

ADFS ىلع ةيلوأل تانايبلا فلم تيبتت

تايوتحمل

[ةمدقمل](#)

[ةيساسأل تابلطتم](#)

[تابلطتم](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[نيوكتلا](#)

[ةحصللا نم ققحتلا](#)

[اهالص او اطاخأل افاشكتسا](#)

[قلص تاذا تامولعم](#)

ةمدقمل

Microsoft Active Directory (ADFS) داخا تامدخ ىلع فيرعتلا تانايب فلم تيبتت ةيفيكت دننسملا اذه حضوي Directory (ADFS).

ةيساسأل تابلطتم

تابلطتم

ةيلاتلا عيضاوملاب ةفرعم كيديل نوكت نأ Cisco ي صوت:

- ةعزوملا تافلما ماطن
- نامأل ةرادا زاهج عم (SAML) نامأل ديكتات زيمت ةغل لمكت

ةمدختسملا تانوكملا

ةيلاتلا ةيدملا تانوكملا او جماربلا تارادصا ىلا دننسملا اذه في ةدراولا تامولعملا دننست:

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

ةصاخ ةيلمعم ةئيب في ةدوجوملا ةزهجالا نم دننسملا اذه في ةدراولا تامولعملا ءاشنإ مت تناك اذا. (يضايرتفا) حوسمم نيوكتب دننسملا اذه في ةمدختسملا ةزهجالا عيمج تادب رمايال لم تحملا ريثاتلل كمهف نم دكاتف، ليغشتلا ديكتكتبش

ةيساسأ تامولعم

م تي تابلطتملا كلت نأ نم دكات، ADFS في ةيلوأل تانايبلا فلم تيبتت متي نأ لبق اهتبلت:

- SMA في SAML نيكتمت
- نامأل ةرادا زاهج ةطساوب اموعدم كتسسؤم همدختست يذلا ةيوهلا رفوم ناك اذا ام ققحت

Microsoft Active Directory داخا تام دخ : نوم و عد م ل ا ة ي و ه ل ا و دوزم م ه ا ل و ه Cisco. ن م ي و ت ح ل م ل ا (ADFS) 2.0 Ping Identity Federate 7.2 ن م ا ز ا ه ج Cisco ن م 9.1 ب ي و ل ا ن ا م ا ز ا ه ج

- ت ن ك ا ذ ا : ة ي و ه ل ا ر ف و م و ز ا ه ج ل ا ن ي ب ل ا ص ا ت ا ل ا ن ي م ا ت ل ة ب و ل ط م ل ا ت ا د ا ه ش ل ا ه ذ ه ي ل ع ل ص ح ا ة ي و ه ل ا ر ف و م ن م د ي ر ت ت ن ك ا ذ ا و ا SAML ة ق د ا ص م ت ا ب ل ط ع ي ق و ت ك ب ص ا خ ل ا ز ا ه ج ل ا ن م د ي ر ت ق و ت و م ق د ص م ع ج ر م ن م ة د ا ه ش و ا ا ي ت ا ذ ة ع ق و م ة د ا ه ش ي ل ع ل ص ح ا ، SAML ت ا د ي ك ا ت ر ي ف ش ت ت ا د ي ك ا ت ي ل ع ة ي و ه ل ا ر ف و م ع ق و ي ن ا د ي ر ت ت ن ك ا ذ ا . ط ب ت ر م ل ا ص ا خ ل ا ح ا ت ف م ل ا و (CA) ه ب ق ق ح ت ل ل ة د ا ه ش ل ا ه ذ ه ك ب ص ا خ ل ا ز ا ه ج ل ا م د خ ت س ي . ة ي و ه ل ا ر ف و م ة د ا ه ش ي ل ع ل ص ح ا ، SAML ة ع ق و م ل ا SAML ت ا د ي ك ا ت ن م

ن ي و ك ت ل ا

ح ض و م و ه ا م ك ، ة ي و ل و ا ل ا ت ا ن ا ي ب ل ا ل ي ز ن ت > SAML > م ا ط ن ل ا ة ر ا د ا د ح و SAML ي ل ل ق ت ن ا . 1 ة و ط خ ل ا ة ر و ص ل ل ا ي .

