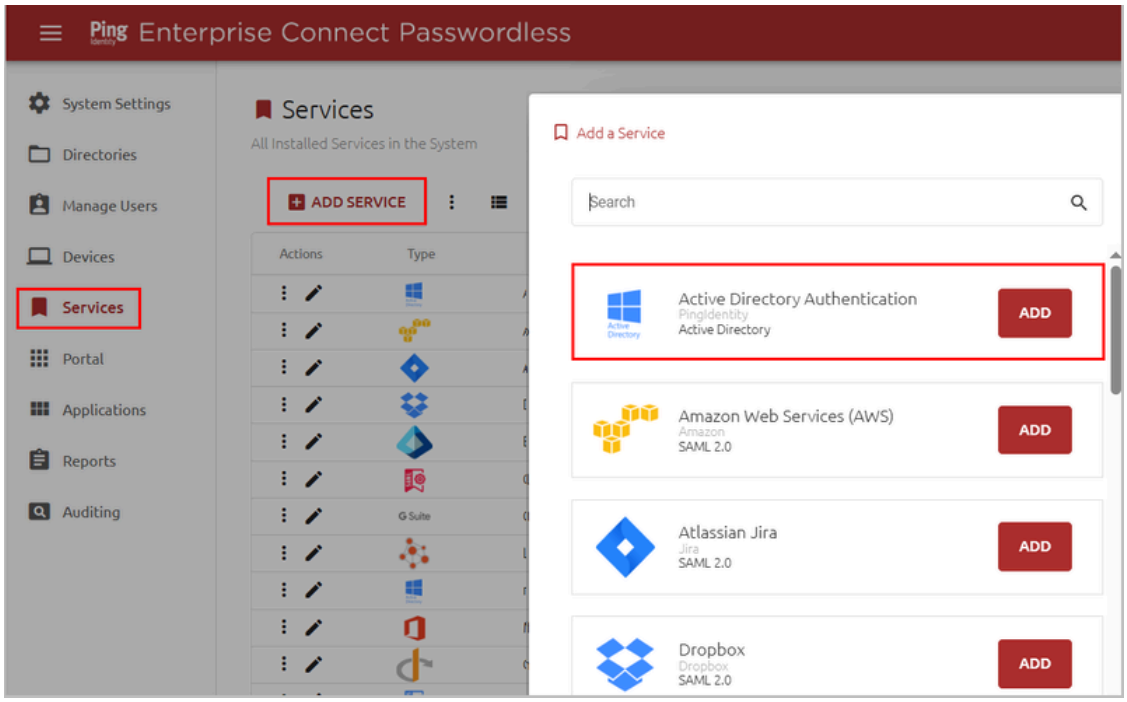
Creating the Active Directory Authentication Service

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.

IMPORTANT: Before starting this procedure, verify that you have integrated your Corporate Active Directory or ForgeRock directory with the Management Console. Refer to the Management Console Admin Guide for detailed instructions on integrating Active Directory and other directory types.

To create the Active Directory Authentication service:

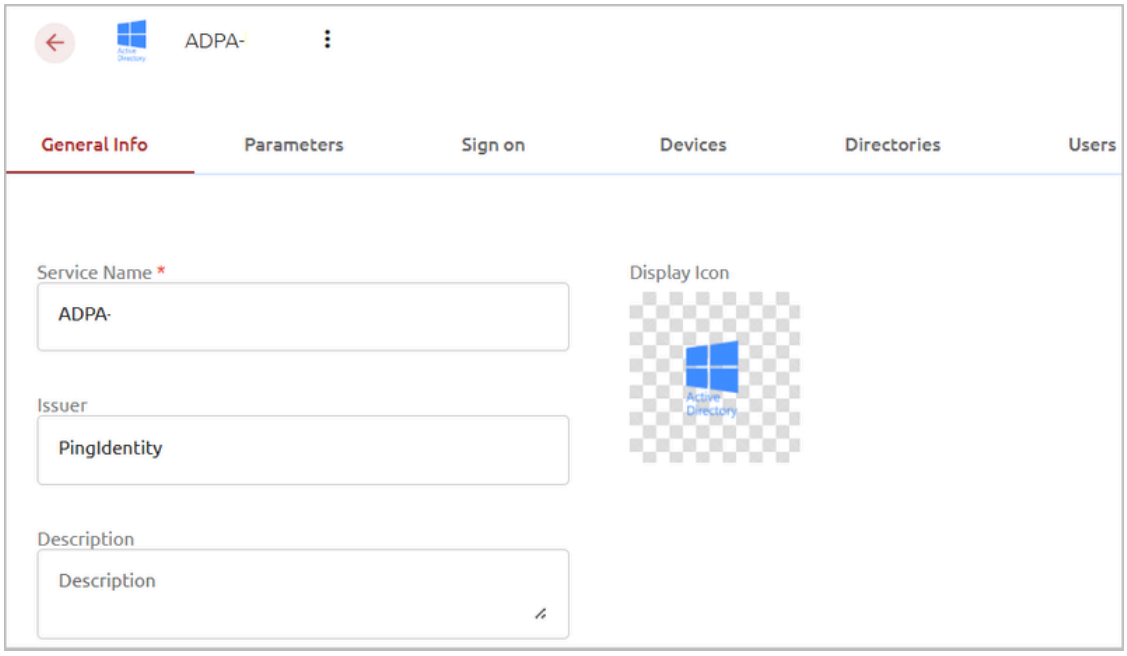
1. From the Management Console, open the **Services** menu and click **Add Service**.
2. In the **Active Directory Authentication** tile, click **Add**.



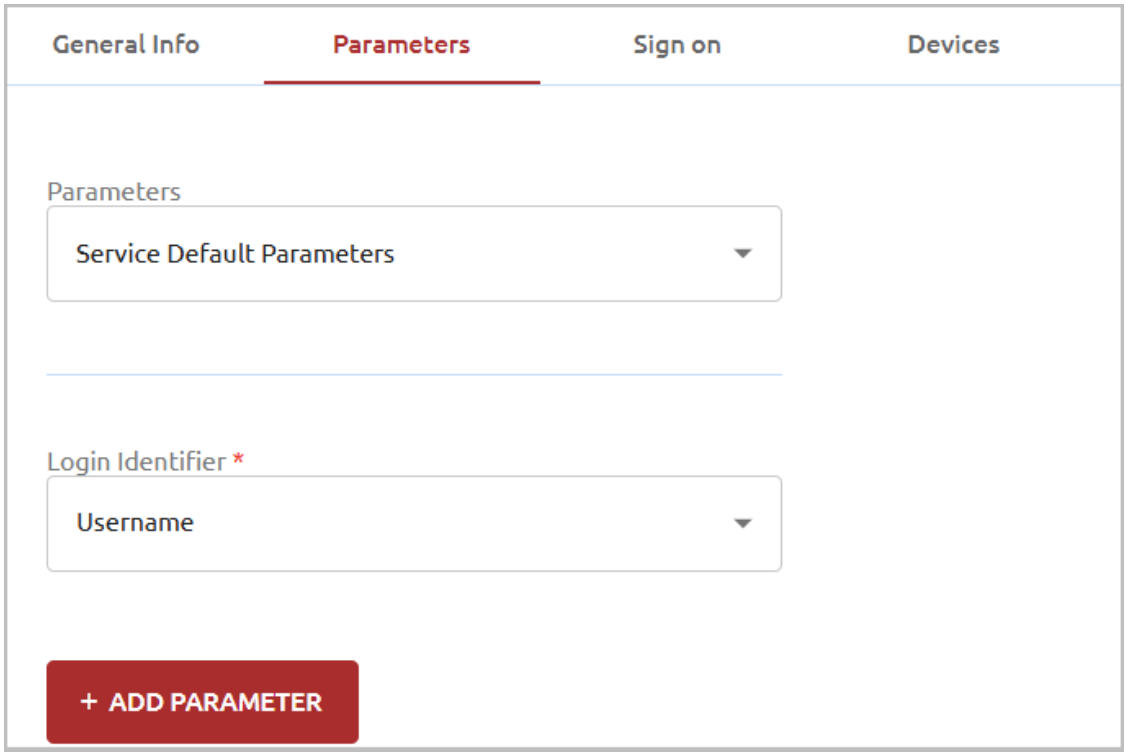
Then, in the dialog that opens, click **Create**.

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 128x128 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** for AD and **UPN** for Entra ID).

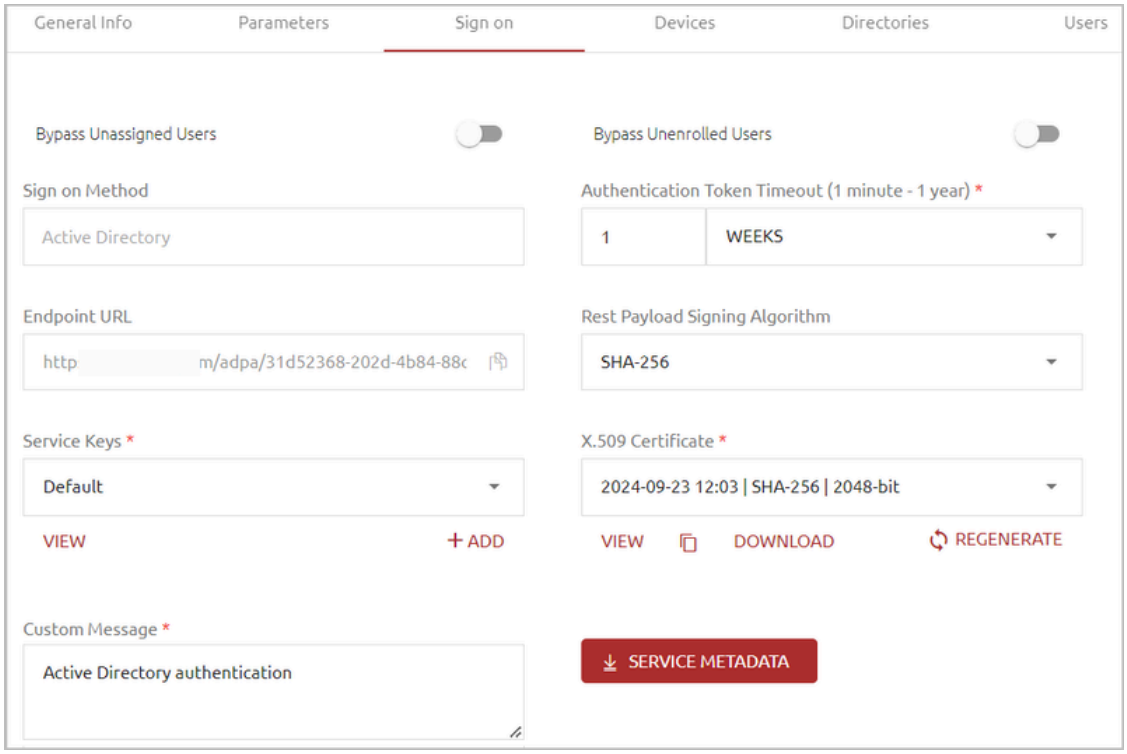


Then, click **Save**.

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 via the Authentication Server. The following options are available: • Click **View** to open a popup from which you can view and copy all active service keys.

Setting	Value / Notes
	● Click **Add** to create a new service key. For more information about service keys, refer to the Management Console Admin Guide.
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**. **Note:** SHA-1 is not supported for Red Hat Enterprise Linux 9.3.
X.509 Certificate	The public certificate used for authentication. ● Click **View** to display the content of the certificate in a popup. The popup provides both Copy and Download options. ● 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. 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
- Installing the Mac Client
- Onboarding Local Users

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 sa me name.

Configuring the XML File

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

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

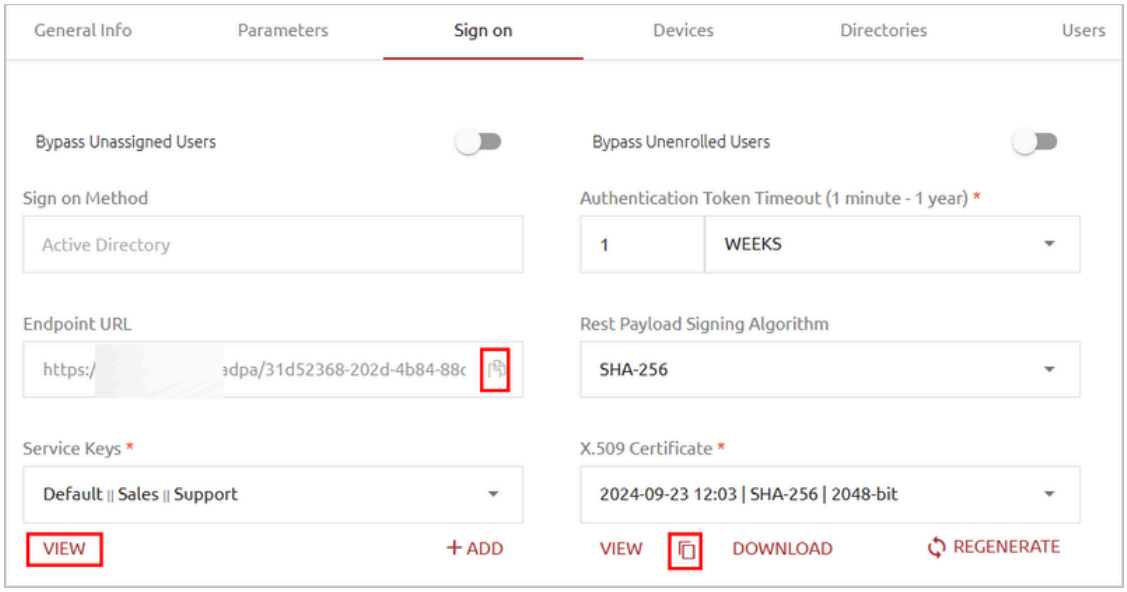
Mandatory Parameters

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

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.



Optional Parameters

The following additional parameters may be defined or updated, as required:

Parameter Name and Syntax	Description	Example / Notes
Features		
sudo	Enables/ Disables authentication on command line sudo. Default value is *false* (disabled).	*<sudo>true</sudo>*
kerberosrealm	When this parameter is defined, a Kerberos ticket is retrieved automatically upon login / unlock, and the **Kerberos** menu appears in the Enterprise Passwordless Preferences. The value should be the organization domain name in all uppercase letters.	*<kerberosrealm>ACMECORP.COM</ kerberosrealm >*

automatickerberossync	When set to *true* (default value), Kerberos tickets renew automatically as long as the user is logged into the workstation.	*<automatickerberossync>true</automatickerberossync>*
Authentication		
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>*
validPasswordIsSufficientForOffline	Determines whether users will be able to log into / unlock **offline** machines using standard password login.	*<validPasswordIsSufficientForOffline>true</validPasswordIsSufficientForOffline>*
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. *<mfa>true</mfa>*
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>*
passwordfree	Enables/Disables the Password Free Experience. Default value is *false* (disabled).	When the Password Free Experience is enabled, users deploy the Mac agent while maintaining control over the password. After the first login, all authentication is Passwordless. *<passwordfree>true</passwordfree>*

Single Sign On		
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 *<ssobrowser>firefox</ssobrowser>*
Password Sync		
autoPasswordSync	When set to *true* (default value), passwords are automatically synced when the server rotates the user's password. Auto password sync occurs in both login and unlock operations. When the value is set to *false*, users are presented with the sync password popup screen.	*<autoPasswordSync>true</autoPasswordSync>*

Force Password Rotation		
forcePasswordRotation	When set to *true*, periodic password rotation is automatically performed for users who authenticate with the Mac Agent infrequently (e.g., users who routinely unlock the machine using Touch ID). The default value is *false*.	*<forcePasswordRotation>true</forcePasswordRotation>*
passwordRotationPeriod	Determines the frequency (in days) of automatic password rotation.	*<passwordRotationPeriod>3</passwordRotationPeriod>*
FileVault Login		
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.	Valid values are: ● client ● server *<filevaultlogin>server</filevaultlogin>*
Custom UI		
customUnlockScreen	When set to *true*, a customized Unlock screen is displayed to support authentication for either the	*<customUnlockScreen>true</customUnlockScreen>* **Important** Touch ID is not supported when the customized Unlock screen is used.

	default user or a guest user. This parameter must be set to *true* to support shared accounts. For more information, refer to Enabling Shared Account Login. The default value is *false*.	
authenticationMethods	An element containing a list of supported methods of authentication as well as configuration options for the Login and Custom Unlock screens. For more information, refer to Configuring Authentication Methods.	For some sample configurations, refer to Configuring Authentication Methods.
Shared Account Support		
sharedaccounts	When set to *true*, the Mac Agent is able to handle authentication of multiple designated users to a single generic shared account. The default value is *false*.	*<sharedaccounts>true</sharedaccounts>* For more details about this feature and its setup, refer to Enabling Shared Account Login.
showSharedAccountLink	When set to *true* (default value), the Mac Login screen will support both the shared account login flow and the standard authentication	*<showSharedAccountLink>true</showSharedAccountLink>* This parameter is enabled only when the *sharedaccounts* parameter is set to *true*.

