MobileIron Email+ 3.8.0 for Android Guide

for MobileIron Core and MobileIron Cloud

December 02, 2020

For Email+ product documentation see:
MobileIron Email+ for Android Product

Contents

New features summary

This guide documents the following new features and enhancements:

- Email+ app new features and enhancements
- Email+ administrator features

Email+ app new features and enhancements

- **Select multiple classification values**: Support for selecting multiple field values for the Email Classification implemented. This can be achieved with multiselectField JSON property in **email_security_classification_json** configuration text. For more information see, Document classification capabilities.
- **Redesigned email detail view**: The email screen is redesigned with the following new features:
  - The email detail view is collapsed by default, to expand the mail details such as email addresses tap on the screen.
  - The email addresses are now comma separated.
  - The signed certificate and encrypted mail labels are now available below the attachments field.
- **New classification picker screen**: A new classification picker screen has been added to the Email+ app. When composing or replying to a mail, tap on the classification field to vies the new classification screen. There are two new values **Information Management Marker** and **Caveat** are added.

Email+ administrator features

- **New key-value pair and restriction added**: A new key-value pair **report_phishing_address** has been added to Android AppConnect, and a new restriction **Report phishing** has been added to configure reporting a suspicious mail. For more information, see Key-value pairs for Email+ (Android AppConnect) and App restrictions descriptions for Email+ (Android enterprise) sections.

Overview of Email+ for Android

The following provide an overview of the Email+ app for Android devices:

About Email+ for Android

MobileIron Email+ provides secure email, calendar, contacts, and tasks on corporate-owned and personal Android devices by communicating with an ActiveSync server in your enterprise.

Email+ for Android is available in two flavors, Android AppConnect and Android enterprise.

- Email+ Android AppConnect
- Email+ for Android enterprise

Email+ Android AppConnect

Email+ is available as an Android AppConnect app.

AppConnect is a MobileIron feature that containerizes apps to protect data on iOS and Android devices. Each AppConnect-wrapped app becomes a secure container whose data is encrypted, and protected from unauthorized access. Because each user has multiple business apps, each app container is also connected to other secure app containers. This connection allows the AppConnect apps to share data, such as documents. AppConnect apps are managed using policies configured in a MobileIron unified endpoint management (UEM) platform. The UEM platform is either MobileIron Core or MobileIron Cloud.

As an AppConnect app, all Email+ data is secured. The app interacts with other apps according to the data loss prevention policies that you specify. You can also take advantage of AppConnect features such as app authorization and app configuration.

Email+ for Android AppConnect has the following secure features:

- **Secure apps passcode**: A secure apps passcode, if you require one, gives device users access to all secure apps. This is the AppConnect passcode, which you define in the MobileIron UEM platform. The AppConnect passcode provides an additional layer of security for secure apps, beyond the device passcode.
- **Data encryption**: AppConnect encrypts all AppConnect-related data on the device, such as Email+ app data, app configurations, and policies. This means app data is secure even if a device is compromised. App data on the device is encrypted using AES-256 encryption. The encryption key is not stored on the device. It is programmatically derived, in part from the device user's AppConnect passcode, if you require an Appconnect passcode.

- **Data loss prevention**: You determine whether device users can take screen captures of protected data. You also determine whether AppConnect apps can access camera photos or gallery images, and whether they can stream media to media players. You can also specify copy/paste restrictions and a web browser policy.
- **Secure apps data deletion**: If a device is retired, or a secure app is retired, the secure app's data is deleted.

For information about AppConnect features and configuration beyond Email+ for Android, see *MobileIron AppConnect and AppTunnel Guide* .

Email+ for Android enterprise

Email+ for Android enterprise has the following secure features:

- **Data loss prevention**: You determine whether device users can take screen captures of protected data as well as specify if users can copy/paste protected data.
- **Data deletion**: App data is removed from a device for any of the following:
  - The device is retired.
  - The app is removed from the label or the app catalog (MobileIron Core)
  - Users are removed from app distribution (MobileIron Cloud)
  - The app is uninstalled from the device

Where to find Email+ for Android

For the current download location, see the *MobileIron Email+ for Android Release Notes*.

Support and compatibility for Email+ for Android

For support and compatibility information, see the *MobileIron Email+ for Android Release Notes*.

About configuring Email+ for Android

You configure settings for Email+ in the MobileIron UEM platform. Because the MobileIron UEM platform provides these settings to the app, device users do not have to manually enter configuration details. By automating the configuration for device users, each user has a better experience when installing and setting up the app. Also, the enterprise has fewer support calls, and the app is secured from misuse due to configuration.

The Email+ settings include, for example:

- the Standalone Sentry that interacts with the ActiveSync server or the ActiveSync server if you are not using Standalone Sentry.
- the user's ID for the ActiveSync server.
- the SCEP or certificate setting for the certificate that the device presents to the Standalone Sentry for authentication, if you are using certificates for authentication.

- custom app configurations that allow administrators to control app behavior.

What users see in Email+ for Android

When users install Email+ for Android, the following apps are available on the home screen:

- Mail: Enables users to send and receive their corporate email, and manage any sub-folders.
- Calendar: Enables users to manage and synchronize their corporate calendar data, including meetings and appointments in a daily, monthly, or list view.
- Contacts: Enables users to manage and synchronize their corporate contacts.
- Tasks: Enables users to manage, synchronize, and create new tasks.

NOTE: When the Email+ app (Android) is installed, the folders and sub-folders are listed in the same order as in mail exchange. If a new folder or sub-folder is added to the exchange, the newly added folder is listed last in the Email+ app and is not listed in the same order as it is in the mail exchange.

Settings is available in each app and allows users to manage settings specific to the app.Users manage their certificates, keys, recognized certificate authorities, S/MIME signing and encryption in **Settings** in the Mail app.

Configuring Email+ for Android AppConnect

The following describe how to set up Email+ for Android AppConnect:

Before you configure Email+ for Android AppConnect

Before you configure Email+ for Android for AppConnect:

- Ensure that all devices to which you plan to deploy Email+ are able to access https://activate-emailplus.mobileiron.com. This URL enables the use of ActiveSync features in Email+. No identifiable information, however, is reported to the server.
- Download the current version of the Email+ for Android app and Secure Apps Manager (SAM) from the MobileIron support download site. SAM is required for Core deployments only. For the current download location see the *MobileIron Email+ for Android Release Notes*.
- If your setup uses certificates, such as, for S/MIME or certificate-based authentication, ensure that the necessary certificate settings are created in the MobileIron UEM.
- **MobileIron Core:** For information about configuring certificates in MobileIron Core, see the "Managing Certificates and Configuring Certificate Authorities" section in the *MobileIron Core Device Management Guide*.
- **MobileIron Cloud:** For information about configuring certificates in MobileIron Cloud, see the "Certificate" and the "Identity Certificate Configuration" sections in the *MobileIron Cloud Administrator Guide*.
- If you are using Standalone Sentry to allow access to your enterprise ActiveSync server, ensure that you have a Standalone Sentry enabled for ActiveSync and the necessary device authentication configured.
- For information on how to set up Standalone Sentry, see the *MobileIron Sentry Guide* for your MobileIron UEM deployment.
- MobileIron recommends the following:
  - Standalone Sentry should use a trusted CA certificate.
  - If your UEM is MobileIron Core, and if the Standalone Sentry self-signed certificate is changed, you must do the following additional setup in Core:
    In the **Services > Sentry** page, for the Standalone Sentry, click the **View Certificate** link. This makes the Standalone Sentry's certificate known to MobileIron Core.

Main configuration steps for Email+ for Android AppConnect (Core)

Following are the main steps for configuring and deploying Email+ for Android AppConnect on MobileIron Core:

1. Adding Email+ for Android AppConnect and Secure Apps Manager to MobileIron Core.
2. Enabling third-party AppConnect apps in MobileIron Core.
3. Configuring the AppConnect global policy in MobileIron Core.
4. Configuring the AppConnect container policy in MobileIron Core.
5. Configuring an AppConnect app configuration for Email+ in MobileIron Core.
6. Configuring email attachment control with Standalone Sentry in MobileIron Core. (For Standalone Sentry deployments only)

Adding Email+ for Android AppConnect and Secure Apps Manager to MobileIron Core

You add Email+ and Secure Apps Manager (SAM), in the same manner you would add any other Android in-house app. After adding the apps to MobileIron Core, you can distribute the apps to devices by applying the apps to labels that contain the devices you want to distribute the apps.

Procedure

1. In the MobileIron Core Admin Portal, go to **Apps > App Catalog > Add+ > In-House**. (Prior to MobileIron Core 8.0 go to **Apps > App Distribution Library**, and select **Add App)**.
2. Add the apps just as you would any in-house app. Add SAM if you have not already uploaded it to support other secure apps.
3. After adding the apps, apply the apps to appropriate labels so that they are available to the required devices.

Next steps

Continue on to Enabling third-party AppConnect apps in MobileIron Core on page 11.

Related topics

For information on adding in-house apps for Android, see “Working with Apps for Android devices” in the *MobileIron Core Apps@Work Guide*.

Enabling third-party AppConnect apps in MobileIron Core

Email+ requires that you enable the licensing option for third-party and in-house AppConnect apps.

Procedure

1. In the MobileIron Core Admin Portal, go to **Settings > System Settings**.
2. Click **Additional Products > Licensed Products**.
3. Select **AppConnect For Third-party And In-house Apps** if your organization has purchased it.

4. Click **Save**.

Next steps

Continue to Configuring the AppConnect global policy in MobileIron Core on page 12.

Configuring the AppConnect global policy in MobileIron Core

Because Email+ for Android is an AppConnect app, you need to configure an AppConnect global policy (if one has not already been configured). This policy specifies settings that apply to all AppConnect apps on a device. For example, you configure the AppConnect passcode requirements.

IMPORTANT: Make sure only one AppConnect global policy applies to each device.

NOTE: On the AppConnect global policy, you can authorize device users to use Email+ even if no AppConnect container policy is applied to the device.

Procedure

1. In the MobileIron Core Admin Portal, go to **Policies & Configs > Policies**.
2. Select **Add New > AppConnect**.
   You can also use an existing AppConnect global policy. Select it, and click **Edit**.
3. Complete the form.
   Most fields default to suitable values, but make sure that you select **AppConnect: Enabled** to enable AppConnect on the device.
4. Click **Save**.
5. Select the policy.
6. Select **Actions > Apply To Label**.
7. Select the labels to which you want to apply this policy.
8. Click **Apply**.

