Ejemplo de Configuración de Unity Connection Versión 10.5 SAML SSO

Contenido

Introducción

Este documento describe cómo configurar y verificar el lenguaje de marcado de aserción de seguridad (SAML) Single Sign-on (SSO) para Cisco Unity Connection (UCXN).

Prerequisites

Requirements

Configuración del protocolo de tiempo de red (NTP)

Para que SAML SSO funcione, debe instalar la configuración NTP correcta y asegurarse de que la diferencia de tiempo entre las aplicaciones Identity Provider (IdP) y Unified Communications no exceda de tres segundos. Para obtener información sobre cómo sincronizar los relojes, vea la sección Configuración de NTP en la Guía de Administración del Sistema Operativo de Cisco Unified Communications.

Configuración del servidor de nombres de dominio (DNS)

Las aplicaciones de Unified Communications pueden utilizar DNS para resolver los nombres de dominio completos (FQDN) a las direcciones IP. Los proveedores de servicios y el IdP deben ser resueltos por el navegador.

El servicio de federación de directorios activos (AD FS) versión 2.0 debe estar instalado y configurado para manejar las solicitudes SAML.

Componentes Utilizados

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

- AD FS versión 2.0 como IdP
- UCXN como proveedor de servicios
- Microsoft Internet Explorer versión 10

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. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

SAML es un formato de datos basado en XML y estándar abierto para el intercambio de datos. Se trata de un protocolo de autenticación utilizado por los proveedores de servicios para autenticar a un usuario. La información de autenticación de seguridad se pasa entre un IdP y el Proveedor de servicios.

SAML es un estándar abierto que permite a los clientes autenticarse con cualquier servicio de colaboración (o Unified Communication) habilitado para SAML, independientemente de la plataforma del cliente.

Todas las interfaces web de Cisco Unified Communication, como Cisco Unified Communications Manager (CUCM) o UCXN, utilizan el protocolo SAML versión 2.0 en la función SAML SSO. Para autenticar al usuario del protocolo ligero de acceso a directorios (LDAP), UCXN delega una solicitud de autenticación en el IdP. Esta solicitud de autenticación generada por UCXN es una solicitud SAML. El IdP autentica y devuelve una afirmación SAML. La afirmación SAML muestra Sí (autenticado) o No (error de autenticación).

SAML SSO permite a un usuario LDAP iniciar sesión en aplicaciones cliente con un nombre de usuario y una contraseña que se autentican en el IdP. El usuario que inicia sesión en cualquiera de las aplicaciones web admitidas en productos de Unified Communication, después de habilitar la función SAML SSO, también obtiene acceso a estas aplicaciones web en UCXN (excepto CUCM y CUCM IM and Presence):

Usuarios de Unity Connection	Aplicaciones web
Usuarios LDAP con derechos de administrador	• Administración de UCXN • Capacidad de servicio de Cisco UCXN • Serviciabilidad de Cisco Unified • Asistente de comunicaciones personales de Cisco • Bandeja de entrada web • Mini bandeja de entrada en la Web (versión de escritorio)
Usuarios LDAP sin derechos de administrador	• Asistente de comunicaciones personales de Cisco • Bandeja de entrada web • Mini bandeja de entrada en la Web (versión de escritorio) • Clientes de Cisco Jabber

