管理安全证书

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/task_view_https_security_certificate_ocf.html on November 13, 2026. Always check docs.netapp.com for the latest.

目录

管理安全证书 . . . 1
在 Active IQ Unified Manager 中查看 HTTPS 安全证书 . . . 1
在 Active IQ Unified Manager 中下载 HTTPS 证书签名请求 . . . 1
在 Active IQ Unified Manager 中安装 CA 签名的 HTTPS 证书 . . . 1
示例证书链 . . . 2
了解在 Active IQ Unified Manager Unified Manager 中使用外部工具生成的 HTTPS 证书 . . . 2
使用 EC 密钥对加载证书的格式 . . . 3
使用 RSA 密钥对加载证书的格式 . . . 3
上传外部生成的证书时的检查 . . . 4
证书管理的页面描述 . . . 5
了解 Active IQ Unified Manager 中的 HTTPS 证书页面 . . . 5
在 Active IQ Unified Manager 中重新生成 HTTPS 证书对话框 . . . 5

管理安全证书

在 Active IQ Unified Manager 中查看 HTTPS 安全证书

您可以将 HTTPS 证书详细信息与浏览器中检索的证书进行比较，以确保浏览器与 Unified Manager 的加密连接不会被截获。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

查看证书使您能够验证重新生成的证书的内容，或查看可以从中访问 Unified Manager 的使用者备用名称（SAN）。

步骤

1. 在左侧导航窗格中，单击 常规 > **HTTPS** 证书。

   此时 HTTPS 证书将显示在页面顶部。

如果您需要查看比 HTTPS 证书页面上显示的更详细的安全证书信息，则可以在浏览器中查看连接证书。

在 Active IQ Unified Manager 中下载 HTTPS 证书签名请求

您可以下载当前 HTTPS 安全证书的证书签名请求，以便将该文件提供给证书颁发机构进行签名。CA 签名证书有助于防止中间人攻击，并提供比自签名证书更好的安全保护。

开始之前

您必须具有应用程序管理员角色。

步骤

1. 在左侧导航窗格中，单击 常规 > **HTTPS** 证书。
2. 单击*下载 HTTPS 证书签名请求*。
3. 保存 `<hostname>.csr`文件。

您可以将文件提供给证书颁发机构以签名，然后安装签名证书。

在 Active IQ Unified Manager 中安装 CA 签名的 HTTPS 证书

您可以在证书颁发机构签名并返回安全证书之后上传并安装它。您上传和安装的文件必须是签名版本的现有自签名证书。CA 签名证书有助于避免受到中间人攻击，且可提供比自签名证书更好的安全保护。

*什么 .开始之前

您必须已完成以下操作：

- 下载证书签名请求文件并由证书颁发机构签名
- 以 PEM 格式保存证书链
- 包括链中的所有证书，从 Unified Manager 服务器证书到根签名证书，包括存在的任何中间证书

您必须具有应用程序管理员角色。

如果为其创建 CSR 的证书的有效期超过 397 天，则 CA 将在签署并返回证书之前将其有效期缩短至 397 天

步骤

1. 在左侧导航窗格中，单击 常规 > **HTTPS** 证书。
2. 单击 安装 **HTTPS** 证书。
3. 在显示的对话框中，单击*选择文件……*以查找要上传的文件。
4. 选择文件，然后单击*安装*以安装文件。

有关信息，请参见 "安装使用外部工具生成的 HTTPS 证书"。

示例证书链

以下示例显示了证书链文件的显示方式：

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

了解在 **Active IQ Unified Manager Unified Manager** 中使用外部工具生成的 **HTTPS** 证书

您可以安装自签名或 CA 签名的证书，这些证书是使用 OpenSSL、BoringSSL 、LetsEncrypt 等外部工具生成的。

您应该将私钥与证书链一起加载，因为这些证书是外部生成的公钥-私钥对。允许的密钥对算法是“RSA”和“EC”。安装 **HTTPS** 证书 选项在常规部分下的 HTTPS 证书页面中提供。您上传的文件应采用以下输入格式。

