

SWA mit SMA integrieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Vorbereitungen](#)

[Schritte zur Integration von SWA in SMA](#)

[Schritt 1: Exportieren der Konfigurationsdatei aus SWA](#)

[Schritt 2: Erstellen des Konfigurations-Managers](#)

[Schritt 3: Configuration Manager-Einstellungen](#)

[Schritt 4: Web-Appliance hinzufügen](#)

[Schritt 5: Validierung der Integration](#)

[Beheben von Fehlern](#)

["Zentralisierte Dienste sind deaktiviert"](#)

["Authentifizierung für IP fehlgeschlagen"](#)

["Cisco Centralized Web Reporting ist im SWA deaktiviert"](#)

["Die Liste der URL-Kategorien auf dieser WSA war älter als die von der SMA veröffentlichte Liste."](#)

["Der Host-Schlüssel scheint sich geändert zu haben."](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird der Prozess der Integration der Secure Web Appliance (SWA) in die Security Management Appliance (SMA) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Zugriff auf die grafische Benutzeroberfläche (GUI) von SWA
- Administratorzugriff auf die SWA.
- Administratorzugriff auf die SMA.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

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.

Vorbereitungen

- 1. Stellen Sie sicher, dass SMA und SWA beide lizenziert sind.
- 2. Überprüfen Sie die Kompatibilitätsmatrix von SWA und SMA, verwenden Sie diesen Link: [SWA-SMA-ESA-Kompatibilitätsmatrix](#).

 Anmerkung: Stellen Sie sicher, dass die Version, die Sie integrieren möchten, nicht bereitgestellt wird.

Compatibility with Secure Web Appliance

Select Version

Secure Web Appliance

Secure Email and Web Manager

Search

Version Compatibility

☒ Show Deprovisioned Releases

Export to Excel

Secure Email and Web Manager	15.5.1-002 (MD)	15.5.0-710 (GD)	15.5.0-574 (GD)	15.5.0-566 (LD)	15.2.5-013 (MD)	15.2.4-022 (MD)	15.2.3-505 (HP)	15.2.3-007 (MD)	15.2.2-009 (MD)	15.2.2-009 (MD)	15.2.1-011 (MD)	15.2.0-164 (GD)	15.0.1-004 (MD)	15.0.0-612 (HP)	15.0.0-604 (MD)
16.0.1-010 (MD)									✓	✓	✓	✓	✓		
16.0.0-195 (GD) [Deprovisioned]*												✓	✓		
15.5.4-007 (MD)									✓	✓	✓	✓	✓		
15.5.3-017 (MD)									✓	✓	✓	✓	✓		

Bild - Nicht bereitgestellte Versionen

Schritte zur Integration von SWA in SMA

Schritt 1: Exportieren der Konfigurationsdatei aus SWA	Schritt 1.1. Navigieren Sie in der GUI zu Systemverwaltung, und wählen Sie Konfigurationsdatei. Schritt 1.2. Stellen Sie sicher, dass Datei auf lokalen Computer herunterladen zum Anzeigen oder Speichern ausgewählt ist. Schritt 1.3. Wählen Sie in den Konfigurationsdateien die Option Kennwörter verschlüsseln aus. Schritt 1.4. (Optional) Wählen Sie einen Namen für
--	---

die Konfigurationsdatei aus.

Schritt 1.5: Klicken Sie auf Senden.

Configuration File

Current Configuration

Configuration File:

- ☒ Download file to local computer to view or save
- ☐ Save file to this appliance (sourceSWA.amojarra.amojarra)
- ☐ Email file to:

Separate multiple addresses with commas. Maximum allowed characters 8192.

Password Display Options:

- ☒ Encrypt passwords in the Configuration Files
- ☐ Mask passphrases in the Configuration Files
Note: Files with masked passphrases cannot be loaded using Load Configuration.
- ☐ Use system-generated file name

Use user-defined file name:
Note: ".xml" will be appended to the specified file-name automatically.

Submit

Bild - Exportieren der Konfigurationsdatei

Schritt 2.1. Klicken Sie in der SMA-GUI auf die Registerkarte Web.

