

Migrar configuración entre dos SWA

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antes de comenzar](#)

[Preparación y Copia de Seguridad del SWA de Origen](#)

[Paso 1. Exportar el archivo de configuración](#)

[Paso 2. Exportar el certificado de descifrado](#)

[Paso 3. Exportar los certificados raíz de confianza personalizados](#)

[Paso 4. Exportar el certificado de la GUI](#)

[Paso 5. Exportar los certificados de ISE](#)

[Paso 6. Licencias/Funciones](#)

[Paso 7. Certificado de redirección de autenticación](#)

[Paso 8. Exportación de Rutas Estáticas](#)

[Paso 9. Configuración de DNS](#)

[Preparación del SWA de destino](#)

[Paso 10. Instalación del SWA virtual](#)

[Paso 11. Configuración inicial de SWA](#)

[Paso 12. Saneamiento del archivo de configuración](#)

[Importación del archivo de configuración al SWA de destino](#)

[Paso 13. Importar certificados raíz de confianza personalizados](#)

[Paso 14. Importar el archivo de configuración](#)

[Paso 15. Cambio de la contraseña de administrador](#)

[Paso 16. Compromiso](#)

[Paso 17. Importación de las Rutas](#)

[Paso 18. Configuración de los parámetros de DNS](#)

[Paso 19. Unirse/volver a unir el SWA a Active Directory](#)

[Paso 20. Vuelva a unirse al SMA](#)

[Corrección de errores](#)

[Error de análisis en el elemento port_name](#)

[Error de análisis en el elemento ise_service](#)

[La conmutación por fallo no funciona en el nuevo SWA virtual](#)

[Información Relacionada](#)

Introducción

En este documento se describe el proceso de restauración de la configuración de un dispositivo web seguro (SWA) a otro.

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- Acceso a la interfaz gráfica de usuario (GUI) de SWA
- Acceso administrativo al SWA
- Acceso administrativo al dispositivo de administración de seguridad (SMA)
- Acceso al portal de licencias de software de Cisco o al archivo de licencia SWA
- Acceso de usuario con privilegios de Active Directory para unirse al SWA en el dominio y crear registros DNS

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antes de comenzar

En este artículo, se describen los pasos para migrar del SWA de origen al SWA de destino. Esta tabla enumera las especificaciones para cada sistema.

	SWA de origen	SWA objetivo
Modelo	S396	S100v
Versión	15.5.0-710	15.5.0-710
Licencia	Licencia inteligente	Licencia inteligente
Directorio activo	Unido	Unido
Integrado con Identity Services Engine (ISE)	Yes	Yes

Número de tarjetas de interfaz de red (NIC)	5	5
Descifrado HTTPS	Habilitado con certificado autofirmado	Habilitado con certificado autofirmado
Redirección transparente	WCCP	WCCP
Administrado por SMA	Yes	Yes
Servidor de registro externo	Pulsación SCP	Pulsación SCP
Alta disponibilidad	Habilitado	Habilitado

 Nota: Asegúrese siempre de que, al instalar un nuevo SWA virtual, todas las interfaces de red recomendadas por Cisco estén presentes y configuradas en la máquina virtual (VM). Las interfaces pueden permanecer desconectadas, pero deben estar disponibles dentro de la VM.

Existen dos situaciones posibles al migrar el SWA de un dispositivo a otro:

[Escenario-1] Sustituyendo el SWA existente: El SWA original se retira y la dirección IP del SWA de destino es la misma que el SWA de origen.

[Escenario 2] Agregando un nuevo SWA: El SWA original permanece en servicio mientras se configura el nuevo SWA.

Preparación y Copia de Seguridad del SWA de Origen

Siga estos pasos para recopilar los archivos y la configuración necesarios del SWA de origen:

Paso 1. Exportar el archivo de configuración	Paso 1.1. Desde la GUI, vaya a Administración del sistema y elija Archivo de configuración. Paso 1.2. Asegúrese de que la opción Descargar archivo al equipo local para verlo o guardarlo está seleccionada. Paso 1.3. Elija Cifrar contraseñas en los archivos de configuración Paso 1.4. (Opcional) Elija un nombre para el archivo de configuración.
--	---

