

# Ripristina versione precedente di Secure Web Appliance

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Operazioni preliminari](#)

[Preparazione e backup dell'SWA](#)

[Passaggio 1. Esportare il file di configurazione](#)

[Passaggio 2. Esportare il certificato di decrittografia](#)

[Passaggio 3. Esportare i certificati radice del trust personalizzato](#)

[Passaggio 4. Esportare il certificato GUI](#)

[Passaggio 5. Esportare i certificati ISE](#)

[Passaggio 6. Licenze/Funzionalità](#)

[Passaggio 7. Certificato di reindirizzamento dell'autenticazione](#)

[Passaggio 8. Esportazione delle route statiche](#)

[Passaggio 9. Impostazioni DNS](#)

[Ripristinare lo SWA](#)

[Passaggio 10. Ripristino dell'SWA](#)

[Configurazione ripristinata SWA](#)

[Passaggio 11. Concessione in licenza dell'SWA](#)

[Passaggio 12. Eseguire l'installazione guidata sistema](#)

[Passaggio 13. Importazione di certificati radice attendibili personalizzati](#)

[Passaggio 14. Importazione del file di configurazione](#)

[Passaggio 15. Importazione dei cicli di lavorazione](#)

[Passaggio 16. Configurare le impostazioni DNS](#)

[Passaggio 17. Aggiungere o riaggiungere l'SWA ad Active Directory](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto come ripristinare la versione precedente di Secure Web Appliance (SWA).

# Prerequisiti

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso all'interfaccia grafica dell'SWA
- Accesso amministrativo all'SWA
- Accesso al portale delle licenze software Cisco o al file di licenza SWA
- Accesso utente privilegiato di Active Directory per l'aggiunta dell'SWA al dominio e la creazione di record DNS

## Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.


## Operazioni preliminari

Il ripristino dell'accessorio è estremamente distruttivo.

Questi sono i dati che vengono distrutti nel processo e di cui è necessario eseguire il backup:

- File di configurazione del sistema corrente.
- Tutti i file di log (per ulteriori informazioni, visitare il sito Web all'indirizzo [Access Secure Web Appliance Logs](#) )
- Tutti i dati dei report (inclusi i report salvati pianificati e archiviati)
- Pagine di notifica personalizzate per l'utente finale.

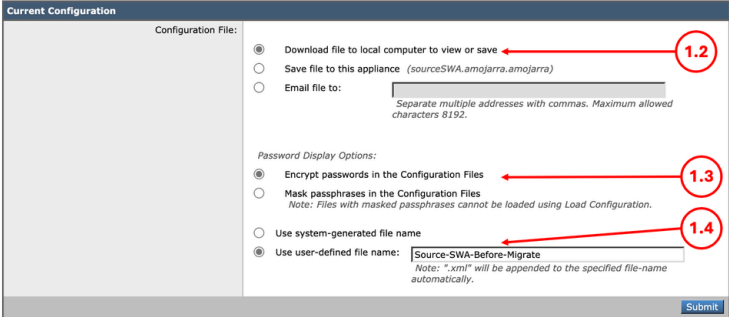

---

 **Avviso:** Prima di ripristinare una versione precedente, assicurarsi di disporre del file di configurazione crittografato corrispondente alla versione specifica. È possibile che il file di configurazione corrente non sia compatibile con versioni software precedenti.

---

# Preparazione e backup dell'SWA

Per raccogliere i file e la configurazione necessari dall'SWA prima del ripristino, attenersi alla procedura descritta di seguito.

