How to Configure Jamf Connect Login, Azure, and IDent for Certificate Provisioning

Contents

Preface 3
Section 1: Creating an App Registration in Azure for IDent 5
Section 2: Configure IDent settings in Jamf Pro 11
Section 3: Uploading IDent and Jamf Connect to the Jamf Pro Server 21
Section 4: Creating installation policies for IDent and Jamf Connect on the Jamf Pro Server 23
Section 5: Test IDent and Jamf Connect on a Mac Computer 26
Section 6: Troubleshooting Commands 29
Section 7: Glossary of terms used in this guide 30

IDent helps to solve challenges seen in bootstrapping trust and provisioning keys as well as certificates to macOS endpoints for device and user identity.

IDent is a client server application used to issue and distribute user certificates for macOS with an IdP gated workflow. This is designed to be deployed along Jamf Connect, as an alternative to the missing user MDM channel.

The IDent Gateway is also a SCEP Proxy Service that allows the use of MDM SCEP profiles used for Device Certificate provisioning. A deployment of IDent and IDent Gateway can substitute or replace a Jamf ADCS Connector setup and connect Jamf via SCEP Proxy Setup to several PKI options. (Windows NDES/ADCS, Cloud PKI providers)

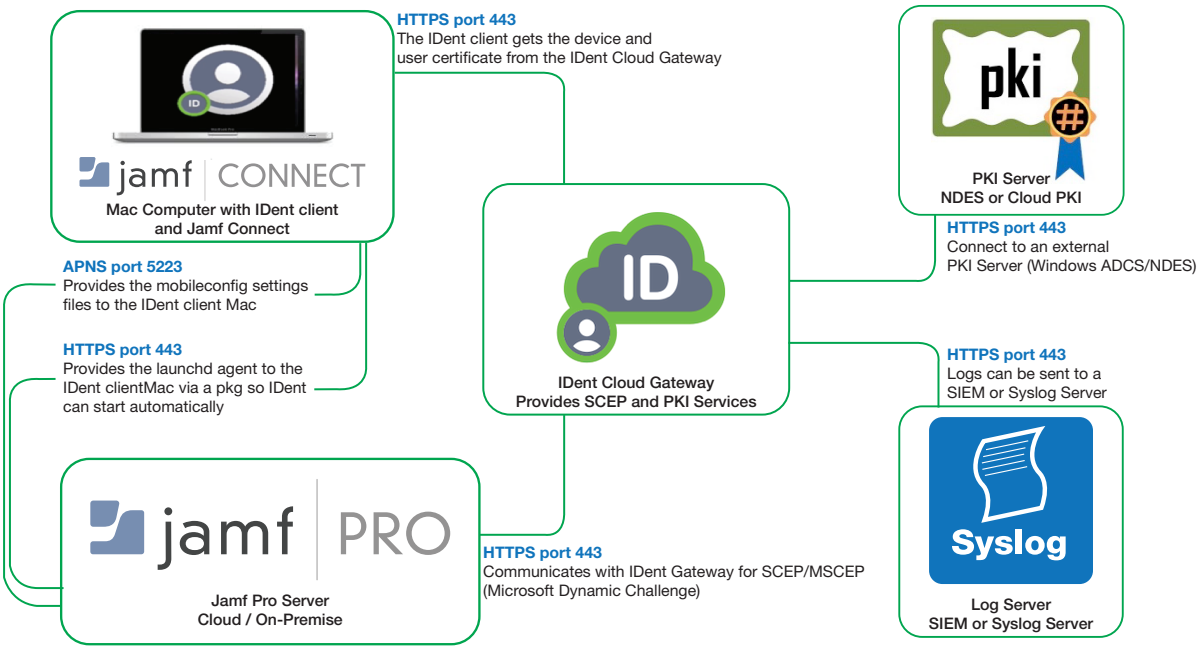
IDent benefits using Jamf Connect instead of Jamf with ADCS connector:

1. Cloud based deployment
2. Includes IdP attestation for user certificate acquisition (self driven process and Jamf Connect Login)
3. Flexible in PKI (Classic Windows, Modern cloud PKI)
4. In depth logging and auditing (option for sending events to SIEM and syslog servers.)
5. SCEP PKI proxy service
6. Private key always on device
7. Additional validation steps in the process

Drawbacks of using Jamf ADCS connector with Jamf Connect:

1. Requires DMZ / Windows VM based deployment.
2. Private key created in Jamf not on device
3. Poor logging (IIS log)
4. Process of all certificate requests without any additional validation steps

How IDent Works



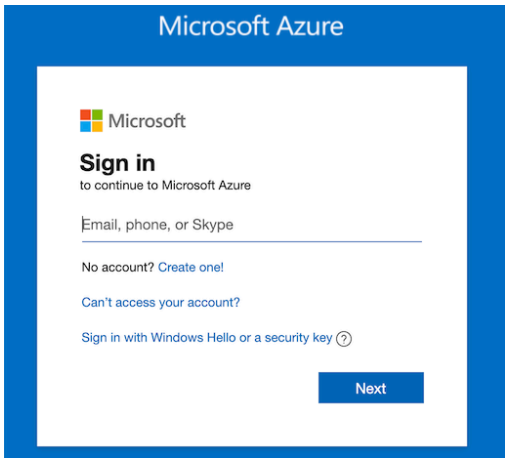
The following was used to create this guide:

- macOS Catalina 10.15.6 - enrolled into Jamf Pro
- Jamf Pro 10.23 cloud hosted
- Jamf Connect Login 1.11.4
- Microsoft Azure

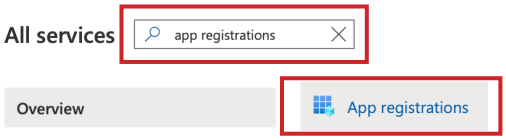
NOTE: In order to follow along with this guide, You will need a trial version of IDent. HCS can assist with getting the IDent trial setup for you and integrating it within your environment. For more info, contact us at info@hcsonline.com.

Section 1: Creating an App Registration in Azure for IDent

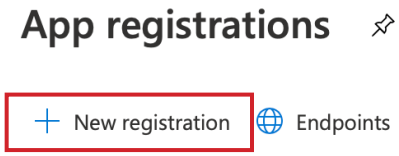
1. Using a web browser of your choosing, go to http://portal.azure.com and sign in to Microsoft Azure with administrative credentials.



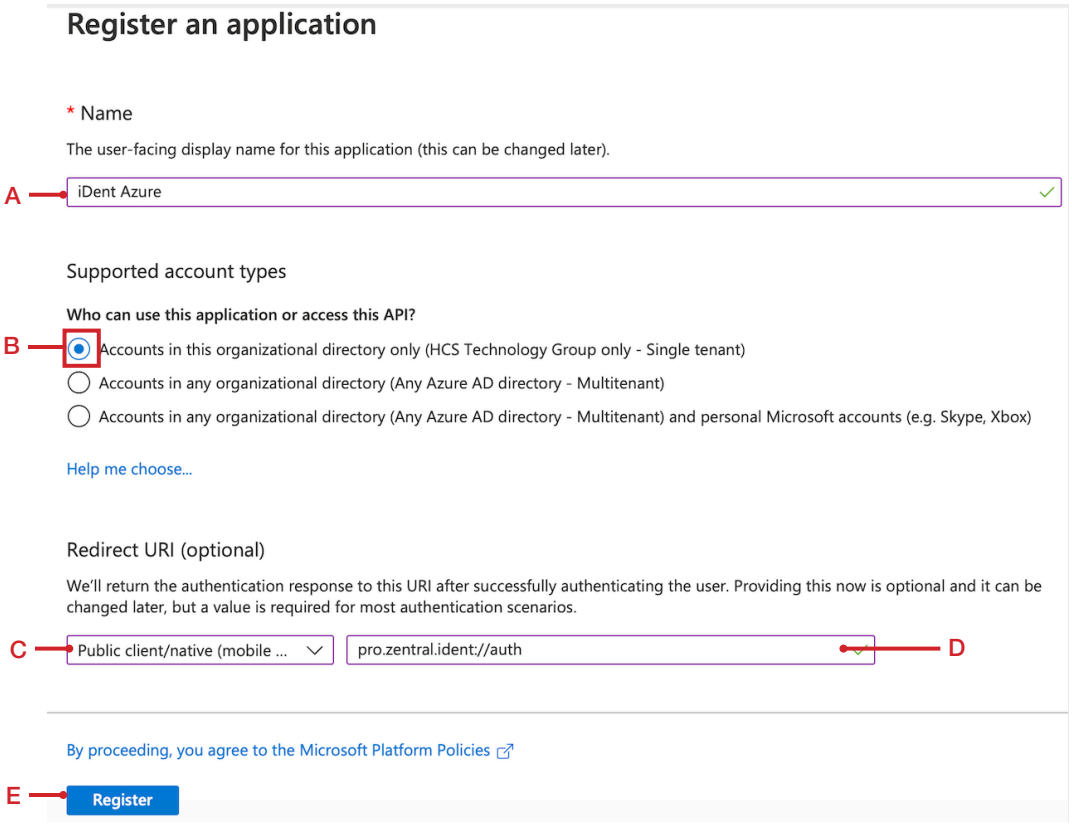
2. Enter app registrations in the search field, then select App registrations.



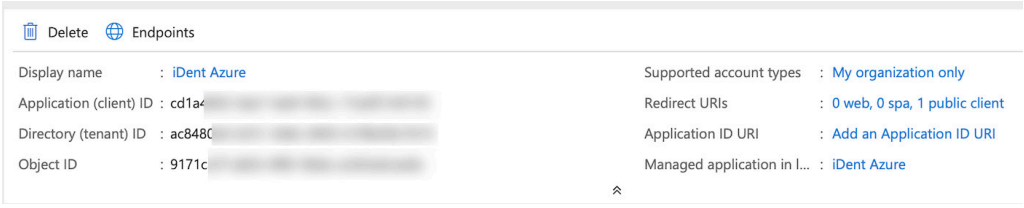
3. Click New registration.



