Secure Mail

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

Secure Mail 概述 30

Secure Mail 中的新增功能 32

- 当前版本中的新增功能 32
  - 适用于 iOS 的 Secure Mail 26.8.0 32
    - 支持 iOS/iPadOS 27 32
    - 支持将 Secure Mail 设置为默认邮件应用程序 32
  - 早期版本中的新增功能 33
    - 适用于 Android 的 Secure Mail 26.5.0 33
      - 支持 Android 17 33
    - 适用于 iOS 的 Secure Mail 26.5.0 33
    - 适用于 iOS 的 Secure Mail 26.1.0 33
      - 支持移动响应式电子邮件格式 33
    - 适用于 Android 的 Secure Mail 25.12.0 33
      - 支持 16KB 内存页大小 33
    - 适用于 iOS 的 Secure Mail 25.9.0 33
      - 支持联系人双向同步 33
      - iOS 15 弃用 34
    - 适用于 Android 的 Secure Mail 25.8.0 34
      - 支持 Android API 级别 35 34
    - 适用于 Android 的 Secure Mail 25.6.0 34
      - 旧版 MDX 弃用 34
    - 适用于 iOS 的 Secure Mail 25.5.0 34
      - 支持 iOS 26 34
      - 支持 TLS 1.3 协议 35
      - 支持 Domino 14 FP1 35
      - 旧版 MDX 弃用 35

© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 Android 的 Secure Mail 25.3.0 35
支持 Android 16 35
支持下载大型附件 35
适用于 Android 的 Secure Mail 25.1.0 36
支持 TLS 1.3 协议 36
适用于 iOS 的 Secure Mail 25.1.0 36
支持下载大型附件 36
适用于 Android 的 Secure Mail 24.11.0 36
查看不带水印的电子邮件附件 36
适用于 iOS 的 Secure Mail 24.11.0 36
适用于 iOS 的 Secure Mail 24.9.0 37
支持 iOS 18 37
适用于 Android 的 Secure Mail 24.9.1 37
支持 Android 15 37
适用于 Android 的 Secure Mail 24.9.0 37
支持 API 级别 34 37
适用于 Android 的 Secure Mail 24.7.0 37
适用于 iOS 的 Secure Mail 24.3.0 37
适用于 iOS 的 Secure Mail 24.2.0 37
适用于 Android 的 Secure Mail 24.1.0 37
支持日历事件的放大功能 37
适用于 iOS 的 Secure Mail 23.9.0 38
支持 iOS 17 38
支持 HCL Domino 12 38
适用于 Android 的 Secure Mail 23.8.2 39
查看没有水印的电子邮件附件 39
适用于 Android 的 Secure Mail 23.8.1 39
查看无水印的电子邮件附件 39

© 1997–2026 Citrix Systems, Inc. All rights reserved.

支持 HCL Domino 12 39

适用于 Android 的 Secure Mail 23.8.0 39

支持 Android 14 39

适用于 Android 的 Secure Mail 23.7.0 40

支持 Microsoft Exchange 累积更新 13 40

支持混合现代身份验证与本地Exchange 40

适用于 iOS 的 Secure Mail 23.7.0 40

支持混合现代身份验证与本地Exchange 40

深色模式 40

适用于 Android 的 Secure Mail 23.6.0 40

深色模式 40

适用于 iOS 的 Secure Mail 23.5.0 40

分屏视图和浮动窗口模式下的多任务处理 40

安全邮件 23.3.5 41

Secure Mail 适用于 Android 41

安全邮件 23.2.0 41

Secure Mail 适用于 Android 41

Secure Mail 适用于 iOS 41

安全邮件 22.11.0 41

Secure Mail 适用于 Android 41

安全邮件 22.9.0 41

Secure Mail 适用于 iOS 41

Secure Mail 适用于 Android 41

安全邮件 22.6.2 42

适用于 iOS 的 Secure Mail 42

安全邮件 22.6.0 42

适用于 iOS 的 Secure Mail 42

适用于 Android 的 Secure Mail 42

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 22.3.0 42
适用于 iOS 的 Secure Mail 42
适用于 Android 的 Secure Mail 42
安全邮件 22.2.0 42
适用于 iOS 的 Secure Mail 42
适用于 Android 的 Secure Mail 43
安全邮件 21.12.0 43
适用于 iOS 的 Secure Mail 43
适用于 Android 的 Secure Mail 43
安全邮件 21.11.0 43
适用于 Android 的 Secure Mail 43
安全邮件 21.10.5 48
适用于 iOS 的 Secure Mail 48
适用于 Android 的 Secure Mail 48
安全邮件 21.10.0 49
适用于 Android 的 Secure Mail 49
安全邮件 21.9.1 49
适用于 Android 的 Secure Mail 49
安全邮件 21.9.0 49
适用于 iOS 的 Secure Mail 49
适用于 Android 的 Secure Mail 49
安全邮件 21.8.5 49
适用于 Android 的 Secure Mail 49
安全邮件 21.8.0 49
适用于 iOS 的 Secure Mail 49
混合环境中基于电子邮件的 Exchange Server 自动发现 50
在运行 Microsoft Office 365 现代身份验证的设置上实现富推送通知 50
先决条件 51

© 1997–2026 Citrix Systems, Inc. All rights reserved.

限制 52
适用于 Android 的 Secure Mail 53
安全邮件 21.7.0 53
适用于 iOS 的 Secure Mail 53
适用于 Android 的 Secure Mail 53
安全邮件 21.6.0 53
适用于 iOS 的 Secure Mail 53
适用于 Android 的 Secure Mail 54
安全邮件 21.5.0 54
适用于 iOS 的 Secure Mail 54
适用于 Android 的 Secure Mail 55
安全邮件 21.4.5 55
适用于 Android 的 Secure Mail 55
安全邮件 21.4.0 55
适用于 iOS 的 Secure Mail 55
安全邮件 21.3.5 56
适用于 Android 的 Secure Mail 56
安全邮件 21.3.0 56
适用于 iOS 的 Secure Mail 56
适用于 Android 的 Secure Mail 56
安全邮件 21.2.0 56
适用于 iOS 的 Secure Mail 56
适用于 Android 的 Secure Mail 56
安全邮件 21.1.5 56
适用于 iOS 的 Secure Mail 56
安全邮件 21.1.0 57
安全邮件 20.12.0 57
适用于 iOS 的 Secure Mail 57

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 20.11.0 57
安全邮件 20.10.5 57
适用于 iOS 的 Secure Mail 57
适用于 Android 的 Secure Mail 57
安全邮件 20.10.0 57
适用于 iOS 的 Secure Mail 57
适用于 Android 的 Secure Mail 58
安全邮件 20.9.5 58
适用于 Android 的 Secure Mail 58
安全邮件 20.9.0 58
先决条件 58
升级后 59
安全邮件 20.8.5 59
适用于 Android 的 Secure Mail 59
安全邮件 20.8.0 60
适用于 Android 的 Secure Mail 60
适用于 iOS 的 Secure Mail 62
安全邮件 20.7.5 62
安全邮件 20.7.0 62
安全邮件 20.6.5 62
安全邮件 20.6.0 62
安全邮件 20.5.0 62
安全邮件 20.4.5 62
适用于 Android 的 Secure Mail 62
安全邮件 20.4.0 62
安全邮件 20.3.0 63
适用于 Android 的 Secure Mail 63
适用于 iOS 的 Secure Mail 63

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 20.2.0 63
适用于 Android 的 Secure Mail 63
最小化草稿 63
安全邮件 20.1.5 64
适用于 iOS 的 Secure Mail 64
适用于 Android 的 Secure Mail 64
安全邮件 20.1.0 64
安全邮件 19.12.5 64
适用于 iOS 的 Secure Mail 64
适用于 Android 的 Secure Mail 64
安全邮件 19.11.5 64
适用于 iOS 的 Secure Mail 64
适用于 Android 的 Secure Mail 65
适用于 iOS 的 Secure Mail 19.10.6 65
安全邮件 19.10.5 65
适用于 iOS 的 Secure Mail 65
适用于 Android 的 Secure Mail 65
安全邮件 19.10.0 65
运行 iOS 的设备 66
运行 Android 的设备 66
安全邮件 19.9.5 66
适用于 iOS 的 Secure Mail 66
适用于 Android 的 Secure Mail 66
安全邮件 19.9.0 67
适用于 iOS 的 Secure Mail 67
适用于 Android 的 Secure Mail 67
适用于 Android 的 Secure Mail 19.8.5 67
安全邮件 19.8.0 67

© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 iOS 的 Secure Mail 67
适用于 Android 的 Secure Mail 68
安全邮件 19.7.5 68
适用于 iOS 的 Secure Mail 68
适用于 Android 的 Secure Mail 68
安全邮件 19.6.5 69
Secure Mail 适用于 iOS 69
Secure Mail 适用于 Android 69
安全邮件 19.5.5 70
Secure Mail 适用于 Android 70
适用于 iOS 的 Secure Mail 70
安全邮件 19.5.0 70
适用于 Android 的 Secure Mail 70
适用于 Android 的 Secure Mail 19.4.6、19.4.5 和 19.3.5 72
安全邮件 19.3.0 72
适用于 iOS 的 Secure Mail 73
适用于 iOS 和 Android 的 Secure Mail 74
安全邮件 19.2.0 76
适用于 iOS 的 Secure Mail 76
适用于 Android 的 Secure Mail 76
适用于 iOS 的 Secure Mail 19.1.6 77
安全邮件 19.1.5 77
安全邮件 19.1.0 78
适用于 iOS 的 Secure Mail 78
适用于 Android 的 Secure Mail 79
安全邮件 18.12.0 79
安全邮件 18.11.5 79
适用于 Android 的 Secure Mail 79

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 18.11.1 81
安全邮件 18.11.0 81
适用于 Android 的安全邮件 81
适用于 iOS 的安全邮件 81
安全邮件 18.10.5 82
安全邮件 18.10.0 83
安全邮件 18.9.0 83
安全邮件 10.8.65 83
安全邮件 10.8.60 84
安全邮件 10.8.55 84
安全邮件 10.8.50 84
安全邮件 10.8.45 86
安全邮件 10.8.40 88
安全邮件 10.8.35 88
安全邮件 10.8.25 90
日历更改 97
联系人更改 97
附件更改 99
安全邮件 10.8.20 99
安全邮件 10.8.15 100
安全邮件 10.8.10 100
已知和已修复的问题 101
适用于 iOS 26.8.0 的 Secure Mail 101
已修复的问题 101
已知问题 101
适用于 Android 26.5.0 的 Secure Mail 101
已修复的问题 101
已知问题 101

© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 iOS 26.5.0 的 Secure Mail 102
已修复的问题 102
已知问题 102
适用于 iOS 26.1.0 的 Secure Mail 102
已修复的问题 102
已知问题 102
适用于 Android 的 Secure Mail 25.12.0 103
已修复的问题 103
已知问题 103
适用于 iOS 的 Secure Mail 25.9.0 103
已修复的问题 103
已知问题 103
适用于 Android 的 Secure Mail 25.8.0 103
已修复的问题 103
已知问题 104
适用于 Android 的 Secure Mail 25.6.0 104
已修复问题 104
已知问题 104
适用于 iOS 的 Secure Mail 25.5.0 104
已修复问题 104
已知问题 104
适用于 Android 的 Secure Mail 25.3.0 105
已修复问题 105
已知问题 105
适用于 Android 的 Secure Mail 25.1.0 105
已修复问题 105
已知问题 105
适用于 iOS 的 Secure Mail 25.1.0 105

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已修复问题 105
已知问题 105
适用于 iOS 的 Secure Mail 24.11.0 105
已修复问题 105
已知问题 105
适用于 Android 的 Secure Mail 24.11.0 106
已修复问题 106
已知问题 106
适用于 Android 的 Secure Mail 24.9.1 106
已修复的问题 106
已知问题 106
适用于 Android 的 Secure Mail 24.9.0 106
已修复的问题 106
已知问题 106
适用于 iOS 的 Secure Mail 24.9.0 107
已修复的问题 107
已知问题 107
适用于 Android 的 Secure Mail 24.7.0 107
已修复的问题 107
已知问题 107
适用于 iOS 的 Secure Mail 24.3.0 107
已修复的问题 107
已知问题 108
适用于 iOS 的 Secure Mail 24.2.0 108
已修复的问题 108
已知问题 108
适用于 Android 的 Secure Mail 24.1.0 108
已修复问题 108

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已知问题 108
适用于 Android 的 Secure Mail 23.10.0 109
已修复问题 109
已知问题 109
适用于 Android 的 Secure Mail 23.8.2 109
已修复的问题 109
已知问题 109
适用于 Android 和 iOS 的 Secure Mail 23.7.0 109
已修复的问题 109
已知问题 109
适用于 Android 的 Secure Mail 23.8.1 110
已修复的问题 110
已知问题 110
适用于 iOS 的 Secure Mail 23.9.0 110
已修复的问题 110
已知问题 110
适用于 Android 的 Secure Mail 23.8.0 110
已修复的问题 110
已知问题 110
适用于 Android 的 Secure Mail 23.7.0 110
已修复的问题 110
已知问题 110
适用于 Android 的 Secure Mail 23.6.0 111
已修复的问题 111
已知问题 111
适用于 iOS 的 Secure Mail 23.5.0 111
已修复的问题 111
已知问题 111

© 1997–2026 Citrix Systems, Inc. All rights reserved.

旧版本中的已知和已修复问题 111
Secure Mail 已知和已修复问题历史记录 112
安全邮件 23.3.5 112
适用于 Android 的 Secure Mail 中的已知问题 112
适用于 Android 的 Secure Mail 中的已修复问题 112
安全邮件 23.2.0 112
适用于 iOS 和 Android 的 Secure Mail 中的已知问题 112
适用于 Android 的 Secure Mail 中的已修复问题 112
Secure Mail for iOS 中已修复的问题 113
安全邮件 22.11.0 113
Secure Mail for Android 中的已知问题 113
Secure Mail for Android 中已修复的问题 113
安全邮件 22.9.0 113
iOS 和 Android 版 Secure Mail 中的已知问题 113
iOS 和 Android 版 Secure Mail 中已修复的问题 113
安全邮件 22.6.2 113
iOS 版 Secure Mail 中的已知问题 113
iOS 版 Secure Mail 中已修复的问题 114
安全邮件 22.6.0 114
iOS 版 Secure Mail 中的已知问题 114
iOS 版 Secure Mail 中已修复的问题 114
安全邮件 22.3.0 114
Secure Mail 22.3.0 中的已知问题 114
Secure Mail 22.3.0 中已修复的问题 114
安全邮件 22.2.0 114
Secure Mail 22.2.0 中的已知问题 114
Secure Mail 22.2.0 中已修复的问题 114
安全邮件 21.12.0 115

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已修复的问题 115
安全邮件 21.11.0 115
安全邮件 21.10.5 115
适用于 Android 的 Secure Mail 中已修复的问题 115
适用于 Android 的 Secure Mail 中的已知问题 115
安全邮件 21.10.0 115
适用于 Android 的 Secure Mail 中的已知问题 115
适用于 Android 的 Secure Mail 中已修复的问题 115
安全邮件 21.9.1 116
适用于 Android 的 Secure Mail 中的已知问题 116
适用于 Android 的 Secure Mail 中已修复的问题 116
安全邮件 21.9.0 116
安全邮件 21.8.5 116
已知问题 116
已修复的问题 116
安全邮件 21.8.0 116
已知问题 116
已修复的问题 117
安全邮件 21.7.0 117
已知问题 117
已修复的问题 117
安全邮件 21.6.0 117
安全邮件 21.5.0 117
安全邮件 21.4.5 117
安全邮件 21.4.0 117
安全邮件 21.3.5 117
安全邮件 21.3.0 118
安全邮件 21.2.0 118

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已知问题 118
已修复的问题 118
安全邮件 21.1.5 118
适用于 iOS 的 Secure Mail 118
安全邮件 21.1.0 118
已知问题 118
已修复的问题 118
安全邮件 20.12.0 118
适用于 iOS 的 Secure Mail 118
安全邮件 20.11.0 118
安全邮件 20.10.5 119
已知问题 119
已修复的问题 119
安全邮件 20.10.0 119
已知问题 119
已修复的问题 119
安全邮件 20.9.5 119
适用于 Android 的 Secure Mail 119
安全邮件 20.9.0 119
已知问题 119
已修复的问题 119
安全邮件 20.8.5 119
适用于 Android 的 Secure Mail 119
已知问题 120
已修复的问题 120
安全邮件 20.8.0 120
安全邮件 20.7.5 120
安全邮件 20.7.0 120

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 20.6.5 120
已知问题 120
已修复的问题 120
安全邮件 20.6.0 120
已知问题 120
已修复的问题 120
安全邮件 20.5.0 121
适用于 iOS 的 Secure Mail 121
已知问题 121
已修复的问题 121
安全邮件 20.4.5 121
已知问题 121
已修复问题 121
安全邮件 20.4.0 121
已知问题 121
已修复问题 121
安全邮件 20.3.0 122
安全邮件 20.2.0 122
安全邮件 20.1.5 122
已知问题 122
已修复问题 122
安全邮件 20.1.0 122
已知问题 122
已修复的问题 122
安全邮件 19.12.5 122
已知问题 122
已修复的问题 123
安全邮件 19.11.5 123

© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 iOS 的 Secure Mail 19.10.6 123
适用于 iOS 的 Secure Mail 中的已知问题 123
适用于 iOS 的 Secure Mail 中已修复的问题 123
安全邮件 19.10.5 123
已知问题 123
已修复问题 123
安全邮件 19.10.0 123
安全邮件 19.9.5 123
已知问题 123
已修复问题 124
安全邮件 19.9.0 124
已知问题 124
已修复问题 124
安全邮件 19.8.5 124
Android 版 Secure Mail 中的已知问题 124
Android 版 Secure Mail 中的已修复问题 124
安全邮件 19.8.0 125
已知问题 125
已修复问题 125
安全邮件 19.7.5 125
已知问题 125
已修复问题 125
安全邮件 19.6.5 125
已知问题 125
已修复的问题 125
安全邮件 19.5.5 126
已知问题 126
已修复的问题 126

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 19.5.0 126
已知问题 126
已修复的问题 126
适用于 Android 的 Secure Mail 19.4.6 126
适用于 Android 的 Secure Mail 中的已知和已修复问题 126
安全邮件 19.4.5 126
已知问题 126
已修复问题 127
安全邮件 19.3.5 127
已知问题 127
已修复问题 127
安全邮件 19.3.0 127
已知问题 127
已修复问题 127
安全邮件 19.2.0 128
已知问题 128
已修复问题 128
适用于 iOS 的 Secure Mail 19.1.6 128
适用于 iOS 的 Secure Mail 中的已知和已修复问题 128
安全邮件 19.1.5 128
已知问题 128
已修复问题 128
安全邮件 19.1.0 129
已知问题 129
已修复的问题 129
安全邮件 18.12.0 129
已修复的问题 129
安全邮件 18.11.1 130

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已修复的问题 130
已知问题 130
安全邮件 18.10.5 130
已修复的问题 130
安全邮件 18.10.0 130
已修复的问题 130
安全邮件 18.9.0 131
已修复的问题 131
安全邮件 10.8.65 131
已修复问题 131
安全邮件 10.8.60 131
已修复问题 131
安全邮件 10.8.55 132
已修复问题 132
版本 10.8.55 中 MDX 相关的已修复问题 132
安全邮件 10.8.50 132
已修复的问题 132
安全邮件 10.8.45 132
已修复的问题 132
安全邮件 10.8.40 132
已修复的问题 132
安全邮件 10.8.35 132
已修复的问题 132
安全邮件 10.8.25 133
已修复的问题 133
安全邮件 10.8.20 133
已修复的问题 133
安全邮件 10.8.10 134

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已修复的问题 134
Secure Mail 适用于 Android 和 iOS - 预览 135
功能标志管理 136
部署 Secure Mail 137
配置 Secure Mail 139
与 Microsoft Office 365 的现代身份验证 139
Citrix Endpoint Management™ 策略先决条件 140
Exchange Server 配置选项 141
使用 `outlook.office365.com` 进行配置 141
使用 Microsoft 统一域 `outlook.cloud.microsoft` 进行配置 141
限制 142
Secure Mail 策略 142
支持 OAuth 的 Secure Mail 兼容性列表 143
适用于 iOS 和 Android 的本地 Exchange 混合现代身份验证支持 143
MDX 策略中所需的更改 143
限制 146
Secure Mail 的后台服务 146
配置 Secure Mail 的后台服务 146
用于后台服务配置的 MDX 应用程序策略 147
直接连接到邮件服务器 149
通过 STA 连接到邮件服务器 150
集成 Exchange 服务器 或 IBM Notes Traveler 服务器 150
为安全邮件配置 IBM Notes Traveler Server 151
系统要求 152
基础架构服务器要求 152
身份验证协议 152
端口要求 152

© 1997–2026 Citrix Systems, Inc. All rights reserved.

配置 SSL/TLS 安全级别 153
配置 Notes Traveler 服务器 154
安全邮件的 S/MIME 154
与数字身份提供程序集成 155
先决条件 156
配置集成 156
使用派生凭据 156
通过电子邮件分发证书 157
先决条件 157
为微软证书服务启用 Web 注册 157
验证 IIS 中的身份验证设置 158
创建新证书模板 158
请求用户证书 162
验证已发布的证书 164
导出用户证书 165
通过电子邮件发送证书 165
在适用于 iOS 和 Android 的 Secure Mail 上启用 S/MIME 165
使用单独的签名和加密证书启用 S/MIME 166
使用单个签名和加密证书启用 S/MIME 170
在 iOS 和 Android 上测试 S/MIME 174
配置公共证书源 178
Secure Mail 的单点登录 178
启用 Secure Mail 中的自动注册 178
配置 Secure Mail 应用程序策略 179
具有自动预配功能的端到端 Secure Mail SSO 用户体验 179
故障排除 180
安全注意事项 181
支持 Microsoft IRM 和 AIP 电子邮件权限保护 181

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 Secure Mail 中启用信息权限管理 181
当您收到受权限保护的电子邮件时 182
撰写受权限保护的电子邮件时 183
电子邮件安全分类 186
iOS 数据保护 189
更改启用 iOS 数据保护策略 189
澳大利亚信号局数据保护 189
模糊屏幕内容 190
iOS 功能 194
支持将 Secure Mail 设置为默认邮件应用程序 194
在 Secure Mail 日历事件中创建 Microsoft Teams 会议 194
最小化草稿 196
使用 MIME 标头报告网络钓鱼电子邮件 196
支持 WkWebView 196
支持 Slack EMM 196
分组通知 196
通知响应选项 196
富推送通知失败消息的增强功能 197
支持 Microsoft 设置上的富推送通知 197
支持 S/MIME 派生凭据 198
富文本签名 198
添加富文本签名 199
Secure Mail 来电显示 199
在日历中设置颜色 199
从“文件”应用附加文件 200
拼写检查功能 200
邮箱屏幕 201
个人账户 202

© 1997–2026 Citrix Systems, Inc. All rights reserved.

日历 202
设置日历事件的颜色 202
搜索 203
在 iOS 上打印电子邮件、日历事件或内联图像 203
先决条件 203
打印电子邮件 203
打印日历事件 210
多个会议代码（拨入会议） 212
拨入会议 213
支持打印电子邮件附件 213
Android 功能 214
在 Secure Mail 日历事件中创建 Microsoft Teams 会议 214
双向联系人同步 215
撤消已发送邮件 216
草稿文件夹中的附件同步 216
PDF 文件的应用内查看 216
将 Web SSO 用于隧道策略，适用于使用 Microsoft Office 365 运行现代身份验证的设置 216
拖放日历事件 216
支持 Google Play 的 64 位应用程序 216
改进了适用于 Android 的 Secure Mail 中的“下拉刷新”UI 216
日历议程小组件 217
网络访问策略 217
Feed 卡增强功能 217
查看附件 218
打印电子邮件和日历事件 218
先决条件 218
打印电子邮件 218
打印内联图像 221

© 1997–2026 Citrix Systems, Inc. All rights reserved.

打印日历事件 221

报告带有 ActiveSync 标头的网络钓鱼电子邮件 223

子文件夹通知 223

启用子文件夹通知 224

通知渠道 226

电子邮件中的会议响应按钮 229

附件增强功能 230

返回按钮增强功能 230

在 Android 中启用从图库附加文件的管理员步骤 230

支持的文件格式 231

日历 234

设置日历事件的颜色 234

搜索 238

后台服务更新 238

Secure Mail 中的 Android 企业版 239

先决条件 239

与 Android Enterprise 兼容的功能 239

限制 241

Secure Mail 的 iOS 和 Android 功能 242

支持 Azure 政府云计算 242

先决条件 242

升级后 243

支持 ICS 文件 243

Secure Mail 中的联系人图片 243

管理您的动态 243

使用 Office 365 Exchange Server 策略定义 Office 365 服务器地址 244

支持加密管理 244

运行 iOS 的设备 244

© 1997–2026 Citrix Systems, Inc. All rights reserved.

运行 Android 的设备 245
支持响应式电子邮件 245
拖放日历事件 245
管理您的源 245
自动前进 245
草稿文件夹自动同步 246
在 MDM + MAM 模式下使用 Microsoft Intune 时支持单点登录 246
联系人功能增强 246
先决条件 247
将会议时间和地点导出到您的本机日历 247
多个 Exchange 帐户 247
联系人 247
在日历中设置颜色 247
内部域 248
人机工程学改进 251
Secure Mail 与 Slack 集成（预览版） 252
报告网络钓鱼电子邮件（作为转发） 252
报告网络钓鱼电子邮件 252
导出 Secure Mail 日历事件 252
适用于 iOS 253
适用于 Android 254
源文件夹 254
查看源卡片 254
信息流文件夹的增强功能 255
来自您经理的信息流 256
从日历加入会议 257
支持的会议类型 258
Microsoft Teams 应用程序 259

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Zoom 应用程序 259
Webex（未封装的应用程序） 259
商务版 Skype 259
斯凯普 259
拨入规范 259
Skype 企业版 260
通用音频会议信息 261
个人日历叠加 264
插入内联图像 264
滑动操作 267
在 iOS 和 Android 上加入 Skype for Business 会议 267
加入 Skype for Business 会议 267
附件的应用内预览及其他附件增强功能 268
选择要附加文件的邮件 268
保存附件以供离线访问 272
从离线文件中删除附件 273
使用其他应用程序打开附件 274
查看附件的源电子邮件或日历事件 276
将用户名迁移到电子邮件地址 (UPN) 276
先决条件 277
迁移到基于 UPN 的身份验证 277
验证迁移 277
个人通讯组列表 277
先决条件 277
查看个人通讯组列表 278
向联系人组撰写邮件 278
向联系人组发送日历邀请 278
文件夹同步 279

© 1997–2026 Citrix Systems, Inc. All rights reserved.

同步您的文件夹 279
照片附件改进 281
将照片附加到电子邮件 281
Secure Mail 在查看电子邮件时呈现嵌入式资源 282
支持现代身份验证 282
允许 Secure Web 域 MDX 策略用于 Secure Mail 282
Secure Web 域策略的配置示例 283
适用于 Android 版 Secure Mail 283
适用于 iOS 版 Secure Mail 283
Secure Mail 与 Slack 集成 284
先决条件 284
在您的设备上启用此功能 284
使用此功能 290
通知和同步 296
适用于 iOS 的 Secure Mail 后台应用刷新 296
安全邮件和 ActiveSync 296
iOS 296
安卓 297
在 Secure Mail 中导出联系人 297
Secure Mail 通知 298
适用于 Secure Mail 的推送通知 298
推送通知的工作原理 298
适用于推送通知的系统要求 299
为 Secure Mail 配置推送通知 299
Exchange 服务器配置 300
Citrix 网关配置 301
故障排除 302
Secure Mail 推送通知常见问题解答 302

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Android 何时向 Secure Mail 传送通知? 302
FCM 如何影响显示在锁定屏幕上的电子邮件通知? 302
APNs 如何影响显示在锁定屏幕上的电子邮件通知? 302
后台应用刷新如何影响 Secure Mail 和 APNs? 302
低电量模式如何影响 Secure Mail 和 APNs? 303
还有哪些其他问题可能导致 FCM 驱动的后台同步失败? 303
还有哪些其他问题可能导致 APNs 驱动的后台同步失败? 303
当通知未送达或未使用 APNs 时，Secure Mail 还会如何生成锁屏通知? 303
Secure Mail 与其他在锁屏上显示内容的应用程序有何不同? 304
适用于 iOS 版 Secure Mail 的富推送通知 305
推送通知在 Secure Mail iOS 中的工作方式 306
不支持富推送通知时的推送通知行为 306
Secure Mail iOS 推送通知常见问题 306
iOS 设备上出现“您有新邮件”通知的原因 307
Secure Mail for iOS 中的推送通知失败消息 309
Secure Mail 与其他移动生产力应用和 Citrix Files 的交互性 309
测试和故障排除 Secure Mail 310
测试 ActiveSync 连接、用户身份验证和 APNs 配置 310
测试先决条件 310
使用 Secure Mail 日志排查连接问题 311
如何从设备获取适用于 iOS 的 Secure Mail 崩溃日志 313
电子邮件、联系人或日历问题疑难解答 313
无限同步最佳实践 313

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure Mail 概述

Citrix Secure Mail™ 允许用户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。为了保持与 Microsoft Outlook 或 IBM Notes 帐户的连续性，Secure Mail 与 Microsoft Exchange Server 和 IBM Notes Traveler Server 同步。

作为 Citrix 应用程序套件的一部分，Secure Mail 受益于与 Citrix Secure Hub 的单点登录 (SSO) 兼容性。用户登录 Secure Hub 后，他们可以无缝地进入 Secure Mail，而无需重新输入其用户名和密码。您可以配置 Secure Mail，使其在设备注册 Secure Hub 时自动推送到用户的设备，或者用户可以从应用商店添加该应用程序。

注意：

- 对 Exchange Server 2010 的支持已于 October 13, 2020 结束。
- 对 Exchange Server 2013 的支持已于 April 11, 2023 结束。

Secure Mail 兼容以下版本：

- Exchange 服务器 SE RTM
- Exchange Server 2019 累积更新 15
- Exchange Server 2019 累积更新 14
- Exchange Server 2019 累积更新 13
- Exchange Server 2019 累积更新 12
- Exchange Server 2019 累积更新 11
- Exchange Server 2019 累积更新 10
- Exchange Server 2019 累积更新 9
- Exchange Server 2019 累积更新 8
- Exchange Server 2019 累积更新 7
- Exchange Server 2019 累积更新 6
- Exchange Server 2016 累积更新 23

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Exchange Server 2016 累积更新 22
- Exchange Server 2016 累积更新 21
- Exchange Server 2016 累积更新 20
- Exchange Server 2016 累积更新 19
- Exchange Server 2016 累积更新 18
- Exchange Server 2016 累积更新 17
- HCL Domino 版本 14.0 FP1
- HCL Domino 版本 12.0.2 FP2
- HCL Traveler 版本 12.0.2.1 构建 202302010413_30
- HCL Domino 11 （前身为 Lotus Notes）
- HCL Domino 10.0.1 （前身为 Lotus Notes）
- HCL Domino 9.0.1 FP10 HF197（以前称为 Lotus Notes）
- HCL Domino 10.0.1.0 构建版本 201811191126_20（以前称为 Lotus Notes）
- HCL Domino 9.0.1.21（以前称为 Lotus Notes）
- 微软 Office 365 (Exchange 在线)

首先，从 Citrix Endpoint Management 下载 下载 Secure Mail 和其他 Endpoint Management 组件。

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

有关 Secure Mail 适用于 iOS 和 Android 的通知（当应用程序在后台运行或关闭时）的信息，请参阅 Secure Mail 的推送通知。

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

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

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

有关用户帮助文档，请参阅 Citrix 用户帮助中心中的 Citrix Secure Mail 页面。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure Mail 中的新增功能

以下部分列出了 Secure Mail 当前版本和早期版本中的新增功能。

有关用户帮助文档，请参阅 Citrix 用户帮助中心中的 Citrix Secure Mail 页面。

注意：

- 截至 2023 年 9 月，Secure Mail 不支持 Android 7.x 和 iOS 12.x。
- 自 Android 25.6.0 版和 iOS 25.5.0 版起，Secure Mail 不支持 Intune。

当前版本中的新增功能

适用于 iOS 的 Secure Mail 26.8.0

支持 iOS/iPadOS 27

从适用于 iOS 的 Secure Mail 26.8.0 版本开始，该应用程序与 iOS/iPadOS 27 兼容。您可以将设备升级到 iOS/iPadOS 27 并继续使用最新版本的 Secure Mail。

支持将 Secure Mail 设置为默认邮件应用程序

从适用于 iOS 的 Secure Mail 26.8.0 版本开始，您可以将 Secure Mail 设置为设备上的默认邮件应用程序。将其设置为默认应用程序后，在“通讯录”、“Safari”或任何其他应用程序中点击 `mailto:` 链接会在 Secure Mail 中打开新草稿，而不是在原生邮件应用程序中打开。因此，您的商务电子邮件将保留在受管容器中。

要将 Secure Mail 设置为默认邮件应用程序，请参阅 支持将 Secure Mail 设置为默认邮件应用程序。

有关错误修复的更多信息，请参阅 已知和已修复问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

早期版本中的新增功能

适用于 Android 的 Secure Mail 26.5.0

支持 Android 17

从适用于 Android 的 Secure Mail 26.5.0 版本开始，该应用兼容 Android 17。您可以将设备升级到 Android 17 并继续使用最新版本的 Secure Mail。

有关错误修复的更多信息，请参阅已知和已修复问题。

适用于 iOS 的 Secure Mail 26.5.0

此版本解决了一些问题，有助于提高整体性能和稳定性。

有关错误修复的更多信息，请参阅已知和已修复问题。

适用于 iOS 的 Secure Mail 26.1.0

支持移动响应式电子邮件格式

从适用于 iOS 的 Secure Mail 26.1.0 版本开始，该应用支持改进的移动响应式电子邮件格式。

有关错误修复的更多信息，请参阅已知和已修复问题。

适用于 Android 的 Secure Mail 25.12.0

支持 16KB 内存页大小

从适用于 Android 的 Secure Mail 25.12.0 版本开始，该应用支持 16KB 内存页大小，以优化性能并符合 Google Play 要求。

有关错误修复的更多信息，请参阅已知和已修复问题。

适用于 iOS 的 Secure Mail 25.9.0

支持联系人双向同步

从适用于 iOS 的 Secure Mail 25.9.0 版本开始，该应用支持在 Secure Mail iOS 应用与设备的联系人系统之间双向同步联系人。升级到 Secure Mail 25.9.0 版本可确保联系人同步的持续支持和兼容性，与现有 Android 实现保持一致。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

- 此功能默认禁用，管理员必须联系 Citrix 客户支持以启用此功能。
- 此功能受 iCloud 联系人同步影响，这会导致数据冲突。如果遇到任何问题，请禁用 iCloud 联系人同步。

iOS 15 弃用

从适用于 iOS 的 Secure Mail 25.9.0 版本开始，对 iOS 15 的支持已弃用，并且该应用不支持运行 iOS 15 的设备。作为替代方案，您可以升级到最新可用版本的 iOS。

有关错误修复的更多信息，请参阅已知和已修复问题。

适用于 Android 的 Secure Mail 25.8.0

支持 Android API 级别 35

从适用于 Android 的 Secure Mail 25.8.0 版本开始，该应用支持 Android API 级别 35，以符合 Google Play 应用更新要求。

有关错误修复的更多信息，请参阅已知和已修复问题。

适用于 Android 的 Secure Mail 25.6.0

旧版 MDX 弃用

从 Secure Mail 25.6.0 for Android 版本开始，该应用始终使用 MAM SDK 策略容器模式，并且不支持与 Intune 集成。要了解有关限制的更多信息，请参阅限制。

有关错误修复的更多信息，请参阅已知问题和已修复问题。

适用于 iOS 的 Secure Mail 25.5.0

支持 iOS 26

从适用于 iOS 的 Secure Mail 25.5.0 版本开始，该应用支持运行 iOS 26 的设备。升级到 Secure Mail 25.5.0 版本可确保对已更新到 iOS 26 的设备提供持续支持和兼容性。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

支持 TLS 1.3 协议

从适用于 iOS 的 Secure Mail 25.5.0 版本开始，该应用在 iOS 设备上支持 TLS 1.3 协议。TLS 1.3 是 TLS 协议的最新版本，与 TLS 1.2 相比，它提供更快的性能、增强的安全性以及更强的抵御网络攻击的能力。TLS 1.3 还可以减少网络延迟，从而实现更快的 HTTPS 连接和更好的用户体验。

要了解有关 TLS 1.3 的更多信息，请参阅传输层安全 (TLS) 协议版本 1.3。

注意：

此功能默认处于禁用状态，管理员必须联系 Citrix 客户支持才能启用此功能。

支持 Domino 14 FP1

从适用于 iOS 的 Secure Mail 25.5.0 版本开始，该应用支持 HCL Domino 14.0 FP1 版。

旧版 MDX 弃用

从适用于 iOS 的 Secure Mail 25.5.0 版本开始，该应用始终使用 MAM SDK 策略容器模式，并且不支持与 Intune 集成。要了解有关限制的更多信息，请参阅限制。

有关错误修复的更多信息，请参阅已知问题和已修复问题。

适用于 Android 的 Secure Mail 25.3.0

支持 Android 16

从 Secure Mail 25.3.0 for Android 版本开始，该应用程序与 Android 16 兼容。您可以将设备升级到 Android 16 并继续使用最新版本的 Secure Mail。

支持下载大型附件

从 Secure Mail 25.3.0 for Android 版本开始，该应用程序支持下载大于 10MB 的附件。

注意：

此功能默认禁用，管理员必须联系 Citrix 客户支持才能启用此功能。

有关错误修复的更多信息，请参阅已知和已修复问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 Android 的 Secure Mail 25.1.0

支持 TLS 1.3 协议

从 Secure Mail 25.1.0 for Android 版本开始，该应用程序在 Android 设备上支持 TLS 1.3 协议。TLS 1.3 是 TLS 协议的最新版本，与 TLS 1.2 相比，它提供更快的性能、增强的安全性以及更强的抵御网络攻击的能力。TLS 1.3 还减少了网络延迟，从而实现更快的 HTTPS 连接和更好的用户体验。

要了解有关 TLS 1.3 的更多信息，请参阅传输层安全 (TLS) 协议版本 1.3。

有关错误修复的更多信息，请参阅已知和已修复问题。

适用于 iOS 的 Secure Mail 25.1.0

支持下载大型附件

从适用于 iOS 的 Secure Mail 25.1.0 版本开始，该应用支持下载大于 10MB 的附件。

注意：

此功能默认禁用，管理员必须联系 Citrix 客户支持才能启用此功能。

有关错误修复的更多信息，请参阅已知问题和已修复问题。

适用于 Android 的 Secure Mail 24.11.0

查看不带水印的电子邮件附件

如果您使用的是适用于 Android 的 Secure Mail 24.9.1 或更早版本，则在查看电子邮件附件时可能会看到水印。要查看不带水印的电子邮件附件，请升级到适用于 Android 的 Secure Mail 24.11.0 或更高版本。

有关错误修复的更多信息，请参阅已知问题和已修复问题。

适用于 iOS 的 Secure Mail 24.11.0

此版本解决了可提高整体性能和稳定性的方面。

有关错误修复的更多信息，请参阅已知问题和已修复问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 iOS 的 Secure Mail 24.9.0

支持 iOS 18

从适用于 iOS 的 Secure Mail 24.9.0 版本开始，Secure Mail 支持运行 iOS 18 或更高版本的设备。升级到 Secure Mail 24.9.0 版本可确保对已更新到 iOS 18 的设备提供持续支持和兼容性。

有关错误修复的更多信息，请参阅已知问题和已修复问题。

适用于 Android 的 Secure Mail 24.9.1

支持 Android 15

将 Secure Mail 版本升级到 24.9.1 可确保持续支持已更新到 Android 15 的设备。

有关错误修复的更多信息，请参阅已知和已修复问题。

适用于 Android 的 Secure Mail 24.9.0

支持 API 级别 34

Secure Mail 支持 Google Play 当前的目标 API 要求，即 API 级别 34。

有关错误修复的更多信息，请参阅已知和已修复问题。

适用于 Android 的 Secure Mail 24.7.0

此版本解决了可提高整体性能和稳定性的方面。

适用于 iOS 的 Secure Mail 24.3.0

此版本解决了可提高整体性能和稳定性的方面。

适用于 iOS 的 Secure Mail 24.2.0

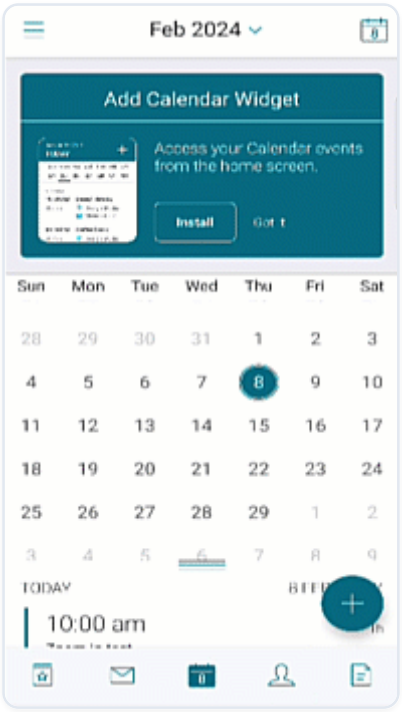
此版本解决了可提高整体性能和稳定性的方面。

适用于 Android 的 Secure Mail 24.1.0

支持日历事件的放大功能

从 24.1.0 版本开始，适用于 Android 的 Secure Mail 支持日历事件的放大功能。此功能默认启用。现在，放大功能适用于邮件和日历事件。增强的放大功能提供了更好的用户体验。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



适用于 iOS 的 Secure Mail 23.9.0

支持 iOS 17

从此版本开始，Secure Mail 支持运行 iOS 17 的设备。升级到 Secure Mail 23.9.0 版本可确保持续支持已更新到 iOS 17 的设备。

支持 HCL Domino 12

从此版本开始，适用于 Android 和 iOS 的 Secure Mail 支持 HCL Domino 12.0.2 FP2 版本和 HCL Traveler 12.0.2.1 Build 202302010413_30 版本。

注意：

如果您从 HCL Domino 11 升级到 HCL Domino 12，请务必更新 Domino 服务器中 **notes.ini** 文件中的以下用户代理。这可确保 Secure Mail 中的所有 ActiveSync 16.1 功能（例如草稿同步和日历附件）继续正常运行。有关详细信息，请参阅如何为 HCL Traveler Exchange ActiveSync 16.1 支持启用 Citrix Secure Mail 客户端。

```
NTS_DEVICE_TYPE_USER_AGENT_APPLE=(\^Apple-(iPhone|iPod|iPad|Touchdown))|(\^Mozilla.(iPhone|iPod|iPad))|(\^WorxMail.(iPhone|iPod|iPad))
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 Android 的 Secure Mail 23.8.2

查看没有水印的电子邮件附件

如果您使用的是 Secure Mail for Android 23.8.1 或更早版本，则在查看电子邮件附件时会看到水印。要查看没有水印的电子邮件附件，请升级到 Secure Mail for Android 23.8.2 或更高版本。

注意：

在 October 31, 2023 之后，升级到 23.8.1 版本无法解决电子邮件附件中的水印问题。因此，建议更新到 23.8.2 版本。

适用于 Android 的 Secure Mail 23.8.1

查看无水印的电子邮件附件

如果您使用的是 Secure Mail for Android 23.8.0 或更早版本，查看电子邮件附件时可能会看到水印。要查看无水印的电子邮件附件，请升级到 Secure Mail for Android 23.8.1 或更高版本。

支持 HCL Domino 12

从本版本开始，适用于 Android 和 iOS 的 Secure Mail 支持 HCL Domino 12.0.2 FP2 版本和 HCL Traveler 12.0.2.1 Build 202302010413_30 版本。

注意：

如果您从 HCL Domino 11 升级到 HCL Domino 12，请务必更新 Domino 服务器中 **notes.ini** 文件中的以下用户代理。这可确保 Secure Mail 中的所有 ActiveSync 16.1 功能（例如草稿同步和日历附件）继续正常运行。有关详细信息，请参阅如何为 HCL Traveler Exchange ActiveSync 16.1 支持启用 Citrix Secure Mail 客户端。

