

BYOD Policy for Microsoft Intune Devices - Deployment Guide

Published**15 May 2020**Document Version**1.0.1**

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.

BYOD Policy for Microsoft Intune Devices - 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.

Revision History

The following table lists changes made to this document:

Document Revision	Release	Date	Feature	Changes
1.0.1	PCS 9.1R5	May 2020	Update	Updated the "Supported Platforms" section.
				Updated the "Configuring PCS with Microsoft Intune" section.
				Updated logging screens.
1.0	PCS 9.1R5	April 2020	Initial release	Initial release

Contents

Revision History	3
Contents	4
	5
I INDERSTANDING THE DEVICE ACCESS MANAGEMENT ERAMEWORK	5
	5
JOLUTION OVERVIEW	/
DEPLOYING A BYOD POLICY FOR MICROSOFT INTUNE MANAGED DEVICES	9
Requirements	9
Supported Devices	9
Configuring the Microsoft Intune MDM Service	9
Configuring PCS with Microsoft Intune	16
Configuring the Microsoft Intune MDM Server	20
USING LOGS TO VERIFY PROPER CONFIGURATION	27
Using Policy Tracing and Debug Logs	29

Introduction

•	Understanding the Device Access Management Framework	5
•	Solution Overview	7
•	Deploying a BYOD Policy for Microsoft Intune Managed Devices	9
•	Using Logs to Verify Proper Configuration	27
•	Using Policy Tracing and Debug Logs	29

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	 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.

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.

Table 3 Policy Reevaluation

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 Microsoft Intune 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 Microsoft Intune[®] for mobile device management (MDM). It includes the following information:

- "Requirements" on page 9
- "Supported Devices" on page 9
- "Configuring the Microsoft Intune MDM Service" on page 9
- "Configuring PCS with Microsoft Intune" on page 16
- "Configuring the Microsoft Intune MDM Server" on page 20

Requirements

Table 5 lists version information for the solution components shown in this example.

Table 5Component Version Information

Component	Version
Connect Secure	Release 9.1R5 or later is required.
Microsoft Intune MDM	Release version 2002 is used in this example. Any version that supports the device ID and device attributes you plan to query is compatible.

Supported Devices

- Google Android 8.0 and later
- Apple iOS 11.0 and later

Configuring the Microsoft Intune MDM Service

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 PCS role mapping that is the basis for network access and resource access policies. When you configure role-mapping rules, you specify the normalized attribute name.

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

Table 6Microsoft Intune Device Attributes

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

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. Create trusted certificate profiles in Intune. For detailed steps, refer to the **procedure** in the Microsoft Intune document.

\equiv Microsoft Azure	• Search resources, services, and docs (G+/)		Σ
Home > Microsoft Intune > Device configu	ration - Profiles > ANDROID_TRUST - Properties >	Trusted Certificate	
ANDROID_TRUST - Properties Device configuration profile	« ×	Trusted Certificate Android Enterprise	\Box ×
✓ Search (Ctrl+/) «	🖫 Save 🗙 Discard	* Certificate file : CA CERT.cer	
1 Overview	Name *	A valid .cer file *	
M	ANDROID_TRUST	Select a file	E
Manage	Description		
HI Properties	Enter a description 🗸		
Assignments			
Monitor	Platform		
Device status	Android Enterprise \checkmark		
User status	Profile type		
Per-setting status	Trusted certificate \checkmark		
	Settings		
	1 configured		
	Scope (Tags)		
	1 scope(s) selected		
		ОК	

Figure 3 Create Trusted Certificate - Android

𝒫 Search resources, services, and docs (G+/) 5. R Microsoft Azure Home > Microsoft Intune > Device configuration - Profiles > TRUST_IOS - Properties > Trusted Certificate TRUST_IOS - Properties Device configuration profile « X **Trusted Certificate** $\Box \times$ iOS/iPadOS \Box Save \times Discard * Certificate file : CA CERT.cer Name * Overview A valid .cer file * TRUST_IOS Select a file Manage Description H Properties Enter a description... Assignments Monitor Platform iOS/iPadOS Device status User status Profile type Trusted certificate Per-setting status Settings > 1 configured Scope (Tags) > 1 scope(s) selected

Figure 4 Create Trusted Certificate - iOS

2. Create and assign SCEP certificate profiles in Intune. For detailed steps, refer to the **procedure** in Microsoft Intune document.

Microsoft Azure ∑ Q > ANDROID_SCEP - Properties > SCEP Certificate × ANDROID_SCEP - Properties \ll \times SCEP Certificate $\Box \rightarrow$ \square Save imes Discard Certificate type 🕕 User \sim Name * ANDROID_SCEP Overview * Subject name format 🕕 IMEI number \sim Last Modified Assigned Manage Subject alternative name ③ Description User principal name (UPN) \sim No 02/3/20, 12:22 pm Properties * Certificate validity period 💿 Years 🗸 1 No 02/3/20, 11:38 am Assignments No 02/3/20, 12:00 pm * Key usage 🕕 Digital signature \sim Monitor Yes 02/3/20, 11:09 am ••• Platform * Key size (bits) 🕕 2048 \sim Device status Android Enterpris Yes 29/2/20, 6:36 pm * Hash algorithm 🕕 SHA-2 User status \sim Yes 02/3/20, 11:10 am Profile type Per-setting status SCEP certificat *Root Certificate ① No 04/6/19, 2:26 pm > Certificates ANDROID_TRUST No 09/8/19, 11:08 pm Settings ... 10 configured 18/12/19, 7:10 pm No * Extended key usage 🕕 Scope (Tags) > Object Identifier Predefined values Name 1 scope(s) selected Add Not configured 🗸 Client Authentication 1.3.6.1.5.5.7.3.2 Enrollment Settings 🕕 * Renewal threshold (%) 🕕 20 * SCEP Server URLs ① Server URL Add https://pcsintuendes-securepulse.msappproxy.net/certsrv/mscep/mscep.dll ОК

\equiv Microsoft Azure	Microsoft Azure C Search resources, services, and docs (G+/)				
Home > Microsoft Intune > Device cor	nfiguration - Profiles > SCEP_IOS - Properties > SCEP	P Certificate			
SCEP_IOS - Properties	« ×	SCEP Certificate			
∠ Search (Ctrl+/) «	🔚 Save 🗙 Discard	Certificate type	User V		
 Overview 	Name * SCEP_IOS	* Subject name format 🛈	IMEI number		
Manage	Description	Subject alternative name 🕕	User principal name (UPN) 🗸		
H Properties	Enter a description 🗸	* Certificate validity period ①			
😤 Assignments		* Key usage 🕡	Digital signature V		
Monitor	Platform	* Kay size (hits)			
Device status	iOS/iPadOS 🗸 🗸	key size (bits) 💿	2046 🗸		
User status	Profile type	*Root Certificate 🕕	>		
Per-setting status	SCEP certificate V	TRUST_IOS	· · · · · · · · · · · · · · · · · · ·		
Certificates	Settings > 9 configured	* Extended key usage () Name Object Identifier	Export Predefined values		
	Scope (Tags)	Not configured Not configured	Not configured V Add		
	1 scope(s) selected	Client Authentication	136155732		
		Enrollment Settings () * Renewal threshold (%) () * SCEP Server URLs () Server URL e.g. https://contoso.com/certsrv/mscep/m https://pcsintuendes-securepulse.msapp	20 Export scep.dll Add proxy.net/certsrv/mscep/mscep.dll ····		
		ОК			

