citrix

Secure Mail

Contents

Secure Mail overview

December 2, 2020

Citrix Secure Mail lets users manage their email, calendars, and contacts on their mobile phones and tablets. To maintain continuity from Microsoft Outlook or IBM Notes accounts, Secure Mail syncs with Microsoft Exchange Server and IBM Notes Traveler Server.

As part of the Citrix suite of apps, Secure Mail benefits from single sign-on (SSO) compatibility with Citrix Secure Hub. After users sign on to Secure Hub, they can move seamlessly into Secure Mail without having to reenter their user names and passwords. You can configure Secure Mail to be pushed to users' devices automatically when the devices enroll in Secure Hub, or users can add the app from the Store.

> **Note:**
>
> Support for Exchange Server 2010 ended on October 13, 2020.

Secure Mail is compatible with:

- Exchange Server 2019 Cumulative Update 7
- Exchange Server 2019 Cumulative Update 6
- Exchange Server 2019 Cumulative Update 5
- Exchange Server 2016 Cumulative Update 18
- Exchange Server 2016 Cumulative Update 17
- Exchange Server 2016 Cumulative Update 16
- Exchange Server 2016 Cumulative Update 13
- Exchange Server 2013 Cumulative Update 23
- Exchange Server 2013 Cumulative Update 22
- Exchange Server 2013 Cumulative Update 21
- IBM Domino Mail Server version 10.0.1
- IBM Domino Mail Server version 9.0.1 FP10 HF197
- IBM Lotus Notes Traveler version 10.0.1.0 build 201811191126_20
- IBM Lotus Notes Traveler version 9.0.1.21
- Microsoft Office 365 (Exchange Online)

To begin, download Secure Mail and other Endpoint Management components from Citrix Endpoint Management Downloads.

For Secure Mail and other mobility app system requirements, see System requirements.

For information about notifications in Secure Mail for iOS and Android when the app is running in the background or closed, see Push notifications for Secure Mail.

For iOS features supported on Secure Mail, see iOS features for Secure Mail.

For Android features supported on Secure Mail, see Android features for Secure Mail.

For iOS and Android features supported on Secure Mail, see iOS and Android features for Secure Mail.

For user help documentation, see the Citrix Secure Mail page in the Citrix User Help Center.

What's new in Secure Mail

January 13, 2021

The following sections list the new features in current and earlier releases of Secure Mail.

For user help documentation, see the Citrix Secure Mail page in the Citrix User Help Center.

> **Note:**
>
> Support is ending for the Android 6.x and iOS 11.x versions of Secure Hub, Secure Mail, Secure Web, and Citrix Workspace app in June 2020.

What's new in the current version

Secure Mail 21.1.0

This release includes bug fixes.

What's new in earlier versions

Secure Mail 20.12.0

Secure Mail for iOS

This release includes bug fixes.

Secure Mail 20.11.0

> **Note:**
>
> Support for Exchange Server 2010 ended on October 13, 2020.

Secure Mail 20.10.5

Secure Mail for iOS

This release includes bug fixes.

Secure Mail for Android

Support for AndroidX libraries. As per Google's recommendation, Secure Mail supports the **AndroidX** libraries, which are a replacement for the **android.support**-packaged libraries.

Secure Mail 20.10.0

From this release onward, Secure Mail includes support for Exchange Server 2019 Cumulative Update 7 and Exchange Server 2016 Cumulative Update 18.

Secure Mail for iOS

Join Microsoft Teams meetings from Secure Mail. In Secure Mail for iOS, you can join Microsoft Teams (MS Teams) meetings directly from invitations in the Calendar. If the MS Teams app is installed, then the app opens and you join the meeting. When the app is not installed, you see an option to go the App Store to install MS Teams. For meetings in the https://teams.microsoft.com/l/meetup-join/meetinglink format, the app opens and you join the meeting directly.

> **Note:**
>
> Ensure that your admin includes `+^msteams:` in the Allowed URLs policy. For details, see App interaction (outbound URL).

Secure Mail for Android

- **Join Microsoft Teams meetings from Secure Mail.** In Secure Mail for Android, you can join Microsoft Teams (MS Teams) meetings directly from invitations in the Calendar. If the MS Teams app is installed, then the app opens and you join the meeting. When the app is not installed, you see an option to go the Google Play to install MS Teams. For meetings in the https://teams.microsoft.com/l/meetup-join/meetinglink format, the app opens and you join the meeting directly.

  > **Note:**
  >
  > Ensure that your admin includes `{ action=android.intent.action.VIEW scheme=msteams package=com.microsoft.teams }` in the Restricted Open-In exception list policy. For details, see App interaction.

- Secure Mail supports Google Play's current target API requirements for Android 10.

Secure Mail 20.9.5

Secure Mail for Android

This release includes bug fixes.

Secure Mail 20.9.0

Support for Azure Government Cloud Computing. Secure Mail for iOS and Android supports Government Cloud Computing (GCC) High for modern authentication (OAuth) on the Azure Active Directory tenant. Secure Mail is registered as an endpoint on the GCC High, to meet the mandatory requirement by Microsoft for all the GCC High service. For details, see What's new for Azure Active Directory in Microsoft 365 Government.

With this change, you are routed to GCC High on the Azure Active Directory tenant for authentication. And the admin is required to allow permissions for Secure Mail on the Azure Active Directory tenant.

Prerequisites

Ensure that the global admin of Azure Active Directory performs the following:

- Download the latest version of Secure Mail on your device.
- Configure your Exchange account on the Secure Mail app, and allow app permission on Azure Active Directory for all users to sign in. Refer to the following screen.

> **Note:**
>
> These steps are specific only to the global admins as a one-time requirement. Once the app is granted access, you can simply upgrade from the App Store.

After the upgrade

After an upgrade, you are prompted for reauthorization after the expiration of the refresh token, which redirects you to GCC High on Azure Active Directory. Validate the preceding workflow to ensure that the authorization request is sent to GCC High on Azure Active Directory.

You can validate the workflow in one of the following ways:

- Secure Mail with app name **Secure Mail-GCC High** appears on the sign-in page in your Azure Active Directory tenant.
- Check the Secure Mail logs to confirm whether the redirects occur via https://login.microsoftonline.us after reauthentication.

Secure Mail 20.8.5

Secure Mail for Android

Secure Mail for Android supports Android 11.

Secure Mail 20.8.0

From this release onward, Secure Mail includes support for Exchange Server 2019 Cumulative Update 6 and Exchange Server 2016 Cumulative Update 17.

Secure Mail for Android

Dual mode for Android release of Secure Mail. A mobile application management (MAM) SDK is available to replace areas of MDX functionality that aren't covered by iOS and Android platforms. The MDX wrapping technology is scheduled to reach end of life (EOL) in September 2021. To continue managing your enterprise applications, you must incorporate the MAM SDK.

From version 20.8.0, Android apps are released with the MDX and MAM SDK to prepare for the MDX EOL strategy mentioned earlier. The MDX dual mode is intended to provide a way to transition to new MAM SDKs from the legacy MDX Toolkit. Using dual mode allows you to either continue managing apps using MDX Toolkit (now Legacy MDX) or switch to the new MAM SDK for app management.

Once you switch to the MAM SDK for app management, Citrix implements further changes and it does not require any action from the administrators.

For more details about the MAM SDK (Preview), see the following articles:

- MAM SDK Overview
- Citrix Developer section on Device Management
- Citrix blog post
- Download SDK when you sign on to Citrix downloads

Prerequisites

For a successful deployment of the dual mode feature, ensure the following:

- Update your Citrix Endpoint Management to versions 10.12 RP2 and later, or 10.11 RP5 and later.
- Update your mobile apps to version 20.8.0 or later.
- Update the policies file to version 20.8.0 or later.
- If your organization uses third-party apps, make sure to incorporate the MAM SDK into your third-party apps before you switch to the MAM SDK option for your Citrix mobile productivity apps. All of your managed apps must be moved to the MAM SDK at one time.

> **Note:**
>
> MAM SDK is supported for all cloud-based customers.

Limitations

- MAM SDK supports only apps published under the Android Enterprise platform on your Citrix Endpoint Management deployment. For the newly published apps, the default encryption is platform-based encryption.
- MAM SDK only supports platform-based encryption, and not MDX encryption.
- If you don't update Citrix Endpoint Management, and the policy files are running on version 20.8.0 and later for the mobile apps, then duplicate entries of the Networking policy are created for Secure Mail.

When you configure Secure Mail in Citrix Endpoint Management, the dual mode feature allows you to either continue managing apps using the MDX Toolkit (now **Legacy MDX**) or switch to the new **MAM SDK** for app management. Citrix recommends that you switch to **MAM SDK**, as MAM SDKs are more modular and intend to allow you to use only a subset of the MDX functionality that your organization uses.

You get the following options for policy settings in the **MDX or MAM SDK policy container**:

- **MAM SDK**
- **Legacy MDX**

In the **MDX or MAM SDK policy container** policy, you can only change your option from **Legacy MDX** to **MAM SDK**. The option to switch from **MAM SDK** to **Legacy MDX** is not allowed, and you need to republish the app. The default value is **Legacy MDX**. Ensure that you set the same policy mode for both Secure Mail and Secure Web running on the same device. You cannot have two different modes running on the same device.

Secure Mail for iOS

Sync optimization for Mailbox. In Secure Mail for iOS, the **Mailbox** synchronization is improved to provide a better user experience. The **Calendar** and the **Contacts** are synced more quickly. Emails that are older than 3 weeks are truncated to reduce the sync time. You can view the complete email when you open it.

Secure Mail 20.7.5

> **Note:**
>
> Support for Android 6.x ended on June 30, 2020.

For latest information on mobile productivity apps, see the article Recent announcements.

Secure Mail 20.7.0

This release includes bug fixes.

Secure Mail 20.6.5

This release includes bug fixes.

Secure Mail 20.6.0

This release includes bug fixes.

Secure Mail 20.5.0

This release includes bug fixes.

Secure Mail 20.4.5

Secure Mail for Android

From this release onward, Secure Mail includes support for Exchange Server 2019 Cumulative Update 5 and Exchange Server 2016 Cumulative Update 16.

Secure Mail 20.4.0

From this release onward, Secure Mail includes support for Exchange Server 2016 Cumulative Update 15 and Exchange Server 2013 Cumulative Update 23.

Secure Mail 20.3.0

Secure Mail for Android

Create folders in Contacts. In Secure Mail for Android, you can add, edit, and delete folders in the **Contacts** section of your email account.

Secure Mail for iOS

This release includes bug fixes.

Secure Mail 20.2.0

Secure Mail for Android

Minimize drafts

In Secure Mail for Android, you can minimize a draft while you're composing an email and navigate within the app. For user help documentation on this feature, see the Citrix User Help Center article Minimize a draft email.

Secure Mail 20.1.5

Secure Mail for iOS

From this release onward, Secure Mail includes support for Exchange Server 2019 Cumulative Update 4.

Secure Mail for Android

- **Two-way contact sync.** In Secure Mail for Android, you can create, edit, and delete Secure Mail contacts from your local contacts list.
- **Support for ICS files.** In Secure Mail for Android, you can preview the ICS files that you receive as attachments, and import it to your calendar as Events.
- From this release onward, Secure Mail includes support for Exchange Server 2019 Cumulative Update 4.

Secure Mail 20.1.0

From this release onward, Secure Mail includes support for Exchange Server 2016 Cumulative Update 14

Secure Mail 19.12.5

Secure Mail for iOS

This release includes bug fixes.

Secure Mail for Android

Undo sent mails. In Secure Mail for Android you can undo a sent mail. Once you tap the **Send** button, you get a toast message that allows you to undo the sent action. Tap **Undo** to revert the sent action and edit the mail, mail recipients, attach or remove attachments, or discard the mail.

Attachments sync in Drafts folder. In Secure Mail for Android, when the **Drafts** folder is synced, the attachments are also synced and they are available across all your devices. This feature is available on devices running Exchange ActiveSync version 16 or later.

Secure Mail 19.11.5

Secure Mail for iOS

Contact picture in Secure Mail. In Secure Mail for iOS, view a picture of a contact when you add recipients in emails or meeting invites. For user help documentation on this feature, see the Citrix User Help Center article Show pictures of your contacts.

Secure Mail for Android

In-app view of PDF files. In Secure Mail for Android, you can view PDF files within the app, along with bookmarks and annotations. Also available is the enhanced view of other Microsoft Office attachments.

Secure Mail for iOS 19.10.6

This release includes bug fixes.

Secure Mail 19.10.5

Secure Mail for iOS

Minimize drafts. In Secure Mail for iOS, you can minimize a draft while you're composing an email and navigate within the app. This feature is available on devices running iOS 13 and later. For user help documentation on this feature, see the Citrix User Help Center article Minimize a draft email.

Secure Mail for Android

This release includes bug fixes.

Secure Mail 19.10.0

Use the Office 365 Exchange Server policy to define the Office 365 server address. In Secure Mail iOS and Android, a new policy called **Office 365 Exchange Server** is added under the section OAuth Support for Office 365. With this policy you can define the host name for the Office 365 mailbox present on Cloud. This policy also enables support of Office 365 for Government agencies. The host name is a single value such as *outlook.office365.com*. The default value is *outlook.office365.com*.

Secure Mail iOS and Android support encryption management. Encryption management allows you to use modern device platform security while also ensuring the device remains in a sufficient state to use platform security effectively. By using encryption management, you eliminate local data encryption redundancy since file system encryption is provided by the iOS or Android platform. To

enable this feature, an admin must configure the **Encryption type** MDX policy to **Platform encryption with compliance enforcement** in the Citrix Endpoint Management console.

To use the encryption management feature, in the Citrix Endpoint Management console, set the **Encryption type** policy to **Platform encryption with compliance enforcement**. This enables encryption management and all the existing encrypted application data on users' devices seamlessly transition to a state that is encrypted by the device and not by MDX. During this transition, the app is paused for a one-time data migration. Upon successful migration, responsibility for encryption of locally stored data is transferred from MDX to the device platform. MDX continues to check compliance of the device upon each app launch. This feature works in both MDM + MAM and MAM-only environments.

When you set the **Encryption type** policy to **Platform encryption with compliance enforcement**, the new policy supersedes your existing MDX Encryption.

For details about the encryption management MDX policies for Secure Mail, see the **Encryption** section in:

- MDX policies for mobile productivity apps for Android
- MDX policies for mobile productivity apps for iOS

When a device falls below the minimum compliance requirements, the **Non-compliant device behavior** policy allows you to select what action is taken:

- **Allow app** – Allow the app to run normally.
- **Allow app after warning** – Warn the user that an app does not meet the minimum compliance requirements and allows the app to run. This is the default value.
- **Block app** – Block the app from running.

Devices running iOS

The following criteria determine whether a device meets the minimum compliance requirements for devices running iOS:

- iOS 10 - An app is running operation system version that is greater than or equal to the specified version.
- Debugger access - An app does not have debugging enabled.
- Jailbroken device - An app is not running on a jailbroken device.
- Device passcode - Device passcode is **ON**.
- Data sharing - Data sharing is not enabled for the app.

Devices running Android

The following criteria determine whether a device meets the minimum compliance requirements for devices running Android:

- Android SDK 24 (Android 7 Nougat) - An app is running operation system version that is greater than or equal to the specified version.
- Debugger Access - An app does not have debugging enabled.
- Rooted devices - An app is not running on a rooted device.
- Device lock - Device passcode is **ON**.
- Device encrypted - An app is running on an encrypted device.

Secure Mail 19.9.5

Secure Mail for iOS

Support for ICS files. In Secure Mail for iOS, you can import ICS files that you receive as attachments to your calendar as an event.

Secure Mail for Android

This release includes bug fixes.

Secure Mail 19.9.0

From this release onward, Secure Mail includes support for the following servers:

- Exchange Server 2016 Cumulative Update 13
- IBM Lotus Notes Traveler version 10.0.1.0 build 201811191126_20
- IBM Domino Mail Server version 10.0.1

Secure Mail for iOS

- Secure Mail for iOS supports iOS 13.
- **Reporting phishing emails with MIME headers.** In Secure Mail for iOS, when a user reports a phishing mail, an EML file is generated as an attachment corresponding to that mail. Admins receive this mail and can view the MIME headers associated with the reported mail. To enable this feature, an admin must configure the Report Phishing Email Address policy and set the Report Phishing Mechanism as Report Via Attachment in the Citrix Endpoint Management console. For details, see Report phishing email as an attachment.
- **Support for responsive emails.** Secure Mail for iOS has been optimized to deliver responsive email. Previously, email content with large tables or images were rendered incorrectly. This feature delivers email content as more readable on all supported devices irrespective of the email format and size.
- **Drag and drop calendar events.** In Secure Mail for iOS, you can change the time of an existing calendar event by dragging and dropping the event. Drag the event and drop it to the desired time slot for the same day, or across days to update.

- **Auto Advance.** In Secure Mail for iOS, when you delete a message in **Conversations**, you can choose which message you return to. To use this feature, navigate to **Settings > Auto Advance**. Then, select your preference from the available choices. For user help documentation on this feature, see the Citrix User Help Center article Delete and auto advance to an email in Conversations.
- **Support for WkWebView.** Secure Mail for iOS supports WkWebView. This feature improves the way Secure Mail email and Calendar events are rendered on your device.

Secure Mail for Android

From this release, Secure Mail for Android is only supported on devices running Android 6 or later.

Secure Mail for Android 19.8.5

This release includes bug fixes.

Secure Mail 19.8.0

Secure Mail for iOS

This release includes performance enhancements and bug fixes.

Secure Mail for Android

- Support for Android Q.
- **Support for 64-bit apps for Google Play.** Secure Mail for Android supports 64-bit architectures.
- **Improvements to the Pull to refresh UI in Secure Mail for Android.** In keeping with Material Design guidelines, we have made minor improvements to the **Pull to refresh** feature. The sync timestamp is available at the bottom of the screen when you tap the hamburger icon.

Secure Mail 19.7.5

Secure Mail for iOS

- **Drafts folder auto-sync.** In Secure Mail for iOS, the drafts folder is automatically synced and your drafts are available across all your devices. This feature is available on setups running Exchange ActiveSync v16 or later. For user help documentation on this feature, see the Citrix User Help Center article, Drafts folder auto-sync.

- **Secure Mail for iOS supports single sign-on when you are using Microsoft Intune in MDM + MAM mode.** To be able to use this feature, ensure that Microsoft Authenticator app is installed on your device. For more information about installing the Microsoft Authenticator app, see **Download and install the Microsoft Authenticator** app on *Docs.microsoft.com*.

Secure Mail for Android

> Note:
>
> Citrix recommends that you upgrade to Secure Mail version 19.7.5 before you upgrade your OS to Android Q.

- **Use Web SSO for tunneling policy for setups running Modern authentication with Microsoft Office 365.** In Secure Mail for Android, a new policy called **Use Web SSO for tunneling** is added. With this policy you can tunnel OAuth traffic to go over Secure Browse. To do so:
  - Set **Use Web SSO for tunneling** policy to **On**.
  - Select the **Tunneled - Web SSO** option in the Network access policy.
  - Exclude any host names related to OAuth from the **Background services** policy.
- **Secure Mail for Android supports single sign-on when you are using Microsoft Intune in MDM + MAM mode.** To be able to use this feature, ensure that Intune Company Portal app is installed on your device. Once you log in to the Intune Company Portal app, you are able to use SSO in the MDM + MAM mode without having to reauthenticate in Secure Mail using your credentials.

Secure Mail 19.6.5

Secure Mail for iOS

Secure Mail for iOS version 19.6.5 includes performance enhancements and bug fixes. For the list of fixed and known issues, see Known and fixed issues.

Secure Mail for Android

- **Drag and drop calendar events.** In Secure Mail for Android, you can change the time of an existing calendar event by dragging and dropping the event. For user help documentation on this feature, see the Citrix User Help Center article, Change a calendar event time.
- **Support for responsive emails.** Secure Mail for Android has been optimized to deliver responsive email. Previously, email content with large tables or images were rendered incorrectly. This feature delivers email content is more readable on all supported devices irrespective of the email format and size.
- **Contact picture in Secure Mail.** In Secure Mail for Android, view image of the contact when you add recipients in emails or meeting invites. The image of the contact is displayed next to the

name. In case of multiple people with the same name, the image helps identifying the correct recipient when you add recipients in emails or meeting invites. To search for contacts that are not saved locally, enter a minimum of four characters of the recipient's name to display the image.

- **Widget for Calendar agenda.** In Secure Mail for Android, the **Calendar** agenda is available as a widget. From this widget, you can view the upcoming events in the **Calendar** for a week. This feature allows you to create a **Calendar** event, view an existing event and edit the details. The **Block screen capture** policy does not apply to the widget placed on the home screen. You can, however, disable the widget using the **Allow Calendar Agenda widget** policy.

Secure Mail 19.5.5

Secure Mail for Android

Secure Mail for Android version 19.5.5 includes performance enhancements and bug fixes. For the list of fixed and known issues, see Known and fixed issues.

Secure Mail for iOS

- Secure Mail for iOS supports single sign-on when you are using Microsoft Intune in MDM + MAM mode. To be able to use this feature, ensure that Microsoft Authenticator app is installed on your device. The Microsoft Authenticator app is available in app stores.
- **Support for Slack EMM:** Slack EMM is for Slack customers with Enterprise Mobility Management (EMM) enabled. Secure Mail for iOS supports the application **Slack EMM**, which allows admins to choose the integration of Secure Mail with either the **Slack** app or the **Slack EMM** app.

Secure Mail 19.5.0

Secure Mail for Android

Manage your feeds. In Secure Mail for Android, you can organize your **Feeds** card based on your requirements.

For more information about managing your feeds, see Manage your Feeds.

Drafts folder auto-sync. In Secure Mail for Android, the drafts folder is automatically synced and your drafts are available across all your devices. For user help documentation on this feature, including a video, see the Citrix User Help Center article, Drafts folder auto-sync.