```
NTS_DEVICE_TYPE_USER_AGENT_APPLE=(\^Apple-(iPhone|iPod|iPad|Touchdown))|(\^Mozilla.(iPhone|iPod|iPad))|(\^WorxMail.(iPhone|iPod|iPad))
```

适用于 Android 的 Secure Mail 23.8.0

支持 Android 14

从本版本开始，Secure Mail 支持运行 Android 14 的设备。升级到 Secure Mail 23.8.0 版本可确保持续支持已更新到 Android 14 的设备。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 Android 的 Secure Mail 23.7.0

支持 Microsoft Exchange 累积更新 13

从 23.7.0 版本开始，Secure Mail 支持 Microsoft Exchange Server 2019 累积更新 13。

支持混合现代身份验证与本地Exchange

Secure Mail 现在支持混合现代身份验证 (HMA)，适用于 Exchange Server 2016 的累积更新 8 和 Exchange Server 2013 的累积更新 19。

适用于 iOS 的 Secure Mail 23.7.0

支持混合现代身份验证与本地Exchange

Secure Mail 现在支持混合现代身份验证 (HMA)，适用于 Exchange Server 2016 的累积更新 8 和 Exchange Server 2013 的累积更新 19。

深色模式

从 23.7.0 版本开始，Secure Mail 支持深色模式。要在深色模式下查看电子邮件，请转到应用程序**设置** > **应用程序主题** > 并选择**深色模式**。

适用于 Android 的 Secure Mail 23.6.0

深色模式

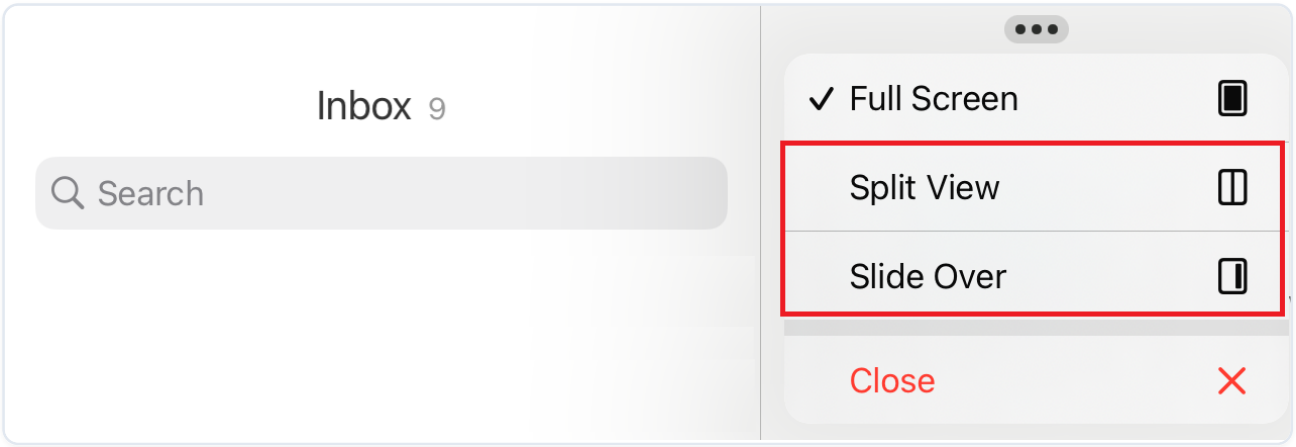
从 23.6.0 版本开始，Secure Mail 支持深色模式。要在深色模式下查看电子邮件，请转到应用程序**设置** > **应用程序主题** > 并选择**深色模式**。

适用于 iOS 的 Secure Mail 23.5.0

分屏视图和浮动窗口模式下的多任务处理

从 23.5.0 版本开始，Secure Mail 支持 iPad 设备上的多任务处理。打开 Secure Mail 并点击省略号 (…) 以选择**分屏视图**或**浮动窗口**选项进行多任务处理。此功能可帮助用户保持高效工作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



在**分屏视图**中，第二个应用程序显示在当前应用程序旁边。在**浮动窗口**布局中，第二个应用程序以全屏模式打开，而当前应用程序会缩小到一个较小的窗口，您可以将其移动到屏幕的右侧或左侧。

安全邮件 23.3.5

Secure Mail 适用于 Android

此版本包含错误修复。

安全邮件 23.2.0

Secure Mail 适用于 Android

此版本包含错误修复。

Secure Mail 适用于 iOS

此版本包含错误修复。

安全邮件 22.11.0

Secure Mail 适用于 Android

此版本包含错误修复。

安全邮件 22.9.0

Secure Mail 适用于 iOS

Secure Mail 现在支持 iOS 16。

Secure Mail 适用于 Android

Secure Mail 现已支持 Android 13。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 22.6.2

适用于 iOS 的 Secure Mail

此版本包含错误修复。

安全邮件 22.6.0

从此版本开始，Secure Mail 支持 Exchange Server 2016 累积更新 23。

适用于 iOS 的 Secure Mail

此版本包含错误修复。

适用于 Android 的 Secure Mail

此版本包含错误修复。

安全邮件 22.3.0

适用于 iOS 的 Secure Mail

支持 HCL Domino 11。从此版本开始，适用于 iOS 的 Secure Mail 支持 HCL Domino 11（以前称为 Lotus Notes）。

Google Analytics。Citrix Secure Mail 使用 Google Analytics 收集应用程序统计信息和使用信息分析数据，以提高产品质量。Citrix 不会收集或存储任何其他个人用户信息。有关禁用 Secure Mail 的 Google Analytics 的详细信息，请参阅禁用 Google Analytics

适用于 Android 的 Secure Mail

支持 HCL Domino 11。从本版本开始，适用于 Android 的 Secure Mail 支持 HCL Domino 11（以前称为 Lotus Notes）。

Google Analytics。Citrix Secure Mail 使用 Google Analytics 收集应用程序统计信息和使用情况分析数据，以提高产品质量。Citrix 不会收集或存储任何其他个人用户信息。有关禁用 Secure Mail 的 Google Analytics 的更多信息，请参阅禁用 Google Analytics

安全邮件 22.2.0

适用于 iOS 的 Secure Mail

在版本 21.5.0 中，管理您的源的选项已弃用。在此版本中，适用于 iOS 的 Secure Mail 中仅显示以下默认源卡片：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 未读
- 会议邀请
- 即将召开的会议
- 来自您的经理

如果您当前已启用并配置此功能，则首选项将被默认卡片覆盖。

适用于 Android 的 Secure Mail

在版本 21.5.0 中，管理您的源的选项已弃用。在此版本中，适用于 iOS 的 Secure Mail 中仅显示以下默认源卡片：

- 未读
- 会议邀请
- 即将召开的会议
- 来自您的经理

如果您当前已启用并配置此功能，则首选项将被默认卡片覆盖。

安全邮件 21.12.0

适用于 iOS 的 Secure Mail

支持自定义用户代理。 从此版本开始，您可以使用自定义用户代理通过 Microsoft Office 365 对 Active Directory 联合身份验证服务 (AD FS) 或身份提供程序 (IdP) 进行身份验证。要使用此功能，您必须在 Citrix Endpoint Management™ 控制台中启用并配置**用于现代身份验证的自定义用户代理**策略。

适用于 Android 的 Secure Mail

此版本包含错误修复。

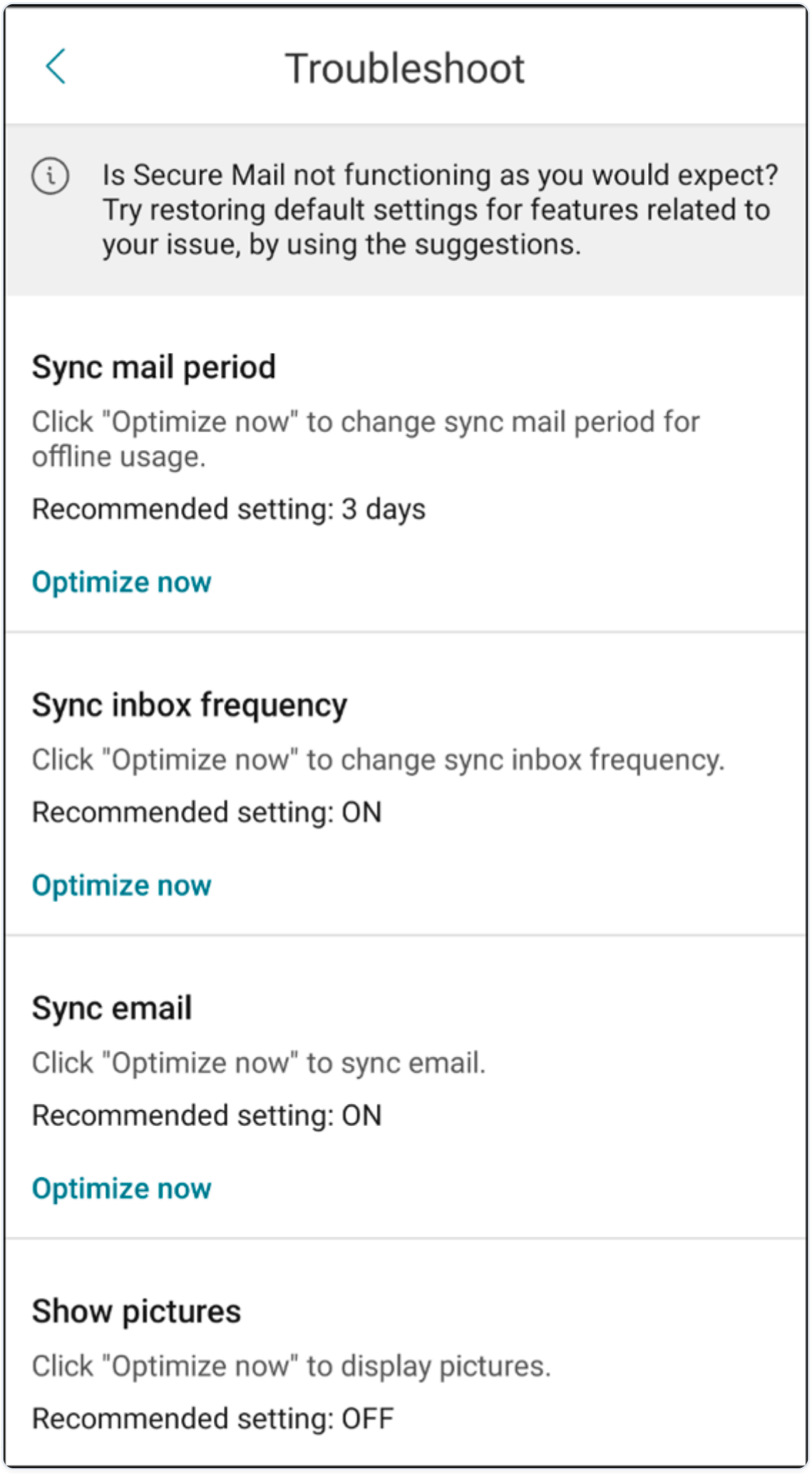
安全邮件 21.11.0

适用于 Android 的 Secure Mail

自诊断工具

您现在可以解决在使用适用于 Android 的 Secure Mail 时可能遇到的任何问题。在应用程序设置中，使用**支持**菜单选项下的**故障排除**按钮。要解决问题，请打开 Secure Mail 并导航至**设置** > **故障排除**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.


Troubleshoot
Is Secure Mail not functioning as you would expect? Try restoring default settings for features related to your issue, by using the suggestions.
Sync mail period
Click "Optimize now" to change sync mail period for offline usage.
Recommended setting: 3 days
Optimize now
Sync inbox frequency
Click "Optimize now" to change sync inbox frequency.
Recommended setting: ON
Optimize now
Sync email
Click "Optimize now" to sync email.
Recommended setting: ON
Optimize now
Show pictures
Click "Optimize now" to display pictures.
Recommended setting: OFF

以下菜单项用于故障排除：

- 清除默认应用程序首选项
- 默认提醒时间
- 忽略电池优化
- 管理日历通知
- 管理邮件通知
- 显示图片
- 同步日历
- 同步联系人
- 同步电子邮件
- 同步收件箱频率
- 同步邮件周期

如果所有这些设置都已恢复为默认值，但您仍在使用 Secure Mail 时遇到问题，请联系您的管理员。

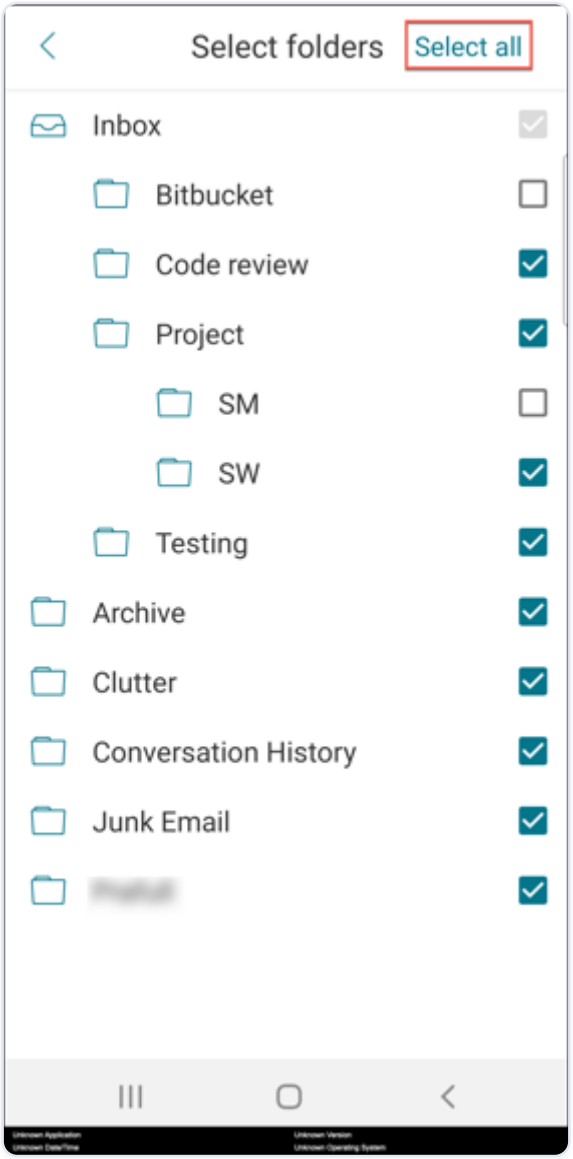
© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

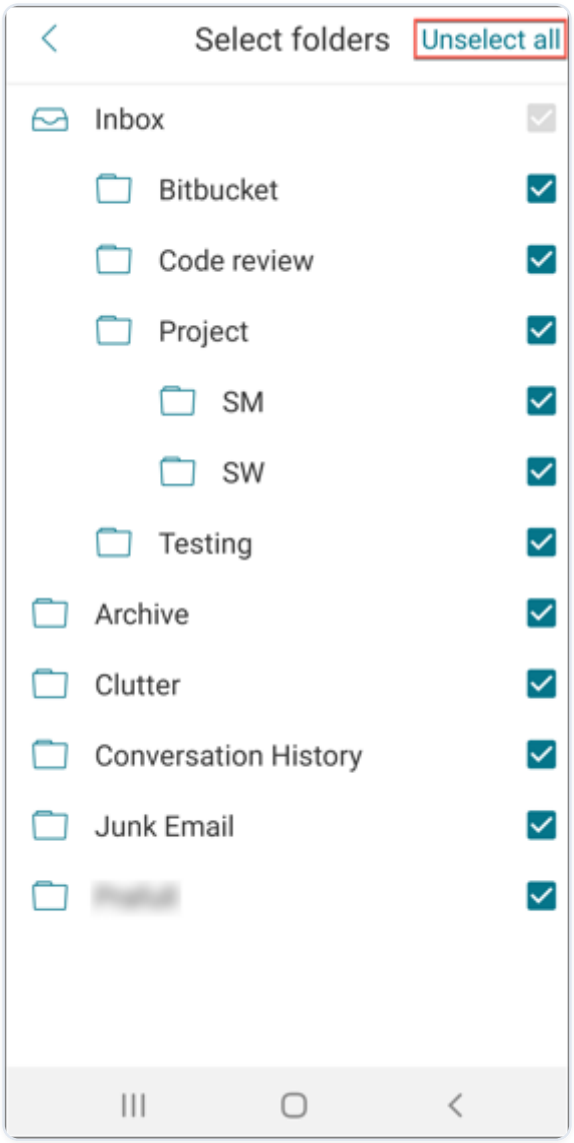
子文件夹通知增强功能

您现在可以通过导航到 **设置** > **通知** > **邮件文件夹**，然后在 **选择文件夹** 屏幕中单击 **全选** 选项来接收所有子文件夹的通知。



您可以单击 **取消全选** 以停止接收所有子文件夹的通知。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



安全邮件 21.10.5

从本版本开始，Secure Mail 支持 Exchange Server 2019 累积更新 11 和 Exchange Server 2016 累积更新 22。

适用于 iOS 的 Secure Mail

此版本包含错误修复。

适用于 Android 的 Secure Mail

此版本包含错误修复。

注意：

Secure Mail 对 Android 7 的支持将于 2021 年 10 月结束。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 21.10.0

适用于 Android 的 Secure Mail

- **支持 Android 12**。从本版本开始，Secure Mail 支持运行 Android 12 的设备。
- Secure Mail 符合 Google Play 针对 Android 11 的当前目标 API 要求（API 级别 30）。

安全邮件 21.9.1

适用于 Android 的 Secure Mail

此版本包含错误修复。

安全邮件 21.9.0

适用于 iOS 的 Secure Mail

此版本包含错误修复。

适用于 Android 的 Secure Mail

此版本包含错误修复。

安全邮件 21.8.5

适用于 Android 的 Secure Mail

支持已注册设备上的 Android 12 Beta 4。 Secure Mail 现在支持 Android 12 Beta 4。如果您正在考虑升级到 Android 12 Beta 4，请确保首先将 Secure Hub 更新到版本 21.7.1。Secure Hub 21.7.1 是升级到 Android 12 Beta 4 所需的最低版本。此版本可确保已注册用户从 Android 11 无缝升级到 Android 12 Beta 4。

注意：

Citrix 致力于为 Android 12 提供首日支持。Secure Mail 的后续版本将收到进一步更新，以完全支持 Android 12。

安全邮件 21.8.0

适用于 iOS 的 Secure Mail

© 1997–2026 Citrix Systems, Inc. All rights reserved.

混合环境中基于电子邮件的 Exchange Server 自动发现

在适用于 iOS 的 Secure Mail 中，您可以使用电子邮件地址配置 Microsoft 365 Exchange 帐户，这可确保混合 Exchange 服务器的顺畅登录体验。此功能也适用于本地 Exchange Server。

注意：

请确保为 Exchange Server 启用自动发现功能。

在运行 Microsoft Office 365 现代身份验证的设置上实现富推送通知

在此版本中，当网络访问策略设置为 **Tunneled - Web SSO** 且 Exchange Web Services (EWS) 主机名包含在**排除列表**中时，Secure Mail 支持推送通知。如果 EWS 和 ActiveSync 主机相同，请确保 ActiveSync 主机包含在**排除列表**策略中。

Secure Mail 的双模式

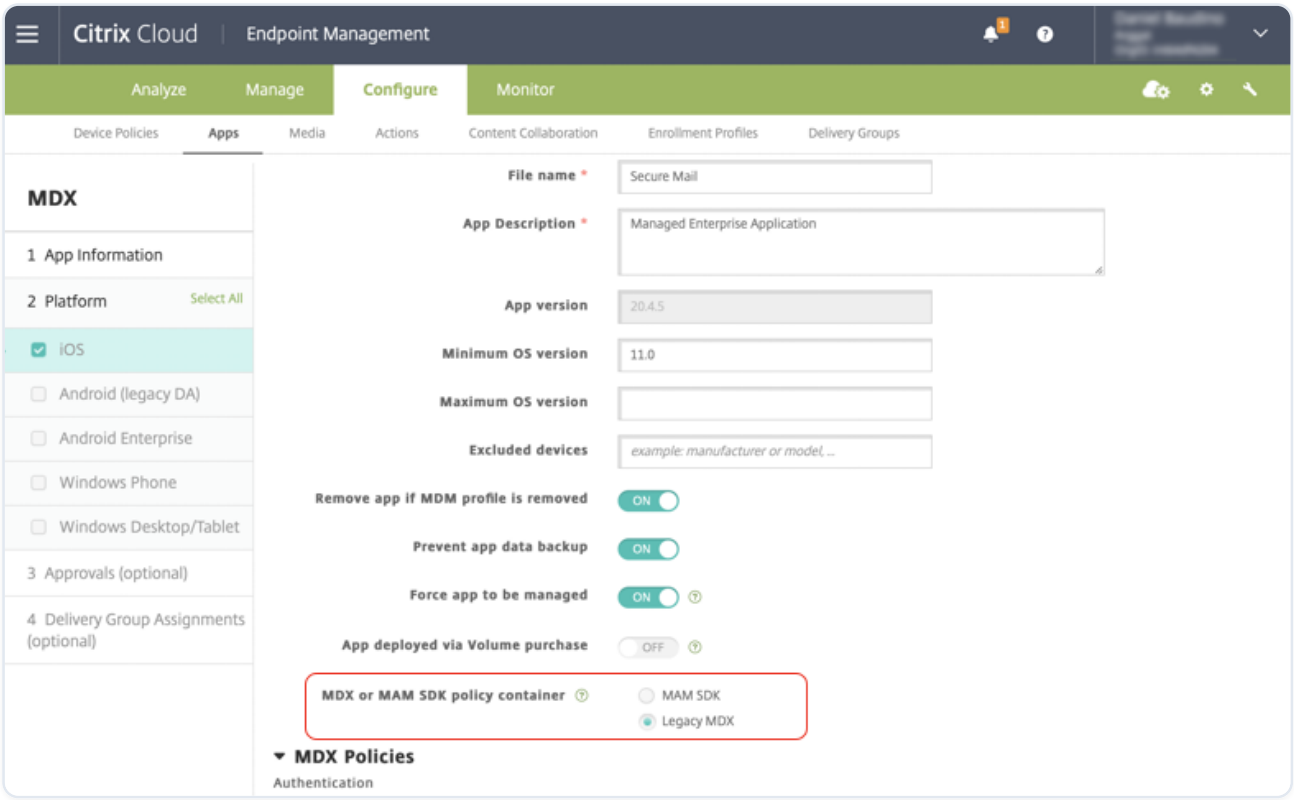
移动应用程序管理 (MAM) SDK 可用于替换 iOS 平台未涵盖的 MDX 功能区域。MDX 包装技术计划于 2023 年 7 月达到生命周期结束 (EOL)。

Citrix Secure Mail™ 发布时同时包含 MDX 和 MAM SDK 框架，以准备应对计划于 2023 年 7 月的 MDX EOL。要继续管理您的企业应用程序，您必须集成 MAM SDK。Citrix 建议您切换到 **MAM SDK**。双模式功能旨在提供一种将 Secure Mail 应用程序过渡到新 MAM SDK 模型的方法。

双模式功能允许您继续使用 MDX（现在是 **Legacy MDX**）管理应用程序，或切换到新的 **MAM SDK**。您可以在 **MDX 或 MAM SDK 策略容器**中获得以下策略设置选项：

- **MAM SDK**
- **旧版 MDX**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



在 **MDX 或 MAM SDK 策略容器**策略中，您可以将选项从 **Legacy MDX** 更改为 **MAM SDK**。 建议您不要从 **MAM SDK** 切换到 **Legacy MDX**，因为此切换需要您重新安装应用程序。默认值为 **Legacy MDX**。请确保为在设备上运行的 Secure Mail 和 Secure Web 设置相同的策略模式。您不能在同一设备上运行两种不同的模式。

当您选择 **MAM SDK** 模式时，应用程序会自动切换到 MAM SDK 框架，并且设备策略会刷新，无需管理员执行任何进一步操作。

注意：

当您从 **Legacy MDX** 切换到 **MAM SDK** 框架时，**网络访问**策略必须修改为 **Tunneled – Web SSO** 或 **Unrestricted**

先决条件

要成功部署双模式功能，请确保满足以下要求：

- 将 Citrix Endpoint Management 更新到 10.12 RP2 或更高版本，或 10.11 RP5 或更高版本。
- 将移动应用程序更新到 21.8.0 或更高版本。
- 如果您的组织使用第三方应用程序，请确保在切换到 MAM SDK 框架之前将 MAM SDK 集成到您的第三方应用程序中。所有托管应用程序必须一次性迁移到 MAM SDK。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

限制

- MAM SDK 仅支持基于平台的加密，不支持 MDX 加密。
- 如果您未将 Citrix Endpoint Management 更新到 10.12 RP2 或更高版本，或 10.11 RP5 或更高版本，则会出现重复的策略条目。如果策略文件运行在 21.8.0 或更高版本上，则会创建重复条目。
- 当您切换到 MAM SDK 应用程序管理模式时，某些功能不受支持或不可用。此外，不同模式下的应用程序之间的互操作性不支持“打开方式”和“复制/粘贴”等操作。例如，您无法将内容从以 **Legacy MDX** 模式管理的应用程序复制到以 **MAM SDK** 模式管理的应用程序，反之亦然。下表列出了 MAM SDK 模式下不可用的功能：

功能	旧版 MDX	MAM SDK
共享设备	是	否
英特云	是	否
SMIME 共享证书保管库	是	否
派生凭据	是	否
UIWebView 隧道	是	否
完整 VPN	是	否

- 以下策略已弃用，在 MAM SDK 模式下不可用：
  - 允许的 Secure Web 域
  - 允许的 Wi-Fi 网络
  - 备用 思杰网关
  - 证书标签
  - Citrix 报告
  - 显式注销通知
  - 需要微型 VPN 会话
  - 需要微型 VPN 会话宽限期（分钟）
  - 报告文件缓存最大值
  - 需要 Wi-Fi
  - 仅通过 Wi-Fi 发送报告

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 上传令牌

注意：

如果您使用客户端证书对内部服务器进行身份验证，则客户端证书必须与 Access Gateway 中使用的证书相同。

有关 MAM SDK 的更多信息，请参阅以下文章：

- MAM SDK 概述
- MAM SDK 的最新版本
- 有关 移动应用程序集成 的 Citrix Developer 文档
- Citrix 博客文章

适用于 Android 的 Secure Mail

此版本包含错误修复。

安全邮件 21.7.0

适用于 iOS 的 Secure Mail

此版本包含错误修复。

适用于 Android 的 Secure Mail

此版本包含错误修复。

安全邮件 21.6.0

适用于 iOS 的 Secure Mail

从此版本开始，不再支持以下“**网络访问**”策略选项：

- **使用以前的设置**
- **隧道式 - 完全 VPN**
- **隧道式 - 完全 VPN 和 Web SSO**

如果您正在使用**隧道式 - 完全 VPN**或**隧道式 - 完全 VPN 和 Web SSO**策略，则必须切换到**隧道式 - Web SSO**策略。如果您继续使用已弃用的策略，您的电子邮件将无法同步。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

要使用安全票证颁发机构 (STA)，必须将**网络访问**策略设置为**隧道式 - Web SSO**。

适用于 Android 的 Secure Mail

通过使用**故障排除**选项支持自诊断。此功能允许您检查对应用程序正常运行至关重要的基本首选项和设置是否已设置为默认值。如果您遇到有关某些 Secure Mail 设置的任何错误，请使用此功能对应用程序进行故障排除。

要访问此功能，请打开应用程序设置并在**支持**下点击**故障排除**。以下菜单选项将显示供您查看和编辑：

- 同步邮件周期
- 同步收件箱频率
- 同步电子邮件
- 显示图片
- 默认提醒时间
- 同步日历
- 同步联系人

要将设置恢复为默认值，请轻按“**应用更改**”。要将所有设置恢复为默认值，请轻按“**全部应用更改**”。

安全邮件 21.5.0

从本版本开始，Secure Mail 支持 Exchange Server 2019 累积更新 9 和 Exchange Server 2016 累积更新 20。

适用于 iOS 的 Secure Mail

- **在 Secure Mail 日历事件中创建 Microsoft Teams 会议。** 在适用于 iOS 的 Secure Mail 中，您可以在创建日历事件时创建 Microsoft Teams 会议邀请。要创建 Microsoft Teams 会议，请打开“**Microsoft Teams 会议**”切换开关。会议邀请链接和详细信息将随事件详细信息自动发送。有关详细信息，请参阅在 Secure Mail 日历事件中创建 Microsoft Teams 会议
- 从本版本开始，以下“**网络访问**”策略选项已弃用，并且从版本 21.6.0 开始不再受支持：
  - **使用以前的设置**
  - **隧道 - 完全 VPN**
  - **隧道 - 完全 VPN 和 Web SSO**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

如果您正在使用“**隧道 - 完全 VPN**”或“**隧道 - 完全 VPN 和 Web SSO**”策略，则必须切换到“**隧道 - Web SSO**”策略。如果您继续使用已弃用的策略，您的电子邮件将无法同步。

注意：

如果您正在使用“**隧道 - 完全 VPN**”并且配置了 Secure Ticket Authority (STA)，则现代身份验证屏幕将无法加载。

适用于 Android 的 Secure Mail

- 在此版本中，“**禁用强制升级**”杂项策略在 Citrix Endpoint Management 控制台中不再可用。您的应用程序将自动升级到 Play 商店中提供的最新版本。
- 在适用于 Android 的 Secure Mail 中，**管理源**选项在此版本中已弃用。如果您当前已启用并配置此功能，您将继续在**源**窗口中看到基于您首选设置的源。如果您是新用户，或者您之前已删除所有源卡，则以下默认源卡可用：
  - 未读
  - 会议邀请
  - 即将召开的会议
  - 来自您的经理

安全邮件 21.4.5

适用于 Android 的 Secure Mail

基于电子邮件的自动发现支持。 在适用于 Android 的 Secure Mail 中，您可以使用电子邮件地址配置 Microsoft O365 Exchange 帐户，这可确保流畅的登录体验。如果在混合环境中启用了自动发现，此功能也适用于本地用户

注意：

此功能仅在 Exchange Server 2016 累积更新 3 及更高版本上受支持。

安全邮件 21.4.0

适用于 iOS 的 Secure Mail

此版本包含错误修复。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 21.3.5

适用于 Android 的 Secure Mail

此版本包含错误修复。

安全邮件 21.3.0

适用于 iOS 的 Secure Mail

Secure Mail iOS 的部署目标已更改为 iOS 12.2。 适用于 iOS 的 Microsoft Intune App SDK 版本 14.1.3 要求目标应用具有最低 iOS 部署版本 iOS 12.2。Secure Mail 的部署目标已更新为 iOS 12.2，以符合此要求。

适用于 Android 的 Secure Mail

在 Secure Mail 日历事件中创建 Microsoft Teams 会议。 在适用于 Android 的 Secure Mail 中，您可以在创建日历事件时创建 Microsoft Teams 会议邀请。 要创建 Microsoft Teams 会议，请打开 **Microsoft Teams 会议**切换开关。会议邀请链接和详细信息将随事件详细信息自动发送。有关详细信息，请参阅在 Secure Mail 日历事件中创建 Microsoft Teams 会议

安全邮件 21.2.0

从此版本开始，Secure Mail 支持 Exchange Server 2019 累积更新 8 和 Exchange Server 2016 累积更新 19。

适用于 iOS 的 Secure Mail

- **Secure Mail 颜色改版。** Secure Mail 符合 Citrix 品牌颜色更新。

适用于 Android 的 Secure Mail

- **Secure Mail 颜色改版。** Secure Mail 符合 Citrix 品牌颜色更新。
- **支持 Microsoft Intune。** 适用于 Android 的 Secure Mail 支持最新版本的 Microsoft Intune 7.2.2。
- **在可折叠设备上稳定运行。** 适用于 Android 的 Secure Mail 包含在可折叠设备上稳定运行的修复程序。

安全邮件 21.1.5

适用于 iOS 的 Secure Mail

此版本包含错误修复。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 21.1.0

此版本包含错误修复。

安全邮件 20.12.0

适用于 iOS 的 Secure Mail

此版本包含错误修复。

安全邮件 20.11.0

注意：

对 Exchange Server 2010 的支持已于 October 13, 2020 结束。

安全邮件 20.10.5

适用于 iOS 的 Secure Mail

此版本包含错误修复。

适用于 Android 的 Secure Mail

支持 AndroidX 库。 根据 Google 的建议，Secure Mail 支持 **AndroidX** 库，这些库是 **android.support** 封装库的替代品。

安全邮件 20.10.0

从本版本开始，Secure Mail 支持 Exchange Server 2019 累积更新 7 和 Exchange Server 2016 累积更新 18。

适用于 iOS 的 Secure Mail

从 Secure Mail 加入 Microsoft Teams 会议。 在适用于 iOS 的 Secure Mail 中，您可以直接从日历中的邀请加入 Microsoft Teams 会议。如果已安装 Microsoft Teams 应用程序，则该应用程序将打开，您可以加入会议。如果未安装该应用程序，您将看到一个选项，可前往 App Store 安装 Microsoft Teams。对于 `https://teams.microsoft.com/l/meetup-join/meetinglink` 格式的会议，应用程序将打开，您可以直接加入会议。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

确保您的管理员在“允许的 URL”策略中包含 `+\^msteams:`。有关详细信息，请参阅应用程序交互（出站 URL）。

适用于 Android 的 Secure Mail

- **从 Secure Mail 加入 Microsoft Teams 会议。** 在适用于 Android 的 Secure Mail 中，您可以直接从日历中的邀请加入 Microsoft Teams 会议。如果已安装 Microsoft Teams 应用程序，则该应用程序将打开，您可以加入会议。如果未安装该应用程序，您将看到一个选项，可前往 Google Play 安装 Microsoft Teams。对于 `https://teams.microsoft.com/l/meetup-join/>meetinglink` 格式的会议，应用程序将打开，您可以直接加入会议。

  注意：

  确保您的管理员在“受限打开方式”例外列表策略中包含 `{action=android.intent.action.VIEW scheme=msteams package=com.microsoft.teams}`。有关详细信息，请参阅应用程序交互。

- Secure Mail 支持 Google Play 针对 Android 10 的当前目标 API 要求。

安全邮件 20.9.5

适用于 Android 的 Secure Mail

此版本包含错误修复。

安全邮件 20.9.0

支持 Azure 政府云计算。 适用于 iOS 和 Android 的 Secure Mail 支持 Azure Active Directory 租户上的政府云计算 (GCC) High，用于现代身份验证 (OAuth)。Secure Mail 已注册为 GCC High 上的一个端点，以满足 Microsoft 对所有 GCC High 服务的强制要求。有关详细信息，请参阅 Microsoft 365 政府版中 Azure Active Directory 的新增功能。

进行此更改后，您将被路由到 Azure Active Directory 租户上的 GCC High 进行身份验证。管理员需要允许 Secure Mail 在 Azure Active Directory 租户上拥有权限。

先决条件

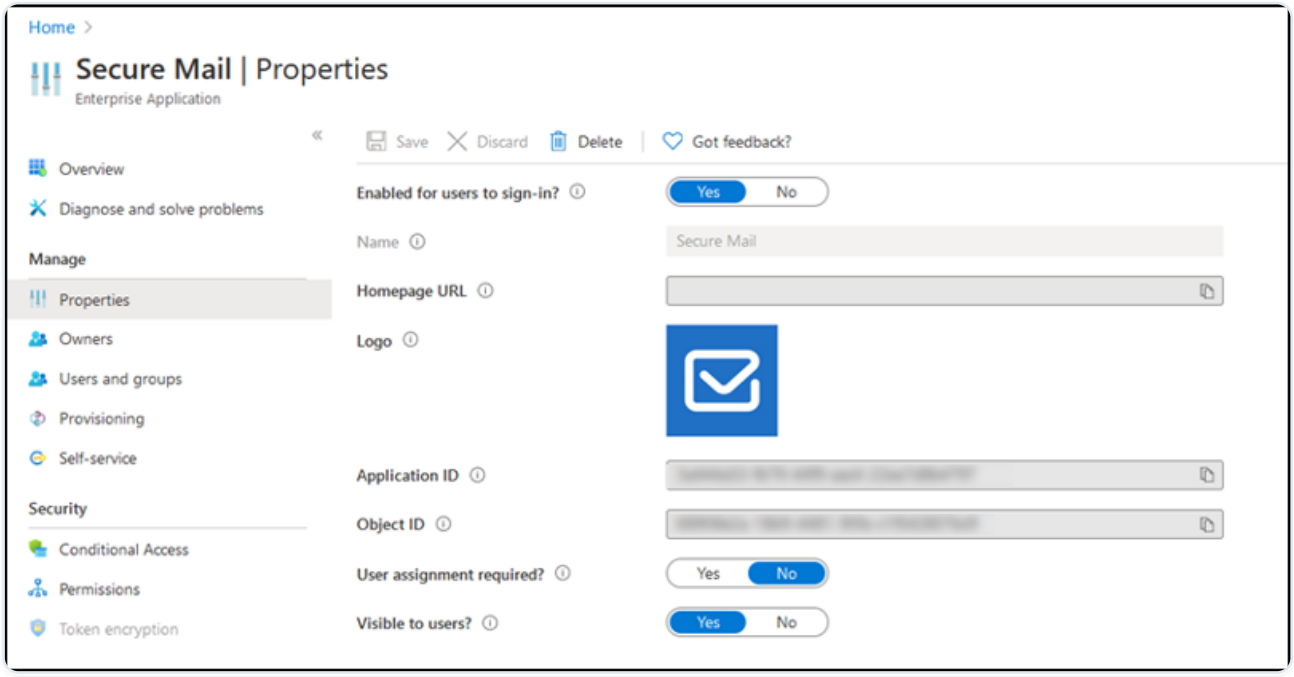
确保 Azure Active Directory 的全局管理员执行以下操作：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 在您的设备上下载最新版本的 Secure Mail。
- 在 Secure Mail 应用程序上配置您的 Exchange 帐户，并允许 Azure Active Directory 上的应用程序权限，以便所有用户登录。请参阅以下屏幕。

注意：

这些步骤仅适用于全局管理员，作为一次性要求。一旦应用程序获得访问权限，您就可以直接从 App Store 升级。



升级后

升级后，刷新令牌过期后会出现重新授权提示，它会将您重定向到 Azure Active Directory 上的 GCC High。验证上述工作流程，以确保授权请求已发送到 Azure Active Directory 上的 GCC High。

您可以通过以下方式之一验证工作流程：

- 应用程序名称为 **Secure Mail-GCC High** 的 Secure Mail 会出现在您的 Azure Active Directory 租户的登录页面上。
- 检查 Secure Mail 日志以确认重新身份验证后重定向是否通过 `<https://login.microsoftonline.us>` 发生。

安全邮件 20.8.5

适用于 Android 的 Secure Mail

适用于 Android 的 Secure Mail 支持 Android 11。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 20.8.0

从本版本开始，Secure Mail 支持 Exchange Server 2019 累积更新 6 和 Exchange Server 2016 累积更新 17。

适用于 Android 的 Secure Mail

Secure Mail 的双模式。 移动应用程序管理 (MAM) SDK 可用于替换 iOS 和 Android 平台未涵盖的 MDX 功能区域。MDX 包装技术计划于 2022 年 3 月达到生命周期结束 (EOL)。要继续管理您的企业应用程序，您必须集成 MAM SDK。

从 20.8.0 版本开始，Android 应用程序随 MDX 和 MAM SDK 一起发布，为之前提到的 MDX EOL 策略做准备。MDX 双模式旨在提供一种从旧版 MDX Toolkit 过渡到新 MAM SDK 的方法。使用双模式，您可以选择继续使用 MDX Toolkit（现为旧版 MDX）管理应用程序，或者切换到新的 MAM SDK 进行应用程序管理。

一旦您切换到 MAM SDK 进行应用程序管理，Citrix 将实施进一步的更改，并且不需要管理员执行任何操作。

有关 MAM SDK（预览版）的更多详细信息，请参阅以下文章：

- MAM SDK 概述
- MAM SDK 的最新版本
- Citrix 开发者部分关于设备管理
- Citrix 博客文章

先决条件

为了成功部署双模式功能，请确保以下事项：

- 将您的 Citrix Endpoint Management 更新到 10.12 RP2 或更高版本，或 10.11 RP5 或更高版本。
- 将您的移动应用程序更新到 20.8.0 或更高版本。
- 将策略文件更新到 20.8.0 或更高版本。
- 如果您的组织使用第三方应用程序，请确保在将 Citrix 移动生产力应用程序切换到 MAM SDK 之前，将 MAM SDK 集成到您的第三方应用程序中。所有托管应用程序必须一次性迁移到 MAM SDK。

注意：

所有基于云的客户均支持 MAM SDK。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

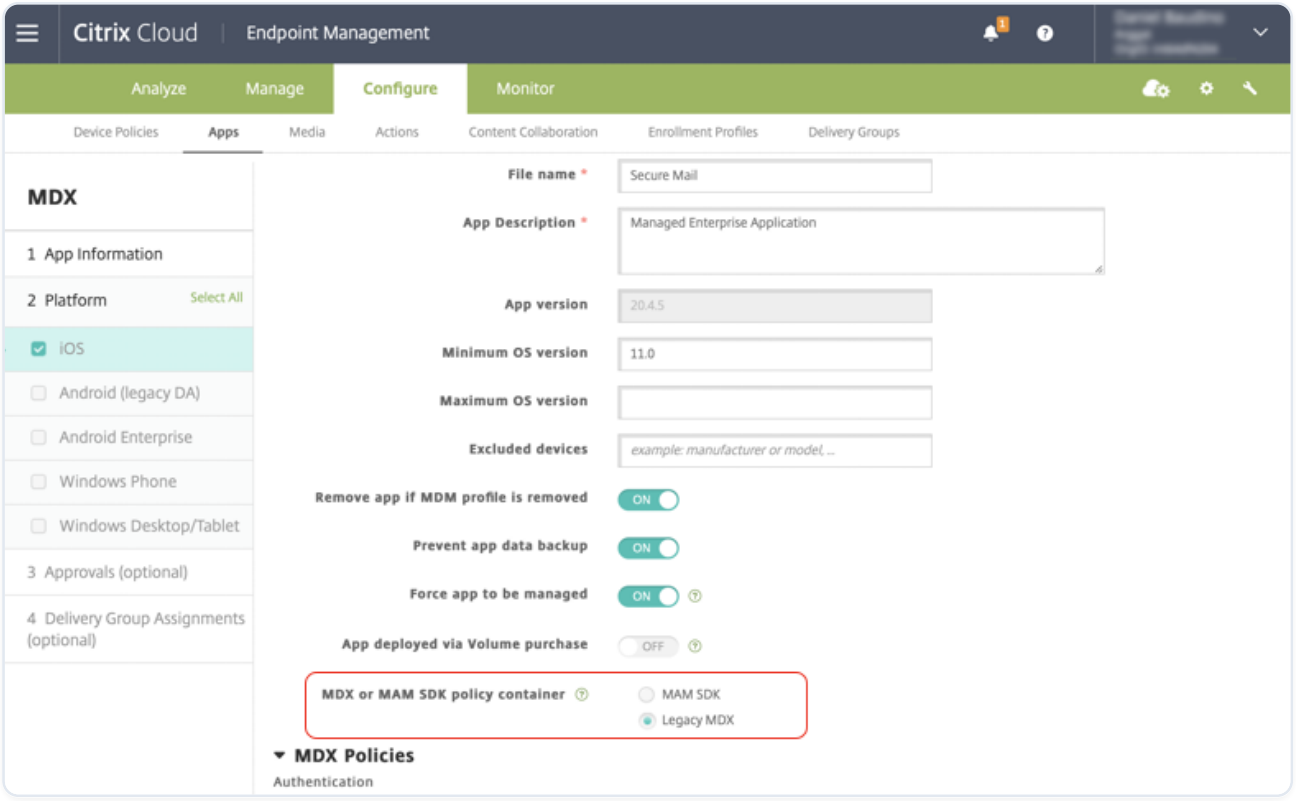
限制

- MAM SDK 仅支持在您的 Citrix Endpoint Management 部署中 Android Enterprise 平台下发布的应用程序。对于新发布的应用程序，默认加密是基于平台的加密。
- MAM SDK 仅支持基于平台的加密，不支持 MDX 加密。
- 如果您不更新 Citrix Endpoint Management，并且策略文件在移动应用程序上运行 20.8.0 及更高版本，则 Secure Mail 会出现重复的网络策略条目。

在 Citrix Endpoint Management 中配置 Secure Mail 时，双模式功能允许您继续使用 MDX Toolkit（现在是 **Legacy MDX**）管理应用程序，或切换到新的 **MAM SDK** 进行应用程序管理。Citrix 建议您切换到 **MAM SDK**，因为 MAM SDK 更具模块化，旨在允许您仅使用组织所使用的 MDX 功能的子集。

您可以在 **MDX 或 MAM SDK 策略容器**中获得以下策略设置选项：

- **MAM SDK**
- **旧版 MDX**



在 **MDX or MAM SDK policy container** 策略中，您只能将选项从 **Legacy MDX** 更改为 **MAM SDK**。不允许从 **MAM SDK** 切换到 **Legacy MDX**，您需要重新发布应用程序。默认值为 **Legacy MDX**。请确保为在同一设备上运行的 Secure Mail 和 Secure Web 设置相同的策略模式。您不能在同一设备上运行两种不同的模式。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 iOS 的 Secure Mail

邮箱同步优化。 在适用于 iOS 的 Secure Mail 中，**邮箱**同步功能得到了改进，以提供更好的用户体验。**日历**和**联系人**同步速度更快。早于 3 周的电子邮件会被截断，以减少同步时间。您可以在打开电子邮件时查看完整的电子邮件。

安全邮件 20.7.5

注意：

对 Android 6.x 的支持已于 June 30, 2020 结束。

有关移动生产力应用程序的最新信息，请参阅文章 最新公告。

安全邮件 20.7.0

此版本包括错误修复。

安全邮件 20.6.5

此版本包括错误修复。

安全邮件 20.6.0

此版本包括错误修复。

安全邮件 20.5.0

此版本包括错误修复。

安全邮件 20.4.5

适用于 Android 的 Secure Mail

从该版本开始，Secure Mail 支持 Exchange Server 2019 累积更新 5 和 Exchange Server 2016 累积更新 16。

安全邮件 20.4.0

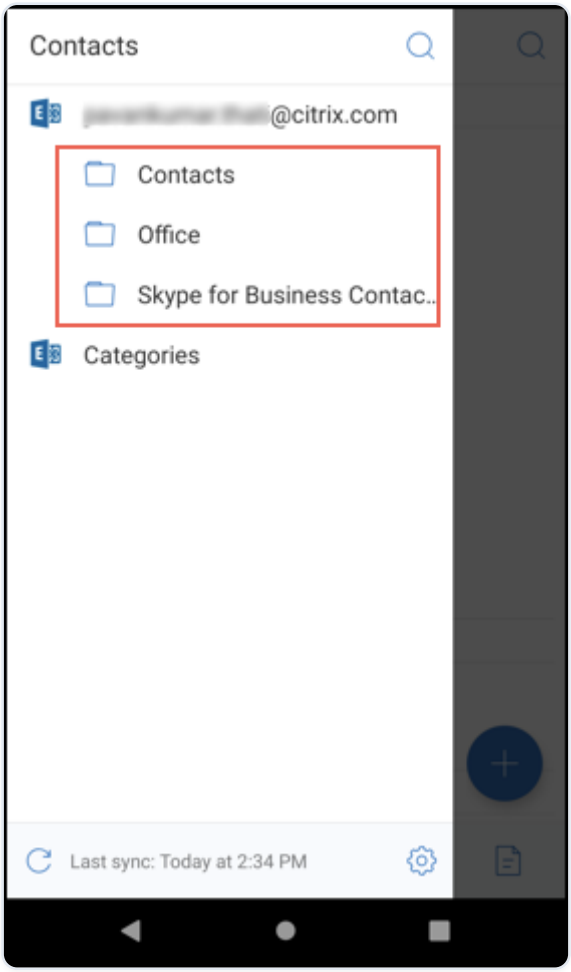
从该版本开始，Secure Mail 支持 Exchange Server 2016 累积更新 15 和 Exchange Server 2013 累积更新 23。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 20.3.0

适用于 Android 的 Secure Mail

在“联系人”中创建文件夹。 在适用于 Android 的 Secure Mail 中，您可以在电子邮件帐户的“**联系人**”部分中添加、编辑和删除文件夹。



适用于 iOS 的 Secure Mail

此版本包括错误修复。

安全邮件 20.2.0

适用于 Android 的 Secure Mail

最小化草稿

在适用于 Android 的 Secure Mail 中，您可以在撰写电子邮件时最小化草稿并在应用程序中导航。有关此功能的帮助文档，请参阅 Citrix 用户帮助中心文章最小化草稿电子邮件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 20.1.5

适用于 iOS 的 Secure Mail

从该版本开始，Secure Mail 支持 Exchange Server 2019 累积更新 4。

适用于 Android 的 Secure Mail

- **双向联系人同步。** 在适用于 Android 的 Secure Mail 中，您可以从本地联系人列表中创建、编辑和删除 Secure Mail 联系人。
- **支持 ICS 文件。** 在适用于 Android 的 Secure Mail 中，您可以预览作为附件收到的 ICS 文件，并将其作为事件导入到日历中。
- 从该版本开始，Secure Mail 支持 Exchange Server 2019 累积更新 4。

安全邮件 20.1.0

从该版本开始，Secure Mail 支持 Exchange Server 2016 累积更新 14

安全邮件 19.12.5

适用于 iOS 的 Secure Mail

此版本包含错误修复。

适用于 Android 的 Secure Mail

撤消已发送邮件。 在适用于 Android 的 Secure Mail 中，您可以撤消已发送邮件。点击“**发送**”按钮后，您会收到一条浮动消息，允许您撤消发送操作。点击“**撤消**”可还原发送操作并编辑邮件、邮件收件人、附加或删除附件，或放弃邮件。

草稿文件夹中的附件同步。 在适用于 Android 的 Secure Mail 中，当“**草稿**”文件夹同步时，附件也会同步，并且可在您的所有设备上使用。此功能适用于运行 Exchange ActiveSync 版本 16 或更高版本的设备。

安全邮件 19.11.5

适用于 iOS 的 Secure Mail

Secure Mail 中的联系人图片。 在适用于 iOS 的 Secure Mail 中，当您在电子邮件或会议邀请中添加收件人时，可以查看联系人的图片。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章显示联系人图片。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 Android 的 Secure Mail

应用内查看 PDF 文件。 在适用于 Android 的 Secure Mail 中，您可以在应用内查看 PDF 文件，包括书签和批注。此外，还提供其他 Microsoft Office 附件的增强视图。

适用于 iOS 的 Secure Mail 19.10.6

此版本包含错误修复。

安全邮件 19.10.5

适用于 iOS 的 Secure Mail

最小化草稿。 在适用于 iOS 的 Secure Mail 中，您可以在撰写电子邮件时最小化草稿并在应用内导航。此功能适用于运行 iOS 13 及更高版本的设备。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章 最小化草稿电子邮件。

适用于 Android 的 Secure Mail

此版本包含错误修复。

安全邮件 19.10.0

使用 Office 365 Exchange Server 策略定义 Office 365 服务器地址。 在 Secure Mail iOS 和 Android 中，在“**OAuth Support for Office 365**”部分下添加了一个名为“**Office 365 Exchange Server**”的新策略。通过此策略，您可以定义云上 Office 365 邮箱的主机名。此策略还支持政府机构使用 Office 365。主机名是一个单一值，例如 *outlook.office365.com*。默认值为 *outlook.office365.com*。

Secure Mail iOS 和 Android 支持加密管理。 加密管理允许您使用现代设备平台安全性，同时确保设备保持在足以有效使用平台安全性的状态。通过使用加密管理，您可以消除本地数据加密冗余，因为文件系统加密由 iOS 或 Android 平台提供。要启用此功能，管理员必须在 Citrix Endpoint Management 控制台中将“**加密类型**”MDX 策略配置为“**平台加密并强制合规**”。

要使用加密管理功能，请在 Citrix Endpoint Management 控制台中，将**加密类型**策略设置为**带合规性强制的平台加密**。这将启用加密管理，并且用户设备上的所有现有加密应用程序数据将无缝转换为由设备而非 MDX 加密的状态。在此转换期间，应用程序会暂停以进行一次性数据迁移。迁移成功后，本地存储数据加密的责任将从 MDX 转移到设备平台。MDX 会在每次应用程序启动时继续检查设备的合规性。此功能在 MDM + MAM 和仅限 MAM 的环境中均可使用。

当您将**加密类型**策略设置为**带合规性强制的平台加密**时，新策略将取代您现有的 MDX 加密。

有关 Secure Mail 的加密管理 MDX 策略的详细信息，请参阅以下内容中的**加密**部分：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 适用于 Android 的移动生产力应用程序的 MDX 策略
- 适用于 iOS 的移动生产力应用程序的 MDX 策略

当设备不符合最低合规性要求时，**不合规设备行为**策略允许您选择要执行的操作：

- **允许应用程序** – 允许应用程序正常运行。
- **警告后允许应用程序** – 警告用户应用程序不符合最低合规性要求，并允许应用程序运行。这是默认值。
- **阻止应用程序** – 阻止应用程序运行。

运行 iOS 的设备

以下条件决定设备是否符合运行 iOS 的设备的最低合规性要求：

- iOS 10 - 应用程序运行的操作系统版本大于或等于指定版本。
- 调试器访问 - 应用程序未启用调试。
- 越狱设备 - 应用程序未在越狱设备上运行。
- 设备密码 - 设备密码为**开**。
- 数据共享 - 未为应用启用数据共享。

运行 Android 的设备

以下标准确定设备是否满足运行 Android 的设备的最低合规性要求：

- Android SDK 24 (Android 7 牛轧糖) - 应用运行的操作系统版本大于或等于指定版本。
- 调试器访问 - 应用未启用调试。
- 已 Root 设备 - 应用未在已 Root 设备上运行。
- 设备锁定 - 设备密码已**开启**。
- 设备已加密 - 应用在已加密设备上运行。

安全邮件 19.9.5

适用于 iOS 的 Secure Mail

支持 ICS 文件。在适用于 iOS 的 Secure Mail 中，您可以将作为附件收到的 ICS 文件导入到日历中作为事件。

适用于 Android 的 Secure Mail

此版本包含错误修复。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 19.9.0

从此版本开始，Secure Mail 支持以下服务器：

- Exchange Server 2016 累积更新 13
- IBM Lotus Notes Traveler 版本 10.0.1.0 内部版本 201811191126_20
- IBM Domino 邮件服务器 版本 10.0.1

适用于 iOS 的 Secure Mail

- 适用于 iOS 的 Secure Mail 支持 iOS 13。
- **使用 MIME 标头报告网络钓鱼电子邮件。** 在适用于 iOS 的 Secure Mail 中，当用户报告网络钓鱼邮件时，将生成一个 EML 文件作为该邮件的附件。管理员会收到此邮件，并可以查看与所报告邮件关联的 MIME 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“通过附件报告”。有关详细信息，请参阅将网络钓鱼电子邮件报告为附件。
- **支持响应式电子邮件。** 适用于 iOS 的 Secure Mail 已优化以提供响应式电子邮件。以前，包含大型表格或图像的电子邮件内容会错误呈现。此功能可在所有受支持的设备上提供更易读的电子邮件内容，无论电子邮件格式和大小如何。
- **拖放日历事件。** 在适用于 iOS 的 Secure Mail 中，您可以通过拖放事件来更改现有日历事件的时间。拖动事件并将其放到同一天或跨天的所需时间段以进行更新。
- **自动前进。** 在适用于 iOS 的 Secure Mail 中，当您删除“**对话**”中的邮件时，可以选择要返回的邮件。要使用此功能，请导航到“**设置 > 自动前进**”。然后，从可用选项中选择您的偏好。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章删除并自动前进到“对话”中的电子邮件。
- **支持 WkWebView。** 适用于 iOS 的 Secure Mail 支持 WkWebView。此功能改进了 Secure Mail 电子邮件和日历事件在设备上的呈现方式。

适用于 Android 的 Secure Mail

从本版本开始，适用于 Android 的 Secure Mail 仅支持运行 Android 6 或更高版本的设备。

适用于 Android 的 Secure Mail 19.8.5

本版本包含错误修复。

安全邮件 19.8.0

适用于 iOS 的 Secure Mail

此版本包含性能增强和错误修复。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 Android 的 Secure Mail

- 支持 Android Q。
- **支持 Google Play 上的 64 位应用程序。** 适用于 Android 的 Secure Mail 支持 64 位体系结构。
- **适用于 Android 的 Secure Mail 中“下拉刷新”UI 的改进。** 为遵循 Material Design 准则，我们对**下拉刷新**功能进行了少量改进。当您点击汉堡包图标时，同步时间戳会显示在屏幕底部。

安全邮件 19.7.5

适用于 iOS 的 Secure Mail

- **草稿文件夹自动同步。** 在适用于 iOS 的 Secure Mail 中，草稿文件夹会自动同步，并且您的草稿可在所有设备上使用。此功能适用于运行 Exchange ActiveSync v16 或更高版本的设置。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章 草稿文件夹自动同步。
- **当您在 MDM + MAM 模式下使用 Microsoft Intune 时，适用于 iOS 的 Secure Mail 支持单点登录。** 要使用此功能，请确保您的设备上已安装 Microsoft Authenticator 应用程序。有关安装 Microsoft Authenticator 应用程序的更多信息，请参阅 *Docs.microsoft.com* 上的“**下载并安装 Microsoft Authenticator**”应用程序。

适用于 Android 的 Secure Mail

注意：

> Citrix 建议您在将操作系统升级到 Android Q 之前，先将 Secure Mail 升级到版本 19.7.5。

- **适用于运行 Microsoft Office 365 现代身份验证的设置的“使用 Web SSO 进行隧道连接”策略。** 在适用于 Android 的 Secure Mail 中，添加了一个名为“**使用 Web SSO 进行隧道连接**”的新策略。通过此策略，您可以将 OAuth 流量通过 Tunneled – Web SSO 进行隧道连接。为此，请执行以下操作：
  - 将“**使用 Web SSO 进行隧道连接**”策略设置为“**开**”。
  - 在网络访问策略中选择 **Tunneled - Web SSO** 选项。
  - 从 **后台服务** 策略中排除任何与 OAuth 相关的主机名。
- **当您在 MDM + MAM 模式下使用 Microsoft Intune 时，Secure Mail for Android 支持单点登录。** 要使用此功能，请确保您的设备上已安装 Intune 公司门户应用程序。登录 Intune 公司门户应用程序后，您可以在 MDM + MAM 模式下使用 SSO，而无需使用您的凭据在 Secure Mail 中重新进行身份验证。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

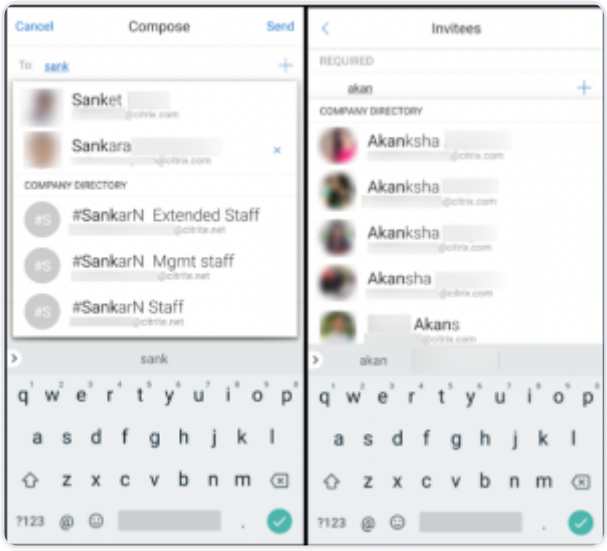
安全邮件 19.6.5

Secure Mail 适用于 iOS

Secure Mail for iOS 19.6.5 版本包含性能增强和错误修复。有关已修复和已知问题的列表，请参阅已知和已修复问题。

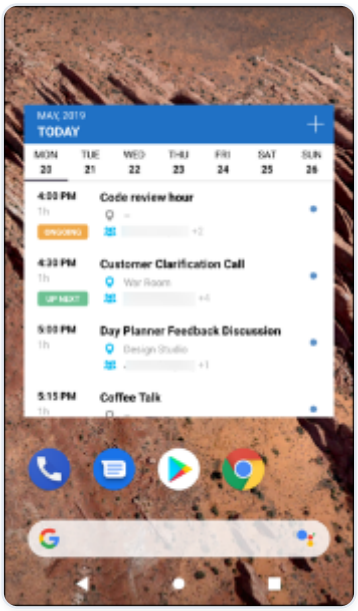
Secure Mail 适用于 Android

- **拖放日历事件。** 在 Secure Mail for Android 中，您可以通过拖放事件来更改现有日历事件的时间。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章更改日历事件时间。
- **支持响应式电子邮件。** Secure Mail for Android 已优化以提供响应式电子邮件。以前，包含大型表格或图像的电子邮件内容会渲染不正确。此功能使电子邮件内容在所有受支持的设备上都更具可读性，无论电子邮件格式和大小如何。
- **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，可以查看联系人图片。联系人图片显示在姓名旁边。如果有多个人同名，该图片有助于在您添加电子邮件或会议邀请中的收件人时识别正确的收件人。要搜索未本地保存的联系人，请输入收件人姓名的至少四个字符以显示图片。



- **日历议程小组件。** 在 Secure Mail for Android 中，**日历**议程可用作小组件。通过此小组件，您可以查看**日历**中一周内的即将发生的事件。此功能允许您创建**日历**事件、查看现有事件并编辑详细信息。**阻止屏幕捕获**策略不适用于放置在主屏幕上的小组件。但是，您可以使用**允许日历议程小组件**策略禁用该小组件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



安全邮件 19.5.5

Secure Mail 适用于 Android

Secure Mail for Android 版本 19.5.5 包含性能增强和错误修复。有关已修复和已知问题的列表，请参阅已知和已修复问题。

适用于 iOS 的 Secure Mail

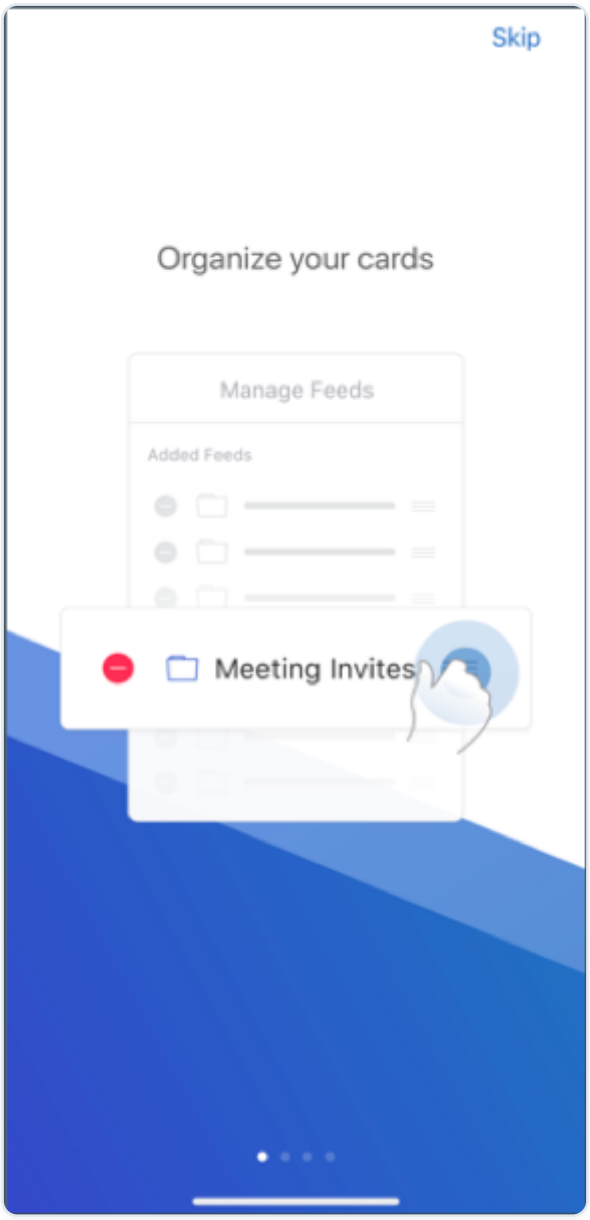
- 当您在 MDM + MAM 模式下使用 Microsoft Intune 时，适用于 iOS 的 Secure Mail 支持单点登录。要使用此功能，请确保您的设备上已安装 Microsoft Authenticator 应用程序。Microsoft Authenticator 应用程序可在应用商店中获取。
- **支持 Slack EMM：** Slack EMM 适用于已启用企业移动管理 (EMM) 的 Slack 客户。适用于 iOS 的 Secure Mail 支持应用程序 **Slack EMM**，它允许管理员选择 Secure Mail 与 **Slack** 应用程序或 **Slack EMM** 应用程序的集成方式。

安全邮件 19.5.0

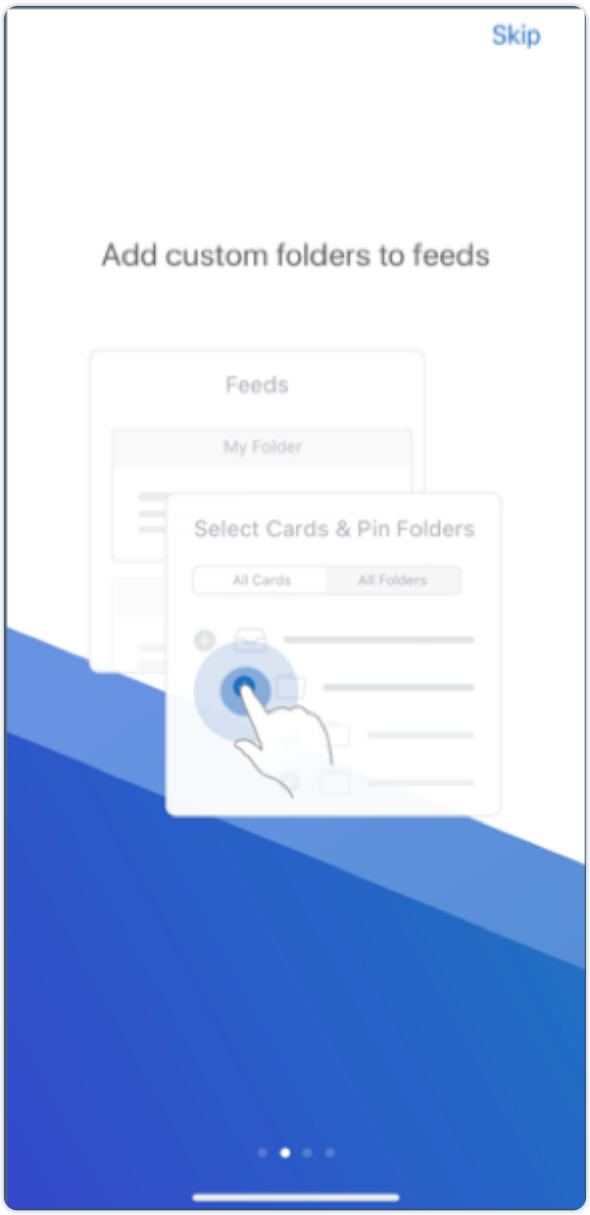
适用于 Android 的 Secure Mail

管理您的源。 在适用于 Android 的 Secure Mail 中，您可以根据您的要求组织您的**源**卡片。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



