Unified Contact Center Enterprise (UCCE) Single Sign On (SSO) Certificates and Configuration

Contents

Introduction Requirements Components Used Part A. SSO Message Flow Part B. Certificates Used in IDP and IDS Part C. IDP Certification in detail and Configuration SSL Certificate (SSO) Steps to configure SSL certificate for SSO (local lab with internal CA signed) Token Signing Certificate How does Cisco IDS server get the public key of Token Singing Certificate? Encryption is NOT enabled Part D. Cisco IDS side Certificate SAML Certificate

Introduction

This document describes certificate configurations that are required for UCCE SSO. Configuration of this feature involves several certificates for HTTPS, Digital Signature and Encryption.

Requirements

Cisco recommends that you have knowledge of these topics:

- UCCE Release 11.5
- Microsoft Active Directory (AD) AD installed on Windows Server
- Active Directory Federation Service (ADFS) Version 2.0/3.0

Components Used

UCCE 11.5

Windows 2012 R2

Part A. SSO Message Flow



When SSO is enabled, when agent logs in to Finesse desktop:

- Finesse server redirects agent browser to communicate with Identity Service (IDS)
- IDS redirects agent browser to Identity Provider (IDP) with SAML request
- IDP generates SAML token and passes to IDS server
- When token was generated, every time agent browses to ppplication, it uses this valid token for log in





IDP Certificates

- SSL Certificate (SSO)
- Token Signing Certificate
- Token decrypting

File Action View Window Help						
• 🤿 🖄 📰 👔						
AD FS	Certificates					
I Service	Subject	Issuer	Effective Date	Expiration Date	Status	Primary
Certificates Claim Descriptions Claims Provider Trusts Claims Provider Trusts Relying Party Trusts Attribute Stores Attribute Stores Per Relving Party Trust	Service communications	CN=col115-COL115-CA,	12/30/2016	12/30/2017		
	CN=ADFS Encryption - col115dc.col115.org.au	CN=ADFS Encryption - co	12/30/2016	12/30/2017		Primary
	CN=ADFS Signing - col115dc.col115.org.au	CN=ADFS Signing - col11	12/30/2016	12/30/2017		Primary

IDS Certificates

- SAML Certificate
- Signature Key
- Encryption Key



Part C. IDP Certification in detail and Configuration

SSL Certificate (SSO)

- This certificate is used between IDP and client. Client must trust SSO certificate
- SSL certificate is placed to encrypt the session between client and IDP server. This certificate is not specific to ADFS, but specific to IIS
- The subject of the SSL certificate must match with the name used in ADFS configuration



Steps to configure SSL certificate for SSO (local lab with internal CA signed)

Step 1. **Create** SSL certificate with Certificate Signing Request (CSR) and sign by internal CA for ADFS.

- 1. Open Server Manager.
- 2. Click Tools.
- 3. Click Internet Information Services (IIS) Manager.
- 4. Select the local server.
- 5. Select Server Certificates.
- 6. Click Open Feature (action panel).
- 7. Click create certificate request.
- 8. Leave the Cryptographic service provider at the default.
- 9. Change the Bit Length to 2048.
- 10. Click Next.
- 11. Select a location to save the requested file.
- 12. Click Finish.

Server Mana	ager							-	<u> </u>
			• (;	ि।	۲.,	Manage	Tools	View	Help
ρ 🗐 ▾ 🕅 ▾	Last Update	Windows Activa		Active Active Active	Directory Directory Directory	y Administr y Domains y Module fo	ative Center and Trusts or Windows Services	Power	Shell
Performance counters not started	1/10/2017 12:59:07 PM	Not activated		Active AD FS ADSI E Certifi	Directory Manager dit cation Au	y Users and ment uthority	I Computers		
				Comp Comp Defrag DNS	onent Se uter Man gment an	rvices agement d Optimize	Drives		
				Event Group Intern	Viewer Policy M et Inform et Inform	lanagemen ation Servic ation Servic	t ces (IIS) 6.0 I ces (IIS) Mar	Manag	er

\$ 3	Internet Information Services (IIS) Manager	_ 🗆 X
0	Sol → FS01 →	📴 🖂 🏠 🔞 -
File View	Request Certificate ?	×
😋 - 📄 🖄	Cryptographic Service Provider Properties	Request
⊢ 💭 A ⊳ - 😺 Si	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.	tificate Certificate
	Cryptographic service provider:	
	Bit length:	
	2048	
	Previous Next Finish Cancel	-
	E Features View Content View	
Ready		•1.:

Step 2. CA signs the CSR that was generated from step 1.

- 1. Open CA server to sing this CSR http:<CA Server ip address>/certsrv/.
- 2. Click Request a certificate.
- 3. Click Advanced certificate request.
- 4. Copy the CSR into Based-64 encoded certificate request.
- 5. Submit.
- 6. Download the signed certificate.

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 >

Step 3. Install the signed certificate back to ADFS server and assign to ADFS feature.

