GovShield
User Guide v1.0

For GovShield Version 1.60.05 or later.

February 6, 2026

Table of Contents

Table of Figures

1 Introduction

This document is intended for administrators responsible for installing, configuring, and/or operating GovShield. Guidance provided in this document allows the reader to deploy the product in an environment that is consistent with the configuration that was evaluated as part of the product's Common Criteria (CC) testing process. It also provides the reader with instructions on how to exercise the security functions that were claimed as part of the CC evaluation. The reader is also expected to be familiar with the general operation of the GovShield product. This guidance also includes information on configuration of the behavior of the platforms upon which GovShield operates.

The reader is also expected to be familiar with the GovShield Version 1.60.05 Security Target and the general CC terminology that is referenced in it. This document references the Security Functional Requirements (SFRs) that are defined in the Security Target document and provides instructions on how to perform the security functions that are defined by these SFRs. The GovShield Version 1.60.05 product, as a whole, provides a great deal of security functionality but only those functions that were in the scope of the evaluation were assessed. Any functionality that is not described in the GovShield Version 1.60.05 Security Target was not evaluated and should be exercised at the user's risk.

GovShield is a Mobile Device Management (MDM) solution for Samsung Android devices. GovShield enforces security policies, access, and usage on managed mobile devices to reduce the risk of misuse. GovShield consists of a MDM Server (i.e., GovShield Server) and a client agent application (i.e., GovShield Client) installed on each managed Samsung Android device (evaluated configuration used Android 15 devices). Android Mobile Device platform's BoringSSL cryptographic module for cryptographic services and the use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE. Additionally, the evaluation does not make any claims of cryptographic strength for any other cryptographic modules or configurations besides what is claimed in the GovShield Version 1.60.05 Security Target. The GovShield Server provides capability to manage devices, users, security policies, and applications. This document will provide guidance on both the GovShield Server and the GovShield Client.

An administrator accesses the GovShield Server's web GUI by using a web browser and entering the GovShield Server's URL as defined in the MDM Properties File. Refer to the GovShield Installation Guide for additional information on defining the URL as part of the installation process. This is the only method of administering GovShield. Administrators will need to enter their username and password to authenticate to the web GUI and must be assigned the Admin role to gain access the web GUI.

The following are operating assumptions so that the operational objectives are fulfilled.

- Trusted components of the TOE: The administrators need to perform assessments and define compliance policies to verify the availability of all TOE components and their audit functions to reduce the risk of an undetected attack on (or failure of) one or more TOE components
- Availability of network connectivity: GovShield Server requires network connectivity in order to perform its functions, specifically its management of mobile devices. In cases where network connectivity is lost between TOE components, security on the mobile devices enrolled into the TOE's management is still enforced.
- Trustworthiness of server platform: The system on which the GovShield server application is installed and the local network that it resides is assumed to be configured securely and to have access to functionality, such as: reliable timestamps, user and group account management, logon and logout services via a local or network directory service, remote access control, and audit log management services.
- Trustworthiness of device platform: The Android GovShield Client will be installed on mobile devices configured in accordance with their own Common Criteria evaluated configurations and will provide access to functionality, such as policy enforcement, cryptographic services, data protection as well as trusted updates and software integrity verification of the GovShield Client.
- Trusted administration: Administrators are expected to be trusted individuals with relevant technical skills for administration of GovShield Server and are expected to read and abide by its configuration instructions, including this supplemental guidance.
- Proper users: Users of mobile devices are expected to not be willfully negligent or hostile and will use the mobile device in a manner that complies with their organizational security policies.

The following table, taken from the GovShield Version 1.60.05 Security Target, lists the commands and policies used to manage and configure the mobile devices being managed. The table lists the management functions that can be performed by an Administrator as well as whether this behavior is enforced by the GovShield Client or by the underlying mobile device platform. These management functions are described within this document.

Command	Claimed in VID11593[1]	Implemented By
1. transition to the locked state	Yes	GovShield Client
2. full wipe of protected data	Yes	GovShield Client

[1] TD0479

3. unenroll from management	Yes	GovShield Client
4. install policies	Yes	GovShield Client
5. query connectivity status	No	GovShield Client
6. query the current version of the MD firmware/software	No	GovShield Client
7. query the current version of the hardware model of the device	No	GovShield Client
8. query the current version of installed mobile applications	No	GovShield Client
9. import X.509v3 certificates into the Trust Anchor Database	Yes	GovShield Client
10. install applications	Yes	GovShield Client
11. update system software	Yes	Platform
12. remove applications	Yes	GovShield Client
13. remove Enterprise applications	Yes	GovShield Client
14. wipe Enterprise data	Yes	GovShield Client
16. alert the user	No	GovShield Client
25. password policy	Yes	GovShield Client
26. session locking policy	Yes	GovShield Client
27. wireless networks (SSIDs) to which the MD may connect	Yes	GovShield Client
28. security policy for each wireless network	Yes	GovShield Client
29. application installation policy	Yes	GovShield Client
30. enable/disable policy for camera and/or microphone across device	Yes	GovShield Client
32. enable/disable policy for cellular and/or NFC	Yes	GovShield Client
33. enable/disable policy for data signaling over USB and/or removable storage card (SD card)	No	GovShield Client
34. enable/disable policy for Wi-Fi tethering	No	GovShield Client
35. enable/disable policy for developer modes	Yes	GovShield Client
36. enable policy for data-at-rest protection	Yes	GovShield Client
37. enable policy for removable media's data-at-rest protection	Yes	GovShield Client
38. enable/disable policy for local authentication bypass	Yes	GovShield Client
47. the unlock banner policy	Yes	GovShield Client
49. enable/disable USB mass storage mode	Yes	GovShield Client
51. enable/disable Hotspot functionality authenticated by passcode	No	GovShield Client

55. enable/disable policy for use of Biometric Authentication Factor	Yes	GovShield Client
58. enable/disable automatic updates of system software	No	GovShield Client

2 Manage Devices

Device Management allows an admin user to whitelist devices, send message alerts to devices, and send commands to individual devices. The device management grid also provides information on each device, including the ID, the assigned name, the assigned policy & version, the operating system & version, the model name, the firmware version, and the last time the device checked in with the MDM server.

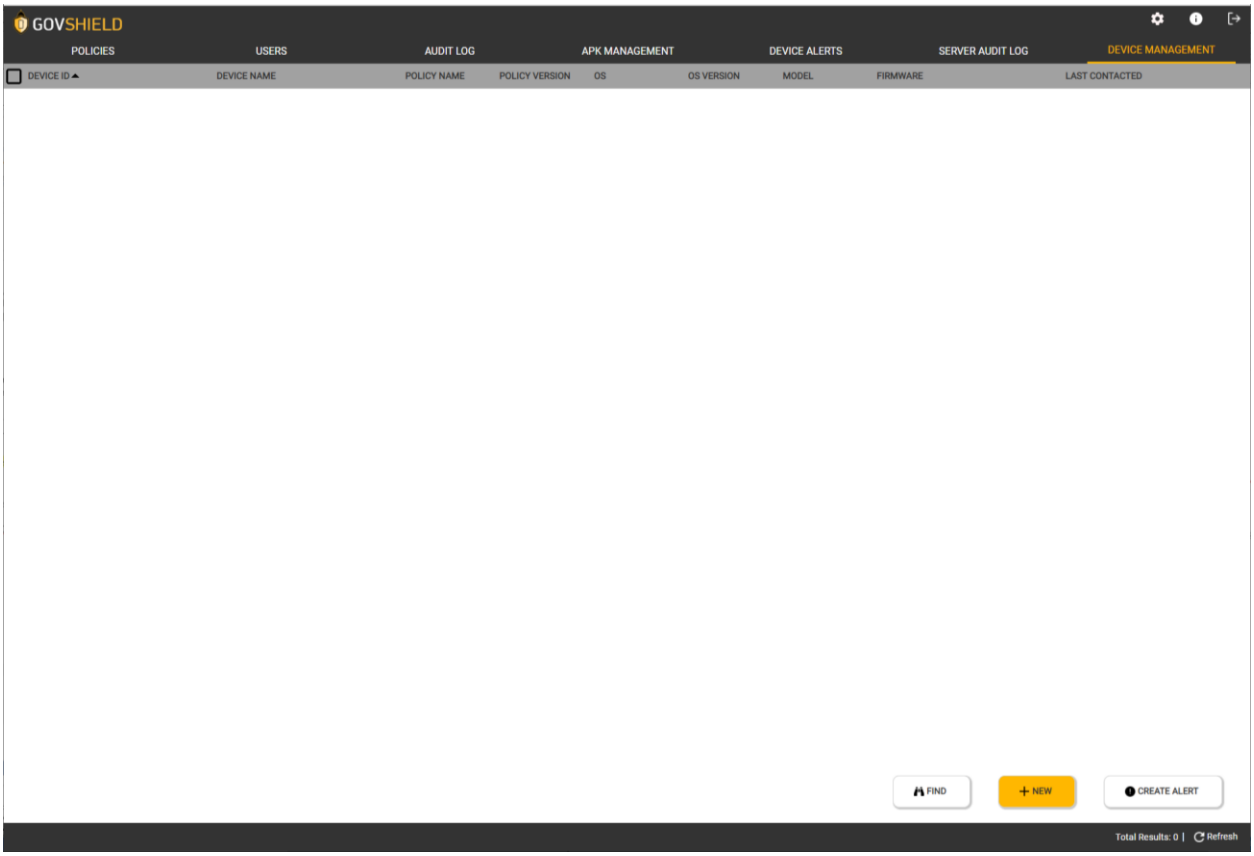


Figure 1 - Device Management Tab

2.1 Whitelist a New Device

Administrators define a whitelist of allowed Android Mobile Devices by their Android Device ID within the 'Device Management' dashboard of the web GUI. Specifying an Android Device ID on the whitelist allows for the device to be enrolled. If the Android Mobile Device's Android Device ID is not found in the whitelist, the enrollment process is stopped. This whitelist of allowed Android Mobile Devices restricts enrollment.

Whitelisting a device requires the device ID, which can be retrieved from the login page of the GovShield Client. When whitelisting a device, you can assign it a device name to more easily identify it.

To whitelist a device, follow these steps,

1. Click the *NEW* button.
2. Enter the Device ID
3. Enter a Device Name for the new device (Optional)
4. Click the Save button.

The device is now whitelisted and can be managed through GovShield. When first whitelisting a device, it will only show the Device ID and Device Name in the list. Once the device has been enrolled with a policy, the rest of the information will be loaded, as shown in Figure 2.

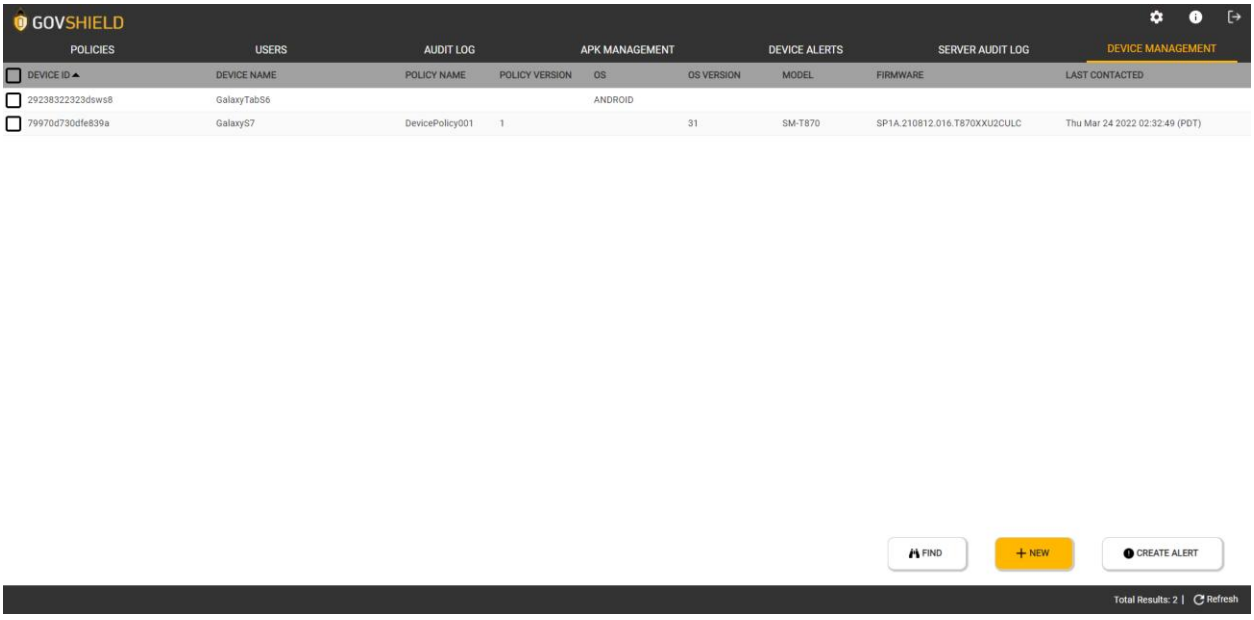


Figure 2 - Managed Device List

2.2 Edit Device

Before provisioning a device, you can still edit the entry in the list to change the device ID and its assigned name. After a device has been provisioned, the edit window can be opened to alter the assigned name, the policy it's assigned to, and the device's password. You can also view the information from the management screen grid, along with a list of the installed applications, with versions, on the device.

To edit a device,

1. Select the device on the management screen.
2. Click the *EDIT* button.

Information about the device can now be viewed and some information can be changed, as shown in Figure 3.

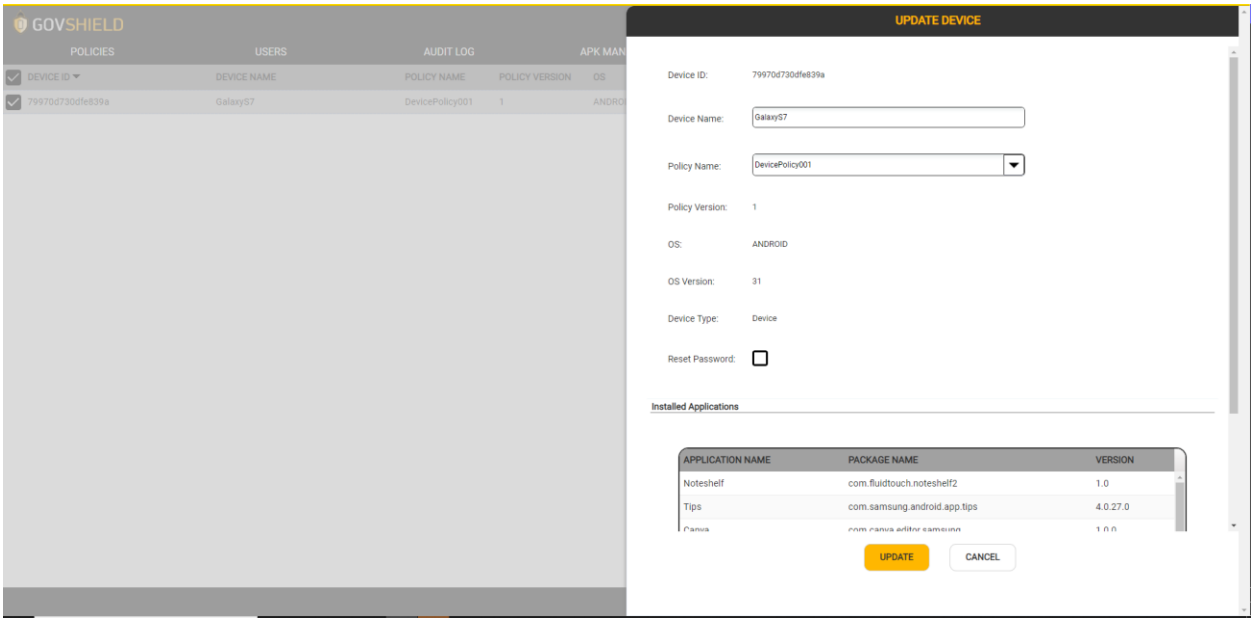


Figure 3 – Device Management Edit Window

2.3 Filter

The list of devices on the management screen can be filtered down based on the ID, device name, assigned policy, policy version, operating system version, device model name, and the firmware version.

To filter the list of devices,

1. Click the *FIND* button.

2. Fill in the criteria you want to filter by.
3. Click the *APPLY* button to filter the list of devices.

To clear the list filter,

1. Click the *FIND* button.
2. Click the *CLEAR* button.
3. Click the *APPLY* button.

See Figure 4 for an example of a device filter.

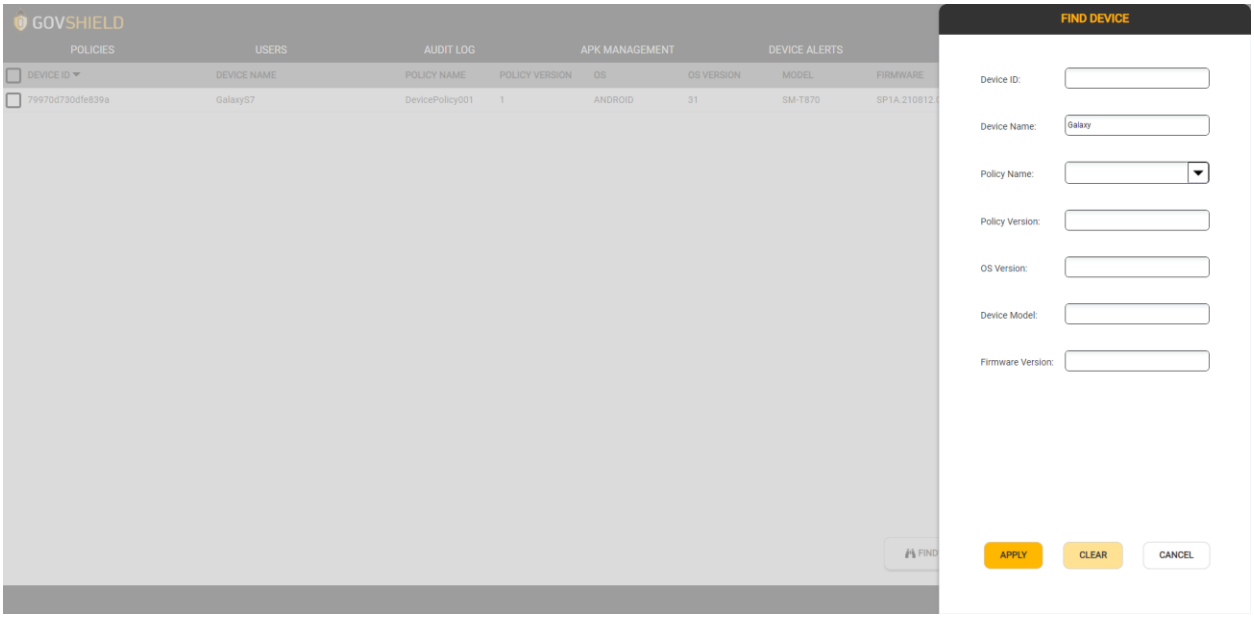


Figure 4 – Device Management Filter Window

2.4 Create Alert

GovShield provides the ability to send Alerts to enrolled devices. You can send alerts to all devices in the list or just to the selected devices.

To send an Alert to a device,

1. Select the device(s) you would like to send an Alert to.
2. Click the *CREATE ALERT* button and then click *Alert to Selected*.
    a. To send to all devices, click the *CREATE ALERT* button and then click *Alert to All*.
3. Type the message that you would like to send to the selected devices.
4. Click the *SAVE* button and your message is on its way to the device(s).

See an example of sending a message alert in Figure 5.