Next steps

Continue to Configuring the AppConnect container policy in MobileIron Core on page 12.

Related topics

For general details on the AppConnect global policy, see “Configuring the AppConnect global policy” in the *MobileIron AppConnect and AppTunnel Guide*.

Configuring the AppConnect container policy in MobileIron Core

This task is only required:

- If you did not select **Authorize for Apps without an AppConnect container policy**, in the AppConnect Global Policy.

- If you want to apply different data loss prevention policies to different devices. When you upload Email+ to MobileIron Core, Core automatically creates an AppConnect container policy for the app. Create an AppConnect container policy, if you want to apply different settings to different devices.

Note The Following:

- Make sure only one AppConnect container policy for Email+ is applied to each device.
- Core keeps in sync the labels that you apply to the app and the labels that you apply to the AppConnect container policy that Core automatically created.

WARNING: When you apply Email+ to a label, Core automatically adds the same label to the automatically-created AppConnect container policy. Be sure to remove that label from the automatically-created AppConnect container policy if you are using that label on a manually created AppConnect container policy.

Procedure

1. In the MobileIron Core Admin Portal, go to **Policies & Configs > Configurations**.
2. Click **Add New > AppConnect > Container Policy**.
   Alternatively, edit the automatically-created AppConnect container Policy for Email+.
3. Enter a name for the policy.
4. Enter a description for the policy.
5. In the **Application** field, choose the Email+.
6. Select **Allow Screen Capture** if you want to override the default restriction on screen capture.

NOTE: The remaining settings do not apply to Android. Also, the ability to open a document is always restricted to the secure container on Android devices.

7. Click **Save**.

Next steps

- If you created a new container policy, continue to Applying the container policy to labels in MobileIron Core on page 13.
- If you edited the automatically-created AppConnect container policy, continue to Configuring an AppConnect app configuration for Email+ in MobileIron Core on page 14.

Applying the container policy to labels in MobileIron Core

Do these steps if you created a new AppConnect container policy.

Procedure

1. Select the container policy.
2. Select **Actions > Apply To Label**.
3. Select the labels to which you want to apply this policy.
4. Click **Apply**.

Next steps

Continue to Removing labels from the automatically-created AppConnect container policy in MobileIron Core on page 14.

Removing labels from the automatically-created AppConnect container policy in MobileIron Core

Do these steps if you are not using the automatically-created AppConnect container policy.

Procedure

1. Select the automatically-created AppConnect container policy.
2. Select **Actions > Remove From Label**.
3. Select any labels that you applied to the AppConnect container policy that you just created.
4. Click **Remove**.

Next steps

Continue to Configuring an AppConnect app configuration for Email+ in MobileIron Core on page 14.

Configuring an AppConnect app configuration for Email+ in MobileIron Core

When you add Email+ for Android AppConnect, an AppConnect app configuration is automatically created for Email+. You can create a new AppConnect app configuration if you want to apply different settings to different devices. Otherwise, edit the automatically-created AppConnect app configuration to configure the ActiveSync server information and other settings that you want to customize.

The AppConnect app configuration for Email+ for Android AppConnect contains information such as:

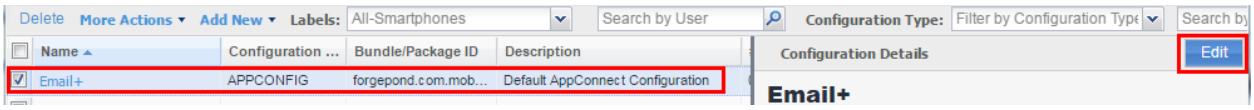
- The fully qualified domain name and user ID for the ActiveSync server.
- Certificate information.
- Key-value pairs that determine the app's settings and behavior.
  The default configuration contains the bundle ID for the app and a set of default key-value pairs that can be edited or deleted. You can also configure additional key-value pairs.

WARNING: Make sure only one AppConnect app configuration for Email+ is applied to each device.

NOTE: Always set the value of the `email_device_id` key to $DEVICE_UUID_NO_DASHES$. Standalone Sentry uses this key-value pair for ActiveSync correlation.

Procedure

1. In the Core Admin Portal, go to **Policy & Configs > Configurations**.
2. Select the automatically-created AppConnect app configuration for Email+ for Android, and click Edit.



3. Edit the configuration as needed.
4. Click **Save**.

The automatically-created app configuration has the same labels you applied to the app. You do not need to apply the automatically-created app configuration to a label.

Related topics

- For a description of the fields see AppConnect app configuration field descriptions.
- For descriptions and list of supported key-value pairs, see Key-value pairs for Email+ (Android AppConnect).

Creating a new AppConnect app configuration for Email+ for Android

Create a new AppConnect app configuration by saving the automatically created AppConnect app configuration for Email+ if you want to apply different settings to different devices.

Procedure

1. In the Admin Portal, go to **Policy & Configs > Configurations**.
2. Select the automatically created AppConnect app configuration for Email+.
3. Click **Actions > Save As** and save it as a new configuration.
4. Enter a new name and description for the configuration.
5. Edit the configuration as needed.
6. Click **Save**.
7. Select the new AppConnect app configuration.
8. Select **Actions > Apply To Label**.
9. Select the labels to which you want to apply this AppConnect app configuration.
10. Click **Apply**.
    The automatically-created app configuration is automatically applied to the same labels you applied to the app. However, only one app configuration should be applied to any one device. Therefore, remove the labels from the automatically-created app configuration.
11. Select the automatically-created AppConnect app configuration.
12. Select **Actions > Remove From Label.**
13. Select any labels that you applied to the AppConnect app configuration that you just created.
14. Click **Remove**.

Related topics

- For a description of the fields, see AppConnect app configuration field descriptions.
- For descriptions and list of supported key-value pairs, see Key-value pairs for Email+ (Android AppConnect).

AppConnect app configuration field descriptions

The following table provides description of the fields in an AppConnect app configuration for Email+ for Android.

TABLE 1. APPCONNECT APP CONFIGURATION FIELD DESCRIPTIONS

Item	Description
Name	Edit the default name if necessary. The name is not the same as the name that appears in the name column in **Policy & Configs > Configurations**.
Description	If necessary, edit the text to clarify the purpose of this AppConnect app configuration.
Application	Email+ is selected.
AppTunnel Rules This section is not applicable for Email+. If you are using a Standalone Sentry, all communication with the ActiveSync server is through a secure connection to the Standalone Sentry.	
App-specific Configurations Add key-value pairs to configure app behavior. The automatically-created app configuration for Email+ contains a set of default key-value pairs. Each key-value pair is configured as a separate row. Do the following: • For the **Value** of the `email_exchange_host` **Key**, enter the fully qualified domain name (FQDN) of the ActiveSync server, or the Standalone Sentry server if you are using a Standalone Sentry. • Edit the default key-value pairs as necessary. • To add a key-value pair, click **Add+** . • To delete a key-value pair, click **X**. The following key-value pairs are required: email_address email_device_id email_exchange_host email_exchange_username	

Configuring email attachment control with Standalone Sentry in MobileIron Core

This is only required if attachment control is enabled in Standalone Sentry.

Procedure

1. In the MobileIron Core Admin Portal, go to **Services > Sentry**.
2. Select the Standalone Sentry that handles email for the devices.
3. Click the edit icon.
4. In the **Attachment Control Configuration** section, for **iOS and Android Using Secure Email Apps**, select **Open With Secure Email App**.
5. Click **Save**.

Related topics

See “Email Attachment Control with Standalone Sentry” in the *MobileIron Sentry Guide for MobileIron Core*.

Main configuration steps for Email+ for Android AppConnect (Cloud)

Following are the main steps for configuring and deploying Email+ for Android AppConnect on MobileIron Cloud:

1. Adding Email+ for Android AppConnect and Secure Apps Manager to MobileIron Cloud.
2. Configuring Email+ for Android AppConnect in MobileIron Cloud.

Adding Email+ for Android AppConnect and Secure Apps Manager to MobileIron Cloud

You add Email+ in the same manner you would add any other Android in-house app. After adding to MobileIron Cloud, you can distribute the app to devices.

Procedure

1. In the MobileIron Cloud, go to **Apps > App Catalog > +Add > In-House**.
   Add the app just as you would any in-house app.
2. After adding the apps, select the distribution option that includes the users and devices to which you want to make Email+ for Android available.
3. Click **Next.**
   If the app was already in the catalog and you are editing the app, click **Save**.

Next steps

- Configuring Email+ for Android AppConnect in MobileIron Cloud on page 17.

Related topics

For details on adding in-house apps for Android, see the *MobileIron Cloud Guide* or click on **Help** in MobileIron Cloud.

Configuring Email+ for Android AppConnect in MobileIron Cloud

The Email+ for Android app configuration contains information such as:

- The fully qualified domain name and user ID for the ActiveSync server.
- Certificate information.
- Key-value pairs that determine the app’s settings and behavior.

The configuration contains a set of default key-value pairs that can be edited or deleted. You can also configure additional key-value pairs.

- The following key-value pairs are required:
  - email_address
  - email_device_id
  - email_exchange_host
  - email_exchange_username

IMPORTANT: MobileIron recommends changing to the default values as listed in Table 2 on page 18 and Table 3 on page 18.

TABLE 2. CHANGE DEFAULT VALUES TO RECOMMENDED VALUE

Key	Default value	Recommended value
email_device_id	$DEVICE_UUID_NO_DASHES$	${deviceSN}
email_exchange_username	$USERID$	${userEmailAddressLocalPart}
email_address	$EMAIL$	${userEmailAddress}

TABLE 3. DELETE RECOMMENDED DEFAULT KEY-VALUE PAIRS

Key	Default value	Recommended action
email_password	$PASSWORD$	DELETE
limit_contact_export_to	$NULL$	DELETE
email_safe_domains	$NULL$	DELETE

NOTE: If you were editing the Email+ app that has already been uploaded to the **App Catalog**, click on the **App Configurations** tab to edit the app installation, promotion, and configuration options.

