CMSでのWebApp SSOの設定およびトラブルシ ューティング

```
内容
<u>はじめに</u>
前提条件
  要件
  <u>使用するコンポーネント</u>
背景
設定
<u>ネットワーク図</u>
<u>ADFSのインストールと初期セットアップ</u>
<u>アイデンティティプロバイダー(IdP)へのCMSユーザのマッピング</u>
IdP用のWebbridgeメタデータXMLの作成
アイデンティティプロバイダー(IdP)へのWebbridgeのメタデータのインポート
IdPでのWebbridgeサービスのクレームルールの作成
Webbridge用のSSOアーカイブZIPファイルを作成します。
  idp config.xmlを取得および設定します
  <u>コンテンツを含むconfig.jsonFileの作成</u>
  <u>sso_sign.keyの設定(オプション)</u>
  <u>sso encrypt.keyを設定します(オプション)。</u>
  <u>SSO ZIPファイルの作成</u>
  WebbridgeへのSSO Zipファイルのアップロード
<u>共通アクセスカード(CAC)</u>
<u>WebApp経由のSSOログインのテスト</u>
<u>トラブルシューティング</u>
  基本的なトラブルシューティング
  <u>Microsoft ADFS障害コード</u>
  認証IDを取得できませんでした
  検証でアサーションが渡されない/一致しない
  Webアプリでサインインに失敗しました:
    <u>シナリオ1:</u>
    <u>シナリオ2:</u>
    シナリオ3:
  <u>ユーザ名が認識されない</u>
    <u>シナリオ1:</u>
    シナリオ2:
  Webbridgeログに示された作業ログの例。結合URLで?trace=trueを使用して生成された例:
関連情報
```

はじめに

このドキュメントでは、シングルサインオン(SSO)のCisco Meeting Server(CMS)Webアプリ実装 を設定およびトラブルシューティングする方法について説明します。

前提条件

要件

次の項目に関する知識があることを推奨しています。

- CMS Callbridgeバージョン3.1以降
- CMS Webbridgeバージョン3.1以降
- Active Directory サーバ
- ・ プロバイダー(IdP)の識別

使用するコンポーネント

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。

- CMS Callbridgeバージョン3.2
- CMS Webbridgeバージョン3.2
- Microsoft Active Directory Windows Server 2012 R2
- Microsoft ADFS 3.0 Windows Server 2012 R2

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、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景

CMS 3.1以降では、IDプロバイダーで1つのセッションが作成されるため、ユーザがログインする たびにパスワードを入力しなくてもSSOを使用してサインインできる機能が導入されました。 この機能は、SSOメカニズムとしてSecurity Assertion Markup Language(SAML)バージョン2.0を 使用しています。

◆ 注: CMSはSAML 2.0でのみHTTP-POSTバインディングをサポートし、使用可能なHTTP-POSTバインディングがないIDプロバイダーを拒否します。 設定

ネットワーク図



ADFSのインストールと初期セットアップ

この展開シナリオでは、Identity Provider (IdP)としてMicrosoft Active Directory Federation Services (ADFS)を使用します。そのため、この構成の前にADFS (または意図したIdP)をイン ストールして実行することをお勧めします。

アイデンティティプロバイダー(IdP)へのCMSユーザのマッピン グ

有効な認証をユーザに取得させるには、IdPによって提供される関連フィールドに対して、アプリ ケーションプログラミングインターフェイス(API)でユーザをマッピングする必要があります。こ のために使用されるオプションは、APIのIdapMapping内のauthenicationIdMappingです。

1. CMS Web管理GUIでConfiguration > APIに移動します。



2.api/v1/ldapMappings/<GUID-of-Ldap-Mapping>の下で既存の(または新しい)LDAPマッピング を見つけます。

API objects

This page shows a list of the objects supported by the API. Where you see a \blacktriangleright control, you can expand that section to either s details of one specific section of configuration.

ilter Idapmappings (2 of 1	29 nodes)			
/api/v1/ldapMappings ٵ				
« start < prev 1 - 2 (of 2) next >	Create new	Table view	XML view	
obje	ect id			iidMapping
458ad270-860b-4bac-9497-b74278e	d2086		\$sAMAccountNar	ne\$@brhuff.com

3. 選択したIdapMappingオブジェクトで、IdPから渡されたLDAP属性への authenticationIdMappingを更新します。この例では、オプション\$sAMAccountNameisをマッピン グ用のLDAP属性として使用しています。

/api/v1/ldapMappings/458ad270-860b-4bac-9497-b74278ed2086

jidMapping	\$sAMAccountName\$@brhuff.com	🛓 - present
nameMapping	□ \$cn\$	- present
cdrTagMapping		
coSpaceUriMapping	\$sAMAccountName\$.space	- present
coSpaceSecondaryUriMapping		
coSpaceNameMapping	□ \$cn\$'s Space	- present
coSpaceCallIdMapping		
authenticationIdMapping	\$sAMAccountName\$	- present
	Modity	

◆ 注:authenticationIdMappingは、callbridge/データベースによってSAMLResponse内の IdPから送信されたクレームを検証し、ユーザにJSON Web Token(JWT)を提供するために 使用されます。

4. 最近変更されたIdapMappingに関連付けられたIdapSourceでLDAP同期を実行します。

例:

/api/v1/ldapSyncs

tenant		Choose
IdapSource	Ob8de8cd-ccce-4ccb-89a8-08ba69e98ec7	Choose
removeWhenFinished	□ <unset> ✓</unset>	
	Create	

5. LDAPの同期が完了したら、CMS APIのConfiguration > api/v1/usersに移動し、インポートされ たユーザを選択して、authenticationIdが正しく入力されていることを確認します。

	Object con	figuration		
d		userJid	jdoe@brhuff.com	
J			John Doe	
-		email	johndoe@brhuff.com	
	auth	enticationId	jdoe	
		userProfile	d5cd50e4-e423-4ba6-b	d17-7492b9ba5eb3

IdP用のWebbridgeメタデータXMLの作成

Microsoft ADFSを使用すると、メタデータXMLファイルを証明書利用者信頼パーティとしてイン ポートして、使用しているサービスプロバイダーを特定できます。この目的でメタデータXMLフ ァイルを作成する方法はいくつかありますが、ファイルに存在する必要がある属性がいくつかあ ります。

必要な値を持つWebbridgeメタデータの例:

1. entityID:これは、Webbridge3サーバアドレス(FQDN/ホスト名)と、ユーザのブラウザが 到達可能な関連ポートです。



注:単一のURLを使用する複数のWebbridgeがある場合、これはロードバランシン グアドレスである必要があります。

- Location:これは、WebbridgeアドレスのHTTP-POST AssertionConsumerServiceが存在す る場所です。これは、サインイン後に認証されたユーザをリダイレクトする場所をIdPに指 示するものです。これは、idpResponse URL:<u>https://<WebbridgeFQDN>:<port>/api/auth/sso/idpResponse</u>に設定する必要があります 。たとえば、https://join.example.com:443/api/auth/sso/idpResponse に保存します。
- 3. オプション:署名用の公開キー:これは署名用の公開キー(証明書)であり、WebbridgeからのAuthRequestを確認するためにIdPによって使用されます。これは、IdPが公開キー(証明書)を使用して署名を検証できるように、WebbridgeにアップロードされたSSOバンドルの秘密キー「sso_sign.key」と一致している必要があります。展開内の既存の証明書を使用できます。 証明書をテキストファイルで開き、その内容をWebbridgeメタデータファイルにコピーします。 sso_xxxx.zipファイルで使用されている証明書と一致するキーをsso_sign.keyファイルとして使用します。

4. オプション:暗号化用の公開キー:これは、Webbridgeに返信されるSAML情報を暗号化す るためにIdPで使用する公開キー(証明書)です。これは、WebbridgeがIdPによって返信さ れたものを復号化できるように、WebbridgeにアップロードされたSSOバンドルの秘密キー 「sso_encrypt.key」と一致する必要があります。 展開内の既存の証明書を使用できます。 証明書をテキストファイルで開き、その内容をWebbridgeメタデータファイルにコピーしま す。 sso_xxxx.zipファイルで使用されている証明書と一致するキーをsso_encrypt.keyファ イルとして使用します。

オプションの公開キー(証明書)データを使用してIdPにインポートされるWebbridgeメタデ ータの例:



0

アイデンティティプロバイダー(IdP)へのWebbridgeのメタデータ のインポート

適切な属性を使用してメタデータXMLが作成されたら、ファイルをMicrosoft ADFSサーバにイン ポートして、証明書利用者信頼を作成できます。

1. ADFSサービスをホストしているWindowsサーバーへのリモートデスクトップ

2. AD FS管理コンソールを開きます。このコンソールには、通常、サーバーマネージャーからア クセスできます。



3. ADFS管理コンソールが表示されたら、左側のペインでADFS > Trust Relationships > Relying Party Trustの順に移動します。



4. ADFS管理コンソールの右側のウィンドウで、[証明書利用者信頼の追加…]オプションを選択します。



5. この選択を行うと、証明書利用者信頼の追加ウィザードが開きます。Start オプションを選択します。

\$ 3	Add Relying Party Trust Wizard	x
Welcome		
Steps Welcome Select Data Source Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Welcome to the Add Relying Party Trust Wizard This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions. The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.	8
	< Previous Start Cancel	

6. [データソースの選択]ページで、[ファイルから証明書利用者に関するデータをインポートする]のオプションボタンを選択し、[参照]を選択して、Webbridgeメタデータファイルの場所に移動します。

		_
\$	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 	Insect data shout the relation party of blocked colors or on a local petund;	
Select Data Source	Use this option to import the necessary data and certificates from a review network.	iehae
 Configure Multifactor Authentication Now? 	its federation metadata address foot pame or URL):	
 Choose Issuance Authorization Rules 	Educidade aduress (nos name or onic).	
 Ready to Add Trust 	Example: fs.contoso.com or https://www.contoso.com/app	
 Finish 	Impgt 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 validate the source of the file. Eederation metadata file location:	not
	C:\MetaData\wb3_config.xml Browse	B
	 Enter data about the relying party manually Use this option to manually input the necessary data about this relying party organization. 	
	< Previous Next > Cance	si 🛛

7.「表示名の指定」ページで、ADFSのエンティティに対して表示される名前を入力します(表示名はADFS通信にサーバー目的ではなく、単に情報を提供するためのものです)。

\$	Add Relying Party Trust Wizard	x
Specify Display Name		
Steps	Enter the display name and any optional notes for this relying party.	
Welcome	Display name:	
Select Data Source	Webbridge CMS SSO	
Specify Display Name	Ngtes:	
 Configure Multifactor Authentication Now? 	This is the relying trust part for CMS SSO with WebApp	^
 Choose Issuance Authorization Rules 		
Ready to Add Trust		
 Finish 		<u> </u>
	< Previous Next > Cance	ł.

8. 「Configure Multi-factor Authentication Now?」ページで、デフォルトのままにして「Next」を 選択します。

\$	Add Relying Party Trust Wizard
Steps Welcome Select Data Source Specify Display Name Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Configure multifactor authentication settings for this relying party trust. Multifactor authentication is required if there is a match for any of the specified requirements. Multifactor Authentication Global Settings Requirements Users/Groups Not configured Device Not configured Location Not configured
	I do not want to configure multifactor authentication settings for this relying party trust at this time. Configure multifactor authentication settings for this relying party trust. You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see <u>Configuring Authentication Policies</u> .

9. [Choose Issuance Authorization Rules]ページで、[Permit all users to access this relying party]を選択したままにします。



10. 信頼を追加する準備の完了ページで、Webbridgeの証明書利用者信頼のインポートされた詳細 をタブで確認できます。WebbridgeサービスプロバイダーのURLの詳細については、IDとエンド ポイントを確認します。



11. [完了] ページで、[閉じる]オプションを選択してウィザードを閉じ、要求ルールの編集を続行 します。



IdPでのWebbridgeサービスのクレームルールの作成

Webbridge用に証明書利用者信頼が作成されたため、SAML応答でWebbridgeに提供される発信要 求タイプに特定のLDAP属性を一致させるために要求規則を作成できます。

1. ADFS管理コンソールで、Webbridgeの証明書利用者信頼を強調表示し、右側のペインで要求 規則の編集を選択します。



2. <DisplayName>の[要求ルールの編集]ページで、[ルールの追加…]を選択します。

Edit Claim Rules for Webbridge3	- 🗆 X
Issuance Transform Rules Issuance Authorization Rules Delegation A	uthorization Rules
The following transform rules specify the claims that will be sent to the	elying party.
Order Rule Name Issued Claims	
1 Webbridge3 uid	
	+
Add Rule Edit Hule Remove Hule	
UK	Apply

