Enterprise Connect Documentation

Version 2.0.3

The use of the information contained in this document is subject to the following conditions and restrictions:

- No part of its contents may be used for any other purpose, disclosed to any person or firm, or reproduced by any means, electronic or mechanical, without the express prior written permission of Apple Inc.
- The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.
- Information in this document is subject to change without notice.

RESTRICTION ON USE, DUPLICATION, OR DISCLOSURE OF PROPRIETARY INFORMATION

This document contains information proprietary to Apple Inc. Each party has a legal obligation to protect such information from unauthorized disclosure, use, or duplication. Any disclosure, use, or duplication of this document or of any of the information contained herein for other than the specific purpose for which it was disclosed is expressly prohibited, except as Apple Inc. may otherwise agree to in writing.

Introduction

What is Enterprise Connect?

Enterprise Connect is an application that enhances Active Directory integration for Mac systems. It performs three main functions:

Kerberos

Enterprise Connect acquires a Kerberos Ticket Granting Ticket (TGT) when it detects your organization's network and automatically refreshes the ticket as needed. A Kerberos TGT is useful for organizations that use Kerberos authentication for resources like web sites or network share points.

Account Management

Enterprise Connect uses the macOS Notification Center to notify a user when their Active Directory password is nearing expiration. The user simply clicks the notification to change their Active Directory password within Enterprise Connect.

Network Share Management

Enterprise Connect can mount an Active Directory network home directory as well as SMB/AFP shares defined by the user or administrator. Additionally, if these shares are disconnected, the shares will be automatically re-mounted when the organizational network comes back online.

Requirements

Enterprise Connect 2.0 requires the following:

- OS X El Capitan (10.11) or later
- An Active Directory domain using Windows Server 2008 or later functional mode
- Connectivity to the network hosting the Active Directory domain
- An Active Directory account

Enterprise Connect does not require a Mac to be bound to Active Directory, nor does it require the user be logged into the Mac with an Active Directory account. Additionally, no server-side components are needed.

How does it work?

Setting up Enterprise Connect is simple. An administrator can configure Enterprise Connect to remind the user to set it up, or the user can double click the Enterprise Connect application and sign in with their Active Directory account.

When your organization's network is detected, Enterprise Connect refreshes the user's Kerberos TGT, checks their password expiration status and re-mounts any shares that have become disconnected. Going forward, the user only needs to interact with Enterprise Connect if they need to change their Active Directory password or configure the application.

New in this release

Enterprise Connect 2.0 is a major release and includes a variety of new features:

- Enterprise Connect has been substantially restructured and broken up into 3 applications. All apps still live inside the Enterprise Connect app bundle in the /Applications directory.
- Enterprise Connect is launched automatically with launchd. Login items or custom processes to launch Enterprise Connect are no longer necessary.
- Setup notifications will make it easier for your users to initially set up Enterprise Connect.
- Fine grained password policy is now supported for determining password expiration.
- Enterprise Connect notifications can be customized with your organization's logo. Set "orgLogoPath" in your Enterprise Connect plist or configuration profile to the path to a JPG, GIF or PNG file with your company logo. The logo should be square and of sufficient resolution.
- Live password testing has been enhanced to display minimum password age and password history requirements.
- You can change the "Username:" label in Enterprise Connect to a custom value, like the name your organization uses for user IDs.
- The Enterprise Connect menu extra is now optional.
- Smart card support has been built into Enterprise Connect.
- Password sync is now supported for smart card users.
- Connection reminders will remind users to connect to the network if they haven't done so for at least 7 days.
- The Enterprise Connect UI has been enhanced.

Basic Installation and Usage

Getting Started

Installation

Installation is simple: just double-click on the Enterprise Connect package to run the Enterprise Connect installer on your Mac. Once the installation is complete, Enterprise Connect will be installed in the Applications folder.

Setup

Connect to your organization's network, then launch Enterprise Connect. When you launch Enterprise Connect for the first time, you'll see a window like this:

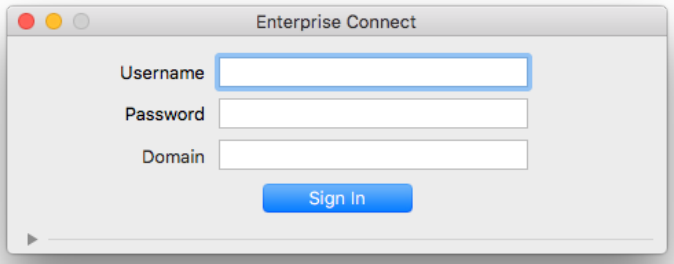


Figure 1: Enterprise Connect Setup Window

Running Enterprise Connect while logged in with an Active Directory (AD) account automatically populates the Username and Domain fields. You'll just need to enter your Active Directory password. Otherwise, fill in the fields as shown below:

Username: The username or UPN for your Active Directory account. Logging in with "DOMAIN\username" is not supported. UPN login is not supported for smart card users.

Password: The password for your Active Directory account.

Domain: The domain that your Active Directory account is in. Use the fully qualified name. For example, use "domain.pretendco.com" instead of "DOMAIN".

Once you've filled in all of the fields, click "Sign In." Enterprise Connect will connect to the domain and authenticate.

Basic setup of Enterprise Connect is now complete! From now on, if the Enterprise Connect icon in your menu bar (the key with a circle around it) is black, you're connected to your organization's network. If the icon is grey, you are not connected to your organization's network.

	Enterprise Connect icon: you're connected
	Enterprise Connect icon: you're not connected

Figure 2: Enterprise Connect Connection Status

Configuring Network Share Points

Overview

Enterprise Connect can mount the network share points you commonly access, including the share point that is defined for your Active Directory account. Moreover, if these shares become disconnected when your Mac leaves your organization's network, Enterprise Connect will automatically re-connect these shares when your Mac is back on your network.

Requirements

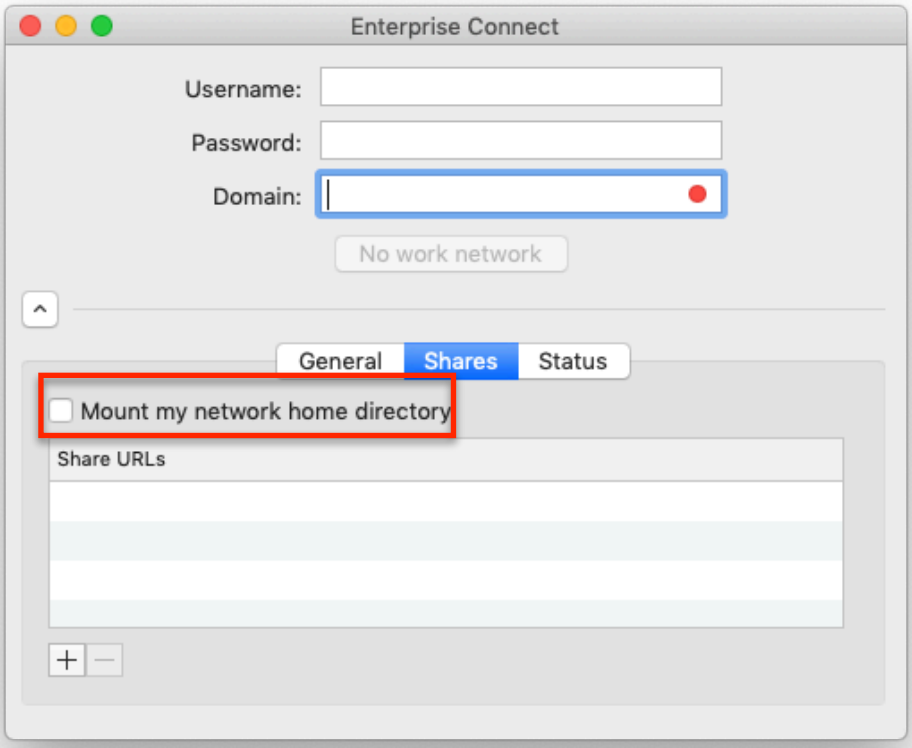
You can use SMB- or AFP-based share points with Enterprise Connect. If you are using a DFS-based share point with Enterprise Connect, you'll be prompted to authenticate unless your Mac is bound to your organization's Active Directory domain. You'll also need to know the URLs of the shares you want Enterprise Connect to automatically mount.