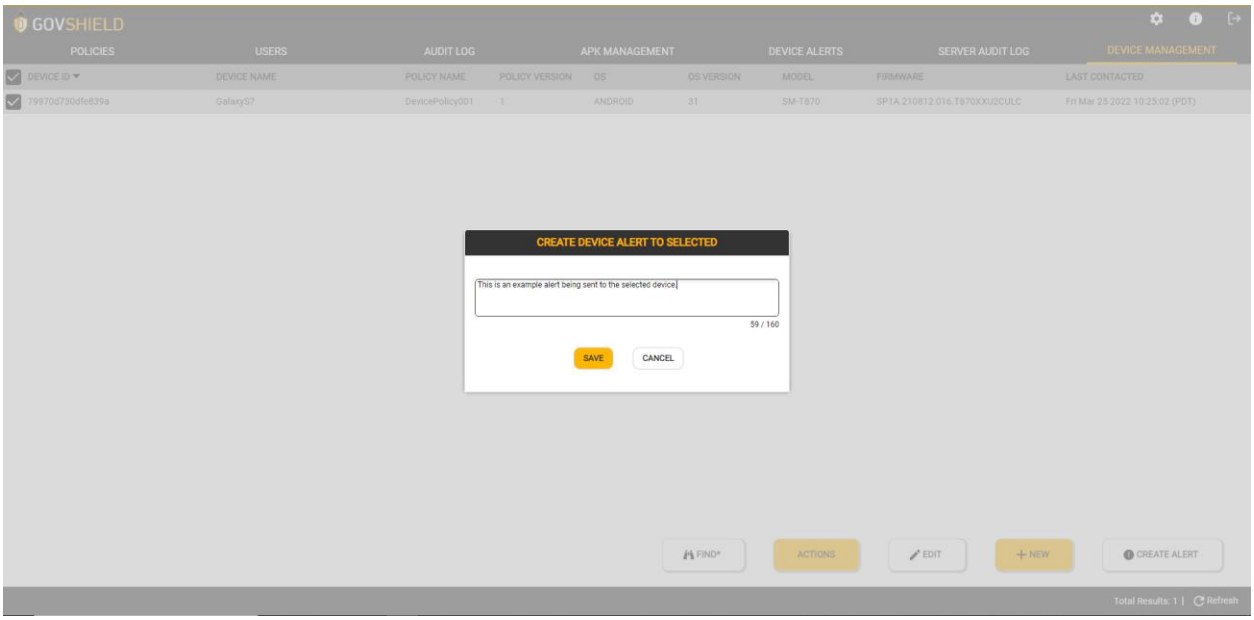


Figure 5 – Create Alert Popup

2.5 Actions

GovShield provides the ability to send different commands to a device. These actions are *Unenroll*, *Wipe*, and *Lock*.

2.5.1 Unenroll Device

Unenrolling a device removes it from being managed by GovShield Server, including the removal of the GovShield Client from the device. This process sets the device back to its original settings from before enrollment, and disallows the device from accessing the GovShield Server.

To unenroll a device,

1. Select the device(s) you wish to unenroll.
2. Click the *ACTIONS* button.
3. Click the *UNENROLL DEVICE* button.
4. The device(s) will now unenroll itself the next time they check in to the GovShield server.

2.5.2 Wipe Device

Wiping a device performs a factory reset on the device. This includes being unenrolled from GovShield Server, including the removal of the GovShield Client from the device. This process

sets the device back to its factory settings like it is brand new and disallows the device from accessing the GovShield Server.

To wipe a device,

1. Select the device(s) you wish to wipe.
2. Click the *ACTIONS* button.
3. Click the *WIPE DEVICE* button.
4. The device(s) will now be wiped the next time they check in to the GovShield server.

2.5.3 Lock Device

Locking a device forces it to lock and require a password to reopen the device.

To lock a device,

1. Select the device(s) you wish to lock.
2. Click the *ACTIONS* button.
3. Click the *LOCK DEVICE* button.
4. The device(s) will now lock the next time they check in to the GovShield ser er.

2.5.4 Uninstall Application

GovShield provides the ability to remotely uninstall an Android application on a provisioned device.

To uninstall an application,

1. Select the device you wish to uninstall application(s) from.
2. Click the *EDIT* button.
3. Select application(s) to uninstall
4. Click the *DELETE* button.
5. Click *YES* to confirm the selection.
6. Click the *UPDATE* button.
7. The selected device(s) will now be notified which applications to uninstall.

2.6 Device Network Connectivity

Administrators have two methods for checking the network connectivity status of an enrolled Android Mobile Device on the web GUI. Under the ‘Device Management’ dashboard, each enrolled Android Mobile Device has a date and time defined under the “Last Contacted” column.

This identifies the overall last time the GovShield Client connected to the GovShield Server for a reachability event, regardless of which reachability event action initiated the alert. Meanwhile, under the 'Device Alerts' dashboard of the web GUI, every reachability event from a GovShield Client is listed as an alert for the Android Mobile Device. Each alert has a date and time defined under the Alert Date column. Therefore, an Administrator can observe all of the reachability events for an Android Mobile Device, with an Android Mobile Device's latest reachability event alert identifying the last time GovShield Client connected to the Server.

3 Manage Users

GovShield provides the ability to manage users through the Users tab of the web GUI. There are two types of user roles, Admin and User. Users with an Admin role are able to log in to the Web GUI application and manage all of the settings. They can also log in to the GovShield Client and use it like any user. Users with a User role cannot use the Web GUI application, but they can use the GovShield Client fully.

3.1 Add a User

Administrators can create new users to allow more access to the Web GUI and GovShield Clients. New users need to define a first name, last name, username, password, and role.

To create a new user,

1. Click the *NEW* button.
2. Fill in the user information.
    a. Take care to use the same password in both password fields.
    b. Make sure to give the new user the correct role to control their privileges.
3. Click the *ADD* button.

The new user is now added to the list of MDM users. The new user window can be seen in Figure 6.

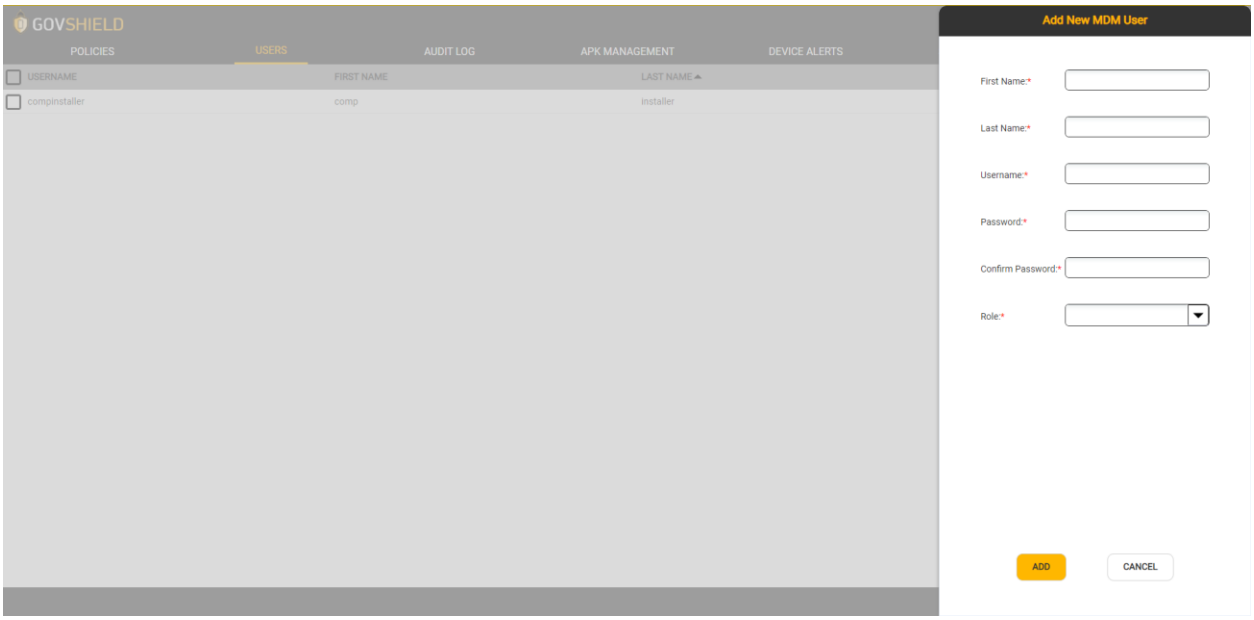


Figure 6 – New User Window

3.2 Edit a User

Administrators can edit information about existing users. Editing a user can serve to fix mistakes, force a password change to secure an account, or update the user's role.

To edit a user,

1. Select the user you want to edit.
2. Click the *EDIT* button.
3. Change the user information you want to edit.
4. Click the *SAVE* button.

An example of the User Edit window can be seen in Figure 7.

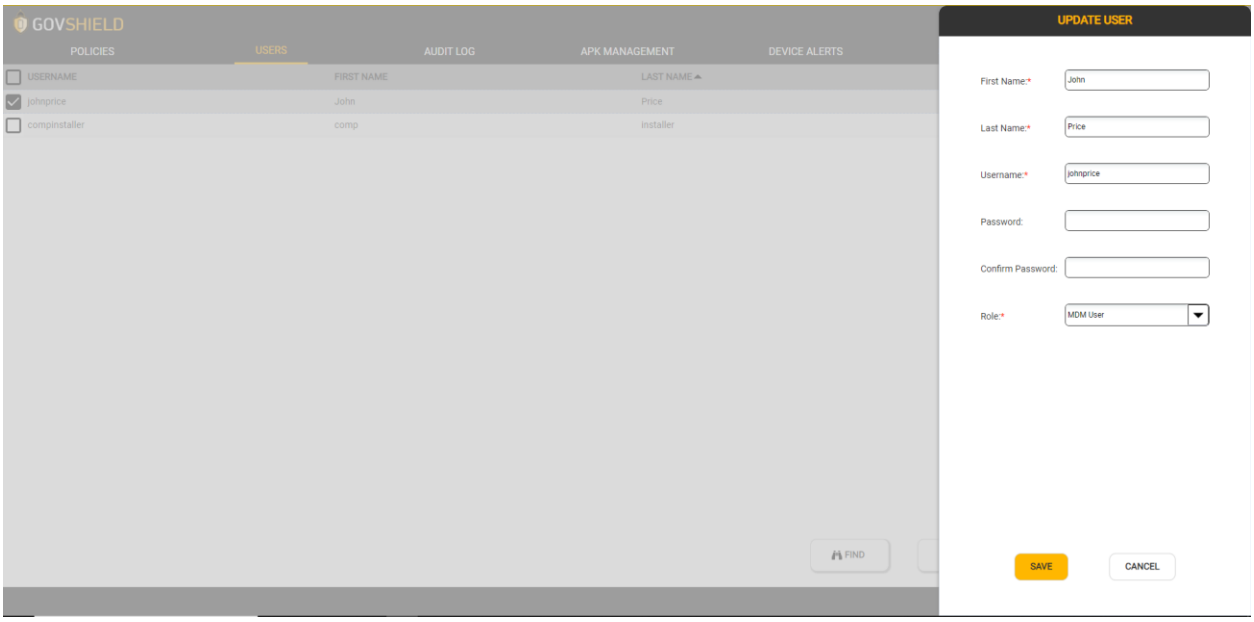


Figure 7 – User Edit Window

3.3 Delete a User

Administrators can delete most other users. All users with a User role can be deleted. An administrator cannot be deleted if they are the last administrator in the system. An administrator also cannot delete themselves from the system.

To delete a user(s),

1. Select the user(s) you want to delete.
2. Click the *DELETE* button.
3. Click the *YES* to confirm the users you want to delete.

The delete confirmation popup can be seen in Figure 8.

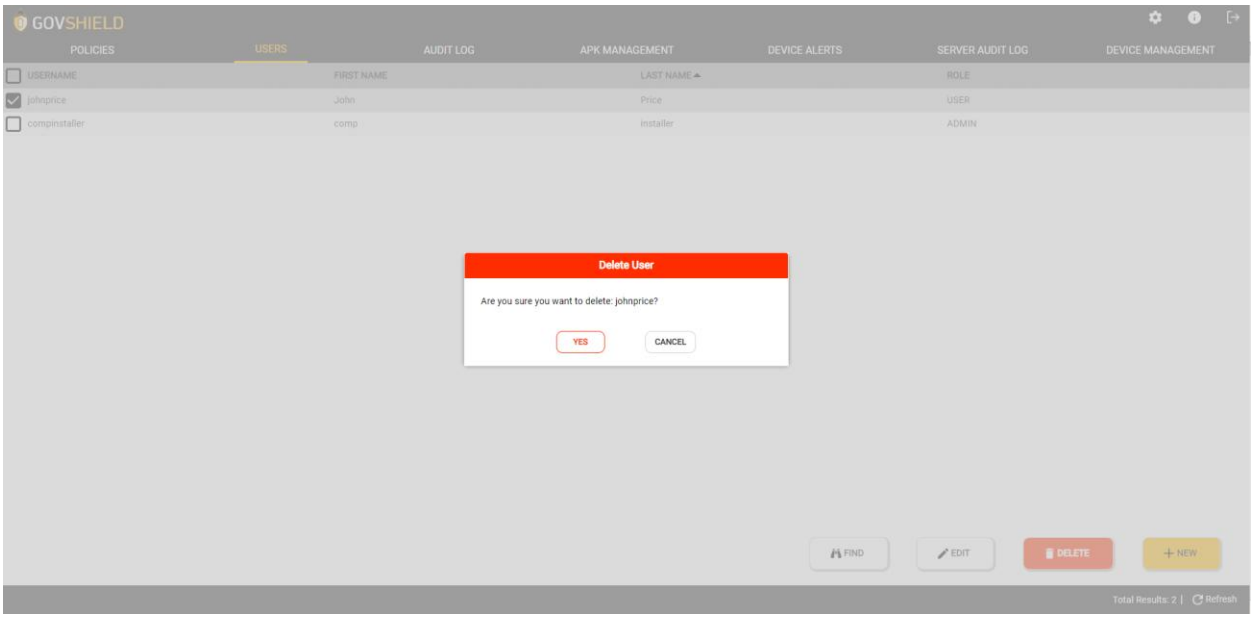


Figure 8 – Delete User Popup

3.4 Filter List of Users

Filtering a list of users only shows the users that fit the criteria set in the filter window. The user list can be filtered by the user's first name, last name, username, and role.

To filter the user list,

1. Click the *FIND* button.
2. Set the fields that you want to filter for.
3. Click the *APPLY* button.

To clear the user list filter,

1. Click the *FIND* button.
2. Click the *CLEAR* button.
3. Click the *APPLY* button.

An example of the user filter window can be seen in Figure 9.

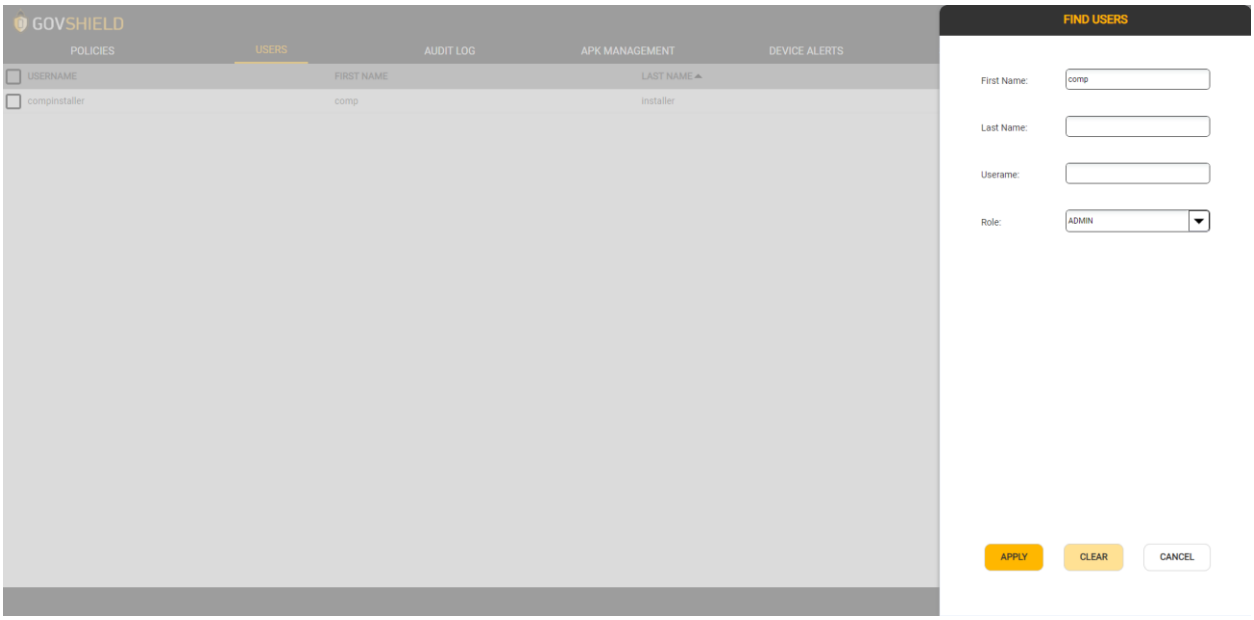


Figure 9 – User Filter Window

4 Manage Policies

4.1 Overview

GovShield uses policies to regulate the behavior of the devices that it manages. A policy contains a set of rules which are enforced on the devices to which the policy is defined. There is one default policy which unless a different policy is selected will automatically be assigned to each enrolled device. A device can only have one policy assigned to it. Each change made to an existing policy will create a new revision of that policy.

The Policies tab provides the capability to create, edit, and view policies. The following columns are shown in the Policy List:

Column Name	Description
Policy Name	Given name of the policy
Version	This number increments each time the policy is edited and saved
Last Updated	The date of the most recent edit to the policy
Created By	The username of the creator of the policy

Default Policy	A checkmark will be displayed if the policy is currently selected is set as default

4.1.1 Create a new Policy

GovShield provides the ability to add new policies. To add a new Policy, perform the following steps,

1. Click the "NEW" button and then click "CREATE"
2. The following fields are required to be filled in order to create a policy:
    a. Name
    b. Toaster Notification Level
    c. Polling Interval (mins)
    d. App Polling Interval (mins)
    e. Audit Log Publishing Rate (hours)
    f. Samsung License Key
    g. Gov Shield Web Service URL
    h. Web GUI Admin Service URL
    i. Server Communication Interval (mins)
    j. Reachability Limit Type
    k. Reachability Limit Action
    l. Max Time (min)/Failed Attempt
3. Click the "SAVE" button
4. The new policy with all settings from the copied policy is now listed in the Policy tab

4.1.2 Find a Policy

The "FIND" button opens a dialogue that allows a use to filter the Policy List. This filters on the following options: Policy Name, Last Updated, Created By, Default Policy. Each of these fields corresponds to the column on the Policy List with the same name. To search for a policy, perform the following steps:

1. Click the "FIND" button
2. Enter the desired search criteria
3. Click the "APPLY" button

4. The search results are now shown
5. To clear the search results, click the “FIND” button again
6. Click the “CLEAR” button
7. Click the “APPLY” button

4.1.3 Edit a Policy

GovShield provides the ability to edit policy information. To edit a policy, perform the following steps,

1. Click the checkbox next to the policy to which you’d like to Edit
2. Click the “EDIT” button
3. Make the desired changes
4. Click the “SAVE” button

4.1.4 Copy a Policy

GovShield provides the ability to copy an existing policy to create a new policy. All settings from the selected policy will be copied over to a new policy. Once copied, changes can then be made. To copy a policy, perform the following steps,

1. Click the checkbox next to the policy to which you’d like to Copy
2. Click the “COPY” button
3. Enter the name of the new policy that you are creating.
4. Click the “SAVE” button
5. The new policy with all settings from the copied policy is now listed in the Policy tab

4.2 Policy Settings

A GovShield Policy consists of four major categories; MDM Settings, Device VPN Profile, Device Policy, Firewall Settings, and optionally Workspace Policy and Workspace VPN Profile. The subsections below will describe each individual setting.

4.2.1 MDM Settings

MDM Settings are the high level settings that define how the Android client agent application will look and behave including how often it will communicate back to the server module.

4.2.1.1 MDM Configurations

Table 1 below provides descriptions of each configuration setting.

Setting	Description
Name	The name of the policy
Toaster Notification Level	The level of notifications that will pop up. The toaster notifications are largely used for debugging purposes. It is recommended that this setting be set to OFF for normal working environments.
Polling Interval (mins)	The number in minutes of the interval at which the client agent application polls the server module for updates, alerts, etc.
App Polling Interval (mins)	The number in minutes of the interval at which the client agent application polls the server module for any changes to the apps that are installed on the device. This includes new apps, app updates, or app removal.
Audit Log Publishing Rate (hours)	The number in minutes of the interval at which the client agent application sends the audit log back to the server module.
Samsung License Key	The license key is required to communicate to use Samsung Knox
Web GUI Admin Web Service URL	The web service URL to which the client agent application will send all polling requests and audit logs
App Installation Policy	Policy dictates the frequency that the device contacts the server for app updates
Enable Workspace	Indicates if a workspace will be created on each device on which the policy is assigned
MDM Icon File	The icon of the client agent application that will appear on each device on which the policy is assigned. A default icon is expected to be used but in special circumstance, that icon can be changed.
Device Lock Screen Message	An optional message that can be displayed on the lock screen of the device.
App Use Consent Message	An optional message that can be displayed on the login page of the GovShield Client.

Table 1 - MDM Configurations Settings

4.2.1.2 App to Server Communications Settings

Table 2 below provides descriptions of each app to server communications setting. These settings are used to verify that they device is still able to communicate with server module.

Setting	Description
Server Communication Interval (min)	How often the app to server check is executed
Reachability Limit Type	The method (Time or number of failed attempts) in which reachability is measured
Reachability Limit Action	The action for the client agent application to take in the case where its determined that the server module is not reachable within the parameters defined
Max Time (min)/Failed Attempts	When Limit Type is Time Limit, this defines the number of minutes allowed of unreachability before the limit action is taken. When Limit Type is Failed Attempts this defines the number of times failed the server poll fails before the limit action is taken.