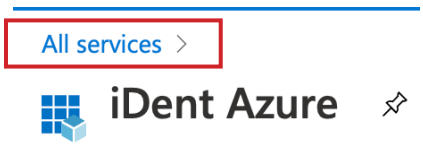
4. Enter the following:
   A. Name: IDent Azure
   B. Supported account types: Accounts in this organization directory (your organization name - Single tenant)
   C. Redirect URI: Select Public client/native from the drop down menu.
   D. Enter this URI: pro.zentral.IDent://auth
   E. Click the Register button



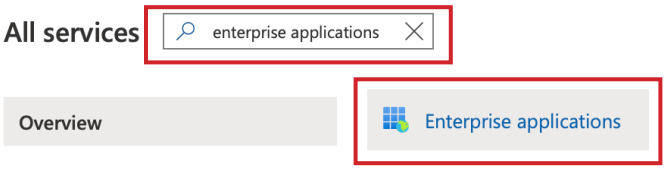
5. Confirm the IDent application registration was created.



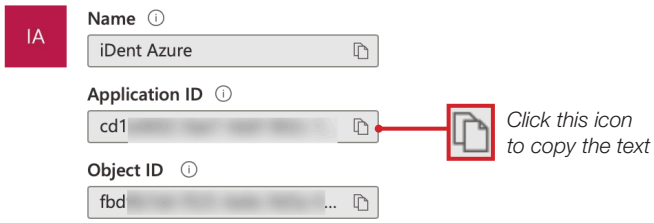
6. Click All services.



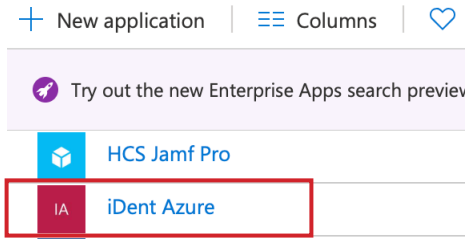
7. In the search field, type: enterprise applications then select the Enterprise applications button.



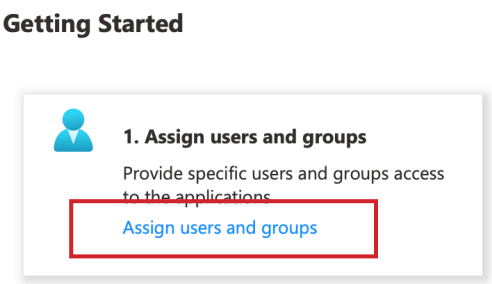
8. Copy the Application ID to a text document. Provide the Application ID to your IDent Integrator so they can configure the OIDCClientID key in the pro.zentral.user-cert-config.plist.



9. Select the IDent Azure application.

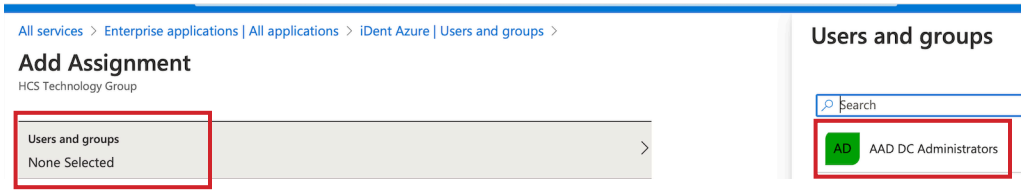


10. Click Assign users and groups.

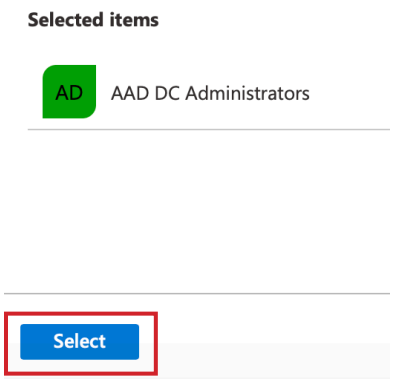


11. Click Add user.

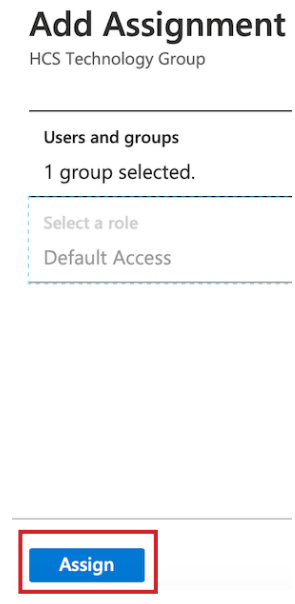
12. In the Add Assignment section, Select Users and groups. In the Users and groups section, select a user or group.



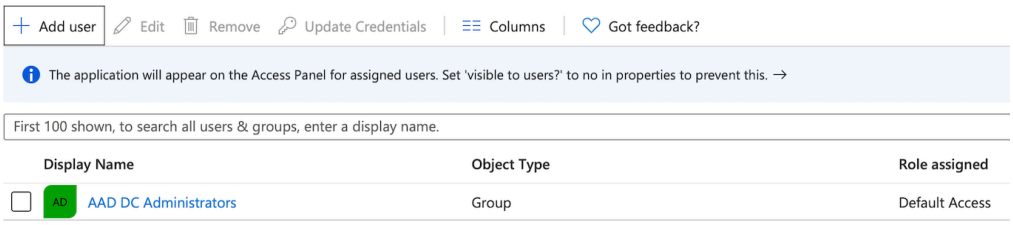
13. Click the Select button.



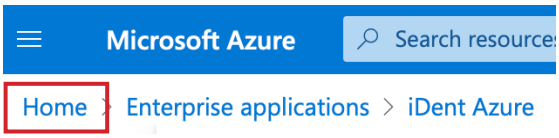
14. Click the Assign button.



15. Confirm the user or group has access to the IDent application.

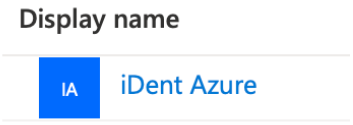


16. Select Home.



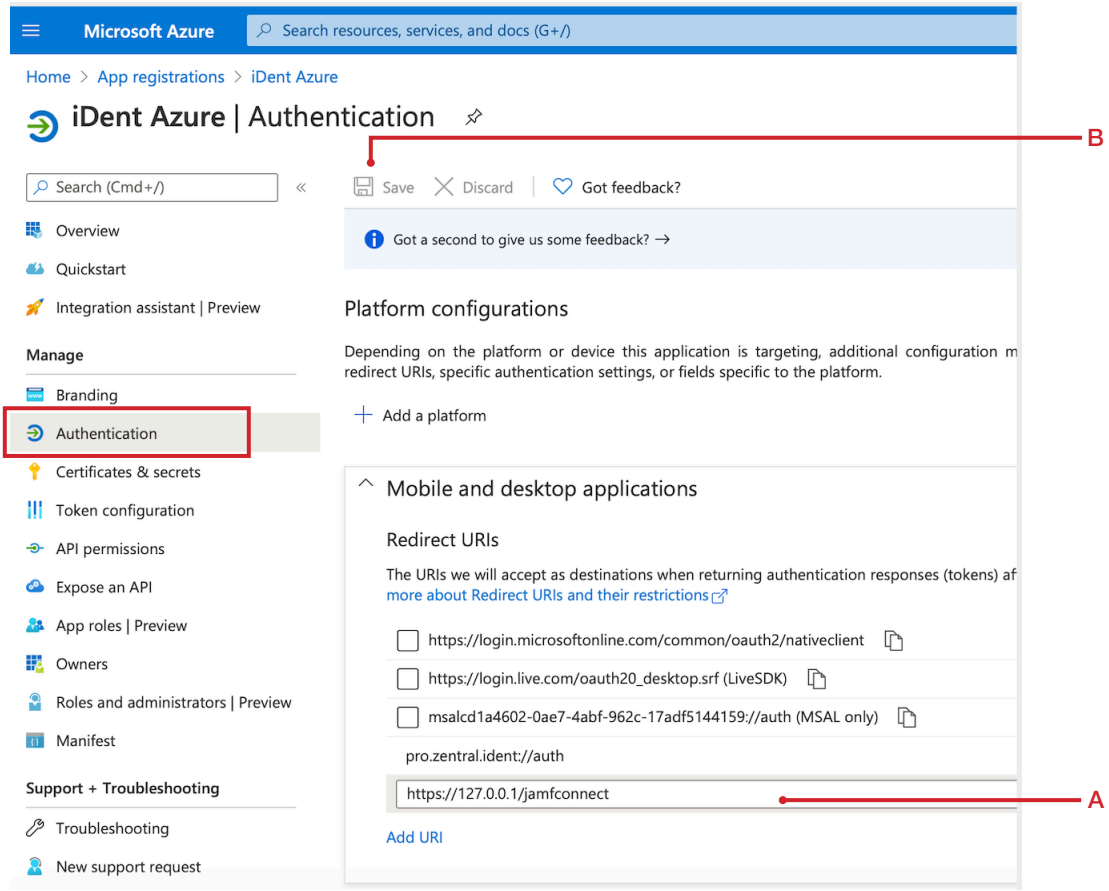
17. Select App registrations.

18. Select iDent Azure.



19. Select Authentication from the left side bar, then select Add URI.
    A. Enter the following in the URI field: https://127.0.0.1/jamfconnect
    B. Select Save.
    C. Log out of Azure.

NOTE: This entry allows Microsoft Azure to interact with Jamf Connect on the local Mac Computer.

