

# Configure Controlled Application Restart in ISE 3.3

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Background Information](#)

### [Configure](#)

[Step 1. Create a Certificate Signing Request \(CSR\)](#)

[Step 2. Import the Root CA that Signed your CSR](#)

[Step 3. Import the Signed CSR](#)

[Step 4. Configure the Restart Time](#)

### [Verify](#)

### [Troubleshoot](#)

### [Related Information](#)

---

## Introduction

This document describes how to configure The Controlled Application Restart for the Admin certificate in ISE 3.3.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- ISE nodes/personas
- ISE certificate renewal/edit/creation

### Components Used

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

- Identity Service Engine (ISE) software version 3.3
- 2 node deployment

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.

## Background Information

In ISE, when the Admin certificate of the Primary Admin Node (PAN) is changed, all the nodes in the deployment are reloaded, first the PAN and then the rest of nodes, and this causes a disruption in all the services.

When the Admin certificate is replaced in any other node, the only node that is restarted is that single node.

ISE 3.3 introduces a new feature that allows you to schedule when the nodes reload. This provides a better control over the restart of each node, and it helps to avoid disruption in all the services.

## Configure

There are different options to change the Admin certificate of the PAN node like:

- Create Certificate Signing Request (CSR) and assigning the Admin role.
- Import certificate, private key and assigning the Admin role.
- Create Self-signed certificate and assigning the Admin role.

This document describes the method using a CSR.

### Step 1. Create a Certificate Signing Request (CSR)

1. On ISE, navigate to **Administration > System > Certificates > Certificate Signing Requests**.
2. Click **Generate Certificate Signing Request (CSR)**.
3. In **Usage**, select **Admin**.
4. In **Node(s)**, select the **Primary Admin** node.
5. Complete the certificate information.
6. Click **Generate**.
7. Export the file and sign it with a valid authority.

Deployment    Licensing    **Certificates**    Logging    Maintenance    Upgrade    Health Checks

**Certificate Management** ▾

- System Certificates
- Admin Certificate Node Restart
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests**
- Certificate Periodic Check Se...

---

**Certificate Authority** >

**ISE Certificate Authority Certificates:**

- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root C
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to i

**Usage**

Certificate(s) will be used for **Admin** ▾

Allow Wildcard Certificates  ⓘ

**Node(s)**

Generate CSR's for these Nodes:

| Node  | CSR Friendly Name     |
|---|-----------------------|
| <input type="checkbox"/> asc-ise33-1037             | asc-ise33-1037#Admin  |
| <input checked="" type="checkbox"/> ██████-ise-33-2 | ██████-ise-33-2#Admin |

**Subject**

Common Name (CN)  
\$FQDN\$ ⓘ

---

Organizational Unit (OU) ⓘ

---

Organization (O)  
TAC ⓘ

CSR Creation

## Step 2. Import the Root CA that Signed your CSR

1. On ISE, navigate to **Administration > System > Certificates > Trusted Certificates**.
2. Click **Import**.
3. Click **Choose File** and select the **Root CA certificate**.
4. Write a **Friendly Name**.
5. Enable the checkboxes:
  1. **Trust for authentication within ISE**.
  2. **Trust for authentication of Cisco Services**.
6. Click **Submit**.

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Certificate Management
 

- System Certificates
- Admin Certificate Node Restart
- Trusted Certificates**
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Se...

Certificate Authority

### Import a new Certificate into the Certificate Store

\* Certificate File **Choose File** No file chosen

Friendly Name **Root-CA**

Trusted For:
 

- Trust for authentication within ISE
- Trust for client authentication and Syslog
- Trust for certificate based admin authentication
- Trust for authentication of Cisco Services
- Trust for Native IPsec certificate based authentication
- Validate Certificate Extensions

Description

**Submit** Cancel

*Import Root Certificate*

### Step 3. Import the Signed CSR

1. On ISE, navigate to **Administration > System > Certificates > Certificate Signing Requests**.
2. Select the CSR and click **Bind Certificate**.
3. Click **Choose file** and select the **signed certificate**.
4. Configure a **Friendly Name**.

