Configure Ciphers in ISE 3.3 and Later

Contents

Introduction

This document describes how to modify the different ciphers used by ISE 3.3 and later in different service so user have control over such mechanisms.

Prerequisites

Requirements

There are no specific requirements for this document.

Component Used

The information in this document is based on these software and hardware versions:

- Cisco ISE version 3.3.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Supported Cipher Suites

Cisco ISE supports TLS versions 1.0,1.1 and 1.2.

From Cisco ISE Release 3.3, TLS 1.3 was introduced for Admin GUI only. These ciphers are supported for admin HTTPS access over TL 1.3 :

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

Cisco ISE supports RSA and ECDSA server certificates. These elliptic curves are supported:

- secp256r1
- secp384r1

- secp521r1

This table lists the supported Cipher Suites:

Cipher Suite	**EAP Authentication/RADIUS DTLS**	**CRL Download from HTTPS or Secure LDAP/Secure Syslog communication/DTLS CoA**
ECDHE-ECDSA-AES256-GCM-SHA384	Yes, when TLS 1.1 is allowed.	Yes, when TLS 1.1 is allowed.
ECDHE-ECDSA-AES128-GCM-SHA256	Yes, when TLS 1.1 is allowed.	Yes, when TLS 1.1 is allowed.
ECDHE-ECDSA-AES256-SHA384	Yes, when TLS 1.1 is allowed.	Yes, when TLS 1.1 is allowed.
ECDHE-ECDSA-AES128-SHA256	Yes, when TLS 1.1 is allowed.	Yes, when TLS 1.1 is allowed.
ECDHE-ECDSA-AES256-SHA	Yes, when SHA-1 is allowed.	Yes, when SHA-1 is allowed.
ECDHE-ECDSA-AES128-SHA	Yes, when SHA-1 is allowed.	Yes, when SHA-1 is allowed.
ECDHE-RSA-AES256-GCM-SHA384	Yes, when ECDHE-RSA is allowed.	Yes when ECDHE-RSA is allowed.
ECDHE-RSA-AES128-GCM-SHA256	Yes, when ECDHE-RSA is allowed.	Yes, when ECDHE-RSA is allowed.
ECDHE-RSA-AES256-SHA384	Yes, when ECDHE-RSA is allowed.	Yes, when ECDHE-RSA is allowed.
ECDHE-RSA-AES128-SHA256	Yes, when ECDHE-RSA is allowed.	Yes, when ECDHE-RSA is allowed.
ECDHE-RSA-AES256-SHA	Yes, when ECDHE-RSA/SHA-1 is allowed.	Yes, when ECDHE-RSA/SHA-1 is allowed.
ECDHE-RSA-AES128-SHA	Yes, when ECDHE-RSA/SHA-1 is allowed.	Yes, when ECDHE-RSA/SHA-1 is allowed.

DHE-RSA-AES256-SHA256	No	Yes
DHE-RSA-AES128-SHA256	No	Yes
DHE-RSA-AES256-SHA	No	Yes, when SHA-1 is allowed.
DHE-RSA-AES128-SHA	No	Yes, when SHA-1 is allowed.
AES256-SHA256	Yes	Yes
AES128-SHA256	Yes	Yes
AES256-SHA	Yes, when SHA-1 is allowed.	Yes, when SHA-1 is allowed.
AES128-SHA	Yes, when SHA-1 is allowed.	Yes, when SHA-1 is allowed.
DES-CBC3-SHA	Yes, when 3DES/SHA-1 is allowed.	Yes, when 3DES/SHA-1 is allowed.
DHE-DSS-AES256-SHA	No	Yes, when 3DES/DSS and SHA-1 are enabled.
DHE-DSS-AES128-SHA	No	Yes, when 3DES/DSS and SHA-1 are enabled.
EDH-DSS-DES-CBC3-SHA	No	Yes, when 3DES/DSS and SHA-1 are enabled.
RC4-SHA	When the **Allow weak ciphers** option is enabled in the **Allowed Protocols** page and when SHA-1 is allowed.	No
RC4-MD5	When the **Allow weak ciphers** option is enabled in the **Allowed Protocols** page and when SHA-1 is allowed.	No
AP-FAST anonymous provisioning only: ADH-AES-128-SHA	Yes	No

