VMware AirWatch Google Sync Integration Guide

Securing Your Email Infrastructure

Workspace ONE UEM v9.4

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Table of Contents

Chapter 1:
Overview

Introduction to Google Sync Integration

Organizations using the Gmail infrastructure may be familiar with the challenge of securing email endpoints for Gmail and preventing mail from circumventing the secure endpoint. Workspace ONE provides you with an end-to-end solution that allows you to fully integrate your Gmail infrastructure without compromising security.

Some benefits of integrating with Workspace ONE:

- Flexible configuration while maintaining tight integration
- Email monitoring and management
- Customizable access control
- Google Sync support

For more information on Google Sync, refer https://support.google.com/a/answer/135937?hl=en.

Requirements for Google Sync Deployment

You must fulfill the system requirements mentioned here in order to successfully integrate your corporate infrastructure with VMware AirWatch.

Disclaimer

Integration with third party product is not guaranteed and dependent upon the proper functioning of those third party solutions.

System Requirements

- Google admin account with Super Admin permissions.
- API Access to Gmail.

Note: The Gmail provisioning API version 2.0 and the new Directory API are not FIPS compliant.

- End users must accept the Google end-user license agreement.

Chapter 2:
Google Sync Integration

Integration Types

Workspace ONE offers different deployment models using which you can integrate Google Sync for your organization.

The different deployment methods decides the manner in which the Workspace ONE server communicates with the Gmail server. Workspace ONE server communicates indirectly with Google server through SEG in the Proxy deployment method. The Direct deployment method involves using the Google directory APIs or the password management configurations.

SEG Proxy Integration with and without Password Management

Classic SEG and SEG V2 supports this configuration. This configuration type involves the SEG Proxy server residing between the Workspace ONE server and the Gmail server. The SEG Proxy server ensures security by not allowing the enrolled devices to communicate directly with the Gmail server. With SEG, you get visibility of both the managed and unmanaged devices on the Email Dashboard. You can also leverage the available email policies.

Direct Integration with Directory APIs

In this configuration type, the Workspace ONE server uses Google's directory APIs to manage email access on mobile devices.

Direct Integration using Password Management

Using the password provisioning configuration type, the Workspace ONE server communicates directly with Google. Since the SEG server is not involved, this configuration uses password switching to block non-compliant devices. Based on your security needs, you may either choose to store or purge the password in your database. There are two types of configuration available:

- Integrating with password retention
- Integrating without password retention

Integrating with password retention

Using this configuration, the Workspace ONE server communicates with the Google directly and retains the Google password in the database by default. You can manage and monitor enrolled devices through the Email Dashboard. Devices are deemed compliant or non-compliant based on the email compliance policies configured within the Workspace ONE UEM console (UEM) console .

Whenever a device is non-compliant, Workspace ONE resets the password on the Google server preventing the user to log in using another device. Once the device is back to compliant status, the old password is reset back on the Google server and the user can gain access using the old password. By default, unmanaged devices are blocked.

Integrating without password retention

VMware AirWatch recommends using this configuration. Using this configuration, the Workspace ONE server communicates with Google directly and does not store the user password in database. You can manage and monitor enrolled devices through the Device Dashboard. Devices are deemed compliant or non-compliant based on the device compliance policies configured within the UEM console .

Since the SEG server is not involved, this approach provides a way to block non-compliant devices and ensure password safety. Once a device is detected as non-compliant, Workspace ONE removes the email profile from the device, thus barring the user from receiving emails. Once the device is back to compliant status, Workspace ONE generates a new password and sends it to Google and onto the device through the email profile.

Integrate SEG (V2) Proxy with Google

To begin integrating the SEG V2 with Google, you must configure Mobile Email Management (MEM) and install SEG V2. You must configure the settings required for SEG Proxy on the UEM console and then proceed with configuring the Security Settings at the Google Admin Console.

Configure SEG V2 using Unified Endpoint Management Console

1. Navigate to **Email > Email Settings** and select **Configure**.The **Add Email Configuration** wizard displays.
2. Select **Add**. The wizard displays the Platform tab.
   a. From Deployment Model, select **Proxy**.
   b. From Gateway Platform, select **V2**.
   c. From Email Type, select **Google** and then select **Next**. The Deployment tab opens and displays the basic settings.
3. From the Deployment tab, select the **Friendly Name** text box and enter a unique name.
4. Configure the External Settings.
   a. Select the **External URL and Port** text box and enter the external URL and the port number to which Workspace ONE sends policy updates. The supported format is **https://<external seg url>:<external port>**.
5. Configure the Internal Settings.
   a. Select the **Listener Port** text box and enter the web listener port for SEG. By default, the port number is 443. If SSL is enabled for SEG, the SSL certificate is bound to this port.
   b. (Optional) From Terminate SSL on SEG, select **Enable** to bind the SSL certificate to the port.
   c. Select the **Upload Locally** check box to upload the SSL certificate. The UEM console supports uploading the certificate locally for easy OTA installation. The certificate can also be provided during run-time.
   d. From SEG Server SSL Certificate, select **Upload** to add the certificate. The SSL certificate can be installed automatically, instead of providing it locally. This setting is useful for larger SEG deployments.
6. Configure the Email Server Settings.
   a. Select **Email Server URL and Port** text box and enter the Google server URL and the port number. The supported format is **https://<email server url>:<email server port>**. This is the Google URL to which SEG proxies email requests to Google. For example, https://m.google.com.
7. Configure Security Settings.
   a. From Ignore SSL Errors between SEG and email server, select **Enable** to ignore the Secure Socket Layer (SSL) certificate errors between the email server and SEG server.

b. From Ignore SSL Errors between SEG and Workspace ONE server, select **Enable** to ignore Secure Socket Layer (SSL) certificate errors between the Workspace ONE server and SEG server. Establish a strong SSL trust between Workspace ONE and SEG server using valid certificates.

c. From Allow email flow if no policies are present on SEG, select **Enable** to allow the email traffic if SEG is unable to load the device policies from the Workspace ONE API. By default, SEG blocks email requests if no policies are locally present.

8. (Optional) Configure Cluster Settings.

   a. From Enable Clustering, select **Enable** if you want to enable clustering of SEG servers. For more information, see **Configure the V2 Platform** section of the **VMware AirWatch Secure Email Gateway** guide.

9. Configure Google Apps Settings.

   a. Under the Google Apps Settings, the Automatic Password Provision is disabled by default. Select **Disabled** if you provide the Google password to your device users or if they are provided with their SSO password that is the same as the Google password. Disabling this setting is considered to be more stable because the Google password is managed within your organization.

   b. (Optional) If you do not provide native passwords to device users, or if they are only provided with SSO password and the primary directory is not Google, select **Enabled**. When enabled, UEM console provisions the Google for your users. Enter the following information for the UEM console to provision the Google password:

      i. Select the **Google Apps Domain** text box and enter the Google Apps domain address.

      ii. Select the **Google Apps Sub-Domain** text box and enter the Google Apps sub domain address.

      iii. Select the **Google Apps admin username** text box and enter the full URL as the Google Apps Admin user name.

      iv. From the **Service account certificate**, select Upload to upload to add the Service account certificate. Enter the certificate password when prompted. The certificate password is created when generating the client ID on the Google console.

      v. Select the **Directory service account email address** text box and enter the Directory service account email address that is generated while creating the Service Account Certificate.

      i. Select the **Application Name** text box and enter the project name.

10. Select **Next** and enter the required settings in the Profiles tab and select **Next**. For more information on the settings in the Profiles tab, see **Configure the V2 Platform** section of the **VMware AirWatch Secure Email Gateway** guide.

11. Select **Finish**.

Configure IP Restriction on Google Admin Console

Configure Google Sync to accept traffic only from SEG. This restricts the communication to SEG and ensures that the devices that attempt to bypass SEG are blocked.