Mounting a network home directory

Enterprise Connect can mount your network home directory. Ask your network administrator if your Active Directory account has a network home directory.

1. Click on Enterprise Connect in your menu bar, then click "Open Enterprise Connect."
2. The main Enterprise Connect window will appear. Click the disclosure triangle on the left side of the window. Next, click the Shares tab. You'll see a window that looks like this:
3. Check the "Mount my network home directory" check box.
4. Click "Mount Shares." Verify that your network home directory mounted in the Finder.

Figure 3: Configure a network home directory to mount via Enterprise Connect's main window



Mounting other share points

Enterprise Connect can mount SMB or AFP share points.

1. Click on Enterprise Connect in your menu bar, then click “Open Enterprise Connect.”
2. The main Enterprise Connect window will appear. Now, click the disclosure triangle on the left side of the window. Finally, click the Shares tab. You’ll see a window that looks like this:
3. Click the “+” button. A new row will appear in the share list.
4. Enter the URL for your share point in the “Path” field. The URL should look like “smb://server.pretendco.com/share” or “afp://server.pretendco.com/share."
5. Repeat step 4 for all of the share points that you’d like Enterprise Connect to mount.
6. Click the Enterprise Connect icon in your menu bar, then click “Reconnect.” Wait a few seconds, then verify all of your network shares have mounted. If any shares didn’t mount, verify that the shares are available and that you entered the correct URL, then try again.

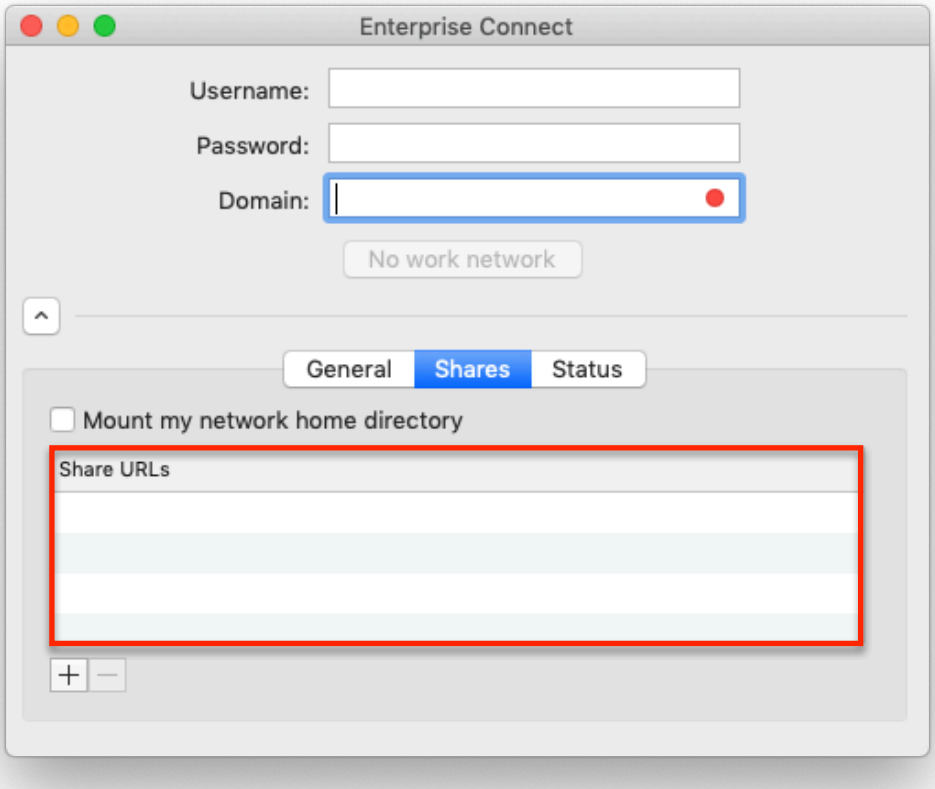


Figure 4: Use the main window to configure network shares for auto-mounting

Managing your Active Directory Account

Overview

Enterprise Connect can help you manage your Active Directory account. Specifically, it will notify you when your password is going to expire and allow you to change your Active Directory password.

Password notifications

By default, Enterprise Connect will begin sending notifications 15 days before your password expires. You'll be notified every 24 hours until you change your password. You need to be connected to your organization's network to receive notifications.

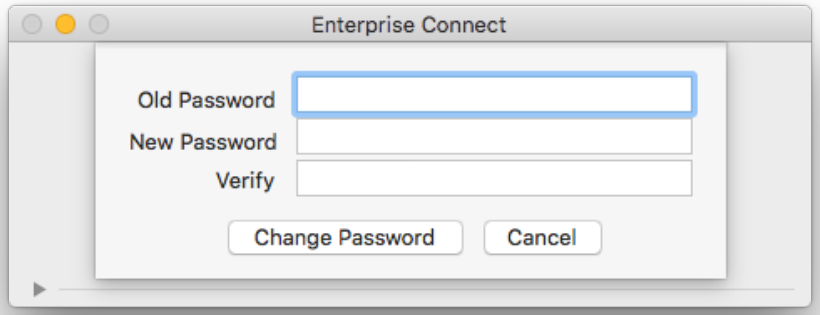
Enterprise Connect delivers notifications via the macOS Notification Center. When you see a notification, you can click a button to change your password or ignore the notification.

Manual password changes

You can change your Active Directory password without receiving a notification. To do so, follow these steps:

1. Make sure you are connected to your organization's network. Password changes will fail unless you are connected to the correct network.
2. Go to the Enterprise Connect menu in your menu bar and select "Change password..." You'll see a menu like this:

Figure 5: Update your password from within Enterprise Connect.



3. Enter in your old password, then enter your new password in the bottom two fields. Now click "Change Password."
4. Click OK to close the Enterprise Connect window after successfully changing your password. In the case your password change wasn't successful, review the error message and attempt your password change again.

Upgrade Process

Enterprise Connect 1.x

Introduction

For most users of Enterprise Connect 1.x, the upgrade process will be unchanged from previous upgrades. Simply push the Enterprise Connect install package to target Macs and they will be silently upgraded. However, in some situations, changes to Enterprise Connect settings may be needed in order to ensure a smooth upgrade.

Upgrade Process

When you install the Enterprise Connect 2.0 installer, the following occurs:

1. Before beginning, the installer checks to see if an older version of Enterprise Connect is already installed. If it is, the installer creates an invisible file in /Users/Shared called ".ecNeedsUpgrade1x".
2. Enterprise Connect is installed.
3. The old version of Enterprise Connect will quit
4. The installer will create a launchd plist in /Library/LaunchAgents to launch ecAgent (Enterprise Connect agent). If a user is logged in, this plist will be loaded and ecAgent will start. If no user is logged in, ecAgent will start when a user logs in.
5. The Enterprise Connect menu extra will load.
6. ecAgent will detect that an upgrade has occurred. It will launch the Enterprise Connect application. Enterprise Connect will then remove the Enterprise Connect login item and re-create the Enterprise Connect keychain entry so that both ecAgent and the Enterprise Connect app have access to it. It will then quit. This process is very fast so the user will see Enterprise Connect running for just a moment.
7. If your network is available, ecAgent will connect to the network. If password sync is enabled, it will verify that your passwords are in sync.
8. Upgrade is complete.

