Unified Communications Manager، رادصإلاا 10.5 SAML SSO Configuration Example

تايوتحملا

ەمدقملا

SSO) نامألا ديكأتل (SAML) يداحألا لوخدلا ليجست ةغل نيوكت ةيفيك دنتسملا اذه فصي (SSO) نامألا ديكأتل (SSO) يداحأل ل اهتحص نم ققحتلاو Cisco Unified Communications Manager (CUCM).

ةيساسألا تابلطتملا

تابلطتملا

(NTP) ةكبشلا تقو لوكوتورب دادعا

رفوم نيب تقولاا قرف نأ نم دكأتلااو حيحصلا NTP دادعإ تيبثت بجي ،SAML SSO لمعي يكل ناوث ثالث زواجتي ال ةدحوملا تالاصتالا تاقيبطتو (IdP) ةيوهلا.

ريغ SAML ةباجتسإ" :أطخلاا اذه ىقلتت ،IdP و CUCM نيب ينمز قباطت مدع كانه ناك اذا يكل .IdP و CUCM مداوخ نيب نمازتم ريغ تقولا نوكي امدنع أطخلا اذه ثدحي دق ".ةحيحص IdP نيب تقولا قرف نأ نم دكأتلاو حيحصلا NTP دادعإ تيبثت كيلع بجي ،SAML SSO لمعي .ناوث ثالث زواجتي ال ةدحوملا تالاصتالاا تاقيبطتو

ل<u>ېل د</u>يف NTP تادادعا مسق ىل عجرا ،تاعاسلا ةنمازم ةيفيك لوح تامولعم ىلع لوصحل NTP تادادعا مسق ىل عجرا ،تاعاسلا <u>مى قدحوملاتال ايغشت ماظن قرادا</u> <u>نم قدحوملا تالاصتالا ليغشت ماظن قرادا</u>

(DNS) لاجملا مسا مداخ دادعا

لماكلاب ةلەؤملا تالاجملا ءامسأ لحل DNS مادختسإ ةدحوملا تالاصتالا تاقيبطتل نكمي ةطساوب لحلل نيلباق فرعملاو ةمدخلا ورفوم نوكي نأ بجي .IP نيوانعل (FQDNs) .ضرعتسملا

ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملاو جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست

- Active Directory Federation Service (AD FS)، اك 2.0 دادصإلا IdP
- ةمدخ دوزمك 10.5 رادصإلا CUCM •
- جمانرب Microsoft Internet Explorer 10

نيوكتب تمق اذإ .اثيدح هتيبثت مت CUCM ىلإ دنتسملا اذه دنتسي :**ريذحت** اقفو تاوطخلا ضعب يطخت ىلإ رطضت دقف ،جاتنإلا يف لعفلاب دوجوم مداخ ىلع SSO جاتنإلا مداخ ىلع تاوطخلا ذيفنتب تمق اذإ ةمدخلا ريثأت مهف اضيأ بجي .كلذل لمعلا مدع تاعاس لالخ ءارجإلاا اذه ذيفنتب ىصويو.

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ مت. تناك اذا .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألاا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ةرشابم كتكبش.

ةيساسأ تامولعم

لوصولا نم نيلوؤسملا نكمي XML ىلع مئاق ةحوتفم ريياعم وذ تانايب قيسنت وه SAML هذه ددأ ىلإ لوخدلا ليجست دعب ةسالسب Cisco نم نواعتلا تاقيبطت نم ةددحم ةعومجم ىلإ نم ءزجك ةيلوألا تانايبلا لدابتي امدنع (CoT) ةقثلا ةرئاد SAML SSO ئشني .تاقيبطتلا ريفوتل IDp مدختسم تامولعم يف ةمدخلا دوزم قثي .ةمدخلا دوزمو IdP نيب ميدقتلا ةيلمع .قفلتخملا تاقيبطتلا وأتامدخلا يلامي

كا 2.0 رادصإلاا SAML ضوفي .ةقداصملاا يف نيكرتشم تامدخلا ورفوم دعي مل :**قظحالم** الباقم ةقداصملاب ليمعلا موقي .تافرعملا ىلإو ةمدخلا يدوزم نع اديعب ةقداصملا قكرش" دوجول ارظن .ةمدخلا رفوم ىلإ ديكأتلا ليمعلا مدقي .ليمعلل ديكأتلا IdP حنميو ليمعلام دويكأتلا يا وصولا قح حنميو ديكأتلا يف ةمدخلا دوزم قثي ،"ءارش.

