

身份服务引擎 — 紧急情况下不信任根证书颁发机构和中间证书颁发机构

目录

目的

以下是身份服务引擎和ISE PIC（被动身份连接器）指南，用于紧急不信任根和中间证书颁发机构。默认情况下，身份服务引擎配置不包括受信任库中的受影响的eMudhra根证书颁发机构和中间证书颁发机构，但应检查ISE配置以确保它们未通过安装后配置使用。

免责声明

本文仅用于帮助查看ISE配置是否存在受影响的证书颁发机构。整个身份服务引擎仍在调查中，将来可能需要进一步配置或软件更新。本文将在<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-emudhra-info-ScS22A1r>上与安全咨询一起进行更新。

系统证书

浏览到Administration -> System -> Certificates -> System Certificates，依次选择分配给节点1的每个证书并选择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

确保受影响的CA或颁发证书不在证书层次结构中。如果正在使用它们，则开始采取措施将该服务迁移到新的证书颁发机构。

受信任证书

浏览到Administration -> System -> Certificates -> Trusted Certificates并查看已安装的根证书和中间证书的列表。如果您在Trusted列表中找到一个或多个受影响的CA，请记下“Trusted For”列，并对每个类型[2]执行以下操作：

☐	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...

- 思科服务 — 思科不对任何服务使用eMudhra，如果这是可以删除证书的唯一条目。
- 基础设施 — 验证终端和/或管理员身份验证角色不是必需的，验证系统证书下未使用来自CA或颁发者的证书
- 终端 — 验证终端是否正在对需要受感染链进行身份验证，如果不确定终端是否正在使用CA或颁发者，请禁用“信任客户端身份验证和系统日志”选项，并监控实时日志和报告客户端身份验证失败。
- AdminAuth — 向您的管理员颁发新证书，因为在颁发新证书时，Admin Authentication可切换回基于密码的登录，这是快捷选项。
- NativeIPSec — 如果使用本地IPSec功能，请将IPSec客户端迁移到新的CA

其他服务

应检查以下服务配置，以确保删除任何受影响的受信任证书不会影响系统的功能。如果这些服务正在使用中，则应重新配置这些服务，以便在删除受信任证书之前使用新证书。

LDAP

浏览到Administration -> Identity Management -> External Identity Sources -> LDAP。在每个LDAP条目下，点击Connection选项卡，如果安全身份验证已启用，请验证“LDAP服务器根CA”和“ISE证书的颁发者CA”设置的链。[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)▼ ⓘ

系统日志

浏览到Administration -> System -> Logging -> Remote Logging Targets，查看已配置受信任根证书的每个已配置安全SYSLOG服务器，如果其中一个受影响的CA证书正在使用中，请验证SYSLOG服务器上的链，并根据需要重新颁发和信任新的根。[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

可以在管理(Administration)->网络资源(Network Resources)->网络设备(Network Devices)下的每个网络设备下选择性地设置“CoA的ISE证书的颁发者CA”(Issuer CA of ISE Certificates)。此设置仅用于选择ISE用来向配置为DTLS的网络设备颁发CoA的客户端证书。该证书将显示在ISE中节点的System Certificates页面上，因此，如果从eMudra证书之一颁发的证书颁发给ISE节点，则只需为每个配置的网络设备验证此设置。

[1] ISE [中的证书管理](#)

[2] ISE受[信任证书设置](#)

[3] ISE[安全LDAP配置](#)

[4]配置[安全系统日志远程日志记录目标](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。