Introduction to Google Apps for Business Integration

Overview

Providing employees with mobile email access can introduce a number of security concerns not addressed by most standard email security infrastructures. Organizations using the Google Apps for Business email infrastructure may be familiar with the challenge of securing email endpoints for Gmail and preventing mail from circumventing the secure endpoint. AirWatch provides you with an end-to-end solution that allows you to fully integrate your corporate infrastructure without compromising security.

Benefits of AirWatch Integration

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

In This Guide

- Before You Begin – This section covers the basic requirements and other topics that would help you get started with the solution.
- Google Apps for Business Implementation – This section covers how to setup and create an account with the proper privileges in the Google Apps for Business.
- Google Apps for Business Configuration – This section covers how to configure Google Apps for Business infrastructure using the AirWatch Mobile Email Management solution.
- Email Management through Google Apps Integration – This section covers how to manage the mobile fleet using the many features of AirWatch Admin Console.

Before You Begin

Overview

The Before you Begin topic provides the information that helps you with the initial setup, configuration, and understanding of the requirements essential for a smooth user experience.

In This Section

- Requirements - The required list of network, hardware, and software.
- Recommended Reading - This section provides helpful background and supporting information available from other AirWatch guides. All of these guides can be accessed via the AirWatch Resources Portal (https://resources.air-watch.com).

System Requirements

- Web-based access to Google services authenticated using a Single Sign On.
- Google Admin Account with special permissions.
- API Access to Google Apps for Business.
- AD/LDAP passwords should not be synced to corresponding Google accounts.
- End users should accept the Google end-user license agreement.

Recommended Reading

- **AirWatch Mobile Email Management Administration Guide** - A comprehensive guide of the AirWatch's mobile email management functionality.
- **AirWatch Mobile Device Management Guide** - A comprehensive guide of the AirWatch's device management functionality.

Google Apps for Business Configuration

Overview

The Google Apps mobile email configuration is designed to work with Google Cloud Email Services. The Google Apps for Business email infrastructure can be set up using the AirWatch Mobile Email Management framework either with or without a proxy (SEG).The following sections explains the different types of integration supported by AirWatch. Once you integrate Google Apps Email system settings, you can deploy Exchange ActiveSync profiles to your devices to automatically configure individual end-user email accounts.

In This Section

- Integrating without SEG and without password purge - Explains this integration and how to configure it from the AirWatch Admin Console.
- Integrating without SEG and with password purge - Explains this integration and how to configure it from the AirWatch Admin Console.
- Integrating with SEG Proxy - Explains this integration and how to configure it from the AirWatch Admin Console.

Integrating without SEG and without password purge

Using this approach, the AirWatch server communicates with the Google Apps directly and retains the Google password 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 AirWatch Admin Console. By default, unmanaged devices are blocked.

System Configuration

1. From the AirWatch Admin Console main menu, navigate to **Email ▶Settings** and then click **Configure**. The MEM Configuration wizard displays.
2. In the Mail Platform wizard form:
   - Select **Google Apps for Business** as the email server type.
   - Select **Without SEG Proxy** as the Deployment Type and click **Next**.
3. In the MEM deployment wizard form:
   - Enter a friendly name for the Google deployment. This name gets displayed on the MEM dashboard screen for devices managed by SEG.
   - Enter the registered Google Apps Domain address and Admin credentials (having required privileges) in the applicable fields.
   - Click **Next**.
4. In the MEM Profile Deployment wizard form:

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.

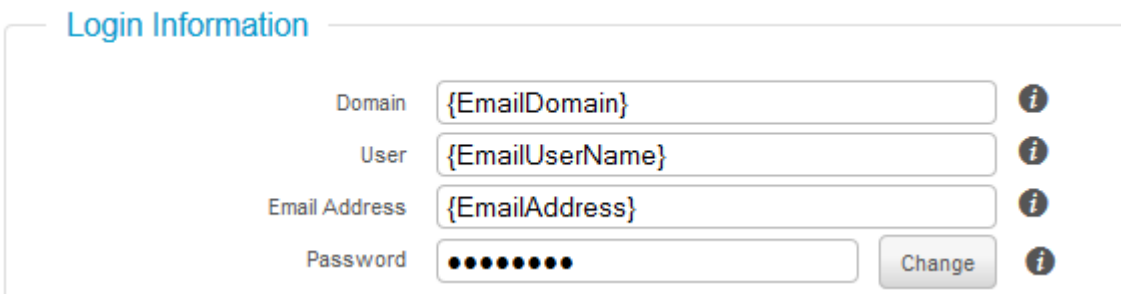
- Select a device platform from the available list.
- Select an email client from the available list.
- Create a new profile or associate an existing profile of the above chosen platform and email client.
- Assign a profile from the displayed list.

