

Deploying a BYOD Policy for AirWatch Managed Devices

This example shows how to use Access Control Service 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:

Solution Overview Requirements Configuring the AirWatch MDM Service Configuring the Wireless Access Point Configuring the Device Access Management Framework Configuring an 802.1x Network Access Policy Configuring a Resource Access Policy

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 network access control solutions restrict user access?

MDM vendors have emerged to address the first issue. MDMs such as AirWatch 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 Control Service access management framework to enforce security policies.

Figure 1 shows a deployment with Access Control Service, a wireless access point, and the AirWatch MDM cloud service.

Figure 1: Solution Topology



The solution shown in this example leverages the Junos Pulse 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 Access Control Service role-mapping rules to implement the policy.

It is possible to use the MAC address as the device identifier, and, indeed, this is supported as a fallback plan. We recommend, however, that you implement the solution as shown here, using client certificates. This example shows how to enable security with the familiar 802.1x framework. 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.

Client certificates provide a more secure way to identity a device than the MAC address, which is vulnerable to spoofing. The 802.1x EAP methods that provide a TLS tunnel (PEAP, TLS and TTLS) can use a client certificate.

The following behavior is illustrative:

- TTLS/MS-CHAPv2—The client certificate presented during the TLS handshake is used to identify the device against the MDM records, and MS-CHAPv2 is used to
 authenticate the user against an authentication server.
- PEAP/MS-CHAPv2—Although PEAP does not allow for user authentication with a client certificate, the client certificate can still be presented during the TLS
 handshake and can be used to identify the device against the MDM records. MS-CHAPv2 is used to authenticate the user against an authentication server.
- TLS—The client certificate can be used to identify the device against the MDM records and authenticate the user against a certificate server.

The Juniper solution supports attribute-based Layer 2 network access control through familiar RADIUS return attribute policies, and it supports Layer 3 enforcement through 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.

Requirements

Table 1 lists version information for the solution components shown in this example.

Table 1: Component Version Information

Component	Version
ACS	Release 4.4R4-MDM or 5.0r1 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.
Wireless access point	Juniper Networks WLC2 wireless LAN controller and WLA322 access point are used in this example. Any wireless access point that supports deployment as an 802.1x authenticator 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 attributes—A standard set of data maintained for each device. For AirWatch, see Table 2.

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

Table 2: AirWatch Device Attributes

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

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.

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:
 - a. Certificate template. Create a configuration that specifies the field and type of identifier for client device certificates. See Figure 2. 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_UDID>, uid=<USER_ID>, o=Company
 - b. Credential profile. Create a configuration that specifies the certificate authority and certificate template configuration. See Figure 3.
 - c. Wi-Fi profile. Create a configuration that specifies the SSID, security options, and the credential configuration. See Figure 4.
- 3. Save and deploy the profile to devices registered with your organization. See Figure 5.
- 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 Access Control Service MDM server configuration. It is sent in the API call. See Figure 6.

Figure 2: AirWatch Certificate Template Configuration

Certificate Template - Add / Edit

Name*	Juniper Device Certificate	
Description		
Certificate Authority*	awlab99-ATL99LABCAD1-CA	•
Issuing Template	certificatetemplate:MobileUser2	
Subject Name*	CN={EnrollmentUser},serialNumber={DeviceUid}	0
Private Key Length [*]	2048	¥
Private Key Type*	Signing 🖉 Encryption 🗭 🚯	
San Type	♦ Add	
Automatic Certificate Renewal	∞ 0	
Auto Renewal Period (days)*	5	
Enable Certificate Revocation	× 0	
Publish Private Key		
	Save Save and Add Another Template Cancel	

Figure 3: AirWatch Credential Configuration

	🚯 General			
	🔦 Passcode	Credentials		
	S Restrictions	Credential Source	Defined Certificate Authority	
	🔶 Wi-Fi 1			
	A VPN	Certificate Authority"	AirWatch-ATLU2PRDCS10-CA	
	🛃 Email Settings	Certificate Template*	Juniper Device Certificate	
	🔀 Exchange ActiveSync			
	Application Control			
	🔀 Bookmarks			
	Credentials 1			
	🔲 Launcher			
	LDAP			
	🎉 Custom Settings			
ŀ				
		Save	Save & Publish Cancel	
F	Figure 4: AirWatch Wi-FI Configuration			
	WiFi with TLS			

General		
🔦 Passcode	VVI-FI	
奈 Wi-Fi 1	Service Set Identifier*	device-auth-8021x
D VPN	Hidden Network	
🛃 Email		
🔀 Exchange Web Services	Auto-Join	
LDAP	Security Type	WPA/WPA2 Enterprise
🛅 CalDAV		
CardDAV	Provv	
🔀 Web Clips	Brewi Turce	Nee
Credentials 1	Proxy type	None
<-→ SCEP		
Dock	Protocols	
S Restrictions	TLS	
A Parental Controls	TIC	
🕷 Gatekeeper	TILS .	
🔆 Custom Settings	LEAP	
	DEAD	
	FEAF	
	Save	Save & Publish Cancel

Page 4 of 27

	ior An watch Managed Devic	es - Teeninear Doeun	lentation	- Support	- Jun
VVIFI WITH TLS					
General	General				
Passcode	Name*	WiFi with TLS			
	Name				
	Description				
Erchange Web Services	Deployment	Managed	•		
CalDAV	Assignment Type	Auto	•		
CardDAV	Minimum Operating System	Anv	•		
🔀 Web Clips					
Credentials 1	Model	Any	-		
> SCEP	Ownership	Any	•		
Imil Dock					
S Restrictions	Allow Removal	Always	•		
A Parental Controls	Managed By	Juniper			
🕷 Gatekeeper					
K Custom Settings	Assigned Organization Groups*	Juniper		×	
		Start typing to add a new group			
	Cave	Save & Publish Cancel			
	Jave	Save & Lubisit Calicei			
Figure 6: AirWatch API Tenant Co	de Configuration				
Location Group					
JUNIPER SYSTEMS INC	stem / Advanced / API / REST				
		General Authentication	Network	Advanced	
System					1
Certificate Authorities	Current Setting \bigcirc Inherit \textcircled{O} Override				
Directory Services Email (SMTP)	pobling ADI appage would automatically apparate the ADI your	or the Lagatian Crown, De apphling the ADLaga	and offer dischling	would concrete a pr	
Enterprise Integration Getting Started		of the Euclation Group. Referabiling the Arriaco	ess aller disability	would generate a ne	w AFTRey.
Remote Control	API Key 4P 000LM AAAt8A9TQB 92	78			Reset
v API					
SOAP API					
Applications					
Device					
	Child Permission* 🔘 Inherit only 🔘 Override only 💿	Inherit or Override			
Email					
Telecom		Sa	ve		

Configuring the Wireless Access Point

The following wireless access point settings are important in this solution:

- 802.1x authentication
- RADIUS authenticator communication with the Access Control Service RADIUS server
- VLANs, if you want to assign user roles to VLANs

Refer to your vendor's documentation for information about the wireless access point 802.1x configuration. For information about Juniper Networks wireless access controllers, refer to the Juniper Networks wireless LAN services documentation.

Figure 7 shows the 802.1x configuration for a Juniper Networks WLC deployment similar to the one used in this example.

Figure 7: WLC 802.1x Authentication Configuration

Configure	Monitor		Maintain		
WIZARDS Quick Start	Ser	vices			
SYSTEM General IP Services	<u>R</u>	Name SP01 Service	SSID Jtest01 RSN	Encryption Yes	n Beacon Yes
VLANs Security		Service D	etails	SP01	View Help 🐲
WIRELESS Services Access Points RE Detect		SSID Authentic Encryptior	ation type	Jtest01 User author Yes	entication (802.1X)
AUTHENTICATION Users Devices RADIUS		Beacon Multicast VLAN Authentica 802.1X pro	conversion ate to otocol	Compliant RADIUS External R	▼ ▼ ADIUS ▼

Figure 8 shows the RADIUS configuration for a Juniper Networks WLC deployment similar to the one used in this example.