Table 2 - App to Server Communication Settings

4.2.1.3 App Configurations

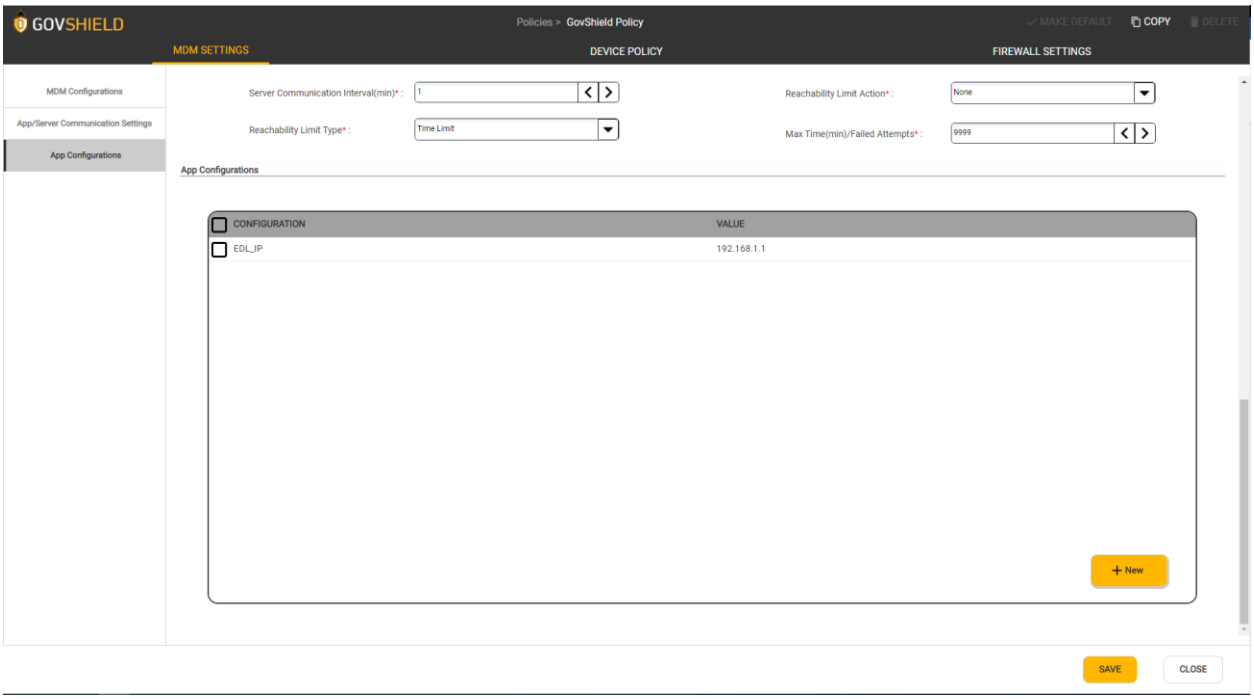


Figure 3 - App Configurations Section

The App Configurations grid is used to store key value pairs for other apps to pull values from.

To add an app configuration to the list, perform the following steps:

1. Click the “New” button
2. Enter the values
3. Click the “SUBMIT” button
4. The app configuration is now added to the list

To edit an app configuration in the list, perform the following steps:

1. Click the checkbox next to the application that you’d like to edit
2. Click the “View/Edit” button
3. Change the values
4. Click the “Submit” button
5. The app configuration is now updated in the list

To delete an app configuration from the list, perform the following steps:

1. Click the checkbox next to the application that you'd like to delete
2. Click the "Delete" button
3. Click the "Yes" button
4. The app configuration is now deleted from the list

4.2.2 Device Policy

Device Policy enforces the organization's security policies on your device to protect corporate data and make it more secure. Once a device is enrolled to a policy, the admin can then update policies and settings which will be reflected onto the enrolled device.

4.2.2.1 Restrictions

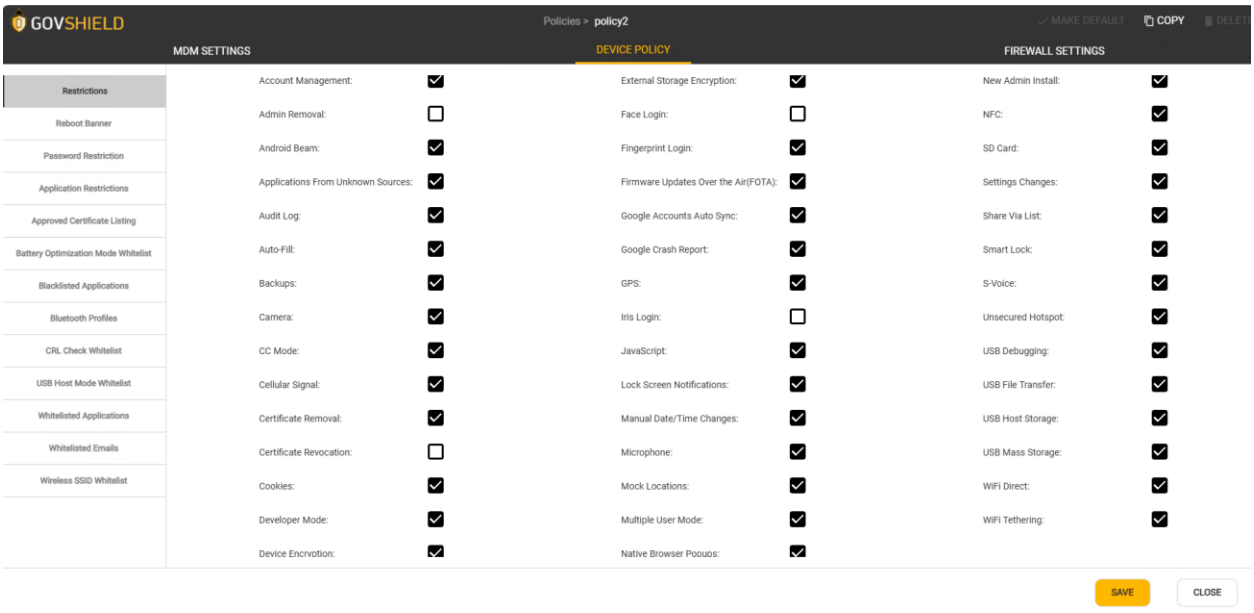


Figure 4 – Device Policy Restrictions

Setting	Description
Account Management	Enable/disable to disable account management for a specific type of account.

Admin Removal	Enable/disable the removable status of an administrator application (i.e., GovShield). If set to true (checked), the user can remove the administrator through the device's Settings application. If set to false (unchecked), the user cannot remove the administrator through the device's Settings application. For the Common Criteria evaluation, this must be set to false (unchecked) for all policies.
Android Beam	Enable/disable use of Android Beam on the device. When Android Beam is disabled, the user is not able to send information (contacts, e-mails, Web addresses, etc.) using Android Beam. S Beam is also disabled when Android Beam is disabled.
Applications Form Unknown Sources	Enable/disable the ability to install an application from an unknown source.
Audit Log	Enable/disable AuditLog feature on device. AuditLog reserves 5% of available storage on device for each administrator, limited to a minimum of 10 MB and a maximum of 50 MB.
Auto-Fill	If set to false, this setting overrides the default browser autofill setting. The setting is applied to the browser in order to prevent any website from providing autofill suggestions when a user is filling in form data on the webpage, even if the user has previously filled in the form. The user cannot change the setting from false to true (i.e., the corresponding UI is also disabled). When checked, the default browser setting is restored, and the user can change the browser autofill setting.
Backups	Enable/disable backing up to Google servers.
Camera	Enable/disable the camera. User or third-party applications cannot enable the camera once it is disabled. The camera is turned off and disabled if the checkbox is not checked. This disables the photo camera, video camera, and video telephony functionality
CC Mode	Enable/disable CC (Common Criteria) mode
Cellular Signal	Enable/disable mobile data connections. If disabled, the user cannot use its data connection through the SIM
Certificate Removal	Enable/disable certificate removal ability. This setting allows a user to delete user-installed digital certificates from the device.

Certificate Revocation	Enable/disable certificate revocation check. This will enable the check for revocation of the server certificate chain during SSL mutual authentication process. This setting only applies to the application if it uses standard TrustManager implementation, this includes most of the native applications, but it does not include third party browsers. Revocation check is primarily done using certificate revocation lists (CRL) that can be downloaded using a CRL distribution point listed in the certificate.
Cookies	This setting overrides the default browser cookies setting. This setting is applied to the browser in order to prevent any website from storing cookies related to the website on the device. A website that make use of cookies to preload user authentication information cannot do so. The user cannot change the setting from false to true (i.e., the corresponding UI is also disabled). When checked, the default browser setting is restored, and the user can change the browser cookies setting
Developer Mode	Enable/disable the user of changing any Developer Mode option in Settings application. Once this policy is applied, every developer option is reset to its default state.
Device Encryption	Enable/disable full device encryption, which includes device memory and an internal Secure Digital (SD) card. Before enabling this setting, the administrator must ensure that the device password is set to alphanumeric quality.
External Storage Encryption (SD Card)	Enable/disable external Secure Digital (SD) card encryption if available. Before enabling this setting, the administrator must ensure that the device password is set to alphanumeric quality.
Face Login	Enable/disable lock screen FACE biometric authentication option.
Fingerprint Login	Enable/disable lock screen Fingerprint biometric authentication option.
Firmware Updates Over the Air (FOTA)	Enable/disable upgrading the operating system (OS) over-the-air (OTA).
Google Accounts Auto Sync	Enable/disable Google accounts to sync automatically. This setting will not block play store from update installed apps because it doesn't rely on Google account auto sync for that. Also, a user will still be able to perform manual sync from inside some applications like Gmail.

Google Crash Report	Enable/disable sending a crash report to Google. If disabled, all possible Google crash reports are blocked.
GPS	Enable/disable the use of GPS.
Iris Login	Enable/disable lock screen IRIS biometric authentication option.
Javascript	If set to false, this setting overrides the browser default JavaScript setting. This setting is applied to Samsung browser in order to prevent the browser from running JavaScript code for a website. A website that requires JavaScript to be active in achieving a function (for example, an animation) is prevented from executing the function. The user cannot change the setting from false to true (i.e., the corresponding UI is also disabled). When checked, the default browser setting is restored, and the user can change the JavaScript setting.
Lock Screen Notifications	Enable/disable the ability to see notifications from the lock screen.
Manual Date/Time Changes	Enable/disable the ability to manually change date and time.
Microphone	Enable/disable the microphone. User or third-party applications cannot enable the microphone once it is disabled. The microphone is turned off and disabled if the checkbox is not checked. This disables only the microphone used for recording, not the phone application microphone.
Mock Locations	Enable/disable mocking the device's GPS location. If checked, the device can change its actual longitude and latitude readings, and GPS applications will show the fake coordinates instead of the actual coordinates.
Multiple User Mode	Enable/disable multiple user support. User or 3rd party applications cannot enable multiple user support when disabled.
Native Browser Popups	If disabled, the setting overrides the default pop-up browser setting to prevent any website from popping up new browser windows when the user navigates to a website that invokes such action. The setting applies to Samsung browser. The user cannot change the setting from false to true (i.e., the corresponding UI is also be disabled). When checked, the default browser setting is restored, and the user can change pop-up settings.

New Admin Install	Enable/disable installation of another administrator application from all sources unless the application installation is done by the administrator enforcing this policy. This setting can only be applied if there are no other administrators activated
NFC	Enable/disable the NFC.
SD Card	Enable/disable Secure Digital (SD) card access.
Settings Changes	Enable/disable access to the Settings application. After disabling Settings, several changes to system preferences cannot be made.
Share via List	Enable/disable the display of the Share Via List, the Share Via List is displayed in certain applications that share data with other applications.
Smart Lock	Enable/disable smart lock keyguard feature.
S-Voice	Enable/disable launching the S-Voice application (Samsung personal assistant). When S-Voice is disabled, the user can neither set a new wake-up command nor unlock the device by using a wake-up command set prior to disallowing S-Voice. In addition, once disabled, the administrator can no longer set a new face and voice lock screen. However, the device can still be unlocked if the lock screen had already been set prior to disallowing S-Voice.
Unsecured Hotspot	An open Wi-Fi hotspot is a Wi-Fi connection with no security constraints that allows any Wi-Fi-capable device to connect. When disabled, the user cannot start an open Wi-Fi hotpot. When enabled back, the user is allowed to start an open Wi-Fi hotspot.
USB Debugging	Enable/disable USB access. This setting blocks any kind of device debugging through Dalvik Debug Monitor Server (DDMS) or ADB.
USB File Transfer	Enable/disable the usage of USB file transfer. This setting controls the ability for a computer to access and manage the internal storage of an Android device via a USB cable.
USB Host Storage	Enable/disable the usage of USB host storage via USB OTG. If enabled, a user can connect any pen drive (portable USB storage), external HD, or Secure Digital (SD) card reader, and it is mounted as a storage drive on the device. If disabled, external storage devices are disallowed from being mounted.

USB Mass Storage	Turns on/off USB mass storage (MTP) when the device is connected to a PC.
USB Media Player	Enable/disable MTP (media transfer protocol). Since Android only supports USB file transfer through MTP, using this setting will block any kind of file transfer through USB. PTP (picture transfer protocol) is a subset of MTP and will also be affected by this setting.
WiFi Direct	Enable/disable WiFi Direct. When WiFi Direct is disabled, any ongoing Wi-Fi Direct connection is interrupted, and the user cannot turn on WiFi Direct. The S-Beam feature which depends on this policy will also be affected by this setting.
WiFi Tethering	Enable/disable the device sharing its carrier data connection with other devices through a Wi-Fi connection. If unchecked, access to WiFi tethering functionality is disabled, and the user cannot turn it on until the administrator enables it again. If checked, access to WiFi tethering is enabled. Enabling access to WiFi tethering does not enable WiFi tethering.

4.2.2.2 Reboot DoD Banner

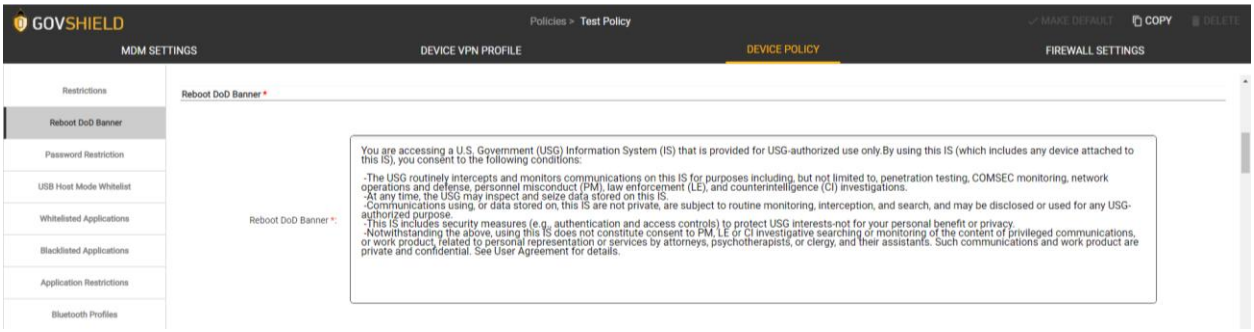


Figure 5 - Reboot Banner Setting

This defines the banner message that is displayed after device reboot. This is specifically implemented for STIG compliance requirement for DoD-US (Department of Defense).

4.2.2.3 Password Restriction

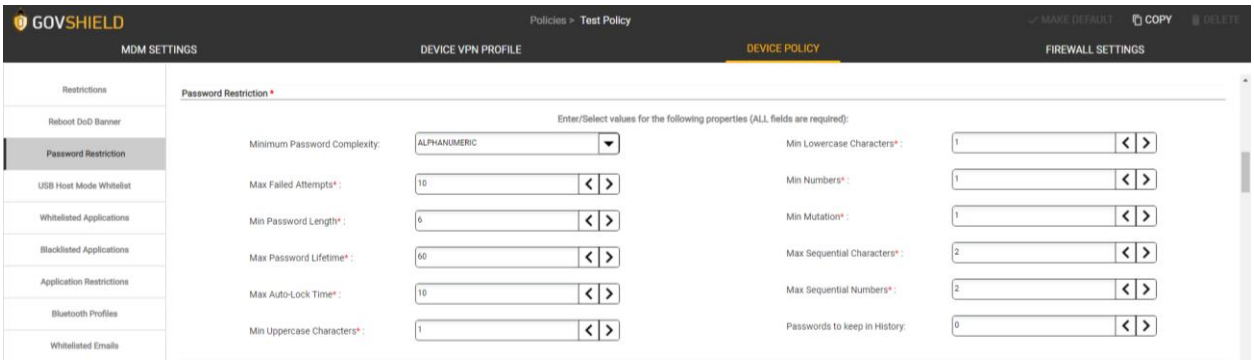


Figure 6 - Password Restriction Settings

These settings together will define the password requirements for the device

Setting	Description
Minimum Password Complexity	Defines what types of passwords are acceptable
Max Failed Attempts	The number of failed attempts of entering a password before action is taken
Min Password Length	The minimum number of characters required for a password
Max Password Lifetime	The number of days that a password can be used before it must be changed
Max Auto-Lock Time	The amount of time in minutes before a device is locked due to inactivity
Min Uppercase Characters	The least number of required uppercase letters required in a password
Min Lowercase Characters	The least number of required lowercase letters required in a password
Min Numbers	The least number of required numbers required in a password
Min Mutation	The minimum number of characters that a new password must be different from the previous password
Max Sequential Characters	The maximum number of the same character in a row permitted in a password

Max Sequential Numbers	The maximum number of the same number in a row permitted in a password
Passwords to Keep in History	The number of passwords that a new password cannot be the same as.

4.2.2.4 USB Host Mode Whitelist

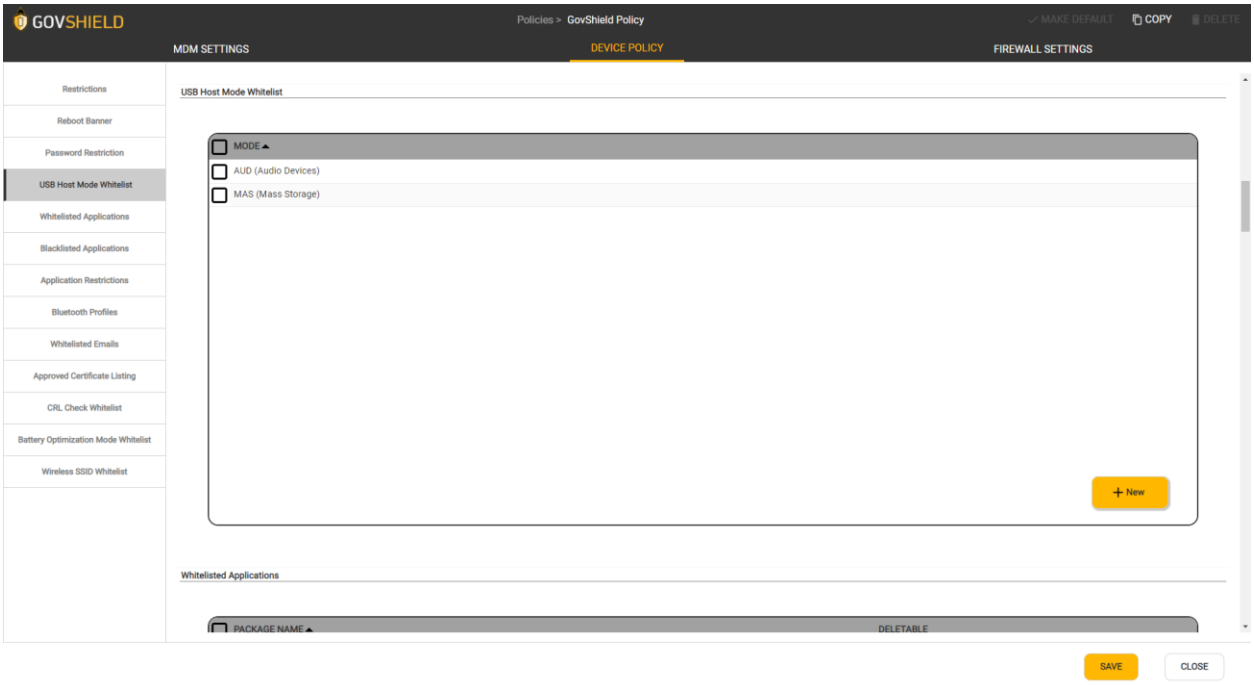


Figure 7 - USB Hose Mode Setting

By default, all USB modes are blacklisted. To enable specific USB modes, they will need to be added to the whitelist.