<p>Passaggio 1. Esportare il file di configurazione</p>	<p>Passaggio 1.1. Dalla GUI, passare a Amministrazione sistema e scegliere File di configurazione.</p> <p>Passaggio 1.2. Assicurarsi che l'opzione Scarica file nel computer locale per visualizzare o salvare sia selezionata.</p> <p>Passaggio 1.3. Scegliere Encrypt password nei file di configurazione</p> <p>Passaggio 1.4. (Facoltativo) Scegliere un nome per il file di configurazione.</p> <p>Passaggio 1.5. Fare clic su Sottometti.</p> <p><b>Configuration File</b></p>  <p>Immagine - Esportazione del file di configurazione</p>
<p>Passaggio 2. Esportare il certificato di decrittografia</p> <hr/> <p> Nota: Se la decrittografia HTTPS è disabilitata, andare al passaggio 3.</p>	<p>Passaggio 2.1. Dalla GUI, selezionare Security Services e fare clic su HTTPS Proxy.</p> <p>Passaggio 2.2. Fare clic su Modifica impostazioni.</p> <p>Passaggio 2.3. Scaricare il certificato di decrittografia HTTPS facendo clic su Scarica certificato... collegamento.</p>

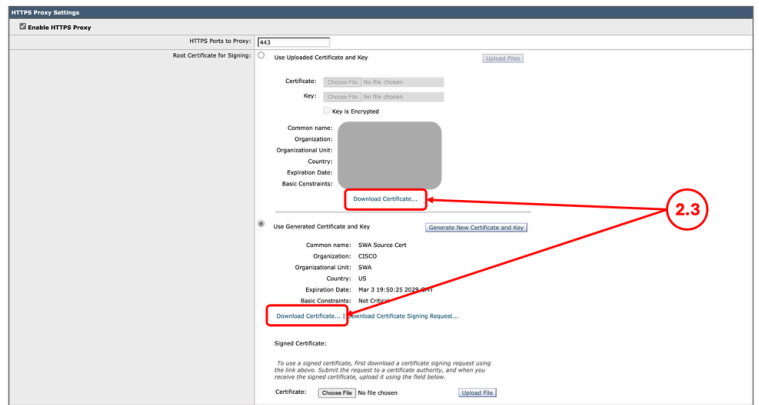


Immagine - Certificato di decrittografia HTTPS



Nota: In questo esempio vengono illustrati entrambi i tipi di certificati di decrittografia HTTPS. tuttavia, nella rete è possibile distribuire un solo tipo.

Passaggio 3. Esportare i certificati radice del trust personalizzato

Passaggio 3.1. Dalla GUI, passare alla rete e fare clic su Gestione certificati.

Passaggio 3.2. Nella sezione Gestione certificati fare clic su Gestisci certificati radice attendibili.

#### Certificate Management

Certificate	Common Name	Issued By	Domains	Status	Time Remaining	Expiration Date	Delete
SWA Source GUI Certificate	SWA Source GUI Certificate	SWA Source GUI Certificate	N/A	Active	799 days	May 11 20:14:56 2028 GMT	

Weak Signature Usage Settings: Restrict Weak Signature Usage: Disabled [Edit Settings](#)

Certificate FQDN Validation Settings: Certificate FQDN Validation Usage: Disabled [Edit Settings](#)

File Type	Last Update	Current Version	New Update
Cisco Trusted Root Certificate Bundle	Success - Fri Feb 27 20:18:56 2026	2.6	Not Available
Cisco Certificate Blocked List	Success - Fri Feb 27 20:18:56 2026	1.3	Not Available

No updates in progress. [Update Now](#)

**Certificate Management**

Trust Root Certificates: 246 certificates in Cisco trusted root certificate list  
6 custom certificates added to trusted root certificate list [Manage Trusted Root Certificates...](#)

Certificate Based Authentication/RADSEC Root Certificates: 0 custom root certificates added to Certificate Based Authentication/RADSEC root certificate list [Manage Certificate Based Authentication/RADSEC Root Certificates...](#)

Blocked Certificates: 19 certificates in Cisco blocked certificate list [View Blocked Certificates...](#)

Immagine - Gestisci certificati radice attendibili


Passaggio 3.3. Espandere ogni certificato radice attendibile personalizzato facendo clic sul relativo

nome e quindi su Scarica certificato...

