ISEでの証明書更新の設定

内容

概要 前提条件 要件 使用するコンポーネント 背景説明 設定 ISE 自己署名証明書の表示 証明書を変更する時期の特定 証明書署名要求の生成 証明書のインストール 警告システムの設定 確認 警告システムの確認 証明書変更の確認 証明書の確認 トラブルシュート 結論

概要

このドキュメントでは、Cisco Identity Services Engine(ISE)で証明書を更新するためのベスト プラクティスとプロアクティブな手順について説明します。 また、証明書の期限切れなどの差し 迫ったイベントについて管理者に警告できるように、アラームと通知を設定する方法についても 説明します。

注:このドキュメントは、証明書の診断ガイドではありません。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- X509 証明書
- Cisco ISE と証明書の設定

使用するコンポーネント

"このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。ネットワークが稼働中の場合は、コマンドの潜在的な影響について確実に理解しておく必要が あります」

- Cisco ISE リリース 3.0.0.458
- アプライアンスまたは VMware

背景説明

ISE 管理者は、いずれは ISE 証明書が期限切れになる状況を経験します。ISEサーバに期限切れ の証明書がある場合、期限切れの証明書を新しい有効な証明書で置き換えない限り、深刻な問題 が発生する可能性があります。

注:拡張認証プロトコル(EAP)に使用される証明書の有効期限が切れると、クライアントが ISE証明書を信頼しなくなるため、すべての認証が失敗する可能性があります。ISE管理証 明書が期限切れになると、リスクはさらに大きくなります。管理者はISEにログインできな くなり、分散導入は機能を停止して複製を行えなくなります。

ISE管理者は、古い証明書が期限切れになる前に、新しい有効な証明書をISEにインストールする 必要があります。このプロアクティブなアプローチにより、ダウンタイムを防止または最小限に 抑え、エンドユーザーへの影響を回避できます。新しくインストールされた証明書の期間が始ま ると、新しい証明書でEAP/Adminまたはその他の役割を有効にできます。

古い証明書が期限切れになる前にアラームを発生させ、新しい証明書のインストールを管理者に 通知するように ISE を設定できます。

注:このドキュメントでは、証明書の更新の影響を実証するために、自己署名証明書としてISE管理証明書を使用しますが、この方法は実稼働システムには推奨されません。EAPロールと管理者ロールの両方にCA証明書を使用することをお勧めします。

設定

ISE 自己署名証明書の表示

ISE をインストールすると、自己署名証明書が生成されます。自己署名証明書は、管理アクセス 、分散型展開内の通信(HTTPS)、およびユーザー認証(EAP)に使用されます。 実稼働システ ムでは、自己署名証明書ではなく CA 証明書を使用してください。

ヒント:追加情報については、『<u>Cisco Identity Services Engine Hardware Installation</u> <u>Guide, Release 3.0 』の「Certificate Management in Cisco ISE 」の項を参照してください</u>

ISE 証明書の形式は、プライバシー強化メール(PEM)または Distinguished Encoding Rules(DER)にする必要があります。

最初の自己署名証明書を表示するには、図のように、ISE GUI で [Administration] > [System] > [Certificates] > [System Certificates] に移動します。

Deployment	Licensing	С	ertificates	Logging	Maintenar	ice Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
Certificate Manageme	et	~	Frien	dly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date
System Certificates			✓ abtomar3	31						
Trusted Certificates OCSP Client Profile Certificate Signing Re	equests		OU+IS ice,CM mar.lo rvices - abto	E Messaging Serv Nabtomar31.abto cal#Certificate Se Endpoint Sub CA mar31#00001	ISE Messaging Service		abtomar31.abtomar.loc al	Certificate Services End point Sub CA - abtomar 31	Mon, 3 May 2021	Mon, 4 May 2026 🥥
Certificate Periodic C	Check Se	>	OU+C Syster abtom al#Cer Endpo mar31	ertificate Services m Certificate,CN= war31.abtomar.loc rtificate Services wint Sub CA - abto #00002	pxGrid		abtomar31.abtomar.loc al	Certificate Services End point Sub CA - abtomar 31	Mon, 3 May 2021	Mon, 4 May 2026 🧶
			Defaul I serve =SAM mar.lo	It self-signed sam er certificate - CN L_abtomar31.abto ical	SAML		SAML_abtomar31.abto mar.local	SAML_abtomar31.abto mar.local	Tue, 4 May 2021	Sun, 3 May 2026 🧶
			Defaul er cen	It self-signed serv tificate	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group 💿	abtomar31.abtomar.loc al	abtomar31.abtomar.loc al	Tue, 4 May 2021	Thu, 4 May 2023 🥥

