在ISE 3.3及更高版本中配置密码

目录

简介

本文档介绍如何修改ISE 3.3及更高版本在不同服务中使用的不同密码，以便用户能够控制此类机制。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科ISE版本3.3。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

支持的密码套件

Cisco ISE支持TLS版本1.0,1.1和1.2。

从思科ISE版本3.3开始，TLS 1.3仅用于管理GUI。通过TL 1.3进行的管理HTTPS访问支持以下密码：

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

Cisco ISE支持RSA和ECDSA服务器证书。支持以下椭圆曲线：

- secp256r1
- secp384r1
- secp521r1

下表列出了支持的密码套件：

密码套件	EAP身份验证/RADIUS DTLS	从HTTPS或安全LDAP/安全系统日志通信/DTLS CoA下载CRL
ECDHE-ECDSA-AES256-GCM-SHA384	是，当允许TLS 1.1时。	是，当允许TLS 1.1时。
ECDHE-ECDSA-AES128-GCM-SHA256	是，当允许TLS 1.1时。	是，当允许TLS 1.1时。
ECDHE-ECDSA-AES256-SHA384	是，当允许TLS 1.1时。	是，当允许TLS 1.1时。
ECDHE-ECDSA-AES128-SHA256	是，当允许TLS 1.1时。	是，当允许TLS 1.1时。
ECDHE-ECDSA-AES256-SHA	是，当允许SHA-1时。	是，当允许SHA-1时。
ECDHE-ECDSA-AES128-SHA	是，当允许SHA-1时。	是，当允许SHA-1时。
ECDHE-RSA-AES256-GCM-SHA384	是，当允许ECDHE-RSA时。	Yes（如果允许ECDHE-RSA）。
ECDHE-RSA-AES128-GCM-SHA256	是，当允许ECDHE-RSA时。	是，当允许ECDHE-RSA时。
ECDHE-RSA-AES256-SHA384	是，当允许ECDHE-RSA时。	是，当允许ECDHE-RSA时。
ECDHE-RSA-AES128-SHA256	是，当允许ECDHE-RSA时。	是，当允许ECDHE-RSA时。
ECDHE-RSA-AES256-SHA	是，当允许ECDHE-RSA/SHA-1时。	是，当允许ECDHE-RSA/SHA-1时。

ECDHE-RSA-AES128-SHA	是，当允许ECDHE-RSA/SHA-1时。	是，当允许ECDHE-RSA/SHA-1时。
DHE-RSA-AES256-SHA256	无	Yes
DHE-RSA-AES128-SHA256	无	Yes
DHE-RSA-AES256-SHA	无	是，当允许SHA-1时。
DHE-RSA-AES128-SHA	无	是，当允许SHA-1时。
AES256-SHA256	Yes	Yes
AES128-SHA256	Yes	Yes
AES256-SHA	是，当允许SHA-1时。	是，当允许SHA-1时。
AES128-SHA	是，当允许SHA-1时。	是，当允许SHA-1时。
DES-CBC3-SHA	是，当允许3DES/SHA-1时。	是，当允许3DES/SHA-1时。
DHE-DSS-AES256-SHA	无	是，当启用3DES/DSS和SHA-1时。
DHE-DSS-AES128-SHA	无	是，当启用3DES/DSS和SHA-1时。
EDH-DSS-DES-CBC3-SHA	无	是，当启用3DES/DSS和SHA-1时。
RC4-SHA	当Allowed Protocols页中启用Allow weak ciphers选项并且允许SHA-1时。	无
RC4-MD5	当Allowed Protocols页中启用Allow weak ciphers选项并且允许SHA-1时。	无