	Paso 1.5. Haga clic en Enviar. 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: Source-SWA-Before-Migrate 1.4 Note: ".xml" will be appended to the specified file-name automatically. Submit Imagen: Exportación del archivo de configuración
Paso 2. Exportar el certificado de descifrado  Nota: Si el descifrado HTTPS está desactivado, vaya al paso 3.	Paso 2.1. Desde la GUI, navegue hasta Servicios de seguridad y haga clic en Proxy HTTPS. Paso 2.2. Haga clic en Editar configuración. Paso 2.3. Descargue el certificado de descifrado HTTPS haciendo clic en Descargar certificado... enlace. HTTPS Proxy Settings ☒ Enable HTTPS Proxy HTTPS Ports to Proxy: 443 Root Certificate for Signing: Use Uploaded Certificates and Key Upload File Certificate: Choose File No file chosen Key: Choose File No file chosen ☐ Key is Encrypted Common name: Organization: Organizational Unit: Country: Expiration Date: Basic Constraints: Download Certificate... 2.3 ☒ Use Generated Certificate and Key Generate New 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 Download Certificate... Download Certificate Signing Request... Signed Certificate: To use a signed certificate, first download a certificate signing request using the link above. Submit the request to a certificate authority, and when you receive the signed certificate, upload it using the field below. Certificate: Choose File No file chosen Upload File Imagen - Certificado de descifrado HTTPS  Nota: En este ejemplo, se ilustran ambos tipos de certificados de descifrado HTTPS; sin embargo, en la red, sólo puede tener implementado un tipo.
Paso 3. Exportar los certificados raíz de confianza personalizados  Nota: Si no se ha agregado ningún	Paso 3.1. Desde la GUI, navegue hasta Red y haga clic en Administración de certificados. Paso 3.2. En la sección Administración de certificados, haga clic en Administrar certificados raíz



certificado raíz de confianza personalizado en el SWA, vaya al paso 4.

de confianza.

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	

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...](#)

Imagen - Administrar certificados raíz de confianza

Paso 3.3. Expanda cada certificado raíz de confianza personalizado haciendo clic en su nombre y haga clic

Expiration Date	On Class List	Delete
Jan 22 12:12:14 2036 GMT	No	

en Descargar certificado...

Imagen - Descargar certificados raíz de confianza

Paso 4.1. Desde la GUI, navegue hasta Red y haga clic en Administración de certificados.

Paso 4.2. En la sección Certificados de dispositivo, haga clic en Exportar certificado.

Paso 4. Exportar el certificado de la GUI



Nota: Si utiliza un certificado de GUI integrado, vaya al paso 5.

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	

[Export Certificate...](#)

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

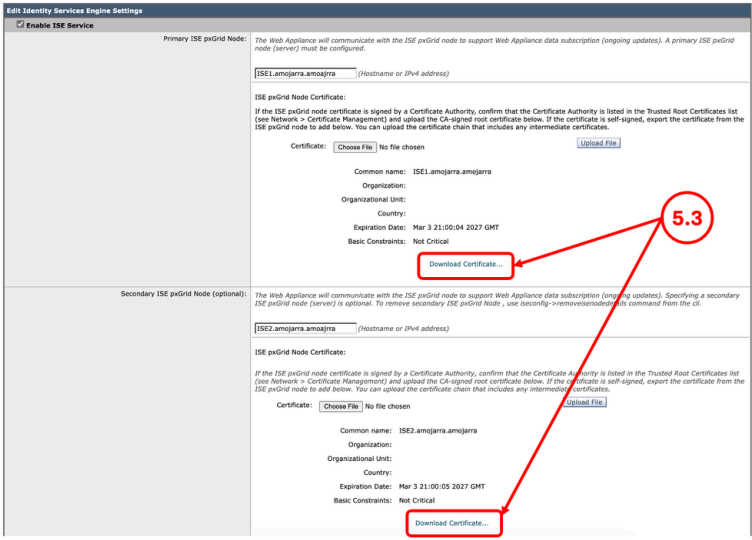
No updates in progress. [Update Now](#)

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...](#)

	Imagen - Exportar certificado de GUI
Paso 5. Exportar los certificados de ISE  Nota: Si no hay SWA, integración con ISE, vaya directamente al paso 6.	Paso 5.1. Desde la GUI, navegue hasta Red y haga clic en Identity Services Engine. Paso 5.2. Haga clic en Editar configuración. Paso 5.3. Descargue todos los certificados disponibles.  Imagen - Descargar certificados ISE
Paso 6. Licencias/Funciones	Paso 6.1. Desde la GUI, navegue hasta Administración del sistema y haga clic en Licencias o en Características depende del tipo de licencia que esté utilizando. Paso 6.2. Realice una captura de pantalla de sus licencias/funciones.
Paso 7. Certificado de redirección de autenticación	Paso 7.1. Desde la GUI, navegue hasta Red y haga clic en Autenticación. Paso 7.2. Si el cifrado de credenciales está habilitado, asegúrese de que tiene el certificado y la clave. Paso 7.3. Realice una captura de pantalla de la configuración actual.

