Guia de Desconfiança do Cisco IOS XE e GuestShell CA Trust Mudhra

Contents

Propósito

Este documento fornece orientação para o Cisco IOS® XE para a desconfiança de emergência de Mudhra Root e Autoridades de Certificação Intermediárias.

Use este guia para auditar e gerenciar o CA trust para serviços cuja configuração permita as hierarquias afetadas. A aplicabilidade do produto e a correção necessária são definidas nas informações da Cisco. Verifique o suporte de comandos e o impacto do serviço para a versão do Cisco IOS XE antes de alterar a confiança.

Informações da Cisco: cisco-sa-emudhra-info-ScS22A1r

Certificados CA de Mudhra afetados: Original e Assinado Cruzado

Inventário verificado em 29 de outubro de 2026. Oito chaves CA emissoras de Mudhra são afetadas: seis para TLS e dois para assinatura de código. Cada chave aparece em um certificado original da CA emitido pelo emSign e em um certificado da CA com assinatura cruzada do Sectigo. Por conseguinte, o inventário contém 16 certificados: 12 TLS e 4 certificados de assinatura de código.

Cada par original/com assinatura cruzada tem o mesmo assunto e chave pública, mas um emissor diferente, número de série e impressão digital do certificado SHA-256. Os dois formulários fornecem caminhos de certificação alternativos e devem ser incluídos em uma auditoria.

A. Emitentes e inventário dos certificados afetados

Emitente A — Certificados TLS originais: CN=emSign Root TLS CA - G3, O=Mudhra Technologies Limited, C=IN.

Emitente B — Certificados de assinatura de código originais: CN=emSign Root CS CA - G3, O=Mudhra Technologies Limited, C=IN.

Emitente C — Todos os certificados com assinatura cruzada: CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB (Sectigo).

Assuntos G3B: O=Mudhra BV, C=NL. Assuntos G3C: O=Mudhra Inc, C=US. Cada célula variante lista sua referência emissora, serial hexadecimal e impressão digital SHA-256 (duas linhas). O preenchimento de zeros à esquerda não altera um valor serial.

CA (CN) emissora afetada	Certificado original Emissor / serial (hexadecimal) / SHA-256	Certificado com assinatura cruzada Sectigo Emissor / serial (hexadecimal) / SHA-256
1. EM DV TLS CA - G3B TLS	Emitente A A4AEE678F23362B4C0E460B772F214 42C4ACCD12C4F59597925E1A08A7A901 02608543809308D50EC427E118BA1493	Emitente C A024FDF4BA665C785CE4A020483858B7 45A883F349AEDFD5F3A649B5498FFB12 1712BA8B448F3F2A91DBC5A766FCDDBE
2. EM OV TLS CA - G3B TLS	Emitente A 6CADA367FB1C100088120EA202D568 98B896625C0C230ADEEC3EB2CF6AAD50 01ECF9156A68644E82374CE5833BC25B	Emitente C E94223BDE92F914E5AB9ACABFDAC3710 5F1DED4DD590AF74631290CF073B122A 2AAC6A1FA479778A0BD43579BD832699
3. EM EV TLS CA - G3B TLS	Emitente A C7C41EFE92D825F05EAE841A4A82C1 E7568FE6E12331F4FD7DE61DA4C755D 0F8EB192A218D4741A3BA75184333838	Emitente C D8F868E4F2BD9D82402A85A1C1EB731 579480AEA166290BD3C643589E795FC0 D0E54E86505D180F1DFF99EFD3199512
4. EM DV TLS CA - G3C TLS	Emitente A 588B2E3C2BB8CDA13E1A1209254321 0164D7CEAE5BB909C272AF151FF44B11 77AE9B47D9424B94F1D9558C30934D19	Emitente C 91F347F1A5B7D39962B95E0E4E299D1 62B7F9868263F72F6911FC78CEAF72C1 979158B7368BF648683BB2AA39B02E72
5. EM OV TLS CA -	Emitente A	Emitente C

