## Solución de problemas de inicio de sesión único de CCE con la administración de certificados de Identity Service (IdS)

### Contenido

Introducción **Prerequisites Requirements** Componentes Utilizados **Antecedentes** Certificado SAML vencido Solución Cambio del algoritmo hash seguro en el proveedor de identidad (IdP) Solución Cambio de dirección IP o nombre de host del servidor Cisco IdS - Editor de CUIC/LiveData/IdS co-residente o Editor de IdS independiente reconstruido -Suscriptor de CUIC/LiveData/IdS co-residente o suscriptor de IdS independiente reconstruido Solución Referencia Cómo agregar una persona de confianza en el ADFS o Cómo habilitar la afirmación SAML firmada Cómo cargar el certificado SSL de AD FS en la confianza Tomcat de IdS de Cisco Cómo eliminar la entidad de confianza de confianza en AD FS Cómo comprobar o cambiar el algoritmo hash seguro configurado en el proveedor de identidad <u>(IdP)</u> Cómo verificar la fecha de vencimiento del certificado SAML del servidor Cisco IdS Cómo descargar los metadatos del servidor de IdS de Cisco Cómo recuperar el certificado SAML del archivo sp.xml Cómo reemplazar el certificado SAML en AD FS Cómo regenerar el certificado SAML en el servidor Cisco IdS Prueba de SSO

## Introducción

Este documento describe los pasos detallados para regenerar e intercambiar certificados SAML en UCCE/PCCE, garantizando procesos seguros y claros.

Colaboración de Nagarajan Paramasivam, ingeniero del TAC de Cisco.

## Prerequisites

### Requirements

Cisco recomienda que conozca estos temas:

- Packaged/Unified Contact Center Enterprise (PCCE/UCCE)
- Plataforma de sistema operativo de voz (VOS)
- Administración de certificados
- Lenguaje de marcado de aserción de seguridad (SAML)
- Secure Socket Layer (SSL)
- Servicios de federación de Active Directory (AD FS)
- Inicio de sesión único (SSO)

### **Componentes Utilizados**

La información de este documento se basa en estos componentes:

- Cisco Identity Service (ID de Cisco)
- Proveedor de identidad (IdP): Microsoft Windows ADFS



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

En UCCE/PCCE, Cisco Identity Service (Cisco IdS) proporciona autorización entre el proveedor de identidad (IdP) y las aplicaciones.

Cuando configura los IdS de Cisco, configura un intercambio de metadatos entre los IdS de Cisco

y el IdP. Este intercambio establece una relación de confianza que luego permite a las aplicaciones utilizar los IdS de Cisco para SSO. Para establecer la relación de confianza, descargue un archivo de metadatos del IdS de Cisco y cárguelo en el IdP.

El certificado SAML es similar a un certificado SSL y, al igual que éste, necesita ser actualizado o cambiado cuando surgen ciertas situaciones. Cuando se vuelve a generar o se intercambia el certificado SAML en el servidor de Cisco Identity Services (IdS), puede producirse una interrupción en la conexión de confianza con el proveedor de identidad (IdP). Esta interrupción puede dar lugar a problemas en los que los clientes o usuarios que confían en el inicio de sesión único no pueden obtener la autorización que necesitan para acceder al sistema.

Este documento tiene como objetivo cubrir una amplia gama de situaciones comunes en las que debe crear un nuevo certificado SAML en el servidor de IdS de Cisco. También se explica cómo proporcionar este nuevo certificado al proveedor de identidad (IdP) para que se pueda reconstruir la confianza. De esta forma, los clientes y usuarios pueden seguir utilizando el inicio de sesión único sin problemas. El objetivo es asegurarse de que tiene toda la información que necesita para manejar el proceso de actualización de certificados sin problemas y sin confusión.

Puntos clave que debe recordar:

1. El certificado SAML se genera de forma predeterminada durante la instalación del servidor Cisco IdS con una validez de 3 años

- 2. El certificado SAML es un certificado autofirmado
- 3. El certificado SAML es un certificado SSL que reside en el editor y suscriptor de Cisco IDS
- 4. La regeneración del certificado SAML sólo se pudo realizar en el nodo del editor IDS de Cisco
- 5. Los tipos disponibles del algoritmo hash seguro para el certificado SAML son SHA-1 y SHA-256

6. El algoritmo SHA-1 se utiliza en IdS 11.6 y en versiones anteriores, el algoritmo SHA-256 se utiliza en IdS 12.0 y en versiones posteriores