5. Click **Next**. The Summary form provides a quick overview of the basic configuration you have just created for the Google deployment. **Save** the settings.
6. Optionally, you can configure the advanced settings. To do this, navigate to **Email ▶Settings** page and then click the  icon.

- Enter the preferred length of the password in the **Google Random Password Length** field. Minimum accepted characters is 8 and maximum is 100.
- Select the **Retain Google Password** checkbox (enabled by default as part of recommended settings) . This option encrypts and stores the Google password in the AirWatch database.
- Click **Save**.

Profile Configuration

1. Navigate to **Devices ▶Profiles ▶List View**.
2. Click **Add** and select the platform for the device that will receive the profile.
3. Enter the **General** settings for the profile.
4. Select **Exchange Active Sync** as the profile payload and then click **Configure**.
5. Select the type of **Mail Client**.
6. Enter your **Account Name**.
7. Enter **m.google.com** as the **Exchange ActiveSync Host**.
8. Under **Login Information**, use Lookup Values to populate the end-user's account information, including {EmailPassword} for the password field.



Integrating without SEG and with password purge

Using this approach, the AirWatch server communicates with the Google Apps directly. 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 AirWatch Admin Console. By default, unmanaged devices are blocked. This is a recommended approach.

To configure Google Apps without SEG:

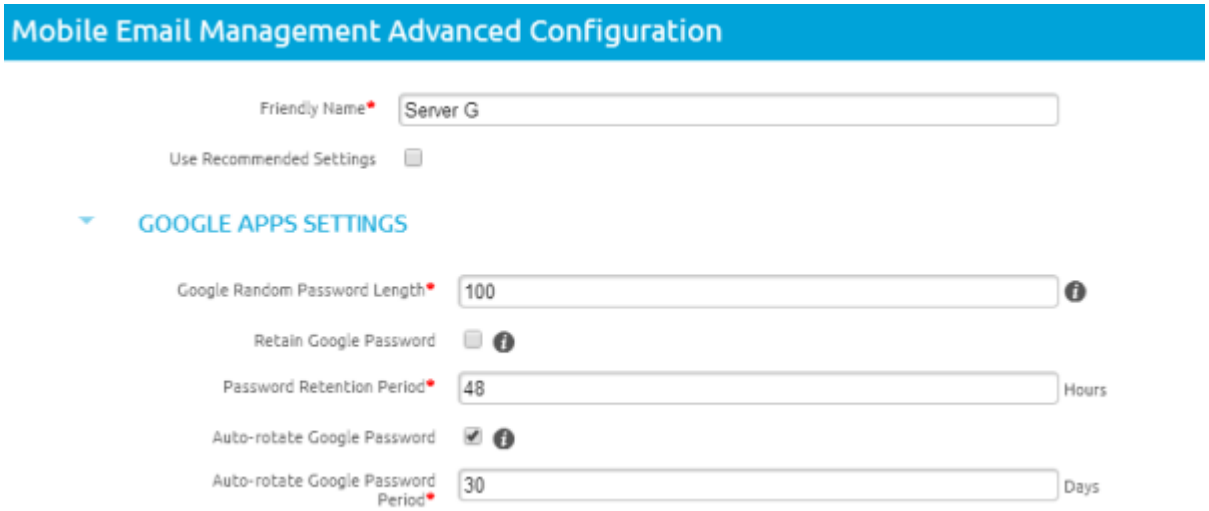
1. From the AirWatch Admin Console main menu, navigate to **Email ▶Settings** and then click **Configure**. The MEM Mail Deployment wizard form displays.
2. Follow the above mentioned steps 2-step 5.
3. In the **Advanced** settings form:

Disable **Use Recommended Settings** and the **Retain Google Password** checkbox. By default, this option is enabled to encrypt and to store the Google password in the AirWatch database.

Note: Please note that if a user has two devices enrolled and when one of the devices un-enrolls, then the Google Apps password resets and new generated password is pushed to the device that is enrolled.

Once this option is deselected, you can also configure the following options:

- **Google Random Password Length** – Enter the preferred random password length. Minimum accepted characters is 8 and maximum is 100.
- **Password Retention Period** – Enter the number of hours the password should be retained temporarily for management purposes. The default value is 48. The minimum accepted characters 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 characters is 1 and maximum is 90.
- **Auto-rotate Google Password Period** – Enter the specific period to reset Google password. The default period is 30 days.