4.2.2.5 Whitelisted Applications

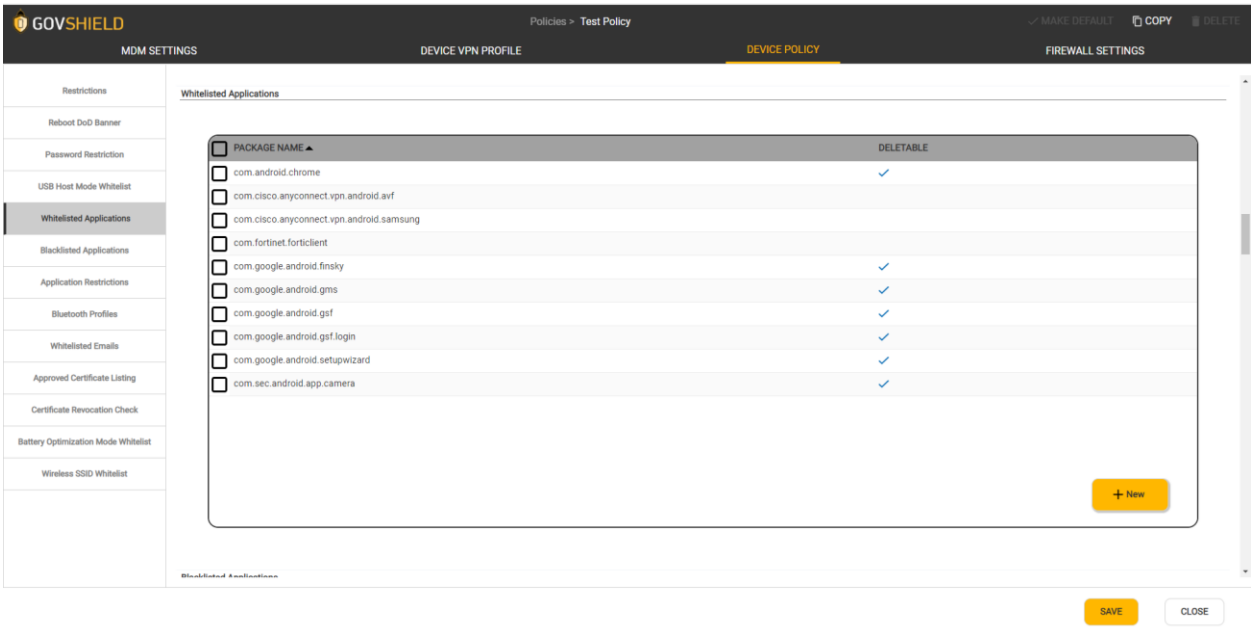


Figure 8 - Whitelisted Applications List

Whitelisted applications are applications that are permitted to be installed on the device. If an application is not in the list than a user will not be able to install it. Applications are identified by their package name.

To add an application to the Whitelist, perform the following steps:

5. Click the “New” button
6. Enter the Package Name
7. Click the “SUBMIT” button
8. The package name is now added to the Whitelist

To edit an application in the Whitelist, perform the following steps:

6. Click the checkbox next to the application that you’d like to edit
7. Click the “View/Edit” button
8. Change the Package Name
9. Click the “Submit” button
10. The package name is now updated in the Whitelist

To delete an application from the Whitelist, perform the following steps:

5. Click the checkbox next to the application that you'd like to delete
6. Click the "Delete" button
7. Click the "Yes" button
8. The package name is now deleted from the Whitelist

4.2.2.6 Blacklisted Applications

Blacklisted applications are applications that are not permitted to be installed on the device. If an application is in the list than a user will not be able to install it. Applications are identified by their package name.

To add an application to the Blacklist, perform the following steps:

1. Click the "New" button
2. Enter the Package Name
3. Click the "SUBMIT" button
4. The package name is now added to the Blacklist

To edit an application in the Blacklist, perform the following steps:

1. Click the checkbox next to the application that you'd like to edit
2. Click the "View/Edit" button
3. Change the Package Name
4. Click the "Submit" button
5. The package name is now updated in the Blacklist

To delete an application from the Blacklist, perform the following steps:

1. Click the checkbox next to the application that you'd like to delete
2. Click the "Delete" button
3. Click the "Yes" button
4. The package name is now deleted from the Blacklist

4.2.2.7 Application Restrictions

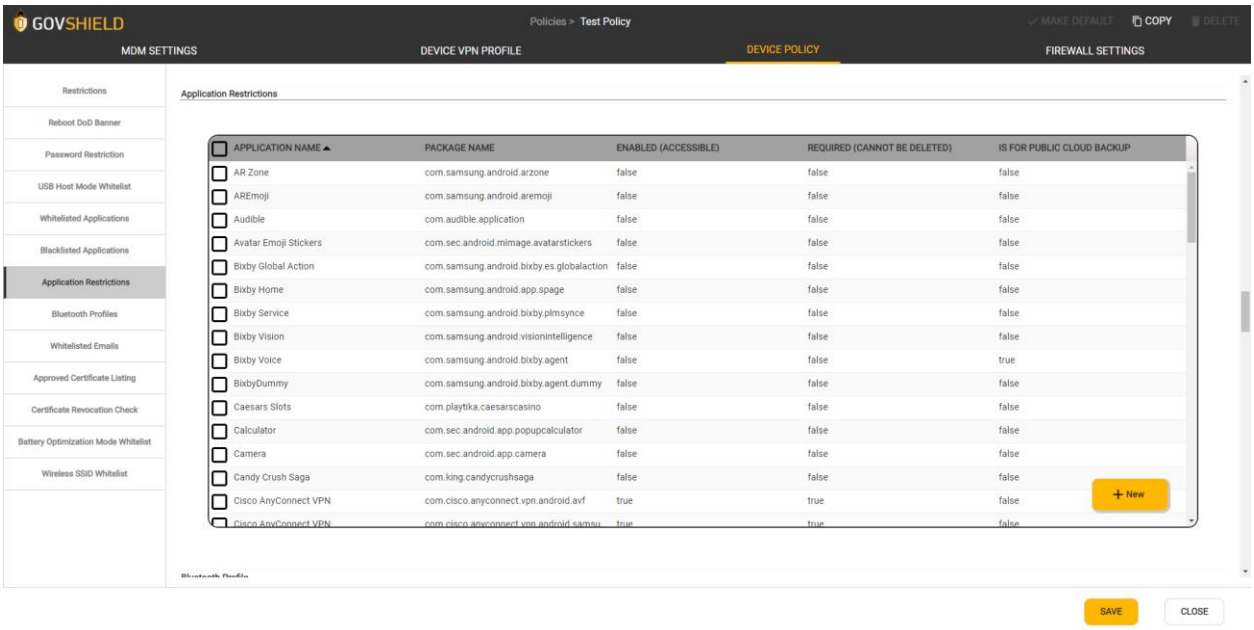


Figure 9 - Applications Restrictions List

Application Restrictions provide a way to control the applications that are installed on a device. Each device comes with a set of applications that cannot be removed/uninstalled. Through Application Restrictions these applications can be disabled so that they are not active and not visible to the user. In addition to enabling/disabling applications, this control also allows applications to be marked as Required which will prevent a user to be able to delete the application from a device.

To add an application to the Application Restrictions List, perform the following steps:

1. Click the “New” button
2. Enter the Application Name
3. Enter the Package Name
4. Indicate if the Application should be Enabled (*it is disabled by default*)
5. Indicate if the Application should be Required (*it is not required by default*)
6. Indicate if the Application should be Backup
7. Click the “SUBMIT” button
8. The package name is now added to the Application Restrictions List

To edit an application in the Application Restrictions List, perform the following steps:

1. Click the checkbox next to the Application that you'd like to edit
2. Click the "View/Edit" button
3. Make desired changes
4. Click the "Submit" button
5. The Application details are now updated

To remove an application from the Application Restrictions List, perform the following steps:

1. Click the checkbox next to the Application that you'd like to remove
2. Click the "Delete" button
3. The application is now removed from the Application Restrictions List and will not be specifically controlled on the device.

4.2.2.8 Bluetooth Profiles

GovShield provides the ability to enable specific Bluetooth profile types on a device which each enable different types of Bluetooth devices to be connected. The Bluetooth profile types that can be enabled on a device are as follows:

- Bluetooth Advanced Audio Distribution Profile (A2DP)
- Bluetooth Audio/Video Remote Control Profile (AVRCP)
- Bluetooth HandsFree Profile (HFP)
- Bluetooth Headset Profile (HSP)
- Bluetooth Phone Book Access Profile (PBAP)
- Bluetooth Serial Port Profile (SPP)

To add an application to the Enabled Bluetooth Profile list, perform the following steps:

1. Click the "New" button
2. Select the desired Bluetooth Profile type
3. Click the "Submit" button
4. The Bluetooth Profile type is now added to the Enabled Bluetooth Profile list

To remove an application from the Enabled Bluetooth Profile list, perform the following steps:

1. Click the checkbox next to the Bluetooth Profile that you'd like to remove
2. Click the "Delete" button
3. The Bluetooth Profile type is now removed from the Enabled Bluetooth Profile list

4.2.2.9 Whitelisted Emails

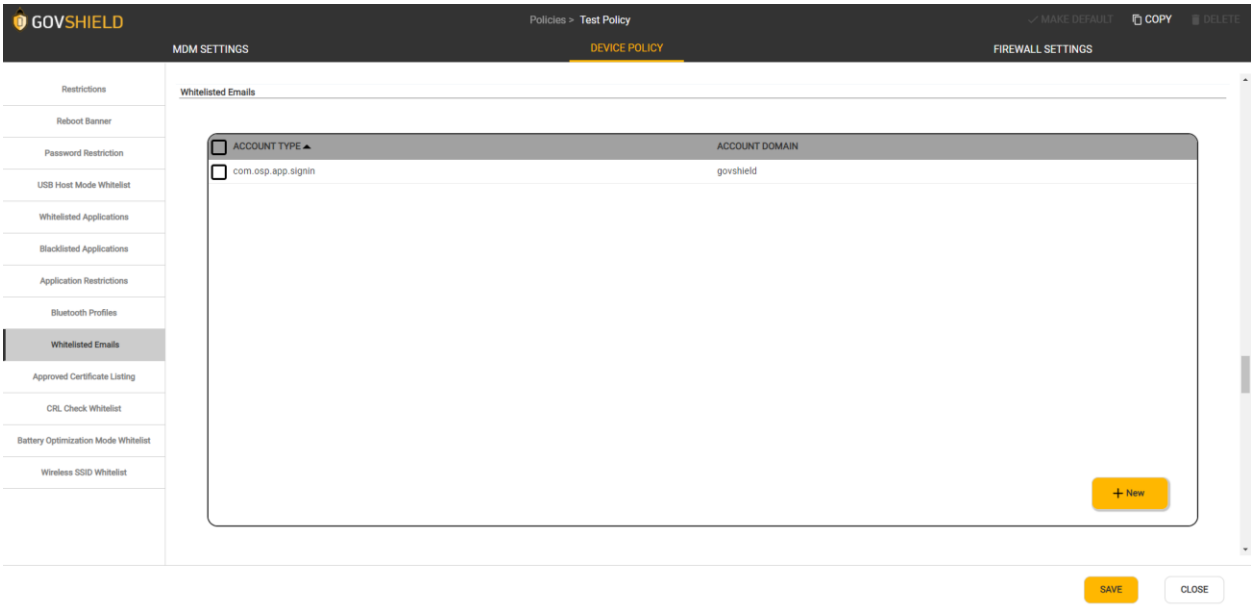


Figure 10 - Whitelisted Emails List

From this section, a list of accounts of a specific account type can be whitelisted and default blacklist all other accounts of that specific account type.

To add an email account to the Email Whitelist, perform the following steps:

1. Click the "New" button
2. Select from the dropdown the Account Type
3. Enter the Account Domain
4. Click the "Submit" button
5. The email account is now added to the Email Whitelist

To view/edit an email account in the Email Whitelist, perform the following steps:

1. Click the "View/Edit" button

2. Modify existing values
3. Click the “Submit” button
4. The email account is now update in the Email Whitelist

To remove an application from the Email Whitelist, perform the following steps:

1. Click the checkbox next to the email account that you’d like to remove
2. Click the “Delete” button
3. The email account is now removed from the Email Whitelist

4.2.2.10 Approved Certificate Listing

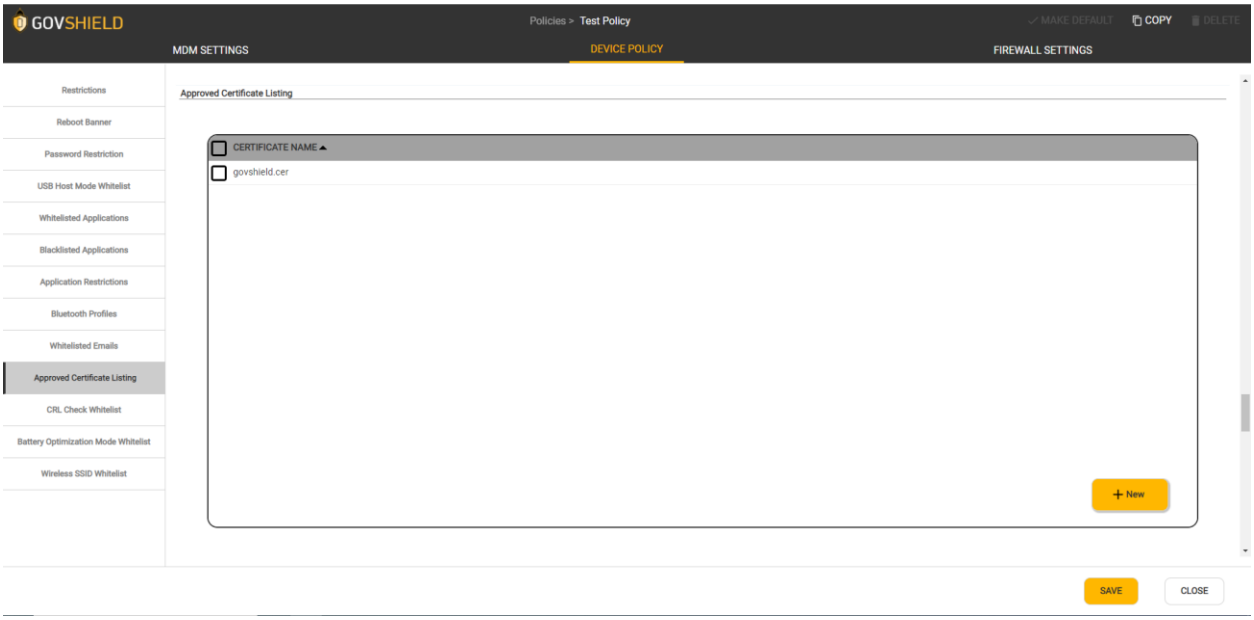


Figure 11 - Approved Certificate List

From this section, a list of approved certificates can be uploaded to be installed on a device.

To upload a certificate to the Approved Certificate Listing, perform the following steps:

1. Click the “New” button
2. Select the upload icon
3. Locate the desired file and click the “Open” button

4. Click the “Save” button
5. The certificate is now added to the Approved Certificate Listing

To remove a certificate from the Approved Certificate Listing, perform the following steps:

1. Click the checkbox next to the certificate that you’d like to remove
2. Click the “Delete” button
3. The certificate is now removed from the Approved Certificate Listing

4.2.2.11 Certificate Revocation Check

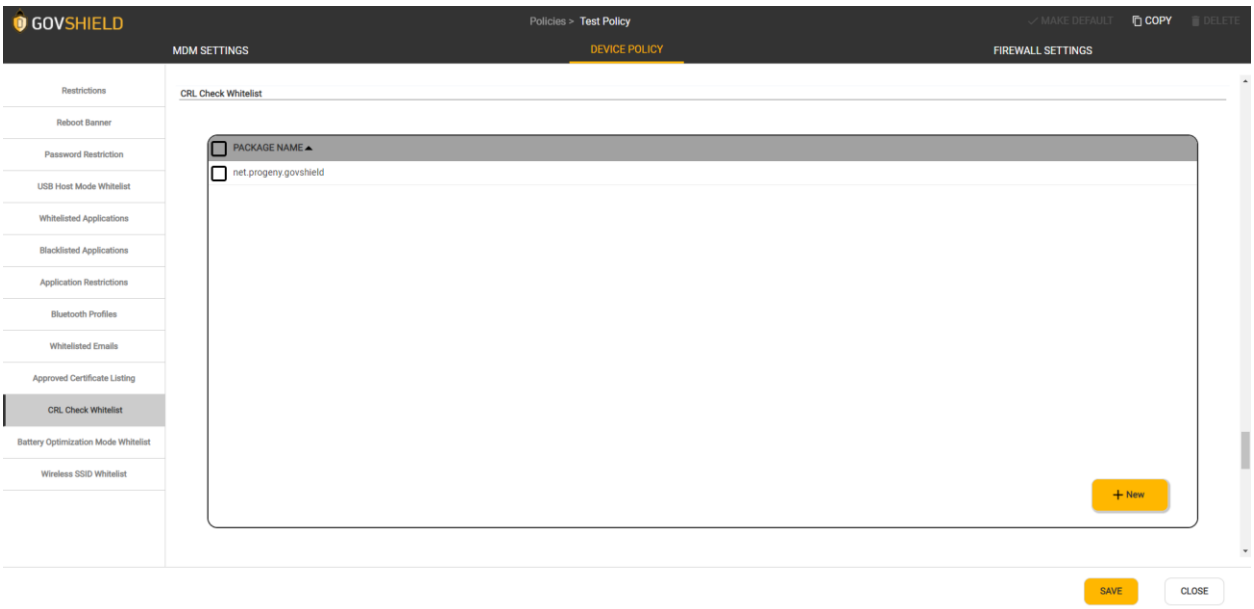


Figure 12 - Certificate Revocation List

From this section, a list of Package Names can be added to the CRL Check Whitelist to bypass the security if the certificate for that Package was revoked.

To add a Package Name to the CRL Check Whitelist, perform the following steps:

1. Click the “New” button
2. Enter the Package Name
3. Locate the desired file and click the “Open” button
4. Click the “Save” button
5. The certificate is now added to the Approved Certificate Listing

To view/edit a Package Name in the CRL Check Whitelist, perform the following steps:

1. Click the “View/Edit” button
2. Modify Package Name
3. Click the “Submit” button
4. The Package Name is now updated in the CRL Check Whitelist

To remove a Package Name from the CRL Check Whitelist, perform the following steps:

1. Click the checkbox next to the Package Name that you’d like to remove
2. Click the “Delete” button
3. The Package Name is now removed from the CRL Check Whitelist

4.2.2.12 Battery Optimization Mode Whitelist

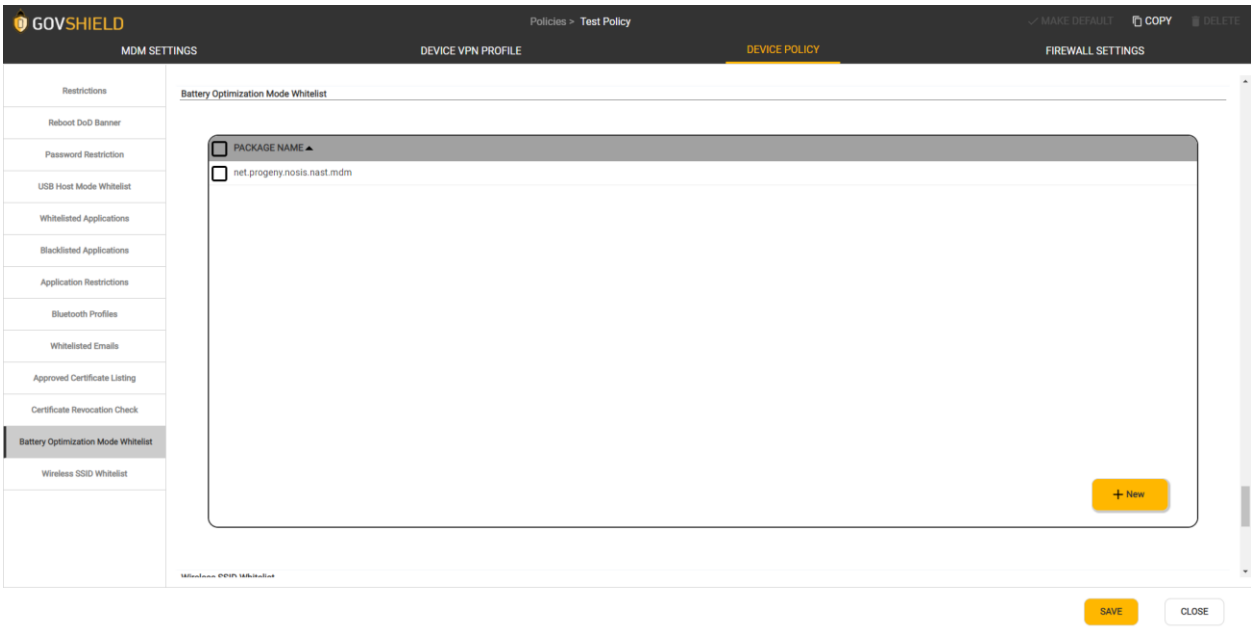


Figure 13 - Battery Optimization Mode List

From this section, devices that are added to the whitelist, will be able to utilize battery optimization mode.