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore

Certificate Management
 

- System Certificates
- Admin Certificate Node Restart
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests**
- Certificate Periodic Check Se...

Certificate Authority

## Certificate Signing Requests

**Generate Certificate Signing Requests (CSR)**

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate. Once bound, it will be removed from this list.

View Export Delete **Bind Certificate**

| <input type="checkbox"/>            | Friendly Name         | Certificate Subject | Key Length | Pr... |
|-------------------------------------|-----------------------|---------------------|------------|-------|
| <input checked="" type="checkbox"/> | <b>ise-33-2#Admin</b> | CN=ise-33-2.a...    | 4096       |       |

*Bind Certificate*

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access

**Certificate Management** ▼

- System Certificates
- Admin Certificate Node Restart
- Trusted Certificates
- OCSF Client Profile
- Certificate Signing Requests**
- Certificate Periodic Check Se...

**Certificate Authority** >

### Bind CA Signed Certificate

\* Certificate File  signed.cer

Friendly Name  ⓘ

Validate Certificate Extensions  ⓘ

Usage

Admin: Use certificate to authenticate the ISE Admin Portal and DataConnect

### Deployment Nodes

[Set Restart Time](#)

| <input type="checkbox"/> | Hostname       | Personas                 | Role(s)   | Services         | Restart Time   | Restart Status |
|--------------------------|----------------|--------------------------|-----------|------------------|----------------|----------------|
| <input type="checkbox"/> | asc-ise33-1037 | Administration, Monit... | SECONDARY | SESSION,PROFILER | Not Configured |                |
| <input type="checkbox"/> | ise-33-2       | Administration, Monit... | PRIMARY   | SESSION,PROFILER | Not Configured |                |

*Bind Certificate*

## Step 4. Configure the Restart Time

1. Now you can see a new section. Here you configure the restart process.
2. You can configure a time per node or select both nodes and apply the same configuration.
3. Choose **one node** and click **Set Restart Time**.
4. Choose the **date, time** and click **Save**.
5. Verify the Time and if everything is correct, click **Submit**.

# Set Restart Time

## Scheduler

Restart Now  Restart Later

Set Date

27/09/2023

Set Time

11:00  PM

cancel

save

Set Restart Time

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access

Certificate Management

- System Certificates
- Admin Certificate Node Restart
- Trusted Certificates
- OCSF Client Profile
- Certificate Signing Requests**
- Certificate Periodic Check Se...

Certificate Authority

### Bind CA Signed Certificate

\* Certificate File  signed.cer

Friendly Name  ⓘ

Validate Certificate Extensions  ⓘ

Usage

Admin: Use certificate to authenticate the ISE Admin Portal and DataConnect

#### Deployment Nodes

| <input type="checkbox"/>            | Hostname       | Personas                 | Role(s)   | Services         | Restart Time            |
|-------------------------------------|----------------|--------------------------|-----------|------------------|-------------------------|
| <input checked="" type="checkbox"/> | asc-ise33-1037 | Administration, Monit... | SECONDARY | SESSION,PROFILER | Wed Sep 27 2023 11:00PM |
| <input type="checkbox"/>            | ise-33-2       | Administration, Monit... | PRIMARY   | SESSION,PROFILER | Wed Sep 27 2023 10:00PM |

Confirm Restart Time

## Verify

New tab is available, navigate to **Administration > System > Certificates > Admin Certificate Node Restart**. You can validate the configuration done and change it if needed.

To change it, click **Set Restart Time** or **Restart Now**.

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Certificate Management  
System Certificates  
**Admin Certificate Node Rest...**  
Trusted Certificates  
OCSP Client Profile  
Certificate Signing Requests  
Certificate Periodic Check Se...