نيوكتلا

ةكبشلل يطيطختلا مسرلا



Figure :SAML Single sign SSO Call Flow for Collaboration Servers

ليلدلا دادعإ

.LDAP ماظن < LDAP < ماظنلا < Cisco نم ةدحوملا CM قرادإ رتخأ .1



- .**ديدج فيضي** ةقطقط .2
- .هتمسو (LDAP) ليلدلا ىلإ لوصولل فيفخلا لوكوتوربلا مداخ عون نيوكتب مق .3
- 4. لدان LDAP نم ةنمازم نكمي ترتخأ.

LDAP System Configuration							
Save							
Status							
(i) Status: Ready							
-IDAP System Informati	ion						
Enable Synchronizing fr	iom I DAP Server						
LDAP Server Type	Microsoft Active Directory						
LDAP Attribute for User ID	sAMAccountName						
Save							

- .5 د < LDAP حماظنلا < Cisco نم ةدحوملا M قرادا رتخأ.5 LDAP نيلد < CM فرادا رتخأ
- :رصانعلا هذه نيوكت .6

مداخ فيضم مساةنمازملا لودجاهتنمازم دارملا مدختسملا تامسLDAP ليلد باسح تادادعإ LDAP ذفنملا مقرو IP ناونع وأ

LDAP Directory	
🔚 Save 🗙 Delete 🗋 Copy	Perform Full Sync Now 🕂 Add New
Status	
(i) Status: Ready	
-LDAP Directory Information-	
LDAP Configuration Name*	LDAP
LDAP Manager Distinguished Name*	CN=Administrator,CN=Users,DC=ciscolive,DC=com
LDAP Password*	•••••
Confirm Password*	•••••
LDAP User Search Base*	CN=Users,DC=ciscolive,DC=com
LDAP Custom Filter	< None >

ةنمآلاا ليصوتلا ذخأم ةقبط مادختسإ ديرت ال تنك اذإ **SSL مادختسإ** ديدحت ءاغلإب مق .7 (SSL) ليلدب لاصتالل LDAP.

ىلإ LDAP ليلد ةداەش ليمحتب مق ،SSL ربع LDAP نيوكت ديرت تنك اذإ :**حيملت** Cisco Unified Communications Manager SRND ليلد ىوتحم عجار .CUCM لضفأو ةددحملا LDAP تاجتنمل باسحلا ةنمازم ةيلآ لوح تامولعم ىلع لوصحلل LDAP. ةنمازمل ةماعلا تاسرامملا

.نآلاا ةلماكلاا ةنمازملاا ءارجاب مق مث ظفح قوف رقنا .8

قوف رقنلاا لبق ةمدخلا بيو ةحفص يف **Cisco DirSync** ةمدخ نيكمت نم دكأت :**قظحالم** ظفح.

Host Name or IP Address for Server ⁸	LDAP Port* Use SSL
adfs1.ciscolive.com	3268
Add Another Redundant LDAP Server	

يرادإلا رودلا محنم ديرت امدختسم ددجو ،**يئامنلا مدختسملا < مدختسملا قرادإ** ىلإ لقتنا .9 ل CUCM لاثملا اذه ددجي) SSO.

System +	Call Routing 👻 Medi	a Resources 👻 Adv	anced Features 👻 D	evice • Application •	User Management 👻	Bulk Administration 👻 H	telp 👻
Find and	l List Users						
🕂 Add	New Eselect All	🔛 Clear All 💥	Delete Selected				
Status							
() 3 m	ecords found						
User	(1 - 3 of 3)						Rows p
User Find Use	(1 - 3 of 3) r where First name		begins with 💽		Find Clear Filter	4 -	Rows p
User Find Use	(1 - 3 of 3) r where First name User ID ^	First Name	begins with 💽	Department	Find Clear Filter	j∳ ⇔ RI	Rows p User Status
User Find Use	(1 - 3 of 3) r where First name User ID *	First Name Saml	begins with 💽 Last Name SSO	Department	Find Clear Filter Directory U	IRI Active LDAP	Rows p User Status Synchronized User