7. Tanto el proveedor de identidad (IdP) como el servicio de identidad (IdS) deben utilizar el mismo tipo de algoritmo.

8. El certificado SAML de Cisco IdS solo se pudo descargar del nodo Cisco IdS Publisher (sp-<Cisco IdS\_FQDN>.xml)

9. Consulte este enlace para conocer la configuración de registro único de UCCE/PCCE. <u>Guía de características de UCCE 12.6.1</u>

## Certificado SAML vencido

El certificado SAML se genera con una validez de 3 años (1095 días) y se requiere renovar el certificado SAML antes de que caduque. El certificado SSL caducado se considera no válido y

rompe la cadena de certificados entre Cisco Identity Service (IdS) y Identity Provider (IdP).

## Solución

- 1. Compruebe la fecha de vencimiento del certificado SAML
- 2. Regenere el certificado SAML
- 3. Descargue el archivo sp.xml
- 4. Recupere el certificado SAML del archivo sp.xml
- 5. Reemplace el antiguo certificado SAML por el nuevo certificado SAML en el IdP
- 6. Consulte la sección de referencia para ver los pasos detallados



(Nota: {Puesto que solo se ha cambiado el certificado SAML, no es necesario el intercambio de metadatos IdS a IdP})

# Cambio del algoritmo hash seguro en el proveedor de identidad (IdP)

Supongamos que se encuentra en un entorno PCCE/UCCE existente con el inicio de sesión único. El servidor IdP y Cisco IdS se ha configurado con el algoritmo hash seguro SHA-1. Teniendo en cuenta la debilidad del SHA-1 necesaria para cambiar el algoritmo hash seguro a SHA-256.

## Solución

1. Cambie el algoritmo hash seguro en la entidad fiduciaria de confianza de AD FS (SHA-1 a SHA-256)

2. Cambie el algoritmo hash seguro en el publicador de IdS en Claves y certificado (SHA-1 a SHA-256)

- 3. Regenere el certificado SAML en el Editor de IdS
- 4. Descargue el archivo sp.xml
- 5. Recupere el certificado SAML del archivo sp.xml
- 6. Reemplace el antiguo certificado SAML por el nuevo certificado SAML en el IdP
- 7. Consulte la sección de referencia para ver los pasos detallados

## Cambio de dirección IP o nombre de host del servidor Cisco IdS -Editor de CUIC/LiveData/IdS co-residente o Editor de IdS independiente reconstruido - Suscriptor de CUIC/LiveData/IdS co-residente o suscriptor de IdS independiente reconstruido

Estas situaciones se producen con poca frecuencia y se recomienda encarecidamente comenzar de nuevo con la configuración de inicio de sesión único (SSO) para garantizar que la funcionalidad de SSO en el entorno de producción se restaura de forma rápida y eficaz. Es esencial priorizar esta reconfiguración para minimizar cualquier interrupción en los servicios de SSO de los que dependen los usuarios.

## Solución

- 1. Suprímase la Parte fiduciaria que confía existente de AD FS
- 2. Cargue el certificado SSL de AD FS en el servidor de IdS de Cisco para la confianza de gato

- 3. Descargue el archivo sp.xml
- 4. Consulte la sección de referencia y la guía de características para ver los pasos detallados
- 5. Configure la parte de confianza de confianza en AD FS
- 6. Añada las reglas de reclamación
- 7. Activar afirmación SAML firmada
- 8. Descargar metadatos de federación de AD FS
- 9. Cargue los metadatos de federación en el servidor de IdS de Cisco
- 10. Realice la prueba SSO

### Referencia

Cómo agregar una persona de confianza en el ADFS o

Cómo habilitar la afirmación SAML firmada

Consulte este documento para ver los pasos detallados: Guía de características de UCCE 12.6.1

Cómo cargar el certificado SSL de AD FS en la confianza Tomcat de IdS de Cisco

- 1. Descargue o recupere el certificado SSL de AD FS
- 2. Acceda a la página de administración de Cisco IdS Publisher OS
- 3. Inicie sesión con la credencial de administrador del sistema operativo
- 4. Acceda a Seguridad > Gestión de Certificados
- 5. Haga clic en Cargar certificado/cadena de certificado y se abrirá una ventana emergente
- 6. Haga clic en el menú desplegable y seleccione tomcat-trust en Certificate Purpose
- 7. Haga clic en Examinar y seleccione el certificado SSL de AD FS
- 8. Pulse Cargar



(Nota: {Los certificados de confianza se replican en los nodos del suscriptor. No es necesario cargar en el nodo de suscriptor.})

