配置单点登录

- 关于 SAML SSO 解决方案， 第 1 页
- SAML SSO 配置任务流程， 第 2 页

关于 SAML SSO 解决方案

重要事项 如果 Cisco Jabber 部署为采用 Cisco Webex Meeting Server，则 Unified Communications Manager 和 Webex Meeting Server 必须位于相同的域中。

SAML 是基于 XML 的开放标准数据格式，可让管理员在登录到其中一个应用后能够无缝访问定义的一组 Cisco 协作应用。 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 Unified Communications Manager）用来验证用户的一种验证协议。 SAML 实现了身份提供程序 (IdP) 和服务提供程序之间安全身份验证信息的交换。

SAML SSO 使用 SAML 2.0 协议为 Cisco 协作解决方案提供跨域和跨产品单点登录。 SAML 2.0 实现了跨 Cisco 应用程序的 SSO 并实现了 Cisco 应用程序和 IdP 之间联盟。 SAML 2.0 允许 Cisco 管理用户访问安全的 web 域，以便在维护高安全性级别的同时在 IdP 与服务提供程序之间交换用户身份验证和授权数据。 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 管理员访问授权基于在 Cisco 协作应用程序上本地配置的基于角色的访问控制 (RBAC)。

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

重要事项 服务提供程序不再参与身份验证。 SAML 2.0 将身份验证从服务提供程序委托给 Idp。

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，并授予访问权限给客户端。

SAML SSO 配置任务流程

完成这些任务以为 SAML SSO 配置 Unified Communications Manager。

开始之前

SAML SSO 配置要求您在配置 Unified Communications Manager 的同时配置身份提供程序 (IdP) 。有关 IdP 特定的配置示例，请参阅：

- Active Directory Federation Services
- Okta
- Open Access Manager
- PingFederate

注释 上述链接仅提供一些示例。有关正式文档，请参阅您的 IdP 文档。

过程

	命令或操作	目的
步骤 1	从 Cisco Unified Communications Manager 导出 UC 元数据， 第 3 页	要创建信任关系，必须在 Unified Communications Manager 和 IdP 之间交换元数据文件。
步骤 2	在身份提供程序 (IdP) 上配置 SAML SSO	完成以下任务： • 上传从 Unified Communications Manager 导出的UC元数据文件，以便完成信任圈关系。 • 在 IdP 上配置 SAML SSO • 导出 IdP 元数据文件。此文件将导入到 Unified Communications Manager
步骤 3	在 Cisco Unified Communications Manager 中启用 SAML SSO	导入 IdP 元数据并在 Unified Communications Manager 中启用 SAML SSO。
步骤 4	重新启动 Cisco Tomcat 服务， 第 5 页	在启用 SSO 之前和之后，您必须在启用 SSO 的所有群集节点上重新启动 Cisco Tomcat 服务。
步骤 5	验证 SAML SSO 配置， 第 6 页	验证 SAML SSO 已成功配置。

从 Cisco Unified Communications Manager 导出 UC 元数据

使用此程序可从服务提供程序 (Unified Communications Manager) 导出 UC 元数据文件。 元数据文件将导入到身份提供程序 (IdP)，以便建立信任圈关系。

过程

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

步骤 2 从 **SAML 单点登录**窗口中，选择 **SSO 模式**字段中的一个选项：

- **群集范围**—群集的单个 SAML 协议。

  注释　如果选择此选项，请确保群集中所有节点的Tomcat服务器具有相同的证书，即多服务器 SAN 证书。

- **每个节点** —每个节点都有单独的 SAML 协议。

步骤 3 从 **SAML 单点登录**窗口中，为**证书**字段选择一个选项 。

- **使用系统生成的自签证书**
- **使用 Tomcat 证书**

步骤 4 单击**导出所有元数据**以导出元数据文件。

注释　如果您在步骤3中选择**群集范围**选项，将会为群集显示一个元数据XML文件以供下载。但是，如果您选择**每个节点**选项，则会为群集的每个节点节点显示一个元数据 XML 文件以供下载。

下一步做什么

完成 IdP 上的以下任务：

- 上传从 Unified Communications Manager 导出的 UC 元数据文件
- 在 IdP 上配置 SAML SSO
- 导出 IdP 元数据文件。 此文件将导入到 Unified Communications Manager，以便完成信任圈关系。

