# 管理 SAML 身份验证设置

## Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/active-iq-unified-manager-918/config/concept_manage_saml_authentication_settings_um.html on November 13, 2026. Always check docs.netapp.com for the latest.

# 目录


管理 SAML 身份验证设置 . . . 1
在 Active IQ Unified Manager 中启用 SAML 身份验证 . . . 1
在 Active IQ Unified Manager 中使用身份提供程序 . . . 1
支持的加密标准 . . . 1
已验证的身份提供程序 . . . 1
ADFS 配置要求 . . . 1
其他配置要求 . . . 2
在 Active IQ Unified Manager 中启用 SAML 身份验证 . . . 2
在 Active IQ Unified Manager 中更改 SAML 身份验证标识提供程序 . . . 3
在 Active IQ Unified Manager 安全证书更改后更新 SAML 身份验证设置 . . . 4
在 Active IQ Unified Manager 中禁用 SAML 身份验证 . . . 5
从 Active IQ Unified Manager 维护控制台禁用 SAML 身份验证 . . . 5
使用 Active IQ Unified Manager 中的 SAML 身份验证页面 . . . 6

# 管理 SAML 身份验证设置

## 在 Active IQ Unified Manager 中启用 SAML 身份验证

配置远程身份验证设置后，您可以启用安全断言标记语言（SAML）身份验证，以便远程用户在访问 Unified Manager Web UI 之前由安全身份提供程序（IdP）进行身份验证。

请注意，只有远程用户才能在启用 SAML 身份验证后访问 Unified Manager 图形用户界面。本地用户和维护用户将无法访问 UI。此配置不会影响访问维护控制台的用户。

## 在 Active IQ Unified Manager 中使用身份提供程序

在将 Unified Manager 配置为使用身份提供程序（IdP）为所有远程用户执行 SAML 身份验证时，您需要了解一些必需的配置设置，以便成功连接到 Unified Manager。

必须在 IdP 服务器中输入 Unified Manager URI 和元数据。您可以从 Unified ManagerSAML 身份验证页面复制此信息。在安全断言标记语言（SAML）标准中，Unified Manager 被视为服务提供程序（SP）。

### 支持的加密标准

- 高级加密标准（AES）：AES-128 和 AES-256
- 安全哈希算法（SHA）：SHA-1 和 SHA-256

### 已验证的身份提供程序

- Shibboleth
- Active Directory 联合身份验证服务（ADFS）

### ADFS 配置要求

- 必须按以下顺序定义三个声明规则，这些规则是 Unified Manager 解析此依赖方信任项的 ADFS SAML 响应所必需的。

| 声明规则 | 值 |
| --- | --- |
| SAM-account-name | 名称 ID |
| SAM-account-name | urn:oid:0.9.2342.19200300.100.1.1 |
| 令牌组 — 未限定名称 | urn:oid:1.3.6.1.4.1.5923.1.5.1.1 |

- 您必须将身份验证方法设置为“表单身份验证”，否则用户在注销 Unified Manager 时可能会收到错误。按照以下步骤操作：
  a. 打开 ADFS 管理控制台。
  b. 单击左侧树视图上的身份验证策略文件夹。
  c. 在右侧的“操作”下，单击“编辑全局主要身份验证策略”。

d. 将 Intranet 身份验证方法设置为“Forms Authentication”，而不是默认的“Windows Authentication”。

- 在某些情况下，当 Unified Manager 安全证书经过 CA 签名时，通过 IdP 登录会被拒绝。有两种解决方法可以解决此问题：
  - 按照链接中标识的说明，在 ADFS 服务器上禁用链式 CA 证书关联依赖方的吊销检查：

    "禁用每个依赖方信任的吊销检查"

  - 请让 CA 服务器驻留在 ADFS 服务器内，以便对 Unified Manager 服务器证书请求进行签名。

### 其他配置要求

- Unified Manager 时钟偏差设置为 5 分钟，因此 IdP 服务器和 Unified Manager 服务器之间的时间差不能超过 5 分钟，否则身份验证将失败。

# 在 Active IQ Unified Manager 中启用 SAML 身份验证

## 您可以启用安全断言标记语言（SAML）身份验证，以便远程用户在访问 Unified Manager Web UI 之前由安全身份提供程序（IdP）进行身份验证。

开始之前

- 您必须已配置远程身份验证并验证其成功。
- 您必须至少创建了一个具有应用程序管理员角色的远程用户或远程组。
- Unified Manager 必须支持身份提供程序（IdP），并且必须对其进行配置。
- 您必须具有 IdP URL 和元数据。
- 您必须能够访问 IdP 服务器。