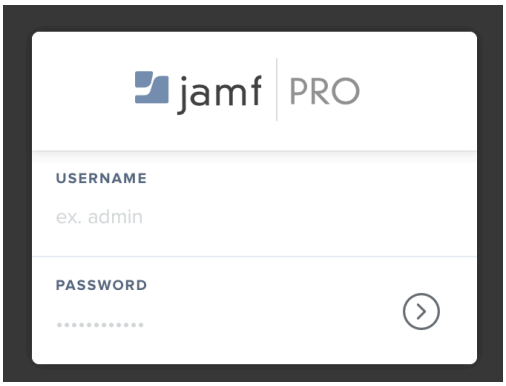


Section 2: Configure IDent settings in Jamf Pro

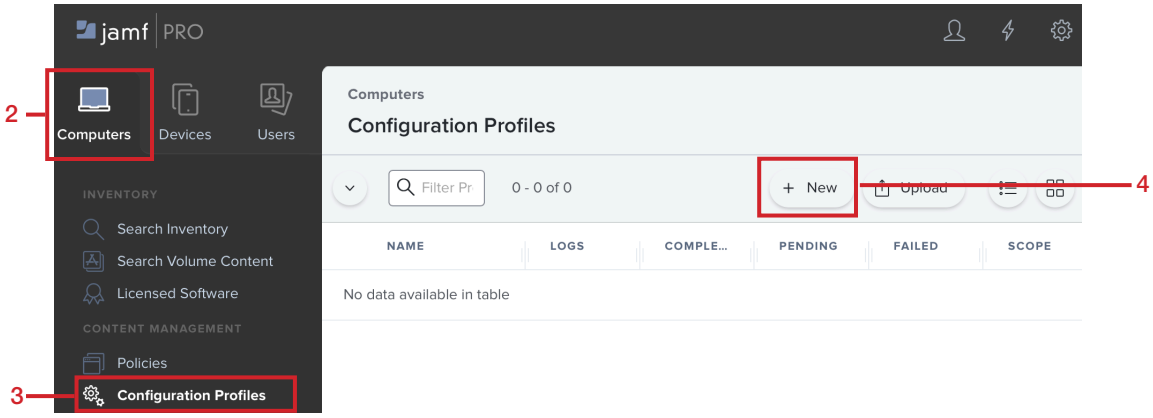
NOTE: This section requires 3 plist files that contain the settings required for IDent. These files will be provided to you by your IDent Integrator.

- com.apple.notificationsettings.plist
- com.jamf.connect.login.plist
- pro.zentral.user-cert-config.plist

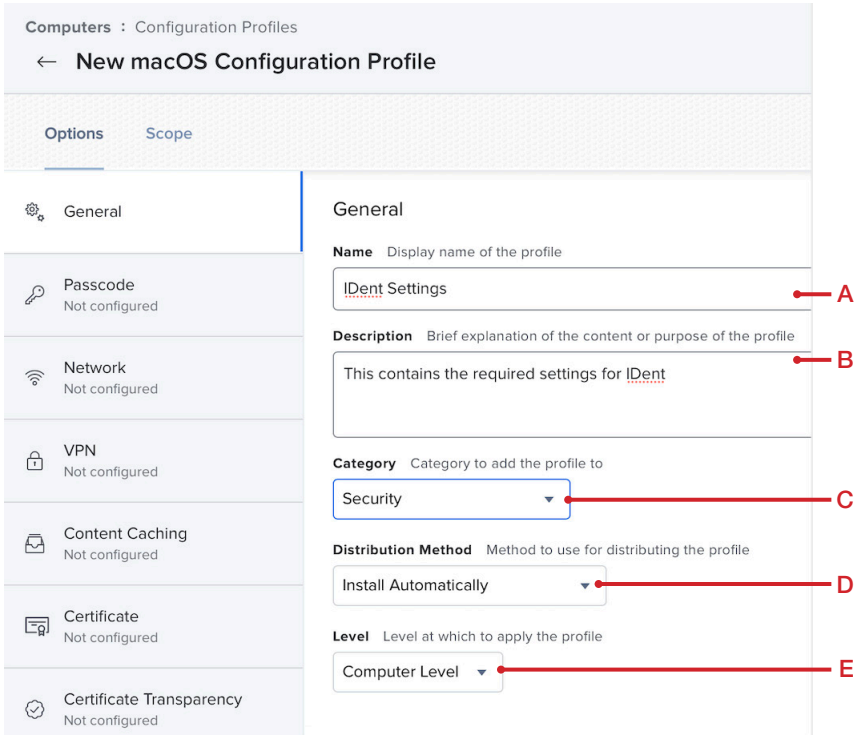
1. Using a web browser of your choosing, log in to your Jamf Pro server.



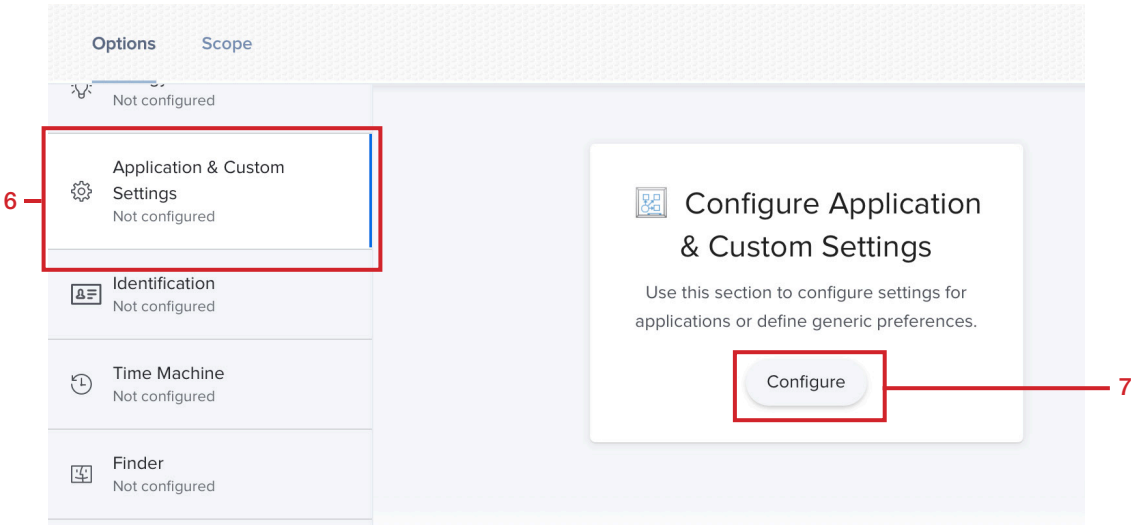
2. Click Computers.
3. Click Configuration Profiles.
4. Click New.



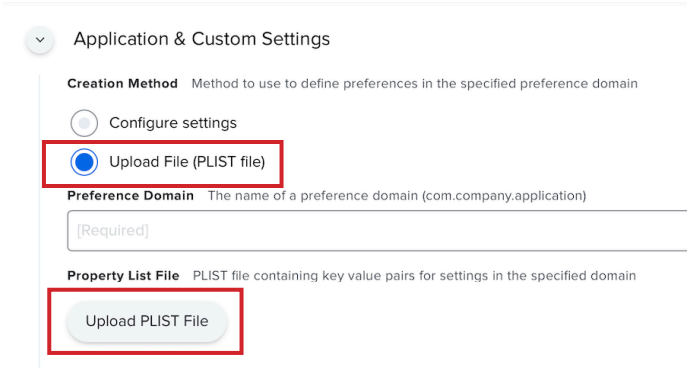
5. In the General Section, Enter the following:
    A. Name: IDent Settings
    B. Description: This contains the required settings for IDent
    C. Category: Security (or a category of your choosing)
    D. Distribution Method: Install Automatically
    E. Level: Computer



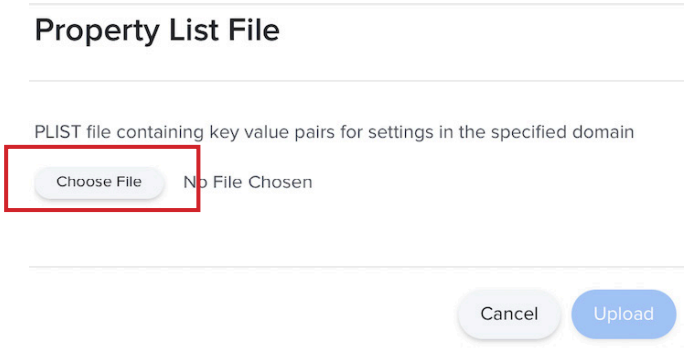
6. In the payload section, select Application & custom Settings.
7. Click Configure.



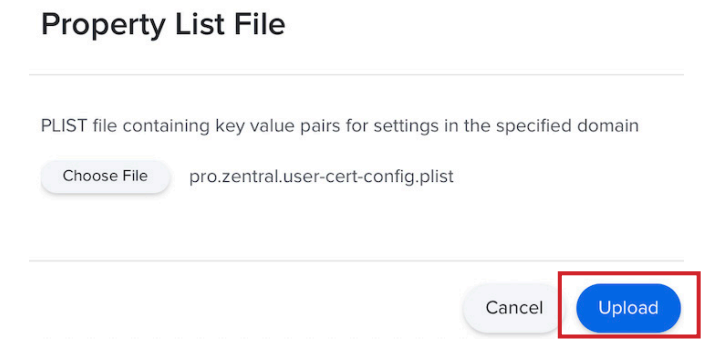
8. In the Application & Custom Settings section, select Upload File (PLIST file) then click the Upload PLIST File button.



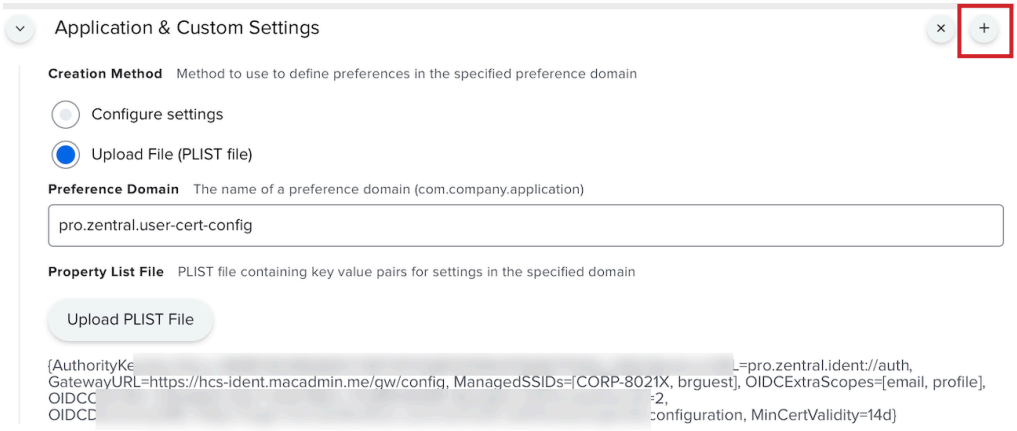
9. Click the Choose File button.