Figure 6 Create SCEP Certificate Profile - iOS

3. Create VPN profile in Intune. For detailed steps, refer to the **procedures** in Microsoft Intune document.

\equiv Microsoft Azure	${\cal P}$ Search resources, services, and docs (G+	/)			
Home > Microsoft Intune > Device config	uration - Profiles > ANDROID_VPN - Prope	rties > Bas	e VPN		
ANDROID_VPN - Properties		« ×	Base VPN Android Enterprise		\Box ×
Search (Ctrl+/)	🖫 Save 🗙 Discard		* Connection name	PCS_VPN	
0 Overview	Name * ANDROID_VPN	~	* IP address or FQDN 🕕	10.96.116.30	
Manage	Description		* Authentication method ①	Certificates	\sim
Properties Assignments	Enter a description	~	*Authentication certificate ① ANDROID_SCEP		>
Monitor	Platform Android Enterprise	\sim	* Connection type ①	Pulse Secure	\checkmark
Licer status	Profile type		Always-on VPN can be configu	red in device restrictions.	
Per-setting status	VPN	\sim	Learn more about configuring	always-on VPN for Android Enterpris	se.
	Settings 3 configured	>			
	Scope (Tags) 1 scope(s) selected	>			
			ок		

Figure 7 Create VPN Profile - Android

Figure 8 Create VPN Profile - iOS

≡	Microsoft Azure	O Search resource	es, services, and docs (G+/)			5 t	ŵ?	🙂 🕬	nerjal@hæcturepulhæ.co PULSESECU	re 🕘
Home	> Microsoft Intune > Device config	uration - Profiles	>_VPN_IOS - Properties > Base VPN > Base VPN	I						
Prop	erties	« ×	Base VPN iOS/iPadOS		× Base	• VPN			I	$\Box \times$
«	Save X Discard		* Connection type ①	Pulse Secure	* Conr	nection name	PCS	_VPN		
		~	*Base VPN		* IP ad	 IP address or FQDN ① Authentication method ① 	10.9	96.116.30		
	Description		2 of 4 settings configured	>	* Auth		Cer	tificates		\sim
	Enter a description 🗸	~	Automatic VPN 1 setting available	*Auth SCEP	*Authentication certificate ① SCEP_IOS				>	
	Platform iOS/iPadOS	\checkmark	Proxy 3 settings available	>	Split tu	unneling ①	\square	Enable	Disable	
	Profile type									
	VPN	\sim								
	Settings	>								
	3 configured									
	Scope (Tags) 1 scope(s) selected	>								
			ОК		C	рк				

Configuring PCS with Microsoft Intune

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

To configure Microsoft Intune MDM server:

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

To obtain Tenant ID, Client ID, Client Secret Key, see "Viewing Client ID, Tenant ID, and Client Secret" on page 24.

3. Click Save changes.

Figure 9 Intune MDM Server

0 -		-								Pulse Connect Secur	e
ς Pι	ulse	Sec	ure	System	Authentication	Administrators	Users	Maintenance	Wizards		1 *
Settings											
*Name: INTU Type: Micros	INE soft Intune	Label to re	eference this serv	PET.							
✓ Server											
* Tenant ID:	. [25f4343b-ced7-	-4135-af22-d3a8a	a04b0b5'	zure AD Tenant ID						
* Client ID:		6a9d4b32-0c13	-47e7-aca1-3fcb	3e5d1e7 _V	Veb application ID that has be	een registered in azure AD					
* Client Sec	ret:				iecret key of the web applicati	ion registered in azure AD					
* Request T	imeout:	15		5	econds (5 - 60)						
Test Intu	une Conne	ection									
Note: Pulse Cor	nnect Secure	e uses endpoints	MAC address to	query attributes	from Microsoft Intune MDM a	uth server.					
Y Device Iden	tifier										
Please check t from the client.	the options o	in the Users > Au	thentication > [Re	ealm] > Authen	tication Policy > Certificate pa	age. For example, enable "Allo	w all users and	remember certificate info	rmation while user i	is signed in' option in order to rea	quest certificate
ID Template	<pre>certDN</pre>	.CN>		Template for c	onstructing device identifier fr	rom certificate attributes.					
	The templat expressions	te can contain tex and policy cond	tual characters a itions. All of the o	s well as varia certificate varia	bles for substitution. Variable bles are available.	s should be enclosed in angle	brackets like th	his «variable». The variab	les are the same as	those used in role mapping cus	tom
	Examples: *certON_ON* *certAttr.seria *certAttr.atNo	First CN fro Number* Certificate s emelacos* Where soos Email The UPN The	om the subject DN serial number can be: Email alternate name Principal Name altern	ale name							
	<pre>>certONText> cert-*certON.0</pre>	The comple DN= The text for	ite subject DN ert-" followed by the f	inst CN from the a	ubject DN						
ID Type:		D Univ Iden	ersal Unique tifier								
	Seria	al Number	Device.								
		D Iden	tifier								
	IMEI	Equi	Ipment Identity								
Save Chang	ges 🛛 R	leset									

4. Select **Authentication > Auth. Servers > Cert Server** and create certificate server.

Figure 10 Cerificate Server

0	-						1. 1. 1. 1.	Pulse Connect Secure		
S Puls	e Secur	e System	Authentication	Administrators	Users	Maintenance	Wizards	6 6 6 1	••	
Auth Servers > Cert se	rver > Settings									
Settings	Jsers									
*Name:	Cert server		Label to reference ti	Label to reference this server.						
User Name Template	<oertdn.cn></oertdn.cn>		Template for constru	Template for constructing user names from certificate attributes.						
	The template can contain to mapping custom expression	extual characters as w ns and policy condition	vell as variables for substitu ns. All of the certificate va	is variables for substitution. Variables should be enclosed in angle brackets like this <variable>. The variables are the same as those used in role All of the certificate variables are available.</variable>						
	Examples: <oertdn.cn> First CN <oertattr.serialnumber>Certifica <oertattr.aitname.xxx> Where xx Email Ti UPN Ti UPN Ti </oertattr.aitname.xxx></oertattr.serialnumber></oertdn.cn>	from the subject DN e serial number x can be: se Email alternate name e Principal Name alternate	: name							
	-certDNText> The com certcertDN.CN> The text 1	; plete subject DN (cert-" followed by the first (CN from the subject DN							
Vuser Record Synd	chronization									
Enable Use	er Record Synchronizatio	n								
Logical Au	th Server Name:									
Save Changes	Reset									

