

Identity Services Engine - Emergenza diffidenza verso le autorità radice e intermedie dei certificati eMudhra

Sommario

Scopo

Di seguito sono riportate le linee guida su Identity Services Engine e ISE PIC (Passive Identity Connector) per la sfiducia in caso di emergenza delle autorità di certificazione principali e intermedie di Mudhra. Per impostazione predefinita, la configurazione di Identity Service Engine non include le Autorità di certificazione principali e intermedie di eMudhra interessate nell'archivio attendibile, ma è necessario esaminare la configurazione ISE per assicurarsi che non siano in uso tramite la configurazione post-installazione.

ESCLUSIONE DI RESPONSABILITÀ

Questo articolo ha lo scopo di fornire assistenza nell'analisi della configurazione ISE per rilevare la presenza delle autorità di certificazione interessate. Identity Services Engine nel suo complesso è ancora in fase di analisi e potrebbe richiedere ulteriori aggiornamenti della configurazione o del software in futuro. Questo articolo verrà aggiornato con l'advisory della sicurezza disponibile all'indirizzo <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-emudhra-info-ScS22A1r>.

Certificati di sistema

Selezionare Amministrazione -> Sistema -> Certificati -> Certificati di sistema, selezionare ogni certificato assegnato ai nodi 1 per 1 e scegliere Visualizza. [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

Verificare che la CA interessata o i certificati di emissione non siano nella gerarchia dei certificati. Se sono in uso, iniziare a eseguire la migrazione del servizio a una nuova autorità di certificazione.

Certificati attendibili

Selezionare Amministrazione -> Sistema -> Certificati -> Certificati attendibili ed esaminare l'elenco dei certificati principali e intermedi installati. Se nell'elenco delle CA attendibili sono presenti una o più CA interessate, annotare la colonna "Attendibile per" ed eseguire l'azione seguente per ogni 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 - Cisco non utilizza eMudhra per alcun servizio, se questa è l'unica voce in cui è possibile eliminare il certificato.
- Infrastruttura - Verificare che il ruolo Endpoint e/o AdminAuth non sia obbligatorio, verificare che nessun certificato della CA o degli emittenti sia utilizzato in Certificati di sistema
- Endpoint: verificare se gli endpoint eseguono l'autenticazione che richiede la catena compromessa. Se non si è certi che gli endpoint utilizzino la CA o gli emittenti, disabilitare l'opzione "Considera attendibili l'autenticazione del client e il syslog" e monitorare i registri attivi e i report per rilevare errori di autenticazione del client.
- AdminAuth: emette nuovi certificati per gli amministratori. L'opzione rapida Admin Authentication consente di tornare all'accesso basato su password durante l'emissione dei nuovi certificati.
- IPSec nativo: se si utilizza la funzionalità IPSec nativo, eseguire la migrazione dei client IPSec in una nuova CA

Altri servizi

Le seguenti configurazioni del servizio devono essere riviste per garantire che l'eliminazione dei certificati protetti interessati non influisca sul funzionamento del sistema. Se questi servizi sono in uso, è necessario riconfigurarli per l'utilizzo di nuovi certificati prima di eliminare i certificati protetti.

LDAP

Selezionare Amministrazione > Gestione identità > Origini identità esterne > LDAP. In ciascuna voce LDAP, fare clic sulla scheda Connessione. Se l'autenticazione protetta è abilitata, verificare la catena per le impostazioni "CA radice server LDAP" e "CA emittente dei certificati 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

Selezionare Amministrazione -> Sistema -> Registrazione -> Destinazioni di registrazione remota, visualizzare ciascun server SYSLOG protetto configurato per il certificato radice attendibile configurato. Se uno dei certificati CA interessati è in uso, verificare la catena sul server SYSLOG e, se necessario, emettere nuovamente e considerare attendibile una nuova radice. [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

Facoltativamente, è possibile impostare il valore "Issuer CA of ISE Certificates for CoA" in ciascun dispositivo di rete in Amministrazione (Administration) -> Risorse di rete (Network Resources) -> Dispositivi di rete (Network Devices). Questa impostazione viene utilizzata solo per selezionare il certificato client che ISE utilizzerà per rilasciare un CoA a un dispositivo di rete configurato per DTLS. Il certificato verrà visualizzato nella pagina Certificati di sistema in ISE per il nodo, quindi questa impostazione dovrà essere verificata per ciascun dispositivo di rete configurato solo se a un nodo ISE viene emesso un certificato emesso da uno dei certificati eMudhra.

[1] [Gestione certificati in ISE](#)

[2] [Impostazioni certificato protetto ISE](#)

[3] [Configurazione ISE Secure LDAP](#)

[4] [Configurazione della destinazione di registrazione remota Syslog sicura](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).