

ISE 2.0: Konfigurationsbeispiel für ASA CLI TACACS+-Authentifizierung und - Befehlsautorisierung

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Konfigurieren der ISE für Authentifizierung und Autorisierung](#)

[Netzwerkgerät hinzufügen](#)

[Konfigurieren von Benutzeridentitätsgruppen](#)

[Konfigurieren von Benutzern](#)

[Device Admin Service aktivieren](#)

[Konfigurieren von TACACS-Befehlssätzen](#)

[Konfigurieren des TACACS-Profiles](#)

[Konfigurieren der TACACS-Autorisierungsrichtlinie](#)

[Konfigurieren der Cisco ASA Firewall für Authentifizierung und Autorisierung](#)

[Überprüfen](#)

[Cisco ASA Firewall-Verifizierung](#)

[ISE 2.0-Verifizierung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

[Ähnliche Diskussionen in der Cisco Support Community](#)

Einführung

In diesem Dokument wird beschrieben, wie die TACACS+-Authentifizierung und - Befehlsautorisierung auf der Cisco Adaptive Security Appliance (ASA) mit Identity Service Engine (ISE) 2.0 und höher konfiguriert wird. Die ISE verwendet einen lokalen Identitätsdatenspeicher, um Ressourcen wie Benutzer, Gruppen und Endpunkte zu speichern.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Die ASA-Firewall ist vollständig betriebsbereit.

- Verbindungen zwischen ASA und ISE
- ISE-Server wird bootstrappert

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Identity Service Engine 2.0
- Cisco ASA Software Version 9.5(1)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

Ziel der Konfiguration ist es,

- SSH-Benutzer über internen Identitätsspeicher authentifizieren
- SSH-Benutzer autorisieren, sodass er nach der Anmeldung in den privilegierten EXEC-Modus versetzt wird
- Überprüfung aller ausgeführten Befehle durch die ISE

Netzwerkdiagramm

Network
Administrator



ISE Server
10.48.17.88



ASA Firewall
10.48.66.202

Konfigurationen

Konfigurieren der ISE für Authentifizierung und Autorisierung

Es werden zwei Benutzer erstellt. Der **Benutzeradministrator** ist Teil der lokalen **Netzwerkadministratorgruppe** für die ISE. Dieser Benutzer verfügt über volle CLI-Berechtigungen. Der Benutzer ist Teil der lokalen Identitätsgruppe **des Netzwerkverwaltungsteams** auf der ISE. Dieser Benutzer darf nur Befehle anzeigen und Ping-Befehle senden.

Netzwerkgerät hinzufügen

Navigieren Sie zu **Work Centers > Device Administration > Network Resources > Network Devices (Arbeitscenter > Geräteverwaltung > Netzwerkressourcen > Netzwerkgeräte)**. Klicken Sie auf **Hinzufügen**. Geben Sie den Namen und die IP-Adresse ein, aktivieren Sie das Kontrollkästchen **TACACS+ Authentication Settings** (TACACS+-Authentifizierungseinstellungen), und geben Sie den **Shared Secret**-Schlüssel ein. Optional können Gerätetyp und -ort angegeben werden.

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

TrustSec Device Administration

Overview Identities User Identity Groups Network Resources Network Device Groups Policy Conditions Policy Results Policy Sets Reports