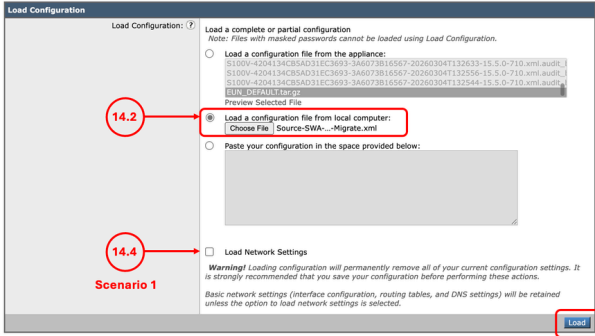
	Authentication Authentication Realms <table><tr><td colspan="7">Add Realm...</td></tr><tr><td>Realm Name</td><td>Server Type</td><td>Scheme(s)</td><td>Servers</td><td>Transparent User Identification</td><td>Base DN or NetBIOS Domain</td><td>Delete</td></tr><tr><td>ADDS</td><td>Active Directory</td><td>Kerberos, NTLMSSP, Basic</td><td>10.48.48.17</td><td>Not Enabled</td><td>AMOJARRA</td><td></td></tr></table> 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 Edit Global Settings... Imagen - Certificado de autenticación Nota: No puede descargar el certificado de autenticación desde la GUI.	Add Realm...							Realm 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				
Add Realm...																									
Realm 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																				
Paso 8. Exportación de Rutas Estáticas Nota: Si tiene previsto utilizar la misma configuración de red y dirección IP para el SWA de destino, vaya directamente al paso 10.	Paso 8.1. Desde la GUI, navegue hasta Red y haga clic en Rutas. Paso 8.2. Para cada tabla de ruteo, haga clic en Guardar tabla de ruteo. Routes IPv4 Routes for Management and Data Traffic (Interface M1: 10.62.131.143, Interface P1: 10.10.10.10, Interface P2: 20.20.20.20) Add Route... Save Route Table... Load Route Table... All ☐ Delete <table><tr><td>Route Name</td><td>Destination</td><td>Gateway</td><td></td></tr><tr><td>10.1.1.0</td><td>10.1.1.0/24</td><td>10.62.131.1</td><td>☐</td></tr><tr><td>10.3.3.0</td><td>10.3.3.0/24</td><td>10.62.131.1</td><td>☐</td></tr><tr><td>10.4.4.0</td><td>10.4.4.0/24</td><td>10.62.131.1</td><td>☐</td></tr><tr><td>10.2.2.0</td><td>10.2.2.0/24</td><td>10.62.131.1</td><td>☐</td></tr><tr><td>Default Route</td><td>All Others</td><td>10.62.131.1</td><td></td></tr></table> Delete Imagen - Exportando tabla de routing	Route Name	Destination	Gateway		10.1.1.0	10.1.1.0/24	10.62.131.1	☐	10.3.3.0	10.3.3.0/24	10.62.131.1	☐	10.4.4.0	10.4.4.0/24	10.62.131.1	☐	10.2.2.0	10.2.2.0/24	10.62.131.1	☐	Default Route	All Others	10.62.131.1	
Route Name	Destination	Gateway																							
10.1.1.0	10.1.1.0/24	10.62.131.1	☐																						
10.3.3.0	10.3.3.0/24	10.62.131.1	☐																						
10.4.4.0	10.4.4.0/24	10.62.131.1	☐																						
10.2.2.0	10.2.2.0/24	10.62.131.1	☐																						
Default Route	All Others	10.62.131.1																							
Paso 9. Configuración de DNS Nota: Si tiene previsto utilizar la misma configuración de red y dirección IP para el SWA de destino, vaya directamente al paso 10.	Paso 9.1. Desde la GUI, navegue hasta Red y haga clic en DNS. Paso 9.2. Realice una captura de pantalla de la configuración DNS.																								