1. Log into the Google Admin console.

2. Navigate to **Device Management** > **Advanced Settings** > **Google Sync** .

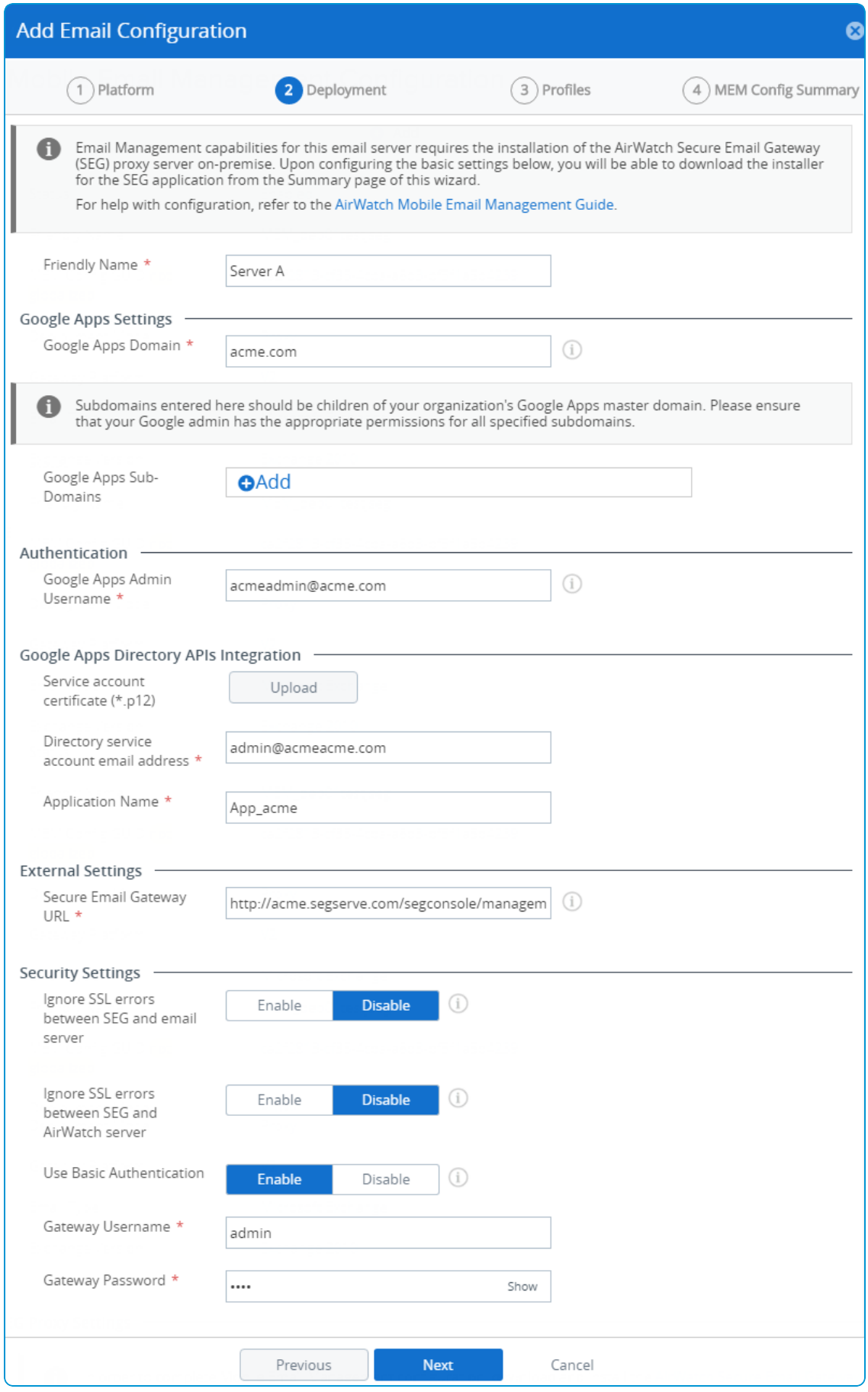
3. Select the **IP Whitelist** text box and enter the external SEG IPs that you want to whitelist.
4. Select **Save**.

Integrate Classic Secure Email Gateway (SEG) Proxy using Password Management

To begin integrating the SEG Proxy with your Google Sync, at first, you must configure the necessary settings required for SEG Proxy on the UEM console .

To configure SEG proxy:

1. Navigate to **Email > Email Settings** and select **Configure**.The **Add Email Configuration** wizard displays.
2. In the Platform tab of the wizard form:
   - Select **Proxy** as the Deployment model.
   - Select **Classic** as the Gateway Platform.
   - Select **Google Apps using Password Provisioning** as the Email Type.
   - Select **Next**.
3. In the Deployment tab of the wizard form, configure the basic settings. Select **Next**.



Settings	Description
Friendly Name	Enter a friendly name for the SEG deployment. This name gets displayed on the MEM dashboard for devices managed by SEG.
Google Apps Settings	
Google Apps Domain	Enter the Google Apps domain address.
Google Apps Sub-Domain	Enter the Google Apps sub domain address.
Authentication	
Google Apps admin username	Enter the Google Apps Admin username. Note that in the Google Apps Admin Username field, you should enter the full email address.
Google Apps Directory APIs Integration	
Service account certificate	Upload the Service account certificate. Enter the certificate password when prompted. The certificate password is created while generating the client ID on the Google console.
Directory service account email address	Enter the Directory service account email address that was generated while creating the Service Account Certificate.
Application Name	Enter the project name that you had earlier created.
Secure Email Gateway URL	Enter the proxy server address to which the API can connect.
Ignore SSL errors between SEG and email server	Select **Enable** to ignore Secure Socket Layer (SSL) certificate errors between email server and the SEG server.
Ignore SSL errors between SEG and Workspace ONE server	Select **Enable** to ignore Secure Socket Layer (SSL) certificate errors between Workspace ONE component and the SEG server.
Use Basic Authentication	Select **Enable** to allow login to the proxy server with basic user credentials.
Gateway Username and Password	Enter the username and password to access the SEG server.

4. In the Profiles tab of the wizard form, create a new profile or associate an existing profile. Select **Next**.

   All Google models require an EAS profile. For new installs, associating an EAS profile is mandatory. For the upgrades, the admin has to manually associate an EAS profile to the MEM configuration after completing the upgrade process.

5. The MEM Config Summary tab of the wizard provides a quick overview of the basic configuration you have just created for the SEG deployment. Select **Finish** to save the settings.

Configure Advance Settings

After you have configured the SEG Proxy, you can configure the advanced settings for your Google Sync deployment.

To configure the advanced settings:

1. Navigate to **Email** > **Settings** page and then select the  icon next to the required Google Sync deployment.
    a. By default, the **Use Recommended Settings** check box is enabled to capture all SEG traffic information from devices. If not enabled, you can specify what information and how frequently the SEG should log for devices.
    b. Select the **Enable Real-time Compliance Sync** option to enable the UEM console to remotely provision compliance policies to the SEG Proxy server.
2. **Save** the settings.

You can now configure Exchange ActiveSync profiles for each end user.

A Note on Password Management

If you choose to set up Email Management with Workspace ONE for Gmail, the passwords for Workspace ONE users with an email address domain matching that of the configured Google domains change. This change is regardless of any settings that you choose (through SEG or without SEG, or with Password Retention or Password Purging). Profile assignment through smart groups does not determine the users for whom the passwords are managed. If you do not prefer password management, then configure the 'Direct Integration with Directory APIs' deployment type.

The Google Apps Directory Sync (GADS) or the Google Apps Password Sync (GAPS) does not work with the password management options. Since GADS or GAPS performs a one-way sync of syncing data from the local LDAP server to Gmail, any change made to the password on Gmail is overwritten with the data from the LDAP server. Workspace ONE recommends the direct Integration with the Directory APIs deployment type in this type of configuration.

Integrate Direct Model using Directory APIs

Using Google's Directory APIs, Workspace ONE manages email access on mobile devices without any password management. Before you configure the deployment type on the UEM console , there are certain options that you must also enable on the Google Admin console if using the Directory APIs model.

Enable Device Activation

Apart from configuring the deployment type on the UEM console , you need to first enable the **Device Activation** option on the Google Admin console. Enabling this option blocks any unmanaged devices from accessing email.

> **Note**: Workspace ONE recommends you not to enable Device Activation setting until you are ready to go live with the email integration. Enabling this before the integration will block new devices and cause related problems.

To enable Device Activation, do the following:

1. On the Google Admin console, navigate to **Device management** > **Mobile** > **Setup**.
2. On the Setup page, select **Device Activation**.
3. Select an organization from the left panel and then select the **Require admin approval for device activation** check box.
4. (Optional) Enter an email address to receive notifications when users enroll their devices. You can also enter a group email address that includes all the administrators who can activate the devices. Select **Save**.

Workspace ONE checks with Google for a device account during enrollment when the profile is pushed onto the device:

- If the enrolled device has an account, Google sends a positive response to Workspace ONE. Workspace ONE then sends an approve command to Google to allow email access.
- If your device does not have a Google account setup before enrolling in Workspace ONE, then Google sends a negative response and Workspace ONE updates the Email Dashboard as 'Update Failed' for that device. After the device enrolls, the profile is already installed on the device, and any attempt to connect, creates a device record in Google. When the Google scheduler runs at a default interval of five minutes, the device is identified and allowed for email access. The Email Dashboard is then updated with the 'Scheduled Sync Update'.
- If the device fails to be identified by the scheduler after two days, then the end user must login to SSP and select **Sync Email** for the device to receive email access.