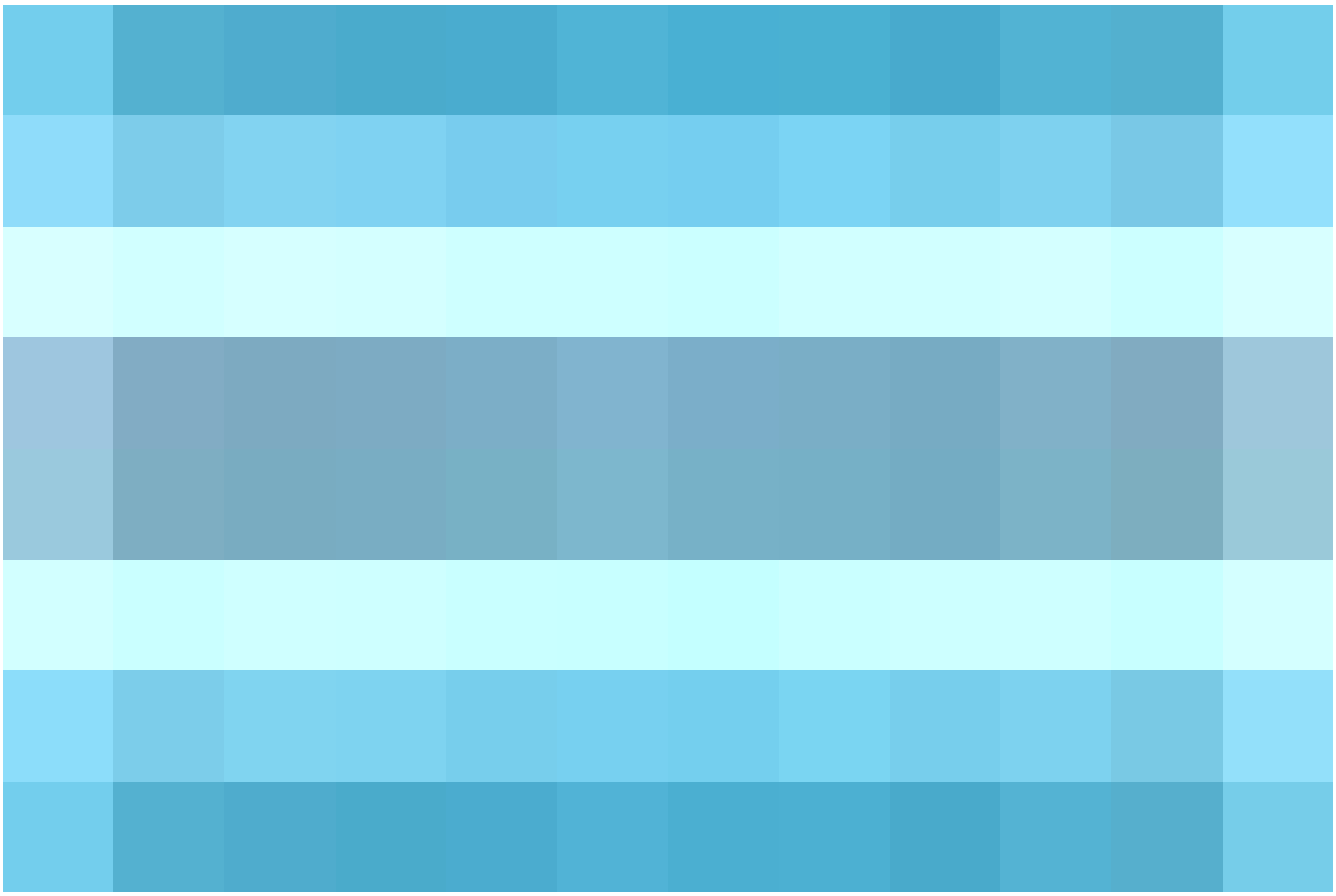
仅AP-FAST匿名调配：ADH-AES-128-SHA	Yes	无
验证密钥用法	对于以下密码，客户端证书可以具有KeyUsage=Key Agreement和ExtendedKeyUsage=Client Authentication： • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384	
验证ExtendedKeyUse	客户端证书必须对这些密码具有KeyUsage=Key Encipherment和ExtendedKeyUsage=Client Authentication： • AES256-SHA256 • AES128-SHA256 • AES256-SHA • AES128-SHA • DHE-RSA-AES128-SHA	服务器证书必须具有ExtendedKeyUsage=服务器身份验证。

