整合客服中心企業版(UCCE)單一登入(SSO)憑證 和設定

目錄

簡介
需求
採用元件
A部分。SSO消息流
B部分.IDP和IDS中使用的證書
C部分:詳細的IDP認證和配置
SSL憑證(SSO)
為SSO配置SSL證書的步驟(本地實驗室已簽署內部CA)
今牌簽名證書
Cisco IDS伺服器如何取得權杖演唱憑證的公鑰?
未啟用加密
D部分。Cisco IDS端證書
SAML證書

簡介

本文檔介紹UCCE SSO所需的證書配置。此功能的設定包括多個HTTPS、數位簽章和加密憑證。

需求

思科建議您瞭解以下主題:

- UCCE版本11.5
- Microsoft Active Directory(AD)- Windows Server上安裝的AD
- Active Directory聯合身份驗證服務(ADFS)版本2.0/3.0

採用元件

UCCE 11.5

Windows 2012 R2

A部分。SSO消息流



啟用SSO後,當代理登入到Finesse案頭時:

- Finesse伺服器重定向代理瀏覽器以與身份服務(IDS)通訊
- IDS使用SAML請求將代理瀏覽器重定向到身份提供程式(IDP)
- IDP生成SAML令牌並傳遞到IDS伺服器
- •生成令牌後,每次代理瀏覽到應用程式時,都會使用此有效令牌進行登入

B部分.IDP和IDS中使用的證書



IDP證書

- SSL憑證(SSO)
- 令牌簽名證書
- 令牌 解密

File Action View Window Help)					
• 🔿 🞽 📰 🚺 🖬						
AD FS	Certificates					
I Service	Subject	Issuer	Effective Date	Expiration Date	Status	Primary
Certificates	Service communications	CN=col115-COL115-CA,	12/30/2016	12/30/2017		
Trust Relationships Claims Provider Trusts Relation Party Trusts	CN=ADFS Encryption - col115dc.col115.org.au	CN=ADFS Encryption - co	12/30/2016	12/30/2017		Primary
Attribute Stores Authentication Policies Per Relving Party Trust	CN=ADFS Signing - col115dc.col115.org.au	CN=ADFS Signing - col11	12/30/2016	12/30/2017		Primary



- SAML證書
- 簽名金鑰
- 加密金鑰



C部分:詳細的IDP認證和配置

SSL憑證(SSO)

- 此證書在IDP和客戶端之間使用。客戶端必須信任SSO證書
- SSL證書用於加密客戶端和IDP伺服器之間的會話。此證書不是特定於ADFS,而是特定於IIS
- SSL證書的主題必須與ADFS配置中使用的名稱匹配



為SSO配置SSL證書的步驟(本地實驗室已簽署內部CA)

步驟1. 使用憑證簽署請求(CSR)建立SSL憑證,並由ADFS的內部CA簽署。

- 1. 開啟伺服器管理器。
- 2. 按一下「工具」。
- 3. 按一下「Internet資訊服務(IIS)管理器」。
- 4. 選擇本地伺服器。
- 5. 選擇伺服器證書。
- 6. 按一下「開啟特徵」(操作面板)。
- 7. 按一下「create certificate request」。
- 8. 將加密服務提供程式保留為預設值。
- 9. 將Bit Length更改為2048。
- 10. 按「Next」(下一步)。
- 11. 選擇儲存請求檔案的位置。
- 12. 按一下「Finish」(結束)。