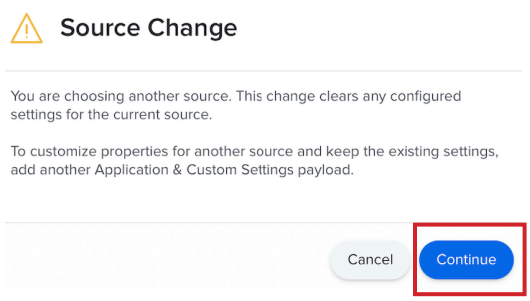
10. Navigate to the location of your IDent plist files that you downloaded at the beginning of section 2. Select the pro.zentral.user-cert-config.plist then click the Upload button.



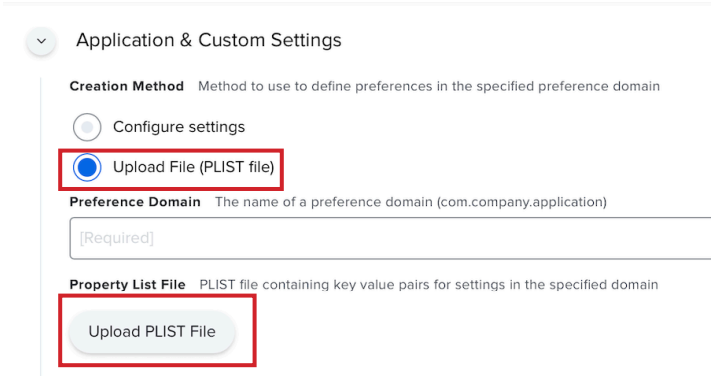
11. The plist file was successfully uploaded. Click Add (+) to add a second plist.



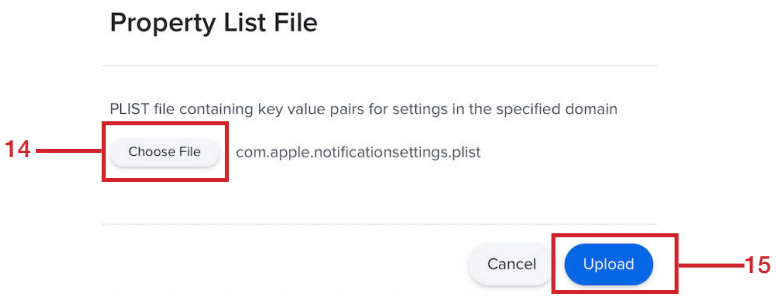
12. Click Continue at the message below.



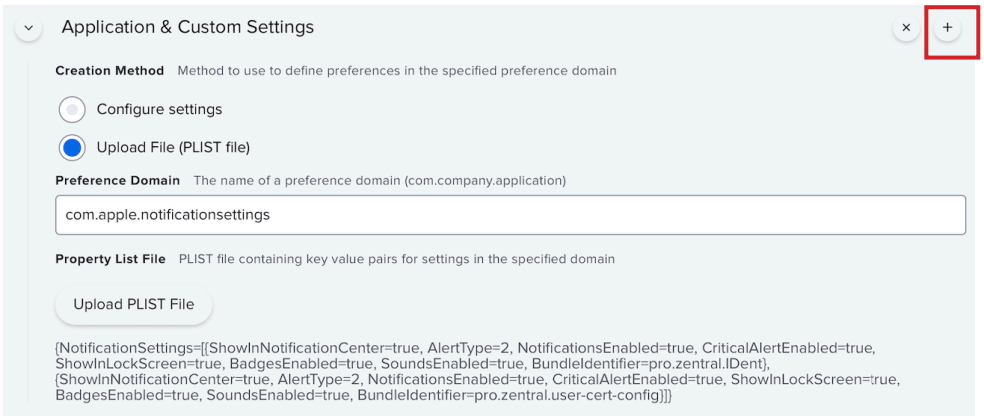
13. In the Application & Custom Settings section, select Upload File (PLIST file) then click the Upload PLIST File button.



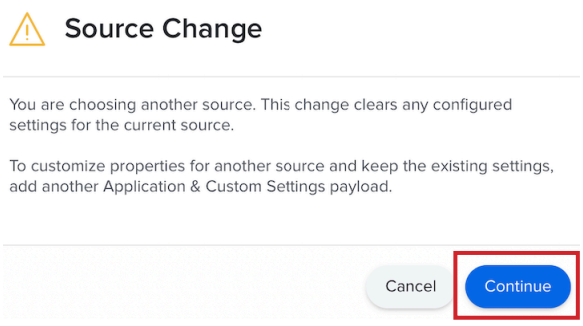
14. Click the Choose File button.
15. Navigate to the location of your IDent plist files that you downloaded at the beginning of section 2. Select the com.apple.notificationsettings.plist then click the Upload button.



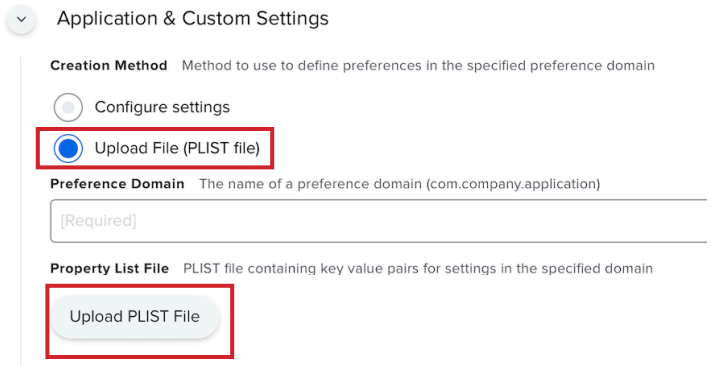
16. The plist file was successfully uploaded. Click Add (+) to add a third plist.



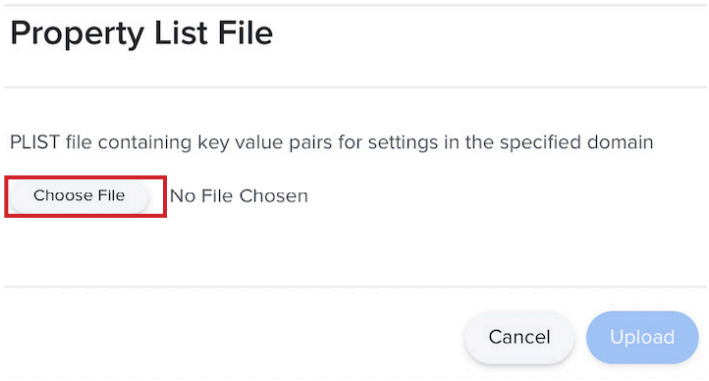
17. Click Continue at the message below.



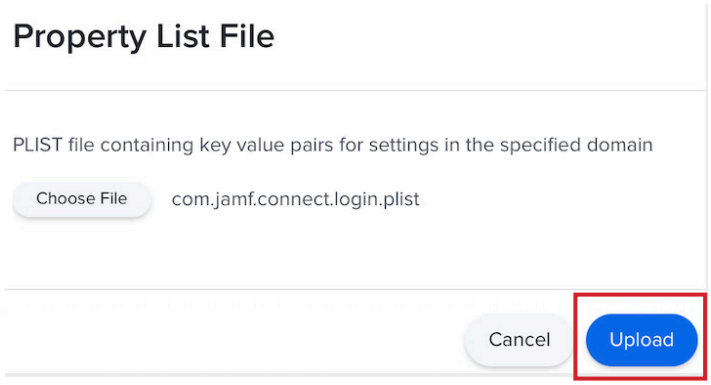
18. In the Application & Custom Settings section, select Upload File (PLIST file) then click the Upload PLIST File button.



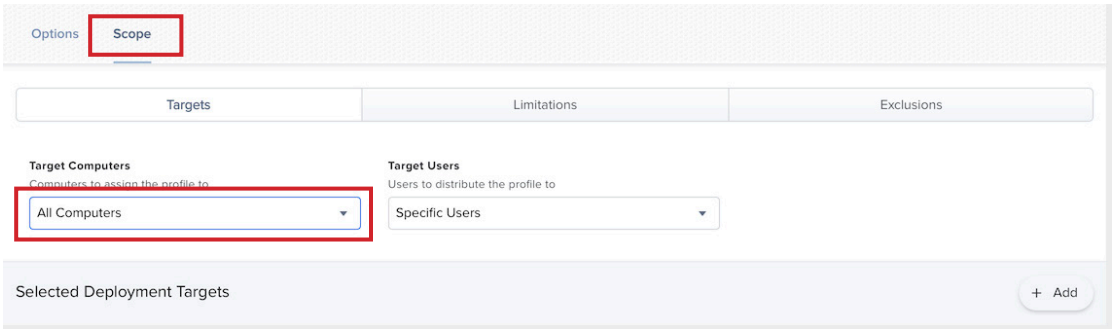
19. Click the Choose File button.



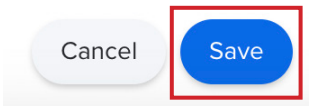
20. Navigate to the location of your IDent plist files that you downloaded at the beginning of section 2. Select the com.jamf.connect.login.plist then click the Upload button.



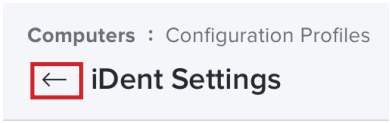
21. Scope to your needs.



