

Konfigurieren der SWA Second Factor-Authentifizierung mit der ISE als RADIUS-Server

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Netzwerktopologie](#)

[Konfigurationsschritte](#)

[ISE-Konfiguration](#)

[SWA-Konfiguration](#)

[Überprüfung](#)

[Referenzen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Authentifizierung des zweiten Faktors auf einer sicheren Web-Appliance mit der Cisco Identity Service Engine als RADIUS-Server konfigurieren.

Voraussetzungen

Anforderungen

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

- Grundkenntnisse in SWA.
- Kenntnis der Konfiguration von Authentifizierungs- und Autorisierungsrichtlinien auf der ISE
- Grundlegendes RADIUS-Wissen

Cisco empfiehlt außerdem Folgendes:

- Administrationszugriff über die Secure Web Appliance (SWA) und die Cisco Identity Service Engine (ISE).
- Ihre ISE ist in Active Directory oder LDAP integriert.
- Active Directory oder LDAP wird mit dem Benutzernamen "admin" konfiguriert, um das SWA-Standardkonto "admin" zu authentifizieren.
- Kompatible WSA- und ISE-Versionen.

Verwendete Komponenten

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

- SWA 14.0.2-012
- ISE 3.0.0

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 Sie die zweite Faktor-Authentifizierung für administrative Benutzer auf SWA aktivieren, überprüft das Gerät nach der Überprüfung der in SWA konfigurierten Anmeldeinformationen die Benutzeranmeldeinformationen beim RADIUS-Server zum zweiten Mal.

Netzwerktopologie



Bild - Netzwerktopologie-Diagramm

Administrative Benutzer greifen mit ihren Anmeldeinformationen auf Port 443 auf SWA zu. SWA verifiziert die Anmeldeinformationen mit dem RADIUS-Server für die zweite Faktor-Authentifizierung.

Konfigurationsschritte

ISE-Konfiguration

Schritt 1: Hinzufügen eines neuen Netzwerkgeräts Navigieren Sie zu Administration > Network Resources > Network Devices > +Add.

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM

Network Devices

Default Device

Device Security Settings

Network Devices

Edit Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location	Type
No data available				

SWA als Netzwerkgerät in der ISE hinzufügen

Schritt 2: Konfigurieren von Netzwerkgeräten in der ISE

Schritt 2.1: Weisen Sie dem Netzwerkgeräteobjekt einen Namen zu.

Schritt 2.2: Geben Sie die SWA-IP-Adresse ein.

Schritt 2.3: Aktivieren Sie das Kontrollkästchen RADIUS.

Schritt 2.4: Definieren Sie einen gemeinsamen geheimen Schlüssel.



Hinweis: Derselbe Schlüssel muss später zur Konfiguration der SWA verwendet werden.

Network Devices

Default Device

Device Security Settings

[Network Devices List > SWA](#)

Network Devices

* Name

Description

IP Address /

* Device Profile  Cisco

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

Gemeinsamer SWA-Schlüssel für Netzwerkgerät konfigurieren

Schritt 2.5: Klicken Sie auf Senden.

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: **RADIUS**

* Shared Secret:

Use Second Shared Secret: ⓘ

CoA Port:

RADIUS DTLS Settings ⓘ

DTLS Required: ⓘ

Shared Secret: ⓘ

CoA Port:

Issuer CA of ISE Certificates for CoA: ⓘ

DNS Name:

General Settings

Enable KeyWrap: ⓘ

* Key Encryption Key:

* Message Authenticator Code Key:

Key Input Format: ASCII HEXADECIMAL

TACACS Authentication Settings

SNMP Settings

Advanced TrustSec Settings

Konfiguration des Netzwerkgeräts senden

Schritt 3: Sie müssen Netzwerkzugriffsbenutzer erstellen, die mit dem in SWA konfigurierten Benutzernamen übereinstimmen. Navigieren Sie zu Administration > Identity Management > Identities > + Add.

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service | Threat Centric NAC

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

Network Access Users

Users

Latest Manual Network Scan Results

Status	Name	Description	First Name	Last Name	Email Address
No data available					

Hinzufügen lokaler Benutzer zur ISE

Schritt 3.1: Weisen Sie einen Namen zu.

Schritt 3.2. (Optional) Geben Sie die E-Mail-Adresse des Benutzers ein.

Schritt 3.3: Passwort festlegen.

Schritt 3.4: Klicken Sie auf Speichern.

