





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	2: Configure IDent settings in Jamf Pro	11
Section 3	3: Uploading IDent and Jamf Connect to the Jamf Pro Server	21
Section 4	4: Creating installation policies for IDent and Jamf Connect on the Jamf Pro Server	23
Section 8	5: Test IDent and Jamf Connect on a Mac Computer	26
Section 6	6: Troubleshooting Commands	29
Section 7	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.

Micro	soft Azure	
Microsoft		
Sign in to continue to Microsoft A	zure	
Email, phone, or Skyp	3	
No account? Create one!		
Can't access your account	t?	
Sign in with Windows Hell	o or a security key 🥎	
	Next	

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

All services	×
Overview	 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

	Register an application
	* Name
	The user-facing display name for this application (this can be changed later).
A —	iDent Azure
	Supported account types
	Who can use this application or access this API?
в —	Accounts in this organizational directory only (HCS Technology Group only - Single tenant)
	Accounts in any organizational directory (Any Azure AD directory - Multitenant)
	O Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
	Help me choose
	Redirect URI (optional)
	We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
с –	Public client/native (mobile V) pro.zentral.ident://auth
- E —	By proceeding, you agree to the Microsoft Platform Policies ♂

5. Confirm the IDent application registration was created.

📋 Delete 🜐 Endpoints			
Display name : iDent Azure		Supported account types	: My organization only
Application (client) ID : cd1a4		Redirect URIs	: 0 web, 0 spa, 1 public client
Directory (tenant) ID : ac8480		Application ID URI	: Add an Application ID URI
Object ID : 9171c		Managed application in I	: iDent Azure
	*		

6. Click All services.





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

All services	\checkmark enterprise applications \times		
Overview		Enterprise applications	5

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.

1.4	Name 🛈				
IA	iDent Azure				
	Application ID ① Cd1 Object ID ①		Click this icon to copy the text		
	fbd 🗈				

9. Select the IDent Azure application.



10. Click Assign users and groups.

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
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.



Users and groups 1 group selected. Select a role Default Access





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



16. Select Home.



17. Select App registrations.



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.

■ Microsoft Azure	resources, services, and docs (G+/)	
Home > App registrations > iDent Azu	re	
iDent Azure Authe	ntication 🖉	
Search (Cmd+/) «	☐ Save × Discard V Got feedback?	
Noverview	(\mathbf{j}) Got a second to give us some feedback? $ ightarrow$	
🍪 Quickstart		
💅 Integration assistant Preview	Platform configurations	
Manage	Depending on the platform or device this application is targeting, additional configuration m redirect URIs, specific authentication settings, or fields specific to the platform.	
💳 Branding	+ Add a platform	
Ə Authentication		
📍 Certificates & secrets	^ Mobile and desktop applications	
Token configuration		
-> API permissions	Redirect URIs	
Expose an API	The URIs we will accept as destinations when returning authentication responses (tokens) af more about Redirect URIs and their restrictions a	
🐣 App roles Preview	https://login.microsoftonline.com/common/oauth2/nativeclient	
🔁 Owners	https://login.live.com/oauth20_desktop.srf (LiveSDK)	
Roles and administrators Preview	msalcd1a4602-0ae7-4abf-962c-17adf5144159://auth (MSAL only)	
0 Manifest	pro.zentral.ident://auth	
Support + Troubleshooting	https://127.0.0.1/jamfconnect	
3 Troubleshooting	Add URI	
New support request		



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.

🛂 jamf 🛛 PRO	
USERNAME ex. admin	
PASSWORD	\bigcirc

- 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

C	Options Scope	
\$ \$	General	General
		Name Display name of the profile
P	Passcode Not configured	IDent Settings
		Description Brief explanation of the content or purpose of the profile
((10	Network Not configured	This contains the required settings for IDent
0	VPN	
	Not configured	Category Category to add the profile to
		Security
ø	Content Caching Not configured	Distribution Method Method to use for distributing the profile
		Install Automatically
	Certificate	
ር የነ	Not configured	Level Level at which to apply the profile

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

	Not configured	
6 —	Application & Custom	Configure Application & Custom Settings
	B≡ Identification Not configured	Use this section to configure settings for applications or define generic preferences.
	D Time Machine Not configured	Configure
	Sinder Not configured	



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

•	Application & Custom Settings
	Creation Method Method to use to define preferences in the specified preference domain
	Configure settings
Γ	Upload File (PLIST file)
	Preference Domain The name of a preference domain (com.company.application)
	[Required]
Г	Property List File PLIST file containing key value pairs for settings in the specified domain
L	Upload PLIST File

9. Click the Choose File button.

IST file conta	ining key value pai	rs for setting	s in the specified	l domain
Choose File	No File Chosen			

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.