22. Click Save.

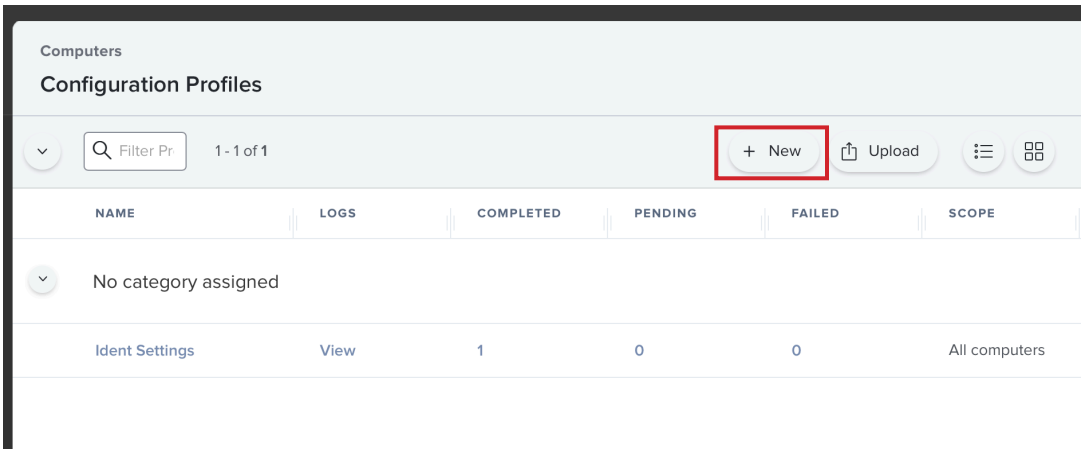


23. Click the back button (Arrow).

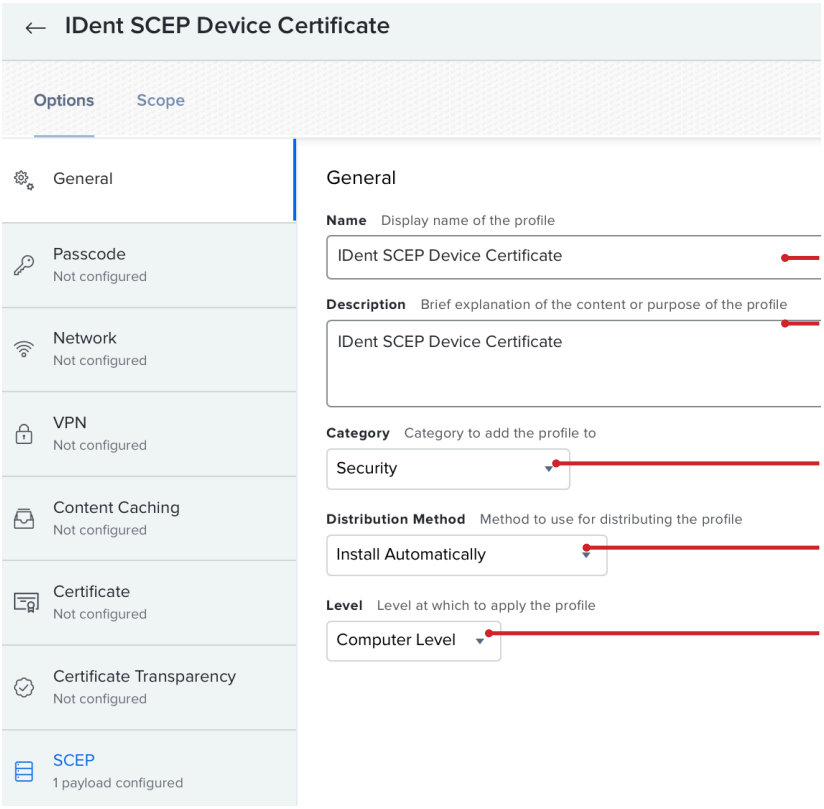


NOTE: The steps below will require you to work with your IDent integrator to get the information needed for your Device Certificate. Test information is used for the purpose of this guide to show the required steps.

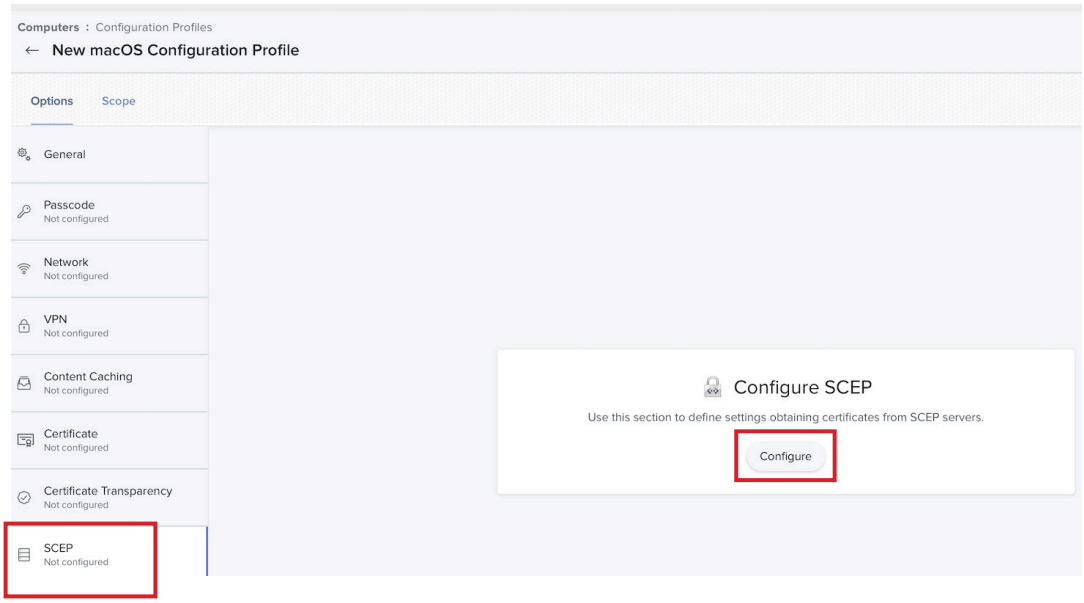
24. Click New.



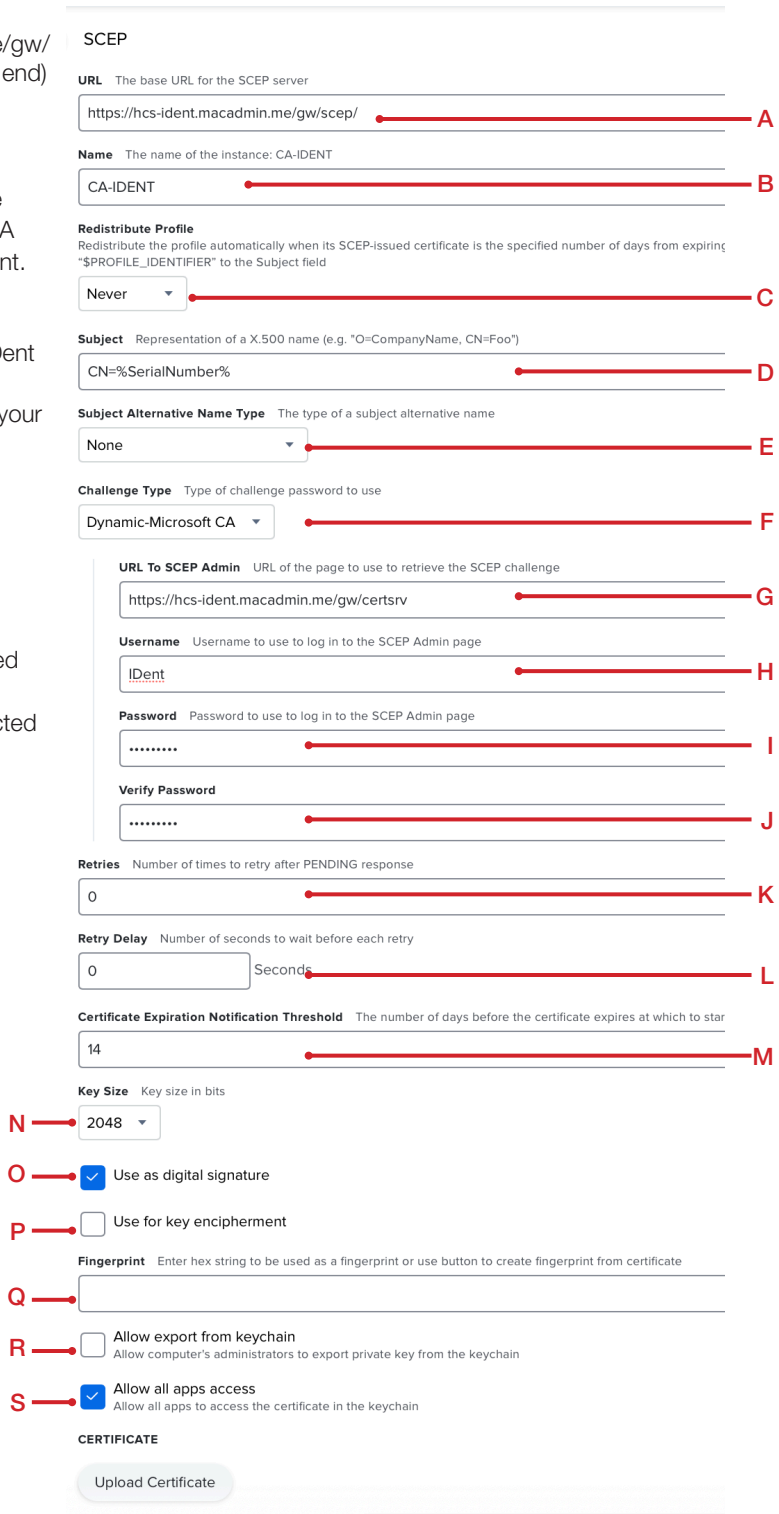
25. In the General section, Enter the following:
    A. Name: IDent SCEP Device Certificate
    B. Description: IDent SCEP Device Certificate
    C. Category: Security (or one of your choosing)
    D. Distribution Method: Install Automatically
    E. Level: Computer Level



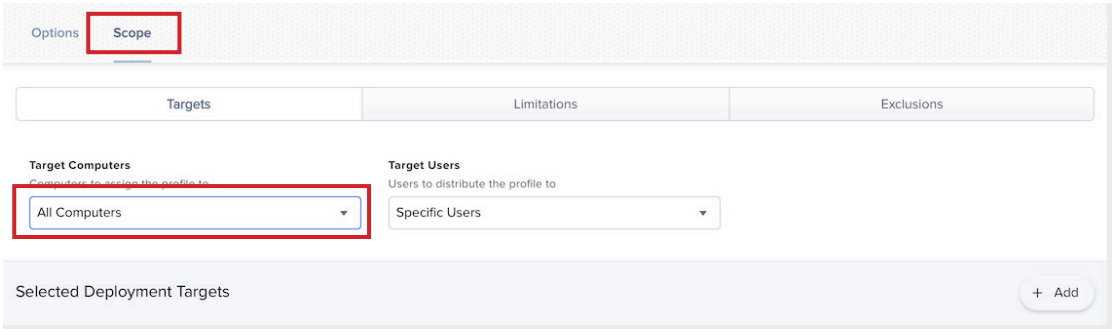
26. Select the SCEP payload on the left, then click configure on the right.



