管理 SAML 单点登录

SAML 单点登录概述

使用 SAML 单点登录 (SSO) 登录到其中一个应用程序后，访问一组定义的 Cisco 应用程序。SAML 描述了受信任的业务合作伙伴之间安全相关信息的交换。它是服务提供程序（例如 Cisco Unified Communications Manager）用来验证用户的一种验证协议。利用 SAML，安全验证信息可在身份提供程序 (IdP) 与服务提供程序之间交换。该功能提供安全机制来跨各种应用程序使用通用凭证和相关信息。

SAML SSO 在部署过程中通过在 IdP 和服务提供程序之间交换元数据和证书建立信任圈 (CoT)。服务提供程序信任 IdP 的用户信息，提供对各种服务或应用的访问权限。

客户端根据 IdP 进行验证，IdP 则向客户端授予断言。客户端将断言提供给服务提供程序。由于建立了 CoT，服务提供程序信任断言，并授予访问客户端的权限。

Cisco Jabber iOS 版本基于证书的 SSO 验证的选择加入控制

此版本的 Cisco Unified Communications Manager 引入了选择加入配置选项，以使用身份提供程序 (IdP) 控制 Cisco Jabber iOS 版本 SSO 登录行为。使用此选项以允许 Cisco Jabber 在受控的移动设备管理 (MDM) 部署中使用 IdP 执行基于证书的验证。

您可以在 Cisco Unified Communications Manager 中通过 **iOS 的 SSO 登录行为** (SSO Login Behavior for iOS) 企业参数配置选择加入控制。

注释 在更改此参数的默认值之前，请参阅位于 http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/tsd-products-support-series-home.html 的 Cisco Jabber 功能支持和文档，以确保 Cisco Jabber iOS 版本支持 SSO 登录行为和基于证书的验证。

要启用此功能，请参阅为 Cisco Jabber iOS 版本配置 SSO 登录行为，第 4 页程序。

SAML 单点登录先决条件

- 为 Cisco Unified Communications Manager 群集配置了 DNS
- 一台身份提供程序 (IdP) 服务器
- 一台受 IdP 服务器信任且受您的系统支持的 LDAP 服务器

以下使用 SAML 2.0 的 Idp 针对 SAML SSO 功能进行了测试：

- OpenAM 10.0.1
- Microsoft® Active Directory® Federation Services 2.0 (AD FS 2.0)
- PingFederate® 6.10.0.4
- F5 BIP-IP 11.6.0

这些第三方应用程序必须满足以下配置要求：

- 必须在 IdP 上配置必需属性 “uid”。此属性必须与 Cisco Unified Communications Manager 中用于 LDAP 同步用户 ID 匹配。
- 必须同步所有参与 SAML SSO 的实体的时钟。有关同步时钟的信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》中的 “NTP 设置”，该文档位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html。

管理 SAML 单点登录

启用 SAML 单点登录

注释 直到验证同步代理测试成功后，才能启用 SAML SSO。

开始之前

- 确保最终用户数据与 Unified Communications Manager 数据库同步。有关详细信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html。
- 验证 Cisco Unified CM IM and Presence Service Cisco 同步代理服务是否已成功完成数据同步。通过选择 **Cisco Unified CM IM and Presence 管理** > **诊断** > **系统故障诊断程序**，检查此测试的状态。如果数据同步已成功完成，“验证同步代理是否已同步相关数据（例如设备、用户、许可信息）”测试显示“测试通过”结果。
- 确保至少一个 LDAP 同步用户添加到“标准 CCM 超级用户”组以允许访问 Cisco Unified CM 管理。有关详细信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html。
- 要配置 IdP 与服务器之间的信任关系，必须从 IdP 获取信任元数据文件，并将该文件导入到所有服务器中。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**系统** > **SAML 单点登录**。