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

Figure 11	Realm
-----------	-------

On L C							Pulse Connect Secure
S Pulse Se	CURE System	Authentication	Administrators	Users	Maintenance	Wizards	
User Realms > Users > General							
General							
General Authentication	Policy Role Mapping	1					
* Name:	Users				Label to reference	e this realm	
Description:	Default authentication realm for users						
	When editing, start on th	e Role Mapping page					
★ Servers							
Specify the servers to use for authenti	cation and authorization. To creat	e or manage servers, see	e the Servers page.				
		_					
Authentication:	Cert server	•			Specify the set	ver to use for authen	ticating users.
User Directory/Attribute:	None	•			Specify the ser	rver to use for author	ization.
Accounting:	None	•			Specify the ser	ver to use for Radius	accounting.
Device Attributes:	Intune				Specify the ser	ver to use for device	authorization.

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

💲 Pulse:	Secure	System	Authentication	Administrators	Users	Maintenance	Wizards
User Realms > tp-mobileiron-m	idm > Role Mapping > Ro	le Mapping Rul	e				
Role Mapping Rule							
Rule based on: Device attrib	oute 🗘 Update						
* Name:	the following attribute v	alues					
Attribute:	(Select an attribute)	 Attribut 	tes				
is	(Select an attribute) complianceReason deviceId deviceName IMEI isCompromised isEnrolled lastSeen macAddress manufacturer meid model osVersion phoneNumber platform serialNumber UDID userEmail	If more than	n one value for this attribut	e should match, enter one p	er line. You ca	n use * wildcards. L	
Stop processing rules To manage roles, see the Roles Save Changes Save Changes Save Changes	userId s configuration page. ve + New	•					

Figure 12 Role Mapping Configuration Page

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

Table 7Microsoft Intune Role Mapping Attributes

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

Configuring the Microsoft Intune MDM Server

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

To configure the Microsoft Intune MDM:

- 1. Enroll the devices with the MDM server.
- 2. Create Azure Active Directory (AAD) web application.
- 3. Go to **portal.azure.com**, click on the **Azure Active Directory** on the left of the screen, click on the **App registrations** and then click on **New registration**.

Figure 13 Creating New Application

Home > Pulsesecure App registrati	ions				
Pulsesecure App reg	gistrat	ions			
	«	+ New registration 🔀 Endpoints 🤌 Troubleshooting 🕴 🛇 Got feedback?			
0 Overview	^	() Welcome to the new and improved App registrations (now Generally Available). See what's new and learn mo	re on how it's changed. $ ightarrow$		
💉 Getting started		All applications Owned applications			
✗ Diagnose and solve problems		Start typing a name or Application ID to filter these results			
Manage		Display name	Application (client) ID	Created on	Certificates & secrets
🚨 Users		Jo JoGy-PCS	117d4f3d-b23a-48b2-bc28-a7a39dafac50	13/9/2019	🔇 Current
A Groups		PCS_Intune	6a9d4b32-0c13-47e7-aca1-3fcb3e5d1e7b	5/12/2019	🔮 Current
Organizational relationships		PP PPS-hdarshan-200.81	5c329da8-6296-4636-b4b4-1f023c04485e	19/12/2019	🔇 Current
Roles and administrators		ec PCS62-Intune	89c46fb2-235e-4b40-834c-0c98f4517a05	6/1/2020	🔮 Current
Administrative units (Preview)		PP PPS.hdarshan-88.99	a5140d0f-fbbc-41dc-96ed-5dcb75cfb921	1/4/2020	📀 Current
Enterprise applications		_			
Devices					
App registrations					

4. Enter the application name, select **Web** app as application type, and enter the IP address/FQDN for redirect-URL and click **Register**.

Figure 14 Registering a New Application

Figure 15 Application Created

Home > Pulsesecure App registrations > Register an application
Register an application
* Name
The user-facing display name for this application (this can be changed later).
Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (Pulsesecure only - Single tenant)
Accounts in any organizational directory (Any Azure AD directory - Multitenant)
Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
Help me choose
Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
Web e.g. https://myapp.com/auth
By proceeding, you agree to the Microsoft Platform Policies 👩
Register

The Application Registration page appears if the registration is successful.

Home > Pulsesecure App registrations				
Pulsesecure App registrat	tions			
	+ New registration 🖶 Endpoints 🤌 Troubleshooting 🛛 🛇 Got feedback?			
Overview	Welcome to the new and improved App registrations (now Generally Available). See whether the second se	at's new and learn more on how it's changed. $ ightarrow$		
💉 Getting started	All applications Owned applications			
× Diagnose and solve problems	Start typing a name or Application ID to filter these results			
Manage	Display name	Application (client) ID	Created on	Certificates & secrets
Lusers	Jo JoGy-PCS	117d4f3d-b23a-48b2-bc28-a7a39dafac50	13/9/2019	Current
A Groups	PCS_Intune	6a9d4b32-0c13-47e7-aca1-3fcb3e5d1e7b	5/12/2019	Current
Organizational relationships	PP PPS-hdarshan-200.81	5c329da8-6296-4636-b4b4-1f023c04485e	19/12/2019	Current
& Roles and administrators	PC PCS62-Intune	89c46fb2-235e-4b40-834c-0c98f4517a05	6/1/2020	Current
Administrative units (Preview)	PPS.hdarshan-88.99	a5140d0f-fbbc-41dc-96ed-5dcb75cfb921	1/4/2020	Current
Enterprise applications				
Devices				
App registrations				
Identity Governance				
Application proxy				
Licenses				
Azure AD Connect				

5. Click the application, then select **API permissions** and click **Add a permission**.

Figure 16 Adding Permissions

Iome > Pulsesecure App registrations > PCS_Intune API permissions									
PCS_Intune API permissio	PCS_Intune API permissions								
	🖒 Refresh								
 Overview Quickstart Manage Branding 	Configured permissions Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permission all the permissions the application needs. Learn more about permissions and consent + Add a permission Grant admin consent for Pulsesecure								
	API / Permissions name	Туре	Description	Admin consent req	Status				
📍 Certificates & secrets	✓ Azure Active Directory Graph (3)								
111 Token configuration	Directory.AccessAsUser.All	Delegated	Access the directory as the signed-in user	-	Granted for Pulsesecure				
API permissions	User.Read	Delegated	Sign in and read user profile	-	Granted for Pulsesecure				
Expose an API	User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Pulsesecure				
Conners	VIntune (1)								
Roles and administrators (Previ	get_device_compliance	Application	Get device state and compliance information from Micr.	Yes	Granted for Pulsesecure				
Manifest	✓ Microsoft Graph (4)								
Support + Troubleshooting	email	Delegated	View users' email address		Granted for Pulsesecure				