Figure 8: WLC RADIUS Configuration

Configure	Monitor		Maintain		
WIZARDS Quick Start	Services				
SYSTEM		Name	SSID	Encryption	Beacon
General	-	SP01	Jtest01	Yes	Yes
IP Services		Contine	DON		
Ports		Service	RSN/V	VPA	
VLANs		Service [)etails		View Help 💕
Security		Service p	rofile name	SP01	
WIRELESS		SSID		Jtest01	
Services		Authentio	ation type	User authentic	ation (802.1X)
Access Points		Encryptic	n	Yes	
RF Detect		Beacon			
AUTHENTICATION		Multicast	conversion		
Users		VLAN		compliant 👻	1
Devices		Authentic	ate to	RADIUS -	1
RADIUS		802.1X p	rotocol	External RADIU	IS 💌
		ОК А	pply		

Figure 9 shows the VLAN configuration for a Juniper Networks WLC deployment similar to the one used in this example.

Figure 9: WLC VLAN Configuration

Configure	Monitor	Maintain		Logout 📊 Save Co	onfig
WIZARDS Quick Start	VLANs			View Help 🝲	-
SYSTEM	ID	Name	IP	Ports	
General	1	default	10.0.1.25 /24	1	
IP Services	🥰 2	compliant	10.0.2.25 /24	1	
Ports	R 3	quest	10.0.3.25 /24	1 🖉	
VLANs		guest	10.0.3.23 724	-	
Security	4	remediation	10.0.4.25 /24	1	•
WIRELESS					-
Services	Create VL	AN			

Page 6 of 27

Configuring the Device Access Management Framework

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

- 1. Configuring an Authentication Protocol Set
- 2. Configuring the MDM Authentication Server
- 3. Configuring the Certificate Server
- 4. Adding the MDM Certificate to the Trusted Client CA Configuration
- 5. Configuring User Roles
- 6. Configuring a Realm and Role Mapping Rules
- 7. Configuring a Sign-In Policy

Configuring an Authentication Protocol Set

The authentication protocol set associated with the sign-in page must include the EAP method selected in the MDM Wi-Fi profile. The predefined authentication protocol set named **802.1x** shown in Figure 10 can be used as-is because it includes all the EAP methods currently configurable on MDMs.

Figure 10: Authentication Protocol Set Configuration Page

Junos Pulse Access Contro	ol Service
– System	
Status 🕨	Authentication Protocols >
Configuration	802.1X
Network	
Clustering •	
IF-MAP Federation	Name: 802.1X Label to reference this Authentication Pro
Log/Monitoring	Description: System created default
Reports •	authentication protocol -
- Authentication	
Signing In	Authentication Protocol
Endpoint Security	
Auth. Servers	Specify authentication protocols in preferred order
- Administrators	Available protocols: Selected protocols:
Admin Realms	CHAP Add > PAP
Admin Roles	EAP-GenericTokenCard EAP-TTLS
- Users	EAP-MD5-Challenge = Remove EAP-PEAP
User Realms	EAP-TLS
User Roles	MS-CHAP *
Junos Pulse	
- UAC	PEAP
MAC Address Realms	If EAP-PEAP is selected in authentication protocol and is not used for inner proxy, specify inner authentic
Infranet Enforcer	order
Network Access	Available protocols: Selected protocols:
Host Enforcer	EAP-GenericTokenCard EAP-JUAC
- Maintenance	EAP-TLS EAP-MS-CHAP-V2
System	Demour
Import/Export	Remove
Push Config	
Archiving	
Troubleshooting	TTLS
	If EAP-TTLS is selected in authentication protocol and is not used for inner proxy, specify inner authentic order
	Available protocols: Selected protocols:
	EAP-MD5-Challenge Add -> PAP
	MS-CHAP
	Remove EAP-MS-CHAP-V2
	EAP-GenericTokenCard
	Save Changes?
	Save Changes
If you want to define a custo	m set for this solution, configure the authentication protocol set.
To configure the authenticati	ion protocol set:
1. Select Signing In > Aut	hentication Protocols to display the configuration page.

- 2. Click New Authentication Protocol or select the predefined 802.1x set and click Duplicate.
- 3. Complete the configuration as described in Table 3.
- 4. Save the configuration.

Table 3: Authentication Protocol Set Configuration Guidelines

Settings	Guidelines
Name	Specify a name for the protocol set.

Settings	Guidelines
Description	Describe the purpose of the set so that other administrators are aware of it.
Authentication Protocol	Use the Add/Remove buttons to select protocols to be used. Use the up/down buttons to list the selected protocols in the preferred order.
PEAP	Use the Add/Remove buttons to select protocols to be used. Use the up/down buttons to list the selected protocols in the preferred order.
TLS	Use the Add/Remove buttons to select protocols to be used. Use the up/down buttons to list the selected protocols in the preferred order.

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 11.
- 3. Complete the configuration as described in Table 4.
- 4. Save the configuration.

Figure 11: Authentication Server Configuration Page

System						
Status 🕨	Auth Servers >					
Configuration +	Airwatch	Airwatch MDM				
Network +						
Clustering >	Settings					
IF-MAP Federation						
Log/Monitoring >						
Reports +	* Name: Alrwat	Ch_MDM Label to reference this server.				
Authentication	Type: Air Wat	ch				
Signing In						
Endnoint Security	Server					
Auth Servers	* Server Url:	https://apidev-as.Awmdm.com				
		link				
Admin Realms	Viewer Url:	https://apidev.awmdm.com/AirWatch/Devices/DeviceDetails/ <deviceattr.< th=""></deviceattr.<>				
Admin Roles		For example: https://cn11.airwatchportals.com/AirWatch/Devices/DeviceDetails/ <deviceattr.de< th=""></deviceattr.de<>				
	* Request Timeo	ut: 15 seco				
Lises Realms	Request filles					
User Relation						
Junos Dulso	Administrator					
	* Username:	admin				
MAC Address Realms	* Password:	*****				
Infranet Enforcer						
Network Access	* Tenant Code:	1040BLAHBLAHBLA				
Host Enforcer	Test Conne	ection				
- Maintenance						
System	Davica Idantifiar					
Import/Export	Please check the	ontions on the Users > Authentication > [Realm] > Authentication Policy > Certificate page. For evan				
Push Config >	users and remem	ber certificate information while user is signed in" option in order to request certificate from the client.				
Archiving >	Device Identity	Require certificate maximize security				
Troubleshooting •		Use certificate if present if certificate is not present, use MAC addres to search the device				
		Always use MAC address in case certificate does not contain device identifier				
	ID Template:	<pre>crefDN serialNumber></pre>				
	ib template.	attributes.				
		The template can contain textual characters as well as variables for substitution. Variables should the brackets like this <variable>. The variables are the same as those used in role mapping custom exp conditions. All of the certificate variables are available.</variable>				
		Examples:				
		<certdn.cn> First CN from the subject DN</certdn.cn>				
		<certattr.serialnumber> Certificate serial number</certattr.serialnumber>				
		<certattr.altname.xxx> Where xxx can be:</certattr.altname.xxx>				
		Email The Email alternate name				
		UPN The Principal Name alternate name				
		etc				
		<certdntext> The complete subject DN</certdntext>				
		cert- <certdn.cn> The text "cert-" followed by the first CN from the subject DN</certdn.cn>				
	ID Type:	UUID Universal Unique Identifier				
		Serial Number				
	Save Changes2					
	Le te enanges:					
	Save Changes Reset					
	Oave O	indigeo incost				

