

# ADFSへのメタデータファイルのインストール

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

このドキュメントでは、Microsoft Active Directory フェデレーション サービス (ADFS) にメタデータファイルをインストール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が推奨されます。

- ADFS
- セキュリティ管理アプライアンスとの Security Assertion Markup Language (SAML) 統合

### 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。

- SMA 11.x.x
- SMA 12.x.x

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。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。

## 背景説明

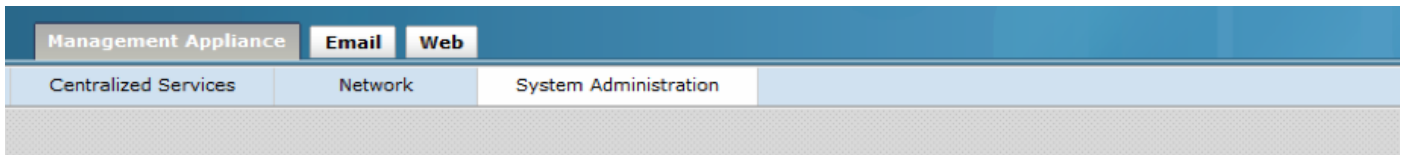
メタデータファイルを ADFS にインストールする前に、次の要件が満たされていることを確認してください。

- SMA で有効な SAML

- 組織で使用されているアイデンティティプロバイダーがCiscoコンテンツセキュリティ管理アプライアンスでサポートされているかどうかを確認します。サポートされているアイデンティティプロバイダーは次のとおりです。 Microsoft Active Directory フェデレーションサービス (ADFS) 2.0 Ping Identity PingFederate 7.2 Cisco Webセキュリティアプライアンス 9.1
- アプライアンスとIDプロバイダー間の通信を保護するために必要な次の証明書を取得します。アプライアンスでSAML認証要求に署名する場合、またはIDプロバイダーでSAMLアサーションを暗号化する場合は、信頼できる認証局(CA)と関連付けられた秘密キーから自己署名証明書または証明書を取得します。アイデンティティプロバイダーがSAMLアサーションに署名するには、アイデンティティプロバイダーの証明書を取得します。アプライアンスはこの証明書を使用して、署名されたSAMLアサーションを確認します

## 設定

ステップ1: SMAに移動し、図に示すように[System Administration] > [SAML] > [Download Metadata]を選択します。



### SAML

SP Profile Name	Entity ID	Assertion Consumer URL	Metadata	Delete
MyLab_SAML	sma.mexesa.com	https://sma.mexesa.com:83/	Download Metadata	

ステップ2 : お客様がADFSメタデータファイルをアップロードすると、アイデンティティプロバイダープロファイルが自動的に入力されます。MicrosoftのデフォルトURLは次のとおりです。  
<https://<ADFS-host>/FederationMetadata/2007-06/FederationMetadata.xml>

ステップ3 : 両方のプロファイルを設定したら、バグ [CSCvh30183](#) に従って、SPプロファイルメタデータを編集する必要 **があります**。図に示すように、メタデータファイルが表示されます。

```

1 <?xml version="1.0"?>
2 <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
3   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
4   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
5   entityID="sma.mexesa.com">
6   <SPSSODescriptor
7     AuthnRequestsSigned="false" WantAssertionsSigned="true"
8     protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
9     <KeyDescriptor use="signing">
10      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
11        <ds:X509Data>
12          <ds:X509Certificate>Bag Attributes
13            localKeyID: D5 4F B4 DA BC 91 71 5C 53 94 4A 78 E0 4A C3 EF C4 BD 4C 8D
14            friendlyName: sma.mexesa.com
15            subject=/C=MX/CN=sma.mexesa.com/L=CDMX/O=Tizoncito Inc/ST=CDMX/OU=IT Security
16            issuer=/C=MX/CN=sma.mexesa.com/L=CDMX/O=Tizoncito Inc/ST=CDMX/OU=IT Security
17            -----BEGIN CERTIFICATE-----
18            MIIDZTCCAk2gAwIBAwIJA0jXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHlxZAJBgNV
19            BAYTAK1YMRcwFQYDVQQDDA5zbWEubWV4ZXXNhLmNvbTENCMAwGA1UEBwwEQ0RNWDEW
20            MBQGA1UECgwNVG16b25jaXRvIEluYzENMAsGA1UECAwEQ0RNWDEUMBIGA1UECwwL
21            SVQGU2VjdXJpdHkwHhcNMjkwNjA1MjEwNTUxWWhcNMjAwNjA0MjEwNTUxWjByMQsw
22            CQYDVQQGEwJNWDEwXzEhLm1leGVzYS5jb20xDTALBgNVBACMBENE
23            TVGxVjAUBGNVBAoMDVRpem9uY210byBJbmMxDTALBgNVBAGMBENETVgxFDASBgNV
24            BAsMC0lUIFNlY3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
25            g7kzRmL114q9TlklcTJzo8cmscu5nRXFWlohFPcJgn/oHXEUkVUnWe+9cTJQ41X4
26            ojbGCP75UjD8GdPczkuBxqAZgkrfgNLR8mopsxTFVWb5x68tVsTBGFNyw8Wtd+Io
27            MVowJ9h9Kju7kSXuYHU1BYoxfPOLyzHHcbAVYKuPM4Fi7y4jwj6rnO4jtvPZp7B
28            cpWjawLlxAfUHVyvrC661Tblo0exG+hZ+AlS3B01+61mTNjF3IcGcGS/TE0chETx
29            glScUk0iMipnPEtAZey/ebyh18EpH/WViNwZkMUjINvmIFq3+LkF8As8B1Pm6YHi
30            L6K8W4vOEj1njtmnC/EQIQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB3vxNL7jb
31            emMTKSRP4hycUld69z2xGQC5e2EeyhnRgHUz7F/TEv0NkORotFii2oOJ6yGEOdWD
32            6+Bvj6wSBp7UoLyBdCcxglyi+vK4Y/R2+iCv13pyaXkbf0QsJvYpzOg7xSjkkZm79
33            +ZIJQkekyCAM5N0of1ZRrJ9oGD5qoYlZjhuD7NHmRBj7LKHrKsFVqpKet/tTXCH7
34            7EuB+ogT7pvrTDJ/QoIKcvYkbXuZ30JNVPxxKacjAVj/ZclXnPBGSMxexo277ECJq
35            ix5aXRSxOMRRtD/72FVRAsGT3x1mBYqu/HTyOBZongM+isJHBhRZxSOMBL+45jFY
36            PO1jBG5MZuWE
37            -----END CERTIFICATE-----
38          </ds:X509Certificate>
39        </ds:X509Data>