To add an application to the Battery Optimization Mode Whitelist, perform the following steps:

1. Click the “New” button

2. Enter the Package Name
3. Click the “Submit” button
4. The Package is now added to the Battery Optimization Mode Whitelist

To remove an application from the Battery Optimization Mode Whitelist, perform the following steps:

1. Click the checkbox next to the Package that you’d like to remove
2. Click the “Delete” button
3. The Package is now removed from the Battery Optimization Mode Whitelist

4.2.2.13 Wireless SSID Whitelist

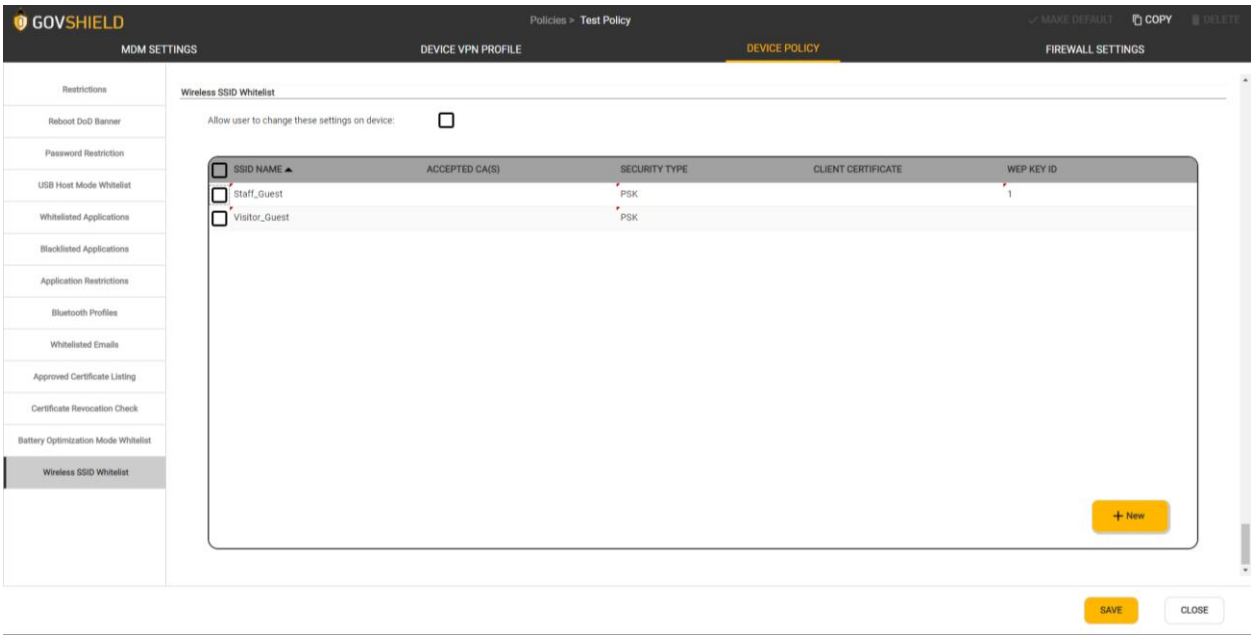


Figure 14 - Wireless SSID Whitelist

The list of approved wireless networks that a device can connect to is controlled here. A device will not be able to connect to a wireless network unless it is listed.

To add an SSID to the Wireless SSID Whitelist, perform the following steps:

1. Click the “New” button
2. Enter the SSID Name
3. Select the Security Type
4. Enter the Accepted Cert Authority Name

5. If WEP is selected for Security Type,
    a. Select the WEP Key ID
    b. Enter the WEP Key 1
    c. Enter the WEP Key 2
    d. Enter the WEP Key 3
    e. Enter the WEP Key 4
6. If WPA/WPA2-Personal is selected for Security Type
    a. Enter the PSK
7. Select the Credentials Type
8. Click the "Submit" button
9. The SSID is now added to the Wireless SSID Whitelist

To edit an SSID in the Wireless SSID Whitelist, perform the following steps:

1. Click the checkbox next to the SSID that you'd like to edit
2. Click the "View/Edit" button
3. Make desired changes
4. Click the "Submit" button
5. The Application details are now updated

To remove an SSID from the Wireless SSID Whitelist, perform the following steps:

1. Click the checkbox next to the SSID that you'd like to remove
2. Click the "Delete" button
3. The SSID is now removed from the Wireless SSID Whitelist.

5 Manage Applications

The APK Management page allows administrators to upload Android application package files, from the filesystem, that can be assigned to specific security policies. These applications are typically custom applications that cannot be found on the Google Play Store. Through this application management mechanism is also where the GovShield Client's software updates would be managed. The administrator can specify whether the application is to be installed on the device. Notes can also be provided with the application to be shown in the GovShield client application.

The GovShield Client software updates are digitally signed during the software build process. The signed software updates must be obtained from General Dynamics Mission Systems and placed in the filesystem of the GovShield server. Once the update is downloaded onto the Android Mobile Device, following the below procedures, the GovShield Client will invoke the platform's application installation process which will verify the software update's digital signature before installing the GovShield Client software update. Only a successful verification of the digital signature will result in the installation of the update to the GovShield Client software, and a failed verification will result in the update process being stopped.

To upload a new APK,

1. Click the *NEW* button.
2. Click the arrow in the *MDM APK File* field, then select the APK file to upload.
3. Select the policy bundle(s) to assign this application to.
4. Select whether or not to install the application on the device.
5. Add any notes to be provided with the release information on the device (optional).
6. Click the *ADD* button.

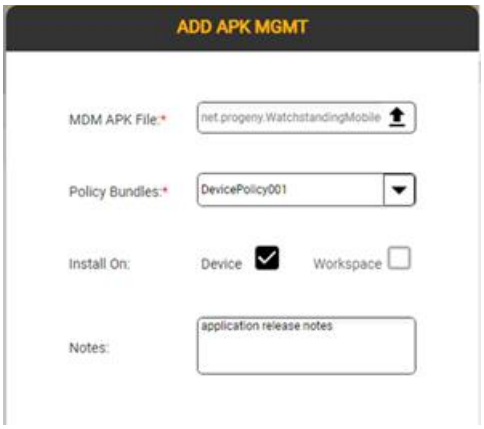


Figure 15 – APK Management Create Window

After an APK has been uploaded, an administrator can edit the assigned policy, the installation selection, and the release notes. The admin can also change the APK file after confirming with a checkbox that they want to update the APK. Other information about the APK upload can also be viewed, like the package name, the app version, and the signature of the APK.

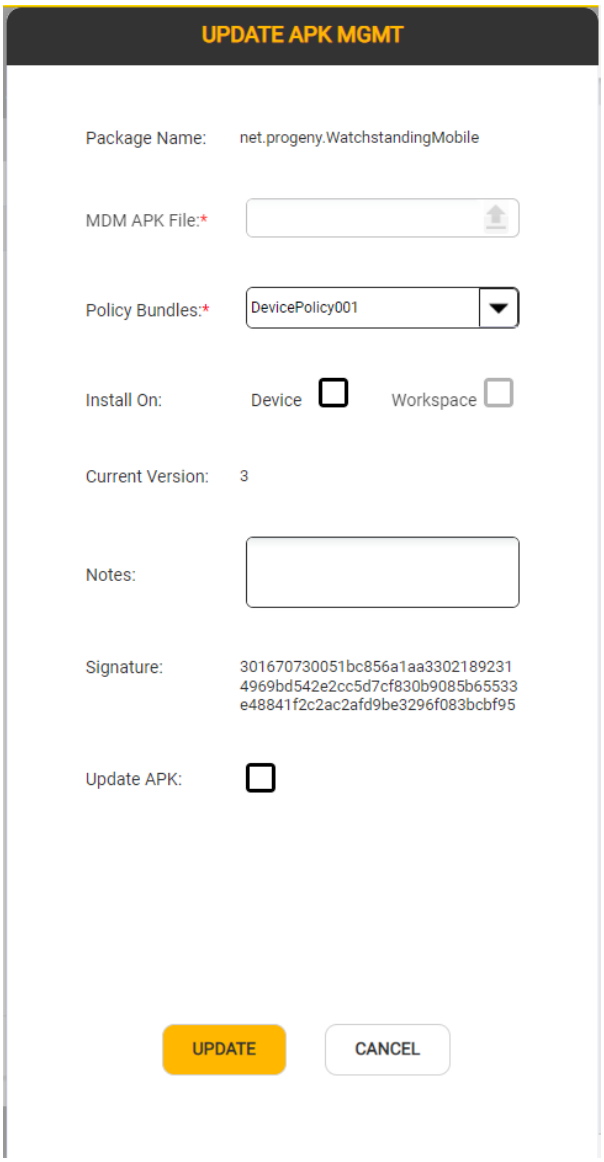


Figure 16 - APK Management Edit Window

The GovShield Client will download the APK (new or update) during the next periodic cycle. Once the application is downloaded, the Android OS will validate the digital signature and if successfully verified will install the APK. Upon successful completion or failure of the installation, the GovShield Client will send an alert message to the GovShield Server. The updated GovShield Client version can be verified by clicking the cog on the home screen and then selecting the *About*. This displays the version of the GovShield Client.

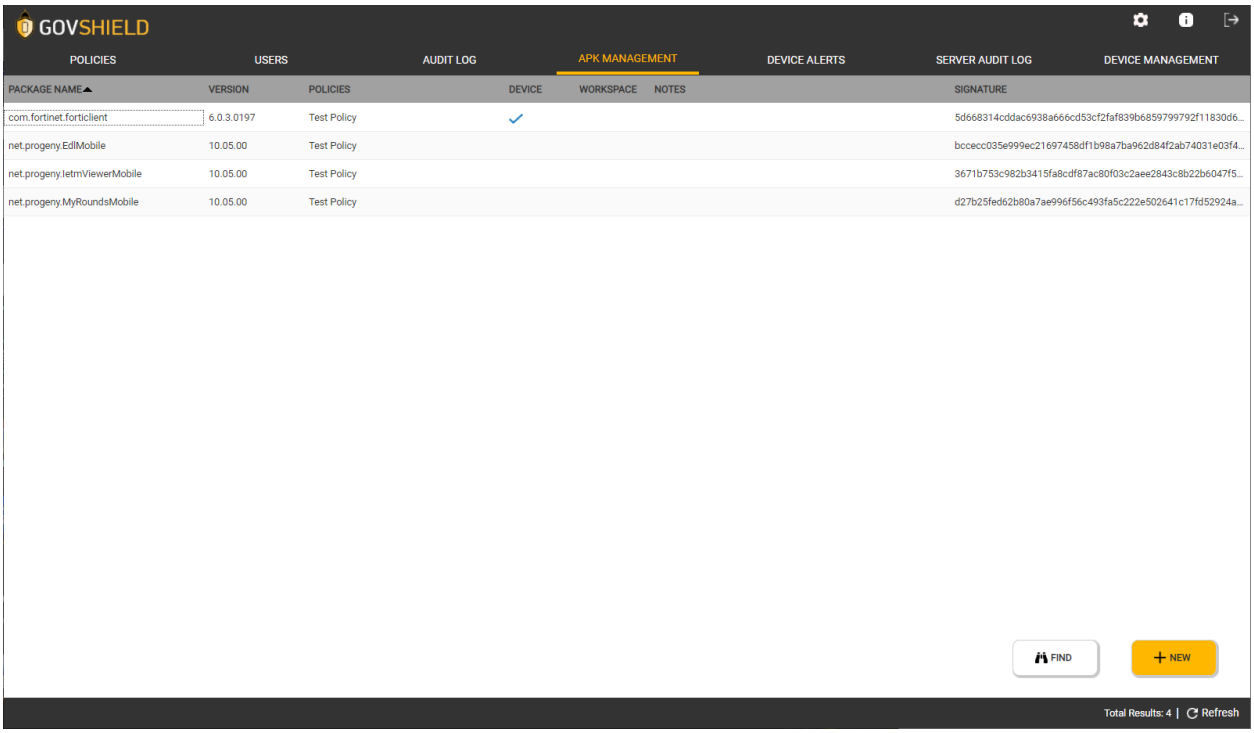


Figure 17 - APK Management

6 Device Alerts

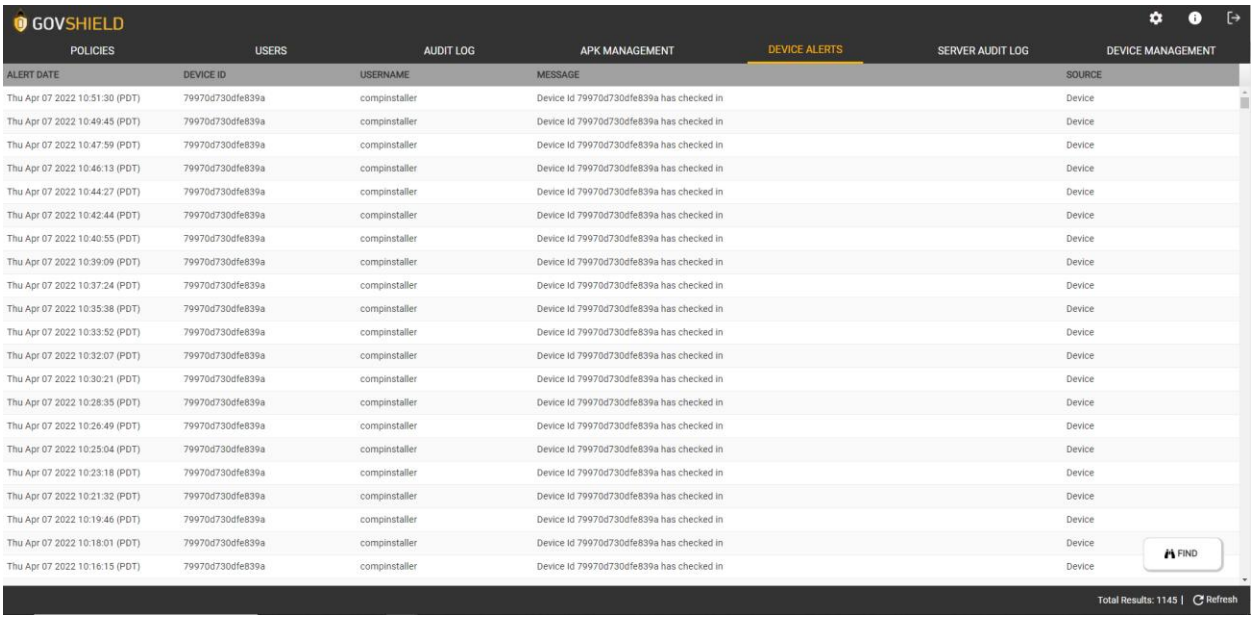


Figure 18 - Device Alerts

The Device Alerts Tab shows a record of events and changes performed on the device. The captured events are recorded describing how an activity is performed and how the system responded.

The Device Alert list can be search. To search the Device Alert list, perform the following steps:

1. Click the “FIND” button”
2. Enter desired search criteria
3. Click the “APPLY” button

To clear the search the results, perform the following steps:

1. Click the “FIND” button
2. Click the “CLEAR” button
3. Click the “APPLY” button

7 Device Audit Logs

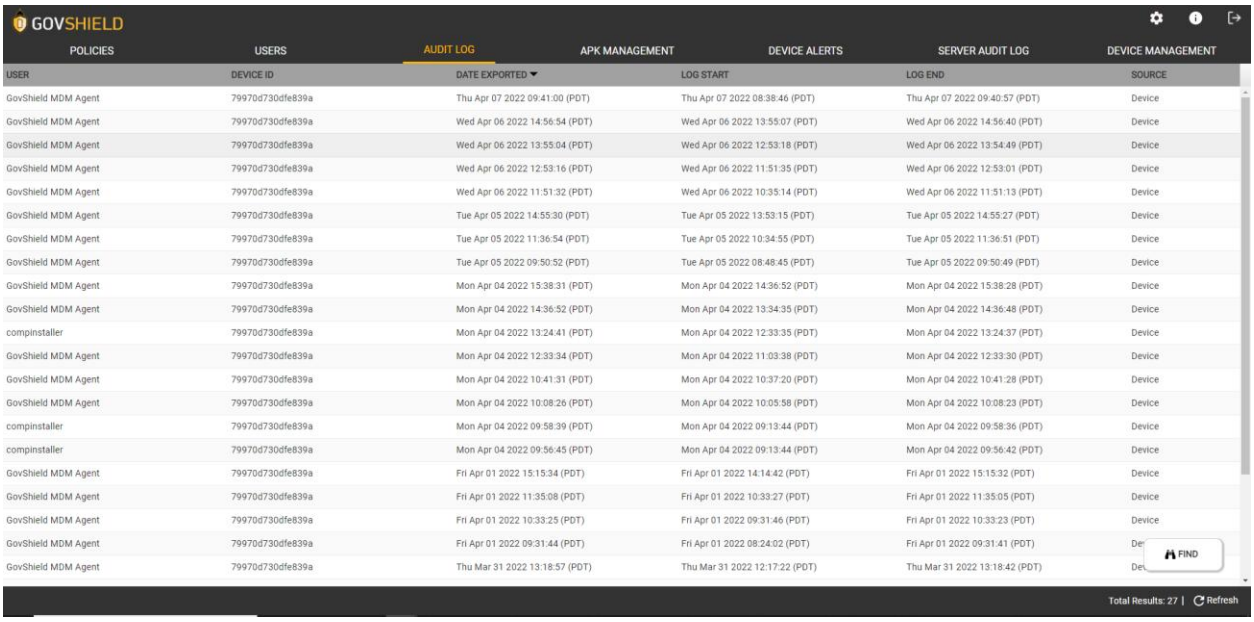


Figure 19 - Audit Report List

The *AUDIT LOG* page shows reports of log messages from devices being managed by the MDM server. The reports can be identified by the device ID and the username associated with each report. If a user is not logged into the client application when GovShield sends an audit report, the username is recorded as "GovShield MDM Agent". Information about each report includes the export date of the report, the start date/time of the logs, the end date/time of the logs and if it came from a device or a workspace. The logs in each report detail different actions and information about what the client application is doing.

To view the log messages in an audit report,

1. Select the audit report you wish to view.
2. Click the *VIEW* button.

Both the list of audit reports and the log message list in each report can be filtered. The list of audit reports can be filtered by username, device ID, export date, start date, end date, and log source. The list of log messages in each report can be filtered by their log level and message contents.

To filter either the list of audit reports or the audit report log messages,

1. Click the *FIND* button.
2. Fill out the information to filter the list by.

3. Click the *APPLY* button.

To cancel either list filter,

1. Click the *FIND* button.
2. Click the *CLEAR* button.
3. Click the *APPLY* button.

Each log message can be viewed individually in its own window. This window shows the application that caused the log, the timestamp of the log, and the log message.

