CITRIX

Secure Mail

Contents

Secure Mail 概述

March 29, 2019

通过 Citrix Secure Mail，用户可以在其移动电话和平板电脑上管理其电子邮件、日历和联系人。为了维护 Microsoft Outlook 或 IBM Notes 帐户的持续性，Secure Mail 会与 Microsoft Exchange Server 和 IBM Notes Traveler 服务器同步。

作为 Citrix 应用程序套件的一部分，由于与 Citrix Secure Hub 的单点登录 (SSO) 兼容性，Secure Mail 从中受益。用户登录 Secure Hub 后，可以无缝移至 Secure Mail，而不需要重新输入其用户名和密码。您可以将 Secure Mail 配置为在 Secure Hub 中注册用户设备时自动推送到用户设备，或者用户可以从 Store 添加该应用程序。

Secure Mail 与以下各项兼容：

- Exchange Server 2019 累积更新 1
- Exchange Server 2016 累积更新 12
- Exchange Server 2013 累积更新 22
- Exchange Server 2016 累积更新 11
- Exchange Server 2016 累积更新 10
- Exchange Server 2016 累积更新 9
- Exchange Server 2016 累积更新 8
- Exchange Server 2013 累积更新 21
- Exchange Server 2013 累积更新 19
- Exchange Server 2010 SP3 更新汇总 26
- Exchange Server 2010 SP3 更新汇总 24
- Exchange Server 2010 SP3 更新汇总 19
- Exchange Server 2010 SP3 更新汇总 22
- IBM Domino 邮件服务器 9.0.1 FP10 HF197
- IBM Domino 邮件服务器 9.0.1 FP9
- IBM Lotus Notes Traveler 9.0.1.21
- IBM Lotus Notes Traveler 9.0.1.9
- Microsoft Office 365 (Exchange Online)

要开始使用，请从 Citrix Endpoint Management 下载下载 Secure Mail 及其他 Endpoint Management 组件。

有关 Secure Mail 及其他移动应用程序的系统要求，请参阅系统要求。

有关应用程序在后台运行或关闭时 Secure Mail for iOS 和 Secure Mail for Android 中的通知信息，请参阅 Secure Mail 的推送通知。

有关 Secure Mail 支持的 iOS 功能，请参阅适用于 Secure Mail 的 iOS 功能。

有关 Secure Mail 支持的 Android 功能，请参阅适用于 Secure Mail 的 Android 功能。

有关 Secure Mail 支持的 iOS 和 Android 功能，请参阅适用于 Secure Mail 的 iOS 和 Android 功能。

Secure Mail 中的新增功能

July 19, 2019

以下各部分列出了当前版本及早期版本的 Secure Mail 中的新增功能。

当前版本中的新增功能

Secure Mail 19.7.5

Secure Mail for iOS

- 草稿文件夹自动同步。在 Secure Mail for iOS 中，草稿文件夹会自动同步，并且草稿可在所有设备上使用。此功能在运行 Exchange ActiveSync v16 或更高版本的设置中可用。

  > 注意：
  >
  > 如果 Secure Mail 草稿包含附件，则不会将附件同步到服务器。

- 在 **MDM + MAM** 模式下使用 **Microsoft Intune** 时，**Secure Mail for iOS** 支持单点登录。为了能够使用此功能，请务必在您的设备上安装 Microsoft Authenticator 应用程序。有关安装 Microsoft Authenticator 应用程序的详细信息，请参阅 *Docs.microsoft.com* 上的下载并安装 **Microsoft Authenticator** 应用程序。

Secure Mail for Android

> 注意：
>
> Citrix 建议您先升级到 Secure Mail 版本 19.7.5，然后再将操作系统升级到 Android Q。

- 对于对 **Microsoft Office 365** 运行新式验证的设置，请使用 **“使用 Web SSO 进行通道传输”** 策略。在 Secure Mail for Android 中，添加了一个名为使用 **Web SSO** 进行通道传输的新策略。通过此策略，您可以通过 Secure Browse 借助通道传输 OAuth 流量。对此，请执行以下操作：
  - 将使用 **Web SSO** 进行通道传输策略设置为开。
  - 在“网络访问”策略中，选择通道 **- Web SSO** 选项。
  - 从后台服务策略中排除与 OAuth 有关的任何主机名。
- 在 **MDM + MAM** 模式下使用 **Microsoft Intune** 时，**Secure Mail for Android** 支持单点登录。为了能够使用此功能，请务必在您的设备上安装 Intune 公司门户应用程序。登录到 Intune 公司门户应用程序后，您可以在 MDM + MAM 模式下使用 SSO，而不需要使用您的凭据在 Secure Mail 中重新进行身份验证。

早期版本中的新增功能

Secure Mail 19.6.5

Secure Mail for iOS

Secure Mail for iOS 19.6.5 包括性能增强和缺陷修复。有关已修复的问题和已知问题的列表，请参阅已知问题和已修复的问题。

Secure Mail for Android

- 拖放日历事件。在 Secure Mail for Android 中，可以通过拖放事件来更改现有日历事件的时间。将事件拖放到与会议发生时同一天的所需时间段。使用定位按钮可展开或收缩事件，并相应地更改持续时间。
- 支持响应式电子邮件。Secure Mail for Android 已优化，能够提供响应式电子邮件。以前，带有大型表格或图像的电子邮件内容呈现不正确。在所有受支持的设备上，无论电子邮件格式和大小如何，此功能都可以提供可读性更强的电子邮件内容。
- **Secure Mail** 中的联系人图片。在 Secure Mail for Android 中，当您在电子邮件或会议邀请中添加收件人时，请查看联系人图像。联系人图像显示在姓名旁边。如果存在具有相同姓名的多个用户，则当您在电子邮件或会议邀请中添加收件人时，图像会帮助识别正确的收件人。要搜索未保存在本地的联系人，请至少输入收件人姓名的四个字符以显示图像。
- 日历日程的小组件。在 Secure Mail for Android 中，日历日程以小组件的形式提供。在此小组件中，您可以查看每周日历中即将发生的事件。此功能允许您创建日历事件、查看现有事件以及编辑详细信息。

Secure Mail 19.5.5

Secure Mail for Android

Secure Mail for Android 19.5.5 包括性能增强和缺陷修复。有关已修复的问题和已知问题的列表，请参阅已知问题和已修复的问题。

Secure Mail for iOS

- 在 MDM + MAM 模式下使用 Microsoft Intune 时，Secure Mail for iOS 支持单点登录。为了能够使用此功能，请务必在您的设备上安装 Microsoft Authenticator 应用程序。Microsoft Authenticator 应用程序在应用商店中提供。
- 支持 **Slack EMM**： Slack EMM 用于启用了企业移动性管理 (EMM) 的 Slack 客户。Secure Mail for iOS 支持应用程序 **Slack EMM**，这允许管理员选择 Secure Mail 与 **Slack** 应用程序或 **Slack EMM** 应用程序的集成。

Secure Mail 19.5.0

Secure Mail for Android

管理您的源。在 Secure Mail for Android 中，可以根据您的要求组织源卡。

有关管理源的详细信息，请参阅管理您的源。

草稿文件夹自动同步。在 Secure Mail for Android 中，草稿文件夹会自动同步，并且草稿可在所有设备上使用。有关详细信息，包括演示此功能的视频，请参阅草稿文件夹自动同步。

Secure Mail for Android 19.4.6、19.4.5 和 19.3.5

这些版本包括性能增强和缺陷修复。

有关已修复的问题和已知问题的列表，请参阅已知问题和已修复的问题。

Secure Mail 19.3.0

从本版本起，Secure Mail 包括对以下服务器的支持：

- Exchange Server 2019 累积更新 1
- Exchange Server 2016 累积更新 12
- Exchange Server 2013 累积更新 22
- Exchange Server 2010 SP3 更新汇总 26

有关 Secure Mail 服务器兼容性的完整列表的详细信息，请参阅 Secure Mail 概述。

Secure Mail for iOS

管理您的源。在 Secure Mail for iOS 中，现在可以根据您的要求组织您的源卡。

> 注意：
>
> 此功能在 iPad 上不可用。

有关管理源的详细信息，请参阅管理您的源。

Secure Mail for iOS 和 Secure Mail for Android

内部域。可以标识和编辑属于外部组织的电子邮件收件人。要使用此功能，请确保已在 Citrix Endpoint Management 中启用内部域策略。

创建、答复或转发电子邮件时，邮件列表中会突出显示外部收件人。联系人图标在屏幕左下角显示为警告。轻按联系人图标可修改邮件列表。

有关内部域的详细信息，请参阅内部域。

人机工程学改进功能。操作按钮将从屏幕顶部移动到底部，以便于访问。这些更改是针对收件箱、日历和联系人屏幕的。

> 注意：
>
> 对于运行 Android 的设备，这些更改是针对收件箱和日历屏幕的。

有关人体工程学改进功能的详细信息，请参阅人机工程学改进功能。

Secure Mail 19.2.0

Secure Mail for iOS

Secure Mail 19.2.0 版本包括性能增强和缺陷修复。

有关已修复的问题和已知问题的列表，请参阅已知问题和已修复的问题。

Secure Mail for Android

- 通讯录增强功能。在 Secure Mail for Android 中，当您轻按通讯录并选择某个联系人时，该联系人的详细信息将显示在联系人选项卡。当您轻按组织选项卡时，将显示经理、直接下属和同级等组织层次结构详细信息。当您轻按屏幕右上方的“更多”图标时，将显示以下选项：
  - 附加到邮件
  - 共享
  - 删除

  在组织选项卡中，轻按经理、直接下属或同级右侧的“更多”图标。然后，也可以是创建电子邮件或日历邀请。电子邮件或日历事件的收件人**:** 字段将自动填充经理、直接下属或同级的详细信息。

  必备条件：

  请确保 Exchange Web 服务 (EWS) 在您的 Exchange Server 上处于启用状态。

  显示的联系人详细信息取决于从 Active Directory 提取的组织详细信息。要显示正确的联系人详细信息，请确保管理员已在 Active Directory 中配置您的组织层次结构。

  > 注意：
  >
  > 此功能在 IBM Lotus Notes 服务器上不受支持。

- 网络访问策略。在 Secure Mail for Android 中，“网络访问”MDX 策略中添加了一个名为通道 **- Web SSO** 的新选项。配置此策略可让您灵活地借助通道通过 Secure Browse 功能和 Secure Ticket Authority (STA) 并行传输内部流量。还可以允许身份验证服务（例如 NTLM、Okta 和 Kerberos）使用 Secure Browse 连接。最初配置 STA 时，需要向后台网络服务策略中添加单个 FQDN 和服务地址端口。但是，如果配置了通道 **- Web SSO** 选项，则不需要进行这些配置。

要在 Citrix Endpoint Management 控制台中为 Secure Mail for Android 启用此策略，请执行以下操作：

1. 下载并使用适用于 Android 的.mdx 文件。有关详细信息，请参阅移动应用程序和 MDX 应用程序的工作原理中的步骤。
2. 在“网络访问”策略中，单击通道 **- Web SSO** 选项。有关详细信息，请参阅应用程序网络访问

Secure Mail for iOS 19.1.6

本版本包括性能增强和缺陷修复。

Secure Mail 19.1.5

从本版本起，Secure Mail 包括对以下服务器的支持：

- Exchange Server 2016 累积更新 11
- Exchange Server 2010 SP3 更新汇总 24

有关 Secure Mail 服务器兼容性的完整列表的详细信息，请参阅 Secure Mail 概述。

Secure Mail 19.1.0

Secure Mail for iOS

- 通讯录增强功能。在 Secure Mail for iOS 中，当您轻按通讯录并选择某个联系人时，该联系人的详细信息将显示在联系人选项卡。当您轻按组织选项卡时，将显示经理、直接下属和同级等组织层次结构详细信息。当您轻按屏幕右上方的“更多”图标时，将显示以下选项：

  - 编辑
  - 添加到 VIP
  - 取消

  在组织选项卡中，您可以轻按经理、直接下属或同级右侧的“更多”图标。此操作允许您创建电子邮件或日历事件。电子邮件或
  日历事件的收件人**:** 字段将自动填充经理、直接下属或同级的详细信息。您可以编写并发送该电子邮件。

  必备条件：

  请确保 Exchange Web 服务 (EWS) 在您的 Exchange Server 上处于启用状态。

  显示的联系人详细信息取决于从 Active Directory 提取的组织详细信息（Outlook 通讯录）。要显示正确的联系人详细信息，请确保管理员已在 Active Directory 中配置您的组织层次结构。

  > 注意：
  >
  > 此功能在 IBM Lotus Notes 服务器上不受支持。

- 将会议时间和地点导出至您的本机日历。在 Secure Mail for iOS 中，将会议时间、地点的新值添加到导出日历 MDX 策略中。此增强功能允许您将 Secure Mail 日历事件的会议时间和地点导出至您的本机日历。

- 在使用新式验证 (O365) 运行 Microsoft Enterprise Mobility + Security (EMS)/Intune 的安装程序上，Secure Mail for iOS 支持丰富的推送通知。

  要启用丰富的推送通知功能，请确保满足以下必备条件：

  - 在 Endpoint Management 控制台中，将推送通知设置“开”。
  - 将网络访问策略设置为不限制。
  - 将控制锁定屏幕通知策略设置为允许或电子邮件发件人或事件标题。
  - 导航到 **Secure Mail** > 设置 > 通知，然后启用邮件通知。

- Secure Mail 用户可以使用 Zoom 应用程序加入会议。有关配置所需的策略以使用 Zoom 应用程序的信息，请参阅从日历加入会议。
- 本版本支持 iPad Pro 11 英寸和 iPad Pro 12.9 英寸。

Secure Mail for Android

- 附件增强功能。在 Secure Mail for Android 中，查看附件的操作已简化。为提升体验，请删除无关紧要的步骤，但要保留已存在于早期版本中的附件选项。

  您可以在 Secure Mail 应用程序中查看附件。如果可以使用 Secure Mail 进行查看，附件将直接打开。如果无法使用 Secure Mail 查看附件，则将显示应用程序列表。您可以选择所需的应用程序以查看附件。有关详细信息，请参阅 查看附件。
- Secure Mail 用户可以使用 Zoom 应用程序加入会议。有关配置所需的策略以使用 Zoom 应用程序的信息，请参阅从日历加入会议。
- 将会议时间和地点导出至您的本机日历。在 Secure Mail for iOS 中，将会议时间、地点的值添加到导出日历 MDX 策略中。此操作允许您将 Secure Mail 日历事件的会议时间和地点导出至您的本机日历。

> 注意：
>
> 针对 Android 5.x 的支持已于 2018 年 12 月 31 日结束。

Secure Mail 18.12.0

Secure Mail 18.12.0 版本包括性能增强和缺陷修复。

有关已修复的问题和已知问题的列表，请参阅已知问题和已修复的问题。

Secure Mail 18.11.5

Secure Mail for Android

- 使用 **ActiveSync** 标头报告网络钓鱼电子邮件。在 Secure Mail for Android 中，当用户报告网络钓鱼邮件时，系统将以附件的形式生成 EML 文件以表示该邮件。管理员将收到该邮件，并可以查看与报告的邮件相关联的 ActiveSync 标头。

  要启用此功能，管理员必须配置报告网络钓鱼电子邮件地址策略并将报告网络钓鱼机制设置为通过附件进行报告。管理员在 Citrix Endpoint Management 控制台中配置这些设置。有关详细信息，请参阅 报告网络钓鱼电子邮件（以附件的形式）。
- 打印电子邮件和日历事件。在 Secure Mail for Android 中，可以从 Android 设备打印电子邮件和日历事件。此打印功能将使用 Android 打印框架。有关详细信息，请参阅 打印电子邮件和日历事件。

- 来自您的经理的源。在 Secure Mail for Android 中，您可以在源屏幕中查看来自您的经理的电子邮件。根据同步邮件期限设置，来自您的经理源下最多显示 5 封电子邮件。要查看来自您的经理的更多电子邮件，请轻按查看全部。

  必备条件：

  请确保 Exchange Web 服务 (EWS) 在您的 Exchange Server 上处于启用状态。

  显示的经理卡片取决于从 Active Directory 提取的组织详细信息（Outlook 通讯录）。要在经理源中显示正确的详细信息，请确保管理员已在 Active Directory 中配置您的组织层次结构。

  > 注意：
  >
  > 此功能在 IBM Lotus Notes 服务器上不受支持。

Secure Mail 18.11.1

> 重要：
>
> 以下问题在 Secure Mail for Android 18.11.1 中已修复
>
> 在连接到 IBM Notes Traveler 9.0.1 SP 10 的 Secure Mail for Android 中，带有附件的电子邮件保存在“发件箱”中。[CXM-58962]

Secure Mail 18.11.0

Secure Mail for Android

- 子文件夹通知。在 Secure Mail for Android 中，您可以在邮件帐户的子文件夹中收到邮件通知。有关详细信息，请参阅 子文件夹通知。
- 在 **Secure Mail for Android** 中对后台服务进行了更新。为了满足运行 Android 8.0（API 级别 26）或更高版本的设备上的 Google Play 后台执行限制要求，我们已升级了 Secure Mail 后台服务。要在您的设备上实现不间断的邮件同步和通知，请启用 Firebase Cloud Messaging (FCM) 服务推送通知。有关启用基于 FCM 的推送通知的更多详细信息，请参阅 Secure Mail 的推送通知

请确保在设备上的 Secure Mail 设置中打开邮件通知。有关此更新的更多详细信息，请参阅此支持知识中心文章。

限制：

- 如果您尚未启用基于 FCM 的推送通知，则每隔 15 分钟进行一次后台同步。此时间间隔因应用程序是在后台运行还是在前台运行而异。
- 当用户从设备设置中手动更新时间时，日历小组件中的日期不会自动更新。

Secure Mail for iOS

- 支持 **iOS 12.1**。Secure Mail for iOS 支持 iOS 12.1。

- 对丰富的推送通知失败消息进行了增强。在 Secure Mail for iOS 中，相应的推送通知失败消息将根据通知失败类型显示在您设备上的通知中心中。有关详细信息，请参阅 “Secure Mail for iOS 中的推送通知失败消息”，请参阅 Secure Mail for iOS 中的推送通知失败消息。
- 来自您的经理的源。在 Secure Mail for iOS 中，您可以在源屏幕中查看来自您的经理的电子邮件。根据同步邮件期限设置，来自您的经理源下最多显示 5 封电子邮件。要查看来自您的经理的更多电子邮件，请轻按查看全部。

  必备条件：

  请确保 Exchange Web 服务 (EWS) 在您的 Exchange Server 上处于启用状态。

  显示的经理卡片取决于从 Active Directory 提取的组织详细信息（Outlook 通讯录）。要在经理源中显示正确的详细信息，请确保管理员已在 Active Directory 中配置您的组织层次结构。

  > 注意：
  >
  > 此功能在 IBM Lotus Notes 服务器上不受支持。

Secure Mail 18.10.5

- **Secure Mail** 与 **Slack**（预览版）集成：现在可以将您的电子邮件对话转移到运行 iOS 或 Android 的设备上的 Slack 应用程序。有关详细信息，请参阅 Secure Mail 与 Slack（预览版）集成。
- 源文件夹的增强功能： 在 Secure Mail for iOS 中，以下是现有 “源” 文件夹的增强功能：
  - 在 “源” 卡中最多可查看五个即将召开的会议。
  - 接下来 24 小时内即将召开的会议将显示在 “源” 卡中，并分类为今天和明天部分。

Secure Mail 18.10.0

- 针对邮件和日历通知的 **Secure Mail** 通知通道： 在运行 Android O 或更高版本的设备上，您可以使用通知通道设置来管理您的电子邮件和日历通知的处理方式。您可以使用此功能来自定义和管理您的通知。有关详细信息，请参阅 通知通道。
- 报告网络钓鱼邮件（以转发的形式）： 在 Secure Mail for iOS 中，您可以使用 “报告为网络钓鱼” 功能报告疑似网络钓鱼的电子邮件（以转发的形式）。您可以将可疑邮件转发到管理员在策略中配置的电子邮件地址。要启用此功能，管理员必须配置 “报告网络钓鱼电子邮件地址” 策略并将报告网络钓鱼机制设置为通过转发进行报告。有关详细信息，请参阅 以转发邮件的形式报告网络钓鱼电子邮件。

Secure Mail 18.9.0

- 格式为 “yy.mm.version” 的新版本编号方案。例如，版本 **18.9.0**
- 报告网络钓鱼电子邮件（以转发的形式）： 在 Secure Mail for Android 中，您可以使用 “报告为网络钓鱼” 功能报告疑似网络钓鱼的电子邮件（以转发的形式）。您可以将可疑邮件转发到管理员配置的电子邮件地址。要启用

此功能，管理员必须配置“报告网络钓鱼电子邮件地址”策略并将“报告网络钓鱼机制”设置为通过转发进行报告。有关详细信息，请参阅 以转发邮件的形式报告网络钓鱼电子邮件。

- 源卡的增强功能： 在 Secure Mail for Android 中，已对现有的源文件夹增强了以下功能：
  - 自动同步的所有文件夹中的会议邀请都显示在“源”卡中。
  - 在“源”卡中最多可查看五个即将召开的会议。
  - 现在，即将召开的会议在以您的当前时间为起点的 24 小时内显示。这些会议邀请被分类为今天和明天。在之前的版本中，您的源中显示的是在当天结束之前即将召开的会议。
- 导出 **Secure Mail** 日历事件： Secure Mail for Android 和 Secure Mail for iOS 可用于将 Secure Mail 日历事件导出到设备的本机日历应用程序中。要启用此功能，请轻按设置，然后将“导出日历事件”滑块拖动到右侧。有关详细信息，请参阅 导出 Secure Mail 日历事件。

Secure Mail 10.8.65

- 适用于 **iOS 12**： 在 Secure Mail for iOS 中，我们支持组通知功能。利用此功能，可以对来自一个邮件线程的对话进行分组。您可以在您的设备的锁屏界面上快速查看分组的通知。默认情况下，在设备上启用组通知设置。
- 在 Secure Mail for iOS 中，保存草稿和删除草稿按钮比以前更大。此增强功能可以让客户更加轻松地区分一个选项与另一个选项。
- 在 Secure Mail for iOS 中，您可以在设备的设置中启用“Secure Mail 来电显示”，以识别来自 Secure Mail 联系人的传入呼叫。启用这些设置后，当您收到传入呼叫时，设备将显示应用程序名称和来电显示，例如“Secure Mail 来电显示: Joe Jay”。有关详细信息，请参阅 Secure Mail 来电显示。