يف مكحتلا ةعومجم ىلا ةفاضا قوف رقناو تانوذألا تامولعم ىلإ لفسأل ريرمتلاب مق .10 رقناو ،**ديدحتلا ةفاضا** رقنا ،**يسايقلا CCM ل نيزيمتملا نيمدختسملا** ددح .**لوصولا** ظفح.

roups	Standard CCM Super Users		
			Add to Access Control Group
			Remove from Access Control Group
		View Details	
les	Standard AXL API Access		
	Standard Admin Rep Tool Admin		
	Standard CCM Admin Users	-	
	Standard CUReporting	View Details	

SAML SSO نيكمت

- 1. مرادإ مدختسم ةهجاو ىلإ لوخدلا ليجستب مق .1
- يداحألا لوخدلا ليجست نيوكت ةذفان حتفيو SAML **يداحأ لوخد ليجست < ماظن** رتخأ .2

SAML.



3. نيكمت قوف رقنا ،ةعومجملا ىلع SAML SSO نيكمتل.

SAML Single Sign-On									
🞸 Enable SAML SSD 🕋 Export All Metadata 🛞 Update IdP Metadata File 🥜 Fix All Disabled Servers									
-Status									
(i) SAML SSO disabl	ed								
SAML Single Sign-	On (1-2 of	2)				Rows per Page 50 -			
Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test			
CUCM	Disabled	N/A	Never	🗄 File	March 30, 2011 7:57:56 PM CEST	Never Run SSO Test			

4. **قعباتم** قوف رقنا ،"ريذحتلا طبض ةداعإ" ةذفان يف.

nttps://cucm.ciscolive.com/?windowtitlekey=genericdialogwindow.windowtitle.ssoenablewindowtitle 💻 🗖	Ľ
	*
Web server connections will be restarted	
Enabling SSO and importing the metadata will cause web services to restart upon completion of the wizard. All affected web applications will drop their connection momentarily and need to be logged into again.	
Click "Export All Metadata" button	
If the server metadata has not already been uploaded to the IdP, it can be done before running the wizard. You can obtain the server metadata by clicking the "Export All Metadata" button on the main page. Then go to the IdP and upload the file.	
Continue Cancel	
	-
Done	. //.

5. في م داريتسال **ضارعتسا** قوف رقنا ،SSO ةشاش ىلع .5 (FederationMetadata.xml ةوطخلا عم (Download IdP Metadata.

System 👻	Call Routing 👻	Media Resources 👻	Advanced Features 👻	Device 🔻	Application +	User Management 👻	Bulk Administration +	Help 🕶
SAML Sin	gle Sign-On	Configuration						
Next								
Status -	is: Ready							
- Downloa To configu manually This	ad Identity pr ure the trust re obtain the file is a manual st	rovider(IdP) Metad lationship between th from the IdP before epi	data Trust File ne IdP and your devic you can upload it to yo	es, you mu our Collabo	st first obtain t pration servers	rust metadata from y	your IdP and import it	t to your servers. You will need to
1)Log in t 2)Click 'N	o your IdP and ext' once you h	download the metad have this file available	lata trust file to your l le locally.	ocal server				
Next	Cancel							

P **فرعم فيرعت تانايب داريتسإ** قوف رقنا ،فيرعتلا تانايب فلم ليمحت درجمب .6 **يلاتلا** قوف رقناو داريتسالا حاجن نم دكأت .CUCM ىلإ فرعملا تامولعم داريتسال .ةعباتملل

System 👻 Call Routing 👻 Media Resources 👻 Advanced Features 👻 Device 👻 Application 👻 User Management 👻 Bulk Administration 👻 Help 👻
SAML Single Sign-On Configuration
Next .
- Status
Ready to import Identity Provider metadata trust file to cluster servers
- Import the IdP Metadata Trust File
This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.
1)Select the IdP Metadata Trust File
C:\Users\Administrator\Desktop\FederationMetadata.xml Browse
2)Import this file to the Collaboration servers
This action must be successful for at least the Publisher before moving on to the next task in this wizard.
Import IdP Metadata
Next Cancel
SAML Single Sign-On Configuration
Next
Status
V Import succeeded for all servers
- Import the IdP Netadata Trust File
This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.
1)Select the IdP Metadata Trust File

Browse...