配置

配置安全设置

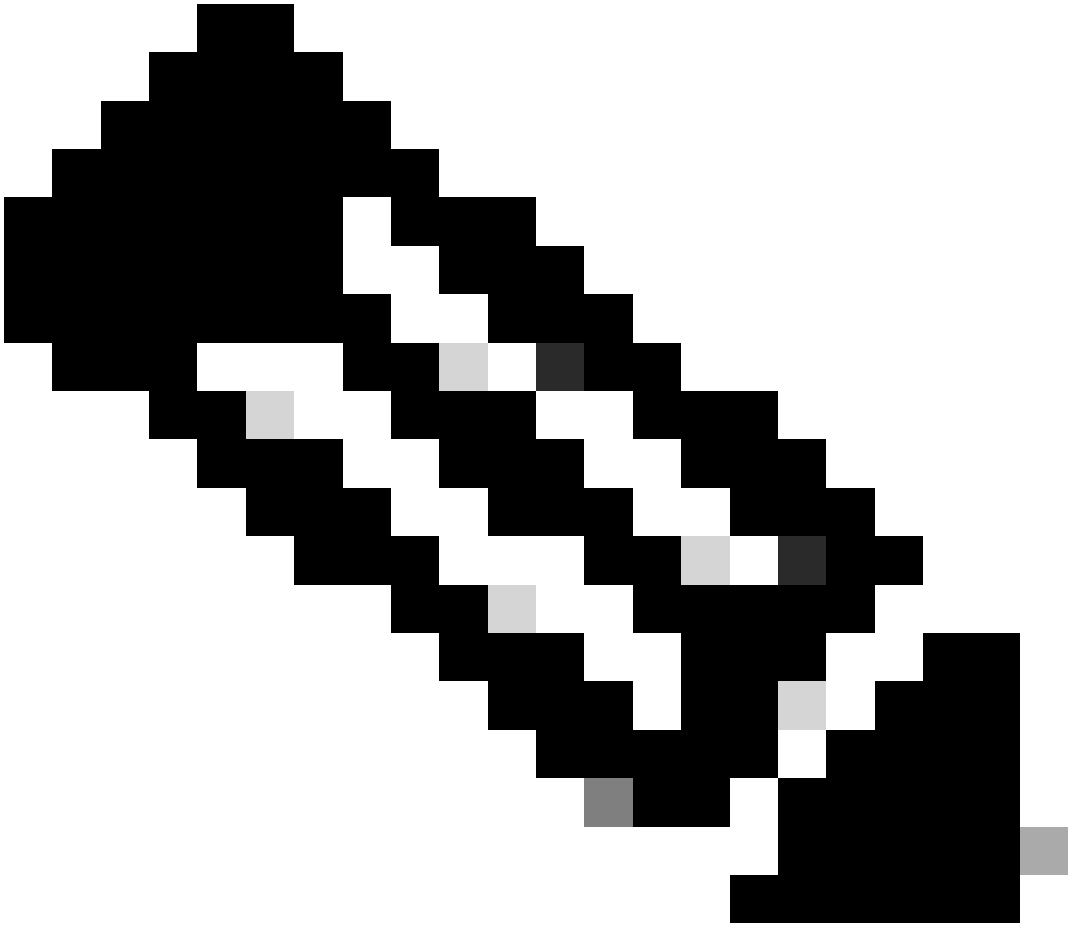
执行此过程以配置安全设置：

1. 在Cisco ISE GUI中，点击菜单图标(



)并选择Administration > System > Settings > Security Settings。

2. 在TLS版本设置部分，选择一个或多个连续的TLS版本。选中要启用的TLS版本旁边的复选框。



注意：默认情况下TLS 1.2处于启用状态，无法将其禁用。如果选择多个TLS版本，则必须选择连续版本。例如，如果您选择TLS 1.0，TLS 1.1将自动启用。更改此处的密码可能会导致ISE重新启动。