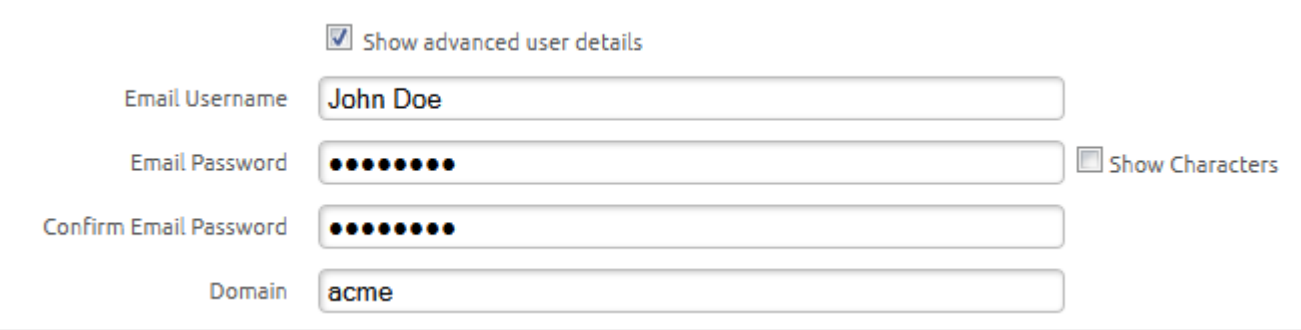


4. Click **Save**.

You can now configure Exchange ActiveSync profiles for each end user as described previously. Ensure the **Exchange ActiveSync Host** is 'm.google.com'.

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.

Note: To avoid the 'invalid user' error when Google API uses the **Email Username** field of the 'User Template' (**Accounts** > **Users**), please enter a valid Google email account and **email username without the domain** in the **Email Username** field. This field becomes available on selecting the **Show advanced user details** checkbox.

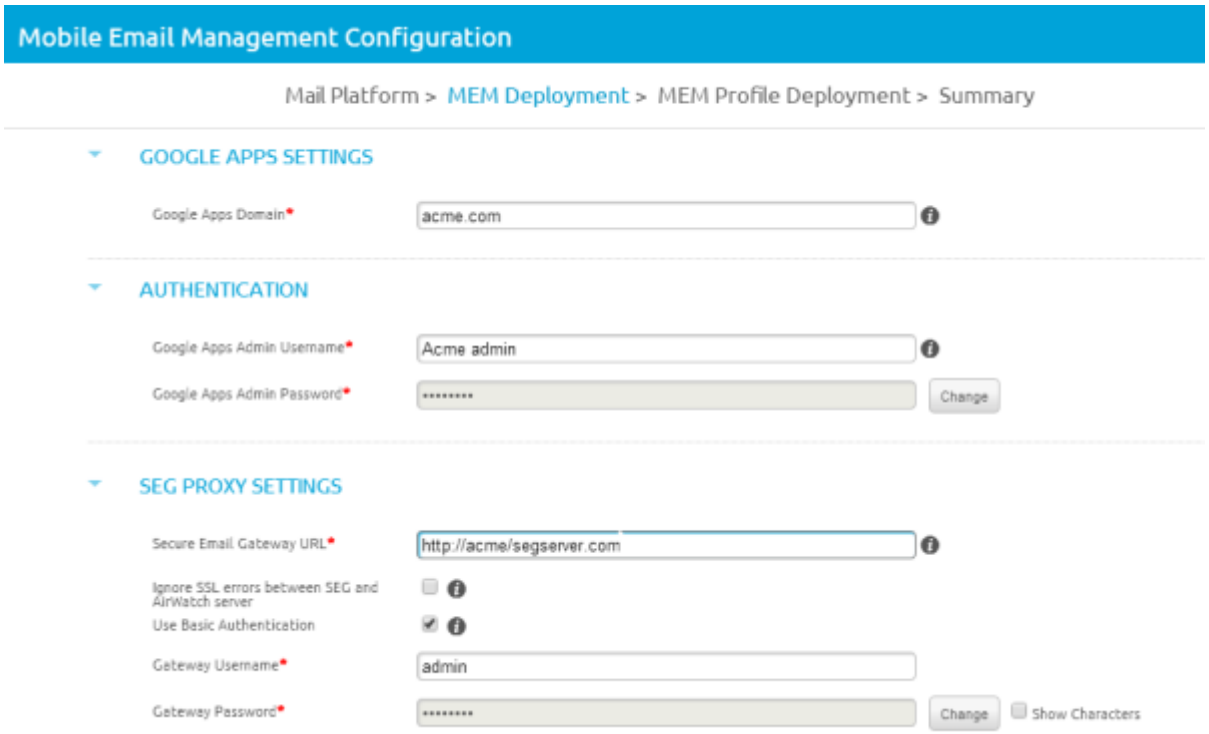


Integrating with SEG Proxy

Using this approach, the SEG proxy server sits in-line between the AirWatch server and the Google Apps. The SEG proxy directs and manages the email traffic to and from the device. With SEG, you get visibility of both the managed and unmanaged devices on the Email Dashboard. You can also benefit from the email policies available. For more information about email policies, refer to the **AirWatch Mobile Email Management Administration Guide**.