6. Select Microsoft Intune API.

Figure 17 Setting Intune Permissions

Home > Pulsesecure App registrations > PCS_Intune API permissions				Request API permissions			
PCS_Intune API permissions				Select an API			
⊘ Search (Ctrl+/)							
Overview	Overview Configured permissions Quickstart Applications are authorized to call APIs when they are granted perm all the permissions the application needs. Learn more about permiss		Commonly used Microsoft APIs				
4 Quickstart			granted perm about permiss	Microsoft Graph			
Manage		nt for Pulsese	Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and mindows 10.				
Branding			single endpoint.				
Authentication	API / Permissions name	Туре	Description				
🕈 Certificates & secrets	✓ Azure Active Directory Graph (3)			Azure Rights Management Services	Azure Service Management	တို့ Dynamics 365 Business Central	
11 Token configuration	Directory AccessAsUser All	Delegated	Access the c	Allow validated users to read and write	Programmatic access to much of the	Programmatic access to data and	
API permissions	User.Read Delegated Sign in and		Sign in and	protected content	functionality available through the Azure portal	functionality in Dynamics 365 Business Central	
Expose an API	User.Read.All	Delegated	Read all use				
Owners	VIntune (1)			🖳 Intune	Office 365 Management APIs 🚯 SharePoint	SharePoint	
Roles and administrators (Previ get_device_compliance Application Get device		Get device s	t device s Programmatic access to Intune data Retrieve information about user, system, and policy actions and e		n, Interact remotely with SharePoint data		
Manifest	✓ Microsoft Graph (4)				from Office 365 and Azure AD activity		
Support + Troubleshooting	email	Delegated	View users'				

7. Under Application Permissions, select **Get device compliance** information from Microsoft Intune and click **Add permissions**.

PCS_Intune | API permissions All APIs https://api.manage.microsoft.com/ Docs C 🕐 Refresh ~ B Overview Configured permissions 1 Intune APIs are available via the Microsoft Graph API. You may want to consider using Microsoft Graph instead. Quickstart Applications are authorized to call APIs when they are granted perm all the permissions the application needs. Learn more about permiss Manage What type of permissions does your application require? + Add a permission Grant admin consent for Pulsese Branding Delegated permissions Application permissions Your application runs as a background service or daemon without a signed-in user. Your application needs to access the API as the signed-in user. Authentication API / Permissions name Туре Description Certificates & secrets ✓ Azure Active Directory Graph (3) Select permissions expand Token configuration Directory.AccessAsUser.All Delegated Access the c Delegated Sign in and API permissions User.Read Permission Expose an API User.Read.All Delegated Read all use Admin consent required Owners VIntune (1) Get data warehouse Get data warehouse information from Microsoft Intune Yes get_device_compliance Roles and administrators (Previ... Application Get device s Get device_compliance Get device state and compliance information from Microsoft Intune ① 11 Manifest Microsoft Graph (4) Yes email Delegated View users' Support + Troubleshooting manage_partner_compliance_policy Manage partner compliance policies with Microsoft Intune. ① Yes Delegated Sign users in openid Troubleshooting profile Delegated View users New support request User.Read Add permissions Discard Delegated Sign in and

Figure 18 Setting Intune Permissions

- 8. (Optional) You must add the following delegated permissions for Microsoft Graph API.
 - Sign in and read user profile
 - Sign Users in
 - View users' email address
 - View users' basic profile
- 9. (Optional) Add the following delegated permissions for Azure Active Directory.
 - Sign in and read user profile
 - Read all users' basic profiles
 - Access the directory as the signed-in user.

Figure 19 Permissions

Home > Pulsesecure App registrations >	PCS_Intune API permissions					
PCS_Intune API permissio	ons					
	🕐 Refresh					
 Overview Quickstart Manage 	Configured permissions Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent					
Branding	+ Add a permission Grant	admin conser	nt for Pulsesecure			
 Authentication 	API / Permissions name	Туре	Description	Admin consent req	Status	
📍 Certificates & secrets	Azure Active Directory Graph (3)					
III Token configuration	Directory.AccessAsUser.All	Delegated	Access the directory as the signed-in user	-	Granted for Pulsesecure	
API permissions	User.Read	Delegated	Sign in and read user profile	-	Granted for Pulsesecure	
Expose an API	User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Pulsesecure	
Owners	VIntune (1)					
Roles and administrators (Previ	get_device_compliance	Application	Get device state and compliance information from Micr	Yes	Granted for Pulsesecure	
III Manifest	Microsoft Graph (4)					
Support + Troubleshooting	email	Delegated	View users' email address		Granted for Pulsesecure	
Troubleshooting	openid	Delegated	Sign users in	-	Granted for Pulsesecure	
Rew support request	profile	Delegated	View users' basic profile	-	Granted for Pulsesecure	
	User.Read	Delegated	Sign in and read user profile	-	Granted for Pulsesecure	

Viewing Client ID, Tenant ID, and Client Secret

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

Figure 20 Client ID/Application ID

Home > Pulsesecure App registrations > PCS_Intune					
PCS_Intune					
	📋 Delete 🜐 Endpoints				
Overview	() Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developed). →			
Quickstart	Display name : PCS_Intune	Supported account types	: My organization only		
	Application (client) ID : 6a9d4b32-0c13-47e7-aca1-3fcb3e5d1e7b	Redirect URIs	: 1 web, 0 public client		
Manage	Directory (tenant) ID : 25f4343b-ced7-4135-af22-d3a8a04b0b57	Application ID URI	: Add an Application ID URI		
Branding	Object ID : 090be418-7e0e-400a-a745-c9e9d19daaec	Managed application in	: PCS_Intune		
Authentication	\$				
Certificates & secrets	Welcome to the new and improved App registrations. Looking to learn how it's changed from App registration	is (Legacy)? Learn more			

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

Figure 21 Tenant ID

Home > Pulsesecure App registrations >	ome > Pulsesecure App registrations > PCS_Intune					
PCS_Intune						
	🗓 Delete 🔀 Endpoints					
R Overview	Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer)	. →				
Quickstart	Display name : PCS_Intune	Supported account types	: My organization only			
	Application (client) ID : 6a9d4b32-0c13-47e7-aca1-3fcb3e5d1e7b	Redirect URIs	: 1 web, 0 public client			
Manage	Directory (tenant) ID : 25f4343b-ced7-4135-af22-d3a8a04b0b57	Application ID URI	: Add an Application ID URI			
Branding	Object ID : 090be418-7e0e-400a-a745-c9e9d19daaec	Managed application in	: PCS_Intune			
Authentication	Â					