有关管理您的源的更多信息，请参阅管理您的源。

草稿文件夹自动同步。 在适用于 Android 的 Secure Mail 中，草稿文件夹会自动同步，并且您的草稿可在所有设备上使用。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章草稿文件夹自动同步。

适用于 Android 的 Secure Mail 19.4.6、19.4.5 和 19.3.5

这些版本包含性能增强和错误修复。

有关已修复和已知问题的列表，请参阅已知和已修复问题。

安全邮件 19.3.0

从本版本开始，Secure Mail 支持以下服务器：

- Exchange Server 2019 累积更新 1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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

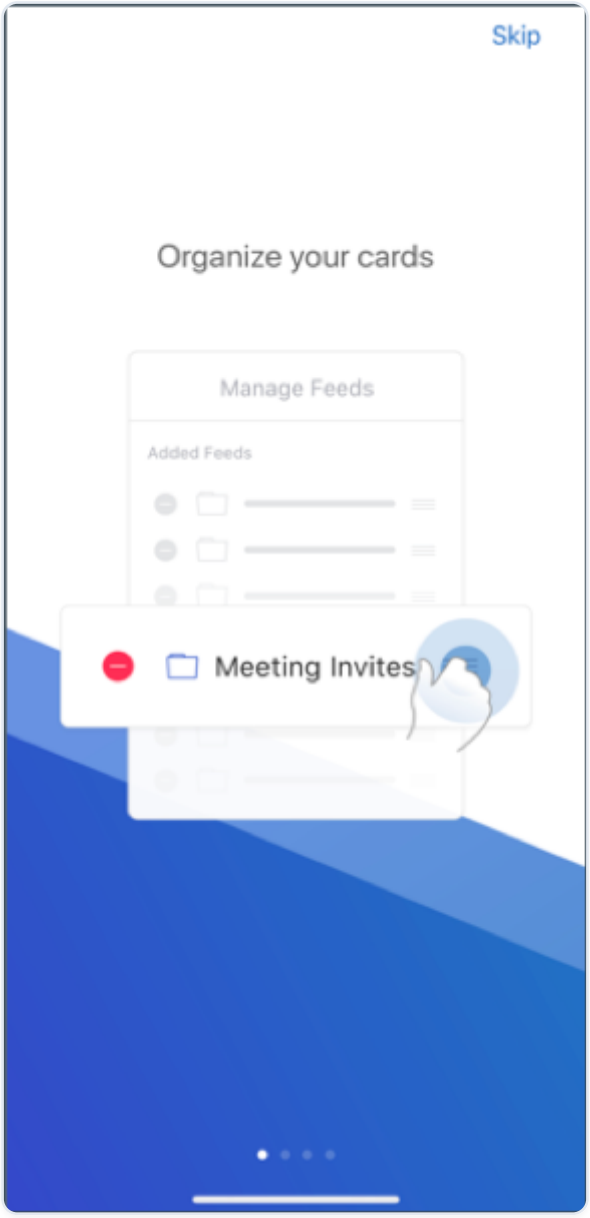
有关 Secure Mail 服务器兼容性完整列表的更多信息，请参阅 Secure Mail 概述。

适用于 iOS 的 Secure Mail

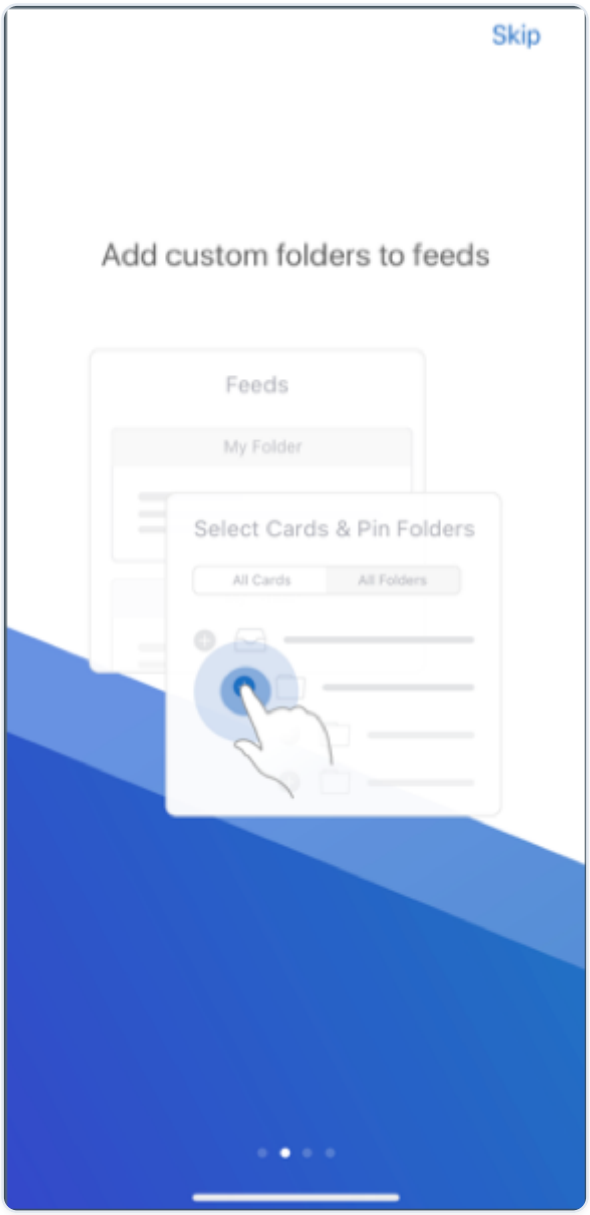
管理您的源。 在适用于 iOS 的 Secure Mail 中，您现在可以根据您的要求组织您的 **Feeds** 卡。

注意：

此功能在 iPad 上不可用。



© 1997–2026 Citrix Systems, Inc. All rights reserved.



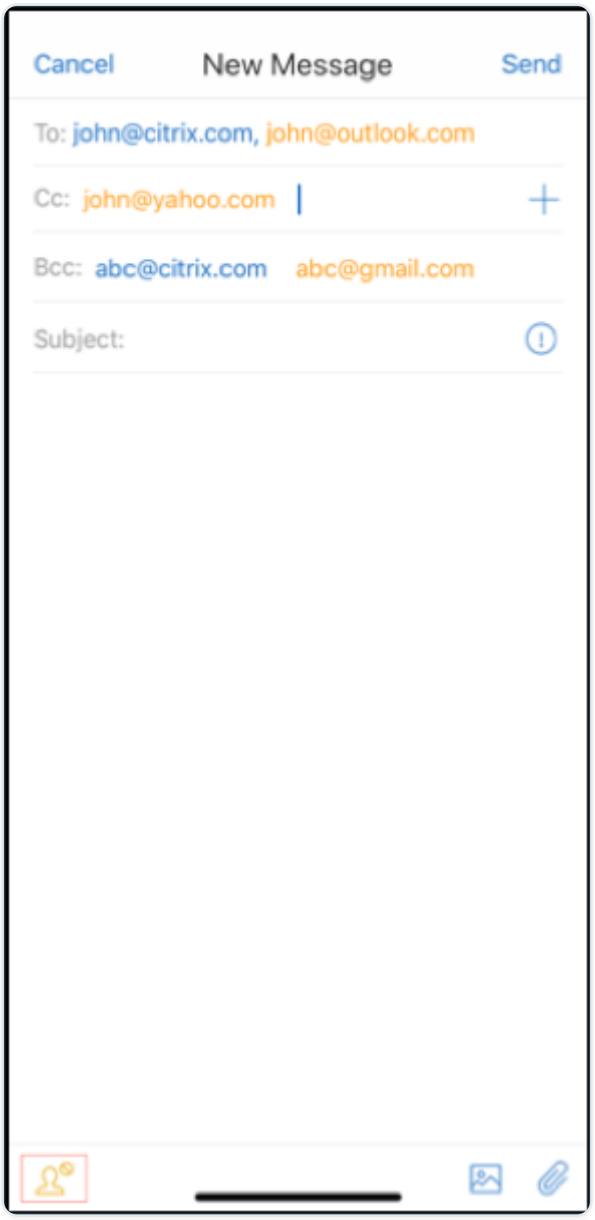
有关管理您的源的更多信息，请参阅 管理您的源。

适用于 iOS 和 Android 的 Secure Mail

内部域。 您可以识别和编辑属于外部组织的电子邮件收件人。要使用此功能，请确保您已在 Citrix Endpoint Management 中启用**内部域**策略。

当您创建、回复或转发电子邮件时，外部收件人会在邮件列表中突出显示。**联系人**图标会作为警告显示在屏幕左下角。点击**联系人**图标以修改邮件列表。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



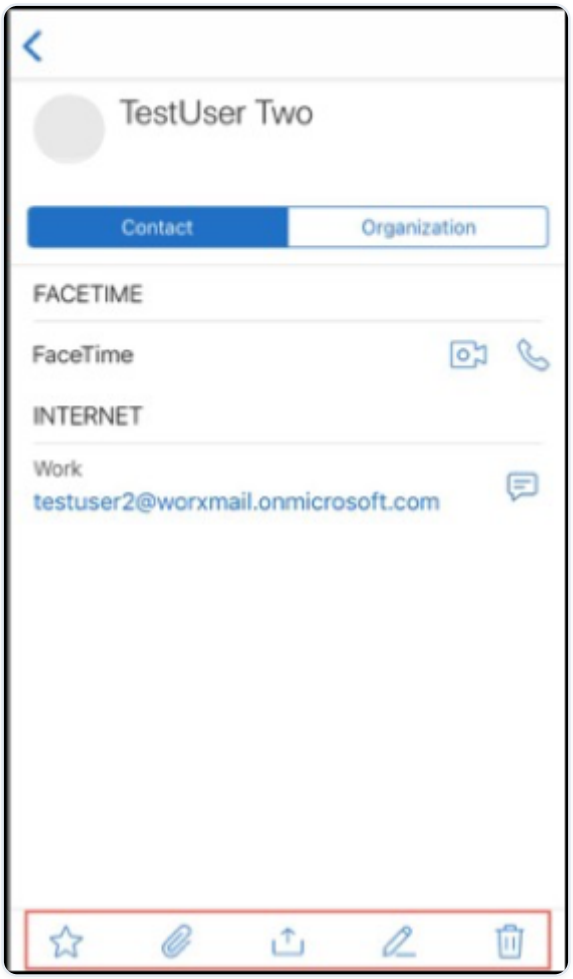
有关内部域的更多信息，请参阅内部域。

人体工程学改进。操作按钮已从屏幕顶部移至底部，以便于访问。这些更改已应用于收件箱、日历和联系人屏幕。

注意：

对于运行 Android 的设备，这些更改已应用于**收件箱**和**日历**屏幕。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



有关人体工程学改进的更多信息，请参阅人体工程学改进。

安全邮件 19.2.0

适用于 iOS 的 Secure Mail

此版本包括性能增强和错误修复。

有关已修复问题和已知问题的列表，请参阅已知和已修复问题。

适用于 Android 的 Secure Mail

- **联系人增强功能。在适用于 Android 的 Secure Mail 中，当您点击联系人**并选择一个联系人时，该联系人的详细信息将显示在**联系人**选项卡下。当您点击**组织**选项卡时，将显示组织层次结构详细信息，例如**经理**、**直接下属**和**同事**。当您点击屏幕右上角的更多图标时，将显示以下选项：
    - **附加到邮件**
    - **共享**
    - **删除**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在“**组织**”选项卡中，点击“**经理**”、“**直接下属**”或“**同事**”右侧的更多图标。然后，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“**同事**”的详细信息。

先决条件：

确保您的 Exchange Server 上已启用 Exchange Web Services (EWS)。

联系人详细信息根据从 Active Directory 中获取的组织详细信息显示。要使联系人显示正确的详细信息，请确保您的管理员已在 Active Directory 中配置了您的组织层次结构。

> **注意：**
>
> IBM Lotus Notes 服务器不支持此功能。

- **网络访问策略**。在适用于 Android 的 Secure Mail 中，网络访问 MDX 策略中新增了一个名为“**隧道 - Web SSO**”的选项。配置此策略可让您灵活地通过“隧道 - Web SSO”和安全票证颁发机构 (STA) 并行隧道传输内部流量。您还可以允许“隧道 - Web SSO”连接用于身份验证服务，例如 NTLM、Okta 和 Kerberos。首次配置 STA 时，必须将服务地址的各个 FQDN 和端口添加到后台网络服务策略中。但是，如果配置“**隧道 - Web SSO**”选项，则无需进行这些配置。

要在 Citrix Endpoint Management 控制台中为适用于 Android 的 Secure Mail 启用此策略：

1. 下载并使用适用于 Android 的 .mdx 文件。有关详细信息，请参阅 添加 MDX 应用程序 中的步骤。
2. 在网络访问策略中，单击“**隧道 - Web SSO**”选项。有关详细信息，请参阅 应用程序网络访问

适用于 iOS 的 Secure Mail 19.1.6

此版本包括性能增强和错误修复。

安全邮件 19.1.5

从本版本开始，Secure Mail 支持以下服务器：

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

有关 Secure Mail 服务器兼容性完整列表的更多信息，请参阅 Secure Mail 概述。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 19.1.0

适用于 iOS 的 Secure Mail

- **联系人增强功能。** 在适用于 iOS 的 Secure Mail 中，当您点击**联系人**并选择一个联系人时，该联系人的详细信息将显示在**联系人**选项卡下。当您点击**组织**选项卡时，将显示组织层次结构详细信息，例如**经理**、**直接下属**和**同事**。当您点击屏幕右上角的更多图标时，将显示以下选项：

  - 编辑
  - 添加到 VIP
  - 取消

  在**组织**选项卡中，您可以点击**经理**、**直接下属**或**同事**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：字段会自动填充经理**、**直接下属**或**同事**的详细信息。您可以撰写并发送电子邮件。

  先决条件：

  确保您的 Exchange Server 上已启用 Exchange Web Services (EWS)。

  联系人详细信息根据从 Active Directory 中获取的组织详细信息（Outlook 联系人）显示。要使您的联系人显示正确的详细信息，请确保您的管理员已在 Active Directory 中配置了您的组织层次结构。

  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到您的本机日历。** 在 Secure Mail for iOS 中，**导出日历** MDX 策略中添加了一个新值 **会议时间、地点**。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到您的本机日历。
- Secure Mail for iOS 支持在运行 Microsoft Enterprise Mobility + Security (EMS)/Intune 并使用现代身份验证 (O365) 的设置上进行富推送通知。

  要启用富推送通知功能，请确保满足以下先决条件：

  - 在 Endpoint Management 控制台中，将 **推送通知** 设置为“开”。
  - **网络访问策略** 设置为 **无限制**。
  - **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**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Secure Mail 用户可以使用 Zoom 应用程序加入会议。有关配置使用 Zoom 应用程序所需策略的信息，请参阅从日历加入会议。
- 此版本支持 iPad Pro 11 英寸和 iPad Pro 12.9 英寸。

适用于 Android 的 Secure Mail

- **附件增强功能。** 在 Secure Mail for Android 中，查看附件的操作已简化。为了获得更好的体验，已删除不必要的步骤，同时保留了早期版本中存在的附件选项。

  您可以在 Secure Mail 应用程序中查看附件。如果附件可以使用 Secure Mail 查看，则会直接打开。如果附件无法使用 Secure Mail 查看，则会显示应用程序列表。您可以选择所需的应用程序来查看附件。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。有关配置使用 Zoom 应用程序所需策略的信息，请参阅从日历加入会议。
- **将会议时间和地点导出到您的本机日历。** 在 Secure Mail for Android 中，**导出日历** MDX 策略中添加了一个值 **会议时间、地点**。这允许您将 Secure Mail 日历事件的会议时间和地点导出到您的本机日历。

注意：

对 Android 5.x 的支持已于 December 31, 2018 结束。

安全邮件 18.12.0

此版本包括性能增强和错误修复。

有关已修复问题和已知问题的列表，请参阅 已知和已修复问题。

安全邮件 18.11.5

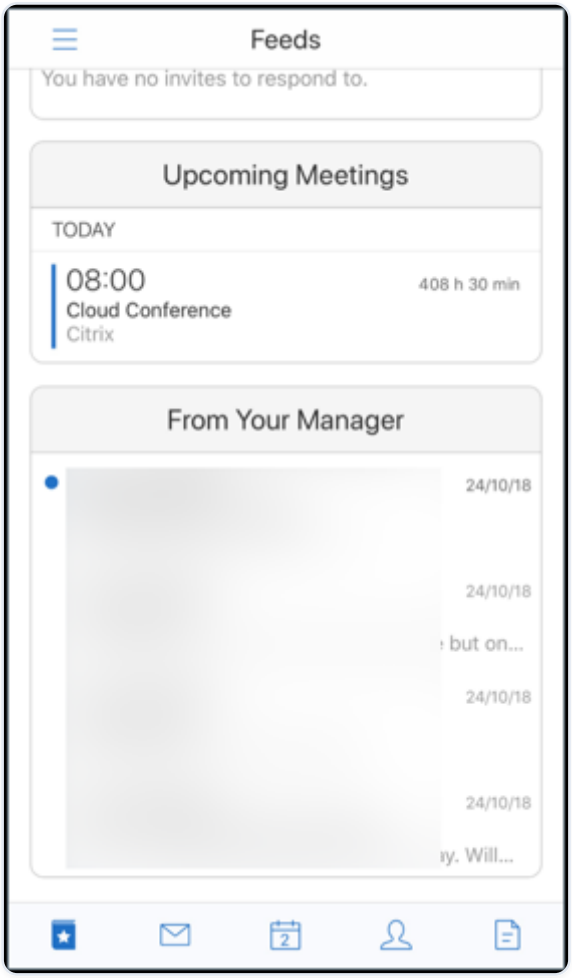
适用于 Android 的 Secure Mail

- **使用 ActiveSync 标头报告网络钓鱼电子邮件。** 在适用于 Android 的 Secure Mail 中，当用户报告网络钓鱼邮件时，将生成一个 EML 文件作为该邮件的附件。管理员会收到此邮件，并可以查看与所报告邮件关联的 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“**通过附件报告**”。管理员在 Citrix Endpoint Management 控制台中配置这些设置。有关为 Secure Mail 配置 MDX 策略的详细信息，请参阅 适用于移动生产力应用程序的 MDX 策略。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **打印电子邮件和日历事件。** 在适用于 Android 的 Secure Mail 中，您可以从 Android 设备打印电子邮件和日历事件。此打印功能使用 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。
- **来自经理的源。** 在适用于 Android 的 Secure Mail 中，您可以在“**源**”屏幕中查看来自经理的电子邮件。根据您的“**同步邮件周期**”设置，最多五封电子邮件会显示在“**来自您的经理**”源下。要查看来自经理的更多电子邮件，请点击“**查看全部**”。



先决条件：

确保在您的 Exchange Server 上启用了 Exchange Web Services (EWS)。

经理卡片根据从 Active Directory 中获取的组织详细信息（Outlook 联系人）显示。要使正确的详细信息显示在经理源中，请确保您的管理员已在 Active Directory 中配置了您的组织层次结构。

注意：

此功能在 IBM Lotus Notes 服务器上不受支持。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 18.11.1

重要提示：

以下问题已在 Secure Mail for Android 18.11.1 中修复

在连接到 IBM Notes Traveler 9.0.1 SP 10 的 Secure Mail for Android 中，带附件的电子邮件仍保留在发件箱中。

安全邮件 18.11.0

适用于 Android 的安全邮件

- **子文件夹通知。** 在 Secure Mail for Android 中，您可以从邮件帐户的子文件夹接收邮件通知。有关详细信息，请参阅子文件夹通知。
- **Secure Mail for Android 后台服务更新。** 为满足在运行 Android 8.0（API 级别 26）或更高版本的设备上 Google Play 后台执行限制的要求，我们已升级 Secure Mail 后台服务。为了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

请确保您已在设备上的 Secure Mail 设置中启用**邮件通知**。

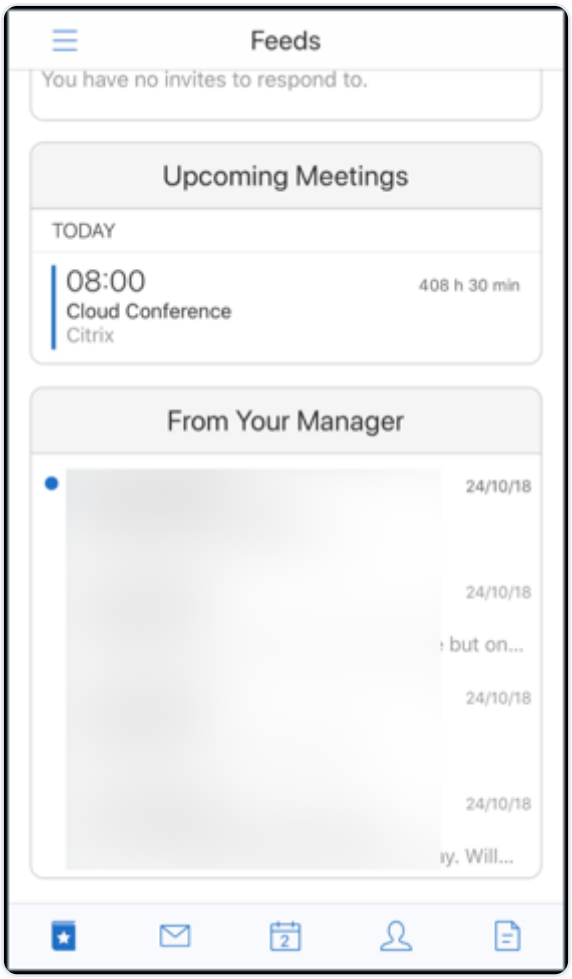
限制：

- 如果您尚未启用基于 FCM 的推送通知，后台同步每 15 分钟进行一次。此间隔因应用程序是在后台还是前台运行而异。
- 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。

适用于 iOS 的安全邮件

- **支持 iOS 12.1。** 适用于 iOS 的 Secure Mail 支持 iOS 12.1 版。
- **富推送通知失败消息的增强功能。** 在适用于 iOS 的 Secure Mail 中，设备上的通知中心会根据通知失败的类型显示相应的推送通知失败消息。有关详细信息，请参阅 适用于 iOS 的 Secure Mail 中的推送通知失败消息。
- **来自经理的动态。** 在适用于 iOS 的 Secure Mail 中，您可以在“**动态**”屏幕中查看来自经理的电子邮件。根据您的“**同步邮件周期**”设置，最多有五封电子邮件显示在“**来自您的经理**”动态下。要查看更多来自经理的电子邮件，请点击“**查看全部**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



先决条件：

确保在您的 Exchange Server 上启用了 Exchange Web Services (EWS)。

经理卡片根据从 Active Directory 获取的组织详细信息（Outlook 联系人）显示。要使正确详细信息显示在经理动态中，请确保您的管理员已在 Active Directory 中配置了您的组织层次结构。

注意：

IBM Lotus Notes 服务器不支持此功能。

安全邮件 18.10.5

- **Secure Mail 与 Slack 集成（预览版）：** 您现在可以将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 集成（预览版）。
- **动态文件夹的增强功能：** 在适用于 iOS 的 Secure Mail 中，现有动态文件夹的增强功能如下：
  - 在您的动态卡片中查看最多五场即将召开的会议。
  - 未来 24 小时内的即将召开的会议将显示在动态卡片中，并分为“**今天**”和“**明天**”部分。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 18.10.0

- **Secure Mail 邮件和日历通知渠道：** 在运行 Android O 或更高版本的设备上，您可以使用通知渠道设置来管理电子邮件和日历通知的处理方式。此功能允许您自定义和管理通知。有关详细信息，请参阅通知渠道。
- **报告网络钓鱼电子邮件（作为转发）：** 在适用于 iOS 的 Secure Mail 中，您可以使用“报告为网络钓鱼”功能来报告您怀疑是网络钓鱼的电子邮件（作为转发）。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**网络钓鱼报告机制**设置为**通过转发报告**。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章报告网络钓鱼电子邮件。

安全邮件 18.9.0

- 新版本编号方案，格式为“yy.mm.version”。例如，版本 **18.9.0**
- **报告网络钓鱼电子邮件（作为转发）：** 在适用于 Android 的 Secure Mail 中，您可以使用“报告为网络钓鱼”功能来报告您怀疑是网络钓鱼的电子邮件（作为转发）。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，并将网络钓鱼报告机制设置为**通过转发报告**。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章报告网络钓鱼电子邮件。
- **Feed 卡增强功能：** 在适用于 Android 的 Secure Mail 中，对现有 **Feeds** 文件夹进行了以下增强：
  - 所有自动同步文件夹中的会议邀请都会显示在您的 Feed 卡中。
  - 在您的 Feed 卡中查看最多五个即将召开的会议。
  - 即将召开的会议现在根据从当前时间开始的 24 小时周期显示。这些会议邀请分为**今天**和**明天**。 在以前的版本中，直到当天结束的即将召开的会议会显示在您的 Feed 中。
- **导出 Secure Mail 日历事件：** 适用于 Android 和 iOS 的 Secure Mail 允许您将 Secure Mail 日历事件导出到设备的本机日历应用。要启用此功能，请轻按**设置**并将“导出日历事件”滑块向右拖动。有关详细信息，请参阅导出 Secure Mail 日历事件。

安全邮件 10.8.65

- **适用于 iOS 12：** 在适用于 iOS 的 Secure Mail 中，我们支持“分组通知”功能。借助此功能，对话会从邮件线程中分组。您可以在设备的锁定屏幕上快速浏览分组通知。“分组通知”设置在设备上默认启用。
- 在适用于 iOS 的 Secure Mail 中，**保存草稿**和**删除草稿**按钮更大。此增强功能使客户更容易区分这两个选项。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 在适用于 iOS 的 Secure Mail 中，通过在设备**设置**中启用 Secure Mail 来电显示来识别来自联系人的来电。启用这些设置后，当您接到呼入电话时，设备会显示应用名称和来电显示，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。

安全邮件 10.8.60

- 安全邮件支持 Android P。
- Secure Mail 现已提供波兰语版本。
- 在适用于 iOS 的 Secure Mail 中，您可以从 iOS 本机文件应用将文件附加到电子邮件。有关详细信息，请参阅 iOS 功能。

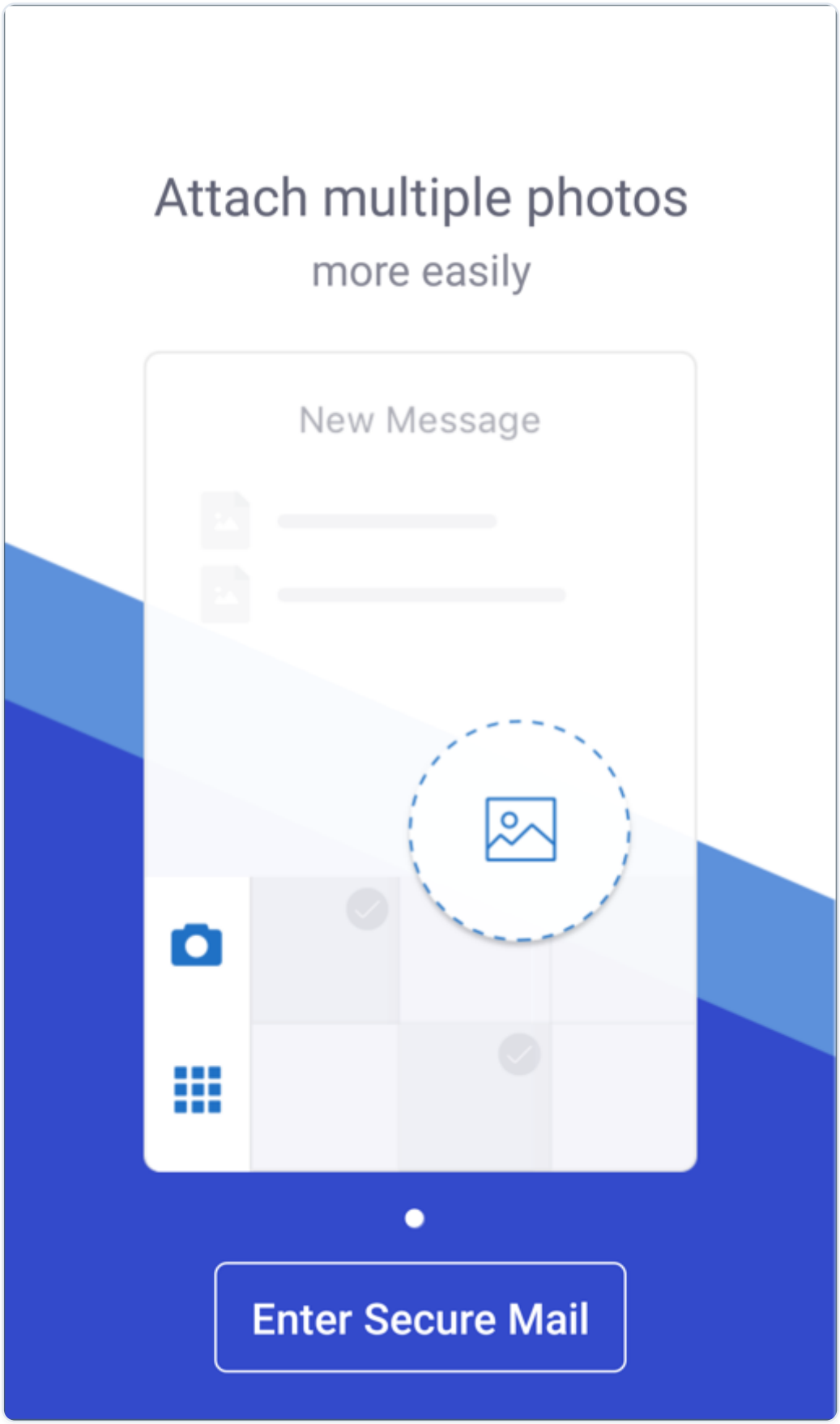
安全邮件 10.8.55

Secure Mail 10.8.55 版本中没有新功能。有关已修复的问题，请参阅 已知和已修复的问题。

安全邮件 10.8.50

照片附件改进。在适用于 iOS 的 Secure Mail 中，您可以通过点击新的“**图库**”图标轻松附加照片。点击“**图库**”图标并选择要附加到电子邮件的照片。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Secure Mail 源屏幕。适用于 iOS 和 Android 的 Secure Mail 在“**源**”屏幕中显示所有未读电子邮件、需要您关注的会议邀请以及即将召开的会议。

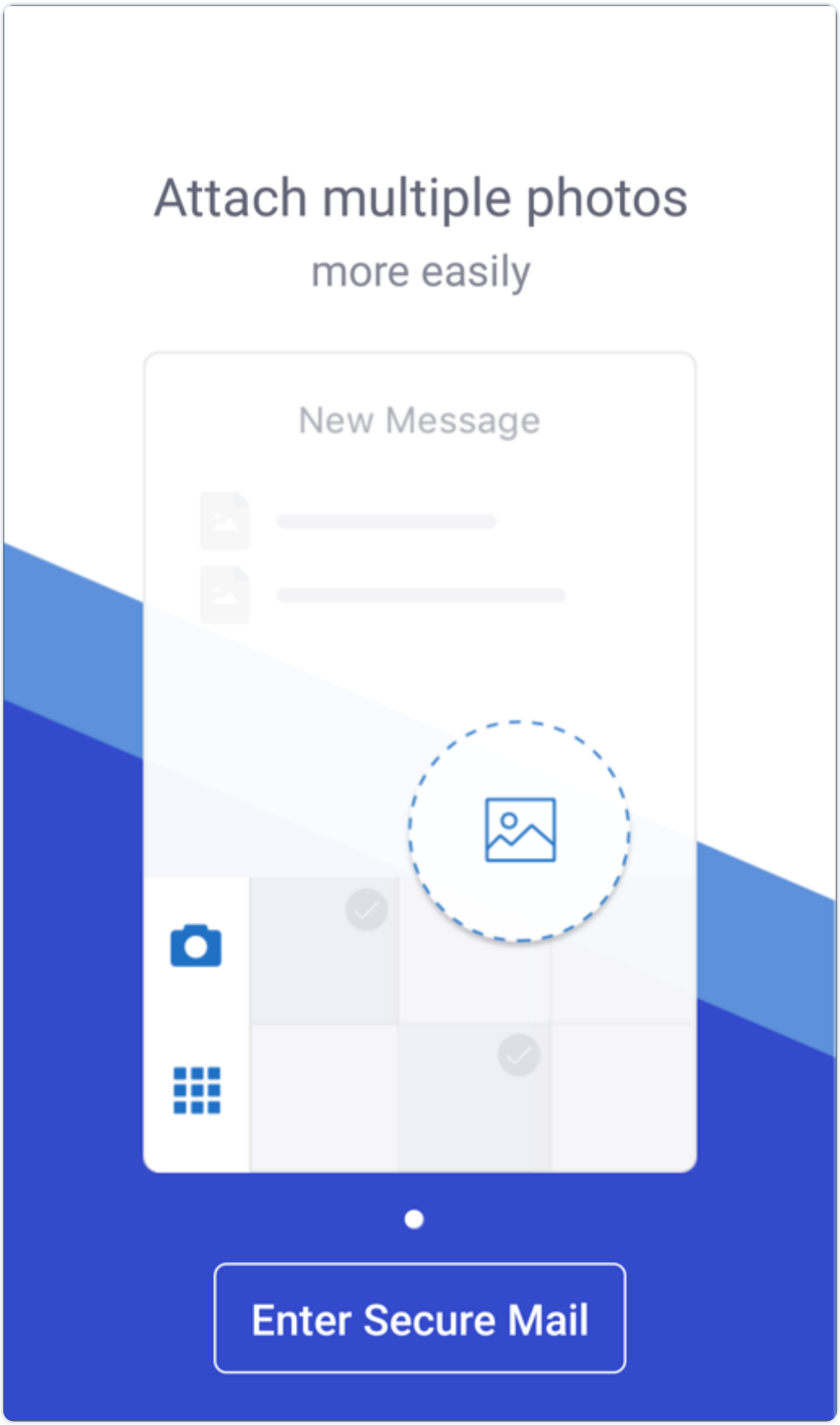
© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 10.8.45

文件夹同步。在适用于 iOS 和 Android 的 Secure Mail 中，您可以点击“**同步**”图标以刷新所有 Secure Mail 内容。“**同步**”图标位于 Secure Mail 的侧滑菜单中，例如“邮箱”、“日历”、“联系人”和“附件”。当您点击“**同步**”图标时，您已配置为自动刷新的文件夹（例如“邮箱”、“日历”、“联系人”）将进行更新。上次同步的时间戳显示在“**同步**”图标旁边。

照片附件改进。在适用于 Android 的 Secure Mail 中，您可以通过点击新的“**图库**”图标轻松附加照片。点击“**图库**”图标并选择要附加到电子邮件的照片。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

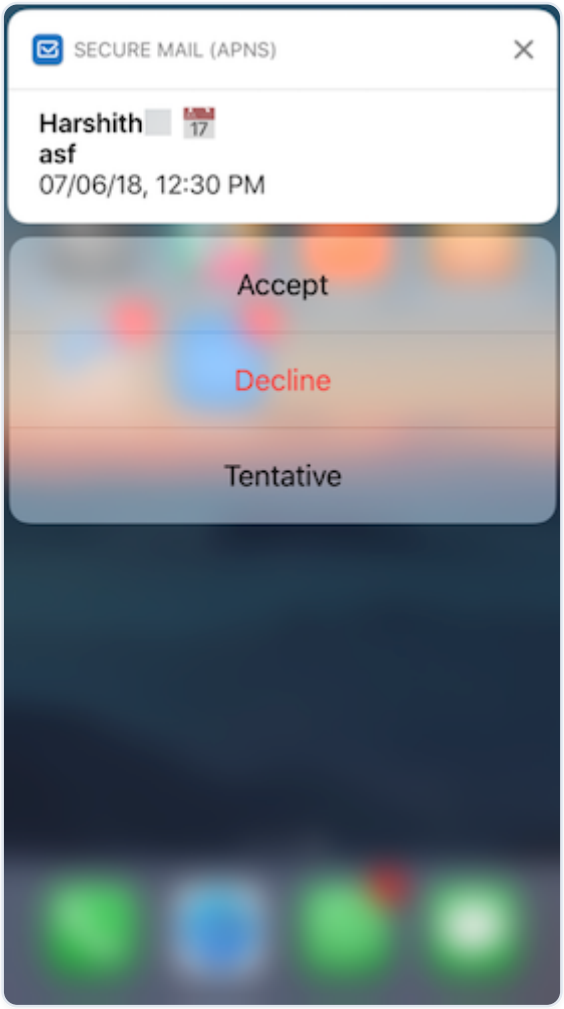
安全邮件 10.8.40

支持搜索日历。在适用于 iOS 的 Secure Mail 中，您可以搜索日历中的事件、与会者或任何其他文本。

安全邮件 10.8.35

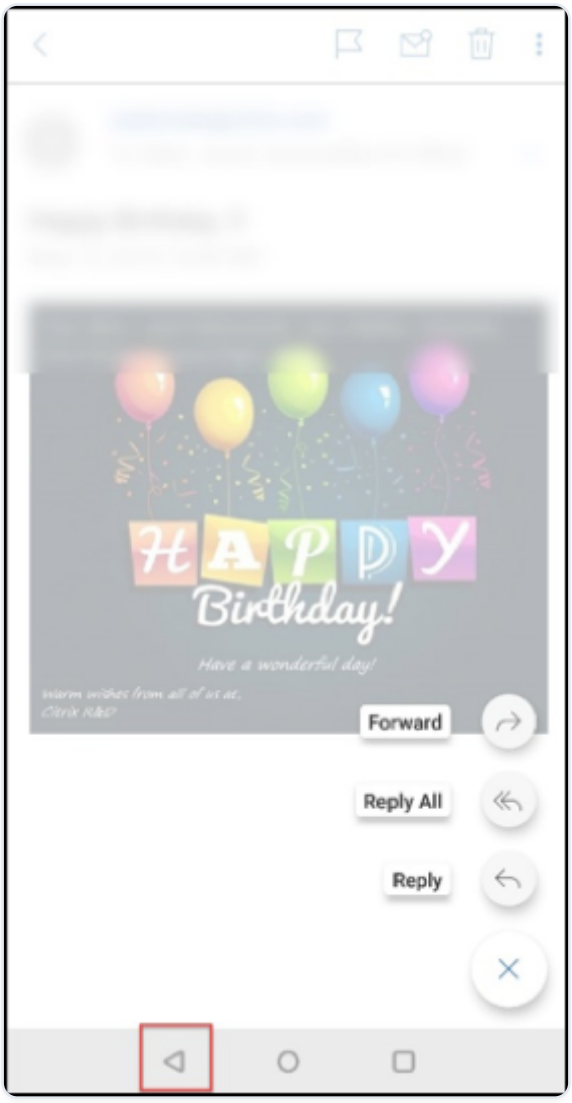
iOS 版 Secure Mail 的版本是 10.8.36。

- **通知响应选项。** 在 iOS 版 Secure Mail 中，用户可以响应会议通知，例如“接受”、“拒绝”和“暂定”。他们可以使用“回复”和“删除”来响应邮件通知。



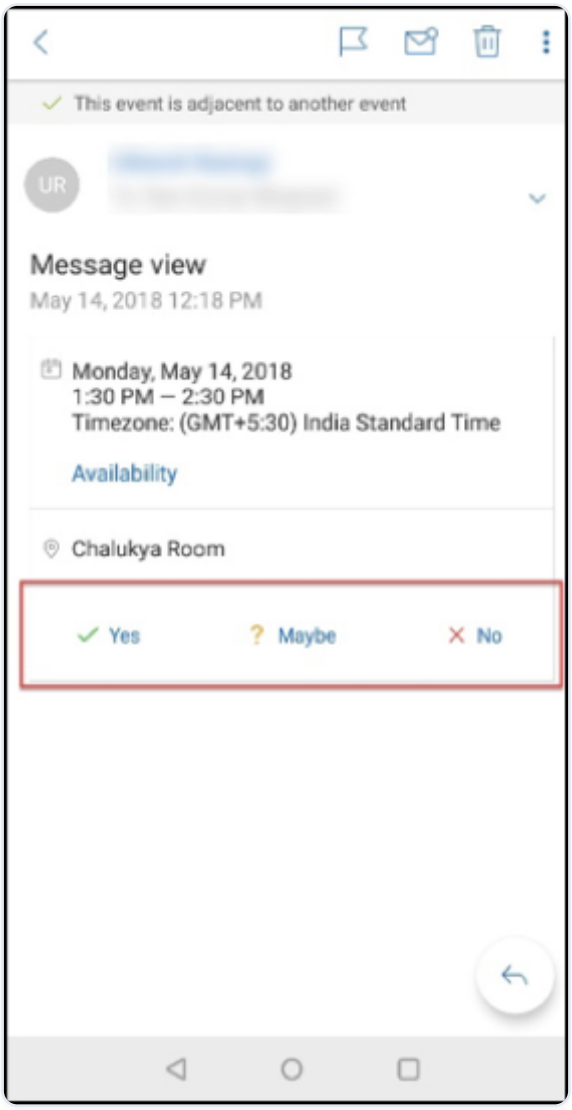
- **Android 版 Secure Mail 返回按钮增强功能。** 在 Android 版 Secure Mail 中，您可以点击设备上的返回按钮以关闭浮动操作按钮的展开选项。如果浮动操作按钮处于展开状态，点击设备上的返回按钮会收起响应选项。此操作会将您带回邮件或事件详细信息视图。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **在 Android 版 Secure Mail 中，会议响应按钮显示在电子邮件中。** 当您收到有关会议邀请的电子邮件通知时，可以通过点击以下选项之一来响应邀请：
  - 是
  - 也许
  - 否

© 1997–2026 Citrix Systems, Inc. All rights reserved.



安全邮件 10.8.25

iOS 版 Secure Mail 现在支持 S/MIME 派生凭据： 要使此功能正常工作，您需要执行以下操作：

- 选择“派生凭据”作为 S/MIME 证书源。有关详细信息，请参阅 iOS 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}`

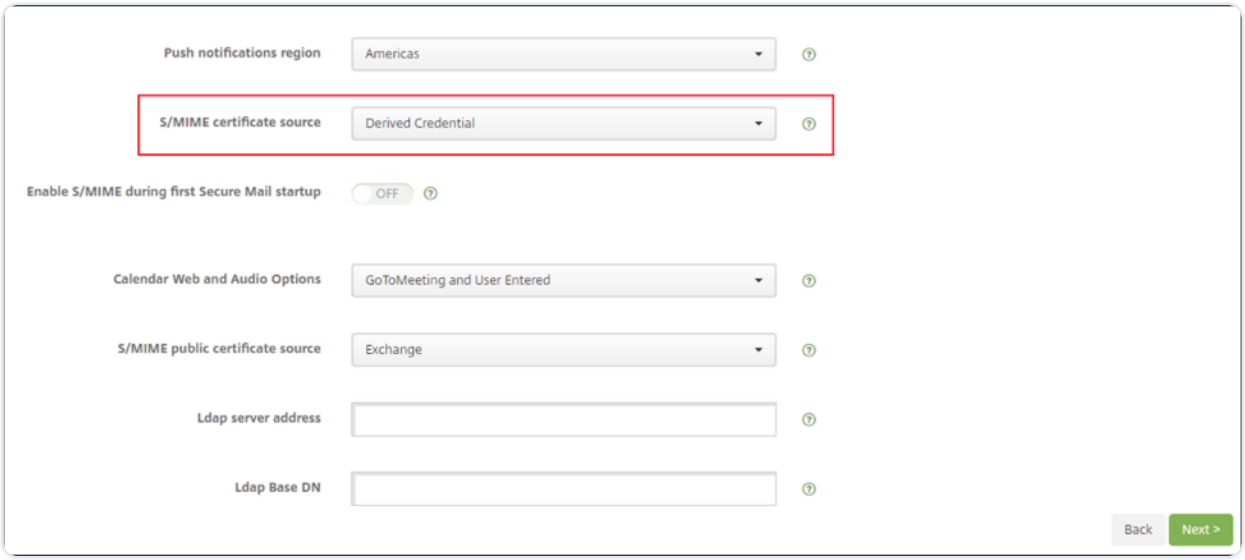
有关如何添加客户端属性的步骤，对于 XenMobile Server，请参阅客户端属性，对于 Endpoint Management，请参阅客户端属性。

有关设备在使用派生凭据时如何注册的更多信息，请参阅使用派生凭据注册设备。

1. 在您的 Endpoint Management 控制台中，导航到 **Configure > Apps**。

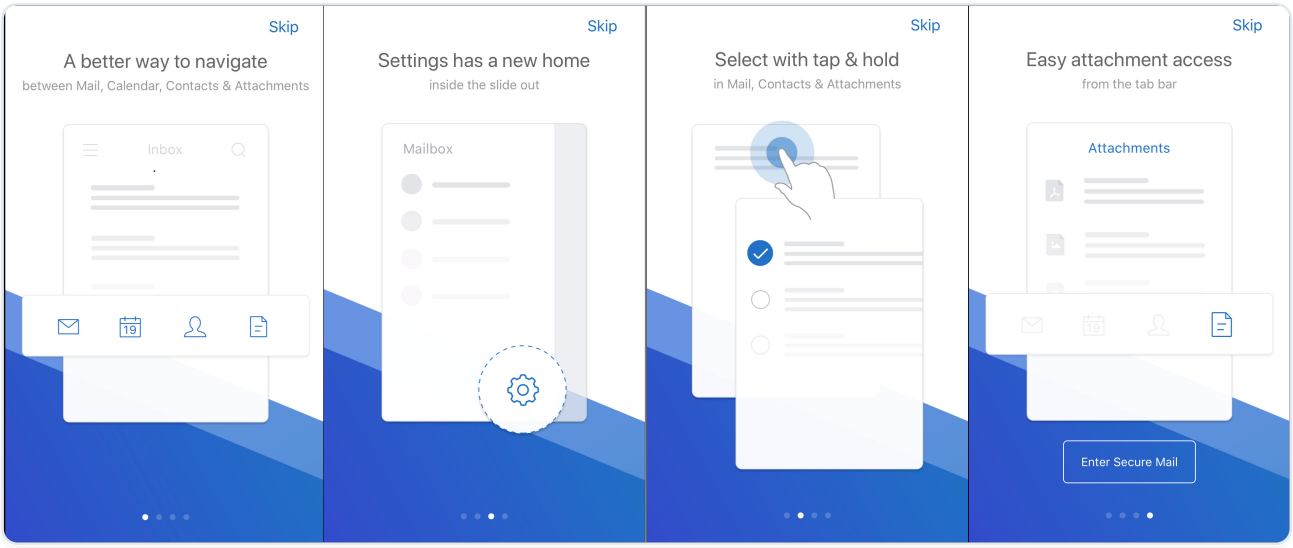
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 选择 **Secure Mail**，然后单击**编辑**。
3. 在 iOS 平台下，对于 S/MIME 证书源，选择**派生凭据**。



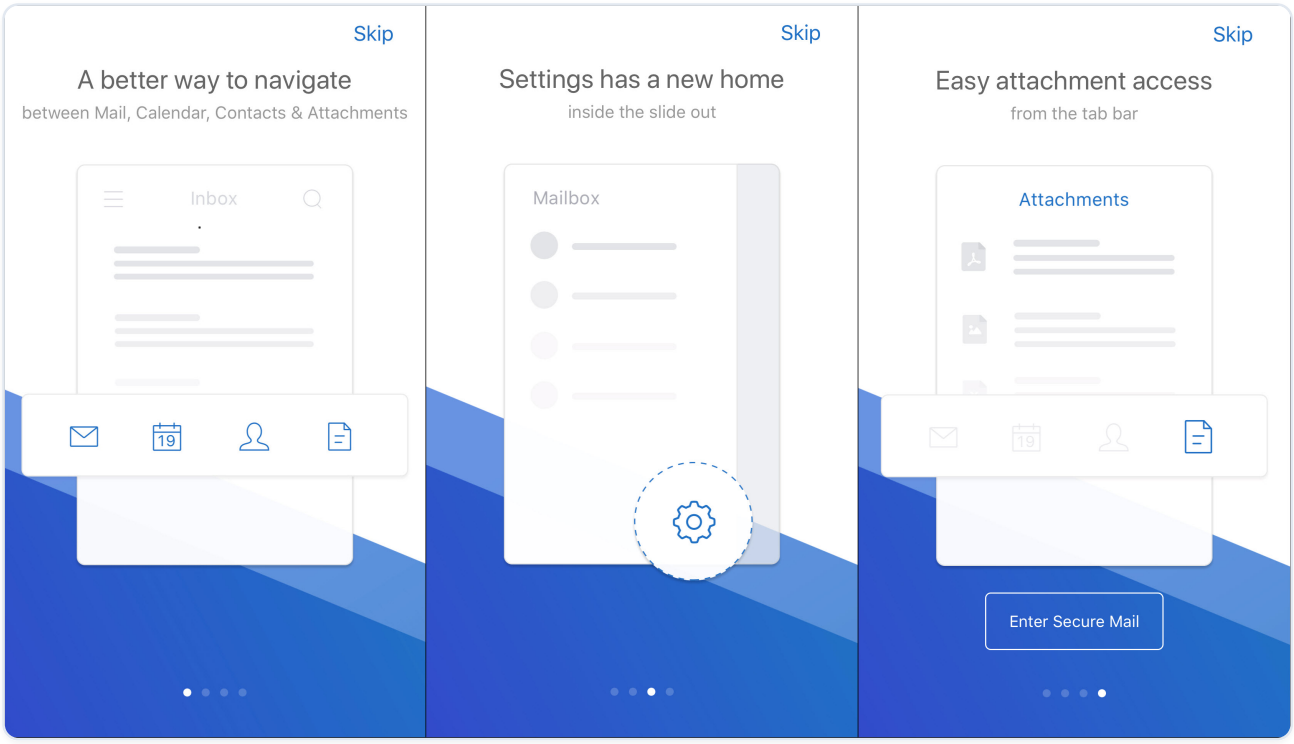
Secure Mail for iOS 和 Android 焕然一新： 我们使用户导航更简单、更高效。我们以导航栏的形式重新排列了菜单和操作按钮。

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。

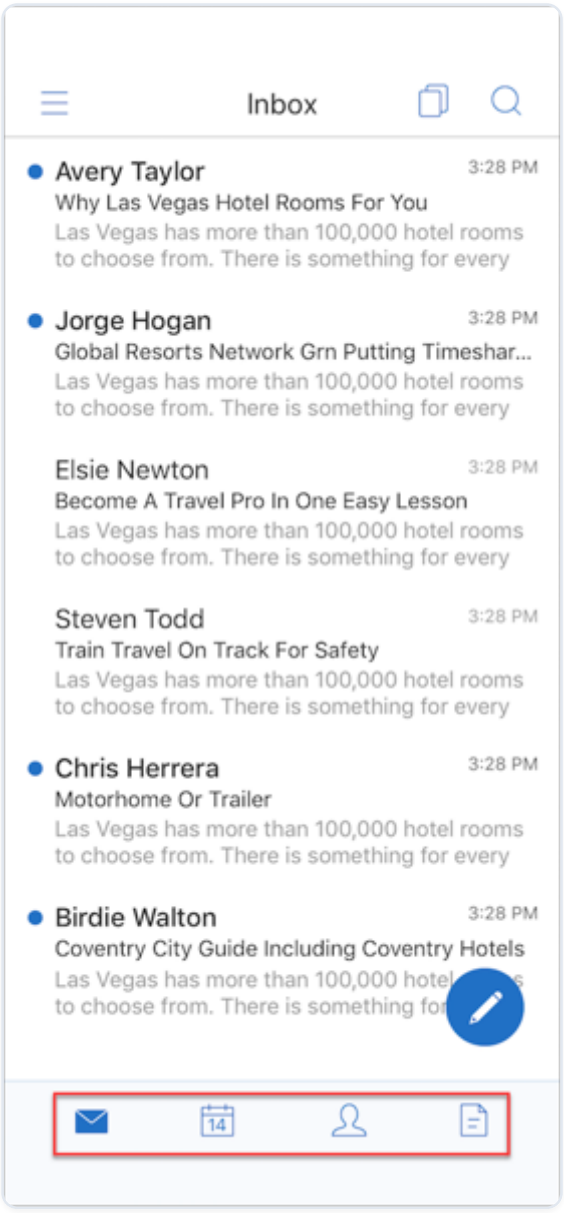
© 1997–2026 Citrix Systems, Inc. All rights reserved.



更改内容：

- 抓取器图标已删除。Secure Mail 功能（例如“邮件”、“日历”、“联系人”和“附件”）现在作为按钮显示在底部选项卡栏中。下图显示了此更改。

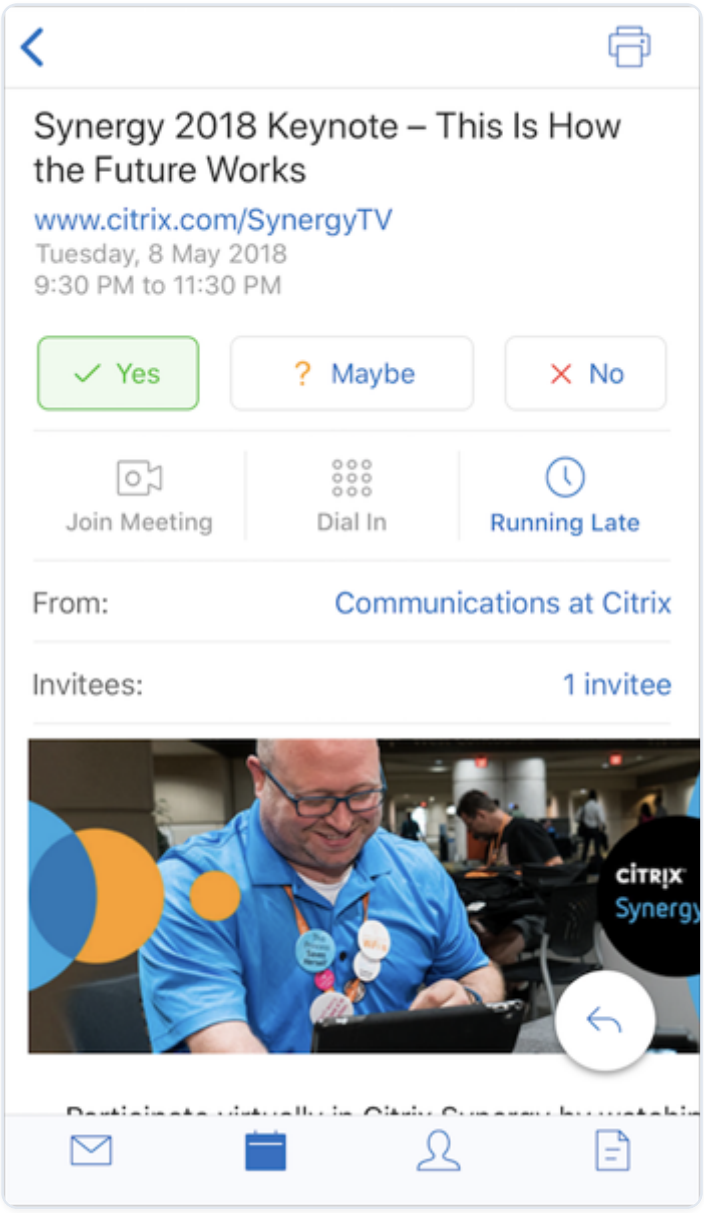
© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意：

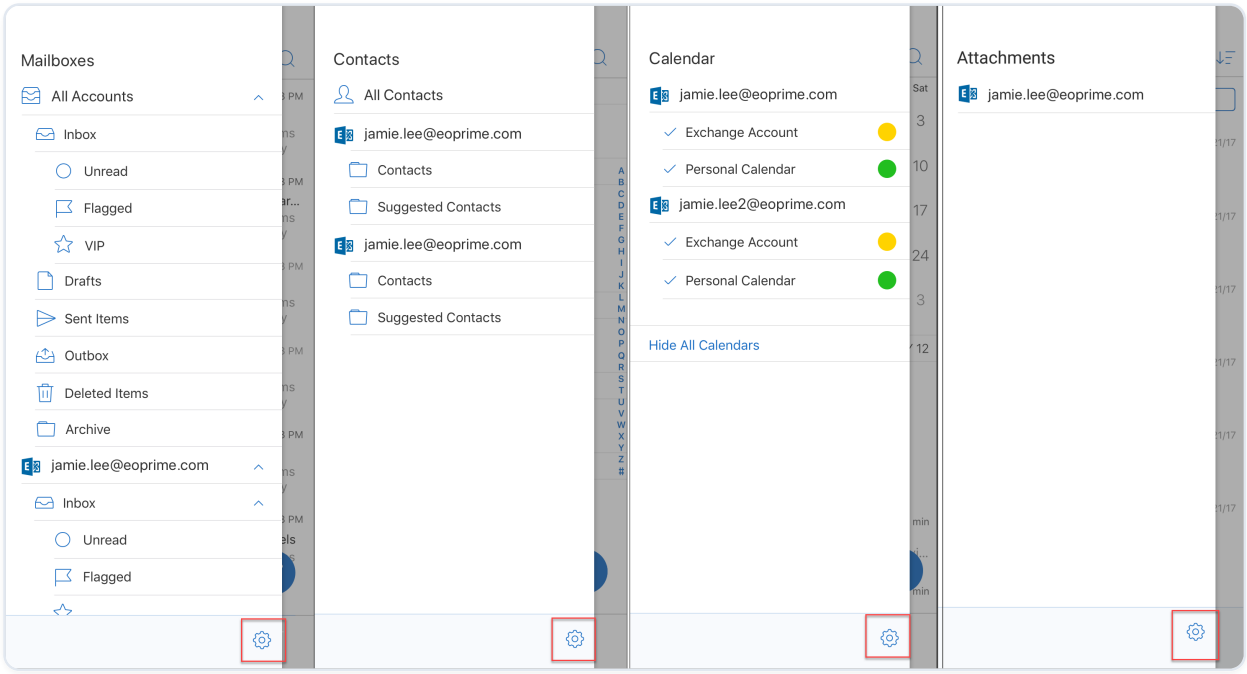
在 Android 设备上，打开邮件项目后，页脚选项卡栏不可用。例如，如下图所示，如果您打开电子邮件或日历事件，页脚选项卡栏将不可用。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

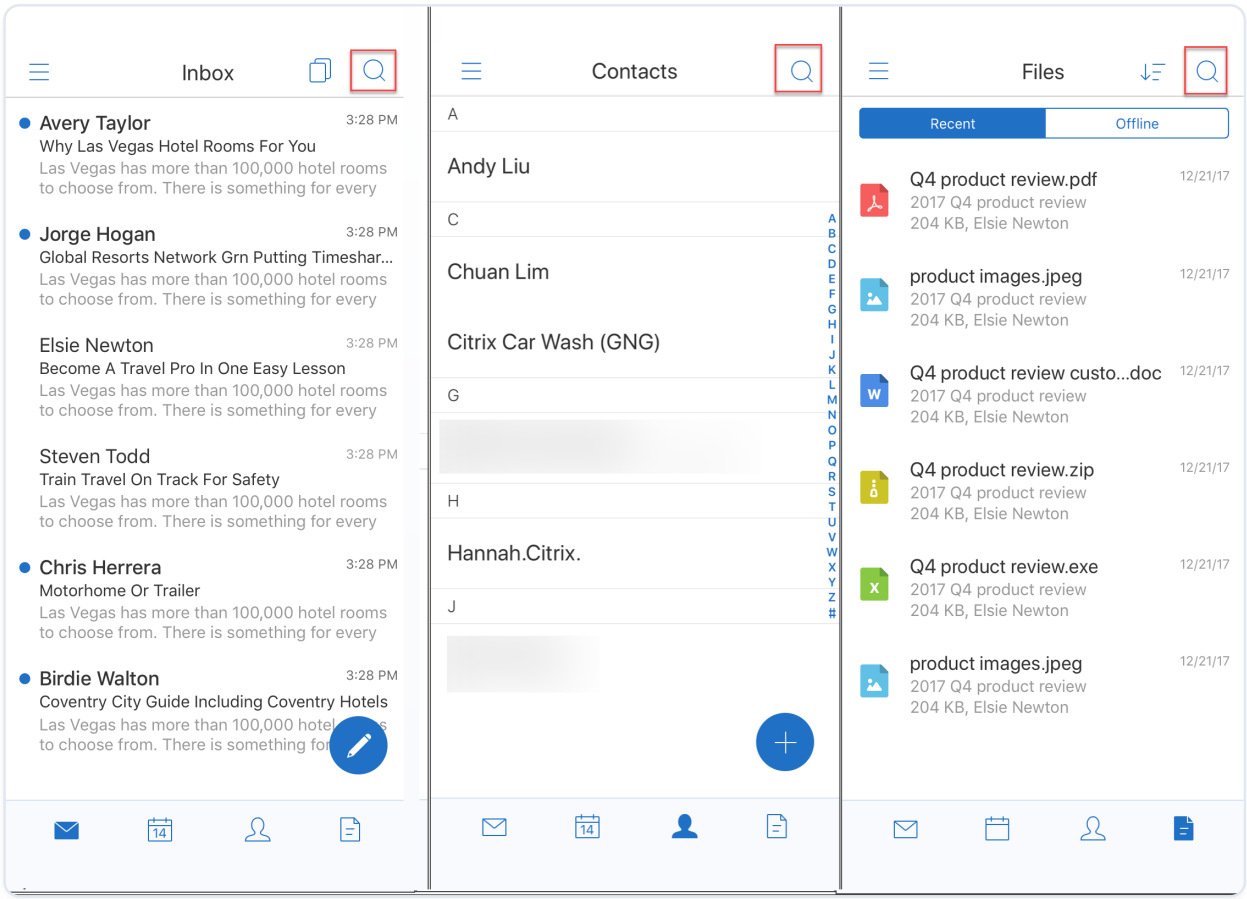


- **设置**菜单在所有菜单中都可用，例如邮件、日历、联系人和附件。要转到**设置**，请点击汉堡图标，然后点击右下角的设置按钮，如下图所示。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

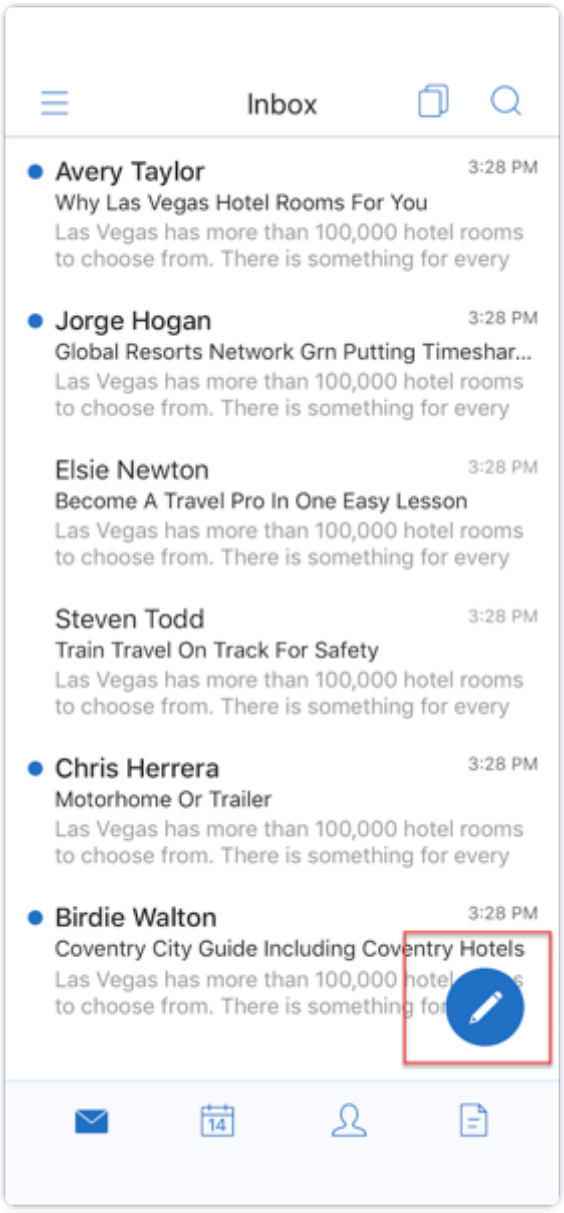


- **搜索**图标取代了搜索栏，可在收件箱、联系人和附件视图中使用。



- 在 iOS 设备上，您可以轻触并按住邮件项目以选择该项目。
- 您可以点击**撰写**浮动操作按钮来撰写新电子邮件，如下图所示。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- 以下菜单选项现在可在屏幕右上角使用：
  - **同步选项：** 点击右上角的溢出图标，然后导航到**更多选项 > 同步**选项以更改您的同步首选项。

    注意：

    此选项仅适用于 Android 设备。

  - **搜索图标：** 点击以搜索电子邮件。
- **分类视图图标：** 点击以查看对话的分类视图。
- **响应浮动操作按钮：** 在查看电子邮件时，点击可转发、全部回复或回复，如下图所示。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

响应浮动操作按钮的图像(/en-us/mobile-productivity-apps/media/inbox-respond-fab-and-actions.png)

- 在查看电子邮件时，屏幕右上角提供以下菜单选项：
  - **标记：** 点击以标记电子邮件。
  - **标记为未读：** 点击以将电子邮件标记为未读。
  - **删除：** 点击以删除电子邮件。
  - **更多选项：** 点击溢出图标以查看其他可用操作，例如“移动”。

日历更改

- 在日历中，您可以点击事件浮动操作按钮以创建事件，如下图所示。

  日历浮动操作按钮的图像(/en-us/mobile-productivity-apps/media/calendar-fab.png)
- 屏幕右上角现在提供以下菜单选项：
  - **今天：** 点击以查看今天的事件。
  - **搜索：** 点击以搜索事件。
  - **响应浮动操作按钮：** 查看事件时，点击以转发、全部回复或回复。

  日历响应选项的图像(/en-us/mobile-productivity-apps/media/calendar-response-options.png)

查看事件时，事件响应操作（例如“是”、“可能”和“否”）会重新对齐并显示在事件详细信息下方。

联系人更改

- 您可以点击**创建新联系人**浮动操作按钮，如下图所示。

  创建新联系人图像的图片(/en-us/mobile-productivity-apps/media/contacts-fab.png)
- **搜索**菜单选项现在位于屏幕右上角。您可以点击该选项以搜索联系人。
- 查看联系人时，屏幕右上角提供以下菜单选项：

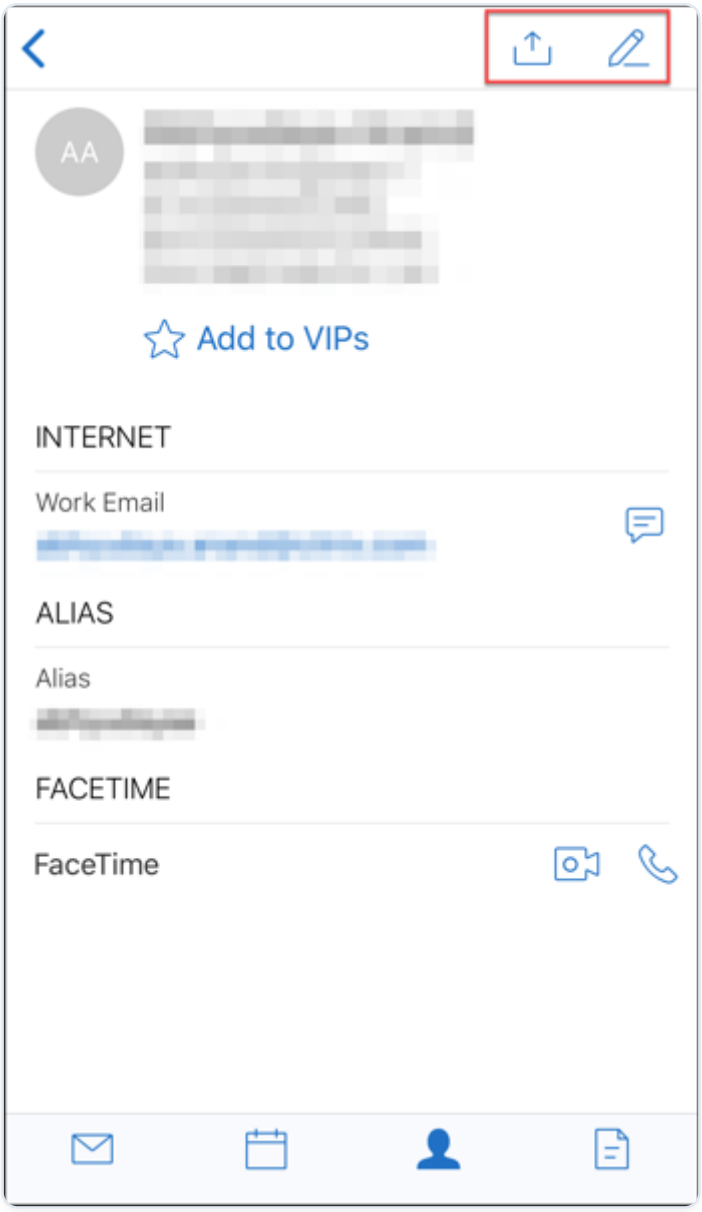
  在 Android 设备上：
  - **编辑：** 点击以编辑联系人。
  - **更多选项：** 点击编辑图标以查看其他可用操作，例如“附加到邮件”、“共享”和“删除”。

  Android 溢出图标的图像(/en-us/mobile-productivity-apps/media/android-contacts-options.png)

  在 iOS 设备上：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

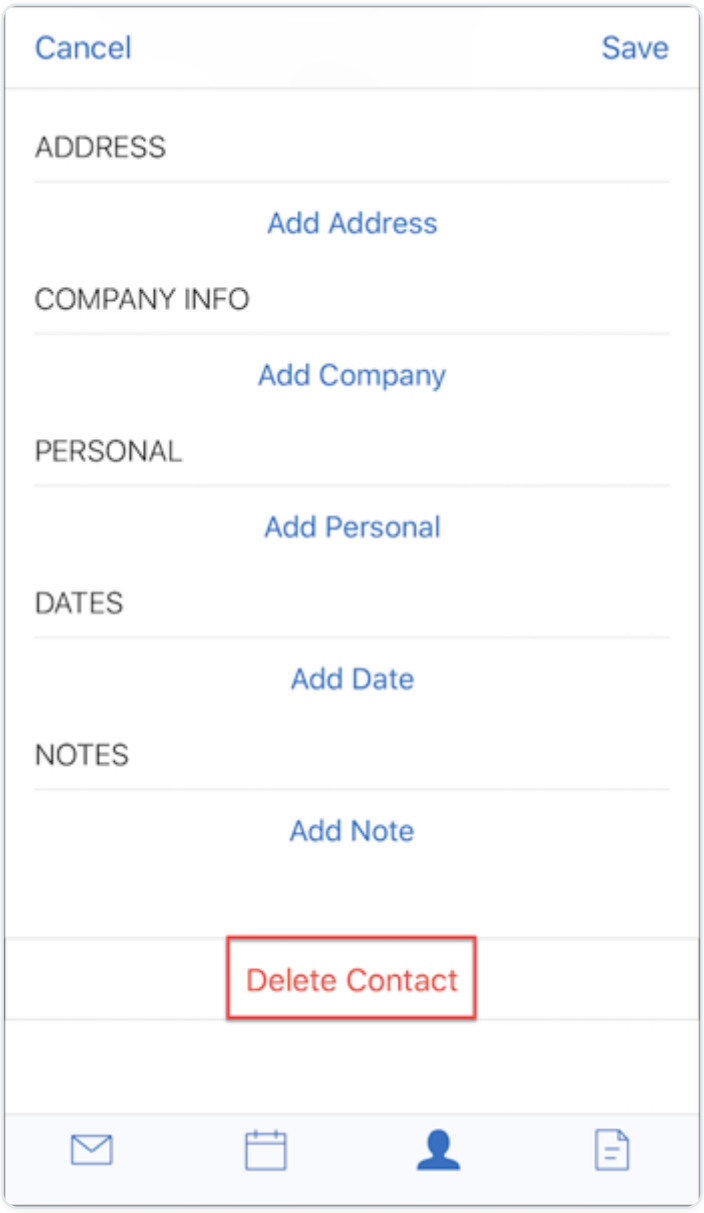
- **编辑：** 点击以编辑联系人。
- **共享：** 点击共享图标以查看其他可用操作，例如“共享联系人”和“附加到邮件”。



注意：

要在 iOS 设备上删除联系人，请选择联系人，点击**编辑**，然后点击屏幕底部的**删除**，如下图所示。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



附件更改

以下附件菜单选项现在可从屏幕右上角获取：

- **排序：点击排序**图标并选择适当的筛选器以对附件进行排序。
- **搜索：**点击以搜索附件。

安全邮件 10.8.20

- 适用于 iOS 的 Secure Mail 现在支持使用派生凭据进行注册和身份验证。有关派生凭据的更多信息，请参阅适用于 iOS 的派生凭据。
- 适用于 iOS 的 Secure Mail 支持富推送通知。富通知可确保即使 Secure Mail 未在后台运行，您也能收到收件箱的锁屏通知。此功能支持基于密码的身份验证和基于客户端的身份验证设置。有关详细信息，请参阅富推送通知。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **注意：**
>
> 由于为支持富推送通知功能而进行的架构更改，**仅限 VIP** 邮件通知不再可用。

- 适用于 iOS 的 Secure Mail 现在支持富文本签名。您可以在电子邮件签名中使用图像或链接。有关详细信息，请参阅富文本签名。

安全邮件 10.8.15

- **适用于 iOS 的 Secure Mail 现在支持富文本签名。** 您可以在电子邮件签名中使用图像或链接。有关详细信息，请参阅富文本签名。
- **Secure Mail 支持 Android Enterprise（以前称为 Android for Work）。** 您可以通过在 Secure Mail 中使用 Android Enterprise 应用程序来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。
- **Secure Mail 在查看电子邮件时呈现嵌入式资源。** 如果资源存在于您的内部网络中（例如，带有内部链接图像 URL 的邮件），Secure Mail 会连接到内部网络以获取内容并进行呈现。
- **Secure Mail 支持现代身份验证。** 现代身份验证是基于 OAuth 令牌的身份验证，使用用户名和密码。此支持包括对 Office 365 的支持，适用于内部和外部 Active Directory 联合身份验证服务 (AD FS) 或身份提供程序 (IdP)。
- **附件存储库的性能增强。** 您可以更快地滚动浏览附件存储库。

安全邮件 10.8.10

- **支持打印电子邮件附件。** 适用于 iOS 的 Secure Mail 支持打印电子邮件附件。
- **使用 Microsoft Office 365 进行现代身份验证。** 适用于 iOS 的 Secure Mail 支持现代身份验证。现代身份验证是基于 OAuth 令牌的身份验证，使用用户名和密码。此支持包括对 Office 365 的支持，适用于外部和内部 Active Directory 联合身份验证服务 (AD FS) 和身份提供程序 (IdP)。有关详细信息，请参阅使用 Microsoft Office 365 进行现代身份验证。

> **注意：**
>
> 此版本不支持与 Microsoft Intune/EMS 集成的 Endpoint Management 的现代身份验证。

此版本在 AD FS 可从外部访问的场景中包含现代身份验证。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已知和已修复的问题

Citrix® 支持从移动生产力应用程序的最近两个版本进行升级。

适用于 iOS 26.8.0 的 Secure Mail

已修复的问题

- 在 iPad 上，电子邮件对话可能只显示最新消息，而较早的消息及其附件在会话中缺失。
- 在 iPad 上，从每周日历视图打开日历项目可能会显示空白屏幕。
- Secure Mail 可能会在运行 iOS 27 的设备上显示白屏。
- 当您将附件共享到另一个应用程序或保存到“文件”时，原始文件名可能会被随机生成的字符串替换。

已知问题

此版本中没有已知问题。

适用于 Android 26.5.0 的 Secure Mail

已修复的问题

- 当邮件服务器上出现 ping 风暴或下载风暴条件导致 HTTP 503 错误时，邮件同步和内容下载可能会失败。
- 适用于 Android 的 Secure Mail 中，网关证书续订可能会失败。
- 由于兼容性问题，Secure Mail 可能无法在 AMAPI 模式下启动。

已知问题

此版本中没有已知问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 iOS 26.5.0 的 Secure Mail

已修复的问题

- 在 iPad 上，Secure Mail 中可能会缺少附件选项。
- 在 iPad 上，HTML 日历邀请正文可能无法在 Secure Mail 中呈现。
- 如果 Secure Hub 未提示重新身份验证，Secure Mail 屏幕可能会闪烁。
- 在首次启动期间，Secure Mail 可能会显示白屏，并且只有在重新启动后才能恢复。
- 在 DEP 设备上执行应用程序擦除时，MDM 配置文件可能不会被删除。

已知问题

此版本中没有已知问题。

适用于 iOS 26.1.0 的 Secure Mail

已修复的问题

- 当 XenMobile 中阻止文本复制时，用户可能仍然可以通过翻译选项复制和粘贴文本。
- 当您尝试使用“**打开方式**”选项打开文件附件时，可能会出现空白文件，并且附件无法打开。
- 在 iPhone 上的 Secure Mail 中尝试打开小附件（小于 1 MB）时，应用程序可能无法打开它们，并显示错误消息：“无法打开附件。”
- 当用户证书过期时，用户可能会收到重复的证书续订提示。
- 当超出最大 PIN 重试限制时，Secure Mail 可能无法恢复。
- 在 Secure Mail 中编辑联系人时，应用程序可能会无响应。
- 使用 Secure Mail 时，应用程序可能会间歇性地显示空白屏幕。
- iPad 上 Secure Mail 中的日历搜索叠加层可能无法正确覆盖背景按钮。

已知问题

此版本中没有已知问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 Android 的 Secure Mail 25.12.0

已修复的问题

- 在已注册的 Android 设备上使用 Secure Mail 时，某些用户有时可能会遇到 Active Directory (AD) 帐户锁定问题。
- 当有效证书已存在时，已注册的 Android 设备可能会收到重复的 Access Gateway (AG) 客户端证书，从而增加 PKI 服务器的负载。
- Secure Mail 推送通知可能不适用于 Android 设备。
- 在适用于 Android 的 Secure Mail 中键入时，滚动可能不起作用。

已知问题

此版本中没有已知问题。

适用于 iOS 的 Secure Mail 25.9.0

已修复的问题

- 在 iPad 上将 Secure Mail 更新到 25.5.0 版本时，某些页面会出现缩放问题，并且显示可能不受支持。
- Secure Mail 可能无法添加 O365 邮件帐户。
- 证书过期后，证书同步和请求可能会失败。
- 从设备中删除 Secure Hub 后，应用程序可能仍然可用。
- 当 AG 会话过期时，Secure Mail 可能无法正常工作。
- 当您使用面容 ID 或触控 ID 解锁设备时，Secure Mail 可能无法显示内容。
- 访问日历事件页面后，Secure Mail 可能无法将应用程序模式切换为深色或浅色。
- 在 iPad 上更新 **工作周开始于** 设置后，Secure Mail 可能无法正确显示设置页面。

已知问题

此版本中没有已知问题。

适用于 Android 的 Secure Mail 25.8.0

已修复的问题

- 在 Android 设备上的 Secure Mail 中单击电子邮件链接时，链接可能无法按预期工作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 在 Android 上的 Secure Mail 中尝试打开大型附件时，应用程序可能会意外关闭，并显示以下错误消息：“内存不足”。
- 当 Access Gateway 证书过期时，Android Secure Mail 可能无法检索电子邮件。

已知问题

此版本中没有已知问题。

适用于 Android 的 Secure Mail 25.6.0

已修复问题

- 将小米设备升级到操作系统 14 时，Secure Mail 可能会崩溃，并且该过程可能不受支持。
- 在启用了证书强映射的 Exchange 环境中使用时，传输层安全 (TLS) 连接可能会失败。
- 将语言设置为荷兰语时，Secure Mail 日历弹出按钮可能无法对齐。

已知问题

此版本中没有已知问题。

适用于 iOS 的 Secure Mail 25.5.0

已修复问题

- 在 Secure Mail 中尝试打开从 Skype 发送的未接来电电子邮件时，应用程序可能会突然关闭。
- Secure Mail 在将补丁 **KB5014754** 应用到域控制器后可能无法连接。
- 如果您重新连接到 Wi-Fi，或者证书或安全票证颁发机构 (STA) 票证过期，应用程序可能无法同步。
- 当您的 Secure Mail 证书过期时，应用程序可能无法续订证书。
- 当您尝试在 Secure Mail 中登录 GoToMeeting 时，该过程可能会失败并显示以下错误消息： “此端点不再有效”。

已知问题

此版本中没有已知问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 Android 的 Secure Mail 25.3.0

已修复问题

此版本解决了可提高整体性能和稳定性的方面。

已知问题

此版本中没有已知问题。

适用于 Android 的 Secure Mail 25.1.0

已修复问题

此版本解决了可提高整体性能和稳定性的方面。

已知问题

本版本中没有已知问题。

适用于 iOS 的 Secure Mail 25.1.0

已修复问题

- 当您尝试在 Secure Mail 中打开大于 10 MB 的电子邮件附件时，附件可能无法下载。
- 当用户在运行 iOS 18 的 iPhone 上的 Secure Mail 中配置了多个邮件帐户时，应用程序可能会突然关闭。

已知问题

本版本中没有已知问题。

适用于 iOS 的 Secure Mail 24.11.0

已修复问题

由于网络连接问题，Secure Mail 无法在 iPhone 和 iPad 设备上同步电子邮件。

已知问题

- 当您断开并重新连接 Wi-Fi 时，Secure Mail 不会与服务器同步。作为一种变通方法，用户可以重新启动 Secure Mail。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 如果用户在 Secure Mail 中添加了两个帐户，Secure Mail 可能会突然关闭。作为一种变通方法，请在横向模式下使用 Secure Mail 以避免此问题。

适用于 Android 的 Secure Mail 24.11.0

已修复问题

本版本中没有已修复的问题。

已知问题

本版本中没有已知问题。

适用于 Android 的 Secure Mail 24.9.1

已修复的问题

在可折叠 Android 手机或 Android 平板电脑上使用 Secure Mail 时，尝试撰写电子邮件时应用程序可能会自动关闭。

已知问题

本版本中没有已知问题。

适用于 Android 的 Secure Mail 24.9.0

已修复的问题

在 MAM 模式下打开 Secure Mail 时，可能会显示以下错误消息：

“不支持更改 SDK 管理策略。”

已知问题

本版本中没有已知问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 iOS 的 Secure Mail 24.9.0

已修复的问题

- 适用于 iOS 的 Secure Mail 可能会显示不正确的推送通知，并显示以下错误消息：“您的会话已过期，我们无法获取此邮件。”
- 当您单击在适用于 iOS 的 Secure Mail 上收到的来自其他日历应用的会议邀请中的 .ics 文件时，该应用可能会错误地将约会安排在错误的时间。
- 在深色模式下使用适用于 iOS 的 Secure Mail 时，当您尝试转发电子邮件时，电子邮件正文内容会变得不可读。
- 当在日历中从月视图切换到日视图时，适用于 iOS 的 Secure Mail 会强制关闭。
- 在适用于 iOS 的 Secure Mail 中，日历邀请页面根据设备设置而不是 Secure Mail 应用主题设置以深色或浅色主题显示。

已知问题

此版本中没有已知问题。

适用于 Android 的 Secure Mail 24.7.0

已修复的问题

此版本中没有已修复的问题。

已知问题

此版本中没有已知问题。

适用于 iOS 的 Secure Mail 24.3.0

已修复的问题

- 尽管 Secure Mail 已成功安装和注册，但最终用户在配置应用程序时可能会收到以下错误消息：

  “连接到服务器超时。请在几分钟后重试”

- 升级到 Secure Mail for iOS 24.2.0 版本后，现有最终用户可能无法访问 Secure Mail，并收到以下错误消息：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

“Secure Mail 无法连接到服务器。请尝试重新输入服务器地址。如果仍然遇到问题，请联系您的 IT 管理员”

- 当最终用户尝试在 iPad 设备上打开 Secure Mail 应用程序时，Secure Mail 会停止响应。此问题特定于运行 iPad 17.3.1 及更高版本的设备。

已知问题

此版本中没有已知问题。

适用于 iOS 的 Secure Mail 24.2.0

已修复的问题

- 在 Secure Mail for iOS 中，您可能无法在日历页面上看到“添加”按钮 (+)，这会阻止您创建新的日历事件。
- 由于网络连接问题，Secure Mail 无法在 iPhone 和 iPad 设备上同步电子邮件。
- 当您在 Secure Mail for iOS 中使用深色模式时，您可能无法阅读电子邮件。

已知问题

此版本中没有已知问题。

适用于 Android 的 Secure Mail 24.1.0

已修复问题

- 当您尝试打开大于 10 MB 的电子邮件附件时，适用于 Android 的 Secure Mail 会无响应。
- 当您尝试打开 .docx 格式且包含阿拉伯字符或超链接的电子邮件附件时，适用于 Android 的 Secure Mail 会无响应。当 Polaris SDK 未更新时，会出现此问题。

已知问题

此版本中没有已知问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 Android 的 Secure Mail 23.10.0

已修复问题

- 当您从 Secure Mail 打开任何附件时，即使您的设备上未安装 **Citrix Files** 应用程序，您也可能会在 **更多 (⋮)** > **打开方式** 选项下找到 **上传到 Citrix Files** 选项。
- 当您预览 Secure Mail 中收到的会议邀请所附的 .ics 文件时，您可能会注意到 .ics 文件预览中显示的会议时间比原始时间晚一小时。此问题发生在夏令时地区。
- 当您将 Secure Mail 升级到版本 23.8.2 并启用深色模式时，您在预览电子邮件附件时可能会遇到问题。当您单击省略号 **(...)** 按钮时，可能无法看到菜单列表。

已知问题

此版本中没有已知问题。

适用于 Android 的 Secure Mail 23.8.2

已修复的问题

此版本中没有已修复的问题。

已知问题

当您将 Secure Mail 升级到 23.8.2 版本并启用深色模式时，在预览电子邮件附件时可能会遇到问题。单击省略号 **(...)** 按钮时，可能无法看到菜单列表。作为一种解决方法，您可以将 Secure Mail 切换到浅色模式。

适用于 Android 和 iOS 的 Secure Mail 23.7.0

已修复的问题

此版本中没有已修复的问题。

已知问题

此版本中没有已知问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 Android 的 Secure Mail 23.8.1

已修复的问题

此版本中没有已修复的问题。

已知问题

此版本中没有已知问题。

适用于 iOS 的 Secure Mail 23.9.0

已修复的问题

- 当您将适用于 iOS 的 Secure Mail 23.2.0 版本与 HCL Domino 11 服务器配合使用时，可能无法发送以前保存的草稿电子邮件。Secure Mail 显示电子邮件已成功发送，但收件人从未收到。

已知问题

此版本中没有已知问题。

适用于 Android 的 Secure Mail 23.8.0

已修复的问题

此版本中没有已修复的问题。

已知问题

此版本中没有已知问题。

适用于 Android 的 Secure Mail 23.7.0

已修复的问题

- 您可能无法收到日历事件的提醒通知。当 Secure Mail 的闹钟和提醒权限被撤销时，会出现此问题。

已知问题

此版本中没有已知问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 Android 的 Secure Mail 23.6.0

已修复的问题

当您查看电子邮件附件时，可能会看到显示“许可证已过期”的水印。如果您使用的是 Secure Mail for Android 23.3.5 或更早版本，则会出现此问题。要在没有水印的情况下查看电子邮件附件，请升级到 Secure Mail for Android 23.6.0 或更高版本。

已知问题

此版本中没有已知问题。

适用于 iOS 的 Secure Mail 23.5.0

已修复的问题

- 当您收到数字签名电子邮件并在 Secure Mail 中打开它们时，电子邮件附件可能不会显示。

已知问题

此版本中没有已知问题。

旧版本中的已知和已修复问题

有关 Secure Mail 早期版本中的已知和已修复问题，请参阅Secure Mail 已知和已修复问题历史记录。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure Mail 已知和已修复问题历史记录

本文列出了 Secure Mail 在最近支持版本之前的已修复和已知问题。有关最新文档，请参阅 Citrix Secure Mail。

安全邮件 23.3.5

适用于 Android 的 Secure Mail 中的已知问题

- 您可能无法收到日历事件的提醒通知。当 Secure Mail 的闹钟和提醒权限被撤销时，会出现此问题。

  作为一种变通方法，转到 **设置** > **应用** > **特殊应用权限** > **闹钟和提醒** > **Secure Mail**，然后点击以开启通知。

适用于 Android 的 Secure Mail 中的已修复问题

- 升级到 Android 13 后，Secure Mail 会无响应。

安全邮件 23.2.0

适用于 iOS 和 Android 的 Secure Mail 中的已知问题

此版本中没有已知问题。

适用于 Android 的 Secure Mail 中的已修复问题

- 在 Secure Mail 中打开附件时，您可能会看到一个灰色水印覆盖了文档的一部分。当 polaris 许可证过期时，会出现此问题。

  当预览的附件为以下格式时，会出现此问题：

  - docx 文件
  - .xls。
  - .ppt。
  - txt 文件

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 当您尝试使用 Secure Mail 中的“**打开方式...**”选项打开 **.docx**、**.pptx** 和 **.xlsx** 文件时，您可能无法在相应的本机应用程序中打开这些文件。当您使用 Android 13 时，会出现此问题。

Secure Mail for iOS 中已修复的问题

- 当您尝试从 Microsoft Teams 打开“**语音邮件**”电子邮件时，Secure Mail 会变得无响应。
- 当您尝试从 Skype 打开“**未接来电**”电子邮件时，Secure Mail 会变得无响应。当全局 Exchange 地址簿不包含外部呼叫者的身份识别时，会出现此问题。

安全邮件 22.11.0

Secure Mail for Android 中的已知问题

此版本中没有已知问题。

Secure Mail for Android 中已修复的问题

- 当您在 Secure Mail for Android 中打开带有附件的电子邮件时，您无法截取附件文件内容的屏幕截图。即使禁用限制策略，也可能出现此问题。
- 当您转发带有附件的电子邮件时，电子邮件会保留在发件箱中。在您手动发送电子邮件（通过启动发送/接收操作）后，收件人无法打开附件。此问题会间歇性发生。
- 从 Secure Mail 日历访问时，Webex 会议链接无法在相应的应用程序中打开。

安全邮件 22.9.0

iOS 和 Android 版 Secure Mail 中的已知问题

此版本中没有已知问题。

iOS 和 Android 版 Secure Mail 中已修复的问题

此版本中没有已修复的问题。

安全邮件 22.6.2

iOS 版 Secure Mail 中的已知问题

此版本中没有已知问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOS 版 Secure Mail 中已修复的问题

- 当您使用 Secure Web 下载文件并尝试使用 Secure Mail 将其发送给收件人时，**新建邮件**选项不会出现。

安全邮件 22.6.0

iOS 版 Secure Mail 中的已知问题

此版本中没有已知问题。

iOS 版 Secure Mail 中已修复的问题

- 在 iOS 版 Secure Mail 中撰写电子邮件时，当您尝试添加联系人时，会出现错误的联系人详细信息。
- 当您打开应用程序时，iOS 版 Secure Mail 和 Secure Web 会无响应。

安全邮件 22.3.0

Secure Mail 22.3.0 中的已知问题

- 当您编辑日历事件并更新会议提醒时间时，会议组织者不会收到提醒。如果您的组织正在运行 HCL Domino 11 服务器（以前称为 Lotus Notes），则会出现此问题。
