



Pulse Policy Secure: Mobile Device Management

Integration Guide

Product Release	9.1R8
Published	August 2020
Document Version	1.0

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

© 2020 by Pulse Secure, LLC. All rights reserved.

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Pulse Policy Secure: Mobile Device Management

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at <http://www.pulsesecure.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

PURPOSE OF THIS GUIDE	1
MDM INTEROPERABILITY WITH PPS.....	3
OVERVIEW.....	3
SUPPORTED MDM SERVERS.....	4
MDM INTEGRATION WORK FLOW.....	4
MDM DICTIONARY ATTRIBUTES.....	4
CONFIGURING PPS WITH MDM SERVERS	11
CONFIGURING AN AUTHENTICATION PROTOCOL SET	12
CONFIGURING THE MDM AUTHENTICATION SERVER	12
CONFIGURING THE CERTIFICATE SERVER.....	15
ADDING THE MDM CERTIFICATE TO THE TRUSTED CLIENT CA CONFIGURATION.....	16
CONFIGURING USER ROLES.....	17
CONFIGURING A REALM AND ROLE MAPPING RULES	22
CONFIGURING A SIGN-IN POLICY.....	34
CONFIGURING PPS WITH PULSE WORKSPACE.....	35
CONFIGURING PPS WITH MICROSOFT INTUNE	37
CONFIGURING THE MICROSOFT INTUNE MDM.....	39
CONFIGURING THE PWS MDM	46
CONFIGURING THE AIRWATCH MDM	47
CONFIGURING THE MOBILEIRON MDM	52
TROUBLESHOOTING	54
USING THE DEBUG LOGS	55
GENERAL NOTES.....	56
DOCUMENTATION	56
TECHNICAL SUPPORT	56

Purpose of this Guide

This guide describes Mobile Device Management (MDM) interoperability with Pulse Policy Secure (PPS).

With this integration, the MDM acts as a device authorization server, and PPS uses the MDM record attributes as the basis for assigning role based policy.

Prerequisites

This guide assumes you are familiar with the use of the following products and their related terminology.

- *Pulse Work Space (PWS)*
- *AirWatch MDM Solution*
- *MobileIron MDM Solution*
- *Microsoft Intune*

MDM Interoperability with PPS

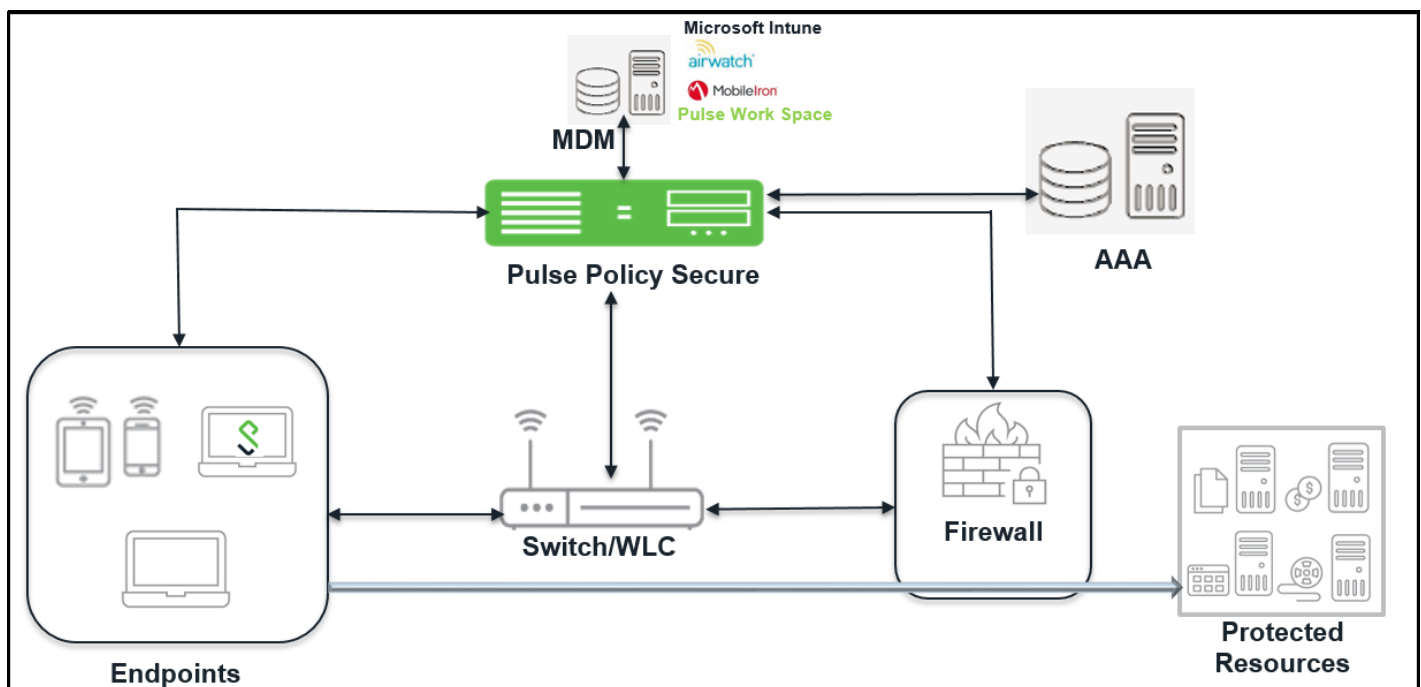
• Overview	3
• Configuring PPS with MDM Servers	11
• Configuring PPS with Pulse Workspace	35
• Configuring PPS with Microsoft Intune	37
• Configuring the Microsoft Intune MDM	39
• Configuring the PWS MDM	46
• Configuring the AirWatch MDM	47
• Configuring the MobileIron MDM	52
• Troubleshooting	54

Overview

Mobile Device Management (MDM) servers secure, monitor, manage, and support mobile devices deployed across mobile operators, service providers, and enterprises. MDM servers consist of a device authorization server that controls the use of some applications on a mobile device (for example, an e-mail application) in the deployed environment. The PPS queries the MDM servers for the necessary device attributes and evaluates them while assigning roles before giving access to the network.

For example, the MDM might detect that a device is out of compliance with PPS role mapping rules. At the next device check interval, PPS queries the MDM for updated attribute data. The compliance check is done periodically and if a formerly compliant device is now non-compliant, it assigns the device the non-compliant role and enforces the same on switch or firewall based on the PPS configuration.

Figure 1 MDM interoperability with PPS



Supported MDM Servers

Pulse Policy Secure(PPS) supports the following MDM servers:

- Pulse Workspace (PWS)
- AirWatch
- MobileIron
- Microsoft Intune

Pulse Policy Secure (PPS) determines the device identifiers using the following methods:

- Device Certificate
- MAC Address

Note: The dynamic policy evaluation feature is not used in the device access management framework.

The device-attribute-based roles are specified for the following policies:

- 802.1x network access control RADIUS return attribute policies (Layer 2)
- Infranet Enforcer resource policies (Layer 3)

MDM Integration Work Flow

The MDM integration work flow is described below:

1. The user associates a device to SSID.
2. (Optional) If the device is not registered, the user goes through the device on-boarding process.
3. Pulse Policy Secure(PPS) queries the MDM server with device details through MAC address or device attributes.
4. The MDM server returns device attributes with which PPS uses one or more attributes to determine device access.
5. Pulse Policy Secure(PPS) allows or denies access based on the attributes.

MDM Dictionary Attributes

This section focuses on the following elements of the MDM configuration that are important to this solution:

- Device identifier—The primary key for device records. Your MDM configuration determines whether a universal unique identifier (UUID), unique device identifier (UDID), or serial number is used as the device identifier.
For AirWatch, UDID is supported and recommended. For MobileIron, UUID is supported and recommended.
- Device attributes—A standard set of data maintained for each device. The device attributes for AirWatch, MobileIron, PWS, and Microsoft Intune are described below.

When the user installs the MDM application on the device and completes enrollment, the MDM pushes the device certificate to the device. After enrollment, the MDM maintains a database record that includes information about the enrollee—attributes related to device identity, user identity, and posture assessment against MDM policies.

Table 1 describes these attributes. In this solution, these attributes are used in PPS role mapping that is the basis for network access and resource access policies. When you configure role-mapping rules, you specify the normalized attribute name.

Table 1 AirWatch Device Attributes

AirWatch Attribute	Normalized Name	Description	Data Type
BlockLevelEncryption	BlockLevelEncryption	True if block-level encryption is enabled; false otherwise.	Boolean
ComplianceStatus	complianceReason	Values: Compliant, Non-Compliant.	String
ComplianceStatus	isCompliant	True if the status is compliant with MDM policies; false otherwise.	Boolean
CompromisedStatus	CompromisedStatus	True if the status is compromised; false otherwise.	Boolean
CompromisedStatus	isCompromised	True if the device is compromised; false otherwise.	Boolean
DataProtectionEnabled	DataProtectionEnabled	True if data protection is enabled; false otherwise.	Boolean
DeviceFriendlyName	deviceName	The concatenated name used to identify the device/ user combination.	String
EnrollmentStatus	isEnrolled	True if MDM value is Enrolled; false otherwise.	Boolean
FileLevelEncryption	FileLevelEncryption	True if file-level encryption is enabled; false otherwise.	Boolean
Id.Value	deviceId	Device identifier.	String
Imei	IMEI	IMEI number of the device.	String
IsPasscodeCompliant	IsPasscodeCompliant	True if the passcode is compliant with the MDM policy; false otherwise	Boolean
IsPasscodePresent	IsPasscodePresent	True if a passcode has been configured; false otherwise.	Boolean
LastComplianceCheckOn	LastComplianceCheckOn	The refresh date and timestamp of the last status reported.	Timestamp
LastCompromisedCheckOn	LastCompromisedCheckOn	The refresh date and timestamp of the last status reported.	Timestamp
LastSeen	lastSeen	Date and time the device last made successful contact with the MDM.	Timestamp
LocationGroupName	LocationGroupName	MDM location group configuration value.	String
MacAddress	macAdress	The Wi-Fi MAC address.	String
Model	model	Model is automatically reported by the device during registration.	String
OperatingSystem	osVersion	OS version.	String
Ownership	ownership	Values: C, E, or S (Corporate, Employee, or Shared).	String
PhoneNumber	phoneNumber	Phone number entered during registration.	String
Platform	platform	Platform specified during registration.	String
SerialNumber	serialNumber	Serial number.	String

AirWatch Attribute	Normalized Name	Description	Data Type
Udid	UDID	Unique device identifier.	String
UserEmailAddress	userEmail	E-mail address of device user.	String
UserName	userName	Name of device user.	String
Uuid	UUID	Universal unique identifier.	String

Table 2 MobileIron Device Attributes

MobileIron Attribute	Normalized Name	Description	Data Type
@id	deviceId	Device identifier.	String
blockedReason	blockedReason	Reason MDM has blocked the device. Can be a multivalued string. Values are: <ul style="list-style-type: none"> AllowedAppControlPolicyOutOfCompliance AppControlPolicyOutOfCompliance DataProtectionNotEnabled DeviceAdminDeactivated DeviceComplianceStatusUnknown DeviceCompliant DeviceCompromised DeviceExceedsPerMailboxLimit DeviceManuallyBlocked DeviceNotRegistered DisallowedAppControlPolicyOutOfCompliance ExchangeReported HardwareVersionNotAllowed OsVersionLessThanSupportedOsVersion PolicyOutOfDate RequiredAppControlPolicyOutOfCompliance 	String
compliance	complianceReason	MDM policy compliance status. Can be a multivalued string. Values are: <ul style="list-style-type: none"> AllowedAppControlPolicyOutOfCompliance AppControlPolicyOutOfCompliance DataProtectionNotEnabled DeviceAdminDeactivated DeviceComplianceStatusUnknown DeviceCompliant DeviceCompromised DeviceExceedsPerMailboxLimit DeviceManuallyBlocked DeviceNotRegistered DisallowedAppControlPolicyOutOfCompliance ExchangeReported HardwareVersionNotAllowed OsVersionLessThanSupportedOsVersion PolicyOutOfDate RequiredAppControlPolicyOutOfCompliance 	String
compliance	isCompliant	True if the device is in compliance with its MDM security policies; false otherwise.	Boolean
compliance	isCompromised	True if the device is compromised; false otherwise.	Boolean
countryName	countryName	Country name corresponding with the country code of the device.	String
currentPhoneNumber	phoneNumber	Phone number entered during registration.	String

