Migrate Configuration Between Two SWAs

Contents

Introduction

Prerequisites

Requirements

Components Used

Before you Begin

Preparing and Backing Up the Source SWA

Step 1. Export the Configuration File

Step 2. Export the Decryption Certificate

Step 3. Export the Custom Trust Root Certificates

Step 4. Export the GUI Certificate

Step 5. Export the ISE Certificates

Step 6. Licences / Features

Step 7. Authentication Redirection Certificate

Step 8. Exporting Static Routes

Step 9. DNS Settings

Preparing the Target SWA

Step 10. Installing the Virtual SWA

Step 11. Initial SWA Setup

Step 12. Sanitizing the Configuration file

Importing the Configuration File to Target SWA

Step 13. Import Custom Trusted Root Certificates

Step 14. Import the Configuration File

Step 15. Changing the admin Password

Step 16. Commit

Step 17. Importing the Routes

Step 18. Configuring the DNS Settings

Step 19. Join/Rejoin the SWA to the Active Directory

Step 20. Re-join to SMA

Fixing Errors

Parse Error on Element port_name

Parse Error on Element ise_service

Failover is not Working on New Virtual SWA

Related Information

Introduction

This document describes the process of restoring the configuration from a Secure Web Appliance (SWA) to another.

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Access ToGraphic User Interface (GUI)of SWA

- Administrative Access to the SWA
- Administrative Access to the Security Management Appliance (SMA)
- Access to Cisco Software Licensing Portal or the SWA license file
- Active Directory privileged user access to join the SWA to domain and create DNS records

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Before you Begin

In this article, we outline the steps to migrate from the source SWA to the target SWA. This table lists the specifications for each system.

	Source SWA	**Target SWA**
Model	S396	S100v
Version	15.5.0-710	15.5.0-710
License	Smart License	Smart License
Active Directory	Joined	Joined
Integrated with Identity Services Engine (ISE)	Yes	Yes
Number of Network Interface Card (NIC)	5	5
HTTPS Decryption	Enabled with Self Signed Certificate	Enabled with Self Signed Certificate

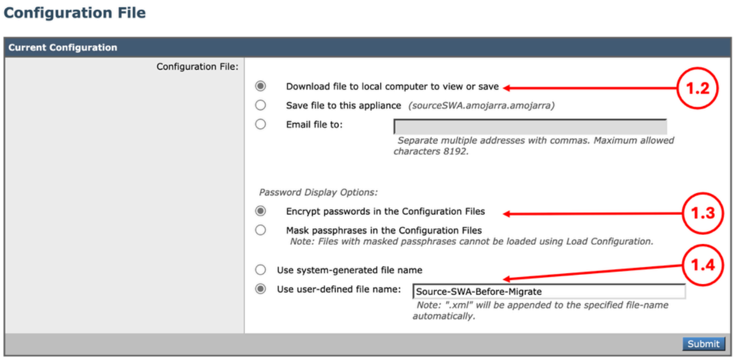
Transparent Redirection	WCCP	WCCP
Managed by SMA	Yes	Yes
External Log Server	SCP Push	SCP Push
High Availability	Enabled	Enabled

Note: Always ensure that, when installing a new virtual SWA, all network interfaces recommended by Cisco are present and configured on the Virtual Machine(VM). The interfaces can remain disconnected, but they must be available within the VM.

There are two possible scenarios when migrating the SWA from one device to another:
[Scenario-1] Replacing the existing SWA: The original SWA is decommissioned and the IP address of the Target SWA is same as the source SWA.
[Scenario-2] Adding a new SWA: The original SWA remains in service while the new SWA is configured.

Preparing and Backing Up the Source SWA

Use these steps to collect the necessary files and configuration from the Source SWA:

Step 1. Export the Configuration File	**Step 1.1.** From the GUI, Navigate to **System Administration** and choose **Configuration File**. **Step 1.2.** Make sure **Download file to local computer to view or save** is selected. **Step 1.3.** Choose **Encrypt passwords in the Configuration Files** **Step 1.4.** (Optional) Choose a name for the configuration file. **Step 1.5.** Click **Submit**.  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: Source-SWA-Before-Migrate *Note: ".xml" will be appended to the specified file-name automatically.* *Image - Exporting the configuration File*

