

Identity Services Engine: desconfianza de emergencia de las autoridades de certificados raíz e intermedias de eMudhra

Contenido

Propósito

A continuación se incluye la guía sobre Identity Services Engine e ISE PIC (Conector de identidad pasivo) para la desconfianza de emergencia de las autoridades de certificados raíz e intermedias de eMudhra. La configuración de Identity Service Engine no incluye de forma predeterminada las autoridades de certificados raíz e intermedias de eMudhra afectadas en el almacén de confianza, pero debe revisarse la configuración de ISE para asegurarse de que no se está utilizando mediante la configuración posterior a la instalación.

DESCARGO

Este artículo solo pretende ayudar a revisar la configuración de ISE para detectar la presencia de las autoridades de certificados afectadas. Identity Services Engine en su conjunto se está investigando y es posible que necesite más actualizaciones de configuración o software en el futuro. Este artículo se actualizará junto con el aviso de seguridad que se encuentra en <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-emudhra-info-ScS22A1r>.

Certificados del sistema

Vaya a Administration (Administración) -> System (Sistema) -> Certificates (Certificados) -> System Certificates (Certificados del sistema), seleccione cada certificado asignado a los nodos 1 por 1 y seleccione view (Ver). [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

Asegúrese de que la CA o los certificados de emisión afectados no estén en la jerarquía de certificados. Si están en uso, comience a tomar medidas para migrar ese servicio a una nueva entidad de certificación.

Certificados de confianza

Vaya a Administration (Administración) -> System (Sistema) -> Certificates (Certificados) -> Trusted Certificates (Certificados fiables) y revise la lista de certificados raíz e intermedios instalados. Si encuentra una o más de las CA afectadas en la lista de confianza, observe la columna "De confianza para" y realice la siguiente acción 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...

- Servicios de Cisco: Cisco no utiliza eMudhra para ningún servicio. Si esta es la única entrada en la que se puede eliminar el certificado.
- Infraestructura: verifique que no se requiera el rol de extremos y/o AdminAuth; verifique que no se esté utilizando ningún certificado de la CA o de los emisores en Certificados del sistema
- Terminales: verifique si los terminales se están autenticando y requieren la cadena comprometida; si no está seguro de si los terminales están usando la CA o los emisores, desactive la opción "Confiar en la autenticación del cliente y Syslog" y supervise los registros en directo y los informes de errores de autenticación del cliente.
- AdminAuth - Emita nuevos certificados para sus administradores, como una opción rápida Admin Authentication puede ser movido de nuevo al login basado en contraseña mientras se emiten nuevos certificados.
- NativeIPSec: si utiliza la función Native IPsec, migre los clientes IPsec a una nueva CA

Otros servicios

Se deben revisar las siguientes configuraciones de servicio para asegurarse de que la eliminación de los certificados de confianza afectados no afecte al funcionamiento del sistema. Si están en uso para estos servicios, los servicios deben volver a configurarse para utilizar nuevos certificados antes de eliminar los certificados de confianza.

LDAP

Vaya a Administration > Identity Management > External Identity Sources > LDAP. En cada entrada de LDAP, haga clic en la ficha Connection (Conexión). Si la autenticación segura está activada, compruebe la cadena de los parámetros "LDAP Server Root CA" (CA raíz del servidor LDAP) y "Issuer CA of ISE Certificates" (CA del emisor 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

Vaya a Administración -> Sistema -> Registro -> Destinos de registro remoto, vea cada servidor SYSLOG seguro configurado para el certificado raíz de confianza configurado, si uno de los certificados de CA afectados está en uso, verifique la cadena en el servidor SYSLOG y vuelva a emitir y confíe en una nueva raíz si es necesario. [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

☐

RADIUS DTLS

Es posible establecer opcionalmente la "CA de emisor de certificados ISE para CoA" en cada dispositivo de red en Administration > Network Resources > Network Devices . Esta configuración solo se usa para seleccionar el certificado de cliente que ISE usará para emitir una CoA a un dispositivo de red configurado para DTLS. El certificado aparecerá en la página Certificados del sistema de ISE para el nodo, por lo que solo será necesario comprobar esta configuración para cada dispositivo de red configurado si se emite un certificado de uno de los certificados de eMudhra a un nodo de ISE.

[1] [Administración de certificados en ISE](#)

[2] [Configuración de certificados de confianza de ISE](#)

[3] [Configuración de ISE Secure LDAP](#)

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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).