CITRIX

Secure Mail

Contents

Secure Mail overview

November 9, 2018

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.

Secure Mail is compatible with:

- Exchange Server 2016 Cumulative Update 10
- Exchange Server 2016 Cumulative Update 9
- Exchange Server 2016 Cumulative Update 8
- Exchange Server 2013 Cumulative Update 21
- Exchange Server 2013 Cumulative Update 19
- Exchange Server 2010 SP3 Update Rollup 19
- Exchange Server 2010 SP3 Update Rollup 22
- IBM Domino Mail Server version 9.0.1 FP10 HF197
- IBM Domino Mail Server version 9.0.1 FP9
- IBM Lotus Notes Traveler version 9.0.1.21
- IBM Lotus Notes Traveler version 9.0.1.9
- 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.

What's new in Secure Mail

January 23, 2019

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**, to either create a new email or a new 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** policy. This allows you to export meeting time and location of Secure Mail calendar events to your native calendar.
- A new MDX policy value **Meeting Time, Location** is available for the calendar event fields that appear in your personal 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.
  - Ensure that 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 Zoom app to join meetings. For information about configuring the required policies to use 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. To provide a better experience, inessential steps are removed but 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 else a list of apps appears. You can select the required app to view the attachment. For details, see Viewing attachments.
- **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** policy. This allows you to export meeting time and location of Secure Mail calendar events to your native calendar.
- A new MDX policy value **Meeting Time, Location** is available for the calendar event fields that appear in your personal calendar.
- Secure Mail users can use Zoom app to join meetings. For information about configuring the required policies to use Zoom app, see Joining meetings from calendar.

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

Secure Mail 18.12.0

The Secure Mail 18.12.0 release includes performace 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 as **Report Via Attachment** in the Citrix Endpoint Management console. For details, see Report phishing email (as an attachment).

- **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 may vary 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 will 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 details, see Report phishing emails as a forward.

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 details, see Report phishing emails as a forward.
- **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**.
    Prior to this release, 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), as well as identity provider (IdP).

  > **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.

  For details, see Modern authentication using Microsoft office 365.

Known and fixed issues

January 23, 2019

This article also includes issues with MDX that affect Secure Mail.

Fixed issues

Fixed issues in version 19.1.0

Secure Mail for iOS:

- When Secure Mail fails to connect to the Exchange Server, the following message appears on the email notification banner:

  "We are unable to fetch this message as your session has expired. Open Secure Mail to renew your session."

  This issue is fixed and the message is updated as follows:

  "Secure Mail is unable to connect to your organization's network. Please contact your administrator." [CXM-59128]

- For users running O365 mailboxes, repeatedly performing notification response actions such as **Yes, No, May be, or Delete** causes Office 365 throttling and the following error message appears:

  "The server is busy. Please try again." [CXM-60123]

Secure Mail for Android:

- In Secure Mail for Android, if you are using the Turkish language, you are unable to send emails to recipients whose address contains the character "I". [CXM-59093]
- In Secure Mail for Android, users are unable to select and highlight the subject line of an email. [CXM-59185]
- In Secure Mail for Android, logon fails if the password contains the character €. [CXM-59654]
- In Secure Mail for Android, when the **Sync with local contacts** setting is enabled, all your Secure Mail contacts are exported to your native contacts. After syncing, phone fields such as mobile, work, home, work fax, and home fax, do not appear in the correct order. For example, in your native contacts, the fax number appears above the mobile number. Users cannot change this order. [CXM-57994]

Fixed issues in version 18.12.0

Secure Mail for iOS:

- In Secure Mail for iOS, when you receive a mail in the Rich Text Format (RTF), certain types of inline attachments and the attachment symbol are not visible. [CXM-59121]
- In Secure Mail for iOS, when rich push notifications are enabled and you turn off and turn on **Mail Notifications**, the **Mail Type** option appears intermittently. [CXM-59122]

Secure Mail for Android:

- If you are running Client Based Authentication mechanism in your environment, Secure Mail is unable to auto sync emails intermittently. Performing a manual sync fetches a few emails only. [CXM-59650]

Fixed issue in version 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]

Fixed issues in version 18.11.0

- In Secure Mail for Android, embedded images are not viewable within an email. [CXM-53556]
- Secure Mail for Android crashes while opening an email whose signature contains an embedded URL, such as `file://C:\...jpg`. [CXM-58219]

Fixed issues in version 18.10.5

Secure Mail for iOS:

- When the Enable iOS data protection MDX policy is enabled, you receive the "You have new email" notification intermittently. [CXM-55491]
- On the iPhone XS, attachments can't be downloaded or sent and downloaded images can't be displayed. [CXM-57030]

Secure Mail for Android:

- When users modify a recurring meeting for accounts running Exchange ActiveSync version 16 and later, the meeting does not update in Exchange Server. As a result, the meeting is not synchronized between Secure Mail and Outlook. [CXM-57200]

Fixed issues in version 18.10.0

- In Secure Mail for Android, users cannot view inline images that point to servers other than Exchange servers. [CXM-56736] [CXM-55843]
- In Secure Mail for Android, the PIN number was not appended with the dial-in number while joining Webex meetings. You have to manually type the PIN number. [CXM-56002]
- Secure Mail for Android crashes while trying to export Secure Mail calendar if your personal calendar is not configured. [CXM-56264]
- On the iPhone XS, in Secure Mail for iOS, attachments can't be downloaded or sent and downloaded images can't be displayed. [CXM-57030]

Fixed issues in version 18.9.0

Secure Mail for Android:

- The client workstation changes randomly with every NT LAN Manager (NTLM) authentication request. [CXM-55177]
- Secure Mail sync on Android P intermittently stops working when the device is in battery saver mode. [CXM-55441]
- Secure Mail crashes while trying to export Secure Mail calendar if your personal calendar is not configured. [CXM-56264]

Fixed issues in version 10.8.65

Secure Mail for iOS:

- When FIPs is enabled and users run Secure Mail for iOS on an iOS 11.3 device, the Cut and Copy, and Paste MDX policies do not work as expected. [CXM-53993]
- When using Secure Mail for iOS on shared devices, new users can view the emails of a previous user even though that user had logged off. If the new user taps a folder to refresh the display, the previous users' emails no longer appear. [CXM-55176]

Fixed issues in version 10.8.60

> **Note:**
>
> Secure Mail versions 10.8.25 to 10.8.60 include no known issues.

- In Secure Mail for iOS running on IBM Lotus Domino servers, you are unable to use the search icon in your inbox. [CXM-53782]
- When users enroll a device running Secure Mail for Android with Intune company portal, Secure Mail stops working. [CXM-54178]
- Secure Mail for iOS crashes while syncing a large number of mail folders from the server during an FTU flow. [CXM-54371]
- In Secure Mail for iOS, print preview of PDFs appear smaller. [CXM-54482]
- In Secure Mail for Android, multiple email IDs are not auto populated while responding to emails. [CXM-54811]

Fixed issues in version 10.8.55

- In Secure Mail for iOS, the Week view of the calendar renders incorrectly on an iPad Pro, when viewed in the landscape mode. [CXM-53723]

MDX-related fixed issues in version 10.8.55

- On Android, Secure Mail crashes when users are signed out of Secure Hub. [CXM-53930]

- On iOS devices, Secure Web and Secure Mail 10.8.45 crash on launch. [CXM-54089]

Fixed issues in version 10.8.50

- Secure Mail for iOS cannot save video files to ShareFile. [CXM-42238]
- When you enable push notifications in Secure Mail for Android, you do not receive notifications for new emails. This issue occurs intermittently. [CXM-53135]

Fixed issues in version 10.8.45

Secure Mail version 10.8.45 included no fixed issues.

Fixed issues in version 10.8.40

In Secure Mail for iOS, a duplicate notification appears intermittently for every new email you receive. [CXM-51473]

Fixed issues in version 10.8.35

- In Secure Mail for Android, automatic synchronization stops intermittently. Users need to synchronize manually in order for some new messages from Office 365 servers to appear in Secure Mail. [CXM-49354, CXM-52716]
- In Secure Mail for Android, even though you disable email notifications in Secure Mail for email and calendar events, the notifications still appear, and a sound notification occurs. [CXM-50479]
- When you create an All-day event using Secure Mail for Android, incorrect dates are displayed in your outlook calendar. [CXM-50612]
- In Secure Mail for Android, Exchange personal contact groups are not synchronizing to the app. [CXM-51190]
- When SSO is configured, Secure Mail for Android SSO to Exchange fails. Users are prompted for a password to sign in. [CXM-51343]

Fixed issues in version 10.8.25

- In Secure Mail for Android, a delay occurs when users sync a calendar invitation with Office 365. The issue occurs when creating or updating a calendar invitation. [CXM-49596]
- In Secure Mail for Android, when users type a single letter in the cc: field and then tap **Send**: Secure Mail sends the message to the first user in the list of frequently used users. Instead, a notification should appear that the cc: field entry is invalid. [CXM-50476]