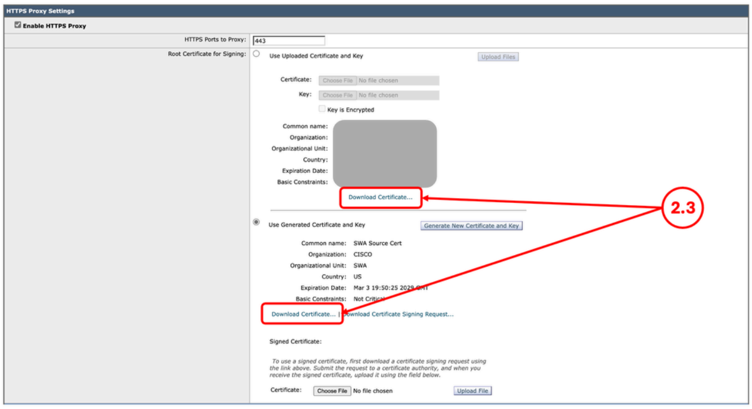
Step 2. Export the Decryption Certificate

Note: If the HTTPS Decryption is disabled, skip to **Step 3**.

Step 2.1. From the GUI, Navigate to **Security Services** and click **HTTPS Proxy**.

Step 2.2. Click **Edit Settings**.

Step 2.3. Download the HTTPS Decryption Certificate, by clicking **Download Certificate...** link.



HTTPS Proxy Settings

☑ Enable HTTPS Proxy

HTTPS Ports to Proxy: 443

Root Certificate for Signing:

○ Use Uploaded Certificate and Key [Upload Files]

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:

[redacted]

Download Certificate...

● 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 19:50:25 2029 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]

Image - HTTPS Decryption Certificate

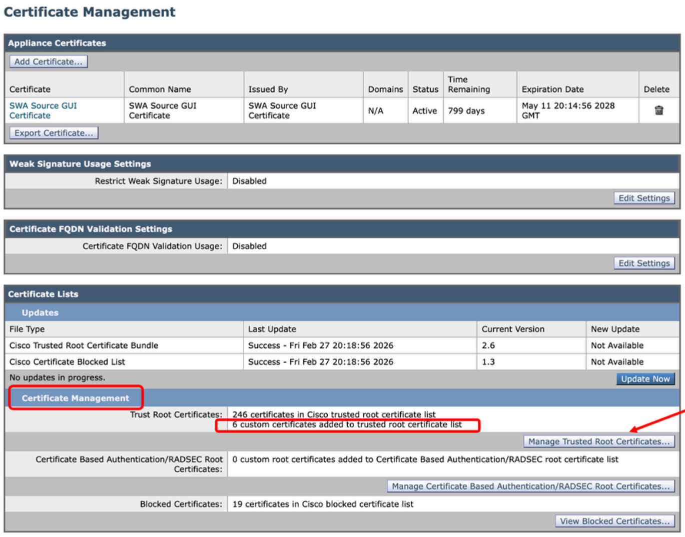
Note: In this example, both types of HTTPS Decryption certificates are illustrated; however, in your network, you can have only one type deployed.

Step 3. Export the Custom Trust Root Certificates

Note: If there no custom trusted root certificate added on the SWA skip to **Step 4**.

Step 3.1. From the GUI, navigate to **Network** and click **Certificate Management**.

Step 3.2. In the **Certificate Management** section, click **Manage Trusted Root Certificates**.



Certificate Management

Appliance Certificates

[Add Certificate...]

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...]

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...]

Image - Manage Trusted Root Certificates

Step 3.3. Expand each **Custom Trusted Root Certificates** by clicking their name and click **Download Certificate...**

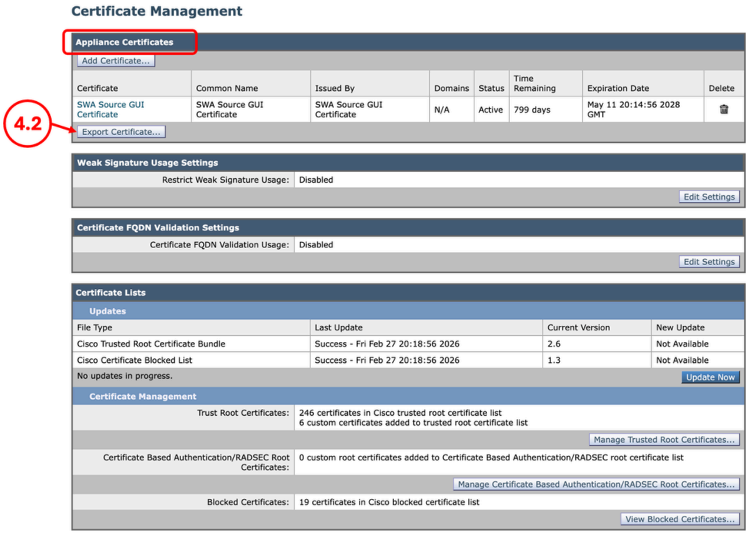
Image - Downlaod Trusted root Certificates

Step 4. Export the GUI Certificate

Note: If you are using built-in GUI certificate, skip to **Step 5**.

