SSL 设置

SSL 设置

在以下位置之一配置 SSL 设置：

- **Configuration > Device Management > Advanced > SSL Settings**
- **配置 > 远程访问 VPN > 高级 > SSL 设置**

ASA 使用安全套接字层 (SSL) 协议和传输层安全 (TLS) 为 ASDM、无客户端 SSL VPN、VPN 和基于浏览器的会话提供安全消息传输支持。此外，DTLS 还会用于安全客户端连接。SSL Settings 面板允许您为客户端和服务器配置 SSL 版本和加密算法。它还允许您将以前配置的信任点应用于特定接口以及为没有关联信任点的接口配置备用信任点。

注释 对于版本 9.3(2)，SSLv3 已废弃。默认值现在为 **tlsv1** 而不是 **any**。**any** 关键字已废弃。如果您选择 **any**、**sslv3** 或 **sslv3-only**，系统将接受设置，但是会显示一条警告。点击**确定 (OK)** 继续操作。在下一个主要 ASA 版本中，这些关键字将从 ASA 中删除。

对于版本 9.4(1)，所有 SSLv3 关键字都已从 ASA 配置中删除，而且 SSLv3 支持也已从 ASA 中删除。如果您启用了 SSLv3，带 SSLv3 选项的命令将出现引导时间错误。ASA 随后将恢复为默认使用 TLSv1。

Citrix Mobile Receiver 可能不支持 TLS 1.1/1.2 协议；有关兼容性，请参阅 https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-receiver-feature-matrix.pdf

字段 (Fields)

- **服务器 SSL 版本** - 指定 ASA 用作下拉列表中的服务器时其所使用的最低 SSL/TLS 协议版本。

任意	接受 SSLv2 客户端问候并协商最高通用版本。
SSL V3	接受 SSLv2 客户端问候并协商 SSLv3（或更高版本）。

SSL 设置

TLS V1	接受 SSLv2 客户端问候并协商 TLSv1（或更高版本）。
TLSV1.1	接受 SSLv2 客户端问候并协商 TLSv1.1（或更高版本）。
TLSV1.2	接受 SSLv2 客户端问候并协商 TLSv1.2（或更高版本）。
TLSV1.3	接受 SSLv2 客户端问候并协商 TLSv1.2（或更高版本）。
DTLSv1	接受 DTLSv1 客户端问候并协商 DTLSv1（或更高版本）
DTLS1.2	接受 DTLSv1.2 客户端问候并协商 DTLSv1.2（或更高版本）

注释 DTLS 的配置和使用方法仅适用于 Cisco Secure 客户端的 AnyConnect VPN 模块连接。

请使用与 DTLS 版本相等或更高版本的 TLS，确保 TLS 会话与 DTLS 会话同样安全或更安全。DTLSV1.2 支持 TLSV1.2 和 TLSV1.2。任何 TLS 版本均可与 DTLS1 配合使用，因为它们都等于或大于 DTLS 1。

TLSV1.3 需要使用 Cisco Secure 客户端版本 5.0 及更高版本。

- **Client SSL Version** - 指定 ASA 用作下拉列表中的客户端时其所使用的最低 SSL/TLS 协议版本。（DTLS 对 SSL 客户端角色不可用）

任意	传输 SSLv3 客户端问候并协商 SSLv3（或更高版本）。
SSL V3	传输 SSLv3 客户端问候并协商 SSLv3（或更高版本）。
TLS V1	传输 TLSv1 客户端问候并协商 TLSv1（或更高版本）。
TLSV1.1	传输 TLSv1.1 客户端问候并协商 TLSv1.1（或更高版本）。
TLSV1.2	传输 TLSv1.2 客户端问候并协商 TLSv1.2（或更高版本）。
TLSv1.3	传输 TLSv1.3 客户端问候并协商 TLSv1.3（或更高版本）。

- **要与 SSL 配合使用的 Diffie-Hellmann 组 (Diffie-Hellmann group to be used with SSL)** - 从下拉列表选择一个组。可用选项为 Group1 - 768 位模数、Group2 - 1024 位模数、Group5 - 1536 位模数、Group14 - 2048 位模数、224 位素数阶和 Group24 - 2048 位模数、256 位素数阶。默认值为 Group2。
- **要与 SSL 配合使用的 ECDH 组 (ECDH group to be used with SSL)** - 从下拉列表选择一个组。可用选项为 Group19 - 256 位 EC、Group20 - 384 位 EC 和 Group21 - 521 位 EC。默认值为 Group19。