从 Unified Manager 启用 SAML 身份验证后，在使用 Unified Manager 服务器主机信息配置 IdP 之前，用户无法访问图形用户界面。因此，在开始配置过程之前，您必须准备好完成连接的两个部分。可以在配置 Unified Manager 之前或之后配置 IdP。

启用 SAML 身份验证后，只有远程用户才能访问 Unified Manager 图形用户界面。本地用户和维护用户将无法访问 UI。此配置不会影响访问维护控制台、Unified Manager 命令或 ZAPI 的用户。

完成此页面上的 SAML 配置后，Unified Manager 将自动重新启动。

步骤

1. 在左侧导航窗格中，单击*常规* > **SAML** 身份验证。
2. 选中 启用 **SAML** 身份验证 复选框。

   将显示配置 IdP 连接所需的字段。

3. 请输入将 Unified Manager 服务器连接到 IdP 服务器所需的 IdP URI 和 IdP 元数据。

   如果可以直接从 Unified Manager 服务器访问 IdP 服务器，您可以在输入 IdP URI 后单击 获取 **IdP** 元数据 按钮，以自动填充 IdP 元数据字段。

4. 复制 Unified Manager 主机元数据 URI，或将主机元数据保存到 XML 文本文件。

   您此时可以使用此信息配置 IdP 服务器。

5. 单击 **Save**。

   此时将显示一个消息框，以确认您要完成配置并重新启动 Unified Manager。

6. 单击 确认并注销，Unified Manager 将重新启动。

下次授权远程用户尝试访问 Unified Manager 图形界面时，他们将在 IdP 登录页面而不是 Unified Manager 登录页面中输入其凭据。

如果尚未完成，请访问您的 IdP 并输入 Unified Manager 服务器 URI 和元数据以完成配置。

> 将 ADFS 用作身份提供程序时，Unified Manager GUI 不会遵守 ADFS 超时，并且将继续工作，直到达到 Unified Manager 会话超时。您可以通过单击 常规 > 功能设置 > 非活动超时 来更改 GUI 会话超时。

# 在 **Active IQ Unified Manager** 中更改 **SAML** 身份验证标识提供程序

您可以更改 Unified Manager 用来验证远程用户的身份提供程序（IdP）。

开始之前

- 您必须具有 IdP URL 和元数据。
- 您必须能够访问 IdP。

可以在配置 Unified Manager 之前或之后配置新的 IdP。

步骤

1. 在左侧导航窗格中，单击*常规* > **SAML** 身份验证。
2. 请输入将 Unified Manager 服务器连接到 IdP 所需的新 IdP URI 和 IdP 元数据。

   如果可以直接从 Unified Manager 服务器访问 IdP，您可以在输入 IdP URL 后单击 获取 **IdP** 元数据 按钮，以自动填充 IdP 元数据字段。

3. 复制 Unified Manager 元数据 URI，或将元数据保存到 XML 文本文件。
4. 单击*保存配置*。

   此时将显示一个消息框，以确认您要更改配置。

5. 单击 **OK**。

请访问新的 IdP 并输入 Unified Manager 服务器 URI 和元数据以完成配置。

下次授权远程用户尝试访问 Unified Manager 图形界面时，他们将在新的 IdP 登录页面而不是旧的 IdP 登录页面中输入其凭据。

# 在 **Active IQ Unified Manager** 安全证书更改后更新 **SAML** 身份验证设置

对 Unified Manager 服务器上安装的 HTTPS 安全证书进行任何更改都需要更新 SAML 身份验证配置设置。如果重命名主机系统、为主机系统分配新的 IP 地址或手动更改系统的安全证书，则会更新证书。

更改安全证书并重新启动 Unified Manager 服务器后，SAML 身份验证将无法运行，用户将无法访问 Unified Manager 图形界面。必须在 IdP 服务器和 Unified Manager 服务器上更新 SAML 身份验证设置，才能重新启用对用户界面的访问。

步骤

1. 登录维护控制台。
2. 在*主菜单*中，输入*禁用 SAML 身份验证*选项的数字。

   系统将显示一条消息，以确认您要禁用 SAML 身份验证并重新启动 Unified Manager。
3. 使用更新的 FQDN 或 IP 地址启动 Unified Manager 用户界面，在浏览器中接受更新的服务器证书，然后使用维护用户凭据登录。
4. 在 设置/身份验证 页面中，选择 **SAML** 身份验证 选项卡并配置 IdP 连接。
5. 复制 Unified Manager 主机元数据 URI，或将主机元数据保存到 XML 文本文件。
6. 单击 **Save**。