Procedure

1. In **App Configurations** for Email+ select the install options and promotion options.
2. Click **Add** to add an **Email+ Configuration**.
3. Enter a **Name** for the configuration.
4. Click **+Add Description**, to add text describing the configuration.
5. In **AppConnect Custom Configuration**, for **email_exchange_host**, enter the fully qualified domain name (FQDN) of the ActiveSync server, or the Standalone Sentry server if you are using a Standalone Sentry.
6. Add, remove, or edit key-value pairs as necessary.
7. If setup uses Standalone Sentry and the Standalone Sentry is set up to authenticate devices using identity certificates, enter the following key-value pair in **AppConnect Certificate Configuration**:

Key	Value
email_login_certificate	Select the **Identity Certificate** setting created for the Certificate Authority certificate for Standalone Sentry. This sets up trust between Sentry and the device.

8. Click **Save**.

Related topics

For descriptions and list of supported key-value pairs, see Key-value pairs for Email+ (Android AppConnect) on page 23.

ActiveSync server synchronization due to app configuration changes (Core and Cloud)

Email+ synchronizes all emails, tasks, contacts, and calendar items with the ActiveSync server when the device user first launches Email+. It also does a full synchronization if you change the values of the following keys in the app configuration:

- email_address
- email_exchange_host
- email_exchange_username
- email_login_certificate

The full synchronization occurs the next time the device checks in after you have changed the app configuration.

Configuring Email+ for Android enterprise

The following describe the configuration for deploying Email+ for Android enterprise (Android for Work):

Before you configure Email+ for Android enterprise

Before you set up Email+ for Android enterprise ensure the following:

- Requirements for configuring Email+ for Android enterprise
- Recommendations for configuring Email+ for Android enterprise

Requirements for configuring Email+ for Android enterprise

The following are requirements for setting up Email+ for Android enterprise:

- Your MobileIron unified endpoint management (UEM) platform must be set up for Android enterprise.
  Your MobileIron UEM is either MobileIron Cloud or MobileIron Core.
  MobileIron Core: See the *MobileIron Core Device Management Guide for Android for Work*.
  MobileIron Cloud: See the MobileIron Cloud online **help** documentation.
- Your MobileIron setup must also include Standalone Sentry configured for ActiveSync.
  For information on how to set up Standalone Sentry, see the *MobileIron Sentry Guide* for your MobileIron UEM deployment.
- Ensure that the appropriate ports are open.
  MobileIron Core: See the *MobileIron On- Premise Installation Guide* for information on required ports and firewall rules associated with Standalone Sentry and different backend resources.
  MobileIron Cloud: See the MobileIron Cloud Architecture and Port Requirements document.
- If you are using certificate-based authentication to the ActiveSync server or to Standalone Sentry, ensure that certificates are distributed to the device.
  MobileIron Core: For information about configuring certificates in MobileIron Core, see the “Managing Certificates and Configuring Certificate Authorities” section in the *MobileIron Core Device Management Guide*.
  MobileIron Cloud: Ensure the certificate configuration is distributed to the same group as the Email+ app.

Recommendations for configuring Email+ for Android enterprise

MobileIron recommends the following:

- Standalone Sentry should use a trusted CA certificate.

- If your UEM is MobileIron Core, and if the Standalone Sentry self-signed certificate is changed, you must do the following additional setup in Core:
  - In the **Services > Sentry** page, for the Standalone Sentry, click the **View Certificate** link. This makes the Standalone Sentry's certificate known to MobileIron Core.

Email+ for Android enterprise app configuration and distribution

You add MobileIron Email+ for Android enterprise from your UEM platform from Google Play and configure the app to make it available to Android enterprise devices.

- Configuring app restrictions and distribution in MobileIron Core
- Configuring app restrictions and distribution in MobileIron Cloud

Configuring app restrictions and distribution in MobileIron Core

If your MobileIron UEM platform is MobileIron Core, you set up app configuration and distribution in the MobileIron Core Admin Portal.

Procedure

1. In the MobileIron Core Admin Portal, go to **Apps > App Catalog**.
2. Click **Add+**.
3. Click **Google Play**.
4. For **Application Name**, enter **MobileIron Email+**.
5. Click **Search**.
6. Select MobileIron Email+ in the search results.
7. Click **Next**.
8. (Optional) Update the following information:
   a. Edit the description for the app.
   b. Select the category you want the app to appear in Apps@Work on the device.
9. Click **Next**.
10. (Optional) In the Apps@Work Catalog section, select the promotion options as needed.
    These options determine if and how Email+ will be promoted in Apps@Work.

NOTE: The **Per App VPN Settings** are not applicable to Android enterprise apps.

11. (Required) In the **Android Enterprise** section, select **Install this app for Android enterprise**.
    You may need to scroll down to see the option. Additional fields are exposed when you select the option.
12. Select the install options as needed.
    These options determine how the app is installed and updated on the device:
    - **Silently Install:** Select to silently install the app without any user action.
    - **Auto Update this App**: Select to automatically update the app on users' devices whenever a new version of the app is available on Google Play.

NOTE: If auto update is selected, but the app fails update on a user's device (for example, if the device has an incompatible Android version), then the app may attempt to update repeatedly. The workaround is to deselect **Auto Update this App** for that app.

- **Block Uninstall**: Select to block device users from uninstalling the app.

13. In the **Configuration Choices** section, add a new configuration or edit the default configuration.
    If you add a new custom configuration be sure apply it to a label. If you have multiple configurations, you can assign priority by moving the configuration higher or lower in the list. The position in list determines the priority. The default configuration has the lowest priority and cannot be moved.
14. Click **Finish**.
15. Apply the Email+ Android enterprise app to the same labels as the app configuration you created in Step 13.

Related topics

See App restrictions descriptions for Email+ (Android enterprise) on page 37 for a description of the fields.

Configuring app restrictions and distribution in MobileIron Cloud

If your MobileIron UEM platform is MobileIron Cloud, you set up app configuration and distribution in the MobileIron Cloud portal. Email+ (Android for Work) is available in the app catalog under **Business Apps**.

Procedure

1. In the MobileIron Cloud portal, go to **Apps >App Catalog**.
2. Select **Email+ (Android for Work)** from **Business Apps**.
   A description and screen shots of the app are displayed.
3. Make changes, as needed, and click **Next**.
4. (Required) Select the check box for **I accept the following app permissions for all users of this app**, and click **Next**.
5. Select a distribution option and click Next.
   The configuration will be distributed to the devices in the group you selected.
6. Click **+** for **Android for Work** to configure settings for the app.
7. Enter a name and description for the configuration.
8. Select **Blocks the user for uninstalling the app** if you do not want device users to uninstall the app.
9. Configure the restrictions for the app and click **Next**.
10. Click **Install Application configuration settings** to configure the install options.
    a. Edit the **Name** and **Description** of the settings if necessary.
    b. **Install on Device**: Enable if you want to require that the app is installed on devices.
    c. **Silently install on Samsung KNOX and Zebra devices**: This option is not applicable to Android enterprise apps.
    d. **Do not show app in end user App Catalog**: Select if you do not want the app displayed in the MobileIron app catalog on users' devices.
11. Click **Next**.
12. Click **Promotion distribution configuration** settings and select a promotion option.
    The promotion option determines how the app appears in the app catalog on the device.
13. Click **Next** and then click Done.

Related topics

See App restrictions descriptions for Email+ (Android enterprise) on page 37 for a description of the restrictions.

Additional configurations using key-value pairs

The following describe how to customize Email+ app behavior:

Key-value pairs for Email+ (Android AppConnect)

Table 4 on page 24 describes the key-value pairs available to administrators to customize Email+ app behavior on Android devices. These key-value pairs define app behavior such as providing detailed notifications to device users and exporting contacts from Email+.

TIP: Key-value pairs marked as Core only are not applicable to MobileIron Cloud. For MobileIron Cloud deployments, these variables are either provided as fields in MobileIron Cloud or are set automatically and do not require action from the administrator. See Configuring Email+ for Android AppConnect in MobileIron Cloud on page 17 for a description of the fields in MobileIron Cloud.

Note The Following:

- Some values can use the MobileIron UEM variables, such as $EMAIL$ for MobileIron Core and ${userEmailAddress} for MobileIron Cloud. The MobileIron UEM substitutes the device user's value when sending the app configuration to the device.
- If you make a mistake in configuring the required key-value pairs, the app displays a message to the device user that the configuration has an error, and to contact the administrator.

You can configure and customize the following features with key-value pairs:

- Required Key-value pairs to configure an account on Email+
- Background email check and user notifications
- Certificates
- S/MIME
- Manage contacts
- Syncing
- Maximum size for email attachments
- Default signature
- Key-value pairs for Email+ (Android AppConnect)
- SSL
- GAL search
- Prompt the device user for password
- Show pictures
- Default network timeout
- Troubleshooting

TABLE 4. KEY-VALUE PAIRS FOR CONFIGURING EMAIL+ FOR ANDROID APPCONNECT APP BEHAVIOR

Key	Value: Enter/Select one	Description
Required Key-value pairs to configure an account on Email+		
email_ address	*Email address of the device user*	To validate that the account signed in is indeed the corporate account (the value is automatically set into modern auth UI, but can be changed there) **MobileIron Core** Typically, this field uses the Core variable $EMAIL$. You can also use combinations of these Core variables, depending on your ActiveSync server requirements: $USERID$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$. **MobileIron Cloud** Typically, this field uses the Cloud variable ${userEmailAddress}. You can also use combinations of the user attribute variables, depending on your ActiveSync server requirements. The user attribute variables are listed in MobileIron Cloud in **Admin > Attributes**.
email_ device_id	*The device ID that the ActiveSync server uses for the device.*	**MobileIron Core** Always use the Core variable $DEVICE_UUID_NO_ DASHES$. **MobileIron Cloud** Always use the Cloud variable ${deviceSN}.
email_ exchange_ host	*FQDN of the ActiveSync server or Standalone Sentry*	The fully qualified domain name (FQDN) of the ActiveSync server or Standalone Sentry. This KVP should be set to **outlook.office365.com**. Example: mySentry.mycompany.com
email_ exchange_ username	*User ID for the ActiveSync server*	**MobileIron Core** Typically, you use the Core variable $USERID$. If your ActiveSync server requires a domain, use *<domain name>*\$USERID$. For example: mydomain\$USERID$. You can also use combinations of these Core

TABLE 4. KEY-VALUE PAIRS FOR CONFIGURING EMAIL+ FOR ANDROID APPCONNECT APP BEHAVIOR (CONT.)

