

Migrazione della configurazione tra due SWA

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Operazioni preliminari](#)

[Preparazione e backup dell'SWA di origine](#)

[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](#)

[Preparazione del file SWA di destinazione](#)

[Passaggio 10. Installazione dell'SWA virtuale](#)

[Passaggio 11. Configurazione iniziale di SWA](#)

[Passaggio 12. Eliminazione dei file di configurazione](#)

[Importazione del file di configurazione nel file SWA di destinazione](#)

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

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

[Passaggio 15. Modifica della password amministratore](#)

[Passaggio 16. Esecuzione](#)

[Passaggio 17. Importazione dei cicli di lavorazione](#)

[Passaggio 18. Configurazione delle impostazioni DNS](#)

[Passaggio 19. Aggiungere o riaggiungere l'SWA ad Active Directory](#)

[Passaggio 20. Partecipare di nuovo a SMA](#)

[Correzione degli errori](#)

[Errore di analisi sull'elemento port_name](#)

[Errore di analisi nell'elemento ise_service](#)

[Il failover non funziona sul nuovo SWA virtuale](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto il processo di ripristino della configurazione da un'appliance Web sicura (SWA) a un'altra.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso all'interfaccia grafica dell'SWA
- Accesso amministrativo all'SWA
- Accesso amministrativo a Security Management Appliance (SMA)
- 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

In questo articolo vengono descritti i passaggi necessari per eseguire la migrazione dal file SWA di origine a quello di destinazione. In questa tabella vengono elencate le specifiche di ciascun sistema.

	SWA di origine	SWA di destinazione
Modello	S396	S100v
Version	15.5.0-710	15.5.0-710
Licenza	Smart License	Smart License
Active Directory	Iscritto	Iscritto
Integrazione con Identity Services Engine (ISE)	Sì	Sì

Numero di schede di interfaccia di rete	5	5
Decrittografia HTTPS	Abilitato con certificato autofirmato	Abilitato con certificato autofirmato
Reindirizzamento trasparente	WCCP	WCCP
Gestito da SMA	Sì	Sì
Server di log esterno	Push SCP	Push SCP
Alta disponibilità	Attivato	Attivato

 Nota: Quando si installa un nuovo SWA virtuale, verificare sempre che tutte le interfacce di rete consigliate da Cisco siano presenti e configurate sulla macchina virtuale (VM). Le interfacce possono rimanere disconnesse, ma devono essere disponibili all'interno della VM.

Esistono due scenari possibili per la migrazione dell'SWA da un dispositivo a un altro:

[Scenario-1] Sostituzione dell'SWA esistente: L'SWA originale viene smantellato e l'indirizzo IP dell'SWA di destinazione coincide con quello dell'SWA di origine.

[Scenario-2] Aggiunta di un nuovo SWA: Il file SWA originale rimane in servizio mentre il nuovo file SWA è configurato.

Preparazione e backup dell'SWA di origine

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

Passaggio 1. Esportare il file di configurazione	Passaggio 1.1. Dalla GUI, passare a Amministrazione sistema e scegliere File di configurazione. Passaggio 1.2. Assicurarsi che l'opzione Scarica file nel computer locale per visualizzare o salvare sia selezionata. Passaggio 1.3. Scegliere Encrypt password nei file di configurazione Passaggio 1.4. (Facoltativo) Scegliere un nome per il file di configurazione.
--	--

Passaggio 1.5. Fare clic su Sottometti.

Configuration File

Current Configuration

Configuration File:

☒ Download file to local computer to view or save 1.2

☐ 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 1.3

☐ 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: 1.4
Note: ".xml" will be appended to the specified file-name automatically.

Immagine - Esportazione del file di configurazione

Passaggio 2.1. Dalla GUI, selezionare Security Services e fare clic su HTTPS Proxy.

Passaggio 2.2. Fare clic su Modifica impostazioni.

Passaggio 2.3. Scaricare il certificato di decrittografia HTTPS facendo clic su Scarica certificato... collegamento.

HTTPS Proxy Settings

☒ Enable HTTPS Proxy

HTTPS Ports to Proxy:

Root Certificate For Signing: ☐ Use Uploaded Certificate and Key

Certificate:

Key:

☐ Key is Encrypted

Common name:

Organization:

Organizational Unit:

Country:

Expiration Date:

Basic Constraints:

2.3

☒ Use Generated Certificate and Key

Common name: SWA Source Cert

Organization: CISCO

Organizational Unit: SWA

Country: US

Expiration Date: Mar 3 19:50:23 2025 GMT

Basic Constraints: Not Critical

Signed Certificate:

To use a signed certificate, first download a certificate signing request using the link above. Select the request for a certificate authority, and when you receive the signed certificate, upload it using the field below.

