



PCS Integration with MDM Servers Deployment Guide

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.

PCS Integration with MDM Servers Deployment Guide

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.

Contents

UNDERSTANDING THE DEVICE ACCESS MANAGEMENT FRAMEWORK	3
SOLUTION OVERVIEW.....	5
DEPLOYING A BYOD POLICY FOR AIRWATCH MANAGED DEVICES.....	6
REQUIREMENTS.....	6
CONFIGURING THE AIRWATCH MDM SERVICE.....	7
CONFIGURING THE DEVICE ACCESS MANAGEMENT FRAMEWORK.....	11
CONFIGURING A RESOURCE POLICY	29
DEPLOYING A BYOD POLICY FOR MOBILEIRON MANAGED DEVICES.....	33
REQUIREMENTS.....	33
CONFIGURING THE MOBILEIRON MDM SERVICE.....	33
CONFIGURING THE DEVICE ACCESS MANAGEMENT FRAMEWORK.....	39
USING LOGS TO VERIFY PROPER CONFIGURATION	60
USING POLICY TRACING AND DEBUG LOGS.....	63

Device Access Management Framework

• Understanding the Device Access Management Framework	3
• Solution Overview	5
• Deploying a BYOD Policy for AirWatch Managed Devices	6
• Deploying a BYOD Policy for MobileIron Managed Devices	33
• Using Logs to Verify Proper Configuration	60
• Using Policy Tracing and Debug Logs	63

Understanding the Device Access Management Framework

The device access management framework leverages mobile device management (MDM) services so that you can use familiar Pulse Connect Secure client policies to enforce security objectives based on your device classification scheme: device status is MDM enrollment complete or incomplete; device status is MDM-policy compliant or non-compliant; device is employee owned or company owned; device platform is iOS, Android, or neither; and so forth.

In this framework, the MDM is a device authorization server, and MDM record attributes are the basis for granular access policy determinations. For example, you can implement policies that allow devices that have a clean MDM posture assessment and are compliant with MDM policies to access the network, but deny access to servers when you want to prevent downloads to employee-owned devices or to a particular platform that might be vulnerable. To do this, you use the device attributes and status maintained by the MDM in Pulse Secure client role-mapping rules, and specify the device-attribute-based roles in familiar Pulse Secure client policies.

The framework simply extends the user access management framework realm configuration to include use of device attributes as a factor in role mapping rules. [Figure 1](#) illustrates the similarities.

Figure 1 User Access Management Framework and Device Access Management Framework

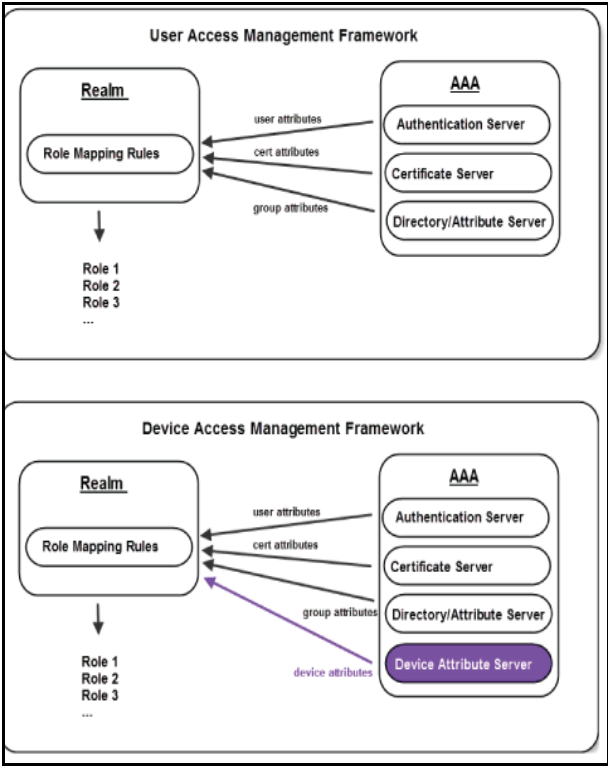


Table 1 summarizes vendor support for this release.

Table 1 MDM Vendors

Product	Vendor
Pulse Connect Secure	<ul style="list-style-type: none">• Pulse Workspace (PWS)• AirWatch MDM• MobileIron MDM• Microsoft Intune

Table 2 summarizes supported methods for determining the device identifiers.

Table 2 Device Identifiers

Product	Policies
Pulse Connect Secure	Device certificate (required)

Table 3 summarizes policy reevaluation features.

Table 3 Policy Reevaluation

Product	Policy Reevaluation
Pulse Connect Secure	The MDM is query and policies evaluated only during sign-in. If desired, you can use the user role session timeout setting to force users to sign in periodically. If you use a certificate server for user authentication, the users are not prompted to sign in again; however, if you have enabled user role notifications, users do receive a notification each time sign-in occurs.

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

Table 4 summarizes the policies in which you can specify device-attribute-based roles.

Table 4 Policies

Product	Policies
Pulse Connect Secure	Resource policies or resource profiles

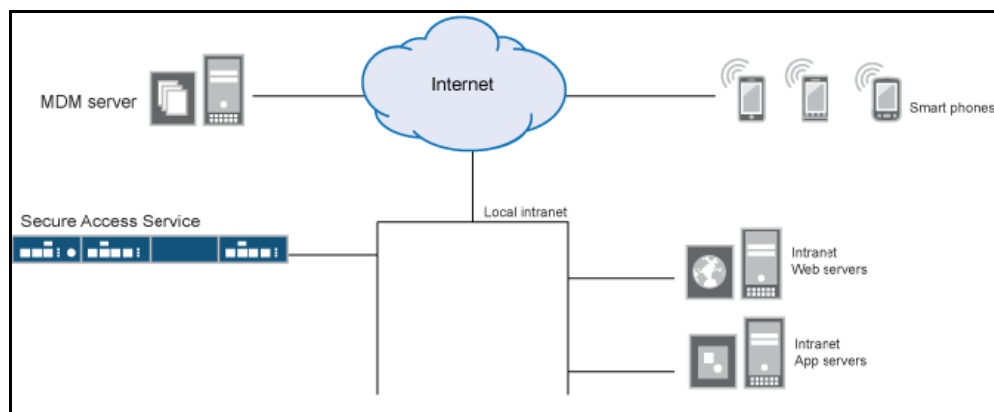
Solution Overview

In the past, to ensure security and manageability of the corporate network, enterprise information technology (IT) departments had restricted network access to company-issued equipment. For mobile phones, the classic example was the company-issued BlackBerry handset. As powerful mobile smart phones and tablets have become commonly held personal possessions, the trend in enterprise IT has been to stop issuing mobile equipment and instead allow employees to use their personal smart phones and tablets to conduct business activities. This has lowered equipment costs, but BYOD environments pose capacity planning and security challenges: how can an enterprise track network access by non-company-issued devices? Can an enterprise implement policies that can restrict the mobile devices that can access the network and protected resources in the same way that SSL VPN solutions restrict user access?

MDM vendors have emerged to address the first issue. MDMs such as AirWatch, MobileIron, Microsoft Intune provide enrollment and posture assessment services that prompt employees to enter data about their mobile devices. The MDM data records include device attributes and posture assessment status that can be used in the access management framework to enforce security policies.

Figure 2 shows a deployment with Pulse Connect Secure and the MDM cloud service.

Figure 2 Solution Topology



The solution shown in this example leverages the Pulse Secure access management framework to support attribute-based network access control for mobile devices. In the device access management framework, the MDM is a device authorization server and MDM record attributes are the basis for access policy determinations. For example, suppose your enterprise wants to enforce a policy that allows access only to mobile devices that have enrolled with the MDM or are compliant with the MDM posture assessment policies. You can use the attributes and status maintained by the MDM in role-mapping rules to implement the policy.

In this framework, a native supplicant is used to authenticate the user of the device. The device itself is identified using a client certificate that contains device identity. The client certificate can be used to identify the device against the MDM records and authenticate the user against a certificate server.

The Pulse Secure solution supports granular, attribute-based resource access policies. For example, you can implement policies that allow devices that have a clean MDM posture assessment and are compliant with MDM policies to access the network, but deny access to servers when you want to prevent downloads to employee-owned devices or to a particular platform that might be vulnerable.

Deploying a BYOD Policy for AirWatch Managed Devices

This example shows how to use policies to enable security based on device identity, device posture, or user identity in a bring your own device (BYOD) environment for an enterprise that uses AirWatch® for mobile device management (MDM). It includes the following information:

- [“Requirements” on page 6](#)
- [“Configuring the AirWatch MDM Service” on page 7](#)
- [“Configuring the Device Access Management Framework” on page 11](#)
- [“Configuring a Resource Policy” on page 29](#)

Requirements

[Table 5](#) lists version information for the solution components shown in this example.

Table 5 Component Version Information

Component	Version
Pulse Connect Secure	Release 8.0r1 or later is required.
AirWatch MDM	Release 6.4.1.2 is used in this example. Any version that supports the device ID and device attributes you plan to query is compatible.

Configuring the AirWatch MDM Service

This solution assumes you know how to configure and use the features of your MDM, and that you can enroll employees and their devices. For more information about the AirWatch MDM, refer to its documentation and support resources. 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.
- **Device attributes** - A standard set of data maintained for each device. For AirWatch, see [Table 6](#).