### Admin Certificate Node Restart

After you add or edit an admin usage certificate on the primary PAN, you must restart all the Cisco ISE nodes. In this window, you can schedule and monitor the status of the node restarts. If more than one node is configured for Restart Now , nodes will restart in sequence

[Set Restart Time](#) [Restart Now](#) All

| <input type="checkbox"/> | Hostname       | Personas                     | Role(s)   | Services         | Restart Time            | Restart Status |
|--------------------------|----------------|------------------------------|-----------|------------------|-------------------------|----------------|
| <input type="checkbox"/> | asc-ise33-1037 | Administration, Monitorin... | SECONDARY | SESSION,PROFILER | Wed Sep 27 2023 10:00PM | Not Restarted  |
| <input type="checkbox"/> | asc-ise33-2    | Administration, Monitorin... | PRIMARY   | SESSION,PROFILER | Wed Sep 27 2023 10:00PM | Not Restarted  |

*Verify Restart Status*

You can validate the node status during the process. The next image is an example when one node reloaded and the other is in progress:

Certificate Management  
System Certificates  
**Admin Certificate Node Rest...**  
Trusted Certificates  
OCSP Client Profile  
Certificate Signing Requests  
Certificate Periodic Check Se...

### Admin Certificate Node Restart

After you add or edit an admin usage certificate on the primary PAN, you must restart all the Cisco ISE nodes. In this window, you can schedule and monitor the status of the node restarts. If more than one node is configured for Restart Now , nodes will restart in sequence

[Set Restart Time](#) [Restart Now](#) All

| <input type="checkbox"/> | Hostname       | Personas                     | Role(s)   | Services          | Restart Time            | Restart Status      |
|--------------------------|----------------|------------------------------|-----------|-------------------|-------------------------|---------------------|
| <input type="checkbox"/> | asc-ise33-2    | Administration, Monitorin... | PRIMARY   | SESSION,PROFIL... | Wed Sep 27 2023 10:00PM | Restart success     |
| <input type="checkbox"/> | asc-ise33-1037 | Administration, Monitorin... | SECONDARY | SESSION,PROFIL... | Wed Sep 27 2023 10:00PM | Restart in progress |

*PAN Restarted*

Verify the changes and reload with the reports.

To check the configuration changes, navigate to **Operations > Reports > Reports > Audit > Change Configuration Audit**.

| Logged At                | Administrator | Server   | Interface | Object Type                          | Object Name               | Event                       |
|--------------------------|---------------|----------|-----------|--------------------------------------|---------------------------|-----------------------------|
| Today                    | admin         | Server   |           | Object Type                          | Object Name               |                             |
| 2023-09-27 15:43:00.0... | admin         | ise-33-2 | GUI       | Admin Certificate Controlled Restart | asc-ise33-1037.aaame...   | Changed configuration       |
| 2023-09-27 15:26:57.9... | admin         | ise-33-2 | GUI       | Admin Certificate Controlled Restart | asc-ise33-1037.aaame...   | Added configuration         |
| 2023-09-27 15:26:57.5... | admin         | ise-33-2 | GUI       | CertificateBinding                   | BindCertificate           | Added configuration         |
| 2023-09-27 14:38:01.6... | admin         | ise-33-2 | GUI       | Certificate Signing Request          | ise-33-2#Admin            | Certificate has been exp... |
| 2023-09-27 14:37:58.8... | admin         | ise-33-2 | GUI       | CertificateSigningRequest            | CertificateSigningRequest | Added configuration         |

Configuration Report

To check the restart, navigate to **Operations > Reports > Reports > Audit > Operations Audit**.

| Logged At                | Administrator | Server    | Interface | Object Type           | Object Name         | Event                      |
|--------------------------|---------------|-----------|-----------|-----------------------|---------------------|----------------------------|
| 2023-09-27 22:04:20.0... |               |           | CLI       | Configuration-Changes |                     | Added configuration        |
| 2023-09-27 22:04:20.0... |               |           | CLI       | Configuration-Changes |                     | Added configuration        |
| 2023-09-27 22:00:16.16   | system        | 127.0.0.1 | CLI       | Process-Management    | ISE process stopped | Application server stopped |