CA (CN) emissora afetada	Certificado original Emissor / serial (hexadecimal) / SHA-256	Certificado com assinatura cruzada Sectigo Emissor / serial (hexadecimal) / SHA-256
G3C TLS	296926C227A3A1526392B19482A504 CB6E15165AC802E9B3F993F16C25D41F 4E81C21EBDE71AE1B012AC00BF9C7C3F	8D5A4811939EF447D77111CDD9849AE9 7485B51C0ED192878FA1D2F948FB529A E1842CC5086C4B67F7BE5B2039DE9489
6. EM EV TLS CA - G3C TLS	Emitente A 8009928A64107601AF05FA2F19F109 432EC25F0D28DE9006D97BF752F17BBB 2CD41F669933FCB072D9A1148D0261F3	Emitente C 05F078752DECE7A1BB8595D303167171 FD9D5C2DBBD4995AB69B8D50C439D952 7B00529199C2FD01B2174EB58F07021F
7. EM OV CS CA - G3B Assinatura de código	Emitente B 7818933F8F85B461A2B35FBA83D0A 9E39DE2881273ACC225A149C72BA3E0F 51424963669AB633EE1DC7DF5DB067B4	Emitente C 41E32B73AC185D6CE0D7480BACF84E69 A496E23AC0CAB8155FC9B117B97EAE36 8EFCBB9041AEC8804D5A308D2D01C2D8
8. EM OV CS CA - G3C Assinatura de código	Emitente B 544B7F922C31AE220A4A922916F6E6 4B2460A466F95FD40113BCDCCA2CEB29 B3B093921DE45474DA7DF48874C630B1	Emitente C D6A5EF613B390F32EF9CDF349F772841 84112972B8E59D14560AE7E711965447 4AAD119990CF3722BFC1E3B91615E1FD

B. Caminhos de certificação para diferenciar

Caminho TLS original

```
emSign ECC Root CA - G3
  +-- emSign Root TLS CA - G3 (issued by emSign ECC Root CA - G3)
       +-- Original EM DV/OV/EV TLS CA - G3B or G3C
            +-- TLS identity certificate
```

Caminho de assinatura de código original (CS raiz confiável diretamente)

```
emSign Root CS CA - G3
  +-- Original EM OV CS CA - G3B or G3C
       +-- Code-signing identity certificate
```

Via com sinal cruzado Sectigo (TLS e assinatura de código)

```
AAA Certificate Services
  +-- One of the eight cross-signed CAs listed above
       +-- TLS or code-signing identity certificate
```

Um caminho TLS também pode terminar em emSign Root TLS CA - G3 quando essa CA é diretamente confiável. Os diagramas mostram as relações relevantes com os emitentes; o caminho aceito depende das âncoras de confiança e da política de validação do serviço de consumo.

As CAs pai/raiz mostradas no exemplo fornecem o contexto da cadeia e não são contadas entre as oito chaves emissoras comprometidas. A decisão de remover ou desconfiar de um pai/raiz é separada da identificação de uma chave intermediária comprometida.

Para identificação, use o emissor do certificado e o número de série junto com a impressão digital SHA-256. Um nome de assunto sozinho é insuficiente. Uma impressão digital do certificado identifica uma variante do certificado; um hash SPKI SHA-256 identifica a chave pública compartilhada por seus formulários original e com assinatura cruzada. A remoção apenas de um intermediário em cache não impede que um peer o apresente por meio de um caminho confiável restante.

Fontes e data de verificação

Em 29 de outubro de 2026, foram verificados os identificadores de certificados em relação aos anexos públicos sobre incidentes. Cada par original/com sinal cruzado contém a mesma chave pública. Use as informações ao vivo da Cisco para verificar a aplicabilidade do produto e o status da correção.

Informações da Cisco: cisco-sa-emudhra-info-ScS22A1r

[Registro de incidente do Mozilla: Compromisso de chave intermediária de Mudhra (2083449)]

[Anexo do certificado CA original (9664066)]

[Anexo de certificado de autoridade de certificação (9664067) com assinatura cruzada AAA]

[Maçã: Caminhos e impressões digitais do certificado TLS original e com assinatura cruzada]

A partir de 31 de outubro de 2026, a CA raiz emSign - G1 não é identificada entre as CAs comprometidas listadas neste guia. Sua confiança contínua permanece sujeita às políticas da sua organização e às atualizações de consultoria subsequentes.

Como o Cisco IOS XE gerencia a confiança de certificados

Os pontos de confiança PKI configurados mantêm certificados de CA/identidade e política de validação. O pool confiável de PKI contém certificados CA internos e baixados para serviços que o usam. Identificar a fonte fiduciária e a política utilizadas por cada serviço relevante; a alteração do pool de confiança não substitui os pontos de confiança configurados separadamente.