Property List File

Choose File	pro zentral user-cert-config plist	
Choose The	protzentral.user-cert-coning.plist	



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

Application & Custom Settings	×	+			
Creation Method Method to use to define preferences in the specified preference domain					
Configure settings					
Upload File (PLIST file)					
Preference Domain The name of a preference domain (com.company.application)					
pro.zentral.user-cert-config					
Property List File PLIST file containing key value pairs for settings in the specified domain					
(AuthorityKe L=pro.zentral.ident://au GatewayURL=https://hcs-ident.macadmin.me/gw/config, ManagedSSIDs=(CORP-8021X, brguest), OIDCExtraScopes=(e -2, OIDCC -2, configuration, MinCertValidity=14d	ith, email, pro }	file],			

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.

•	Application & Custom Settings					
	Creation Method Method to use to define preferences in the specified preference domain					
	Configure settings Upload File (PLIST file)					
	Preference Domain The name of a preference domain (com.company.application)					
	[Required]					
	Property List File PLIST file containing key value pairs for settings in the specified domain Upload PLIST File					



- 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.

Property List File

	PLIST file conta	ining key value pairs for	settings in the specified	d domain	
14 —	Choose File	com.apple.notification	settings.plist		
		-			
			Cancel	Upload	15

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

~	Application & Custom Settings	× +					
	Creation Method Method to use to define preferences in the specified preference domain						
	Configure settings						
	Upload File (PLIST file)						
	Preference Domain The name of a preference domain (com.company.application) com.apple.notificationsettings						
	Property List File PLIST file containing key value pairs for settings in the specified domain Upload PLIST File						
	(NotificationSettings=[[ShowInNotificationCenter=true, AlertType=2, NotificationsEnabled=true, CriticalAlertEnabled=true, ShowInLockScreen=true, BadgesEnabled=true, SoundsEnabled=true, BundleIdentifier=pro.zentral.IDent), (ShowInNotificationCenter=true, AlertType=2, NotificationsEnabled=true, CriticalAlertEnabled=true, ShowInLockScreen=tru BadgesEnabled=true, SoundsEnabled=true, BundleIdentifier=pro.zentral.user-cert-config]])	ıe,					

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.

`	Application & Custom Settings						
	Creation Method Method to use to define preferences in the specified preference domain						
	Configure settings						
][Upload File (PLIST file)						
1	Preference Domain The name of a preference domain (com.company.application)						
	[Required]						
	Property List File PLIST file containing key value pairs for settings in the specified domain						
	Upload PLIST File						

19. Click the Choose File button.

Property List File	
LIST file containing key value pairs for setti Choose File No File Chosen	ngs in the specified domain

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.

Property List File
PLIST file containing key value pairs for settings in the specified domain Choose File com.jamf.connect.login.plist
Cancel



21. Scope to your needs.

Targets		Limitations	Exclusions
arget Computers		Target Users Users to distribute the profile to	
All Computers	*	Specific Users 🔹	

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.

Comp Con	^{outers} figuration Profiles					
\bigcirc	Q Filter Pr 1-1 of 1			[+ New Ĉ L	Upload
	NAME	LOGS	COMPLETED	PENDING	FAILED	SCOPE
•	No category assigned					
	Ident Settings	View	1	0	0	All computers



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

$\leftarrow \ \text{IDent SCEP Device Certificate}$

ô} ₄	General	General
		Name Display name of the profile
Э	Passcode Not configured	IDent SCEP Device Certificate
		Description Brief explanation of the content or purpose of the profile
llin	Network Not configured	IDent SCEP Device Certificate
÷	VPN	Category Category to add the profile to
	Not configured	Security -
3	Content Caching	Distribution Method Method to use for distributing the profile
	Not conligured	Install Automatically
<u>p</u>	Certificate Not configured	Level Level at which to apply the profile
		Computer Level 📌
2	Certificate Transparency Not configured	
_	SCEP	