3. Add Transform Claim Rule Wizardページで、Claim Rule templateオプションに対してSend LDAP Attributes as Claimsを選択し、Nextを選択します。

S	Add Transform Claim Rule Wizard	×
Select Rule Template		
Steps Choose Rule Type	Select the template for the claim rule that you want to create from the following list. The description provid details about each claim rule template.	es
 Configure Claim Rule 	Claim rule template: Send LDAP Attributes as Claims Claim rule template description: Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute	
	store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to creat a rule that will extract attribute values for authenticated users from the displayName and telephoneNumb Active Directory attributes and then send those values as two different outgoing claims. This rule may als be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.	e er io
	< Previous Next > Cancel	

- 4. 要求規則の構成ページで、証明書利用者信頼の要求規則を次の値で構成します。
 - 1. クレームルール名 = ADFSでルールに指定する名前である必要があります(ルール参照のみ)
 - 2. 属性ストア= Active Directory
 - 3. LDAP属性 = Callbridge APIのauthenticationIdMappingと一致している必要があります(例: \$sAMAccountName\$)。
 - 4. 発信クレームタイプ =これは、Webbridge SSO config.json内のauthenticationIdMappingと一 致する必要があります。(たとえば、uid)。

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim r	ule name:		
Webb	ridge3		
Rule to	emplate: Send LDAP Attributes as Claims		
Antoha	te store.		
Active	Directory	~	
Mappi	ng of LDAP attributes to outgoing claim type	5C	
	LDAP Attribute (Select or type to add more)	Outgoing Claim Ty	pe (Select or type to add more)
۶.	SAM-Account-Name V	uid	~
*			×
Vew	Rule Language		OK Cancel

Webbridge用のSSOアーカイブZIPファイルを作成します。

この設定は、サポートされているドメインや認証マッピングなどのSSO設定を検証するために Webbridgeが参照するものです。設定のこの部分では、次のルールを考慮する必要があります。

- ZIPファイルは、ファイル名の前にsso_を付けて開始する必要があります(たとえば、 sso_cmstest.zip)。
- このファイルがアップロードされると、Webbridgeは基本認証を無効にし、アップロードさ れたWebbridgeに対してSSOのみを使用できます。
- ・ 複数のIDプロバイダーを使用している場合は、異なる命名スキーマを使用して(sso_のプレ

フィックスを付けたまま)個別のZIPファイルをアップロードする必要があります。

• zipファイルを作成するときは、ファイルの内容を強調表示してzip圧縮し、必要なファイル をフォルダに配置してそのフォルダをzipしないでください。

zipファイルの内容は、暗号化が使用されているかどうかによって、2 ~ 4ファイルで構成されます。

filename	説明	必要 ?
idp_config.xml	これは、idPが収集できるMetaDataファイルです。ADFSでは、 <u>https://<adfsfqdn>/FederationMetadata/2007-</adfsfqdn></u> <u>06/FederationMetadata.xml</u> に移動して、これを見つけることができま す。	はい
config.json	これは、Webbridgeがサポートされているドメイン、SSOの認証マッ ピングを検証するために使用するJSONファイルです。	はい
sso_sign.keyキー	これは、IDプロバイダーで構成された公開署名キーの秘密キーです。 署名されたデータのセキュリティ保護にのみ必要	NO
sso_encrypt.key(暗 号化キー)	これは、IDプロバイダーで構成された公開暗号化キーの秘密キーです 。暗号化されたデータのセキュリティ保護にのみ必要	NO

idp_config.xmlを取得および設定します

1. ADFSサーバ(またはADFSにアクセスできる場所)で、Webブラウザを開きます。

2. WebブラウザでURL <u>https://<ADFSFQDN>/FederationMetadata/2007-</u> <u>06/FederationMetadata.xml</u>を入力します(ADFSサーバでローカルに操作する場合は、FQDNの 代わりにlocalhostを使用することもできます)。 これにより、ファイル FederationMetadata.xmlがダウンロードされます。

		S New Tab	×	+
$\ \ \leftarrow \ \ \rightarrow \ \ G$	i) adfs.brhuff.c	om/FederationMetadata/2007-06/FederationMetadata.xml		7
	-			Gma
🖭 Federatio	onMetadaxml 🗠			

3. ダウンロードしたファイルをzipファイルを作成する場所にコピーし、名前をidp_config.xmlに 変更します。

		SSOconfig
	Name	^
	Config.json FederationMetad	ata.xml
	Open	
	Edit	
E	Share with Skype	
۲ 🗧	Move to OneDrive	
4	7-Zip	>
	CRC SHA	>
	Edit with Notepad++	
K	9 Share	
	Open with	>
1	Cisco AMP For Endpoints	>
	Restore previous versions	
-	Send to	>
1 -	Cut	
	Сору	
	Create shortcut	
	Delete	
	Rename	
	Properties	

Local Disk (D:) > brentssoconfig > SSOconfig



コンテンツを含むconfig.jsonファイルの作成

config.jsonには次の3つの属性が含まれており、これらは角カッコ{}で囲む必要があります。

- supportedDomains:IdPに対してSSO認証がチェックされるドメインのリストです。複数のドメインはカンマで区切ることができます。
- authenticationIdMapping:これは、ADFS/IdPから出力要求ルールの一部として返されるパラメータです。これは、IdPの出力要求の種類の名前の値と一致する必要があります。クレームルール:
- 3. ssoServiceProviderAddress:これは、識別プロバイダーがSAML応答を送信する先の FQDN URLです。これはWebbridgeのFQDNである必要があります。



sso_sign.keyの設定(オプション)

このファイルには、IdPにインポートされたWebbridgeメタデータでの署名に使用される証明書の 秘密キーが含まれている必要があります。署名に使用する証明書は、ADFSでのWebbridgeメタデ ータのインポート中に、<KeyDescriptor use=signing>セクションの下の証明書情報を使用して X509Certificateを設定することで設定できます。また、ADFSのWebbridge Relying Trust Partyの Properties > Signatureで表示(およびインポート)することもできます。

次の例では、ADFSにインポートされる前にWebbridgeメタデータに追加されたcallbridge証明書 (CN=cmscb3.brhuff.local)を確認できます。sso_sign.keyに挿入された秘密キーは、 cmscb3.brhuff.local証明書と一致する秘密キーです。

これはオプションの設定であり、SAML応答を暗号化する場合にのみ必要です。



sso_encrypt.keyを設定します(オプション)。

このファイルには、IdPにインポートされたwebbridgeメタデータ内の暗号化に使用される証明書 の秘密キーが含まれている必要があります。暗号化に使用される証明書は、ADFSでの Webbridgeメタデータのインポート中に、<KeyDescriptor use=encryption>セクションの下の証明 書情報を使用してX509Certificateを設定することで設定できます。また、ADFSのWebbridge証明 書利用者信頼パーティのProperties > Encryptionで表示(およびインポート)することもできます。