Secure Mail for Android 19.4.6, 19.4.5, and 19.3.5

These releases include performance enhancements and bug fixes.

For the list of fixed and known issues, see Known and fixed issues.

Secure Mail 19.3.0

From this release onward, Secure Mail includes support for the following servers:

- Exchange Server 2019 Cumulative Update 1
- Exchange Server 2016 Cumulative Update 12
- Exchange Server 2013 Cumulative Update 22
- Exchange Server 2010 SP3 Update Rollup 26

For more information about the complete list of Secure Mail server compatibility, see Secure Mail overview.

Secure Mail for iOS

Manage your feeds. In Secure Mail for iOS, you can now organize your **Feeds** card based on your requirements.

> **Note:**
>
> This feature is not available on iPads.

For more information about managing your feeds, see Manage your Feeds.

Secure Mail for iOS and Android

Internal Domains. You can identify and edit email recipients that belong to external organizations. To use this feature, ensure that you have enabled the **Internal Domains** policy in Citrix Endpoint Management.

When you create, reply to, or forward an email, external recipients are highlighted in the mailing list. The **Contacts** icon appears as a warning at the bottom left of the screen. Tap the **Contacts** icon to modify the mailing list.

For more information about internal domains, see Internal domains.

Ergonomic improvements. The action buttons are moved from the top of the screen to the bottom for easy access. These changes are made to the **Inbox**, **Calendar**, and **Contacts** screens.

> **Note:**
>
> For devices running Android, the changes are made to **Inbox** and **Calendar** screens.

For more information about ergonomic improvements, see Ergonomic improvements.

Secure Mail 19.2.0

Secure Mail for iOS

This release includes performance enhancements and bug fixes.

For the list of fixed and known issues, see Known and fixed issues.

Secure Mail for Android

- **Enhancements to Contacts.** In Secure Mail for Android, when you tap **Contacts** and select a contact, the details of that contact appear under the **Contact** tab. When you tap the **Organization** tab, the organization hierarchy details, such as **MANAGER**, **DIRECT REPORTS**, and **PEERS**, appear. When you tap the more icon on the top right of the screen, the following options appear:
  - **Attach to Mail**
  - **Share**
  - **Delete**

  In the **Organization** tab, tap the more icon to the right of **MANAGER**, **DIRECT REPORTS**, or **PEERS**. Then, either create an email or calendar invite. The **To:** field of the email or calendar event is automatically populated with the details of **MANAGER**, **DIRECT REPORTS**, or **PEERS**.

  Prerequisites:

  Ensure that Exchange Web Services (EWS) is enabled on your Exchange Server.

  The contact details appear based on the organizational details fetched from Active Directory. For the correct details to appear for your contacts, ensure that your admin has configured your organizational hierarchy in Active Directory.

  > **Note:**
  >
  > This feature is not supported on IBM Lotus Notes server.

- **Network access policy**. In Secure Mail for Android, a new option called **Tunneled - Web SSO** is added to the Network Access MDX policy. Configuring this policy gives you the flexibility to tunnel internal traffic over Secure Browse and Secure Ticket Authority (STA) in parallel. You can also allow Secure Browse connections for authentication services, like NTLM, Okta, and Kerberos. When you initially configure STA, you must add individual FQDNs and ports of service addresses to the Background network services policy. If you configure the **Tunneled - Web SSO** option, however, you need not make these configurations.

To enable this policy for Secure Mail for Android in the Citrix Endpoint Management console:

1. Download and use the .mdx file for Android. For details see steps in Add an MDX app.
2. In the Network access policy, click **Tunneled – Web SSO** option. For more information, see App Network Access

Secure Mail for iOS 19.1.6

This release includes performance enhancements and bug fixes.

Secure Mail 19.1.5

From this release onward, Secure Mail includes support for the following servers:

- Exchange Server 2016 Cumulative Update 11
- Exchange Server 2010 SP3 Update Rollup 24

For more information about the complete list of Secure Mail-server compatibility, see Secure Mail overview.

Secure Mail 19.1.0

Secure Mail for iOS

- **Enhancements to Contacts.** In Secure Mail for iOS, when you tap **Contacts** and select a contact, the details of that contact appear under the **Contact** tab. When you tap the **Organization** tab, the organization hierarchy details, such as **Manager**, **Direct Reports**, and **Peers** appear. When you tap the more icon on the top right of the screen, the following options appear:
  - Edit
  - Add to VIP
  - Cancel

  In the **Organization** tab, you can tap the more icon to the right of **Manager**, **Direct Reports**, or **Peers**. This action allows you to either create an email or a calendar event. The **To:** field of the email or
  calendar event is automatically populated with the details of **Manager**, **Direct Reports**, or **Peers**. You can compose and send the email.

  Prerequisites:

  Ensure that Exchange Web Services (EWS) is enabled on your Exchange Server.

  The contact details appear based on the organizational details (Outlook contact) fetched from Active Directory. For the correct details to appear for your contacts, ensure that your admin has configured your organizational hierarchy in Active Directory.

  > **Note:**
  >
  > This feature is not supported on IBM Lotus Notes server.

- **Export Meeting Time and Location to your native calendar.** In Secure Mail for iOS, a new value **Meeting Time, Location** is added to **Export Calendar** MDX policy. This enhancement

allows you to export meeting time and location of Secure Mail calendar events to your native calendar.

- Secure Mail for iOS supports rich push notifications on setups running Microsoft Enterprise Mobility + Security (EMS)/Intune with modern authentication (O365).

  To enable the rich push notifications feature, ensure that the following prerequisites are met:

  - In the Endpoint Management console, set **Push notifications** to ON.
  - The **Network access policy** is set to **Unrestricted**.
  - The **Control locked screen notifications** policy is set to **Allow** or **Email sender or event title**.
  - Navigate to **Secure Mail** > **Settings** > **Notifications** and then enable **Mail Notifications**.

- Secure Mail users can use the Zoom app to join meetings. For information about configuring the required policies to use the Zoom app, see Joining meetings from calendar.
- This release includes support for iPad Pro 11 inch and iPad Pro 12.9 inch.

Secure Mail for Android

- **Enhancement to attachments.** In Secure Mail for Android, viewing attachments is simplified. For a better experience, inessential steps are removed, while attachment options that existed in the earlier releases are retained.

  You can view attachments within Secure Mail app. The attachment opens directly, if it can be viewed using Secure Mail. If the attachment cannot be viewed using Secure Mail, a list of apps appears. You can select the required app to view the attachment. For details, see Viewing attachments.

- Secure Mail users can use the Zoom app to join meetings. For information about configuring the required policies to use the Zoom app, see Joining meetings from calendar.
- **Export Meeting Time and Location to your native calendar.** In Secure Mail for Android, a value **Meeting Time, Location** is added to **Export Calendar** MDX policy. This allows you to export meeting time and location of Secure Mail calendar events to your native calendar.

> **Note:**
>
> Support for Android 5.x ended on December 31, 2018.

Secure Mail 18.12.0

This release includes performance enhancements and bug fixes.

For the list of fixed and known issues, see Known and fixed issues.

Secure Mail 18.11.5

Secure Mail for Android

- **Report phishing emails with ActiveSync headers.** In Secure Mail for Android, when a user reports a phishing mail, an EML file is generated as an attachment corresponding to that mail. Admins receive this mail and can view the ActiveSync headers associated with the reported mail.

  To enable this feature, an admin must configure the **Report Phishing Email Address** policy and set **Report Phishing Mechanism** to **Report Via Attachment**. The admin configures these settings in the Citrix Endpoint Management console. For details about configuring MDX policies for Secure Mail, see MDX policies for mobile productivity apps.

- **Print emails and calendar events.** In Secure Mail for Android, you can print emails and calendar events from your Android device. This print functionality uses Android Print framework. For details, see Print emails and calendar events.

- **Feeds from your Manager.** In Secure Mail for Android, you can view emails from your manager in the **Feeds** screen. Up to five emails appear under the **From Your Manager** feeds, based on your **Sync mail period** settings. To view more emails from your manager, tap **See all**.

  Prerequisites:

  Ensure that Exchange Web Services (EWS) is enabled on your Exchange Server.

  The manager card appears based on the organizational details (Outlook contact) fetched from Active Directory. For the correct details to appear in the manager feed, ensure that your admin has configured your organizational hierarchy in Active Directory.

  > **Note:**
  >
  > This feature is not supported on IBM Lotus Notes server.

Secure Mail 18.11.1

> Important:
>
> The following issue is fixed in Secure Mail for Android 18.11.1
>
> In Secure Mail for Android with connections to IBM Notes Traveler 9.0.1 SP 10, emails with attachments remain in the Outbox. [CXM-58962]

Secure Mail 18.11.0

Secure Mail for Android

- **Subfolder notifications.** In Secure Mail for Android, you can receive mail notifications from subfolders of your mail account. For details, see Subfolder notifications.

- **Updates to background services in Secure Mail for Android.** To meet the Google Play Background Execution Limits requirement on devices running Android 8.0 (API level 26) or later, we have upgraded Secure Mail background services. For uninterrupted mail sync and notifications on your device, enable Firebase Cloud Messaging (FCM) service push notifications. For more details about enabling FCM-based push notifications, see Push notifications for Secure Mail

Ensure that you turn on **Mail notifications** in Secure Mail settings on your device. For more details about this update, see this Support Knowledge Center article.

Limitations:

- If you have not enabled FCM-based push notifications, background sync occurs once in every 15 minutes. This interval varies depending on whether the app is running in the background or the foreground.
- When users manually update the time from device settings, the date in the calendar widget does not update automatically.

Secure Mail for iOS

- **Support for iOS 12.1.** Secure Mail for iOS supports iOS version 12.1.
- **Enhancements to rich push notification failure messages.** In Secure Mail for iOS, appropriate push notification failure messages appear in the notification center on your device based on the type of notification failure. For details, see Push notification failure messages in Secure Mail for iOS, see Push notification failure messages in Secure Mail for iOS.
- **Feeds from your Manager.** In Secure Mail for iOS, you can view emails from your manager in the **Feeds** screen. Up to five emails appear under the **From Your Manager** feeds, based on your **Sync mail period** settings. To view more emails from your manager, tap **See all**.

  Prerequisites:

  Ensure that Exchange Web Services (EWS) is enabled on your Exchange Server.

  The manager card appears based on the organizational details (Outlook contact) fetched from Active Directory. For the correct details to appear in the manager feed, ensure that your admin has configured your organizational hierarchy in Active Directory.

  > **Note:**
  >
  > This feature is not supported on IBM Lotus Notes server.

Secure Mail 18.10.5

- **Secure Mail integration with Slack (Preview):** You can now take your email conversation over to Slack app on devices running iOS or Android. For details, see Secure Mail integration with

Slack (Preview).

- **Enhancements to Feeds folder:** In Secure Mail for iOS, the following are enhancements to the existing Feeds folder:
  - View up to five upcoming meetings in your Feeds card.
  - Upcoming meetings for the next 24-hour period appear in the Feeds card and are categorized into **Today** and **Tomorrow** sections.

Secure Mail 18.10.0

- **Secure Mail notification channels for mail and calendar notifications:** On devices running Android O or later, you can use the notifications channel settings to manage how your email and calendar notifications are handled. This feature allows you to customize and manage your notifications. For details, see Notification channels.
- **Report phishing email (as a forward):** In Secure Mail for iOS, you can use the Report as phishing feature to report an email (as a forward) that you suspect of phishing. You can forward the suspicious messages to email addresses that admins configure in the policy. To enable this feature, an admin must configure the Report Phishing Email Address policy and set the **Report Phishing Mechanism** as **Report Via Forward**. For user help documentation on this feature, see the Citrix User Help Center article, Report a phishing email.

Secure Mail 18.9.0

- New version numbering scheme in the format "yy.mm.version." For example, version **18.9.0**
- **Report phishing email (as a forward):** In Secure Mail for Android, you can use the Report as phishing feature to report an email (as a forward) that you suspect of phishing. You can forward the suspicious messages to email addresses that admins configure. To enable this feature, an admin must configure the Report Phishing Email Address policy and set Report Phishing Mechanism as **Report Via Forward**. For user help documentation on this feature, see the Citrix User Help Center article, Report a phishing email.
- **Enhancements to Feed cards:** The following enhancements have been made to the existing **Feeds** folder, in Secure Mail for Android:
  - Meeting invites from all auto-synced folders appear in your Feeds card.
  - View up to five Upcoming meetings in your Feeds card.
  - Upcoming meetings now appear based on a 24-hour period starting from your current time. These meeting invites are categorized into **Today** and **Tomorrow**.
    In previous releases, upcoming meetings until the end of the day would appear in your feeds.

- **Export Secure Mail calendar events:** Secure Mail for Android and iOS allow you to export Secure Mail calendar events to your device's native calendar app. To enable this feature, tap **Settings** and drag the slider for Export Calendar Events to the right. For details, see Export Secure Mail calendar events.

Secure Mail 10.8.65

- **Available with iOS 12:** In Secure Mail for iOS, we support the Group Notifications feature. With this feature, conversations are grouped from a mail thread. You can quickly glance at grouped notifications on the lock screen of your device. Group Notification settings are enabled by default on the device.
- In Secure Mail for iOS, the **Save draft** and **Delete draft** buttons are larger. This enhancement makes it easier for customers to distinguish one option from the other.
- In Secure Mail for iOS, you can identify incoming calls from your Secure Mail contacts by enabling Secure Mail Caller ID in device **Settings**. On enabling these settings, when you get an incoming call, the device displays the App name with the Caller ID, such as "Secure Mail Caller ID: Joe Jay". For details, see Secure Mail Caller ID.

Secure Mail 10.8.60

- Secure Mail supports Android P.
- Secure Mail is now available in Polish.
- In Secure Mail for iOS, you can attach files to your email from iOS native Files app. For details, see iOS features.

Secure Mail 10.8.55

There are no new features in Secure Mail version 10.8.55. For fixed issues, see Known and fixed issues.

Secure Mail 10.8.50

Photo attachment improvements. In Secure Mail for iOS, you can attach photos easily by tapping the new **Gallery** icon. Tap the **Gallery** icon and select photos that you want to attach to your email.

Secure Mail feeds screen. Secure Mail for iOS and Android feature all your unread emails, meeting invites that require your attention, and your upcoming meetings in the **Feeds** screen.

Secure Mail 10.8.45

Folder sync. In Secure Mail for iOS and Android, you can tap the **Sync** icon to refresh all Secure Mail content. The **Sync** icon is present in Secure Mail slide outs such as Mailboxes, Calendars, Contacts,

and Attachments. When you tap the **Sync** icon, those folders that you have configured to auto refresh, such as Mailboxes, Calendars, Contacts, are updated. The timestamp of the last sync appears next to the **Sync** icon.

Photo attachment improvements. In Secure Mail for Android, you can attach photos easily by tapping the new **Gallery** icon. Tap the **Gallery** icon and select photos that you want to attach to your email.

Secure Mail 10.8.40

Support to search calendar. In Secure Mail for iOS, you can search the calendar for events, attendees, or any other text.

Secure Mail 10.8.35

The version for Secure Mail for iOS is 10.8.36.

- **Notification response options.** In Secure Mail for iOS, users can respond to meeting notifications, such as Accept, Decline, and Tentative. They can respond to message notifications with Reply and Delete.
- **Secure Mail for Android back button enhancements.** In Secure Mail for Android, you can tap the back button on your device to dismiss the expanded options of the Floating Action Button. If the Floating Action Button is in the expanded state, tapping the back button on your device collapses the response options. This action takes you back to the message or event details view.
- **In Secure Mail for Android, meeting response buttons appear within the email.** When you receive an email notification about meeting invites, you can respond to the invite by tapping on one of the following options:
  - Yes
  - Maybe
  - No

Secure Mail 10.8.25

Secure Mail for iOS now supports S/MIME for derived credentials: In order for this feature to work, you need to do the following:

- Select Derived Credential as the S/MIME certificate source. For details, see Derived credentials for iOS.
- Add the LDAP Attributes client property in Citrix Endpoint Management. Use the following information:
  - **Key:** SEND_LDAP_ATTRIBUTES

- **Value:** `userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme =${ user.samaccountname } ,displayName=${ user.displayName } ,mail= ${ user.mail }`

For steps on how to add a client property, for XenMobile Server, see Client properties and for Endpoint Management, see Client properties.

For more information about how devices enroll when using derived credentials, see Enrolling devices by using derived credentials.

1. On your Endpoint Management Console, navigate to **Configure > Apps**.
2. Select **Secure Mail** and then click **Edit**.
3. Under the iOS platform, for the S/MIME certificate source, select **Derived Credential**.

Secure Mail for iOS and Android have a revamped look and feel: We've made the user navigation simpler and more efficient. We've realigned the Secure Mail menu and action buttons in the form of a navigation bar. For a video demonstrating the user navigation changes, see:

The following figure shows the new navigation bar on iOS devices.

The following figure shows the new navigation bar on Android devices.

What's changed:

- The grabber icon has been removed. Secure Mail features, such as Mail, Calendar, Contacts, and Attachments, are now available as buttons in the footer tab bar. The following figure shows this change.

  > **Note:**
  >
  > On Android devices, the footer tab bar is not available after you open a mail item. For example, as shown in the following figure, if you open an email or a calendar event, the footer tab bar is not available.

- The **Settings** menu is available within all menus, such as Mail, Calendar, Contacts, and Attachments. To go to **Settings**, tap the hamburger icon and then tap the settings button available at the bottom right, as shown in the following figure.
- The **Search** icon replaces the Search bar and is available in the Inbox, Contacts, and Attachments views.
- On iOS devices, you can tap and hold on a mail item to select the item.
- You can tap the **Compose** floating action button to compose a new email, as shown in the following figure.
- The following menu options are now available on the top right of your screen:

  - **Sync options:** Tap the overflow icon on the top right and navigate to **More options > Sync** options to change your sync preferences.

    > **Note:**
    >
    > This option is available on Android devices only.

  - **Search icon:** Tap to search for an email.

- **Triage view icon:** Tap for triage view of the conversation.
- **Respond floating action button:** While viewing an email, tap to Forward, Reply All, or Reply, as shown in the following figure.
- While viewing an email, the following menu options are available from the top right of your screen:
  - **Flag:** Tap to flag the email.
  - **Mark As Unread:** Tap to mark email as unread.
  - **Delete:** Tap to delete the email.
  - **More options:** Tap the overflow icon to view other available actions, such as Move.

Calendar changes

- From the calendar, you can tap an event floating action button to create an event, as shown in the following figure.
- The following menu options are now available from the top right of your screen:
  - **Today:** Tap to view today's events.
  - **Search:** Tap to search for an event.
  - **Respond floating action button:** While viewing an event, tap to Forward, Reply All, or Reply.

When you view an event, the event response actions such as Yes, Maybe, and No are realigned and available below the event details.

Contacts changes

- You can tap a **Create New Contact** floating action button, as shown in the following figure.
- The **Search** menu option is now available from the top right of the screen. You can tap the option to search for a contact.
- While viewing a contact, the following menu options are available from the top right of your screen:

  On Android devices:

- **Edit:** Tap to edit the contact.
- **More options:** Tap the edit icon to view other available actions, such as Attach to Mail, Share, and Delete.

On iOS devices:

- **Edit:** Tap to edit the contact.
- **Share:** Tap the share icon to view other available actions, such as Share contact and Attach to Mail.

> **Note:**
>
> To delete a contact on iOS devices, select the contact, tap **Edit** and then tap **Delete** at the bottom of the screen, as shown in the following figure.

Attachments changes

The following menu options for attachments are now available from the top right of your screen:

- **Sort:** Tap the **Sort** icon and choose appropriate filters to sort attachments.
- **Search:** Tap to search for an attachment.

Secure Mail 10.8.20

- Secure Mail for iOS now supports the use of derived credentials for enrollment and authentication. For more information on derived credentials, see Derived Credentials for iOS.
- Secure Mail for iOS supports rich push notifications. Rich notifications ensure that you receive lock screen notifications for your inbox even when Secure Mail is not running in the background. This feature is supported on password-based authentication and client-based authentication setups. For details, see Rich push notifications.

  > **Note:**
  >
  > Due to the change in architecture to support the rich push notifications feature, the **VIP Only** mail notifications is no longer available.

- Secure Mail for Android, along with iOS now supports rich text signatures. You can use images or links in your email signature. For details, see Rich text signatures.

Secure Mail 10.8.15

- **Secure Mail for iOS now supports rich text signatures.** You can use images or links in your email signature. For details, see Rich text signatures.

- **Secure Mail supports Android Enterprise, formerly known as Android for Work**. You can create a separate work profile by using Android Enterprise apps in Secure Mail. For details, see Android Enterprise in Secure Mail.
- **Secure Mail renders embedded resources while viewing an email.** If the resources are present in your internal network, such as mails with image URLs that are internal links, Secure Mail connects to the internal network to fetch the content and render it.
- **Secure Mail supports modern authentication**. Modern authentication is OAuth token-based authentication with user name and password. This support includes support for Office 365 for internal and external Active Directory Federation Services (AD FS) or identity provider (IdP).
- **Performance enhancements to the Attachments repository**. You can scroll through your Attachments repository much faster.

Secure Mail 10.8.10

- **Support to print email attachments**. Secure Mail for iOS supports printing email attachments.
- **Modern authentication with Microsoft Office 365**. Secure Mail for iOS supports modern authentication. Modern authentication is OAuth token-based authentication with user name and password. This support includes support for Office 365 for external and internal Active Directory Federation Services (AD FS) and identity provider (IdP). For details, see Modern authentication using Microsoft office 365.

> **Notes:**
>
> This release does not support modern authentication with Endpoint Management integration with Microsoft Intune/EMS.
>
> This release includes modern authentication in a scenario where AD FS is accessible externally.

Known and fixed issues

January 13, 2021

Citrix supports upgrades from the last two versions of the mobile productivity apps.