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

Computers : Configuration Profiles ← New macOS Configuration Profile	
Options Scope	
® _e General	
Passcode Not configured	
Network Not configured	
VPN Not configured	
Content Caching Not configured	Generation Configure SCEP
GP Certificate Not configured	Use this section to define settings obtaining certificates from SCEP servers. Configure
Certificate Transparency Not configured	
SCEP Not configured	



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

N O

Ρ

Q R

s

S. Allow all apps access: Selected

URL	The base URL for the SCEP server
htt	ps://hcs-ident.macadmin.me/gw/scep/
Nam	e The name of the instance: CA-IDENT
СА	-IDENT
Redi Redi: \$PR	stribute Profile stribute the profile automatically when its SCEP-issued certificate is the specified number of days from expirin OFILE_IDENTIFIER* to the Subject field
Ne	ver 🔻
Subj	ect Representation of a X.500 name (e.g. "O=CompanyName, CN=Foo")
CN	I=%SerialNumber%
Subj	ect Alternative Name Type The type of a subject alternative name
No	ne v
-nal	neme type type of challenge password to use
Dy	
	URL To SCEP Admin URL of the page to use to retrieve the SCEP challenge
	https://hcs-ident.macadmin.me/gw/certsrv
	Username Username to use to log in to the SCEP Admin page
	IDent
	Password Password to use to log in to the SCEP Admin page
	•
	Verify Password
	- Number of Alexandra Ana PENDING services
etri	
Retry	Number of seconds to wait before each retry
0	Seconds
Certi	ficate Expiration Notification Threshold The number of days before the certificate expires at which to sta
14	•
(ey l	Size Key size in bits
20	48 🔻
	use as aigitai signature
<u>~</u>	Use for key encipherment
<u>~</u>	erprint Enter hex string to be used as a fingerprint or use button to create fingerprint from certificate
- ing	
ing	
-ing	Allow export from keychain Allow computer's administrators to export private key from the keychain
	Allow export from keychain Allow computer's administrators to export private key from the keychain Allow all apps access



28. Select Scope and scope to you needs

Targets	Limitations	Exclusions
rget Computers	Target Users Users to distribute the profile to	
All Computers	✓ Specific Users ✓	

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.

Jamf PRO		L 4 🔯
Computers Devices Users	All Settings	Computer Management
VERSION 10.25.0-b.1.t1600114893 MANAGED Computers: 1 Mobile Devices: 0 UNMANAGED	Image: System Settings Image: Set	Packages Scripts Printers Image: Configurations Disk Encryption Configurations Dock Items Configurations Pach Image: Configurations Pach Image: Configurations Image: Configurations
Computers: 0 Mobile Devices: 0	Server Infrastructure Network Organization Computer Management	Computer Management - Management Framework
Collapse Menu	Device Management	Inventory Inventory Check-In Security Extension Autorun Collection Display Check-In Security Extension Autorun Imaging Removable App Updates MAC Artdrossee

4. Select New.

Settings : Co ← Pack	omputer Management ages				
					+ New
NAME	^ CATEGORY	PRIORITY	FUT	FEU	INDEXED
No Packages					



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

Settings : Computer Management > Packages				
← New Package				
General Options Limitations				
Display Name Display name for the package				
[Required]				
Security				
Eilename Eilename of the package on the distribution point (e.g. "MyPackage.dmg") Choose File				

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.

	.kaye
General Op	ations Limitations
Display Name Disp	lay name for the package
IDent-1.0.pkg	
IDent-1.0.pkg Category Category	to add the package to
IDent-1.0.pkg Category Category Security	to add the package to
IDent-1.0.pkg Category Category Security Filename Filename	to add the package to for the package on the distribution point (e.g. "MyPackage.dmg")





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

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

	🖆 jamf PRO				<u></u>	
1—	Computers Devices Users	Computers Policies				
	INVENTORY	V Rilter Pc 1-1 of 1			+ New := 99	— 3
	Search Inventory	NAME	^ FREQUENCY	TRIGGER	SCOPE	
	CONTENT MANAGEMENT	 No category assigned 				
2 —	Policies Configuration Profiles	Update Inventory	Once every week	Check-in	All computers	
	 Restricted Software PreStage Imaging 					

