# Certificati e configurazione Single Sign-On (SSO) UCCE (Unified Contact Center Enterprise)

## Sommario

Introduzione Requisiti Componenti usati Parte A. Flusso messaggi SSO Parte B. Certificati utilizzati in IDP e IDS Parte C. Certificazione IDP in dettaglio e configurazione Certificato SSL (SSO) Passaggi per la configurazione del certificato SSL per SSO (laboratorio locale con CA interna firmata) Certificato per la firma di token In che modo il server Cisco IDS ottiene la chiave pubblica del certificato Token Singing? Crittografia NON abilitata Parte D. Certificato laterale Cisco IDS Certificato SAML

## Introduzione

In questo documento vengono descritte le configurazioni dei certificati necessarie per UCCE SSO. La configurazione di questa funzionalità richiede diversi certificati per HTTPS, firma digitale e crittografia.

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- UCCE release 11.5
- Microsoft Active Directory (AD) AD installato in Windows Server
- Active Directory Federation Service (ADFS) versione 2.0/3.0

## Componenti usati

UCCE 11.5

Windows 2012 R2

## Parte A. Flusso messaggi SSO



Quando SSO è abilitato, quando l'agente accede al desktop Finesse:

- Il server Finesse reindirizza il browser dell'agente per comunicare con Identity Service (IDS)
- IDS reindirizza il browser dell'agente al provider di identità (IDP) con richiesta SAML
- IDP genera il token SAML e lo passa al server IDS
- Al momento della generazione del token, ogni volta che l'agente passa all'applicazione, utilizza questo token valido per l'accesso





#### Certificati IDP

- Certificato SSL (SSO)
- Certificato per la firma di token
- Token decrittografia

File Action View Window Help						
• 🔿 🙍 🖬						
AD FS	Certificates					
i 🧮 Service	Subject	Issuer	Effective Date	Expiration Date	Status	Primary
Endpoints	Service communications					
Certificates	CN=col115dc col115 org au OU=TAC O=Cisco	CN=col115-COL115-CA	12/30/2016	12/30/2017		
Claim Descriptions			12/00/2010	12/30/2017		
ı 📔 Trust Relationships	Token-decrypting					
📔 Claims Provider Trusts	E CN=ADFS Encryption - col115dc.col115.org.au	CN=ADFS Encryption - co	12/30/2016	12/30/2017		Primary
🧮 Relying Party Trusts	Token-signing					
Attribute Stores	CN=ADFS Signing - col115dc.col115.org.au	CN=ADFS Signing - col11	12/30/2016	12/30/2017		Primary
🛛 📔 Authentication Policies						
<ol> <li>Per Relving Party Trust</li> </ol>						

#### Certificati IDS

- Certificato SAML
- Chiave firma
- Chiave di crittografia



## Parte C. Certificazione IDP in dettaglio e configurazione

### Certificato SSL (SSO)

- Questo certificato viene utilizzato tra IDP e il client. Il client deve considerare attendibile il certificato SSO
- Il certificato SSL viene posizionato per crittografare la sessione tra il client e il server IDP. Questo certificato non è specifico di ADFS, ma specifico di IIS
- Il soggetto del certificato SSL deve corrispondere al nome utilizzato nella configurazione ADFS



Passaggi per la configurazione del certificato SSL per SSO (laboratorio locale con CA interna firmata)

**Passaggio 1**. **Creare un** certificato SSL con CSR (Certificate Signing Request) e firmarlo con la CA interna per ADFS.

- 1. Aprire Server Manager.
- 2. Fare clic su Strumenti.
- 3. Fare clic su Gestione Internet Information Services (IIS).
- 4. Selezionare il server locale.
- 5. Selezionare Certificati server.
- 6. Fate clic su Apri feature (Open Feature) nel pannello azioni.
- 7. Fare clic su crea richiesta certificato.
- 8. Non modificare il provider del servizio di crittografia come predefinito.
- 9. Impostate Lunghezza bit (Bit Length) a 2048.
- 10. Fare clic su Next (Avanti).
- 11. Selezionare un percorso in cui salvare il file richiesto.
- 12. Fare clic su Finish (Fine).

