

Konfigurieren von kontrolliertem Anwendungsneustart in ISE 3.3

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Schritt 1: Erstellen einer Zertifikatsignierungsanforderung \(CSR\)](#)

[Schritt 2: Importieren Sie die Stammzertifizierungsstelle, die Ihren CSR signiert hat.](#)

[Schritt 3: Signierten CSR importieren](#)

[Schritt 4: Konfigurieren der Neustartzeit](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie der gesteuerte Anwendungsneustart für das Administratorzertifikat in ISE 3.3 konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- ISE-Knoten/Personas
- Verlängerung/Bearbeitung/Erstellung von ISE-Zertifikaten

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Hardware- und Software-Versionen:

- Identity Service Engine (ISE) Softwareversion 3.3
- Bereitstellung von 2 Knoten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Wenn in der ISE das Admin-Zertifikat des primären Admin-Knotens (PAN) geändert wird, werden alle Knoten in der Bereitstellung neu geladen, zuerst das PAN und dann die übrigen Knoten. Dies führt zu einer Unterbrechung aller Dienste.

Wenn das Administratorzertifikat in einem anderen Knoten ersetzt wird, wird nur dieser einzelne Knoten neu gestartet.

ISE 3.3 führt eine neue Funktion ein, mit der Sie das erneute Laden der Knoten planen können. Dies bietet eine bessere Kontrolle über den Neustart jedes Knotens und trägt dazu bei, Unterbrechungen bei allen Services zu vermeiden.

Konfigurieren

Es gibt verschiedene Optionen zum Ändern des Admin-Zertifikats des PAN-Knotens:

- Erstellen einer Zertifikatsanforderung (Certificate Signing Request, CSR) und Zuweisen der Administratorrolle
- Zertifikat importieren, privater Schlüssel und Zuweisung der Admin-Rolle.
- Erstellen Sie ein selbstsigniertes Zertifikat, und weisen Sie die Administratorrolle zu.

In diesem Dokument wird die Methode mithilfe einer CSR-Anfrage beschrieben.

Schritt 1: Erstellen einer Zertifikatsignierungsanforderung (CSR)

1. Navigieren Sie auf der ISE zu Administration > System > Certificates > Certificate Signing Requests.
2. Klicken Sie auf CSR (Certificate Signing Request) generieren.
3. Wählen Sie unter Usage (Nutzung) die Option Admin.
4. Wählen Sie in Node(s) (Knoten) den primären Admin-Knoten aus.
5. Füllen Sie die Zertifikatsinformationen aus.
6. Klicken Sie auf Erstellen.
7. Exportieren Sie die Datei, und unterzeichnen Sie sie mit einer gültigen Berechtigung.

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-Erstellung

Schritt 2: Importieren Sie die Stammzertifizierungsstelle, die Ihren CSR signiert hat.

1. Navigieren Sie auf der ISE zu Administration > System > Certificates > Trusted Certificates.
2. Klicken Sie auf Importieren.
3. Klicken Sie auf Choose File (Datei auswählen), und wählen Sie das Zertifikat der Stammzertifizierungsstelle aus.
4. Schreiben Sie einen Anzeigenamen.
5. Aktivieren Sie die Kontrollkästchen:
 1. Authentifizierung innerhalb der ISE als vertrauenswürdig einstufen.
 2. Vertrauen Sie auf die Authentifizierung von Cisco Services.
6. Klicken Sie auf Senden.

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

Stammzertifikat importieren

Schritt 3: Signierten CSR importieren

1. Navigieren Sie auf der ISE zu Administration > System > Certificates > Certificate Signing Requests.
2. Wählen Sie den CSR aus, und klicken Sie auf Zertifikat binden.
3. Klicken Sie auf Choose file, und wählen Sie das signierte Zertifikat aus.
4. Konfigurieren eines Anzeigenamens.

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

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	Pe
<input checked="" type="checkbox"/>	ise-33-2#Admin	CN=ise-33-2.a...	4096	

Zertifikat binden

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	

Zertifikat binden

Schritt 4: Konfigurieren der Neustartzeit

1. Jetzt können Sie einen neuen Abschnitt sehen. Hier konfigurieren Sie den Neustartvorgang.
2. Sie können eine Zeit pro Knoten konfigurieren oder beide Knoten auswählen und die gleiche Konfiguration anwenden.
3. Wählen Sie einen Knoten aus, und klicken Sie auf Set Restart Time (Neustartzeit festlegen).
4. Wählen Sie das Datum und die Uhrzeit aus, und klicken Sie auf Speichern.
5. Überprüfen Sie die Uhrzeit, und klicken Sie auf Submit (Senden).

Set Restart Time

Scheduler

Restart Now Restart Later

Set Date

27/09/2023

Set Time

11:00 PM

cancel

save

Neustartzeit festlegen

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

Certificate Management

- System Certificates
- Admin Certificate Node Restart
- Trusted Certificates
- OCSP 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

Neustartzeit bestätigen

Überprüfung

Eine neue Registerkarte ist verfügbar. Navigieren Sie zu Administration > System > Certificates > Admin Certificate Node Restart. Sie können die durchgeführte Konfiguration validieren und bei Bedarf ändern.

Klicken Sie zum Ändern auf Set Restart Time (Neustartzeit festlegen) oder Restart Now (Jetzt neu starten).

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

Überprüfen des Neustartstatus

Sie können den Knotenstatus während des Prozesses überprüfen. Das nächste Bild ist ein Beispiel, wenn ein Knoten neu geladen wird und der andere Knoten ausgeführt wird:

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 neu gestartet

Überprüfen Sie die Änderungen, und laden Sie die Berichte neu.

Um die Konfigurationsänderungen zu überprüfen, navigieren Sie zu Operations > Reports > Reports > Audit > Change Configuration Audit.

Export Summary	Change Configuration Audit						Add to My Reports	Export
My Reports	From 2023-09-27 00:00:00.0 To 2023-09-27 16:24:49.0						Reports exported in last 7 days 0	
Reports							Filter	Refresh
Audit								
Adaptive Network Control ...								
Administrator Logins								
Change Configuration Audit								
Cisco Support Diagnostics...								
Data Purging Audit								
Endpoints Purge Activities								
Internal Administrator Sum...								
OpenAPI Operations								
Operations 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

Konfigurationsbericht

Um den Neustart zu überprüfen, navigieren Sie zu Operationen > Berichte > Audit > Operations Audit.

Operations Audit					Add to My Repo
From 2023-09-27 00:00:00.0 To 2023-09-27 22:50:14.0					
Reports exported in last 7 days 0					
2023-09-27 22:04:20.0...		CLI	Configuration-Changes	Added configuration	Filter
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

Bericht neu starten

Beispielprotokolle von ***-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
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.Admini
updateRestartStatus updating restarted status
2023-09-27 22:00:00,288 INFO [DefaultQuartzScheduler_Worker-3][[]] cpm.infrastructure.certmgmt.api.Admini
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

```

Beispielprotokolle von ***-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

```

Beispielprotokolle von 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:-----
```

Fehlerbehebung

Um die Informationen zu dieser Funktion zu überprüfen, können Sie die folgenden Dateien überprüfen:

- ise-psc.log
- restartutil.log

Um sie in Echtzeit über die Befehlszeile zu überprüfen, können Sie die folgenden Befehle verwenden:

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

Zugehörige Informationen

- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.