1. Auditoria e preparação

Verifique a versão do software, a hora do dispositivo e os certificados instalados:

<#root>

```
show version show clock show crypto pki trustpoints show running-config | section crypto pki trustpoint
```

Comparar o Emissor do certificado completo e o número de série hexadecimal com o inventário, usando o Assunto como contexto de suporte. Quando o Cisco IOS XE exibe apenas impressões digitais MD5 e SHA1, a impressão digital SHA-256 do inventário não pode ser comparada diretamente nessa saída; ele é fornecido para verificação de arquivos de certificado fora do dispositivo. O preenchimento inicial de 00 em números de série pode ser diferente. As pesquisas de nome de fornecedor identificam apenas os candidatos. Registre os serviços que dependem de cada ponto confiável e verifique os caminhos originais e cruzados, incluindo intermediários diretamente confiáveis.

Examples: CA raiz e SubCA afetada

Exemplos abreviados do certificado detalhado são exibidos; outros campos são omitidos. Compare o Assunto, Emissor e número de série.

Exemplo de CA raiz: emSign ECC Root CA - G3

```
CA Certificate
  Certificate Serial Number (hex): 3CF607A968700EDA8B84
  Issuer:
    cn=emSign ECC Root CA - G3
  Subject:
    cn=emSign ECC Root CA - G3
  Associated Trustpoints: <NAME-OR-Trustpool>
```

Exemplo de SubCA afetado: certificado original emitido pelo emSign

```
CA Certificate
  Certificate Serial Number (hex): 00A4AEE678F23362B4C0E460B772F214
  Issuer:
    cn=emSign Root TLS CA - G3
  Subject:
    cn=EM DV TLS CA - G3B
  Associated Trustpoints: <NAME-OR-Trustpool>
```

Exemplo de SubCA afetado: Certificado com assinatura cruzada Sectigo

```
CA Certificate
  Certificate Serial Number (hex): 00A024FDF4BA665C785CE4A020483858B7
  Issuer:
    cn=AAA Certificate Services
  Subject:
    cn=EM DV TLS CA - G3B
  Associated Trustpoints: <NAME-OR-Trustpool>
```

Ambos os formulários SubCA têm o mesmo assunto, mas emissores e séries diferentes. Corresponder o emitente e o número de série completos ao inventário; o preenchimento inicial de 00 pode ser diferente. Registre os Pontos de Confiança Associados para localizar o ponto de confiança ou pool proprietário. A raiz mostrada é o contexto da cadeia; não é uma das oito chaves de emissão comprometidas.

Mantenha disponíveis um método de acesso para recuperação e um pacote de substituição aprovado. Use o procedimento de backup de certificado/chave aprovado quando necessário. Fazer backup da configuração; esta cópia sozinha não é um backup de chave privada:

<#root>

```
copy running-config <BACKUP-CONFIG-URL>
```

Substitua os espaços reservados para suporte angular por valores específicos de dispositivos aprovados. Use um sistema de arquivos mostrado pelo comando show file systems, como flash: ou bootflash:.

2. Revisar Caminhos de Confiança

Remover SubCAs afetadas diretamente confiáveis

Remova as SubCAs afetadas diretamente confiáveis dos pontos de confiança e dos pacotes de pool confiável baixados. Não confie nas configurações de revogação para substituir a confiança direta em uma autoridade de certificação comprometida.

Remoção opcional de CA raiz

A remoção da CA raiz é uma recomendação opcional para proteção adicional. Uma raiz necessária pode permanecer confiável quando as verificações de CRL/OCSP do serviço real obtêm o status atual, avaliam a SubCA afetada sob um pai confiável, rejeitam cadeias mais longas originais afetadas, assinadas cruzadas e aplicáveis e falham na validação se nenhum dos métodos configurados fornecer o status utilizável. Sob essas condições verificadas, a verificação de revogação protege contra os emissores comprometidos identificados sem excluir a raiz.

Considere remover âncoras de raiz/confiança desnecessárias para reduzir a dependência de serviços de revogação. Avalie primeiro as dependências do serviço: a remoção dos serviços de certificado AAA pode interromper cadeias legítimas não relacionadas. Aborde os caminhos Mudhra e AAA. Excluir apenas uma SubCA armazenada em cache não bloqueia uma cópia fornecida pelo mesmo nível por meio de um pai confiável restante.