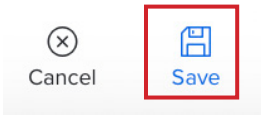
27. Enter the following information:
    A. URL: https://hcs-ident.macadmin.me/gw/scep/ (must have trailing slash at the end)
    B. Name: CA-IDENT
    C. Redistribute Profile: Never
    D. Subject: CN=%SerialNumber%
    E. Subject Alternative Name Type: None
    F. Challenge Type: Dynamic Microsoft CA
    G. URL to SCEP Admin: https://hcs-ident.macadmin.me/gw/certsrv
    H. User Name: IDent
    I. Password: (will be provided by your IDent Integrator)
    J. Verify Password: (will be provided by your IDent Integrator)
    K. Retries: 0
    L: Retry Delay: 0
    M: Certificate Expiration Notification Threshold: 14
    N. Key Size: 2048
    O. User as digital signature: Selected
    P. Use for key encipherment: De Selected
    Q. Fingerprint: blank
    R. Allow export from keychain: De Selected
    S. Allow all apps access: Selected



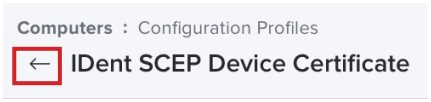
28. Select Scope and scope to you needs



29. Click Save.



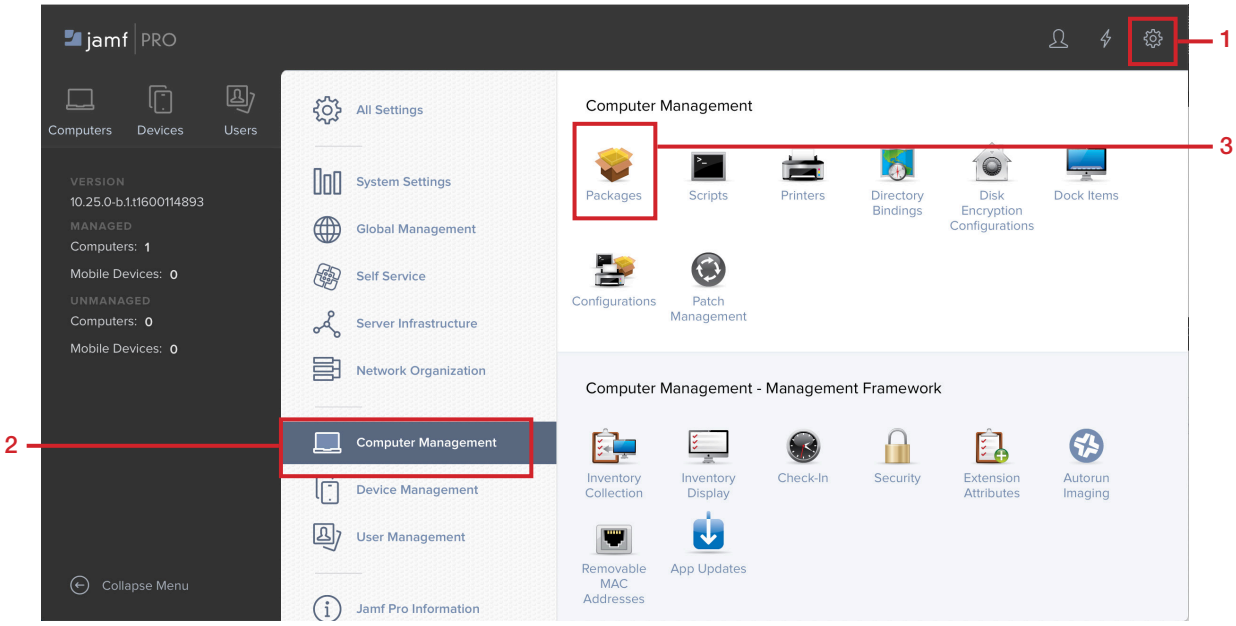
30. Click the back button (Arrow).



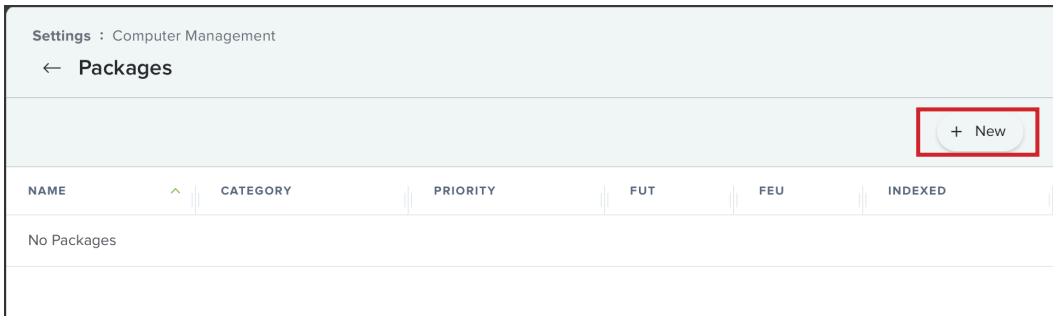
Section 3: Uploading IDent and Jamf Connect to the Jamf Pro Server

NOTE: Your IDent integrator will provide you with a custom installer pkg for the IDent application. If you don't have that file you cannot move forward with this guide.

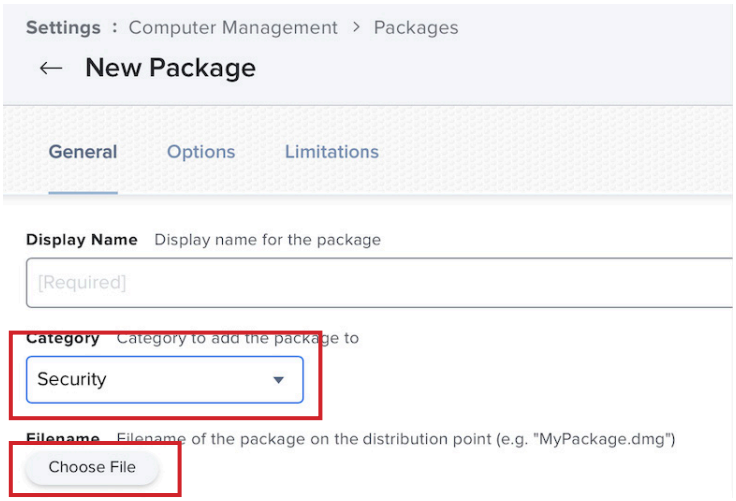
1. Click All Settings (gear icon in the right corner).
2. Select Computer Management.
3. Select Packages.



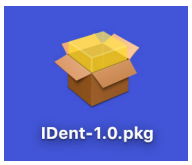
4. Select New.



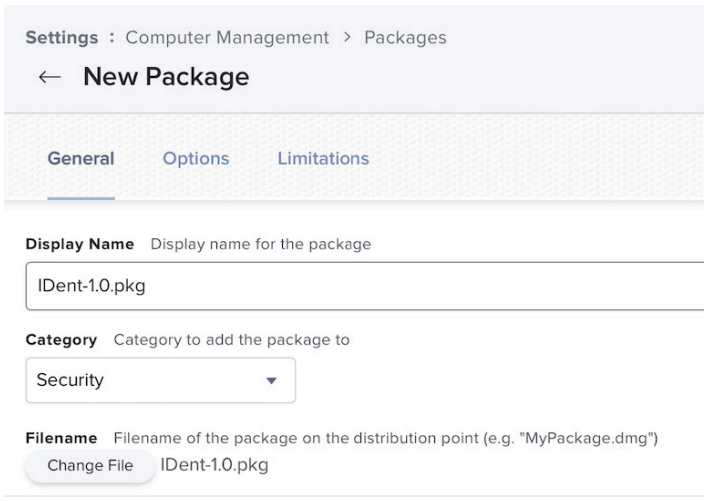
5. Select a Category of your choosing, then select the Choose file button.



6. Navigate to the location of the IDent-1.0.pkg file and choose it.
Note: This file was provided to you by your IDent integrator.



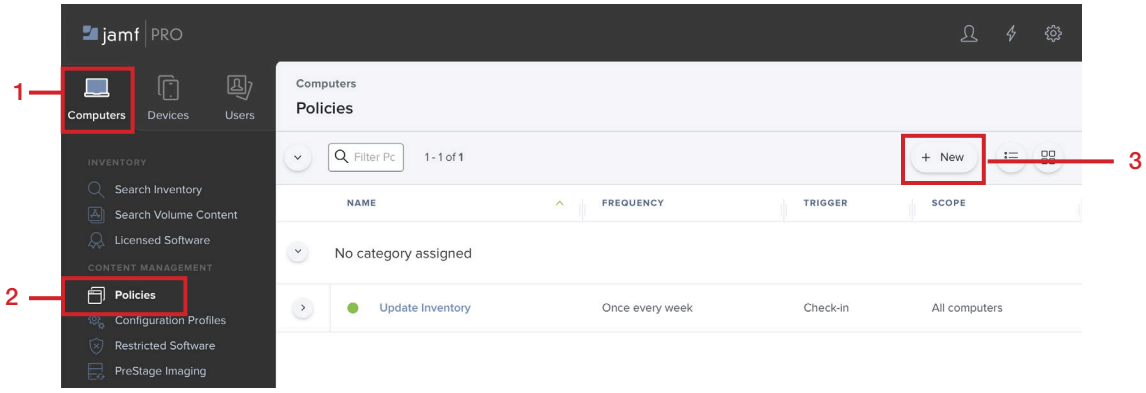
7. Confirm the file is ready for upload.