The screenshot shows the Cisco Identity Management console interface. At the top, there are tabs for 'Management Appliance', 'Email', and 'Web'. Below these are 'Centralized Services', 'Network', and 'System Administration'. The main content area is titled 'SAML' and is divided into 'Service Provider' and 'Identity Provider' sections. The 'Service Provider' section contains a table with columns for 'SP Profile Name', 'Entity ID', 'Assertion Consumer URL', 'Metadata', and 'Delete'. A row is visible for 'MyLab_SAML' with 'sma.mexesa.com' as the Entity ID and 'https://sma.mexesa.com:83/' as the Assertion Consumer URL. A 'Download Metadata' button is highlighted in yellow. A red arrow points from this button to a file dialog box titled 'Opening MyLab_SAML_metadata.xml'. The dialog box shows the file 'MyLab_SAML_metadata.xml' which is an XML file from 'https://10.31.124.137'. It asks 'What should Firefox do with this file?' and has options to 'Open with Notepad++', 'Save File' (which is selected), or 'Do this automatically for files like this from now on'. 'OK' and 'Cancel' buttons are at the bottom.

ف ل م ل ي م ح ت ب ل ي م ع ل ا م و ق ي ا م د ن ع ا ي ا ق ل ت ة ي و ه ل ا ر ف و م ف ي ر ع ت ف ل م ع ل م م ت ي . 2 ة و ط خ ل ا ب ي ض ا ر ت ف ا URL ن ا و ن ع Microsoft ي د ل د ج و ي . ه ب ص ا خ ل ا ADFS ف ي ر ع ت ت ا ن ا ي ب <https://<ADFS-host>/FederationMetadata/2007-06/FederationMetadata.xml>.

ف ي ر ع ت ف ل م ف ي ر ع ت ت ا ن ا ي ب ر ي ر ح ت ب ج ي ، ف ي ر ع ت ل ا ت ا ف ل م ن م ل ك د ا د ع ا م ت ي ن ا م . 3 ة و ط خ ل ا ة ر و ص ل ل ا ي ح ض و م و ه ا م ك ة ي و ل و ا ل ا ت ا ن ا ي ب ل ا ف ل م ر ه ط ي . CSCvh30183 ا ط خ ل ا ب س ح ، SP

```

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            BAYTAk1YMRcwFQYDVQQDDA5zbWEubWV4ZXXNhLmNvbTENCAsGA1UEBwwEQ0RNWDEW
20            MBQGA1UECgwNVG16b25jaXRvIEluYzENMAsGA1UECAwEQ0RNWDEUMBIGA1UECwwL
21            SVQGU2VjdXJpdHkwHhcNMjkwNjA1MjEwNTUxWWhcNMjkwNjA1MjEwNTUxWjByMQsw
22            CQYDVQQGEwJNWDEwXG90Z21hLm1leGVzYS5jb20xDTALBgNVBACMBENE
23            TVGxVjAUBG90Z21hLm1leGVzYS5jb20xDTALBgNVBAGMBENETVgxFDASBgNV
24            BAsMC0lUIFNlY3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
25            g7kzRmL114q9TlklcTJzo8cmscu5nRXFWlohFPcJgn/oHXEUkVUnWe+9cTJQ41X4
26            ojbGCP75UjD8GdPczkuBxqAZgkrfgNLR8mopsxTFVWb5x68tVsTBGFNyw8Wtd+Io
27            MVowJ9h9Kju7kSXuYHU1BYoxfPOLyzHHcbAVYKuPM4Fi7y4jwj6rn04jtvPZj7B
28            cpWjawLlxAfUHVyvrC661Tblo0exG+hZ+AlS3B01+61mTNjF3IcGcGS/TE0chETx
29            glScUk0iMipnPEtAZey/ebyh18EpH/WViNwZkMUjINvmIFq3+LkF8As8B1Pm6YHi
30            L6K8W4vOEj1njtmnC/EQIQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB3vxNL7jb
31            emMTKSRP4hycUld69z2xGQC5e2EeyhnRgHUz7F/TEv0NkORotFii2oOJ6yGEOdWD
32            6+Bvj6wSBp7UoLyBdCcxglyi+vK4Y/R2+iCv13pyaXkbf0QsJvYpzOg7xSjKxZm79
33            +ZIJQkekyCAM5N0of1ZRrJ9oGD5qoYlZjhuD7NHmRbj7LKHrKsFVqpKet/tTXCH7
34            7EuB+ogT7pvrTDJ/QoIKcvYkbXuZ30JNVPxxKacjAVj/ZclXnPBGSMxex0277ECJq
35            ix5aXRSxOMRRtD/72FVRAsGT3x1mBYqu/HTyOBZongM+isJHBhRZxSOMBL+45jFY
36            PO1jBG5MZuWE
37            -----END CERTIFICATE-----
38          </ds:X509Certificate>
39        </ds:X509Data>

