# Instalar archivo de metadatos en ADFS

# Contenido

Introducción Prerequisites Requirements Componentes Utilizados Antecedentes Configurar Verificación Troubleshoot Información Relacionada

#### Introducción

Este documento describe cómo instalar el archivo de metadatos en Microsoft Active Directory Federation Services (ADFS).

### Prerequisites

#### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- ADFS
- Integración del lenguaje de marcado de aserción de seguridad (SAML) con el dispositivo de administración de seguridad

#### **Componentes Utilizados**

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

#### Antecedentes

Antes de instalar el archivo de metadatos en el ADFS, asegúrese de que se cumplen estos requisitos:

- SAML habilitado en SMA
- Compruebe si el dispositivo de administración de seguridad de contenido de Cisco admite el proveedor de identidad utilizado por su organización. Estos son los proveedores de identidad admitidos: Servicios de federación de Microsoft Active Directory (ADFS) 2.0Ping Identity Federate 7.2Dispositivo de seguridad Cisco Web Security Appliance 9.1
- Obtenga los siguientes certificados necesarios para proteger la comunicación entre el dispositivo y el proveedor de identidad:Si desea que su dispositivo firme solicitudes de autenticación SAML o si desea que su proveedor de identidad cifre las aserciones SAML, obtenga un certificado autofirmado o un certificado de una autoridad de certificación (CA) de confianza y la clave privada asociada.Si desea que el proveedor de identidad firme afirmaciones SAML, obtenga el certificado del proveedor de identidad. Su dispositivo utiliza este certificado para verificar las afirmaciones de SAML firmadas

#### Configurar

Paso 1. Navegue hasta su SMA y seleccione **Administración del sistema > SAML > Descargar metadatos**, como se muestra en la imagen.

	Network				
Centralized Services		System Administratio	n		
SAML					
Service Provider					
Add Service Provider					
SP Profile Name	Entity ID	Asser	tion Consumer URL	Metadata	Delete
MyLab_SAML	sma.mexesa.com	https://s	sma.mexesa.com:83/	Download Metadata	ŵ
Identity Provider Add Identity Provider Profiles ha	ave been defined. ystems, Inc. All right	s reserved.   Privacy Sta	Opening MyLab_SAML_metadata.xm You have chosen to open: MyLab_SAML_metadata.xml which is: XML file from: https://10.31.124.137 What should Firefox do with this f ○ Open with Notepad++ : a f ② Save File Do this automatically for files	file? file? free (GNU) source code editor ( s like this from now on.	

Paso 2. El perfil del proveedor de identidad se rellena automáticamente cuando el cliente carga su archivo de metadatos ADFS. Microsoft tiene una URL predeterminada: https://<ADFS-host>/FederationMetadata/2007-06/FederationMetadata.xml.

Paso 3. Una vez configurados ambos perfiles, se deben editar los metadatos del perfil SP, según el error <u>CSCvh30183</u>. El archivo de metadatos aparece como se muestra en la imagen.

1	xml version="1.0"?
2	<entitydescriptor <="" th="" xmlns="urn:oasis:names:tc:SAML:2.0:metadata"></entitydescriptor>
3	<pre>xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"</pre>
4	<pre>xmlns:ds="http://www.w3.org/2000/09/xmldsig#"</pre>
5	<pre>entityID="sma.mexesa.com"&gt;</pre>
6	<spssodescriptor< th=""></spssodescriptor<>
7	AuthnRequestsSigned="false" WantAssertionsSigned="true"
8	protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
9	<pre><keydescriptor use="signing"></keydescriptor></pre>
10	<pre>ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"&gt;</pre>
11	<pre>ds:X509Data&gt;</pre>
12	<pre>ds:X509Certificate&gt;Bag Attributes</pre>
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	<pre>subject=/C=MX/CN=sma.mexesa.com/L=CDMX/O=Tizoncito Inc/ST=CDMX/OU=IT Security</pre>
16	issuer=/C=MX/CN=sma.mexesa.com/L=CDMX/O=Tizoncito Inc/ST=CDMX/OU=IT Security
17	BEGIN CERTIFICATE
18	MIIDZTCCAk2gAwIBAwIJAOjXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
19	BAYTAk1YMRcwFQYDVQQDDA5zbWEubWV4ZXNhLmNvbTENMAsGA1UEBwwEQ0RNWDEW
20	MBQGA1UECgwNVG16b25jaXRvIEluYzENMAsGA1UECAwEQ0RNWDEUMBIGA1UECwwL
21	SVQgU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWhcNMjAwNjA0MjEwNTUxWjByMQsw
22	CQYDVQQGEwJNWDEXMBUGA1UEAwwOc21hLm11eGVzYS5jb20xDTALBgNVBAcMBENE
23	TVgxFjAUBgNVBAoMDVRpem9uY210byBJbmMxDTALBgNVBAgMBENETVgxFDASBgNV
24	BASMC01UIFN1Y3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
25	g/kzRmL114q9T1k1cTJzo8cmscu5nRXFW1ohFPcJgn/oHXEUKvUnWe+9cTJQ41X4
20	ojbGCF/Sujb8GaPCZKuBXqAZgKrfgNLR8mopSXTFVWb5X68tVsTBGFNyV8Wtd+Io
21	MVOWJ9N9KJU/KSXUYHUIBYOXIPOLYZHHCDAVYKUPM4F1/Y4JWJ6rnO4JtVpZPJ/B
28	cpwjawLixAIUHVyVrcbbITDIOUEXG+nZ+AIS3B01+61mTNjF3ICGCGS/TEOChETX
29	GISCOKVIMIDNEETAZEY/EDYNIGEDH/WVINWZKMUJINVMIEGJ+LKEGASOBIEMBIHI
30	LONGWAYOLJINJUNIC/EQIQIDAQABNAUGUSQUSIDSDQEBUWUAA4IBAQBYSVXNL/JD
31	ELEVINGER THY COLD 522X GQC 562 EEVIN KGHOZ / F / TEVON KOKO F 112000 SY GEODWD
32	+ZTiOkekuCMEN00f1ZPrJ9cCD5coV1ZibuD7NUmPDi7LKUDVcFUcoVet /+mVCU7
34	7FuBtoom7purmp.I/OoTKouVkbYu230.TNUPvvKacjaVj/2c1VpBBCSMvec277FC.To
35	iv5aVPSvOMPP+D/72FUPAedm3v1mPVou/HTvOPZonCM+ie.TUPhPZvSOMPL+45+FV
36	PO1 +BG5MZuWE
37	END CERTIFICATE
38	-
39	
	1, me the second s