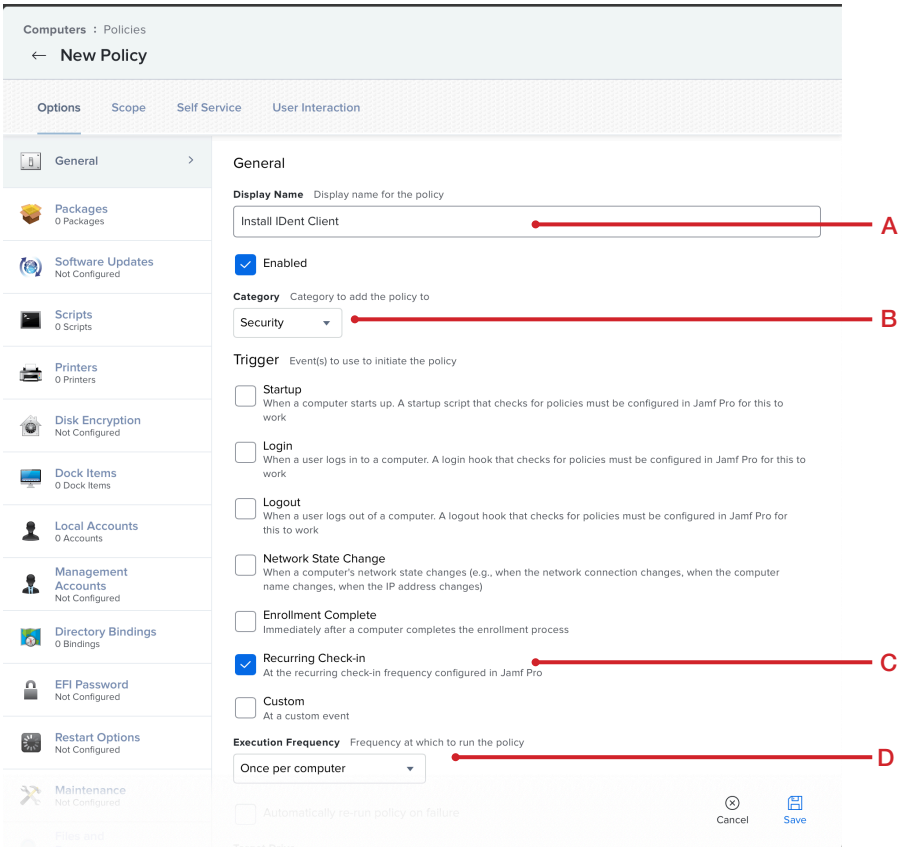
8. Click Save.

Section 4: Creating installation policies for IDent and Jamf Connect on the Jamf Pro Server

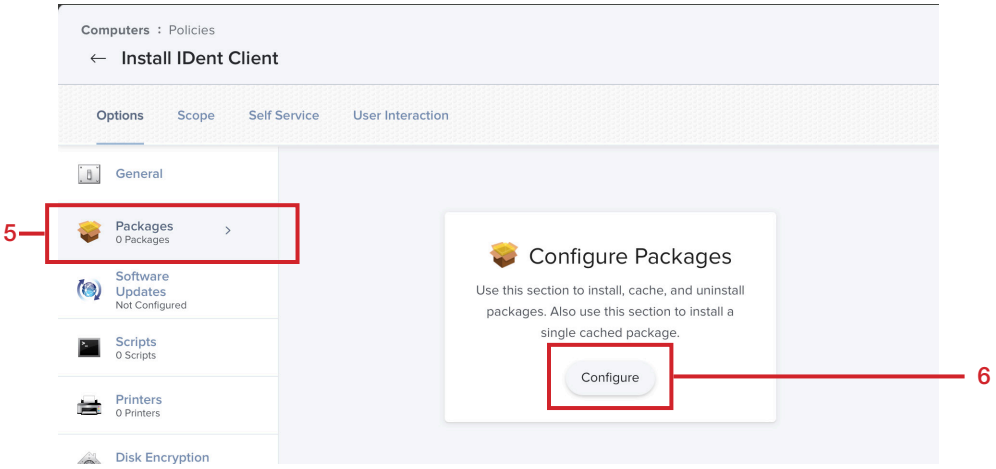
1. Click Computers.
2. Click Policies.
3. Click New.



4. In the General section, configure the following:
   A. Display Name: Install IDent Client
   B. Category: Security (Or one of your choosing)
   C. Trigger: Recurring Check-In
   D. Execution Frequency: Once per computer

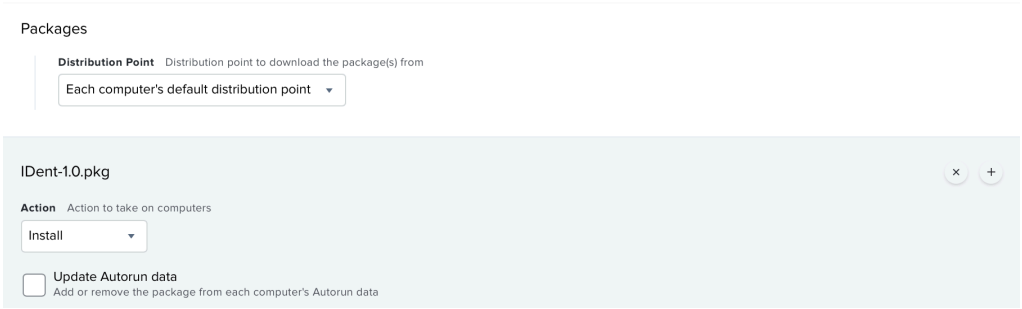


5. Click Packages.
6. Click Configure.

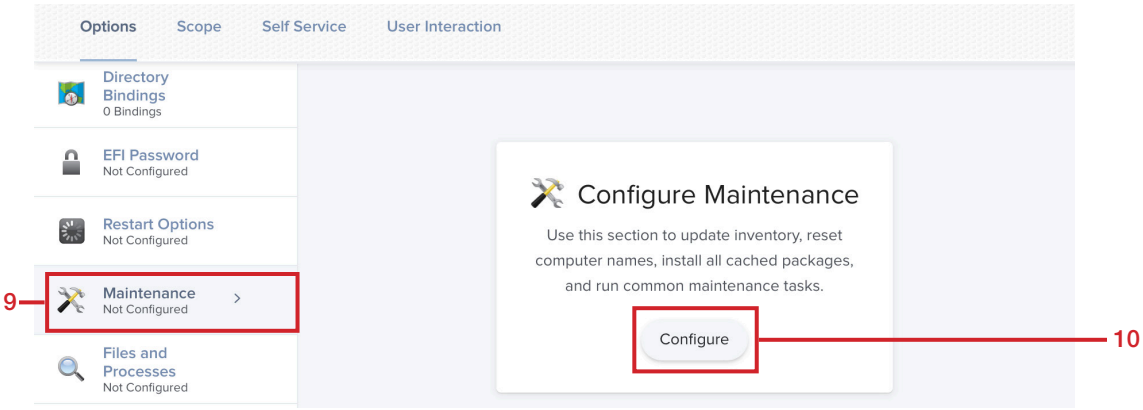


7. Select Add for the IDent-1.0.pkg.

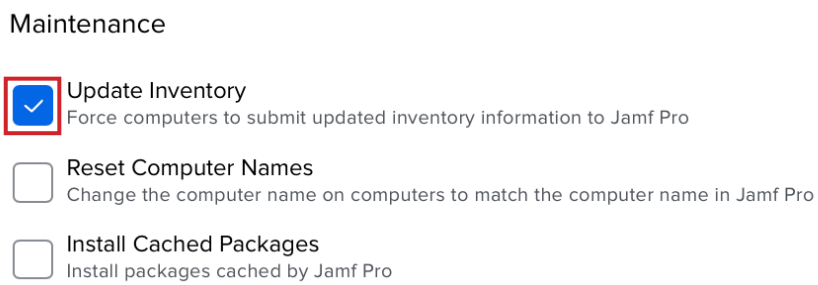
8. Confirm the IDent-1.0.pkg. is there.



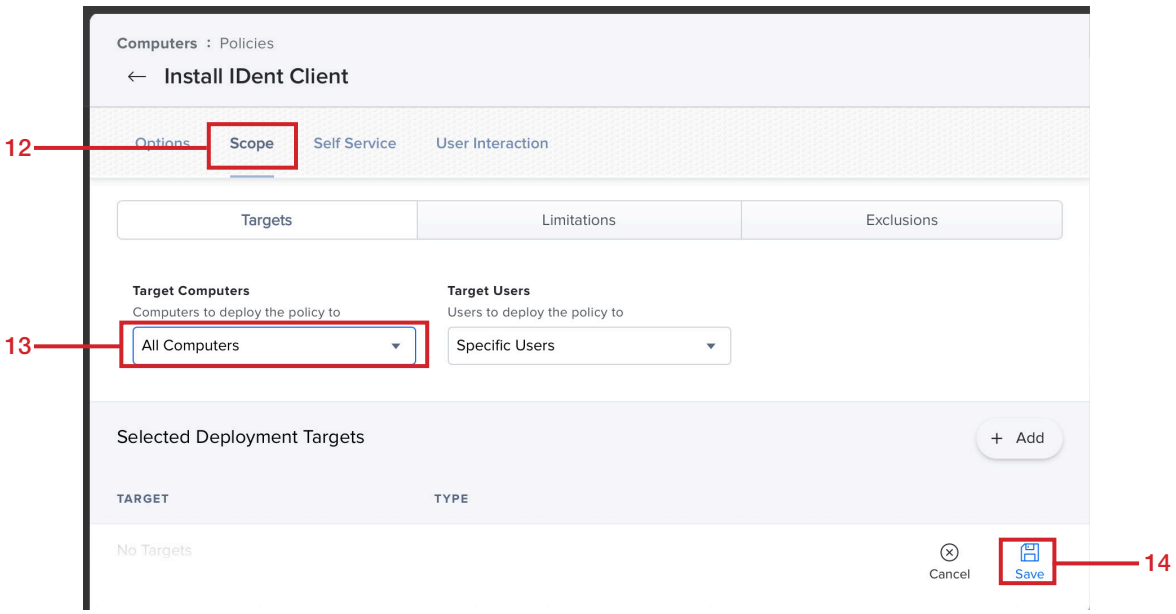
9. Click Maintenance.
10. Click Configure.