Table 4: Authentication Server Configuration Guidelines

Settings	Guidelines
Name	Specify a name for the configuration.
Туре	Select AirWatch.
Server	
Server Url	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:
	https://apidev-as.Awmdm.com
	Note: You must configure your firewalls to allow communication between these two nodes over port 443.
Viewer Url	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:
	https://apidev.awmdm.com/AirWatch/Devices/DeviceDetails/ <deviceattr.deviceid></deviceattr.deviceid>
Request Timeout	Specify a timeout period (0-60 seconds) for queries to the MDM server. The default is 15 seconds.
Administra	tor

Settings	Guidelines
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 6.
Device Ide	ntifier
Device	Access Control Service only.
identity	Select an option on whether to require that the MDM certificate is presented by the endpoint when signing in:
	 Require—Require that the device certificate pushed to client devices during enrollment be used at sign-in. If this option is selected, and the client device does not have a certificate, authorization fails. Use this option when you require endpoints to adhere to your certificate security requirements.
	 Use Certificate if present—Use the certificate to derive the device ID if the certificate is presented at sign-in, but do not reject authentication i the certificate is not present. You can use this option in conjunction with a role mapping rule and a remediation VLAN to identify devices that have not perfected MDM enrollment.
	 Always Use MAC address—In some cases, the MDM certificate might be configured without a device identifier. When the endpoint uses an 802.1x framework to authenticate, the Access Control Service can obtain the MAC address from the RADIUS return attribute callingStationID. The system can then use the MAC address as the device identifier.
	Note: This option is not present in Secure Access Service. A device certificate is required to determine device identity.
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>.</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>.</certdn.cn></user_id></device_udid>
ID Type	Select the device identifier type that matches the selection in the MDM certificate configuration:
	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.

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 12.
- 3. Complete the configuration as described in Table 5.
- 4. Save the configuration.

Figure 12: Certificate Server Configuration Page

- System					
Status 🔸	<u>Auth Servers</u> >				
Configuration >	New Certificate	e Server			
Network +					
Clustering >					
IF-MAP Federation >	* Name:	AirWatch_MDM_Ce	rt		Lab
Log/Monitoring	Lleer Name Templater	coortDN CNS			
Reports >	user Name remplate:	<cendiv.civ></cendiv.civ>			Ten
Authentication		The template can contain of the certificate variables	textual	characters as well as	varia
Signing In 🔹 🕨		or the certificate variable.	o are avi		
Endpoint Security		Examples:			
Auth. Servers		<certdn.cn></certdn.cn>	First C	N from the subject DN	i i
Administrators		<certattr.serialnumber></certattr.serialnumber>	Certific	ate serial number	
Admin Realms		<certattr.altname.xxx></certattr.altname.xxx>	Where:	xox can be:	
Admin Roles			Email	The Email alternate	name
🖃 Users			UPN	The Principal Name	alteri
User Realms				etc	
User Roles		<certdntext></certdntext>	The co	mplete subject DN	
Junos Dulso		cert- <certdn.cn></certdn.cn>	The tex	ct "cert-" followed by t	the fir
	Save Changes?				
MAC Address Realms					
Infranet Enforcer +	Save Change	Bosot			
Network Access	Save Change:	Reset			
Lines Colones					

Table 5: Certificate Server Settings

Settings	Guidelines
Name	Specify a name to identify the server within the system.

Settings	Guidelines
User Name Template	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 Access Control Service system. This value populates the <user> and <username> session variables for use throughout the rest of the system configuration.</username></user>
	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>.</certdn.uid></user_id></device_udid>

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 13.

Figure 13: Trusted Client CA Management Page

Junos Pulse Access Con	trol Service			Help Guidance Sign
- System				
Status 🔹	A Configuration			
Configuration				
Network •	Certificates			
Clustering •	Licensing Security Certificates	DMI Agent	Sensors Guest Access	
IF-MAP Federation	Device Certificates	As Trusted Serv	er CAs	
Log/Monitoring	Tusted Circlineates			
- Authentication	Users can be required to present va	lid client-side cer	rtificates to sign in(see th	ne realm-specific Certificate
Signing In	Authentication Policy page). Specify	trusted certification	ate authorities.	
Endpoint Security				
Auth. Servers	Auto-import options Prox	Delete		
- Administrators				
Admin Realms		Trusted for		
Admin Roles		client	M-Ed datas	Charles also dive
- Users		authentication?	valid dates	Status checking
User Realms	asgic36.asglab.juniper.net	Yes	2011/12/2 - 2017/05/24	Use OCSP
User Roles 🔹 🕨				

2. Click Import CA Certificate to display the page shown in Figure 14. Figure 14: Import Trusted Client CA Page

Junos Pulse Access Control Service					
– System					
Status	•	Configuration > Trusted Client CAs >			
Configuration	•	Import Trusted Client CA			
Network	•				
Clustering	•	Certificate file			
IF-MAP Federation	•				
Log/Monitoring	•	Import from: Browse			
 Authentication 					
Signing In	•	Import Trusted Client CA?			
Endpoint Security	•				
Auth. Servers					
- Administrators		Import Certificate			
Admin Realms	- 1-				

3. Browse to the certificate file, select it, and click Import Certificate to complete the import operation.

 Click the link for the Trusted Client CA to display its details. Figure 15 shows the configuration for this example. Figure 15: Trusted Client CA Configuration for AirWatch

Junos Pulse Access Contro	ol Service			
- System				
Status 🕨	Configuration > Trusted Client CAs >			
Configuration	Trusted Client CA			
Network •				
Clustering •	Certificate			
IF-MAP Federation				
Log/Monitoring	Issued Io: Dawlab99-ATL99LABCA01-CA			
Reports 🕨	Issued By: 🌗 awlab99-ATL99LABCA01-CA			
Authentication	Valid Dates: Apr 10 17:59:07 2012 GMT - Apr 10 18:09:05 2			
Signing In 🔹 🕨	Details: • Other Certificate Details			
Endpoint Security				
Auth. Servers				
- Administrators	Renew Certificate			
Admin Realms 🔹 🕨				
Admin Roles 🔹 🕨	Client certificate status checking			
- Users				
User Realms 🔹 🕨	None			
User Roles 🔹 🕨				
Junos Pulse	Use OCSP (Online Certification Status Protocol)			
- UAC	Use CRLs (Certificate Revocation Lists)			
MAC Address Realms	Use OCSP with CRL fallback			
Infranet Enforcer				
Network Access	Inherit from root CA			
Host Enforcer				
	Verify Trusted Client CA			
Import/Export	In addition to verifying the validity of client certificates, you can also			
Push Confin	and repeat up the chain until reaching the root trusted client CA.			
Archiving				
Troubleshooting	Trusted for Client Authentication			
	Uncheck here to exclude the CA from being trusted for client certifica			
	Advanced Certificate Processing Settings			
	Note: Enabling the certificate policy settings below will cause parts to be rejected.			
	Initial Inhibit Policy Mapping			
	Balicy managing for cortificate path is inhibited			
	Policy mapping for certificate path is inhibited			
	Initial Require Explicit Policy			
	Initial Require Explicit Policy			
	Path must be valid for at least one of the tertificate policies in the fi			
	Initial Policy Set:			
	Save Changes			

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 16.
- 3. Complete the configuration for general options as described in Table 6.
- 4. Save the configuration.
- 5. Click **UI options** to display the configuration page shown in Figure 17.
- 6. Complete the configuration for UI options as described in Table 6.
- 7. Save the configuration.
- 8. Click Session Options to display the configuration page shown in Figure 18.
- 9. Complete the configuration for session options as described in Table 6.

10. Save the configuration.

- 11. Click Agentless to display the configuration page shown in Figure 19.
- 12. Complete the configuration for agentless options as described in Table 6.
- 13. Save the configuration.