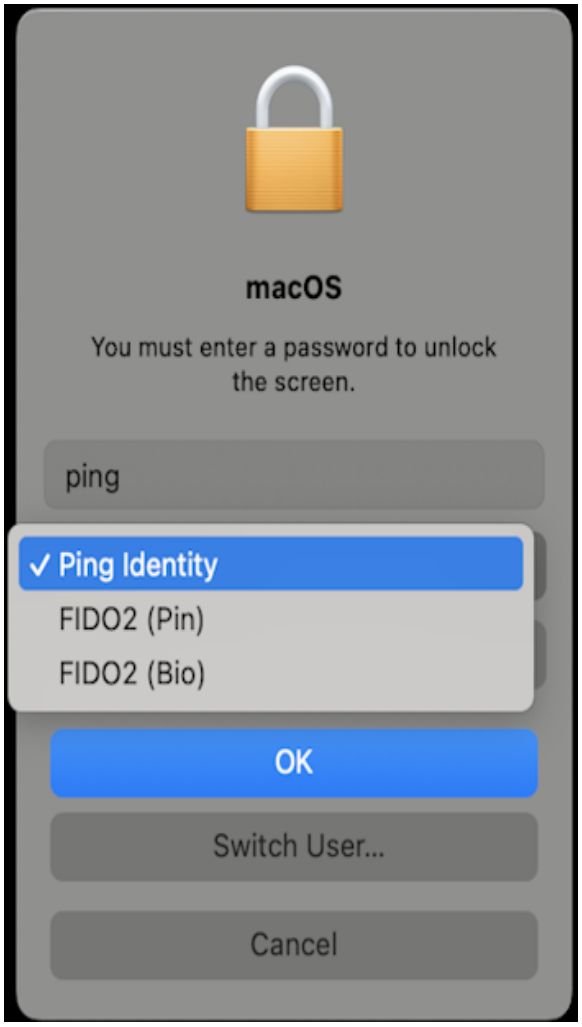
	flow (to a non-shared account).	
defaultToRegularAccount	When set to *true* (default value), the standard authentication flow (to a non-shared account) is displayed on the Mac Login screen initially by default. However, if the last login / unlock was to a shared account, the shared account login flow continues to be displayed for the next login / unlock.	*<defaultToRegularAccount>true</defaultToRegularAccount>* This parameter is enabled only when the *showSharedAccountLink* parameter is set to *true*.
nameForUseSharedAccountLink	Enables you to customize the text for the **Use Shared Account** link on the Login and Unlock screens. When the parameter is defined, the default text is replaced with the specified value.	*<nameForUseSharedAccountLink>Shared Account Logon</nameForUseSharedAccountLink>* This parameter is enabled only when the *showSharedAccountLink* parameter is set to *true*.
nameForRemoveSharedAccountLink	Enables you to customize the text for the **Remove Shared Account** link on the Login and Unlock screens. When the parameter is defined, the default text is replaced with the specified value.	*<nameForRemoveSharedAccountLink>Regular Logon</nameForRemoveSharedAccountLink>* This parameter is enabled only when the *showSharedAccountLink* parameter is set to *true*.
Other		

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>*

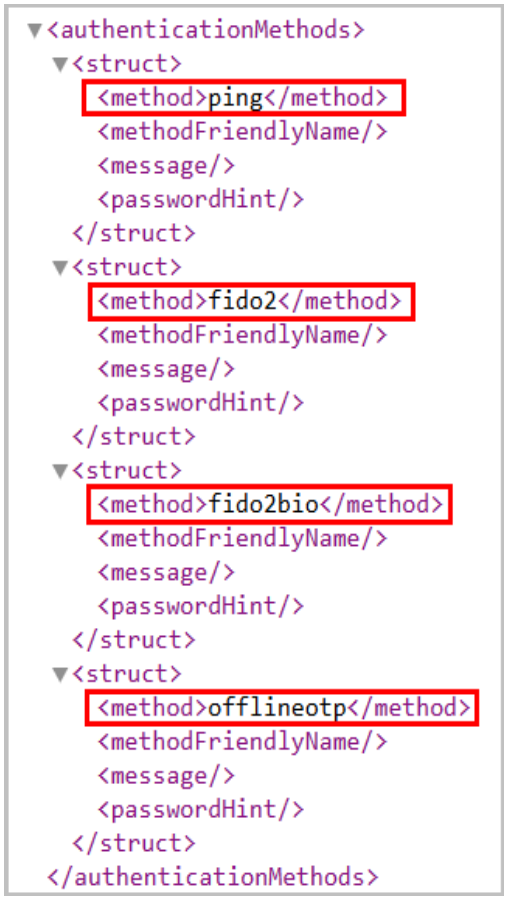
Configuring Authentication Methods

Enterprise Connect Passwordless for Mac features a custom Login screen that enables users to choose a preferred authentication method.

When the Custom Unlock screen is enabled, the list of authentication methods is displayed there as well.



The methods displayed on these screens are defined in the *authenticationMethods* element of the XML configuration file. Default supported methods are Ping Identity, FIDO PIN, FIDO BIO, and Offline OTP. All the methods except Offline OTP can be used for either Passwordless or multi-factor authentication. (Offline OTP is relevant for MFA only.)



Important

If there is *any* authentication method that you do NOT want to include, be sure to delete that entire sub-element from the XML file.

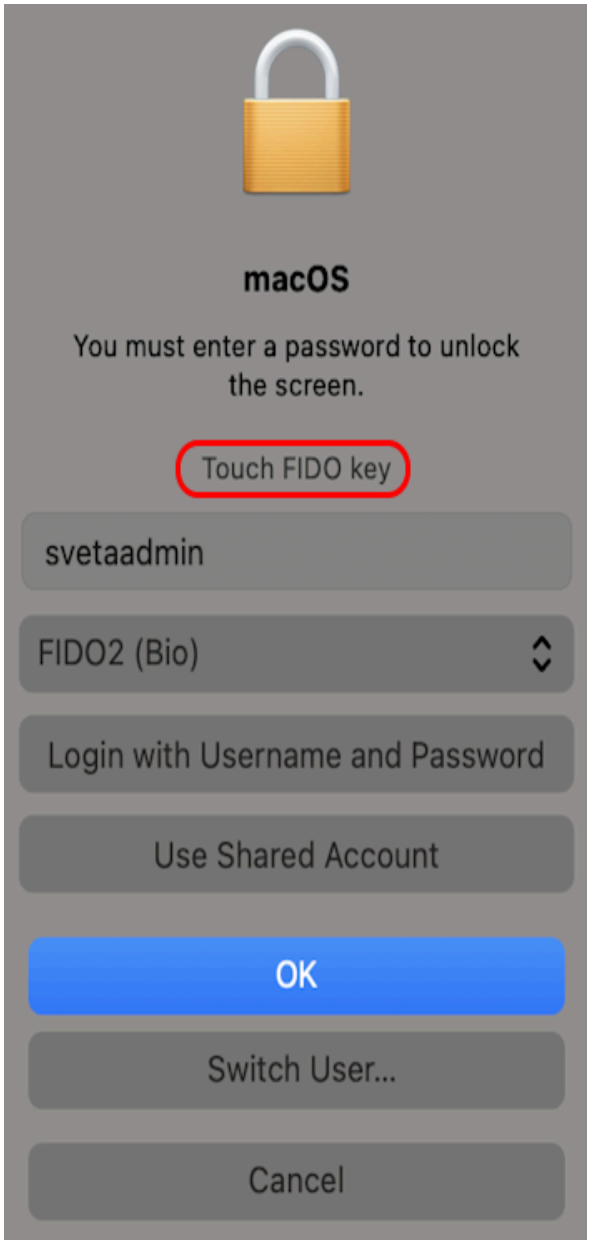
You can define the following optional parameters for each supported authentication method:

- **methodFriendlyName**: A customized name or term for the authentication method. When this parameter is defined, the default name for the method (Ping Identity / FIDO2 (Pin) / FIDO2 (Bio) / Offline OTP) is replaced by the specified string.

  For example: *<methodFriendlyName>FIDO token</methodFriendlyName>*

- **message**: Notes or instructions for the user that appear on the Custom Unlock screen, above the **Username** field.

  For example: *<message>Touch FIDO key</message>*



- **passwordHint**: Customized text for the hint (prompt) displayed in the **Password** field. When the parameter is defined, the default hint is replaced with the specified string.

  For example: *<passwordHint>PIN</passwordHint>*

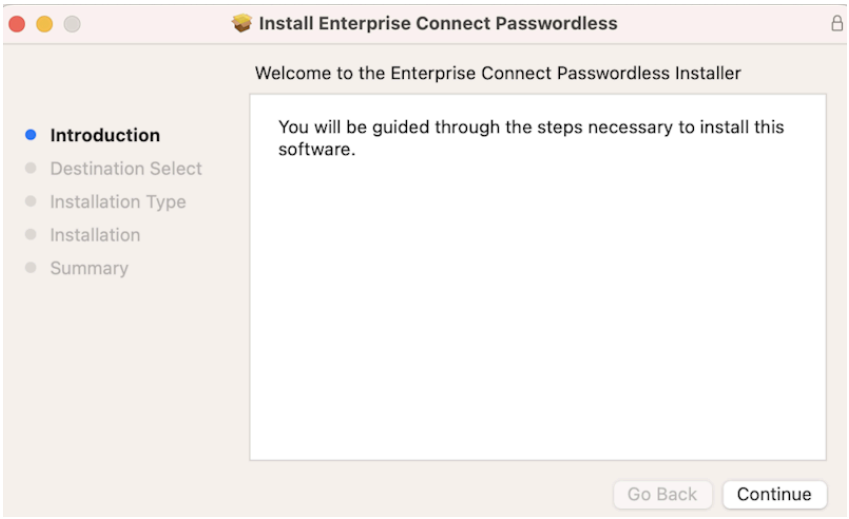
Installing the Mac Client

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.

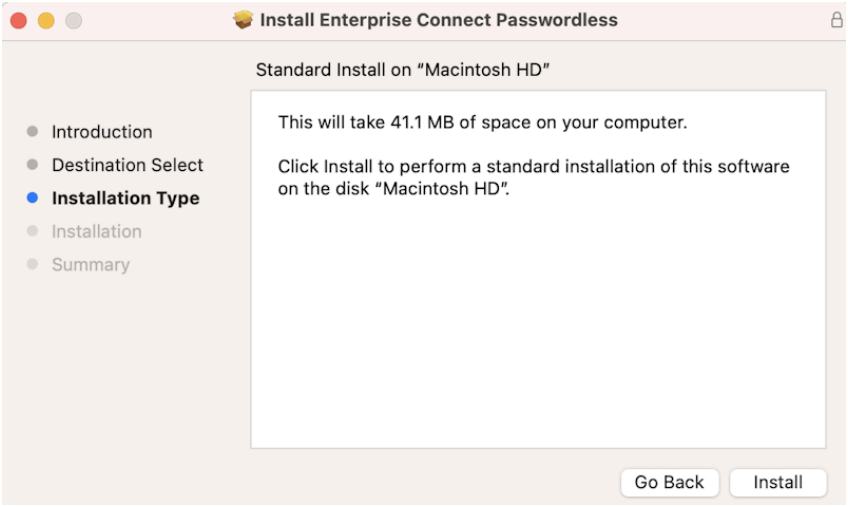
To install Enterprise Connect Passwordless for Mac:

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

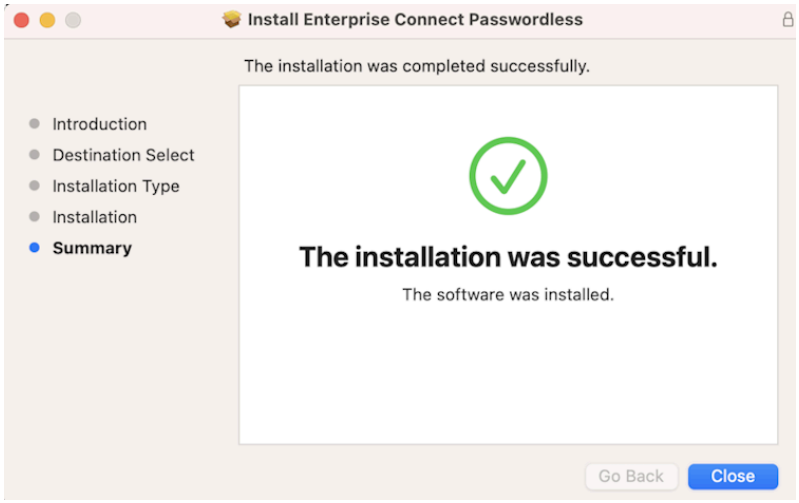
   On the **Introduction** page, click **Continue**.



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.

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 PingID, FIDO or OTP authenticators. Follow the procedures in the sections below to onboard each Local user:

- Enabling the Mobile Authenticator
- Enabling FIDO Authentication
- Enabling OTP Authentication

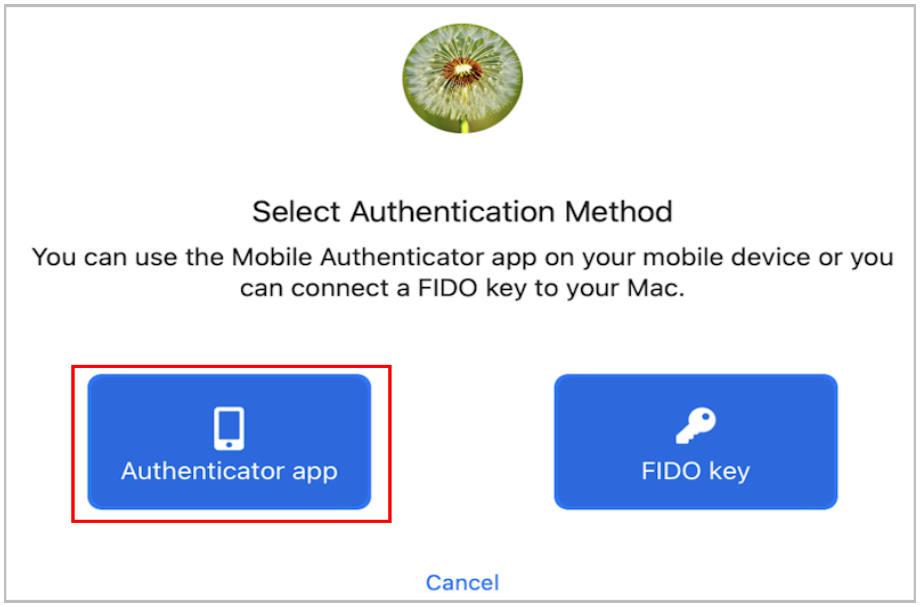
Enabling the Mobile Authenticator

Follow the steps below to enable Local users to log into their machines using the mobile authenticator app.