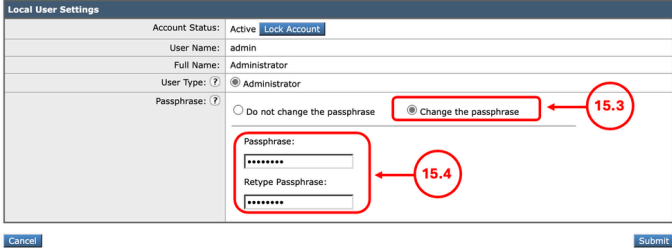
Preparación del SWA de destino

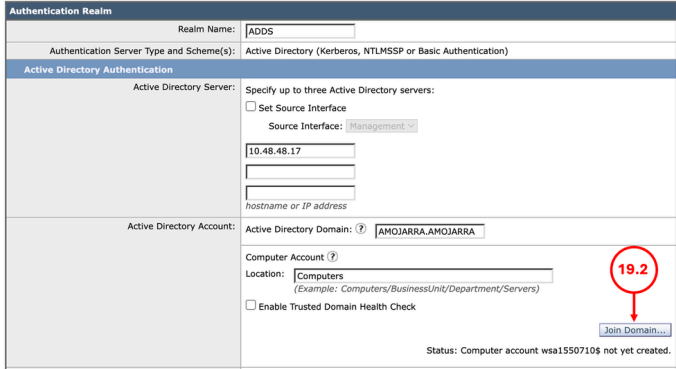
Paso 10. Instalación del SWA virtual	Paso 10.1. Utilice estas guías para instalar el SWA virtual: • Instalación de Secure Web Appliance en Vmware ESXi • Instalación de Secure Web Appliance en Microsoft Hyper-V Paso 10.2. Asegúrese de que el nuevo SWA tenga el acceso a la red recomendado: • Configuración del firewall para el dispositivo web seguro
 Nota: Si el SWA de destino es físico, puede saltar al paso 11.	
Paso 11. Configuración inicial de SWA	Paso 11.1. Configure la dirección IP. Paso 11.2. Configure la puerta de enlace predeterminada. Paso 11.3. Configuración del servidor DNS. Paso 11.4. otorgar licencia al dispositivo. Paso 11.5. Habilite las funciones. Paso 11.6. Ejecute el asistente de configuración del sistema. Puede encontrar los pasos detallados en este artículo: Secure Web Appliance Initial Setup
Paso 12. Saneamiento del archivo de configuración	Paso 12.1. Revise la sección Corrección de errores de este artículo para eliminar la configuración del certificado ISE del archivo de copia de seguridad XML.
 Nota: Si no va a integrar ISE con el SWA, puede saltar al paso 13.	

Importación del archivo de configuración al SWA de destino

Paso 13. Importar certificados raíz de confianza personalizados	Paso 13.1. Desde la GUI, navegue hasta Red y haga clic en Administración de certificados. Paso 13.2. En la sección Administración de certificados, haga clic en Administrar
 Nota: Si no está utilizando ningún	

 certificado raíz de confianza personalizado, vaya al paso 14.	certificados raíz de confianza. Paso 13.3. Haga clic en Importar. Paso 13.4. Cargue los certificados que se descargaron anteriormente en el Paso 3.  Precaución: Cuando los certificados raíz e intermedios estén disponibles, comience por cargar el certificado de CA raíz. Después de enviar y confirmar los cambios, proceda a importar el certificado intermedio.
Paso 14. Importar el archivo de configuración	Paso 14.1. Desde la GUI, vaya a Administración del sistema y elija Archivo de configuración. Paso 14.2. En la sección Cargar configuración, seleccione Cargar un archivo de configuración desde el equipo local. Paso 14.3. Haga clic en Choose File y seleccione el archivo de configuración XML. Paso 14.4. Si la migración coincide con el Escenario 1 y la dirección IP anterior se debe utilizar en el nuevo SWA, seleccione la casilla de verificación Cargar configuración de red; de lo contrario, no seleccione esta opción. Paso 14.5. Haga clic en Cargar. Paso 14.6. Haga clic en Continuar en la ventana emergente Confirmar configuración de carga.  Imagen: Importación de la configuración