Figure 16: User Role Configuration Page – General Settings

Junos Pulse Access Contro	ol Service	
– System		
Status 🕨 🕨	Roles >	
Configuration •	Compromised	
Network 🛛 🔸		
Clustering +	General Agent Agentless	
IF-MAP Federation	Overview Restrictions Session Options UI Options	
Log/Monitoring		
Reports 🕨 🕨	* Name: Compromised	
Authentication	Name. Compromised	
Signing In 🛛 🕨	Description:	
Endpoint Security		
Auth. Servers	· ·	
- Administrators		
Admin Realms 🔹 🕨	Save Changes	
Admin Roles 🔹 🕨	ouve onlanges	
- Users	Ontions	
User Realms 🔹 🕨	Options	
User Roles 🔹 🕨	If these settings are not specified by any roles assigned to t	he user the s
Junos Pulse 🔹 🕨	In these settings are not specified by any roles assigned to t	the user, the s
- UAC		(= 1).)
MAC Address Realms	Session Options	(Edit)
Infranet Enforcer 🔷 🕨	VI Options	(Edit)
Network Access	Odvesev Settings for IC Access	(Edit)
Host Enforcer	- Ouyssey Settings for 10 Access	(Luit)
 Maintenance 	Odyssey Settings for Preconfigured Installer	(Edit)
System 🕨	Enable Guest User Account Management Rights	
Import/Export •		
Push Config 🔋 🕨 🕨	Cause shappers?	
Archiving •	Save changes?	
Troubleshooting •	Save Changes	

Figure 17: User Role Configuration Page – UI Options

Junos Pulse Access Contr	ol Service					
– System						
Status 🕨	Roles >					
Configuration	Compromised					
Network 🕨						
Clustering	General Agent Agentless					
IF-MAP Federation	Overview Restrictions Session Options UI Options					
Beports						
Authentication	Save Changes Restore Factory Defaults					
Signing In						
Endpoint Security	Header					
Auth. Servers						
- Administrators	Current appearance: JUNIPEC					
Admin Realms	NE TWOPKS					
Admin Roles	Logo image: Browse					
Users	Less than 40 p					
User Roles	Background color: #E3E3E3 Select from pa					
Junos Pulse						
- UAC						
MAC Address Realms	User Toolbar					
Infranet Enforcer	Determine the tools that are available to users at the top of the page on the IC.					
Network Access	Session Counter					
Host Enforcer	Post-Auth Sign-In Notification					
- Maintenance	If Role-based Post-Auth Sign-in Notification is configured in the sign-in url and this r					
Import/Export						
Push Config	(None)					
Archiving •	(
Troubleshooting	Personalized greeting					
	Show notification message on user's welcome page					
	Display the following message as a notification on the user's welcome page (if I					
	HTML tags are not supported and message size is limited. Consult your MDM se					
	Your device is compromised. Network					
	access may be limited.					
	Informative					
	Display the following message as a instruction on the user's welcome page (if b					
	Control Service Do not navigate away					
	from this page, or you will lose access					
	to protected resources.					
	Ψ					
	User Admin					
	Show User Admin instruction message					
	Display the following message as a instruction on the user admin page (if blank					
	tags to format the text.):					
	Ψ					
	Enable bulk user creation					
	Other					
	Show copyright notice and "Secured by Juniper Networks" label in footers					
	Save changes?					
	Save Changes Restore Eastery Defaults					
	Save Changes Restore Factory Defaults					

Figure 18: User Role Configuration Page – Session Options

Junos Pulse Access Control Se	rvice				
– System					
Status Ro	les >				
Configuration 🕨 U	Users				
Network					
Clustering G	eneral Agent Agentless				
IF-MAP Federation O	verview Restrictions Session	Options UI C	ptions		
Log/Monitoring	artbeat Interval is greater than o	r equal to Max Se	ession Length:	6 minutes.	
Reports •		the second s	2.02		
Authentication	Save Changes				
Signing In 🛛 🕨	Save Changes				
Endpoint Security					
Auth. Servers Se	ssion lifetime				
 Administrators 	* Max. Session Length:	6	minutes	(min: 6)	
Admin Realms		000	Ξ.		
Admin Roles 🔹 🕨	* Heartbeat Interval:	900	seconds	(15 - 1800	
Users	* Heartbeat Timeout:	1800	seconds		
User Realms	* Auth Table Timeout:	60	seconds	(60 - 8640)	
Junos Pulse					
	* Reminder Time:	3	minutes	(min: 3)	
MAC Address Realms	Enable Session Extensi	on		Allow User t	
Infranet Enforcer 🔹 🕨				Allow Enforc	
Network Access	Allow VPN Through Fire	wall		Useful for e	
Host Enforcer	········			consideratio	
- Maintenance					
System En	able session timeout warning				
Import/Export +					
Push Config 🔹 🕨	Enabled				
Archiving •	Oisabled				
Troubleshooting					
Ro	aming session				
	Roaming sessions allow user sessions to work across source IP addresses in from their desk and continue working from a conference room.				
	Enabled (maximize mobility)				
	Limit to subnet (some r	nobility, increase	ed security)		
	Disabled (maximize security)				
Sa	Save changes?				
	Save Changes				
Figure 19: User Role Configur	ation Page – Agentless Access				

anos Pulse Access Control Service			
– System			
Status 🕨 🕨	Roles >		
Configuration +	Users		
Network +			
Clustering +	General Agent Agentless		
IF-MAP Federation			
Log/Monitoring	Options		
Reports +	,		
- Authentication	Enable Agentless Access for this role		
Signing In 🛛 🕨			
Endpoint Security	Disable use of AJAX for heartbeats		
Auth. Servers			
- Administrators	Hide the Agentless page after Captive Portal redirect		
Admin Realms 🔹 🕨	6 1 1		
Admin Roles 🛛 🕨	save changes?		
- Users	Save Changes		
User Realms	Save Onlanges		

Table 6: User Role Configuration Guidelines

Settings	Guidelines
Overview tab	
Name	Specify a name for the configuration.
Description	Describe the purpose of the role so that other administrators are aware of it.
Options	Select UI Options so that you can customize a message to be sent to the device when the role is applied.
UI Options tab	

Settings	Guidelines
Personalized greeting	Select the Show notification message option and enter a message to be sent to the device (through the MDM API) after sign-in and this role has been applied, or after role reevaluation if it results in a role change to this role.
	In this example, we are using the system to enforce MDM enrollment by flagging compromised devices. The message, therefore, is:
	Your device is compromised. Network access may be limited.
	The message is forwarded to the device using the MDM server Push Notification feature.
	The content of your notification message can vary depending on whether the switch or access point supports change of authorization (CoA). If the CoA is supported, reauthentication is automatic, so your message might simply state that "your level of access has changed." If CoA is not supported, reauthentication needs to be done manually by the user in which case the message might state that "your level of access has changed, please reconnect."
	Note: When multiple roles are assigned, UI options are not merged. The UI options for the first role that matches are applied.
Session Optio	ns
Allow VPN Through Firewall	Enable this option to allow Infranet Enforcer traffic to act as a heartbeat and keep the session alive. This option is useful for iOS devices.

Agentless	
Enable agentless access	Select this option for roles that you provision to access the network from BYOD devices. The solution that integrates with MDMs depends on the native supplicant, not a Juniper agent.

Configuring a Realm and Role Mapping Rules

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

To configure the realm and role mapping rules:

- 1. Select Users > User Realms > New User Realm to display the configuration page shown in Figure 20.
- 2. Complete the configuration as described in Table 7.
- 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 21.
- 5. Complete the configuration as described in Table 8.
- 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 22.
- 8. Complete the configuration as described in Table 10.
- 9. Save the configuration.

