ivanti

Email Plus Android Guide

ivanti

CONTENTS

1. Ivanti Email+ 5.0.0 - 5.5.0 for Android Guide

September 2026

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

[New features summary]

[Revision history]

2. Revision history

Date	Revision
September 03, 2026	Updated for Email+ 5.5.0 release.
April 29, 2026	Updated for Email+ 5.4.0 release.
January 21, 2026	Updated for Email+ 5.3.0 release.
October 02, 2025	Updated for Email+ 5.1.0 release.
August 27, 2025	Updated for Email+ 5.0.0 release.

3. New features summary

These are cumulative release notes. If a release does not appear in this section, then there were no associated new features and enhancements.

Ivanti Email+ 5.5.0 New features summary

Ivanti Email+ app features and enhancements:

- **Support for Android 17**: The Email+ app now supports Android 17.
- **Graph API Support for Delegated/Shared Mailbox**: Delegated mailbox, Shared mailbox, features now use Microsoft Graph API, ensuring continued functionality after the planned deprecation of Exchange Web Services (EWS) in Microsoft 365.
- **Graph API Support for Delegated/ Shared Calendar**: Delegated calendar and Shared calendar features now use Microsoft Graph API, ensuring continued functionality after the planned deprecation of Exchange Web Services (EWS) in Microsoft 365.

Ivanti Email+ administrator features and enhancements

- **Migration from Exchange Web Services to Microsoft Graph API: Email+ is transitioning Microsoft 365 connectivity from Exchange Web Services (EWS) to the Microsoft Graph API. Users can continue to use core email and calendar features with Microsoft 365 accounts. However, delegated and shared account functionality may behave differently under Microsoft Graph due to Microsoft Graph API capabilities, permissions, and service-specific requirements.**
- **New restriction added for Microsoft Graph Support**: A new restriction, **CNS Host for Graph**, has been added with the value **<notification_server_host>** to enable delivery of notifications for delegated mailbox and calendar activities through Microsoft Graph..
  To migrate to Microsoft Graph, configuring the existing **Exchange Host for Graph** app restriction with the value **graph.microsoft.com** and enabling the **graph_api** feature flag in **Optional Features** is mandatory. Both settings are required for delegated and shared mailbox and calendar functionality to use Microsoft Graph. For more information, see **App restrictions descriptions for Ivanti Email+ (Android Enterprise)**

Ivanti Email+ 5.4.0 New features summary

Ivanti Email+ app features and enhancements:

- **Integrated Microsoft Teams into Email+ calendar**: The Email+ Calendar app is is integrated with Microsoft Teams, that allows the users to insert Microsoft Teams meeting links directly into Event Notes without switching to the Microsoft Outlook or the Teams app. This is applicable only for Microsoft Office 365 server, as it uses graph API. For more information, see **Microsoft Teams Integration in Email+ Calendar**.
- **Added improvements to the Shared Mailbox**: The following improvements are made for the Shared Mailbox:
  - Improved the logic of adding or using Shared and Delegated mailboxes and sharing permissions to folders.
  - Email+ app now shows Delegated and Shared mailbox as one category called "Delegated Mailboxes".
  - Drafts folder is only displayed when mail drafts are available created.

Ivanti Email+ administrator features and enhancements

- **New value added**: A new value **microsoft_teams_meetings** added to **Optional Features** restriction to enable integration between Microsoft Teams and Email+ Calendar.
- **New restriction added**: A new restriction, **Exchange host for Graph**, has been added with the value 'graph.microsoft.com' to enable the Microsoft Teams feature.
  When configuring Microsoft Graph, administrators must use graph.microsoft.com as the default Exchange host. Users may need to use different endpoints depending on their national cloud deployments,. For further details and a comprehensive list of supported Microsoft Graph endpoints, please refer to the official documentation: **Supported Microsoft Cloud Endpoints**.
  For more information, see **App restrictions descriptions for Ivanti Email+ (Android Enterprise)**

Ivanti Email+ 5.3.0 New features summary

Ivanti Email+ app features and enhancements:

- **Enhanced large attachment download with MIME**: When a single attachment download fails because it exceeds 10 MB, an alert now appears with a **Download MIME** option. This allows you to download the full email along with all attachments. Additionally, the **Download All** button always downloads the complete MIME file, regardless of attachment size, ensuring access to large files without interruption. For more information, see **Downloading large email attachments**.

Ivanti Email+ administrator features and enhancements

This release does not include new administrator features and enhancements.

Ivanti Email+ 5.1.0 New features summary

Ivanti Email+ app features and enhancements

- **ActiveSync 16 updated**: ActiveSync 16 is now enabled by default. For more information, see ActiveSync16 for Android devices.
- **Support for attachments added to the Calendar events**: You can now add, remove, and view attachments to the Calendar event in the Email+ app. This feature is supported only when EAS16 and EWS are enabled. For more information, see Calendar attachments.

Ivanti Email+ administrator features and enhancements

- **eas_16 enabled by default**: The **eas_16** value is now enabled by default. The **eas_16** value is removed from **Optional features** and added to **Disabled features** restriction.

Ivanti Email+ 5.0.0 New features summary

Ivanti Email+ app features and enhancements

- **Migration from Azure Active Directory Authentication Library (ADAL) to Microsoft Authentication Library** (**MSAL**): The Email+ Android app migrates from ADAL to MSAL to support Microsoft Conditional Access.

Ivanti Email+ administrator features and enhancements

- **Replaced email exchange username with email address restriction**: The Email+ app now uses **email address** restriction for authentication instead of **email exchange username** restriction. This is updated because the Microsoft Azure Active Directory Authentication Library (ADAL) is now deprecated and replaced with Microsoft Authentication Library (MSAL). Use same values for both **email address** and **email exchange username** restrictions when upgrading to Email+ 5.0.0.
- **New restrictions added**: New restriction **MSAL Client Id** and **MSAL Resource Scope** are added:
  - **MSAL Client Id**: Replaces the default application ID used by Microsoft Authentication Library (MSAL) with a custom value.
  - **MSAL Resource Scope**: Defines the resource scopes required by Microsoft Authentication Library (MSAL) to acquire access tokens for protected resources.

For more information, see App restrictions descriptions for Ivanti Email+ (Android Enterprise).

4. Overview of Ivanti Email+ for Android

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

About Ivanti Email+ for Android

About configuring Ivanti Email+ for Android

What users see in Email+ for Android

4.1. About Ivanti Email+ for Android

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+ can be downloaded using enterprise PlayStore. Email+ for Android, like all secure apps for Android, can only be distributed as an in-house app. When you distribute Email+, distributing the Secure Apps Manager is required.

You can make Email+ for Android available to device users as an in-house app in the App Catalog in the Ivanti EPMM Admin and Ivanti Neurons for MDM (under Apps > App Catalog > In-House). The device user launches Mobile@Work for Android to discover and install Email+, where it will appear under Secure Apps within the Mobile@Work app.

> Android AppConnect is deprecated and not supported on Email+.

Ivanti 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 (Ivanti EPMM).
  - Users are removed from app distribution (Ivanti Neurons for MDM).
  - The app is uninstalled from the device.

Ivanti Email+ for AppStation

Email+ is available as an Android AppStation app for Ivanti Neurons for MDM only. AppStation is specifically designed as the UEM client for a MAM-only deployment with Ivanti Neurons for MDM. In a AppStation MAM-only deployment, only apps available through AppStation are managed. The following types of apps are supported:

- AppConnect apps (wrapped with Secure Apps Manager for AppStation)
- Non-AppConnect apps (in-house or from the Google Play Store)
- Device users must have a valid user ID and password to access content sites

Where to find Ivanti Email+ for Android

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

4.2. About configuring Ivanti Email+ for Android

You configure settings for Email+ in the UEM platform. Because the 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.

4.3. 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.
- Notes: Enables users to manage, synchronize and create new Exchange notes

> 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.

> User can not open attachments from Compose or Edit screen in Android Enterprise, but can only manage them to add new or remove existing attachment.

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.

5. Configuring Ivanti Email+ for Android Enterprise

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

5.1. Before you configure Ivanti Email+ for Android Enterprise

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

- Requirements for configuring Ivanti Email+ for Android Enterprise
- Recommendations for configuring Ivanti Email+ for Android Enterprise

Requirements for configuring Ivanti Email+ for Android Enterprise

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

- Your unified endpoint management (UEM) platform must be set up for Android Enterprise. Your UEM is either Ivanti Neurons for MDM or Ivanti EPMM.
  - **Ivanti EPMM**: See the *Ivanti EPMM Device Management Guide for Android for Work*.
  - **Ivanti Neurons for MDM**: See the Ivanti Neurons for MDM online **help** documentation.
- Your setup must also include Standalone Sentry configured for ActiveSync. For information on how to set up Standalone Sentry, see the Ivanti Sentry Guide for Ivanti EPMM and Ivanti Sentry Guide for Ivanti Neurons for MDM for your UEM deployment.
- Ensure that the appropriate ports are open.
  - **Ivanti EPMM**: See the Ivanti On-Premise Installation Guide for Ivanti EPMM and Enterprise Connector for information on required ports and firewall rules associated with Standalone Sentry and different backend resources.
  - **Ivanti Neurons for MDM**: See the Ivanti Neurons for MDM 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.
  - **Ivanti EPMM**: For information about configuring certificates in Ivanti EPMM, see the “Managing Certificates and Configuring Certificate Authorities” section in the Ivanti EPMM Device Management Guide.
  - **Ivanti Neurons for MDM**: Ensure the certificate configuration is distributed to the same group as the Email+ app.

Recommendations for configuring Ivanti Email+ for Android Enterprise

Ivanti, Inc recommends the following:

- Standalone Sentry should use a trusted CA certificate.
- If your UEM is Ivanti EPMM, and if the Standalone Sentry self-signed certificate is changed, you must do the following additional setup in Ivanti EPMM:
  - In the Services > Sentry page, for the Standalone Sentry, click the View Certificate link. This makes the Standalone Sentry’s certificate known to Ivanti EPMM.

5.2. Ivanti Email+ for Android Enterprise app configuration and distribution

Navigate to your UEM platform, add the Email+ app for Android Enterprise from Google Play, and configure it so that Android Enterprise devices can use it.

- Configuring app restrictions and distribution in Ivanti EPMM
- Configuring app restrictions and distribution in Ivanti Neurons for MDM

Configuring app restrictions and distribution in Ivanti EPMM

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

Procedure

1. In the Ivanti EPMM Admin Portal, go to Apps > App Catalog.
2. Click Add+.
3. Click Google Play.
4. For Application Name, enter Email+.
5. Click Search.
6. Select Email+ in the search results.
7. Click Next.
8. (Optional) Update the following information:
    1. Edit the description for the app.
    2. 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.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. 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 make sure to 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 **In the Configuration Choices section, add a new configuration or edit the default configuration. If you add a new custom configuration make sure to 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.**

Related topics

See **App restrictions descriptions for Ivanti Email+ (Android Enterprise)** for a description of the fields.