Configure Deployment on UEM Console

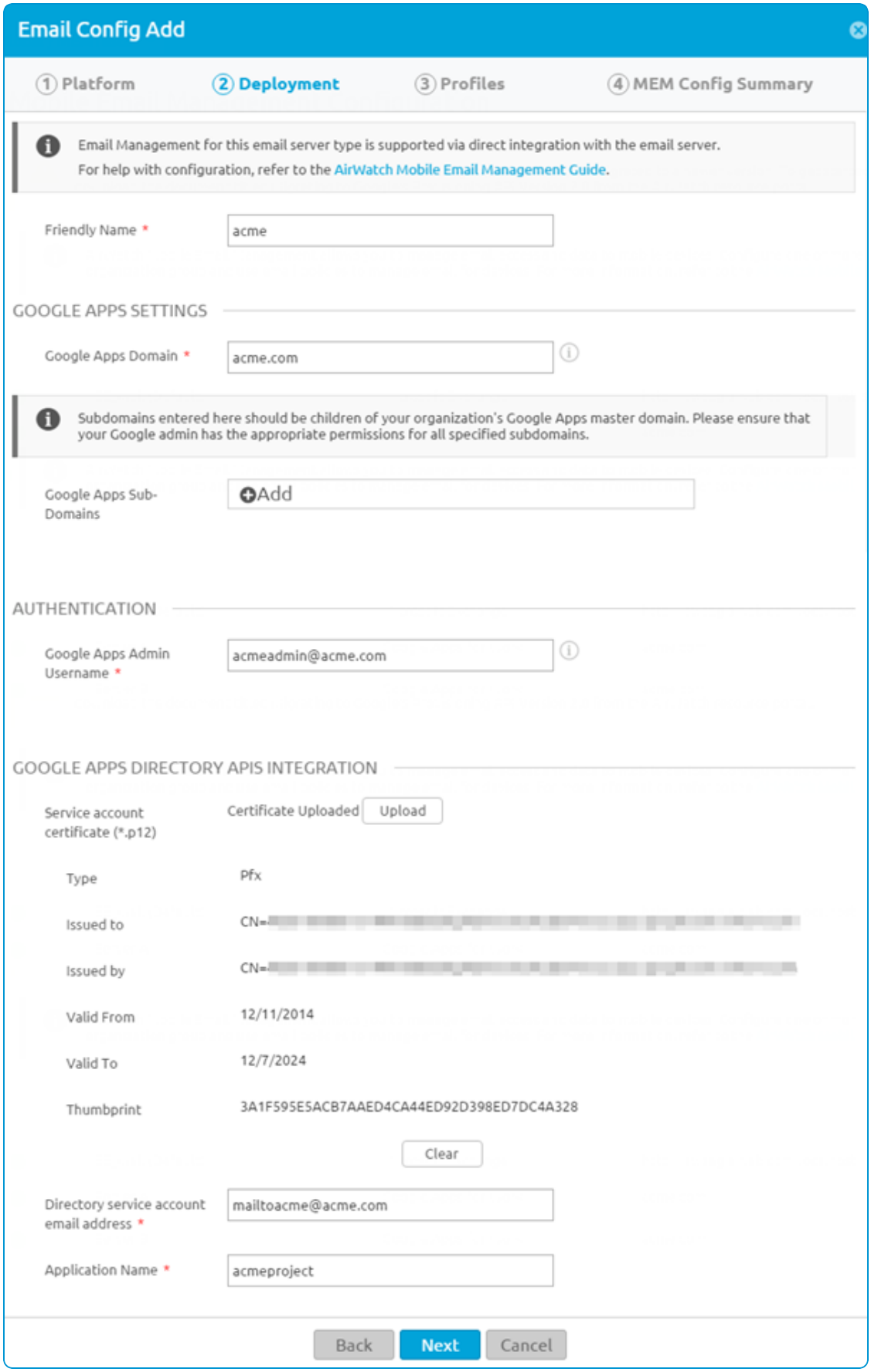
After you have enabled the options on the Google Admin console, configure the DIrect APIs deployment type on the UEM console .

To configure the deployment:

1. Navigate to **Email > Email Settings** and select **Configure**.The Email Config Add wizard displays.

2. In the Platform wizard form:
   a. Select **Direct** as the Deployment Model.
   b. Select **Google Apps with Direct API** as the Email Type.
   c. Select **Next**.
3. In the Deployment wizard form:

Setting	Description
Friendly Name	Enter a friendly name for the Gmail deployment.
Google Apps Settings	
Google Apps Domain	Enter the registered Google Apps Domain address.
Google Apps Sub-Domain	Enter the Google Apps sub domain address.
Authentication	
Google Apps Admin Username	Enter the full email address in the Google Apps Admin username field.
Google Apps Directory APIs Integration	
Service account certificate (*.p12)	Upload the Service account certificate. Enter the certificate password when prompted. The certificate password is created while generating the Service Account client ID on the Google console.
Directory service account email address	Enter the Service Account email address.
Application Name	Enter the project name that you created earlier.



Integrate Direct Model using Password Management

While configuring your Gmail deployment using the Password Management approach, you can choose if you want to retain or not retain the Google password in the Workspace ONE database.

The non-compliant devices are blocked depending on whether you chose to retain or not retain the password. The devices are blocked either by resetting the password on the Google server or by removing the email profile from the device.

Note: Irrespective of the type of email client, for password provisioning to occur, all the Gmail models require an EAS profile. For new installs, associating an EAS profile is mandatory. For the upgrades, the admin has to manually associate an EAS profile to the MEM configuration after completing the upgrade process.

To configure deployment on the UEM console :

1. From the UEM console main menu, navigate to **Email > Email Settings**, and then select **Configure**.
2. In the Platform wizard form:
   - Select **Direct** as the Deployment Model.
   - Select **Google Apps using Password Provisioning** as the Email Type.
   - Select **With Password Retention** or **Without Password Retention** as the Google Deployment Type. Select **Next**.
3. In the Deployment wizard form

Setting	Description
Friendly Name	Enter a friendly name for the Gmail deployment.
Google Apps Settings	
Google Apps Domain	Enter the registered Google Apps domain address.
Google Apps Sub-Domain	Enter the Google Apps sub domain address, if applicable.
Authentication	
Google Apps Admin Username	Enter the full email address in the Google Apps Admin Username field.
Google Apps Directory APIs Integration	
Service account certificate (*.p12)	Upload the Service account certificate. Enter the certificate password when prompted. The certificate password is created while generating the Service Account client ID on the Google console.

Setting	Description
Directory service account email address	Enter the Service Account email address that was generated while creating the Service Account Certificate.
Application Name	Enter the project name that you had created earlier.

4. Select **Next**.
5. In the Profiles wizard form, create a new profile or associate an existing profile. Select **Next**.
6. The MEM Config Summary form provides a quick overview of the basic configuration you have just created for the Gmail deployment. **Save** the settings.

Configure Advanced Settings

After configuring your Gmail deployment, configure the advanced settings for the deployment. These settings vary depending on whether you have chosen to retain your password or not.

With Password Retention

If you have chosen to retain the password, then you can configure the settings to set up the preferred password length.

Note: Workspace ONE does not provision passwords for newly enrolled devices or make any change to the password for the devices that change status while the email compliance policies are disabled.

To configure the advanced setting for this configuration:

1. Navigate to **Email** > **Settings** page and then select the  icon.
2. By default, the **Use Recommended Settings** check box is enabled. Disable this check box to enter the preferred length of the password in the **Google Random Password Length** field. Minimum accepted character is 8 and maximum is 100.
3. Select **Save**.

Without Password Retention

If you have chosen not to retain the password in the Workspace ONE database, then disable the settings which by default encrypts and stores the Google password in the Workspace ONE database.

The Email Compliance policies are not applicable for this type of integration. By default, unmanaged devices are blocked.

Note: Workspace ONE provisions passwords to devices during enrollment regardless of the MEM settings. The MDM compliance policies determines this approach.

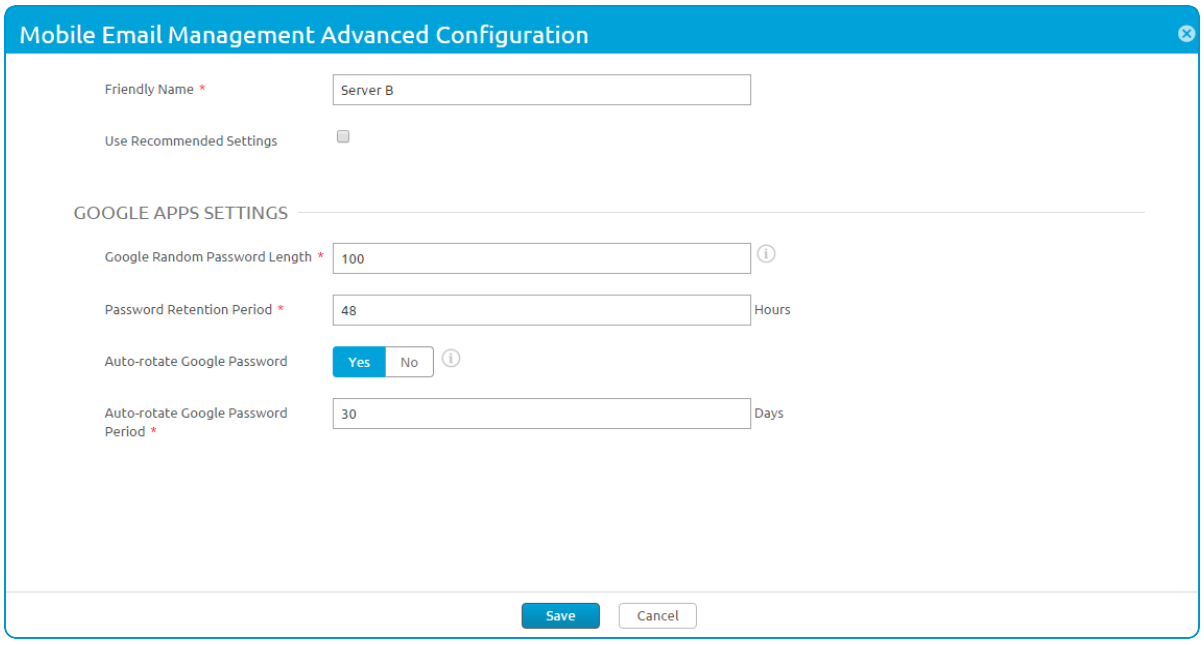
To configure the advanced setting for this configuration:

1. Navigate to **Email** > **Settings** page and then select the icon.
2. Disable the **Use Recommended Settings** check box to configure the Google Apps Settings options. By default, this option is enabled to encrypt and to store the Google password in the Workspace ONE database.

Note that if a user has two devices enrolled and when one of the devices unenrolls, then the Google password resets and new generated password is pushed to the device that is enrolled.

Once you disable the **Use Recommended Settings** check box, you can configure the following options:

Setting	Description
Google Random Password Length	Enter the preferred random password length. Minimum accepted character is 8 and maximum is 100
Password Retention Period	Enter the number of hours the password should be retained temporarily for management purposes. The retention ensures that all the enrolled devices belonging to a user receives the password. The default value is 48. The minimum accepted character is 1 and maximum is 100.
Auto-rotate Google Password	Select this check box to reset the password once within the specific period. The Scheduler runs to check if any user's password need to be reset within the specified period. The minimum accepted character is 1 and maximum is 90.
Auto-rotate Google Password Period	Enter the specific period to reset the Google password. The default period is 30 days.