Immagine - Scarica certificati radice attendibili



## Passaggio 4. Esportare il certificato GUI

 Nota: Se si utilizza un certificato GUI incorporato, andare al passaggio 5.

Passaggio 4.1. Dalla GUI, passare alla rete e fare clic su Gestione certificati.

Passaggio 4.2. Nella sezione Certificati accessorio fare clic su Esporta certificato.

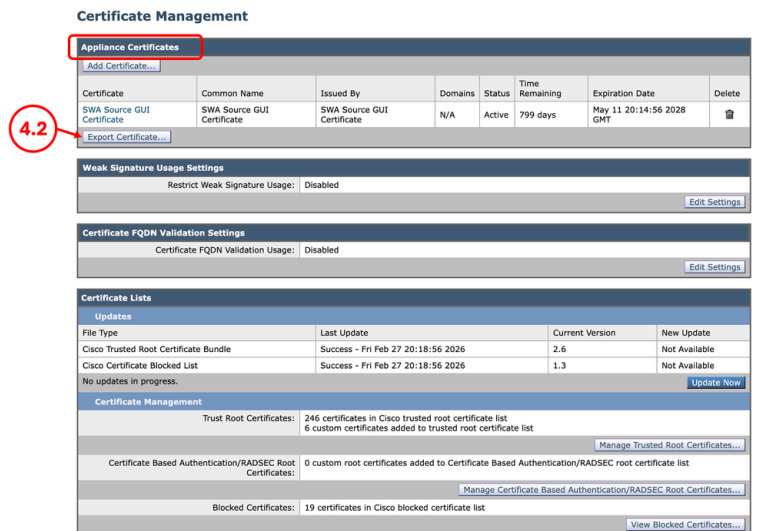



Immagine - Esporta certificato GUI

## Passaggio 5. Esportare i certificati ISE

 Nota: Se non ci sono SWA, integrazione ISE, andare al passo 6.

Passaggio 5.1. Dalla GUI, spostarsi su Network e fare clic su Identity Services Engine.

Passaggio 5.2. Fare clic su Modifica impostazioni.

Passaggio 5.3. Scaricare tutti i certificati disponibili.

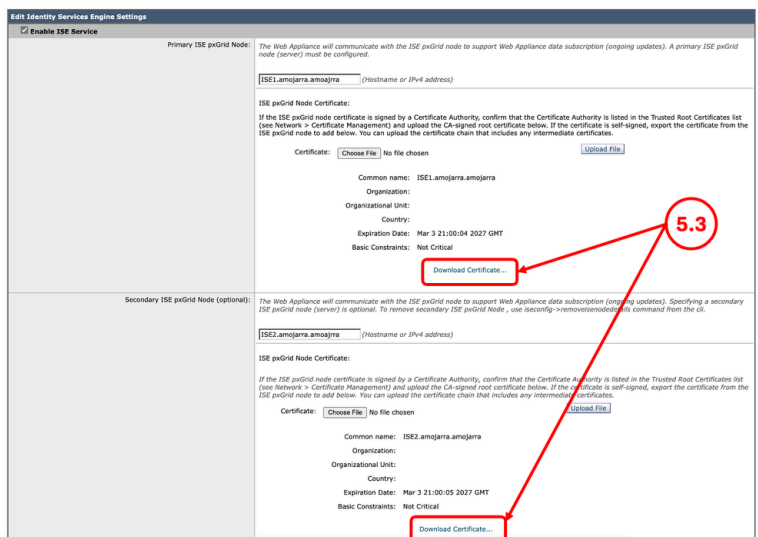


Immagine - Download dei certificati ISE

## Passaggio 6. Licenze/Funzionalità

Passaggio 6.1. Dalla GUI, selezionare System Administration e fare clic su Licenze o Funzionalità a

seconda del tipo di licenza in uso.

Passaggio 6.2. Acquisire una schermata delle licenze e delle funzionalità.