Step 4.1. From the GUI, Navigate to **Network** and click **Certificate Management**.

Step 4.2. In the **Appliance Certificates** section, click **Export Certificate**.



Certificate Management

Appliance Certificates

Add Certificate...

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...

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...

Image - Export GUI Certificate

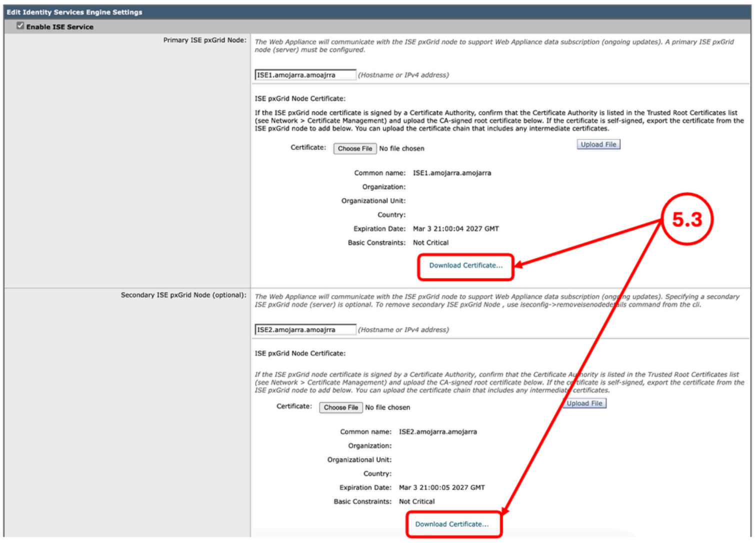
Step 5. Export the ISE Certificates

Note: If there are no SWA, ISE integration, skip to **Step 6**.

Step 5.1. From the GUI, Navigate to **Network** and click **Identity Services Engine**.

Step 5.2. Click **Edit Settings**.

Step 5.3. Download all available certificates.



Edit Identity Services Engine Settings

☑ Enable ISE Service

Primary ISE pxGrid Node: *The Web Appliance will communicate with the ISE pxGrid node to support Web Appliance data subscription (ongoing updates). A primary ISE pxGrid node (server) must be configured.*

ISE1.amojarra.amoajrra *(Hostname or IPv4 address)*

ISE pxGrid Node Certificate:

If the ISE pxGrid node certificate is signed by a Certificate Authority, confirm that the Certificate Authority is listed in the Trusted Root Certificates list (see Network > Certificate Management) and upload the CA-signed root certificate below. If the certificate is self-signed, export the certificate from the ISE pxGrid node to add below. You can upload the certificate chain that includes any intermediate certificates.

Certificate: Choose File No file chosen Upload File

Common name: ISE1.amojarra.amojarra
Organization:
Organizational Unit:
Country:
Expiration Date: Mar 3 21:00:04 2027 GMT
Basic Constraints: Not Critical

Download Certificate...

Secondary ISE pxGrid Node (optional): *The Web Appliance will communicate with the ISE pxGrid node to support Web Appliance data subscription (ongoing updates). Specifying a secondary ISE pxGrid node (server) is optional. To remove secondary ISE pxGrid Node , use iseconfig->removeisenodedetails command from the cli.*

ISE2.amojarra.amoajrra *(Hostname or IPv4 address)*

ISE pxGrid Node Certificate:

If the ISE pxGrid node certificate is signed by a Certificate Authority, confirm that the Certificate Authority is listed in the Trusted Root Certificates list (see Network > Certificate Management) and upload the CA-signed root certificate below. If the certificate is self-signed, export the certificate from the ISE pxGrid node to add below. You can upload the certificate chain that includes any intermediate certificates.

Certificate: Choose File No file chosen Upload File

Common name: ISE2.amojarra.amojarra
Organization:
Organizational Unit:
Country:
Expiration Date: Mar 3 21:00:05 2027 GMT
Basic Constraints: Not Critical

Download Certificate...

Image - Download ISE Certificates

Step 6. Licences / Features

Step 6.1. From the GUI, Navigate to **System Administration** and click **Licenses** or **Features** depends on the type of the license you are using.