SSL 设置

注释 ECDSA 和 DHE 密码具有最高优先级。

- **Encryption** - 指定您想要支持的版本、安全级别和 SSL 加密算法。点击**编辑 (Edit)**，使用“配置密码算法/自定义字符串”(Configure Cipher Algorithms/Custom String) 对话框定义或修改表项。选择 SSL 密码安全级别，然后点击**确定 (OK)**。
  - **密码版本** - 列出 ASA 支持和用于 SSL 连接的密码版本。
  - **Cipher Security Level** - 列出 ASA 支持和用于 SSL 连接的密码安全级别。选择以下选项之一：

    All 包括 NULL-SHA 等所有密码。

    Low 包括除 NULL-SHA 之外的所有密码。

    medium 包括所有密码，但 NULL-SHA、DES-CBC-SHA、RC4-MD5（这是默认密码）、RC4-SHA 和 DES-CBC3-SHA 除外。

    High 包含带有 SHA-2 加密的 AES-256，并且仅适用于 TLS 版本 1.2 和 TLS 版本 1.3 支持的密码。

    Custom 包括您在 Cipher algorithms/custom string 框中指定的一个或多个密码。此选项使您可以使用 OpenSSL 密码定义字符串对密码套件进行全面控制。
  - **Cipher Algorithms/Custom String** - 列出 ASA 支持和用于 SSL 连接的加密算法。有关使用 OpenSSL 的加密的详细信息，请参阅https://www.openssl.org/docs/manmaster/man1/ciphers.html。

    ASA 将受支持密码的优先级顺序指定为：优先级最高的是仅受 TLSv1.3/TLSv1.2 支持的密码，优先级最低的是 TLSv1.1、TLSv1.2 或 TLSv1.2 不支持的密码。

支持以下密码：

- **服务器名称指示 (SNI)** - 指定域名并与之关联。点击**添加 (Add)** 或**编辑 (Edit)**，使用“添加/编辑服务器名称指示”(Add/Edit Server Name Indication [SNI]) 对话框定义或编辑每个接口的域和信任点。

密码	TLSv1.1/DTLSV1	TLSV1.2/DTLSV1.2	TLSv1.3
TLS_AES_128_GCM_SHA256	否	否	是
TLS_CHACHA20_POLY1305_SHA256	否	否	是
AES256-GCM-SHA384	否	否	是
AES128-GCM-SHA256	否	是	否
AES128-SHA	是	是	否
AES128-SHA256	否	是	否

SSL 设置

密码	TLSv1.1/DTLSV1	TLSV1.2/DTLSV1.2	TLSv13
AES256-GCM-SHA384	否	是	否
AES256-SHA	是	是	否
AES256-SHA256	否	是	否
DERS-CBC-SHA	否	否	否
DES-CBC-SHA	是	是	否
DHE-RSA-AES128-GCM-SHA256	否	是	否
DHE-RSA-AES128-SHA	是	是	否
DHE-RSA-AES128-SHA256	否	是	否
DHE-RSA-AES256-GCM-SHA384	否	l	否
DHE-RSA-AES256-SHA	是	是	否
ECDHE-ECDSA-AES128-GCM-SHA256	否	是	否
ECDHE-ECDSA-AES128-SHA256	否	是	否
ECDHE-ECDSA-AES256-GCM-SHA384	否	是	否
ECDHE-ECDSA-AES256-SHA384	否	是	否
ECDHE-RSA-AES128-GCM-SHA256	是	是	否
ECDHE-RSA-AES128-SHA256	否	是	否
ECDHE-RSA-AES256-GCM-SHA384	否	是	否
ECDHE-RSA-AES256-SHA384	否	是	否
NULL-SHA	否	否	否
RC4-MD5	否	否	否
RC4-SHA	否	否	否

注释 DTLS1.2 隧道适用于 TLSv1.3，但 DTLS1.2 不支持 TLSv1.3 密码。为 DTLS1.2 隧道选择支持的最高优先级密码。

- Specify domain - 输入域名。

SSL 设置

  - “选择要与域关联的信任点 ”(Select trustpoint to associate with domain) - 从下拉列表选择信任点。

- **Certificates** - 为每个接口上的 SSL 身份验证分配要使用的证书。点击**编辑 (Edit)**，使用“选择 SSL 证书”(Select SSL Certificate) 对话框为每个接口定义或修改信任点。
  - “主要登记的证书”(Primary Enrolled Certificate) - 为此接口上的证书选择要使用的信任点。
  - “负载均衡登记的证书”(Load Balancing Enrolled Certificate) - 选择配置 VPN 负载均衡时用于证书的信任点。
- **回退证书 (Fallback Certificate)** - 点击以选择要用于没有关联证书的接口的证书。如果您选择**无 (None)**，则 ASA 将使用默认 RSA 密钥对和证书。
- **Forced Certification Authentication Timeout** - 配置证书身份验证超时之前等待的分钟数。
- **应用 (Apply)** - 点击以保存您的更改。
- **重置 (Reset)** - 点击以删除所做的更改并将 SSL 参数重置为之前定义的值。

SSL 设置

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。