Passaggio 7.1. Dalla GUI, selezionare Network (Rete) e fare clic su Authentication (Autenticazione).

Passaggio 7.2. Se la crittografia delle credenziali è abilitata, assicurarsi di disporre del certificato e della chiave.

Passaggio 7.3. Catturare uno screenshot della configurazione corrente.

Passaggio 7. Certificato di reindirizzamento dell'autenticazione

#### Authentication

Realms Name	Server Type	Scheme(s)	Servers	Transparent User Identification	Base DN or NetBIOS Domain	Delete
ADDS	Active Directory	Kerberos, NTLMSSP, Basic	10.48.48.17	Not Enabled	AMOJARRA	

**Global Authentication Settings**

Action if Authentication Service Unavailable: Block all traffic if authentication fails  
Failed Authentication Handling: Log Guest User by: IP Address  
Re-authentication: Disabled  
Basic Authentication Token TTL: 3600

**Authentication Settings**

Credential Encryption: Enabled  
HTTPS Redirect Port: 443  
Redirect Hostname: P1-SWA-Source.amojarra.amojarra  
Credential Cache Options: Surrogate Timeout: 3600 seconds, Client IP Idle Timeout: 3600 seconds  
User Session Restrictions: Disabled  
Header Based Authentication: Disabled  
Secure Authentication Certificate: Common name: SWA Source Authentication Certificate, Organization: Cisco, Organizational Unit: SWA, Country: US, Expiration Date: Mar 3 20:31:36 2027 GMT, Basic Constraints: Not Critical

Immagine - Certificato di autenticazione



Nota: Non è possibile scaricare il certificato di autenticazione dalla GUI.

Passaggio 8. Esportazione delle route statiche

Passaggio 8.1. Dalla GUI, selezionare Network (Rete) e fare clic su Routing.


Passaggio 8.2. Per ciascuna tabella di routing, fare clic su Salva tabella di routing.



Nota: Se si intende utilizzare la stessa configurazione di rete e lo stesso indirizzo IP per il file SWA di destinazione, andare al passo 10.

#### Routes




Route Name	Destination	Gateway	All
10.1.1.0	10.1.1.0/24	10.62.131.1	<input type="checkbox"/>
10.3.3.0	10.3.3.0/24	10.62.131.1	<input type="checkbox"/>
10.4.4.0	10.4.4.0/24	10.62.131.1	<input type="checkbox"/>
10.2.2.0	10.2.2.0/24	10.62.131.1	<input type="checkbox"/>
Default Route	All Others	10.62.131.1	<input type="checkbox"/>

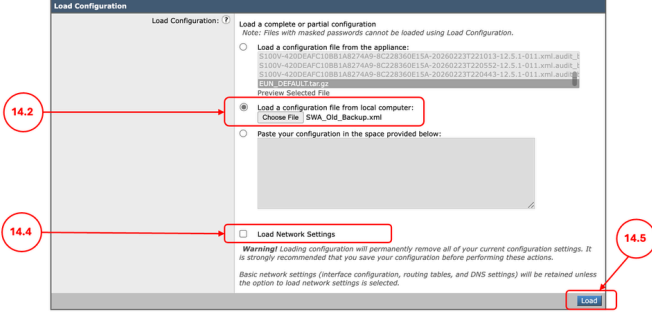


	Immagine - Esportazione tabella di routing
Passaggio 9. Impostazioni DNS	Passaggio 9.1. Dalla GUI, passare a Rete e fare clic su DNS.
 Nota: Se si intende utilizzare la stessa configurazione di rete e lo stesso indirizzo IP per il file SWA di destinazione, andare al passo 10.	Passaggio 9.2. Acquisire una schermata della configurazione DNS.

