Jamf Pro Overview

macOS Smart card Functionality

Jamf Pro Overview 1
Overview 6
History 7
Mac OS X 10.6 and below 7
Mac OS X 10.7 - 10.12 7
Mac OS X Sierra 10.12 - macOS High Sierra 10.13 7
Mac OS X Sierra 10.12.0-10.12.4 7
Mac OS X Sierra 10.12.4 - macOS High Sierra 10.13.1 7
macOS High Sierra 10.13.2 8
macOS High Sierra 10.13.4 8
macOS Mojave 10.14.0 - 10.14.6 8
macOS Mojave 10.14.6 8
macOS Catalina 10.15.0 9
Pre-10.12 Support 10
Additional USB Drivers 10
FileVault 11
Basic Setup 11
Advanced Setup 11
Active Directory 12
Native Support for AD bound Macs 12
Local User Account - Attribute Mapping 12
Mobile User Account - Attribute Mapping 12
Advanced Integration 13
Configuration Profile 14
Note 15
Jamf Pro 10.3 15
Enforce Smart card 16
Verify Smart card Certificate 16
Jamf Pro 10.12 16
Mandatory use of Smart cards 17
1. Device Enrollment 17

2. Enforce FileVault 17
3. Set up a FileVault User 17
4. Smart card Pairing 17
Non-Directory Services 17
Active Directory 17
5. Configuration Profile 18
6. Terminal Commands 18
Alternative Distribution 19
Scripts 20
Enforce ‘sudo’ to use Smart card 20
Enforce ‘su’ to use Smart card 20
Enforce ‘login’ to use Smart card 20
Enforce Screensaver to activate on removal of Smart card 20
Active Directory Attribute Mapping 21
Extension Attributes 22
Validate Smart card Pairing is enabled 22
Review if a Smart card is in User’s Keychain 22
Display Smart card enabled user 22
Smart card Logging 22
Review Screensaver Setting for Smart card Removal 22
Review if ‘login’ command has been protected with Smart card Authentication 23
Review if ‘sudo’ command has been protected with Smart card Authentication 23
Review if ‘su’ command has been protected with Smart card Authentication 23
Troubleshooting 24
Validate Smart card Pairing is enabled 24
Review if a Smart card is in User’s Keychain 24
Smart card Logging 24
Review the hash for Smart card enabled user 24
Smart card Manual 24
Smart card Diagnostic 24
System-wide Diagnostic Report 25
PAM Module 25

Review current Login Window Settings 25
Smart card Information from System Profiler 25
Review the list of Smart cards 25
References 26
Apple Documentation 26
TokenD 26
CryptoTokenKit 26
MDM Reference 26
PIV Mandatory 26

Jamf has made all efforts to ensure that this guide is accurate.

Jamf
100 Washington Ave S
Suite 1100
Minneapolis, MN 55401-2155
(612) 605-6625

Overview

With user-friendly and easy to use products, along with an ever-expanding ecosystem of apps and resources, it's no surprise that Apple continues to make substantial strides in enterprise settings around the world. Apple devices all come with built-in security features that make them a logical choice for any security-conscious organization. However, government and financial sectors often need more than what Apple offers out of the box.

To accommodate these organizations, Smart cards can be leveraged as an extra layer of security authentication on Mac.

In this white paper, we explain the history of Smart card usage with Apple and provide guidance to Jamf customers on the best methods for managing and reporting on Smart cards, like Personal Identity Verification (PIV) or Common Access Card - Next Gen (CAC-NG*), for Apple devices.

You'll learn how to:

- Deploy tools like Centrify and ADmitMac PKI that contain drivers for reading Smart cards on older macOS devices
- Leverage macOS built in CryptoTokenKit
- Create local user accounts to support Smart cards
- Support Active Directory binding natively or through additional tools
- Create configuration profiles to centrally manage and enforce Smart card services
- Leverage extension attributes to report on various Mac settings, including Smart cards
- Troubleshoot steps if an issue should arise

* CAC-NG card specification requires the card include a PIV credential

This document will focus most attention on macOS High Sierra 10.13 and the Jamf Pro management solution. You should have advanced knowledge of how to use Jamf Pro in secure environments.

