安全与合规

NetApp Console setup and administration

NetApp
February 09, 2026

目录

安全与合规

身份联合

使用NetApp Console的身份联合实现单点登录

单点登录（联合）允许用户使用其公司凭证登录NetApp Console，从而简化了登录过程并增强了安全性。您可以使用身份提供商 (IdP) 或NetApp支持站点启用单点登录 (SSO)。

所需角色

组织管理员、联盟管理员、联盟查看器。"了解有关访问角色的更多信息。"

使用 **NetApp Support Site** 单点登录

与NetApp支持站点联合允许用户使用相同的凭据登录控制台、 Active IQ Digital Advisor和其他相关应用程序。

如果您与NetApp支持站点联合，则您不能与您的企业身份管理提供商联合。选择最适合您组织的一种。

步骤

1. 下载并完成 "NetApp联合申请表"。
2. 将表格提交至表格中指定的电子邮件地址。

   NetApp支持团队将审核并处理您的请求。

使用身份提供程序单一登录

您可以与身份提供商建立联合连接，以启用控制台的单点登录 (SSO)。该过程涉及配置您的身份提供商以信任NetApp作为服务提供商，然后在控制台中创建连接。

如果您之前使用NetApp Cloud Central（控制台的外部应用程序）配置了联合，则需要使用联合页面导入联合以在控制台内进行管理。"了解如何导入您的联盟。"

支持的身份提供者

NetApp支持以下联合协议和身份提供程序：

协议

- 安全断言标记语言 (SAML) 身份提供者
- Active Directory 联合身份验证服务 (AD FS)

身份提供者

- 微软Entra ID
- Ping联邦

NetApp仅支持服务提供商发起的（SP发起的） SSO。您需要首先配置身份提供者以信任NetApp作为服务提供商。然后，您可以在控制台中创建使用身份提供者配置的连接。

您可以与您的电子邮件域或您拥有的其他域联合。要与不同于您的电子邮件域的域联合，请首先验证您拥有该域。

1 验证您的域名（如果不使用您的电子邮件域名）

要与不同于您的电子邮件域的域联合，请验证您拥有该域。您无需任何额外步骤即可联合您的电子邮件域。

2 配置您的 **IdP** 以信任**NetApp**作为服务提供商

通过创建新应用程序并提供 ACS URL、实体 ID 或其他凭证信息等详细信息，将您的身份提供商配置为信任NetApp 。服务提供商信息因身份提供商而异，因此请参阅特定身份提供商的文档以了解详细信息。您需要与您的 IdP 管理员合作来完成此步骤。

3 在控制台中创建联合连接

提供来自身份提供商的 SAML 元数据 URL 或文件以创建连接。此信息用于建立控制台和您的身份提供者之间的信任关系。您提供的信息取决于您使用的 IdP。例如，如果您使用 Microsoft Entra ID，则需要提供客户端 ID、密钥和域。

4 在控制台中测试您的联盟

在启用联合连接之前对其进行测试。使用控制台中联合页面上的测试选项来验证您的测试用户是否可以成功进行身份验证。如果测试成功，则可以启用连接。

5 在控制台中启用您的连接

启用连接后，用户可以使用其公司凭证登录控制台。

查看相应协议或 IdP 的主题以开始：

- "与 AD FS 设置联合连接"
- "与 Microsoft Entra ID 建立联合连接"
- "使用 PingFederate 设置联合连接"
- "与 SAML 身份提供商建立联合连接"

域验证

验证联合连接的电子邮件域

如果您想要与不同于您的电子邮件域的域联合，您必须首先验证您拥有该域。您只能使用已验证的域进行联合。

必需角色

需要联盟管理员角色来创建和管理联盟。联盟查看者可以查看联盟页面。"了解有关访问角色的更多信息。"

验证您的域名涉及向您的域名的 DNS 设置添加 TXT 记录。此记录用于证明您拥有该域并允许NetApp Console信任该域进行联合。您可能需要与您的 IT 或网络管理员协调来完成此步骤。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”以查看“**Federations**”页面。
3. 选择*配置新联合*。
4. 选择*验证域名所有权*。
5. 输入您要验证的域名并选择*继续*。
6. 复制提供的 TXT 记录。
7. 转到您域的 DNS 设置并配置作为您域的 TXT 记录提供的 TXT 值。如果需要，请与您的 IT 或网络管理员合作。
8. 添加TXT记录后，返回控制台并选择*验证*。