```

وه امك نوكي نأ بحجي ةيلوأل تانايبلا ةياهن فلم يف ، ةزربملا تامولعمل ا ةلازا 4. ةوطخلا ةروصل يف حضورم.


```

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 BAYTAk1YMRcwFQYDVQQDDA5zbWEubWV4ZlZlLnVzTENMAAGA1UEBwwEQ0RNWDEW
15 MBQGA1UECgwNVG16b25jaXRvIEluYzENMAAGA1UECAwEQ0RNWDEUMBIGA1UECwwL
16 SVQGU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWWhcNMjAwNjA0MjEwNTUxWjByMQsw
17 CQYDVQQGEwJNWDEUMBUGA1UEAAwOc21hLm1leGVzYS5jb20xDTALBgNVBACMBENE
18 TVGxFjAUBGNVBAoMDVRpem9uY210byBJbMmxDTALBgNVBAGMBENETVgxFDASBgNV
19 BAsMC01UIFNlY3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
20 g7kzRmL114q9T1klcTJzo8cmscu5nRXFWlohFpcJgn/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/Zc1XnPBGSMxex0277ECJq
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 BAYTAk1YMRcwFQYDVQQDDA5zbWEubWV4ZlZlLnVzTENMAAGA1UEBwwEQ0RNWDEW
42 MBQGA1UECgwNVG16b25jaXRvIEluYzENMAAGA1UECAwEQ0RNWDEUMBIGA1UECwwL
43 SVQGU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWWhcNMjAwNjA0MjEwNTUxWjByMQsw

```

تاوداً في ةررحملا ةيلوألانا ايبال فلم جاردا ب مقوكب صاخلا ADFS لى لقتنا 5. ةوطخلا ةروصلال في حضورم وه امك ، دامتعالا فرط ةقت ةفاصلا > AD FS ةرادا > ADFS

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.

تابل لاطم لدع اوق نيوك تب مق ، حاجنب فيرعتل تانايب فلم داريتساب كم ايق دع ب . 6 ةوطخل لاسرا > ةب لاطم لدع اق بلاق دح ، اتيح اهؤاشن مت يتل "لوعم ل فرطلا ةقت" ب ةصاخلا ةروصلل يف حضوم وه امك ، LDAP تامس

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.