MobileIron Attribute	Normalized Name	Description	Data Type
emailAddress	userEmail	E-mail address of device user.	String
employeeOwned	Ownership	Values: Employee or Corporate.	String
homeOperator	homeOperator	The service operator for the device when it is not roaming.	String
iPhone IMEI (iOS), imei (Android)	Imei	IMEI number of the device.	String
iPhone UDID	UDID	Unique device identifier.	String
isBlocked	isBlocked	True if the device is blocked from accessing the ActiveSync server; false otherwise.	Boolean
isQuarantined	isQuarantined	True if the device is quarantined by the MDN; false otherwise.	Boolean
lastConnectAt	lastSeen	Date and time the device last made successful contact with the MDM.	Timestamp
manufacturer	manufacturer	Manufacturer is automatically reported by the device during registration.	String
mdmManaged	mdmManaged	True if the MDM profile is enabled on the device; false otherwise. This field applies only to iOS devices. For other devices, the value is always false.	Boolean
ModelName, model, device_model	Model	Model is automatically reported by the device during registration.	String
name	deviceName	The concatenated name used to identify the device/user combination.	String
operator	Operator	Service provider. The value PDA indicates no operator is associated with the device.	String
OSVersion (iOS), os_version (Android)	osVersion	OS version.	String
platform	Platform	Platform specified during registration.	String
principal	userId	User ID.	String

MobileIron Attribute	Normalized Name	Description	Data Type
quarantinedReason	quarantinedReason	MDM policy compliance status. Can be a multivalued string. Values are: <ul style="list-style-type: none"> AllowedAppControlPolicyOutOfCompliance AppControlPolicyOutOfCompliance DataProtectionNotEnabled DeviceAdminDeactivated DeviceComplianceStatusUnknown DeviceCompliant DeviceCompromised DeviceExceedsPerMailboxLimit DeviceManuallyBlocked DeviceNotRegistered DisallowedAppControlPolicyOutOfCompliance ExchangeReported HardwareVersionNotAllowed OsVersionLessThanSupportedOsVersion PolicyOutOfDate RequiredAppControlPolicyOutOfCompliance 	
SerialNumber	serialNumber	Serial number.	String
statusCode	isEnrolled	True if the device has completed enrollment or registration; false otherwise.	Boolean
uuid	UUID	Universal unique device identifier.	String
userDisplayName	userName	Name of device user.	String
wifi_mac (iOS), wifi_mac_addr (Android)	macAdress	The Wi-Fi MAC address.	String

Table 3 Microsoft Intune Device Attributes

Intune Attribute	Normalized Name	Description	Data Type
complianceState	isCompliant	True or false (string) based on whether device is compliant or non-compliant.	Boolean
isManaged	isEnrolled	True or false (indicating whether the client is managed by Intune or not).	Boolean
macAddress	macAddress	MAC address of the device.	String
serialNumber	serialNumber	Serial number of the device. Applies to iOS Devices only.	String
imei	IMEI	The device unique identifier. IMEI (15 decimal digits: 14 digits plus a check digit) or IMEISV (16 digits) includes information on the origin, model, and serial number of the device.	String
udid	UDID	The device unique identifier. Unique Device Identifier (UDID), which is a sequence of 40 letters and numbers that is specific to iOS devices.	String
meid	MEID	MEID is 56 bits long (14 hex digits). It consists of three fields, including an 8-bit regional code (RR), a 24-bit manufacturer code, and a 24-bit manufacturer-assigned serial number.	String
osVersion	osVersion	OS Version of the device.	String
model	Model	Model of the device.	String
manufacturer	manufacturer	Device Manufacturer.	String
azureDeviceId	deviceId	The device Id of the device after it has work place joined with Azure Active Directory.	String
lastContactTime Utc	lastSeen	The date time when the device last checked in with the Intune management service endpoint.	String The format is MM/DD/YYYY HH:MM:SS

Refer to third-party documentation for complete information and configuration details.

Configuring PPS with MDM Servers

This section describes the basic steps for configuring the device access management framework:

- [“Configuring an Authentication Protocol Set” on page 12](#)
- [“Configuring the MDM Authentication Server” on page 12](#)
- [“Configuring the Certificate Server” on page 15](#)
- [“Adding the MDM Certificate to the Trusted Client CA Configuration” on page 16](#)

- [“Configuring User Roles” on page 17](#)
- [“Configuring a Realm and Role Mapping Rules” on page 22](#)
- [“Configuring a Sign-In Policy” on page 34](#)

Configuring an Authentication Protocol Set

The authentication protocol set associated with the sign-in page must include the EAP method selected in the MDM Wi-Fi profile. The predefined authentication protocol set named 802.1x can be used as-is because it includes all the EAP methods currently configurable on MDMs.

To configure the authentication protocol set:

1. Select **Signing In > Authentication Protocols** to display the configuration page.
2. Click **New Authentication Protocol** or select the predefined 802.1x set. If anything other than MAC address is used as a device identifier then you must use cert auth and the protocol set has to be used for cert auth.
3. Click **Save**.

Configuring the MDM Authentication Server

The MDM authentication server configuration is used by PPS to communicate with the MDM. In the device access management framework, the MDM server is used as the device authorization server.

To configure the authentication server:

1. Select **Authentication > Auth Servers** to navigate to the authentication server configuration pages.
2. Select **MDM Server** and click **New Server** to display the configuration page.
3. Complete the configuration as described in Table below.
4. Save the configuration.

Figure 2 Authentication Server Configuration Page

Pulse Secure System **Authentication** Administrators Users Maintenance Wizards

Auth Servers > AirWatchMDM

AirWatchMDM

Settings

*Name: Label to reference this server.

Type: Air Watch

▼ **Server**

* Server Url:

Viewer Url: Link to device details page
For example: https://cn11.airwatchportals.com/AirWatch/Devices/DeviceDetails/<deviceAttr.deviceId>

* Request Timeout: seconds

▼ **Administrator**

* Username:

* Password:

* Tenant Code:

Test Connection

▼ **Device Identifier**

Please check the options on the Users > Authentication > [Realm] > Authentication Policy > Certificate page. For example, enable "Allow all users and remember certificate from the client."

ID Template: Template for constructing device identifier from certificate

The template can contain textual characters as well as variables for substitution. Variables should be enclosed in angle brackets like this <variable>. To use custom expressions and policy conditions. All of the certificate variables are available.

Examples:

- <certDN.CN> First CN from the subject DN
- <certAttr.serialNumber> Certificate serial number
- <certAttr.name.xxx> Where xxx can be:
 - Email The Email alternate name
 - UPN The Principal Name alternate name
 - ... etc
- <certDNText> The complete subject DN
- cert-<certDN.CN> The text "cert-" followed by the first CN from the subject DN

ID Type:

- ☐ UUID Universal Unique Identifier
- ☐ Serial Number
- ☒ UDID Unique Device Identifier

Save Changes **Reset**

Table 4 Authentication Server Configuration Guidelines

Settings	Guidelines
Name	Specify a name for the configuration.
Type	Select the MDM server.
Server	
Server Url	<p>Specify the URL for your AirWatch server. This is the URL AirWatch has instructed you to use to access its RESTful Web API (also called a RESTful Web service). The URL for the AirWatch MDM server used in this example has the following form:</p> <p>https://apidev-as.Awmmdm.com</p> <p>https://m.mobileiron.net/pulsesecuretest</p> <p>Note: You must configure your firewalls to allow communication between these two nodes over port 443.</p>
Viewer Url	<p>Specify the URL for the AirWatch report viewer. This URL is used for links from the Active Users page to the AirWatch report viewer. The URL for the AirWatch MDM viewer for this example has the following form:</p> <p><a href="https://apidev.awmmdm.com/AirWatch/Devices/DeviceDetails/<deviceAttr.deviceId>">https://apidev.awmmdm.com/AirWatch/Devices/DeviceDetails/<deviceAttr.deviceId></p> <p>https://m.mobileiron.net/pulsesecuretest/admin/admin.html#smartphones:all</p>
Request Timeout	<p>Specify a timeout period (0-60 seconds) for queries to the MDM server. The default is 15 seconds. Calibrate this value based on your observations on how long a query to the MDM server takes over your network. If your network experiences latency when querying the MDM cloud service, increase the timeout to account for the latency. The system queries the MDM when a user attempts to sign in. If a timeout occurs, role mapping proceeds without attributes.</p>
Administrator	
Username	Specify the username for an account that has privileges to access the MDM RESTful Web API.
Password	Specify the corresponding password.
Tenant Code	Copy and paste the AirWatch API tenant code.
Device Identifier	

Settings	Guidelines
Device identity	<p>Select an option on whether to require that the MDM certificate is presented by the endpoint when signing in:</p> <ul style="list-style-type: none"> • Require—Require that the device certificate pushed to client devices during enrollment be used at sign-in. If this option is selected, and the client device does not have a certificate, authorization fails. Use this option when you require endpoints to adhere to your certificate security requirements. • Use Certificate if present—Use the certificate to derive the device ID if the certificate is presented at sign-in, but do not reject authentication if the certificate is not present. You can use this option in conjunction with a role mapping rule and a remediation VLAN to identify devices that have not perfected MDM enrollment. • Always Use MAC address—In some cases, the MDM certificate might be configured without a device identifier. When the endpoint uses an 802.1x framework to authenticate, PPS can obtain the MAC address from the RADIUS return attribute callingStationID. The system can then use the MAC address as the device identifier.
ID Template	<p>Construct a template to derive the device identifier from the certificate attributes. The template can contain textual characters as well as variables for substitution. The variables are the same as those used in role mapping custom expressions and policy conditions. Enclose variables in angle brackets like this <variable>.</p> <p>For example, suppose the certificate DN is: CN=<EnrollmentUser>, serialNumber=<DeviceUid>, o=Company. With this configuration, the certificate could identify both the user and the device. In this example, the device ID template is <certDN.serialNumber>.</p>
ID Type	<p>Select the device identifier type that matches the selection in the MDM certificate configuration:</p> <ul style="list-style-type: none"> • UUID—The device universal unique identifier. This is the key device identifier supported by MobileIron MDM. • Serial Number—The device serial number. • UDID—The device unique device identifier. This is supported by the AirWatch MDM.


Configuring the Certificate Server

The certificate server configuration enables device users to authenticate using the certificate pushed to the device by the MDM. The certificates are used for user authentication, and the users do not have to enter user credentials.

To configure authentication with the certificate server:

1. Select **Authentication > Auth. Servers**.
2. Select **Certificate Server** and click **New Server** to display the configuration page.
3. Complete the configuration as described in table below.
4. Save the configuration.

Figure 3 Certificate Server Configuration Page



Pulse Secure

System Authentication

Auth Servers > New Certificate Server

New Certificate Server

*Name:

AirWatchCert

Label to r

User Name Template:

<certDN.CN>

Template

The template can contain textual characters as well as variables for custom expressions and policy conditions. All of the certificate variables are listed below.