Remover um ponto de confiança selecionado

Para um ponto confiável configurado pelo administrador selecionado para remoção:

<#root>

```
configure terminal no crypto pki trustpoint <TRUSTPOINT-NAME> end
```

Revise a confirmação antes de aceitá-la. A remoção do ponto de confiança destrói seus certificados associados. Se uma identidade de dispositivo precisar de substituição, obtenha um certificado de substituição correspondente à chave do dispositivo e atualize sua associação de serviço usando o procedimento de registro de serviço. Instalar um novo certificado CA sozinho não substitui a identidade do dispositivo.

Para entradas de pool confiável baixadas, use o procedimento de substituição de pacote. Âncoras integradas ou gerenciadas por recursos exigem a atualização do produto suportado ou a orientação do Cisco TAC.

3. Atualize o Trustpool baixado, se necessário

Siga estas etapas quando um pacote baixado precisar ser substituído. Um pai/raiz necessário pode permanecer confiável sob as condições de revogação verificadas na Etapa 2.

3.1 Verifique se um pacote baixado está instalado e em uso

<#root>

```
show running-config | section crypto pki certificate pool show crypto pki trustpool verbose show crypto
```

Procure entradas de pacote no pool de certificados crypto pki e registros CA marcados como Trustpool: Baixado. Os nomes de arquivo do pacote podem ser diferentes de ios.p7b ou ios_core.p7b. Um arquivo armazenado ou URL de atualização configurada sozinha não prova que seus certificados estão instalados ou usados por um serviço. Confirme se o serviço usa o pool confiável e compare seus registros CA com o inventário afetado. Se não houver CAs descarregadas instaladas, ignore a limpeza e a substituição; avaliam outras fontes de confiança.

3.2 Limpar o pool confiável baixado

Mantenha o acesso à recuperação e um pacote de recuperação aprovado disponível antes da limpeza. O download posterior poderá falhar se a transferência depender da confiança que está sendo removida. Plano para interrupção de serviços dependentes.

<#root>

```
configure terminal crypto pki trustpool clean end
```

```
show crypto pki trustpool verbose
```

Confirme se os registros de CA baixados foram removidos. A limpeza remove todos os certificados de pool confiável baixados e seus arquivos de pacote gerenciados; CAs incorporados e pontos de confiança separados permanecem. Não salve até que a substituição e as verificações de serviço tenham êxito.

3.3 Obter e instalar o pacote de substituição aprovado

Obtenha um pacote aprovado e assinado pela Cisco. Selecione ios.p7b ou ios_core.p7b para os serviços necessários e confirme se ele exclui os certificados afetados e as âncoras de confiança indesejadas identificadas acima. Os pacotes herdados verificados em 31 de outubro de 2026 contêm CA raiz emSign - G1 em ios.p7b, mas nem Mudhra nem CAs de serviços de certificado AAA em ios_core.p7b. O núcleo tem um conjunto de confiança menor: verifique as dependências do serviço antes de alternar e verifique o conteúdo do pacote que você instala. Prepare-o fora do armazenamento de pool de confiança gerenciado usando transferência HTTPS ou SCP aprovada.

Pacote completo de CA da Cisco: ios.p7b

Pacote principal de CA da Cisco: ios_core.p7b

<#root>

```
show file systems copy <APPROVED-BUNDLE-SOURCE-URL> <STAGED-BUNDLE-URL> configure terminal crypto pki tr
```

Por exemplo, a URL preparada pode ser flash:approved-ios.p7b. Se a importação falhar, restaure um pacote aprovado antes de salvar. Verifique as autoridades de certificação desejadas e as conexões necessárias. A limpeza não é uma lista de negação de certificado: confirme os pontos de confiança restantes, as CAs internas e os caminhos alternativos rejeitam as cadeias afetadas por meio de revogação forçada ou remoção do caminho de confiança.

4. Configurar Validação e Política de Atualização

Antes de fazer alterações, registre a política de pool confiável existente, as políticas de ponto confiável afetadas, as associações de mapa de certificado e atualize as URLs para que possam ser restauradas, se necessário.

Para pontos de confiança configurados relevantes:

<#root>

```
configure terminal crypto pki trustpoint <VALIDATION-TRUSTPOINT> revocation-check crl ocsp exit end
```

Para serviços que usam a política trustpool:

<#root>

```
configure terminal crypto pki trustpool policy chain-validation revocation-check crl ocsp exit end show
```

Verifique se a política de pool confiável exibida continua a validação para a raiz e lista o ocsp crl. O dispositivo tenta primeiro a CRL e tenta o OCSP quando a recuperação da CRL não está disponível. Um resultado revogado falha na validação quando o certificado afetado é avaliado. Não adicione nenhum quando a verificação de revogação bem-sucedida for necessária.