Key	Value: Enter/Select one	Description
		variables, depending on your ActiveSync server requirements: $EMAIL$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$. **MobileIron Cloud** Typically, you use ${userEmailAddressLocalPart}. If your ActiveSync server requires a domain, use <domain name>\${userEmailAddressLocalPart}. Example: mydomain\${userEmailAddressLocalPart}. Depending on your ActiveSync server requirements, you can use ${userEmailAddress}
Background email check and user notifications		
allow_ detailed_ notifications	• true • false	true: Device users see detailed notifications. The details can include sensitive information such as email subject and body previews, or event titles and times. false: Device users see normal notifications. Default if no key-value is configured: false.
Certificates The necessary certificate setting must have been created in the MobileIron UEM.		
email_login_ certificate	The certificate setting from the dropdown list	The MobileIron UEM sends the contents of the certificate as the value. Is also used when CBA is configured (to check if supported by Android) If the certificate is password-encoded, MobileIron Core automatically sends another key-value pair. The key's name is the following string: *<name of key for certificate>*_MI_CERT_PW The value is the certificate's password. Default if no key-value is configured: Certificates are not used.
email_trust_ all_ certificates	• true • false	true: Email+ automatically accepts untrusted certificates. Typically, you enter true only when working in a test environment. false: Email+ does not accept untrusted certificates.

TABLE 4. KEY-VALUE PAIRS FOR CONFIGURING EMAIL+ FOR ANDROID APPCONNECT APP BEHAVIOR (CONT.)

Key	Value: Enter/Select one	Description
		Default if no key-value is configured: false.
email_certificate_*X*, where X is 1 through 10	The certificate setting from the dropdown list	Email+ imports the certificate into its keystore of trusted certificates, and trusts any certificates derived from the CA root certificate in its keystore. The certificate must be DER-encoded. You can add up to ten certificate authority (CA) root certificates. Reasons for designating a CA root certificate as trusted: • Standalone Sentry requires a certificate, whose certificate authority is not in the Email+ keychain, for device authentication. A common scenario is if Standalone Sentry uses a self-signed certificate or a certificate that is not derived from a well-known certificate authority. NOTE: You specify this certificate to Email+ in the key email_login_certificate. It corresponds to the certificate you specified for device authentication in Standalone Sentry configuration in the MobileIron Core Admin Portal. • Certificates configured for encrypting or signing S/MIME emails are self-signed or not derived from a well-known certificate authority. NOTE: You specify these certificates in the keys email_encryption_certificate and email_signing_certificate. NOTE: Use .DER format instead of normal .PEM format for email_certificate_X certificates. The trusted CA root certificate is listed in Email+ in **Settings > Advanced Settings > KeyStore**.
eas_min_allowed_auth_mode	• basic • cert_base • modern_auth	Defines the authentication method to the Exchange ActiveSync server. • basic: Uses user name and password. • cert_base: Uses identity certificates for certificate-based authentication. • modern_auth:Uses enable modern auth for

TABLE 4. KEY-VALUE PAIRS FOR CONFIGURING EMAIL+ FOR ANDROID APPCONNECT APP BEHAVIOR (CONT.)

Key	Value: Enter/Select one	Description
		corresponding protocol. Enables Oauth 2.0 authorization. For certificate-based authentication, the key email_ login_certificate must also be configured. Default if no key-value is configured: basic.
allow_ certificate_ revocation_ check	• true • false	The admin can use this KVP to check certificates validity. The CRL check for server certificate is performed only if th **email_trust_ all_ certificates** KVP is set to "false".
S/MIME		
email_ encryption_ certificate	The certificate setting from the dropdown list	Specifies the certificate to use for encrypting S/MIME emails. The MobileIron UEM sends the contents of the certificate as the value. Email+ imports the key into the keystore and selects the certificate as the encryption certificate. If you change the certificate, Email+ imports the new certificate into the keystore and selects the new certificate as the encryption certificate. It leaves the previous certificate in the keystore. If you delete the key-value pair, Email+ leaves the certificate in the keystore. It changes its settings to specify that no certificate is selected as the encryption certificate. Using the Email+ user interface, the device user can: • change the encryption certificate by manually importing one and selecting it for use. • encrypt all emails with the certificate or encrypt a specific email with the certificate. NOTE: Email+ automatically encrypts emails if the emails in the thread are encrypted. For more information about configuring S/MIME for Email+, see S/MIME support in Email+ for Android for identity and encryption on page 47. Default if no key-value is configured: Certificate is not configured.

TABLE 4. KEY-VALUE PAIRS FOR CONFIGURING EMAIL+ FOR ANDROID APPCONNECT APP BEHAVIOR (CONT.)

Key	Value: Enter/Select one	Description
		NOTE: For S/MIME certificates use .DER format instead of normal .PEM format.
email_ signing_ certificate	The certificate setting from the dropdown list	Specifies the certificate to use for signing S/MIME emails. The MobileIron UEM sends the contents of the certificate as the value. Email+ imports the key into the keychain and selects the certificate as the signing certificate. If you change the certificate, Email+ imports the new certificate into the keystore and selects the new certificate as the signing certificate. It leaves the previous certificate in the keystore. If you delete the key-value pair, Email+ leaves the certificate in the keystore and changes its settings to specify that no certificate is selected as the signing certificate. Using the Email+ user interface, the device user can: • change the signing certificate by manually importing one and selecting it for use. • sign all emails with the certificate or sign a specific email with the certificate. For more information about configuring S/MIME for Email+, see S/MIME support in Email+ for Android for identity and encryption on page 47. Default if no key-value is configured: Certificate is not configured.
Manage contacts		
allow_ export_ contacts	• true • false	true: Allows Email+ users to export the Email+ contacts outside of the AppConnect container to the native contacts app. Device users can select the “Sync to personal profile” option, in the settings of the Email+ Contacts app, to export the contacts. Exporting contacts allows users to see the caller ID of incoming calls from phone numbers in the list of corporate contacts. Third-party apps can also access the corporate contacts. If contacts are not exported, users see the caller ID only for personal contacts.

TABLE 4. KEY-VALUE PAIRS FOR CONFIGURING EMAIL+ FOR ANDROID APPCONNECT APP BEHAVIOR (CONT.)

Key	Value: Enter/Select one	Description
		false: Device users cannot export the Email+ contacts. They see the caller ID only for personal contacts. NOTE: When the device is retired or Email+ is retired, the corporate contacts are removed from both Email+ and the native contacts app. Default if no key-value is configured: true.
allow_ export_ contacts_ to_email	• true • false	true: Device users have the option to export contacts as an attachment to an outgoing email. The attachment is an unencrypted VCF (Virtual Contact File) file. false: Device users do not have the option to export contacts as an attachment to an outgoing email. Default if no key-value is configured: true.
allow_ export_ contacts_ to_sdcard	• true • false	true: Device users have the option to export the contacts to the SD card. If the device user chooses the option, Email+ exports the contacts as an encrypted VCF (Virtual Contact File) file. The encrypted VCF file is readable only by Email+ and other secure apps. false: Device users do not have the option to export contacts to the SD card. Default if no key-value is configured: true.
limit_ contact_ export_to	• name_number • all	name_number: Limits the exported contact information to each contact's name and number information. Use this setting to minimize the exposure of corporate data. all: Exports all the contact information. This field is used only if `allow_export_contacts` is set to `true`. NOTE: If you enter a value other than `all` or `name_number`, Email+ uses the value `all`. Default if no key-value is configured: all.
email_safe_	*comma-separated list of safe*	Ensure that there are no spaces before or after the

TABLE 4. KEY-VALUE PAIRS FOR CONFIGURING EMAIL+ FOR ANDROID APPCONNECT APP BEHAVIOR (CONT.)

Key	Value: Enter/Select one	Description
domains	*domains*	comma. Email addresses not in the safe domain list are displayed in red color when composing new emails or creating new calendar invitations in Email+. You may want to use this key-value pair if you company has multiple domains and you want to identify the company domains as opposed to domains that are not company domains. To disable this feature, you can set the value to "*" Example: mycompany.com,mycompany.net,internal.mycompany.com Default if no key-value is configured: Only the domain of the user's email address is considered safe. All other domains will be highlighted in red.
email_alert_unsafe_domains	• true • false	true: Users see an alert if the recipients in an email or calendar invite include addresses that are not in a safe domain. If the key is configured but safe domains are not configured, only the domain of the user's email address is considered safe. Device users have the option to either proceed or cancel sending the email. false: An alert is not displayed for addresses not in a safe domain. Default if key-value is not configured: false.
Syncing		
email_max_sync_period	• 0 • 1 • 2 • 3 • 4 • 5	Specifies the maximum sync period for which emails are downloaded: 0: all emails. 1: emails received over the last one day. 2: emails received over the last three days. 3: emails received over the last seven days. 4: emails received over the last two weeks. 5: emails received over the last one month. Default if no key-value is configured: 0.

TABLE 4. KEY-VALUE PAIRS FOR CONFIGURING EMAIL+ FOR ANDROID APPCONNECT APP BEHAVIOR (CONT.)

Key	Value: Enter/Select one	Description
email_ default_ sync_period	• 1 • 2 • 3 • 4 • 5	Specifies the default period for which emails are downloaded. 1: emails received over the last one day. 2: emails received over the last three days. 3: emails received over the last seven days. 4: emails received over the last two weeks. 5: emails received over the last one month. If configured, all options will be available in Email+. Device users can change the default value. If email_ max_sync_period is also configured, options greater than sync period specified in email_max_sync_period will not be available on the device. Default if no key-value is configured: 2. Additionally, the default value is used in the following cases: • If the value is not 1,2,3,4, or 5. • The value is larger than the value for email_max_ sync_period. After an upgrade, the app retains the default sync period set by the device user.
Maximum size for email attachments		
email_max_ attachment	*A number*	Specifies the maximum size in megabytes of an email that Email+ will send without a warning to the device user. The maximum size includes the body of the email plus its attachments. Allowed values are integers starting with 1. NOTE: If the Exchange server has an email size limit that is less than the limit specified in `email_max_attachment`, the Exchange server does not deliver the email. Default if no key-value is configured: 10 MB.
Maximum size for email attachments		
email_max_ body_size	*A number*	Specifies the maximum limit for email message body size that can be received by the Email+ app. Default: 4 MB

TABLE 4. KEY-VALUE PAIRS FOR CONFIGURING EMAIL+ FOR ANDROID APPCONNECT APP BEHAVIOR (CONT.)