Examples:

<certDN.CN>

First CN from the subject DN

<certAttr.serialNumber>

Certificate serial number

<certAttr.altName.xxx>

Where xxx can be:

Email

The Email alternate name

UPN

The Principal Name alternate name

...

etc

<certDNText>

The complete subject DN

cert-<certDN.CN>

The text "cert-" followed by the first CN from the subject DN

▼ User Record Synchronization

☐ Enable User Record Synchronization

Logical Auth Server Name:

Save Changes

Reset

* indicates required field

Table 5 Certificate Server Settings

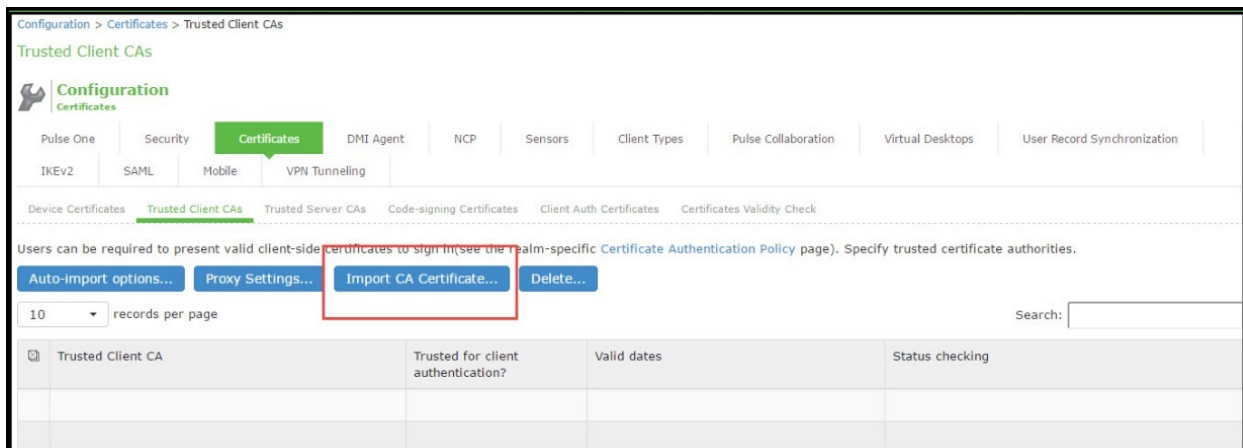
Settings	Guidelines
Name	Specify a name to identify the server within the system.
User Name Template	<p>Specify a username template. Specify how the system should construct a username. You may use any combination of certificate variables contained in angle brackets and plain text. The username template you configure must be consistent with the MDM certificate template configuration. Your goal is to identify the values specified in the MDM certificate that are to be used as the username in PPS system. This value populates the <USER> and <USERNAME> session variables for use throughout the rest of the system configuration.</p> <p>For example, suppose the certificate DN is: CN=<EnrollmentUser>, serialNumber=<DeviceUid>, o=Company. With this configuration, the certificate could identify both the user and the device. In this example, the username template is <certDN.CN>.</p>

Adding the MDM Certificate to the Trusted Client CA Configuration

The system uses the uploaded certificate to verify that the browser-submitted certificate is valid. You must upload the MDM certificate that signed the client certificate that was pushed to the mobile devices. Typically, you obtain this certificate from the MDM when your company establishes its account with them.

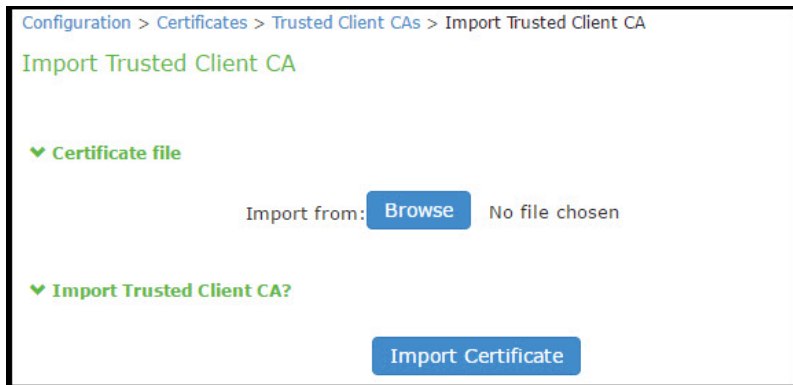
To import a trusted client CA certificate:

1. Select **System > Configuration > Certificates > Trusted Client CAs**.



2. Click **Import Trusted Client CA Certificate**.

Figure 4 Import Trusted Client CA Page



3. Browse to the certificate file, select it, and click **Import Certificate** to complete the import operation.
4. Click the link for the Trusted Client CA to display its details.

Configuring User Roles

User roles are classifiers for network access control policies. You create a set of roles to use in your classification scheme: device status is MDM enrollment complete or incomplete; device status is MDM-policy compliant or noncompliant; device is employee owned or company owned; device platform is iOS, Android, or neither; and so forth.

The user role configuration also includes options to customize user interface features that are appropriate for a particular role. For MDM deployments, you can use the Personalized Greeting UI option to send a notification message to the device when the role has been applied.

To configure user roles:

1. Select **Users > User Role** to navigate to the role configuration page.
2. Click **New Role** to display the configuration page.

3. Complete the configuration for general options as described in below table.
4. Save the configuration.
5. Click **UI options** to display the configuration page.
6. Complete the configuration for UI options as described in below table.
7. Save the configuration.
8. Click **Session Options** to display the configuration page.
9. Complete the configuration for session options as described in below table.
10. Save the configuration.
11. Click **Agentless** to display the configuration page.
12. Complete the configuration for agentless options as described in below table.
13. Save the configuration.

Figure 5 User Role Configuration Page – General Settings

Pulse Secure System Authentication Administrators **Users** Maintenance Wizards

User Roles > New Role

New Role

Name:

Description:

Options

Session and appearance options are specified in [Default Options](#). Check the following if this role should override these defaults.

- ☐ VLAN/Source IP
- ☒ Session Options
- ☒ UI Options
- ☐ Pulse Secure client Dynamically deliver Pulse Secure client to Windows and MAC OSX users

Access Features

Check the features to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user.

- ☐ Web
- ☐ Files, Windows
- ☐ Files, UNIX/NFS
- ☐ Telnet/SSH
- ☐ Email Client
- ☐ Secure Application Manager
 - ☐ Windows version Note: On Windows Mobile, Pulse Secure client is delivered via WSAM
 - ☐ Java version
- ☐ Terminal Services
- ☐ Virtual Desktops
- ☐ HTML5 Access
- ☐ Meetings
- ☐ VPN Tunneling (includes IKEv2)

Enterprise Device Onboarding

Check the Enterprise Device Onboard profiles to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user.

- ☐ Secure Mail
- ☐ Enterprise Onboarding (VPN, Wifi and Certificate Profiles)

Save Changes

Figure 6 User Role Configuration Page – UI Options

Pulse Secure System Authentication Administrators **Users** Maintenance Wizards Pulse Connect Secure

User Roles > Compromised > General > UI Options

UI Options

General Web Files SAM Telnet/SSH Terminal Services Virtual Desktops HTML5 Access Meetings VPN Tunneling

Enterprise Onboarding

Overview Restrictions VLAN/Source IP Session Options **UI Options**

[Save Changes](#) [Restore Factory Defaults](#)

Header

Current appearance:

Logo image: [Browse](#) No file chosen Recommended size: Less than 40 pixels tall and 10KB.

Background color: #E3E3E3 [Select from palette or type hexadecimal RGB](#)

Sub headers

Current appearance:

Background color: #336699 [Select from palette or type hexadecimal RGB](#)

Text color: #FFFFFF [Select from palette or type hexadecimal RGB](#)

Start page

The start page determines where a user starts after signing in.

☒ Bookmarks page

Welcome message:

Portal Name:

☐ Meetings page

☐ Custom page

Start page URL: Example: <http://www.domain.com/>

☐ Also allow access to directories below this url

Bookmarks Panel Arrangement

Determine the location and order of panels on the the user's bookmarks page. Note that all panels may not be displayed.

Left Column	Right Column
<div>Move Up</div> <div>Welcome</div> <div>Move Down</div>	<div>Move Up</div> <div>HTML5 Access Sess</div> <div>Move Down</div>
<div>Web Bookmarks</div> <div>Files</div> <div>Terminal Sessions</div> <div>Client Application S</div> <div>Virtual Desktops</div>	<div>< Move</div>

Help Page

☐ Disable help link

☒ Standard help page

☐ Custom help page

Help page URL: Example: <http://www.domain.com/help>

☐ Also allow access to directories below this url

Window size: width height

User Toolbar

Determine the tools that are available to users at the top of the secure gateway pages on the IVE.

☒ Home

☒ Preferences

☐ Session Counter

☐ Client Application Sessions

If this is not displayed on the toolbar, it will be displayed as a panel on the user's home page.

Browsing toolbar

Determine the tools that are available to users when browsing pages not located on the IVE, such as external web sites.

☒ Show the browsing toolbar

Toolbar type: ☒ Standard ☐ Framed

Toolbar logo: [Browse](#) No file chosen Recommended size: Less than 24 pixels tall and 6KB.

Toolbar logo (mobile): [Browse](#) No file chosen Recommended size: Less than 12 pixels tall and 3KB.

Logo links to:

☐ Bookmarks page

☒ "Start Page" settings

☐ Custom URL: An access control rule will be created for this url.

☐ Also allow access to directories below this url

☐ Enable "Home" link

☒ Enable "Add Bookmark" link

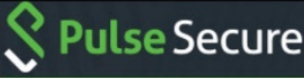
☒ Enable "Bookmark Favorites" link

☐ Display Session Counter

☒ Enable "Help" link

☐ Use Iframe in Toolbar

Figure 7 User Role Configuration Page – Session Options



SystemAuthenticationAdministrators**Users**MaintenanceWizards

Pulse Connect Secure

User Roles > Compromised > General > Session Options

Session Options

GeneralWebFilesSAMTelnet/SSHTerminal ServicesVirtual DesktopsHTML5 AccessMeetingsVPN Tunneling

Enterprise Onboarding

OverviewRestrictionsVLAN/Source IP**Session Options**UI Options

Save Changes

Session lifetime

* Idle Timeout:

minutes

(min: 5)

* Max. Session Length:

minutes

(min: 6)

* Reminder Time:

minutes

(min: 3)

☐ Use Session/Idle timeout values sent by the primary Radius authentication Server

☐ Enable Session Extension

Allow User to Extend Existing Session

Note: VPN Tunnel, SAM or Terminal services require a difference of 10 or greater between Idle Timeout and Reminder Time.

Table 6 User Role Configuration Guidelines

Settings	Guidelines
Overview tab	
Name	Specify a name for the configuration.
Description	Describe the purpose of the role so that other administrators are aware of it.
Options	Select UI Options so that you can customize a message to be sent to the device when the role is applied.
UI Options tab	
Personalized greeting	<p>Select the Show notification message option and enter a message to be sent to the device (through the MDM API) after sign-in and this role has been applied, or after role reevaluation if it results in a role change to this role.</p> <p>In this example, we are using the system to enforce MDM enrollment by flagging compromised devices. The message, therefore, is:</p> <p>Your device is compromised. Network access may be limited.</p> <p>The message is forwarded to the device using the MDM server Push Notification feature.</p> <p>The content of your notification message can vary depending on whether the switch or access point supports change of authorization (CoA). If the CoA is supported, reauthentication is automatic, so your message might simply state that "your level of access has changed." If CoA is not supported, reauthentication needs to be done manually by the user in which case the message might state that "your level of access has changed, please reconnect."</p> <p>NOTE: When multiple roles are assigned, UI options are not merged. The UI options for the first role that matches are applied.</p>
Session Options	
Allow VPN Through Firewall	Enable this option to allow Intranet Enforcer traffic to act as a heartbeat and keep the session alive. This option is useful for iOS devices.
Agentless	
Enable agentless access	Select this option for roles that you provision to access the network from BYOD devices. The solution that integrates with MDMs depends on the native supplicant, not a Pulse Secure agent.

