Endpoint Manager Mobile (EPMM) System 12 Common Criteria Administrative Guidance

Version 1.5

October 2025

2400 Research Blvd
Suite 395
Rockville, MD 20850

TABLE OF CONTENTS

1 Introduction 9

1.1 Purpose 9

1.2 Audience 9

1.3 Product Overview 9

1.4 Common Criteria Evaluated Platforms 10

1.5 Obtaining Support 11

1.6 Security Functionalities covered in the CC evaluation 12

2 General Guidelines 15

2.1 Overview 15

2.2 Accessing administrative interfaces 16

2.3 Connecting to EPMM from the CLI 16

2.4 Logging in 16

2.5 Logging out 16

2.6 Help commands 16

3 Initializing EPMM Server 17

3.1 Overview 17

3.2 Deployment 18

3.2.1 Configuring the EPMM Admin Portal 18

3.3 EPMM Server Installation and Configuration 19

3.3.1 Enabling Common Criteria mode 19

3.3.2 Enabling FIPS mode 20

3.3.3 Define Administrators and Users 22

3.3.4 Disable SSH 25

3.3.5 Import certificates 25

3.3.6 Configure TLS 25

3.3.7 Configure Syslog 25
3.3.8 Disable automatic updates 25
3.3.9 Configuring Email Alerts 26

4 Initializing EPMM Client 28
4.1 Overview 28
4.2 Deployment 28
4.2.1 EPMM Client Installation and configuration 28
4.2.2 Configure Common Criteria mode for MDM agents 29

5 Device Enrollment 33
5.1 Overview 33
5.2 Device Enrollment process 33
5.3 Prohibiting device users from unenrolling 36

6 Configuring Transport Layer Security (TLS) 36
6.1 Configure TLS 36
6.1.1 Configuring Cipher Suites 37
6.1.2 Configuring TLS Certificates for EPMM Server 39
6.2 Configuring Reference Identifiers 39
6.2.1 For MDM Server 40
6.2.2 For MDM Agent 42
6.3 Mutual Authentication 42
6.3.1 Configuring mutual authentication 42
6.3.2 Mutual authentication Trust certificate 43
6.4 Configuring a client identity certificate for mutual authentication 43
6.4.1 Generating a self-signed certificate 43
6.4.2 Configuring an Intermediate CA 44
6.4.3 Certificate enrollment for Local CA 45

6.4.4 Certificate enrollment for Client Identity Certificate 45
6.5 Importing x509v3 certificates as trusted root certificates 46
6.5.1 Deleting a Trusted Certificate 47
6.6 Configure the HTTPS Administrator HTTPS Port Settings 47

7 EPMM Server Management 48
7.1 Overview 48
7.2 FMT_SMF SFR Management Commands 48
7.2.1 Transition to the Locked State 48
7.2.2 Full Wipe of Protected Data 49
7.2.3 Unenroll From Management 51
7.2.4 Install Policies 51
7.2.5 Query Connectivity Status 59
7.2.6 Query Current Version of the Mobile Device Firmware/Software 60
7.2.7 Query Current Version of the Mobile Device Hardware 61
7.2.1 Query Current Version of the MDM Agent Software 62
7.2.2 Query the Current Versions of Installed Mobile Device Applications 67
7.2.3 Import X.509v3 Certificates 68
7.2.4 Install Applications 69
7.2.5 Update EPMM Software 70
7.2.6 Remove Applications 70
7.2.7 Update Password Parameters 70
7.2.8 Configuring Session Locking Parameters 72
7.2.9 Configure Wireless Network Policy 73
7.2.10 Configure Wireless Network Security Policy 76
7.2.11 Configure Application Installation Policy 77
7.2.12 Configure Enable/Disable Camera and Microphone 77
7.2.13 Security management Roles 79
7.3 System Management Commands 80

7.3.1 Overview 80
7.3.2 Configure Device Limit 80
7.3.3 Configure Unenrolling Devices 81
7.3.4 Configuring the Application Access Groups 82
7.3.5 Download Applications to Android Device 83
7.3.6 Configuring Server Alerts 83
7.3.7 Configuring the Sync Interval for a Device 86

8 Updating the EPMM System Software 88
8.1 Overview 88
8.2 Updating the EPMM Server Software 88
8.2.1 Determining The Current Version of the EPMM Server 88
8.2.2 Updating the EPMM Server Manually 89
8.2.3 Upgrade using Repository 92
8.3 Updating the Android Client 94
8.3.1 Determining The Current Running Version of the Android Client 94
8.3.2 Installing the MDM Agent software 94
8.3.3 Updating the MDM Agent Software 98
8.4 Self-Tests 98

9 Compliance 99
9.1 Configuring the Security Policy 99
9.2 Configuring an Android OS version alert 101
9.3 Defining a custom compliance action 102
9.4 Configuring Compliance Parameters 102

10 EPMM System Logs and Events Management 104
10.1 Auditable Events 104
10.2 Viewing Auditable Events on EPMM server 104

10.3 Configuring Audit Events on Android Devices 104
10.4 Pulling Android Device Logs 109
10.5 Exporting Android Device Audit Records 111

11 EPMM System Audit Record Examples 114
11.1 Audit events and their corresponding messages 148

12 Terms and Abbreviations 152

Figure 1: EPMM Admin Portal 19
Figure 2: Enable common criteria mode 20
Figure 3: CC mode status 20
Figure 4: Enabling FIPS mode 21
Figure 5: FIPS mode status 22
Figure 6: Add User 23
Figure 7: User creation 23
Figure 8: Assigning roles to users 24
Figure 9: Disable auto updates 26
Figure 10: Email Settings 26
Figure 11: Installing APK 28
Figure 12: Configuring DO mode 28
Figure 13: Selecting Device details 30
Figure 14: CA certificate installation 31
Figure 15: Device enrollment and management 33
Figure 16: Enrolling device 34
Figure 17: Device registration completed 35
Figure 18: TLS/SSL Page 36
Figure 19: Inbound cipher configuration 37
Figure 20: Outbound cipher configuration 38
Figure 21: MDM server reference identifier configuration 41
Figure 22: DNS Name 42
Figure 23: Creating certificate 44
Figure 24: Importing X509 certificates 46
Figure 25: Uploading certificate file 46
Figure 26: HTTPS Settings 47
Figure 27: Selecting device 48
Figure 28: Lock pop-up window 49

Figure 29: Wipe warning 50
Figure 30: Wipe Pop-up Window 50
Figure 31: Default policy 51
Figure 32: Configuring policy 52
Figure 33: Android policies 53
Figure 34: Select Device 59
Figure 35: Device detail window 60
Figure 36: Finding device 60
Figure 37: MD firmware version 61
Figure 38: Finding device model 61
Figure 39: Hardware model query 62
Figure 40: MDM Agent Home Page 63
Figure : Android Home Pull Down Menu 64
Figure : Android Mobile@Work Home > Settings Page 65
Figure : Android Mobile@Work Home > Settings About Page 66
Figure : Android Mobile@Work Home > Settings > About > Product Detail Page 67
Figure 45: View App version 68
Figure : New certificate import 69
Figure : Policy details 71
Figure : Security Policy, Password Parameters 72
Figure : Session lockout 73
Figure : Application repository(s) 77
Figure : Security Policy Page 78
Figure : Lockdown policy configurational window 78
Figure : User roles 80
Figure : Device enrollment limit 81
Figure : Add label 82
Figure : Event Settings 84
Figure : Device Status Event window 85
Figure : Default sync policy 87
Figure : Modify Sync policy 87
Figure : Admin portal dashboard 88
Figure : Information window 89
Figure : Online updates 90
Figure : Ivanti Support - Device and Platform Page Example 90
Figure : Update using repository 93
Figure : Policies Page 100
Figure : Security Policy modify window 101
Figure : Android version check 103
Figure : Audit logs 104
Figure : Samsung General Policy 106
Figure : Samsung general policy configuration 107
Figure : Audit Events configuration 109

Figure : Device selection for pulling logs 110
Figure : Pull client logs 111

1 INTRODUCTION

1.1 PURPOSE

This document details the operational and preparative procedures for the Common Criteria evaluation. It highlights the specific TOE configuration and administration functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration as defined in the Security Target [Endpoint Manager Mobile (EPMM) System 12 Security Target]. This document does not mandate configuration settings for the features of the TOE that are outside the evaluation scope.

1.2 AUDIENCE

This document is written for administrators configuring the TOE, specifically the Ivanti EPMM. To use this guide, a security administrator needs a broad understanding of networks in general and the internet in particular, networking principles, and network configuration. All the Sections in the Document are written in a sequence based on the steps an administrator should follow after receiving a brand new Ivanti Connect Secure Device.

1.3 PRODUCT OVERVIEW

The Ivanti Endpoint Manager Mobile (EPMM) System includes the Ivanti Endpoint Manager Mobile (EPMM) and the MDM Client software.

Ivanti Endpoint Manager Mobile (EPMM) is mobile management software that enables Administrators to set policies for mobile devices, applications, and content. EPMM enables mobile device management, mobile application management, and mobile content management capabilities and includes the following tools:

- Mobile Device Management (MDM) – Provides tools that manage and track mobile devices.
- Mobile Application Management (MAM) – Allows access to specific applications.
- Mobile Content Management (MCM) - Supports creating, organizing, governing, and storing digital assets.

EPMM enables administrators to securely manage the lifecycle of mobile devices and mobile applications, from registering a device with Ivanti EPMM, to retiring the device from EPMM management. Users of an Ivanti EPMM managed device can securely access corporate data, email, and mobile apps that are controlled and distributed using Ivanti EPMM.

The Common Criteria Target of Evaluation (TOE) is the Ivanti Endpoint Mobile Manager (EPMM) 12 System (Version 12). The TOE (EPMM) is a distributed TOE and consists of two software components: the EPMM MDM Server and the EPMM MDM Agent (also referred to as MDM Server and MDM Agent).

This Ivanti CC evaluation includes the Mobile Device Management (MDM) and the Mobile Application Management (MAM) functionality of the Ivanti EPMM. The Mobile Content Management (MCM) functionality of the EPMM is excluded from the CC evaluation. Additionally, the Target of Evaluation (TOE) includes Mobile Application Store (MAS) functionality that hosts

applications, authenticates Agents, and securely transmits applications to enrolled mobile devices.

The MDM Server is deployed as a virtual machine and manages and monitors one or more instances of an MDM Agent. The MDM Agent is an application running on an Android device. This evaluation includes MDM Agent running on two different Android devices and operating system version:

- Galaxy S22 Ultra 5G running Android 13
- Galaxy S23 Ultra 5G running Android 14

1.4 Common Criteria Evaluated Platforms

The MDM Server runs on a virtual system and is described in the following tables.

Table 1: MDM Server Hardware Detail (Operational Environment)

Model	Processor	GHz	Hypervisor
Dell PowerEdge R640 Server	*Intel(R) Xeon(R) Gold 5215 CPU (Cascade Lake)*	*2.10Ghz*	*VMware ESXi 7.02*

Table 2: MDM Server Software Detail (Operational Environment)

Item	Software
Operating System	*Oracle Linux 8.9*
Runtime Environment	*Java SE Run Java SE Runtime Environment v8 (1.8) on Oracle Linux 8.9*
Hypervisor	*VMWare ESXi 7.02*
Kernel	*Red Hat Compatible Kernel (RHCK) kernel package kernel-4.18.0-80.el8*

Table 3: The MDM Server TOE Component Build

Build Name	Cryptographic Libraries included in the Build	CAVP #	Other Libraries included in the Build
EPMM 12.3.1.0 Build 84	Ivanti MDM Bouncy Castle 1.0.2.4	#A6073	Apache 2.4
	Ivanti MDM OpenSSL Component 1.1.1g	#A6074	OTS Libraries identified in Appendix B

The MDM Agent consists of a software application deployed on one of two Android mobile devices.

Galaxy S22 Ultra 5G Android 13
Samsung Electronics Co., Ltd.
Galaxy S23 Ultra 5G Android 14
Samsung Electronics Co., Ltd.

The following tables include the Android device details.

Table 4: MDM Agent Host Hardware Detail (Operational Environment)

Manufacturer	Device Name	Models	Chipset Vendor	SoC	Microarchitecture
Samsung	Galaxy S22 Ultra 5G	SM-S908B, SM-S908B/DS, SM-S908U, SM-S908U1, SM-S908W, SM-S908N, SM-S9080, SM-S908E, SM-S908E/DS	Samsung	Exynos 2200 (AMD RDNA™ 3)	ARMv8
Samsung	Galaxy S23 Ultra 5G	SM-S918B, SM-S918B/DS, SM-S918U, SM-S918U1, SM-S918W, SM-S918N, SM-S9180, SM-S918E, SM-S918E/DS	Qualcomm	Snapdragon 8 Gen 2 Mobile Platform	ARMv8

1.5 Obtaining Support

In the event of software failure, customers may report security issues related to Ivanti EPMM https://forums.ivanti.com/s/contactsupport?language=en_US. Product Functionality not Included in the Scope of the Evaluation

- Ivanti Sentry is not included in the evaluation.
- The evaluated configuration does not include a CLI interface, or the Self-Service User Portal user interface.
- The EPMM evaluation does not include the Non-admin and Guest roles supported by Android devices.
- The EPMM evaluated configuration does not support connecting to the MDM Server using the SSH network protocol. SSH, also known as Secure Shell or Secure Socket Shell, provides a CLI.
- The EPMM Agent that was evaluated is the Federal Build and is acquired through Ivanti personnel. It is not the Ivanti commercial EPMM Agent, also known as mobile@work, available via Google Play and the Ivanti website.
- The Trusted Front End (TFE) functionality is not included in the evaluated configuration.

- SAML is not enabled in the CC evaluated configuration.
- ActiveSync is not enabled in the evaluated configuration.

1.6 Security Functionalities covered in the CC evaluation

The following security functionalities were evaluated as part of the Common Criteria evaluation. Each functionality is listed with a brief description of its role in the security of the TOE:

- **FAU_ALT_EXT.1 – Server Alerts (MDM_PP)**
  Ensures that the server can generate alerts to notify administrators of security-relevant events.

- **FAU_ALT_EXT.2 – Agent Alerts (AGT_PPM)**
  Ensures that the mobile device agent generates alerts for security-relevant events at the device level.

- **FAU_CRP_EXT.1 – Compliance Reporting of Mobile Device Configuration (MDM_PP)**
  Provides mechanisms to verify and report whether managed mobile devices comply with defined security policies.

- **FAU_GEN.1(1) – Audit Data Generation (MDM_PP)**
  Requires the server to generate audit records for defined security events.

- **FAU_GEN.1(2)/AGT – Audit Data Generation (AGT_PPM)**
  Ensures that the mobile agent generates audit records for relevant security events.

- **FAU_GEN.1(2)/SRV – Audit Generation (MAS Server) (MDM_PP)**
  Extends audit generation capabilities to the MAS server component.

- **FAU_NET_EXT.1 – Network Reachability Review (MDM_PP)**
  Provides functionality to determine and review the network reachability of managed devices.

- **FAU_SAR.1 – Audit Review (MDM_PP)**
  Allows administrators to review audit records for security analysis.

- **FAU_SEL.1(2) – Security Audit Event Selection (AGT_PPM)**
  Enables filtering and selection of audit events by administrators.

- **FAU_STG_EXT.1 – External Trail Storage (MDM_PP)**
  Supports secure storage of audit records on external systems.

- **FAU_STG_EXT.2 – Audit Event Storage (MDM_PP)**
  Ensures reliable storage of generated audit events on the TOE.

- **FCO_CPC_EXT.1 – Component Registration Channel Definition (MDM_PP)**
  Defines secure communication channels used during component registration.

- **FCS_CKM.1 – Cryptographic Key Generation (MDM_PP)**
  Specifies secure generation of cryptographic keys based on approved algorithms.

- **FCS_CKM.2 – Cryptographic Key Establishment (MDM_PP)**
  Ensures secure agreement or distribution of cryptographic keys.

- **FCS_CKM_EXT.4 – Cryptographic Key Destruction (MDM_PP)**
  Defines secure methods for destroying cryptographic keys when no longer needed.

- **FCS_COP.1.1(1) – Cryptographic Operation (Confidentiality Algorithms) (MDM_PP)**
  Requires use of approved algorithms for encryption to protect confidentiality.

- **FCS_COP.1.1(2) – Cryptographic Operation (Hashing Algorithms) (MDM_PP)**
  Requires use of secure hashing algorithms for integrity protection.

- **FCS_COP.1.1(3) – Cryptographic Operation (Signature Algorithms) (MDM_PP)**
  Ensures support for digital signatures using approved signature schemes.

- **FCS_COP.1.1(4) – Cryptographic Operation (Keyed-Hash Message Authentication) (MDM_PP)**
  Provides support for keyed-hash functions to verify message authenticity.

- **FCS_HTTPS_EXT.1 – HTTPS Protocol (MDM_PP)**
  Requires implementation of HTTPS using secure ciphersuites.

- **FCS_IV_EXT.1 – Initialization Vector Generation (MDM_PP)**
  Defines secure generation of initialization vectors for cryptographic operations.

- **FCS_RBG_EXT.1/AGT – Random Bit Generation (AGT_PPM)**
  Ensures the mobile agent generates random numbers using approved mechanisms.

- **FCS_RBG_EXT.1/SRV – Random Bit Generation (MDM_PP)**
  Ensures the server generates random numbers using approved mechanisms.

- **FCS_STG_EXT.1 – Cryptographic Key Storage (MDM_PP)**
  Provides secure storage mechanisms for cryptographic keys.

- **FCS_STG_EXT.1(2) – Cryptographic Key Storage (AGT_PPM)**
  Extends secure key storage requirements to the mobile agent.

- **FCS_TLS_EXT.1 – TLS Protocol (TLS_PKG)**
  Requires support for TLS to protect communications.

- **FCS_TLSC_EXT.1 – TLS Client Protocol (TLS_PKG)**
  Specifies secure behavior of the TLS client role.

- **FCS_TLSC_EXT.2 – TLS Client Mutual Authentication (TLS_PKG)**
  Ensures that the TLS client supports mutual authentication with the server.

- **FCS_TLSC_EXT.5 – TLS Client Supported Groups Extension (TLS_PKG)**
  Requires support for elliptic curve groups and secure negotiation.

- **FCS_TLSS_EXT.1 – TLS Server Protocol (TLS_PKG)**

Specifies secure behavior of the TLS server role.

- **FCS_TLSS_EXT.2 – TLS Server Mutual Authentication (TLS_PKG)**
  Ensures TLS server supports mutual authentication with clients.

- **FIA_CLI_EXT.1 – X.509 Unique Certificate (MDM_PP)**
  Requires each client to be uniquely identifiable using X.509 certificates.

- **FIA_ENR_EXT.1 – Enrollment of Mobile Device (MDM_PP)**
  Defines secure enrollment of devices into management.

- **FIA_ENR_EXT.2 – Agent Enrollment of Mobile Device (AGT_PPM)**
  Extends enrollment functionality to the mobile agent.

- **FIA_UAU.1 – Timing of Authentication (MDM_PP)**
  Requires user authentication at defined points of access.

- **FIA_X509_EXT.1(1) – X.509 Certificate Validation (MDM_PP)**
  Defines requirements for validating X.509 certificates.

- **FIA_X509_EXT.2 – X.509 Certificate Authentication (MDM_PP)**
  Ensures authentication using validated X.509 certificates.

- **FMT_MOF.1(1) – Management of Functions (MDM_PP)**
  Specifies management of defined TOE functions.

- **FMT_MOF.1(2) – Management of Functions (Enrollment) (MDM_PP)**
  Defines management responsibilities related to enrollment.

- **FMT_MOF.1(3) – Management of Functions (MAS Server Downloads) (MDM_PP)**
  Extends management functions to MAS server operations.

- **FMT_POL_EXT.1 – Trusted Policy Update (MDM_PP)**
  Requires trusted mechanisms for updating policies.

- **FMT_POL_EXT.2 – Agent Trusted Policy Update (AGT_PPM)**
  Ensures policy updates are trusted at the mobile agent level.

- **FMT_SMF.1(1) – Specification of Management Functions (Server-to-Agent) (MDM_PP)**
  Defines management functions for configuring agents from the server.

- **FMT_SMF.1(2) – Specification of Management Functions (Server-to-Server) (MDM_PP)**
  Defines management functions for configuring the EPMM server.

- **FMT_SMF.1(3) – Specification of Management Functions (MAS Server) (MDM_PP)**
  Defines management functions for MAS server.

- **FMT_SMF_EXT.4 – Specification of Management Functions (AGT_PPM)**
  Extends management function specifications to the mobile agent.

- **FMT_SMR.1(1) – Security Management Roles (MDM_PP)**
  Defines roles responsible for managing security functions on the server.

- **FMT_SMR.1(2) – Security Management Roles (MAS Server) (MDM_PP)**
  Defines roles responsible for managing security functions on the MAS server.

- **FMT_UNR_EXT.1 – User Unenrollment Prevention (AGT_PPM)**
  Prevents unauthorized removal of devices from management.

- **FPT_API_EXT.1 – Use of Supported Services and APIs (MDM_PP)**
  Ensures use of only approved and supported APIs.

- **FPT_ITT.1(2) – Internal TSF Data Transfer (MDM Agent) (MDM_PP)**
  Protects data transfer within the TOE boundary.

- **FPT_LIB_EXT.1/AGT – Use of Third-Party Libraries (AGT_PPM)**
  Ensures third-party libraries used by the agent are properly identified and controlled.

- **FPT_LIB_EXT.1/SRV – Use of Third-Party Libraries (MDM_PP)**
  Ensures third-party libraries used by the server are properly identified and controlled.

- **FPT_TST_EXT.1 – Functionality Testing (MDM_PP)**
  Requires testing of the TOE's security-relevant functionality.

- **FPT_TUD_EXT.1 – Trusted Update (MDM_PP)**
  Defines mechanisms for securely updating the TOE.

- **FTP_ITC.1(1) – Inter-TSF Trusted Channel (MDM_PP)**
  Requires secure trusted channels with authorized external IT entities.

- **FTP_ITC_EXT.1 – Trusted Channel (MDM_PP)**
  Ensures communications between TOE components are protected.

- **FTP_TRP.1(1) – Trusted Path for Remote Administration (MDM_PP)**
  Provides a secure channel for administrative access.

- **FTP_TRP.1(2) – Trusted Path for Enrollment (MDM_PP)**
  Provides a secure channel during device enrollment.

2 General Guidelines

2.1 Overview

The section provides a general overview of the administrative interface, and details on its access methods general instructions for logging in and logging out form the system and information about other commands for user assistance.

2.2 ACCESSING ADMINISTRATIVE INTERFACES

During setup, two local users having the same credentials are created, one for the Admin Portal and one for the System Manager. If you make changes to the roles or password for the Admin Portal user, the changes do not affect the System Manager user.

Use the following URLs to access the configuration screens in this document.

- **Admin Portal:** https://<fully-Qualified-Domain-name>:443/mifs
- **System Manager:** https://<fully-Qualified-Domain-name>:8443/mics

Note: The **Admin Portal** and the **System Manager** interfaces collectively act as the MDM server within the system. The Admin Portal is used for management and administrative tasks related specifically to the MDM agent, while the System Manager is responsible for the broader management and operation of the MDM server itself within the EPMM system. Thus, the EPMM serves as both, the MDM server and the MAS server.

2.3 CONNECTING TO EPMM FROM THE CLI

The CLI, or command line interface, enables authorized administrators to access certain functions from the command line in a terminal window.

2.4 LOGGING IN

To log into EPMM securely, use the network protocol SSH, also known as Secure Shell or Secure Socket Shell. SSH gives users, particularly system administrators, a secure way to access a computer over an unsecured network.

Procedure:

1. Use SSH to make the connection to EPMM.
2. Log in as the Administrator user established during installation.
3. Enter the password and click **Enter**.

The SSH interface is used to configure the system into the evaluated configuration, but once configured, the interface is then disabled.

2.5 LOGGING OUT

Enter **Ctrl-d** to terminate the CLI session and close the terminal window. You can also enter one of the following commands:

- **logout**
- **exit**

2.6 HELP COMMANDS

Two commands are available to help you use the CLI:

- help
- **?** (question mark)

Enter **help** to display a description of the interactive help system, including:

- Auto-complete keys
- Movement keys
- Deletion keys

Enter **?** to list available commands in the current mode or details for the current command. For example, the following command lists all commands in the current mode:
>?

3 INITIALIZING EPMM SERVER

3.1 OVERVIEW

This section describes how to initially install the EPMM Server software and itemizes the configuration steps that are required to deploy and initialize the EPMM Server into the Common Criteria evaluated configuration.
Once this is complete, refer to

Initializing EPMM Client to configure the Android Clients (EPMM Clients).

3.2 DEPLOYMENT

Complete the following steps to install Ivanti EPMM using Kernel-based Virtual Machine (KVM).
Procedure:

1. Create a VM that meets the specifications recommended below:
    - Minimum configuration of host machine:
        - Quad Ivanti EPMM CPU, 2 GHz clock rate
        - 16 GB RAM
        - 8 GB guest memory
    - **Supported KVM version**: QEMU emulator version 2.0.0 (Debian 2.0.0+dfsg-2ubuntu1.22) Ivanti EPMM supports only this KVM version, but later versions are compatible.
    - **Supported Virtual Machine Manager version**: 0.9.5 Ivanti EPMM supports only this Virtual Machine Manager version, but later versions are compatible.
    - **Supported Linux distribution**: Ubuntu Server version 14.4 (3.19.0-25-generic #26~14.04.1-Ubuntu SMP) Ivanti EPMM supports only this Linux distribution, but other Linux distributions are compatible.

2. In the Virtual Machine Manager, when creating a new virtual machine, select Generic for the OS type and the Version.
    - **Boot from BIOS firmware**: Ivanti defines supported and compatible as follows:
    - **Supported product versions**: The functionality of the product and version with currently supported releases was systematically tested as part of the current release and, therefore, will be supported.
    - **Compatible product versions**: The functionality of the product and version with currently supported releases has not been systematically tested as part of the current release and therefore is not supported. Based on previous testing (if applicable), the product and version are expected to function with currently supported releases.

3. Make sure the MAC address is set to: Static allocation.

3.2.1 CONFIGURING THE EPMM ADMIN PORTAL

The Admin Portal is installed as part of the system setup and is used to manage users, devices, apps, and configurations, settings, and policies.

Procedure:

1. Using the **EPMM System Manager**, navigate to **Settings > DNS and Hostname**.
2. The following page will appear.

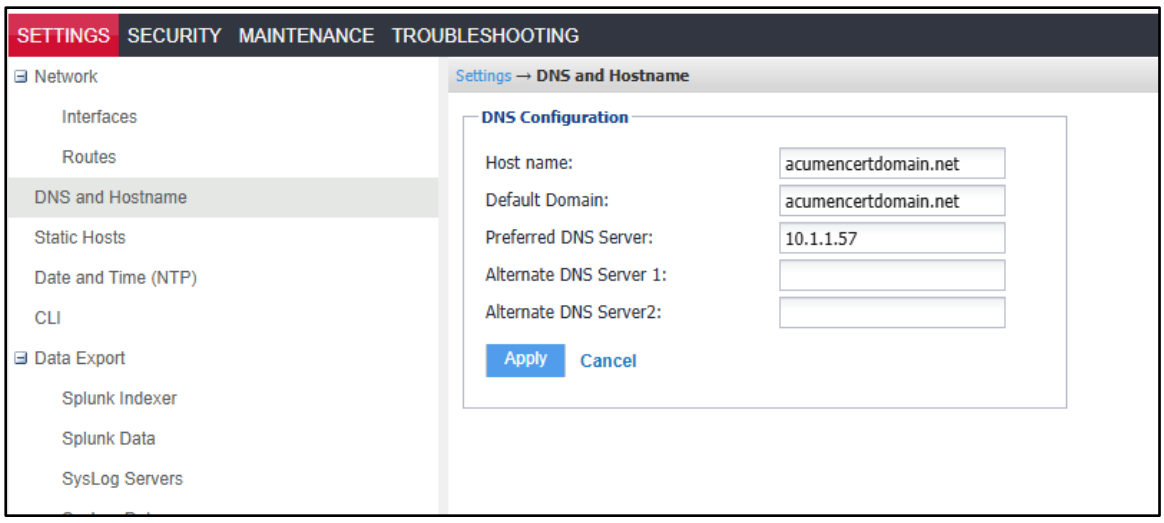


Figure 1: EPMM Admin Portal

3. Fill in the fields and select **Apply**.

3.3 EPMM Server Installation and Configuration

The following parameters must be configured and enabled for initializing the EPMM server in a common criteria evaluated configuration:

1. Enable Common Criteria mode
2. Enable FIPS
3. Define Administrators and Users
4. Disable SSH
5. Import certificates
6. Configure TLS
7. Configure Syslog
8. Disable automatic updates
9. Configuring Email Alerts

3.3.1 Enabling Common Criteria mode

The following steps must be executed using the CLI configuration utility of the EPMM server appliance.

Procedure:

1. Enter the enable mode by typing **enable**.

2. When prompted, enter the correct enable secret you set when you installed EPMM.
3. Once in enable mode, enter the config mode by typing **configure terminal**.
4. Once in the config mode, execute the command - **common_criteria_mode**.

```
EPMM(12.3.1.0-78)@acumencertdomain.net/config#common_criteria_mode
Turning on Common Criteria Mode.
Restarting iptupdate (via systemctl):                    [  OK  ]
Please reload the system for changes to take effect
```

Figure 2: Enable common criteria mode

5. Once the message as seen in the **Figure 2** is prompted, perform a reboot for the changes to take effect (common criteria mode). A reboot can be issued by executing the **do reload** command. (The system will not be reachable until the reboot is complete.)
6. The following messages would be prompted once **do reload** command has been issued:

   System configuration may have been modified. Save? [yes/no]

   a Enter **yes**.

   Configuration saved.

   Proceed with reload? [yes/no]

   b Enter **yes**.

   The system is going down for reboot NOW!

7. Once rebooted, enter **show common_criteria_mode_status** to see the EPMM server's status pertaining to CC mode.

```
EPMM(12.3.1.0-78)@acumencertdomain.net> show common_criteria_mode_status
Common Criteria Mode is enabled.
EPMM(12.3.1.0-78)@acumencertdomain.net>
```

Figure 3: CC mode status

Once enabled, the system would prompt a message stating "Common Criteria Mode is enabled." as depicted in **Figure 3**.

3.3.2 Enabling FIPS mode

The Federal Information Processing Standards (FIPS) Publication 140-3 is a U.S. government computer security standard used to accredit cryptographic modules. FIPS 140-3 defines four levels of security, simply named Level 1 to Level 4. Ivanti's EPMM products are FIPS 140-3 Level 1 Compliant.

The following steps must be executed using the CLI configuration utility of the EPMM

server appliance.

Prerequisites:
The Product(s) must be configured in the Common Criteria evaluated configuration.

Procedure:

1. Enter the enable mode by typing **enable**.
2. When prompted, enter the correct enable secret you set when you installed EPMM.
3. Once in enable mode, enter the config mode by typing **configure terminal**.
4. Enter the following command to enable FIPS: **fips**

```
EPMM(12.3.1.0-78)@acumencertdomain.net/config#fips
Setting system policy to FIPS
Note: System-wide crypto policies are applied on application start-up.
It is recommended to restart the system for the change of policies
to fully take place.
FIPS mode will be enabled.
Please reboot the system for the setting to take effect.

1/2 Updating /boot/grub2/grub.cfg ...

Generating grub configuration file ...
done

1/2 Updating /boot/grub2/grub.cfg ...Done


2/2 Updating prelink configuration


2/2 Updating prelink configuration...Done

Must reload system before FIPS 140 enabled.
EPMM(12.3.1.0-78)@acumencertdomain.net/config#
```

Figure 4: Enabling FIPS mode

5. Once the message as seen in the **Figure 4** is prompted, perform a reboot for the changes to take effect (FIPS mode). A reboot can be issued by executing the **do reload** command. (The system will not be reachable until the reboot is complete.)

6. The following messages would be prompted once the **do reload** command has been issued:

   System configuration may have been modified. Save? [yes/no]

   a Enter **yes**.

   Configuration saved.

   Proceed with reload? [yes/no]

   b Enter **yes**.

   The system is going down for reboot NOW!

7. Once rebooted, enter **show fips** to see the EPMM server's status pertaining to FIPS mode.

```
EPMM(12.3.1.0-78)@acumencertdomain.net> show fips
FIPS 140 mode is enabled.
EPMM(12.3.1.0-78)@acumencertdomain.net>
```

Figure 5: FIPS mode status

Once enabled, the system would prompt a message stating "FIPS 140 mode is enabled." as depicted in **Figure 5**.

3.3.3 Define Administrators and Users

3.3.3.1 User types

The product allows the following user and administrator types:
Device users: end users who use the managed devices (owned by themselves or the enterprise).

Super Administrators: manage devices and users throughout Ivanti EPMM. These administrators are assigned to the global space. The role that these administrators have that set them apart is Manage administrators and device spaces. Only administrators with this role can create and manage device spaces and assign roles and device spaces to administrators. Ivanti EPMM can have one or more Super Administrators.

Global Administrators: manage devices throughout Ivanti EPMM. These administrators are assigned to global space and can be assigned any roles other than Manage administrators and device spaces.

Device Space Administrators: manage only the devices and users assigned to the device spaces to which they are assigned. For example, an administrator assigned to the Dallas Help Desk device space can only manage devices assigned to that device space. The roles that can be assigned to Device Space Administrators are limited. For example, Device Space Administrators, if assigned the correct role, can view configurations or apply and remove configurations from a label. However, they cannot create or edit configurations.

3.3.3.2 User management

Users can be created on the EPMM server by the administrators. The users can be assigned roles which ultimately determine the amount of control it has over configuring the product. The following steps must be followed for creating the user and assigning them specific roles:

Procedure:

1. Using the **Admin Portal**, navigate to **Devices & Users > Users**.
2. For creating a new user, click on **Add > Add Local User**. A new window would be prompted in which the relevant user information must be added.

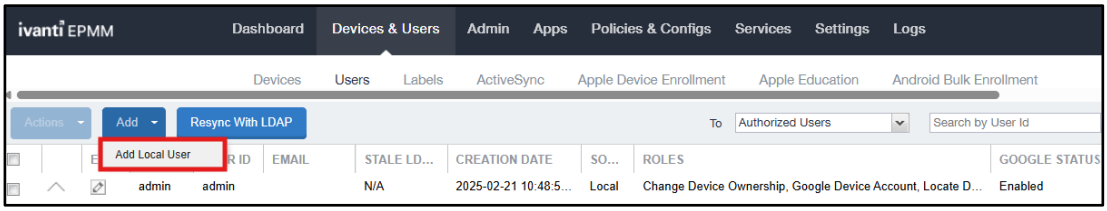


Figure 6: Add User

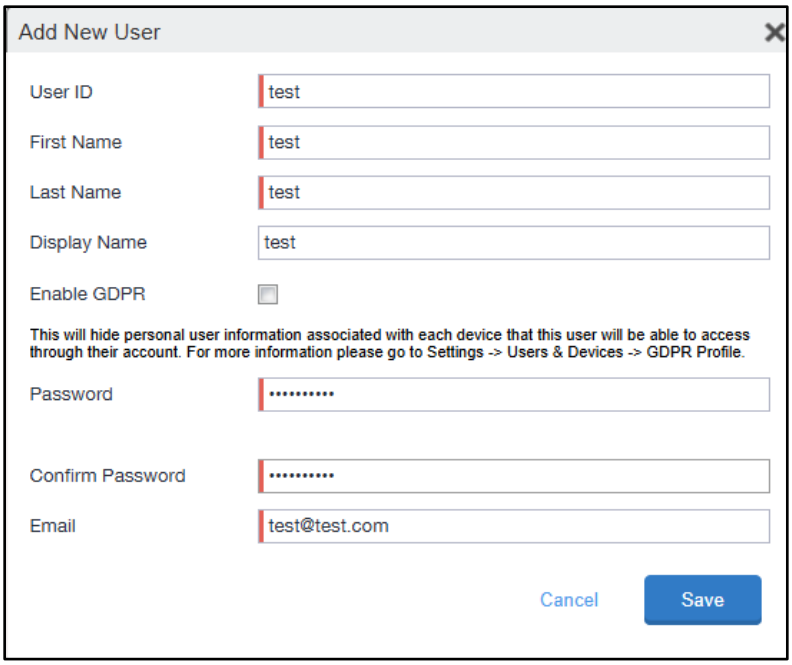


Figure 7: User creation

Use the following guidelines to complete the information:

Table 5: Add new user table

Field	Description
User ID	Enter the unique identifier to assign to this user. The following characters are allowed when entering a UserID. All other characters, including spaces, are prohibited. Letters (uppercase and lowercase) Numbers (0-9) Dashes (-) Underscores (_) Periods (.) At sign (@) Dollar sign ($) Hash tag (#) Extended ASCII/UTF-8
First Name	Enter the user's first name.
Last Name.	Enter the user's last name

Display Name	Optional name used to identify the device user. If you leave this field blank, then the display name will have the following format: Firstname Lastname
Password	Enter a password for the user. Valid passwords are determined by the password policy for local users. For passwords, the following password complexity requirements must be met: Minimum and maximum password length Minimum number of character classes in a password Character classes are: Lower case alphabetic characters Upper case alphabetic characters Numeric characters 0 through 9 Special characters, which are → ! = ({ [_ : - ; ~ ,) }] @ # ^ | $ In addition to the requirements specified, Ivanti EPMM enforces the following requirements: The password cannot have 4 or more repeating characters. The password cannot be the same as the user ID.
Confirm Password	Confirm the password for the user.
Email	Enter the user's email address.

Once all the user information has been filled, click on the Save button to create the new user.

3. Once a user has been created, specific roles can be assigned to the user. Select the desired user and click **Actions** and select **Assign Roles**.

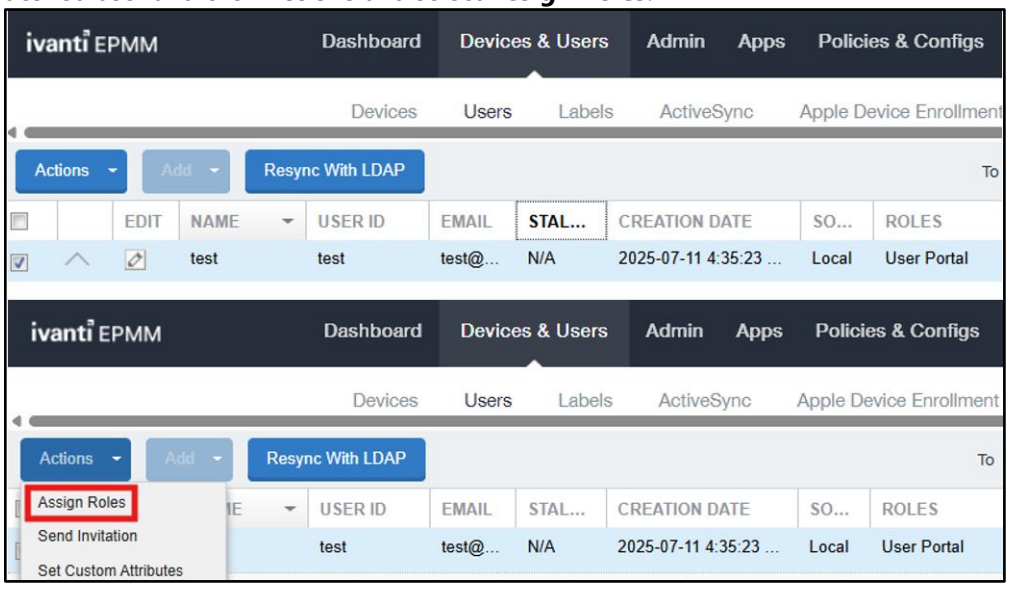


Figure 8: Assigning roles to users

4. Select roles for the users and click **Save**.

3.3.4 Disable SSH

To disable Secure Shell network protocol (SSH) and the command line interface (CLI), disable the option in the System Manager.

Procedure:

1. Using the **EPMM System Manager portal**, navigate to **Settings > CLI**.
   The CLI Configuration page displays.
2. For SSH, select **Disable**.
3. Click **Apply**.

3.3.5 Import certificates

The EPMM server supports importing and creation of x509 certificates. For further details, refer sections Configuring a client identity certificate for mutual authentication and Importing x509v3 certificates as trusted root certificates.

3.3.6 Configure TLS

The appliance employs secure communication between the product components (MDM server and agent) as well as with external IT entities using TLS. For further details, refer section Configuring Transport Layer Security (TLS).

3.3.7 Configure Syslog

The product allows transferring of logs to an external IT entity securely using TLS. A syslog server can be configured on the EPMM server. Refer section Configuring Reference Identifiers for the configurational information.

3.3.8 Disable automatic updates

Automatic system updates can be disabled. This can be done by performing the following:

Procedure:

1. Using the **Ivanti EPMM System Manager**, navigate to **Maintenance > Software Updates > Device and Platform Updates.**

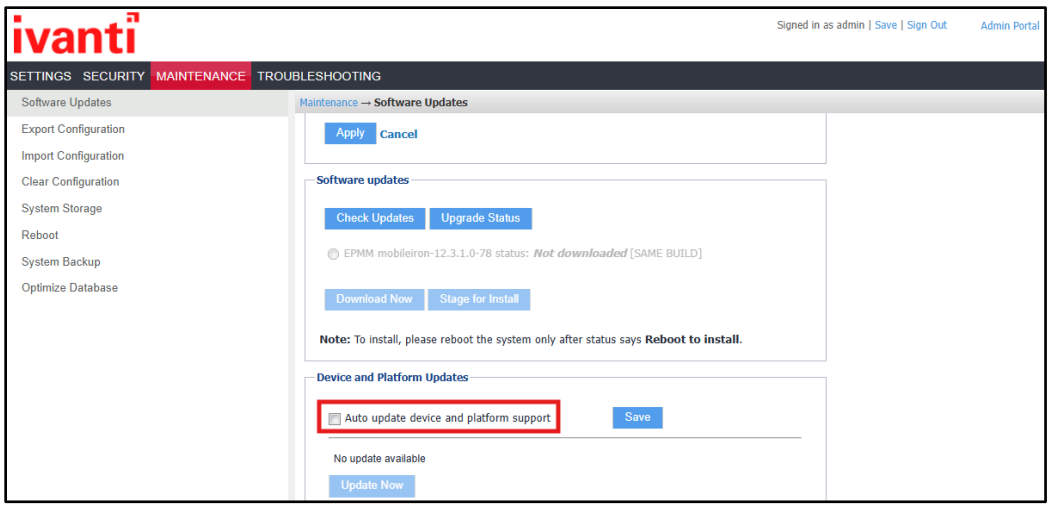


Figure 9: Disable auto updates

2. Uncheck the **Auto update device and platform support** checkbox.

3. Click **Save**.

3.3.9 Configuring Email Alerts

Procedure:

1. Using the **Ivanti EPMM System Manager**, navigate to **Settings > Email Settings**.

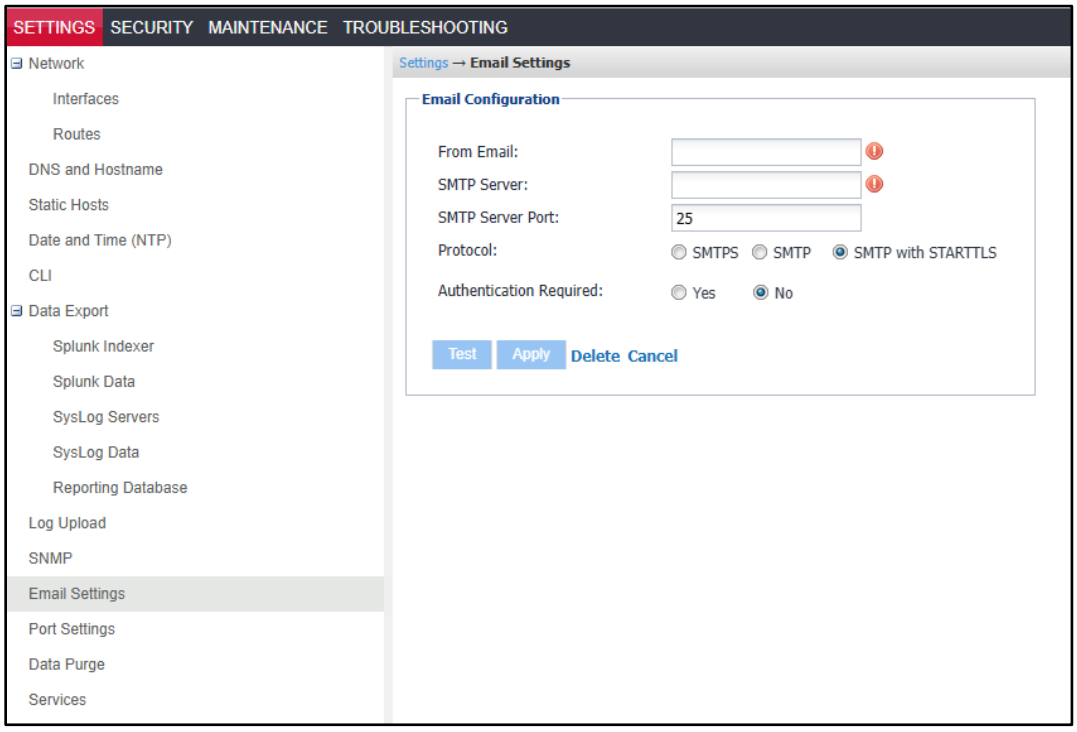


Figure 10: Email Settings

2. Use the following guide to fill in the fields:

Fields	Description
From Email	Specify the email address to use in the From field for all administrative email notifications. Make sure that the account for this email address has the right privileges to send emails to internal and external email domains.
SMTP Server	Specify the IP address or fully-qualified host name for the SMTP server the server will use
SMTP Server Port	Specify the port configured for the SMTP server.
Protocol	If the SMTP server you are configuring is a secured server, that is, it uses the SMTPS protocol, then select the **SMTPS** button. Otherwise, leave **SMTP** selected. If you want to allow an existing connection to upgrade to an encrypted connection, select **SMTP with STARTTLS**.
Authentication Required	Specify whether this SMTP server requires authentication. In most cases, this field will be set to **Yes**.
User Name	If you select **Yes** for **Authentication Required**, then this field displays. Enter the user name required for SMTP authentication.
Password	If you select **Yes** for **Authentication Required**, then this field displays. Enter the password required for SMTP authentication.
Confirm Password	If you select **Yes** for **Authentication Required**, then this field displays. Confirm the password required for SMTP authentication.

3. Once filled, click **Apply**.

4 INITIALIZING EPMM CLIENT

4.1 OVERVIEW

This section describes how to initially install the EPMM client software and itemizes the configuration steps that are required to deploy and initialize the EPMM client into the Common Criteria evaluated configuration.

4.2 DEPLOYMENT

This section details the procedure followed for deploying and initializing the MDM agent.

Procedure:

1. Ivanti's MobileIron product i.e. mobile client for an MDM (Mobile Device Management) platform must first be obtained on a device (laptop or desktop) with a compatible OS. This can be obtained with assistance from Ivanti's support team as an Android application package (APK).
2. Using command-line operation on the Android device using adb (Android Debug Bridge) install the APK by issuing the following command - **adb install <*APK_file_name*>**

   Note: The APK_file_name is the name of the APK file to be installed (for example, "mdmpp-MIClient-12.5.1.0.s.apk").

   This installation can be confirmed by observing the Success message on the screen.

```
C:\Program Files\platform-tools>adb install mdmpp-MIClient-12.5.1.0.s.apk
Performing Streamed Install
Success
```

Figure 11: Installing APK

3. Run the following command to provision the device into Device Owner (DO) mode – **adb shell dpm set-device-owner com.mobileiron/.receiver.MIDeviceAdmin**

```
C:\Program Files\platform-tools>adb shell dpm set-device-owner com.mobileiron.mdmpp/com.mobileiron.receiver.MIDeviceAdmi
n
Success: Device owner set to package com.mobileiron.mdmpp/com.mobileiron.receiver.MIDeviceAdmin
Active admin set to component com.mobileiron.mdmpp/com.mobileiron.receiver.MIDeviceAdmin
```

Figure 12: Configuring DO mode

4. Register the device by entering the server URL, username, and password.

Once the MDM Agent is deployed, proceed with registering and enrolling the MDM agent on the MDM server (EPMM server) using the Admin Portal. For more information, refer to section Device Enrollment.

4.2.1 EPMM CLIENT INSTALLATION AND CONFIGURATION

The following parameters must be configured and enabled for initializing the EPMM client in a common criteria evaluated configuration:

1. Configure Common Criteria mode for MDM agents
2. Enable FIPS on MDM agents
3. Import certificates on MDM agents

A device is available for management via the Ivanti EPMM server after it has been registered/enrolled by a device user or administrator. For more details refer section Device Enrollment.

4.2.2 Configure Common Criteria mode for MDM agents

To enable Common Criteria mode:
Procedure:

1. Using the **Admin Portal**, navigate to **Policies & Configs > Policies**.
2. Select **Add New > Security**.
3. In the Android section, select **Common Criteria Mode (Samsung Only and LG Only)**.

> Although EPMM passes the setting to LG devices, EPMM supports Common Criteria mode only with Samsung devices.