Validate KeyUsage	Client certificate can have KeyUsage=Key Agreement and ExtendedKeyUsage=Client Authentication for these ciphers: • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384	
Validate ExtendedKeyUsage	Client certificate must have KeyUsage=Key Encipherment and ExtendedKeyUsage=Client Authentication for these ciphers: • AES256-SHA256 • AES128-SHA256 • AES256-SHA • AES128-SHA • DHE-RSA-AES128-SHA	Server certificate must have ExtendedKeyUsage=Server Authentication.

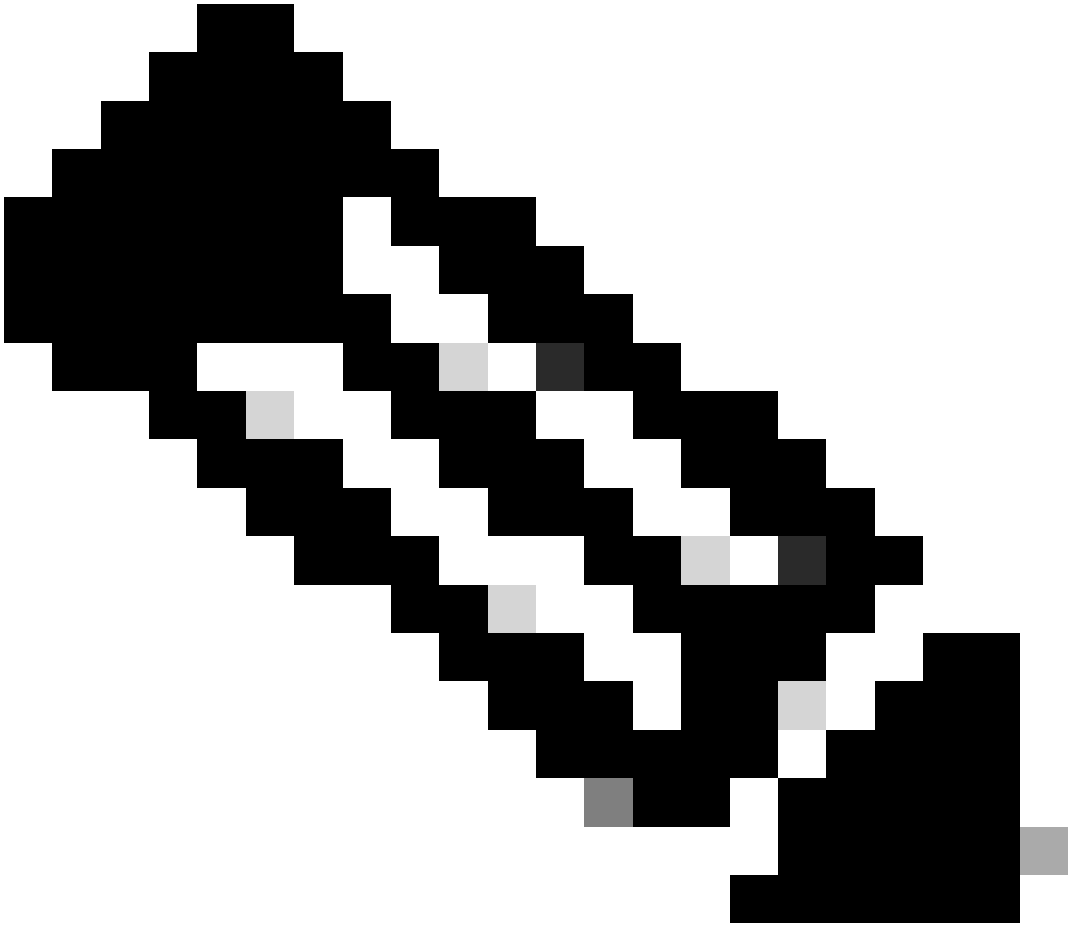
Configurations

Configure Security Settings

Perform this procedure to configure the security settings:

1. In the Cisco ISE GUI, click the menu icon ( ) and choose **Administration > System > Settings > Security Settings**.

2. In the **TLS Versions Settings** section, choose one or a range of consecutive TLS versions. Check the check box next to the TLS versions that you want to enable.