Configuring a Realm and Role Mapping Rules

The user realm configuration associates the authentication server data and MDM server data with user roles.

To configure the realm and role mapping rules:


1. Select **Users > User Realms > New User Realm** to display the configuration page.
2. Upon saving the new realm, the system displays the role mapping rules page.
3. Click **New Rule** to display the configuration page.
4. Complete the configuration as described in table.

5. Click the **Authentication Policy** tab and then click the **Certificate subtab** to display the certificate restriction configuration page.

Table 7 Realm Configuration Guidelines

Settings	Guidelines
Name	Specify a name for the realm. If you enable sign-in using a realm suffix in the sign-in policy configuration, the realm name must match the username realm suffix configured in the MDN Wi-Fi profile.
Description	Describe the purpose of the realm so that other administrators are aware of it.
Servers	
Authentication	Select the user authentication server for this realm's users. This example uses the certificate server configured in the earlier step. When you use a certificate server, users are not prompted for their credentials. You can also select the authentication server used for employees. In that case, users are prompted by the sign-in page to provide their username and password.
User Directory/Attribute	This option is not used.
Accounting	This option is not used.
Device Attributes	Select the MDM server configured for device authorization.
Device Check Interval	Select this feature to leverage the MDM posture assessment checks and enforce compliance. For example, the MDM might detect that a device is out of compliance with its security policies, such as a password policy. At the next device check interval, PPS queries the MDM for updated attribute data. In this example, it learns that a formerly compliant device is now noncompliant. It assigns the device the noncompliant role and sends the 802.1x authenticator the corresponding RADIUS attribute to place it in a remediation VLAN. Specify the interval at which to query the MDM for updated attribute data. Specify 0 to disable periodic queries. The minimum is 10 minutes and the maximum is 10080 minutes (7 days). Specify an interval that is appropriate for the MDM. Some MDMs, for example, update records every 4 hours, so a 10-minute interval would not be productive.
Dynamic Policy Evaluation	
Dynamic Policy Evaluation	This option is not used.

Figure 8 Role Mapping Configuration Page

 **Pulse Secure**

SystemAuthenticationAdministrators**Users**Maintenance

User Realms > All Roles Realm - NC Client > Role Mapping > Role Mapping Rule

Role Mapping Rule

* Name:

▼ Rule:if username...

is

*

If more than one username should match, enter one username per line. You can use * wildcards.

▼ then assign these roles

Available Roles:

AAA QA Role

Client QA Role

Core QA Role

Default QA VLAN Role

JSAM Role

Add ->

Remove

Selected Roles:

Terminal Services Role

Web Role

STA Role

WSAM Role

HTML5 Role

☐ Stop processing rules when this rule matches

To manage roles, see the [Roles](#) configuration page.

Save Changes

Save as Copy

Table 8 Role Mapping Configuration Guidelines

Settings	Guidelines
Rule based on	Select Device Attribute and click Update to update the configuration page so that it displays settings for role mapping using device attributes.
Name	Specify a name for the configuration.
Rule	Select a device attribute and a logical operator (is or is not), and type a matching value or value pattern. In this example, select isCompromised and the logical operator is, and enter the value 1 (true). This means that devices with a compromised status match the rule.
Role assignment	Select the roles to apply if the data matches the rule.

Table 9 describes the AirWatch record attributes that can be used in role mapping rules.

Table 9 AirWatch Device Attributes

Role Mapping Attribute Name	AirWatch Attribute Name	Description	Data Type
BlockLevelEncryption	BlockLevelEncryption	True if block-level encryption is enabled; false otherwise.	Boolean
complianceReason	ComplianceStatus	Values: Compliant, Non-Compliant.	String
CompromisedStatus	CompromisedStatus	True if the status is compromised; false otherwise.	Boolean
DataProtectionEnabled	DataProtectionEnabled	True if data protection is enabled; false otherwise.	Boolean
deviceId	Id.Value	Device identifier.	String
deviceName	DeviceFriendlyName	The concatenated name used to identify the device/user combination.	String
FileLevelEncryption	FileLevelEncryption	True if file-level encryption is enabled; false otherwise.	Boolean
IMEI	Imei	IMEI number of the device.	String
isCompliant	ComplianceStatus	Values: Compliant.	String
isCompromised	CompromisedStatus	True if the device is compromised; false otherwise.	Boolean
isEnrolled	EnrollmentStatus	True if MDM value is Enrolled; false otherwise.	Boolean
IsPasscodeCompliant	IsPasscodeCompliant	True if the passcode is compliant with the MDM policy; false otherwise	Boolean
IsPasscodePresent	IsPasscodePresent	True if a passcode has been configured; false otherwise.	Boolean
LastComplianceCheckOn	LastComplianceCheckOn	The refresh date and timestamp of the last status reported.	Timestamp
LastCompromisedCheckOn	LastCompromisedCheckOn	The refresh date and timestamp of the last status reported.	Timestamp
lastSeen	LastSeen	Date and time the device last made successful contact with the MDM.	Timestamp
LocationGroupName	LocationGroupName	MDM location group configuration value.	String
macAdress	MacAddress	The Wi-Fi MAC address.	String
model	Model	Model is automatically reported by the device during registration.	String
osVersion	OperatingSystem	OS version.	String
ownership	Ownership	Values: C, E, or S (Corporate, Employee, or Shared).	String
phoneNumber	PhoneNumber	Phone number entered during registration.	String
platform	Platform	Platform specified during registration.	String

Role Mapping Attribute Name	AirWatch Attribute Name	Description	Data Type
serialNumber	SerialNumber	Serial number.	String
UDID	Udid	Unique device identifier.	String
userEmail	UserEmailAddress	E-mail address of device user.	String
userName	UserName	Name of device user.	String
UUID	Uuid	Universal unique identifier.	String

Table 10 describes the MobileIron record attributes that can be used in role mapping rules.

Table 10 MobileIron Device Attributes

Role Mapping Attribute Name	MobileIron Attribute Name	Description	Data Type
blockedReason	blockedReason	Reason MDM has blocked the device. Can be a multivalued string. Values are: <ul style="list-style-type: none"> AllowedAppControlPolicyOutOfCompliance AppControlPolicyOutOfCompliance DataProtectionNotEnabled DeviceAdminDeactivated DeviceComplianceStatusUnknown DeviceCompliant DeviceCompromised DeviceExceedsPerMailboxLimit DeviceManuallyBlocked DeviceNotRegistered DisallowedAppControlPolicyOutOfCompliance ExchangeReported HardwareVersionNotAllowed OsVersionLessThanSupportedOsVersion PolicyOutOfDate RequiredAppControlPolicyOutOfCompliance 	String
complianceReason	compliance	MDM policy compliance status. Can be a multivalued string. Values are: <ul style="list-style-type: none"> AllowedAppControlPolicyOutOfCompliance AppControlPolicyOutOfCompliance DataProtectionNotEnabled DeviceAdminDeactivated DeviceComplianceStatusUnknown DeviceCompliant DeviceCompromised DeviceExceedsPerMailboxLimit DeviceManuallyBlocked DeviceNotRegistered DisallowedAppControlPolicyOutOfCompliance ExchangeReported HardwareVersionNotAllowed OsVersionLessThanSupportedOsVersion PolicyOutOfDate RequiredAppControlPolicyOutOfCompliance 	String
countryName	countryName	Country name corresponding with the country code of the device.	String
deviceId	@id	Device identifier.	String
deviceName	name	The concatenated name used to identify the device/user combination.	String
homeOperator	homeOperator	The service operator for the device when it is not roaming.	String
Imei	iPhone IMEI (iOS), imei (Android)	IMEI number of the device.	String

Role Mapping Attribute Name	MobileIron Attribute Name	Description	Data Type
isBlocked	isBlocked	True if the device is blocked from accessing the ActiveSync server; false otherwise.	Boolean
isCompliant	compliance	True if the device is in compliance with its MDM security policies; false otherwise.	Boolean
isCompromised	compliance	True if the device is compromised; false otherwise.	Boolean
isEnrolled	statusCode	True if the device has completed enrollment or registration; false otherwise.	Boolean
isQuarantined	isQuarantined	True if the device is quarantined by the MDM; false otherwise.	Boolean
lastSeen	lastConnectAt	Date and time the device last made successful contact with the MDM.	Timestamp
manufacturer	manufacturer	Manufacturer is automatically reported by the device during registration.	String
macAddress	wifi_mac (iOS), wifi_mac_addr (Android)	The Wi-Fi MAC address.	String
mdmManaged	mdmManaged	True if the MDM profile is enabled on the device; false otherwise. This field applies only to iOS devices. For other devices, the value is always false.	Boolean
model	ModelName, model, device_model	Model is automatically reported by the device during registration.	String
operator	operator	Service provider. The value PDA indicates no operator is associated with the device.	String
osVersion	OSVersion (iOS), os_version (Android)	OS version.	String
ownership	employeeOwned	Values: Employee or Corporate.	String
phoneNumber	currentPhoneNumber	Phone number entered during registration.	String
platform	platform	Platform specified during registration.	String

Role Mapping Attribute Name	MobileIron Attribute Name	Description	Data Type
quarantinedReason	quarantinedReason	MDM policy compliance status. Can be a multivalued string. Values are: <ul style="list-style-type: none"> AllowedAppControlPolicyOutOfCompliance AppControlPolicyOutOfCompliance DataProtectionNotEnabled DeviceAdminDeactivated DeviceComplianceStatusUnknown DeviceCompliant DeviceCompromised DeviceExceedsPerMailboxLimit DeviceManuallyBlocked DeviceNotRegistered DisallowedAppControlPolicyOutOfCompliance ExchangeReported HardwareVersionNotAllowed OsVersionLessThanSupportedOsVersion PolicyOutOfDate RequiredAppControlPolicyOutOfCompliance 	
serialNumber	SerialNumber	Serial number.	String
UDID	iPhone UDID	Unique device identifier.	String
userEmail	emailAddress	E-mail address of device user.	String
userId	principal	User ID.	String
userName	userDisplayName	Name of device user.	String
UUID	uuid	Universal unique device identifier.	String

Table 11 PWS Device Attributes

Role Mapping Attribute Name	PWS Attribute Name	Description	Data Type
osVersion	os_version	OS version	String
UUID	uuid	Unique device identifier	String
IMEI	imei	IMEI number of the device.	String
macAddress	wifi_mac	The Wi-Fi MAC address.	String
serialNumber	serial_number	Serial number of the device.	String
lastSeen	last_seen	Date and time the device last made successful contact with the MDM.	Time Stamp
isCompliant isCompromised complianceReason	is_compliant	True if the device is in compliance with its MDM security policies; false otherwise.	Boolean
isEnrolled	state	True or false (indicating whether the client is managed by PWS or not).	Boolean
UDID	ios_udid	The device unique identifier. Unique Device Identifier (UDID), which is a sequence of 40 letters and numbers that is specific to iOS devices.	String
model	model	Model of the device.	String
phoneNumber	PhoneNumber	Phone number entered during registration.	String
userName	username	Name of device user.	String
carrier	carrier	User ID.	String
manufacturer	manufacturer	Device manufacturer name.	String
deviceName	devicename	Name of the device.	String

Table 12 Microsoft Intune Device Attributes

Role Mapping Attribute Name	Microsoft Intune Attribute Name	Description	Data Type
deviceId	azureDeviceId	The device Id of the device after it has work place joined with Azure Active Directory.	String
IMEI	imei	The device unique identifier. IMEI (15 decimal digits: 14 digits plus a check digit) or IMEISV (16 digits) includes information on the origin, model, and serial number of the device.	String
isCompliant	complianceState	True or false (string) based on whether device is compliant or non-compliant.	Boolean
isEnrolled	isManaged	True or false (indicating whether the client is managed by Intune or not).	Boolean
lastSeen	lastContactTimeutc	The date time when the device last checked in with the Intune management service endpoint.	String The format is MM/DD/YYYY HH:MM:SS
macAddress	macAddress	MAC address of the device.	String
manufacturer	manufacturer	Device Manufacturer.	String
meid	meid	MEID is 56 bits long (14 hex digits). It consists of three fields, including an 8-bit regional code (RR), a 24-bit manufacturer code, and a 24-bit manufacturer-assigned serial number.	String
model	model	Model of the device.	String
osVersion	osVersion	OS Version of the device.	String
serialNumber	serialNumber	Serial number of the device. Applies to iOS Devices only.	String