Certificate:

Immagine - Certificato di decrittografia HTTPS

Passaggio 2. Esportare il certificato di decrittografia



Nota: Se la decrittografia HTTPS è disabilitata, andare al passaggio 3.



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



Nota: Se nel file SWA non è stato

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.



aggiunto alcun certificato radice attendibile personalizzato, andare al passaggio 4.

Certificate Management

Appliance Certificates

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](#)

Certificate Lists

Updates

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

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

Passaggio 4. Esportare il certificato GUI



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

Certificate Management

Appliance Certificates

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](#)

Certificate Lists

Updates

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 - 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.

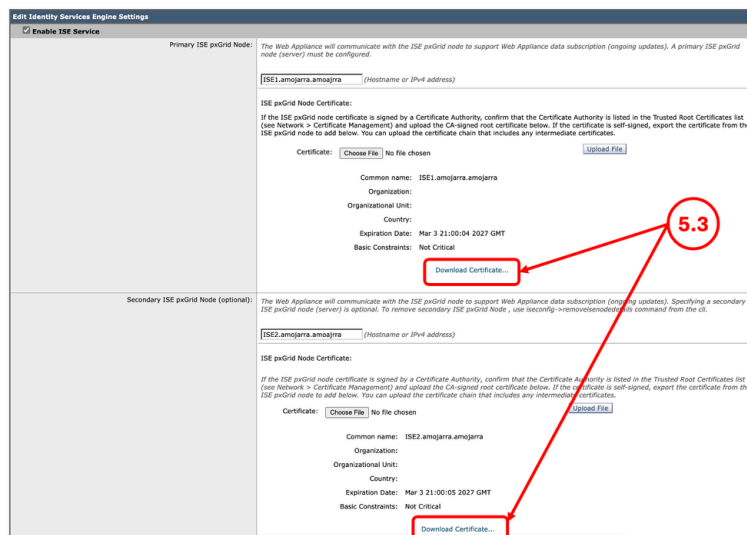


Immagine - Download dei certificati ISE

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.

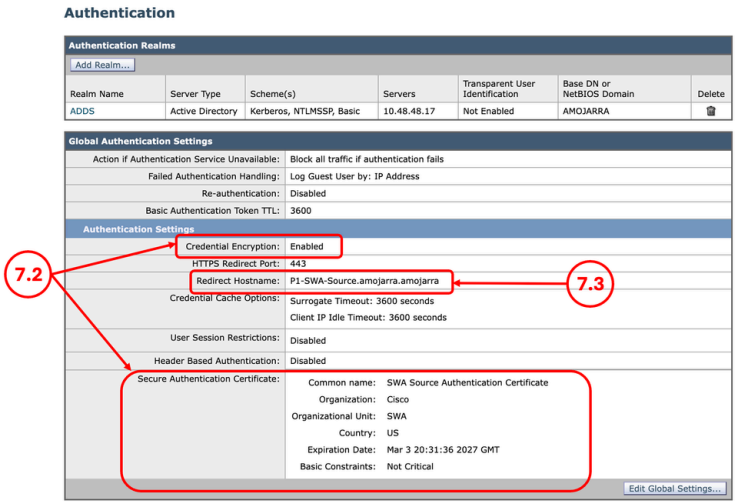
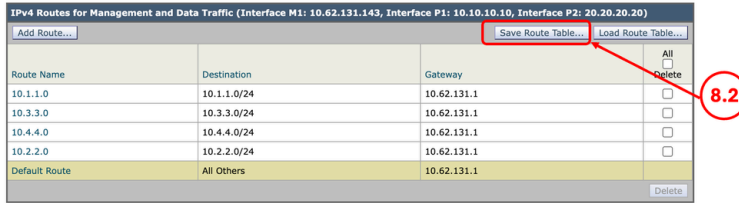
Passaggio 6.2. Acquisire una schermata delle licenze e delle funzionalità.

Passaggio 7. Certificato di reindirizzamento dell'autenticazione

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.

	Authentication  Immagine - Certificato di autenticazione  Nota: Non è possibile scaricare il certificato di autenticazione dalla GUI.
Passaggio 8. Esportazione delle route statiche  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 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. Routes  Immagine - Esportazione tabella di routing
Passaggio 9. Impostazioni 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 9.1. Dalla GUI, passare a Rete e fare clic su DNS. Passaggio 9.2. Acquisire una schermata della configurazione DNS.