History

Smart card support within macOS has changed over the years. Here is a record of what type of support Apple has built into each version of macOS.

(Note: Most data related to this section was obtained on Cem Pava's blog. [See References])

Mac OS X 10.6 and below

Mac OS X systems used to contain a low level module service called 'tokend'. This service allowed native reading of certain Smart cards (1):

1. BELPIC.Tokend: Belgian National ID (BELPIC) compliant Smart cards
2. CAC.Tokend: Common Access Card (CAC) compliant Smart cards
3. JPKI.Tokend: japanese PKI (JPKI) compliant Smart cards
4. PIV.Tokend: Personal Identity Verification (PIV) compliant Smart cards
5. tokendPKCS11.so: PKCS-11 shim over TokenD (Mac OS X 10.6 only)

Mac OS X 10.7 - 10.12

Smart card services with TokenD were removed from Mac OS X and moved into an open source platform.

This is placed within Apple's macOS forge site: https://www.macosforge.org
Smart card Services specifically at: https://smartcardservices.github.io

Customers could utilize third-party applications and drivers to support Smart cards. Centrify and ADmitMac are two primary solutions that offer support.

Mac OS X Sierra 10.12 - macOS High Sierra 10.13

Apple transitioned to native support of Smart cards using CryptoTokenKit (CTK) with new management functionalities through mobile device management (MDM). More information can be found in Terminal with the 'man SmartCardServices' command.

Legacy Smart card services using TokenD (CDSA) are still supported in Sierra and High Sierra using the GitHub project: https://smartcardservices.github.io

Mac OS X Sierra 10.12.0-10.12.4

Apple built-in CTK supported Smart cards natively with command-line interface management. This can be reviewed by using "man SmartCardServices" and "man sc_auth" in Terminal.

Mac OS X Sierra 10.12.4 - macOS High Sierra 10.13.1

Apple began adding MDM Configuration Profile settings to centrally manage some components of the Smart card functionality. These included:

1. Allow Smart card
2. Only allow one Smart card per user
3. Allow user pairing
4. Verify the certificate is trusted - boolean on or off

macOS High Sierra 10.13.2

A mandatory enforcement of Smart card usage was introduced to meet the US Government requirements, known as PIV-M or mandatory use of PIV credentials. This is a response to Homeland Security Presidential Directive - 12. [See References]

This setting enforces Smart card on macOS functions. Terminal related functions (i.e. ‘sudo’, ‘login’, ‘su’, etc.) can be set up with Smart card mandatory authentication using settings from Page 15.

This does not allow a per-user management of Smart cards.

The following MDM configuration profile setting was introduced to support PIV-M.

1. Force Smart card authentication on all users

Apple changed the MDM Configuration Profile key that controls the certificate trust check behavior, adding two additional options for check revocation (soft) and check revocation (hard). Soft requires the device to check revocation upon network connectivity to OCSP/CRL, whereas Hard validates revocation immediately against OCSP/CRL.

1. Check Certificate Trust (with soft revocation check)
2. Check Certificate Trust (with hard revocation check)

macOS High Sierra 10.13.4

Apple added new management functionality to allow the local administrator to change the Smart card PIN using ‘sc_auth’.

macOS Mojave 10.14.0 - 10.14.6

Apple added new management functionality for configuration profiles to enforce the “Lock screensaver on Smart card removal”

macOS Mojave 10.14.6

Take a hash of the domain of your certificate, allowing you to identify only certain domains can pair and authenticate.

PCSC bug fixes

macOS Catalina 10.15.0

Apple added updates to the “man SmartCardServices” in referencing various Smart card functionality to CTK. These include:

Identity Picker - Ability to choose which identity needs to be used for authentication.