							_	_	
		• (*	)।	ľ.,	Manage	Tools	View	He	lp
	Mindaus Astro		Active Active Active	Directory Directory Directory	y Administra y Domains a y Module fo	ative Center and Trusts or Windows I	Powers	Shell	
Performance counters not started 1/10/2017	12:59:07 PM Not activated		Active Active AD FS ADSI E	Directory Directory Manager dit	y Sites and S y Users and ment	Services Computers			
			Certifie Comp Comp Defrac	cation Au onent Ser uter Man ament an	ithority rvices agement d Optimize	Drives			
			DNS Event Group Interne	Viewer Policy M et Inform	lanagement ation Servic	es (IIS) 6.0 M	lanage	er	

<b>S</b>	Internet Information Services (IIS) Manager	_ 🗆 X
0	Image: PS01 → PS01 →	📅 🖂 🏠 🔞 -
File View	Request Certificate ?	×
😋 - 📄 🖄	Cryptographic Service Provider Properties	Request
–	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: Microsoft RSA SChannel Cryptographic Provider	
	Bit length:	
	2048 🗸	
	Previous Next Finish Cancel	
<	III > Features View Content View	
Ready		91.:

Passaggio 2. CA firma il CSR generato dal passaggio 1.

- 1. Aprire il server CA per utilizzare questo CSR http:<indirizzo IP server CA>/certsrv/.
- 2. Fare clic su Richiedi certificato.
- 3. Fare clic su Richiesta avanzata certificati.
- 4. Copiare il CSR nella richiesta di certificato con codifica Based-64.
- 5. Invia.
- 6. Scaricare il certificato firmato.

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 >

**Passaggio 3.** Reinstallare il certificato firmato nel server ADFS e assegnarlo alla funzionalità ADFS.

1. Reinstallare il certificato firmato nel server ADFS. A tale scopo, **aprire Server** manager>Strumenti>Fare clic su Gestione Internet Information Services (IIS)>.

Server locale>Certificato server>Apri funzionalità (pannello azioni).

2. Fare clic su Completa richiesta certificato.

3. Selezionare il percorso del file CSR completo completato e scaricato dal provider di certificati di terze parti.

- 4. Inserire il nome descrittivo del certificato.
- 5. Selezionare Personale come archivio certificati.
- 6. Fare clic su OK.

🕤 📲 🕨 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. In questa fase sono stati aggiunti tutti i certificati. A questo punto è necessario assegnare il certificato SSL.

8. Espandere il server locale>Espandi siti>Seleziona sito Web predefinito >Associazioni clic (riquadro delle azioni).

9.Fare clic su Add (Aggiungi).

- 10. Modificare il tipo in HTTPS.
- 11. Selezionare il certificato dal menu a discesa.
- 12. Fare clic su OK.

View Help		Site Bindings ? ×
ctions Start Page COL115 (COL1 COL15 (COL15 (COL1 COL15 (COL15 (COL1 COL15 (COL15 (C	Type http https	Add Site Binding     Type:   IP address:   Port:   https   All Unassigned   443     Host name:   Require Server Name Indication
		SSL certificate: Not selected View OK Cancel

A questo punto è stato assegnato il certificato SSL per il server ADFS.

**Nota:** Durante l'installazione della funzionalità ADFS, è necessario utilizzare un certificato SSL precedente.

#### Certificato per la firma di token

ADFS genera un certificato autofirmato per il certificato per la firma di token. Per impostazione predefinita è valido per un anno.

Il token SAML generato da IDP è firmato dalla chiave privata ADFS (parte privata del certificato per la firma di token). IDS quindi utilizza la chiave pubblica ADFS per la verifica. Il token firmato con garanzia non viene modificato.

Il certificato per la firma di token viene utilizzato ogni volta che un utente deve accedere a un'applicazione relying party (Cisco IDS).