Secure Mail 10.8.60

- Secure Mail 支持 Android P。
- Secure Mail 现在支持波兰语。
- 在 Secure Mail for iOS 中，您可以从 iOS 本机文件应用程序向您的电子邮件附加文件。有关详细信息，请参阅 iOS 功能。

Secure Mail 10.8.55

Secure Mail 10.8.55 中没有任何新增功能。有关已修复的问题，请参阅已知问题和已修复的问题。

Secure Mail 10.8.50

照片附件改进功能。在 Secure Mail for iOS 中，可以通过轻按新的库图标轻松附加照片。轻按库图标并选择要附加到您的电子邮件的照片。

Secure Mail 源屏幕。Secure Mail for iOS 和 Secure Mail for Android 在源屏幕中主要包含您的所有未读电子邮件、需要注意的会议邀请以及即将召开的会议。

Secure Mail 10.8.45

文件夹同步。在 Secure mail for iOS 和 Secure mail for Android 中，可以轻按同步图标以刷新 Secure Mail 的所有内容。同步图标存在于 Secure Mail 的滑出式菜单中，例如“邮箱”、“日历”、“通讯录”和“附件”。轻按同步图标时，已配置为自动刷新的文件夹（例如“邮箱”、“日历”、“通讯录”）将更新。上次同步的时间戳将在同步图标旁边显示。

照片附件改进功能。在 Secure Mail for Android 中，可以通过轻按新的库图标轻松附加照片。轻按库图标并选择要附加到您的电子邮件的照片。

Secure Mail 10.8.40

支持搜索日历。在 Secure Mail for iOS 中，可以在日历中搜索事件、参与者或任何其他文本。

Secure Mail 10.8.35

Secure Mail for iOS 的版本为 10.8.36。

- 通知响应选项。在 Secure Mail for iOS 中，用户可以响应会议通知，例如“接受”、“拒绝”和“暂定”。用户可以使用“答复”和“删除”响应邮件通知。
- **Secure Mail for Android** 返回按钮的增强功能。在 Secure Mail for Android 中，可以轻按设备上的返回按钮消除浮动操作按钮的展开的选项。如果浮动操作按钮处于展开状态，轻按设备上的返回按钮将折叠响应选项。此操作将使您返回到邮件或事件详细信息视图。
- 在 **Secure Mail for Android** 中，会议响应按钮在电子邮件中显示。收到有关会议邀请的电子邮件通知时，可以通过轻按以下选项之一响应邀请：
  - 是
  - 暂定
  - 否

Secure Mail 10.8.25

Secure Mail for iOS 现在支持对派生凭据使用 **S/MIME**： 要使此功能运行，需要执行以下操作：

- 选择派生凭据作为 S/MIME 证书来源。有关详细信息，请参阅 适用于 iOS 的派生凭据。
- 在 Citrix Endpoint Management 中添加“LDAP 属性”客户端属性。使用以下信息：
  - 键： SEND_LDAP_ATTRIBUTES
  - 值： `userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme=${ user.samaccountname } ,displayName=${ user.displayName } ,mail=${ user.mail }`

有关如何添加客户端属性的步骤，对于 XenMobile Server，请参阅客户端属性，对于 Endpoint Management，请参阅客户端属性。

有关使用派生凭据时设备如何注册的详细信息，请参阅使用派生凭据注册设备。

1. 在 Endpoint Management 控制台中，导航到配置 **>** 应用程序。
2. 选择 **Secure Mail**，然后单击编辑。
3. 在 “iOS 平台” 下，对于 S/MIME 证书来源，请选择派生凭据。

Secure Mail for iOS 和 **Secure Mail for Android** 改进了外观： 我们使得用户导航更加简单、更加高效。我们以导航栏的形式重新调整了 Secure Mail 菜单和操作按钮。有关演示用户导航变更的视频，请参阅：

下图显示了 iOS 设备上的新导航栏。

下图显示了 Android 设备上的新导航栏。

变更内容：

- 删除了提取器图标。Secure Mail 功能（例如邮件、日历、通讯录和附件）现在页脚选项卡栏中作为按钮提供。下图显示了此变更。

  > 注意：
  >
  > 在 Android 设备上，页脚选项卡栏在打开邮件项目后不可用。例如，如下图所示，如果打开电子邮件或日历事件，页脚选项卡栏将不可用。

- 设置菜单在所有菜单中提供，例如邮件、日历、通讯录和附件。要转至设置，请轻按汉堡型图标，然后轻按右下角提供的设置按钮，如下图所示。
- 搜索图标取代了搜索栏，在 “收件箱”、“通讯录” 和 “附件” 视图中提供。
- 在 iOS 设备上，可以按住某个邮件项目以选择该项目。
- 可以轻按撰写浮动操作按钮以撰写新电子邮件，如下图所示。
- 以下菜单选项现在屏幕右上角提供：
  - 同步选项： 轻按右上角的溢出图标，然后导航到更多选项 **>** 同步选项可更改同步首选项。

    > 注意：
    >
    > 此选项仅在 Android 设备上可用。

  - **“搜索”** 图标： 轻按可搜索电子邮件。
- 分类视图图标： 轻按可获取对话的分类视图。
- **“答复”** 浮动操作按钮： 查看电子邮件时，轻按可转发、全部回复或答复，如下图所示。
- 查看电子邮件时，以下菜单选项可从屏幕右上角获取：
  - 标记： 轻按可标记电子邮件。

  - 标记为 **“未读”**： 轻按可将电子邮件标记为未读。
  - 删除： 轻按可删除电子邮件。
  - 更多选项： 轻按溢出图标可查看其他可用操作，例如 “移动”。

日历变更

- 在日历中，可以轻按事件浮动操作按钮以创建事件，如下图所示。
- 以下菜单选项现在可从屏幕右上角获取：
  - 今天： 轻按可查看今天的事件。
  - 搜索： 轻按可搜索事件。
  - **“答复”** 浮动操作按钮： 查看事件时，轻按可转发、全部回复或答复。

查看事件时，事件响应操作（例如，“是”、“暂定” 和 “否”）已重新调整，可从事件详细信息下获取。

联系人变更

- 可以轻按创建新联系人浮动操作按钮，如下图所示。
- 搜索菜单选项现在可以从屏幕右上角获取。可以轻按此选项以搜索联系人。
- 查看联系人时，以下菜单选项可以从屏幕右上角获取：

  在 **Android** 设备上：

  - 编辑： 轻按可编辑联系人。
  - 更多选项： 轻按编辑图标可查看其他可用操作，例如 “附加到邮件”、“共享” 和 “删除”。

  在 **iOS** 设备上：

  - 编辑： 轻按可编辑联系人。
  - 共享： 轻按共享图标可查看其他可用操作，例如 “共享联系人” 和 “附加到邮件”。

  > 注意：
  >
  > 要删除 iOS 设备上的某个联系人，请选择该联系人，然后依次轻按编辑和屏幕底部的删除，如下图所示。

附件变更

面向附件的以下菜单选项现在可以从屏幕右上角获取：

- 排序： 轻按排序图标并选择恰当的过滤器可对附件进行排序。
- 搜索： 轻按可搜索附件。

Secure Mail 10.8.20

- Secure Mail for iOS 现在支持使用派生凭据进行注册和身份验证。有关派生凭据的详细信息，请参阅适用于 iOS 的派生凭据。
- Secure Mail for iOS 支持丰富的推送通知。丰富通知可确保即使 Secure Mail 不在后台运行时，您的收件箱也可以接收锁屏界面通知。此功能在基于密码的身份验证和基于客户端的身份验证设置中受支持。有关详细信息，请参阅 丰富的推送通知。

  > 注意：
  >
  > 由于体系结构中存在为支持丰富的推送通知功能所做的变更，仅限 **VIP** 邮件通知不再可用。

- Secure Mail for Android 以及 Secure Mail for iOS 现在支持 RTF 签名。可以在您的电子邮件签名中使用图像或链接。有关详细信息，请参阅 RTF 签名。

Secure Mail 10.8.15

- **Secure Mail for iOS** 现在支持 **RTF** 签名。可以在您的电子邮件签名中使用图像或链接。有关详细信息，请参阅 RTF 签名。
- **Secure Mail** 支持 **Android Enterprise**，以前称为 **Android for Work**。可以在 Secure Mail 中使用 Android 企业应用程序创建单独的工作配置文件。有关详细信息，请参阅 Secure Mail 中的 Android Enterprise。
- 查看电子邮件时，**Secure Mail** 将呈现嵌入的资源。如果资源存在于您的内部网络中，例如，包含属于内部链接的图像 URL 的邮件，Secure Mail 将连接到内部网络以提取内容并进行呈现。
- **Secure Mail** 支持新式验证。新式验证是基于 OAuth 令牌的身份验证与用户名和密码的结合使用。此支持包括支持对 Office 365 使用内部和外部 Active Directory 联合身份验证服务 (AD FS) 或身份提供程序 (IdP)。
- 增强了附件存储库的性能。可以更加快速地滚动浏览您的附件存储库。

Secure Mail 10.8.10

- 支持打印电子邮件附件。Secure Mail for iOS 支持打印电子邮件附件。
- 面向 **Microsoft office 365** 的新式验证。Secure Mail for iOS 支持新式验证。新式验证是基于 OAuth 令牌的身份验证与用户名和密码的结合使用。此支持包括支持对 Office 365 使用外部和内部 Active Directory 联合身份验证服务 (AD FS) 以及身份提供程序 (IdP)。

  > 注意：
  >
  > - 此版本不支持对 Endpoint Management 与 Microsoft Intune/EMS 的集成使用新式验证。
  > - 此版本包括可从外部访问 AD FS 的场景中的新式验证。

  有关详细信息，请参阅 使用 Microsoft Office 365 的新式验证。

已知问题和已修复的问题

July 19, 2019

下面是当前版本的 Secure Mail 中的已知问题或已修复的问题：

Secure Mail 19.7.5 中的已知问题和已修复的问题

Secure Mail 19.7.5 中的已知问题

此版本中没有已知问题。

Secure Mail 19.7.5 中已修复的问题

- 在 Secure Mail for Android 中，您收到针对已读电子邮件的多个通知。[CXM-67588]
- 在 Secure Mail for iOS 中，日历不同步，并出现以下错误：“无法同步日历”。[CXM-69023]

早期版本中的已知问题和已修复的问题

Secure Mail 19.6.5 中的已知问题

此版本中没有已知问题。

Secure Mail 19.6.5 中已修复的问题

- 在 Secure Mail for iOS 中，当您响应电子邮件时，只有您的响应在“发件箱”中可见，而非整个会话。[CXM-63994]
- 在 Secure Mail for Android 中，无法正确呈现电子邮件内容。[CXM-66710]
- 通过拖放事件来修改日历事件的时间并发送更新时，不会重置被邀请者的响应。[CXM-68078]
- 当您尝试通过拖放事件来更改日历事件的时间时，Secure Mail for Android 间歇性崩溃。[CXM-68080]

Secure Mail 19.5.5 中的已知问题和已修复的问题

Secure Mail 19.5.5 中的已知问题

- 在 Secure Mail for Android 中，当网络访问策略设置为通道 **- Web SSO** 时，您将无法建立 HttpURLConnection。[CXM-66317]
- 在 Secure Mail for iOS 中，应用程序不在前台或后台运行时通知响应选项不起作用。[CXM-68079]

Secure Mail 19.5.5 中已修复的问题

在 Secure Mail for Android 中，当您发送一封电子邮件时，收件人将多次收到该电子邮件。此问题出现在运行 Android 8 或更高版本的设备上。[CXM-66290]

Secure Mail 19.5.0 中的已知问题

在运行 iOS 的设备上，可以连接到在允许使用的 **Wi-Fi** 网络 MDX 策略中定义的允许使用的 Wi-Fi 网络。此问题允许您通过未在 MDX 策略中列出的网络打开 Secure Mail for iOS 和 Secure Web for iOS。[CXM-66730]

Secure Mail 19.5.0 中已修复的问题

- 在 Secure Mail for Android 中，您无法在撰写新电子邮件时将电子邮件地址粘贴到收件人**:** 或抄送**/**密件抄送**:** 字段中。但是，当您回复电子邮件时，可以将电子邮件地址粘贴到收件人**:** 或抄送**/**密件抄送**:** 字段中。[CXM-64752]
- 在 Secure Mail for Android 中，注册 Android Enterprise 设备时，您无法保存帐户配置设置。[CXM-65138]
- 在 Secure Mail for Android 中，使用几天后收件箱变空。[CXM-67159]

Secure Mail for Android 19.4.6 中的已知问题和已修复的问题

本版本中没有已知问题或已修复的问题。

Secure Mail 19.4.5 中的已知问题

此版本中没有已知问题。

Secure Mail 19.4.5 中已修复的问题

- 在 Secure Mail for iOS 中，当您在 Outlook 中发送会议请求并在 Secure Mail 中进行编辑时，会议不会在 Outlook 中更新。收件人也不会收到更新。在 Secure Mail 中创建会议请求并在 Secure Mail 中进行编辑时，也会出现此问题。[CXM-62511]
- 在 Secure Mail for iOS 中，日历不同步，并出现以下错误：“无法同步日历”。[CXM-62796]
- 在 Secure Mail for Android 中，使用 Outlook 创建的某些会议邀请不会反映在您的 Secure Mail 日历中。[CXM-63552]
- 在 Secure Mail for Android 中，定期循环会议在延迟的时间出现，并且对会议所做的更新未正确同步。[CXM-65263]

Secure Mail 19.3.5 中的已知问题

此版本中没有已知问题。

Secure Mail 19.3.5 中已修复的问题

- 在 Secure Web for iOS 中，无法在浏览器中粘贴 bitly URL。[CXM-56276]
- 在 Secure Mail for iOS 中，您收到的没封邮件都会显示以下错误消息：无法提取此邮件。请打开 Secure Mail。[CXM-56418]
- 在 Secure Mail for iOS 中，当用户打开应用程序并输入 PIN 时，他们将长收到以下错误消息：“公司网络不可用”。[CXM-59776]
- 切换到多重身份验证后，Secure Mail for iOS 无法同步。[CXM-62176]

Secure Mail 19.3.0 中的已知问题

本版本中没有已知问题。

Secure Mail 19.3.0 中已修复的问题

- 在 Secure Mail for iOS 中，如果请求由于网络会话无效而超时，则当您收到电子邮件时会间歇性显示以下通知横幅：由于请求超时，**Secure Mail** 无法提取此邮件。[CXM-62561]
- 在 Secure Mail for Android 中，您无法接收来自 mozaiekwonen.xm.cloud.com 的 Firebase Cloud Messaging (FCM) 通知。[CXM-62146]
- 在 Secure Mail for Android 中，当您更新日历事件时，所做的更改不与 Outlook Office 365 同步。[CXM-62227]
- 在 Secure Mail for Android 中，当网络连接质量不佳或者没有网络连接时，不会发送包含附件的电子邮件。即使在恢复了网络连接之后，这些电子邮件仍然保留在发件箱中。[CXM-64297]

Secure Mail 19.2.0 中的已知问题

在 Secure Mail for iOS 中，当证书在联机证书状态协议 (OCSP) 装订中启用了透明度选项时，Secure Mail 配置在 iOS 12.1.1 及更高版本中出现故障。

Secure Mail 19.2.0 中已修复的问题

- 在 Secure Mail for iOS 中，您无法将文本从 Secure Mail 中的主题字段复制到 Secure Notes 10.8.6.6。[CXM-61060]
- 在 Secure Mail for Android 中，如果在 Samsung 设备上启用了预测文本，文本的最后一个字为下划线。如果您没有留下空格，签名中的最后一个字将使用下划线保存，收件人也可以看到最后一个字。[CXM-60894]

- 在 Secure Mail for Android 中，当您收到电子邮件摘要时，不会显示图像。[CXM-62280]
- 安装了 Intune 公司门户版本 5.0.4324.0 时，Secure Mail for Android 在启动时崩溃。有关更多详细信息，请参阅此支持知识中心文章。[CXM-62516]

Secure Mail for iOS 版本 **19.1.6** 中的已知问题和已修复的问题

本版本中没有已知问题或已修复的问题。

Secure Mail 19.1.5 中的已知问题

此版本中没有已知问题。

Secure Mail 19.1.5 中已修复的问题

- 在 Secure Mail for iOS 中，您收到的没封邮件都会显示以下错误消息：无法提取此邮件。请打开 **Secure Mail** [CXM-56418]
- 在 Secure Mail for iOS 中，您经常会在打开应用程序并输入 PIN 码时收到以下错误消息：“公司网络不可用”。[CXM-59766]
- 在打包的 Android 应用程序中，UserAgent 字符串被附加多次，从而导致标头大小增加。此行为将导致出现错误，并且页面无法加载。[CXM-59869]

Secure Mail 19.1.0 中已修复的问题

- 当 Secure Mail 无法连接到 Exchange Server 时，电子邮件通知横幅中将显示以下消息：

  “由于您的会话已过期，我们无法提取此邮件。请打开 Secure Mail 以续订您的会话。”

  此问题已修复且消息将更新，如下所示：

  “Secure Mail 无法连接到贵组织的网络。请与您的管理员联系。” [CXM-59128]
- 对于运行 O365 邮箱的用户，重复执行通知响应操作（例如是、否、可能或删除）会导致 Office 365 停止响应并显示以下错误消息：

  “服务器正忙。请重试。” [CXM-60123]
- 在 Secure Mail for Android 中，如果您使用的土耳其语，您将无法向其地址中包含字符 “I” 的收件人发送电子邮件。[CXM-59093]
- 在 Secure Mail for Android 中，用户将无法选择并突出显示电子邮件的主题行。[CXM-59185]
- 在 Secure Mail for Android 中，如果密码包含字符 €，登录将失败。[CXM-59654]

- 在 Secure Mail for Android 中，启用与本地通讯录同步设置后，所有的 Secure Mail 联系人都将导出到您的本地通讯录。同步后，手机、工作电话、家庭电话、工作传真和家庭传真等电话字段将不会以正确的顺序显示。例如，在您的本机通讯录中，传真号码将显示在手机号码上方。用户无法更改此顺序。[CXM-57994]

Secure Mail 18.12.0 中已修复的问题

- 在 Secure Mail for iOS 中，当您收到富文本格式 (RTF) 的邮件时，某些类型的嵌入式附件和附件符号不可见。[CXM-59121]
- 在 Secure Mail for iOS 中，当启用丰富的推送通知并关闭后再打开邮件通知时，邮件类型选项将间歇性显示。[CXM-59122]
- 如果您在您的环境中运行基于客户端的身份验证机制，Secure Mail 将无法时不时地自动同步电子邮件。执行手动同步仅同步几封电子邮件。[CXM-59650]

Secure Mail 18.11.1 中已修复的问题

- 在连接到 IBM Notes Traveler 9.0.1 SP 10 的 Secure Mail for Android 中，带有附件的电子邮件保存在“发件箱”中。[CXM-58962]

Secure Mail 18.11.0 中已修复的问题

- 在 Secure Mail for Android 中，无法在电子邮件中查看嵌入式图像。[CXM-53556]
- 打开签名中包含嵌入式 URL 的电子邮件时，Secure Mail for Android 将崩溃，例如 `file://C:\...jpg`. [CXM-58219]

Secure Mail 18.10.5 中已修复的问题

- 如果启用了“启用 iOS 数据保护”MDX 策略，您将间歇性地收到“You have new email”（您有新的电子邮件）通知。[CXM-55491]
- 在 iPhone XS 上，无法下载或发送附件且已下载的图像无法显示。[CXM-57030]
- 当用户修改运行 Exchange ActiveSync 版本 16 及更高版本的帐户的定期循环会议后，该会议在 Exchange Server 中不更新。因此，该会议在 Secure Mail 与 Outlook 之间不同步。[CXM-57200]

Secure Mail 18.10.0 中已修复的问题

- 在 Secure Mail for Android 中，用户无法查看指向 Exchange Server 以外的其他服务器的内联图像。[CXM-56736] [CXM-55843]
- 在 Secure Mail for Android 中，加入 Webex 会议时，拨入号码不附带 PIN 码。您必须手动键入 PIN 码。[CXM-56002]

- 如果未配置您的个人日历，则尝试导出 Secure Mail 日历时，Secure Mail for Android 会发生崩溃。[CXM-56264]
- 在 iPhone XS 上的 Secure Mail for iOS 中，无法下载或发送附件且已下载的图像无法显示。[CXM-57030]

Secure Mail 18.9.0 中已修复的问题

- 对于每个 NT LAN Manager (NTLM) 身份验证请求，客户端工作站随机变化。[CXM-55177]
- 当设备处于节电模式时，Android P 上的 Secure Mail 同步间歇性停止操作。[CXM-55441]
- 如果未配置您的个人日历，则尝试导出 Secure Mail 日历时，Secure Mail 发生崩溃。[CXM-56264]

Secure Mail 10.8.65 中已修复的问题

- 启用了 FIP，并且用户在 iOS 11.3 设备上运行 Secure Mail for iOS 时，“剪切和复制” 和 “粘贴”MDX 策略无法按预期工作。[CXM-53993]
- 在共享设备上使用 Secure Mail for iOS 时，新用户可以查看前一个用户的电子邮件，即使该用户已注销也是如此。如果新用户轻按文件夹以刷新显示，前一个用户的电子邮件将不再显示。[CXM-55176]

Secure Mail 10.8.60 中已修复的问题

> 注意：
>
> Secure Mail 版本 10.8.25 到 10.8.60 没有任何已知问题。

- 在运行 IBM Lotus Domino 服务器的 Secure Mail for iOS 中，您将无法在收件箱中使用搜索图标。[CXM-53782]
- 当用户通过 Intune 公司门户注册运行 Secure Mail for Android 的设备时，Secure Mail 停止运行。[CXM-54178]
- 在 FTU 流程中从服务器同步大量邮件文件夹时，Secure Mail for iOS 发生崩溃。[CXM-54371]
- 在 Secure Mail for iOS 中，PDF 的打印预览以更小的尺寸显示。[CXM-54482]
- 在 Secure Mail for Android 中，回复电子邮件时不会自动填充多个电子邮件 ID。[CXM-54811]

Secure Mail 10.8.55 中已修复的问题

- 在 Secure Mail for iOS 中，在横向模式下查看时，日历的 “周” 视图将在 iPad Pro 上错误地呈现。[CXM-53723]