配置联合

将**NetApp Console**与 **Active Directory** 联合服务 **(AD FS)** 联合起来

将您的 Active Directory 联合身份验证服务 (AD FS) 与NetApp Console联合起来，以便为NetApp Console启用单点登录 (SSO)。这允许用户使用他们的公司凭证登录控制台。

必需角色

需要联盟管理员角色来创建和管理联盟。联盟查看者可以查看联盟页面。"了解有关访问角色的更多信息。"

您可以与您的企业 IdP 或NetApp支持站点联合。 NetApp建议选择其中一个，但不要同时选择两者。

NetApp仅支持服务提供商发起的（SP发起的） SSO。首先，配置身份提供者以信任NetApp Console作为服务提供者。然后，使用您的身份提供商的配置在控制台中创建连接。

您可以与 AD FS 服务器建立联合，以启用NetApp Console的单点登录 (SSO)。该过程涉及配置您的 AD FS 以信任控制台作为服务提供商，然后在NetApp Console中创建连接。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”以查看“**Federations**”页面。
3. 选择*配置新联合*。
4. 输入您的域名详细信息：
   a. 选择您是否要使用已验证的域名或您的电子邮件域名。电子邮件域是与您登录的帐户关联的域。
   b. 输入您正在配置的联盟的名称。

c. 如果您选择已验证的域，请从列表中选择该域。

5. 选择“下一步”。
6. 对于您的连接方法，选择*协议*，然后选择*Active Directory 联合身份验证服务 (AD FS)*。
7. 选择“下一步”。
8. 在您的 AD FS 服务器中创建依赖方信任。您可以使用 PowerShell 或在 AD FS 服务器上手动配置它。有关如何创建信赖方信任的详细信息，请参阅 AD FS 文档。

   a. 使用以下脚本通过 PowerShell 创建信任：

   ```
   (new-object Net.WebClient -property @{Encoding = [Text.Encoding]
   ::UTF8}).DownloadString("https://raw.github.com/auth0/AD FS-
   auth0/master/AD FS.ps1") | iex
   AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-
   cloud-account.auth0.com/login/callback"
   ```

   b. 或者，您可以在 AD FS 管理控制台中手动创建信任。创建信任时使用以下NetApp Console值：

      - 创建依赖信任标识符时，使用 **YOUR_TENANT** 值： `netapp-cloud-account`
      - 当您选择 启用对 **WS-Federation** 的支持 时，请使用 **YOUR_AUTH0_DOMAIN** 值： `netapp-cloud-account.auth0.com`

   c. 创建信任后，从 AD FS 服务器复制元数据 URL 或下载联合元数据文件。您需要此 URL 或文件来完成控制台中的连接。

   NetApp建议使用元数据 URL 让NetApp Console自动检索最新的 AD FS 配置。如果您下载联合元数据文件，则每当 AD FS 配置发生更改时，都需要在NetApp Console中手动更新它。

9. 返回控制台，然后选择“下一步”来创建连接。
10. 创建与 AD FS 的连接。

    a. 输入您在上一步中从 AD FS 服务器复制的 **AD FS URL** 或上传您从 AD FS 服务器下载的联合元数据文件。

11. 选择*创建连接*。建立连接可能需要几秒钟。
12. 选择“下一步”。
13. 选择*测试连接*来测试您的连接。您将被引导至 IdP 服务器的登录页面。使用您的身份提供商凭据登录。登录后，返回控制台启用连接。