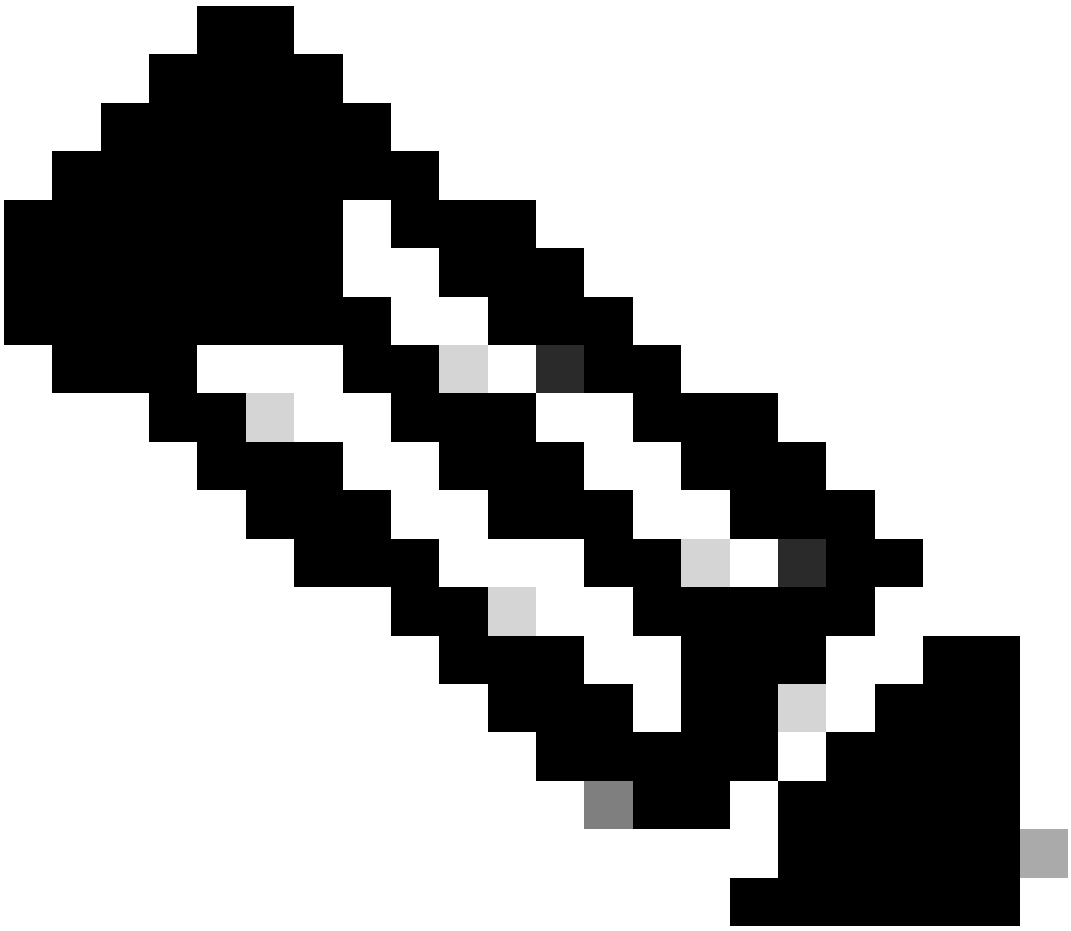
允许TLS 1.0、1.1和1.2：为下一个服务启用TLS 1.0、1.1和1.2。此外，允许SHA-1密码：允许SHA-1密码与以下工作流的对等体通信：

- EAP 身份验证.
- 从HTTPS服务器下载CRL。
- ISE和外部系统日志服务器之间的安全系统日志通信。
- ISE作为安全LDAP客户端。
- ISE作为安全ODBC客户端。
- ERS服务。
- pxGrid服务。
- 所有ISE门户（例如访客门户、客户端调配门户、我的设备门户）。
- MDM通信。
- PassiveID代理通信。

