

Controle a negociação TLS na entrega no ESA

Índice

[Introdução](#)

[Permita o TLS na entrega](#)

[Definições do ajuste TLS](#)

[Permita o TLS no GUI](#)

[Permita o TLS no CLI](#)

Introdução

Este documento descreve como controlar a negociação do Transport Layer Security (TLS) na entrega na ferramenta de segurança do email (ESA).

Como definido no RFC 3207, o “TLS é uma extensão ao serviço SMTP que permite que um servidor SMTP e um cliente usem o Transport Layer Security para fornecer uma comunicação privada, autenticada sobre o Internet. O TLS é um mecanismo popular para aumentar comunicações TCP com privacidade e autenticação.”

Permita o TLS na entrega

Você pode exigir STARTTLS para a entrega do email aos domínios específicos com qualquer um destes métodos descritos neste documento:

- Use o comando do **destconfig** CLI.
- Do GUI escolha **políticas do correio > controles do destino**.

O destino controla a página ou o comando do **destconfig** permite que você especifique cinco ajustes diferentes para o TLS para um domínio dado quando você inclui um domínio. Além, você pode ditar se a validação do domínio é necessária.

Definições do ajuste TLS

Ajuste TLS	Significado
Padrão	O ajuste do padrão TLS que está ajustado quando você usar a página dos controles do destino ou o destconfig - > subcommand do padrão usado para conexões de saída do ouvinte ao agente de transferência de mensagem (MTA) para o domínio. O valor “padrão” é ajustado se você responde não à pergunta: “Você deseja aplicar um ajuste específico TLS para este domínio?”
1. No	O TLS não é negociado para conexões de saída da relação ao MTA para o domínio. O TLS é negociado da relação ESA ao MTA para o domínio. Contudo, se a negociação TLS falha (antes de receber uma resposta 220), a transação de SMTP continua “na claro”
2. Preferido	(não cifrado). Nenhuma tentativa está feita para verificar se o certificado origina de um Certificate Authority confiado. Se um erro ocorre depois que a resposta 220 está recebida, a transação de SMTP não cai de volta ao texto claro.
3. Necessário	O TLS é negociado da relação ESA ao MTA para o domínio. Nenhuma tentativa é feita para verificar o certificado do domínio. Se a negociação falha, nenhum email está enviado através da conexão. Se a negociação sucede, o correio está entregue através de uma

sessão de criptografia.

O TLS é negociado do ESA ao MTA para o domínio. O dispositivo tenta verificar o certificado do domínio. Três resultados são possíveis:

4. **Preferido (verifique)**
- O TLS é negociado e o certificado é verificado. O correio é entregue através de uma sessão de criptografia.
 - O TLS é negociado, mas o certificado não é verificado. O correio é entregue através de uma sessão de criptografia.
 - Nenhuma conexão TLS é feita e, o certificado não é verificado subsequentemente. O mensagem de Email é entregue no texto simples.

O TLS é negociado do ESA ao MTA para o domínio. A verificação do certificado do domínio é exigida. Três resultados são possíveis:

5. **Exigido (verifique)**
- Uma conexão TLS é negociada e o certificado é verificado. O mensagem de Email é entregue através de uma sessão de criptografia.
 - Uma conexão TLS é negociada, mas o certificado não é verificado por uma autoridade confiada de Certificate (CA). O correio não é entregue.
 - Uma conexão TLS não é negociada. O correio não é entregue.

A diferença entre o **TLS exigido - Verifique** e **TLS exigido - Verifique que as opções de domínio hospedadas** colocam no processo de verificação da identidade. A maneira como a identidade apresentada é processada e que tipo de identificadores da referência é permitido ser usado faz a diferença sobre um resultado final.

6. **Exigido - Verifique domínios hospedados**
- A identidade apresentada é derivada primeiramente da extensão do subjectAltName do tipo dNSName. Se não há nenhuma harmonia entre o dNSName e essa das identidades aceitas da referência (REF-ID), a verificação não falha nenhuma matéria se o CN existe no campo de assunto e poderia passar uma verificação mais adicional da identidade. O CN derivado do campo de assunto é validado somente quando o certificado não contém alguma da extensão do subjectAltName do tipo dNSName.