## Ripristinare lo SWA

Passaggio 10. Ripristino dell'SWA	<p>Passaggio 10.1. Connettersi alla CLI.</p> <p>Passaggio 10.2. Digitare revert e premere Invio.</p> <p>Passaggio 10.3. Digitare Y e premere Invio per continuare? [N]&gt; "</p> <p>Passaggio 10.4. Digitare Y e premere Invio per "Continuare? [N]&gt;"</p> <p>Passaggio 10.5. Scegliere il numero associato alla versione che si desidera ripristinare dall'elenco e premere Invio.</p> <pre>SWA_CLI&gt; revert</pre> <p>This command will revert the appliance to a previous version of AsyncOS.</p> <p>Warning: Reverting the appliance is extremely destructive. The following data will be destroyed in the process and should be backed up:</p> <ul style="list-style-type: none"> <li>- current system configuration file</li> <li>- all log files</li> <li>- all reporting data (including saved scheduled and archived reports)</li> <li>- any custom end user notification pages</li> </ul> <p>This command will try to preserve the current network settings.</p> <p>Reverting the device will cause a reboot to take place. After rebooting, the appliance reinitializes itself and reboots again to the desired version, with the earlier system configuration.</p> <pre>Do you want to continue? [N]&gt; Y Are you sure you want to continue? [N]&gt; Y</pre> <pre> Available versions ===== 1. 12.5.1-011 Please select an AsyncOS version: 1 You have selected "12.5.1-011". The system will now reboot to perform the revert operation.</pre>
-----------------------------------	---

## Configurazione ripristinata SWA

Passaggio 11. Concessione in licenza dell'SWA	Passaggio 11.1. Per ulteriori informazioni, visitare il sito Web all'indirizzo <a href="#">Configure Secure Web Appliance Initial Setup</a> .
Passaggio 12. Eseguire l'Installazione guidata sistema	Passaggio 12.1. Per ulteriori informazioni, visitare il sito Web all'indirizzo: <a href="#">Configure Secure Web Appliance Initial Setup</a> .
Passaggio 13. Importazione di certificati radice attendibili personalizzati	Passaggio 13.1. Dalla GUI, passare alla rete e fare clic su Gestione certificati. Passaggio 13.2. Nella sezione Gestione certificati fare clic su Gestisci certificati radice attendibili. Passaggio 13.3. Fare clic su Import.
 Nota: Se non si utilizza un certificato radice attendibile personalizzato, andare al passaggio 14.	Passaggio 13.4. Caricare i certificati precedentemente scaricati nel Passaggio 3.
	 Attenzione: Quando sono disponibili sia i certificati radice che i certificati intermedi, iniziare caricando il certificato CA radice. Dopo l'invio e il commit delle modifiche, procedere con l'importazione del certificato intermedio.
Passaggio 14. Importazione del file di configurazione	Passaggio 14.1. Dalla GUI, selezionare System Administration e scegliere Configuration File. Passaggio 14.2. Nella sezione Carica configurazione, selezionare Carica file di configurazione dal computer locale.
 Attenzione: Accertarsi di importare il file di configurazione corrispondente alla versione corrente e non il file di configurazione esportato al punto 1.	Passaggio 14.3. Fare clic su Scegli file e selezionare il file di configurazione XML correlato alla versione corrente. Passaggio 14.4. (Facoltativo) Se il ripristino ha rimosso l'indirizzo IP e la configurazione di rete,