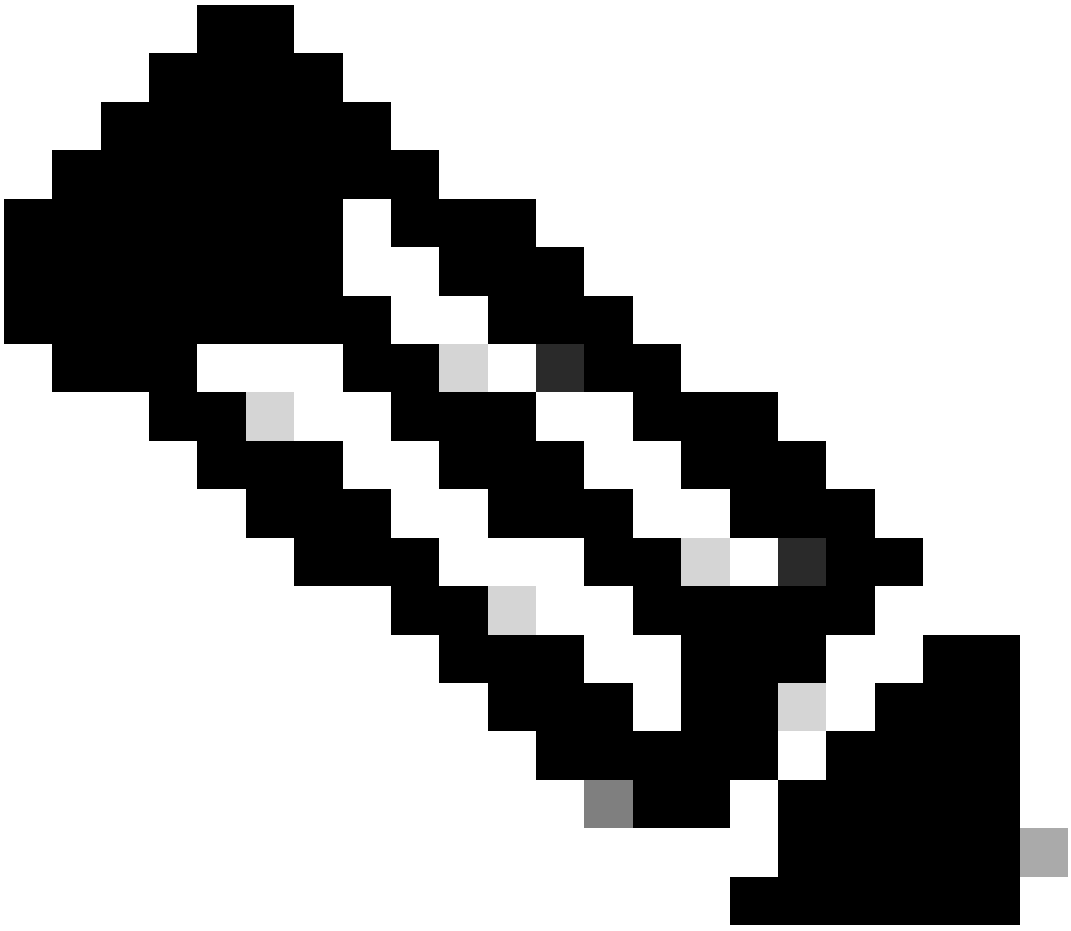
Note: **TLS 1.2** is enabled by default and cannot be disabled. If you choose more than one TLS version, you must choose consecutive versions. For example, if you choose **TLS 1.0**, **TLS 1.1** is automatically enabled. Changing the ciphers here can cause restart of ISE.