- 证书颁发机构设置。
- 管理GUI访问。

顶部列出的组件使用这些端口进行通信：

- 管理员访问权限：443
- Cisco ISE门户：9002、8443、8444、8445、8449或任何为ISE门户配置的端口。
- ERS： 9060、9061、9063
- pxGrid：8910



注意：默认情况下禁用Allow SHA-1 Ciphers选项。我们建议您使用SHA-256或SHA-384密码来增强安全性。

启用或禁用Allow SHA-1 Ciphers选项后，必须重新启动部署中的所有节点。如果重新启动不成功，则不会应用配置更改。

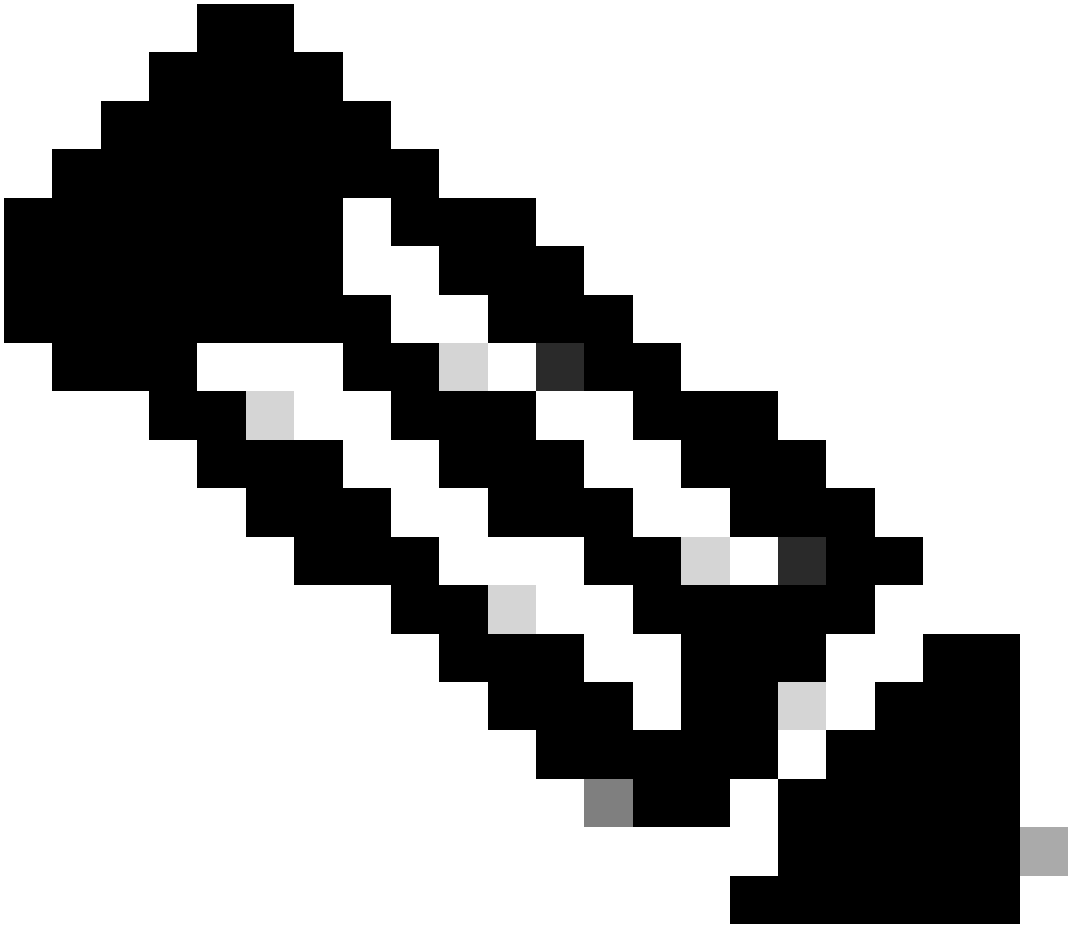
当Allow SHA-1 Ciphers选项被禁用时，如果仅使用SHA-1密码的客户端尝试连接到思科ISE，握手会失败，并且您可在客户端浏览器中看到错误消息。