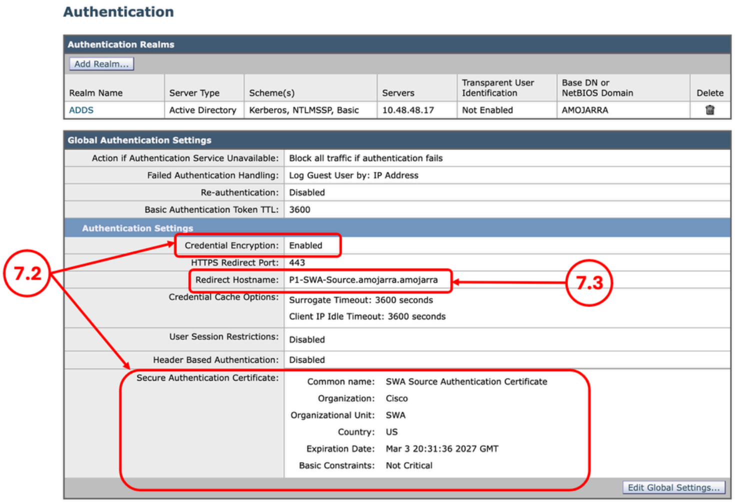
Step 6.2. Take a screenshot of your Licenses / Features.

Step 7. Authentication Redirection Certificate

Step 7.1. From the GUI, Navigate to **Network** and click **Authentication**.

Step 7.2. If the **Credential Encryption** is enabled, Make sure you have the Certificate and the Key.

Step 7.3. Take a screenshot of the current configuration.



Authentication

Authentication Realms

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	🗑

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

Image - Authentication Certificate

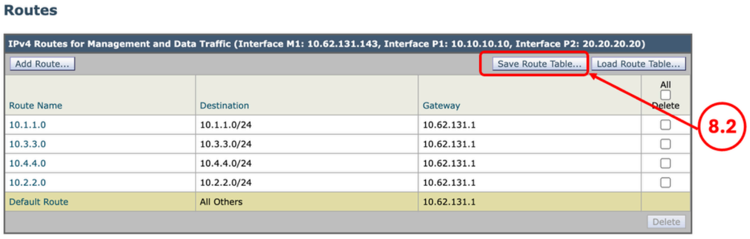
Note: You cannot download the Authentication certificate from the GUI.

Step 8. Exporting Static Routes

Note: If you are planning to use the same Network configuration and IP address for the target SWA, skip to **Step 10**.

Step 8.1. From the GUI, Navigate to **Network** and click **Routes**.

Step 8.2. For each routing table, click **Save Route Table**.



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)

Route Name	Destination	Gateway	All □ Delete
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	

Image - Exporting Routing Table

Step 9. DNS Settings

Step 9.1. From the GUI, Navigate to **Network** and click **DNS**.

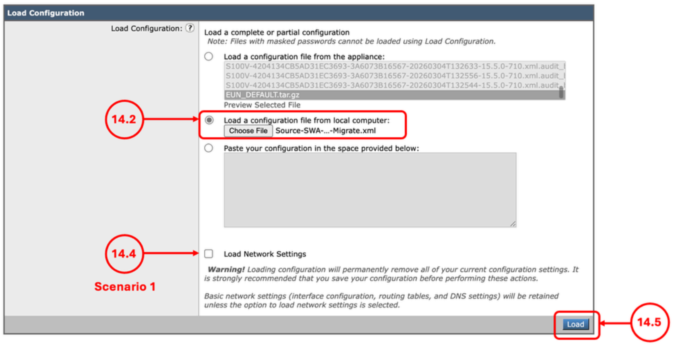
Note: If you are planning to use the same Network configuration and IP address for the target SWA, skip to **Step 10**.	**Step 9.2.** Take a screenshot of the DNS configuration.