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service | Threat Centric NAC

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

Users

Latest Manual Network Scan Results

Network Access Users List > New Network Access User

Network Access User

* Name:

Status: Enabled

Email:

Passwords

Password Type:

Password:
 Re-Enter Password:
 ⓘ

* Login Password:
 ⓘ

Enable Password:
 ⓘ

Hinzufügen eines lokalen Benutzers zur ISE

Schritt 4: Erstellen Sie einen Richtlinienatz, der der SWA-IP-Adresse entspricht. Dadurch wird der Zugriff auf andere Geräte mit diesen Benutzeranmeldeinformationen verhindert.

Navigieren Sie zu Policy > PolicySets, und klicken Sie in der linken oberen Ecke auf das Symbol +.

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

Policy Sets | Profiling | Posture | Client Provisioning | Policy Elements

Policy Sets

+	Status	Policy Set Name	Description	Conditions
Search				

Richtliniensatz in ISE hinzufügen

Schritt 4.1: Eine neue Zeile wird oben in Ihren Richtlinienätzen platziert. Geben Sie einen Namen für die neue Richtlinie ein.

Schritt 4.2: Fügen Sie eine Bedingung für das RADIUS NAS-IP-Address-Attribut hinzu, damit es mit der SWA-IP-Adresse übereinstimmt.

Schritt 4.3: Klicken Sie auf Verwenden, um die Änderungen beizubehalten und den Editor zu beenden.

Conditions Studio



Library

Search by Name

📍 🗨️ 📄 📁 🖨️ 📧 📧 📧 📧 📧 📧 📧 📧 📧 📧

- Catalyst_Switch_Local_Web_Authentication ⓘ
- Switch_Local_Web_Authentication ⓘ
- Switch_Web_Authentication ⓘ
- Wired_802.1X ⓘ
- Wired_MAB ⓘ
- Wireless_802.1X ⓘ
- Wireless_Access ⓘ
- Wireless_MAB ⓘ
- WLC_Web_Authentication ⓘ

Editor

Radius-NAS-IP-Address

📍 Equals 10.106.38.176

Set to 'is not'

Duplicate Save

+ New AND OR

Close

Use

Hinzufügen einer Richtlinie zum Zuordnen eines SWA-Netzwerkgeräts

Schritt 4.4: Klicken Sie auf Speichern.

Policy Sets

Reset Policyset Hitcounts

Reset

Save

	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	🟢	SWA Access		📍 Radius-NAS-IP-Address EQUALS 10.106.38.176	Default Network Access x +		⚙️	➔
	🟢	Default	Default policy set		Default Network Access x +	0	⚙️	➔

Reset

Save

Richtlinie speichern



Hinweis: In diesem Beispiel wurde die Liste der Standardprotokolle für den Netzwerkzugriff zugelassen. Sie können eine neue Liste erstellen und sie nach Bedarf eingrenzen.

Schritt 5: Um die neuen Richtlinienätze anzuzeigen, klicken Sie in der Spalte Ansicht auf das Symbol ">".

Schritt 5.1: Erweitern Sie das Menü Authorization Policy (Autorisierungsrichtlinie), und klicken Sie auf das +-Symbol, um eine neue Regel hinzuzufügen, die den Zugriff für alle authentifizierten Benutzer ermöglicht.

Schritt 5.2: Legen Sie einen Namen fest.

Schritt 5.3: Legen Sie die Bedingungen fest, die dem Dictionary Network Access mit dem Attribut AuthenticationStatus gleich AuthenticationPassed entsprechen, und klicken Sie auf Use (Verwenden).

Conditions Studio

Library

- Search by Name
- BYOD_is_Registered
 - Catalyst_Switch_Local_Web_Authentication
 - Compliance_Unknown_Devices
 - Compliant_Devices
 - Guest_Flow
 - Network_Access_Authentication_Passed
 - Non_Cisco_Profiled_Phones
 - Non_Compliant_Devices
 - Switch_Local_Web_Authentication
 - Switch_Web_Authentication
 - Wired_802.1X
 - Wired_MAB
 - Wireless_802.1X
 - Wireless_MAB
 - WLC_Web_Authentication

Editor

Network Access:AuthenticationStatus

Equals AuthenticationPassed

Set to 'Is not'

Duplicate Save

+ New AND OR

Close Use

Autorisierungsbedingung auswählen

Schritt 6: Legen Sie PermitAccess als Autorisierungsprofil fest, und klicken Sie auf Speichern.