Figure 20: Realm Configuration Page

Junos Pulse Access Contr	ol Service		
System			
Status 🕨	User Authentication Realms >		
Configuration •	AIRWATCH-CERTAUTH		
Network 🕨			
Clustering +	General Authentication Pol	icy Role Mapping	
IF-MAP Federation			
Log/Monitoring	* Name:		
Reports +		AIRWATOIFOEIRIAOTT	
Authentication	Description:	<u>^</u>	
Signing In 🔹 🕨			
Endpoint Security		Ŧ	
Auth. Servers			
- Administrators		When editing, start on the Role Mar	
Admin Realms 🔹 🕨		,,,	
Admin Roles 🔹 🕨	Servers		
- Users			
User Realms 🔹 🕨	Specify the servers to use for	authentication and authorization. To creat	
User Roles 🔹 🕨			
Junos Pulse 🔹 🕨	Authentication:	AirWatch Cert Auth	
UAC	Uses Bisselses (All inter-	Nana	
MAC Address Realms	User Directory/Attribute:	None	
Infranet Enforcer 🔹 🕨	Accounting:	None 💌	
Network Access	Device Attributes:	AirWatch 💌	
Host Enforcer			
- Maintenance	Device Check Interval:	10 minutes	
System 🕨			
Import/Export	Dynamic policy evalua	ation	
Push Config 🛛 🕨			
Archiving •	Other Settings		
Troubleshooting •	_		
	Authentication Policy:	Certificate restrictions	
	Role Manning	A Rules	
	Kole Mapping:	4 Kules	
	Save changes?		
	Save Changes		

Table 7: Realm Configuration Guidelines

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

Settings	Guidelines
Refresh roles	Do not select.
Refresh resource policies	Do not select.
Session Migration	n
Session Migration	Do not select this option. Session migration is useful for endpoints running Junos Pulse client software, which is not the case for the

Figure 21: Role Mapping Configuration Page

endpoints in this MDM example.

Junos Pulse Access Contro	bl Service		
– System			
Status 🕨	User Authentication Realms > AIRWATCH-CER	TAUTH >	
Configuration	Role Mapping Rule		
Network 🔸			
Clustering •	* Name: Compromised		
IF-MAP Federation			
Log/Monitoring	* Rule: If device has any of the following attr	ibute values	
Reports 🕨 🕨	Attributer licCompromicod	Attributes	
Authentication	Attribute: IsCompromised •	Altribules	
Signing In 🔹 🕨	is 🔽 1	▲ If more than one v	
Endpoint Security 🔹 🕨		If more than one v	
Auth. Servers			
- Administrators		· · ·	
Admin Realms 🔹 🕨			
Admin Roles 🔹 🕨	then assign these roles		
– Users			
User Realms 🔹 🕨	Available Roles:	Selected Roles:	
User Roles 🔹 🕨	Android Add ->	Compromised	
Junos Pulse 🔹 🕨	DeviceSecurityOK		
UAC	Remove		
MAC Address Realms	MAC Book		
Infranet Enforcer 🔹 🕨	MAC BOOK		
Network Access			
Host Enforcer	Stop processing rules when this rule m	atches	
- Maintenance			
System •	To manage roles, see the <u>Roles</u> configurati	on page.	
Import/Export •			
Push Config 🛛 🕨	Save changes?		
Archiving			
Troubleshooting +	Save Changes Save as Copy		

Table 8: Role Mapping Configuration Guidelines

Settings	Guidelines	
Rule based on	Select Device Attribute and click Update to update the configuration page so that it displays settings for role mapping using device attributes.	
Name	Specify a name for the configuration.	
Rule	Select a device attribute (see Table 9) and a logical operator (is or is not), and type a matching value or value pattern.	
	In this example, select isCompromised and the logical operator is , and enter the value 1 (true). This means that devices with a compromised status match the rule.	
Role assignment	Select the roles to apply if the data matches the rule.	

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

Table 9: AirWatch Device Attributes

Role Mapping Attribute Name	AirWatch Attribute Name	Description	Data Type
BlockLevelEncryption	BlockLevelEncryption	True if block-level encryption is enabled; false otherwise.	Boolean
complianceReason	ComplianceStatus	Values: Compliant, Non-Compliant.	String
CompromisedStatus	CompromisedStatus	True if the status is compromised; false otherwise.	Boolean
DataProtectionEnabled	DataProtectionEnabled	True if data protection is enabled; false otherwise.	Boolean

0

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

1

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 a issue in this release, you must use 1 for true and 0 for false.

Figure 22: Realm Configuration Page – Certificate Restrictions

Junos Pulse Access Cont	rol Service	Help Guid	
– System			
Status 🔹 🕨	User Authentication Realms >		
Configuration >	AIRWATCH-CERTAUTH		
Network			
Clustering 🔰	General Authentication Policy Role Mapping		
IF-MAP Federation	Source IP Browser Certificate Host Checker Limits RADIU	S Request Policies	
Log/Monitoring			
Reports)	Allow all users (no client-side certificate required)		
- Authentication			
Signing In	Allow all users and remember certificate information while user is signed in.		
Endpoint Security	Only allow users with a client-side certificate signed by Trusted Clier	nt CAs to sign in. To change the certification authority, see the Trusted Client CA	
Auth. Servers			
 Administrators 	You can optionally require specific values in the client certificate:		
Admin Realms 🔹 🕨	Castificate field (suggests "as")		
Admin Roles 🔹 🕨	Certificate field (example ch)	expected value	
– Users		Add	
User Realms 🔹 🕨			
User Roles 🔹 🔹			
Junos Pulse 🔹 🕨			
- UAC			
MAC Address Realms			
Infranet Enforcer	Save Changes		
	-		

Table 10: 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.

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

Configuring a Sign-In Policy

A sign-in policy associates devices with a realm.

To configure a sign-in policy:

- 1. Select Authentication > Signing In > Sign-In Policies to navigate to the sign-in policies configuration page.
- 2. Click New URL to display the configuration page shown in Figure 23.
- 3. Complete the configuration as described in Table 11.
- 4. Save the configuration.

Figure 23: Sign-In Policy Configuration Page

Junos Pulse Access Contr	ol Service		
– System			
Status 🕨	Signing In >		
Configuration	*/mdm/		
Network 🕨	, ,		
Clustering +	Save Changes		
IF-MAP Federation			
Log/Monitoring			
Reports 🕨	User type: () Users () Administrators		
- Authentication	Sign-in URL: */mdm/ Format:		
Signing In 🔹 🕨	Description:		
Endpoint Security			
Auth. Servers			
- Administrators	· · · · · · · · · · · · · · · · · · ·		
Admin Realms 🔹 🕨	Sign-in page: Default Sign-In Page		
Admin Roles 🔹 🕨	To create or manage pages, see <u>Sign-In pages</u> .		
- Users			
User Realms 🔹 🕨	Authentication realm		
User Roles 🔹 🕨	Specify what realms will be available when signing in.		
Junos Pulse 🔹 🕨			
- UAC			
MAC Address Realms	Delete		
Infranet Enforcer			
Network Access 🔹 🕨	Available realms Authentication protocol set		
Host Enforcer	AIRWATCH 🔹 - Not applicable - 💌 Add		
 Maintenance 	MOBILEIRON 802.1X-Phones		
System 🕨			
Import/Export	AIRWATCH 802.1X		
Push Config	AIRWATCH-CERTAUTH 802.1X-Phones		
Archiving			
Iroubleshooting			
	If more than one realm appears above, Odyssey Access Client or the IC sign-in page the first suitable realm from the list. If no realms appear above, sign-in will fail.		
	User may specify the realm name as a username suffix		
	When this option is selected, the username suffix will be used to specify a realr		
	Remove realm suffix before passing to authentication server		
	when this option is selected, the username surfix will be stripped from the		
	Configure Sign-in Notifications		
	Pre-Auth Sign-in Notification		
	Post-Auth Sign-in Notification		
	Save changes?		
	Save Changes		

Table 11: Sign-In Policy Configuration Guidelines

Settings 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 Rea	Im		
Realm	Select the realm you configured in the earlier step.		
Authentication Protocol Set	Select the protocol you configured in the earlier step.		
Realm name as a username suffix	Select this option if the username sent during sign-in includes a realm suffix.		
	To use this option, the realm name must match the username realm suffix configured in the MDN Wi-Fi profile. See Figure 4.		
	This configuration enables you to dedicate the realm to the MDM traffic. Non-MDM traffic passing through the same switch then belongs to a different realm.		
	Note: In some cases, you can use authentication protocol sets to segregate traffic into a particular realm. For example, assuming only mobile endpoints use TLS and other endpoints do not, an authentication protocol set containing only TLS can be created and associated with a particular realm through a sign-in policy.		
Remove realm suffix	Remove the realm suffix within system processes, such as rule processing and logs.		
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 an 802.1x Network Access Policy

The 802.1x network access policy framework is used for network communication between the wireless access point and the Access Control Service. This section describes the key configuration elements:

- 1. Configuring a Location Group
- 2. Configuring a RADIUS Client
- 3. Configuring a RADIUS Return Attributes Policy

Configuring a Location Group

A location group associates the RADIUS framework with sign-in pages.