- 当您将重复事件更新为每日事件并尝试编辑其中一个实例时，编辑选项不会出现。如果您的组织正在运行 HCL Domino 11 服务器，则会出现此问题。
- 当您更改重复事件的单个实例的日期或时间时，该会议会被重新安排到随机日期。如果您的组织正在运行 HCL Domino 11 服务器，则会出现此问题。

Secure Mail 22.3.0 中已修复的问题

此版本中没有已修复的问题。

安全邮件 22.2.0

Secure Mail 22.2.0 中的已知问题

此版本中没有已知问题。

Secure Mail 22.2.0 中已修复的问题

- 在 Samsung SM-A315 和 SM-F926 设备上，Secure Mail 在设置过程中崩溃。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 21.12.0

已修复的问题

- 当您打开附加的 Microsoft Office 文件时，适用于 Android 的 Secure Mail 会崩溃。当设备语言设置为土耳其语时，会出现此问题。
- 在 Active Directory 中更改适用于 Android 的 Secure Mail 帐户密码后，您无法登录该应用程序。

安全邮件 21.11.0

此版本中没有已知问题或已修复问题。

安全邮件 21.10.5

适用于 Android 的 Secure Mail 中已修复的问题

当您使用本地 Citrix Endpoint Management™ (CEM) 且**网络访问**设置为**隧道式 Web SSO** 模式时，Microsoft Teams 会议创建失败。此问题是由于 Citrix Gateway 中的一个已知问题导致的，其中应用程序交付控制器 (ADC) 会删除包含持有者令牌的授权标头。

适用于 Android 的 Secure Mail 中的已知问题

此版本中没有已知问题。

安全邮件 21.10.0

适用于 Android 的 Secure Mail 中的已知问题

此版本中没有已知问题。

适用于 Android 的 Secure Mail 中已修复的问题

- 在适用于 Android 的 Secure Mail 中，当您在运行 Android 12 Beta 4 的设备上打开交互式 PDF 文件时，该文件会崩溃。
- 在适用于 Android 的 Secure Mail 中，打开包含嵌入图像的电子邮件时，会出现空白屏幕。
- 当您从蜂窝网络切换到 Wi-Fi 网络再切换回来时，系统会提示您登录适用于 Android 的 Secure Hub。提供 PIN 进行身份验证后，登录失败，因为 Secure Mail 提示您的帐户已过期。
- 您的电子邮件在升级到适用于 Android 版本 21.7.0 的 Secure Mail 后无法同步

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 21.9.1

适用于 Android 的 Secure Mail 中的已知问题

- 在运行 Android 12 Beta 4 的设备上打开交互式 PDF 文件时，文件会崩溃。
- 如果工作配置文件中已安装外部 Web 浏览器，则在 Secure Web 不是默认浏览器的情况下，链接会在外部浏览器应用程序中打开。

适用于 Android 的 Secure Mail 中已修复的问题

- 您无法在工作配置文件模式下注册的设备上启动 Secure Mail 21.8.0 版。如果您的环境运行的是与 Microsoft Intune/EMS 集成的 Citrix Endpoint Management，则会出现此问题。
- 如果您的设备启用了深色模式，则适用于 Android 的 Secure Mail 中的附件会显示为深色，并且内容难以辨认。

安全邮件 21.9.0

此版本中没有已知或已修复的问题。

安全邮件 21.8.5

已知问题

- 在运行 Android 12 Beta 4 的设备上打开交互式 PDF 文件时，文件会崩溃。
- 如果工作配置文件中已安装外部 Web 浏览器，则在 Secure Web 不是默认浏览器的情况下，链接会在外部浏览器应用程序中打开。

已修复的问题

此版本中没有已修复的问题。

安全邮件 21.8.0

已知问题

此版本中没有已知问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已修复的问题

- 在适用于 Android 的 Secure Mail 中，点击 Zoom 会议链接会打开 Microsoft Teams 应用。当您的设备上同时安装了 Microsoft Teams 和 Zoom 时，会出现此问题。
- 当您创建日期格式为 dd-mm-yyyy 的 Excel 文件并在适用于 Android 的 Secure Mail 中打开此文件时，日期格式会更改为“mm-dd-yyyy”。
- 当您在适用于 Android 的 Secure Mail 中打开 PDF 文件时，签名不会显示以供验证。

安全邮件 21.7.0

已知问题

此版本中没有已知问题。

已修复的问题

在适用于 iOS 的 Secure Mail 中，非英语语言的个人联系人组无法同步。

安全邮件 21.6.0

此版本中没有已知或已修复的问题。

安全邮件 21.5.0

此版本中没有已知或已修复的问题。

安全邮件 21.4.5

此版本中没有已知或已修复的问题。

安全邮件 21.4.0

此版本中没有已知或已修复的问题。

安全邮件 21.3.5

此版本中没有已知或已修复的问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 21.3.0

此版本中没有已知或已修复的问题。

安全邮件 21.2.0

已知问题

当您点击照片图标以将图片附加到正在撰写的电子邮件时，相机应用会崩溃。 如果您的设备运行的是 Android 11 并且 Secure Mail 配置为工作配置文件模式，则会出现此问题。

已修复的问题

此版本中没有已修复的问题。

安全邮件 21.1.5

适用于 iOS 的 Secure Mail

此版本中没有已知或已修复的问题。

安全邮件 21.1.0

已知问题

此版本中没有已知问题。

已修复的问题

在适用于 iOS 的 Secure Mail 中，点击包含在尖括号内的会议链接无法启动会议。出现空白屏幕。

安全邮件 20.12.0

适用于 iOS 的 Secure Mail

此版本中没有已知或已修复的问题。

安全邮件 20.11.0

此版本中没有已知或已修复的问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 20.10.5

已知问题

在适用于 iOS 的 Secure Mail 中，通知设置中缺少“子文件夹”(**邮件文件夹**) 选项。

已修复的问题

此版本中没有已修复的问题。

安全邮件 20.10.0

已知问题

在适用于 iOS 的 Secure Mail 中，通知设置中缺少“子文件夹”(**邮件文件夹**) 选项。

已修复的问题

此版本中没有已修复的问题。

安全邮件 20.9.5

适用于 Android 的 Secure Mail

此版本中没有已知或已修复的问题。

安全邮件 20.9.0

已知问题

在适用于 iOS 的 Secure Mail 中，通知设置中缺少“子文件夹”(**邮件文件夹**) 选项。

已修复的问题

在适用于 iOS 的 Secure Mail 中，当处于亚利桑那州时区时，会议邀请中显示的时间不正确（相差 1 小时）。

安全邮件 20.8.5

适用于 Android 的 Secure Mail

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已知问题

在某些运行 Android 11 的设备上，**联系人**和**日历**会议详细信息无法全屏打开。

已修复的问题

此版本中没有已修复的问题。

安全邮件 20.8.0

此版本中没有已知或已修复的问题。

安全邮件 20.7.5

此版本中没有已知或已修复的问题。

安全邮件 20.7.0

此版本中没有已知或已修复的问题。

安全邮件 20.6.5

已知问题

本版本中没有已知问题。

已修复的问题

- 在适用于 iOS 的 Secure Mail 中，即使字体大小设置为大，您也无法在邮件视图中以大尺寸查看文本。
- 在适用于 iOS 的 Secure Mail 中，当您在同一域中配置多个帐户时，无法接收通知。

安全邮件 20.6.0

已知问题

本版本中没有已知问题。

已修复的问题

- 在运行 iOS 的设备上，修改 IBM Traveler 服务器上的某些 HTTP 标头后，Secure Mail 会停止同步。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 在适用于 iOS 的 Secure Mail 中，当您收到电子邮件时，无法通过点击通知来打开电子邮件。您会收到以下错误：**无法获取电子邮件。**

安全邮件 20.5.0

适用于 iOS 的 Secure Mail

已知问题

本版本中没有已知问题。

已修复的问题

- 在运行 iOS 13.4 的 iPad 上，Secure Mail 中无法进行文本选择。
- 在适用于 iOS 的 Secure Mail 中，**VoiceOver** 功能无法读取电子邮件。

安全邮件 20.4.5

已知问题

此版本中没有已知问题。

已修复问题

- 在适用于 iOS 的 Secure Mail 中，iPhone 上的邮件撰写窗口中未遵循辅助功能大小。
- 在适用于 iOS 的 Secure Mail 中，在 iPad 上使用“**共享到**”选项时无法添加附件。

安全邮件 20.4.0

已知问题

此版本中没有已知问题。

已修复问题

- 在运行 iOS 的设备上，当您在撰写电子邮件时粘贴从 Secure Mail 复制的图像时，收件人无法查看该图像。
- 在适用于 iOS 的 Secure Mail 中，迁移到 Office 365 后会收到多个身份验证提示。
- 在适用于 iOS 的 Secure Mail 中，当您编辑在 Outlook 上创建的日历邀请时，无法查看说明。如果您修改邀请，说明将被删除。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 20.3.0

此版本中没有已知问题或已修复问题。

安全邮件 20.2.0

此版本中没有已知问题或已修复问题。

安全邮件 20.1.5

已知问题

此版本中没有已知问题。

已修复问题

- 在适用于 iOS 的 Secure Mail 中，电子邮件通知在运行 T-Mobile LTE 网络的设备上失败。
- 在适用于 iOS 的 Secure Mail 中，当设备从纵向模式切换到横向模式时，电子邮件中的图像不会调整大小。

安全邮件 20.1.0

已知问题

- 在适用于 Android 的 Secure Mail 中，您无法从日历事件登录到 GTM。
- 在适用于 Android 的 Secure Mail 中，当您从“附件”选项卡附加文件时，无法发送邮件。
- 在运行 Android 7 的设备上，当您从版本 19.12.7 升级到版本 20.1.0 时，Secure Mail 会间歇性崩溃。

已修复的问题

- 当您在主屏幕上长按 Secure Mail 图标，然后在 iPad 上轻按日历时，收件箱会显示。
- 在适用于 Android 的 Secure Mail 中，您无法打开数字版权管理 (DRM) 附件。

安全邮件 19.12.5

已知问题

在运行 iOS 13 的设备上，当您查看某些 PDF 文件时，适用于 iOS 的 Secure Mail 会崩溃。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已修复的问题

- 在运行 iOS 13 的设备上，Secure Mail 反复崩溃。此崩溃发生在最新的 Apple 设备上，例如 iPhone XS、11 Pro 和 11 Pro Max。
- 在适用于 iOS 的 Secure Mail 中，iPhone 的语音听写和 Apple 智能键盘箭头键等功能在 iOS 13 上不起作用。

安全邮件 19.11.5

此版本中没有已知或已修复的问题。

适用于 iOS 的 Secure Mail 19.10.6

适用于 iOS 的 Secure Mail 中的已知问题

此版本中没有已知问题。

适用于 iOS 的 Secure Mail 中已修复的问题

在适用于 iOS 的 Secure Mail 中，运行 iOS 13 的设备在撰写电子邮件时会间歇性崩溃。

安全邮件 19.10.5

已知问题

此版本中没有已知问题。

已修复问题

在运行 iOS 13 的 iPhone 上，用户从任何 MDX 应用程序下载文件后，无法在 Secure Mail 中打开该文件。

安全邮件 19.10.0

此版本中没有已知或已修复的问题。

安全邮件 19.9.5

已知问题

此版本中没有已知问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已修复问题

- 在适用于 Android 的 Secure Mail 中，运行基于证书的身份验证的设备无法同步大型电子邮件。
- 在适用于 iOS 的 Secure Mail 中，当您在 IBM Lotus Traveler 上重新预配用户实例时，电子邮件文件夹会重复。
- 在适用于 Android 的 Secure Mail 中，您无法接收通知。

安全邮件 19.9.0

已知问题

运行 Microsoft Intune/EMS 的 iOS 版 Secure Mail 在您通过点击“**共享 > 复制到 Word**”使用 MS Word 应用打开 MS Word 文档时崩溃。

已修复问题

- 在 Android 版 Secure Mail 中，当您删除已读邮件时，它会在 Outlook 和 Secure Mail 的“**已删除邮件**”中显示为未读邮件。
- 在 iOS 版 Secure Mail 中，如果发送带有附件的数字签名电子邮件，电子邮件收件人不会收到附件。
- 当您尝试连接到 Active Directory Federation Services (ADFS) 和 Outlook 365 时，Secure Mail iOS 会崩溃。
- 在运行 Android 的设备上，您无法对 Secure Mail 进行身份验证。出现以下错误：“我们在身份验证过程中遇到错误。”

安全邮件 19.8.5

Android 版 Secure Mail 中的已知问题

此版本中没有已知问题。

Android 版 Secure Mail 中的已修复问题

- 如果日历事件提醒出现在通知栏中，则您不会收到后续日历提醒的通知警报。如果您创建了批量日历提醒，并且您的设备处于空闲或休眠模式，Secure Mail 日历通知会延迟。
- 在 Android 版 Secure Mail 中，当您点击“设置”时，会弹出一个窗口，其中包含使用 Secure Mail 或第三方应用完成操作的选项。
- 在 Android 版 Secure Mail 中，您收到的某些电子邮件的日期为 Jan 1, 1970。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 在适用于 Android 的 Secure Mail 中，您无法同步包含 500 多个成员的联系人组。

安全邮件 19.8.0

已知问题

当您点击电子邮件通知并使用触控 ID 登录时，适用于 iOS 的 Secure Mail 会崩溃。当应用程序未在后台运行时，会出现此问题。

已修复问题

此版本中没有已修复的问题。

安全邮件 19.7.5

已知问题

此版本中没有已知问题。

已修复问题

- 在适用于 Android 的 Secure Mail 中，您会收到已读电子邮件的多个通知。
- 在适用于 iOS 的 Secure Mail 中，日历无法同步，并显示以下错误：**无法同步日历**。

安全邮件 19.6.5

已知问题

此版本中没有已知问题。

已修复的问题

- 在适用于 iOS 的 Secure Mail 中，当您回复电子邮件时，发件箱中仅显示您的回复，而不是整个邮件会话。
- 在适用于 Android 的 Secure Mail 中，电子邮件内容未正确呈现。
- 当您通过拖放事件来修改日历事件的时间，然后发送更新时，受邀者的回复不会重置。
- 在通过拖放事件修改日历事件时间时，适用于 Android 的 Secure Mail 会间歇性崩溃。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 19.5.5

已知问题

- 在适用于 Android 的 Secure Mail 中，当**网络访问**策略设置为 **Tunneled - Web SSO** 时，您无法建立 HttpURLConnection。
- 在适用于 iOS 的 Secure Mail 中，当应用程序未在前台或后台运行时，通知响应选项不起作用。

已修复的问题

在适用于 Android 的 Secure Mail 中，当您发送电子邮件时，收件人会多次收到该电子邮件。此问题发生在运行 Android 8 或更高版本的设备上。

安全邮件 19.5.0

已知问题

在运行 iOS 的设备上，您可以连接到在**允许的 Wi-Fi 网络** MDX 策略中定义的允许的 Wi-Fi 网络之外的 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适用于 iOS 的 Secure Mail 和 Secure Web。

已修复的问题

- 在适用于 Android 的 Secure Mail 中，撰写新电子邮件时无法将电子邮件地址粘贴到“**收件人:**”或“**抄送/密送:**”字段中。但是，在回复电子邮件时，可以将电子邮件地址粘贴到“**收件人:**”或“**抄送/密送:**”字段中。
- 在适用于 Android 的 Secure Mail 中，注册 Android Enterprise 设备时无法保存帐户配置设置。
- 在适用于 Android 的 Secure Mail 中，使用几天后收件箱会变空。

适用于 Android 的 Secure Mail 19.4.6

适用于 Android 的 Secure Mail 中的已知和已修复问题

此版本中没有已知或已修复问题。

安全邮件 19.4.5

已知问题

此版本中没有已知问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已修复问题

- 在适用于 iOS 的 Secure Mail 中，当您在 Outlook 中发送会议请求并在 Secure Mail 中对其进行编辑时，会议不会在 Outlook 中更新。收件人也不会收到更新。当您在 Secure Mail 中创建会议请求并在 Secure Mail 中对其进行编辑时，也会出现此问题。
- 在适用于 iOS 的 Secure Mail 中，日历不同步，并显示以下错误：**无法同步日历**。
- 在适用于 Android 的 Secure Mail 中，您使用 Outlook 创建的一些会议邀请不会反映在您的 Secure Mail 日历中。
- 在适用于 Android 的 Secure Mail 中，定期会议会延迟显示，并且对会议所做的更新未正确同步。

安全邮件 19.3.5

已知问题

此版本中没有已知问题。

已修复问题

- 在适用于 iOS 的 Secure Web 中，您无法在浏览器中粘贴 Bitly URL。
- 在适用于 iOS 的 Secure Mail 中，您收到的每封邮件都会显示以下错误消息：无法获取此邮件。请打开 Secure Mail。
- 在适用于 iOS 的 Secure Mail 中，当用户打开应用程序并输入 PIN 时，他们会频繁收到以下错误消息：“公司网络不可用”。
- 切换到多重身份验证后，适用于 iOS 的 Secure Mail 无法同步。

安全邮件 19.3.0

已知问题

此版本中没有已知问题。

已修复问题

- 在适用于 iOS 的 Secure Mail 中，当由于网络会话无效而导致请求超时时，您收到电子邮件时会间歇性地出现以下通知横幅：**Secure Mail 因请求超时而无法获取此邮件**。
- 在适用于 Android 的 Secure Mail 中，您无法从 mozaiekwonen.xm.cloud.com 接收 Firebase Cloud Messaging (FCM) 通知。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 在适用于 Android 的 Secure Mail 中，当您更新日历事件时，更改不会与 Outlook Office 365 同步。
- 在适用于 Android 的 Secure Mail 中，当网络连接不良或没有网络连接时，包含附件的电子邮件不会发送。即使网络连接恢复，这些电子邮件仍保留在发件箱中。

安全邮件 19.2.0

已知问题

当证书启用了透明度选项并使用在线证书状态协议 (OCSP) 装订时，Secure Mail 配置在 iOS 12.1.1 及更高版本上会失败。

已修复问题

- 在适用于 iOS 的 Secure Mail 中，您无法将 Secure Mail 主题字段中的文本复制到 Secure Notes 10.8.6.6 版。
- 在适用于 Android 的 Secure Mail 中，如果三星设备上启用了预测文本，则文本的最后一个单词会带下划线。当您不留空格时，签名中的最后一个单词会带下划线保存，收件人也能看到。
- 在适用于 Android 的 Secure Mail 中，当您收到电子邮件摘要时，图像不显示。
- 当安装了 Intune Company Portal 5.0.4324.0 版时，适用于 Android 的 Secure Mail 在启动时崩溃。

适用于 iOS 的 Secure Mail 19.1.6

适用于 iOS 的 Secure Mail 中的已知和已修复问题

此版本中没有已知或已修复问题。

安全邮件 19.1.5

已知问题

此版本中没有已知问题。

已修复问题

- 在适用于 iOS 的 Secure Mail 中，您收到的每封邮件都会显示以下错误消息：**无法获取此邮件。请打开 Secure Mail**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 在适用于 iOS 的 Secure Mail 中，当用户打开应用程序并输入 PIN 时，会频繁收到以下错误消息：公司网络不可用。
- 在封装的 Android 应用程序中，UserAgent 字符串会被多次附加，导致标头大小增加。此行为会导致错误，并且页面无法加载。

安全邮件 19.1.0

已知问题

此版本中没有已知问题。

已修复的问题

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

  “您的会话已过期，我们无法获取此邮件。请打开 Secure Mail 以续订您的会话。”

  此问题已修复，消息已更新为：

  “Secure Mail 无法连接到您组织的网络。请联系您的管理员。”
- 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 限制，并显示以下错误消息：

  “服务器正忙。请稍后重试。”
- 在适用于 Android 的 Secure Mail 中，如果您使用土耳其语，则无法向地址中包含字符“I”的收件人发送电子邮件。
- 在适用于 Android 的 Secure Mail 中，用户无法选择和突出显示电子邮件的主题行。
- 在适用于 Android 的 Secure Mail 中，如果密码包含字符 €，则登录失败。
- 在适用于 Android 的 Secure Mail 中，如果启用了**与本地联系人同步**设置，则所有 Secure Mail 联系人都将导出到您的本机联系人。同步后，电话字段（例如移动电话、工作电话、家庭电话、工作传真和家庭传真）不会按正确顺序显示。例如，在您的本机联系人中，传真号码显示在手机号码上方。用户无法更改此顺序。

安全邮件 18.12.0

已修复的问题

- 在适用于 iOS 的 Secure Mail 中，当您收到富文本格式 (RTF) 的邮件时，某些类型的内联附件和附件符号不可见。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 在适用于 iOS 的 Secure Mail 中，当启用富推送通知并关闭再打开**邮件通知**时，**邮件类型**选项会间歇性出现。
- 如果您的环境中运行基于客户端的身份验证机制，Secure Mail 会间歇性地无法自动同步电子邮件。执行手动同步只能获取少量电子邮件。

安全邮件 18.11.1

已修复的问题

- 在适用于 Android 的 Secure Mail 中，连接到 IBM Notes Traveler 9.0.1 SP 10 时，带附件的电子邮件会保留在发件箱中。

已知问题

- 在适用于 Android 的 Secure Mail 中，电子邮件中嵌入的图像不可见。
- 在打开签名中包含嵌入式 URL（例如 `file://C:...jpg.`）的电子邮件时，适用于 Android 的 Secure Mail 会崩溃。

安全邮件 18.10.5

已修复的问题

- 当启用 iOS 数据保护 MDX 策略时，您会间歇性地收到“您有新邮件”通知。
- 在 iPhone XS 上，附件无法下载或发送，并且下载的图像无法显示。
- 当用户修改运行 Exchange ActiveSync 16 及更高版本的帐户的定期会议时，该会议不会在 Exchange Server 中更新。因此，会议不会在 Secure Mail 和 Outlook 之间同步。

安全邮件 18.10.0

已修复的问题

- 在适用于 Android 的 Secure Mail 中，用户无法查看指向 Exchange 服务器以外的服务器的内联图像。
- 在适用于 Android 的 Secure Mail 中，加入 Webex 会议时，PIN 码未附加到拨入号码。您必须手动输入 PIN 码。
- 如果未配置个人日历，则在尝试导出 Secure Mail 日历时，适用于 Android 的 Secure Mail 会崩溃。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 在 iPhone XS 上，适用于 iOS 的 Secure Mail 中，附件无法下载或发送，并且下载的图像无法显示。

安全邮件 18.9.0

已修复的问题

- 客户端工作站会随着每个 NT LAN Manager (NTLM) 身份验证请求随机更改。
- 当设备处于省电模式时，Android P 上的 Secure Mail 同步会间歇性停止工作。
- 如果未配置个人日历，则在尝试导出 Secure Mail 日历时，Secure Mail 会崩溃。

安全邮件 10.8.65

已修复问题

- 当启用 FIPs 且用户在 iOS 11.3 设备上运行 Secure Mail for iOS 时，剪切、复制和粘贴 MDX 策略不起作用。
- 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，即使该用户未登录。如果新用户点击文件夹以刷新显示，则前一个用户的电子邮件将不再显示。

安全邮件 10.8.60

已修复问题

注意：

Secure Mail 10.8.25 到 10.8.60 版本不包含任何已知问题。

- 在 IBM Lotus Domino 服务器上运行的 Secure Mail for iOS 中，您无法使用收件箱中的搜索图标。
- 当用户使用 Intune 公司门户注册运行 Secure Mail for Android 的设备时，Secure Mail 停止工作。
- 在 FTU 流程中从服务器同步大量邮件文件夹时，Secure Mail for iOS 崩溃。
- 在 Secure Mail for iOS 中，PDF 的打印预览显示较小。
- 在 Secure Mail for Android 中，回复电子邮件时，多个电子邮件 ID 未自动填充。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 10.8.55

已修复问题

- 在 Secure Mail for iOS 中，在横向模式下查看时，日历的“周”视图在 iPad Pro 上显示不正确。

版本 10.8.55 中 MDX 相关的已修复问题

- 在 Android 上，当用户从 Secure Hub 注销时，Secure Mail 会崩溃。
- 在 iOS 设备上，Secure Web 和 Secure Mail 10.8.45 在启动时崩溃。

安全邮件 10.8.50

已修复的问题

- 适用于 iOS 的 Secure Mail 无法将视频文件保存到 ShareFile。
- 当您在适用于 Android 的 Secure Mail 中启用推送通知时，您不会收到新电子邮件的通知。此问题间歇性发生。

安全邮件 10.8.45

已修复的问题

Secure Mail 10.8.45 版本不包含任何已修复的问题。

安全邮件 10.8.40

已修复的问题

在适用于 iOS 的 Secure Mail 中，您收到的每封新电子邮件都会间歇性地出现重复通知。

安全邮件 10.8.35

已修复的问题

- 在适用于 Android 的 Secure Mail 中，自动同步会间歇性停止。用户必须手动同步，才能使 Office 365 服务器中的某些新邮件显示在 Secure Mail 中。
- 在适用于 Android 的 Secure Mail 中，即使您在 Secure Mail 中禁用了电子邮件和日历事件的电子邮件通知，通知仍会显示，并且会发出声音通知。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 使用适用于 Android 的 Secure Mail 创建全天事件时，Outlook 日历中会显示不正确的日期。
- 在适用于 Android 的 Secure Mail 中，Exchange 个人联系人组未同步到应用程序。
- 配置 SSO 后，适用于 Android 的 Secure Mail SSO 到 Exchange 失败。系统会提示用户输入密码才能登录。

安全邮件 10.8.25

已修复的问题

- 在适用于 Android 的 Secure Mail 中，用户将日历邀请与 Office 365 同步时会出现延迟。此问题在创建或更新日历邀请时发生。
- 在适用于 Android 的 Secure Mail 中，当用户在“抄送:”字段中键入单个字母，然后轻按 **发送** 时：Secure Mail 会将邮件发送给常用用户列表中的第一个用户。相反，应该显示一条通知，指出“抄送:”字段条目无效。
- 在运行 Android 7 的 Zebra T51 设备上，用户无法安装 Citrix Launcher 应用程序。
- 当 NetScaler® Gateway 配置了基于证书的身份验证时：在适用于 iOS 的 Secure Mail 中，每当用户收到新邮件时，都会显示“您有新邮件”消息。相反，通知应列出发件人姓名、主题和正文预览。

安全邮件 10.8.20

已修复的问题

- 如果 Intune 公司门户应用程序安装在以仅 MAM 模式注册的 Android 设备上，则在 Endpoint Management 中，Secure Mail 会尝试重定向到 Microsoft 登录页面。将显示以下错误消息：“未收到应用程序的任何配置。请联系您的管理员配置应用程序。”
- 在适用于 Android 的 Secure Mail 中，如果您的用户名或密码包含特殊字符（例如 ä、ö、ü 或 €），则登录会失败。
- 在 Android 设备上，重新启动允许您绕过身份验证以访问 Secure Mail。
- 在适用于 Android 的 Secure Mail 中，当您在内联图像下载之前回复电子邮件时，邮件会滞留在您的发件箱中。当您的设置中启用了“**显示图片**”设置时，会出现此问题。
- 在适用于 iOS 的 Secure Mail 中，如果 IRM 策略为“**ON**”且电子邮件分类设置为“**Protected**”，则在下载完整邮件时无法查看附件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全邮件 10.8.10

已修复的问题

- 更新到适用于 iOS 的 Secure Mail 10.7.25 后，Message-ID 标头缺少括号（< 和 >）。
- 在适用于 iOS 的 Secure Mail 中，用户从 Outlook 添加日历邀请后，应用程序会间歇性崩溃。如果您的日历邀请包含表情符号，则会出现此问题。
- 在 iOS 上，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，Secure Mail 会变慢，如果保持打开状态则会崩溃。
- 在适用于 iOS 的 Secure Mail 中，如果“控制锁定屏幕通知”策略设置为“**仅计数**”，则会间歇性出现重复通知。
- 在适用于 Android 的 Secure Mail 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，应用程序会崩溃。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure Mail 适用于 Android 和 iOS - 预览

敬请期待即将发布的版本中的新功能和已解决的问题。

有关当前版本的更多信息，请参阅 Secure Mail 中的新增功能。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

功能标志管理

管理员可以管理功能标志，以访问预览功能并动态控制生产环境中的功能。为确保功能标志下的功能正常运行，您需要启用指向 URL `features.netscalergateway.net` 的流量。有关更多信息，请参阅功能标志管理。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

部署 Secure Mail

要使用 Citrix Endpoint Management™（以前称为 XenMobile）部署 Secure Mail，请按照以下一般步骤操作：

1. 您可以将 Secure Mail 与 Exchange Server 或 IBM Notes Traveler Server 集成，以使 Secure Mail 与 Microsoft Exchange 或 IBM Notes 保持同步。如果您使用 IBM Notes，请配置 IBM Notes Traveler 服务器。此配置使用 Active Directory 凭据向 Exchange 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 Server。

   重要提示：

   您无法将 Secure Mail 中的邮件与 IBM Notes Traveler（以前称为 IBM Lotus Notes Traveler）同步。目前不支持此 Lotus Notes 第三方功能。因此，当您从 Secure Mail 中删除已回复的会议邮件时，该邮件不会在 IBM Notes Traveler 服务器上删除。如果用户接受日历事件，然后他们通过评论拒绝该事件或对评论采取行动，则评论会丢失。

2. 您可以选择从 Secure Hub 启用 SSO。为此，您需要在 Endpoint Management 控制台中配置 Citrix Files 帐户信息，以将 Endpoint Management 启用为 Citrix Files 的 SAML 身份提供程序。此配置使用 Active Directory 凭据向 Citrix Files 进行身份验证。

   在 Endpoint Management 控制台中配置 Citrix Files 帐户信息是一次性设置，适用于所有 Citrix 客户端、Citrix Files 客户端和非 MDX Citrix Files 客户端。有关详细信息，请参阅在 Endpoint Management 控制台中配置 Citrix Files 帐户信息以实现 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

> 从 Secure Mail 10.6.5 版开始，您可以为适用于 iOS 和 Android 的 Secure Mail 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 详细程度策略允许您指定数据是与您的公司域关联还是匿名收集。选择**匿名**将使用户选择不将公司域包含在所收集的数据中。此新策略取代了早期的 Google Analytics 策略。

当策略设置为匿名时，我们会收集以下类型的数据。我们绝对无法将这些数据链接到单个用户或公司，因为我们不请求用户可识别信息。不会向 Google 发送任何个人身份信息。

- 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 APN 注册、邮件同步和发送、附件下载和日历同步。

除了公司域之外，当策略设置为 **完整** 时，不会收集其他可识别信息。默认设置为 **完整**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

配置 Secure Mail

可以在 Secure Mail 中配置和集成以下功能：

- 使用 Office 365 进行新式身份验证(/zh-cn/citrix-secure-mail/modern-authentication-office-365.html)
- 使用本地 Exchange 进行混合新式身份验证(/zh-cn/citrix-secure-mail/hybrid-modern-authentication-on-premises-exchange.html)
- Secure Mail 的后台服务(/zh-cn/citrix-secure-mail/configuring-background-services-secure-mail.html)
- 集成 Exchange 服务器或 IBM Notes Traveler 服务器
- 安全邮件的 S/MIME
- 安全邮件的单点登录

与 Microsoft Office 365 的现代身份验证

Secure Mail 支持通过 Microsoft Office 365 进行现代身份验证，适用于 Active Directory 联合身份验证服务 (AD FS) 或身份提供程序 (IDP)。现代身份验证是基于 OAuth 令牌的身份验证，使用用户名和密码。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。当他们登录 Secure Mail 时，用户通过使用客户端证书进行身份验证，而不是输入其凭据。

在继续之前，请执行以下操作：

1. 为 Microsoft Office 365 启用现代身份验证 (OAuth)。
2. 在防火墙中启用 Office 365 端点、URL 和 IP 地址范围，以确保最佳网络连接。有关详细信息，请参阅 Microsoft 文档中的 Office 365 URL 和 IP 地址范围。

注意：

- 要迁移或创建混合 Exchange 邮箱解决方案，请参阅 Microsoft 文档中的 Exchange ActiveSync 设备设置与 Exchange 混合部署。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management™ 策略先决条件

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：** 使用此策略指示在 Office 365 上配置帐户时用于身份验证的 OAuth 机制。此策略具有以下必须配置的值：
  - **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，使用此策略进行 OAuth 协议。用户必须提供其用户名和密码，并且可以选择提供多重身份验证代码以进行 OAuth 流程。
  - **将 OAuth 与客户端证书结合使用：** 如果 Office 365 配置为执行基于证书的身份验证，请使用此策略。默认配置为“**不使用 OAuth**”。

对于运行 Android 的设备：

- **用于 O365 的现代身份验证：** 在身份验证期间，将此策略用于 OAuth 协议。
- **用于隧道的 Web SSO 策略：** 使用此策略通过隧道 – Web SSO 隧道传输 OAuth 流量。为此：
  - 将**用于隧道的 Web SSO** 策略设置为**开**。
  - 在网络访问策略中选择**隧道 – Web SSO** 选项。

    注意：

    有关启用 STA 的信息，请参阅通过 STA 连接到邮件服务器。
  - 从**后台服务**策略中排除任何与 OAuth 相关的主机名。

iOS 和 Android 设备通用策略：

- **用于现代身份验证的自定义用户代理：** 使用此策略更改现代身份验证的默认用户代理字符串。
- **受信任的 Exchange Online 主机名：** 使用此策略定义受信任的 Exchange Online 主机名列表，这些主机名在配置帐户时使用 OAuth 机制进行身份验证。这是一个逗号分隔的格式，例如 server.company.com, server.company.co.uk。此列表可以包含默认值或虚荣 URL，但不能为空。默认值为 **outlook.office365.com**。
- **受信任的 AD FS 主机名：** 使用此策略定义受信任的 AD FS 主机名列表，用于在 Office 365 OAuth 身份验证期间自动填充密码的网页。这是一个逗号分隔的格式，例如 `sts.companyname.com, sts.company.co.uk`。如果列表为空，Secure Mail 不会自动填充密码。Secure Mail 会将列出的主机名与 Office 365 身份验证期间遇到的网页主机名进行匹配，并

© 1997–2026 Citrix Systems, Inc. All rights reserved.

检查该页面是否使用 HTTPS 协议。例如，当 `sts.company.com` 是列出的主机名且用户导航到 `https://sts.company.com` 时，如果页面包含密码字段，Secure Mail 会填充密码。默认值为 `login.microsoftonline.com`。

- **Office 365 Exchange Server：** 使用此策略定义云上 Office 365 邮箱的主机名。主机名是单个值，例如 `outlook.office365.com`。默认值为 `outlook.office365.com`。
- **Secure Mail Exchange Server：** 使用此策略定义您的 Exchange Server 地址。您可以根据需要使用此策略定义本地服务器地址或云服务器地址。
- **配置 HTTP 451 重定向：** 有关如何配置重定向的更多信息，请参阅知识中心文章 Secure Mail ActiveSync redirect 451。

在设备上刷新策略后，适用于 iOS 的 Secure Mail 现已启用现代身份验证。

Exchange Server 配置选项

您可以使用 `outlook.office365.com` 或 Microsoft 统一域 `outlook.cloud.microsoft` 配置 Secure Mail。

使用 `outlook.office365.com` 进行配置

要将 `outlook.office365.com` 配置为 Secure Mail Exchange Server，请执行以下操作：

- 将 **安全邮件 Exchange 服务器** 设置为 `outlook.office365.com`。
- 将 `outlook.office365.com:443` 添加到 **后台网络服务**。
- 将 **Trusted Exchange Online Hostnames** 保留为默认值 `outlook.office365.com`。
- 将 **Office 365 Exchange Server** 保留为默认值 `outlook.office365.com`。

使用 Microsoft 统一域 `outlook.cloud.microsoft` 进行配置

要将 `outlook.cloud.microsoft` 配置为 Secure Mail Exchange Server，请执行以下操作：

- 将 **Secure Mail Exchange 服务器** 设置为 `outlook.cloud.microsoft`。
- 将 `outlook.cloud.microsoft:443` 添加到 **后台网络服务**。
- 将 `outlook.cloud.microsoft` 添加到 **受信任的 Exchange Online 主机名**。
- 将 **Office 365 Exchange Server** 保留为默认值 `outlook.office365.com`。请勿将其替换为新域。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

限制

- 如果您的环境中使用现代身份验证，则 iOS 的富推送通知功能不可用。有关富推送通知的详细信息，请参阅 Secure Mail 的推送通知。
- 运行基于证书的身份验证的设置不支持多个帐户。

Secure Mail 策略

以下两个表列出了根据您的 Exchange 基础结构所需的 Secure Mail 策略：

EXCHANGE 基础结构	OFFICE 365 身份验证机制/对 O365 使用现代身份验证	受信任的 AD FS ONLINE 主机名	受信任的 EXCHANGE ONLINE 主机名
本地	关闭	不适用	不适用
混合*	开启	AD FS/IDP	`Outlook.office365.com` 或自定义 URL
Exchange 在线	开	AD FS/IDP	`Outlook.office365.com` 或自定义 URL

EXCHANGE 基础架构	安全邮件 EXCHANGE 服务器	后台网络服务 (IOS)	后台网络服务 (ANDROID)
本地部署	Exchange 本地部署主机名	本地部署	本地部署
混合*	本地部署、Exchange Online 主机名	本地部署、本地 Exchange 主机名	本地部署、本地 Exchange 主机名、AD FS/IDP（仅限内部）
易捷在线	`Outlook.office365.com`	Exchange Online 主机名	本地 Exchange 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迁移到 Exchange Online，Secure Mail 会自动检测此更改并提示用户进行现代身份验证，而无需重新配置其帐户。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

支持 OAuth 的 Secure Mail 兼容性列表

下表列出了 iOS 和 Android 设备上 Secure Mail 的 OAuth 支持矩阵：

身份验证类型	IDP/外部 AD FS	IDP/内部 AD FS	艾泽活动目录	英通
用户名和密码	是	是	是	是
客户端证书	是	仅限 Android	否	否

适用于 iOS 和 Android 的本地 Exchange 混合现代身份验证支持

混合现代身份验证 (HMA) 是一种用户身份管理解决方案，它采用更安全的用户身份验证和授权方法。它现在可用于 Exchange Server 本地混合部署。

HMA 是一种基于 OAuth 令牌的身份验证，使用用户名和密码。它允许本地邮箱用户使用 OAuth 令牌访问本地 Exchange。OAuth 令牌从云端获取。使用现代身份验证管理用户身份为管理员提供了许多不同的工具来保护资源，并为本地 Exchange 提供了更安全的身份管理方法。

有关 HMA 的更多信息，请参阅 宣布推出适用于本地 Exchange 的混合现代身份验证。

MDX 策略中所需的更改

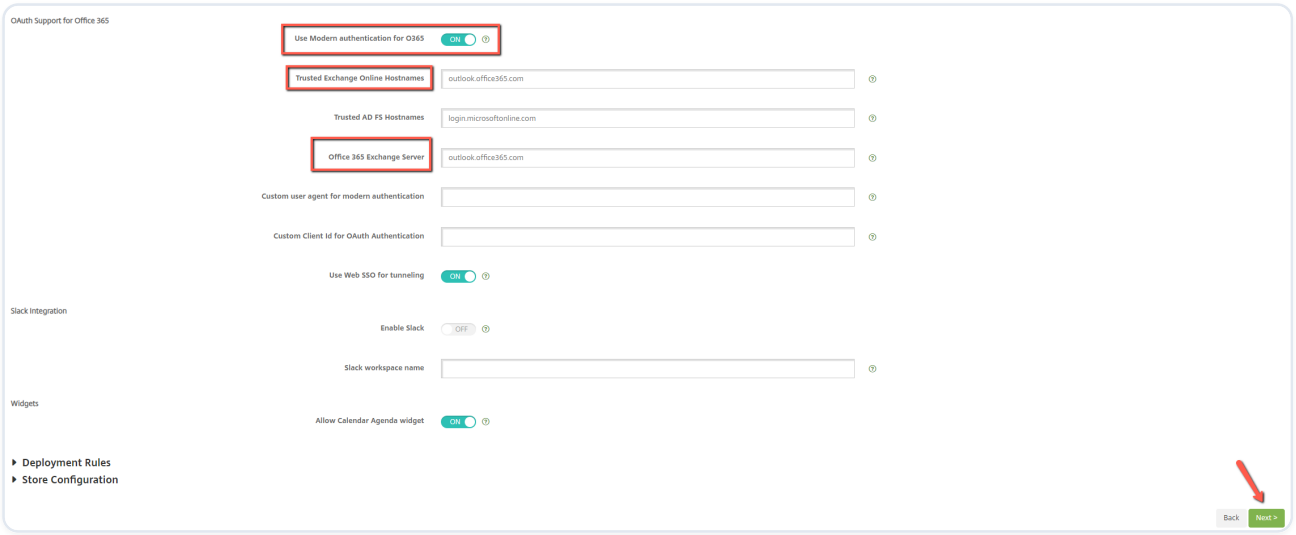
要使 HMA 在 Secure Mail iOS 和 Android 上运行，请在 MDX 策略的“**OAuth Support for Office 365**”部分下执行以下更改：

- 对于 Android，启用**使用 O365 现代身份验证**选项。 对于 iOS，将**Office 365 身份验证机制**设置为**使用 OAuth 和用户名密码**。
- 在“**Trusted Exchange Online Hostnames**”文本字段中输入客户的本地 Exchange URL。
- 在“**Office 365 Exchange Server**”文本字段中输入客户的本地 Exchange URL。
- 单击“**Next**”。

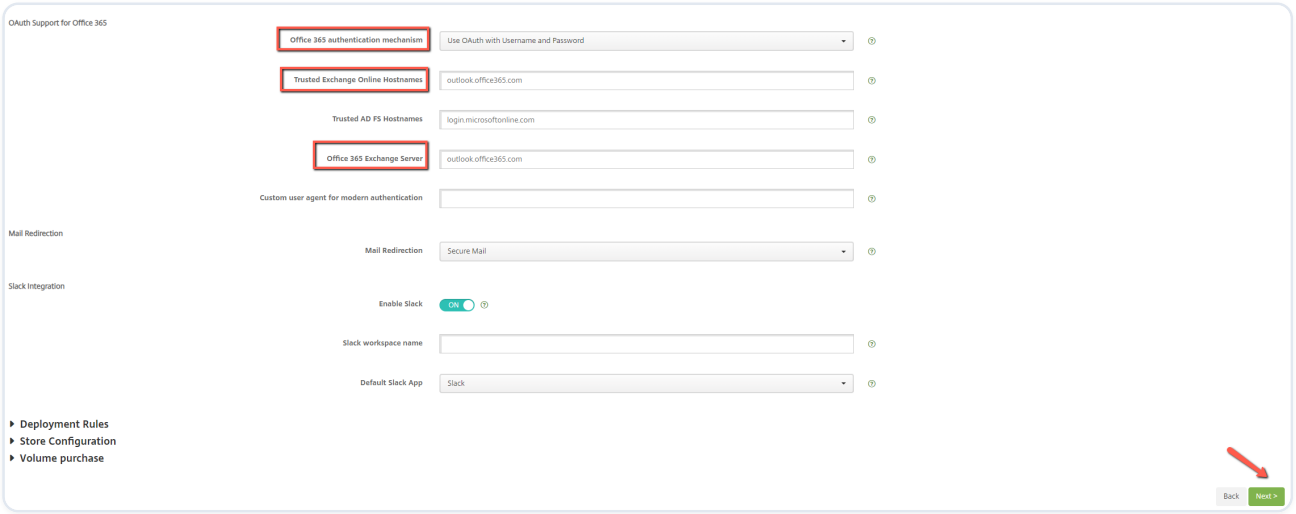
注意：在对 MDX 策略进行上述更改之前，请确保 Exchange 上的 HMA 设置已启用。否则，请禁用“**Use Modern authentication for O365**”选项。

Android 中的**Office 365 的 OAuth 支持**部分：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

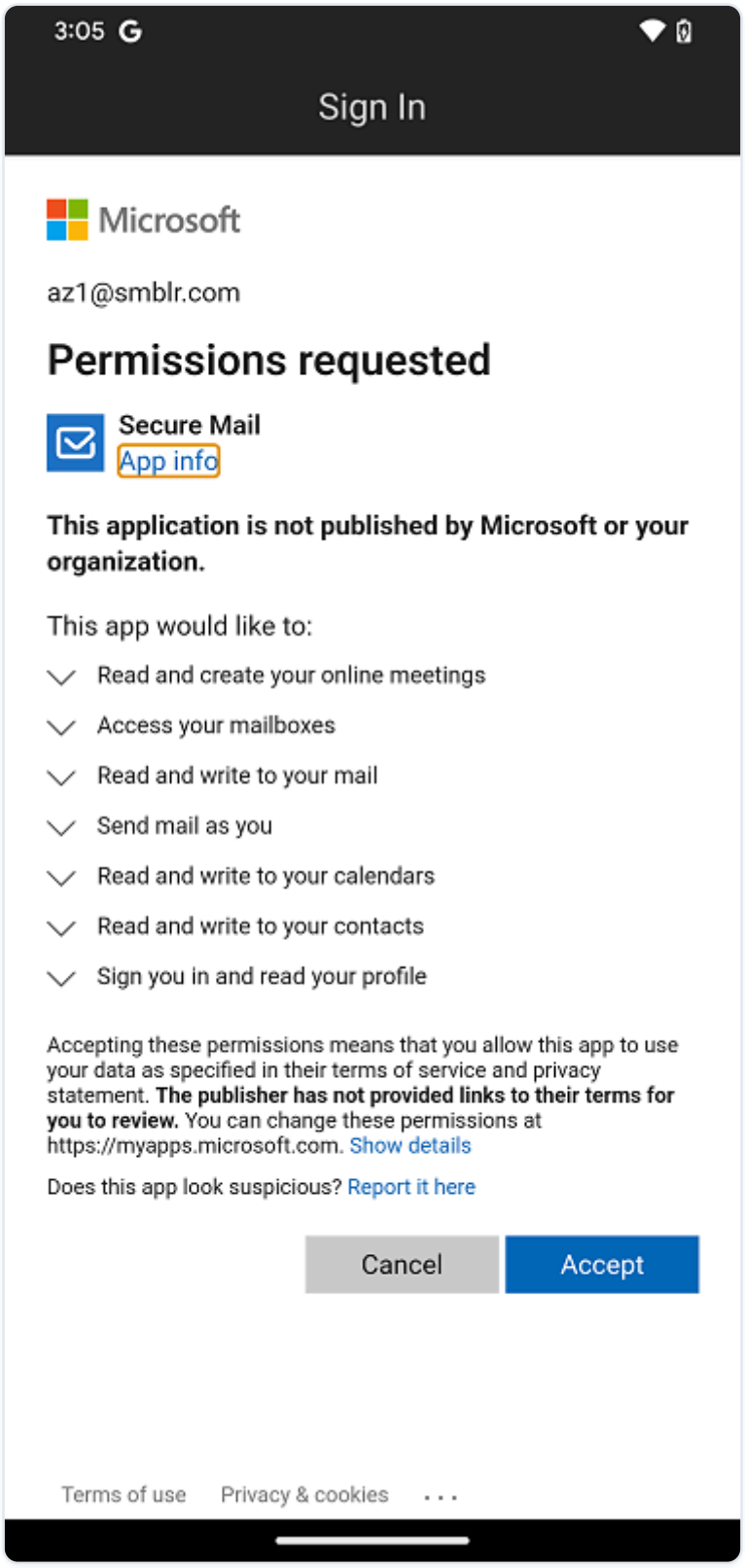


iOS 中的“**OAuth Support for Office 365**”部分：



首次用户成功登录后，将显示以下同意页面。单击**接受**。

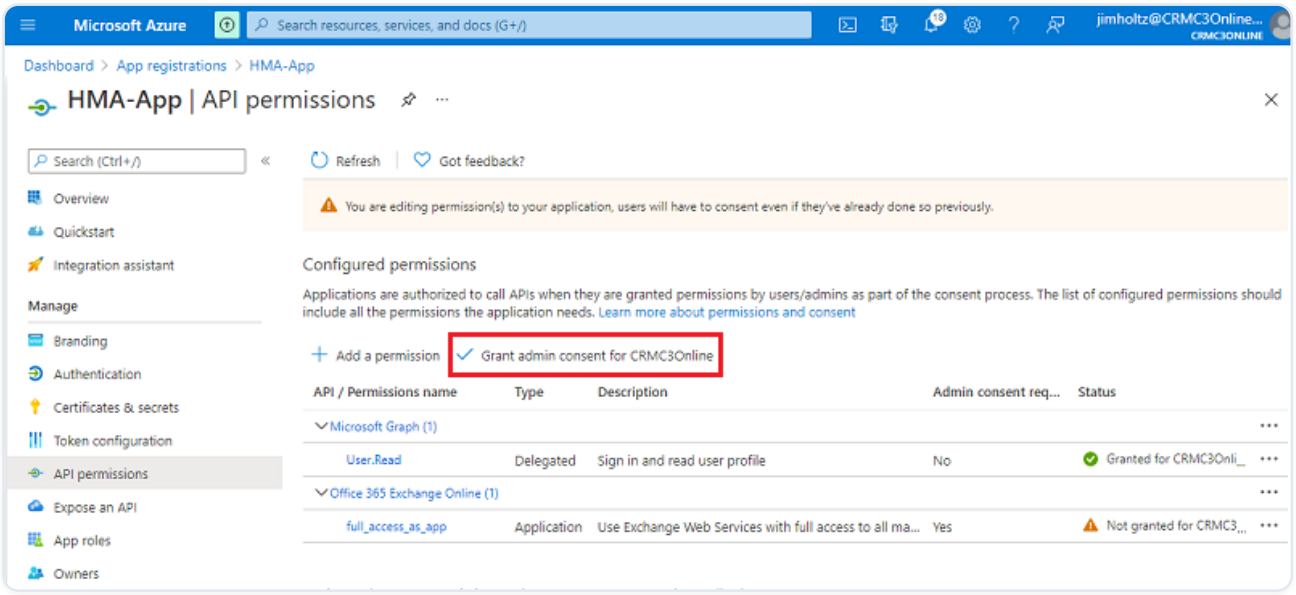
© 1997–2026 Citrix Systems, Inc. All rights reserved.



可选：要停止显示此同意页面，请执行以下步骤：

- 打开 Microsoft Azure 门户。
- 从仪表板导航到**应用注册 > HMA-App**。
- 在**已配置的权限**部分下，启用**授予 CRMC3Online 的管理员同意**选项。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



限制

- 要从 HMA 切换到基本授权，您必须删除现有帐户并在 Secure Mail 上重新创建新帐户。
- 如果 MDX 策略和 Exchange 策略不匹配，用户将无法登录 Secure Mail。

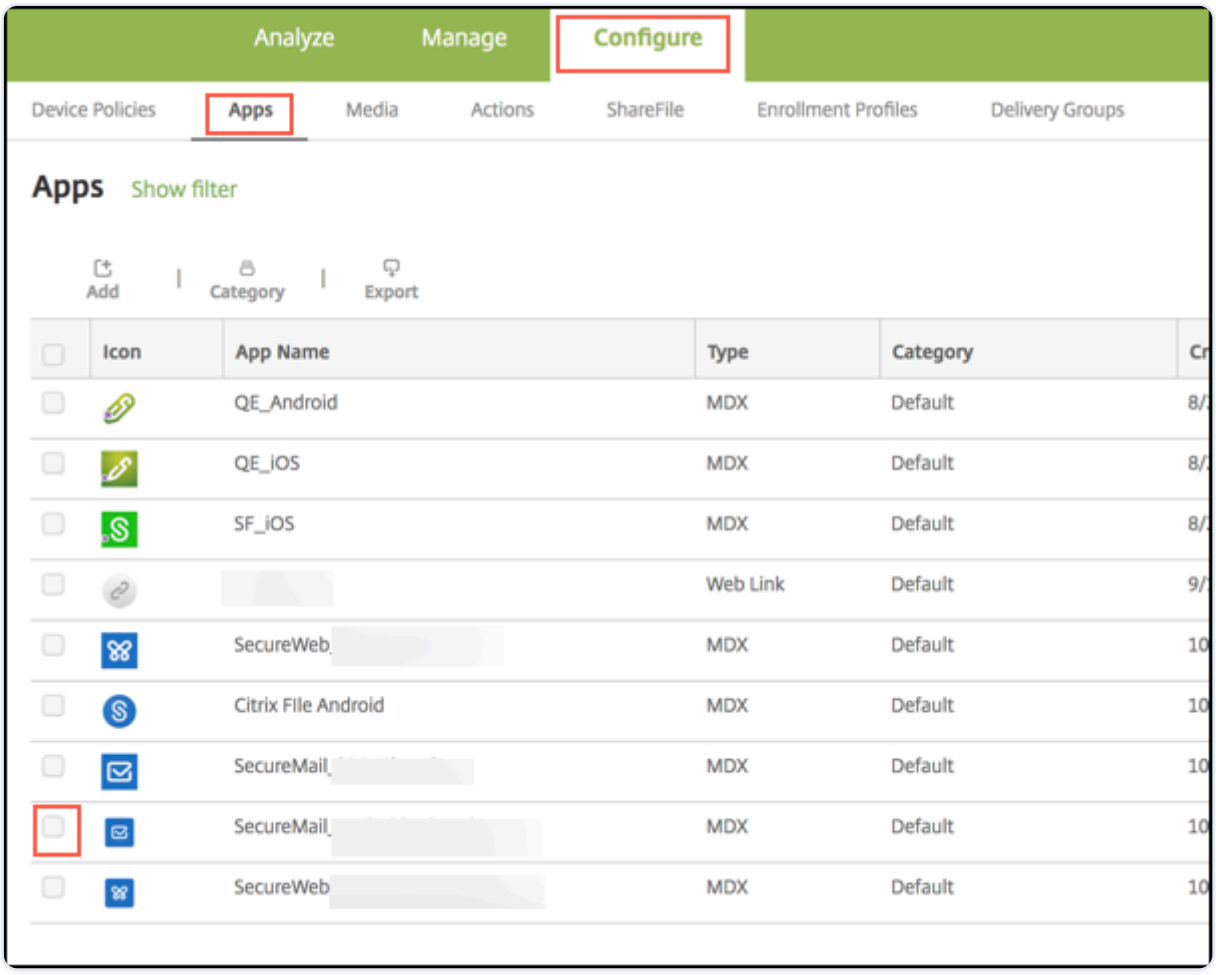
Secure Mail 的后台服务

要通过 Citrix Gateway 访问您的邮件服务器，您需要为 Secure Mail 配置后台服务。当您将 Secure Mail 添加到 Citrix Endpoint Management™（以前称为 XenMobile）时，请在 MDX 应用程序策略设置中配置后台服务。

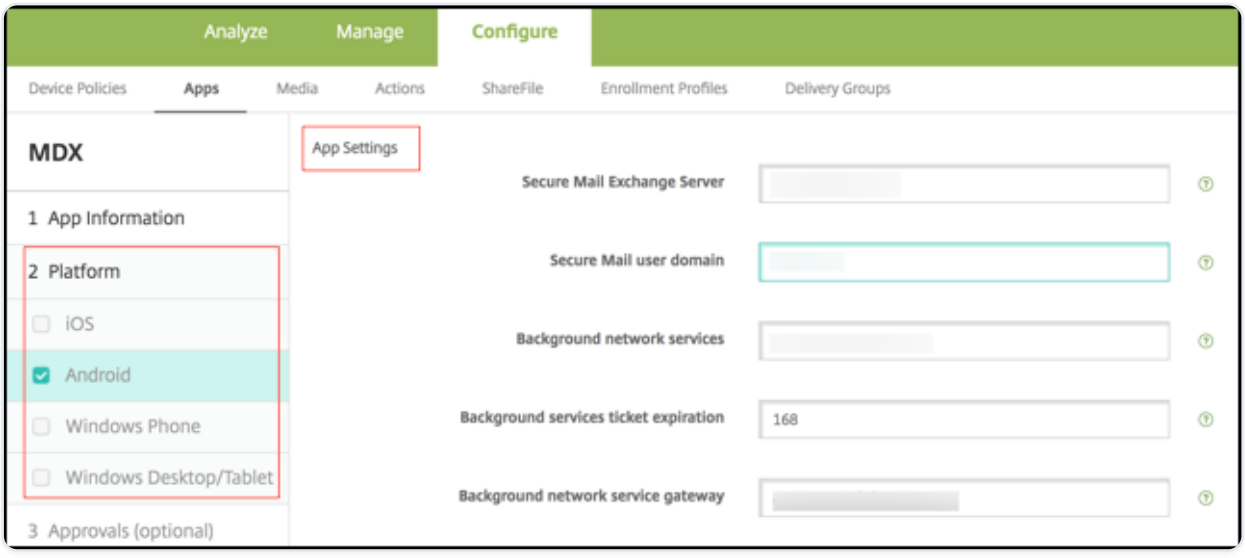
配置 Secure Mail 的后台服务

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**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 在“**MDX 策略设置**”页面上，在“**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。



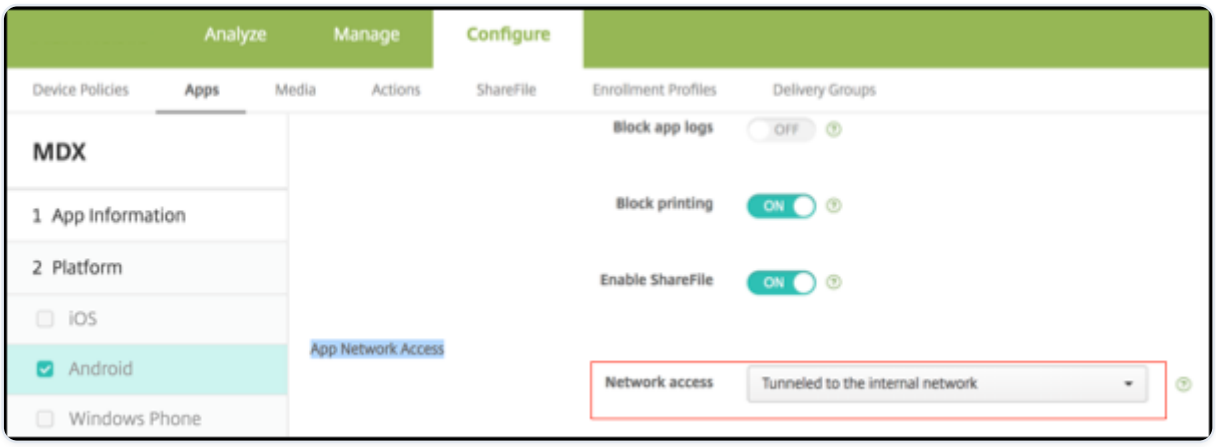
用于后台服务配置的 MDX 应用程序策略