Paso 15. Cambio de la contraseña de administrador	15.1. En la GUI, vaya a Administración del sistema y seleccione Usuarios. 15.2. haga clic en el nombre de usuario admin. 15.3. Seleccione Cambiar la frase de contraseña. 15.4. Introduzca la contraseña. 15.5. haga clic en Enviar.
 Nota: Si dispone de la contraseña de administrador de SWA de origen, vaya directamente al paso 16.	Edit Local User  Imagen: cambio de contraseña de administrador
Paso 16. Compromiso	Paso 16.1. Ahora puede registrar los cambios.
Paso 17. Importación de las Rutas  Nota: Si carga los parámetros de red al importar la configuración, vaya directamente al paso 19.	Paso 17.1. Desde la GUI, navegue hasta Red y haga clic en Rutas. Paso 17.2. Para cada tabla de ruteo, haga clic en Cargar tabla de ruteo. Paso 17.3. Elija el archivo que exportó en el Paso 8. Paso 17.4. Haga clic en Enviar. Paso 17.5. Realice los cambios.
Paso 18. Configuración de los parámetros de DNS  Nota: Si carga parámetros de red mientras importa la configuración, vaya al paso 19.	Paso 18.1. Desde la GUI, navegue hasta Red y haga clic en DNS. Paso 18.2. Haga clic en Editar configuración. Paso 18.3. Utilice la captura de pantalla del Paso 9 Paso 18.4. Haga clic en Enviar.

	Paso 18.5. Realice los cambios.
Paso 19. Unirse/volver a unir el SWA a Active Directory	Paso 19.1. Desde la GUI, Navegue hasta Red y haga clic en Autenticación. Paso 19.2. haga clic en el nombre del Nombre de rango de autenticación.
	 Consejo: Si se asigna una nueva dirección IP y un nombre de host al SWA, asegúrese de que se crean los registros DNS necesarios en el servicio DNS de Active Directory.
	Paso 19.2. Haga clic en Unirse al dominio e ingrese las credenciales: Edit Realm 
	Imagen - Unirse al dominio de Active Directory Paso 19.3. Haga clic en Enviar. Paso 19.4. Asegúrese de que el nombre de host de redirección sea correcto. Paso 19.5. Si el cifrado de credenciales está habilitado, asegúrese de que el certificado de autenticación segura sea correcto.

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

[Edit Global Settings...](#)

Imagen - Configuración de autenticación

Paso 19.6. Realice los cambios.



Nota: Si no reemplazó el SWA existente (situación 2) y el SWA migrado tiene una nueva dirección IP, agregue el SWA como nuevo dispositivo al SMA y omita el paso 20.

Paso 20.1. Conexión a CLI del SMA.

Paso 20.2. ejecute logconfig.

Paso 20.3. Ingrese HOSTKEYCONFIG.

Paso 20.4. Escriba DELETE y presione Enter.

Paso 20.5. Escriba el número asociado al SWA que se ha migrado recientemente y pulse Intro hasta que finalice el asistente.

Paso 20.6. Escriba commit y presione Intro para guardar los cambios.

Paso 20.7. Desde la GUI de SMA, navegue hasta Dispositivo de administración. Seleccione Servicios centralizados y haga clic en Dispositivos de seguridad.

Paso 20.8. haga clic en el nombre del SWA migrado recientemente.



Consejo: Puede ver que la columna

Paso 20. Vuelva a unirse al SMA



Nota: Si SMA no administra el SWA, omita este paso.



Conexión establecida está establecida en No.

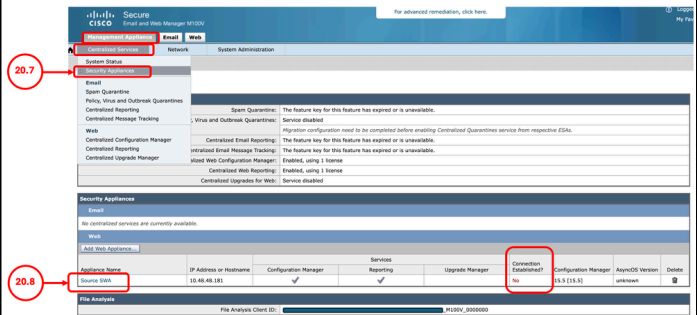


Imagen - Estado del dispositivo de seguridad SMA

Paso 20.9. haga clic en Establecer conexión.

Paso 20.10. Introduzca el nombre de usuario y la frase de paso y haga clic en Establecer conexión.

