Migrar configuração entre dois SWAs

Contents

Introdução

Este documento descreve o processo de restauração da configuração de um Secure Web Appliance (SWA) para outro.

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Acesso à interface gráfica do usuário (GUI) do SWA

- Acesso administrativo ao SWA
- Acesso administrativo ao Security Management Appliance (SMA)
- Acesso ao Cisco Software Licensing Portal ou ao arquivo de licença SWA
- Acesso de usuário privilegiado do Ative Diretory para ingressar o SWA no domínio e criar registros DNS

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Antes de Começar

Neste artigo, descrevemos as etapas para migrar do SWA de origem para o SWA de destino. Esta tabela lista as especificações para cada sistema.

	SWA de origem	SWA de destino
Modelo	S396	S100V
Versão	15.5.0-710	15.5.0-710
Licença	Licença inteligente	Licença inteligente
Diretório ativo	Ingressou	Ingressou
Integrado ao Identity Services Engine (ISE)	Yes	Yes

Número de NICs (Network Interface Card, placa de interface de rede)	5	5
Descriptografia HTTPS	Habilitado com Certificado Autoassinado	Habilitado com Certificado Autoassinado
Redirecionamento Transparente	WCCP	WCCP
Gerenciado pelo SMA	Yes	Yes
Servidor de Log Externo	Push SCP	Push SCP
Alta Disponibilidade	Habilitado	Habilitado

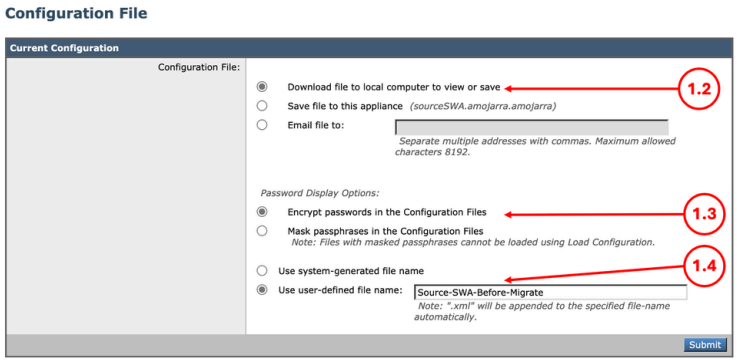
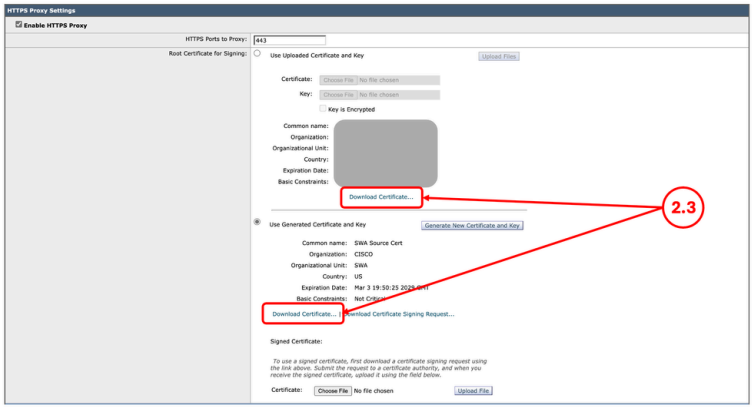
Note: Certifique-se sempre de que, ao instalar um novo SWA virtual, todas as interfaces de rede recomendadas pela Cisco estejam presentes e configuradas na máquina virtual (VM). As interfaces podem permanecer desconectadas, mas devem estar disponíveis na VM.

Há dois cenários possíveis ao migrar o SWA de um dispositivo para outro:
[Cenário 1] Substituição do SWA existente: O SWA original é desativado e o endereço IP do SWA de destino é o mesmo do SWA de origem.
[Cenário 2] Adicionando um novo SWA: O SWA original permanece em serviço enquanto o novo SWA é configurado.