Configurar

Diagrama de la red

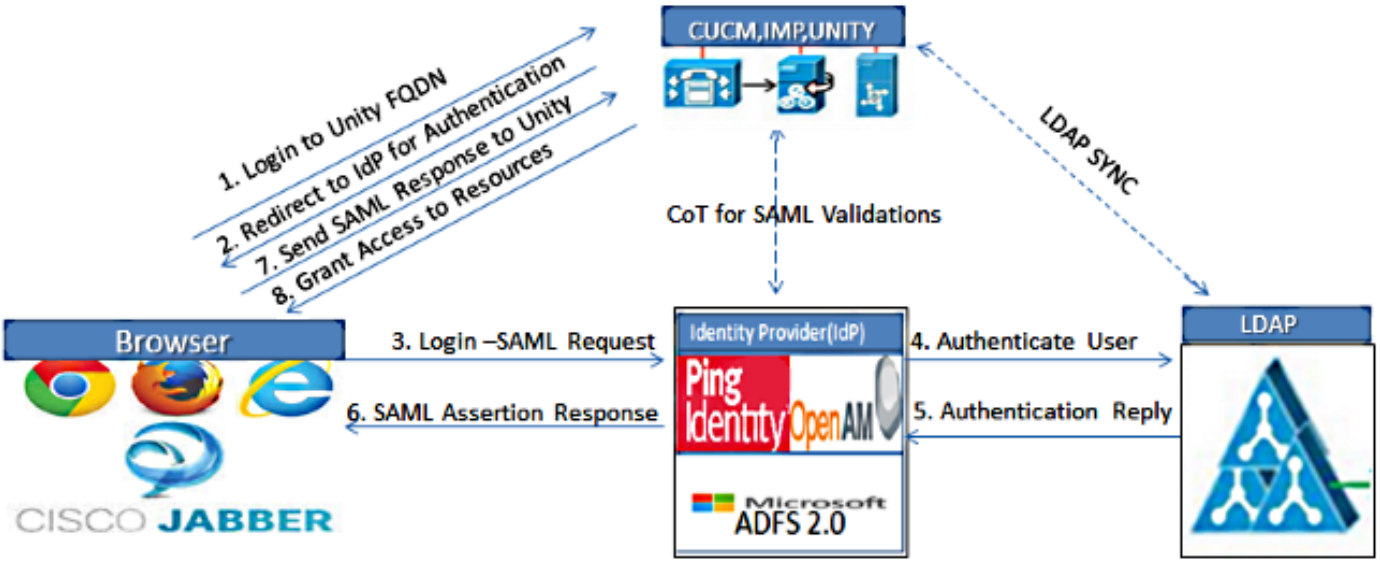
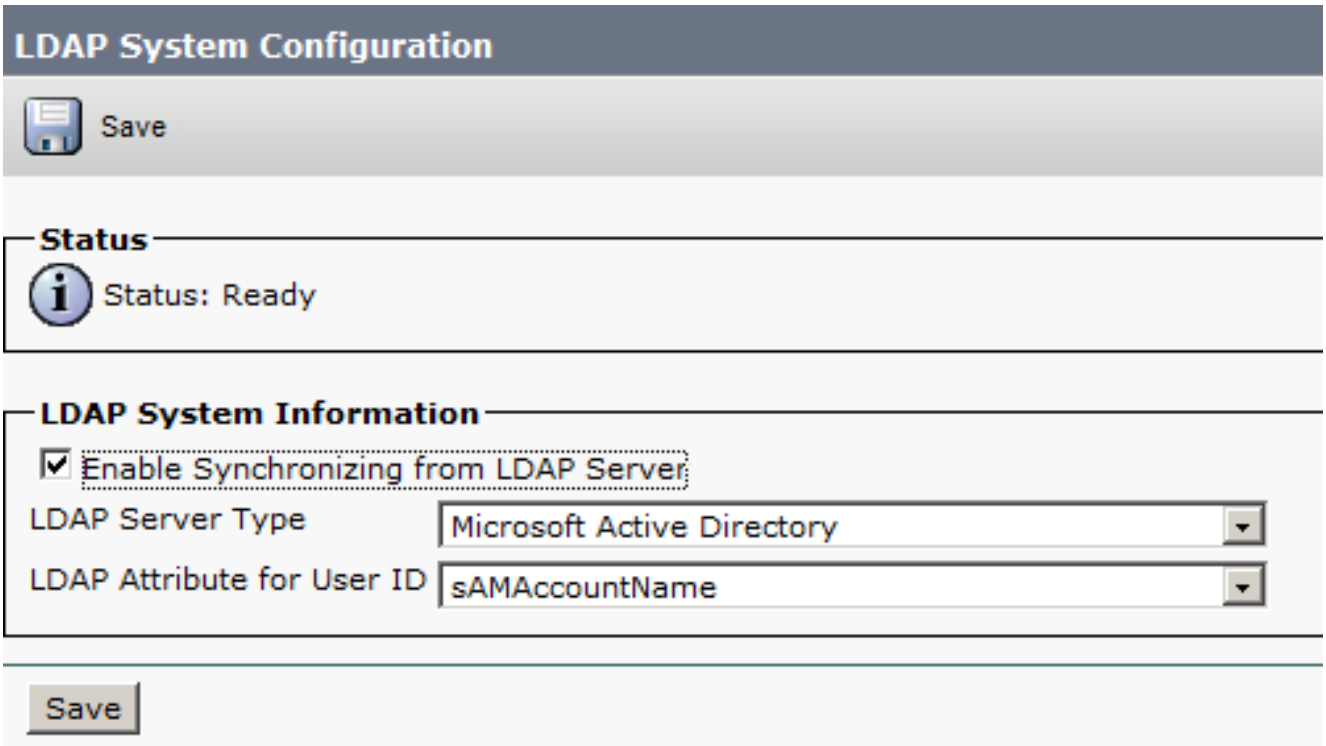