For most users, additional steps will not be needed.

Additional steps

You may need to take additional action if any of the following applies to your deployment:

1. You are running a Windows Server 2003 based domain. Enterprise Connect 2.0 requires a domain using Windows Server 2008 or greater functional mode. Either upgrade your domain to a more modern functional level before upgrading or continue to use Enterprise Connect 1.9.5.
2. You are using a script or solution of some kind to launch Enterprise Connect automatically upon installation. You no longer need to do this - Enterprise Connect launches automatically and uses Setup Notifications to make it easy for your users to get signed in. Remove this script or solution from any Macs that are upgraded to Enterprise Connect 2.0.
3. You were using something other than the standard login item to launch Enterprise Connect 1.x. For example, you might have been using a custom launchd plist or a managed login item (from a configuration profile). Remove these prior to upgrade - they are no longer needed with Enterprise Connect 2.0.
4. You are using AppleScript to interact with Enterprise Connect. In your AppleScripts, instead of using "tell application "Enterprise Connect"", use "tell application "ecAgent"". If you are using eccl, no modifications are needed.

Enterprise Connect PKI

Introduction

The process for upgrading to Enterprise Connect 2.0 from Enterprise Connect PKI requires some minor additional steps, on top of the above additional steps:

1. If you are using a configuration profile for Enterprise Connect PKI, duplicate it and change the preferences domain from "com.apple.enterpriseconnectPKI" to "com.apple.Enterprise-Connect". Doing so will allow Enterprise Connect 2.0 to use existing Enterprise Connect PKI managed settings.
2. In your new configuration profile, set "smartCardMode" to true. This is a boolean value. Doing this will automatically configure Enterprise Connect 2.0 to use smart cards.
3. After installation of Enterprise Connect 2.0, quit and remove Enterprise Connect PKI. See the Appendix for a simple script that performs this function.
4. Your end users will need to sign into Enterprise Connect 2.0. They simply need to click on the setup notification or launch the Enterprise Connect application, choose their smart card identity and click "Sign in". Entering a username is no longer required.

Advanced Usage

Advanced Settings

Introduction

Enterprise Connect has several settings that an advanced user or IT department can use to customize the application. Some of these settings are accessible from the Enterprise Connect GUI, but others are not. The following section details the functions and use of these settings.

Setup notifications

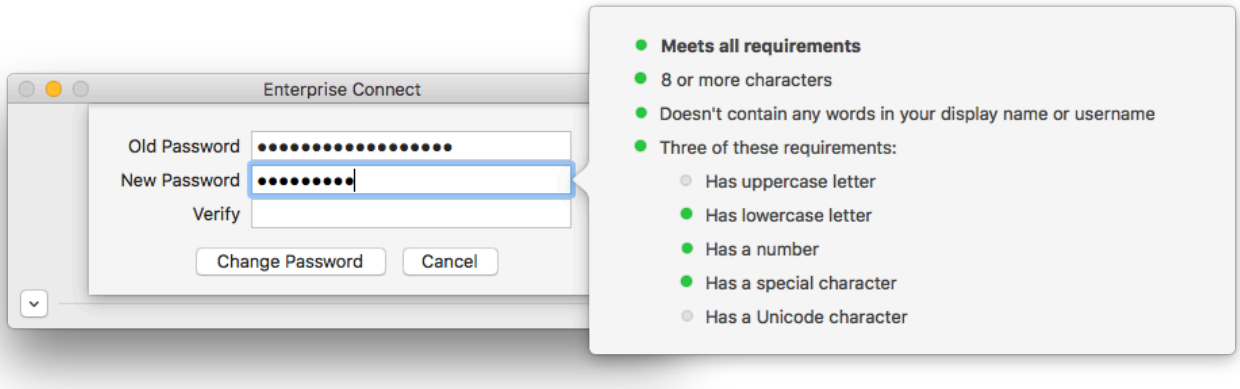
Setup notifications make it easy for your users to get started with Enterprise Connect. When your network becomes available, users will be prompted to set up Enterprise Connect if they haven't already done so. They will be prompted to set up Enterprise Connect every 24 hours, until they set the application up. To use setup notifications, simply set "adRealm" (the FQDN of your domain) in your Enterprise Connect configuration profile.

Connection reminders

Connection reminders are notifications to remind your users to connect to the corporate network if they haven't done so recently. To use connection reminders, simply set "connectReminderTime" to the amount of time (in seconds) after which you want to remind users to connect to the network. We recommend starting with 7 days.

Live password testing

In many Active Directory configurations, Enterprise Connect can test the user's new password as they enter it and tell the user what password requirements they still must meet before changing their password. When configured, the user will see this popover when entering their new password:



To use this feature, your Active Directory domain must only use standard Active Directory password policies. By default, Active Directory allows an administrator to require that a password be "complex" and that a password be a certain length. To learn more about what constitutes a complex password, see:

https://technet.microsoft.com/en-us/library/cc786468(v=ws.10).aspx

You may not be able to use this feature if your domain uses third-party tools or DLLs to extend standard Active Directory password policy. For example, if you are not allowed to use certain words other than your username in your password or you must use a specific amount of special characters in your password, you might be using third-party password policy extensions. If you're unsure, ask your Active Directory administrator for more information.

If your Active Directory domain meet the requirements, here's how you enable live password testing:

1. In your Enterprise Connect configuration profile, set "pwReqComplexity" to true (boolean) if your organization requires complex passwords.
2. In your Enterprise Connect configuration profile, set "pwReqLength" to the required password length (integer).
3. (Optional) In your Enterprise Connect configuration profile, set "pwReqHistoryCount" to the amount of previous passwords that cannot be re-used (integer).
4. (Optional) In your Enterprise Connect configuration profile, set "pwReqMinimumPasswordAge" to your domain's minimum password age, in days (integer).
5. If you want to disable the Unicode character requirement, set "pwReqComplexityDisableUnicode" to true (boolean) in your configuration profile.
6. Restart Enterprise Connect for these changes to take effect.

Live password testing has some limitations. It cannot test if a password has already been used. It is also unable to test if your password contains your Active Directory display name if you don't already have a Kerberos ticket. This may happen if you are setting your password for the first time or if your password has expired. All other tests will work normally.

Password requirements display

If you can't use live password testing, you can configure Enterprise Connect to display a document with your organization's password requirements as they enter their new password. Here's how you enable password requirements display:

1. Create an RTF or RTFD document containing your password requirements. Keep this document concise so your user doesn't have to scroll too much. If you embed an image into your RTFD file,

make sure the image will display properly inside Enterprise Connect and will not be clipped or require excessive scrolling.

2. Deploy the RTF document you created to your Mac systems, preferably with a management solution. The RTF document needs to be copied to the same file system location on all of your Mac systems. Make sure your users have read permissions to this file.
3. In your Enterprise Connect configuration profile, set "pwReqText" to the path to your RTF file.
4. Restart Enterprise Connect for these changes to take effect.

Changing or disabling password functionality

Some organizations may not be able to use Enterprise Connect's standard password change functionality. These organizations may need their users to change their password somewhere other than Active Directory, like a password change website.

Since version 1.5, Enterprise Connect has allowed you to disable all password-related functionality. In version 1.7, administrators gained more control over the password change process. You can still set the "disablePasswordFunctions" preferences key to true (boolean) to disable all password related functionality. If you just want Enterprise Connect to disable password expiration checking, you can set "disablePasswordExpirationChecking" to true (boolean).