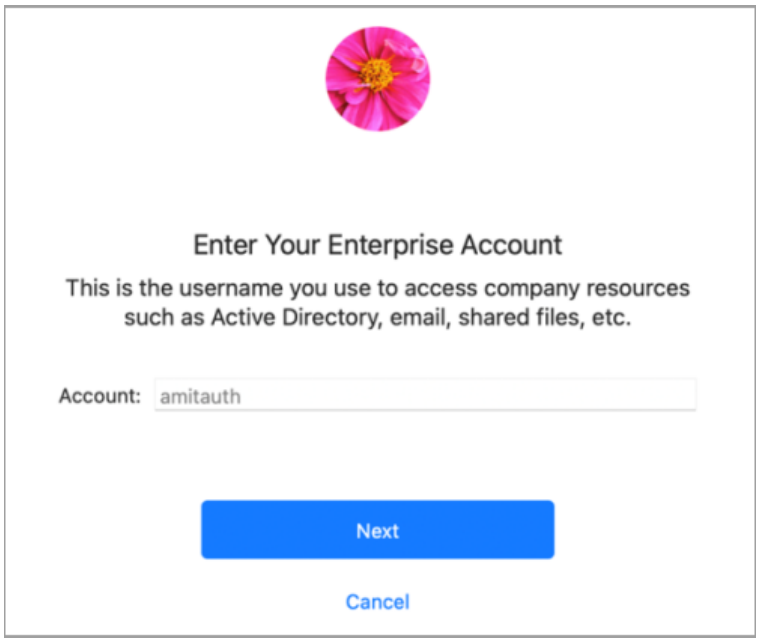
To onboard a Local user:

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

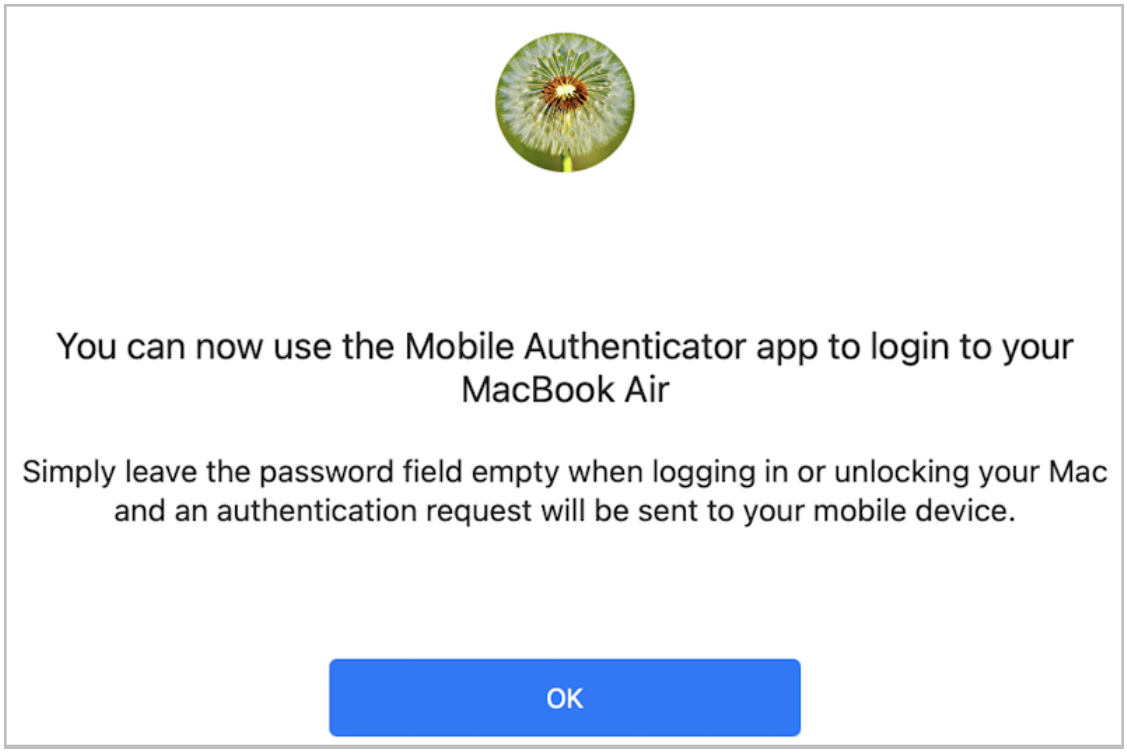
2. From the **Select Authentication Method** dialog, click **Authenticator app**.



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 the app.



Enabling FIDO Authentication

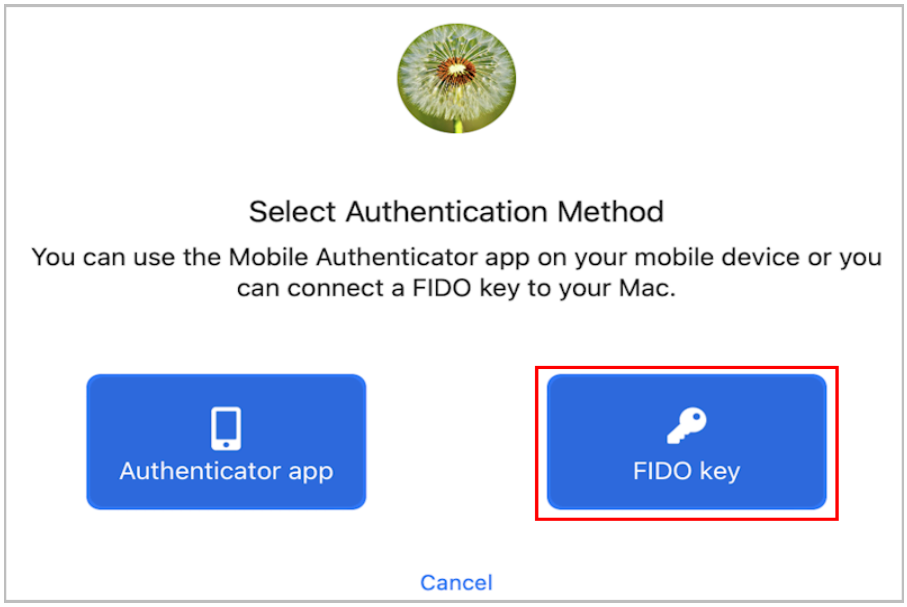
Follow the steps below to enable Local users to log into their machines using a FIDO Authenticator.

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

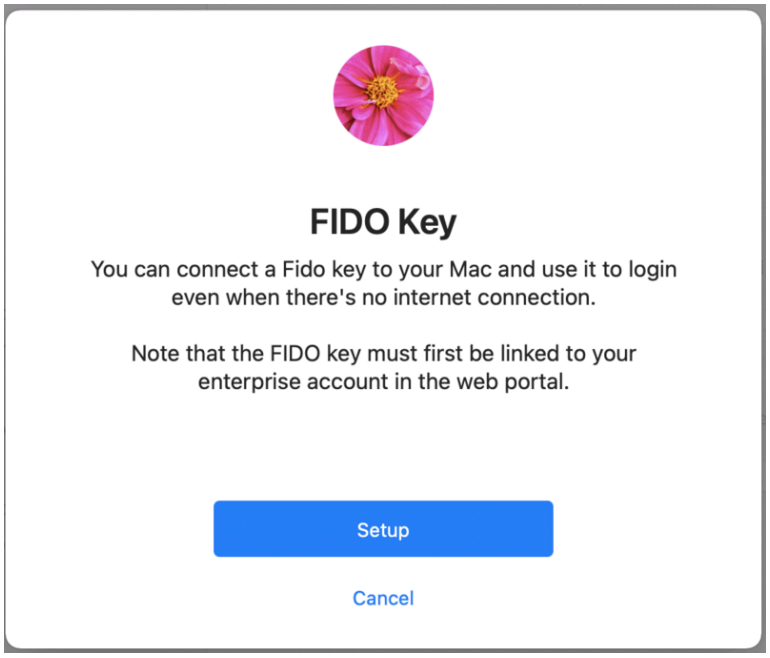
To onboard a Local user:

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

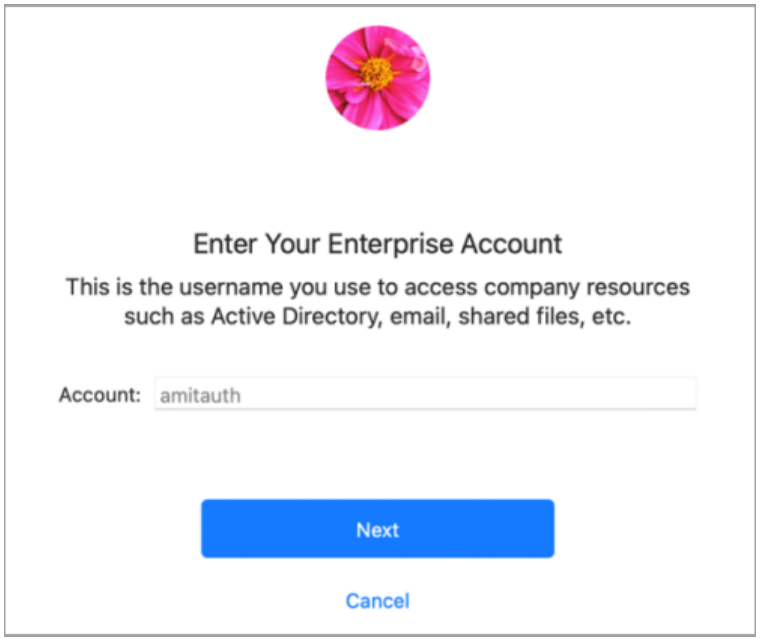
2. On the **Select Authentication Method** dialog, click **FIDO key**.



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

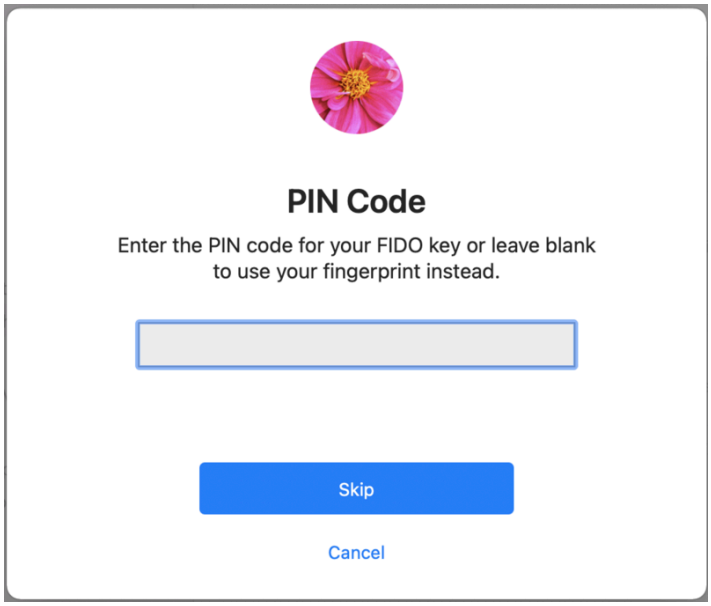


4. To enable Enterprise Connect Passwordless for Mac Authentication, enter the user's credentials in the **Account** field, and click **Next**.

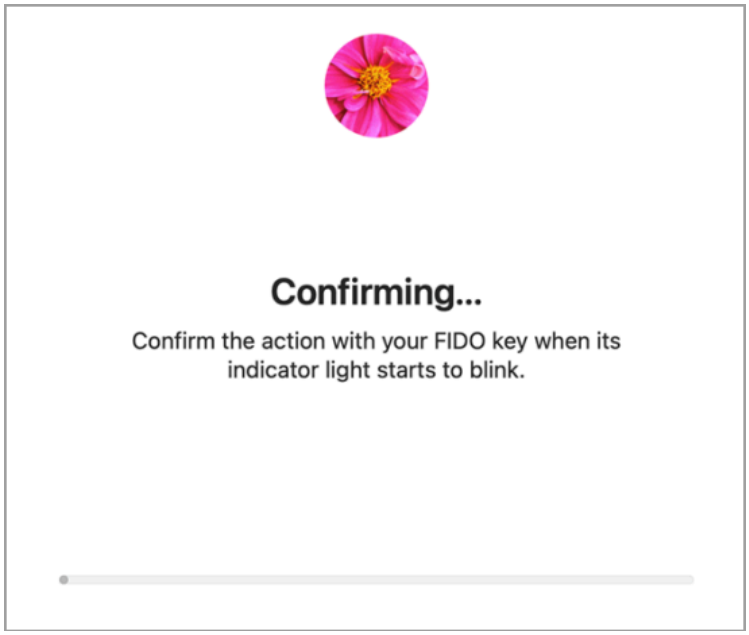


5. If the FIDO key requires a PIN (non-biometric key), enter the PIN code now.

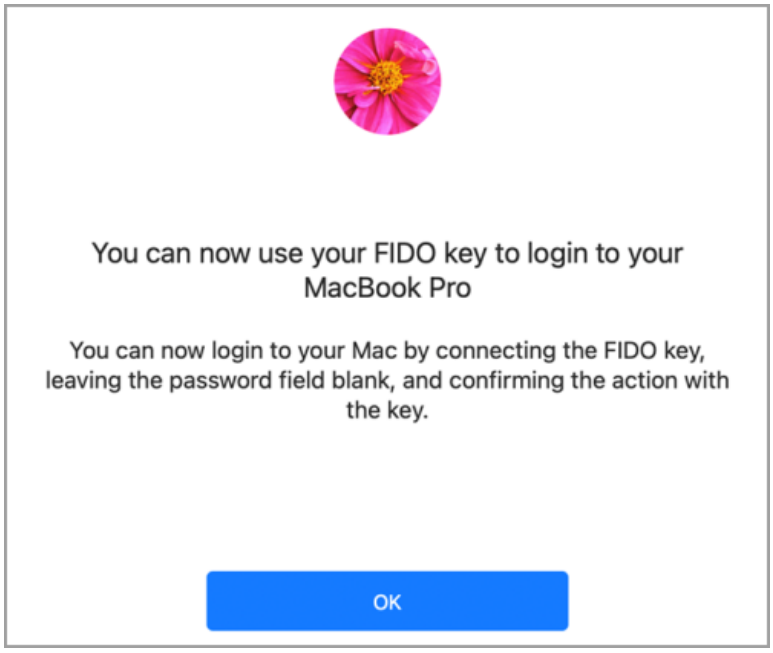
   For biometric keys, leave the field blank and click **Skip**.



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

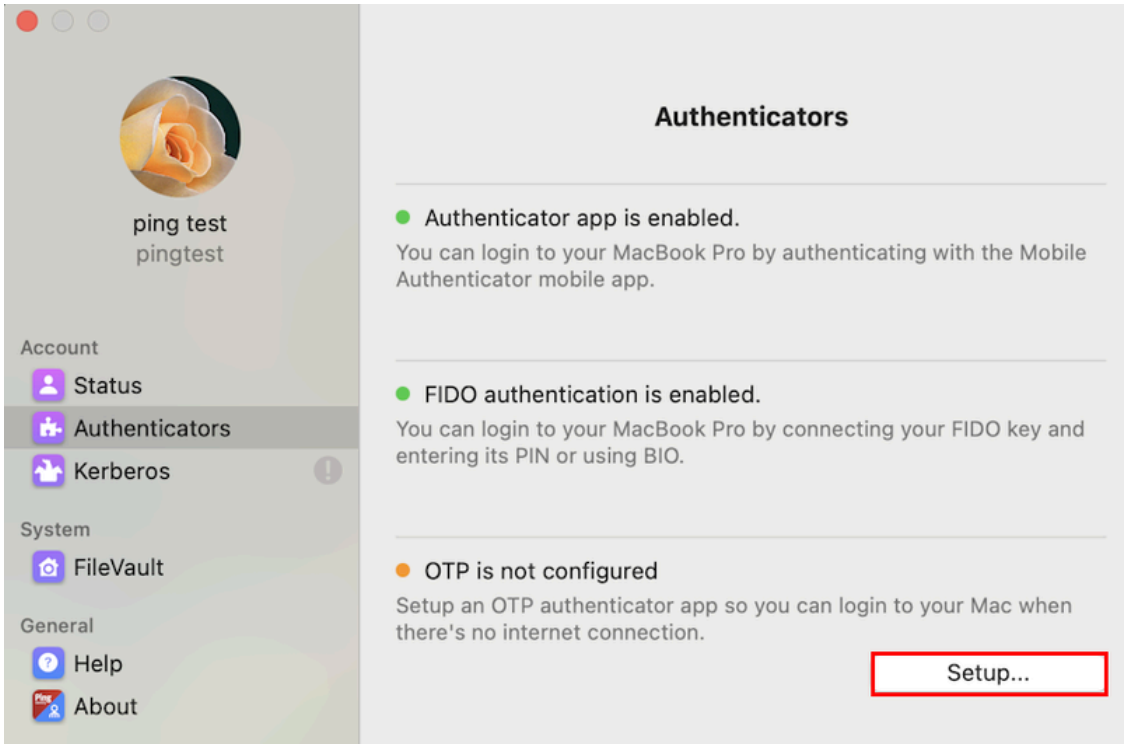
Enterprise Connect Passwordless for Mac supports use of a one-time password as an offline MFA method.

IMPORTANT: OTP is relevant for traditional password-based MFA. This option is available only when the Mac client configuration file is set to work in MFA mode. For details, refer to Configuring the XML File.

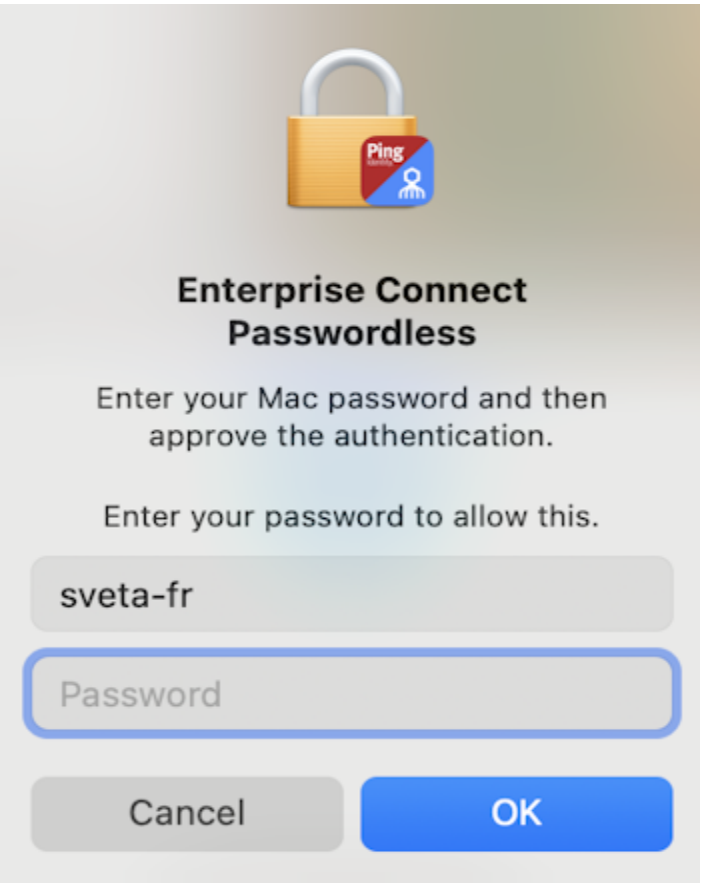
Follow the steps below to configure OTP authentication. Before you begin, open the Authenticator mobile app so you can add the OTP account.