版本 **10.8.55** 中与 **MDX** 有关的已修复问题

- 在 Android 中，Secure Mail 在用户退出 Secure Hub 时崩溃。[CXM-53930]
- 在 iOS 设备上，Secure Web 和 Secure Mail 10.8.45 在启动时崩溃。[CXM-54089]

Secure Mail 10.8.50 中已修复的问题

- Secure Mail for iOS 无法将视频文件保存到 ShareFile。[CXM-42238]
- 在 Secure Mail for Android 中启用了推送通知时，收不到新电子邮件的通知。此问题间歇性发生。[CXM-53135]

Secure Mail 10.8.45 中已修复的问题

Secure Mail 10.8.45 中没有任何已修复的问题。

Secure Mail 10.8.40 中已修复的问题

在 Secure Mail for iOS 中，重复的通知会间歇性针对您收到的每封新电子邮件显示。[CXM-51473]

Secure Mail 10.8.35 中已修复的问题

- 在 Secure Mail for Android 中，自动同步会间歇性停止。用户需要手动同步，以便 Office 365 服务器中的某些新邮件能够在 Secure Mail 中显示。[CXM-49354、CXM-52716]
- 在 Secure Mail for Android 中，即使在 Secure Mail 中禁用了面向电子邮件和日历事件的电子邮件通知，这些通知仍然显示，并出现声音通知。[CXM-50479]
- 使用 Secure Mail for Android 创建全天事件时，您的 Outlook 日历中将显示不正确的日期。[CXM-50612]
- 在 Secure Mail for Android 中，Exchange 个人联系人组不同步到该应用程序。[CXM-51190]
- 配置 SSO 时，从 Secure Mail for Android 通过 SSO 登录 Exchange 失败。系统将提示用户输入密码以登录。[CXM-51343]

Secure Mail 10.8.25 中已修复的问题

- 在 Secure Mail for Android 中，当用户与 Office 365 同步日历邀请时将出现延迟。创建或更新日历邀请时将出现此问题。[CXM-49596]
- 在 Secure Mail for Android 中，当用户在 “抄送:” 字段中键入一个字母，然后轻按发送时：Secure Mail 将邮件发送到频繁使用的用户列表中的第一个用户。但是，通知应显示 “抄送:” 字段条目无效。[CXM-50476]
- 在运行 Android 7 的 Zebra T51 设备上，用户无法安装 Citrix Launcher 应用程序。[CXM-50621]
- 当 NetScaler Gateway 配置了基于证书的身份验证时：在 Secure Mail for iOS 中，每次用户收到新邮件时，都会显示 “您有新邮件” 消息。但是，通知应列出发件人姓名、主题和正文预览。[CXM-51075]

Secure Mail 10.8.20 中已修复的问题

- 如果在仅 MAM 模式下注册的 Android 设备上安装了 Intune 公司门户应用程序，则在 Endpoint Management 中，Secure Mail 将尝试重定向到 Microsoft 登录页面。此时将显示以下错误消息：“未收到该应用程序的任何配置。请联系您的管理员以配置该应用程序。” [CXM-48135]

- 在 Secure Mail for Android 中，如果您的用户名或密码包含特殊字符，例如 ä、ö、ü 或 €，登录将失败。[CXM-48197]
- 在 Android 设备上，重新启动将允许您跳过身份验证来访问 Secure Mail。[CXM-48444]
- 在 Secure Mail for Android 中，在下载内联图像之前答复电子邮件时，邮件将卡在您的发件箱中。显示图片设置在您的设置中处于启用状态时会出现此问题。[CXM-49222]
- 在 Secure Mail for iOS 中，如果 IRM 策略设置为开，电子邮件分类设置为保护，下载完整邮件时您将无法查看附件。[CXM-49544]

Secure Mail 10.8.10 中已修复的问题

- 更新到适用于 iOS 的 Secure Mail 10.7.25 后，Message-ID 标题将缺少括号（< 和 >）。[CXM-46029]
- 在 Secure Mail for iOS 中，当用户从 Outlook 添加日历邀请后，应用程序将立即崩溃。如果您的日历邀请包含表情符号，则会出现此问题。[CXM-46250]
- 在 iOS 中，将移动生产力应用程序升级到 10.7.30 后，如果日志级别设置为 11 或更高级别，Secure Mail 在保留为打开状态时速度将变得缓慢并发生崩溃。[CXM-46721]
- 在 Secure Mail for iOS 中，如果“控制锁定屏幕通知”策略设置为仅计数，则将立即显示重复通知。[CXM-47461]
- 在 Secure Mail for Android 中，当用户在“收件人:”字段中复制并粘贴四个或更多电子邮件地址时，应用程序将崩溃。[CXM-46578]

版本 **19.1.0** 中的已知问题

版本 19.1.0 中没有已知问题。

部署 **Secure Mail**

July 8, 2019

要在 Citrix Endpoint Management（以前称为 XenMobile）中部署 Secure Mail，请按照以下常规步骤进行操作：

1. 可以将 Secure Mail 与 Exchange Server 或 IBM Notes Traveler 服务器集成在一起，从而使 Secure Mail 与 Microsoft Exchange 或 IBM Notes 保持同步。如果您使用的是 IBM Notes，请配置 IBM Notes Traveler 服务器。配置使用 Active Directory 凭据向 Exchange Server 或 IBM Notes Traveler 服务器进行身份验证。有关详细信息，请参阅 集成 Exchange Server 或 IBM Notes Traveler 服务器。

   > 重要：
   >
   > 无法将 Secure Mail 中的邮件与 IBM Notes Traveler（以前称为 IBM Lotus Notes Traveler）同步。此 Lotus Notes 第三方功能当前不受支持。因此，当您从 Secure Mail 中删除响应过的会议邮件时，将不在 IBM Notes Traveler 服务器上删除该邮件。如果用户接受某个日历事件，然后拒绝该事件并添加备

> 注或根据备注执行操作，备注会丢失。[CXM-47936] 要了解有关 IBM/Lotus Notes 的已知限制，请参阅此 Citrix 博客文章。

2. 可以选择启用从 Secure Hub 进行 SSO。为此，请在 Endpoint Management 控制台中配置 Citrix Files 帐户信息，以将 Endpoint Management 用作 Citrix Files 的 SAML 身份提供程序。配置使用 Active Directory 凭据向 Citrix Files 进行身份验证。

   在 Endpoint Management 控制台中配置 Citrix Files 帐户信息是用于所有 Citrix 客户端、Citrix Files 客户端和非 MDX Citrix Files 客户端的一次性设置。有关详细信息，请参阅 在 Endpoint Management 控制台中配置 Citrix Files 帐户信息以用于 SSO。

3. 从 Citrix 下载站点下载 Secure Mail .mdx 文件。
4. 将 Secure Mail 添加到 Endpoint Management 并配置 MDX 策略。有关详细信息，请参阅 [添加应用程序。]。(/en-us/citrix-endpoint-management/apps.html)

> 注意：
>
> 自 Secure Mail 10.6.5 版起，可以为 Secure Mail for iOS 和 Secure Mail for Android 配置新的 MDX 分析策略。Citrix 收集分析数据以提高产品质量。“Google Analytics 的详细信息级别” 策略允许您指定数据可以与您的公司域相关联，还是匿名收集。选择匿名允许用户选择退出包括收集的数据的公司域。这一新策略替换了之前的 Google Analytics 策略。

将此策略设置为匿名时，我们将收集以下类型的数据。我们绝对无法将此数据链接到个人用户或公司，因为我们不请求用户身份信息。所有个人身份信息都不发送到 Google。

- 设备统计信息，例如操作系统版本、应用程序版本和设备型号
- 平台信息，例如 ActiveSync 版本和 Secure Mail 服务器版本
- 产品质量的故障点，例如 APNs 注册、邮件同步和发送，以及附件下载和日历同步。

与公司域不同，当此策略设置为完整时，将不收集任何其他身份信息。默认值为完整。

配置 **Secure Mail**

June 11, 2019

可以在 Secure Mail 中配置并集成以下功能：

- Secure Mail 与 Microsoft Intune/EMS 的集成
- 使用 Office 365 的新式验证
- Secure Mail 的后台服务
- 集成 Exchange Server 或 IBM Notes Traveler 服务器
- 适用于 Secure Mail 的 S/MIME
- 面向 Secure Mail 的 SSO

Secure Mail 与 Microsoft Intune/EMS 的集成

June 11, 2019

通过此集成，您能够以更安全的方式管理和交付 Citrix Secure Mail，以提高生产力。

Secure Mail 支持多种 Intune 配置。您可以将 Secure Mail 连接到本地 Exchange 或 Office 365 邮箱。要设置 Endpoint Management 与 EMS/Intune 的集成，请参阅 Citrix Endpoint Management 与 Microsoft Intune/EMS 的集成

Secure Mail 支持以下部署模式：

- Intune MAM
- Intune MAM 和 Intune 移动设备管理 (MDM)
- Intune MAM 以及 Endpoint Management 仅 MDM
- Intune MAM 以及 Endpoint Management MDM 和 MAM

受支持的邮件服务器

- Exchange Online
- Exchange Server 2016
- Exchange Server 2013

限制

Secure Mail 不支持基于证书的身份验证。

> 重要：
>
> 要在 MDM 模式以及 Citrix Endpoint Management（MDM 和 MAM）中使用 Secure Mail，必须配置环境中的 Secure Hub。

为 **Intune** 配置 **Secure Mail**

如果在 Citrix Endpoint Management MDM 模式下配置您的环境，则 Secure Mail 将自动填充 FTU 体验中的用户名。

要启用此功能，必须在 Endpoint Management 控制台中配置自定义策略。有关详细信息，请参阅 Endpoint Management 文档配置 Secure Mail。

与 **Intune** 不兼容的功能

以下 Secure Mail 功能与含有 EMS/Intune 的 Endpoint Management 集成不兼容：

- Secure Ticket Authority (STA)
- 使用单点登录 (SSO) 注册电子邮件
- 丰富的推送通知
- Citrix Files（以前称为 ShareFile）
- S/MIME 签名和加密
- Microsoft 信息权限管理
- 安全浏览 + 非 KCD SSO 内部 Exchange Server

面向 **Microsoft office 365** 的新式验证

June 27, 2019

Secure Mail 支持面向 Microsoft office 365 的新式验证用作 Active Directory 联合身份验证服务 (AD FS) 或身份提供程序 (IDP)。新式验证是基于 OAuth 令牌的身份验证与用户名和密码的结合使用。使用 iOS 设备的 Secure Mail 用户在连接到 Office 365 时可以利用基于证书的身份验证。登录到 Secure Mail 时，用户通过客户端证书进行身份验证，而非通过键入其凭据进行身份验证。

在继续操作之前，请执行以下操作：

1. 为 Microsoft office 365 启用新式验证 (OAuth)
2. 在防火墙中启用 Office 365 端点、URL 和 IP 地址范围，以确保网络连接达到最佳状态。有关详细信息，请参阅 Office 365 URL 和 IP 地址范围 上的 Microsoft 文档。

Citrix Endpoint Management 策略必备条件

在 Citrix Endpoint Management 控制台中启用以下策略：

对于运行 **iOS** 的设备：

- **Office 365** 身份验证机制：此策略用于指示在 Office 365 中配置帐户时使用 OAuth 机制进行身份验证。此策略具有必须配置的以下值：
  - 不使用 **OAuth**：在帐户配置期间使用此策略进行基本身份验证。
  - 将 **OAuth** 与用户名和密码结合使用： 在身份验证期间使用此策略作为 OAuth 协议。用户必须为 OAuth 流提供用户名和密码以及多重身份验证代码（可选）。
  - 将 **OAuth** 与客户端证书结合使用：如果将 Office 365 配置为执行基于证书的身份验证，请使用此策略。默认配置是不使用 **OAuth**。

对于运行 **Android** 的设备：

- 对 **O365** 使用新式验证：在身份验证期间使用此策略作为 OAuth 协议。
- 新式验证的自定义用户代理：此策略用于更改新式验证的默认用户代理字符串。

iOS 和 **Android** 设备共用的策略：

- 可信 **Exchange Online** 主机名：使用此策略定义在配置帐户时使用 OAuth 机制进行身份验证的可信 Exchange Online 主机名的列表。这是逗号分隔的格式，例如 server.company.com, server.company.co.uk。此列表可以包含默认值或虚 URL，但不能为空。默认值为 **outlook.office365.com**。
- 可信 **AD FS** 主机名：使用此策略定义密码在 Office 365 OAuth 身份验证过程中填充的 Web 页面的可信 AD FS 主机名列表。此列表是逗号分隔的格式，例如 `sts.companyname.com`， `sts.company.co.uk`。如果该列表为空，Secure Mail 将不自动填充密码。Secure Mail 将列出的主机名与 Office 365 身份验证过程中遇到的 Web 页面的主机名进行匹配，并检查页面是否使用 HTTPS 协议。例如，`sts.company.com` 是列出的一个主机名且用户导航到 `https://sts.company.com` 时，在页面具有密码字段的情况下，Secure Mail 将填充密码。默认值为 `login.microsoftonline.com`。
- **Secure Mail Exchange Server**： 使用此策略定义 Exchange Server 的地址。

在设备上刷新策略后，Secure Mail for iOS 现在将通过新式验证启用。

限制

- 如果您在您的环境中使用新式验证，则无法使用适用于 iOS 的丰富推送通知功能。有关丰富的推送通知的详细信息，请参阅 Secure Mail 的推送通知。
- 在设置运行基于证书的身份验证时，不支持多个帐户。

Secure Mail 策略

以下两个表列出了根据 Exchange 基础结构需要的 Secure Mail 策略：

Exchange 基础结构	Office 365 身份验证机制/对 O365 使用新式验证	可信 AD FS Online 主机名	可信 Exchange Online 主机名
本地	关	不适用	不适用
混合 *	开	AD FS/IDP	`Outlook.office365.com` 或虚 URL
Exchange Online	开	AD FS/IDP	`Outlook.office365.com` 或虚 URL

Exchange 基础结构	Secure Mail Exchange Server	后台网络服务 (iOS)	后台网络服务 (Android)
本地	Exchange 本地主机名	本地	本地
混合 *	本地、Exchange Online 主机名	本地、Exchange 本地主机名	本地、Exchange 本地主机名、AD FS/IDP（仅限内部）
Exchange Online	`Outlook.office365.com`	Exchange Online 主机名	Exchange 本地主机名、AD FS、IDP

*Secure Mail 支持具有已迁移邮箱的混合 Exchange 基础结构。

如果本地用户的邮箱已迁移到 Exchange Online，Secure Mail 将自动检测此更改，并提示用户使用新式验证，而无需重新配置其帐户。

> 注意：
>
> 仅当您的邮件服务器和 AD FS 为内部时才配置后台网络服务。

Secure Mail 与 OAuth 支持列表

下表列出了 iOS 和 Android 设备上的 Secure Mail OAuth 支持列表：

身份验证类型	IDP/外部 AD FS	IDP/内部 AD FS	Azure AD	Intune
用户名和密码	是	是	是	是
客户端证书	是	仅限 Android	否	否

Secure Mail 的后台服务

June 11, 2019

要通过 Citrix Gateway 访问邮件服务器，您需要配置 Secure Mail 的后台服务。将 Secure Mail 添加到 Citrix Endpoint Management（以前称为 XenMobile）后，请在 MDX 应用程序策略设置中配置后台服务。

配置 Secure Mail 的后台服务

1. 使用管理员凭据登录到 Endpoint Management 控制台。

2. 在该控制台中，单击配置选项卡，单击应用程序，选择 Secure Mail 应用程序，然后单击编辑。
3. 在 **MDX** 策略设置页面的平台部分中，根据需要选择 iOS 或 Android 平台。
4. 在应用程序设置部分中，配置策略。

后台服务的 **MDX** 应用程序策略配置

以下 MDX 应用程序策略影响 Secure Mail 与 Citrix Gateway、Citrix Endpoint Management 服务器、Secure Ticket Authority (STA) 服务器以及邮件服务器的通信。

网络访问：“网络访问”策略指定 Secure Mail 是否可以使用 VPN 访问后台网络服务，或者所有流量是否可以无限制地通过该 Internet。

- 如果将网络访问策略设置为通过通道连接到内部网络，则仅在后台网络服务中列出的 URL 可以通过 Citrix Gateway。剩余流量则可以无限制地通过 Internet。默认情况下，Secure Mail 访问为通过通道连接到内部网络。
- 如果将网络访问策略设置为不限制，则可以通过 Internet 无限制地发送来自 Secure Mail 的所有流量。不使用 VPN 访问后台服务。

Secure Mail Exchange Server：请将 **Secure Mail Exchange Server** 策略设置为邮件服务器的完全限定的域名 (FQDN)。

后台网络服务：“后台网络服务”策略指定允许通过 Citrix Gateway 进行访问的邮件服务器的列表。列出主机名和采用逗号分隔值形式的端口号。请确保值之间没有前导空格和尾随空格。对于邮件服务器地址，包括：`hostnameFQDN:portnumber`。例如：`mail1.example.com:443,mail2.example.com:443`（逗号之间没有空格）。

后台网络服务网关：“后台网络服务网关”策略指定 Secure Mail 用于连接到邮件服务器的 Citrix Gateway。对于 Citrix Gateway 地址，包括：`citrixgatewayFQDN:portnumber`。例如：`gateway3.example.com:443`。

后台服务票据过期日期：此策略指定后台网络服务票据的有效期。当 Secure Mail 通过 Citrix Gateway 连接到邮件服务器时，Citrix Endpoint Management 会发出一个用于连接到内部邮件服务器的令牌。此设置确定在 Secure Mail 可以使用此令牌之前的持续时间。如果该令牌处于活动状态，则不需要用于身份验证的新令牌并连接到邮件服务器。超过时间限制后，用户必须重新登录以生成新令牌。此令牌的默认值为 168 小时（7 天）。

有关后台服务的 MDX 应用程序策略的详细信息，请参阅：

- 适用于 Android 的 Secure Mail 应用程序设置策略
- 适用于 iOS 的 Secure Mail 应用程序设置策略

下图显示了通信流以及这些策略适用的情形。

以下各图显示了 Secure Mail 与邮件服务器的连接类型。每个图后面是相关策略设置的列表。

直接连接到邮件服务器：

直接连接到邮件服务器的策略：

- 网络访问：无限制

如果网络访问为“不限制”，则以下策略不适用：

- 后台网络服务：不适用
- 后台服务票据过期日期：不适用
- 后台网络服务网关：不适用

通过 **STA** 连接到邮件服务器：

用于通过 STA 连接到邮件服务器的策略：

- 网络访问：通过通道连接到内部网络
- 后台网络服务：`mail.example.com:443,mail1.example1.com:443`
- 后台服务票据过期日期：**168**
- 后台网络服务网关：`gateway3.example.com:443`

> 注意：
>
> Citrix 建议 Secure Mail 使用 STA 连接，因为 STA 连接支持长时间的会话连接。

有关 STA 的详细信息，请参阅此 Citrix 知识中心文章。

集成 **Exchange Server** 或 **IBM Notes Traveler** 服务器

June 11, 2019

为了使 Secure Mail 与邮件服务器保持同步，可以将 Secure Mail 与位于内部网络中或 Citrix Gateway 后面的 Exchange Server 或 IBM Notes Traveler 服务器相集成。

- 要配置 Secure Mail 的后台服务，请参阅：Secure Mail 的后台服务。
- 要为 Secure Mail 配置 IBM Notes Traveler 服务器，请参阅：为 Secure Mail 配置 IBM Notes Traveler 服务器。

> 重要：
>
> 无法将 Secure Mail 中的邮件与 IBM Notes Traveler（以前称为 IBM Lotus Notes Traveler）同步。此 Lotus Notes 第三方功能当前不受支持。因此，举例而言，当您从 Secure Mail 中删除会议邮件时，将不在 IBM Notes Traveler 服务器上删除该邮件。[CXM-47936]
> 要了解有关 IBM/Lotus Notes 的已知限制，请参阅此 Citrix 博客文章。

同步还适用于 Secure Notes 和 Secure Tasks。但请注意，Secure Notes 和 Secure Tasks 已于 2018 年 12 月 31 日达到生命周期结束 (EOL) 状态。有关详细信息，请参阅 EOL 和已弃用的应用程序。

- 要同步 Secure Notes for iOS，请将其与 Exchange Server 集成。
- 要将 Secure Notes 与 Secure Tasks for Android 同步，请使用 Secure Mail for Android 帐户。

将 Secure Mail、Secure Notes 和 Secure Tasks 添加到 Citrix Endpoint Management（以前称为 XenMobile）后，请按后台服务的 MDX 应用程序策略配置中所述配置 MDX 策略。

> 注意：
>
> Secure Mail for Android 和 Secure Mail for iOS 支持为 Notes Traveler 服务器指定的完整路径。例如：`https://mail.example.com/traveler/Microsoft-Server-ActiveSync`。
>
> 无需再为 Traveler 服务器配置带有 Web 站点替换规则的 Domino Directory。

为 **Secure Mail** 配置 **IBM Notes Traveler** 服务器

在 IBM Notes 环境中，必须先配置 IBM Notes Traveler 服务器才能部署 Secure Mail。本节提供了此配置的部署图和系统要求。

> 重要：
>
> 如果您的 Notes Traveler 服务器使用 SSL 3.0，则请注意，SSL 3.0 包含一个名为 Padding Oracle On Downgraded Legacy Encryption (POODLE) 攻击的漏洞，这是一种中间人攻击，影响连接到使用 SSL 3.0 的服务器的任何应用程序。为了解决 POODLE 攻击引入的漏洞，Secure Mail 默认禁用 SSL 3.0 连接，并使用 TLS 1.0 连接到服务器。因此，Secure Mail 无法连接到使用 SSL 3.0 的 Notes Traveler 服务器。有关建议的解决方法的详细信息，请参阅集成 Exchange Server 或 IBM Notes Traveler 服务器中的“配置 SSL/TLS 安全级别”部分。

在 IBM Notes 环境中，必须先配置 IBM Notes Traveler 服务器才能部署 Secure Mail。

下图显示了一个示例部署中 IBM Notes Traveler 服务器和 IBM Domino 邮件服务器的网络部署情况。

系统要求

基础结构服务器要求

- IBM Domino 邮件服务器 9.0.1
- IBM Notes Traveler 9.0.1

身份验证协议

- Domino 数据库
- Lotus Notes 身份验证协议
- 轻型目录身份验证协议

端口要求

- Exchange：默认 SSL 端口为 443。
- IBM Notes：使用端口 443 支持 SSL。默认情况下，使用端口 80 支持非 SSL。

配置 **SSL/TLS** 安全级别

Citrix 对 Secure Mail 进行了修改，解决了前面“重要”注意事项中所述的 POODLE 攻击引入的漏洞。如果您的 Notes Traveler 服务器使用 SSL 3.0，因此，要启用连接，建议的解决方法是在 IBM Notes Traveler Server 9.0 上使用 TLS 1.2。