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 6](#) describes these attributes. In this solution, these attributes are used in the role mapping that is the basis for network access and resource access policies. When you configure role-mapping rules, you select the normalized Connect Secure attribute name.

Table 6 AirWatch Device Attributes

AirWatch Attribute	Normalized Connect SecureName	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

AirWatch Attribute	Normalized Connect SecureName	Description	Data Type
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	macAddress	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
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

To configure the MDM:

1. Enroll devices in the MDM using the methods supported by the MDM.
2. Create a profile. The profile determines many MDM management options. The following configurations are key to this solution:

1. Certificate template. Create a configuration that specifies the field and type of identifier for client device certificates. See [Figure 3](#).

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

2. Credential profile. Create a configuration that specifies the certificate authority and certificate template configuration. See [Figure 4](#).
3. VPN profile. Create a configuration that specifies the system VPN, security options, and the credential configuration. See [Figure 5](#).
3. Save and deploy the profile to devices registered with your organization. See [Figure 6](#)
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 the system MDM server configuration. It is sent in the API call. See [Figure 7](#).

Figure 3 AirWatch Certificate Template Configuration

The screenshot shows the 'Certificate Template - Add / Edit' form in the AirWatch console. The form contains the following fields and options:

- Name:** Pulse Device Certificate
- Description:** (empty)
- 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:** ☐

At the bottom of the form are three buttons: **Save**, **Save and Add Another Template**, and **Cancel**.

Figure 4 AirWatch Profile Credential Configuration

The screenshot shows the 'android-vpn-profile' configuration window. The left sidebar contains a list of settings: General, Passcode, Restrictions, Wi-Fi, VPN (highlighted with a green '1'), Email Settings, Exchange ActiveSync, Application Control, Bookmarks, Credentials (highlighted with a blue bar and a green '1'), Launcher, and Custom Settings. The main content area is titled 'Credentials' and contains three dropdown menus: 'Credential Source' set to 'Defined Certificate Authority', 'Certificate Authority*' set to 'awlab99-ATL99LABCA01-CA', and 'Certificate Template*' set to 'MobileUser3'. At the bottom right of the main area are '+' and '-' buttons. At the bottom of the window are 'Save', 'Save & Publish', and 'Cancel' buttons.

Figure 5 AirWatch Profile VPN Configuration

The screenshot shows the 'android-vpn-profile' configuration window with the 'VPN' tab selected. The left sidebar is the same as in Figure 4, with 'VPN' highlighted with a green '1' and 'Credentials' with a green '1'. The main content area is titled 'VPN' and includes a note: 'All VPN Options Below Are Supported By: Android 2.2+'. The configuration fields are: 'Connection Type*' set to 'Junos Pulse', 'Connection Name*' set to 'Secure Access Service 101', 'Server*' set to '10.209.112.112', 'Use Web Login For Authentication' (unchecked), 'Username' (empty), 'Realm' (empty), 'Role' (empty), 'Password' (empty), and 'Identity Certificate' set to 'Certificate #1'. At the bottom right of the main area are '+' and '-' buttons. At the bottom of the window are 'Save', 'Save & Publish', and 'Cancel' buttons.

Figure 6 Deploying a Profile to Your Organization's Managed Devices

The screenshot shows the 'android-vpn-profile' configuration window. The 'General' tab is active, displaying the following fields:

- Name: android-vpn-profile
- Description: (empty)
- Assignment Type: Auto
- Minimum Operating System: Any
- Model: Any
- Ownership: Any
- Allow Removal: Always
- Managed By: Juniper
- Assigned Organization Groups: Juniper

At the bottom, there are three buttons: 'Save' (highlighted in blue), 'Save & Publish', and 'Cancel'.

Figure 7 AirWatch API Tenant Code Configuration

The screenshot shows the 'System / Advanced / API / REST' configuration page. The 'General' tab is selected, and the 'Enable API Access' checkbox is checked. The 'API Key' field contains the value '4P00QLM AAA18A9TQB92B'. The 'Save' button is visible at the bottom.

Configuring the Device Access Management Framework

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

- “Configuring the MDM Authentication Server” on page 12
- “Configuring the Certificate Server” on page 14
- “Adding the MDM Certificate to the Trusted Client CA Configuration” on page 15
- “Configuring User Roles” on page 17
- “Configuring a Realm and Role Mapping Rules” on page 20
- “Configuring a Sign-In Policy” on page 28

Configuring the MDM Authentication Server

The MDM authentication server configuration is used by the system 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 shown in [Figure 8](#).
3. Complete the configuration as described in [Table 7](#).
4. Save the configuration.

Figure 8 Authentication Server Configuration Page

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

Auth Servers > New SAML Server

New SAML Server

Server Name:

Settings

*SAML Version: ☐ 1.1 ☒ 2.0

*Connect Secure Entity ID: Unique SAML identifier of the SAML Auth Server. Uses host name configured at [SAML Settings](#).

*Configuration Mode: ☒ Manual ☐ Metadata Uses metadata files configured at [SAML Metadata](#) for metadata file based configuration.

*Identity Provider Entity ID: Unique SAML identifier of the Identity Provider.

Identity Provider Single Sign On Service URL: User is redirected to this URL in destination first scenario.

User Name Template:
Example: <assertionNameDN.uid>, uid from XS09SubjectName.
The entire assertion name identifier if not specified; Or
<userAttr.attr>, attr from AttributeStatement attributes.

Allowed Clock Skew (minutes): 0 - 9999 minutes

☐ Support Single Logout If checked, Connect Secure supports sending and receiving single logout requests.

SSO Method

☐ Artifact ☒ Post

Response Signing Certificate:
Issued To:
Issued By:
Valid:
Details: [Other Certificate Details](#)

Upload Certificate: No file chosen

☐ Enable Signing Certificate status checking
(Uses configuration in [Trusted Client CAs](#). This applies to the certificate configured above as well as the one comes along with the SAML response.)

Select Device Certificate for Signing: Certificate used for signing the Requests initiated by Connect Secure for the SAML Auth Server. Select "Not Applicable" if Request signing is not required.

Select Device Certificate for Encryption: Certificate used by the IdP for wrapping encryption keys for the SAML Auth Server. Select "Not Applicable" if encryption is not required.

Select Requested Authn Context Classes to be sent in the AuthRequest:

Available:

Selected:

Comparison Method for Authentication Classes:

Service Provider Metadata Settings

Metadata Validity: days 1 - 9999. Specifies the time in days after which metadata for the SAML Auth Server should be refreshed by the Identity Provider. This is used to populate the cache data in the generated metadata.

☐ Do Not Publish Connect Secure Metadata Prevents the Metadata for the SAML Auth Server to be published at the location specified by the Connect Secure Entity ID.

User Record Synchronization

☐ Enable User Record Synchronization

Logical Auth Server Name:

Table 7 Authentication Server Configuration Guidelines

Settings	Guidelines
Name	Specify a name for the configuration.
Type	Select AirWatch .
Server	

Settings	Guidelines
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.Awmdm.com</p> <p>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.awmdm.com/AirWatch/Devices/DeviceDetails/<deviceAttr.deviceId>">https://apidev.awmdm.com/AirWatch/Devices/DeviceDetails/<deviceAttr.deviceId></p>
Request Timeout	Specify a timeout period (5-60 seconds) for queries to the MDM server. The default is 15 seconds.
Administrator	
Username	Specify the username for an account that has privileges to access the AirWatch RESTful Web API.
Password	Specify the corresponding password.
Tenant Code	Copy and paste the AirWatch API tenant code. See Figure 9 .
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 - Not applicable for the AirWatch MDM. • Serial Number - The device serial number. • UDID - The device unique device identifier. This is supported by the AirWatch MDM. • IMEI - Not applicable for 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 shown in [Figure 55](#).
3. Complete the configuration as described in [Table 8](#).
4. Save the configuration.

Figure 9 Certificate Server Configuration Page

Pulse Secure System **Authentication**

Auth Servers > New Certificate Server

New Certificate Server

*Name: Label to r

User Name Template: Template

The template can contain textual characters as well as variables f
custom expressions and policy conditions. All of the certificate var

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 sub

▼ User Record Synchronization

☐ Enable User Record Synchronization

Logical Auth Server Name:

* indicates required field

Table 8 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 the 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>

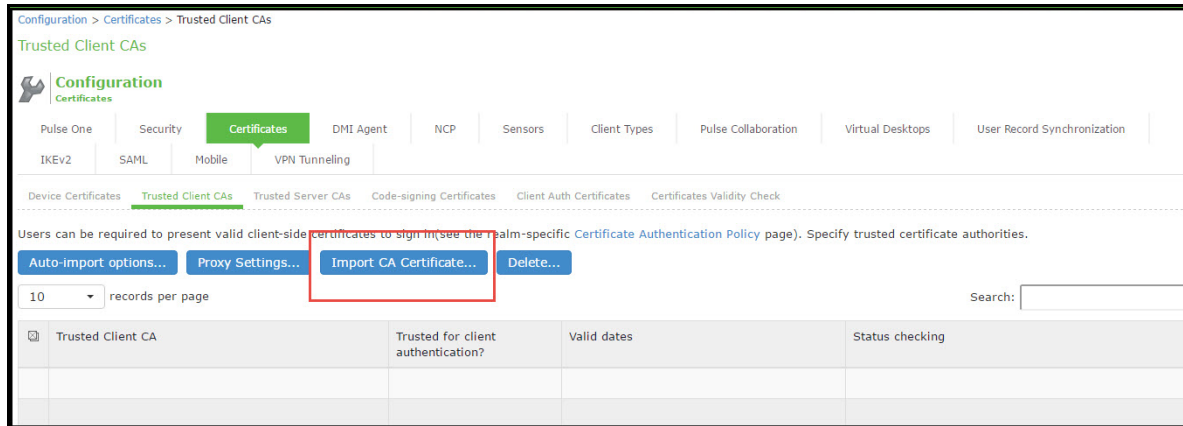
Adding the MDM Certificate to the Trusted Client CA Configuration