以下 MDX 应用程序策略会影响 Secure Mail 与 Citrix Gateway、Citrix Endpoint Management 服务器、安全票证颁发机构 (STA) 服务器以及邮件服务器之间的通信。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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，或者所有流量是否通过 Internet 不受限制地传输。

- 如果网络访问策略设置为“**隧道连接到内部网络**”，则只有后台网络服务中列出的 URL 才能通过 Citrix Gateway。其余流量通过 Internet 不受限制地传输。默认情况下，Secure Mail 访问设置为“**隧道连接到内部网络**”。
- 如果网络访问策略设置为“**无限制**”，则所有源自 Secure Mail 的流量都通过 Internet 不受限制地传输。VPN 不用于访问后台服务。



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

后台网络服务： 后台网络服务策略指定允许通过 Citrix Gateway 访问的邮件服务器列表。将主机名和端口号列为逗号分隔值。确保值之间没有前导和尾随空格。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`。

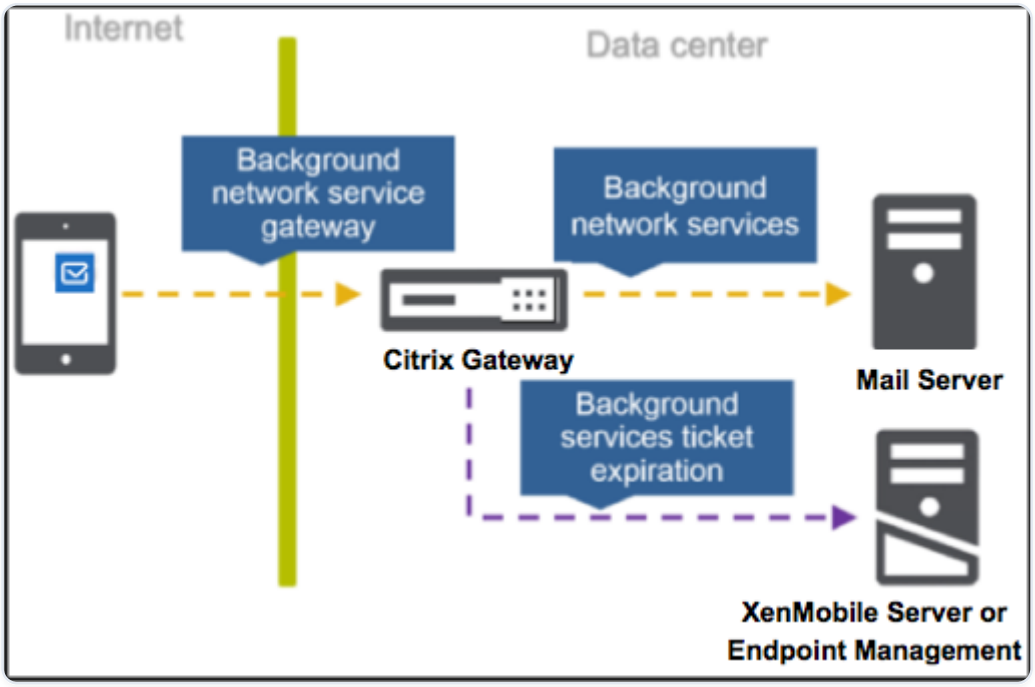
后台服务票证过期： 此策略指定后台网络服务票证的有效期。当 Secure Mail 通过 Citrix Gateway 连接到邮件服务器时，Citrix Endpoint Management 会颁发一个用于连接到内部邮件服务器的令牌。此设置确定 Secure Mail 可以使用此令牌的持续时间。如果令牌处于活动状态，则无需新的令牌进行身份验证和连接到邮件服务器。当时间限制到期时，用户必须重新登录以生成新令牌。此令牌的默认值为 168 小时（7 天）。

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

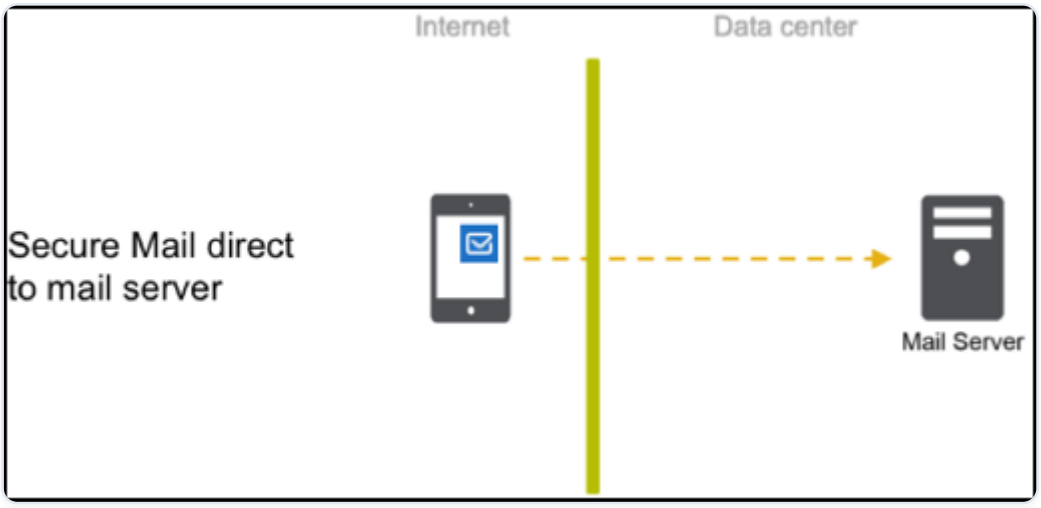
© 1997–2026 Citrix Systems, Inc. All rights reserved.

下图显示了通信流以及这些策略的适用位置。



下图显示了 Secure Mail 连接到邮件服务器的类型。每张图后面都列出了相关的策略设置。

直接连接到邮件服务器



直接连接到邮件服务器的策略：

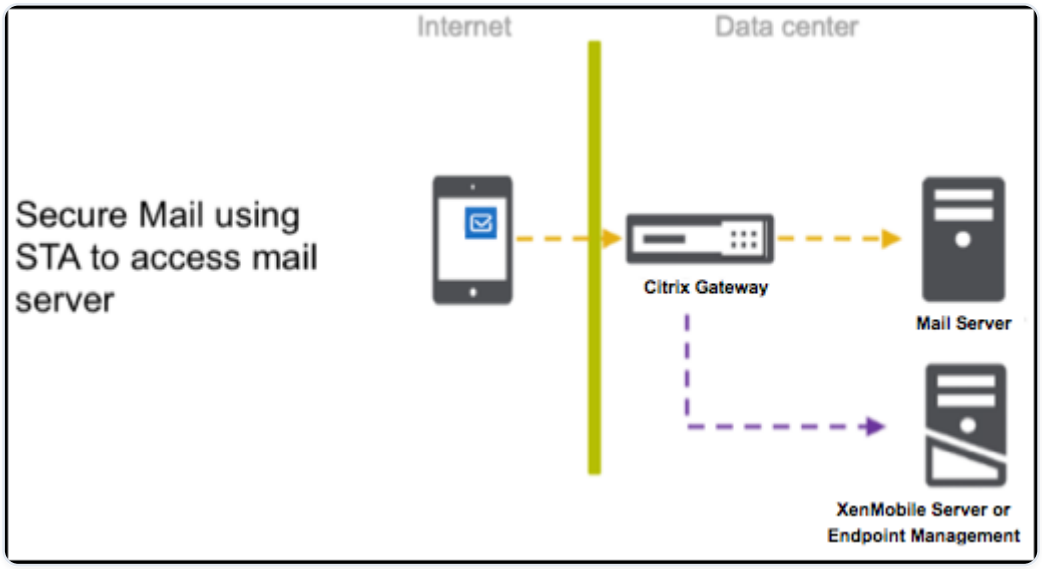
- 网络访问：**无限制**

如果网络访问不受限制，则以下策略不适用：

- 后台网络服务: 不适用
- 后台服务票证过期: 不适用
- 后台网络服务网关: 不适用

© 1997–2026 Citrix Systems, Inc. All rights reserved.

通过 STA 连接到邮件服务器



通过 STA 连接到邮件服务器的策略:

- 网络访问: **Tunneled - Web SSO**
- 后台网络服务: `mail.example.com:443,mail1.example1.com:443, outlook.office365.com:443 or vanity URL:443`
- 后台服务票证过期: **168**
- 后台网络服务网关: `gateway3.example.com:443`

注意:

> Citrix 建议您为 Secure Mail 使用 STA 连接，因为 STA 连接支持长时间会话连接。

有关 STA 的更多信息，请参阅此 Citrix 知识中心文章。

集成 Exchange 服务器 或 IBM Notes Traveler 服务器

为使 Secure Mail 与您的邮件服务器保持同步，请将 Secure Mail 与位于内部网络中或 Citrix Gateway 后面的 Exchange Server 或 IBM Notes Traveler Server 集成。

- 要为 Secure Mail 配置后台服务，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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要：

您无法将 Secure Mail 中的邮件与 IBM Notes Traveler（以前称为 IBM Lotus Notes Traveler）同步。目前不支持此 Lotus Notes 第三方功能。因此，例如，当您从 Secure Mail 中删除会议邮件时，该邮件不会在 IBM Notes Traveler 服务器上删除。

Secure Notes 和 Secure Tasks 也可进行同步。但请注意，Secure Notes 和 Secure Tasks 已于 December 31, 2018 达到生命周期终止 (EOL) 状态。有关详细信息，请参阅EOL 和已弃用的应用程序。

- 要同步适用于 iOS 的 Secure Notes，请将其与 Exchange Server 集成。
- 要同步适用于 Android 的 Secure Notes 和 Secure Tasks，请使用适用于 Android 的 Secure Mail 帐户。

将 Secure Mail、Secure Notes 和 Secure Tasks 添加到 Citrix Endpoint Management（以前称为 XenMobile）时，请按照后台服务配置的 MDX 应用程序策略 中所述配置 MDX 策略。

注意：

适用于 Android 和 iOS 的 Secure Mail 支持为 Notes Traveler Server 指定的完整路径。例如：`https://mail.example.com/traveler/Microsoft-Server-ActiveSync`。

不再需要为 Traveler Server 使用网站替换规则配置 Domino Directory。

为安全邮件配置 IBM Notes Traveler Server

在 IBM Notes 环境中，必须在部署 Secure Mail 之前配置 IBM Notes Traveler 服务器。本节将展示此配置的部署图以及系统要求。

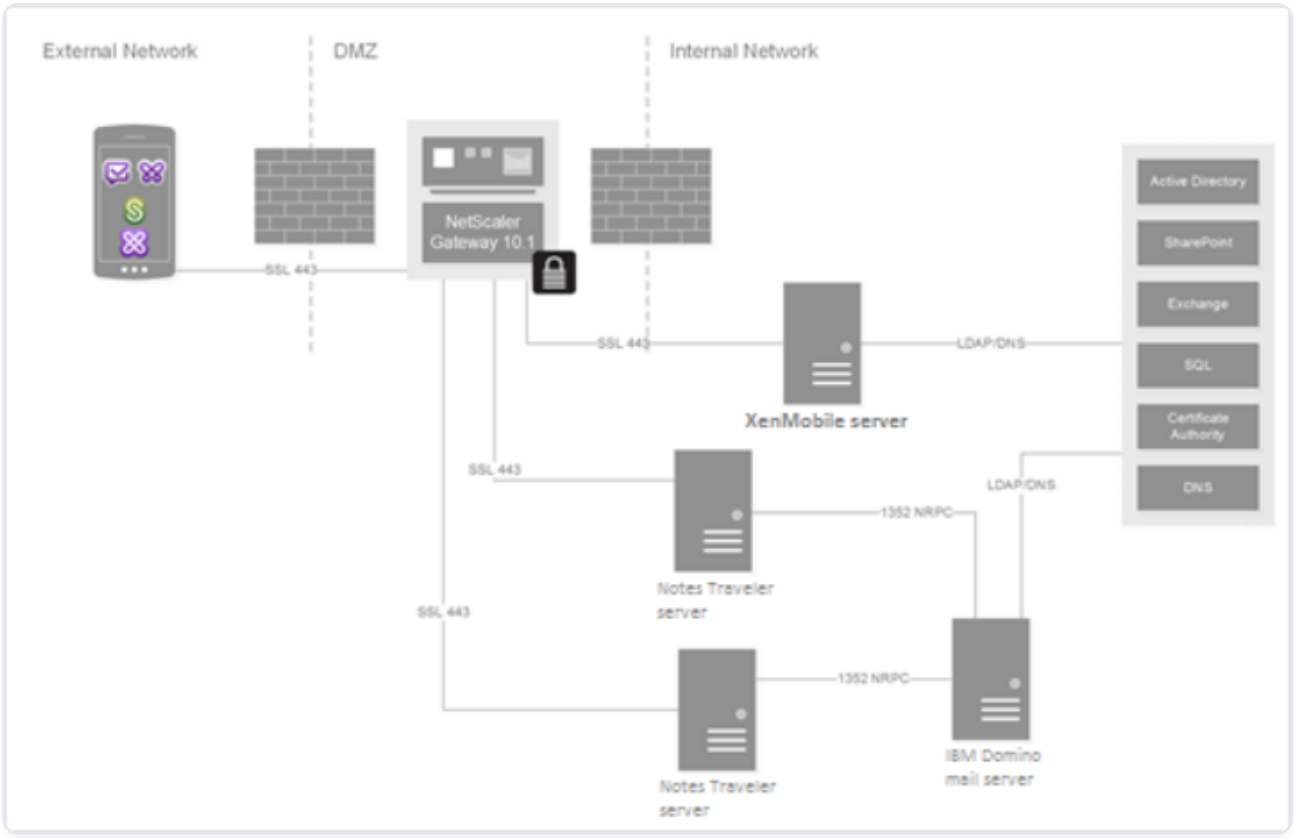
重要提示：

如果您的 Notes Traveler 服务器使用 SSL 3.0，请注意 SSL 3.0 包含一个名为降级旧版加密填充提示 (POODLE) 攻击的漏洞，这是一种中间人攻击，会影响任何使用 SSL 3.0 连接到服务器的应用程序。为解决 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，请参阅(/zh-cn/citrix-secure-mail/exchange-ibm.html#configuring-ssltls-security-level)中的“配置 SSL/TLS 安全级别”部分。

在 IBM Notes 环境中，您必须在部署 Secure Mail 之前配置 IBM Notes Traveler 服务器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

下图显示了示例部署中 IBM Notes Traveler 服务器和 IBM Domino 邮件服务器的网络位置。



系统要求

基础架构服务器要求

- IBM Domino 邮件服务器 9.0.1
- IBM 诺茨 特拉维勒 9.0.1

身份验证协议

- Domino 数据库
- Lotus Notes 身份验证协议
- 轻量级目录身份验证协议

端口要求

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

配置 SSL/TLS 安全级别

Citrix 对 Secure Mail 进行了修改，以解决 POODLE 攻击引入的漏洞，如前述重要说明中所述。因此，如果您的 Notes Traveler Server 使用 SSL 3.0 来启用连接，建议的解决方法是在 IBM Notes Traveler Server 9.0 上使用 TLS 1.2。

IBM 发布了一个补丁，以防止在 Notes Traveler 安全服务器到服务器通信中使用 SSL 3.0。该补丁于 2014 年 11 月发布，作为以下 Notes Traveler 服务器版本的临时修复更新：9.0.1 IF7、9.0.0.1 IF8 和 8.5.3 Upgrade Pack 2 IF8（并将包含在所有未来的版本中）。

作为替代解决方法，当您将 Secure Mail 添加到 Endpoint Management 时，请将“连接安全级别”策略更改为 **SSLv3 和 TLS**。

下表根据“连接安全级别”策略值，按操作系统指示 Secure Mail 支持的协议。您的邮件服务器也必须能够协商该协议。

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

操作系统类型	安全套接字层版本3	TLS
iOS 9 及更高版本	否	是
早于 Android M	是	是
安卓 M 和 安卓 N	是	是
安卓 O	否	是

下表显示了当连接安全级别为 TLS 时 Secure Mail 支持的协议。

操作系统类型	安全套接字层V3	TLS
iOS 9 及更高版本	否	是
早于 Android M 的版本	否	是
Android M 版本和 Android N 版本	否	是
Android O 版本	否	是

© 1997–2026 Citrix Systems, Inc. All rights reserved.

配置 Notes Traveler 服务器

以下信息对应于 IBM Domino Administrator 客户端中的配置页面。

- **安全性：** Internet 身份验证设置为“更少的名称变体，更高的安全性”。此设置用于在 LDAP 身份验证协议中将 UID 映射到 AD 用户 ID。
- **NOTES.INI 设置：** 添加 **NTS_AS_ENFORCE_POLICY=false**。这允许 Endpoint Management 而非 Traveler 管理 Secure Mail 策略。此设置可能与当前客户部署冲突，但会简化 Endpoint Management 部署中设备的管理。
- **同步协议：** Secure Mail 目前不支持 IBM Notes 上的 SyncML 和移动设备同步。Secure Mail 通过内置于 Traveler 服务器中的 Microsoft ActiveSync 协议同步邮件、日历和联系人项目。如果 SyncML 被强制作为主要协议，Secure Mail 将无法通过 Traveler 基础架构连接。
- **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。

安全邮件的 S/MIME

Secure Mail 支持安全/多用途 Internet 邮件扩展 (S/MIME)，使用户能够对邮件进行签名和加密，以提高安全性。签名可向收件人保证邮件是由已识别的发件人发送的，而不是冒名顶替者。加密只允许拥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 表示 Secure Mail 在设备操作系统上支持 S/MIME 功能。

S/MIME 功能	IOS	安卓
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，这是一个用于敏感应用程序数据的安全存储区域。Secure Mail 从共享保管库获取证书。有关详细信息，请参阅(#integrating-with-a-digital-identity-provider)部分。	X	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

S/MIME 功能	IOS	安卓
派生凭据支持	Secure Mail 支持使用派生凭据作为证书源。有关派生凭据的详细信息，请参阅 Citrix Endpoint Management 文档中的(/zh-cn/citrix-endpoint-management/authentication/derived-credentials.html)文章。	
通过电子邮件分发证书： 通过电子邮件分发证书需要您创建证书模板，然后使用这些模板请求用户证书。安装并验证证书后，您将导出用户证书，然后通过电子邮件将其发送给用户。然后，用户在 Secure Mail 中打开电子邮件并导入证书。有关详细信息，请参阅(#distributing-certificates-by-email)部分。	X	X
自动导入单用途证书： Secure Mail 会检测证书是仅用于签名还是加密，然后自动导入证书并通知用户。如果证书用于两种目的，系统会提示用户导入它。	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，就会发生这种情况。

数字身份提供程序证书到 Secure Mail 的路径图(/en-us/mobile-productivity-apps/media/xmob-securemail-smime-cert-flow.png)

MDX 共享保管库是一个安全的存储区域，用于存储敏感应用程序数据，例如证书。只有由 Endpoint Management 启用的应用程序才能访问共享保管库。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

先决条件

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 以获取要封装的 .ipa 文件。
   - 使用 MDX Toolkit 封装应用程序。

     如果您将此应用程序部署给已在 Endpoint Management 环境之外拥有该应用程序版本的用户，请为此应用程序使用唯一的应用程序 ID。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 应用程序商店。
   - 告知用户他们必须从 Secure Hub 安装身份提供程序应用程序。根据需要提供有关任何安装后步骤的指导。

     根据您在下一步中配置 Secure Mail 的 S/MIME 策略的方式，Secure Mail 可能会提示用户安装证书或在 Secure Mail 设置中启用 S/MIME。这两个过程的步骤位于在 iOS 版 Secure Mail 上启用 S/MIME。

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

   - 将 S/MIME 证书源策略设置为 **共享保管库**。此设置表示 Secure Mail 使用数字身份提供商存储在其共享保管库中的证书。
   - 要在 Secure Mail 首次启动期间启用 S/MIME，请配置“在 Secure Mail 首次启动期间启用 S/MIME”策略。此策略确定当共享保管库中存在证书时 Secure Mail 是否启用 S/MIME。如果没有可用证书，Secure Mail 会提示用户导入证书。如果未启用此策略，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，这意味着用户必须通过 Secure Mail 设置启用 S/MIME。

使用派生凭据

您可以允许使用派生凭据，而不是与数字身份提供商集成。

将 Secure Mail 添加到 Endpoint Management 时，请将 S/MIME 证书源策略配置为 **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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

通过电子邮件分发证书

您可以通过电子邮件向用户分发证书，而不是与数字身份提供商集成或使用派生凭据。此选项需要本节中详述的以下常规步骤。

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. 创建用于签名和加密电子邮件的证书模板。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发送给用户。
4. 用户在 Secure Mail 中打开电子邮件并导入证书。因此，这些证书仅适用于 Secure Mail。它们不会出现在 iOS 的 S/MIME 配置文件中。

先决条件

本节中的说明基于以下组件：

- XenMobile® Server 10 及更高版本
- 受支持的 Citrix Gateway 版本，以前称为 NetScaler® Gateway
- 适用于 iOS 的 Secure Mail（最低版本 10.8.10）；适用于 Android 设备的 Secure Mail（最低版本 10.8.10）
- Microsoft Windows Server 2008 R2 或更高版本，其中 Microsoft Certificate Services 充当根证书颁发机构 (CA)
- 微软 Exchange：
  - Exchange Server 2016 累积更新 4
  - Exchange Server 2013 累积更新 15
  - Exchange Server 2010 SP3 更新汇总 16

在配置 S/MIME 之前，请完成以下先决条件：

- 通过手动方式或通过 Endpoint Management 中的凭据设备策略将根证书和中间证书交付到移动设备。有关详细信息，请参阅凭据设备策略。
- 如果您正在使用私有服务器证书来保护到 Exchange Server 的 ActiveSync 流量，请执行以下操作：在移动设备上安装所有根证书和中间证书。

为微软证书服务启用 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，检查是否已安装“**证书颁发机构 Web 注册**”。
3. 如果需要，选择“**添加角色服务**”以安装证书颁发机构 Web 注册。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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，点击**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（私有或公共）进行保护。
- 必须通过 HTTPS 访问 Web 注册站点。

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，查找角色服务**。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，选择运行用于 Web 注册的 IIS 实例的服务器。
5. 点击**身份验证**。
6. 确保**Active Directory 客户端证书身份验证**已**启用**。
7. 在右侧窗格中，点击**站点 > Microsoft Internet Information Services 的默认站点 > 绑定**。
8. 如果 HTTPS 绑定不存在，请添加一个。
9. 转到默认网站主页。
10. 点击**SSL 设置**，然后点击**接受客户端证书**。

创建新证书模板

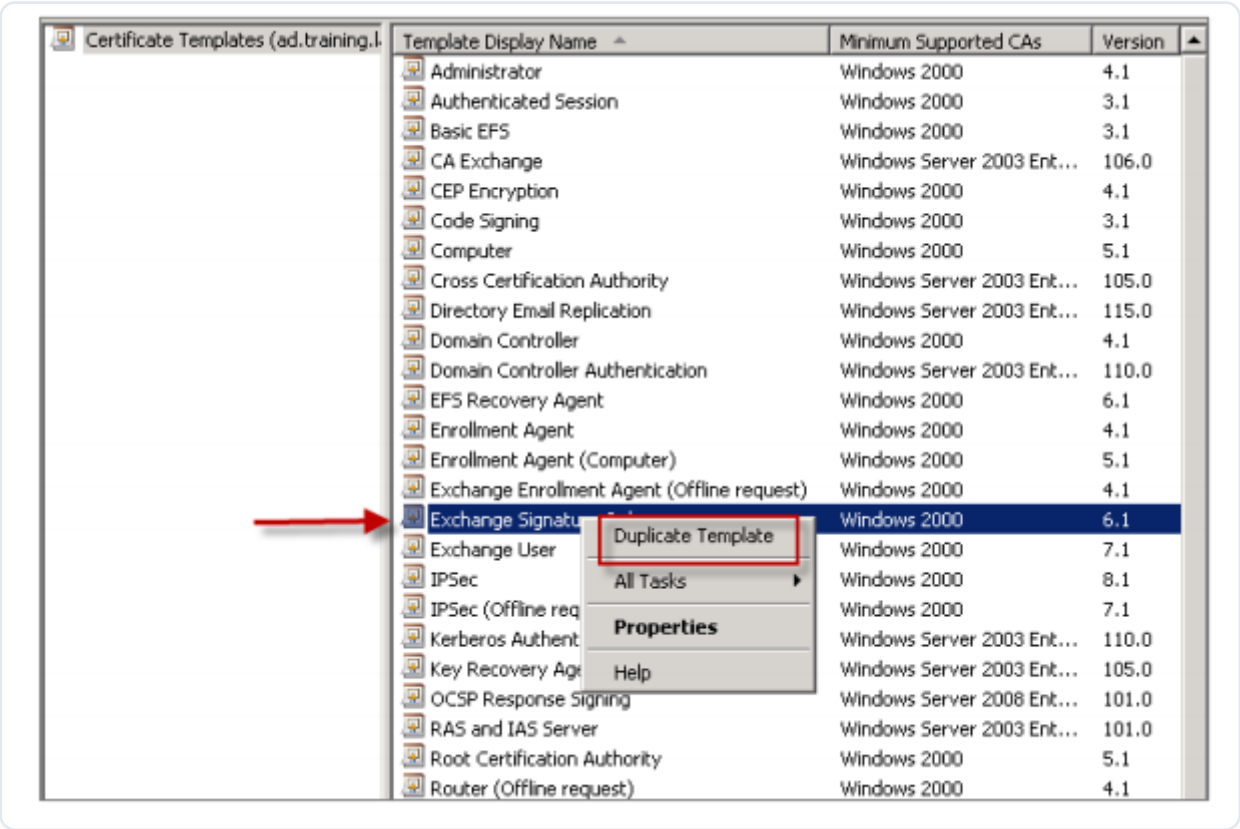
为了签署和加密电子邮件，Citrix 建议您在 Microsoft Active Directory 证书服务上创建证书。如果您将同一个证书用于这两种目的并存档加密证书，则可能会恢复签名证书并允许模拟。

以下过程复制证书颁发机构 (CA) 服务器上的证书模板：

- 仅限 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. 右键单击，然后单击“**管理**”。
4. 搜索“仅限 Exchange 签名”模板，右键单击该模板，然后单击“**复制模板**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

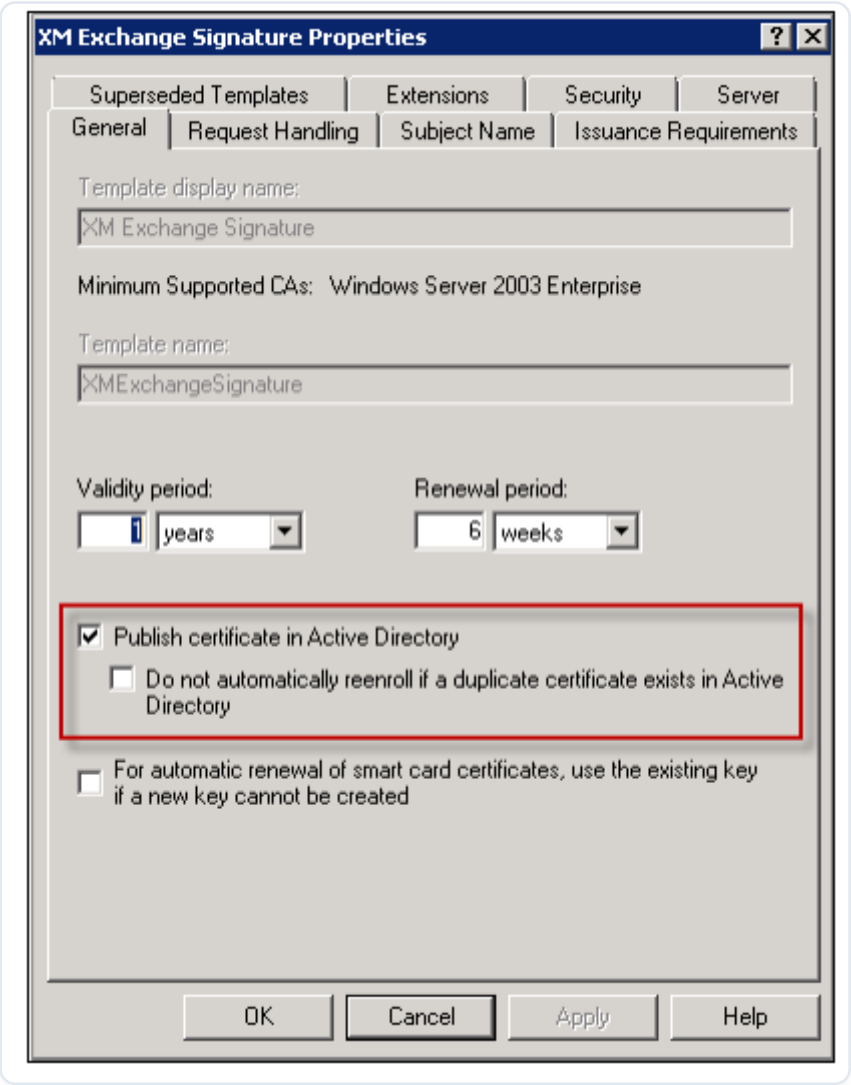


5. 分配任意名称。
6. 选中“**在 Active Directory 中发布证书**”复选框。

注意：

如果您未选中“**在 Active Directory 中发布证书**”复选框，则用户必须手动发布用户证书（用于签名和加密）。他们可以通过“**Outlook 邮件客户端 > 信任中心 > 电子邮件安全性 > 发布到 GAL (全局地址列表)**”来完成此操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. 单击“**请求处理**”选项卡，然后设置以下参数：

   - **用途：** 签名
   - **最小密钥大小：** 2048
   - **允许导出私钥复选框：** 已选中
   - **无需任何用户输入即可注册主题复选框：** 已选中

   请求处理选项卡图像(/en-us/mobile-productivity-apps/media/smime-5.png)

8. 单击“**安全**”选项卡，并在“**组或用户名**”下，确保已添加“**经过身份验证的用户**”（或任何所需的域安全组）。此外，请确保在“**经过身份验证的用户的权限**”下，“**读取和注册**”复选框已选中“**允许**”。

   安全选项卡图像(/en-us/mobile-productivity-apps/media/smime-6.png)

9. 对于所有其他选项卡和设置，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。

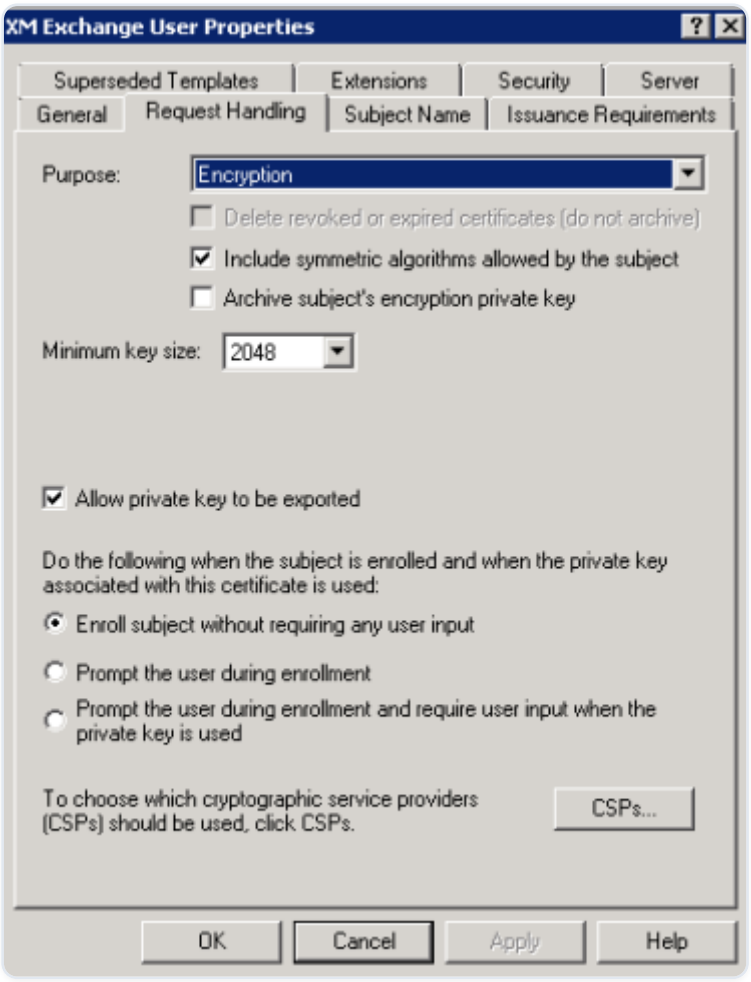
    证书模板对话框图像(/en-us/mobile-productivity-apps/media/smime-7.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

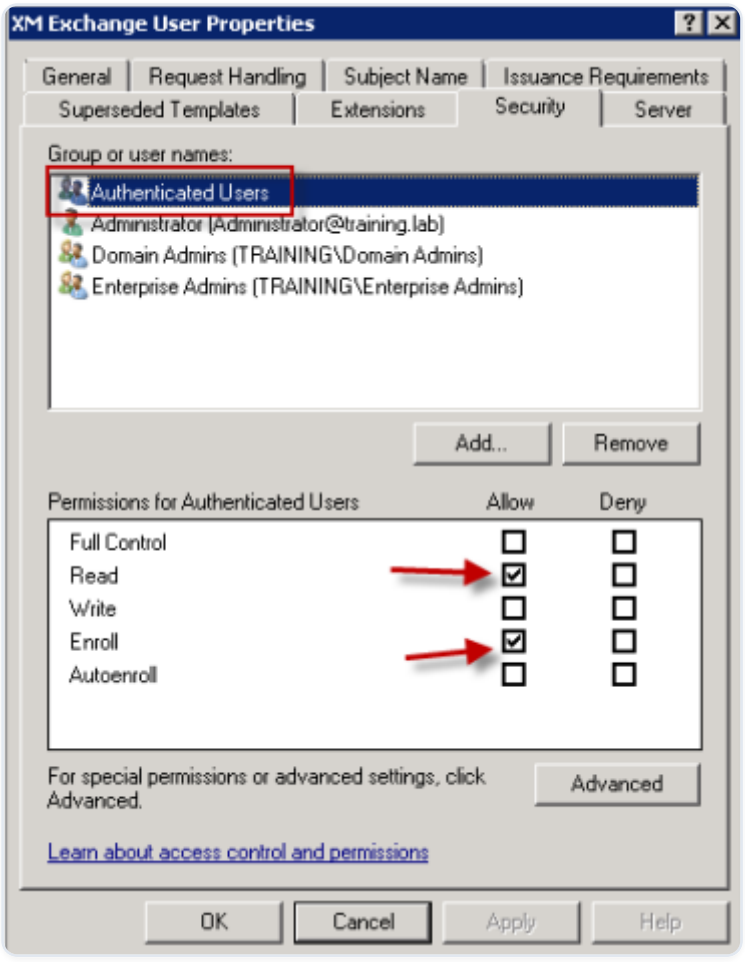
对于新的 Exchange 用户模板，请使用与原始模板相同的默认设置。

11. 单击“**请求处理**”选项卡，然后设置以下参数：

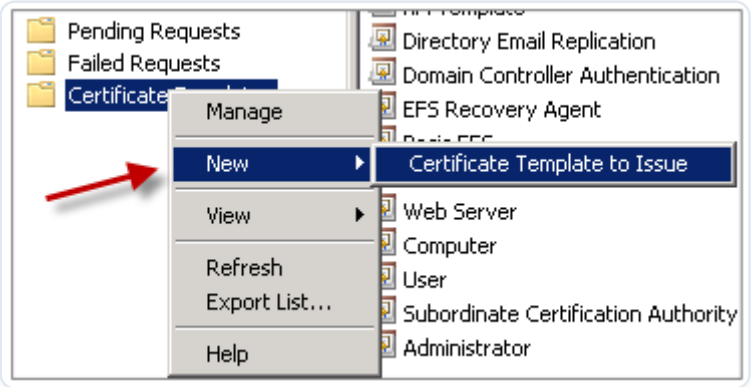
    - **用途：** 加密
    - **最小密钥大小：** 2048
    - **允许导出私钥复选框：** 已选中
    - **注册主题，无需用户输入复选框：** 已选择



© 1997–2026 Citrix Systems, Inc. All rights reserved.



12. 创建这两个模板后，请务必颁发这两个证书模板。单击**新建**，然后单击**要颁发的证书模板**。



请求用户证书

此过程使用“user1”导航到 Web 注册页面；例如，`https://ad.domain.com/certsrv/`。此过程请求两个用于安全电子邮件的新用户证书：一个用于签名，另一个用于加密。您可以对其他需要通过 Secure Mail 使用 S/MIME 的域用户重复相同的过程。

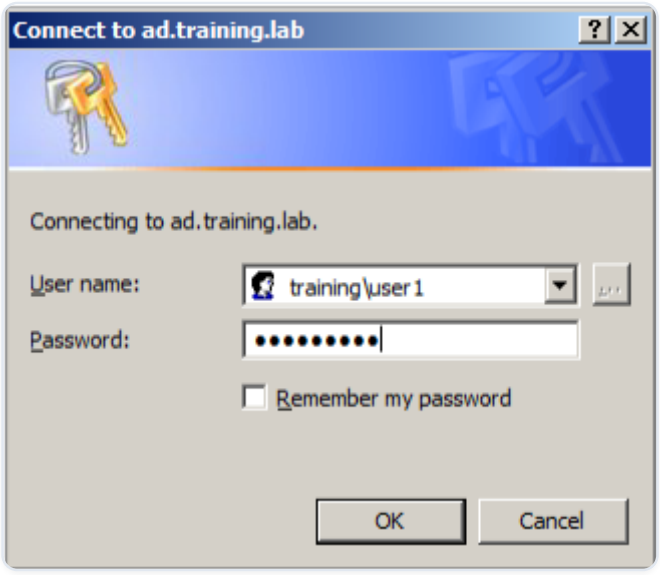
通过 Microsoft 证书服务上的 Web 注册站点（例如，`https://ad.domain.com/certsrv/`）进行手动注册，以生成用于签名和加密的用户证书。另一种方法是通过组策略为将使用此功能的用户组配置自动注册。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

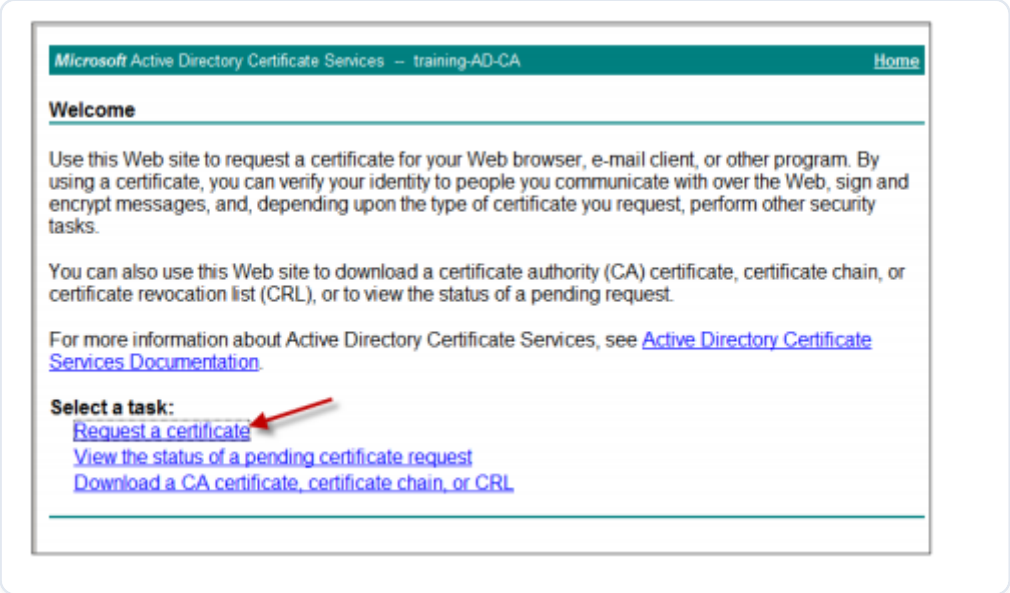
1. 在基于 Windows 的计算机上，打开 Internet Explorer 并转到 Web 注册站点以请求新的用户证书。

   注意：

   请务必使用正确的域用户登录以请求证书。

2. 登录后，单击**请求证书**。

3. 单击**高级证书请求**。
4. 点击“**创建并向此 CA 提交请求**”。
5. 生成用于签名的用户证书。选择相应的模板名称并输入您的用户设置，然后在“**请求格式**”旁边，选择“**PKCS10**”。

   请求已提交。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

高级证书请求选项的图像(/en-us/mobile-productivity-apps/media/smime-17.png)

6. 点击“**安装此证书**”。
7. 验证证书是否已成功安装。

   安装成功确认的图像(/en-us/mobile-productivity-apps/media/smime-19.png)

8. 重复相同的过程，但现在用于加密电子邮件。在同一用户登录到 Web 注册站点的情况下，转到“主页”链接以请求新证书。
9. 选择用于加密的新模板，然后输入您在步骤 5 中输入的相同用户设置。

   新模板选项的图像(/en-us/mobile-productivity-apps/media/smime-21.png)

10. 确保您已成功安装证书，然后重复相同的过程，为另一个域用户生成一对用户证书。此示例遵循相同的过程，并为“User2”生成一对证书。

> **注意：**
>
> 此过程使用同一台基于 Windows 的计算机为“User2”请求第二对证书。

验证已发布的证书

1. 为确保证书已正确安装在域用户配置文件中，请转到“**Active Directory 用户和计算机 > 查看 > 高级功能**”。

   高级功能选项的图像(/en-us/mobile-productivity-apps/media/smime-22.png)

2. 转到用户属性（本例中为 User1），然后单击**已发布的证书**选项卡。确保两个证书都可用。您还可以验证每个证书是否具有特定用途。

   已发布的证书选项卡的图像(/en-us/mobile-productivity-apps/media/smime-23.png)

   此图显示了用于加密电子邮件的证书。

   用于加密电子邮件的证书图像(/en-us/mobile-productivity-apps/media/smime-24.png)

   此图显示了用于签署电子邮件的证书。

   用于签署电子邮件的证书图像(/en-us/mobile-productivity-apps/media/smime-25.png)

   确保已将正确的加密证书分配给用户。您可以在**Active Directory 用户和计算机 > 用户属性**下验证此信息。

   用户属性图像(/en-us/mobile-productivity-apps/media/smime-49.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure Mail 的工作方式是通过 LDAP 查询检查 userCertificate 用户对象属性。您可以在**属性编辑器**选项卡上读取此值。如果此字段为空或具有不正确的用户加密证书，Secure Mail 将无法加密（或解密）邮件。

属性编辑器选项卡的图像(/en-us/mobile-productivity-apps/media/smime-50.png)

导出用户证书

此过程将“User1”和“User2”对证书以 .PFX (PKCS#12) 格式与私钥一起导出。导出后，证书将通过 Outlook Web Access (OWA) 以电子邮件形式发送给用户。

1. 打开 MMC 控制台，然后转到**证书 - 当前用户**管理单元。您会看到“User1”和“User2”对证书。

   当前用户证书的图像(/en-us/mobile-productivity-apps/media/smime-26.png)
2. 右键单击证书，然后单击“**所有任务 > 导出**”。
3. 通过选择“**是，导出私钥**”来导出私钥。
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。

   个人信息交换选项的图像(/en-us/mobile-productivity-apps/media/smime-29.png)
5. 导出第一个证书后，对用户的其余证书重复相同的过程。

   注意：

   清楚地标明哪个证书是签名证书，哪个证书是加密证书。在此示例中，证书标记为 userX-sign.pfx 和 userX-enc.pfx。

   证书标签的图像(/en-us/mobile-productivity-apps/media/smime-30.png)

通过电子邮件发送证书

将所有证书导出为 PFX 格式后，可以使用 Outlook Web Access (OWA) 通过电子邮件发送它们。此示例的登录名为 User1，发送的电子邮件包含两个证书。

用于发送证书的 OWA 邮件图像(/en-us/mobile-productivity-apps/media/smime-31.png)

对 User2 或域中的其他用户重复相同的过程。

在适用于 iOS 和 Android 的 Secure Mail 上启用 S/MIME

电子邮件送达后，下一步是使用 Secure Mail 打开邮件，并使用适当的签名和加密证书启用 S/MIME。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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. 点击签名证书以下载和导入。
3. 输入从服务器导出签名证书时分配给私钥的密码。

   私钥密码选项的图像(/en-us/mobile-productivity-apps/media/smime-34.png)

   您的证书已导入。
4. 点击 **打开签名**

   导入签名证书选项的图像(/en-us/mobile-productivity-apps/media/smime-32.png)
5. 或者，您可以导航到 **设置** > 和 **S/MIME**，然后点击 S/MIME 以打开签名证书。

   S/MIME 设置的导入证书图像(/en-us/mobile-productivity-apps/media/smime-33.png)
6. 在 **签名** 屏幕中，验证是否导入了正确的签名证书。

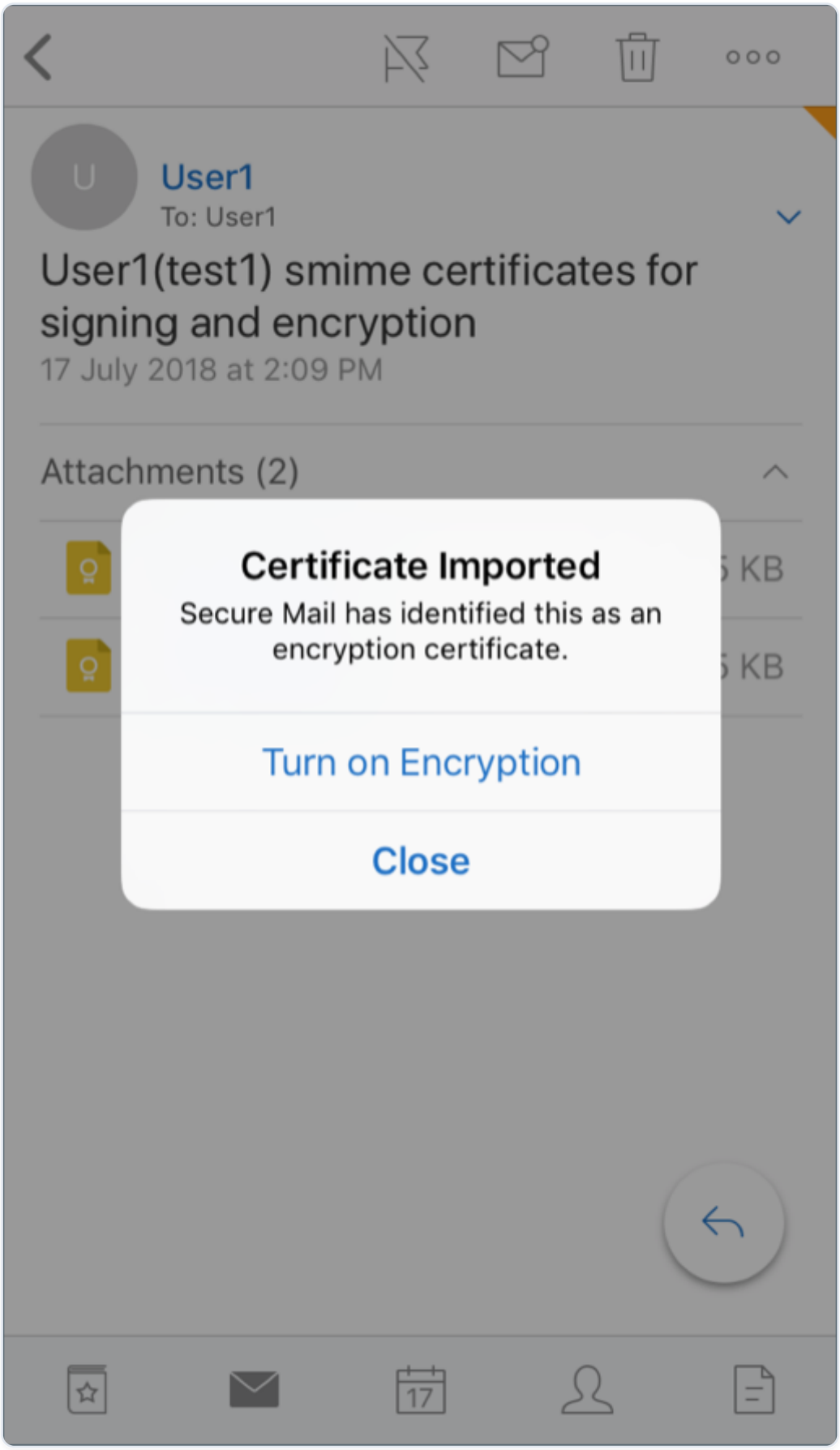
   签名证书确认的图像(/en-us/mobile-productivity-apps/media/smime-37.png)
7. 返回电子邮件，然后点击加密证书以下载和导入。

   导入加密证书选项的图像(/en-us/mobile-productivity-apps/media/smime-38.png)
8. 输入从服务器导出加密证书时分配给私钥的密码。

   密码提示的图像(/en-us/mobile-productivity-apps/media/smime-39.png)

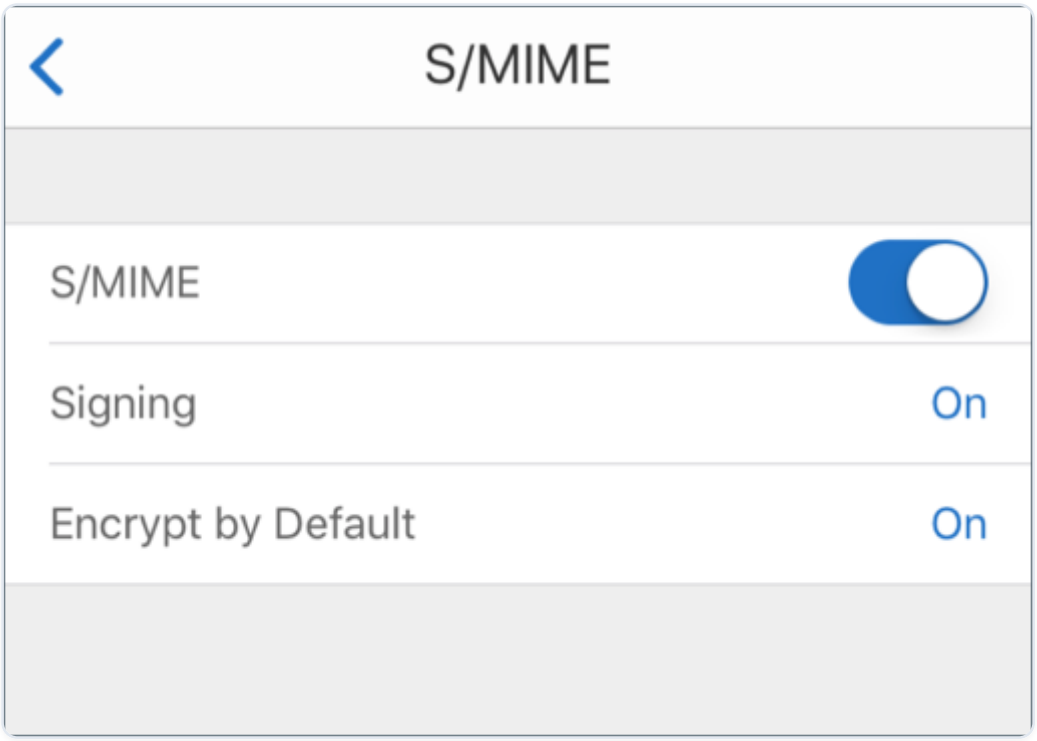
   您的证书已导入。
9. 点击 **打开加密**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

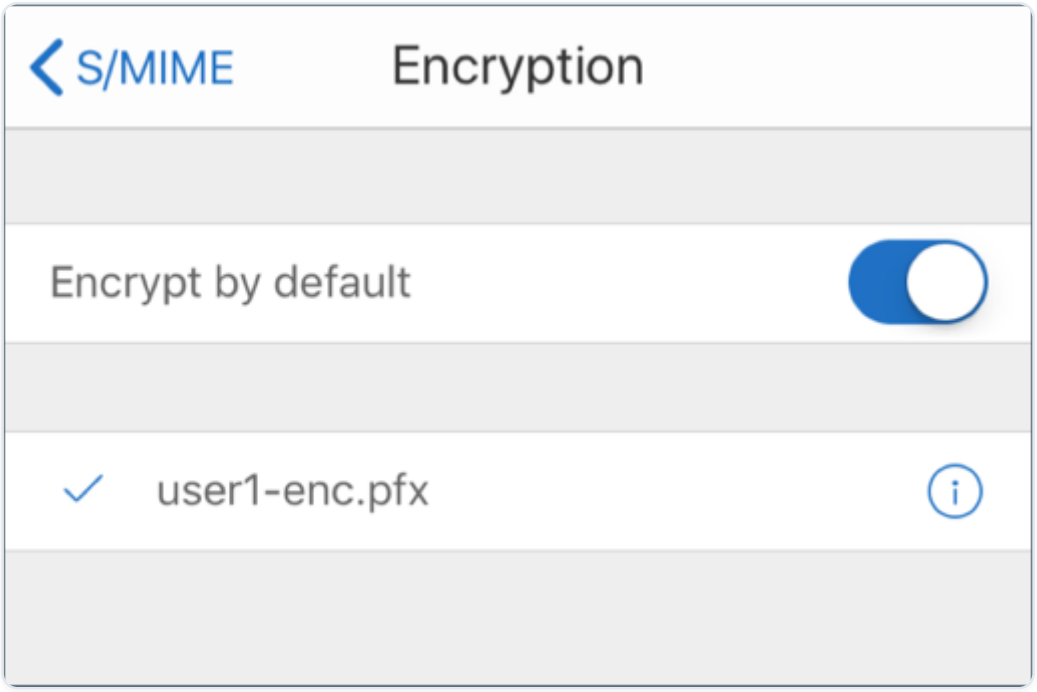


10. 或者，您可以导航到 **设置** > 和 **S/MIME**，然后点击 S/MIME 以启用 **默认加密**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



11. 在 **加密** 屏幕中，验证是否已导入正确的加密证书。



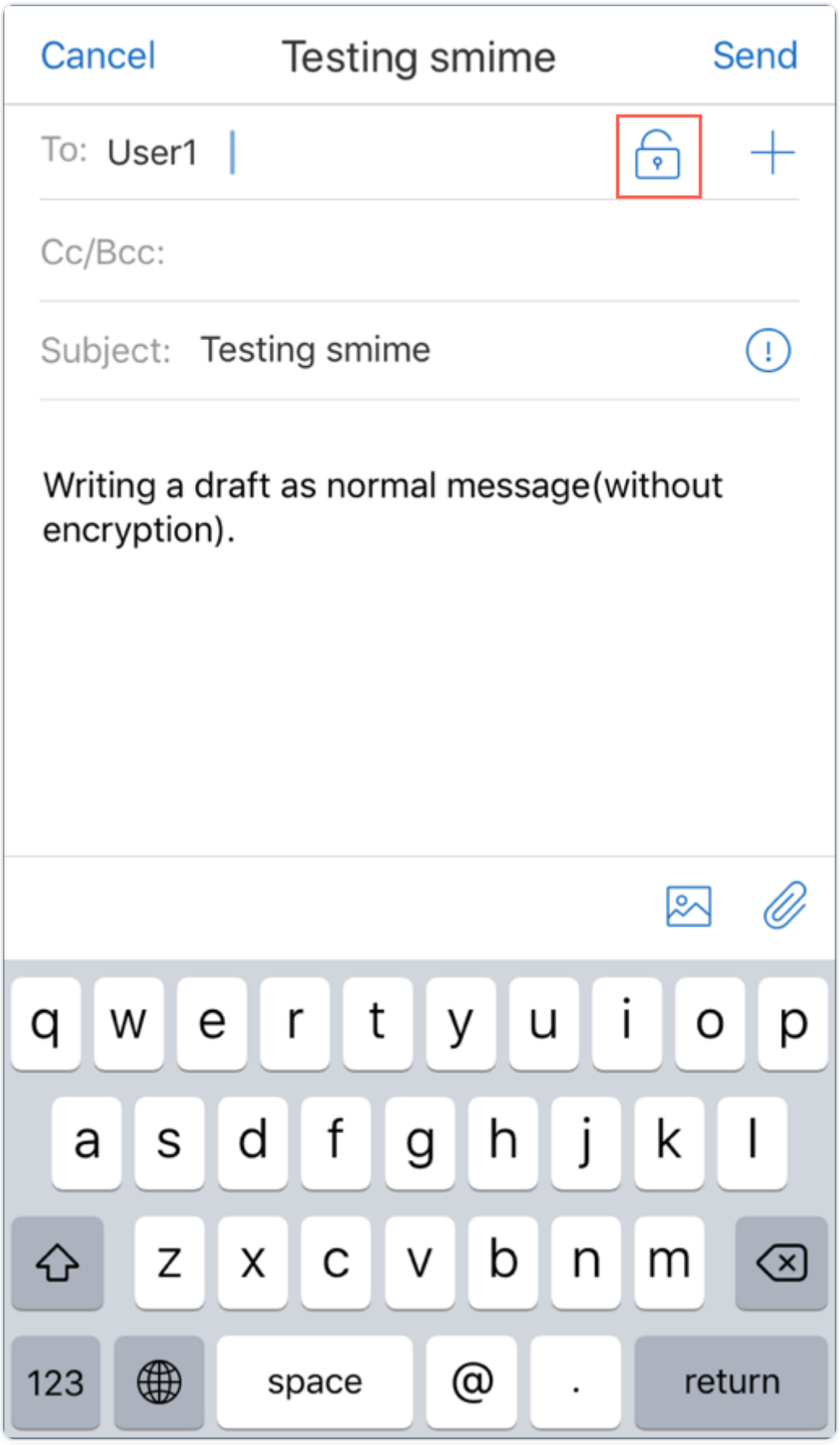
© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

a. 如果电子邮件使用 S/MIME 进行数字签名，包含附件，并且收件人未启用 S/MIME，则不会收到附件。此行为是 Active Sync 的限制。要有效接收 S/MIME 邮件，请在 Secure Mail 设置中打开 S/MIME。

b. **默认加密** 选项可让您最大限度地减少加密电子邮件所需的步骤。如果此功能处于“开”状态，则在撰写时您的电子邮件将处于加密状态。如果此功能处于“关”状态，则在撰写时您的电子邮件将处于未加密状态，您必须点击 **锁定** 图标才能加密。

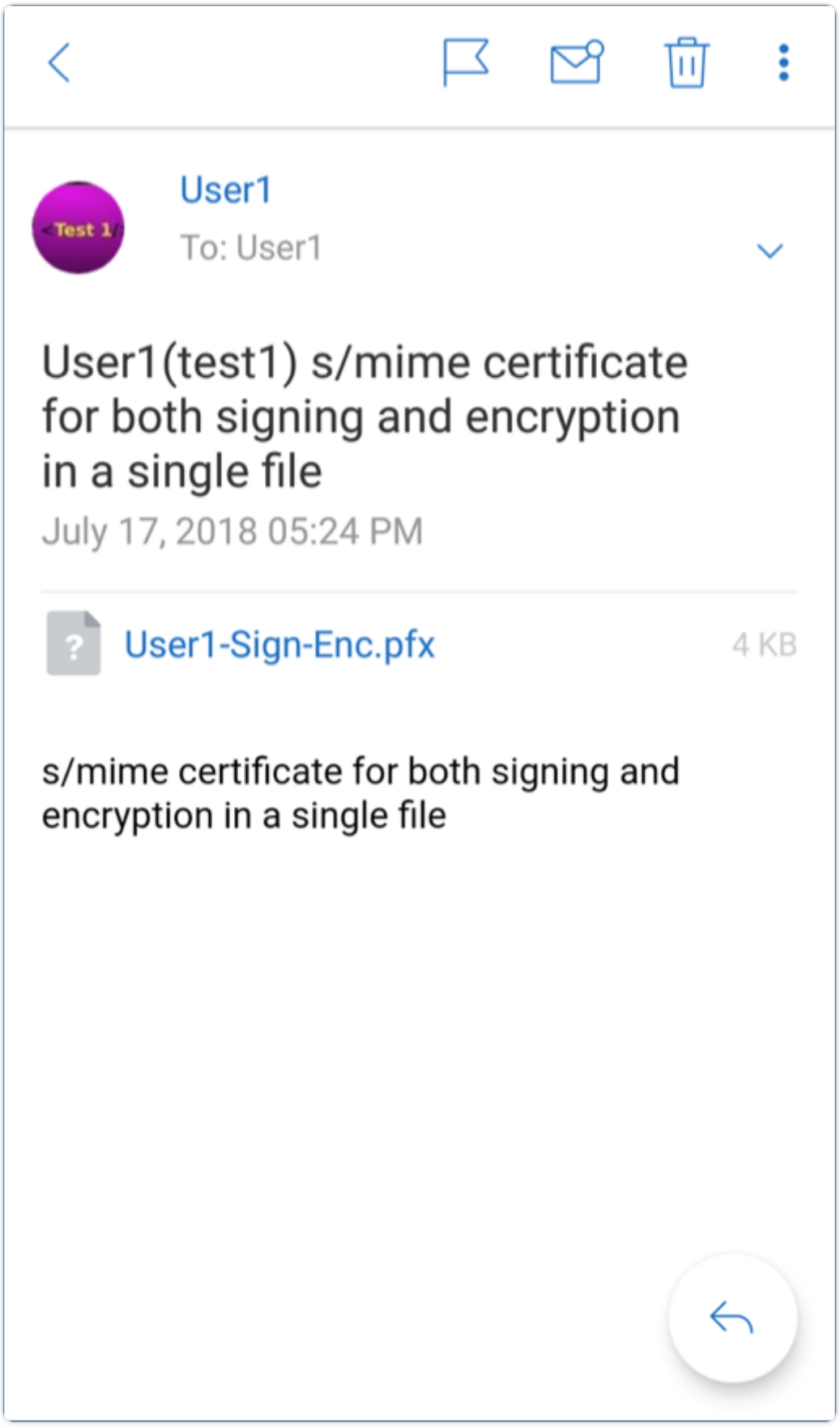
© 1997–2026 Citrix Systems, Inc. All rights reserved.



使用单个签名和加密证书启用 S/MIME

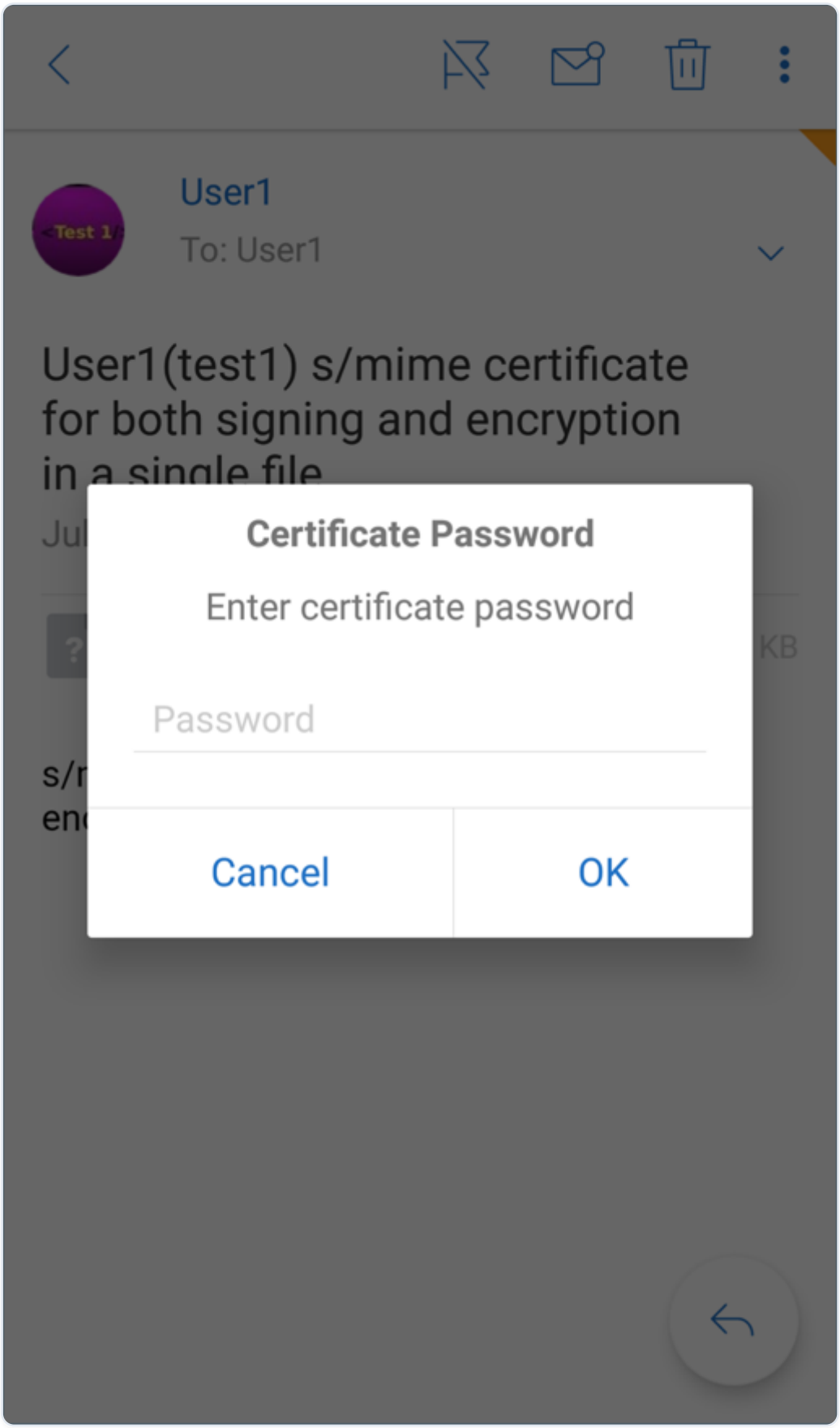
1. 打开 Secure Mail，导航到包含 S/MIME 证书的电子邮件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



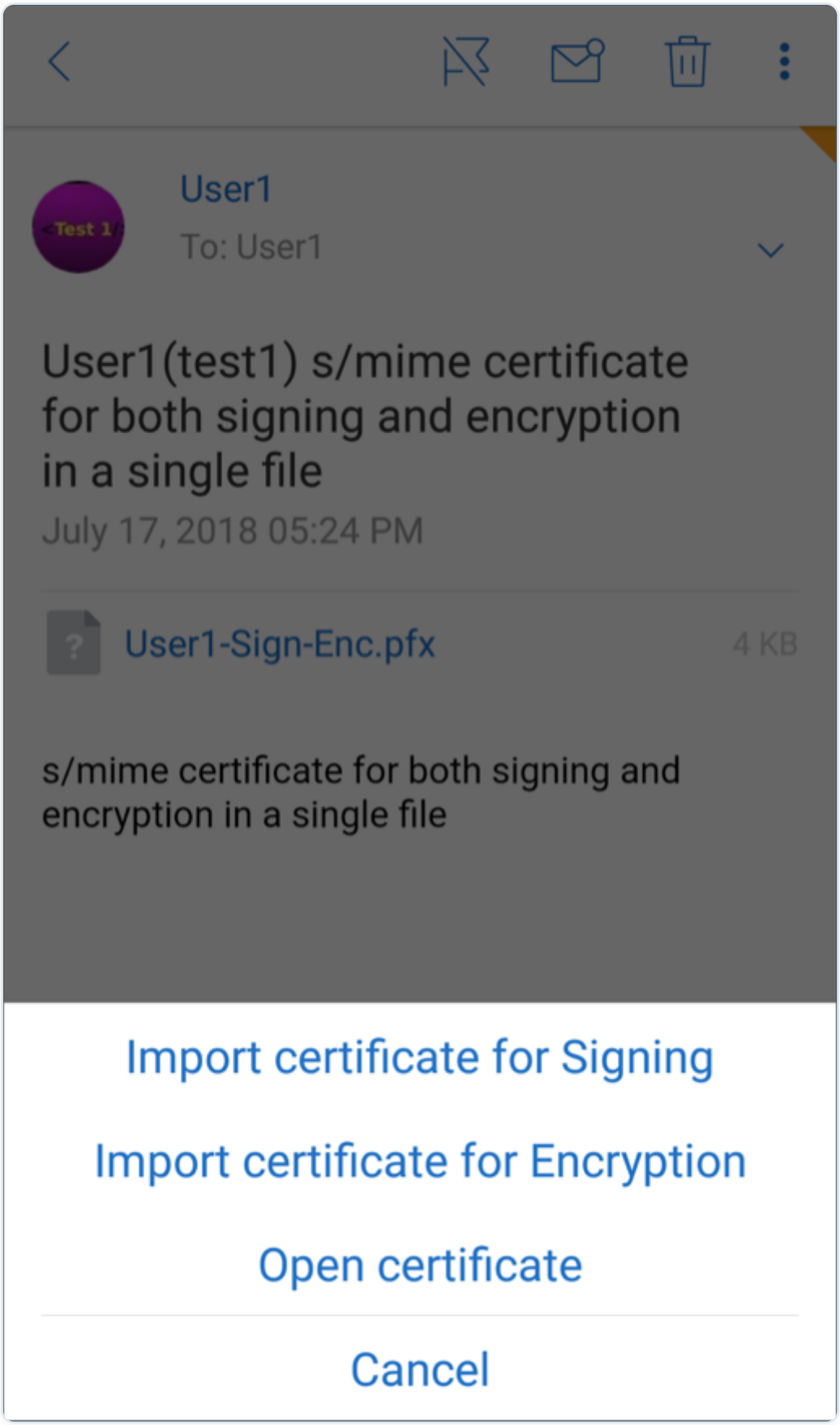
2. 点击 S/MIME 证书以下载和导入。
3. 输入从服务器导出证书时分配给私钥的密码。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 从出现的证书选项中，点击相应的选项以导入签名证书或加密证书。 点击**打开证书**以查看证书的详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



您的证书已导入。

您可以通过导航到**设置 > S/MIME**来查看已导入的证书。

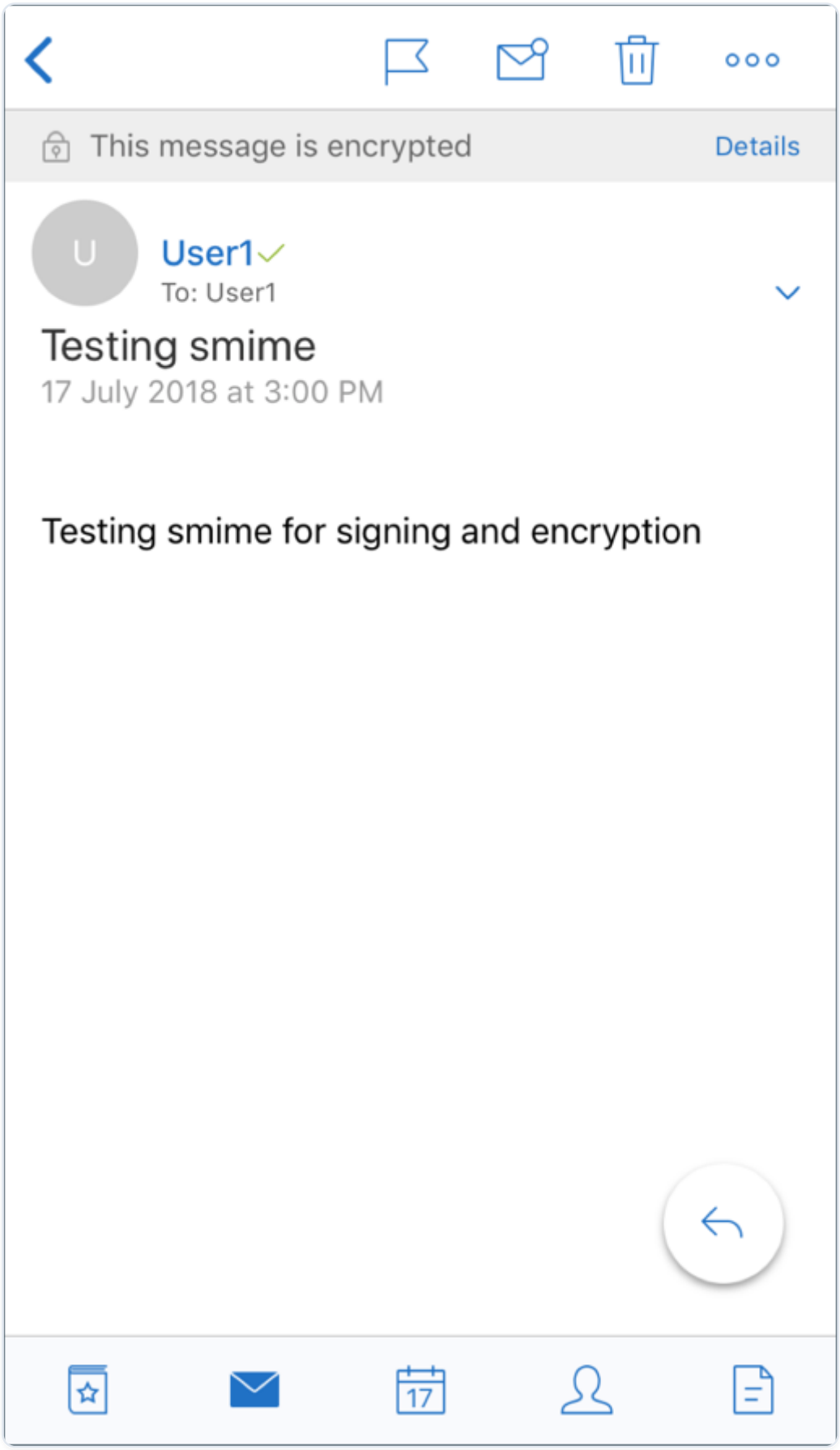
© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 iOS 和 Android 上测试 S/MIME

完成上一节中列出的步骤后，收件人即可阅读您已签名和加密的邮件。

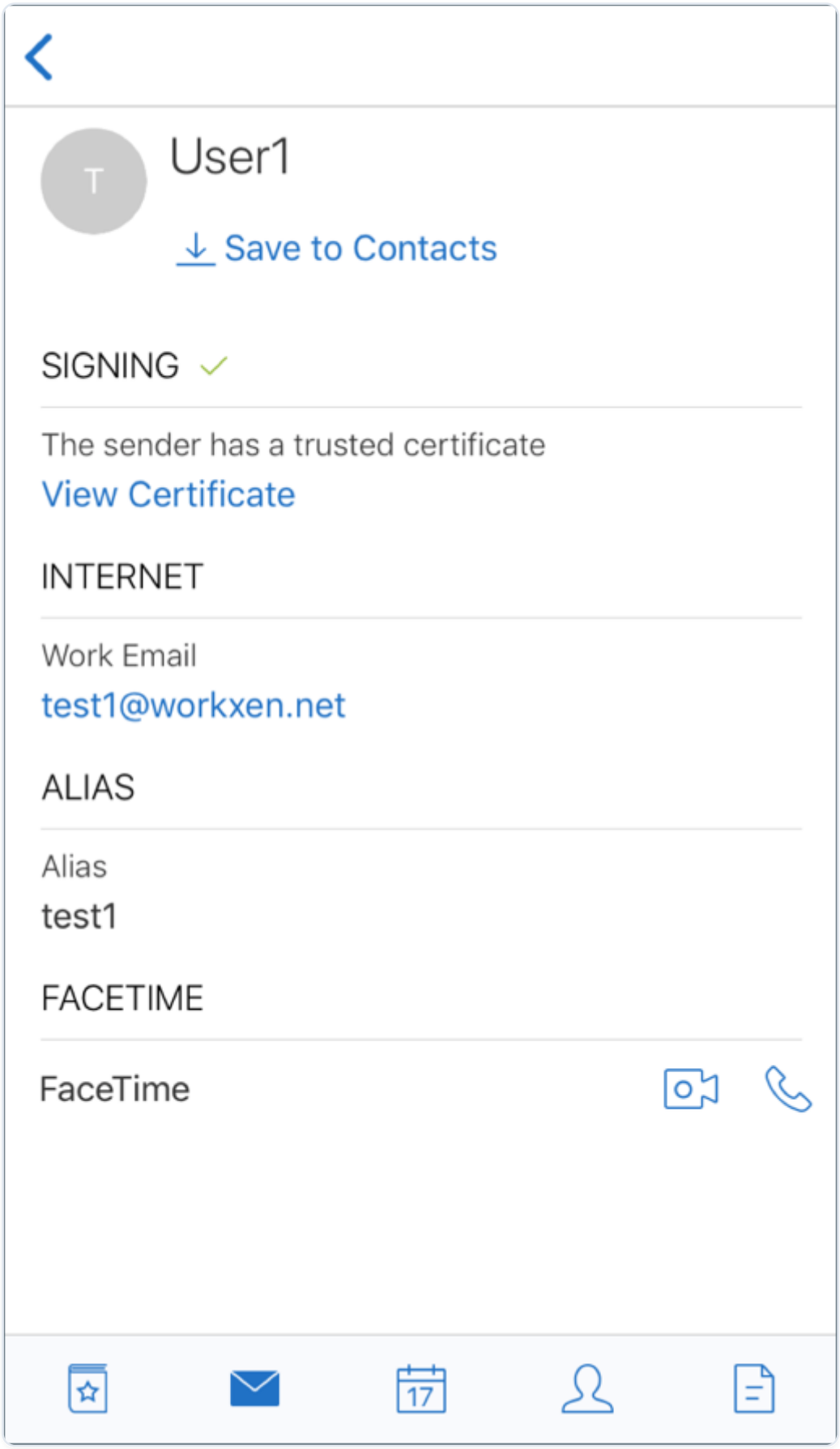
下图显示了收件人阅读的加密邮件示例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



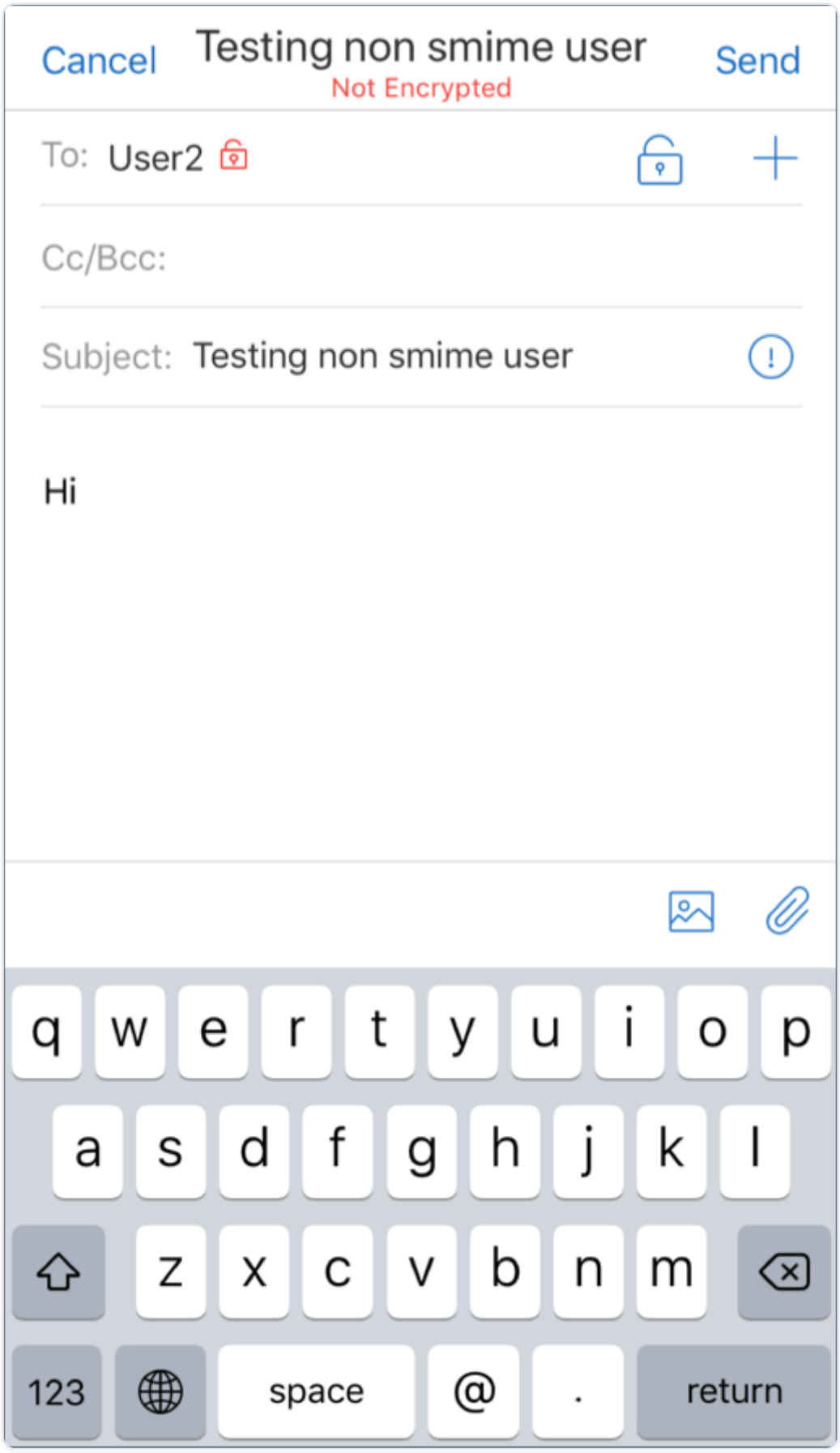
下图显示了已签名受信任证书的验证示例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Secure Mail 会在 Active Directory 域中搜索收件人的公共加密证书。如果用户向没有有效公共加密密钥的收件人发送加密邮件，则该邮件将以未加密形式发送。在群组邮件中，即使只有一个收件人没有有效密钥，该邮件也会以未加密形式发送给所有收件人。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

配置公共证书源

要使用 S/MIME 公共证书，请配置 S/MIME 公共证书源、LDAP 服务器地址、LDAP 基本 DN 和匿名访问 LDAP 策略。

除了应用程序策略之外，请执行以下操作。

- 如果 LDAP 服务器是公共的，请确保流量直接流向 LDAP 服务器。为此，请将 Secure Mail 的网络策略配置为**隧道连接到内部网络**，并为 Citrix ADC 配置拆分 DNS。
- 如果 LDAP 服务器位于内部网络上，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。如果您配置了该策略，用户将频繁收到身份验证提示。
  - 对于 Android，请确保您在后台网络服务网关策略的列表中添加了 **LDAP 服务器 URL**。

Secure Mail 的单点登录

您可以将 Endpoint Management 配置为在用户注册 Secure Hub 时自动注册 Secure Mail。用户无需输入更多信息或执行更多步骤即可注册 Secure Mail。对于使用电子邮件凭据注册 Secure Hub 的用户，此功能要求启用自动发现。如果未启用自动发现，则可以为以下注册方法启用此功能：

- Endpoint Management 的地址信息会从 Secure Hub 传输到 Secure Mail。
- 用户在注册 Secure Hub 时输入 Endpoint Management 地址。

启用 Secure Mail 中的自动注册

1. 在 Endpoint Management 客户端属性中，在“**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. 添加此配置：

   - **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：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 **User email address**。
   - 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自动发现服务。如需支持，请联系您的 Microsoft Exchange 管理员。本文假设您通过查询 DNS 以获取 SRV 记录来配置自动发现服务。

配置 Secure Mail 应用程序策略

将 Secure Mail 应用程序上传到 Endpoint Management。上传与正确版本的 Secure Mail 应用程序关联的 .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 **User email address**。
2. 在 **Initial authentication credentials** 中，单击 **userPrincipalName** 或 **sAMAccountName**。您的选择取决于针对用户 Exchange 邮件服务器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，并进行必要的交付组分配。

具有自动预配功能的端到端 Secure Mail SSO 用户体验

确保满足以下先决条件。

1. 从 Apple 应用商店 (iOS) 或 Google Play 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注册 Endpoint Management。
3. 从 Apple 应用商店 (iOS) 或 Google Play 商店 (Android) 安装 Secure Mail。
4. 打开 Secure Mail 并点击 **确定**。此步骤允许 Secure Hub 管理 Secure Mail。打开后，Secure Mail 会自动配置。

与用户邮箱数据库对应的 Exchange Server 是从您配置的自动发现服务中获取的。DNS SRV 记录查询利用从 Secure Hub 获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，均从 Secure Hub 获取。

配置帐户后，用户可以在设备上通过 **Secure Mail** > **设置** > **帐户** 查看详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

故障排除

如果 SSO 配置出现任何问题，您可以尝试以下步骤。

1. 确保 XenMobile Server 版本为 10.5 或更高版本。
2. 确保 Endpoint Management 已配置为使用自动发现服务，并且用户注册已配置为使用电子邮件地址。
3. 确保 Exchange Server 域已配置自动发现。确保 SRV 记录查询返回 ActiveSync 邮件客户端的预期邮件服务器详细信息。
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。
    - 收集最高日志级别的 Secure Mail 诊断日志。
    - 从托管自动发现服务的 Exchange Server 的目录 C:\inetpub\logs\LogFiles\W3SVC1 中收集 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全注意事项

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

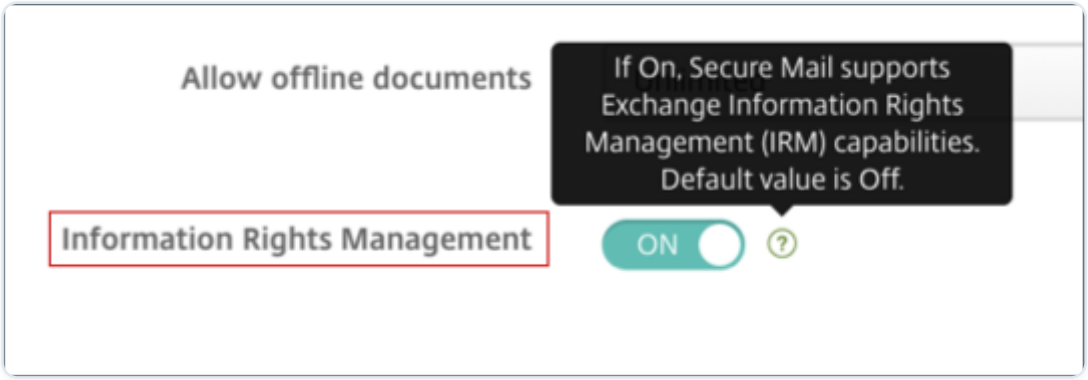
支持 Microsoft IRM 和 AIP 电子邮件权限保护

适用于 Android 和 iOS 的 Secure Mail 支持受 Microsoft 信息权限管理 (IRM) 和 Azure 信息保护 (AIP) 解决方案保护的邮件。此支持受 Citrix Endpoint Management 上配置的 IRM 策略的约束。

此功能允许使用 IRM 的组织对消息内容应用保护。该功能还允许移动设备用户创建和使用受权限保护的内容。默认情况下，IRM 支持处于**关闭**状态。要启用 IRM 支持，请将信息权限管理策略设置为**开启**。

在 Secure Mail 中启用信息权限管理

1. 登录到 Endpoint Management，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，选择并上传 .mdx 文件。
5. 在“**应用程序设置**”下启用信息权限管理。



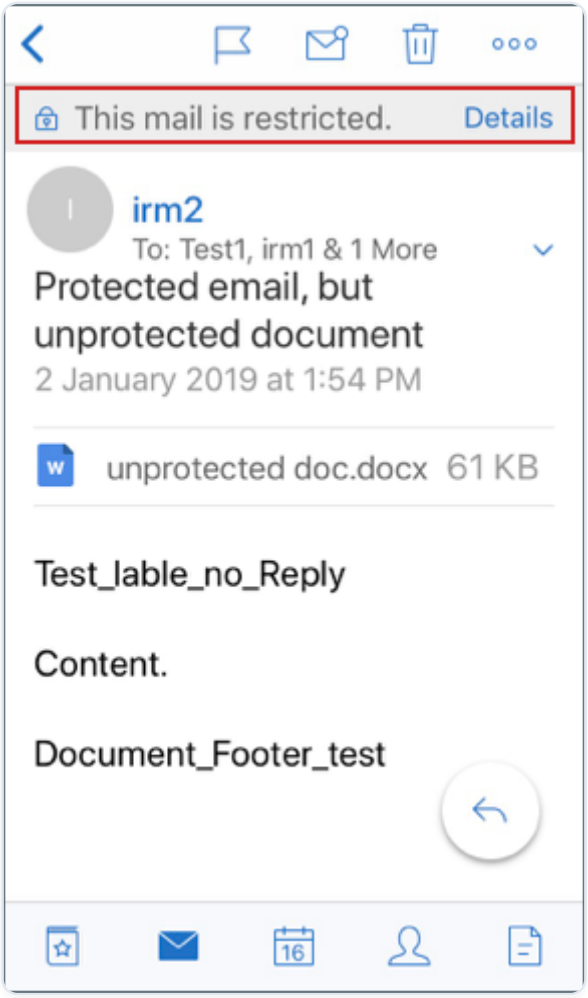
注意：

为 iOS 和 Android 启用信息权限管理。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

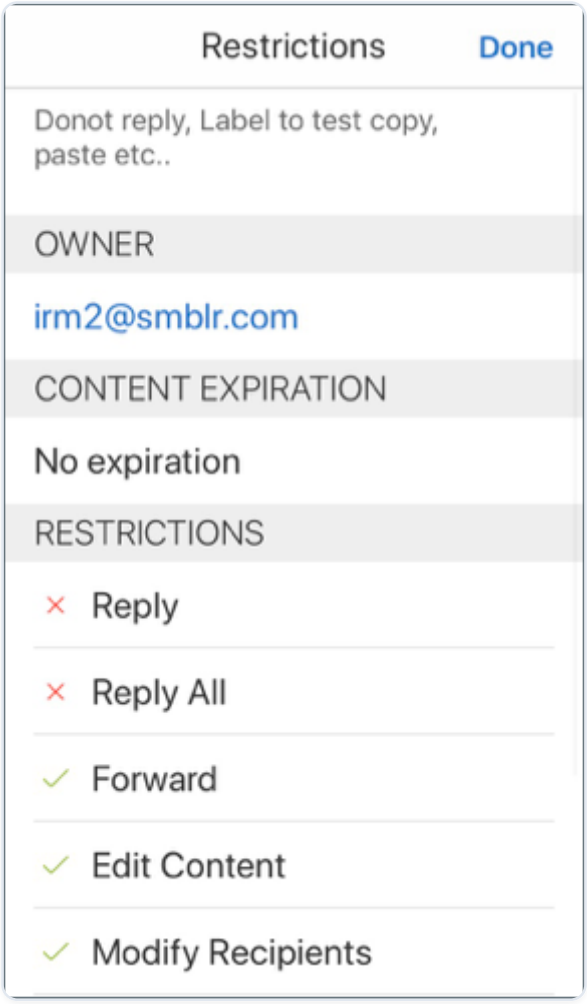
当您收到受权限保护的电子邮件时

当用户收到包含受保护内容的邮件时，他们会看到以下屏幕：



要查看用户有权获得的详细信息，请点击**详细信息**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



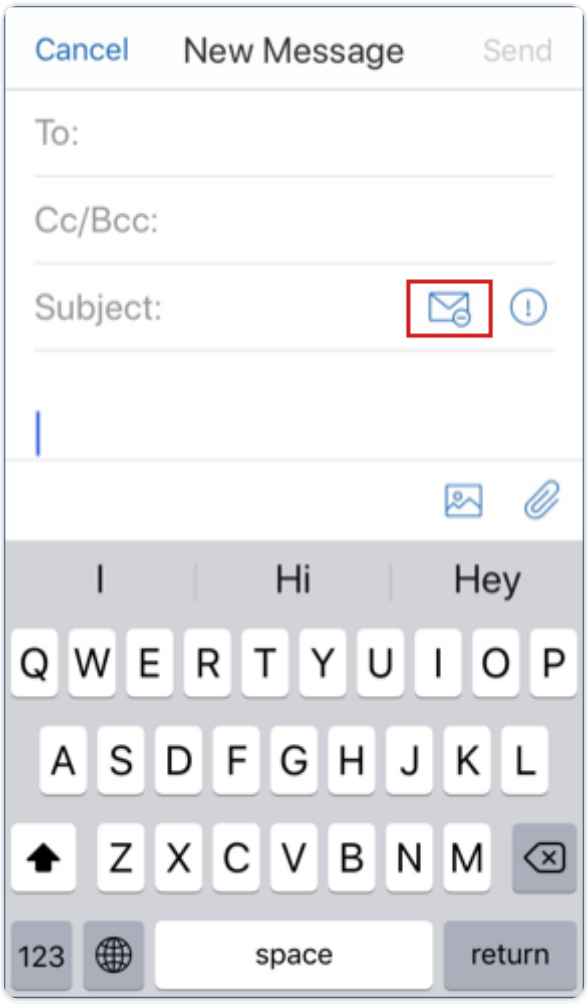
撰写受权限保护的电子邮件时

用户撰写邮件时，可以设置限制配置文件以启用电子邮件保护。

要为您的电子邮件设置限制：

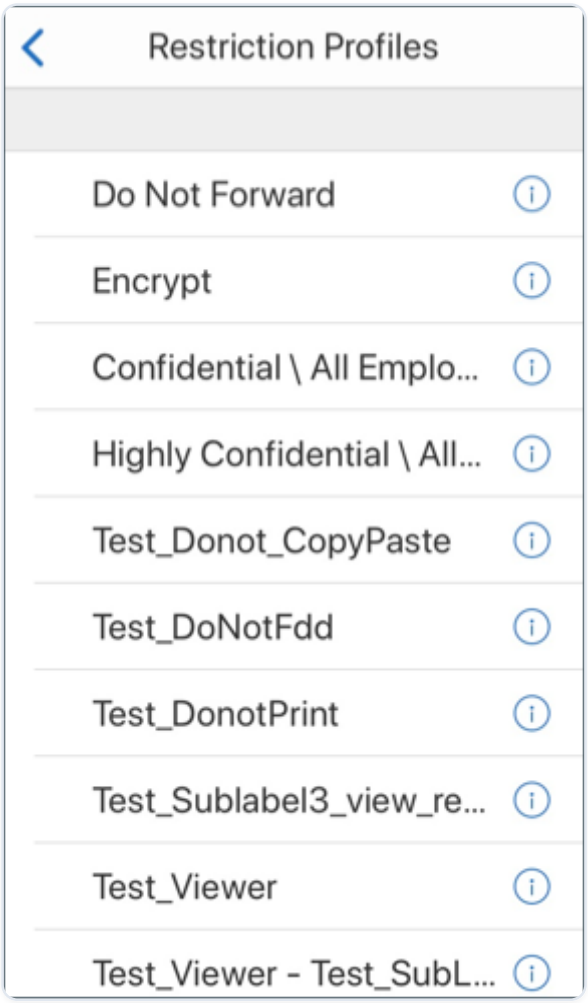
1. 登录 Secure Mail 并点击**撰写**图标。
2. 在撰写屏幕中，点击**电子邮件限制**图标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



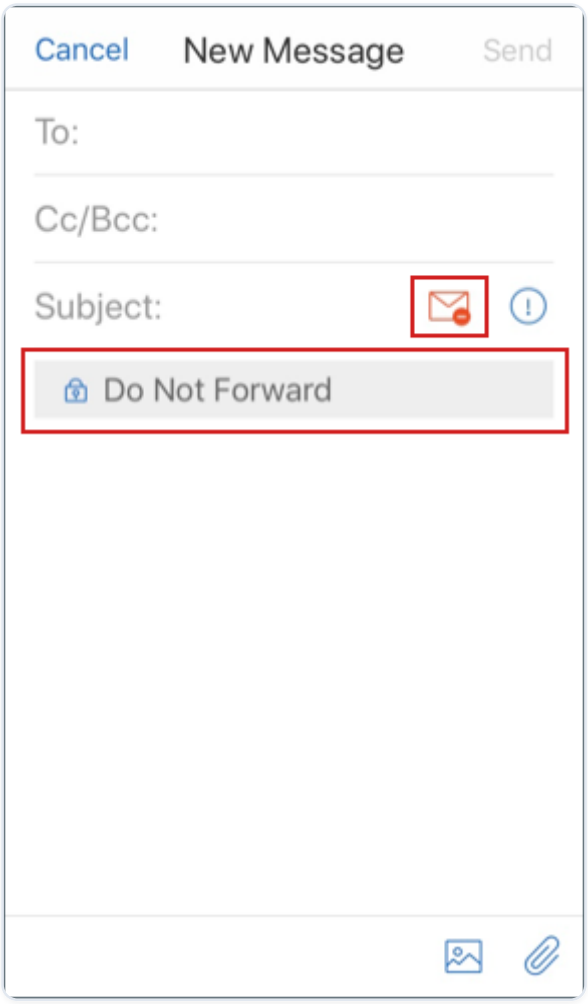
3. 在**限制配置文件**屏幕中，点击要应用于电子邮件的所需限制，然后点击返回。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



应用的限制显示在主题字段下方。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



某些组织可能要求严格遵守其 IRM 策略。有权访问 Secure Mail 的用户可能会尝试通过篡改 Secure Mail、操作系统甚至硬件平台来绕过 IRM 策略。

尽管 Endpoint Management 可以检测到某些攻击，但请考虑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南。
- 使用 Endpoint Management 功能或其他方式相应地配置设备。
- 为您的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御此类攻击。

电子邮件安全分类

适用于 iOS 和 Android 的 Secure Mail 支持电子邮件分类标记，使用户能够在发送电子邮件时指定安全 (SEC) 和传播限制标记 (DLM)。SEC 标记包括“受保护”、“机密”和“秘密”。DLM 包括“敏感”、“法律”或“个人”。撰写电子邮件时，Secure Mail 用户可以选择一个标记来指示电子邮件的分类级别，如以下图像所示。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure Mail 中的安全分类链接(/en-us/mobile-productivity-apps/media/worx-mail-security-class-selection1.png)

Secure Mail 中的安全分类列表(/en-us/mobile-productivity-apps/media/worx-mail-security-class-selection2.png)

收件人可以在电子邮件主题中查看分类标记。例如：

- 主题：规划
- 主题：规划
- 主题：规划

电子邮件标头包含作为 Internet 消息标头扩展的分类标记，在此示例中以粗体文本显示：

日期: Fri, 01 May 2015 12:34:50 +530

主题：规划

优先级: 正常

X-优先级: 正常 **`X-Protective-Marking: VER-2012.3, NS=gov.au,SEC = PROTECTED, DLM = Sensitive,`**`ORIGIN=operations@example.com`

发件人：`operations@example.com`

收件人：团队 **`<`**`mylist@example.com`**`>`**

MIME 版本：1.0 内容类型：**`multipart/alternative;boundary="_com.example.email_6428E5E4-9DB3-4133-9F48-155913E39A980"`**

Secure Mail 仅显示分类标记。该应用程序不根据这些标记执行操作。

当用户回复或转发带有分类标记的电子邮件时，SEC 和 DLM 值默认为原始电子邮件的标记。用户可以选择不同的标记。Secure Mail 不会验证与原始电子邮件相关的此类更改。

您可以通过以下 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 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显示为“X-Protective-Marking”值。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：**指定所用分类标准在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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **电子邮件分类版本：**指定所用分类标准在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：指定如果用户未选择标记，Secure Mail 将应用于电子邮件的保护性标记。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：**指定可供用户使用的分类标记。如果列表为空，Secure Mail 不会包含保护性标记列表。标记列表包含由分号分隔的值对。每对都包含在 Secure Mail 中显示的列表值以及附加到 Secure Mail 中电子邮件主题和标头的标记值。例如，在标记对“UNOFFICIAL,SEC=UNOFFICIAL;”中，列表值为“UNOFFICIAL”，标记值为“SEC=UNOFFICIAL”。

默认值是您可以修改的分类标记列表。Secure Mail 提供了以下标记。

- UNOFFICIAL,SEC=UNOFFICIAL
- UNCLASSIFIED,SEC=UNCLASSIFIED
- 仅供官方使用,DLM=For-Official-Use-Only
- 敏感,DLM=敏感
- 敏感:法律,DLM=敏感:法律
- 敏感:个人,DLM=敏感:个人
- PROTECTED,SEC=PROTECTED
- 受保护+敏感,SEC=受保护
- 受保护+敏感:法律,SEC=受保护 DLM=敏感:法律
- 受保护+敏感:个人,SEC=受保护 DLM=敏感:个人
- 受保护+敏感:档案,SEC=受保护,DLM=敏感:档案
- CONFIDENTIAL,SEC=CONFIDENTIAL
- 机密+敏感,SEC=机密,DLM=敏感
- 机密+敏感:法律,SEC=机密 DLM=敏感:法律
- 机密+敏感:个人,SEC=机密,DLM=敏感:个人
- 机密+敏感:档案,SEC=机密 DLM=敏感:档案
- SECRET,SEC=SECRET
- 绝密+敏感,SEC=绝密,DLM=敏感
- 秘密+敏感:法律,SEC=秘密,DLM=敏感:法律
- 秘密+敏感:个人,SEC=秘密,DLM=敏感:个人
- 秘密+敏感:内阁,SEC=秘密,DLM=敏感:内阁

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- TOP-SECRET,SEC=TOP-SECRET
- 绝密+敏感,SEC=绝密,DLM=敏感
- 绝密+敏感:法律,SEC=绝密 DLM=敏感:法律
- 绝密+敏感:个人,SEC=绝密 DLM=敏感:个人
- 绝密+敏感:内阁,SEC=绝密 DLM=敏感:内阁

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使用 Secure Mail 和 Secure Web 的“**启用 iOS 数据保护**”策略。默认情况下，这些策略处于“**关闭**”状态。

当 Secure Web 的“**启用 iOS 数据保护**”设置为“**开**”时，Secure Web 会对沙盒中的所有文件使用 A 级保护级别。有关 Secure Mail 数据保护的详细信息，请参阅 澳大利亚信号局数据保护。如果您启用此策略，将使用最高数据保护级别，因此无需再指定“**最低数据保护级别**”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 中：对于新应用，请导航到“**配置 > 应用 > 添加**”，然后单击“**MDX**”。对于升级，请参阅 升级 MDX 或企业应用。
2. 对于 Secure Mail，请浏览到“**应用**”设置，找到“**启用 iOS 数据保护**”策略，并将其设置为“**开**”。启用此策略时，运行旧版操作系统的设备不受影响。
3. 对于 Secure Web，请浏览到“**应用**”设置，找到“**启用 iOS 数据保护**”策略，并将其设置为“**开**”。启用此策略时，运行旧版操作系统的设备不受影响。
4. 照常配置应用策略并保存设置，以将应用部署到 Endpoint Management 应用商店。

澳大利亚信号局数据保护

Secure Mail 支持澳大利亚信号局 (ASD) 数据保护，适用于必须满足 ASD 计算机安全要求的企业。默认情况下，“启用 iOS 数据保护”策略为 **“关”**，Secure Mail 提供 C 类数据保护或使用预配配置文件中设置的数据保护。

如果策略为 **“开”**，Secure Mail 会在应用沙盒中创建和打开文件时指定保护级别。Secure Mail 对以下各项设置 A 类数据保护：

- 发件箱项目
- 摄像头或相机胶卷中的照片
- 从其他应用粘贴的图像

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 下载的文件附件

Secure Mail 对以下各项设置 B 类数据保护：

- 存储的邮件
- 日历项目
- 联系人
- ActiveSync 策略文件

B 类保护允许锁定设备进行同步，并允许在下载开始后设备被锁定时完成下载。

启用数据保护后，当设备锁定时，排队的收件箱项目不会发送，因为文件无法打开。如果设备在锁定时终止并重新启动 Secure Mail，则 Secure Mail 无法同步，直到设备解锁并启动 Secure Mail。