在 Cisco Unified Communications Manager 中启用 SAML SSO

使用此程序在服务提供程序 (Unified Communications Manager) 上启用 SAML SSO。 此程序包括将 IdP 元数据导入到 Unified Communications Manager 服务器中。

重要事项 Cisco 建议您在启用或禁用 SAML SSO 后重新启动 Cisco Tomcat 服务。

注释 在启用或禁用 SAML SSO 之后，Cisco CallManager 管理、Unified CM IM and Presence 管理、Cisco CallManager 功能配置和 Unified IM and Presence 功能配置等服务重新启动。

开始之前

在完成此程序之前，请确保以下各项：

- 您需要从 IdP 导出的元数据文件。
- 确保最终用户数据与 Unified Communications Manager 数据库同步
- 验证 Unified Communications Manager IM and Presence Cisco 同步座席服务已成功完成数据同步。通过选择**诊断** > **系统故障诊断程序**，在 **Cisco Unified CM IM and Presence 管理**中检查此测试的状态。如果数据同步已成功完成，“验证同步座席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
- 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 管理”。有关同步最终用户数据以及将 LDAP 同步用户添加到组中的详细信息，请参阅《Unified Communications Manager 管理指南》中的“系统设置”和“最终用户设置”部分。

过程

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

步骤 2 单击**启用 SAML SSO**，然后单击**继续**。

警告消息会通知您所有服务器连接都将重新启动。

步骤 3 如果您配置了**群集范围**的 SSO 模式，则单击**测试多服务器 tomcat 证书**按钮。 否则，您可以跳过此步骤。

步骤 4 单击**下一步**。

此时将显示一个可让您导入 IdP 元数据的对话框。 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。

步骤 5 导入您从 IdP 导出的元数据文件：

a) **浏览**以查找并选择导出的 IdP 元数据文件。
b) 单击**导入 IdP 元数据**。
c) 单击**下一步**。
d) 在**下载服务器元数据并在 IdP 上安装**屏幕上，单击**下一步**

注释　仅当IdP元数据文件至少在群集中的一个节点上成功导入时，**下一步**按键才处于启用状态。

步骤 6 测试连接并完成配置：

a) 在**最终用户配置**窗口中，从**权限信息**列表框中选择已 LDAP 同步并拥有“标准 CCM 超级用户”权限的用户。

b) 单击**运行测试**。

IdP 登录窗口将会显示。

注释　直到测试成功后，才能启用 SAML SSO。

c) 输入有效的用户名和密码。

在成功验证之后，将会显示以下消息：

`SSO 测试成功`

看到此消息之后关闭浏览器窗口。

如果身份验证失败或用时超过 60 秒，IdP 登录窗口上会显示“登录失败”消息。“SAML 单点登录”窗口上显示以下消息：

`SSO 元数据测试超时`

要再次尝试登录 IdP，请选择另一个用户，然后运行另一个测试。

d) 单击**完成**以完成 SAML SSO 设置。

此时即启用 SAML SSO，并且所有参与 SAML SSO 的 Web 应用程序都重新启动。 Web 应用程序重新启动可能需要一到两分钟的时间。

重新启动 Cisco Tomcat 服务

启用或禁用 SAML 单点登录之前和之后，请在运行单点登录的所有 Unified CM 以及 IM and Presence Service 群集节点上重新启动 Cisco Tomcat 服务。

过程

步骤 1 登录到命令行界面。

步骤 2 运行 `utils service restart Cisco Tomcat` CLI 命令。

步骤 3 在启用了单点登录的所有群集节点上重复此程序。

验证 SAML SSO 配置

在服务提供程序 (Unified Communications Manager) 和 IdP 上配置 SAML SSO 后，在 Unified Communications Manager 中使用此程序确认配置正常。

开始之前

确认以下各项：

- Unified CM 管理中的 **SAML 单点登录配置**窗口表明您已成功导入 **IdP 元数据信任**文件。
- 服务提供程序元数据文件安装在 IdP 上。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**系统** > **SAML 单点登录** ， **SAML 单点登录配置** 窗口即会打开，然后单击**下一步**。

步骤 2 从**有效的管理员用户名**区域选择管理用户 ，然后单击**运行 SSO 测试 ...** 按钮。

注释 测试用户必须具有管理员权限，并且已作为用户添加到 IdP 服务器上。 “有效的管理员用户名”区域显示可被选择来运行测试的用户列表。

如果测试成功，SAML SSO 即会被配置成功。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。