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:

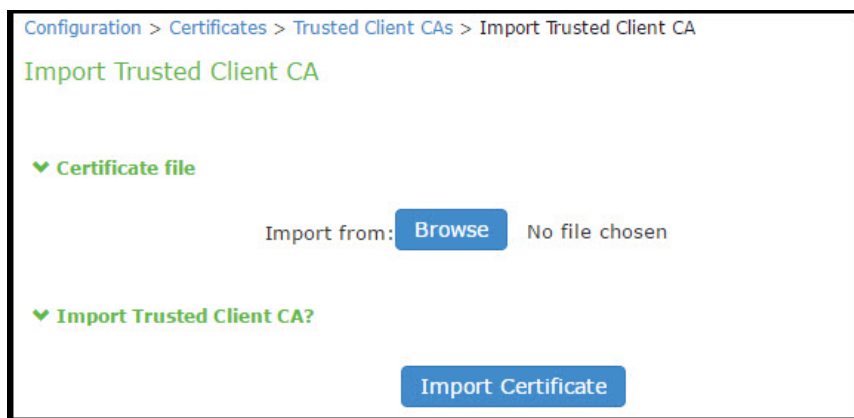
1. Select **System > Configuration > Certificates > Trusted Client CAs** to display the page shown in [Figure 10](#).

Figure 10 Trusted Client CA Management Page



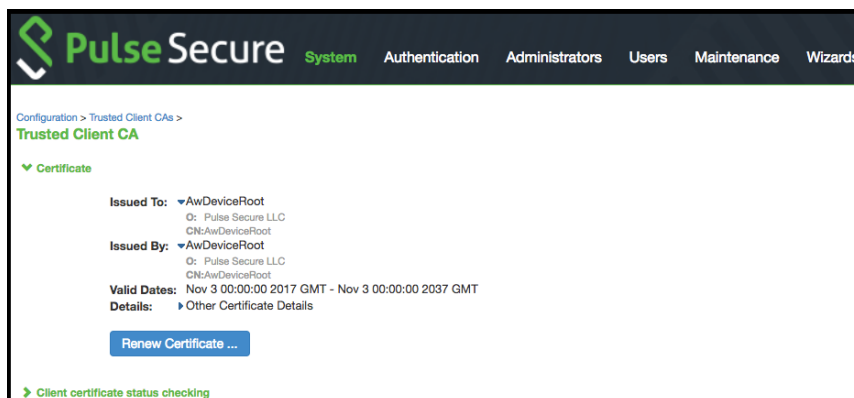
2. Click **Import CA Certificate** to display the page shown in [Figure 11](#).

Figure 11 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. [Figure 12](#) shows the configuration for this example.

Figure 12 Trusted Client CA Configuration for AirWatch



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 shown in [Figure 13](#)
3. Complete the configuration for general options as described in [Table 9](#).
4. Save the configuration.
5. Click **UI options** to display the configuration page shown in [Figure 14](#).
6. Complete the configuration for UI options as described in [Table 10](#).
7. Save the configuration.
8. Click **Session Options** to display the configuration page shown in [Figure 15](#).
9. Complete the configuration for session options as described in [Table 11](#).
10. Save the configuration.

Figure 13 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

☐ HTMLS 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 14 User Role Configuration Page - UI Options

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

User Roles > Comprehensive > 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: **Label**

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 user's bookmarks page. Note that all panels may not be displayed.

Left Column: **Move Up** **Move Down**

- Welcome
- Web Bookmarks
- Files
- Terminal Sessions
- Client Application Sessions
- Virtual Desktops

Right Column: **Move >** **Move <** **Move Up** **Move Down**

- HTML5 Access Sessions

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

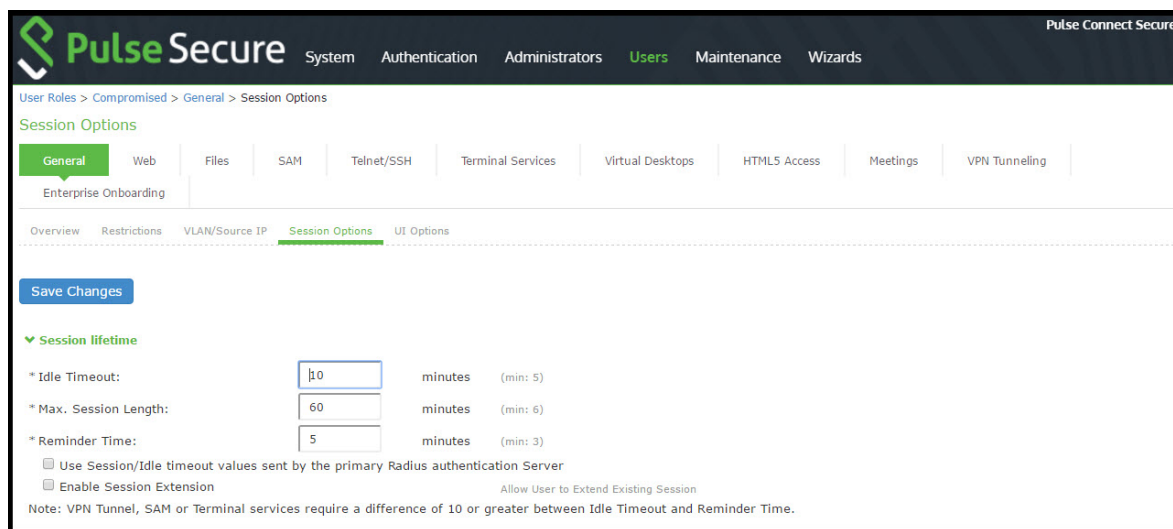
☒ Enable "Bookmark Favorites" link

☐ Display Session Counter

☒ Enable "Help" link

☐ Use IFrame in Toolbar

Figure 15 User Role Configuration Page - Session Options



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

User Roles > Compromised > General > Session Options

Session 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

▼ 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 9 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.</p> <p>In this example, we are using the system to enforce MDM enrollment by flagging compromised devices. The message, therefore, is:</p> <p><i>Your device is compromised. Network access may be limited.</i></p> <p>The message is forwarded to the device using the MDM server Push Notification feature.</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	
Session lifetime	Use the session lifetime options to establish the time limits that would require the user to sign in again.

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 shown in [Figure 16](#)
2. Complete the configuration as described in [Table 10](#).
3. Save the configuration.

Upon saving the new realm, the system displays the role mapping rules page.

4. Click **New Rule** to display the configuration page shown in [Figure 16](#)
5. Complete the configuration as described in [Table 10](#).
6. Save the configuration.
7. Click the **Authentication Policy** tab and then click the **Certificate** sub-tab to display the certificate restriction configuration page shown in [Figure 19](#)
8. Complete the configuration as described in [Table 10](#).
9. Save the configuration.

Figure 16 Realm Configuration Page

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

User Realms > tp-aw-mdm > General

General Authentication Policy Role Mapping

* Name: tp-aw-mdm
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: AirWatch Cert Auth
User Directory/Attribute: None
Accounting: None
Device Attributes: tp-aw-mdm

▼ Additional Authentication Server
☐ Enable additional authentication server

▼ Dynamic policy evaluation
☐ Enable dynamic policy evaluation

▼ Session Migration

► Other Settings

Save Changes

Table 10 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 configured in the VPN profile.
Description	Describe the purpose of the realm so that other administrators are aware of it.
Servers	

Settings	Guidelines
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	Do not select.
Accounting	Do not select.
Device Attributes	Select the MDM server configured in the earlier step.
Dynamic Policy Evaluation	
Dynamic Policy Evaluation	Do not select this option. A limitation for this release is that role evaluation occurs only when the user signs in. To force role reevaluation, you must force the users to sign in again.
Refresh interval	Do not select.
Refresh roles	Do not select.
Refresh resource policies	Do not select.
Session Migration	
Session Migration	Do not select this option. Session migration is useful for endpoints running Pulse Secure client software, which is not the case for the endpoints in this MDM example.

Figure 17 Role Mapping Configuration Page

Table 11 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	<p>Select a device attribute (see Table 11) and a logical operator (is or is not), and type a matching value or value pattern.</p> <p>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.</p>
Role assignment	Select the roles to apply if the data matches the rule.

Note: You likely are to create multiple roles and role-mapping rules to assign roles for different policy purposes. Your realm can have a set of rules based on user attribute, group membership, and device attribute. Be mindful that the user and device can map to multiple roles. Use stop rules and order your rules carefully to implement the policy that you want.

Table 12 describes the AirWatch record attributes that can be used in role mapping rules.