    在受限模式下使用控制台时，请将 URL 复制到隐身浏览器窗口或单独的浏览器中，以登录到您的身份提供商 (IdP)。

14. 在控制台中，选择“下一步”以查看摘要页面。
15. 设置通知。

    您可以选择七天或三十天。系统会通过电子邮件向具有以下角色的任何用户发送到期通知，并在控制台中显示这些通知：超级管理员、组织管理员、联盟管理员和联盟查看者。

16. 查看联盟详细信息，然后选择“启用联盟”。
17. 选择“完成”以完成该过程。

启用联合身份验证后，用户可以使用其企业凭据登录NetApp Console。

将**NetApp Console**与 **Microsoft Entra ID** 联合起来

与您的 Microsoft Entra ID IdP 提供商联合，为NetApp Console启用单点登录 (SSO)。这允许用户使用他们的公司凭证登录。

必需角色

需要联盟管理员角色来创建和管理联盟。联盟查看者可以查看联盟页面。"了解有关访问角色的更多信息。"

> 您可以与您的企业 IdP 或NetApp支持站点联合。 NetApp建议选择其中一个，但不要同时选择两者。

NetApp仅支持服务提供商发起的（SP发起的） SSO。您需要首先配置身份提供者以信任NetApp作为服务提供商。然后，您可以在控制台中创建使用身份提供者配置的连接。

您可以与 Microsoft Entra ID 建立联合连接，以启用控制台的单点登录 (SSO)。该过程涉及配置您的 Microsoft Entra ID 以信任控制台作为服务提供商，然后在控制台中创建连接。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”以查看“**Federations**”页面。
3. 选择*配置新联合*。

域名详细信息

1. 输入您的域名详细信息：
   a. 选择您是否要使用已验证的域名或您的电子邮件域名。电子邮件域是与您登录的帐户关联的域。
   b. 输入您正在配置的联盟的名称。
   c. 如果您选择已验证的域，请从列表中选择该域。
2. 选择“下一步”。

连接方法

1. 对于您的连接方法，选择*提供商*，然后选择*Microsoft Entra ID*。
2. 选择“下一步”。

配置说明

1. 配置您的 Microsoft Entra ID 以信任NetApp作为服务提供商。您需要在 Microsoft Entra ID 服务器上执行此步骤。
   a. 注册 Microsoft Entra ID 应用程序以信任控制台时，请使用以下值：

- 对于 重定向 **URL** ，使用 https://services.cloud.netapp.com
- 对于 回复 **URL**，使用 https://netapp-cloud-account.auth0.com/login/callback

b. 为您的 Microsoft Entra ID 应用创建客户端机密。您需要提供客户端 ID、客户端密钥和 Entra ID 域名来完成联合。

2. 返回控制台，然后选择“下一步”来创建连接。

创建连接

1. 使用 Microsoft Entra ID 创建连接
   a. 输入您在上一步中创建的客户端 ID 和客户端密钥。
   b. 输入 Microsoft Entra ID 域名。
2. 选择*创建连接*。系统在几秒钟内建立连接。

测试并启用连接

1. 选择“下一步”。
2. 选择*测试连接*来测试您的连接。您将被引导至 IdP 服务器的登录页面。使用您的身份提供商凭据登录。登录后，返回控制台启用连接。

> 在受限模式下使用控制台时，请将 URL 复制到隐身浏览器窗口或单独的浏览器中，以登录到您的身份提供商 (IdP)。

3. 在控制台中，选择“下一步”以查看摘要页面。
4. 设置通知。

   您可以选择七天或三十天。系统会通过电子邮件向具有以下角色的任何用户发送到期通知，并在控制台中显示这些通知：超级管理员、组织管理员、联盟管理员和联盟查看者。

5. 查看联盟详细信息，然后选择“启用联盟”。
6. 选择“完成”以完成该过程。

启用联合身份验证后，用户可以使用其企业凭据登录NetApp Console。

使用 **PingFederate** 联合**NetApp Console**

与您的 PingFederate IdP 提供商联合，为NetApp Console启用单点登录 (SSO)。这允许用户使用他们的公司凭证登录。

必需角色

需要联盟管理员角色来创建和管理联盟。联盟查看者可以查看联盟页面。"了解有关访问角色的更多信息。"

> 您可以与您的企业 IdP 或NetApp支持站点联合。 NetApp建议选择其中一个，但不要同时选择两者。

NetApp仅支持服务提供商发起的（SP发起的） SSO。您需要首先配置身份提供者以信任NetApp作为服务提供商。然后，您可以在控制台中创建使用身份提供者配置的连接。