To create the secret key:

1. Click the **Web Application/API** and then click **Certificates & Secrets**.

Home > Pulsesecure App registrations >	PCS_Intune		
PCS_Intune			
	Delete 🕀 Endpoints		
📕 Overview	Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developed). →	
Quickstart	Display name : PCS_Intune	Supported account types	: My organization only
	Application (client) ID : 6a9d4b32-0c13-47e7-aca1-3fcb3e5d1e7b	Redirect URIs	: 1 web, 0 public client
Manage	Directory (tenant) ID : 25f4343b-ced7-4135-af22-d3a8a04b0b57	Application ID URI	: Add an Application ID URI
Branding	Object ID : 090be418-7e0e-400a-a745-c9e9d19daaec	Managed application in	: PCS_Intune
Authentication	*		
📍 Certificates & secrets	1 Welcome to the new and improved App registrations. Looking to learn how it's changed from App registration	is (Legacy)? Learn more	
Token configuration			
API permissions			

2. Click on New client secret.

PCS_Intune Certificates &	secrets					
Search (Ctrl+/)	Thumbprint	Start date	Expires			
🗮 Overview 🔗 Quickstart	No certificates have been added for this ap	plication.				
Manage						
Branding	Client secrets					
Authentication	A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.					
Certificates & secrets	+ New client secret					
Token configuration	Description	Expires	Value			
API permissions	119	5/12/2020	sgl*********	1		
Expose an API	163	6/12/2020	U=V**************	1		
Contraction Contraction	PPS	10/12/2020	7xu******************************	ii ii		
Roles and administrators (Previ	165	6/1/2021	PH6**************	1		
10 Manifest	CPBHARATH	13/2/2021	LTp****************	Û		
Support + Troubleshooting	55.17	23/3/2021	Jo***************	Î		
Troubleshooting						
New support request						

3. Enter appropriate description and click Add.

Home > Pulsesecure App registrations >	Home > Pulsesecure App registrations > PCS_Intune Certificates & secrets				
PCS_Intune Certificates	PCS_Intune Certificates & secrets				
	Add a client secret				
OverviewQuickstart	Description test				
Manage	Expires In 1 year In 2 years Never				
🔤 Branding					
Authentication					
📍 Certificates & secrets					
H Token configuration					
- API permissions	Cancel				

The client secret is created.

PCS_Intune Certificates & secrets					
	Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.				
Overview	no ceraneates note ocen adaea for ans appir	CALINITI:			
Quickstart					
Manage	Client secrets				
Branding	A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.				
Authentication	+ New client secret				
📍 Certificates & secrets	Description	Expires	Value		
Token configuration	119	5/12/2020	sgl******	iii	
 API permissions 	163	6/12/2020	U=V****************	iii	
Expose an API	PPS	10/12/2020	7xu************************************	iii	
Owners	165	6/1/2021	PH6*****	<u>i</u>	
Roles and administrators (Previ	CPBHARATH	13/2/2021	LTp***************	<u>í</u>	
III Manifest	55.17	23/3/2021	.Jo************	Î	
Support + Troubleshooting	test	5/5/2021	kw6AYrrtrsEX3DD/2R1hp_@@a1YOfv.I	ñ 🗎	
ℬ Troubleshooting					

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 22 shows the configuration page for Pulse Connect Secure.

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

Figure 22 Events Log Settings Configuration Page - Pulse Connect Secure

	Pulse Connect Secure
Version Secure System Authentication Administrators Users Maintenance Wizards	
Log/Monitoring > Events > Log settings	
Log settings	
Events User Access Admin Access Sensors Client Logs SNMP Statistics	
Log Settings Filters	
Save Changes Reset	
✓ Maximum Log Size	
Max Log Size: 200 MB	
Note: To archive log data, see the Archiving page.	
✓ Select Events to Log	
Connection Requests Statistics	
System status Fellominance Reverse Proxy	
System Errors M Email Proxy Events	
MDM API Trace	
Pulse One Events	

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 23 shows the Events log for Pulse Connect Secure.

Figure 23 Events Log - Pulse Connect Secure

$\overline{\mathbb{S}}$	Puls	Pulse Connect Secure Pulse Connect Secure System Authentication Administrators Users Maintenance Wizards
Log/Monito	ring > Events	> Logs
Logs		
Events	User	Access Admin Access Sensors Client Logs SIMP Statistics Advanced Settings
Log S	ettings Filte	5
View by filt	er: Standard:	Standard (dofault) Show 200 items
Edit Query		
	Update	Reset Query Save Query
Save Lo	ng As	Clear Log Save All Logs Clear All Logs
F I Q Export For	ilter:Standard Date:Oldest to uery: mat:Standard	(default) leavest
Severity	ID	Message
Info	MDM31026	20 4.2 01 54 17 - ite - 1127 0.1 11 Rott-System (III - Htune Resonse 91432411 - Status 200 - ComplianceApEndorinAddress" "VisitatiessPlacSenceVicenceianceVicences" "deveApEndorinAddress" "VisitatiessPlacSenceVicenceianceApEndorinAddress" "VisitatiessPlacSenceVi
Info	MDM31024	2020-04-30-16-54-17 - Iw - 1/27-0.0.1] Rost=System(C) - Intume Request 91482411: GET /services?api-version=1.0
info	MDM31026	2000-01-00 15:54.17 - ine - 1(27:0.0.1] Rest: System (C) - Haven Response 960601765: Status: 200 (Felsen, type)": Bearer, "expres_in": "3597; "rest_expres_in": "3597; "res
Info	MDM31025	2020-04-30 16 54.16 - Iw - [127.0 0.1] Rost:=System(0] - Intune Request 950601769: POST /259331b ced7.4135.et22.43ala04b0b57/oauth2holan resource=https://gpi.manage.microsoft.com/&clent_secret=******&clent_d=&s54b12-2x1-3hcbe5f1e7b&gart_type=clent_cedentals
Info	MDM31025	2003-04.30 IF 54 If - In- (127.0 II) Rost: System(II) - Itanes Response 112779996; Status: 200. ["codata metadata" "https://jpap.windows.net/258/31b-cef7.415-a02_d3alab4b0b7/3mtadatadfreetoryObjects", "akive" ["codata bye" "Microsoft. DirectorySenices SeniceEndpoint", "abject]" winces and participations and particip
Info	MDM31024	2020-04-30 16 54.16 - Ire - [127.0.0.1] Rost:System(0] - Intune Request 112379595: GET 254343b-ced7-4135-at22-43aba04b0657/senicePrincipalsByAppld/0000000a-0000-0000-0000-0000-0000-0000
Info	MDM31026	2020-04-30 16-54:16 - Im - [127.0.0.1] Rost:System([]) - Intune Response 523015751: Status: 200. ("token: type": "Baarer", "expires in "13599", "expires in "13599","expires on "1158249537", "Interconce", "Tokes: System([]) - Intune Response 523015751: Status: 200. ("token: type": "Baarer", "expires in "13599","expires on "1158249537", "Interconce", "158249537", "Interconce", "Tokes: System([]) - Intune Response 523015751: Status: 200. ("token: type": "Baarer", "expires in "13599","expires on "1158249537", "Interconce", "158249537", "Interconce", "Tokes: System([]) - Intune Response 523015751: Status: 200. ("token: type": "Baarer", "expires in "13599","expires on "1158249537", "Interconce", "Tokes: System([]) - Intune Response 523015751: Status: 200. ("token: type": "Baarer", "expires in "13599","expires on "1158249537", "Interconce", "Tokes: System([]) - Intune Response 523015751: Status: 200. ("token: type": "Baarer", "expires in "13599","expires on "1158249537", "Interconce", "158249537", "Interconce", "Tokes: System([]) - Intune Response 523015751: Status: 200. ("token: type": "Baarer", "expires in "13599","expires on "1158249537", "Interconce", "Tokes: System([]) - Intune Response 523015751: Status: 200. ("token: type: "Baarer", "expires in "13599","expires on "1158249537","Interconce", "Tokes: System([]) - Intune Response 523015751: Status: 200. ("token: type: "Baarer", "expires in "13599","expires on "1158249537","Interconce", "Tokes: System([]) - Interconce", "Tokes: System([]) - Interconce, "Tokes: System([])