Policy Sets → SWA Access

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
🟢	SWA Access		Radius NAS-IP-Address EQUALS 10.106.38.176	Default Network Access	6

▼ Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
🟢	Default		AI_User_ID_Stores	6	Options

► Authorization Policy - Local Exceptions

► Authorization Policy - Global Exceptions

▼ Authorization Policy (2)

Status	Rule Name	Conditions	Results Profiles	Security Groups	Hits	Actions
🟢	SWA Users	Network_Access_Authentication_Passed	PermitAccess	Select from list	5	+
🟢	Default		DenyAccess	Select from list	0	+

Reset Policyset Hitcounts Reset Save

Reset Save

Autorisierungsprofil auswählen

SWA-Konfiguration

Schritt 1: Navigieren Sie in der SWA-GUI zu Systemverwaltung, und klicken Sie auf Benutzer.

Schritt 2: Klicken Sie in den Second Factor Authentication-Einstellungen auf Aktivieren.

Cisco Secure Web Appliance S100V

Reporting | Web Security Manager | Security Services | Network | System Administration | Secure We

Users

Add User...

<input type="checkbox"/> All Accounts	User Name	Full Name	User Type	Account Status	Passphrase Expires	Delete
<input type="checkbox"/>	admin	Administrator	Administrator	Active	n/a	

Enforce Passphrase Changes

Local User Account & Passphrase Settings

Account Lock:	Not configured.
Passphrase Reset:	Not configured.
Passphrase Rules:	Require at least 8 characters. Additional rules configured...

Edit Settings...

External Authentication

External Authentication is disabled.

Enable...

Second Factor Authentication Settings

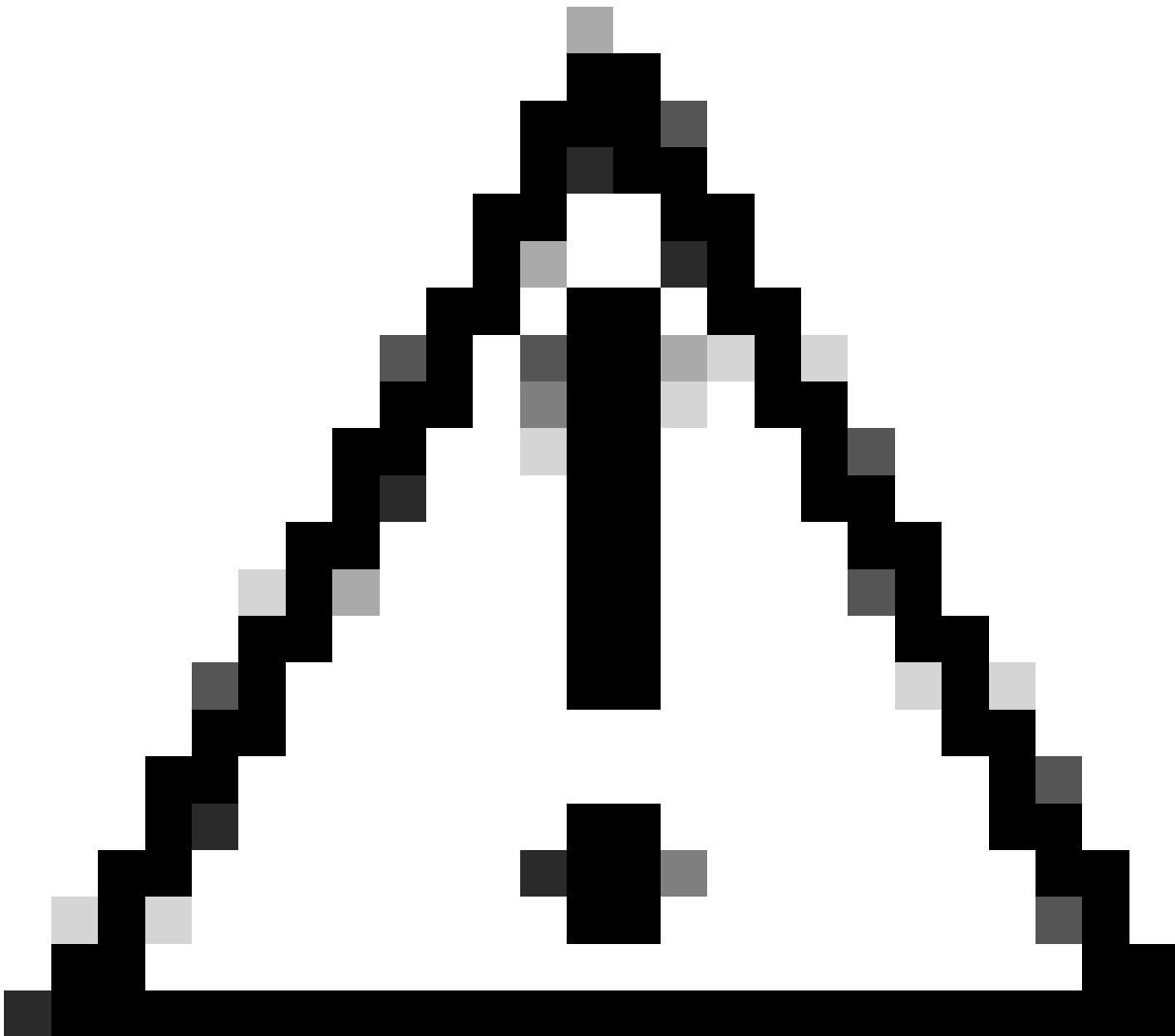
Two Factor Authentication is disabled.