次の例では、ADFSにインポートされる前にWebbridgeメタデータに追加されたcallbridge証明書 (CN=cmscb3.brhuff.local)を確認できます。「sso_encrypt.key」に挿入された秘密キーは、 cmscb3.brhuff.local証明書と一致する秘密キーです。

これはオプションの設定であり、SAML応答を暗号化する場合にのみ必要です。



SSO ZIPファイルの作成

1. SSO設定ファイルに使用するすべてのファイルを強調表示します。





注意:ファイルが含まれているフォルダは圧縮しないでください。圧縮すると、SSOが 機能しなくなります。

2. ハイライトファイルを右クリックし、Send to > Compressed (zip)フォルダを選択します。

	Name		^	
:ess	📓 config.json			
ade at	idp_config.xml			
Move to On	eDrive		<u> </u>	
7-Zip		>		
CRC SHA		>		
Edit with Not	tepad++			
Share				
Cisco AMP F	or Endpoints	>		
Send to		>	0	Bluetooth device
Cut				Compressed (zipped) folder
Сору				Desktop (create shortcut)
Create short	cut	_	E	Documents

3. ファイルを圧縮した後、sso_プレフィクスを使用して目的の名前にファイル名を変更します。

Name

🔟 config.json	
🔟 idp_config.xml	
sso_encrypt.key	
sso_sign.key	
sso_testfile.zip	

WebbridgeへのSSO Zipファイルのアップロード

SFTP/SCPクライアントを開き(この例ではWinSCPが使用されています)、Webbridge3をホストするサーバに接続します。

1. 左側のペインで、SSO Zipファイルが存在する場所に移動し、右クリックしてアップロードを 選択するか、ファイルをドラッグアンドドロップします。

iame	Size	Туре	<u>^</u>	Changed	Name
- -		Parent die	ectory	3/30/2021 9:44:49 PM	s
ar sso_cmscb3.zin	A.KR	7IP File		3/30/2021 12:58:22 PM	Ez logbundle.tar.
🔛 Ope	n				log
📝 Edit		•			fibus 🗍
Uple	vad	ES •	🔒 U	pload	Ne.json
🗙 Dele	te.	F8	😭 U	pload in Background	cms.lic
nd Ren	ame	F2	(a) U	pload and Delete F6	Mark boot json
File	Custom Com	mands +	-		keytest.key
File	Names	,			keytest.csr
De Proc	oerties	F9	1		admin-a-202104
Sust	em Menu				onecert.key
400			1		anecert.csr

2. ファイルが完全にWebbridge3サーバにアップロードされたら、SSHセッションを開いてコマン ドwebbridge3 restartを実行します。

cmscb3>	webbridge3 restart
SUCCESS:	HTTPS Key and certificate pair match
SUCCESS:	HTTPS full chain of certificates verifies correctly
SUCCESS:	C2W Key and certificate pair match
SUCCESS:	C2W full chain of certificates verifies correctly
SUCCESS:	Webbridge3 enabled
cmscb3>	

3. syslogで、次のメッセージはSSOのイネーブルが成功したことを示します。

client_backend:	INFO :	SamlManager : Attempting to configure SSO information from:sso_cmscb3.zip	
client_backend:	INFO :	SamlManager : Successfully saved config.json to ./FWD04e/config.json	
client backend:	INFO :	SamlManager : Successfully saved idp_config.xml to ./FWDo4e/idp_config.xml	
client_backend:	INFO :	SamlManager : Validated signing idp credential: /CN=ADFS Signing - adfs.brhuff.com	
client backend:	INFO :	SamlManager : SAML SSO configured, entityId:http://adfs.brhuff.com/adfs/services/trust	

共通アクセスカード(CAC)

共通アクセスカード(CAC)は、現役の軍関係者、DoDの民間従業員、および適格な契約作業員の 標準IDとして機能するスマートカードです。

CACカードを使用するユーザのサインインプロセス全体を次に示します。

- 1. PCの電源を入れ、CACカードに貼り付けます
- 2. ログインし(証明書を選択する場合もあります)、Pinを入力します。
- 3. ブラウザを開く
- 4. 参加URLに移動し、会議に参加またはサインインオプションを確認します
- 5. サインイン: jidMappingとして設定されているユーザ名を入力します。Active DirectoryはCACログインから要求されます。

- 6. サインインを押す
- 7. ADFSページが短時間表示され、自動的に入力されます
- 8. ユーザはこの時点でログインします。



ADFSがCACカードに使用するものと同じ方法で、jidMapping(これはユーザのサインイン名)をLdapmappingに設定します。 \$userPrincipalName\$など(大文字と小文字が区別されます)

また、ADFSのクレームルールで使用されている属性と一致するように、 authenticationIdMappingに同じLDAP属性を設定します。

このクレームルールは、\$userPrincipalName\$をUIDとしてCMSに返信することを示しています。

Iss	Edit Ru	le - webbridge sso		×									
1	You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.												
	Claim ru	le name:											
	webbrid	dge sso											
	Rule ter	nplate: Send LDAP Attributes as Claims											
	Attribute	store:											
	Active	Directory		*									
	Mappin	g of LDAP attributes to outgoing claim types	¢										
		LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Sele	ct or type to add more)									
	F.	User-Principal-Name v	uid	~									
	•	~		~									

T

WebApp経由のSSOログインのテスト

SSOの設定が完了したので、サーバをテストできます。

1. WebアプリケーションのWebbridge URLに移動し、Sign inボタンを選択します。



2. ユーザーには、ユーザー名を入力するオプションが表示されます(このページにはパスワード ・オプションがないことに注意してください)。



3. 次に、ユーザはADFSページにリダイレクトされます(ユーザ詳細の入力後)。ここで、ユー ザはIdPに対して認証するためにクレデンシャルを入力する必要があります。

adfs.brhuff.com/adfs/ls/		Ŕ
	Brhuff SSO	
	Sign in with your organizational account	
	someone@example.com	
	Password	
	Sign in	

4. ユーザーは、IdPを使用してクレデンシャルを入力および検証した後、Web Appホームページ にアクセスするためのトークンでリダイレクトされます。

meet.brhuff.local/en-US/portal	neet.brhuff.local/en-US/portal								
٠ (
Guest/Host Space									
Guest/HostSameURland	John Doe's Home								
Guest/HostUniqueURland	Last login 2021-05-04 at 18:08. See details								
John Doe's Space	Join a meeting								