To configure a location group:

- 1. Select UAC > Network Access > Location Group to navigate to the location group configuration pages.
- 2. Click New Location Group to display the configuration page shown in Figure 24.
- 3. Complete the configuration as described in Table 12.
- 4. Save the configuration.

Figure 24: Location Group Configuration Page

Junos Pulse Access Control Service			
System			
Status 🕨 🕨	Location Group >		
Configuration +	MDM		
Network 🔹 🕨			
Clustering +			
IF-MAP Federation	Location Group		
Log/Monitoring	* News	МРМ	
Reports 🕨	* Name:	MDM	
Authentication	Description:		
Signing In			
Endpoint Security	* Sign-in Policy:	*/mdm/ 💌	
Auth. Servers	Sign in Folicy.	/man/	
- Administrators	MAC Authentication Realm:	(none)	
Admin Realms 🔹 🕨			
Admin Roles 🔹 🕨	Save Changes?		
– Users			
User Realms	Save Changes		
Table 12: Location Group Configuration Guidelines			

Settings Guidelines Name Specify a name for the configuration.

Settings	Guidelines
Description	Describe the purpose of the location group so that other administrators are aware of it.
Sign-In Policy	Select the sign-in policy you configured in the earlier step.
MAC Authentication Realm	Do not select for this solution.

Configuring a RADIUS Client

The RADIUS client configuration is used for communication with the 802.1x authenticator—in this case, the wireless access point.

To configure a RADIUS client:

- 1. Select UAC > Network Access > RADIUS client to display the RADIUS client configuration pages.
- 2. Click New RADIUS Client to display the configuration page shown in Figure 25.
- 3. Complete the configuration as described in Table 13.

4. Save the configuration.

Figure 25: RADIUS Client Configuration Page

Junear Dullar Assess Control	C
Junos Pulse Access Control	Service

– System			
Status 🕨	RADIUS Client >		
Configuration	New RADIUS Client		
Network 🕨			
Clustering •			
IF-MAP Federation	RADIUS Client		
Log/Monitoring	* Name	MIC RIDA EL 2	
Reports 🕨	Name:	WLC-Blu-A-FI-3	
Authentication	Description:	3 FL WAP.	
Signing In 🔹 🕨			
Endpoint Security	* ID Address	10 1 1 1	
Auth. Servers	IF Address.	10.1.1.1	
- Administrators	* IP Address Range:	256	
Admin Realms 🔹 🕨	* Shared Secret:		
Admin Roles 🔹 🕨	Sharea Secret.		
- Users	* Make/Model:	Trapeze Networks	
User Realms 🔹 🕨	* Location Group:	MDM 🔽	
User Roles 🔹 🕨			
Junos Pulse 🔹 🕨	Dynamic Authorization Support		
- UAC	Synamic Autometicin Support		
MAC Address Realms	Support Disconnect Messages		
Infranet Enforcer 🔹 🕨			
Network Access	Save Changes?		
Host Enforcer			
- Maintenance	Save Changes		
System 🕨			

Table 13: RADIUS Client Configuration Guidelines

Settings	Guidelines
RADIUS Client	
Name	Specify a name for the configuration.
Description	Describe the purpose of the configuration so that other administrators are aware of it.
IP Address	Specify the IP address for the RADIUS authenticator.
IP Address Range	Specify the number of IP Addresses for the RADIUS authenticator.
Shared Secret	Specify the shared secret that matches the shared secret in the RADIUS authenticator configuration.
Make/Model	Select the Make/Model of the RADIUS authenticator.
Location Group	Select the location group you configured in the earlier step.
Dynamic Authorization Support	
Support Disconnect Messages	Send disconnect messages to supplicants if access is no longer authorized.

Configuring a RADIUS Return Attributes Policy

The RADIUS return attributes policy is a framework for role-based assignment of traffic to VLANs. The policy specifies the return list attributes to send to an 802.1X network access device, such as which VLAN that endpoints must use to access the network. If no policy applies, Open Port is the default action.

To configure a RADIUS return attributes policy:

- 1. Select UAC > Network Access > RADIUS Attributes > Return Attributes to display the RADIUS return attributes policy configuration pages.
- 2. Click New Policy to display the configuration page shown in Figure 26.

3. Complete the configuration as described in Table 14.

4. Save the configuration.

Figure 26: RADIUS Return Attributes Policy Configuration Page

Junos Pulse Access Contro	ol Service	
– System		
Status •	RADIUS Return Attribute	s Policies >
Configuration	MDM	
Network •		
Clustering	General	
IF-MAP Federation		
Log/Monitoring	* **	Commissed
Reports •	* Name:	Compromised
Authentication	Description:	A
Signing In		
Endpoint Security		
Auth, Servers		Ψ
- Administrators		
Admin Realms		
	Location Group	
User Realms		Specify the Location Group for which this policy applies,
User Roles		
Junos Pulse		Available Location Groups: Selected Location Group
UAC		Default MDM
MAC Address Realms		, Nud +
Infranet Enforcer 🔹 🕨		Remove
Network Access		
Host Enforcer		
- Maintenance	RADIUS Attributes	
System 🕨	KADIOS Attibutes	
Import/Export	Open port	
Push Config		10
	VLAN:	10 (1 - 4094)
Troubleshooting	Return Attribute:	
		Delete
		Radius Auth
		Server Attribute
		Value Value
		Filter-Id
	Add Session-Tim	eout attribute with value equal to the session lifetime
		Add Termination-Action attribute with value equal 1
	Interface	
	Interface	
		Specify the Interface which endpoints on this VLAN use to connect to th
		 Automatic (use configured VLANs)
		O Internal
		U External
	Roles	
	S	
		Policy applies to ALL roles
		Policy applies to SELECTED roles
		Policy applies to all roles OTHER THAN those selected below
		Available releas
		Available roles: Selected roles:
		Android Add -> Compromised
		MAC Book
		Test
		UAC 🔻
	Save changes?	
		NOTE: changes to this page will cause all L2 clients to drop their conne
		Save Changes Save as Conv
		Cure us oupy

Table 14: RADIUS Return Attributes 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.
Location Group	Select the location groups for which this policy applies. In this example scenario, select the location group you configured in the earlier step.
RADIUS Attributes	
Open port	Return authorization to open the port. This option does not restrict access to a particular VLAN.
VLAN	Return a VLAN ID that designates the VLAN for the session. In this example, the VLAN option is configured to place noncompliant traffic in a remediation VLAN.
Return Attribute	Select and configure other RADIUS attributes to send in the return message. None are configured for this example.
Add Session-Timeout attribute	Select this option to specify a session timeout. You can also use the role configuration to specify a session timeout.
Add Termination-Action attribute	Select this option to attempt reauthentication after session termination.
Interface	
Interface	Select the interface endpoints use to connect to the system.
Roles	
Roles	Select the roles to which the policy applies.

Configuring a Resource Access Policy

A resource policy enforces role-based access to resources protected by an Infranet Enforcer firewall. 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.

This example assumes you have deployed Infranet Enforcers to protect Web servers in your network. This example does not explain how to deploy an Infranet Enforcer. For information on the Infranet Enforcer, refer to its documentation.

In this scenario, the role configuration and role mapping configuration create a classification for Android devices. Figure 27 shows the user role configuration.