Schritt 2.2. Wählen Sie aus den Dienstprogrammen Configuration Manager aus.

Schritt 2.3. Wenn der Konfigurations-Manager noch nicht initialisiert ist, klicken Sie auf den Link Initialisieren für den gewünschten Konfigurations-Manager, andernfalls fahren Sie mit Schritt 2.5 fort.



Tipp: Die Configuration Manager-Version muss auf die ersten beiden Segmente der SWA-Version abgestimmt sein. Wenn Ihre SWA-Version beispielsweise 15.5.0-710 ist, müssen Sie Configuration Manager 15.5 verwenden.

Schritt 2: Erstellen des Konfigurations-Managers



Anmerkung: Wenn der Konfigurations-Manager bereits in der SMA konfiguriert ist, fahren Sie mit Schritt 4 fort.

Schritt 2.4. Wählen Sie Standardeinstellungen verwenden aus, und klicken Sie auf Initialisieren.

Schritt 2.5: Klicken Sie für den gewünschten Configuration Manager auf Import Configuration (Konfiguration importieren).

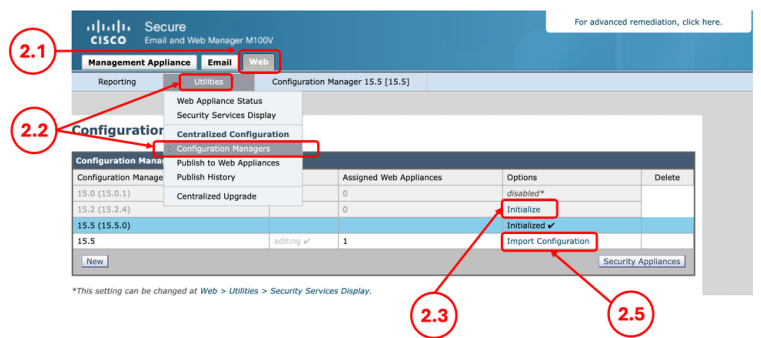


Bild - Konfigurationsmanager

Schritt 2.6. Wählen Sie aus der Konfigurationsquelle auswählen die Option Webkonfigurationsdatei aus.

Schritt 2.7. Wählen Sie die Konfigurationsdatei aus, die Sie in Schritt 1 exportiert haben.

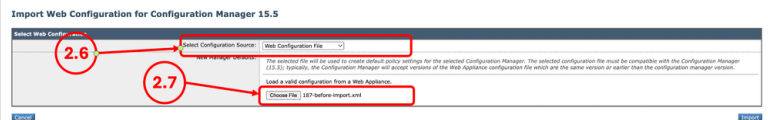


Bild - Konfiguration importieren

Schritt 2.8: Klicken Sie auf Importieren.

Schritt 2.9: Bestätigen Sie die Änderungen.

Schritt 3: Configuration Manager-Einstellungen

Schritt 3.1. Klicken Sie in der SMA-GUI auf die Registerkarte Web.

Schritt 3.2. Wählen Sie aus Dienstprogramme die Option Sicherheitsservices anzeigen aus.

Schritt 3.3. Stellen Sie sicher, dass die gewünschten Funktionen richtig konfiguriert sind, können Sie die Funktionen über Anzeigeeinstellungen bearbeiten aktivieren oder deaktivieren.

Schritt 3.4. Falls Sie Änderungen vorgenommen haben, senden und bestätigen.