Verifique a hora correta, os endpoints de status que podem ser acessados e publicados pela CA, os formatos de resposta aceitos e a ausência de exceções aplicáveis de cancelamento de revogação. O status das SubCAs afetadas deve ser avaliado sob um pai confiável. A confiança direta nessa SubCA pode interromper a validação antes que seu pai seja verificado. Verifique se o serviço real obtém o status atual utilizável e rejeita as cadeias afetadas. Se o acesso ao servidor de status e o comportamento de rejeição não puderem ser verificados, não trate a configuração sozinha como uma proteção confirmada; remova os caminhos de confiança relevantes quando exigido pelo seu plano de mitigação. Não adicione nenhum para ignorar o status indisponível.

Atualizar CRLs em cache antes de verificar a proteção

Uma CRL utilizável já existente no cache/banco de dados local pode ser reutilizada mesmo depois que a CA publicar uma CRL mais recente. Verifique a acessibilidade do servidor de status e limpe as CRLs antigas antes de validar a proteção:

<#root>

```
show crypto pki crls clear crypto pki crl show crypto pki crls
```

O comando clear remove CRLs locais para todos os pontos de confiança; ele não faz download de substituições. Confirme se as entradas antigas foram removidas e inicie uma nova conexão ou validação de certificado no serviço afetado. Execute show crypto pki crls novamente e verifique cada emissor relevante, LastUpdate, NextUpdate e ponto de distribuição em relação à publicação atual das autoridades de certificação. Inclua a CRL de emissores pai que cobre a subCA afetada, não apenas a CRL de emissor de certificados de identificação. Confirmar se as cadeias afetadas foram rejeitadas. A limpeza pode afetar temporariamente novas conexões enquanto os dados de status são buscados; reter validação de fail-closed.

Revisar a fonte de atualização do pacote

Para dispositivos conectados, configure opcionalmente a origem aprovada de atualização de pacote orientada por expiração:

<#root>

```
configure terminal crypto pki trustpool policy cabundle url <APPROVED-REFRESH-BUNDLE-URL> exit end show
```

Revise todas as origens de pacotes configuradas. A atualização orientada por expiração não substitui uma atualização de segurança imediata e não deve restaurar um caminho de confiança indesejado.

Filtro de mapa de certificado opcional: cobertura e limitação

Um mapa de certificado do Cisco IOS XE (mapa de certificado) corresponde aos atributos do certificado, como o nome do emissor. Como medida adicional, o filtro pode ajudar a rejeitar certificados de ID (folha) emitidos diretamente pelas oito CAs listadas. Revise a diretiva de certificado de correspondência existente dos pontos confiáveis antes de aplicá-la.

O comportamento foi testado em 29 de outubro de 2026 usando identidades de laboratório sob EM DV TLS CA - G3B em dispositivos experimentais de laboratório. Na validação do certificado de pares PKI, o filtro rejeitou uma identidade diretamente emitida, mas não bloqueou uma identidade emitida através de uma subautoridade de certificação filha adicional; um emissor legítimo não listado foi aprovado. A cobertura comportamental usou um emissor afetado, com revogação desabilitada apenas em pontos confiáveis de laboratório temporários para isolar o filtro. Handshakes de aplicativo e outras versões não foram validados com este filtro; testar o serviço real antes de confiar nele.

<#root>

```
configure terminal crypto pki certificate map EMSIGN-ISSUER-FILTER 10 issuer-name nc cn=EM DV TLS CA - G
```

Aqui, nc significa "não contém". Mantenha todas as oito condições negativas de nome do emissor na mesma entrada, sequência 10: todos devem corresponder para que o certificado passe neste filtro. Um emissor direto correspondente a qualquer nome listado falha no filtro.

O Cisco IOS XE pode exibir entradas normalizadas, por exemplo nome-emissor nc cn = em dv tls ca - g3b. Este formato de minúsculas e espaçamento estava presente no teste comportamental. Confirme o mapa e sua associação ao ponto de confiança de validação realmente usado pelo serviço:

<#root>

```
show running-config | section crypto pki certificate map show running-config | section crypto pki trustp
```

O filtro não fornece uma lista de negações de CA em toda a cadeia. Por exemplo:

```
Trusted root CA
  +-- Affected SubCA
       +-- New child SubCA
            +-- ID (leaf) certificate
```

O emissor de certificados de ID é a nova SubCA filha, portanto, seu filtro de nome do emissor não identifica a CA afetada mais acima na cadeia. Outras verificações, incluindo restrições CA e revogação, ainda se aplicam. Use este filtro apenas como proteção adicional juntamente com a validação de revogação e os procedimentos opcionais de remoção de raiz neste guia. Testar certificados filho-subCA e legítimos emitidos diretamente com o serviço real.