- 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

General Ceneral Display Name Display Name Display Name Display Name O Packages Install IDent Client Software Updates Install IDent Client Nat Configured Image: Category Category to add the policy to Scripts Security Printers Trigger Printers Satup Orkingured Satup Disk Encryption Satup Nat Configured Using Dock Items Logoit Uccal Accounts Logoit When a user logs in to a computer. A login hook that checks for policies must be configured in Jamf Pro for this to work Dock Items Logoit When a user logs out of a computer. A login hook that checks for policies must be configured in Jamf Pro for this to work Dock Items Logoit When a user logs out of a computer. A login thook that checks for policies must be configured in Jamf Pro for this to work Directory Bindings Percolingued O Brackages Encollment Complete Immediately after a computer completes the enrollment process O Brackages Restant Queters O Brackages Execution Frequen	General Ceneral Display Name Display Name Display Name Display Name O Packages Install IDent Client Software Updates Category Not Configured Category Scripts Security O Printers Trigger Desk tencyption Startup Not Configured Category Dock tens Category Doback tens Category <	Options Scope Self	Service User Interaction
Display Name Display Name <td< th=""><th>Packages Display Name Display name for the policy Install Dent Client Install Dent Client Software Updates Image: Category Category to add the policy to Scripts Security O Printers Fridger Event(s) to use to initiate the policy Printers Disk Encryption Nat Configured Using Category to add the policy to add the policy to Disk Encryption Sarup When a computer starts up. A startup script that checks for policies must be configured in Jamf Pro for this to work Dock Items Logoit Obck Items User logs out of a computer. A login hook that checks for policies must be configured in Jamf Pro for this to work O Accounts Network State Change Management Network State Changes Accounts Enrollment Completer Directory Bindings Enrollment Completer Directory Bindings Recurning Check-in Act configured At the recurning check-in frequency configured in Jamf Pro Net Configured At a custom event Net Configured Escution Prequency Trequency at which to run the policy Order per computer The configured in Jamf Pro Directory Bindings Escution Prequ</th><th>General ></th><th>General</th></td<>	Packages Display Name Display name for the policy Install Dent Client Install Dent Client Software Updates Image: Category Category to add the policy to Scripts Security O Printers Fridger Event(s) to use to initiate the policy Printers Disk Encryption Nat Configured Using Category to add the policy to add the policy to Disk Encryption Sarup When a computer starts up. A startup script that checks for policies must be configured in Jamf Pro for this to work Dock Items Logoit Obck Items User logs out of a computer. A login hook that checks for policies must be configured in Jamf Pro for this to work O Accounts Network State Change Management Network State Changes Accounts Enrollment Completer Directory Bindings Enrollment Completer Directory Bindings Recurning Check-in Act configured At the recurning check-in frequency configured in Jamf Pro Net Configured At a custom event Net Configured Escution Prequency Trequency at which to run the policy Order per computer The configured in Jamf Pro Directory Bindings Escution Prequ	General >	General
Software Updates Image: Execution of the policy in thepolicy in thepolicy in the policy in the policy in the p	Software Updates Nat Configured Image: Category Loaded the policy to Scripts Scripts 0 Scripts Security ↓ Printers 0 Printers Trigger Event(s) to use to initiate the policy 0 Printers Disk Encryption Nat Configured Sartup When a computer starts up. A startup script that checks for policies must be configured in Jamf Pro for this to work Dock Items 0 Dock Items 0 Dock Items Sartup When a user logs in to a computer. A login hook that checks for policies must be configured in Jamf Pro for this to work Local Accounts 0 Accounts Network State Change When a user logs out of a computer. A logout hook that checks for policies must be configured in Jamf Pro for this to work Management Accounts 0 Catingured Network State Change When a computer's network state changes (e.g., when the network connection changes, when the computer name changes, when the IP address changes) Directory Bindings 0 Bindings Enrollment Complete Interdiately first a computer completes the enrollment process Prestart Options Net Configured Recurring Check-in A the recurring check-in frequency configured in Jamf Pro A ta c ustom event Restart Options Net Configured Execution Frequency Trequency at which to run the policy Once per computer Maintenance	Packages 0 Packages	Display Name Display name for the policy Install IDent Client
Act Collingued Category Category to add the policy to Scripts Security O Finters Trigger Event(s) to use to initiate the policy. O Finters Startup When a computer starts up. A startup script that checks for policies must be configured in Jamf Pro for this to work Disk Encryption Login Dock Items Login Used accounts Logout When a user logs in to a computer. A login hook that checks for policies must be configured in Jamf Pro for this to work Local Accounts Logout When a user logs out of a computer. A logout hook that checks for policies must be configured in Jamf Pro for this to work Management Accounts Network State Change When a computer's network state changes (e.g., when the network connection changes, when the computer name changes, when the IP address changes) Directory Bindings Errollment Complete Immediately after a computer completes the enrollment process Mat the recurring check-in frequency configured in Jamf Pro Net Configured At the recurring check-in frequency configured in Jamf Pro What a custom event Execution Frequency Frequency at which to run the policy	Category Category to add the policy to Scripts O Scripts O Printers O Printers O Printers Disk Encryption Not Configured Dock Items Difectory Bindings Difectory Bindings Difectory Bindings Difectory Bindings	Software Updates	✓ Enabled