User based Enforcement - No longer tied to device based enforcement. Allow login for unpair user. Ability to relax mandatory Smart card policy for an identified group of users. Allowed to make a local user group or directory based group that is allowed to bypass the Smart card mandatory (PIV-M) policy.

Certificate pinning - Ability to restrict Smart card login to cards issued from specific domains TokenD is now dead.

Pre-10.12 Support

Jamf Pro can assist any customer in deploying tools like Centrify and ADmitMac PKI that contain drivers for reading Smart cards in systems prior to Mac OS X 10.12.

Additional USB Drivers

Apple has built in support for a very wide range of PIV and CAC-NG Smart cards, therefore, the need to build any additional drivers would be rare. If you have a need to build an additional Smart card driver please review Apple's man page for Smart card Services:

OS X (macOS) has built-in support for USB CCID class-compliant Smart card readers. For other readers, install the reader driver in /usr/local/libexec/SmartcardServices/drivers. Each driver is a bundle. The bundle contains an XML file Info.plist which contains the device's USB vendor ID and product ID. For detailed description of the plist format and how to write a reader driver, see http://pcsclite.alioth.debian.org/api/group__IFDHandler.html

Utilize Jamf Pro to push out any new XML data for understanding other Smart card USB readers.

Contact your Apple Systems Engineer to obtain more information on creating new drivers.

FileVault

At this time, FileVault does not offer Smart card support. Therefore, one local user account must be created on the Mac that will be utilized for FileVault pre-boot authentication. This account can be restricted from logging into the Mac.

Basic Setup

This method will allow your environment to utilize a Local User password for FileVault while forcing the use of a Smart card at Login Window. The following command disallows the passthrough of the password from pre-boot authentication to the Login Window.

```
defaults write /Library/Preferences/com.apple.loginwindow
DisableFDEAutoLogin -bool YES
```

Advanced Setup

Many government and regulated commercial customers utilize the following method to set up a local user account from Jamf Pro on the Mac that does not have access to login at the Login Window. This will enforce that all users who attempt to log into the Mac be forced to use their Smart card for authentication at the Login Window. The FileVault enabled user will not have any capabilities outside of FileVault authentication screen.

1. Set up FileVault using Jamf Pro to escrow the individual recovery key
2. Set up a local user account that is FileVault enabled
3. Use the following command to disallow that user from logging into the system, only to be used to unlock FileVault:

```
dscl . -append /Users/username AuthenticationAuthority
";DisabledUser;"
```

4. Use the following command to disallow any local admin account that has Smart card paired to be used to unlock FileVault:

```
fdesetup remove -user username
```

5. Remove the shadow hash from the user's account in dscl, if necessary

Active Directory

Jamf can assist customers in supporting Active Directory binding natively and through additional tools. Jamf has found in multiple environments that the use of native Active Directory binding within macOS does not function well. However, it is recommended that Jamf customers review these solutions.

Native Support for AD bound Macs

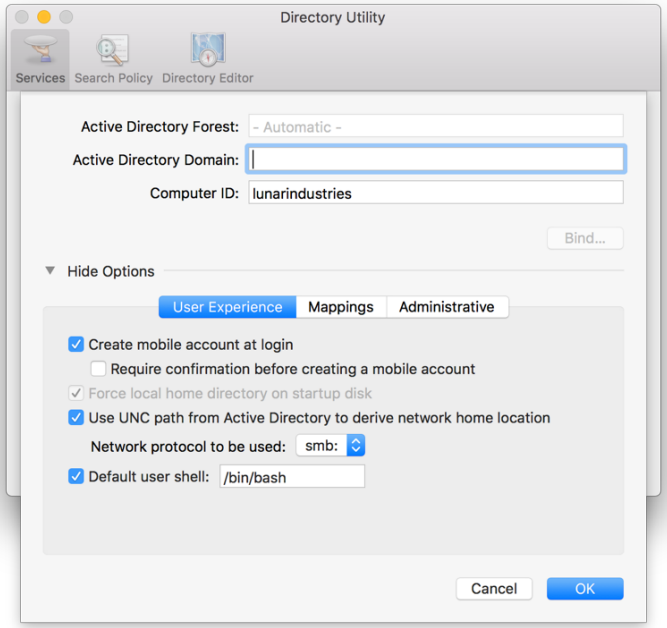
For organizations that currently support Smart cards within existing AD infrastructure, Apple supports native Smart card pairing for local and mobile user accounts.