Table 12 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

Role Mapping Attribute Name	AirWatch Attribute Name	Description	Data Type
LocationGroupName	LocationGroupName	MDM location group configuration value.	String
macAddress	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
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

Note: By design, you should be able to specify true or false, or 1 or 0, for Boolean data types in your role mapping rules. Due to an issue in this release, you must use 1 for true and 0 for false.

Figure 18 Realm Configuration Page - Certificate Restrictions

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

User Realms > All Roles Realm - NC Client > Authentication Policy > Certificate

Certificate

General **Authentication Policy** Role Mapping

Source IP Browser **Certificate** Password Host Checker Limits

☒ Allow all users (no client-side certificate required)
☐ Allow all users and remember certificate information while user is signed in.
☐ 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.

You can optionally require specific values in the client certificate:

10 records per page

Certificate field (example "cn")	Expected value
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

[Save Changes](#)

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	<p>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.</p> <p>TIP: Without a certificate, device attributes cannot be determined, and the session can be mapped only to roles that do not require particular device attributes. You might use this option to grant restricted access or to send a notification that MDM enrollment is required for a greater level of access.</p>
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 shown in [Figure 20](#)
3. Complete the configuration as described in [Table 14](#).
4. Save the configuration.

Figure 19 Sign-In Policy Configuration Page

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

Signing In > Sign-In Policies > */mdm/

***/mdm/**

User type: ☒ Users ☐ Administrators ☐ Authorization Only Access

Sign-in URL: Format: <host>/<path>; Use * as wildcard in the beginning of the host name.

Description:

URL for signing in from user owned devices.

Sign-in page:

Default Sign-In Page

To create or manage pages, see [Sign-In pages](#).

Meeting URL:

Authentication realm

Specify how to select an authentication realm when signing in.

☒ **User types the realm name**
The user must type the name of one of the available authentication realms.

☐ **User picks from a list of authentication realms**
The user must choose one of the following selected authentication realms when they sign in. If only one realm is selected, it is automatically used (the sign-in page will not display the

Available realms:

Android_CloudSecure_Realm
iOS_CloudSecure_Realm
Mac_CloudSecure_Realm
Users
Windows_CloudSecure_Realm

Add -> Remove

Selected realms:

tp-aw-mdm

Move Up Move Down

Configure SignIn Notifications

☐ Pre-Auth Sign-in Notification

☐ Post-Auth Sign-in Notification

Save Changes

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	
User experience	Select one of the following options: <ul style="list-style-type: none"> • User types the realm name • User picks from a list of authentication realms
Realm	Select the realm you configured in the earlier step.
Configure Sign-in Notifications	
Pre-Auth Sign-in Notification	Not used in this scenario.
Post-Auth Sign-in Notification	Not used in this scenario.

Configuring a Resource Policy

A resource policy enforces role-based access to resources accessed during the SSL VPN session. You use the device access management framework to assign roles to devices, and you use the resource policy to deny access to resources that should not be downloaded onto a specific device platform—in this example, Android devices.

In this scenario, the role configuration and role mapping configuration create a classification for Android devices. [Figure 21](#) shows the user role configuration.

Figure 20 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

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

Save Changes

Figure 21 shows the role mapping configuration.

Figure 21 Role Mapping Configuration Page

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

User Realms > Users > Role Mapping > Role Mapping Rule

Role Mapping Rule

Rule based on: User attribute Update

* Name: Android

▼ Rule: If username...

is not *android* If more than one username should match, enter one username per line. You can use * wildcards.

▼ then assign these roles

Available Roles: Compromised test test1 Users WSAM Add -> Remove

Selected Roles: Android

☐ Stop processing rules when this rule matches


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

Save Changes Save + New

To configure a resource policy:

1. Select **Resource Policies > VPN Tunneling > Access Control** to display the access control policy configuration pages.
2. Click **New Policy** to display the configuration page shown in [Figure 22](#).
3. Complete the configuration as described in [Table 15](#).
4. Save the configuration.

Figure 22 Resource Access Policy Configuration Page

 **Pulse Secure**

SystemAuthenticationAdministratorsUsersMaintenanceWizards

Resource Policies > VPN Tunneling Access Control > New Policy

New Policy

* Name:

Financial Servers

Required: Label to refer

Description:

Do not allow employees to download Finance Server content on BYOD devices.

Resources

Specify the resources for which this policy applies, one per line.

* Resources:

10.10.10.0/24

Examples:
tcp://*:1-1024
tcp://*:80,443
udp://10.10.10.0/24:*
icmp://10.10.10.10/255.255.255.255
10.10.10.0/24

Roles

☒ Policy applies to ALL roles

☐ Policy applies to SELECTED roles

☐ Policy applies to all roles OTHER THAN those selected below

Available roles:

Compromised

Users

WSAM

test

test1

Add ->

Remove

Selected roles:

Android

Actions

☐ Allow access

☒ Deny access

☐ Use Detailed Rules (available after you click 'Save Changes')

Save Changes

Save as Copy

Table 15 Resource Access Policy Configuration Guidelines

Settings	Guidelines
Name	Specify a name for the configuration.

Settings	Guidelines
Description	Describe the purpose of the configuration so that other administrators are aware of it.
Resources	
Resources	Specify the resources for which this policy applies, one per line.
Roles	
Roles	Select the roles to which the policy applies. In this example, Android is selected.
Action	
Action	<p>Select one of the following actions:</p> <ul style="list-style-type: none"> • Allow Access • Deny Access • Use Detailed Rules <p>In this example, we deny access from Android devices.</p>

Deploying a BYOD Policy for MobileIron Managed Devices

This example shows how to use policies to enable security based on device identity, device posture, or user identity in a bring your own device (BYOD) environment for an enterprise that uses MobileIron® for mobile device management (MDM). It includes the following information:

- [“Requirements” on page 33](#)
- [“Configuring the MobileIron MDM Service” on page 33](#)
- [“Configuring the Device Access Management Framework” on page 39](#)
- [“Configuring a Resource Policy” on page 56](#)

Requirements

Table 16 lists version information for the solution components shown in this example.

Table 16 Component Version Information

Component	Version
Connect Secure	Release 8.0r1 or later is required.
MobileIron MDM	Release 5.6 is used in this example. Any version that supports the device ID and device attributes you plan to query is compatible.

Configuring the MobileIron MDM Service

This solution assumes you know how to configure and use the features of your MDM, and that you can enroll employees and their devices. For more information about the MobileIron MDM, refer to its documentation and support resources. 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 MobileIron, UUID is supported and recommended.
- **Device attributes** - A standard set of data maintained for each device. For MobileIron, see [Table 17](#).

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

Table 17 MobileIron Device Attributes

MobileIron Attribute	Normalized Connect Secure Name	Description	Data Type
@id	deviceId	Device identifier.	String
blockedReason	blockedReason	<ul style="list-style-type: none"> Reason MDM has blocked the device. Can be a multivalued string. Values are: AllowedAppControlPolicyOutOfCompliance AppControlPolicyOutOfCompliance DataProtectionNotEnabled DeviceAdminDeactivated DeviceComplianceStatusUnknown DeviceCompliant DeviceCompromised DeviceExceedsPerMailboxLimit DeviceManuallyBlocked DeviceNotRegistered DisallowedAppControlPolicyOutOfCompliance ExchangeReported HardwareVersionNotAllowed OsVersionLessThanSupportedOsVersion PolicyOutOfDate RequiredAppControlPolicyOutOfCompliance 	String

MobileIron Attribute	Normalized Connect Secure Name	Description	Data Type
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
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

MobileIron Attribute	Normalized Connect Secure Name	Description	Data Type
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
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)	macAddress	The Wi-Fi MAC address.	String

To configure the 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. See [Figure 23](#).

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 VPN configuration that specifies the Pulse Secure SSL connection type and the URL for the system sign-in page. See [Figure 24](#). During the enrollment process, this profile is provisioned to the device. Select the SCEP configuration completed in Step 1.
4. Select the VPN configuration and apply it to a group label you have provisioned to manage this group of devices. See [Figure 25](#).
5. Apply the group label to the devices when you add them to the MDM. See [Figure 26](#) 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 23 MobileIron SCEP Configuration

New SCEP Setting

Name:

Description:

Enable Proxy: ☒

☐ Cache locally generated keys

☐ User Certificate ☒ Device Certificate

Setting Type:

Local CAs:

Subject:

Subject Common Name Type:

Subject Alternative Name Type:

Subject Alternative Name Value:

Figure 24 MobileIron VPN Configuration

Modify VPN Setting

Save Cancel

Name: demo-SA-vpn

Description: Demo VPN Profile

Connection Type: SSL ⓘ

Server: sa4-eng.acmegizmo.com/de

User Name: \$USERID\$ ⓘ

Role:

Realm:

User Authentication: Certificate

Identity Certificate: Pulse Device Certificate

VPN on Demand: ☒

☐ Match Domain or Host **Connection Option**

Add New Delete

Proxy: None

Save Cancel

Figure 25 Applying the VPN Configuration to a Label

MobileIron ADMIN PORTAL

USERS & DEVICES APPS **POLICIES & CONFIGS** SETTINGS LOGS & EVENTS

Dashboard Configurations Policies Default Policies ActiveSync Policies Cor

Delete More Actions Add New Labels: All-Smartphones Search by User

Name	Setting Type	Bundle/Package ID	Descr...	# Phones	Labels	WatchList	Quarantined
pulseqa-client-auth	CERTIFICATE		client...	0		0	0
pulseqa-client-auth	CERTIFICATE		test	0		0	0
SDELANEY-T400-ca	CERTIFICATE			0		0	0
sumit-cn-email-cert-auth	CERTIFICATE		email...	0		0	0
Outlook Cloud	EMAIL			0		0	0
lprasad-uac-cert	SCEP		UAC...	1	AccessPoint_UAC_lprasad	0	0
Manoj-MobileIron-Int-CA-Cert	SCEP			0		0	0
<input checked="" type="checkbox"/> sa-148-vpn	VPN			5	sumit	1	0
sa-195-vpn	VPN			5	sumit	1	0
sa-53-vpn	VPN			5	sumit	1	0
sdelaney - VPN	VPN			0	Juniper - sdelaney	0	0
pbu-soln-wpa2	WIFI		Pulse...	0	mnreddy-devices	0	0

Figure 26 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' (highlighted), 'ActiveSync Associations', 'Labels', 'Users', and 'Retired Devices'. The main content area has a toolbar with 'Actions', '+ Add', 'Labels: All-Smartphones', 'Search by User or Device', 'Advanced Search', and 'Pending Device Report'. A dropdown menu for '+ Add' is open, showing 'Single Device' and 'Multiple Devices'. Below the menu is a table of registered devices.