Allow TLS 1.0, 1.1 and 1.2: Enables TLS 1.0,1.1 and 1.2 for the next services. Also, allow SHA-1 Ciphers: Allows SHA-1 ciphers to communicate with peers for these workflows:

- EAP Authentication.
- CRL download from HTTPS server.
- Secure Syslog communication between ISE and external syslog server.
- ISE as a secure LDAP client.
- ISE as a secure ODBC client.
- ERS services.
- pxGrid services.
- All ISE Portals (E.g Guest Portal, Client Provisioning Portal, MyDevices Portal).
- MDM Communication.
- PassiveID Agent communication.
- Certificate Authority provisionin.
- Admin GUI Access.

These ports are used by the components listed on top for communication:

- Admin Access: 443
- Cisco ISE Portals: 9002, 8443, 8444, 8445, 8449 or any ports configured for ISE portals.
- ERS: 9060, 9061, 9063
- pxGrid: 8910



> **Note**: The **Allow SHA-1 Ciphers** option is disabled by default. We recommend that you use SHA-256 or SHA-384 ciphers for enhanced security.

You must restart all the nodes in a deployment after enabling or disabling the **Allow SHA-1 Ciphers** option. If restart is not successful, the configuration changes are not applied.

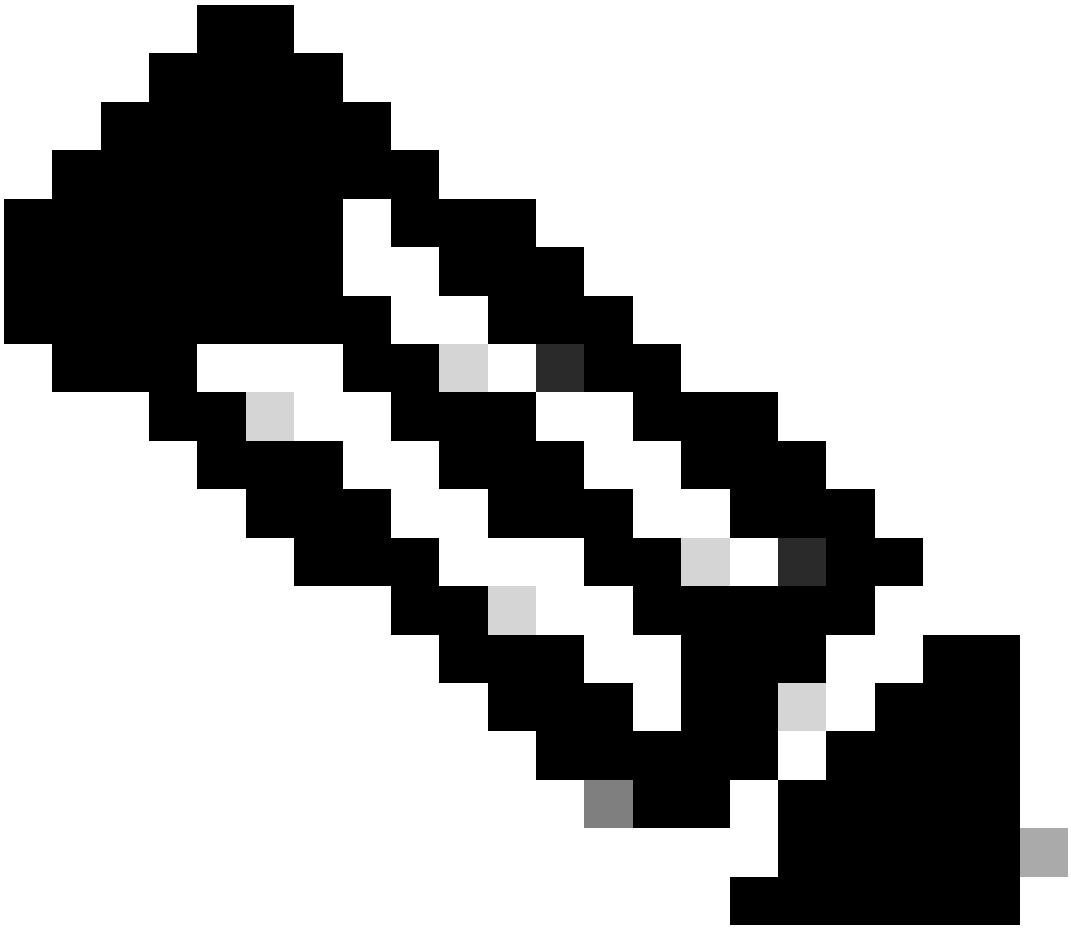
When the **Allow SHA-1 Ciphers** option is disabled, if a client with only SHA-1 ciphers tries to connect to Cisco ISE, the handshake fails, and you can see an error message on the client browser.