```

ステップ4：強調表示された情報を削除します。最後のメタデータファイルは、図に示すように指定する必要があります。

```
1 <?xml version="1.0"?>
2 <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
3   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
4   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
5   entityID="sma.mexesa.com">
6   <SPSSODescriptor
7     AuthnRequestsSigned="false" WantAssertionsSigned="true"
8     protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
9     <KeyDescriptor use="signing">
10      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
11       <ds:X509Data>
12        <ds:X509Certificate>
13        MIIDZTCCAk2gAwIBAwIJA0jXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHIXCzAJBgNV
14        BAYTAk1YMRcwFQYDVQQDDA5zbWEubWV4ZlZlLnVzTENMAAGAlUEBwwEQ0RNWDEW
15        MBQGA1UECgwNVG16b25jaXRvIEluYzENMAAGAlUECAwEQ0RNWDEUMBIGAlUECwwL
16        SVQGU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWWhcNMjAwNjA0MjEwNTUxWjByMQsw
17        CQYDVQQGEwJNWDEwMDVhLm1leGVzYS5jb20xDTALBgNVBAAcMBENE
18        TVGxFjAUBGNVBAoMDVRpem9uY210byBjBmMxDTALBgNVBAGMBENETVGxvFDASBgNV
19        BAsMC0lUIFNlY3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
20        g7kzRmL114q9TlklcTJzo8cmscu5nRXFWlohFpCJgn/oHXEUKvUnWe+9cTJQ41X4
21        ojbGCP75UjD8GdPczkuBxqAZgkrfgNLR8mopsxTFVWb5x68tVsTBGFNv8Wtd+Io
22        MVowJ9h9Kju7kSXuYHU1BYoxfPOLyzHHcbAVYKuPM4Fi7y4jwj6rnO4jtvPZPj7B
23        cpWjawLlxAfUHVvrc661Tblo0exG+hZ+AlS3B0l+6lmTNjF3IcGcGS/TE0chETx
24        glScUk0iMipnPEtAZey/ebyh18EpH/WViNwZkMUjINvmIFq3+LkF8As8B1Pm6YHi
25        L6K8W4vOEj1njtmnC/EQIQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB3vxNL7jb
26        emMTKSRP4hycUld69z2xGQC5e2EeyhnRgHUz7F/TEv0NkORotFii2oOJ6yGEOdWD
27        6+Bvj6wSBp7UoLyBdCxglyi+vK4Y/R2+iCv13pyaXkbF0QsJvYpzOg7xSjKxZm79
28        +ZIjQkekyCAM5N0of1ZRrJ9oGD5qoY1ZjhUd7NHmRBJ7LKHRSFVqpKet/tTXCH7
29        7EuB+ogT7pvrTDJ/QoIKcvYkbXuZ30JNVPxxKacjAVj/ZclXnPBGSMxex0277ECJq
30        ix5aXRSxOMRRtD/72FVRASgT3xlmBYqu/HTyOBZonGM+isJHBhRZxSOMBL+45jFY
31        PO1jBG5MZuWE
32        </ds:X509Certificate>
33      </ds:X509Data>
34    </ds:KeyInfo>
35  </KeyDescriptor>
36  <KeyDescriptor use="encryption">
37    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
38      <ds:X509Data>
39      <ds:X509Certificate>
40      MIIDZTCCAk2gAwIBAwIJA0jXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHIXCzAJBgNV
41      BAYTAk1YMRcwFQYDVQQDDA5zbWEubWV4ZlZlLnVzTENMAAGAlUEBwwEQ0RNWDEW
42      MBQGA1UECgwNVG16b25jaXRvIEluYzENMAAGAlUECAwEQ0RNWDEUMBIGAlUECwwL
43      SVQGU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWWhcNMjAwNjA0MjEwNTUxWjByMQsw
```