IBM 发布了一款修补程序，用于阻止在 Notes Traveler 安全服务器到服务器通信中使用 SSL 3.0。该修补程序于 2014 年 11 月发布，作为以下 Notes Traveler 服务器版本的中间修复更新包含在内：9.0.1 IF7、9.0.0.1 IF8 和 8.5.3 Upgrade Pack 2 IF8（将包含在所有将来的版本中）。有关该修补程序的详细信息，请参阅 LO82423: DISABLE SSLV3 FOR TRAVELER SERVER TO SERVER COMMUNICATION（LO82423：对 TRAVELER 服务器到服务器通信禁用 SSLV3）。。

另一个解决方法：将 Secure Mail 添加到 Endpoint Management 中时，请将“连接安全级别”策略更改为 **SSLv3** 和 **TLS**。有关此问题的最新信息，请参阅在 Secure Mail 10.0.3 上默认禁用 SSLv3 连接。

下表基于“连接安全级别”策略值，按操作系统指出了 Secure Mail 支持的协议。您的邮件服务器必须也可以协商协议。

下表显示了连接安全级别为 SSLv3 和 TLS 时 Secure Mail 支持的协议。

操作系统类型	SSLv3	TLS
iOS 9 及更高版本	否	是
Android M 之前的版本	是	是
Android M 和 Android N	是	是
Android O	否	是

下表显示了连接安全级别为 TLS 时 Secure Mail 支持的协议。

操作系统类型	SSLv3	TLS
iOS 9 及更高版本	否	是
Android M 之前的版本	否	是
Android M 和 Android N	否	是
Android O	否	是

配置 **Notes Traveler** 服务器

以下信息与 IBM Domino Administrator 客户端中的配置页面相对应。

- 安全：Internet 身份验证设置为“Fewer name variations with higher security”（名称变化更少，安全性

更高）。此设置用于将 UID 映射到 LDAP 身份验证协议中的 AD User ID（AD 用户 ID）。

- **NOTES.INI** 设置：添加 **NTS_AS_ENFORCE_POLICY=false**。这样可以让 Secure Mail 策略受 Endpoint Management 管理，而不是受 Traveler 管理。此设置可能与当前的客户部署冲突，但会简化 Endpoint Management 部署中设备的管理。
- 同步协议： Secure Mail 当前不支持在 IBM Notes 上使用同步协议 SyncML 以及执行移动设备同步。Secure Mail 通过 Traveler 服务器中内置的 Microsoft ActiveSync 协议同步 “邮件”、“日历” 和 “联系人” 项目。如果将 SyncML 强制作为主要协议，则 Secure Mail 不能通过 Traveler 基础结构回连。
- **Domino** 目录配置 **- Web Internet** 站点： 覆盖 /traveler 的 “会话身份验证”，以禁用基于表单的身份验证。

适用于 **Secure Mail** 的 **S/MIME**

July 19, 2019

Secure Mail 支持安全/多用途 Internet 邮件扩展 (S/MIME)，让用户可以对邮件进行签名和加密，以提高安全性。签名可向收件人确保邮件是由已识别的发件人（而非冒充者）发送的。启用加密后，将仅允许具有兼容证书的收件人打开邮件。

有关 S/MIME 的详细信息，请参阅 Microsoft TechNet。

在下表中，X 指示 Secure Mail 在设备操作系统中支持 S/MIME 功能。

S/MIME 功能	iOS	Android
数字身份提供程序集成： 您可以将 Secure Mail 与受支持的第三方数字身份提供程序集成。您的身份提供程序主机向用户设备上的身份提供程序应用程序提供证书。该应用程序将证书发送到 Endpoint Management 共享保管库（用于存储敏感应用程序数据的安全存储区域）。Secure Mail 从共享保管库中获取证书。有关详细信息，请参阅与数字身份提供程序集成。	X	
派生凭据支持	Secure Mail 支持使用派生凭据作为证书来源。有关派生凭据的详细信息，请参阅适用于 iOS 的派生凭据。	

S/MIME 功能	iOS	Android
通过电子邮件分发证书：通过电子邮件分发证书要求您先创建证书模板，然后使用这些模板请求用户证书。安装并验证证书后，导出用户证书，然后通过电子邮件将其发送给用户。之后用户在 Secure Mail 中打开该电子邮件并导入证书。有关详细信息，请参阅通过电子邮件分发证书。	X	X
自动导入用途单一的证书：Secure Mail 检测证书是否仅用于签名或加密，然后自动导入证书并通知用户。如果证书用于签名和加密，则会提示用户将其导入。	X	

与数字身份提供程序集成

下图显示了证书从数字身份提供程序主机传送到 Secure Mail 的路径。当您将 Secure Mail 与受支持的第三方数字身份提供程序集成时将出现此问题。

MDX 共享保管库是用于存储敏感应用程序数据（例如证书）的安全存储区域。仅受 Endpoint Management 支持的应用程序才可以访问共享保管库。

必备条件

Secure Mail 支持与 Entrust IdentityGuard 集成。

配置集成

1. 准备身份提供程序应用程序并将其提供给用户：
    - 联系 Entrust 以获得.ipa 进行打包。
    - 使用 MDX Toolkit 打包应用程序。

      如果为已在 Endpoint Management 环境外部安装了此应用程序的某个版本的用户部署此应用程序，请使用此应用程序的唯一应用程序 ID。请为此应用程序和 Secure Mail 使用相同的预配配置文件。
    - 将应用程序添加到 Endpoint Management 并将其发布到 Endpoint Management 应用商店。

- 告知您的用户必须从 Secure Hub 安装身份提供程序应用程序。根据需要提供与任何安装后步骤有关的指导。

  Secure Mail 可能会提示用户安装证书，或者在 Secure Mail 设置中启用 S/MIME，具体取决于您如何在下一步骤中为 Secure Mail 配置 S/MIME 策略。这两个过程的步骤在在 Secure Mail for iOS 上启用 S/MIME中进行介绍。

2. 将 Secure Mail 添加到 Endpoint Management 时，请务必配置以下策略：

   - 将 S/MIME 证书源策略配置为共享保管库。此设置表示 Secure Mail 将使用您的数字身份提供程序存储在其共享保管库中的证书。
   - 要在首次启动 Secure Mail 过程中启用 S/MIME，请配置“首次启动 Secure Mail 过程中启用 S/MIME”策略。该策略决定共享保管库中存在证书时 Secure Mail 是否启用 S/MIME。如果没有证书，Secure Mail 将提示用户导入证书。如果未启用该策略，用户可以在 Secure Mail 设置中启用 S/MIME。默认情况下，Secure Mail 不启用 S/MIME，这表示用户必须通过 Secure Mail 设置启用 S/MIME。

使用派生凭据

可以允许使用派生凭据来代替与数字身份提供程序的集成。

将 Secure Mail 添加到 Endpoint Management 时，请将“S/MIME 证书来源”策略配置为派生凭据。有关派生凭据的详细信息，请参阅适用于 iOS 的派生凭据。

通过电子邮件分发证书

可以通过电子邮件向用户分发证书来代替与数字身份提供程序集成或使用派生凭据。此方案需要执行本部分内容详细介绍的以下常规步骤。

1. 使用服务器管理器启用 Microsoft 证书服务的 Web 注册并验证 IIS 中的身份验证设置。
2. 创建证书模板，用于对电子邮件消息进行签名和加密。使用这些模板请求用户证书。
3. 安装并验证证书，然后导出用户证书并通过电子邮件将其发送给用户。
4. 用户在 Secure Mail 中打开电子邮件并导入证书。如此一来，证书仅可用于 Secure Mail。它们不会出现在 S/MIME 的 iOS 配置文件中。

必备条件

本部分中的说明基于以下组件：

- XenMobile Server 10 及更高版本
- 受支持的 Citrix Gateway（以前称为 NetScaler Gateway）版本
- Secure Mail for iOS（最低版本为 10.8.10）、适用于 Android 设备的 Secure Mail（最低版本为 10.8.10）

- Microsoft Windows Server 2008 R2 或更高版本，并将 Microsoft 证书服务用作根证书颁发机构 (CA)
- Microsoft Exchange：
  - Exchange Server 2016 Cumulative Update 4
  - Exchange Server 2013 Cumulative Update 15
  - Exchange Server 2010 SP3 Update Rollup 16

配置 S/MIME 之前，请完成以下必备条件：

- 手动或通过 Endpoint Management 中的凭据设备策略向移动设备交付根证书和中间证书。有关详细信息，请参阅 凭据设备策略。
- 如果正在使用专用服务器证书来保护流向 Exchange Server 的 ActiveSync 流量安全，请执行以下操作：将所有根证书和中间证书安装在移动设备上。

启用 **Microsoft** 证书服务的 **Web** 注册

1. 转到管理工具，然后选择服务器管理器。
2. 在 **Active Directory** 证书服务下，查看是否已安装证书颁发机构 **Web** 注册。
3. 如果需要，请选择添加角色服务来安装证书颁发机构 Web 注册。
4. 选中证书颁发机构 **Web** 注册，然后单击下一步。
5. 安装完成后，单击关闭或完成。

验证 **IIS** 中的身份验证设置

- 确保用于请求用户证书的 Web 注册站点（例如，`https://ad.domain.com/certsrv/`）使用 HTTPS 服务器证书（专用或公用）进行保护。
- Web 注册站点必须通过 HTTPS 进行访问。

1. 转到管理工具，然后选择服务器管理器。
2. 在 **Web** 服务器 **(IIS)** 中的角色服务下进行查找。验证是否已安装客户端证书映射身份验证和 IIS 客户端证书映射身份验证。如果未安装，请安装这些角色服务。
3. 转到管理工具，然后选择 **Internet Information Services (IIS)** 管理器。
4. 在 **IIS** 管理器窗口的左侧窗格中，选择运行 IIS 实例的服务器以进行 Web 注册。
5. 单击身份验证。
6. 确保 **Active Directory** 客户端证书身份验证设置为已启用。
7. 单击右侧窗格中的站点 **> Microsoft Internet Information Services** 的默认站点 **>** 绑定。
8. 如果不存在 HTTPS 绑定，请添加一个。
9. 转到默认 Web 站点主页。
10. 单击 **SSL** 设置，然后单击接受客户端证书。

创建新证书模板

要对电子邮件进行签名和加密，Citrix 建议您在 Microsoft Active Directory 证书服务中创建证书。如果为这两个目的使用相同的证书并存档加密证书，则可以恢复签名证书并允许模拟。

以下过程将在证书颁发机构 (CA) 服务器上复制证书模板：

- 仅 Exchange 签名（用于签名）
- Exchange 用户（用于加密）

1. 打开证书颁发机构管理单元。
2. 展开 CA，然后转到证书模板。
3. 单击鼠标右键，然后单击管理。
4. 搜索“仅 Exchange 签名”模板，在此模板上单击鼠标右键，然后单击复制模板。
5. 分配任意名称。
6. 选中在 **Active Directory** 中发布证书复选框。

   > 注意：
   >
   > 如果未选中在 **Active Directory** 中发布证书复选框，用户必须手动发布用户证书（以用于签名和加密）。用户可以通过 **Outlook** 邮件客户端 **>** 信任中心 **>** 电子邮件安全性 **>** 发布到全局地址列表来实现。

7. 单击请求处理选项卡，然后设置以下参数：
   - 目的： 签名
   - 最小密钥大小： 2048
   - **“**允许导出私钥**”** 复选框： 选中
   - **“**注册证书使用者时无需用户输入**”** 复选框： 选中
8. 单击安全性选项卡，在组或用户名下，确保添加已通过身份验证的用户（或所需的任何域安全组）。此外，还请务必在已通过身份验证的用户的权限下，选中允许对应的读取和注册复选框。
9. 对于其他选项卡和设置，请保留默认设置。
10. 在证书模板中，单击 **Exchange** 用户，然后重复步骤 4 到 9。

    对于新的“Exchange 用户”模板，请使用与原始模板相同的默认设置。

11. 单击请求处理选项卡，然后设置以下参数：
    - 目的： 加密
    - 最小密钥大小： 2048
    - **“**允许导出私钥**”** 复选框： 选中
    - **“**注册证书使用者时无需用户输入**”** 复选框： 选中
12. 两个模板均创建完成后，请务必颁发两个证书模板。单击新建，然后单击要颁发的证书模板。

请求用户证书

本过程使用 user1 导航到 Web 注册页面（如 `https://ad.domain.com/certsrv/`）。本过程为保护电子邮件安全请求两个新用户证书：一个证书用于签名，另一个用于加密。可以为需要通过 Secure Mail 使用 S/MIME 的其他域用户重复执行相同的过程。

在 Microsoft 证书服务上的 Web 注册站点（如 `https://ad.domain.com/certsrv/`）上使用手动注册以生成用于签名和加密的用户证书。另一种方法是，通过组策略为要使用此功能的用户组配置自动注册。

1. 在基于 Windows 的计算机上，打开 Internet Explorer 并转到 Web 注册站点以请求新用户证书。

   > 注意：
   >
   > 请务必使用正确的域用户登录以便请求证书。

2. 登录后，单击请求证书。
3. 单击高级证书请求。
4. 单击创建并向此 **CA** 提交一个请求。
5. 生成用于签名的用户证书。选择合适的模板名称并键入您的用户设置，然后在请求格式旁边，选择 **PKCS10**。

   此时已提交请求。
6. 单击安装此证书。
7. 确认证书安装成功。
8. 现在，为实现加密电子邮件目的重复执行相同过程。在同一个用户登录 Web 注册站点的情况下，转至主页链接以请求新证书。
9. 选择用于加密的新模板，然后键入与第 5 步相同的用户设置。
10. 确保证书安装成功，然后重复执行相同的过程，为另一个域用户生成一对用户证书。本示例按照相同的过程，为“User2”生成一对证书。

    > 注意：
    >
    > 本过程使用同一个基于 Windows 的计算机，为“User2”请求第二对证书。

验证已发布的证书

1. 为确保证书正确安装到域用户配置文件中，请转到 **Active Directory** 用户和计算机 **>** 查看 **>** 高级功能。
2. 转到用户的属性（本示例中为 User1），然后单击发布的证书选项卡。请确保两个证书均可用。您还可以验证每个证书是否有特殊用法。

   下图显示了用于加密电子邮件的证书。

   下图显示了用于对电子邮件进行签名的证书。

请务必向用户分配正确的加密证书。可以在 **Active Directory** 用户和计算机 **>** 用户属性下面验证此信息。

Secure Mail 的工作方式是通过 LDAP 查询来检查 userCertificate 用户对象属性。您可以在属性编辑器选项卡上读取此值。如果此字段为空，或用于加密的用户证书错误，Secure Mail 将无法加密（或解密）邮件。

导出用户证书

此过程采用.PFX (PKCS#12) 格式导出 “User1” 和 “User2” 的证书对以及私钥。导出时，证书通过电子邮件发送给使用 Outlook Web Access (OWA) 的用户。

1. 打开 MMC 控制台并转到证书 **-** 当前用户管理单元。您将看到 “User1” 和 “User2” 证书对。
2. 右键单击证书，然后单击所有任务 **>** 导出。
3. 选择是，导出私钥以导出私钥。
4. 选中如果可能，包括证书路径中的所有证书和导出所有扩展属性复选框。
5. 导出第一个证书后，为用户的剩余证书重复执行相同过程。

> 注意：
>
> 明确标记要用于签名的证书和要用于加密的证书。在本示例中，证书被标记为 userX-sign.pfx 和 userX-enc.pfx。

通过电子邮件发送证书

所有证书采用 PFX 格式导出后，可以使用 Outlook Web Access (OWA) 通过电子邮件发送这些证书。在本示例中，登录名是 User1，发送的电子邮件包含两个证书。

为 User2 或域中的其他用户重复执行相同过程。

在 **Secure Mail for iOS** 和 **Secure Mail for Android** 上启用 **S/MIME**

电子邮件传送后，下一步是使用 Secure Mail 打开邮件，然后启用 S/MIME，使用相应的证书进行签名和加密。

使用单独的签名和加密证书启用 **S/MIME**

1. 打开 Secure Mail，导航到包含 S/MIME 证书的电子邮件。
2. 轻按要下载并导入的签名证书。
3. 键入从服务器导出签名证书时分配给私钥的密码。

   现已导入您的证书。
4. 轻按打开签名

5. 或者，也可以导航到设置 > **S/MIME**，轻按 S/MIME 以打开签名证书。
6. 在签名屏幕中，确认导入了正确的签名证书。
7. 返回到电子邮件并轻按要下载并导入的加密证书。
8. 键入从服务器导出加密证书时分配给私钥的密码。

   现已导入您的证书。
9. 轻按打开加密
10. 或者，也可以导航到设置 > **S/MIME**，轻按 S/MIME 以启用默认加密。
11. 在加密屏幕中，确认导入了正确的加密证书。

> 注意：
>
> a) 如果电子邮件通过 S/MIME 进行数字签名、具有附件，而收件人未启用 S/MIME，则无法接收附件。此行为属于 Active Sync 限制。要接收 S/MIME 邮件，请在 Secure Mail 设置中启用 S/MIME。
>
> b) 使用默认加密选项可以最大程度地减少加密电子邮件所需的步骤。如果此功能处于打开状态，您的电子邮件将在撰写时处于加密状态。如果此功能处于关闭状态，您的电子邮件将在撰写时处于未加密状态，您必须轻按锁定图标才会加密。

使用单个签名和加密证书启用 **S/MIME**

1. 打开 Secure Mail，导航到包含 S/MIME 证书的电子邮件。
2. 轻按要下载并导入的 S/SMIME 证书。
3. 键入从服务器导出证书时分配给私钥的密码。
4. 从显示的证书选项中，轻按相应选项以导入签名证书或加密证书。
   轻按打开证书以查看证书的详细信息。

   现已导入您的证书。

   您可以导航到设置 **> S/MIME** 来查看导入的证书

在 **iOS** 和 **Android** 上测试 **S/MIME**

执行了上一节中所列步骤后，您的收件人可以读取您发送的已签名和加密的邮件。

下图显示了收件人已读的加密邮件的示例。

下图显示了确认签名可信证书的示例。

Secure Mail 在 Active Directory 域中搜索收件人的公用加密证书。如果用户向无有效公用加密密钥的收件人发送加密的邮件，则该邮件将作为未加密邮件发送。在组邮件中，如果有一个收件人无有效的密钥，则邮件将作为未加密邮件发送给所有收件人。

配置公用证书来源

要使用 S/MIME 公用证书，请配置 S/MIME 公用证书来源、LDAP 服务器地址、LDAP 基础 DN 以及匿名访问 LDAP 策略。

除配置应用程序策略外，还请执行以下操作。

- 如果 LDAP 服务器为公共服务器，请确保流量直接传输到 LDAP 服务器。为此，请将 Secure Mail 的网络策略配置为通过通道连接到内部网络并为 Citrix ADC 配置拆分 DNS。
- 如果 LDAP 服务器位于内部网络中，请执行以下操作：
  - 对于 iOS，请确保您未配置 “后台网络服务网关” 策略。如果配置了该策略，用户会频繁收到身份验证提示。
  - 对于 Android，请务必在 “后台网络服务网关” 策略的列表中添加 **LDAP** 服务器 **URL**。

面向 **Secure Mail** 的 **SSO**

April 18, 2019

可以将 Endpoint Management 配置为当用户在 Secure Hub 中注册时自动在 Secure Mail 中注册这些用户。用户无需输入更多信息或执行额外的步骤即可注册 Secure Mail。对于使用电子邮件凭据在 Secure Hub 中注册的用户，此功能要求启用自动发现。如果未启用自动发现，可以为以下注册方法启用此功能：

- 将 Endpoint Management 地址从 Secure Hub 传递到 Secure Mail。
- 用户在 Secure Hub 中注册时输入 Endpoint Management 地址。

在 **Secure Mail** 中启用自动注册

1. 在 Endpoint Management 客户端属性的设置页面上，执行以下操作：

   a. 将以下值设置为 **true**：

   - ENABLE_PASSCODE_AUTH
   - ENABLE_PASSWORD_CACHING
   - ENABLE_CREDENTIAL_STORE

   b. 添加以下配置：

   - 显示名称：SEND_LDAP_ATTRIBUTES
   - 值：userPrincipalName=${user.userprincipalname},sAMAccountNAme=${user.samaccountname}, displayName= ${ user.displayName} ,mail= ${ user.mail}

2. 在设置页面上，将此配置添加到服务器属性中：

   将 MAM_MACRO_SUPPORT 设置为 **true**

3. 配置以下 Secure Mail 属性：
   - 将“初始身份验证机制”设置为用户电子邮件地址。
   - 将“初始身份验证凭据”设置为 **userPrincipalName**。
4. 为用户的 Exchange Server 邮箱配置基于电子邮件的 AutoDiscovery Service。要获取支持，请联系您的 Microsoft Exchange 管理员。本文假定您通过查询 DNS 中的 SRV 记录配置了 Autodiscovery Service。

配置 **Secure Mail** 应用程序策略

将 Secure Mail 应用程序上载到 Endpoint Management。上载与 Secure Mail 应用程序的正确版本关联的.mdx 文件。然后，配置以下 Secure Mail 应用程序设置：

1. 在“初始身份验证机制”中，单击用户电子邮件地址。
2. 在初始身份验证凭据中，单击 **userPrincipalName** 或 **sAMAccountName**。您的选择基于针对用户的 Exchange Mail Server 配置的身份验证类型。
3. 将 Secure Mail Exchange Server 和 Secure Mail 用户域字段留空。
4. 根据需要配置 Secure Mail 应用程序的其他策略并做出必要的交付组分配。

使用自动预配功能的端到端 **Secure Mail SSO** 用户体验

确保您满足以下必备条件。

1. 从 Apple App Store (iOS) 或 Google Play 应用商店 (Android) 安装 Secure Hub。
2. 打开 Secure Hub 并输入电子邮件地址和密码以便在 Endpoint Management 中注册。
3. 从 Apple App Store (iOS) 或 Google Play 应用商店 (Android) 安装 Secure Mail。
4. 打开 Secure Mail 并轻按确定。此步骤允许 Secure Hub 管理 Secure Mail。打开过程中，Secure Mail 将自动配置。