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

Configuración del directorio

1. Inicie sesión en la página de administración de UCXN y seleccione **LDAP** y haga clic en **Configuración de LDAP**.

2. Marque **Enable Synchronizing from LDAP Server** y haga clic en **Save**.



3. Haga clic en **LDAP**.

4. Haga clic en **Configuración del directorio LDAP**.

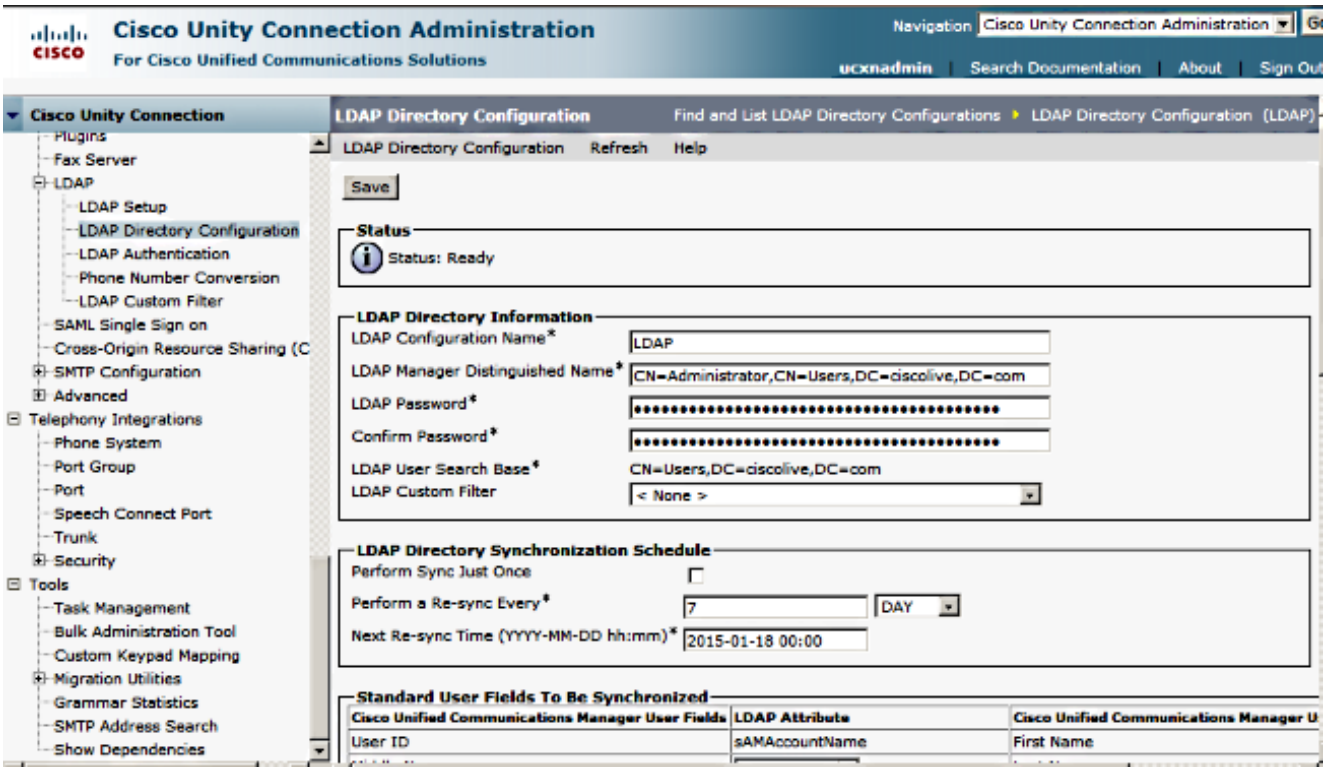
5. Haga clic en **Agregar nuevo**.