Oscillus Trigger Event(s) to use to initiate the policy Of htmess Startup Of htmess Startup Disk Encryption Net Configured Login Dock Items O Dock Items Login Local Accounts O Accounts Logout When a user logs out of a computer. A login hook that checks for policies must be configured in Jamf Pro for this to work Local Accounts O Accounts Logout When a user logs out of a computer. A logout hook that checks for policies must be configured in Jamf Pro for this to work Management Accounts O Bindings Network State Change When a computer's network state changes (e.g., when the network connection changes, when the computer name changes, when the IP address changes) Errolsment Accounts O Bindings Errollment Complete Immediately after a computer completes the enrollment process Processord Net Configured At the recurring check-in frequency configured in Jamf Pro Custom At a custom event Restart Options Net Configured Execution Frequency Frequency	Outstage Trigger Printers Startup Disk Encryption Startup Net Configured Login Dock ttems Cugoni O Dock ttems Cugoni Disk Encryption Cugoni Disk tencyption Cugoni Disk tencyption Cugoni Dock ttems Cugoni Dock ttems Cugoni Dock ttems Cugoni Net configured Network State Change Management Network State Change Net Configured Enrollment Complete Immediately after a computer completes the enrollment process Recurring Check-in At the recurring check-in frequency configured in Jamf Pro Net Configured Recurring Check-in At a custom event At a custom event Restart Options Execution Frequency Trequency at which to run the policy Once per computer	Scripts	Category Category to add the policy to Security •
Disk Encryption When a computer starts up. A startup script that checks for policies must be configured in Jamf Pro for this to work Disk Encryption Usen a computer starts up. A startup script that checks for policies must be configured in Jamf Pro for this to work Dock Items Using Obox Items Network State Change Mena acomputer's network state changes (e.g., when the network connection changes, when the computer name changes, when the IP address changes) Directory Bindings Enrollment Complete Binangs Restart Options Restart Options Execution Frequency Restart Options Execution Frequency	Disk Encryption When a computer starts up. A startup script that checks for policies must be configured in Jamf Pro for this to work Dock Items Dock Items Directory Bindings Encolleated It after computer completes the enrollment process Directory Bindings Recurring Check-In At the recurring check-in frequency configured in Jamf Pro Matternamed At a custom event Restart Options Execution Frequency It whi	Printers 0 Printers	Trigger Event(s) to use to initiate the policy
Login Ucgin When a user logs in to a computer. A login hook that checks for policies must be configured in Jamf Pro for this to work Dock Items Logout Uccal Accounts Logout 0 Accounts Network State Change Management Accounts Nation Configured Network State Change (e.g., when the network connection changes, when the computer name changes, when the P address changes) Directory Bindings Enrollment Complete Immediately after a computer completes the enrollment process EFI Password Nat Configured At the recurring check-in frequency configured in Jamf Pro Nat configured Execution Frequency Frequency at which to run the policy	Login Login Dock Items Dock Items Obock Items Login I Dock Items Login I Local Accounts Mena user logs out of a computer. A logut hook that checks for policies must be configured in Jamf Pro for this to work Management Network State Change Nat Configured Performed acomputer's network state changes (e.g., when the network connection changes, when the computer name changes, when the IP address changes) Directory Bindings Enrollment Complete Directory Bindings Recurring Check-in At the recurring check-in frequency configured in Jamf Pro Act configured At a custom event Restart Options Execution Frequency Terguency at which to run the policy Once per computer Imagement Maintenance Maintenance	Disk Encryption Not Configured	When a computer starts up. A startup script that checks for policies must be configured in Jamf Pro for this to work
Local Accounts Logout Occounts When a user logs out of a computer. A logout hook that checks for policies must be configured in Jamf Pro for this to work Management Accounts Nat Configured Network State Change Directory Bindings Enrollment Complete Immediately after a computer completes the enrollment process Bindings Recurring Check-in frequency configured in Jamf Pro EFI Password Net Configured At the recurring check-in frequency configured in Jamf Pro Restart Options Execution Frequency Frequency at which to run the policy	Local Accounts Logout Understand O Accounts When a user logs out of a computer. A logout hook that checks for policies must be configured in Jamf Pro for this to work Management Accounts Not Configured Network State Change When a computer's network state changes (e.g., when the network connection changes, when the computer name changes, when the iP address changes) Directory Bindings Enrollment Complete Immediately after a computer completes the enrollment process O Bindings Q Recurring Check-in At the recurring check-in frequency configured in Jamf Pro Restart Options Net Configured Execution Frequency Frequency at which to run the policy Maintenance Maintenance Maintenance	Dock Items 0 Dock Items	Login Update a user logs in to a computer. A login hook that checks for policies must be configured in Jamf Pro for this to work