<b>V</b> #	AD FS
🧌 File Action View Window Help	Certificate
🗢 🔿 🙍 🖬 🖬 🖬	General Details Certification Path
AD FS  AD FS  Cartificates  Cartificates  Cartificates  Cartificates  Cartificates  Cartificates  Cartificates  Subject Service communications  Cartificates  Cartificates Cartificates  Cartificates  Cartificates	Issuer       Certificate Information         OU=TAC, O=Cisco CN=col115-COL11       This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.         Sdc.col115.org.au       CN=ADFS Encrypt         Issued to:       ADFS Signing - col115dc.col115.org.au         Issued to:       ADFS Signing - col115dc.col115.org.au         Valid from       12/30/2016 to       12/30/2017         Install Certificate       Issuer Statement

#### In che modo il server Cisco IDS ottiene la chiave pubblica del certificato Token Singing?

A tale scopo, caricare i metadati ADFS nel server IDS e quindi passare la chiave pubblica di ADFS al server IDS. In questo modo IDS ottiene la chiave pubblica del server ADFS.

Ènecessario **scaricare** i metadati IDP da ADFS. Per scaricare i metadati IDP, fare riferimento al collegamento **https:// <FQDN of ADFS>/federationmetadata/2007-06/federationmetadata.xml**.

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>MIIC6DCCAdCgAwIBAgIQFpYJVs99CK9LN50rMdF5nDANBgkqhkiG9w0BAQsFADAwMS4wLAYDVQQDEyVBRE2TIFNp225pbmcgLSBjb2wxMTVkYy5jb2wxMTUkYy5jb2wxMTUkY</x509certificate>
	4XDTE2MTIzMDAxMDMyOFoXDTE3MTIzMDAxMDMyOFoxMDEUMCwGA1UEAxM1QURGUyBTaWduaW5n1C0gY29sMTE1ZGMuY29sMTE1Lm9yZy5hdTCCASIwDQYJKoZIhveNAQEBBQADggEB
	gEBAKteyslepEkw#pH4gH2DG+h1z+rbhjwS49J#7FXNUPN3HLNBOCERNIETSFldqSQD/wlot4+2KkxEpovKjNpztuUNU7tgqenLkWDBLosKu2E7OUrDHdgEHw2EXKON83+1711
Dai	metadati



carica metadati ADFS in IDS **Decrittografia token** 

Questo certificato viene generato automaticamente dal server ADFS (autofirmato). Se il token richiede la crittografia, ADFS utilizza la chiave pubblica IDS per decrittografarlo. Tuttavia, quando viene visualizzata la crittografia token ADFS, NON significa che il token sia crittografato.

§.		AD FS					
Image: Second system         Second system         Second system         Help           Image: Second system         Image: Second syste							
AD FS	Certificates						Actions
⊿ Service	Subject	Issuer	Effective Date	Expiration Date	Status	Primary	Certificates
Certificates	Service communications	ON	10/00/0010	10/00/0017		_	Add Token-
Claim Descriptions	Ess Chreat Houckon Hourg au, OUHTAC, OHOIses	CIVICOLLID-COLLID-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 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							Refresh
							🛛 Help
							CN=col115dd
							View Certifie

Se si desidera verificare se la crittografia del token è stata abilitata per un'applicazione relying party specifica, è necessario selezionare la scheda crittografia in un'applicazione relying party specifica.

Nell'immagine viene mostrato come la crittografia del token NON sia stata abilitata.

• 🔿 🖄 📰 👔			
AD FS	Relying Party Trusts		
<ul> <li>Service</li> <li>Endpoints</li> <li>Certificates</li> <li>Claim Descriptions</li> <li>Trust Relationships</li> <li>Claims Provider Trusts</li> <li>Relying Party Trusts</li> <li>Attribute Stores</li> <li>Authentication Policies</li> </ul>	Display Name Device Registration col115idspub.col11!	Enabled       Type       Identifier         coll115idspub.coll115.org.au       Properties       Image: Coll of the state	.au

## Crittografia NON abilitata

## Parte D. Certificato laterale Cisco IDS

- certificato SAML
- Chiave di crittografia
- Chiave firma

#### **Certificato SAML**

Questo certificato viene generato dal server IDS (autofirmato). Per impostazione predefinita è valido per 3 anni.