4. In the **Password** section:
    a. **Password** field: Select **Mandatory**.
    b. **Minimum Password Length**: Enter the required minimum.
    c. **Minimum Number of Complex Characters**: Enter the required minimum.
    d. **Maximum Password Age**: Enter the required maximum age of the password in days.
    e. **Maximum Number of Failed Attempts**: Select **0**.
    f. **Password History**: Select **0.**
5. Set **Device Encryption** (data-at-rest protection) to **On**.
6. Set **SD Card Encryption** (removable media data-at-rest protection) to **On**.
7. You can also select these other settings that support Common Criteria mode (**Bold** text indicates the field on the security policy):
    a. Session locking policy (**Maximum Inactivity Timeout**)
    b. Strict TLS requirements (**Require strict TLS for Apps@Work**)
8. Click **Save**.
9. Select **Actions > Apply To Label**.

10. Select a label that identifies the targeted Samsung devices.

11. Click **Apply** > **OK**.

4.2.2.1 Confirming Common Criteria mode on Samsung devices

To confirm that Common Criteria mode has been enabled for a Samsung device:
Procedure:

1. Using the **Admin Portal**, navigate to **Devices & Users**.
2. In the Devices page, find the entry for the device.
3. Display device details (see next figure).

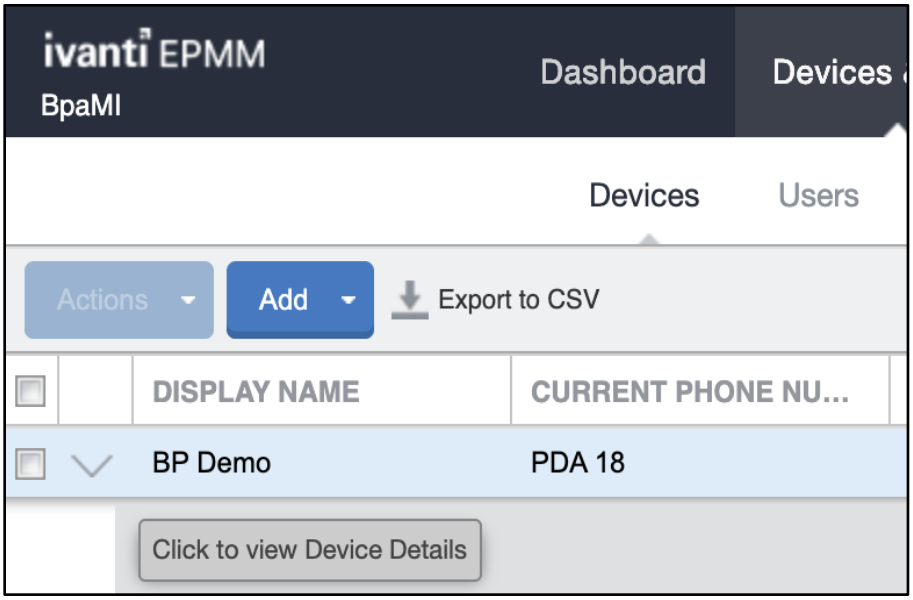


Figure 13: Selecting Device details

4. Click the **Policies** tab.
5. Scroll down to the Common Criteria Mode setting.
   Once the entry for this setting displays Enabled in the Device Value column, Common Criteria Mode is considered as enabled for the client.

4.2.2.2 Enable FIPS on MDM agents

To enable FIPS mode for Ivanti's Mobile@Work (MobileIron) client on a Samsung device running Android 13, FIPS support must be configured on the Ivanti EPMM server-side. Refer section Enabling FIPS mode for more information.

4.2.2.3 Import certificates on MDM agents

Note: The following procedure is applicable only for Samsung Galaxy S22 Ultra 5G running

Android 13 and Galaxy S23 Ultra 5G running Android 14 devices.
This method is primarily applicable when a closed certificate structure is used, such as for testing with self-signed certificates. It does not apply to certificates issued by third-party trusted CAs.

Procedure:

1. Navigate to device **Settings**.
2. Go to **Security and privacy > More security settings > Install from device storage > CA certificate.**
3. Click on the **Install anyway** option.
   Select the certificate file (CA certificate) from the local storage for uploading on to the device (MDM agent).
   Once installed, a message would be prompted indicating successful installation.

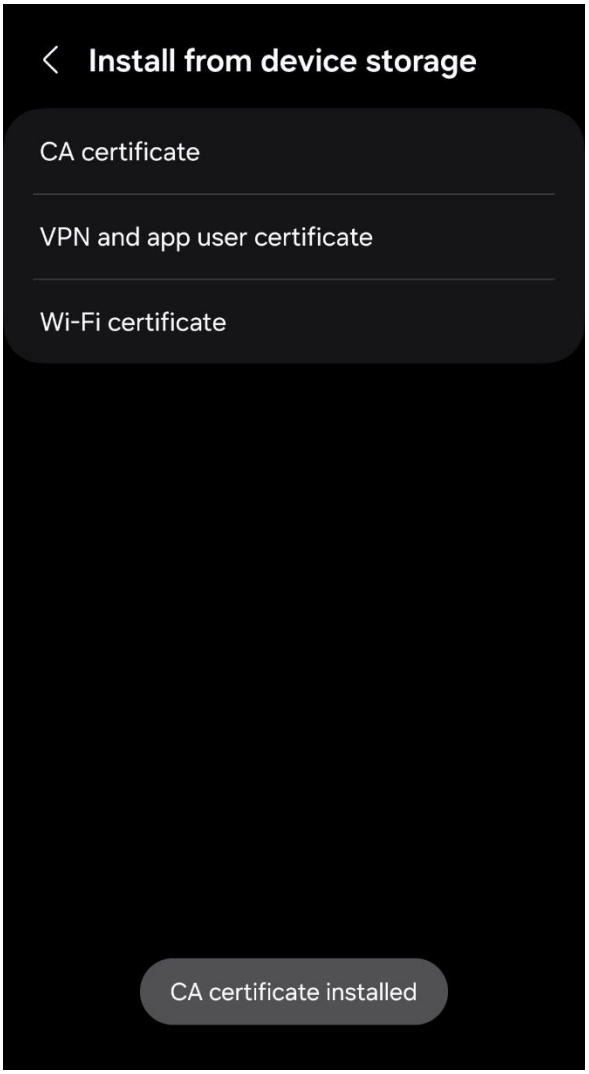


Figure 14: CA certificate installation

4. The certificate post installation can be verified under **Security and privacy > More security settings > View security certificates > User**

5 DEVICE ENROLLMENT

5.1 OVERVIEW

This section describes the process of enrolling/registering a device (MDM agent) on the EPMM server (MDM server). *Registering* and *enrolling* are two terms used to describe the same process of associating a mobile device with a EPMM mobile device management (MDM) server.

Figure 15 provides a visual representation of the device enrollment procedure and configuration for management via Ivanti EPMM server.

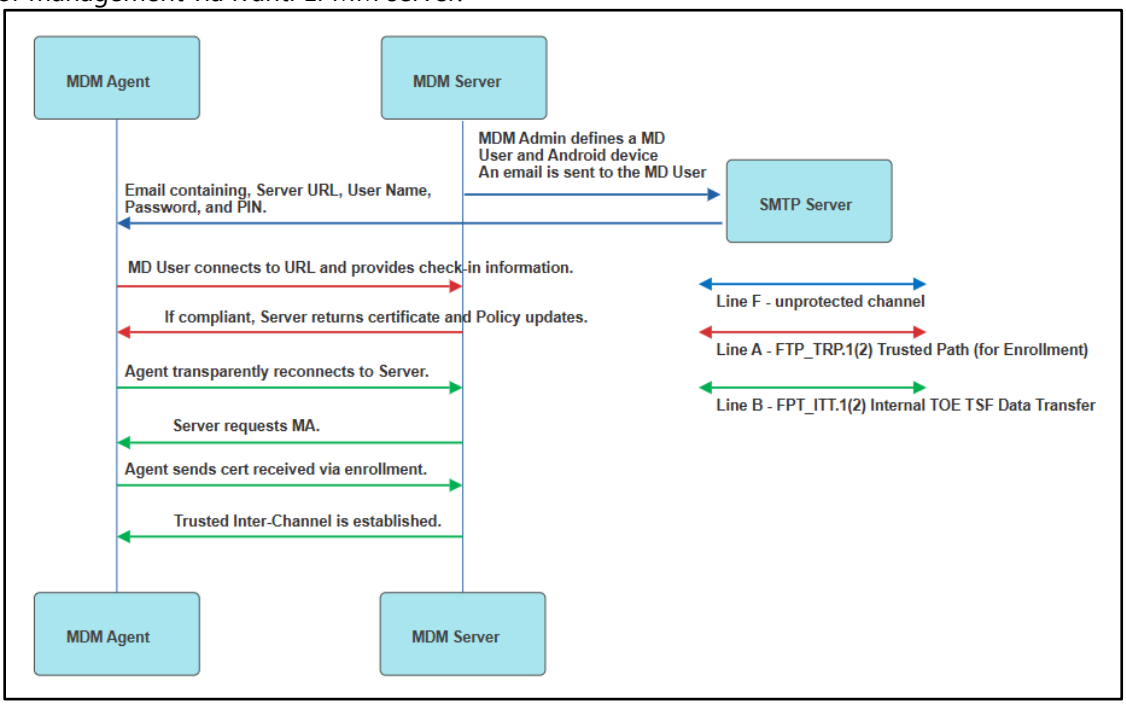


Figure 15: Device enrollment and management

5.2 DEVICE ENROLLMENT PROCESS

Prerequisites:

1. The user (local or LDAP) associated with the device must be available for selection at the time of registration.
2. User Portal role must be assigned to the user.
3. The following information must be available for the device:
    - Phone number (if any)
    - Country
    - Platform

Procedure:

1. Using the **Admin Portal**, navigate to **Devices & Users > Devices**.
2. Click on **Add > Single Device**.
3. A pop-up window would be displayed. Modify one or more of the following fields, as necessary.

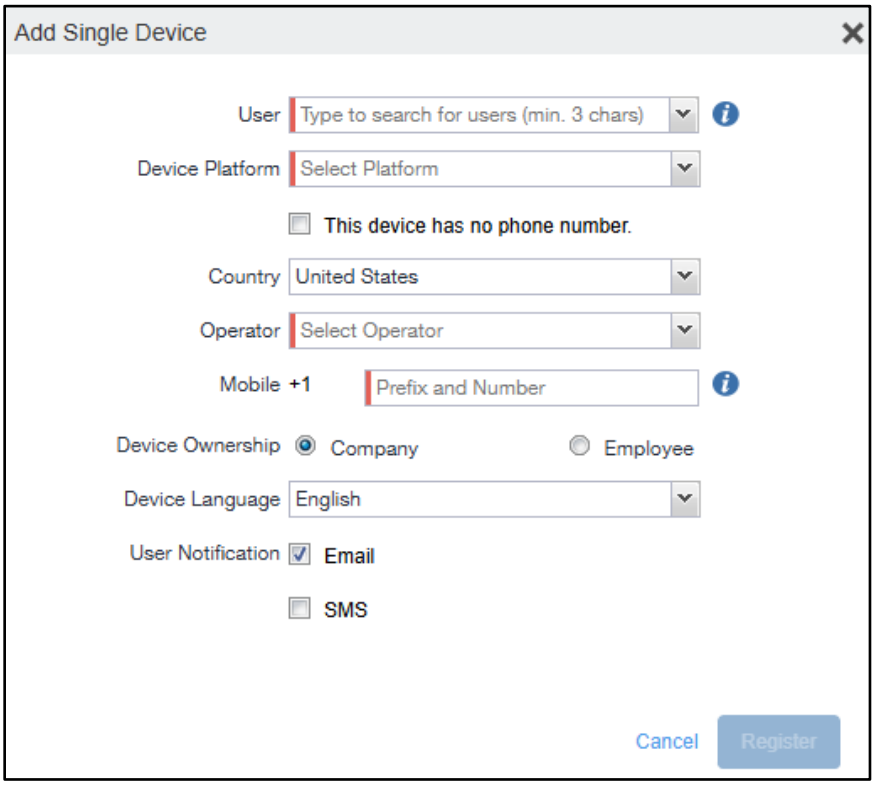


Figure 16: Enrolling device

4. Refer **Table 6: Enrolling device fields** for details on filling each field.

Table 6: Enrolling device fields

Fields	Description
User	Enter user information to locate the user account. For example, you might enter the user ID, first name, last name, or email address. Select the user you want to work with from the drop-down list of matching accounts.
Device Platform	Select the name of the operating system used on the phone. (MDM agent/device)
This device has no phone number (checkbox)	If the device is not associated with a cellular operator or a data plan with the current operator, checkmark this option.
Country	Select one of the supported countries from the drop-down list. Selecting the correct country populates the Country Code field. If the country you need is not displayed, you may need to alter the default country list. **Select Settings >**

	System Settings > Users & Devices > Registration.
Operator	Select the name of the mobile service operator for this phone. If a country having a country code other than 1 is selected, then this field is hidden.
Mobile	Enter the phone number for the device. Your selection from the Country list will populate the Country Code field. Enter the prefix and number without spaces, dashes, leading zeros, or parentheses.
Device Ownership	Select Company if this phone is owned by the enterprise. Select Employee if this phone is owned by the user.
Device Language	To communicate with the device user in a language other than the default language, select a language from the drop-down list. Languages must first be enabled under **Settings > System Settings > General > Language**. If the device reports a locale associated with a different language, then the language associated with the locale will be used.
User Notification	• **Email**: Select this check box if the notification concerning registration status for the device is to be sent to the registered user via email. • **SMS**: Select this check box if the notification concerning registration status for the device is to be sent to the registered user via SMS messages. This option is disabled by default. If set to true, the device must have a phone number registered with Ivanti EPMM.

Note: The change in the enrollment status for the device would be notified to the user/administrator via the options selected in the *User Notification* field during the device enrollment process.

5. Once completed, click **Register**.

   After a brief pause, a pop-up window lists instructions for the next step. The content of this pop-up window varies based on the OS and type of the device. Consider leaving this message displayed until the registration has been completed. Note that the instructions also appear in the log.

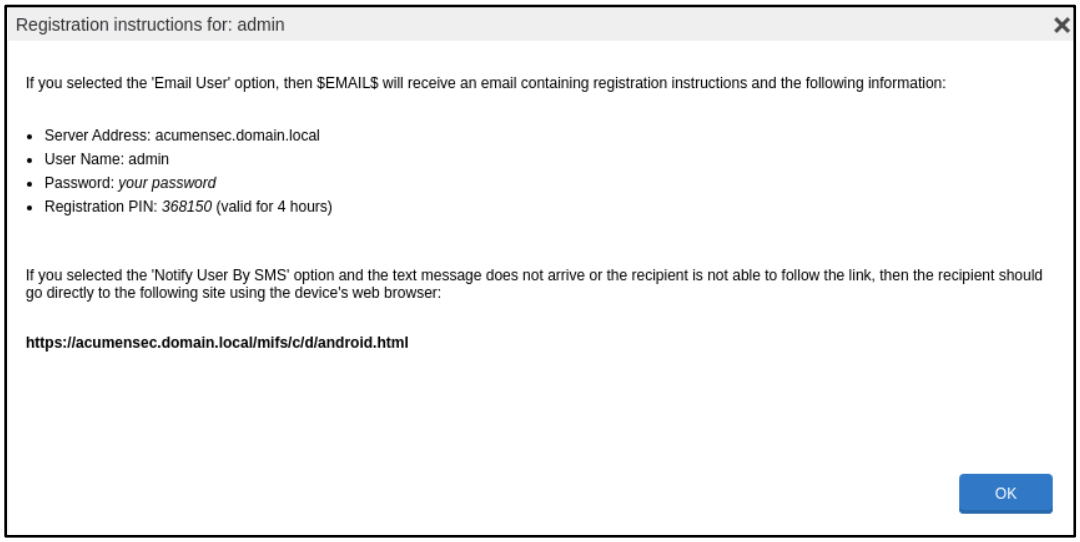


Figure 17: Device registration completed

5.3 PROHIBITING DEVICE USERS FROM UNENROLLING

The product (MDM agent) is intended for use on enterprise-owned devices designated for general enterprise purposes. Thus, the TSF enforces restrictions that prevent Mobile Device Users (MAS MD User or MD User roles) from unenrolling their devices from enterprise management. The TSF does not provide any functionality that would enable a user to initiate or complete an unenrollment process.

Furthermore, within the evaluated configuration of the EPMM System, Mobile Device Users are assigned non-administrative privileges. As a result, they cannot uninstall or remove the Ivanti MDM Agent application from the device, thereby ensuring continuous enterprise management and compliance.

6 CONFIGURING TRANSPORT LAYER SECURITY (TLS)

WARNING

The use of cryptographic mechanisms beyond those specifically evaluated and tested within the scope of this Common Criteria evaluation is not supported. Employing unsupported cryptographic mechanisms may impact the intended security behavior of the product and may render the product non-compliant with the evaluated security objectives.

6.1 CONFIGURE TLS

Procedure:

1. From the **Admin Portal**, go to **Settings** > **System Settings** > **Security** > **TLS/SSL.** The following page will be displayed.

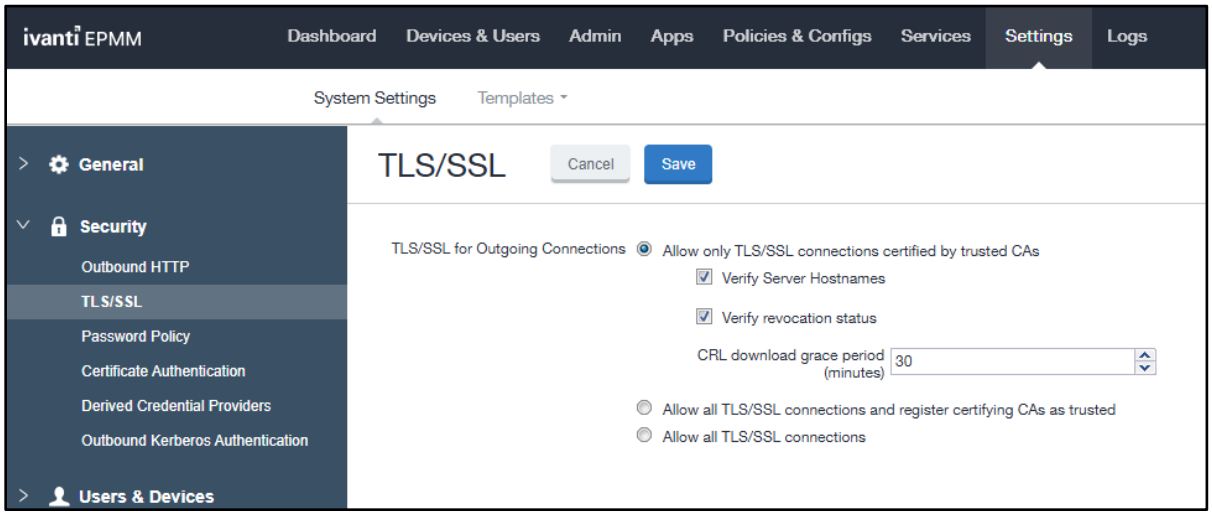


Figure 18: TLS/SSL Page

2. Select **Allow only TLS/SSL connection certified by trusted CAs.**

3. Select **Verify revocation status.**
4. Select **Save.**

6.1.1 Configuring Cipher Suites

The incoming and outgoing cipher suites must be configured to communicate with the appliance via TLS.
The product supports TLS connection (in both TLS server and TLS client capacity) using only TLSv1.2 and any connection attempt using older SSL or TLS versions is rejected.
The available cipher suites and the default list of selected cipher suites are displayed in the System Manager.

To configure the incoming cipher suites, navigate to **Security > Advanced > Incoming SSL Configuration**.

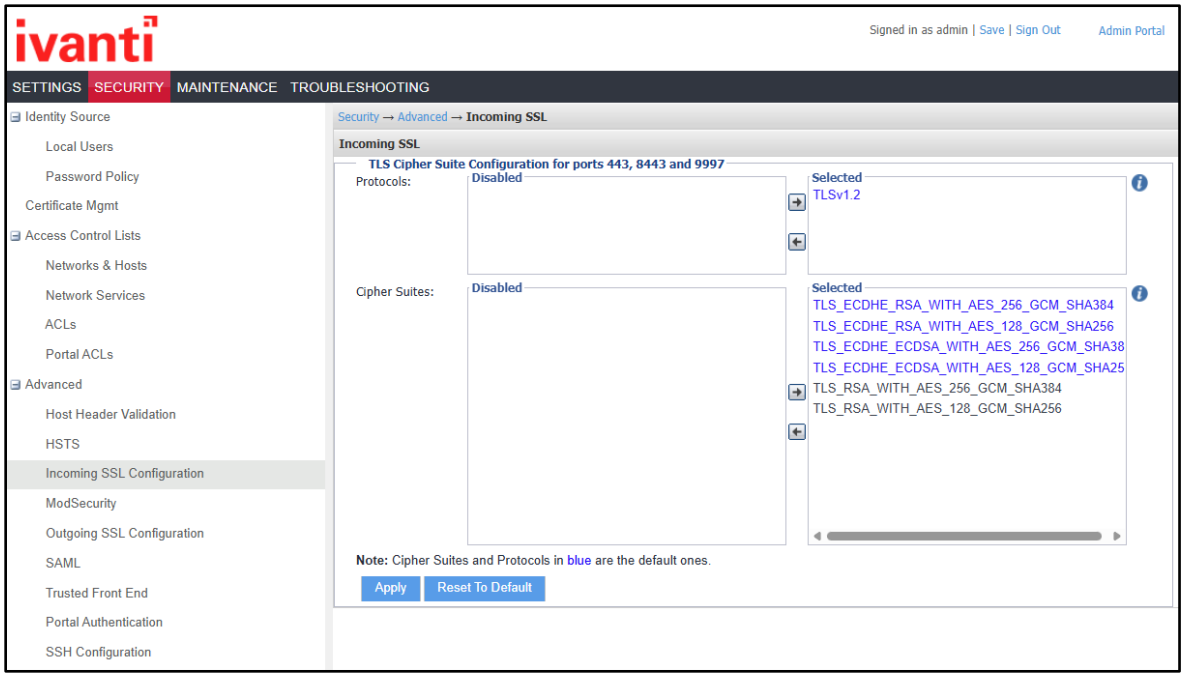


Figure 19: Inbound cipher configuration

To configure the outgoing cipher suites, navigate to **Security > Advanced > Outgoing SSL Configuration**.

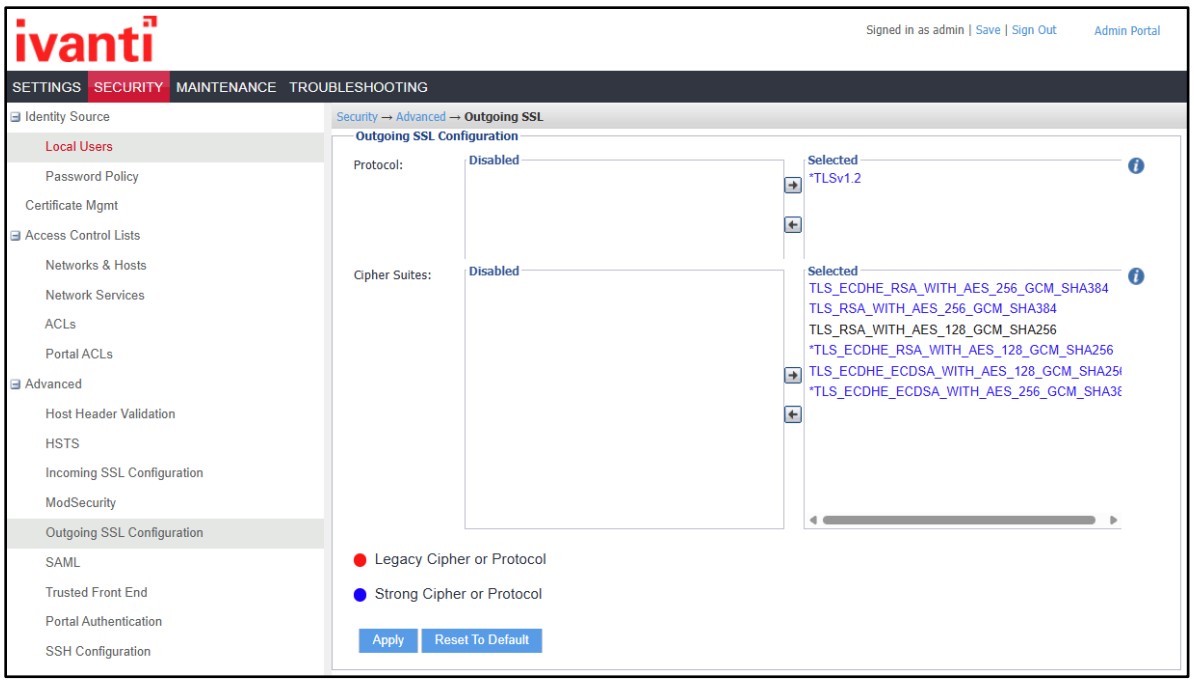


Figure 20: Outbound cipher configuration

When EPMM is in Common Criteria mode, the System Manager displays all supported incoming and outgoing cipher suites. The following cipher suites (and the RFCs in which they are defined) are the only ones allowed while operating in the evaluated configuration:

- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,

Note: The key generation parameters (such as scheme and key size) are determined by the cryptographic algorithm or cipher suite selected, and the keys are generated accordingly.

6.1.1.1 KEY AGREEMENT PARAMETERS

The key agreement parameters are dynamically generated by the product during a TLS handshake process. The NIST-recommended elliptic curves of secp256r1, secp384r1, and secp521r1 are utilized while using ECC schemes and key sizes of 2048, 3072, and 4096 bits while using RSA schemes for this process. (RSA schemes meet FIPS PUB 186-5, 'Digital Signature Standard (DSS)', Section 4. ECDSA Schemes meet FIPS PUB 186-5, 'Digital Signature Standard (DSS)', Section 5).

Note: The product does not require any additional configuration to utilize the ECDSA and RSA based key exchange algorithms, as these are implicitly applied when the respective cipher suites are selected.

The specific curve parameters are chosen to correspond with the server certificate that has been configured for client access, thereby ensuring a robust and secure key exchange. The application of these parameters is consistently observed whether the product is being used in a TLS server capacity or as a TLS client.

6.1.1.2 HASHING

The product provides cryptographic hashing services as specified in FIPS Pub 180-4. Hashing is used for the following:

- TLS communication,
- Digital signing (MDM Server) and verification (MDM Agent) of Policies,
- Digital signature verification by both TOE components as part of trusted update validation.

Hashing is performed using the following set of algorithms:

- SHA-256
- SHA-384
- SHA-512

The product uses a byte-oriented mode for hashing.
Both the MDM Server and MDM Agent components implement the hash functionality. The MDM Servers use the 'Ivanti MDM OpenSSL Component cryptography library' for all TLS paths/channels except the initial TLS connection to the Syslog Server. For that connection, 'Ivanti MDM Bouncy Castle Cryptographic library' is used. The MDM Agents use the 'Ivanti MDM Android Client OpenSSL Component cryptography library'.

Note: The hash values used while establishing TLS communication, digital signing and certificate verification cannot be configured manually on the product. The hash algorithm used during these processes is determined at the time the certificate is created and issued by a Certificate Authority (CA). This algorithm is permanently embedded within the certificate in the *signatureAlgorithm* field.

6.1.2 CONFIGURING TLS CERTIFICATES FOR EPMM SERVER

1. Login to the System Manager.
2. Selection **Security** and then **Security Management**.
3. Select **Manage Certificate.**
4. Select the certificate to be used as the TLS certificate for the EPMM Server in .p12 format.
5. Select **Upload Certificate**.
6. Once the successful upload occurs, a pop-up window appears indicating successful upload.

6.2 CONFIGURING REFERENCE IDENTIFIERS

Administrators can configure how the product's components (MDM Server and Agent) communicate with each other, and with other trusted IT systems (such as syslog). This is done using the intuitive administrative commands available within the web-based graphical user interface (GUI). The inter-component communication and communication with the external IT entity happens securely over TLS version 1.2 (HTTPS OR Syslog).

For all communications, a DNS Name must be used as the reference identifier that aligns with the standards outlined in RFC 6125 Section 6.

During certificate validation, the comparison of the Distinguished Name (DN) or Subject Alternative Name (SAN) in the received certificate against the expected identifier is a critical step. The MDM Server and MDM Agent perform this verification automatically by checking whether the DN or SAN values match the administrator-configured identifier. This identifier is typically the Fully Qualified Domain Name (FQDN) of the remote network entity. Only when the comparison succeeds is the certificate accepted as valid, ensuring that the connection is established with the intended trusted entity.

The audit server is required to comply with the standards outlined in RFC 6125 Section 6 for all communications. To communicate with the audit server, the TOE must be configured with a valid Distinguished Name (DN) or Subject Alternative Name (SAN) that matches the identifier configured on the audit server. The TOE automatically performs this matching during certificate validation. The syslog server must use the correct DNS name as its identifier, and users are expected to upload a valid certificate chain for the server.

Note: The product does not support using IP addresses as reference identifiers for any of the communications.

6.2.1 For MDM Server

To set a reference identifier for establishing communication with an external IT entity on the MDM server, using the **Admin Portal**, navigate to **Settings > Data Export > Syslog Servers**.

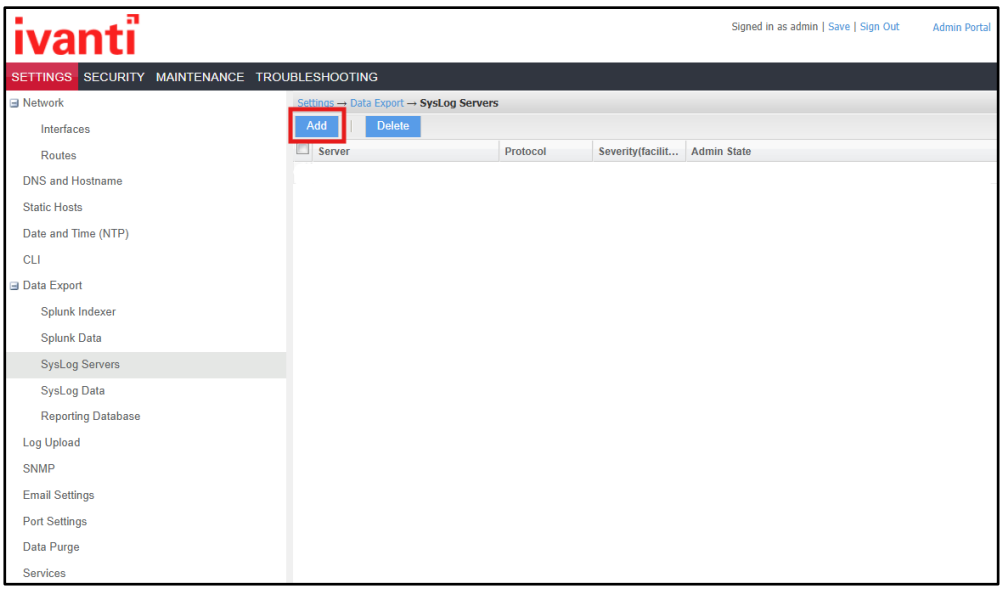
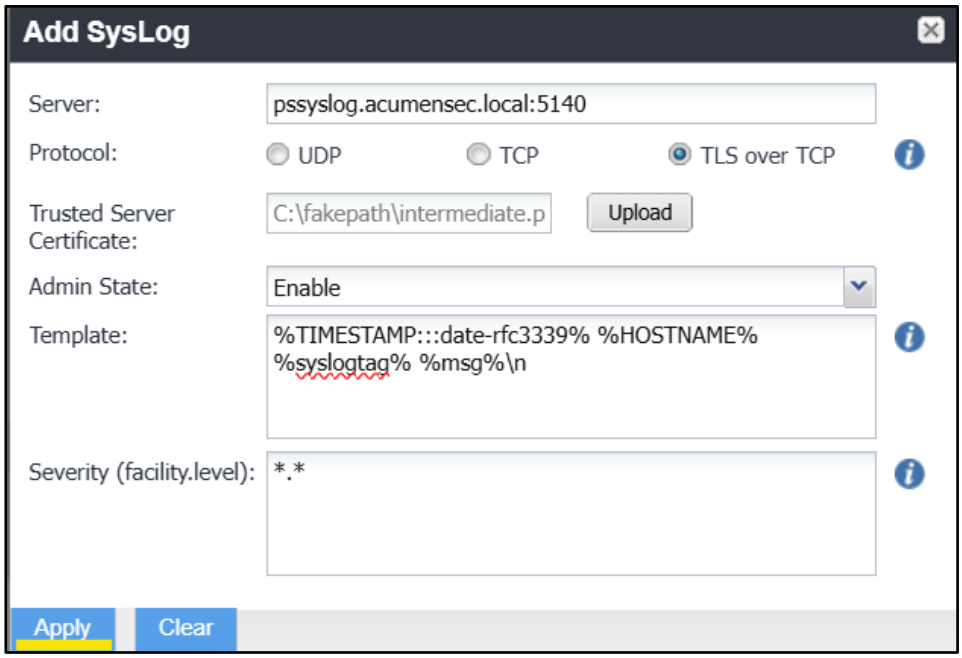


Figure 21: MDM server reference identifier configuration

To add a new syslog server, click on the **Add** utility and enter the correct reference identifier (DNS Name) in the **Server** configuration option. Other configurational parameters such as protocol, admin state, template and severity settings can also be set through here.

Make sure to upload a complete chain of valid trust certificate(s) for the syslog server in the **Trusted Server Certificate** field.



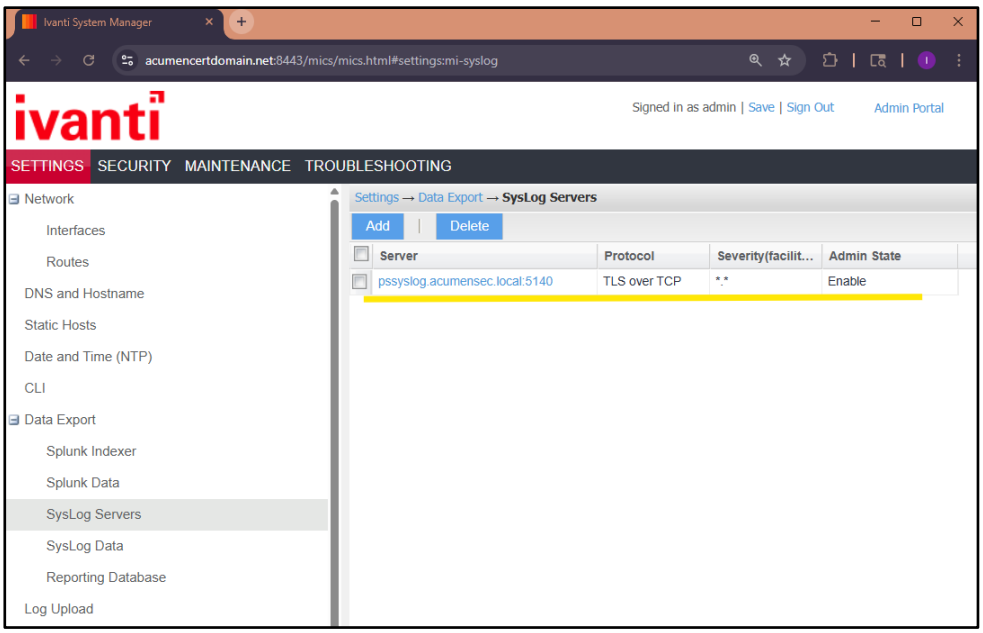


Figure 22: DNS Name

Note: Syslog events are stored on Ivanti EPMM and are copied simultaneously to the configured syslog servers. The logs remain on Ivanti EPMM until deleted as part of the default log rotation process. View the data in System Manager at **TroubleShooting > Logs > View Module Logs**.

6.2.2 For MDM Agent

The MDM Agent must first be registered on the MDM server. During the initial registration process on the MDM agent, as the mobile application prompts to enter the company email select the "**Or register with server URL**" option and enter the correct server URL. This serves as the reference identifier (DNS Name).

6.3 Mutual Authentication

6.3.1 Configuring Mutual Authentication

For mutual authentication, EPMM uses one server certificate (the Portal HTTPS certificate) to identify itself for all the agent devices and external IT entities. Identity certificates are required for Android and iOS devices, as specified by the certificate enrollment setting of the MDM server.

To enable mutual authentication via the **Admin Portal,** navigate to **Settings > System Settings > Security > Certificate Authentication**; and check the "**Enable client mutual authentication on Android client, IOS client, iOS and MacOS MDM and AppConnect communications**" option to enable mutual authentication.
Mutual Authentication is enabled by default on all new installations.

Before you enable client mutual certificate authentication, change the Apps@Work port in the

System Manager. Ivanti recommends port 7443. However, you can use any port except the 443 or 8443 which are reserved for other EPMM services.

Note: Once mutual authentication is enabled on EPMM, it cannot be disabled.

6.3.2 Mutual authentication Trust certificate

By default, the system EPMM, acts as a local Certificate Authority (CA) for generating certificates that are used in mutual authentication. However, a custom certificate can be used for which can be added by navigating to **Services > Trusted Root certificates** on the **Admin portal** (Section "Importing x509v3 certificates as trusted root certificates" covers the certificate importing in detail)

Note: Important Considerations for Custom Settings:

- Any custom certificate enrollment setting used for mutual authentication cannot be repurposed for other functions, such as VPN or Wi-Fi configurations. It's dedicated to mutual authentication only.
- If the custom certificate involves an intermediate Certificate Authority, it's crucial to ensure that all intermediate CA certificates, along with the root CA certificate, are imported and trusted within EPMM's trusted root store. This step is vital for the system to validate the certificate chain correctly.

6.4 Configuring a client identity certificate for mutual authentication

For mobile devices, the client identity certificate that the device presents to EPMM must use either ECDSA (Elliptical Curve Digital Signature Algorithm) or RSA (Rivest, Shamir, Adleman) based algorithms/ciphers (Refer section Configuring Cipher Suites for more information on the use if the ciphers) For this purpose, EPMM behaves as the Root CA that issues the client identity certificate.

6.4.1 Generating a self-signed certificate

To configure EPMM to generate the self-signed certificate:

Procedure:

1. Log into the Admin Portal.

2. Go to **Services > Local CA**.

3. Select **Add > Generate Self-Signed Cert**.

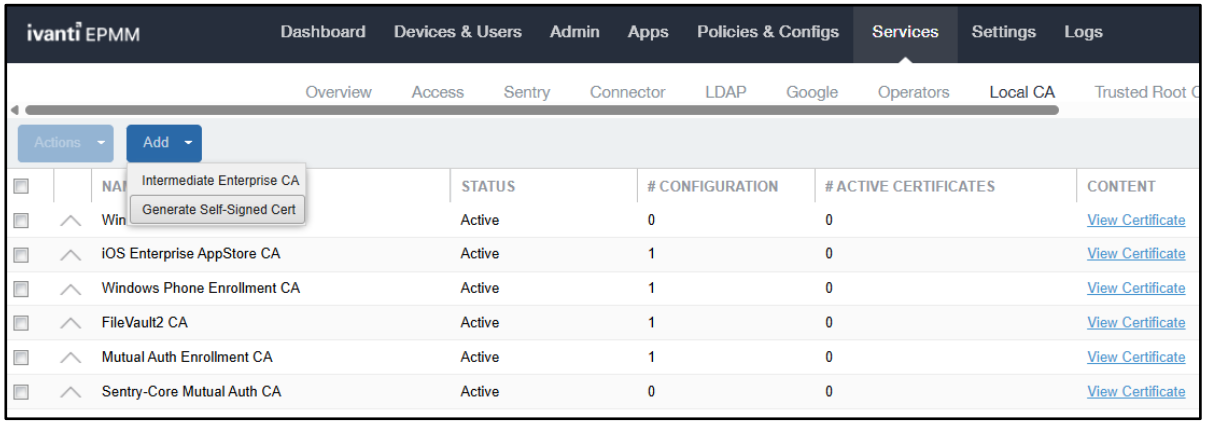


Figure 23: Creating certificate

4. Change the following fields:

   a. **Local CA Name**: Enter a recognizable name to identify the self-signed certificate. This name will appear in the list of local certificate authorities in **Services > Local CA**.

   b. **Key Type**: Specify the key type. The options are RSA (default) or Elliptical Curve.

   c. **Key Length**: Specify the key length. The values are P-256, P-384 or P-521.

   d. **CSR Signature Algorithm**: The values are SHA256, SHA384 (the default), and SHA512.

      a. **Issuer Name**: Requires an X.509 name. For example, CN=www.yourcompany.com,

5. Click **Generate**. The **Certificate Template** window displays.

6. Click **Save**.

6.4.2 Configuring an Intermediate CA

Organizations can configure EPMM to function as an Intermediate Certificate Authority (CA). By establishing EPMM as an Intermediate CA, organizations empower their mobile device users to securely authenticate not only with the EPMM system but also with other servers and resources across the company's intranet. To enable this functionality, administrators must first acquire the necessary certificate (CA trust certificate) from their existing certificate vendor and subsequently import it into EPMM.

Procedure:

1. Using the EPMM **Admin Portal**, navigate to **Services** > **Local CA**.
2. Click **Add** > **Intermediate Enterprise CA**.
3. Click **Browse** and navigate to the combined file.
4. Click **Open**.
5. Enter a name you can recognize in the **Local CA Name** field.
6. Click **Upload Certificate**. Your local certificate authority is now available to use. The local CA will be listed in **Services** > **Local**.

6.4.3 Certificate enrollment for Local CA

Once a self-signed certificate has been generated, create a local CA certificate enrollment setting for the self-signed certificate.

Procedure:

1. Log into the Admin Portal.
2. Go to **Policies & Configs** > **Configurations.**
3. Click **Add New** > **Certificate Enrollment** > **Local**.
4. For **Name**, enter brief text that identifies this certificate enrollment setting.
5. For **Local CAs**, select the certificate you created in Generating a self-signed certificate.
6. For **Subject**, enter **CN=<*value*>**
7. Click **OK**.
8. Click **Save**.

6.4.4 Certificate enrollment for Client Identity Certificate

Once the certificate enrollment setting for the local CA is created, configure EPMM to provide the client identity certificates for mutual authentication.

Procedure:

1. In the Admin Portal, go to **Settings** > **System Setting** > **Security** > **Certificate Authentication**.

2. For Certificate Enrollment Setting, select the certificate enrollment setting you created in Certificate enrollment for Local CA.

3. Click **Save**.

6.5 IMPORTING X509V3 CERTIFICATES AS TRUSTED ROOT CERTIFICATES

Additional x509v3 trust certificates (Root CA and ICA certificates) can be imported on the EPMM server's trust store.

Procedure:

1. Using the **Admin Portal**, navigate to **Services > Trusted Root Certificates**.

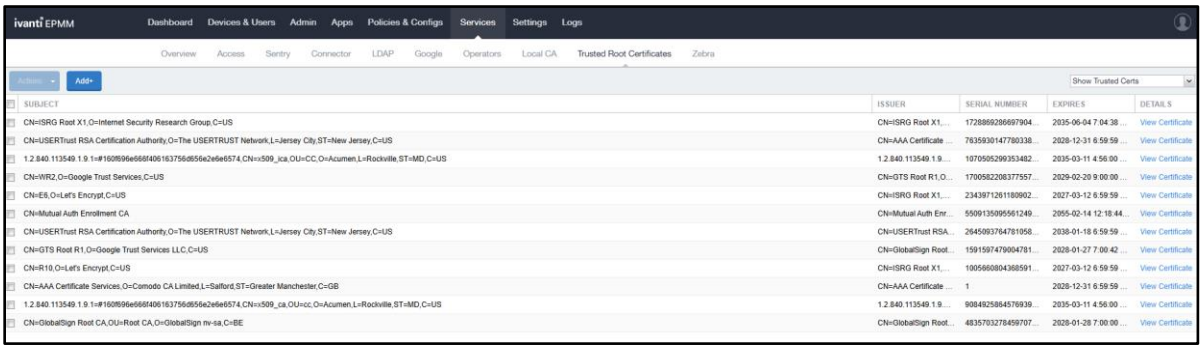


Figure 24: Importing X509 certificates

2. Click **Add** to open the **Upload Trust Root Certificate** dialog.

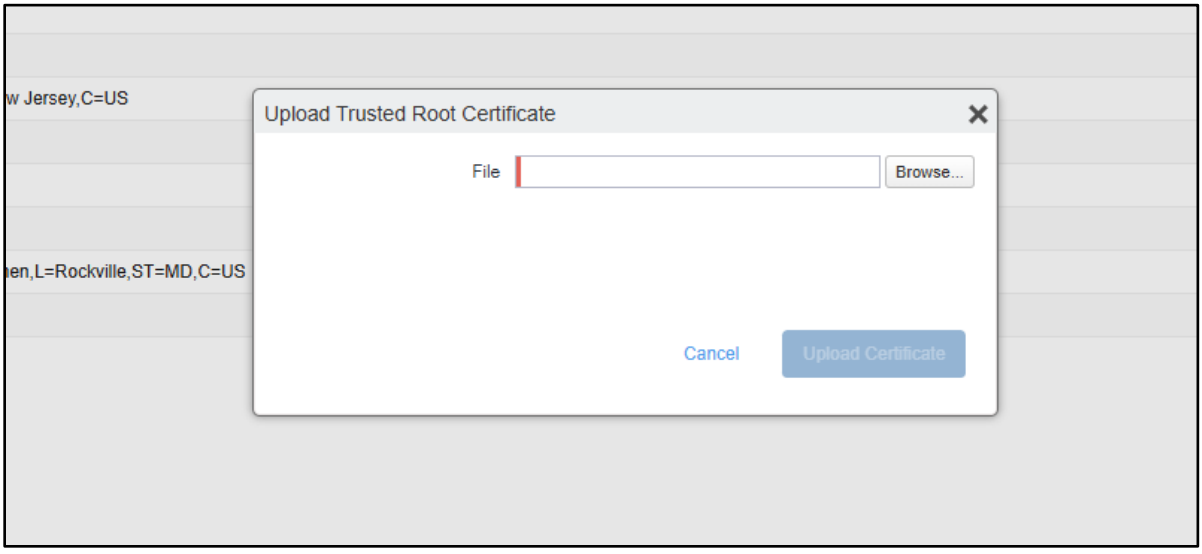


Figure 25: Uploading certificate file

3. Add the certificate to the **File** box using the **Browse** button.

4. Click **Upload Certificate**.

5. Click **OK**.

The CA certificate should be now on the list of trusted root certificates.

6.5.1 Deleting a Trusted Certificate

Procedure:

1. From the **Admin Portal**, go to **Services > Trusted Root Certificates**.
2. Click the drop-down box to the right, and select one of the following options:
3. Select one or more certificates.
4. Select **Actions > Delete**.
5. Click **Yes** in the confirmation box.

> The server must be rebooted to complete the process if deleting the selected trusted certificate

6.6 Configure the HTTPS Administrator HTTPS Port Settings

To change the port settings:

Procedure:

1. Using the **Ivanti EPMM System Manager**, navigate to **Settings > Port Settings**.

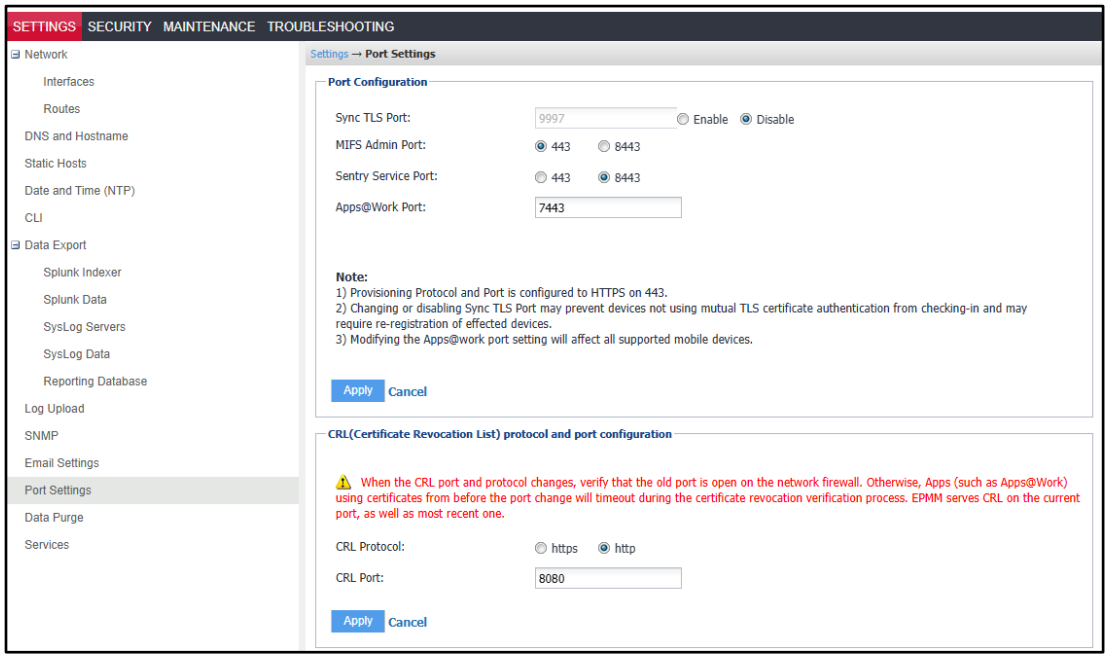


Figure 26: HTTPS Settings

2. Set **Sync Service Port** to **Disable**.

3. Set **Provision Protocol** to **https**.
   All remote administration access to the Admin Portal and the System Manager must be performed through a HTTPS/TLS protected connection. Do not allow non-secure protocols such as HTTP.

4. Click **Apply.**

7 EPMM Server Management

7.1 Overview

This section describes the EPMM Server management commands and configuration methods.

7.2 FMT_SMF SFR Management Commands

This section describes how to perform the management functions required for the Common Criteria evaluation. Specifically,

- FMT_SMF.1(1) *Specification of Management Functions (Server configuration of Agent) (MDM_PP)*
- FMT_SMF.1(2) *Specification of Management Functions (Server Configuration of Server) (MDM_PP)*
- FMT_SMF.1(3) *Specification of Management Functions (MAS Server) (MDM_PP)*
- FMT_SMF_EXT.4 *Specification of management Functions (AGT_PPM)*

7.2.1 Transition to the Locked State

Prerequisites:

The Product(s) must be configured in the Common Criteria evaluated configuration.

Procedure:

1. Using the **Admin Portal**, navigate to **Devices & Users > Devices.**
2. Find the row displaying the device that needs to be transitioned into a locked state and select it using its corresponding checkbox.

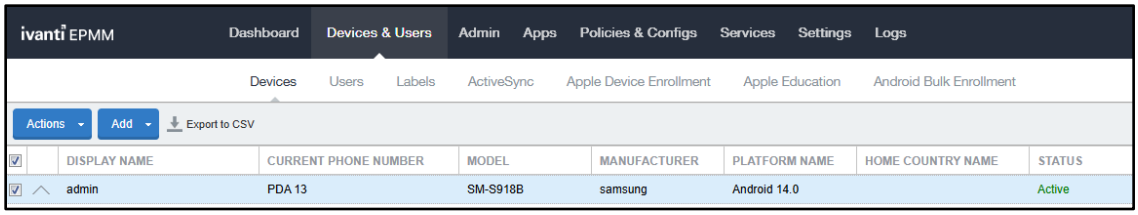


Figure 27: Selecting device

3. Once the device is selected, click on the **Actions** option. The Actions drop-down menu will be displayed.

4. Select the **Lock** option from the dropdown menu. The Lock pop-up window will appear.



Figure 28: Lock pop-up window

Note: The top window will be populated with the User and Phone displayed on the Device & Users page. (In the example shown in **Figure 28: Lock pop-up window**, the two fields are admin and PDA 13.)

5. Select the **Lock** option in the lower right of the Lock pop-up window.

   The device would be transitioned into a locked state.

7.2.2 Full Wipe of Protected Data

Prerequisites

- The Product(s) must be configured in the Common Criteria evaluated configuration.
- The Notification must be configured during device enrollment.

Procedure

1. Using the **Admin Portal**, navigate to **Devices & Users > Devices**.
2. Find the row displaying the device that needs a full wipe out of data and select it using its corresponding checkbox:
3. Once the device is selected, click on the **Actions** option. The Actions drop-down menu will be displayed.
4. Select the **Wipe** option from the dropdown menu. Wipe Warning pop-up window will appear.

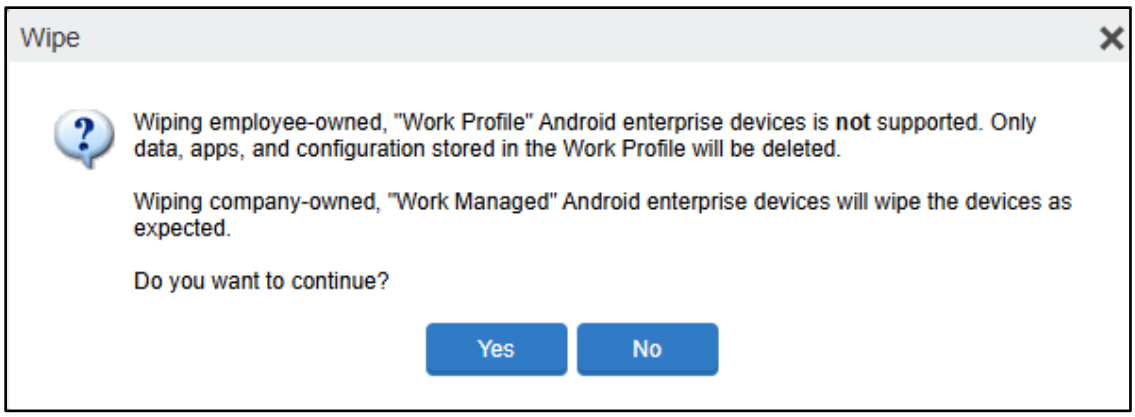


Figure 29: Wipe warning

8. Select **Yes**. The Wipe pop-up window will appear.

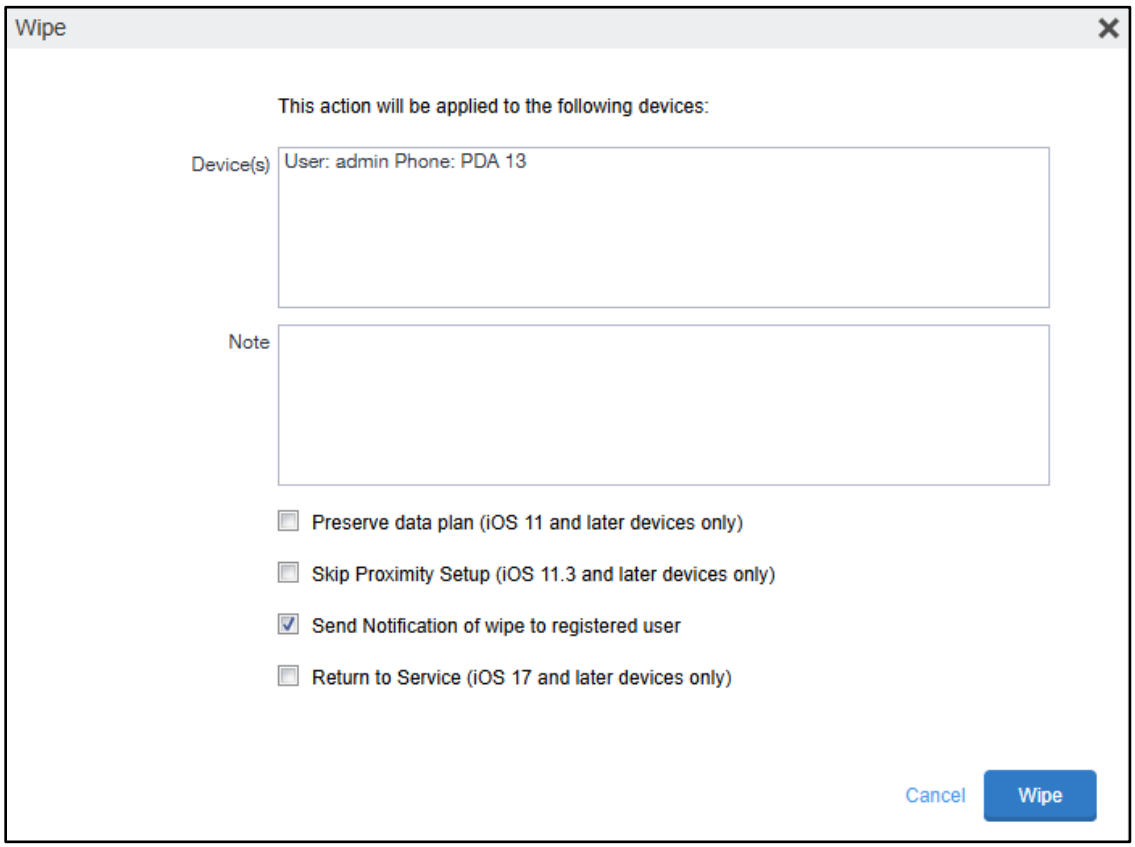


Figure 30: Wipe Pop-up Window

Note: The top window will be populated with the User and Phone displayed on the Device & Users page. (In the example shown in **Figure** *29*, the two fields are admin and PDA 13.)

9. Select the **Send Notification of wipe to registered user** option.
10. Select the **Wipe** option in the lower right of the Wipe pop-up window.

Note: Once the device is unenrolled/wiped from the MDM Server, any communication from the MDM Server to the MDM Agent is disabled and visa versa.

7.2.3 Unenroll From Management

Mobile Device (MDM agents) can be unenrolled from the EPMM System by the system administrators using the EPMM server (Admin portal). For unenrolling a mobile device, a **wipe** must be issued with respect to the device. For detailed instructions view section Full Wipe of Protected Data.

Note: The EPMM system does not allow a Mobile Device User (MAS MD User or MD User role) to unenroll from the enterprise. No functionality to unenroll is present on the MDM agent.

7.2.4 Install Policies

The EPMM Server supports configuring multiple policies.

Default policies are the policies applied to a device (MDM agent) automatically when it is registered. Default policy values are also used as a starting point when you create a custom policy.
Ivanti EPMM provides the values for each default policy specification. When building customized policies, the default policies can be used as a starting point. Unlike configurations, a device can have only one policy of each type. The default settings for each policy type are listed in the section for each type.

Note: The certificate used for policy signing is the same as the one used for TLS communications. During the initial handshake, the MDM agent validates the certificate for TLS. The same TLS certificate is used subsequently while pushing policies.

Refer to Section 6.1.2 Configuring TLS Certificates for EPMM Server for guidance about uploading the certificate.

7.2.4.1 Building on default policy

For customizing one of the default policies use the following procedure:

Procedure:

7. From the **Admin Portal**, navigate to **Policies & Configs > Policies**.
8. The policies will be displayed. Find the row for the currently installed Secure Policy or the Default Security Policy.

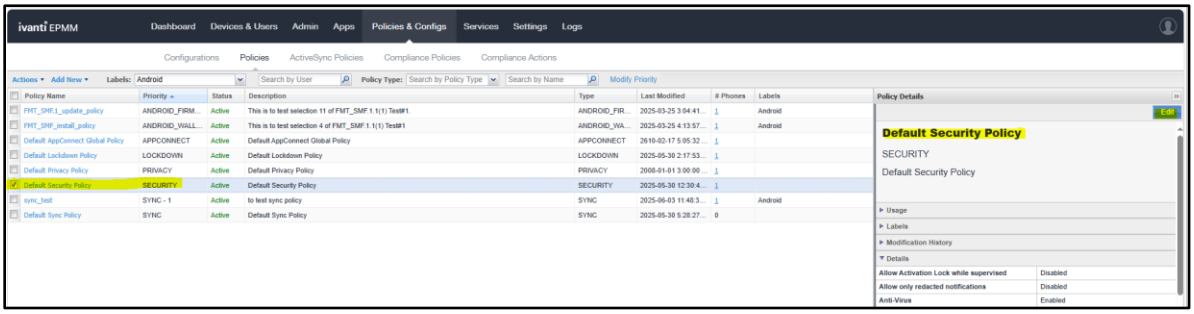


Figure 31: Default policy

9. Select the security policy you want to modify.
10. Select the **Edit** button in the upper right corner of the pop-up window. The details of the policy will be displayed.
11. Edit the values and fields as desired for creating the policy.
12. Select **Save**.
13. Select **OK**
14. Confirm that the security policy is applied to a label that is also applied to the target devices.
    a. Select the security policy.
    b. Click **Actions > Apply To Label**.
    c. If necessary, select the appropriate labels and click **Apply**

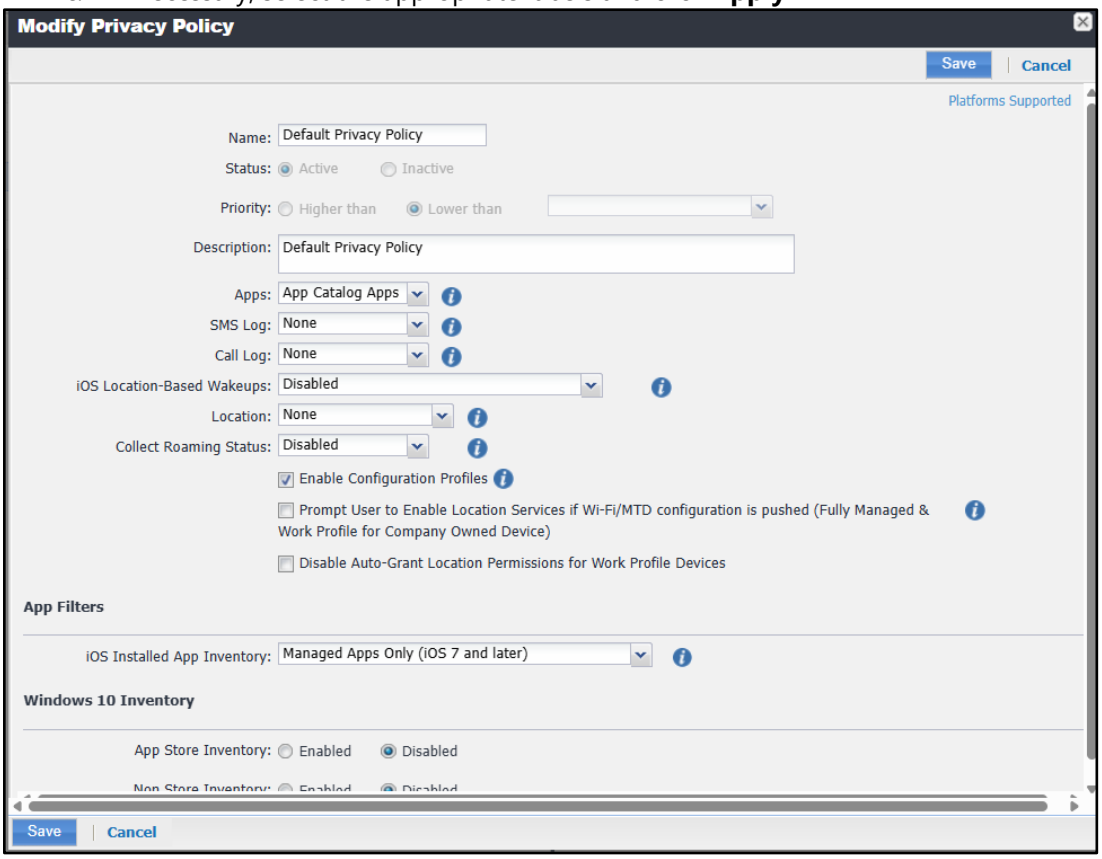


Figure 32: Configuring policy

7.2.4.2 CONFIGURING NEW ANDROID POLICY

For creating a new policy for android devices use the following procedure:
Procedure:

1. From the **Admin Portal**, navigate to **Policies & Configs > Policies**.

2. The configured/default policies will be displayed. Select **Add New > Android**. Once here, select the policy that needs to be configured on the android device.

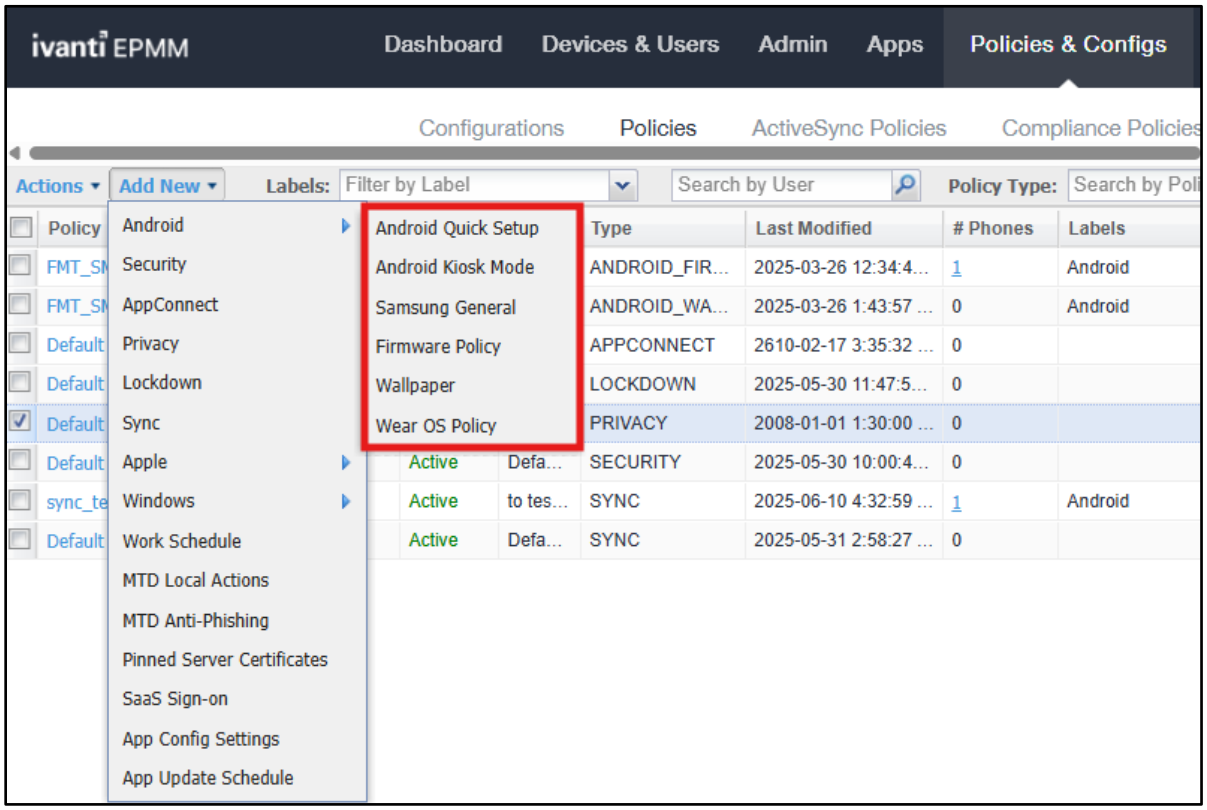


Figure 33: Android policies

7.2.4.2.1 Android Quick Setup Policy

The Android Quick Setup policy offers additional options for getting devices configured quickly:

Procedure:

1. Go to **Policies & Configs > Policies**.
2. Click **Add New > Android > Android Quick Setup**.
3. Use the following guidelines to complete the form:

Action	Example
Name	Required. Enter a descriptive name for this policy. This is the text that will be displayed to identify this policy throughout the Admin Portal. This name must be unique within this policy type. Note: Though using the same name for different policy types is allowed (e.g., Executive), consider keeping the names unique to ensure clearer log entries.
Status	Select Active to turn on this policy. Select Inactive to turn off this policy.

	Why: Use the Status feature to turn a policy on or off across all phones affected by it. The policy definition is preserved in case you want to turn it on again.
Priority	Specifies the priority of this custom policy relative to the other custom policies of the same type. This priority determines which policy is applied if more than one policy is associated with a specific device. Select “Higher than” or “Lower than”, then select an existing policy from the drop-down list. For example, to give "Policy A" a higher priority than Policy B, you would select “Higher than” and “Policy B”. Because this priority applies only to custom policies, this field is not enabled when you create the first custom policy of a given type.
Description	Enter an explanation of the purpose of this policy.
Policy Parameters	Clear the Device Administrator option to complete registration without applying the Device Administrator role to the Ivanti Mobile@Work app. Clearing this option streamlines the registration process by eliminating the need for the device user to approve granting the Device Administrator role. Clearing the option also disables the following features on the device: • Password requirements • Device encryption • Device lock/unlock • Wipe • Camera lock • Lockdown policies • Samsung Knox features • Samsung native email configuration • Samsung Knox container • Kiosk mode
User registration password for	Select the Exchange and/or Wi-Fi check box to cache the registration password on the device for use in configuring the Exchange and/or Wi-Fi settings. Selecting these options streamlines the configuration process if you are using LDAP for authentication as part of the registration and Exchange/Wi-Fi configuration processes. Note that the password is cached in memory only. Terminating the app drops the password from memory.

4. Click **Save**.

5. Apply the policy to the appropriate labels (**Actions > Apply to Labels**).

7.2.4.2.2 Android Kiosk Mode Policy

This policy is dedicated pertaining to a staging user. This policy is not active until a label is applied to the staging policy.

Procedure:

1. Using the **Admin Portal**, go to Policies & Configs > Policies.
2. Click **Add New > Android > Android Kiosk Mode**.
3. In the New Android Kiosk App Setting Policy dialog box, enter a **Name** and **Description** for the policy.
4. Select **Active** for the **Status** field to enable this policy.
5. Scroll down to the lower part of the Kiosk Settings section:
    a. **Disable Quick Settings** - Select so that the device will not display the system notification dropdown menu at the top of the screen. If you enable the following options, the settings are displayed as menu items in the shared-kiosk mode on the device.
    b. **Allow User to Access WIFI Settings**. This is an optional setting.
    c. **Allow User to Access Bluetooth Settings**. This is an optional setting.
    d. **Allow User to Access Location Settings**. This is an optional setting.
    e. Enter a 4 - 6 digit PIN in the **Kiosk Exit PIN** field.
    A pin to the staging user kiosk policy can be assigned. However, it is not mandatory. Without a kiosk exit pin, the staging user cannot exit the kiosk mode.
    f. Select the **Enable Shared Device** check box. This is a mandatory setting.
        i. **Enable Login (Only for Staging user)** - This option does not apply to shared-kiosk mode. Select **Display Recent Users on Login Screen** to track the users logging into the kiosk mode. If the option is not selected, the recent users will not be displayed for the client.
        ii. **Enable Logout** - Select to use and then set the number of hours in the **Logout user is session exceeds (0) hours** drop-down.
6. Scroll up to the Kiosk Branding section, customize the kiosk with a background color and background image if desired.
7. Click **Save**.

7.2.4.2.3 Samsung general policy

Use the Samsung general policy to manage Samsung Knox license keys on Samsung devices.

Procedure:

1. Go to **Policies & Configs > Policies**.
2. Select **Add New > Android > Samsung General**.
3. Use the following guidelines to complete this form:

Item	Description

Name	Enter a unique name for the policy
Status	Select Active to turn on this policy. Select Inactive to turn off this policy
Priority	Select Higher than or Lower than, then select an existing policy from the drop-down list. If you have multiple policies, use the Priority setting to select which policy gets applied. See "Prioritizing policies" in Getting Started with Ivanti EPMM.
Description	Enter a description for the policy
Activate License key	Select Enable to activate Knox features.
KNOX License key	Enter the Samsung Knox license key
KNOX Device Attestation Enabled	To enable attestation, first select the "I understand" check box, then select Knox Device Attestation Enabled.
Audit Collection Controls	Select Enable to enable event logging to the device logs on Samsung Knox devices.

4. Select **Save**.

7.2.4.2.4 Firmware policy

Administrators can limit device users from managing system updates on Android 6.0 devices (or later releases that are supported by Ivanti, Inc).

Prerequisites:

- Activate your Samsung license.
- Verify that effected devices are running Samsung Knox version 2.7.1 and above.

Procedure:

1. Log into the Admin Portal.
2. Go to **Policies & Configs > Policies**.
3. Click **Add New > Android > Firmware policy**.
4. Enter a unique name for the policy in the **Name** field.
5. Select a **Status**.
    a. **Active**: to turn on this policy.
    b. **Inactive**: to turn off this policy.
6. Select **Priority** then select **Higher than** or **Lower than** to select an existing policy from the dropdown list.

7. This option is only available if there is more than one priority.
8. Enter a **Description** (optional).
9. Select the **System Update Policy for Android 6.0 or higher** check box and enable the following options:
    a. **Automatic**: silently apply the policy whenever new firmware is available.
    b. **Update Window**: schedule a time period to silently apply the new firmware.
    c. Select a start and end time to schedule the firmware update.
    d. **Postpone**: this is hard-coded by the OS and skips any OS updates for up to 30 days after which it becomes automatic.
10. (Optional) In the **Freeze Period** section, click **+Add Freeze Date**. The Start Date and End Date fields display. The Freeze Period cannot be more than 90 days and the next Freeze Period can be selected only after 60 days from the previous calendar end date.
11. Click **Save**.
12. Select the policy then select **Actions > Apply to Label**.
13. Select one or more labels.
14. Click **Apply**.

7.2.4.2.5 Wallpaper Policy

The device wallpaper configuration defines a default wallpaper image for the Home screen and Lock screen of Android (10.0 devices in Work Managed Device mode).

Note: The uploaded image must be in .jpg or .png format.

The wallpaper will be applied automatically to the device. Refer to the device manufacturer's specifications for screen resolution. Ivanti recommends to create separate configurations with appropriate screen size and resolution of the device type.

Procedure:

1. Using the Admin Portal, navigate to **Polices & Configurations > Policies**.
2. Click **Add New > Android > Wallpaper**.
3. Use the following guidelines to complete the form:

Item	Description
Name	Required. Enter a descriptive name for this policy.
Description	Enter an explanation of the purpose of this policy.
Upload Android wallpaper	
Use the same image for Home screen and Lock	Select to upload a single image for both the screens.

Screen	
Home Screen	Drag and drop the image file or click Choose File to select it.
Lock Screen	Drag and drop the image file or click Choose File to select it.

4. Click **Done**.

7.2.4.2.6 Wear OS policy

The Wear OS policy is used to send various Wear OS details to the server. If there isn't a policy in place or the watch app is not installed, then the Wear OS tab will not be displayed. If there is a policy and there are no watches paired to Ivanti Mobile@Work , the Wear OS tab does not display. If there is a policy and the watch is paired (via Bluetooth) to the phone but the watch app is not installed on the watch, then Wear OS tab will not display. Once the policy has been implemented, the device continues to report watch details and inventory even when the device is quarantined.

Procedure:

1. Select **Policies & Configs** > **Policies**.
2. Select **Add New** > **Android** > **Wear OS policy**.
3. In the Add Wear OS Policy dialog box dialog box, use the guidelines to complete this form.
4. Select **Save**.
5. Apply the policy to a label using the following:

Item	Description
Name	Enter a name for the Wear OS policy.
Status	Select the relevant radio button to indicate whether the policy is **Active** or **Inactive**. If multiple policies are active with different policy labels to, only the policy with the highest-priority is assigned to any given device.
Priority	Specifies the priority of this policy relative to the other custom policies of the same type. This priority determines which policy is applied if more than one policy is available. Select Higher than or Lower than, then select an existing policy from the dropdown list. For example, to give Policy A higher priority than Policy B, you would select “Higher than” and “Policy B”
Description	Enter an explanation of the purpose of this policy
Collect Wear OS device	• Enables (default) the collection of the device's Wear OS details to the server.

details	• De-select to turn off the collection of Wear OS device details, including app inventory Note: If the "Collect Wear OS device details" and "Collect Wear OS application inventory" fields are both selected, the collection of both device inventory and app inventory will occur.
Collect Wear OS application inventory	• Select to enable the collection of Wear OS application inventory. • De-select (default) to turn off the collection of Wear OS application inventory. Once this field is de-selected, old application inventory data will display in the Wear OS tab until the client explicitly sends a report to Ivanti EPMM with no application inventory details or updated inventory details. Note: De-selecting this field will also de-select the "Collect Wear OS device details" field.

7.2.5 Query Connectivity Status

Prerequisites:

The Product(s) must be configured in the Common Criteria evaluated configuration.

Procedure:

1. Using the **Admin Portal**, navigate to **Devices & Users > Devices.**
2. Find the row displaying the device of which the status needed to be queried and click on the up arrow to the left of the display name for the device.

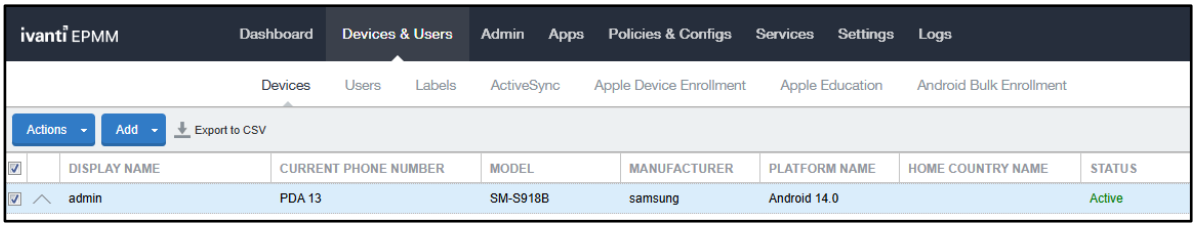


Figure 34: Select Device

Note: The **STATUS** column reports the status as active.

3. The status can be additionally verified by double clicking on the **DISPLAY NAME** entry. The device detail window will appear.

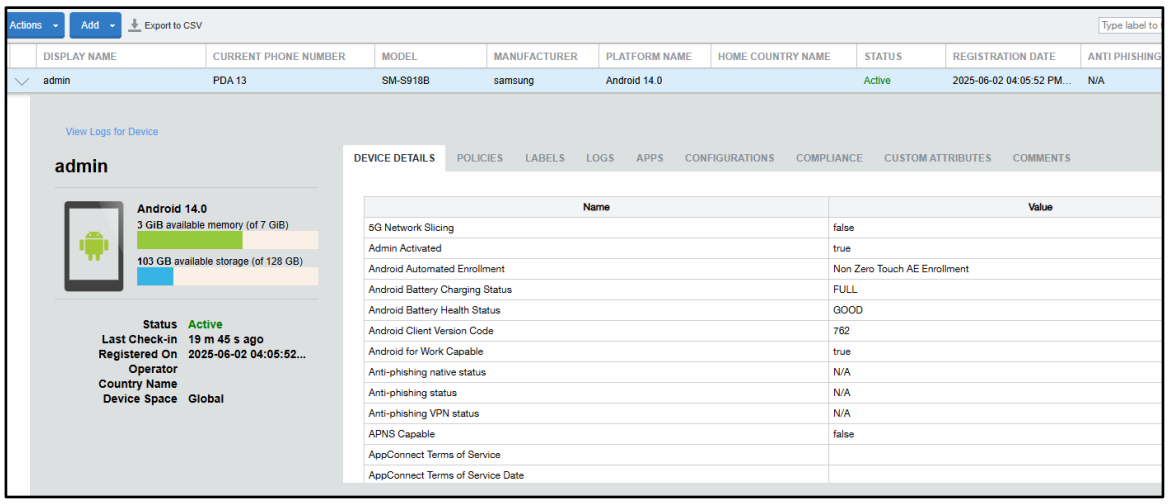


Figure 35: Device detail window

Note: The window includes device Status as well as Last Check-in date.

7.2.6 Query Current Version of the Mobile Device Firmware/Software

Prerequisites:

The Product(s) must be configured in the Common Criteria evaluated configuration.

Procedure:

1. Using the **Admin Portal**, navigate to **Devices & Users > Devices.**
2. Find the row displaying the device of which the status needed to be queried and click on the up arrow to the left of the display name for the device.

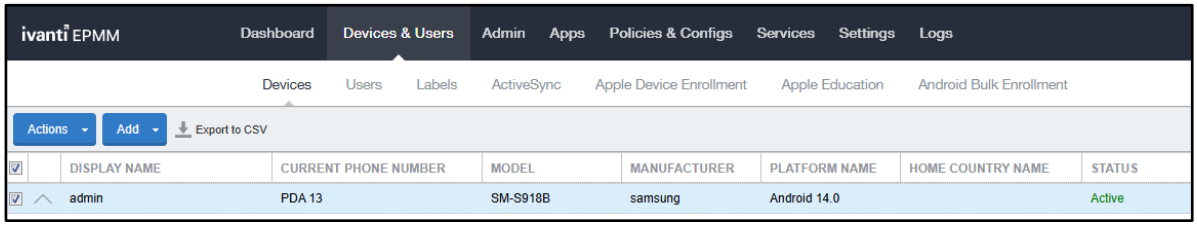


Figure 36: Finding device

3. The version can be verified by double clicking on the **DISPLAY NAME** entry. The device detail window will appear.
4. The **Device Details** panel displays more information about the mobile device. Scroll down until you view the **OS Version** entry.

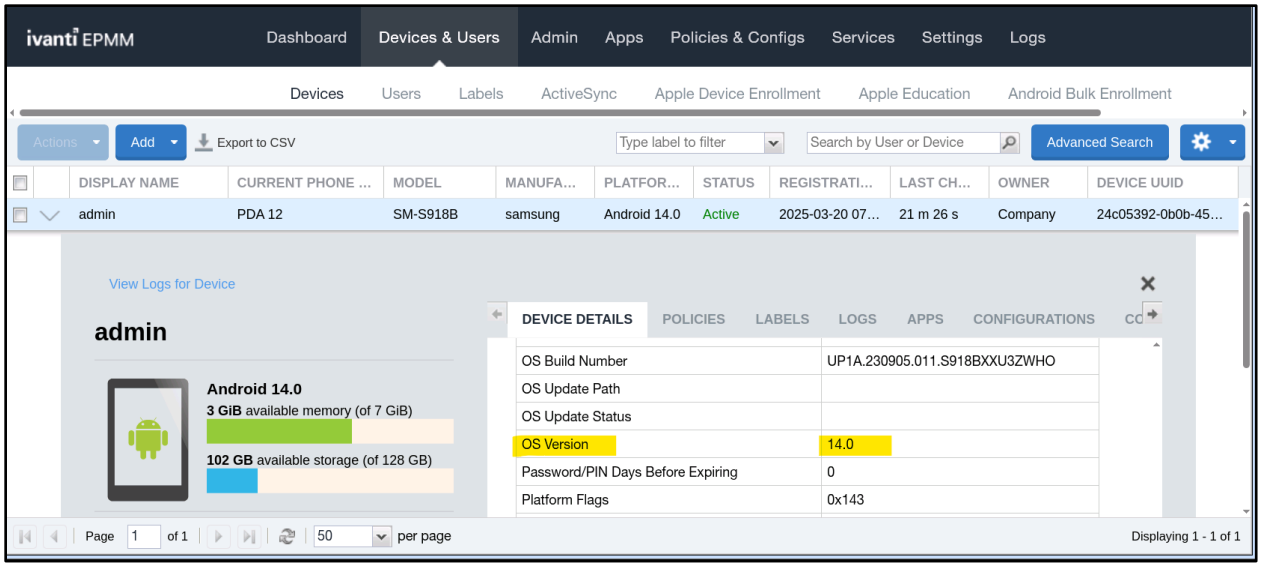


Figure 37: MD firmware version

Note: The above example screenshot shows OS version as 14.0.

7.2.7 Query Current Version of the Mobile Device Hardware

Prerequisites:

The Product(s) must be configured in the Common Criteria evaluated configuration.

Procedure:

1. Using the **Admin Portal**, navigate to **Devices & Users > Devices.**
2. Find the row displaying the device of which the status needed to be queried and click on the up arrow to the left of the display name for the device.

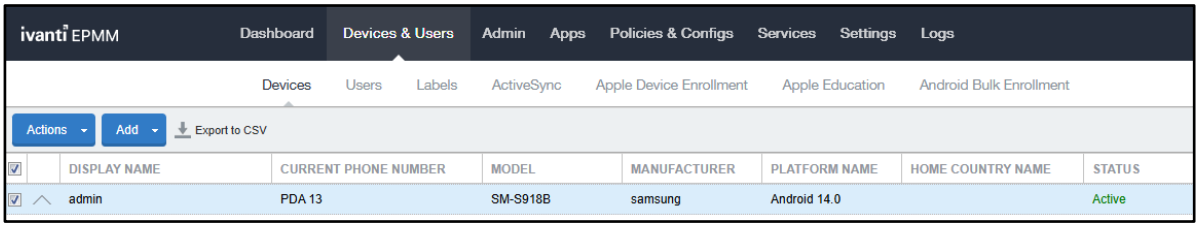


Figure 38: Finding device model

Note: The **MODEL** column reports the hardware model of the device.

3. The hardware model can be additionally verified by double clicking on the **DISPLAY NAME** entry. The device detail window will appear.

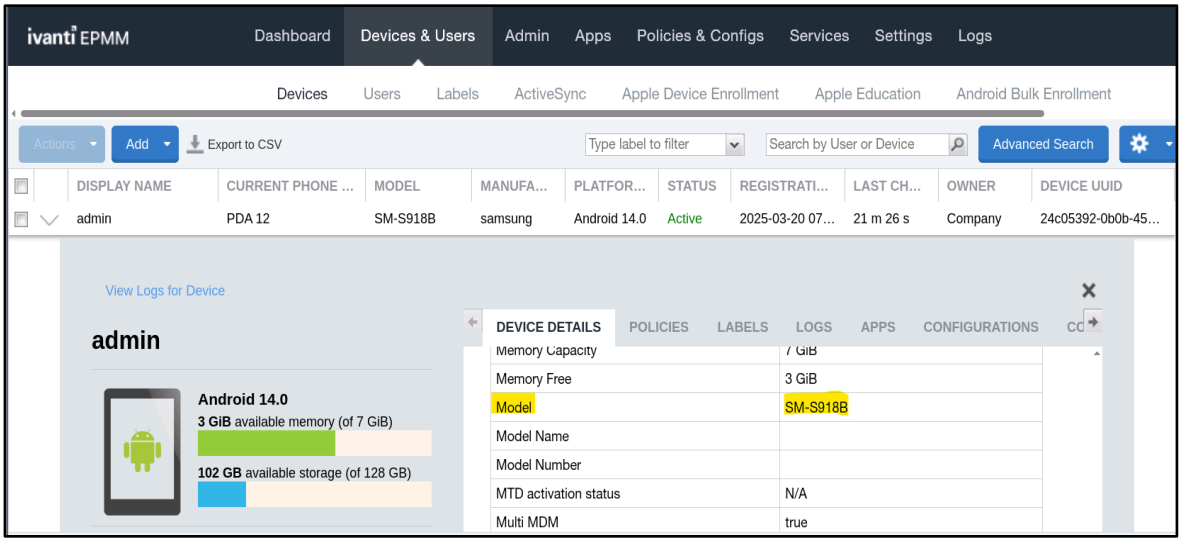


Figure 39: Hardware model query

Note: The above example screenshot shows Model SM-S918B (**MODEL** row).

7.2.1 Query Current Version of the MDM Agent Software

Prerequisites:
The Product(s) must be configured in the Common Criteria evaluated configuration.

Procedure:

1. From the Android device go to the Mobile@Work Home page.

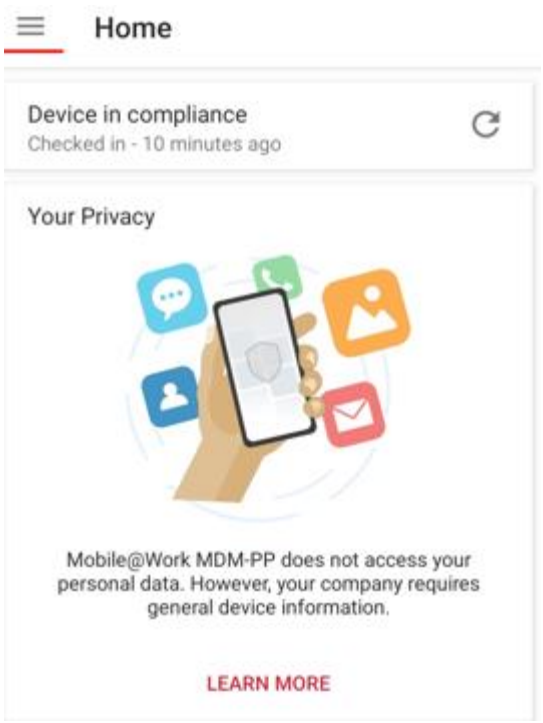


Figure 40: MDM Agent Home Page

2. Select the pull down menu from the upper left.

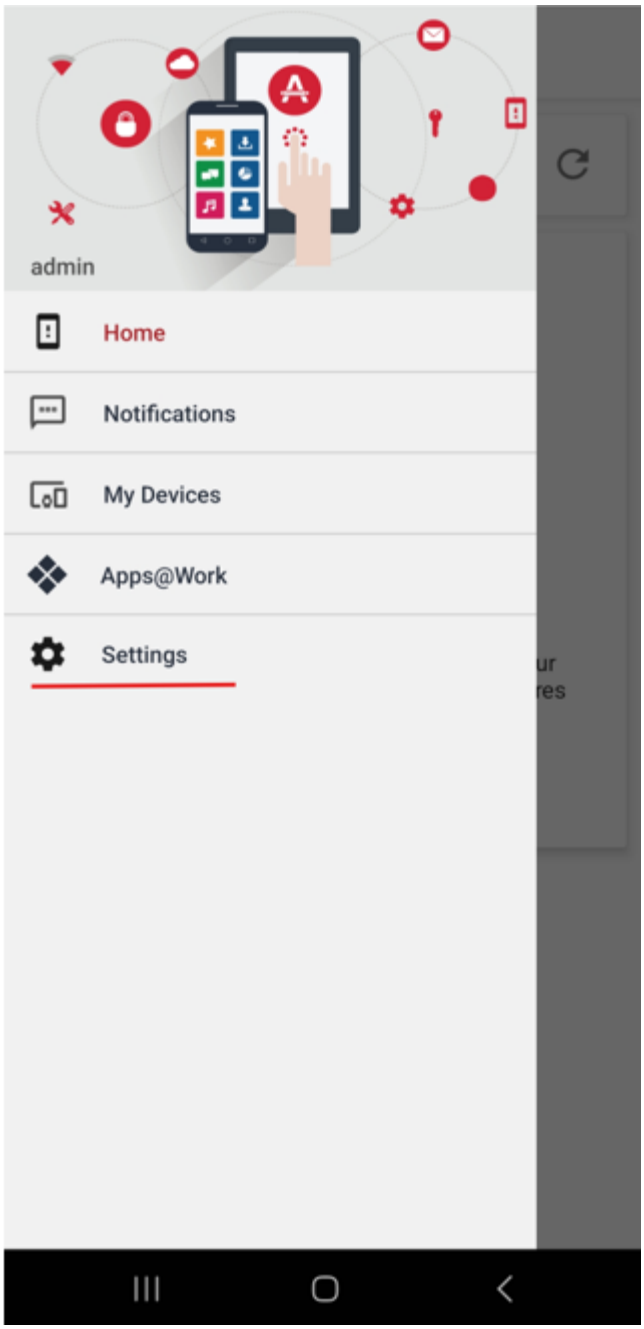


Figure 41: Android Home Pull Down Menu

3. Select **Settings**.

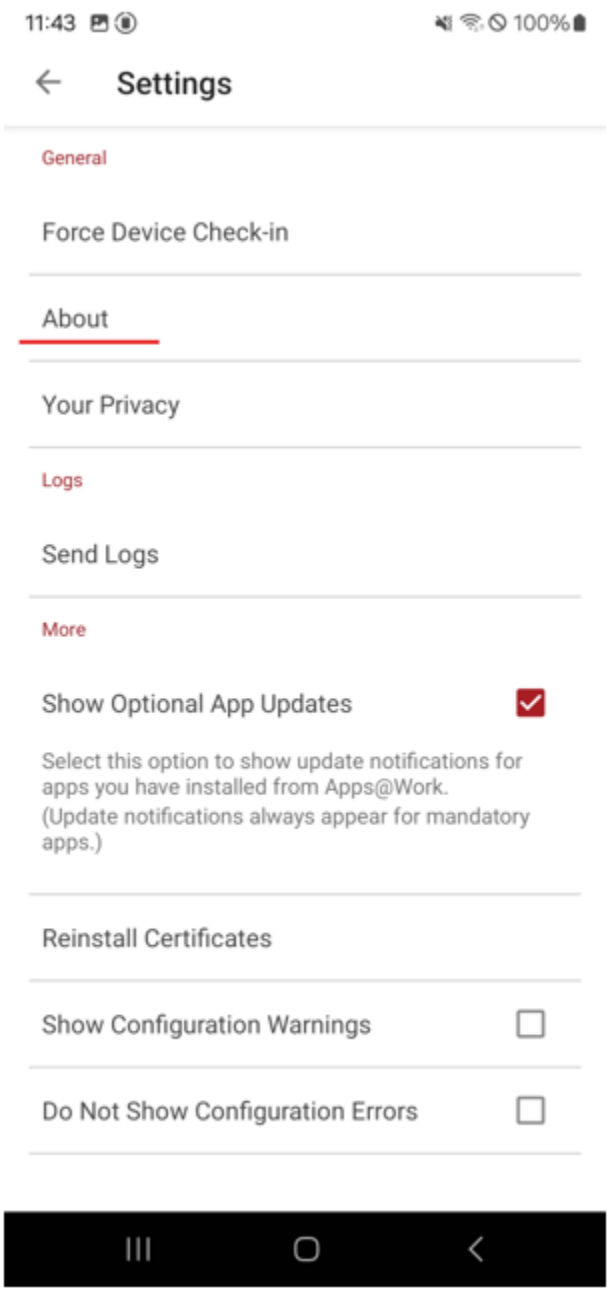


Figure 42: Android Mobile@Work Home > Settings Page

4. Select **About.**
5. Select **Product Detail**.

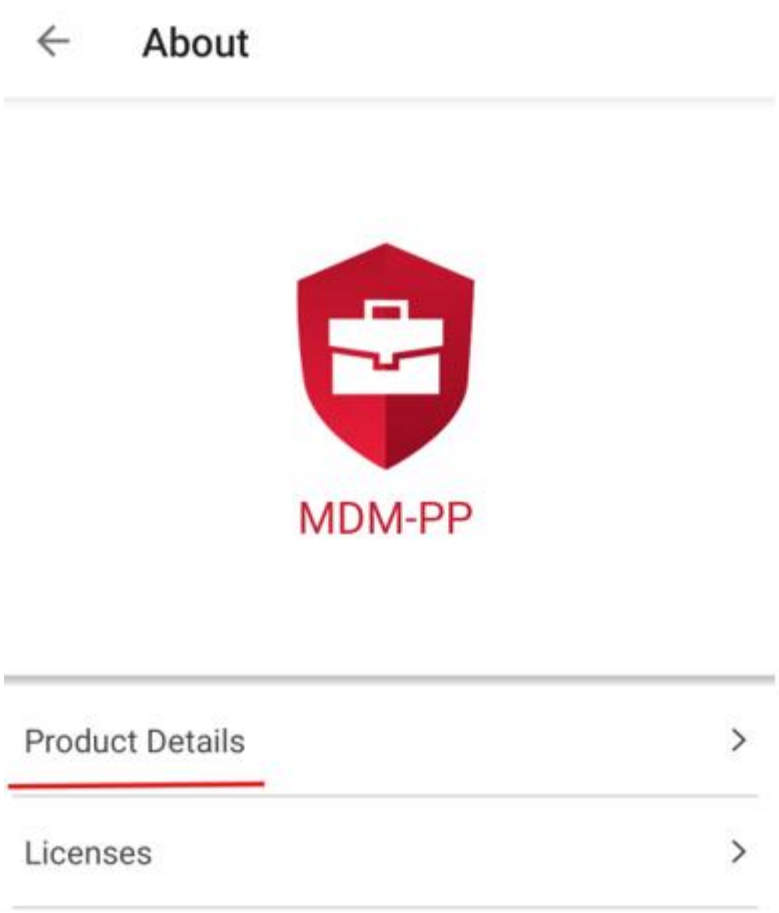


Figure 43: Android Mobile@Work Home > Settings About Page

6. View the MDM Agent version in the **Version** field.

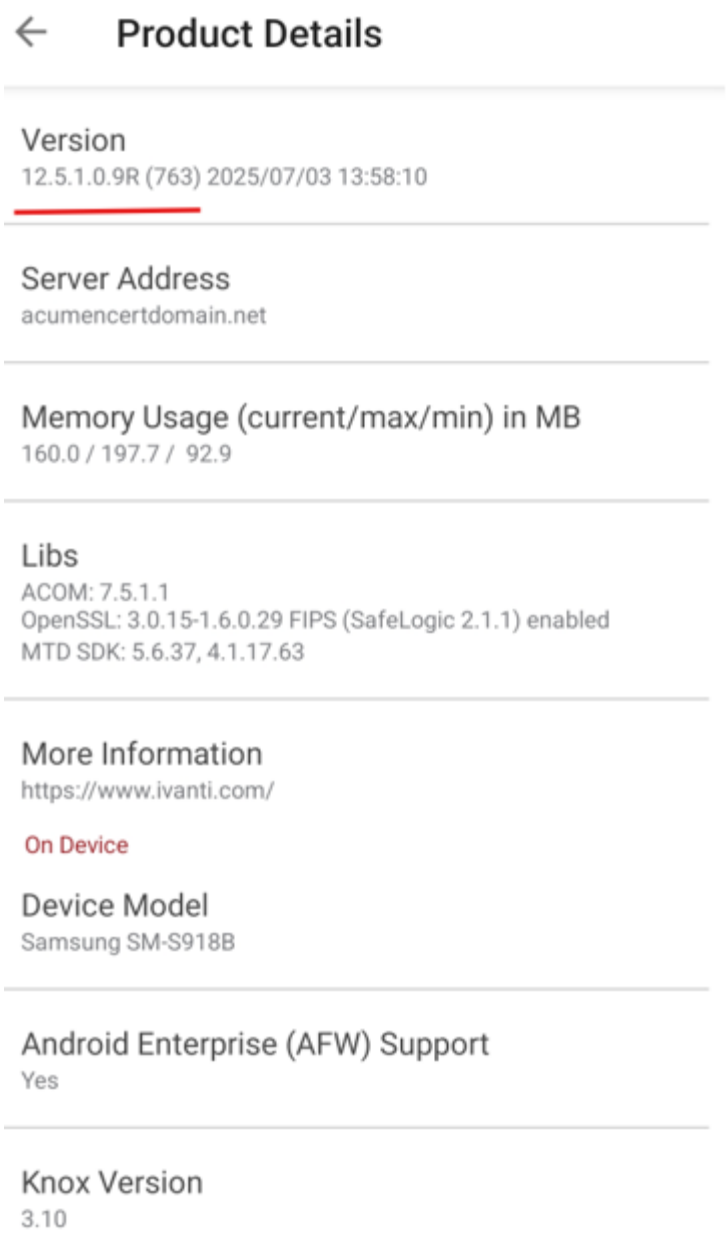


Figure 44: Android Mobile@Work Home > Settings > About > Product Detail Page

7.2.2 Query the Current Versions of Installed Mobile Device Applications

Prerequisites:
The Product(s) must be configured in the Common Criteria evaluated configuration.

Procedure:

7. From the Admin Portal, go to **Devices & Users > Devices.**
8. Find the row for the device. You can scroll down for the device or use the label filter or search filter.

9. Click on the up arrow to the left of the display name for the device. The device details panel displays.
10. Click the **Apps** tab. The list of apps installed on the device and their versions will be displayed.

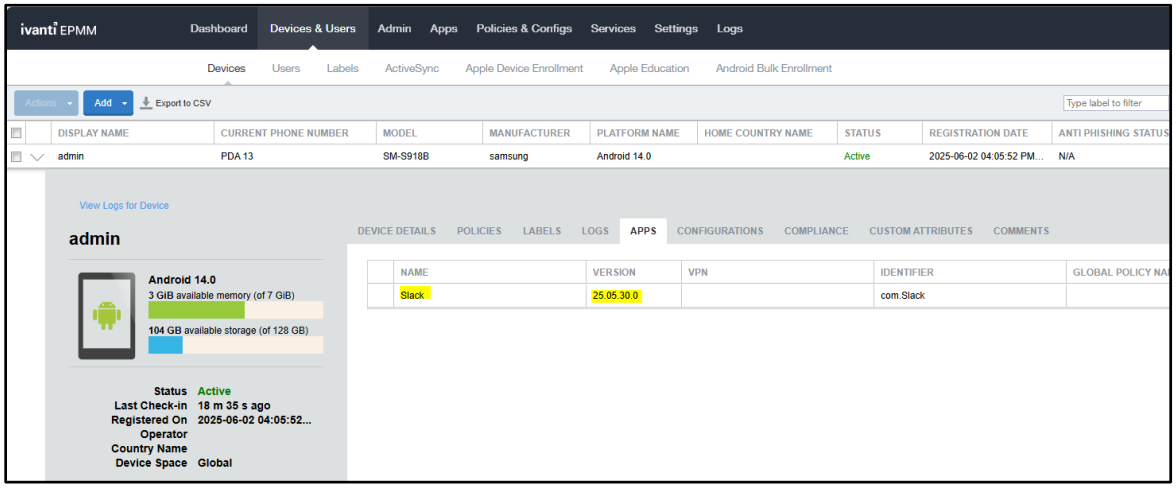


Figure 45: View App version

11. The name of the application installed can be viewed in the **NAME** column and the version in the **VERSION** column.

    Note: In this example the application installed is Slack with version 25.05.30.0.

7.2.3 Import X.509v3 Certificates

The EPMM allows importing of X509 certificates.

Procedure:

1. Using the **Admin Portal**, navigate to **Policies & Configs > Configurations.**
2. Click on **Add New > Certificates.** A new pop-up window will appear.

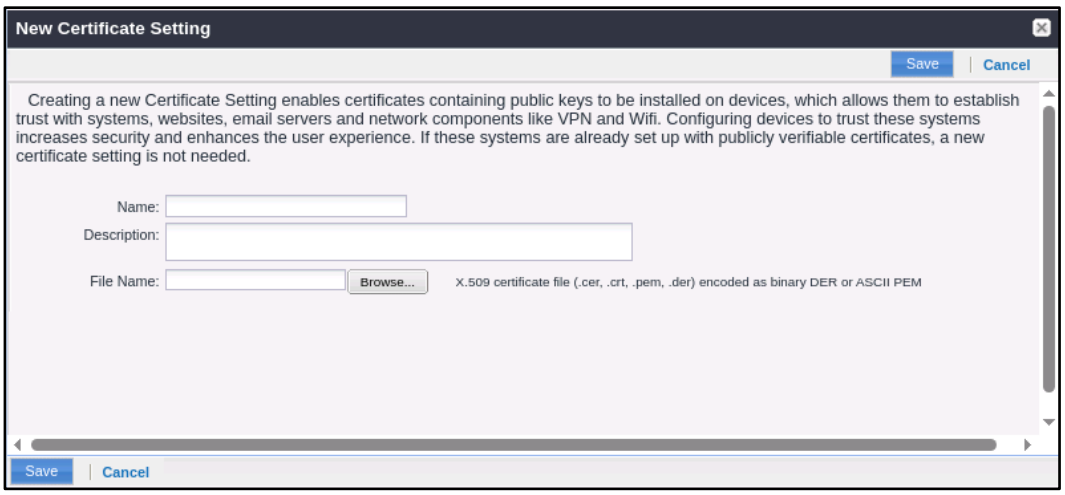


Figure 46: New certificate import

3. Fill all the required information:
    a. Name: Name to be displayed for the certificate being imported.
    b. Description: A brief description of certificate that is being imported.
    c. File name: Certificate file to be uploaded form the local storage (accepted formats .crt, .cer, .pem or .der)
4. Click **Save**
5. Click **OK**

The selected certificate file would be uploaded onto the EPMM server.
For more information pertaining to certificate configuration, refer sections Mutual authentication Trust certificate, Configuring a client identity certificate for mutual authentication and Importing x509v3 certificates as trusted root certificates.

7.2.4 Install Applications

Prerequisites:

The Product(s) must be configured in the Common Criteria evaluated configuration.

Procedure:

1. Using the **Admin Portal**, navigate to **Apps > App Catalog**.
2. Click on **Add** and select the application that is to be installed on the device.
3. Once the app is selected, click **Next.**
4. Add the required information (Application Name, Description and select the category)
5. Click **Next**.
6. Select the following option in the App Configuration page:
    i. **User Global App Config Policy**.
    ii. **Feature this App in the Apps@Work catalog** under the APPS@CATALOG

section

iii. **Per App VPN by Label Only** under the Per App VPN Settings section.

iv. **Install this app for Android enterprise** under the Android enterprise (all modes) section.

7. Select **Finish**. The app would be added successfully to the Admin portal.
8. Select the added application by clicking on the checkbox beside it and select **Actions > Apply to Labels**
9. Select anyone the labels created previously and click **Apply**. The label would be applied.
10. Navigate to **Devices & Users** and select the device.
11. Click on **Actions > Apply to Label** and select the Label which was previously selected in step 8.
12. Click **Apply.** The selected Label would be successfully queued for applying on the EPMM android client.
13. On the **EPMM android client**, open the **Mobile@Work** application.
14. Navigate to **Home > New Releases.**
15. The application can be installed on the EPMM android client by tapping on it.

7.2.5 Update EPMM Software

EPMM allows updating the device software. For more information, refer to section Updating the Android Client.

7.2.6 Remove Applications

Prerequisites:

- The Product(s) must be configured in the Common Criteria evaluated configuration.
- An application must be installed on the EPMM android client via the EPMM server.

Procedure:

1. Using the **Admin Portal**, navigate to **Apps > App Catalog**.
2. Locate the application to be removed and select it using the corresponding checkbox.
3. Once selected, go to **Actions > Remove from Labels.**
4. A new pop-up window would be displayed. Locate the applicable Label(s) to be removed and select it using the corresponding checkbox.
5. Once selected, click **Remove.** The application would be removed from the App catalog and the EPMM android client.

7.2.7 Update Password Parameters

Prerequisites:

The Product(s) must be configured in the Common Criteria evaluated configuration.

Procedure:

1. Using the **Admin Portal**, navigate to **Policies & Configs > Policies**.
2. All the configured and default policies will be displayed.
3. To configure the password parameters, either the default security policy can be modified, or a new policy can be created. (Refer section Install Policies for more information).
4. Select the Select the **Default Security Policy** using its corresponding checkbox. The policy parameters will appear in a separate pop-up window.

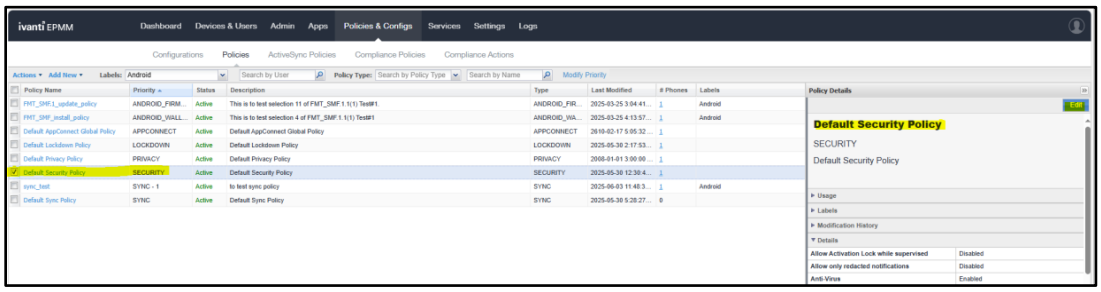


Figure 47: Policy details

5. Select the **Edit** button in the upper right corner of the pop-up window. The details of the policy will be displayed.
6. Adjust the password parameters using the following attributes:
    a. Enable password function → **Password: Mandatory**.
    b. Set password length → **Minimum Password Length**: *A Password length in the rage **1 – 16** is allowed.*
    c. Set password complexity → **Password Type**: *Can be Simple Alphanumeric or a combination of both.*
    d. Set password lifetime = **Maximum Password Age:** *Number of days before password renewal.*

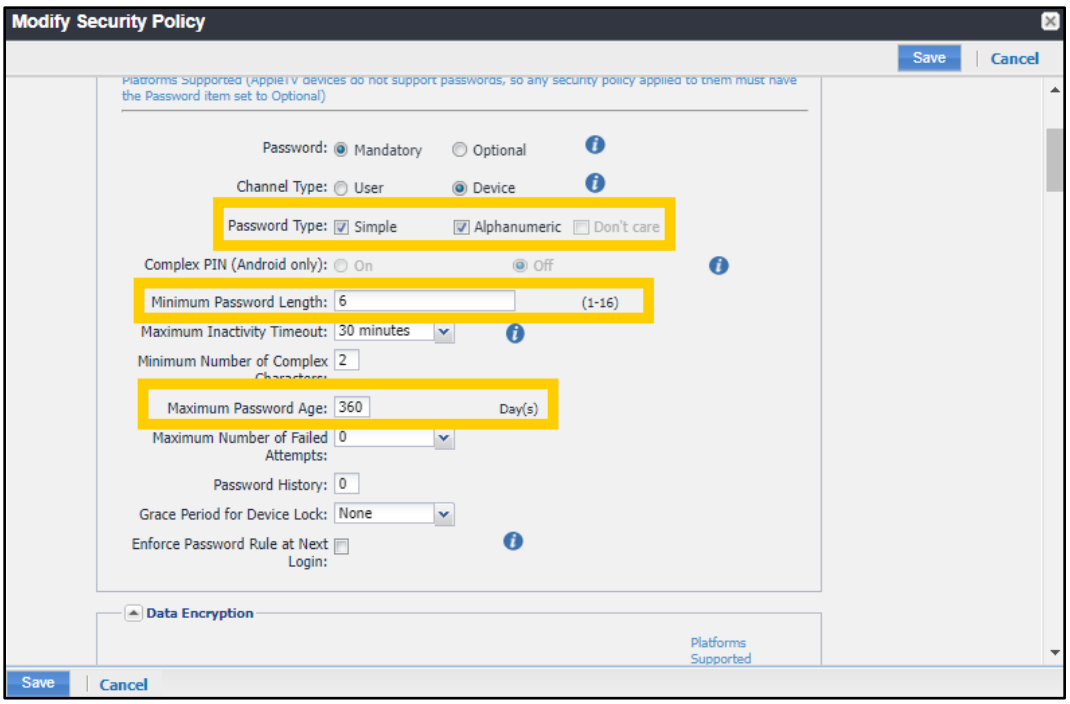


Figure 48: Security Policy, Password Parameters

7. Once all the password parameters have been modified as desired, select **Save**.
8. Click **OK**.

7.2.8 Configuring Session Locking Parameters

Prerequisites:

The Product(s) must be configured in the Common Criteria evaluated configuration.

Procedure:

1. Using the **Admin Portal**, navigate to **Policies & Configs > Policies**.
2. All the configured and default policies will be displayed.
3. To configure the password parameters, either the default security policy can be modified, or a new policy can be created. (Refer section Install Policies for more information).
4. Select the **Default Security Policy** using its corresponding checkbox. The policy parameters will appear in a separate pop-up window.
5. Select the **Edit** button in the upper right corner of the pop-up window. The details of the policy will be displayed.
6. Adjust the screen locking parameters using the following attributes:

a. Enable screen lock → **Password: Mandatory**

b. Disable screen lock → **Password: Optional**

c. Set screen lock timeout → **Maximum Inactivity**: *Number (in minutes) for idle timeout before triggering screen lock*

d. Set number of authentication failures → **Maximum Number of Failed**: *Number defining maximum login attempts before lockout*.

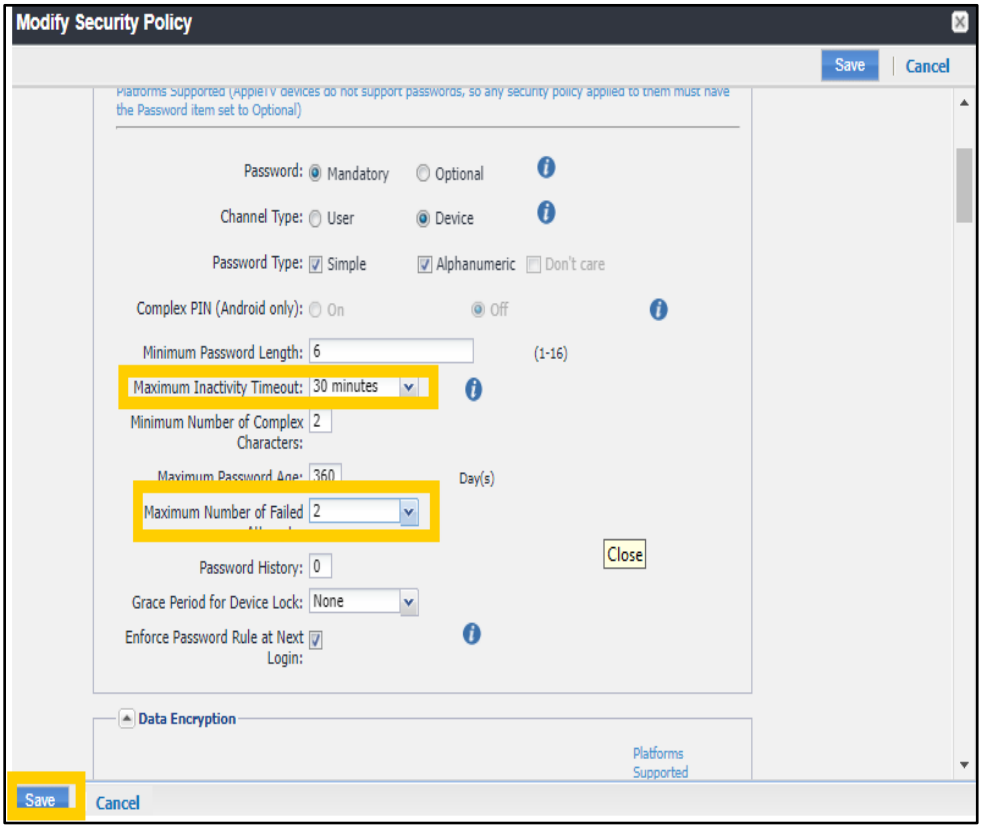


Figure 49: Session lockout

7. Once all the password parameters have been modified as desired, select **Save**.

8. Click **OK**.

7.2.9 Configure Wireless Network Policy

Prerequisites:

The Product(s) must be configured in the Common Criteria evaluated configuration.

Procedure:

1. Using the **Admin Portal**, navigate to **Policies & Configs > Configurations**.

2. Create a new certificate setting by clicking on **Add New > Certificates**. A new pop-up window will appear.

   Note: Creating a new Certificate Setting enables certificates containing public keys to be installed on devices, which allows them to establish trust with systems, websites, email servers and network components like VPN and Wifi.

3. Enter the following details:
   a. Certificate name in the **Name** field.
   b. Description in the **Description** field. (*optional*)
   c. Upload the trust certificate file in the **File name** field from the local storage. The file can be browsed by clicking on the **Browse** option.

4. Click **Save** and then click **OK**. A new certificate setting will be created successfully.

5. Select this newly created certificate setting using its corresponding checkbox.

6. Click **Edit**. The new pop-up window will appear for 'new single file identity certificate enrollment setting'.

7. Enter the following details:
   a. Certificate name in the **Name** field.
   b. Description in the **Description** field. (*optional*)
   c. Upload the trust certificate file in the **File name** field from the local storage. The file can be browsed by clicking on the **Browse** option.
   d. Password (*optional*)

8. Click **Save**.

9. Create a new Wi-Fi setting by clicking on **Add New > Wi-Fi**. A new pop-up window will appear to configure Wi-Fi settings

10. Enter configurational details as per the following:

Item	Description
Name	Enter the name to use to reference this configuration in Ivanti EPMM.
Network Name (SSID)	Enter the name (i.e., service set identifier) of the Wi-Fi network these settings apply to. This field is case sensitive. If the profile name and SSID are different, Windows devices will not connect to Wi-Fi.
Description	Enter additional text to clarify the purpose of this group of

	Wi-Fi settings.
Hidden Network	Select this option if the SSID is not broadcast.
Authentication	Select one: • WPA2 Enterprise • WPA2 Enterprise (iOS 8 or later except Apple TV) • WPA3 Enterprise (iOS 13 or later)
Data Encryption	Select the data encryption method associated with the selected authentication type. For WPA2 Enterprise authentication, the following encryption options are available: • AES • TKIP
User Name	Specify the variable to use as the user name when establishing the Wi-Fi connection.
Password	Specify the variable to use and any necessary custom formatting for the WiFi password. The default variable selected is $PASSWORD$. Enter additional variables or text in the text box adjacent to the Password field. Entries in this text box are kept hidden and will not be visible to any Ivanti EPMM administrator. If $PASSWORD$ is specified, the **Save User Password** must also be enabled which is located under **Settings > System Settings > Users & Devices > Registration** Note: All variables and text up to the last valid variable will be visible. Anything after the last valid variable will not be visible. The valid variable may appear in either of the password fields. Valid variables are variables in the drop-down list.
Apply to Certificate	Configure this field with the CA certificate needed to validate the Identity Certificate presented by the Wi-Fi Access Point. It is not the CA certificate needed to validate the Identity Certificate sent to the device in the Wi-Fi configuration.
Trusted Certificate Names	If you did not specify trusted certificates in the Apply to Certificates list, then enter the names of the authentication servers to be trusted. You can specify a particular server, such as server.mycompany.com or a partial name such as *.mycompany.com.
Allow Trust exceptions	Select this option to let users decide to trust a server when the chain of trust can't be established. To avoid these prompts, and to permit connections only to trusted services, turn off this option and upload all necessary

	certificates.
User pre-connection Password	Select this option to prompt the user to enter a password each time the device connects to the Wi-Fi network.
EAP type	Select the authentication protocol used: • EAP-FAST • EAP-SIM • LEAP • PEAP • TLS • TTLS **If EAP-FAST is selected**, then the Protected Access Credential (PAC) must also be specified. **If TLS is selected**, then an Identity Certificate must also be specified. **If TTLS is selected**, then the Inner Identity Authentication Protocol must also be specified. (Specification of an Outer Identity is optional).
Connects To	Select Internet or Work.
Apple Settings	These features are not supported on Windows devices.
Android Settings	These settings apply only to Android devices.
Windows Settings	Specifies whether a proxy is configured and which type is configured. The available types are **Manual** and **Auto**. Note: The Auto type is only available for Windows 10 Mobile devices.

11. Once the configuration is finished, click **Save**.
12. Click **OK**.
13. Select this newly created Wi-Fi setting using its corresponding checkbox and click on **Actions > Apply to Label.** A new pop-up window will appear.
14. Select the **Android** label using its corresponding checkbox.
15. Click on **Apply**. A message window confirming the action would appear.
16. Click **OK**.

7.2.10 Configure Wireless Network Security Policy

A wireless network security policy can be configured on the EPMM server. Security can be

implemented by employing one of the following:

1. WPA-Enterprise: Uses TKIP with RC4 encryption.
2. WPA2-Enterprise: Uses AES encryption with RC4 encryption.
3. WPA3: Uses Simultaneous Authentication of Equals (SAE) to provide stronger defenses against password guessing. SAE is a secure key establishment protocol.

For configurational information refer section Configure Wireless Network Policy.

7.2.11 Configure Application Installation Policy

Prerequisites:

The Product(s) must be configured in the Common Criteria evaluated configuration.

Procedure:

1. Using the **Admin Portal**, navigate to **Services > Google**.

2. The page will enable the administrator to enable or disable Android Users access to applications via Google Play or Apps@Work.

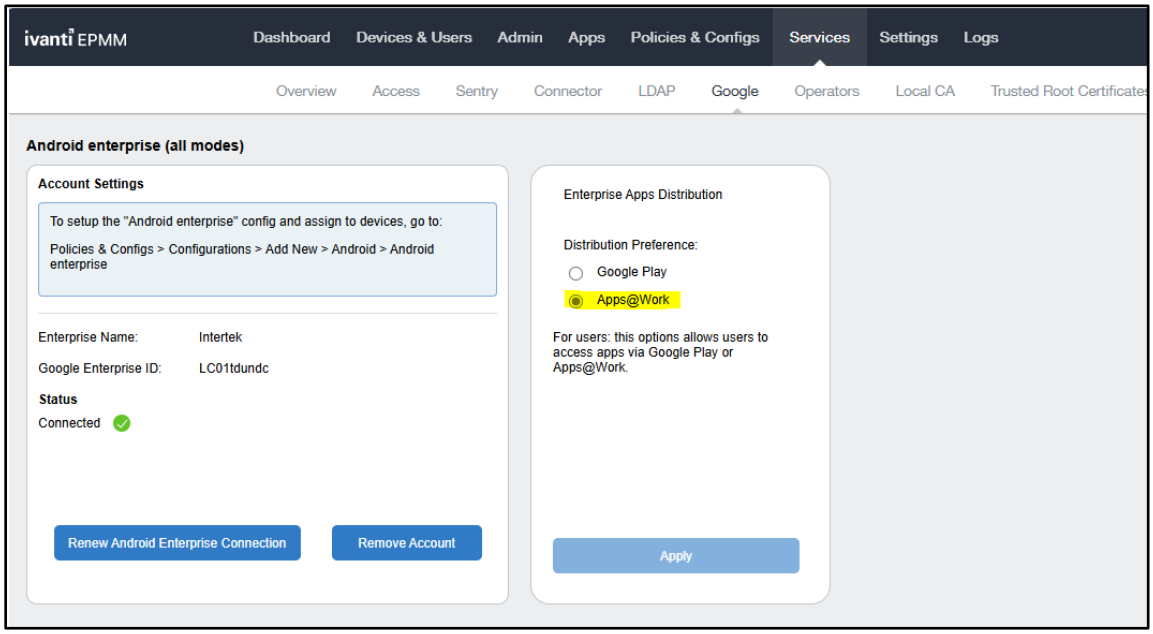


Figure 50: Application repository(s)

3. Select the desired option (Google Play/Apps@Work).

4. Click **Apply**.

7.2.12 Configure Enable/Disable Camera and Microphone

Prerequisites:

The Product(s) must be configured in the Common Criteria evaluated configuration.

Procedure:

1. Using the **Admin Portal**, navigate to **Policies & Configs > Policies**.

2. All the configured policies will be displayed. For Android devices, the **Lockdown Policy** is applicable for enabling/disabling of camera and microphone functions. Find the row for the for the currently installed Lockdown Policy or the Default Lockdown Policy.

3. Select the policy using its corresponding checkbox. A pop-up window explaining the details will appear.

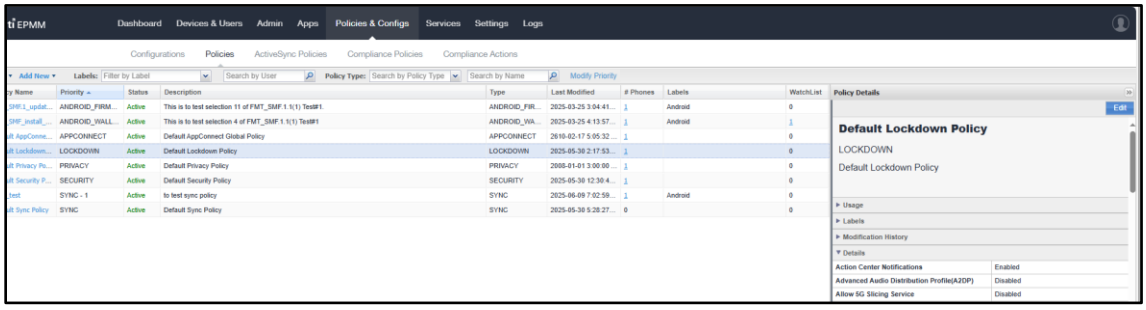


Figure 51: Security Policy Page

4. Click the **Edit** setting and a new pop-up window explaining the configurational parameters will appear.

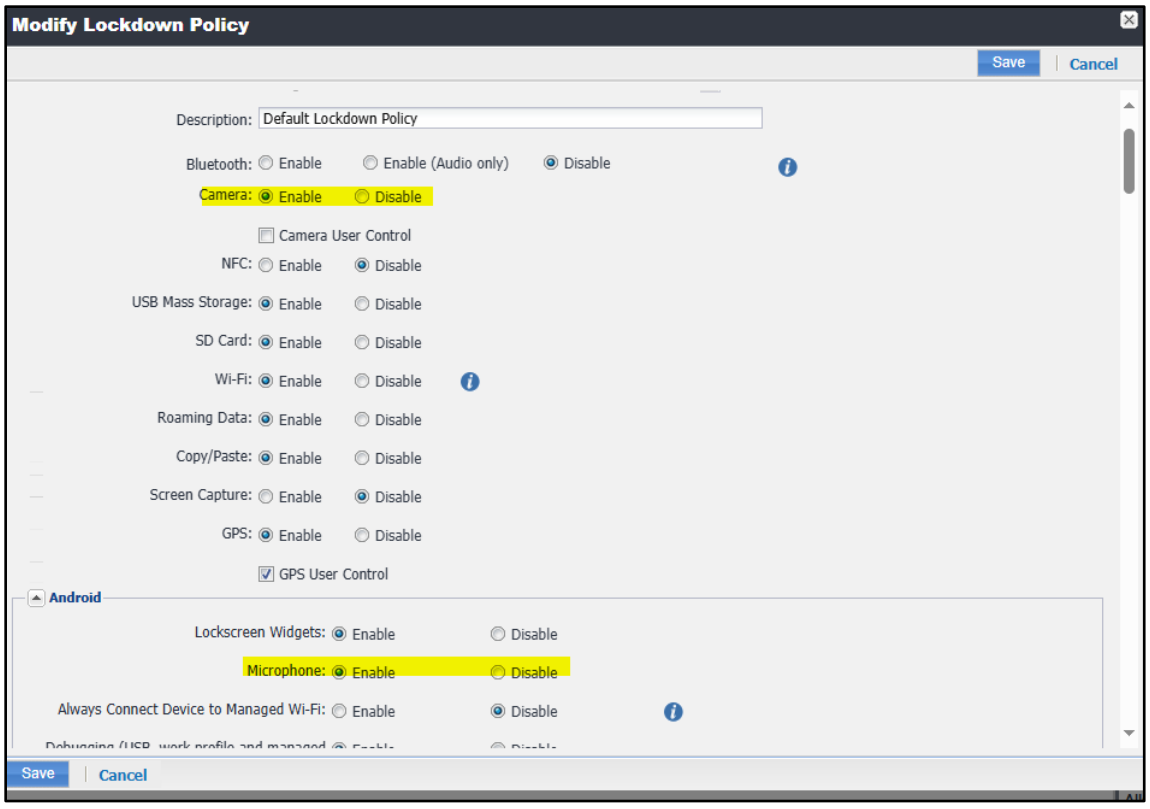


Figure 52: Lockdown policy configurational window

5. The camera and microphone can be configured by using the following:
    a. **Camera**: Can be Enable/Disable by selecting the corresponding checkbox.
    b. **Microphone**: Can be Enable/Disable by selecting the corresponding checkbox.
6. Select **Save**.

7.2.13 SECURITY MANAGEMENT ROLES

The MDM Server component of the TOE supports permission-based roles. The permissions are fine-grained and include viewing and managing devices; applying and removing policies, configurations, and labels; viewing logs and events, and managing administrators and device spaces.

The permissions are grouped into the following categories.

- Device Management – includes permissions that enable an administrator to view and manage devices which include adding and deleting devices, applying and removing device labels, wiping devices, locking and unlocking devices, force a device check-in, push profiles to a device, and retire a device.
- Privacy Control - includes permissions that enable an administrator to view apps in device detail, View device IP and MAC addresses, and locate devices.
- Label Management - includes permissions that enable an administrator to view and manage labels assigned to devices.
- User Management - includes permissions that enable an administrator to view and manage users and user attributes.
- App Management - includes permissions that enable an administrator to view apps resident on the EPMM Server Host, distribute apps, import and edit apps, and manage app licenses.
- Configuration Management – view and manage configuration, apply and remove configuration label, and delete configuration.
- Policy Management - includes permissions that enable an administrator to view and manage policies, apply and remove the policy label, delete policies, and manage the compliance action policy.
- Compliance Policy Management – view and modify the Security Policy which contains compliance information.
- Logs and Events Management - includes permissions that enable an administrator to view audit logs, manage and view events, and manage and view certificates.
- Admin Management - includes permissions that enable an administrator to manage administrators ad device spaces.

Procedure:

1. Using the **Admin Portal**, navigate to **Devices & Users > Users > Add > Add Local User** to add a new user.

2. A new **Add New User** window would appear. Add all the necessary details to create a new user.
3. Select the newly created user (or existing default users) using its corresponding checkbox.
4. Once selected, click on **Actions > Assign Roles.**

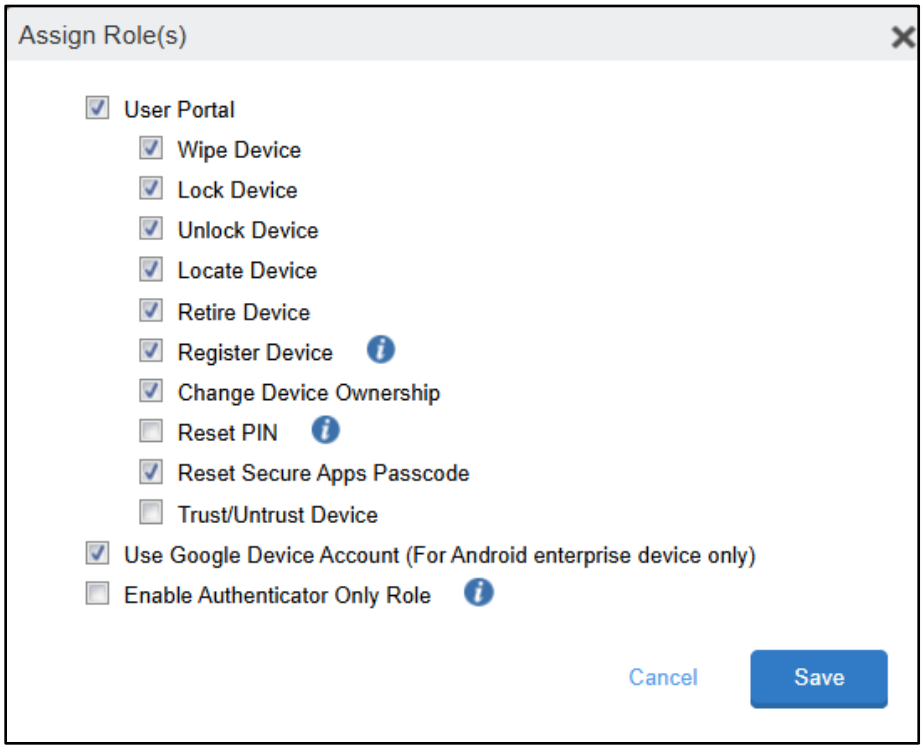


Figure 53: User roles

5. Select the roles that are to be assigned to the user.
6. Click **Save**

7.3 System Management Commands

7.3.1 Overview

This section describes the non-FMT_SMF SFR management functions required by the EPMM Server for the Common Criteria Evaluation.

7.3.2 Configure Device Limit

Prerequisites:

The Product(s) must be configured in the Common Criteria evaluated configuration.

Procedure:

1. Using the **Admin Portal**, navigate to **Settings > Users & Devices >**

Registration

2. The device enrollment limit can be configured using the following two parameters:

   i. **Registration PIN and passcode expiry:** Device enrollment can be restricted by setting password, PIN, or both during registration. By default, the user is required to enter a password to register the device, however this can be changed by the administrator.

      - Passcode Expiry (hours): After the configured number of hours, the registration passcode expires. The default is 4 hours. The minimum value is 1 hour. The maximum value is 4320 hours (6 months).
      - Registration PIN Code Length (6-12): By default, device users must enter a password to register a device.

   ii. **Per-User Device Limit:** The device enrollment limit can be configured by defining a limit on the number of devices that can be enrolled on the EPMM server using the **Per-User Device Limit** function.

   Note: The device range must lie within the range of 1-50 devices or can selected as none.

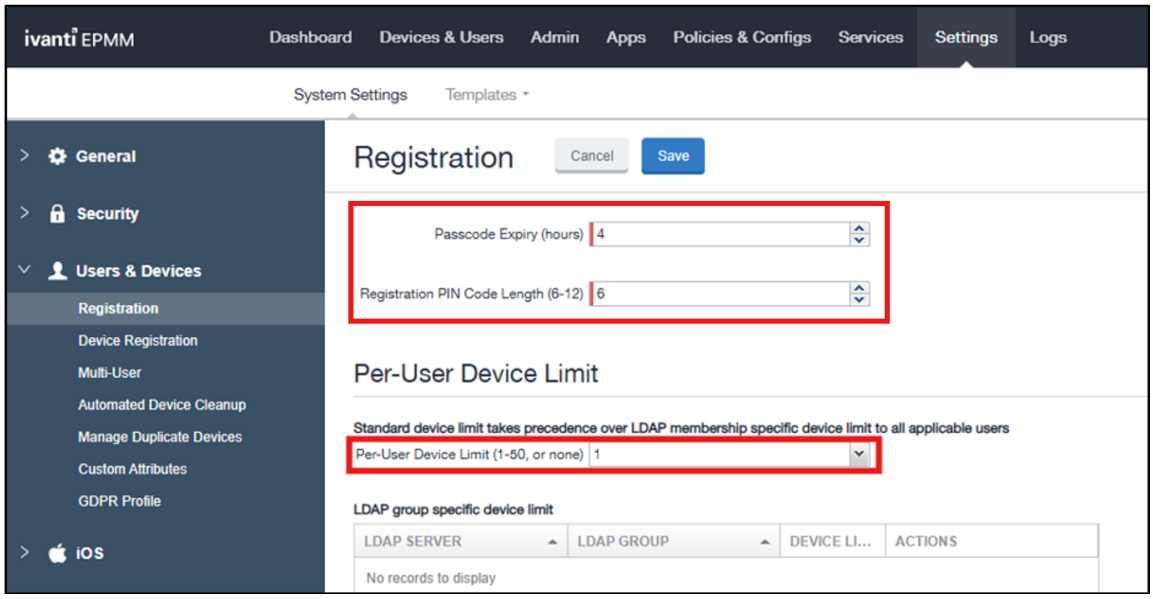


Figure 54: Device enrollment limit

7.3.3 Configure Unenrolling Devices

The EPMM system does not allow configured Mobile Device User (MAS MD User or MD User role) to unenroll from the enterprise. The EPMM system does not provide the functionality that enables a user to unenroll. Additionally, Mobile Device Users enrolled and using the EPMM System are in the evaluated configuration non-Android

administrators. This non-administrator privilege status means the MAS MD User and MD User cannot uninstall or remove the MDM Agent Ivanti application.

7.3.4 Configuring the Application Access Groups

Application Access Groups refer to collections of users or devices that are granted controlled access to specific mobile applications or app configurations. Ivanti EPMM allows configuring the application access groups using **Labels**.

Note: Label is a dynamic tag used to group devices based on specific criteria, enabling targeted policy enforcement, app distribution, or configuration management.

7.3.4.1 Creating labels

There are two ways to create a label:

1. Use Advanced Search and save the criteria to a new label.
2. Create a new label.

Procedure:

1. Using the **Admin Portal**, navigate to **Device & Users > Labels**.
2. Click **Add Label**. The Add Label pop-up window will appear.

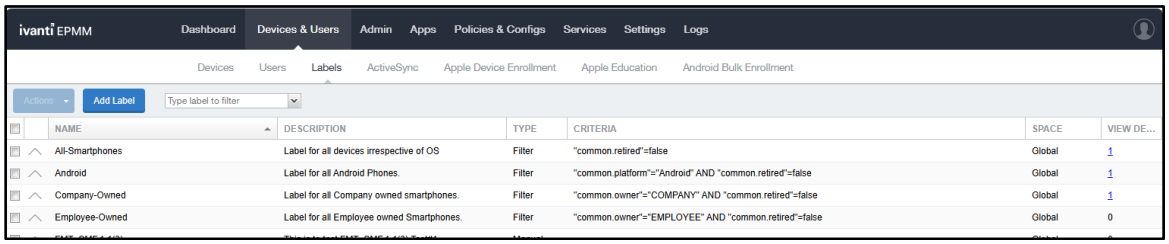


Figure 55: Add label

3. Refer to the guidelines below to complete the fields for the Add label window.

Field	Description
Name	Enter a unique name that clearly identifies the purpose of the label. The following characters are allowed when entering a label name. All other characters, including spaces, are prohibited. • Letters (uppercase and lowercase) • Numbers (0-9) • Dashes (-) • Underscores (_) • Periods (.) • At sign (@) • Dollar sign ($) • Hash tag (#) • Extended ASCII/UTF-8

Description	Provide additional meaning and usage information.
Type	By default, the type is **Filter**. Change it to **Manual** if you want to manually associate devices with the label.
Criteria	If the type is Filter, use the query builder to create a search expression that defines the devices to apply the label to. Alternatively, manually enter a search expression. The matching devices are automatically displayed.

4. Click **Save**.
5. Once configured, the device can be applied a label tag by following the procedure in the section Applying a device to a label.

7.3.4.2 APPLYING A DEVICE TO A LABEL

Procedure:

1. Using the **Admin Portal**, navigate to **Device & Users > Devices**.
2. Select the check box for the device.
3. Click **Apply To Label** from the **Actions** menu.
4. Select the label to apply from the **Apply To Label** dialog.
   Note: Only labels that have not already been associated with this device will be displayed. For example, iOS devices are automatically applied to the iOS label, Android devices to the Android label, and so on. Also, automatic labels that are not applicable to this device do not appear in the list. For example, the Windows label and Windows Phone label will not appear for a device from a different platform.
5. Click **Apply**.

7.3.5 DOWNLOAD APPLICATIONS TO ANDROID DEVICE

EPMM allows downloading of applications to an android device (EPMM client MDM agent). Refer section Install Applications for more information.

7.3.6 CONFIGURING SERVER ALERTS

EPMM logs device status events. Device status events alert the administrators in the following events:

1. Change in enrollment status

2. Failure to apply policies to a mobile device

Prerequisites:

The Product(s) must be configured in the Common Criteria evaluated configuration.

Procedure:

1. Using the **Admin Portal**, navigate to **Logs > Event Settings**.

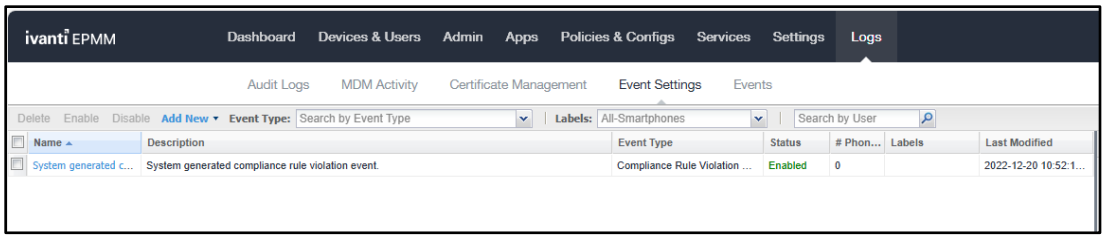
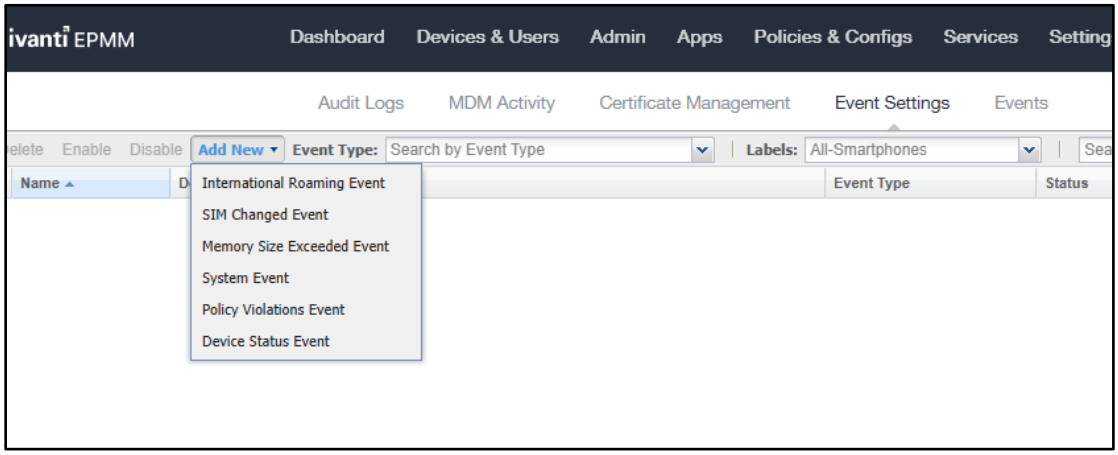


Figure 56: Event Settings

2. Select the **Add New** pull-down menu option. The following pull-down menu will be displayed.



3. Select **Device Status Event**. A device status event configuration pop-up window will appear.

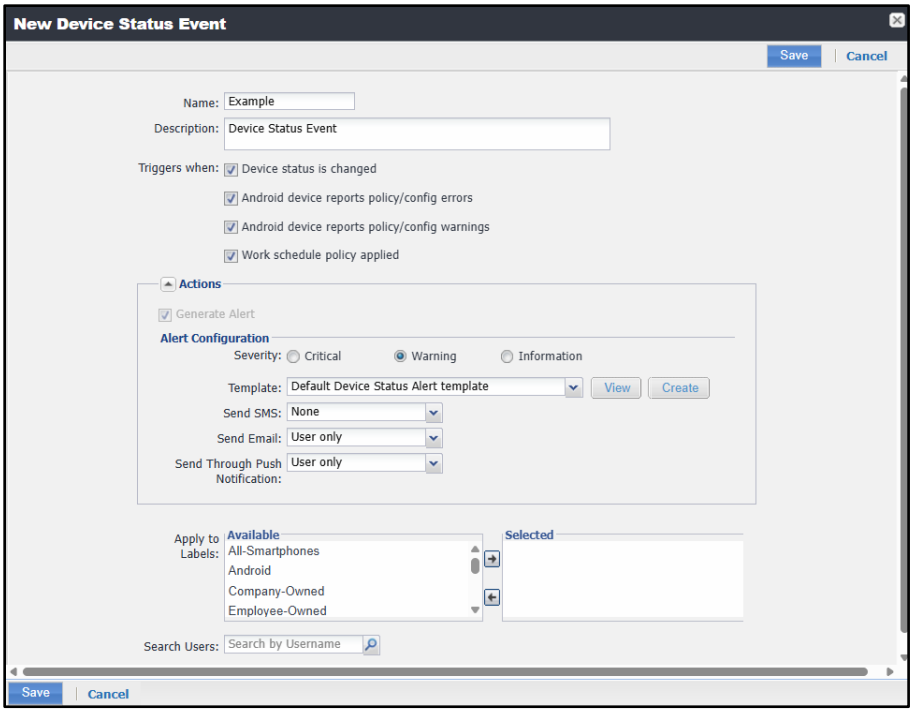


Figure 57: Device Status Event window

4. Use the following guidelines to fill in the fields:

Field	Description
Name	Identifier for this event.
Description	Additional text to clarify the purpose of this notification.
Triggers when	Specifies the conditions on the device that will trigger an alert: • Device status is changed (Android and iOS) • Android device reports policy/config errors • Android device reports policy/config warnings • Work schedule policy applied (Android and iOS)
Actions	
Severity	Specifies the severity you define for this alert. Select **Critical**, **Warning**, or **Information**.
Template	Specifies the template to populate the resulting alert. Select **View** to display the content of the current template. Select an alternate template from the drop-down or Select **Create** to create a new template.
Sends SMS	Specifies whether to send an alert in a text message, and whether to send it to the user, the administrator, or both. Specify users in the Apply to Users section or by selecting a label in the Apply to Labels section. If you select "Admin only" or "User + Admin", then the CC to Admins section appears. Use

	this section to specify administrative users who should receive the alert.
Send Email	Specifies whether to send an alert in an email, and whether to send it to the user, the administrator, or both. Specify users in the Apply to Users section or by selecting a label in the Apply to Labels section. If you select "Admin only" or "User + Admin", then the CC to Admins section appears. Use this section to specify administrative users who should receive the alert.
Send through Push Notification	Specifies whether to send a message, and whether to send it to the user, the administrator, or both. Specify users in the Apply to Users section or by selecting a label in the Apply to Labels section. If you select "Admin only" or "User + Admin", then the CC to Admins section appears. Use this section to specify administrative users who should receive the alert. The length of the message is limited to 255 characters.
Apply to Labels	Send the alert to users in the selected labels. (Refer section Configuring the Application Access Groups for labels)
Search Users	Enter the user ID to find users to which you want to send the alert.
Apply to Users	Send the alert to the selected users.
CC to Admins	If "Admin only" or "User + Admin" is selected, then the CC to Admins section appears. Use this section to specify administrative users who should receive the alert.

Note: The "Triggers when" field determines the alerts condition. Selecting the "Device status is changed (Android and iOS)", "Android device reports policy/config errors" and the "Android device reports policy/config warnings" options would alert the administrator in case of changes in the device enrollment status and failure to apply policies.

5. Select **Save**.

7.3.7 Configuring the Sync Interval for a Device

Prerequisites:

The Product(s) must be configured in the Common Criteria evaluated configuration.

Procedure:

1. Using the **Admin Portal**, navigate to **Policies & Configure > Policies**.
2. Click on the **Default Sync Policy** and a separate window will appear displaying certain parameters.