步骤 2 单击**启用 SAML SSO**。

步骤 3 看到通知您所有服务器连接都将重新启动的警告消息后，单击**继续**。

步骤 4 单击**浏览**查找并上传 IdP 元数据文件。

步骤 5 单击**导入 IdP 元数据**。

步骤 6 单击**下一步**。

步骤 7 单击**下载信任元数据文件集**将服务器元数据下载到系统。

步骤 8 将服务器元数据上传到 IdP 服务器。

步骤 9 单击**下一步**继续操作。

步骤 10 从有效管理员 ID 列表中选择具有管理权限的 LDAP 同步用户。

步骤 11 单击**运行测试**。

步骤 12 输入有效的用户名和密码。

步骤 13 看到成功消息之后，关闭浏览器窗口。

步骤 14 单击**完成**，等待 1 到 2 分钟，让 Web 应用程序重新启动。

为 Cisco Jabber iOS 版本配置 SSO 登录行为

过程

步骤 1 在 Cisco Unified CM 管理中，选择**系统** > **企业参数**。

步骤 2 要配置选择加入控制，在 SSO 配置部分，为 **iOS 的 SSO 登录行为** (SSO Login Behavior for iOS) 参数选择**使用本机浏览器**选项：

注释 **iOS 的 SSO 登录行为** (SSO Login Behavior for iOS) 参数包括以下选项：

- **使用嵌入式浏览器** — 如果启用此选项，Cisco Jabber 会使用嵌入式浏览器进行 SSO 验证。使用此选项可允许版本 9 之前的 iOS 设备使用 SSO 而无需交叉启动进入本机 Apple Safari 浏览器。默认情况下会启用此选项。
- **使用本机浏览器** — 如果启用此选项，Cisco Jabber 会在 iOS 设备上使用 Apple Safari 框架，在 MDM 部署中使用身份提供程序 (IdP) 执行基于证书的验证。

  注释 除了在受控的 MDM 部署中，不建议配置此选项，因为使用本机浏览器不如使用嵌入式浏览器安全。

步骤 3 单击**保存**。

升级后在 WebDialer 上启用 SAML 单点登录

执行这些任务以在升级后在 Cisco WebDialer 上重新激活 SAML 单点登录。如果在启用 SAML 单点登录之前 Cisco WebDialer 已激活，则默认情况下 SAML 单点登录未在 Cisco WebDialer 上启用。

过程

	命令或操作	目的
步骤 1	禁用 Cisco WebDialer 服务，第 4 页	如果 Cisco WebDialer Web 服务已激活，请将其停用。
步骤 2	禁用 SAML 单点登录，第 5 页	如果 SAML 单点登录已启用，请将其禁用。
步骤 3	激活 Cisco WebDialer 服务，第 5 页	
步骤 4	启用 SAML 单点登录，第 2 页	

禁用 Cisco WebDialer 服务

如果 Cisco WebDialer Web 服务已激活，请将其停用。

过程

步骤 1 从 Cisco Unified 功能配置中，选择**工具** > **服务激活**。

步骤 2 从**服务器**下拉列表中，选择列出的 Cisco Unified Communications Manager 服务器。

步骤 3 从 **CTI 服务**中，取消选中 **Cisco WebDialer Web 服务**复选框。

步骤 4 单击**保存**。

下一步做什么

禁用 SAML 单点登录，第 5 页

禁用 SAML 单点登录

如果 SAML 单点登录已启用，请将其禁用。

开始之前

禁用 Cisco WebDialer 服务，第 4 页

过程

从 CLI，运行命令 **utils sso disable**。

下一步做什么

激活 Cisco WebDialer 服务，第 5 页

激活 Cisco WebDialer 服务

开始之前

禁用 SAML 单点登录，第 5 页

过程

步骤 1 从 Cisco Unified 功能配置中，选择 **工具** > **服务激活**。

步骤 2 从**服务器**下拉列表中，选择列出的 Unified Communications Manager 服务器。

步骤 3 从 **CTI 服务**中，选中 **Cisco WebDialer Web 服务**复选框。

步骤 4 单击**保存**。

步骤 5 从 Cisco Unified 功能配置中，选择 **工具** > **控制中心 - 功能服务**，以确认 CTI Manager 服务为活动状态且处于启动模式。