Role Mapping Attribute Name	Microsoft Intune Attribute Name	Description	Data Type
UDID	udid	The device unique identifier. Unique Device Identifier (UDID), which is a sequence of 40 letters and numbers that is specific to iOS devices.	String
UUID	uuid	Universal unique device identifier.	String

Figure 9 Realm Configuration Page – Certificate Restrictions

The screenshot shows the Pulse Secure web interface. The top navigation bar includes links for System, Authentication, Administrators, Users (highlighted), Maintenance, and Wizards. The breadcrumb trail indicates the path: User Realms > All Roles Realm - NC Client > Authentication Policy > Certificate. The 'Certificate' tab is selected under the 'Authentication Policy' section. Below this, there are sub-tabs: Source IP, Browser, Certificate (selected), Password, Host Checker, and Limits. Three radio button options are presented for user authentication: 'Allow all users (no client-side certificate required)' (selected), 'Allow all users and remember certificate information while user is signed in.', and 'Only allow users with a client-side certificate signed by Trusted Client CAs to sign in. To change the certification authority, see the [Trusted Client CA](#) page.' Below these options, a message states 'You can optionally require specific values in the client certificate:' followed by a dropdown menu set to '10' and the text 'records per page'. A table with two columns, 'Certificate field (example "cn")' and 'Expected value', contains three empty rows for configuration. At the bottom left, there is a 'Save Changes' button.

Table 13 Realm Configuration Certificate Restriction Guidelines

Settings	Guidelines
Allow all users	Do not select this option. If you select this option, the system does not request a client certificate during the TLS handshake.
Allow all users and remember certificate	If you select this option, the system requests a client certificate during the TLS handshake. It does allow endpoints to authenticate without a client certificate. For those with a client certificate, the certificate attributes are placed in the session context.
Only allow users with a client-side certificate	If you select this option, the system requests a client certificate during the TLS handshake. It does not allow endpoints to authenticate without a valid client certificate. If the realm is configured with a certificate server, like this example, this option is the only option that can be selected.

Configuring a Sign-In Policy

A sign-in policy associates devices with a realm.

To configure a sign-in policy:

1. Select **Authentication > Signing In > Sign-In Policies** to navigate to the sign-in policies configuration page.
2. Click **New URL** to display the configuration page.
3. Complete the configuration as described below.
4. Save the configuration.

Table 14 Sign-In Policy Configuration Guidelines

Settings	Guidelines
User type	Select Users.
Sign-in URL	Enter a URL.
Description	Describe the purpose of the sign-in policy so that other administrators are aware of it.
Sign-In Page	Select a sign-in page.
Authentication Realm	
Realm	Select the realm you configured in the earlier step.
Authentication Protocol Set	Select the protocol you configured in the earlier step.
Realm name as a username suffix	<p>Select this option if the username sent during sign-in includes a realm suffix.</p> <p>To use this option, the realm name must match the username realm suffix configured in the MDN Wi-Fi profile.</p> <p>This configuration enables you to dedicate the realm to the MDM traffic. Non-MDM traffic passing through the same switch then belongs to a different realm.</p> <p>NOTE: In some cases, you can use authentication protocol sets to segregate traffic into a particular realm. For example, assuming only mobile endpoints use TLS and other endpoints do not, an authentication protocol set containing only TLS can be created and associated with a particular realm through a sign-in policy.</p>
Remove realm suffix	Remove the realm suffix within system processes, such as rule processing and logs.

Configuring PPS with Pulse Workspace

Pulse Workspace is the Pulse Secure MDM server which provides the device compliance status for the mobile devices. PPS retrieves the device attributes from PWS and uses it for compliance assessments and role assignment.

To configure PWS MDM:

1. Select **System > Configuration > Pulse One > Settings** to register PPS with Pulse One.
2. Enter the **PWS registration URL** and registration code details and register PPS to PWS.
3. Click **Save Changes**.

The registration status and the notification channel status turns green if the connection is successful.

Figure 10 PWS MDM Configuration

The screenshot displays the Pulse Secure System Administration web interface. The top navigation bar includes the Pulse Secure logo and tabs for System, Authentication, Administrators, Users, Endpoint Policy, Maintenance, and Wizards. The breadcrumb trail indicates the path: Configuration > Pulse One > Settings. The 'Settings' page has a sub-tab for 'Pulse One' which is currently selected. Below the tabs, there are sections for 'Registration Host', 'Registration Code', 'Credential Renegotiation Interval', 'Preferred network interface', and 'Credentials Exchange time'. Each section includes a text input field, a dropdown menu, or a radio button, along with a descriptive tooltip. For example, the 'Registration Host' field contains 'api.pulseone.net' and the tooltip says 'The Host to which the appliance connects to for starting registration flow'. The 'Credential Renegotiation Interval' is set to '6 days' with a tooltip '1 - 7 days. The time after which credentials are renegotiated'. Below these settings, there is a 'Registration Result Details' section with a green checkmark icon, followed by a 'Status Information' section with two radio buttons for 'Registration Status' and 'Notification Channel Status'. At the bottom, there is an 'Actions' section with three buttons: 'Save Changes', 'Clear Configuration', and 'Renegotiate Credential'.

Configuration > Pulse One > Settings

Settings

Licensing **Pulse One** Security Certificates DMI Agent Sensors Client Types Guest Access

Settings

*Registration Host: The Host to which the appliance connects to for starting registration flow

*Registration Code: The registration code provided by Pulse One

*Credential Renegotiation Interval: days 1 - 7 days. The time after which credentials are renegotiated

Preferred network interface: If the selected network interface is disabled, defaults to 'Internal Port'

Credentials Exchange time: The last successful credential exchange time.

✓ Registration Result Details

On successful registration the following information is received from Pulse One

Hashing Algorithm: Hashing algorithm used for HAWK authentication.

Client Device Id: Unique id of the appliance on Pulse One

Notification URL: The URL for establishing notification channel

✓ Status Information

Registration Status: ☐

Notification Channel Status: ☐

✓ Actions

4. Select **Authentication > Auth. Servers > New MDM Server**. Enter the name, select Pulse Workspace as **MDM** and click **Save changes**.
5. Select **Users > User Realms** and select the **Device Attribute server for PWS**.
6. Select **Role Mapping** tab of the user realm to create role mapping rules. Configure the role mapping rules based on the PWS supported device attributes.

Figure 11 Role Mapping PWS MDM Server

Configuring PPS with Microsoft Intune

Microsoft Intune is an MDM server which provides the device compliance status for the mobile devices. PPS retrieves the device attributes from Microsoft Intune and uses it for compliance assessments and role assignment. This feature integrates Microsoft Intune and PPS for providing compliance check and onboarding of devices.

To configure Microsoft Intune MDM server:

1. Select **Authentication > Auth. Servers > New MDM Server**.
2. Enter the server name, select Microsoft Intune as MDM.
 - Enter the Azure AD Tenant ID.
 - Enter the Web application ID or Client ID that is registered in Azure AD.
 - Enter the Client Secret key registered in the Azure AD.
 - Enter the Timeout duration in seconds. Default is 15 seconds.

To obtain Tenant ID, Client ID, Client Secret Key, see [“Viewing Client ID, Tenant ID, and Client Secret” on page 43](#)

3. Click **Save changes**.

Figure 12 Intune MDM Server

Pulse Secure System **Authentication** Administrators Users Endpoint Policy Maintenance Wizards

Auth Servers > New MDM Server

New MDM Server

*Name: Label to reference this server.

Type: ☐ Pulse Workspace ☐ Air Watch ☐ Mobile Iron ☒ Microsoft Intune

▼ Server

* Tenant ID: Azure AD Tenant ID

* Client ID: Web application ID that has been registered in azure AD

* Client Secret: Secret key of the web application registered in azure AD

* Request Timeout: seconds (5 - 60)

Test Intune Connection

Note: Pulse Policy Secure uses endpoint's MAC address to query attributes from Microsoft Intune MDM auth server.

Save Changes **Reset**

* indicates required field

4. Select **Users > User Realms** and select the **Device Attribute server** for Microsoft Intune.

Figure 13 Realm

Pulse Secure System Authentication Administrators **Users** Endpoint Policy Maintenance Wizards

User Realms > Users > General

General Authentication Policy Role Mapping

* Name: Label to reference this realm

Description:

☐ When editing, start on the Role Mapping page

▼ Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication: Specify the server to use for authenticating users.

User Directory/Attribute: Specify the server to use for authorization.

Accounting: Specify the server to use for Radius accounting.

Device Attributes: Specify the server to use for device authorization.

Device Check Interval: minutes Specify the interval to check device attributes server. disable=0, min=10, max=10080 minutes

5. Select **Role Mapping** tab of the user realm to create role mapping rules. Configure the role mapping rules based on the Microsoft Intune supported device attributes.

Figure 14 Role Mapping Intune MDM Server

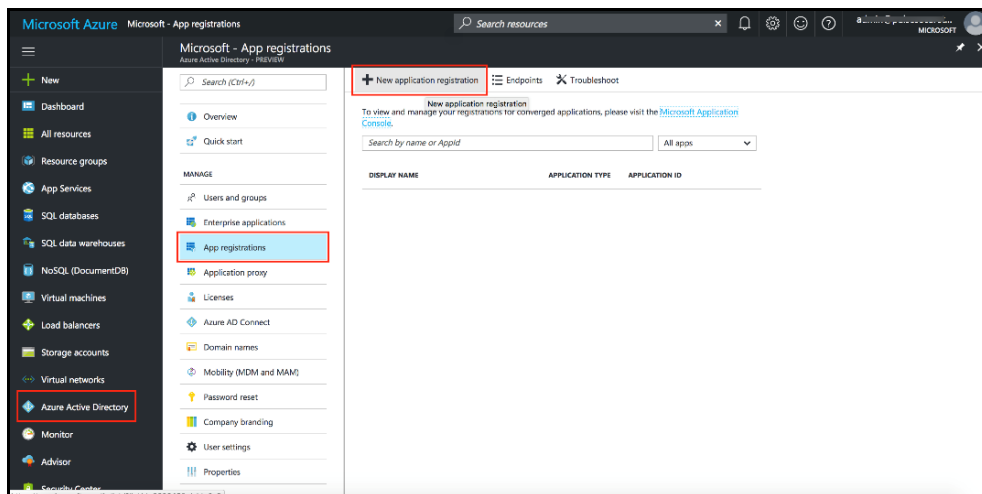
Configuring the Microsoft Intune MDM

Microsoft Intune acts as the Mobile Device Management (MDM) Server for PPS solution. PPS users have to register their mobile devices with Microsoft Intune. As part of registration, the relevant Profiles get automatically provisioned to mobile device.