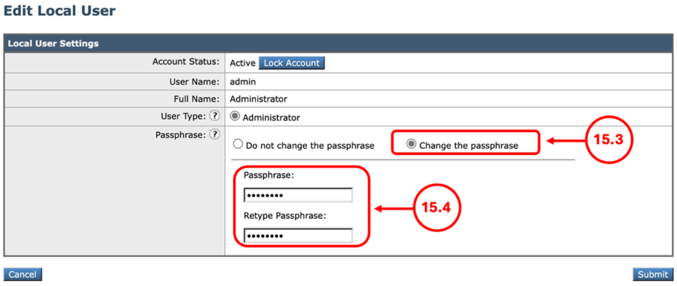
Preparing the Target SWA

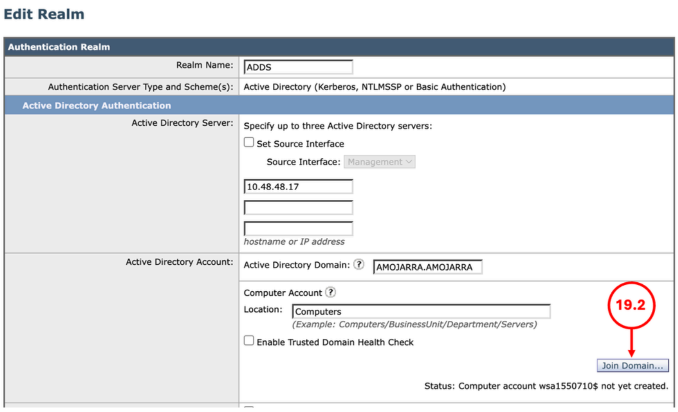
Step 10. Installing the Virtual SWA **Note**: If the target SWA is physical you can skip to **Step 11**.	**Step 10.1.** Use these guides to install the virtual SWA: • Install Secure Web Appliance on Vmware ESXi • Install Secure Web Appliance on Microsoft Hyper-V **Step 10.2.** Make sure the new SWA has the recommended network access: • Configure Firewall for Secure Web Appliance
Step 11. Initial SWA Setup	**Step 11.1.** Configure the IP address. **Step 11.2.** Configure the default Gateway. **Step 11.3.** Configure the DNS server. **Step 11.4.** license the Appliance. **Step 11.5.** Enable the Features. **Step 11.6.** Run the system setup wizard. You can find the detailed steps in this article: Secure Web Appliance Initial Setup
Step 12. Sanitizing the Configuration file **Note**: If you are not integrating ISE with the SWA, you can skip to **Step 13**.	**Step 12.1.** Review the **Fixing Errors** section in this article to remove the ISE certificate configuration from the XML backup file.

Importing the Configuration File to Target SWA

Step 13. Import Custom Trusted Root Certificates **Note**: If you are not using any Custom Trusted Root Certificate, skip to **Step 14**.	**Step 13.1.** From the GUI, Navigate to **Network** and click **Certificate Management**. **Step 13.2.** In the **Certificate Management** section, click **Manage Trusted Root Certificates**. **Step 13.3.** Click **Import**.

	Step 13.4. Upload the certificates that previously was downloaded in **Step 3**. ⚠ **Caution**: When both root and intermediate certificates are available, begin by uploading the root CA certificate. After submitting and committing the changes, proceed to import the intermediate certificate.
Step 14. Import the Configuration File	**Step 14.1.** From the GUI, Navigate to **System Administration** and choose **Configuration File**. **Step 14.2.** In the **Load Configuration** section, Select **Load a configuration file from local computer**. **Step 14.3.** Click **Choose File** and select the XML configuration file. **Step 14.4.** If the migration matches the **Scenario 1** and the previous IP address must be use in the new SWA, Select the check box **Load Network Settings**, else do not select this option. **Step 14.5.** Click **Load**. **Step 14.6.** Click **Continue** in the **Confirm Load Configuration** pop up.  Load Configuration Load Configuration: ? Load a complete or partial configuration *Note: Files with masked passwords cannot be loaded using Load Configuration.* ○ Load a configuration file from the appliance: S100V-4204134CB5AD31EC3693-3A6073B16567-20260304T132633-15.5.0-710.xml.audit_l S100V-4204134CB5AD31EC3693-3A6073B16567-20260304T132556-15.5.0-710.xml.audit_l S100V-4204134CB5AD31EC3693-3A6073B16567-20260304T132544-15.5.0-710.xml.audit_l EUN_DEFAULT.tar.gz Preview Selected File ● Load a configuration file from local computer: Choose File Source-SWA-...-Migrate.xml ○ Paste your configuration in the space provided below: □ Load Network Settings ***Warning!** Loading configuration will permanently remove all of your current configuration settings. It is strongly recommended that you save your configuration before performing these actions.* *Basic network settings (interface configuration, routing tables, and DNS settings) will be retained unless the option to load network settings is selected.* Load *Image - Importing the Configuration*
Step 15. Changing the admin Password ✎ **Note**: If you have the **Source SWA** admin password, Skip to **Step 16**.	**15.1.** From the GUI, Navigate to **System Administration** and choose **Users**. **15.2.** click the **admin** user name. **15.3.** Select **Change the passphrase**. **15.4.** Enter the password. **15.5.** click **Submit**.