要使 WebDialer 正常运行，CTI Manager 服务必须为活动状态且处于启动模式。

下一步做什么

启用 SAML 单点登录，第 2 页

访问恢复 URL

使用恢复 URL 以绕过 SAML 单点登录并登录到“Cisco Unified Communications Manager 管理”和“Cisco Unified CM IM and Presence Service”界面进行故障诊断。例如，在更改服务器的域或主机名之前启用恢复 URL。登录恢复 URL 便于更新服务器元数据。

开始之前

- 只有具有管理权限的应用程序用户才能访问恢复 URL。
- 如果启用 SAML SSO，默认情况下启用恢复 URL。您可以从 CLI 启用或禁用恢复 URL。有关用于启用和禁用恢复 URL 的 CLI 命令的详细信息，请参阅《*Cisco Unified Communications* 解决方案的命令行界面指南》。

过程

在浏览器中，输入 `https://hostname:8443/ssosp/local/login`。

在域或主机名更改之后更新服务器元数据

域或主机名更改之后，SAML 单点登录将不起作用，直到您执行此程序。

注释 如果即使在执行此程序之后，仍然无法登录 **SAML 单点登录**窗口，请清除浏览器缓存，然后再次尝试登录。

开始之前

如果禁用恢复 URL，则它不会出现以让您绕过单点登录链接。要启用恢复 URL，请登录 CLI 并执行以下命令：**utils sso recovery-url enable**。

过程

步骤 1 在您的 Web 浏览器的地址栏中，输入以下 URL：

https://<Unified CM-server-name>

其中 <Unified CM-server-name> 是服务器的主机名或 IP 地址。

步骤 2 单击**恢复 URL 以绕过单点登录 (SSO)**。

步骤 3 输入具有管理员角色的应用程序用户的凭证，然后单击**登录**。

步骤 4 在 Cisco Unified CM 管理中，选择**系统** > **SAML 单点登录**。

步骤 5 单击**导出元数据**，下载服务器元数据。

步骤 6 将服务器元数据文件上传到 IdP。

步骤 7 单击**运行测试**。

步骤 8 输入有效的用户 ID 和密码。

步骤 9 看到此成功消息之后，关闭浏览器窗口。

删除服务器后更新服务器元数据

从群集中删除服务器后导出 Unified CM 元数据时，我们建议您在 IdP 上导入此文件，以确保索引值的匹配项介于两者之间。

开始之前

注释 如果禁用恢复 URL，则它不会出现以让您绕过单点登录链接。要启用恢复 URL，请登录 CLI 并执行以下命令：**utils sso recovery-url enable**。

过程

步骤 1 在您的 Web 浏览器的地址栏中，输入以下 URL：

https://<Unified CM-server-name>

其中 <Unified CM-server-name> 是服务器的主机名或 IP 地址。

步骤 2 单击**恢复 URL 以绕过单点登录 (SSO)**。

步骤 3 输入具有管理员角色的应用程序用户的凭证，然后单击**登录**。

步骤 4 在 Cisco Unified CM 管理中，选择 **系统** > **SAML 单点登录**。

步骤 5 单击**导出元数据**，下载服务器元数据。

步骤 6 将服务器元数据文件上传到 IdP。

步骤 7 单击**运行测试**。

步骤 8 输入有效的用户 ID 和密码。

步骤 9 看到此成功消息之后，关闭浏览器窗口。

手动配置服务器元数据

要在身份提供程序中为多个 UC 应用程序配置一个连接，您必须手动配置服务器元数据，同时配置身份提供程序与服务提供程序之间的信任圈。有关配置信任圈的详细信息，请参阅 IdP 产品文档。

一般 URL 语法如下：

```
https://<SP FQDN>:8443/ssosp/saml/SSO/alias/<SP FQDN>
```

过程

要手动配置服务器元数据，请使用 Assertion Customer Service (ACS) URL。

示例：

ACS URL 示例：`<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://cucm.ucsso.cisco.com:8443/ssosp/saml/SSO/alias/cucm.ucsso.cisco.com" index="0"/>`