Security Services Display

Configuration Manager Settings for Display of Security Services			
Features	Configuration Managers		
	15.0 (disabled)	15.2 (disabled)	15.5
Transparent mode	Yes	Yes	Yes
Range Request Forwarding	Yes	No	No
FTP Proxy	Yes	Yes	No
HTTPS Proxy	Yes	Yes	No
SOCKS Proxy	No	Yes	No
Upstream Proxy Groups	No	Yes	No
Acceptable Use Controls	Cisco Web Usage Controls (with Application Visibility and Control)	Cisco Web Usage Controls (with Application Visibility and Control)	Cisco Web Usage Controls (with Application Visibility and Control)
AnyConnect Secure Mobility	No	IP Range	No
Web Reputation Filters	Yes (Adaptive Scanning: Yes)	Yes (Adaptive Scanning: Yes)	Yes (Adaptive Scanning: Yes)
Advanced Malware Protection (File Reputation)	Yes (File Analysis: Yes)	Yes (File Analysis: Yes)	Yes (File Analysis: Yes)
Webroot Anti-Malware	Yes	Yes	Yes
McAfee Anti-Malware	No	Yes	No
Sophos Anti-Malware	Yes	Yes	Yes
End-User Acknowledgement	No	Yes	No
Cisco Data Security Filters	Yes	Yes	Yes
External DLP Servers	No	Yes	No
Credential Encryption	Yes	No	No
Identity Provider for SaaS	No	Yes	No

3.3

Bild - Sicherheitsservices-Anzeige

Schritt 4.1. Klicken Sie in der SMA-GUI auf die Registerkarte Management Appliance.

Schritt 4.2. Wählen Sie aus Zentralen Services Security Appliances aus.

Schritt 4.3. Klicken Sie auf Web-Appliance hinzufügen

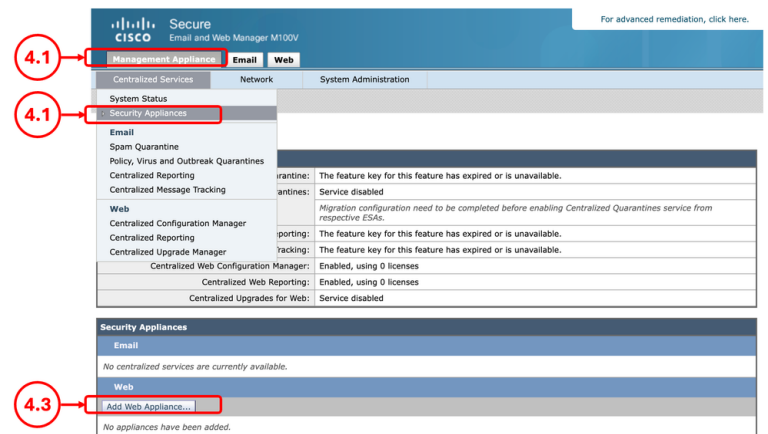


Bild: Web-Appliance hinzufügen

Schritt 4.4: Geben Sie den Appliance-Namen und die IP-Adresse oder den Hostnamen ein.

Schritt 4.5: Klicken Sie auf Verbindung herstellen.

Schritt 4.6: Geben Sie den Benutzernamen und die Passphrase ein, und klicken Sie auf Verbindung herstellen.

Schritt 4.7: Zuweisen des Konfigurations-Managers

Schritt 4: Web-Appliance hinzufügen

Bild - Hinzufügen des SWA

Schritt 4.8: Senden und bestätigen Sie die Änderungen.

Schritt 5.1. Klicken Sie in der SMA-GUI auf die Registerkarte Web.

Schritt 5.2. Wählen Sie unter Dienstprogramme die Option Web-Appliance-Status aus.

Schritt 5.3. Wenn eine Warnmeldung angezeigt wird, ist Aufmerksamkeit erforderlich. Klicken Sie auf den Namen der Appliance, klicken Sie auf den Namen der SWA, und zeigen Sie die Details an.

Web Appliance Status

⚠ Attention Required. Click on the appliance name for details.

Total Web Appliances: 1

Web Appliances							
Appliance Name	IP Address or Hostname	AsyncoS Version	User	Last Published Configuration		Security Services	
				Job Name	Configuration	Enabled	Disabled
SWA SMA Integration	10.48.48.181	15.5.0-710	admin	admin.10_Mar_2026.09:37	15.5	12	11

Bild - Status der Web-Appliance

Tipp: Weitere Informationen zur Fehlerbehebung finden Sie im Abschnitt Behebungsfehler in diesem Artikel.