- On Zebra T51 devices running Android 7, users cannot install the Citrix Launcher app. [CXM-50621]
- When NetScaler Gateway is configured with certificate-based authentication: In Secure Mail for iOS, every time users receive a new message, the "You have new mail" message appears. Instead, the notification should list the sender name, subject, and body preview. [CXM-51075]

Fixed issues in version 10.8.20

- If the Intune Company Portal app is installed on Android devices enrolled in the MAM-Only mode, in Endpoint Management, Secure Mail attempts to redirect to the Microsoft Login page. The following error message appears: "Did not receive any configuration for the app. Please contact your administrator to configure the app." [CXM-48135]
- In Secure Mail for Android, sign in fails if your user name or password contains special characters such as ä, ö, ü, or €. [CXM-48197]
- On Android devices, a restart allows you to bypass authentication to access Secure Mail. [CXM-48444]
- In Secure Mail for Android, when you reply to emails before inline images are downloaded, mails are stuck in your Outbox. This issue occurs when the **Show pictures** setting is enabled in your settings. [CXM-49222]
- In Secure Mail for iOS, if the IRM policy is **ON** and email classification is set to **Protected**, you are not able to view attachments when you download the complete mail. [CXM-49544]

Fixed issues in version 10.8.10

Secure Mail for iOS:

- After updating to Secure Mail 10.7.25 for iOS, the Message-ID header is missing brackets (< and >). [CXM-46029]
- In Secure Mail for iOS, after users add a calendar invitation from Outlook, intermittently the app crashes. This issue occurs if your calendar invitation contains an Emoji. [CXM-46250]
- On iOS, after upgrading Mobile productivity apps to 10.7.30, if Log Level is set to 11 or higher, Secure Mail is extremely slow and crashes if left open. [CXM-46721]
- In Secure Mail for iOS, duplicate notifications appear intermittently if the Control Locked Screen Notifications policy is set to **Count Only**. [CXM-47461]

Secure Mail for Android:

In Secure Mail for Android, when users copy and paste four or more email addresses in the To: field, the app crashes. [CXM-46578]

Known issues

Known issues in version 19.1.0

In Secure Mail for iOS, when admins leave the log level as the default (4) in Citrix Endpoint Management, after users send logs for Secure Mail from Secure Hub, occasionally the Secure Mail log files are empty. As a workaround, admins can set the log level to 15. [CXM-60674]

Known issues in version 18.11.5

- There are no known issues in version 18.11.5.

Known issues in version 18.11.0

- There are no known issues in version 18.11.0

Known issues in version 18.10.5

- There are no known issues in version 18.10.5.

Known issues in version 18.10.0

- In Secure Mail for Android, internal sites do not load with micro VPN configured. [CXM-56744]

Known issues in version 18.9.0

- There are no known issues in version 18.9.0.

Known issues in version 10.8.65

- There are no known issues in version 10.8.65.

Deploying Secure Mail

November 14, 2018

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

November 14, 2018

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

Secure Mail now 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 the following custom policies first:

1. From your Endpoint Management console, go to **Settings > Server Properties** and then click **Add**.
2. In the list, click **Custom Key** and then in the **Key** field, type *xms.store.idpuser_attrs***.
3. Set the value to **true **** and then in **Display** name, type *xms.store.idpuser_attrs*. Click **Save**.
4. Click **Client Properties** and then click **Add**.
5. Select **Custom Key** and then type *SEND_LDAP_ATTRIBUTES* in the **Key** field.
6. Type *userPrincipalName=${user.userprincipalname},email=${user.mail},displayname=${user.displayname},sA* in the **Value** field, enter a description and then click **Save**.