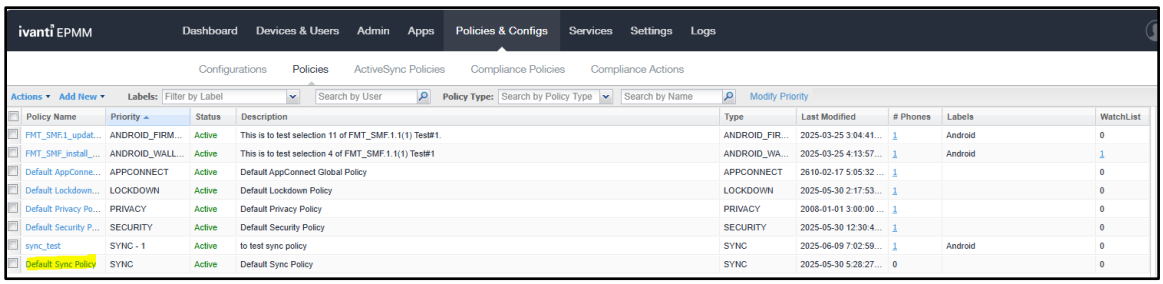


Figure 58: Default sync policy

3. Click on **Edit** option and the configurational pop-up window will appear.

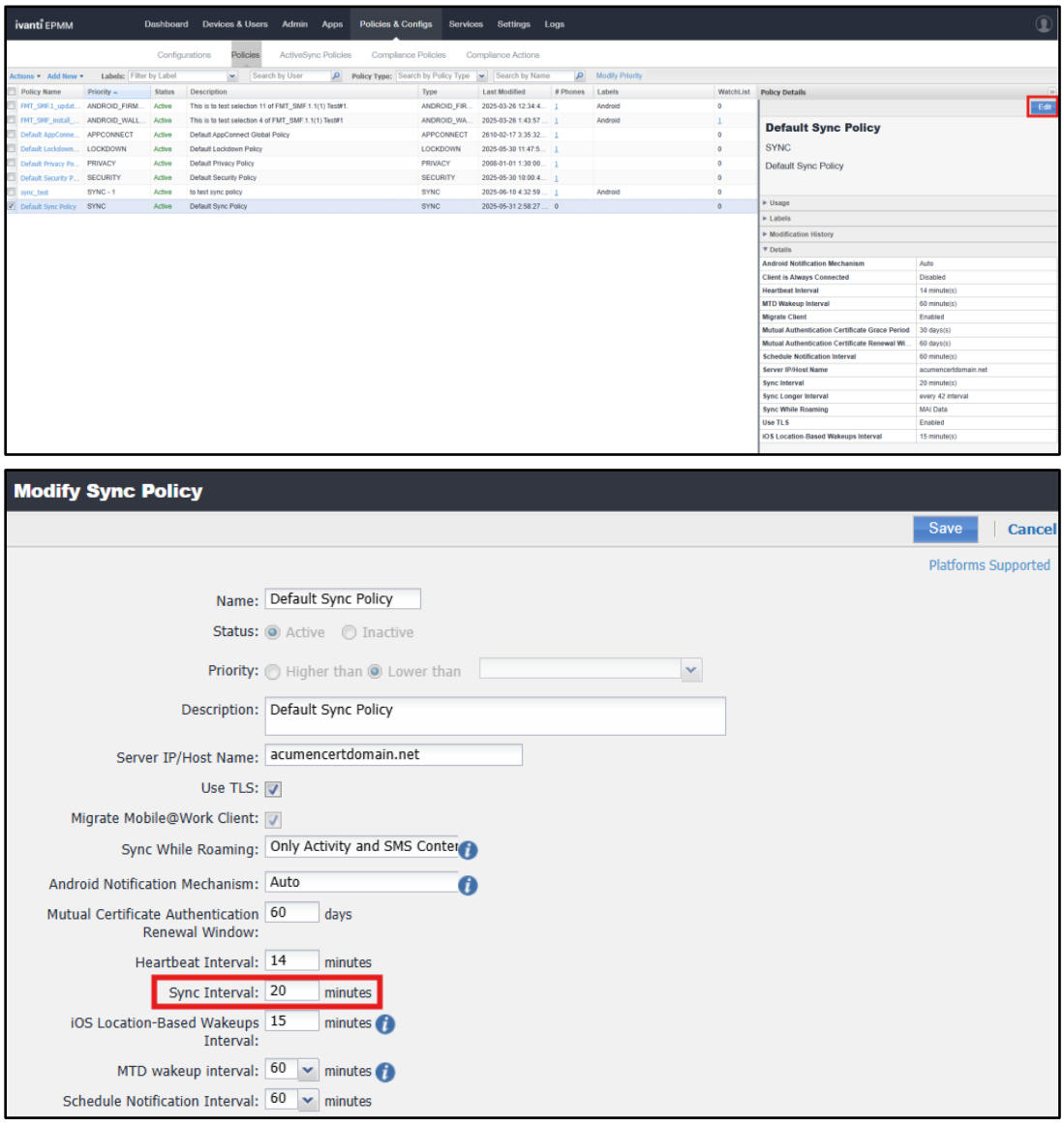


Figure 59: Modify Sync policy

4. Set the desired sync interval (in minutes) using the **Sync Interval** field.

8 Updating the EPMM System Software

8.1 Overview

This section explains the configuration steps required to update the software on both the EPMM Server and the MDM agent. The following sub-sections describe how to check the currently installed software version, obtain the latest available software, carry out the update process, and verify that the updates have been successfully applied.

8.2 Updating the EPMM Server Software

8.2.1 Determining The Current Version of the EPMM Server

Prerequisites:

The Product(s) must be configured in the Common Criteria evaluated configuration.

Procedure:

1. Using the **Admin Portal**, navigate to **Dashboard**
2. Expand the user menu on the top right.

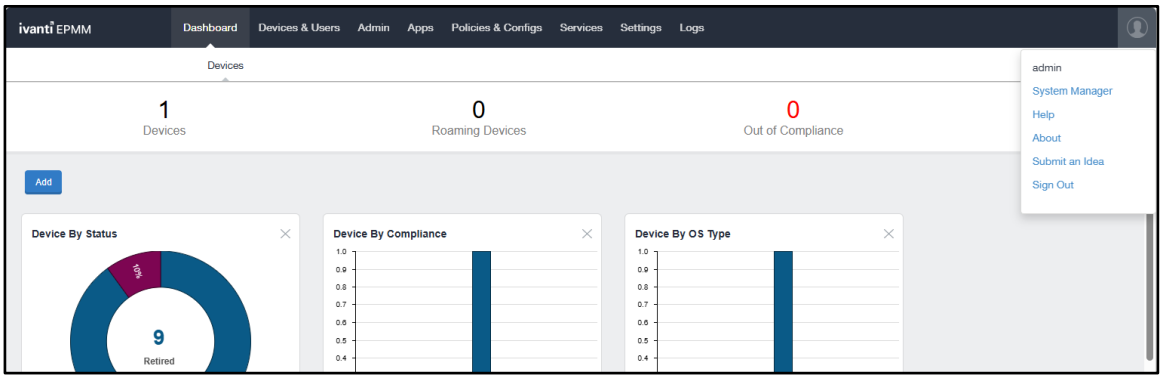


Figure 60: Admin portal dashboard

3. Click on **About** from the pull-down menu. An information window would be displayed.
4. The information against the **Release Version** tag displays the current version.



Figure 61: Information window

Note: In the example show in **Figure 61: Information window**, the release version is 'EPMM 12.3.1.0 Build 73', however, the actual **Release Version** should match the Build Name as displayed in Table 3 of this document

5. Click on **OK**. (To close the window)

8.2.2 Updating the EPMM Server Manually

8.2.2.1 Fetching updates online

Prerequisites:

- The Product(s) must be configured in the Common Criteria evaluated configuration.
- You must have Ivanti login credentials.

Procedure:

1. Log into the **EPMM System Manager**.
2. Navigate to **Maintenance > Software Updates** to display the **Software Updates** options.
3. Scroll down to the **Manually Update OS, Device and other EPMM data:** section

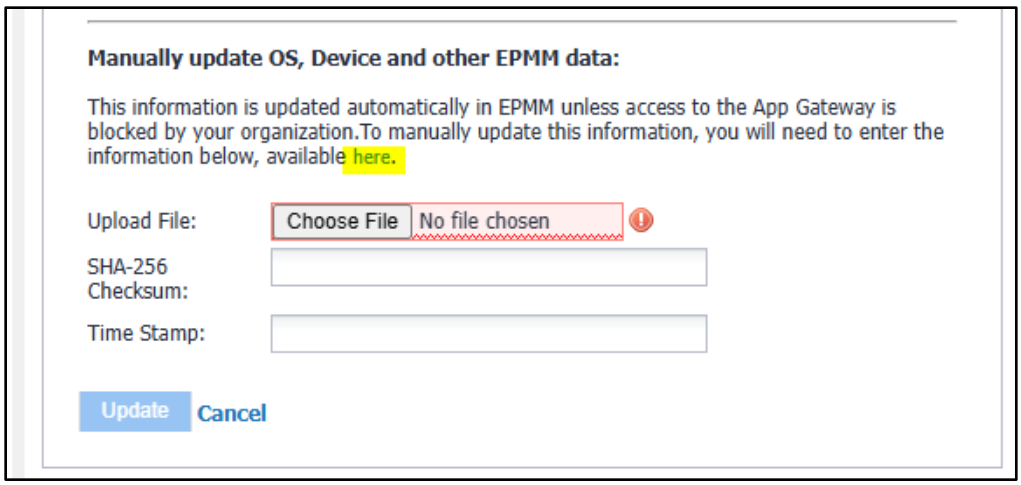


Figure 62: Online updates

4. Click on the **here** option. (Refer **Figure 62: Online updates**)
5. A page will appear showing the latest version that is available for download.



Figure 63: Ivanti Support - Device and Platform Page Example

6. The information displayed will detail the latest version.

   Note: The EPMM Server used for testing and creation of this manual is a later version than the publicly available EPMM Server at the time. Hence the display of older versions of code. Once, EPMM Server is CC certified and released, Version will reflect the evaluated version or a later version i.e. the Version will be later than the 12.3.1.0 Build 73 evaluated version.

7. If the version displayed is later than the version installed, click on the **Download Update File** option. The file will be downloaded on your computer in .zip format.

8.2.2.2 INSTALLING/UPDATING THE EPMM SERVER

Prerequisites:

The Product(s) must be configured in the Common Criteria evaluated configuration.

Procedure:

1. Log into the **EPMM System Manager**.
2. Navigate to **Maintenance > Software Updates** to display the **Software Updates** options.
3. Scroll down to the Manually Update OS, Device and other EPMM data:
4. Go to the **Software repository configuration** group.
5. Enter the credentials assigned by Ivanti Support.
6. Click **Apply > OK**.
7. Click **Check Updates** to show a list of the available updates.
8. Select the update you want.
9. Click **Download Now** if you want to download the update now and complete the installation later.
10. Refresh the screen and click **Check Updates**. After the download is complete, the status for the update changes to Downloaded.
11. Click **Validate** to validate the database and select one of the following options:
12. Validate Database structure (schema) to verify that the existing database has the right database structure to proceed with upgrade.

    - **Validate the Database structure and Data** to copy the database to a temporary database to run the validation then click **Yes** to stop EPMM services, (required for validation). Validating the database with data can take up to 4 hours, depending on the database size.

      The Validation Status includes the following options:

      - Not Running
      - Validation Running
      - Validation Failed
      - Validation is Successful

    Note: If the validation fails, do not proceed with the upgrade and contact Ivanti Support. When the database validations have no errors, then you can proceed with upgrading the environment.

13. Refresh the screen and click **Check Updates**.

14. Click **Stage for Install** when the software is ready to install.
    - If you have already downloaded the selected update, the system stages the update for installation.
    - If you did not previously download the selected update, it is downloaded and staged for installation.

15. After the software update has been staged for installation, the status for the update changes to **Reboot to Install** and the software image can be installed by issuing a reboot. If the status of an update is not **Reboot to Install**, rebooting the system will not install the update.

    Note: Software updates are verified using digital signatures during the download process. When a matching signature is confirmed, the status for the update changes to **Reboot to Install**.

16. Select **Maintenance > Reboot** to reboot Ivanti EPMM.

17. Verifying the upgrade is complete. Refer section Verifying the EPMM Upgrade/Installation is Complete.

8.2.2.3 Verifying the EPMM Upgrade/Installation is Complete

Procedure:

1. Log into the **EPMM System Manager**.

2. Navigate to **Maintenance > Software Updates**

3. Verify the EPMM version using the **Software Version** section. Confirm that the current version is correct.

8.2.3 Upgrade using Repository

Note: TLS authentication is mandatory for users to upgrade the software. The user must enable the Mutual authentication check box on the Ivanti EPMM admin portal under **Settings > Security > Certificate Authentication**.

To upgrade Ivanti EPMM software using the System Manager:

Procedure:

1. Using the **EPMM System Manager**, navigate to **Maintenance > Software Updates**. This page will display the Software Updates options.

2. Go to the **Software repository configuration** section.

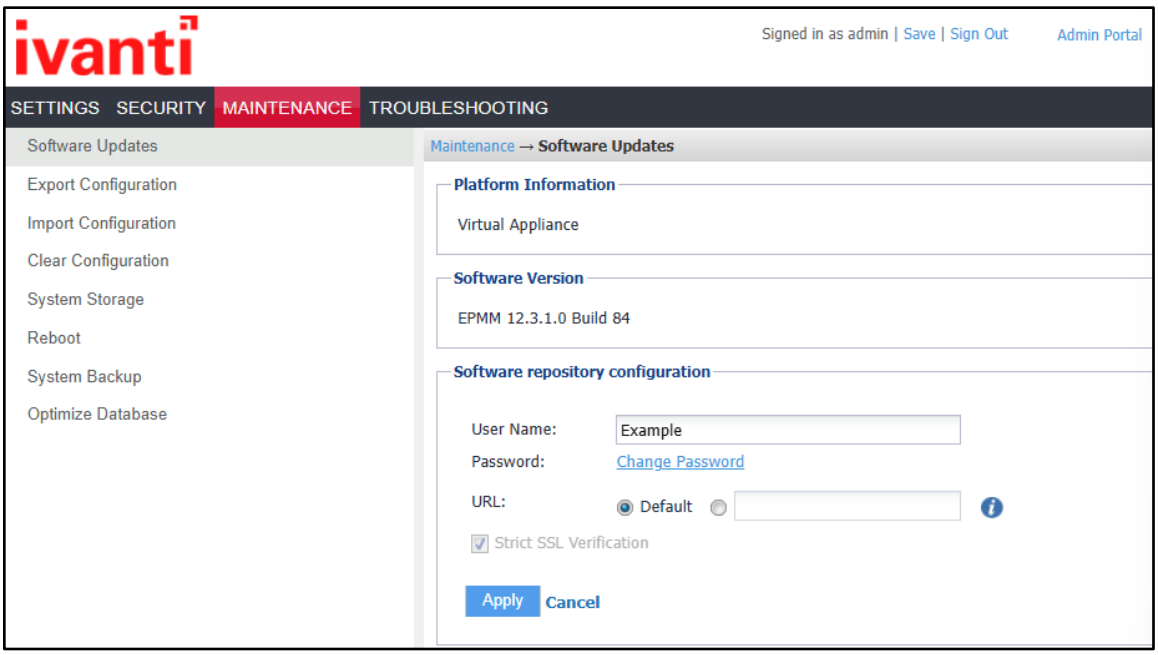


Figure 64: Update using repository

3. Enter the credentials assigned by Ivanti Support.

   Note: The upgrade procedure presented here assumes the usage of the default upgrade URL. If you intend to specify an alternate URL, be sure to include the build number of the target upgrade. Go to Maintenance > Software Updates> software repository configuration > Uncheck Default and enter the alternate URL.

4. Click **Apply > OK**.

5. Click **Check Updates** to show a list of the available updates.

6. Select the required update.

7. Click **Download Now** and complete the installation at a later time.

8. Refresh the screen and click **Check Updates**.
   After the download is complete, the status for the update changes to **Downloaded**.

9. Click **Validate** to validate the database and select one of the following options:

   a. **Validate Database structure (schema)** to verify that the existing database has the right database structure to proceed with upgrade. If the validation fails, do not proceed with the upgrade and contact Ivanti Support.

b. **Validate the Database structure and Data** to copy the database to a temporary database to run the validation then click **Yes** to stop EPMM services, (required for validation).

Note: The Validation Status include the following options:

- Not Running
- Validation Running
- Validation Failed
- Validation is Successful

10. Refresh the screen and click **Check Updates**.
    After the software update has been staged for installation, the status for the update changes to **Reboot to Install** and can be installed by rebooting the system. If the status of an update is not Reboot to Install, rebooting the system will not install the update.

11. Select **Maintenance > Reboot** to reboot Ivanti EPMM.

12. Click **Stage for Install** when the update is ready for installation. If the selected software (for update) has already been downloaded, the system stages the update for installation. And if not, it is downloaded and staged for installation.

13. Click **Yes** to agree to the End User License Agreement and proceed further.

14. Refresh the screen and click **Check Updates**.

15. Verifying the upgrade is complete. Refer section Verifying the EPMM Upgrade/Installation is Complete.

8.3 Updating the Android Client

8.3.1 Determining The Current Running Version of the Android Client

The current software of the MDM Agent component of the TOE (Ivanti MDM Agent for Android) installed by viewing the app's About Screen from their Android deviceQuery Current Version of the Mobile Device Firmware/Software.

8.3.2 Installing the MDM Agent software

Use this installation method if the device users prefer installing the Federal build themselves. The overall steps for installing from a web site are:

- Put the certified MDMPP Federal build for Android APK file on a website and disclose its URL to your device users.

- Device users put the URL in a browser on their device to download the APK file.

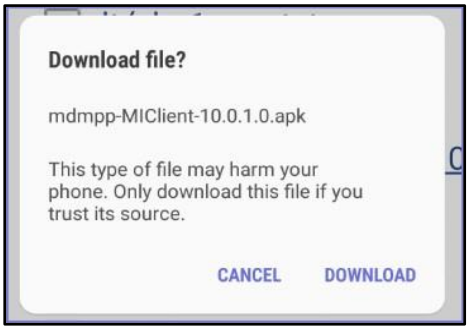
Procedure:

1. Download the Federal build APK file from https://support.mobileiron.com/MIClient-latest.apk to any computer/laptop.
2. Upload the Federal build APK to a network location accessible to your device users.
3. Provide the URL to device users.
4. Each device user does the following:

   Note: The screen shots in these steps are examples to illustrate the procedure. The actual screen shots may vary depending upon the device in use.

   a Enter the provided URL that the address bar of a browser on the device.

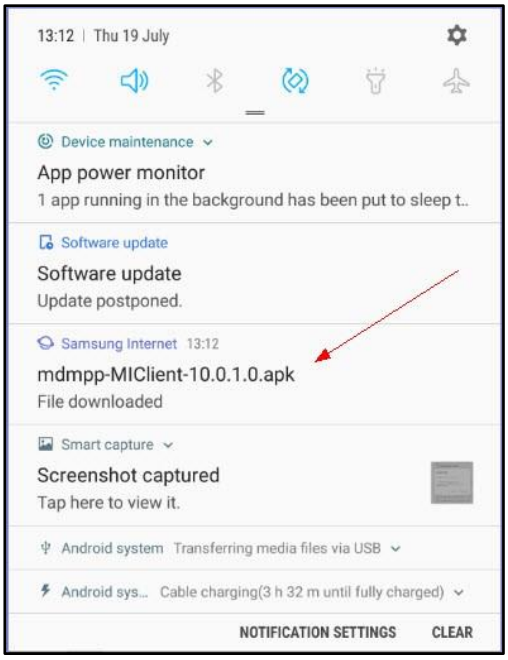
   b When the browser has loaded the URL, it prompts the device user to accept the APK file, as in the following example:



   c Tap **Download**.

   d The download of Federal build begins in the background.

   e Pull down the device's notification bar to see the download progress, which is completed in the following example:

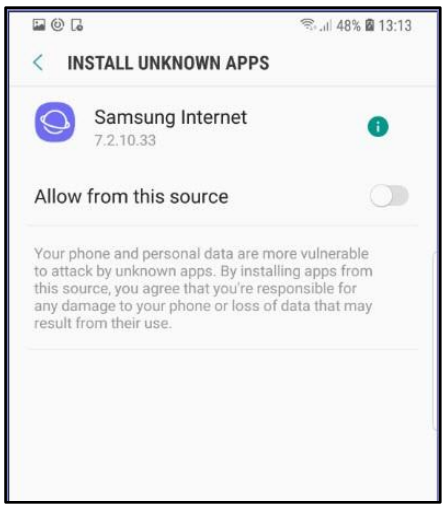


f When the download is complete, tap the notification to begin the installation.

g If the Unknown sources setting is not enabled already, a prompt appears to go to the device's settings to enable it.

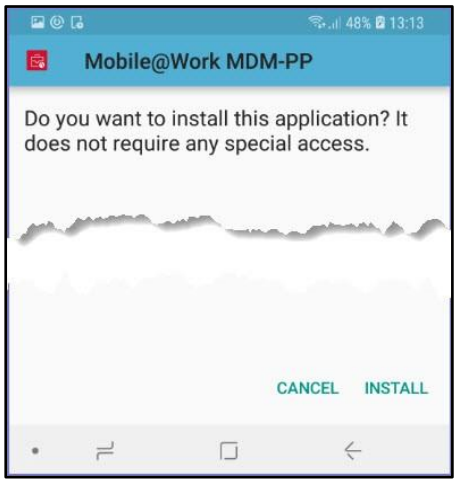


h Tap **Settings**.



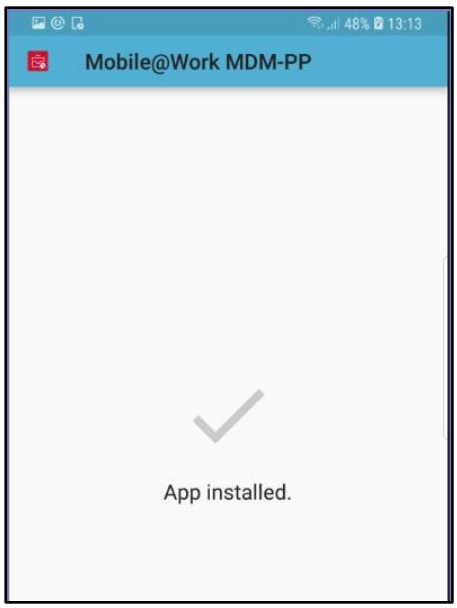
i Tap **Allow from this source**.

j A request is presented to install the app.



k Tap **Install** and follow further installation instructions.

l When the installation completes, the following screen displays.



Federal build is now installed and ready to use on the device.

Note: Ivanti recommends that the device user disables **Unknown sources** in the device's settings if it is still enabled. This setting prohibits app installation from unknown sources such as a web site or SD card. You can also apply a lockdown policy that selects **Disable** for the **Unknown sources** option.

8.3.3 Updating the MDM Agent Software

1. The Android User will be notified by the EPMM Server Administrator upon notification from Ivanti on an upgrade of the MDM Agent software.
2. If the Android User confirms an upgrade is required, the following commands are issued.
3. adb install <apk file>
4. The success or failure of the command will be displayed on the console. The upgrade is successfully performed only if the digital signature of the new build matches the digital signature of the current build.

8.4 SELF-TESTS

The self-test are initiated during initial power-up of the TOE as well as whenever the administrator issues a reboot for the MDM Server.

The MDM Server component of the TOE relies on both the Operational Environment and the TOE to perform self-tests. The MDM Server uses the Operational Environment's RPM Package Manager (RPM) functions of the TOE to verify the integrity of its own executable files. Additionally, the MDM Server's FIPS certified cryptographic modules (Ivanti MDM Bouncy Castle and Ivanti MDM OpenSSL Component) include self-tests to ensure the available cryptographic operations are performing correctly when starting up. Any errors are reported on the VMWare ESXi console and the MDM Server will attempt to restart if an error is detected without intervention by an Administrator.

At system start-up, the MDM Server uses the Operational Environment's RPM Package Manager (RPM) functions of the TOE to verify the integrity of its own executable files. The RPM Package Manager maintains a database of all installed RPMs, including the TSF, and during boot each RPM is checked for integrity with the standard Linux (Oracle) RPM integrity checking functions. Any errors are reported on the console and the MDM Server will attempt to restart if an error is detected without intervention by an Administrator. This RPM integrity test is sufficient to guarantee the integrity of the stored TOE executable code has not been compromised.

Once the RPM integrity tests pass and the system has entered into the operational state, the TSF performs self-tests on all approved cryptographic algorithms. This includes both the Ivanti MDM Bouncy Castle crypto library and the Ivanti MDM OpenSSL Component crypto library. The tests run, include but are not limited to, the algorithms identified in Table 27: CAVP Algorithm Certificate References of the Security Target. During these tests, services are not available, and data output is inhibited during the conditional self-tests. If any of these tests fail, the system transitions to the Error State. Specifically, the tests run by each cryptographic library are:

- Known Answer Tests – These tests verify the correct operation of cryptographic algorithms before they can be used in FIPS mode. They execute predefined tests vectors and compare outputs against known correct values.
- Power-on Self-Test (POST) – This test runs automatically when and ensures that the crypto library is ready for FIPS compliance.
- Hash Function Self-tests – These tests support multiple SHA variants using a unified testing framework.
- Algorithm Size Calculation Functions – Each algorithm implements size calculation functions to determine memory requirements. These tests help ensure that the algorithms function correctly and are not susceptible to attacks.

If any of these tests fail, an error message with be displayed on the console, the system will transition to the Error State, and halts processing. If this occurs, the Administrator should contact Ivanti support at https://forums.ivanti.com/s/contactsupport?language=en_US. Otherwise, if the tests are successful, the system transitions into the operational state.

9 COMPLIANCE

When a mobile device checks in, the mobile device performs a compliance check based on configured policies.

9.1 CONFIGURING THE SECURITY POLICY

Prerequisites:

The Product(s) must be configured in the Common Criteria evaluated configuration.

Procedure:

1. From the **Admin Portal**, go to **Policies & Configs > Policies.**
2. The policies will be displayed. Find the row for the currently installed **Secure Policy** or the **Default Security Policy**.

3. Select the security policy you want to modify.
4. Select the **Edit** button in the upper right corner of the pop-up window. The details of the policy will be displayed.

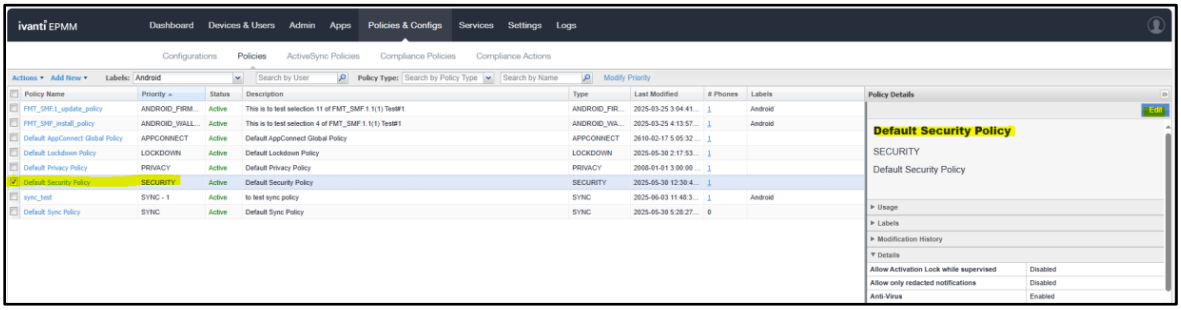


Figure 65: Policies Page

5. Scroll down to the **Access Control** section.
6. Under **For Android devices**, select the checkbox **for when Android version is less than**.
7. On the same line in the dropdown list, select **Send Alert**.
8. On the same line, in the dropdown list for Android OS versions, select the appropriate OS version.

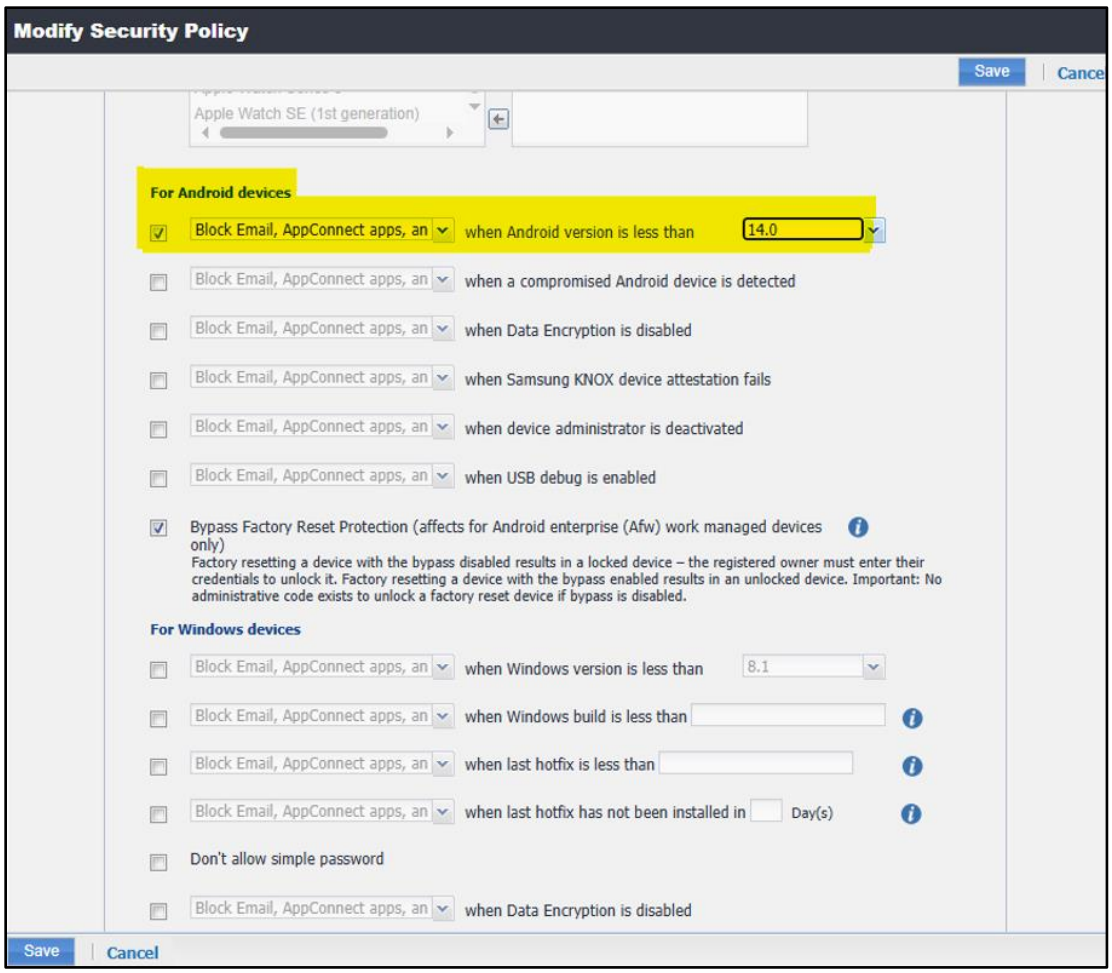


Figure 66: Security Policy modify window

9. Select **Save**.
10. Select **OK**
11. Confirm that the security policy is applied to a label that is also applied to the target devices.
    a. Select the security policy.
    b. Click **Actions > Apply To Label**.
    c. If necessary, select the appropriate labels and click **Apply**.

9.2 Configuring an Android OS version alert

To trigger an alert when a device is using a disallowed Android operating system:

Procedure:

1. Using the **Admin Portal**, navigate to **Logs > Event Settings**.

2. Select **Add New > Policy Violations Event**.
3. Enter a name for the event.
4. In the **Security Policy Triggers** section, under the **Android** heading, confirm that the app control alert **Disallowed Android OS version** found is selected.
5. Deselect all the other checkboxes.
6. In the **Apply to Labels** section, select the appropriate labels in the **Available** column, and click the right arrow to move them to the **selected** column.
7. Click **Save**.



When creating a policy violations event, you can choose to alert an administrator with an email. For EPMM to send this email, configure the email settings in the System Manager at **Settings > Email Settings**.

9.3 Defining a Custom Compliance Action

To define custom compliance actions for your devices:

Procedure:

1. Using the **Admin Portal**, navigate to **Policies & Configs > Compliance Actions**.
2. Click **Add+** to open the **Add Compliance Action** dialog.
3. Enter a name for the compliance action.
4. Select **Enforce Compliance Actions Locally on Devices**.
5. In the **Alert** section, select **Send a compliance notification or alert to the user**.
6. In the **Block Access** section, **select Block email access and AppConnect apps**.
7. In the **Quarantine** section, select **Quarantine the device**.
8. Select **Remove All Configurations**.
9. Click **Save**.

9.4 Configuring Compliance Parameters

Procedure:

1. In Admin Portal, go to **Policies & Configs > Policies**.

2. Select the security policy you want to work with.
3. Click **Edit**.
4. Scroll down to the **Access Control** section of the **Modifying Security Policy** dialog.
5. Under **For Android devices**, select the checkbox for **when Android version is less than**.
6. On the same line, in the dropdown list, select the custom compliance action that you just created.
7. On the same line, in the dropdown list for Android OS versions, select the appropriate OS version.

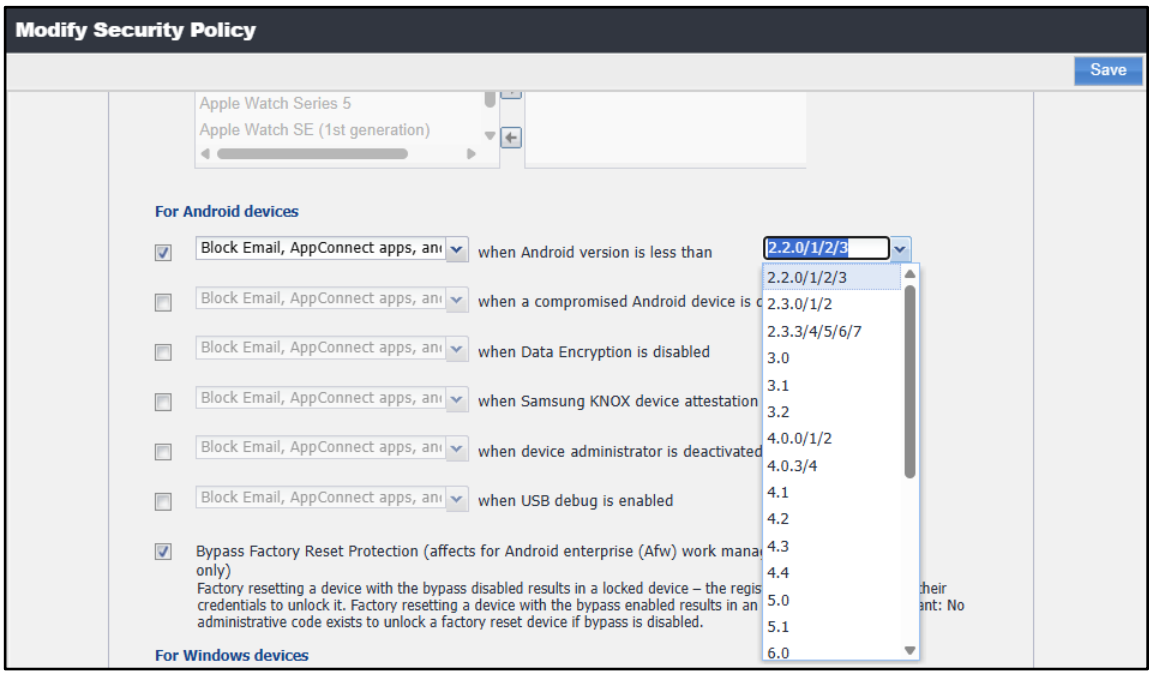


Figure 67: Android version check

8. Click **Save**.
9. Click **OK**.
10. Confirm that the security policy is applied to a label that is also applied to the target devices.
    a. Select the security policy.
    b. Click **Actions > Apply To Label**.
    c. If necessary, select the appropriate labels and click **Apply**.

10 EPMM System Logs and Events Management

10.1 Auditable Events

The TOE creates audit logs for specific events related to the Protection Profile for Mobile Device Management, Version 4.0, 25 April 2019 [PP_MDM_V4.0] requirements and PP-Module for MDM Agents, Version 1.0, 25 April 2019 [MOD_MDM_AGENT_V1.0].
The Audit Logs page displays the information that Ivanti EPMM records for the EPMM instance. Filters and the search functions can be used for finding specific information.

10.2 Viewing Auditable Events on EPMM server

Procedure:

1. Using the **Admin Portal**, navigate to **Logs > Audit Logs**. EPMM displays the Audit Logs page.

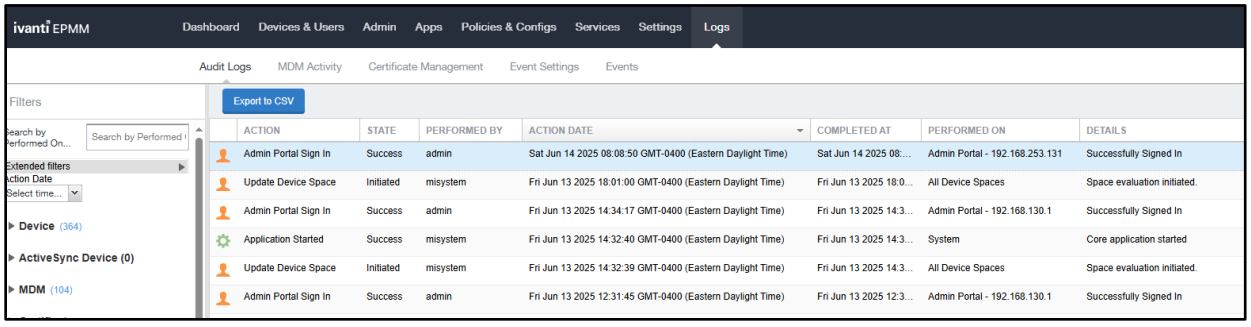


Figure 68: Audit logs

The information panel displays:

- **ACTION** – a short description of the event.
- **STATE** – success or failure.
- **PERFORMED BY** – login of person who caused the event.
- **ACTION DATE** – date the event was started. Specifically, day of week | month | day | year | time zone.
- **COMPLETED AT** – date the event occurred. Specifically, day of week | month | day | year | time | time zone.
- **PERFORMED ON** – the system on which the event occurred on.
- **DETAILS** – displays the outcome of the event

10.3 Configuring Audit Events on Android Devices

The operational guidance ensures that specific audit records are consistently recorded, irrespective of the selection criteria currently enforced. The MDM Agent stores the majority of audit records in the mobile device's audit log, utilizing the device's selection capabilities to filter audited events based on the following attributes: event type, success of auditable security events, and failure of

auditable security events within the operational environment.

The following audit events, available through the Samsung General Policy, are recorded in the mobile device audit log and subject to the device's selection criteria:

i. CA certificate import
ii. CA certificate removal
iii. Request current software version
iv. Request current hardware version
v. Report app inventory
vi. Upload logs
vii. Enable/Disable camera
viii. Enable/Disable microphone

The other auditable events included in the list that are considered security relevant and therefore not subject to the selection criteria are:

i. Audit configuration change
ii. TLS session failure
iii. Transition to locked state
iv. Enrollment in management
v. Unenrollment from management
vi. Policy validation failure
vii. ID certificate import
viii. ID certificate removal
ix. Install application
x. Remove application
xi. Device OS upgrade
xii. Server request client check-in
xiii. Configure App Store quarantine compliance action

In addition to the above-mentioned events, other events such as policy signature-related audits and agent alerts are not stored in the platform audit log. These events are always audited, meaning they cannot be deselected, and are stored locally by the MDM Agent in its dedicated data space until they are successfully delivered to the MDM Server.

The Samsung General Policy provides audit collection control settings. These settings control what audit events are logged to the device logs on Samsung devices based on an event's severity, outcome, and audit group.
These settings impact logs collected on the Samsung device: logs made by the Samsung platform, as well as logs made by Ivanti Mobile@Work.
The device logs are pulled to Ivanti EPMM, and then can be accessed using the System Manager.

Prerequisites:

The Product(s) must be configured in the Common Criteria evaluated configuration.

Procedure:

1. Using the **Admin Portal**, navigate **Policies & Configs > Policies.**

2. Click on **Add New > Android.**

3. Select **Samsung General** from the Android option.

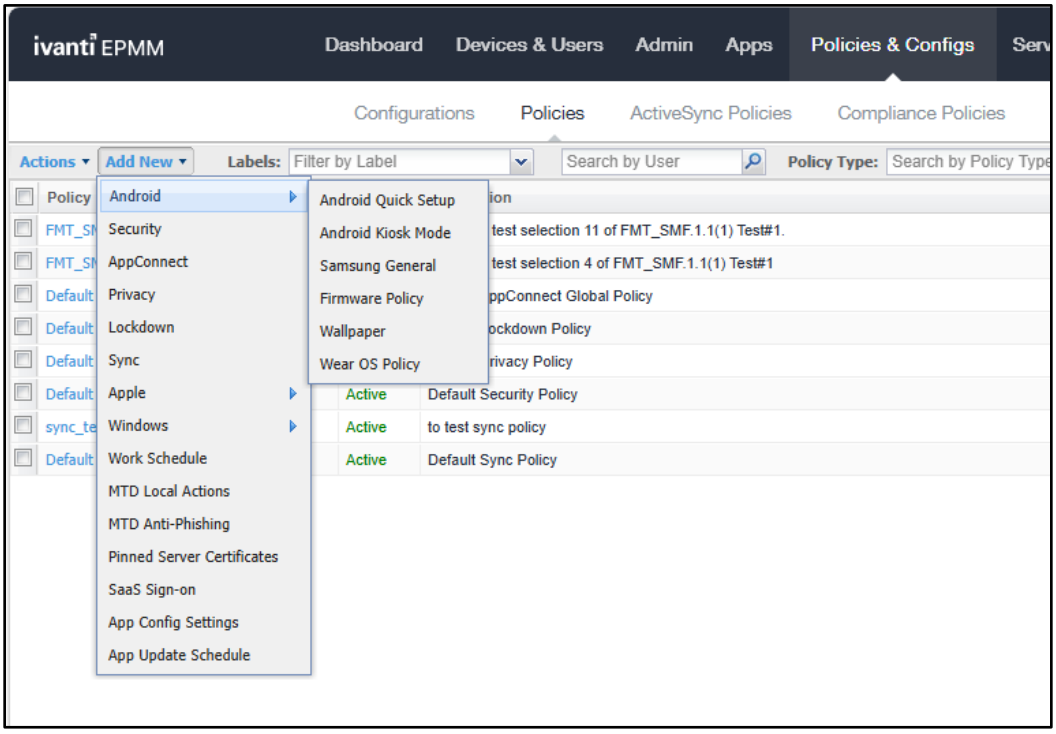


Figure 69: Samsung General Policy70

4. The Samsung General Policy will be displayed.

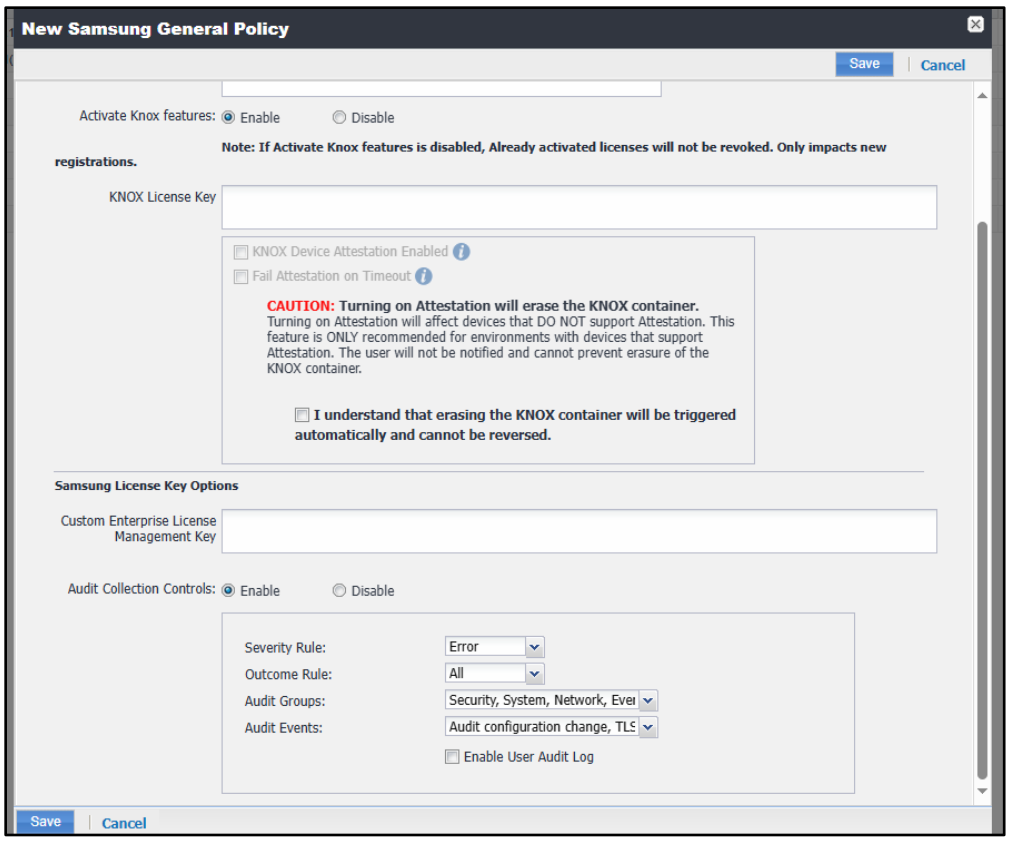


Figure 71: Samsung general policy configuration

5. Select **Audit Collection Controls** as **Enable**

6. For **adb**, select the severity level of events you want to collect. Only audit events of the chosen severity level or higher will be collected.

   For example, if you select Error, only Error, Critical, and Alert audit events will be collected. The severity levels are, from most severe to least severe, are:
   - Alert
   - Critical
   - Error (the default)
   - Warning
   - Notice
   - Debug
   - Information

   *The CC evaluated configuration requires **Error** or lower.*

7. **Outcome Rule** determines what events to collect based on the action's outcome. For example, only events indicating success, events indicating failure, or all.
   *The CC evaluated configuration requires the setting to be **All**.*

8. **Audit Groups** determines what events or event groups to collect based on the type of event. Select one or more **Security, System, Network, Events,** and **Applications**.

9. **Audit Events** determine what sort of events must be considered for auditing (recording logs). The events selected here are considered as auditable events.

   *The CC evaluated configuration requires **all items mentioned below:***

   i. Audit configuration change
   ii. TLS session failure
   iii. Transition to locked state
   iv. Enrollment in management
   v. Unenrollment from management
   vi. Policy validation failure
   vii. CA certificate import
   viii. ID certificate import
   ix. CA certificate remove
   x. ID certificate remove
   xi. Install application
   xii. Remove application
   xiii. Device OS upgrade
   xiv. Server request client checkin
   xv. Request current software version
   xvi. Request current hardware version
   xvii. Report app inventory
   xviii. Upload logs
   xix. Configure App Store quarantine compliance action
   xx. Enable/Disable camera
   xxi. Enable/Disable mic

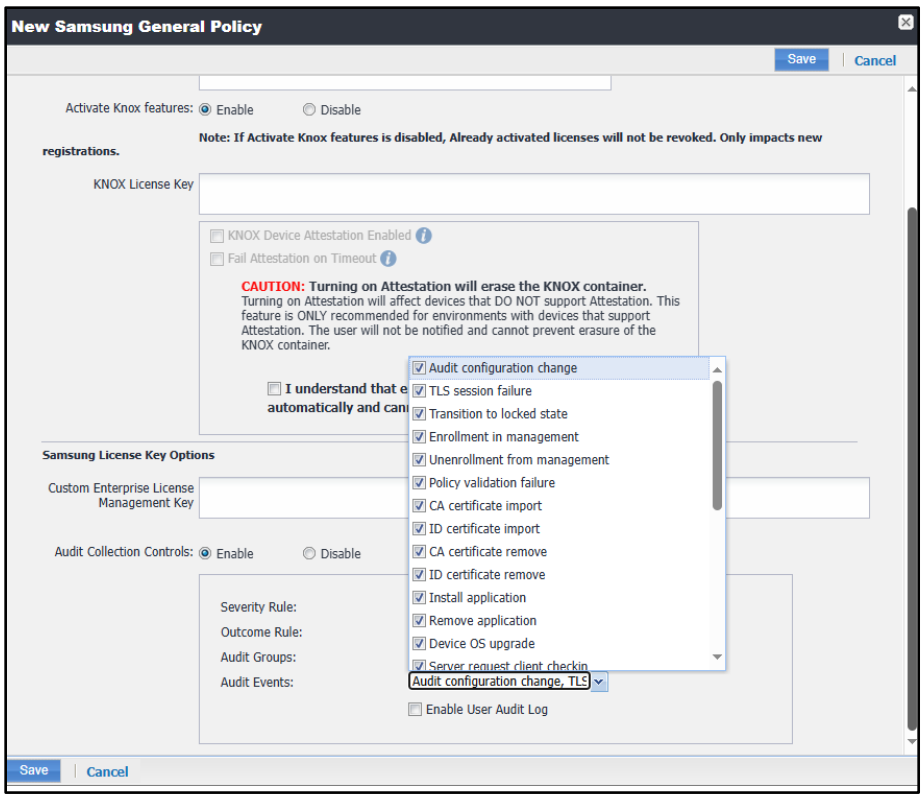


Figure 72: Audit Events configuration

10. Select **Save.**

10.4 Pulling Android Device Logs

When the Pull client logs command is delivered to the device, it instructs the Ivanti Agent client to collect logs running on the device. This may include logs from all the secure apps running on the device. These logs are pulled to the server's file storage.

The device logs include log.txt file and the dump.gz file.

Note: The Pull client log command is not available to delegated administrators; only administrators who have the Manage Devices role can use this feature.

Prerequisites:

- The Product(s) must be configured in the Common Criteria evaluated configuration.
- A SAMSUNG GENERAL Policy has been applied to the device.

Procedure:

1. Using the **Admin Portal**, navigate to **Devices & Users > Devices**.
2. Select the check box next to the device from which the logs are to be pulled.
3. Select the device **Actions** option on the left. The Actions pull-down menu will be displayed.