3. Select **Save**.

Note: Irrespective of the type of email client, all the Google models require an EAS profile. For new installs, associating an EAS profile is mandatory. For the upgrades, the admin has to manually associate an EAS profile to the MEM configuration after completing the upgrade process.

Chapter 3:
Google Sync Implementation

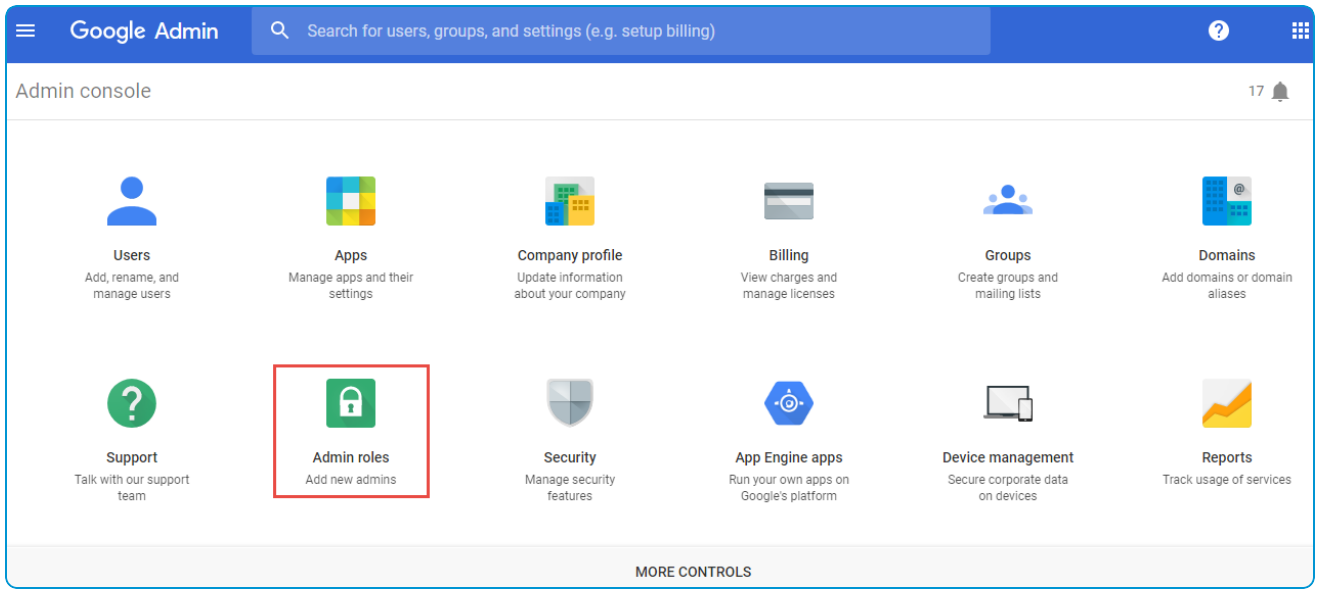
Create an Admin Role for Gmail Integration

To manage Google users, Workspace ONE requires a Gmail administrator account with specific privileges. Either a super user account or an administrator account with specific privileges can be used.

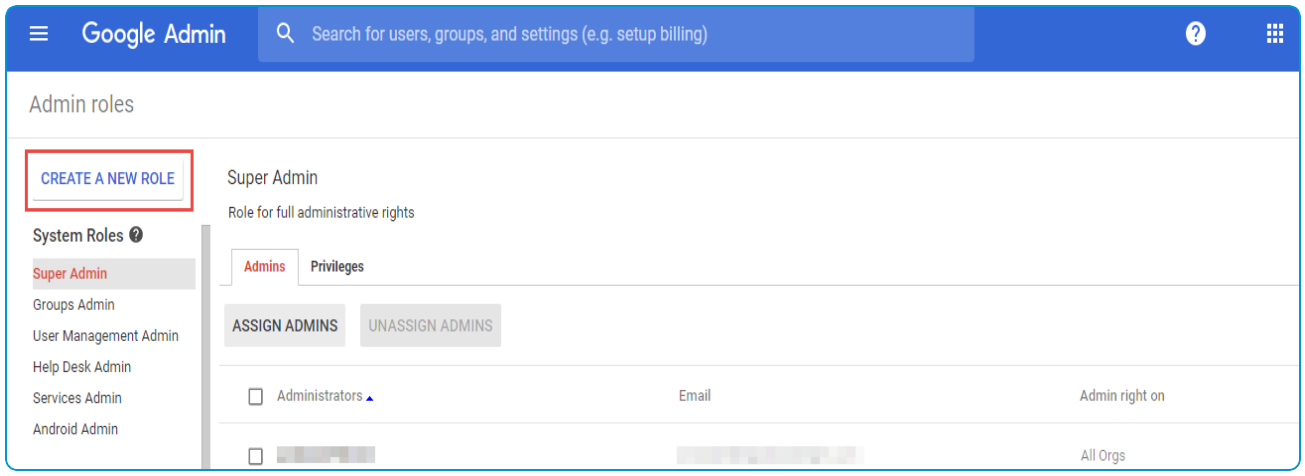
To create a custom set of admin permissions:

Note: 1. If you choose to use a super admin account, skip to step 5.
2. Use a service account if you do not want Workspace ONE to change or revoke the admin password from the Google console.

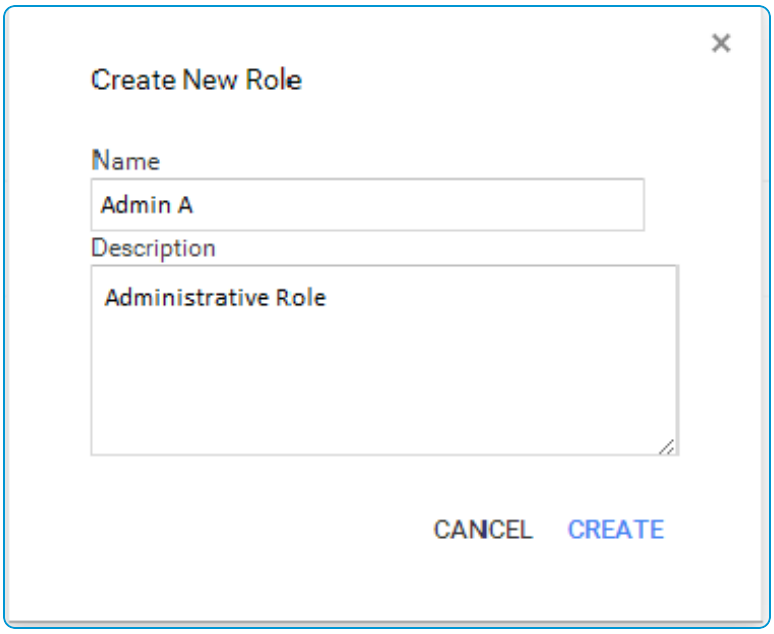
1. Log into your Google dashboard and navigate to **Admin Roles**.



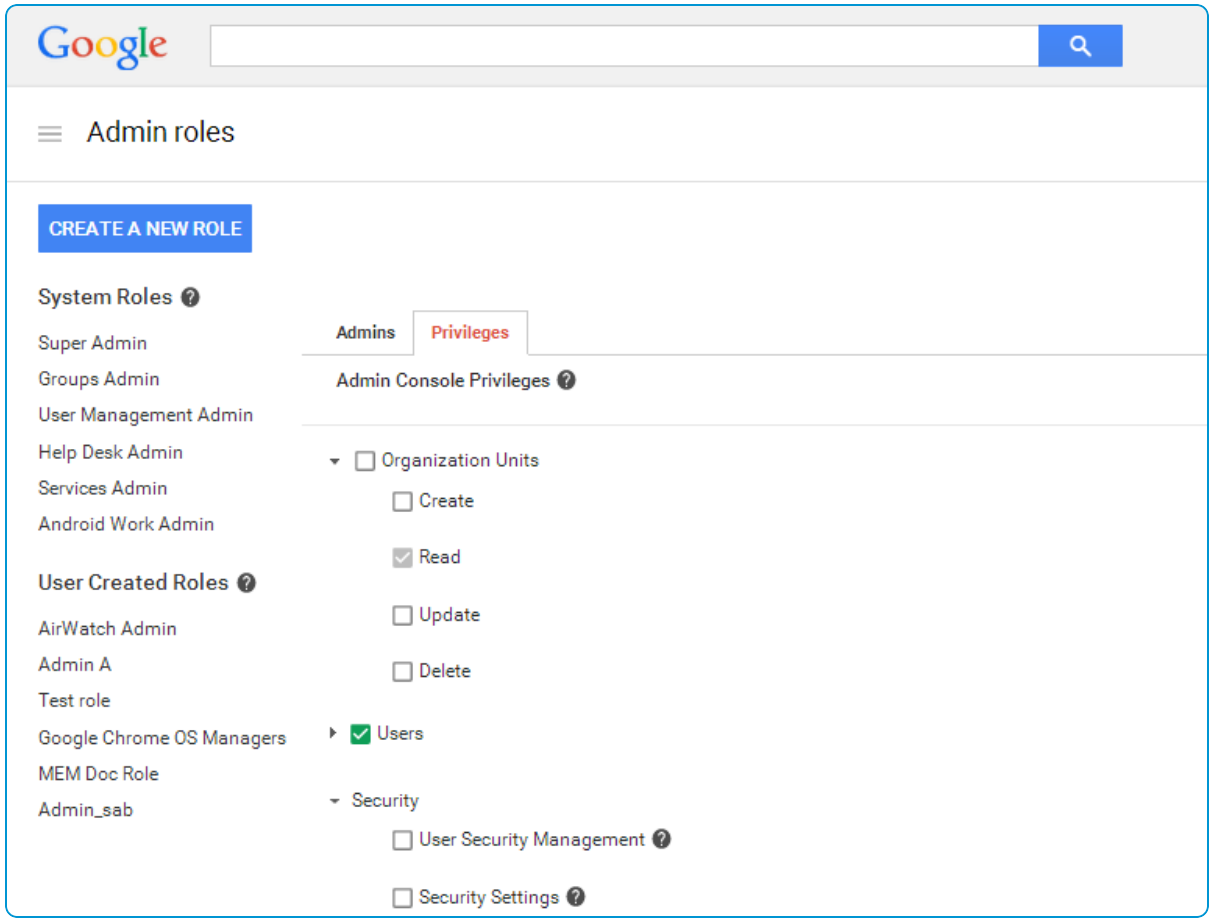
2. Select **Create A NEW ROLE**. The Create New Role form displays.