Preparazione del file SWA di destinazione

Passaggio 10. Installazione dell'SWA virtuale	Passaggio 10.1. Utilizzare queste guide per installare l'SWA virtuale: • Installazione di Secure Web Appliance su Vmware ESXi • Installare Secure Web Appliance in Microsoft Hyper-V
 Nota: Se l'SWA di destinazione è fisico, è possibile passare al punto 11.	Passaggio 10.2. Verificare che il nuovo SWA disponga dell'accesso alla rete consigliato: • Configurare il firewall per Secure Web Appliance
Passaggio 11. Configurazione iniziale di SWA	Passaggio 11.1. Configurare l'indirizzo IP. Passaggio 11.2. Configurare il gateway predefinito. Passaggio 11.3. Configurare il server DNS. Passaggio 11.4. concedere in licenza l'accessorio. Passaggio 11.5. Abilitare le funzionalità. Passaggio 11.6. Eseguire l'installazione guidata del sistema. La procedura dettagliata è illustrata in questo articolo: Secure Web Appliance Initial Setup
Passaggio 12. Eliminazione dei file di configurazione	Passaggio 12.1. Esaminare la sezione Correzione degli errori in questo articolo per rimuovere la configurazione del certificato ISE dal file di backup XML.
 Nota: Se non si sta integrando ISE con l'SWA, andare al punto 13.	

Importazione del file di configurazione nel file SWA di destinazione

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
--	--



Nota: Se non si utilizza un certificato radice attendibile personalizzato, andare al passaggio 14.

certificati fare clic su Gestisci certificati radice attendibili.

Passaggio 13.3. Fare clic su Import.

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.

Passaggio 14.3. Fare clic su Scegli file e selezionare il file di configurazione XML.

Passaggio 14.4. Se la migrazione corrisponde allo scenario 1 e nel nuovo SWA deve essere utilizzato l'indirizzo IP precedente, selezionare la casella di controllo Carica impostazioni di rete, altrimenti non selezionare questa opzione.

Passaggio 14.5. Fare clic su Carica.

Passaggio 14.6. Fare clic su Continue (Continua) nel popup Confirm Load Configuration (Conferma caricamento configurazione).

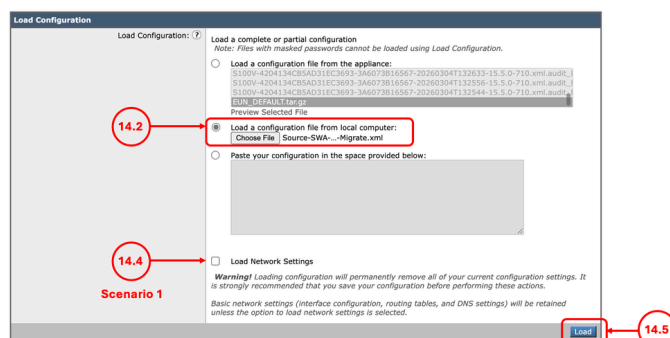
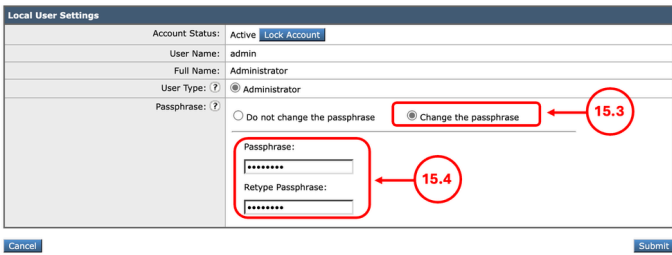


	Immagine - Importazione della configurazione
Passaggio 15. Modifica della password amministratore  Nota: se si dispone della password dell'amministratore SWA di origine, andare al passo 16.	15.1. Dalla GUI, passare a System Administration e scegliere Users. 15.2. fare clic sul nome utente admin. 15.3. Selezionare Change the passphrase (Cambia la passphrase). 15.4. Inserire la password. 15.5. fare clic su Invia.  Immagine - Modifica della password amministratore
Passaggio 16. Esecuzione	Passaggio 16.1. È ora possibile eseguire il commit delle modifiche.
Passaggio 17. Importazione dei cicli di lavorazione  Nota: se si caricano le impostazioni di rete durante l'importazione della configurazione, andare al passo 19.	Passaggio 17.1. Dalla GUI, selezionare Network (Rete) e fare clic su Routing. Passaggio 17.2. Per ciascuna tabella di routing, fare clic su Carica tabella di routing. Passaggio 17.3. Scegliere il file esportato al passaggio 8. Passaggio 17.4. Fare clic su Sottometti. Passaggio 17.5. Confermare le modifiche.
Passaggio 18. Configurazione delle impostazioni DNS  Nota: Se si caricano le impostazioni di rete durante l'importazione della	Passaggio 18.1. Dalla GUI, passare a Rete e fare clic su DNS. Passaggio 18.2. Fare clic su Modifica impostazioni. Passaggio 18.3. Usare lo screenshot dal



configurazione, andare al passo 19.