	 Edit Local User Local User Settings Account Status: Active Lock Account User Name: admin Full Name: Administrator User Type: ● Administrator Passphrase: ○ Do not change the passphrase ● Change the passphrase Passphrase: •••••••• Retype Passphrase: •••••••• Cancel Submit *Image - Changing Admin Password*
Step 16. Commit	**Step 16.1.** Now you can **Commit** the changes.
Step 17. Importing the Routes **Note**: If you **Load Network Settings** while importing the configuration, skip to **Step 19**.	**Step 17.1.** From the GUI, Navigate to **Network** and click **Routes**. **Step 17.2.** For each routing table, click **Load Route Table**. **Step 17.3.** Choose the file you exported on **Step 8**. **Step 17.4**. Click **Submit**. **Step 17.5. Commit** the changes.
Step 18. Configuring the DNS Settings **Note**: If you **Load Network Settings** while importing the configuration, skip to **Step 19**.	**Step 18.1.** From the GUI, Navigate to **Network** and click **DNS**. **Step 18.2.** Click **Edit Settings**. **Step 18.3.** Use the screenshot from **Step 9** **Step 18.4.** Click **Submit**. **Step 18.5. Commit** the changes.
Step 19. Join/Rejoin the SWA to the Active Directory	**Step 19.1.** From the GUI, Navigate to **Network** and click **Authentication**. **Step 19.2.** click the name of the Authentication **Realm Name**. **Tip**: If the SWA is assigned a new IP address and host-name, ensure that the necessary DNS records are created in the Active Directory DNS service. **Step 19.2.** Click **Join Domain** and enter the credentials:



Edit Realm

Authentication Realm

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

Active Directory Authentication

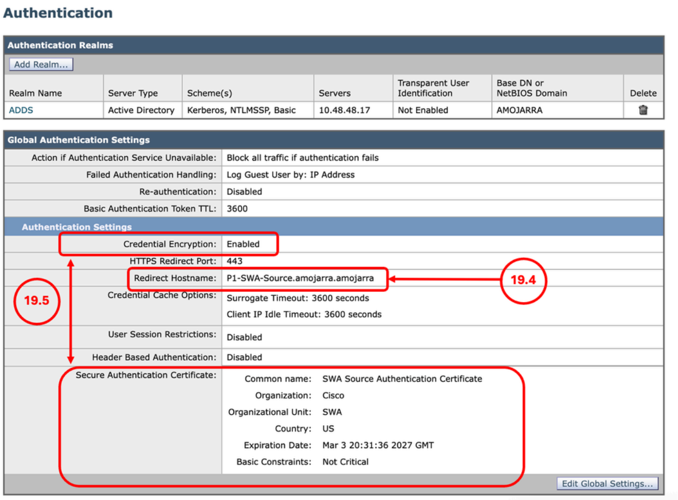
Active Directory Server:	Specify up to three Active Directory servers: □ Set Source Interface Source Interface: Management 10.48.48.17 hostname or IP address
Active Directory Account:	Active Directory Domain: AMOJARRA.AMOJARRA Computer Account Location: Computers (Example: Computers/BusinessUnit/Department/Servers) □ Enable Trusted Domain Health Check Join Domain... Status: Computer account wsa1550710$ not yet created.

Image - Join to Active Directory Domain

Step 19.3. Click **Submit**.

Step 19.4. Make sure the **Redirect Hostname** is correct.

Step 19.5. If the **Credential Encryption** is enabled, Make sure the **Secure Authentication Certificate** is correct.



Authentication

Authentication Realms

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	🗑

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...

Image - Authentication Settings

Step 19.6. Commit the changes.

Step 20. Re-join to SMA

Note: If the SWA is not managed by SMA, skip this step.

Note: If you did not replace the existing SWA (Scenario-2), and the migrated SWA having a new IP address, add the SWA as a new device to SMA and skip **Step 20**.

Step 20.1. Connect to CLI of the SMA.

Step 20.2. run **logconfig**.

Step 20.3. Enter **HOSTKEYCONFIG**.

Step 20.4. Type **DELETE** and press **Enter**.