To view an individual log message,

1. Open up an audit report.
2. Select the log you wish to view.
3. Click the *VIEW* button.

Figure 20 - Audit Report Log Message

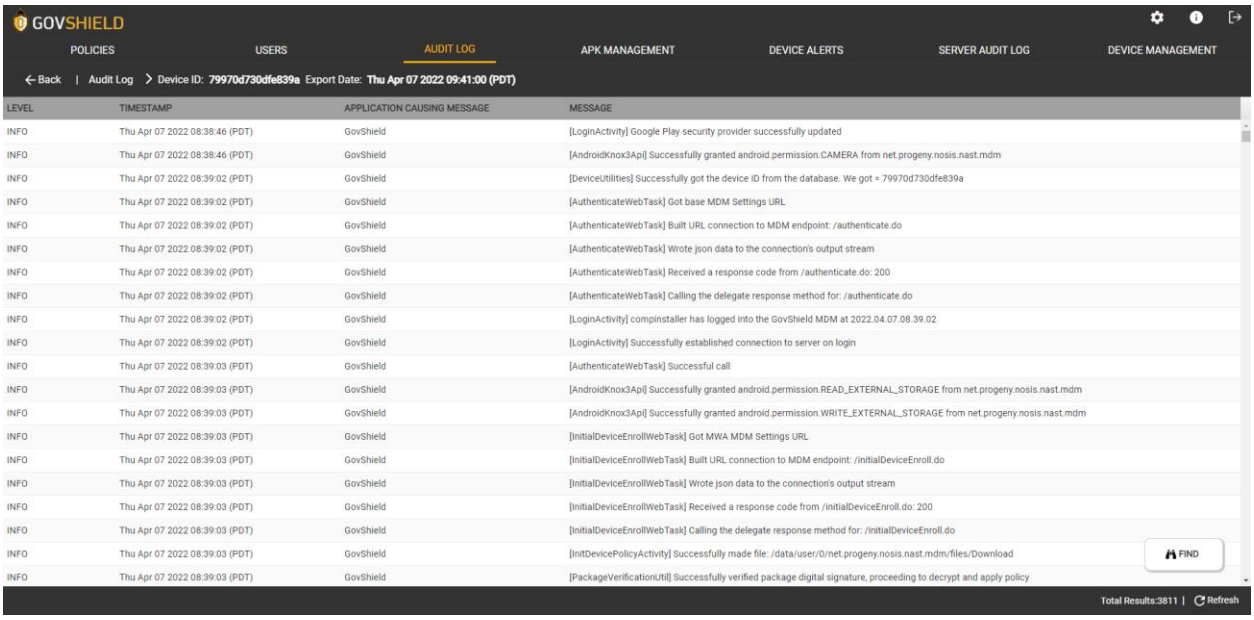
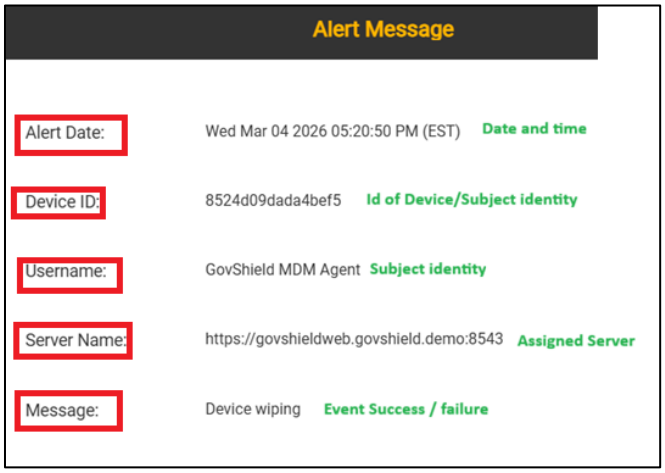
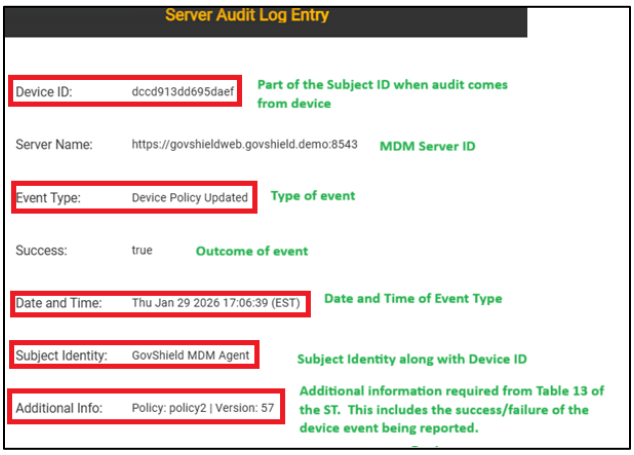


Figure 21 – Audit Report Log Messages view

7.1 Audit Record Explanation

Each Device audit record uses a templated box that has a Date and Timestamp, identifies the Device ID as part of subject identity, Username as part of subject identity, Server Name to which device is assigned, Message which is the Event Type and Success/Failure. The audit record information is the same but is displayed slightly differently depending on whether it is viewed on the Alerts page or the Server Audit Log Entry page. Examples of both formats are depicted below.





7.2 Example Audit Records

Requirement	Auditable Events	Additional Audit Record Contents
FAU_ALT_EXT.2	Success/failure of sending alert.	No additional information.

Alert Message

Alert Date:	Wed Feb 14 2024 09:47:29 AM (EST)
Device ID:	fd62a940039bec3e
Username:	GovShield MDM Agent
Server Name:	https://govshieldweb.govshield.demo:8543
Message:	Device Id fd62a940039bec3e has checked in

with connectivity to server

Alert Message

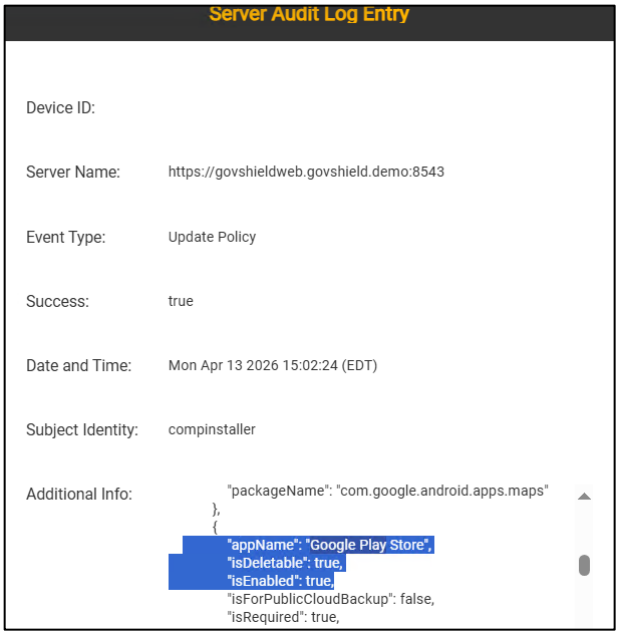
Alert Date:	Wed Feb 14 2024 09:58:50 AM (EST)
Device ID:	fd62a940039bec3e
Username:	GovShield MDM Agent
Server Name:	https://govshieldweb.govshield.demo:8543
Message:	Device Id fd62a940039bec3e failed to check in

without connectivity to server

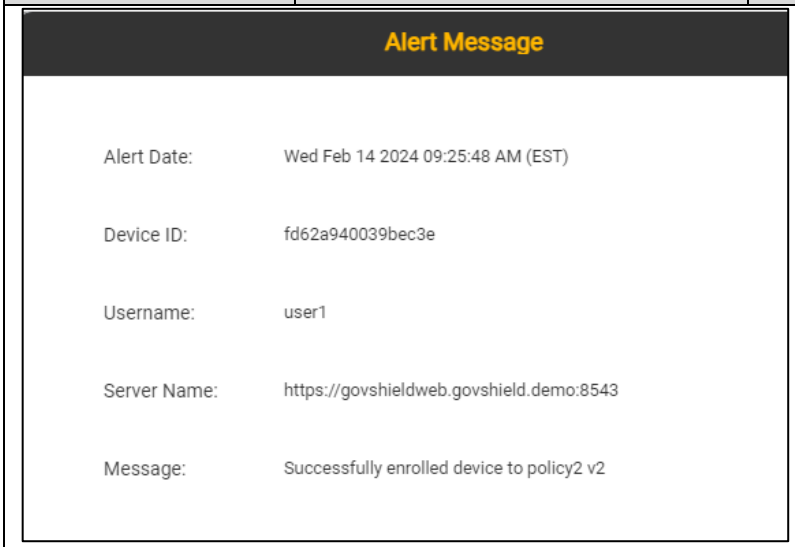
FAU_SEL.1(2)	All modifications to the audit configuration that occur while the audit collection functions are operating.	No additional information.

There is no specific configuration to turn on and off auditing on the TOE, thus the GovShield Client and its underlying platform will always perform auditing. However, an Authorized Administrator creates policies on the GovShield Server and will assign them to one or more Android Mobile Devices. These policies include requirements for the GovShield Client to generate audit records for the functionality configured in the policies. Once the GovShield Client receives and applies a policy requiring auditing, the GovShield Client will always generate the necessary audit records. For example, the following policy update creates the need to download an application, and the audit record for a failed installation of the application (per FAU_GEN.1(2)) would only be generated based upon

Requirement	Auditable Events	Additional Audit Record Contents
this policy being created and consumed by the GovShield Client. For this reason, the selection of auditable events is configurable through policy.		

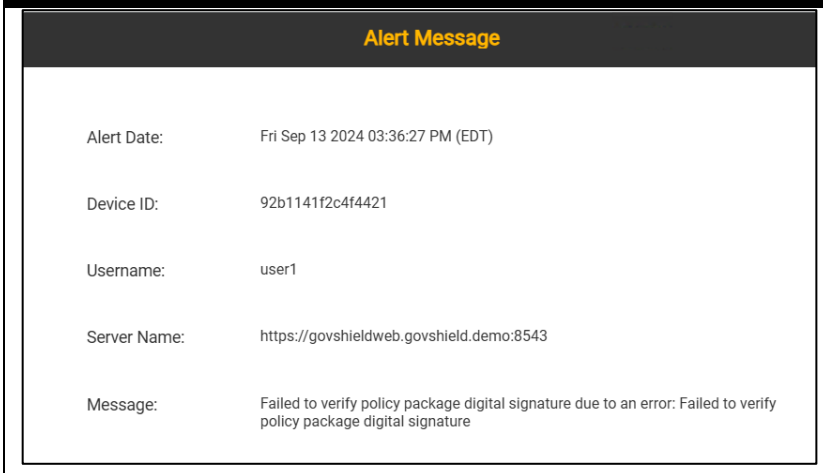


FIA_ENR_EXT.2	Enrollment in management.	Reference identifier of MDM Server.

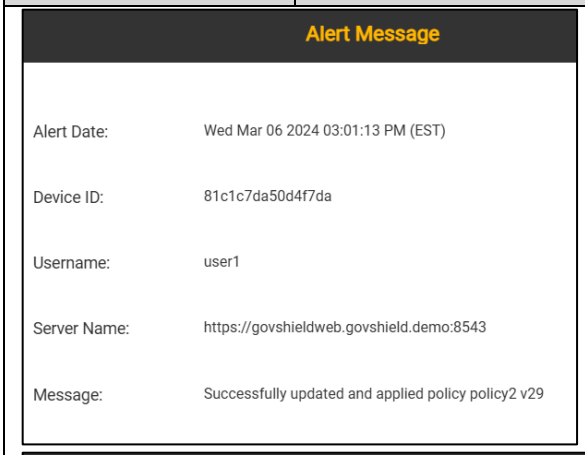


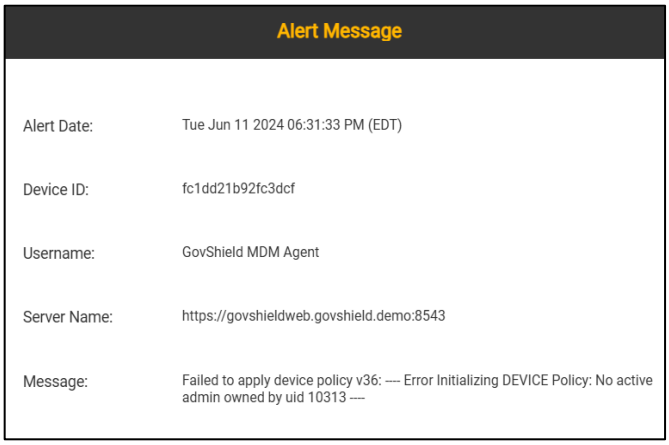
FMT_POL_EXT.2	Failure of policy validation.	Reason for failure of validation.

Requirement	Auditable Events	Additional Audit Record Contents

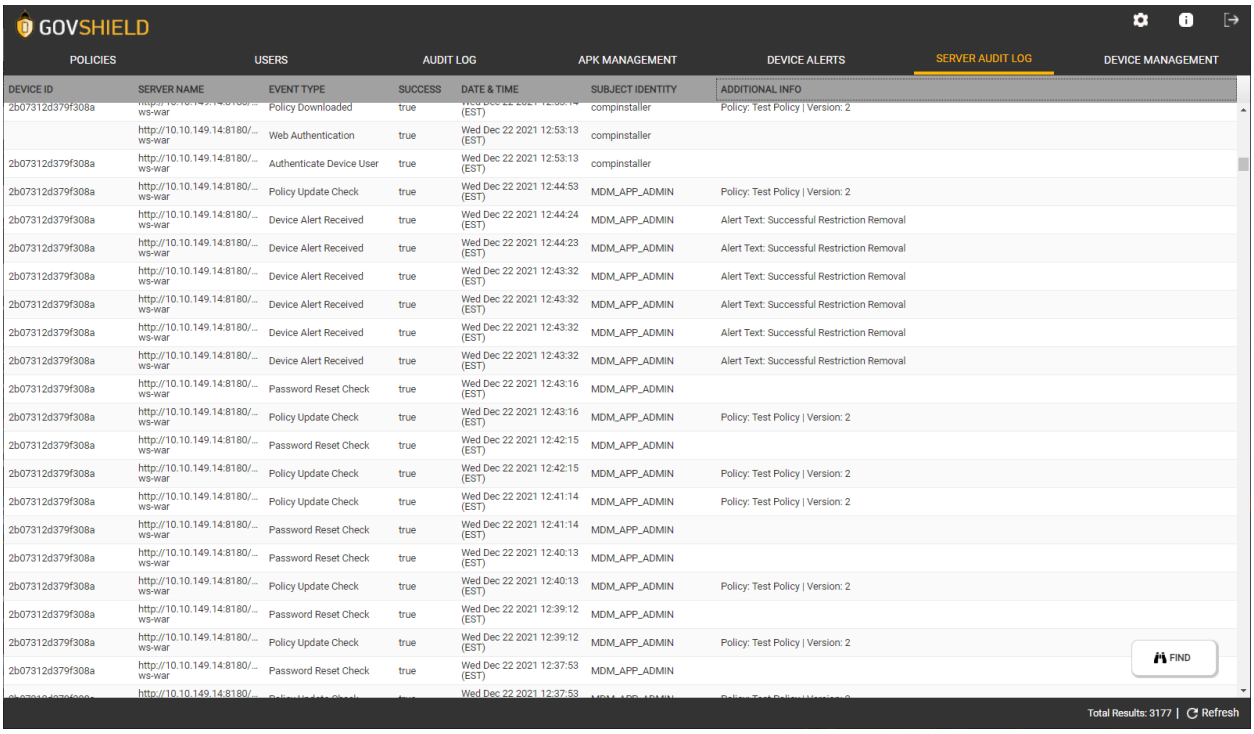


FMT_SMF_EXT.4	Outcome (Success/failure) of function.	No additional information.





8 Server Audit Logs



All GovShield server activity events can be monitored via the Server Audit Log tab. Server Event Type that are shown in the Server Audit Log are:

- App Details
- App Downloaded
- App Downloaded Check
- App Install
- App Restrictions Upload
- App Uninstall
- App Updated
- Assign Policy
- Audit Log Received
- Authenticate Device User
- Banner Updated

- Certificate Downloaded
- Create Policy
- Delete Policy
- Device Alert Check
- Device Alert Created
- Device Alert Received
- Device Authentication
- Device Not Whitelisted
- Device Policy Copied
- Device Policy Default
- Device Query
- Device Software Updated
- Device Un-enrolled
- Device Unenroll Check
- Device Whitelisted
- Display Banner
- Display Default Data
- Display Device Log Data
- Display Device Pairings
- Display Policy List
- Display User Data
- Enroll Device
- Image Download
- Import Bundle XML
- Lock Device
- Lock Device Command Received
- New App Uploaded
- Password Reset Check

- Policy Details
- Policy Downloaded
- Policy Update Check
- Reachability Event
- Save Device Audit Log
- Un-enroll Device
- Update Policy
- User Created
- User Deleted
- User Updated
- View Policy
- Web Authentication
- Whitelist Device
- Wipe Device
- Wipe Device Command Received

The Server Audit Log list can be search. To search the Log, perform the following steps:

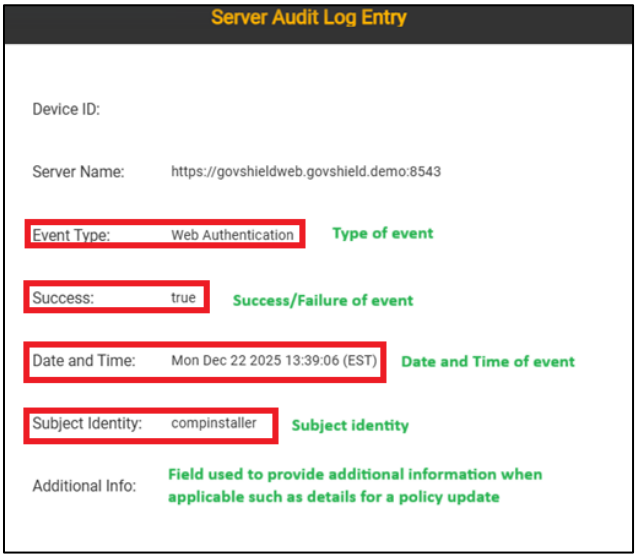
1. Click the “FIND” button”
2. Enter desired search criteria
3. Click the “APPLY” button

To clear the search the results, perform the following steps:

1. Click the “FIND” button
2. Click the “CLEAR” button
3. Click the “APPLY” button

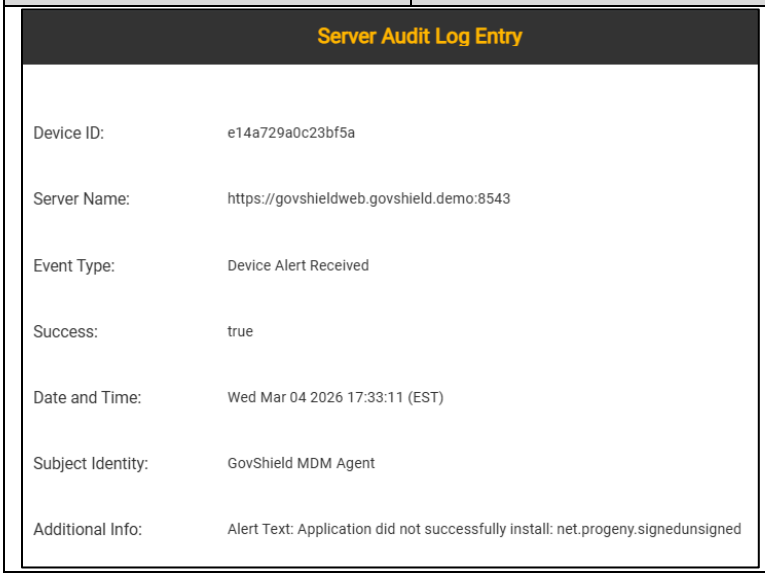
8.1 Audit Record Explanation

Each MDM Server record uses a templated box that identifies the Device ID (if applicable), Server Name, Event Type, Success/Failure, Date and Time, Subject Identity, and Additional Information.

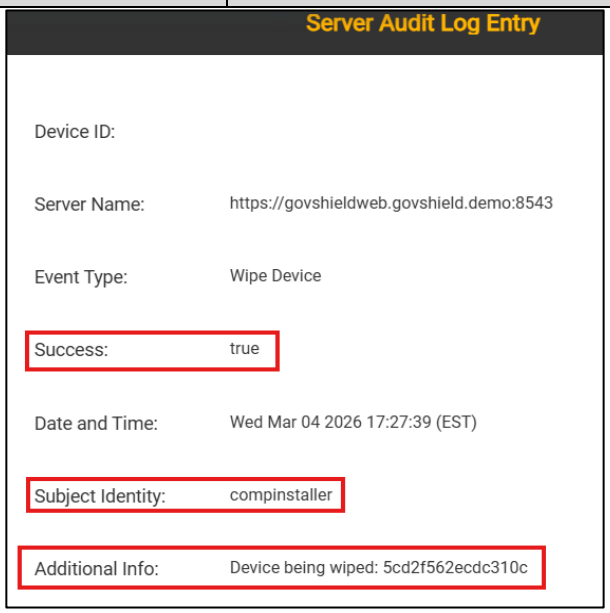


8.2 Example Audit Records

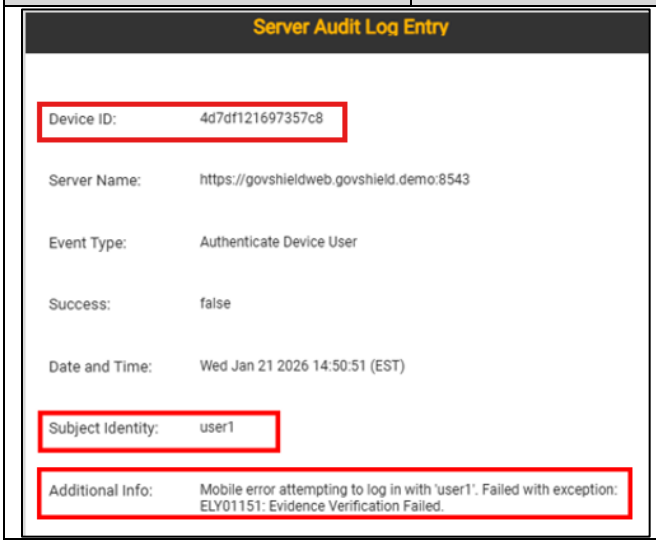
Requirement	Auditable Events	Additional Audit Record Contents
FAU_ALT_EXT.1 (man)	Type of alert.	Identity of Mobile Device that sent alert.



FCO_CPC_EXT.1 (obj)	Enabling or Disabling communications between a pair of components.	Identities of the endpoints pairs enabled or disabled.



FCS_RBG_EXT.1 (man)	Failure of the randomization process.	No additional information.
Note: Platform auditing is responsible for generating RBG failure audit records.		
FIA_ENR_EXT.1 (man)	Failure of MD user authentication.	Presented username.