System Configuration

1. Navigate to **Email ▶Settings** and click **Configure**.The MEM Configuration wizard displays
2. In the Mail Platform wizard form
   - Select **Google Apps for Business** as the Email Server Type.
   - Select **With SEG Proxy** as the Deployment Type.
   - Click **Next**.
3. In the MEM Deployment wizard form:



- Enter a friendly name for the SEG deployment. This name gets displayed on the MEM dashboard screen for devices managed by SEG.
- Enter the Google Apps Domain address.
- Enter the Google Apps Admin credentials in the applicable fields.
- Configure the following SEG Proxy settings:
- **Secure Email Gateway URL** - Enter the proxy server address to which the API can connect.
- **Ignore SSL errors between SEG and AirWatch server** - You may choose to enable the this check box to ignore Secure Socket Layer (SSL) certificate errors between AirWatch component and the SEG server.
- **Use Basic Authentication** - Select this check box 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.

Note: For information on how to configure and install SEG, please refer to the **Secure Email Gateway AdministrationGuide**.

4. In the MEM Profile Deployment wizard form:

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.

- Select a device platform from the available list.
- Select a email client from the available list.
- Create a new profile or associate an existing profile of the above chosen platform and email client.
- Assign a profile from the displayed list.

5. Click **Next**. The Summary form provides a quick overview of the basic configuration you have just created for the SEG deployment. **Save** the settings.
6. Optionally, you can configure the advanced settings. To do this, navigate to **Email ▶Settings** page and then click the  icon located on the right-hand side of the required Google deployment.
    - By default, the **Use Recommended Settings** check box is enabled to capture all SEG traffic information from devices. Otherwise, specify what information and how frequently the SEG should log for devices.
    - Select the **Enable Real-time Compliance Sync** option to enable the AirWatch Admin Console to remotely provision compliance policies to the SEG Proxy server.
    - Enable the **Ignore SSL Errors** check box to ignore Secure Socket Layer (SSL) certificate errors between SEG and the email server.
    - Enable the **Ignore SSL Errors** check box to ignore Secure Socket Layer (SSL) certificate errors between AirWatch component and SEG server.
7. **Save** the settings.

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

Warning! : If you choose to set up Email Management with AirWatch for Google Apps for Business, all the passwords will change regardless of any settings that you choose i.e via SEG or without SEG, or with Password Retention or Password Purging.
If you want to keep the users passwords the same then DO NOT integrate Google Apps with AirWatch. The only option then would be to push the EAS profile but keep in mind that this would cause loss of MEM tracking capabilities.

Google Apps for Business Implementation

Overview

In order to manage and provision Google user's passwords, AirWatch requires a Google Apps for Business administrator account with specific privileges. Either a super user account or an administrator account with the privileges displayed below can be used.

In This Section

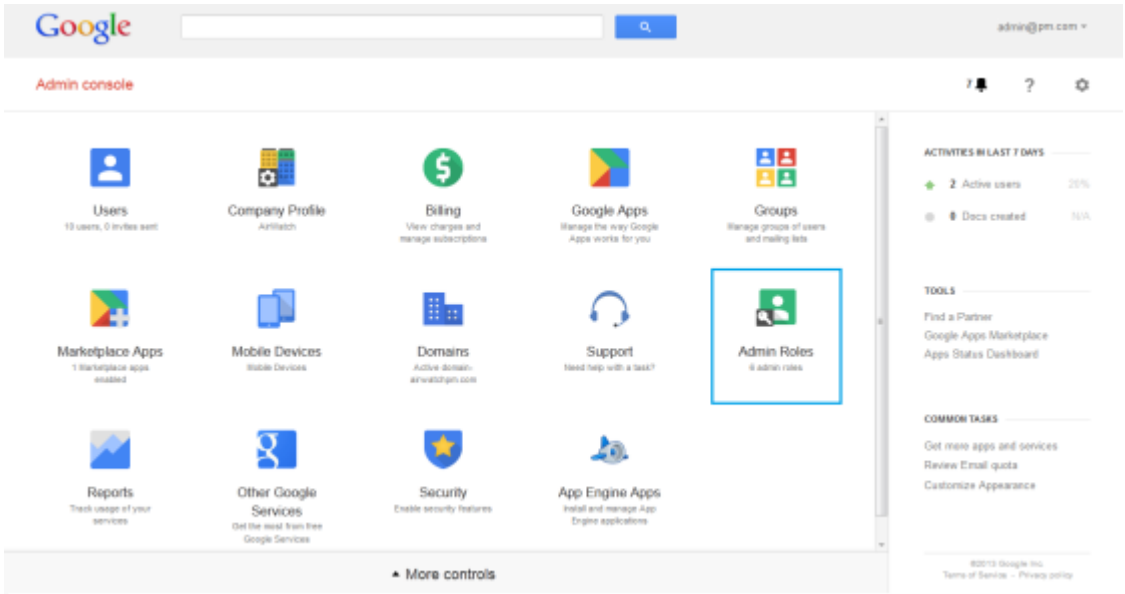
- Creating an Admin Role - Details how to create a admin role to manage the Google App integration.
- Enabling the Google API - Describes the steps required to provision user's password.