您可以使用 PingFederate 设置联合连接，以启用控制台的单点登录 (SSO)。该过程涉及配置您的 PingFederate 服务器以信任控制台作为服务提供商，然后在控制台中创建连接。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”以查看“**Federations**”页面。
3. 选择*配置新联合*。
4. 输入您的域名详细信息：
   a. 选择您是否要使用已验证的域名或您的电子邮件域名。电子邮件域是与您登录的帐户关联的域。
   b. 输入您正在配置的联盟的名称。
   c. 如果您选择已验证的域，请从列表中选择该域。
5. 选择“下一步”。
6. 对于您的连接方法，选择*提供商*，然后选择*PingFederate*。
7. 选择“下一步”。
8. 配置您的 PingFederate 服务器以信任NetApp作为服务提供商。您需要在 PingFederate 服务器上执行此步骤。
   a. 配置 PingFederate 以信任NetApp Console时，请使用以下值：
      - 对于 回复 **URL** 或 断言消费者服务 **(ACS) URL**，使用 `https://netapp-cloud-account.auth0.com/login/callback`
      - 对于*注销 URL*，使用 `https://netapp-cloud-account.auth0.com/logout`
      - 对于*受众/实体 ID*，使用 `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>`其中 `<fed-domain-name-pingfederate>` 是联合的域名。例如，如果您的域名是 `example.com`，受众/实体 ID 将是 `urn:auth0:netappcloud-account:fed-example-com-pingfederate`。
   b. 复制 PingFederate 服务器 URL。在控制台中创建连接时，您将需要此 URL。
   c. 从您的 PingFederate 服务器下载 X.509 证书。它需要采用 Base64 编码的 PEM 格式（.pem、.crt、.cer）。
9. 返回控制台，然后选择“下一步”来创建连接。
10. 使用 PingFederate 创建连接
    a. 输入您在上一步中复制的 PingFederate 服务器 URL。
    b. 上传 X.509 签名证书。证书必须采用 PEM、CER 或 CRT 格式。
11. 选择*创建连接*。系统在几秒钟内建立连接。
12. 选择“下一步”。
13. 选择*测试连接*来测试您的连接。您将被引导至 IdP 服务器的登录页面。使用您的身份提供商凭据登录。登录后，返回控制台启用连接。

> 在受限模式下使用控制台时，请将 URL 复制到隐身浏览器窗口或单独的浏览器中，以登录到您的身份提供商 (IdP)。

14. 在控制台中，选择“下一步”以查看摘要页面。
15. 设置通知。

    您可以选择七天或三十天。系统会通过电子邮件向具有以下角色的任何用户发送到期通知，并在控制台中显示这些通知：超级管理员、组织管理员、联盟管理员和联盟查看者。

16. 查看联盟详细信息，然后选择“启用联盟”。
17. 选择“完成”以完成该过程。

启用联合身份验证后，用户可以使用其企业凭据登录NetApp Console。

与 **SAML** 身份提供商联合

与您的 SAML 2.0 IdP 提供商联合，为 NEtApp 控制台启用单点登录 (SSO)。这允许用户使用他们的公司凭证登录。

所需角色

需要联盟管理员角色来创建和管理联盟。联盟查看者可以查看联盟页面。"了解有关访问角色的更多信息。"

您可以与您的企业 IdP 或NetApp支持站点联合。你不能与两者结成联盟。

NetApp仅支持服务提供商发起的（SP发起的） SSO。您需要首先配置身份提供者以信任NetApp作为服务提供商。然后，您可以在控制台中创建使用身份提供者配置的连接。