   The following steps only apply for iOS devices:
7. Go to **Configure > Device Policies**, click **Add**, and then select the **App Configuration policy**.
8. Enter a policy name and then click **Next**.
   In the Identifier list, click **Add new**. In the text box that appears, enter the bundle ID for your Secure Mail app.
9. In the **Dictionary** content box, type the following text:

```
<dict>

<key>XenMobileUserAttributes</key>

<dict>

<key>userPrincipalName</key>

<string>${
 user.userprincipalname }
 </string>

<key>email</key>
```



```
14
15 <string>${
16  user.mail }
17  </string>
18
19 <key>displayname</key>
20
21 <string>${
22  user.displayname }
23  </string>
24
25 <key>sAMAccountName</key>
26
27 <string>${
28  user.samaccountname }
29  </string>
30
31 <key>aadupn</key>
32
33 <string>${
34  user.id_token.upn }
35  </string>
36
37 <key>aadtid</key>
38
39 <string>${
40  user.id_token.tid }
41  </string>
42
43 </dict>
44
45 <key>IntuneMAMUPN</key>
46
47 <string>${
48  user.id_token.upn }
49  </string>
50
51 </dict>
```

10. Clear the Windows Phone and Windows Desktop/Tablet check boxes and then click **Next**.
11. Select the user groups to which you want the policy deployed and then click **Save**.

Features that are incompatible with Intune

The following table lists the Secure Mail features that are not compatible with Microsoft Intune/EMS:

- 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

January 8, 2019

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.

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.

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.

> **Note:**
>
> Configure the Background network services only if your mail server and AD FS are internal.

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

December 11, 2018

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 Android policies
- Secure Mail iOS policies

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 8, 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
Earlier than iOS 9	Yes	Yes
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
Earlier than iOS 9	No	Yes
iOS 9 and later	No	Yes
Earlier than Android M	No	Yes
Android M and Android N	No	Yes

Operating system type	SSLv3	TLS
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

November 1, 2018

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

December 11, 2018

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. Set these Endpoint Management client properties to **true**:
   - ENABLE_PASSCODE_AUTH
   - ENABLE_PASSWORD_CACHING
   - ENABLE_CREDENTIAL_STORE
2. Add this Endpoint Management client property:

   Display name: SEND_LDAP_ATTRIBUTES

   Value:userPrincipalName=${user.userprincipalname},sAMAccountNAme=${user.samaccountname}, displayName= ${ user.displayName} ,mail= ${ user.mail}
3. Add this Endpoint Management property:

   MAM_MACRO_SUPPORT set to **true**
4. Configure these Secure Mail properties:
   - Set Initial Authentication Mechanism to **User email address**.
   - Set Initial Authentication Credentials to **userPrincipalName**.
5. 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

January 17, 2019

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

Microsoft IRM and and AIP email rights protection support

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

This feature allows organizations that use IRM to apply protection to messaging content and 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**.

Enable Information Rights Management in Secure Mail

Perform the following steps to enable Information Rights Management in Secure Mail:

1. Log on to XenMobile Server 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 restriiction profiles to enable email protection.

To set restrictioins 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, you may want to 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 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 any 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 those 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 who 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. And, if the device terminates and then restarts Secure Mail when a device is locked, Secure Mail is unable to 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.

Android features

January 23, 2019

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

Viewing attachments

In Secure Mail for Android, viewing mail and calendar attachments is now much easier. The attachment either opens directly within the app or a list of supported apps appears. You can select the required app to view the attachment.

Secure Mail supports viewing txt, word, audio, video, html, zip files, images, .eml files, and .vcf contact file formats.

Prerequisites:

Ensure an admin configures the following MDX policies in the Citrix Endpoint Management console:

- Document Exchange (Open In) policy set to **Unrestricted**.
- Allow Offline documents policy set to **Unlimited**.

For information about these policies, see here.

Actions when viewing attachments

You can perform the following actions when viewing attachments:

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

You can preview attachments while:

- Viewing a message.
- Composing a new message.
- Forwarding a message.

You can also preview attachments from:

- The **Attachments** folder.
- The Calendar events.

Attach files to an existing email or a new email

You can attach files to an existing email or you can create an email to attach files.

1. Tap **Attachments** folder, long press to select multiple attachments, or just tap to select an attachment.
2. Tap the **Attach** icon on the screen. The mailbox appears.
3. You can perform one of the following:
    - To attach the file to an existing email, select an existing message.
    - To attach the file to a new email, tap **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 then tap **Save 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 then tap **Remove from Offline Files**.

To open the attachment by using different apps

1. Open the attachment.
2. Tap the **More** icon on the top right of the page and then tap **Open with**.
3. From the options that appear, tap the app you want to open the attachment with.
4. Alternatively, you can swipe left to see the list of Actions that can be used to view or open an attachment.

To view the source email or calendar event of the attachment

1. Tap the **Attachments** icon on the bottom right of your screen.
2. Tap the attachment and then tap the **More** icon on the top right of the screen.

3. Tap **View Original Email** or **View Original Calendar** to view the source of an email or a calendar event.

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 prints 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, see Report phishing email (as an attachment).