Secure Mail 21.1.0

Known issues in Secure Mail 21.1.0

There are no known issues in this release.

Fixed issues in Secure Mail 21.1.0

In Secure Mail for iOS, tapping on a meeting link that is enclosed within angle brackets does not start the meeting. A blank screen appears. [CXM-90668]

Secure Mail 20.12.0

Secure Mail for iOS

There are no known or fixed issues in this release.

Secure Mail 20.11.0

There are no known or fixed issues in this release.

Known and fixed issues in older versions

For known and fixed issues in older versions of Secure Mail, see History of Secure Mail known and fixed issues.

Deploying Secure Mail

April 30, 2020

To deploy Secure Mail with Citrix Endpoint Management (formerly, XenMobile), follow these general steps:

1. You can integrate Secure Mail with an Exchange Server or IBM Notes Traveler Server to keep Secure Mail in sync with Microsoft Exchange or IBM Notes. If you use IBM Notes, configure the IBM Notes Traveler server. The configuration uses Active Directory credentials to authenticate to Exchange or the IBM Notes Traveler server. For details, see Integrating Exchange Server or IBM Notes Traveler Server.

   > **Important:**
   >
   > You cannot sync mail from Secure Mail with IBM Notes Traveler (formerly IBM Lotus Notes Traveler). This Lotus Notes third-party capability is not currently supported. As a result, when you delete a responded meeting mail from Secure Mail, the mail is not deleted on the IBM Notes Traveler server. If users accept a calendar event, and then they decline the event with a comment or they act on a comment, the comment is missing. [CXM-47936]
   > To learn about known limitations with IBM/Lotus Notes, see this Citrix blog post.

2. You can optionally enable SSO from Secure Hub. To do so, you configure Citrix Files account information in the Endpoint Management console to enable Endpoint Management as a SAML identity provider for Citrix Files. The configuration uses Active Directory credentials to authenticate to Citrix Files.

   Configuring the Citrix Files account information in Endpoint Management console is a one-time setup used for all Citrix clients, Citrix Files clients, and non-MDX Citrix Files clients. For details, see To configure Citrix Files account information in Endpoint Management console for SSO.

3. Download the Secure Mail .mdx file from the Citrix Downloads site.
4. Add Secure Mail to Endpoint Management and configure MDX policies. For details, see Add apps.

> Note:
>
> As of Secure Mail version 10.6.5, you can configure a new MDX analytics policy for Secure Mail for iOS and Android. Citrix collects analytics data to improve product quality. The Google Analytics level of detail policy lets you specify whether the data is associated with your company domain or is collected anonymously. Selecting **Anonymous** opts users out of including the company domain with the data that is collected. This new policy replaces an earlier Google analytics policy.

When the policy is set to anonymous, we collect the following types of data. We have absolutely no way to link this data to an individual user or company because we do not request user identifiable information. No personally identifiable information is sent to Google.

- Device statistics, such as the operating system version, app version, and device model
- Platform information, such as ActiveSync version and Secure Mail server version
- Failure points for product quality, such as APNs registrations, mail sync and send, and attachment download and calendar sync.

Other than company domain, no other identifiable information is collected when the policy is set to **Complete**. Default is **Complete**.

Configuring Secure Mail

January 21, 2019

The following features can be configured and integrated in Secure Mail:

- Secure Mail integration with Microsoft Intune/EMS
- Modern authentication with Office 365
- Background services for Secure Mail
- Integrate Exchange Server or IBM Notes Traveler Server
- S/MIME for Secure Mail
- SSO for Secure Mail

Secure Mail integration with Microsoft Intune/EMS

August 12, 2020

With this integration, you can manage and deliver Citrix Secure Mail with more security and the means to enhance productivity.

Secure Mail supports various Intune configurations. You can connect Secure Mail to on-premises Exchange or Office 365 mailboxes. To set up Endpoint Management integration with EMS/Intune, see Citrix Endpoint Management integration with Microsoft Intune/EMS

Secure Mail supports the following deployment modes:

- Intune MAM
- Intune MAM and Intune mobile device management (MDM)
- Intune MAM with Endpoint Management MDM-only
- Intune MAM with Endpoint Management MDM and MAM

Supported mail servers

- Exchange Online
- Exchange Server 2016
- Exchange Server 2013

Limitations

Secure Mail does not support certificate-based authentication.

> **Important:**
>
> To use Secure Mail in MDM mode along with Citrix Endpoint Management (MDM and MAM) you must configure Secure Hub in your environment.

To configure Secure Mail for Intune

If your environment is configured in the Citrix Endpoint Management MDM mode, Secure Mail automatically populates user names in an FTU experience.

To enable this feature, you must configure custom policies in the Endpoint Management console. For details, see the Endpoint Management documentation, Configure Secure Mail.

Features that are incompatible with Intune

The following Secure Mail features are not compatible with Endpoint Management integration with EMS/Intune:

- Secure Ticket Authority (STA)
- Email enrollment with single sign-on (SSO)
- Rich push notifications
- Citrix Files (Formerly ShareFile)
- S/MIME signing and encryption
- Microsoft Information Rights Management
- Secure Browse + Non KCD SSO Internal Exchange server

Modern authentication with Microsoft Office 365

August 12, 2020

Secure Mail supports modern authentication with Microsoft Office 365 for Active Directory Federation Services (AD FS) or Identity Provider (IDP). Modern authentication is OAuth token-based authentication with user name and password. Secure Mail users with iOS devices can take advantage of certificate-based authentication when connecting to Office 365. When they sign on to Secure Mail, users authenticate by using a client certificate, instead of typing their credentials.

Before you proceed, do the following:

1. Enable modern authentication (OAuth) for Microsoft Office 365.
2. Enable Office 365 endpoints, URLS, and IP address ranges in your firewall to ensure optimum network connectivity. For details, see the Microsoft documentation on Office 365 URLs and IP address range.

Citrix Endpoint Management policy prerequisites

Enable the following policies in the Citrix Endpoint Management console:

For devices running iOS:

- **Office 365 authentication mechanism:** Use this policy to indicate the OAuth mechanism used for authentication while configuring an account on Office 365. This policy has the following values that you must configure:
  - **Do not use OAuth:** Use this policy for basic authentication during account configuration.
  - **Use OAuth with Username and Password:** Use this policy for OAuth protocol during authentication. Users must provide their username and password and optionally a multifactor authentication code for the OAuth flow.

  - **User OAuth with client Certificate:** Use this policy if Office 365 is configured to perform certificate-based authentication. The default configuration is **Do not use OAuth**.

For devices running Android:

- **Use Modern authentication for O365:** Use this policy for OAuth protocol during authentication.
- **Custom user agent for modern authentication:** Use this policy to change the default user agent string for modern authentication.
- **Web SSO for tunneling policy:** Use this policy to tunnel the OAuth traffic to go over Secure Browse. To do so:
  - Set **Use Web SSO for tunneling** policy to **On**.
  - Select the **Tunneled - Web SSO** option in the Network access policy.
  - Exclude any hostnames related to OAuth from the **Background services** policy.

Policies common to iOS and Android devices:

- **Trusted Exchange Online Hostnames:** Use this policy to define a list of trusted Exchange Online hostnames that use the OAuth mechanism for authentication while configuring an account. This is a comma-separated format, such as server.company.com, server.company.co.uk. This list can either contain a default value or vanity URLs, but cannot be empty. Default value is **outlook.office365.com**.
- **Trusted AD FS Hostnames:** Use this policy to define a list of trusted AD FS hostnames for webpages where the password populates during Office 365 OAuth authentication. This is a comma-separated format, such as `sts.companyname.com`, `sts.company.co.uk`. If the list is empty, Secure Mail does not auto-populate passwords. Secure Mail matches the listed hostnames with the hostname of the webpage encountered during Office 365 authentication and checks if the page uses HTTPS protocol. For instance, when `sts.company.com` is a listed hostname and the user navigates to `https://sts.company.com`, Secure Mail populates the password, provided the page has a password field. The default value is `login.microsoftonline.com`.
- **Secure Mail Exchange Server:** Use this policy to define the address of your Exchange Server. You can use this policy to define either the on-premise server address or the Cloud server address, based on your requirement.

Secure Mail for iOS is now enabled with modern authentication after the policies are refreshed on the device.

Limitations

- If you are using modern authentication in your environment, the rich push notifications feature for iOS is not available. For details about rich push notifications, see Push notifications for Secure Mail.

- Multiple accounts are not supported on setups running certificate-based authentication.

Secure Mail policies

The following two tables list the Secure Mail policies that are required based on your Exchange infrastructure:

Exchange Infrastructure	Office 365 authentication mechanism/ Use Modern authentication for O365	Trusted AD FS Online Hostnames	Trusted Exchange Online Hostnames
On-premises	OFF	NA	NA
Hybrid*	ON	AD FS/IDP	`Outlook.office365.com` or vanity URL
Exchange online	ON	AD FS/IDP	`Outlook.office365.com` or vanity URL

Exchange Infrastructure	Secure Mail Exchange Server	Background network services (iOS)	Background network services (Android)
On-premises	Exchange on-premises Hostname	On-premises	On-premises
Hybrid*	on-premises, Exchange online Hostnames	On-premises, Exchange on-premises Hostname	On-premises, Exchange on-premises Hostname, AD FS/IDP (Internal only)
Exchange online	`Outlook.office365.com`	Exchange Online Hostnames	Exchange on-premises Hostname, AD FS, IDP

*Secure Mail supports a hybrid Exchange infrastructure with migrated mailboxes.

If on-premises users' mailbox is migrated to Exchange online, Secure Mail automatically detects this change and prompts the users for modern authentication without the need for reconfiguring their account.

Secure Mail with OAuth support matrix

The following table lists the Secure Mail OAuth support matrix on iOS and Android devices:

Authentication type	IDP/External AD FS	IDP/Internal AD FS	Azure AD	Intune
User name and password	Yes	Yes	Yes	Yes
Client certificate	Yes	Android only	No	No

Background services for Secure Mail

August 12, 2020

To access your mail server via the Citrix Gateway, you need to configure background services for Secure Mail. When you add Secure Mail to Citrix Endpoint Management (formerly, XenMobile), configure background services in MDX app policies settings.

To configure background services for Secure Mail

1. Sign on to the Endpoint Management console using administrator credentials.
2. In the console, click the **Configure** tab, click **Apps**, select the Secure Mail app, and then click **Edit**.
3. On the **MDX policy settings** page, in the **Platform** section, select the iOS or Android platform as required.
4. In the **App settings** section, configure the policies.

MDX app policies for the background services configuration

The following MDX app policies affect Secure Mail communication with Citrix Gateway, Citrix Endpoint Management server, Secure Ticket Authority (STA) servers, and the mail server.

Network access: The Network Access policy specifies if Secure Mail can use VPN to access background network services or if all traffic goes unrestricted via that Internet.

- If the network access policy is set to **Tunneled to the internal network**, only URLs listed in background network services pass through Citrix Gateway. The rest of the traffic goes unrestricted via the Internet. By default, Secure Mail access is **Tunneled to the internal network**.
- If the network access policy is set to **Unrestricted**, all traffic originating from Secure Mail is sent unrestricted via the Internet. VPN isn't used to access background services.

Secure Mail Exchange Server: Set the **Secure Mail Exchange Server** policy to the fully qualified domain name (FQDN) for the mail server.

Background network service: The Background network service policy specifies the list of mail servers that are allowed access through Citrix Gateway. List hostnames and the port number as a comma-separated value. Ensure there are no leading and trailing spaces between the values. For mail server addresses, include: `hostnameFQDN:portnumber`. For example: `mail1.example.com:443,mail2.example.com:443` (no space between the comma).

Background network service gateway: The Background network service gateway policy specifies the Citrix Gateway that Secure Mail uses to connect to the mail server. For the Citrix Gateway address, include: `citrixgatewayFQDN:portnumber`. For example: `gateway3.example.com:443`.

Background services ticket expiration: This policy specifies the validity of the background network service ticket. When Secure Mail connects through Citrix Gateway to a mail server, Citrix Endpoint Management issues a token that is used to connect to the internal mail server. This setting determines the duration until which Secure Mail can use this token. A new token for authentication and connection to the mail server is not required if the token is active. When the time limit expires, users must log on again to generate a new token. Default value of this token is 168 hours (7 days).

For more information about MDX app policies for background services, see:

- Secure Mail App settings policies for Android
- Secure Mail App settings policies for iOS

The following figure shows the communication flow and where these policies are applicable.

The following figures show the types of Secure Mail connections to a mail server. After each figure is a list of the related policy settings.

Direct connection to a mail server:

Policies for a direct connection to a mail server:

- Network access: **Unrestricted**

If network access is unrestricted, the following policies are not applicable:

- Background network services: N/A
- Background services ticket expiration: N/A
- Background network service gateway: N/A

Connection to a mail server via the STA:

Policies for connecting to a mail server via the STA:

- Network access: **Tunneled to the internal network**
- Background network services: `mail.example.com:443,mail1.example1.com:443`
- Background services ticket expiration: **168**
- Background network service gateway: `gateway3.example.com:443`

> Note:
>
> Citrix recommends that you use a STA connection for Secure Mail because a STA connection supports long-lived session connections.

For more information about the STA, see this Citrix Knowledge Center article.

Integrating Exchange Server or IBM Notes Traveler Server

January 25, 2019

To keep Secure Mail in sync with your mail servers, integrate Secure Mail with an Exchange Server or IBM Notes Traveler Server that resides in your internal network or is behind Citrix Gateway.

- To configure background services for Secure Mail, see: Background services for Secure Mail.
- To configure IBM Notes Traveler Server for Secure Mail, see: Configuring IBM Notes Traveler Server for Secure Mail.

> **Important:**
>
> You cannot sync mail from Secure Mail with IBM Notes Traveler (formerly IBM Lotus Notes Traveler). This Lotus Notes third-party capability is not currently supported. As a result, for example, when you delete a meeting mail from Secure Mail, the mail is not deleted on the IBM Notes Traveler server. [CXM-47936]
> To learn about known limitations with IBM/Lotus Notes, see this Citrix blog post.

Syncing is also available for Secure Notes and Secure Tasks. Note, however, that Secure Notes and Secure Tasks reached End of Life (EOL) status on December 31, 2018. For details, see EOL and deprecated apps.

- To sync Secure Notes for iOS, integrate it with an Exchange Server.
- To sync Secure Notes and Secure Tasks for Android, use the Secure Mail for Android account.

When you add Secure Mail, Secure Notes, and Secure Tasks to Citrix Endpoint Management (formerly, XenMobile), configure the MDX policies as mentioned in MDX app policies for the background services configuration.

> **Note:**
>
> Secure Mail for Android and iOS support the full path specified for a Notes Traveler Server. For example: `https://mail.example.com/traveler/Microsoft-Server-ActiveSync`.
>
> It is no longer necessary to configure your Domino Directory with web site substitution rules for the Traveler Server.

Configuring IBM Notes Traveler Server for Secure Mail

In IBM Notes environments, you must configure the IBM Notes Traveler server before you deploy Secure Mail. This section shows a deployment illustration of this configuration as well as system requirements.

> **Important:**
>
> If your Notes Traveler Server uses SSL 3.0, be aware that SSL 3.0 contains a vulnerability called the Padding Oracle On Downgraded Legacy Encryption (POODLE) attack, which is a man-in-the-middle attack affecting any app that connects to a server using SSL 3.0. To address the vulnerabilities introduced by the POODLE attack, Secure Mail disables SSL 3.0 connections by default and uses TLS 1.0 to connect to the server. As a result, Secure Mail cannot connect to a Notes Traveler Server that uses SSL 3.0. For details on a recommended workaround, see the Configuring SSL/TLS Security Level section in Integrating Exchange Server or IBM Notes Traveler Server.

In IBM Notes environments, you must configure the IBM Notes Traveler server before deploying Secure Mail.

The following diagram shows the network placement of IBM Notes Traveler servers and an IBM Domino mail server in a sample deployment.

System requirements

Infrastructure server requirements

- IBM Domino Mail Server 9.0.1
- IBM Notes Traveler 9.0.1

Authentication protocols

- Domino Database
- Lotus Notes Authentication Protocol
- Lightweight Directory Authentication Protocol

Port requirements

- Exchange: Default SSL port is 443.
- IBM Notes: SSL is supported on port 443. Non-SSL is supported, by default, on port 80.

Configuring SSL/TLS security level

Citrix made modifications to Secure Mail to address vulnerabilities introduced by the POODLE attack, as described in the preceding Important note. If your Notes Traveler Server uses SSL 3.0, therefore, to enable connections, the recommended workaround is to use TLS 1.2 on the IBM Notes Traveler Server 9.0.

IBM has a patch to prevent the use of SSL 3.0 in Notes Traveler secure server-to-server communication. The patch, released in November 2014, is included as interim fix updates for the following Notes Traveler server versions: 9.0.1 IF7, 9.0.0.1 IF8 and 8.5.3 Upgrade Pack 2 IF8 (and will be included in all future releases). For details about the patch, see LO82423: DISABLE SSLV3 FOR TRAVELER SERVER TO SERVER COMMUNICATION.

As an alternative workaround, when you add Secure Mail to Endpoint Management, change the Connection security level policy to **SSLv3 and TLS**. For the latest information about this issue, see SSLv3 Connections Disabled by Default on Secure Mail 10.0.3.

The following tables indicate the protocols that Secure Mail supports, by operating system, based on the Connection security level policy value. Your mail server must also be able to negotiate the protocol.

The following table shows supported protocols for Secure Mail when the connection security level is SSLv3 and TLS.

Operating system type	SSLv3	TLS
iOS 9 and later	No	Yes
Earlier than Android M	Yes	Yes
Android M and Android N	Yes	Yes
Android O	No	Yes

The following table shows supported protocols for Secure Mail when the connection security level is TLS.

Operating system type	SSLv3	TLS
iOS 9 and later	No	Yes

Operating system type	SSLv3	TLS
Earlier than Android M	No	Yes
Android M and Android N	No	Yes
Android O	No	Yes

Configuring Notes Traveler Server

The following information corresponds to the configuration pages in the IBM Domino Administrator client.

- **Security:** Internet authentication is set to Fewer name variations with higher security. This setting is used to map UID to AD User ID in LDAP authentication protocols.
- **NOTES.INI Settings:** Add **NTS_AS_ENFORCE_POLICY**=**false**. This allows Secure Mail policies to be managed by Endpoint Management rather than Traveler. This setting may conflict with current customer deployments, but will simplify the management of the device in Endpoint Management deployments.
- **Synchronization protocols:** SyncML on IBM Notes and mobile device synchronization are not supported by Secure Mail at this time. Secure Mail synchronizes Mail, Calendar and Contacts items through the Microsoft ActiveSync protocol built into Traveler servers. If SyncML is forced as the primary protocol, Secure Mail cannot connect back through the Traveler infrastructure.
- **Domino Directory Configuration - Web Internet Sites:** Override Session Authentication for /traveler to disable form-based authentication.

S/MIME for Secure Mail

July 11, 2019

Secure Mail supports Secure/Multipurpose Internet Mail Extensions (S/MIME), enabling users to sign and encrypt messages for greater security. Signing assures the recipient that the identified sender sent the message not an imposter. Encryption allows only the recipients with a compatible certificate to open the message.

For details about S/MIME, see Microsoft TechNet.

In the following table, X indicates that Secure Mail supports an S/MIME feature on a device OS.

S/MIME Feature	iOS	Android
Digital identity provider integration: You can integrate Secure Mail with a supported third-party digital identity provider. Your identity provider host supplies certificates to an identity provider app on user devices. That app sends certificates to the Endpoint Management shared vault, a secure storage area for sensitive app data. Secure Mail obtains certificates from the shared vault. For details, see Integrating with a Digital Identity Provider.	X	
Derived Credential support	Secure Mail supports the use of derived credentials as a certificate source. For more information on derived credentials, see Derived Credentials for iOS.	

S/MIME Feature	iOS	Android
Certificate distribution by email: Distributing certificates by email requires that you create certificate templates and then use those templates to request user certificates. After you install and validate the certificates, you export the user certificates and then email them to users. Users then open the email in Secure Mail and import the certificates. For details, see Distributing Certificates by Email.	X	X
Auto-import of single-purpose certificates: Secure Mail detects if a certificate is only for signing or encryption and then automatically imports the certificate and notifies the user. If a certificate is for both purposes, users are prompted to import it.	X	

Integrating with a digital identity provider

The following diagram shows the path that a certificate takes from the digital identity provider host to Secure Mail. This happens when you integrate Secure Mail with a supported third-party digital identity provider.

The MDX shared vault is a secure storage area for sensitive app data such as certificates. Only app enabled by Endpoint Management can access the shared vault.

Prerequisites

Secure Mail supports integration with Entrust IdentityGuard.

Configuring the integration

1. Prepare the identity provider app and provide it to users:
    - Contact Entrust to get the .ipa to wrap.
    - Use the MDX Toolkit to wrap the app.

      If you deploy this app to users who already have a version of the app outside of the Endpoint Management environment, use a unique app ID for this app. Use the same provisioning profile for this app and Secure Mail.
    - Add the app to Endpoint Management and publish it to the Endpoint Management app store.
    - Let your users know that they must install the identity provider app from Secure Hub. Provide guidance, as needed, about any post-installation steps.

      Depending on how you configure the S/MIME policies for Secure Mail in the next step, Secure Mail might prompt users to install certificates or enable S/MIME in Secure Mail settings. Steps for both of those procedures are in Enabling S/MIME on Secure Mail for iOS.
2. When you add Secure Mail to Endpoint Management, be sure to configure these policies:
    - Set the S/MIME certificate source policy to **Shared vault**. This setting means that Secure Mail uses the certificates stored in its shared vault by your digital identity provider.
    - To enable S/MIME during the initial startup of Secure Mail, configure the Enable S/MIME during first Secure Mail startup policy. The policy determines if Secure Mail enables S/MIME when there are certificates in the shared vault. If no certificates are available, Secure Mail prompts the user to import certificates. If the policy isn't enabled, users can enable S/MIME in the Secure Mail settings. By default, Secure Mail does not enable S/MIME, which means that users must enable S/MIME through Secure Mail settings.