与用户的邮箱数据库对应的 Exchange Server 是从您配置的 Autodiscovery Service 获取的。DNS SRV 记录查询利用从 Secure Hub 提取的用户电子邮件地址。

帐户配置所需的所有详细信息（例如电子邮件地址、userPrincipalName/sAMAccountName 和密码）都是从 Secure Hub 提取的。

配置帐户时，用户可以在 **Secure Mail** > 设置 > 帐户中查看与设备有关的详细信息。

对问题进行故障排除

如果 SSO 配置出现任何问题，都可以尝试执行以下步骤。

1. 确保 XenMobile Server 版本为 10.5 或更高版本。

2. 确保为 Endpoint Management 配置了 AutoDiscovery Service，并且将用户注册配置为使用电子邮件地址。
3. 确保为 Exchange Server 域配置了自动发现。确保 SRV 记录的查询返回 ActiveSync 邮件客户端的预期邮件服务器。
4. 如果此功能出现问题，请收集以下信息并联系 Citrix 技术支持：
    - 下载 Endpoint Management 诊断日志。
    - 收集具有最高日志级别的 Secure Mail 诊断日志。
    - 从托管 Autodiscovery Service 的 Exchange Server 收集 C:\inetpub\logs\LogFiles\W3SVC1 目录中的 IIS 日志。有关 Microsoft 自动发现服务的更多详细信息，请参阅 Exchange Server 中的自动发现服务。

安全注意事项

June 11, 2019

本文探讨 Secure Mail 的安全注意事项以及您可以启用以帮助提高数据安全性的特定设置。

Microsoft IRM 和 AIP 电子邮件权限保护支持

Secure Mail for Android 和 Secure Mail for iOS 支持受 Microsoft 信息权限管理 (IRM) 保护的邮件和 Azure 信息保护 (AIP) 解决方案。此支持受 Citrix Endpoint Management 上已配置的 IRM 策略的制约。

此功能允许使用 IRM 的组织对消息内容应用保护。此功能还允许移动设备用户能够创建和使用受权限保护的内容。默认情况下，IRM 支持设置为关。要启用 IRM 支持功能，请将“信息权限管理”策略设置为开。

在 Secure Mail 中启用信息权限管理

1. 登录到 Endpoint Management 并导航到配置 > 应用程序，然后单击添加。
2. 在添加应用程序屏幕中，单击 **MDX**。
3. 在应用程序信息屏幕中，输入应用程序详细信息，然后单击下一步。
4. 根据您的设备操作系统，选择并上载.mdx 文件。
5. 在应用程序设置下启用信息权限管理。

> 注意：
>
> 启用适用于 iOS 和 Android 的信息权限管理。

收到受权限保护的电子邮件时

当用户收到内容受保护的邮件时，他们会看到以下屏幕：

要查看用户享有的权限的详细信息，请轻按详细信息。

撰写受权限保护的电子邮件时

在撰写邮件时，用户可以设置限制配置文件以启用电子邮件保护。

要对电子邮件设置限制，请执行以下操作：

1. 登录到 Secure Mail 并轻按编写图标。
2. 在撰写屏幕中，轻按电子邮件限制图标。
3. 在限制配置文件屏幕中，轻按所需的限制以应用到电子邮件，然后单击“后退”。

   应用的限制将显示在主题字段下方。

一些组织可能要求严格遵守他们的 IRM 策略。具有 Secure Mail 访问权限的用户可尝试通过篡改 Secure Mail、操作系统甚至硬件平台跳过 IRM 策略。

虽然 Endpoint Management 可以检测某些攻击，但是请考虑采取以下预防措施以提高安全性：

- 查看设备供应商提供的安全指导。
- 使用 Endpoint Management 功能或其他功能，相应地配置设备。
- 为用户提供有关正确使用 IRM 功能（包括 Secure Mail）的指导。
- 部署其他第三方安全软件，以抵抗此类型攻击。

电子邮件安全性分类

Secure Mail for iOS 和 Secure Mail for iOS Android 支持电子邮件分类标记，允许用户在发送电子邮件时指定安全性 (SEC) 标记和分发限制标记 (DLM)。SEC 标记包括“Protected”（受保护）、“Confidential”（私密）和“Secret”（机密）。DLM 包括“Sensitive”（敏感）、“Legal”（法律）或“Personal”（个人）。撰写电子邮件时，Secure Mail 用户可以选择一个标记以指示电子邮件的分类级别，如下图所示。

收件人可以在电子邮件主题中查看分类标记。例如：

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

电子邮件标头包括作为 Internet 邮件标头扩展的分类标记，如下例中粗体文本所示：

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 仅显示分类标记。该应用程序不会根据这些标记采取操作。

用户答复或转发带有分类标记的电子邮件时，SEC 和 DLM 值将默认为原始电子邮件的标记。用户可以选择其他标记。Secure Mail 不验证与原始电子邮件有关的此类更改。

可以通过以下 MDX 策略配置电子邮件分类标记。

- 电子邮件分类： 如果设置为开，Secure Mail 将支持 SEC 和 DLM 的电子邮件分类标记。分类标记在电子邮件标头中作为 X 保护标记的值显示。请务必配置相关的电子邮件分类策略。默认值为关。
- 电子邮件分类命名空间： 根据所使用的分类标准指定电子邮件标头中所需的分类命名空间。例如，命名空间 gov.au 在标头中显示为 NS=gov.au。默认值为空。
- 电子邮件分类版本： 根据所使用的分类标准指定电子邮件标头中所需的分类版本。例如，版本 2012.3 在标头中显示为 VER=2012.3。默认值为空。
- 默认电子邮件分类： 指定用户未选择标记时，Secure Mail 对电子邮件应用的保护标记。此值必须在“电子邮件分类标记”策略的列表中。默认值为 **UNOFFICIAL**。
- 电子邮件分类标记： 指定最终用户可用的分类标记。如果列表为空，Secure Mail 将不包括保护标记列表。标记列表中包含冒号分隔的值对。每个值对中都包含 Secure Mail 中显示的列表值以及标记值（在 Secure Mail 中附加到电子邮件主题和标头的文本）。例如，在标记对 UNOFFICIAL,SEC=UNOFFICIAL 中，列表值为 UNOFFICIAL，标记值为 SEC=UNOFFICIAL。

默认值为能够修改的分类标记列表。Secure Mail 附带以下标记。

- 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 数据保护

必须满足澳大利亚信号局 (ASD) 数据保护要求的企业可以对 Secure Mail 和 Secure Web 使用启用 **iOS** 数据保护策略。默认情况下，策略设置为关。

对于 Secure Web，启用 **iOS** 数据保护设置为开时，Secure Web 为沙盒中的所有文件使用 A 类保护级别。有关 Secure Mail 数据保护的详细信息，请参阅澳大利亚信号局 (Australian Signals Directorate) 数据保护。如果启用此策略，将使用最高数据保护类，因此无需再指定最低数据保护类策略。

更改 **“**启用 **iOS** 数据保护**”** 策略

1. 使用 Endpoint Management 控制台将 Secure Web 和 Secure Mail MDX 文件加载到 Endpoint Management：对于新应用程序，请导航到配置 **>** 应用程序 **>** 添加，然后单击 **MDX**。有关升级的信息，请参阅升级 MDX 或企业应用程序。
2. 对于 Secure Mail，请浏览到应用程序设置，找到启用 **iOS** 数据保护策略，然后将其设置为开。启用此策略不会影响运行较低操作系统版本的设备。
3. 对于 Secure Web，请浏览到应用程序设置，找到启用 **iOS** 数据保护策略，然后将其设置为开。启用此策略不会影响运行较低操作系统版本的设备。
4. 正常配置应用程序策略并保存设置，以将应用程序部署到 Endpoint Management 应用商店。

澳大利亚信号局 **(Australian Signals Directorate)** 数据保护

Secure Mail 为必须满足澳大利亚信号局 (ASD) 计算机安全要求的企业支持 ASD 数据保护。默认情况下，“启用 iOS 数据保护”策略设置为关，Secure Mail 提供 C 类数据保护或使用预配文件中设置的数据保护。

如果此策略设置为开，Secure Mail 在应用程序沙盒中创建和打开文件时指定保护级别。Secure Mail 为以下各项设置 A 类数据保护：

- 发件箱项目
- 相机或本机照片中的照片
- 从其他应用程序粘贴的图像
- 下载的文件附件

Secure Mail 为以下各项设置 B 类数据保护：

- 存储的邮件
- 日历项目
- 通讯录
- ActiveSync 策略文件

B 类保护使锁定设备可以同步，并在下载开始后锁定设备的情况下使下载可以完成。

启用数据保护后，设备锁定时将不发送排队的发件箱项目，因为文件无法打开。如果设备在锁定时终止 Secure Mail，然后又将其重新启动，Secure Mail 在设备解锁并启动 Secure Mail 之前将无法进行同步。

Citrix 建议，如果启用此策略，仅在需要避免创建采用 C 类数据保护的日志文件时启用 Secure Mail 日志记录。

iOS 功能

July 19, 2019

本文探讨 Secure Mail 中支持的 iOS 功能。

管理您的源

可以根据您的要求组织您的源卡。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章组织您的电子邮件。

组通知

利用组通知功能，可以将电子邮件线索中的对话编组在一起。您可以在您的设备的锁屏界面上快速查看分组的通知。默认情况下，在设备上启用组通知设置。此功能要求使用 iOS 12。

Secure Mail 来电显示

在 Secure Mail for iOS 中，可以在设备设置中启用“Secure Mail 来电显示”，以识别来自 Secure Mail 联系人的传入呼叫。必须启用以下管理必备条件：在 Citrix Endpoint Management 中，确保已启用 CallerIDSupportEnabled MDX 策略。

有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章设置来电显示。

在日历中设置颜色

有关此日历功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章为已同步的 Secure Mail 日历设置颜色。

从文件应用程序附加文件

在 Secure Mail for iOS 中，您可以从 iOS 本机文件应用程序附加文件。有关 iOS 文件应用程序的详细信息，请参阅 Apple 文章文件应用程序。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章查看和附加文件。

拼写检查功能

Secure Mail 拼写检查功能按以下方式与设备的“自动转换为大写”和“检查拼写”设置（位于常规 > 键盘下方）交互：

在设备上自动更正	在设备上检查拼写	在 Secure Mail 中检查拼写	行为
开	开	开	显示红色下划线。轻按时，单词将突出显示为粉色，同时显示建议的拼写。
关	关	开	显示红线。轻按时，不显示任何建议。
开	开	关	不显示红色下划线。轻按时，单词将突出显示为粉色，同时显示建议的拼写
关	关	关	不显示红色下划线、突出显示或建议的拼写。
开	关	开	显示红色下划线。轻按时，单词将突出显示为粉色，同时显示建议的拼写。
关	开	开	显示红色下划线。轻按时，单词将突出显示为粉色，同时显示建议的拼写。

在设备上自动更正	在设备上检查拼写	在 Secure Mail 中检查拼写	行为
开	关	关	不显示红色下划线。轻按时，单词将突出显示为粉色，同时显示建议的拼写。
关	开	关	不显示红色下划线。轻按时，单词将突出显示为粉色，同时显示建议的拼写。

“邮箱”屏幕

邮箱屏幕显示您配置的所有帐户，并具有以下视图：

- 所有帐户： 包含您配置的所有 Exchange 帐户的电子邮件。
- 单个帐户：包含单个帐户的电子邮件和文件夹。这些帐户显示为一个列表，您可以展开该列表以查看子文件夹。

默认情况下，所有帐户邮箱是全局视图。此视图包含您在您的设备上配置的所有 Exchange 帐户的附件和电子邮件。

所有帐户邮箱具有以下菜单项：

- 所有附件
- 收件箱
  - 未读
  - 已添加标志
- 草稿
- 已发送邮件
- 发件箱
- 已删除邮件

尽管所有帐户视图集中显示多个帐户的电子邮件，但是以下操作使用默认帐户或主帐户的电子邮件地址：

- 新建邮件
- 新建事件

要在从所有帐户视图撰写新邮件时更改发件人电子邮件地址，请轻按发件人**:** 字段中的默认地址，然后从显示的邮件帐户中选择其他帐户。

> 注意：
>
> 如果从对话视图撰写电子邮件，发件人**:** 字段中会自动填充对话发送到的电子邮件地址。

单个帐户

您配置的所有帐户以列表形式显示在所有帐户下面。默认帐户或主帐户始终显示在首位，后接按字母顺序排列的其他帐户。

单个帐户显示您可能创建的任何子文件夹。您可以轻按文件夹旁边的 **V** 图标查看文件夹的子文件夹。

以下操作仅限于单个帐户：

- 移动项目。
- 从对话视图撰写电子邮件。
- 导入 vCard。
- 保存通讯录。

日历

日历显示属于您设备上多个帐户的所有事件。您可以为单个帐户设置颜色，以区分属于单个帐户的日历事件。

为日历事件设置颜色

1. 轻按页脚栏中的日历图标，然后轻按左上方的汉堡型图标。
   日历屏幕将显示您配置的所有帐户。
2. 轻按 Exchange 帐户右侧显示的默认颜色。
   “颜色”屏幕将显示该帐户的可用颜色。
3. 选择您要的颜色，然后轻按保存。
4. 要返回到上一屏幕，请轻按取消。
   将对属于该 Exchange 帐户的所有日历事件设置选定颜色。

创建日历邀请或事件时，组织者字段中会自动填充默认帐户的电子邮件地址。要更改邮件帐户，请轻按此电子邮件地址，然后选择另一个帐户。

> 注意：
>
> 退出然后启动 Secure Mail 后，应用程序会还原您设备上上次配置的日历设置。

搜索

您可以从邮箱或联系人视图执行全局搜索。此操作显示在应用程序中搜索所有帐户得到的相应结果。
在单个帐户内部进行的所有搜索都仅显示属于该帐户的结果。

在 **iOS** 中打印电子邮件、日历事件或内联图像

您现在可以从自己的 iOS 设备打印电子邮件、日历事件或内联图像。

必备条件

开始操作之前，请确保满足以下要求：

- 阻止 **AirPrint** 选项设置为关。
- 允许查看者打印在 IRM 中处于禁用状态。

默认情况下，打印功能在 Secure Mail for iOS 中处于启用状态。打印功能必须由您的管理员经由 Apple AirPrint 或 Microsoft 信息权限管理 (IRM) 通过管理策略进行控制。在这些情况下，打印电子邮件、日历事件或内联图像将不起作用，并且可能会显示一条错误消息。

打印电子邮件

1. 打开要打印的电子邮件项目。
2. 轻按屏幕左上方的“更多”图标。此时将显示以下选项：
   - 移动
   - 打印
3. 轻按打印。
   此时将显示打印机选项屏幕。
4. 要选择打印机，请轻按选择打印机。
   此时将显示打印机屏幕。
5. 选择要打印到的打印机。
6. 轻按 **–** 或 **+** 减少或增加要打印的份数。
7. 要打印特定页或几个连续页，请轻按范围。
   此时将显示页码范围屏幕。默认情况下，选择所有页。
8. 要更改页码选择，请向上或向下轻扫页码。
9. 轻按打印机选项返回到打印机选项屏幕。
10. 要进行黑白打印，请轻按黑白按钮。默认情况下，Secure Mail 进行彩色打印。
11. 轻按右上方的打印可打印电子邮件。
12. 要取消打印作业，请轻按左上方的取消。

打印日历事件

1. 导航到日历并选择一个事件。
2. 轻按“打印”图标并按照前面的打印电子邮件部分中提及的相同说明进行操作。

要打印内联图像，请执行以下操作：

1. 打开包含内联图像的电子邮件项目。
2. 轻按“更多”图标。此时将显示以下选项：
    - 移动
    - 打印
    - 取消
3. 轻按打印并按照前面的打印电子邮件部分中提及的说明进行操作。

多个会议代码（拨入到会议）

Secure Mail for iOS 支持多个会议代码。您现在可以从可用会议代码列表中选择一个会议代码以加入会议。

拨入会议

1. 打开会议邀请并轻按拨入。
2. 从显示的电话号码列表中，选择一个号码以拨入。
3. 从显示的会议代码列表中，选择一个代码以加入会议。
4. 轻按呼叫加入会议。

使用 **Microsoft Office 365** 的新式验证

Secure Mail for iOS 支持使用 Microsoft Office 365 的新式验证。有关详细信息，请参阅 使用 Office 365 的新式验证。

Android 功能

July 19, 2019

本文探讨 Secure Mail 中支持的 Android 功能。

草稿文件夹自动同步

在 Secure Mail for Android 中，草稿文件夹会自动同步，并且草稿可在所有设备上使用。

此功能在运行 Office 365 或 Exchange Server 2016 及更高版本的设备上可用。

> 注意：
>
> 如果 Secure Mail 草稿包含附件，则不会将附件同步到服务器。

下面的一分钟视频演示了此功能的工作原理：

管理您的源

在 Secure Mail for Android 中，现在可以根据您的要求组织源卡。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章组织您的电子邮件。

查看附件

在 Secure Mail for Android 中，查看邮件和日历附件非常简单。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章查看和附加文件。

打印电子邮件和日历事件

在 Secure Mail for Android 中，可以从 Android 设备打印电子邮件和日历事件。此打印功能将使用 Android 打印框架。

必备条件

- 确保管理员已在 Citrix Endpoint Management 控制台中将块打印策略设置为关。有关适用于 Android 的此策略的信息，请参阅阻止打印策略。
- 如果电子邮件受 IRM 保护，请确保您在电子邮件中启用了允许查看者打印选项。

如果未正确设置这些策略，您将无法打印电子邮件或日历事件。

> 注意：
>
> 此打印功能具有以下已知限制：
>
> - 内联图像仅在您通过轻按显示图片下载图像时才会打印。如果您未轻按显示图片，则仅打印图像占位符。
> - 在 Secure Mail 中，大型电子邮件会被截断。打印之前，请轻按下载完整邮件以打印完整的电子邮件。如果未下载完整的邮件，则将打印被截断的电子邮件。
> - 打印这些项目时，将不添加地电子邮件或事件中的元数据。

打印电子邮件

1. 打开要打印的电子邮件。
2. 轻按屏幕左上方的“更多”图标。此时将显示以下选项：
    - 移动
    - 打印

> 注意：
>
> 在平板电脑上，可以直接使用屏幕左上角的打印图标来打印电子邮件。

1. 轻按打印。此时将显示电子邮件的预览。
2. 轻按列表，将显示以下选项：
    - 另存为 PDF
    - 所有打印机
3. 轻按另存为 **PDF** 以 PDF 格式保存您的电子邮件。
4. 轻按所有打印机。根据您的需求安装打印机。
5. 安装打印机后，轻按选择打印机以选择打印机。此时将显示打印机屏幕。

    > 注意：
    >
    > 打印选项因所选的打印机而异。以下图片来自 Canon E480 打印机，且仅用于表示目的。

6. 选择要打印到的打印机。使用以下打印选项：
    - 手动输入要用于打印的份数。
    - 从列表中选择纸张大小。
    - 从列表中选择颜色。
    - 根据需要选择页面方向。
    - 选择一个页面或一系列页面，然后手动输入页面范围。
7. 设置打印选项后，轻按屏幕上的“打印”图标。

打印内联图像

- 轻按电子邮件中的显示图片并按照前面的打印电子邮件部分中提及的说明进行操作。

打印日历事件

1. 导航到日历并轻按一个事件。
2. 轻按“打印”图标并按照前面的打印电子邮件部分中提及的相同说明进行操作。

使用 **ActiveSync** 标头报告网络钓鱼电子邮件

在 Secure Mail for Android 中，当用户报告网络钓鱼邮件时，系统将以附件的形式生成 EML 文件以表示该邮件。管理员将收到该邮件，并可以查看与报告的邮件相关联的 ActiveSync 标头。

要启用此功能，管理员必须在 Citrix Endpoint Management 控制台中配置“报告网络钓鱼电子邮件地址”策略并将“报告网络钓鱼机制”设置为通过附件进行报告。有关详细信息，请参阅 报告网络钓鱼电子邮件（以附件的形式）。

子文件夹通知

在 Secure Mail for Android 中，您可以在邮件帐户的子文件夹中收到邮件通知。

> 注意：
>
> - 请确保基于 FCM 的推送通知在 Endpoint Management 控制台中处于启用状态，以收取子文件夹的通知。有关基于 FCM 的推送通知的配置步骤，请参阅 Secure Mail 的推送通知。
> - 子文件夹通知功能对 Lotus Notes 服务器不可用。

启用子文件夹通知

1. 转至设置，然后在常规下轻按通知。
2. 在通知屏幕中，轻按邮件文件夹。此时收件箱中将显示一系列子文件夹。
3. 轻按以选择要从其接收通知的文件夹。收件箱默认处于选中状态。

   > 注意：
   >
   > 启用子文件夹通知将启用自动同步。

要禁用子文件夹通知，请取消选中与不希望从其接收通知的子文件夹所对应的复选框。

通知通道

在运行 Android O 或更高版本的设备上，您可以使用通知通道设置来管理您的电子邮件和日历通知的处理方式。您可以使用此功能来自定义和管理您的通知。

要为邮件或日历提醒配置通知，请打开 Secure Mail 并导航到设置 **>** 通知，然后选择所需的通知选项。

然后可以导航到管理邮件通知或管理日历通知分别管理电子邮件或日历通知。

或者，也可以长按设备上的 Secure Mail 应用程序图标，选择应用程序信息，然后轻按通知。

如果您的“振动”设置以前设为仅在静音时，则在使用此功能时，该设置将更改为默认振动设置（关）。

> 注意：
>
> 锁屏界面上的通知功能的可用情况基于您的管理员配置控制锁定屏幕通知 MDX 策略的方式。

从 **Android** 中的库启用文件附件的管理步骤

在 Secure Mail 10.3.5 及更高版本中，如果“入站文档交换 (打开方式)”策略设置为限制，用户无法直接从库应用程序附加图片。如果要让此策略保持设置为限制，但允许用户从库添加照片，请在 Endpoint Management 控制台中按以下步骤进行操作。