Passaggio 9

Passaggio 18.4. Fare clic su Sottometti.

Passaggio 18.5. Confermare le modifiche.

Passaggio 19.1. Dalla GUI, selezionare Network (Rete) e fare clic su Authentication (Autenticazione).

Passaggio 19.2. fare clic sul nome del 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 19.2. Fare clic su Aggiungi a dominio e immettere le credenziali:

Edit Realm

Immagine - Aggiunta al dominio Active Directory

Passaggio 19.3. Fare clic su Sottometti.

Passaggio 19.4. Verificare che il nome host di reindirizzamento sia corretto.

Passaggio 19.5. Se la crittografia delle credenziali è abilitata, verificare che il certificato di autenticazione sicura sia corretto.

Passaggio 19. Aggiungere o riaggiungere l'SWA ad Active Directory

Authentication

Authentication Realms						
Add Realm...						
Realm Name	Server Type	Scheme(s)	Servers	Transparent User Identification	Base DN or NetBIOS Domain	Delete
ADOS	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:	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 - Impostazioni di autenticazione

Passaggio 19.6. Confermare le modifiche.



Nota: Se l'SWA esistente (Scenario-2) non è stato sostituito e l'SWA migrato ha un nuovo indirizzo IP, aggiungere l'SWA come nuovo dispositivo all'SMA e saltare il passaggio 20.

Passaggio 20. Partecipare di nuovo a SMA



Nota: Se l'SWA non è gestito da SMA, ignorare questo passaggio.

Passaggio 20.1. Connettersi alla CLI dello SMA.

Passaggio 20.2. eseguire logconfig.

Passaggio 20.3. Immettere HOSTKEYCONFIG.

Passaggio 20.4. Digitare DELETE e premere Invio.

Passaggio 20.5. Digitare il numero associato all'SWA migrato di recente e premere Invio fino al termine della procedura guidata.

Passaggio 20.6. Digitare commit e premere Invio per salvare le modifiche.

Passaggio 20.7. Dalla GUI di SMA, passare a Management Appliance. Selezionare Centralized Services e fare clic su Security Appliance.

Passaggio 20.8. fare clic sul nome dell'SWA migrato di recente.



Suggerimento: È possibile vedere che la colonna Connessione stabilita è impostata su No.

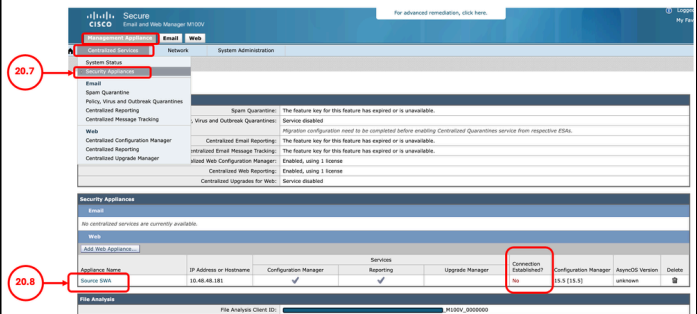


Immagine - Stato di SMA Security Appliance

Passaggio 20.9. fare clic su Stabilisci connessione.

Passaggio 20.10. Immettere il nome utente e la passphrase e fare clic su Stabilisci connessione.

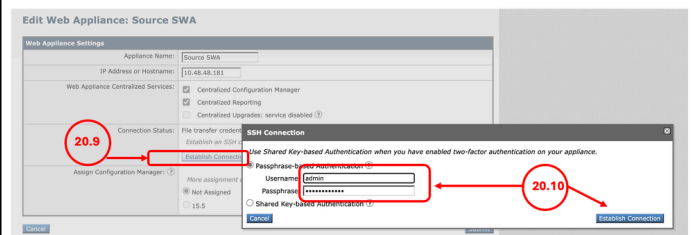


Immagine - Stabilire la connessione con l'SWA

Passaggio 20.11. Assegnare Configuration Manager.