証明書署名要求(CSR)を介して ISE にサーバー証明書をインストールし、Admin または EAP プロトコルに関して証明書を変更しても、自己署名サーバー証明書は残りますが、未使用のステ ータスになります。

注意:Admin プロトコルの変更の場合は、ISE サービスの再起動が必要です。これにより、数分のダウンタイムが発生します。EAP プロトコルの変更は、ISE サービスの再起動が トリガーされず、ダウンタイムが発生しません。

証明書を変更する時期の特定

インストールされた証明書がもうすぐ期限切れになるとします。証明書が期限切れになってから 更新するのと、証明書が期限切れになる前に変更するのとどちらが適切だと思いますか。証明書 の切り替えを計画し、切り替えによって発生するダウンタイムを管理する時間を確保するには、 有効期限が切れる前に証明書を変更する必要があります。

証明書はいつ変更する必要がありますか。開始日が古い証明書の失効日より前である新しい証明 書を取得します。この2つの日付の間の期間が移行期間です。

注意:Admin を有効にすると、ISE サーバーでサービスが再起動し、数分間のダウンタイムが発生します。

次の図は、間もなく期限切れになる証明書の情報を示しています。

	Default self-signed ser ver certificate	Admin, Portal, EAP	Default Portal Certificate Group ()	abtomar31.abtomar.loc al	abtomar31.abtomar.loc al	Tue, 4 May 2021	Wed, 5 May 2021 💔
0		Authentication, RADIUS DTLS					

証明書署名要求の生成

次の手順では、CSR を介して証明書を更新する方法を説明します。

1. ISE コンソールで [Administration] > [System] > [Certificates] > [Certificate Signing Requests] に移動して、[Generate Certificate Signing Request] をクリックします。 [Certificate Subject] テキスト フィールドに入力する必要がある最小限の情報は CN=ISEfqdn です。ここで、ISEfqdn は ISE の完全修飾ドメイン名(FQDN)です。O(組織)、OU(組 織単位)、C(国)などのフィールドをカンマで区切って [Certificate Subject] に追加します

o

Cloce 155			Administrati	oit - System			A commence of the bar
storent Usersite	etfores Loupe No	Humanos Ubgrade	Health Directo	Oackup & Restore	Agent Jooms	Settings	
w non-temperat	(and an international second						
when hardfulges	land the second second	City Insuity Insuity					
velot betteroise							
OF Oast Hotel	and an arriver of	access most coa					
arthurs bying byparts	Semport						
ACTURE PERSON DISCH DE	SFC8HD		0				
these believes a laboration of the							
	Organizational Line (Sul)		~				
	Organization 215						
	01/63						
	low (27)						
	Courtery SLI						
	Lapse Assessmentaries (2014)						
	1.0.000	~ 16106.0208	- +				
	: INS Notes	- altonad Labaraci	- +	۵			
	1702/504						
	RBA Y	- O					
	1997.002						
	1948	0					
	Sale 200						
	(new Cal						
	Children Patient						

- [Subject Alternative Name (SAN)] テキスト フィールド行の 1 つで、ISE FQDN を繰り返す 必要があります。代行名またはワイルドカード証明書を使用する場合、2 つ目の SAN フィ ールドを追加できます。
- 4. [Generate] をクリックすると、ポップアップウィンドウに CSR フィールドが正しく入力さ れているかどうかが示されます。