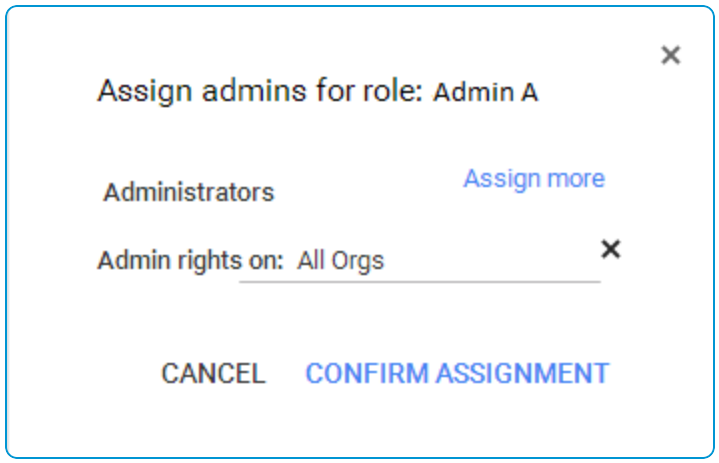
3. Enter the **Name** and **Description** for the role, and then select **Create**.



4. On the **Privileges** tab, select the privileges for the new role. The required privileges include:
   - Admin console Privileges
     - Organization Units - Read
     - Users - Read
     - Update - Rename users, Move users, Reset Password, Force Password, Add or Remove Aliases, Suspend Users
   - Admin API Privileges
     - Organization Units - Read
     - Users - Read
     - Update - Rename users, Move users, Reset Password, Force Password, Add/Remove Aliases, Suspend Users



5. Select **Save**.
6. Select the **Admins** tab and then **Assign admins** to assign the created role to an administrator and then select **Confirm Assignment**.

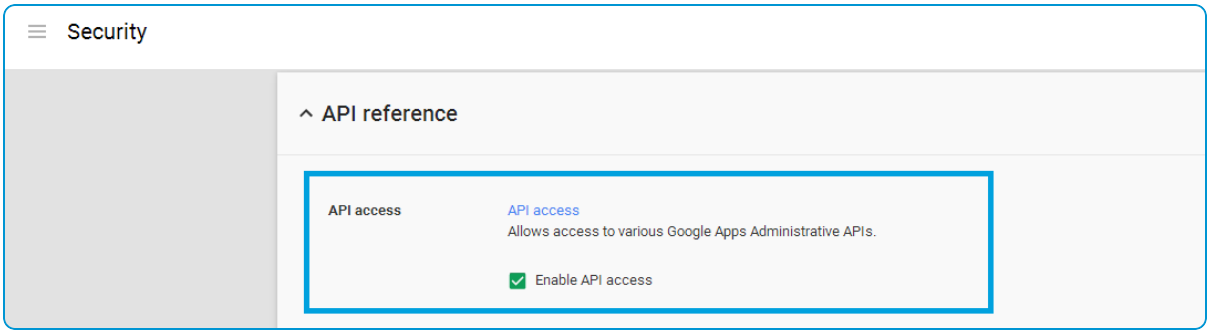


Enable the Google API

In order for Workspace ONE to provision users' passcodes, the Google API must be enabled using the Google control panel. This is optional for Direct Integration with Directory API type of configuration.

To access the control panel:

1. Sign in to the Google Admin console.
2. Once logged in, navigate to **Security** > **API Reference**. Select the **Enable API access** check box and select **Save**.

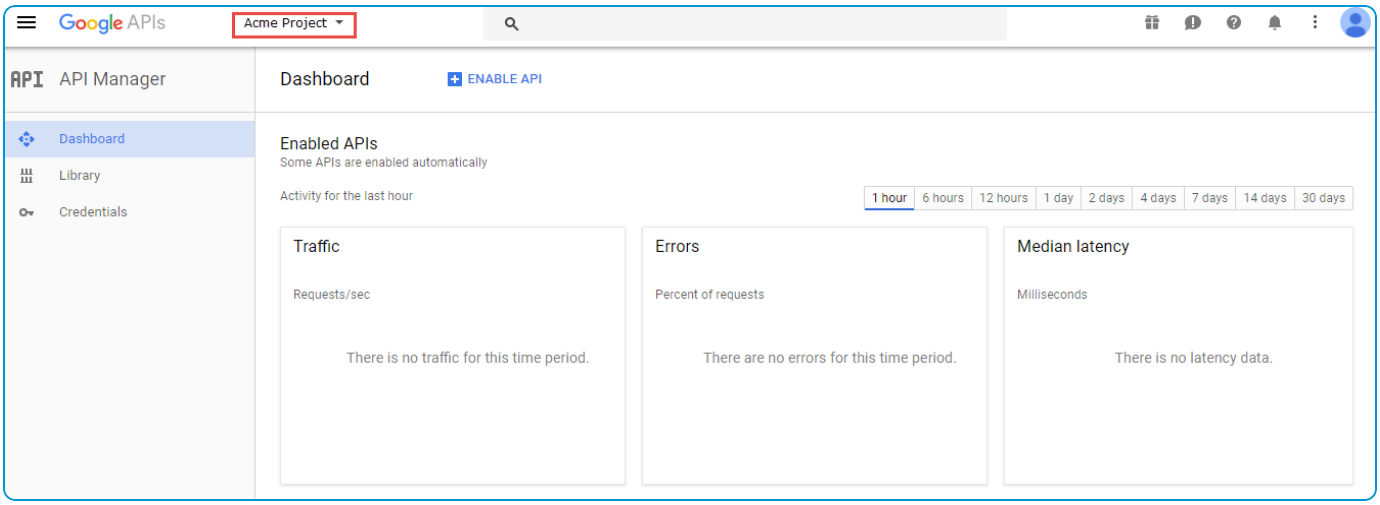


Create Service Account Certificate

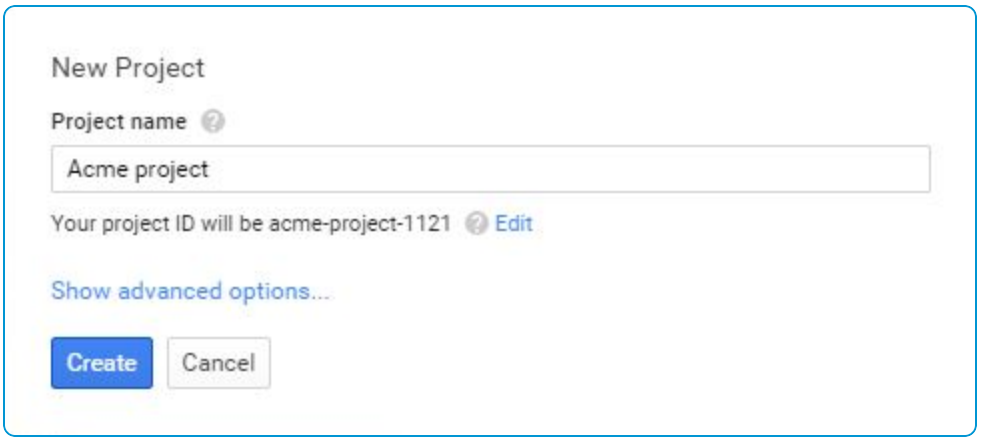
The Service Account Certificate is required for using the Google APIs. You can create the certificate from the Google Admin console and then upload it on the UEM console while configuring the email integration.

On the Google Developer Console

1. Navigate to **https://console.developers.google.com** and login using your super admin credentials. You are on the API Dashboard page.
2. Select the projects list drop-down menu and then select '**+**' to create a project.

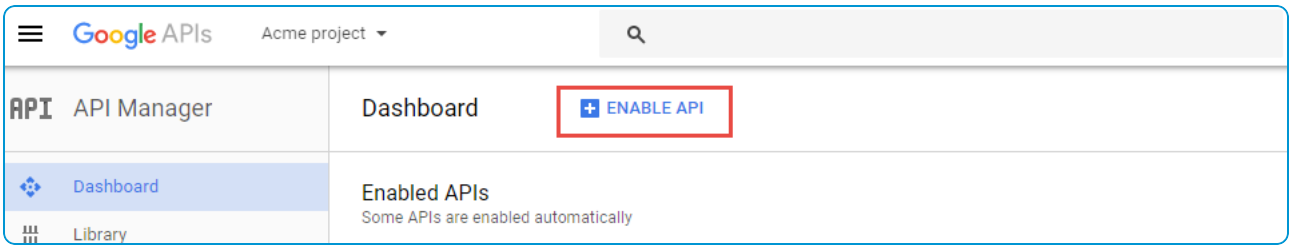


3. Enter the **Project name** and select **Create**. The project ID is generated.

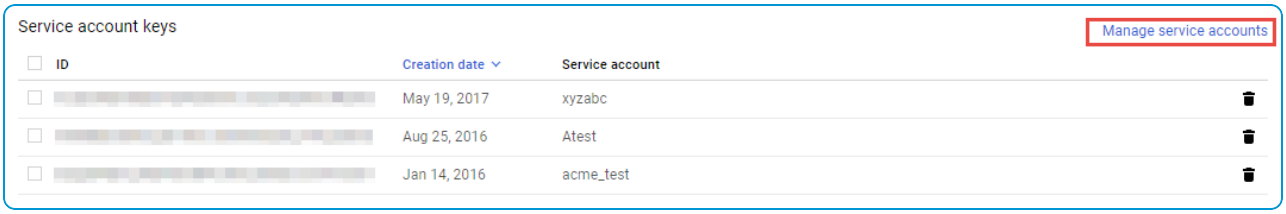


The project ID cannot be changed once the project is created. In case you wish to change the project ID, select **Edit** before you create the project.