To enable OTP authentication:

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



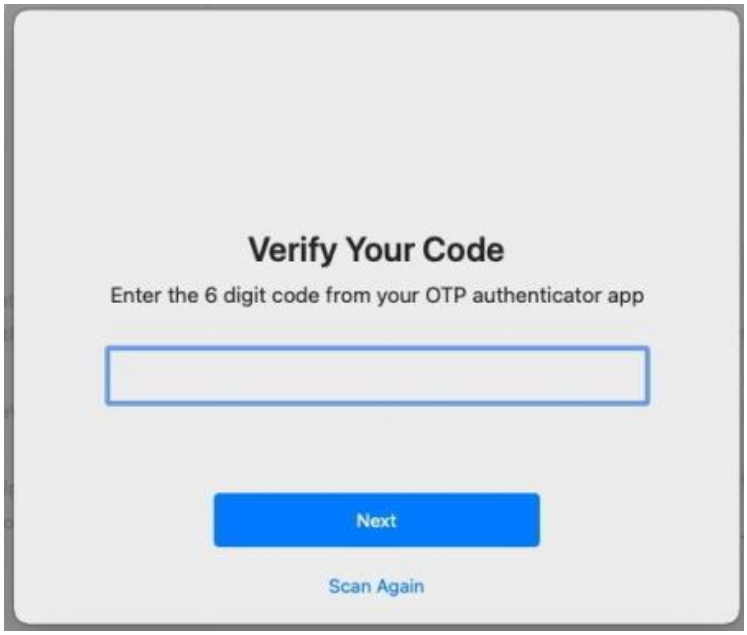
2. On the screen that opens, enter your Mac password and then click **Authenticate**.



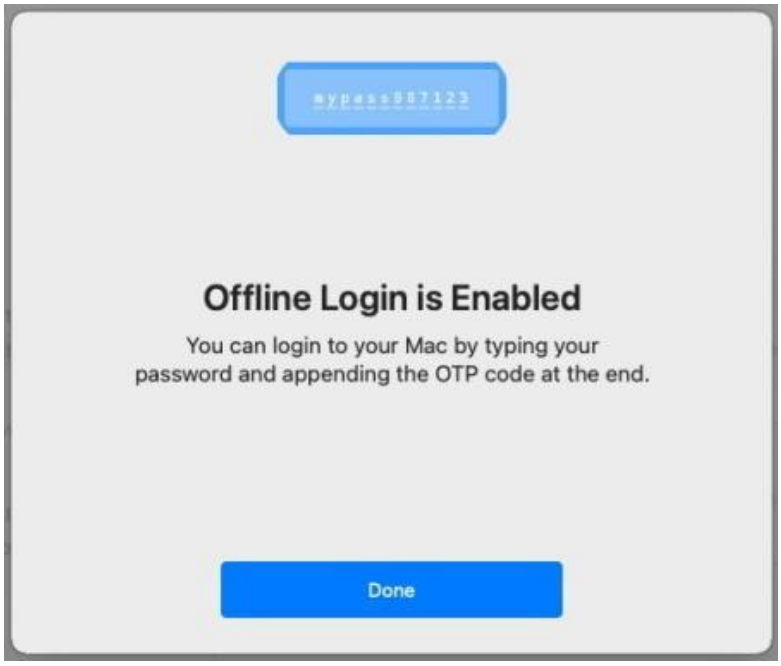
The following screen opens:

3. In your Authenticator mobile app, tap **Add Account** and scan the QR code. Then, on your Mac, click **Next**.

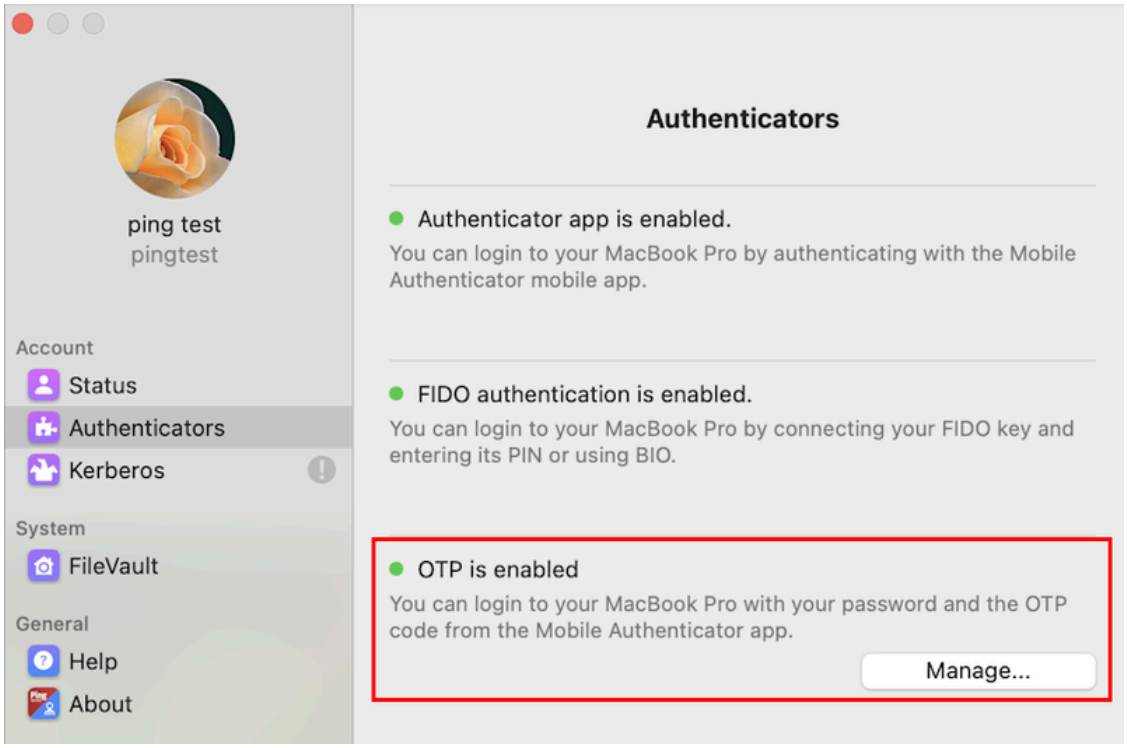
4. On the screen that opens, enter the code displayed in the account you added in the Authenticator mobile app. Then, click **Next**.



5. 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 authentication 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*.

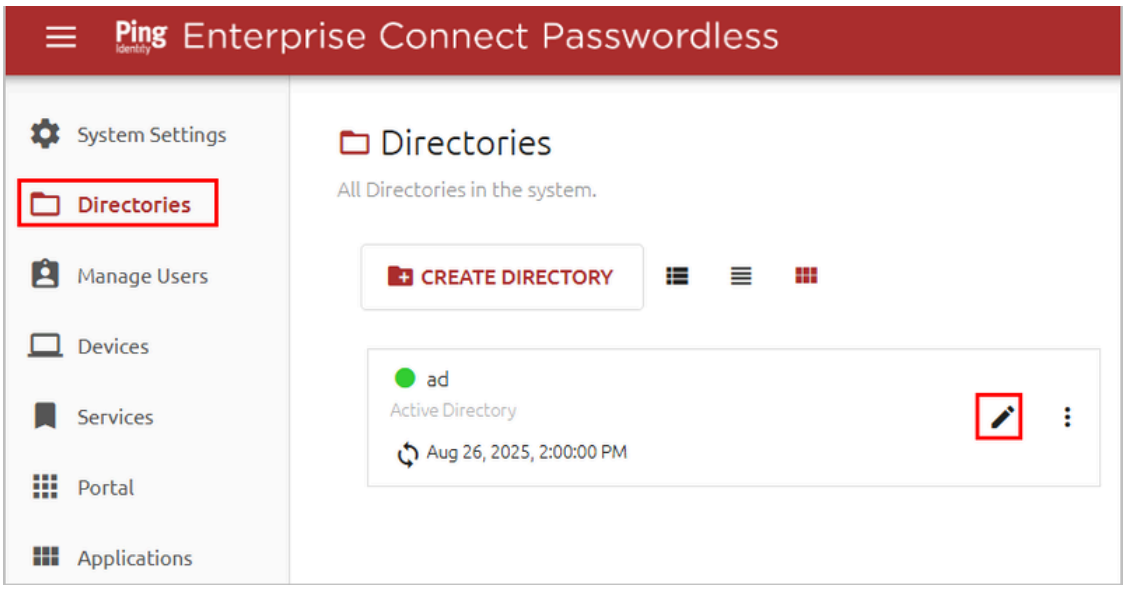
```
<!--
    Password Free Experience (default: 'false')

    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.

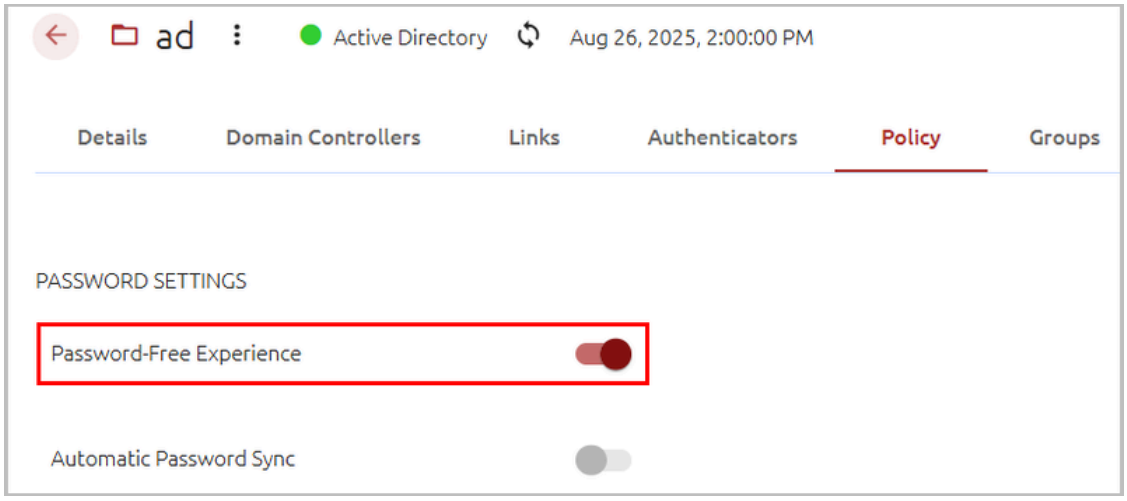
Management Console Configuration

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 ✎.

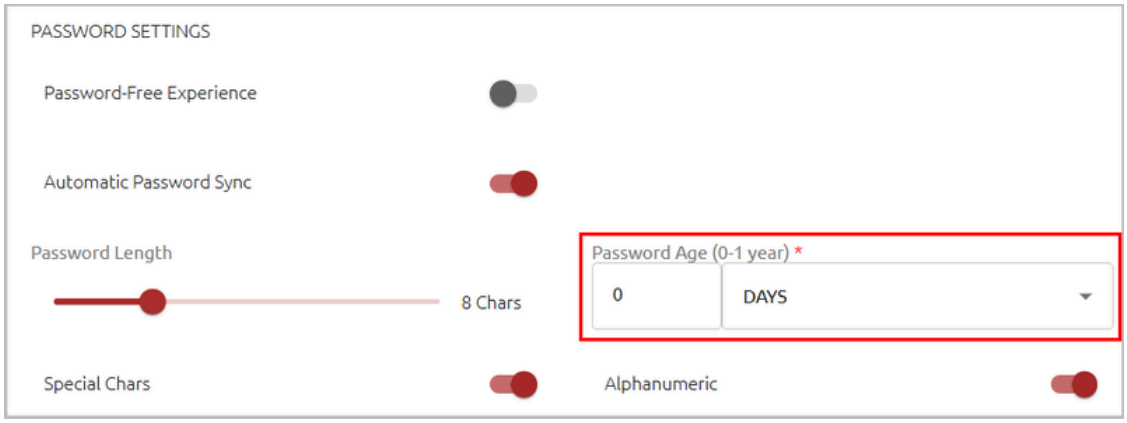


2. Select the **Policy** tab.
3. If Compatibility Mode is OFF, make sure that the **Password-Free Experience** toggle is enabled.



Then, go to Step 5 (below).

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

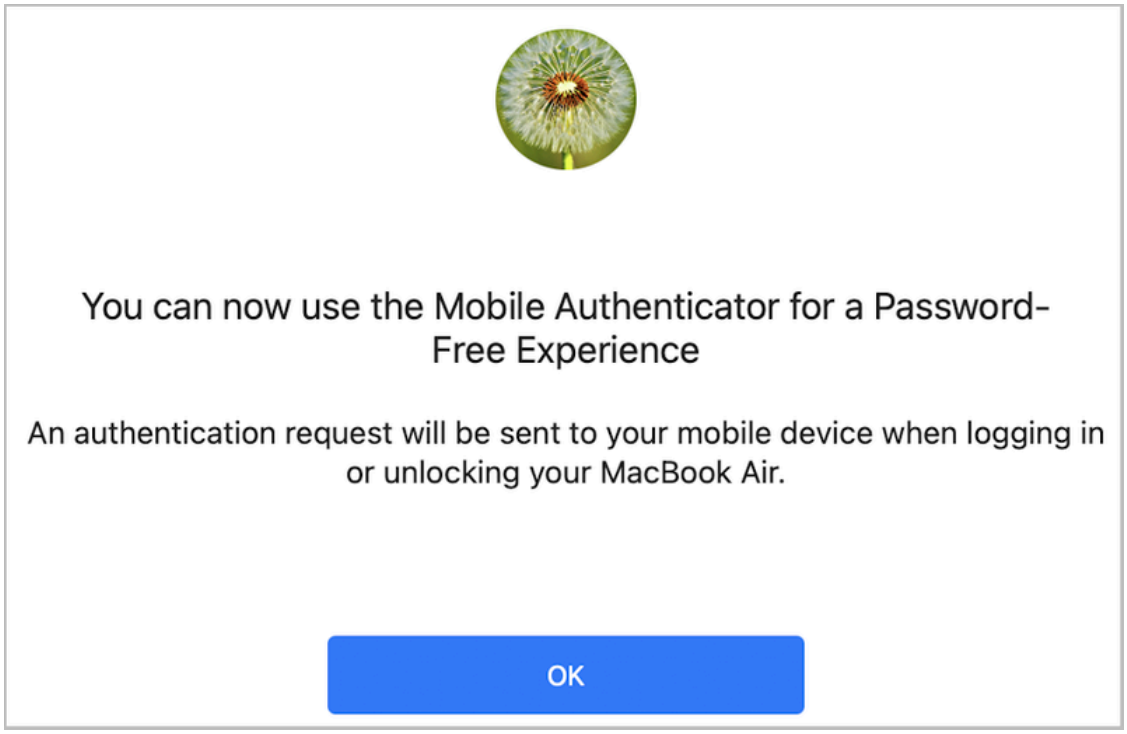


When the value is **0**, the system never rotates the password, and the password is managed directly on the directory or the AD.

5. 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 Enterprise Connect Passwordless, 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).