トラブルシューティング

基本的なトラブルシューティング

SSO問題の基本的なトラブルシューティングの場合:

- 1. IdPの証明書利用者信頼としてインポートするために使用されるWebbridge3用に構築された メタデータが正しく設定されていること、および設定されたURLがconfig.json内の ssoServiceProviderAddressと正確に一致することを確認します。
- 2. IdPから提供され、Webbridge3 ssoコンフィギュレーションファイルに圧縮されたメタデー タが、IdPから取得した最新のメタデータであることを確認します。これは、サーバのホス ト名や証明書などに変更があった場合と同様で、再エクスポートしてコンフィギュレーショ ンファイルに圧縮する必要があります。
- 著名と暗号化の秘密キーを使用してデータを暗号化する場合は、正しい一致キーが webbridgeにアップロードしたsso_xxxx.zipファイルに含まれていることを確認します。可 能であれば、オプションの秘密キーなしでテストを行い、この暗号化オプションなしで SSOが機能するかどうかを確認します。
- 4. SSOドメインの正しい詳細、Webbridge3 URL、およびSAMLResponseから一致する予想される認証マッピングを使用してconfig.jsonが設定されていることを確認します。

また、ログの観点からトラブルシューティングを試みることも理想的です。

- 1. Webbridge URLに移動するときに、CMS syslogの詳細なロギングを有効にするには、 URLの最後に?trace=trueを配置します。(例:<u>https://join.example.com/en-</u> <u>US/home?trace=true</u>)。
- Webbridge3サーバでsyslog followを実行して、テスト中にライブキャプチャを行うか、 URLにtraceオプションを追加してテストを実行し、Webbridge3およびCMS Callbridgeサー バからlogbundle.tar.gzを収集します。 webbridgeとcallbridgeが同じサーバにある場合、単 ーのlogbundle.tar.gzファイルだけが必要です。

Microsoft ADFS障害コード

場合によっては、SSOプロセスに障害が発生し、IdP設定またはIdPとの通信に障害が発生する可 能性があります。ADFSを使用する場合は、次のリンクを確認して障害が発生しているかどうか を確認し、修復アクションを実行するのが理想的です。

<u>Microsoftステータスコード</u>

client_backend:エラー:SamlManager:SAML認証要求_e135ca12-4b87-4443-abe1-30d396590d58が次の理由で失敗しました:urn:oasis:names:tc:SAML:2.0:status:Responder

このエラーは、前のドキュメントによると、IdPまたはADFSが原因でエラーが発生したため、解 決するにはADFSの管理者による処理が必要であることを示します。

認証IDを取得できませんでした

SAMLResponseをIdPから元に戻す交換中に、Webbridgeがログに次のエラーメッセージを表示し、SSO経由でのログインに失敗する場合があります。

client_backend:情報:SamlManager: [57dff9e3-862e-4002-b4fa-683e4aa6922c] Failed obtaining an authenticationId

これは、認証交換中にIdPから返されたSAMLResponseデータを確認する際に、Webbridge3が authenticationIdのconfig.jsonと比較して、応答に有効な照合属性を見つけられなかったことを示 します。

通信が署名と暗号化の秘密キーを使用して暗号化されていない場合、SAML応答はWebブラウザ 経由でDeveloper Tools Network Loggingから抽出し、base64を使用してデコードできます。応答 が暗号化されている場合は、IdP側から復号化されたSAML応答を要求できます。

開発者ツールのネットワークロギング出力はHARデータとも呼ばれ、name列の下で idpResponseを探し、Payloadを選択してSAML応答を確認します。 前述したように、これは base64デコーダを使用してデコードできます。

				_							
Name	•	X Headers	Payload	Preview	Response	Initiator		Cook			
			<u> </u>	_							
illustration.png?id=183128		Form Data	view sour	rce viev	w URL-encod	ed					
webclient-infield.html		SAMLRespo	nse: PHNhb	Wxw01J1c38	BvbnNlIE1EP	SJFYTEwYj	1iYmIt01	gz0500	MDIyLWFmNT	ctNjdkYTYwY	2E4N2I1IIIWZ
🗊 ls/		XJzaW9uPSI	y LjAiIEl zo	3V1SW5zdG	FudD0iMjAy	hyðwNiðwN\	/QxNzoz0	DozMC4	1NjVaIiBEZ)	KN0aW5hdG1v	oj0iaHR0cH <mark>M</mark> 6L
💷 runtime.js		y9tZWV0LmJ	yaHVmZi5st	2NhbDo0ND	MvYXBpL2F1	dGgvc3NvL2	21kcFJ1c	38vbnN	lIiBDb25zZ	W50PSJ1cm46	o2FzaXM6beFtZ
3.chunk.js		XM6dGM6U0F	NTDoyLjA6Y	29uc2VudD	p1bnNwZWNp	ZmllZCIgSW	15SZXNwb	25zZVR	PSJFOWIXY	jgzYzYtZWUxI	Ni00Zjk3Lk <mark>Fm</mark> M
💷 61.chunk.js		WQtZDQwNTc	yowm2zgmy1	iB4bWxucz	pzYW1scD0i	dXJuOm9hc2	21zOm5hb	WzOnR	j01NBTUw6M	i4wOnByb3Rv	(29sIj48SX <mark>N</mark> zd
🖾 infield.chunk.js		WVyIHhtbG5	zPSJ1cm46b	2FzaXM6bm	FtZXM6dGM6	JØFNTDoyL	jA6YXNzZ	XJ0aW9	uIj5odHRwO	i8vYWRmcy5i	mh1ZmYuY29tL
🗐 idpResponse		2FkZnMvc2V	ydmljZXMvd	HJ1c3Q8L0	lzc3Vlcj48	c2FtbHA6U	BRhdHVzP	jxzYW1	scDpTdGF0d	XNDb2R11FZh	oHV1PSJ1cr 46b
C faviconico		2FzaXM6bmF	tZXM6dGM6l	ØFNTDoyLj	A6c3RhdHVz	DIN1Y2N1c	3MiIC8+P	C9zYW1	scDpTdGF0d)	KM+PEVuY3J5	:HR1ZEFzc2Vyd
meet.brhuff.local		GlvbiB4bWx	ucz0idXJu0	m9hc21zOm	5hbWzOnRj	D1NBTUw6Mi	i4wOmFzc	2VydG1	vbiI+PHhlb	mM6RW5jcnlw	IGVkRGFØYS <mark>8</mark> Ue
unsupp.css		XB1PSJodHR	wOi8vd3d3l	.nczLm9yZy	8yMDAxLzA0	L3htbGVuYy	NFbGVtZ	W50IiB4	4bWxuczp4ZI	w5jPSJodHRw	Di8vd3d3LnczL
meeting.2df79b17ca8cd955		∎9yZy8yMDA	xLzA0L3htb	GVuYyMiPj	x4ZW5jOkVu	Y3J5cHRpb2	25NZXRob	2QgQWx	nb3JpdGhtP	SJodHRw0i8v	13d3LnczL <mark>r</mark> 9yZ
💷 modernizr.eb6230209009ce		y8yMDAxLzA	0L3htbGVuY	yNhZXMyNT	YtY2JjIiAv	PjxLZX1Jbm	ZvIHhtb	G5zPSJ	odHRwOi8vd	3d3LnczLm9y	Zy8yMDAwLzA5L
💷 vendors~meeting.07098caf		3htbGRzaWc	jIj48ZTpFt	mNyeX80ZW	RLZXkgeG1s	bnM6ZT0iaH	RØcDovL	3d3dy5	3My5vcmcvM	jAwMS8wNC94	oWxlbmMjIj <mark>4</mark> 8Z
meeting.2ddfb54d3ef4fe7e		TpFbmNyeXB	0aW9uTWV0a	G9kIEFsZ2	9yaXRobT0i	aHRØcDovL	3d3dy53M	y5vcmc	vMjAwMS8wN	C94bWx1bmMj	nNhLW9hZXAtb
🖸 unsupp.js		WdmMXAiPjx	EaWdlc3RN2	XRob2QgQW	xnb3JpdGht	PSJodHRwO	i8vd3d3L	nczLm9	yZy8yMDAwL	zA5L3htbGRz	Wcjc2hhMS <mark>IgL</mark>
= sign_in_background.jpg		z48L2U6RW5	jcnlwdGlvt	k11dGhvZD	48S2V5SW5m	bz48ZHM6WC	OUwOURhd	GEgeG1	sbnM6ZHM9I	nhØdHA6Ly93	13cudzMub3)nL
📼 sian in Ioao.nna	•	zIwMDAvMDk	veG1sZHNp2	yMiPjxkcz	pynta55XNz	dWyU2Vyak	FsPjxkc	ZPYNTA	5SXNzdWVyTr	mFtZT5DTj1i	:mh1ZmYtQLQyM
257 requests 26.2 MB transferr		DEVLUNBLCB	EOzlicmh12	mYsIERDPW	xvY2FsPC9k	czpYNTA5S)	(NzdWVyT	mFtZT4	8ZHM6WDUw0	VN1cm1hbE51	wJlci4xMzM4M