1. Active IQ Unified Manager 主机所属服务器的私钥

2. 与私钥匹配的服务器证书
3. 反向直至根证书的 CA 证书，用于签署上述证书

使用 **EC** 密钥对加载证书的格式

允许的曲线为“prime256v1”和“secp384r1”。具有外部生成的 EC 对的证书示例：

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

使用 **RSA** 密钥对加载证书的格式

属于主机证书的 RSA 密钥对的允许密钥大小为 2048、3072 和 4096。具有外部生成的 **RSA** 密钥对 的证书：

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
```

```
-----END CERTIFICATE-----
```

上传证书后，您应重新启动 Active IQ Unified Manager 实例以使更改生效。

上传外部生成的证书时的检查

系统在上传使用外部工具生成的证书时会执行检查。如果任何检查失败，则证书将被拒绝。此外，还包括对从产品内的 CSR 生成的证书以及使用外部工具生成的证书的验证。

- 输入中的私钥将根据输入中的主机证书进行验证。
- 根据主机的 FQDN 检查主机证书中的通用名称（CN）。
- 主机证书的公用名称（CN）不应为空或空白，也不应设置为 localhost。
- 有效期开始日期不应为将来日期，证书的有效期到期日期不应为过去日期。
- 如果存在中间 CA 或 CA，则证书的有效期开始日期不应在未来，有效期到期日期不应在过去。



输入中的私钥不应加密。如果存在任何已加密的私钥，则会被系统拒绝。

示例 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

示例 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

示例 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

如果证书安装失败，请参阅知识库 (KB) 文章：https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate["ActiveIQ Unified Manager 无法安装外部生成的证书"^]

证书管理的页面描述

了解 **Active IQ Unified Manager** 中的 **HTTPS** 证书页面

可使用 HTTPS 证书页面查看当前安全证书、下载证书签名请求、生成新的自签名 HTTPS 证书或安装新的 HTTPS 证书。

如果您尚未生成新的自签名 HTTPS 证书，则此页面上显示的证书就是在安装过程中生成的证书。

命令按钮

命令按钮可用于执行以下操作：

- 下载 **HTTPS** 证书签名请求

  下载当前安装的 HTTPS 证书的证书请求。您的浏览器会提示您保存 <hostname>.csr 文件，以便您可以将该文件提供给证书颁发机构进行签名。

- 安装 **HTTPS** 证书

  使您能够在证书颁发机构签名并返回后上传和安装安全证书。重新启动管理服务器后，新证书即生效。

- 重新生成 **HTTPS** 证书

  使您能够生成新的自签名 HTTPS 证书，以替换当前的安全证书。重新启动 Unified Manager 后，新证书即生效。

在 **Active IQ Unified Manager** 中重新生成 **HTTPS** 证书对话框

通过“重新生成 HTTPS 证书”对话框，您可以自定义安全信息，然后使用该信息生成新的 HTTPS 证书。

此页面上将显示当前证书信息。

“使用当前证书属性重新生成”和“更新当前证书属性”选项使您可以使用当前信息重新生成证书或使用新信息生成证书。

- 通用名称

  必需。要保护的完全限定域名 (FQDN)。

  在 Unified Manager 高可用性配置中，使用虚拟 IP 地址。

- 电子邮件

  可选。用于联系您组织的电子邮件地址；通常是证书管理员或 IT 部门的电子邮件地址。

- 公司

  可选。通常是公司的法定名称。

- 部门

  可选。公司部门名称。

- 城市

  可选。公司所在的城市位置。

- **State**

  可选。公司所在的州或省/自治区/直辖市位置（非缩写）。

- 国家/地区

  可选。公司所在的国家/地区位置。这通常是指国家/地区的两个字母的 ISO 代码。

- 备用名称

  必需。除了现有本地主机或其他网络地址以外，还可以使用其他非主域名来访问此服务器。每个替换名称均使用英文逗号进行分隔。

  如果要从证书的“备用名称”字段中删除本地标识信息，请选中 “Exclude local identifying information (e.g. localhost)” 复选框。选中此复选框时，仅在“备用名称”字段中使用您在该字段中输入的内容。留空时，生成的证书将完全没有“备用名称”字段。

- 密钥大小（密钥算法：**RSA**）

  密钥算法设置为 RSA。您可以选择一种密钥大小：2048、3072 或 4096 位。默认密钥大小设置为 2048 位。

- 有效期

  默认有效期为 397 天。如果您已从早期版本升级，您可能会看到以前的证书有效期保持不变。

有关详细信息，请参见"生成 HTTPS 证书"。

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。