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	
Product Overview	
Prerequisites	
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	
Enabling OTP Authentication	22
Enabling the Password Free Experience	
XML File Configuration	
Management Console Configuration	
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.

Search		Q
Active Directo	Active Directory Authentication Secret Double Octopus Active Directory	ADD
- egi	Amazon Web Services (AWS) Amazon SAML 2.0	ADD
<	Atlassian Jira Jira SAML 2.0	ADD
\$	Dropbox Dropbox SAML 2.0	ADD
IN	Generic SAML	ADD

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

Active Directory Authentication	
ssuer *	
Secret Double Octopus	Diman

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.

Active Dire	ectory Authentication	:		
General Info	Parameters	Sign on	Directories	Users
Service Name *	thentication		Display Icon	
issuer *				
Secret Double Octo	opus			
Description				
Description		li.		
SAVE				

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**).

Active Dire	ectory Authentication	:	
General Info	Parameters		Sign on
Parameters			
Service Parameters			-
Login Identifier *		_	
Username or Email			-
+ ADD PARAMETE	R		
SAVE			

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.

General Info	Parameters	Sign on	Direct	cories	Users	
Bypass Unassigned U	isers		Bypass Unen	rolled Users		
Sign on Method			Authenticatio	on Token Timeout	(1 minute - 1 year) *	
Active Directory			1	WEEKS		•
Endpoint URL			Rest Payload	Signing Algorithn	n	
https:/,	lo.com/adpa/3f560767	-0402-4bf 🖺	SHA-256			*
Service Keys *			X.509 Certific	ate *		
Default Sales Su	upport R&D	*	2022-02-17	12:05 SHA-256	2048-bit	•
VIEW		+ ADD	VIEW	DOWNLOA	D 🗘 REC	GENERATE
Custom Message *			_		_	
Active Directory a	uthentication		± SERVIC	e metadata 👻		
		1.				

- 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**.

General Info	Parameters	Sign on	Directories
DIRECTORIES IN SERV	ЛСЕ		
AD - sync: false	e e e e e e e e e e e e e e e e e e e		
AD - sync: true			
LOCAL ORACLE - synct	true		
CAVE			
SAVE			

8. Open the **Users** tab and click **Add**.

A popup opens, with a list of directories displayed on the left.

- 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.



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

```
Enterprise Connect Passwordless for Mac
Copyright © 2023 ForgeRock, All Rights Reserved.
```

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.

General Info	Parameters	Sign on	Direct	ories	Users
Bypass Unassigned User	rs		Bypass Unenr	olled Users	
Sign on Method			Authenticatio	n Token Timeout (1 n	ninute - 1 year) *
Active Directory			1	WEEKS	•
Endpoint URL			Rest Payload	Signing Algorithm	
https:/,	lo.com/adpa/3f560767	2-0402-4bf 🖺	SHA-256		Ŧ
Service Keys *			X.509 Certific	ate *	
Default Sales Sup	port R&D	-	2022-02-17	12:05 SHA-256 20	48-bit 👻
VIEW		+ ADD		DOWNLOAD	🗘 REGENERATE
Custom Message *					
Active Directory auth	hentication		<u></u> ⊻ SERVICI	e metadata 👻	
		11			

The following additional parameters may be updated, as required:

Parameter	Description	Example / Notes

mfa	Enables/Disables MFA. Default value is <i>false</i> (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 <i>false</i> (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 <i>false</i> .	<validpasswordissufficient>true</validpasswordissufficient>
forceLockAfterOfflineLogin	When set to <i>true</i> (default value), users who have logged in using offline authentication are required to reauthenticate when the workstation goes back online.	<forcelockafterofflinelogin>true<!--<br-->forceLockAfterOfflineLogin></forcelockafterofflinelogin>

Parameter	Description	Example / Notes
thirdparty	Determines whether users will have to approve authentication requests using a third party service. Default value is <i>false</i> (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 <!--<br-->ssourl></ssourl>
ssobrowser	When <i>ssourl</i> is defined, this parameter determines which browser is used to open the SSO portal. The default value, <i>system</i> , 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 <i>client</i> (default value), users can create their own password for FileVault Login. When set to <i>server</i> , the password is created and managed by the server	<ssobrowser>firefox</ssobrowser> Valid values are: • client • server <filevaultlogin>server</filevaultlogin>
automatickerberossync	When set to <i>true</i> (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<!--<br-->kerberosrealm ></kerberosrealm>
sudo	Enables/Disables authentication on command line sudo. Default value is <i>false</i> (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 info

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.

-	Welcome to the Enterprise Connect Decoverdings Installer	
 Introduction Destination Select Installation Type Installation Summary 	Welcome to the Enterprise Connect Passwordless Installer You will be guided through the steps necessary to install this software.	
	Go Back Continu	0

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

	🥪 Install Enterprise Connect Passwordless	8
	Standard Install on "Macintosh HD"	
 Introduction Destination Select Installation Type Installation Summary 	This will take 41.1 MB of space on your computer. Click Install to perform a standard installation of this software on the disk "Macintosh HD".	
	Go Back Install	5

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.)