Management Accounts Nat Configured Network State Change When a computer's network state changes (e.g., when the network connection changes, when the computer name changes, when the IP address changes) Directory Bindings 0 Bindings Enrollment Complete Immediately after a computer completes the enrollment process EFI Password Net Configured Resurring Check-in At a custom event Restart Options Net Configured Execution Frequency Frequency	Management Accounts Not Configured When a computer's network state changes (e.g., when the network connection changes, when the computer name changes, when the Pladdress changes) Directory Bindings 0 Bindings Enrollment Complete Immediately after a computer completes the enrollment process V Recurring Check-in Net Configured At the recurring check-in frequency configured in Jamf Pro Custom Net Configured Custom Custom Net configured Restart Options Not Configured Execution Frequency Frequency at which to run the policy Once per computer Maintenance Maintenance	Local Accounts	Logout When a user logs out of a computer. A logout hook that checks for policies must be configured in Jamf Pro for this to work
Directory Bindings Enrollment Complete Directory Bindings Immediately after a computer completes the enrollment process 0 Bindings Recurring Check-in X the recurring check-in frequency configured in Jamf Pro Custom X the curring check-in frequency configured in Jamf Pro Custom Restart Options Execution Frequency Frequency at which to run the policy	Interconfigured Enrollment Complete Directory Bindings Enrollment Complete Disindings Recurring Check-in Immediately after a computer completes the enrollment process Recurring Check-in Immediately after a computer completes the enrollment process Recurring Check-in Immediately after a computer completes the enrollment process Immediately after a computer completes the enrollment process Immediately after a computer completes the enrollment process Immediately after a computer completes the enrollment process Immediately after a computer completes the enrollment process Immediately after a computer completes the enrollment process Immediately after a computer completes the enrollment process Immediately after a computer completes the enrollment process Immediately after a computer completes the enrollment process Immediately after a computer completes the enrollment process Immediately after a computer completes the enrollment process Immediately after a complete in the process Immediately after a computer completes the enrollment process Immediately after a complete in the process Immediately after a computer completes the enrollment process Immediately after a complete Immediately after a computer complete Immediately after a complete in the process Immediately after a complete in the process Immediately after a completely	Management Accounts	Network State Change When a computer's network state changes (e.g., when the network connection changes, when the computer name changes, when the IP address changes)
EFI Password Net Configured At the recurring Check-in frequency configured in Jamf Pro EFI Password Net Configured Custom At a custom event La custom event Restart Options Net Configured Execution Frequency Frequency at which to run the policy	EFI Password Not Configured Recurring Check-in frequency configured in Jamf Pro Execution Configured At the recurring check-in frequency configured in Jamf Pro Restart Options Net Configured La custom event Execution Frequency Frequency at which to run the policy Once per computer Maintenance Image: Configured	Directory Bindings	Enrollment Complete Immediately after a computer completes the enrollment process
Restart Options Execution Frequency at which to run the policy Restart Options Execution Frequency Frequency at which to run the policy	Costom event Costom event Execution Frequency Frequency at which to run the policy Once per computer Maintenance Costom Prequency Trequency at which to run the policy Once per computer Costom Prequency Trequency at which to run the policy Once per computer Costom Prequency Trequency at which to run the policy Costom Prequency Trequency at which to run the policy Costom Prequency Trequency at which to run the policy Costom Prequency Trequency at which to run the policy Costom Prequency Trequency Trequency at which to run the policy Costom Prequency Trequency Trequency at which to run the policy Costom Prequency Trequency Trequency Trequency At which to run the policy Costom Prequency Trequency Trequency Trequency At which to run the policy Costom Prequency Trequency Trequency At which to run the policy Costom Prequency Trequency Trequency At which to run the policy Costom Prequency Trequency At which to run the policy Costom Prequency Trequency At which to run the policy Costom Prequency Trequency At which to run the policy Costom Prequency Trequency At which to run the policy Costom Prequency Trequency At which to run the policy Costom Prequency Costom Prequency At which to run the policy Costom Prequency	EFI Password Not Configured	Recurring Check-in At the recurring check-in frequency configured in Jamf Pro
	Maintenance	Restart Options Not Configured	Execution Frequency Frequency at which to run the policy