To configure the Microsoft Intune MDM:

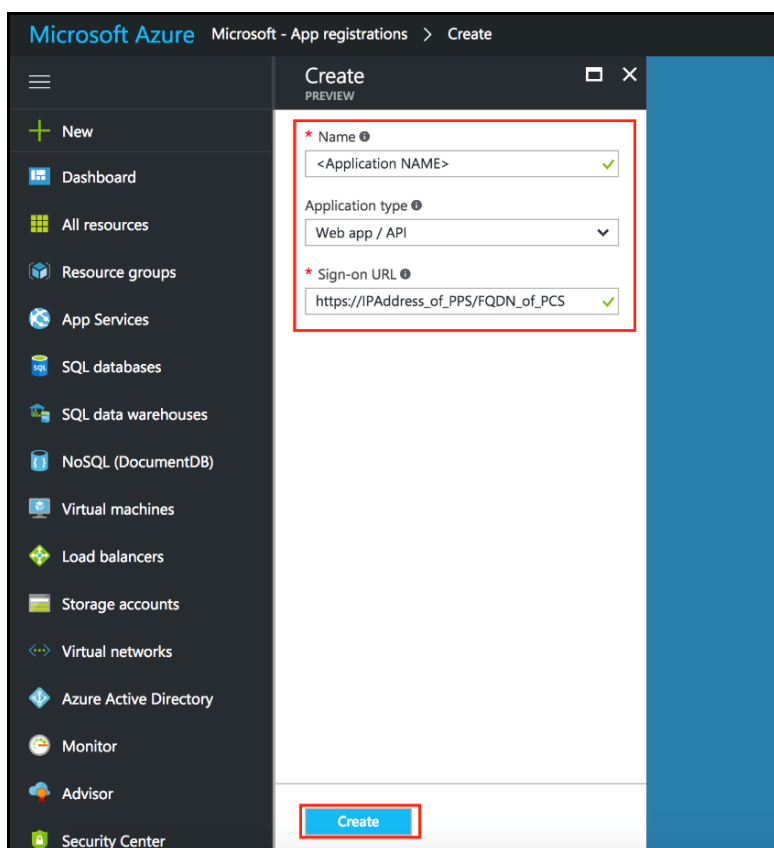
1. Enroll the devices with the MDM server.
2. Create an enterprise WiFi profile.
3. Configure PPS with a role and realm for the user. Microsoft Intune provides the user with a link to provision the created policy and then pushes the profile information. PPS does the role assignment and either allows or denies based on the device assessment. For more information, see [Configuring PPS](#)
4. Create Azure Active Directory (AAD) web application.
5. Go to portal.azure.com, click on the Azure Active Directory on the left of the screen, click on to App registrations and click on New application registration.

Figure 15 Creating New Application



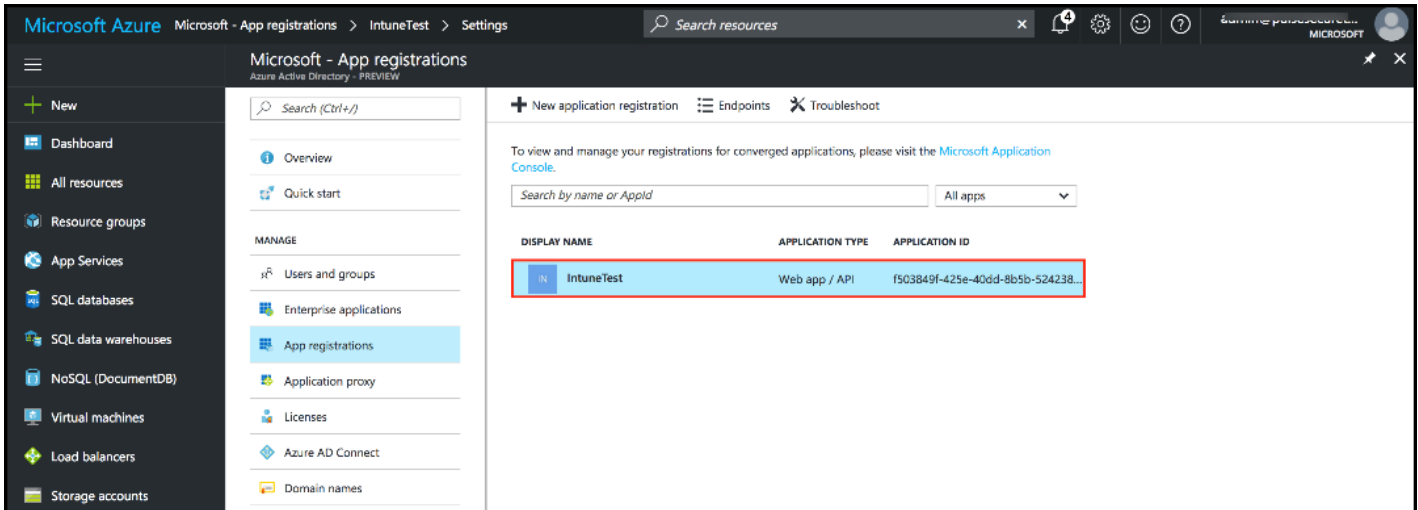
6. Enter the application name, select Web app/API as application type, and enter the IP address/FQDN for sign-on-URL and Click Create.

Figure 16 Setting up the New Application



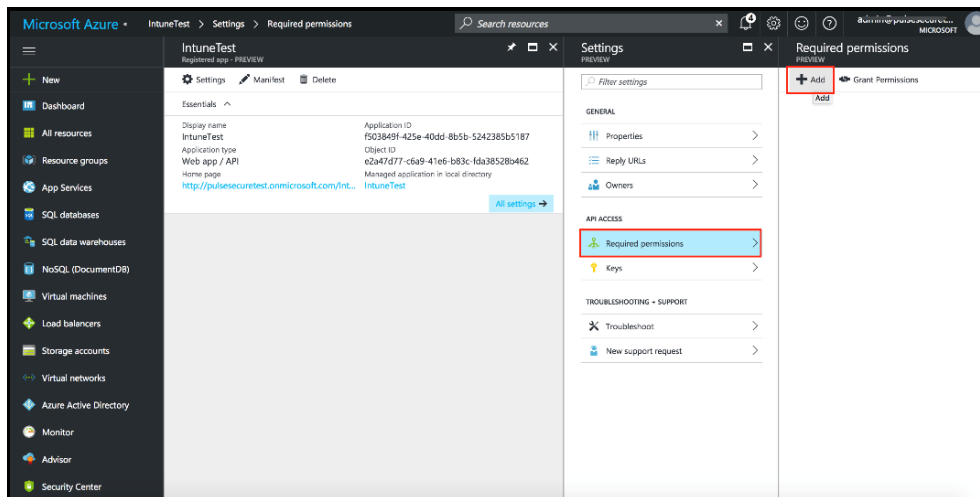
The Application Registration page appears if the registration is successful.

Figure 17 Application Created



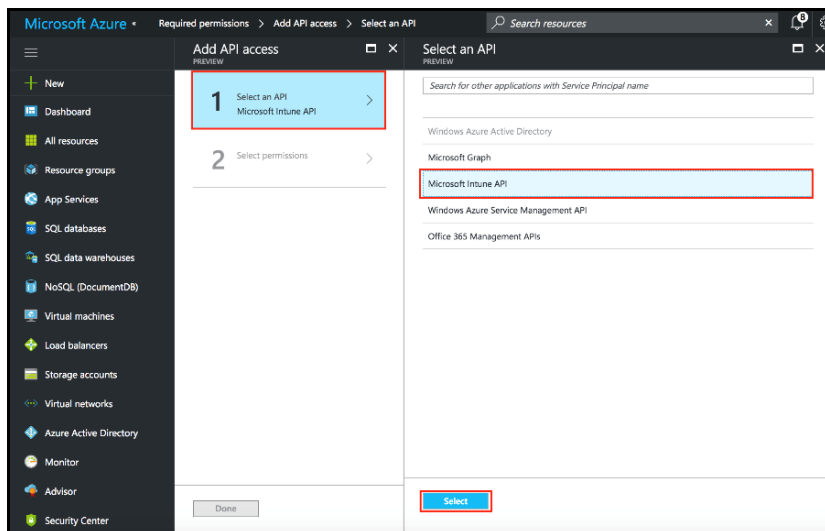
- Click the application and select the required permissions and click **Add**.

Figure 18 Adding Permissions



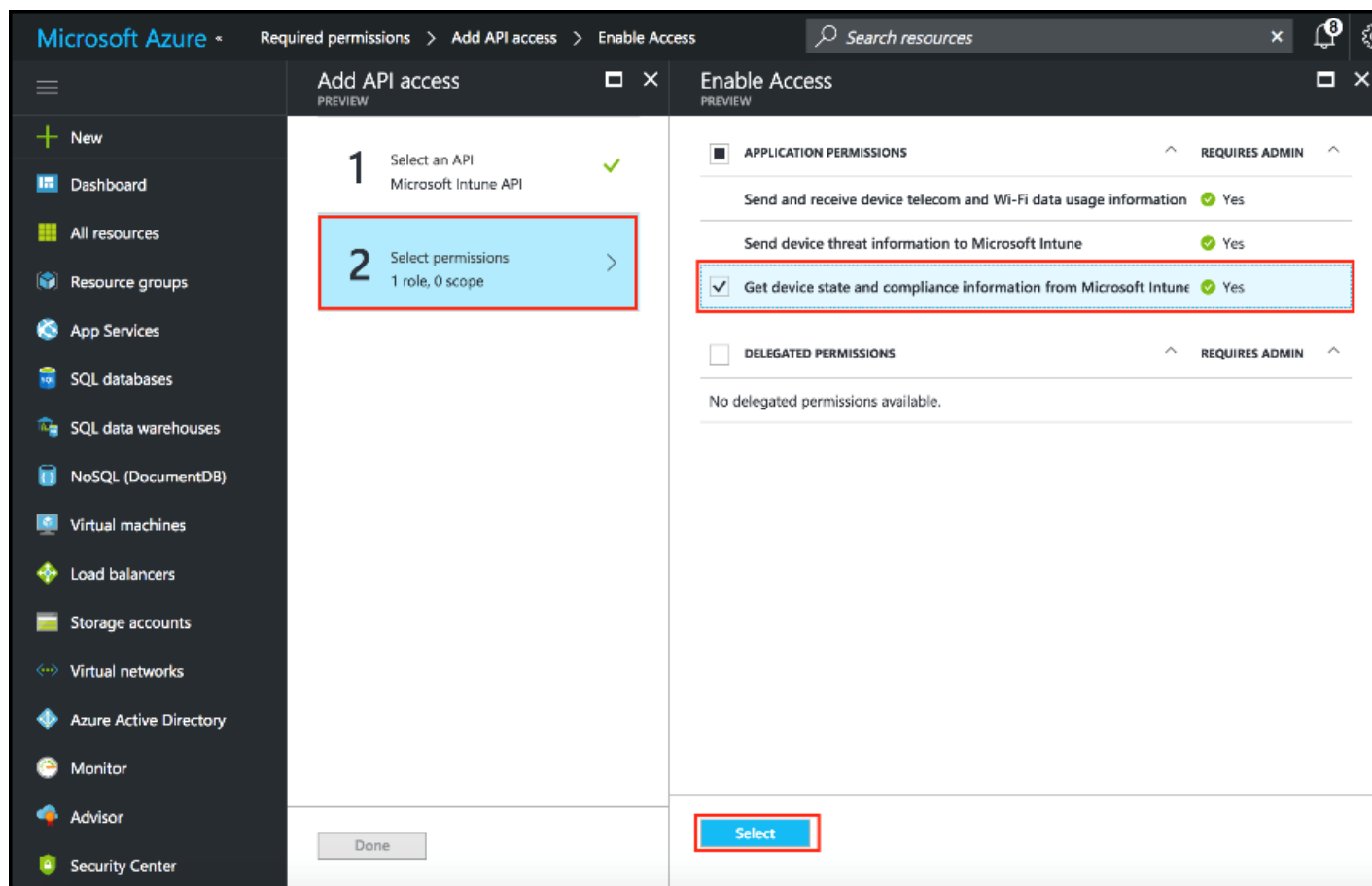
- Click **Grant Permission**.
- Select **Microsoft Intune API**.

Figure 19 Setting Intune Permissions



Under Application Permissions, select Get device and compliance information from Microsoft Intune.