Configuring app restrictions and distribution in Ivanti Neurons for MDM

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

Procedure

1. In the Ivanti Neurons for MDM 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.
    1. Edit the Name and Description of the settings if necessary.
    2. Install on Device: Enable if you want to require that the app is installed on devices.
    3. Silently install on Samsung KNOX and Zebra devices: This option is not applicable to Android Enterprise apps.
    4. Do not show app in end user App Catalog: Select if you do not want the app displayed in the 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 Ivanti Email+ (Android Enterprise)** for a description of the restrictions.

5.3. Configuring Email+ with Ivanti Tunnel for Android Enterprise

Configure Email+ with Ivanti Tunnel to setup access to Exchange server through Exchange Web Services (EWS) protocol and to support Email+ configuration when VPN access is required.

Before you begin

- Configure Email+ Android Enterprise
- Add Local certificate authority (CA), see Configuring Ivanti EPMM as an independent root CA (Self-Signed) section in the Ivanti EPMM Device Management Guide for Android and Android Enterprise Devices

The following steps describe how to configure AppTunnel with Standalone Sentry.

Procedure

1. In the Ivanti EPMM Admin Portal, go to **Services > Sentry > Add New > Standalone Sentry**.
2. In the New Standalone Sentry window, enter the **Sentry Hostname / IP** name.
3. Select the **Enable AppTunnel** check box, and deselect **Enable ActiveSync** .
   If Enable AppTunnel is enabled, other Sentry services such as **Kerberos Proxy** and **Email+ Notification Service** are disabled.
4. In the **Device Authentication Configuration** section:
   - Select **Identity Certificate** from the drop-down menu.
   - Upload Local CA to the **Trusted Root Certificate Upload** field.
5. In the **AppTunnel Configuration** section, add **<IP_ANY>** as AppTunnel service in **Services.**
6. In the Ivanti EPMM Admin Portal, go to **Services > Sentry > Standalone Sentry** and click on **Manage Certificate** for configuring Standalone Sentry.
7. In the **Manage Certificate** window, from the **Certificate Options** drop-down menu select **Upload Certificate** to add public certificate to Standalone Sentry.

Configuring Ivanti Tunnel for Email+ Android Enterprise

The following steps describe how to configure Ivanti Tunnel rules for Email+.

Procedure

1. In the **Ivanti EPMM Admin Portal**, go to **Apps > App Catalog > +Add.**
2. Select the **Ivanti Tunnel** app for Android Enterprise and click **Edit**.
3. Scroll down to **Configuration Choices**.
4. Click **Add+** to add a new Tunnel configuration. In the **Default Configuration for Ivanti Tunnel** section update the following restrictions.

Restriction	Description
Sentry Server	Specify the FQDN for the Sentry server that is configured with the IP_ANY service. Configure Sentry Server if you selected one of the following Tunnel profile modes: • Sentry Profile Only • Sentry + Access Profile
Added Routes	Enter the network routes that are allowed through Tunnel. Use CIDR format. Each entry in the list is separated by a semicolon (;). IPv4 only. This enables split tunneling where only specific traffic can be taken through Tunnel. The routes configured only impact apps that use Tunnel. Example: 10.0.0.0/8;101.210.48.9/32
ClientCertAlias	This is the certificate alias set up with local certificate from the same CA that was uploaded to sentry. The value is $CERT_ALIAS:<name-of-SCEP>$ where <name-of-SCEP> is the Certificate Enrollment setting configured in Ivanti EPMM UI. Example: $CERT_ALIAS:scepIdentityCert$ where scepIdentityCert is the name of the SCEP configured in Ivanti EPMM.
Disable Pinning	Check **Disable pinning**

After configuring and successfully connecting the Email+ app with Ivanti Tunnel, the Tunnel record appears in **Apps > App Tunnels**.

6. Additional configurations using key-value pairs

The following describe how to customize Email+ app behavior:

6.1. Key-value pairs for Ivanti Email+ (Android AppConnect)

Key-value pairs for configuring Email+ for Android AppConnect app behavior 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+.

Key-value pairs marked as Ivanti EPMM only are not applicable to Ivanti Neurons for MDM. For Ivanti Neurons for MDM deployments, these variables are either provided as fields in Ivanti Neurons for MDM or are set automatically and do not require action from the administrator.

See **Configuring Email+ for Android AppConnect in Ivanti Neurons for MDM** for a description of the fields in Ivanti Neurons for MDM.

- Some values can use the UEM variables, such as $EMAIL$ for Ivanti EPMM and $ for Ivanti Neurons for MDM. The 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.
- Before configuring new key-value pairs, the user should update to the latest Email+ application and then the administrator should configure the new key-value pairs.

> When there are multiple values available within a KVP, the different features should be specified as a list of Comma Separated Strings, with or without a space. A semicolon between them will not work.

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**
- **SSL**
- **GAL search**
- **Prompt the device user for password**
- **Show pictures**
- **Default network timeout**
- **Troubleshooting**

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) **Ivanti EPMM** Typically, this field uses the Ivanti EPMM variable $EMAIL$. You can also use combinations of these Ivanti EPMM variables, depending on your ActiveSync server requirements: $USERID$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$. **Ivanti Neurons for MDM** Typically, this field uses the Ivanti Neurons for MDM variable $. You can also use combinations of the user attribute variables, depending on your ActiveSync server requirements. The user attribute variables are listed in Ivanti Neurons for MDM in Admin > Attributes.
email_device_id	*The device ID that the ActiveSync server uses for the device.*	**Ivanti EPMM** Always use the Ivanti EPMM variable $DEVICE_UUID_NO_DASHES$. **Ivanti Neurons for MDM** Always use the Ivanti Neurons for MDM variable $.
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*	**Ivanti EPMM** Typically, you use the Ivanti EPMM variable $USERID$. If your ActiveSync server requires a domain, use *<domain name>*\$USERID$. For example: mydomain\$USERID$. You can also use combinations of these Ivanti EPMM variables, depending on your ActiveSync server requirements: $EMAIL$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$. **Ivanti Neurons for MDM** Typically, you use $. If your ActiveSync server requires a domain, use <domain name>\$. Example: mydomain\$. Depending on your ActiveSync server requirements, you can use $

Key	Value: Enter/Select one	Description
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 UEM.		
email_login_certificate	The certificate setting from the dropdown list	The 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, Ivanti EPMM 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. 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. 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 Ivanti EPMM Admin Portal. • Certificates configured for encrypting or signing S/MIME emails are self-signed or not derived from a well-known certificate authority. You specify these certificates in the keys email_encryption_certificate and email_signing_certificate.

Key	Value: Enter/Select one	Description
		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 corresponding protocol. Enables Oauth 2.0 authorization. Modern Auth Authority URL and Modern Auth Resource URL: when configured through sentry uses the following values: • **modern_auth_authority_url**: https://<SentryHostname>/proxyservice • **modern_auth_resource_url**: https://<SentryHostname> 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 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. Email+ automatically encrypts emails if the emails in the thread are encrypted. For more information about configuring S/MIME for Email+, see **SMIME support in Email+ for Android for identity and encryption**. Default if no key-value is configured: Certificate is not configured. 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 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.

Key	Value: Enter/Select one	Description
		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 **SMIME support in Email+ for Android for identity and encryption**. Default if no key-value is configured: Certificate is not configured.
email_signing_digest	• SHA-1 • SHA-256 • SHA-384 • SHA-512	Configures signature algorithm. The default value is set to SHA-1. The restriction is empty by default. If there is no value or invalid value set, then SHA-1 is used.
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. false: Device users cannot export the Email+ contacts. They see the caller ID only for personal contacts. 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.

Key	Value: Enter/Select one	Description
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. 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_domains	*comma-separated list of safe domains*	Ensure that there are no spaces before or after the 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.
email_default_sync_period	• 0 • 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.

Key	Value: Enter/Select one	Description
		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. Also applicable for Delegated Mailbox. Allowed values are integers starting with 1. 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
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+.
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. 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.

Key	Value: Enter/Select one	Description
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_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. 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. 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+. Ivanti, Increcommends deleting the key. **Ivanti EPMM** You can use the Ivanti EPMM variable $PASSWORD$ if you have checked Save User Password in Settings > Users&Devices > Registration. Ivanti EPMM 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. 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 Ivanti EPMM Device Management Guide for your device platform.

Key	Value: Enter/Select one	Description
		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 turning the Show Pictures option on or off. 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	if the highest ActiveSync version for the server is 16.1 or higher, enable Email+ to sync via EAS 16.1 version.if the highest ActiveSync version for the server is 16.0, enable Email+ to sync via EAS 16.0 versionif the highest ActiveSync version for the server is lower than 16.0,

Key	Value: Enter/Select one	Description
	• show_formatting • block_external_gal • rms_support • multiple_accounts • allow_shortcuts • eas_16 • calendar_delegation • delegated_shared_mailbox	then it works as per the current settings. **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 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 ata 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. **rms_support**: Enables fetching, displaying and composing of the protected messages. **multiple_accounts**: Enables secondary email account on the same device. **allow_shortcuts**: Enables the user to create shortcuts for Calendar, Contacts, Tasks, and Notes. **eas_16**: Enables ActiveSync 16 specific folder synchronization features in Email+. When Email+ receives "eas_16" the first time, Folder resync is expected. When "eas_16" protocol is added to enabled_features KVP: **calendar_delegation**: Enables the **Add Delegated Calendar** option. **delegated_shared_mailbox**: Enables the delegated mailbox option. When this value is removed: • All added Delegated mailbox accounts are removed from Email and Setting's screen. • "**Add a Mailbox**" button is removed under Email screen and Setting's screen. • If only Primary account is added then the arrow to expand and collapse to show different mailbox's and Add a Mailbox label are also removed. • If Secondary account is available then arrow to expand and collapse to show different mailbox's will be available but **Add a Mailbox** label is not available.
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.

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.
Mail organization		
organize_by_date	• true • false	Disables email treading for email messages. false: "Email Threading" is turned "ON".
Calendar week view		
show_week_number	• true • false	Displays the week number in the week and month view for Calendar. You can enable or disable week number view from device Settings. Default if no key-value is configured: true
Setup access to Exchange server via EWS protocol		
email_ews_host	FQDN of the EWS server	To support EWS authentication when email_exchange_host KVP does not contain a fully qualified domain name (FDQN) of the EWS server, email_ews_host KVP should be added and have a FDQN as the value for the EWS server.

Key	Value: Enter/Select one	Description
		If not configured, the value of email_exchange_host KVP is used as the EWS server by Email+. Update the host name in the **email_ews_host** key-value pair.
ews_min_allowed_auth_mode	• basic • modern_auth • cert_base	Defines the authentication method for the Exchange server through EWS protocol. Supported authentication methods are: • basic authentication: Uses username and password. • modern authentication: Uses enable modern auth for corresponding protocol. Enables Oauth 2.0 authentication. • certificate based authentication: Uses identity certificates for authentication

6.2. App restrictions descriptions for Ivanti Email+ (Android Enterprise)

The app restriction described in the following table are available for Email+ for Android Enterprise. Before configuring new restrictions, the user should update to the latest Email+ application and then the administrator should configure new restrictions.

> When there are multiple values available within a Restriction, the different features should be specified as a list of Comma Separated Strings, with or without a space. A semicolon between them will not work.

