

身份服務引擎 — 緊急不信任木德拉根和中間證書頒發機構

目錄

目的

以下是身份服務引擎和ISE PIC（被動身份聯結器）指南，用於緊急不信任根和中間證書頒發機構。預設情況下，身份服務引擎配置不包括受信任儲存中受影響的eMudra根證書頒發機構和中間證書頒發機構，但應檢查ISE配置，以確保它們未通過安裝後配置使用。

簡介

本文僅用於幫助檢視ISE配置是否存在受影響的證書頒發機構。整個身份服務引擎仍在調查中，將來可能需要進一步配置或軟體更新。本文將在<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-emudhra-info-ScS22A1r>上的安全諮詢部分進行更新。

系統憑證

瀏覽到Administration -> System -> Certificates -> System Certificates，依次選擇分配給節點1的每個證書，然後選擇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

確保受影響的CA或頒發證書不在證書層次結構中。如果正在使用它們，則開始採取措施將該服務遷移到新的證書頒發機構。

受信任的證書

瀏覽到Administration -> System -> Certificates -> Trusted Certificates，並檢視已安裝的根證書和中間證書的清單。如果您在「受信任」(Trusted)清單中找到一個或多個受影響的CA，請記下「信任對象」(Trusted For)列，並對每種型別[2]採取以下操作：

☐	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...

- 思科服務 — 思科不對任何服務使用互助，如果這是唯一可以刪除憑證的條目。
- 基礎架構 — 驗證是否不需要終端和/或AdminAuth角色，驗證系統證書下是否未使用來自CA或發行者的證書
- 終端 — 驗證終端是否正在對要求受危害的鏈進行身份驗證；如果不確定終端是否正在使用CA或頒發者，請禁用「信任客戶端身份驗證和系統日誌」選項，並監控即時日誌和報告客戶端身份驗證失敗。
- AdminAuth — 向您的管理員頒發新證書，因為在頒發新證書時，管理員身份驗證可以切換回基於密碼的登入，這是一個快速選項。
- NativeIPSec — 如果使用本地IPSec功能，請將IPSec客戶端遷移到新的CA

其他服務

應檢查以下服務配置，以確保刪除任何受影響的受信任證書不會影響系統的功能。如果正在使用這些服務，則應重新配置這些服務，以便在刪除受信任證書之前使用新證書。

LDAP

瀏覽到Administration -> Identity Management -> External Identity Sources -> LDAP。在每個LDAP條目下，按一下Connection（連線）頁籤，如果啟用Secure Authentication（安全身份驗證），則驗證「LDAP伺服器根CA」和「ISE證書的頒發者CA」設定的鏈。[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)  

系統日誌

瀏覽到Administration -> System -> Logging -> Remote Logging Targets，檢視已配置受信任根證書的每個已配置安全SYSLOG伺服器（如果其中一個受影響的CA證書正在使用中），驗證SYSLOG伺服器上的鏈，並根據需要重新頒發和信任新的根。[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 — > 網路資源 — > 網路裝置下的每個網路裝置下選擇性地設定「CoA的ISE證書的頒發者CA」。此設定僅用於選擇ISE將用於向配置為DTLS的網路裝置頒發CoA的客戶端證書。該證書將顯示在ISE中節點的「系統證書」(System Certificates)頁面上，因此，如果從eMudra證書之一頒發的證書頒發給ISE節點，則只需為每個配置的網路裝置驗證此設定。

[1] ISE [中的證書管理](#)

[2] ISE受 [信任證書設定](#)

[3] [ISE安全LDAP配置](#)

[4] 配置 [安全系統日誌遠端日誌記錄目標](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。