Figure 20 Setting Intune Permissions



10. (Optional) You must add the following delegated permissions for Microsoft Graph API.

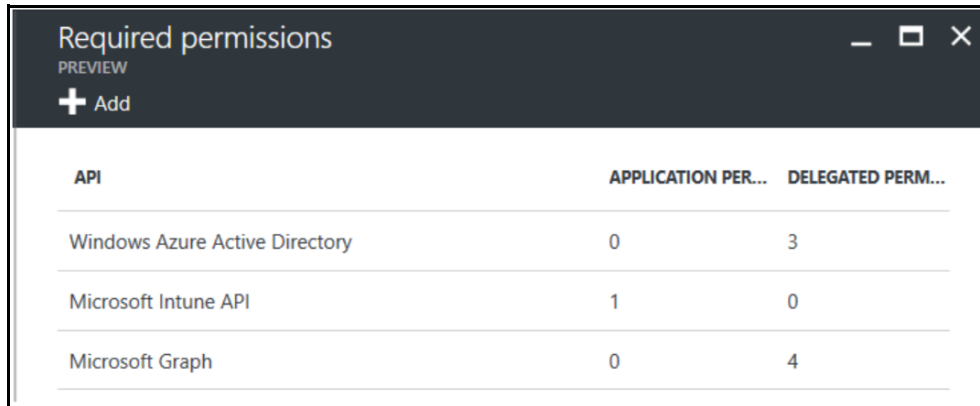
- Sign in and read user profile
- Sign Users in

- View users' email address
- View users' basic profile

11. (Optional) Add the following delegated permissions for Azure Active Directory.

- Sign in and read user profile
- Read all users' basic profiles
- Access the directory as the signed-in user.

Figure 21 Permissions



API	APPLICATION PERMISSIONS	DELEGATED PERMISSIONS
Windows Azure Active Directory	0	3
Microsoft Intune API	1	0
Microsoft Graph	0	4

Viewing Client ID, Tenant ID, and Client Secret

The Client ID/Application ID is created automatically once the AAD web application/API is created. You can view the client ID/application ID from the application properties page.

Figure 22 Client ID/Application ID

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a breadcrumb trail (IntuneTest > Settings > Required permissions > Enable Access), and a search bar. The left sidebar contains a 'New' button and a list of resource types: Dashboard, All resources, Resource groups, App Services, SQL databases, SQL data warehouses, NoSQL (DocumentDB), Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, and Security Center. The main content area displays the 'IntuneTest' application settings. The 'Essentials' tab is active, showing the following details:

Property	Value
Display name	IntuneTest
Application type	Web app / API
Home page	http://pulsesecuretest.onmicrosoft.com/Int...
Application ID	f503849f-425e-40dd-8b5b-5242385b5187
Object ID	e2a47d77-c6a9-41e6-b83c-fda38528b462
Managed application in local directory	IntuneTest

An 'All settings' button is located at the bottom right of the Essentials section.

Every organization in Microsoft cloud is called tenant and it is organization specific. Each Tenant will be having a unique Tenant ID. Select the web application/API and click Endpoints tab and then you can copy the tenant ID.

Figure 23 Client ID/Application ID

The screenshot shows the Microsoft Azure portal interface. The breadcrumb navigation at the top reads: Microsoft Azure > IntuneTest > Settings > Required permissions > Enable Access. A search bar on the right contains the text 'Search resources'. The left-hand navigation pane lists various Azure services, with 'New' at the top. The main content area has three tabs: '+ New application registration', 'Endpoints' (which is selected and highlighted with a red box), and 'Troubleshoot'. Below the tabs, there is a message: 'To view and manage your registrations for converged applications, please visit the [Microsoft Application Console](#).' Below this message is a search bar labeled 'Search by name or AppId' and a dropdown menu set to 'All apps'. A table displays the application registration details:

DISPLAY NAME	APPLICATION TYPE	APPLICATION ID
IN IntuneTest	Web app / API	f503849f-425e-40dd-8b5b-524238...

The first row of the table is highlighted with a red box.

The screenshot shows the Microsoft Azure portal interface, specifically the 'Endpoints' tab for an application registration. The breadcrumb navigation at the top reads: Microsoft Azure > Microsoft - App registrations > Endpoints. A search bar on the right contains the text 'Search resources'. The left-hand navigation pane lists various Azure services, with 'New' at the top. The main content area has a 'PREVIEW' section titled 'Endpoints'. It lists several endpoints with their corresponding URLs and a document icon to the right:

- FEDERATION METADATA DOCUMENT: <https://login.windows.net/6c488131-7bc7-4405-bdec-797b85099ccc/federationmetadata/2007-06/federationmetadata.xml>
- WS-FEDERATION SIGN-ON ENDPOINT: <https://login.windows.net/6c488131-7bc7-4405-bdec-797b85099ccc/ws/fed>
- SAML-P SIGN-ON ENDPOINT: <https://login.windows.net/6c488131-7bc7-4405-bdec-797b85099ccc/saml2>
- SAML-P SIGN-OUT ENDPOINT: <https://login.windows.net/6c488131-7bc7-4405-bdec-797b85099ccc/saml2>
- MICROSOFT AZURE AD GRAPH API ENDPOINT: <https://graph.windows.net/6c488131-7bc7-4405-bdec-797b85099ccc>
- OAuth 2.0 TOKEN ENDPOINT: <https://login.windows.net/6c488131-7bc7-4405-bdec-797b85099ccc/oauth2/token>
- OAuth 2.0 AUTHORIZATION ENDPOINT: <https://login.windows.net/6c488131-7bc7-4405-bdec-797b85099ccc/oauth2/authorize>

The 'MICROSOFT AZURE AD GRAPH API ENDPOINT' row is highlighted with a red box.

To create the secret key, click the Web Application/API and then click Keys.

Microsoft Azure - App registrations > IntuneTest > Settings > Keys

Settings PREVIEW

Keys PREVIEW

Save Discard

DESCRIPTION	EXPIRES	VALUE
TestKey1	4/19/2018	Hidden

Key description Duration Value will be displayed on save

Keys PREVIEW

Save Discard

⚠ Copy the key value. You won't be able to retrieve after you leave this blade.

DESCRIPTION	EXPIRES	VALUE
TestKey1	4/19/2018	Hidden
test2	12/31/2299	vpAB0naSPwGLqXDIT90uP7bB38jXCWMuf7g9edHUleM=

Key description Duration Value will be displayed on save

Configuring the PWS MDM

Pulse Workspace acts as the Mobile Device Management (MDM) Server for PPS solution. PPS users have to register their mobile devices with Pulse Workspace. As part of registration, the relevant Profiles get automatically provisioned to mobile device.

To configure the PWS MDM:

1. Enroll the devices in the MDM.
2. Create an enterprise WiFi profile. For more information, see [Enterprise WiFi configuration](#)
3. Configure PPS with a role and realm for the user using the Certificate authentication server. PWS provides the user with a link to provision the created policy and then pushes the profile information. PPS does the role assignment and either allows or denies based on the device assessment. For more information, see [Configuring PPS](#)

Configuring the AirWatch MDM

To configure the AirWatch MDM:

1. Enroll devices in the MDM using the methods supported by the MDM.
2. Create a profile with the following MDM management options:
 - Certificate template- Create a configuration that specifies the field and type of identifier for client device certificates.
The MDM configuration templates provide flexibility in how the device identifier can be placed in the device certificate's subject or alternative subject. We recommend you include the user ID in the certificate, so the certificate can identify both the user and the device. For example:
 - CN=<EnrollmentUser>, serialNumber=<DeviceUid>, o=Company
 - Credential profile- Create a configuration that specifies the certificate authority and certificate template configuration.
 - Wi-Fi profile- Create a configuration that specifies the SSID, security options, and the credential configuration.
3. Save and deploy the profile to devices registered with your organization.
4. Enable API access and generate the AirWatch API key (tenant code).

The tenant code is part of the REST API configuration. The tenant code must be included in PPS MDM server configuration.

Figure 24 AirWatch Certificate Template Configuration

Certificate Template - Add / Edit

Name*

Pulse Secure Device Certificate

Description

Certificate Authority*

awlab99-ATL99LABCA01-CA

Issuing Template

certificatetemplate:MobileUser2

Subject Name*

CN={EnrollmentUser},serialNumber={DeviceUid}

Private Key Length*

2048

Private Key Type*

Signing ☒ Encryption ☒

San Type

Add

Automatic Certificate Renewal

☒

Auto Renewal Period (days)*

5

Enable Certificate Revocation

☒

Publish Private Key

☐

Save

Save and Add Another Template

Cancel

Figure 25 AirWatch Credential Configuration

General

Passcode

Restrictions

Wi-Fi

VPN

Email Settings

Exchange ActiveSync

Application Control

Bookmarks

Credentials

Launcher

LDAP

Custom Settings

Credentials

Credential Source

Defined Certificate Authority

Certificate Authority*

AirWatch-ATL02PRDCS10-CA

Certificate Template*

Pulse Device Certificate

Save

Save & Publish

Cancel

Figure 26 AirWatch Wi-Fi Configuration

The screenshot displays the 'WiFi with TLS' configuration page in the AirWatch admin console. On the left is a sidebar menu with various settings categories. The 'Wi-Fi' option is selected and highlighted in blue. The main content area is titled 'Wi-Fi' and contains several configuration fields. The 'Service Set Identifier' is set to 'device-auth-8021x'. The 'Hidden Network' checkbox is unchecked. The 'Auto-Join' checkbox is checked. The 'Security Type' is set to 'WPA/WPA2 Enterprise'. Below this is a 'Proxy' section with 'Proxy Type' set to 'None'. At the bottom is a 'Protocols' section with checkboxes for TLS (checked), TTLS, LEAP, and PEAP. At the very bottom of the page are three buttons: 'Save', 'Save & Publish', and 'Cancel'.

WiFi with TLS

General

- Passcode
- Wi-Fi**
- VPN
- Email
- Exchange Web Services
- LDAP
- CalDAV
- CardDAV
- Web Clips
- Credentials**
- SCEP
- Dock
- Restrictions
- Parental Controls
- Gatekeeper
- Custom Settings