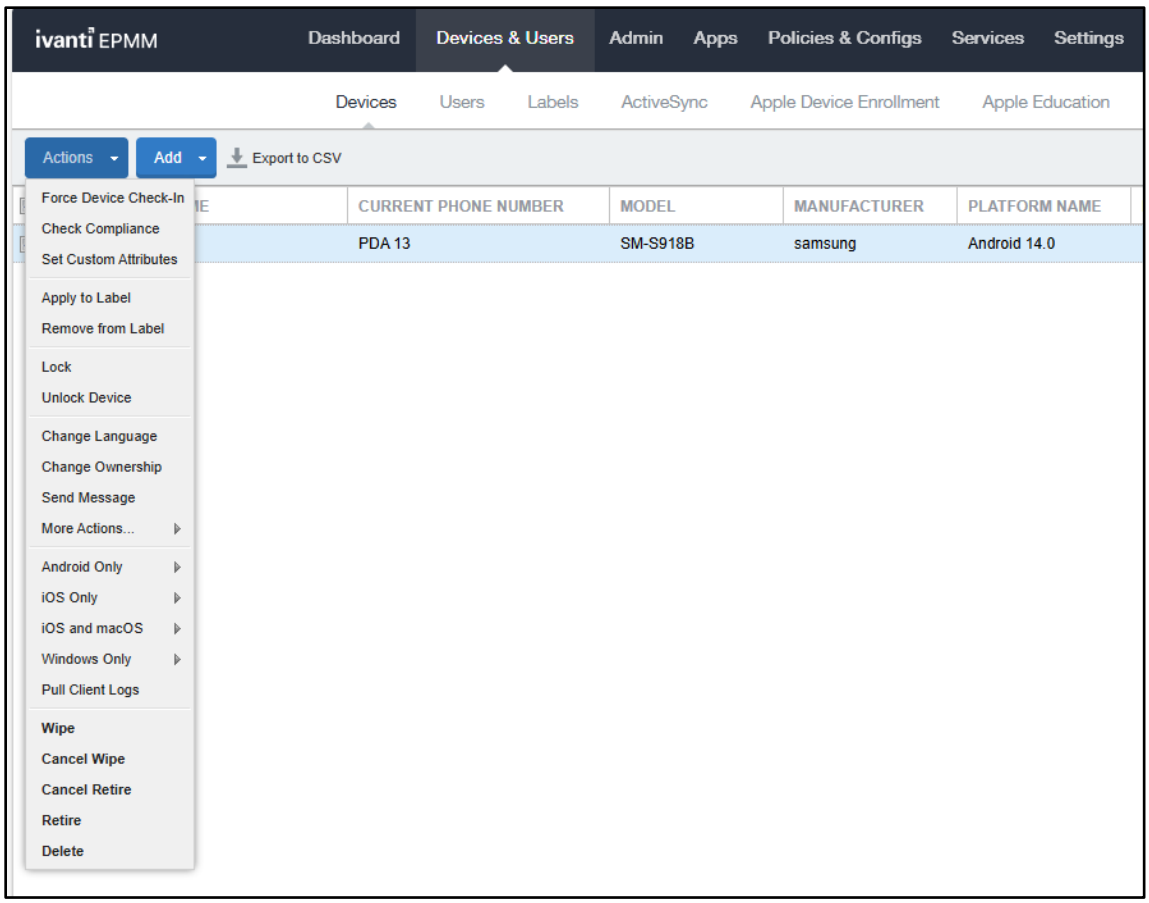


Figure 73: Device selection for pulling logs

4. Select the Pull Client Logs option. The Pull Client Logs dialog box displays. The Devices field displays the name of the device that you selected.

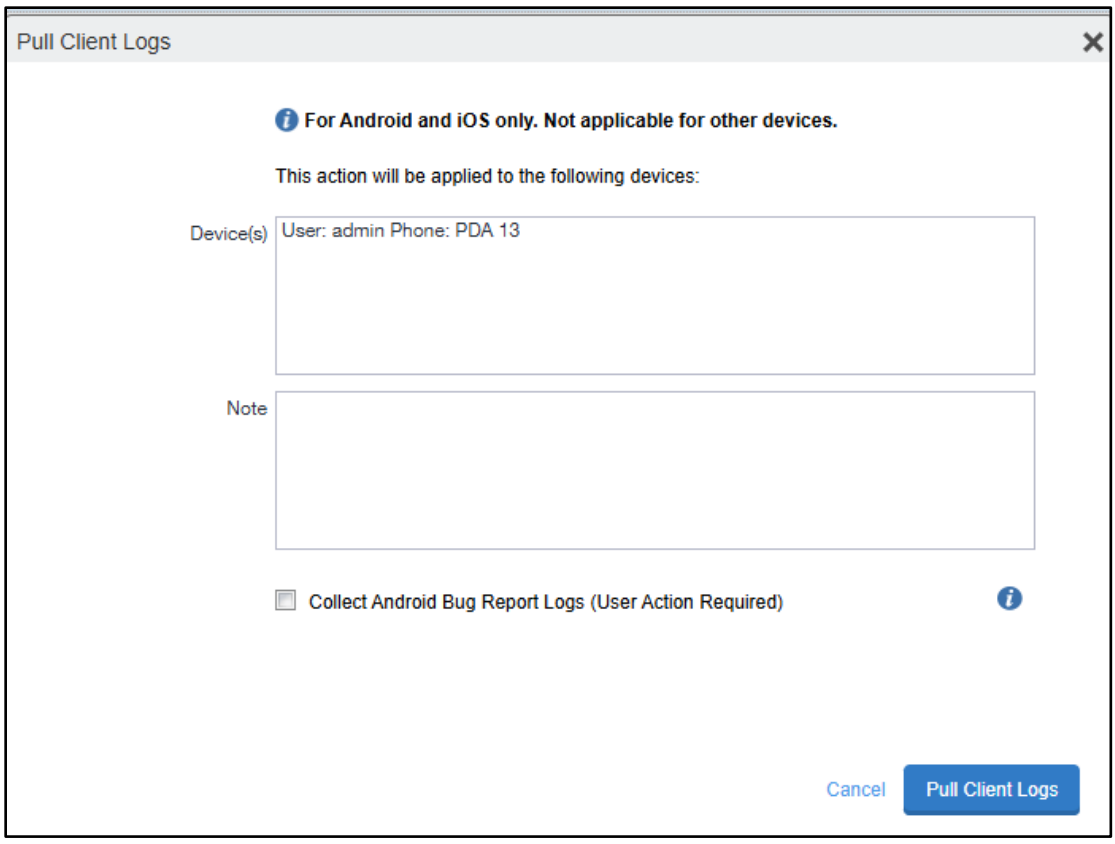


Figure 74: Pull client logs

5. (Optional) Add notes about this action in the Notes section.
6. (Optional) Checkbox for Collect Android Bug Report Logs
    a. Select the checkbox for client logs along with android bug report to be requested from Mobile at Work.
    b. Deselect the checkbox for silent logs to be requested from Mobile at Work. The android bug report is excluded in this request.
7. Click the **Pull Client Logs** button to launch this request to the server.

10.5 Exporting Android Device Audit Records

The System Manager interface is used to pull device logs from agents and to export System Manager audit logs. Use the following instructions to obtain an archive file containing the audit logs and device logs.

Procedure:

1. Using the **Ivanti EPMM System Manager**, navigate to the **Troubleshooting** tab.
2. Scroll down to section **Export Logs**.
3. Select the log to download (Module) as **Show Tech (All Logs).**

4. Select a database option.

   Show tech logs can include database information that some companies consider too sensitive to send to Customer Support. Therefore, the Database Options can be used to specify whether to include data and whether to remove potentially sensitive information from the output.

   The following options are available:

   i. **Sanitize**: Remove sensitive information. This is the default selection. If the Sanitize option is selected, the following data is removed:

      a. email addresses
      b. device tokens
      c. unlock tokens
      d. phone numbers
      e. last locations
      f. unsent alerts
      g. events

   ii. **Standard**: Sensitive information included.

   iii. **No Database**: All database information omitted.

5. Select **SFTP Upload, HTTPS Upload** or **Download** from the **Type** drop-down list, depending on the method you want to use.

   Note: For Self-service user portal (SSP) log files, Download is the only supported Export option.

   If SFTP Upload or HTTPS Upload is selected, select the Alternate Location check box and configure a backup location or user authentication in case transmission to the primary server or user fails.

   The following additional fields for the alternate location are displayed:

   - Host/IP or URL (e.g., https://support.ivanti.com)
   - User Name
   - Password
   - Confirm Password

6. Click **SFTP Upload, HTTPS Upload** or **Download**.

   Note: *For CC evaluated configurations, the **Download** method is selected.*

7. Click the **Export (Download)** button.

   EPMM downloads an archive file (tgz file) containing the following files:

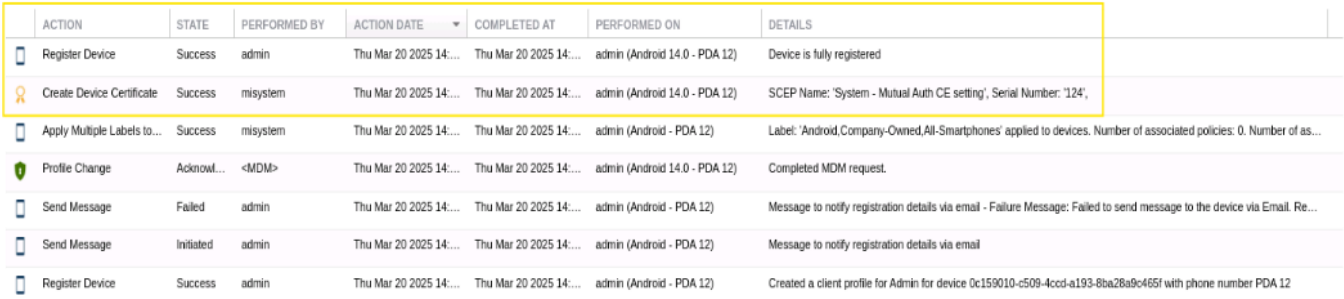
   - MICS.log
   - MIFS.log
   - Application.log
   - /var/log/httpd/https-error_log

- /var/log/httpd/portal_error_log
- /var/log/secure
- upgrade.log.

11 EPMM System Audit Record Examples

The following table provides examples of the audit records that are relevant to this common criteria evaluation.

Table 7: Auditable events for MDM server

<table>
<tr><th>Requirement</th><th>Auditable Events</th><th>Additional Audit Record Contents</th></tr>
<tr><td>FAU_ALT_EXT.1</td><td>Type of alert.</td><td>Identity of Mobile Device that sent</td></tr>
<tr><td colspan="3">

<table>
<tr><th>ACTION</th><th>STATE</th><th>PERFORMED BY</th><th>ACTION DATE</th><th>COMPLETED AT</th><th>PERFORMED ON</th><th>DETAILS</th></tr>
<tr><td>Register Device</td><td>Success</td><td>admin</td><td>Thu Mar 20 2025 14:...</td><td>Thu Mar 20 2025 14:...</td><td>admin (Android 14.0 - PDA 12)</td><td>Device is fully registered</td></tr>
<tr><td>Create Device Certificate</td><td>Success</td><td>misystem</td><td>Thu Mar 20 2025 14:...</td><td>Thu Mar 20 2025 14:...</td><td>admin (Android 14.0 - PDA 12)</td><td>SCEP Name: 'System - Mutual Auth CE setting', Serial Number: '124',</td></tr>
<tr><td>Apply Multiple Labels to...</td><td>Success</td><td>misystem</td><td>Thu Mar 20 2025 14:...</td><td>Thu Mar 20 2025 14:...</td><td>admin (Android - PDA 12)</td><td>Label: 'Android,Company-Owned,All-Smartphones' applied to devices. Number of associated policies: 0. Number of as...</td></tr>
<tr><td>Profile Change</td><td>Acknowl...</td><td><MDM></td><td>Thu Mar 20 2025 14:...</td><td>Thu Mar 20 2025 14:...</td><td>admin (Android 14.0 - PDA 12)</td><td>Completed MDM request.</td></tr>
<tr><td>Send Message</td><td>Failed</td><td>admin</td><td>Thu Mar 20 2025 14:...</td><td>Thu Mar 20 2025 14:...</td><td>admin (Android - PDA 12)</td><td>Message to notify registration details via email - Failure Message: Failed to send message to the device via Email. Re...</td></tr>
<tr><td>Send Message</td><td>Initiated</td><td>admin</td><td>Thu Mar 20 2025 14:...</td><td>Thu Mar 20 2025 14:...</td><td>admin (Android - PDA 12)</td><td>Message to notify registration details via email</td></tr>
<tr><td>Register Device</td><td>Success</td><td>admin</td><td>Thu Mar 20 2025 14:...</td><td>Thu Mar 20 2025 14:...</td><td>admin (Android - PDA 12)</td><td>Created a client profile for Admin for device 0c159010-c509-4ccd-a193-8ba28a9c465f with phone number PDA 12</td></tr>
</table>
Note: In the mentioned snippet “Action” refers to the type of alert and “Performed On” refers to Identity of the mobile device.
</td></tr>
<tr><td>FCO_CPC_EXT.1</td><td>Enabling or disabling communications between a pair of components</td><td>Identities of the endpoints pairs enabled or disabled.</td></tr>
</table>

Requirement	Auditable Events	Additional Audit Record Contents
Enabling communications: [Mon Jul 28 15:13:30.452554 2025] [ssl:info] [pid 108308] [client 192.168.128.39:52040] AH01964: Connection to child 5 established (server acumensec.domain.local:443) [Mon Jul 28 15:13:30.452677 2025] [ssl:trace2] [pid 108308] ssl_engine_rand.c(126): Server: Seeding PRNG with 144 bytes of entropy [Mon Jul 28 15:13:30.452758 2025] [ssl:trace3] [pid 108308] ssl_engine_kernel.c(2213): [client 192.168.128.39:52040] OpenSSL: Handshake: start [Mon Jul 28 15:13:30.452780 2025] [ssl:trace3] [pid 108308] ssl_engine_kernel.c(2222): [client 192.168.128.39:52040] OpenSSL: Loop: before SSL initialization [Mon Jul 28 15:13:30.541350 2025] [ssl:trace3] [pid 108308] ssl_engine_kernel.c(2217): [client 192.168.128.39:52040] OpenSSL: Handshake: done [Mon Jul 28 15:13:30.541364 2025] [ssl:debug] [pid 108308] ssl_engine_kernel.c(2266): [client 192.168.128.39:52040] AH02041: Protocol: TLSv1.2, Cipher: AES256-GCM-SHA384 (256/256 bits) [Mon Jul 28 15:13:30.541372 2025] [authz_core:debug] [pid 108308] mod_authz_core.c(846): [client 192.168.128.39:52040] AH01628: authorization result: granted (no directives) **Disabling communication:** [Mon Jul 28 15:39:04.278087 2025] [core:trace8] [pid 121385] core_filters.c(575): [client 192.168.128.39:50370] brigade contains: bytes: 0, non-file bytes: 0, eor buckets: 0, morphing buckets: 0 [Mon Jul 28 15:39:04.278091 2025] [ssl:debug] [pid 121385] ssl_engine_io.c(1112): [client 192.168.128.39:50370] AH02001: Connection closed to child 6 with standard shutdown (server acumensec.domain.local:7443) [Mon Jul 28 15:39:04.278130 2025] [core:trace8] [pid 121385] core_filters.c(575): [client 192.168.128.39:50370] brigade contains: bytes: 0, non-file bytes: 0, eor buckets: 0, morphing buckets: 0		
FCS_HTTPS_EXT.1	Failure of the certificate validity check.	Issuer Name and Subject Name of certificate.
2025-03-17 19:20:47,214 DEBUG [CertificateUtils.openCertificate:1423] (http-nio-127.0.0.1-9081-exec-3:[]) Trying PKCS12... match found. 2025-03-17 19:20:47,215 INFO [ApplicationLoggingHelper.log:94] (http-nio-127.0.0.1-9081-exec-3:[]) Certificate Expired. Subject: EMAILADDRESS=info@acumen.net, CN=acumencertdomain.net, OU=CC, O=Acumen, L=Rockville, ST=MD, C=US Serial Number: 3733470652126645570 Issuer: CN=Acumen_ICA, OU=CC, O=Acumen, L=Rockville, ST=MD, C=US Not After: Fri Feb 28 17:14:00 UTC 2025 2025-03-17 19:20:47,216 WARN [MICSController.handleUploadCertificate:4101] (http-nio-127.0.0.1-9081-exec-3:[]) Failed to upload certificate(s). Reason: Certificate with subject 'EMAILADDRESS=info@acumen.net, CN=acumencertdomain.net, OU=CC, O=Acumen, L=Rockville, ST=MD, C=US' expired on 2/28/25 5:14 PM		
FCS_RBG_EXT.1/SRV	Failure of the randomization process.	No additional information.
2025-10-07 07:00:47,958 INFO [ApplicationLoggingHelper.log:82] (http-nio-127.0.0.1-9081-exec-10:[]) SecureRandom.nextBytes failed to generate random data, retry_count 1		
FCS_TLSC_EXT.1	Failure to establish a TLS session.	Reason for failure.
	Failure to verify presented identifier.	Presented identifier and reference identifier.

Without EKU:

2025-07-10T00:21:35.638004+00:00 acumencertdomain rsyslogd: nsd_ossl: TLS Connection initiated with remote syslog server. [v8.2102.0-15.el8]

2025-07-10T00:21:35.640704+00:00 acumencertdomain rsyslogd: Certificate error at depth: 0 issuer = /C=US/ST=MD/L=Rockville/O=Acumen/OU=CC/CN=intermediate/emailAddress=info@acumen.net subject = /C=US/ST=MD/L=Rockville/O=Acumen/OU=CC/CN=pssyslog.acumensec.local/emailAddress=info@acumen.net err 26:unsupported certificate purpose [v8.2102.0-15.el8]

2025-07-10T00:21:35.640731+00:00 acumencertdomain rsyslogd: SSL_ERROR_SSL Error in 'osslHandshakeCheck Client': 'error:00000001:lib(0):func(0):reason(1)(1)' with ret=-1 [v8.2102.0-15.el8]

2025-07-10T00:21:35.640735+00:00 acumencertdomain rsyslogd: nsd_ossl:OpenSSL Error Stack: error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed [v8.2102.0-15.el8]

2025-07-10T00:21:35.640738+00:00 acumencertdomain rsyslogd: nsd_ossl:TLS session terminated with remote syslog server. [v8.2102.0-15.el8]

Unsupported Server Certificate:

2025-06-18T16:16:20.136895+00:00 acumencertdomain rsyslogd: nsd_ossl: TLS Connection initiated with remote syslog server. [v8.2102.0-15.el8]

2025-06-18T16:16:20.148556+00:00 acumencertdomain rsyslogd: Certificate error at depth: 2 issuer = /C=US/ST=MD/L=Rockville/O=Acumen/OU=CC/CN=ec_root/emailAddress=info@acumen.net subject = /C=US/ST=MD/L=Rockville/O=Acumen/OU=CC/CN=ec_root/emailAddress=info@acumen.net err 19:self signed certificate in certificate chain [v8.2102.0-15.el8]

2025-06-18T16:16:20.148611+00:00 acumencertdomain rsyslogd: SSL_ERROR_SSL Error in 'osslHandshakeCheck Client': 'error:00000001:lib(0):func(0):reason(1)(1)' with ret=-1 [v8.2102.0-15.el8]

2025-06-18T16:16:20.148615+00:00 acumencertdomain rsyslogd: nsd_ossl:OpenSSL Error Stack: error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed [v8.2102.0-15.el8]

2025-06-18T16:16:20.148618+00:00 acumencertdomain rsyslogd: nsd_ossl:TLS session terminated with remote syslog server. [v8.2102.0-15.el8]

NULL Cipher:

2025-06-06T15:11:49.683860+00:00 acumencertdomain rsyslogd: nsd_ossl: TLS Connection initiated with remote syslog server. [v8.2102.0-15.el8]

2025-06-06T15:11:49.781128+00:00 acumencertdomain rsyslogd: SSL_ERROR_SSL Error in 'osslHandshakeCheck Client': 'error:00000001:lib(0):func(0):reason(1)(1)' with ret=-1 [v8.2102.0-15.el8]

2025-06-06T15:11:49.781135+00:00 acumencertdomain rsyslogd: nsd_ossl:OpenSSL Error Stack: error:1421C0F8:SSL routines:set_client_ciphersuite:unknown cipher returned [v8.2102.0-15.el8]

2025-06-06T15:11:49.781138+00:00 acumencertdomain rsyslogd: nsd_ossl:TLS session terminated with remote syslog server. [v8.2102.0-15.el8]

Undefined TLS version:

2025-06-09T16:25:52.149896+00:00 acumencertdomain rsyslogd: nsd_ossl: TLS Connection initiated with remote syslog server. [v8.2102.0-15.el8]

2025-06-09T16:25:52.244758+00:00 acumencertdomain rsyslogd: SSL_ERROR_SSL Error in 'osslHandshakeCheck Client': 'error:00000001:lib(0):func(0):reason(1)(1)' with ret=-1 [v8.2102.0-15.el8]

2025-06-09T16:25:52.244763+00:00 acumencertdomain rsyslogd: nsd_ossl:OpenSSL Error Stack: error:1425F102:SSL routines:ssl_choose_client_version:unsupported protocol [v8.2102.0-15.el8]

2025-06-09T16:25:52.244765+00:00 acumencertdomain rsyslogd: nsd_ossl:TLS session terminated with remote syslog server. [v8.2102.0-15.el8]

Unsupported TLS version:

```
2025-06-06T15:26:50.423799+00:00 acumencertdomain rsyslogd:  nsd_ossl: TLS Connection initiated with remote syslog server. [v8.2102.0-15.el8]
2025-06-06T15:26:50.519809+00:00 acumencertdomain rsyslogd:  SSL_ERROR_SSL Error in 'osslHandshakeCheck Client': 'error:00000001:lib(0):func(0):reason(1)(1)' with ret=-1  [v8.2102.0-15.el8]
2025-06-06T15:26:50.519815+00:00 acumencertdomain rsyslogd:  nsd_ossl:OpenSSL Error Stack: error:1425F102:SSL routines:ssl_choose_client_version:unsupported protocol [v8.2102.0-15.el8]
2025-06-06T15:26:50.519818+00:00 acumencertdomain rsyslogd:  nsd_ossl:TLS session terminated with remote syslog server. [v8.2102.0-15.el8]
```

Modified Server Nonce:

```
2025-06-09T16:13:51.526122+00:00 acumencertdomain rsyslogd:  nsd_ossl: TLS Connection initiated with remote syslog server. [v8.2102.0-15.el8]
2025-06-09T16:13:51.626161+00:00 acumencertdomain rsyslogd:  SSL_ERROR_SSL Error in 'osslHandshakeCheck Client': 'error:00000001:lib(0):func(0):reason(1)(1)' with ret=-1  [v8.2102.0-15.el8]
2025-06-09T16:13:51.626188+00:00 acumencertdomain rsyslogd:  nsd_ossl:OpenSSL Error Stack: error:04091068:rsa routines:int_rsa_verify:bad signature [v8.2102.0-15.el8]
2025-06-09T16:13:51.626192+00:00 acumencertdomain rsyslogd:  nsd_ossl:OpenSSL Error Stack: error:1416D07B:SSL routines:tls_process_key_exchange:bad signature [v8.2102.0-15.el8]
2025-06-09T16:13:51.626195+00:00 acumencertdomain rsyslogd:  nsd_ossl:TLS session terminated with remote syslog server. [v8.2102.0-15.el8]
```

Unsupported Cipher suite:

```
2025-06-06T15:50:21.537625+00:00 acumencertdomain rsyslogd:  nsd_ossl: TLS Connection initiated with remote syslog server. [v8.2102.0-15.el8]
2025-06-06T15:50:21.629680+00:00 acumencertdomain rsyslogd:  SSL_ERROR_SSL Error in 'osslHandshakeCheck Client': 'error:00000001:lib(0):func(0):reason(1)(1)' with ret=-1  [v8.2102.0-15.el8]
2025-06-06T15:50:21.629690+00:00 acumencertdomain rsyslogd:  nsd_ossl:OpenSSL Error Stack: error:1421C105:SSL routines:set_client_ciphersuite:wrong cipher returned [v8.2102.0-15.el8]
2025-06-06T15:50:21.629693+00:00 acumencertdomain rsyslogd:  nsd_ossl:TLS session terminated with remote syslog server. [v8.2102.0-15.el8]
```

Modified Server Key Exchange:

```
2025-06-09T16:51:33.490127+00:00 acumencertdomain rsyslogd:  SSL_ERROR_SSL Error in 'osslHandshakeCheck Client': 'error:00000001:lib(0):func(0):reason(1)(1)' with ret=-1 [v8.2102.0-15.el8]
2025-06-09T16:51:33.490137+00:00 acumencertdomain rsyslogd:  nsd_ossl:OpenSSL Error Stack: error:0407008A:rsa routines:RSA_padding_check_PKCS1_type_1:invalid padding [v8.2102.0-15.el8]
2025-06-09T16:51:33.490141+00:00 acumencertdomain rsyslogd:  nsd_ossl:OpenSSL Error Stack: error:04067072:rsa routines:rsa_ossl_public_decrypt:padding check failed [v8.2102.0-15.el8]
2025-06-09T16:51:33.490144+00:00 acumencertdomain rsyslogd:  nsd_ossl:OpenSSL Error Stack: error:1416D07B:SSL routines:tls_process_key_exchange:bad signature [v8.2102.0-15.el8]
2025-06-09T16:51:33.490147+00:00 acumencertdomain rsyslogd:  nsd_ossl:TLS session terminated with remote syslog server. [v8.2102.0-15.el8]
```

Modified Server Finish:

```
2025-06-06T16:37:03.026049+00:00 acumencertdomain rsyslogd:  nsd_ossl: TLS Connection initiated with remote syslog server. [v8.2102.0-15.el8]
2025-06-06T16:37:03.045543+00:00 acumencertdomain rsyslogd:  SSL_ERROR_SSL Error in 'osslHandshakeCheck Client': 'error:00000001:lib(0):func(0):reason(1)(1)' with ret=-1 [v8.2102.0-15.el8]
```

```
2025-06-06T16:37:03.045551+00:00 acumencertdomain rsyslogd:  nsd_ossl:OpenSSL Error Stack:
    error:1408F119:SSL routines:ssl3_get_record:decryption failed or bad record mac
    [v8.2102.0-15.el8]
    2025-06-06T16:37:03.045554+00:00 acumencertdomain rsyslogd:  nsd_ossl:TLS session
    terminated with remote syslog server. [v8.2102.0-15.el8
```

Random bytes after change cipher spec issued by server:

```
2025-06-06T16:45:29.702246+00:00 acumencertdomain rsyslogd:  nsd_ossl: TLS Connection
    initiated with remote syslog server. [v8.2102.0-15.el8]
2025-06-06T16:45:29.769976+00:00 acumencertdomain rsyslogd:  SSL_ERROR_SSL Error in
    'osslHandshakeCheck Client': 'error:00000001:lib(0):func(0):reason(1)(1)' with ret=-1
    [v8.2102.0-15.el8]
2025-06-06T16:45:29.769981+00:00 acumencertdomain rsyslogd:  nsd_ossl:OpenSSL Error Stack:
    error:1408F119:SSL routines:ssl3_get_record:decryption failed or bad record mac
    [v8.2102.0-15.el8]
    2025-06-06T16:45:29.769984+00:00 acumencertdomain rsyslogd:  nsd_ossl:TLS session
    terminated with remote syslog server. [v8.2102.0-15.el8]
    Invalid Certificate path:
    <Test is currently failing>
    Revoked Certificate:
    <Test is currently failing>
    Expired Certificate:
    2025-06-05T21:31:01.757921+00:00 acumencertdomain rsyslogd:  nsd_ossl: TLS Connection
    initiated with remote syslog server. [v8.2102.0-15.el8]
    2025-06-05T21:31:01.762895+00:00 acumencertdomain rsyslogd:  Certificate EXPIRED at
    depth: 0   issuer  =
    /C=US/ST=MD/L=Rockville/O=Acumen/OU=CC/CN=intermediate/emailAddress=info@acumen.net
    subject =
    /C=US/ST=MD/L=Rockville/O=Acumen/OU=CC/CN=pssyslog.acumensec.local/emailAddress=info@acum
    en.net  err 10:certificate has expired [v8.2102.0-15.el8]
    2025-06-05T21:31:01.762901+00:00 acumencertdomain rsyslogd:  SSL_ERROR_SSL Error in
    'osslHandshakeCheck Client': 'error:00000001:lib(0):func(0):reason(1)(1)' with ret=-1
    [v8.2102.0-15.el8]
    2025-06-05T21:31:01.762904+00:00 acumencertdomain rsyslogd:  nsd_ossl:OpenSSL Error
    Stack: error:1416F086:SSL routines:tls_process_server_certificate:certificate verify
    failed [v8.2102.0-15.el8]
    2025-06-05T21:31:01.762906+00:00 acumencertdomain rsyslogd:  nsd_ossl:TLS session
    terminated with remote syslog server. [v8.2102.0-15.el8]
```

Failure to verify presented identifier

```
2025-07-30 21:14:37,363 DEBUG [CertificateUtils.getCertificates:675] (http-nio-127.0.0.1-
9081-exec-6:[])  Acquiring certificates for TLS pssyslog.acumensec.local:6515
2025-07-30 21:14:37,366 DEBUG [CertificateUtils.getCertificates:695] (http-nio-127.0.0.1-
9081-exec-6:[])  configure cipher suites in TLS
socket=[TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384]
2025-07-30 21:14:37,371 DEBUG [CertificateUtils.getCertificates:722] (http-nio-127.0.0.1-
9081-exec-6:[])  pssyslog.acumensec.local:6515 Server sent 3 certificates
2025-07-30 21:14:37,372 DEBUG [CertificateUtils.sortCertificateChain:1168] (http-nio-
127.0.0.1-9081-exec-6:[])  *** Original Certificate List:
2025-07-30 21:14:37,372 DEBUG [CertificateUtils.sortCertificateChain:1170] (http-nio-
127.0.0.1-9081-exec-6:[])     cert:
1.2.840.113549.1.9.1=#160f696e666f406163756d656e2e6e6574,CN=pssyslog.*.acumensec.local,OU=CC,
O=Acumen,L=Rockville,ST=MD,C=US
2025-07-30 21:14:37,372 DEBUG [CertificateUtils.sortCertificateChain:1170] (http-nio-
127.0.0.1-9081-exec-6:[])     cert:
1.2.840.113549.1.9.1=#160f696e666f406163756d656e2e6e6574,CN=pssyslog_ICA,OU=CC,O=Acumen,L=Roc
kville,ST=MD,C=US
```

```
2025-07-30 21:14:37,372 DEBUG [CertificateUtils.sortCertificateChain:1170] (http-nio-
127.0.0.1-9081-exec-6:[])     cert:
1.2.840.113549.1.9.1=#160f696e666f406163756d656e2e6e6574,CN=pssyslog_CA,OU=CC,O=Acumen,L=Rock
ville,ST=MD,C=US
2025-07-30 21:14:37,384 DEBUG [CertificateUtils.sortCertificateChain:1196] (http-nio-
127.0.0.1-9081-exec-6:[])  *** Final Certificate List:
2025-07-30 21:14:37,384 DEBUG [CertificateUtils.sortCertificateChain:1198] (http-nio-
127.0.0.1-9081-exec-6:[])     cert:
1.2.840.113549.1.9.1=#160f696e666f406163756d656e2e6e6574,CN=pssyslog.*.acumensec.local,OU=CC,
O=Acumen,L=Rockville,ST=MD,C=US
2025-07-30 21:14:37,384 DEBUG [CertificateUtils.sortCertificateChain:1198] (http-nio-
127.0.0.1-9081-exec-6:[])     cert:
1.2.840.113549.1.9.1=#160f696e666f406163756d656e2e6e6574,CN=pssyslog_ICA,OU=CC,O=Acumen,L=Roc
kville,ST=MD,C=US
2025-07-30 21:14:37,384 DEBUG [CertificateUtils.sortCertificateChain:1198] (http-nio-
127.0.0.1-9081-exec-6:[])     cert:
1.2.840.113549.1.9.1=#160f696e666f406163756d656e2e6e6574,CN=pssyslog_CA,OU=CC,O=Acumen,L=Rock
ville,ST=MD,C=US
2025-07-30 21:14:37,384 DEBUG [CertificateUtils.openCertificate:1393] (http-nio-127.0.0.1-
9081-exec-6:[])  Trying DER...
2025-07-30 21:14:37,385 DEBUG [CertificateUtils.openCertificateAsDER:1462] (http-nio-
127.0.0.1-9081-exec-6:[])  Trying DER...
2025-07-30 21:14:37,385 DEBUG [CertificateUtils.openCertificate:1396] (http-nio-127.0.0.1-
9081-exec-6:[])  Trying DER... match found.
2025-07-30 21:14:37,385 DEBUG [SysLogConfigImpl.validateServerCertificate:1074] (http-nio-
127.0.0.1-9081-exec-6:[])  CA certificate chain length 2 for pssyslog.acumensec.local:6515
2025-07-30 21:14:37,386 DEBUG [CertificateUtils.sortCertificateChain:1168] (http-nio-
127.0.0.1-9081-exec-6:[])  *** Original Certificate List:
2025-07-30 21:14:37,386 DEBUG [CertificateUtils.sortCertificateChain:1170] (http-nio-
127.0.0.1-9081-exec-6:[])     cert:
1.2.840.113549.1.9.1=#160f696e666f406163756d656e2e6e6574,CN=pssyslog.*.acumensec.local,OU=CC,
O=Acumen,L=Rockville,ST=MD,C=US
2025-07-30 21:14:37,386 DEBUG [CertificateUtils.sortCertificateChain:1170] (http-nio-
127.0.0.1-9081-exec-6:[])     cert:
1.2.840.113549.1.9.1=#160f696e666f406163756d656e2e6e6574,CN=pssyslog_ICA,OU=CC,O=Acumen,L=Roc
kville,ST=MD,C=US
2025-07-30 21:14:37,386 DEBUG [CertificateUtils.sortCertificateChain:1170] (http-nio-
127.0.0.1-9081-exec-6:[])     cert:
1.2.840.113549.1.9.1=#160f696e666f406163756d656e2e6e6574,CN=pssyslog_CA,OU=CC,O=Acumen,L=Rock
ville,ST=MD,C=US
2025-07-30 21:14:37,391 DEBUG [CertificateUtils.sortCertificateChain:1196] (http-nio-
127.0.0.1-9081-exec-6:[])  *** Final Certificate List:
2025-07-30 21:14:37,392 DEBUG [CertificateUtils.sortCertificateChain:1198] (http-nio-
127.0.0.1-9081-exec-6:[])     cert:
1.2.840.113549.1.9.1=#160f696e666f406163756d656e2e6e6574,CN=pssyslog.*.acumensec.local,OU=CC,
O=Acumen,L=Rockville,ST=MD,C=US
2025-07-30 21:14:37,392 DEBUG [CertificateUtils.sortCertificateChain:1198] (http-nio-
127.0.0.1-9081-exec-6:[])     cert:
1.2.840.113549.1.9.1=#160f696e666f406163756d656e2e6e6574,CN=pssyslog_ICA,OU=CC,O=Acumen,L=Roc
kville,ST=MD,C=US
2025-07-30 21:14:37,392 DEBUG [CertificateUtils.sortCertificateChain:1198] (http-nio-
127.0.0.1-9081-exec-6:[])     cert:
1.2.840.113549.1.9.1=#160f696e666f406163756d656e2e6e6574,CN=pssyslog_CA,OU=CC,O=Acumen,L=Rock
ville,ST=MD,C=US
2025-07-30 21:14:37,393 INFO  [SysLogConfigImpl.validateServerCertificate:1089] (http-nio-
127.0.0.1-9081-exec-6:[])  certificate order in the chain EMAILADDRESS=info@acumen.net,
CN=pssyslog.*.acumensec.local, OU=CC, O=Acumen, L=Rockville, ST=MD, C=US
2025-07-30 21:14:37,393 INFO  [SysLogConfigImpl.validateServerCertificate:1089] (http-nio-
127.0.0.1-9081-exec-6:[])  certificate order in the chain EMAILADDRESS=info@acumen.net,
CN=pssyslog_ICA, OU=CC, O=Acumen, L=Rockville, ST=MD, C=US
2025-07-30 21:14:37,394 INFO  [SysLogConfigImpl.validateServerCertificate:1089] (http-nio-
127.0.0.1-9081-exec-6:[])  certificate order in the chain EMAILADDRESS=info@acumen.net,
CN=pssyslog_CA, OU=CC, O=Acumen, L=Rockville, ST=MD, C=US
```

Requirement	Auditable Events	Additional Audit Record Contents
2025-07-30 21:14:37,394 DEBUG [SysLogConfigImpl.validateServerCertificate:1101] (http-nio-127.0.0.1-9081-exec-6:[]) complete certificate chain length 3 for pssyslog.acumensec.local:6515 2025-07-30 21:14:37,394 ERROR [CommonCriteriaX509ValidationService.validateMDMPPX509CertificateCompliance:94] (http-nio-127.0.0.1-9081-exec-6:[]) syslogServer SAN or CN validation failed for the certificates.		
FCS_TLSS_EXT.1	Failure to establish a TLS session.	Reason for failure.

RSA WITH 3DES EDE CBC SHA:

[Thu Jan 16 18:48:56.306845 2025] [ssl:info] [pid 115109] [client 192.168.130.1:44874] AH02008: SSL library error 1 in handshake (server acumencertdomain.net:443)

[Thu Jan 16 18:48:56.306888 2025] [ssl:info] [pid 115109] SSL Library Error: error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared cipher -- Too restrictive SSLCipherSuite or using DSA server certificate?

[Thu Jan 16 18:48:56.306895 2025] [ssl:info] [pid 115109] [client 192.168.130.1:44874] AH01998: Connection closed to child 0 with abortive shutdown (server acumencertdomain.net:443)

NULL WITH NULL NULL:

[Thu Jan 16 18:48:56.313950 2025] [ssl:info] [pid 115133] [client 192.168.130.1:44888] AH02008: SSL library error 1 in handshake (server acumencertdomain.net:443)

[Thu Jan 16 18:48:56.313960 2025] [ssl:info] [pid 115133] SSL Library Error: error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared cipher -- Too restrictive SSLCipherSuite or using DSA server certificate?

[Thu Jan 16 18:48:56.313966 2025] [ssl:info] [pid 115133] [client 192.168.130.1:44888] AH01998: Connection closed to child 5 with abortive shutdown (server acumencertdomain.net:443)

modified EncryptedPreMasterSecret:

[Tue Mar 25 20:25:54.069721 2025] [ssl:trace3] [pid 31358] ssl_engine_kernel.c(2232): [client 10.1.3.204:37742] OpenSSL: Write: error

[Tue Mar 25 20:25:54.069724 2025] [ssl:trace3] [pid 31358] ssl_engine_kernel.c(2251): [client 10.1.3.204:37742] OpenSSL: Exit: error in error

[Tue Mar 25 20:25:54.069728 2025] [ssl:info] [pid 31358] [client 10.1.3.204:37742] AH02008: SSL library error 1 in handshake (server acumencertdomain.net:443)

[Tue Mar 25 20:25:54.069747 2025] [ssl:info] [pid 31358] SSL Library Error: error:1408F119:SSL routines:ssl3_get_record:decryption failed or bad record mac

[Tue Mar 25 20:25:54.069751 2025] [ssl:info] [pid 31358] [client 10.1.3.204:37742] AH01998: Connection closed to child 9 with abortive shutdown (server acumencertdomain.net:443)

Modified client Finished Handshake:

[Thu Jan 16 19:12:34.680321 2025] [ssl:trace3] [pid 115131] ssl_engine_kernel.c(2232): [client 192.168.130.1:57252] OpenSSL: Write: error

[Thu Jan 16 19:12:34.680325 2025] [ssl:trace3] [pid 115131] ssl_engine_kernel.c(2251): [client 192.168.130.1:57252] OpenSSL: Exit: error in error

[Thu Jan 16 19:12:34.680329 2025] [ssl:info] [pid 115131] [client 192.168.130.1:57252] AH02008: SSL library error 1 in handshake (server acumencertdomain.net:443)

[Thu Jan 16 19:12:34.680363 2025] [ssl:info] [pid 115131] SSL Library Error: error:1408F119:SSL routines:ssl3_get_record:decryption failed or bad record mac

[Thu Jan 16 19:12:34.680369 2025] [ssl:info] [pid 115131] [client 192.168.130.1:57252] AH01998: Connection closed to child 3 with abortive shutdown (server acumencertdomain.net:443)

Random bytes after ChangeCipherSpec:

[Tue Mar 25 20:42:43.001992 2025] [ssl:trace3] [pid 31057] ssl_engine_kernel.c(2232): [client 10.1.3.204:47270] OpenSSL: Write: error

[Tue Mar 25 20:42:43.001997 2025] [ssl:trace3] [pid 31057] ssl_engine_kernel.c(2251): [client 10.1.3.204:47270] OpenSSL: Exit: error in error

[Tue Mar 25 20:42:43.002005 2025] [ssl:info] [pid 31057] [client 10.1.3.204:47270] AH02008: SSL library error 1 in handshake (server acumencertdomain.net:443)

[Tue Mar 25 20:42:43.002051 2025] [ssl:info] [pid 31057] SSL Library Error: error:14094091:SSL routines:ssl3_read_bytes:data between ccs and finished

[Tue Mar 25 20:42:43.002061 2025] [ssl:info] [pid 31057] [client 10.1.3.204:47270] AH01998: Connection closed to child 10 with abortive shutdown (server acumencertdomain.net:443)

Requirement	Auditable Events	Additional Audit Record Contents
Unsupported SSL versions: **SSL v2.0:** [Thu Jan 16 19:45:59.391557 2025] [ssl:info] [pid 115110] [client 192.168.130.1:39336] AH02008: SSL library error 1 in handshake (server acumencertdomain.net:443) [Thu Jan 16 19:45:59.391592 2025] [ssl:info] [pid 115110] SSL Library Error: error:142090FC:SSL routines:tls_early_post_process_client_hello:unknown protocol [Thu Jan 16 19:45:59.391598 2025] [ssl:info] [pid 115110] [client 192.168.130.1:39336] AH01998: Connection closed to child 1 with abortive shutdown (server acumencertdomain.net:443) **SSL v3.0:** [Thu Jan 16 19:45:59.443159 2025] [ssl:trace3] [pid 115132] ssl_engine_kernel.c(2232): [client 192.168.130.1:39338] OpenSSL: Write: error [Thu Jan 16 19:45:59.443164 2025] [ssl:trace3] [pid 115132] ssl_engine_kernel.c(2251): [client 192.168.130.1:39338] OpenSSL: Exit: error in error [Thu Jan 16 19:45:59.443168 2025] [ssl:info] [pid 115132] [client 192.168.130.1:39338] AH02008: SSL library error 1 in handshake (server acumencertdomain.net:443) [Thu Jan 16 19:45:59.443179 2025] [ssl:info] [pid 115132] SSL Library Error: error:1420918C:SSL routines:tls_early_post_process_client_hello:version too low [Thu Jan 16 19:45:59.443185 2025] [ssl:info] [pid 115132] [client 192.168.130.1:39338] AH01998: Connection closed to child 4 with abortive shutdown (server acumencertdomain.net:443) **TLS v1.0:** [Thu Jan 16 19:45:59.482696 2025] [ssl:trace3] [pid 115161] ssl_engine_kernel.c(2232): [client 192.168.130.1:39350] OpenSSL: Write: error [Thu Jan 16 19:45:59.482699 2025] [ssl:trace3] [pid 115161] ssl_engine_kernel.c(2251): [client 192.168.130.1:39350] OpenSSL: Exit: error in error [Thu Jan 16 19:45:59.482703 2025] [ssl:info] [pid 115161] [client 192.168.130.1:39350] AH02008: SSL library error 1 in handshake (server acumencertdomain.net:443) [Thu Jan 16 19:45:59.482715 2025] [ssl:info] [pid 115161] SSL Library Error: error:14209102:SSL routines:tls_early_post_process_client_hello:unsupported protocol [Thu Jan 16 19:45:59.482718 2025] [ssl:info] [pid 115161] [client 192.168.130.1:39350] AH01998: Connection closed to child 7 with abortive shutdown (server acumencertdomain.net:443) **TLS 1_1:** [Thu Jan 16 19:45:59.528338 2025] [ssl:trace3] [pid 115162] ssl_engine_kernel.c(2232): [client 192.168.130.1:39356] OpenSSL: Write: error [Thu Jan 16 19:45:59.528341 2025] [ssl:trace3] [pid 115162] ssl_engine_kernel.c(2251): [client 192.168.130.1:39356] OpenSSL: Exit: error in error [Thu Jan 16 19:45:59.528344 2025] [ssl:info] [pid 115162] [client 192.168.130.1:39356] AH02008: SSL library error 1 in handshake (server acumencertdomain.net:443) [Thu Jan 16 19:45:59.528353 2025] [ssl:info] [pid 115162] SSL Library Error: error:14209102:SSL routines:tls_early_post_process_client_hello:unsupported protocol [Thu Jan 16 19:45:59.528357 2025] [ssl:info] [pid 115162] [client 192.168.130.1:39356] AH01998: Connection closed to child 8 with abortive shutdown (server acumencertdomain.net:443)		
FIA_ENR_EXT.1	Failure of MD user authentication.	Presented username.

Requirement	Auditable Events	Additional Audit Record Contents
Failed User Authentication: 2025-04-08 17:53:41,196 WARN [DeviceRegistrationServiceImpl.getDeviceUUIDForValidRegistrationPin:2473] (http-nio-127.0.0.1-8081-exec-1:[]) {pathInfo=/api/v2/Enrollment/CertReq.enroll} No registration PIN found 2025-04-08 17:53:41,196 INFO [ApplicationLoggingHelper.log:94] (http-nio-127.0.0.1-8081-exec-1:[]) {pathInfo=/api/v2/Enrollment/CertReq.enroll} Registration failed for device with platform: Android. Reason: Device not found for provided PIN - User: admin 2025-04-08 17:53:41,199 ERROR [MIDeviceServiceImpl.authenticateUserByPin:5879] (http-nio-127.0.0.1-8081-exec-1:[]) {pathInfo=/api/v2/Enrollment/CertReq.enroll} PinAuthFailed: Device not found for the PIN you entered. Check your PIN and try again. 2025-04-08 17:53:41,201 INFO [MIUserServiceImpl.updateFailedLoginStatus:3532] (http-nio-127.0.0.1-8081-exec-1:[]) {pathInfo=/api/v2/Enrollment/CertReq.enroll} User admin failed to login attempt 1 from ipaddress null 2025-04-08 17:53:41,212 WARN [MIDeviceServiceImpl.registerViaHelper:4812] (http-nio-127.0.0.1-8081-exec-1:[]) {pathInfo=/api/v2/Enrollment/CertReq.enroll} Couldn't authenticate user, regMode=PASSWORD_AND_PIN 2025-04-08 17:53:41,213 ERROR [EnrollmentServiceImpl.process:1552] (http-nio-127.0.0.1-8081-exec-1:[]) {pathInfo=/api/v2/Enrollment/CertReq.enroll} User Registration Failed: Authentication Failed: Invalid Credentials. 2025-04-08 17:53:41,213 ERROR [EnrollmentServiceImpl.process:1607] (http-nio-127.0.0.1-8081-exec-1:[]) {pathInfo=/api/v2/Enrollment/CertReq.enroll} User Registration Failed: com.mobileiron.enrollment.service.EnrollmentException: Authentication Failed: Invalid Credentials.at com.mobileiron.enrollment.service.EnrollmentServiceImpl.process(EnrollmentServiceImpl.java:1553) ~[classes/:?] org.apache.tomcat.util.threads.TaskThread$WrappingRunnable.run(TaskThread.java:63) ~[tomcat-util.jar:9.0.86] at java.lang.Thread.run(Thread.java:750) ~[?:1.8.0_382] 2025-04-08 17:53:41,215 ERROR [RegModeEnrollmentController.handleRequestInternal:94] (http-nio-127.0.0.1-8081-exec-1:[]) {pathInfo=/api/v2/Enrollment/CertReq.enroll} Filed to process the request, Reason: Authentication Failed: Invalid Credentials.		
FIA_X509_EXT.1(1)	Failure to validate X.509 certificate.	Reason for failure.