Local User Account - Attribute Mapping

1. After the Mac is bound, deploy the following .plist to the Mac using Jamf Pro.
2. Deploy the Local-SmartcardLogin.plist to the Mac allowing any user with valid Smart card to authenticate at the Login Window.

Mobile User Account - Attribute Mapping

1. After the Mac is bound, verify inside Directory Utility -> Active Directory -> Show Options -> User Experience -> “Require confirmation before creating a mobile account” is disabled/unchecked.



2. Deploy the Mobile-SmartcardLogin.plist to the Mac, allowing any user with a valid Smart card to build a Mobile User Account.

https://github.com/hardstriker/SmartCard-Scripts/tree/master/Attribute%20Mapping

Please contact your Apple Systems Engineer or AppleCare Enterprise Support for more information about AD Attribute Mapping for Smart card services.

Advanced Integration

If you require more advanced user capabilities than offered by the existing Smart card support, please review the following external solutions:

1. Apple Professional Services - AD Integration Services

AD Integration Services provides Mac users with a secure connection to an Active Directory (AD) domain and resources with Enterprise Connect.

Enterprise Connect PKI provides support for native Smart cards in macOS.

For more information, please contact either your Apple Systems Engineer or Jamf Systems Engineer.

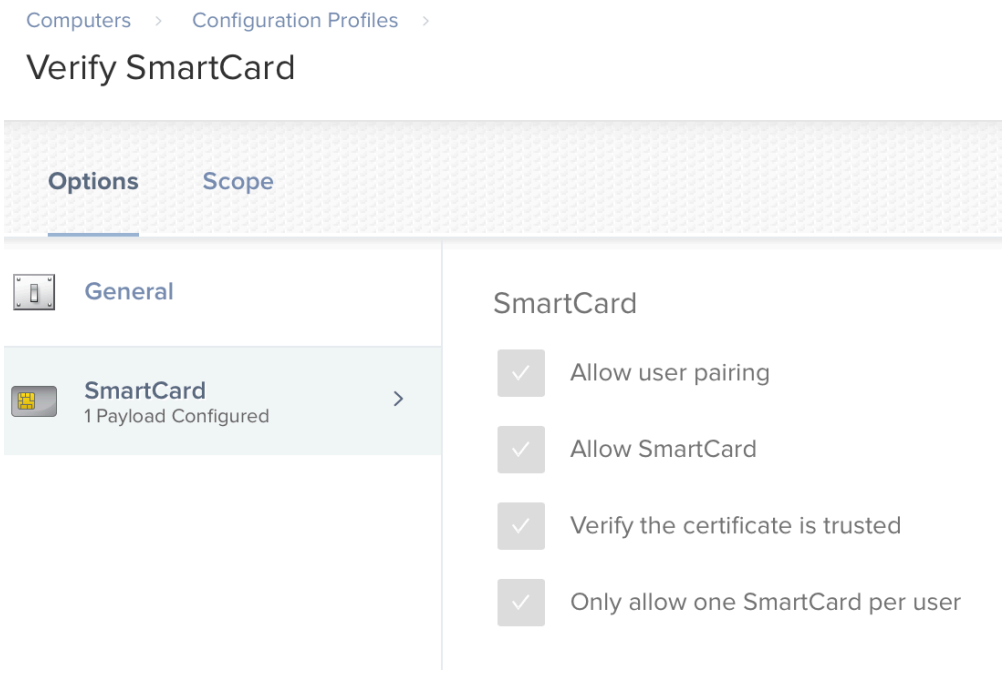
Apple Link: http://business-static.apple.com/us/apple-professional-services/Apple_Professional_Services_AD_Integration_Services.pdf

Configuration Profile

Jamf Pro 9.100.0 and later includes the following MDM configuration profile payload keys for centrally managing Smart card services in Mac OS X Sierra 10.12.4 and above:

1. Allow Smart card
2. Only allow one Smart card per user
3. Allow user pairing
4. Verify the certificate is trusted

These keys can be configured within Computers -> Configuration Profiles -> SmartCard payload, as seen here:



These key pairs reflect Apple's documentation shown here:

Key	Type	Value
`UserPairing`	Boolean	Optional. If `false`, users will not get the pairing dialog, although existing pairings will still work. Default is `true`.
`allowSmartCard`	Boolean	Optional. If `false`, the SmartCard is disabled for logins, authorizations, and screensaver unlocking. It is still allowed for other functions, such as signing emails and web access. A restart is required for a change of setting to take effect. Default is `true`.
`checkCertificateTrust`	Boolean	Optional. If `true`, certificates on the card must be valid in these ways: its issuer is system-trusted, the certificate is not expired, its "valid-after" date is in the past, and it passes CRL and OCSP checking. User overrides are not allowed. Usually this key is set to `true` for SmartCard use in corporate environments. Default is `false`.
`oneCardPerUser`	Boolean	Optional. If `true`, a user can pair with only one SmartCard, although existing pairings will be allowed if already set up. Default is `false`.

Source: Apple Configuration Profile Reference Guide

Note

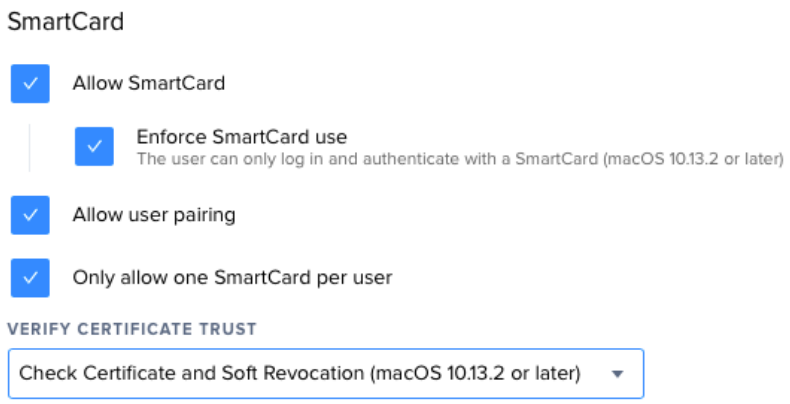
Prior to Jamf Pro 10.2, Jamf did not support the changes in macOS High Sierra 10.13.2. This includes the following keys:

`enforceSmartCard`	Boolean	Optional. If `true`, a user can only login or authenticate with a SmartCard. Default is `false`.

Jamf Pro 10.3

Jamf Pro 10.3 added support for the changes in macOS High Sierra 10.13.2.

This version enabled enforcement of Smart card and new Smart card Certificate validation options by creating a new configuration profile with Smart card payload, as shown below:



Reflecting the following key pairs from Apple:

Key	Type	Value
`UserPairing`	Boolean	Optional. If `false`, users will not get the pairing dialog, although existing pairings will still work. Default is `true`.
`allowSmartCard`	Boolean	Optional. If `false`, the SmartCard is disabled for logins, authorizations, and screensaver unlocking. It is still allowed for other functions, such as signing emails and web access. A restart is required for a change of setting to take effect. Default is `true`.
`checkCertificateTrust`	Integer	Optional. Valid values are 0–3: ▪ 0: certificate trust check is turned off ▪ 1: certificate trust check is turned on. Standard validity check is being performed but this does not include additional revocation checks. ▪ 2: certificate trust check is turned on, plus a soft revocation check is performed. Until the certificate is explicitly rejected by CRL/OCSP, it is considered as valid. This implies that unavailable/unreachable CRL/OCSP allows this check to succeed. ▪ 3: certificate trust check is turned on, plus a hard revocation check is performed. Unless CRL/OCSP explicitly says "this certificate is OK", the certificate is considered as invalid. The is the most secure option. Default is `0`.
`oneCardPerUser`	Boolean	Optional. If `true`, a user can pair with only one SmartCard, although existing pairings will be allowed if already set up. Default is `false`.
`enforceSmartCard`	Boolean	Optional. If `true`, a user can only login or authenticate with a SmartCard. Default is `false`.