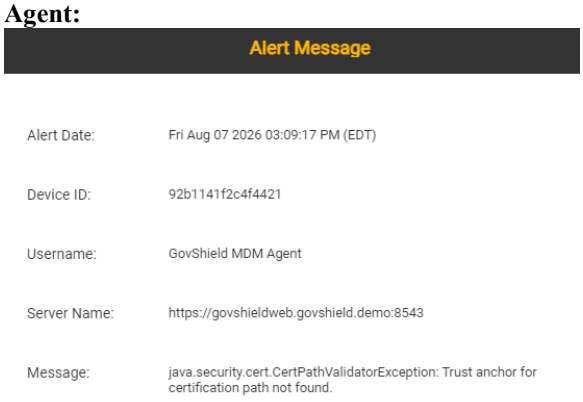


FIA_X509_EXT.1(1) (man)	Failure to validate X.509 certificate.	Reason for failure.

Note: Platform auditing is responsible for generating X509 validation audit records for: (1) TLS/HTTPS communication, and (2) verifying signed policies is invoked by the GovShield Client platform's signature services.

Server:
2026-03-04 14:29:48,096 INFO [org.springframework.web.servlet.mvc.method.annotation.RequestMappingHandlerMapping] (ServerService Thread Pool -- 96) Mapped "{[/mwaDeviceAccess/saveDeviceAlert],methods=[POST]}" onto public void mil.navy.mdm.controller.MdmDeviceAccessController.saveDeviceAlert(javax.servlet.http.HttpServletRequest,mil.navy.mdm.ejb.entity.mdm.DeviceAlert,javax.servlet.http.HttpServletResponse) throws mil.navy.mdm.ejb.exception.NosisEJBValidationException,java.net.UnknownHostException

Agent:

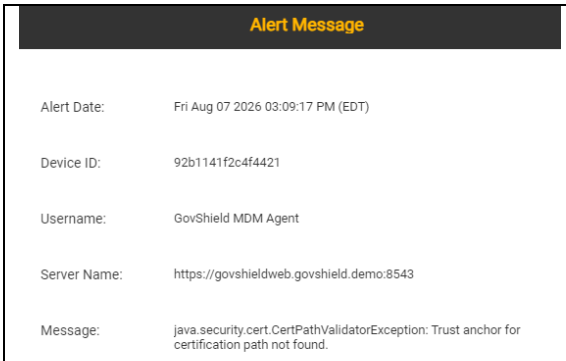


FIA_X509_EXT.2 (man)	Failure to establish connection to determine revocation status.	No additional information.

Note: Platform auditing is responsible for generating X509 validation audit records for: (1) TLS/HTTPS communication, and (2) verifying signed policies is invoked by the GovShield Client platform's signature services.

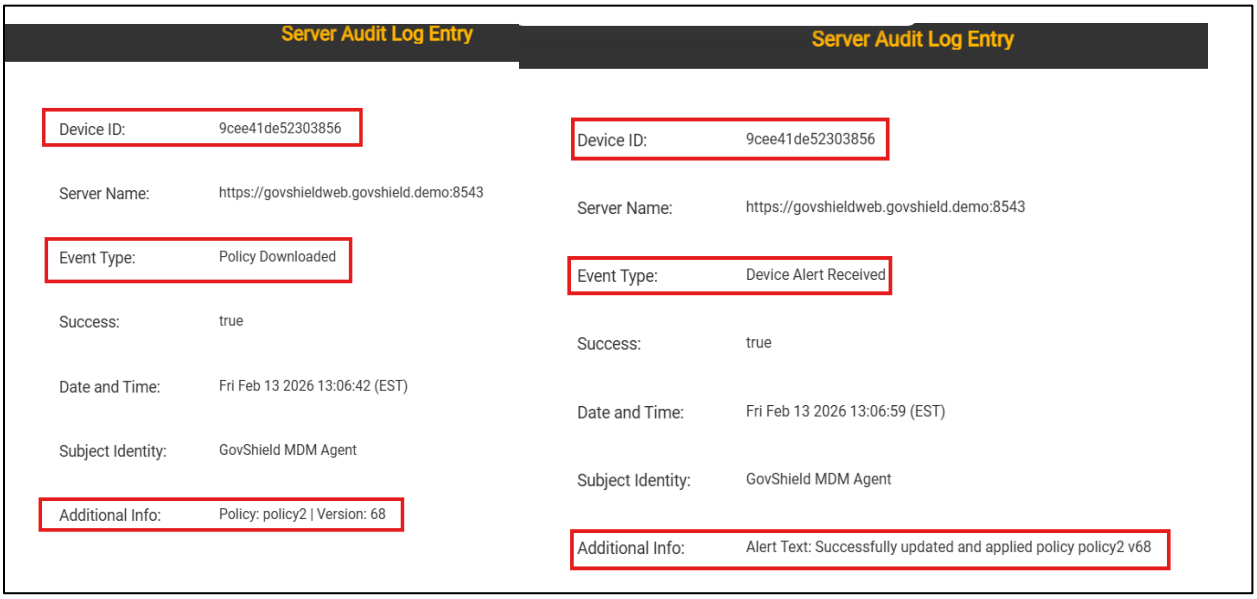
Server:
2026-02-20 15:06:59,649 ERROR [stderr] (default task-1) javax.net.ssl|SEVERE|BF|default task-1|2026-02-20 15:06:59.648 EST|null:-1|Fatal (CERTIFICATE_UNKNOWN): sun.security.validator.ValidatorException: PKIX path validation failed: java.security.cert.CertPathValidatorException: Certificate revocation check failed: could not determine revocation status

Agent:

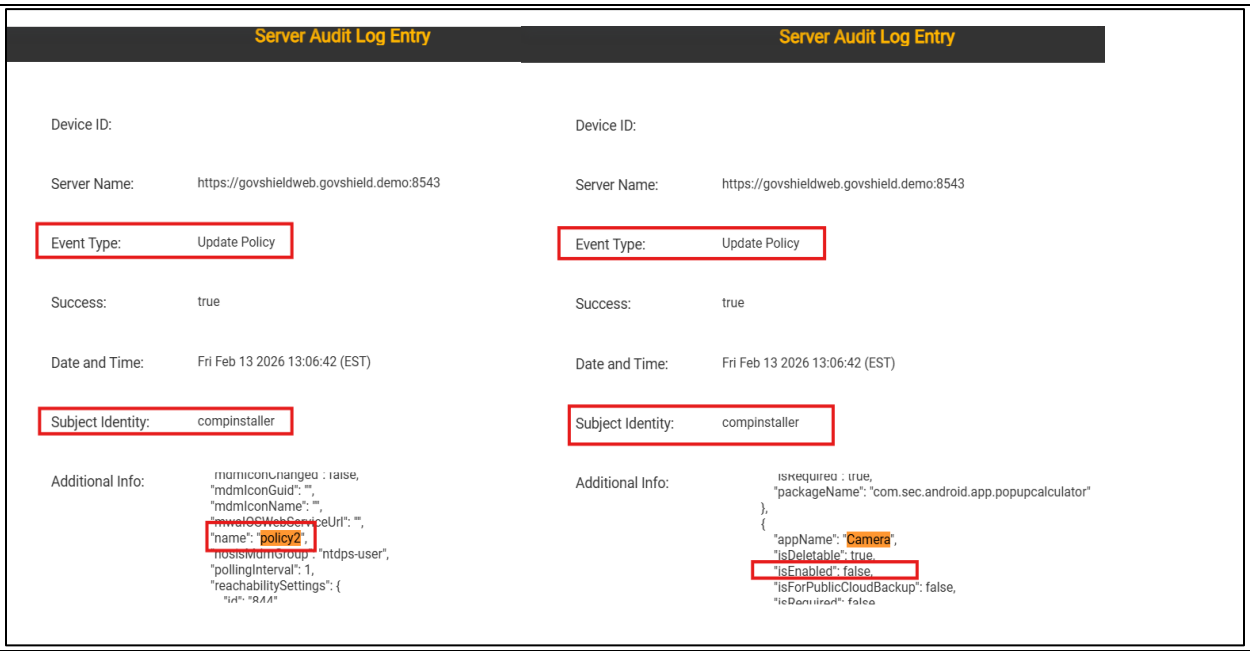


FMT_MOF.1(1) (man)	Issuance of command to perform function. Change of policy settings.	Command sent and identity of MDM Agent recipient(s). Policy changed and value or full policy.

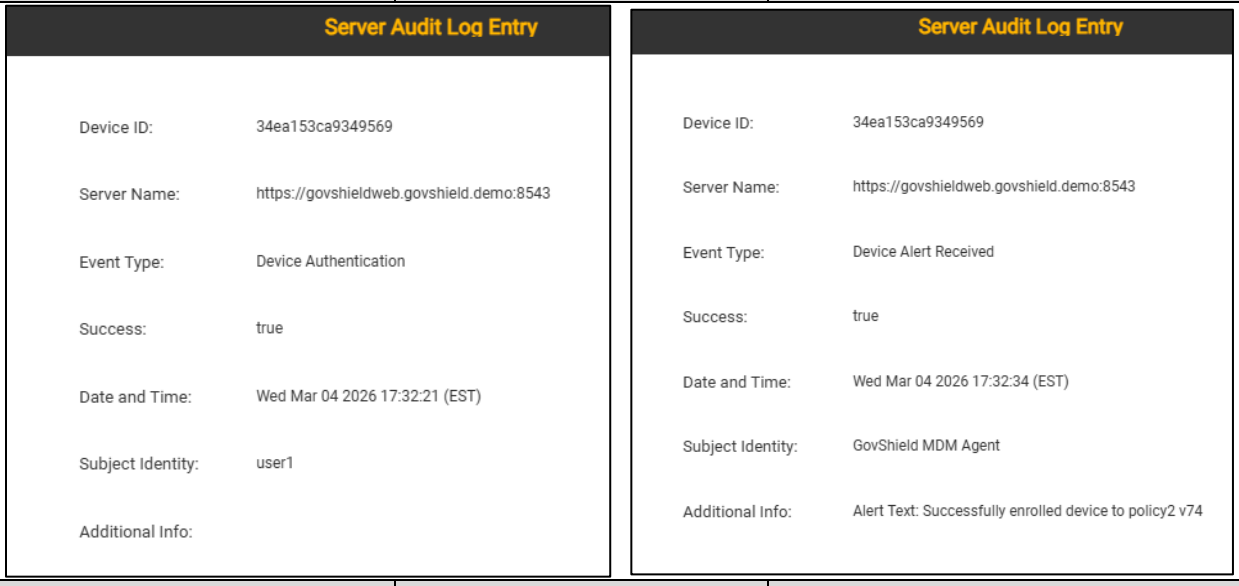
Issuance of command to perform function.



Change of policy settings.

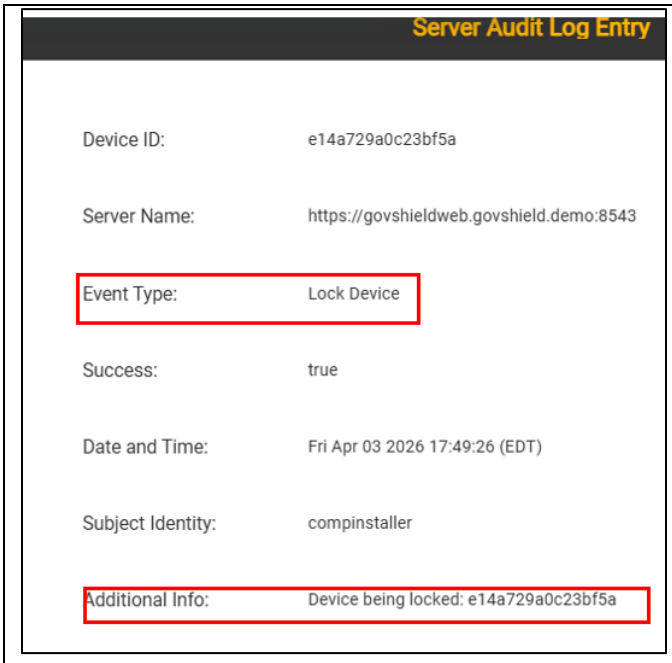


FMT_MOF.1(2) (man)	Enrollment by a user.	Identity of user.

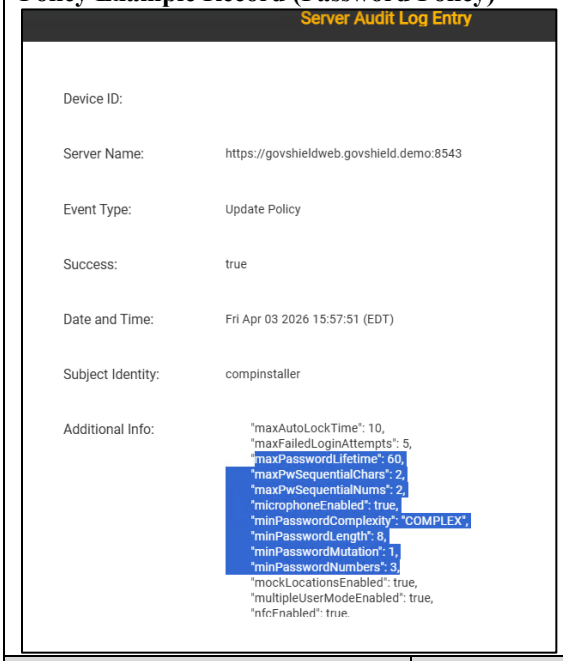


FMT_SMF.1(2) (man)	Success or failure of function.	No additional information.

Command Example (Transition to the Locked State)



Policy Example Record (Password Policy)

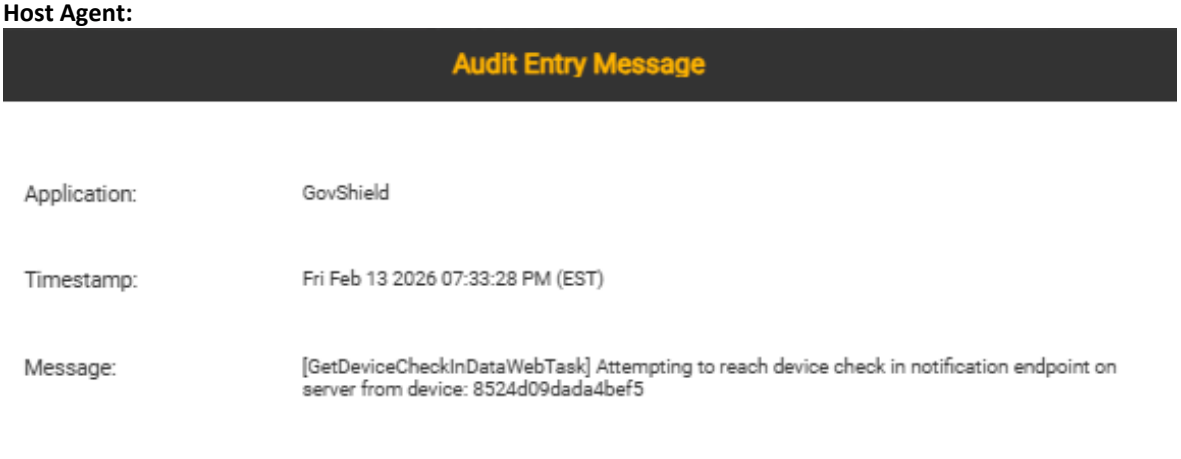


FPT_ITT.1(2) (sel)	Initiation and termination of the trusted channel.	Trusted channel protocol. Identity of initiator and recipient.

Note: Platform auditing is responsible for generating X509 validation audit records for: (1) TLS/HTTPS communication, and (2) verifying signed policies is invoked by the GovShield Client platform's signature services.

Server:
2026-04-16 14:04:32,967 INFO [mil.navy.tls.audit] (default I/O-1) accepting connection from 10.137.2.69:25452
2026-04-16 14:04:32,968 INFO [mil.navy.tls.audit] (default I/O-1) established connection with 10.137.2.69:25452 (cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256)
2026-04-16 14:05:50,981 INFO [mil.navy.tls.audit] (default I/O-1) disconnected from 10.137.2.69:25452

Host Agent:



FPT_TST_EXT.1 (man)	Initiation of self-test. Failure of self-test. Detected integrity violation.	Algorithm that caused failure. The TSF code file that caused the integrity violation.

Note: Platform auditing is responsible for generating self-test mechanisms audit records.

Initiation of Self-Test:

2024-08-28 12:45:04,202 INFO [org.jboss.as.jpa] (ServerService Thread Pool -- 73) WFLYJPA0010: Starting Persistence Unit (phase 1 of 2) Service 'MDM-NIAP.ear/MDM-ejb.jar#MDM'

Failed Self-Test

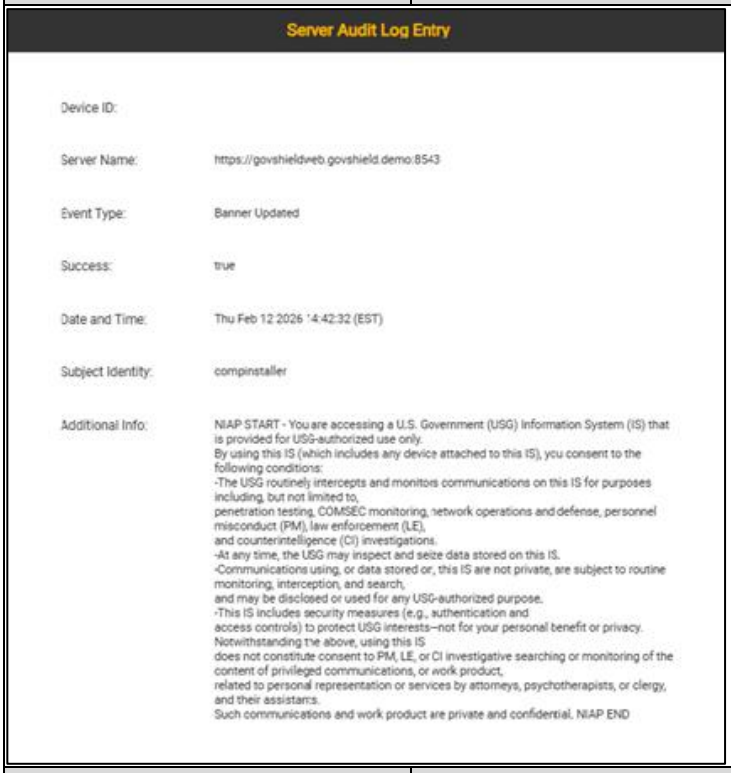
2024-08-28 12:12:12,053 INFO [org.jboss.as.controller] (DeploymentScanner-threads - 1) WFLYCTL0183: Service status report
WFLYCTL0186: Services which failed to start: service jboss.deployment.unit."MDM-NIAP.ear".STRUCTURE: WFLYSRV0153: Failed to process phase STRUCTURE of deployment "MDM-NIAP.ear"

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

Note: Platform auditing is responsible for generating audit records for the checking of the digital signature for software updates.

2026-02-26 13:5543,146 ERROR [org.jboss.msc.service.fail] (MSC service thread 1-4) MSC000001: Failed to start service
Caused by: org.jboss.as.server.deployment.DeploymentUnitProcessingException: SECURITY REJECTION: The parent EAR 'MDM_1.60.03_unsigned.ear' is NOT digitally signed. Blocking deployment of: MDM-ejb.jar

FTA_TAB.1 **(opt)**	Change in banner setting.	No additional information.



FTP_ITC.1(1) **(man)**	Initiation and termination of the trusted channel.	Trusted channel protocol. Non-TOE endpoint of connection.

Initiation during startup and is persistent.

2026-04-16 14:03:24,231 INFO [org.flywaydb.core.internal.dbsupport.DbSupportFactory] (ServerService Thread Pool -- 90) Database: jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=govshielddb.govshield.demo)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=ntdps))) (Oracle 19.0)

Failed:
2025-12-18 16:42:59,499 WARN [org.hibernate.engine.jdbc.env.internal.JdbcEnvironmentInitiator] (ServerService Thread Pool -- 74) HHH000342: Could not obtain connection to query metadata : javax.resource.ResourceException: IJ000453: Unable to get managed connection for java:/NTDPSOracleDS

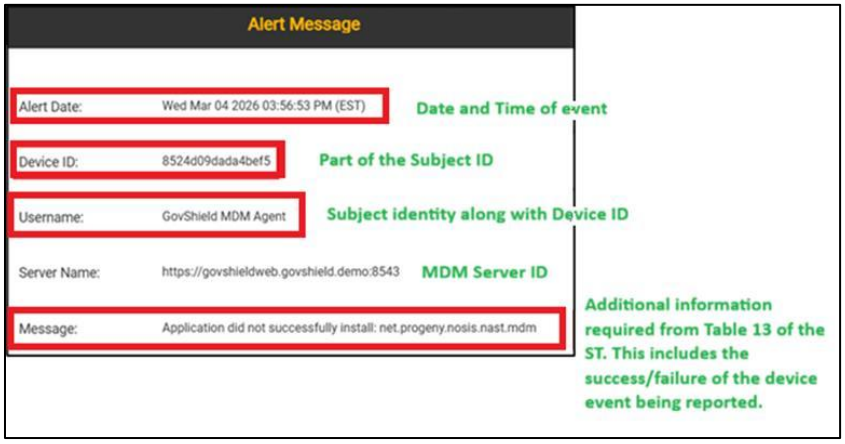
FTP_TRP.1(1) **(man)**	Initiation and termination of the trusted channel.	Trusted channel protocol. Identity of administrator.