```
<!-- ********************************************************************************** -->
<!-- ***  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>
```

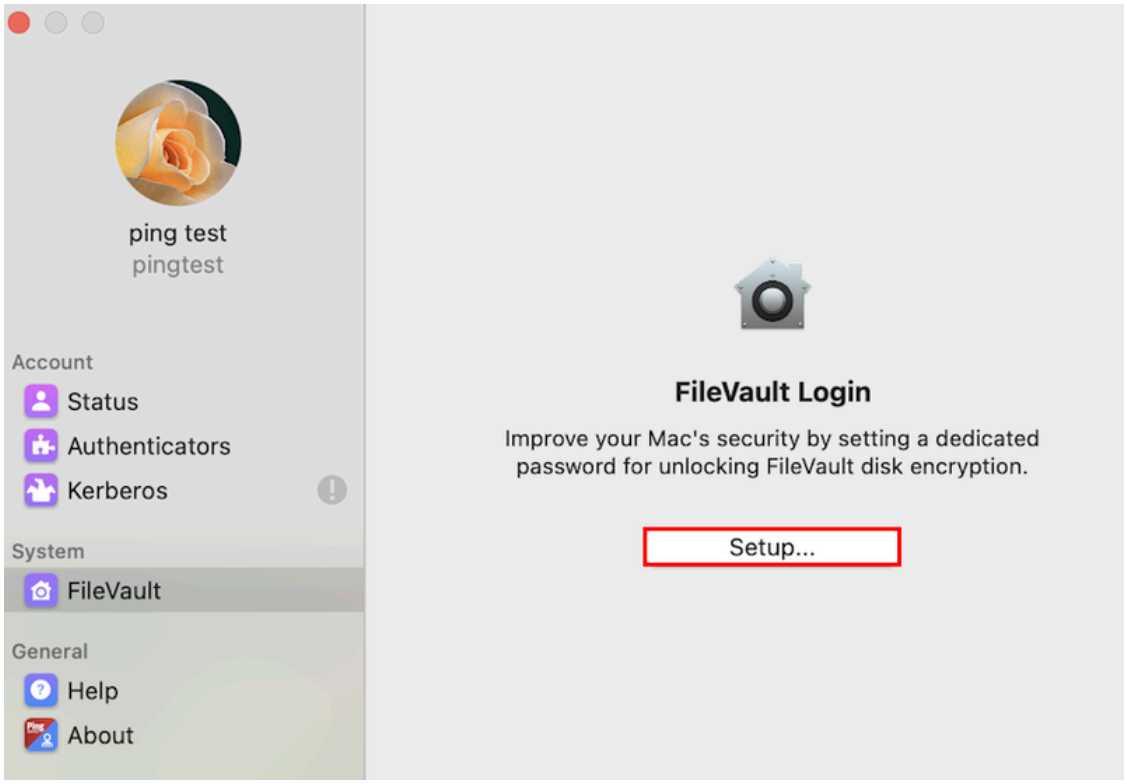
Enabling FileVault Login

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.

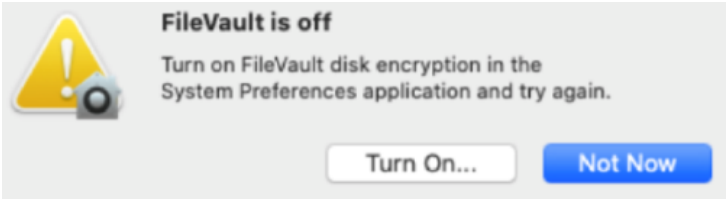
To enable FileVault login:

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



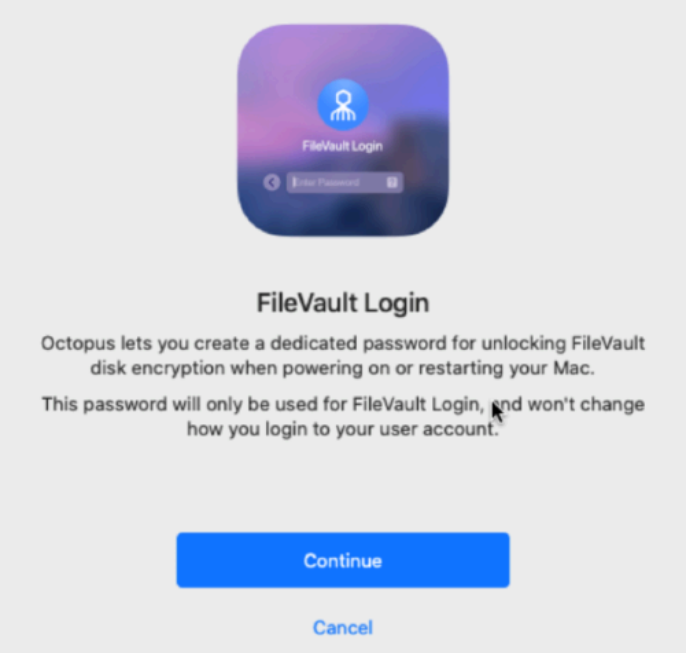
If FileVault is turned on, skip to Step 3.

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



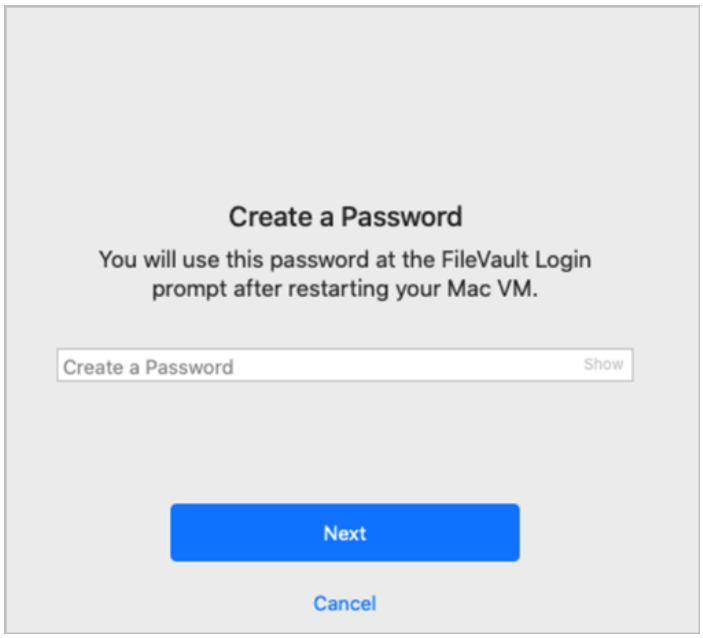
Click **Turn On** and then enable FileVault in the **Security & Privacy** settings.

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

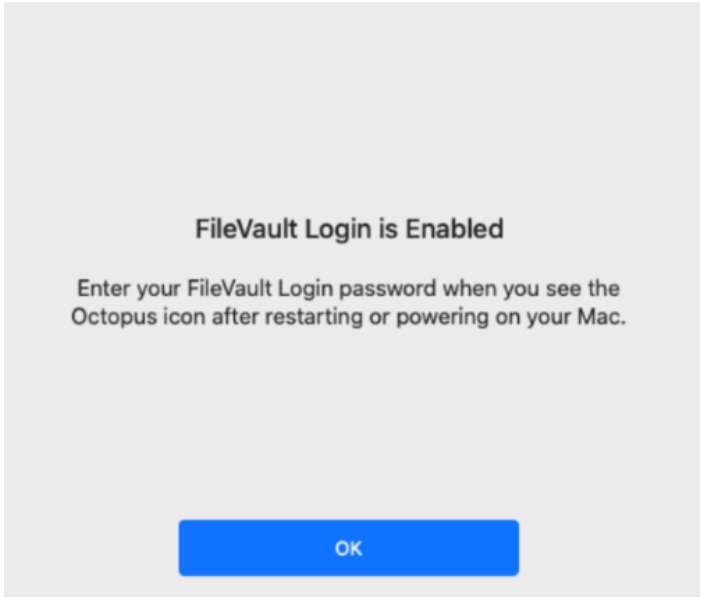


The **Create a Password** dialog opens.

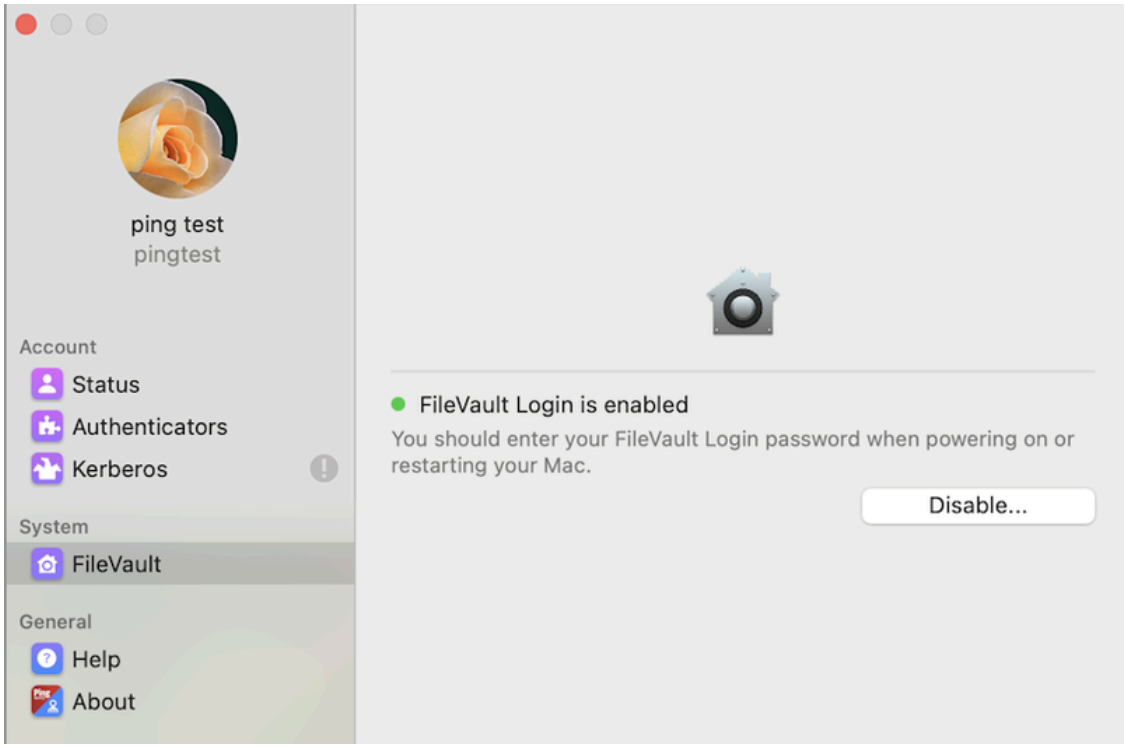
4. Enter a password for FileVault Login, and then click **Next**.



A confirmation message is displayed on the Mac.



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



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:

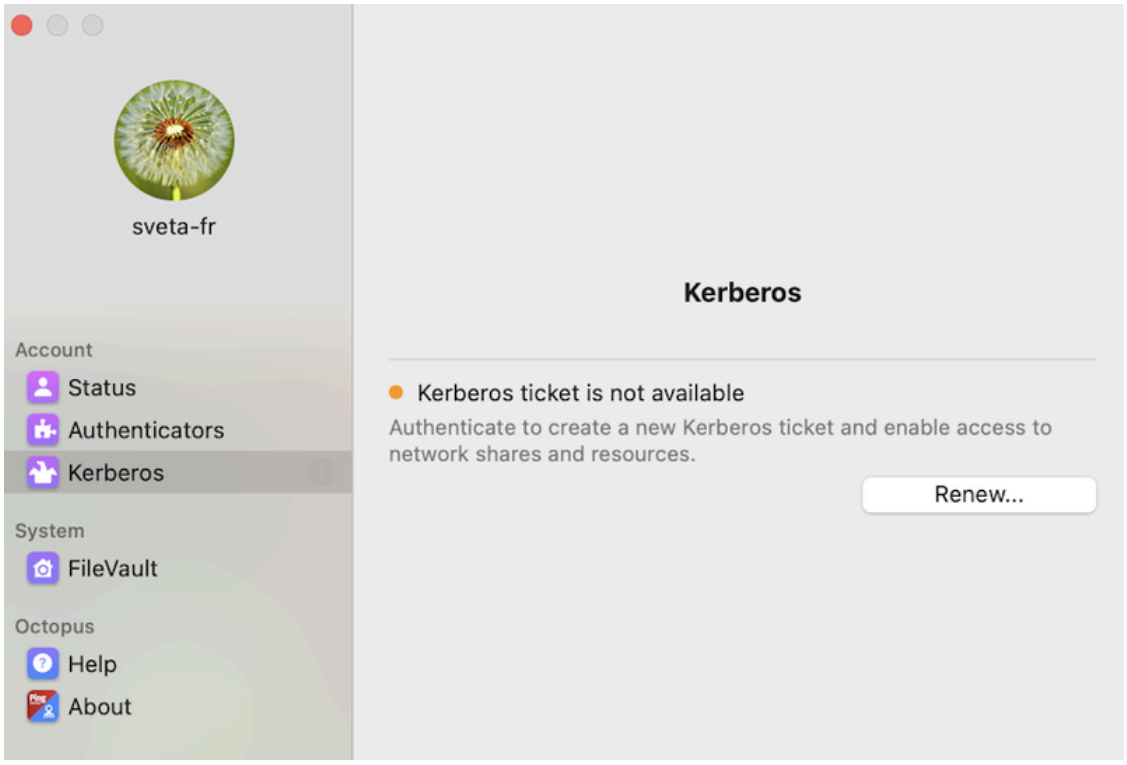
- The *kerberosrealm* parameter must be defined in the **enterprise-connect-passwordless.xml** file. For details, refer to Configuring the XML File.
- If the workstation is NOT domain-joined, the local password must match the AD password.

  For details about making the workstation domain-joined, refer to Adding Your Machine to the Active Directory.

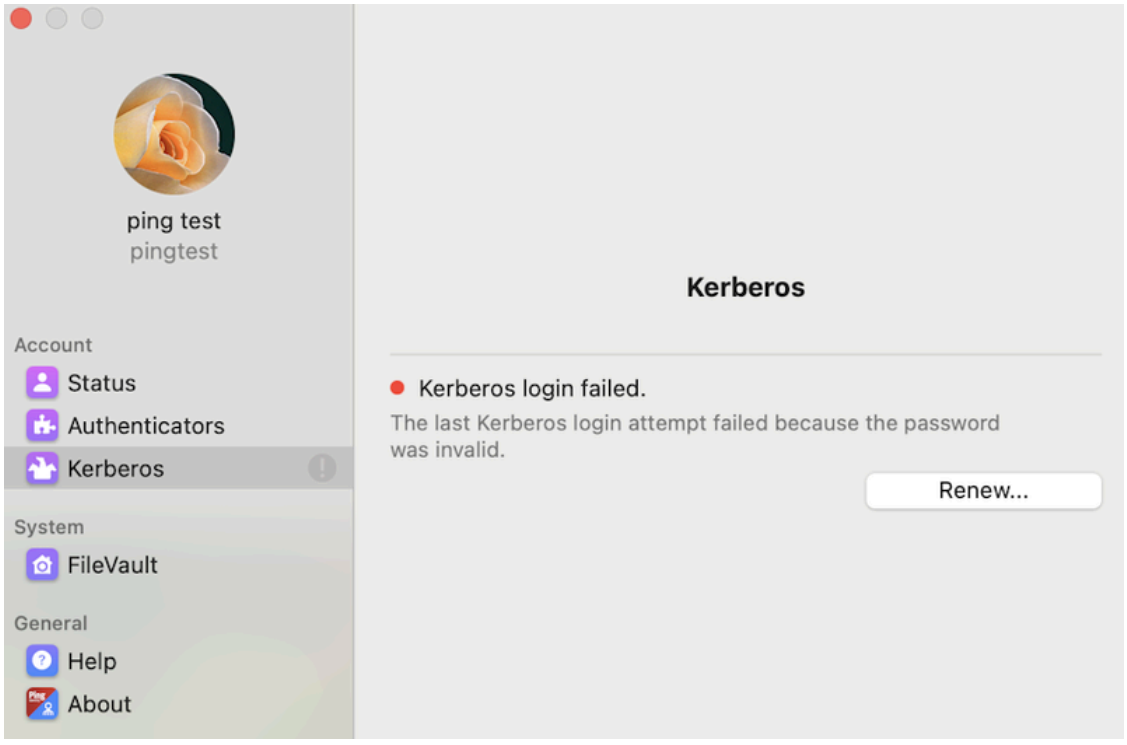
Viewing Kerberos Ticket Status

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.

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

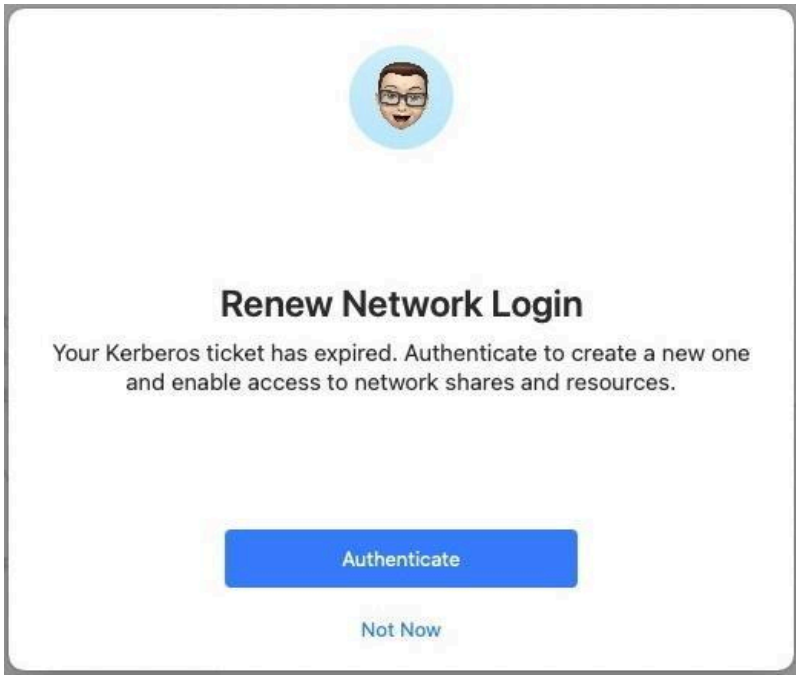