Figure 27: User Role Configuration Page – General Settings

Junos Pulse Access Contro	ol Service			
– System				
Status 🕨	Roles >			
Configuration	Android			
Network 🔹 🕨				
Clustering •	General Agent	Agentless		
IF-MAP Federation	Overview Restr	ictions Session Options UI Options		
Log/Monitoring				
Reports 🕨	* Name	Android		
Authentication	Name:	Android		
Signing In 🔹 🕨	Description:	A		
Endpoint Security 🔹 🕨				
Auth. Servers		Ψ		
- Administrators				
Admin Realms 🔹 🕨		Save Changes		
Admin Roles 🔹 🕨		ouve onlanges		
- Users	Ontions			
User Realms	options			
User Roles 🔹 🕨		If these settings are not specified by any roles assigned to	the user, the settings sr	
Junos Pulse 🔹 🕨		In these settings are not specified by any roles assigned to	and abory and bearings of	
- UAC		Consider Onlines	(5.4%)	
MAC Address Realms		Session Options		
Infranet Enforcer 🔹 🕨		VI Options	(Edit)	
Network Access		Odvssev Settings for IC Access	(Edit)	
Host Enforcer			(<u>cuic</u>)	
- Maintenance		Odyssey Settings for Preconfigured Installer	(<u>Edit</u>)	
System 🕨		Enable Guest User Account Management Rights		
Import/Export				
Push Config 🛛 🕨	Favo changes?			
Archiving	save changes?			
Troubleshooting •				
		Save Changes		

Figure 28: Role Mapping Configuration Page

Figure 28 shows the role mapping configuration.

System Status Configuration Network Clustering IF-MAP Federation Log/Monitoring Reports Authentication Signing In Endpoint Security Auth. Servers Admin Realms Admin Realms Admin Realms Junos Pulse User Realms Junos Pulse MAC Address Realms Infranet Enforcer Mattentace System Infranet Enforcer Mattentace System Instruct Export Mac Book Troubleshooting System Troubleshooting	Junos Pulse Access Contro	ol Service	
Status Configuration Network Clustering If-MAP Federation Log/Monitoring Reports Authentication Signing In Endpoint Security Auth.servers Administrators Admin Realms Junos Pulse WaC Address Realms Infranet Enforcer Maintenance System Import/Export Push Config Archiving Troubleshooting Save Changes Save Changes	– System		
Configuration Role Mapping Rule Network Clustering Clustering Rule based on: Device attribute Update IF-MAP Federation * Name: Android Log/Monitoring * Name: Android Reports * Rule: If device has any of the following attribute values Signing In * Rule: If device has any of the following attribute values Endpoint Security Attribute: model Auth. Servers Administrators Admin Realms Admin Realms Admin Realms Admin Realms Junes Pulsethen assign these roles Junes Pulse Available Roles: Orac Compromised Mac Address Realmsthen assign these roles Junes Pulsethen assign these roles Junes Pulsethen assign these roles Mac Address Realmsthen assign these roles Infranet Enforcerthen assign these roles Mac Address Realmsthen assign these roles Infranet Enforcerthen assign these roles Mac Cookthen assign these roles Systemthen assign these roles Import/Exportthen assign rules when this rule matches Troubleshooting Save changes Save Changes Save + New	Status 🔸	User Authentication Realms > AIRWATCH-CERTA	AUTH >
Network Clustering IF-MAP Federation Log/Monitoring Reports Authentication Signing In Endpoint Security Auth. Servers Administrators Addmin Roles User Roles Junos Pulse • UAC MAC Address Realms Infranet Enforcer Natintenance System Import/Export Push Config Archiving Troubleshooting Save Changes Save Changes	Configuration	Role Mapping Rule	
Clustering Rule based on: Device attribute Update IF-MAP Federation * Name: Android Constraints * Name: Android * Name: Android * Rule: If device has any of the following attribute values Signing In * Rule: If device has any of the following attribute values Signing In * Rule: If device has any of the following attribute values Signing In * Rule: If device has any of the following attribute values Signing In * Rule: If device has any of the following attribute values Signing In * Rule: If device has any of the following attribute values Administrators Admin Realms Admin Roles * android* Users Users User Realmsthen assign these roles Junos Pulse Available Roles: Oser Realmsthen assign these roles Add cess Selected Roles: Oropromised Add -> Push Config Add cess Archiving Stop processing rules when this rule matches Import/Export For manage roles, see the Roles configuration page. Push Config Save changes Save Changes Save + New	Network 🔹 🕨		s <u>eo</u> 2%
IF-MAP Federation Log/Monitoring Reports Authentication Signing In Endpoint Security Auth. Servers Administrators Administrators Administrators Administrators Administrators Administrators Administrators Administrators Junos Pulse User Realms User Roles Junos Pulse Auto C MAC Address Realms Infranct Enforcer Network Access Host Enforcer Maintenance System Import/Export Push Config Archiving Troubleshooting Save Changes Save Changes Save + New	Clustering +	Rule based on: Device attribute	Update
Log/Monitoring Reports Authentication Signing In Endpoint Security Auth. Servers Administrators Addinistrators Junos Pulse User Roles Junos Pulse Available Roles: Compromised DeviceSecurityOK group iOS Mac Book WAC Book Water Booting Stop processing rules when this rule matches To manage roles, see the Roles Save Changes Save Changes Save Changes	IF-MAP Federation		<u> </u>
Reports Authentication Signing In Endpoint Security Auth. Servers Administrators Admin Realms Admin Roles User Roles Junos Pulse User Roles Junos Pulse User Roles Junos Pulse Out C MAC Address Realms Infranet Enforcer Maintenance System Import/Export Push Config Archiving Troubleshooting Save Changes Save Changes Save + New	Log/Monitoring	* Name: Android	
 Authentication * Rule: If device has any of the following attribute values * Rule: If device has any of the following attribute values * Rule: If device has any of the following attribute values * Rule: If device has any of the following attribute values * Rule: If device has any of the following attribute values * Rule: If device has any of the following attribute values * Rule: If device has any of the following attribute values * Rule: If device has any of the following attribute values * Rule: If device has any of the following attribute values * Rule: If device has any of the following attribute values * Rule: If device has any of the following attribute values * Administrators Administrators Administrators Administrators Administrators Administrators Users Users Users Users User Realms Junos Pulse Available Roles: Compromised Device SecurityOK Group Remove Android Device Book WAC Book Wate Book Stop processing rules when this rule matches To manage roles, see the Roles configuration page. Save changes Save changes Save the Roles Save the Roles 	Reports 🕨		
Signing In Endpoint Security Auth. Servers Administrators Admin Realms Admin Roles Users User Roles Junos Pulse Uac MAC Address Realms Infranet Enforcer Network Access Host Enforcer Maintenance System System Import/Export Push Config Archiving Troubleshooting Signing In Attribute: Maintenance System Import/Export Push Config Archiving Troubleshooting Save Changes Save Changes Save Changes	- Authentication	* Rule: If device has any of the following attrib	ute values
Endpoint Security Auth. Servers Administrators Admin Realms Admin Roles User Realms User Realms User Roles Junos Pulse • UAC MAC Address Realms Infranet Enforcer Network Accesss Host Enforcer System Import/Export Push Config Archiving Troubleshooting Save changes Save Changes Attributes Maintenance Save Changes Save Changes Save + New	Signing In 🔹 🕨		
Auth. Servers Administrators Admin Realms Admin Roles Users User Roles Junos Pulse Uac MAC Address Realms Infranet Enforcer Network Access Host Enforcer System Import/Export Push Config Archiving Troubleshooting Save Changes Save Changes If more than one values I	Endpoint Security	Attribute: model 💌	Attributes
Administrators Admin Realms Admin Roles Users User Roles Junos Pulse UAC MAC Address Realms Infranet Enforcer Network Access Host Enforcer System Import/Export Push Config Archiving Troubleshooting Save changes Save Changes Save + New	Auth. Servers	ic 🖉 kan dan dak	
Admin Realms Admin Roles Users User Roles Junos Pulse UAC MAC Address Realms Infranet Enforcer Network Access Host Enforcer System Import/Export Push Config Archiving Troubleshooting Save changes Save Changes	- Administrators	is • "android"	If more than one val
Admin Roles Users User Roles Junos Pulse UAC MAC Address Realms Infranet Enforcer Network Access Host Enforcer System Import/Export Push Config Archiving Troubleshooting Save changes Save Changes	Admin Realms 🔹 🕨		
Users User Realms User Roles Junos Pulse UAC MAC Address Realms Infranet Enforcer Network Access Host Enforcer System Import/Export Push Config Archiving Troubleshooting Save Changes Save Changes	Admin Roles 🔹 🕨		-
User Realms then assign these roles User Roles then assign these roles Junos Pulse Available Roles: UAC Compromised Add → MAC Address Realms Infranet Enforcer Add → Network Access Posice SecurityOK Add → Maintenance Maintenance System Stop processing rules when this rule matches Import/Export To manage roles, see the Roles configuration page. Save Changes Save + New	- Users		
User Roles Junos Pulse Junos Pulse Available Roles: WAC Compromised MAC Address Realms Infranet Enforcer Infranet Enforcer OS Network Access MAC Book Maintenance Stop processing rules when this rule matches System ✓ Stop processing rules when this rule matches Import/Export ✓ Stop processing rules when this rule matches Push Config To manage roles, see the Roles configuration page. Save changes Save Changes	User Realms 🔹 🕨	then accient have relat	
Junos Pulse Available Roles: Selected Roles: WAC MAC Address Realms Infranet Enforcer Add -> Network Access IOS Remove Host Enforcer MAC Book Import/Export Push Config Troubleshooting Save changes Save Changes Save + New	User Roles 🔹 🕨	then assign these roles	
Infranet Enforcer Compromised Add -> Network Access Book Remove Host Enforcer MAC Book Remove Maintenance System Stop processing rules when this rule matches Import/Export Push Config To manage roles, see the Roles configuration page. Troubleshooting Save Changes Save + New	Junos Pulse 🔹 🕨	Available Roles: S	elected Roles:
MAC Address Realms Infranet Enforcer Network Access Host Enforcer Maintenance System Import/Export Push Config Archiving Troubleshooting Save changes Save Changes	🖃 UAC	Compromised	Android
Infranet Enforcer Network Access Host Enforcer Maintenance System Import/Export Push Config Archiving Troubleshooting Save changes Save Changes Save + New	MAC Address Realms	DeviceSecurityOKAdd ->	
Network Access iOS Host Enforcer MAC Book Maintenance System System Stop processing rules when this rule matches Import/Export To manage roles, see the Roles configuration page. Archiving Save changes? Save Changes Save + New	Infranet Enforcer 🔹 🕨	group	
Host Enforcer MAC Book Maintenance System System Stop processing rules when this rule matches Import/Export To manage roles, see the Roles configuration page. Archiving Save changes? Save Changes Save + New	Network Access	iOS	
Maintenance System Import/Export Push Config Archiving Troubleshooting Save changes? Save Changes	Host Enforcer	MAC Book *	
System Import/Export Import/Export Stop processing rules when this rule matches Push Config To manage roles, see the Roles configuration page. Archiving Save changes? Save Changes Save + New	- Maintenance		
Import/Export Import/Export Push Config To manage roles, see the Roles configuration page. Archiving Save changes? Save Changes Save + New	System 🕨	📝 Stop processing rules when this rule mat	tches
Push Config To manage roles, see the Roles configuration page. Archiving To manage roles, see the Roles configuration page. Troubleshooting Save changes? Save Changes Save + New	Import/Export +		
Archiving Troubleshooting Save changes Save + New	Push Config 🛛 🕨	To manage roles, see the Poles configuration	
Troubleshooting Save changes? Save Changes Save + New	Archiving •	To manage roles, see the <u>Koles</u> computation	r page.
Save Changes Save + New	Troubleshooting •	Save changes?	
		Save Changes Save + New	