6. Configure estos elementos:

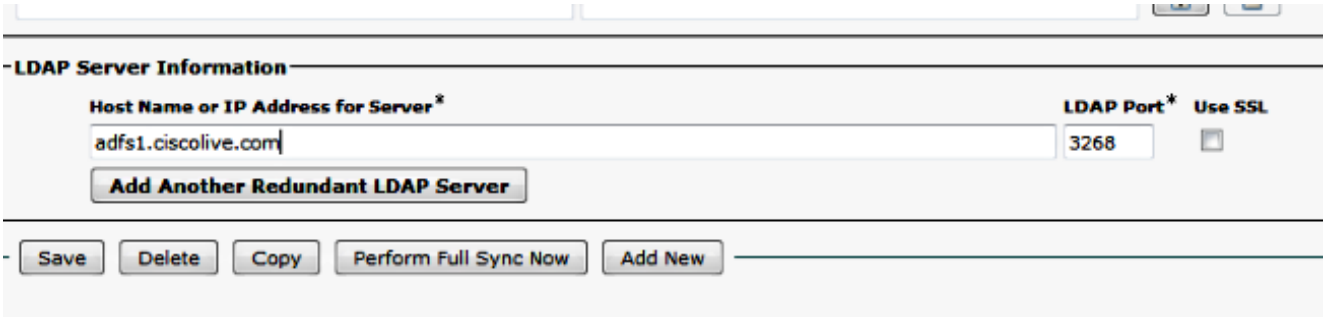
   Configuración de la cuenta de directorio LDAPAtributos de usuario que se van a sincronizarProgramación de sincronizaciónNombre de host o dirección IP del servidor LDAP y número de puerto

7. Marque **Use SSL** si desea utilizar Secure Socket Layer (SSL) para comunicarse con el directorio LDAP.

   Consejo: Si configura LDAP sobre SSL, cargue el certificado de directorio LDAP en CUCM. Refiérase al contenido del directorio LDAP en el SRND de Cisco Unified Communications Manager para obtener información sobre el mecanismo de sincronización de cuentas para productos LDAP específicos y prácticas recomendadas generales para la sincronización LDAP.



8. Haga clic en **Realizar sincronización completa ahora**.



Nota: Asegúrese de que el servicio **Cisco DirSync** esté habilitado en la página web Serviceability antes de hacer clic en Save (Guardar).