	<p>selezionare la casella di controllo Carica impostazioni di rete, altrimenti non selezionare questa opzione.</p> <p>Passaggio 14.5. Fare clic su Carica.</p> <p>Passaggio 14.6. Fare clic su Continue (Continua) nel popup Confirm Load Configuration (Conferma caricamento configurazione).</p>  <p>Immagine - Carica il file di configurazione precedente</p> <p>Passaggio 14.7. Confermare le modifiche.</p>
<p>Passaggio 15. Importazione dei cicli di lavorazione</p> <hr/> <p> Nota: se si caricano le impostazioni di rete durante l'importazione della configurazione, andare al passo 17.</p>	<p>Passaggio 15.1. Dalla GUI, selezionare Network (Rete) e fare clic su Routing.</p> <p>Passaggio 15.2. Per ciascuna tabella di routing, fare clic su Carica tabella di routing.</p> <p>Passaggio 15.3. Scegliere il file esportato al passaggio 8.</p> <p>Passaggio 15.4. Fare clic su Sottometti.</p> <p>Passaggio 15.5. Confermare le modifiche.</p>
<p>Passaggio 16. Configurare le impostazioni DNS</p> <hr/> <p> Nota: Se si caricano le impostazioni di rete durante l'importazione della configurazione, andare al passo 17.</p>	<p>Passaggio 16.1. Dalla GUI, passare a Rete e fare clic su DNS.</p> <p>Passaggio 16.2. Fare clic su Modifica impostazioni.</p> <p>Passaggio 16.3. Usare lo screenshot dal Passaggio 9</p> <p>Passaggio 16.4. Fare clic su Submit (Invia).</p>

Passaggio 16.5. Confermare le modifiche.

Passaggio 17.1. Dalla GUI, selezionare Network (Rete) e fare clic su Authentication (Autenticazione).

Passaggio 17.2. Fare clic sul nome del realm di autenticazione.



Suggerimento: Se all'SWA vengono assegnati un nuovo indirizzo IP e un nuovo nome host, verificare che nel servizio DNS di Active Directory siano stati creati i record DNS necessari.

Passaggio 17.3. Fare clic su Aggiungi a dominio e immettere le credenziali:

**Add Realm**

Authentication Realm

Realm Name: ADDS

Authentication Server Type and Scheme(s): Active Directory (Kerberos, NTLMSSP or Basic Authentication)

**Active Directory Authentication**

Active Directory Server: Specify up to three Active Directory servers:

Set Source Interface

Source Interface: Management

10.48.48.17

hostname or IP address

Active Directory Account: Active Directory Domain: amojarra.amojarra

Computer Account: Computers

Location: Computers (Example: Computers/BusinessUnit/Department/Servers)

Enable Trusted Domain Lookup

**Join Domain...**

Status: Computer account fordwsa125\$ not yet created.

Immagine - Aggiungi ad Active Directory

Passaggio 17.4. Fare clic su Sottometti.

Passaggio 17.5. Se la crittografia delle credenziali è abilitata, importare il certificato di autenticazione sicura.

Passaggio 17.6. Verificare che il nome host di reindirizzamento sia corretto.

Passaggio 17. Aggiungere o riaggiungere l'SWA ad Active Directory

## Authentication

Authentication Realms						
Add Realm...						
Realm Name	Server Type	Schema(s)	Servers	Transparent User Identification	Base DN or NetBIOS Domain	Delete
ADDS	Active Directory	Kerberos, NTLMSSP, Basic	10.48.48.17	Not Enabled	AMQJARRA	

Global Authentication Settings	
Action if Authentication Service Unavailable:	Block all traffic if authentication fails
Failed Authentication Handling:	Log Guest User by: IP Address
Re-authentication:	Disabled
Basic Authentication Token TTL:	3600

Authentication Settings	
Credential Encryption:	Disabled
Redirect Hostname:	wsa-source.cisco.local
Credential Cache Options:	Surrogate Timeout: 3600 seconds Client IP Idle Timeout: 3600 seconds
User Session Restrictions:	Disabled
Header Based Authentication:	Enabled

[Edit Global Settings...](#)

17.5

17.6

Immagine - Impostazioni di autenticazione

Passaggio 17.7. Confermare le modifiche.

## Informazioni correlate

- [Guida per l'utente di AsyncOS 15.2 per Cisco Secure Web Appliance](#)
- [Installazione iniziale di Secure Web Appliance](#)
- [Utilizzare le procedure ottimali per Secure Web Appliance](#)
- [Accesso ai registri protetti di Web Appliance](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).