Network Devices List > New Network Device

Network Devices

Default Devices

TACACS External Servers

TACACS Server Sequence

1 * Name ASA

Description

2 * IP Address: 10.48.66.202 / 32

* Device Profile Cisco

Model Name

Software Version

* Network Device Group

Location All Locations Set To Default

Device Type Firewall Set To Default

RADIUS Authentication Settings

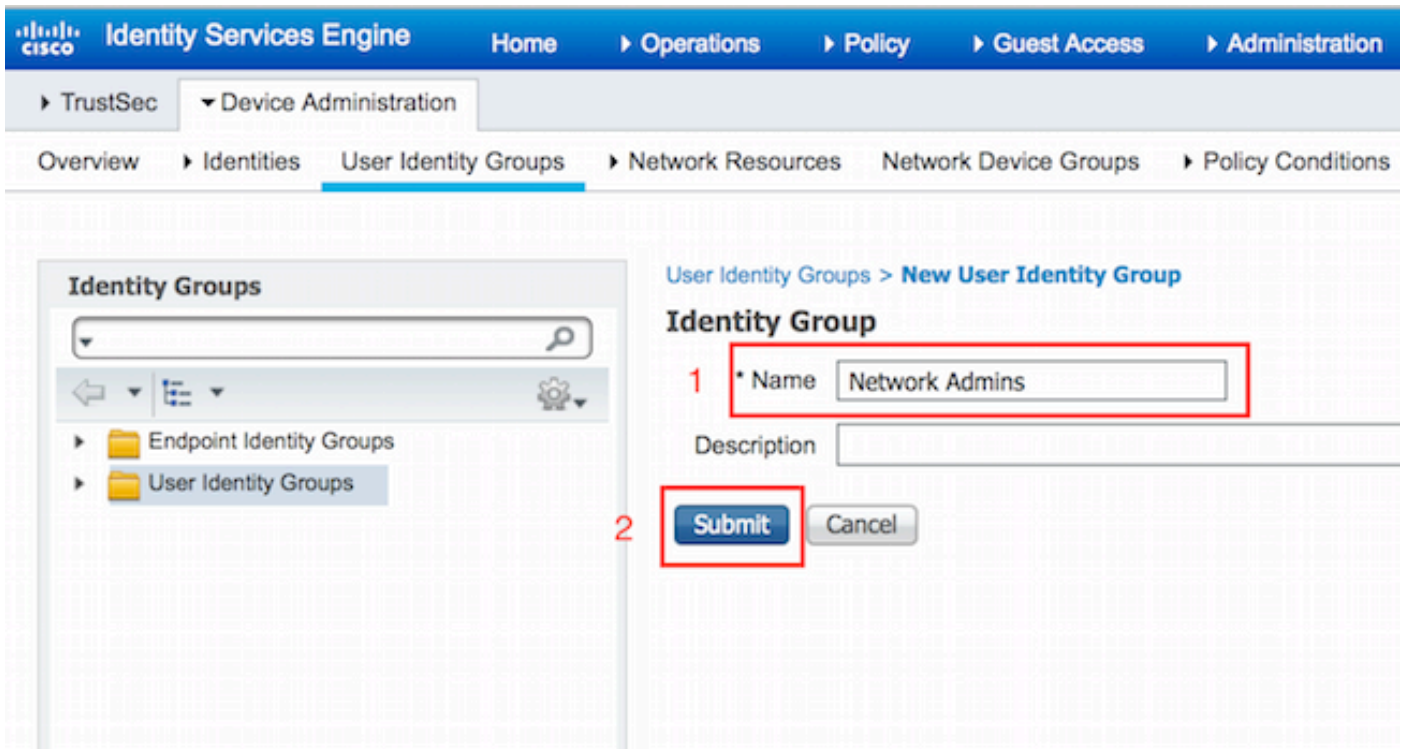
TACACS+ Authentication Settings

Shared Secret ***** Show

Enable Single Connect Mode

Konfigurieren von Benutzeridentitätsgruppen

Navigieren Sie zu **Work Center > Device Administration > User Identity Groups (Arbeitscenter > Geräteverwaltung > Benutzeridentitätsgruppen)**. Klicken Sie auf **Hinzufügen**. Geben Sie den Namen ein, und klicken Sie auf **Senden**.



Wiederholen Sie den gleichen Schritt, um die Benutzeridentitätsgruppe für **Network Maintenance Team** zu konfigurieren.

Konfigurieren von Benutzern

Navigieren Sie zu **Work Center > Device Administration > Identities > Users**. Klicken Sie auf **Hinzufügen**. Geben Sie den Namen, das Anmeldekennwort und die Benutzergruppe ein, und klicken Sie auf **Senden**.

▼ **Network Access User**

* Name 1

Status Enabled ▼

Email

▼ **Passwords** 2

	Password	Re-Enter Password	
* Login Password	<input type="password" value="....."/>	<input type="password" value="....."/>	<input type="button" value="i"/>
Enable Password	<input type="text"/>	<input type="text"/>	<input type="button" value="i"/>

▼ **User Information**

First Name

Last Name

▼ **Account Options**

Description

Change password on next login 3

▼ **User Groups**

Wiederholen Sie die Schritte, um den **Benutzer** zu konfigurieren und die Benutzeridentitätsgruppe für das **Network Maintenance Team** zuzuweisen.