Preparando e fazendo backup do SWA de origem

Use estas etapas para coletar os arquivos e a configuração necessários do SWA de origem:

Etapa 1. Exportar o arquivo de configuração	Etapa 1.1. Na GUI, navegue até System Administration (Administração do sistema) e escolha Configuration File. Etapa 1.2. Certifique-se de que Download file to local computer to view or save está selecionado. Etapa 1.3. Escolha Criptografar senhas nos arquivos de configuração Etapa 1.4. (Opcional) Escolha um nome para o

	arquivo de configuração. Etapa 1.5. Clique em Submit.  Imagem - Exportando o arquivo de configuração
Etapa 2. Exportar o certificado de descriptografia Note: Se a Descriptografia HTTPS estiver desativada, vá para a Etapa 3.	Etapa 2.1. Na GUI, navegue até Security Services e clique em HTTPS Proxy. Etapa 2.2. Clique em Edit Settings. Etapa 2.3. Faça o download do certificado de descriptografia HTTPS, clicando em Download do certificado... link.  Imagem - Certificado de descriptografia HTTPS Note: Neste exemplo, os dois tipos de certificados de descriptografia HTTPS estão ilustrados; no entanto, em sua rede, você pode ter apenas um tipo implantado.
Etapa 3. Exportar os certificados raiz de confiança personalizados	Etapa 3.1. Na GUI, navegue até Network e clique em Certificate Management. Etapa 3.2. Na seção Gerenciamento de certificados,

Note: Se nenhum certificado de raiz confiável personalizado for adicionado ao SWA, vá para a Etapa 4.

clique em Gerenciar certificados raiz confiáveis.

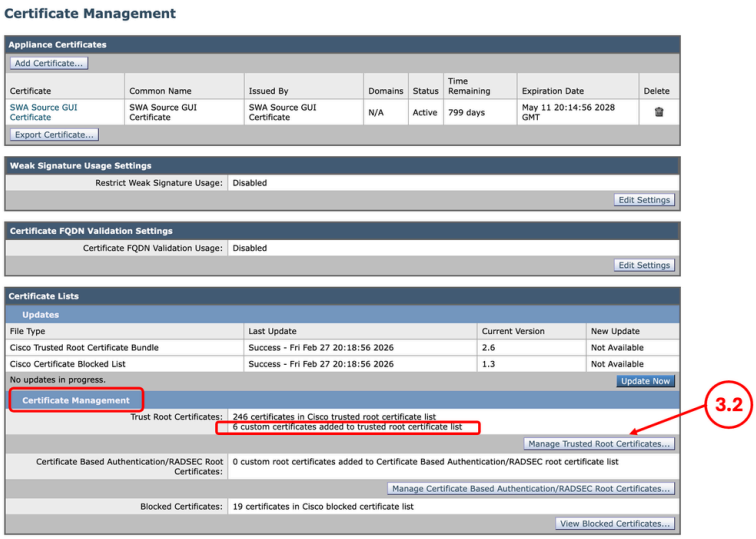


Imagem - Gerenciar Certificados Raiz Confiáveis

Etapa 3.3. Expanda cada Certificado de Raiz Confiável Personalizado clicando em seu nome e clique em Baixar Certificado...

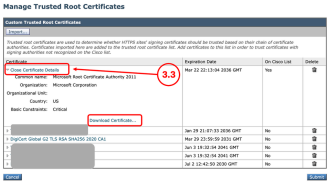


Imagem - Baixar Certificados raiz Confiáveis

Etapa 4. Exportar o Certificado da GUI

Note: Se você estiver usando um certificado de GUI integrado, vá para a Etapa 5.

Etapa 4.1. Na GUI, navegue até Network e clique em Certificate Management.

Etapa 4.2. Na seção Certificados do equipamento, clique em Exportar certificado.