11. Select Update Inventory.



12. Select Scope.
13. Scope according to your needs.
14. Select Save.

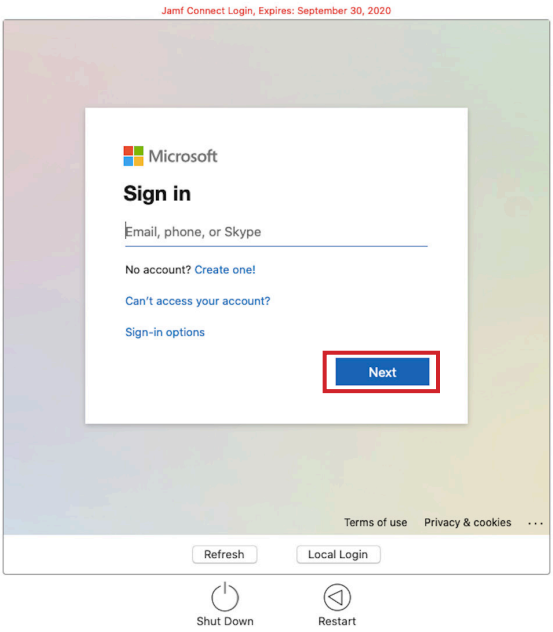


15. Follow the same steps above to configure a policy to install Jamf Connect.

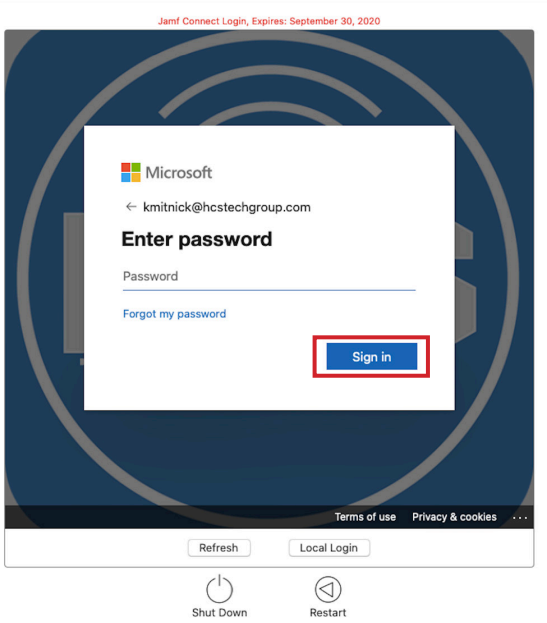
Section 5: Test IDent and Jamf Connect on a Mac Computer

NOTE: A client Mac computer that is enrolled into Jamf Pro is required for this section. We are assuming the IDent Application and mobile configuration files are installed along with Jamf Connect Login.

1. Log into a client Mac computer when prompted by Jamf Connect Login. Enter your Microsoft Azure credentials then click Next.

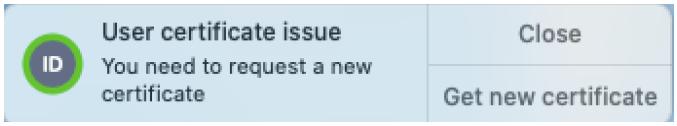


2. Enter your password then click Sign In. This will create a new local user account on the Mac computer.

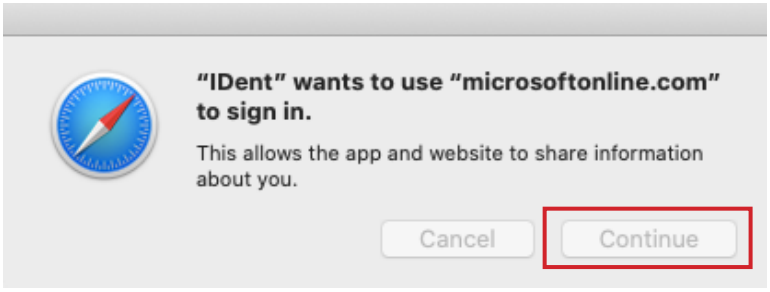


3. Enter a password for the newly created local account then click Create Account.

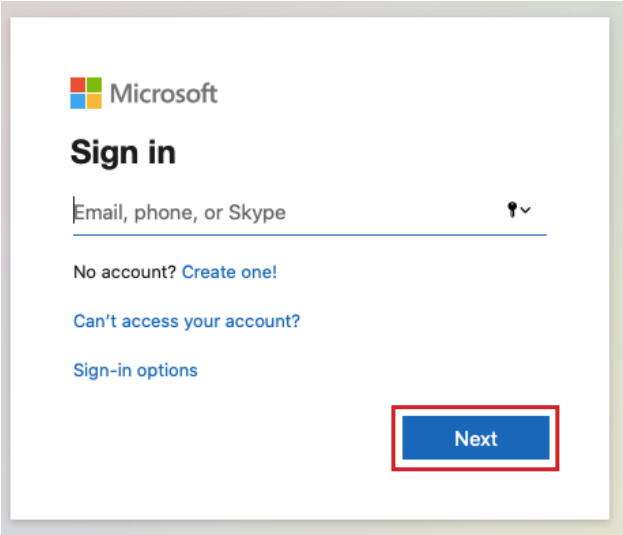
4. Once logged in, you will get a notification from IDent requesting a new user certificate. Click Get new certificate.



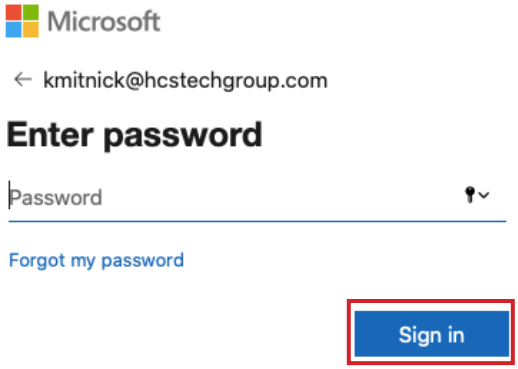
5. Safari will open. Click continue at the message below.



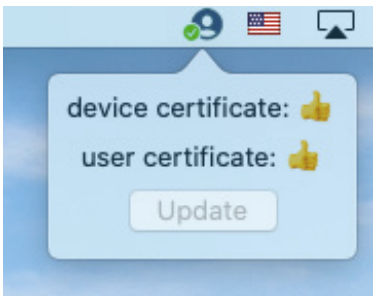
6. Enter your Microsoft Azure credentials then click Next.



7. Enter your password then click Sign In. This will create a user certificate for the logged in account on the Mac computer.



8. The IDent icon in the menu bar shows a valid device and user certificate.



Section 6: Troubleshooting Commands

You can collect logs to help understand, configure, and troubleshoot the application processes. Log streaming allows the viewing of log entries made in real-time. Use the commands below to enable and view debug logs for one or more application processes.

Enable log stream for Jamf Connect:

```
log stream --predicate 'subsystem == "com.jamf.connect.login"' --debug --info
```

Enable log stream for IDent:

```
sudo log stream --debug --info --predicate 'subsystem == "pro.zentral.user-cert-config"'
```

Enable log stream for Jamf Connect and IDent:

```
sudo log stream --debug --info --predicate 'process == "logger" || subsystem == "com.jamf.
connect.login" || subsystem == "pro.zentral.user-cert-config"'
```

Enable log stream for Jamf Connect and IDent and SCEP:

```
sudo log stream --debug --info --predicate 'process == "logger" || subsystem == "com.jamf.
connect.login" || subsystem == "pro.zentral.user-cert-config" || subsystem == "com.apple.SCEP"'
```

MDM and SCEP Debug Log for Last Hour:

```
log show --info --debug --predicate '(subsystem == "com.apple.ManagedClient") &&
(senderImagePath ENDSWITH "Certificate")' --last 1h
```

Jamf Connect and IDent and SCEP Log for Last Hour:

```
sudo log show --debug --info --predicate 'process == "logger" || subsystem == "com.jamf.
connect.login" || subsystem == "pro.zentral.user-cert-config"|| subsystem == "com.apple.SCEP"'
--last 1h
```

Section 7: Glossary of terms used in this guide

ADCS :
Active Directory Certificate Services provides customizable services for issuing and managing public key infrastructure certificates used in software security systems that employ public key technologies. The digital certificates that AD CS provides can be used to encrypt and digitally sign electronic documents and messages. Further, these digital certificates can be used for authentication of the computer, user, or device accounts on a network.

Device Certificate :
A device certificate is an electronic document that is embedded into a hardware device and can last for the life of the device. The certificate's purpose is similar to that of a driver's license or passport: it provides proof of the device's identity and, by extension, the identity of the device owner.

IdP:
An Identity Provider is a system entity that creates, maintains, and manages identity information for principals while providing authentication services to relying applications within a federation or distributed network. Identity providers offer user authentication as a service.

NDES:
The Network Device Enrollment Service allows software on routers and other network devices running without domain credentials to obtain certificates based on the Simple Certificate Enrollment Protocol (SCEP).

OIDC:
OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol, which allows computing clients to verify the identity of an end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end-user in an interoperable and REST-like manner. In technical terms, OpenID Connect specifies a RESTful HTTP API, using JSON as a data format.
OpenID Connect allows a range of kinds of clients, including Web-based, mobile, and JavaScript clients, to request and receive information about authenticated sessions and end-users. The specification suite is extensible, supporting optional features such as encryption of identity data, discovery of OpenID Providers, and session management.

PKI:
Public Key Infrastructure is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.

ROPG:
Resource Owner Password Grant authenticates the user's cloud username and password directly to your IdP's token endpoint. This authentication method is only used for password synchronization.

SCEP:
Simple Certificate Enrollment Protocol was developed to support the secure, scalable issuance of certificates to network devices by using existing certification authorities (CAs). The protocol supports CA and registration authority public key distribution, certificate enrollment, certificate revocation, certificate queries, and certificate revocation queries.

SIEM:
Security Information and Event Management is a software solution that aggregates and analyzes activity from many different resources across your entire IT infrastructure. SIEM collects security data from network devices, servers, domain controllers, and more.

User Certificate:
A User Certificate can be used to perform many functions, including authentication. A certificate can be used to represent a user's digital identity. In most cases, a user certificate is mapped back to a user account. Access control will then be based on this user account.

If you'd like help implementing the solution in this white paper, we are ready to help; contact us at info@hcsonline.com or (866) 518-9672.

If you have corrections please send them to info@hcsonline.com.

For more white papers, visit https://hcsonline.com/support/white-papers. For more information about HCS, visit https://hcsonline.com.