

Identity Services Engine - Desconfiança de Emergência da Raiz de Mudhra e Autoridades de Certificação Intermediárias

Contents

Propósito

Veja abaixo as orientações sobre o Identity Services Engine e o ISE PIC (Passive Identity Connector) para a desconfiança de emergência da raiz de Mudhra e das autoridades de certificação intermediárias. A configuração do Identity Service Engine não inclui as autoridades de certificado intermediário e raiz de Mudhra afetadas por padrão no Repositório Confiável, mas a configuração do ISE deve ser revisada para garantir que não estejam em uso por meio da configuração pós-instalação.

RESSALVA

Este artigo destina-se apenas a auxiliar na revisão da configuração do ISE para verificar a presença das autoridades de certificação afetadas. O Identity Services Engine como um todo ainda está sendo investigado e pode exigir mais atualizações de configuração ou software no futuro. Este artigo será atualizado junto com o Security Advisory localizado em <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-emudhra-info-ScS22A1r>.

Certificados do sistema

Navegue até Administration -> System -> Certificates -> System Certificates, selecione cada certificado atribuído aos nós 1 por 1 e selecione view. [1]



Certificate Hierarchy

Certificate Services Root CA - zer0k-ise1

Certificate Services Node CA - zer0k-ise1

Certificate Services Endpoint Sub CA - zer0k-ise1

zer0k-ise1.zer0k.org



zer0k-ise1.zer0k.org

Issued By : Certificate Services Endpoint Sub CA - zer0k-ise1

Expires : Mon, 4 Aug 2031 10:52:08 EDT

Certificate status is good

Details

Issued To

Common Name (CN) zer0k-ise1.zer0k.org

Certifique-se de que a autoridade de certificação ou os certificados emissores afetados não estejam na Hierarquia de Certificados. Se estiverem em uso, comece a executar etapas para migrar esse serviço para uma nova autoridade de certificação.

Certificados confiáveis

Navegue até Administração -> Sistema -> Certificados -> Certificados confiáveis e examine a lista de certificados raiz e intermediários instalados. Se você encontrar uma ou mais autoridades de certificação afetadas na lista Confiável, anote a coluna "Confiável para" e execute a seguinte ação para cada tipo [2]:

☐	Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From
		Endpoints				
☐	Cisco Root CA 2048	Endpoints Infrastructure	5F F8 7B 28 2...	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004
☐	Cisco Root CA 2099	Cisco Services	01 9A 33 58 7...	Cisco Root CA 2099	Cisco Root CA 2099	Tue, 9 Aug 2016
☐	Cisco Root CA M1	Infrastructure Cisco Services Endpoints AdminAuth NativeIPSec	2E D2 0E 73 4...	Cisco Root CA M1	Cisco Root CA M1	Tue, 18 Nov 20...

- Cisco Services - A Cisco não usa Mudhra para nenhum serviço, se esta for a única entrada que o certificado pode ser excluído.
- Infraestrutura - verifique se a função Endpoints e/ou AdminAuth não é necessária, verifique se nenhum certificado da CA ou dos Emissores está sendo usado em Certificados do Sistema
- Endpoints - Verifique se os endpoints estão se autenticando e exigindo a cadeia comprometida; se não tiver certeza se os endpoints estão usando a CA ou os Emissores, desabilite a opção "Trust for client authentication and Syslog" e monitore os logs e relatórios dinâmicos para verificar se há falhas de autenticação do cliente.
- AdminAuth - Emita novos certificados para seus administradores, como uma opção rápida, a Autenticação Admin pode ser movida de volta para o login baseado em senha enquanto novos certificados estão sendo emitidos.
- NativeIPSec - Se estiver usando o recurso Native IPSec, migre os clientes IPSec para uma nova CA

Outros serviços

As configurações de serviço a seguir devem ser analisadas para garantir que a exclusão de qualquer certificado de confiabilidade afetado não afete a função do sistema. Se estiverem em uso nesses serviços, eles deverão ser reconfigurados para usar novos certificados antes que os certificados confiáveis sejam excluídos.

LDAP

Navegue até Administração -> Gerenciamento de identidades -> Fontes de identidade externas -> LDAP. Em cada entrada LDAP, clique na guia Connection (Conexão). Se a autenticação segura estiver habilitada, verifique a cadeia de configurações "LDAP Server Root CA" (CA raiz do servidor LDAP) e "Issuer CA of ISE Certificates" (CA emissora de certificados ISE). [3]

LDAP Server Root CA VeriSign Class 3 Public Pri... ⓘ

LDAP Server Root CA VeriSign Class 3 Public Pri... ⓘ

Issuer CA of ISE Certificates DigiCert Global Root CA ⓘ

Issuer CA of ISE Certificates Select if required (optional) ⓘ

SYSLOG

Navegue até Administração -> Sistema -> Log -> Destinos de Log Remoto, exiba cada Servidor SYSLOG Seguro configurado para o certificado Raiz Confiável configurado, se um dos certificados CA afetados estiver em uso, verifique a cadeia no servidor SYSLOG e emita novamente e confie em uma nova raiz, se necessário. [4]

Select CA Certificate

Cisco Root CA M1



Note: The CA certificates should be imported into the Certificate Store, enabled, and trusted for client authentication prior to configuring Secure Syslog. Ensure that a local certificate signed by the selected CA exists on the primary and secondary nodes.

If a local certificate signed by the selected CA does not exist, the self-signed local certificate will be used.

Ignore Server Certificate validation

☐

DTLS RADIUS

É possível definir opcionalmente a "CA do emissor de certificados ISE para CoA" em cada dispositivo de rede em Administração -> Recursos de rede -> Dispositivos de rede. Essa configuração é usada apenas para selecionar o certificado de cliente que o ISE usará para emitir um CoA para um dispositivo de rede configurado para DTLS. O certificado será exibido na página Certificados do sistema no ISE para o nó, portanto, essa configuração só precisará ser verificada para cada dispositivo de rede configurado se um problema de certificado de um dos certificados Mudhra for emitido para um nó do ISE.

[1] [Gerenciamento de certificados no ISE](#)

[2] [Configurações de Certificado Confiável do ISE](#)

[3] [Configuração LDAP segura do ISE](#)

[4] [Configurar o destino de registro remoto do Syslog seguro](#)

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.