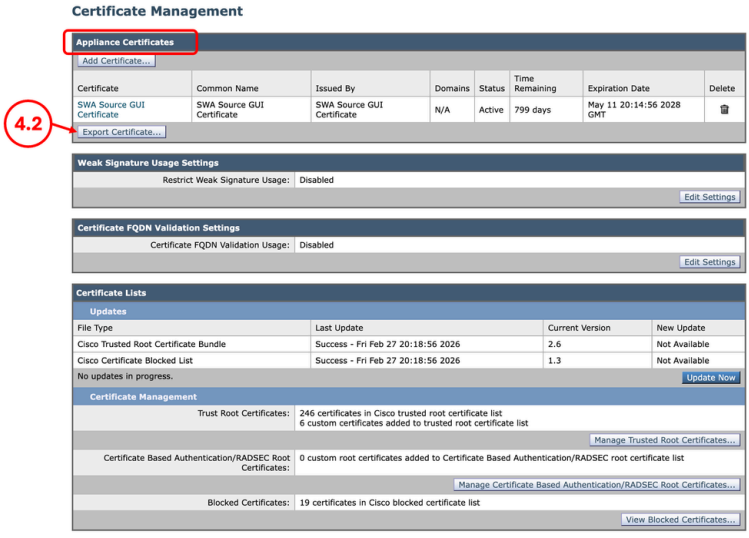
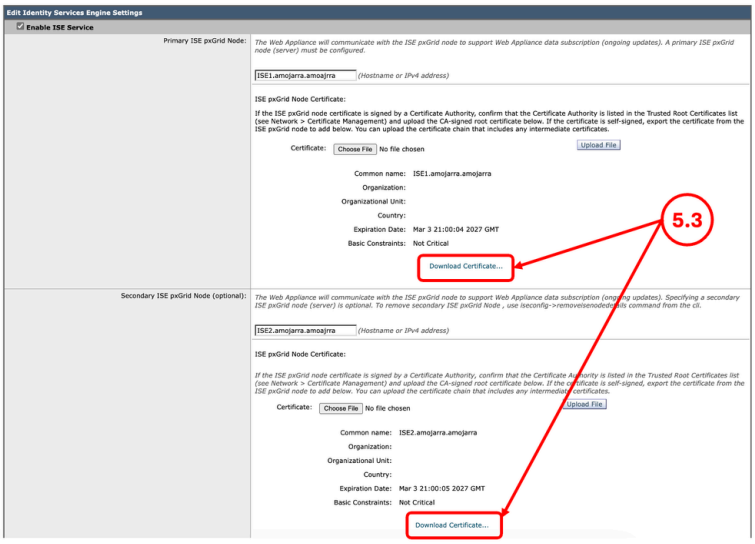


	Imagem - Exportar certificado da GUI
Etapa 5. Exportar os certificados do ISE Note: Se não houver SWA, integração do ISE, vá para a Etapa 6.	Etapa 5.1. Na GUI, navegue até Network e clique em Identity Services Engine. Etapa 5.2. Clique em Edit Settings. Etapa 5.3. Faça o download de todos os certificados disponíveis.  Imagem - Fazer download de certificados ISE
Etapa 6. Licenças / Recursos	Etapa 6.1. Na GUI, vá até System Administration (Administração do sistema) e clique em Licenses ou Features dependendo do tipo de licença que você está usando. Etapa 6.2. Faça uma captura de tela de suas Licenças / Recursos.
Etapa 7. Certificado de redirecionamento de autenticação	Etapa 7.1. Na GUI, navegue até Network e clique em Authentication. Etapa 7.2. Se a Criptografia de credencial estiver habilitada, verifique se você tem o Certificado e a Chave. Etapa 7.3. Faça uma captura de tela da configuração atual.

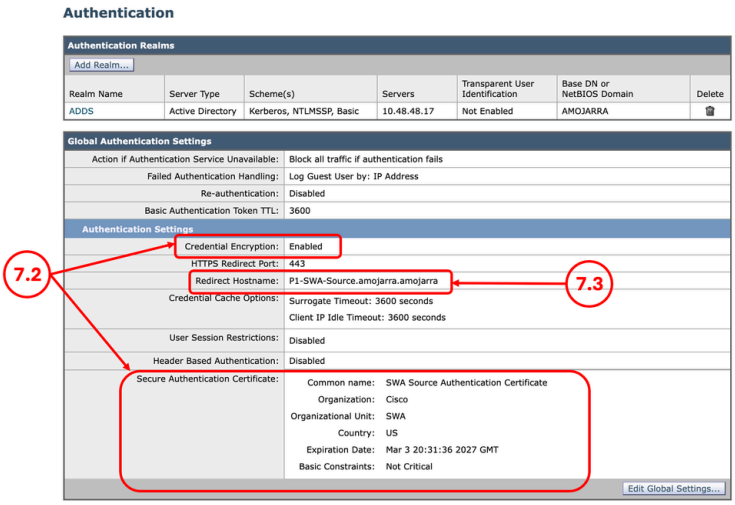
<table>
<tr>
<td></td>
<td> 

Imagem - Certificado de autenticação

Note: Não é possível fazer o download do certificado de autenticação a partir da GUI.</td>
</tr>
<tr>
<td>Etapa 8. Exportar rotas estáticas

Note: Se você estiver planejando usar a mesma configuração de rede e o mesmo endereço IP para o SWA de destino, vá para a Etapa 10.</td>
<td>Etapa 8.1. Na GUI, navegue até Network e clique em Routes.