您可以与 SAML 2.0 提供商建立联合连接，以便为控制台启用单点登录 (SSO)。该过程涉及配置您的提供商以信任NetApp作为服务提供商，然后在控制台中创建连接。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”以查看“**Federations**”页面。
3. 选择*配置新联合*。
4. 输入您的域名详细信息：
    a. 选择您是否要使用已验证的域名或您的电子邮件域名。电子邮件域是与您登录的帐户关联的域。
    b. 输入您正在配置的联盟的名称。
    c. 如果您选择已验证的域，请从列表中选择该域。
5. 选择“下一步”。
6. 对于您的连接方法，选择*协议*，然后选择*SAML 身份提供者*。
7. 选择“下一步”。
8. 配置您的 SAML 身份提供商以信任NetApp作为服务提供商。您需要在 SAML 提供商服务器上执行此步骤。
    a. 确保您的 IdP 具有属性 `email`设置为用户的电子邮件地址。这是控制台正确识别用户所必需的：

```
<saml:AttributeStatement
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        <saml:AttributeValue
xsi:type="xs:string">email@domain.com</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

1. 在控制台中注册 SAML 应用程序时，请使用以下值：
   - 对于 回复 **URL** 或 断言消费者服务 **(ACS) URL**，使用 `https://netapp-cloud-account.auth0.com/login/callback`
   - 对于*注销 URL*，使用 `https://netapp-cloud-account.auth0.com/logout`
   - 对于*受众/实体 ID*，使用 `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>`其中 `<fed-domain-name-saml>` 是您想要用于联合的域名。例如，如果您的域名是 `example.com`，受众/实体 ID 将是 `urn:auth0:netapp-cloud-account:fed-example-com-samlp`。
2. 创建信任后，从 SAML 提供商服务器复制以下值：
   - 登录网址
   - 退出 URL（可选）
3. 从您的 SAML 提供商服务器下载 X.509 证书。它需要采用 PEM、CER 或 CRT 格式。
   a. 返回控制台，然后选择“下一步”来创建连接。
   b. 使用 SAML 创建连接。
4. 输入您的 SAML 服务器的 登录 **URL**。
5. 上传从 SAML 提供商服务器下载的 X.509 证书。
6. 或者，输入您的 SAML 服务器的 退出 **URL**。
   a. 选择*创建连接*。系统在几秒钟内建立连接。
   b. 选择“下一步”。
   c. 选择*测试连接*来测试您的连接。您将被引导至 IdP 服务器的登录页面。使用您的身份提供商凭据登录。登录后，返回控制台启用连接。

      在受限模式下使用控制台时，请将 URL 复制到隐身浏览器窗口或单独的浏览器中，以登录到您的身份提供商 (IdP)。

   d. 在控制台中，选择“下一步”以查看摘要页面。
   e. 设置通知。

      您可以选择七天或三十天。系统会通过电子邮件向具有以下角色的任何用户发送到期通知，并在控制台中显示这些通知：超级管理员、组织管理员、联盟管理员和联盟查看者。

f. 查看联盟详细信息，然后选择“启用联盟”。

g. 选择“完成”以完成该过程。

启用联合身份验证后，用户可以使用其企业凭据登录NetApp Console。

管理联盟

在NetApp Console中管理联合

您可以在NetApp Console中管理您的联合。您可以禁用它，更新过期的凭据，以及在不再需要它时禁用它。

必需角色

需要联盟管理员角色来创建和管理联盟。联盟查看者可以查看联盟页面。"了解有关访问角色的更多信息。"

您还可以向现有联盟添加额外的已验证域，从而允许您为联盟连接使用多个域。