Using derived credentials

Instead of integrating with a digital identity provider, you can allow the use of derived credentials.

When you add Secure Mail to Endpoint Management, configure the S/MIME certificate source policy to **Derived Credentials**. For more information on derived credentials, see Derived Credentials for iOS.

Distributing certificates by email

Instead of integrating with a digital identity provider or using derived credentials, you can distribute certificates to users by email. This option requires the following general steps, detailed in this section.

1. Use Server Manager to enable web enrollment for Microsoft Certificate Services and to verify your authentication settings in IIS.

2. Create certificate templates for signing and encrypting email messages. Use those templates to request user certificates.
3. Install and validate the certificates, then export the user certificates and email them to users.
4. Users open the email in Secure Mail and import the certificates. The certificates are thus available only to Secure Mail. They do not appear in the iOS profile for S/MIME.

Prerequisites

The instructions in this section are based on the following components:

- XenMobile Server 10 and later
- A supported version of Citrix Gateway, formerly NetScaler Gateway
- Secure Mail for iOS (minimum version 10.8.10); Secure Mail for Android devices (minimum version 10.8.10)
- Microsoft Windows Server 2008 R2 or later with Microsoft Certificate Services acting as the Root Certificate Authority (CA)
- Microsoft Exchange:
  - Exchange Server 2016 Cumulative Update 4
  - Exchange Server 2013 Cumulative Update 15
  - Exchange Server 2010 SP3 Update Rollup 16

Complete the following prerequisites before configuring S/MIME:

- Deliver the root and intermediate certificates to the mobile devices either manually or through a credentials device policy in Endpoint Management. For details, see Credentials device policy.
- If you are using private server certificates to secure the ActiveSync traffic to Exchange Server, do the following: Have all the root and intermediate certificates installed on the mobile devices.

Enabling Web enrollment for Microsoft Certificate Services

1. Go to **Administrative Tools** and the select **Server Manager**.
2. Under **Active Directory Certificate Services**, check to see if **Certificate Authority Web Enrollment** is installed.
3. Select **Add Role Services** to install Certificate Authority Web Enrollment, if needed.
4. Check **Certificate Authority Web Enrollment** and then click **Next**.
5. Click **Close** or **Finish** when the installation is complete.

Verifying your authentication settings in IIS

- Ensure that the Web enrollment site used to request user certificates (for example, `https://ad.domain.com/certsrv/`) is secured with an HTTPS server certificate (private or public).

- The Web enrollment site must be accessed through HTTPS.

1. Go to **Administrative Tools** and then select **Server Manager**.
2. In **Web Server (IIS)**, look under **Role Services**. Verify that Client Certificate Mapping Authentication and IIS Client Certificate Mapping Authentication are installed. If not, install these role services.
3. Go to **Administrative Tools** and then select **Internet Information Services (IIS) Manager**.
4. In the left pane of the **IIS Manager** window, select the server running the IIS instance for web enrollment.
5. Click **Authentication**.
6. Ensure that **Active Directory Client Certificate Authentication** is **Enabled**.
7. Click **Sites > Default site for Microsoft Internet Information Services > Bindings** in the right pane.
8. If an HTTPS binding does not exist, add one.
9. Go to the Default Web Site Home.
10. Click **SSL Settings** and then click **Accept for Client Certificates**.

Creating new certificate templates

To sign and encrypt email messages, Citrix recommends that you create certificates on Microsoft Active Directory Certificate Services. If you use the same certificate for both purposes and archive the encryption certificate, it is possible to recover a signing certificate and allow impersonation.

The following procedure duplicates the certificate templates on the Certificate Authority (CA) server:

- Exchange Signature Only (for Signing)
- Exchange User (for Encryption)

1. Open the Certificate Authority snap-in.
2. Expand the CA and then go to **Certificate Templates**.
3. Right-click and then click **Manage**.
4. Search for the Exchange Signature Only template, right-click the template and then click **Duplicate Template**.
5. Assign any name.
6. Select the **Publish certificate in Active Directory** check box.

> **Note:**
>
> If you do not select the **Publish certificate in Active Directory** check box, users must publish the user certificates (for signing and encryption) manually. They can do this through **Outlook mail client > Trust Center > Email Security > Publish to GAL (Global Address**

> **List)**.

7. Click the **Request Handling** tab and then set the following parameters:
   - **Purpose:** Signature
   - **Minimum key size:** 2048
   - **Allow private key to be exported check box:** selected
   - **Enroll subject without requiring any user input check box:** selected
8. Click the **Security** tab and, under **Group or user names**, ensure that **Authenticated Users** (or any desired Domain Security Group) is added. Also ensure that, under **Permissions for Authenticated Users**, the **Read and Enroll** check boxes are selected for **Allow**.
9. For all other tabs and settings, leave the default settings.
10. In **Certificate Templates**, click **Exchange User** and then repeat steps 4 though 9.

    For the new Exchange User template, use the same default settings as for the original template.
11. Click the **Request Handling** tab and then set the following parameters:
    - **Purpose:** Encryption
    - **Minimum key size:** 2048
    - **Allow private key to be exported check box:** selected
    - **Enroll subject without requiring any user input check box:** selected
12. When both templates are created, be sure to issue both certificate templates. Click **New** and then click **Certificate Template to Issue**.

Requesting user certificates

This procedure uses “user1” to navigate to the Web enrollment page; for example, `https://ad.domain.com/certsrv/`. The procedure requests two new user certificates for secure email: one certificate for signing and the other for encryption. You can repeat the same procedure for other domain users that require the use of S/MIME through Secure Mail.

Manual enrollment is used through the Web enrollment site (example, `https://ad.domain.com/certsrv/`) on Microsoft Certificate Services to generate the user certificates for signing and encryption. An alternative is to configure auto-enrollment through a Group Policy for the group of users who would use this feature.

1. On a Windows-based computer, open Internet Explorer and go to the Web enrollment site to request a new user certificate.

> **Note:**
>
> Be sure you log on with the correct domain user to request the certificate.

2. When logged in, click **Request a certificate**.
3. Click **Advanced Certificate Request**.
4. Click **Create and Submit a request to this CA**.
5. Generate the user certificate for signing purposes. Select the appropriate template name and type your user settings, and then next to **Request Format**, select **PKCS10**.

   The request has been submitted.
6. Click **Install this certificate**.
7. Verify that the certificate is installed successfully.
8. Repeat the same procedure but now for encrypting email messages. With the same user logged on to the Web enrollment site, go to the Home link to request a new certificate.
9. Select the new template for encryption and then type the same user settings you entered in step 5.
10. Ensure you installed the certificate successfully and then repeat the same procedure to generate a pair of user certificates for another domain user. This example follows the same procedure and generates a pair of certificates for “User2”.

> **Note:**
>
> This procedure uses the same Windows-based computer to request the second pair of certificates for “User2”.

Validating Published Certificates

1. To ensure that the certificates are properly installed in the domain user profile, go to **Active Directory Users and Computers > View > Advanced Features**.
2. Go to the properties of the user (User1 for this example) and then click the **Published Certificates** tab. Ensure that both certificates are available. You can also verify that each certificate has a specific usage.

   This figure shows a certificate to encrypt email messages.

   This figure shows a certificate to sign email messages.

   Ensure that the correct encrypted certificate is assigned to the user. You can verify this information under **Active Directory Users and Computers > user properties**.

The way Secure Mail works is by checking the userCertificate user object attribute via LDAP queries. You can read this value on the **Attribute Editor** tab. If this field is empty or has the incorrect user certificate for encryption, Secure Mail cannot encrypt (or decrypt) a message.

Exporting the user certificates

This procedure exports both “User1” and “User2” pair certificates in .PFX (PKCS#12) format with the private key. When exported, the certificates are sent through email to the user using Outlook Web Access (OWA).

1. Open the MMC console and go to the snap-in for **Certificates - Current User**. You see both “User1” and User2” pair of certificates.
2. Right-click the certificate and then click **All Tasks > Export**.
3. Export the private key by selecting **Yes, export the private key.**
4. Select the **Include all certificates in the certification path if possible** and **Export all extended properties** check boxes.
5. When you export the first certificate, repeat the same procedure for the remaining certificates for users.

> **Note:**
>
> Clearly label which certificate is the signing certificate and which certificate is the encryption certificate. In the example, the certificates are labeled as userX-sign.pfx and “userX-enc.pfx.

Sending certificates through email

When all certificates are exported in PFX format, you can use Outlook Web Access (OWA) to send them through email. The logon name for this example is User1 the sent email contains both certificates.

Repeat the same procedure for User2 or other users in your domain.

Enabling S/MIME on Secure Mail for iOS and Android

After the email is delivered, the next step is to open the message using Secure Mail and enable S/MIME with the appropriate certificates for signing and encryption.

To enable S/MIME with individual signing and encryption certificates

1. Open Secure Mail, navigate to the email containing the S/MIME certificates.
2. Tap on the signing certificate to download and import.

3. Type the password assigned to the private key when the signing certificate was exported from the server.

   Your certificate has been imported.

4. Tap **Turn on signing**
5. Alternatively, you can navigate to **Settings** > and **S/MIME** and tap S/MIME to turn on signing certificate.
6. In the **Signing** screen, verify that the correct signing certificate is imported.
7. Go back to the email and tap on the encryption certificate to download and import.
8. Type the password assigned to the private key when the encryption certificate was exported from the server.

   Your certificate has been imported.

9. Tap **Turn on Encryption**
10. Alternatively, you can navigate to **Settings** > and **S/MIME** and tap S/MIME to enable **Encrypt by Default**.
11. In the **Encryption** screen, verify that the correct encryption certificate is imported.

> **Note:**
>
> a) If an email is digitally signed with S/MIME, has attachments, and the recipient does not have S/MIME enabled, attachments are not received. This behavior is an Active Sync limitation. To receive S/MIME messages effectively, turn on S/MIME in Secure Mail settings.
>
> b) The **Encrypt by Default** option allows you to minimize the steps required to encrypt your email. If this feature is On, your email will be in the encrypted state while composing. If this feature is Off, your email will be in the unencrypted state while composing and you must tap the **Lock** icon to encrypt.

To enable S/MIME with a single signing and encryption certificate

1. Open Secure Mail, navigate to the email containing the S/MIME certificate.
2. Tap on the S/SMIME certificate to download and import.
3. Type the password assigned to the private key when the certificate was exported from the server.
4. From the certificate options that appear, tap the appropriate option to import signing certificate or encryption cerficate.
   Tap **Open certificate** to view details about the certificate.

Your certificate has been imported.

You can view the imported certificates by navigating to **Settings > S/MIME**

Testing S/MIME on iOS and Android

Once you have performed the steps listed in the preceding section, your recipient can read your mail which is signed and encrypted.

The following image shows an example of an encrypted message as read by the recipient.

The following image shows an example of verification of signed trusted certificate.

Secure Mail searches the Active Directory domain for public encryption certificates of recipients. If a user sends an encrypted message to a recipient who does not have a valid public encryption key, the message is sent unencrypted. In a group message, if even one recipient doesn't have a valid key, the message is sent unencrypted to all recipients.

Configuring public certificate sources

To use S/MIME public certificates, configure the S/MIME public certificate source, LDAP server address, LDAP Base DN, and Access LDAP Anonymously policies.

In addition to the app policies, do the following.

- If the LDAP servers are public, ensure that the traffic goes directly to LDAP servers. To do so, configure the network policy for Secure Mail to be **Tunneled to the internal network** and configure split DNS for Citrix ADC.
- If the LDAP servers are on an internal network, do the following:
  - For iOS, ensure that you don't configure the Background network service gateway policy. If you do configure the policy, users receive frequent authentication prompts.
  - For Android, ensure that you add the **LDAP server URL** in the list for the Background network service gateway policy.

SSO for Secure Mail

April 8, 2019

You can configure Endpoint Management to enroll users automatically in Secure Mail when they enroll in Secure Hub. Users don't have to enter more information or take more steps to enroll in Secure Mail. For users who enroll in Secure Hub with email credentials, this feature requires that autodiscovery is enabled. If autodiscovery is not enabled, you can enable this feature for the following enrollment methods:

- The Endpoint Management address is passed to Secure Mail from Secure Hub.
- Users enter the Endpoint Management address when enrolling in Secure Hub.

To enable the automatic enrollment in Secure Mail

1. In the Endpoint Management client properties, on the **Settings** page, do the following:

   a. Set the following values to **true**:

   - ENABLE_PASSCODE_AUTH
   - ENABLE_PASSWORD_CACHING
   - ENABLE_CREDENTIAL_STORE

   b. Add this configuration:

   - **Display name**: SEND_LDAP_ATTRIBUTES
   - **Value**: userPrincipalName=${user.userprincipalname},sAMAccountNAme=${user.samaccountname}, displayName= ${ user.displayName} ,mail= ${ user.mail}

2. On the **Settings** page, add this configuration to the server property:

   MAM_MACRO_SUPPORT set to **true**

3. Configure these Secure Mail properties:

   - Set Initial Authentication Mechanism to **User email address**.
   - Set Initial Authentication Credentials to **userPrincipalName**.

4. Configure email-based AutoDiscovery Service for the user's Exchange Server mailbox. For support, reach out to your Microsoft Exchange administrator. This article assumes that you configure Autodiscovery Service by querying DNS for an SRV record.

To configure the Secure Mail app policy

Upload the Secure Mail app to Endpoint Management. Upload the .mdx file associated with the correct version of the Secure Mail app. Then, configure the following Secure Mail app settings:

1. In Initial authentication mechanism, click **User email address**.
2. In **Initial authentication credentials**, click **userPrincipalName** or **sAMAccountName**. Your selection is based on the authentication type configured against the user's Exchange Mail Server.
3. Leave the Secure Mail Exchange Server and Secure Mail user domain fields empty.
4. Configure other policies of the Secure Mail app as required and make necessary delivery group assignments.

The end-to-end Secure Mail SSO user experience with automatic provisioning

Ensure that you meet the following prerequisites.

1. Install Secure Hub from the Apple App Store (iOS) or the Google Play Store (Android).
2. Open Secure Hub and enter an email address and password for enrolling in Endpoint Management.
3. Install Secure Mail from the Apple App Store (iOS) or the Google Play Store (Android).
4. Open Secure Mail and tap **OK**. This step allows Secure Hub to manage Secure Mail. Upon opening, Secure Mail is automatically configured.

The Exchange Server that corresponds to the user's mailbox database is obtained from the Autodiscovery Service you configured. The DNS SRV Record query makes use of the user's email address fetched from Secure Hub.

All the required details for account configuration, such as email address, userPrincipalName/sAMAccountName, and password are fetched from Secure Hub.

When the account is configured, users can view details on the device in **Secure Mail** > **Settings** > **Account**.

Troubleshoot issues

If any issues occur with the SSO configuration, you can try the following steps.

1. Ensure that the XenMobile Server version is 10.5 or later.
2. Ensure that Endpoint Management is configured for AutoDiscovery Service and user enrollment is configured for use with an email address.
3. Ensure that the Exchange Server domain is configured with autodiscovery. Make sure the query for the SRV record returns the expected mail server details for ActiveSync mail clients.
4. In case of an issue with this functionality, collect the following information and contact Citrix Technical Support:
    - Download Endpoint Management Diagnostic Logs.
    - Collect Secure Mail Diagnostic Logs with the highest log level.
    - Collect IIS logs from the directory C:\inetpub\logs\LogFiles\W3SVC1 from the Exchange Server hosting the Autodiscovery Service. For more details on Microsoft Autodiscovery Service, see the Autodiscover service in Exchange Server.

Security considerations

February 8, 2019

This article discusses Secure Mail security considerations and specific settings that you can enable to help increase data security.

Microsoft IRM and AIP email rights protection support

Secure Mail for Android and iOS support messages protected with Microsoft Information Rights Management (IRM) and the Azure Information Protection (AIP) solution. This support is subject to the configured IRM policy on Citrix Endpoint Management.

This feature allows organizations that use IRM to apply protection to messaging content. The feature also allows mobile device users to be able to create and consume rights-protected content. By default IRM support is **Off**. To enable IRM support, set the Information Rights Management policy to **On**.

To enable Information Rights Management in Secure Mail

1. Log on to Endpoint Management and navigate to **Configure** > **Apps** and click **Add**.
2. In the **Add App** screen, click **MDX**.
3. In the **App Information** screen, enter the app details and click **Next**.
4. Based on your device OS, select and upload the .mdx file.
5. Enable Information Rights Management under **App Settings**.

> Note:
>
> Enable Information Rights Management for both iOS and Android.

When you receive a rights protected email

When users receive a mail with protected content, they see the following screen:

To view details about the rights that user is entitled to, tap **Details**.

When you compose a rights protected email

When users compose a mail, they can set restriction profiles to enable email protection.

To set restrictions to your email:

1. Log in to Secure Mail and tap the **Compose** icon.
2. In the compose screen, tap the **Email Restriction** icon.
3. In the **Restriction Profiles** screen, tap the desired restrictions to apply to the email and then click back.

   The applied restrictions appear below the subject field.

Some organizations may require strict adherence to their IRM policy. Users with access to Secure Mail may attempt to bypass the IRM policy by tampering with Secure Mail, the operating system, or even the hardware platform.

Although Endpoint Management can detect certain attacks, consider the following precautionary measures to increase security:

- Review the security guidance supplied by the device vendor.
- Configure devices accordingly, using Endpoint Management capabilities or otherwise.
- Provide guidance to your users for the appropriate use of IRM features, including Secure Mail.
- Deploy additional third-party security software to resist this type of attack.

Email security classifications

Secure Mail for iOS and Android supports email classification markings, enabling users to specify security (SEC) and dissemination limiting markers (DLM) when sending emails. SEC markings include Protected, Confidential, and Secret. DLM includes Sensitive, Legal, or Personal. When composing an email, a Secure Mail user can select a marking to indicate the classification level of the email, as shown in the following images.

Recipients can view the classification marking in the email subject. For example:

- Subject: Planning [SEC = PROTECTED, DLM = Sensitive]
- Subject: Planning [DLM = Sensitive]
- Subject: Planning [SEC = UNCLASSIFIED]

Email headers include classification markings as an Internet Message Header Extension, shown in bold text in this example:

Date: Fri, 01 May 2015 12:34:50 +530

Subject: Planning [SEC = PROTECTED, DLM = Sensitive]

Priority: normal

X-Priority: normal **X-Protective-Marking: VER-2012.3, NS=gov.au,SEC = PROTECTED, DLM = Sensitive,ORIGIN=operations@example.com**

From: **operations@example.com**

To: Team <mylist@example.com>

MIME-Version: 1.0 Content-Type: multipart/alternative;boundary="_com.example.email_6428E5E4-9DB3-4133-9F48-155913E39A980"

Secure Mail only displays classification markings. The app does not take actions based on those markings.

When a user replies to or forwards an email that has classification markings, the SEC and DLM values default to the marking of the original email. The user can choose a different marking. Secure Mail does not validate such changes in relation to the original email.

You configure email classification markings through the following MDX policies.

- **Email classification:** If **On**, Secure Mail supports email classification markings for SEC and DLM. Classification markings appear in email headers as "X-Protective-Marking" values. Be sure to configure the related email classification policies. Default value is **Off**.
- **Email classification namespace:** Specifies the classification namespace that is required in the email header by the classification standard used. For example, the namespace "gov.au" appears in the header as "NS=gov.au". Default value is empty.
- **Email classification version:** Specifies the classification version that is required in the email header by the classification standard used. For example, the version "2012.3" appears in the header as "VER=2012.3". Default value is empty.
- **Default email classification:** Specifies the protective marking that Secure Mail applies to an email if a user does not choose a marking. This value must be in the list for the Email classification markings policy. Default value is **UNOFFICIAL**.
- **Email classification markings:** Specifies the classification markings to be made available to users. If the list is empty, Secure Mail does not include a list of protective markings. The markings list contains value pairs that are separated by semicolons. Each pair includes the list value that appears in Secure Mail and the marking value that is the text appended to the email subject and header in Secure Mail. For example, in the marking pair "UNOFFICIAL,SEC=UNOFFICIAL;", the list value is "UNOFFICIAL" and the marking value is "SEC=UNOFFICIAL".

Default value is a list of classification markings that you can modify. The following markings are provided with Secure Mail.

- UNOFFICIAL,SEC=UNOFFICIAL
- UNCLASSIFIED,SEC=UNCLASSIFIED
- For Official Use Only,DLM=For-Official-Use-Only
- Sensitive,DLM=Sensitive
- Sensitive:Legal,DLM=Sensitive:Legal
- Sensitive:Personal,DLM=Sensitive:Personal
- PROTECTED,SEC=PROTECTED

- PROTECTED+Sensitive,SEC=PROTECTED
- PROTECTED+Sensitive:Legal,SEC=PROTECTED DLM=Sensitive:Legal
- PROTECTED+Sensitive:Personal,SEC=PROTECTED DLM=Sensitive:Personal
- PROTECTED+Sensitive:Cabinet,SEC=PROTECTED,DLM=Sensitive:Cabinet
- CONFIDENTIAL,SEC=CONFIDENTIAL
- CONFIDENTIAL+Sensitive,SEC=CONFIDENTIAL,DLM=Sensitive
- CONFIDENTIAL+Sensitive:Legal,SEC=CONFIDENTIAL DLM=Sensitive:Legal
- CONFIDENTIAL+Sensitive:Personal,SEC=CONFIDENTIAL,DLM=Sensitive:Personal
- CONFIDENTIAL+Sensitive:Cabinet,SEC=CONFIDENTIAL DLM=Sensitive:Cabinet
- SECRET,SEC=SECRET
- SECRET+Sensitive,SEC=SECRET,DLM=Sensitive
- SECRET+Sensitive:Legal,SEC=SECRET,DLM=Sensitive:Legal
- SECRET+Sensitive:Personal,SEC=SECRET,DLM=Sensitive:Personal
- SECRET+Sensitive:Cabinet,SEC=SECRET,DLM=Sensitive:Cabinet
- TOP-SECRET,SEC=TOP-SECRET
- TOP-SECRET+Sensitive,SEC=TOP-SECRET,DLM=Sensitive
- TOP-SECRET+Sensitive:Legal,SEC=TOP-SECRET DLM=Sensitive:Legal
- TOP-SECRET+Sensitive:Personal,SEC=TOP-SECRET DLM=Sensitive:Personal
- TOP-SECRET+Sensitive:Cabinet,SEC=TOP-SECRET DLM=Sensitive:Cabinet

iOS data protection

Enterprises that must meet Australian Signals Directorate (ASD) data protection requirements can use the **Enable iOS data protection** policies for Secure Mail and Secure Web. By default, the policies are **Off**.