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

	Enter Your Enterprise Account
This is t su	he username you use to access company resources ch as Active Directory, email, shared files, etc.
Account	amitauth
Account.	
Account.	

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**.

PIN Code
Enter the PIN code for your FIDO key or leave blank to use your fingerprint instead.
Skip
Cancel

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:

Scan the QR code with the OTP app on your mobile device:
Next
Cancel

- 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.

	authenticati mobile app.	on on the	Octopus Au	thenticator
am	Enter your pas	sword to allo	w this.	
	User Name:	Amit Lavi		
	Password:			
			Cancel	Authenticat

The following screen opens:

	Verife Veur Cede	
	verify your Code	
Enter the 6	digit code from your OTP authentic	ator app
	Construction of the Constr	
	Next	

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 **enterpriseconnect-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*.



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 🧨.

😑 🛷 Enterpr	ise Connect Passwordless		Posicist	۵	
 System Settings Directories 	Directories All Directories and Agents in the System. Agents are used to support remote	directories.			
Manage Users			Search		Q
Devices	AD - sync: false	AD - sync: true			
Services	Q :	May 12, 2023, 9:00:00 PM		:	
Portal	ORACLE - sunc' false	ORACLE - synct true			
Q Auditing	Oracle/Open LDAP 🖌 🖬	Oracle/Open LDAP	1	:	

2. Select the **Policy** tab.

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

🗖 AD - syr	nc: true : 🔎	Active Directory	🗘 🛛 Jun 11, 202	3, 4:00:00 PM	
Details	Domain Controllers	Links	Authenticators	Policy	Groups
PASSWORD SETT	INGS				
Password-Free Ex	Password-Free Experience Automatic Password Sync				
Password Length			Password Age (0)-1 уеаг)	
		8 Chars	20	DAYS	~
Special Chars			Alphanumeric		-

Then, go to Step 5 (below).

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

PASSWORD SETTINGS				
Password-Free Experience		Automatic Pas	ssword Sync	-
Password Length		Password Age	(0-1 year) *	
•	8 Chars	0	DAYS	•
Special Chars		Alphanumeric		

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]).



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.

• • •	
QA Doubleoctopus qadoubleoctopus	0
Account () Status	FileVault Login
System	Improve your Mac's security by setting a dedicated password for unlocking FileVault disk encryption.
FileVault	
Octopus	Setup
💿 Help	
💽 About	
If FileVault is turned on, skip to Ste	pg 3.
FileVault is off	na kokak okono.
Turn on FileVault disk end	cryption in the

Not Now

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

Turn On...

2.



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

FileVault Login
Flievault Login
Octopus lets you create a dedicated password for unlocking FileVaul disk encryption when powering on or restarting your Mac.
This password will only be used for FileVault Login, and won't change how you login to your user account.
Continue
Cancel

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**.

sveta		
Account System	• FileVault Login isn't fully configured FileVault Login is enabled on this Mac but your be configured to use it.	user account needs to
👩 FileVault 🕕		Configure
Octopus Pelp About		

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

Authentication Required

Open the Octopus Authenticator app on your mobile device and approve the operation.

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.

MACOS FILE VAULT PASSWORD SETTINGS				
Password Length		Password Age (0-1 year) *	
•	8 Chars	90	DAYS	-
Special Chars	-	Alphanumeric		-

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

😑 🔣 Enterpris	se Connect Passwordless				0 8		٩	🗸 Supe	r Admin
 System Settings Directories Manage Users 	Devices All Workstations in the System Workstations III IIII					Search			() Q
Powered by SECRET	Actions Hame AMIT_LAPTOP_LOC AMIT_LAPT	App Name c : for Windows Octopus for Mac	App Version 03.04.00.4089 02.03.02.143	OS Hame Windows 10 Pro macOS	05 Version 19042 11.3.1	Manufacturer VMware, Inc. Apple Items per page	Model VMwarr e: 10 1-:	17,1 17,1 20072 <	>

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.

• • • • • • • • • • • • • • • • • • •	
	Kerberos
Account	
🔼 Status	Kerberos login failed.
Authenticators	The last Kerberos login attempt failed because the password was invalid.
L Reibelos	Renew
System System FileVault Octopus Help About	

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.

Gene	ral FileVault Firewall P	rivacy
😵 Photos	Allow the apps below to	o control your computer.
Camera	AEServer	
Microphone		
Speech Recognition	Octopus	
Accessibility		
Input Monitoring		
Full Disk Access	+ -	
Files and Folders		
Screen Recording		
Media & Apple Music		

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**.