选择其中一个选项，同时允许SHA-1密码与旧版对等体通信：

- Allow all SHA-1 Ciphers：允许所有SHA-1密码与旧版对等体通信。
- 仅允许TLS_RSA_WITH_AES_128_CBC_SHA：仅允许TLS_RSA_WITH_AES_128_CBC_SHA密码与旧版对等体通信。

允许TLS 1.3：允许TLS 1.3通过端口443对管理员HTTPS访问，以：

- 思科ISE管理GUI
- 为端口443启用的API（开放式API、ERS、MnT）。



注意：AAA通信和所有类型的节点间通信都不支持TLS 1.3。在思科ISE以及相关客户端和服务器上启用TLS 1.3，以便通过TLS 1.3进行管理员访问。

允许ECDHE-RSA和3DES密码：允许ECDHE-RSA密码针对以下工作流程与对等点进行通信：

- 思科ISE配置为EAP服务器
- 思科ISE配置为RADIUS DTLS服务器
- 思科ISE配置为RADIUS DTLS客户端
- 思科ISE从HTTPS或安全LDAP服务器下载CRL
- 思科ISE配置为安全系统日志客户端
- 思科ISE配置为安全LDAP客户端

允许ISE的DSS密码作为客户端：当Cisco ISE作为客户端时，允许DSS密码与服务器进行以下工作流程通信：

- 思科ISE配置为RADIUS DTLS客户端
- 思科ISE从HTTPS或安全LDAP服务器下载CRL
- 思科ISE配置为安全系统日志客户端
- 思科ISE配置为安全LDAP客户端

允许将ISE作为客户端的传统不安全TLS重新协商：允许与不支持这些工作流的安全TLS重新协商的传统TLS服务器进行通信：

- 思科ISE从HTTPS或安全LDAP服务器下载CRL
- 思科ISE配置为安全系统日志客户端
- 思科ISE配置为安全LDAP客户端

披露无效用户名：默认情况下，由于用户名不正确，思科ISE显示身份验证失败的无效消息。为了帮助调试，此选项强制Cisco ISE在报告中显示用户名，而不是无效消息。请注意，对于不是由于用户名不正确而导致的身份验证失败，始终显示用户名。