Enable...

Second Factor Authentication in SWA aktivieren

Schritt 3: Geben Sie die IP-Adresse der ISE in das Feld RADIUS Server Hostname ein, und geben Sie Shared Secret ein, das in Schritt 2 der ISE-Konfiguration konfiguriert wurde.

Schritt 4: Wählen Sie die erforderlichen vordefinierten Rollen aus, für die die Durchsetzung des zweiten Faktors aktiviert werden soll.



Vorsicht: Wenn Sie die zweite Faktor-Authentifizierung in SWA aktivieren, wird das Standard-Admin-Konto auch mit Second Factor-Durchsetzung aktiviert. Sie müssen die ISE in LDAP oder Active Directory (AD) integrieren, um die Anmeldeinformationen "admin" zu authentifizieren, da die ISE es Ihnen nicht erlaubt, "admin" als Netzwerkzugriffsbenutzer zu konfigurieren.



Users

Users						
Add User...						
<input type="checkbox"/>	User Name	Full Name	User Type	Account Status	Passphrase Expires	Delete
<input type="checkbox"/>	admin	Administrator	Administrator	Active	n/a	
Enforce Passphrase Changes						

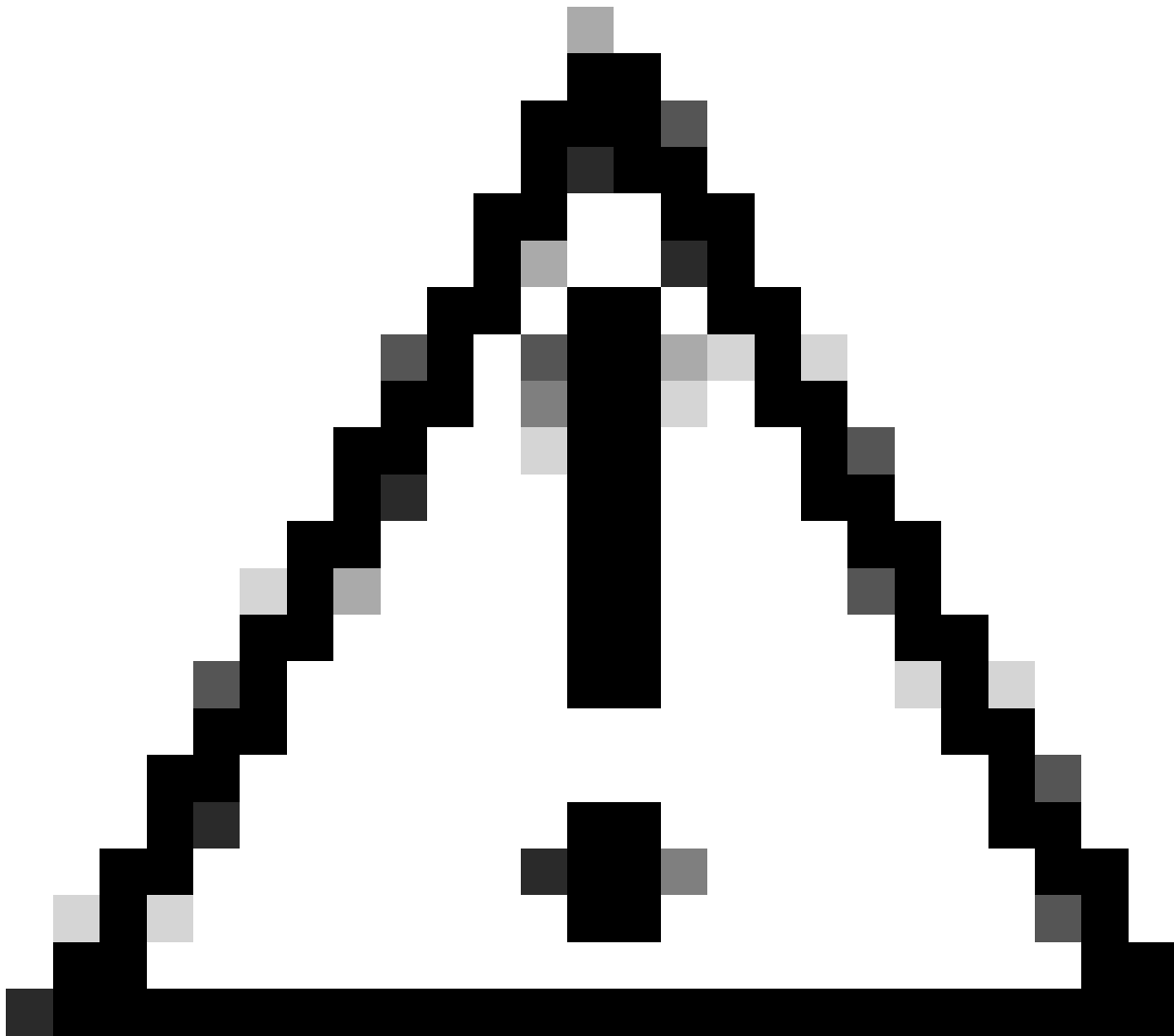
Local User Account & Passphrase Settings	
Account Lock:	Not configured.
Passphrase Reset:	Not configured.
Passphrase Rules:	Require at least 8 characters. <i>Additional rules configured...</i>
Edit Settings...	