	User	Phone	OS	Country	Status	Registered on Date	Last Check-In	E/C	Open
	Pulse T	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&

Configuring the Device Access Management Framework

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

- “Configuring the MDM Authentication Server” on page 39
- “Configuring the Certificate Server” on page 41
- “Adding the MDM Certificate to the Trusted Client CA Configuration” on page 15
- “Configuring User Roles” on page 17
- “Configuring a Realm and Role Mapping Rules” on page 20
- “Configuring a Sign-In Policy” on page 28


Configuring the MDM Authentication Server

The MDM authentication server configuration is used by the system 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 shown in [Figure 27](#).
3. Complete the configuration as described in [Table 18](#).
4. Save the configuration.

Figure 27 Authentication Server Configuration Page

 **Pulse Secure**

System **Authentication** Administrators Users Maintenance Wizards

Auth Servers > New MDM Server

New MDM Server

*Name: Label to reference this server.

Type: ☐ Air Watch ☒ Mobile Iron

▼ Server

* Server Url:

Viewer Url:

For example: https://m.mobileiron.net/<Enterprise Name>/admin/admin.html#smartphones:all

* Request Timeout:

▼ Administrator

* Username:

* Password:

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 request 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>. All of the certificate variables are available.

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

ID Type: ☒ UUID ☐ Serial Number ☐ UDID

Universal Unique Identifier

Unique Device Identifier

Save Changes Reset

Table 18 Authentication Server Configuration Guidelines

Settings	Guidelines
Name	Specify a name for the configuration.
Type	Select MobileIron.
Server	
Server Url	<div>Specify the URL for your MobileIron server. This is the URL MobileIron has instructed you to use to access its RESTful Web API (also called a RESTful Web service). The URL for the MobileIron server used in this example has the following form:</div> <div>https://m.mobileiron.net/pulsesecuretest</div> <div>Note: You must configure your firewalls to allow communication between these two nodes over port 443.</div>

© 2020 Pulse Secure, LLC.

40

Settings	Guidelines
Viewer Url	Specify the URL for the MobileIron report viewer. This URL is used for links from the Active Users page to the MobileIron report viewer. The URL for the MobileIron viewer for this example has the following form: https://m.mobileiron.net/pulsesecuretest/admin/admin.html#smartphones:all
Request Timeout	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.
Administrator	
Username	Specify the username for an account that has privileges to access the MobileIron RESTful Web API.
Password	Specify the corresponding password.
Device Identifier	
ID Template	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>. For example, suppose the certificate DN is: CN=<DEVICE_UDID>, uid=<USER_ID>, o=Company. With this configuration, the certificate could identify both the user and the device. In this example, the device ID template is <certDN.CN>.
ID Type	Select the device identifier type that matches the selection in the MDM certificate configuration: <ul style="list-style-type: none"> • UUID-Not applicable for the MobileIron MDM. • Serial Number-The device serial number. • UDID-The device unique device identifier. This is supported by the MobileIron 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**.
3. Complete the configuration as described in [Table 19](#).
4. Save the configuration.

Table 19 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 the 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=<DEVICE_UDID>, uid=<USER_ID>, o=Company. With this configuration, the certificate could identify both the user and the device. In this example, the username template is <certDN.UID>.</p>

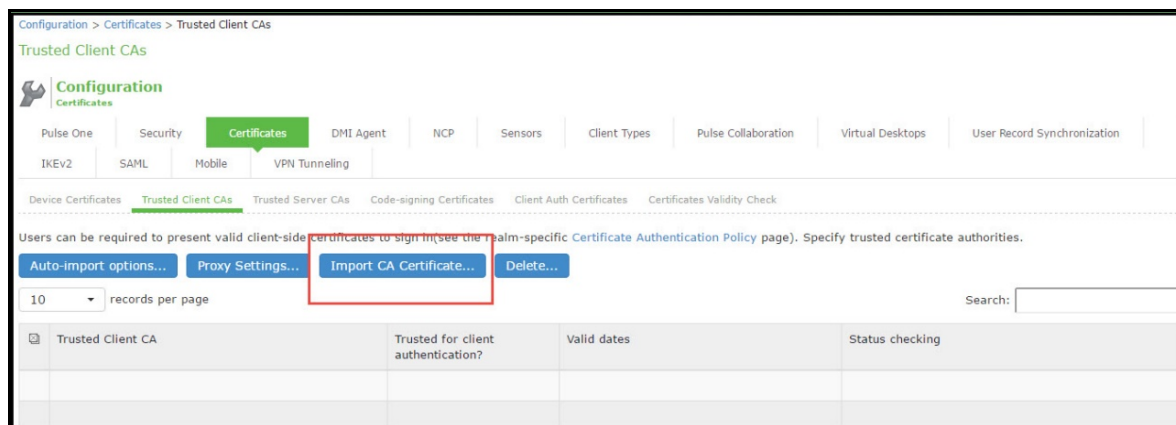
Adding the MDM Certificate to the Trusted Client CA Configuration

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:

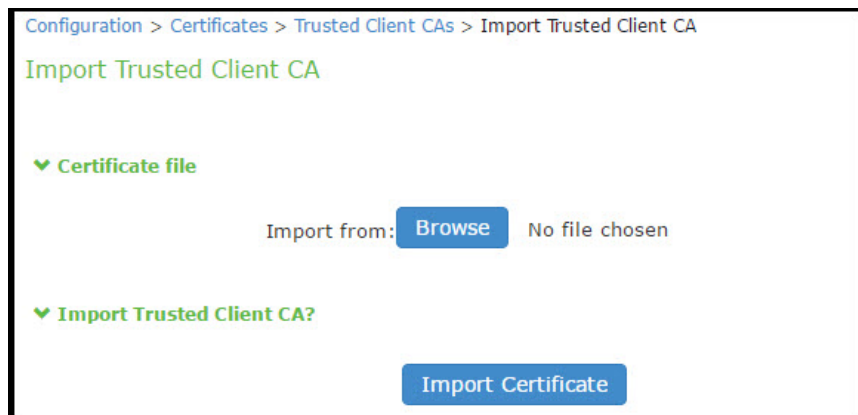
1. Select **System > Configuration > Certificates > Trusted Client CAs** to display the page shown in [Figure 28](#).

Figure 28 Trusted Client CA Management Page



2. Click **Import CA Certificate** to display the page shown in [Figure 29](#).

Figure 29 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. Figure 30 shows the configuration for this example.

Figure 30 Trusted Client CA Configuration for MobileIron



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 non-compliant; 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 shown in Figure 31.
3. Complete the configuration for general options as described in Table 20.

4. Save the configuration.
5. Click **UI options** to display the configuration page shown in [Figure 32](#).
6. Complete the configuration for UI options as described in [Table 20](#).
7. Save the configuration.
8. Click **Session Options** to display the configuration page shown in [Figure 33](#).
9. Complete the configuration for session options as described in [Table 20](#).
10. Save the configuration.

Figure 31 User Role Configuration Page - General Settings

PulseSecure System Authentication Administrators **Users** Maintenance Wizards

User Roles > New Role

New Role

Name: Compromised

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

☐ Secure Mail

☐ Enterprise Onboarding (VPN, Wifi and Certificate Profiles)

[Save Changes](#)

Figure 32 User Role Configuration Page - UI Options

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

User Roles > Comprehensive > 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: No file chosen Recommended size: Less than 40 pixels tall and 10KB.

Background color: #E3E3E3

Sub headers

Current appearance:

Background color: #336699

Text color: #FFFFFF

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 user's bookmarks page. Note that all panels may not be displayed.

Left Column: Welcome Web Bookmarks Files Terminal Sessions Client Application Sessions Virtual Desktops

Right Column: HTML5 Access Sessions

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.

Browning 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: No file chosen Recommended size: Less than 24 pixels tall and 6KB

Toolbar logo (mobile): 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 33 User Role Configuration Page - Session Options

Table 20 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.</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>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	
Session lifetime	Use the session lifetime options to establish the time limits that would require the user to sign in again.

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 shown in [Figure 34](#).
2. Complete the configuration as described in [Table 21](#).
3. Save the configuration.