9. Expanda **Users** y seleccione **Import Users**.

10. En la lista **Buscar usuarios finales de Unified Communications Manager**, seleccione **Directorio LDAP**.

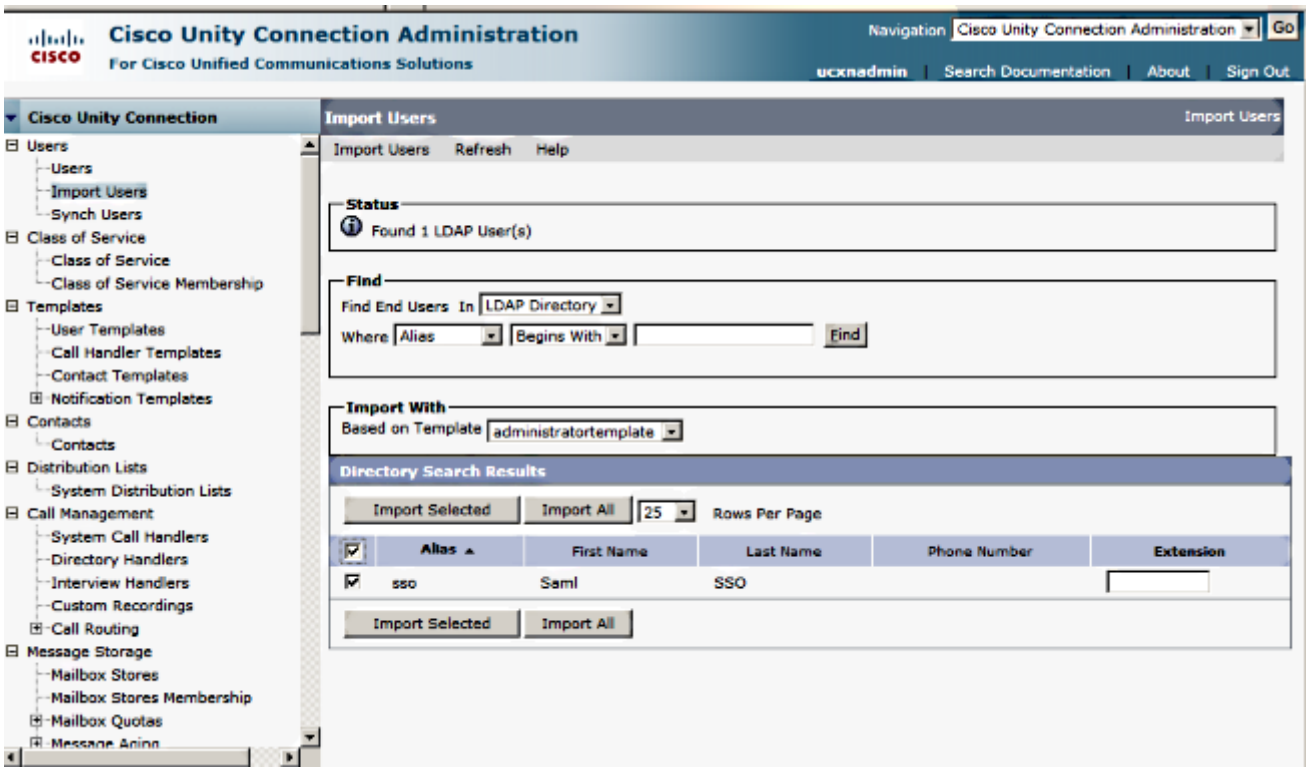
11. Si desea importar sólo un subconjunto de los usuarios en el directorio LDAP con el que ha integrado UCXN, introduzca las especificaciones aplicables en los campos de búsqueda.

12. Seleccione **Find**.

13. En la lista Basado en plantilla, seleccione la **plantilla de administrador** que desea utilizar UCXN cuando cree los usuarios seleccionados.

    Precaución: Si especifica una plantilla de administrador, los usuarios no tendrán buzones.

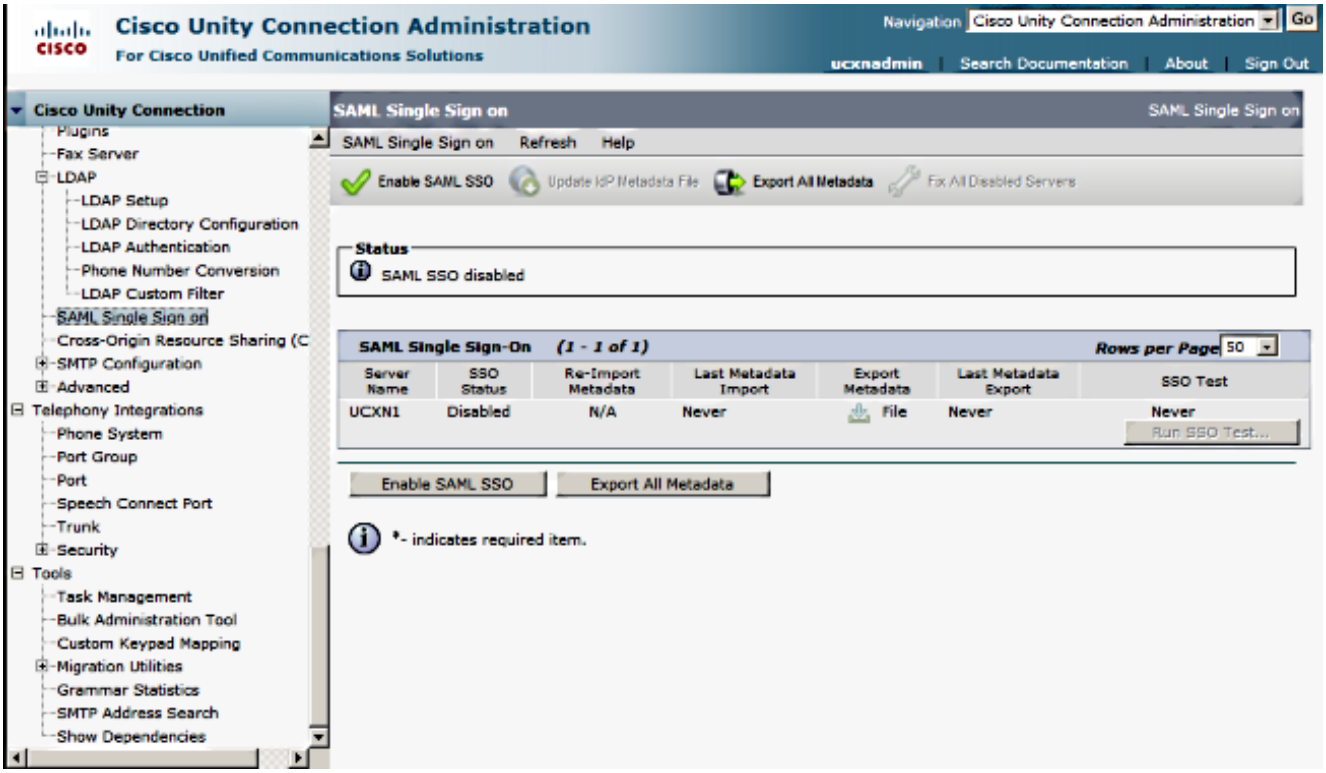
14. Active las casillas de verificación de los usuarios LDAP para los que desea crear usuarios UCXN y haga clic en **Importar seleccionados**.