External Authentication
<i>External Authentication is disabled.</i>
Enable...

Second Factor Authentication Settings
<i>Two Factor Authentication is disabled.</i>
Enable...



Second Factor Authentication in SWA aktivieren



Vorsicht: Wenn Sie die zweite Faktor-Authentifizierung in SWA aktivieren, wird das Standard-Admin-Konto auch mit Second Factor-Durchsetzung aktiviert. Sie müssen die ISE in LDAP oder Active Directory (AD) integrieren, um die Anmeldeinformationen "admin" zu authentifizieren, da die ISE es Ihnen nicht erlaubt, "admin" als Netzwerkzugriffsbenutzer zu konfigurieren.

Second Factor Authentication

Second Factor Authentication Settings

Enable Second Factor Authentication

Authentication Type: RADIUS

Protocol: UDP

RADIUS Server Information:	RADIUS Server Hostname	Port	Shared Secret	Timeout Value (in seconds)	Authentication protocol	Add Row
	10.106.38.150	1812	*****	5	PAP	

User Role Privileges

Configure user roles for Second Factor Authentication

Second Factor Authentication is enforced to:

Predefined Roles

- Administrator
- Operator
- Read-Only Operator
- Guest

Two Factor Login Page

Appearance:

Current Logo:

Use Current Logo

Upload Custom Logo from Local Computer: Browse... No file selected.

Company Name:
(Max 150 characters only)

Custom text Information:
(Max 500 characters only)

Login help Information:
(Examples: For login trouble Please contact, Contact Name ,123-1234-123,admin@example.com or help URL. Note:Max 500 characters only)

[View Existing Two Factor Login Page](#)

Cancel
Submit

Zweite Faktorauthentifizierung konfigurieren

Schritt 5: Um Benutzer in SWA zu konfigurieren, klicken Sie auf Benutzer hinzufügen. Geben Sie den Benutzernamen ein, und wählen Sie den für die gewünschte Rolle erforderlichen Benutzertyp aus. Geben Sie die Passphrase ein, und geben Sie sie erneut ein.

Users

Users

Add User...

* When RADIUS external authentication is enabled, all local user accounts except "admin" are disabled. If all RADIUS services fail, local user accounts will be used for authentication.

All Accounts	User Name	Full Name	User Type*	Account Status	Passphrase Expires	Delete
<input type="checkbox"/>	adminuser	Admin User	Administrator	Active	n/a	
<input type="checkbox"/>	rouser	RO User	Read-Only Operator	Active	n/a	

Benutzerkonfiguration in SWA

Schritt 6: Klicken Sie auf Senden und Änderungen bestätigen.

Überprüfung

Zugriff auf die SWA-GUI mit den konfigurierten Benutzeranmeldeinformationen Nach erfolgreicher Authentifizierung werden Sie zur sekundären Authentifizierungsseite weitergeleitet. Hier müssen Sie die sekundären, in ISE konfigurierten Authentifizierungsdaten eingeben.



Passcode:

Login

Copyright © 2003-2022 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

Zweite Faktor Anmeldung überprüfen

Referenzen

- [Bedienungsanleitung für AsyncOS 14.0 für Cisco Secure Web Appliance](#)
- [ISE 3.0 - Administratorhandbuch](#)
- [ISE-Kompatibilitätstmatrix für Secure Web Appliance](#)
- [AD für ISE-GUI und CLI integrieren Anmelden](#)

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.