When **Enable iOS data protection** is **On** for Secure Web, Secure Web uses Class A protection level for all files in the sandbox. For details about Secure Mail data protection, see Australian Signals Directorate Data Protection. If you enable this policy, the highest data protection class is used so there is no need to also specify the **Minimum data protection class** policy.

To change the Enable iOS data protection policy

1. Use the Endpoint Management console to load the Secure Web and Secure Mail MDX files to Endpoint Management: For a new app, navigate to **Configure > Apps > Add** and then click **MDX**. For an upgrade, see Upgrade MDX or enterprise apps.
2. For Secure Mail, browse to the **App** settings, locate the **Enable iOS data protection** policy, and set it to **On**. Devices running older operating system versions are not affected when this policy is enabled.

3. For Secure Web, browse to the **App** settings, locate the **Enable iOS data protection policy**, and set it to **On**. Devices running older operating system versions are not affected when this policy is enabled.
4. Configure the app policies as usual and save your settings to deploy the app to the Endpoint Management app store.

Australian Signals Directorate Data Protection

Secure Mail supports Australian Signals Directorate (ASD) data protection for those enterprises that must meet ASD computer security requirements. By default, the Enable iOS data protection policy is **Off** and Secure Mail provides Class C data protection or uses the data protection set in the provisioning profile.

If the policy is **On**, Secure Mail specifies the protection level when creating and opening files in the app sandbox. Secure Mail sets Class A data protection on:

- Outbox items
- Photos from the camera or camera roll
- Images pasted from other apps
- Downloaded file attachments

Secure Mail sets Class B data protection on:

- Stored mail
- Calendar items
- Contacts
- ActiveSync policy files

Class B protection enables a locked device to sync and enables downloads to complete if a device is locked after the download starts.

With data protection enabled, queued outbox items are not sent when a device is locked because the files cannot be opened. If the device terminates and then restarts Secure Mail when a device is locked, Secure Mail cannot sync until the device is unlocked and Secure Mail starts.

Citrix recommends that, if you enable this policy, you enable Secure Mail logging only when needed to avoid the creation of log files with Class C data protection.

iOS features

May 18, 2020

This article discusses the iOS features that are supported in Secure Mail.

Minimize drafts

In Secure Mail for iOS, you can minimize a draft while you're composing an email and navigate within the app. This feature is available on devices running iOS 13 and later. For user help documentation on this feature, see the Citrix User Help Center article Minimize a draft email.

Reporting phishing emails with MIME headers

In Secure Mail for iOS, when a user reports a phishing mail, an EML file is generated as an attachment corresponding to that mail. Admins receive this mail and can view the MIME headers associated with the reported mail. To enable this feature, an admin must configure the Report Phishing Email Address policy and set the Report Phishing Mechanism as Report Via Attachment in the Citrix Endpoint Management console. For details, see Report phishing email as an attachment.

Support for WkWebView

Secure Mail for iOS supports WkWebView. This feature improves the way Secure Mail email and Calendar events are rendered on your device.

Support for Slack EMM

Slack EMM is for Slack customers with Enterprise Mobility Management (EMM) enabled. Secure Mail for iOS supports the application **Slack EMM**, which allows admins to choose the integration of Secure Mail with either the **Slack** app or the **Slack EMM** app.

Group notifications

With the Group notification feature, conversations in an email thread are grouped. You can quickly glance at grouped notifications on the lock screen of your device. Group notification settings are enabled by default on the device. The feature requires iOS 12.

Notification response option

In Secure Mail for iOS, users can respond to meeting notifications, such as Accept, Decline, and Tentative. They can respond to message notifications with Reply and Delete.

Enhancements to rich push notification failure messages

In Secure Mail for iOS, appropriate push notification failure messages appear in the notification center on your device based on the type of notification failure. For details, see Secure Mail notifications.

Support for rich push notifications on Microsoft setups

Secure Mail for iOS supports rich push notifications on setups running Microsoft Enterprise Mobility + Security (EMS)/Intune with modern authentication (O365). To enable the rich push notifications feature, ensure that the following prerequisites are met:

- In the Endpoint Management console, set **Push notifications** to ON.
- The **Network access policy** is set to **Unrestricted**.
- The **Control locked screen notifications** policy is set to **Allow** or **Email sender or event title**.
- Navigate to **Secure Mail** > **Settings** > **Notifications** and then enable **Mail Notifications**.

Support for S/MIME for derived credentials

Secure Mail for iOS supports S/MIME for derived credentials. For this feature to work, you need to do the following:

- Select Derived Credential as the S/MIME certificate source. For details, see Derived credentials for iOS.
- Add the LDAP Attributes client property in Citrix Endpoint Management. Use the following information:
  - **Key:** SEND_LDAP_ATTRIBUTES
  - **Value:** `userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme =${ user.samaccountname } ,displayName=${ user.displayName } ,mail= ${ user.mail }`

For steps on how to add a client property, for XenMobile Server, see Client properties and for Endpoint Management, see Client properties.

For more information about how devices enroll when using derived credentials, see Enrolling devices by using derived credentials.

1. On your Endpoint Management Console, navigate to **Configure > Apps**.
2. Select **Secure Mail** and then click **Edit**.
3. Under the iOS platform, for the S/MIME certificate source, select **Derived Credential**.

Secure Mail Caller ID

In Secure Mail for iOS, you can identify incoming calls from your Secure Mail contacts by enabling Secure Mail Caller ID in your device settings. You must enable the following administrative prerequisite: In Citrix Endpoint Management, ensure that the CallerIDSupportEnabled MDX policy is enabled.

For user help documentation on this feature, see the Citrix User Help Center article, Set up caller ID.

Set colors in Calendars

For user help documentation on this Calendar feature, see the Citrix User Help Center article, Set colors for synchronized Secure Mail calendars.

Attach files from the Files app

In Secure Mail for iOS, you can attach files from the iOS native **Files** app. For more information about the iOS Files App, see the Apple article, Files App. For user help documentation on this feature, see the Citrix User Help Center article, View and attach files.

Spellcheck feature

Secure Mail spellcheck interacts with the device Auto-Capitalization and Check Spelling settings under **General > Keyboard** in the following ways:

Auto-Correction on Device	Check Spelling on Device	Check Spelling in Secure Mail	Behavior
ON	ON	ON	Red underline shows. When tapped, the word is highlighted in pink and a suggestion appears.
OFF	OFF	ON	Red line shows. When tapped, no suggestion appears.
ON	ON	OFF	No red underline shows. When tapped, the word is highlighted in pink and a suggestion appears
OFF	OFF	OFF	No red underline, highlighting, or suggestion appear.

Auto-Correction on Device	Check Spelling on Device	Check Spelling in Secure Mail	Behavior
ON	OFF	ON	Red underline shows. When tapped, the word is highlighted in pink and a suggestion appears.
OFF	ON	ON	Red underline shows. When tapped, the word is highlighted in pink and a suggestion appears.
ON	OFF	OFF	No red underline shows. When tapped, the word is highlighted in pink and a suggestion appears.
OFF	ON	OFF	No red underline shows. When tapped, the word is highlighted in pink and a suggestion appears.

Mailboxes screen

The **Mailboxes** screen displays all the accounts you have configured and has the following views:

- **All Accounts:** Contains emails from all Exchange accounts that you have configured.
- **Individual accounts:** Contains emails and folders of an individual account. These accounts appear as a list that you can expand to view the subfolders.

The **All Accounts** mailbox is the global view by default. This view contains attachments and emails from all Exchange accounts that you have configured on your device.

The **All Accounts** mailbox has the following menu items:

- All attachments
- Inbox

  - Unread
  - Flagged
- Drafts
- Sent Items
- Outbox
- Deleted Items

Although the **All Accounts** view displays your emails from multiple accounts collectively, the following actions use the email address of the default or primary account:

- New message
- New event

To change the email address of the sender while composing a new mail from the **All Accounts** view, tap the default address in the **From:** field and select a different account from the mail accounts that appear.

> **Note:**
>
> Composing an email from the conversation view auto-populates the **From**: field with the email address that conversation is addressed to.

Individual accounts

All the accounts you have configured appear as a list below **All Accounts.** The default or the primary account always appears first followed by the other accounts in alphabetical order.

The individual accounts display any subfolders you might have created. You can view the subfolders folders by tapping the **V** icon next to the folder.

The following actions are limited to individual accounts only:

- Moving items.
- Composing emails from conversation view.
- Importing vCard.
- Saving contacts.

Calendar

The calendar displays all events pertaining to the multiple accounts on your device. You can set colors to individual accounts to differentiate calendars events pertaining to individual accounts.

To set colors to calendar events

1. Tap the **Calendar** icon in the footer bar and then tap the hamburger icon in the top left.
   The **Calendar** screen displays all the accounts you have configured.

2. Tap on the default color displayed on the right of an Exchange account.
   The Colors screen displays the available colors for that account.
3. Select a color of your choice and then tap **Save**.
4. To return to the previous screen, tap **Cancel**.
   The selected color is set for all calendar events pertaining to that Exchange account.

When you are creating a calendar invitation or event, the **Organizer** field auto-populates with the email address of the default account. To change the mail account, tap this email address and select another account.

> **Note:**
>
> When you exit and then launch Secure Mail, the app restores the last configured calendar settings on your device.

Search

You can perform a global search from the **Mailboxes** or the **Contacts** view. This action displays the appropriate results after searching all the accounts in the app.
All searches from within an individual account displays results pertaining to that account only.

Print emails, calendar events, or inline images on iOS

You can now print emails, calendar events, or inline images from your iOS device.

Prerequisites

Before you begin, ensure that the following requirements are met:

- The **Block AirPrint** option is set to **OFF**.
- The **Allow viewers to print** option is disabled in IRM.

By default, the print feature is enabled in Secure Mail for iOS. The printing feature might be controlled by your administrator through administrative policies via Apple AirPrint or Microsoft Information Rights Management (IRM). In these scenarios, printing an email, calendar event, or inline image will not work and an error message might appear.

To print emails

1. Open the email item you want to print.
2. Tap the More icon on the top left of the screen. The following options appear:
   - Move

- Print

3. Tap **Print**.
   The **Printer Options** screen appears.
4. To select a printer, tap **Select Printer**.
   The **Printer** screen appears.
5. Select the printer you want to print to.
6. Tap **–** or **+** to decrease or increase the number of copies you want to print.
7. To print a specific page or a range of pages, tap **Range**.
   The **Page Range** screen appears. By default, **All Pages** is selected.
8. To change the page selection, swipe the page numbers up or down.
9. Tap **Printer Options** to go back to the **Printer Options** screen.
10. To print in black and white, tap the **Black & White** button. By default, Secure Mail prints in color.
11. Tap **Print** on the top right to print the email.
12. To cancel the print job, tap **Cancel** on the top left.

To print a calendar event

1. Navigate to calendar and select an event.
2. Tap the Print icon and follow the same instructions as mentioned in the preceding section **To print emails**.

To print inline images:

1. Open the email item with the inline image.
2. Tap the More icon. The following options appear:
   - Move
   - Print
   - Cancel
3. Tap **Print** and follow the instructions as mentioned in the proceeding section **To print emails**.

Multiple conference codes (Dial-In to a meeting)

Secure Mail for iOS supports multiple conference codes. You can now select a conference code, from a list of available conference codes, to join a meeting.

To dial-in to a meeting

1. Open a meeting invite and tap **Dial In**.
2. From the list of phone numbers that appear, select one to dial in.
3. From the list of conference codes that appear, select one to join the meeting.
4. Tap **Call** to join the meeting.

Support to print email attachments

Secure Mail for iOS supports printing email attachments.

Android features

October 23, 2020

This article discusses the Android features that are supported in Secure Mail.

Two-way contact sync

In Secure Mail for Android, you can create, edit, and delete Secure Mail contacts from your local contacts list.

Undo sent mails

In Secure Mail for Android you can undo a sent mail. Once you tap the **Send** button, you get a toast message that allows you to undo the sent action. Tap **Undo** to revert the sent action and edit the mail, mail recipients, attach or remove attachments, or discard the mail

Attachments sync in Drafts folder

In Secure Mail for Android, when the **Drafts** folder is synced, the attachments are also synced and they are available across all your devices. This feature is available on devices running Exchange ActiveSync version 16 or later.

In-app view of PDF files

In Secure Mail for Android, you can view PDF files within the app, along with bookmarks and annotations. Also available is the enhanced view of other Microsoft Office attachments.

Use Web SSO for tunneling policy for setups running Modern authentication with Microsoft Office 365

In Secure Mail for Android, a new policy called **Use Web SSO for tunneling** is added. With this policy you can tunnel OAuth traffic to go over Secure Browse. To do so:

- Set **Use Web SSO for tunneling** policy to **On**.
- Select the **Tunneled - Web SSO** option in the Network access policy.
- Exclude any host names related to OAuth from the **Background services** policy.

Drag and drop calendar events

In Secure Mail for Android, you can change the time of an existing calendar event by dragging and dropping the event. For user help documentation on this feature, see the Citrix User Help Center article, Change a calendar event time.

Support for 64-bit apps for Google Play

Secure Mail for Android supports 64-bit architectures.

Improvements to the Pull to refresh UI in Secure Mail for Android

In keeping with Material Design guidelines, we have made minor improvements to the **Pull to refresh** feature. The sync timestamp is available at the bottom of the screen when you tap the hamburger icon.

Widget for Calendar agenda

In Secure Mail for Android, the **Calendar** agenda is available as a widget. From this widget, you can view the upcoming events in the **Calendar** for a week. This feature allows you to create a **Calendar** event, view an existing event and edit the details. The **Block screen capture** policy does not apply to the widget placed on the home screen. You can, however, disable the widget using the **Allow Calendar Agenda widget** policy.

Network access policy

In Secure Mail for Android, a new option called **Tunneled - Web SSO** is added to the Network Access MDX policy. Configuring this policy gives you the flexibility to tunnel internal traffic over Secure Browse and Secure Ticket Authority (STA) in parallel. You can also allow Secure Browse connections for authentication services, like NTLM, Okta, and Kerberos. When you initially configure STA, you must

add individual FQDNs and ports of service addresses to the Background network services policy. If you configure the **Tunneled - Web SSO** option, however, you need not make these configurations.

To enable this policy for Secure Mail for Android in the Citrix Endpoint Management console:

1. Download and use the .mdx file for Android. For details see steps in Add an MDX app.
2. In the Network access policy, click **Tunneled – Web SSO** option. For more information, see App Network Access

Enhancements to Feed cards

The following enhancements have been made to the existing **Feeds** folder, in Secure Mail for Android:

- Meeting invites from all auto-synced folders appear in your Feeds card.
- View up to five Upcoming meetings in your Feeds card.
- Upcoming meetings now appear based on a 24-hour period starting from your current time. These meeting invites are categorized into **Today** and **Tomorrow**. In previous releases, upcoming meetings until the end of the day would appear in your feeds.

Viewing attachments

In Secure Mail for Android, viewing mail and calendar attachments is easy. For user help documentation on this feature, see the Citrix User Help Center article, View and attach files.

Print emails and calendar events

In Secure Mail for Android, you can print emails and calendar events from your Android device. This print functionality uses Android Print framework.

Prerequisites

- Ensure that an administrator has set the **Block Printing policy** to **OFF** in the Citrix Endpoint Management console. For information about this policy for Android, see Block Printing policy.
- If an email is IRM protected, ensure you enable the **Allow viewers to print** option in the email.

You cannot print an email or a calendar event if these policies are set inappropriately.

> **Note:**
>
> This print capability has the following known limitations:
>
> - Inline images print only if you have downloaded images by tapping **Show Pictures**. If you don't tap **Show Pictures**, only the image placeholders print.
> - In Secure Mail, large-sized emails are truncated. Before printing, tap **Download complete**

> **message** to print the complete email. If the complete message doesn't download, a truncated email prints.
> - No metadata from an email or event is added while printing these items.

To print an email

1. Open the email that you want to print.
2. Tap the More icon on the top left of the screen. The following options appear:
   - Move
   - Print

> **Note:**
>
> On tablets, you can directly use the print icon on the top left of the screen to print an email.

1. Tap **Print**. A preview of your email appears.
2. Tap the list and the following options appear:
   - Save as PDF
   - All printers
3. Tap **Save as PDF** to save your email in a PDF format.
4. Tap **All printers**. Install the printer as per your requirement.
5. Once the printer is installed, tap **Select Printer** to select a printer. The **Printer** screen appears.

   > **Note:**
   >
   > Print options vary based on the printer selected. The following image is from a Canon E480 printer and is used for representational purpose only.

6. Select the printer you want to print to. Use the following print options:
   - Manually enter the number of copies you want to print.
   - Select the paper size from the list.
   - Select the color from the list.
   - Choose the page orientation as required.
   - Select a page or a range of pages and manually enter the page range.
7. After setting up the print options, tap the Print icon on the screen.

To print an inline image

- Tap **Show pictures** within the email and follow the instructions as mentioned in the preceding section To print an email.

To print a calendar event

1. Navigate to calendar and tap an event.
2. Tap the Print icon and then follow the same instructions as mentioned in the preceding section To print an email.

Report phishing emails with ActiveSync headers

In Secure Mail for Android, when a user reports a phishing mail, an EML file is generated as an attachment corresponding to that mail. Admins receive this mail and can view the ActiveSync headers associated with the reported mail.

To enable this feature, an admin must configure the Report Phishing Email Address policy and set the Report Phishing Mechanism as **Report Via Attachment** in the Citrix Endpoint Management console. For details about configuring MDX policies for Secure Mail, see MDX policies for mobile productivity apps.

Subfolder notifications

In Secure Mail for Android, you can receive mail notifications from subfolders of your mail account.

> **Note:**
>
> - Ensure that the FCM-based push notification is enabled in the Endpoint Management console to get notifications for subfolders. For steps to configure FCM-based push notifications, see Push notifications for Secure Mail.
> - The subfolder notification feature is not available for Lotus Notes Server.

To enable notifications for subfolders

1. Go to **Settings** and then under **General**, tap **Notifications**.
2. In the **Notifications** screen, tap **Mail folders**. A list of subfolders within the inbox appears.
3. Tap to select the subfolders you want to receive notifications from. Inbox is selected by default.

   > **Note:**
   >
   > Enabling notifications for subfolders enables auto sync.

To disable subfolder notifications, clear the check boxes for subfolders you do not want to receive notifications from.

Notification channels

On devices running Android O or later, you can use the notifications channel settings to manage how your email and calendar notifications are handled. This feature allows you to customize and manage your notifications.

To configure notifications for mail or calendar reminders, open Secure Mail and navigate to **Settings > Notifications** and select the desired notification option.

You can then navigate to either **Manage mail notifications** or **Manage calendar notifications** to manage your email or calendar notifications respectively.

Alternatively, you can long press on the Secure Mail app icon on your device, select **App info** and then tap **Notifications**.

If your Vibrate setting was previously set to **Only when silent**, the Vibrate setting will change to the default vibrate setting (**Off**) with this feature.

> Note:
>
> The notifications on the lock screen are available based on how your admin has configured the Control locked screen notifications MDX policy.

Meeting response buttons within the email

In Secure Mail for Android, meeting response buttons appear within the email. When you receive an email notification about meeting invites, you can respond to the invite by tapping on one of the following options:

- Yes
- Maybe
- No

Enhancement to attachments

In Secure Mail for Android, viewing attachments is simplified. For a better experience, inessential steps are removed, while attachment options that existed in the earlier releases are retained.

You can view attachments within Secure Mail app. The attachment opens directly, if it can be viewed using Secure Mail. If the attachment cannot be viewed using Secure Mail, a list of apps appears. You can select the required app to view the attachment. For user help documentation on this feature, see the Citrix User Help Center article, View and attach files.

Back button enhancements

In Secure Mail for Android, you can tap the back button on your device to collapse the expanded options of the **Floating Action** button. This action takes you back to the message or event details view.

Admin steps to enable file attachments from the Gallery in Android

In Secure Mail versions 10.3.5 and later, users can't attach images directly from the Gallery app if the Inbound document exchange (Open-in) policy is set to **Restricted**. If you want to keep this policy set to **Restricted**, but allow users to add photos from the Gallery, follow these steps in the Endpoint Management console.

1. Set **Block gallery** to **Off**.
2. Get the Gallery package ID for devices. Some examples:
    - **LG Nexus 5:**
      com.google.android.gallery3d, com.google.android.apps.photos
    - **Samsung Galaxy Note 3:**
      com.sec.android.gallery3d, com.sec.android.gallery3d.panorama360view, com.google.android.apps.p
    - **Sony Expire:**
      com.sonyericsson.album, com.google.android.apps.photos
    - **HTC:**
      com.google.android.apps.photos, com.htc.album
    - **Huawei:**
      com.android.gallery3d, com.google.android.apps.photos
3. Make the hidden policy InboundDocumentExchangeWhitelist visible:
    - Download the WorxMail APK file and wrap the file with the MDX Toolkit.
    - Find the .mdx file on your computer and change the file suffix to .zip.
    - Open the .zip file and find the policy_metadata.xml file
    - Search for and change InboundDocumentExchangeWhitelist from `PolicyHidden>**true**</PolicyHidden>` to `<PolicyHidden>**false**</PolicyHidden>`.
    - Save the policy_metadata.xml file.
    - Select all the files in that folder and compress to create the .zip file.