Habilitar SAML SSO

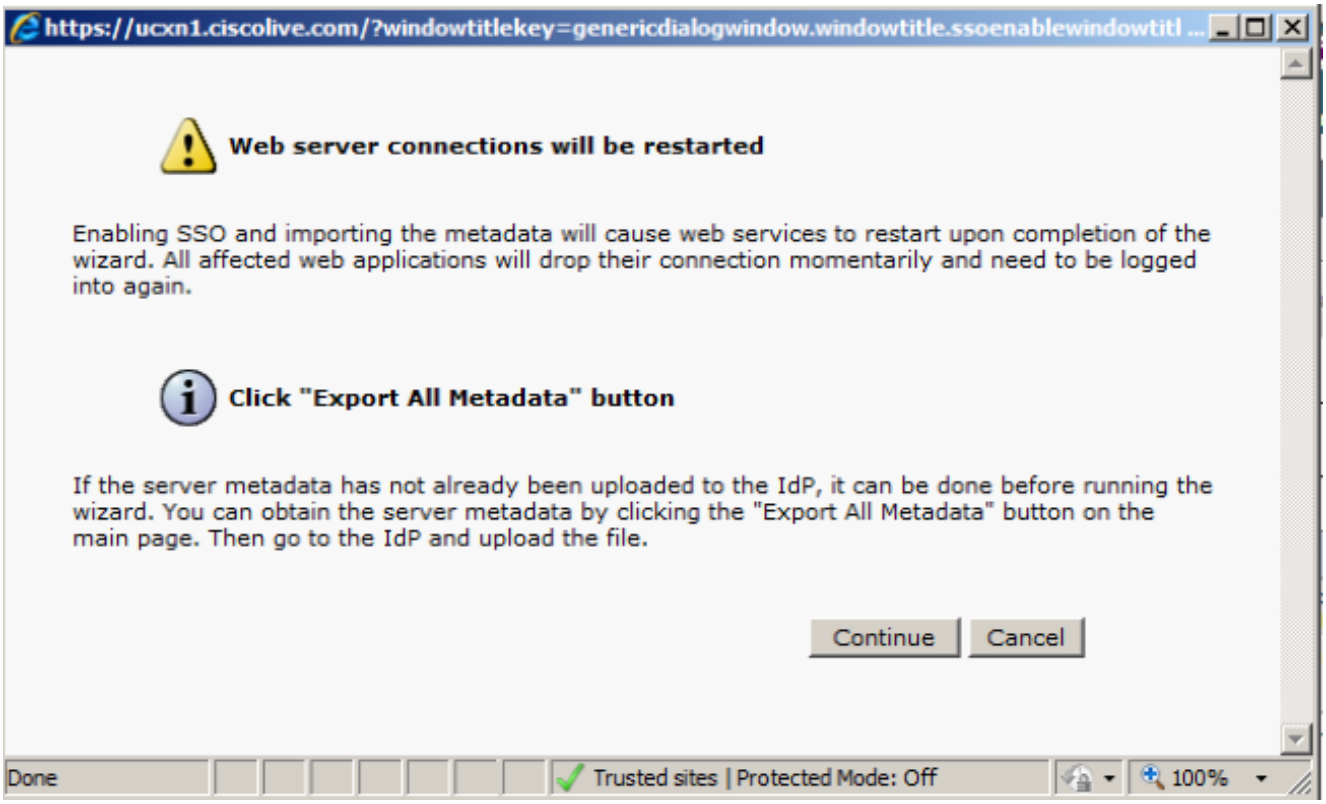
1. Inicie sesión en la interfaz de usuario de Administración de UCXN.