Choose one of the options while allowing SHA-1 ciphers to communicate with legacy peers:

- **Allow all SHA-1 Ciphers**: Allows all SHA-1 ciphers to communicate with legacy peers.
- **Allow only TLS_RSA_WITH_AES_128_CBC_SHA**: Allows only TLS_RSA_WITH_AES_128_CBC_SHA cipher to communicate with legacy peers.

Allow TLS 1.3: Allows TLS 1.3 for administrator HTTPS access over port 443 for:

- Cisco ISE Admin GUI
- APIs enabled for port 443 (Open API, ERS, MnT).



Note: AAA communications and all types of internode communications do not support TLS 1.3. Enable TLS 1.3 on Cisco ISE and the relevant clients and servers for admin access over TLS 1.3.

Allow ECDHE-RSA and 3DES Ciphers: Allows ECDHE-RSA ciphers to communicate with peers for these workflows:

- Cisco ISE is configured as an EAP server
- Cisco ISE is configured as a RADIUS DTLS server

- Cisco ISE is configured as a RADIUS DTLS client
- Cisco ISE downloads CRL from HTTPS or a secure LDAP server
- Cisco ISE is configured as a secure syslog client
- Cisco ISE is configured as a secure LDAP client

Allow DSS ciphers for ISE as a client: when Cisco ISE acts as a client, allows DSS ciphers to communicate with a server for these workflows:

- Cisco ISE is configured as a RADIUS DTLS client
- Cisco ISE downloads CRL from HTTPS or a secure LDAP server
- Cisco ISE is configured as a secure syslog client
- Cisco ISE is configured as a secure LDAP client

Allow Legacy Unsafe TLS Renegotiation for ISE as a Client: Allows communication with legacy TLS servers that do not support safe TLS renegotiation for these workflows:

- Cisco ISE downloads CRL from HTTPS or a secure LDAP server
- Cisco ISE is configured as a secure syslog client
- Cisco ISE is configured as a secure LDAP client

Disclose invalid usernames: by default, Cisco ISE displays the invalid message for authentication failures because of incorrect usernames. To aid in debugging, this option forces Cisco ISE to display usernames in reports, instead of the invalid message. Notice that usernames are always displayed for failed authentications that are not because of incorrect usernames.