Creating an Admin Role for Google Apps Integration

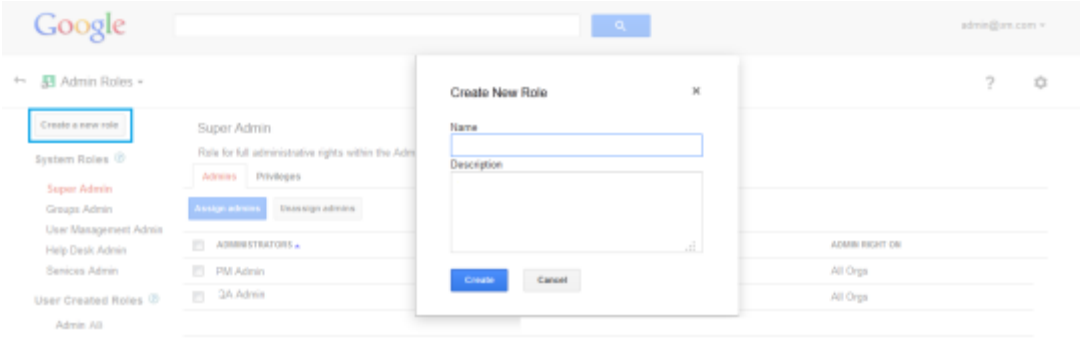
To create a custom set of admin permissions:

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

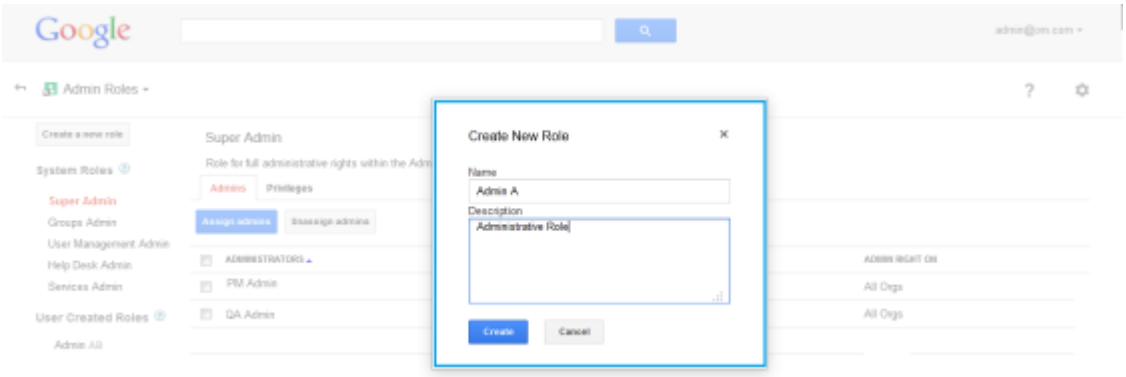
> **Note**: 1. If you choose to use a super admin account, skip to step 5.
> 2. Use a service account if you do not want AirWatch to change or revoke the admin password from the Google console.



2. Select **Create a new role**. The **Create New Role** form displays.



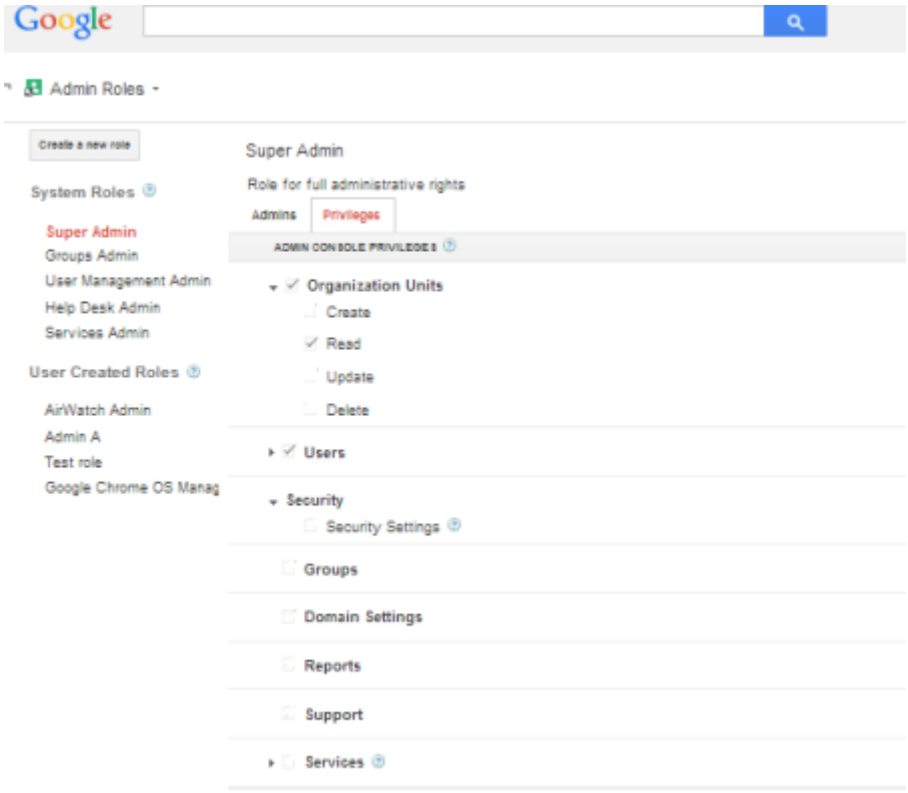
3. Enter the **Name** and **Description** for the role, and then click **Create**.