Identity Service	ce Management	administ
Nodes	}	
Notes * - Indicates Prim	ary Node	
Node	Status	SAML Certificate Expiry
col115idspub.	.col115.org.au \star 🔹 In Service	• 12-14-2019 18:58 (930 days left)
Settings File Action View Window AD FS Catificates Claim Descriptions Claims Provider Trusts Relying Party Trusts Attribute Stores Per Relying Party Trust	Contention       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       III       >         Add.       View       Remove       Personal       >	Certificate       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: col115/dspub.col115.org.au         Issued by:       col115/dspub.col115.org.au         Valid from       12/14/2015       to       12/14/2019

Questo certificato viene utilizzato per firmare la richiesta SAML e inviarla all'IDP (ADFS). La chiave pubblica è inclusa nei metadati IDS e deve essere importata nel server ADFS.

1. Scaricare i metadati SAML SP dal server IDS.

#### 2. Passare a https://<FQDN server ids>:8553/idsadmin/.

3. Selezionare le impostazioni, scaricare i metadati SAML SP e salvarli.



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:				
<ul> <li>Welcome</li> </ul>	Import data about the relying party published 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 publishes				
Configure Multi-factor Authentication Now?	its federation metadata online or on a local network.				
<ul> <li>Choose Issuance Authorization Rules</li> </ul>					
<ul> <li>Ready to Add Trust</li> </ul>	Example: fs.contoso.com or https://www.contoso.com/app				
<ul> <li>Finish</li> </ul>	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				
	<ul> <li>Enter data about the relying party manually</li> </ul>				
	Use this option to manually input the necessary data about this relying party organization.				

#### importa nel server ADFS

÷		AD FS	
File Action View Window	col115idspub.col115.org.au Prop	perties <b>x</b>	Certificate
AD FS Service Certificates Claim Descriptions Trust Relationships	Organization         Endpoints         Proxy Endpoints         No           Monitoring         Identifiers         Encryption         Signature           Specify the signature verification certificates for requests party.         Subject         Issuer         Effective D           Subject         Issuer         Effective D         12/14/201	tes Advanced Accepted Claims from this relying Ate Expiration 16 6:5 12/14/2	General Details Certification Path
Claims Provider Trusts  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 Remove		Valid from 12/14/2016 to 12/14/2019 Install Certificate Issuer Statement
	OK Cance	Apply	

#### Verifica dal lato ADFS

Quando IDS rigenera il certificato SAML (quello utilizzato per firmare la richiesta SAML), esegue lo scambio di metadati.

### Chiave di crittografia/firma

Per impostazione predefinita, la crittografia non è attivata. Se la crittografia è abilitata, deve essere caricata in 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:	(a) a dial dial dial dial dial dial dial di	« Wir	ndows + ADFS +	~ C	Search ADFS	م	
Expiration date:	Organize 👻 New fo	older				· 🔟 🔞	
Browse View Remove	🔶 Favorites	^	Name		Date modified	Туре	
	Desktop		📔 ar		8/23/2013 1:39 AM	File folde	
	Downloads		🔒 bg		8/23/2013 1:39 AM	File folde	
	E Recent places		📕 cs		8/23/2013 1:39 AM	File folde	
			🔰 da		8/23/2013 1:39 AM	File folde	
	🌉 This PC	≡	鷆 de		8/23/2013 1:39 AM	File folde	
	膧 Desktop		鷆 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		🍌 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:) I	R				>	
	File name:			¥	Certificate Files (*.cer;*.sst;*.p7t ∨		
					Open	Cancel	

#### Riferimento:

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