- 5. Click Packages.
- 6. Click Configure.

Options Options Image: Constraint of the second	Scope Self Service User inter	Configure Packages	
 Packages 0 Packages Software Updates Not Configur 	>	😴 Configure Packages	
(Updates Not Configure		· · · · · · · · · · · · · · · · ·	
0 Scripts	d	Use this section to install, cache, and uninstall packages. Also use this section to install a single cached package.	
Printers 0 Printers		Configure	6

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

IDent-1.0.pkg	Security	Add

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

Packages	
Distribution Point Distribution point to download the package(s) from	
Each computer's default distribution point 🔹	
iDent-1.0.pkg	× +
Action Action to take on computers	
Install -	
Update Autorun data	
Add or remove the package from each computer's Autorun data	

- 9. Click Maintenance.
- 10. Click Configure.

B	Directory Bindings 0 Bindings			
	EFI Password Not Configured		X Configure Maintenance	
N N N N N N N N N N N N N N N N N N N	Restart Options Not Configured		Use this section to update inventory, reset computer names, install all cached packages,	
X	Maintenance Not Configured	>	and run common maintenance tasks.	



11. Select Update Inventory.

Mai	ntenance
~	Update Inventory Force computers to submit updated inventory information to Jamf Pro

Reset Computer Names
 Change the computer name on computers to match the computer name in Jamf Pro

Install Cached Packages Install packages cached by Jamf Pro

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

12	Computers : Policies ← Install IDent Client	User Interaction	
	Targets	Limitations	Exclusions
13—	Target Computers Computers to deploy the policy to All Computers	Target Users Users to deploy the policy to Specific Users	
	Selected Deployment Targets		+ Add
	TARGET	ТҮРЕ	
	No Targets		Cancel Save 1

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.

Microsoft
Sign in
 Email, phone, or Skype
No account? Create one!
Can't access your account?
Sign-in options
Terms of use Privacy & cookies · ·
Refresh Local Login
\bigcirc \bigcirc
Shut Down Restart

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.



(
Shut Down	Restart

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.

Z	"IDent" wants to use "microsoftonline.com" to sign in. This allows the app and website to share information about you.
	Cancel Continue



6. Enter your Microsoft Azure credentials then click Next.

Microsoft	
Sign in	
Email, phone, or Skype	† ~
No account? Create one!	
Can't access your account?	
Sign-in options	
	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.

ldP:

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.