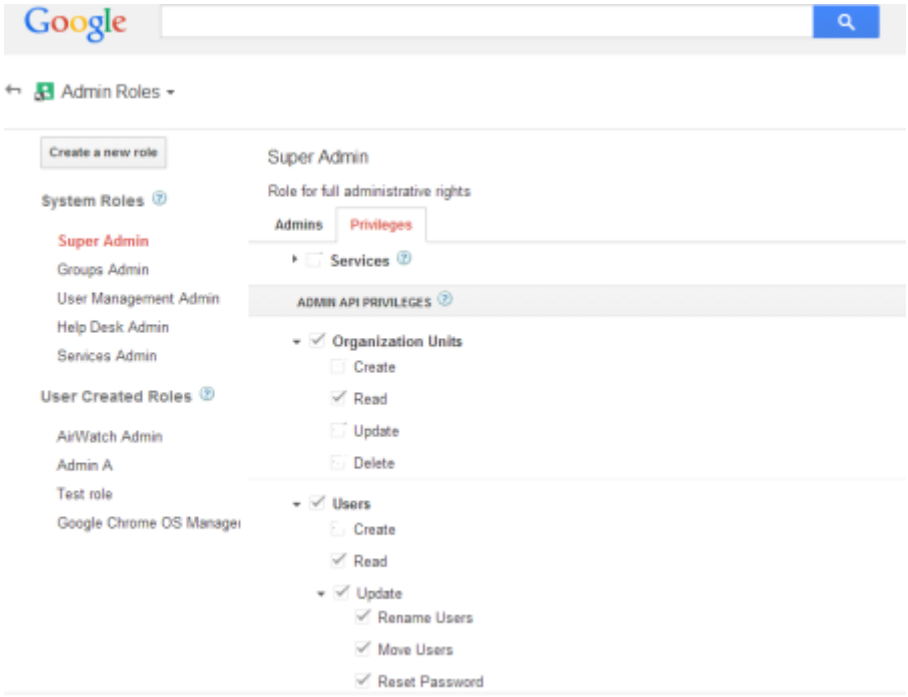


4. Select the **Privileges** tab and enable the required privileges. The required privileges include:

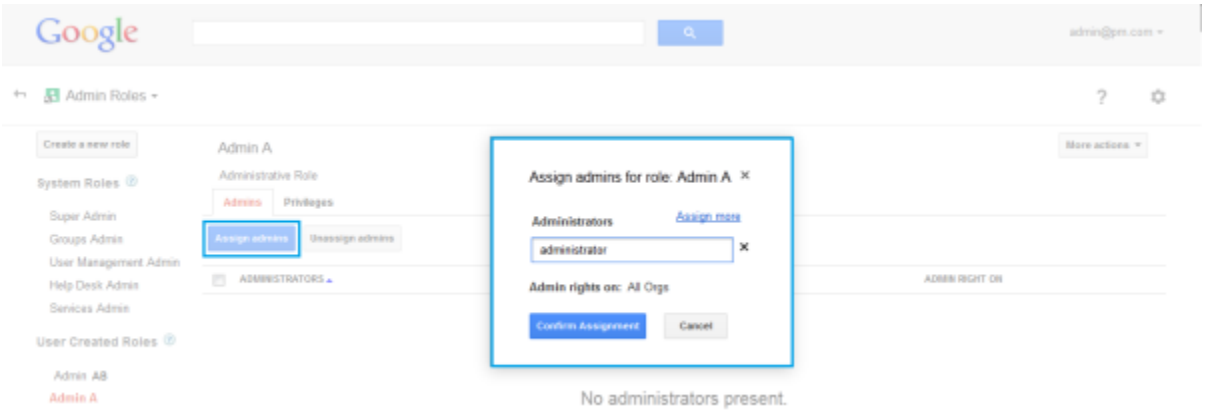
- Admin Console Privileges
  - Organization Units - Read
  - Users -Read
  - Update - Rename users, Move users, Reset Password, Force Password, Add/Remove Aliases, Suspend Users
- Admin API Privileges
  - Organization Units - Read
  - Users -Read
  - Update - Rename users, Move users, Reset Password, Force Password, Add/Remove Aliases, Suspend Users

Click **Save Changes**.