Restriction	Value: Enter/Select one	Description
Email address	*Substitution variable for email address*	Required. Defines the email address for the email account. **Ivanti EPMM** Typically, enter $EMAIL$. You can also enter combinations of these variables, depending on your ActiveSync server requirements: $USERID$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$ **Ivanti Neurons for MDM** Typically, enter $.
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. **Ivanti EPMM** 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: $EMAIL$, $USER_CUSTOM1$, $USER_CUSTOM2$, $USER_CUSTOM3$, $USER_CUSTOM4$. **Ivanti Neurons for MDM** Typically, use $. If your ActiveSync server requires a domain, use <domain name>\$. Example: mydomain\$. Depending on your ActiveSync server requirements, you can use: $
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. Ivanti, Inc recommends leaving this field blank. **Ivanti EPMM only** You can use the variable $PASSWORD$ if you have checked Save User Password in Settings > Preferences. Ivanti EPMM 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.

Restriction	Value: Enter/Select one	Description
		Default if restriction is not configured: User is prompted for ActiveSync password.
Device ID **(Ivanti EPMM only)**	$DEVICE_UUID_NO_DASHES$	Required.
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 password attempt. Therefore, Ivanti, Inc recommends selecting this restriction if the email server allows only a small number of password attempts.
Email login certificate	**Ivanti EPMM** $CERT_ALIAS:certificate enrollment setting name$ **Ivanti Neurons for MDM** Certificate setting from the dropdown list	Configure for certificate-based authentication to the ActiveSync server or to Standalone Sentry. **Ivanti EPMM** 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. **Ivanti Neurons for MDM** 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	**Ivanti EPMM** $CERT_ALIAS:certificate enrollment setting name$ **Ivanti Neurons for MDM** Certificate setting from the dropdown list	Specifies the certificate to use for signing S/MIME emails. **Ivanti EPMM** 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. **Ivanti Neurons for MDM** The certificate setting is configured in Configurations > Add > Certificate or Identity Certificate.
Email encryption	**Ivanti EPMM** $CERT_ALIAS:certificate enrollment	Specifies the certificate to use for encrypting S/MIME emails. **Ivanti EPMM**

Restriction	Value: Enter/Select one	Description
certificate	setting name$ **Ivanti Neurons for MDM** Certificate setting from the dropdown list	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. **Ivanti Neurons for MDM** The certificate setting is configured in Configurations > Add > Certificate or Identity Certificate.
Signing digest algorithm	• SHA-1 • SHA-256 • SHA-384 • SHA-512	Configures signature algorithm. The restriction is empty by default. If there is no value or invalid value set, then SHA-1 is used.
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. 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.

Restriction	Value: Enter/Select one	Description
		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	Ivanti EPMM: $DEFAULT$ Ivanti Neurons for MDM: 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 Ivanti EPMM, 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+.
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. 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: 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. Also applicable for Delegated Mailbox. Allowed values are integers starting with 1. 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	Specifies the maximum number of days for which emails are downloaded: 0: all emails. 1: emails received over the last one day. 2: emails received over the last three days.

Restriction	Value: Enter/Select one	Description
	• 3 • 4 • 5	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 • multiple_accounts • allow_shortcuts • calendar_delegation • entrust_certificates • smime_suppress_certificate_email_check • delegated_shared_mailbox • calendar_folders • microsoft_teams_meetings • graph_api	**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. **multiple_accounts**: Enables secondary email account on the same device. **allow_shortcuts**: Enables the user to create shortcuts for launch Calendar, Contact, Notes, and Tasks. **calendar_delegation**: Enables the Add Delegated Calendar option. **entrust_certificates**: Enable support for entrust certificate for Android Enterprise cloud. The Email+ app now fetches these certificates from the keystore. This is applicable for Android Enterprise device registration mode such as Profile Owner, Device Owner, and EPO with Microsoft Office 365 using Modern auth. The Email+ Android Enterprise apps uses the certificates is as follows: • **Authorization Cert**: This certificate is used to login to the Email+ app. • **Signing /Encryption**: This certificate is used for SMIME functionality. **smime_suppress_certificate_email_check**: Automatic certificate verification using email address is suppressed and the user can manually add a certificate using the Keystore and GALoptions. **delegated_shared_mailbox**: **delegated_shared_mailbox**: Enables the delegated mailbox option. When this value is removed: • All added Delegated mailbox accounts are removed from Email and Setting's screen. • "**Add a Mailbox**" button is removed under Email screen and Setting's screen. • If only Primary account is added then the arrow to expand and collapse to show different mailbox's and Add a Mailbox label are also removed. • If Secondary account is available then arrow to expand and collapse to show different mailbox's will be available but **Add a Mailbox** label is not available.

Restriction	Value: Enter/Select one	Description
		calendar_folders: Syncs all the calendar folders and their events to the primary account. This feature is currently available for the primary mail account. **microsoft_teams_meetings: To enable microsoft teams in the Calendar settings.** **graph_api**: To enable Microsoft Graph API for delegated and shared mailbox and calendar functionality.
Disabled Features	• save_attachment • print • show_snippet • personal_events • crl_signature_check • eas_16	**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. **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. **eas_16**: Disables support for Exchange ActiveSync16,
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 • Modern Authentication	Defines the authentication method to the Exchange ActiveSync service. • Basic Authorization: user name and password • Certificate-Based Authentication: identity certificates • Modern Authentication: enable modern auth for corresponding protocol. Enables Oauth 2.0 authorization. Modern Auth Authority URL and Modern Auth Resource URL: when configured through sentry uses the following values: • **modern_auth_authority_url**: https://<SentryHostname>/proxyservice • **modern_auth_resource_url**: https://<SentryHostname> 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 domain of the user's email address is considered safe. Device users have the option to either

Restriction	Value: Enter/Select one	Description
		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. 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 phishin	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.

Restriction	Value: Enter/Select one	Description
g		
Organize by date	• true • false	Disables email treading for email messages. false: "Email Threading" is turned "ON".
Show week number	• true • false	Displays the week number in the week and month view for Calendar. You can enable or disable week number view from device Settings. Default: true
Exchange host for EWS	FQDN of the EWS server	To support EWS authentication when Exchange host restriction contains NOT the fully qualified domain name (FDQN) of the EWS server, Exchange host for EWS restriction should have a FDQN as the value for the EWS server. If not configured, the value of Exchange host restriction is used as the EWS server.
EWS Authentication Mode	• Basic Authentication • Modern Authentication • Certificate Based Authentication	Defines the authentication method to the EWS. • Basic Authentication: username and password • Modern Authentication: enable modern auth for corresponding protocol. Enables Oauth 2.0 authentication • Certificate Based Authentication: support delegated calendar with certificate based authentication. Default: Basic Authentication
(Optional) Encryption algorithm	• 3des (currently used by Email+, the most compatible and default) • aes256 • aes192 • aes128	Configures encryption algorithm. The restriction is empty by default. if there is no value of invalid set, then 3des is used.
Calendars sync period	• 0: sync all events • 1: sync events for one month • 3: sync events for three months	Calendars sync period is added to sync all calendar events matching the sync period provided in Email+, with default value set to 1 for syncing one month calendar events.

Restriction	Value: Enter/Select one	Description
	• 6: sync events for six months	
MSAL Client Id		Replaces the default application ID used by the Microsoft Authentication Library (MSAL) with a custom value.
MSAL Resource Scope		Defines the resource scope required by MSAL to acquire access tokens for protected resources. Specify the multiple scopes with a single comma-separated string (for example, user.read, mail.read, and so on).
Exchange graph host email_graph_host	graph.microsoft.com	This key allows the admin to enable or disable Graph API operations.
cns host for graph notification_server_host	https://cns.mobileiron.com/PROD	Enabled delivery of notifications for delegated mailbox and calendar activities through Microsoft Graph..

6.3. SMIME support in Email+ for Android for identity and encryption

Email+ for Android supports SMIME (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 SMIME encryption certificate.
- Decrypt SMIME encrypted emails using a configured SMIME encryption certificate.

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

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

The following describes SMIME behavior in Email+

- **SMIME 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 (Ivanti EPMM)**
- **Configuring SMIME certificates for Android AppConnect (Ivanti Neurons for MDM)**
- **Configuring SMIME certificates for Email+ for Android Enterprise (Ivanti EPMM and Ivanti Neurons for MDM)**

Configuring S/MIME certificates for Android AppConnect (Ivanti EPMM)

The following describes the configuration in Ivanti EPMM.

Procedure

1. In the Ivanti EPMM 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**.

Configuring SMIME certificates for Android AppConnect (Ivanti Neurons for MDM)

The following describes the configuration in Ivanti Neurons for MDM.

Procedure

1. In Ivanti Neurons for MDM, 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**.

Configuring SMIME certificates for Email+ for Android Enterprise (Ivanti EPMM and Ivanti Neurons for MDM)

The following describes the configuration for Android Enterprise. The procedure is applicable in Ivanti EPMM and Ivanti Neurons for MDM.

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

- **Ivanti Email+ for Android Enterprise app configuration and distribution**.
- **App restrictions descriptions for Ivanti Email+ (Android Enterprise)**.

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.

SMIME behavior in Email+

Email+ does the following with the SMIME 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.
- 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.

Fetching certificates from GAL

Email+ fetches all available certificates for recipients from GAL while sending encrypted email, if the certificate is not found in GAL the Email+ app fetches the certificate from Keystore.

6.4. 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

6.5. Downloading large email attachments

Email+ for Android allows the user to download email attachments larger than 10 MB that may fail due to Microsoft's attachment size limitation.

If an attachment fails to download, the application displays an alert with the message: **Failed to Retrieve Attachment**.

You will see two options:

Download MIME – It appears when a single attachment fails. It retrieves the entire email (MIME) so all attachments are downloaded together.

OK – Dismisses the alert without downloading.

Download Options

Choose an option below to download the full email.

- **Download MIME** – It retrieves the full email with all attachments when a single attachment fails.
- **Download All** - It downloads the complete email (MIME), regardless of attachment size.

Scope and support

- This feature is supported for ActiveSync accounts, including Microsoft Office 365 and on-premises Exchange accounts that use ActiveSync.
- This feature is not applicable to Delegated and Shared mailboxes.
- This feature is not supported for EWS accounts, as EWS already allows downloading attachments larger than 10 MB by default.

6.6. 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.
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".