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 24 shows the User Access log for Pulse Connect Secure.

Figure 24 User Access Log

\diamond	_	Pulse Connect Secure	
\mathbf{S}	Puls	e Secure _{System} Authentication Administrators Users Maintenance Wizards	• •
C Q Export Fo	Date:Oldest to N Lery: rmat:Standard	Newest	
Severity	ID	Message	
Info	NWC30477	2020-03-02 09:19:45 - Ive - [172.21.18.72] cpbharath(Users)[Users] - VPN Tunneling: User with IP 10.96.126.137 connected with ESP transport mode.	
Info	NWC23508	2020-03-02 09:19:44 - Ive - [172.21.18.72] cpbharath(Users)[Users] - Key Exchange number 1 occurred for user with NCIP 10.96.126.137	
Info	NWC23464	2020-03-02 09:19:44 - Ive - [172.21.18.72] cpbharath(Users)[Users] - VPN Tunneling: Session started for user with IPv4 address 10 96.126.137, hostname localhost	
Info	ERR31271	2020-03-02.09:19:44 - ive - [127.0.0.1] System()] - VPN Tunneling: Optimized ACL count = 2.	
Info	ERR24670	2020-03-02 09:19:44 - ive - [127.0.0.1] System()] - VPN Tunneling: ACL count = 2.	
Info	AUT31002	2020-03-02.09:19:44 - Ive - [172.21.18.72] cpbharath(Users)[Users] - Connected to TUN-VPN port 443	
Major	AUT31085	2020-03-02 09-19-34 - ive - [127.0.0.1] System()] - Number of concurrent users (2) exceeded the system limit (2).	
Info	AUT31504	2020-03-02 09 19:33 - Ive - [172 21 18 72] cpbharath(Users)[Users] - Login succeeded for cpbharath/Users (session 0000000) from 172 21 18 72 with PulseSecureAndroid (Compatible with JunosPulseAndroid) Mozillai 5 0 (Linux; Android 8 0.0; SM-G935F Build	/R16NW;
Info	AUT24326	2020-03-02 09:19:32 - Ive - [172:21.18.72] cpbharath(Users)[] - Primary authentication successful for cpbharath/cert srvr from 172:21.18.72	
Info	CRT30663	2020-03-02 09-19 32 - ive - [172 21 18.72] System()[] - client certificate receivedBEGIN CERTIFICATE MIGODCCBScgAwtBadTcwAAAHLxVs4vhOmwAAAAD8TAHBgknikG9w6BACsFADBeMEMMECYYKC2miZPLGGBGRYDbnV0MSEwhwYKC2miZPyLG0BGRYErtYsc2VzZWH1cm/hY2Nic3MdjAgBjNVBAMTGXB1bHNic2VjKXJIYVMjZVkLUNTQUQIODE-wirhchM /cnk/g9hW0IZTAVszthP850GYSpAljnJal8UQr849jz35bKoMS8udFDg0Ntx9cHODeof0icosgFC8ELugaDcEgise0U1risBitLjZVWmiMihTa7z0zF0J22F0U32q0VBBEEWVndvjIj0v56KY1jphtB94nG6RDegtBg3t2bitK7AhV;TYalyJOUgnqV8WTJDcyjb2thjNiht/Thur41ULXNKe MCMDBg4QVKWrBBAGCKwCCA6AnDCVjCo307XhdGhAc2VjkJLrHvs2Ju25Id4Mby5NivZnoU*29MB8GA1Ud5g0WBB5LOMw+hpCmiZ2VNtoBpRY56hTABgHVrIsMECDAWgBTVYDtELTBarEZVitxdTnSOLntEBTCSgnVDvK0BHMMHiTTMix41ULXNKe MCMDBg4QVKWrBBAGCKwCCA6AnDCVjCo307XhdGhAc2VjkJLrHvs2Ju25Id4Mby5NivZnoU*29MB8GA1Ud5g0WBB5LOMw+hpCmiZ2XIVS02F012Sq0WBBEEWVndvjWVDEELUBAECEVataTnsOchtEBTCSgnVDvK0BHMMHiTTMIAHV /mEZT9VmpYVSRDb6Fzz1JUkEzXI000000000000000000000000000000000000	ijAwMjI5M 3XaXVcLi ioHHbGR iWNIcyxD QBgjcKA +juCK6tF
Info	AUT31556	2020-03-02 09:19:32 - Ive - [172.21.18.72] System()[] - Unauthenticated request url /dana-na/auth/url_default/login cgi?realm=Users came from IP 172.21.18.72.	
Info	AUT31556	2020-03-02 09:19:21 - Ive - [172:21.18.72] System()[] - Unauthenticated request url /dana-na/auth/url_default/welcome cgi came from IP 172:21.18.72.	
Info	AUT31556	2020.02.02 00:10 21 _ No _ 1172 21 18 721 System/01 _ Inauthenticated request unit (came from ID 172 21 18 72	

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 29
- "Using the Debug Log" on page 31

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.