1. 将阻止库设置为关。
2. 获取设备的库程序包 ID。下面是一些示例：
   - **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
   - 华为:
     com.android.gallery3d, com.google.android.apps.photos
3. 使隐藏的策略 InboundDocumentExchangeWhitelist 可见：
   - 下载 WorxMail APK 文件并使用 MDX Toolkit 打包该文件。
   - 在您的计算机上找到.mdx 文件，并将文件后缀更改为.zip。
   - 打开.zip 文件，找到 policy_metadata.xml 文件
   - 搜索 InboundDocumentExchangeWhitelist 并将其从 `PolicyHidden>**true**</PolicyHidden` > 更改为 <PolicyHidden>**false**</PolicyHidden>。
   - 保存 policy_metadata.xml 文件。
   - 选择该文件夹中的所有文件，并压缩以创建.zip 文件。

     > 注意：
     >
     > 请勿压缩外部文件夹。请选择文件夹中的所有文件，并压缩选中的文件。
   - 单击生成的压缩文件。
   - 选择获取信息并将文件后缀改回.mdx。

4. 将修改后的.mdx 文件上载到 Endpoint Management 控制台，并将库软件包 ID 列表添加到当前可见的入站文档交换白名单策略。

   请确保程序包 ID 以逗号分隔：

   com.sec.android.gallery3d, com.sec.android.gallery3d.panorama360view, com.google.android.apps.photo

5. 保存并部署 Secure Mail。

Android 用户现在可以从库应用程序附加图片。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章查看和附加文件。

支持的文件格式

X 指示可以在 Secure Mail 中附加、查看和打开的文件格式。

格式	iOS	Android
视频：H.263 AMR NB codec_Mp4		X
视频：H.263 AMR NB codec_3gp		X
视频：H.264 AAC codec_3gp	X	X
视频：H.264 AAC codec_mp4	X	X
视频：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
OGG		X
ICO	X	X

格式	iOS	Android
JPEG	X	X
PNG	X	X
TIF（仅限单页）	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

通讯录

轻按标签栏中的通讯录图标，然后轻按屏幕右上方的汉堡型图标。通讯录屏幕显示以下项目：

- 所有联系人： 显示多个电子邮件帐户中的所有联系人。此选项仅在配置了多个电子邮件帐户时才显示。
- 单个电子邮件帐户：显示与所配置的单个电子邮件帐户有关的联系人。
- 类别：向组联系人显示您可能已从预定义的列表中创建或选择的联系人类别。

查看通讯录文件夹

> 注意：
>
> 通讯录子文件夹在 Secure Mail for Android 上不受支持。如果您已使用 Microsoft Outlook 为联系人创建了文件夹或子文件夹，则无法在 Secure Mail 中看到它们。

1. 在通讯录屏幕中：
   - 轻按所有联系人以查看多个电子邮件帐户中的所有联系人。
   - 轻按单个电子邮件帐户以查看与特定的电子邮件帐户关联的联系人。
2. 轻按类别以查看分组到特定类别下的联系人。您可以选择按照您创建的类别对联系人进行分组，也可以将其分组到预定义列表中的类别下。

您可以将属于单个帐户的联系人同步到您的本地通讯录。

与本地通讯录同步

1. 打开 Secure Mail。
2. 轻按“设置”图标，导航到通讯录 **>** 与本地通讯录同步，然后轻按 > 展开菜单。
3. 在同步本地通讯录屏幕中，启用要同步其通讯录的帐户。
4. 轻按确定。
5. 在系统提示允许 Secure Mail 访问您的通讯录时，轻按确定。

现在，您已成功导出帐户的通讯录。
要撤消此操作，请转到设置 **>** 通讯录 **>** 与本地通讯录同步，然后轻按帐户旁边的开关禁用此功能。轻按确定确认您的操作。

日历

日历显示属于您设备上多个帐户的所有事件。您可以为单个帐户设置颜色，以区分属于单个帐户的日历事件。

> 注意：
>
> 如果启用了个人日历功能，该功能将始终与您的主帐户或默认帐户关联。

为日历事件设置颜色

1. 轻按页脚栏中的日历图标，然后轻按左上方的汉堡型图标。
   日历屏幕将显示您配置的所有帐户。
2. 轻按 Exchange 帐户右侧显示的默认颜色。
   “颜色”屏幕将显示该帐户的可用颜色。
3. 选择您要的颜色，然后轻按保存。

4. 要返回到上一屏幕，请轻按取消。
   将对属于该 Exchange 帐户的所有日历事件设置选定颜色。

创建日历邀请或事件时，组织者字段中会自动填充默认帐户的电子邮件地址。要更改邮件帐户，请轻按此电子邮件地址，然后选择另一个帐户。

搜索

您可以从邮箱或所有联系人视图执行全局搜索。此操作显示在应用程序中搜索所有帐户得到的相应结果。

在单个帐户内部进行的所有搜索都仅显示属于该帐户的结果。

Secure Mail 中的 Android Enterprise

Secure Mail for Android 和 Secure Web for Android 与 Android Enterprise（以前称为 Android for Work）兼容。

必备条件

- 请确保您的设备运行 Android 5.0 或更高版本，以便能够使用此功能。
- 对于本地部署，必须将 **afw.accounts** Endpoint Management 属性设置为 **TRUE**。

在 Endpoint Management 上设置 Android Enterprise 后，移动生产力应用程序将在您的设备上可用。Android Enterprise 图标标识这些应用程序，如下图中突出显示的部分所示。

与 Android Enterprise 兼容的功能

下表列出了与 Android Enterprise 兼容的 Secure Mail 功能。

功能	支持
Exchange Server 自动发现	X
Secure Ticket Authority (STA)	X
导出联系人	X
Microsoft 信息权限管理	X
锁屏界面通知	X
邮件同步	X
电子邮件分类	X
S/MIME 签名和加密	X

功能	支持
Firebase Cloud Messaging (FCM) 服务	X
新式验证 (OAuth)	
多个 Exchange 帐户	X
个人日历	
导出邮件设置	X
共享设备	
Endpoint Management integration with Microsoft Intune/EMS	
Office 365	X
LDAP Exchange Server 2010、2013 和 2016	X
基于证书的身份验证 (CBA)	
GoToMeeting	X
Skype for Business	
个人通讯组列表	X
Citrix Files 兼容性	X
使用单点登录的电子邮件注册	X

下表列出了与 Android Enterprise 兼容的 Secure Web 功能。

功能	支持
安全浏览模式	X
完整 VPN 模式	X
所有应用程序功能	X
与 Secure Mail 的兼容性	X

限制

- 如果在工作配置文件模式下将适用于 Android Enterprise 的允许使用状态栏设备限制策略设置为开，状态栏中将不显示 Secure Mail for Android 中的日历导出进度和推送通知。但是，如果允许，这些通知将显示在锁定屏幕上。有关详细信息，请参阅Android Enterprise 设置。

适用于 **Secure Mail** 的 **iOS** 和 **Android** 功能

July 19, 2019

本文介绍了 Secure Mail 上支持的 iOS 和 Android 功能。

多个 **Exchange** 帐户

现在可以从 Secure Mail 中的“设置”添加多个 Exchange 电子邮件帐户以及在它们之间切换。借助此功能，您可以在一个位置监视您的所有邮件、联系人和日历。管理必备条件如下所示：

- 需要用户名和密码才能配置更多帐户。自动注册或凭据存储配置仅适用于应用程序中的第一个帐户设置。请为所有其他帐户键入用户名和密码。
- 如果您创建的第一个帐户是基于证书的，则无法再添加基于证书的帐户。其他帐户必须使用基于 Active Directory 的身份验证。配置多个帐户时，Secure Mail 不支持基于证书的身份验证。
- 必须在 Citrix ADC 中将拆分通道设置为开，才能允许更多帐户连接到外部网络中的域或 Exchange Server。
- Secure Mail for iOS 仅支持 Exchange 和 Office 365 邮件服务器。

有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章添加 Exchange 帐户。

通讯录

有关联系人的用户帮助文档，请参阅 Citrix 用户帮助中心文章查看并同步您的联系人。

在日历中设置颜色

有关此日历功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章为已同步的 Secure Mail 日历设置颜色。

内部域

可以标识和编辑属于外部组织的邮件收件人。

必备条件： 确保已在 Citrix Endpoint Management 中启用内部域策略，并重新启动应用程序。

创建、答复或转发电子邮件时，邮件列表中会突出显示外部收件人。联系人图标在屏幕左下角显示为警告。轻按联系人图标可修改邮件列表。

在运行 iOS 的设备上：

在运行 Android 的设备上：

轻按联系人图标时，将显示一个弹出窗口，其中包含用于编辑列表或全部删除的选项。轻按编辑列表可选择要删除的收件人。选择收件人后，轻按回收站图标。

在运行 iOS 的设备上：

在运行 Android 的设备上：

人机工程学改进功能

应用此增强功能后，操作按钮将从屏幕顶部移动到底部，以便于访问。这些更改是针对收件箱、日历和联系人屏幕的。

> 注意：
>
> 对于 Android，这些更改是针对收件箱和日历屏幕的。

在运行 iOS 的设备上

在运行 Android 的设备上

响应浮动操作按钮得以增强，与 Citrix 品牌和风格指南保持一致。

此外，应用此增强功能后，删除了从打开的电子邮件访问主“收件箱”屏幕上的按钮的选项。必须退出打开的电子邮件，才能访问诸如源、日历、联系人和附件等项目。

iOS 页脚栏中的选项已更改，有助于保持 iOS 与 Android 之间的统一性。

报告网络钓鱼电子邮件

您可以根据管理员配置的策略报告网络钓鱼电子邮件。

- 报告网络钓鱼电子邮件（以转发邮件的形式）
- 报告网络钓鱼电子邮件（以附件的形式）

报告网络钓鱼电子邮件（以转发邮件的形式）

您可以使用“报告为网络钓鱼”功能报告疑似网络钓鱼的电子邮件（以转发邮件的形式）。您可以将可疑邮件转发到管理员在策略中配置的电子邮件地址。
要启用此功能，管理员必须在 Endpoint Management 控制台中配置“报告网络钓鱼电子邮件地址”策略并将“报告网络钓鱼机制”设置为通过转发进行报告。

重要：

- 仅单独的电子邮件支持“报告为网络钓鱼”功能，整个对话则不支持此功能。
- 对于 IBM Lotus Notes 服务器，系统将以附件的形式报告网络钓鱼邮件。该附件会被发送到在“报告网络钓鱼邮件地址”策略中配置的某个电子邮件地址或一系列地址。
- 报告为网络钓鱼并转发到在该策略中配置的电子邮件地址的原始电子邮件不会从收件箱中删除或隐藏。
- 报告了来自某个特定发件人的网络钓鱼电子邮件后，系统将不会自动阻止未来来自该发件人的电子邮件。
- 当您报告疑似网络钓鱼的电子邮件时，主题行保持不变。

报告网络钓鱼电子邮件（以转发邮件的形式）

1. 使用以下选项之一：
    - 打开电子邮件，轻按更多图标，然后选择报告为网络钓鱼。
    - 在疑似网络钓鱼的电子邮件上向左轻扫，然后轻按更多。
2. 从滑出式菜单中，轻按报告为网络钓鱼。
3. 在确认框中，轻按报告。

系统将报告该电子邮件并将其转发到管理员在策略中配置的一个或多个电子邮件地址。

报告网络钓鱼电子邮件（以附件的形式）

Secure Mail for iOS 和 Secure Mail for Android 允许您报告疑似网络钓鱼的邮件。必须配置报告网络钓鱼邮件地址策略，才能启用此功能。

可以提供一个电子邮件地址或者以逗号分隔的电子邮件地址列表，以报告网络钓鱼邮件。

报告网络钓鱼电子邮件

1. 要报告电子邮件，请向左轻扫并轻按更多。
2. 轻按报告为网络钓鱼。
3. 轻按报告并删除进行确认。

此电子邮件将报告到您配置的一个或多个地址。

导出 **Secure Mail** 日历事件

使用 Secure Mail for iOS 和 Secure Mail for Android，可以将 Secure Mail 日历事件导出到设备的本机日历应用程序中。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章导出 Secure Mail 日历事件。

以下 MDX 策略值适用于您的个人日历中显示的日历事件字段：

- 无 (不导出)
- 会议时间
- 会议时间、地点
- 会议时间、主题、地点
- （对于 **Android**）会议时间、主题、地点和备注
- （对于 **iOS**）会议时间、可用性、与会者、主题、地点、备注

Android 选项：

iOS 选项：

对于 **iOS**

尽管从 Secure Mail 中导出的日历事件可读/写，但在 Secure Mail 外部无法更改事件。

重要：

- 在以下任一情况下，此功能在 Secure Mail 中可见但处于禁用状态：
  - “导出日历”策略设置为关。
  - 您的 MDX 版本不包含该策略
- 如果您的个人日历应用程序中已配置了电子邮件帐户并且您的 iCloud 帐户处于禁用状态，则无法使用此功能。如果您的个人日历应用程序中没有配置其他帐户，则可以使用此功能。
- 要从您的个人日历启动 URL 并编辑 Secure Mail 日历事件，请确保 **“ctxevent:”** 值包含在“应用程序 URL 方案”MDX 策略中。

对于 **Android**

从 Secure Mail 中导出的日历事件是只读事件。要编辑 Secure Mail 事件，请轻按日历事件中的 **Secure Mail** 事件链接。

重要：

- 在以下任一情况下，此功能在 Secure Mail 中可见但处于禁用状态：
  - “导出日历”策略设置为关。
  - 您的 MDX 版本不包含该策略。
- 请确保“入站文档交换”MDX 策略设置为不限制。
- Secure Mail 事件链接在 Samsung 和 Huawei 设备上不可用。

源文件夹

Secure Mail for iOS 和 Secure Mail for Android 在源文件夹中主要包含您的所有未读电子邮件、需要注意的会议邀请以及即将召开的会议。

查看您的源卡

轻按右下角的页脚选项卡栏中的源图标。

此时将显示以下源卡：

- 未读

- 会议邀请
- 即将召开的会议

默认情况下，Secure Mail 将仅显示来自您的主帐户的源。如果配置了多个帐户，则可以查看来自另一个帐户的源。要查看来自其他帐户的源，请轻按源，轻按汉堡型图标，然后选择相应的帐户。

源根据项目的时间戳排序，并具有以下显示上限：

- 五封未读电子邮件
- 两个会议邀请
- 三个即将召开的会议

要查看源卡中的所有项目，请轻按查看全部。

> 注意
>
> ：每个卡中显示的源数量取决于您的设备上设置的邮件同步期限。

源文件夹的增强功能

下面是对现有源文件夹的增强功能：

- 自动同步的所有文件夹中的会议邀请都显示在“源”卡中。
- 在“源”卡中最多可查看五个即将召开的会议。
- 接下来 24 小时内即将召开的会议将显示在“源”卡中，并分类为今天和明天部分。

从日历加入会议

在 Secure Mail 中，用户可以直接从日历中的邀请加入会议。下表列出了支持的会议类型和电话号码格式以及每种类型和格式的拨入要求。

支持的会议类型

会议类型	标识要求	轻按“加入会议”后的操作
GoToMeeting (GTM)	会议内容中的以下内容之一：1) 此类型的 URL：`https://www1.gotomeeting.com/join/1234567892`；2) 以下任意格式的 GTM 访问代码：GTM: 123456789、GTM – 123456789、G2M – 123456789、G2M: 123456789	如果安装了 GTM 应用程序，应用程序将打开，并且用户将加入会议。如果未安装该应用程序，用户将看到一个用于转至应用商店以安装 GTM 的选项。对于 gotomeet.me/username 格式的 GTM，应用程序将打开，用户将加入该会议。

会议类型	标识要求	轻按“加入会议”后的操作
WebEx		Citrix Secure Web 将打开，并打开未打包的 WebEx 应用程序（如果已安装在设备上）。必须在 Android 上的 Secure Web“受限制的打开方式例外列表”中以及 iOS 上的“允许的 URL”策略中将 WebEx 添加为例外。
Skype for Business		用户可以单击在 Secure Web 中打开的链接，该链接随后将打开未打包的 Skype for Business 应用程序（如果已安装在设备上）。在 Android 上的 Secure Web“受限制的打开方式例外列表”策略中将 Skype for Business 应用程序添加为例外。在 iOS 上的“允许的 URL”策略中添加例外。

配置以下策略列表以允许用户轻按会议链接来打开相关应用程序。

Zoom 应用程序

- **iOS -“**允许的 **URL”** 策略：+ˆzoomus:
- **Android -“**打开方式排除项**”** 策略：{action=android.intent.action.VIEW scheme=zoomus package=us.zoom.videomeetings}

Webex（未封装的应用程序）

- **iOS -“**允许的 **URL”** 策略: +ˆwbx: 示例策略字符串为：ˆhttp:,ˆhttps:,ˆmailto:=ctxmail:,+ˆcitrixreceiver:,+ˆtelprom g2m-2:,+ˆcol-g2w-2:,+ˆwbx:,+ˆmaps:ios_addr:
- **Android -“**打开方式排除项**”** 策略：{action=android.intent.action.VIEW scheme=wbx package=com.cisco.webex.meetings}

Skype for Business

- **iOS -“**允许的 **URL”** 策略：+ˆlync:
- **Android -“**打开方式排除项**”** 策略：**{action=an**droid.intent.action.VIEW scheme=lync package=com.microsoft.office.lync15}

Skype

- **iOS -“**允许的 **URL”** 策略： +^skype:
- **Android -“**打开方式排除项**”** 策略： {action=android.intent.action.VIEW scheme=skype package=com.skype.raider}

拨入规范

下面列出了会议类型以及每种类型分别支持的电话号码格式和会议代码格式。

GoToMeeting (GTM):

支持的电话号码格式：

- GTM 格式的任何电话号码。示例：
  - 印度 (免费电话): 000 800 100 7855
  - 美国 (免费电话): 1 877 309 2073
- 满足 RFC 3966 格式标准的任何电话号码。有关详细信息，请参阅 Internet 标准跟踪协议文档。

支持的会议代码格式：

会议代码从会议正文中的以下任意格式中进行选择：

- URL (*.gotomeeting.com/join/123456789)
- URL（`gotomeet.me/username` 格式）
- “GTM” 格式，例如 “GTM:123456789”
- “G2M” 格式，例如 “G2M:123456789”
- “访问代码: 123456789” 等格式

WebEx:

支持的电话号码格式：

- WebEx 拨入格式的任何电话号码。示例（Verizon 和美国）：
  - 1-866-652-5088
  - 1-517-466-3109
- WebEx 音频连接格式的任何电话号码。示例：
  - 1-650-479-3207 (美国免费电话)
- 满足 RFC 3966 格式标准的任何电话号码。

支持的会议代码格式：

会议内容必须包含以下格式之一：

- 会议编码: 123 456 789
- 访问代码: 123 456 789

> 注意：
>
> 对于 9 位数或更少位数的会议代码，将自动添加 # 键以拨入会议。

Skype for Business

支持的电话号码格式：

- RFC 3966 格式的任何电话号码有关详细信息，请参阅 Internet 标准跟踪协议文档。

支持的会议代码格式：

会议正文包含此文本：“会议 ID: 123456789”

> 注意：
>
> 对于 Skype for Business 会议，将自动添加 # 键。

通用音频会议信息

支持的电话号码格式：

- RFC 3966 格式的任何电话号码。有关详细信息，请参阅 Internet 标准跟踪协议文档。示例：
  - 5555555555
  - (555) 555-5555
  - 555-555-5555
  - 555-555-555-5555（如果存在国家/地区代码）
  - 1-555-555-5555
  - +1-555-555-5555

> 注意：
>
> 电话号码中的数字之间应使用一个分隔符。例如，“) –” 会导致数字无法识别。

支持的会议代码格式：

建议的格式：”(电话号码)”,”(代码)”

最多可以指定四个逗号并提供 # 键（如有需要）。请参见本文档中的表格，了解支持的格式列表。

对于音频会议，以下格式允许用户轻按拨入。但是，如果轻按日历会议的正文中的电话号码，则可以拨入会议。用户随后必须手动输入会议代码。支持以下电话号码和会议代码格式。

支持的电话号码格式	会议代码分隔符	示例
RFC 3966 格式的任何电话号码示例：5555555555；(555) 555-5555；555-555-5555；555-555-555-5555（如果存在国家/地区代码）；1-555-555-5555；+1-555-555-5555	参与代码	1-888-999-9999 参与代码：9999999
	参与者 PIN	1-888-999-9999 参与者 PIN：99999999
	来宾代码	1-888-999-9999 来宾代码：99999999
	来宾 PIN	1-888-999-9999 来宾 PIN：99999999
	参与者/来宾代码	1-888-999-9999 参与者/来宾代码：99999999
	席位代码	1-888-999-9999 席位代码：99999999
	席位 PIN	1-888-999-9999 席位 PIN：99999999
	出席者代码	1-888-999-9999 出席者代码：99999999
	出席者 PIN	1-888-999-9999 出席者 PIN：99999999
	主机 PIN	1-888-999-9999 主机 PIN：99999999
	PIN	1-888-999-9999 PIN：99999999
	访问代码	1-888-999-9999 访问代码：99999999
	代码	1-888-999-9999 代码：99999999
	会议代码	1-888-999-9999 会议代码：99999999
	会议 ID	1-888-999-9999 会议 ID：99999999

支持的电话号码格式	会议代码分隔符	示例
	、	+1 (631) 992-3240,958209234#
	„	+1 (631) 992-3240„958209234#
	„,	+1 (631) 992-3240„,958209234#
	„„	+1 (631) 992-3240„„958209234#
	passcode	+1 (631) 992-3240 passcode 958209234#
	ext:	+1 (631) 992-3240 ext:958209234#
	ext.	+1 (631) 992-3240 ext. 958209234#
	;ext=	+1 (631) 992-3240 ext. 958209234#
	extn	+1 (631) 992-3240 extn 958209234#
	HC	+1 (631) 992-3240 HC 958209234#
	xtn	+1 (631) 992-3240 xtn 958209234#
	xt	+1 (631) 992-3240 xt 958209234#
	x	+1 (631) 992-3240 x 958209234#
	PC	+1 (631) 992-3240 PC 958209234#
	pc	+1 (631) 992-3240 pc 958209234#

个人日历叠加

在 iOS 和 Android 设备上，可以从本机日历应用程序导入您的个人日历并在 Secure Mail 中查看您的个人事件。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章查看您的个人日历事件。

插入内联图像

以下过程介绍了如何插入内联图像。

1. 要在您的电子邮件中附加内联图像，请在邮件正文中长按。在显示的选项中，轻按插入图片。
2. Secure Mail 可能会提示您访问照片。此时将显示照片库。导航到库并轻按要插入的图片。
3. 邮件现在将包含您选择的图片。