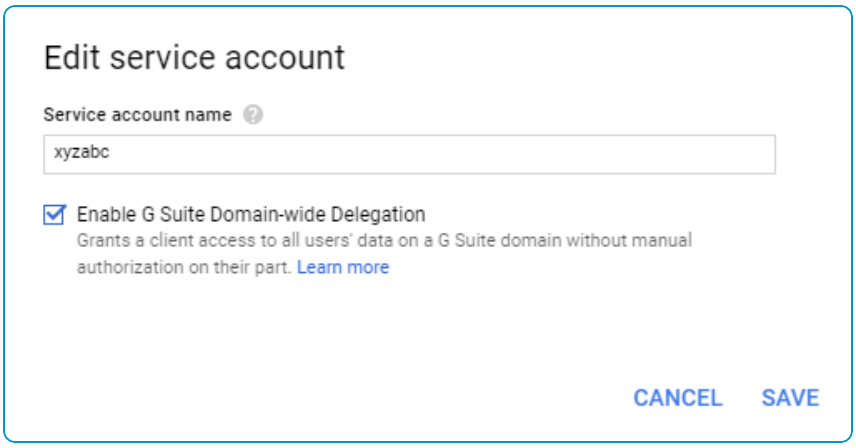
4. Select **Enable API** .



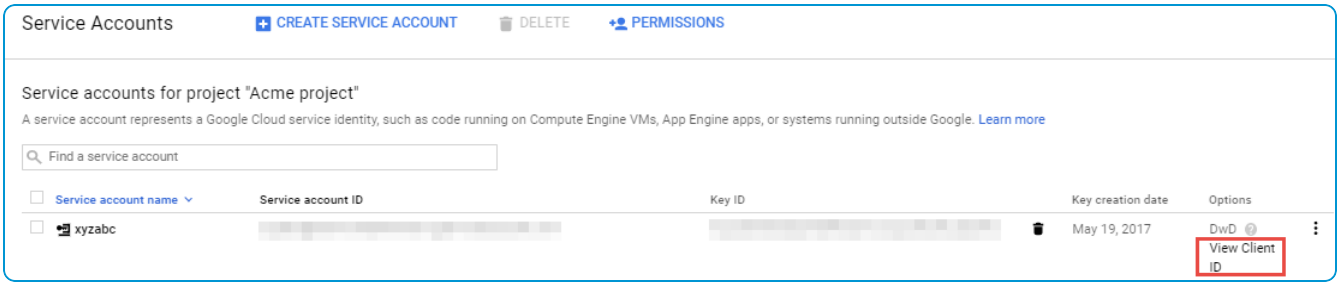
5. Select **Library** from the API Manager sidebar. The list of Google APIs appear.
6. Select **Admin SDK** available under G Suite APIs and then select **ENABLE**.
7. Select **Credentials** from the API Manager sidebar. The credentials page appears.
   - Select **Create credentials** and then select **Service account key** option.
   - Select **New service account** from the Service account drop-down menu. Provide the **Service account name**, **Service account ID** and the **Role** for the service account email address.
   - Select **P12** as the Key type.
   - Select **Create**. The new service account has been created. Save the .p12 certificate with private key to your machine. Please make a note of the generated password for the private key.
8. Select **Manage service accounts** on the credentials page. The **Service accounts** page is displayed.



9. Select the service account you created and then select **Edit** from the corresponding menu (⋮). The **Edit service account** screen appears.
10. Select the **Enable G Suite Domain-wide Delegation** check box. Select **SAVE**.



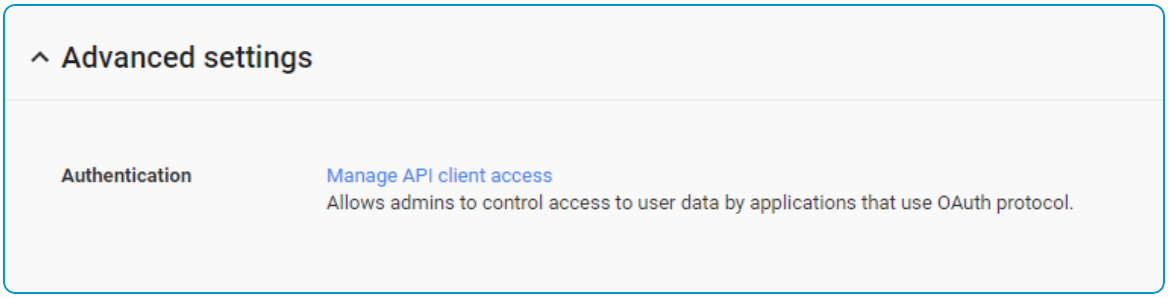
Now, the Client ID is generated and **View Client ID** appears under **Options** for your service account in the Service accounts page. Currently, there is no way to delete a Client ID once it has been generated. The only alternative is to delete and re-create the whole project.



11. Select **View Client ID** to view the generated Client ID and the service account email address.

On the Google Admin Console

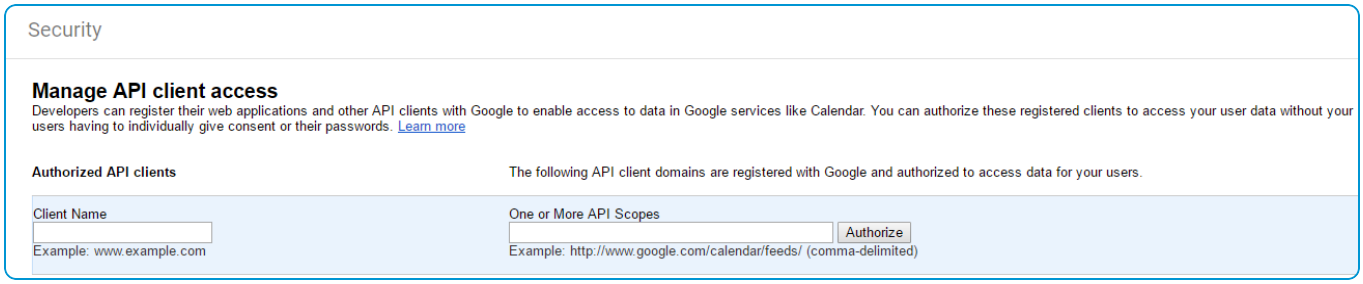
1. Navigate to **https://admin.google.com** and login with your super admin credentials.
2. Select **Security** > **Advanced Settings**.
3. Select **Manage API client Access** hyperlink from the Advanced settings pop-up menu.



4. Enter the previously generated Client ID (as mentioned in step 8 of **On the Google Developer console** section) in the **Client Name** field.

5. Next, you must authorize your client ID for the required API scopes. Enter the API scope, listed below, that are required by the application in the **One or More API Scopes** field and then select **Authorize**.

   https://www.googleapis.com/auth/admin.directory.user,https://www.googleapis.com/auth/admin.directory.user.readonly,https://www.googleapis.com/auth/admin.directory.device.mobile.readonly,https://www.googleapis.com /auth/admin.directory.device.mobile.action



Note: The above mentioned **API Scopes** must be added as a comma delimited string containing no spaces.

Chapter 4:
Email Management through Google Sync Integration

Device Discovery

After the Gmail integration setup is complete, you can manage the connected device email traffic, set email policies, and take appropriate actions on the devices from the UEM console . The features available here depends on the type of deployment that you choose.

Before you can begin managing the device from the Email Dashboard, the configured MEM should discover the devices enrolled to the organization group. On getting integrated with a MEM deployment, devices are discovered either through:

With EAS profile

Ensure all the managed devices receive the EAS profile.

Without EAS profile

Profiles are a must for this type of deployment except while integrating with Directory APIs. Unless the devices are provisioned with the profiles, the configured Gmail deployment cannot identify and subsequently manage the device.

Device Management with SEG Proxy Integration

Manage your devices with the email compliance policies applicable for SEG Proxy configuration. These compliance policies help you prevent non-compliant, unmanaged, or blocked devices from accessing corporate emails.

Apart from compliance policies, you can also use the Email dashboard and the list view page to effectively manage your corporate devices. You can view the status of the devices using the Email Dashboard and the user-specific or device-specific information using the List View page.

Note: Workspace ONE will not provision passwords for new users, but SEG will continue to proxy the requests for devices that were previously enrolled successfully to Google.

Compliance Policies

The compliance policies mentioned in this section can be activated from the **Email** > **Compliance Policies** page.

General Email Policies

- **Sync Settings** – Prevent the device from syncing with specific EAS folders. Note that Workspace ONE prevents devices from syncing with the selected folders irrespective of other compliance policies. For the policy to take effect, you must republish the EAS profile to the devices (this forces devices to resync with the email server).
- **Managed Device** – Restrict email access only to managed devices.
- **Mail Client** – Restrict email access to a set of mail clients.
- **User** – Restrict email access to a set of users.
- **EAS Device Type** – Allow or block devices based on the EAS Device Type attribute reported by the end-user device.