Г		×	
	Successfully generated CSR(s)		
	abtomar31#Multi-Use		
	Click Export to download CSR(s) or OK to return to list of CSR(s) screen OK Export		
30			

5. CSR をエクスポートするために、左側のパネルで [Certificate Signing Requests] をクリックし、CSR を選択し、[Export] をクリックします。

Cisco ISE	Administration - System									
Deployment Licensing	Certificates Logging	Maintenance	Upgrade Health Check	s Backup & Rest	tore Admin Access	Settings				
Certificate Management v System Certificates Trusted Certificates OCSP Client Profile	Certificate S	igning Requ	Jests	n deursiand one or more filling	an bait they may be simply by an	enternal a Martin Alfar a second has	have size of size			
Certificate Signing Requests	Once a CSR is bound, it will be	removed from this list.								
Certificate Periodic Check Se	Q View db Export	Delete Bind Cer	rtificate							
Certificate Authority	Friendly Name	,	Gertificate Subject	Key Length Portal	pro Timestamp	< Host				
	abtomard 1 Mult	-Use	CN1abtomar01.abtomar.local	2048	Tue, 4 May 2021	abtomar31				

6. CSRはコンピュータに保存されます。それを署名用に CA に送信します。

証明書のインストール

CAから最終的な証明書を受信したら、その証明書を ISE に追加する必要があります。

1. ISE コンソールで、[Administration] > [System] > [Certificates] > [Certificate Signing Requests] に移動し、CRS のチェックボックスをオンにして [Bind Certificate] をクリックし ます。

≡ Cisco IS	ε					Administ	ration - Syst	9400			
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Check	s Backu	p & Restore	Admin Access	S	ottings
Certificate Managem System Certificates	ent v	Certifi	cate Sig	ning Req	uests						
Trusted Certificates OCSP Client Profile		Generate O A Certificate Sig	Certificate Signi pring Requests (CSRs	ng Requests (CSR) must be sent to and sig	a pred by an external a	uthority. Citck "export" I	to dowriticed one or	more CSRs so that	they may be signed by an	external a	sthority. After a request has been sig
Certificate Signing	Requests	Once a CSR Is I	bound, it will be remov	ed from this list.							
Certificate Periodic	Check Se	Q view d	b Expert 👩 0	elete Bind Co	ertificate						
Certificate Authority	>	D Pr	iendly Name		Certificat	e Subject	Key Length	Portal gro	Timestamp	^	Host
		2 *	otomar318Multi-Use		GN=abtom	er31.abtomar.local,	2048		Tue, 4 May 2021		abtomar31

2. [Friendly Name] テキストフィールドに証明書の簡単でわかりやすい説明を入力し、[Submit] をクリックします。

注:この時点では、EAP または Admin プロトコルを有効にしないでください。 3. [System Certificate] の下に、次に示すように未使用の新しい証明書があります。

Admin(58

4. 古い証明書が期限切れになる前に新しい証明書がインストールされるため、日付範囲の指定 が未来になっていることを報告するエラーが表示されます。

Thu, 4 May 2023



5. 継続するには [Yes] をクリックします。緑色で強調表示されているように、これで証明書は インストールされましたが、使用中にはなっていません。

AdminISE	Not in use		abtomar31.abtomar.loc al	abiomar-WIN-231PNBS 4IPH-CA	Tue, 4 May 2021	Thu, 4 May 2023 🥥
Default self-signed ser ver certificate	Admin, Portal, EAP Authentication, RADUIS DTLS	Default Portal Certificate Group ()	abtomar31.abtomar.loc al	abtomar31.abtomar.loc al	Tue, 4 May 2021	Wed, 5 May 2021