Restart Report

Sample logs from `***-ise-33-2, ise-psc.log`:

<#root>

**Configuration applied:**

```
2023-09-27 15:26:12,109 INFO [DefaultQuartzScheduler_Worker-6][[]] admin.caservice.certmgmt.scheduler.
Restart is Not configured , Hence skipping restart status check for asc-ise33-1037
2023-09-27 15:26:57,775 INFO [admin-http-pool6][[]] cpm.admin.infra.action.RestartAction --:admin:::
adminCertRestartData received --{"items":[{"hostName":"asc-ise33-1037","restartTime":"2023-09-27:10:00PM"},
{"hostName":"***-ise-33-2","restartTime":"2023-09-27:10:00PM"}]}
```

**Restart starts:**

```
2023-09-27 21:59:11,952 INFO [DefaultQuartzScheduler_Worker-6][[]] admin.caservice.certmgmt.scheduler.
Executing AdminCertControlledRestartStatusJob [AdminCertControlledRestart[id=4af7d9c4-31d9-48e0-83dc-19
noderestartconfig=2023-09-27:10:00PM,noderestartstatus=Not Restarted,details=Not Restarted,maxdate=Thu
AdminCertControlledRestart[id=38b811df-03b5-4a64-87b6-363290b6b4ce,hostname=asc-ise33-1037,noderestartc
noderestartstatus=Not Restarted,details=Not Restarted,maxdate=Thu Oct 12 2023 14:43:01 GMT-0600 (hora e
2023-09-27 21:59:12,113 INFO [DefaultQuartzScheduler_Worker-6][[]] admin.caservice.certmgmt.scheduler.
Restart configured , proceeding to trackRestartStatus for ***-ise-33-2
2023-09-27 21:59:12,113 INFO [DefaultQuartzScheduler_Worker-6][[]] admin.caservice.certmgmt.scheduler.
Restart configured , proceeding to trackRestartStatus for asc-ise33-1037
2023-09-27 22:00:00,003 INFO [DefaultQuartzScheduler_Worker-3][[]] admin.caservice.certmgmt.scheduler.
```



```

Executing AdminCertControlledRestartSchedulerJob
2023-09-27 22:00:00,022 INFO [DefaultQuartzScheduler_Worker-3][[]] admin.caservice.certmgmt.scheduler.
Executing AdminCertControlledRestartSchedulerJob [AdminCertControlledRestart[id=4af7d9c4-31d9-48e0-83dc
noderestartconfig=2023-09-27:10:00PM,noderestartstatus=Not Restarted,details=Not Restarted,maxdate=Thu
AdminCertControlledRestart[id=38b811df-03b5-4a64-87b6-363290b6b4ce,hostname=asc-ise33-1037,noderestartc
noderestartstatus=Not Restarted,details=Not Restarted,maxdate=Thu Oct 12 2023 14:43:01 GMT-0600 (hora e
2023-09-27 22:00:00,288 INFO [DefaultQuartzScheduler_Worker-3][[]] admin.caservice.certmgmt.scheduler.
Restart failed or not restarted yet , hence preparing restart for ***-ise-33-2
2023-09-27 22:00:00,288 INFO [DefaultQuartzScheduler_Worker-3][[]] admin.caservice.certmgmt.scheduler.
Configured Date is now , hence proceeding for restart , for ***-ise-33-2
2023-09-27 22:00:00,288 INFO [DefaultQuartzScheduler_Worker-3][[]] cpm.infrastructure.certmgmt.api.Admin
updateRestartStatus updating restarted status
2023-09-27 22:00:00,288 INFO [DefaultQuartzScheduler_Worker-3][[]] cpm.infrastructure.certmgmt.api.Admin
Updating the data for node: ***-ise-33-2
2023-09-27 22:00:00,313 INFO [DefaultQuartzScheduler_Worker-3][[]] admin.caservice.certmgmt.scheduler.
Restart failed or not restarted yet , hence preparing restart for asc-ise33-1037
2023-09-27 22:00:00,313 INFO [DefaultQuartzScheduler_Worker-3][[]] admin.caservice.certmgmt.scheduler.
Configured Date is now , hence proceeding for restart , for asc-ise33-1037
2023-09-27 22:00:00,324 INFO [DefaultQuartzScheduler_Worker-3][[]] admin.caservice.certmgmt.scheduler.
restartNowList : ***-ise-33-2.aaamexrub.com,asc-ise33-1037.aaamexrub.com