A red icon indicates that the most recent Kerberos login failed. The cause of the login failure is described below the status.

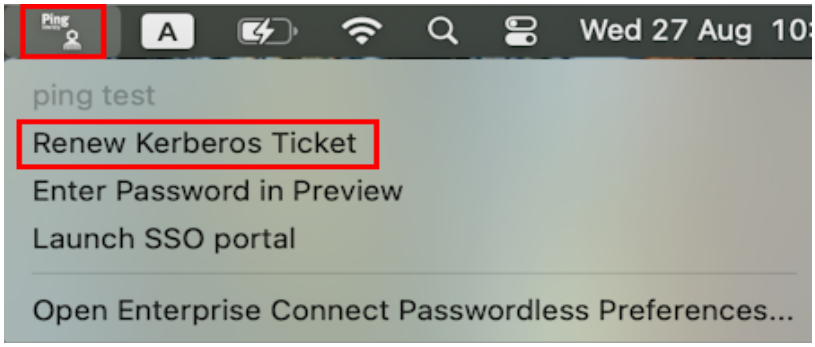


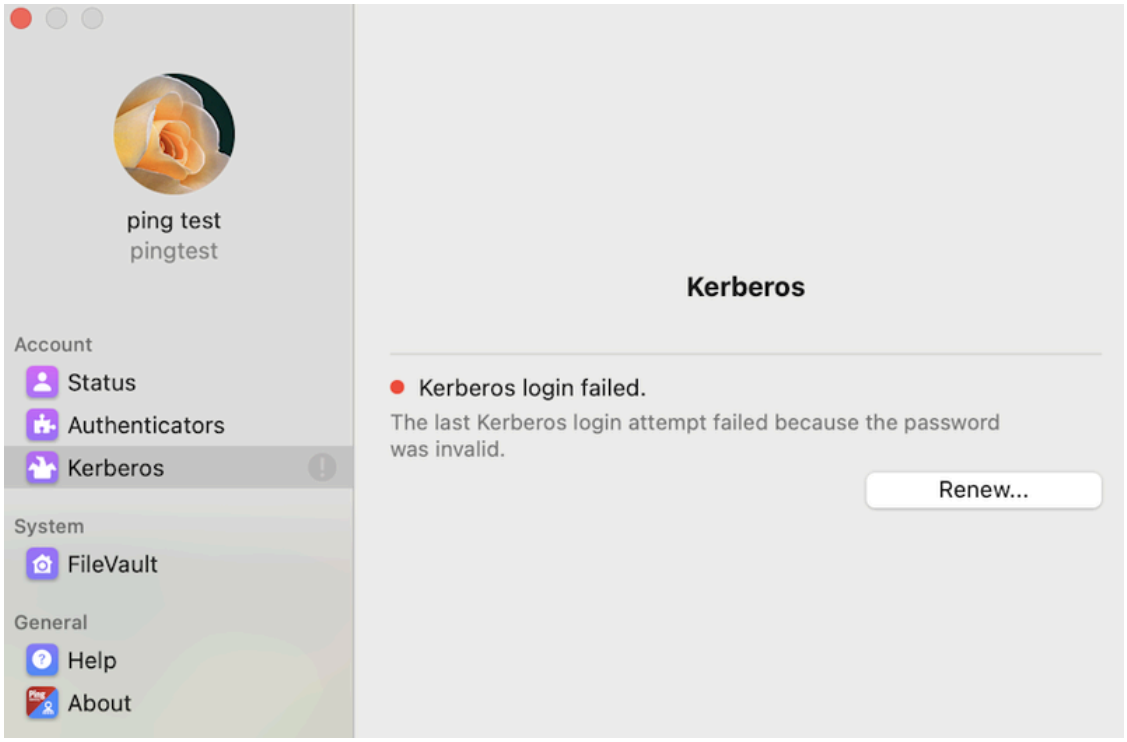
Renewing the Ticket

In the event that 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.

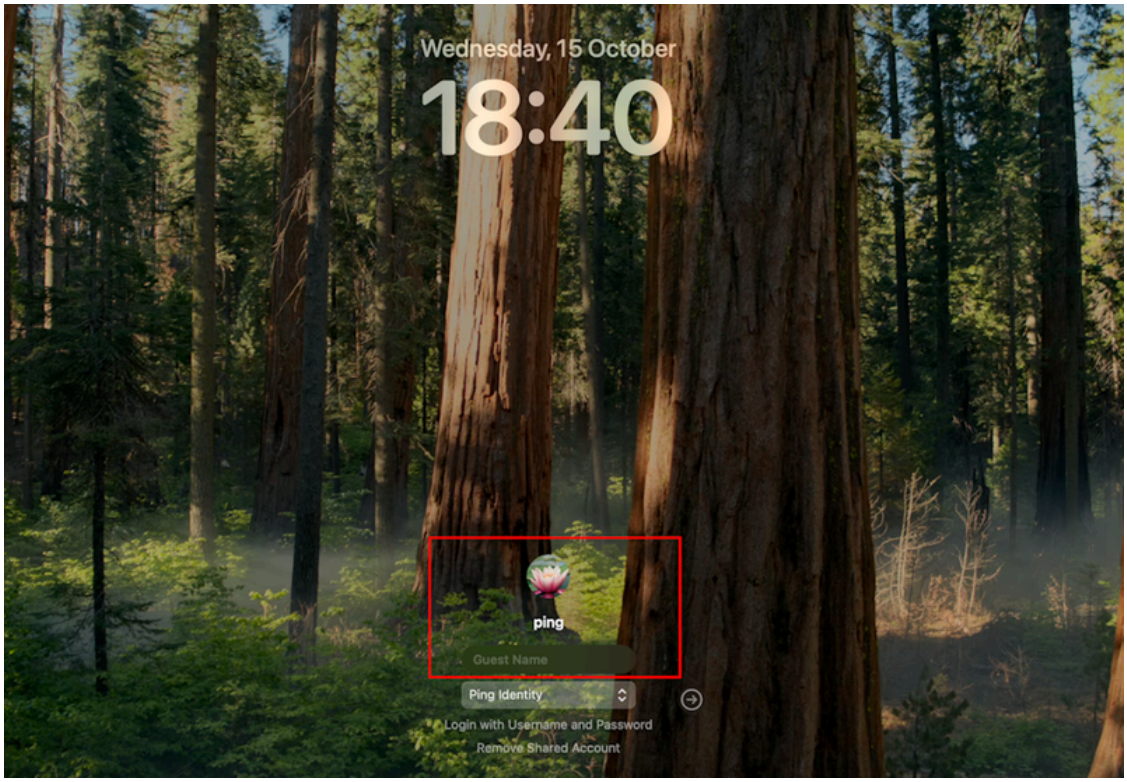




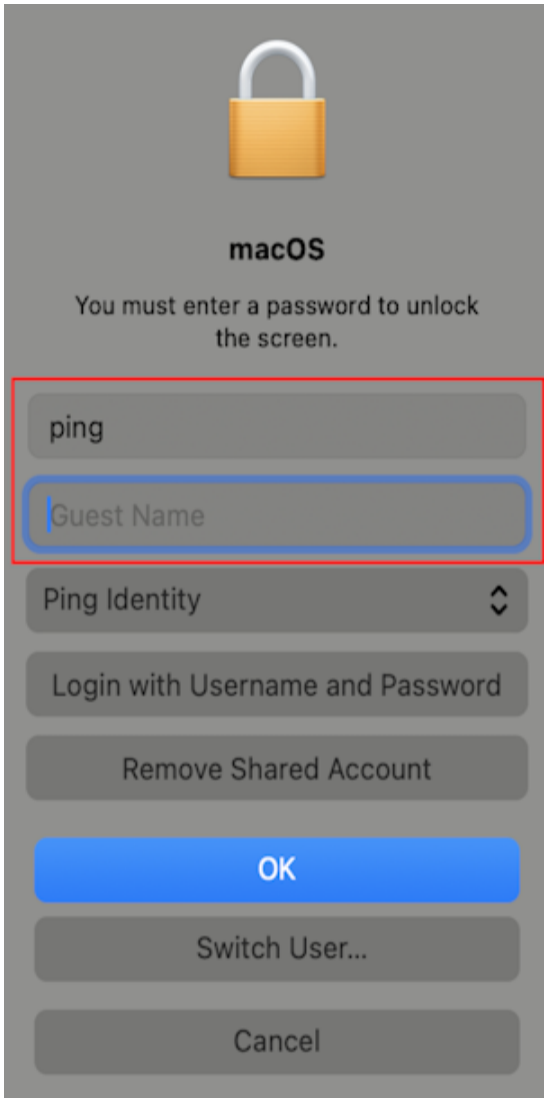
Enabling Shared Account Login

The Shared Account feature enables designated users to log into a generic account on a workstation using their personal credentials and devices. Account sharing is particularly useful for specific groups of personnel who require occasional access to user workstations (e.g., the IT team).

When account sharing is activated, users who are authorized to access the account enter two usernames on the Login screen: the name by which the shared account is known, and their own username. They then complete the login process by authenticating with their personal mobile device, FIDO key, etc.



The same presentation is displayed on the Custom Unlock screen.



To enable support of shared accounts, some updates need to be done in the Agent configuration file and in the Enterprise Connect Passwordless Management Console, as described in the following sections.

> **Important**
>
> To support shared account login to the workstation, FileVault needs to be disabled or unlocked.

Mac Agent Configuration

To enable shared account login, make the following updates in the **enterprise-connect-passwordless.xml** configuration file:

- In the **Custom UI** section, set the *customUnlockScreen* parameter to *true*. For more information about the Custom Unlock screen and related configuration options, refer to Configuring the XML File.