Enforce Smart card

** NOTE **

When enabling “Enforce SmartCard use” within the configuration profile, it will enforce the use of Smart card for authentication of all users on the Mac. Therefore, any user that has not paired a Smart card at the time of deployment will be locked out of the system.

If you disable “Allow SmartCard” it will automatically disable the “Enforce SmartCard use” setting.

Verify Smart card Certificate

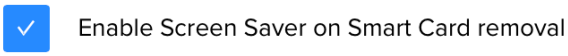
Apple’s macOS High Sierra 10.13.2 has four options for checking if the Smart card certificates are valid. The configuration profile that Jamf Pro 10.3 can push has four options:

0 - Certificate trust check is turned off
1 - Certificate trust check is turned on
2 - Certificate trust check is turned on and revocation check is set to the soft level (unreachable OCSP/CRL means success)
3 - Certificate trust check is turned on and revocation check is set to the hard level (verified positive response is needed to succeed)

(As reviewed within Apple’s man page for SmartCardServices)

Jamf Pro 10.12

Jamf introduced the profile key to manage the enforcement of Screensaver activation upon Smart card removal. This was introduced in macOS 10.13.4.



Mandatory use of Smart cards

Enforcement Setup

When considering the enforcement of Smart cards on Macs managed by Jamf Pro, it is suggested to follow this order of operation to ensure users don't get locked out of the Mac.

1. Device Enrollment

Identify the method of device enrollment, either Apple's Device Enrollment Program (DEP), Jamf imaging, or user-initiated enrollment. Jamf Pro supports multiple methods of enrollment that can be reviewed here.

Each Mac needs to be enrolled into Jamf Pro first.

2. Enforce FileVault

Use Jamf Pro to enforce FileVault encryption, allowing the organization to escrow the FileVault recovery keys. Jamf recommends deploying the configuration profile for key escrow while using a Jamf policy to enforce FileVault encryption.

** NOTE: Possibly bind the Mac to AD, if needed, with attribute mapping from Page 9.

3. Set up a FileVault User

As mentioned above, FileVault pre-boot authentication is currently not capable of Smart card authentication. It is recommended that each Mac use a local user account that is both enabled for FileVault's pre-boot authentication and is disabled from logging into the Mac (via Login Window).

Read Page 10 for more information about enabling these settings.

4. Smart card Pairing

Non-Directory Services

The primary user of the Mac should pair a Smart card to their account. This will allow for Smart card enforcement (PIV-M) settings to be deployed without rendering all user accounts unusable.

Active Directory

Any user that has a valid Smart card may insert it in to the Mac as long as the SmartcardLogin.plist file has been correctly deployed. (See Page 10)

5. Configuration Profile

Jamf Pro can deploy all of the Smart card settings onto the device using the Smart card payload of configuration profiles. This can include ‘Enforce Smart card’ given that at least one user account has a paired Smart card.

6. Terminal Commands

Jamf Pro can push out scripts and extension attributes that determine that the following terminal commands have Smart card enforcement: ‘login’, ‘ssh’, ‘su’, and ‘sudo’.

Alternative Distribution

Jamf has multiple recommendations for distribution of Smart card enforcement and settings. We will outline some methods for distribution here. Additional assistance can be provided by Jamf Professional Services.