轻扫操作

在 iOS 和 Android 设备上，您可以通过向左或向右轻扫电子邮件来执行操作。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章使用轻扫操作。

在 **iOS** 和 **Android** 中加入 **Skype for Business** 会议

可以通过 Secure Mail 无缝加入 Skype for Business 会议。此功能要求在您的设备上安装 Skype for Business 应用程序。

加入 **Skype for Business** 会议

1. 轻按 Skype for Business 会议提醒或日历事件。
2. 在事件详细信息屏幕中，轻按 Skype 加入会议。Skype for Business 会议将在新窗口中启动。

   如果未在您的设备上安装 Skype for Business，请轻按安装 **Skype** 以安装该应用程序。

附件的应用内预览以及附件的其他增强功能

您现在可以在 Secure Mail 应用内预览附件（MS Office 和图片），来代替通过使用第三方应用程序（例如 QuickEdit）将其打开。

查看附件时可以执行以下操作：

- 从邮箱中选择要将文件附加到的现有邮件。
- 选择要将文件附加到的新邮件。
- 保存附件以供脱机访问。
- 从脱机文件中删除附件。
- 使用其他应用程序打开附件。
- 查看附件的来源电子邮件或日历事件。

> 注意：
>
> 仅当查看附件存储库中的附件时，才能查看来源电子邮件或日历事件。

还可以在以下情况下预览附件：

- 查看邮件。
- 撰写新邮件。
- “附件”文件夹。
- 日历事件。

选择要将文件附加到的邮件

1. 打开包含附件的电子邮件。
2. 轻按该附件。
3. 轻按附加图标。

   此时将显示“收件箱”。
4. 选择要将此文件附加到的现有邮件，或者轻按新建邮件以将此文件附加到新邮件。

保存附件以供脱机访问

1. 打开附件。
2. 轻按页面右上方的更多图标，然后轻按保存以供脱机访问来保存附件以供脱机访问。

从脱机文件中删除附件

1. 打开附件。
2. 轻按页面右上方的更多图标，然后轻按从脱机文件中删除以从脱机文件中删除附件。

使用其他应用程序打开附件

1. 打开附件。
2. 轻按页面右上方的更多图标，然后轻按打开方式。以使用其他应用程序打开附件。
3. 从显示的选项中，轻按要用于打开附件的一个选项。

查看附件的来源电子邮件或日历事件

1. 轻按屏幕右下方的附件图标。
2. 轻按脱机。
3. 轻按附件，然后轻按屏幕右上方的更多图标。
4. 此时将显示来源电子邮件。

将用户名迁移到电子邮件地址 **(UPN)**

在 Secure Mail for iOS 和 Secure Mail for Android 中，可以从基于 Exchange 用户名和密码的身份验证迁移到基于 UPN 和密码的身份验证。

启用此功能后，您将不需要执行以下任何操作：

- 重新安装 Secure Mail。
- 在 Secure Mail 中删除和添加帐户。
- 在 Secure Mail 中更改用户名。

必备条件

继续进行此迁移之前，请确保用户正在运行 Secure Mail 10.7.25 或更高版本。
必须启用“在身份验证失败时尝试迁移用户名”策略，才能使用此功能。

迁移到基于 **UPN** 的身份验证

1. 在 Endpoint Management 中启用“在身份验证失败时尝试迁移用户名”策略。
2. 将您的 Exchange 用户帐户迁移到与用户的主 SMTP 电子邮件地址匹配的新 UPN。
   这将触发身份验证失败操作。Secure Mail 尝试使用主 SMTP 电子邮件地址进行身份验证。

身份验证成功时，用户帐户将被迁移到更新后的 UPN。

验证迁移

在 **iOS** 设备上： 转至设置，然后轻按帐户以查看详细信息。迁移成功时，主 SMTP 电子邮件地址将显示在帐户屏幕上的用户名字段中。

在 **Android** 设备上： 转至设置，然后轻按帐户以查看详细信息。迁移成功时，主 SMTP 电子邮件地址将显示在帐户详细信息屏幕上的用户名字段中。

私人通讯组列表

必备条件

- Exchange Web 服务 (EWS) 在您的 Exchange Server 上处于启用状态。
- Microsoft Exchange Server 10 SP1 或更高版本。

Secure Mail for iOS 和 Secure Mail for Android 支持私人联系人组。可以查看您在 Secure Mail 中的 Outlook 桌面客户端创建的联系人组。创建的联系人组在 Secure Mail 的“通讯录”中显示。

> 注意：
>
> 不能在 Secure Mail 中查看嵌入的联系人组的成员。

撰写电子邮件或创建日历事件时，可以使用私人通讯组列表。如果使用 Exchange 创建了私人联系人组（通讯组列表），则可以在 Secure Mail 中查看这些组。

查看私人通讯组列表

1. 在 Secure Mail 中，打开通讯录。
2. 键入联系人组的名称。
   联系人组将在搜索结果中显示。
3. 轻按该联系人组以查看成员。

> 注意：
>
> 不能在 Secure Mail 中编辑联系人组。

撰写发送给联系人组的邮件

1. 打开 Secure Mail 并轻按编辑浮动操作按钮以撰写邮件。
2. 在新建邮件屏幕中的收件人**:** 字段中键入联系人组的名称。
3. 在显示的联系人列表中，选择联系人组。

   联系人组将通过以下图标表示：

向联系人组发送日历邀请

1. 打开 Secure Mail 并导航到日历。
2. 轻按 **+** 图标以创建日历事件。
3. 在新建事件屏幕中，轻按被邀请者以添加成员。
4. 键入联系人组的名称以向该组发送邀请。

5. 在显示的联系人列表中，选择联系人组。

RTF 签名

在 Secure Mail for iOS 和 Secure Mail for Android 中，可以在您的电子邮件签名中使用图像或链接。要更新您的签名，只需在签名字段中复制并粘贴图像或链接。

添加 **RTF** 签名

1. 复制要使用的图像或 URL。
2. 导航到 **Secure Mail >** 设置 **>** 签名。
3. 粘贴图像或 URL。

或者，在 iOS 设备上，可以长按签名字段，然后轻按插入图片以从库中选择图像。

文件夹同步

在 Secure mail for iOS 和 Secure mail for Android 中，可以轻按同步图标以刷新 Secure Mail 的所有内容。同步图标存在于 Secure Mail 的滑出式菜单中，例如“邮箱”、“日历”、“通讯录”和“附件”。轻按同步图标时，已配置为自动刷新的文件夹（例如“邮箱”、“日历”、“通讯录”）将更新。上次同步的时间戳将在同步图标旁边显示。

同步文件夹

1. 打开 Secure Mail。
2. 在页脚选项卡栏的可用文件夹中，轻按要同步的文件夹。
3. 轻按屏幕左上角的汉堡型图标。
4. 轻按屏幕左下角的同步图标。
5. 文件夹将同步并且内容将刷新。时间戳将在同步图标旁边显示。

照片附件改进功能

在 Secure Mail for iOS 和 Secure Mail for Android 中，可以通过轻按新的库图标轻松附加照片。

将照片附加到您的电子邮件中

1. 打开 Secure Mail。
2. 轻按撰写以创建邮件，或者轻按答复浮动操作按钮以答复电子邮件。
3. 轻按屏幕右下角的附件图标旁边的库图标。
4. 此时将在屏幕底部显示您的库以及相机和最近使用过的文件图标。
5. 浏览并选择要从库中附加的图像，或者轻按相机图标以拍摄照片。

> 注意：
>
> 轻按附件图标时，将显示以下选项：
>
> - 文件
> - ShareFile（现在称为 Citrix Files）
> - 来自邮件附件

针对 **Secure Mail** 的 “允许 **Secure Web** 域”**MDX** 策略

在 Secure Mail 中，某些外部 URL 必须在本机浏览器而非 Secure Web 中打开。因此，默认情况下，所有 URL 都将在本机浏览器中打开。但是，您可以创建想要专门在 Secure Web 中打开的 URL 的列表。为此，您可以在 Citrix Endpoint Management 控制台中配置名为 “允许 Secure Web 域” 的 MDX 策略。

部署该策略后，以逗号分隔的 URL 主机域列表与应用程序通常发送到外部处理程序的任何 URL 的主机名部分相匹配。通常，您会将此策略配置为 Secure Web 要处理的内部域的列表。

如果将该策略留空（默认设置），则所有 Web 流量都将被发送到 Secure Web，直到将这些 URL 明确排除在过滤之外，否则将重定向 URL。要重定向 URL，您可以配置 “排除域的 URL 过滤器”MDX 策略。此策略指示必须在本机浏览器中打开 URL。此策略的优先级高于 Secure Web 域策略。

您可以配置适用于 Android 和 iOS 的 MDX 策略。

Secure Web 域策略的示例配置

以下过程显示如何提示使用 Secure Mail for Android 的用户在本机 Chrome 浏览器或 Secure Web 中打开 URL。在 iOS 上，这些步骤显示通常能够在 Safari 浏览器中打开的 URL 会自动在 Secure Web 中打开。

对于 **Secure Mail for Android**

1. 在 “应用程序交互” 策略列表中，请在 “受限制的打开方式例外列表” 中输入 *{package=com.android.chrome}*。
2. 在 “应用程序交互”（出站 URL）策略列表中，请在允许 **Secure Web** 域中添加内部站点的 DNS 后缀。

对于其他第三方浏览器，请根据情况使用以下格式：

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


对于 **Secure Mail for iOS**

1. 在“应用程序交互”（出站 URL）策略列表中，请在允许的 **URL** 中添加 +^*safari:*
2. 在应用程序 **URL** 方案中，添加 *safari:*
3. 在允许 **Secure Web** 域中，添加内部站点的 DNS 后缀。

Secure Mail 与 **Slack**（预览版）集成

March 29, 2019

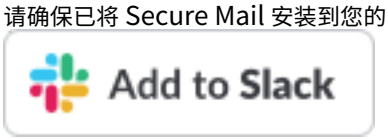
现在可以将您的电子邮件对话转移到运行 iOS 或 Android 的设备上的 Slack 应用程序。

启用此功能后，可以执行以下操作：

- 从邮件无缝切换到 Slack 对话。
- 创建包含您的邮件收件人的 Slack 组对话。
- 在包含您的邮件收件人的 Slack 中创建直接消息。

必备条件

- 对于管理员：
  - 请确保已将 Secure Mail 安装到您的 Slack 工作区。单击下面的 **Add to Slack**（添加到 Slack）按钮。

  - 确保 **Enable Slack**（启用 Slack）策略设置为 **On**（开）。有关策略的详细信息，请参阅：
    * 启用适用于 iOS 的 Slack 策略
    * 启用适用于 Android 的 Slack 策略
- 对于用户：继续操作之前，请确保您具有 Slack 帐户并且您的设备上安装了 Slack 应用程序。

在设备上启用此功能

1. 打开 Secure Mail 并轻按汉堡型图标。
2. 在邮箱屏幕中，轻按屏幕右下角的设置图标。
3. 在设置屏幕中，轻按集成下列出的 **Slack**。
4. 提供您的工作区 Slack URL，然后轻按继续。
5. 提供您的凭据，然后轻按登录。
6. 请求授权 Secure Mail 对信息的访问权限时，轻按授权。

您现在已连接到 Slack。

使用此功能

1. 在 Secure Mail 中打开任意电子邮件对话，然后轻按浮动操作按钮。
2. 在可用选项中，轻按在 **Slack** 中聊天。
3. 对话将切换到包含您的电子邮件中的收件人的 Slack。

请谨记以下几点：

- 在运行 Secure Mail for iOS 或 Secure Mail for Android 的设备上，可以创建最多包含您的电子邮件中的八个收件人的 Slack 对话。如果您的电子邮件中的收件人超过八个，则默认情况下，Secure Mail 将选取您的电子邮件对话中存在的前八个收件人。

通知和同步

June 27, 2019

本文探讨 Secure Mail 的通知和电子邮件同步功能及配置。

Secure Mail for iOS 后台应用程序刷新

如果 Secure Mail for iOS 配置为通过 iOS 后台应用程序刷新（而非 APNs）提供通知，Secure Mail 电子邮件刷新将通过以下方式进行：

- 用户在设备上从设置菜单启用后台应用程序刷新，并且 Secure Mail 在后台运行时，邮件将与服务器同步。同步频率取决于多种因素。
- 如果用户禁用了后台应用程序刷新，则在后台运行时应用程序不会接收电子邮件。
- 用户将 Secure Mail 移至后台时，该应用程序在挂起之前会继续在宽限期内运行。
- 在前台运行时，Secure Mail 将显示实时电子邮件活动，无论后台应用程序刷新设置如何。

Secure Mail 和 **ActiveSync**

Secure Mail 通过 ActiveSync 消息传送协议与 Exchange Server 进行同步。通过此功能，用户可以实时访问其 Outlook 邮件、联系人、日历事件、自动生成的邮箱以及用户创建的文件夹。

> 注意：
>
> ActiveSync 不支持同步 Exchange 公用文件夹。在 Exchange Server 2013 中，ActiveSync 不会同步“草稿”文件夹。

要同步用户创建的文件夹，请执行下列步骤：

iOS

1. 转到设置 **>** 自动刷新。
2. 将自动刷新设置为打开。
3. 轻按打开。将显示所有邮箱的列表。
4. 轻按要同步的文件夹。

Android

1. 转到“邮箱”列表。
2. 轻按要同步的邮箱。
3. 轻按右下角的“更多”图标。
4. 轻按同步选项。
5. 在检查频率下，选择您希望使用的文件夹同步频率。

导出 **Secure Mail** 中的联系人

Secure Mail 用户可以不断地将其联系人与手机的通讯簿同步、一次性将各个联系人导出到手机的通讯簿或者以 vCard 附件形式共享联系人。

要允许使用这些功能，请在 Endpoint Management 控制台中将 Secure Mail 的“导出联系人”策略设置为开。

该策略设置为开时，以下选项在 Secure Mail 中处于启用状态：

- “设置”中的与本地通讯录同步
- 导出各个联系人
- 以 vCard 附件形式共享联系人

“导出联系人”策略设置为关时，这些选项在该应用程序中不显示。

启用该策略后，用户需要将与本地通讯录同步设置为开，才能不断地将联系人从邮件服务器同步到手机的通讯簿。只要与本地通讯录同步设置为开，在 Exchange 或 Secure Mail 中对联系人所做的任何更新都会触发对本地联系人的更新。

由于 Android 存在限制，因此，如果任何 Exchange 或 Hotmail 帐户已设置为与本地通讯录同步，Secure Mail 都无法同步通讯录。

在 iOS 中，可以导出 Secure Mail 联系人并将其与手机联系人同步，即使用户在设备上设置了 Hotmail 或 Exchange 亦如此。请在 Endpoint Management 中通过 Secure Mail 的“覆盖本机联系人检查”策略配置此功能。此策略决定 Secure Mail 是否应覆盖在本机“通讯录”应用程序中配置的 Exchange/Hotmail 帐户中的联系人的检查。如果设置为开，应用程序会将联系人同步到设备，即使在本机“通讯录”应用程序配置了 Exchange/Hotmail 帐户亦如此。如果设置为关，应用程序将继续阻止联系人同步。默认值为开。

Secure Mail 通知

下表概述了 Secure Mail 在前台或后台运行时，如何为支持的移动设备处理通知。

Secure Mail 在前台或后台运行：	iOS 上的通知处理方式	Android 上的通知处理方式
前台	Secure Mail 维护永久 ActiveSync 连接以同步电子邮件和日历活动。	Secure Mail 维护永久 ActiveSync 连接以同步电子邮件和日历活动。
后台（或已终止）	Secure Mail 通过 iOS 后台应用程序刷新功能或 APNs（如果已配置）接收通知。	Secure Mail 维护永久 ActiveSync 连接。

有关配置详细信息，请参阅Secure Mail for iOS 的推送通知。

丰富的推送通知

Secure Mail for iOS 支持丰富的推送通知。丰富通知可确保即使 Secure Mail 不在后台运行时，您的收件箱也可以接收锁屏界面通知。此功能在基于密码的身份验证和基于客户端的身份验证设置中受支持。

> 注意：
>
> 由于体系结构中存在为支持此功能所做的变更，仅限 VIP 邮件通知功能不再可用。

要启用丰富的推送通知功能，请确保满足以下必备条件：

- 在 Endpoint Management 控制台中，将“推送通知”设置开。
- “网络访问”策略设置为不限制或通过通道连接到内部网络。如果您的“网络访问”策略设置为通过通道连接到内部网络，请务必在“后台网络服务”策略中配置 Exchange Web 服务 (EWS) 主机。如果 EWS 和 ActiveSync 主机相同，则请务必在“后台网络服务”策略中配置 ActiveSync 主机。
- “控制锁定屏幕通知”策略设置为允许或电子邮件发件人或事件标题。
- 导航到 **Secure Mail >** 设置 **>** 通知并启用邮件通知。

如果运行的是以下任意设置，则此功能不受支持：

- 面向 Microsoft office 365 的新式验证 (Oauth)
- Endpoint Management 托管的应用程序与 Microsoft InTune/EMS 的集成
- 使用派生凭据注册的设备

iOS 设备上显示“您有新邮件”通知的原因

Secure Mail 在提取邮件详细信息所需的指定 30 秒时间内未收到来自 Exchange Web 服务 (EWS) 的响应时，iOS 设备上将显示“您有新邮件”通知。

您可能还会在 Wi-Fi 或数据连接质量不佳的设备上遇到此行为。

除 EWS 响应延迟外，Secure Mail 还会在以下情况下显示“您有新邮件”通知：

- 当 Secure Mail 无法从安全容器中读取所需的信息时。重新启动您的设备之后以及解锁设备之前，通常会出现这种情况。
- 当 Secure Mail 无法通过 Citrix Gateway 或 EWS 连接到安全通道或设置安全通道时。
- 当您的凭据已过期或者您修改了凭据，但这些凭据尚未在 Secure Mail 中更新时。下图显示了这种情况下通知的显示方式。
- 当 Secure Mail 从 Exchange Server 收到面向来自 Secure Mail 的有效请求的意外响应时。有关 EWS 响应代码的详细信息，请参阅 Microsoft 开发人员文档。

Secure Mail for iOS 中的推送通知失败消息

在 Secure Mail for iOS 中，相应的推送通知失败消息将显示在设备上的通知中心中。这些通知根据通知失败的类型而显示。

根据不同的失败场景，将显示以下通知消息：

- **Secure Mail** 无法连接到贵组织的网络。当 Secure Mail 无法建立与 Citrix Gateway 的 SOCKS5 连接时，将显示该通知。
- **Secure Mail** 无法连接到贵组织的网络。请与您的管理员联系。无法访问 Citrix Gateway 时将显示该通知。请确保已正确配置 Citrix ADC，并且可从外部网络进行访问。
- **Secure Mail** 无法安全地连接到贵组织的网络。请与您的管理员联系。当 Secure Mail 无法建立与 Citrix Gateway 的 SSL 连接时，将显示该通知。请确保您的 SSL 证书有效。
- **Secure Mail** 无法安全地连接到您的邮件服务器。请与您的管理员联系。当 Secure Mail 无法建立与 Exchange Server 的 SSL 连接时，将显示该通知。请确保 Exchange Server 上的 SSL 证书有效。如果希望即使拥有的证书无效时也能将应用程序连接到 Exchange Server，请确保已启用“接受所有 SSL 证书”MDX 策略。
- 由于邮件服务器错误，**Secure Mail** 无法提取邮件。请与您的管理员联系。当 Secure Mail 无法解析来自 Exchange Server 的 EWS 响应时，将显示该通知。
- 由于请求超时，**Secure Mail** 无法提取邮件。当 Secure Mail 无法在 30 秒内收到来自服务器的响应时，将显示该通知。此通知可能会因为您设备上的数据或 Wi-Fi 连接不佳时出现。请等待几分钟后重试。
- 无法提取邮件。请打开 **Secure Mail**。当 Secure Mail 无法从安全容器读取您的凭据时，将显示该通知。当您的设备已重新启动但尚未解锁时，可能会显示该通知。请解锁您的设备以自动允许 Secure Mail 访问安全容器。如果您仍会收到此通知，请打开 Secure Mail 以在安全容器中自动更新您的凭据。

Secure Mail 的推送通知

June 27, 2019

应用程序在后台运行或关闭时，Secure Mail for iOS 和 Secure Mail for Android 可以接收与电子邮件和日历活动有关的通知。Secure Mail for iOS 支持通过后台应用程序刷新提供的通知或通过 Apple 推送通知服务 (APNs) 提供的推送通知。Secure Mail for Android 支持通过 Firebase Cloud Messaging (FCM) 服务提供的通知。

推送通知的工作原理

Secure Mail 发送以下收件箱活动的推送通知：

- 新邮件、会议请求、会议取消、会议更新： APNs 向收件箱推送通知时，Secure Mail 会更新包括“日历”在内的所有文件夹，以便会议变更立即反映在用户的日历中。
- 对于 **iOS**，**Secure Mail** 状态从已读更改为未读（反之亦然）。Secure Mail 图标仅显示 Exchange 收件箱文件夹中未读邮件和新邮件的总数。当用户在桌面或便携式计算机上读取电子邮件后，Secure Mail 更新该图标。

  对于 iOS，Secure Mail 仍提供同步期间收件箱未读电子邮件的计数。如果“控制锁定屏幕通知”策略设置为开，推送通知将在 iOS 唤醒 Secure Mail 以执行同步后显示在锁定设备屏幕上。

  安装或升级过程中，Secure Mail for iOS 将提示用户允许推送通知。用户还可以稍后通过 iOS 设置允许推送通知。

为提供针对 iOS 和 Android 的推送通知，Citrix 在 Amazon Web Services (AWS) 上托管侦听器服务以执行以下功能：

- 侦听存在收件箱活动时 Exchange Server 发送的 Exchange Web 服务 (EWS) 推送通知。Exchange 不将任何邮件内容发送到 Citrix 服务。

  Citrix 服务不存储任何个人可识别信息。相反，设备令牌和订阅 ID 标识特定设备以及 Secure Mail 中要更新的收件箱文件夹。

- 向 iOS 设备上的 Secure Mail 发送 APNs 通知（仅包含徽章计数）。
- 向 Android 设备上的 Secure Mail 发送 FCM 通知。

Citrix 侦听器服务不影响邮件数据流量，该流量通过 ActiveSync 不断在用户设备与 Exchange Server 之间流动。在以下三个区域提供侦听器服务（为高可用性和灾难恢复配置）：