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

Figure 25 shows policy trace results.

Figure 25 Policy Tracing Results

٥.		Pulse Connect Secure
<u>ې</u> ۲	Juls	eSecure System Authentication Administrators Users Maintenance Wizards
Date:	Current P Earliest D	olicy Trace Log
User Name Realm Nam	: 35 202707 e: cpbharath	1295807 0 relam
Export For	mat: Standard	- Lindela Sava Lan As Clear Lan
Snow	uu iten	Is update Save Lug As Uteat Lug
Severity	ID	Message
Info	PTR10103	2020/05/04 19:22:53 - [49:207.62.57] - anand(Admin Users)[.Administrators] - 35 202707 295507 0:opbharath relam - Policy Tracing turned on
Info	PTR23344	2020/05/04 19:25:15 - [49:207.62:57] - 35 202707 295507 O(opbharath relam)[] - Authentication successful to auth server "cert server9"
Info	PTR31021	2020/05/04 19:25:15 - [49.207.62.57] - 35 202707 295507 O(opbharath relam)[] - Getting device information from server "INtune"
Info	PTR31022	2020/05/04 19:25:15 - [49.207.82.57] - 35 202707 295507 0(opbharath relam)[] - Finished getting device information from server "INtune"
Info	PTR10209	2020/05/04 19:25:15 - [49:207.62.57] - 35 202707 295507 0(opbharath relam)[] - Realm opbharath relam running 1 mapping rules for user 35 202707 295507 0
Info	PTR10305	2020/05/04 19:25:15 - [49:207.62.57] - 35 202707 295507 0(opbharath relam)[] - Variable sourcelp = 49:207.62.57
Info	PTR10305	2020/05/04 19:25:15 - [49:207:62:57] - 35 202707 295507 0(opbharath relam)[] - Variable SourceIPStr = "49:207:62:57"
info	PTR10305	2020/05/04 19:25:15 - [49:207.62:57] - 35 202707 295507 0(cpoharath relam)[] - Variable user = "35 202707 295507 0"
Info	PTR10305	2020/05/04 19:25:15 - [49:207.62.57] - 35 202707 295507 0(opbharath relam)[] - Variable password = "*****
Info	PTR10305	2020/05/04 19:25:15 - [49:207.52.57] - 35 202707 295507 0(opbharath relam)[] - Variable userName = "35 202707 295507 0"
Info	PTR10305	2020/05/04 19:25:15 - [49.207.62.57] - 35 202707 295507 O(opbharath relam)[] - Variable protocol =
Info	PTR10305	2020/05/04 19:25:15 - [49.207.62.57] - 35 202707 295507 0(opbharath relam)[] - Variable realm • "opbharath relam"
Info	PTR10305	2020/05/04 19:25:15 - [49.207.62.57] - 35 202707 295507 0(opbharath relam)[] - Variable loginTime - Mon May 4 19:25:15 2020
Info	PTR10305	2020/05/04 19:25:15 - [49.207.62.57] - 35 202707 295507 0(opbharath reliam)[] - Variable deviceAttr.osVersion - "IOS 12.4.4"
Info	PTR10305	2020/05/04 19:25:15 - [49.207.62.57] - 35 202707 295507 0(opbharath relam)[] - Variable deviceAttr.UDID = "09e88e1715e43f45e7c2704aeaa0aa2d8b94400e"
Info	PTR10305	2020/05/04 19:25:15 - [49:207.62.57] - 35 202707 295507 0(opbharath relam)[] - Variable deviceAttr.deviceId = "e154e638-a662-44d3-9e2e-b906286595b5"
info	PTR10305	2020/05/04 19:25:15 - [49:207.62.57] - 35 202707 295507 0(opbharath relam)[] - Variable deviceAttr.IMEI = "352027072955070"
Info	PTR10305	2020/05/04 19:25:15 - [49.207.62.57] - 35 202707 295507 0(opbharath relam)[] - Variable devloeAttr.model = "IPhone 6"
Info	PTR10305	2020/05/04 19:25:15 - [49.207.62.57] - 35 202707 295507 0(opbharath relam)[] - Variable userAgent = "PulseSecureIPhone(Compatible with JunosPulseIPhone) Moziliai5.0 (IPhone; CPU IPhone OS 12_4_1 like Mac OS X) AppleWebKite
Info	PTR10305	2020/05/04 19:25:15 - [49.207.62.57] - 35 202707 295507 0(cpbharath relam)[] - Variable language = "en"
Info	PTR10305	2020/05/04 19:25:15 - [49:207.62.57] - 35 202707 295507 0(cpbharath relam)[] - Variable loginURL = ""(cpbharath)"
Info	PTR10305	2020/05/04 19:25:15 - [49:207.62.57] - 35 202707 295507 0(cpbharath relam)[] - Variable loginHost = "stg1,pwsmobilesami.net"
Info	PTR10305	2020/05/04 19:25:15 - [49:207.62.57] - 35 202707 295507 0(cpbharath relam)[] - Variable loginHostAddr = "192.168.5.23"
Info	PTR10305	2020/05/04 19:25:15 - [49:207.62.57] - 35 202707 295507 0(cpbharath relam)[] - Variable networkiF = "external"
Info	PTR10305	2020/05/04 19:25:15 - [49.207.62.57] - 35 202707 295507 0(cpbharath relam)[] - Variable certVerity = "SUCCESS"
info	PTR10305	2020/05/04 19:25:15 - [49.207.62.57] - 35 202707 295507 0(opbharath relam)[] - Variable certDnText = "CN=35 202707 295507 0"
Info	PTR10305	2020/05/04 19:25:15 - [49.207.62.57] - 35 202707 295507 0(cpbharath relam)[] - Variable certDn.CN - "35 202707 295507 0"
Info	PTR10305	2020/05/04 19:25:15 - [49:207.62.57] - 35 202707 295507 0(cpbharath relam)[] - Variable certAttr.CN • "35 202707 295507 0"
info	PTR10305	2020/05/04 19:25:15 - [49:207.62.57] - 35 202707 295507 0(cpbharath relam)[] - Variable certAttr serialNumber = "730000044CEAD9C3DE86FF4F490000000044C"
info	PTR10305	2020/05/04 19:25:15 - [49:207.62.57] - 35 202707 295507 0(cpbharath relam)[] - Variable certAttr.EKUText - "TLS Web Client Authentication,E-mail Protection,Microsoft Encrypted File System"