Password change web site support

Enterprise Connect 1.7 and greater can be configured to open a password change web site in the user's default browser when they select "Change password" or click on a password expiration notice. We recommend using this feature only while logged in with a local account.

In your configuration profile, set "passwordChangeURL" to the URL of your password change website. When a user changes their password, Enterprise Connect will ask them if they want to sign out. If they choose to sign out, they will be signed out of Enterprise Connect and the password change website will open. Once the user has changed their password, they will need to sign back into Enterprise Connect with their updated password. If local password sync is enabled, the user will be asked for their local password and the password change script will run (if configured).

Pre-populated usernames

Enterprise Connect 1.9 and greater can be configured with a pre-populated username. An administrator can pre-populate the Enterprise Connect Username field with a username of their choice. Upon launching the application, or upon sign out, the Username field will be pre-populated with the specified username.

To use the pre-populated username, run the command below as the user who will be running Enterprise Connect:

```
defaults write com.apple.Enterprise-Connect prepopulatedUsername -string
jappleseed
```

Replace "jappleseed" with the username you want to pre-populate.

You should not use the prepopulatedUsername key in a configuration profile, as this setting will be different on every system.

Branding

In Enterprise Connect 2.0 you can customize the icon used in notifications, as well as the text used in the label for the "Username:" field. See the "Using configuration profiles" section of this document for information on "orgUsernameLabel" and "orgLogoPath". Some guidelines:

1. In "orgUsernameLabel", you can omit the colon (:).
2. Deploy the organization logo to a consistent location on all of your Macs, and make sure all users have read access to it.
3. The organization logo should be of an adequate size to look good on your organization's displays. 512x512 is a good starting place.

Active Directory to local password sync

Enterprise Connect can set the user's local password to match their Active Directory password. To enable this feature, the user can simply check the "Keep my Mac login and Active Directory passwords in sync" checkbox under the General tab in Enterprise Connect. Alternatively, an administrator can configure this feature via a configuration profile.

When Enterprise Connect is used to change the password, this feature sets the user's local password to match the user's Active Directory password. Additionally, should the local and Active Directory passwords fall out of sync, Enterprise Connect will bring them back into sync. Here's how this works:

- Upon enabling this feature, and upon every subsequent connection attempt by Enterprise Connect, the user's Active Directory password will be checked against the local account. If the Active Directory password is able to authenticate against the local account, the passwords are in sync and no action is needed. If the Active Directory password cannot authenticate the local account, Enterprise Connect will prompt the user for their local password. Once the user supplies their local password, Enterprise Connect will set their local password to match their Active Directory password.
- Password changes work in a similar fashion. When the user performs a password change with Enterprise Connect, the user's old Active Directory password will be checked against the local account. If the old Active Directory password and the local password match, Enterprise Connect will change both passwords. If they do not match, only the Active Directory password will be

changed, then the user will be prompted for their local password during the next connection attempt.

To use this feature, please be aware of the following:

1. If the user is logged into their Mac with an Active Directory (not a local) account, the "Keep my Mac login and Active Directory passwords in sync" checkbox will be disabled. This feature is only intended for use with local accounts – if the user is logged into their Mac with an Active Directory account, this feature is not needed.
2. If password policy is being enforced on local accounts, for example, via a configuration profile or via the `pwpolicy` command, make sure the password policy matches, or is less strict than the Active Directory password policy. If local password policy is more strict than Active Directory policy, Enterprise Connect may accept a password that meets Active Directory requirements, but fails to set the local password, since the password does not meet local password requirements. If local password policy must be more strict than Active Directory password policy, you should not use this feature.
3. The local username is not set to match the Active Directory username— only passwords are set to match.

Scripting support

Overview

Enterprise Connect exposes several of its functions and properties via AppleScript. Additionally, an administrator can use a command line tool called "eccl" to perform all of the same tasks available to AppleScript.

AppleScript Dictionary

Enterprise Connect includes an AppleScript dictionary which describes all of the commands and properties available for use with Enterprise Connect.

You can view the dictionary by doing the following:

1. Launch the "Script Editor" application in your Mac's "Utilities" folder.
2. Choose "File->Open Dictionary...".
3. Choose Enterprise Connect from the list of applications.
4. In the list on the top left, click "Enterprise Connect Suite".

Sample AppleScripts

Enterprise Connect includes some sample AppleScripts that use Enterprise Connect's AppleScript functionality. These scripts aren't intended for use "as-is" – they should be used to help you get started with writing your own scripts. In the folder you downloaded that includes the Enterprise Connect installer, open the "Enterprise Connect scripting support" folder to see example AppleScripts.

Command line support

You can also access Enterprise Connect's scripting functionality from the command line. Enterprise Connect includes a tool called "eccl" which allows you to access this functionality. For more information, run:

```
/Applications/Enterprise\ Connect.app/Contents/SharedSupport/eccl –h
```

Extension attributes

You may want to make information from your Enterprise Connect scripts available as extension attributes via your management solution. If you choose to do this, your extension attributes should not directly request the information from Enterprise Connect in most cases. If Enterprise Connect is not running or a user is not logged in, your extension attributes will not be populated correctly.

Instead, refer to the "Enterprise Connect scripting support" folder. We've included a script that should be run as a "connection completed" script (see below). It gathers the information you request from Enterprise Connect, then puts that information in a special preferences list (plist). Your extension attributes then read the information you want to use in extension attributes from this plist. Using this method, your extension attributes will be correctly populated, even if Enterprise Connect is not running.

Event scripts

Overview

Enterprise Connect can run scripts when the following events occur:

- When your corporate network is detected
- After Enterprise Connect completes its connection process
- Upon a successful password change

Enterprise Connect cannot run scripts as root. All scripts are executed as the currently logged-in user. As such, your script shouldn't use the sudo command or attempt any actions that require root privileges.

All scripts are passed the username and domain of the user signed into Enterprise Connect. From your script, you can access these values as $1 and $2.

Enterprise Connect will not execute scripts that don't have correct permissions. Specifically, permissions must be set so that:

- Only the root user can modify the script.
- The user running Enterprise Connect can read and execute, but not modify the script.

Audit script

Enterprise Connect can run a script before connecting to your network. This script is intended to be used to audit the target Mac to make sure your organization's security requirements are met. Enterprise Connect will notify users if their Mac doesn't meet requirements to run Enterprise Connect and will advise them to contact IT. Users will see the status of the audit script in the Enterprise Connect menu.

To enable the audit script, do the following:

1. Write a shell script that checks for system for compliance. It should return 0 if the system is compliant and some other number if it's not compliant. Put this script in a location where users have permissions to read and make it executable.
2. Put the script in your preferred location. Set the owner of the script to "root" and set POSIX permissions to "755", like so:

   ```
   chmod 755 /path/to/script
   ```
3. In your Enterprise Connect configuration profile, set the runAuditScript key (Boolean) to true.
4. In your Enterprise Connect configuration profile, set the runAuditScriptPath key (String) to the path to your audit script.
5. The audit script will execute the next time Enterprise Connect connects to your network.

If you do not set runAuditScriptPath, Enterprise Connect will look for and execute a script at /Library/Scripts/enterpriseConnect.

Connection Completed Script

Enterprise Connect can run a script after connecting to your network. This script can be used to perform any tasks needed after making a successful connection to the network.