Key	Value: Enter/Select one	Description
Default signature		
email_ default_ signature	*The default email signature*	The value of this key is the default email signature for all emails. However, the device user can override the default email signature at any time. After the user defines the default email signature, Email+ does not use the value in the key, even if you update it. Default if no key-value is configured: Sent by Email+ secured by MobileIron.
SSL		
email_ssl_ required	• true • false	true: Secures communication using HTTPS to the server specified in `email_exchange_host`. Typically, set this field to true unless you are working in a test environment. Default if no key-value is configured: true.
GAL search		
gal_search_ minimum_ characters	*A number*	The minimum number of characters Email+ uses for automatic Global Address List (GAL) lookup in Mail, Calendar, and Contacts. When device users enter the specified number of characters of a name, Email+ searches the GAL, and presents the matches that it finds. IMPORTANT: On your Exchange server, set the minimum number of characters for GAL search to the same value you set for this key. If you do not, GAL search will not work properly in Email+. Default if no key-value is configured: 4.
gal_search_ display_ name	• true • false	true: Enables Display Name in Email+ Settings > Contacts by default. false: Disables Display Name in Email+ Settings > Contacts by default. Default if key-value is not configured: true
contacts_ display_	• first_last • last_first	Sets the default display order for contact names in search results. Device users can change the display

TABLE 4. KEY-VALUE PAIRS FOR CONFIGURING EMAIL+ FOR ANDROID APPCONNECT APP BEHAVIOR (CONT.)

Key	Value: Enter/Select one	Description
order		order in Email+ in Settings > Contacts. The values are case sensitive; enter in lower case. first_last: Contact names in search results are displayed with first name followed by the last name. last_first: Contact names in search results are displayed with last name followed by the first name. Default if key-value is not configured: first_last.
Prompt the device user for password		
prompt_email_password	• true • false	true: Email+ prompts the user for the email password *before* attempting to connect to the email server. false: When Email+ first launches and connects to the email server, Email+ provides the password set in the Email+ configuration to the server. If a password is not configured, an empty string is provided to the server. In this case, after the connection is established, Email+ prompts the user for a password. If the email server limits the number of password attempts, the server counts the first connection as one failed attempt. Set the value of this key to true if the email server allows only a small number of password attempts. Example: If the email server allows only three attempts, setting this value to true ensures that device users get three attempts, not two attempts. NOTE: Kerberos-based authentication is designed to work without user passwords. Since setting `prompt_email_password` to `true` always prompts the user for a password, be sure the value is `false` (the default) if using Kerberos-based authentication. Default if no key-value is configured: false.
email_password	*User's password for the ActiveSync server*	If configured, Email+ does not prompt users for a password. Delete this key if you want the device user to enter the password when using Email+. MobileIron recommends deleting the key.

TABLE 4. KEY-VALUE PAIRS FOR CONFIGURING EMAIL+ FOR ANDROID APPCONNECT APP BEHAVIOR (CONT.)

Key	Value: Enter/Select one	Description
		MobileIron Core You can use the Core variable $PASSWORD$ if you have checked **Save User Password** in **Settings > Users&Devices > Registration**. Core then passes the user's password as the value to the device. WARNING: If you plan to use the $PASSWORD$ variable, be sure to set **Save User Password** to **Yes** before any device users register. If a device user was registered before you set **Save User Password**, Email+ prompts the user to enter the password manually. For Google accounts, as part of a larger setup for synchronizing Google account data, you can use $GOOGLE_AUTOGEN_PASSWORD$. For more information, see "Synchronizing Google account data" section in the *MobileIron Core Device Management Guide* for your device platform. Default if no key-value is configured: Email+ requests device users to enter the password.
Dialing		
show_ dialing_ confirmation	• true • false	true: Users see a confirmation dialog when they tap on a phone number in an email. Tapping on the phone number in the dialog, dials the phone number. Tapping the back arrow cancels the call. false: Users do not see a confirmation dialog. When a user taps on a phone number in Email+, the number is automatically dialed. Default if no key-value is configured: false.
Show pictures		
show_ pictures_ default	• true • false	true: Enables the **Show Pictures** option. Device users automatically see images when opening an email. false: Disables the **Show Pictures** option. Device users must tap **Show Pictures** to view images when opening an email. Device users can override the value you configure by

TABLE 4. KEY-VALUE PAIRS FOR CONFIGURING EMAIL+ FOR ANDROID APPCONNECT APP BEHAVIOR (CONT.)

Key	Value: Enter/Select one	Description
		turning the **Show Pictures** option on or off. NOTE: If you change the key's value, Email+ does not change the **Show Pictures** option until Email+ does a full synchronization. A full synchronization occurs only when you change certain fundamental key-value pairs like `email_address`, or when the device user uninstalls and reinstalls Email+. Default if no key-value is configured: false.
Default network timeout		
default_ network_ timeout	*A positive integer*	The value is represented in seconds. The value overwrites the default connection timeout value for all requests. You may want to configure the key-value pair to manage slow connections with the ActiveSync server or for syncing large folders and emails. If the value is 0, negative, or non-integer, the default value is used. Default if no key-value is configured: 90 seconds.
Troubleshooting		
disable_ analytics	• true • false	true: Disables sending Email+ analytics. false: Enables sending Email+ analytics. Default if no key-value is configured: False.
allow_ logging	• true • false	true: Email+ logs data in the Android logging system.This is useful for problem diagnosis. Typically, you enter true only when working in a test environment. Otherwise, enter false. Default if no key-value is configured: false.
enabled_ features	• export_contacts • skip_empty_links • show_formatting • block_external_gal • lotus	**export_contacts**: If allow_export_contacts key-value pair is set to true and export_contacts value is added to the keyvalue pair then Email+ contacts will be automatically synced to native Contacts app. **skip_empty_links**: Some exchange servers block

TABLE 4. KEY-VALUE PAIRS FOR CONFIGURING EMAIL+ FOR ANDROID APPCONNECT APP BEHAVIOR (CONT.)

Key	Value: Enter/Select one	Description
	• rms_support • multiple_accounts	custom links and the hyperlinks are stripped from the email body. For example, the url mibrowser:// that is used to launch Web@Work and may not become click-able when sent via email. The work around for this problem is, Email+ has additional capability to detect such emails and automatically fetch their body as MIME data that is unmodified by exchange. We recommend that administrators evaluate this capability in their environment by adding "skip_ empty_links" into the "enabled_features" KVP. Fetching MIME data may not work in all configurations. **show_formatting**: Enables the “Always show formatting” option if it was not previously changed manually. **block_external_gal**: Disables contacts search through Email+ contacts for external applications. **lotus**: Enables Lotus server support **rms_support**: Enables fetching, displaying and composing of the protected messages. **multiple_accounts**: Enables secondary email account on the same device.
disabled_ features	• save_attachment • print • show_snippet • personal_events • crl_signature_check	**save_attachment**: Disables the save attachments option. When this option is added the “Save As” button is not available for email attachments. Attachments can still be opened and viewed in Docs@Work or mail application. **print**: Disables the ability to print a message. **show_snippet**: This option removes "Text preview" setting and disables message preview displaying. If this option is enabled the user can set the number of lines visible for message preview, through Email+ app Settings on the mobile device. By default the number of lines set for preview is set to two. **personal_events**:Adding 'personal_events' value to 'disabled_features' KVP removes "Overlay personal events" in Settings by admin.

TABLE 4. KEY-VALUE PAIRS FOR CONFIGURING EMAIL+ FOR ANDROID APPCONNECT APP BEHAVIOR (CONT.)

Key	Value: Enter/Select one	Description
		When 'personal_events' value is removed from 'disabled_features', the "Overlay personal events" appears in Settings and has previous state that user had applied. **crl_signature_check**: Disables CRL check for the email signature certificates.
Microsoft Office 365 authority and resource URL		
modern_ auth_ authority_url	https://login.microsoftonline.com/common	This KVP is added to specify Microsoft Office 365 authority url.
modern_ auth_ resource_url	https://outlook.office365.com	This KVP is added to specify Microsoft Office 365 resource url.
Document classification capabilities		
email_ security_ classification_json	Default value for this key is empty.	Enables the email classification feature. If present, it specifies the list of classification values to be used and all the supported permutations. See *Document classification capabilities* section for more information.
Report phishing		
report_ phishing_ address	email address	Enabling 'Report Phishing' option onView screen in the "More" menu. Phishing email is sent to email address set in value.

App restrictions descriptions for Email+ (Android enterprise)

The app restriction described in the following table are available for Email+ for Android enterprise.

TABLE 5. APP RESTRICTION DESCRIPTION FOR EMAIL+ (ANDROID ENTERPRISE)

Restriction	Value: Enter/Select one	Description
Email address	*Substitution variable for email address*	Required. Defines the email address for the email account. **Core** Typically, enter $EMAIL$. You can also enter combinations of these variables, depending on your ActiveSync server requirements: $USERID$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$ **Cloud** Typically, enter ${userEmailAddress}.
Exchange host	*FQDN of the ActiveSync server or Standalone Sentry*	Required. The fully qualified domain name (FQDN) of the ActiveSync server or Standalone Sentry. Example: mySentry.mycompany.com
Exchange username	*Substitution variable for username*	Required. Defines the username for the email account. **Core** Typically, use $USERID$. If your ActiveSync server requires a domain, use <*domain name*>\$USERID$. Example: mydomain\$USERID$. Depending on your ActiveSync server requirements, you can also use combinations of these variables: $EMAIL$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$. **Cloud** Typically, use ${userEmailAddressLocalPart}. If your ActiveSync server requires a domain, use <*domain name*>\${userEmailAddressLocalPart}. Example: mydomain\${userEmailAddressLocalPart}. Depending on your ActiveSync server requirements, you can use:

TABLE 5. APP RESTRICTION DESCRIPTION FOR EMAIL+ (ANDROID ENTERPRISE) (CONT.)