Property	Description
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"

}

]

}

The Email classification markers consists of JSON formatted data. The following table describes the generic classification and sample format:

Classification	Value	Sample format

Fields	Array of JSON objects of the classification field configurations.
	• **name**: The name is a combination of alphabets and numbers. The first letter of the name should be in uppercase.
	• **title**: The text that is displayed to a user in classification picker. It consists of letters, numbers, and spaces. The default value is equal to **name** value. (Optional)
	• **description**: The text displayed in the Classification Picker, to provide users with more information about the Field. The default value is an empty string. (Optional)
	• **required**: When set to "true" a user is required to select a value for this field Boolean. The default value is set to false. (Optional)
	• **onReply**: Possible values:
	• **UPGRADE_ONLY** - allows to upgrade this classification field on email reply.
	• **LOCK** - prevents from changing this classification field on email reply. (Optional)
	• **ANY** - allows any change to this classification field on email reply. The default value is set to "ANY". (Optional)
	• **allowCustomValue**: When "true" a user would be able to add a custom value manually in the picker. Possible only when "onReply" is "ANY". Boolean. The default value is set to false. (Optional)
	• **selectionsMaxNumber**:When enabled, you can select multiple field values. The default value is set to 1.
		"fields":[
		{
		"name":"SEC",
		"type":"text",
		"title":"Security Classification",
		"description":"",
		"onReply":"UPGRADE_ONLY"
		},
		{
		"name":"ACCESS",
		"title":"Information Management Marker",
		"parent":"SEC",
		"required":false,
		"onReply":"LOCK"
		},
		{
		"name":"CAVEAT",
		"title":"Caveat",
		"required":false,
		"allowCustomValue":true
		}
		]

Values	Array of JSON objects of the classification fields values. • **$Fields.name$**: Array on the classification values for the appropriate field. The same field name can be declared multiple times for the unique "parentRange" • **value**: A value to be used for the specific classification marking. Must not contain semi-colons or be comprised of only spaces. Must be declared in the priority order, from the least secure to the most. (Required) • **title**: The text that is displayed as a classification value in the picker. The default value is equal to "value". (Optional) • **description**: The text that is displayed as a description to the specific classification value. The default value is an empty string. (Optional) • **defaultValue**: Classification selected by default on a message compose start. Object of the field-value pairs. The default is an empty field.	"values":[{ "SEC":[{ "value":"UNOFFICIAL", "title":"Unofficial", "description":"Non work-related email" }, { "value":"OFFICIAL", "title":"Official", "description":" Work-related emails that do not carry a security classification" }, { "value":"OFFICIAL:Sensitive", "title":"Official:Sensitive",

Classification	Value	Sample format

	• **conditionality**: Defines the dependencies between different fields. One field may be dependent just to a single another one.
	• **target**: defines a parent field and its values in "field":["value_1", ...,"value_n"] format.
	• **dependent**: defines a child field with a list of values that a user would be shown when any of the "target" fields is selected.
		"description":"Sensitive but not security classified information"
		},
		{
		"value":"PROTECTED",
		"title":"Protected"
		},
		{
		"value":"SECRET",
		"title":"Secret"
		},
		{
		"value":"TOP-SECRET",
		"title":"Top secret"
		},
		],
		
		},
		{
		"ACCESS":[{"value":"Personal-Privacy"},
		{"value":"Legal-Privilege"},
		{"value":"Legislative-Secrecy"}]
		},
		{
		"CAVEAT":[{"value":"SH:CABINET",
		title:"Cabinet"}, {"value":"REL:AU",
		title:"Australia"}],
		}
		],
		"defaultValue":{"SEC":"OFFICIAL",
		"ACCESS":"Personal-Privacy" },
		"conditionality":[
		{
		"targetField":"SEC",
		"dependentField":"ACCESS",
		"dependencies":[{"targetValues":
		["OFFICIAL","OFFICIAL:Sensitive","PROTECTED","SECRET","TOP-SECRET"],
		"dependentValues":["Personal-Privacy","Legal-Privilege","Legislative-Secrecy"]}]
		},
		{

Classification	Value	Sample format
		"targetField":"SEC", "dependentField":"CAVEAT", "dependencies":[{"targetValues": ["PROTECTED","SECRET","TOP- SECRET"],"dependentValues": ["SH:CABINET","$custom$"] }] },] }

Send Options	JSON object that defines the actions that would be applied to a message while sending and to a new event after creation.
	• **xHeader**: Object to define the X-Header key and value to be sent with each email.Optional.
	• **subjectSuffix**: Text to be appended to a classified message subject.
	• **bodyHeader** and **bodyFooter**: Formatted text to be appended to the start or the end of a message before an email sending. Optional.
	◦ **text**: text in Special formatting. **"\\n"** is resolved as a new line within the text.
	Required.
	▪ **color**: defines text color in #RRGGBB. Optional, default "#000000".
	▪ **alignment**: defines text alignment with "LEFT"|"CENTER"|"RIGHT" values. Optional, default "LEFT".
	▪ **style** - defines text style in HTML style format. When defined, "color" and "alignment" properties would be ignored.
	▪ **conditions**: allows to modify "bodyHeader" or "bodyFooter" values ("text", "color", "alignment") depending on "when" condition.
	▪ **when**: includes a field name and values. On an email sending with any of these classification values, a property from "result" would override the original "bodyHeader"/"bodyFooter" properties.
	• **allowNotClassified**: Boolean value that identifies if Email can be sent without classification selected. Boolean. Optional. Default value "false".
		"sendOptions": {
		"subjectSuffix" : "[(SEC=$SEC.value$){, }
		(ACCESS=$ACCESS.value$){, }
		(CAVEAT=$CAVEAT.value$){, }
		(CAVEAT=$CAVEAT.value_1$){, }
		(CAVEAT=$CAVEAT.value_2$)]",
		"bodyHeader":{
		"text":"($CAVEAT.title$: $CAVEAT.value$){, }
		($CAVEAT.value_1$){, }($CAVEAT.value_2$)",
		"color":"#000000",
		"alignment":"CENTER",
		"conditions":[{"when":{"SEC":
		["PROTECTED"]},"result":
		{"color":"#FF0000"}}]
		},
		"bodyFooter":{
		"text":"($CAVEAT.title$: $CAVEAT.value$){, }
		($CAVEAT.value_1$){, }($CAVEAT.value_2$)",
		"color":"#000000",
		"alignment":"CENTER",
		"conditions":[{"when":{"SEC":
		["PROTECTED"]},"result":
		{"color":"#FF0000"}}]
		},
		"allowNotClassified":true
		}

ReceiveM	Defines a list of patterns to parse classification from a received message. The order in which the patterns are applied is defined in "priorities".	"receiveMarking": {

Classification	Value	Sample format
arking	• **xHeaderPatterns**: Rules to parse classification value from the X-Header.The X-Header key is searched by "headerName" values with left-to-right priority. (Optional) • **subjectSuffixPatterns**: Rules to parse classification value from an email subject. ◦ **boundaries** define the range of characters in the subject to check for the classification. The "rules" are applied to the text starting from the first inclusion of "start" text and the last of "end". Whole subject is checked when not defined. (Optional) • **priorities**: Defines which patterns to fetch classification value. The default value is set to "priorities". ["xHeaderPatterns","subjectSuffixPatterns"]. (Optional)	"priorities": ["xHeaderPatterns","subjectSuffixPatterns"], "xHeaderPatterns":{ "headerName" : ["X-Protective-Marking", "X-Classification"], "rules":["SEC=SEC", "sec=SEC", "SEC:SEC", "sec:SEC", "ACCESS=$ACCESS$", "access=$ACCESS$", "ACCESS:$ACCESS$", "access:$ACCESS$", "CAVEAT=$CAVEAT$", "caveat=$CAVEAT$", "caveat:$CAVEAT$", "caveat:$CAVEAT$"], "separatorRegex":"[^a-zA-Z\d\-_\s]" }, "subjectSuffixPatterns":{ "rules":["SEC=SEC", "sec=SEC", "SEC:SEC", "sec:SEC", "ACCESS=$ACCESS$", "access=$ACCESS$", "ACCESS:$ACCESS$", "access:$ACCESS$", "CAVEAT=$CAVEAT$", "caveat=$CAVEAT$", "caveat:$CAVEAT$", "caveat:$CAVEAT$"], "boundaries":{"start":"[", "end":"]"}, "separatorRegex":"[^a-zA-Z\\d\\-_\\s:]" } },
Version	**version** value should be defined to differ between JSON schemas. (Required)	classification version: 2.0.0

6.7. 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

> 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**.

6.8. Entrust certificates

The Email+ Android Enterprise app for Ivanti Neurons for MDM uses Entrust Authorization, Signing, and Encryption certificates that were generated in the PIV-D app and stored in keystore and use them to perform the functions:

- **Authorization Certificate**: This certificate is used to login to the Email+ app.
- **Signing /Encryption Certificate**: This certificate is used for SMIME functionality.

This is applicable for Android Enterprise Device Registration mode such as Profile Owner, Device Owner, and EPO modes with Microsoft Office 365 using Modern auth.

To configure entrust certificates new value **entrust_certificates** is added to Optional features restriction for Android Enterprise.

Enabling Ivanti Email+ to use certificates from keystore

The Go client allows Email+to use the certificates from the keystore only when the Manage Certificates option is enabled.

1. In the Ivanti Neurons for MDM portal, go to **Apps >App Catalog**.
2. Select Email+ (Android) from Business Apps.
3. In App Configurations for Email+, select **Delegated Device Permissions > Manage Certificates** option to enable entrust certificates for Email+ Android Enterprise.

6.9. Suppress certificate email check

The Email+ app can now suppress the verification of certificates using email address in case of email address or domain mismatch. To enable this feature add the **smime_suppress_certificate_email_check** value to the Optional features restriction. When the Email+ app receives an email signed with a certificate, where the email address or domain differs from the sender's emails address, the Email+ app associates the certificate with the sender's email address, so that the Email+ app can use the certificate when sending encrypted emails to the sender.

The Email+ app adds an encryption certificate when a signed email is sent. The encryption certificate is automatically saved and associated to the certificate if the certificate in the email is different than the sender's email. The user can also add the certificate manually using the **Add from Keystore** or **Add from Global Address List** options.

> If email in the SMIME certificate doesn't correspond to email of the Exchange user, then this certificate cannot be retrieved by server when we search GAL.

> Currently with SMIME implementation, when Email+ tries to encrypt an email it first checks for the certificate in local cache and if the certificate is not available then Email+ tries to download available certificate from GAL.

New 'Recipient certificates' option appears in **Compose email** screen. Tap '**Recipient certificates**' option to view the list of recipients with associated certificates. User can also add and delete certificates on this screen.

> The receiver should save the encryption certificate and make association for the certificate if the certificate in the email is different than the sender's email.

7. 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 Email+ Android app.

Setting permissions on Ivanti 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.

8. Additional email accounts

Email+ Android supports additional 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 additional accounts.

When additional 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 additional accounts are displayed in different colors.

Adding a additional 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.

Configuring additional account for Android AppConnect

The following are account specific key-values pairs supported for additional 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 remove additional account from your device for **Android AppConnect** remove the “**multiple_accounts**” value from “**enabled_features**”.

Configuring secondary account for Android Enterprise

Email+ supports up to 10 additional accounts for Android Enterprise. After the Email+ 4.9.0 upgrade, when new additional accounts are configured and pushed to the devices then the existing additional accounts are also re-synced.

> Ivanti recommends to upgrade Email+ to 4.9.0 on device and then add multiple additonal account in the Email+ config from server.

The following message is displayed on the Email+ app when a new account is configured. This is to inform users that mail, calendar, contacts, notes, tasks for the configured account sync is in progress. Once the sync is completed the message will disappears.

"**Email sync in progress. This may take sometime.**"

To configure additional 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

> If the **Allow unmanaged devices to receive email and data** key-value pair is set to False in the Sentry configuration. The Sentry exchange server does not allow the users to log in to the additional email accounts. Ivanti recommends you to enable the **Default Unmanagaed Device Behavior** configuration when using the additional email account.