Active Directory > تامس ل لنخم دح م ، ةب لاطم لدع اق مس ا ةيمس تب مق . 7 ةوطخل

ةروضلا يف حضوم وه امك ، LDAP صئاصخ طيطخت 8. ةوطخلا

- ينورتكللال ديربلل نيوانع > LDAP ةمس
- ينورتكللال ديربلل ناووع > ةرداصلال ةبلالاطملا عون

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: charela_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

حضوم وه امك ، تامولعمل هذه مادختساب ةديج ةصصخم ةبلالاطم ةدعاق عاشناب مق 9. ةوطخلا ةروضلا يف

ةصصخملا ةبلالاطملا ةدعاق ىلإ اهتفاضل بجي يتل ةصصخملا ةدعاقلا يه هذه

```
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:

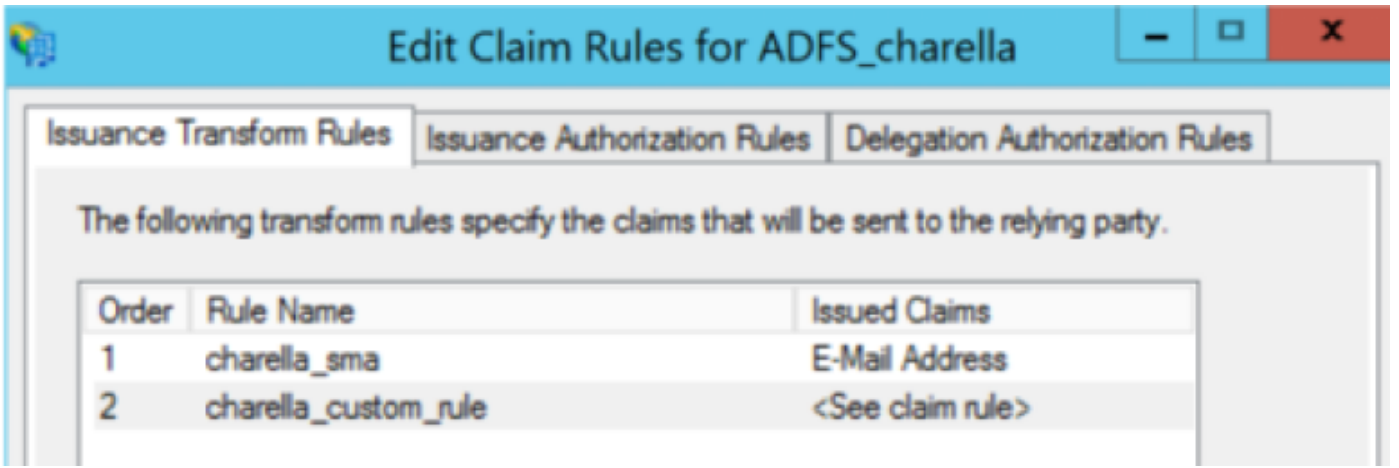
```
c:[Type ==
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue (Type =
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value,
ValueType = c.ValueType, Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "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

- ئىبىلىك (SMA) ئىشلىتىش ئۈچۈن مەسلىھەت سېلىش لازىم. URL ئورنىنى ئۆزگەرتىش ئۈچۈن CES، euq1.<distribution>.iphmx.com) نى ئۆزگەرتىش لازىم.

ئۆزگەرتىش لازىم. 10. ئۆزگەرتىش لازىم. ئۆزگەرتىش لازىم. ئۆزگەرتىش لازىم. ئۆزگەرتىش لازىم.



ADFS. فيضم الـ هيجوتال دي عي نأ بجي و، EUQ، الـ لوخلال ليجستب مق 11. ةوطخلال

ةحصلال نم ققحتال

نـيوكتال اذه ةحص نم ققحتال لـ ءارجلـ آيـ لـ احـ دجوي الـ

اهـالـصـإـوـءـاطـخـأـلـ فـاشـكـتـسـا

نـيوكتال اذهـلـ اهـالـصـإـوـءـاطـخـأـلـ فـاشـكـتـسـاـلـ ةـدـدـحـمـ تـامـولـعـمـ آيـ لـ احـ رـفـوتـ الـ

ةـلـصـ تـاذـ تـامـولـعـم

- [CSCvh30183](#)
- [تـادـنـتـسـمـلـاـوـيـنـقـتـالـ مـعـدلـا - Cisco Systems](#)