Jamf Recommendation for Distribution

1. Create a new script in Jamf Pro
2. Present script to users in Jamf Self Service
3. Allow the user to take the motions of pairing their Smart card with High Sierra
4. Scope a logout script that validates that the user has a Smart card paired
5. Once Jamf Pro has acknowledged a Smart card has been paired with at least one user, the configuration profile is scoped to that Smart Computer Group

Troubleshooting Steps:

Possible distribution workflow

1. Create a new Jamf Pro policy that informs the user of the upcoming enforcement of Smart cards
2. Offer the option for the user to open Self Service to opt-out, as they might not have a Smart card assigned
3. Separate Jamf Pro policy with an API script to add that computer to exception list of the Smart card configuration profile
4. Gives the Jamf Pro admins a full list of computers that are asking for exceptions to the Smart card enforcement

User was found to not have a paired Smart card

1. Find the configuration profile with the “Enforce SmartCard use” payload
2. Select Scope
3. Select Exception
4. Add the computer to the exception list
5. Select the “Distribute to All” option

Scripts

Jamf Pro allows all Mac administrators the ability to send and enforce local shell or bash scripts to be run on the Mac on a certain frequency with root access. Listed below are a few scripts needed to help enforce Smart card usage on the Mac.

All of the following scripts can be found at:
https://github.com/jamfprofessionalservices/SmartCard-Scripts

The following scripts for enabling Smart card authentication for certain Terminal commands change the native PAM modules of macOS.

Enforce ‘sudo’ to use Smart card

Mac OS X Sierra 10.12.6 and above, enforcement of Smart card on ‘sudo’ is enabled by default.

For earlier versions of Mac OS X, use Jamf Pro to send out the following package to any computer that reports in authorization with a Smart card on ‘sudo' command.

https://github.com/jamfprofessionalservices/SmartCard-Scripts/tree/master/SmartCard%20enabled%20sudo

Enforce ‘su’ to use Smart card

Use Jamf Pro to send out the following package to any computer that reports in authorization with a Smart card on ‘su' command.

https://github.com/jamfprofessionalservices/SmartCard-Scripts/tree/master/SmartCard%20enabled%20su

Enforce ‘login’ to use Smart card

Use Jamf Pro to send out the following package to any computer that reports in authorization with a Smart card on ‘login' command.

https://github.com/jamfprofessionalservices/SmartCard-Scripts/tree/master/SmartCard%20enabled%20login

Enforce Screensaver to activate on removal of Smart card

Use Jamf Pro to send out the following script to any computer that reports in that screensaver will not activate upon Smart card removal.

https://github.com/jamfprofessionalservices/SmartCard-Scripts/blob/master/setScreensaverOnSCRemoval.sh

Active Directory Attribute Mapping

Sierra 10.12 and High Sierra 10.13 have built-in capabilities to allow Smart card to be used without any local user account creation. Jamf Pro can push out the following .plist to Macs to enable this function.

https://github.com/jamfprofessionalservices/SmartCard-Scripts/tree/master/Attribute%20Mapping

Extension Attributes

Jamf Pro gives all customers the ability to report on various aspects of the Mac, including many attributes of the Smart card settings enabled and used on a Mac. The following attributes will be constantly reviewed and reported into Jamf Pro on a consistent basis. Please review all the following extension attributes:

Validate Smart card Pairing is enabled

Reviews if the Smart card Pairing User Interface is enabled on the logged in user of the Mac.

https://www.jamf.com/jamf-nation/third-party-products/files/967/smartcard-gui-enabled

Review if a Smart card is in User's Keychain

Displays if any Smart card data exists within the logged in user's keychain.

https://www.jamf.com/jamf-nation/third-party-products/files/968/smartcard-user-s-keychain

Display Smart card enabled user

Displays which local user account has been Smart card enabled and with what type of Smart card.

https://www.jamf.com/jamf-nation/third-party-products/files/905/review-smartcard-enabled-users

Smart card Logging

Reviews if Smart card logging has been enabled on this Mac. Should only be enabled during debugging, gets disabled after shutdown, restart or Smart card reader gets disconnected.

https://www.jamf.com/jamf-nation/third-party-products/files/966/smartcard-logging