- 如果您使用NetApp Cloud Central 配置了联合，请通过 **Federation** 页面导入它以在控制台中进行管理。"了解如何导入您的联盟"
- 您可以在“审核”页面上查看联盟管理事件，例如启用、禁用和更新联盟。 "了解有关在NetApp Console中监控操作的更多信息。"

启用联盟

如果您已经创建了联盟但尚未启用，您可以通过*联盟*页面启用它。启用联合允许与联合关联的用户使用其公司凭据登录控制台。在启用联合之前，请先成功创建并测试联合。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”选项卡。
3. 选择操作菜单 ••• 旁边的您想要启用的联盟并选择*启用*。

将已验证的域添加到现有联合

您可以在控制台中将已验证的域添加到现有联合，以便使用具有相同身份提供商 (IdP) 的多个域。

您必须先在控制台中验证该域，然后才能将其添加到联合中。如果您尚未验证域名，可以按照以下步骤进行验证"在控制台中验证您的域"。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”选项卡。
3. 选择操作菜单 ⋮ 在您要添加已验证域的联盟旁边，然后选择*更新域*。 *更新域*对话框显示已与此联合关联的域。
4. 从可用域列表中选择一个已验证的域。
5. 选择*更新*。新域用户可以在 30 秒内获得联合控制台访问权限。

更新即将到期的联合连接

您可以在控制台中更新联合的详细信息。例如，如果证书或客户端机密等凭证过期，则需要更新联合。在需要时，更新通知日期以提醒您在连接到期之前更新连接。

在更新您的 IdP 之前，请先更新控制台以避免登录问题。在此过程中保持登录控制台。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”选项卡。
3. 选择要更新的联合旁边的操作菜单（三个垂直点），然后选择*更新联合*。
4. 根据需要更新联盟的详细信息。
5. 选择*更新*。

测试现有的联盟

测试现有联合的连接以验证其是否正常工作。这可以帮助您识别联盟中的任何问题并进行故障排除。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”选项卡。
3. 选择操作菜单旁边的您想要添加已验证域的联盟，然后选择*测试连接*。
4. 选择*测试*。系统提示您使用公司凭证登录。如果连接成功，您将被重定向到NetApp Console。如果连接失败，您会看到一条错误消息，表明联合存在问题。
5. 选择“完成”返回“联合”选项卡。

禁用联合

如果您不再需要联合，您可以禁用它。这可以防止与联盟关联的用户使用其公司凭证登录控制台。如果需要，您可以稍后重新启用联合。

在删除联合之前，请先禁用它，例如在停用 IdP 或停止联合时。如果需要的话，您可以稍后重新启用它。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”选项卡。
3. 选择操作菜单在您要添加已验证域的联盟旁边，然后选择*禁用*。

删除联盟

如果您不再需要联盟，您可以将其删除。这将删除联合并阻止与联合关联的任何用户使用其公司凭据登录控制台。例如，如果 IdP 被停用或者不再需要联合。

删除联合后，您将无法恢复它。您必须创建一个新的联盟。

您必须先禁用联合，然后才能删除它。一旦删除联盟，就无法恢复删除。

步骤

1. 选择“管理”>“身份和访问”。
2. 选择“**Federations**”以查看“**Federations**”页面。
3. 选择操作菜单：在您要添加已验证域的联盟旁边，然后选择*删除*。

将您的联合导入**NetApp Console**

如果您之前已通过NetApp Cloud Central（ NetApp Console的外部应用程序）设置联合，则联合页面会提示您将现有的联合连接导入控制台，以便您可以在新界面中对其进行管理。然后，您可以利用最新的增强功能，而无需重新创建联合连接。

导入现有联盟后，您可以从“联盟”页面管理该联盟。"了解有关管理联盟的更多信息。"

所需角色

组织管理员或联盟管理员。"了解有关访问角色的更多信息。"

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”选项卡。
3. 选择*导入联合*。

强制实施**ONTAP Advanced View**（**ONTAP**系统管理器）的**ONTAP**权限