      > **Note:**
      >
      > Don't zip the outer folder. Select all files inside the folder and compress the selected files.

    - Click the resulting compressed file.

- Choose **Get Info** and change the file suffix back to .mdx.

4. Upload the modified .mdx file to the Endpoint Management console and add the list of Gallery package IDs to the now-visible Inbound document exchange whitelist policy.

   Ensure that the package IDs are comma-separated:

   com.sec.android.gallery3d, com.sec.android.gallery3d.panorama360view, com.google.android.apps.photo
5. Save and deploy Secure Mail.

Android users can now attach an image from the Gallery app. For user help documentation on this feature, see the Citrix User Help Center article, View and attach files.

Supported file formats

An X indicates a file format that can be attached, viewed, and opened in Secure Mail.

Format	iOS	Android
Video: H.263 AMR NB codec_Mp4		X
Video: H.263 AMR NB codec_3gp		X
Video: H.264 AAC codec_3gp	X	X
Video: H.264 AAC codec_mp4	X	X
Video: H.264 Acclc codec_mp4	X	X
GTM recorded_wmv		X
AVI		X
WAV	X	X
MP4	X	X
3GP	X	X
Flac		X
AAC	X	X
M4A	X	X
3GP(AMR-NB)	X	X
MP3	X	X
WAV	X	X

Format	iOS	Android
OGG		X
ICO	X	X
JPEG	X	X
PNG	X	X
TIF (single-page only)	X	
BMP	X	X
GIF	X	X
WebP		X
DOT	X	X
DOTX		X
PDF	X	X
PPT	X	X
PPTX	X	X
PPS		X
PPSX		X
DOC	X	X
DOCX	X	X
XLS	X	X
XLSM	X	X
XLSX	X	X
TXT	X	X
POT	X	X
POTX		X
HTM	X	X
HTML	X	X
ZIP	X	X
EML	X	X

Calendar

The calendar displays all events pertaining to the multiple accounts on your device. You can set colors to individual accounts to differentiate calendars events pertaining to individual accounts.

> **Note:**
>
> The Personal calendar feature is always associated with your primary or default account if enabled.

To set colors to calendar events

1. Tap the **Calendar** icon in the footer bar and then tap the hamburger icon in the top left.
   The **Calendars** screen displays all the accounts you have configured.
2. Tap on the default color displayed on the right of an Exchange account.
   The Colors screen displays the available colors for that account.
3. Select a color of your choice and then tap **Save**.
4. To return to the previous screen, tap **Cancel**.
   The selected color is set for all calendar events pertaining to that Exchange account.

When you are creating a calendar invitation or event, the **Organizer** field auto-populates with the email address of the default account. To change the mail account, tap this email address and select another account.

Search

You can perform a global search from the **Mailboxes** or the **All Contacts** view. This action displays the appropriate results after searching all the accounts in the app.

All searches from within an individual account displays results pertaining to that account only.

Updates to background services

To meet the Google Play Background Execution Limits requirement on devices running Android 8.0 (API level 26) or later, we have upgraded Secure Mail background services. For uninterrupted mail sync and notifications on your device, enable Firebase Cloud Messaging (FCM) service push notifications. For more details about enabling FCM-based push notifications, see Push notifications for Secure Mail

Ensure that you turn on **Mail notifications** in Secure Mail settings on your device. For more details about this update, see this Support Knowledge Center article.

Limitations:

- If you have not enabled FCM-based push notifications, background sync occurs once in every 15 minutes. This interval varies depending on whether the app is running in the background or the foreground.
- When users manually update the time from device settings, the date in the calendar widget does not update automatically.

Android Enterprise in Secure Mail

Secure Mail and Secure Web for Android is compatible with Android Enterprise, formerly known as Android for Work.

Prerequisites

- To be able to use this feature, ensure that your device is running Android 5.0 or later.
- For on-premises deployments, the **afw.accounts** Endpoint Management property must be set to **TRUE**.

After you have set up Android Enterprise in Endpoint Management, the mobile productivity apps are available on your device. The Android Enterprise icon identifies the apps, as highlighted in the following image.

Features that are compatible with Android Enterprise

The following table lists the Secure Mail features that are compatible with Android Enterprise.

Feature	Support
Exchange Server auto discovery	X
Secure Ticket Authority (STA)	X
Export contacts	X
Microsoft Information Rights Management	X
Lock-screen notifications	X
Mail sync	X
Email classification	X
S/MIME signing and encryption	X
Firebase Cloud Messaging (FCM) service	X
Modern authentication (OAuth)	

Feature	Support
Multiple Exchange accounts	X
Personal calendar	
Export mail settings	X
Shared devices	
Endpoint Management integration with Microsoft Intune/EMS	
Office 365	X
LDAP Exchange Server 2010, 2013, and 2016	X
Certificate based authentication (CBA)	
Go ToMeeting	X
Skype for Business	
Personal distribution list	X
Citrix Files compatibility	X
Email enrollment with single sign-on	X

The following table below lists the Secure Web features that are compatible with Android Enterprise.

Feature	Support
Secure Browse mode	X
Full VPN mode	X
All app features	X
Compatibility with Secure Mail	X

Limitations

- If **Allow use of the status bar** device restrictions policy is set **ON** for Android Enterprise in Work profile mode then calendar export progress and push notifications in Secure Mail for Android is not displayed in the status bar. However, these notifications are seen on the locked screen when allowed. For more information, see Android Enterprise settings.

iOS and Android features for Secure Mail

September 28, 2020

This article describes the iOS and Android features that are supported on Secure Mail.

Support for Azure Government Cloud Computing

Secure Mail supports Government Cloud Computing (GCC) High for modern authentication (OAuth) on the Azure Active Directory tenant. Secure Mail is registered as an endpoint on the GCC High, to meet the mandatory requirement by Microsoft for all the GCC High service. For details, see What's new for Azure Active Directory in Microsoft 365 Government.

With this change, you are routed to GCC High on the Azure Active Directory tenant for authentication. And the admin is required to allow permissions for Secure Mail on the Azure Active Directory tenant.

Prerequisites

Ensure that the global admin of Azure Active Directory performs the following:

- Download the latest version of Secure Mail on your device.
- Configure your Exchange account on the Secure Mail app, and allow app permission on Azure Active Directory for all users to sign in. Refer to the following screen.

> **Note:**
>
> These steps are specific only to the global admins as a one-time requirement. Once the app is granted access, you can simply upgrade from the App Store.

After the upgrade

After an upgrade, you are prompted for reauthorization after the expiration of the refresh token, which redirects you to GCC High on Azure AD. Validate the preceding workflow to ensure that the authorization request is sent to GCC High on Azure AD.

You can validate the workflow in one of the following ways:

- Secure Mail with app name **Secure Mail-GCC High** appears on the sign-in page in your Azure Active Directory tenant.
- Check the Secure Mail logs to confirm whether the redirects occur via https://login.microsoftonline.us after reauthentication.

Support for ICS files

In Secure Mail, you can preview the ICS files that you receive as attachments, and import it to your calendar as Events.

Contact picture in Secure Mail

In Secure Mail, view a picture of a contact when you add recipients in emails or meeting invites. For user help documentation on this feature, see the Citrix User Help Center article Show pictures of your contacts.

Manage your feeds

In Secure Mail, you can now organize your **Feed** card based on your requirements. For user help documentation on this feature, see the Citrix User Help Center article, Organize your email.

Use the Office 365 Exchange Server policy to define the Office 365 server address

In Secure Mail, a new policy called **Office 365 Exchange Server** is added under the section OAuth Support for Office 365. With this policy you can define the host name for the Office 365 mailbox present on Cloud. This policy also enables support of Office 365 for Government agencies. The host name is a single value such as *outlook.office365.com*. The default value is *outlook.office365.com*.

Support for encryption management

Encryption management allows you to use modern device platform security while also ensuring the device remains in a sufficient state to use platform security effectively. By using encryption management, you eliminate local data encryption redundancy since file system encryption is provided by the iOS or Android platform. To enable this feature, an admin must configure the **Encryption type** MDX policy to **Platform encryption with compliance enforcement** in the Citrix Endpoint Management console.

To use the encryption management feature, in the Citrix Endpoint Management console, set the **Encryption type** policy to **Platform encryption with compliance enforcement**. This enables encryption management and all the existing encrypted application data on users' devices seamlessly transition to a state that is encrypted by the device and not by MDX. During this transition, the app is paused for a one-time data migration. Upon successful migration, responsibility for encryption of locally stored data is transferred from MDX to the device platform. MDX continues to check compliance of the device upon each app launch. This feature works in both MDM + MAM and MAM-only environments.

When you set the **Encryption type** policy to **Platform encryption with compliance enforcement**, the new policy supersedes your existing MDX Encryption.

For details about the encryption management MDX policies for Secure Mail, see the **Encryption** section in:

- MDX policies for mobile productivity apps for Android
- MDX policies for mobile productivity apps for iOS

When a device falls below the minimum compliance requirements, the **Non-compliant device behavior** policy allows you to select what action is taken:

- **Allow app** – Allow the app to run normally.
- **Allow app after warning** – Warn the user that an app does not meet the minimum compliance requirements and allows the app to run. This is the default value.
- **Block app** – Block the app from running.

Devices running iOS

The following criteria determine whether a device meets the minimum compliance requirements for devices running iOS:

- iOS 10 - An app is running operation system version that is greater than or equal to the specified version.
- Debugger access - An app does not have debugging enabled.
- Jailbroken device - An app is not running on a jailbroken device.
- Device passcode - Device passcode is **ON**.
- Data sharing - Data sharing is not enabled for the app.

Devices running Android

The following criteria determine whether a device meets the minimum compliance requirements for devices running Android:

- Android SDK 24 (Android 7 Nougat) - An app is running operation system version that is greater than or equal to the specified version.
- Debugger Access - An app does not have debugging enabled.
- Rooted devices - An app is not running on a rooted device.
- Device lock - Device passcode is **ON**.
- Device encrypted - An app is running on an encrypted device.

Support for responsive emails

Secure Mail has been optimized to deliver responsive email. Previously, email content with large tables or images were rendered incorrectly. This feature delivers email content as more readable on all supported devices irrespective of the email format and size.

Drag and drop calendar events

In Secure Mail, you can change the time of an existing calendar event by dragging and dropping the event. For user help documentation on this feature, see the Citrix User Help Center article, Change a calendar event time.

Manage your feeds

In Secure Mail, you can now organize your **Feed** card based on your requirements. For user help documentation on this feature, see the Citrix User Help Center article, Organize your email.

Auto Advance

In Secure Mail, when you delete a message in **Conversations**, you can choose which message you return to. To use this feature, navigate to **Settings > Auto Advance**. Then, select your preference from the available choices. For user help documentation on this feature, see the Citrix User Help Center article Delete and auto advance to an email in Conversations.

Drafts folder auto-sync

The drafts folder is automatically synced and your drafts are available across all your devices. This feature is available on devices running Office 365 or Exchange Server 2016 and later.

> **Note:**
>
> If your Secure Mail draft contains attachments, the attachments are not synced to the server.

For user help documentation on this feature, including a video, see the Citrix User Help Center article, Drafts folder auto-sync.

Support for single sign-on while using Microsoft Intune in MDM + MAM mode

For devices running iOS:

To be able to use this feature, ensure that Microsoft Authenticator app is installed on your device. For more information about installing the Microsoft Authenticator app, see **Download and install the Microsoft Authenticator** app on Docs.microsoft.com.

For devices running Android:

To be able to use this feature, ensure that Intune Company Portal app is installed on your device. Once you log in to the Intune Company Portal app, you are able to use SSO in the MDM + MAM mode without having to reauthenticate in Secure Mail using your credentials

Enhancements to Contacts

In Secure Mail, when you tap **Contacts** and select a contact, the details of that contact appear under the **Contact** tab. When you tap the **Organization** tab, the organization hierarchy details, such as **Manager**, **Direct Reports**, and **Peers** appear. When you tap the more icon on the top right of the screen, the following options appear:

- Edit
- Add to VIP
- Cancel

In the **Organization** tab, you can tap the more icon to the right of **Manager**, **Direct Reports**, or **Peers**. This action allows you to either create an email or a calendar event. The **To:** field of the email or calendar event is automatically populated with the details of **Manager**, **Direct Reports**, or **Peers**. You can compose and send the email.

Prerequisites

Ensure that Exchange Web Services (EWS) is enabled on your Exchange Server.

The contact details appear based on the organizational details (Outlook contact) fetched from Active Directory. For the correct details to appear for your contacts, ensure that your admin has configured your organizational hierarchy in Active Directory.

> **Note:**
>
> This feature is not supported on IBM Lotus Notes server.

Export Meeting Time and Location to your native calendar

In Secure Mail, a new value **Meeting Time, Location** is added to **Export Calendar** MDX policy. This enhancement allows you to export meeting time and location of Secure Mail calendar events to your native calendar.

Multiple Exchange accounts

From Settings within Secure Mail, you can add multiple Exchange email accounts and switch between them. This feature allows you to monitor all your mails, contacts, and calendars in one place. The

admin prerequisites are as follows:

- A user name and password is required to configure more accounts. Automatic enrollment or credential store configurations applies only to the first account setup in the app. Type the user name and password for all additional accounts.
- If the first account you create is certificate-based, you cannot add further certificate-based accounts. Additional accounts must use authentication based on Active Directory. Secure Mail does not support certificate-based authentication when configuring multiple accounts.
- To allow more accounts to connect to a domain or Exchange Server in an external network, you must set split tunneling to **ON** in Citrix ADC.
- Secure Mail for iOS supports Exchange and Office 365 mail servers only.

For user help documentation on this feature, see the Citrix User Help Center article, Add Exchange accounts.

Contacts

For user help documentation on Contacts, see the Citrix User Help Center article, View and sync your contacts.

Set colors in Calendars

For user help documentation on this Calendar feature, see the Citrix User Help Center article, Set colors for synchronized Secure Mail calendars.

Internal domains

You can identify and edit mail recipients that belong to external organizations.

Prerequisite: Ensure that you have enabled the **Internal Domains** policy in Citrix Endpoint Management, and restarted the application.

When you create, reply to, or forward an email, external recipients are highlighted in the mailing list. The **Contacts** icon appears as a warning at the bottom left of the screen. Tap the **Contacts** icon to modify the mailing list.

On devices running iOS:

On devices running Android:

When you tap the **Contacts** icon, a pop-up window appears with options to edit list or remove all. Tap **Edit list** to choose the recipients that you want to remove. After selecting the recipients, tap the **Bin** icon.

On devices running iOS:

On devices running Android:

Ergonomic improvements

With this enhancement, the action buttons are moved from the top of the screen to the bottom for easy access. These changes are made to the **Inbox**, **Calendar**, and **Contacts** screens.

> Note:
>
> For Android, the changes are made to the **Inbox** and **Calendar** screens.

On devices running iOS

On devices running Android

The **Respond** floating action button is enhanced to align with Citrix branding and style guide.

Also, with this enhancement the option to access the buttons on the main Inbox screen from an open email is removed. You have to exit from the opened email to access items such as **Feeds**, **Calendar**, **Contacts**, and **Attachments**.

The options in the footer bar of iOS have been changed, which helps maintain uniformity between both iOS and Android.

Secure Mail integration with Slack (Preview)

You can now take your email conversation over to Slack app on devices running iOS or Android. For details, see Secure Mail integration with Slack (Preview).

Report phishing email (as a forward)

In Secure Mail, you can use the Report as phishing feature to report an email (as a forward) that you suspect of phishing. You can forward the suspicious messages to email addresses that admins configure in the policy. To enable this feature, an admin must configure the Report Phishing Email Address policy and set the **Report Phishing Mechanism** as **Report Via Forward**. For user help documentation on this feature, see the Citrix User Help Center article, Report a phishing email.

Report a phishing email

You can report a phishing email based on the policy an admin configures. For user help documentation on this feature, including details on admin settings, see the Citrix User Help Center article, Report a phishing email.

Export Secure Mail calendar events

Using Secure Mail for iOS and Android, you can export Secure Mail calendar events to your device's native calendar app. For user help documentation on this feature, see the Citrix User Help Center article, Export your Secure Mail calendar events.

The following MDX policy values are available for the calendar event fields that appear in your personal calendar:

- None (Don't Export)
- Meeting Time
- Meeting Time, Location
- Meeting Time, Subject, Location
- **(For Android)** Meeting Time, Subject, Location, Notes
- **(For iOS)** Meeting Time, Availability, Attendees, Subject, Location, Notes

Android options:

iOS options:

For iOS

Although calendar events exported from Secure Mail are **read/write**, changes made to events outside of Secure Mail are not available.

Important:

- This feature is visible but disabled in Secure Mail if one of the following is true:
  - The Export Calendar policy is set to **OFF**.
  - Your MDX version does not contain the policy
- This feature does not work if email accounts are already configured in your personal calendar app and your iCloud account is disabled. This feature works if no other account is configured in your personal calendar app.
- To launch the URL and edit the Secure Mail calendar events from your personal calendar, ensure that the value **"ctxevent:"** is included in the App URL Schemes MDX policy.

For Android

Calendar events that are exported from Secure Mail are read-only. To edit Secure Mail events, tap the **Secure Mail Event** link in your calendar event.

Important:

- This feature is visible but disabled in Secure Mail if one of the following is true:
  - The Export Calendar policy is set to **OFF**.

  - Your MDX version does not contain the policy.
- Ensure that the Inbound Document Exchange MDX policy is set to **Unrestricted**.
- The Secure Mail Event link is not available on Samsung and Huawei devices.

Feed folders

Secure Mail features all your unread emails, meeting invites that require your attention, and your upcoming meetings in the **Feeds** folder.

To view your feed cards

Tap the **Feeds** icon at the bottom right in the footer tab bar.

The following feed cards appear:

- Unread
- Meeting invites
- Upcoming meetings

By default, Secure Mail displays feeds from your primary account only. If you have configured more than one account, you can view feeds from another account. To view feeds from other account, tap **Feeds**, tap the hamburger icon, and then select the respective account.

Feeds are sorted based on the timestamp of the item and appear with the following upper limit:

- Five unread emails
- Two meeting invites
- Three upcoming meetings

To view all the items in a feed card, tap **See all**.

> **Note:**
>
> The number of feeds displayed in each card depends on the sync mail period you have set on your device.

Enhancements to the Feeds folder

Following are the enhancements to the existing **Feeds** folder:

- Meeting invites from all auto-synced folders appear in your Feeds card.
- View up to five upcoming meetings in your Feeds card.
- Upcoming meetings for the next 24-hour period appear in the Feeds card and are categorized into **Today** and **Tomorrow** sections.

Feeds from your Manager

In Secure Mail, you can view emails from your manager in the **Feeds** screen. Up to five emails appear under the **From Your Manager** feeds, based on your **Sync mail period** settings. To view more emails from your manager, tap **See all**.

Prerequisites:

Ensure that Exchange Web Services (EWS) is enabled on your Exchange Server.

The manager card appears based on the organizational details (Outlook contact) fetched from Active Directory. For the correct details to appear in the manager feed, ensure that your admin has configured your organizational hierarchy in Active Directory.

> **Note:**
>
> This feature is not supported on IBM Lotus Notes server.

Joining meetings from calendar

In Secure Mail, users can join meetings directly from invitations in Calendar. The following tables list which meeting types and phone number formats are supported, and dial-in requirements for each.

Supported meeting types

Meeting type	Identification requirements	Action after tapping Join Meeting
GoToMeeting (GTM)	One of the following in the meeting content: 1) This type of URL: `https://www1.gotomeeting.com/join/1234567892`; 2) GTM access code in any of these formats: GTM: 123456789, GTM – 123456789, G2M – 123456789, G2M: 123456789	If the GTM app is installed, the app opens and user joins meeting. If the app is not installed, the user sees an option to go the app store to install GTM. For GTMs in the gotomeet.me/username format, the app opens and the user joins the meeting.

Meeting type	Identification requirements	Action after tapping Join Meeting
WebEx		Citrix Secure Web opens and opens the unwrapped WebEx app, if installed on the device. WebEx must be added as an exception in the Secure Web Restricted Open-in exception list on Android and in the Allowed URLs policy on iOS.
Skype for Business		Users can click a link that opens in Secure Web, which then opens the unwrapped Skype for Business app if installed on the device. Add the Skype for Business app as an exception in the Secure Web Restricted Open-In exception list policy on Android. Add the exception in the Allowed URLs policy on iOS.

Configuring the following list of policies allows users to tap a meeting link to open the relevant app.

Zoom app

- **iOS - "Allow URLs" Policy":** +^zoomus:
- **Android - "Open-in Exclusions" Policy:**{action=android.intent.action.VIEW scheme=zoomus package=us.zoom.videomeetings}

Webex (unwrapped app)

- **iOS - "Allow URLs" Policy":** +^wbx: Example policy string is ^http:,^https:,^mailto:=ctxmail:,+^citrixreceiver g2m-2:,+^col-g2w-2:,+^wbx:,+^maps:ios_addr:
- **Android - "Open-in Exclusions" Policy:** {action=android.intent.action.VIEW scheme=wbx package=com.cisco.webex.meetings}

Skype for Business

- **iOS - "Allow URLs" Policy":** +^lync:
- **Android - "Open-in Exclusions" Policy:**{action=android.intent.action.VIEW scheme=lync package=com.microsoft.office.lync15}

Skype

- **iOS - "Allow URLs" Policy":** +^skype:
- **Android - "Open-in Exclusions" Policy:** {action=android.intent.action.VIEW scheme=skype package=com.skype.raider}

Dial-in specifications

The following list indicates the type of meeting and the respective supported phone number format and conference code format for each.