Info	PTR10305	2020/05/04 19:25:15 - [49:207.62.57] - 35 202707 295507 0(opbharath relam)[] - Variable certAth:EKUOID = "1.3.6.1.5.5.7.3.2,1.3.6.1.5.5.7.3.4,1.3.6.1.4.1.311.10.3.4"
Info	PTR10305	2020/05/04 19:25:15 - [49.207.62.57] - 35 202707 295507 0(cpbharath relam)[] - Variable certAttr.altName.UPN = "cpbharath@securepulse.onmicrosoft.com"
Info	PTR10305	2020/05/04 19:25:15 - [49.207.62.57] - 35 202707 295507 0(cpbharath relam)[] - Variable certAttr.altName.UPNuld = "cpbharath"
Info	PTR10305	2020/05/04 19:25:15 - [49.207.62.57] - 35 202707 295507 0(opbharath relam)[] - Variable certAttraitName.UPNdomain - "securepuise.onmicrosoft.com"
Info	PTR10305	2020/05/04 19:25:15 - [49.207.62.57] - 35 202707 295507 0(cpbharath relam)[] - Variable certAttr.criDist = " Full Name: URLidap:///CN-pulsesecureaccess-CSAD-CA,CN-csad,CN-CDP,CN-Public%20Key%20Services,CN-Services,CN-
info	PTR10305	2020/05/04 19:25:15 - [49.207.62.57] - 35 202707 295507 0(cpbharath relam)[] - Variable cerlAttr.publickey = "MIIBCgKCAQEAISYTQDWI80pVecxbo5uff3UKQ0I0qT/FFU5p87q5+CpDMbUV7Z+kensyvjCQvvGPTJ0R0UgpI8ISPTX1AFvxXaGS9k8Aiq0a7HFDjGd3y1U3PY[5]bjdIEDR0zg6nG2rluY0dGVmma8SRG26787PispdUSrinlircPFF2h8iqz
Info	PTR10305	2020/05/04 19:25:15 - [49.207.62.57] - 35 202707 295507 0(opbharath relam)[] - Variable certissuerDnText = "CN-pulsesecureaccess-CSAD-CA, DC-pulsesecureaccess, DC+net"
Info	PTR10305	2020/05/04 19:25:15 - [49.207.62.57] - 35 202707 295507 0(opbharath relam)[] - Variable certissuerDn.CN - "pulseseoureaccess-CSAD-CA"
Info	PTR10305	2020/05/04 19:25:15 - [49.207.62.57] - 35 202707 295507 0(cpbharath relam)[] - Variable certissuerDn.DC = "pulsesecureaccess"
Info	PTR10305	2020/05/04 19:25:15 - [49.207.62.57] - 35 202707 295507 0(cpbharath relam)[] - Variable certissuerDn.DC - "net"
info	PTR10305	2020/05/04 19:25:15 - [49:207.62.57] - 35 202707 295507 0(cpbharath relam)[] - Variable deviceAttr@INtune.UDID = "09e88e1715e43f45e7c2704aea0aa2d8b94400e"
info	PTR10305	2020/05/04 19:25:15 - [49:207.62.57] - 35 202707 295507 0(opbharath relam)[] - Variable deviceAttr@INtune.deviceId = "e154e638-a662-44d3-9e2e-b906286595b5"
info	PTR10305	2020/05/04 19:25:15 - [49:207.62.57] - 35 202707 295507 0(opbharath relam)[] - Variable deviceAttr@INtune.IMEI = "352027072955070"
info	PTR10305	2020/05/04 19:25:15 - [49:207:62:57] - 35 202707 295507 0(cpbharath relam)[] - Variable deviceAttr@INtune.model = "IPhone 6"
info	PTR10212	2020/05/04 19:25:15 - [49:207:62:57] - 35 202707 295507 0(cpbharath relam)[] - Mapped to roles cpbharath role by rule 'user = ***
info	PTR10205	2020/05/04 19:25:15 - [49:207.62.57] - 35 202707 295507 0(opbharath relam)[] - Realm opbharath relam mapped user 35 202707 295507 0 to roles opbharath role
Info	PTR23353	2020/05/04 19:25:15 - [49:207.62.57] - 35 202707 295507 0(opbharath relam)[] - Role restrictions successfully passed for roles: opbharath role
Info	PTR23362	2020/05/04 19:25:15 - [49:207.62.57] - 35 202707 295507 0(cpbharath relam)(cpbharath role] - Sign-In successful, creating session
info	PTR23363	2020/05/04 19:25:15 - [49:207.62.57] - 35 202707 295507 0(cpbharath relam)(cpbharath role] - Session created, redirecting user to start page. Sign-In done.
Info	PTR24559	2020/05/04 19:25:15 - [49.207.62.57] - 35 202707 295507 0(opbharath relam)(opbharath role] - Automatically redirected from page 'login' to the next start page 'ldana/home/starter0.cgl?check=yes' before starting the session.
Info	PTR23471	2020/05/04 19:25:18 - [49:207.62.57] - 35 202707 295507 0(opbharath relam)(opbharath role] - VPN Tunneling: IP Address Pools obtained for the current session are 10.96.18.16
Info	PTR24639	2020/05/04 19:25:18 - [49:207:62:57] - 35 202707 295507 0(opbharath relam)(opbharath role] - VPN Tunneling: ACL rule [1] resource = ":", action = ACCEPT
info	PTR23468	2020/05/04 19:25:18 - [49.207.62.57] - 35 202707 295507 0(opbharath relam)(opbharath role] - VPN Tunneling: Session started with IP 10.96.18.13, hostname Bharaths-IPhone
Info	PTR10104	2020/05/04 19:25:38 - [49:207.52.57] - anand(Admin Users)[.Administrators] - 35 202707 205907 0:opbharath reliam - Policy Tracing turned off

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:

1. Select **Troubleshooting > Monitoring > Debug Log** to display the configuration page.

Figure 26 shows the configuration page for Pulse Connect Secure.

- 2. Complete the configuration as described in Table 8.
- 3. Click **Save Changes**. When you save changes with Debug Logging On selected, the system begins generating debug log entries.
- 4. 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.
- 5. 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.
- 6. Clear the **Debug Logging On** check box and click **Save Changes** to turn off debug logging.

Figure 26	Debug Logging Co	onfiguration Page	
-		Statute . In second of	-

	Monitoring	Tools	System Snapshot	Remote Debugging
bualoa Node N	Annitor Cluster	Diagnostic Logs		
buy Log nood i	ionitor orașter			
Save Changes	Reset	Save Debug Log	Clear Log	
Debug Log Settin	igs			
Current Log Size		39448	92 bytes	
ebug Logging Or	n			
1ax Debug Log S	ize	2	MB	
	Level	0		
ebug Log Detail)				
)ebug Log Detail nclude logs		s		
Debug Log Detail nclude logs				

Table 8Debug 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.