Upon saving the new realm, the system displays the role mapping rules page.

4. Click **New Rule** to display the configuration page shown in [Figure 35](#).
5. Complete the configuration as described in [Table 21](#).
6. Save the configuration.
7. Click the **Authentication Policy** tab and then click the Certificate subtab to display the certificate restriction configuration page shown in [Figure 36](#).
8. Complete the configuration as described in [Table 21](#).
9. Save the configuration.

Figure 34 Realm Configuration Page

The screenshot shows the Pulse Secure web interface for configuring a realm. The breadcrumb trail is "User Realms > tp-mobileiron-mdm > General". The "General" tab is selected, with sub-tabs for "General", "Authentication Policy", and "Role Mapping".

General

- Name: tp-mobileiron-mdm
- Description: (empty text area)
- ☐ 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: Mobileiron Cert Auth
- User Directory/Attribute: None
- Accounting: None
- Device Attributes: tp-mobileiron

Additional Authentication Server

- ☐ Enable additional authentication server

Dynamic policy evaluation

- ☐ Enable dynamic policy evaluation

Session Migration

Other Settings

[Save Changes](#)

Table 21 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 configured in the VPN profile. See Figure 75.
Description	Describe the purpose of the realm so that other administrators are aware of it.
Servers	

Settings	Guidelines
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	Do not select.
Accounting	Do not select.
Device Attributes	Select the MDM server configured in the earlier step.
Dynamic Policy Evaluation	
Dynamic Policy Evaluation	Do not select this option. A limitation for this release is that role evaluation occurs only when the user signs in. To force role reevaluation, you must force the users to sign in again.
Refresh interval	Do not select.
Refresh roles	Do not select.
Refresh resource policies	Do not select.
Session Migration	
Session Migration	Do not select this option. Session migration is useful for endpoints running Pulse Secure client software, which is not the case for the endpoints in this MDM example.

Figure 35 Role Mapping Configuration Page

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

User Realms > tp-mobileiron-mdm > Role Mapping > Role Mapping Rule

Role Mapping Rule

Rule based on: Device attribute Update

* Name: Compromised

▼ Rule: If device has any of the following attribute values...

Attribute: complianceReason Attributes...

is DeviceCompromised If more than one value for this attribute should match, enter one per line. You can use * wildcards.

▼ then assign these roles

Available Roles: Add -> Remove

- Android_CloudSecure_Role
- CloudSecure_Remedy_Role
- iOS_CloudSecure_Role
- Mac_CloudSecure_Role
- Users
- Windows_CloudSecure_Role

Selected Roles: Compromised

☐ Stop processing rules when this rule matches

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

Save Changes Save + New

*indicates required field

Table 22 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	<p>Select a device attribute (see Table 26) and a logical operator (is or is not), and type a matching value or value pattern.</p> <p>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.</p>
Role assignment	Select the roles to apply if the data matches the rule.

Note: You likely are to create multiple roles and role-mapping rules to assign roles for different policy purposes. Your realm can have a set of rules based on user attribute, group membership, and device attribute. Be mindful that the user and device can map to multiple roles. Use stop rules and order your rules carefully to implement the policy that you want.

Table 23 describes the MobileIron record attributes that can be used in role mapping rules.

Table 23 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

Role Mapping Attribute Name	MobileIron Attribute Name	Description	Data Type
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
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 MDN; 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
macAdress	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 	String
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

Note: By design, you should be able to specify true or false, or 1 or 0, for Boolean data types in your role mapping rules. Due to an issue in this release, you must use 1 for true and 0 for false

Figure 36 Realm Configuration Page - Certificate Restrictions

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

User Realms > tp-mobileiron-mdm > Authentication Policy > Certificate

Certificate

General **Authentication Policy** Role Mapping

Source IP Browser **Certificate** Host Checker Limits

☐ Allow all users (no client-side certificate required)
☐ Allow all users and remember certificate information while user is signed in.
☒ 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.

You can optionally require specific values in the client certificate:

10 records per page Search:

Certificate field (example "cn")	Expected value	
<input type="text"/>	<input type="text"/>	Add
<input type="text"/>	<input type="text"/>	
<input type="text"/>	<input type="text"/>	
<input type="text"/>	<input type="text"/>	

Save Changes

← Previous 1 Next →

Table 24 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	<p>If you select this option, the system requests a client certificate during the TLS handshake. If the realm has been configured with a user authentication server, 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.</p> <p>Without a certificate, device attributes cannot be determined, and the session can be mapped only to roles that do not require particular device attributes. You might use this option to grant restricted access or to send a notification that MDM enrollment is required for a greater level of access.</p>
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 shown in [Figure 37](#)
3. Complete the configuration as described in [Table 26](#)
4. Save the configuration.

Figure 37 Sign-In Policy Configuration Page

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

Signing In > Sign-in Policies > */mdm/

***/mdm/**

User type: ☒ Users ☐ Administrators ☐ Authorization Only Access

Sign-in URL: Format: <host>/<path>/; Use * as wildcard in the beginning of the host name.

Description:

Sign-in page: To create or manage pages, see [Sign-In pages](#).

Meeting URL:

Authentication realm

Specify how to select an authentication realm when signing in.

☐ **User types the realm name**
The user must type the name of one of the available authentication realms.

☒ **User picks from a list of authentication realms**
The user must choose one of the following selected authentication realms when they sign in. If only one realm is selected, it is automatically used (the sign-in page will not display the realms).

Available realms:

- Android_CloudSecure_Realm
- iOS_CloudSecure_Realm
- Mac_CloudSecure_Realm
- Users
- Windows_CloudSecure_Realm

Selected realms:

- tp-mobileiron-mdm

Configure SignIn Notifications

☐ Pre-Auth Sign-in Notification

☐ Post-Auth Sign-in Notification

Table 25 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	
User experience	Select one of the following options: <ul style="list-style-type: none"> User types the realm name User picks from a list of authentication realms
Realm	Select the realm you configured in the earlier step.
Configure Sign-in Notifications	
Pre-Auth Sign-in Notification	Not used in this scenario.
Post-Auth Sign-in Notification	Not used in this scenario.

Configuring a Resource Policy

A resource policy enforces role-based access to resources accessed during the SSL VPN session. You use the device access management framework to assign roles to devices, and you use the resource policy to deny access to resources that should not be downloaded onto a specific device platform—in this example, Android devices.

In this scenario, the role configuration and role mapping configuration create a classification for Android devices. [Figure 38](#) shows the user role configuration.

Figure 38 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

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

Save Changes

Figure 39 shows the role mapping configuration.

Figure 39 Role Mapping Configuration Page

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

User Realms > tp-mobileiron-mdm > Role Mapping > Role Mapping Rule

Role Mapping Rule

* Name:

▼ Rule: If device has any of the following attribute values...

Attribute:

If more than one value for this attribute should match, enter one per line. You can use * wildcards.

▼ then assign these roles

Available Roles:

- Android_CloudSecure_Role
- CloudSecure_Removed_Role
- Compromised
- iOS_CloudSecure_Role
- Mac_CloudSecure_Role
- Users

Selected Roles:

- Android

☐ Stop processing rules when this rule matches

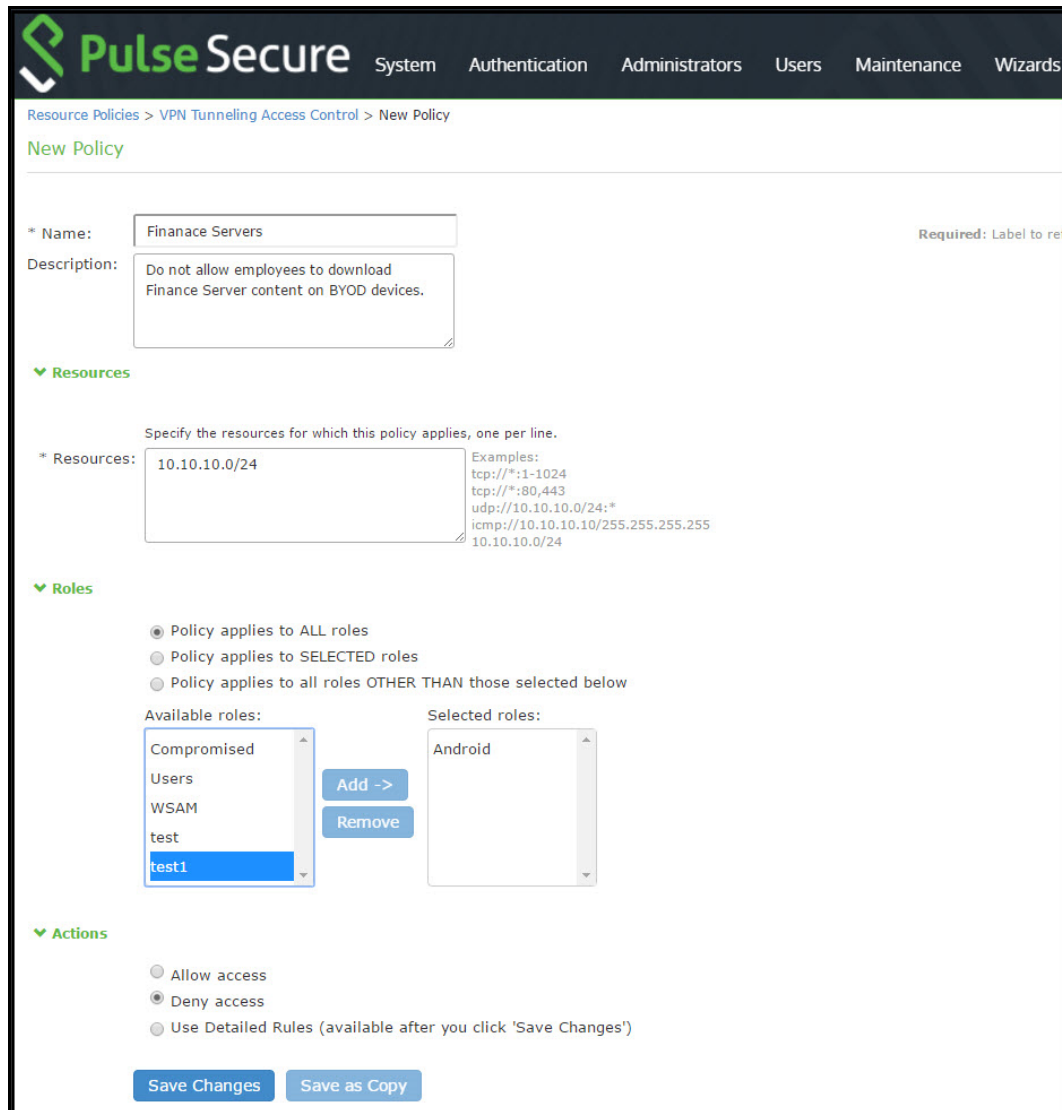
To manage roles, see the [Roles](#) configuration page.