Google
Admin Roles
Create a new role
System Roles
Super Admin
Groups Admin
User Management Admin
Help Desk Admin
Services Admin
User Created Roles
AirWatch Admin
Admin A
Test role
Google Chrome OS Manag
Super Admin
Role for full administrative rights
Admins
Privileges
ADMIN CONSOLE PRIVILEGES
Organization Units
Create
Read
Update
Delete
Users
Security
Security Settings
Groups
Domain Settings
Reports
Support
Services


Google
Admin Roles
Create a new role
System Roles
Super Admin
Groups Admin
User Management Admin
Help Desk Admin
Services Admin
User Created Roles
AirWatch Admin
Admin A
Test role
Google Chrome OS Manage
Super Admin
Role for full administrative rights
Admins
Privileges
Services
ADMIN API PRIVILEGES
Organization Units
Create
Read
Update
Delete
Users
Create
Read
Update
Rename Users
Move Users
Reset Password

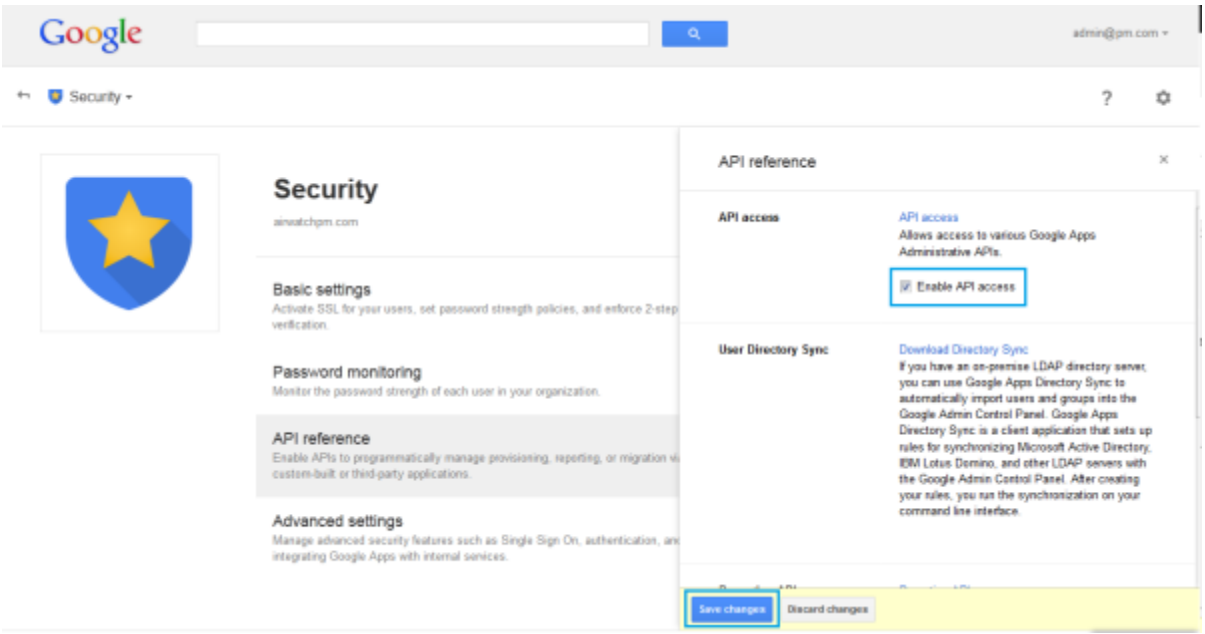
5. Next, click the **Admins** tab and then **Assign admins** to assign the created role to an administrator and then click **Confirm Assignment**.



Enabling the Google API

In order for AirWatch to provision user's passcodes, the Google API must be enabled via the Google Apps control panel. 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 click **Save Changes**.



Email Management through Google Apps Integration

Overview

After the Google integration setup is complete, you can manage the connected device email traffic, set email policies, and take appropriate actions on the devices from the AirWatch Admin console. The features available here depends on the type of deployment that you choose. Please see the below sections for more information.

In This Section

- Managing Devices without SEG and without Password Purge Integration - This section covers the features available in AirWatch managed Google Apps for Business without integrating SEG and password purging that enable you to manage devices effectively.
- Managing Devices without SEG and with Password Purge Integration - This section covers the features available in AirWatch managed Google Apps for Business without integrating SEG that enable you to manage devices effectively.
- Managing devices with SEG Proxy Integration - This section covers the features that are available in AirWatch managed Google Apps for Business with integrated SEG that enable you to manage devices effectively.