### Cómo eliminar la entidad de confianza de confianza en AD FS

1. Inicie sesión en el servidor del proveedor de identidad (IdP) con la credencial con privilegios de administrador

- 2. Abra el Administrador de servidores y elija AD FS > Herramientas > Administración de AD FS
- 3. En el árbol del lado izquierdo, seleccione Confianza de la parte que confía en AD FS
- 4. Haga clic con el botón derecho del ratón en el servidor de Cisco IdS y seleccione Eliminar



Cómo comprobar o cambiar el algoritmo hash seguro configurado en el proveedor de identidad (IdP)

1. Inicie sesión en el servidor del proveedor de identidad (IdP) con la credencial con privilegios de administrador

- 2. Abra el Administrador de servidores y elija AD FS > Herramientas > Administración de AD FS
- 3. En el árbol del lado izquierdo, seleccione Confianza de la parte que confía en AD FS
- 4. Haga clic con el botón derecho del ratón en el servidor de Cisco IdS y seleccione propiedades
- 5. Acceda a la pestaña Avanzado

6. La opción Secure Hash Algorithm muestra el algoritmo hash seguro configurado en el servidor de AD FS.



7. Haga clic en el menú desplegable y seleccione el algoritmo hash seguro deseado.

Cómo verificar la fecha de vencimiento del certificado SAML del servidor Cisco IdS

1. Inicie sesión en el nodo de editor o suscriptor del servidor de Cisco IdS con las credenciales de usuario de la aplicación

2. Después de iniciar sesión correctamente en la página, se abre Identity Service Management > Nodes

3. Muestra el nodo de editor y suscriptor de IdS de Cisco, el estado y el vencimiento del certificado SAML

altalta cisco	Identity Service Management			
	Nodes			
	👷 - Indicates Primary Node			
Nodes	Node	Status	SAML Certificate Expiry	
\$	CUICPUB-126.vcce.com 🗙	In Service	<ul> <li>11-30-2025 16:18 (997 days left)</li> </ul>	
Settings	CUICSEC-126.vcce.com	In Service	<ul> <li>11-30-2025 16:18 (997 days left)</li> </ul>	
				_

Cómo descargar los metadatos del servidor de IdS de Cisco

1. Inicie sesión en el nodo Cisco IdS Publisher con la credencial de usuario de la aplicación

- 2. Haga clic en el icono Configuración
- 3. Acceda a la pestaña Confianza de IDS

4. Haga clic en el enlace Download (Descargar) para descargar los metadatos del clúster Cisco IdS

altalta cisco	Identity Service Management	n appadmin	
	Settings		
Nodes	145 Trust Security Troubleshooting		
Settings	Download		
Ø	SP Entity ID	Description	Metadata file
Clients	CUICPUB-126.vcce.com	SAML SP to configure IdS access via LAN/WAN	Download
	Note : This operation can be performed only on the primary node.		

Cómo recuperar el certificado SAML del archivo sp.xml

- 1. Abra el archivo sp.xml con un editor de texto
- 2. Copie los datos sin procesar entre el encabezado <ds:X509Certificate></ds:X509Certificate>



- 3. Abra otro editor de texto y pegue los datos copiados
- 4. guarde el archivo en formato .CER

SIMI cer - Notenad	- n x l	
File Edit Format View Help	Save As	×
MIIC7TCCAdWgAwIBAgIECOjgBTANBgkqhkiG9w0BAQsFADAfMR0wGwYDVQQDExRD VUlDUFVCLTEyNi52Y2NlLmNvbTAeFw0yMjEyMDExMDQ4MzRaFw0yNTExMZAxMDQ4	$\leftarrow \rightarrow \sim \uparrow$ 3 > This PC > Downloads > New folder (3)	V O Search New folder (3)
MzRaMB8xHTAbBgHVBAMTFENVSUNQVUItMTI2LnZjY2UuY29tMIIBIjANBgkqhkiG 9w8BADEFAAOCADBAMIIBCgKCADEA2Z3MwEaYDC3P775wcZoTv2ODIIId3mlCwhHB	Organize - New folder	III • 📀
E2iRZDPS1oEDAVHxh4+N6L6u8hgHQvXYrUKuDfvkXdY+XJjE8KJJcjRTy1xDdzY+	A Name A	Date modified Type Size
Ixx6c7tH14jMnxmjVX77M/Pe/NJQuxabrtc7BKm4ru10ndUgFs2TWgGCt+UVpWW BLAjBuSP2PMv23VThtHTW53gt2UMsKX74QbiHcOP10qHT28YSTTMi/f6gXYUU YTMOeZd6F2P/KBDUUEivkcY/5Dy1FqWjt7r+9kgCvN1mf9pu6MzPep3zalVmBC+ iu8b1F2KVTd82a1oEe6M3Hq1w5Mcw1nCoHth1H1p5XB152Hp3H1DAQABozEWLZAO BgNVHQ8BAf8EBAMCBAAHQYDVR00BBYEFBu3Qbua5Xy/n/zwoh1sp1FegnjMA6G CSqGS1b3DQEBCwUAA4IBAQCqVVVydYnmofPpQRh20B7Hyqh12CDhG3MG22aUVwaAU VS9/oLdiev1VUl0Abn0Galt71NZYg1f8Bt1Q35Ubi/T2wzRicgZjtUwLnyhEMwsM uv2Lb2R7F+PFr/LuX7YPLomzny53G654/B59u30ReUSPT2sZE2VRAzgLAMW9Vmqv LsEqf/EzpGYQR1ZBYAUYPO3PRG76ohskU3XxFAepBEUd71Wq1DkFe5MHKgcESd09	Image: Construction     Image: Construction       Imag	10-03-2023 05x40 Security Certificate 2
oogowinpculasksjioboooriskiircoinbvriworbokj	JDK JRE 8U3; #	
	Browser Loas V C	
	File pame: SAMLcer	~
	Save as type: All Files (*.*)	×
Ln 16, Cr	Hide Folders     Encoding: UTF-8	Save Cancel

5. Abra el certificado para revisar la información del certificado

👼 Certif	ficate				×
General	Details	Certification Pat	1		
Show:	<all></all>		$\sim$		
Field			Value		^
E Ver	rsion rial numbe	r	V3		
Sig	nature alg	gorithm	sha256RSA		
🔄 Sig	nature ha	ish algorithm	sha256		
E Iss	uer		CUICPUB-126.	e.com	
🛄 Va	id from		01 December 20	22 16:18:34	
🖂 Va	id to		30 November 20	025 16:18:34	~
	hiect		CLITCPLIB-126	com	
		E	dit Properties	Copy to File	
				0	К

Cómo reemplazar el certificado SAML en AD FS

- 1. Copie el archivo de certificado SAML en el servidor AD FS que se recupera del archivo sp.xml
- 2. Abra el Administrador de servidores y elija AD FS > Herramientas > Administración de AD FS
- 3. En el árbol del lado izquierdo, seleccione Confianza de la parte que confía en AD FS
- 4. Haga clic con el botón derecho del ratón en el servidor de Cisco IdS y seleccione propiedades
- 5. Acceda a la pestaña Firma
- 6. Haga clic en Agregar y seleccione el certificado SAML recién generado
- 7. Seleccione el certificado SAML antiguo y haga clic en Eliminar
- 8. Aplicar y guardar



Cómo regenerar el certificado SAML en el servidor Cisco IdS

- 1. Inicie sesión en el nodo Cisco IdS Publisher con la credencial de usuario de la aplicación
- 2. Haga clic en el icono Configuración
- 3. Acceda a la pestaña Seguridad
- 4. Seleccione la opción Claves y Certificados

#### uluilu cisco Identity Service Management Settings . IdS Trust Security Nodes Generate Keys and SAML Certificate Tokens ₩ Set Token Expiry Encryption/Signature key Settings Regenerate key for token encryption and signing. Regenerate Ð Clients SAML Certificate Regenerate certificate for signing SAML request. Select secure hash algorithm. SHA-256 ŧ Ensure that the selected algorithm type is same as in IdP. Perform the metadata exchange after the certificate is regenerated and ensure that the SSO Test is

### 5. haga clic en el botón Regenerar en la sección Certificado SAML (resaltado)

Prueba de SSO

Siempre que haya un cambio en el certificado SAML, asegúrese de que el SSO DE PRUEBA sea exitoso en el servidor de IdS de Cisco y vuelva a registrar todas las aplicaciones desde la página CCEAdmin.

- 1. Acceda a la página CCEAdmin desde el servidor de AW principal
- 2. Inicie sesión en el portal CCEAdmin con los privilegios de nivel de administrador
- 3. Acceda a Visión General > Funciones > Inicio de sesión único
- 4. Haga clic en el botón Register (Registrarse) debajo de Register with Cisco Identity Service
- 5. Realice la prueba SSO

### 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).