SAMLResponseデータを受信する場合は、<AttributeStatement>のセクションを確認して返信される属性名を見つけます。このセクション内には、設定されてIdPから送信される要求タイプがあります。例:

<属性ステートメント> <Attribute Name="<u><共通名のURL</u>"> <AttributeValue>testuser1</AttributeValue> </属性> <Attribute Name="<u><NameIDのURL</u>"> <Attribute Name="<u><NameIDのURL</u>"> <AttributeValue>testuser1</AttributeValue> </属性> <Attribute Name="uid"> <Attribute Name="uid"> <AttributeValue>testuser1</AttributeValue> </属性> </AttributeStatement>

前の名前を確認すると、Attribute Statementセクションの下の<AttributeName>を調べて、それぞれの値をSSO config.jsonのauthenticationIdmappingセクションで設定した値と比較できます。

前の例では、authenticationIdMappingの設定が渡された内容と正確に一致せず、一致する authenticationIdを見つけられなかったことを確認できます。

認証IDマッピング:<u>http://example.com/claims/NameID</u>

この問題を解決するには、次の2つの方法があります。

- Webbridge3のconfig.jsonのauthenticationIdMappingで設定されている内容と正確に一致 する一致するクレームを持つように、IdP送信クレームルールを更新できます。 (<u>http://example.com/claims/NameID</u>のIdPに追加されたクレームルール) または
- Webbridge3でconfig.jsonを更新して、「authenticationIdMapping」が、IdPで設定され た出力要求ルールの1つとして正確に一致するようにできます。(つまり、「uid」、「 <URL>/NameID」、または「<URL>/CommonName」のいずれかの属性名に一致する ように更新される「authenticationIdMapping」です。渡されたときにCallbridge APIで 設定された期待値と(正確に)一致する限り)

検証でアサーションが渡されない/一致しない

IdPからのSAMLResponseの交換中に、アサーションの照合に失敗したことを示す次のエラーが Webbridgeで表示され、サーバ設定に一致しないアサーションがスキップされることがあります 。

client_backend:エラー: SamlManager:検証に合格したアサーションがありません client_backend: INFO : SamlManager :許可された対象ユーザー内に存在しないアサーショ ンをスキップしています

このエラーが示しているのは、IdPからSAMLResponseを確認する際に、Webbridgeが一致するア サーションを見つけられなかったため、一致しない障害をスキップし、最終的に失敗したSSOロ グインが発生したことです。

この問題を特定するには、IdPからSAMLResponseを確認することが理想的です。 通信が署名と 暗号化の秘密キーを使用して暗号化されていない場合、Webブラウザ経由でDeveloper Tools Network LoggingからSAML応答を抽出し、base64を使用してデコードできます。応答が暗号化さ れている場合は、IdP側から復号化されたSAML応答を要求できます。

SAMLResponseデータを調べる際は、応答の<AudienceRestriction>セクションを見ると、この応 答が制限されているすべての対象ユーザを確認できます。

<条件NotBefore=2021-03-30T19:35:37.071Z NotOnOrAfter=2021-03-30T19:36:37.071Z> <対象者制限> <Audience><u>https://cisco.example.com</Audience</u>> </AudienceRestriction> </条件>

<Audience>セクション(<u>https://cisco.example.com)</u>)の値を使用して、Webbridge設定の config.json内のssoServiceProviderAddressと比較し、完全に一致するかどうかを検証できます。 この例では、「Audience does NOT MATCH the Service provider address in the configuration」が 原因でエラーが発生したことがわかります。これは、このアドレスの末尾に「:443」が追加され ているためです。

ssoServiceProviderAddress:https://cisco.example.com:443

このような障害が発生しないようにするには、これらの間で完全に一致する必要があります。この例では、次の2つの方法のいずれかが修正されます。

1. config.jsonのssoServiceProviderAddressセクションのアドレスから:443を削除して、IdPの SAMLResponseで提供されるAudienceフィールドに一致するようにできます。 または