Citrix® 建议，如果您启用此策略，仅在需要时启用 Secure Mail 日志记录，以避免创建包含 C 类数据保护的日志文件。

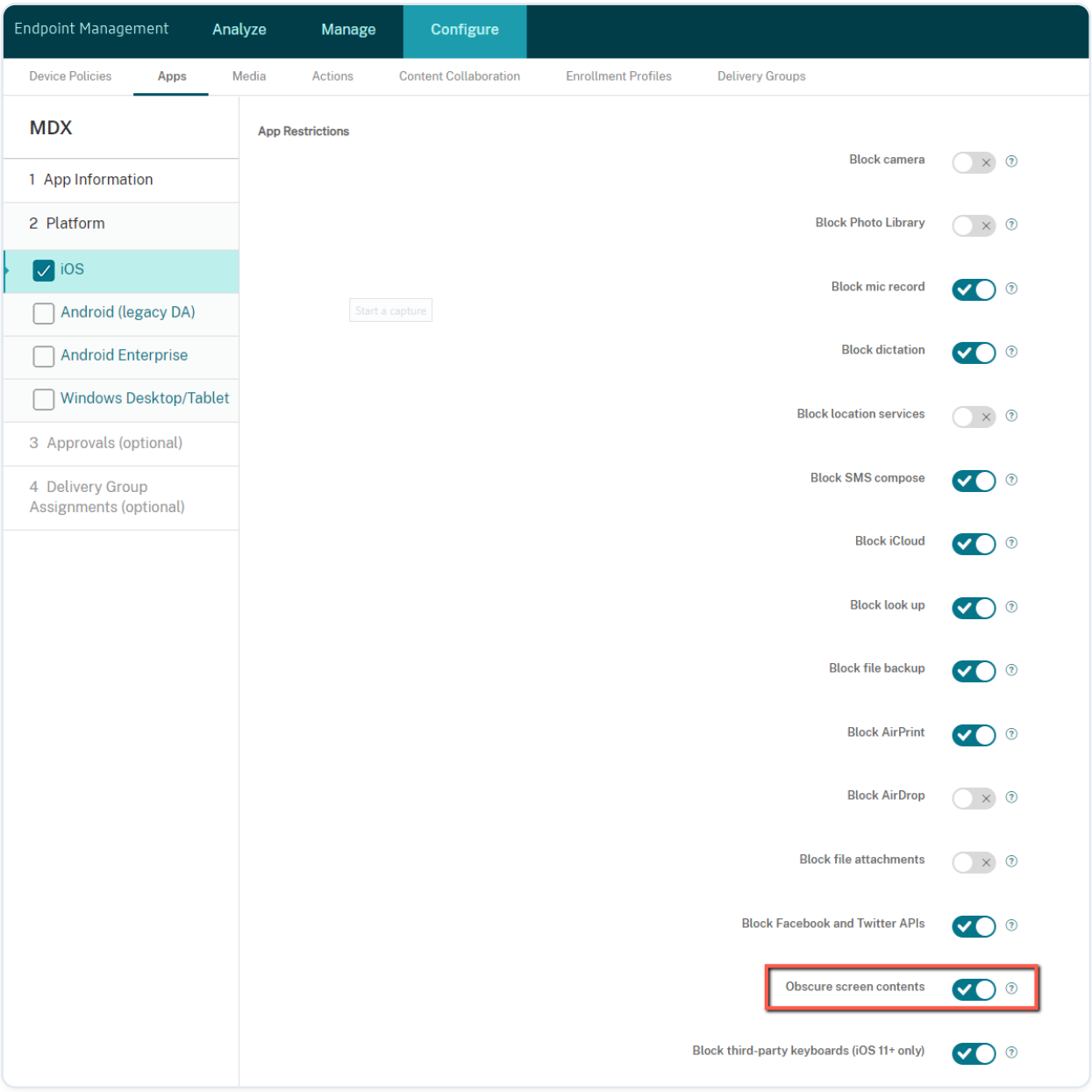
模糊屏幕内容

适用于 Android 和 iOS 的 Secure Mail 支持在应用程序进入后台时模糊屏幕。此功能可增强用户隐私、保护敏感数据并防止未经授权的访问。要在 iOS 或 Android 设备上为 Secure Mail 启用此功能，请参阅以下部分。

在 iOS 设备上：

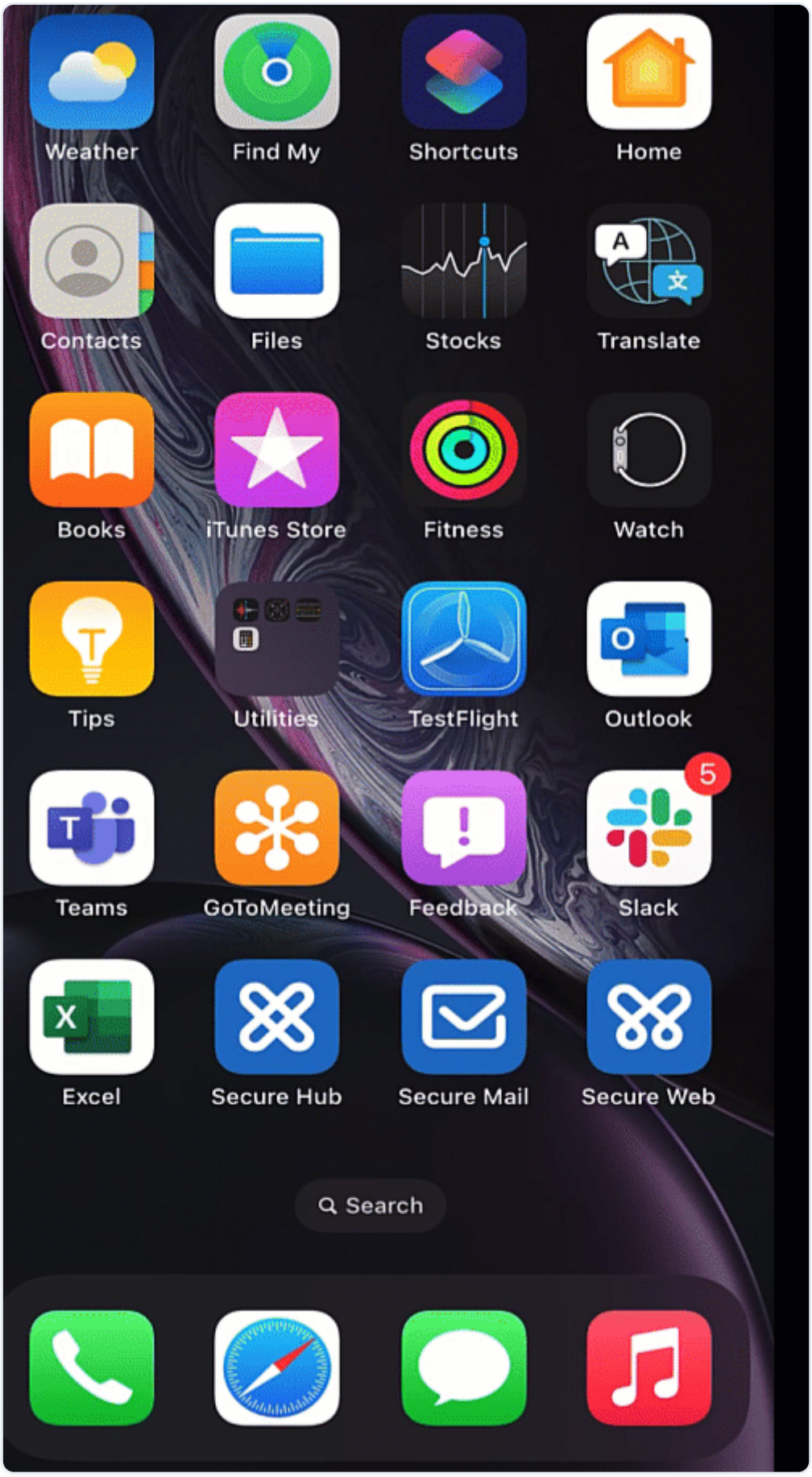
1. 使用管理员凭据登录 Citrix Endpoint Management 控制台。
2. 导航到 **Configure** > **Apps** > **MDX**。
3. 在 **Platform** 部分下选择 **iOS** 选项。
4. 在 **App Restrictions** 部分下启用 **Obscure screen contents** 选项。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



启用 **Obscure screen contents** 选项后，当应用程序进入后台时，Secure Mail 会显示灰色屏幕。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



在 Android 设备上：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要模糊 Secure Mail 应用程序内容，您可以使用我们用于限制屏幕捕获的策略，即 **Allow screen capture** 策略。禁用此策略也会在应用程序进入后台时模糊应用程序内容。有关禁用 **Allow screen capture** 策略的更多信息，请参阅 Citrix Endpoint Management 文档中的 Android 设置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOS 功能

本文讨论 Secure Mail 支持的 iOS 功能。

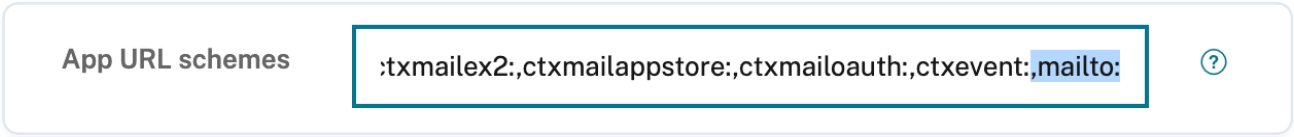
支持将 Secure Mail 设置为默认邮件应用程序

在适用于 iOS 的 Secure Mail 中，您可以将 Secure Mail 设置为设备上的默认邮件应用程序。将其设置为默认应用程序后，在“通讯录”、Safari 或任何其他应用程序中轻按电子邮件地址将会在 Secure Mail 中打开新邮件。要启用此功能，请完成以下步骤：

- **管理员：** 允许 Secure Mail MDX 策略中的 `mailto:` 方案。
- **用户：** 在设备上选择 Secure Mail 作为默认邮件应用程序。

允许 mailto: 方案：

1. 在 Endpoint Management 控制台上，导航到 **Configure > Apps**（配置 > 应用程序）。
2. 选择 **Secure Mail**，然后单击 **Edit**（编辑）。
3. 在 iOS 平台下，展开 **App interaction**（应用程序交互），然后将 `,mailto:` 附加到 **App URL schemes**（应用程序 URL 方案）。



将 Secure Mail 设置为默认邮件应用程序：

1. 在设备上，打开 iOS **Settings**（设置）应用程序。
2. 轻按 **Apps > Default Apps > Mail**（应用程序 > 默认应用程序 > 邮件）。
3. 选择 **Secure Mail**。

在 Secure Mail 日历事件中创建 Microsoft Teams 会议

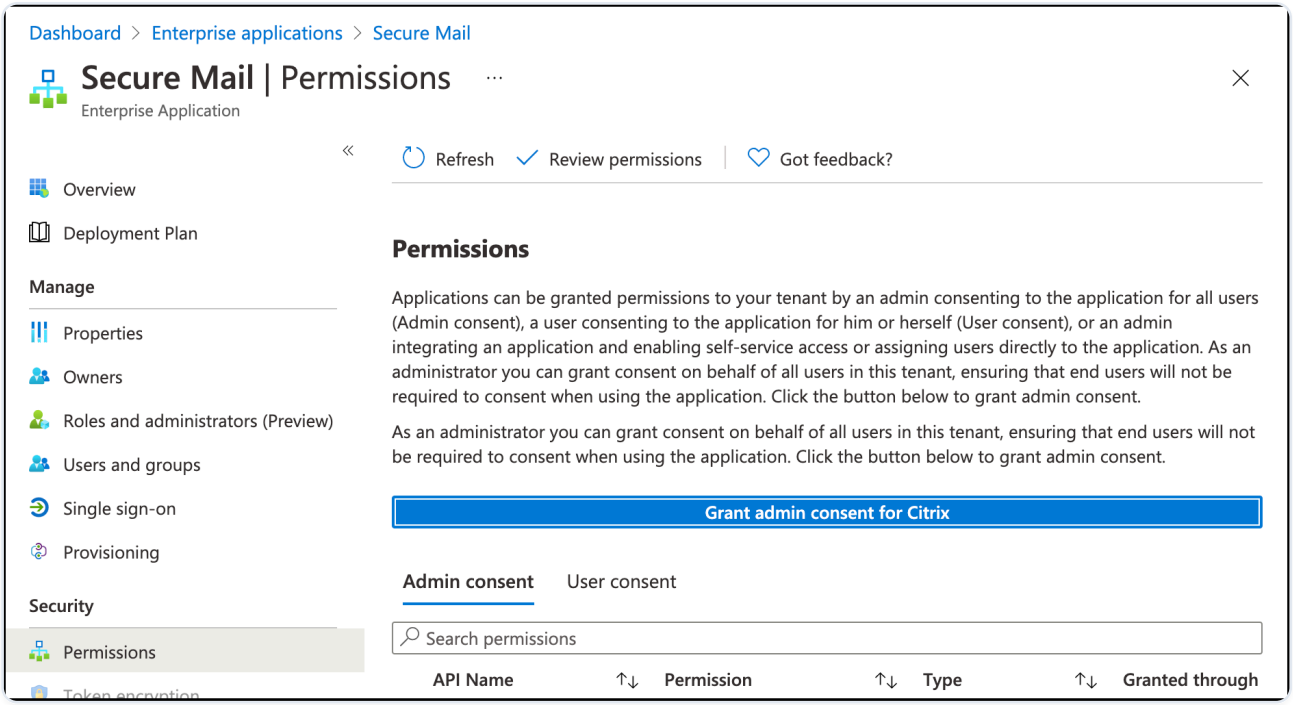
在适用于 iOS 的 Secure Mail 中，您可以在创建日历事件时创建 Microsoft Teams 会议邀请。要创建 Microsoft Teams 会议，请打开**Microsoft Teams 会议**切换开关。会议邀请链接和详细信息将随事件详细信息自动发送。有关详细信息，请参阅在 Secure Mail 日历事件中创建 Microsoft Teams 会议

先决条件：

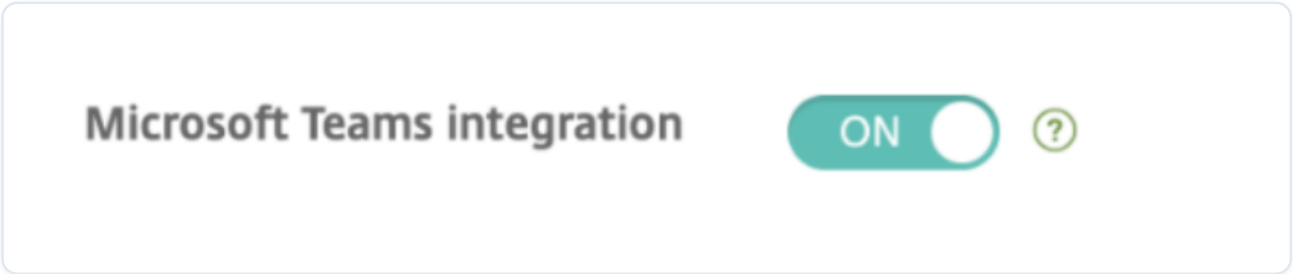
© 1997–2026 Citrix Systems, Inc. All rights reserved.

确保 Azure Active Directory 的全局管理员执行以下操作：

- 启用新式身份验证 (OAuth)，并确保您是拥有有效 Microsoft Teams 许可证的 Exchange Online 邮箱用户。
- 向 Secure Mail 应用程序提供租户范围的管理员同意。
- 在 Secure Mail 应用程序上配置您的 Exchange 帐户，并允许所有用户登录的应用程序权限。请参阅以下屏幕：



- 启用 Microsoft Teams 集成策略。



限制：

对于在 Secure Mail 上创建的会议，目前该功能在 Microsoft Outlook 日历上存在以下限制：

- **在线加入**选项不可用
- **会议已开始**通知不可用

© 1997–2026 Citrix Systems, Inc. All rights reserved.

最小化草稿

在 Secure Mail for iOS 中，您可以在撰写电子邮件时最小化草稿并在应用程序内导航。此功能适用于运行 iOS 13 及更高版本的设备。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章 最小化草稿电子邮件。

使用 MIME 标头报告网络钓鱼电子邮件

在 Secure Mail for iOS 中，当用户报告网络钓鱼邮件时，会生成一个 EML 文件作为该邮件的附件。管理员会收到此邮件，并可以查看与所报告邮件关联的 MIME 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，并在 Citrix Endpoint Management 控制台中将“报告网络钓鱼机制”设置为“通过附件报告”。有关详细信息，请参阅 将网络钓鱼电子邮件报告为附件。

支持 WkWebView

Secure Mail for iOS 支持 WkWebView。此功能改进了 Secure Mail 电子邮件和日历事件在设备上的呈现方式。

支持 Slack EMM

Slack EMM 适用于已启用企业移动管理 (EMM) 的 Slack 客户。Secure Mail for iOS 支持应用程序 **Slack EMM**，它允许管理员选择 Secure Mail 与 **Slack** 应用程序或 **Slack EMM** 应用程序的集成方式。

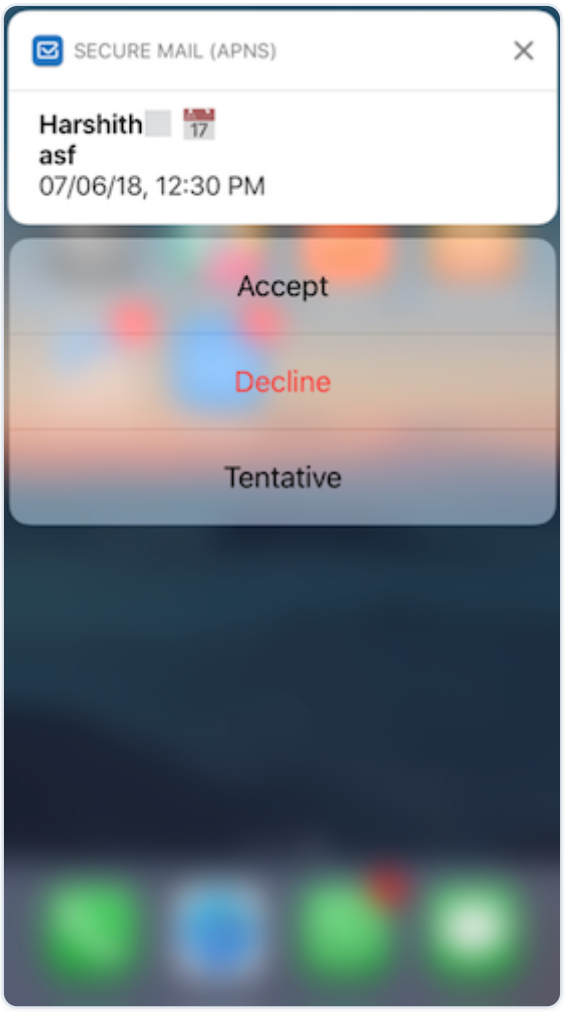
分组通知

借助分组通知功能，电子邮件线程中的对话会进行分组。您可以在设备的锁定屏幕上快速浏览分组通知。分组通知设置在设备上默认启用。此功能需要 iOS 12。

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”。他们可以使用“回复”和“删除”来响应消息通知。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



富推送通知失败消息的增强功能

在 Secure Mail for iOS 中，设备通知中心会根据通知失败的类型显示相应的推送通知失败消息。有关详细信息，请参阅 Secure Mail 通知。

支持 Microsoft 设置上的富推送通知

适用于 iOS 的 Secure Mail 支持在运行 Microsoft Enterprise Mobility + Security (EMS)/Intune 并使用现代身份验证 (O365) 的设置上实现富推送通知。要启用富推送通知功能，请确保满足以下先决条件：

- 在 Endpoint Management 控制台中，将**推送通知**设置为“开”。
- **网络访问策略**设置为**无限制**。
- **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**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

支持 S/MIME 派生凭据

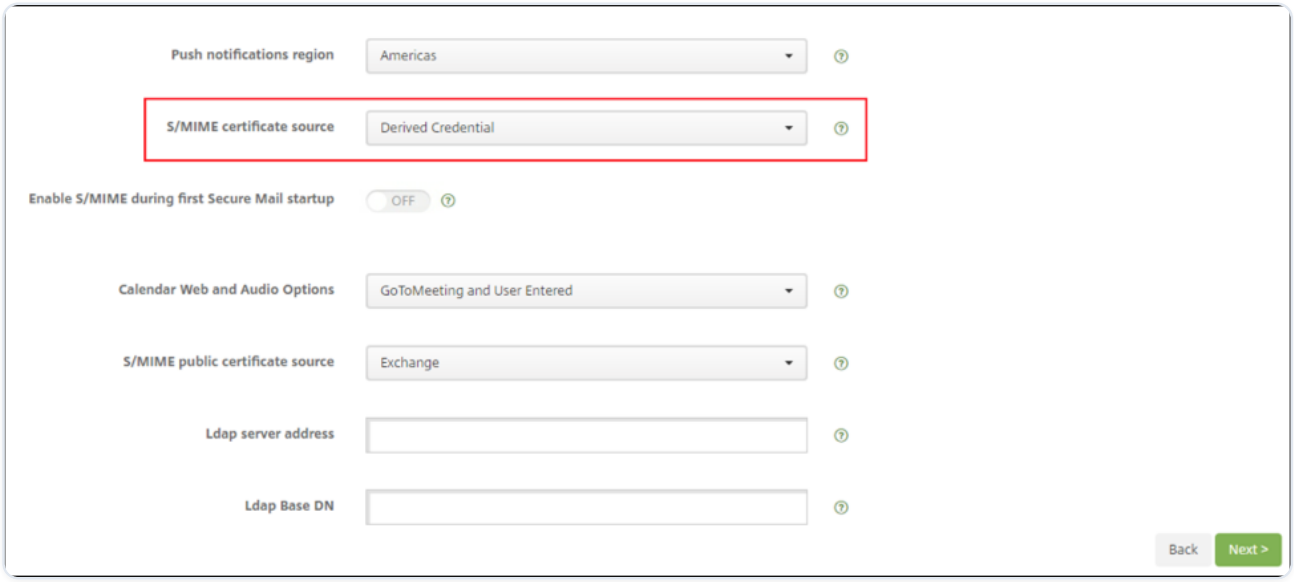
适用于 iOS 的 Secure Mail 支持 S/MIME 派生凭据。要使此功能正常工作，您需要执行以下操作：

- 选择“派生凭据”作为 S/MIME 证书源。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：
  - **密钥：** 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。

有关设备在使用派生凭据时如何注册的更多信息，请参阅使用派生凭据注册设备。

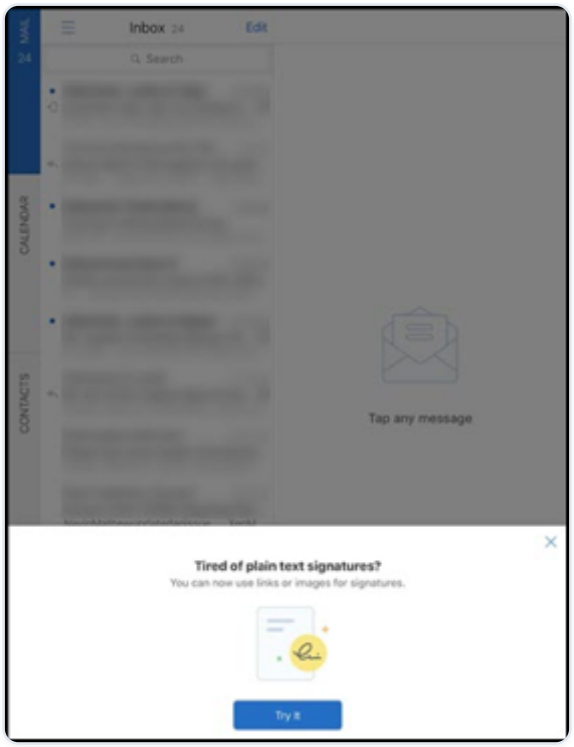
1. 在 Endpoint Management 控制台中，导航到**配置 > 应用程序**。
2. 选择 **Secure Mail**，然后单击**编辑**。
3. 在 iOS 平台上，对于 S/MIME 证书源，选择 **Derived Credential**。



富文本签名

您可以在电子邮件签名中使用图像或链接。要更新签名，只需将图像或链接复制并粘贴到签名字段中即可。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



添加富文本签名

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，您可以长按签名字段，然后点击**插入图片**以从图库中选择图像。

Secure Mail 来电显示

在 Secure Mail for iOS 中，您可以通过在设备设置中启用 Secure Mail 来电显示来识别来自 Secure Mail 联系人的来电。您必须启用以下管理先决条件：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：为同步的 Secure Mail 日历设置颜色。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

从“文件”应用附加文件

在适用于 iOS 的 Secure Mail 中，您可以从 iOS 原生**文件**应用附加文件。有关 iOS 文件应用的更多信息，请参阅 Apple 文章文件 App。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 拼写检查与设备在**通用 > 键盘**下的“自动大写”和“检查拼写”设置通过以下方式交互：

设备上的自动更正	设备上的检查拼写	SECURE MAIL 中的检查拼写	行为
开	开	开	显示红色下划线。点击时，单词会以粉色突出显示并显示建议。
关	关	开	显示红线。点击时，不显示建议。
开	开	关	不显示红色下划线。点击时，单词会以粉色突出显示并出现建议
关	关	关	不显示红色下划线、突出显示或建议。
开	关	开	显示红色下划线。点击时，单词会以粉色突出显示并出现建议。
关	开	开	显示红色下划线。点击时，单词会以粉色突出显示并出现建议。
开	关	关	不显示红色下划线。点击时，单词会以粉色突出显示并出现建议。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

设备上的自动更正	设备上的检查拼写	SECURE MAIL 中的检查拼写	行为
关	开	关	不显示红色下划线。点击时，单词会以粉色突出显示并出现建议。

邮箱屏幕

邮箱屏幕显示您已配置的所有帐户，并具有以下视图：

- **所有帐户：**包含您已配置的所有 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，您可以展开以查看子文件夹。

所有帐户邮箱是默认的全局视图。此视图包含您在设备上配置的所有 Exchange 帐户的附件和电子邮件。

“**所有账户**”邮箱包含以下菜单项：

- 所有附件
- 收件箱
  - 未读
  - 已标记
- 草稿
- 已发送邮件
- 发件箱
- 已删除邮件

尽管“**所有账户**”视图会集中显示来自多个账户的电子邮件，但以下操作会使用默认或主账户的电子邮件地址：

- 新邮件
- 新建事件

若要在“**所有账户**”视图中撰写新邮件时更改发件人的电子邮件地址，请点击“**发件人：**”字段中的默认地址，然后从显示的邮件账户中选择其他账户。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

从对话视图撰写电子邮件时，“**发件人：**”字段会自动填充该对话所针对的电子邮件地址。

个人账户

您配置的所有账户都将显示在 **所有账户** 下方列表中。默认账户或主账户始终排在首位，其他账户按字母顺序排列。

个人账户会显示您可能已创建的任何子文件夹。您可以通过点击文件夹旁边的 **V** 图标来查看子文件夹。

以下操作仅限于个人账户：

- 移动项目。
- 从会话视图撰写电子邮件。
- 导入 vCard。
- 保存联系人。

日历

日历会显示您设备上与多个账户相关的所有事件。您可以为各个账户设置颜色，以区分与不同账户相关的日历事件。

设置日历事件的颜色

1. 点击页脚栏中的 **日历** 图标，然后点击左上角的汉堡包图标。 **日历** 屏幕会显示您配置的所有账户。
2. 点击 Exchange 账户右侧显示的默认颜色。 “颜色”屏幕会显示该账户可用的颜色。
3. 选择您喜欢的颜色，然后点击 **保存**。
4. 要返回上一屏幕，请点击 **取消**。 所选颜色将应用于与该 Exchange 账户相关的所有日历事件。

当您创建日历邀请或事件时，**组织者**字段会自动填充默认帐户的电子邮件地址。要更改邮件帐户，请点击此电子邮件地址并选择另一个帐户。

注意：

当您退出并重新启动 Secure Mail 时，应用程序会恢复设备上上次配置的日历设置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

搜索

您可以从**邮箱**或**联系人**视图执行全局搜索。此操作会在搜索应用程序中的所有帐户后显示相应结果。 从单个帐户内执行的所有搜索仅显示与该帐户相关的结果。

在 iOS 上打印电子邮件、日历事件或内联图像

您现在可以从 iOS 设备打印电子邮件、日历事件或内联图像。

先决条件

在开始之前，请确保满足以下要求：

- **阻止 AirPrint** 选项设置为**关闭**。
- IRM 中已禁用**允许查看者打印**选项。

默认情况下，Secure Mail for iOS 中已启用打印功能。打印功能可能由您的管理员通过 Apple AirPrint 或 Microsoft 信息权限管理 (IRM) 的管理策略进行控制。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，并且可能会出现错误消息。

打印电子邮件

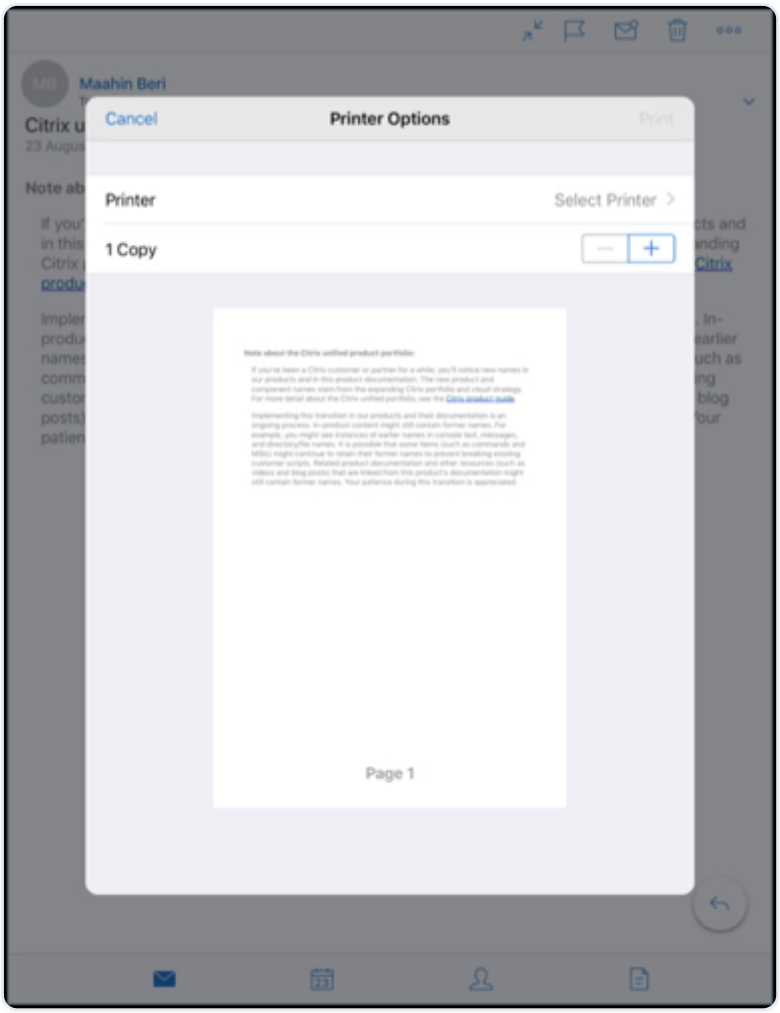
1. 打开要打印的电子邮件项目。
2. 点击屏幕左上角的“更多”图标。将显示以下选项：
    - 移动
    - 打印

© 1997–2026 Citrix Systems, Inc. All rights reserved.



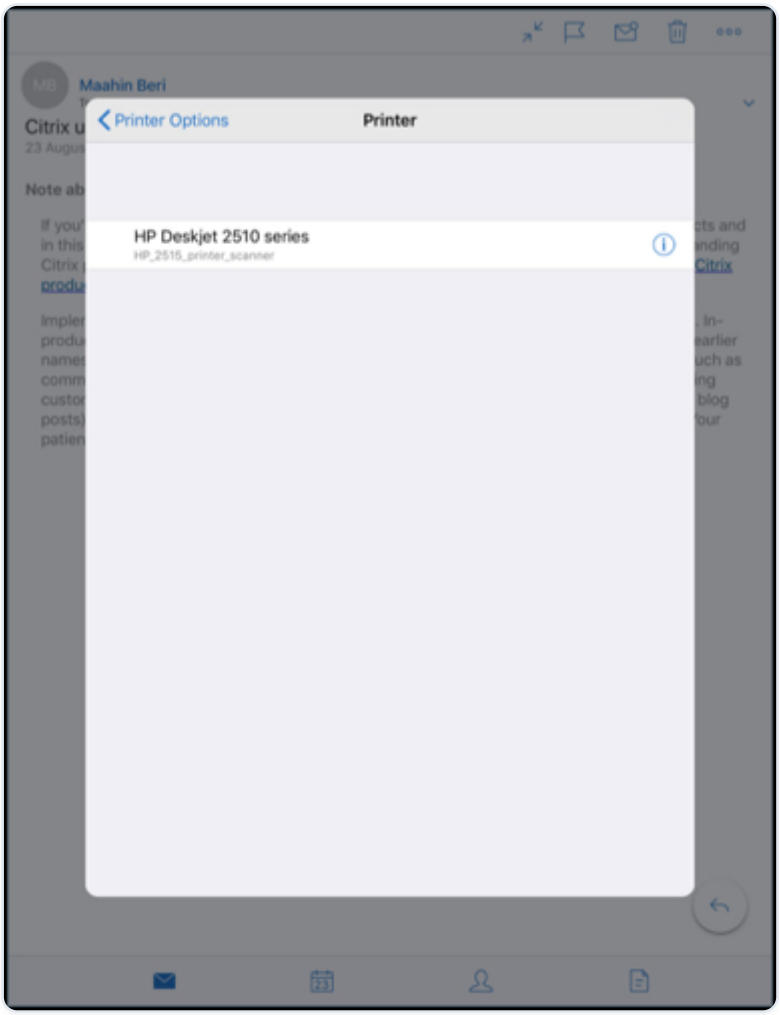
3. 轻按**打印**。 此时将显示**打印机选项**屏幕。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



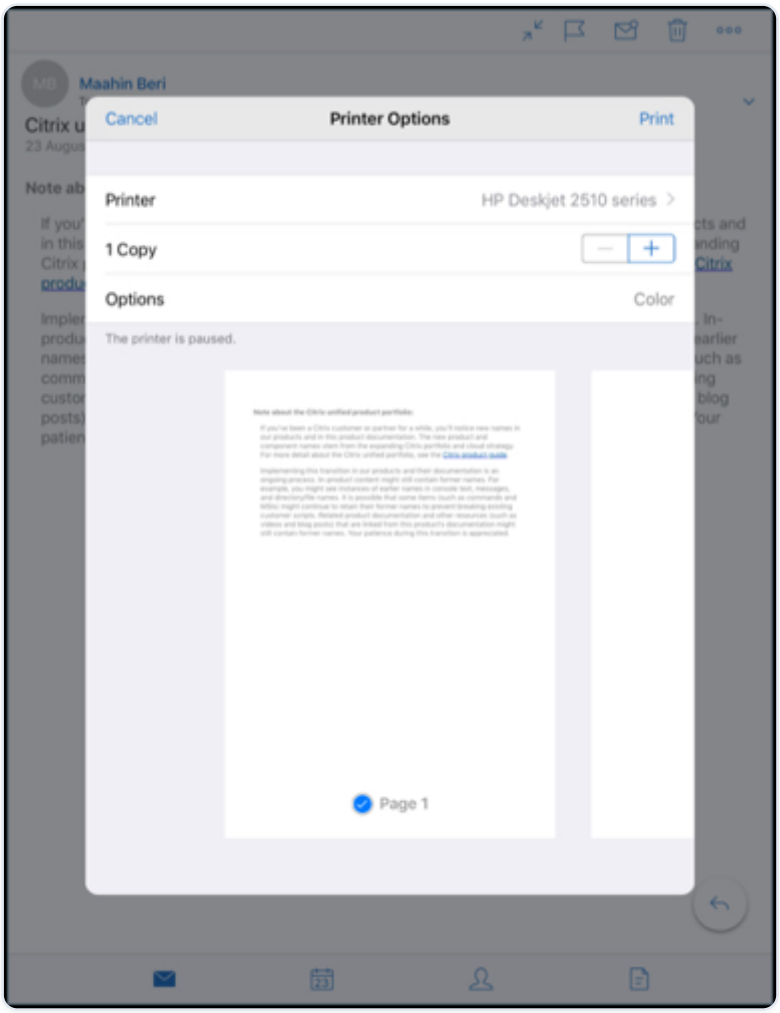
4. 要选择打印机，请轻按**选择打印机**。 此时将显示**打印机**屏幕。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 选择要打印到的打印机。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. 轻按**–**或**+**可减少或增加要打印的份数。
7. 要打印特定页面或页面范围，请轻按**范围**。 此时将显示**页面范围**屏幕。默认情况下，会选择**所有页面**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



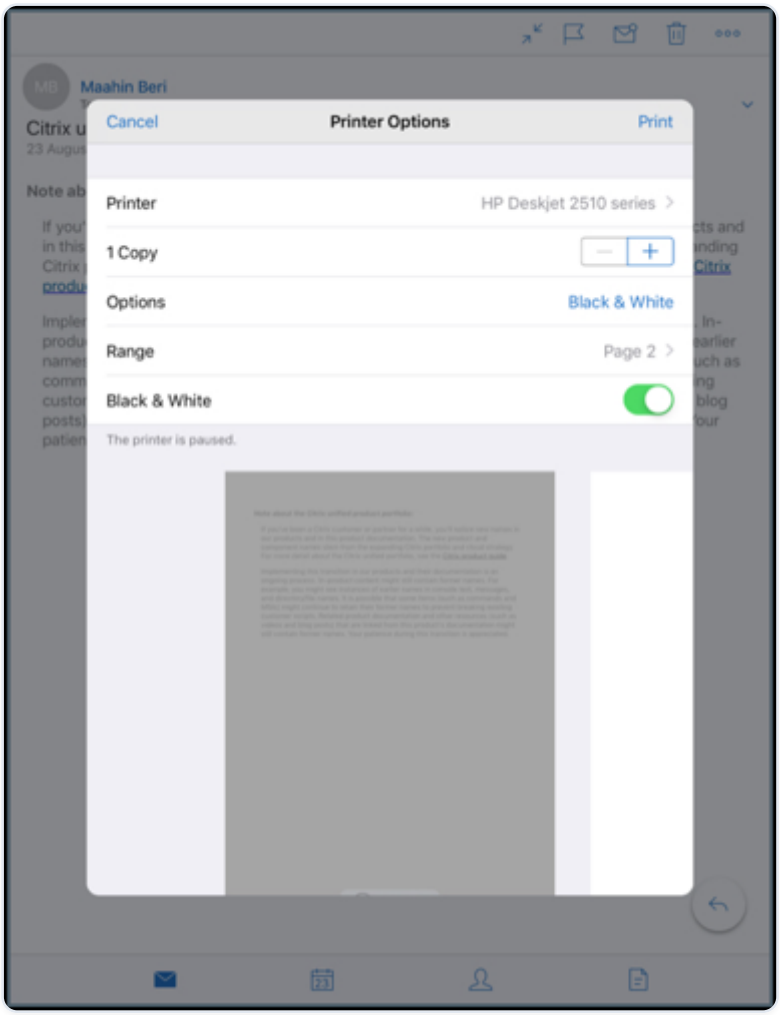
8. 要更改页面选择，请向上或向下轻扫页码。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



9. 轻按**打印机选项**可返回**打印机选项**屏幕。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

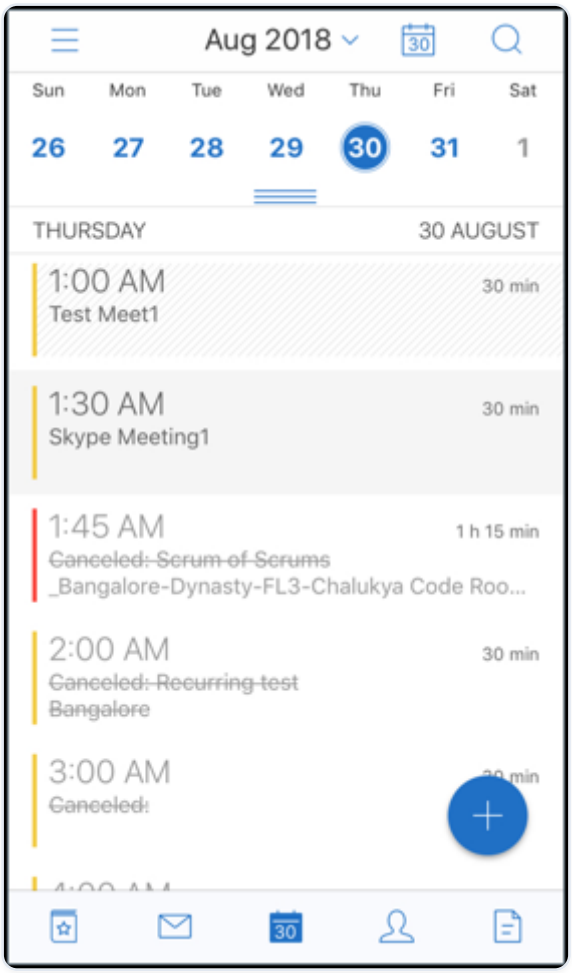


10. 要以黑白打印，请点击**黑白**按钮。默认情况下，Secure Mail 以彩色打印。
11. 点击右上角的**打印**以打印电子邮件。
12. 要取消打印作业，请点击左上角的**取消**。

打印日历事件

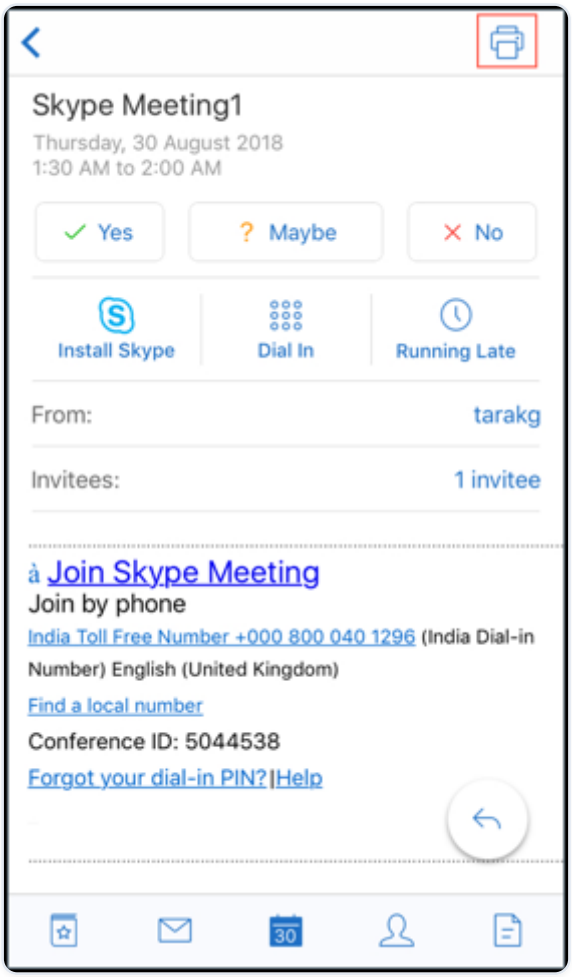
1. 导航到日历并选择一个事件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 点击打印图标，并按照上一节**打印电子邮件**中提到的相同说明进行操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



打印内联图像：

1. 打开包含内联图像的电子邮件项目。
2. 点击更多图标。将显示以下选项：

    - 移动
    - 打印
    - 取消

    电子邮件选项的图像(/en-us/mobile-productivity-apps/media/SM-iOS-Print14.png)
3. 点击**打印**并按照后续部分**打印电子邮件**中提及的说明进行操作。

多个会议代码（拨入会议）

适用于 iOS 的 Secure Mail 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

拨入会议

1. 打开会议邀请并点击**拨入**。
2. 从出现的电话号码列表中，选择一个进行拨入。
3. 从出现的会议代码列表中，选择一个以加入会议。
4. 点击**呼叫**以加入会议。

支持打印电子邮件附件

适用于 iOS 的 Secure Mail 支持打印电子邮件附件。

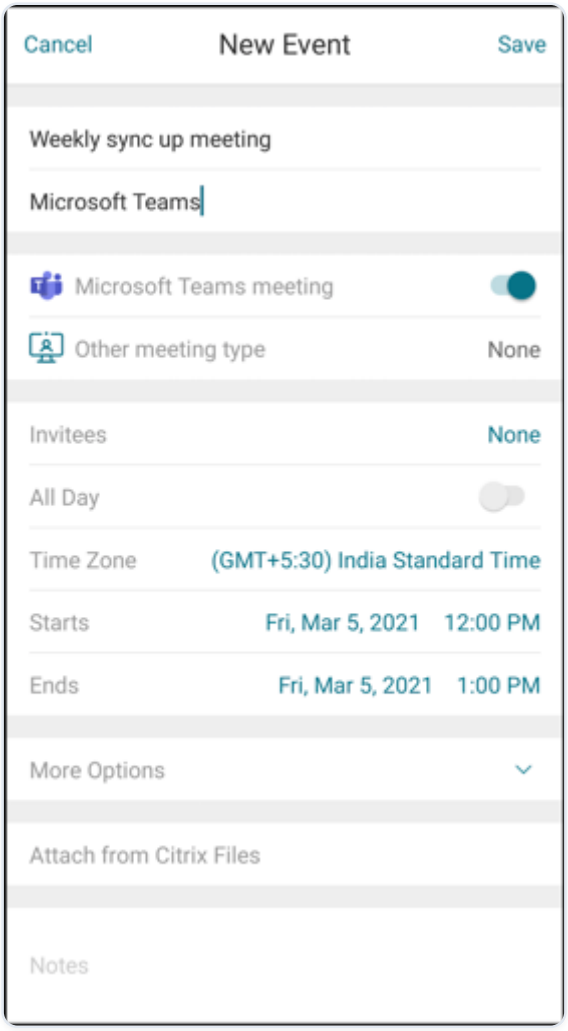
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Android 功能

本文讨论 Secure Mail 中支持的 Android 功能。

在 Secure Mail 日历事件中创建 Microsoft Teams 会议

在适用于 Android 的 Secure Mail 中，您可以在创建日历事件时创建 Microsoft Teams 会议邀请。要创建 Microsoft Teams 会议，请打开 **Microsoft Teams 会议** 切换开关。会议邀请链接和详细信息将随事件详细信息自动发送。

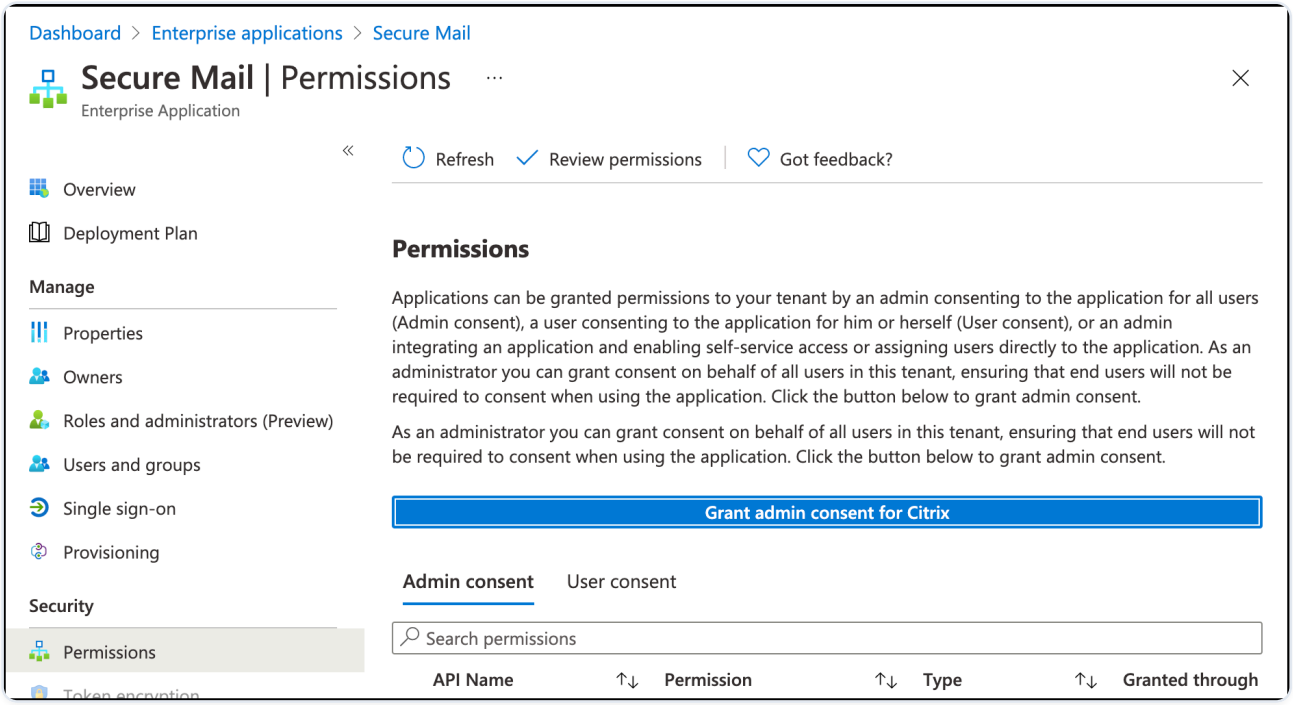


先决条件：

确保 Azure Active Directory 的全局管理员执行以下操作：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 启用新式身份验证 (OAuth)，并确保您是拥有有效 Microsoft Teams 许可证的 Exchange Online 邮箱用户。
- 向 Secure Mail 应用程序提供租户范围的管理员同意。
- 在 Secure Mail 应用程序上配置您的 Exchange 帐户，并允许所有用户登录的应用程序权限。请参阅以下屏幕：



- 启用 Microsoft Teams 集成策略。



限制：

对于在 Secure Mail 上创建的会议，目前该功能在 Microsoft Outlook 日历上存在以下限制：

- “**在线加入**”选项不可用
- “**会议已开始**”通知不可用

双向联系人同步

在适用于 Android 的 Secure Mail 中，您可以从本地联系人列表中创建、编辑和删除 Secure Mail 联系人。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

撤消已发送邮件

在适用于 Android 的 Secure Mail 中，您可以撤消已发送邮件。点击**发送**按钮后，您会收到一条浮动消息，允许您撤消发送操作。点击**撤消**可恢复发送操作并编辑邮件、邮件收件人、附加或删除附件，或丢弃邮件

草稿文件夹中的附件同步

在适用于 Android 的 Secure Mail 中，当**草稿**文件夹同步时，附件也会同步，并且可在您的所有设备上使用。此功能适用于运行 Exchange ActiveSync 版本 16 或更高版本的设备。

PDF 文件的应用内查看

在适用于 Android 的 Secure Mail 中，您可以在应用内查看 PDF 文件，以及书签和注释。此外，还提供其他 Microsoft Office 附件的增强视图。

将 Web SSO 用于隧道策略，适用于使用 Microsoft Office 365 运行现代身份验证的设置

在适用于 Android 的 Secure Mail 中，添加了一项名为**将 Web SSO 用于隧道**的新策略。通过此策略，您可以将 OAuth 流量通过隧道传输到 Tunneled – Web SSO。为此，请执行以下操作:

- 将**将 Web SSO 用于隧道**策略设置为**开**。
- 在网络访问策略中选择**隧道 - Web SSO**选项。
- 从**后台服务**策略中排除任何与 OAuth 相关的主机名。

拖放日历事件

在适用于 Android 的 Secure Mail 中，您可以通过拖放现有日历事件来更改其时间。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章：更改日历事件时间。

支持 Google Play 的 64 位应用程序

适用于 Android 的 Secure Mail 支持 64 位体系结构。

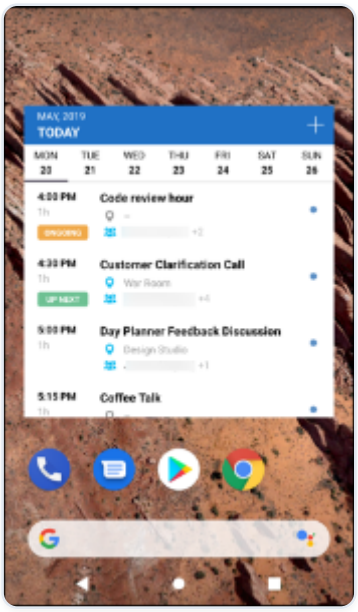
改进了适用于 Android 的 Secure Mail 中的“下拉刷新”UI

根据 Material Design 准则，我们对**下拉刷新**功能进行了一些小改进。点击汉堡图标时，同步时间戳会显示在屏幕底部。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

日历议程小组件

在适用于 Android 的 Secure Mail 中，**日历**议程可用作小组件。通过此小组件，您可以查看一周内**日历**中的即将发生的事件。此功能允许您创建**日历**事件、查看现有事件和编辑详细信息。**阻止屏幕捕获**策略不适用于放置在主屏幕上的小组件。但是，您可以使用**允许日历议程小组件**策略禁用该小组件。



网络访问策略

在适用于 Android 的 Secure Mail 中，网络访问 MDX 策略中添加了一个名为**隧道 - Web SSO** 的新选项。配置此策略使您能够灵活地通过隧道 - Web SSO 和安全票证颁发机构 (STA) 并行地隧道化内部流量。您还可以允许隧道 - Web SSO 连接用于身份验证服务，例如 NTLM、Okta 和 Kerberos。首次配置 STA 时，必须将服务地址的各个 FQDN 和端口添加到后台网络服务策略。但是，如果配置**隧道 - Web SSO** 选项，则无需进行这些配置。

要在 Citrix Endpoint Management™ 控制台中为适用于 Android 的 Secure Mail 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，请参阅添加 MDX 应用程序中的步骤。
2. 在网络访问策略中，单击**隧道 - Web SSO** 选项。有关详细信息，请参阅应用程序网络访问

Feed 卡增强功能

Secure Mail for Android 中现有的 **Feeds** 文件夹已进行以下增强：

- 所有自动同步文件夹中的会议邀请都会显示在您的 Feeds 卡片中。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 在您的 Feeds 卡片中查看最多五场即将召开的会议。
- 即将召开的会议现在根据从当前时间开始的 24 小时周期显示。这些会议邀请分为“**今天**”和“**明天**”。在以前的版本中，直到当天结束的即将召开的会议会显示在您的 Feeds 中。

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，您可以从 Android 设备打印电子邮件和日历事件。此打印功能使用 Android 打印框架。

先决条件

- 确保管理员已在 Citrix Endpoint Management 控制台中将“**阻止打印策略**”设置为“**关闭**”。有关 Android 的此策略信息，请参阅 阻止打印策略。
- 如果电子邮件受 IRM 保护，请确保在电子邮件中启用“**允许查看者打印**”选项。

如果这些策略设置不当，您将无法打印电子邮件或日历事件。

注意：

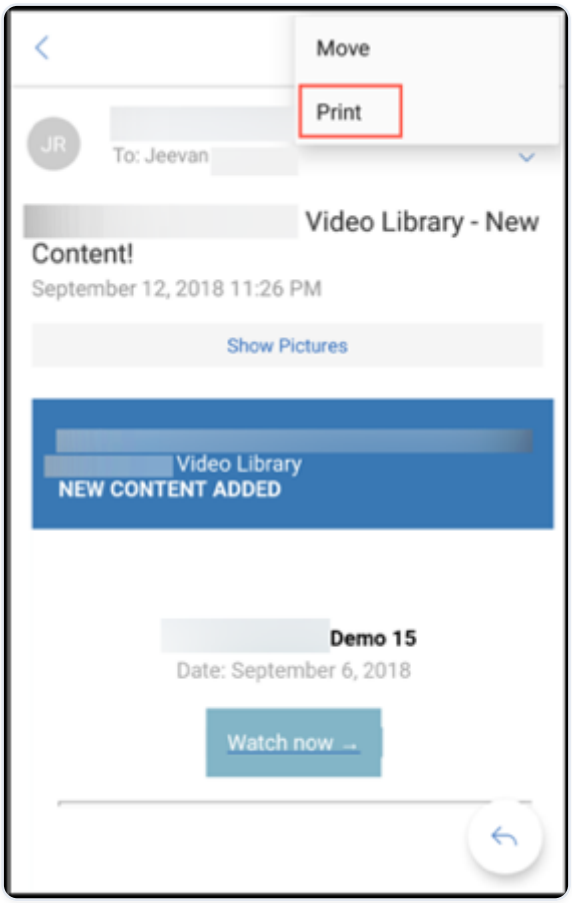
此打印功能存在以下已知限制：

- 只有在您点击“**显示图片**”下载图片后，内联图片才会打印。如果您不点击“**显示图片**”，则只会打印图片占位符。
- 在 Secure Mail 中，大尺寸电子邮件会被截断。打印前，点击**下载完整邮件**以打印完整邮件。如果完整邮件未下载，则会打印截断的邮件。
- 打印这些项目时，不会添加来自电子邮件或事件的任何元数据。

打印电子邮件

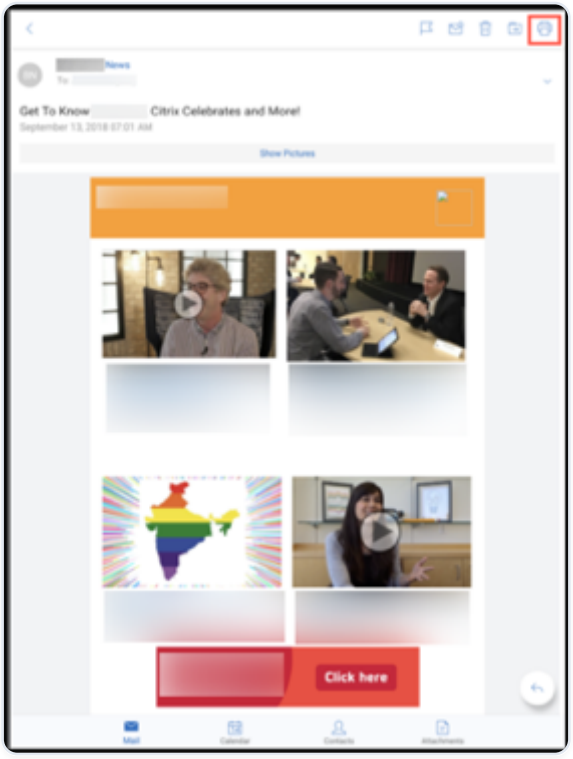
1. 打开要打印的电子邮件。
2. 点击屏幕左上方的“更多”图标。将显示以下选项：
    - 移动
    - 打印

© 1997–2026 Citrix Systems, Inc. All rights reserved.



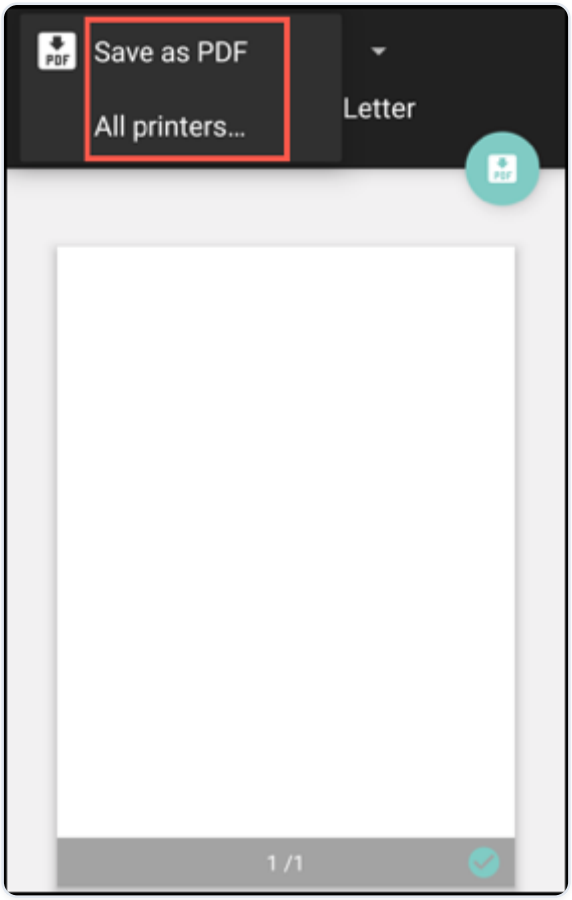
注意：

在平板电脑上，您可以直接使用屏幕左上方的打印图标来打印电子邮件。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

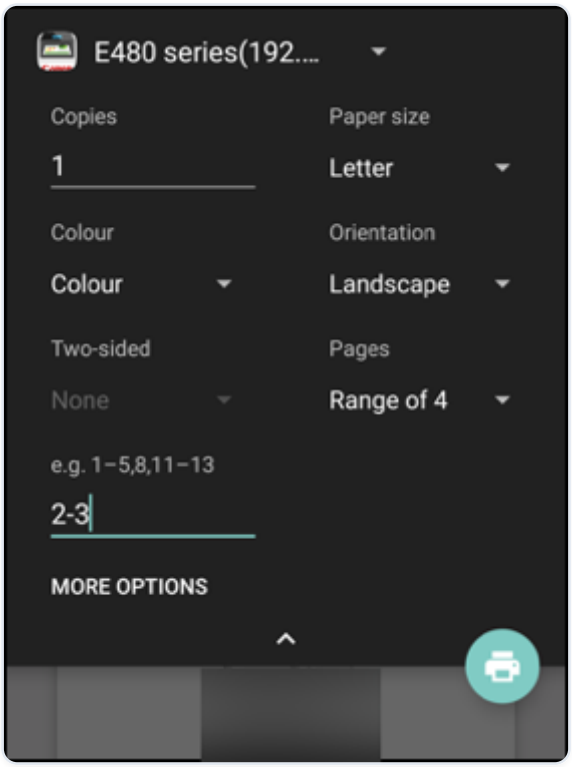
1. 点击**打印**。将显示电子邮件预览。
2. 点击列表，将显示以下选项：
   - 保存为 PDF
   - 所有打印机



3. 点击 **另存为 PDF** 将您的电子邮件保存为 PDF 格式。
4. 点击 **所有打印机**。根据您的要求安装打印机。
5. 打印机安装完成后，点击 **选择打印机** 选择一台打印机。**打印机** 屏幕随即出现。

> **注意：**
>
> 打印选项因所选打印机而异。以下图像来自 Canon E480 打印机，仅用于表示目的。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. 选择要打印到的打印机。使用以下打印选项：
   - 手动输入要打印的份数。
   - 从列表中选择纸张尺寸。
   - 从列表中选择颜色。
   - 根据需要选择页面方向。
   - 选择一个页面或一个页面范围，并手动输入页面范围。
7. 设置好打印选项后，点击屏幕上的打印图标。

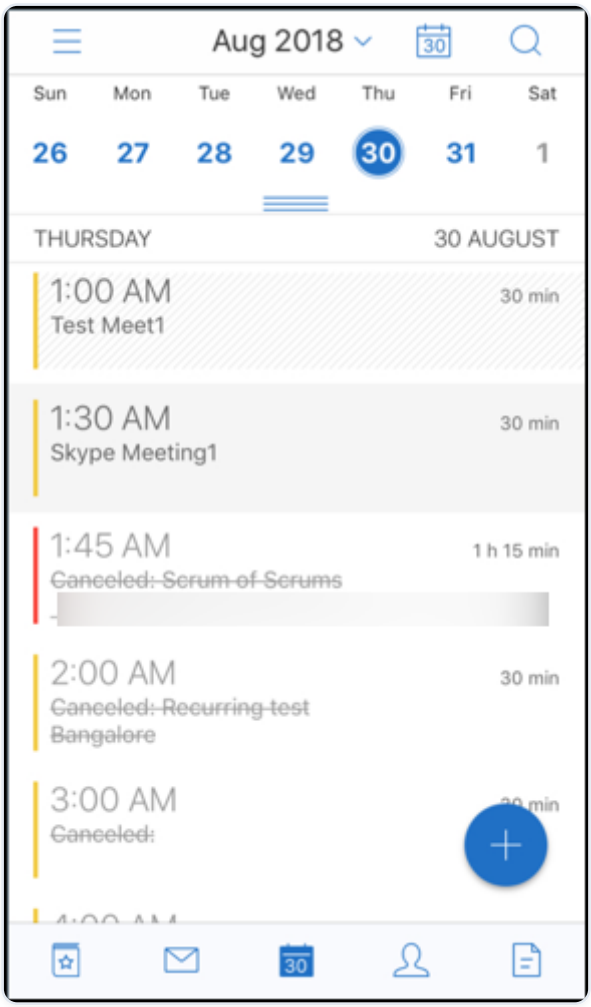
打印内联图像

- 在电子邮件中点击“**显示图片**”，并按照上一节 打印电子邮件 中所述的说明进行操作。

打印日历事件

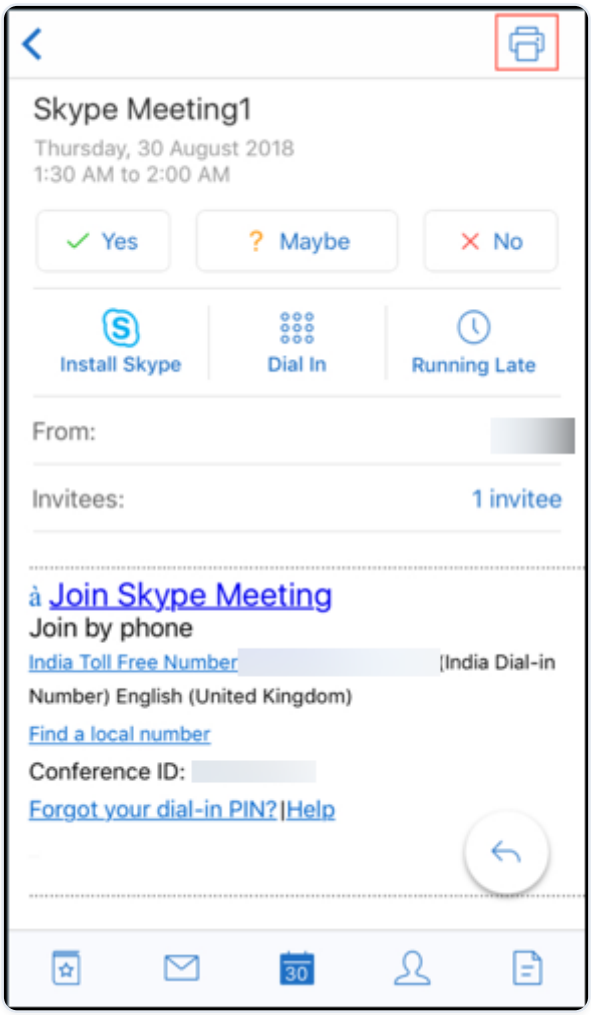
1. 导航到日历并点击一个事件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 点击打印图标，然后按照上一节 打印电子邮件 中所述的相同说明进行操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



报告带有 ActiveSync 标头的网络钓鱼电子邮件

在适用于 Android 的 Secure Mail 中，当用户报告网络钓鱼邮件时，会生成一个 EML 文件作为该邮件的附件。管理员会收到此邮件，并可以查看与所报告邮件关联的 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“**通过附件报告**”。有关为 Secure Mail 配置 MDX 策略的详细信息，请参阅 适用于移动生产力应用程序的 MDX 策略。

子文件夹通知

在适用于 Android 的 Secure Mail 中，您可以从邮件帐户的子文件夹接收邮件通知。

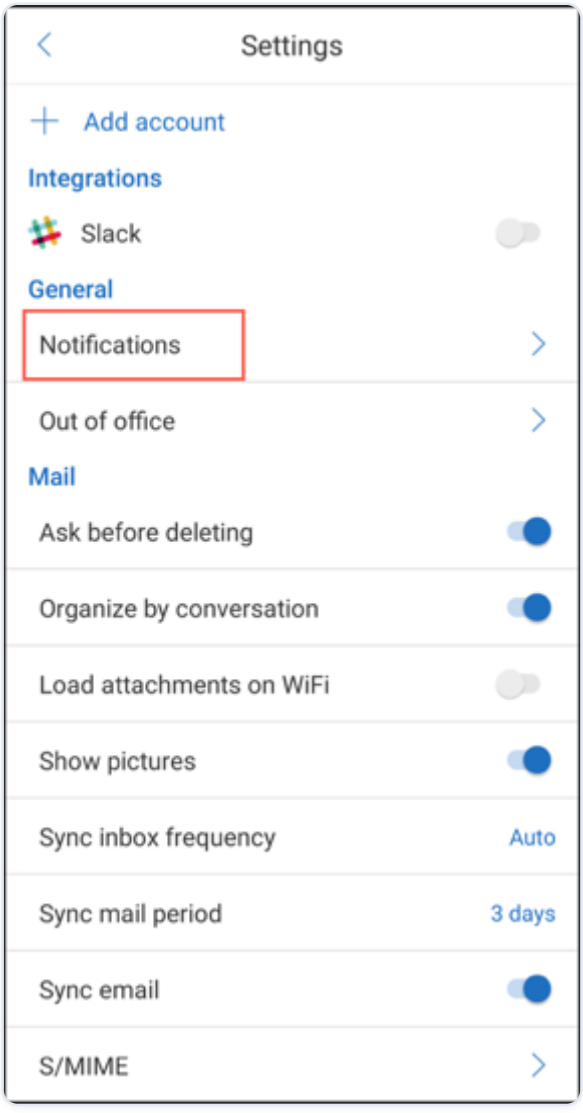
© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

- 确保在 Endpoint Management 控制台中启用了基于 FCM 的推送通知，以获取子文件夹的通知。有关配置基于 FCM 的推送通知的步骤，请参阅 Secure Mail 的推送通知。
- 子文件夹通知功能不适用于 Lotus Notes Server。

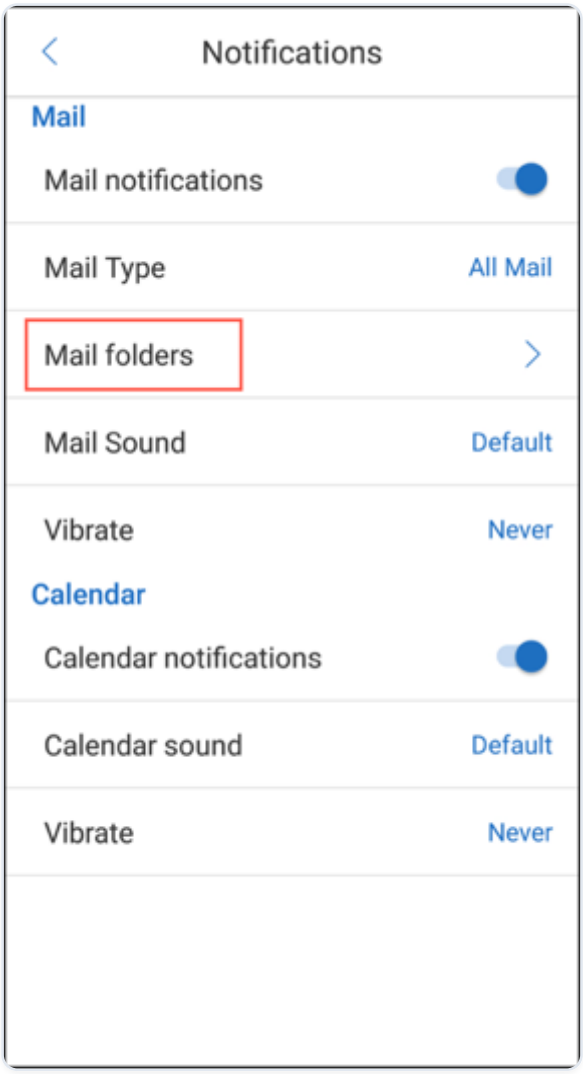
启用子文件夹通知

1. 前往**设置**，然后在**通用**下，点击**通知**。



2. 在**通知**屏幕中，点击**邮件文件夹**。收件箱中的子文件夹列表随即出现。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

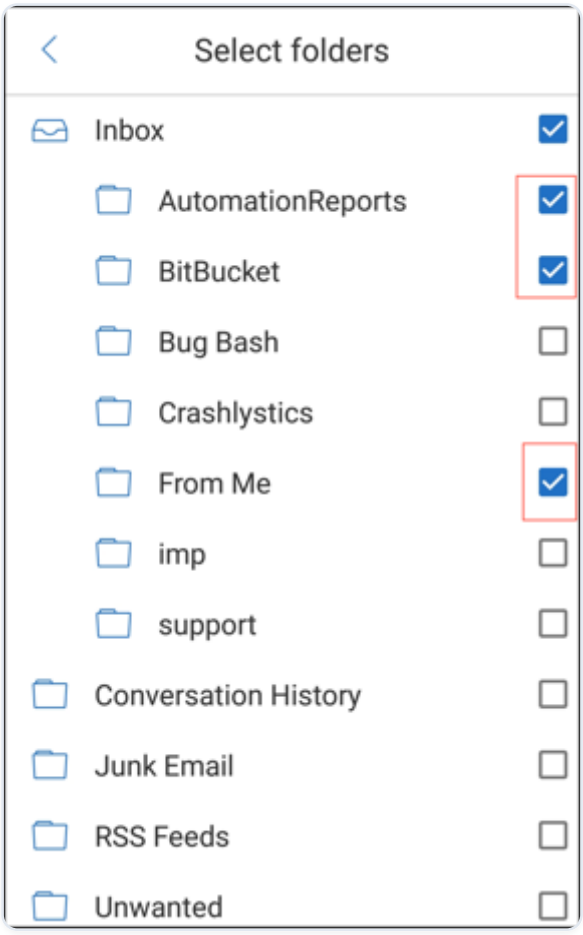


3. 点击以选择您要接收通知的子文件夹。收件箱默认处于选中状态。

注意：

为子文件夹启用通知会启用自动同步。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



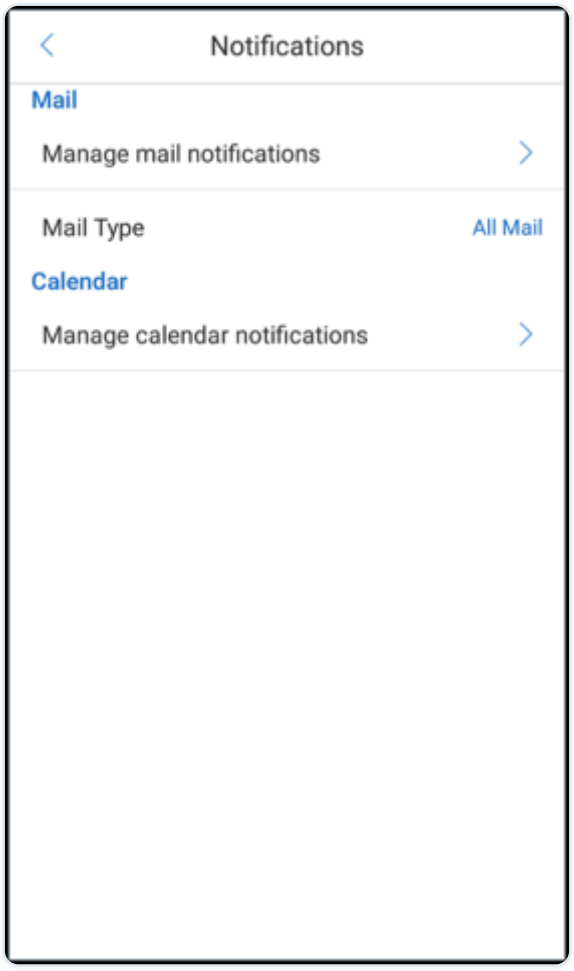
要禁用子文件夹通知，请清除您不想接收通知的子文件夹的复选框。

通知渠道

在运行 Android O 或更高版本的设备上，您可以使用通知渠道设置来管理电子邮件和日历通知的处理方式。此功能允许您自定义和管理通知。

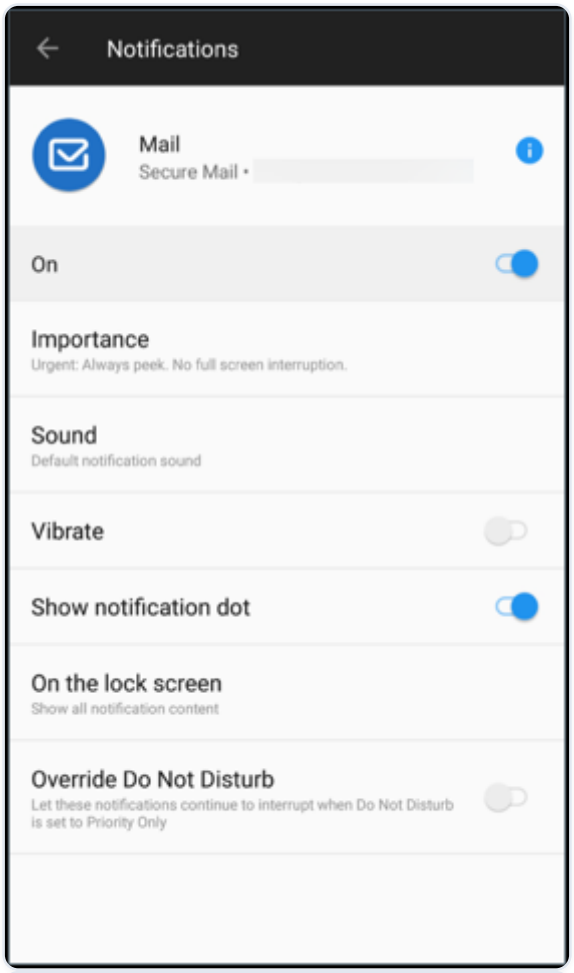
要配置邮件或日历提醒的通知，请打开 Secure Mail 并导航到**设置 > 通知**，然后选择所需的通知选项。

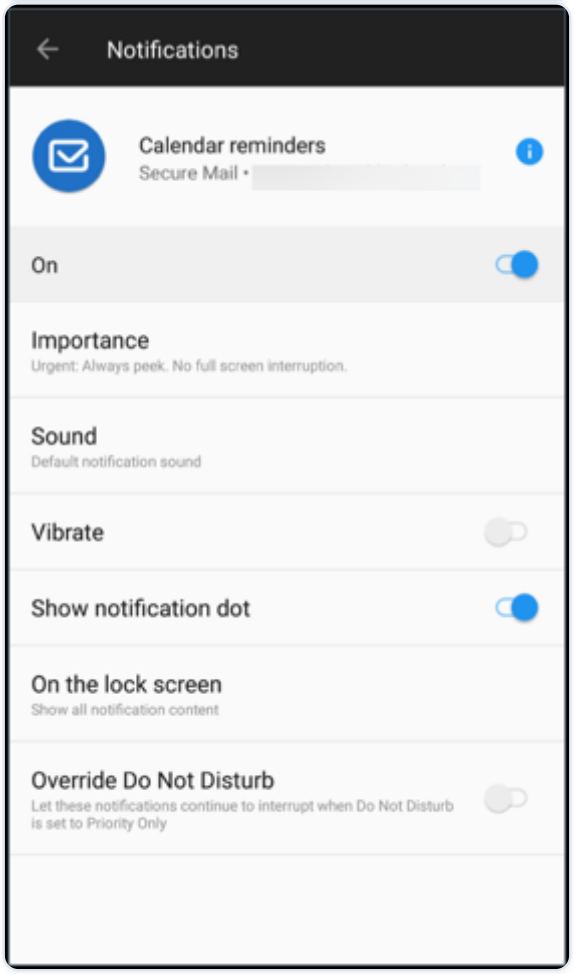
© 1997–2026 Citrix Systems, Inc. All rights reserved.



然后，您可以导航到**管理邮件通知**或**管理日历通知**，分别管理您的电子邮件或日历通知。

© 1997–2026 Citrix Systems, Inc. All rights reserved.





© 1997–2026 Citrix Systems, Inc. All rights reserved.

或者，您可以长按设备上的 Secure Mail 应用程序图标，选择 **应用信息**，然后点击 **通知**。

如果您的振动设置之前设置为 **仅在静音时**，则此功能会将振动设置更改为默认振动设置（**关闭**）。

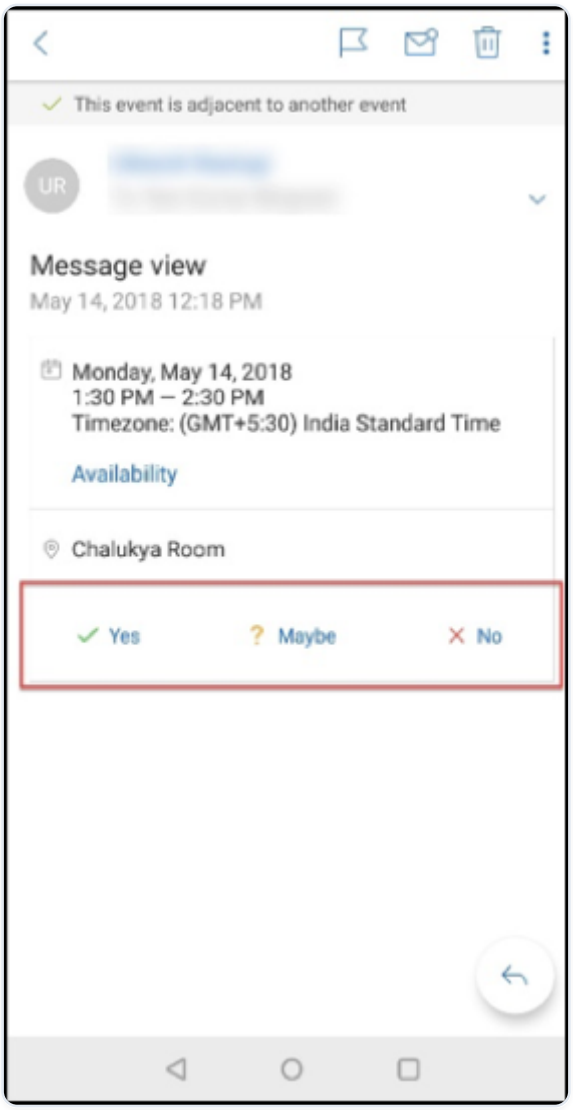
注意：

> 锁屏上的通知可用性取决于您的管理员如何配置“控制锁屏通知”MDX 策略。

电子邮件中的会议响应按钮

在适用于 Android 的 Secure Mail 中，会议响应按钮会显示在电子邮件中。当您收到有关会议邀请的电子邮件通知时，可以通过点击以下选项之一来响应邀请：

- 是
- 可能
- 否



© 1997–2026 Citrix Systems, Inc. All rights reserved.

附件增强功能

在适用于 Android 的 Secure Mail 中，查看附件变得更简单。为了提供更好的体验，我们移除了不必要的步骤，同时保留了早期版本中已有的附件选项。

您可以在 Secure Mail 应用程序中查看附件。如果附件可以使用 Secure Mail 查看，它会直接打开。如果附件无法使用 Secure Mail 查看，则会显示一个应用程序列表。您可以选择所需的应用程序来查看附件。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章 查看和附加文件。

返回按钮增强功能

在适用于 Android 的 Secure Mail 中，您可以点击设备上的返回按钮以折叠 **浮动操作** 按钮的展开选项。此操作会将您带回邮件或事件详细信息视图。

Android 返回按钮增强功能的图像(/en-us/mobile-productivity-apps/media/secure-mail-android-back-button.png)

在 Android 中启用从图库附加文件的管理员步骤

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 **受限**，用户无法直接从图库应用附加图像。如果您希望将此策略保持设置为 **受限**，但允许用户从图库添加照片，请在 Endpoint Management 控制台中执行以下步骤。

1. 将 **阻止图库** 设置为 **关闭**。
2. 获取设备的图库包 ID。例如：
    - **LG Nexus 5 手机：** com.google.android.gallery3d, com.google.android.apps.photos
    - **三星 Galaxy Note 3：** com.sec.android.gallery3d, com.sec.android.gallery3d.panorama360view, com.google.android.apps.photos
    - **索尼 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. 使隐藏策略 InboundDocumentExchangeWhitelist 可见：
    - 下载 WorxMail APK 文件并使用 MDX Toolkit 包装该文件。
    - 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 文件并找到 policy_metadata.xml 文件

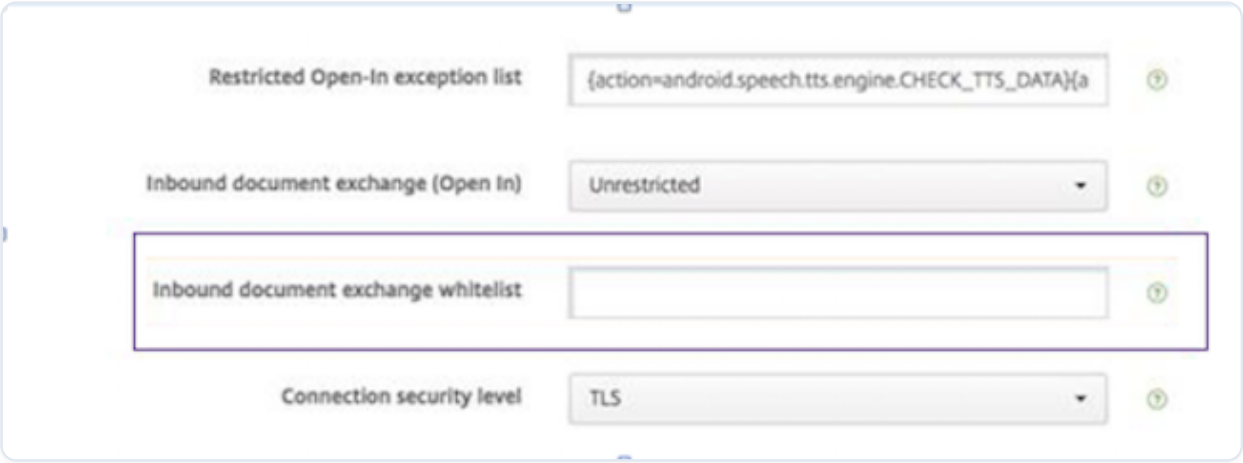
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 搜索并将 InboundDocumentExchangeWhitelist 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：**
>
> 不要压缩外部文件夹。选择文件夹内的所有文件并压缩选定的文件。

- 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 文件上传到 Endpoint Management 控制台，并将图库包 ID 列表添加到现在可见的入站文档交换白名单策略中。



确保包 ID 以逗号分隔：

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

5. 保存并部署 Secure Mail。

Android 用户现在可以从图库应用附加图像。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 表示可在 Secure Mail 中附加、查看和打开的文件格式。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

格式	IOS	安卓
视频: H.263 AMR NB codec_Mp4		是
视频: H.263 AMR NB codec_3gp		是
视频: H.264 AAC codec_3gp	是	是
视频: H.264 AAC codec_mp4	是	是
视频: H.264 Acclc codec_mp4	是	是
GTM recorded_wmv		X
AVI		X
WAV	X	X
MP4	X	X
3GP	X	X
FLAC 音频		X
AAC	X	X
M4A	X	X
3GP(AMR-NB) 格式	X	X
MP3	X	X
WAV	X	X
OGG		X
ICO	X	X
JPEG	X	X
PNG	X	X

© 1997–2026 Citrix Systems, Inc. All rights reserved.

格式	IOS	安卓
TIF (仅限单页)	X	
BMP	X	X
GIF	X	X
WebP		X
DOT	X	X
DOTX		X
PDF	X	X
PPT	是	是
PPTX	是	是
PPS		是
PPSX		是
DOC	是	是
DOCX	是	是
XLS	是	是
XLSM	是	是
XLSX	是	是
TXT	是	是
POT	是	是
POTX		X
HTM	X	X
HTML	X	X

© 1997–2026 Citrix Systems, Inc. All rights reserved.

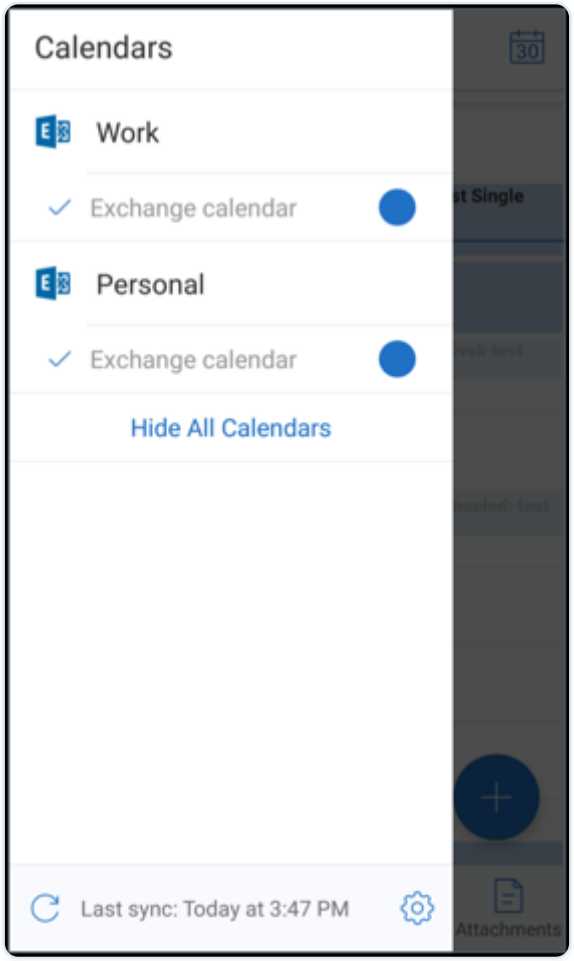
格式	IOS	安卓
ZIP	X	X
EML	X	X

日历

日历显示设备上所有账户的相关事件。您可以为各个账户设置颜色，以区分与各个账户相关的日历事件。

注意：

如果启用，个人日历功能始终与您的主要或默认账户关联。

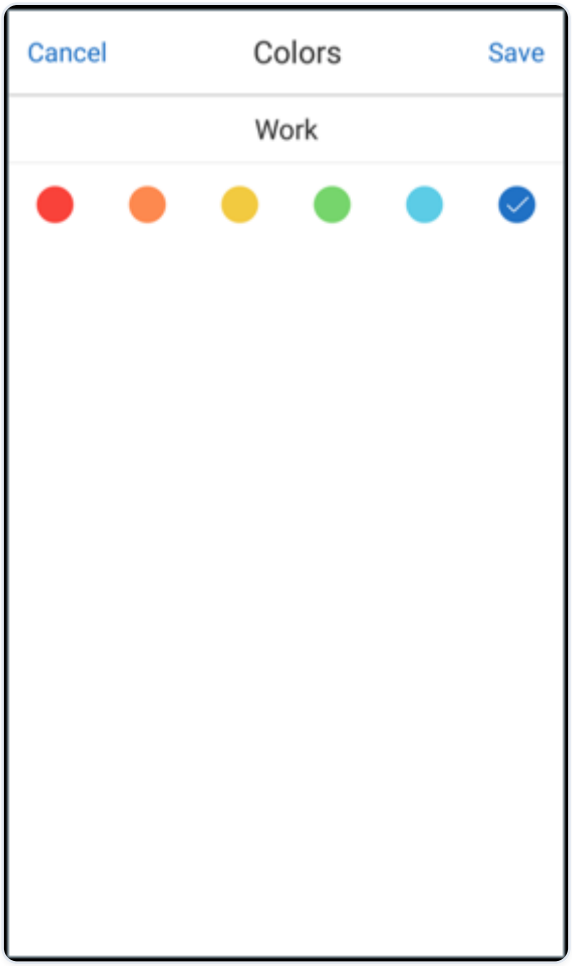


设置日历事件的颜色

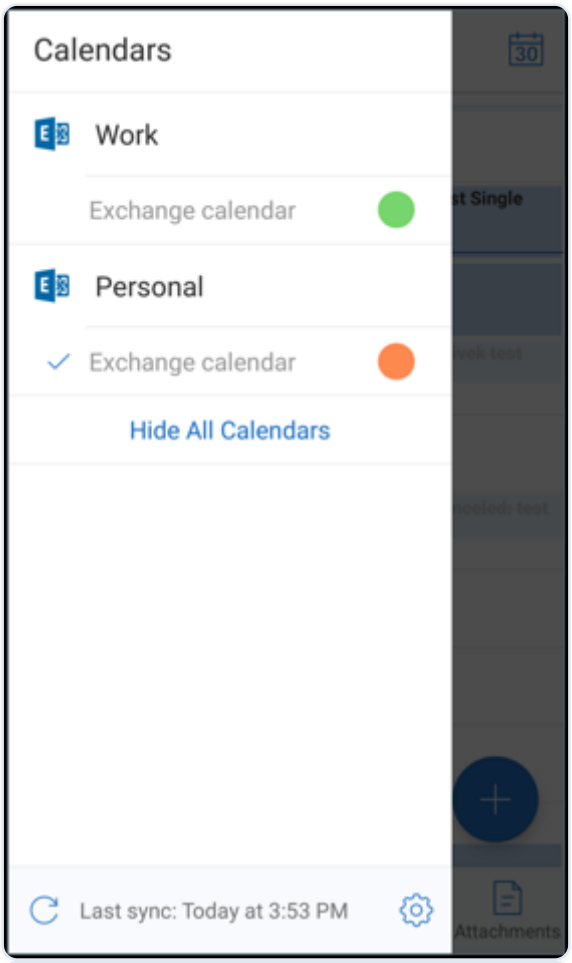
1. 点击页脚栏中的“**日历**”图标，然后点击左上角的汉堡图标。 “**日历**”屏幕会显示您已配置的所有账户。

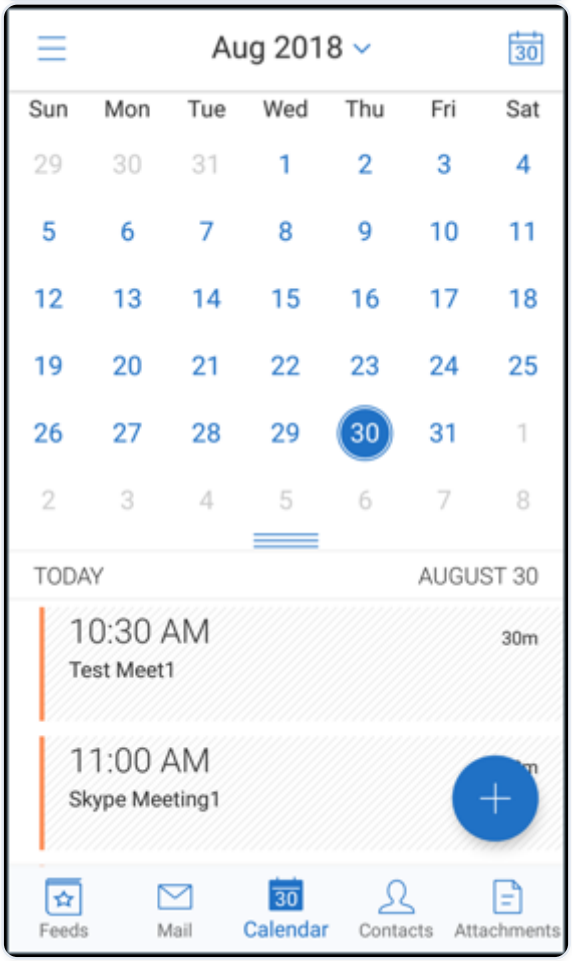
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 点击 Exchange 账户右侧显示的默认颜色。 “颜色”屏幕会显示该账户可用的颜色。
3. 选择您喜欢的颜色，然后点击“**保存**”。
4. 要返回上一屏幕，请点击“**取消**”。 所选颜色将应用于该 Exchange 账户的所有日历事件。



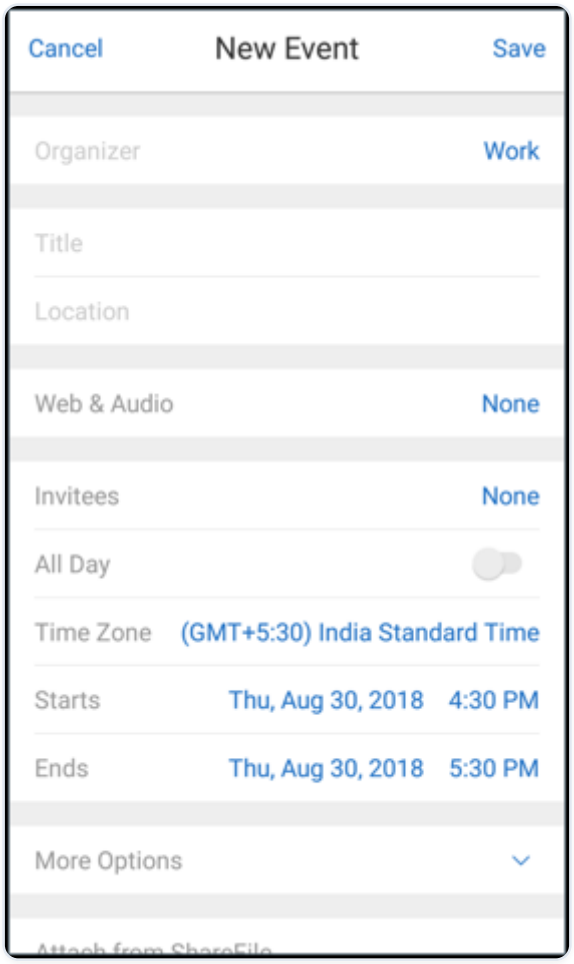
© 1997–2026 Citrix Systems, Inc. All rights reserved.



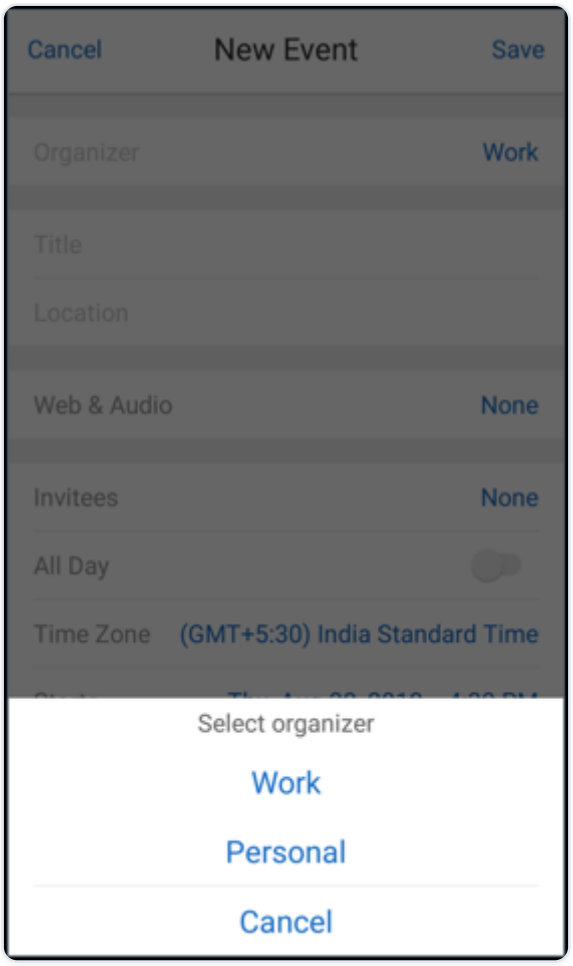


© 1997–2026 Citrix Systems, Inc. All rights reserved.

当您创建日历邀请或事件时，“**组织者**”字段会自动填充默认账户的电子邮件地址。要更改邮件账户，请点击此电子邮件地址并选择另一个账户。



© 1997–2026 Citrix Systems, Inc. All rights reserved.



搜索

您可以从“**邮箱**”或“**所有联系人**”视图执行全局搜索。此操作会在搜索应用中的所有帐户后显示相应结果。

在单个帐户中执行的所有搜索仅显示与该帐户相关的结果。

后台服务更新

为满足在运行 Android 8.0（API 级别 26）或更高版本的设备上 Google Play 后台执行限制的要求，我们已升级 Secure Mail 后台服务。为确保设备上的邮件同步和通知不中断，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**”。 **限制：**

- 如果您未启用基于 FCM 的推送通知，则后台同步每 15 分钟发生一次。此间隔因应用程序是在后台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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

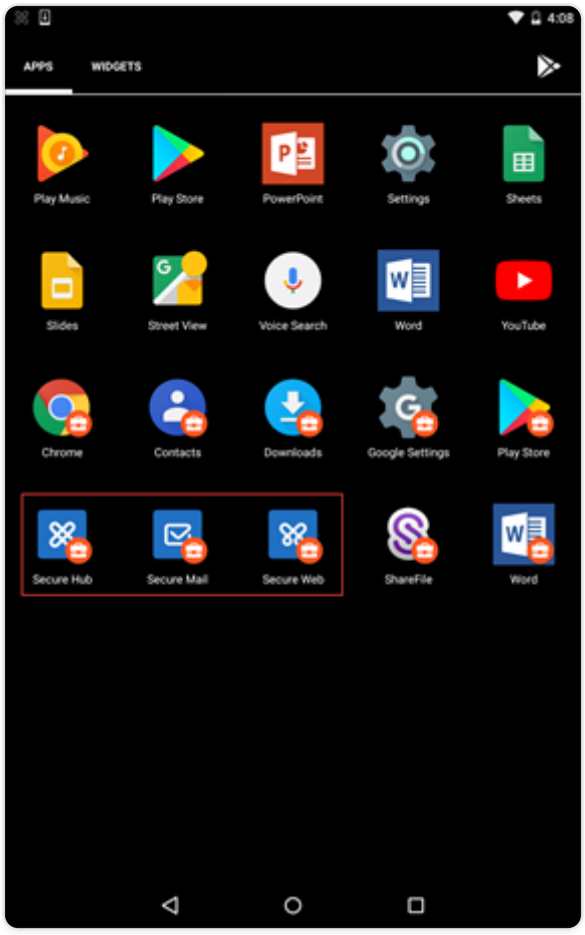
Secure Mail 中的 Android 企业版

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

先决条件

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

在 Endpoint Management 中设置 Android Enterprise 后，移动生产力应用程序将在您的设备上可用。Android Enterprise 图标标识了这些应用程序，如以下图像中突出显示。



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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

功能	支持
安全票证颁发机构 (STA)	X
导出联系人	X
Microsoft 信息权限管理	X
锁屏通知	X
邮件同步	X
电子邮件分类	X
S/MIME 签名和加密	X
Firebase 云消息传递 (FCM) 服务	X
现代身份验证 (OAuth)	
多个 Exchange 帐户	X
个人日历	
导出邮件设置	X
共享设备	
端点管理与 Microsoft Intune/EMS 集成	
微软 Office 365	X
LDAP Exchange 服务器 2010、2013 和 2016	X
基于证书的身份验证 (CBA)	
Go ToMeeting	X
Skype 企业版	
个人通讯组列表	X
Citrix Files 兼容性	X

© 1997–2026 Citrix Systems, Inc. All rights reserved.

功能	支持
通过单点登录进行电子邮件注册	X

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

功能	支持
隧道式 – Web SSO 模式	X
完整 VPN 模式	X
所有应用功能	X
与 Secure Mail 的兼容性	X

限制

- 如果针对工作配置文件模式下的 Android Enterprise 将**允许使用状态栏**设备限制策略设置为**开**，则 Android 版 Secure Mail 中的日历导出进度和推送通知不会显示在状态栏中。但是，如果允许，这些通知会显示在锁定屏幕上。有关详细信息，请参阅Android Enterprise 设置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure Mail 的 iOS 和 Android 功能

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

支持 Azure 政府云计算

Secure Mail 支持 Azure Active Directory 租户上用于现代身份验证 (OAuth) 的政府云计算 (GCC) High。Secure Mail 已注册为 GCC High 上的一个端点，以满足 Microsoft 对所有 GCC High 服务的强制要求。有关详细信息，请参阅 Microsoft 365 Government 中 Azure Active Directory 的新增功能。

通过此更改，您将被路由到 Azure Active Directory 租户上的 GCC High 进行身份验证。管理员需要允许 Secure Mail 在 Azure Active Directory 租户上拥有权限。

先决条件

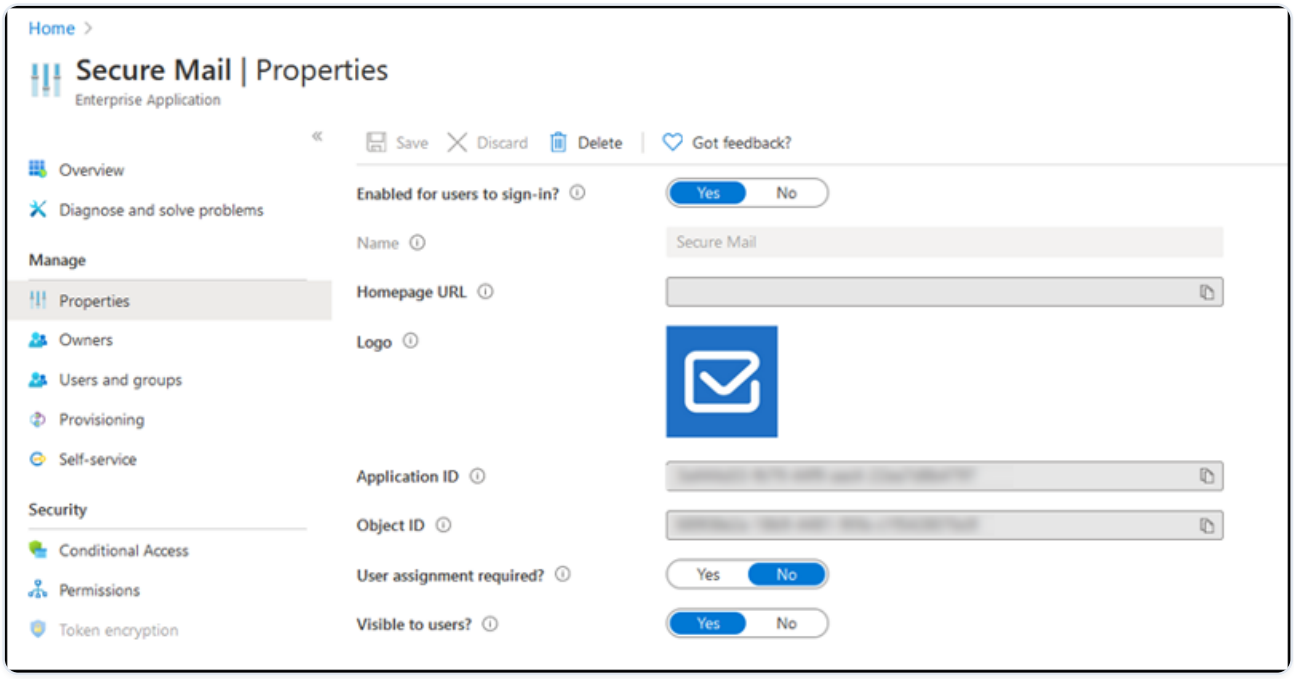
确保 Azure Active Directory 的全局管理员执行以下操作：

- 在您的设备上下载最新版本的 Secure Mail。
- 在 Secure Mail 应用程序上配置您的 Exchange 帐户，并允许 Azure Active Directory 上的应用程序权限，以便所有用户登录。请参阅以下屏幕。

注意：

这些步骤仅适用于全局管理员，作为一次性要求。一旦应用程序获得访问权限，您就可以直接从 App Store 升级。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



升级后

升级后，刷新令牌过期后会提示您重新授权，这会将您重定向到 Azure AD 上的 GCC High。验证上述工作流程，以确保授权请求已发送到 Azure AD 上的 GCC High。

您可以通过以下方式之一验证工作流程：

- 应用程序名称为 **Secure Mail-GCC High** 的 Secure Mail 会显示在您的 Azure Active Directory 租户的登录页面上。
- 检查 Secure Mail 日志以确认重新身份验证后重定向是否通过 `<https://login.microsoftonline.us>` 发生。

支持 ICS 文件

在 Secure Mail 中，您可以预览作为附件收到的 ICS 文件，并将其作为事件导入到您的日历中。

Secure Mail 中的联系人图片

在 Secure Mail 中，当您在电子邮件或会议邀请中添加收件人时，可以查看联系人图片。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章 显示您的联系人图片。

管理您的动态

在 Secure Mail 中，您现在可以根据您的要求组织您的 **动态** 卡片。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章 整理您的电子邮件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用 Office 365 Exchange Server 策略定义 Office 365 服务器地址

在 Secure Mail 中，在“Office 365 的 OAuth 支持”部分下添加了一个名为 **Office 365 Exchange Server** 的新策略。通过此策略，您可以定义云上存在的 Office 365 邮箱的主机名。此策略还支持政府机构使用 Office 365。主机名是一个单一值，例如 *outlook.office365.com*。默认值为 *outlook.office365.com*。

支持加密管理

加密管理允许您使用现代设备平台安全性，同时确保设备保持足够的状态以有效使用平台安全性。通过使用加密管理，您可以消除本地数据加密冗余，因为文件系统加密由 iOS 或 Android 平台提供。要启用此功能，管理员必须在 Citrix Endpoint Management™ 控制台中将 **加密类型** MDX 策略配置为 **带合规性强制的平台加密**。

要使用加密管理功能，请在 Citrix Endpoint Management 控制台中，将 **加密类型** 策略设置为 **带合规性强制的平台加密**。这将启用加密管理，并且用户设备上所有现有的加密应用程序数据将无缝转换为由设备而非 MDX 加密的状态。在此转换期间，应用程序会暂停以进行一次性数据迁移。迁移成功后，本地存储数据加密的责任将从 MDX 转移到设备平台。MDX 会在每次应用程序启动时继续检查设备的合规性。此功能在 MDM + MAM 和仅 MAM 环境中均可使用。

当您将 **加密类型** 策略设置为 **带合规性强制的平台加密** 时，新策略将取代您现有的 MDX 加密。

有关 Secure Mail 的加密管理 MDX 策略的详细信息，请参阅以下内容中的“**加密**”部分：

- 适用于 Android 移动生产力应用的 MDX 策略(/zh-cn/mobile-productivity-apps/administrator-tasks/policies-android.html#encryption)
- 适用于 iOS 移动生产力应用的 MDX 策略(/zh-cn/mobile-productivity-apps/administrator-tasks/policies-ios.html)

当设备不符合最低合规性要求时，**不合规设备行为**策略允许您选择要执行的操作：

- **允许应用** – 允许应用正常运行。
- **警告后允许应用** – 警告用户应用不符合最低合规性要求，并允许应用运行。这是默认值。
- **阻止应用** – 阻止应用运行。

运行 iOS 的设备

以下条件决定设备是否符合运行 iOS 的设备的最低合规性要求：

- iOS 10 - 应用运行的操作系统版本大于或等于指定版本。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 调试器访问 - 应用未启用调试。
- 越狱设备 - 应用未在越狱设备上运行。
- 设备密码 - 设备密码为**开**。
- 数据共享 - 应用未启用数据共享。

运行 Android 的设备

以下条件决定设备是否符合运行 Android 的设备的最低合规性要求：

- Android SDK 24 (Android 7 牛轧糖) - 应用程序运行的操作系统版本大于或等于指定版本。
- 调试器访问 - 应用程序未启用调试功能。
- 已 Root 设备 - 应用程序未在已 Root 设备上运行。
- 设备锁定 - 设备密码为 **ON**。
- 设备已加密 - 应用程序正在加密设备上运行。

支持响应式电子邮件

Secure Mail 已优化以提供响应式电子邮件。以前，包含大型表格或图像的电子邮件内容会错误呈现。此功能可使电子邮件内容在所有受支持的设备上更具可读性，无论电子邮件格式和大小如何。

拖放日历事件

在 Secure Mail 中，您可以通过拖放事件来更改现有日历事件的时间。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章：更改日历事件时间。

管理您的源

在 Secure Mail 中，您现在可以根据自己的要求组织 **Feed** 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：整理您的电子邮件。

自动前进

在 Secure Mail 中，当您在“**对话**”中删除邮件时，可以选择返回到哪封邮件。要使用此功能，请导航到“**设置 > 自动前进**”。然后，从可用选项中选择您的偏好。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章：删除并自动前进到“对话”中的电子邮件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

草稿文件夹自动同步

草稿文件夹会自动同步，您的草稿可在所有设备上使用。此功能适用于运行 Office 365 或 Exchange Server 2016 及更高版本的设备。

注意：

如果您的 Secure Mail 草稿包含附件，则附件不会同步到服务器。

有关此功能的用户帮助文档（包括视频），请参阅 Citrix 用户帮助中心文章 草稿文件夹自动同步。

在 MDM + MAM 模式下使用 Microsoft Intune 时支持单点登录

对于运行 iOS 的设备：