•••		
QA Doubleoctopus qadoubleoctopus	Hel	p
Account	Troubleshooting Enterprise Connect Passwordless is o	configured to write basic logging
🔼 Status 🕕 🕕	Messages. No private information will	Bug Report
System		bug keport
o FileVault	Uninstall	
Octopus	Requires authenticating as a user wit make sure you know your current Ma	h administrator privileges. Please c password before uninstalling.
O Help		Uninstall
🔀 About	- 5	

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**.

	۵
6	svetika
	Renew Kerberos Ticket
	Enter Password in Finder
	Launch SSO portal with Octopus Authenticator / Bypass token
	Open Enterprise Connect Passwordless Preferences

Then, select the Help menu.

QA Doubleoctopus gadoubleoctopus	Help	
Account	Troubleshooting Enterprise Connect Passwordless is configured t messages. No private information will be written View Logs	o write basic logging to the logs.
System FileVault Octopus	Uninstall Requires authenticating as a user with administra make sure you know your current Mac password	ator privileges. Please before uninstalling.
 Help 		Uninstall
Mout About		

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.

		🖬 ibsdo.doubleoctopus.net		0	A 0 +
Good Evening Amit Lavi	1				Search
Cotopus Manager	ment Console 550	Microsoft Office365	550	Slack	SSO
JIRA Production	an Jira sso	er AWS (Customer Success)	\$50	disco VPN	850
zoom ZOON	550	😂 Dropbox	\$\$0	🛫 Amazon Web Services (AW	/S) sso
Powered by Octopus Authenticator					

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.

Current User admin ✓ Other Users Groups	Automatic login: Off Clist of users Display login window as: List of users Name and password Show the Sleep, Restart, and Shut Down buttons Show lnput menu in login window Show password hints Show fast user switching menu as Full Name Use VoiceOver in the login window
Login Options	Network Account Server: 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**.

000	Users & Groups	Q Search
Current User admin Admin Conter Users Guest Us Off Groups Cuest Us Cuest Cuest Cuest Cuest Cuest Cuest Cues	Server: D.com You can enter the address of an Open Directory Server or Active Directory Domain. Active Directory Settings: (required) Client Computer ID: admins-mac-2 AD Admin User: AD Admin Password: Open Directory Utility Cancel O ions Network Account Server: Join	 ▼ ▼ ▼ ×
Click the	lock to prevent further changes.	?

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.

Server:			~
You can e Directory	nter the address of an Op Domain.	en Directory Server or Acti	ve
Open	Directory Utility	Cancel	OK

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

Service Active Directory LDAPv3 LDAPv3 Click the lock to make changes. () Apply In the dialog that opens, click Bind. Directory Utility	Directory Uti	lity
Click the lock to make changes. Click the lock to make changes. Apply In the dialog that opens, click Bind . Directory Utility	Service Active Directory LDAPv3	
In the dialog that opens, click Bind .	Click the lock to make changes.	? Apply
Directory Utility	In the dialog that opens, click Bind .	
Services Search Policy Directory Editor	Directory	Utility

7.

Active Directory Forest:	- Auto	matic -		
Active Directory Domain:	RITT	.com		
Computer ID:	admin	s-mac-2		
				Bind
 Hide Options 				
User Expe	rience	Mappings	Administrative)
 Create mobile account Require confirmatio Force local home direct Use UNC path from Action 	at login on before tory on s tive Dire	e creating a m startup disk ectory to deriv	nobile account ve network home k	ocation
Network protocol to be	e used:	smb: ᅌ		
✓ Default user shell: /bi	n/bash			

The Network Administrator Required popup opens.

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

	Network Administrator R	lequired
Username:	administrator	
Password:	••••	
Computer OU:	CN=Computers,D	C=com
	Use for authentication	
	🗸 Use for contacts	
		Cancel 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.

$\bullet \bullet \circ \checkmark $	Users & Groups	Q Search
Current User	Automatic login: Off Display login window as: List of users Name and passw Show the Sleep, Restart, and Shut Down b Show Input menu in login window Show password hints Show fast user switching menu as Full N Use VoiceOver in the login window Allow network users to log in at login window	vord uttons lame © ow Options
Login Options	Network Account Server:	
Click the lock to preven	t further changes.	?

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.

Personal	Security	Authenticators	Devices	Services	Invitations
LOCAL MC ADMI	IN PASSWORD				
Account Passwo	rd				
Account Passy	word				
Password Confir	mation				
Password Con	firmation				
VOICECALL AUTI	HENTICATION PI	N			
ONE TIME PASSV	INE TIME PASSWORD (OTP)		3RD PARTY AUTHENTICATOR		
Status: Unenro	olled		9	Status: Unenrolled	ł
DELETE OTP			[DELETE ENROLLM	AENT
ACCOUNT PASS	WORD				
RESET PASSW	ORD FORC	E PASSWORD CHANGE	REFRESH	USER PROFILE	
AUTHENTICATO	R				
BYPASS USER	•				
SAVE					

- 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.