Managed Device Policies

- **Inactivity** – Allows you to prevent inactive, managed devices from accessing email. You can specify the number of days a device shows up as inactive (that is, does not check in to Workspace ONE), before email access is cut off.

- **Device Compromised** – Allows you to prevent compromised devices from accessing email. Note that this policy does not block email access for devices that have not reported compromised status to Workspace ONE.
- **Encryption** – Allows you to prevent email access for unencrypted devices. Note that this policy is applicable only to devices that have reported data protection status to Workspace ONE.
- **Model** – Allows you to restrict email access based on the Platform and Model of the device.
- **Operating System** – Allows you to restrict email access to a set of operating systems for specific platforms.
- **Require ActiveSync Profile** - Allows you to restrict email access to devices whose email is managed through an Exchange ActiveSync profile.

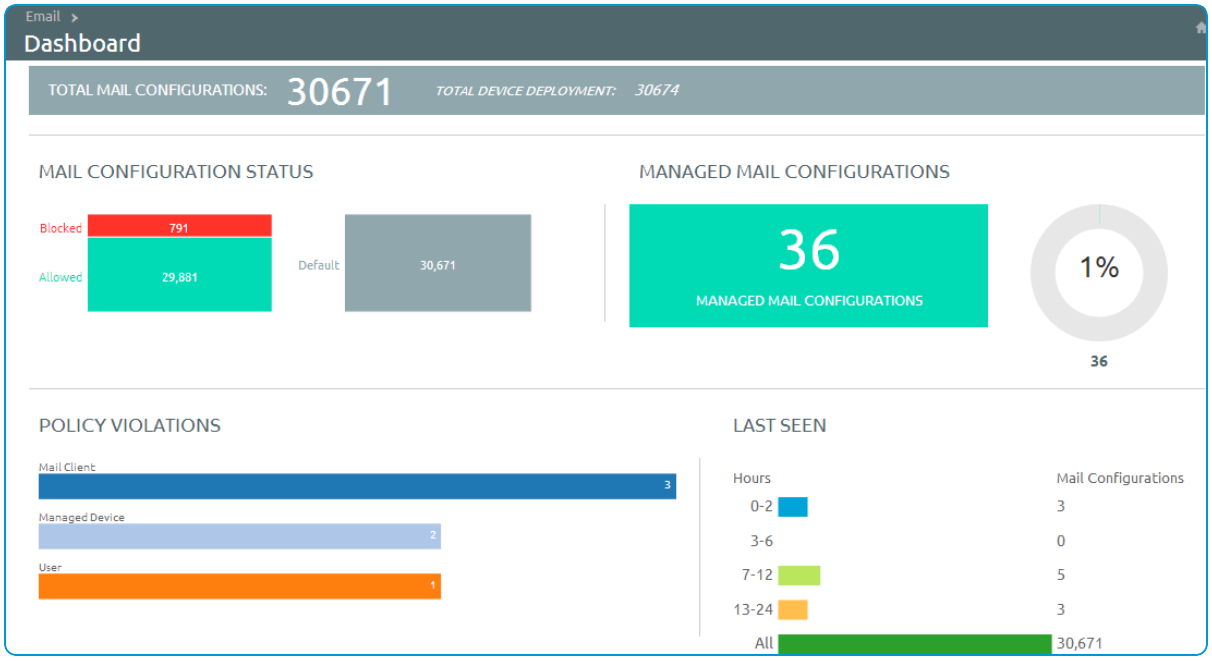
Email Security Policies

- **Email Security Classification** – Define the action for the SEG to take on emails with and without security tags. You may either allow or block the emails on AirWatch Inbox or other email clients.
- **Attachments (managed devices)** – Encrypt email attachments of the selected file types. These attachments are secured on the device and are only available for viewing on the VMware Content Locker. Currently, this feature is only available on managed iOS, Android, and Windows Phone devices with the VMware Content Locker application. For other managed devices, you can choose to either allow encrypted attachments, block attachments, or allow unencrypted attachments.
- **Attachments (unmanaged devices)** – Allow encrypted attachments, block attachments, or allow unencrypted attachments for unmanaged devices.
- **Hyperlink** – Allow device users to open hyperlinks contained within an email directly with VMware Browser present on the device. The Secure Email Gateway dynamically modifies the hyperlink to open in VMware Browser. You may choose one of the Modification Type:
  - All - Choose to open all the hyperlinks with VMware Browser.
  - Include - Choose if you want the device users to open only the hyperlinks through the VMware Browser. Mention the included domains in the **Only modify hyperlinks for these domains** field. You can bulk upload the domain names from a CSV file as well.
  - Exclude - Choose if you do not want the device users to open the mentioned domains through the VMware Browser. Mention the excluded domains in the **Modify all hyperlinks except for these domains** field. You can bulk upload the domain names from a CSV file as well.

Email Dashboard

Gain visibility into the email traffic and monitor the devices through the Workspace ONE **Email Dashboard**. This dashboard gives you a real-time summary of the status of the devices connected to the email traffic. You can access the Dashboard from **Email > Dashboard**. The email dashboard enables you to:

- Whitelist or blacklist a device to allow or deny access of email
- View the devices which are managed, unmanaged, compliant, non- compliant, blocked, or allowed
- View the device details such as OS, Model, Platform, Phone Number, IMEI, IP address



From the Dashboard, you can also use the available Graphs to filter your search. For example, if you want to view all the managed devices of that organization group, select the Managed Devices graph. This displays the results in the List View screen.

List View

View all the real-time updates of your end user devices that you are managing with Workspace ONE MEM. You can access the **List View** from **Email** > **List View**. You can view the device or user-specific information by switching between the two tabs: **Device** and **User**. You can change the **Layout** to either view the summary or the detailed list of the information based on your requirement.

The List View screen provides detailed information that includes:

- **Last Request** - In PowerShell integration, this column displays the last state change of the device either from Workspace ONE or from Exchange. In SEG integration, this column shows the last time a device synced mail.
- **User** - The user account name.
- **Friendly Name** - The friendly name of the device.
- **MEM Config** - The configured MEM deployment that is managing the device.
- **Email Address** - The email address of the user account.
- **Identifier** - The unique alpha-numeric identification code associated with the device.
- **Mail Client** - The email client syncing the emails on the device.
- **Last Command** - The command triggers the last state change of the device and populates the **Last Request** column.
- **Last Gateway Server** -The server to which the device connected.
- **Status** - The real time status of the device and whether email is blocked or allowed on it as per the defined policy.
- **Reason** - The reason code for allowing or blocking email on a device.

Note: The reason code displays 'Global' when access state is defined by the default organization allow/block/quarantine policy. The reason code is 'Individual' when device ID is explicitly set for a given mailbox by Exchange admin or Workspace ONE. The reason code is 'Policy' when device is blocked by any EAS policy.

- **Platform, Model, OS, IMEI, EAS Device Type, IP Address** - The device information displays in these fields.
- **Mailbox Identity** - The location of the user mailbox in the Active Directory.

Filters for Quick Search

The **Filter** option is available on the List View page. Using this filter, you can narrow your device search based on:

- **Last Seen** - All, less than 24 hours, 12 hours, 6 hours, 2 hours.
- **Managed** - All, Managed, Unmanaged.
- **Allowed** - All, Allowed, Blocked.
- **Policy Override**: All, Blacklisted, Whitelisted, Default.
- **Policy Violation** - Compromised, Device Inactive, Not data Protected/Enrolled/MDM Compliant, Unapproved EAS Device Type/Email Account/Mail Client/Model/OS.
- **MEM Config** - Filter devices based on the configured MEM deployments.

Performing Actions

The **Override**, **Actions** and **Administration** drop-down menu provides a single location to perform multiple actions on the device.

Note: Please note that these actions once performed cannot be undone.

Override

Select the check box corresponding to a device to perform actions on it.

- **Whitelist** - Allows a device to receive emails.
- **Blacklist** - Blocks a device from receiving emails.
- **Default** - Allows or blocks a device based on whether the device is compliant or non-compliant.

Actions

- **Run Compliance** - Triggers the compliance engine to run for the selected MEM configuration. For any device that has a state change (that is, compliant to non-compliant or conversely), Workspace ONE sends out an Allow/Block command accordingly.
- **Test Mode** - Tests email policies without applying them on devices.

Administration

- **Dx Mode On** - Runs the diagnostic for the selected user mailbox providing you the history of the device activity. After enabling this option, Workspace ONE starts recording the activity of the device. This feature is available for SEG only.
- **Dx Mode Off** - Turns off the diagnostic for the selected user mailbox. This feature is available for SEG only.
- **Update Encryption Key** - Resets the encryption and the resyncs the emails for the selected devices. This feature is available for SEG only.
- **Delete Unmanaged Devices** - Deletes the selected unmanaged device record from the dashboard. Please note that this record may reappear after the next sync.
- **Migrate Devices** - Migrates selected device to other chosen MEM configurations by deleting the installed EAS profile and pushing the EAS profile of the chosen configuration on the device.

Device Management with Directory APIs Integration

Manage your devices using the email compliance policies that are applicable for Directory APIs configuration. Along with the compliance policies, the Email Dashboard and the List View page also lets you effectively manage your corporate devices.

While the Email Dashboard displays the device status, the List View page displays user and device-specific information either in a summarized or detailed manner.

General Email Policies

- **Managed device** – Allow/block unenrolled devices from accessing email.