1. Install the signed certificate back to ADFS server. In order to do this, **open Server manager>Tools>Click Internet Information Services(IIS) Manager>**.

Local Server>Server Certificate>Open Feature (Action Panel).

2. Click Complete Certificate Request.

3. Select the path to the complete CSR file that you completed and downloaded from the third party certificate provider.

- 4. Enter the friendly name for the certificate.
- 5. Select Personal as the certificate store.
- 6. Click **OK**.

🕤 📲 🕨 COL115 🕨	Complete Certificate Request ? X
View Help ctions	Specify Certificate Authority Response
Start Page COL115 (COL1150\Adminit 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. At this stage, all certificate were added. Now, SSL certificate assignment is required.

8. Expand the local server>Expand Sites>Select Default Web Site >Click Bindings (actions pane).

9.Click Add.

- 10. Change the type to HTTPS.
- 11. Select your certificate from the drop down menu.
- 12. Click **OK**.

View Help		Site Bindings ? X
tions	Type http https	Add Site Binding ? × Type: IP address: Port: https ✓ All Unassigned ✓ Host name: Require Server Name Indication
p-gr Cer		SSL certificate: Not selected View OK Cancel

Now, SSL certificate for ADFS server was assigned.

Note: During installation of ADFS feature, previous SSL certificate must be used.

Token Signing Certificate

ADFS generates self-signed certificate for token signing certificate. By default it is valid for a year.

SAML token generated by IDP is singed by ADFS private key (Token Signing Certificate Private Part). Then, IDS uses ADFS public key to verify. This guarantees signed token isn't get modified.

The Token Signing Certificate is used every time that a user needs to gain access to a relying party application (Cisco IDS).



How does Cisco IDS server get the public key of Token Singing Certificate?

This is done by uploading ADFS metadata to IDS server, and then passing ADFS' public key to IDS server. In this way, IDS gains the public key of ADFS server.

You need to **download** IDP metadata from ADFS. In order to download IDP metadata, refer to the link https:// <FQDN of ADFS>/federationmetadata/2007-06/federationmetadata.xml.



Metadata



upload ADFS Metadata to IDS Token Decryption

This certificate generates automatically by ADFS server (self-signed). If the token needs encryption, ADFS uses IDS public key to decrypt it. But, when you see ADFS token-dcrypting, it does NOT mean the token is encrypted.

11831CP11 V	VILLERING							
%			AD FS					
🗌 File Action View Window H	elp							
🗢 🔿 🙍 🖬 🛛								
ad FS		Certificates						Actions
Service Endpoints		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-C0L115-CA,	12/30/2016	12/30/2017			Add Token-
Trust Relationships Claims Provider Trusts		CN=ADFS Encryption - col115dc.col115.org.au	CN=ADFS Encryption - co	12/30/2016	12/30/2017		Primary	Set Service (
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
A uthentication Policies Per Relying Party Trust								Refresh
								P Help
								CN=col115dd
								View Certifie

If you want to see whether the token encryption was enabled for a specific relying party application, you need to check the encryption tab on a specific relying party application.

This image shows, token encryption was NOT enabled.

• 🔿 🖄 🔝 🚺			
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 Sorg Organization Endpoints Proxy Endpoints Notes Advanced Monitoring Identifiers Encryption Signature Accepted Claims Specify the encryption certificate for this relying party trust. Encryption certificate: Issuer: Subject: Issuer: Subject: Effective date: Expiration date: Image: Construction date: Browse View Remove Remove	j.au

Encryption is NOT enabled

Part D. Cisco IDS side Certificate

- SAML certificate
- Encryption key
- Signature Key

SAML Certificate

This certificate is generated by IDS server (self-signed). By default it is valid for 3 years.

Identity Servic	e Management		administ
Nodes			
Nodes 🛧 - indicates Prima	ary Node		
Node		Status	SAML Certificate Expiry
col115idspub.c	col115.org.au ★	In Service	• 12-14-2019 18:58 (930 days left)
Settings File Action View Window AD FS AD FS Certificates Claim Descriptions Claims Provider Trusts Relying Party Trusts Attribute Stores Authentication Policies Per Relying Party Trust	Coll15idspub.coll15 Organization Endpoints Proxy E Monitoring Identifiers Encryption Specify the signature verification certifica party. Subject Issuer CN=coll115ids CN=coll115idspu	5.org.au Properties X Endpoints Notes Advanced a Signature Accepted Claims ates for requests from this relying Effective Date Expiratio u 12/14/2016 6:5 12/14/2	General Details Certification Path General Details Certification Path Image: Certificate Information This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store. Issued to: col115/dspub.col115.org.au Issued by: col115/dspub.col115.org.au Valid from 12/14/2016 to 12/14/2019
	Add View	Remove	Install Certificate Issuer Statement

This certificate is used to sign SAML request, and send to IDP (ADFS). This public key is in the IDS metadata, and must be imported to ADFS server.