To configure a resource access policy:

- 1. Select UAC > Infranet Enforcer > Resource Access to display the resource access policy configuration pages.
- 2. Click New Policy to display the configuration page shown in Figure 29.
- 3. Complete the configuration as described in Table 15.
- 4. Save the configuration.

Figure 29: Resource Access Policy Configuration Page

Junos Pul	se Access	Contro	Service

Junos Pulse Access Contr	ol Service				
– System					
Status 🕨	Infranet Enforce	Infranet Enforcer Resource Access Policies >			
Configuration	New Pol	icv			
Network 🕨		,			
Clustering •					
IF-MAP Federation	* Namo	Einanco Sonvers			
Log/Monitoring	Name:	Finance Servers			
Reports •	Description:	Currently, Android devices are not 🔺			
- Authentication		permitted to download from Finance			
Signing In 🔹 🕨		Servers.			
Endpoint Security		v			
Auth. Servers					
- Administrators	Resources				
Admin Realms		Conside the second second by this policy poplicy, one pay line			
Admin Roles 🔹 🕨		specify the resources for which this policy applies, one per line.			
- Users	* Resources:	10.10.0/24			
User Realms		tcp://*:1-1024 tcp://*:80,443			
User Roles 🔹 🕨		udp://10.10.10.0/24:*			
Junos Pulse 🔹 🕨		Ticmp://10.10.10.10/255.255.255.			
- UAC					
MAC Address Realms	Infranet Enfor	rcer			
Infranet Enforcer					
Network Access		Specify the Infranet Enforcer(s) to which this policy applies.			
Host Enforcer		Available Enforcers: Selected Enforcers:			
- Maintenance					
System 🕨		SRX650 (SRX) Add -> SIX 3400 (SIXX)			
Import/Export	Þ.	SRX5800 (SRX)			
Push Config 🛛 🕨		Remove			
Archiving					
Troubleshooting					

	Policy applies to ALL roles
	Policy applies to SELECTED roles
	Policy applies to all roles OTHER THAN those selected below
	Available roles: Selected roles:
	AnonGuest AnyHost AnyLoginURL AnyTime
Action	
	Allow access
	 Deny access
	 Reject access The Infranet Enforcer will reject access by sending an ICMP unreachable message for and by sending a TCP-RST for TCP traffic. 'Reject access' only works with ScreenOS v 6.3r11 and later. Previous versions will handle it as 'Deny access'.
	Deny / Reject Message:
Enforcer O	ptions
	Specify the Enforcer options that should be enabled. If enabled here, the option must also be take effect.
	ALL Enforcer Options
	SELECTED Enforcer Options
	Enforcer Options OTHER THAN those selected below
	Available options: Selected options:
	Antispam Logging IDP Web Filtering Antivirus
	VSYS:
Save chan	VSYS:
Save chan	VSYS: ges? NOTE: changes to this page will cause a slight interruption of service for Infranet Enforcer Res

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.
Infranet Enforcer	
Infranet Enforcer	Select the Infranet Enforcer that is deployed to protect the specified resources.
Roles	
Roles	Select the roles to which the policy applies. In this example, Android is selected.
Action	
Action	Select one of the following actions:
	 Allow Access
	 Deny Access
	 Reject Access
	In this example, we deny access from Android devices.
Enforcer Options	
Enforcer Options	Select all Infranet Enforcer features that should be applied to matching sessions.

Related Documentation

IC, MAG, SA Series

- Using Logs to Verify Proper Configuration
- Using Policy Tracing and Debug Logs
- Understanding the Device Access Management Framework
 IC, MAG Series
- User and Policy Administration Overview

Published: 2013-11-18

Site Map / RSS Feeds / Careers / Accessibility / Feedback / Privacy & Policy / Legal Notices

Copyright© 1999-2014 Juniper Networks, Inc. All rights reserved.