To enable the Connection Completed script, do the following:

1. Write a shell script that performs any tasks that you choose.
2. Put the script in your preferred location. Set the owner of the script to "root" and set POSIX permissions to "755", like so:

   ```
   chmod 755 /path/to/script
   ```

3. In your Enterprise Connect configuration profile, set the connectionCompletedScriptPath key (String) to the path to your connection completed script.
4. The connection completed script will be executed the next time Enterprise Connect connects to your organization's network.

Password Change Script

Enterprise Connect can run a script after a user has performed a successful password change. This script can potentially be used to remove old Keychain entries and a variety of other tasks you may choose to complete upon password changes.

To enable the password change script, do the following:

1. Write a shell script that performs any tasks that you choose.
2. Put the script in your preferred location. Set the owner of the script to "root" and set POSIX permissions to "755", like so:
   ```
   chmod 755 /path/to/script
   ```
3. In your Enterprise Connect configuration profile, set the passwordChangeScriptPath key (String) to the path to your connection completed script.
4. Restart Enterprise Connect. The password change script will be executed the next time the user successfully changes their password.

Distribution and Management

Overview

Most organizations that use Enterprise Connect will need to distribute and manage the application via a Mac management solution. Without a Mac management solution, Enterprise Connect and other applications may be difficult to manage, especially in a larger deployment. We strongly recommend using Enterprise Connect in tandem with a Mac management solution.

Distributing Enterprise Connect

Enterprise Connect can be distributed to Mac systems using any management solution that supports the distribution and installation of PKG files. Simply configure your management solution to distribute the supplied Enterprise Connect PKG file.

Managed Preferences

Organizations often need to pre-set basic settings for Enterprise Connect before deployment. There are two ways of pre-setting basic settings:

- Custom configuration profile payload (recommended): You can create a configuration profile that contains a Custom Settings payload. This payload can contain a list of

preference keys and values for Enterprise Connect. If these preference keys are managed with a configuration profile, corresponding fields in Enterprise Connect are disabled so that users cannot edit their contents. See the Appendix for instructions on creating a configuration profile using Profile Manager. You can easily modify these instructions to work with other popular Mac management solutions.

- Configuration via script: Upon installation, your management solution can run a script that calls defaults or PlistBuddy to pre-configure Enterprise Connect before the user launches it. See the Appendix for an example script.

Troubleshooting

Connection process

Enterprise Connect fails to connect

The most common cause for this event is a problem with the user's account or password. Should this occur, the Enterprise Connect main window will appear and the user will be told that their credentials are incorrect. The user can then re-enter her/his password and sign in.

Should this not resolve the issue, Enterprise Connect likely couldn't find a domain controller on the current network. Make sure a domain controller is available, then try again.

Enterprise Connect says "No work network found"

Enterprise Connect will report this status if it determines your organization's network is not available. You'll see the Enterprise Connect icon turn grey. This status is normal if your organization's network is not available.

You may also see this status if your network connection is intermittent. Should this happen, and you know that your network is available, click the Enterprise Connect icon in your menu bar, then select "Reconnect". Enterprise Connect will reattempt its connection process.

The Enterprise Connect menu bar icon pulses for a long time

If Enterprise Connect's menu bar icon is pulsing, it is performing its connection process. If the icon pulses for a long time, Enterprise Connect may be searching for a valid domain controller. Enterprise Connect will loop through a list of your organization's domain controllers until it finds one that is available. Once Enterprise Connect has failed to connect to 5 domain controllers, the connection process will abort. The connection process may take an excessive amount of time should many domain controllers not be available.

Kerberos/Single sign on

Single sign-on to resources like file servers or web sites fails

Make sure that the resource you are connecting to supports Kerberos authentication. Windows file servers generally support Kerberos authentication by default. Other resources, like web sites, generally require that an administrator enable Kerberos authentication support. NTLM support is not sufficient – Enterprise Connect requires Kerberos support to perform single sign-on.

If you're sure Kerberos support is enabled, make sure your client application has Kerberos support enabled. Safari will attempt Kerberos authentication without any additional configuration. Other

popular web browsers support Kerberos authentication with some additional configuration. See the browser's documentation for details.

Single sign-on to a DFS share fails

If your Mac is not bound to your Active Directory domain, connections to DFS shares will fall back to using NTLM authentication. You can still log into your Mac with a local account — the Mac itself must be bound to the domain.

Passwords

Enterprise Connect reports that my password doesn't expire

This issue may have several different causes:

- Your Active Directory domain does not expire passwords.
- Your account's password is set to never expire.
- A problem occurred querying a domain controller for password expiration policy. Enable debug logging, then restart Enterprise Connect for more details.

Enterprise Connect reports that my network isn't available when I change my password

You may see this error if Enterprise Connect loses its connection to your domain during a password change.

If your Mac is bound to Active Directory and you are logged into your Mac with an Active Directory account, you may also see this error if your Mac's binding to Active Directory is not working. Try unbinding and rebinding your Mac to AD, then try changing your password again.

Enterprise Connect reports that it cannot change my local password

If you see this error, there is likely a problem with your local password policy. Your local password policy shouldn't be more strict than your Active Directory password policy. Keep the following criteria in mind when creating a local password policy:

- Make sure to allow simple passwords. This means that a password can contain subsequent characters, like "123" or "ABC". By default, Active Directory does not have an equivalent restriction.
- Avoid using local password history. Password sync may fail if a user has set their Active Directory password to a password that has already been used locally on their Mac.
- Use caution with the "Number of complex characters" setting. There is no equivalent to this policy in Active Directory. In Active Directory, a password is considered to be complex if it meets several different criteria. A "number of complex characters" is not part of this criteria.

Advanced troubleshooting

Determining network accessibility and the periodic state check

By default, Enterprise Connect does a DNS lookup against the domain you've provided to determine if your organization's network is available. Once Enterprise Connect does the DNS lookup, it performs a DNS service record (SRV) lookup to verify that your network is online. If the SRV lookup returns a list of domain controllers, this is a good indicator that your organization's network is available.

Every 15 seconds, Enterprise Connect will perform a periodic state check (a DNS service record lookup) to determine if the availability of your network has changed. If availability of your network has changed, Enterprise Connect will take appropriate action. This feature is intended to improve Enterprise Connect's ability to detect changes in connection status with non-standard network configurations. Customers that expose their DNS publicly will need to disable this feature. See the "Using Configuration Profiles" section for details.

Preferences domain

Enterprise Connect uses the "com.apple.Enterprise-Connect" preferences domain. You'll need to refer to this when editing the application's preferences or creating custom configuration profiles. To delete all of Enterprise Connect's locally stored preferences, run:

```
defaults delete com.apple.Enterprise-Connect
```

Debugging mode

In the event of a problem with Enterprise Connect, you may need to use the application's debugging mode for troubleshooting purposes. To enable debug mode, run this command (with user level access):

```
defaults write com.apple.Enterprise-Connect debugMode -bool true
```

When Enterprise Connect restarts, it writes debugging information to the log database (macOS Sierra and up) and /var/log/system.log (prior to macOS Sierra). Look in the Console application for entries containing "ECDebug". These entries will usually tell you what the problem is.

Appendix

Creating the Audit script

Considerations

You have considerable flexibility when writing your Audit script, provided your script follows these rules:

- The script should run quickly and exit. If it does not, Enterprise Connect login will be delayed.
- If your script is successful, it should return a zero exit code. If your script is not successful, it should return a non-zero exit code.
- Your script will run as the logged in user. Your script shouldn't attempt to do anything that requires root access or access as another user.