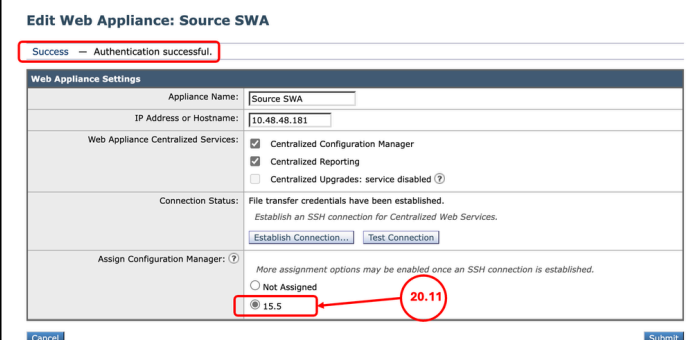


Immagine - Assegna Configuration Manager

Passaggio 20.12. Sottomettere e confermare le modifiche.

Passaggio 20.13. (Facoltativo) è possibile eseguire il test pubblicando la configurazione

	nell'SWA.
	 Suggerimento: L'SMA conserva tutti i dati di reporting e di tracciamento del precedente SWA.

Correzione degli errori

Errore di analisi sull'elemento port_name

Il nome della porta di rete deve essere ['Management', 'P1', 'P2', 'T1', 'T2']:

Configuration File	
Error	— Configuration File was not loaded. Parse Error on element "port_name" line number 85 column 18 with value "M2": The network port name must be one of ['Management', 'P1', 'P2', 'T1', 'T2'] (with optional "_v6" suffix), or start with "VLAN" or "Loopback".

Immagine - Errore di denominazione interfaccia di rete

Error — Configuration File was not loaded. Parse Error on element "port_name" line number 85 colu

Questo errore si verifica quando si esegue la migrazione da SWA fisico a Virtual. l'interfaccia SWA virtuale ha solo 5 NIC e l'interfaccia M2 non è valida. Per correggere l'errore, modificare il file di configurazione XML in un editor di testo e rimuovere le righe seguenti:

M2

M2

M2

autoselect

aa:bb:cc:00:00:00

Errore di analisi nell'elemento ise_service

Configuration File

Error — Configuration File was not loaded. Parse Error on element "ise_service" line number 548 column 17:
b4Y4mw.crt.pem ISE certificate not present in /data/db/isecerts/.

Immagine - Errore certificato ISE

Error - Configuration File was not loaded. Parse Error on element "ise_service" line number 548 column 17:
b4Y4mw.crt.pem ISE certificate not present in /data/db/isecerts/.

Poiché i certificati ISE non sono inclusi nell'esportazione della configurazione SWA e vengono caricati direttamente sul dispositivo, è necessario rimuovere la configurazione dei certificati dal file XML e, dopo l'importazione, configurare ISE manualmente. per risolvere il problema, modificare il file di configurazione XML nell'editor di testo e cercare il nome del certificato nell'errore (in questo esempio, cercare AA11AA) ed eliminarlo dal file di configurazione:

Before:

AA11AA

BB22BB

After:

Oltre al nome del certificato, è necessario rimuovere anche il nome del certificato client di Web Appliance.

In questo esempio, il certificato client di Web Appliance è un certificato autofirmato:

Before:

1

xAcK6T

After:

0

Il failover non funziona sul nuovo SWA virtuale

Se l'opzione Alta disponibilità (failover) non funziona nell'interfaccia SWA virtuale di destinazione, verificare che l'hypervisor sia configurato correttamente. Per ulteriori informazioni, visitare il sito Web all'indirizzo: [Verifica della corretta funzionalità del gruppo WSA HA virtuale in un ambiente VMware](#)

Informazioni correlate

- [Guida per l'utente di AsyncOS 15.2 per Cisco Secure Web Appliance](#)
- [Installazione di Secure Web Appliance su VMware ESXi](#)
- [Installare Secure Web Appliance in Microsoft Hyper-V](#)
- [Installazione iniziale di Secure Web Appliance](#)
- [Guida all'installazione di Cisco Secure Email e Web Virtual Appliance](#)
- [Configurazione di categorie URL personalizzate in Secure Web Appliance - Cisco](#)
- [Utilizzare le procedure ottimali per Secure Web Appliance](#)
- [Configurare il firewall per Secure Web Appliance](#)
- [Configura certificato di decrittografia in Appliance Web sicura](#)
- [Risoluzione dei problemi relativi al servizio DNS Secure Web Appliance](#)
- [Garantire la corretta funzionalità del gruppo WSA HA virtuale in un ambiente VMware](#)

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).