- 美洲地区
- 欧洲、中东和非洲地区 (EMEA)
- 亚太地区 (APAC)

推送通知的系统要求

如果 Citrix Gateway 配置包括 Secure Ticket Authority (STA)，并且拆分通道已关闭，Citrix Gateway 必须允许流量（从 Secure Mail 通过通道传输时）传输到以下 Citrix 侦听器服务 URL：

地理区域	URL	IP 地址
美洲地区	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

为 **Secure Mail** 配置推送通知

要为 Secure Mail 设置 Apple 推送通知或 FCM 以进行应用商店分发，请在 Endpoint Management 控制台中，将“推送通知”设置为开，然后选择您所在的区域。下图显示了 iOS 的设置。

对于 Android，下图显示了与 iOS 相同的推送通知设置。此外，如果 EWS 托管在与邮件服务器所在的区域不同的区域中，请完成 **EWS** 主机名设置。默认设置为空。如果将此设置留空，Endpoint Management 将使用邮件服务器的主机名。

配置 Exchange 和 Citrix ADC 以允许流量流向侦听器服务。

Exchange Server 配置

允许从防火墙到 Exchange Server 所在区域的 Citrix 侦听器服务 URL 的出站 SSL（通过端口 443）。例如：

地理区域	URL	IP 地址
美洲地区	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

地理区域	URL	IP 地址
APAC	https://ap-southeast-1.mailboxlistener.xm.citrix.com	52.74.231.240、54.169.87.20

如果您在 Exchange Web 服务 (EWS) 与 Citrix 侦听器设备之间配置了代理服务器，则可以执行以下操作之一。

- 通过该代理发送 EWS 流量，然后登录到侦听器设备。
- 跳过该代理并将 EWS 流量直接路由到侦听器设备。

要通过代理服务器发送 EWS 流量，请在 ClientAccess\exchweb\ews 文件夹中配置 EWS web.config 文件，如下所示。

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

有关配置代理的更多详细信息，请参阅代理配置。

对于 Exchange 2013 环境，必须手动向 web.config 文件中添加 `system.net` 部分。否则，本文中描述的配置应适用于 Exchange 2013。要进行故障排除，请联系您的 Exchange 管理员。

要跳过代理服务器，请配置跳过列表以允许 Exchange 与 Citrix 侦听器服务建立连接。

通过基于证书的身份验证注册 Secure Hub 时，还必须将 Exchange Server 配置为执行基于证书的身份验证。有关详细信息，请参阅此 Endpoint Management 高级概念一文。

Citrix Gateway 配置

Exchange Server 需要允许将流量传输到侦听器服务，而 Citrix ADC 必须允许将流量传输到注册服务。通过这种方式，设备可以连接以注册发送推送通知。

如果 EWS 和 ActiveSync 服务器不同，请将 Citrix ADC 流量策略配置为允许 EWS 流量。

故障排除

要对出站连接进行故障排除，请查看 Exchange 事件日志，其中包含订阅请求或订阅的通知无效或失败时的日志条目。还可以在 Exchange Server 上运行 Wireshark 跟踪，以跟踪流向 Citrix 侦听器服务的出站流量。

有关其他问题，请尝试使用 Secure Mail Test Tool。

Secure Mail 推送通知常见问题解答

iOS 何时将通知传送至 **Secure Mail**

如果 Secure Mail 在前台运行，通知始终传送至 Secure Mail。这是唯一一种 Citrix 可以保证传送通知的情况。Secure Mail 进入后台时，应用程序徽章计数会始终更新。但是，通知（锁屏界面通知和横幅通知）依赖于后台应用程序刷新（尤其是 iOS 挂起或终止应用程序时），因此通知具有不确定性。以下因素不在 Citrix 的控制范围内。

以下情况可能会影响通知的传送：

- 电池电量低。
- 很少使用 Secure Mail（很少打开到前台）。
- 在核心使用时间范围之外（此时该应用程序在后台挂起一段较长时间）接收了电子邮件；例如，在午夜和早上 6 点之间。

在以下情况下，通知不传送至 Secure Mail：

- 如果用户关闭 Secure Mail，直到用户手动重新打开该应用程序。
- 如果系统已终止 Secure Mail，并且该应用程序尚未自动重新启动。
- Secure Mail 未处于活动状态时。

> 重要：
>
> Secure Mail 由于多种原因而未处于活动状态时，通知可能无法传送至 Secure Mail，包括但不限于以下情况：
>
> - 如果设备处于低功耗模式，且 Secure Mail 在后台运行。这是不传送通知的最常见情况。
> - 如果针对 Secure Mail 的后台应用程序刷新处于关闭状态，并且如果 Secure Mail 在后台运行。请注意，用户控制此设置。
> - 如果设备的网络连接较差。此情况完全取决于 iOS 设备。

Secure Mail 未收到通知时，Secure Mail 不会将新数据同步到设备。因此，会发生以下情况：

- Secure Mail 仅在用户将该应用程序置于前台时同步数据。
- 有新邮件时不显示锁屏界面通知。但日历提醒仍会显示。

Android 何时将通知传送至 **Secure Mail**

在 Android 中，通知始终传送至 Secure Mail。

FCM 如何影响锁屏界面上显示的电子邮件通知

设备锁屏界面上显示的新邮件通知是根据 Secure Mail 同步到设备的数据生成。重要说明：此信息不是来自侦听器服务。

为了显示新邮件通知，Secure Mail 必须能够从 Exchange 同步数据，以便 Secure Mail 具有信息来创建通知。

接收新邮件时，将显示您有新邮件 FCM 通知。电子邮件同步在后台完成后，新邮件将在 Secure Mail 中显示。

后台应用程序刷新如何影响 **Secure Mail** 和 **APNs**

如果用户关闭后台应用程序刷新，会发生以下情况：

- Secure Mail 不是后台应用程序时，Secure Mail 将不接收通知。
- Secure Mail 不在锁屏界面上更新新电子邮件通知。

禁用后台应用程序刷新对 Secure Mail 的行为有重大影响。如前所述，仍然会根据 APNs 进行徽章更新，但在此模式下，电子邮件不会同步到设备。

低功耗模式如何影响 **Secure Mail** 和 **APNs**

在低功耗模式下与 Secure Mail 相关的系统行为与禁用了后台应用程序刷新时相同。在低功耗模式下，设备不会因为定期刷新而唤醒应用程序，且不会向后台应用程序传送通知。因此，负面影响与上文“后台应用程序刷新”部分中列出的影响相同。请注意，在低功耗模式下，徽章更新仍将发生，具体取决于 APNs 通知。

APNs 如何影响锁屏界面上显示的电子邮件通知

设备锁屏界面上显示的新邮件通知是根据 Secure Mail 同步到设备的数据生成。重要说明：此信息不是来自侦听器服务。

为了显示新邮件通知，Secure Mail 需要能够从 Exchange 同步数据，以便 Secure Mail 具有信息来创建通知。

如果 APNs 通知未传送至后台的 Secure Mail，Secure Mail 将不检测通知，因此不会同步新数据。由于 Secure Mail 没有可用的新数据，因此不会在设备锁屏界面上生成任何电子邮件通知，即使在 APNs 通知未传送时也是如此。

哪些其他问题可以导致 **FCM** 驱动的同步在后台失败

多种问题可以导致 FCM 驱动的同步请求失败，包括：

- STA 票据无效。
- Secure Mail 在瞌睡模式下唤醒时，该应用程序有 10 秒的时间从服务器同步所有数据。

如果出现上述任意情况，Secure Mail 将无法同步数据。因此，锁屏通知可能不会显示。

哪些其他问题可以导致 **APNs** 驱动的同步在后台失败

许多问题可以导致 APNs 驱动的同步请求失败，包括：

- STA 票据无效。
- 网络连接较慢。Secure Mail 在后台唤醒时，该应用程序有 30 秒的时间从服务器同步所有数据。
- 如果启用了数据保护策略且 Secure Mail 被 APNs 通知唤醒，当设备处于锁定状态时，Secure Mail 无法访问数据存储，因此不会进行同步。请注意，这是唯一一种系统尝试冷启动 Secure Mail 的情况。如果用户已经在解锁设备后的某个时间启动了 Secure Mail，则即使设备处于锁定状态，APNs 驱动的同步也会成功。

如果发生上述情况中的任何一种，Secure Mail 都无法同步数据，因此无法显示锁屏界面通知。

通知未传送或未使用 **APNs** 时，**Secure Mail** 是否还有别的方法生成锁屏界面通知**?**

如果 APNs 被禁用，Secure Mail 仍会被 iOS 的定期后台应用程序刷新事件唤醒，前提是后台应用程序刷新已启用，且低功率模式处于关闭状态。

在这些唤醒事件中，Secure Mail 从 Exchange Server 同步新电子邮件。之后，此新电子邮件可以用于在锁屏界面上生成电子邮件通知。因此，即使 APNs 通知未传送或 APNs 被禁用，Secure Mail 仍可以在后台同步数据。

重要注意事项：实际发生这种情况的概率低于 APNs 已使用且 APNs 通知传送至 Secure Mail 时的情况。当 iOS 将 APNs 通知路由至 Secure Mail 时，该应用程序会立即从服务器同步数据，且锁屏界面通知会实时显示。

在需要后台应用程序刷新唤醒的情况下，不会实时生成锁屏界面通知。在这种情况下，以完全由 iOS 确定的频率唤醒 Secure Mail。因此，在电子邮件到达 Exchange 上用户的收件箱与 Secure Mail 同步该邮件并生成锁屏界面通知之间可能会间隔一段时间。

另请注意，即使 APNs 已使用时，Secure Mail 仍会收到这些定期唤醒。在后台应用程序刷新唤醒 Secure Mail 的所有情况下，Secure Mail 都会尝试从 Exchange 同步数据。

Secure Mail 与在锁屏界面上显示内容的其他应用程序有什么差异**?**

一个非常重要的差异（也是导致混淆的差异）是 Secure Mail 并不像 Gmail、Microsoft Outlook 及其他应用程序那样总是实时在锁屏界面上显示新电子邮件。这个差异的主要原因是安全性。为了与其他应用程序的行为保持一致，Citrix 侦听器服务需要用户凭据以向 Exchange 进行身份验证来获取电子邮件内容，另外还通过 Citrix 侦听器服务以及 Apple APNs 服务传送此电子邮件内容。Citrix 向 APNs 通知提供的方法不要求 Citrix 侦听器服务获取或存储用户的密码。侦听器服务无权访问用户的邮箱或密码。

有关本机 iOS 邮件应用程序的注意事项：iOS 允许其自己的电子邮件应用程序维持与邮件服务器的持续型连接，这可确保总是传送通知。对于本机邮件范围外的第三方应用程序，不允许使用此功能。

Gmail 应用程序行为： Google 拥有并控制 Gmail 应用程序和 Gmail 服务器。这意味着 Google 可以读取邮件内容，并在 APNs 通知有效负载中包含该邮件内容。当 iOS 从 Gmail 接收此 APNs 通知时，iOS 执行以下操作：

- 将应用程序徽章设置为通知有效负载中指定的值。
- 使用通知有效负载中包含的邮件文本来显示锁屏通知。

这是关键差异：是 iOS 而不是 Gmail 应用程序，根据有效负载中包含的数据来显示锁屏界面通知。其实，iOS 可能从不会唤醒 Gmail 应用程序，这与 iOS 可能不会在有通知时唤醒 Secure Mail 类似。但是，由于有效负载包含邮件代码段，因此 iOS 可以在没有任何邮件数据同步到设备的情况下显示锁屏通知。

在 Secure Mail 中，这种情况有所不同。Secure Mail 必须先从 Exchange 同步邮件数据，应用程序才可以显示锁屏界面通知。

Outlook for iOS 应用程序行为： Microsoft 控制 Outlook for iOS。但是，用户所属的组织控制从其获取数据的 Exchange Server。尽管有此设置，Outlook 仍可以根据 Microsoft 在 APNs 通知中提供的数据来显示锁屏界面通

知，因为 Outlook for iOS 利用 Microsoft 存储用户凭据所采用的模式。之后 Microsoft 直接从其云服务访问用户邮箱，并确定是否有新邮件。

如果有新邮件，Microsoft 云服务将生成包含新邮件数据的 APNs 通知。此模式运行方式与 Gmail 模式类似，即 iOS 仅获取数据并根据该数据生成锁屏界面通知。Outlook iOS 应用程序不参与该过程。

Outlook for iOS 重要安全注意事项： Outlook for iOS 方法有明确的安全含义。组织需要信任 Microsoft 并向其提供其用户的密码，以便 Microsoft 可以访问用户的邮箱，这会构成安全风险。有关 Microsoft 管理用户密码的方式的详细信息，请参阅 Microsoft TechNet。

要查看特定于管理员的与推送通知有关的更多常见问题解答，请参阅此支持知识中心文章。要查看特定于用户的更多常见问题解答，请参阅此支持知识中心文章。

Secure Mail 与其他移动生产力应用程序和 **Citrix Files** 的交互

February 11, 2019

Secure Mail 与其他移动生产力应用程序和 Citrix Files 的交互使用户能够无缝访问、编辑、共享和保存文档，而不需要离开组织的策略所设置的安全环境。例如，在 Secure Mail 中轻按链接可在 Secure Web 中打开站点。用户可以使用适用于 Endpoint Management 的 Citrix QuickEdit 打开和编辑附件。附件下载到用户的 Citrix Files for Endpoint Management 空间。

有关每个平台的完整 Secure Mail 功能列表，请参阅功能（按平台）。

Secure Mail 测试和故障排除

July 8, 2019

如果 Secure Mail 不能正常运行，通常是连接问题所致。本文介绍了如何避免出现连接问题。如果确实出现问题，本文还介绍了如何对问题进行故障排除。

测试 **ActiveSync** 连接、用户身份验证和 **APNs** 配置

可以使用 Endpoint Management Analyzer 执行 Secure Mail 自动发现服务检查。它将引导您下载 Endpoint Management Exchange ActiveSync Test 应用程序。邮件测试选项将检查与邮件服务器的基本连接设置。此工具还可帮助您对 ActiveSync 服务器进行故障排除，以确认其是否已准备好在 Endpoint Management 环境中部署。有关详细信息，请参阅 Endpoint Management Analyzer 工具。

Analyzer 中的 “Mail test”（邮件测试）选项确认以下情况：

- iOS 和 Android 设备与 Microsoft Exchange 或 IBM Traveler 服务器的连接情况。

- 用户身份验证。
- iOS 的推送通知配置，包括 Exchange Server、Exchange Web 服务 (EWS)、Citrix Gateway、APNs 证书及 Secure Mail。有关配置推送通知的信息，请参阅 Secure Mail for iOS 的推送通知。

此工具提供用于更正问题的完整建议列表。

> 注意：
>
> 邮件测试应用程序 MailTest.ipa 已被弃用。请改为访问 Endpoint Management Analyzer 中的相同功能。

执行测试的必备条件

- 请确保未阻止“网络访问”策略。
- 将“阻止电子邮件撰写”策略设置为关。

使用 **Secure Mail** 日志对连接问题进行故障排除

要获取 Secure Mail 日志，请执行以下操作。

1. 转至 **Secure Hub >** 帮助 **>** 报告问题。
2. 从应用程序列表中选择 **Secure Mail**。

   此时将打开一封发送给贵组织的技术支持人员的电子邮件。
3. 填写主题行和正文，用几句话描述您的问题。
4. 选择问题的发生时间。
5. 只有在支持团队指示您这样做时才更改日志设置。
6. 单击发送。

   将打开完成消息，指出已附加压缩的日志文件。
7. 再次单击 **Send**（发送）。

   发送的 zip 文件包括以下日志：

   CtxLog_AppInfo.txt (iOS)、Device_And_AppInfo.txt (Android)、logx.txt 和 WH_logx.txt (Windows Phone)

应用程序信息日志包括与设备和应用程序有关的信息。请验证使用的硬件型号和平台版本是否受支持。验证所使用的 Secure Mail 和 MDX Toolkit 版本是否最新且兼容。有关详细信息，请参阅Secure Mail 的系统要求和Endpoint Management 兼容性。

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

仅会为 Secure Hub 提供 VPN 配置日志。检查 Citrix ADC 版本 `ServerBuildVersion` 以确保所使用的是最新的 Citrix ADC 版本。检查 `SplitDNS` 和 `SplitTunnel` 设置，如下所示：

- 如果“Split DNS”（拆分 DNS）设置为 **Remote**（远程）、**Local**（本地）或 **Both**（二者），确认通过 DNS 正确解析邮件服务器 FQDN。（拆分 DNS 适用于 Android 上的 Secure Hub。）
- 如果“拆分通道”设置为开，请确保邮件服务器作为其中一个可以在后端访问的 Internet 应用程序列出。
- CtxLog_AppPolicies.xml (iOS)、Policy.xml（Android 和 Windows Phone）

策略日志提供截止到获取日志的时间为止，应用于 Secure Mail 的所有 MDX 策略的值。对于连接问题，请确认 <BackgroundServices> 和 <BackgroundServicesGateway> 策略的值。

- 诊断日志（位于“diagnostics”（诊断）文件夹中）

对于 Secure Mail 的初始配置，最常见的问题是“当前无法访问公司网络”。要使用诊断日志对连接问题进行故障排除，请执行以下操作。

诊断日志中的键列包括“Timestamp”（时间戳）、“Message Class”（消息类）和“Message”（消息）。当 Secure Mail 中出现错误消息时，请记下时间，以便快速地在 **Timestamp**（时间戳）列查找相关日志条目。

要确定从设备到 Citrix Gateway 的连接是否成功：请查看 AG Tunneler 条目。以下消息表示连接成功：

- AG policy Intercepting FQDN:443 for STA tunneling（AG 策略正在为 STA 通道拦截 FQDN:443）
- New TCP proxy connection to (null):443 established（与 (null):443 的新 TCP 代理连接已建立）

要确定从 Citrix Gateway 到 Endpoint Management 的连接是否成功（并因此可以验证 STA 票据），请执行以下操作：访问 Secure Hub 诊断日志，并检查设备注册时间“Message Class”（消息类）下面的 INFO (4) 条目。以下消息表示 Secure Hub 从 Endpoint Management 获取了 STA 票据：

- Getting STA Ticket（正在获取 STA 票据）。
- Got STA Ticket response（已获取 STA 票据响应）。
- STA Ticket - Success obtaining STA ticket for App – Secure Mail（STA 票据 - 成功获取应用程序的 STA 票据 – Secure Mail）。

> 注意：
>
> 注册期间，Secure Hub 向 Endpoint Management 发送获取 STA 票据的请求。Endpoint Management 将 STA 票据发送到设备，然后该 STA 票据存储在该设备上并添加到 Endpoint Management STA 票据列表中。

要确定 Endpoint Management 是否向用户签发了 STA 票据，请检查包含在支持包中的 UserAuditLogFile.log。此文件中列出每个票据的发放时间、用户名、用户设备和结果。例如：

Time: 2015-06-30T 12:26:34.771-0700（时间: 2015-06-30T 12:26:34.771-0700）

User: user2（用户：user2）

Device: Mozilla/5.0 (iPad; CPU OS 8_1_2 like macOS)(设备: Mozilla/5.0 (iPad；CPU OS 8_1_2，如 macOS)）

Result: Successfully generated STA ticket for user ‘user2’ for app ‘Secure Mail’（结果: 已成功为应用程序 Secure Mail 的用户 user2 生成 STA 票据）

要检查从 Citrix Gateway 到邮件服务器的通信：请检查是否正确配置了 DNS 和网络连接。为此，请使用 Secure Web 访问 Outlook Web Access (OWA)。与 Secure Mail 类似，Secure Web 也可以使用 Micro VPN 通道与 Citrix

Gateway 建立连接。Secure Web 充当所要访问的内部或外部资源的代理。通常情况下，尤其是在 Exchange 环境中，OWA 托管在邮件服务器上。

要测试配置，请打开 Secure Web 并输入 OWA 页面的 FQDN。此请求所采用的路由和 DNS 解析与 Citrix Gateway 和邮件服务器之间的通信相同。如果 OWA 页面打开，则可以确定 Citrix Gateway 正在与邮件服务器通信。

如果上述所有检查都指示通信成功，则可以确定问题与您的 Citrix 设置无关。相反，该问题与 Exchange 或 Traveler 服务器有关。

您可以收集信息并将其提供给 Exchange 或 Traveler 服务器管理员。首先，通过在 Secure Mail 诊断日志中搜索 “Error” 一词，检查 Exchange 或 Traveler 服务器是否存在 HTTP 问题。如果错误包含 HTTP 代码并且您拥有多个 Exchange 或 Traveler 服务器，请诊断各个服务器。Exchange 和 Traveler 具有 HTTP 日志，其中显示来自客户端设备的 HTTP 请求和响应。Exchange 的日志为 C:\inetpub\LogFiles\W3SVC1\U_EX.log。Traveler 的日志为 IBM_TECHNICAL_SUPPORT>HTTHR.log。

从设备获取 **Secure Mail for iOS** 的崩溃日志

1. 在您的 iOS 设备上，转至设置 > 隐私 > 分析 > 分析数据。
2. 在数据列表中，单击应用程序的名称和相关时间戳。此时将显示日志。

对电子邮件、联系人或日历问题进行故障排除

可以对 Secure Mail 问题进行故障排除，例如一封或多封电子邮件卡在 “草稿” 中、丢失联系人或日历项目未同步。要解决这些问题，请使用 Exchange ActiveSync 邮箱日志。这些日志显示设备发送的传入请求和邮件服务器的传出响应。

有关更多详细信息，请参阅 Under The Hood: Exchange ActiveSync Mailbox Log Analysis（内部结构：Exchange ActiveSync 邮箱日志分析） TechNet 博客文章。

无限制同步最佳实践

当用户将其同步邮件期限设置为全部时，他们具有无限制同步。使用无限制同步时，意味着用户管理其邮箱大小，即收件箱及所有同步的子文件夹。为了获得最佳性能，请注意以下几点：

1. 如果邮箱大小超过 18,000 封邮件或 600 MB 总的大小，电子邮件同步会变慢。
2. 建议您不要启用在 **WiFi** 中加载附件以进行无限制同步。此选项会导致设备上的邮件大小快速膨胀。
3. 为防止您的用户使用无限制同步选项，请将最大同步间隔应用程序策略设置为全部之外的值。
4. 建议您的用户不要将全部设置为默认同步时间间隔。

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