Removing secondary account

To remove secondary account from your device:

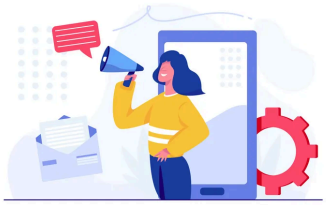
- **For Android AppConnect** remove the “multiple_accounts” value from “enabled_features”.
- **For Android Enterprise** remove "multiple_accounts" restriction from “Optional items”.

> When there are changes to the existing app restrictions, then the "**Update**"options is enabled. If there are more than one additional accounts in App configurations, clicking on **Update** all the accounts will be removed and reset to default primary account only. This issue does not impact if you have only primary account configured.

9. Ivanti Email+ 5.0.0 - 5.5.0 for Android Guide

September 2026

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



New features summary

Revision history

10. Delegated calendar

Ivanti Email+ supports delegated access for Calendar. The delegated calendar option enables the calendar owner to assign their calendar to a delegated user within the organization's exchange Global Address List (GAL). To enable the **Add Calendar** option in Email+, configure the **calendar_delegation** value in **enabled_features** key value pair or in **Optional Features** restriction.

Email+ supports delegated calendar permissions similar to Microsoft Exchange server such as Reviewer, Editor, and Author level permissions. The delegated user can view events related updates on the Email+ app with these permissions.

> The Email+ app does not display private events, all private events in delegated calendar are hidden.

The following table displays the different delegation permissions and the actions they can perform:

Permission level	Action allowed
Reviewer	With the Reviewer level permissions you can perform the following actions: • Appointments (event without attendees) - no options • Delegated calendar owner's created invite - Reply All on behalf of • Received invite - Reply or Reply All on behalf of
Author	With the Author level permissions you can perform the following actions: • Appointments (event without attendees) - no options • Delegated calendar owner's created invite - Reply All on behalf of • Received invite - Reply or Reply All on behalf of • Author created appointments - no options • Author created invites - Reply All and Forward on behalf of
Editor	With the Editor level permissions you can perform the following actions: • Appointments (event without attendees) - no options • Delegated calendar owner's created invite - Reply All and Forward on behalf of • Received invite - Reply or Reply All or Forward on behalf of • Editor created appointments - no options • Editor created invite - Reply All and Forward on behalf of

To configure delegation on **Android AppConnect** or **Android Enterprise**, configure the following key-value pairs or restrictions:

- Add **calendar_delegation** value to **enabled_features** key-value pair or **calendar_delegation** value to **Optional Features** restriction to add the **Add Delegated Calendar** option in the Email+ app
- Add **email_ews_host** key-value pair or **Exchange host for EWS** restriction with EWS host value as FQDN to provide access to EWS server when the values for **email_exchange_host** key-value pair or **Exchange host** restriction are not fully qualified domain name of the exchange server.
- Add **ews_min_allowed_auth_mode** key value pair or **EWS Authentication Mode** restriction to enable basic, modern_auth, and cert_based authentication methods to the exchange server through EWS protocol. If Email+ is configured with **eas_min_allowed_mode** KVP or **Authorization mode** restriction as Modern Auth, add **ews_min_allowed_auth_mode** KVP with **modern_auth** or **EWS Authentication Mode** restriction with **Modern Authentication** value to enable modern authentication method to the EWS server.

- If EWS server is not accessible publicly (located in private network), then VPN should be configured. For more information see, **Configuring Email+ with AppTunnel for Android AppConnect** and **Configuring Email+ with Ivanti Tunnel for Android Enterprise**

When a calendar is delegated, a system generated mail is sent to the delegated user with details of the calendar owner. The calendar owner has the ability to assign or deny access to the delegated calendar.

Adding delegated calendar

In the Email+ app, go to **Calendar > Add Calendar** option and enter the calendar owner's email address. Select the calendar owner to add the delegated calendar. you can assign a color to the delegated calendar to differentiate between assigned calendars.

> The calendar owner delegates the calendar from the Microsoft Outlook on the web (OWA). For more information on delegation, see **Microsoft documentation**.

The user can manually remove the delegated calendar from the Email+ app. If the access to the deleted calendar is available, then user can again add that delegated calendar.

When the calendar owner removes access to the delegated calendar, Email+ receives "**Delegated Calendar access has been denied**" notification when the Email+ app is launched.

Disabling delegated calendar feature

The admin can disable the **Add Calendar** option from the Email+ app by removing **calendar_delegation** value from the **enabled_features** key value pair or from the **Optional Features** restriction. For more information on the supported key-value pairs and restriction, see **Key-value pairs for Ivanti Email+ (Android AppConnect)** and **App restrictions descriptions for Ivanti Email+ (Android Enterprise)** sections.

Ivanti Email+ configurations supported for Delegated Calendar

The following table lists the supported Email+ and EWS configurations.

Before you begin

EWS must have Basic Auth enabled in Internet Information Services (IIS) manager (Microsoft Exchange server) for Android.

> If EWS server is not accessible publicly (located in private network), then VPN should be configured.

> Update the host name in the **email_ews_host** key-value pair.

Email+ Configuations	Additional Configurations for EWS	Supported
Android AppConnect: Ivanti EPMM and Ivanti Neurons for MDM with sentry, Modern auth with or without **email_password** KVP, Microsoft Office 365	Add **email_ews_host** KVP with EWS server value Add **ews_min_allowed_auth_mode = modern_auth** KVP	Yes
Android AppConnect and Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, without sentry, Modern auth with or without **email_password** KVP, Microsoft Office 365	Add **ews_min_allowed_auth_mode = modern_auth** KVP	Yes
Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, with sentry, Modern auth with or without **email_password** KVP, Microsoft Office 365	**Exchange host for EWS** should have value of the EWS server **EWS Authentication Mode** should have **Modern Authentication** value	Yes
Android AppConnect and Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, with sentry + Local certificate, Basic auth with or without **email_password** KVP, Microsoft Exchange versions 2016 and 2019, Microsoft Office 365	Android AppConnect: add **email_ews_host** with EWS server value Android Enterprise: **Exchange host for EWS** should have value of the EWS server	Yes
Android AppConnect and Android Enterprise: Ivanti EPMM, with sentry + group certificate, Basic auth with or without **email_password** KVP, Microsoft Exchange versions 2016 and 2019, Microsoft Office 365	Android AppConnect: Add **email_ews_host** with EWS server value Android Enterprise: **Exchange host for EWS** should have value of the EWS server	Yes
Android AppConnect and Android Enterprise: Ivanti EPMM, with Sentry + MS scep certificate, Basic auth with or without **email_password** KVP, Microsoft Exchange versions 2016 and 2019, Microsoft Office 365	Android AppConnect: add **email_ews_host** with EWS server value Android Enterprise: **Exchange host for EWS** should have value of the EWS server	Yes
Android AppConnect and Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, with Sentry, Kerberos with **prompt_email_password=true** and enter password on Email+ login screen, Microsoft Exchange versions 2016 and 2019	Android AppConnect: add **email_ews_host** with EWS server value Android Enterprise: **Exchange host for EWS** should have value of the EWS server	Yes
Android AppConnect and Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, with Sentry, Kerberos with **email_password** KVP with hard coded value (which is not probably a use case), Microsoft Exchange versions 2016 and 2019	Android AppConnect: add **email_ews_host** with EWS server value. Android Enterprise: **Exchange host for EWS** should have value of the EWS server	Yes

Email+ Configuations	Additional Configurations for EWS	Supported
Android AppConnect and Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, without sentry, Basic auth (with or without 'email_password' KVP), Microsoft Exchange versions 2016 and 2019, Microsoft Office 365	Android AppConnect: add **email_ews_host** with EWS server value. 'ews_min_allowed_auth_mode' = cert_base KVP should be added Android Enterprise: Exchange host for EWS' should have value of the EWS server 'EWS Authentication Mode' should have 'Certificate-Based Authentication' value	Yes
Android AppConnect and Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, with or without sentry, Certificate based auth, Microsoft Exchange versions 2016 and 2019.	Android AppConnect: add 'ews_min_allowed_auth_mode' = cert_base KVP Android Enterprise: add 'EWS Authentication Mode' should have 'Certificate-Based Authentication' value. For **cert_base** value, Mocrosoft Office 365 is not supported.	Yes
Android AppConnect and Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, with sentry, Kerberos (without 'email_password' KVP), Microsoft Exchange versions 2016 and 2019		No

Limitations

- Email+ does not support attachments for delegated events.
- Email+ does not support reminders and notifications for delegated events.

11. Shared calendar

Email+ supports shared access for Calendar. The shared calendar option enables the calendar owner share their calendar with a user or group of users within the organization's exchange Global Address List (GAL). To enable the **Add Calendar** option in Email+, configure the **calendar_delegation** value in **enabled_features** key value pair or in **Optional Features** restriction.

Email+ supports Shared Calendar for both Microsoft Exchange and Microsoft O365 server. There are different permission settings Microsoft Exchange and Microsoft Office 365 server.

The following table displays the different permissions for exchange server supported by Email+:

Permission level	Descrption
None	Indicates that the user has no permissions on the folder.
Owner	Indicates that the user can create, read, edit, and delete all items in the folder, and create subfolders. The user is both folder owner and folder contact.
PublishingEditor	Indicates that the user can create, read, edit, and delete all items in the folder, and create subfolders.
Editor	Indicates that the user can create, read, edit, and delete all items in the folder.
PublishingAuthor	Indicates that the user can create and read all items in the folder, edit and delete only items that the user creates, and create subfolders.
Author	Indicates that the user can create and read all items in the folder, and edit and delete only items that the user creates.
NoneditingAuthor	Indicates that the user can create and read all items in the folder, and delete only items that the user creates.
Reviewer	Indicates that the user can read all items in the folder.
Contributor	Indicates that the user can create items in the folder. The contents of the folder do not appear.
Custom	Indicates that the user has custom access permissions on the folder. Includes a custom collection of individual permissions.

The following table displays the different permissions for Shared Calendar for Microsoft Office 365 supported by Email+:

Permission level	Descrption
Can view all details	Email+will show all the details of user's appointments, just like what they see.
Can edit	Indicates that user has edit permissions.

To configure Shared Calendar on **Android AppConnect** or **Android Enterprise**, configure the following key-value pairs or restrictions:

- Add **calendar_delegation** value to **enabled_features** key-value pair or **calendar_delegation** value to **Optional Features** restriction to add the **Add Calendar** option in the Email+ app.
- Add **email_ews_host** key-value pair or **Exchange host for EWS** restriction with EWS host value as FQDN to provide access to EWS server when the values for **email_exchange_host** key-value pair or **Exchange host** restriction are not fully qualified

domain name of the exchange server.

- Add **ews_min_allowed_auth_mode** key value pair or **EWS Authentication Mode** restriction to enable basic, modern_auth, and cert_based authentication methods to the exchange server through EWS protocol. If Email+ is configured with **eas_min_allowed_mode** KVP or **Authorization mode** restriction as Modern Auth, add **ews_min_allowed_auth_mode** KVP with **modern_auth** or **EWS Authentication Mode** restriction with **Modern Authentication** value to enable modern authentication method to the EWS server.
- If EWS server is not accessible publicly (located in private network), then VPN should be configured. For more information see, **Configuring Email+ with AppTunnel for Android AppConnect** and **Configuring Email+ with Ivanti Tunnel for Android Enterprise**

The Email+ app sends a notification when access to Shared Calendar is canceled by the calendar owner. The user receives notification when the Email+ app is launched or is running in the background. The Shared Calendar is removed from the Email+ app.