ステップ5 : 図に示すように、ADFSに移動し、編集したメタデータファイルを[ADFS Tools] > [AD FS Management] > [Add Relying Party Trust]にインポートします。

### Add Relying Party Trust Wizard

#### 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 certificates 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 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:

Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

< Previous    Next >    Cancel

ステップ6：メタデータファイルを正常にインポートした後、新しく作成した証明書利用者信頼の要求ルールを設定し、図に示すように[要求ルールテンプレート] > [LDAP属性の送信]を選択します。

### Add Transform Claim Rule Wizard

#### Select Rule Template

**Steps**

- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

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 create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also 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.

ステップ7：要求ルール名に名前を付け、[Attribute Store] > [Active Directory]を選択します。

ステップ8 : 図に示すように、LDAP属性をマッピングします。

- [LDAP Attribute] > [E-Mail-Addresses]
- [Outgoing Claim Type] > [E-Mail-Address]

**Add Transform Claim Rule Wizard**

### Configure Rule

**Steps**

- Choose Rule Type
- Configure Claim Rule

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: charella\_sma

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping 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	E-Mail Address
*		

< Previous Finish Cancel

ステップ9 : 図に示すように、この情報を使用して新しいカスタム要求ルールを作成します。

これは、カスタム要求ルールに追加する必要があるカスタムルールです。

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"] =>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] = "https://<smahostname>:83");
```

## Edit Rule - charella\_custom\_rule

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:

charella\_custom\_rule

Rule template: Send Claims Using a Custom Rule

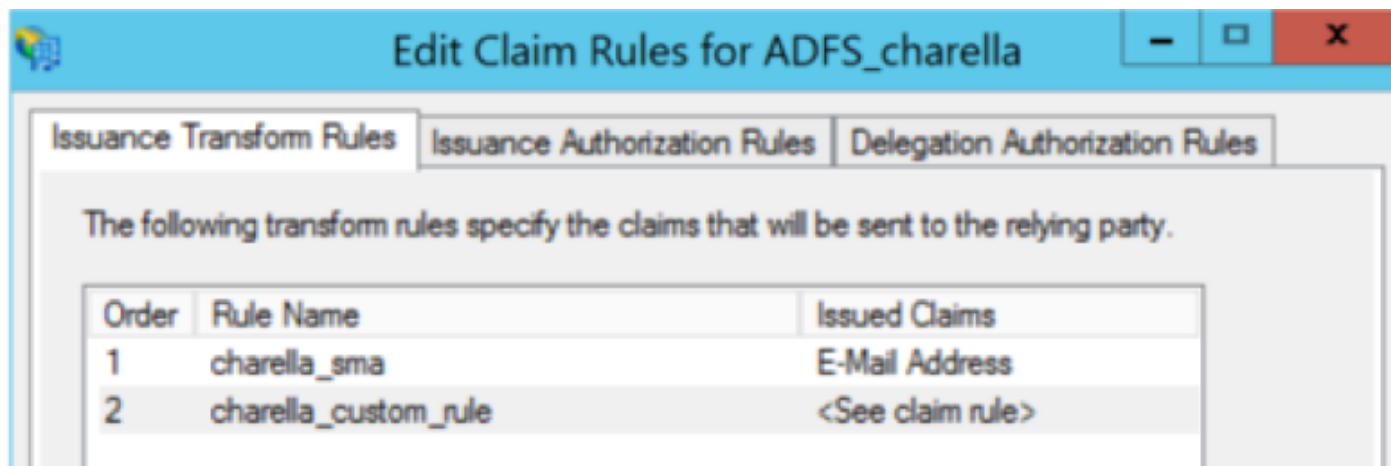
Custom rule:

```
c:[Type ==  
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]  
=> issue (Type =  
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",  
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value,  
ValueType = c.ValueType, Properties  
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",  
Properties  
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spname  
qualifier"] = "https://dh106-euq1.rl.ces.cisco.com/");
```

OK

Cancel

- SMAのホスト名とポートを使用して強調表示されたURLを変更します（CES環境では、ポートは不要ですが、euq1.<allocation>.iphmx.comをポイントする必要があります）
- ステップ10:[Claim rule order]が図に示すように、LDAP要求ルールが最初に、カスタム要求ルールが2番目に表示されます。



ステップ11:EUQにログインし、ADFSホストにリダイレクトする必要があります。

## 確認

現在、この設定に使用できる確認手順はありません。

## トラブルシューティング

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。

## 関連情報

- [CSCvh30183](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)