Etapa 8.2. Para cada tabela de roteamento, clique em Save Route Table.

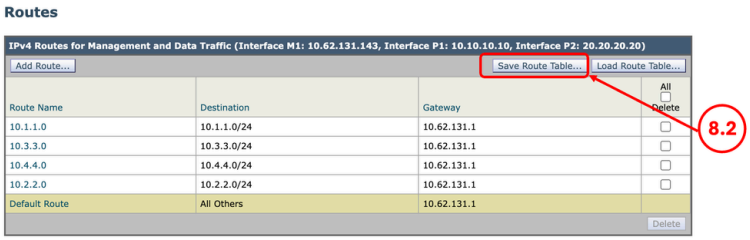
 

Imagem - Exportando a tabela de roteamento</td>
</tr>
<tr>
<td>Etapa 9. Configurações DNS

Note: Se você estiver planejando usar a mesma configuração de rede e o mesmo endereço IP para o SWA de destino, vá para a Etapa 10.</td>
<td>Etapa 9.1. Na GUI, navegue até Network e clique em DNS.

Etapa 9.2. Faça uma captura de tela da configuração do DNS.</td>
</tr>
</table>

Preparação do SWA de destino

Etapa 10. Instalar o SWA virtual Note: Se o SWA de destino for físico, você poderá ir para a Etapa 11.	Etapa 10.1. Use estes guias para instalar o SWA virtual: • Instale o Secure Web Appliance no Vmware ESXi • Instale o Secure Web Appliance no Microsoft Hyper-V Etapa 10.2. Certifique-se de que o novo SWA tenha o acesso de rede recomendado: • Configurar firewall para dispositivo seguro da Web
Etapa 11. Configuração inicial do SWA	Etapa 11.1. Configure o endereço IP. Etapa 11.2. Configure o Gateway padrão. Etapa 11.3. Configurar o servidor DNS. Etapa 11.4. licenciar o equipamento. Etapa 11.5. Ative os recursos. Etapa 11.6. Execute o assistente de configuração do sistema. Você pode encontrar as etapas detalhadas neste artigo: Configuração inicial do dispositivo da Web seguro
Etapa 12. Limpar o arquivo de configuração Note: Se você não estiver integrando o ISE com o SWA, pule para a Etapa 13.	Etapa 12.1. Revise a seção Correção de erros neste artigo para remover a configuração do certificado ISE do arquivo de backup XML.

Importação do arquivo de configuração para o SWA de destino

Etapa 13. Importar certificados de raiz confiáveis personalizados	Etapa 13.1. Na GUI, navegue até Network e clique em Certificate Management. Etapa 13.2. Na seção Gerenciamento de