Device Admin Service aktivieren

Navigieren Sie zu **Administration > System > Deployment**. Wählen Sie den erforderlichen Knoten aus. Aktivieren Sie das Kontrollkästchen **Device Admin Service aktivieren**, und klicken Sie auf **Speichern**.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', 'Administration', and 'Work Centers'. The main content area displays the configuration for a node named 'Joey.example.com' with IP address '10.48.17.88'. Under the 'Personas' section, several services are listed with checkboxes and roles. The 'Enable Device Admin Service' checkbox is checked and highlighted with a red box, with a red '1' next to it. The 'Save' button is also highlighted with a red box, with a red '2' next to it. Other settings include 'Administration' (Role: STANDALONE), 'Monitoring' (Role: PRIMARY), 'Policy Service' (with sub-options for Session, Profiling, and SXP services), and 'pxGrid'.

Hinweis: Für TACACS muss eine separate Lizenz installiert sein.

Konfigurieren von TACACS-Befehlssätzen

Es werden zwei Befehlssätze konfiguriert. First **PermitAllCommands** für den **Administrator-Benutzer**, der alle Befehle auf dem Gerät zulässt. Second **PermitPingShowCommands** für **Benutzer**, die nur Befehle zum Ein- und Pingen zulassen.

1. Navigieren Sie zu **Work Centers > Device Administration > Policy Results > TACACS Command Sets**. Klicken Sie auf **Hinzufügen**. Geben Sie das **Kontrollkästchen Name PermitAllCommands** an, wählen Sie den **Befehl Zulassen** für einen Befehl aus, der unten nicht **aufgeführt ist**, und klicken Sie auf **Senden**.

TACACS Command Sets > New

Command Set

1

Name *

PermitAllCommands

Description

2

Permit any command that is not listed below

+ Add 🗑️ Trash ▼ ✎ Edit ↑ Move Up ↓ Move Down			
<input type="checkbox"/>	Grant	Command	Arguments
No data found.			

2. Navigieren Sie zu **Work Centers > Device Administration > Policy Results > TACACS Command Sets**. Klicken Sie auf **Hinzufügen**. Geben Sie den Namen **PermitPingShowCommands** an, klicken Sie auf **Hinzufügen** und lassen Sie **die Befehle show,ping und exit** zu. Wenn Argumente leer gelassen werden, werden standardmäßig alle Argumente eingeschlossen. Klicken Sie auf **Senden**.

Command Set

1 Name * PermitPingShowCommands

Description

Permit any command that is not listed below

+ Add Trash Edit Move Up Move Down

Grant	Command	Arguments
<input type="checkbox"/> PERMIT	exit	
<input type="checkbox"/> PERMIT	show	
<input type="checkbox"/> PERMIT	ping	

2

Cancel Save

Konfigurieren des TACACS-Profiles

Es wird nur ein TACACS-Profil konfiguriert. Die tatsächliche Befehlsdurchsetzung erfolgt über Befehlssätze. Navigieren Sie zu **Work Centers > Device Administration > Policy Results > TACACS Profiles**. Klicken Sie auf **Hinzufügen**. Geben Sie den Namen **ShellProfile** ein, aktivieren Sie das Kontrollkästchen **Default Privilege** (Standardberechtigung), und geben Sie den Wert 15 ein. Klicken Sie auf **Senden**.

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

TrustSec Device Administration

Overview Identities User Identity Groups Network Resources Network Device Groups Policy Conditions Policy Results Policy Sets Reports Settings

TACACS Command Sets

TACACS Profiles

TACACS Profiles > New

TACACS Profile

1 Name * ShellProfile

Description

Task Attribute View Raw View

Common Tasks

2 Default Privilege 15 (Select 0 to 15)

Maximum Privilege (Select 0 to 15)

Access Control List

Auto Command

No Escape (Select true or false)

Timeout

Idle Time

Konfigurieren der TACACS-Autorisierungsrichtlinie

Die Authentifizierungsrichtlinie verweist standardmäßig auf All_User_ID_Stores, das auch den lokalen Store enthält, sodass er unverändert bleibt.