Sample Audit script

```
#!/bin/sh

# Sample Enterprise Connect audit script
#
# This is a sample audit script for use with Enterprise Connect.
# The script performs a series of tests, then the script exits
# with a non-zero exit status and quits if any test fails.
# There's a lot of flexibility to script anything you want here based
# on your level of scripting ability.

ecUser=$1
ecDomain=$2

# Check if FileVault is on.
fdesetup status | grep 'FileVault is On'

if [ $? -ne 0 ]; then
        # Write a message to the system log and exit with a non-zero status.
        logger -t "ECAudit" "Audit script failed - FileVault is not enabled"
        exit 1
fi
```

```
# Check if the computer is enrolled in Casper.
jamf about


if [ $? -ne 0 ]; then
        # Write a message to the system log and exit with a non-zero status.
        logger -t "ECAudit" "Audit script failed - Casper isn't installed"
        exit 1
fi

# Check if the computer has an application installed.
# "-d" is a test for the existence of a directory, in this case
# an application bundle.
if [ ! -d "/Applications/Chess.app" ]; then
        # Write a message to the system log and exit with a non-zero status.
        logger -t "ECAudit" "Audit script failed - Casper isn't installed"
        exit 1
fi

# If we got here, the system passed the audit, so exit with a 0 (success)
# exit code
exit 0
```

Creating the Connection Completed script

Considerations

You have considerable flexibility when writing your Connection Completed script, provided your script follows these rules:

- The script should run quickly and exit. It it does not, Enterprise Connect will pause until the script is completed.
- Your script will run as the logged-in user. Your script shouldn't attempt to do anything that requires root access or access as another user.

Sample Connection Completed script

```
#!/bin/sh

# Sample Enterprise Connect connection completed script

ecUser=$1

ecDomain=$2

logger -t “EC Connection Completed” “User $ecUser from domain $ecDomain has successfully connected”

exit 0
```

Creating the Password Change script

Considerations

You have considerable flexibility when writing your Password Change script, provided your script follows these rules:

- The script should run quickly and exit. If it does not, the password change dialog will stay open until the script is completed.
- Your script will run as the logged-in user. Your script shouldn't attempt to do anything that requires root access or access as another user.

A sample password change script is available along with the download link for this documentation.

Using Configuration Profiles

Keys for configuration profiles

Enterprise Connect allows you to manage most of the preference keys and values it uses.

Warning: Do not add preferences keys not listed here to your configuration profile. This may cause Enterprise Connect to behave incorrectly.

Here are the keys you can manage and their permitted values:

Key	Type	Contents
adRealm	string	The host name of your organization's Active Directory domain. This is blank by default.
alwaysGetNewTicket	Boolean	If true, always get a new Kerberos ticket, even if the current ticket isn't expired. The default value is false.
checkForNetworkServer	string	Set this to the host Enterprise Connect should check for when connecting. This is blank by default. Only set if you set the above key to "true."
checkForNetworkType	boolean	Tells Enterprise Connect how to check for your organization's network. Set to "false" for default behavior, and set to "true" to check for a specific host. Should you do this, you must also set checkForNetworkServer.
checkShowLegacyCertifi-cates	Boolean	This value, if set, tells Enteprise Connect PKI to automatically check the "Show Legacy Certificates" option in the certificate chooser window. The default value is false.
connectDelay	integer	This value, if set, tells Enterprise Connect to delay starting its connection process when your organization's network is de-tected. This may be useful for customers who use Cisco NAC and need to delay connection while host checks are per-formed. Set connectDelay to the value in seconds that you need to delay connections for. The default value is 0.
connectionCompletedScript-Path	string	Path where Enterprise Connect looks for a Connection Com-pleted script.
connectReminderNagInterval	Integer	The interval, in seconds between connection reminders. The default is 86400 (24 hours).
connectReminderTime	integer	The interval, in seconds, at which Enterprise Connect should begin reminding the user to connect to the network.
dailyReconnectTime	integer	The interval, in seconds, that Enterprise Connect should at-tempt its daily reconnect. The default value is 86400 (24 hours). Set this to 0 to disable the daily reconnect.
debugMode	boolean	This key, if set to true, enables debugging mode. The default value is false.
destroyKerbTicketUponCar-dRemoval	boolean	If set to false, the user's Kerberos ticket will not be destroyed upon smart card removal. The default value is true.

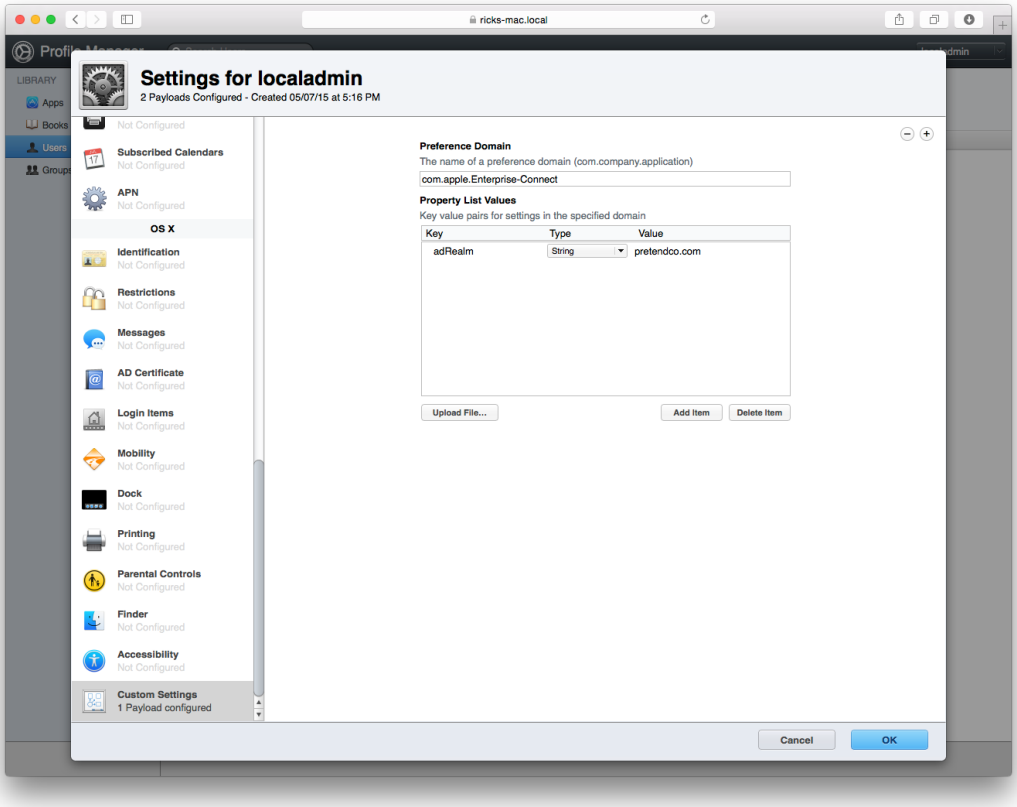
Key	Type	Contents
disablePasswordExpiration-Checking	boolean	Set this key to true to disable Enterprise Connect's password expiration checking, but still leave intact the ability for the user to change their password with Enterprise Connect.
disablePasswordFunctions	boolean	Set this key to true to disable Enterprise Connect's password management abilities, including expiration notices and the "Change Password" menu item. This is useful for customers who don't change their passwords in AD. The default value is false.
managedshares	other	This key contains a list of shares that Enterprise Connect should attempt to mount. Users will still be able to add their own shares. This key is an array which contains a dictionary for each share you wish to mount. See the sample configuration profile included with Enterprise Connect for an example. The default value is blank.
mountNetworkHomeDirectory	boolean	Determines if Enterprise Connect mounts the user's network home directory. This is "false" by default. Set to "true" to enable.
orgLogoPath	String	The path to a file containing your organization's logo, in PNG, JPG or GIF format.
orgUsernameLabel	String	The name your organization gives usernames.
passwordChangeScriptPath	string	Path where Enterprise Connect looks for password change script.
passwordChangeURL	string	If set, Enterprise Connect will open this URL in the user's default web browser when they use Enterprise Connect to change their password. Standard password change functionality will no longer work.
passwordExpireOverride	integer	Use this value to override domain password policy when calculating password expiration. The default value is blank.
passwordNotificationDays	integer	Determines the amount of days before password expiration that the user receives expiration notifications. The default value is 15. Set this to any positive value you wish.
preferredDC	string	Tells Enterprise Connect to prefer the specified domain controller when doing LDAP queries and getting a Kerberos TGT. If this domain controller is unavailable, Enterprise Connect will fall back to domain controllers it discovers from DNS.
prepopulatedUsername	string	Upon launch or sign out, Enterprise Connect will pre-populate the Username field with this username. The default value is empty.
pwReqComplexity	boolean	Tells Enterprise Connect that passwords should meet Active Directory's definition of complexity. Used to enable and configure live password testing. The default value is false.
pwReqComplexityDisableUnicode	boolean	If set to true, the "Has a Unicode character" password test is removed from live password testing. The default value is false.