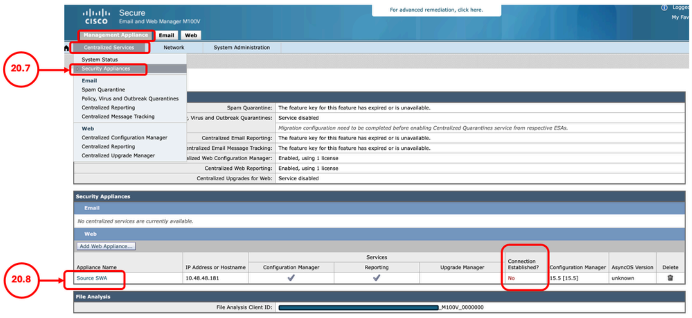
Step 20.5. Type the number associated to the SWA that has been recently migrated and press **Enter** until the wizard is finished.

Step 20.6. Type **commit** and press **Enter** to save the changes.

Step 20.7. From the SMA GUI, navigate to **Management Appliance**. Select **Centralized Services** and click **Security Appliances**.

Step 20.8. click the name of the SWA that recently were migrated.

Tip: You can see the **Connection Established** column is set to **No**.



Spam Quarantine:	The feature key for this feature has expired or is unavailable.
, Virus and Outbreak Quarantines:	Service disabled
	Migration configuration need to be completed before enabling Centralized Quarantines service from respective ESAs.
Centralized Email Reporting:	The feature key for this feature has expired or is unavailable.
entralized Email Message Tracking:	The feature key for this feature has expired or is unavailable.
alized Web Configuration Manager:	Enabled, using 1 license
Centralized Web Reporting:	Enabled, using 1 license
Centralized Upgrades for Web:	Service disabled

Security Appliances

Email

No centralized services are currently available.

Web

Appliance Name	IP Address or Hostname	Services			Connection Established?	Configuration Manager	AsyncOS Version	Delete
		Configuration Manager	Reporting	Upgrade Manager				
Source SWA	10.48.48.181	✓	✓		No	15.5 [15.5]	unknown	🗑

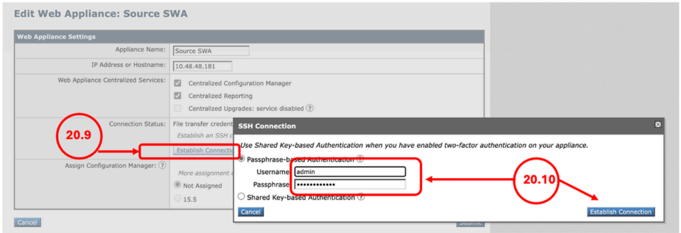
File Analysis

File Analysis Client ID: M100V_0000000

Image - SMA Security Appliance Status

Step 20.9. click **Establish Connection**.

Step 20.10. Enter the **Username** and **Passphrase** and click **Establish Connection**.



Edit Web Appliance: Source SWA

Web Appliance Settings

Appliance Name: Source SWA

IP Address or Hostname: 10.48.48.181

Web Appliance Centralized Services:
☑ Centralized Configuration Manager
☑ Centralized Reporting
□ Centralized Upgrades: service disabled

Connection Status: File transfer credent
Establish an SSH c

Assign Configuration Manager:
More assignment o
● Not Assigned
○ 15.5

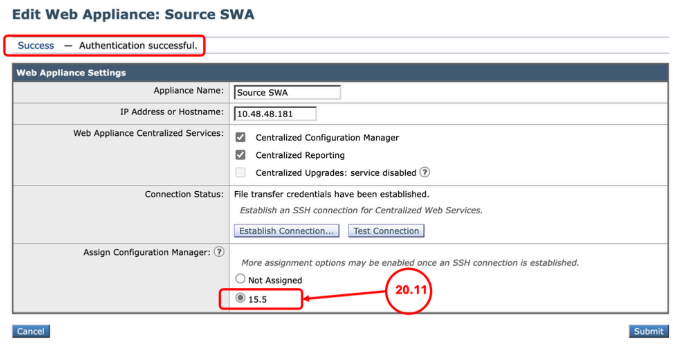
SSH Connection

Use Shared Key-based Authentication when you have enabled two-factor authentication on your appliance.

● Passphrase-based Authentication
Username: admin
Passphrase: •••••••••••••
○ Shared Key-based Authentication

Image - Establish Connection to the SWA

Step 20.11. Assign the configuration Manager.



Edit Web Appliance: Source SWA

Success — Authentication successful.

Web Appliance Settings

Appliance Name:	Source SWA
IP Address or Hostname:	10.48.48.181
Web Appliance Centralized Services:	☑ Centralized Configuration Manager ☑ Centralized Reporting □ Centralized Upgrades: service disabled
Connection Status:	File transfer credentials have been 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

Image - Assign Configuration Manager

Step 20.12. Submit and **Commit** the changes.