Connection failure with syslog server (TOE acting as a client):

```
2025-06-16T19:55:42.732282+00:00 acumencertdomain rsyslogd:  nsd_ossl: TLS Connection initiated with remote syslog server. [v8.2102.0-15.
el8]
2025-06-16T19:55:42.734859+00:00 acumencertdomain rsyslogd:  Certificate EXPIRED at depth: 0   issuer  = /C=US/ST=MD/L=Rockville/O=Acumen
/OU=CC/CN=intermediate/emailAddress=info@acumen.net  subject = /C=US/ST=MD/L=Rockville/O=Acumen/OU=CC/CN=pssyslog.acumensec.local/emailAd
dress=info@acumen.net  err 10:certificate has expired [v8.2102.0-15.el8]
2025-06-16T19:55:42.734868+00:00 acumencertdomain rsyslogd:  SSL_ERROR_SSL Error in 'osslHandshakeCheck Client': 'error:00000001:lib(0):f
unc(0):reason(1)(1)' with ret=-1  [v8.2102.0-15.el8]
2025-06-16T19:55:42.734872+00:00 acumencertdomain rsyslogd:  nsd_ossl:OpenSSL Error Stack: error:1416F086:SSL routines:tls_process_server
_certificate:certificate verify failed [v8.2102.0-15.el8]
2025-06-16T19:55:42.734875+00:00 acumencertdomain rsyslogd:  nsd_ossl:TLS session terminated with remote syslog server. [v8.2102.0-15.el8
]
```

Failure to upload a CA certificate on the TOE:

```
2025-03-17 19:20:47,004 INFO [MICSController.handleUploadCertificate:3741] (http-nio-
    127.0.0.1-9081-exec-3:[]) Uploading the certificate of type: portal
2025-03-17 19:20:47,005 DEBUG [MICSController.handleUploadCertificate:3771] (http-nio-
    127.0.0.1-9081-exec-3:[]) Got file: x509_server_expired.p12 of data length 2883
2025-03-17 19:20:47,005 DEBUG [CertificateUtils.openCertificate:1390] (http-nio-127.0.0.1-
    9081-exec-3:[]) Trying DER...
2025-03-17 19:20:47,006 DEBUG [CertificateUtils.openCertificateAsDER:1459] (http-nio-
    127.0.0.1-9081-exec-3:[]) Trying DER...
2025-03-17 19:20:47,006 DEBUG [CertificateUtils.openCertificate:1397] (http-nio-127.0.0.1-
    9081-exec-3:[]) Trying PEM...
2025-03-17 19:20:47,006 DEBUG [CertificateUtils.openCertificateAsPEM:1472] (http-nio-
    127.0.0.1-9081-exec-3:[]) Trying PEM...
2025-03-17 19:20:47,007 DEBUG [CertificateUtils.openCertificate:1405] (http-nio-127.0.0.1-
    9081-exec-3:[]) Trying PKCS7...
2025-03-17 19:20:47,007 DEBUG [CertificateUtils.openPKCS7:1485] (http-nio-127.0.0.1-9081-
    exec-3:[]) Trying PKCS7...
2025-03-17 19:20:47,007 DEBUG [CertificateUtils.openCertificate:1420] (http-nio-127.0.0.1-
    9081-exec-3:[]) Trying PKCS12...
2025-03-17 19:20:47,185 DEBUG [CertificateUtils.openKeyStore:1635] (http-nio-127.0.0.1-9081-
    exec-3:[]) alias: 76133c9e9f8aa250d827db9a6bd55fa2b0fc831c (isKey true, isCert false)
2025-03-17 19:20:47,214 DEBUG [CertificateUtils.openKeyStore:1664] (http-nio-127.0.0.1-9081-
    exec-3:[]) key: PKCS#8
2025-03-17 19:20:47,214 DEBUG [CertificateUtils.openCertificate:1423] (http-nio-127.0.0.1-
    9081-exec-3:[]) Trying PKCS12... match found.
2025-03-17 19:20:47,215 INFO [ApplicationLoggingHelper.log:94] (http-nio-127.0.0.1-9081-exec-
    3:[]) Certificate Expired. Subject: EMAILADDRESS=info@acumen.net, CN=acumencertdomain.net,
    OU=CC, O=Acumen, L=Rockville, ST=MD, C=US Serial Number: 3733470652126645570 Issuer:
    CN=Acumen_ICA, OU=CC, O=Acumen, L=Rockville, ST=MD, C=US Not After: Fri Feb 28 17:14:00
    UTC 2025
2025-03-17 19:20:47,216 WARN [MICSController.handleUploadCertificate:4101] (http-nio-
    127.0.0.1-9081-exec-3:[]) Failed to upload certificate(s). Reason: Certificate with
    subject 'EMAILADDRESS=info@acumen.net, CN=acumencertdomain.net, OU=CC, O=Acumen,
    L=Rockville, ST=MD, C=US' expired on 2/28/25 5:14 PM
2025-03-17 19:20:47,216 DEBUG [CommonUtilities.getProperty:395] (http-nio-127.0.0.1-9081-
    exec-3:[]) Getting property : portal_certificate_path
2025-03-17 19:20:47,216 DEBUG [CertificateUtils.openCertificate:1390] (http-nio-127.0.0.1-
    9081-exec-3:[]) Trying DER...
2025-03-17 19:20:47,216 DEBUG [CertificateUtils.openCertificateAsDER:1459] (http-nio-
    127.0.0.1-9081-exec-3:[]) Trying DER...
2025-03-17 19:20:47,217 DEBUG [CertificateUtils.openCertificate:1393] (http-nio-127.0.0.1-
    9081-exec-3:[]) Trying DER... match found.
2025-03-17 19:20:47,218 DEBUG [CommandExecConfigImpl.execCommand:40] (http-nio-127.0.0.1-
    9081-exec-3:[]) into execCommandimpl
    2025-03-17 19:20:47,218 DEBUG [ConfigServiceHandler.handleMessage:301] (http-nio-
    127.0.0.1-9081-exec-3:[]) userService is set
```

Requirement	Auditable Events	Additional Audit Record Contents
FIA_X509_EXT.2	Failure to establish connection to determine revocation status.	No additional information.

Connection failure with syslog server (TOE acting as a client):

```
2025-06-24T20:19:01.848943+00:00 acumencertdomain rsyslogd:  nsd_ossl: TLS Connection
initiated with remote syslog server. [v8.2102.0-15.el8]
2025-06-24T20:19:01.848949+00:00 acumencertdomain rsyslogd:  rsyslogd[internal_messages]: 309
   messages lost due to rate-limiting (500 allowed within 5 seconds)
2025-06-24T20:19:01.859345+00:00 acumencertdomain rsyslogd:  Certificate error at depth: 1
   issuer  =
   /C=US/ST=MD/L=Rockville/O=Acumen/OU=CC/CN=intermediate/emailAddress=info@acumen.net
   subject = /CN=Intermediate-NoBasicConstraints  err 24:invalid CA certificate [v8.2102.0-
   15.el8]
2025-06-24T20:19:01.859352+00:00 acumencertdomain rsyslogd:  SSL_ERROR_SSL Error in
   'osslHandshakeCheck Client': 'error:00000001:lib(0):func(0):reason(1)(1)' with ret=-1
   [v8.2102.0-15.el8]
2025-06-24T20:19:01.859355+00:00 acumencertdomain rsyslogd:  nsd_ossl:OpenSSL Error Stack:
   error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed
   [v8.2102.0-15.el8]
2025-06-24T20:19:01.859357+00:00 acumencertdomain rsyslogd:  nsd_ossl:TLS session terminated
   with remote syslog server. [v8.2102.0-15.el8]
```

Failure to upload a CA certificate on the TOE:

```
2025-03-17 21:18:57,248 DEBUG [CertificateUtils.processData:1935] (http-nio-127.0.0.1-9081-
   exec-1:[]) CERT[3]:
   1.2.840.113549.1.9.1=#160f696e666f406163756d656e2e6e6574,CN=X509_RSA_CA,OU=CC,O=Acumen,L=R
   ockville,ST=MD,C=US /
   1.2.840.113549.1.9.1=#160f696e666f406163756d656e2e6e6574,CN=X509_RSA_CA,OU=CC,O=Acumen,L=R
   ockville,ST=MD,C=US
2025-03-17 21:18:57,257 ERROR
   [CommonCriteriaX509ValidationService.validateMDMPPX509CertificateCompliance:66] (http-nio-
   127.0.0.1-9081-exec-1:[]) portal Extended key usage validation failed for the uploaded
   certificate.
2025-03-17 21:18:57,257 INFO [ApplicationLoggingHelper.log:69] (http-nio-127.0.0.1-9081-exec-
   1:[]) CA certificates must have Basic Constraints set.
-----BEGIN CERTIFICATE-----
MIIEczCCA1ugAwIBAgIICCyKPGWIAOMwDQYJKoZIhvcNAQELBQAwgYQxCzAJBgNV
BAYTAlVTMQswCQYDVQQIEwJNRDESMBAGA1UEBxMJUm9ja3ZpbGxlMQ8wDQYDVQQK
EwZBY3VtZW4xCzAJBgNVBAsTAkNDMRYwFAYDVQQDDA1YNTA5X1JTQV9JQ0ExMR4w
HAYJKoZIhvcNAQkBFg9pbmZvQGFjdW1lbi5uZXQwHhcNMjUwMzExMTkxNTAwWhcN
MzUwMzExMTkxMTAwWjCBgzELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1EMRIwEAYD
VQQHEwlSb2NrdmlsbGUxDzANBgNVBAoTBkFjdW1lbjELMAkGA1UECxMCQ0MxFTAT
BgNVBAMMDFg1MDlfUlNBX0lDMjEeMBwGCSqGSIb3DQEJARYPaW5mb0BhY3VtZW4u
bmV0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlw10JVOK4K3pr5VF
jKzzA8Ha/QSVBqfl1dDeVKy7R9YWGJEuKHq8pr2ZjRDFznXu/EDBqKZeFyvdgXGT
iwmRBk/SHjsHlyPTAhKgxlMWBTlSmDhhWN+k+vJldtco7/AD0qGqgBTZ6FATfc1D
BcnJOXhrb0Sv+B24dFWSc/dZNC9btRFTGtGtjnBU3pd9cSoxL37t177NLbExfCGe
4x+fk4Icif4sO03opIocfcWOlXLWwnNgqry+t3BEr7AAGRMy2+Yhyg3/jW+O6jwa
fTx+kLrNdglqeDINpqgmN08Pe9ClMhTOQYlmWSxZGdIImF8LNi7FArFozbcWZQsv
6Z4PIQIDAQABo4HnMIHkMB0GA1UdDgQWBBSv39sMN2p1CTWO4htkq4ozhp/lLDAf
BgNVHSMEGDAWgBRnKCIcGqmwrtOX6NF1qSMLslyOzDALBgNVHQ8EBAMCAd4wJwYD
VR0lBCAwHgYIKwYBBQUHAwEGCCsGAQUFBwMCBggrBgEFBQcDCTA5BgNVHR8EMjAw
MC6gLKAqhihodHRwOi8vMTAuMS4zLjE0OTo4MDgwL1g1MDlfUlNBX0lDQTEuZGVy
MBEGCWCGSAGG+EIBAQQEAwIABzAeBglghkgBhvhCAQ0EERYPeGNhIGNlcnRpZmlj
YXRlMA0GCSqGSIb3DQEBCwUAA4IBAQA6Apj1fq7tXC0bYAV4O+hgaEz/y5AbZdqp
gyEzI2buRnaNUnCuL13qFburXVlegqgoq0CmWQuT5DWoZma1Vm4N+0mcv9Ik8tEv
292CAPtZ8uVm0PB2oIFiHmKrVBVugGDoY/sQ8SGTeUWUuGD8W+lBSB43rhdU3LLr
NckTF01eb9R+q3aEn9lQCgwicbDmx+o5rtDg4FVCMFTbiK3KD0Z4Cu+826sBdq/V
cg4JW8XgYbGVsxPY7NtifEROal9ICljcriCrUpzSgSlBYU+Un3z3Y0HftAaw643/
ZGgS2Q5joSuasXSh6Hqs9I4CURGAfSW/lOAUong38O0VR6HM7hqI
-----END CERTIFICATE-----
2025-03-17 21:18:57,258 INFO [ApplicationLoggingHelper.log:82] (http-nio-127.0.0.1-9081-exec-
   1:[]) Certificate chain path length error. Certificate is not a valid CA certificate:
   certificate EMAILADDRESS=info@acumen.net, CN=X509_RSA_IC2, OU=CC, O=Acumen, L=Rockville,
   ST=MD, C=US with serial number 5889976432847751 39
```

Requirement	Auditable Events	Additional Audit Record Contents
2025-03-17 21:18:57,258 ERROR [CommonCriteriaX509ValidationService.validateMDMPPX509CertificateCompliance:102] (http-nio-127.0.0.1-9081-exec-1:[]) portal Basic constraint pathlen validation failed for the uploaded certificates.		
FMT_MOF.1(1)	Issuance of command to perform function.	Command sent and identity of MDM Agent recipient(s).
	Change of policy settings.	Policy changed and value or full policy.

Issuance of command to perform function:

	ACTION	STATE	PERFORMED ...	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
	Lock	Success	admin	Mon Mar 24 2025 20:22:31 GMT+...	Mon Mar 24 2025 20:22:31 GMT+0000 (...	admin (Android 14.0 - PDA 12)	This is to test FMT_SMF.1.1(1) Test#1
	Lock Device (Android)	Acknowl...	<MDM>	Mon Mar 24 2025 20:22:31 GMT+...	Mon Mar 24 2025 20:22:34 GMT+0000 (...	admin (Android 14.0 - PDA 12)	Completed MDM request.

Note: Here "Action" refers to command issued and "performed on" refers to the identity of MDM agent.

Change of policy settings:

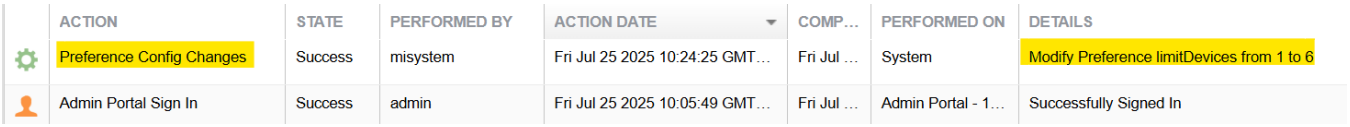
	ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
	Apply Label To Policy	Success	admin	Tue Mar 25 2025 20:...	Tue Mar 25 2025 20:15:40 GMT+00...	Android WallPaper - FMT_SMF_install_pol...	Label 'Android' is applied to policy 'FMT_SMF_install_policy'.
	Activate Policy	Success	admin	Tue Mar 25 2025 20:...	Tue Mar 25 2025 20:13:57 GMT+00...	Android WallPaper - FMT_SMF_install_pol...	Policy 'FMT_SMF_install_policy' is activated successfully.
	Modify Policy Priority	Success	admin	Tue Mar 25 2025 20:...	Tue Mar 25 2025 20:13:57 GMT+00...	Android WallPaper - FMT_SMF_install_pol...	The priority for policy 'FMT_SMF_install_policy' is modified.
	Add Policy	Success	admin	Tue Mar 25 2025 20:...	Tue Mar 25 2025 20:13:57 GMT+00...	Android WallPaper - FMT_SMF_install_pol...	Policy 'FMT_SMF_install_policy' is added successfully.

FMT_MOF.1(2)	Enrollment by a user.	Identity of user

	ACTION	STATE	PERFORME...	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
	Register Device	Success	admin	Thu Mar 20 2025 19:28:43 GM...	Thu Mar 20 2025 19:28:43 GMT+0...	admin (Android 14.0 - PDA 12)	Device is fully registered
	Create Device Certificate	Success	misystem	Thu Mar 20 2025 19:28:43 GM...	Thu Mar 20 2025 19:28:43 GMT+0...	admin (Android 14.0 - PDA 12)	SCEP Name: 'System - Mutual Auth CE setting', Serial Number: '125',
	Apply Multiple Labels to...	Success	misystem	Thu Mar 20 2025 19:20:32 GM...	Thu Mar 20 2025 19:20:32 GMT+0...	admin (Android - PDA 12)	Label: 'Android,Company-Owned,All-Smartphones' applied to devices. Number of associated polici...
	Profile Change	Acknowl...	<MDM>	Thu Mar 20 2025 19:20:32 GM...	Thu Mar 20 2025 19:28:44 GMT+0...	admin (Android 14.0 - PDA 12)	Completed MDM request.
	Send Message	Failed	admin	Thu Mar 20 2025 19:20:27 GM...	Thu Mar 20 2025 19:20:27 GMT+0...	admin (Android - PDA 12)	Message to notify registration details via email - Failure Message: Failed to send message to the d...
	Send Message	Initiated	admin	Thu Mar 20 2025 19:20:27 GM...	Thu Mar 20 2025 19:20:27 GMT+0...	admin (Android - PDA 12)	Message to notify registration details via email
	Register Device	Success	admin	Thu Mar 20 2025 19:20:27 GM...	Thu Mar 20 2025 19:20:27 GMT+0...	admin (Android - PDA 12)	Created a client profile for Admin for device 24c05392-0b0b-45ed-87ed-3709b08f6752 with phone ...

Note: Here "Action" refers to command issued and "performed on" refers to the identity of MDM agent.

FMT_SMF.1(2)	Success or failure of function.	No additional information.

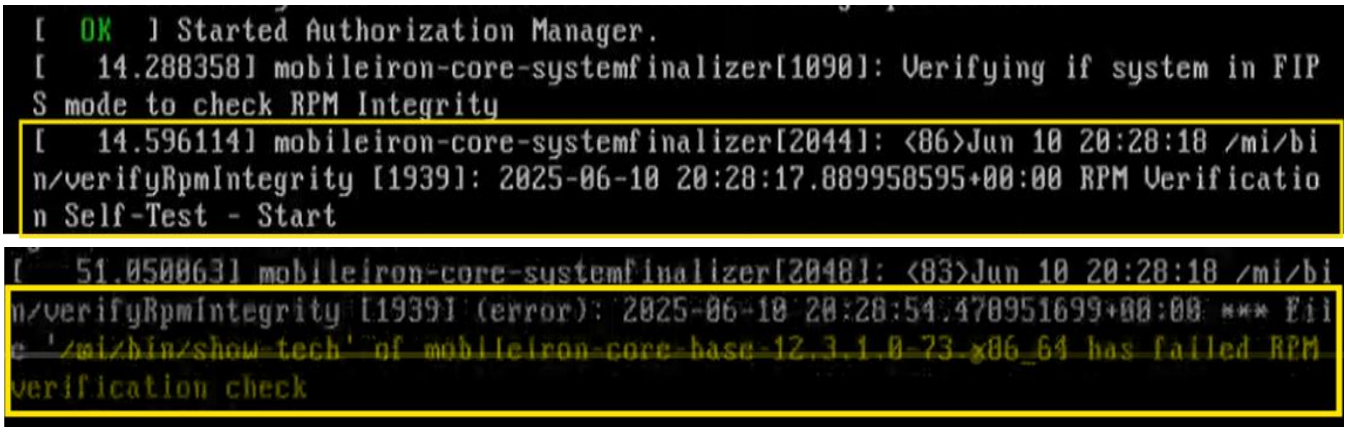
Requirement	Auditable Events	Additional Audit Record Contents
Configure the devices specified by a unique device ID:  **Configure the number of devices allowed:** 		
FPT_ITT.1(2)	Initiation and termination of the trusted channel.	Trusted channel protocol. Identity of initiator and recipient.
Initiation: [Mon Jul 28 15:13:30.452554 2025] [ssl:info] [pid 108308] [client 192.168.128.39:52040] AH01964: Connection to child 5 established (server acumensec.domain.local:443) [Mon Jul 28 15:13:30.452677 2025] [ssl:trace2] [pid 108308] ssl_engine_rand.c(126): Server: Seeding PRNG with 144 bytes of entropy [Mon Jul 28 15:13:30.452758 2025] [ssl:trace3] [pid 108308] ssl_engine_kernel.c(2213): [client 192.168.128.39:52040] OpenSSL: Handshake: start [Mon Jul 28 15:13:30.452780 2025] [ssl:trace3] [pid 108308] ssl_engine_kernel.c(2222): [client 192.168.128.39:52040] OpenSSL: Loop: before SSL initialization [Mon Jul 28 15:13:30.541350 2025] [ssl:trace3] [pid 108308] ssl_engine_kernel.c(2217): [client 192.168.128.39:52040] OpenSSL: Handshake: done [Mon Jul 28 15:13:30.541364 2025] [ssl:debug] [pid 108308] ssl_engine_kernel.c(2266): [client 192.168.128.39:52040] AH02041: Protocol: TLSv1.2, Cipher: AES256-GCM-SHA384 (256/256 bits) [Mon Jul 28 15:13:30.541372 2025] [authz_core:debug] [pid 108308] mod_authz_core.c(846): [client 192.168.128.39:52040] AH01628: authorization result: granted (no directives) **Termination:** [Mon Jul 28 15:39:04.278087 2025] [core:trace8] [pid 121385] core_filters.c(575): [client 192.168.128.39:50370] brigade contains: bytes: 0, non-file bytes: 0, eor buckets: 0, morphing buckets: 0 [Mon Jul 28 15:39:04.278091 2025] [ssl:debug] [pid 121385] ssl_engine_io.c(1112): [client 192.168.128.39:50370] AH02001: Connection closed to child 6 with standard shutdown (server acumensec.domain.local:7443) [Mon Jul 28 15:39:04.278130 2025] [core:trace8] [pid 121385] core_filters.c(575): [client 192.168.128.39:50370] brigade contains: bytes: 0, non-file bytes: 0, eor buckets: 0, morphing buckets: 0		
FPT_TST_EXT.1	Initiation of self-test. Failure of self-test. Detected integrity violation.	Algorithm that caused failure. The TSF code file that caused the integrity violation.

Requirement	Auditable Events	Additional Audit Record Contents

Initiation of self-test:

```
Jun    10    19:38:21    acumencertdomain    /mi/bin/verifyRpmIntegrity    [1950]:    2025-06-10
    19:38:21.127458264+00:00 RPM Verification Self-Test - Start
Jun    10    19:38:44    acumencertdomain    /mi/bin/verifyRpmIntegrity    [1950]:    2025-06-10
    19:38:44.572227501+00:00 MD5 Sum has changed for /etc/denyhosts.conf
Jun    10    19:38:59    acumencertdomain    /mi/bin/verifyRpmIntegrity    [1950]:    2025-06-10
    19:38:59.738899371+00:00 All RPMs verified successfully
```

Failure of self-test:



FPT_TUD_EXT.1	Success or failure of signature verification.	No additional information

Failure of signature verification:

```
   upgradestatus-localhost
[MIRROR] mobileiron-core-mifs-12.3.1.0-76.noarch.rpm: Downloading successful, but checksum
    doesn't match. Calculated:
    ce4c839a350cd7cdefd9f8a577062b246b087fd76f900ec60a93badf682b7e56(sha256) Expected:
    454a314b82c29220d8220315123bcd6dff118acc28729a97d2db152f31f27dcb(sha256)
[MIRROR] mobileiron-core-mifs-12.3.1.0-76.noarch.rpm: Downloading successful, but checksum
    doesn't match. Calculated:
    ce4c839a350cd7cdefd9f8a577062b246b087fd76f900ec60a93badf682b7e56(sha256) Expected:
    454a314b82c29220d8220315123bcd6dff118acc28729a97d2db152f31f27dcb(sha256)
2025-03-28 18:36:30,339 INFO get-supported-upgrades [/mi/bin/get-supported-upgrades.py:207]
    System information: {'mi_release_string': 'VSP 12.3.1.0 Build 59 (Branch core-
    12.3.1.0)\n', 'product': 'VSP', 'version': '12.3.1.0', 'deployment': 'Build', 'build':
    '59', 'branding': 'mobileiron'}
2025-03-28 18:36:30,339 INFO get-supported-upgrades [/mi/bin/get-supported-upgrades.py:510]
    Unable to determine credentials, trying with out credentials
2025-03-28 18:36:40,753 INFO get-supported-upgrades [/mi/bin/get-supported-upgrades.py:207]
    System information: {'mi_release_string': 'VSP 12.3.1.0 Build 59 (Branch core-
    12.3.1.0)\n', 'product': 'VSP', 'version': '12.3.1.0', 'deployment': 'Build', 'build':
    '59', 'branding': 'mobileiron'}
    2025-03-28 18:36:40,753 INFO get-supported-upgrades [/mi/bin/get-supported-
    upgrades.py:510] Unable to determine credentials, trying with out credentials
```

Success:

Refer to Table 11 *Management activities audit logs* entry 11.

Requirement	Auditable Events	Additional Audit Record Contents
FTP_ITC.1(1)	Initiation and termination of the trusted channel.	Trusted channel protocol. Non-TOE endpoint of connection.

Initiation:

```
2025-06-10T23:04:10.621286+00:00 acumencertdomain rsyslogd: PRODUCT=Core_12.3.1.0_73,
   nsd_ossl: TLS Connection initiated with remote syslog server. [v8.2102.0-15.el8]
```

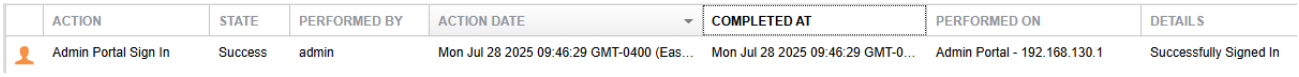
Termination:

```
2025-07-10T00:21:35.640738+00:00 acumencertdomain rsyslogd:  nsd_ossl:TLS session terminated
with remote syslog server. [v8.2102.0-15.el8]
```

FTP_TRP.1(1) and FTP_TRP.1(2)	Initiation and termination of the trusted channel.	Trusted channel protocol. Identity of administrator.

Initiation:

For admin portal:



ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Admin Portal Sign In	Success	admin	Mon Jul 28 2025 09:46:29 GMT-0400 (Eas...	Mon Jul 28 2025 09:46:29 GMT-0...	Admin Portal - 192.168.130.1	Successfully Signed In

For EPMM system manager:

```
[Mon Jul 28 13:57:02.334125 2025] [proxy:debug] [pid 48510] proxy_util.c(2647): [client
192.168.130.1:51890] AH00947: connected /mics/mics.html?dc=1753711019735 to 127.0.0.1:9081,
referer: https://acumencertdomain.net:8443/mics/mics.html
[Mon Jul 28 13:57:00.944597 2025] [ssl:info] [pid 113364] [client 192.168.130.1:51887]
AH01964: Connection to child 4 established (server acumencertdomain.net:8443)
[Mon Jul 28 13:57:00.944689 2025] [ssl:trace2] [pid 113364] ssl_engine_rand.c(126): Server:
Seeding PRNG with 144 bytes of entropy
[Mon Jul 28 13:57:00.944739 2025] [ssl:trace3] [pid 113364] ssl_engine_kernel.c(2213):
[client 192.168.130.1:51887] OpenSSL: Handshake: start
```

Termination:

For admin portal:

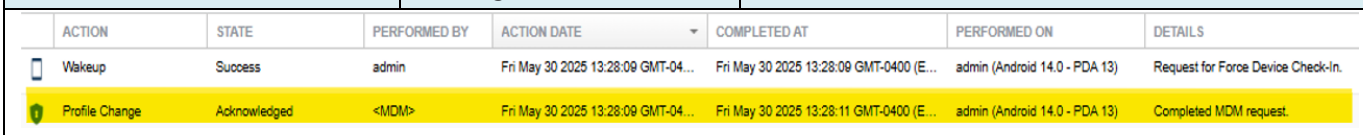


ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Admin Portal Sign Out	Success	admin	Tue Jul 22 2025 04:51:50 GMT-0400 (Easter...	Tue Jul 22 2025 04:51:50 GMT-0400 (Eastern...	admin	User admin logged out successfully.

For EPMM system manager:

```
[Mon Jul 28 13:50:56.479306 2025] [ssl:debug] [pid 48511] ssl_engine_io.c(1112): [client
192.168.130.1:51828] AH02001: Connection closed to child 6 with standard shutdown (server
acumencertdomain.net:8443
```

FAU_ALT_EXT.2	Success/failure of sending alert.	No additional information.



ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Wakeup	Success	admin	Fri May 30 2025 13:28:09 GMT-04...	Fri May 30 2025 13:28:09 GMT-0400 (E...	admin (Android 14.0 - PDA 13)	Request for Force Device Check-In.
Profile Change	Acknowledged	<MDM>	Fri May 30 2025 13:28:09 GMT-04...	Fri May 30 2025 13:28:11 GMT-0400 (E...	admin (Android 14.0 - PDA 13)	Completed MDM request.

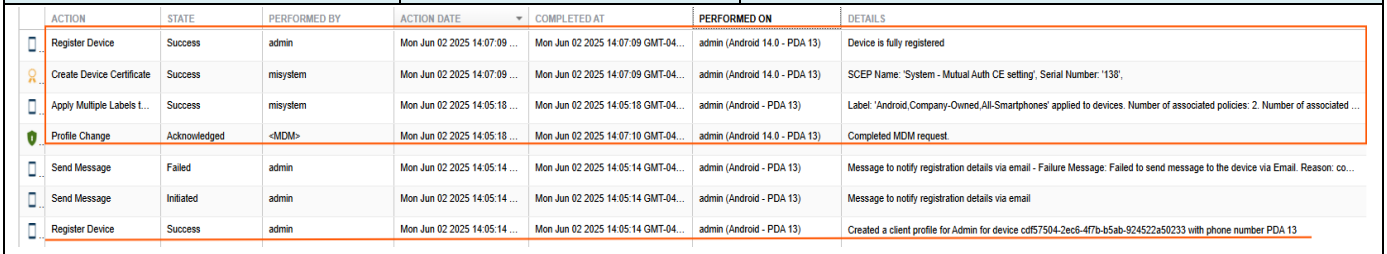
Requirement	Auditable Events	Additional Audit Record Contents
FAU_SEL.1(2)	All modifications to the audit configuration that occur while the audit collection functions are operating.	No additional information.

Requirement	Auditable Events	Additional Audit Record Contents
Audit data collection Function: 2025-08-28 10:39:58.267 6230 8324 I =ProvisionManager: AuditLog enabling result: true 2025-08-28 10:39:58.278 6230 8324 I =ProvisionManager: AuditLog level=ALERT success=true comp=com.mobileiron.mdmpp/ProvisionManager log=AUDIT_CONFIGURATION_CHANGE : AuditLog configuration changed: severityRule = 1 outcomeRule = 1 groupsRule = [1, 2, 3, 4, 5] usersList = [0] events: [AUDIT_CONFIGURATION_CHANGE, TLS_SESSION_FAILURE, TRANSITION_TO_LOCKED_STATE, ENROLLMENT_IN_MANAGEMENT, UNENROLLMENT_FROM_MANAGEMENT, POLICY_VALIDATION_FAILURE, CA_CERTIFICATE_IMPORT, ID_CERTIFICATE_IMPORT, CA_CERTIFICATE_REMOVE, ID_CERTIFICATE_REMOVE, INSTALL_APPLICATION, REMOVE_APPLICATION, SYSTEM_SOFTWARE_UPGRADE, WAKEUP_FROM_SERVER, QUERY_CURRENT_SOFTWARE_VERSION, QUERY_CURRENT_HARDWARE_VERSION, REPORT_APP_INVENTORY, UPLOAD_LOGS, APP_STORE_QUARANTINE_ACTION_CONFIGURED, ENABLE_DISABLE_CAMERA, ENABLE_DISABLE_MIC, ENABLE_DISABLE_VPN, ENABLE_DISABLE_RADIOS, ENABLE_DISABLE_DEVELOPMENT_MODE, CONFIGURE_UNLOCK_BANNER, ENABLE_DISABLE_USB_TETHER, ENABLE_DISABLE_LOCATION_SERVICES, ENABLE_DISABLE_BIOMETRICS] **Modified audit configuration:** 2025-08-28 13:21:04.701 6230 8324 D =DeviceOwnerLockdownConfigurator: apply: DO lockdown 2025-08-28 13:21:04.702 6230 26149 D =TLV_LOG: Version: 0x2 2025-08-28 13:21:04.703 6230 8182 D =TLV_LOG: Length: 156 2025-08-28 13:21:04.704 6230 8324 D =DeviceSideLockdownConfigurator: apply: device side lockdown 2025-08-28 13:21:04.705 6230 26149 D =TLV_LOG: Flags (0x2): HBT=0, Ack=1, Nak=0, Compress=0 2025-08-28 13:21:04.708 6230 8182 D =TLV_LOG: SenderId: 0x40000043 2025-08-28 13:21:04.708 6230 8324 I =DevicePolicyManagerUtils: disabling screen capture to false 2025-08-28 13:21:04.709 6230 26149 D =TLV_LOG: Length: 40 2025-08-28 13:21:04.710 6230 26149 D =TLV_LOG: SenderId: 0x0 2025-08-28 13:21:04.712 6230 26149 D =TLV_LOG: RecieverId: 0x40000043 2025-08-28 13:21:04.712 6230 8182 D =TLV_LOG: RecieverId: 0x0 2025-08-28 13:21:04.715 6230 26149 D =TLV_LOG: PacketId: 381 2025-08-28 13:21:04.716 6230 8182 D =TLV_LOG: PacketId: 382 2025-08-28 13:21:04.716 6230 8324 D =DevicePolicyManagerUtils: setting disable camera to : false 2025-08-28 13:21:04.717 6230 26149 D =TLV_LOG: Number of TLVs: 1 2025-08-28 13:21:04.718 6230 8182 D =TLV_LOG: Number of TLVs: 1 2025-08-28 13:21:04.720 6230 26149 D =TLV_LOG: TLV #0:		
FCS_RBG_EXT.1/AGT	Failure of the randomization process.	No additional information.

Requirement	Auditable Events	Additional Audit Record Contents
2025-10-06 13:36:39.833 3654 3654 V OpenSSLWrapper: FIPS self-test: Start CTR DRBG **2025-10-06 13:36:39.833 3654 3654 V OpenSSLWrapper: FIPS self-test: Corrupt CTR DRBG** **2025-10-06 13:36:39.833 3654 3654 V OpenSSLWrapper: FIPS self-test: Pass CTR DRBG** The RBG is tested at startup and the system will not continue booting if there is an error.		
FCS_TLSC_EXT.1	Failure to establish a TLS session.	Reason for failure.

```
2025-05-22 10:37:10.338 32754   676 D =ConnectionManager: Connecting to acumencertdomain.net:443
2025-05-22 10:37:10.577 32754   676 V OpenSSLWrapper: SSL_context 0xb4000079a95fb340 allocated
   for SSL: 0xb400007a38e35000
2025-05-22  10:37:10.582  32754      676  V  OpenSSLWrapper:  FIPS  self-test:  Start  ECDSA
   Conditional_PCT
2025-05-22  10:37:10.586  32754      676  V  OpenSSLWrapper:  FIPS  self-test:  Corrupt  ECDSA
   Conditional_PCT
2025-05-22 10:37:10.588 32754   676 V OpenSSLWrapper: FIPS self-test: Pass ECDSA Conditional_PCT
2025-05-22 10:37:10.696 32754    676 E OpenSSLWrapper: SSL_connect() failure
2025-05-22  10:37:10.696  32754    676  E  OpenSSLWrapper:  error:0A0000F8:SSL  routines::unknown
   cipher returned in ssl/statem/statem_clnt.c (set_client_ciphersuite): 1313 data:  flags: 1
2025-05-22 10:37:10.696 32754   676 V OpenSSLWrapper: SSL_context 0xb4000079a95fb340 deallocated
   for SSL: 0xb400007a38e35000
2025-05-22   10:37:10.697   32754        676   D   =ConnectionManager:   SSL   connection   to
   acumencertdomain.net:443 failed
2025-05-22 10:37:10.700 32754   676 I =SteadyStateMipTlsCallback: onFailed: NO_CONNECTIVITY
2025-05-22 10:37:10.701 32754   676 D =ProvisionManager: slot: REPORT_AUDIT_EVENT
2025-05-22 10:37:10.702 32754   676 D =ConnectionManager: Failed to open MIP socket.
2025-05-22 10:37:10.703 32754   676 D =ConfigMarshaller: slot: CONNECTION_CLOSED
2025-05-22 10:37:10.704 32754   676 D =ConfigMarshaller: slot: CONNECTION_ERROR
```

FIA_ENR_EXT.2	Enrollment in management.	Reference identifier of MDM Server.



ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Register Device	Success	admin	Mon Jun 02 2025 14:07:09 ...	Mon Jun 02 2025 14:07:09 GMT-04...	admin (Android 14.0 - PDA 13)	Device is fully registered
Create Device Certificate	Success	misystem	Mon Jun 02 2025 14:07:09 ...	Mon Jun 02 2025 14:07:09 GMT-04...	admin (Android 14.0 - PDA 13)	SCEP Name: 'System - Mutual Auth CE setting', Serial Number: '138',
Apply Multiple Labels t...	Success	misystem	Mon Jun 02 2025 14:05:18 ...	Mon Jun 02 2025 14:05:18 GMT-04...	admin (Android - PDA 13)	Label: 'Android,Company-Owned,All-Smartphones' applied to devices. Number of associated policies: 2. Number of associated ...
Profile Change	Acknowledged	<MDM>	Mon Jun 02 2025 14:05:18 ...	Mon Jun 02 2025 14:07:10 GMT-04...	admin (Android 14.0 - PDA 13)	Completed MDM request.
Send Message	Failed	admin	Mon Jun 02 2025 14:05:14 ...	Mon Jun 02 2025 14:05:14 GMT-04...	admin (Android - PDA 13)	Message to notify registration details via email - Failure Message: Failed to send message to the device via Email. Reason: co...
Send Message	Initiated	admin	Mon Jun 02 2025 14:05:14 ...	Mon Jun 02 2025 14:05:14 GMT-04...	admin (Android - PDA 13)	Message to notify registration details via email
Register Device	Success	admin	Mon Jun 02 2025 14:05:14 ...	Mon Jun 02 2025 14:05:14 GMT-04...	admin (Android - PDA 13)	Created a client profile for Admin for device cdf57504-2ec6-4f7b-b5ab-924522a50233 with phone number PDA 13

FIA_X509_EXT.1(1)	Failure to validate X.509 certificate.	Reason for failure.

```
2025-05-23 10:36:59.714  3537  4000 V OpenSSLWrapper: verify_callback error: num=10 :
certificate has expired
2025-05-23 10:36:59.715  3537  4000 V OpenSSLWrapper: verify_callback: preverify not ok
2025-05-23 10:36:59.715  3537  4000 E OpenSSLWrapper: SSL_connect() failure
```

FIA_X509_EXT.2	Failure to establish connection to determine revocation status.	No additional information.

Requirement	Auditable Events	Additional Audit Record Contents
2025-05-27 15:19:20.487 2470 3266 V OpenSSLWrapper: verify_callback error: num=20 : unable to get local issuer certificate 2025-05-27 15:19:20.488 2470 3266 V OpenSSLWrapper: verify_callback: preverify not ok 2025-05-27 15:19:20.488 2470 3266 E OpenSSLWrapper: SSL_connect() failure		
FMT_POL_EXT.2	Failure of policy validation.	Reason for failure of validation.

```
2025-05-21 13:34:01.238 32754   676 D =ConnectionManager: Connecting to
acumencertdomain.net:443
2025-05-21 13:34:01.476 32754   676 V OpenSSLWrapper: SSL_context 0xb400007999c15080
allocated for SSL: 0xb400007999aa0000
2025-05-21 13:34:01.479 32754   676 V OpenSSLWrapper: FIPS self-test: Start ECDSA
Conditional_PCT
2025-05-21 13:34:01.481 32754   676 V OpenSSLWrapper: FIPS self-test: Corrupt ECDSA
Conditional_PCT
2025-05-21 13:34:01.482 32754   676 V OpenSSLWrapper: FIPS self-test: Pass ECDSA
Conditional_PCT
2025-05-21 13:34:01.498 32754   676 V OpenSSLWrapper: verify_callback error: num=19 : self-
signed certificate in certificate chain
2025-05-21 13:34:01.498 32754   676 V OpenSSLWrapper: verify_callback: preverify not ok
2025-05-21 13:34:01.499 32754   676 E OpenSSLWrapper: SSL_connect() failure
2025-05-21 13:34:01.499 32754   676 E OpenSSLWrapper: error:16000069:STORE
routines::unregistered scheme in crypto/store/store_register.c (ossl_store_get0_loader_int):
237 data: scheme=file flags: 3
2025-05-21 13:34:01.499 32754   676 E OpenSSLWrapper: error:80000002:system library::No such
file or directory in providers/implementations/storemgmt/file_store.c (file_open): 267 data:
calling stat(/usr/local/ssl/certs) flags: 3
2025-05-21 13:34:01.499 32754   676 E OpenSSLWrapper: error:16000069:STORE
routines::unregistered scheme in crypto/store/store_register.c (ossl_store_get0_loader_int):
237 data: scheme=file flags: 3
2025-05-21 13:34:01.499 32754   676 E OpenSSLWrapper: error:80000002:system library::No such
file or directory in providers/implementations/storemgmt/file_store.c (file_open): 267 data:
calling stat(/usr/local/ssl/certs) flags: 3
2025-05-21 13:34:01.499 32754   676 E OpenSSLWrapper: error:16000069:STORE
routines::unregistered scheme in crypto/store/store_register.c (ossl_store_get0_loader_int):
237 data: scheme=file flags: 3
2025-05-21 13:34:01.499 32754   676 E OpenSSLWrapper: error:80000002:system library::No such
file or directory in providers/implementations/storemgmt/file_store.c (file_open): 267 data:
calling stat(/usr/local/ssl/certs) flags: 3
2025-05-21 13:34:01.499 32754   676 E OpenSSLWrapper: error:16000069:STORE
routines::unregistered scheme in crypto/store/store_register.c (ossl_store_get0_loader_int):
237 data: scheme=file flags: 3
2025-05-21 13:34:01.499 32754   676 E OpenSSLWrapper: error:80000002:system library::No such
file or directory in providers/implementations/storemgmt/file_store.c (file_open): 267 data:
calling stat(/usr/local/ssl/certs) flags: 3
2025-05-21 13:34:01.499 32754   676 E OpenSSLWrapper: error:0A000086:SSL
routines::certificate verify failed in ssl/statem/statem_clnt.c
(tls_post_process_server_certificate): 1890 data:  flags: 0
2025-05-21 13:34:01.499 32754   676 V OpenSSLWrapper: SSL_context 0xb400007999c15080
deallocated for SSL: 0xb400007999aa0000
2025-05-21 13:34:01.500 32754   676 D =ConnectionManager: SSL connection to
acumencertdomain.net:443 failed
2025-05-21 13:34:01.501 32754   676 D =ConnectionManager: cert error: 19
2025-05-21 13:34:01.502 32754   676 I =SteadyStateMipTlsCallback: onCertificateError: 19
2025-05-21 13:34:01.503 32754   676 I =SteadyStateMipTlsCallback: onFailed:
SERVER_CERTIFICATE_ERROR
2025-05-21 13:34:01.504 32754   676 D =ProvisionManager: slot: REPORT_AUDIT_EVENT
2025-05-21 13:34:01.504 32754   676 D =ConnectionManager: Failed to open MIP socket.
2025-05-21 13:34:01.505 32754   676 D =ConfigMarshaller: slot: CONNECTION_CLOSED
2025-05-21 13:34:01.506 32754   676 D =ConfigMarshaller: slot: CONNECTION_ERROR
```

Note: The certificate used for policy signing is the same as the one used for TLS communications. During the initial handshake, the MDM agent (TOE) validates the certificate for TLS. Since this initial authentication is successful, the subsequent checks for policy signatures using the same certificate will also pass, as the certificate has already been verified as valid.

Requirement	Auditable Events	Additional Audit Record Contents
FMT_SMF_EXT.4	Outcome (Success/failure) of function.	No additional information.

Success:

```
2025-06-02 14:06:11.213  8924 10572 D =ConnectionManager: Connected to acumencertdomain.net:443
2025-06-02 14:06:11.214  8924 10572 D =ProvisionManager: slot: REPORT_AUDIT_EVENT_NAME
2025-06-02 14:06:11.215  8924 10572 D =ConfigMarshaller: posting checkin command setting mode to MODE_AWAITING_GUP
2025-06-02 14:06:11.216  8924 10572 D =MAIManager: logMAIState reason: 1
2025-06-02 14:06:11.217  8924 10572 W =MAIManager: client config not registered. Aborting logMAIState.
2025-06-02 14:06:11.218  8924 10572 D =ConfigMarshaller: posting MICheckInCommand
2025-06-02 14:06:11.219  8924 10572 I =ProtocolEngine: put command: CONNECT
2025-06-02 14:06:11.220  8924 10572 D =RegisterActivity: wait for signal AUTH_REQUIREMENTS...
2025-06-02 14:06:11.220  8924  9536 D =ProtocolEngine: Got command CONNECT queue size now = 0
2025-06-02 14:06:11.221  8924  9536 I =CommandHandler: process() command CONNECT
2025-06-02 14:06:11.222  8924  9536 I =CommandHandler: Check in, forceConnect:true
2025-06-02 14:06:11.223  8924  9536 I =ProtocolEngine: put command: GET_UPDATED_PROFILE
2025-06-02 14:06:11.223  8924  9536 D =ProtocolEngine: Got command GET_UPDATED_PROFILE queue size now = 0
2025-06-02 14:06:11.224  8924  9536 I =CommandHandler: process() command GET_UPDATED_PROFILE
2025-06-02 14:06:11.225  8924  9536 I =CommandHandler: GetUpdateProfile
2025-06-02 14:06:11.226  8924  9536 I =MIClientProfile: Empty cookie, sending registration request
2025-06-02 14:06:11.227  8924  9536 D =MISendTask: Have work to do
2025-06-02 14:06:11.228  8924  9537 D =AbstractMIReceivingState: Get an event, typeCode:1000
2025-06-02 14:06:11.229  8924  9537 D =MISendTask: Found work without waiting
2025-06-02 14:06:11.230  8924  9537 I =ConnectionManager: Send to: https://acumencertdomain.net/Enrollment/RegMode
```

Failure:

	ACTION	STATE	PERFORM...	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
	Retire	Failed	admin	Fri Feb 28 2025 22:25:05 GMT+0...	Fri Feb 28 2025 22:25:05 GMT+000...	admin (Android 14.0 - PDA 8)	This is to test FMT_UNR_EXT.1 Test#1 - Failure Reason: Mobile platform not supported

FMT_UNR_EXT.1	[Attempt to unenroll]	No additional information.

	ACTION	STATE	PERFORM...	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
	Retire	Failed	admin	Fri Feb 28 2025 22:25:05 GMT+0...	Fri Feb 28 2025 22:25:05 GMT+000...	admin (Android 14.0 - PDA 8)	This is to test FMT_UNR_EXT.1 Test#1 - Failure Reason: Mobile platform not supported

Table 8: Management activities audit logs

SFR	Management Actions
1. FMT_SMF.1.1(1)	Transition to the locked state.

	ACTION	STATE	PERFORMED ...	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
	Lock	Success	admin	Mon Mar 24 2025 20:22:31 GMT+...	Mon Mar 24 2025 20:22:31 GMT+0000 (...	admin (Android 14.0 - PDA 12)	This is to test FMT_SMF.1.1(1) Test#1
	Lock Device (Android)	Acknowl...	<MDM>	Mon Mar 24 2025 20:22:31 GMT+...	Mon Mar 24 2025 20:22:34 GMT+0000 (...	admin (Android 14.0 - PDA 12)	Completed MDM request.

2. FMT_SMF.1.1(1)	Full wipe of protected data.

ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Wipe	Pending	admin	Wed Mar 26 2025 13:48:06 ...	Wed Mar 26 2025 13:48:06 GMT+00...	admin (Android 14.0 - PDA 12)	Device is in a wipe state
Wipe	Success	admin	Wed Mar 26 2025 13:48:01 ...	Wed Mar 26 2025 13:48:01 GMT+00...	admin (Android 14.0 - PDA 12)	This is to to test selection - 2 of FMT_SMF.1.1(1) Test#1
Wipe Device (Android)	Acknowl...	<MDM>	Wed Mar 26 2025 13:48:01 ...	Wed Mar 26 2025 13:48:06 GMT+00...	admin (Android 14.0 - PDA 12)	Completed MDM request.

3. FMT_SMF.1.1(1)	Unenroll the Android device.

ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Wipe	Pending	admin	Wed Mar 26 2025 13:48:06 ...	Wed Mar 26 2025 13:48:06 GMT+00...	admin (Android 14.0 - PDA 12)	Device is in a wipe state
Wipe	Success	admin	Wed Mar 26 2025 13:48:01 ...	Wed Mar 26 2025 13:48:01 GMT+00...	admin (Android 14.0 - PDA 12)	This is to to test selection - 2 of FMT_SMF.1.1(1) Test#1
Wipe Device (Android)	Acknowl...	<MDM>	Wed Mar 26 2025 13:48:01 ...	Wed Mar 26 2025 13:48:06 GMT+00...	admin (Android 14.0 - PDA 12)	Completed MDM request.

Note: The MDM agent (mobile device) get unenrolled when a wipe is issued.

4. FMT_SMF.1.1(1)	Install policies on an Android Device.

ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Apply Label To Policy	Success	admin	Tue Mar 25 2025 20:...	Tue Mar 25 2025 20:15:40 GMT+00...	Android WallPaper - FMT_SMF_install_pol...	Label 'Android' is applied to policy 'FMT_SMF_install_policy'.
Activate Policy	Success	admin	Tue Mar 25 2025 20:...	Tue Mar 25 2025 20:13:57 GMT+00...	Android WallPaper - FMT_SMF_install_pol...	Policy 'FMT_SMF_install_policy' is activated successfully.
Modify Policy Priority	Success	admin	Tue Mar 25 2025 20:...	Tue Mar 25 2025 20:13:57 GMT+00...	Android WallPaper - FMT_SMF_install_pol...	The priority for policy 'FMT_SMF_install_policy' is modified.
Add Policy	Success	admin	Tue Mar 25 2025 20:...	Tue Mar 25 2025 20:13:57 GMT+00...	Android WallPaper - FMT_SMF_install_pol...	Policy 'FMT_SMF_install_policy' is added successfully.

5. FMT_SMF.1.1(1)	Query connectivity status of an Android device.

ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Wakeup	Success	admin	Tue Aug 05 2025 11:25:46 GMT-0...	Tue Aug 05 2025 11:25:46 GMT-...	admin (Android 13.0 - PDA 13)	Request for Force Device Check-In.
Profile Change	Acknowledged	<MDM>	Tue Aug 05 2025 11:25:46 GMT-0...	Tue Aug 05 2025 11:25:49 GMT-...	admin (Android 13.0 - PDA 13)	Completed MDM request.