要使用此功能，请确保您的设备上已安装 Microsoft Authenticator 应用。有关安装 Microsoft Authenticator 应用的更多信息，请参阅 Docs.microsoft.com 上的 **下载并安装 Microsoft Authenticator** 应用。

对于运行 Android 的设备：

要使用此功能，请确保您的设备上已安装 Intune 公司门户应用。登录 Intune 公司门户应用后，您无需使用凭据在 Secure Mail 中重新进行身份验证即可在 MDM + MAM 模式下使用 SSO。

联系人功能增强

在 Secure Mail 中，当您点击“**联系人**”并选择一个联系人时，该联系人的详细信息将显示在“**联系人**”选项卡下。当您点击“**组织**”选项卡时，将显示组织层次结构详细信息，例如“**经理**”、“**直接下属**”和“**同事**”。当您点击屏幕右上角的更多图标时，将显示以下选项：

- 编辑
- 添加到 VIP
- 取消

在“**组织**”选项卡中，您可以点击“**经理**”、“**直接下属**”或“**同事**”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“**同事**”的详细信息。您可以撰写并发送电子邮件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

先决条件

确保您的 Exchange Server 上已启用 Exchange Web Services (EWS)。

联系人详细信息根据从 Active Directory 获取的组织详细信息（Outlook 联系人）显示。要使您的联系人显示正确的详细信息，请确保您的管理员已在 Active Directory 中配置了您的组织层次结构。

注意：

IBM Lotus Notes 服务器不支持此功能。

将会议时间和地点导出到您的本机日历

在 Secure Mail 中，**导出日历** MDX 策略中添加了一个新值 **会议时间、地点**。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到您的本机日历。

多个 Exchange 帐户

在 Secure Mail 的“设置”中，您可以添加多个 Exchange 电子邮件帐户并在它们之间切换。此功能允许您在一个位置监控所有邮件、联系人和日历。管理员先决条件如下：

- 配置更多帐户需要用户名和密码。自动注册或凭据存储配置仅适用于应用程序中设置的第一个帐户。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，则无法添加其他基于证书的帐户。其他帐户必须使用基于 Active Directory 的身份验证。Secure Mail 在配置多个帐户时不支持基于证书的身份验证。
- 要允许更多帐户连接到外部网络中的域或 Exchange Server，您必须在 Citrix ADC 中将拆分隧道设置为 **ON**。
- 适用于 iOS 的 Secure Mail 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。

联系人

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

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：为同步的 Secure Mail 日历设置颜色。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

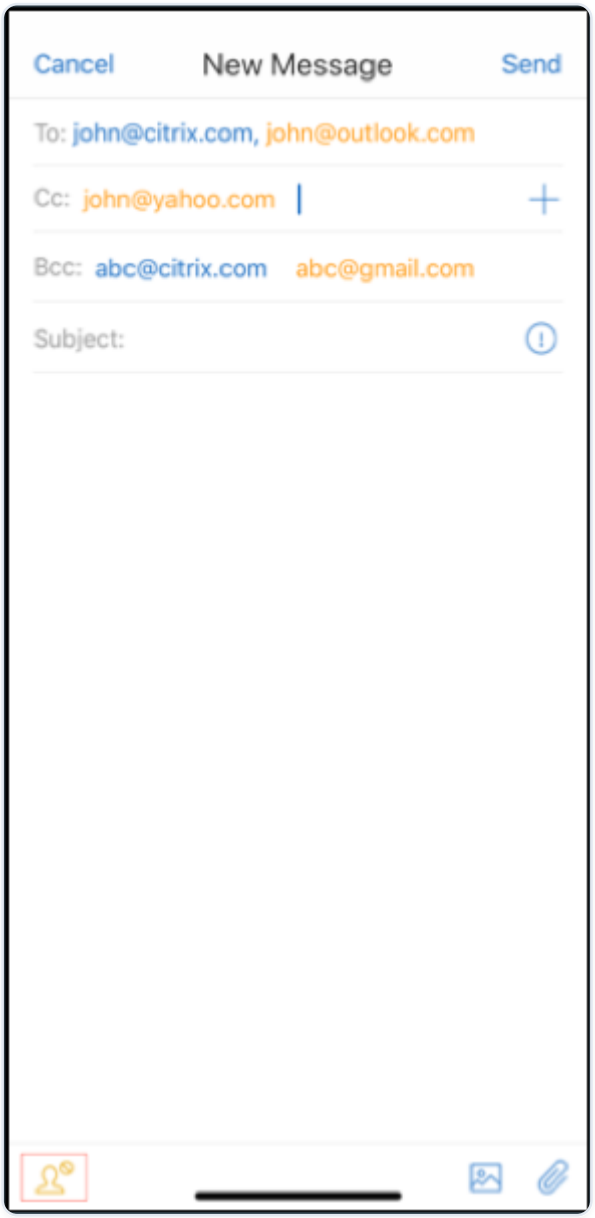
内部域

您可以识别和编辑属于外部组织的邮件收件人。

先决条件： 确保您已在 Citrix Endpoint Management 中启用**内部域**策略，并已重新启动应用程序。

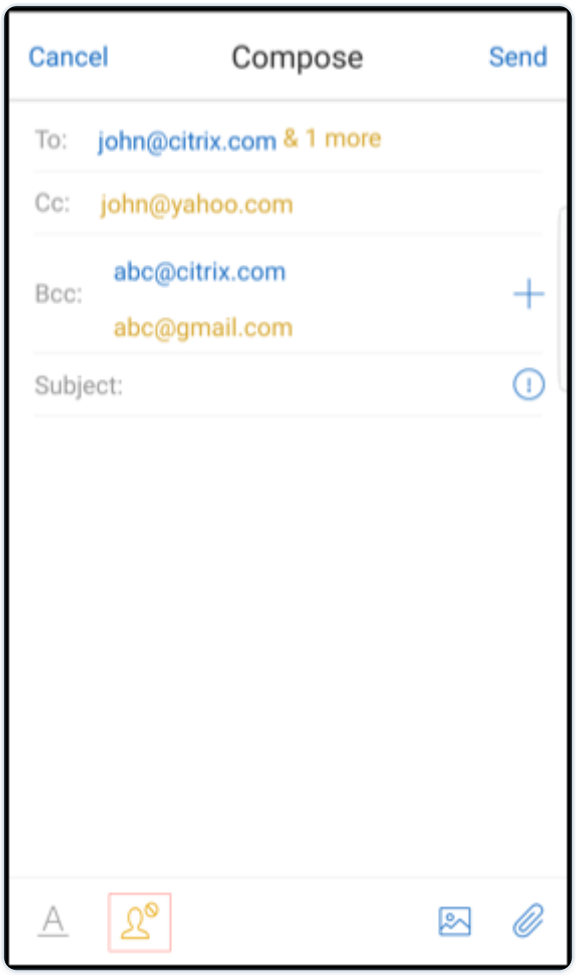
当您创建、回复或转发电子邮件时，外部收件人会在邮件列表中突出显示。**联系人**图标会作为警告显示在屏幕左下方。点击**联系人**图标以修改邮件列表。

在运行 iOS 的设备上：



在运行 Android 的设备上：

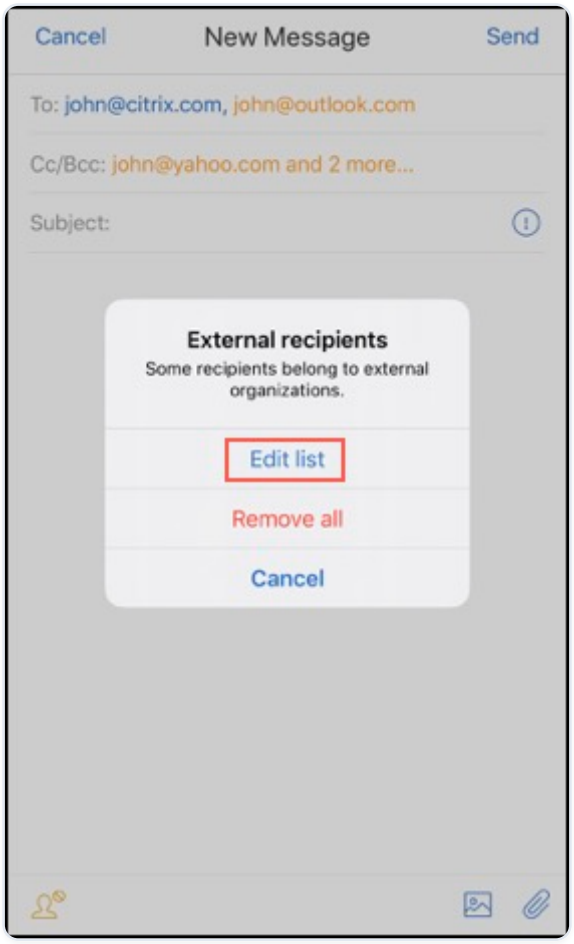
© 1997–2026 Citrix Systems, Inc. All rights reserved.



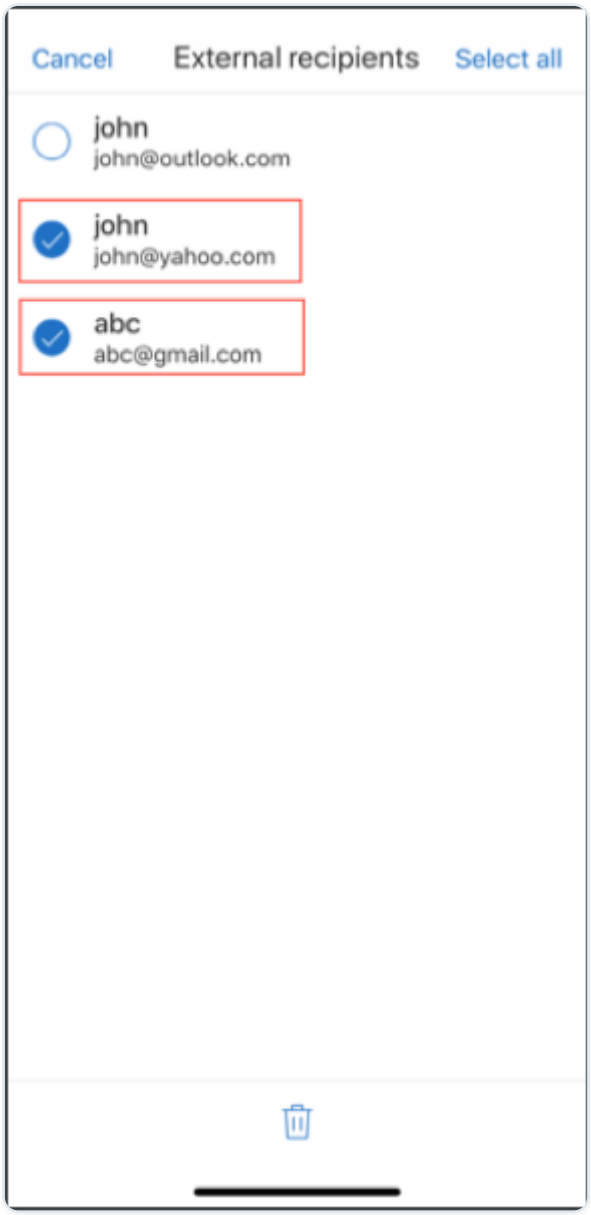
点击**联系人**图标时，将出现一个弹出窗口，其中包含编辑列表或全部删除的选项。点击**编辑列表**以选择要删除的收件人。选择收件人后，点击**垃圾桶**图标。

在运行 iOS 的设备上：

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



在运行 Android 的设备上：

编辑列表(/en-us/mobile-productivity-apps/media/extrecipients-android-editlist1.png)

删除收件人(/en-us/mobile-productivity-apps/media/extrecipients-android-editlist2.png)

人机工程学改进

通过此增强功能，操作按钮从屏幕顶部移至底部，以便于访问。这些更改已应用于**收件箱**、**日历**和**联系人**屏幕。

注意：

> 对于 Android，这些更改已应用于**收件箱**和**日历**屏幕。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在运行 iOS 的设备上

人机工程学改进(/en-us/mobile-productivity-apps/media/ergonomic-improvements-ios.png)

在运行 Android 的设备上

人机工程学改进(/en-us/mobile-productivity-apps/media/ergonomic-improvements-android.png)

已增强**响应**浮动操作按钮，使其与 Citrix 品牌和样式指南保持一致。

此外，通过此增强功能，已删除从打开的电子邮件访问主收件箱屏幕上按钮的选项。您必须退出已打开的电子邮件才能访问**源**、**日历**、**联系人**和**附件**等项目。

iOS 底部栏中的选项已更改，这有助于保持 iOS 和 Android 之间的一致性。

Secure Mail 与 Slack 集成（预览版）

您现在可以将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 集成（预览版）。

报告网络钓鱼电子邮件（作为转发）

在 Secure Mail 中，您可以使用“报告为网络钓鱼”功能报告您怀疑是网络钓鱼的电子邮件（作为转发）。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“**通过转发报告**”。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章：报告网络钓鱼电子邮件。

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。有关此功能的用户帮助文档（包括管理员设置的详细信息），请参阅 Citrix 用户帮助中心文章：报告网络钓鱼电子邮件。

导出 Secure Mail 日历事件

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

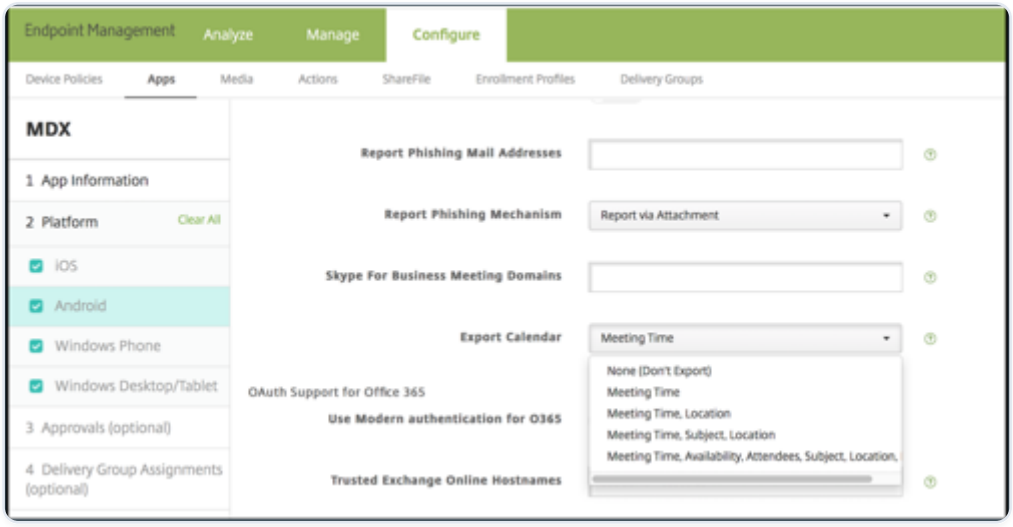
以下 MDX 策略值可用于显示在您的个人日历中的日历事件字段：

- 无（不导出）
- 会议时间

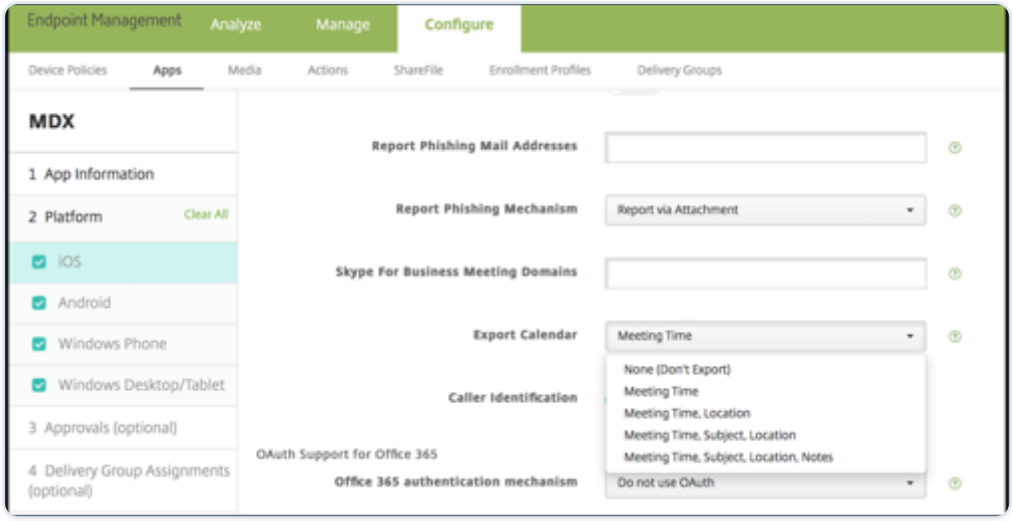
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 会议时间、地点
- 会议时间、主题、地点
- **（适用于 Android）** 会议时间、可用性、与会者、主题、地点、备注
- **（适用于 iOS）** 会议时间、主题、地点、备注

Android 选项：



iOS 选项：



适用于 iOS

尽管从 Secure Mail 导出的日历事件是**读/写**的，但在 Secure Mail 外部对事件所做的更改不可用。

重要提示：

- 如果满足以下任一条件，则此功能在 Secure Mail 中可见但已禁用：
  - 导出日历策略设置为**关闭**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - 您的 MDX 版本不包含该策略

- 如果您的个人日历应用中已配置电子邮件帐户且您的 iCloud 帐户已禁用，则此功能不起作用。如果您的个人日历应用中未配置其他帐户，则此功能有效。
- 要从您的个人日历启动 URL 并编辑 Secure Mail 日历事件，请确保值 **“ctxevent:”** 包含在“应用 URL 方案”MDX 策略中。

适用于 Android

从 Secure Mail 导出的日历事件是只读的。要编辑 Secure Mail 事件，请点击日历事件中的“**Secure Mail 事件**”链接。

重要提示：

- 如果满足以下任一条件，则此功能在 Secure Mail 中可见但已禁用：
    - 导出日历策略设置为**关闭**。
    - 您的 MDX 版本不包含此策略。
- 确保“入站文档交换”MDX 策略设置为“**无限制**”。
- Secure Mail 事件链接在三星和华为设备上不可用。

源文件夹

Secure Mail 在“**源**”文件夹中显示所有未读电子邮件、需要您关注的会议邀请以及即将召开的会议。

查看源卡片

点击页脚选项卡栏右下角的“**源**”图标。

源图标的图像(/en-us/mobile-productivity-apps/media/Feeds_pd.jpg)

将显示以下源卡片：

- 未读
- 会议邀请
- 即将召开的会议

默认情况下，Secure Mail 仅显示来自主帐户的源。如果您配置了多个帐户，则可以查看来自其他帐户的源。要查看来自其他帐户的源，请点击“**源**”，点击汉堡图标，然后选择相应的帐户。

源图标的图像(/en-us/mobile-productivity-apps/media/feeds_settings.jpg)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

源根据项目的时间戳进行排序，并显示以下上限：

- 五封未读电子邮件
- 两个会议邀请
- 三个即将召开的会议

要查看信息流卡中的所有项目，请点击“**查看全部**”。

注意：

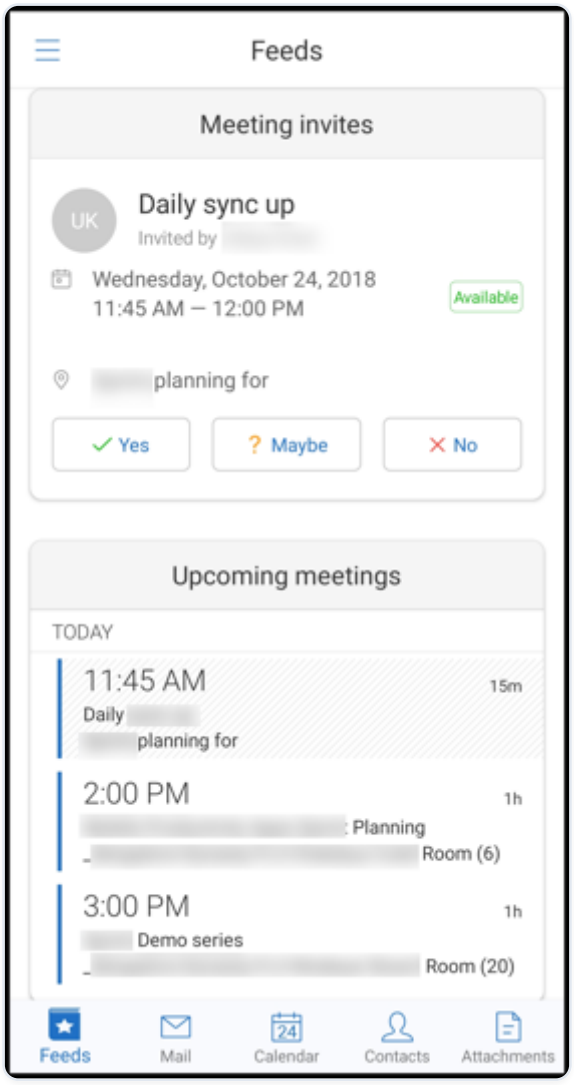
每张卡片中显示的信息流数量取决于您在设备上设置的同步邮件周期。

信息流文件夹的增强功能

以下是对现有**信息流**文件夹的增强功能：

- 来自所有自动同步文件夹的会议邀请会显示在您的信息流卡中。
- 在您的信息流卡中查看最多五个即将召开的会议。
- 未来 24 小时内的即将召开的会议会显示在信息流卡中，并分为“**今天**”和“**明天**”部分。

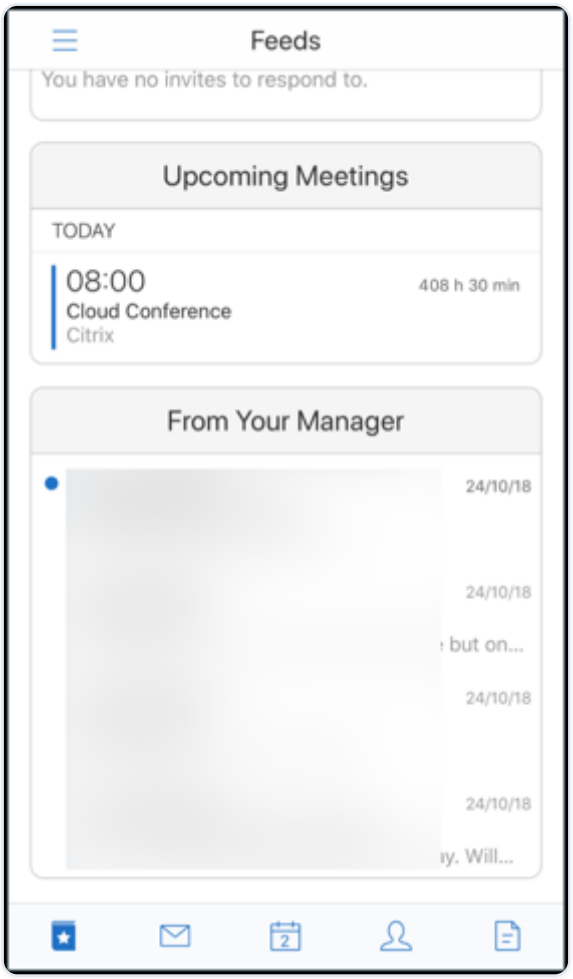
© 1997–2026 Citrix Systems, Inc. All rights reserved.



来自您经理的信息流

在 Secure Mail 中，您可以在“**信息流**”屏幕中查看来自经理的电子邮件。根据您的“**同步邮件周期**”设置，最多五封电子邮件会显示在“**来自您的经理**”信息流下。要查看更多来自经理的电子邮件，请点击“**查看全部**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



先决条件：

确保您的 Exchange Server 上已启用 Exchange Web Services (EWS)。

经理卡片根据从 Active Directory 获取的组织详细信息（Outlook 联系人）显示。为了使正确的详细信息显示在经理源中，请确保您的管理员已在 Active Directory 中配置了您的组织层次结构。

注意：

此功能不支持在 IBM Lotus Notes 服务器上使用。

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，以及每种类型的拨入要求。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

支持的会议类型

会议类型	识别要求	点击“加入会议”后的操作
微软 Teams		如果已安装 Microsoft Teams 应用程序，应用程序将打开，用户加入会议。如果未安装该应用程序，用户会看到从应用商店安装 Microsoft Teams 的选项。
GoToMeeting (GTM)	会议内容中包含以下任一信息：1) 此类 URL：`https://www1.gotomeeting.com/join/1234567892`；2) 采用以下任一格式的 GTM 访问代码：GTM: 123456789, GTM – 123456789, G2M – 123456789, G2M: 123456789	如果安装了 GTM 应用程序，则该应用程序会打开，用户加入会议。如果未安装该应用程序，用户会看到一个选项，可前往应用商店安装 GTM。对于 gotomeet.me/username 格式的 GTM，该应用程序会打开，用户加入会议。
WebEx		如果设备上安装了未封装的 WebEx 应用程序，Citrix Secure Web™ 会打开该应用程序。必须将 WebEx 添加为 Android 上 Secure Web 受限打开例外列表和 iOS 上允许的 URL 策略中的例外。
商务版 Skype		用户可以单击在 Secure Web 中打开的链接，如果设备上安装了未封装的 Skype for Business 应用程序，则 Secure Web 会打开该应用程序。将 Skype for Business 应用程序添加为 Android 上 Secure Web 受限打开例外列表策略中的例外。在 iOS 上允许的 URL 策略中添加例外。

配置以下策略列表允许用户点击会议链接以打开相关应用程序。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Teams 应用程序

- **iOS - “允许的 URL”策略”：\^msteams:
- **Android - “打开排除项”策略：{action=android.intent.action.VIEW scheme=msteams package=com.microsoft.teams}

Zoom 应用程序

- **iOS - “允许的 URL”策略：**+\^zoomus:
- **Android - “打开排除项”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：**+\^wbx: 示例策略字符串为 \^http:,\^https:, \^mailto:=ctxmail:,+\^citrixreceiver:,+\^telprompt:,+\^tel:,+\^col-g2m-2:,+\^col-g2w-2:,+\^wbx:,+\^maps:ios_addr:
- **Android - “打开排除项”策略：**{action=android.intent.action.VIEW scheme=wbx package=com.cisco.webex.meetings}

商务版 Skype

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

斯凯普

- **iOS - “允许 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

以下列表指明了每种会议类型及其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）：000 800 100 7855

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - 美国（免费）：1 877 309 2073

- 任何符合 RFC 3966 格式标准的电话号码。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何格式中获取：

- 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”
- 格式，例如“Access Code: 123456789”

WebEx：

支持的电话号码格式：

- WebEx 呼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（美国长途）
- 符合 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：

- 会议号码：123 456 789
- 访问代码：123 456 789

注意：

对于九位或更少数字的会议代码，系统会自动添加 # 键以拨入会议。

Skype 企业版

支持的电话号码格式：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

支持的会议代码格式：

会议正文包含以下文本：“会议 ID：123456789”

注意：

对于 Skype for Business 会议，系统会自动添加 # 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，请参阅互联网标准跟踪协议文档。示例：
  - 5555555555
  - (555) 555-5555
  - 555-555-5555
  - 555-555-555-5555 (在有国家代码的情况下)
  - 1-555-555-5555
  - +1-555-555-5555

注意：

在电话号码的数字之间使用单个分隔符。例如，使用“) –”可能导致号码无法识别。

支持的会议代码格式：

推荐格式：“(电话号码)”,“(代码)”

您最多可以指定四个逗号，并在必要时提供 # 键。有关支持的格式列表，请参阅本文档后面的表格。

对于音频会议，以下格式允许用户点击**拨入**。但是，如果他们从日历会议正文中点击电话号码，他们可以拨入会议。然后他们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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

支持的电话号码格式	会议代码分隔符	示例
采用 RFC 3966 格式的任何电话号码。示例：5555555555; (555) 555-5555; 555-555-5555; 555-555-555-5555（包含国家/地区代码时）； 1-555-555-5555;+1-555-555-5555	参与者代码	1-888-999-9999 参与者代码: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
	主持人代码	1-888-999-9999 主持人代码:99999999
	主持人 PIN	1-888-999-9999 主持人 PIN:99999999
	主席代码	1-888-999-9999 主席代码:99999999
	主席 PIN	1-888-999-9999 主席 PIN:99999999
	主持人 PIN	1-888-999-9999 主持人 PIN:99999999
	PIN	1-888-999-9999 PIN:99999999
	访问代码	1-888-999-9999 访问代码:99999999

© 1997–2026 Citrix Systems, Inc. All rights reserved.

支持的电话号码格式	会议代码分隔符	示例
	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
	,	+1 (631) 992-3240,958209234#
	,,	+1 (631) 992-3240,,958209234#
	,,,	+1 (631) 992-3240,,,958209234#
	,,,,	+1 (631) 992-3240,,,,958209234#
	密码	+1 (631) 992-3240 密码 958209234#
	分机	+1 (631) 992-3240 分机:958209234#
	分机号.	+1 (631) 992-3240 分机号 958209234#
	；分机号=	+1 (631) 992-3240；分机号 958209234#
	分机号	+1 (631) 992-3240 分机号 958209234#
	HC	+1 (631) 992-3240 HC 958209234#
	分机号	+1 (631) 992-3240 分机号 958209234#

© 1997–2026 Citrix Systems, Inc. All rights reserved.

支持的电话号码格式	会议代码分隔符	示例
	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

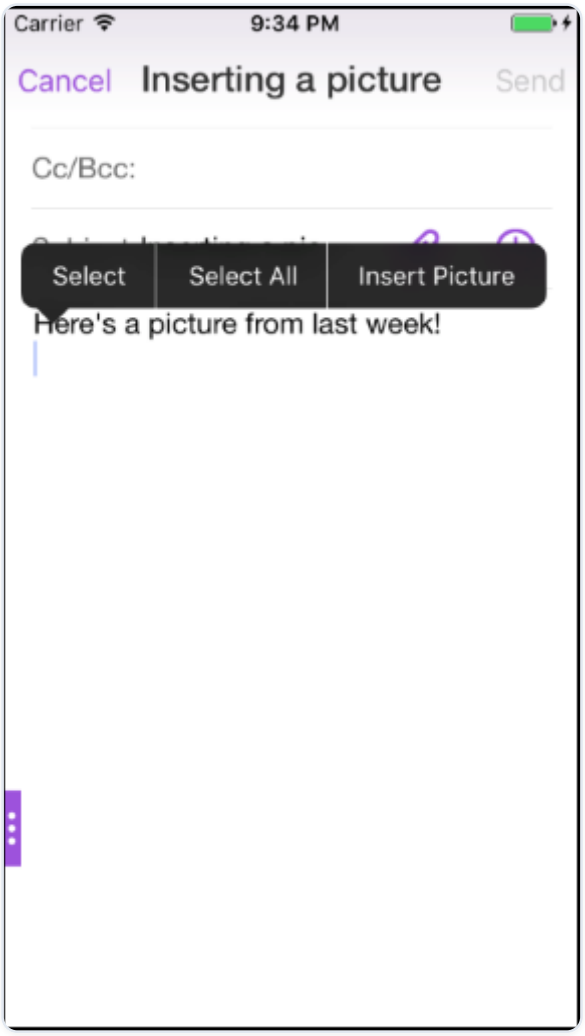
在 iOS 和 Android 设备上，您可以从本机日历应用导入个人日历，并在 Secure Mail 中查看您的个人日程。有关此功能的用户帮助文档，请参阅 Citrix 用户帮助中心文章：查看您的个人日历日程。

插入内联图像

以下过程介绍如何插入内联图像。

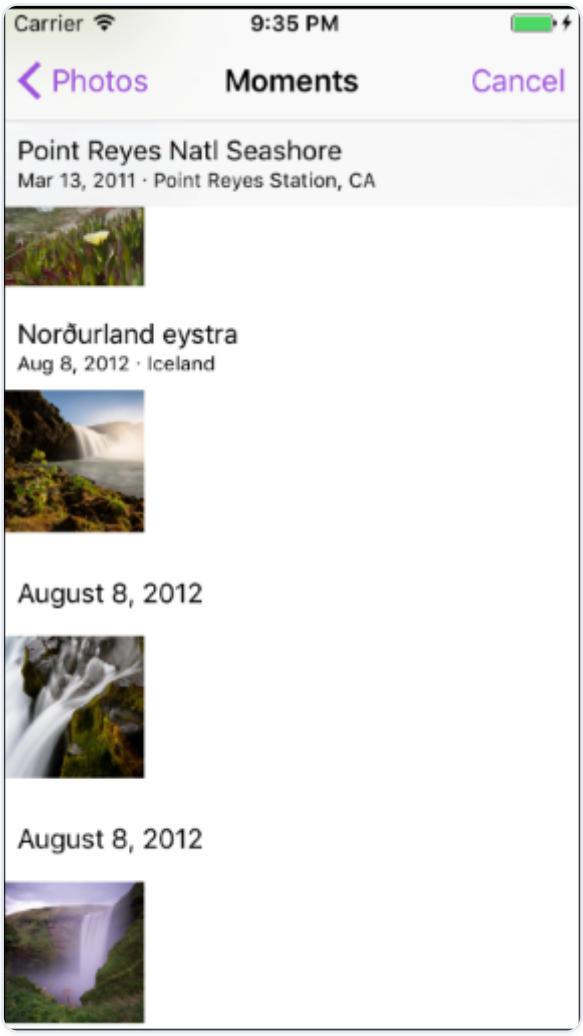
1. 要将内联图像附加到电子邮件中，请在邮件正文中长按。在出现的选项中，点击**插入图片**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Secure Mail 可能会提示您授予访问照片的权限。照片库随即出现。导航到图库并点击您要插入的图片。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 邮件现在包含您选择的图像。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



滑动操作

在 iOS 和 Android 设备上，您可以通过向左或向右滑动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：使用滑动操作。

在 iOS 和 Android 上加入 Skype for Business 会议

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

加入 Skype for Business 会议

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

   如果您的设备上未安装 Skype for Business，请点击“**安装 Skype**”以安装该应用程序。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

附件的应用内预览及其他附件增强功能

您现在可以在 Secure Mail 应用内预览附件（MS Office 和图像），而无需使用 QuickEdit 等第三方应用程序打开它们。

查看附件时，您可以执行以下操作：

- 从邮箱中选择现有邮件以附加文件。
- 选择新邮件以附加文件。
- 保存附件以供离线访问。
- 从离线文件中删除附件。
- 使用其他应用程序打开附件。
- 查看附件的源电子邮件或日历事件。

注意：

仅当从“**附件**”存储库查看附件时，您才能查看源电子邮件或日历事件。

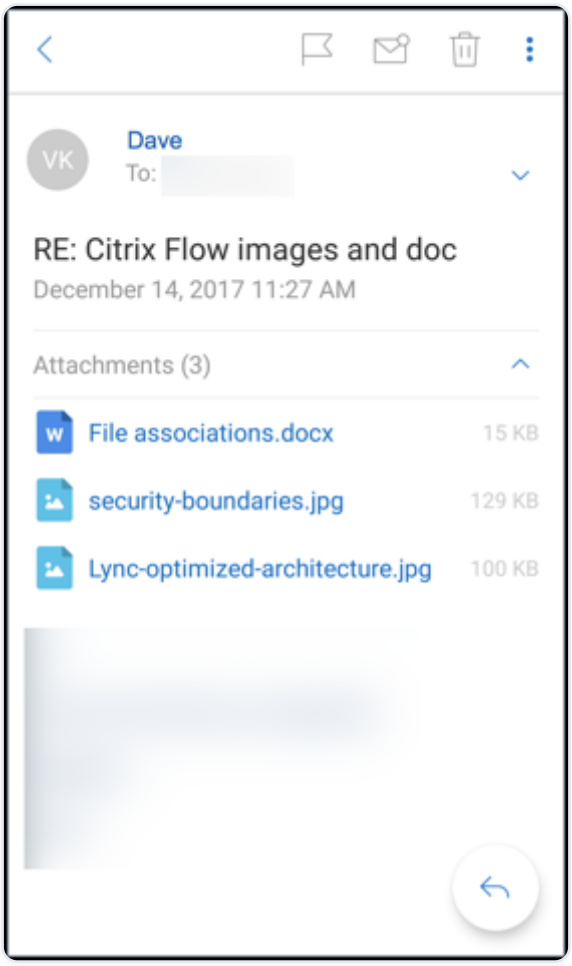
您还可以在以下情况下预览附件：

- 查看邮件。
- 撰写新邮件。
- 附件文件夹。
- 日历事件。

选择要附加文件的邮件

1. 打开包含附件的电子邮件。

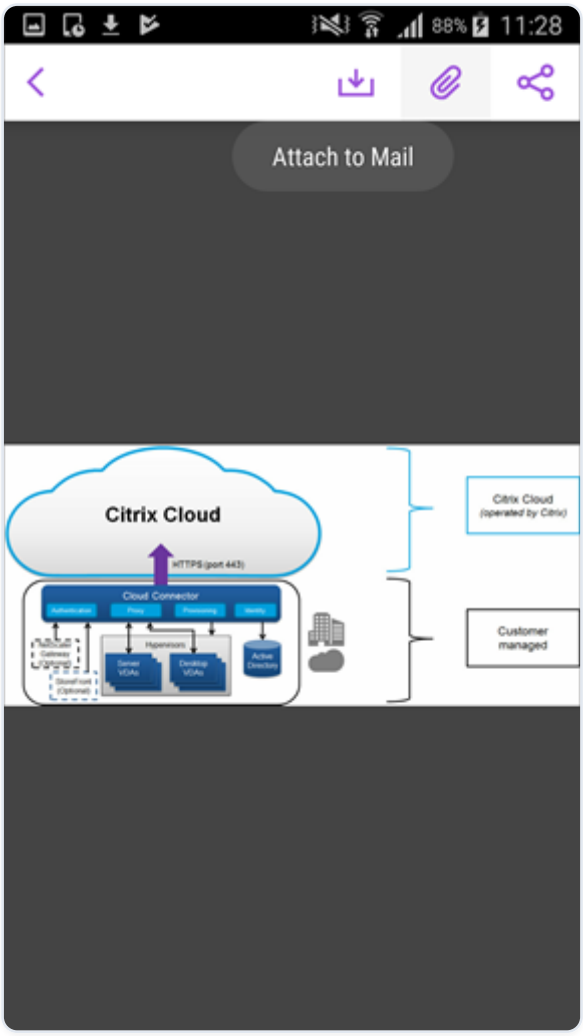
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 点击附件。
3. 点击**附加**图标。

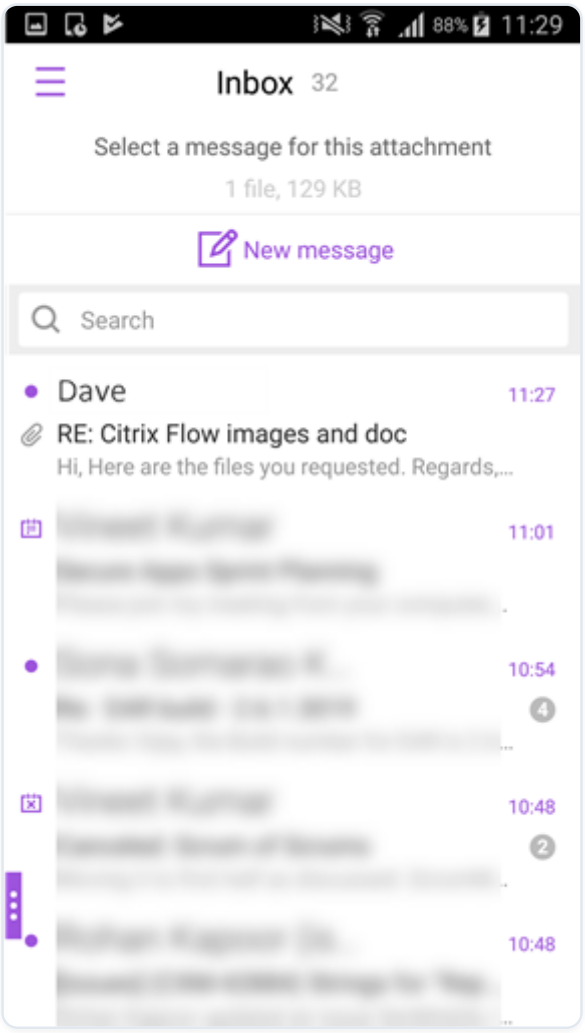
   出现收件箱。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

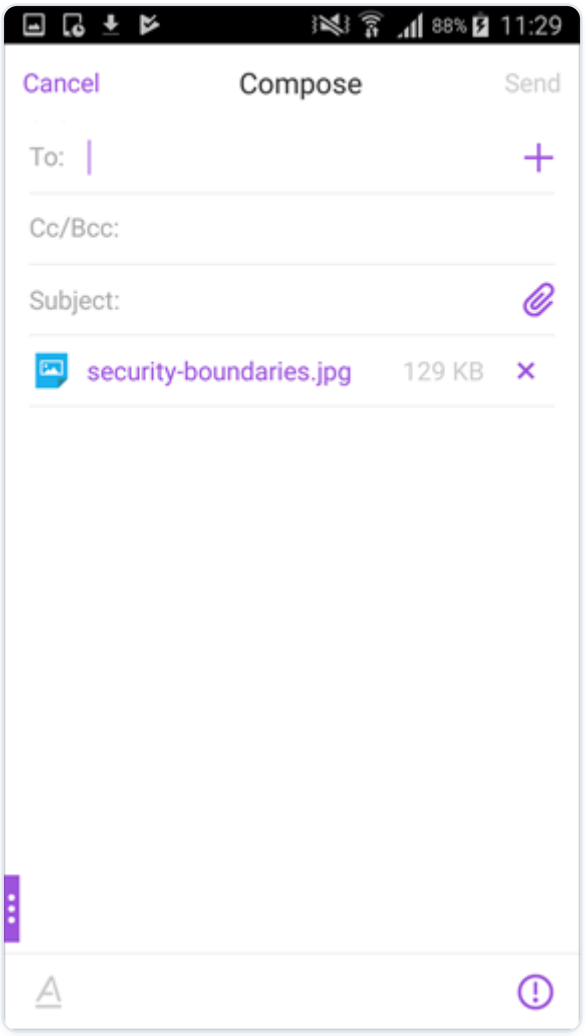


4. 选择现有邮件以附加此文件，或点击**新邮件**以将此文件附加到新邮件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



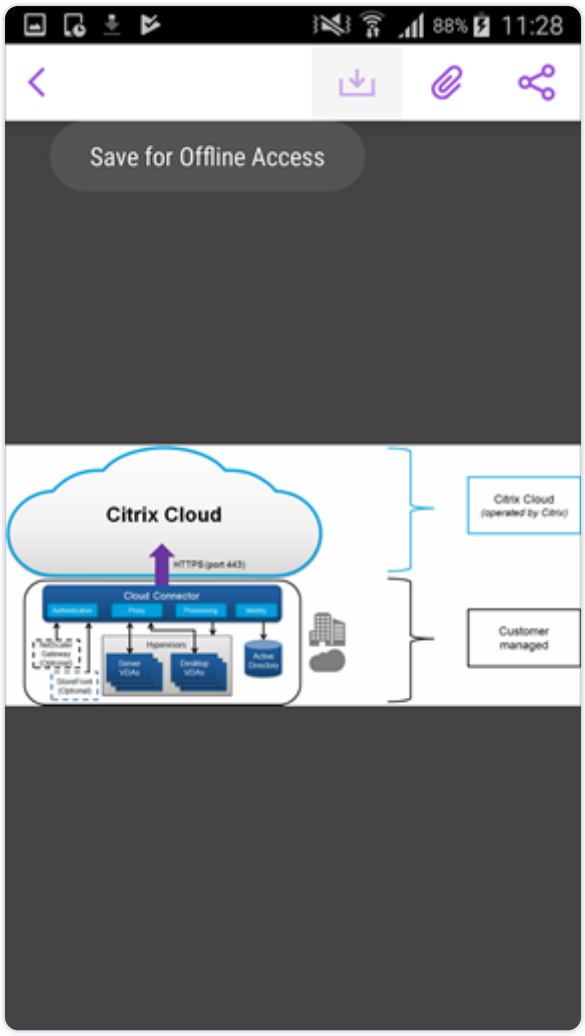
© 1997–2026 Citrix Systems, Inc. All rights reserved.



保存附件以供离线访问

1. 打开附件。
2. 点击页面右上角的**更多**图标，然后点击**保存以供离线访问**，以保存附件供离线访问。

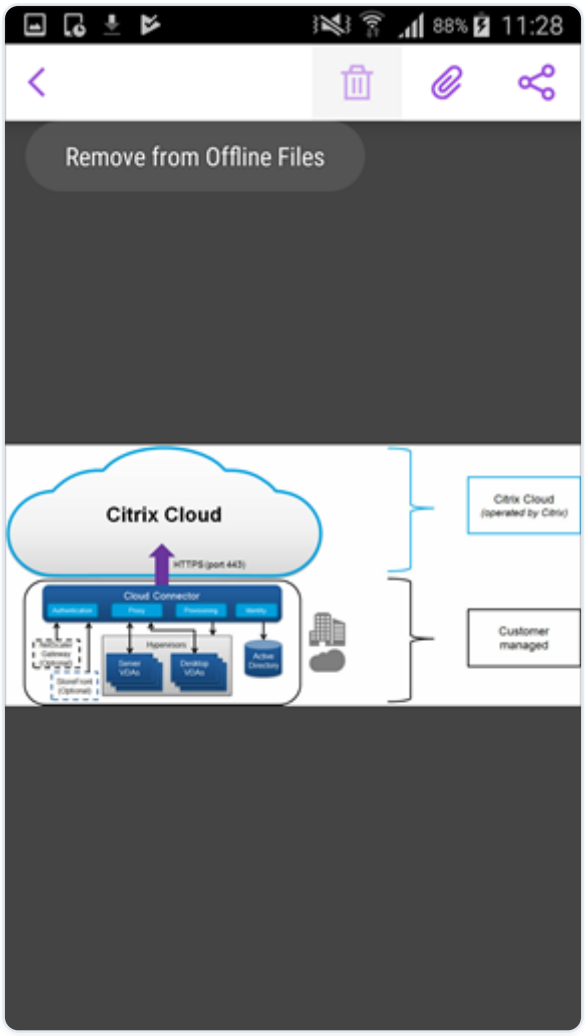
© 1997–2026 Citrix Systems, Inc. All rights reserved.



从离线文件中删除附件

1. 打开附件。
2. 点击页面右上角的**更多**图标，然后点击**从离线文件中删除**，以从离线文件中删除附件。

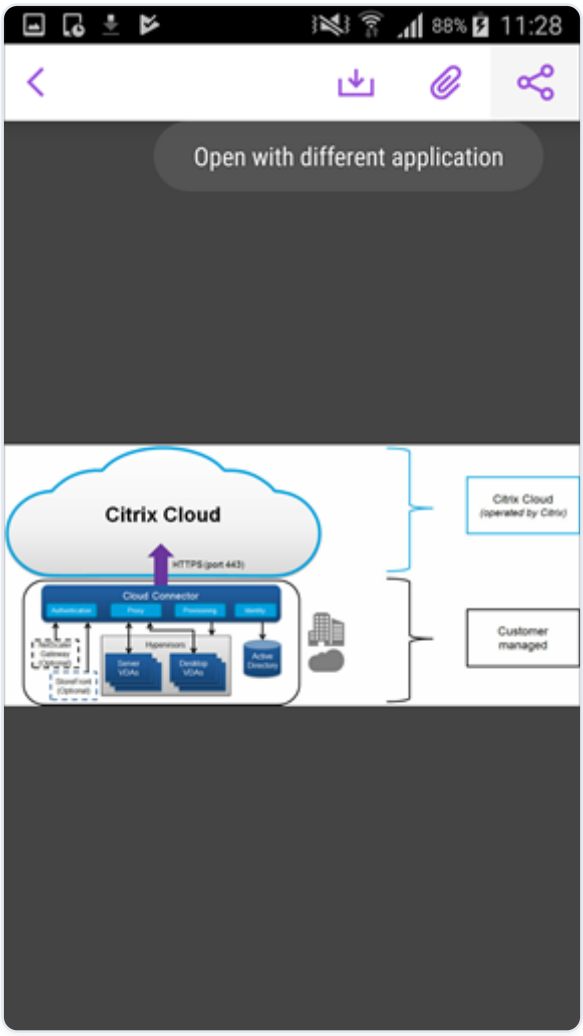
© 1997–2026 Citrix Systems, Inc. All rights reserved.



使用其他应用程序打开附件

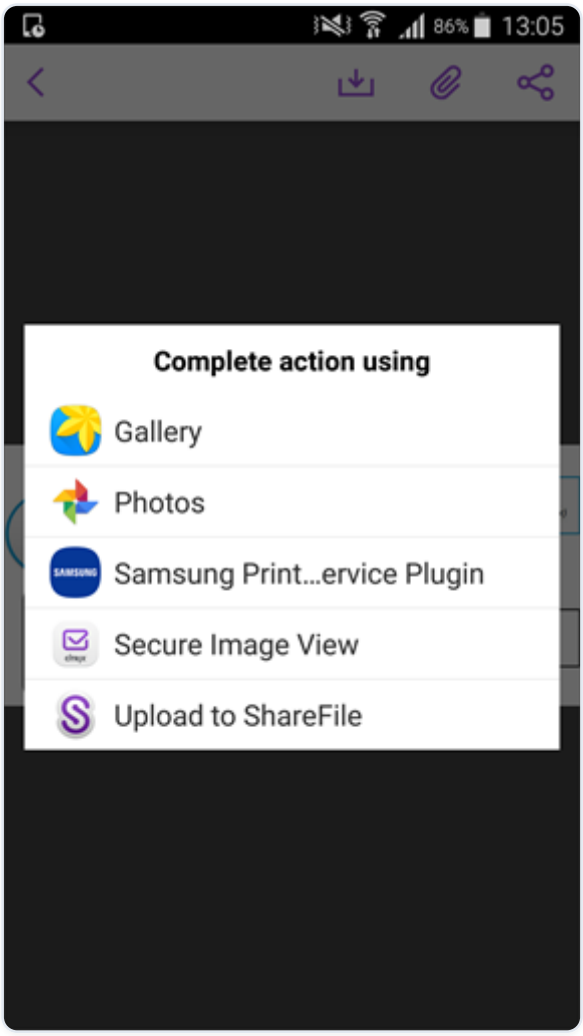
1. 打开附件。
2. 点击页面右上角的**更多**图标，然后点击**打开方式**，以使用其他应用程序打开附件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 从出现的选项中，点击您想要用来打开附件的选项。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



查看附件的源电子邮件或日历事件

1. 点击屏幕右下角的**附件**图标。
2. 点击**离线**。

   离线文件图片(/en-us/mobile-productivity-apps/media/OFFLINE-files.png)
3. 点击附件，然后点击屏幕右上角的**更多**图标。

   信息图标图片(/en-us/mobile-productivity-apps/media/more-icon.png)
4. 源电子邮件出现。

   源电子邮件图片(/en-us/mobile-productivity-apps/media/inapp-preview.png)

将用户名迁移到电子邮件地址 (UPN)

在适用于 iOS 和 Android 的 Secure Mail 中，您可以从基于 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。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

启用此功能后，您无需执行以下任何操作：

- 重新安装 Secure Mail。
- 在 Secure Mail 中删除并添加帐户。
- 更改 Secure Mail 中的用户名。

先决条件

在继续此迁移之前，请确保用户运行的是 Secure Mail 10.7.25 或更高版本。 要使用此功能，您必须启用“尝试在身份验证失败时迁移用户名”策略。

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用户名迁移”策略。
2. 将您的 Exchange 用户帐户迁移到与用户主要 SMTP 电子邮件地址匹配的新 UPN。 这将触发身份验证失败。Secure Mail 会尝试使用主要 SMTP 电子邮件地址进行身份验证。

身份验证成功后，用户帐户将迁移到更新的 UPN。

验证迁移

在 iOS 设备上： 转到**设置**，然后点击帐户以查看详细信息。迁移成功后，主要 SMTP 电子邮件地址将显示在**帐户**屏幕的**用户名**字段中。

在 Android 设备上： 转到**设置**，然后点击帐户以查看详细信息。迁移成功后，主要 SMTP 电子邮件地址将显示在**帐户详细信息**屏幕的**用户名**字段中。

个人通讯组列表

先决条件

- 您的 Exchange Server 上已启用 Exchange Web Services (EWS)。
- Microsoft Exchange Server 版本 10 SP1 或更高版本。

适用于 iOS 和 Android 的 Secure Mail 支持个人联系人组。您可以在 Secure Mail 中查看在 Outlook 桌面客户端上创建的联系人组。您创建的联系人组将显示在 Secure Mail 的“联系人”中。

注意：

您无法在 Secure Mail 中查看嵌套联系人组的成员。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

您可以在撰写电子邮件或创建日历事件时使用个人通讯组列表。如果您已使用 Exchange 创建了个人联系人组（通讯组列表），则可以在 Secure Mail 中查看该列表。

查看个人通讯组列表

1. 在 Secure Mail 中，打开“**联系人**”。
2. 键入联系人组的名称。 该组将显示在搜索结果中。
3. 点击联系人组以查看成员。

   联系人组的图像(/en-us/mobile-productivity-apps/media/iOS-group-expanded.png)

注意

- 您无法在 Secure Mail 中编辑联系人组。

向联系人组撰写邮件

1. 打开 Secure Mail 并点击“**编辑**”浮动操作按钮以撰写邮件。
2. 在“**新建邮件**”屏幕中，在“**收件人:**”字段中键入联系人组的名称。
3. 从显示的联系人列表中，选择联系人组。

   联系人列表的图像(/en-us/mobile-productivity-apps/media/iOS-message-compose-PDL.png)

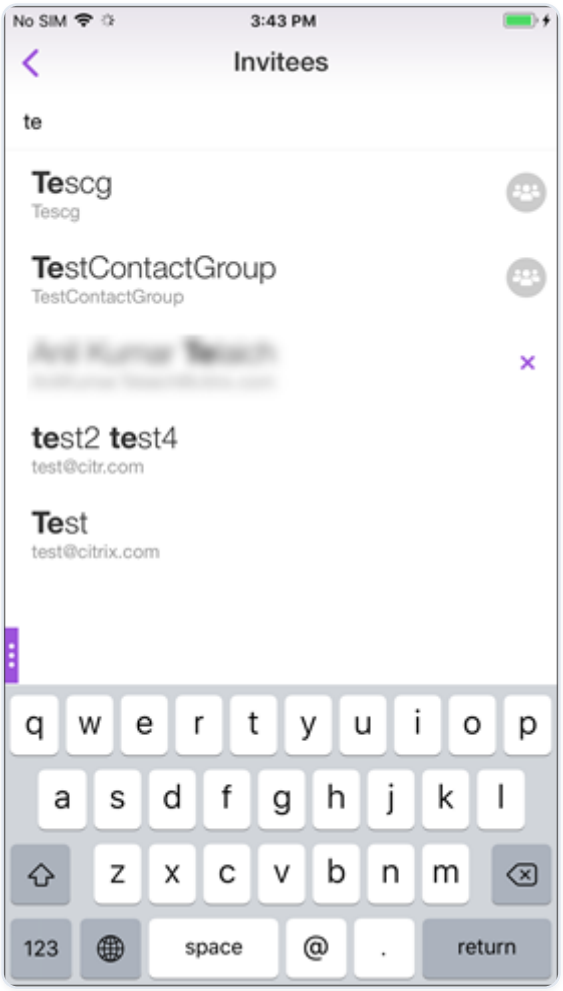
   联系人组由以下图标表示：

   联系人组图标的图像(/en-us/mobile-productivity-apps/media/contact-group-icon.png)

向联系人组发送日历邀请

1. 打开 Secure Mail 并导航到**日历**。
2. 点击 **+** 图标以创建日历事件。
3. 在**新建事件**屏幕中，点击**受邀者**以添加成员。
4. 键入联系人组的名称，将邀请发送给该组。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 从出现的联系人列表中，选择联系人组。

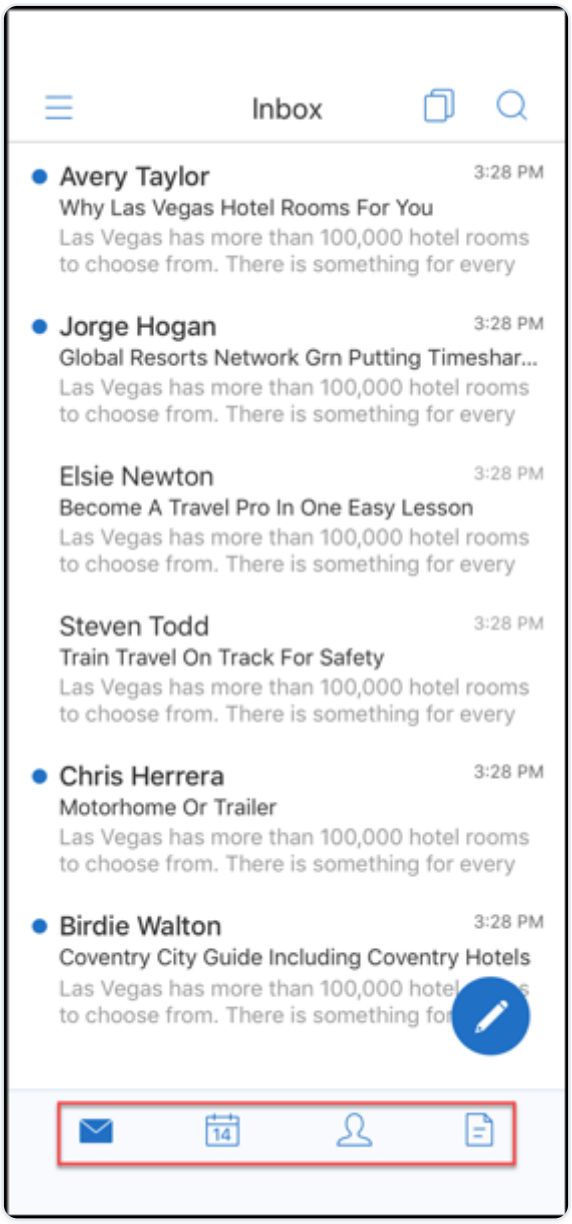
文件夹同步

在适用于 iOS 和 Android 的 Secure Mail 中，您可以点击**同步**图标以刷新所有 Secure Mail 内容。**同步**图标位于 Secure Mail 的侧滑菜单中，例如邮箱、日历、联系人和附件。当您点击**同步**图标时，您已配置为自动刷新的文件夹（例如邮箱、日历、联系人）将得到更新。上次同步的时间戳显示在**同步**图标旁边。

同步您的文件夹

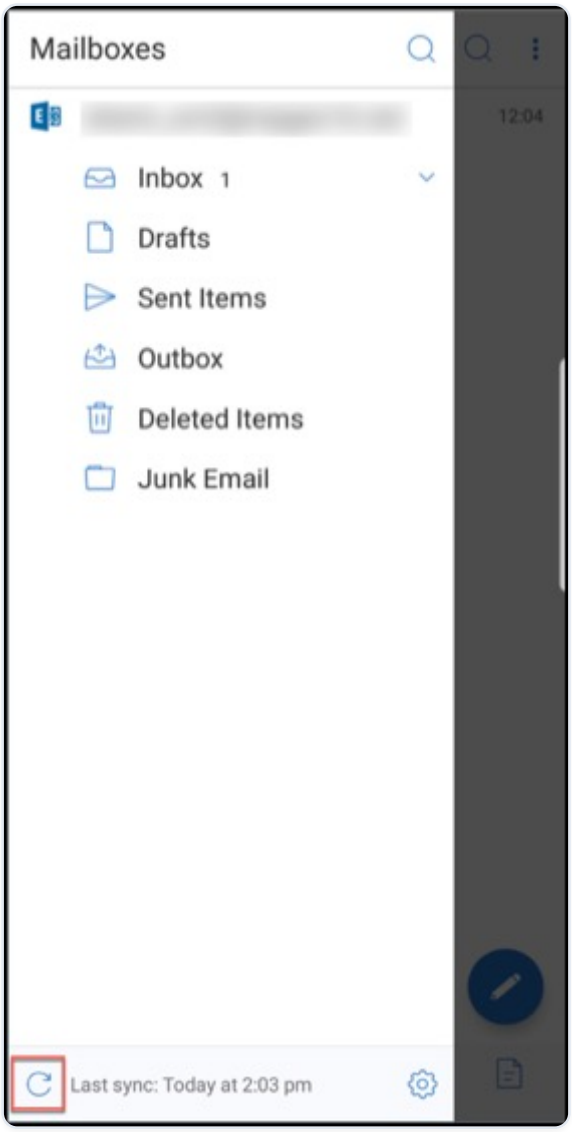
1. 打开 Secure Mail。
2. 从底部选项卡栏中可用的文件夹中，点击您要同步的文件夹。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 点击屏幕左上角的汉堡图标。
4. 点击屏幕左下角的**同步**图标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



同步进度图像(/en-us/mobile-productivity-apps/media/Sync-progress.jpg)

5. 文件夹已同步，您的内容已刷新。时间戳显示在“**同步**”图标旁边。

照片附件改进

在适用于 iOS 和 Android 的 Secure Mail 中，您可以通过点击新的“**图库**”图标轻松附加照片。

将照片附加到电子邮件

1. 打开 Secure Mail。
2. 点击“**撰写**”以创建邮件，或点击“**回复**”浮动操作按钮以回复电子邮件。
3. 点击屏幕右下角“**附件**”图标旁边的“**图库**”图标。

   图库图标图像(/en-us/mobile-productivity-apps/media/photo-attachment-gallery-icon.jpg)
4. 您的图库会显示在屏幕底部，以及“**相机**”和“**最近**”图标。
5. 从图库中导航并选择要附加的图像，或点击“**相机**”图标拍照。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

选择图像选项的图像(/en-us/mobile-productivity-apps/media/select-images.png)

注意：

当您点击“**附件**”图标时，将显示以下选项：

- 文件
- ShareFile（现在是 Citrix Files）
- 来自邮件附件 附件选项的图像(/en-us/mobile-productivity-apps/media/Photo-Attachment-options.jpg)

Secure Mail 在查看电子邮件时呈现嵌入式资源

如果资源存在于您的内部网络中，例如包含内部链接图像 URL 的邮件，Secure Mail 会连接到内部网络以获取内容并进行呈现。

支持现代身份验证

现代身份验证是基于 OAuth 令牌的身份验证，使用用户名和密码。此支持包括对内部和外部 Active Directory Federation Services (AD FS) 或身份提供程序 (IdP) 的 Office 365 的支持。

允许 Secure Web 域 MDX 策略用于 Secure Mail

在 Secure Mail 中，某些外部 URL 必须在原生浏览器而不是 Secure Web 中打开。因此，默认情况下，所有 URL 都在原生浏览器中打开。但是，您可以创建希望在 Secure Web 中打开的特定 URL 列表。为此，您需要在 Citrix Endpoint Management 控制台中配置一个名为“允许的 Secure Web 域”的 MDX 策略。

部署策略后，逗号分隔的 URL 主机域列表将与应用程序通常发送到外部处理程序的任何 URL 的主机名部分进行匹配。通常，您会将此策略配置为 Secure Web 处理的内部域列表。

如果您将策略留空（这是默认设置），则所有 Web 流量都将发送到 Secure Web，直到您明确将 URL 从过滤中排除或以其他方式重定向 URL。要重定向 URL，您需要配置“排除域的 URL 过滤器”MDX 策略。此策略指示必须在原生浏览器中打开的 URL。此策略优先于 Secure Web 域策略。

您可以为 Android 和 iOS 配置这些 MDX 策略。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure Web 域策略的配置示例

以下过程演示了如何提示使用 Secure Mail for Android 的用户在原生 Chrome 浏览器或 Secure Web 中打开 URL。在 iOS 上，这些步骤显示通常在 Safari 浏览器中打开的 URL 会自动在 Secure Web 中打开。

适用于 Android 版 Secure Mail

1. 在“应用交互”策略列表中，在“受限打开方式例外列表”中，输入 *{package=com.android.chrome}* 。
2. 在“应用交互(出站 URL)”策略列表中，在“**允许安全 Web 域**”中，添加内部站点的 DNS 后缀。

对于其他第三方浏览器，请相应地使用以下格式：

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

适用于 iOS 版 Secure Mail

1. 在“应用交互(出站 URL)”策略列表中，在“**允许的 URL**”中，添加 +\^*safari:*。
2. 在“**应用 URL 方案**”中，添加 *safari:*。
3. 在“**允许安全 Web 域**”中，添加内部站点的 DNS 后缀。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure Mail 与 Slack 集成

Citrix Secure Mail and its integration with Slack is not created by, affiliated with, or supported by Slack Technologies, Inc.

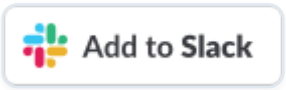
您现在可以在运行 iOS 或 Android 的设备上将电子邮件对话转移到 Slack 应用程序中。

启用此功能后，您可以执行以下操作：

- 从邮件无缝切换到 Slack 对话。
- 与邮件收件人创建 Slack 群组对话。
- 与邮件收件人在 Slack 中创建直接消息。

先决条件

- 对于管理员：
  - 确保您已将 Secure Mail 安装到您的 Slack 工作区。单击下方的 **Add to Slack** 按钮。

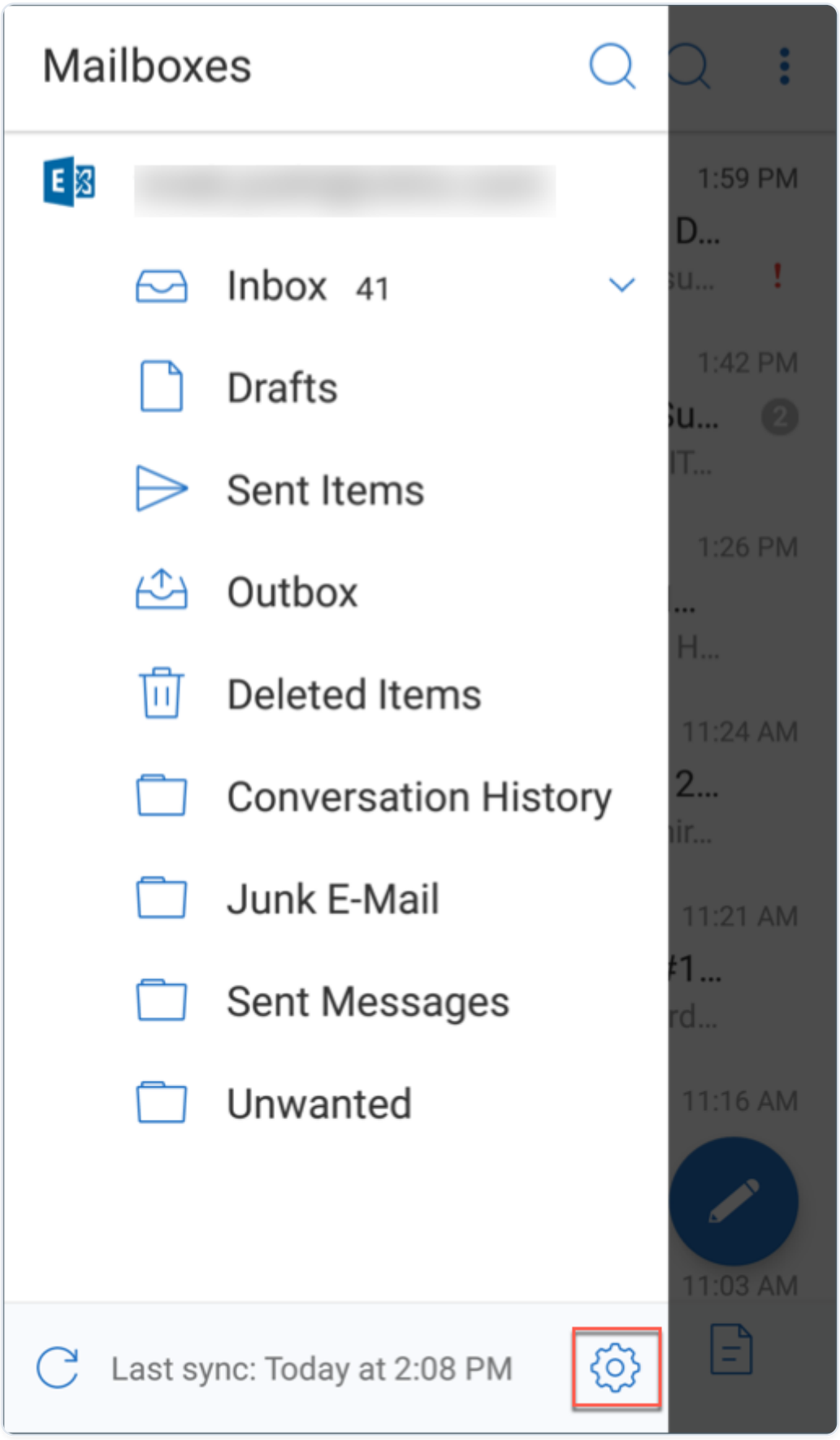
    

  - 确保 **Enable Slack** 策略已设置为 **On**。有关策略详细信息，请参阅：
    - 适用于 iOS 的启用 Slack 策略
    - 适用于 Android 的启用 Slack 策略
- 对于用户：在继续之前，请确保您拥有 Slack 帐户并且您的设备上已安装 Slack 应用程序。

在您的设备上启用此功能

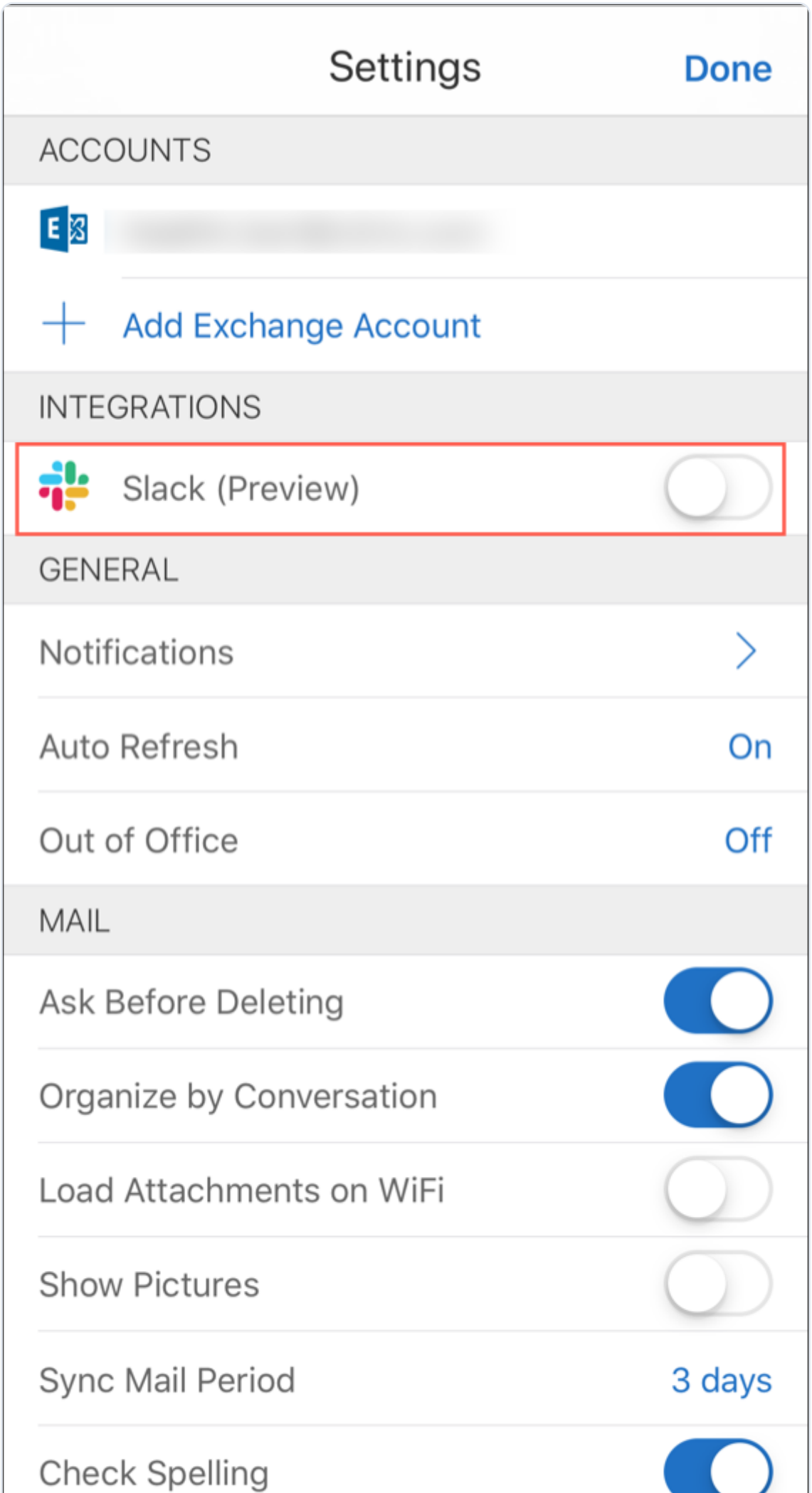
1. 打开 Secure Mail 并点击汉堡图标。
2. 在“**邮箱**”屏幕中，点击屏幕右下角的设置图标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

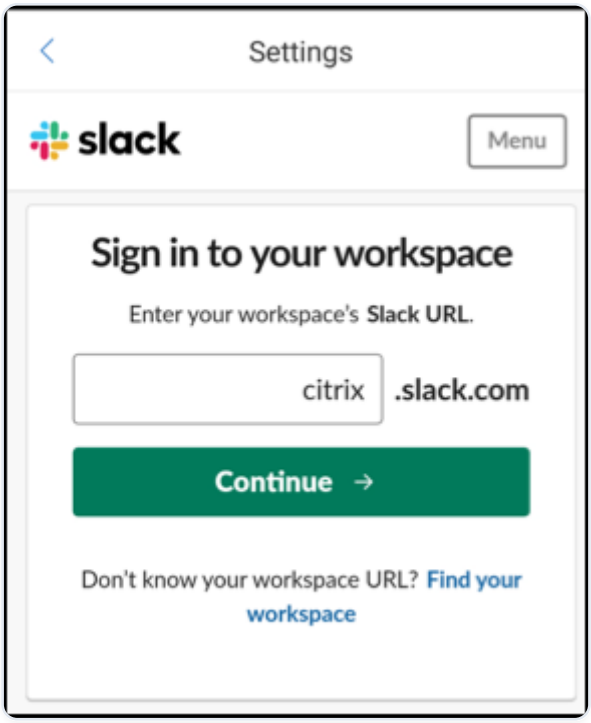


3. 在“**设置**”屏幕中，点击“**集成**”下列出的“**Slack**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

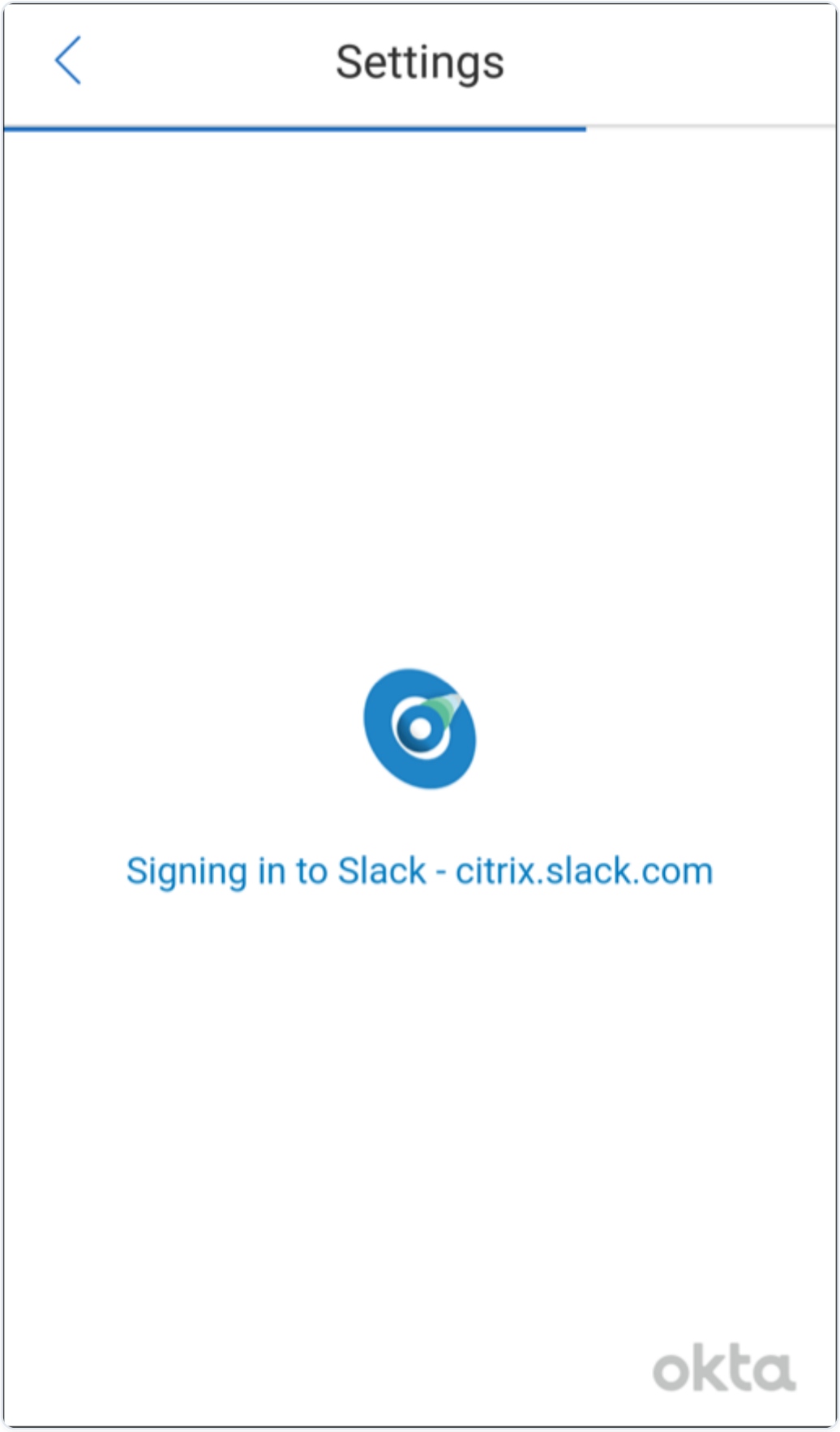

Settings
Done
ACCOUNTS
Add Exchange Account
INTEGRATIONS
Slack (Preview)
GENERAL
Notifications
Auto Refresh
On
Out of Office
Off
MAIL
Ask Before Deleting
Organize by Conversation
Load Attachments on WiFi
Show Pictures
Sync Mail Period
3 days
Check Spelling

4. 提供您的工作区 Slack URL，然后点击“**继续**”。



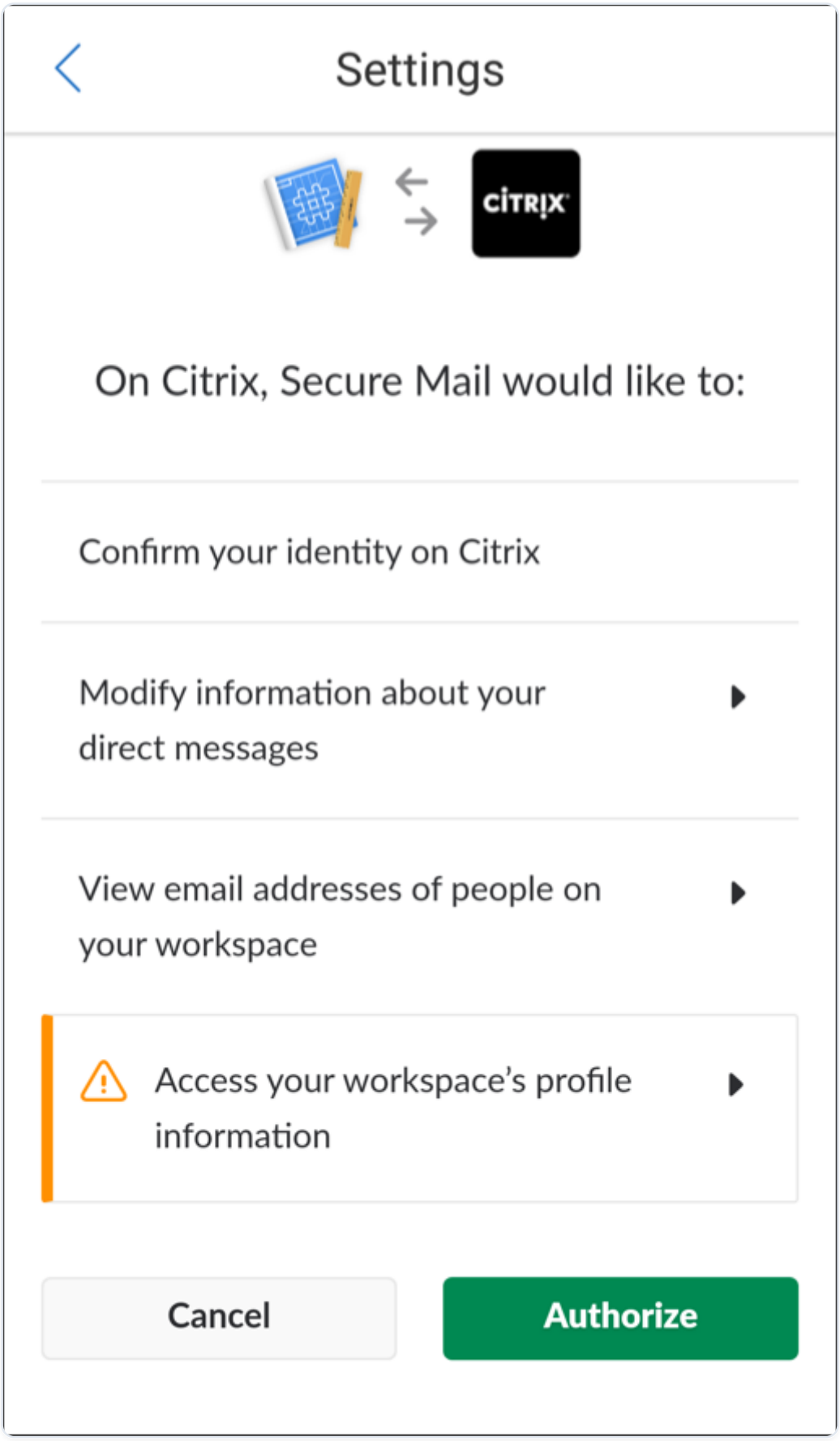
5. 提供您的凭据，然后点击“**登录**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. 当请求授权 Secure Mail 访问信息时，点击“**授权**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



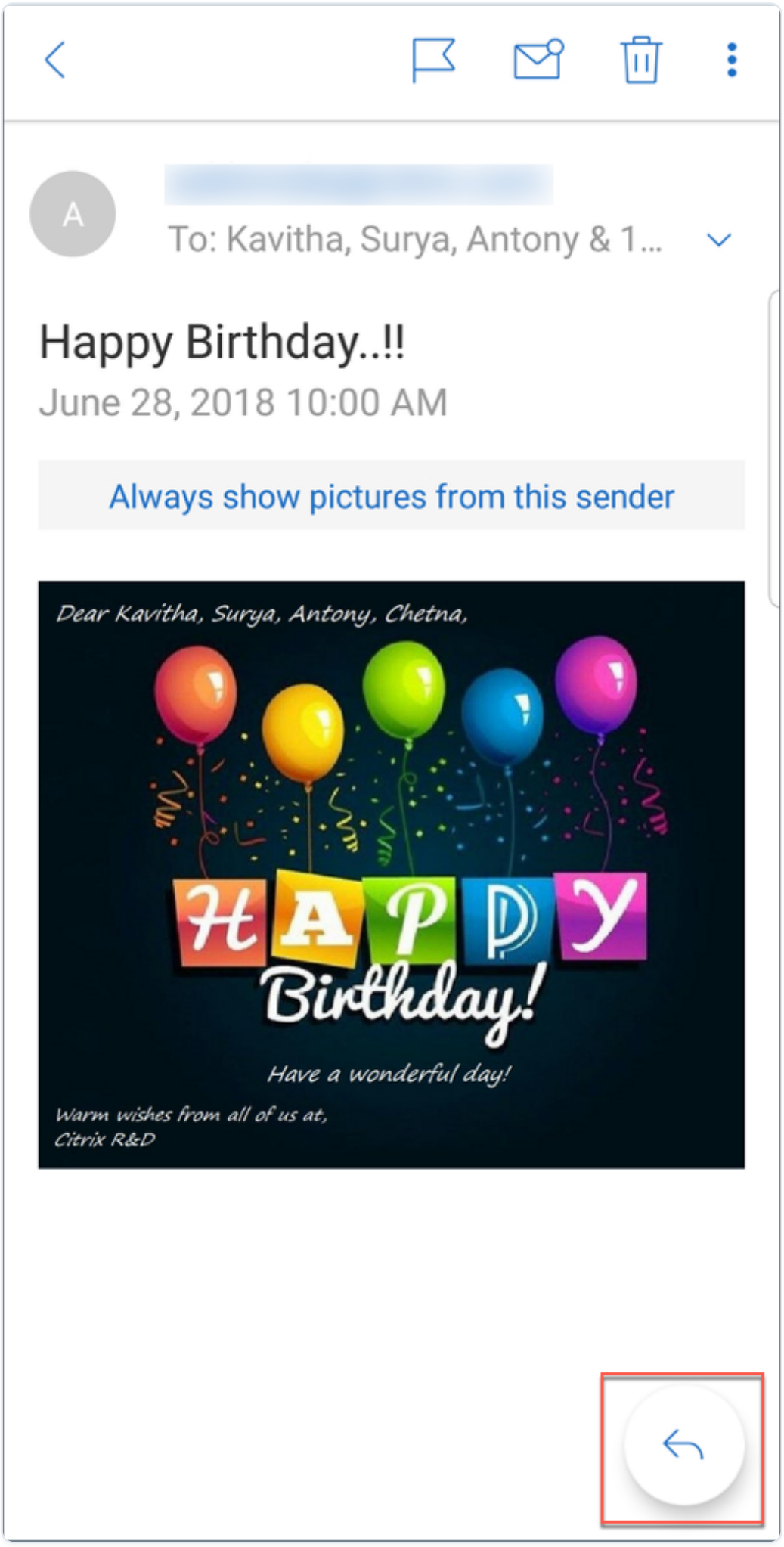
您现在已连接到 Slack。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用此功能

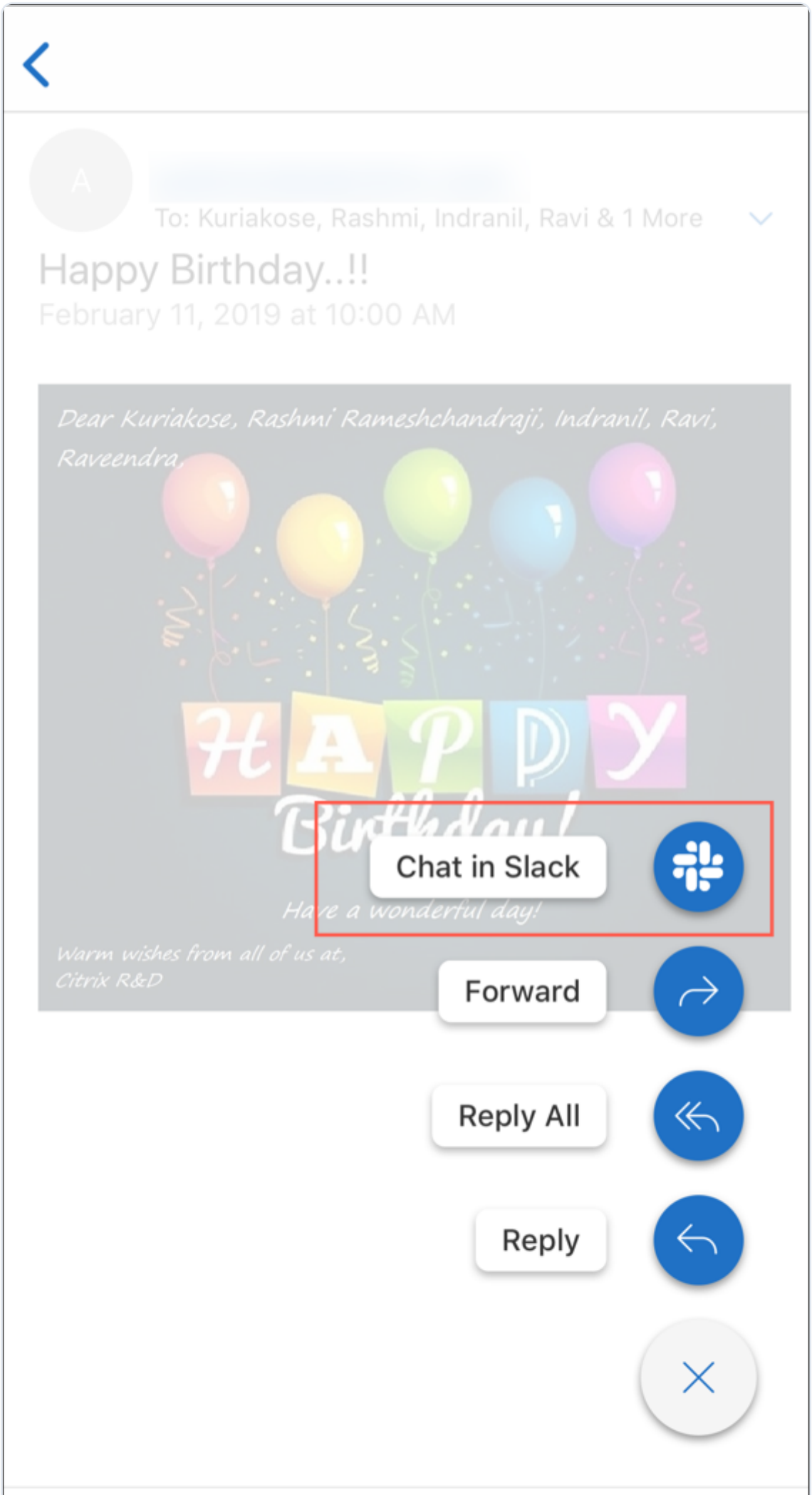
1. 在 Secure Mail 中打开任何电子邮件对话，然后点击浮动操作按钮。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

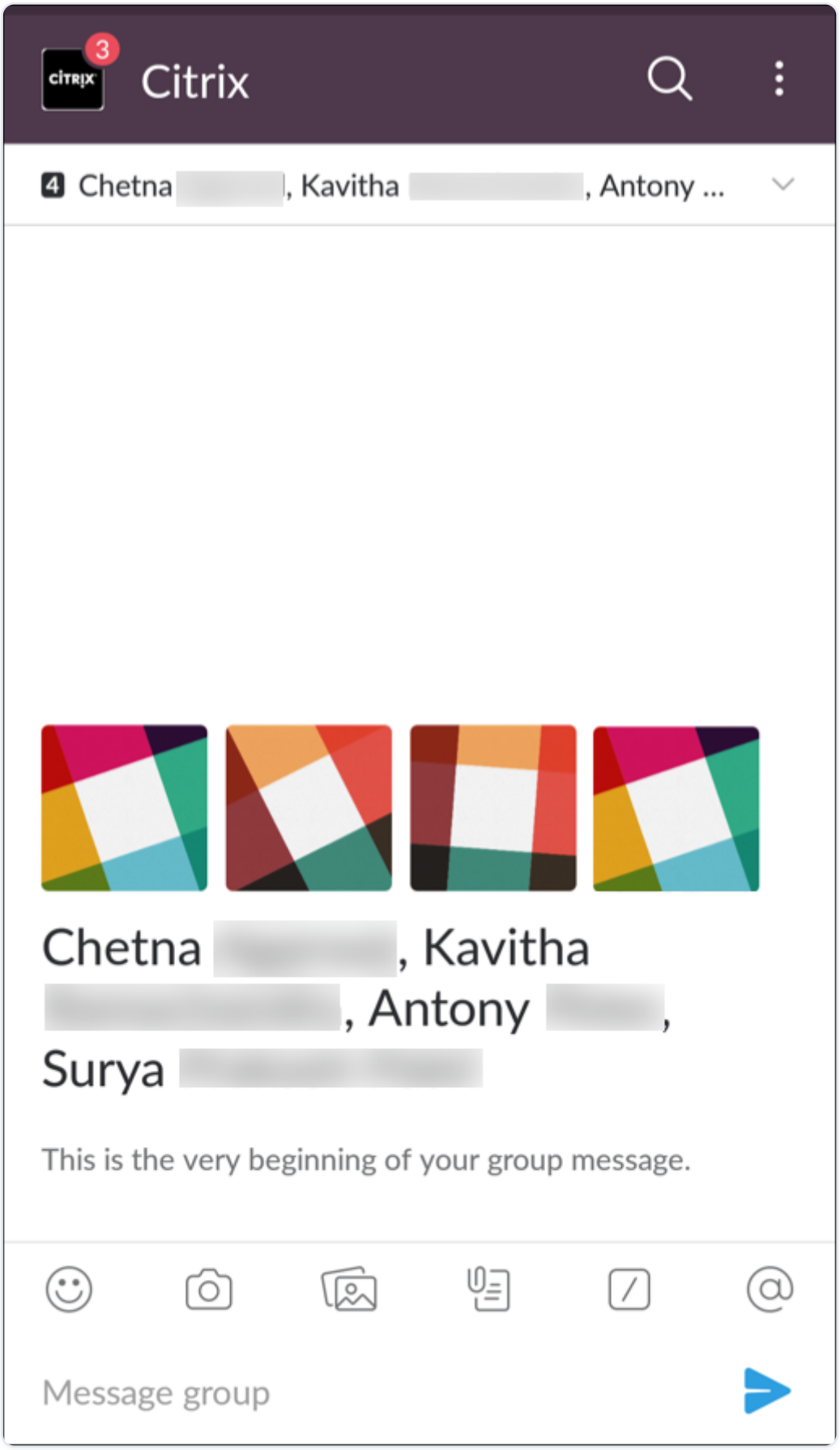

A
To: Kavitha, Surya, Antony & 1...
Happy Birthday..!!
June 28, 2018 10:00 AM
Always show pictures from this sender
Dear Kavitha, Surya, Antony, Chetna,
HAPPY
Birthday!
Have a wonderful day!
Warm wishes from all of us at,
Citrix R&D

2. 从可用选项中，轻点**在 Slack 中聊天**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.


To: Kuriakose, Rashmi, Indranil, Ravi & 1 More
Happy Birthday..!!
February 11, 2019 at 10:00 AM
Dear Kuriakose, Rashmi Rameshchandraji, Indranil, Ravi, Raveendra,
Have a wonderful day!
Warm wishes from all of us at,
Citrix R&D
Chat in Slack
Forward
Reply All
Reply

3. 对话将切换到 Slack，并包含您电子邮件中的收件人。



请注意以下事项：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 在运行适用于 iOS 或 Android 的 Secure Mail 的设备上，您可以创建最多可包含您电子邮件中的八个收件人的 Slack 对话。如果您的电子邮件中有八个以上的收件人，默认情况下，Secure Mail 会选择电子邮件对话中出现的前八个收件人。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

通知和同步

本文讨论 Secure Mail 的通知和电子邮件同步功能及配置。

适用于 iOS 的 Secure Mail 后台应用刷新

如果 Secure Mail for iOS 配置为通过 iOS 后台应用刷新（而非 APN）提供通知，则 Secure Mail 电子邮件刷新按以下方式工作：

- 当用户从“**设置**”菜单在设备上启用“**后台应用刷新**”且 Secure Mail 在后台运行时，邮件会与服务器同步。同步频率取决于多种因素。
- 如果用户禁用“**后台应用刷新**”，则应用在后台运行时永远不会收到电子邮件。
- 当用户将 Secure Mail 移到后台时，应用会在暂停之前继续运行一段时间。
- 在前台运行时，无论“**后台应用刷新**”设置如何，Secure Mail 都会显示实时电子邮件活动。

安全邮件和 ActiveSync

Secure Mail 通过 ActiveSync 消息传递协议与 Exchange Server 同步。此功能使用户能够实时访问其 Outlook 邮件、联系人、日历事件、自动生成的邮箱和用户创建的文件夹。

注意：

ActiveSync 不支持 Exchange 公用文件夹的同步。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，请执行以下步骤：

iOS

1. 转到“**设置 > 自动刷新**”。
2. 将**自动刷新**设置为**开**。
3. 点击**开**。将显示所有邮箱的列表。
4. 点击要同步的文件夹。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安卓

1. 转到邮箱列表。
2. 点击要同步的邮箱。
3. 点击右下角的更多图标。
4. 点击**同步选项**。
5. 在**检查频率**下，选择您希望文件夹同步的频率。

在 Secure Mail 中导出联系人

Secure Mail 用户可以持续将其联系人与手机通讯录同步，一次性将单个联系人导出到手机通讯录，或将联系人作为 vCard 附件共享。

要启用这些功能，请在 Endpoint Management 控制台中将 Secure Mail 的“导出联系人”策略设置为**开**。

当策略设置为**开**时，Secure Mail 中将启用以下选项：

- “设置”中的**与本地联系人同步**
- 导出单个联系人
- 将联系人共享为 vCard 附件

当**导出联系人策略**设置为**关闭**时，这些选项不会显示在应用程序中。

启用此策略后，要将联系人从邮件服务器持续同步到手机通讯录，用户需要将**与本地联系人同步**设置为**开启**。只要**与本地联系人同步**处于**开启**状态，Exchange 或 Secure Mail 中对联系人的任何更新都会触发本地联系人的更新。

由于 Android 的限制，如果任何 Exchange 或 Hotmail 帐户已设置为与本地联系人同步，Secure Mail 将无法同步联系人。

在 iOS 上，Secure Mail 联系人可以导出并与手机联系人同步。即使设备上设置了 Hotmail 或 Exchange，也可以导出和同步联系人。您可以通过 Endpoint Management 中 Secure Mail 的“覆盖本机联系人检查”策略配置此功能。此策略确定 Secure Mail 是否覆盖对本机“通讯录”应用中配置的 Exchange/Hotmail 帐户联系人的检查。如果设置为**开启**，即使本机“通讯录”应用配置了 Exchange/Hotmail 帐户，应用程序也会将联系人同步到设备。如果设置为**关闭**，应用程序将继续阻止联系人同步。默认设置为**开启**。

限制：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

启用**与本地联系人同步**后，仅同步默认联系人文件夹。您可能拥有的任何子文件夹都不会包含在同步的联系人中。

Secure Mail 通知

下表列出了 Secure Mail 在前台或后台运行时，支持的移动设备如何处理通知。

SECURE MAIL 在前台或后台运行时：	IOS 的通知处理方式	ANDROID 的通知处理方式
前台	Secure Mail 维护持久的 ActiveSync 连接以同步电子邮件和日历活动。	Secure Mail 维护持久的 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 后台应用刷新功能接收通知，如果已配置，则通过 APN 接收通知。	Secure Mail 保持持久的 ActiveSync 连接。

有关配置详细信息，请参阅适用于 iOS 的 Secure Mail 推送通知。

适用于 Secure Mail 的推送通知

适用于 iOS 的 Secure Mail 和适用于 Android 的 Secure Mail 可以在应用程序在后台运行或关闭时接收有关电子邮件和日历活动的通知。适用于 iOS 的 Secure Mail 支持通过 Apple Push Notification service (APNs) 提供的远程推送通知。适用于 Android 的 Secure Mail 支持通过 Firebase Cloud Messaging service (FCM) 提供的通知。

推送通知的工作原理

为了向 iOS 和 Android 提供推送通知，Citrix® 在 Amazon Web Services (AWS) 上托管侦听器服务以执行以下功能：

- 侦听当收件箱有活动时由 Exchange Server 发送的 Exchange Web Services (EWS) 推送通知。Exchange 不会向 Citrix 服务发送任何邮件内容。

  Citrix 服务不存储任何个人身份信息。相反，设备令牌和订阅 ID 用于识别 Secure Mail 中要更新的特定设备和收件箱文件夹。
- 向 iOS 设备上的 Secure Mail 发送仅包含徽章计数的 APNs 通知。
- 向 Android 设备上的 Secure Mail 发送 FCM 通知。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix 侦听器服务不影响邮件数据流量，邮件数据流量继续通过 ActiveSync 在用户设备和 Exchange Server 之间流动。侦听器服务配置为高可用性和灾难恢复，在以下三个区域可用：

- 美洲
- 欧洲、中东和非洲 (EMEA)
- 亚太地区 (APAC)

适用于推送通知的系统要求

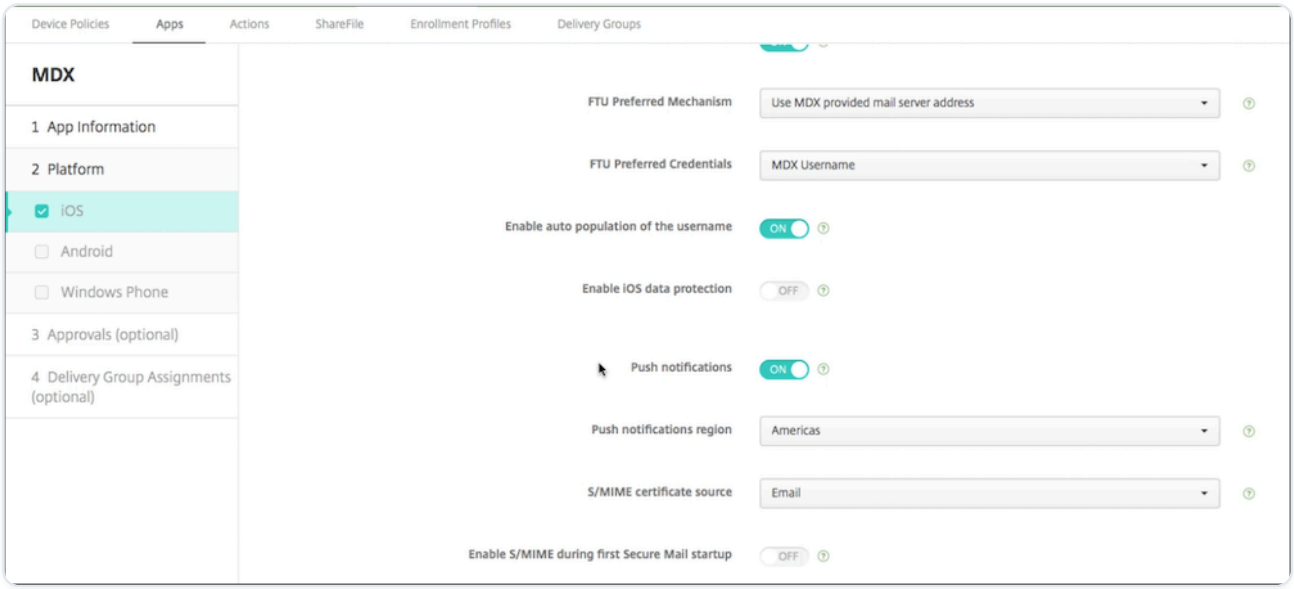
如果您的 Citrix Gateway 配置包含 Secure Ticket Authority (STA) 且分流隧道已关闭，则 Citrix Gateway 必须允许流量（当从 Secure Mail 隧道传输时）流向以下 Citrix 侦听器服务 URL：

区域	URL	IP 地址
美洲	`https://us-east-1.pushreg.xm.citrix.com`	52.7.65.6; 52.7.147.0
欧洲、中东和非洲	`https://eu-west-1.pushreg.xm.citrix.com`	54.154.200.233; 54.154.204.192
亚太地区	`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

要为应用商店分发设置 Secure Mail 的 Apple 推送通知或 FCM，请在 Endpoint Management 控制台中，将“推送通知”设置为 **ON**，然后选择您的区域。下图显示了 iOS 的设置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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区域不同的区域，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。

在 Endpoint Management 中 Android 推送通知设置的图片(/en-us/mobile-productivity-apps/media/android-push-notification.jpg)

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

Exchange 服务器配置

允许从您的防火墙到 Citrix 侦听器服务 URL 的出站 SSL（通过端口 443），适用于您的 Exchange Server 所在的区域。例如：

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

如果在 Exchange Web Services (EWS) 和 Citrix 侦听器设备之间有代理服务器，您可以执行以下操作之一。

- 通过代理将 EWS 流量发送到侦听器设备。
- 绕过代理，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，请按如下方式配置 ClientAccess\\exchweb\\ews 文件夹中的 EWS web.config 文件。