```
<!-- ********************************************************************************** -->
<!-- ***  CUSTOM UI                                                                 *** -->
<!-- ********************************************************************************** -->


<!--
    Custom Unlock Screen (default: false)

    If this element exists with a value of 'true', a customized Unlock screen is displayed.

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

Important

Touch ID is not supported when the customized Unlock screen is used.

- In the **Shared Accounts Support** section, set the *sharedaccounts* parameter to *true*.

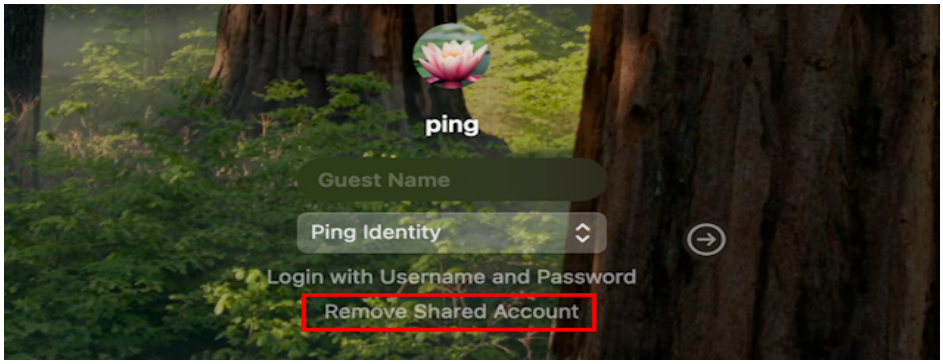
```
<!-- ********************************************************************************** -->
<!-- ***  SHARED ACCOUNTS SUPPORT                                                   *** -->
<!-- ********************************************************************************** -->

<!--
    Shared Accounts Support (default: false)

    If this element exists with a value of 'true' then Octopus for Mac
    will allow Shared Accounts support. Otherwise this feature is disabled.

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

Important

BOTH of these parameters must be set to *true* to support shared account login.

The following additional parameters related to the Shared Account feature are optional:

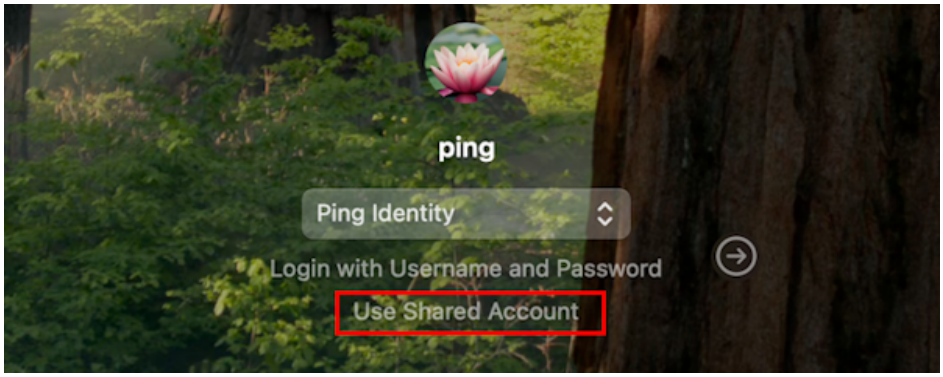
- *showSharedAccountLink*: When set to *true*, the Login screen supports both the shared account login flow and the standard login flow (to a non-shared account). By default, when switching is allowed, the Login screen presents the shared account login flow. A link at the bottom of the screen enables users to switch between the two login options.



Note

It is possible to customize the text of the **Remove Shared Account** link. For details, refer to Configuring the XML File.

- *defaultToRegularAccount*: When set to *true* , the standard authentication flow (to a non-shared account) is displayed on the Mac Login screen initially by default.



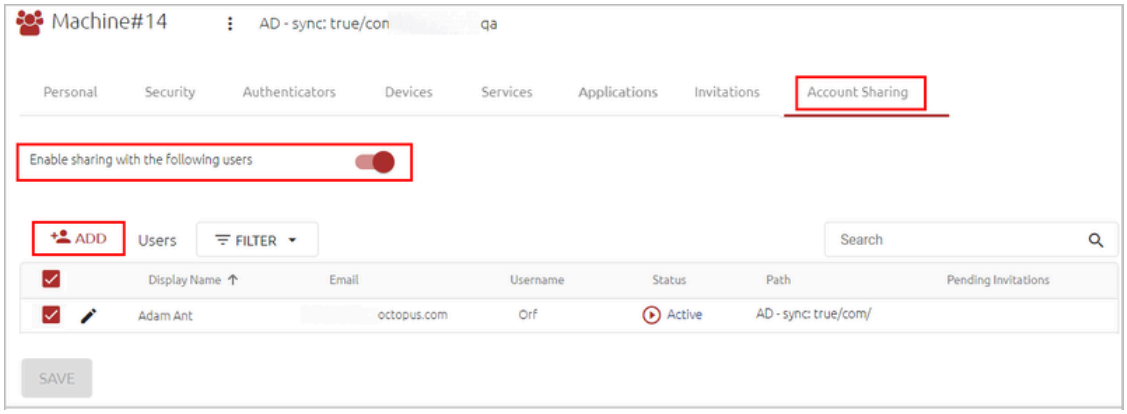
If the most recent login / unlock was to a shared account, the shared account login flow continues to be displayed for the next login / unlock.

Management Console Configuration

Shared user accounts are designated and managed from the user details of the relevant account.

To activate account sharing:

1. From the **Manage Users** menu of the Management Console, navigate to the relevant user and click ✎ to open the user details.
2. From the **Account Sharing** tab, select the **Enable sharing** toggle button.



3. To allow users to log into the shared account, click **Add** and select the relevant user(s) from the dialog that opens.

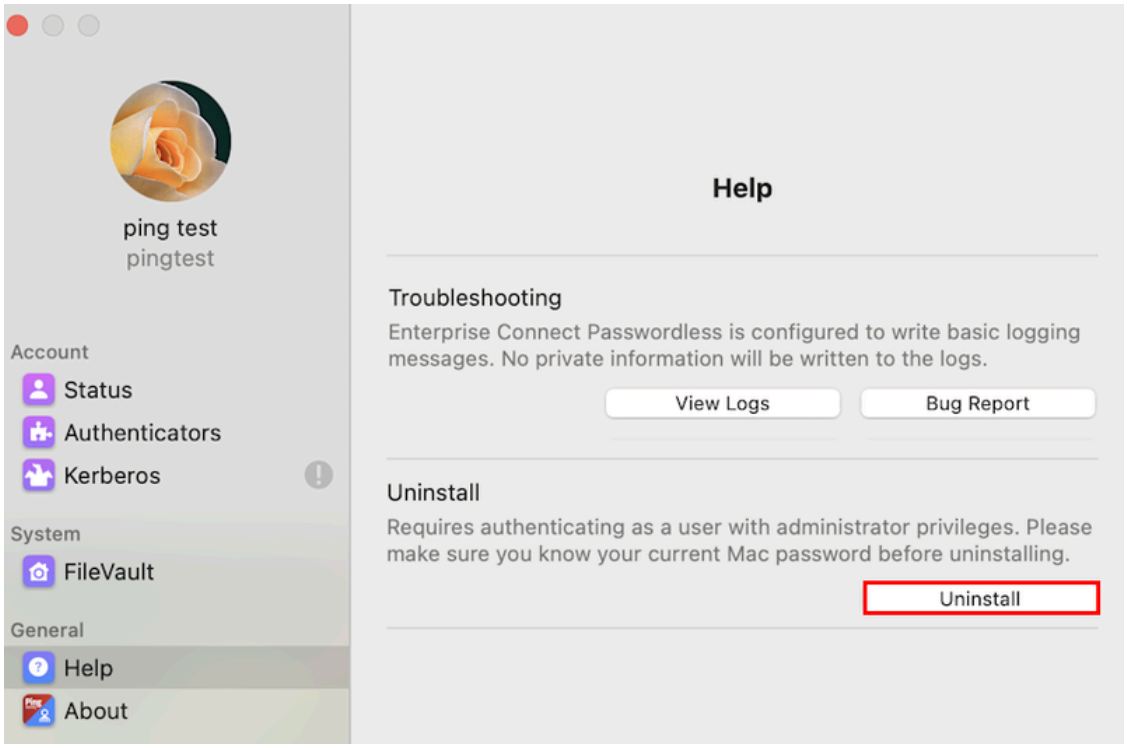
Once users are added, you can temporarily block their access to the account when required, by clearing the checkbox in the row of the relevant user(s).

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

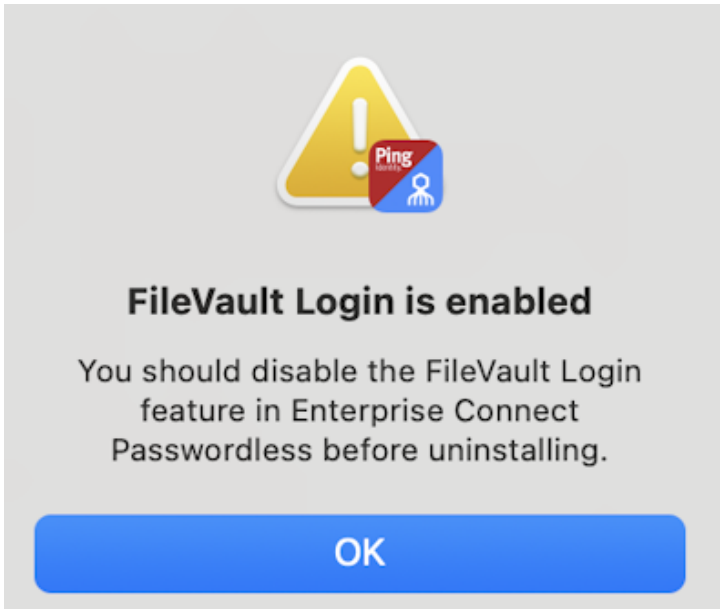
For more details about shared accounts, refer to the Enterprise Connect Passwordless Management Console Admin Guide.

Uninstalling the Mac Client

If it becomes necessary to uninstall the client, you can remove it directly from the Enterprise Connect Passwordless Preferences. From the **Help** menu, click **Uninstall**.



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

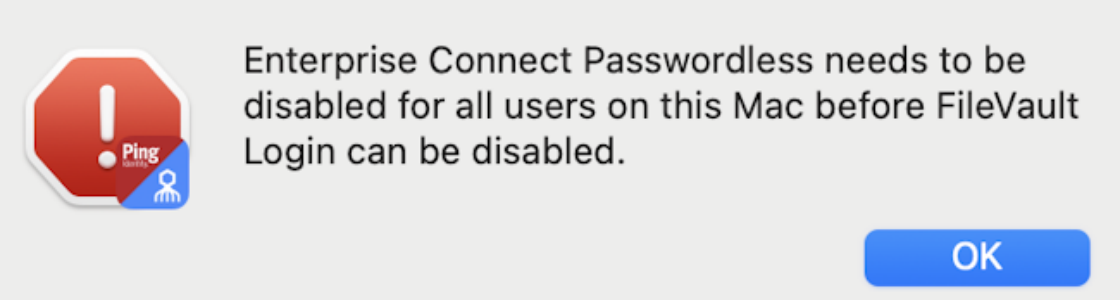


To disable FileVault Login:

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, the following warning popup opens:



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

Troubleshooting

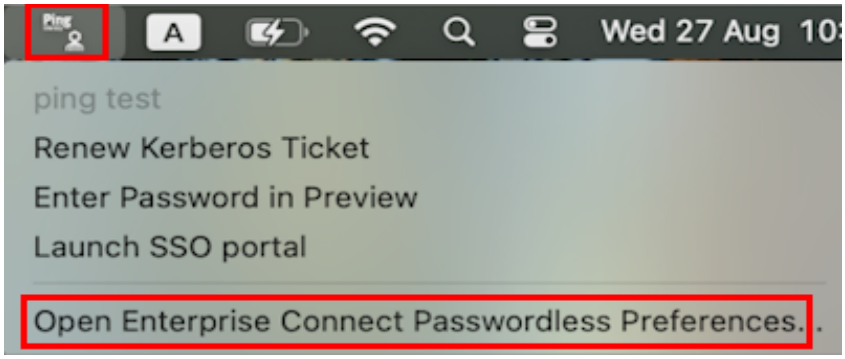
This section provides guidelines for understanding the audit records and for handling issues that you may encounter when working with Enterprise Connect Passwordless for Mac.

Enterprise Connect Passwordless Preferences Help Menu

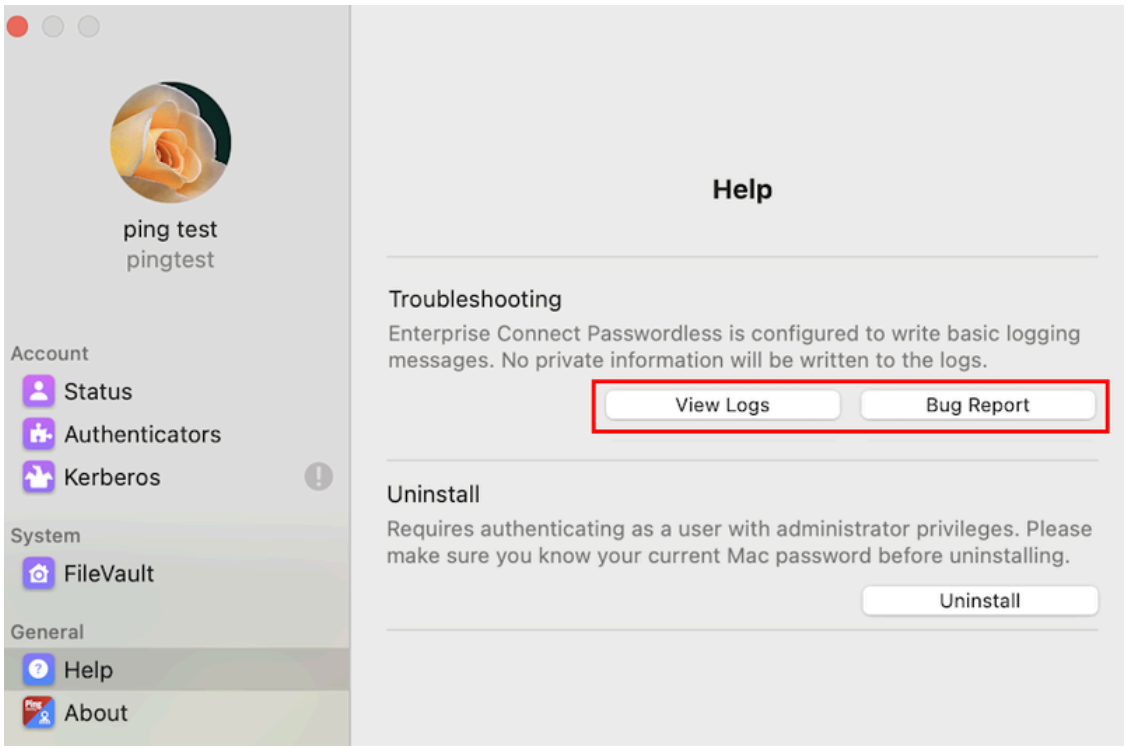
The **Help** menu of the Enterprise Connect Passwordless preferences provides the following troubleshooting options:

- **View Logs:** Displays the application 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

To access these options, click the app icon and select **Open Enterprise Connect Passwordless Preferences**.



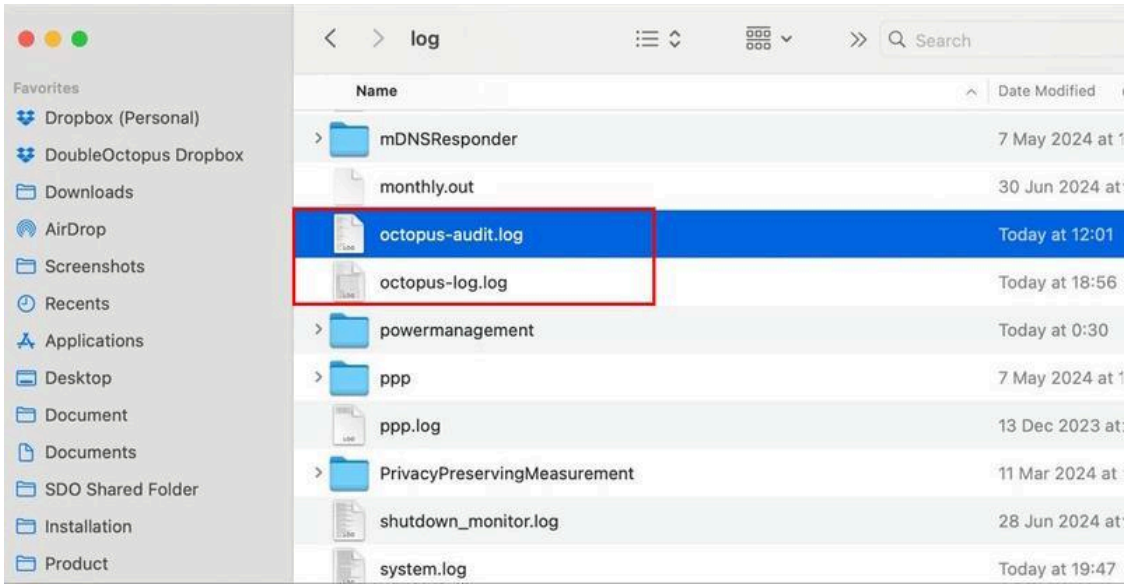
Then, select the **Help** menu.



Viewing Mac Agent Events

You can view the Mac Agent logs at any time. The following files are stored in the **/var/log** directory:

- octopus-audit.log
- octopus-log.log



Events in the **octopus-audit.log** file are displayed together with specific codes and clear descriptions, enabling you to quickly and easily trace the entire flow of events that occurred during an authentication session. The *maxAuditFileSize* parameter in the XML configuration file allows you to control the file size. (Default maximum size is 10 MB.)

List of Event Codes

The following table lists the event codes and their descriptions. If you require more advanced troubleshooting and/or debugging, please reach out to support@doubleoctopus.com.

Event Code	Event Description
5020	Logon initiated