Reveja por favor o [processo de verificação TLS para a Segurança do email de Cisco](#) para mais informação.

Permita o TLS no GUI

1. Escolha **Montior > controles do destino**.
2. O clique **adiciona o destino**.
3. Adicionar o domínio do destino no campo de destino.
4. Selecione o método do apoio TLS da lista de drop-down do apoio TLS.
5. O clique **submete-se** a fim submeter as mudanças.

Destination Controls	
Destination:	example.com
IP Address Preference:	Default (IPv6 Preferred)
Limits:	Concurrent Connections: <input checked="" type="radio"/> Use Default (500) <input type="radio"/> Maximum of <input type="text" value="500"/> (between 1 and 1,000)
	Maximum Messages Per Connection: <input checked="" type="radio"/> Use Default (50) <input type="radio"/> Maximum of <input type="text" value="50"/> (between 1 and 1,000)
	Recipients: <input checked="" type="radio"/> Use Default (No Limit) <input type="radio"/> Maximum of <input type="text" value="0"/> per <input type="text" value="60"/> minutes <i>Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60</i>
	Apply limits: Per Destination: <input checked="" type="radio"/> Entire Domain <input type="radio"/> Each Mail Exchanger (MX Record) IP address Per ESA hostname: <input checked="" type="radio"/> System Wide <input type="radio"/> Each Virtual Gateway <i>(recommended if Virtual Gateways are in use)</i>
TLS Support:	Required
<i>A security certificate/key has not yet been configured. Enabling TLS will automatically enable the "Demo" certificate/key. (To configure a different certificate/key, start the CLI and use the certconfig command.)</i>	
Bounce Verification:	Perform address tagging: <input checked="" type="radio"/> Default (No) <input type="radio"/> No <input type="radio"/> Yes <i>Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.</i>
Bounce Profile:	Default <i>Bounce Profile can be configured at Network > Bounce Profiles.</i>

Cancel Submit

Permita o TLS no CLI

Este exemplo usa o comando do **destconfig** a fim exigir conexões TLS e conversações cifradas para o domínio *example.com*. Note que este exemplo mostra que o TLS está exigido para um domínio que use o certificado da demonstração instalado no dispositivo. Você pode permitir o TLS com o certificado da demonstração para propósitos testando, mas não é seguro e não é recomendado para o uso geral.

O valor “padrão” é ajustado se você responde **não** à pergunta: “Você deseja aplicar um ajuste específico TLS para este domínio?” Se você responde **sim**, escolha o **nenhum**, **preferido**, ou **exigido**.

```
ESA> destconfig
```

```
Choose the operation you want to perform:
```

- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.

```
[> new
```

```
Enter the domain you wish to configure.
```

[]> **example.com**

Choose the operation you want to perform:

- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.

[]> **new**

Enter the domain you wish to configure.

[]> **example.com**

Do you wish to configure a concurrency limit for example.com? [Y]> **N**

Do you wish to apply a messages-per-connection limit to this domain? [N]> **N**

Do you wish to apply a recipient limit to this domain? [N]> **N**

Do you wish to apply a specific TLS setting for this domain? [N]> **Y**

Do you want to use TLS support?

1. No
2. Preferred
3. Required
4. Preferred - Verify
5. Required - Verify
6. Required - Verify Hosted Domains

[1]> **3**

You have chosen to enable TLS. Please use the 'certconfig' command to ensure that there is a valid certificate configured.

Do you wish to apply a specific bounce verification address tagging setting for this domain? [N]> **N**

Do you wish to apply a specific bounce profile to this domain? [N]> **N**

Do you wish to apply a specific IP sort preference to this domain? [N]> **N**

There are currently 3 entries configured.

Choose the operation you want to perform:

- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.

[]> **list**

Domain	Rate Limiting	TLS	Bounce Verification	Bounce Profile	IP Version Preference
example.com	Default	On	Default	Default	Default
(Default)	On	Off	Off	(Default)	Prefer IPv6