Restriction	Value: Enter/Select one	Description
		${userEmailAddress}
Email password	*The user's password for the ActiveSync server*	If you provide a password, Email+ does not prompt the device user for the password. NOTE: MobileIron recommends leaving this field blank. **Core only** You can use the variable $PASSWORD$ if you have checked **Save User Password** in **Settings > Preferences**. Core then passes the user's password as the value to the device. If you plan to use the $PASSWORD$ variable, be sure to set **Save User Password** to **Yes** before any device users register. If a device user was registered before you set **Save User Password**, Email+ prompts the user to enter the password manually. Default if restriction is not configured: User is prompted for ActiveSync password.
Device ID **(Core only)**	$DEVICE_UUID_NO_DASHES$	Required. NOTE: The restriction is no longer available with MobileIron Core version 9.4.0.0. The value is automatically set to $DEVICE_SN$.
SSL required	Check box	Select if you want secure communication using https: to the server that you specified for Exchange host. Default: Selected.
Trust all certificates	Check box	Select to allow the app to automatically accepts untrusted certificates. Typically, you select this option only when working in a test environment. Default: Not selected.
Prompt email password	Check box	Select to prompt the user for the email account password when the user attempts to launch Email+. Default: Not selected. If the restriction is not selected, Email+ provides the password to the ActiveSync server when Email+ connects with the server. The ActiveSync server counts the initial connection initiated by Email+ as a

TABLE 5. APP RESTRICTION DESCRIPTION FOR EMAIL+ (ANDROID ENTERPRISE) (CONT.)

Restriction	Value: Enter/Select one	Description
		password attempt. Therefore, MobileIron recommends selecting this restriction if the email server allows only a small number of password attempts.
Email login certificate	**Core** $CERT_ALIAS:*certificate enrollment setting name*$ **Cloud** Certificate setting from the dropdown list	Configure for certificate-based authentication to the ActiveSync server or to Standalone Sentry. **Core** The *certificate enrollment setting name* is the name you gave to the certificate enrollment setting, which is configured in **Configurations > Add New > Certificates or Certificate Enrollment**. **Cloud** The certificate setting is configured in **Configurations > Add > Certificate** or **Identity Certificate**. For certificate-based authentication, the **Authorization Mode** restriction must also be set to **Certificate-based Authentication**.
Email signing certificate	**Core** $CERT_ALIAS:*certificate enrollment setting name*$ **Cloud** Certificate setting from the dropdown list	Specifies the certificate to use for signing S/MIME emails. **Core** The *certificate enrollment setting name* is the name you gave to the certificate enrollment setting, which is configured in **Configurations > Add New > Certificates or Certificate Enrollment**. **Cloud** The certificate setting is configured in **Configurations > Add > Certificate or Identity Certificate**.
Email encryption certificate	**Core** $CERT_ALIAS:*certificate enrollment setting name*$ **Cloud** Certificate setting from the dropdown list	Specifies the certificate to use for encrypting S/MIME emails. **Core** The *certificate enrollment setting name* is the name you gave to the certificate enrollment setting, which is configured in **Configurations > Add New > Certificates or Certificate Enrollment**. **Cloud** The certificate setting is configured in **Configurations**

TABLE 5. APP RESTRICTION DESCRIPTION FOR EMAIL+ (ANDROID ENTERPRISE) (CONT.)

Restriction	Value: Enter/Select one	Description
		> Add > Certificate or Identity Certificate.
Email safe domains	*Comma-separated list of safe domains*	Specifies the safe domains. Example: mycompany.com,mycompany.net,internal.mycompany.com Ensure that there are no empty spaces before and after the comma. Email addresses not in the safe domain list are displayed in red color in Email+. You may want to use this key-value pair if your company has multiple domains and you want to identify the company domains as opposed to domains that are not company domains. To disable this feature, you can set the value to "*" Default if the restriction is not configured: Only the domain of the user's email address is considered safe. All other domains will be highlighted in red.
Allow logging	Check box	Select to allow Email+ to log data in the Android logging system. If selected, the **Send Logs** and **Download Logs** options are available in Email+ in **General Settings** in the Mail app. Device users can send log files via Email+ by the tapping **Send Logs** option or download logs by tapping the **Download Logs** option. The download option is useful if emails cannot be sent due to sync issues. Log data is useful for problem diagnosis. Typically, you select this option in a test environment. Default: Not selected.
Allow export contacts to email	Check box	Select to give device users the option to export contacts as an attachment in an email. Default: Check box is selected.
Allow detailed notifications	Checkbox	Select to allow device users see detailed notifications. The details can include sensitive information such as email subject and body previews, or event titles and times.

TABLE 5. APP RESTRICTION DESCRIPTION FOR EMAIL+ (ANDROID ENTERPRISE) (CONT.)

Restriction	Value: Enter/Select one	Description
		Default: Check box is not selected. Device users see normal notifications.
Show picture by default	Checkbox	Select to allow device users to automatically see images in an email. The setting turns on the **Show Pictures** option on the device. Device users can override the configuration in the UEM by turning the **Show Pictures** option on or off on the device. NOTE: If you change the value, Email+ does not change the **Show Pictures** option until Email+ does a full synchronization. A full synchronization occurs only when you change certain fundamental values like **Email address**, or when the device user uninstalls and reinstalls Email+. Default: Check box is not selected. The Show Pictures option is turned off.
Default signature	Core: $DEFAULT$ Cloud: *The default email signature*	The value entered is the default email signature for all emails. However, the device user can override the default email signature at any time. After the device user defines the default email signature, Email+ does not use the value entered in this field, even if the value is updated. For Core, with $DEFAULT$, the system default is used. If $DEFAULT$ is not configured, a signature is not provided. Default if the restriction is not configured (system default): Sent by Email+ secured by MobileIron.
GAL search minimum characters	*A number*	The minimum number of characters for Email+ to use for automatic Global Address List (GAL) lookup in Mail and Contacts. When entering a name, after the specified number of characters, Email+ starts searching the GAL and presents the matches that it finds. WARNING: On your Exchange server, set the minimum number of characters for GAL search to the same value you

TABLE 5. APP RESTRICTION DESCRIPTION FOR EMAIL+ (ANDROID ENTERPRISE) (CONT.)

Restriction	Value: Enter/Select one	Description
		set for this key. If you do not, GAL search will not work properly in Email+. Default: 4.
Max attachment size (MB)	*A number*	Specifies the maximum size in megabytes of an email that Email+ will send without a warning to the device user. The maximum size includes the body of the email plus its attachments. Allowed values are integers starting with 1. NOTE: If the Exchange server has an email size limit that is less than the maximum size entered, the Exchange server does not deliver the email. Default: 10 MB.
Max mail body size	*A number*	Specifies the maximum limit for email message body size that can be received by the Email+ app. Default: 4 MB
Default sync period	• 1 • 2 • 3 • 4 • 5	Specifies the default period for which emails are downloaded: 1: emails received over the last one day. 2: emails received over the last three days. 3: emails received over the last seven days. 4: emails received over the last two weeks. 5: emails received over the last one month. If configured, all options will be available in Email+. Device users can change the default value. If the Max sync period restriction is also configured, options greater than sync period specified in the restriction will not be available on the device. Default: 2.
Max sync period	• 0 • 1 • 2 • 3 • 4	Specifies the maximum number of days for which emails are downloaded: 0: all emails. 1: emails received over the last one day.

TABLE 5. APP RESTRICTION DESCRIPTION FOR EMAIL+ (ANDROID ENTERPRISE) (CONT.)

Restriction	Value: Enter/Select one	Description
	• 5	2: emails received over the last three days. 3: emails received over the last seven days. 4: emails received over the last two weeks. 5: emails received over the last one month. Default: 0.
Disable Usage Statistics	Checkbox	Disables sending Email+ analytics. Default: Unchecked
Optional Features	• block_external_gal • skip_empty_links • show_formatting • lotus • multiple_accounts	block_external_gal: Disables global address lookup (GAL) of Email+ contacts in the native Contacts app. Configure the value only if the Google account configured for Android enterprise supports GAL. skip_empty_links: Some exchange servers block custom links and the hyperlinks are stripped from the email body. For example, the url mibrowser:// that is used to launch Web@Work and may not become click-able when sent via email. The work around for this problem is, Email+ has additional capability to detect such emails and automatically fetch their body as MIME data that is unmodified by exchange. We recommend that administrators evaluate this capability in their environment by adding "skip_empty_links" into the "enabled_features" KVP. Fetching MIME data may not work in all configurations. show_formatting: Enables the “Always show formatting” option if it was not previously changed manually. lotus: Enables Lotus server support. multiple_accounts: Enables secondary email account on the same device.
Disabled Features	• save_attachment • print • show_snippet • personal_events • crl_signature_check	• **save_attachment**: Disables the save attachments option. When this value is added the "Save as" button is not available for email attachments. Attachments can still be opened in Docs@Work. • **print**: Disables the Print option for email messages.

TABLE 5. APP RESTRICTION DESCRIPTION FOR EMAIL+ (ANDROID ENTERPRISE) (CONT.)

Restriction	Value: Enter/Select one	Description
		• **show_snippet**: This option removes "Text preview" setting and disables message preview displaying. If this option is enabled the user can set the number of lines visible for message preview, through Email+ app Settings on the mobile device. By default the number of lines set for preview is set to two. • **personal_events**: Disables the "Overlay personal events" option in the calendar Settings by admin. • **crl_signature_check**: Disables CRL check for the email signature certificates.
Default Network Timeout	*A positive integer*	The value is represented in seconds. The value overwrites the default connection timeout value for all requests. You may want to configure the key-value pair to manage slow connections with the ActiveSync server or for syncing large folders and emails. If the value is 0, negative, or non-integer, the default value is used. Default: 90 seconds.
Authorization Mode	• Basic Authorization • Certificate-based Authentication	Defines the authentication method to the Exchange ActiveSync service. • Basic Authorization: user name and password • Certificate-Based Authentication: identity certificates For certificate-based authentication, the **Email login certificate** restriction must also be configured. If you have configured Certificate-Based Authentication and there are errors in your configuration, the authentication method defaults to basic. Default: Basic Authorization.
Alert unsafe domains	Checkbox	Select to alert Email+ users if the recipients in an email or calendar invite include addresses that are not in a safe domain. If the restriction is configured, but safe domains (**Email safe domains**) are not configured, only the

TABLE 5. APP RESTRICTION DESCRIPTION FOR EMAIL+ (ANDROID ENTERPRISE) (CONT.)