Navigieren Sie zu **Work Centers > Device Administration > Policy Sets > Default > Authorization Policy > Edit > Insert New Rule Oove.**

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Status	Name	Description
<input checked="" type="checkbox"/>	Default	Tacacs_Default

Regular Proxy Sequence

▶ **Authentication Policy**

▼ **Authorization Policy**

▶ **Exceptions (0)**

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	Tacacs_Default	if no matches, then	DenyAllCommands	

Es werden zwei Autorisierungsregeln konfiguriert. Die erste Regel weist dem **ShellProfile**-Profil des **TACACS-Profiles** und dem Befehl Set **PermitAllCommands** auf der Grundlage der Mitgliedschaft der **Network Admins** User Identity Group zu. Die zweite Regel weist **ShellProfile** des **TACACS-Profiles** und den Befehl Set **PermitPingShowCommands** basierend auf der Mitgliedschaft der **Network Maintenance Team** User Identity Group zu.

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Status	Name	Description
<input checked="" type="checkbox"/>	Default	Tacacs_Default

Regular Proxy Sequence

▼ **Proxy Server Sequence**

Proxy server sequence:

▶ **Authentication Policy**

▼ **Authorization Policy**

▶ **Exceptions (0)**

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	ASAPermitAllCommands	if Network Admins then	PermitAllCommands AND ShellProfile	Edit
<input checked="" type="checkbox"/>	ASAPermitShowPingCommands	if Network Maintenance Team then	PermitPingShowCommands AND ShellProfile	Edit

Konfigurieren der Cisco ASA Firewall für Authentifizierung und Autorisierung

1. Erstellen Sie einen lokalen Benutzer mit voller Berechtigung für Fallback mit dem Befehl **username**, wie hier gezeigt

```
ciscoasa(config)# username cisco password cisco privilege 15
```

2. Definieren Sie die TACACS-Server-ISE, geben Sie die Schnittstelle, die Protokoll-IP-Adresse und den **takacs**-Schlüssel an.

```
aaa-server ISE protocol tacacs+
aaa-server ISE (mgmt) host 10.48.17.88
key cisco
```

Hinweis: Der Serverschlüssel muss mit dem auf dem ISE-Server zuvor definierten Schlüssel übereinstimmen.

3. Testen Sie die Erreichbarkeit des TACACS-Servers mit dem Befehl **test aaa** wie gezeigt.

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

Die Ausgabe des vorherigen Befehls zeigt, dass der TACACS-Server erreichbar ist und der Benutzer erfolgreich authentifiziert wurde.

4. Konfigurieren Sie die Authentifizierung für ssh-, exec-Autorisierung und Befehlsautorisierungen wie unten gezeigt. Mit **aaa authorized exec authentication-server auto-enable** werden Sie automatisch in den privilegierten EXEC-Modus versetzt.

```
aaa authentication ssh console ISE
aaa authorization command ISE
aaa authorization exec authentication-server auto-enable
```

Hinweis: Mit den oben genannten Befehlen erfolgt die Authentifizierung auf der ISE, der Benutzer wird direkt in den Berechtigungsmodus versetzt und die Befehlsautorisierung erfolgt.

5. Erlauben Sie ssh auf der Mgmt-Schnittstelle.

```
ssh 0.0.0.0 0.0.0.0 mgmt
```

Überprüfen

Cisco ASA Firewall-Verifizierung

1. Führen Sie die ASA-Firewall als **Administrator** ein, der der Benutzeridentitätsgruppe mit vollem Zugriff angehört. Die Gruppe **Netzwerkadministratoren** ist dem auf der ISE festgelegten **ShellProfile**- und **PermitAllCommands**-Befehl zugeordnet. Versuchen Sie, einen beliebigen Befehl auszuführen, um den vollständigen Zugriff sicherzustellen.

```
EKORNEYC-M-K04E:~ ekorneyc$ ssh administrator@10.48.66.202
administrator@10.48.66.202's password:
Type help or '?' for a list of available commands.
ciscoasa#
ciscoasa# configure terminal
```

```

ciscoasa(config)# crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)# encryption aes
ciscoasa(config-ikev1-policy)# exit
ciscoasa(config)# exit
ciscoasa#