> The sync period for all existing events for the Shared Calendar is set to a duration of one month. Events older than a month are not synced.

Adding shared calendar

In the Email+ app, go to **Calendar > Add Calendar** option and enter the calendar owner's email address. Select the calendar owner to add the shared calendar. You can assign a color to the shared calendar to differentiate between assigned calendars.

Disabling shared calendar feature

The admin can disable the **Add Calendar** option from the Email+ app by removing **calendar_delegation** value from the **enabled_features** key value pair or from the **Optional Features** restriction. For more information on the supported key-value pairs and restriction, see **Key-value pairs for Ivanti Email+ (Android AppConnect)** and **App restrictions descriptions for Ivanti Email+ (Android Enterprise)** sections.

For more information on Email+ configuration, see **Email+ configurations supported for Delegated Calendar** section in **Delegated calendar** .

Microsoft limitations

The shared calendar has following Microsoft limitations:

1. Reply event and Reply all options are available but reply mail cannot be sent. The message is moved to Drafts and error message is displayed.
2. The 'Invite people' field is blocked and proper notification is displayed.
3. For Exchange server: If Shared user has ‘Create items’ permission, but do not have the ‘Edit own’ or ‘Edit all’ - it is not possible to create invite with attendees. So, in Email+ when user tries to create new event the ‘Invite people’ field is blocked and proper label is displayed.
4. As Exchange 2013 server will be deprecated in April, the Shared calendar feature is not supported by Email+ 4.6.0 on this server.
5. Email+ 4.6.0 does not provide support for the following permissions:
    1. For Exchange server: 'Time, Subject, or Location', 'Free or Busy time'
    2. For Office 365: 'Can view when I’m busy', 'Can view titles and locations'.

Ivanti Email+ configurations supported for Shared Calendar

The following table lists the supported Email+ and EWS configurations.

Before you begin

EWS must have Basic Auth enabled in Internet Information Services (IIS) manager (Microsoft Exchange server) for Android.

> If EWS server is not accessible publicly (located in private network), then VPN should be configured.

Email+ Configuations	Additional Configurations for EWS	Supported
Android AppConnect: Ivanti EPMM and Ivanti Neurons for MDM with sentry, Modern auth with or without **email_password** KVP, Microsoft Office 365	Add **email_ews_host** KVP with EWS server value Add **ews_min_allowed_auth_mode = modern_auth** KVP	Yes
Android AppConnect and Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, without sentry, Modern auth with or without **email_password** KVP, Microsoft Office 365	Add **ews_min_allowed_auth_mode = modern_auth** KVP	Yes
Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, with sentry, Modern auth with or without **email_password** KVP, Microsoft Office 365	**Exchange host for EWS** should have value of the EWS server **EWS Authentication Mode** should have **Modern Authentication** value	Yes
Android AppConnect and Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, with sentry + Local certificate, Basic auth with or without **email_password** KVP, Microsoft Exchange versions 2016 and 2019, Microsoft Office 365	Android AppConnect: add **email_ews_host** with EWS server value Android Enterprise: **Exchange host for EWS** should have value of the EWS server	Yes
Android AppConnect and Android Enterprise: Ivanti EPMM, with sentry + group certificate, Basic auth with or without **email_password** KVP, Microsoft Exchange versions 2016 and 2019, Microsoft Office 365	Android AppConnect: Add **email_ews_host** with EWS server value Android Enterprise: **Exchange host for EWS** should have value of the EWS server	Yes
Android AppConnect and Android Enterprise: Ivanti EPMM, with Sentry + MS scep certificate, Basic auth with or without **email_password** KVP, Microsoft Exchange versions 2016 and 2019, Microsoft Office 365	Android AppConnect: add **email_ews_host** with EWS server value Android Enterprise: **Exchange host for EWS** should have value of the EWS server	Yes
Android AppConnect and Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, with Sentry, Kerberos with **prompt_email_password=true** and enter password on Email+ login screen, Microsoft Exchange versions 2016 and 2019	Android AppConnect: add **email_ews_host** with EWS server value Android Enterprise: **Exchange host for EWS** should have value of the EWS server	Yes
Android AppConnect and Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, with Sentry, Kerberos with **email_password** KVP with hard coded value (which is not probably a use case), Microsoft Exchange versions 2016 and 2019	Android AppConnect: add **email_ews_host** with EWS server value. Android Enterprise: **Exchange host for EWS** should have value of the EWS server	Yes

Email+ Configuations	Additional Configurations for EWS	Supported
Android AppConnect and Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, without sentry, Basic auth (with or without 'email_password' KVP), Microsoft Exchange versions 2016 and 2019, Microsoft Office 365		Yes
Android AppConnect and Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, with or without sentry, Certificate based auth, Microsoft Exchange versions 2016 and 2019, Microsoft Office 365	Android AppConnect: add 'ews_min_allowed_auth_mode' = cert_base KVP Android Enterprise: add 'EWS Authentication Mode' should have 'Certificate-Based Authentication' value	Yes
Android AppConnect and Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, with sentry, Kerberos (without 'email_password' KVP), Microsoft Exchange versions 2016 and 2019		No

Limitations

- Email+ does not support attachments for shared events.
- Email+ does not support reminders and notifications for shared events.

12. Delegated mailbox

Ivanti Email+ supports delegated access for Mailbox. Currently, we support delegation of up to four mailboxes. In case of multiple mailboxes, each mailbox is independent and has its own Delegated Mailbox account settings.

When configuring the mailbox delegation, the owner delegates mailbox to another user (Delegate) to manage it as per delegation level set on Outlook.

The delegated user can add upto four delegated mailboxes from multiple owners. .When multiple accounts are available then only mailboxes delegated to primary account can be added to Email+.

To configure Delegated Mailbox on **Android AppConnect** or **Android Enterprise**, configure the following key-value pairs or restrictions:

- Add **delegated_shared_mailbox** value to **enabled_features** key-value pair or to **Optional Features** restriction to add the **Add Mailbox** option in the Email+ app.

When you select the **Add a Mailbox** option, Email+ searches email address in GAL and provides list of contacts to add mailbox. If the search result is successful, the **'Mailbox added**' pop-up is displayed and Delegated Mailbox is added. Once Delegated Mailbox is added, the **Add Mailbox option** appears in the navigation drawer and Settings.

Email+ supports delegated mailbox permissions similar to Microsoft Exchange server such as Reviewer, Editor, and Author level permissions. Ivanti Email+ 4.7.0 supports only 'Reviewer' level permission. Starting Ivanti Email+ 4.10.0 all permissions levels are supported in Email+.

Delegated user can now save draft mail in the Delegated Mailbox. The Delegated Drafts folder is not synced with the server and only available locally. Delegate can store draft emails in "**Drafts**" folder. These folders are local and are not synced with the server.

Delegated Mailbox with Reviewer permission can perform the following actions:

- Mark as Unread or Read
- Download and view attachments from mail or invite mails.

> Search of the delegated mails is out of scope for Email+ 4.7.0 release.

All the folders are auto synced when the user clicks on each folder to start and stop the sync. The delegated user can manually delete the delegated mailbox added from the Email+ app.

> Microsoft server does not provide any permissions to load sub folders and doesn't return in requests for the sub folders synchronization so sub folder in the Inbox is not displayed for added delegated mailbox of such accounts in Email+ as well as on Outlook.

The mailbox owner can change permissions from any role (Reviewer/Author/Editor) to any role (Reviewer/Author/Editor), also for existing drafts.

- When the **Owner** revokes access to Delegated Mailbox completely, or the user removes the Delegated Mailbox manually from the Email+ settings, related Drafts folder is removed with all its content.
- When the **Owner** revokes access to Delegated Calendar, all related drafts from the "Delegated Drafts", Delegated Mailbox "Drafts", and Outbox (if any emails are stuck there) folders are removed.

- When the **Admin** removes the **delegated_shared_mailbox**key-value pair from the Email+app config, then all Delegated Mailbox drafts are deleted from the app along with the other information from the Delegated Mailbox.

The mailbox owner can update the following permission combinations:

Permission level	Combinations
Reviewer	• Reviewer > Author • Reviewer > Editor • Reviewer > None
Author	• Author > Reviewer • Author > Editor • Author > None
Editor	• Editor > Author • Editor > Reviewer • Editor > None

The following table displays the different delegation permissions and the actions they can perform:

Action	Reviewer	Author	Editor
Reading emails	Yes	Yes	Yes
Downloading and viewing email attachment	Yes	Yes	Yes
Searching emails	Yes	Yes	Yes
Marking emails as Read/Unread	Yes	Yes	Yes
Flagging emails	No	No	Yes
Moving an email to a different folder within the account	No	No	Yes
Deleting emails	No	No	Yes
Sending emails with attachments	No	Yes	Yes
Options to Reply/Reply All/Forward emails	No	Yes	Yes
Saving draft emails locally in the app. *Reviewer cannot compose emails and create drafts. The only possible way to create draft is an edge case when doing Reply/Reply All/Forward a delegated calendar event.	Yes	Yes	Yes
Responding to meeting invites from emails (no delegated calendar added)	No	No	No
Responding to meeting invites from emails (DC added). * Becomes available if the Delegated Calendar of the same owner's account is added with Author or Editor permissions.	Yes	Yes	Yes
Reading signed and/or encrypted emails	Yes	Yes	Yes
Sending signed and/or encrypted emails	No	Yes	Yes
Reading emails with Classification	Yes	Yes	Yes
Sending emails with Classification	No	Yes	Yes

Adding delegated mailbox to the Email+ app

To add the delegated mailbox to the Email+ app on your Android device, perform the following steps:

Before you begin

- Configure the enabled_features key-value pair and add the **delegated_shared_mailbox** value.
- Set both EWS and Exchange host
- Set EWS Authorization mode,
  - For Modern Auth, set value to **modern_auth**
  - For Certificate based Auth, set value to **cert_base**

Procedure

1. In the Email+ app, go to **Settings > Mail > Accounts > Add**.
2. On the **Add delegated Mailbox** screen, type the **Email ID** of the mailbox owner. Delegated mailbox is added in Mail section - Mailboxes. The delegate gets access to Inbox, sub folders, and smart folders.

Support for SMIME

The signing and encryption functionality is extended to support Delegated Mailboxes, the functionality works similar to that of Primary Account. Delegated user can:

- Read/Send signed/encrypted emails depending upon the user permission
- Read emails with Classification

The keychain is common for all mailboxes and not only for the mailbox you are working on. The app searches certificates in the keychain and GAL (same as the primary account).

The process of adding certificates to the Keychain is:

- Through **email_signing_certificate** and **email_encryption_certificate** KVPs.
- From the email attachment

Signing

A Delegate can view, search, reply, and forward signed emails in the delegator's mailbox (depending on permissions).

In the received email, the sender's signing certificate can be verified if their public certificate is available in GAL, or if it is available in the delegate's keystore in Email+. Otherwise, the certificate will be marked red as not trusted.