2. IdP内のWebbridge3のメタデータOR証明書利用者信頼は、URLに:443が追加されるように更新 できます(メタデータが更新されている場合は、ADFS上の証明書利用者信頼として再度インポー トする必要があります。ただし、IdPウィザードから直接証明書利用者信頼を変更する場合は、再 インポートする必要はありません)。

Webアプリでサインインに失敗しました:



user.info cmscb3-1 client_backend:INFO : SamlManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] SAMLトークン要求のSSO_2024.zipと一致

3月19日10:47:07.927 user.info cmscb3-1 client_backend:INFO : SamlManager : [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] Attempting to find SSO in SAML Token Request

3月19日10:47:07.930 user.info cmscb3-1 client_backend:情報: SamlManager: [63cdc9ed-ab52-455c-8bb2-9e925cb9e16b] SAMLトークンが正常に生成されました

シナリオ2:

ユーザがwebbridgeサインインページのSSO zipファイルにないドメインを使用してサインインし ようとしました。 クライアントは、ユーザが入力したユーザ名のペイロードを含む tokenRequestを送信します。 Webbridgeは、ログイン試行をただちに停止します。

CMS Webbridgeトレース(?trace=trueが使用されている場合)

3月18日14:54:52.698 user.err cmscb3-1 client_backend: ERROR : SamlManager : Invalid SSO login attempt

3月18日14:54:52.698 user.info cmscb3-1 client_backend:INFO : SamlManager : [3f93fd14-f4c9-4e5e-94d5-49bf6433319e] SAMLトークン要求でSSOを検出できませんで した

3月18日14:54:52.698 user.info cmscb3-1 client_backend:INFO : SamlManager : [3f93fd14-f4c9-4e5e-94d5-49bf6433319e] Attempting to find SSO in SAML Token Request

シナリオ3:

ユーザが正しいユーザ名を入力し、SSOサインインページが表示されます。 ユーザはここに正 しいユーザ名とパスワードも入力しますが、「Sign in Failed」と表示されます

CMS Webbridgeトレース(?trace=trueが使用されている場合)

3月19日16:39:17.714 user.info cmscb3-1 client_backend:INFO : SamlManager :[ef8fe67f-685c-4a81-9240-f76239379806] SAMLトークン要求のSSO_2024.zipと一致

3月19日16:39:17.714 user.info cmscb3-1 client_backend:情報: SamlManager : [ef8fe67f-685c-4a81-9240-f76239379806] Attempting to find SSO in SAML IDP Response

3月19日16:39:17.720 user.err cmscb3-1 client_backend: ERROR : SamlManager : No authenticationId mapped element found in signed SAML Assertions

Mar 19 16:39:17.720 user.info cmscb3-1 client_backend: INFO : SamlManager : [ef8fe67f-685c-4a81-9240-f76239379806] Failed obtaining an authenticationID

シナリオ3の原因は、IdPのクレームルールで使用されているクレームタイプが、

webbridgeにアップロードされたSSO zipファイルで使用されるconfig.jsonファイルの authenticationIdMappingと一致していなかったことです。 WebbridgeはSAML応答を調 べ、属性名がconfig.jsonで設定されているものと一致することを想定しています。

2	Edit Ru	ile - Webbridge3	×								
	You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.										
	Claim n	ule name:									
	Webbr	idge3									
	Rule te	mplate: Send LDAP Attributes as Claims									
	Antonia										
	Actinout	e store:									
	Active	Directory									
	Mappin	ig of LDAP attributes to outgoing claim types:									
		LDAP Attribute (Select or type to add more) Outgoing Claim Type (Select or type to add more)									
	•	E-Mail-Addresses V E-Mail Address	v								
		~	~								

ADFSのクレームルール

🔚 hosts 🛙	3 🔚 o	onfig.json 🗵 🔚 idp_config.xml 🗵 🔚 new 1 🖾
1		
2		"authenticationIdMapping" : "uid",
3		"ssoServiceProviderAddress" : "https://meet.brhuff.local:443",
- 4		"supportedDomains" : ["brhuff.com"]
5	L)	

config.jsonの例

ユーザ名が認識されない

シナリオ1:

ユーザが誤ったユーザ名でサインインした(ドメインが、webbridge3にアップロードされたSSO zipファイルの内容と一 致するが、ユーザが存在しない)



ユーザ名が認識されない

user.info cmscb3-1 client_backend:INFO : SamlManager : [79e9a87e-0fa4-44df-a914bbcabb6c87c6] SAMLトークン要求のSSO_2024.zipと一致

3月18日14:58:47.777 user.info cmscb3-1 client_backend:INFO : SamlManager : [79e9a87e-0fa4-44df-a914-bbcabb6c87c6] Attempting to find SSO in SAML Token Request

3月18日14:58:47.780 user.info cmscb3-1 client_backend:情報: SamlManager: [79e9a87e-0fa4-44df-a914-bbcabb6c87c6]正常に生成されたSAMLトークン

3月18日14:58:48.072 user.info cmscb3-1 client_backend:INFO : SamlManager : [79e9a87e-0fa4-44df-a914-bbcabb6c87c6] SAMLトークン要求のSSO_2024.zipと一致

3月18日14:58:48.072 user.info cmscb3-1 client_backend:INFO : SamlManager : [79e9a87e-0fa4-44df-a914-bbcabb6c87c6] Attempting to find SSO in SAML IDP Response

3月18日14:58:48.077 user.info cmscb3-1 client_backend:情報: SamlManager: [79e9a87e-0fa4-44df-a914-bbcabb6c87c6]正常に認証IDを取得しました :darmckin@brhuff.com

Mar 18 14:58:48.078 user.info cmscb3-1 host:server:INFO : WB3Cmgr: [79e9a87e-0fa4-44df-a914-bbcabb6c87c6] AuthRequestReceived for connection id=64004556-faea-479f-aabe-691e17783aa5 registration=40a4026c-02 2a1-b125-136fdf5612a5 (user=steve@brhuff.com)

Mar 18 14:58:48.092 user.info cmscb3-1 host:server:INFO : no user found for authorization

3月18日14:58:48.092 user.info cmscb3-1 host:server:INFO: unsuccessful login request from steve@brhuff.com

シナリオ2:

ユーザがWebアプリに正しいサインイン情報を入力し、SSOページでLDAP認証のための正しい クレデンシャルを入力しましたが、ログインに失敗し、「Username is not recognized」と表示さ れます。



user.info cmscb3-1 client_backend:INFO : SamlManager : [d626bbaf-80c3-4286-8284-fac6f71eb140] SAMLトークン要求のSSO_2024.zipと一致