Reversão da Etapa 4

Restaure os métodos de revogação gravados, as configurações de validação de cadeia e as associações de mapa de certificado. Remova os URLs de atualização adicionados por este procedimento e restaure os URLs anteriores que foram alterados. Este exemplo remove apenas o URL de atualização adicionado e a associação de filtro; ele não restaura as outras configurações de diretiva:

<#root>

```
configure terminal crypto pki trustpool policy no cabundle url <ADDED-REFRESH-BUNDLE-URL> exit

crypto pki trustpoint <VALIDATION-TRUSTPOINT> no match certificate EMSIGN-ISSUER-FILTER exit end
```

Execute essas remoções apenas onde a URL e a associação foram adicionadas por este procedimento. Se uma associação de mapa de certificado anterior tiver sido substituída, restaure-a. Remova um mapa recém-criado somente depois de confirmar que nenhuma outra configuração faz referência a ele.

Use a política no crypto pki trustpool somente quando a redefinição para padrões for o resultado pretendido e aprovado. Essa redefinição ampla limpa os URLs de atualização configurados e redefine a verificação de revogação para nenhum; ele não restaura a política personalizada anterior. A reversão de política não restaura certificados excluídos, reverte o pacote instalado ou restaura CRLs limpas. Verifique novamente os serviços necessários e a rejeição da cadeia afetada antes de salvar.

5. Verificar Proteção e Salvar

- Confirme se as cadeias originais e com assinatura cruzada afetadas foram rejeitadas, incluindo uma intermediária fornecida pelo mesmo nível. Quando cadeias mais longas forem relevantes, verifique a rejeição quando a CA afetada estiver mais alta na cadeia.
- Confirme se as conexões legítimas necessárias ainda funcionam e se qualquer identidade de substituição está vinculada ao serviço pretendido.
- Verifique o comportamento quando os dados de revogação não estiverem disponíveis. As sessões TLS/IPsec existentes não são automaticamente comprovadas e revalidadas por uma alteração de política; use o procedimento de reconexão suportada pelo serviço quando necessário.

Após o êxito das verificações:

<#root>

```
show crypto pki certificates verbose show crypto pki trustpool policy write memory
```

Verifique a persistência após o próximo recarregamento planejado e, quando aplicável, no dispositivo de standby. Se os resultados forem diferentes da diretiva de confiança esperada, retenha os logs e entre em contato com o TAC da Cisco antes de considerar as alterações de confiança verificadas.

Leitura Adicional

[Gerenciamento de pool confiável PKI do Cisco IOS XE]

[Cisco: Configurar certificados CA assinados com PKI do Cisco IOS XE]

[Cisco: Cache de CRL e verificação de revogação]

Guia de Confiança de CA de GuestShell do Cisco IOS XE

Passo 1: Auditando Estado de Implantação do GuestShell do Dispositivo

A correção é necessária apenas em sistemas Cisco IOS XE em que o GuestShell esteja instalado e no estado RUNNING ou DEPLOYED. Se o GuestShell estiver no estado DEPLOYED, ele deverá primeiro ser habilitado com o comando 'guestshell enable' antes de executar comandos de correção. Se show app-hosting list indicar 'Nenhum aplicativo encontrado' (GuestShell não está implantado ou habilitado), nenhuma ação será necessária no GuestShell.

A. GuestShell no estado DEPLOYED (Ação necessária: Deve Habilitar Primeiro)

Quando show app-hosting list relata o GuestShell no estado DEPLOYED, o armazenamento do contêiner do GuestShell existe, mas o contêiner é interrompido. Você deve executar 'guestshell enable' antes de entrar no bash (e, opcionalmente, 'guestshell disable' após concluir a correção se estiver retornando a um estado parado):

<#root>

```
Router#

show app-hosting list

App id                                   State
------------------------------------------------------------
guestshell                               DEPLOYED
```

B. GuestShell no estado RUNNING (Ação necessária: Continuar Diretamente)

Quando show app-hosting list relata o GuestShell no estado RUNNING, o GuestShell está em execução ativa e você pode prosseguir diretamente para o bash:

<#root>

```
Router#

show app-hosting list

App id                                   State
---------------------------------------------------------
guestshell                               RUNNING
```

B. GuestShell Não Habilitado/Não Implantado (Nenhuma Ação Necessária)

Se show app-hosting list indicar Nenhum aplicativo encontrado, o GuestShell não está instalado ou habilitado no sistema, e nenhuma ação adicional é necessária:

<#root>

```
Router#

show app-hosting list

No App found
```

Passo 2: Como acessar o GuestShell e aplicar a confiança da CA

Execute estes comandos a partir do prompt EXEC privilegiado ('enable') do Cisco IOS XE. Se o GuestShell estiver no estado IMPLANTADO, habilite-o primeiro. Em seguida, insira o shell bash, transfira para a raiz e configure a lista de bloqueio CA usando a seleção de pasta dinâmica para garantir a compatibilidade em todas as versões do Cisco IOS XE:

<#root>

```
! 1. If GuestShell is in DEPLOYED state, enable it first:
Router#

guestshell enable


! 2. Enter GuestShell bash shell:
Router#

guestshell run bash
```

```
! 3. Escalate to root user inside GuestShell:
[guestshell@guestshell ~]$

sudo -s


! 4. Prepare the ca-trust blocklist directory (compatible with 17.15.x and 17.18.x):
d=/etc/pki/ca-trust/source/blocklist
[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist
mkdir -p "$d"
```

Certificados Mudhra comprometidos

Execute os comandos trust extract para extrair cada certificado do eMudhra comprometido diretamente no diretório de lista de bloqueio do ca-trust, seguido pela reconstrução do armazenamento confiável do sistema:

```
trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-%20G3;type=cert' \
  "$d/emSign_ECC_Root_CA_-_G3.pem"

trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=Comodo%20AAA%20Services%20root;type=cert' \
  "$d/Comodo_AAA_Services_root.pem"

trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-%20C3;type=cert' \
  "$d/emSign_ECC_Root_CA_-_C3.pem"

trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=emSign%20Root%20CA%20-%20C1;type=cert' \
  "$d/emSign_Root_CA_-_C1.pem"

update-ca-trust extract
```

Passo 3: Verificação de certificados desconfiáveis no GuestShell

Verifique se os quatro certificados extraídos aparecem na política de desconfiança/lista de bloqueio do sistema e são excluídos das âncoras de confiança ativas usando o comando de verificação abaixo. O comando confirma que os certificados estão registrados na política de lista de bloqueio.

```
###Verify with below command
[guestshell@guestshell ~]$ trust list --filter=trust-policy --purpose=server-auth | grep -E -A3 'emSign
    label: AAA Certificate Services
    trust: distrusted
    category: authority
```

```
--
    label: emSign ECC Root CA - C3
    trust: distrusted
    category: authority

--
    label: emSign ECC Root CA - G3
    trust: distrusted
    category: authority

--
    label: emSign Root CA - C1
    trust: distrusted
    category: authority

--
    label: emSign Root CA - G1
    trust: anchor
    category: authority

Output will vary based on CentOS Stream version
###Verify CentOS Stream Version
[guestshell@guestshell ~]$ cat /etc/redhat-release
CentOS Stream release 8

OS                          CentOS Stream 8       CentOS Stream 9
Directory                   blacklist only        blocklist
Result shown                 trust: blacklisted    trust: distrusted
```

Passo 4: Persistência de estado e ciclo de vida do contêiner

Observação sobre a persistência do contêiner: Essas modificações de desconfiança de certificado persistem nas operações 'guestshell enable' e 'guestshell disable' e reinicializações de dispositivo porque /etc/pki/ca-trust reside no armazenamento de contêiner persistente.

Retornando ao estado IMPLANTADO (se aplicável): Se o GuestShell estava originalmente no estado DEPLOYED e habilitado exclusivamente para executar esse procedimento de desconfiança, retorne o GuestShell ao seu estado anterior parado, saindo do bash e executando 'guestshell disable' no prompt EXEC privilegiado do IOS:

<#root>

```
[root@guestshell ~]#

exit

[guestshell@guestshell ~]$

exit

Router#
```

```
guestshell disable
```

Considerações importantes sobre o ciclo de vida: Se o GuestShell for completamente destruído com 'guestshell destroy', o sistema de arquivos de contêiner será removido. Se o GuestShell for reabilitado posteriormente, o contêiner será recriado a partir da imagem base do sistema e essas etapas de correção de desconfiança deverão ser reaplicadas.