注:分散導入で自己署名証明書を使用する場合は、プライマリ自己署名証明書をセカンダ リISE サーバの信頼できる証明書ストアにインストールする必要があります。 同様に、セ カンダリ自己署名証明書をプライマリISE サーバの信頼できる証明書ストアにインストー ルする必要があります。これにより、ISE サーバは相互に認証できます。 これがないと、 導入が中断する可能性があります。サードパーティ CA から証明書を更新する場合は、ルー ト証明書チェーンが変更されているかどうかを確認し、それに応じてISE 内の信頼できる 証明書ストアを更新します。両方のシナリオで、ISEノード、エンドポイント制御システム 、サプリカントがルート証明書チェーンを検証できることを確認します。

警告システムの設定

Cisco ISE はローカル証明書の失効日が 90 日以内に迫ったときに通知します。このような事前通 知により、証明書の期限切れを回避して、証明書の更新を計画し、ダウンタイムを阻止または最 小限に抑えることができます。

この通知はいくつかの方法で表示されます。

- ・色づけされた有効期限のステータスのアイコンが、[Local Certificates] ページに表示されます。
- •期限切れメッセージが Cisco ISE システム診断レポートに表示されます。
- •期限切れアラームは、期限切れの 90 日前と 60 日前に生成されたあと、期限切れ前の 30 日 間は毎日生成されます。

期限切れアラームの電子メール通知を行うように ISE を設定します。ISE コンソールで、 [Administration] > [System] > [Settings] > [SMTP Server] に移動して、Simple Mail Transfer Protocol(SMTP)サーバを特定し、アラームの電子メール通知が送信されるようにその他のサー バ設定を定義します。

Deployment	Licensing	Certificates L	ogging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	
Client Provisioning		SMTP S	Server	Settings					
FIPS Mode Security Settings Narm Settings		Configure a Sim sponsors to ser and enable gue themselves and	ple Mail Tran d email notifi sts to automa with actions	sfer Protocol(SMTP cation to guests wit rtically receive their to take before their) server to serv th their login cre login credentia guest account	d email notifications for adentials and password is after they successful s expire.	alarma, to enable reset instructions, y register		
Posture	>	SMTP Server*	mailser	ver.example.com					
Profiling		SMTP Port*	25	0					
Protocola	>	Connection Time	60 tuoi	seconds	0				
Indpoint Scripts	>	Encryption s	ettings						
roxy		Enable TLS/SSL to the SMTP ma	connection il server befo	encryption to requir ore sending e-mail.	e ISE to establi	sh an encrypted connec	ction		
MTP Server		Use TLS/SS	Encryption ()					
MS Gateway									
ystem Time		Authenticatio	on Setting	s					
IRS Settings		Use Password	Authentication						
API Gateway Setting						_			

通知をセットアップするには、次の2つの方法があります。

管理者に通知するには、管理者アクセスを使用します。

[Administration] > [System] > **[Admin Access] > [Administrators] > [Admin Users] に移動しま** す。

アラーム通知を受信する必要のある管理者ユーザの [Include system alarms in emails] **チェッ クボックスをオンにします。**アラーム通知の送信者の電子メール アドレスは ise@*hostname* としてハードコードされています。

≡ Cisco	SE			Administration	n • System		
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore
Authentication		✓ Admin * Name	Jser				
Authorization	>		admin				
Administrators	~	Status	🛃 Enal	bled 🗸			
Admin Users		Email	admin@	Pexample.com		Include system alarms	in emails
Admin Groups		External	0				
Settings	>	Change Pas Read Only	sword				
		inactive acc	ount never disable	id 🔽			
		> User Ir	nformation				
		> Accou	nt Options				
		✓ Admin	Groups				
			Super Adm	'n	<u>~</u>		

• ユーザに通知するには、ISE アラーム設定を構成します。

下図に示す [Administration] > [System] > [Settings] > [Alarm Settings] > [Alarm Configuration] に移動します。

Deployment Licensing	Certificates Logging Maintenance Up	ograde Health Dhecks Backup &	Restore Admin Access	Settings	0	că here ta do visitality setup be
Olast Provisioning	Alarm Settings					
Cecurity Settings						
Alarm Settings	Astro Congustan Astro hosticaton					
Postare)	/ 10 + AN 9 2000					Introduct
Poling	Alarm Name	~	Category	Security	Status	User Defined
Preloads	Co. Server is direct		Administrative and Specificial Auto-	A		
Endpoint Sectors 2	C CE Server IS 40		Administrative and Operational Audit	0	×	
Pros	C CDA Parley		BE Densions	<u> </u>		
SMTP Server	C Dit, Bettered Tabled		Administrative and Operational Audit	0		
3MB Balance	Centification Representation		Administrative and Operational Autor	Â.		
CRS Settings	Cethan tiped		Administrative and Operational Auto-	•		A
APT Salesway Satisfya	Carthala Kawalang Intelator Inte		Administrative and Specificial Auto-	9		
Relators Bassans Dispectition (Continues Replaced in Falled		Administrative and Operational Auto-	•		
0HOP & DAS Services	Central Replaces Temporty Faled		Administrative and Operational Auto-	٥		
Was Sessions	O Dethus fever		Administrative and Specificket Auto-	A		
Light Date Detribution	Centrifusite required torquinting latinal		Administrative and Operational Autor	0		
Presented help	O Decempeter expension of decemperature		Administrative and Operational Audit			

注:アラームを発生させたくないカテゴリのステータスを無効にします。[Certificate Expiration] を選択して、[Alarm Notification] をクリックし、通知先のユーザーの電子メールア ドレスを入力して、設定変更を保存します。変更がアクティブになるまでに最大15分かかる 場合があります。

Alarm Settings

Alarm Configuration Alarm N	otification
Alarm Name:	Certificate Expiration
Description:	This certificate will expire soon. When it expires, ISE may fail when attempting to establish secure communications with clients. Inter-node communication may also be affected
Suggested Actions:	Replace the certificate. For a trust certificate, contact the issuing Certificate Authority (CA). For a CA-signed local certificate, generate a CSR and have the CA create a new certificate. For a self-signed local certificate, use ISE to extend the expiration date. You can just delete the certificate if it is no longer used
• Status:	
e Severity:	
Send Syslog Message	<u>a</u>
Enter multiple e-mails separated with comma	admin@abtomax.com
Notes in Email (0 to 4000 characters)	

確認

ここでは、設定が正常に機能しているかどうかを確認します。

警告システムの確認

警告システムが正しく機能していることを確認します。この例では、設定の変更によって、情報 の重大度を含むアラートが生成されます(情報アラームが最も低い重大度ですが、証明書の期限 切れはそれよりも高い重大度である警告を生成します)。

Total Endpoints 🕡	Active Endpoints 🕟	Rejected Endp	sainta 🕠	Anomalicus Beh	avior 🕟	Authenticated Gu	estis 🕟	EVDD Endpoints 🕕	Compliance 🕢	
0	0	0		0		0		0	0	
AUTHENTIGATIONS U		# 0 ×	E ALAMS				αO×	E SYSTEM SUMMARY C		
enyton merytona henet h	erte futuri fesco		Beverity	Nate	Out. Last Data	red		1 meteor abtomar31		A8 -
	No dete available.			Natur						
			<u> </u>	ISE Authentication in	55 iess than 1	nia				
			0	Configuration Chang	31 14 million av					
			0	No Configuration Ball	3 15 million ag					
				Health Status Granali-	1 13 hos all -	ini				
								01/	Mehony Lingé	Automotion La

ISE から送信される電子メール アラームの例を以下に示します。

● ●○ ∅ 0 🗳 👘 👘	SE Alarm : Info : Configuration Changed: Admin-admin; Object Type+MnT-Settings; Object Name+ExternalEmailAddresses - Inbox			
Message				
Delete Reply Reply Toreard D Associated	a and a sector of the sector o			
ISE Alarm : Info : Configuration Changed: Admin=admin; Object Type=MnT-Settings; Object Name=ExternalEmailAddresses				
Alarm Name : Configuration Changed				
Denils : Configuration Changed: Admin-admin; Object Type-MeiT Settings; Object Name-ExternalEstalAddresses				
Description : BEE configuration is updated				
Sevenity : Info				
Suggested Actions : Check if the configuration change is espected				
*** This message is generated by Cisco Identity Services Engine	e (SH) ***			

証明書変更の確認

この手順では、証明書が正しくインストールされていることを確認する方法、およびEAPや管理 者の役割を変更する方法について説明します。

1. ISE コンソールで [Administration] > [Certificates] > [System Certificates] に移動し、新しい 証明書を選択して、詳細情報を表示します。

注意:Admin の使用を有効にすると、ISE サービスが再起動するため、サーバーのダウン タイムが発生します。

E Cisco ISE			Administration · System	
Deployment Licensing	Certificates Logging	Maintenance Upgrade		
Certificate Management	Issuer		Warning	
Trusted Certificates	Issuer		Enabling Admin role for this certificate will cause an application server restart on the selected node.	
Certificate Signing Requests	* Friendly Name	AdminISE	OK	
	Description			
Certificate Authority	Subject	CN=abtomar31.abtomar.local,OU=cisco		
	Subject Alternative Name (SAN)	IP Address: 10.106.120.85 DNS Name: abtomar31.abtomarJocal		
	Issuer	abtomar-WIN-231PN8S4IPH-CA		
	Valid From	Tue, 4 May 2021 21:00:34 IST		
	Valid To (Expiration)	Thu, 4 May 2023 21:00:34 IST		
	Serial Number	22 00 00 00 11 DB BC 40 BD 11 C0 68 3E	00 00 00 00 11	
	Signature Algorithm	SHA256WITHRSA		
	Key Length	2048		
	Certificate Policies			
	Usage			
	Admin: Use certificate to authent	cate the ISE Admin Portal		
	EAP Authentication: Use certifica	te for EAP protocols that use SSL/TLS tunneling		
	RADIUS DTLS: Use certificate fo	r the RADSec server		
	prodeted: Use certificate for the part	and Controller		
	SAME Like settificate for SAME	Incase for the TSE Messaging Service		

2. ISE サーバ上の証明書ステータスを確認するために、次のコマンドを CLI に入力します。

CLI:> show application status ise

- 3. すべてのサービスがアクティブになったら、管理者としてログインします。
- 分散導入シナリオの場合は、[Administration] > [System] > [Deployment] に移動します。ノードに緑色のアイコンがあることを確認します。アイコンの上にカーソルを置き、凡例に「Connected」と表示されていることを確認します。
- 5. エンドユーザー認証が成功することを確認します。これを行うには、[Operations] > [RADIUS] > [Livelogs]に移動します。 特定の認証試行を検索し、それらの試行が正常に認 証されたことを確認できます。

証明書の確認

証明書を外部からチェックする場合は、組み込みの Microsoft Windows ツールまたは OpenSSL ツールキットを使用します。

OpenSSL はセキュア ソケット レイヤ(SSL)プロトコルのオープン ソース実装です。証明書で 独自のプライベート CA が使用されている場合は、ローカル マシンにルート CA 証明書を配置し て、OpenSSL オプション -*CApath* を使用する必要があります。中間 CA が存在する場合は、そ れも同じディレクトリに配置する必要があります。

証明書に関する一般情報を取得してそれを検証するには、以下を使用します。

openssl x509 -in certificate.pem -noout -text openssl verify certificate.pem また、OpenSSLツールキットを使用して証明書を変換することも役立ちます。

openssl x509 -in certificate.der -inform DER -outform PEM -out certificate.pem

トラブルシュート

現在、この設定に関する特定の診断情報はありません。

結論

アクティブになる前に新しい証明書を ISE にインストールできるため、古い証明書が期限切れに なる前に新しい証明書をインストールすることをお勧めします。古い証明書の失効日と新しい証 明書の開始日の間の重複期間が、証明書を更新してそれらのインストールを最小限のダウンタイ ムでまたはダウンタイムなしで計画するための時間になります。新しい証明書が有効な日付範囲 に入ったら、EAP か Admin または両方を有効にします。Admin の使用を有効にすると、サービ スが再起動されることに注意してください。 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。