Import succeeded for all servers

SAML Single Sign-On Configuration
Head Head Head
- Status
If Admin has already uploaded the server metadata to IdP then skip the steps below and click Next. Otherwise follow the steps below to upload the server metadata to IdP
IdP Metadata has been imported to servers in this cluster
- Download Sarvar Metadata and install on the IdD
Download the metadata trust file from Collaboration servers and manually install it on the IdP server to complete SSO setup.
1)Download the server metadata trust files to local storage
Download Trust Metadata File
This is a manual step!
2)Log in to your IdP and upload the server metadata trust file.
3)Click 'Next' once you have installed the server metadata on the IdP.
Back Next Cancel

فيرعت تانايبو CUCM ظفحل (يرايتخإ) **ةقثلا فيرعت تانايب فلم ليزنت** قوف رقنا .7 <u>فرطلا ةقثك CUCM ةفاضا</u> ىلإ لقتناو يلحم دلجم ىلإ ةيلوألا روضحلاو CUCM IM <u>فرطل</u>ا م

8. ددح SSO رابتخإ ليغشت قوف رقناو يرادإ مدختسمك SSO ددح

This action must be successful for at least the Publisher before moving on to the next task in this wizard.

.8 ةوطخلا ىلإ لقتنا ،AD FS نيوكت لامتكا درجمب .

2)Import this file to the Collaboration servers

Import IdP Metadata

Next Cancel

System +	Call Ro	uting 🛨	Media Reso	urces 🔻	Advanced F	Features 👻	Device +	Application +	User Management	 Bulk Administratic 	, 10	Help 🛨	
SAML SI	ngle Sig	gn-On	Configurat	ion									
de Back													
- Status -													_^
🔥 The	server	metada	ta file must	be insta	lled on the I	IdP before	this test is	run.					
- Test SS	0 Setu	p											-
This test SSO has	verifies been er	that the abled.	e metadata i SSO setup o	iles are annot b	correctly co e completed	onfigured a d unless th	nd will allo s test is su	w SSO to start ccessful.	up on the server	a. This test can be r	un on	any server for troubleshooting once	
1)Pick a	valid use	ername	to use for t	his test									
You must This user	t already must h	y know ave adr	the passwor ninistrator r	d for th ights an	e selected u d also exist i	sername. in the IdP.							
🔥 Plea	ise use	one of t	the Usernam	es sho	wn below. Us	sing any ot	her Userna	me to log into	the IdP may resu	lt in administrator le	ockout	t.	
Valid adn	ninistrat	or User	names										
2)Launch	SSO te	st page											
Run	SSO Te	st											
Back	Cance	L											-

لخدأ ،دامتعالا تانايب كنم بلطي امدنع .ةعباتملا ةلصاومو ةداەشلا تاريذحت لەاجت .9 ق**فاوم** رقناو مدختسملا SSO ل رورملا ةملكو مدختسملا مسا.

		,
Windows Secu	rity	🔟 usted certifi
Connecting to	ADFS1.ciscolive.com.	ent website'
	550	ercept any c
	Domain: CISCOLIVE	e to this we
	Remember my credentials	
	OK Cancel	
		•
•		•

قالغا قوف رقنا ."!SSO رابتخإ حجن" ةلاسر ضرع متي ،تاوطخلا عيمج لامتكا دعب .10 SSO ىلع SSO نيكمتل حاجنب نيوكتلا ماهم نآلا تلمكأ دقل .ةعباتملل "**ءاهنإ**و مادختساب



ا مب 11. كال CUCM قفاضا نيوكت بجي ،CUCM كرتشم لثم نالمعي Presence و CUCM IM نأ امب 11. ةحفص نم SAML SSO نيكمتل **SSO رابتخإ** ليغشت مث <u>دامتعال ا فرط ةقثك دجاوتلاو</u> داهسفن CUCM SAML SSO .

تمقو IdP ىلع دقعلاا ةفاك فيرعت تانايبل XML تافلم نيوكتب تمق اذإ :**قظحالم** دقعلا عيمج ىلع SAML SSO نيكمت متيسف ،ةدحاو ةدقع ىلع SSO ةيلمع نيكمتب .ةعومجملا ماظن يف

ةەجك ةعومجم ماظن يف روضحلاو CUCM IM و CUCM دقع عيمجل AD FS ةئيەت بجي لاصتا.