A Delegate can sign emails with the actual sender's certificate (Primary account) and send signed emails from the Primary account on behalf of the delegator.

If the certificate of the signed email cannot be validated (there is no user certificate in the keychain and in GAL), the red check mark icon is be displayed according to the existing logic.

Encryption

A Delegate can encrypt emails with the actual sender's certificate (Primary account) and send encrypted emails from the Primary account on behalf of the Delegator.

A Delegate can decrypt emails if the Delegator provides the Delegate with their private certificates, and these certificates are added to the app Keychain.

Suppressing Name Check on certificate mismatch

When the feature flag for suppressing name checks on certificate mismatch is enabled by admin, the feature is available for delegated mailboxes. Existing certificate associations are automatically accessible for delegated mailboxes.

The user can encrypt/decrypt emails using existing certificate associations and create new associations.

Classification

When classification is configured by Admin, it is available for delegated mailboxes. The user is able to parse emails in the delegated mailboxes having classification, reply/forward, and compose new emails.

The delegate receives a notification when a new mail is received in the delegated mailbox. Also, the delegated user receives following notification when the owner removes the access to the delegated mailbox:

Mailbox access has been denied

> You cannot delegate a particular sub folder in a mailbox, you can only delegate only the mailbox

Ivanti Email+ configurations supported for Delegated and Shared Mailbox

The following table lists the supported Email+ and EWS configurations.

Before you begin

EWS must have Basic Auth enabled in Internet Information Services (IIS) manager (Microsoft Exchange server) for Android.

> If EWS server is not accessible publicly (located in private network), then VPN should be configured.

> Update the host name in the **email_ews_host** key-value pair.

Email+ Configuations	Additional Configurations for EWS	Supported
Android AppConnect: Ivanti EPMM and Ivanti Neurons for MDM with sentry, Modern auth with or without **email_password** KVP, Microsoft Office 365	Add **email_ews_host** KVP with EWS server value Add **ews_min_allowed_auth_mode = modern_auth** KVP	Yes
Android AppConnect and Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, without sentry, Modern auth with or without **email_password** KVP, Microsoft Office 365	Add **ews_min_allowed_auth_mode = modern_auth** KVP	Yes
Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, with sentry, Modern auth with or without **email_password** KVP, Microsoft Office 365	**Exchange host for EWS** should have value of the EWS server **EWS Authentication Mode** should have **Modern Authentication** value	Yes
Android AppConnect and Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, with sentry + Local certificate, Basic auth with or without **email_password** KVP, Microsoft Exchange versions 2016 and 2019, Microsoft Office 365	Android AppConnect: add **email_ews_host** with EWS server value Android Enterprise: **Exchange host for EWS** should have value of the EWS server	Yes
Android AppConnect and Android Enterprise: Ivanti EPMM, with sentry + group certificate, Basic auth with or without **email_password** KVP, Microsoft Exchange versions 2016 and 2019, Microsoft Office 365	Android AppConnect: Add **email_ews_host** with EWS server value Android Enterprise: **Exchange host for EWS** should have value of the EWS server	Yes
Android AppConnect and Android Enterprise: Ivanti EPMM, with Sentry + MS scep certificate, Basic auth with or without **email_password** KVP, Microsoft Exchange versions 2016 and 2019, Microsoft Office 365	Android AppConnect: add **email_ews_host** with EWS server value Android Enterprise: **Exchange host for EWS** should have value of the EWS server	Yes
Android AppConnect and Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, with Sentry, Kerberos with **prompt_email_password=true** and enter password on Email+ login screen, Microsoft Exchange versions 2016 and 2019	Android AppConnect: add **email_ews_host** with EWS server value Android Enterprise: **Exchange host for EWS** should have value of the EWS server	Yes
Android AppConnect and Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, with Sentry, Kerberos with **email_password** KVP with hard coded value (which is not probably a use case), Microsoft Exchange versions 2016 and 2019	Android AppConnect: add **email_ews_host** with EWS server value. Android Enterprise: **Exchange host for EWS** should have value of the EWS server	Yes

Email+ Configuations	Additional Configurations for EWS	Supported
Android AppConnect and Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, without sentry, Basic auth (with or without 'email_password' KVP), Microsoft Exchange versions 2016 and 2019, Microsoft Office 365		Yes
Android AppConnect and Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, with or without sentry, Certificate based auth, Microsoft Exchange versions 2016 and 2019, Microsoft Office 365	Android AppConnect: add 'ews_min_allowed_auth_mode' = cert_base KVP Android Enterprise: add 'EWS Authentication Mode' should have 'Certificate-Based Authentication' value	Yes
Android AppConnect and Android Enterprise: Ivanti EPMM or Ivanti Neurons for MDM, with sentry, Kerberos (without 'email_password' KVP), Microsoft Exchange versions 2016 and 2019		No

13. Shared mailbox

Ivanti Email+ supports shared access for Mailbox. In case of multiple mailboxes, each mailbox is independent and has its own Shared Mailbox account settings. A Shared Mailbox is a type of user mailbox that does not have a username or password. It provides access to multiple users to use a mailbox as per the permissions set on Microsoft Outlook. To access a Shared Mailbox, the admin must add the user as a member of the mailbox. Email+ supports Shared Mailbox permissions similar to Microsoft Exchange server:

- **Full Access**: The full access permission allows the user to open the Shared Mailbox and act as the owner of that mailbox. The user can access mails, read, view, delete, move mails, download and view attachments, and search mails on the local device and server. However, the user cannot send mail
- **Send as**: The send as permission allows the user to impersonate the Shared Mailbox when sending mails. The user can Reply or Reply All, and Forward messages from the Shared Mailbox.
- **Send on behalf**: The send on behalf permission allows the user to send mail on the behalf of the Shared Mailbox. The user can Reply or Reply All, and Forward messages from the Shared Mailbox, but the recipients would receive the mail from <User on behalf of the Shared Mailbox name>.

The user can add signature to mails for both delegated and shared mailbox similar to the primary mail box. Separate section for **Shared Mailbox** and **Delegated Mailbox** accounts is added under the Email+ Settings. The settings for these two sections appear only if there is at least one account is available for each mailbox.

The Email+ app displays notification for both Primary and Shared mailbox accounts along with account details. The Notification rules for primary user account are applicable for Shared mailbox. The following rules are supported:

- Receive notification when the Email+ app is opened or closed.
- Notification sound
- Notification silent
- Bundle notification
- Detailed notification (When applied from Email+ config should be enabled for delegated mailbox as well).

To configure Shared Mailbox on **Android Enterprise**, configure the following restrictions:

- Add **delegated_shared_mailbox** value to **Optional Features** restriction to add the **Add Mailbox** option in the Email+ app.

When you select the **Add a Mailbox** option, Email+ searches email address in GAL and provides list of contacts to add mailbox. If the search result is successful, the **'Mailbox added**' pop-up is displayed and Shared Mailbox is added. Once Shared Mailbox is added, the **Add Mailbox option** appears in the navigation drawer and Settings.

All the folders are auto synced when the user clicks on each folder to start and stop the sync. The delegated user can manually delete the delegated mailbox added from the Email+ app.

> Ivanti Email+ does not support SMIME and Classification for Shared Mailbox.

Adding shared mailbox to the Email+ app

To add the shared mailbox to the Email+ app on your Android device, perform the following steps:

Before you begin

- Configure the Optional features and add the **delegated_shared_mailbox** value.
- Set both EWS and Exchange host
- Set EWS Authorization mode,
  - For Modern Auth, set value to **modern_auth**
  - For Certificate based Auth, set value to **cert_base**

Procedure

1. To add new mailbox, choose any of the following methods:
   1. In the Email+ app, go to **Settings > Add a mailbox** . OR
   2. In the Email+ app, open **Navigation menu > Add a mailbox**.
2. On the **Add shared Mailbox** screen, type the **Email ID** of the mailbox owner. Shared mailbox is added in Mail section - Mailboxes. The shared user

For more information on supported configuration on shared mailbox, see **Ivanti Email+ configurations supported for Delegated and Shared Mailbox** section Delegated mailbox.

Updated and optimized features.

- Improved the logic of adding or using Shared or Delegated mailboxes and sharing permissions to folders.
- Email+ app now shows Delegated or Shared mailbox as one category called "Delegated Mailboxes".
- Drafts folder is only displayed when mail drafts are available created.

14. ActiveSync16 for Android devices

Ivanti Email+ supports **ActiveSync 16** protocol for Android devices. The **ActiveSync 16** protocol allows mobile devices to synchronize email and other data with Microsoft Exchange mailbox. The ActiveSync 16 protocol supports latest Exchange platform starting from Exchange 2016 and Exchange Online.

> Starting from Email+ 5.1.0 version, ActiveSync 16 is enabled by default on all the Android devices that are supported by Email+.

The following capabilities that are supported through ActiveSynce16 protocol:

- **ActiveSync 16 support**: Sets up the synchronization engine to use ActiveSync 16 protocol.
- **Display BCC contacts in Sent items**: Allows the sender to view BCC contacts in sent emails.
- **Calendar attachments**: Calendar attachments are synced through ActiveSync 16 protocol.
- **Drafts folder synchronization**: Enables access and editing of emails in the Drafts folder from all the devices synchronized with Microsoft Exchange server.

The **eas_16** is enabled by default and this value is moved from **Optional features** to **Disabled features** restrictions

> ActiveSync 16 is unavailable if the server's highest supported version is below 16.0.

15. Configuring Azure Conditional Access (Optional)

The Azure Conditional Access validates user, device, location, and risk level before granting or denying access. The Email+ app is migrated from Azure Active Directory Authentication Library (ADAL) to Microsoft Authentication Library (MSAL) to support Azure Conditional Access.

> Optionally, configure Azure Conditional Access to restrict non compliant devices and un-managed Microsoft 365 accounts.

Creating a new Conditional Access policy

The following procedure describes how to create a new policy using Azure admin portal:

Procedure

1. In the Azure admin portal, login as admin.
2. Go to **Security > Protect > Conditional Access**.
3. In **Conditional Access** settings, click **Create new policy** to create a new policy.
4. In **New** Conditional Access Policy page, update the following fields to create a new policy:

Fields	Option
Name	Enter name of the policy.
Assignments	Controls the access based on who the policy will be applied to, such as users and groups, workload identities, directory roles or external guests, and so on. Under **Users** select: • **Include** • **Exclude**
Target resources	Select **Email+Auth**
Conditions	Select device platforms : • **Android** • **iOS**
Access controls	**Grant**: Controls access enforcement to block or grant access. Select the **Require device to be marked as compliant** option.
Enable Policy	Toggle and select from the following options: **Report-only**: Policies in Report-only more requiring compliant devices may prompt users on macOS, iOS, Android, and Linux to select a device certificate • **On** • **Off**

5. Click **Create** to save the policy.

Editing a Conditional Access policy

The following procedure describes how to edit the existing policy to configure Azure Conditional Access using the Email+Auth:

Procedure

1. In the **Azure admin portal**, login as admin.
2. Go to **Security > Protect > Conditional Access > Policies.**
3. Select and edit the policy, and update the following:
    1. Add **Email+ Auth** application as a target resource.
    2. Go to **Access Controls > Grant** and select the **Require device to be marked as compliant** option.