Review Screensaver Setting for Smart card Removal

Validates that if the Smart card is removed from the sled (USB card reader), that Screensaver is activated immediately.

https://www.jamf.com/jamf-nation/third-party-products/files/969/smartcard-screensaver-lock

Review if ‘login’ command has been protected with Smart card Authentication

Validates that the login command within pam.d has been forced to use Smart card authentication.

https://www.jamf.com/jamf-nation/third-party-products/files/970/smartcard-login-command

Review if ‘sudo’ command has been protected with Smart card Authentication

Validates that the sudo command within pam.d has been forced to use Smart card authentication.

https://www.jamf.com/jamf-nation/third-party-products/files/972/smartcard-sudo-command

Review if ‘su’ command has been protected with Smart card Authentication

Validates that the su command within pam.d has been forced to use Smart card authentication.

https://www.jamf.com/jamf-nation/third-party-products/files/971/smartcard-su-command

Troubleshooting

Below are various aspects of troubleshooting the use of Smart cards on macOS.

Validate Smart card Pairing is enabled

```
sc_auth pairing_ui -s status
```

Reviews if the Smart card Pairing User Interface is enabled on the logged in user of the Mac.

Review if a Smart card is in User's Keychain

```
system_profiler SPSmartcardsDataType | grep "Available Smartcards
(keychain)"
```

Displays if any Smart card data exists within the logged in user's keychain.

Smart card Logging

```
sudo defaults read /Library/Preferences/com.apple.security.smartcard
Logging
```

Reviews if Smart card logging has been enabled on this Mac.

Enabled Smart card logging using the following command:

```
sudo defaults write /Library/Preferences/com.apple.security.smartcard
Logging -bool YES
```

Disconnecting the Smart card reader will disable logging.

Review the hash for Smart card enabled user

```
sc_auth list username
```

Prints out the shadow hash of the user with a paired Smart card.

Smart card Manual

```
man SmartCardServices
```

Prints out the manual for Smart card services for CryptoTokenKit.

Smart card Diagnostic

```
pcsctest
```

Reads the currently connected Smart card state, protocol, ATR size and value, and other settings.

System-wide Diagnostic Report

```
sysdiagnose
```

Compiles a system-wide diagnostic report helpful in investigating issues with Smart cards.

PAM Module

```
man pam_smartcard
```

Read more about the Smart card PAM module.

Review current Login Window Settings

```
defaults read /etc/SmartcardLogin.plist
```

Read the Login Window settings of macOS.

Smart card Information from System Profiler

```
system_profiler SPSmartCardsDataType
```

Displays useful information as seen with System Profiler about Smart cards with CryptoTokenKit and TokenD.

Review the list of Smart cards

```
security list-smartcards
```

Displays the list of Smart card information available

References

1. The history of Smart card services in macOS by Cem Paya through 2015 -
   SmartCard Logon for OS X (Part I)
   SmartCard Logon for OS X (Part II)
   SmartCard Logon for OS X (Part III)

2. Richard Purves - Great documentation on multiple aspects of using Smart cards and scripts.
Blog: http://www.richard-purves.com
GitHub: https://github.com/franton

Apple Documentation

macOS Help - Smart cards
https://help.apple.com/deployment/macos/#/apd731e6a3c4

macOS Deployment Guide
https://help.apple.com/deployment/macos/

TokenD

TokenD Support - https://smartcardservices.github.io/components/tokend/

CryptoTokenKit

CryptoTokenKit
https://developer.apple.com/documentation/cryptotokenkit/authenticating_users_with_a_cryptographic_token

Add Support for new types of tokens for CTK
https://developer.apple.com/library/content/samplecode/PIVToken/Introduction/Intro.html

MDM Reference

Configuration Profile Reference Guide
https://developer.apple.com/library/content/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html

PIV Mandatory

Apple has released a great resource to learn more about handling the PIV-M (PIV Mandate under HSPD-12) on macOS High Sierra 10.13.2 devices:

https://support.apple.com/en-us/HT208372