Wi-Fi

Service Set Identifier*

Hidden Network ☐

Auto-Join ☒

Security Type

Proxy

Proxy Type

Protocols

TLS ☒

TTLS ☐

LEAP ☐

PEAP ☐

Save **Save & Publish** **Cancel**

Figure 27 Deploying a Profile to Your Organization's Managed Devices

WiFi with TLS

General

Passcode

Wi-Fi **1**

VPN

Email

Exchange Web Services

LDAP

CalDAV

CardDAV

Web Clips

Credentials **1**

SCEP

Dock

Restrictions

Parental Controls

Gatekeeper

Custom Settings

General

Name* WiFi with TLS

Description

Deployment Managed

Assignment Type Auto

Minimum Operating System Any

Model Any

Ownership Any

Allow Removal Always

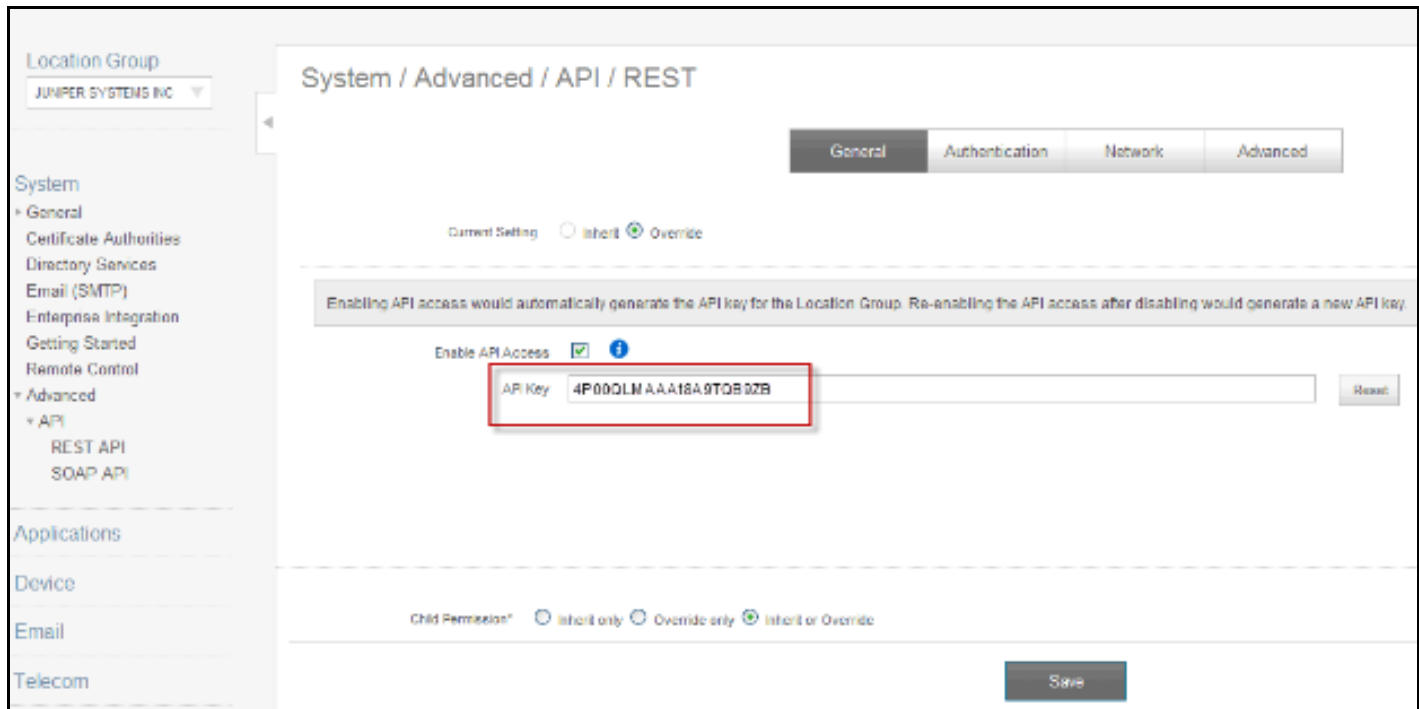
Managed By Pulse

Assigned Organization Groups* Pulse **X**

Start typing to add a new group

Save Save & Publish Cancel

Figure 28 AirWatch API Tenant Code Configuration



Configuring the MobileIron MDM

To configure the MobileIron MDM:

1. Enroll devices in the MDM using the methods supported by the MDM.
2. Create a Simple Certificate Enrollment Protocol (SCEP) configuration that specifies the field and type of identifier for client device certificates.

The MDM configuration templates provide flexibility in how the device identifier can be placed in the device certificate's subject or alternative subject. We recommend you include the user ID in the certificate, so the certificate can identify both the user and the device. For example:

CN=<DEVICE_UUID>, uid=<USER_ID>, o=Company

3. Create a Wi-Fi configuration that specifies the SSID and security options. During the enrollment process, this profile is provisioned to the device. Select the SCEP configuration completed in Step 2.
4. Select the Wi-Fi Profile configuration and apply it to a group label you have provisioned to manage this group of devices.

Note: Wi-Fi connect fails if it is configured to use a device certificate that is signed by an intermediate CA and selects this in Wi-Fi profile trusted CA. Root CA has to be selected to properly work.

5. Apply the group label to the devices when you add them to the MDM. If they have already been added to the MDM, use the edit configuration utilities in the device inventory page to apply the group label.

Figure 29 MobileIron Wi-Fi Configuration

New Wifi Setting

Name: Pulse Secure Access

Network Name (SSID): device-auth-802d

Description:

Hidden Network: ☐

Authentication: WPA2 Enterprise

Data Encryption: AES

User Name: \$USERID\$

Password: \$PASSWORD\$

Apply to Certificates: Available

- System - iOS Enrollment CA Certificate
- sumitclientauth
- System - iOS MDM CA Certificate
- new

Selected:

Trusted Certificate Names:

(Note: Enter comma (,) separated certificate names for multiple authentication servers.)

Allow Trust Exceptions: ☐

Use Per-connection Password: ☐

EAP Type: ☐ EAP-FAST ☐ EAP-SIM ☐ LEAP ☐ PEAP ☒ TLS ☐ TTLS

Identity Certificate: Pulse Device Certificate

Save Cancel

Figure 30 Applying the Wi-Fi Configuration to a Label

Microsoft Azure - App registrations

Search resources

Microsoft - App registrations

Search (Ctrl+F)

+ New application registration

Endpoints Troubleshoot

New application registration

To view and manage your registrations for converged applications, please visit the [Microsoft Application Console](#).

Search by name or AppId

All apps

DISPLAY NAME	APPLICATION TYPE	APPLICATION ID
--------------	------------------	----------------

MANAGE

- Users and groups
- Enterprise applications
- App registrations
- Application proxy
- Licenses
- Azure AD Connect
- Domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties

Figure 31 Adding a Device to the MDM

The screenshot shows the MobileIron Admin Portal interface. The top navigation bar includes 'MobileIron ADMIN PORTAL', 'USERS & DEVICES' (highlighted in red), 'APPS', 'POLICIES & CONFIGS', 'SETTINGS', and 'LOGS & EVENTS'. Below this is a sub-navigation bar with 'Dashboard', 'Devices' (selected), 'ActiveSync Associations', 'Labels', 'Users', and 'Retired Devices'. The main content area has an 'Actions' dropdown with a '+ Add' button. A 'Labels' dropdown is set to 'All-Smartphones'. A search bar is present with 'Search by User or Device' and links for 'Advanced Search' and 'Pending Device Report'. A table of devices is displayed with columns: User, Phone, OS, Country, Status, Registered on Date, Last Check-In, E/C, and Open. The 'Single Device' option in the 'Add' dropdown is highlighted by a mouse cursor.

User	Phone	OS	Country	Status	Registered on Date	Last Check-In	E/C	Open
Pulse	Galaxy Nexus by sams...	Android 4.2		Active	2013-07-12	33 d 2 h	C	
Pulse TME	+14084315645 iPhone 4	iOS 6.1	United States	Active	2013-07-10	20 d 2 h	C	AT&
Pulse TME	PDA 6 iPad, 3rd gen	iOS 6.1	United States	Active	2013-07-15	55 m 39 s	C	AT&

Troubleshooting

During initial configuration, enable event logs for MDM API calls. You can use these logs to verify proper configuration. After you have verified proper configuration, you can disable logging for these events. Then, enable only for troubleshooting.

To enable logging for MDM API calls:

1. Select **System Log/Monitoring**.
2. Click the **Events** tab.
3. Click the **Settings** tab to display the configuration page.

After you have completed the MDM server configuration, you can view system event logs to verify that the polling is occurring.

To display the Events log:

1. Select **System Log/Monitoring**.
2. Click the **Events** tab.
3. Click the **Log** tab.

Next, to verify user access, you can attempt to connect to a wireless access point with your smart phone, and then view the user access logs.

To display the User Access log:

1. Select **System Log/Monitoring**.
2. Click the **User Access** tab.
3. Click the **Log** tab.

After you have verified proper configuration, you are not likely to need to tune the authentication server configuration, the 802.1x framework, or the enforcement points. However, based on user experience, MDM capabilities, and security threats, there are a few configuration elements you might want to tune from time to time.

Table 15 describes these configuration elements.

Table 15 Tuning the Configuration

Configuration Element	Tuning
Remediation	<p>In a network access control solution, noncompliant endpoints are typically placed in a remediation VLAN that serves a Web page. The Web page explains the steps users can take to make their endpoints compliant so that they can access the network.</p> <p>Your reasons for denying access might change from time to time. For example, your initial policy might be based on compliance with an MDM policy, and you can give steps on how to bring a device into compliance. You want to set an expectation on how long it takes for the MDM to reassess compliance. You might want to factor in PPS device check interval to estimate how long until the device can access the network.</p> <p>When there are new threats that exploit vulnerabilities in specific mobile platforms, you might create rules on the fly that deny access from specific platforms. If events like this occur, you might want to update your remediation message so that users can understand why access is denied.</p>
Realm – Device Check Interval	<p>You might want to tune this setting as you learn how frequently the MDM updates device records, or if the standard practice of the MDM changes. If the MDM records are updated every four hours, it does not make sense to poll every 10 minutes. If the MDM records are updated in real time, it might make sense to poll every 10 minutes.</p>
Roles and role mapping rules	<p>As you learn about mobile security threats and vulnerabilities, you might make changes to roles and role mapping rules or create new classifications. In general, you list restrictive rules first and set the stop flag. For example, if a device is noncompliant and maps to a noncompliant role, you would list it near the top of the rules for the realm and set the stop flag.</p> <p>Classification based on device type or platform can be more complicated. When you initially role out your BYOD solution, you might want to use roles to merely classify the devices, and so the rule classifying it would not need to be near the top of the list and would not need to have a stop flag. In response to a threat, however, you might want to use the role and role mapping configuration to deny access from a specific device platform. If events like this occur, you can edit your rules to map the vulnerable platform to an appropriate role and set the stop flag so that permissive roles are not assigned.</p>
RADIUS return attribute policy	<p>Likewise, in response to threats and vulnerabilities, you can edit your rules to place formerly trusted device types into a remediation or guest VLAN instead of an employee VLAN; and then allow access again when you are no longer concerned with the threat.</p>
Infranet Enforcer resource access policy	<p>Likewise, in response to threats and vulnerabilities, you can edit your rules to deny access from formerly trusted device types; and then allow access again when you are no longer concerned with the threat.</p>

Using the Debug Logs

The Pulse Secure Global Support Center (PSGSC) might direct you to create a debug log to assist them in helping you debug an issue with the system. The debug log is used only by PSGSC.

To use debug logging:

1. Select **Troubleshooting > Monitoring > Debug Log** to display the configuration page. Complete the configuration as described in table below.
2. Click **Save Changes**. When you save changes with **Debug Logging On** selected, the system begins generating debug log entries.
3. Initiate the action you want to debug, such as a user sign in. You can reset the debug log file to restart debug logging if it takes you too long to initiate the action.
4. Click **Save Debug Log** to save the debug log to a file that you can send to PSGSC. You can clear the log after you have saved it to a file.
5. Clear the Debug Logging On check box and click **Save Changes** to turn off debug logging.

Table 16 Debug Log Configuration Guidelines

Settings	Guidelines
Current Log Size	Displays the size of the current log file. If it is large, use the controls to save, reset, or clear the log file.
Debug Logging On	Select to turn on debug logging.
Debug Log Size	Specify a maximum debug logfile size. The default is 2 MB. The maximum is 250 MB.
Debug Log Detail Level	Specify the debug log detail level. Obtain this from PSGSC.
Include logs	Select this option to include system logs in the debug log file. Recommended.
Process Names	Specify the process name. Obtain this from PSGSC.
Event Codes	Specify the event code. Obtain this from PSGSC. For MDM integration issues, PSGSC typically likes to collect debugging information for codes MDM, Auth, agentman, and Realm. The text is not case sensitive.

General Notes

For policy reasons, security issues are not normally mentioned in release notes. To find more information about our security advisories, please see our [security advisory page](#).

Documentation

Pulse Secure documentation is available at <https://www.pulsesecure.net/techpubs/>

Technical Support

When you need additional information or assistance, you can contact "Pulse Secure Global Support Center (PSGSC):

- <https://support.pulsesecure.net>
- support@pulsesecure.net

Call us at 1- 844-751-7629 (toll-free USA)

For more technical support resources, browse the support website <https://support.pulsesecure.net>