Paso 4. Quite la información resaltada, al final el archivo de metadatos debe ser como se muestra en la imagen.

1	<pre><?xml version="1.0"?></pre>	
2	<entitydescriptor <="" td="" xmlns="urn:oasis:names:tc:SAML:2.0:metadata"><td></td></entitydescriptor>	
3	<pre>xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"</pre>	
4	<pre>xmlns:ds="http://www.w3.org/2000/09/xmldsig#"</pre>	
5	entityID="sma.mexesa.com">	
6	<spssodescriptor< th=""><th></th></spssodescriptor<>	
7	AuthnRequestsSigned="false" WantAssertionsSigned="true"	
8	<pre>protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol'</pre>	'>
9	<keydescriptor use="signing"></keydescriptor>	
10	<pre>ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"&gt;</pre>	
11	<ds:x509data></ds:x509data>	
12	<ds:x509certificate></ds:x509certificate>	
13	MIIDZTCCAk2gAwIBAwIJAOjXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV	
14	BAYTAk1YMRcwFQYDVQQDDA5zbWEubWV4ZXNhLmNvbTENMAsGA1UEBwwEQ0RNWDEW	
15	MBQGA1UECgwNVG16b25jaXRvIEluYzENMAsGA1UECAwEQ0RNWDEUMBIGA1UECwwL	
16	SVQgU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWhcNMjAwNjA0MjEwNTUxWjByMQsw	
17	CQYDVQQGEwJNWDEXMBUGA1UEAwwOc21hLm11eGVzYS5jb20xDTALBgNVBAcMBENE	
18	TVgxFjAUBgNVBAoMDVRpem9uY210byBJbmMxDTALBgNVBAgMBENETVgxFDASBgNV	
19	BAsMC01UIFN1Y3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA	
20	g7kzRmL114q9TlklcTJzo8cmscu5nRXFWlohFPcJgn/oHXEUKvUnWe+9cTJQ41X4	
21	ojbGCP75UjD8GdPczkuBxqAZgkrfgNLR8mopsxTFVWb5x68tVsTBGFNyv8Wtd+Io	
22	MVowJ9h9Kju7kSXuYHU1BYoxfPOLyzHHcbAVYKuPM4Fi7y4jwj6rnO4jtvpZPj7B	
23	cpWjawLlxAfUHVyvrc661Tblo0exG+hZ+AlS3B01+61mTNjF3IcGcGS/TE0chETx	
24	glScUk0iMipnPEtAZey/ebyh18EpH/WViNwZkMUjINvmIFq3+LkF8As8B1Pm6YHi	
25	L6K8W4v0Ej1njtmnC/EQIQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBy3vxNL7jb	
26	emMTKSRP4hycU1d69z2xGQC5e2EeyhnRgHUz7F/TEv0NkORotFii2oOJ6yGEOdWD	
27	6+Bvj6wSBp7UoLyBdCxglyi+vK4Y/R2+iCv13pyaXkbf0QSJvYpzOg7xSjkxZm79	
28	+ZIjQkekyCAM5N00f1ZRrJ9oGD5qoY1ZjhuD7NHmRBj7LKHRKsFVqpKet/tTXCH7	
29	7EuB+ogT7pvrTDJ/QoIKcvYkbXuZ30JNVPxxKacjAVj/Zc1XnPBGSMxeo277ECJq	
30	ix5aXRSxOMRRtD/72FVRAsgT3x1mBYqu/HTyOBZonGM+isJHBhRZxSOMBL+45jFY	
31	PO1jBG5MZuWE	
32		
33	-	
34	-	
35		
36	<keydescriptor use="encryption"></keydescriptor>	
37	<pre><ds:keyinfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"></ds:keyinfo></pre>	
38	<pre><ds:x509data></ds:x509data></pre>	
39	<pre><ds:x509certificate></ds:x509certificate></pre>	
40	MIIDZTCCAk2gAwIBAwIJAOjXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV	
41	BAYTAk1YMRcwFQYDVQQDDA5zbWEubWV4ZXNhLmNvbTENMAsGA1UEBwwEQ0RNWDEW	
42	MBQGA1UECgwNVG16b25jaXRvIEluYzENMAsGA1UECAwEQ0RNWDEUMBIGA1UECwwL	
43	SVQgU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWhcNMjAwNjA0MjEwNTUxWjByMQsw	