Managing Devices without Secure Email Gateway (SEG) and without Password Purge Integration

Since this deployment does not include SEG integration, the email and attachment policies are not applicable.

Managed Device Polices

Enable the below policies from **Email ▶Compliance Policies**.You can activate or deactivate the policies using the colored buttons under the **Active** column. Use the edit policy icon under the **Actions** column to allow or block a policy.

- **Inactivity** – Allows you to prevent inactive, managed devices from accessing email. You can specify the number of days a device shows up as inactive (i.e. does not check-in to AirWatch), 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 AirWatch.
- **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 AirWatch.
- **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.

Email Dashboard

Access the Email Dashboard page from **Email ▶Dashboard**. The **Actions** dropdown 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

Managing Devices without SEG and with Password Purge Integration

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 should 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**.

Managing Devices with SEG Proxy Integration

Compliance Policies

Enable the below policies from **Email ▶Compliance Policies**.You can activate or deactivate the policies using the colored circles under the **Active** column. Use the edit policy icon under the **Actions** column to allow or block a policy.

General Email Policies

- **Sync Settings** – Prevent the device from syncing with specific EAS folders. Note that AirWatch 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 re-sync 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 (i.e. does not check-in to AirWatch), 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 AirWatch.
- **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 AirWatch.
- **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.

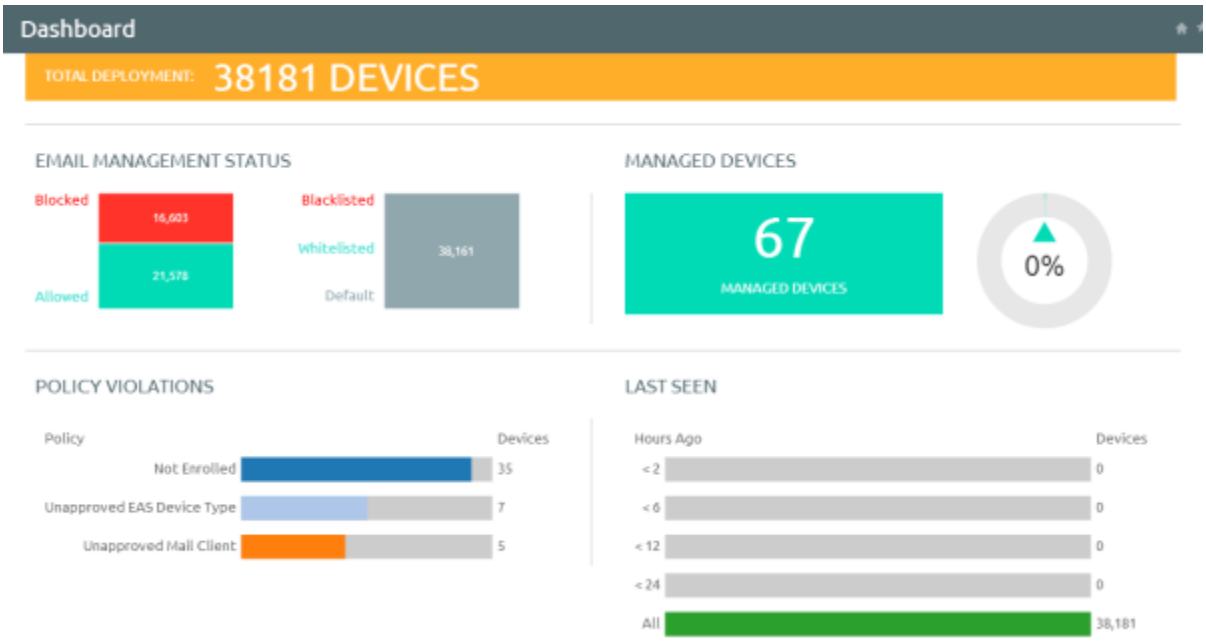
Email Security Policies

- **Hyperlink** – Allow device users to open hyperlinks contained within an email directly with a secure AirWatch application (e.g. AirWatch Browser) present on the device. Based on the application list sample, AirWatch dynamically modifies the hyperlink for the appropriate application on the device.

Email Dashboard

Gain visibility into the email traffic and monitor the devices through the AirWatch**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, un-managed, 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 AirWatch 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 include:

- **Last Request** - In PowerShell integration, this column displays the last state change of the device either from AirWatch 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. Please note that the reason code displays 'Global' and 'Individual' only when the access state of the email is changed by an entity other than AirWatch (for example, an external administrator).
- **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

From here, using the **Filter** option,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** dropdown 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.
- **Test Mode** - Tests email policies without applying them on devices.

Administration

- **Dx Mode On** - Runs the diagnostic for the selected user mailbox.
- **Dx Mode Off** - Turns off the diagnostic for the selected user mailbox.
- **Update Encryption Key** - Resets the encryption and the re-syncs the emails for the selected devices.
- **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.