Beheben von Fehlern

"Zentrale Dienste sind deaktiviert"

Wenn Sie versuchen, einen zentralen Dienst auszuwählen, klicken Sie, wenn das Kontrollkästchen inaktiv ist, auf das Fragezeichen (?) und der Leitfaden navigiert Sie durch den Pfad, um diesen Dienst zu aktivieren.

Add Web Appliance

Web Appliance Settings	
Appliance Name:	SWA SMA Integration
IP Address or Hostname:	10.48.48.1
Web Appliance Centralized Services:	☒ Centralized Configuration Manager ☒ Centralized Reporting ☐ Centralized Upgrades: service disabled ?
Connection Status:	Not established. Establish an SSH connection for Centralized W Establish Connection... Test Connection
Assign Configuration Manager: ?	More assignment options may be enabled once an SSH connection is established. ☒ Not Assigned ☐ 15.5

Upgrade Enable

To enable the services navigate to centralized services -> centralized upgrade Manager .

Cancel Submit

Bild - Die zentralen Dienste sind deaktiviert.

"Authentifizierung für IP fehlgeschlagen"

Wenn Sie diesen Fehler erhalten, stellen Sie bei der Integration der SWA in SMA sicher, dass die IP-Adresse oder der Hostname und die Anmeldeinformationen korrekt sind.

Add Web Appliance

Error — Authentication Failed for IP: 10.48.48.181.

Web Appliance Settings	
Appliance Name:	SWA SMA Integration
IP Address or Hostname:	10.48.48.181
Web Appliance Centralized Services:	☒ Centralized Configuration Manager ☒ Centralized Reporting ☐ Centralized Upgrades: service disabled ?
Connection Status:	Not established. Establish an SSH connection for Centralized Web Services. Establish Connection... Test Connection
Assign Configuration Manager: ?	More assignment options may be enabled once an SSH connection is established. ☒ Not Assigned ☐ 15.5

Cancel Submit

Bild - Authentifizierung fehlgeschlagen

"Cisco Centralized Web Reporting ist im SWA deaktiviert"

Wenn die SMA mit dem zentralen Web-Reporting konfiguriert ist und Sie diese Funktion dem SWA zuweisen, während Sie das SWA in SMA in "Schritt 4" integrieren, müssen Sie Cisco

zentrales Web-Reporting aktivieren:

Security Services					
 One or more of the services on the Web Appliance does not match the corresponding <i>Security Service Display</i> setting on the Management Appliance.					
Description	Services		Feature Keys		
	Web Appliance Service	Is Service Displayed on Management Appliance?	Status	Time Remaining	Expiration Date
Cisco Web Proxy & DVS(TM) Engine	Enabled	Yes	Active	Perpetual	N/A
Cisco L4 Traffic Monitor	Enabled	N/A	Active	Perpetual	N/A
Proxy Mode	Transparent	Yes (Bypass Proxy)			
Range Request Forwarding	Disabled	No			
FTP Proxy	Disabled	No			
Cisco HTTPS Proxy	Disabled	No	Active	Perpetual	N/A
SOCKS Proxy	Disabled	No			
Upstream Proxy Groups	Configured	No (Routing Policies)			
AnyConnect Secure Mobility	Disabled	No	Active	Perpetual	N/A
Cisco URL Filtering	N/A	N/A	N/A	N/A	N/A
Cisco Web Usage Controls	Enabled	Yes	Active	Perpetual	N/A
Application Visibility and Control	Enabled	Yes			
Application Discovery and Control	Disabled	No			
Cisco Centralized Web Reporting	Disabled	Yes			
Cisco Web Reputation Filters	Enabled	Yes	Active	Perpetual	N/A
Adaptive Scanning	Enabled	Yes			
Advanced Malware Protection (File Reputation)	Enabled	Yes	Active	Perpetual	N/A
File Analysis	Enabled	Yes	Active	Perpetual	N/A
Webroot Anti-Malware	Enabled	Yes	Active	Perpetual	N/A
McAfee Anti-Malware	N/A	No	N/A	N/A	N/A
Sophos Anti-Malware	Enabled	Yes	Active	Perpetual	N/A
End-User Acknowledgement	Disabled	No			
Cisco Data Security Filters	Enabled	Yes			
External DLP Servers	Not Configured	No			
Credential Encryption	Disabled	No			
Identity Provider for SaaS	Not Configured	No			