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.

Attaching files 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.

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
PDF	X	
PPT	X	X
PPTX	X	X
DOC	X	X
DOCX	X	X
XLS	X	X
XLSM	X	X
XLSX	X	X
TXT	X	X
POT	X	X
HTM	X	X
HTML	X	X
ZIP	X	X
EML	X	X

Multiple Exchange accounts for Android

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

Prerequisites

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.
- 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.

To add an Exchange email account for Android

1. Open Secure Mail, tap the hamburger icon, and then tap the **Settings** icon.
2. Under **Accounts**, tap **Add account**.
3. In the **Add accouunt** screen, type the credentials for the new account.

   Optionally, you can set values for the following parameters:

   - **Sync mail period:** Tap to select a value for the sync mail period. The value you set specifies the number of mail days for Secure Mail to synchronize. Your administrator sets the default value.
   - **Make this my default account:** Tap to set the new account as your default account. The value is set to **OFF** by default.
4. Tap **Sign In** to create the account.

   You can view the new account in the **Settings** screen under the **Accounts** menu.

> **Note:**
>
> Additional accounts must use authentication based on Active Directory. Secure Mail does not support certificate-based authentication when configuring multiple accounts.

To edit an account

You can edit the password and description of email account for Android.

1. Open Secure Mail, tap the hamburger icon, and then tap the **Settings** icon.
2. Under **Accounts**, tap the account you want to edit.
3. In the **Account** screen, edit the fields.
4. Tap **Save** to confirm your action or tap **Cancel** to return to the **Settings** screen.

To delete an account for Android

1. Open Secure Mail, tap the hamburger icon, and then tap the **Settings** icon.
2. Under **Accounts**, tap the account you want to delete.
3. In the **Account details** screen, tap **Delete account** at the bottom of the screen or tap **Cancel** to return to the **Settings** screen.
4. Tap **DELETE** to confirm your action.

> **Note:**
>
> If you delete the default account, the next account will become the default account.

To set a default account for Android

Secure Mail uses the default account in the following scenarios:

- **Composing emails:** The **From:** field auto-populates with the email ID of the default account.
- **Creating calendar events:** The **Organizer** field auto-populates with the email ID of the default account.

When you add one or more email accounts, the first account you create is the default account. To change the default account, navigate to **Settings** and then tap **Default** under **General**.

In the **Default account** screen, tap the account you want to set as default.

Settings for multiple Exchange accounts for Android

If you have configured multiple Exchange accounts, some of the Secure Mail settings are available to each of these accounts individually, whereas other settings are global. The following settings are account-specific:

- Default
- Notifications
- Out of Office
- Sync inbox frequency
- Sync mail period
- Sync email
- S/MIME
- Offline Files
- Signature
- Quick responses
- Sync calendar
- Sync contacts

- Sync with local contacts
- Export Settings

These settings appear with the > icon. Tap the > icon to view the accounts on your device.

To apply the setting to a specific account, expand a setting item by tapping **>** and then select the email account.

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.

To view your mailboxes, open Secure Mail and tap the hamburger icon, In the **Mailboxes** screen, tap the account to expand the options.

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 then 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

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.

The following actions are limited to individual accounts only:

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

Contacts

Tap the **Contacts** icon in the tab bar, and then tap the hamburger icon on the top right of the screen. The **Contacts** screen displays the following items:

- **All Contacts:** Displays all contacts from multiple email accounts. This option appears only if multiple email accounts are configured.
- **Individual email account:** Displays contacts pertaining to the individual email account that are configured.
- **Categories:** Displays contact categories that you may have created or selected from the predefined list to group contacts.

To view the contact folder

> **Note:**
>
> Contact subfolders are not supported on Secure Mail for Android. If you have created folders or subfolders for your contacts using Microsoft Outlook, you can't view them in Secure Mail.

1. In the contacts screen:
    - Tap on all contacts to view all the contacts from multiple email accounts.
    - Tap on individual email account to view contacts associated with a particular email account.
2. Tap on categories to view the contacts grouped under specific categories. You can choose to group contacts based on a category you create or group them under a category from a predefined list.

You can synchronize contacts pertaining to an individual account to your local contacts.

To sync with local contacts

1. Open Secure Mail.
2. Tap the Settings icon, and then navigate to **Contacts > Sync with Local Contacts** and then tap > to expand the menu.
3. In the **Sync Local Contacts** screen, enable the account whose contacts you want to sync.
4. Tap **OK**.
5. When prompted to allow Secure Mail to access your contacts, tap **OK**.