Key	Type	Contents
pwReqHistoryCount	Integer	Tells Enterprise Connect how many previous passwords cannot be re-used. The default value is null
pwReqLength	Integer	Tells Enterprise Connect that passwords should be at least as long as the specified value. Used to enable and configure live password testing. The default value is null.
pwReqMinimumPasswordAge	Integer	Tells Enterprise Connect the minimum age of passwords before they can be changed. The default value is null.
pwReqText	string	Tells Enterprise Connect to display the specified RTF file for the user during password changes. Supply the path to the RTF file you want to display. The default value is null.
runAuditScript	boolean	Tells Enterprise Connect to execute an audit script.
runAuditScriptPath	string	Path where Enterprise Connect looks for an audit script.
runPasswordChangeScriptOnLocalPasswordSync	boolean	If set to false, Enterprise Connect will not run the password change script upon a local password sync. The default value is true.
runPeriodicStateCheck	boolean	This value, if set to false, tells Enterprise Connect to disable periodic state checking. Customers who expose their DNS to the public Internet will need to disable periodic state checking. The default value is true.
setupReminderNagInterval	Integer	The interval, in seconds, between setup notifications. The default value is 86400 (24 hours).
shareMountWaitSeconds	integer	This value, if set, tells Enterprise Connect to delay the mounting of network shares when your organization's network is detected. This may be useful for customers who use Cisco NAC and need to delay connection while host checks are performed. Set shareMountWaitSeconds to the value in seconds that you need to delay share mounting for. The default value is 0.
showKeychainIdentities	boolean	If enabled, identities in the user's default keychain will be available to choose in the certificate chooser window. The default value is false.
showMenuExtra	boolean	Determines whether the Enterprise Connect menu extra is loaded. The default value is true.
showUsernameWithSmartcard	Boolean	Determines if Enterprise Connect should display the username field if smart card mode is enabled. The default value is false.
smartCardMode	Boolean	Determines whether smart card mode should be enabled. The default value is false.
syncLocalPassword	boolean	Enables Active Directory to local account password sync. This only works if the user is logged into their Mac with a local account. Set to "true" to enable.

Creating a configuration profile

You can easily create a configuration profile for Enterprise Connect using Profile Manager, Jamf Pro, and other Mobile Device Management (MDM) tools. Here is the process of creating the configuration profile using Profile Manager:

1. Log in to your Profile Manager server.
2. Select a user, group, device, or device group that you want to apply the profile to. Click the Settings tab and then the Edit button. For most configurations, applying the profile at device level is sufficient.
3. Scroll to the bottom of the payloads list (left side of the window); choose Custom Settings.
4. Set the preference domain to "com.apple.Enterprise-Connect".
5. Click the "Add Item" button. We'll add an item for "adRealm".
6. Fill in the fields like you see in the screenshot below:



7. Repeat step 6 for items you'd like to manage. Make sure you set the "Type" field correctly.
8. Click OK to save the profile.

Using a Script to Configure Enterprise Connect

Considerations

We highly recommend using configuration profiles to configure Enterprise Connect. However, in certain instances, you may want to configure Enterprise Connect with a script instead of a configuration profile. These include:

- You want to preconfigure some application settings for the first time your user runs Enterprise Connect, then you want to let the user change those settings.
- You cannot deploy configuration profiles.

Keys for configuration via script

Here are the keys you can manage and permitted values:

Key	Type	Contents
adRealm	string	The host name of your organization's Active Directory domain. This is blank by default.
alwaysGetNewTicket	Boolean	If true, always get a new Kerberos ticket, even if the current ticket isn't expired. The default value is false.
checkForNetworkServer	string	Set this to the host Enterprise Connect should check for when connecting. This is blank by default. Only set if you set the above key to "true."
checkForNetworkType	boolean	Tells Enterprise Connect how to check for your organization's network. Set to "false" for default behavior, and set to "true" to check for a specific host. Should you do this, you must also set checkForNetworkServer.
checkShowLegacyCertifi-cates	Boolean	This value, if set, tells Enteprise Connect PKI to automatically check the "Show Legacy Certificates" option in the certificate chooser window. The default value is false.
connectDelay	integer	This value, if set, tells Enterprise Connect to delay starting its connection process when your organization's network is de-tected. This may be useful for customers who use Cisco NAC and need to delay connection while host checks are per-formed. Set connectDelay to the value in seconds that you need to delay connections for. The default value is 0.
connectionCompletedScript-Path	string	Path where Enterprise Connect looks for a Connection Com-pleted script.
connectReminderNagInterval	Integer	The interval, in seconds between connection reminders. The default is 86400 (24 hours).
connectReminderTime	integer	The interval, in seconds, at which Enterprise Connect should begin reminding the user to connect to the network.

Key	Type	Contents
dailyReconnectTime	integer	The interval, in seconds, that Enterprise Connect should attempt its daily reconnect. The default value is 86400 (24 hours). Set this to 0 to disable the daily reconnect.
debugMode	boolean	This key, if set to true, enables debugging mode. The default value is false.
destroyKerbTicketUponCardRemoval	boolean	If set to false, the user's Kerberos ticket will not be destroyed upon smart card removal. The default value is true.
disablePasswordExpirationChecking	boolean	Set this key to true to disable Enterprise Connect's password expiration checking, but still leave intact the ability for the user to change their password with Enterprise Connect.
disablePasswordFunctions	boolean	Set this key to true to disable Enterprise Connect's password management abilities, including expiration notices and the "Change Password" menu item. This is useful for customers who don't change their passwords in AD. The default value is false.
disableQuitMenu	boolean	Set this key to true to remove the Quit menu item from Enterprise Connect. The default value is false.
managedshares	other	This key contains a list of shares that Enterprise Connect should attempt to mount. Users will still be able to add their own shares. This key is an array which contains a dictionary for each share you wish to mount. See the sample configuration profile included with Enterprise Connect for an example. The default value is blank.
mountNetworkHomeDirectory	boolean	Determines if Enterprise Connect mounts the user's network home directory. This is "false" by default. Set to "true" to enable.
orgLogoPath	String	The path to a file containing your organization's logo, in PNG, JPG or GIF format.
orgUsernameLabel	String	The name your organization gives usernames.
passwordChangeScriptPath	string	Path where Enterprise Connect looks for password change script.
passwordChangeURL	string	If set, Enterprise Connect will open this URL in the user's default web browser when they use Enterprise Connect to change their password. Standard password change functionality will no longer work.
passwordExpireOverride	integer	Use this value to override domain password policy when calculating password expiration. The default value is blank.
passwordNotificationDays	integer	Determines the amount of days before password expiration that the user receives expiration notifications. The default value is 15. Set this to any positive value you wish.