Bild - Centralized Web Reporting ist im SWA deaktiviert

Um das Problem zu beheben, stellen Sie über die CLI eine Verbindung mit dem SWA her, geben Sie `reportingconfig` ein, und wählen Sie **CENTRALIZED (ZENTRALISIERT)** aus. Folgen Sie dem Assistenten, um das zentrale Reporting zu aktivieren und bestätigen Sie die Änderungen.

```
SWA_CLI> reportingconfig
```

Choose the operation you want to perform:

- COUNTERS - Limit counters recorded by the reporting system.
 - WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
 - AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
 - WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
 - CTROBSERVABLE - Enable or Disable CTR observable based indexing.
 - CENTRALIZED - Enable/Disable Centralized Reporting for this Secure Web Appliance.
- ```
[> CENTRALIZED
```

Reporting service status: Local Reporting enabled. (Show usernames in reports.)

```
Do you want to enable Centralized Reporting for this appliance? [N]> Y
```

Do you want to anonymize usernames in reports? [N]> N

Reporting service status: Centralized Reporting enabled. (Show usernames in reports.)

Choose the operation you want to perform:

- COUNTERS - Limit counters recorded by the reporting system.
- WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
- AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
- WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
- CTROBSERVABLE - Enable or Disable CTR observable based indexing.
- CENTRALIZED - Enable/Disable Centralized Reporting for this Secure Web Appliance.

[>

SWA\_CLI> commit

"Die Liste der URL-Kategorien auf dieser WSA war älter als die von der SMA veröffentlichte Liste."

Wenn Sie während des Veröffentlichens der Konfiguration in SWA und des Empfangens des Fehlers darauf hinweisen, dass die URL-Kategorieliste in SWA und SMA nicht identisch ist, stellen Sie sicher, dass beide Geräte eine Verbindung mit dem Cisco Update Server herstellen können und es keine Fehler in "updater\_logs" gibt:

### Publish in Progress: admin.10\_Mar\_2026.13:19

**Warning** — Configuration Publish job admin.10\_Mar\_2026.13:19 has completed. The configuration was not successfully published to at least one of the destination web appliances.

| Job admin.10_Mar_2026.13:19 Started at 10 Mar 2026 13:19 (GMT) |             |                                                                                                           |
|----------------------------------------------------------------|-------------|-----------------------------------------------------------------------------------------------------------|
| Web Appliances                                                 | Progress    | Status                                                                                                    |
| SWA SMA Integration                                            | <div></div> | Failure: The list of URL categories on this WSA was older than the list published... <a href="#">more</a> |

Final status of this job will be reported on the [Publish History](#) page.

Close

Bild: Die Liste der URL-Kategorien stimmt nicht überein.

Um SWA oder SMA zu zwingen, das Update herunterzuladen, geben Sie `updatenow` aus der CLI ein.

Um die SMA oder SMA anzuzeigen, geben Sie im CLI-Typ `grep` die zu aktualisierenden Protokolle ein, und wählen Sie die Nummer aus, die mit `updater_logs` verknüpft ist, und folgen Sie dem Assistenten.

 Tipp: Um die Live-Protokolle anzuzeigen, geben Sie "Y" in die Antwort `Do you want to tail the logs` (Möchten Sie die Protokolle zurückverfolgen) ein. [N]>.

"Der Host-Schlüssel scheint sich geändert zu haben."

Wenn Sie die SWA in die SMA integrieren und den Fehler erhalten, dass der Host-Schlüssel

geändert wurde, liegt dies daran, dass SMA einen anderen Host-Schlüssel für dieselbe IP-Adresse in seinem Schlüsselspeicher gespeichert hat.