Restriction	Value: Enter/Select one	Description
		domain of the user's email address is considered safe. Device users have the option to either proceed or cancel sending the email. Default: Not selected. An alert is not displayed for addresses not in a safe domain.
Show dialing confirmation	Checkbox	Select to present a confirmation dialog when users tap on a phone number in an email. Tapping on the phone number in the dialog, dials the phone number. Tapping the back arrow cancels the call. Default if no key-value is configured: Not selected. Users do not see a confirmation dialog. When a user taps on a phone number in Email+, the number is automatically dialed.
Display Order	• first_last • last_first	Sets the default display order for contact names in search results. Device users can change the display order in Email+ in Settings > Contacts. first_last: Contact names in search results are displayed with first name followed by the last name. last_first: Contact names in search results are displayed with last name followed by the first name. Default: first_last.
Use Display Name	• true • false	true: Enables Display Name in Email+ Settings > Contacts by default. false: Disables Display Name in Email+ Settings > Contacts by default. Default: true
Modern Auth Authority URL	*https://login.microsoftonline.com/common*	This is enabled to specify Microsoft Office 365 authority url.
Modern Auth Resource URL	*https://outlook.office365.com*	This is enabled to specify Microsoft Office 365 resource url.
Security classification JSON	Default value for this key is empty.	Enables the email classification feature. If present, it specifies the list of classification values to be used and all the supported permutations.

TABLE 5. APP RESTRICTION DESCRIPTION FOR EMAIL+ (ANDROID ENTERPRISE) (CONT.)

Restriction	Value: Enter/Select one	Description
		See *Document classification capabilities*section for more information.
Allow certificate revocation check	• true • false	This is enabled to check certificate validity. The CRL check for server certificate is performed when **Allow certificate revocation check** is set to **true** and **Trust all certificates** is set to **false**.
Allow files from personal apps	• true • false	Enable this option to allow import or add attachments from personal profile applications. For example, importing certificates from storage or attaching images from photo gallery.
Report phishing	email address	Enable the 'Report Phishing' option on view screen in the "More" menu. The suspicious mail is deleted and sent to a pre-configured (for security review) email address.

S/MIME support in Email+ for Android for identity and encryption

Email+ for Android supports S/MIME (Secure/Multipurpose Internet Mail Extensions). S/MIME allows device users to do the following:

- Digitally sign emails so that the email can be verified by the recipient.
- Verify digitally signed emails.
- Send encrypted emails using the recipient's S/MIME encryption certificate.
- Decrypt S/MIME encrypted emails using a configured S/MIME encryption certificate.

Using these S/MIME features requires that device users import an S/MIME certificate into Email+. You can use one of the following methods to import the S/MIME certificates:

- Importing certificates to Email+ for Android using app-specific configuration.
- Importing certificates using email attachments.

The following describes S/MIME behavior in Email+

- S/MIME behavior in Email+

Importing certificates to Email+ for Android using app-specific configuration

For the best user experience, use app-specific configuration to make Email+ automatically import a signing certificate and encryption certificate. This method does not require user action.

- Configuring S/MIME certificates for Android AppConnect (Core)
- Configuring S/MIME certificates for Android AppConnect (Cloud)
- Configuring S/MIME certificates for Email+ for Android enterprise (Core and Cloud)

Configuring S/MIME certificates for Android AppConnect (Core)

The following describes the configuration in MobileIron Core.

Procedure

1. In the Core Admin Portal, go to **Policy & Configs > Configurations**.
2. Select the AppConnect app configuration for Email+ for Android, and click **Edit**.
3. In **App-specific Configurations,** add the following key-value pairs:
   - email_signing_certificate: From the dropdown list, select the certificate enrollment setting you want to use to sign the email.
   - email_encryption_certificate: From the dropdown list, select the identity certificate setting you want to use to encrypt the email.
4. Click **Save**.

Related topics

The key-value pairs are described in Key-value pairs for configuring Email+ for Android AppConnect app behavior on page 24.

Configuring S/MIME certificates for Android AppConnect (Cloud)

The following describes the configuration in MobileIron Cloud.

Procedure

1. In MobileIron Cloud, go to **Apps > App Catalog** and click on **Email+** for Android (AppConnect**)**.
2. Go to **App Configurations > Email+ Configuration**.
3. Click on the Email+ configuration you want to edit, and click **Edit**.
4. In **AppConnect Certificate Configuration,** add the following key-value pairs:
   - email_signing_certificate: From the dropdown list, select the identity certificate setting you want to use to sign the email.
   - email_encryption_certificate: From the dropdown list, select the identity certificate setting you want to use to encrypt the email.
5. Click **Update** to save the settings.

Related topics

The key-value pairs are described in Key-value pairs for configuring Email+ for Android AppConnect app behavior on page 24.

Configuring S/MIME certificates for Email+ for Android enterprise (Core and Cloud)

The following describes the configuration for Android enterprise. The procedure is applicable in MobileIron Core and MobileIron Cloud.

Procedure

1. Edit the Email+ for Android for Work configuration.
2. Configure the **Email signing certificate** and **Email encryption certificate** restrictions.
3. Save the settings.

Related topics

- Email+ for Android enterprise app configuration and distribution on page 21.
- App restrictions descriptions for Email+ (Android enterprise) on page 37.

Importing certificates using email attachments

Using app-specific configuration you can set up Email+ to automatically import a signing certificate and encryption certificate. Alternatively, users can send themselves the certificate in an email. This section describes how users can email the certificates and import the certificate into the keystore.

Procedure

1. From a computer, users can an email themselves, as an attachment, the certificate that they use for S/MIME on their computers. This certificate must be a PFX file.
2. Users open the email using Email+ on the device, and tapsto open the attachment.
3. Email+ prompts users for the certificate's password.
4. Users enter the certificate's password.
5. Email+ imports the certificate into its keystore.

Related topics

Importing certificates to Email+ for Android using app-specific configuration on page 48.

S/MIME behavior in Email+

Email+ does the following with the S/MIME encryption key it receives:

- Imports the key into the keystore.
- Selects the certificate as the encryption certificate.

If you change the certificate, Email+ imports the new certificate into the keystore and selects the new certificate as the encryption certificate. It leaves the previous certificate in the keystore.

If you remove the restriction, Email+ leaves the certificate in the keystore. It changes its settings to specify that no certificate is selected as the encryption certificate.

Using the Email+ user interface, the device user can:

- change the encryption certificate by manually importing one and selecting it for use.
- encrypt all emails with the certificate or encrypt a specific email with the certificate. Note that Email+ automatically encrypts emails if the emails in the thread are encrypted.

Note The Following:

- To send an encrypted email, a user needs the recipient's public key. If you provide users' public keys in the Active Directory, Email+ uses global address lookup to retrieve a public key as needed.
  Another way for a user to have the public key of another user is possible, but more limiting. Specifically, if a user receives a signed email, and the signing certificate is the same as the encryption certificate, Email+ now has the sender's public key. The user can now send an encrypted email to the user who sent the signed email.
- Make sure users' encryption certificates are the same on all devices.
  A user needs his private key and certificate to read encrypted emails. The encryption key and certificate must be the same on all email clients using S/MIME, including desktop email clients.
- When an encryption key/certificate is renewed, the existing email on a device cannot be decrypted unless the original key certificate is available. Keep a backup copy of the encryption key and certificate or consider using a third-party escrow service.
- To restore an encryption key and certificate from a backup, the user can send himself the key/certificate as an email attachment, as described in the following section.

Email attachment download to secure SD card folder

Email+ for Android allows the device user to download email attachments to a secure folder. The stored attachment is encrypted. The device user can view the attachment later using a secure app such as Docs@Work. Only secure apps can view the attachment; apps that are not AppConnect-enabled cannot access the attachment.

Email+ automatically removes emails older than the number of days that the device user specifies in the Email+ settings from the device. This feature allows the device user to securely save and view the attachment even after the email has been removed.

When the device user downloads an email attachment, it is saved in the following folder:

```
sdcard/Download
```

Document classification capabilities

Document classification capabilities provides the ability to manage protective markings to emails. Email+ lists user interface fields to the user when viewing messages, replying to messages, or composing new messages.

The messages that are sent through Email+, adds the markings to the subject line, header, and optionally on the top and the bottom of message body. Email+ supports Protective Marking Standard for the Australian Government (2012 and 2018 versions) and Generic.

- Classification - To identify the overall sensitivity of the message
- Distribution Limiting Markers - To limit the distribution

Email classification JSON has two major parts:

- Scheme
- Values

Scheme

Scheme includes properties to define email classification behavior. The following table describes the general properties:

Property	Description
topOfBody	Email classification marker to add text at the top of a classified message. Can include sec, dlm, $title$, $caveat$ variables. Default value for AU_2018: {"default" : "sec, $caveat$, dlm", "noSec" : "dlm, $caveat$", "noDlm" : "sec, $caveat$", "noCaveat" : "sec, dlm" } Default value for AU_2012: {"default" : "sec, dlm", "noSec" : "dlm", "noDlm" : "sec"}. To remove the header and footer the "topOfBody" and "bottomOfBody" value should be set to an empty value: {} or {"default" : ""}.
bottomOfBody	Email classification marker to add text at the bottom of a classified message. Can include sec, dlm, $title$, $caveat$ variables. Default value for AU_2018: {"default" : "sec, $caveat$, dlm", "noSec" : "dlm, $caveat$", "noDlm" : "sec, $caveat$", "noCaveat" : "sec, dlm" }. Default value for AU_2012: {"default" : "sec, dlm", "noSec" : "dlm", "noDlm" : "sec"}. To remove the header and footer "topOfBody" and "bottomOfBody" values should be set to an empty value: {} or {"default" : ""}.
bodyTextColor	Email classification marker to apply color to the the text in "topOfBody" and "bottomOfBody" text in #AARRGGBB or #RRGGBB format. Text value. Default value: "#FFFF0000". Examples: #ff0000, #a2ff230c;
default	Email classification marker to apply a default value. Format: { "sec" : "existing sec value", "dlm" : "existing dlm value" }. Should be one of the markers defined in "values". If value is not set or marker does not exists - "" will be used.

Property	Description
textAlert	Warning message to display when a user is trying to send message without selected classification. Text value. Default: "Classification is required".
textRequired	Warning text to display in "#FFFF0000" color instead of classification marking while classification is not selected. Text value. Default: "Classification is required".
lockDlm	When set to "true" only markers with the same dlm as in original message should be available to select. Boolean value. Default: "false".
multiselectField	The fields from "multiselectField" JSON array supports multiple selections. The default value is empty. When multiple values are selected $field$ notation is replaced with the appropriate values separated with "multiselectSeparator" text. "multiselectSeparator" default value is ", ".