*indicates required field

To configure a resource policy:

1. Select **Resource Policies > VPN Tunneling > Access Control** to display the access control policy configuration pages.
2. Click **New Policy** to display the configuration page shown in [Figure 40](#)
3. Complete the configuration as described in [Table 26](#).
4. Save the configuration.

Figure 40 Resource Access Policy Configuration Page



The image shows the Pulse Secure web interface for configuring a new Resource Access Policy. The page has a dark header with the Pulse Secure logo and navigation tabs: System, Authentication, Administrators, Users, Maintenance, and Wizards. Below the header, a breadcrumb trail reads: Resource Policies > VPN Tunneling Access Control > New Policy. The main content area is titled "New Policy" and contains several sections:

- Name:** A text input field containing "Finanace Servers". A note on the right says "Required: Label to ref".
- Description:** A text area containing "Do not allow employees to download Finance Server content on BYOD devices."
- Resources:** A section with a green arrow icon. It includes a text input field with "10.10.10.0/24" and a list of examples: tcp://*:1-1024, tcp://*:80,443, udp://10.10.10.0/24:*, icmp://10.10.10.10/255.255.255.255, and 10.10.10.0/24.
- Roles:** A section with a green arrow icon. It contains three radio buttons: "Policy applies to ALL roles" (selected), "Policy applies to SELECTED roles", and "Policy applies to all roles OTHER THAN those selected below". Below these are two lists: "Available roles" (Compromised, Users, WSAM, test, test1) and "Selected roles" (Android). There are "Add ->" and "Remove" buttons between the lists.
- Actions:** A section with a green arrow icon. It contains three radio buttons: "Allow access", "Deny access" (selected), and "Use Detailed Rules (available after you click 'Save Changes')".

At the bottom of the form are two buttons: "Save Changes" and "Save as Copy".

Table 26 Resource Access Policy Configuration Guidelines

Settings	Guidelines
Name	Specify a name for the configuration.
Description	Describe the purpose of the configuration so that other administrators are aware of it.
Resources	
Resources	Specify the resources for which this policy applies, one per line.
Roles	
Roles	Select the roles to which the policy applies. In this example, Android is selected.
Action	
Action	<p>Select one of the following actions:</p> <ul style="list-style-type: none"> • Allow Access • Deny Access • Use Detailed Rules <p>In this example, we deny access from Android devices.</p>

Using Logs to Verify Proper Configuration

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.

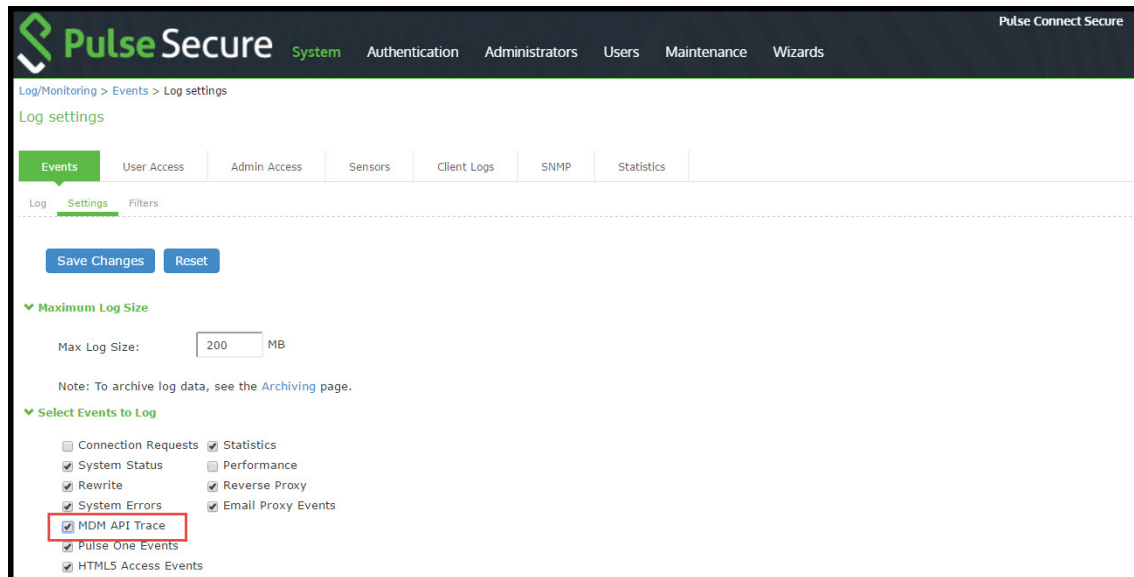
To enable logging for MDM API calls:

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

Figure 41 shows the configuration page for Pulse Connect Secure.

4. Enable logging for MDM API events and save the configuration.

Figure 41 Events Log Settings Configuration Page - Pulse Connect Secure



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.

Figure 42 shows the Events log for Pulse Connect Secure.

Figure 42 Events Log - Pulse Connect Secure

Pulse Secure System Authentication Administrators Users Maintenance Wizards

Pulse Connect Secure on cl62

Log/Monitoring > Events > Logs

Logs

Events User Access Admin Access Sensors Client Logs SNMP Statistics Advanced Settings

Log Settings Filters

View by filter: Standard:Standard (default) Show 200 items

Edit Query:

Update Reset Query Save Query...

Save Log As... Clear Log Save All Logs Clear All Logs

Filter: Standard (default)
Date: Oldest to Newest
Query:
Export Format: Standard

Severity	ID	Message
Critical	SYS30913	2018-02-02 02:18:03 - cl62 - [127.0.0.1] System() - Active Directory authentication server 'AD Server': Domain trust check failed. Administrator may need to rejoin to the domain.
Critical	SYS30913	2018-02-02 02:18:03 - cl62 - [127.0.0.1] System() - Active Directory authentication server 'AD-pcstltan': Domain trust check failed. Administrator may need to rejoin to the domain.
Critical	SYS30913	2018-02-02 02:18:03 - cl62 - [127.0.0.1] System() - Active Directory authentication server 'AD Server1': Domain trust check failed. Administrator may need to rejoin to the domain.
Critical	SYS30913	2018-02-02 02:15:03 - cl62 - [127.0.0.1] System() - Active Directory authentication server 'AD Server': Domain trust check failed. Administrator may need to rejoin to the domain.
Critical	SYS30913	2018-02-02 02:15:03 - cl62 - [127.0.0.1] System() - Active Directory authentication server 'AD-pcstltan': Domain trust check failed. Administrator may need to rejoin to the domain.

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.

Figure 43 shows the User Access log for Pulse Connect Secure.

Figure 43 User Access Log

Pulse Secure System Authentication Administrators Users Maintenance Wizards

Log/Monitoring > User Access > Logs

Logs

Events **User Access** Admin Access Sensors Client Logs SNMP Statistics

Log Settings Filters

View by filter: Standard:Standard (default) Show 200 Items

Edit Query:

Update Reset Query Save Query...