```
&lt;configuration>

&lt;system.net>

&lt;defaultProxy>

&lt;proxy usesystemdefault="true" bypassonlocal="true" />

&lt;/defaultProxy>

&lt;/system.net>

&lt;/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，您必须手动将 `system.net` 部分添加到 web.config 文件中。否则，本文中描述的配置应适用于 Exchange 2013。有关故障排除，请联系您的 Exchange 管理员。

要绕过代理服务器，请配置旁路列表以允许 Exchange 连接到 Citrix 侦听器服务。

当 Secure Hub 使用基于证书的身份验证注册时，您还必须为 Exchange Server 配置基于证书的身份验证。有关详细信息，请参阅Endpoint Management 高级概念文章。

Citrix 网关配置

尽管 Exchange Server 需要允许流量流向侦听器服务，但 Citrix ADC 必须允许流量流向注册服务。通过这种方式，设备可以连接以注册推送通知。

如果您的 EWS 和 ActiveSync 服务器不同，请配置您的 Citrix ADC 流量策略以允许 EWS 流量。有关将 Citrix Endpoint Management 与 Citrix Gateway 集成的更多信息，请参阅与 Citrix Gateway 和 Citrix ADC 集成部分。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

故障排除

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

Secure Mail 推送通知常见问题解答

Android 何时向 Secure Mail 传送通知?

在 Android 中，通知始终会传送到 Secure Mail。

FCM 如何影响显示在锁定屏幕上的电子邮件通知?

显示在设备锁定屏幕上的新邮件通知是根据 Secure Mail 同步到设备的数据生成的。重要的是，此信息并非来自侦听器服务。

要显示新邮件通知，Secure Mail 必须能够从 Exchange 同步数据，以便 Secure Mail 拥有可用于创建通知的信息。

收到新邮件时，将显示“**您有新邮件**”FCM 通知。电子邮件在后台同步完成后，新邮件将显示在 Secure Mail 中。

APNs 如何影响显示在锁定屏幕上的电子邮件通知?

显示在设备锁定屏幕上的新邮件通知是根据 Secure Mail 同步到设备的数据生成的。重要的是，此信息并非来自侦听器服务。

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 拥有可用于创建通知的信息。

如果 APNs 通知未在后台传送到 Secure Mail，则 Secure Mail 不会检测到这些通知，因此不会同步新数据。由于 Secure Mail 没有可用的新数据，因此即使未传送 APNs 通知，设备锁定屏幕上也不会生成电子邮件通知。

后台应用刷新如何影响 Secure Mail 和 APNs?

如果用户关闭后台应用刷新，则会出现以下情况：

- Secure Mail 不会收到通知，即使 Secure Mail 处于后台应用中。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

仅当富推送通知被禁用时，才会出现此情况。有关富推送通知的详细信息，请参阅适用于 iOS 的 Secure Mail 富推送通知。

- Secure Mail 不会用新电子邮件通知更新锁屏。

禁用后台应用刷新对 Secure Mail 的行为有重大影响。如前所述，基于 APNs 的徽章更新仍然会发生，但在这种模式下，没有电子邮件会同步到设备。

低电量模式如何影响 Secure Mail 和 APNs?

系统在低电量模式下对 Secure Mail 的行为与禁用后台应用刷新时的行为相同。在低电量模式下，设备不会唤醒应用进行定期刷新，也不会向后台应用发送通知。因此，副作用与上面“后台应用刷新”部分中列出的相同。请注意，在低电量模式下，基于 APNs 通知，徽章更新仍然会发生。

还有哪些其他问题可能导致 FCM 驱动的后台同步失败?

各种问题都可能导致 FCM 驱动的同步请求失败，包括：

- 无效的 STA 票证。
- 当 Secure Mail 在休眠模式下被唤醒时，应用有 10 秒钟的时间从服务器同步所有数据。

如果发生上述任何情况，Secure Mail 将无法同步数据。因此，锁屏通知不会显示。

还有哪些其他问题可能导致 APNs 驱动的后台同步失败?

许多问题都可能导致 APNs 驱动的同步请求失败，包括：

- 无效的 STA 票证。
- 网络连接缓慢。当 Secure Mail 在后台被唤醒时，应用有 30 秒钟的时间从服务器同步所有数据。
- 如果启用了数据保护策略，并且 Secure Mail 被 APNs 通知唤醒，当设备锁定时，Secure Mail 无法访问数据存储，并且不会发生同步。请注意，这仅适用于系统尝试冷启动 Secure Mail 的情况。如果用户在解锁设备后已在某个时间点启动了 Secure Mail，即使设备已锁定，APNs 驱动的同步也会成功。

如果发生上述任何情况，Secure Mail 将无法同步数据，因此无法显示锁屏通知。

当通知未送达或未使用 APNs 时，Secure Mail 还会如何生成锁屏通知?

如果 APNs 被禁用，Secure Mail 仍会通过 iOS 的定期后台应用刷新事件唤醒，前提是后台应用刷新已启用且低电量模式已关闭。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在这些唤醒事件期间，Secure Mail 会从 Exchange Server 同步新电子邮件。然后，这些新电子邮件可用于在锁屏上生成电子邮件通知。因此，即使 APNs 通知未送达或 APNs 被禁用，Secure Mail 仍可在后台同步数据。

重要的是要注意，这比使用 APNs 和 APNs 通知送达 Secure Mail 时实时性要差。当 iOS 将 APNs 通知路由到 Secure Mail 时，应用程序会立即从服务器同步数据，并且锁屏通知会显示为实时。

如果需要后台应用刷新唤醒，锁屏通知不会实时发生。在这种情况下，Secure Mail 会以 iOS 完全决定的频率唤醒。因此，以下两种情况之间可能会经过一段时间：

- 电子邮件到达用户在 Exchange 上的收件箱时。
- Secure Mail 同步该邮件并生成锁屏通知时。

另请注意，即使在使用 APNs 时，Secure Mail 也会收到这些定期唤醒。在所有后台应用刷新唤醒 Secure Mail 的情况下，Secure Mail 都会尝试从 Exchange 同步数据。

Secure Mail 与其他在锁屏上显示内容的应用程序有何不同?

一个重要的区别（可能导致混淆）是 Secure Mail 并非总是在锁屏上实时显示新电子邮件。此行为与 Gmail、Microsoft Outlook 和其他应用程序不同。造成这种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才能通过 Exchange 进行身份验证。需要凭据才能获取电子邮件内容。还需要凭据才能将此电子邮件内容通过 Citrix 侦听器服务传递到 Apple APNs 服务。Citrix 处理 APNs 通知的方法不需要 Citrix 侦听器服务获取或存储用户密码。侦听器服务无权访问用户的邮箱或密码。

关于原生 iOS 邮件应用程序的说明：iOS 允许其自己的邮件应用程序与邮件服务器保持持久连接，这确保了通知始终送达。原生邮件之外的第三方应用程序不允许拥有此功能。

Gmail 应用程序行为： Google 拥有并控制 Gmail 应用程序和 Gmail 服务器。此行为意味着 Google 可以读取邮件内容并将该邮件内容包含在 APNs 通知负载中。当 iOS 从 Gmail 收到此 APNs 通知时，iOS 会执行以下操作：

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

这是一个关键区别：是 iOS（而不是 Gmail 应用程序）根据负载中包含的数据显示锁屏通知。实际上，iOS 可能永远不会唤醒 Gmail 应用程序，这与通知到达时 iOS 可能不会唤醒 Secure Mail 的方式类似。但是，由于负载包含邮件片段，iOS 可以显示锁屏通知，而无需将任何邮件数据同步到设备。

在 Secure Mail 中，这种情况有所不同。Secure Mail 必须首先从 Exchange 同步邮件数据，然后应用才能显示锁屏通知。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Outlook for iOS 应用行为： Microsoft 控制 Outlook for iOS。但是，用户所属的组织控制着获取数据的 Exchange 服务器。尽管有此设置，Outlook 仍可以根据 Microsoft 在 APNs 通知中提供的数据显示锁屏通知。原因是 Outlook for iOS 使用了一种模型，其中 Microsoft 存储用户凭据。然后，Microsoft 直接从其云服务访问用户的邮箱，并确定是否存在新邮件。

如果有新邮件可用，Microsoft 云服务会生成一个包含新邮件数据的 APNs 通知。此模型与 Gmail 模型的操作方式类似。在 Gmail 模型中，iOS 只是获取数据并根据该数据生成锁屏通知。Outlook iOS 应用不参与此过程。

关于 Outlook for iOS 的重要安全说明： Outlook for iOS 的方法存在明显的安全隐患。组织需要信任 Microsoft 来管理其用户的密码。这种信任允许 Microsoft 访问用户的邮箱，这会带来安全风险。

有关推送通知的更多管理员特定常见问题解答，请参阅此支持知识中心文章。有关更多用户特定常见问题解答，请参阅此支持知识中心文章。

适用于 iOS 版 Secure Mail 的富推送通知

适用于 iOS 版 Secure Mail 支持富推送通知。富通知可确保即使 Secure Mail 未在后台运行，您也能收到收件箱的锁屏通知。此功能支持基于密码的身份验证和基于客户端的身份验证设置。

注意：

由于为支持此功能而进行的架构更改，VIP 邮件通知功能不再可用。

要启用富推送通知功能，请确保满足以下先决条件：

- 在 Endpoint Management 控制台中，将“推送通知”设置为 **ON**。
- 网络访问策略设置为 **Unrestricted** 或 **Tunnel to internal network**。如果您的网络访问策略设置为 **Tunnel to internal network**，请确保在后台网络服务策略中配置了 Exchange Web Services (EWS) 主机。如果 EWS 和 ActiveSync 主机相同，请确保在后台网络服务策略中配置了 ActiveSync 主机。
- “控制锁屏通知”策略设置为 **Allow** 或 **Email sender or event title**。
- 导航到 **Secure Mail > 设置 > 通知**，然后启用 **邮件通知**。

如果您运行以下任何设置，则不支持此功能：

- 使用 Microsoft Office 365 的现代身份验证
- 通过 Endpoint Management 与 Microsoft InTune/EMS 集成管理的应用程序
- 使用派生凭据注册的设备

© 1997–2026 Citrix Systems, Inc. All rights reserved.

推送通知在 Secure Mail iOS 中的工作方式

Secure Mail 接收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**：当 APNs 将远程通知推送到 iOS Secure Mail 时，Secure Mail 会更新所有标记为自动刷新的文件夹。

  注意：

  默认情况下，收件箱、日历和联系人文件夹被标记为自动刷新。用户可以从 **Secure Mail** > **设置** > **自动刷新** 中选择任何其他邮件文件夹进行自动刷新。

- Secure Mail 图标仅显示 Exchange 收件箱文件夹中未读和新邮件的总数。用户在台式机或笔记本电脑上阅读电子邮件后，Secure Mail 会更新该图标。
- 在安装或升级期间，适用于 iOS 的 Secure Mail 会提示用户允许推送通知。用户也可以稍后通过 iOS 设置允许推送通知。

不支持富推送通知时的推送通知行为

对于 iOS 富推送通知功能不支持的配置，Secure Mail 仍会提供同步周期内未读收件箱电子邮件的数量。如果**控制锁定屏幕通知策略**为**开启**，则在 iOS 唤醒 Secure Mail 执行同步后，推送通知会显示在锁定的设备屏幕上。

Secure Mail iOS 推送通知常见问题

iOS 何时向 Secure Mail 传递通知？

启用富推送通知功能后，iOS 会向 Secure Mail 传递远程通知。即使应用程序未在后台运行或处于低功耗模式，这些通知也会发生。

注意：

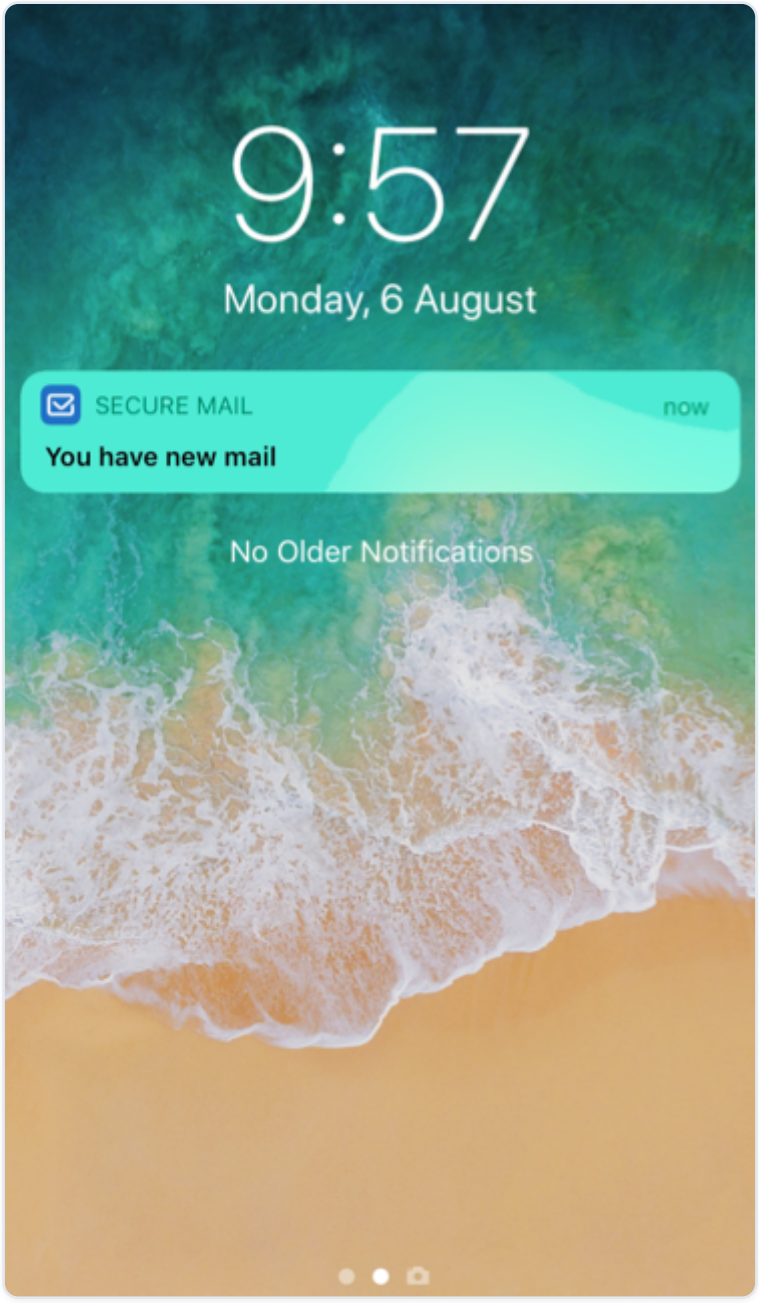
当未启用富推送通知时，如果 Secure Mail 未处于活动状态，则可能不会向 Secure Mail 传递通知：这种情况的发生有多种原因，例如以下原因：

- 如果设备处于低功耗模式且 Secure Mail 在后台运行：这是通知未送达的最常见情况。
- 如果 Secure Mail 的**后台应用刷新**为**关闭**，并且 Secure Mail 在后台运行：请注意，用户控制此设置。
- 如果设备网络连接不佳：这种情况取决于 iOS 设备。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iOS 设备上出现“您有新邮件”通知的原因

当 Secure Mail 未在指定时间内从 Exchange Web Services (EWS) 收到响应时，iOS 设备上会出现“您有新邮件”通知。获取邮件详细信息所需的时间为 30 秒。

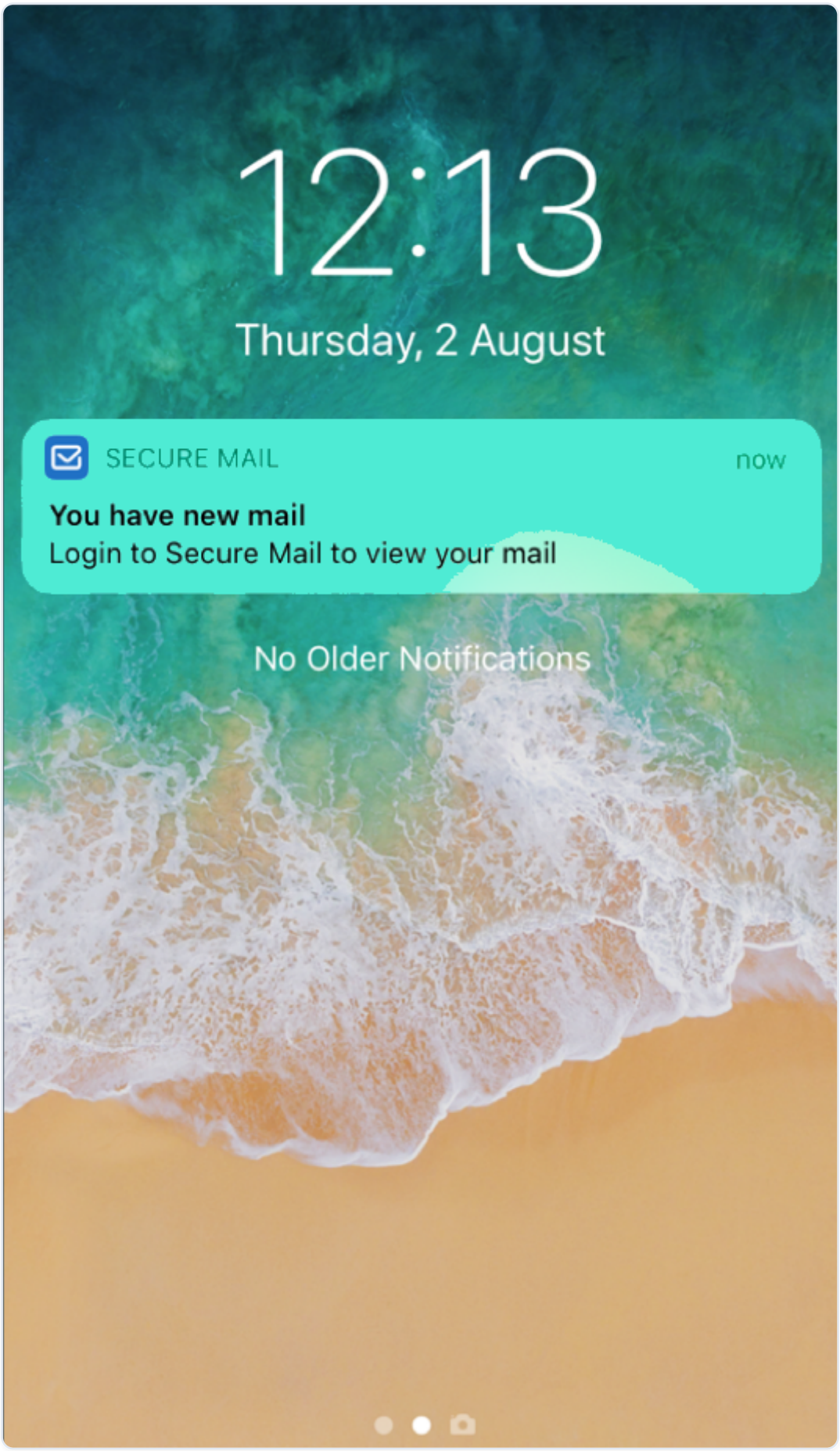


由于 Wi-Fi 或数据连接不佳，您的设备上也可能会出现此行为。

除了 EWS 响应延迟之外，Secure Mail 还在以下情况下显示“您有新邮件”通知：

- 当 Secure Mail 无法从安全容器读取所需信息时。此情况通常发生在您重新启动设备后但在解锁设备之前。
- 当 Secure Mail 无法连接到 Citrix Gateway 或 EWS 或无法与其建立安全通道时。
- 当您的凭据已过期或您已修改凭据但 Secure Mail 中未更新时。下图显示了在此情况下通知的显示方式。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 当 Secure Mail 从 Exchange Server 收到对其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会显示在您设备的通知中心。这些通知根据通知失败的类型显示。

以下通知消息根据不同的失败场景显示如下：

- **Secure Mail 无法连接到您的组织网络**。当 Secure Mail 无法与 Citrix Gateway 建立 SOCKS5 连接时，将显示此通知。
- **Secure Mail 无法连接到您的组织网络。请联系您的管理员。** 当 Citrix Gateway 无法访问时，将显示此通知。请确保您的 Citrix ADC 配置正确且可从外部网络访问。
- **Secure Mail 无法安全连接到您的组织网络。请联系您的管理员**。当 Secure Mail 无法与 Citrix Gateway 建立 SSL 连接时，将显示此通知。请确保您的 SSL 证书有效。
- **Secure Mail 无法安全连接到您的邮件服务器。请联系您的管理员**。当 Secure Mail 无法与 Exchange Server 建立 SSL 连接时，将显示此通知。请确保您的 Exchange Server 上的 SSL 证书有效。如果您希望应用程序在证书无效的情况下仍连接到 Exchange Server，请确保您已启用“接受所有 SSL 证书”MDX 策略。
- **由于邮件服务器错误，Secure Mail 无法获取邮件。请联系您的管理员**。当 Secure Mail 无法解析来自 Exchange Server 的 EWS 响应时，将显示此通知。
- **由于请求超时，Secure Mail 无法获取邮件**。当 Secure Mail 未能在 30 秒内收到服务器响应时，将显示此通知。此通知可能由于您设备上的数据或 Wi-Fi 连接不良而出现。请等待几分钟后重试。
- **无法获取邮件。请打开 Secure Mail**。当 Secure Mail 无法从安全容器读取您的凭据时，将显示此通知。当您的设备已重新启动但未解锁时，可能会出现此通知。解锁您的设备以自动允许 Secure Mail 访问安全容器。如果您仍然收到此通知，请打开 Secure Mail 以自动更新安全容器中的凭据。

Secure Mail 与其他移动生产力应用和 Citrix Files 的交互性

Secure Mail 与其他移动生产力应用和 Citrix Files 的交互性使用户能够无缝地访问、编辑、共享和保存文档，而无需离开您的组织策略设置的安全环境。例如，在 Secure Mail 中点击链接会在 Secure Web 中打开该站点。用户可以使用适用于 Endpoint Management 的 Citrix QuickEdit™ 打开和编辑附件。附件将下载到用户的适用于 Endpoint Management 的 Citrix Files 空间中。

有关每个平台的 Secure Mail 功能的完整列表，请参阅按平台列出的功能。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

- 适用于 XenMobile 的 Citrix Files 已于 July 1, 2023 达到 EOL。有关详细信息，请参阅EOL和已弃用应用

测试和故障排除 Secure Mail

当 Secure Mail 无法正常工作时，通常是连接问题导致的。本文介绍了如何避免连接问题。如果出现问题，本文将介绍如何排查这些问题。

测试 ActiveSync 连接、用户身份验证和 APNs 配置

您可以使用 Endpoint Management Analyzer 执行 Secure Mail 自动发现服务检查。它会指导您下载 Endpoint Management Exchange ActiveSync 测试应用程序。邮件测试选项会检查与邮件服务器的基本连接设置。该工具还可以帮助您排查 ActiveSync 服务器，以确保它们已准备好部署到 Endpoint Management 环境中。

Analyzer 中的邮件测试选项会验证以下内容：

- iOS 和 Android 设备与 Microsoft Exchange 或 IBM Traveler 服务器的连接。
- 用户身份验证。
- iOS 的推送通知配置，包括 Exchange Server、Exchange Web Services (EWS)、Citrix Gateway、APNs 证书和 Secure Mail。有关配置推送通知的信息，请参阅 适用于 iOS 的 Secure Mail 推送通知。

该工具提供了纠正问题的全面建议列表。

注意：

邮件测试应用程序 MailTest.ipa 已弃用。请改用 Endpoint Management Analyzer 中的相同功能。

测试先决条件

- 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”**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用 Secure Mail 日志排查连接问题

要获取 Secure Mail 日志，请执行以下操作。

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

   将打开一封发送给您组织帮助台的电子邮件。
3. 在主题行和正文中填写一些描述您问题的内容。
4. 选择问题发生的时间。
5. 仅当您的支持团队指示您更改时才更改日志设置。
6. 单击 **发送**。

   完成的消息将打开，并附带压缩的日志文件。
7. 再次单击 **发送**。

   发送的 zip 文件包含以下日志：

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

应用程序信息日志包含有关设备和应用程序的信息。验证所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 版本是否为最新且兼容。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 (安卓)

VPN 配置日志仅适用于 Secure Hub。检查 Citrix ADC 版本 `ServerBuildVersion` 以确保使用的是最新的 Citrix ADC 版本。按如下方式检查 `SplitDNS` 和 `SplitTunnel` 设置：

- 如果“拆分 DNS”设置为**远程**、**本地**或**两者**，请验证您是否通过 DNS 正确解析了邮件服务器 FQDN。（拆分 DNS 适用于 Android 上的 Secure Hub。）
- 如果“拆分隧道”设置为**开**，请确保邮件服务器被列为后端可访问的 Internet 应用程序之一。
- CtxLog_AppPolicies.xml (iOS), Policy.xml (安卓和 Windows Phone)

策略日志提供您获取日志时应用于 Secure Mail 的所有 MDX 策略的值。对于连接问题，请验证 `<BackgroundServices>` 和 `<BackgroundServicesGateway>` 策略的值。

- 诊断日志（在诊断文件夹中）

© 1997–2026 Citrix Systems, Inc. All rights reserved.

对于 Secure Mail 的初始配置，最常见的问题是“您的公司网络当前不可用。”要使用诊断日志排查连接问题，请执行以下操作。

诊断日志中的关键列是 Timestamp、Message Class 和 Message。当 Secure Mail 中出现错误消息时，请记下时间，以便您可以在 **Timestamp** 列中快速找到相关的日志条目。

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

- AG 策略拦截 FQDN:443 以进行 STA 隧道连接
- 已建立到 (null):443 的新建 TCP 代理连接

要确定从 Citrix Gateway 到 Endpoint Management 的连接是否成功（从而可以验证 STA 票证），请执行以下操作：转到 Secure Hub 诊断日志，查看 Message Class 下的 INFO (4) 条目，以查找设备注册时间。以下消息表示 Secure Hub 从 Endpoint Management 获取了 STA 票证：

- 正在获取 STA 票证。
- 已获取 STA 票证响应。
- STA 票证 – 成功获取应用程序的 STA 票证 -- Secure Mail。

注意：

> 在注册期间，Secure Hub 会向 Endpoint Management 发送 STA 票证请求。Endpoint Management 会将 STA 票证发送到设备，票证将在设备上存储并添加到 Endpoint Management STA 票证列表中。

要确定 Endpoint Management 是否向用户颁发了 STA 票证，请检查支持包中包含的 UserAuditLogFile.log。它会列出每张票证的颁发时间、用户名、用户设备和结果。例如：

时间： 2015-06-30T 12:26:34.771-0700

用户： user2

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

结果： 成功为应用“Secure Mail”的用户“user2”生成了 STA 票证

要检查 Citrix Gateway 到邮件服务器的通信：检查 DNS 和网络是否配置正确。为此，请使用 Secure Web 访问 Outlook Web Access (OWA)。与 Secure Mail 类似，Secure Web 可以使用微型 VPN 隧道建立与 Citrix Gateway 的连接。Secure Web 充当应用程序正在访问的内部或外部资源的代理。通常，尤其是在 Exchange 环境中，OWA 托管在邮件服务器上。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要测试配置，请打开 Secure Web 并输入 OWA 页面的 FQDN。该请求采用与 Citrix Gateway 和邮件服务器之间通信相同的路由和 DNS 解析。如果 OWA 页面打开，则表示 Citrix Gateway 正在与邮件服务器通信。

如果上述检查表明通信成功，则说明问题不在您的 Citrix 设置中。相反，问题出在 Exchange 或 Traveler 服务器上。

您可以为 Exchange 或 Traveler 服务器管理员收集信息。首先，通过在 Secure Mail 诊断日志中搜索“Error”一词来检查 Exchange 或 Traveler 服务器上的 HTTP 问题。如果错误包含 HTTP 代码并且您有多个 Exchange 或 Traveler 服务器，请调查每个服务器。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 的日志是 C:\inetpub\LogFiles\W3SVC1\U_EX.log。Traveler 的日志是 IBM_TECHNICAL_SUPPORT>HTTHR.log。

如何从设备获取适用于 iOS 的 Secure Mail 崩溃日志

1. 在 iOS 设备上，转至 **设置** > **隐私** > **分析** > **分析数据**。
2. 在**数据**列表中，单击应用程序名称和相关时间戳。日志随即显示。

电子邮件、联系人或日历问题疑难解答

您可以对 Secure Mail 问题进行故障排除，例如电子邮件或多封电子邮件卡在草稿中、联系人丢失或日历项目不同步。要解决这些问题，请使用 Exchange ActiveSync 邮箱日志。日志显示设备发送的传入请求以及邮件服务器发出的传出响应。

无限同步最佳实践

当用户将其邮件同步周期设置为**所有**时，他们将拥有无限同步。在无限同步的情况下，假设用户管理其邮箱大小，即收件箱和所有同步的子文件夹。以下是为获得最佳性能需要记住的几点。

1. 如果邮箱大小超过 18,000 封邮件或总大小超过 600 MB，邮件同步可能会变慢。
2. 不建议在无限同步的情况下启用**在 WiFi 上加载附件**。此选项可能导致设备上的邮件大小迅速膨胀。
3. 为防止无限同步成为用户的选项，请将**最大同步间隔**应用程序策略设置为**所有**以外的值。
4. 不建议将**所有**设置为用户的**默认同步间隔**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.