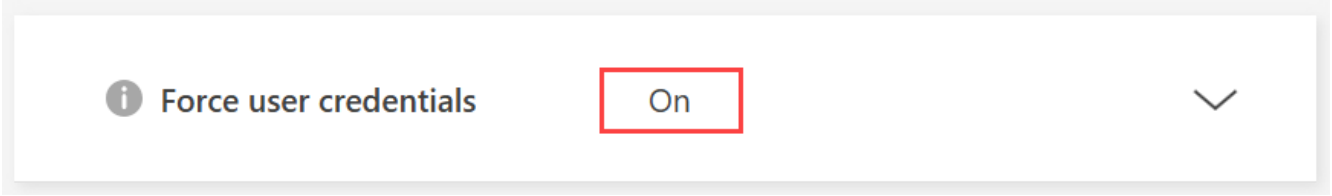
默认情况下，控制台代理凭据允许用户访问高级视图（ONTAP系统管理器）。您可以提示用户输入他们的ONTAP凭据。这可确保用户在Cloud Volumes ONTAP和ONTAP本地集群中使用ONTAP集群时应用其ONTAP权限。

您必须具有组织管理员角色才能编辑控制台代理设置。

步骤

1. 选择“管理 > 代理”。
2. 在*概览*页面上，选择控制台代理的操作菜单，然后选择*编辑代理*。

   控制台代理必须处于活动状态才能对其进行编辑。
3. 展开*强制凭证*选项。
4. 选中复选框以启用*强制凭证*选项，然后选择*保存*。
5. 验证“强制凭证”选项是否已启用。



为NetApp Console组织启用只读模式

为安全起见，您可以为NetApp Console组织启用只读模式。在只读模式下，用户可以查看资源和设置，但不能进行任何更改。

在只读模式下，具有管理员角色的用户必须手动提升权限才能进行更改，这确保了更改是有意为之的。

所需访问权限

超级管理员或组织管理员。

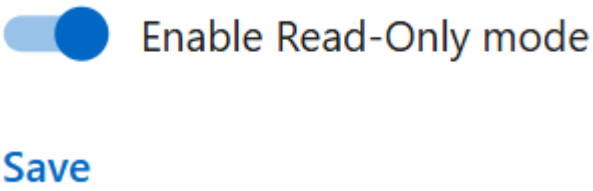
为您的控制台组织启用只读模式

启用只读模式以限制对控制台组织的更改。所有用户仍然可以查看资源。拥有管理员角色的用户，如果不手动提升权限，则无法在控制台中执行任何操作。

启用只读模式后，用户会看到一个横幅，通知他们该组织处于只读模式。用户必须前往用户设置来提升其角色。

步骤

1. 选择*管理>身份和访问*。
2. 在“组织”选项卡中，选择要设置为只读模式的组织的“编辑组织设置”。
3. 在“只读模式”部分，将开关拨到“开”位置启用只读模式，然后选择“保存”。



以初始组织管理员身份注册NetApp Console

如果贵公司还没有NetApp Console组织，请注册创建一个。第一个用户是管理员，负责管理帐户和权限。您可以稍后更新角色并添加管理员。

步骤

1. 打开 Web 浏览器并转到 "NetApp Console"
2. 如果您拥有NetApp支持站点帐户，请直接在“登录”页面上输入与您的帐户关联的电子邮件地址。

   控制台会在您首次登录时使用您的NetApp支持站点凭据进行注册。

3. 如果您想通过创建控制台登录来注册，请选择*注册*。
   a. 在*注册*页面上，输入所需信息并选择*下一步*。

      注册表格中只允许使用英文字符。

   b. 检查您的收件箱，查找来自NetApp的电子邮件，其中包含验证您的电子邮件地址的说明。

      请验证您的电子邮件地址以完成注册。

4. 登录后，请阅读并接受最终用户许可协议。
5. 在“欢迎”页面上，创建一个组织。
6. 选择*让我们开始吧*。

+ 作为首次担任管理员的用户，请按照引导流程添加存储、创建控制台代理等。 "了解如何使用控制台助手。"

下一步

作为管理员，在完成控制台助手中包含的步骤后，您应该规划身份和访问策略，将用户添加到您的组织，并分配角色。 "了解NetApp Console的身份和访问管理"

如果组织已存在，请注册或登录NetApp Console。

如果贵公司已有NetApp Console组织，请注册或登录以访问它。您的注册或登录方式取决于您的公司是否使用身份联合或拥有NetApp支持站点凭据。如果还没有，请创建NetApp Console登录帐户。

步骤

1. 打开 Web 浏览器并转到 "NetApp Console"
2. 如果您拥有NetApp支持站点帐户，或者您的公司已设置单点登录 (SSO)，请在“登录”页面上输入您关联的电子邮件地址或 SSO 凭据。按照提示完成登录。

   在这两种情况下，您都会在初始登录时注册控制台。

3. 如果您想通过创建控制台登录来注册，请选择*注册*。
   a. 在*注册*页面上，输入所需信息并选择*下一步*。

      注册表格中只允许使用英文字符。

   b. 检查您的收件箱，查找来自NetApp的电子邮件，其中包含验证您的电子邮件地址的说明。

      请验证您的电子邮件地址以完成注册。

4. 登录后，请阅读并接受最终用户许可协议。
5. 如果系统提示您创建组织，请关闭对话框并告知控制台管理员，以便他们可以将您添加到控制台组织并授予您访问权限。 "了解如何联系组织管理员。"

下一步

获得组织访问权限后，即可开始管理存储和使用分配给您的数据服务。