Version properties

Version properties defines which classification type will be used. When **version** is not defined **Generic** classification will be used.

- **version** - Defines email classification type.
  - **Supported version**: "**AU**" or "**AU_2012**" for Email Protective Marking 2012 Standard and "**AU_2018**" for Email Protective Marking 2018 Standard for the Australian Government.
- **versionValue** - Defines version number used for sending classification.
  - **Default value for "AU" and "AU_2012"**: "VER=2012.3,NS=gov.au". With "AU_2018" "VER=2018.1,NS=gov.au" is used.

Values

Values is used to define a list of Email classification markings. One of the following values must be presented in values field, that is they are optional in place where we substitute them (Subject, Body, Mime Headers and so on).

- SEC - single SEC or array of SEC values.
- DLM - single DLM or array of DLM values. With AU_2018 version should be used for the ACCESS(Information management marker) values.
- CAVEAT - single CAVEAT or array of CAVEAT values.

One of "sec" or "dlm" must be presented in "values" item. When "sec" or "dlm" value is array all the permutations of "sec" + "dlm" should be used. Priorities are in ascending order from top to bottom, from left to right.

JSON is considered invalid and classification markers are not displayed when the values for SEC or DLM is empty or duplicated.

When values item defines a single classification marking that the next properties can be set such as:

- title - defines text to use for marking title in the classifications picker when the classification is a single value.

Valid classification for AU 2018 contains only:

- sec, caveat*, access*
- sec, caveat*
- sec, access*
- sec

Where (*) is for one or several items)

A regular expression for AU 2018 Subject

[(SEC=<securityClassification>)(, CAVEAT=<caveatType>:<caveatValue>)*(, EXPIRES=(<genDate>|<event>), DOWNTO=(<securityClassification>)?(,ACCESS=<InformationManagementMarker>)*]

Header:

X-Protective-Marking: VER=<ver>, NS=gov.au, (SEC=<securityClassification>)(, CAVEAT=<caveatType>:<caveatValue>)*(, EXPIRES=(<genDate>|<event>), DOWNTO= (<securityClassification>)?(, ACCESS=< InformationManagementMarker>)*(, NOTE=<comment>)?, ORIGIN=<authorEmail>

The following is example for the Australian classification:

```
{
"scheme" : {
"topOfBody" : {"default" : "$sec$, $caveat$, $dlm$", "noCaveat" : "$sec$, $dlm$", "noDlm" :
"$sec$, $caveat$", "onlySec" : "$sec$"},
"bottomOfBody" : {"default" : "$sec$, $caveat$, $dlm$", "noCaveat" : "$sec$, $dlm$", "noDlm"
: "$sec$, $caveat$", "onlySec" : "$sec$"},
"bodyTextColor" : "#ffff0000",
"version" : "AU_2018",
"versionValue" : "VER=2018.1,NS=gov.au",
"default" : { "sec" : "OFFICIAL" },
"lockDlm" : "true",
"multiselectField" : ["dlm"],
"multiselectSeparator" : ", "
},

"values" : [
{
"sec": "UNOFFICIAL",
"title" : "Unofficial"
},
{
"sec": "OFFICIAL",
"title": "Official"
},
{
"sec": "OFFICIAL:Sensitive",
"dlm": ["","Personal-Privacy","Legal-Privilege","Legislative-Secrecy"]
},
{
"sec": "PROTECTED",
"dlm": ["","Personal-Privacy","Legal-Privilege","Legislative-Secrecy"],
"caveat": ["","SH:Cabinet"]
}
]
}
```

For Generic classification the following properties must be defined:

- subjectSuffix - suffix that is appended to subject when sending an email. Can include sec, dlm variables. Format: {"default" : "sec, dlm", "noSec" : "dlm", "noDlm" : "sec"}. Default: {"default" : "[sec]"}.
- xHeaderName - email header that is added to an email. On reply and forward will overwrite the original header if its protection header cannot be parsed. Text value. Default: "x-classification".
- xHeaderValue - value for "xHeaderName". Can include sec variable. Format: {"default" : "sec, dlm", "noSec" : "dlm", "noDlm" : "sec"}. Default: {"default" : "[sec]"}.

The following is an example of Generic classification:

```
{
"scheme" : {
"subjectSuffix" : {"default" : "[$sec$]"},
"topOfBody" : {"default" : "$sec$, $dlm$", "noSec" : "$dlm$", "noDlm" : "$sec$"},
"xHeaderName" : "x-classification",
"xHeaderValue" : {"default" : "[$sec$]"},
"default" : { "sec" : "-Public-" }
},

"values" : [
{
"sec" : "-Public-",
"title" : "All external email"
},
{
"sec" : "-Internal-",
"title" : "BB&T Internal email"
},
{
"sec" : "-Secret-",
"title" : "BB&T Secret email"
}
]
}
```

For more information on JSON samples, see the Android Email+ 3.x Security Classification Guide KB article.

Configuring personal events calendar

The Email+ Android app now displays personal events calendar on work calendar in read-only mode. All personal Calendars are added to Email+ app. The users can select which calendars they want to be displayed inside the navigation drawer. Different calendars are highlighted in different colors for easy identification.

The personal_events restriction for Android enterprise is available only when it is configured either in native calendar or an app in Android enterprise container. Calendar events that are configured in personal space are not displayed on Email+ in Android enterprise.

The following personal events are supported on Email+ Calendar:

- Events (Invited/Created)
- Holidays
- Birthdays
- Goals

NOTE: Reminders (from Google Calendar) and tasks (from Samsung) are not added to events, also no notifications appear for personal events from Email+.

The **Overlay personal events** option is enabled in general Calendar Settings. It's regulated with check box. When user turns on option for the first time, Email+ displays alert requesting permissions to access calendar data.

The ability to add personal events is enabled by default, however the admin can disable it by adding the value **personal_events** to **disabled_features**.

Rights Management System for Android Overview

The Rights Management System (RMS) enables you to share encrypted mails to protect the content that is shared over email when using Microsoft Mail Exchange server.

When enabled the sender can control the distribution of the content shared over the mail. A rights managed email message is used to protect email content from inappropriate access, use, and distribution.

A rights policy template specifies whether a user can edit, forward, reply, reply all, print, extract (copy), export (remove protection), or programmatically access the content in the rights-managed email message.

Rights Management is supported in EAS versions: 14.1, 16.0, 16.1.

The admin can apply the following options to secure mail exchange as indicated by the **RightsManagementLicense** element included in the response. The RightsManagementLicense include:

- **ContentExpiryDate** - specifies the expiration date for the license (set to "9999-12-30T23:59:59.999Z" if the rights management license has no expiration date set).
- **ContentOwner** - specifies the email address of the content owner.
- **EditAllowed** - specifies if the content of the original email can be modified by the user when the user forwards, replies, or replies all to the email message.
- **ExportAllowed** - specifies if the IRM protection on the e-mail message can be removed by the user. The user can remove the IRM protection of the original message's content in the outgoing message when the user forwards, replies, or replies all to the original e-mail message;
- **ExtractAllowed** - specifies if the user can copy content out of the e-mail message (the content of the e-mail message can be cut, copied, or a screen capture can be taken of the content).
- **ForwardAllowed** - specifies if the user can forward the e-mail message.
- **ModifyRecipientsAllowed** – specifies if the user can modify the recipient list.
- **Owner** - value of TRUE indicates that the authenticated user has owner rights on this message. This element is used for information presentation purposes only.
- **PrintAllowed** - specifies if the email can be printed by the user.
- **ProgrammaticAccessAllowed** - specifies if the contents of the e mail message can be accessed programmatically by third party applications.
- **ReplyAllAllowed** - specifies if the user can reply to all the recipients of the original e-mail message.
- **ReplyAllowed** - specifies if the user can reply to the e-mail message.
- **TemplateDescription** - This element is used for informational presentation purposes only.
- **TemplateID** - It contains a string that identifies the rights policy template.
- **TemplateName** - specifies the name of the rights policy template.

For more information on **To create a new Azure information protection template**, see Microsoft documentation

Setting permissions on an email

The permissions for email protection can be set on MobileIron Email+ Android app.

Setting permissions on Email+ Android app

Using the Email+ app to set email permissions.

Procedure

1. In the Email+ app, click on the compose mail icon.
2. From the **context menu** select **Protect** option.
3. In the **Set permissions** window, select permission you want to apply to the mail from the drop-down menu.
4. Click **Ok**.

Result: The selected permission is applied to the mail.

Secondary email accounts

Email+ Android supports secondary email accounts on a single device. The administrator can sync all the accounts for which they need to receive mail and calendar notifications. You can have different account settings for secondary account.

When secondary email account is configured, you can switch between accounts in Navigation drawer. The mails from selected email account is displayed on the top of the navigation drawer. The Calendar events for secondary accounts are displayed in different colors.

Adding a secondary account

In addition to your primary mail account you can configure and customize a secondary account on the same device using key-value pairs. To add and customize the secondary email account, add the prefix acc2_ to a key. The prefix acc2_ indicates that the key-value pair is applied only to the secondary account. Key-value pairs that do not need to be specifically configured for the secondary account are generally applicable to both the primary and secondary accounts.

The following are account specific key-values pairs supported for secondary account for Android AppConnect version:

- acc2_email_address
- acc2_email_device_id
- acc2_email_exchange_host
- acc2_email_exchange_username

Optional KVPs:

- acc2_email_password
- acc2_email_ssl_required
- acc2_email_trust_all_certificates
- acc2_email_login_certificate
- acc2_email_signing_certificate
- acc2_email_encryption_certificate
- acc2_email_default_signature
- acc2_email_max_attachment
- acc2_email_max_sync_period
- acc2_email_default_sync_period
- acc2_eas_min_allowed_auth_mode
- acc2_prompt_email_password
- acc2_email_login_certificate_MI_CERT_PW

To configure secondary accounts on Android enterprise, the following restrictions should be configured in **Apps > App Catalog > Configuration > Additional accounts** section:

- Email address
- Device ID
- Exchange host
- Exchange username

Optional Restrictions:

- Email password
- Email login certificate
- Email signing certificate
- Default signature
- Max attachment size(Mb)
- Max sync period
- Default Network Timeout
- Authorization Mode

Removing secondary account

To remove secondary account from your device:

- **For Android AppConnect** remove the “multiple_accounts” value from “enabled_features”.
- **For Android enterprise** remove "multiple_accounts" restriction from “Optional items”.