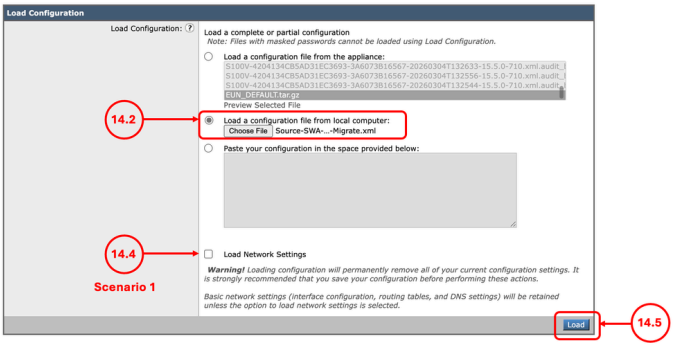
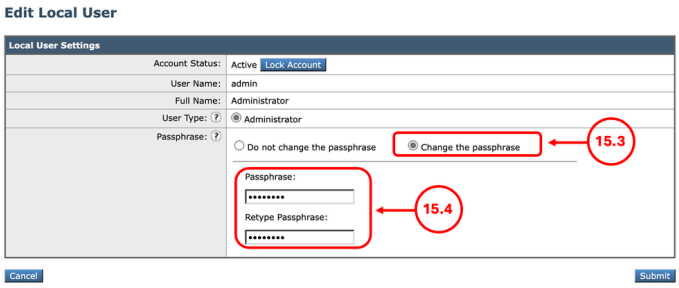
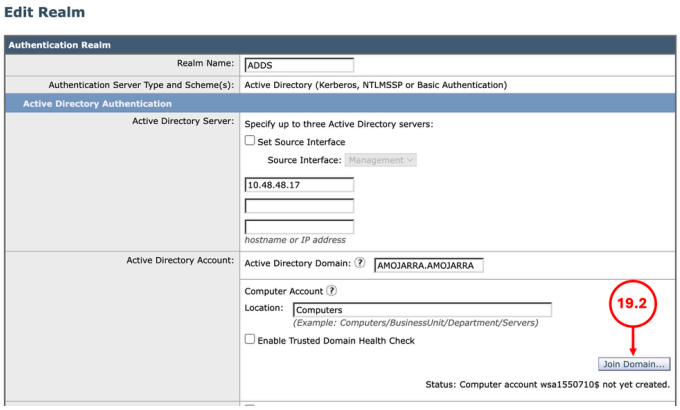
Note: Se você não estiver usando nenhum Certificado raiz confiável personalizado, vá para a Etapa 14.	certificados, clique em Gerenciar certificados raiz confiáveis. Etapa 13.3. Clique em Importar. Etapa 13.4. Carregue os certificados que foram baixados anteriormente na Etapa 3. Caution: Quando os certificados raiz e intermediários estiverem disponíveis, comece carregando o certificado CA raiz. Após enviar e confirmar as alterações, continue a importar o certificado intermediário.
Etapa 14. Importar o arquivo de configuração	Etapa 14.1. Na GUI, navegue até System Administration (Administração do sistema) e escolha Configuration File. Etapa 14.2. Na seção Carregar configuração, selecione Carregar um arquivo de configuração do computador local. Etapa 14.3. Clique em Choose File e selecione o arquivo de configuração XML. Etapa 14.4. Se a migração corresponder ao cenário 1 e o endereço IP anterior precisar ser usado no novo SWA, marque a caixa de seleção Load Network Settings, caso contrário, não selecione essa opção. Etapa 14.5. Clique em Carregar. Etapa 14.6. Clique em Continuar no pop-up Confirmar configuração de carregamento. 

	Imagem - Importando a configuração
Etapa 15. Alterar a senha do administrador Observação: se você tiver a senha de administrador do SWA de origem, vá para a Etapa 16.	15.1. Na GUI, navegue até System Administration (Administração do sistema) e escolha Users. 15.2. clique no nome de usuário admin. 15.3. Selecione Alterar a senha. 15.4. Digite a senha. 15.5. clique em Enviar.  Imagem - Alterando a senha do administrador
Etapa 16. Confirmar	Etapa 16.1. Agora você pode Confirmar as alterações.
Etapa 17. Importar as Rotas Observação: se você carregar as configurações de rede ao importar a configuração, vá para a Etapa 19.	Etapa 17.1. Na GUI, navegue até Network e clique em Routes. Etapa 17.2. Para cada tabela de roteamento, clique em Load Route Table. Etapa 17.3. Escolha o arquivo exportado na Etapa 8. Etapa 17.4. Clique em Enviar. Etapa 17.5. Confirme as alterações.
Etapa 18. Definir as configurações DNS Note: Se você Carregar as Configurações de Rede ao importar a configuração, vá para a Etapa 19.	Etapa 18.1. Na GUI, navegue até Network e clique em DNS. Etapa 18.2. Clique em Edit Settings. Etapa 18.3. Use a captura de tela da Etapa 9

	Etapa 18.4. Clique em Enviar. Etapa 18.5. Confirme as alterações.
Etapa 19. Ingressar/Reingressar o SWA no Ative Diretory	Etapa 19.1. Na GUI, navegue até Network e clique em Authentication. Etapa 19.2. clique no nome do Nome do território de autenticação. Tip: Se o SWA receber um novo endereço IP e nome de host, certifique-se de que os registros DNS necessários sejam criados no serviço DNS do Ative Diretory. Etapa 19.2. Clique em Ingressar no Domínio e insira as credenciais:  Imagem - Ingressar no Domínio do Ative Diretory Etapa 19.3. Clique em Submit. Etapa 19.4. Certifique-se de que o nome de host de redirecionamento esteja correto. Etapa 19.5. Se a Criptografia de Credencial estiver habilitada, verifique se o Certificado de Autenticação Segura está correto.