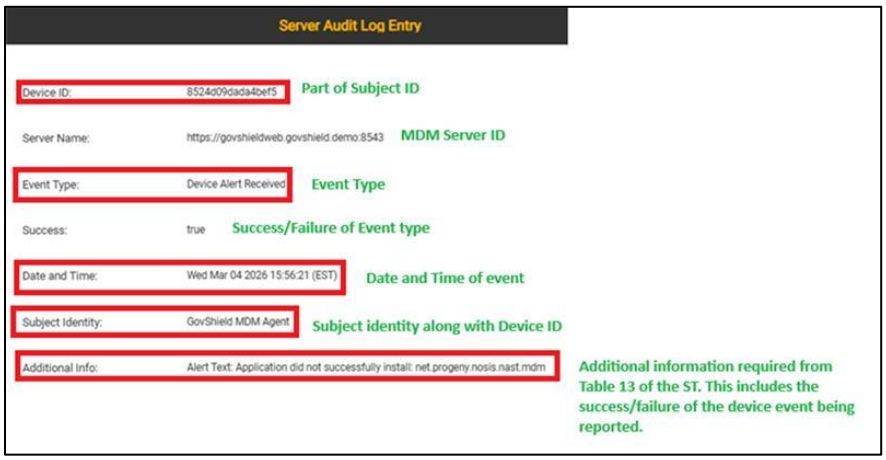
2026-04-16 14:35:08,832 INFO [mil.navy.tls.audit] (default I/O-3) accepting connection from 192.168.0.106:32443
2026-04-21 09:11:03,701 INFO [mil.navy.tls.audit] (default I/O-3) established connection with 192.168.0.106:32443 (cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256)

2026-04-21 09:11:03,725 INFO [mil.navy.tls.audit] (default I/O-3) disconnected from 192.168.0.106:32443		
FTP_TRP.1(2) (man)	Initiation and termination of the trusted channel.	Trusted channel protocol.
Note: Platform auditing is responsible for generating TLS/HTTPS communication audit records 2026-04-16 14:04:32,967 INFO [mil.navy.tls.audit] (default I/O-1) accepting connection from 10.137.2.69:25452 2026-04-16 14:04:32,968 INFO [mil.navy.tls.audit] (default I/O-1) established connection with 10.137.2.69:25452 (cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) 2026-04-16 14:05:50,981 INFO [mil.navy.tls.audit] (default I/O-1) disconnected from 10.137.2.69:25452		

8.3 MAS Server Audit Record Explanation

Each MAS Server record uses a templated box that identifies the Device ID (if applicable), Server Name, Event Type, Success/Failure, Date and Time, Subject Identity, and additional information. The audit record requires an alert message (first figure) from the device to be sent and received by the MDM server (second figure) for application installation, including failing to push a new application and failing to update an existing application on a managed mobile device.





9 System Settings

GovShield contains a menu option to view different system settings. These settings include system configuration options, an option to provision a device through a QR code, and an About page describing the system. To view the System Settings options, click the gear icon in the top right corner of the screen.

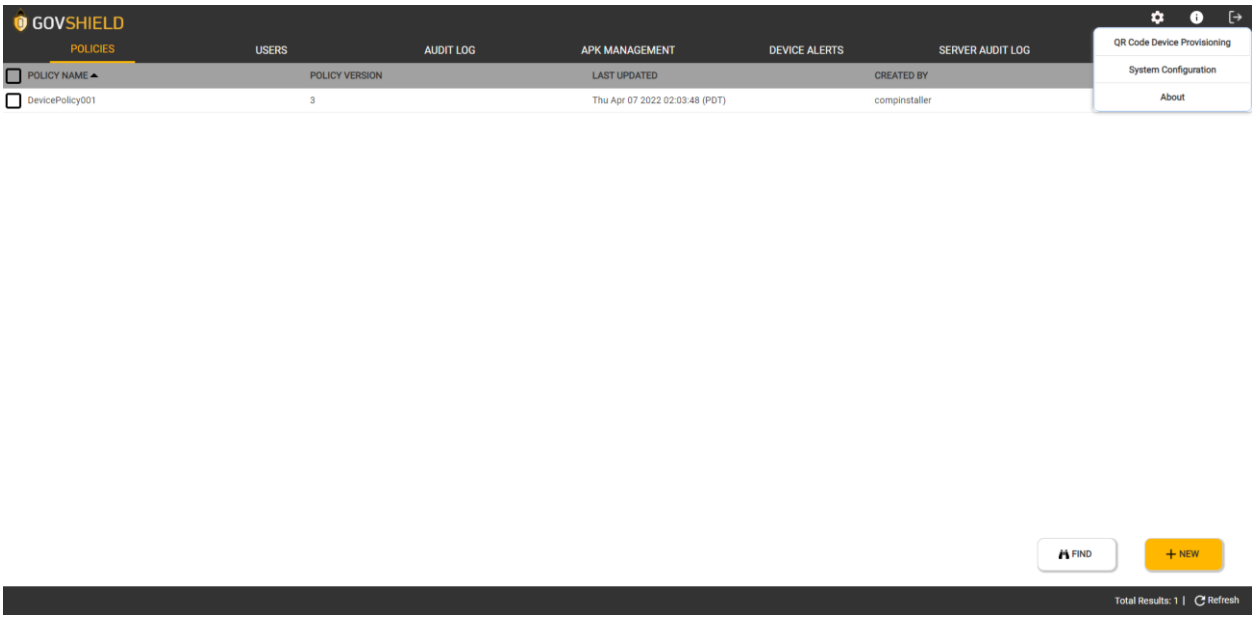


Figure 22 - System Settings Option Menu

9.1 System Configuration

System Configuration options allow you to create/view a signing certificate that will be used to secure policy bundles for sending to devices, along with setting the consent banner message that administrators must accept before logging in to the GovShield Server.

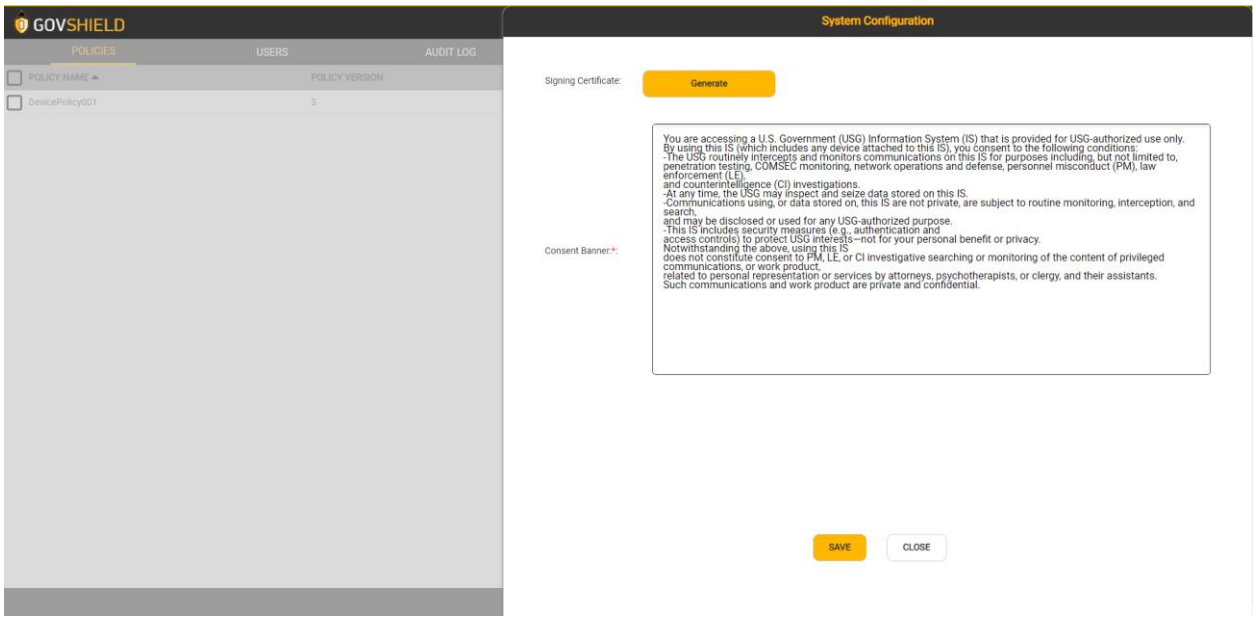


Figure 23 - System Configuration Window

9.1.1 Signing Certificate

The signing certificate is used by the GovShield Server to sign security policy bundles before they are sent to a managed device. If the signing certificate cannot be found, then an administrator must create one through the System Configuration page by clicking the ‘enerate’ button. After creating a signing certificate, the serial number, creation date, and expiration date can be viewed.

9.1.2 Consent Banner

The consent banner contains a message that administrative users must accept before accessing the GovShield web application. The consent banner contains usage terms that the user agrees to when they click the *ACCEPT* button. An administrator can edit the message on the consent banner through the System Configuration page.

9.2 QR Code Device Provisioning

Provisioning a device is provided through the System Settings menu, provisioning via QR code. An administrator can create a QR code for provisioning by uploading an APK of the GovShield agent application and specifying a WiFi network with credentials. After supplying this information, the administrator can click the *SAVE* button and a QR code will be created.

Within the QR code there is an embedded URL for the GovShield Server. The GovShield Client will record the URL of the GovShield Server during a successful enrollment of the Android

Mobile Device. The URL will then be used as the GovShield Server's reference identifier for subsequent communications between the GovShield Client and GovShield Server.

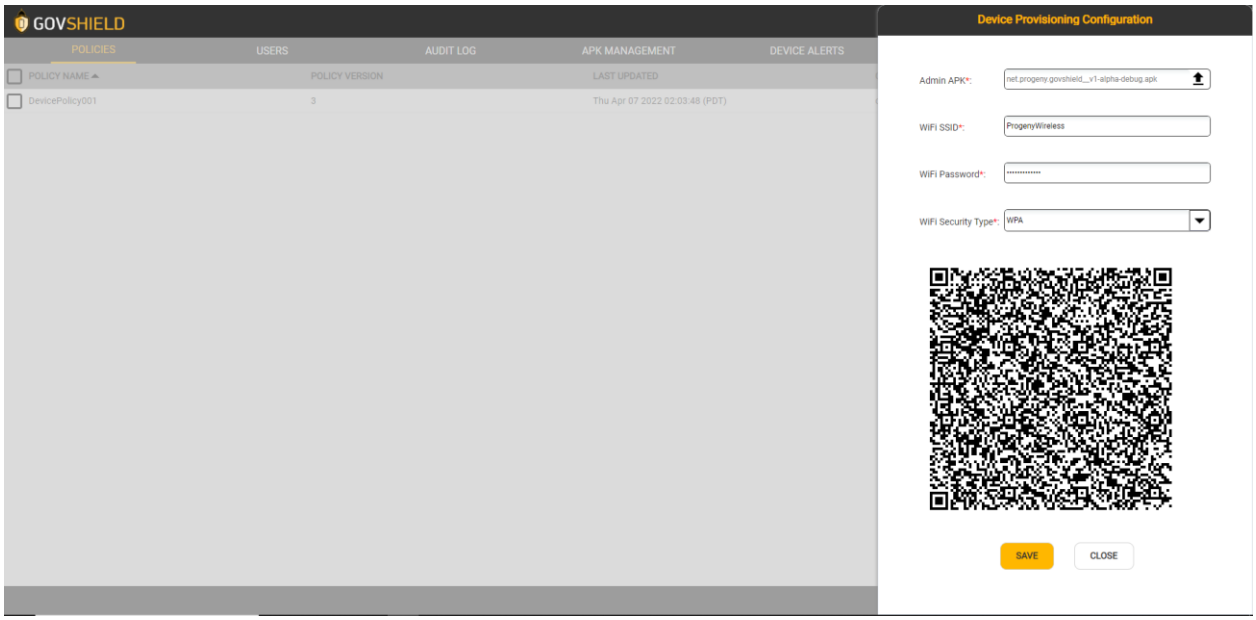


Figure 24 - QR Code Device Provisioning

To provision a device with a QR code, the device must be factory reset. After the reset, tap the same spot on the screen 7 times, the device will restart and then open up a camera view. After scanning the previously created QR code, the device will install the GovShield agent application, give it device ownership, and provision the device with the default security policy.

To complete the enrollment of a device complete the following steps:

1. As part of the Android device setup, on each setup screen, disable any options and click the next button until the device home screen loads.
2. Load the GovShield Server's Root Certificate Authority Public Certificate per the directions in Section 10.1 'Load CA Public Certificate on the Android Device'.
3. Whitelist the device by completing the steps in Section 2.1 'Whitelist a New Device'.
4. Enter the username and password combination for the user or Administrator.

If the above steps are successful, the GovShield Server requests an X.509v3 certificate using Certificate Management Protocol (CMP) from the CA Server. The enrolling Android Mobile Device will use this unique X.509v3 certificate for post-enrollment HTTPS/TLS communications with the GovShield. The GovShield Server then creates an initial payload for that Android Mobile

Device which includes its unique X.509v3 certificate and the public key to verify the signature of policies received by the GovShield Client. The GovShield Server sends the initial payload to the GovShield Client for configuration and storage of the payload contents. The GovShield Client then downloads its assigned policy from the GovShield Server and will request its platform to verify the signed policy, before applying the policy. Included within the policy received by the GovShield Client is the Knox Key. Before any other part of the policy is applied, the GovShield Client provides the Knox Key (contains the Samsung Knox Licensing Server's FQDN) to the Android Mobile Device and the device connects to the Samsung Knox Licensing Server to register the Android Mobile Device's Knox license using the Knox Key. Once the Knox license is validated, the Android Mobile Device's Knox Platform is activated and the GovShield Client applies the remaining portions of the policy to the Android Mobile Device. Once complete, the GovShield Client informs the GovShield Server that the policy was implemented, and the enrollment process is complete.

9.3 Product Version

The *About* option in the System Settings menu of the web GUI displays a popup on the screen that contains the version of the GovShield MDM.

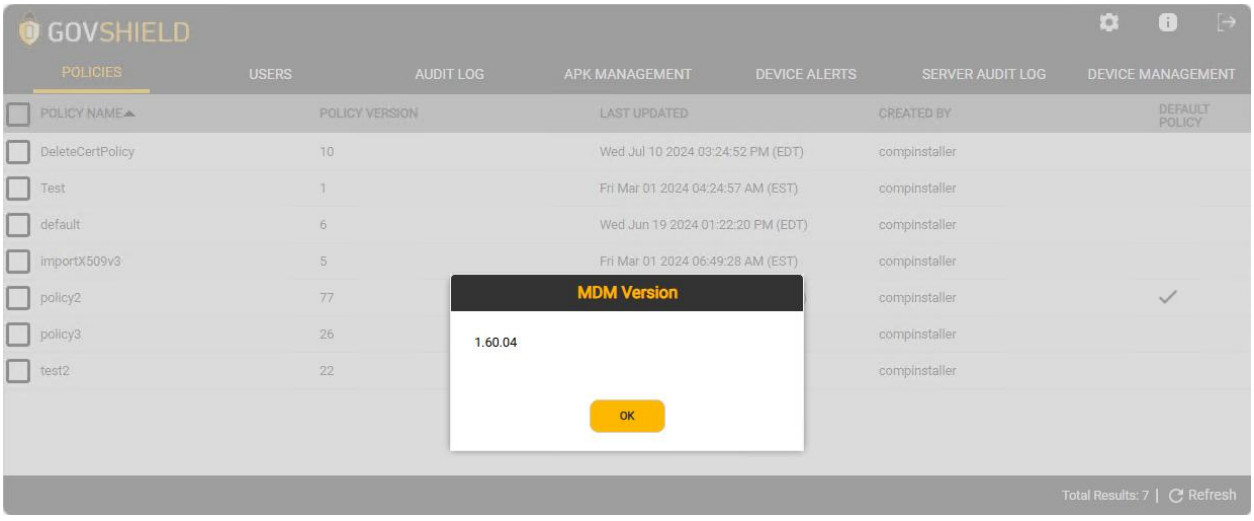


Figure 25 - MDM Version Information

The *About* popup, accessed by clicking the cog on the home screen, of the GovShield Client displays the version of the GovShield Client.

Figure 26 – GovShield Client Version Information

10 Device Setup

10.1 Load CA Public Certificate on the Android Device

All devices will need to have the Root Certificate Authority Public Certificate (Root Certificate) installed in the device's Security Certificates to trust all signed certificates. To do this, plug the device in the computer by USB cord, if not already connected, and copy the provided Root Certificate into a directory on the device. After copying is complete, open the GovShield Client Application and click the Gear Button. Click on the Install CA button and navigate to the location of the Root Certificate previously copied. Clicking on the certificate will install it to the device and the device can now trust the certificates sent by the MDM Server.

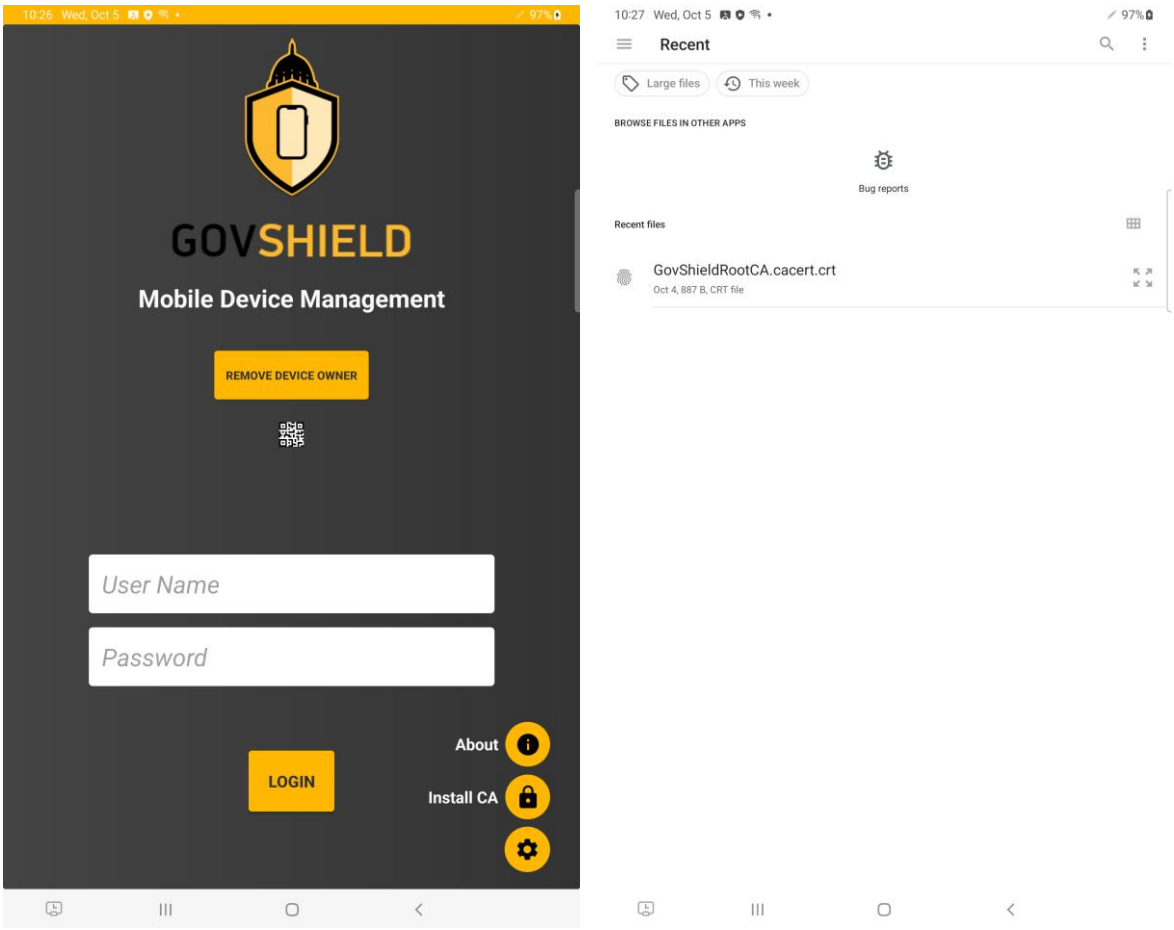


Figure 27 - Android Install CA Screens