   此时将显示一个消息框，以确认您要完成配置并重新启动 Unified Manager。
7. 单击 确认并注销，Unified Manager 将重新启动。
8. 请访问您的 IdP 服务器并输入 Unified Manager 服务器 URI 和元数据以完成配置。

| 身份提供程序 | 配置步骤 |
| --- | --- |
| ADFS | a. 删除 ADFS 管理 GUI 中的现有依赖方信任条目。<br>b. 使用更新后的 Unified Manager 服务器中的 `saml_sp_metadata.xml`添加新的依赖方信任项。<br>c. 定义 Unified Manager 解析此依赖方信任条目的 ADFS SAML 响应所需的三个声明规则。<br>d. 重新启动 ADFS Windows 服务。 |
| Shibboleth | a. 将 Unified Manager 服务器的新 FQDN 更新到 `attribute-filter.xml`和 `relying-party.xml`文件中。<br>b. 重新启动 Apache Tomcat Web 服务器，并等待端口 8005 联机。 |

9. 登录到 Unified Manager，并通过 IdP 验证 SAML 身份验证是否按预期工作。

# 在 Active IQ Unified Manager 中禁用 SAML 身份验证

如果要在远程用户登录到 Unified Manager Web UI 之前停止通过安全身份提供程序（IdP）对其进行身份验证，则可以禁用 SAML 身份验证。禁用 SAML 身份验证时，已配置的目录服务提供程序（如 Active Directory 或 LDAP）将执行登录身份验证。

禁用 SAML 身份验证后，除了已配置的远程用户外，本地用户和维护用户还可以访问图形用户界面。

如果您无权访问图形用户界面，也可以使用 Unified Manager 维护控制台禁用 SAML 身份验证。

禁用 SAML 身份验证后，将自动重新启动 Unified Manager。

步骤

1. 在左侧导航窗格中，单击*常规* > **SAML** 身份验证。
2. 取消选中 启用 **SAML** 身份验证 复选框。
3. 单击 **Save**。

   此时将显示一个消息框，以确认您要完成配置并重新启动 Unified Manager。

4. 单击 确认并注销，Unified Manager 将重新启动。

下次远程用户尝试访问 Unified Manager 图形界面时，他们将在 Unified Manager 登录页面而不是 IdP 登录页面中输入其凭据。

请访问您的 IdP 并删除 Unified Manager 服务器 URI 和元数据。

# 从 Active IQ Unified Manager 维护控制台禁用 SAML 身份验证

当无法访问 Unified Manager GUI 时，您可能需要从维护控制台禁用 SAML 身份验证。这可能发生在配置错误或 IdP 不可访问的情况下。

开始之前

您必须能够以维护用户的身份访问维护控制台。

禁用 SAML 身份验证时，已配置的目录服务提供程序（如 Active Directory 或 LDAP）将执行登录身份验证。除了已配置的远程用户外，本地用户和维护用户也将能够访问图形用户界面。

您还可以从 UI 中的“设置/身份验证”页面禁用 SAML 身份验证。

禁用 SAML 身份验证后，将自动重新启动 Unified Manager。

步骤

1. 登录维护控制台。
2. 在*主菜单*中，输入*禁用 SAML 身份验证*选项的数字。

   系统将显示一条消息，以确认您要禁用 SAML 身份验证并重新启动 Unified Manager。

3. 键入 **y**，然后按 Enter，Unified Manager 将重新启动。

下次远程用户尝试访问 Unified Manager 图形界面时，他们将在 Unified Manager 登录页面而不是 IdP 登录页面中输入其凭据。

如果需要，请访问您的 IdP 并删除 Unified Manager 服务器 URL 和元数据。

# 使用 **Active IQ Unified Manager** 中的 **SAML** 身份验证页面

## 您可以使用 SAML 身份验证页面将 Unified Manager 配置为使用 SAML 通过安全身份提供程序（IdP）对远程用户进行身份验证，然后他们才能登录到 Unified Manager web UI。

- 您必须具有应用程序管理员角色才能创建或修改 SAML 配置。
- 您必须事先配置远程身份验证。
- 您必须事先至少配置一个远程用户或远程组。

配置远程身份验证和远程用户后，您可以选中启用 SAML 身份验证复选框，以启用使用安全身份提供程序的身份验证。

- **IdP URI**

  从 Unified Manager 服务器访问 IdP 的 URI。以下列出了示例 URI。

  ADFS 的示例 URI：

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  Shibboleth 的示例 URI：

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **IdP** 元数据

  XML 格式的 IdP 元数据。

  如果可以从 Unified Manager 服务器访问 IdP URL，则可以单击 获取 **IdP** 元数据 按钮以填充此字段。

- 主机系统（**FQDN**）

  安装期间定义的 Unified Manager 主机系统的 FQDN。如有必要，您可以更改此值。

- 主机 **URI**

  用于从 IdP 访问 Unified Manager 主机系统的 URI。

- 主机元数据

  XML 格式的主机系统元数据。

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。