1. Download SAML SP metadata from IDS server.

2. Broswer to https://<ids server FQDN>:8553/idsadmin/.

3. Select settings and download SAML SP metadata and save it.



<ds:X509Certificate>MIIC+TCCAeGgAwIBAgIEWD4KtDANBgkqhkiG9w0BAQUFADAlMSMwIQYDVQQDExpjb2wxMTVpZHNw dWIuY295MTE1Lm9yZy5hdTAeFw0xNjEyMTQwNzU4MjVaFw0xOTEyMTQwNzU4MjVaMCUxIzAhBgNV BAMTGmNvbDExNWlkc3B1Yi5jb2wxMTUub3jnLmF1MIIBJANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB CaKCAOEAaAOccn0amutwXcHU+2M5(Xb+27C2YX10C0w00d0050bfmccmJ26(C)H9wElloZb1wA2az9

W	Add Relying Party Trust Wizard
Select Data Source	
Select Data Source Steps • Welcome • Select Data Source • Configure Multi-factor Authentication Now? • Choose Issuance Authorization Rules • Ready to Add Trust • Finish	Select an option that this wizard will use to obtain data about this relying party: Import data about the relying party published online or on a local network. Use this option to import the necessary data and cettficates from a relying party organization that publishes its federation metadata online or on a local network. Federation metadata address (host name or URL): Example: fs.contoso.com or https://www.contoso.com/app Import data about the relying party from a file Use this option to import the necessary data and cettficates 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: Ensure that file location:
	 Enter data about the relying party manually Use this option to manually input the necessary data about this relying party organization.

import to ADFS Server

÷		AD F3)
File Action View Window	col115idspub.col115.org	g.au Properties	Certificate
AD FS Certificates Claim Descriptions Trust Relationships Claims Provider Trusts	Organization Endpoints Proxy Endpoints Monitoring Identifiers Encryption Specify the signature verification certificates fr party. Subject Issuer Subject Issuer Subject Issuer	Notes Advanced Signature Accepted Claims or requests from this relying Effective Date Expiration 12/14/2016 6:5 12/14/2	General Details Certification Path Image: Certificate Information Certificate Information This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
 Relying Party Trusts Attribute Stores Authentication Policies Per Relying Party Trust 			Issued to: coll15idspub.coll15.org.au Issued by: coll15idspub.coll15.org.au
	< III Add View Ren	NOVE	Valid from 12/14/2016 to 12/14/2019 Install Certificate Issuer Statement
	ОК	Cancel Apply	

Verify from ADFS side

When IDS re-generates the SAML certificate-the one is used to sign the SAML request- it performs Metadata exchange.

Encryption/Signature Key

Encryption is not enabled by default. If encryption is enabled, it needs to be uploaded to ADFS.

col115idspub.col115.org.au P	roperties					
Organization Endpoints Proxy Endpoints	Notes Advanced					
Monitoring Identifiers Encryption Signatu	Ire Accepted Claims					
Specify the encryption certificate for this relying party	trust.		AD	FS		
Encryption certificate:						
Issuer:			Select an Encryption	Certificate		2
Subject: Effective date:	⊚ ⊚ ∞ ↑ 🍺	« Windows	► ADFS ►	~ ¢	Search ADFS	م
Expiration date:	Organize 👻 New f	older				· 🔟 🔞
Browse View Remove	😭 Favorites	^ Nam	e		Date modified	Туре
	Desktop		ar		8/23/2013 1:39 AM	File folde
	🐌 Downloads	🔒 t	og		8/23/2013 1:39 AM	File folde
	🖳 Recent places	🔋 👔 🤅	5		8/23/2013 1:39 AM	File folde
		📄 🔒 d	da		8/23/2013 1:39 AM	File folde
	🌉 This PC	= 🔒 d	de		8/23/2013 1:39 AM	File folde
	膧 Desktop	📄 🔒 e	el		8/23/2013 1:39 AM	File folde
	Documents	📄 🔒 e	en		12/30/2016 11:59	File folde
	🗼 Downloads	🔋 🔒 e	en-US		12/30/2016 11:59	File folde
	🐌 Music	🔋 🔒 e	5		8/23/2013 1:39 AM	File folde
ОК С) Pictures	— 🔒 e	et		8/23/2013 1:39 AM	File folde
	📑 Videos	🛛 🔒 f	i		8/23/2013 1:39 AM	File folde
	📷 Local Disk (C:)	📃 🔒 f	r		8/23/2013 1:39 AM	File folde
	🖆 DVD Drive (D:) I	R ~ <				>
		File name:		~	Certificate Files (*.cer;*.s	sst;*.p7t ∨
					Open	Cancel

Referecne :

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/ icm_enterprise_11_5_1/Configuration/Guide/UCCE_BK_U882D859_00_ucce-featuresguide/UCCE_BK_U882D859_00_ucce-features-guide_chapter_0110.pdf