Passo 5: Procedimento de reversão (restaurando a confiança da autoridade de certificação)

Para reverter a configuração de desconfiança e restaurar a confiança de CA padrão em qualquer versão do Cisco IOS XE, selecione dinamicamente o diretório de lista de bloqueio ativo ($d), remova especificamente os quatro arquivos de certificado adicionados por este procedimento (incluindo a raiz de Comodo AAA Services) e recrie o armazenamento de confiança:

<#root>

```
! Escalate to root user inside GuestShell:
[guestshell@guestshell ~]$

sudo -s


d=/etc/pki/ca-trust/source/blocklist
[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist

! Remove only the four certificate files added during remediation:
rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" \
      "$d/emSign_ECC_Root_CA_-_C3.pem" "$d/emSign_Root_CA_-_C1.pem"

! Rebuild the system CA trust store:
update-ca-trust extract
```

Verifique se o diretório da lista de bloqueio não contém mais os arquivos removidos:

<#root>

```
[root@guestshell ~]#

ls -l "$d"/

total 0
```

Confirmar restauração da confiança da autoridade de certificação: Verifique se todos os cinco certificados retornaram às âncoras de confiança ativas executando novamente o comando de

verificação da Etapa 3 (todas as entradas reportam confiança:):

<#root>

```
[root@guestshell ~]#

trust list --filter=trust-policy --purpose=server-auth | grep -E -A3 'emSign|AAA'

    trust: anchor
    trust: anchor
    trust: anchor
    trust: anchor
    trust: anchor
```

Exemplo de Transcrição de Execução de Ponta a Ponta

A transcrição ilustra uma auditoria completa e bem-sucedida do GuestShell, correção e sessão de verificação em um dispositivo Cisco IOS XE:

<#root>

```
Router#

guestshell run bash

[guestshell@guestshell ~]$ sudo -s
bash-4.4#

d=/etc/pki/ca-trust/source/blocklist

bash-4.4#

[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist

bash-4.4#

mkdir -p "$d"

bash-4.4#

trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-

bash-4.4#

trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=Comodo%20AAA%20Services%20ro

bash-4.4#
```

```
trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-

bash-4.4#

trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=emSign%20Root%20CA%20-%20C1;

bash-4.4#

update-ca-trust extract

bash-4.4#

trust list --filter=trust-policy --purpose=server-auth | grep -E -A3 'emSign|AAA'

    label: emSign ECC Root CA - G3
    trust: blacklisted
    category: authority

--
    label: AAA Certificate Services
    trust: blacklisted
    category: authority

--
    label: emSign ECC Root CA - C3
    trust: blacklisted
    category: authority

--
    label: emSign Root CA - C1
    trust: blacklisted
    category: authority

--
    label: emSign Root CA - G1
    trust: anchor
    category: authority

bash-4.4#

cat /etc/redhat-release

CentOS Stream release 8
bash-4.4#

d=/etc/pki/ca-trust/source/blocklist

bash-4.4#

[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist

bash-4.4#

rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" \ >       "$d/emSign_ECC_Root_C
```

```
bash-4.4#
bash-4.4#

update-ca-trust extract

bash-4.4#

ls -l "$d"/

total 0
```

Matriz de resumo de comandos

Tarefa operacional	
Auditoria de Estado de GuestShell	`show app-hosting list`
Habilitar GuestShell (se IMPLANTADO)	`guestshell enable`
Inserir Bash de GuestShell	`guestshell run bash`
Alternar para Usuário Raiz	`sudo -s`
Preparar diretório de lista de bloqueio	`d=/etc/pki/ca-trust/source/blocklist; [ -d "$d" ] || d=/etc/pki/ca-trust/source/blac`
Extrair ACs para Lista de Bloqueio	`trust extract --overwrite --format=pem-bundle ... (x4 CAs)`

Recriar Repositório Confiável de Autoridade de Certificação	`update-ca-trust extract`
Verificar a política de confiança	`trust list --filter=trust-policy --purpose=server-auth`
Restaurar estado IMPLANTADO (opcional)	`guestshell disable`
Reverter/Restaurar Confiança	`rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" "$d/emSign_`

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.