The Email+ application is now set up for Azure Conditional Access to support complaint devices.

16. Calendar attachments

Ivanti Email+ now supports attachments for the **Calendar** events. This feature is supported for the following:

- Primary email accounts
- Additional email accounts
- Delegated calendar
- Shared calendar

Configure the following to enable calendar attachment:

- **EAS16**: Primary and Secondary accounts
- **EWS**: Delegated and Shared Calendars

> You don't need to set up both EAS16 and EWS together as they can be enabled separately.

If **EAS16** is added to **Disabled Features**, attachments are disabled only for **Primary** and **Secondary** accounts.

Configure **EWS** to use **Delegated** or **Shared** calendar features.

You can add, remove, and view attachments in both single and recurring calendar events. Different file formats such as documents, images, and zip archives are supported.

You can select and upload multiple files as an attachment to your events. There is no restriction on the number of files attached but it should not exceed the size that is configured as per the **Max attachment size (MB)** restriction.

> An **Attachment size warning** dialog box is displayed if the max attachment size is exceeded.

The attachments are synced with the calendar event when the invite is sent. You can add attachments in offline mode; it will automatically sync when the device is online.

Adding files to calendar events

Procedure

To attach files to your calendar events, follow these steps:

1. In the Email+ app, go to **Calendar > New Event**.
2. Enter **Event Name**.
3. Click **Add Attachments**.
4. Browse for the file you want to attach and select it.
5. Under **Add Attachments**, selected files are displayed.
6. Click **Save** to create the calendar event with the attachment.

Viewing and editing event details

Procedure

To view and edit the details of an event, follow these steps:

1. In the Email+ app, go to **Calendar** tab. A list of saved events is displayed.

2. Select the event you want to view. The **View Event** page is displayed.

3. Click **Edit** to modify the event.

17. Microsoft Teams Integration in Email+ Calendar

Ivanti Email+ for Android devices now supports Microsoft Teams from calendar screen. This feature enables you to add Microsoft Teams meeting links directly into your calendar events with a toggle, removing the need to switch between different applications such as Outlook or the Teams application. Currently, support is available only for Microsoft Office 365 servers as it uses Graph API.

Configuring Microsoft Teams in Email+ Calendar

To configure Microsoft Teams, use the following key-value pairs:

- Add **microsoft_teams_meetings** under **App Restriction** (Optional Features) from MDM server as admin.
- Add app restriction host under **Exchange host for Graph** with value **graph.microsoft.com** to enable Microsoft Teams feature.

Joining a teams meeting

To join a meeting perform the following steps:

Procedure

1. In the Email+ app, open the event in your calendar.
2. Click Teams meeting link in the **Notes** section, or use the **Join** button.
3. The meeting will open in your browser or the Microsoft Teams app (if installed).

> Joining Microsoft Teams meetings is available for all accounts

> Delegated accounts cannot create Microsoft Teams meetings.

18. Main configuration steps for Ivanti Email+ for Android AppConnect (Ivanti EPMM)

Following are the main steps for configuring and deploying Email+ for Android AppConnect on Ivanti EPMM:

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

Adding Ivanti Email+ for Android AppConnect and Secure Apps Manager to Ivanti EPMM

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 Ivanti EPMM, 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 Ivanti EPMM Admin Portal, go to Apps > App Catalog > Add+ > In-House. (Prior to Ivanti EPMM 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 Ivanti EPMM**.

Related topics

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

Enabling third-party AppConnect apps in Ivanti EPMM

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

Procedure

1. In the Ivanti EPMM 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 Ivanti EPMM**.

Configuring the AppConnect global policy in Ivanti EPMM

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.

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

> 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 Ivanti EPMM 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 Ivanti EPMM**.

Related topics

For general details on the AppConnect global policy, see “Configuring the AppConnect global policy” in the Ivanti AppConnect for Ivanti EPMM Guide and Ivanti Tunnel for Android Guide.

Configuring the AppConnect container policy in Ivanti EPMM

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 Ivanti EPMM, Ivanti EPMM automatically creates an AppConnect container policy for the app. Create an AppConnect container policy, if you want to apply different settings to different devices.
- Make sure only one AppConnect container policy for Email+ is applied to each device.
- Ivanti EPMM keeps in sync the labels that you apply to the app and the labels that you apply to the AppConnect container policy that Ivanti EPMM automatically created.

> When you apply Email+ to a label, Ivanti EPMM 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 Ivanti EPMM Admin Portal, go to Policies & Configs > Configurations.
2. Click Add New > AppConnect > Container Policy.
3. Alternatively, edit the automatically-created AppConnect container Policy for Email+.
4. Enter a name for the policy.
5. Enter a description for the policy.
6. In the Application field, choose the Email+.
7. Select Allow Screen Capture if you want to override the default restriction on screen capture.
8. 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.
9. Click Save.

Next steps

- If you created a new container policy, continue to **Applying the container policy to labels in Ivanti EPMM**.
- If you edited the automatically-created AppConnect container policy, continue to **Configuring an AppConnect app configuration for Ivanti Email+ in Ivanti EPMM**.

Applying the container policy to labels in Ivanti EPMM

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 Ivanti EPMM**.

Removing labels from the automatically-created AppConnect container policy in Ivanti EPMM

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 Ivanti Email+ in Ivanti EPMM**.

Configuring an AppConnect app configuration for Ivanti Email+ in Ivanti EPMM

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.

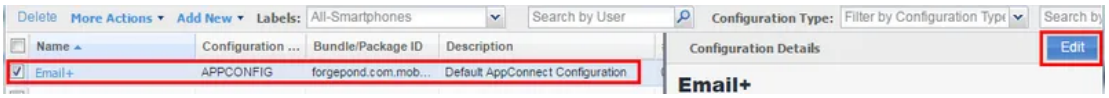
The default configuration contains the bundle ID for the app and a set of default key-value pairs that can be edited or deleted. You can also configure additional key-value pairs.

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

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 Ivanti EPMM 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.



1. 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 Ivanti Email+ (Android AppConnect)**.

Creating a new AppConnect app configuration for Ivanti 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 Ivanti 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.

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 To configure AppTunnel for Android AppConnect, see **Configuring Email+ with AppTunnel for Android AppConnect**. Email+ app might use AppTunnel as VPN if the email_exhcnage_host KVP is set as the ActiveSync server and if this server is not accessible from public network. AppTunnel is not used if Standalone Sentry used in the email_exchange_host KVP. 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 Ivanti EPMM

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

Procedure

1. In the Ivanti EPMM 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 Ivanti Sentry Guide for Ivanti EPMM.

19. Main configuration steps for Email+ for Android AppConnect (Ivanti Neurons for MDM)

Following are the main steps for configuring and deploying Email+ for Android AppConnect on Ivanti Neurons for MDM:

1. **Adding Email+ for Android AppConnect and Secure Apps Manager to Ivanti Neurons for MDM**.
2. **Configuring Email+ for Android AppConnect in Ivanti Neurons for MDM**.

Adding Email+ for Android AppConnect and Secure Apps Manager to Ivanti Neurons for MDM

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

Procedure

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

Next steps

- **Configuring Email+ for Android AppConnect in Ivanti Neurons for MDM**.

Related topics

For details on adding in-house apps for Android, see the Ivanti Neurons for MDM Administrator Guide or click on Help in Ivanti Neurons for MDM.

Configuring Email+ for Android AppConnect in Ivanti Neurons for MDM

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

Ivanti, Inc recommends changing to the default values as listed in **Change default values to recommended value** and **Delete recommended default key-value pairs**.

Key	Default value	Recommended value
email_device_id	$DEVICE_UUID_NO_DASHES$	$
email_exchange_username	$USERID$	$
email_address	$EMAIL$	$

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

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 Ivanti Email+ (Android AppConnect)**.

20. Configuring Email+ with AppTunnel for Android AppConnect

Configure Email+ with AppTunnel to setup access to Exchange server through Exchange Web Services (EWS) protocol and to support Email+ configuration when VPN access is required.

Before you begin

Configure Email+ AppConnect

The following steps describe how to configure AppTunnel with Standalone Sentry.

Procedure

1. In the Ivanti EPMM Admin Portal, go to **Services > Sentry > Add New > Standalone Sentry**.
2. In the **New Standalone Sentry** window, enter the **Sentry Hostname / IP**.
3. Select the **Enable AppTunnel** checkbox, and deselect **Enable ActiveSync** .
   If Enable AppTunnel is enabled, other Sentry services such as Kerberos Proxy and Email+ Notification Service are disabled.
4. In the **Device Authentication Configuration** section:
   - Select **Identity Certificate** from the drop-down menu.
   - Upload Local CA to the **Trusted Root Certificate Upload** field.
5. In the **AppTunnel Configuration** section, add **<TCP_ANY>** as AppTunnel service in **Services.**
6. Go to **Policies & Configs > Add New > Certificate Enrolment > Local**. As Local CAs select Local CA uploaded to Sentry.

Configuring AppTunnel rules for Email+

The following steps describe how to configure AppTunnel rules for Email+.

Procedure

1. In the Admin Portal, go to **Policies & Configs > Configurations**.
2. Select the **Email+ configuration** and click **Edit**.
3. In the **AppTunnel Rules** section, create new rules as follows:

Item	Description
AppTunnel Rules	
Sentry	Select the Standalone Sentry that you want to tunnel the URLs listed in this AppTunnel entry. The drop-down list contains all Standalone Sentrys that are configured to support AppTunnel.
Service	Select a Service Name from the drop-down list. This service name specifies an AppTunnel service configured in the App Tunneling Configuration section of the specified Sentry.
URL Wildcard	Enter one of the following: • A content server's hostname Example: finance.yourcompany.com • A hostname with wildcards. The wildcard character is Example: *.yourcompanyname.com If you want finer granularity regarding what requests the Standalone Sentry tunnels, configure multiple AppTunnel rows.
Port	Enter the port number that Email+ requests to access. App data is tunneled only if the app's request matches the hostname in the URL Wildcard field and this port number. If a port number is not configured, for http and https traffic, the default port is used. The default port used for http is 80 and the default port used for https is 443.

4. In the **AppTunnel Rules** section, go to **Identity Certificate** and select the certificate that you configured in Step 6 from the drop-down menu.

> After configuring and successfully connecting the Email+ app with AppTunnel, the Tunnel record appears in **Apps > App Tunnels**.

For more information on configuring Standalone Sentry for AppTunnel, see **Standalone Sentry for AppTunnel** section in the Ivanti Sentry Guide for Ivanti EPMM

21. Documentation resources

Product documentation is available on the **Ivanti documentation website**, help.ivanti.com. You can directly access Email+ for iOS documentation at **this link**.

To use the documentation:

1. Navigate to the **Ivanti documentation website**.
2. Optionally, select a product category and language.
3. Enter a search term.
4. Select a product from the results.
5. Click the associated documentation links.

> If you have an Ivanti Neurons for MDM deployment, the *Ivanti Neurons for MDM Administrator Guide* is also available from your instance of Ivanti Neurons for MDM through the Help link in the user interface. See **Accessing online help**.