Save Log As... Clear Log Save All Logs Clear All Logs

Filter: Standard (default)
Date: Oldest to Newest
Query:
Export Format: Standard

Severity	ID	Message
Info	AUT23457	2016-03-14 23:50:29 - ive - [172.20.24.28] admin(Users)[] - Login failed using auth server System Local (Local Authentication). Reason: Failed
Info	AUT24327	2016-03-14 23:50:29 - ive - [172.20.24.28] admin(Users)[] - Primary authentication failed for admin/System Local from 172.20.24.28
Info	AUT23457	2016-02-29 05:14:23 - ive - [172.20.24.23] admin(Users)[] - Login failed using auth server System Local (Local Authentication). Reason: Failed
Info	AUT24327	2016-02-29 05:14:23 - ive - [172.20.24.23] admin(Users)[] - Primary authentication failed for admin/System Local from 172.20.24.23
Info	AUT23457	2016-02-29 05:14:08 - ive - [172.20.24.23] admin(Users)[] - Login failed using auth server System Local (Local Authentication). Reason: Short Password
Info	AUT23277	2016-02-29 05:14:08 - ive - [172.20.24.23] admin(Users)[] - Testing Password realm restrictions failed for admin/Users
Info	ERR24670	2016-02-21 20:14:55 - ive - [127.0.0.1] System()[] - VPN Tunneling: ACL count = 0.
Info	AUT23457	2016-02-18 09:13:55 - ive - [172.20.24.20] admin(Users)[] - Login failed using auth server System Local (Local Authentication). Reason: Failed
Info	AUT24327	2016-02-18 09:13:55 - ive - [172.20.24.20] admin(Users)[] - Primary authentication failed for admin/System Local from 172.20.24.20
Info	AUT23457	2016-02-09 21:43:11 - ive - [172.20.24.25] admin(Users)[] - Login failed using auth server System Local (Local Authentication). Reason: Failed
Info	AUT24327	2016-02-09 21:43:11 - ive - [172.20.24.25] admin(Users)[] - Primary authentication failed for admin/System Local from 172.20.24.25
Info	AUT23457	2016-02-09 21:41:11 - ive - [172.20.24.25] admin(Users)[] - Login failed using auth server System Local (Local Authentication). Reason: Failed

Using Policy Tracing and Debug Logs

This topic describes the troubleshooting tools available to diagnose issues. It includes the following information:

- “Using Policy Tracing to Troubleshoot Access Issues” on page 63
- “Using the Debug Log” on page 64

Using Policy Tracing to Troubleshoot Access Issues

It is common to encounter a situation where the system denies a user access to the network or to resources, and the user logs a trouble ticket. You can use the policy tracing utility and log to determine whether the system is working as expected and properly restricting access, or whether the user configuration or policy configuration needs to be updated to enable access in the user's case.

To create a policy trace log:

1. Select **Troubleshooting > User Sessions > Policy Tracing** to display the configuration page.
2. Specify the username, realm, and source IP address if you know it. If you provide the source IP address, the policy trace log can include events that occur before the user ID is entered into the system.
3. Select the events to trace, typically all but **Host Enforcer** and **IF-MAP**, unless you have enabled those features.
4. Click **Start Recording**.
5. Initiate the action you want to trace, such as a user sign in.
6. Click **View Log** to display the policy trace results log.

- Click **Stop Recording** when you have enough information.

Figure 44 shows policy trace results.

Figure 44 Policy Tracing Results

Current Policy Trace Log		
Date:	Earliest Date to Latest Date	
User Name:	devuser	
Realm Name:	LDAPServer	
Export Format:	Standard	
Show:	1000 items	<input type="button" value="Update"/> <input type="button" value="Save Log As..."/> <input type="button" value="Clear Log"/>
Severity	ID	Message
Info	PTR10103	2017/11/13 23:08:13 - cl62 - [172.21.8.78] - leema(Admin Users[Administrators] - devuser:LDAPServer - Policy Tracing turned on
Info	PTR23328	2017/11/13 23:08:21 - cl62 - [172.21.8.78] - devuser(LDAPServer[]) - User "devuser" starting sign-in to realm LDAPServer
Info	PTR23333	2017/11/13 23:08:21 - cl62 - [172.21.8.78] - devuser(LDAPServer[]) - Sign-in prompt username = "devuser"
Info	PTR23331	2017/11/13 23:08:21 - cl62 - [172.21.8.78] - devuser(LDAPServer[]) - Sign-in browser = "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.89 Safari/537.36"
Info	PTR23331	2017/11/13 23:08:21 - cl62 - [172.21.8.78] - devuser(LDAPServer[]) - Sign-in Preferred Language = "en"
Info	PTR23331	2017/11/13 23:08:21 - cl62 - [172.21.8.78] - devuser(LDAPServer[]) - Sign-in URL = "/"test/"
Info	PTR23331	2017/11/13 23:08:21 - cl62 - [172.21.8.78] - devuser(LDAPServer[]) - Sign-in host name = "10.209.113.62"
Info	PTR23331	2017/11/13 23:08:21 - cl62 - [172.21.8.78] - devuser(LDAPServer[]) - Sign-in host address = "10.209.113.62"
Info	PTR23331	2017/11/13 23:08:21 - cl62 - [172.21.8.78] - devuser(LDAPServer[]) - Sign-in network interface = "internal"
Info	PTR23331	2017/11/13 23:08:21 - cl62 - [172.21.8.78] - devuser(LDAPServer[]) - Sign-in time zone offset = "330"
Info	PTR23333	2017/11/13 23:08:21 - cl62 - [172.21.8.78] - devuser(LDAPServer[]) - Sign-in prompt password = "*****"
Info	PTR23370	2017/11/13 23:08:21 - cl62 - [172.21.8.78] - devuser(LDAPServer[]) - Attempting to authenticate user "devuser" with auth server "ldap"

Using the Debug Log

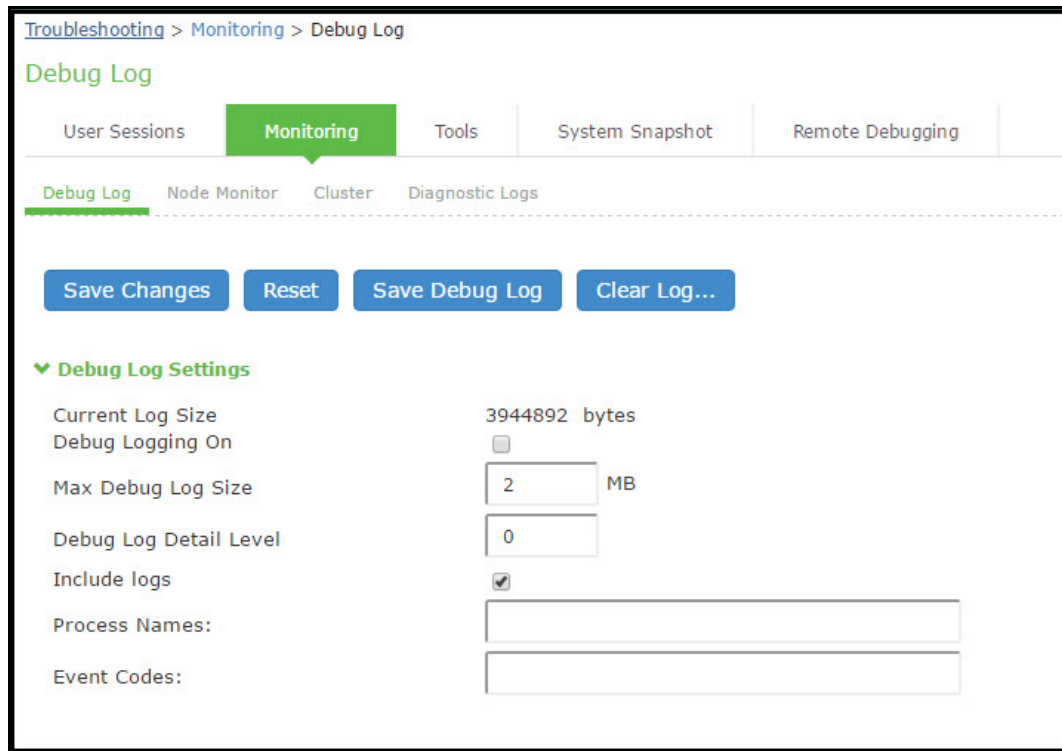
The Pulse Secure Global Support Center (PSGSC) might direct you to create a debug log to assist them in helping you debug an issue with the system. The debug log is used only by Pulse Secure Global Support Center.

In 9.1R3 release, the last-hit timestamp is included in each debug log statement. This timestamp helps the support in debugging and correlating timings of certain critical logs in some events.

To use debug logging:

- Select **Troubleshooting > Monitoring > Debug Log** to display the configuration page.
Figure 45 shows the configuration page for Pulse Connect Secure.
- Complete the configuration as described in Table 27.
- Click **Save Changes**. When you save changes with Debug Logging On selected, the system begins generating debug log entries.
- 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.
- Click **Save Debug Log** to save the debug log to a file that you can send to Pulse Secure Global Support Center. You can clear the log after you have saved it to a file.
- Clear the **Debug Logging On** check box and click **Save Changes** to turn off debug logging.

Figure 45 Debug Logging Configuration Page



Troubleshooting > Monitoring > Debug Log

Debug Log

User Sessions | **Monitoring** | Tools | System Snapshot | Remote Debugging

Debug Log | Node Monitor | Cluster | Diagnostic Logs

Save Changes | Reset | Save Debug Log | Clear Log...

▼ Debug Log Settings

Current Log Size 3944892 bytes

Debug Logging On ☐

Max Debug Log Size MB

Debug Log Detail Level

Include logs ☒

Process Names:

Event Codes:

Table 27 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 Pulse Secure Global Support Center.
Include logs	Select this option to include system logs in the debug log file. Recommended.
Process Names	Specify the process name. Obtain this from Pulse Secure Global Support Center.
Event Codes	Specify the event code. Obtain this from Pulse Secure Global Support Center. For MDM integration issues, Pulse Secure Global Support Center typically likes to collect debugging information for codes MDM, Auth, agentman, and Realm. The text is not case sensitive.