GoToMeeting (GTM):

Supported phone number formats:

- Any phone number in GTM formats. Examples:
  - India (toll-free): 000 800 100 7855
  - United States (toll-free): 1 877 309 2073
- Any phone number that satisfies RFC 3966 format standards. For details, see the Internet standards track protocol document.

Supported conference code formats:

The conference code is picked up from any of the following formats in the meeting body:

- URL (*.gotomeeting.com/join/123456789)
- URL (`gotomeet.me/username` format)
- "GTM" formats, such as "GTM:123456789"
- "G2M" formats such as "G2M:123456789"
- Formats, such as "Access Code: 123456789"

WebEx:

Supported phone number formats:

- Any phone number in WebEx Call-in formats. Examples (both Verizon and U.S.):
  - 1-866-652-5088
  - 1-517-466-3109
- Any phone number in WebEx Audio Connection formats. Example:
  - 1-650-479-3207 (US toll)

- Any phone number that satisfies RFC 3966 format standards.

Supported conference code formats:

The meeting content must contain one of these formats:

- Meeting number: 123 456 789
- Access code: 123 456 789

> **Note:**
>
> For conference codes that are nine digits or fewer, the # key is added automatically to dial in to the meeting.

Skype for Business

Supported phone number formats:

- Any phone number in RFC 3966 formats. For details, see the Internet standards track protocol document.

Supported conference code formats:

The meeting body contains this text: “Conference ID: 123456789”

> **Note:**
>
> The # key is added automatically for Skype for Business meetings.

Generic audio conference information

Supported phone number formats:

- Any phone number in RFC 3966 formats For details, see the Internet standards track protocol document. Examples:
  - 5555555555
  - (555) 555-5555
  - 555-555-5555
  - 555-555-555-5555 (in case of country code)
  - 1-555-555-5555
  - +1-555-555-5555

> **Note:**
>
> Use a single separator between digits in the phone number. For example, “) –” can cause the number not to be recognized.

Supported conference code formats:

Recommended format: “(phone number)”,”(code)”

You can specify up to four commas and provide the # key if necessary. See the table later in this document for a list of supported formats.

For an audio conference, the following formats let users tap **Dial In**. If they tap the phone number from the body of the calendar meeting, however, they can dial into the meeting. They must then type conference codes manually. The following phone number and conference code formats are supported.

Supported phone number formats	Conference code separator	Example
Any phone number in RFC 3966 formats. Examples: 5555555555; (555) 555-5555; 555-555-5555; 555-555-555-5555 (in case of country code); 1-555-555-5555;+1-555-555-5555	Participant Code	1-888-999-9999 Participant Code: 9999999
	Participant PIN	1-888-999-9999 Participant PIN: 99999999
	Guest Code	1-888-999-9999 Guest Code: 99999999
	Guest PIN	1-888-999-9999 Guest PIN:99999999
	Participant/Guest Code	1-888-999-9999 Participant/Guest Code:99999999
	Chair Code	1-888-999-9999 Chair Code:99999999
	Chair PIN	1-888-999-9999 Chair PIN:99999999
	Chairperson Code	1-888-999-9999 Chairperson Code:99999999
	Chairperson PIN	1-888-999-9999 Chairperson PIN:99999999
	Host PIN	1-888-999-9999 Host PIN:99999999

Supported phone number formats	Conference code separator	Example
	PIN	1-888-999-9999 PIN:99999999
	Access Code	1-888-999-9999 Access Code:99999999
	Code	1-888-999-9999 Code:99999999
	Conference Code	1-888-999-9999 Conference Code:99999999
	Conference ID	1-888-999-9999 Conference ID:99999999
	,	+1 (631) 992-3240,958209234#
	„	+1 (631) 992-3240„958209234#
	„,	+1 (631) 992-3240„,958209234#
	„„	+1 (631) 992-3240„„958209234#
	passcode	+1 (631) 992-3240 passcode 958209234#
	ext:	+1 (631) 992-3240 ext:958209234#
	ext.	+1 (631) 992-3240 ext. 958209234#
	;ext=	+1 (631) 992-3240; ext. 958209234#
	extn	+1 (631) 992-3240 extn 958209234#
	HC	+1 (631) 992-3240 HC 958209234#
	xtn	+1 (631) 992-3240 xtn 958209234#
	xt	+1 (631) 992-3240 xt 958209234#

Supported phone number formats	Conference code separator	Example
	x	+1 (631) 992-3240 x 958209234#
	PC	+1 (631) 992-3240 PC 958209234#
	pc	+1 (631) 992-3240 pc 958209234#

Personal calendar overlay

On iOS and Android devices, you can import your personal calendar from the native calendar app and view your personal events in Secure Mail. For user help documentation on this feature, see the Citrix User Help Center article, View your personal calendar events.

Insert an inline image

The following procedure describes how to insert an inline image.

1. To attach an inline image to your email, long press in the mail body. From the options that appear, tap **Insert Picture**.
2. Secure Mail may prompt you for access to your Photos. The Photos gallery appears. Navigate to the gallery and tap picture you want to insert.
3. The mail now contains the image you selected.

Swiping actions

On iOS and Android devices, you perform actions by swiping an email either left or right. For user help documentation on this feature, see the Citrix User Help Center article, Use swipe actions.

Join Skype for Business meetings on iOS and Android

You can join Skype for Business meetings seamlessly through Secure Mail. This feature requires the Skype for Business app to be installed on your device.

To join a Skype for Business meeting

1. Tap on the Skype for Business meeting reminder or calendar event.

2. In the **Event Details** screen, tap the Skype **Join Meeting**. The Skype for Business meeting starts in a new window.

   If you have not installed Skype for Business on your device, tap **Install Skype** to install the app.

In-app preview of attachments and other enhancements to attachments

You can now preview attachments (MS Office and images) in Secure Mail in-app, rather than by opening it by using third-party apps, such as QuickEdit.

You can perform the following actions when viewing attachments:

- Select an existing message from your mailboxes to attach the file to.
- Select a new message to attach the file to.
- Save attachment for offline access.
- Delete attachment from offline files.
- Open attachment using a different application.
- View the source email or calendar event of the attachment.

> **Note:**
>
> You can view the source email or calendar event when viewing attachments from the **Attachments** repository only.

You can also preview attachments in the following cases:

- Viewing a message.
- Composing a new message.
- Attachments folder.
- Calendar events.

To select a message to attach the file to

1. Open the email with the attachment.
2. Tap the attachment.
3. Tap the **Attach** icon.

   The Inbox appears.
4. Select an existing message to attach this file to or tap **New message** to attach this file to a new message.

To save the attachment for offline access

1. Open the attachment.

2. Tap the **More** icon on the top right of the page and tap **Save for Offline Access** to save the attachment for offline access.

To delete the attachment from offline files

1. Open the attachment.
2. Tap the **More** icon on the top right of the page and tap **Remove from Offline Files** to delete the attachment from the offline files.

To open the attachment by using a different application

1. Open the attachment.
2. Tap the **More** icon on the top right of the page and tap **Open with.** to open the attachment using a different application.
3. From the options that appear, tap on the one you want to open the attachment with.

To view the source email or calendar event of the attachment

1. Tap the **Attachments** icon in the bottom right of your screen.
2. Tap **OFFLINE**.
3. Tap the attachment and then tap the **More** icon on the top right of the screen.
4. The source email appears.

Migrating user names to email addresses (UPN)

In Secure Mail for iOS and Android, you can migrate from an Exchange user name and password based authentication to a UPN and password based authentication.

With this feature enabled, you do not have to do any of the following:

- Reinstall Secure Mail.
- Delete and add the account in Secure Mail.
- Change the user name in Secure Mail.

Prerequisites

Before you proceed with this migration, ensure that users are running Secure Mail version 10.7.25 or later.
To use this feature, you must enable the Attempt Username Migration On Auth Failure policy.

To migrate to UPN-based authentication

1. Enable the Attempt Username Migration On Auth Failure policy in Endpoint Management.
2. Migrate your Exchange user account to a new UPN that matches the user's primary SMTP email address.
   This triggers an Authentication Failure. Secure Mail attempts authentication by using the primary SMTP email address.

On successful authentication, the user account is migrated to the updated UPN.

To verify the migration

On iOS devices: Go to **Settings** and then tap the account to view the details. On successful migration, the primary SMTP email address appears in the **User Name** field in the **ACCOUNT** screen.

On Android devices: Go to **Settings** and then tap the account to view the details. On successful migration, the primary SMTP email address appears in the **Username** field in the **Account details** screen.

Personal distribution lists

Prerequisites

- Exchange Web Services (EWS) is enabled on your Exchange Server.
- Microsoft Exchange Server version 10 SP1 or later.

Secure Mail for iOS and Android supports Personal Contact Groups. You can view contact groups that you have created on your Outlook desktop client in Secure Mail. The contact groups that you have created appear in Contacts in Secure Mail.

> **Note:**
>
> You cannot view members of a nested contact group in Secure Mail.

You can use the Personal distribution lists when you compose an email or create a calendar event. If you have created a Personal Contact Group (Distribution List) using Exchange, you can view the list in Secure Mail.

To view a personal distribution list

1. In Secure Mail, open **Contacts**.
2. Type the name of the contact group.
   The group appears in the search result.
3. Tap the contact group to view the members.

> **Note**:
>
> You cannot edit a contact group in Secure Mail.

To compose a mail to a contact group

1. Open Secure Mail and tap the **Edit** floating action button to compose a mail.
2. In the **New Message** screen, type the contact group's name in the **To:** field.
3. From the list of contacts that appear, select the contact group.

   Contact groups are denoted by the following icon:

To send a calendar invite to a contact group

1. Open Secure Mail and navigate to **Calendar**.
2. Tap the **+** icon to create a calendar event.
3. In the **New Event** screen, tap **Invitees** to add members.
4. Type the contact group's name to send the invite to the group.
5. From the list of contacts that appear, select the contact group.

Rich text signatures

In Secure Mail for iOS and Android, you can use images or links in your email signature. To update your signature, simply copy and paste images or links in the signature field.

To add a rich text signature

1. Copy the image or URL you want to use.
2. Navigate to **Secure Mail > Settings > Signature**.
3. Paste the image or URL.

Alternatively, on iOS devices, you can long press in the signature field and tap **Insert Picture** to select an image from your gallery.

Folder sync

In Secure Mail for iOS and Android, you can tap the **Sync** icon to refresh all Secure Mail content. The **Sync** icon is present in Secure Mail slide outs, such as Mailboxes, Calendars, Contacts, and Attachments. When you tap the **Sync** icon, those folders that you have configured to auto refresh such as

Mailboxes, Calendars, Contacts are updated. The timestamp of the last sync appears next to the **Sync** icon.

To sync your folders

1. Open Secure Mail.
2. From the available folders at the footer tab bar, tap the folder you want to sync.
3. Tap the hamburger icon in the top left of your screen.
4. Tap the **Sync** icon in the bottom left of your screen.
5. The folder is synced and your content is refreshed. The timestamp appears next to the **Sync** icon.

Photo attachment improvements

In Secure Mail for iOS and Android, you can attach photos easily by tapping the new **Gallery** icon.

To attach photos to your email

1. Open Secure Mail.
2. Tap **Compose** to create a mail or tap the **Respond** floating action button to respond to an email.
3. Tap the **Gallery** icon next to the **Attachments** icon in the bottom right of your screen.
4. Your gallery appears at the bottom of your screen along with the **Camera** and **Recent** icons.
5. Navigate and select the images you want to attach from your gallery or tap the **Camera** icon to take a picture.

> **Note:**
>
> When you tap the **Attachments** icon, the following options appear:
>
> - Files
> - ShareFile (now, Citrix Files)
> - From Mail Attachments

Secure Mail renders embedded resources while viewing an email

If the resources are present in your internal network, such as mails with image URLs that are internal links, Secure Mail connects to the internal network to fetch the content and render it.

Support for modern authentication

Modern authentication is OAuth token-based authentication with user name and password. This support includes support for Office 365 for internal and external Active Directory Federation Services (AD FS) or identity provider (IdP).

Allow Secure Web domains MDX policy for Secure Mail

In Secure Mail, some external URLs must open in a native browser rather than in Secure Web. As a result, by default, all URLs open in a native browser. You can, however, create a list of URLs that you specifically want to open in Secure Web. To do so, you configure an MDX policy in the Citrix Endpoint Management console called Allowed Secure Web Domains.

After you deploy the policy, a list of comma-separated URL host domains are matched against the host name portion of any URL the application would normally send to an external handler. Typically, you configure this policy as a list of internal domains for Secure Web to handle.

If you leave the policy blank, which is the default setting, all web traffic is sent to Secure Web, until you explicitly exclude the URLs from filtering or otherwise redirect the URLs. To redirect the URLs, you configure the Exclude URL filter for domains MDX policy. This policy indicates the URLs that must open in the native browser. This policy takes priority over the Secure Web domains policy.

You can configure these MDX policies for Android and iOS.

Example configuration of Secure Web domains policy

The following procedures show how to prompt users with Secure Mail for Android to open URLs in the native Chrome browser or Secure Web. On iOS, the steps show that URLs that would normally open in a Safari browser open automatically in Secure Web.

For Secure Mail for Android

1. In the App Interaction policy list, in Restricted Open-In exception list, enter *{package=com.android.chrome}*.
2. In the App Interaction (Outbound URL) policy list, in **Allow Secure Web domains**, add the DNS suffix of the internal site.

For other third-party browsers, use the following format, accordingly:

```
{ package=<packageID of the browser> }
```

For Secure Mail for iOS

1. In the App Interaction (Outbound URL) policy list, in **Allowed URLs**, add +^*safari:*
2. In **App URL schemes**, add *safari:*

3. In **Allow Secure Web domains**, add the DNS suffix of the internal site.

Secure Mail integration with Slack (Preview)

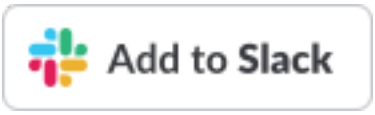
March 21, 2019

You can now take your email conversation over to the Slack app on devices running iOS or Android.

Once you enable this feature, you can do the following:

- Seamlessly switch from mail to a Slack conversation.
- Create a Slack group conversation with your mail recipients.
- Create a direct message in Slack with your mail recipient.

Prerequisites

- For admins:
  - Ensure that you have installed Secure Mail to your Slack workspace. Click **Add to Slack** button below. 

  - Ensure the **Enable Slack** policy is turned **On**. For policy details see:
    - Enable Slack policy for iOS
    - Enable Slack policy for Android
- For users: Before you proceed, ensure that you have a Slack account and the Slack app is installed on your device.

To enable this feature on your device

1. Open Secure Mail and tap the hamburger icon.
2. In the **Mailboxes** screen, tap the settings icon on the bottom right of the screen.
3. In the **Settings** screen, tap **Slack** listed under **Integrations**.
4. Provide your workspace Slack URL and then tap **Continue**.
5. Provide your credentials and then tap **Sign In**.
6. When requested to authorize Secure Mail access to information, tap **Authorize**.

You are now connected to Slack.

To use this feature

1. Open any email conversation in Secure Mail and then tap the floating action button.
2. From the available options, tap **Chat in Slack**.
3. The conversation switches over to Slack with the recipients in your email.

Keep in mind the following:

- On devices running Secure Mail for iOS or Android, you can create a Slack conversation with a maximum of eight recipients from your email. If you have more than eight recipients in your email, by default, Secure Mail picks the first eight recipients present in your email conversation.

Notifications and synchronization

May 15, 2020

This article discusses notification and email synchronization functionality and configurations for Secure Mail.

Secure Mail for iOS background app refresh

If Secure Mail for iOS is configured to provide notifications through iOS background app refresh (and not APNs), Secure Mail email refresh works in the following ways:

- When users enable **Background App Refresh** on the device from the **Settings** menu and Secure Mail is running in the background, mail is synced with the server. The sync frequency depends on various factors.
- If the user disables **Background App Refresh**, the app never receives email while running in the background.
- When users move Secure Mail to the background, the app continues to run within a grace period before the app is suspended.
- While running in the foreground, Secure Mail shows real-time email activity, regardless of the **Background App Refresh** setting.

Secure Mail and ActiveSync

Secure Mail syncs with Exchange Server via the ActiveSync messaging protocol. This functionality gives users real-time access to their Outlook mail, contacts, calendar events, automatically generated mailboxes, and user-created folders.

> **Note:**
>
> ActiveSync doesn't support the synchronization of Exchange public folders. In Exchange Server 2013, ActiveSync doesn't sync the Drafts folder.

To sync user-created folders, follow these steps:

iOS

1. Go to **Settings > Auto Refresh**.
2. Set **Auto Refresh** to **On**.
3. Tap **On**. A list of all mailboxes appears.
4. Tap the folders you want to sync.

Android

1. Go to the Mailboxes list.
2. Tap the mailbox you want to sync.
3. Tap the More icon in the lower-right corner.
4. Tap **Sync options**.
5. Under **Check frequency**, select how often you want the folder to sync.

Exporting contacts in Secure Mail

Secure Mail users can continuously sync their contacts with the phone address book, do a one-time export of an individual contact to the phone address book, or share a contact as a vCard attachment.

To allow these features, set the Export Contacts policy for Secure Mail in the Endpoint Management console to **ON**.

When the policy is **ON**, the following options are enabled in Secure Mail:

- **Sync with Local Contacts** in Settings
- Exporting individual contacts
- Share contacts as vCard attachments

When the Export Contacts policy is **OFF**, those options do not appear in the app.

When the policy is enabled, to sync contacts from the mail server to the phone address book continuously, users need to set **Sync with Local Contacts** to **ON**. As long as **Sync with Local Contacts** is **ON**, any updates to contacts in Exchange or Secure Mail triggers an update to local contacts.

Due to Android limitations, if any Exchange or Hotmail account is already set to sync with local contacts, Secure Mail is unable to sync contacts.

On iOS, Secure Mail contacts can be exported and synced with the phone contacts. The contacts can be exported and synced even if users have Hotmail or Exchange set up on the device. You configure this feature in Endpoint Management through the Override Native Contacts Check policy for Secure Mail. This policy determines if Secure Mail overrides the check for contacts from an Exchange/Hotmail Account configured in the native Contacts app. If **On**, the app syncs contacts to the device even if the native Contacts app is configured with Exchange/Hotmail Account. If **Off**, the app continues to block contacts sync. Default is **On**.

Secure Mail notifications

The following table lists how notifications are handled for supported mobile devices when Secure Mail is running in the foreground or background.

With Secure Mail running in the foreground or background:	Notifications are handled for iOS	Notifications are handled for Android
Foreground	Secure Mail maintains a persistent ActiveSync connection to sync email and calendar activity.	Secure Mail maintains a persistent ActiveSync connection to sync email and calendar activity.
Background (or terminated)	Secure Mail receives notifications through the iOS background app refresh functionality or, if configured, APNs.	Secure Mail maintains a persistent ActiveSync connection.

For configuration details, see Push notifications for Secure Mail for iOS.

Push notifications for Secure Mail

January 11, 2021

Secure Mail for iOS and Secure Mail for Android can receive notifications about email and calendar activity when the app is running in the background or is closed. Secure Mail for iOS supports notifications provided through Remote Push Notifications provided through the Apple Push Notification service (APNs). Secure Mail for Android supports notifications provided through the Firebase Cloud Messaging service (FCM).

How push notifications work

To provide push notifications for iOS and Android, Citrix hosts a listener service on Amazon Web Services (AWS) to perform the following functions:

- Listen for Exchange Web Services (EWS) push notifications sent by Exchange Servers when there is Inbox activity. Exchange does not send any mail content to the Citrix service.

  No personally identifiable information is stored by the Citrix service. Instead, a device token and subscription ID identifies the specific device and Inbox folder to be updated within Secure Mail.

- Send APNs notifications, containing only badge counts, to Secure Mail on iOS devices.
- Send FCM notifications to Secure Mail on Android devices.

The Citrix listener service does not impact mail data traffic, which continues to flow between user devices and Exchange Servers through ActiveSync. The listener service, which is configured for high availability and disaster recovery, is available in three regions:

- Americas
- Europe, Middle East and Africa (EMEA)
- Asia Pacific (APAC)

System requirements for push notifications

If your Citrix Gateway configuration includes Secure Ticket Authority (STA) and split tunneling is off, Citrix Gateway must allow traffic (when tunneled from Secure Mail) to the following Citrix listener service URLs:

Region	URL	IP Address
Americas	`https://us-east-1.pushreg.xm.citrix.com`	52.7.65.6; 52.7.147.0
EMEA	`https://eu-west-1.pushreg.xm.citrix.com`	54.154.200.233; 54.154.204.192
APAC	`https://ap-southeast-1.pushreg.xm.citrix.com`	52.74.236.173; 52.74.25.245

Configuring Secure Mail for push notifications

To set up Apple Push Notifications or FCM for Secure Mail for app store distribution, in the Endpoint Management console, set Push notifications to **ON** and then select your region. The following figure shows the setting for iOS.

For Android, the following figure shows the same **Push notification setting** as for iOS. In addition, if the EWS is hosted in a different region from where the mail server resides, complete the **EWS Host-Name** setting. The default setting is empty. If you leave the setting empty, Endpoint Management uses the host name of the mail server.

Configure Exchange and Citrix ADC to allow traffic to flow to the listener service.

Exchange Server configuration

Allow outbound SSL (over port 443) from your firewall to the Citrix listener service URL for the region where your Exchange Server is located. For example:

Region	URL	IP Address
Americas	`https://us-east-1.mailboxlistener.xm.citrix.com`	52.6.252.176; 52.4.180.132
EMEA	`https://eu-west-1.mailboxlistener.xm.citrix.com`	54.77.174.172; 52.17.147.220
APAC	`https://ap-southeast-1.mailboxlistener.xm.citrix.com`	52.74.231.240; 54.169.87.20

If you have a proxy server between Exchange Web Services (EWS) and the Citrix listener device, you can do one of the following.