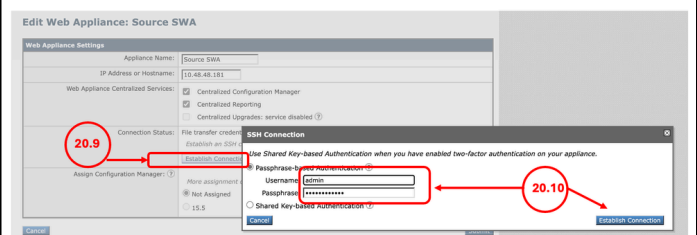


Imagen: establezca una conexión con el SWA

Paso 20.11. Asigne el Administrador de configuración.

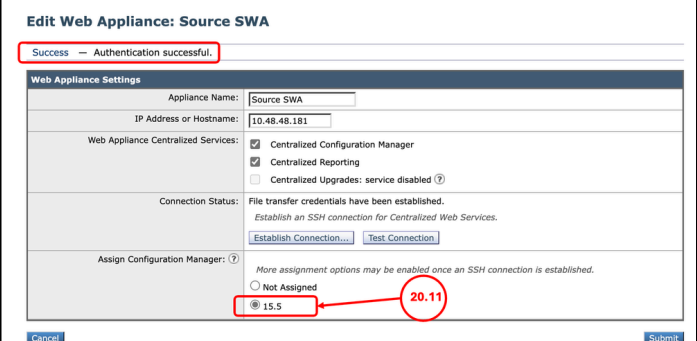


Imagen - Asignar Administrador de configuración

Paso 20.12. Enviar y Registrar los cambios.

Paso 20.13. (Opcional) Puede probar publicando la configuración en el SWA.



Consejo: El SMA conserva todos los datos de notificación y seguimiento del SWA anterior.

Corrección de errores

Error de análisis en el elemento port_name

El nombre del puerto de red debe ser uno entre ['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".

Imagen - Error de denominación de interfaz de red

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".

Este error se produce cuando se migra de un entorno de seguridad físico a un entorno virtual. el SWA virtual solo tiene 5 NIC y la interfaz M2 no es válida. Para corregir el error, edite el archivo de configuración XML en un editor de texto y elimine estas líneas:

M2

M2

M2

autoselect

aa:bb:cc:00:00:00

Error de análisis en el 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/.

Imagen - Error de certificado de ISE

Error - Configuration File was not loaded. Parse Error on element "ise_service" line number 548 column 17:

Dado que los certificados de ISE no se incluyen en la exportación de configuración de SWA y se cargan directamente en el dispositivo, debe eliminar la configuración de certificados del archivo

XML y, después de realizar la importación correctamente, configurar ISE manualmente. para solucionar este problema, edite el archivo de configuración XML en el editor de texto y busque el nombre del certificado en el error (en este ejemplo, busque AA11AA) y elimínelo del archivo de configuración:

Before:

AA11AA

BB22BB

After:

Aparte del nombre del certificado, también debe quitar el nombre del certificado de cliente de dispositivo web.

En este ejemplo, el certificado de cliente de dispositivo web es un certificado autofirmado:

Before:

1

xAck6T

After:

0

La conmutación por fallo no funciona en el nuevo SWA virtual

Si High Availability (Failover) no funciona en el SWA virtual de destino, asegúrese de que el hipervisor esté configurado correctamente. Para obtener más información, visite: [Garantizar la correcta funcionalidad del grupo HA de WSA virtual en un entorno VMware](#)

Información Relacionada

- [Guía del usuario de AsyncOS 15.2 para Cisco Secure Web Appliance](#)
- [Instalación de Secure Web Appliance en VMware ESXi](#)
- [Instalación de Secure Web Appliance en Microsoft Hyper-V](#)
- [Configuración inicial del dispositivo web seguro](#)
- [Guía de instalación de Cisco Secure Email and Web Virtual Appliance](#)
- [Configurar categorías de URL personalizadas en el dispositivo web seguro - Cisco](#)
- [Uso de las prácticas recomendadas de Secure Web Appliance](#)
- [Configuración del firewall para el dispositivo web seguro](#)
- [Configurar certificado de descifrado en dispositivo web seguro](#)
- [Solucionar problemas del servicio DNS de dispositivo web seguro](#)
- [Garantizar la correcta funcionalidad del grupo HA de WSA virtual en un entorno VMware](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).