3月18日15:08:52.114 user.info cmscb3-1 client_backend:INFO : SamlManager : [d626bbaf-80c3-4286-8284-fac6f71eb140] Attempting to find SSO in SAML Token Request

3月18日15:08:52.117 user.info cmscb3-1 client_backend:情報: SamlManager: [d626bbaf-80c3-4286-8284-fac6f71eb140] SAMLトークンが正常に生成されました

3月18日15:08:52.386 user.info cmscb3-1 client_backend:INFO : SamlManager : [d626bbaf-80c3-4286-8284-fac6f71eb140] SAMLトークン要求のSSO_2024.zipと一致

3月18日15:08:52.386 user.info cmscb3-1 client_backend:INFO : SamlManager : [d626bbaf-80c3-4286-8284-fac6f71eb140] Attempting to find SSO in SAML IDP Response

3月18日15:08:52.391 user.info cmscb3-1 client_backend:情報: SamlManager: [d626bbaf-80c3-4286-8284-fac6f71eb140]認証ID:darmckin@brhuff.comを正常に取得しま した

Mar 18 15:08:52.391 user.info cmscb3-1 host:server:INFO : WB3Cmgr: [d626bbaf-80c3-4286-8284-fac6f71eb140] AuthRequestReceived for connection id=64004556-faea-479f-aabe-691e17783aa5 registration=40a4026c 272-42a1-b125-136fdf5612a5 (user=darmckin@brhuff.com)

Mar 18 15:08:52.399 user.warning cmscb3-1 host:server: WARNING : rejecting login attempt from user 'darmckin@brhuff.com' — authenticationId incorrect

3月18日15:08:52.412 user.info cmscb3-1 host:server:INFO: unsuccessful login request from darmckin@brhuff.com

CMS IdapmappingのAuthenticationIdMappingが、ADFSのクレームルールに使用される設定済み のLDAP属性と一致しません。次の行の「Successfully obtain authenticationID:darmckin@brhuff.com」は、ADFSにはActive Directoryから darmckin@brhuff.comを取得する属性で設定されたクレームルールがあることを示していますが 、CMS API > UsersのAuthenticationIDはがDARMCKINであることを示示しています。 CMS IdapMappingsでは、AuthenticationIDは\$sAMAccountName\$として設定されていますが、 ADFSのクレームルールは電子メールアドレスを送信するように設定されているため、これは一 致しません。

修正方法:

次のいずれかの操作を行います。

- 1. CMS Idapmapping内のAuthenticationIDをADFSのクレームルールで使用されている値と一 致するように変更し、新しい同期を実行します
- 2. ADFS要求ルールで使用されるLDAP属性を、CMS Idapmappingで設定されている属性と一 致するように変更します

Related objects: /api/v1/idapMappings							
Table view XML view							
Object configuration							
jidMapping	\$sAMAccountName\$@brhuff.com						
nameMapping	\$cn\$						
cdrTagMapping							
coSpaceNameMapping	\$cn\$'s Space						
coSpaceUriMapping	\$sAMAccountName\$.space						
coSpaceSecondaryUriMapping	\$extensionAttribute12\$						
coSpaceCallIdMapping							
authenticationIdMapping	\$sAMAccountName\$						

API LDAPマッピング

Object configuration	
userJid	darmckin@brhuff.com
name	Darren McKinnon
email	darmckin@brhuff.com
authenticationId	darmckin
userProfile	d5cd50e4-e423-4ba6-bd17-7492b9ba5eb3

APIユーザの例

Edit Ru	le - Webbridge3		>				
You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.							
Claim rule name:							
Webbr	Webbridge3						
Rule te	mplate: Send LDAP Attributes as Claims						
Attributi	e store:						
Activo	Directory		~				
Mappin	Manoing of LDAP attributes to outgoing claim types:						
	LDAP Attribute (Select or type to add more)		Outgoing Claim Type (Select or type to add more)				
۲.	E-Mail-Addresses	×	uid ~				
•		\sim	~				
View	Rule Language		OK Cancel				

ADFSからのクレームルール

Webbridgeログに示された作業ログの例。 結合URLで?trace=trueを使用して生成 された例:

3月18日14:24:01.096 user.info cmscb3-1 client_backend:INFO : SamlManager : [7979f13c-d490-4f8b-899c-0c82853369ba] SAMLトークン要求のSSO_2024.zipと一致

3月18日14:24:01.096 user.info cmscb3-1 client_backend:INFO : SamlManager : [7979f13c-d490-4f8b-899c-0c82853369ba] Attempting to find SSO in SAML IDP Response

3月18日14:24:01.101 user.info cmscb3-1 client_backend:INFO : SamlManager : [7979f13c-d490-4f8b-899c-0c82853369ba] Successfully obtain authenticationID:darmckin@brhuff.com

3月18日14:24:01.102 user.info cmscb3-1 host:server : 情報:WB3Cmgr: [7979f13cd490-4f8b-899c-0c82853369ba] AuthRequestReceived for connection id=64004556-faea-479f-aabe-691e17783aa5 registration=40a4026c-024 2a1-b125-136fdf5612a5 (user=darmckin@brhuff.com)

3月18日14:24:01.130 user.info cmscb3-1 host:server:INFO : successful login request from darmckin@brhuff.com

3月18日14:24:01.130 user.info cmscb3-1ホスト:サーバ:情報:WB3Cmgr: [7979f13cd490-4f8b-899c-0c82853369ba] issuing JWT ID e2a860ef-f4ef-4391-b5d5-9abdfa89ba0f

3月18日14:24:01.132 user.info cmscb3-1ホスト:サーバ:情報:WB3Cmgr: [7979f13cd490-4f8b-899c-0c82853369ba] sending auth response (jwt length=1064, connection=64004556-faea-479f-aabe-691e17783aa5)

3月18日14:24:01.133 local7.info cmscb3-1 56496041063b wb3_frontend: [Auth:darmckin@brhuff.com, Tracing:7979f13c-d490-4f8b-899c-0c82853369ba] 14.0.25.247 - [2024年3月18日: 18:24:01 +000] "ステータス0 POST /api/auth/sso/idpResponse HTTP/1.1" bytes_sent 0 http_referer " <u>https://adfs.brhuff.com/</u>" http_user_agent "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML、Geckoなど) Chrome/122.0.0.0 Safari/537.36" to upstream 192.0.2.2:9000: upstream_response_time 0.038 request_time 0.039 msec 1710786241.133 upstream_response_length 24 200

関連情報

シスコのテクニカルサポートとダウンロード

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。