# Configuración de la VPN de AnyConnect de ASA con Microsoft Azure MFA a través de SAML

## Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Componentes SAML
Certificados para operaciones de firma y cifrado
Diagrama de la red
Configurar
Agregue Cisco AnyConnect desde la Galería de aplicaciones de Microsoft
Asignar usuario de Azure AD a la aplicación
Configuración de ASA para SAML mediante CLI
Verificación
Probar AnyConnect con autenticación SAML
Problemas comunes
ID de entidad no coincidente
Discordancia de tiempo
Certificado de firma IdP incorrecto utilizado
Audiencia de aserción no válida
URL incorrecta para el servicio al consumidor de aserción
Cambios de configuración de SAML que no surten efecto
Troubleshoot
Información Relacionada

## Introducción

Este documento describe cómo configurar el Lenguaje de marcado de aserción de seguridad (SAML) con un enfoque en ASA AnyConnect a través de Microsoft Azure MFA.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

• Conocimiento básico de la configuración VPN de RA en el dispositivo de seguridad

adaptable (ASA).

- Conocimiento básico de SAML y Microsoft Azure.
- Licencias AnyConnect habilitadas (APEX o solo VPN).

### **Componentes Utilizados**

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

- Una suscripción de Microsoft Azure AD.
- Cisco ASA 9.7+ y Anyconnect 4.6+
- Trabajando con el perfil VPN de AnyConnect

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

SAML es un marco basado en XML para intercambiar datos de autenticación y autorización entre dominios de seguridad. Crea un círculo de confianza entre el usuario, un proveedor de servicios (SP) y un proveedor de identidad (IdP) que permite al usuario iniciar sesión una sola vez para varios servicios. Microsoft Azure MFA se integra a la perfección con el dispositivo VPN Cisco ASA para proporcionar seguridad adicional para los inicios de sesión de Cisco AnyConnect VPN.

### **Componentes SAML**

Metadatos: Es un documento basado en XML que asegura una transacción segura entre un IdP y un SP. Permite al IdP y al SP negociar acuerdos.

Roles admitidos por los dispositivos (IdP, SP)

Un dispositivo puede soportar más de un rol y puede contener valores tanto para un SP como para un IdP. Debajo del campo EntityDescriptor hay un IDPSSODescriptor, si la información que contiene es para un identificador de inicio de sesión único, o un SPSSODescriptor si la información que contiene es para un proveedor de servicios de inicio de sesión único. Esto es importante ya que los valores correctos deben ser tomados de las secciones apropiadas para configurar SAML exitosamente.

Id. de entidad: este campo es un identificador único para un SP o un IdP. Un único dispositivo puede tener varios servicios y puede utilizar diferentes ID de entidad para diferenciarlos. Por ejemplo, ASA tiene diferentes ID de entidad para diferentes grupos de túnel que necesitan ser autenticados. Un IdP que autentica cada grupo de túnel tiene entradas de Id. de entidad separadas para cada grupo de túnel para identificar con precisión esos servicios.

ASA puede admitir varios IdP y tiene un ID de entidad independiente para cada IdP para

diferenciarlos. Si cualquiera de los lados recibe un mensaje de un dispositivo que no contiene un ID de entidad que se haya configurado previamente, es probable que el dispositivo descarte este mensaje y la autenticación SAML falle. El ID de entidad se puede encontrar en el campo EntityDescriptor junto a entityID.

URL de servicio: definen la URL de un servicio SAML proporcionado por el SP o el IdP. Para los IdPs, esto es comúnmente el Servicio de cierre de sesión único y el Servicio de inicio de sesión único. Para los SP, esto es comúnmente el servicio de consumidor de aserción y el servicio de cierre de sesión único.

El SP utiliza la URL del servicio de Single Sign-On que se encuentra en los metadatos IdP para redirigir al usuario al IdP para la autenticación. Si este valor está configurado incorrectamente, el IdP no recibe o no puede procesar satisfactoriamente la solicitud de autenticación enviada por el SP.

El IdP utiliza la URL de Assertion Consumer Service que se encuentra en los metadatos del SP para redirigir al usuario al SP y proporcionar información sobre el intento de autenticación del usuario. Si se configura incorrectamente, el SP no recibe la aserción (la respuesta) o no puede procesarla correctamente.

La URL de Single Logout Service se puede encontrar tanto en el SP como en el IdP. Se utiliza para facilitar la desconexión de todos los servicios SSO del SP y es opcional en el ASA. Cuando la URL del servicio SLO de los metadatos IdP se configura en el SP, cuando el usuario se desconecta del servicio en el SP, el SP envía la solicitud al IdP. Una vez que el IdP ha cerrado correctamente la sesión del usuario en los servicios, redirige al usuario de nuevo al SP y utiliza la URL del servicio SLO que se encuentra dentro de los metadatos del SP.

Enlaces SAML para URLs de Servicio: Los enlaces son el método que el SP utiliza para transferir información al IdP y viceversa para los servicios. Esto incluye HTTP Redirect, HTTP POST y Artefacto. Cada método tiene una forma diferente de transferir datos. El método de enlace admitido por el servicio se incluye en la definición de dicho servicio. Por ejemplo: SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location= Servicio SSO >. ASA no admite la vinculación de Artefactos. ASA siempre utiliza el método de redireccionamiento HTTP para las solicitudes de autenticación SAML, por lo que es importante elegir la URL del servicio SSO que utiliza el enlace de redireccionamiento HTTP para que el IdP lo espere.

### Certificados para operaciones de firma y cifrado

Para proporcionar confidencialidad e integridad a los mensajes enviados entre el SP y el IdP, SAML incluye la capacidad de cifrar y firmar los datos. El certificado utilizado para cifrar y/o firmar los datos puede incluirse dentro de los metadatos para que el extremo que recibe pueda verificar el mensaje SAML y asegurarse de que proviene del origen esperado. Los certificados utilizados para la firma y el cifrado se pueden encontrar en los metadatos bajo KeyDescriptor use=signing y KeyDescriptor use=encryption, respetuosamente, luego X509Certificate. ASA no admite el cifrado de mensajes SAML.

## Diagrama de la red



## Configurar

Agregue Cisco AnyConnect desde la Galería de aplicaciones de Microsoft

Paso 1. Inicie sesión en el Portal de Azure y elija Azure Active Directory.

Azur	e service	S								
	+	٩		•	۲		SQL	<b></b>	8	$\rightarrow$
Cr	reate a source	Azure Active Directory	All resources	Virtual machines	App Services	Storage accounts	SQL databases	Azure Database for PostgreS	Azure Cosmos DB	More services
Navi	gate									
•	Subscriptio	ons	[📬 R	esource groups		All resource	25	Da:	shboard	

Paso 2. Como se muestra en esta imagen, elija Aplicaciones empresariales.



Paso 3. Ahora, elija New Application, como se muestra en esta imagen.

Enterprise applicatio	ns   All applications		
Overview	≪ + New application   ≡≡ Colum	nns	
1 Overview	Try out the new Enterprise Apps	search preview! Click to enable the previe	w. $\rightarrow$
	Application Type	Applications status	Application visibility
	Enterprise Applications	Any 🗸	Any 🗸

Paso 4. En la sección Agregar de la galería, escriba AnyConnect en el cuadro de búsqueda, elija Cisco AnyConnect en el panel de resultados y, a continuación, agregue la aplicación.

Add an application				Add app	
Add an application				Cisco Systems, Inc.	
<ul> <li>Click here to try out the new</li> <li>Add your own app</li> </ul>	w and improved app gallery. $ ightarrow$			Empower your employees to work from anywhere, on company laptops or personal mobile devices, at any time. AnyConnect	
Application you're developing	Application you're developing			simplifies secure endpoint access and provides the security necessary to help keep your organization safe and protected.	
Register an app you're working on to integrate it with Azure AD	Configure Azure AD Application Proxy to enable secure remote access.	Integrate any other application that you don't find in the gallery		Use Microsoft Azure AD to enable user access to Cisco AnyConnect.	
				Requires an existing Cisco AnyConnect subscription.	
Add from the gallery				Name ①	
Category All (3422) V AnyConnect V				Cisco AnyConnect	
				Publisher 〇 Cisco Systems, Inc.	
1 applications matched "A	AnyConnect".			Single Sign-On Mode	
Name		Category	_	SAML-based Sign-on	
Cisco AnyConn	ect	Business management			
			_	https://www.ciscoanyconnect.com/	
				Logo 🛈	
				Add	

Paso 5. Elija el elemento de menú Single Sign-on, como se muestra en esta imagen.

AnyConnectVPN   Overvie	ew		
»			
Overview	Properties		
Deployment Plan	Name		
X Diagnose and solve problems	AnyConnectVPN		
Manage	Application ID ①		
Properties			
A Owners	Object ID 🕕		
Users and groups			
Single sign-on	Getting Started		
Provisioning			
Application proxy	2. 1. Assign users and groups	2. Set up single sign on	(3) 3. Provision User Accounts
<ul> <li>Self-service</li> </ul>	Provide specific users and groups access to the applications	Enable users to sign into their application	Automatically create and delete user
Security	Assign users and groups	Get started	Get started
Conditional Access			
A Permissions			
Token encryption	4. Conditional Access	S. Self service	
Activity	Secure access to this application with a customizable access policy.	Enable users to request access to the application using their Azure AD	
Sign-ins	Create a policy	credentials Get started	
ាំរាំ Usage & insights (Preview)			

Paso 6. Elija SAML, como se muestra en la imagen.



Paso 7. Edite la Sección 1 con estos detalles.

#### <#root>

```
a. Identifier (Entity ID) - https://<VPN URL>/saml/sp/metadata/<TUNNEL-GROUP NAME>
```

```
b. Reply URL (Assertion Consumer Service URL) - https://<VPN URL>/+CSCOE+/sam1/sp/acs?tgname=<TUNNEL-G
```

Example: vpn url called

#### asa.example.com

and tunnel-group called

AnyConnectVPN-1

Basic SAML Configuration	
Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional

Paso 8. En la sección Certificado de firma SAML, elija Descargar para descargar el archivo del certificado y guárdelo en su computadora.

SAML Signing Certificate		Ø
Status	Active	
Thumbprint		
Expiration	5/1/2023, 4:04:04 PM	
Notification Email		
App Federation Metadata Url	https://l	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	

Paso 9. Esto es necesario para la configuración de ASA.

- Azure AD Identifier Este es el mismo idp en nuestra configuración VPN.
- Login URL (URL de inicio de sesión): se trata del inicio de sesión de URL.
- Logout URL (URL de cierre de sesión): Se trata de la URL de cierre de sesión.

You'll need to configure the appli	cation to link with Azure AD.	
Login URL	https://	
Azure AD Identifier	https://	
Logout URL	https://	

### Asignar usuario de Azure AD a la aplicación

En esta sección, Test1 está habilitado para utilizar el inicio de sesión único de Azure, ya que concede acceso a la aplicación Cisco AnyConnect.

Paso 1. En la página de descripción general de la aplicación, seleccione Usuarios y grupos y, a continuación, Agregar usuario.

	Cisco AnyConnect   Users and groups Enterprise Application					
		«	🕂 Add user 🖉 Edit 📋 Remove	Description Descripti Description Description Description Description Desc		
14	Overview		The application will appear on the Ac	cress Panel for assigned users. Set 'visible to users?' to no in properties to prevent this. $\rightarrow$		
	Deployment Plan					
×	Diagnose and solve problems		First 100 shown, to search all users & groups, enter a display name.			
M	Manage		Display Name	Object Type	Role assigned	
			No application assignments found			
	Properties					
	Owners	-				
*	Users and groups					
Э	Single sign-on					

Paso 2. Elija Usuarios y grupos en el cuadro de diálogo Agregar asignación.

Add Assignment rchogs-azure-ad	, ₽ Search
Users and groups >	
Select Role Select	
	TE Test1

Paso 3. En el cuadro de diálogo Add Assignment, haga clic en el botón Assign.

Users and groups 1 user selected.	>
Select Role User	>
User	

Configuración de ASA para SAML mediante CLI

Paso 1. Cree un punto de confianza e importe el certificado SAML.

```
config t
crypto ca trustpoint AzureAD-AC-SAML
  revocation-check none
  no id-usage
  enrollment terminal
  no ca-check
crypto ca authenticate AzureAD-AC-SAML
-----BEGIN CERTIFICATE-----
...
PEM Certificate Text you downloaded goes here
...
-----END CERTIFICATE-----
quit
```

Paso 2. Estos comandos proveen su IdP de SAML.

webvpn

```
saml idp https://xxx.windows.net/xxxxxxxx/ - [Azure AD Identifier]
url sign-in https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxx/saml2 - [Login URL]
url sign-out https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0 - Logout URL
trustpoint idp AzureAD-AC-SAML - [IdP Trustpoint]
trustpoint sp ASA-EXTERNAL-CERT - [SP Trustpoint]
no force re-authentication
no signature
base-url https://asa.example.com
```

Paso 3. Aplique la autenticación SAML a una configuración de túnel VPN.

```
tunnel-group AnyConnectVPN-1 webvpn-attributes
  saml identity-provider https://xxx.windows.net/xxxxxxxxxx/
  authentication saml
end
```

write memory

Nota: Si realiza cambios en la configuración del IdP, debe eliminar la configuración del proveedor de identidad saml del grupo de túnel y volver a aplicarla para que los cambios entren en vigor.

## Verificación

Probar AnyConnect con autenticación SAML

Paso 1. Conéctese a la URL de su VPN e ingrese sus detalles de inicio de sesión en Azure AD.

Paso 2. Aprobar solicitud de inicio de sesión.

Paso 3. AnyConnect está conectado.



•••	AnyConnect Secure Mobility Client	cisco
	VPN: Connected	<ul> <li>Disconnect</li> </ul>
00:00:22		IPv4

### Problemas comunes

ID de entidad no coincidente

Ejemplo de depuración:

[SAML] consumer\_assertion: #LassoServer desconoce el identificador de un proveedor. Para registrar un proveedor en un objeto #LassoServer, debe utilizar los métodos lasso\_server\_add\_provider() o lasso\_server\_add\_provider\_from\_buffer().

Problema: Generalmente, significa que el comando saml idp [entityID] bajo la configuración webvpn del ASA no coincide con el IdP Entity ID encontrado en los metadatos del IdP.

Solución: compruebe el ID de entidad del archivo de metadatos del IdP y cambie el comando saml idp [entity id] para que coincida.

Discordancia de tiempo

Ejemplo de depuración:

[SAML] NotBefore:2017-09-05T23:59:01.896Z NotOnOrAfter:2017-09-06T00:59:01.896Z tiempo de espera: 0

[SAML] consumer\_assertion: la afirmación ha caducado o no es válida

Problema 1. La hora de ASA no se sincroniza con la hora de IdP.

Solución 1. Configure ASA con el mismo servidor NTP utilizado por IdP.

Problema 2. La aserción no es válida entre el tiempo especificado.

Solución 2. Modifique el valor de tiempo de espera configurado en el ASA.

### Certificado de firma IdP incorrecto utilizado

Ejemplo de depuración:

[Lasso] func=xmlSecOpenSSLEvpSignatureVerify:file=signature.c:line=493:obj=rsa-sha1:subj=EVP\_VerifyFinal:error=18:los datos no coinciden:la firma no coincide

[SAML] consumer\_assertion: el perfil no puede verificar una firma en el mensaje

Problema: ASA no puede verificar el mensaje firmado por el IdP o no hay firma para que ASA la verifique.

Solución: Verifique el certificado de firma de IdP instalado en el ASA para asegurarse de que coincide con lo que envía el IdP. Si esto se confirma, asegúrese de que la firma esté incluida en la respuesta SAML.

### Audiencia de aserción no válida

Ejemplo de depuración:

[SAML] consumer\_assertion: la audiencia de aserción no es válida

Problema: IdP define la audiencia incorrecta.

Solución: corrija la configuración de Audience en el IdP. Debe coincidir con la ID de entidad de ASA.

### URL incorrecta para el servicio al consumidor de aserción

Ejemplo de depuración: no se puede recibir ninguna depuración después de enviar la solicitud de autenticación inicial. El usuario puede ingresar credenciales en el IdP pero el IdP no redirige al ASA.

Problema: IdP está configurado para la URL de servicio de consumidor de aserción incorrecta.

Solución(es): compruebe la URL base en la configuración y asegúrese de que es correcta. Verifique los metadatos ASA con show para asegurarse de que la URL de Assertion Consumer Service sea correcta. Para probarlo, navegue por él, si ambos son correctos en el ASA, verifique el IdP para asegurarse de que la URL sea correcta.

Cambios de configuración de SAML que no surten efecto

Ejemplo: después de modificar o cambiar una URL de inicio de sesión único, el certificado SP,

SAML sigue sin funcionar y envía configuraciones anteriores.

Problema: ASA necesita volver a generar sus metadatos cuando hay un cambio de configuración que le afecta. No lo hace automáticamente.

Solución: después de realizar los cambios, en el grupo de túnel afectado, quite y vuelva a aplicar el comando saml idp [entity-id].

## Troubleshoot

La mayoría de los solucionadores de problemas de SAML implican un error de configuración que se puede encontrar cuando se comprueba la configuración de SAML o se ejecutan depuraciones. debug webvpn saml 255 se puede utilizar para solucionar la mayoría de los problemas; sin embargo, en escenarios donde esta depuración no proporciona información útil, se pueden ejecutar depuraciones adicionales:

debug web∨pn saml 255 debug web∨pn 255 debug web∨pn session 255 debug web∨pn request 255

## Información Relacionada

• Inicio de sesión único de SAML para aplicaciones in situ con proxy de aplicación

### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).