Paso 5. Navegue hasta su ADFS e importe el archivo de metadatos editado en ADFS Tools > AD FS Management > Add Reliying Party Trust, como se muestra en la imagen.

<b>N</b>	Add Relying Party Trust Wizard
Select Data Source	
<ul> <li>Steps</li> <li>Welcome</li> <li>Select Data Source</li> <li>Configure Multi-factor Authentication Now?</li> <li>Choose Issuance Authorization Rules</li> <li>Ready to Add Trust</li> <li>Finish</li> </ul>	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 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: <u>Example: Stot Mycharella_mea_userul_metadata (1).</u> Browse
	< Previous Next > Cancel

Paso 6. Después de importar correctamente el archivo de metadatos, configure las reglas de reclamación para la confianza de la parte que confía recientemente, seleccione la **plantilla de regla reclamación > Enviar atributos LDAP**, como se muestra en la imagen.

<b>\$</b> 1	Add Transform Claim Rule Wizard
Select Rule Template	
Steps	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.
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 storm such as Active Directory to send as claims to the rehims party. Midicia attributes may be send 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.

Paso 7. Asigne el nombre de la regla de reclamación y seleccione **Almacén de atributos > Active Directory**.

Paso 8. Asignar atributos LDAP, como se muestra en la imagen.

- Atributo LDAP > Direcciones de correo electrónico
- Tipo de reclamación saliente > Dirección de correo electrónico

<b>S</b> a		Add Transform Claim Rule	e Wiz	ard	x	
Configure Rule						
Steps Choose Rule Type	You o which	an configure this rule to send the values of to extract LDAP attributes. Specify how the	LDAP attrib	attributes as claims. Select an attribute store from utes will map to the outgoing claim types that will b		
Configure Claim Rule	Claim	f from the rule. rule name:				
	chare	charella_sma				
	Attribu	te store: e Directory ing of LDAP attributes to outgoing claim two	es:	¥		
		LDAP Attribute (Select or type to add more)	Out	going Claim Type (Select or type to add more)	٦	
	•	E-Mail-Addresses	/ EM	al Address	¥	
	*		<u> </u>		¥	
				< Previous Finish Cance		

Paso 9. Cree una nueva regla de reclamación personalizada con esta información, como se muestra en la imagen.

#### Ésta es la regla personalizada que debe agregarse a la regla de reclamación personalizada:

```
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.r1.ces.cisco.com/");
```

 Modifique la dirección URL resaltada con el nombre de host y el puerto de SMA (si se encuentra en un entorno de CES, no se necesita un puerto pero debe apuntar a euq1.<location>.iphmx.com)

Paso 10. Asegúrese de que el orden de la regla de reclamación es: Regla de reclamación LDAP primero y regla de reclamación personalizada en segundo lugar, como se muestra en la imagen.

OK

Cancel

<b>a</b>	E	dit Claim Rules for ADI	FS_charella 🗕 🗖	X
Issuance	Transform Rules	Issuance Authorization Rules	Delegation Authorization Rules	
The folk	owing transform ru	ules specify the claims that will b	e sent to the relying party.	
Order	Rule Name	k	ssued Claims	
1	charella_sma	E	E-Mail Address	
2	charella_custor	n_rule <	(See claim rule>	

Paso 11. Inicie sesión en la EUQ, debe redirigir al host ADFS.

#### Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

# Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

### Información Relacionada

- CSCvh30183
- Soporte Técnico y Documentación Cisco Systems