Server Mana	ager							-	o >
			• (;	ि।	ľ.,	Manage	Tools	View	Help
				Active Active Active	Director Director	y Administr y Domains a y Module fo	ative Cente and Trusts or Windows	Power	Shell
bility	Last Update	Windows Activa		Active	Director	y Sites and	Services		
Performance counters not started	1/10/2017 12:59:07 PM	Not activated		Active AD FS ADSLE Certifi Comp Defrag DNS Event Group	Director Manage Edit cation Au onent Se uter Man gment an Viewer Policy N et Inform	y Users and ment uthority rvices agement of Optimize	Drives	Manao	er
				Intern	et Inform	ation Service	ces (IIS) Mar	nager	

e 3	Internet Information Services (IIS) Manager	- 🗆 X
0	Sol → FS01 →	📅 🗟 🏠 🔞 -
File View	Request Certificate ?	×
Connection	Cryptographic Service Provider Properties	Request
(2) A ⊳-33 Sr	Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.	rtificate Certificate
	Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider	
	Bit length:	
	2048 🗸	
	Previous Next Finish Cancel	
<	III > Features View Content View	
Ready		• <u>1</u> .:

- 1. 開啟CA伺服器以使用此CSR http:<CA Server ip address>/certsrv/。
- 2. 按一下「Request a certificate」。
- 3. 按一下「advanced certificate request」。
- 4. 將CSR複製到Based-64編碼憑證要求。
- 5. 提交。
- 6. 下載已簽名的證書。

Microsoft Active Directory Certificate Services -- col115-COL115-CA

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your ide communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to v pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:	
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	
Additional Attributes:	
Attributes:	
	Submit >

步驟3.將簽名證書安裝回ADFS伺服器並分配給ADFS功能。

1.將簽名證書安裝回ADFS伺服器。為此,請開啟**Server manager**>Tools>按一下Internet Information Services(IIS)Manager>。

Local Server>Server Certificate>Open Feature(操作面板)。

2.按一下「完成證書申請」。

3.選擇您完成並從第三方證書提供商下載的完整CSR檔案的路徑。

4. 輸入憑證的友好名稱。

5.選擇「個人」作為證書儲存。

6.按一下**確定**。

🕤 📲 🕨 COL115 🕨	Complete Certificate Request ? X
View Help ctions	Specify Certificate Authority Response
Start Page COL115 (COL1150\Adminis Application Pools Sites	Complete a previously created certificate request by retrieving the file that contains the certificate authority's response. File name containing the certification authority's response: Friendly name: ADFS Select a certificate store for the new certificate: Personal

7.在此階段,新增了所有證書。現在,必須分配SSL證書。

8.展開**本地**服務器>展開站點>選擇預設網站>按一下繫結(操作窗格)。

9.按一下Add。

10.**將**型別更改為HTTPS。

11.從下拉選單中選擇您的證書。

12.按一下**OK**。

COL11	5 Sites Default Web Site	
View Help	Site Bindings ? ×	
ections	ype ttp ttps Type: IP address: Port: https v All Unassigned v 443 Host name: Require Server Name Indication	issio inge licat ial (
	SSL certificate: Not selected V Select View OK Cancel	Veb 30 (1