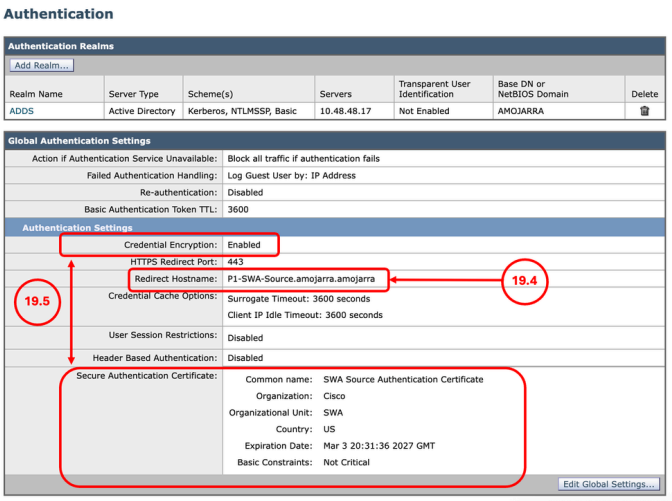


Imagem - Configurações de autenticação

Etapa 19.6. Confirme as alterações.

Etapa 20. Reingressar no SMA

Note: Se o SWA não for gerenciado pelo SMA, ignore esta etapa.

Note: Se você não substituiu o SWA existente (Cenário 2) e o SWA migrado tiver um novo endereço IP, adicione o SWA como um novo dispositivo ao SMA e ignore a Etapa 20.

Etapa 20.1. Conectar-se ao CLI do SMA.

Etapa 20.2. execute logconfig.

Etapa 20.3. Digite HOSTKEYCONFIG.

Etapa 20.4. Digite DELETE e pressione Enter.

Etapa 20.5. Digite o número associado ao SWA que foi migrado recentemente e pressione Enter até que o assistente seja concluído.

Etapa 20.6. Digite commit e pressione Enter para salvar as alterações.

Etapa 20.7. Na GUI do SMA, navegue até Management Appliance. Selecione Centralized Services e clique em Security Appliances.

Etapa 20.8. clique no nome do SWA que foi migrado recentemente.

Tip: Você pode ver que a coluna Conexão Estabelecida está definida como Não.

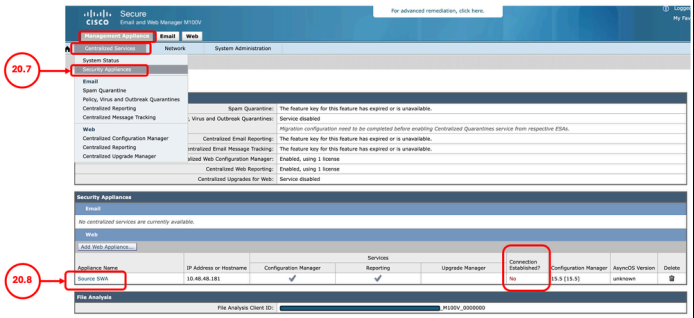


Imagem - Status do dispositivo de segurança SMA

Etapa 20.9. clique em Establish Connection.

Etapa 20.10. Insira o nome de usuário e a senha e clique em Estabelecer conexão.

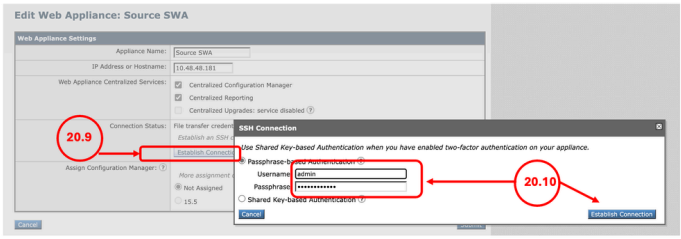


Imagem - Estabelecer conexão com o SWA

Etapa 20.11. Atribuir o gerenciador de configurações.

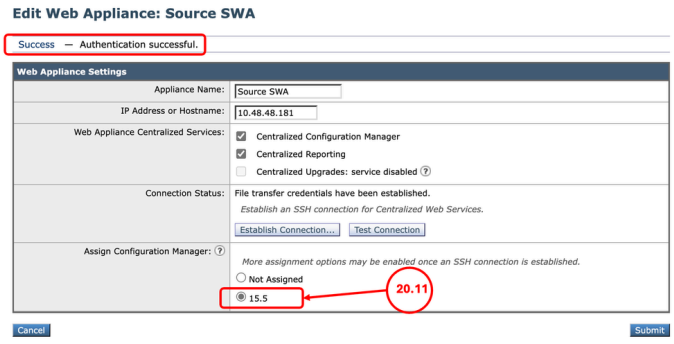


Imagem - Atribuir o Gerenciador de configurações

Etapa 20.12. Enviar e confirmar as alterações.