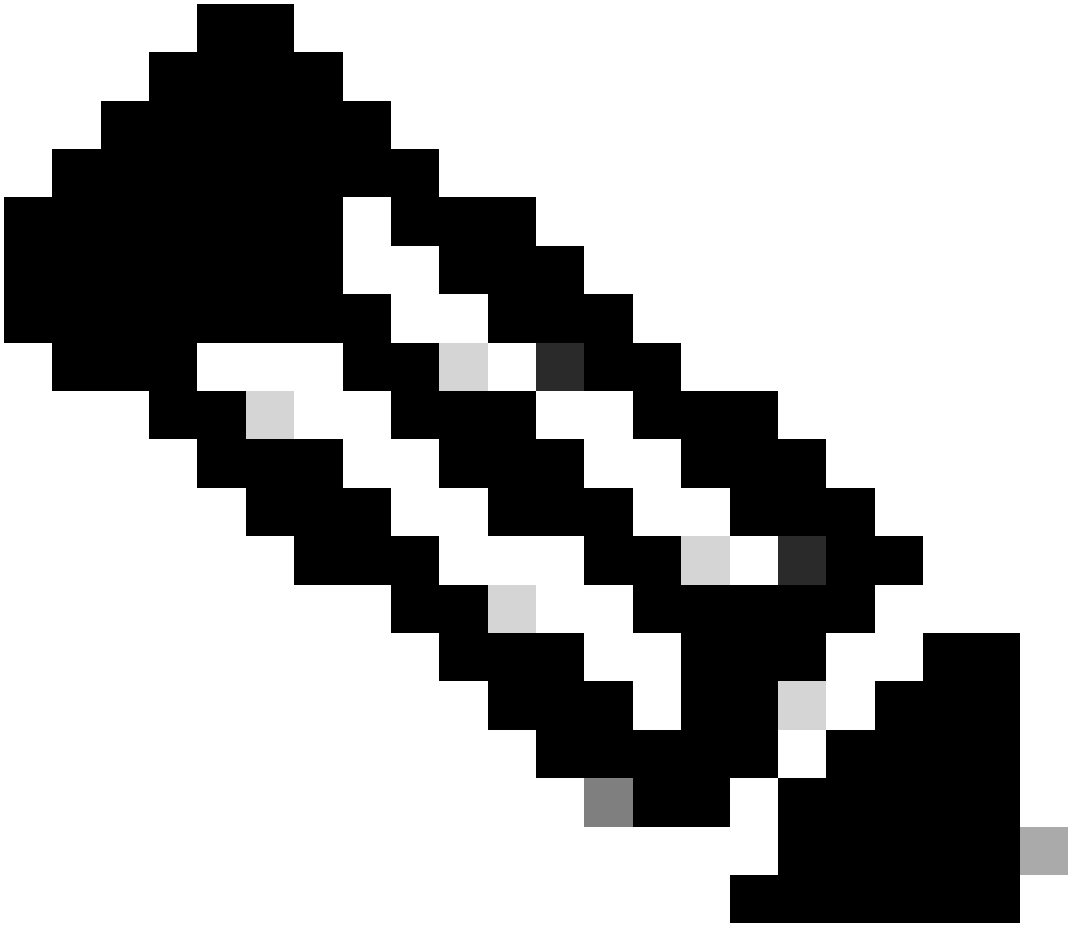
This feature is supported for Active Directory, Internal Users, LDAP, and ODBC identity sources. It is not supported for other identity sources, such as RADIUS token, RSA, or SAML.

Use FQDN-based certificates for communication with third party vendors (TC-NAC): FQDN-based certificates must comply with these rules:

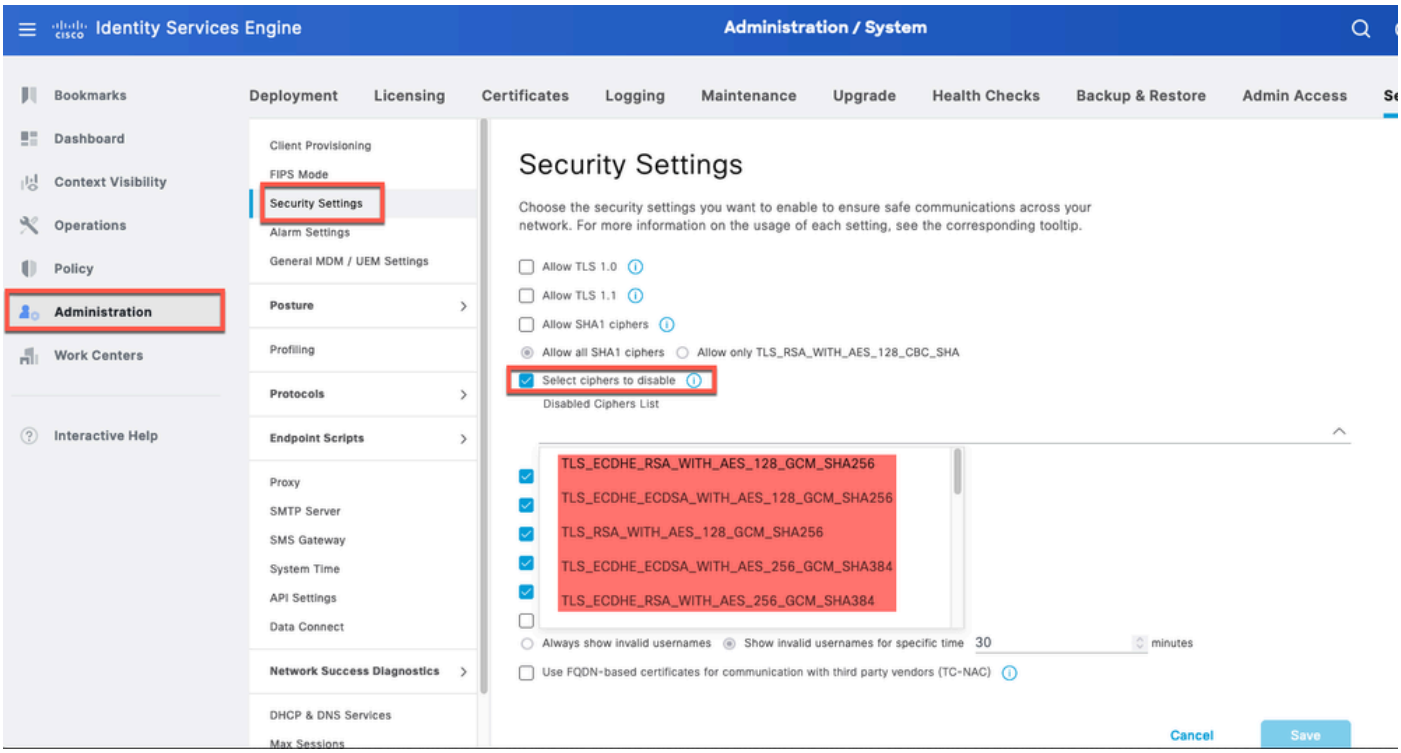
- The SAN and CN fields in the certificate must contain FQDN values. Hostnames and IP addresses are not supported.
- Wildcard certificates must contain the wildcard character only in the far-left fragment.
- The FQDN provided in a certificate must be DNS resolvable.

Disable Specific Ciphers

Check the **Manually Configure Ciphers List** option if you want to manually configure ciphers to communicate with these Cisco ISE components: admin UI, ERS, OpenAPI, secure ODBC, portals, and pxGrid. A list of ciphers is displayed with allowed ciphers already selected. For example, if the **Allow SHA1 Ciphers** option is enabled, SHA1 ciphers are enabled in this list. If the **Allow Only TLS_RSA_WITH_AES_128_CBC_SHA** option is selected, only this SHA1 cipher is enabled in this list. If the **Allow SHA1 Ciphers** option is disabled, you cannot enable any SHA1 cipher in this



Note: When you edit the list of ciphers to be disabled, the application server restarts on all the Cisco ISE nodes. When the FIPS mode is enabled or disabled, application servers on all the nodes are restarted resulting in significant system downtime. If you have disabled any ciphers using the **Manually Configure Ciphers List** option, check the list of disabled ciphers after the application servers are restarted. The disabled ciphers list is not changed because of FIPS mode transition.



Option to Disable Ciphers ISE 3.3

- From ISE CLI you can run the command application configure iseand use Option 37, highlighted in this screenshot, **Enable/Disable/Current_status of RSA_PSS signature for EAP-TLS**. The related bug is Cisco bug 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
```

Option to Disable/Enable RSA_PSS for EAP-TLS

Related Information

- Cisco Technical Support & Downloads