Note: The EPMM server (Admin portal) does not provide a specific query to retrieve this information; instead, it is accessed via the Devices section, which displays connectivity status, device firmware, hardware, and installed mobile apps after the MDM agent has checked in to the server.

6. FMT_SMF.1.1(1)	Query the current version of the Android device's firmware/software.

Refer the FMT_SMF.1.1(1) audit logs for 'Query connectivity status of an Android device' management action.

7. FMT_SMF.1.1(1)	Query the current version of the Android device's hardware.

Refer the FMT_SMF.1.1(1) audit logs for 'Query connectivity status of an Android device' management action.

8. FMT_SMF.1.1(1)	Query the current version of the Android device's installed mobile applications.

Refer the FMT_SMF.1.1(1) audit logs for 'Query connectivity status of an Android device's management action.

9. FMT_SMF.1.1(1)	Import X.509v3 certificates into the Android device's Trust Anchor Database.

ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Add Configuration	Success	admin	Tue Mar 25 2025 18:...	Tue Mar 25 2025 18:26:40 GMT+0...	Certificate - FMT_SMF.1.1(1) Te...	Configuration FMT_SMF.1.1(1) Test#1 added

10. FMT_SMF.1.1(1)	Install an application on an Android device.

ACTION	STATE	PERFOR...	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Modify App	Success	admin	Tue Mar 25 2025 17:28:30 GMT+0...	Tue Mar 25 2025 17:28:30 GMT+0...	Slack (Android - Public)	Application 'Slack' supported on Android platform is updated to catalog
Save Restrictions for A...	Success	admin	Tue Mar 25 2025 17:28:30 GMT+0...	Tue Mar 25 2025 17:28:30 GMT+0...	com.Slack	Successfully saved restrictions
Modify App	Success	admin	Tue Mar 25 2025 17:27:19 GMT+0...	Tue Mar 25 2025 17:27:19 GMT+0...	Slack (Android - Public)	Application 'Slack' supported on Android platform is updated to catalog
Save Restrictions for A...	Success	admin	Tue Mar 25 2025 17:27:19 GMT+0...	Tue Mar 25 2025 17:27:19 GMT+0...	com.Slack	Successfully saved restrictions
Add App	Success	admin	Tue Mar 25 2025 17:26:43 GMT+0...	Tue Mar 25 2025 17:26:43 GMT+0...	Slack (Android - Public)	Application 'Slack' supported on Android platform is added to catalog

ACTION	STATE	PERFOR...	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Apply Label To App	Success	admin	Tue Mar 25 2025 17:29:42 GMT+0...	Tue Mar 25 2025 17:29:42 GMT+0...	Slack (Android - Public)	Label 'FMT_SMF.1.1(3)' is applied to application 'Slack'.

ACTION	STATE	PERFORM...	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Apply Label	Success	admin	Tue Mar 25 2025 17...	Tue Mar 25 2025 17:40:42 GMT+0...	admin (Android 14.0 - PDA 12)	Label: 'FMT_SMF.1.1(3)' applied to devices. Number of associated policies: 0. Number of associated configurations: 0.

11. FMT_SMF.1.1(1)	Update the EPMM software on an Android device.

ACTION	STATE	PERFOR...	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Apply Label To Policy	Success	admin	Tue Mar 25 2025 19:...	Tue Mar 25 2025 19:06:09 GMT+...	Android Firmware - FMT_SMF.1_update_policy : ...	Label 'Android' is applied to policy 'FMT_SMF.1_update_policy'.
Activate Policy	Success	misystem	Tue Mar 25 2025 19:...	Tue Mar 25 2025 19:04:41 GMT+...	Android Firmware - FMT_SMF.1_update_policy : ...	Policy 'FMT_SMF.1_update_policy' is activated successfully.
Modify Policy Priority	Success	misystem	Tue Mar 25 2025 19:...	Tue Mar 25 2025 19:04:41 GMT+...	Android Firmware - FMT_SMF.1_update_policy : ...	The priority for policy 'FMT_SMF.1_update_policy' is modified.
Add Policy	Success	misystem	Tue Mar 25 2025 19:...	Tue Mar 25 2025 19:04:41 GMT+...	Android Firmware - FMT_SMF.1_update_policy : ...	Policy 'FMT_SMF.1_update_policy' is added successfully.

ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Profile Change	Acknowl...	<MDM>	Tue Mar 25 2025 19:...	Tue Mar 25 2025 19:09:08 GMT+0...	admin (Android 14.0 - PDA 12)	Completed MDM request.

12. FMT_SMF.1.1(1)	Remove an application from an Android device.

ACTION	STATE	PERFORME...	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Remove Label From App	Success	admin	Tue Mar 25 2025 19:...	Tue Mar 25 2025 19:23:48 GMT+0000...	Slack (Android - Public)	Label 'FMT_SMF.1.1(3)' is removed from application 'Slack'.

13. FMT_SMF.1.1(1)	Update an Android device's Password Policy that includes specifying: • Minimum password length • Minimum password complexity and • Maximum password lifetime.

ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Modify Policy	Success	admin	2024-08-27 02:21:20...	2024-08-27 02:21:20...	Security - FMT_POL_EXT.1 : Ve...	Policy 'FMT_POL_EXT.1' is ...

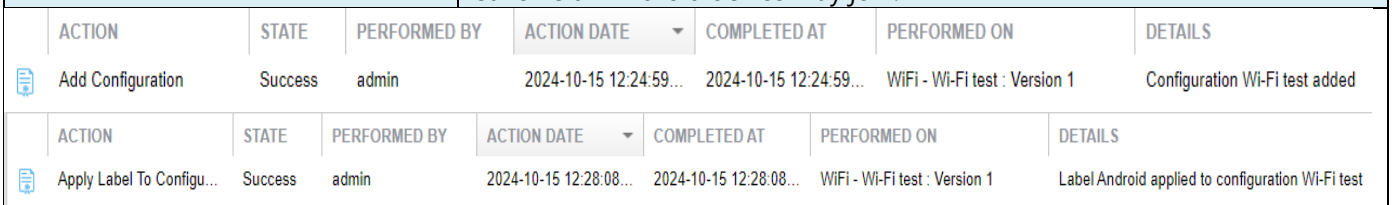
Note: The password length, password complexity and password lifetime parameters were modified in the security policy.

14. FMT_SMF.1.1(1)	Update an Android device's Session Locking Policy that includes specifying: • Screen-lock enable/disable, • Screen-lock timeout, • Number of authentication attempts.

ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Modify Policy	Success	admin	2024-08-27 02:53:04...	2024-08-27 02:53:04...	Security - FMT_POL_EXT.1 : Ve...	Policy 'FMT_POL_EXT.1' is ...

Note: While the screen-locking parameter was enabled, screen-lock timeout and number of authentication attempts were modified in the security policy.

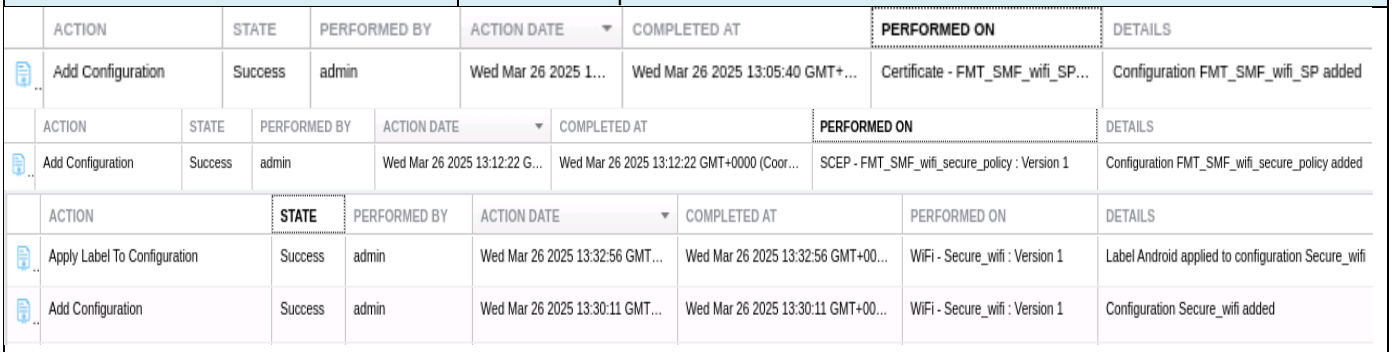
15. FMT_SMF.1.1(1)	Update an Android device's wireless network Policy that defines which networks an Android device may join.



ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Add Configuration	Success	admin	2024-10-15 12:24:59...	2024-10-15 12:24:59...	WiFi - Wi-Fi test : Version 1	Configuration Wi-Fi test added

ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Apply Label To Configu...	Success	admin	2024-10-15 12:28:08...	2024-10-15 12:28:08...	WiFi - Wi-Fi test : Version 1	Label Android applied to configuration Wi-Fi test

16. FMT_SMF.1.1(1)	Update the Security Policy for each wireless network that • Specifies the FQDN of acceptable WLAN authentication server certificates. • Specifies the security type. • Specifies the authentication protocol. • Specifies the client credentials to be used for authentication.

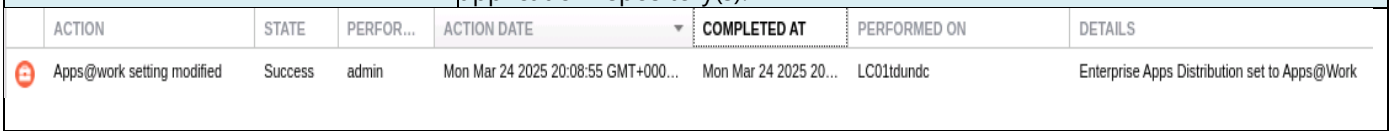


ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Add Configuration	Success	admin	Wed Mar 26 2025 1...	Wed Mar 26 2025 13:05:40 GMT+...	Certificate - FMT_SMF_wifi_SP...	Configuration FMT_SMF_wifi_SP added

ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Add Configuration	Success	admin	Wed Mar 26 2025 13:12:22 G...	Wed Mar 26 2025 13:12:22 GMT+0000 (Coor...	SCEP - FMT_SMF_wifi_secure_policy : Version 1	Configuration FMT_SMF_wifi_secure_policy added

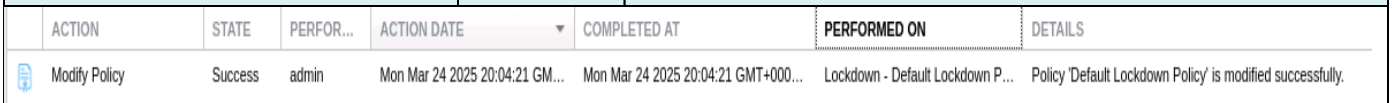
ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Apply Label To Configuration	Success	admin	Wed Mar 26 2025 13:32:56 GMT...	Wed Mar 26 2025 13:32:56 GMT+00...	WiFi - Secure_wifi : Version 1	Label Android applied to configuration Secure_wifi
Add Configuration	Success	admin	Wed Mar 26 2025 13:30:11 GMT...	Wed Mar 26 2025 13:30:11 GMT+00...	WiFi - Secure_wifi : Version 1	Configuration Secure_wifi added

17. FMT_SMF.1.1(1)	Specify an application installation policy that specifies an authorized application repository(s).



ACTION	STATE	PERFOR...	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Apps@work setting modified	Success	admin	Mon Mar 24 2025 20:08:55 GMT+000...	Mon Mar 24 2025 20...	LC01tdundc	Enterprise Apps Distribution set to Apps@Work

18. FMT_SMF.1.1(1)	Update an Android device's enable/disable Policy for • Camera • microphone



ACTION	STATE	PERFOR...	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Modify Policy	Success	admin	Mon Mar 24 2025 20:04:21 GM...	Mon Mar 24 2025 20:04:21 GMT+000...	Lockdown - Default Lockdown P...	Policy 'Default Lockdown Policy' is modified successfully.

Note: The default lockdown policy was modified to disable camera and microphone.

19. FMT_SMF.1.1(2)	Configure devices by specifying o a unique device ID o a number of devices

Configure the devices specified by a unique device ID:

ACTION	STATE	PERFORME...	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Register Device	Success	admin	Thu Mar 20 2025 19:28:43 GM...	Thu Mar 20 2025 19:28:43 GMT+0...	admin (Android 14.0 - PDA 12)	Device is fully registered
Create Device Certificate	Success	misystem	Thu Mar 20 2025 19:28:43 GM...	Thu Mar 20 2025 19:28:43 GMT+0...	admin (Android 14.0 - PDA 12)	SCEP Name: 'System - Mutual Auth CE setting', Serial Number: '125',
Apply Multiple Labels to...	Success	misystem	Thu Mar 20 2025 19:20:32 GM...	Thu Mar 20 2025 19:20:32 GMT+0...	admin (Android - PDA 12)	Label: 'Android,Company-Owned,All-Smartphones' applied to devices. Number of associated polici...
Profile Change	Acknowl...	<MDM>	Thu Mar 20 2025 19:20:32 GM...	Thu Mar 20 2025 19:28:44 GMT+0...	admin (Android 14.0 - PDA 12)	Completed MDM request.
Send Message	Failed	admin	Thu Mar 20 2025 19:20:27 GM...	Thu Mar 20 2025 19:20:27 GMT+0...	admin (Android - PDA 12)	Message to notify registration details via email - Failure Message: Failed to send message to the d...
Send Message	Initiated	admin	Thu Mar 20 2025 19:20:27 GM...	Thu Mar 20 2025 19:20:27 GMT+0...	admin (Android - PDA 12)	Message to notify registration details via email
Register Device	Success	admin	Thu Mar 20 2025 19:20:27 GM...	Thu Mar 20 2025 19:20:27 GMT+0...	admin (Android - PDA 12)	Created a client profile for Admin for device 24c05392-0b0b-45ed-87ed-3709b08f6752 with phone ...

Configure the number of devices allowed:

ACTION	STATE	PERFORMED BY	ACTION DATE	COMP...	PERFORMED ON	DETAILS
Preference Config Changes	Success	misystem	Fri Jul 25 2025 10:24:25 GMT...	Fri Jul ...	System	Modify Preference limitDevices from 1 to 6
Admin Portal Sign In	Success	admin	Fri Jul 25 2025 10:05:49 GMT...	Fri Jul ...	Admin Portal - 1...	Successfully Signed In

20. FMT_SMF.1.1(3)	Configure application access groups

ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Add Label	Success	admin	Fri Mar 21 2025 18:21:23 GM...	Fri Mar 21 2025 18:21:23 GMT+00...	FMT_SMF.1.1(3)	Label 'FMT_SMF.1.1(3)' is added successfully.

21. FMT_SMF.1.1(3)	Download applications.

ACTION	STATE	PERFORM...	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Apply Label	Success	admin	Tue Mar 25 2025 17...	Tue Mar 25 2025 17:40:42 GMT+0...	admin (Android 14.0 - PDA 12)	Label: 'FMT_SMF.1.1(3)' applied to devices. Number of associated policies: 0. Number of associated configurations: 0.

22. FMT_SMF_EXT.4.1	Import the certificates to be used for authentication of MDM Agent communications

ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Add Configuration	Success	admin	Tue Mar 25 2025 18:...	Tue Mar 25 2025 18:26:40 GMT+0...	Certificate - FMT_SMF.1.1(1) Te...	Configuration FMT_SMF.1.1(1) Test#1 added

ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Apply Label To Configuration	Success	admin	Tue Mar 25 2025 18:...	Tue Mar 25 2025 18:33:14 GMT...	Certificate - FMT_SMF.1.1(1) Te...	Label Android applied to configuration FMT_SMF.1.1(1) Test#1

ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Profile Change	Acknowledged	<MDM>	Tue Mar 25 2025 18:...	Tue Mar 25 2025 18:36:13 GMT+0000 (C...	admin (Android 14.0 - PDA 12)	Completed MDM request.

23. FMT_SMF_EXT.4.2	Enroll in management

ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Register Device	Success	admin	Mon Jun 02 2025 14:07:09 ...	Mon Jun 02 2025 14:07:09 GMT-04...	admin (Android 14.0 - PDA 13)	Device is fully registered
Create Device Certificate	Success	misystem	Mon Jun 02 2025 14:07:09 ...	Mon Jun 02 2025 14:07:09 GMT-04...	admin (Android 14.0 - PDA 13)	SCEP Name: 'System - Mutual Auth CE setting', Serial Number: '138',
Apply Multiple Labels t...	Success	misystem	Mon Jun 02 2025 14:05:18 ...	Mon Jun 02 2025 14:05:18 GMT-04...	admin (Android - PDA 13)	Label: 'Android,Company-Owned,All-Smartphones' applied to devices. Number of associated policies: 2. Number of associated ...
Profile Change	Acknowledged	<MDM>	Mon Jun 02 2025 14:05:18 ...	Mon Jun 02 2025 14:07:10 GMT-04...	admin (Android 14.0 - PDA 13)	Completed MDM request.
Send Message	Failed	admin	Mon Jun 02 2025 14:05:14 ...	Mon Jun 02 2025 14:05:14 GMT-04...	admin (Android - PDA 13)	Message to notify registration details via email - Failure Message: Failed to send message to the device via Email. Reason: co...
Send Message	Initiated	admin	Mon Jun 02 2025 14:05:14 ...	Mon Jun 02 2025 14:05:14 GMT-04...	admin (Android - PDA 13)	Message to notify registration details via email
Register Device	Success	admin	Mon Jun 02 2025 14:05:14 ...	Mon Jun 02 2025 14:05:14 GMT-04...	admin (Android - PDA 13)	Created a client profile for Admin for device cdf57504-2ec6-4f7b-b5ab-924522a50233 with phone number PDA 13

24. FMT_SMF_EXT.4.2	Configure whether users can unenroll from management

ACTION	STATE	PERFORME...	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Register Device	Success	admin	Thu Mar 20 2025 19:28:43 GM...	Thu Mar 20 2025 19:28:43 GMT+0...	admin (Android 14.0 - PDA 12)	Device is fully registered
Create Device Certificate	Success	misystem	Thu Mar 20 2025 19:28:43 GM...	Thu Mar 20 2025 19:28:43 GMT+0...	admin (Android 14.0 - PDA 12)	SCEP Name: 'System - Mutual Auth CE setting', Serial Number: '125',
Apply Multiple Labels to...	Success	misystem	Thu Mar 20 2025 19:20:32 GM...	Thu Mar 20 2025 19:20:32 GMT+0...	admin (Android - PDA 12)	Label: 'Android,Company-Owned,All-Smartphones' applied to devices. Number of associated polici...
Profile Change	Acknowl...	<MDM>	Thu Mar 20 2025 19:20:32 GM...	Thu Mar 20 2025 19:28:44 GMT+0...	admin (Android 14.0 - PDA 12)	Completed MDM request.
Send Message	Failed	admin	Thu Mar 20 2025 19:20:27 GM...	Thu Mar 20 2025 19:20:27 GMT+0...	admin (Android - PDA 12)	Message to notify registration details via email - Failure Message: Failed to send message to the d...
Send Message	Initiated	admin	Thu Mar 20 2025 19:20:27 GM...	Thu Mar 20 2025 19:20:27 GMT+0...	admin (Android - PDA 12)	Message to notify registration details via email
Register Device	Success	admin	Thu Mar 20 2025 19:20:27 GM...	Thu Mar 20 2025 19:20:27 GMT+0...	admin (Android - PDA 12)	Created a client profile for Admin for device 24c05392-0b0b-45ed-87ed-3709b08f6752 with phone ...

Note: Once enrolled, the MDM agent cannot be unenrolled directly from the device itself. Unenrolling the agent is an action that must be initiated through the MDM server (using wipe), as the EPMM system does not support unenrollment from the agent's end.

25. FMT_SMF_EXT.4.2	Configure periodicity of reachability events.

ACTION	STATE	PERFORM...	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Modify Policy	Success	admin	Fri May 30 2025 16:49:17 GMT-04...	Fri May 30 2025 16:49:17 GMT-...	Sync - Default Sync Policy : Version 11	Policy 'Default Sync Policy' is modified successfully.

ACTION	STATE	PERFORM...	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Profile Change	Acknowledged	<MDM>	Fri May 30 2025 16:49:22 GMT-0400 (Eastern Daylight Time)	Fri May 30 2025 16:51:59 GMT-0400 (Eastern Daylight Time)	admin (Android 14.0 - PDA 13)	Completed MDM request.

Table 9: Sample Audit Records (MDM Agent)

Requirement	SFR Source PP/Module /Functional Package	Auditable Events	Additional Audit Record Contents
Security audit (FAU)			
FAU_ALT_EXT.2	MOD_MDM_AGENT_V1.0	Success/failure of sending alert.	No additional information.

Alert from MDM agent to MDM server:

ACTION	STATE	PERFORMED BY	ACTION DATE	COMPLETED AT	PERFORMED ON	DETAILS
Profile Change	Acknowl...	<MDM>	Fri May 30 2025 12:30:48 GMT-...	Fri May 30 2025 12:34:28 GMT-040...	admin (Android 14.0 - PDA 13)	Completed MDM request.

Applied Policy:

```
2025-05-30 12:34:21.494  9850 10273 D MSPasswordManager: Create password policy. blockFingerprint:false, blockSmartLock:true->true, blockFaceUnlock:true, blockIrisScan:true,
SmartLocks: [Block SmartLocks - Bluetooth:true, Nfc:true, Location:false, Face:true, Onbody:false, Voice:false]
2025-05-30 12:34:21.495  9850 10273 D MSPasswordManager: needsInternalPasscodeConfig:false
2025-05-30 12:34:21.496  9850 10273 D MSPasswordManager: Password not required.
2025-05-30 12:34:21.497  9850 10273 D MSPasswordManager: Password policy is new or has changed. Applying.
2025-05-30 12:34:21.497  9850 10273 D MSPasswordManager: Applying password policy. Password quality:0
```

FAU_GEN.1(2)	MOD_MDM_AGENT_V1.0	None.	N/A

Requirement	SFR Source PP/Module /Functional Package	Auditable Events	Additional Audit Record Contents
FAU_SEL.1(2)	MOD_MDM_AGENT_V1.0	All modifications to the audit configuration that occur while the audit collection functions are operating.	No additional information.

Requirement	SFR Source PP/Module /Functional Package	Auditable Events	Additional Audit Record Contents

Audit data collection Function:

```
2025-08-28 10:39:58.267  6230  8324 I =ProvisionManager: AuditLog enabling result: true
2025-08-28 10:39:58.278  6230  8324 I =ProvisionManager: AuditLog level=ALERT success=true
comp=com.mobileiron.mdmpp/ProvisionManager log=AUDIT_CONFIGURATION_CHANGE : AuditLog
configuration changed: severityRule = 1 outcomeRule = 1 groupsRule = [1, 2, 3, 4, 5]
usersList = [0] events: [AUDIT_CONFIGURATION_CHANGE, TLS_SESSION_FAILURE,
TRANSITION_TO_LOCKED_STATE, ENROLLMENT_IN_MANAGEMENT, UNENROLLMENT_FROM_MANAGEMENT,
POLICY_VALIDATION_FAILURE, CA_CERTIFICATE_IMPORT, ID_CERTIFICATE_IMPORT,
CA_CERTIFICATE_REMOVE, ID_CERTIFICATE_REMOVE, INSTALL_APPLICATION, REMOVE_APPLICATION,
SYSTEM_SOFTWARE_UPGRADE, WAKEUP_FROM_SERVER, QUERY_CURRENT_SOFTWARE_VERSION,
QUERY_CURRENT_HARDWARE_VERSION, REPORT_APP_INVENTORY, UPLOAD_LOGS,
APP_STORE_QUARANTINE_ACTION_CONFIGURED, ENABLE_DISABLE_CAMERA, ENABLE_DISABLE_MIC,
ENABLE_DISABLE_VPN, ENABLE_DISABLE_RADIOS, ENABLE_DISABLE_DEVELOPMENT_MODE,
CONFIGURE_UNLOCK_BANNER, ENABLE_DISABLE_USB_TETHER, ENABLE_DISABLE_LOCATION_SERVICES,
ENABLE_DISABLE_BIOMETRICS]
```

Modified audit configuration:

```
2025-08-28 13:21:04.701  6230  8324 D =DeviceOwnerLockdownConfigurator: apply: DO lockdown
2025-08-28 13:21:04.702  6230 26149 D =TLV_LOG:         Version: 0x2
2025-08-28 13:21:04.703  6230  8182 D =TLV_LOG:         Length: 156
2025-08-28 13:21:04.704  6230  8324 D =DeviceSideLockdownConfigurator: apply: device side
lockdown
2025-08-28 13:21:04.705  6230 26149 D =TLV_LOG:         Flags (0x2): HBT=0, Ack=1, Nak=0,
Compress=0
2025-08-28 13:21:04.708  6230  8182 D =TLV_LOG:         SenderId: 0x40000043
2025-08-28 13:21:04.708  6230  8324 I =DevicePolicyManagerUtils: disabling screen capture
to false
2025-08-28 13:21:04.709  6230 26149 D =TLV_LOG:         Length: 40
2025-08-28 13:21:04.710  6230 26149 D =TLV_LOG:         SenderId: 0x0
2025-08-28 13:21:04.712  6230 26149 D =TLV_LOG:         RecieverId: 0x40000043
2025-08-28 13:21:04.712  6230  8182 D =TLV_LOG:         RecieverId: 0x0
2025-08-28 13:21:04.715  6230 26149 D =TLV_LOG:         PacketId: 381
2025-08-28 13:21:04.716  6230  8182 D =TLV_LOG:         PacketId: 382
2025-08-28 13:21:04.716  6230  8324 D =DevicePolicyManagerUtils: setting disable camera
to : false
2025-08-28 13:21:04.717  6230 26149 D =TLV_LOG:         Number of TLVs: 1
2025-08-28 13:21:04.718  6230  8182 D =TLV_LOG:         Number of TLVs: 1
2025-08-28 13:21:04.720  6230 26149 D =TLV_LOG:         TLV #0:
```

Requirement	SFR Source PP/Module /Functional Package	Auditable Events	Additional Audit Record Contents
FCS_TLSC_EXT.1	PKG_TLS_v1.1	Failure to establish a TLS session.	Reason for failure.
		Failure to verify presented identifier.	Presented identifier and reference identifier.
		Establishment/termination of a TLS session	Non-TOE endpoint of connection.

Connection Establishment:

```
2025-05-21 16:26:47.999 32754   676 D =ConnectionManager: Connected to
acumencertdomain.net:443
```

```
Termination of TLS connection:
2025-05-21 17:16:21.270 32754   677 D =ConfigMarshaller: slot: CONNECTION_CLOSED
```

```
Failure to establish TLS session:
2025-08-20 17:00:37 616 12340 12762 D =ConnectionManager: SSL connection to
acumencertdomain.net:443 failed
```

```
Reason for failure:
Wrong certificate:
```

```
2025-08-20 17:00:37 614 12340 12762 E OpenSSLWrapper: error:0A00017F:SSL routines::wrong
certificate type in ssl/statem/statem_clnt c (tls_post_process_server_certificate): 1920
data:  flags: 1
```

```
Unknown Cipher:
2025-05-22 10:37:10 696 32754   676 E OpenSSLWrapper: SSL_connect() failure
```

```
2025-05-22 10:37:10 696 32754   676 E OpenSSLWrapper: error:0A0000F8:SSL routines::unknown
cipher returned in ssl/statem/statem_clnt c (set_client_ciphersuite): 1313 data:  flags: 1
```

```
Unsupported protocol:
2025-05-22 11:04:51 442 32754   677 E OpenSSLWrapper: SSL_connect() failure
```

```
2025-05-22 11:04:51 443 32754   677 E OpenSSLWrapper: error:0A000102:SSL
routines::unsupported protocol in ssl/statem/statem_lib c (ssl_choose_client_version): 1962
data:  flags: 1
Wrong cipher:
2025-05-22 11:55:15 567 32754   676 E OpenSSLWrapper: SSL_connect() failure
```

```
2025-05-22 11:55:15 567 32754   676 E OpenSSLWrapper: error:0A000105:SSL routines::wrong
cipher returned in ssl/statem/statem_clnt c (set_client_ciphersuite): 1329 data:  flags: 1
```

```
Bad Signature:
2025-05-27 11:15:13 633  3537  4001 E OpenSSLWrapper: error:1C880004:Provider routines::RSA
lib in providers/implementations/signature/rsa_sig c (rsa_verify): 774 data:  flags: 1
```

```
2025-05-27 11:15:13 633  3537  4001 E OpenSSLWrapper: error:0A00007B:SSL routines::bad
signature in ssl/statem/statem_clnt c (tls_process_key_exchange): 2306 data:  flags: 1
```

```
Failure to verify presented identifier:
```

```
2025-05-21 17:16:21 259 32754   677 V OpenSSLWrapper: verify_callback error: num=62 :
hostname mismatch
```

```
Presented Identifier and reference identifier:
```

```
2025-05-21 16:15:58.771 32754 32754 D =BaseFragment: showDialogWithDismissButton: twoButton=
false, message= The server connection is rejected because an unsafe SSL certificate is
detected. Details: Hostname mismatch. Connecting to host: acumencertdomain.net; name in
certificate:  acumencert.net
```

Identification and authentication (FIA)

<table>
<tr><th>Requirement</th><th>SFR Source PP/Module /Functional Package</th><th>Auditable Events</th><th>Additional Audit Record Contents</th></tr>
<tr><td>FIA_ENR_EXT.2</td><td>MOD_MDM_AGENT_V 1.0</td><td>Enrollment in management.</td><td>Reference identifier of MDM Server.</td></tr>
<tr><td colspan="4">Enrolment with reference identifier of server:
2025-06-02 16:05:18.481 2763 3111 I =ConnectionManager: Send to:
https://acumencertdomain.net/Enrollment/RegMode</td></tr>
<tr><td>FIA_X509_EXT.1(1)</td><td>PP_MDM_V4.0</td><td>Failure to validate X.509 certificate.</td><td>Reason for failure.</td></tr>
<tr><td colspan="4">Failure to validate X.509 certificate :
2025-05-23 14:03:26.550 3537 4000 D =ConnectionManager: SSL connection to acumencertdomain.net:443 failed 2025-05-23 14:03:26.552 3537 4000 D =ConnectionManager: cert error: 79 2025-05-23 14:03:26.553 3537 4000 I =SteadyStateMipTlsCallback: onCertificateError: 79 2025-05-23 14:03:26.554 3537 4000 I =SteadyStateMipTlsCallback: onFailed: SERVER_CERTIFICATE_ERROR

Reason for Failure:
Invalid CA:
2025-05-23 13:51:50 094 3537 4000 V OpenSSLWrapper: verify_callback error: num=79 : invalid CA certificate

Expired certificate:
2025-05-23 10:36:59 714 3537 4000 V OpenSSLWrapper: verify_callback error: num=10 : certificate has expired

Revoked certificate:
2025-08-21 16:35:28 806 5130 5969 W =CrlUtils: checkOCSP: java security cert CertPathValidatorException: Certificate has been revoked, reason: UNSPECIFIED, revocation date: Wed Aug 06 11:11:09 EDT 2025, authority: EMAILADDRESS=info@acumen net, CN=intermediate_responder, OU=CC, O=Acumen, L=Rockville, ST=MD, C=US, extension OIDs: []
2025-08-21 16:35:28 807 5130 5969 W =CrlUtils: Revoked certificate serial number: 13c1ed31d944f3fe</td></tr>
<tr><td>FIA_X509_EXT.2</td><td>PP_MDM_V4.0</td><td>Failure to establish connection to determine revocation status.</td><td>No additional information.</td></tr>
</table>

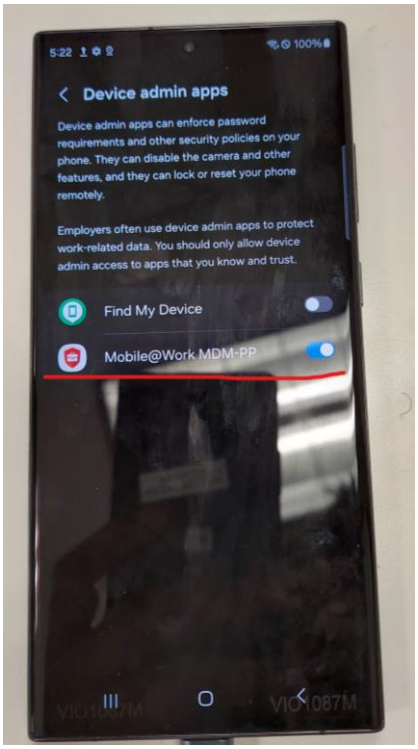
Requirement	SFR Source PP/Module /Functional Package	Auditable Events	Additional Audit Record Contents
			

2025-08-21 15:07:07 801 5130 5130 D =BaseFragment: showDialogWithDismissButton: twoButton= false, message= There was an error in certificate validation Please contact your administrator

2025-08-21 15:07:07 801 5130 5130 D =BaseFragment: Error (The certificate for this server doesn't have a CRL Serial Number: 40c0918df0ada03c, Subject: 1 2 840 113549 1 9 1=#160f696e666f406163756d656e2e6e6574,CN= acumencertdomain.net,OU=CC,O=Acumen,L=Rockville,ST=MD,C=US, Issuer: 1 2 840 113549 1 9 1=#160f696e666f406163756d656e2e6e6574,CN=ocsp_intermediate,OU=CC,O=Acumen,L=Rockville,ST=MD,C =US

Security management (FMT)			
FMT_POL_EXT.2	MOD_MDM_AGENT_V 1.0	Failure of policy validation.	Reason for failure of validation.
2025-08-20 15:51:08 927 12340 12751 W =PayloadSignatureVerifier: Payload signature verification failed with cert: wpLCjjFvw6BRFcKND8KcwrHCvcOjZsOqERfCogFp			
FMT_SMF_EXT.4	MOD_MDM_AGENT_V 1.0	Outcome (Success/failure) of function.	No additional information.

Requirement	SFR Source PP/Module /Functional Package	Auditable Events	Additional Audit Record Contents
Check -in : 2025-05-30 17:59:29.703 9850 10264 I =ConnectionManager: Send to: https://acumencertdomain.net/mifs/c/miprotocol/miclien 2025-05-30 17:59:29.704 9850 11272 D =TaskScheduler: Next action:Disconnect in 120.0 seconds 2025-05-30 17:59:29.705 9850 10264 D =TLV_LOG: ---------- SEND ---------- 2025-05-30 17:59:29.706 9850 11272 D =mobileiron:WakeupNotifyWorker: Register Wake Up in 120000 2025-05-30 17:59:29.708 9850 10264 D =TLV_LOG: Packet Decode: **Application install:** 2025-06-02 16:55:09.711 2763 23736 D =TLV_LOG: Type(0x51): (P) Update Application Inventory 2025-06-02 16:55:09.711 2763 3122 D =MSComplianceManager: PasswordManager: STATUS_COMPLIANT 2025-06-02 16:55:09.712 2763 23736 D =TLV_LOG: Request/Response: Response 2025-06-02 16:55:09.713 2763 3122 D =ComplianceThreadTracking: Calling getComplianceState on manager AfwDeviceOwnerManager 2025-06-02 16:55:09.714 2763 23736 D =TLV_LOG: Length: 4 2025-06-02 16:55:09.715 2763 23736 D =TLV_LOG: UpdateAppInventoryTLVHandler 2025-06-02 16:55:09.716 2763 23736 D =MITLVManager: processTLVs - opcode(0): 51 length: 4 2025-06-02 16:55:09.717 2763 23736 I =MITLVManager: Received TLV UpdateAppInventoryTLVHandler Response 2025-06-02 16:55:09.718 2763 23736 D =ProvisionManager: slot: REPORT_AUDIT_EVENT 2025-06-02 16:55:09.718 2763 3122 D =AccountManagerUtils: getManagedGooglePlayAccount: found - work-BA68205C210887A441040C3D49DC0A@android-for-work.gserviceaccount.com 2025-06-02 16:55:09.719 2763 23736 I =MISendTask: response: Success 2025-06-02 16:55:09.720 2763 3122 D =AfwConfigMarshaller: AppPolicy: package: com.Slack 2025-06-02 16:55:09.720 2763 23736 D =AbstractMIReceivingState: Get an event, typeCode:1000 2025-06-02 16:55:09.721 2763 3111 D =MISendTask: Success response received for (Q) Update Application Inventory 2025-06-02 16:55:09.722 2763 3122 D =AbstractAfwManager(DOM): checkCompliance: AFW app restrictions config in PENDING_ENABLE state: 1E3519D79982489BAA5490314C3F9DE673AADB76 com.Slack 2025-06-02 16:55:09.722 2763 23736 D =ProtocolEngine: commandsInProgress:true 2025-06-02 16:55:16.606 2763 2763 D =AppStoreWebViewClient: onPageStarted: https://acumencertdomain.net:7443/mifs/asfV3x/appstore?clientid=1073741879&vspver=12.3.1.0 2025-06-02 16:55:16.608 2763 2763 D =AppStoreWebChromeClient: AppStoreWebChromeClient: onProgressChanged: 22 2025-06-02 16:55:16.669 2763 2763 D =AppStoreWebChromeClient: AppStoreWebChromeClient: onProgressChanged: 100 2025-06-02 16:55:16.670 2763 2763 D =AppStoreWebChromeClient: AppStoreWebChromeClient: onProgressChanged: 100 2025-06-02 16:55:16.671 2763 2763 D =AppStoreWebViewClient: onPageFinished: https://acumencertdomain.net:7443/mifs/asfV3x/appstore?clientid=1073741879&vspver=12.3.1.0 2025-06-02 16:55:17.065 2763 15482 D =WebAppStoreFragment: isInstalledApp https://acumencertdomain.net:7443/mifs/c/apix/v4/appstore/apps/116/install/3361a6c3426969c8/111944842088068756939? clientid=1073741879&id=com.Slack&vc= 2025-06-02 16:55:17.066 2763 15482 D =WebAppStoreFragment: isInstalledApp for package: com.Slack = installed 2025-06-02 16:55:17.068 2763 15482 D =WebAppStoreFragment: isInstalledApp https://acumencertdomain.net:7443/mifs/c/apix/v4/appstore/apps/116/install/3361a6c3426969c8/111944842088068756939? clientid=1073741879&id=com.Slack&vc= 2025-06-02 16:55:17.069 2763 15482 D =WebAppStoreFragment: isInstalledApp for package: com.Slack = installed 2025-06-02 16:55:17.070 2763 15482 D =WebAppStoreFragment: isDowngradeApp: https://acumencertdomain.net:7443/mifs/c/apix/v4/appstore/apps/116/install/3361a6c3426969c8/111944842088068756939? clientid=1073741879&id=com.Slack&vc= 2025-06-02 16:55:17.072 2763 15482 D =WebAppStoreFragment: isInstalledApp https://acumencertdomain.net:7443/mifs/c/apix/v4/appstore/apps/116/install/3361a6c3426969c8/111944842088068756939? clientid=1073741879&id=com.Slack&vc= 2025-06-02 16:55:17.073 2763 15482 D =WebAppStoreFragment: isInstalledApp for package: com.Slack = installed 2025-06-02 16:55:17.075 2763 15482 D =WebAppStoreFragment: isInstalledApp			
FMT_UNR_EXT.1	MOD_MDM_AGENT_V 1.0	[Attempt to unenroll]	No additional information.

Requirement	SFR Source PP/Module /Functional Package	Auditable Events	Additional Audit Record Contents
  Note: The greyed-out functionality confirms that the user cannot unenroll when the device is configured in Device-Admin mode.			

11.1 AUDIT EVENTS AND THEIR CORRESPONDING MESSAGES

Table 10: Events and messages

Event	Description of when the event is logged	Message	Severity
Audit configuration change	A change in audit configuration (which is part of Samsung General Policy)	AUDIT_CONFIGURATION_CHANGE: AuditLog configuration changed: _ description_of_change Note: The value **_description_of_ change_** shows the current severity rule, current outcome rule, and the list of active audit groups, audit events, and UID list after the	Alert

Event	Description of when the event is logged	Message	Severity
		change. For example: severityRule = 5 outcomeRule = 2 groupsRule = [4] usersList = [0] events: [AUDIT_CONFIGURATION_ CHANGE, POLICY_APPLICATION]	
Transition to locked state	Device becomes locked either due to user action on the device or administrator action on EPMM.	TRANSITION_TO_LOCKED_STATE :	Transition to locked state
Policy validation failure	Finding a discrepancy in policy validation.	POLICY_VALIDATION_FAILURE: _ description_of_policy_error_	Error for policy errors. Warning for policy warnings.
CA certificate import	Installation (success or failure) of CA certificates.	CA_CERTIFICATE_IMPORT: Import of CA certificate _alias_ succeeded/failed	Notice if success. Error if failure.
ID certificate import	Installation (success or failure) of identity certificates.	ID_CERTIFICATE_IMPORT: Import of ID certificate _alias_ succeeded/failed	Notice if success. Error if. failure
CA certificate remove	Removal (success or failure) of CA certificates.	CA_CERTIFICATE_REMOVE: Removal of CA certificate _alias_ succeeded/failed	Notice if success. Error if failure.
ID certificate remove	Removal (success or failure) of identity certificates.	ID_CERTIFICATE_REMOVE: Removal of ID certificate _alias_ succeeded/failed	Notice
Install application	Installation of an application.	INSTALL_APPLICATION: _package_ name_	Notice
Remove application	Removal of an application.	REMOVE_APPLICATION: _package_ name_	Notice

Event	Description of when the event is logged	Message	Severity
Device OS upgrade	Device system software upgrade.	SYSTEM_SOFTWARE_UPGRADE: _ current_os_version_	Notice
Server request client checkin	Logs wakeup command from EPMM that results in a device checkin from Federal build.	WAKEUP_FROM_SERVER: CheckIn with server initiated	Notice
Request current software version	Attempt to fetch and report current software version.	QUERY_CURRENT_SOFTWARE_VERSION: _ OS_VERSION_	Notice
Request current hardware version	Attempt to fetch and report current hardware version.	QUERY_CURRENT_HARDWARE_VERSION: _ device_model_	Notice
Report app inventory	Attempt to report apps inventory.	REPORT_APP_INVENTORY: Reporting of app inventory succeeded/failed.	Notice if success. Error if failure
Upload logs	Attempt to upload logs to server.	UPLOAD_LOGS: Client logs uploaded/Client logs upload failed: _error_code_	Notice if success. Error if failure.
Configure App Store quarantine compliance action	Apps@Work (in Federal build) is quarantined or taken out of quarantine.	APP_STORE_QUARANTINE_ACTION_ CONFIGURED: Qurantined/Unquarantined	Notice
Enable/Disable camera	Enabling/disabling camera.	ENABLE_DISABLE_CAMERA: Enabled/Disabled	Notice
Enable/Disable mic	Enabling/disabling microphone.	ENABLE_DISABLE_MIC: Enabled/Disabled	Notice
Enable/Disable radios	Enabling/disabling any of Wi-Fi, NFC, cellular, or Bluetooth.	ENABLE_DISABLE_RADIOS: NFC/WIFI/Bluetooth enabled/disabled	Notice
Enable/Disable development mode	Enabling/disabling development mode.	ENABLE_DISABLE_DEVELOPMENT_MODE: Enabled/Disabled	Notice

Event	Description of when the event is logged	Message	Severity
Configure unlock banner	Changing and applying unlock banner policy.	CONFIGURE_UNLOCK_BANNER: Enabled/Disabled	Notice if success. Error if failure.
Enable/Disable usb tether	Enabling/disabling of USB tethering.	ENABLE_DISABLE_USB_TETHER: Enabled/Disabled	Notice
Enable/Disable location services	Enabling/disabling of location services.	ENABLE_DISABLE_LOCATION_SERVICES: Enabled/Disabled	Notice
Enable/Disable biometrics	Enabling/disabling biometric authentication.	ENABLE_DISABLE_BIOMETRICS: Fingerprint/Iris/Face unlock enabled/enabling failed.	Notice if success. Error if failure.
Failure to establish a TLS session	Failure in establishing TLS session, including noting any certificate error.	TLS_SESSION_FAILURE: _description_ of_failure_reason	Warning
TLS session established	Established TLS session with EPMM.	TLS_SESSION_ESTABLISHED:	Notice
TLS session terminated	Terminated TLS session with EPMM	TLS_SESSION_TERMINATED:	Warning
Failure to verify presented identity	Failure to verify presented identity	TLS_SESSION_FAILURE : The server connection is rejected because an unsafe SSL certificate is detected. Details: Hostname mismatch. <*Ivanti EPMM FQDN*> != <*hostname in the certificate*>	Warning
Android shutdown	Android is shutting down. This event belongs to the System audit group and is logged if the System group is selected in the **Audit** **Groups** field of the Samsung General Policy These events are logged	1541176318823 5/2/1/3377/1/ShutdownThread/Android will be shutdown	Notice

Event	Description of when the event is logged	Message	Severity
	by the Samsung device rather than Federal build so the format is different.		
Android startup completed	Android startup has completed. This event belongs to the System audit group and is logged if the System group is selected in the **Audit** **Groups** field of the Samsung General Policy These events are logged by the Samsung device rather than Federal build so the format is different.	1541176421450 5/2/1/3379/1/ActivityManagerService/Android boot completed	Notice

12 TERMS AND ABBREVIATIONS

Table 11: Terms and Abbreviations

Acronym	Definition
SAFE	In context of Samsung, SAFE stands for Samsung approved for enterprise.
AES	Advanced Encryption Standard
AOSP	Android Open Source Project
API	Application Programming Interface
APK	Android Package
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CN	Common Name
CRL	Certificate Revocation List
DN	Distinguished Name
DNS	Domain Name System
DSS	Digital Signature Standard

Acronym	Definition
ECC	Eliptic Curve Cryptography
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EP	Extended Package
EPMM	Endpoint Mobile Manager
FIPS	Federal Information Processing Standard
FRSE	Freed or secure from harm
GCM	Galois/Counter Mode
GUI	Graphical User Interface
HMAC	Hash-based Message Authentication Code
HTTP	HyperText Transfer Protocol
HTTP/TLS	HTTP over TLS or HTTPS
HTTPS	HyperText Transfer Protocol Secure (HTTP over TLS)
IETF	Internet Engineering Task Force
IP	Internet Protocol
KAS-ECC-SCC	Key Agreement Scheme (KAS)
KeyGen	Key Generation
LAN	Local Area Netork
MA	Mutual Authentication
MAM	Mobile Application Management
MAS	Mobile Application Store
MCM	Mobile Content Management
MD	Mobile Device
MDF	Mobile Device Fundamentals
MDM	Mobile Device Management
MIFS	MobileIron Admin Port (433 (default) or 8433)
MOD_MDM_AGENT_V1.0	PP-Module for MDM Agents, Version 1.0
NIAP	Nation Information Assurance Partnership
NIST	National Institute of Standards and Technology
N/A	Not Applicable
OCSP	Online Certificate Status Protocol
OE	Operational Environment
OS	Operating System
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PKG_TLS_V1.1	Functional Package for Transport Layer Security (TLS), Version 1.1
PP	Protection Profile
PP_MDM_V4.0	Protection Profile for Mobile Device Management, Version 4.0
PP-Module	Protection Profile Module
Pub	Publication

Acronym	Definition
RSA	Rivest, Shamir & Adleman
SAN	Subject Alternative Name
SAR	Security Assurance Requirement
SHA	Secure Hash Algorithm
SigGen	Signature Generation
SigVer	Signature Verification
SFR	Security Functional Requirement
SMS	Short Message Server
SMTP	Simple Mail Trasfer Protocol
SSH	Secure Shell
SSID	Service Set Identifier
ST	Security Target
TD	Technical Decisions
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Summary Functionality
TSS	TOE Summary Specification
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
WiFi	Wireless Fidelity
WLAN	Wireless LAN
WS	Work Station
XML	eXtensible Markup Language

Table 12: Terms and definitions

Term	Definition
Alert vs Event	An Alert is a asynchronous message sent verses an Event, which is a message sent as the result of an action.
Android Key Store	The Android Keystore system is a security feature that allows you to store cryptographic keys in a secure container, making them difficult to extract from the device. Once keys are stored in the keystore, they can be used for cryptographic operations while keeping the key material non-exportable.
AppConnect	AppConnect is an application integration software that connects app
Apps@Work	Apps@Work is an enterprise app storefront that facilitates the secure distribution of software and apps. It is integrated into Go app and Mobile@Work clients for iOS, Android and macOS.
Enterprise	The company data and applications the TOE protects.
MD User	A Mobile Device User.
MDM Agent	The name of the MDM Agent component of the TOE.
Push Notification	Push notifications are messages sent from any server to a user's device without the user explicitly requesting them. They are called "push" because the server pushes the information to the device. Push notifications are commonly used in mobile apps and web applications to alert users about important events, updates, or actions they need to take.
Trusted Front End (TSF)	A Trusted Front End (TFE) is a TLS inspection proxy that is installed between the untrusted network and Ivanti EPMM. The TFE intercepts and decrypts HTTPS network traffic, and when it determines that the final destination is Ivanti EPMM, it re-encrypts and forwards the traffic to EPMM. The devices that register to Ivanti EPMM must send HTTPS requests to the TFE rather than to Ivanti EPMM. The devices must use port 443. Also, the TFE must be provisioned with digital certificates that establish an identity chain of trust with a legitimate server verified by a trusted third-party certificate authority.