Etapa 20.13. (Opcional) você pode testar publicando a configuração no SWA.

Tip: O SMA retém todos os dados de relatório e rastreamento do SWA anterior.

Corrigindo erros

Erro de Análise no Elemento port_name

O nome da porta de rede deve ser um de ['Management', 'P1', 'P2', 'T1', 'T2']:

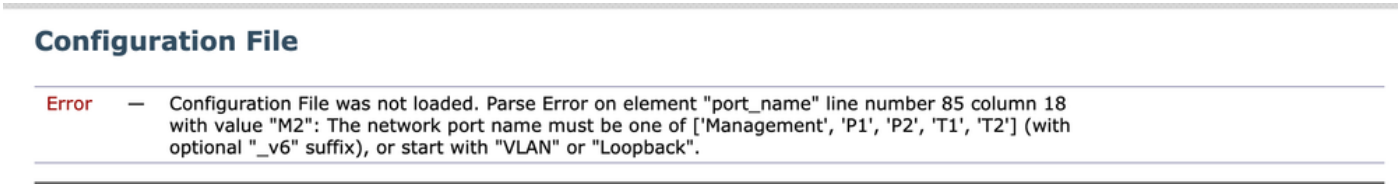


Imagem - Erro de Nomeação de Interface de Rede

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

Este erro ocorre quando você está migrando de SWA físico para Virtual. o SWA virtual tem apenas 5 NICs e a interface M2 é inválida. Para corrigir o erro, edite o arquivo de configuração XML em um editor de texto e remova estas linhas:

```
        M2
```

```
        M2
```

```
M2

autoselect

aa:bb:cc:00:00:00
```

Erro de análise no elemento ise_service

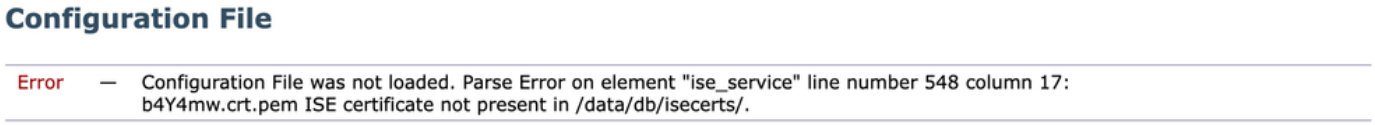


Imagem - Erro de certificado ISE

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

Como os certificados ISE não estão incluídos na exportação da configuração SWA e são carregados diretamente no dispositivo, você precisa remover a configuração de certificados do arquivo XML e, após a importação bem-sucedida, configurar o ISE manualmente. para corrigir esse problema, edite o arquivo de configuração XML no editor de texto e procure o nome do certificado no erro (neste exemplo, procure AA11AA) e exclua-o do arquivo de configuração:

```
Before:

        AA11AA

        BB22BB

After:
```

Além do nome do certificado, você também precisa remover o nome do Certificado de cliente do equipamento da Web.

Neste exemplo, o Certificado de cliente de dispositivo da Web é um certificado autoassinado:

```
Before:

       1

       xAcK6T

After:

       0
```

O failover não está funcionando no novo SWA virtual

Se o High Availability (Failover) não estiver funcionando no SWA virtual de destino, verifique se o hipervisor está configurado corretamente. Para obter mais informações, visite: Garantir a funcionalidade adequada do grupo HA do WSA Virtual em um ambiente VMware

Informações Relacionadas

- Manual do usuário do AsyncOS 15.2 para Cisco Secure Web Appliance
- Instale o Secure Web Appliance no Vmware ESXi
- Instale o Secure Web Appliance no Microsoft Hyper-V
- Configuração inicial do Secure Web Appliance
- Guia de instalação do Cisco Secure Email and Web Virtual Appliance
- Configurar categorias de URL personalizadas no Secure Web Appliance - Cisco
- Use as práticas recomendadas de dispositivos da Web seguros
- Configurar firewall para dispositivo seguro da Web
- Configurar certificado de descriptografia no aplicativo da Web seguro
- Solucionar problemas do serviço DNS do Secure Web Appliance
- Garanta a funcionalidade adequada do grupo HA do Virtual WSA em um ambiente VMware

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.