```

2. Führen Sie die ASA-Firewall als **Benutzer** aus, der der Benutzeridentitätsgruppe mit beschränktem Zugriff angehört. Die Gruppe **Netzwerkwartung** ist dem auf der ISE festgelegten Befehlssatz **ShellProfile** und **PermitPingShowCommands** zugeordnet. Führen Sie einen beliebigen Befehl aus, um sicherzustellen, dass nur Befehle zum Ein- und Pingen ausgegeben werden können.

```

EKORNEYC-M-K04E:~ ekorneyc$ ssh user@10.48.66.202
administrator@10.48.66.202's password:
Type help or '?' for a list of available commands.
ciscoasa#
ciscoasa# show version | include Software
Cisco Adaptive Security Appliance Software Version 9.5(1)
ciscoasa# ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/30 ms
ciscoasa# configure terminal
Command authorization failed
ciscoasa# traceroute 8.8.8.8
Command authorization failed

```

ISE 2.0-Verifizierung

1. Navigieren Sie zu **Operations > TACACS Livelog**. Stellen Sie sicher, dass die oben beschriebenen Versuche angezeigt werden.

Generated Time	Status	Details	Username	Type	Authentication Policy	Authorization Policy	ISE N
2015-08-19 13:47:24.135	✘		user	Authorization	Tacacs_Default >> ASAPermitShowPingComma...	Joey	
2015-08-19 13:47:15.139	✘		user	Authorization	Tacacs_Default >> ASAPermitShowPingComma...	Joey	
2015-08-19 13:47:07.452	✔		user	Authorization	Tacacs_Default >> ASAPermitShowPingComma...	Joey	
2015-08-19 13:46:56.816	✔		user	Authorization	Tacacs_Default >> ASAPermitShowPingComma...	Joey	
2015-08-19 13:46:49.961	✔		user	Authorization	Tacacs_Default >> ASAPermitShowPingComma...	Joey	
2015-08-19 13:46:35.595	✔		user	Authorization	Tacacs_Default >> ASAPermitShowPingComma...	Joey	
2015-08-19 13:46:35.581	✔		user	Authentication	Tacacs_Default >> Default >> Default	Joey	
2015-08-19 13:46:20.209	✔		administrator	Authorization	Tacacs_Default >> ASAPermitAllCommands	Joey	
2015-08-19 13:42:05.838	✔		administrator	Authorization	Tacacs_Default >> ASAPermitAllCommands	Joey	
2015-08-19 13:42:04.886	✔		administrator	Authorization	Tacacs_Default >> ASAPermitAllCommands	Joey	
2015-08-19 13:42:02.575	✔		administrator	Authorization	Tacacs_Default >> ASAPermitAllCommands	Joey	

2. Klicken Sie auf die Details eines der roten Berichte, der fehlgeschlagene Befehl, der früher ausgeführt wurde, wird angezeigt.

Overview

Request Type	Authorization
Status	Fail
Session Key	Joey/229297775/274
Message Text	Failed-Attempt: Command Authorization failed
Username	user
Authorization Policy	Tacacs_Default >> ASAPermitShowPingCommands
Shell Profile	
Matched Command Set	
Command From Device	traceroute 8.8.8.8

Fehlerbehebung

Fehler: Fehlgeschlagener Versuch: Befehlsautorisierung fehlgeschlagen

Überprüfen Sie das SelectedCommandSet-Attribut, um sicherzustellen, dass die erwarteten Befehlsätze von der Autorisierungsrichtlinie ausgewählt wurden

Zugehörige Informationen

[Technischer Support und Dokumentation - Cisco Systems](#)

[ISE 2.0 Versionshinweise](#)

[ISE 2.0 - Hardware-Installationsanleitung](#)

[ISE 2.0-Upgrade-Leitfaden](#)

[Leitfaden für die Migration von ACS zur ISE](#)

[ISE 2.0 Active Directory-Integrationsanleitung](#)

[ISE 2.0 Engine - Administratoranleitung](#)