- Send EWS traffic through the proxy and then on to the listener device.
- Bypass the proxy and route EWS traffic to the listener device directly.

To send EWS traffic through the proxy server, configure the EWS web.config file in the ClientAccess\exchweb\ews folder, as follows.

```
1 <configuration>
2 <system.net>
3 <defaultProxy>
```



```
<proxy usesystemdefault="true" bypassonlocal="true" />
</defaultProxy>
</system.net>
</configuration>
```

For more details about configuring proxies, see Proxy Configuration.

For Exchange 2013 environments, you must add the `system.net` section to the web.config file manually. Otherwise, configurations described in this article should work for Exchange 2013. For troubleshooting, contact your Exchange administrator.

To bypass the proxy server, configure the bypass list to allow Exchange to make connections to the Citrix listener service.

When Secure Hub is enrolled with certificate-based authentication, you must also configure Exchange Server for certificate-based authentication. For details, see Endpoint Management Advanced Concepts article.

Citrix Gateway configuration

Although the Exchange Server needs to allow traffic to the listener service, Citrix ADC must allow traffic to the registration service. In this way, devices can connect to register for push notifications.

If your EWS and ActiveSync servers are different, configure your Citrix ADC traffic policy to allow EWS traffic. For more information about integrating Citrix Endpoint Management with Citrix Gateway, see the section Integrating with Citrix Gateway and Citrix ADC.

Troubleshooting

To troubleshoot outbound connections, check the Exchange event logs, which include log entries when a subscription request or the notification for a subscription is invalid or fails. You can also run Wireshark traces on the Exchange Server to track outbound traffic to the Citrix listener service.
For other issues, use the Endpoint Management Analyzer.

Secure Mail Push Notifications FAQs

When does Android deliver notifications to Secure Mail?

In Android, notifications are always delivered to Secure Mail.

How does FCM affect email notifications that appear on the lock screen?

New mail notifications that appear on the device lock screen are generated based on data that is synced down to the device by Secure Mail. Importantly, this information does not come from the

listener service.

To show new mail notifications, Secure Mail must be able to sync data from Exchange so that Secure Mail has the information available to create the notifications.

When you receive a new mail, the **You have new messages** FCM notification appears. Once the email sync completes in the background, the new mail appears in Secure Mail.

How does Background App Refresh affect Secure Mail and APNs?

If the user turns off Background App Refresh, the following situations occur:

- Secure Mail does not receive notifications when Secure Mail is not the background app.
- Secure Mail does not update the lock screen with new email notifications.

Disabling Background App Refresh has a major effect on the behavior of Secure Mail. As stated earlier, badge updates based on APNs still occur, but no email is synced to the device in this mode.

How does Low Power Mode affect Secure Mail and APNs?

The behavior of the system with respect to Secure Mail is the same in Low Power Mode as it is when Background App Refresh is disabled. In Low Power Mode, the device does not wake up apps for periodic refresh and does not deliver notifications to apps in the background. The side effects are therefore the same as those listed in the Background App Refresh section above. Note that in Low Power Mode, badge updates still occur, based on APNs notifications.

How does APNs affect email notifications that appear on the lock screen?

New mail notifications that appear on the device lock screen are generated based on data that is synced down to the device by Secure Mail. Importantly, this information does not come from the listener service.

In order to show new mail notifications, Secure Mail needs to be able to sync data from Exchange so that Secure Mail has the information available to create the notifications.

If APNs notifications are not delivered to Secure Mail in the background, Secure Mail does not detect the notifications and hence does not sync new data. Because no new data is available to Secure Mail, no email notifications are generated on the device lock screen, even when APNs notifications are not delivered.

What other issues can cause FCM-driven sync to fail in the background?

Various issues can cause FCM-driven sync requests to fail, including the following:

- An invalid STA ticket.

- When Secure Mail is woken in the doze mode, the app has 10 seconds to sync all data from the server.

If any of the preceding conditions occurs, Secure Mail cannot sync data. As a result, lock screen notifications do not appear.

What other issues can cause APNs-driven sync to fail in the background?

A number of issues can cause APNs-driven sync requests to fail, including the following:

- An invalid STA ticket.
- A slow network connection. When Secure Mail is woken in the background, the app has 30 seconds to sync all data from the server.
- If the data protection policy is enabled and Secure Mail is woken by an APNs notification, when the device is locked, Secure Mail cannot access the data store and sync does not occur. Note that this is only the case in which the system is attempting to cold start Secure Mail. If a user has already started Secure Mail at some point after unlocking the device, APNs-driven sync succeeds even when the device is locked.

If any of the preceding conditions occur, Secure Mail cannot sync data and hence cannot display locks screen notifications.

How else does Secure Mail generate lock screen notifications when notifications are not delivered or APNs is not in use?

If APNs is disabled, Secure Mail is still woken by periodic Background App Refresh events from iOS, assuming that Background App Refresh is enabled and assuming that Low Power Mode is off.

During these wakeup events, Secure Mail syncs new email from the Exchange Server. This new email can then be used to generate email notifications on the lock screen. Thus, even when APNs notifications are not delivered or APNs is disabled, Secure Mail can sync data in the background.

It's important to note that this will occur less in real time than when APNs is in use and when APNs notifications are delivered to Secure Mail. When iOS routes APNs notifications to Secure Mail, the app immediately syncs data from the server and the lock screen notifications appear to be real time.

In the event that Background App Refresh wakeups are required, lock screen notifications do not occur in real time. In this case, Secure Mail is woken up at a frequency that iOS completely determines. As such, some time may elapse between these two situations:

- When an email arrives in a user's Inbox on Exchange.
- When Secure Mail syncs that message and generates the lock screen notification.

Also note that Secure Mail receives these periodic wakeups even when APNs is in use. In all cases

in which Background App Refresh wakes up Secure Mail, Secure Mail attempts to sync data from Exchange.

How does Secure Mail differ from other apps that show content on the lock screen?

An important difference, that may lead to confusion, is that Secure Mail does not always show new email in real time on the lock screen. This behavior differs from Gmail, Microsoft Outlook, and other apps. The primary reason for this difference is security. To align with the behavior of the other apps, the Citrix listener service requires the user credentials to authenticate with Exchange. The credentials are required to get the email content. The credentials are also required to pass this email content through the Citrix listener service and to the Apple APNs service. The approach by Citrix to APNs notifications does not require the Citrix listener service to acquire or store the users' password. The listener service has no access to the users' mailbox or password.

A note about the native iOS mail app: iOS allows its own email app to maintain a persistent connection with the mail server, which ensures that notifications are always delivered. Third-party apps outside of the native mail are not allowed this capability.

Gmail app behavior: Google owns and controls both the Gmail app and the Gmail server. This behavior means that Google can read message content and include that message content in the APNs notification payload. When iOS receives this APNs notification from Gmail, iOS does the following:

- Sets the application badge to the value that is specified in the notification payload.
- Displays the lock screen notification using the message text that is contained in the notification payload.

This is a critical difference: It is iOS, not the Gmail app, that displays the lock screen notification, based on the data contained in the payload. In fact, iOS may never wake the Gmail app, similar to the way that iOS may not wake Secure Mail when a notification arrives. However, because the payload contains the message snippet, iOS can display the lock screen notification without any mail data having to be synced to the device.

In Secure Mail, this situation is different. Secure Mail must first sync message data from Exchange before the app can show the lock screen notification.

Outlook for iOS app behavior: Microsoft controls Outlook for iOS. The organization to which the user belongs, however, controls the Exchange Servers from which data is obtained. Despite this setup, Outlook can display lock screen notifications based on data that Microsoft provides in the APNs notification. The reason is that Outlook for iOS makes use of a model in which Microsoft stores user credentials. Microsoft then directly accesses the user's mailbox from its cloud service and determines the existence of new mail.

If new mail is available, the Microsoft cloud service generates an APNs notification that contains the new mail data. This model operates in a similar way to the Gmail model. In the Gmail model, iOS

simply takes the data and generates a lock screen notification based on that data. The Outlook iOS app is not involved in the process.

Important security note on Outlook for iOS: There are clear security implications in the Outlook for iOS approach. Organizations need to trust Microsoft with passwords for their users. This trust allows Microsoft to access the user's mailbox, which poses a security risk.

For more FAQs specific to administrators on push notifications, see this Support Knowledge Center article. For more user-specific FAQs, see this Support Knowledge Center article.

Rich push notifications for Secure Mail for iOS

May 26, 2020

Secure Mail for iOS supports rich push notifications. Rich notifications ensure that you receive lock screen notifications for your Inbox even when Secure Mail is not running in the background. This feature is supported on password-based authentication and client-based authentication setups.

> **Note:**
>
> Due to the change in architecture to support this feature, the VIP Only mail notifications feature is no longer available.

To enable the rich push notifications feature, ensure that the following prerequisites are met:

- In the Endpoint Management console, set Push notifications to **ON**.
- Network access policy is set to **Unrestricted** or **Tunnel to internal network**. If your Network access policy is set to **Tunnel to internal network**, ensure that Exchange Web Services (EWS) host is configured in the Background network services policy. If EWS and ActiveSync hosts are the same, then ensure that the ActiveSync host is configured in the Background network services policy.
- The Control locked screen notifications policy is set to **Allow** or **Email sender or event title**.
- Navigate to **Secure Mail > Settings > Notifications** and then enable **Mail Notifications**.

This feature is not supported if you are running any of the following setups:

- Modern authentication with Microsoft Office 365
- Apps managed by Endpoint Management integration with Microsoft InTune/EMS
- Devices enrolled by using derived credentials

How push notifications work in Secure Mail iOS

Secure Mail receives push notifications for the following Inbox activities:

- **New mail, meeting requests, meeting cancellations, meeting updates**: When APNs pushes remote notifications to iOS Secure Mail and Secure Mail updates all folders marked for auto refresh.

  > **Note:**
  >
  > By default, the Inbox, Calendar, and Contact folders are marked for auto refresh. Users can select any other mail folder for auto refresh from **Secure Mail** > **Settings** > **Auto Refresh**.

- The Secure Mail icon shows the total count of unread and new messages in the Exchange Inbox folder only. Secure Mail updates the icon after users read emails on a desktop or laptop computer.
- During an installation or upgrade, Secure Mail for iOS prompts users to allow push notifications. Users can also allow push notifications later by using iOS Settings.

Push notifications behavior without rich push notifications support

For configurations that are not supported by the rich push notifications feature for iOS, Secure Mail still provides the count of unread Inbox emails for the sync period. If the **Control locked screen notifications policy** is **On**, push notifications appear on a locked device screen after iOS wakes up Secure Mail to perform a sync.

Secure Mail iOS push notifications FAQs

When does iOS deliver notifications to Secure Mail?

When the rich push notification feature is enabled, iOS delivers remote notifications to Secure Mail. These notifications happen even if the app is not running in background or is in low power mode.

> **Note:**
>
> When rich push notifications is not enabled, notifications may not be delivered to Secure Mail when Secure Mail is not active: This situation occurs for many reasons, such as the following reasons:

- If the device is in Low Power Mode and Secure Mail is in the background: This is the most common case in which notifications are not delivered.
- If **Background App Refresh** is **Off** for Secure Mail and if Secure Mail is in the background: Note that users control this setting.
- If the device has poor network connectivity: This situation depends on the iOS device.

Reasons for the “You have new mail” notification to appear on iOS devices

The “You have new mail” notification appears on iOS devices when Secure Mail does not receive a response from Exchange Web Services (EWS) within the specified time. The time required to fetch the message details is 30 seconds.

You may also experience this behavior on your device based on poor Wi-Fi or data connectivity.

Other than the delayed EWS response, Secure Mail displays the “You have new mail” notification in the following situations:

- When Secure Mail fails to read the required information from the secure container. This scenario generally occurs after you restart your device and before you unlock the device.
- When Secure Mail fails to connect to or set up a secure channel with Citrix Gateway or EWS.
- When your credentials have expired or you have modified the credentials, but they are not updated in Secure Mail. The following figure shows the way the notification appears in this scenario.
- When Secure Mail receives an unexpected response from the Exchange Server for a valid request from Secure Mail. For details about EWS response codes, see the Microsoft developer documentation.

Push notification failure messages in Secure Mail for iOS

In Secure Mail for iOS, appropriate push notification failure messages appear in the notification center on your device. These notifications appear based on the type of notification failure.

The following notification messages appear based on different failure scenarios as follows:

- **Secure Mail is unable to connect to your organization’s network**. This notification appears when Secure Mail fails to establish a SOCKS5 connection with Citrix Gateway.
- **Secure Mail is unable to connect to your organization’s network. Please contact your administrator.** This notification appears Citrix Gateway is unreachable. Ensure that your Citrix ADC is configured correctly and is reachable from external networks.
- **Secure Mail is unable to connect securely to your organization’s network. Please contact your administrator**. This notification appears when Secure Mail fails to establish an SSL connection with the Citrix Gateway. Ensure that your SSL certificate is valid.
- **Secure Mail is unable to connect securely to your mail server. Please contact your administrator**. This notification appears when Secure Mail fails to establish an SSL connection with the Exchange Server. Ensure that the SSL certificate on your Exchange Server is valid. If you want the app to connect to the Exchange Server despite having an invalid certificate, ensure that you have enabled the Accept all SSL certificates MDX policy.

- **Secure Mail is unable to fetch message due to a mail server error. Please contact your administrator**. This notification appears when Secure Mail cannot parse the EWS response from the Exchange Server.
- **Secure Mail is unable to fetch message due to a request timeout**. This notification appears when Secure Mail fails to receive a response from the server within 30 seconds. This notification could appear due to poor data or Wi-Fi connection on your device. Try again after waiting a few minutes.
- **Unable to fetch message. Please open Secure Mail**. This notification appears when Secure Mail cannot read your credentials from the secure container. This notification could appear when your device has been restarted, but not unlocked. Unlock your device to automatically allow Secure Mail access to the secure container. If you are still receiving this notification, then open Secure Mail to automatically update your credentials in the secure container.

Secure Mail interactivity with other mobile productivity apps and Citrix Files

August 12, 2020

Secure Mail interactivity with other mobile productivity apps and Citrix Files lets users access, edit, share, and save documents seamlessly, without leaving the secure environment set by your organization's policies. For example, tapping a link in Secure Mail opens the site in Secure Web. Users can open and edit attachments with Citrix QuickEdit for Endpoint Management. Attachments are downloaded into the user's Citrix Files for Endpoint Management space.

For a full list of Secure Mail features for each platform, see Features by platform.

Testing and troubleshooting Secure Mail

January 8, 2020

When Secure Mail isn't working properly, connection issues are typically the cause. This article describes how to avoid connection issues. If issues occur, this article describes to troubleshoot the issues.

Testing ActiveSync connections, user authentication, and APNs configuration

You can use Endpoint Management Analyzer to conduct Secure Mail autodiscovery service checks. It guides you in downloading the Endpoint Management Exchange ActiveSync Test application. The

Mail test option checks basic connection settings to the mail server. The tool also helps you troubleshoot the ActiveSync servers for their readiness to be deployed within an Endpoint Management environment. For details, see Endpoint Management Analyzer Tool.

The Mail test option in the Analyzer verifies the following:

- iOS and Android device connections with Microsoft Exchange or IBM Traveler servers.
- User authentication.
- Push notification configuration for iOS, including Exchange Server, Exchange Web Services (EWS), Citrix Gateway, APNs certificates, and Secure Mail. For information about configuring push notifications, see Push Notifications for Secure Mail for iOS.

The tool provides a comprehensive list of recommendations for correcting issues.

> Note:
>
> The Mail Test App, MailTest.ipa, is deprecated. Instead, access the same functionality in Endpoint Management Analyzer.

Prerequisites for testing

- Ensure that the Network Access policy is not blocked.
- Set the Block Email Compose policy to **Off**.

Using Secure Mail logs to troubleshoot connection issues

To obtain Secure Mail logs, do the following.

1. Go to **Secure Hub > Help > Report Issue**.
2. Select **Secure Mail** from the list of apps.

   An email addressed to your organization help desk opens.
3. Fill in the subject line and body with a few words describing your issue.
4. Select the time when it happened.
5. Change log settings only if your support team has instructed you to do so.
6. Click **Send**.

   The completed message opens with zipped log files attached.
7. Click **Send** again.

   The zip files sent include the following logs:

   CtxLog_AppInfo.txt (iOS), Device_And_AppInfo.txt (Android), logx.txt, and WH_logx.txt (Windows Phone)

App info logs include information about the device and app. Verify that the hardware model and platform version in use are supported. Verify that the versions of Secure Mail and MDX Toolkit in use are the latest and are compatible. For details, see System Requirements for Secure Mail and Endpoint Management compatibility.

- CtxLog_VPNConfig.xml (iOS) and VpnConfig.xml (Android)

The VPN configuration logs are provided for Secure Hub only. Check the Citrix ADC version `ServerBuildVersion` to ensure the latest Citrix ADC release is in use. Check the `SplitDNS` and `SplitTunnel` settings as follows:

- If Split DNS is set to **Remote**, **Local**, or **Both**, verify that you are correctly resolving the mail server FQDN through DNS. (Split DNS is available for Secure Hub on Android.)
- If Split Tunnel is set to **On**, ensure that mail server is listed as one of the Internet apps accessible on the backend.
- CtxLog_AppPolicies.xml (iOS), Policy.xml (Android and Windows Phone)

The policies logs provide the values of all MDX policies applied to Secure Mail as of the time you obtained the log. For connection issues, verify the values for the <`BackgroundServices`> and <`BackgroundServicesGateway`> policies.

- Diagnostic logs (in the diagnostics folder)

For initial configurations of Secure Mail, the most common issue is "Your Company Network Is Not Currently Available." To use the diagnostic logs to troubleshoot connection issues, do the following.

The key columns in the diagnostic logs are Timestamp, Message Class, and Message. When an error message appears in Secure Mail, make note of the time so you can quickly locate related log entries in the **Timestamp** column.

To determine whether the connection from the device to Citrix Gateway succeeded: Review the AG Tunneler entries. The following messages indicate successful connection:

- AG policy Intercepting FQDN:443 for STA tunneling
- New TCP proxy connection to (null):443 established

To determine whether the connection from Citrix Gateway to Endpoint Management succeeded (and thus can validate the STA ticket), do the following: Go to the Secure Hub diagnostic log and review the INFO (4) entries under Message Class for the time the device was enrolled. The following messages indicate that Secure Hub obtained a STA ticket from Endpoint Management:

- Getting STA Ticket.
- Got STA Ticket response.
- STA Ticket – Success obtaining STA ticket for App – Secure Mail.

> Note:
>
> During enrollment, Secure Hub sends a request to Endpoint Management for a STA ticket. Endpoint Management sends the STA ticket to the device, where it is stored and added to the Endpoint Management STA ticket list.

To determine if Endpoint Management issued a STA ticket to a user, check the UserAuditLogFile.log, included in the support bundle. It lists for each ticket, the issue time, user name, user devices, and result. For example:

Time: 2015-06-30T 12:26:34.771-0700

User: user2

Device: Mozilla/5.0 (iPad; CPU OS 8_1_2 like macOS)

Result: Successfully generated STA ticket for user 'user2' for app 'Secure Mail'

To check the communication from Citrix Gateway to the mail server: Check if DNS and networking are configured correctly. To do so, use Secure Web to access Outlook Web Access (OWA). Like Secure Mail, Secure Web can use a micro VPN tunnel to establish a connection to Citrix Gateway. Secure Web acts as a proxy to the internal or external resource the app is accessing. Usually and particularly in an Exchange environment, OWA is hosted on the mail server.

To test the configuration, open Secure Web and enter the FQDN of the OWA page. That request takes the same route and DNS resolution as communication between Citrix Gateway and the mail server. If the OWA page opens, you know that Citrix Gateway is communicating with the mail server.

If the preceding checks indicate successful communications, you know that the issue isn't with your Citrix setup. Instead, the issue is with the Exchange or Traveler servers.

You can collect information for your Exchange or Traveler server administrators. First check for HTTP issues on the Exchange or Traveler servers by searching the Secure Mail diagnostic log for the word Error. If the errors include HTTP codes and you have multiple Exchange or Traveler servers, investigate each server. Exchange and Traveler have HTTP logs that show HTTP requests and responses from client devices. The log for Exchange is C:\inetpub\LogFiles\W3SVC1\U_EX.log. The log for Traveler is IBM_TECHNICAL_SUPPORT>HTTHR.log.

To obtain crash logs from a device for Secure Mail for iOS

1. On your iOS device, go to **Settings** > **Privacy** > **Analytics** > **Analytics Data**.
2. In the **Data** list, click the name of the app and the relevant time stamp. The logs appear.

Troubleshooting issues with email, contacts, or calendar

You can troubleshoot Secure Mail issues, such as an email or emails stuck in drafts, missing contacts, or calendar items out-of-sync. To troubleshoot these issues, use Exchange ActiveSync mailbox logs. The logs show incoming requests sent by the devices and the outgoing responses from the mail server.

Unlimited sync best practices

When users set their sync mail period to **All**, they have unlimited sync. With unlimited sync, the assumption is that users manage their mailbox size, which is the Inbox and all synced subfolders. Here are a few points to keep in mind for best performance.

1. If the mailbox size exceeds 18,000 messages or 600 MB in total size, email sync can slow down.
2. It is not recommended to enable **Load Attachments on WiFi** with unlimited sync. This option can cause the mail size to bloat quickly on the device.
3. To prevent unlimited sync as an option for users, set the **Max sync interval** app policy to a value other than **All**.
4. It is not recommended to set **All** as the **Default sync interval** for users.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States