### Edit Web Appliance: Source SWA

**Error** — The host key for 10.48.48.181 appears to have changed.

- It is possible that someone is trying to hijack the encrypted connection to the remote host. Please use the `logconfig->hostkeyconfig` command to verify (and possibly update) the SSH host key for 10.48.48.181.

| Web Appliance Settings              |                                                                                                                                                                                                         |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Appliance Name:                     | Source SWA                                                                                                                                                                                              |
| IP Address or Hostname:             | 10.48.48.181                                                                                                                                                                                            |
| Web Appliance Centralized Services: | <input checked="" type="checkbox"/> Centralized Configuration Manager<br><input checked="" type="checkbox"/> Centralized Reporting<br><input type="checkbox"/> Centralized Upgrades: service disabled ? |
| Connection Status:                  | File transfer credentials have been established.<br><i>Establish an SSH connection for Centralized Web Services.</i><br><a href="#">Establish Connection...</a> <a href="#">Test Connection</a>         |
| Assign Configuration Manager: ?     | <i>More assignment options may be enabled once an SSH connection is established.</i><br><input checked="" type="radio"/> Not Assigned<br><input type="radio"/> 15.5                                     |

[Cancel](#) [Submit](#)

Bild - Der Host-Schlüssel scheint sich geändert zu haben.

Um diesen Fehler zu beheben, melden Sie sich bei der CLI von SMA an, führen Sie `logconfig` aus, und geben Sie `HOSTKEYCONFIG` ein. Geben Sie `LÖSCHEN` ein, und drücken Sie die Eingabetaste. Wählen Sie dann die Nummer aus, die dem SWA zugeordnet ist, und drücken Sie die Eingabetaste, bis der Assistent beendet ist.

Bestätigen Sie die Änderungen:

```
SMA_CLI> logconfig
```

Currently configured logs:

| Log Name            | Log Type            | Retrieval       | Interval |
|---------------------|---------------------|-----------------|----------|
| -----               |                     |                 |          |
| 1. aggregatord_logs | Aggregatord Logs    | Manual Download | None     |
| 2. authentication   | Authentication Logs | Manual Download | None     |
| ...                 |                     |                 |          |

Choose the operation you want to perform:

- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- DELETELOGFILE - Delete log files
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.

```
[> HOSTKEYCONFIG
```

Currently installed host keys:

```
1. 10.48.48.182 ssh-rsa AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...ZhW4gEXWE=
2. 10.48.48.181 ssh-rsa BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBb...4p74b9Q9k=
```

Choose the operation you want to perform:

- NEW - Add a new key.
  - EDIT - Modify a key.
  - DELETE - Remove a key.
  - SCAN - Automatically download a host key.
  - PRINT - Display a key.
  - HOST - Display system host keys.
  - FINGERPRINT - Display system host key fingerprints.
  - USER - Display system user keys.
  - REGENERATESCPKEYS - Regenerate SSH Keys for SCP Log Subscription Retrieval.
- ```
[> DELETE
```

Enter the number of the key you wish to delete.

```
[> 2
```

Currently installed host keys:

```
1. 10.62.131.143 ssh-rsa AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...ZhW4gEXWE=
```

```
...
```

```
SMA_CLI> commit
```

Zugehörige Informationen

- [Bedienungsanleitung für AsyncOS 15.2 für Cisco Secure Web Appliance](#)
- [Installieren der sicheren Web-Appliance auf VMware ESXi](#)
- [Installieren der sicheren Web-Appliance auf Microsoft Hyper-V](#)
- [Ersteinrichtung der sicheren Web-Appliance](#)
- [Installationsleitfaden für die Cisco Secure Email und Web Virtual Appliance](#)
- [Benutzerdefinierte URL-Kategorien in einer sicheren Web-Appliance konfigurieren - Cisco](#)
- [Best Practices für sichere Web-Appliances](#)
- [Firewall für sichere Web-Appliance konfigurieren](#)
- [Entschlüsselungszertifikat in sicherer Web-Appliance konfigurieren](#)
- [Fehlerbehebung beim DNS-Dienst der sicheren Webappliance](#)

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.