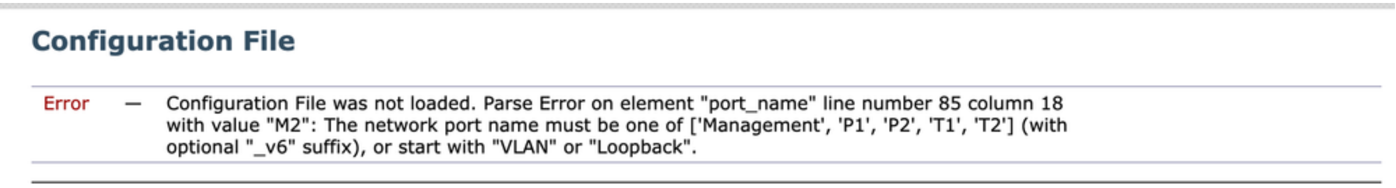
Step 20.13. (Optional) you can test by publishing configuration to the SWA.

Tip: The SMA retains all Reporting and Tracking data from the previous SWA.

Fixing Errors

Parse Error on Element port_name

The network port name must be one of **['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".

Image - Network Interface Naming Error

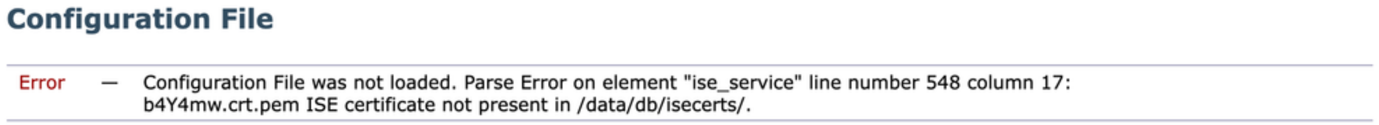
```
Error    –    Configuration File was not loaded. Parse Error on element "port_name" line number 85 colu
```

This error happens when you are migrating from physical SWA to Virtual. the Virtual SWA has only 5 NICs and the M2 interface is invalid. To fix the error, edit the XML configuration file in a text editor and remove these lines:

```
<port_interface>
      <port_name>M2</port_name>
      <direct>
        <jack>M2</jack>
      </direct>
</port_interface>
```

```
<ethernet>
      <ethernet_interface>M2</ethernet_interface>
      <media>autoselect</media>
      <media_opt></media_opt>
      <macaddr>aa:bb:cc:00:00:00</macaddr>
</ethernet>
```

Parse Error on Element 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/.

Image - ISE Certificate Error

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

Since the ISE certificates are not included in the SWA configuration export, and are uploaded on the device directly, you need to remove the certificates configuration from the XML file and after successful import, configure ISE manually. to fix this issue, edit the XML configuration file in the text editor and search for the certificate name in the error (in this example, search for **AA11AA**) and delete it from the configuration file:

```
Before:
      <ise_service_pxgrid_certs>
         <pxgrid_cert>AA11AA</pxgrid_cert>
         <pxgrid_cert>BB22BB</pxgrid_cert>
      </ise_service_pxgrid_certs>

After:
      <ise_service_pxgrid_certs></ise_service_pxgrid_certs>
```

Other than the certificate name, you need to remove the **Web Appliance Client Certificate** name as well.

In this example, the **Web Appliance Client Certificate** is a self signed certificate:

```
Before:
<ise_service_cert_generated>1</ise_service_cert_generated>
<ise_service_generated_name>xAcK6T</ise_service_generated_name>

After:
```

```
<ise_service_cert_generated>0</ise_service_cert_generated>
<ise_service_generated_name></ise_service_generated_name>
```

Failover is not Working on New Virtual SWA

If the High Availability (Failover) is not working on the target virtual SWA, ensure that the Hypervisor is configured correctly. For more information, visit: Ensure Proper Virtual WSA HA Group Functionality in a VMware Environment

Related Information

- User Guide for AsyncOS 15.2 for Cisco Secure Web Appliance
- Install Secure Web Appliance on Vmware ESXi
- Install Secure Web Appliance on Microsoft Hyper-V
- Secure Web Appliance Initial Setup
- Cisco Secure Email and Web Virtual Appliance Installation Guide
- Configure Custom URL Categories in Secure Web Appliance - Cisco
- Use Secure Web Appliance Best Practices
- Configure Firewall for Secure Web Appliance
- Configure Decryption Certificate in Secure Web Appliance
- Troubleshoot Secure Web Appliance DNS Service
- Ensure Proper Virtual WSA HA Group Functionality in a VMware Environment