```

Sample logs from \*\*\*-ise-33-2, restartutil.log:

```

[main] Wed Sep 27 22:00:09 EST 2023:-----
[main] Wed Sep 27 22:00:09 EST 2023:RestartUtil: BEGIN - Restart called with args apponly:1377:***-ise-
[main] Wed Sep 27 22:00:09 EST 2023:-----
[main] Wed Sep 27 22:00:14 EST 2023:RestartUtil: Restarting Local node
[main] Wed Sep 27 22:00:14 EST 2023:[/usr/bin/sudo, /opt/CSC0cpm/bin/cpmcontrol.sh, restart_appserver_e
[main] Wed Sep 27 22:27:13 EST 2023:RestartUtil: Restarted local node and waiting for it to come up...
[main] Wed Sep 27 22:37:47 EST 2023:RestartUtil: Restart success for local node .
[main] Wed Sep 27 22:37:48 EST 2023:RestartUtil: Restarting node asc-ise33-1037.aaamexrub.com
[main] Wed Sep 27 22:37:54 EST 2023:RestartUtil: statusLine>>>HTTP/1.1 200
[main] Wed Sep 27 22:37:54 EST 2023:RestartUtil: Waiting for node asc-ise33-1037.aaamexrub.com to come
[main] Wed Sep 27 22:52:43 EST 2023:RestartUtil: Restart successful on node: asc-ise33-1037.aaamexrub.c
[main] Wed Sep 27 22:52:43 EST 2023:RestartUtil: cred file deleted
[main] Wed Sep 27 22:52:43 EST 2023:-----
[main] Wed Sep 27 22:52:43 EST 2023:RestartUtil:END- Restart called with args apponly:1377:***-ise-33-
[main] Wed Sep 27 22:52:43 EST 2023:-----
[main] Wed Sep 27 23:00:10 EST 2023: Usage RestartUtil local||remote apponly|full

```

Sample logs from asc-ise33-1037, restartutil.log:

```

[main] Wed Sep 27 19:00:10 UTC 2023: Usage RestartUtil local||remote apponly|full
[main] Thu Sep 28 04:37:14 UTC 2023:-----
[main] Thu Sep 28 04:37:14 UTC 2023:RestartUtil: BEGIN - Restart called with args apponly:1377:localhos
[main] Thu Sep 28 04:37:14 UTC 2023:-----
[main] Thu Sep 28 04:37:16 UTC 2023:RestartUtil: Restarting Local node
[main] Thu Sep 28 04:37:16 UTC 2023:[/usr/bin/sudo, /opt/CSC0cpm/bin/cpmcontrol.sh, restart_appserver_e
[main] Thu Sep 28 04:52:41 UTC 2023:RestartUtil: Restarted local node and waiting for it to come up...
[main] Thu Sep 28 04:53:12 UTC 2023:RestartUtil: Restart success for local node .

```

```
[main] Thu Sep 28 04:53:12 UTC 2023:RestartUtil: cred file deleted
[main] Thu Sep 28 04:53:12 UTC 2023:-----
[main] Thu Sep 28 04:53:12 UTC 2023:RestartUtil:END- Restart called with args apponly:1377:localhost
[main] Thu Sep 28 04:53:12 UTC 2023:-----
```

## Troubleshoot

To check the information about this feature, you can check these files:

- ise-psc.log
- restartutil.log

To check them in real time from the command line, you can use these commands:

```
show logging application restartutil.log tail
show logging application ise-psc.log tail
```

## Related Information

- [Cisco Technical Support & Downloads](#)