Key	Type	Contents
preferredDC	string	Tells Enterprise Connect to prefer the specified domain controller when doing LDAP queries and getting a Kerberos TGT. If this domain controller is unavailable, Enterprise Connect will fall back to domain controllers it discovers from DNS.
prepopulatedUsername	string	Upon launch or sign out, Enterprise Connect will pre-populate the Username field with this username. The default value is empty.
pwReqComplexity	boolean	Tells Enterprise Connect that passwords should meet Active Directory's definition of complexity. Used to enable and configure live password testing. The default value is false.
pwReqComplexityDisableUnicode	boolean	If set to true, the "Has a Unicode character" password test is removed from live password testing. The default value is false.
pwReqHistoryCount	Integer	Tells Enterprise Connect how many previous passwords cannot be re-used. The default value is null
pwReqLength	Integer	Tells Enterprise Connect that passwords should be at least as long as the specified value. Used to enable and configure live password testing. The default value is null.
pwReqMinimumPasswordAge	Integer	Tells Enterprise Connect the minimum age of passwords before they can be changed. The default value is null.
pwReqText	string	Tells Enterprise Connect to display the specified RTF file for the user during password changes. Supply the path to the RTF file you want to display. The default value is null.
runAuditScript	boolean	Tells Enterprise Connect to execute an audit script.
runAuditScriptPath	string	Path where Enterprise Connect looks for an audit script.
runPasswordChangeScriptOnLocalPasswordSync	boolean	If set to false, Enterprise Connect will not run the password change script upon a local password sync. The default value is true.
runPeriodicStateCheck	boolean	This value, if set to false, tells Enterprise Connect to disable periodic state checking. Customers who expose their DNS to the public Internet will need to disable periodic state checking. The default value is true.
setupReminderNagInterval	Integer	The interval, in seconds, between setup notifications. The default value is 86400 (24 hours).
shareMountWaitSeconds	integer	This value, if set, tells Enterprise Connect to delay the mounting of network shares when your organization's network is detected. This may be useful for customers who use Cisco NAC and need to delay connection while host checks are performed. Set shareMountWaitSeconds to the value in seconds that you need to delay share mounting for. The default value is 0.

Key	Type	Contents
shares	other	This key contains a list of shares that Enterprise Connect should attempt to mount. This key is an array which contains a dictionary for each share you wish to mount. The default value is blank.
showKeychainIdentities	boolean	If enabled, identities in the user's default keychain will be available to choose in the certificate chooser window. The default value is false.
showMenuExtra	boolean	Determines whether the Enterprise Connect menu extra is loaded. The default value is true.
showUsernameWithSmartcard	Boolean	Determines if Enterprise Connect should display the username field if smart card mode is enabled. The default value is false.
smartCardMode	Boolean	Determines whether smart card mode should be enabled. The default value is false.
syncLocalPassword	boolean	Enables Active Directory to local account password sync. This only works if the user is logged into their Mac with a local account. Set to "true" to enable.

Preferences keys for administrators

Summary

Enterprise Connect writes information to its preferences file (plist) that may be useful to an administrator. Administrators can read these values from the Enterprise Connect plist and use them in their own scripts or store their values in a Mac management solution for inventory purposes.

Preferences keys

Here are some useful preference keys:

Key	Type	Contents
configurationNamingContext	string	The distinguished name of your domain's configuration container. This value may be useful from scripts that perform LDAP queries.
dateLastConnected	date	This key contains the date that Enterprise Connect was last able to successfully connect. This value may be useful for inventory purposes.
datePasswordExpires	date	This key contains the date that the user's password expires.
daysToExpire	integer	The amount of days until the user's password expires.
defaultNamingContext	integer	The distinguished name of your domain's default container. This value may be useful from scripts that perform LDAP queries.
kerbCacheName	string	The name of the Kerberos credentials cache being managed by Enterprise Connect. This value may be useful in certain scripting situations.
lastSiteName	string	The Active Directory site this system was in the last time that Enterprise Connect connected. This value may be useful for scripts that need to be location aware and for inventory purposes.
localADPasswordsInSync	boolean	This key, if set to true, indicates that the user's local and Active Directory passwords are in sync. This value is useful for inventory purposes.
rootDomainNamingContext	boolean	The distinguished name of your forest's default container. This value may be useful from scripts that perform LDAP queries.

Sample configuration script

This sample script is configured to run as a login policy for Jamf Pro. It configures a preferences plist for Enterprise Connect, then launches Enterprise Connect as the user in question. You could also slightly modify this script to be triggered by launchd the first time a user logs into the Mac.

```
#!/bin/bash


userName=$(stat -f %Su /dev/console)

adRealm=pretendco.com

passwordReminder=30


# Add pretendco.com domain

sudo -u $userName -H defaults write ~/Library/Preferences/com.apple.Enterprise-Connect adRealm
-string "$adRealm"


# Notify the user 30 days before password expiration

sudo -u $userName -H defaults write ~/Library/Preferences/com.apple.Enterprise-Connect
passwordNotificationDays -int "$passwordReminder"


# Populate Enterprise Connect share

sudo -u $userName -H /usr/libexec/PlistBuddy -c "add :shares array" ~/Library/Preferences/
com.apple.Enterprise-Connect.plist

sudo -u $userName -H /usr/libexec/PlistBuddy -c "add :shares:dict:path string smb://
server.pretendco.com/Users/$userName" /Users/$userName/Library/Preferences/com.apple.Enterprise-
Connect.plist


# Open Enterprise Connect so the user can enter credentials

sudo -u $userName -H open "/Applications/Enterprise Connect.app"
```

Uninstalling Enterprise Connect

To completely uninstall Enterprise Connect from your Mac:

1. In Terminal, run "launchctl unload /Library/LaunchAgents/com.apple.ecAgent.plist".
2. Still in Terminal, run "killall Enterprise\ Connect\ Menu".
3. Quit Enterprise Connect, then delete the Enterprise Connect application from the Applications folder.
4. Delete ecAgent's launchd plist at /Library/LaunchAgents/com.apple.ecAgent.plist.
5. Open the Keychain Access application. Select your login keychain, find the Enterprise Connect keychain item, then delete it.

If you are using Enterprise Connect 1.6 or greater, the uninstallation process is complete. If you are using an older version of Enterprise Connect, open Terminal and run the following commands:

```
sudo launchctl unload /Library/LaunchDaemons/com.apple.Enterprise-Connect.kerbHelper.plist

sudo rm /Library/LaunchDaemons/com.apple.Enterprise-Connect.kerbHelper.plist

sudo rm /Library/PrivilegedHelperTools/com.apple.Enterprise-Connect.kerbHelper

sudo security authorizationdb remove com.apple.Enterprise-Connect.writeKDCs
```

The above steps remove the helper tool that older versions of Enterprise Connect use to update the Mac's Kerberos configuration. If you are running version 1.6 or greater, these steps are not needed – the installer performs them automatically.

Uninstalling Enterprise Connect PKI

Here is a simple script that removes Enterprise Connect PKI. Run this as root:

```
#!/bin/sh

killall Enterprise\ Connect\ PKI

rm -rf /Applications/Enterprise\ Connect\ PKI
```

For most users, this should be enough. If you want to be more thorough, have the user sign out of Enterprise Connect PKI before uninstall. Doing so will remove the Enterprise Connect PKI login item and the Enterprise Connect PKI keychain entry.