اذإ SAML SSO ل دجاوتلاو CUCM IM و Cisco Unity Connection نيوكت اضيأ بجي :**حيملت** قبرجت مادختسإ ديرت تنك SAML SSO ءالمعل SAML SSO قبرجت مادختسإ ديرت تنك

ةحصلا نم ققحتلا

حيحص لكشب نيوكتلا لمع ديكأتل مسقلا اذه مدختسا.

- .1 ل FQDN ل CUCM لخدأو بيو ضرعتسم حتفا
- 2. قوف رقنا Cisco Unified Communications Manager.
- 3. بجي مث نمو ،Go طغضاو (قدحوملا Cisco ريراقت/قدحوملا قمدخلا/CM قرادا) WebApp ددح مدختسملا دامتعا تانايب لاخدا درجمب .AD FS قطساوب دامتعالا تانايب لاخداب كتبلاطم SSO، تقدحوملا قمدخلا قحفص، CM قرادا قحفص) ددحملا WebApp يل كلوخد ليجست متي Cisco Unified Reporting).

Attp://cucm.ciscolive.com/ - Windows Internet Explorer		_ # ×
🚱 🕗 ♥ 🛍 http://cucm.ciscolive.com/	💌 🕁 🗶 👂 Bing	ρ.
😭 Favorites 🛛 🚖 🔊 Suggested Sites 🔹 🔊 Web Sice Galery 🔹		
tatis http://cucm.ciscolive.com/	🦄 + 🔂 - 🖃 👼 + Page + S	iafety - Tools - 🔞 -
		- î
ahaha		
CISCO		
Installed Applications		
Cisco Unified Communications Manager		
 Recovery URL to bypass Single Sign On (SSO) Cisco Unified Communications Self Care Portal 		
Cisco Prime License Manager		
Cisco Unified Reporting Cisco Unified Serviceability		
Platform Applications		
Plation Applications		
Disaster Recovery System		
 Cisco Unified Communications OS Administration 		

:تاحفصلا هذه ىلإ لوصولا SAML SSO نكمي ال :**ةظحالم**

- Prime صيخرتلا ريدم -
- ليغشتلا ماظن ةرادإ -

ثراوكلا دعب لمعلا ىلع ةردقلا ةداعتسإ ماظن -

اهحالصإو ءاطخألا فاشكتسا

رايخلاا مدختسأ ،لوخدلا ليجست ىلع ارداق نكت ملو SAML نيكمت ىلع ارداق نكت مل اذا **لوخدلا ليجست زواجتل ةداعتسالل URL ناونع ىمسملاو** ةتبثملا تاقيبطتلا تحت ديدجلا مت يتلا دامتعالا تانايب مادختساب لوخدلا ليجستل همادختسا نكمي يذلاو ،(SSO) يداحألا ايلحم اهؤاشنا مت نيذلا CUCM ل نييرادإلا نيمدختسملا وأ تيبثتلا ءانثا اهؤاشنا

🔏 Cisco Unifi	ied CM Console - Windows Internet Explorer			_ 0 >
00-1	https://cuam.dscolive.com/camadmin/showRecovery.do	💌 😵 Certificate Error	++ 🗙 🔎 Bing	ρ.
🚖 Favorites	🝰 🙋 Suggested Sites 🔹 🙋 Web Silce Gallery 🔹			
🔏 Cisco Unifi	ed CM Console		🏠 • 🔂 - 🖻 🖶 • I	Page - Safety - Tools - 😥 -
cisco	Cisco Single Sign On Recovery Administration For Cisco Unified Communications Solutions			
Cisco This pag running This pag	D Single Sign On Recovery Administrat ge will validate credentials locally, allowing access only to application on this server, and will not leverage SAML SSO authentication. ge can be disabled through the CLI.	ion ns that are	Username ccmadmin Password •••••• Login Reset	
Copyright @	1999 - 2015 Cisco Systems, Inc.			

All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our Export Compliance Product Report web site.

For information about Cisco Unified Communications Manager please visit our Unified Communications System Documentation web site.

For Cisco Technical Support please visit our Technical Support web site.

<u>اهحالصاو SAML SSO ءاطخاً فاشكتساً</u> ىلإ عجرا ،اهحالصإو ءاطخاًلا فاشكتساً نم ديزمل .10.x نواعتلا تاجتنمل

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما