Unity Connection バージョン 10.5 SAML SSO 設 定例

内容

概要 <u>前提条件</u> <u>要件</u> <u>Network Time Protocol (NTP)の設定</u> <u>ドメイン ネーム サーバ (DNS)の設定</u> <u>使用するコンポーネント</u> <u>背景説明</u> <u>設定</u> <u>ネットワーク図</u> <u>ディレクトリ セットアップ</u> <u>SAML SSO の有効化</u> <u>確認</u> トラブルシュート

概要

このドキュメントでは、Cisco Unity Connection(UCXN)用の Security Assertion Markup Language(SAML)シングル サインオン(SSO)の設定と検証の方法について説明します。

前提条件

要件

Network Time Protocol (NTP)の設定

SAML SSO を動作させるには、正しい NTP 設定をインストールする必要があり、ID プロバイダー(IdP)と Unified Communications アプリケーションの間の時間差が 3 秒を超えていないこと を確認する必要があります。クロックの同期については、<u>Cisco Unified Communications オペレ</u> <u>ーティング システム アドミニストレーション ガイド [英語]</u> で、NTP の設定についての項を参照 してください。

ドメイン ネーム サーバ (DNS)の設定

Unified Communications アプリケーションは、完全修飾ドメイン名を IP アドレスに解決するために DNS を使用することができます。サービス プロバイダーと IdP は、ブラウザにより確定できる必要があります。

SAML要求を処理するには、Active Directory フェデレーション サービス(AD FS)バージョン 2.0 をインストールおよび設定しておく必要があります。 このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- IdP としての AD FS バージョン 2.0
- ・サービス プロバイダーとしての UCXN
- Microsoft Internet Explorer バージョン 10

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 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

背景説明

SAML は、XML をベースとしたオープン スタンダードのデータ交換形式です。サービス プロバ イダーによってユーザの認証に使用される認証プロトコルです。IdP とサービス プロバイダーと の間で、セキュリティ認証情報がやり取りされます。

オープン スタンダードである SAML を使用すると、クライアントはそのプラットフォームの種類 に関係なく、SAML 対応のどのようなコラボレーション(またはユニファイド コミュニケーショ ン)サービスに対しても認証を実行できます。

Cisco Unified Communications Manager(CUCM)、UCXN など、あらゆる Cisco Unified Communications Web インターフェイスでは、SAML SSO 機能の SAML バージョン 2.0 プロト コルを使用します。Lightweight Directory Access Protocol(LDAP)ユーザを認証する場合、 UCXN は認証要求を IdP に委任します。UCXN が生成するこのような認証要求を、SAML 要求と 呼びます。IdP は認証を実行し、SAML アサーションを返します。SAML アサーションは、 Yes(認証成功)または No(認証失敗)のいずれかを示します。

SAML SSO を有効化すると、LDAP ユーザは IdP での認証に使用したユーザ名とパスワードで、 クライアント アプリケーションにログインできます。ユニファイド コミュニケーション製品でサ ポートされるいずれかの Web アプリケーションにサインインしたユーザは、SAML SSO 機能が 有効化されると、UCXN 上のこれらの Web アプリケーションにもアクセスできるようになりま す(ただし CUCM、CUCM IM とプレゼンスを除く)。

Unity Connection ユーザ	Web アプリケーション
-	 UCXN Administration
	 Cisco UCXN Serviceability
	• Cisco Unifiedサービスアビリティ
管理者権限を持つ LDAP ユーザ	 Cisco Personal Communications Assistant
	Web Inbox
	• Mini Web Inbox(デスクトップ バージョ
	ン)
	 Cisco Personal Communications Assistant
	Web Inbox
管理者権限のない LDAP ユーザ	• Mini Web Inbox(デスクトップ バージョ
	ン)
	• Cisco Jabber クライアント

設定

ネットワーク図



Figure :SAML Single sign SSO Call Flow for Collaboration Servers

ディレクトリ セットアップ

- 1. [UCXN Administration] ページにサインインし、[LDAP] を選択して、[LDAP Setup] をクリックします。
- 2. [Enable Synchronizing from LDAP Server] チェックボックスをオンにし、[Save] をクリック します。

LDAP System Configurat	ion
Save	
Status	
Status: Ready	
U Status, Ready	
LDAP System Information	on
Enable Synchronizing fr	om LDAP Server
LDAP Server Type	Microsoft Active Directory
LDAP Attribute for User ID	sAMAccountName

Save

- 3. [LDAP] をクリックします。
- 4. [LDAP Directory Configuration] をクリックします。
- 5. [Add New] をクリックします。
- 6. 次の項目を設定します。

LDAP ディレクトリ アカウント設定同期対象のユーザ属性同期スケジュールLDAP サーバの ホスト名、または IP アドレスおよびポート番号

7. Secure Socket Layer (SSL)を使用して LDAP ディレクトリと通信するには、[Use SSL] を オンにします。

ヒント: LDAP over SSL を設定するには、LDAP ディレクトリ証明書を CUCM にアップロ ードします。特定の LDAP 製品のアカウント同期メカニズム、および LDAP 同期の一般的 なベスト プラクティスの詳細については、<u>Cisco Unified Communications Manager SRND</u> <u>の LDAP ディレクトリの情報を参照してください。</u>

Cisco Unity Conr Cisco For Cisco Unified Comm	nection Administration	u	Navigation Cisco Unity	y Connection Administration 💌 G umentation About Sign Ou
Cisco Unity Connection Plugins -fax Server -LDAP Setup -LDAP Directory Configuration -LDAP Directory Configuration -LDAP Custom Filter -SAML Single Sign on -Cross-Origin Resource Sharing (C B-SMTP Configuration B Advanced Telephony Integrations -Phone System -Port Speech Connect Port -Trunk B-Security Tools -Task Management -Bulk Administration Tool		Find and List LDAP Direct efresh Help LDAP te [*] CN-Administrator, CN-Users, CN-Users, DC-ciscolive, DC-ci CN-Users, DC-ciscolive, DC-ci None > ton Schedule 7 hhtmm)* [2015-01-18-00-00	DC-ciscolive,DC-com	rmentation About Sign Ou P Directory Configuration (LDAP)
- Custom Keypad Mapping Higration Utilities - Grammar Statistics - SMTP Address Search - Show Dependencies	Standard User Fields To Be S Gisco Unified Communications Mar	ynchronized nager User Fields LDAP Attribute sAMAccountNam	Cisco U ne First N	Jnified Communications Manager U ame

8. [Perform Full Sync Now] をクリックします。

Ho	st Name or IP Address for Server [*]	LDAP Port*	Use SSI
ad	ffs1.ciscolive.com	3268	
	Add Another Redundant LDAP Server		

注:[Save] をクリックする前に、Cisco DirSync サービスが Serviceability Web ページで有 効になっていることを確認します。

- 9. [Users] を展開して、[Import Users] を選択します。
- 10. [Find Unified Communications Manager End Users] リストから、[LDAP Directory] を選択 します。
- 11. UCXN を統合した LDAP ディレクトリからユーザのサブセットのみをインポートする場合 は、検索フィールドに該当する条件を入力します。
- 12. [Find] を選択します。
- 13. [Based on Template] リストから、選択したユーザの作成時に UCXN で使用するための管 理者テンプレートを選択します。

注意:管理者テンプレートを指定した場合、ユーザはメールボックスを持たなくなります。

14. UCXN ユーザを作成する LDAP ユーザのチェックボックスをオンにし、[Import Selected] をクリックします。

alada Cisco Unity Connec		ction Administration				Navigation Cisco Unity Connection Administration 💽 Go		
CISCO For Cisco Unified C	ommur	nications Solut	tions		ucxn	admin 📘 Search Docum	rentation About Sign Out	
 Cisco Unity Connection 		Import Users					Import Users	
Users Users Import Users	1	Import Users	Refresh	Help				
Synch Users Class of Service Class of Service Class of Service Class of Service		Found 1	LDAP User(:	s)				
Templates User Templates Call Handler Templates Contact Templates		Find End Use Where Alias	rs In LDAF	P Directory 💌 Begins With 💌	Eine	1		
El Notification Templates		Based on Ter	h mplate adm	ninistratortemplate 💌				
Distribution Lists		Directory S	earch Resi	ults				
System Distribution Lists Call Management		Import S	elected	Import All 25 •	Rows Per Page			
Directory Handlers		N .	las 🔺	First Name	Last Name	Phone Number	Extension	
Interview Handlers Custom Recordings		Import S	ielected	Saml	SSO			
Message Storage								
Mailbox Stores Mailbox Stores Membership E-Mailbox Quotas								
Message Aging	्रम							

SAML SSO の有効化

- 1. UCXN 管理ユーザ インターフェイスにログインします。
- 2. [System] > [SAML Single Sign-on] の順にクリックすると、[SAML SSO Configuration] ウィ ンドウが開きます。

diala Cisco Unity Con	nection Administra	tion		Navig	ation Cisco Unity Con	nection Administration 💌 Go
For Cisco Unified Comm	unications Solutions			ucxnadmin	Search Document	tation About Sign Out
Cisco Unity Connection	SAML Single Sign on					SAML Single Sign on
Plugins	SAML Single Sign on Re	fresh Help				
G-LDAP	🤣 Enable SAML SSO (Update IdP Metada	ta File 👔 Export All	Metadata 🥜	Fix All Disabled Servers	
LDAP Directory Configuration LDAP Authentication Phone Number Conversion LDAP Custom Filter	Status SAML SSO disabled					
Cross-Origin Resource Sharing (C	SAML Single Sign-On	(1 - 1 of 1)				Rows per Page 50
B-SMTP Configuration E-Advanced	Server SSO Name Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
Telephony Integrations Phone System Port Group Port Society Root	UCXN1 Disabled Enable SAML SSO	N/A Export All	Never Metadata	📥 File	Never	Never Run BSO Test
-Trunk E-Security	(i) *- indicates require	d item.				
Tools Task Management Bulk Administration Tool Custom Keyped Mapping Migration Utilities Grammar Statistics SMTP Address Search Show Dependencies	-					

- 3. クラスタで SAML SSO を有効にするには、[Enable SAML SSO] をクリックします。
- 4. [Reset Warning] ウィンドウで [Continue] をクリックします。

https://ucxn1.ciscolive.com/?windowtitlekey=genericdialogwindow.windowtitle.ssoenablewindowtitl	
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. SSO画面で[Browse]をクリックし、**FederationMetadata**.xmlメタデータXMLファイルを [**Download Idp Metadata**]ステップを使用してイン**ポートし**ます。

diada Cisco Unity Conn	ection Administration	Navigation Cisco Unity Connection Administration 🗾 Go
For Cisco Unified Commu	inications Solutions	ucxnadmin Search Documentation About Sign Out
Cisco Unity Connection	SAML Single Sign on Configuration	SAML Single Sign on Configuration
Plugins	SAML Single Sign on Configuration Refresh Help	
LDAP	Next	
LDAP Directory Configuration LDAP Authentication	C Status	
	Ready to import Identity Provider metadata trust file to	o cluster servers
- SAML Single Sign on - Cross-Origin Resource Sharing (C H-SMTP Configuration	Import the IdP Metadata Trust File This step uploads the file acquired from the IdP in the previ	ous manual step to the Collaboration servers.
Advanced	1)Select the IdP Metadata Trust File	
Telephony Integrations Phone System	C:\Users\Administrator\Desktop\FederationMetadata.xml	Browse
Port Group Port	2)Import this file to the Collaboration servers	
Speech Connect Port Trunk	Import IdP Metadata	ore moving on to the next task in this wizard.
Security		
H Tools	Next Cancel	
Bulk Administration Tool		
Custom Keypad Mapping		
Migration Utilities		
Grammar Statistics		
SMTP Address Search		
Show Dependencies	-	
<u>د ا</u>		
Done		🌇 🗸 Trusted sites Protected Mode: Off 🛛 🍕 + 💐 100% +

6. メタデータ ファイルがアップロードされたら、[Import IdP Metadata] をクリックして IdP 情報を UCXN にインポートします。インポートが成功したことを確認し、[Next] をクリック して続行します。

cisco Ear Cisco Unity Com	nection Administration	Navigation Cisco Unity Connection Administration 💌
-		ucxnadmin Search Documentation About Sign C
 Cisco Unity Connection 	SAML Single Sign on Configuration	SAML Single Sign on Configuratio
Plugins East Sector	SAML Single Sign on Configuration Refresh He	elp
E-LOAD	A and	
-LDAP Setup	Next	
-I DAP Directory Configuration	8	
LDAP Authentication	- Status	
-Phone Number Conversion	Import succeeded for all servers	
LDAP Custom Filter		
SAML Single Sign on		
-Cross-Origin Resource Sharing (C	🖉 🖵 Import the IdP Metadata Trust File ————	
SMTP Configuration	This step uploads the file acquired from the IdP in t	the previous manual step to the Collaboration servers.
Advanced	1)Select the IdP Metadata Trust File	
Telephony Integrations		Brours
Phone System	8	biomse
Port Group	2)Import this file to the Collaboration sequent	
Port	This action must be successful for at least the Public	linkes before maximum to the part tools in this winned.
Speech Connect Port	This action must be successful for at least the Publi	hisher before moving on to the next task in this wizard.
Trunk		- 🦉 Import succeeded for
H-Security	Import IdP Hetadata	W all servers
Task Management	Next Cancel	
Custom Keyand Mansing		
H-Moration Utilities		
Grammar Statistics		
Show Dependencies	-	
4 D		
lone		🏹 🗸 Trusted sites Protected Mode: Off 🛛 🍕 🔹 🔍 100%

7. [Download Trust Metadata Fileset] をクリックして(UCXN メタデータによる ADFS の設定 がまだ済んでない場合のみ)、UCXN メタデータをローカルフォルダに保存し、[<u>Add</u> <u>UCXN as Relaying Party Trust</u>] に移動します。AD FS 設定が完了したら、手順 8 に進みま す。

Cisco Unity Conr Cisco For Cisco Unified Comm	nection Administration	Navigation Cisco Unity Connection Administration 💽 Go
Cisco Unity Connection For Cisco Unity Comment For Cisco Unity Connection Plugins Fax Server CibAP CibAP Setup CibAP Directory Configuration CibAP Authentication CibAP Custom Filter SAML Single Sign on Cross-Origin Resource Sharing (C SMTP Configuration G-Advanced Telephony Integrations Phone System	SAML Single Sign on Configuration Refresh Help If Admin has already uploaded the server metadata If Admin has already uploaded the server metadata to IdP If Admin has already uploaded the server metadata to IdP If Pownload Server Metadata and install on the IdP Download Server Metadata and install on the IdP Download the server metadata trust file from Collaboration server 1)Download the server metadata trust files to local storation Download Trust Metadata File	ucxnadmin Search Documentation About Sign Out SAML Single Sign on Configuration a to IdP then skip the steps below and click Next. Otherwise follow the duster File Download X Do you want to open or save this file? Name: SPMetadata.zip Type: Compressed (zpped) Folder, 1.57/8
Port Speech Connect Port Trunk S-Security Tools Grash Management Grash Management Grash Management Grash Margation Utilities Grash Statistics SMTP Address Search Show Dependencies	This is a manual step! 2)Log in to your IdP and upload the server metadata true 3)Click 'Next' once you have installed the server metadat Back Next Cancel	From: ucon1.ciscolive.com Prom: ucon1.ciscolive.com Prom: ucon1.ciscolive.com Prom: Save Cancel Prom: Ucon2 Prom: Ucon2

8. 管理ユーザとして SSO を選択し、 Run SSO Test をクリックします。

ucxnadmin Search Documentation About Sion Ou
re this test is run. d and will allow SSO to start up on the servers. This test can habled. SSO setup cannot be completed unless this test is e. dP. other Username to log into the IdP may result in
e.

9. 証明書に関する警告は無視し、次に進みます。クレデンシャルの入力を促されたら、ユーザ SSO のユーザ名およびパスワードを入力し、[OK] をクリックします。

Windows Securit	γ	🔟 usted certifi
Connecting to A	DFS1.ciscolive.com.	ent website'
	sso Domain: CISCOLIVE Remember my credentials	ercept any c
1		
	OK Cancel	
		•
•		•

注:この設定例は、UCXN と AD FS 自己署名証明書に基づいています。認証局(CA)の証 明書を使用する場合、適切な証明書を AD FS と UCXN の両方にインストールする必要があ ります。詳細については、「<u>証明書の管理と検証」を参照してください。</u>

10. すべての手順が完了すると、「SSO Test Succeeded!」 メッセージに応答します。[Close] 、[Finish] **の順にクリックして続行します。**



以上で、AD FS を使用して UCXN で SSO を有効にするための設定作業が完了しました。

重要な注意事項:SAML SSO を有効化するには、クラスタの場合は、UCXN サブスクライ バに対して SSO テストを実行します。クラスタ内のすべての UCXN ノードに対し、AD FS を設定する必要があります。

ヒント: IdP ですべてのノードのメタデータ XML ファイルを設定し、1 つのノードで SSO の動作を有効にすると、SAML SSO はクラスタのすべてのノードで自動的に有効になります。

また、SAML SSO に CUCM、CUCM IM とプレゼンスを設定することで、Cisco Jabber Clients に対して SAML SSO を使用し、エンドユーザに本来の SSO 体験を提供できます。

確認

Web ブラウザを開き、UCXN の FQDN を入力すると、[Installed Applications] の下位に、新たに [Recovery URL to bypass Single Sign-on (SSO)] というオプションが表示されます。 [Cisco Unity Connection] リンクをクリックすると、AD FS によってクレデンシャルの入力が促されます。ユ ーザの SSO 用のクレデンシャルを入力すると、[Unity Administration] ページおよび [Unified Serviceability] ページにログインできます。

🖉 https://ucon1.ci	scolive.com/ - Winds	ows Internet Explorer			_	8 ×
G 🖸 🗸 htt	tps://ucxn1. ciscolive.co	m/	💌 👰 Certificate Error	😽 🗙 🔎 Bing		۰ ۹
🚖 Favorites 🛛 🙀	🙆 Suggested Sites 🔹	🖉 Web Sice Gallery 🔹				
88 • Certificat	te Error: Navigation	Chttps://ucxn1.ciscolive.c 🗙		🚹 • 🔂 - 🖃 👼 • Pag	e • Safety • Tools •	۰9
	cisco					•
	Installed App	lications				. 1
	 Cisco Unity o Reco Cisco Prim Cisco Unifie 	Connection very URL to bypass Single Sign C e License Manager ad Serviceability	Dn (SSO)			
	Platform App	lications				
	Disaster Re Cisco Unifie	ecovery System ed Communications OS Administr	ration			

注:SAML SSO では次のページにアクセスはできません。

- Prime Licensing Manager
- OS Administration
- Disaster Recovery system

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

詳細については、<u>Collaboration 製品 10.x における SAML SSO のトラブルシューティング [英語]</u> <u>を参照してください。</u>