Active Directory、内部用户、LDAP和ODBC身份源支持此功能。不支持其他身份源，例如RADIUS令牌、RSA或SAML。

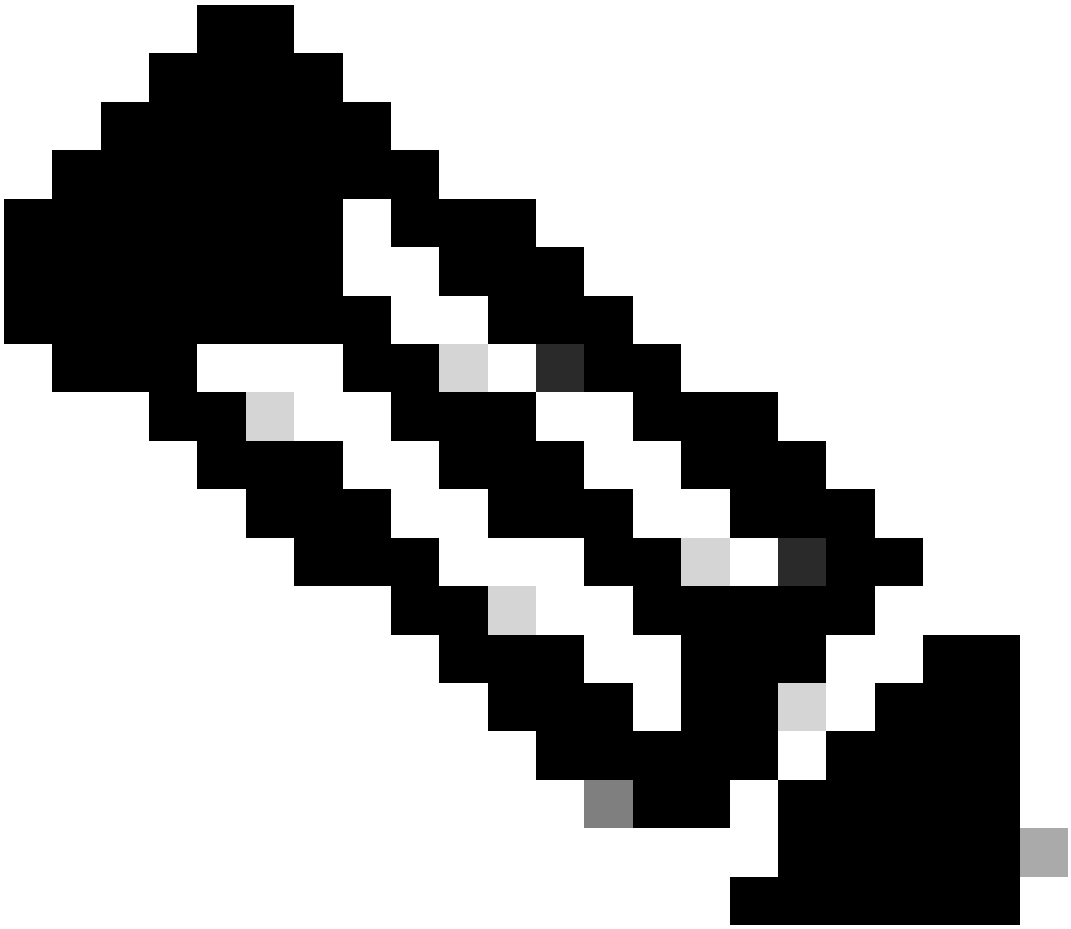
使用基于FQDN的证书与第三方供应商(TC-NAC)通信：基于FQDN的证书必须遵守以下规则：

- 证书中的SAN和CN字段必须包含FQDN值。不支持主机名和IP地址。
- 通配符证书必须仅在最左侧的片段中包含通配符。
- 证书中提供的FQDN必须是DNS可解析的。

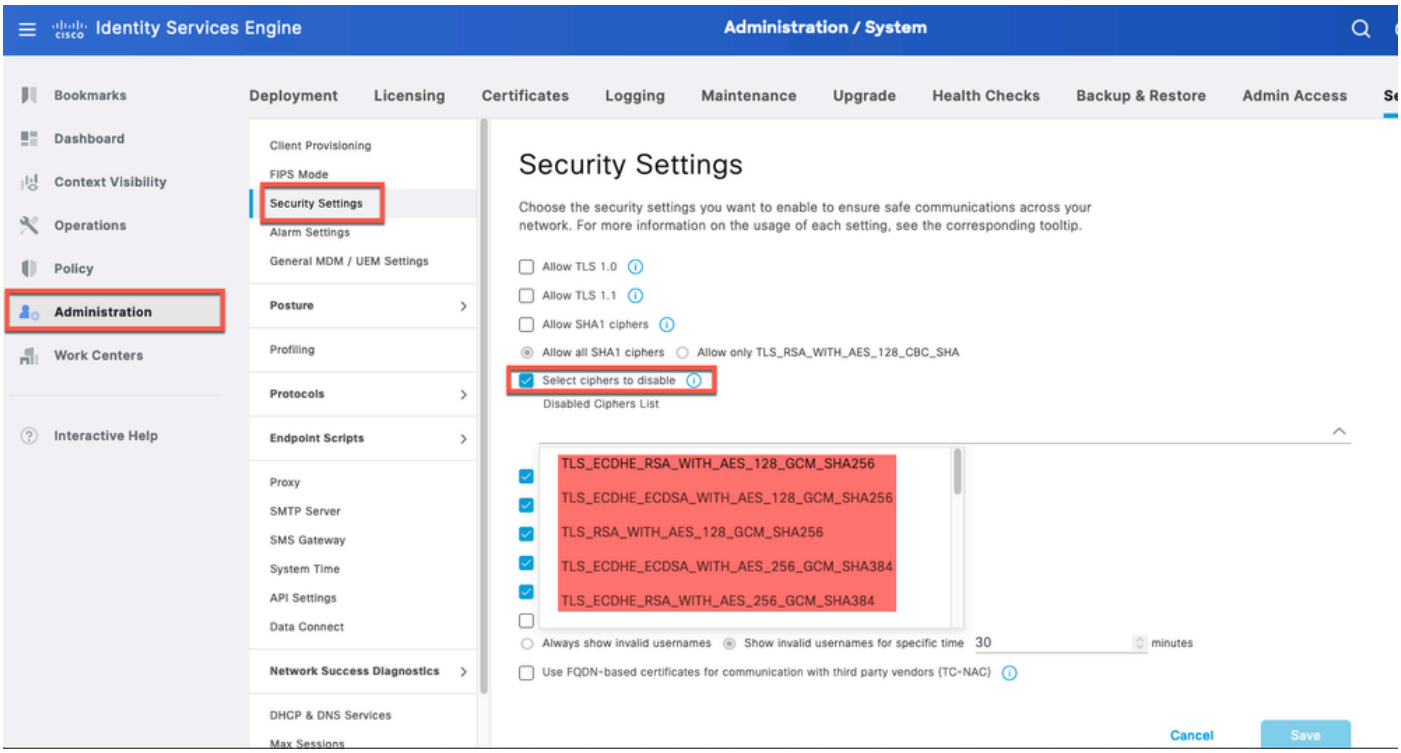
禁用特定密码

如果要手动配置密码以便与以下Cisco ISE组件通信，请选中Manually Configure Ciphers List选项

：admin UI、ERS、OpenAPI、secure ODBC、门户和pxGrid。将显示密码列表，其中已选定允许的密码。例如，如果启用Allow SHA1 Ciphers选项，则在此列表中启用SHA1密码。如果选择了Allow Only TLS_RSA_WITH_AES_128_CBC_SHA选项，则此列表中只会启用此SHA1加密器。如果Allow SHA1 Ciphers选项已禁用，则无法在此模式下启用任何SHA1密码



注：当您编辑要禁用的密码列表时，应用服务器在所有思科ISE节点上重新启动。当启用或禁用FIPS模式时，所有节点上的应用服务器都会重新启动，从而导致系统严重停机。如果已使用手动配置密码列表选项禁用了任何密码，请在重新启动应用程序服务器后检查已禁用的密码列表。由于FIPS模式转换，禁用密码列表未更改。



用于禁用密码ISE 3.3的选项

- 从ISE CLI中，您可以运行application configure ise命令并使用选项37，在此屏幕截图中突出显示**EAP-TLS的RSA_PSS签名的启用/禁用/当前状态。相关的漏洞是思科漏洞ID** CSCwb77915。

```
isedemo-33/admin#application configure ise

Selection configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[19]Establish Trust with controller
[20]Reset Context Visibility
[21]Synchronize Context Visibility With Database
[22]Generate Heap Dump
[23]Generate Thread Dump
[24]Force Backup Cancellation
[25]CleanUp ESR 5921 IOS Crash Info Files
[26]Recreate undotablespace
[27]Reset Upgrade Tables
[28]Recreate Temp tablespace
[29]Clear Sysaux tablespace
[30]Fetch SGA/PGA Memory usage
[31]Generate Self-Signed Admin Certificate
[32]View Certificates in NSSDB or CA_NSSDB
[33]Recreate REPLOGNS tablespace
[34]View Native IPSec status
[35]Enable/Disable/Current_status of Audit-Session-ID Uniqueness
[37]Enable/Disable/Current_status of RSA_PSS signature for EAP-TLS
```

用于为*EAP-TLS*禁用/启用*RSA_PSS*的选项

相关信息

-

思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。