5021	Logon successful
5022	Logon failed
5041	Unlock initiated
5042	Unlock successful
5043	Unlock failed
5051	Sudo initiated

Event Code	Event Description
5052	Sudo successful
5053	Sudo failed
5061	Manual password retrieval initiated
5062	Manual password retrieval succeeded
5063	Manual password retrieval failed
5064	Password copied to clipboard
5065	Password removed from clipboard
5071	Manual password sync started
5072	Manual password sync succeeded
5073	Manual password sync failed
5081	Automatic password sync started
5082	Automatic password sync succeeded
5083	Automatic password sync failed
5091	Account password changed
5101	Kerberos login initiated
5102	Kerberos login succeeded
5103	Kerberos login failed
5104	Kerberos session renew initiated

Event Code	Event Description
5105	Kerberos session renew succeeded
5106	Kerberos session renew failed
5121	FileVault setup initiated
5122	FileVault setup succeeded
5123	FileVault setup failed
5124	FileVault disabling initiated
5125	FileVault disabling succeeded
5126	FileVault disabling failed
5127	FileVault password changed
5141	Enabling Octopus initiated
5142	Enabling Octopus succeeded
5143	Enabling Octopus failed
5144	Disabling Octopus initiated
5145	Disabling Octopus succeeded
5146	Disabling Octopus failed
5151	FIDO setup started
5152	FIDO setup succeeded
5153	FIDO setup failed

Event Code	Event Description
5161	SSO Portal launched
5164	Manual SSO portal launch initiated
5165	Manual SSO portal launch succeeded
5166	Manual SSO portal launch failed
5201	Online connection detected - locking the workstation
5202	Credentials expiration detected - locking the workstation
5301	Online authentication initiated
5302	Online authentication succeeded
5303	Online authentication failed
5304	Authentication challenge received
5308	Pre-authentication request succeeded
5309	Pre-authentication request failed
5321	Get Password request initiated
5322	Get Password request succeeded
5323	Get Password request failed
5331	Change Password request initiated
5332	Change Password request succeeded
5333	Change Password request failed

Event Code	Event Description
5401	BLE authentication initiated
5402	BLE authentication succeeded
5403	BLE authentication failed
5411	Offline authentication initiated
5412	Offline authentication succeeded
5413	Offline authentication failed
5422	Bypass success

Appendix A: Mac User Experience

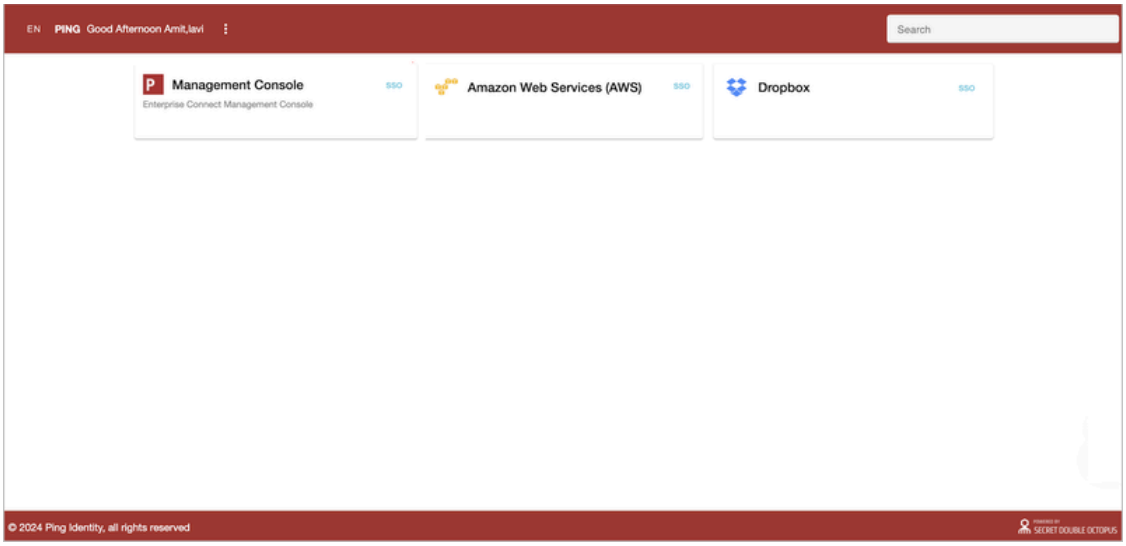
The following sections present various scenarios related to user experience:

- Accessing the User Portal
- Updating System Preferences
- Adding Your Machine to the Active Directory

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.

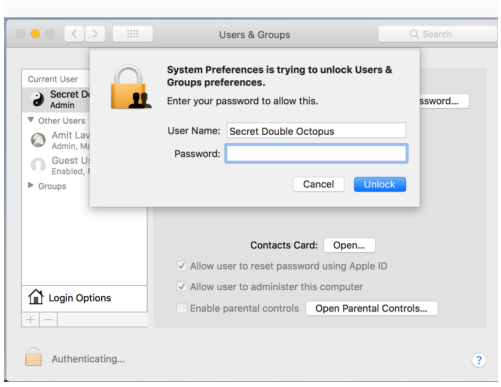
If the *ssourl* parameter of the configuration XML file is defined, that URL is used (Configuring the XML File.) If that parameter is empty, the target URL is taken from the Authentication Server.



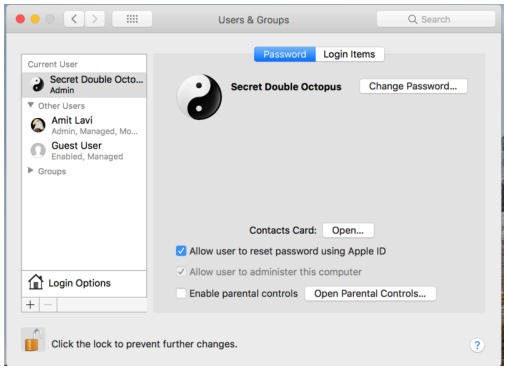
Updating System Preferences

Enterprise Connect Passwordless 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 mobile app.



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



Adding Your Machine to the Active Directory

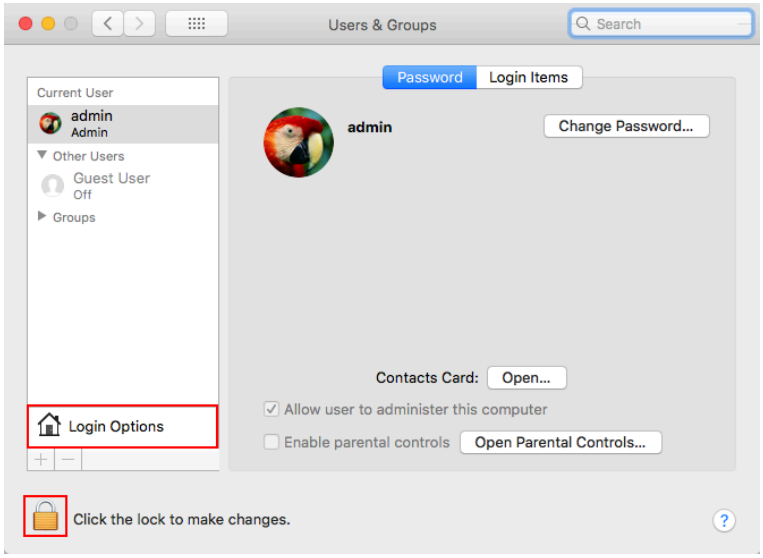
The following procedure describes how to add your Mac to the corporate Active Directory.

To add your machine to the AD:

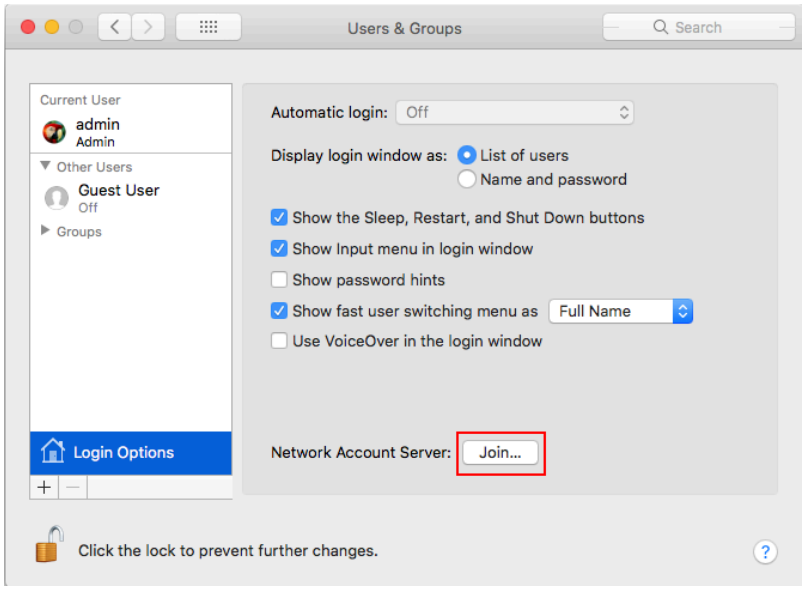
1. Open **System Preferences** and select **Users & Preferences**.

   The **Users & Preferences** dialog opens.

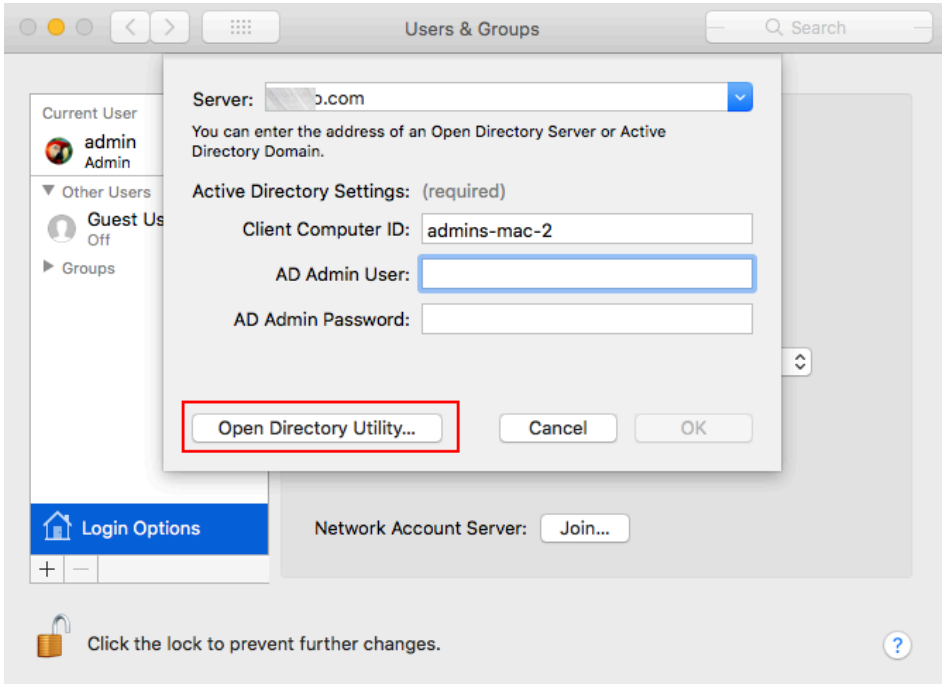
2. Click the Lock icon to enable editing mode. Then, click **Login Options**.



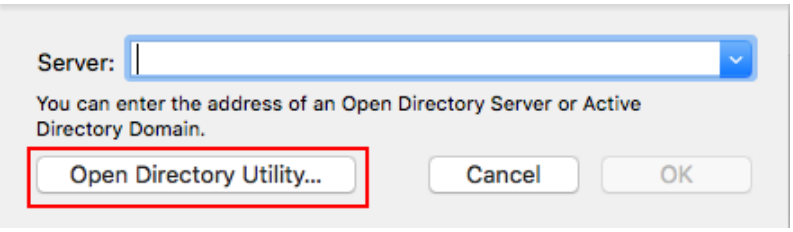
3. Next to **Network Account Server**, click **Join**.



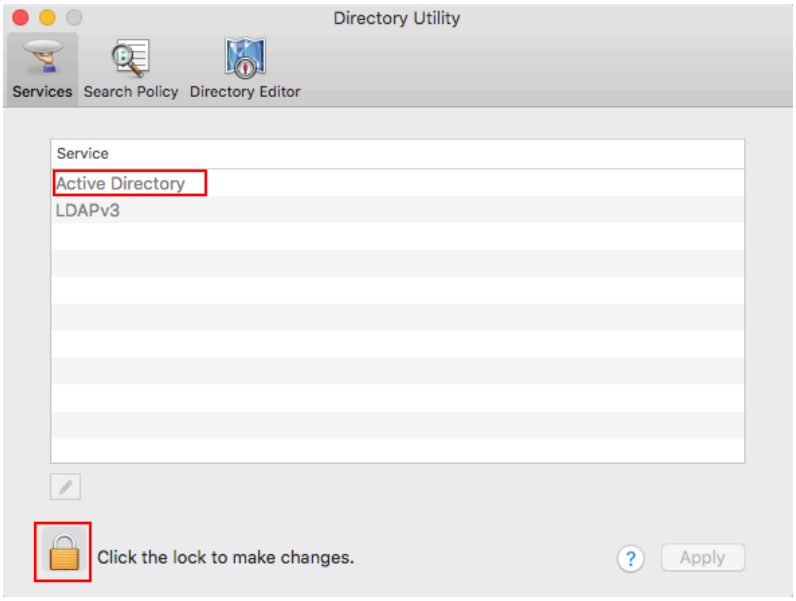
4. In the popup that opens, enter the address of the AD server and the credentials of the AD Admin. Then, click **Open Directory Utility**.



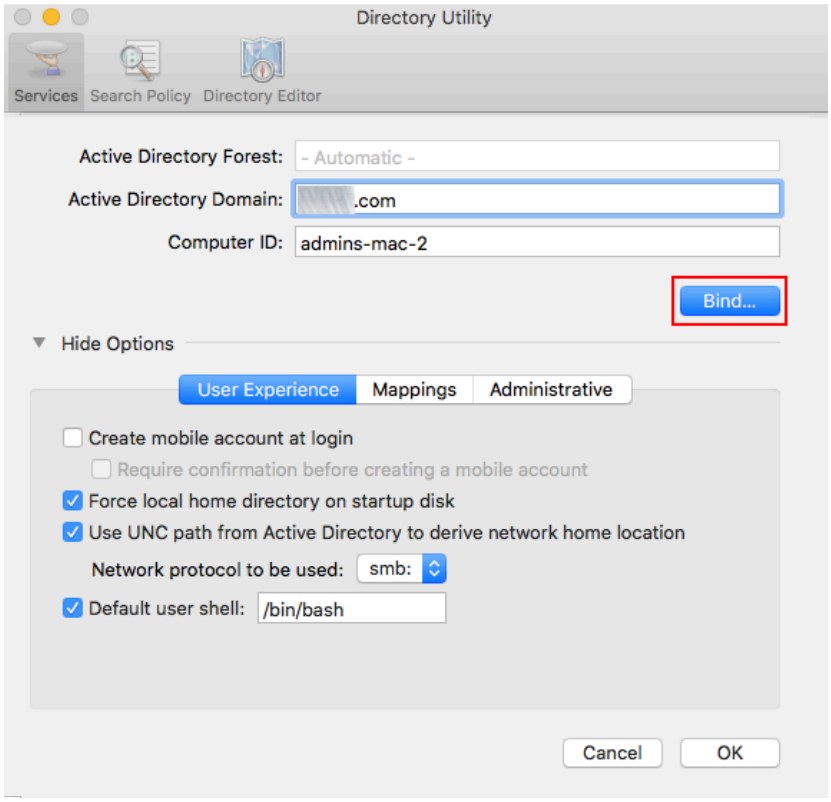
5. In the second popup that opens, re-enter the address of the server and then click **Open Directory Utility**.to open the **Directory Utility** dialog.



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

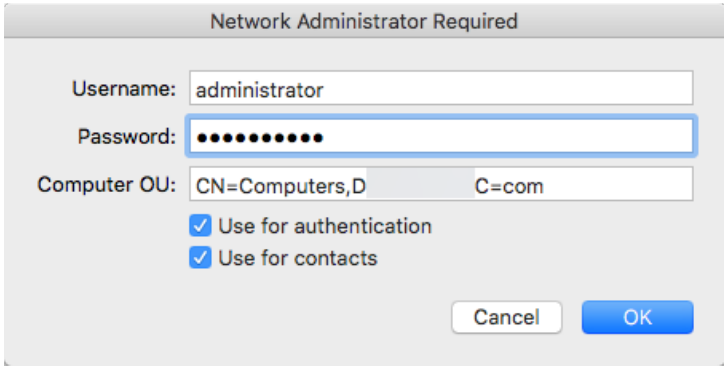


7. In the dialog that opens, click **Bind**.



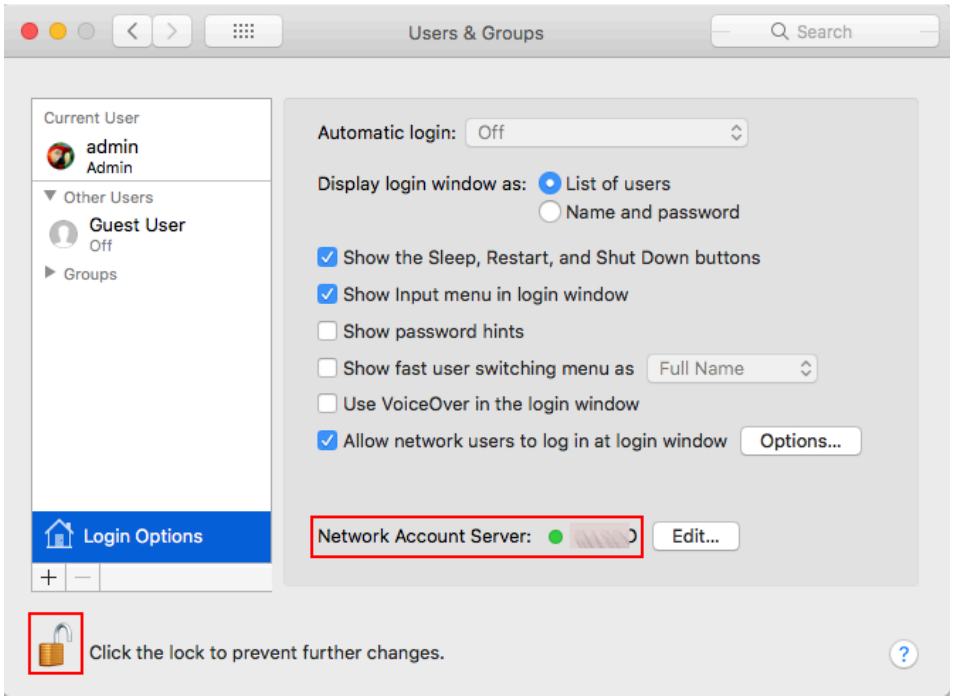
The **Network Administrator Required** popup opens.

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.

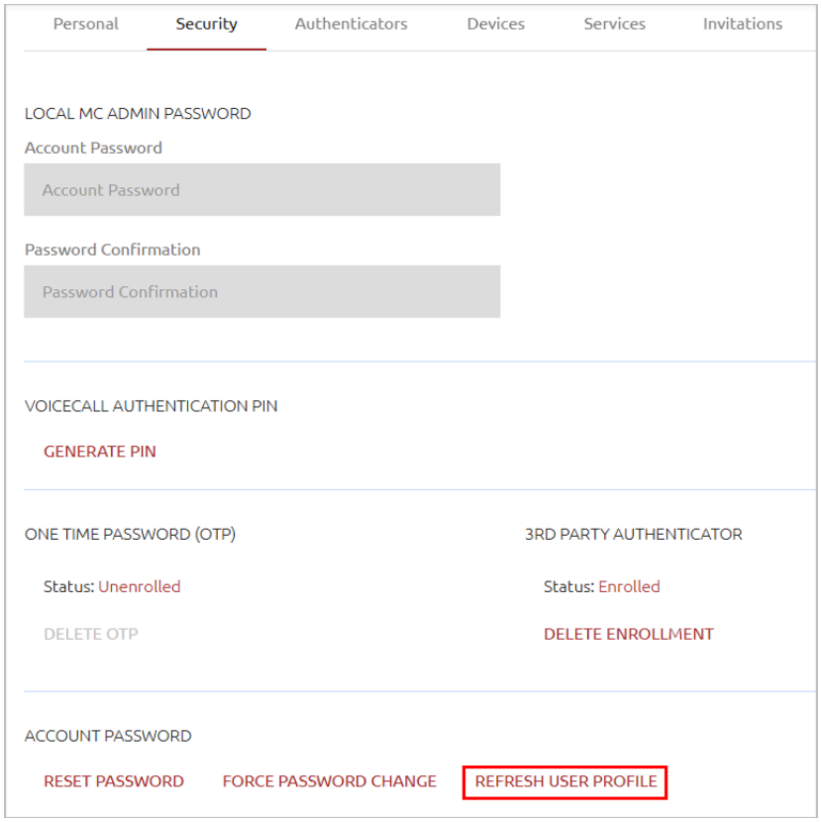


Appendix B: Known Issues

The following issues, discovered during software testing, will not be resolved in version 4.3:

- **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.
- **Password sync failure related to multiple user accounts:** Passwords do not automatically update when there is switching between accounts. Users need to lock and unlock the machine to initiate the password sync.
- **Automatic password sync:** The automatic password sync feature works only on the latest MacOS (Sonoma). Users of previous MacOS versions will receive the sync password popup screen.
- **Issues related to mobile accounts:**
    - FileVault Login cannot be enabled using the server configuration method.
    - FileVault Login cannot be disabled for mobile accounts.