現在,已分配ADFS伺服器的SSL證書。

附註:在安裝ADFS功能期間,必須使用以前的SSL證書。

令牌簽名證書

ADFS為令牌簽名證書生成自簽名證書。預設情況下,它在一年內有效。

IDP生成的SAML令牌由ADFS私鑰(令牌簽名證書私密部分)簽名。 然後,IDS使用ADFS公鑰進 行驗證。此保證簽名令牌不會被修改。

每當使用者需要獲取對信賴方應用程式(Cisco IDS)的訪問許可權時,都會使用令牌簽名證書。

10 10 10 10 10 10 10 10 10 10 10 10 10 1	
🙀 File Action View Window Help	os Certificate X
	General Details Certification Path
AD FS Certificates Image: Service Subject Image: Service communications Service communications Image: Service communications Service control 115dc coll15.org.au CN=ADFS Encryption - coll115dc coll115.org.au Image: Service communication Policies Service communication Policies Service coll 115dc coll115.org.au CN=ADFS Signing - coll115dc coll115.org.au Image: Service communication Policies Service coll 115dc coll 115.org.au CN=ADFS Signing - coll 115dc coll 115.org.au Image: Service communication Policies Service coll 115dc coll 115.org.au CN=ADFS Signing - coll 115dc coll 115.org.au <tr< td=""><td>Certificate Information This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store. Issued to: ADFS Signing - col115dc.col115.org.au Issued by: ADFS Signing - col115dc.col115.org.au Valid from 12/30/2016 to 12/30/2017 Install Certificate Issuer Statement CK</td></tr<>	Certificate Information This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store. Issued to: ADFS Signing - col115dc.col115.org.au Issued by: ADFS Signing - col115dc.col115.org.au Valid from 12/30/2016 to 12/30/2017 Install Certificate Issuer Statement CK

Cisco IDS伺服器如何取得權杖演唱憑證的公鑰?

這是通過將ADFS後設資料上載到IDS伺服器,然後將ADFS的公鑰傳遞到IDS伺服器來實現的。這 樣,IDS就可以獲得ADFS伺服器的公鑰。

您需要從ADFS下載IDP後設資料。要下載IDP後設資料,請參閱連結https:// <ADFS的 FQDN>/federationmetadata/2007-06/federationmetadata.xml。

0.4	
85	
86	- <keydescriptor use="signing"></keydescriptor>
87 88	
89	- <keyinfo xmlns="http://www.w3.org/2000/09/xmldsig#"></keyinfo>
90	
91	
92	- <x509data></x509data>
93	
94	<x509certificate>MIIC6DCCAdCgAwIBAgIQFpYJVa99CK9LN50rMdF5nDANBgkghkiG9w0BAQsFADAwMS4wLAYDVQQDEyVBREZTIFNpZ25pbmcgLSBjb2wxMTUkYy5jb2wxMTUk</x509certificate>
	4XDTE2MTIzMDAxMDMyOFoXDTE3MTIzMDAxMDMyOFowMDEuMCwGA1UEAxM1QURGUyBTaWduaW5nIC0gY29sMTE1ZGMuY29sMTE1Lm9yZy5hdTCCASIwDQYJKoZIhvcNAQEBBQADggE
	gEBAKfeys1epEkwWspH4qIB2hG+h1z+rbhjwS49Js7FXMUPN3HLMB0CBKM18fSFlddq5QD/wlot4+2kkx6povXjNpzfuUMU7tgqes1kWD8LoSKu2E70UrDHdg6HvW2HX0KN8j+1v1N
	SUITER BALLET MADE BANG AND THE AND AND THE PART AND AND THE PART AND AND THE
ſΈAI	UFS後設賃料



將ADFS後設資料上載到IDS 權杖解密

此證書由ADFS伺服器(自簽名)自動生成。如果令牌需要加密,ADFS使用IDS公鑰對其進行解密。但是,當您看到ADFS令牌加密時,並不意味著令牌已加密。

IDOICPTI WITCOW	Δ						
\$		AD FS					
输 File Action View Window Help							
🗢 🔿 🙍 📰 🛛 🖬							
ad FS	Certificates						Actions
⊿ Service	Subject	Issuer	Effective Date	Expiration Date	Status	Primary	Certificates
Certificates	Service communications						Add Token-
Claim Descriptions	CN=col115dc.col115.org.au, OU=TAC, O=Cisco	CN=col115-COL115-CA,	12/30/2016	12/30/2017			Add Token
4 📑 Trust Relationships	roken-decrypting						
Claims Provider Trusts	CN=ADFS Encryption - col115dc.col115.org.au	CN=ADFS Encryption - co	12/30/2016	12/30/2017		Primary	Set Service 0
📔 Relying Party Trusts	Token signing						View
Attribute Stores	CN=ADFS Signing - col115dc.col115.org.au	CN=ADFS Signing - col11	12/30/2016	12/30/2017		Primary	New Windo
Authentication Policies Per Relving Party Trust							C Refresh
							Help
							CN=col115do
							View Certifie

如果要檢視是否對特定信賴方應用程式啟用了令牌加密,則需要檢查特定信賴方應用程式上的「加 密」頁籤。

下圖顯示,未啟用令牌加密。

• 🔿 🖄 📰 🔢 🖬		
AD FS	Relying Party Trusts	
 Service Endpoints Certificates Claim Descriptions Trust Relationships Claims Provider Trusts Relying Party Trusts Attribute Stores Authentication Policies 	Display Name Device Registration col115idspub.col11	Enabled Type Identifier coll115idspub.coll115.org.au Properties i.org.au Organization Endpoints Proxy Endpoints Notes Advanced Monitoring Identifiers Encryption Signature Accepted Claims Specify the encryption certificate for this relying party trust. Encryption certificate: Issuer: Issuer: Subject: Effective date: Expiration date: Image: Construction date: Image: Construction date: Browse View Remove Image: Construction date: Image: Construction date:

未啟用加密

D部分。Cisco IDS端證書

- SAML證書
- 加密金鑰
- 簽名金鑰

SAML證書

此證書由IDS伺服器(自簽名)生成。 預設情況下,有效期為3年。

cisco Identity	Service Management	administ
	des	
Nodes 🛧 - Indica	tes Primary Node	
Node	Status	SAML Certificate Expiry
col115	idspub.col115.org.au 🛨 🔹 In Service	• 12-14-2019 18:58 (930 days left)
Settings File Action View W Action View W Action View W Action View W Action View W Action View W Comment Certificates Claim Descriptions Claims Provider True Relying Party Trust Attribute Stores Authentication Policies Per Relying Party Trust	Indow Coll115idspub.coll115.org.au Properties X Organization Endpoints Proxy Endpoints Notes Advanced Monitoring Identifiers Encryption Signature Accepted Claims Specify the signature verification certificates for requests from this relying party. Subject Issuer Effective Date Expiration Subject Issuer Effective Date Expiration 12/14/2016 6:5 12/14/2 ists Add View Remove	Certificate General Details Certification Path Certificate Information This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store. Issued to: coll115/dspub.coll15.org.au Issued by: coll115/dspub.coll15.org.au Valid from 12/14/2016 to 12/14/2019

此證書用於簽署SAML請求並傳送到IDP(ADFS)。 此公鑰在IDS後設資料中,必須匯入到ADFS伺服 器。

1.從IDS伺服器下載SAML SP後設資料。

2.瀏覽到https://<ids server FQDN>:8553/idsadmin/。

3.選擇設定並下載SAML SP後設資料並儲存。

O A https://coll15idspub.coll15.org.au/0553/idsedmin/Main.jsp#/Settings	C Q Search					
Identity Service Management		administ				
Settings	IdS Trust	Security Troubleshooting				
Nodes Settings	$\overline{\diamondsuit}$					
Download	d SAML SP Metadata					
Clients Begin configuring the trust relationship Server (lidS) by obtaining a SAML SP to configure trust relationship in Identi	Begin configuring the trust relationship between the Identity Provider(IdP) and the Identity Server (IdS) by obtaining a SAML SP metadata file from the IdS Server. Use this metadata file to configure trust relationship in Identity Provider (IdP).					
Dov	mload Metadata File					
		Next				
———— 來自IDS伺服器的後設資料						
<pre><?xml version="1.0" encoding="UTF-8"?> <entitydescriptor entityid="col11Sidspub.col115.org.au" xmlns="urn:oa:</th><th>sis:names:tc:SAML:2.0:metadata"> SAML:2.0:protocol" WantAssertionsSigned: sig#"> tDANBgkqhkiG9w0BAQUFADAIMSMwIQ tzU4MjVaFw0xOTEyMTQwNzU4MjVaMC</entitydescriptor></pre>	="true" AuthnRequestsSigned="true"> YDVQQDExpjb2wxMTVpZHNw UxIzAhBgNV					

BAMTGmNvbDExNWlkc3B1Yi5jb2wxMTUub3JnLmF1MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB

- M	Add Relying Party Trust Wizard						
Select Data Source							
Steps	Select an option that this wizard will use to obtain data about this relying party:						
Welcome	Import data about the relation party or blehed online or on a local network.						
Select Data Source	Use this option to import the necessary data and certificates from a relying party organization that outlishes						
 Configure Multi-factor Authentication Now? 	Its federation metadata online or on a local network.						
 Choose Issuance Authorization Rules 							
Ready to Add Trust	Example: fs.contoso.com or https://www.contoso.com/app						
 Finish 	Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.						
	Federation metadata file location:						
	Browse						
	 Enter data about the relying party manually 						
	Use this option to manually input the necessary data about this relying party organization.						

匯入到ADFS伺服器

File Action View Window	col115idspub.col115.org.au Properties	Certificate		
AD FS	Organization Endpoints Proxy Endpoints Notes Advanced	General Details Certification Path		
Service Endpoints Certificates Claim Descriptions	Monitoring Identifiers Encryption Signature Accepted Claims Specify the signature verification certificates for requests from this relying party. Subject Issuer Effective Date Expiration	Certificate Information This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification		
Claims Provider Trusts Relying Party Trusts Attribute Stores Authentication Policies Per Relying Party Trust		Authorities store.		
		Issued to: col115idspub.col115.org.au		
		Issued by: col115idspub.col115.org.au		
		Valid from 12/14/2016 to 12/14/2019		
	< III >			
	Add View Remove	Install Certificate Issuer Statement		
	OK Cancel Apply			

AD FS

從ADFS端驗證

當IDS重新生成SAML證書時(該證書用於對SAML請求進行簽名),它將執行後設資料交換。

加密/簽名金鑰

預設情況下未啟用加密。如果啟用加密,則需要將其上載到ADFS。

col115idspub.col115.org.au P	roperties					
Organization Endpoints Proxy Endpoints	Notes Advanced					
Monitoring Identifiers Encryption Signatu	re Accepted Claims					
Specify the encryption certificate for this relying party trust.				AD FS		
Encryption certificate:						
Issuer:	Select an Encryption Certificate					
Subject: Effective date:	(e) (e) < ↑ (i)	« Wi	ndows + ADFS +	~ ¢	Search ADFS	Q
Expiration date:	Organize 🔻 New f	older			=	· 🔟 🎯
Browse View Remove	🔆 Favorites	^	Name		Date modified	Туре
	Desktop		温 ar		8/23/2013 1:39 AM	File folde
	Downloads		🎉 bg		8/23/2013 1:39 AM	File folde
	🖳 Recent places		🐌 cs		8/23/2013 1:39 AM	File folde
			퉬 da		8/23/2013 1:39 AM	File folde
	🌉 This PC	≡	퉬 de		8/23/2013 1:39 AM	File folde
	隆 Desktop		🍌 el		8/23/2013 1:39 AM	File folde
	Documents		鷆 en		12/30/2016 11:59	File folde
	🐌 Downloads		퉬 en-US		12/30/2016 11:59	File folde
	🚺 Music		鷆 es		8/23/2013 1:39 AM	File folde
ок с	📔 Pictures		鷆 et		8/23/2013 1:39 AM	File folde
	🔡 Videos		鷆 fi		8/23/2013 1:39 AM	File folde
	🔝 Local Disk (C:)		🍌 fr		8/23/2013 1:39 AM	File folde
	DVD Drive (D:)	R 🖄	<			>
		File na	ame:	×	Certificate Files (*.cer;*.	sst;*.p7t ∨
					Open	Cancel

參考:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/i cm_enterprise_11_5_1/Configuration/Guide/UCCE_BK_U882D859_00_ucce-featuresguide/UCCE_BK_U882D859_00_ucce-features-guide_chapter_0110.pdf