You have now successfully exported contacts for the account.
To undo this action, go to **Settings > Contacts > Sync with Local Contacts** and then tap on the switch next to the account to disable this feature. Tap **OK** to confirm your action.

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.

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** XenMobile Server property must be set to **TRUE**.

After you have set up Android Enterprise on the XenMobile Server, 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)	
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

Feature	Support
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

Secure Mail integration with Slack (Preview)

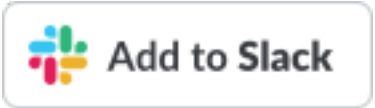
December 11, 2018

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

November 9, 2018

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 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 should override 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 summarizes 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.

Rich push notifications

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 (Oauth)
- Apps managed by Endpoint Management integration with Microsoft InTune/EMS
- Devices enrolled by using derived credentials

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 of 30 seconds required to fetch the message details.

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 as well:

- When Secure Mail fails to read the required information from 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 yet. 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 your device but not unlocked yet. 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.

Push notifications for Secure Mail

January 8, 2019

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 Background App Refresh or 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

Secure Mail sends push notifications for the following Inbox activities:

- **New mail, meeting requests, meeting cancellations, meeting updates:** When APNs pushes notifications to an inbox, Secure Mail updates all folders, including Calendar, so that meeting changes are reflected immediately in users' calendars.
- **For iOS, the Secure Mail status changes from read to unread and vice versa.** 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.

  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.

  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.

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 addtion, 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.

```
<configuration>
<system.net>
<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 this Endpoint Management Advanced Concepts article.

Citrix Gateway configuration

While 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.

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, try the Secure Mail Test Tool.

Secure Mail Push Notifications FAQs

When does iOS deliver notifications to Secure Mail?

If Secure Mail is running in the foreground, notifications are *always* delivered to Secure Mail. This is the only time that Citrix can guarantee that notifications are delivered. When Secure Mail enters the background, the application badge count always updates. However, notifications (lockscreen and banner notifications) rely on Background App Refresh and, particularly when iOS suspends or terminates the app, notifications are not a certainty. The following factors are outside the control of Citrix.

The following cases may affect the delivery of notifications:

- The battery is low.
- Secure Mail is not used frequently (rarely opened into the foreground).
- Emails received outside of core usage times in which the app is suspended for an extended period in the background; for example, between midnight and 6 a.m.

Notifications *are not* delivered to Secure Mail in the following cases:

- If the user closes Secure Mail, until the user manually reopens the app.
- If the system has terminated Secure Mail. and the app has not been automatically restarted.
- When Secure Mail is not active.

> **Important:**
>
> Notifications may not be delivered to Secure Mail when it is not active for many reasons, including but not limited to the following cases:
>
> - 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 entirely on the iOS device.

When Secure Mail does not receive a notification, Secure Mail does not sync new data to the device. As a consequence, the following situations occur:

- Secure Mail syncs data only when users bring the app to the foreground.
- Lockscreen notifications stop occurring for new mail. Calendar reminders still appear, however.

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 lockscreen 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 lockscreen, 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, lockscreen 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 locksscreen notifications.

How else does Secure Mail generate lockscreen 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 lockscreen notifications appear to be real time.

In the event that Background App Refresh wakeups are required, lockscreen 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 when an email arrives in a user's Inbox on Exchange and Secure Mail syncs that message and generates the lockscreen 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?

A very important difference - and one that leads to confusion - is that Secure Mail does not always show new email in real time on the lock screen in the same way that Gmail, Microsoft Outlook, and other apps do. The primary reason for this difference is security. To align with the behavior of the other apps, the Citrix listener service would require the user credentials to authenticate with Exchange to get the email content and also pass this email content through the Citrix listener service, as well as 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 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 lockscreen 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 lockscreen 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 lockscreen 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 lockscreen 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 lockscreen notifications based on data that Microsoft provides in the APNs notification, because 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 which iOS simply takes the data and generates a lockscreen 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 so that Microsoft can access the user's mailbox, which poses a security risk. For more information about the way Microsoft manages user's passwords, see Microsoft TechNet.

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.

Secure Mail interactivity with other mobile productivity apps and Citrix Files

January 8, 2019

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

November 1, 2018

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.

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.

For more details, see these TechNet blog posts:

Exchange ActiveSync Mailbox Logging

Under the Hood: Exchange ActiveSync Mailbox Log Analysis

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