Managed Device Polices

Note: Workspace ONE does not set access against Google for any devices that enroll while compliance is disabled, nor change the access state for any previously enrolled devices that change compliance status.

The policies mentioned here can be activated from **Email** > **Compliance Policies** page.

- **Inactivity** – Allows you to prevent inactive, managed devices from accessing email. You can specify the number of days a device shows up as inactive (that is, does not check-in to Workspace ONE), before email access is cut off.
- **Device Compromised** – Allows you to prevent compromised devices from accessing email. Note that this policy does not block email access for devices that have not reported compromised status to Workspace ONE.

Note: Note that unenrolled devices are blocked by default.

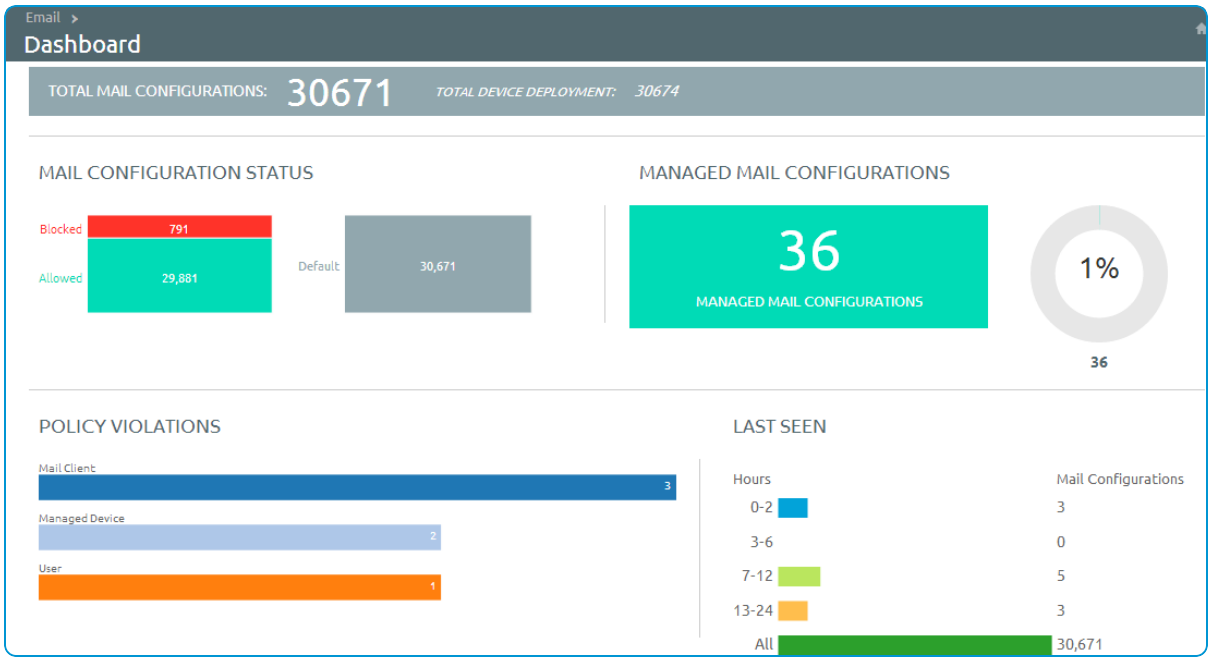
- **Encryption** – Allows you to prevent email access for unencrypted devices. Note that this policy is applicable only to devices that have reported data protection status to Workspace ONE.
- **Model** – Allows you to restrict email access based on the Platform and Model of the device.

- **Operating System** – Allows you to restrict email access to a set of operating systems for specific platforms.
- **Require ActiveSync Profile** – Allows you to restrict email access to devices whose email is managed through an Exchange ActiveSync profile.

Email Dashboard

Gain visibility into the email traffic and monitor the devices through the Workspace ONE **Email Dashboard**. This dashboard gives you a real-time summary of the status of the devices connected to the email traffic. You can access the Dashboard from **Email > Dashboard**. The email dashboard enables you to:

- Whitelist or blacklist a device to allow or deny access of email
- View the devices which are managed, unmanaged, compliant, non- compliant, blocked, or allowed
- View the device details such as OS, Model, Platform, Phone Number, IMEI, IP address



From the Dashboard, you can also use the available Graphs to filter your search. For example, if you want to view all the managed devices of that organization group, select the Managed Devices graph. This displays the results in the List View screen.

List View

View all the real-time updates of your end user devices that you are managing with Workspace ONE MEM. You can access the **List View** from **Email** > **List View**. You can view the device or user-specific information by switching between the two tabs: **Device** and **User**. You can change the **Layout** to either view the summary or the detailed list of the information based on your requirement.

The List View screen provides detailed information that includes:

- **Last Request** – The last state change of the device. In SEG integration, this column shows the last time a device synced mail.
- **User** – The user account name.

- **Friendly Name** – The friendly name of the device.
- **MEM Config** – The configured MEM deployment that is managing the device.
- **Email Address** – The email address of the user account.
- **Identifier** – The unique alpha-numeric identification code associated with the device.
- **Mail Client** – The email client syncing the emails on the device.
- **Last Command** – The command triggers the last state change of the device and populates the **Last Request** column.
- **Last Gateway Server** – The gateway server to which the device connected.
- **Status** – The real time status of the device and whether email is blocked or allowed on it as per the defined policy.
- **Reason** – The reason code for allowing or blocking email on a device.

Note: The reason code displays 'Global' when access state is defined by the default organization allow/block/quarantine policy. The reason code is 'Individual' when device ID is explicitly set for a given mailbox by Exchange admin or Workspace ONE. The reason code is 'Policy' when device is blocked by any EAS policy.

- **Platform, Model, OS, IMEI, EAS Device Type, IP Address** – The device information displays in these fields.
- **Mailbox Identity** – The location of the user mailbox in the Active Directory.

Filters for Quick Search

The **Filter** option is available on the List View page. Using this filter, you can narrow your device search based on:

- **Last Seen** – All, less than 24 hours, 12 hours, 6 hours, 2 hours.
- **Managed** – All, Managed, Unmanaged.
- **Allowed** – All, Allowed, Blocked.
- **Policy Override** – All, Blacklisted, Whitelisted, Default.
- **Policy Violation** – Compromised, Device Inactive, Not data Protected/Enrolled/MDM Compliant, Unapproved EAS Device Type/Email Account/Mail Client/Model/OS.
- **MEM Config** – Filter devices based on the configured MEM deployments.

Performing Actions

The **Override**, **Actions**, and **Administration** drop-down menu provides a single location to perform multiple actions on the device.

Note: Note that these actions once performed cannot be undone.

Override

Select the check box corresponding to a device to perform actions on it.

- **Whitelist** – Allows a device to receive emails.
- **Blacklist** – Blocks a device from receiving emails.
- **Default** – Allows or blocks a device based on whether the device is compliant or non-compliant.

Actions

- **Run Compliance** – Triggers the compliance engine to run for the selected MEM configuration. For any device that has a state change (that is, compliant to non-compliant or conversely), Workspace ONE sends out an Allow/Block command accordingly.

Administration

- **Remote Wipe** – Resets the device to factory settings.
- **Migrate Devices** – Migrates selected device to other chosen MEM configurations by deleting the installed EAS profile and pushing the EAS profile of the chosen configuration on the device.

Best Practice

Testing the email policies before deploying on the devices is a good practice. Workspace ONE recommends using the following method to test the capabilities of these policies before applying them on the devices.

- Disable the **Compliance** option available on the **Email Policies** page during the testing phase. Use separate organization groups to test out policies against a subset of enrollment users who also belong to the Gmail environment.

Device Management with Direct Password Management Integration

The Direct Integration using Password Management deployment does not involve SEG integration, thus, the Email and Attachment Policies are not applicable.

If using the password retention approach, you can use the compliance policies and the Email Dashboard to manage the devices and view the device status. If you choose not to retain the password, then the email policies are not applicable and the device status is not displayed on the Email Dashboard.

With Password Retention

Managed Device Polices

Activate the following policies from **Email** > **Compliance Policies** page. .

- **Inactivity** – Allows you to prevent inactive, managed devices from accessing email. You can specify the number of days a device shows up as inactive (that is, does not check in to Workspace ONE), before email access is cut off.
- **Device Compromised** – Allows you to prevent compromised devices from accessing email. Note that this policy does not block email access for devices that have not reported compromised status to Workspace ONE.
- **Encryption** – Allows you to prevent email access for unencrypted devices. Note that this policy is applicable only to devices that have reported data protection status to Workspace ONE.
- **Model** – Allows you to restrict email access based on the Platform and Model of the device.
- **Operating System** – Allows you to restrict email access to a set of operating systems for specific platforms.

- **Require ActiveSync Profile** - Allows you to restrict email access to devices whose email is managed through an Exchange ActiveSync profile.

Email Dashboard

Access the Email Dashboard page from **Email** > **Dashboard**. The **Actions** drop-down menu provides a single location to perform multiple actions on the device. Select the check box corresponding to a device to perform actions on it.

- **Whitelist** - Allows a device to receive emails
- **Blacklist** - Blocks a device from receiving emails
- **Default** - Allows or blocks a device based on whether the device is compliant or non-compliant

Without Password Retention

Device Compliance Policies

In this type of deployment, email compliance policies are not applicable. You can only assign the device compliance policies that are available at **Devices** > **Compliance Policies** > **List View**. You can set these policies as 'Remove EAS Profile' to ensure removal of email connectivity once the device is found to be non compliant.

Device Dashboard

In this type of deployment, Email Dashboard does not display the devices. You can view and manage devices of this deployment through the Device Dashboard available at **Devices** > **Dashboard**.