2. Elija **System > SAML Single Sign-on** y se abrirá la ventana SAML SSO Configuration.

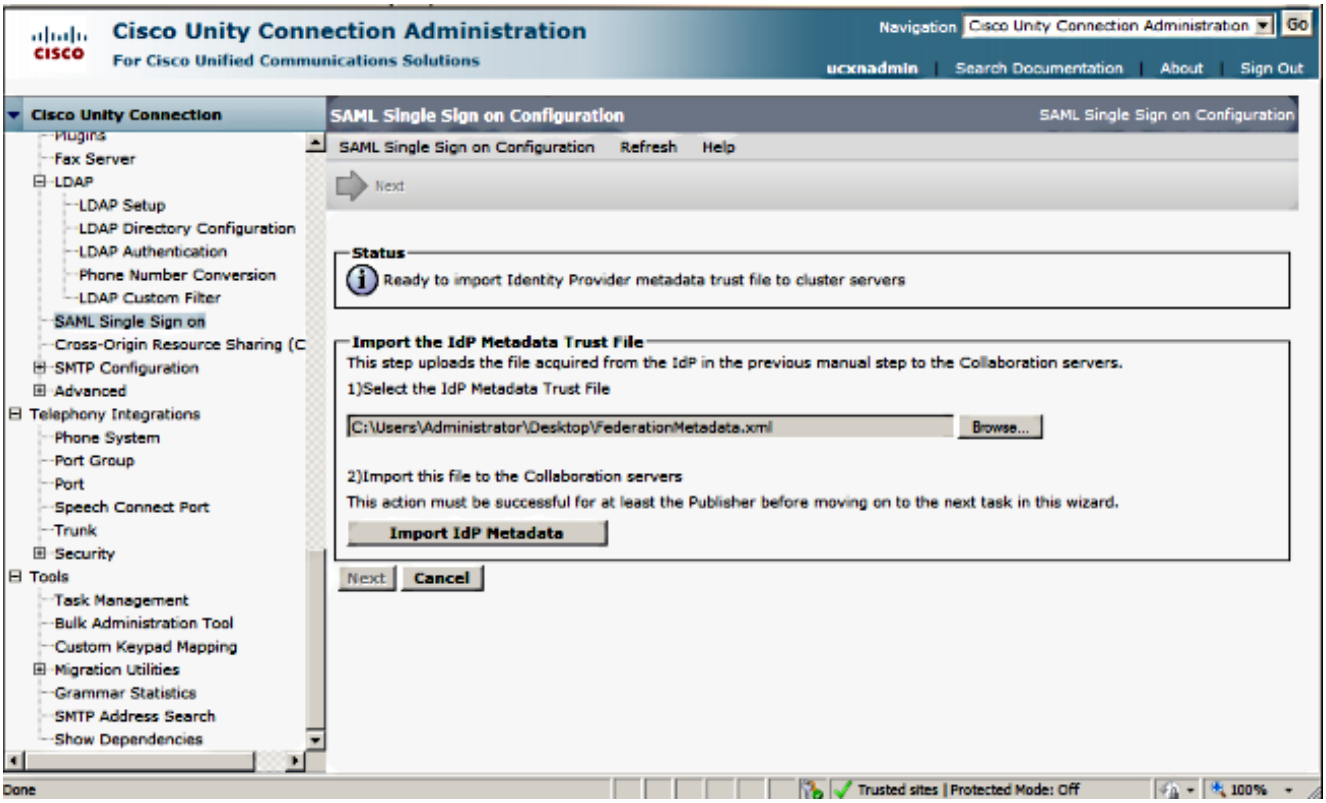


3. Para habilitar SAML SSO en el clúster, haga clic en **Habilitar SAML SSO**.

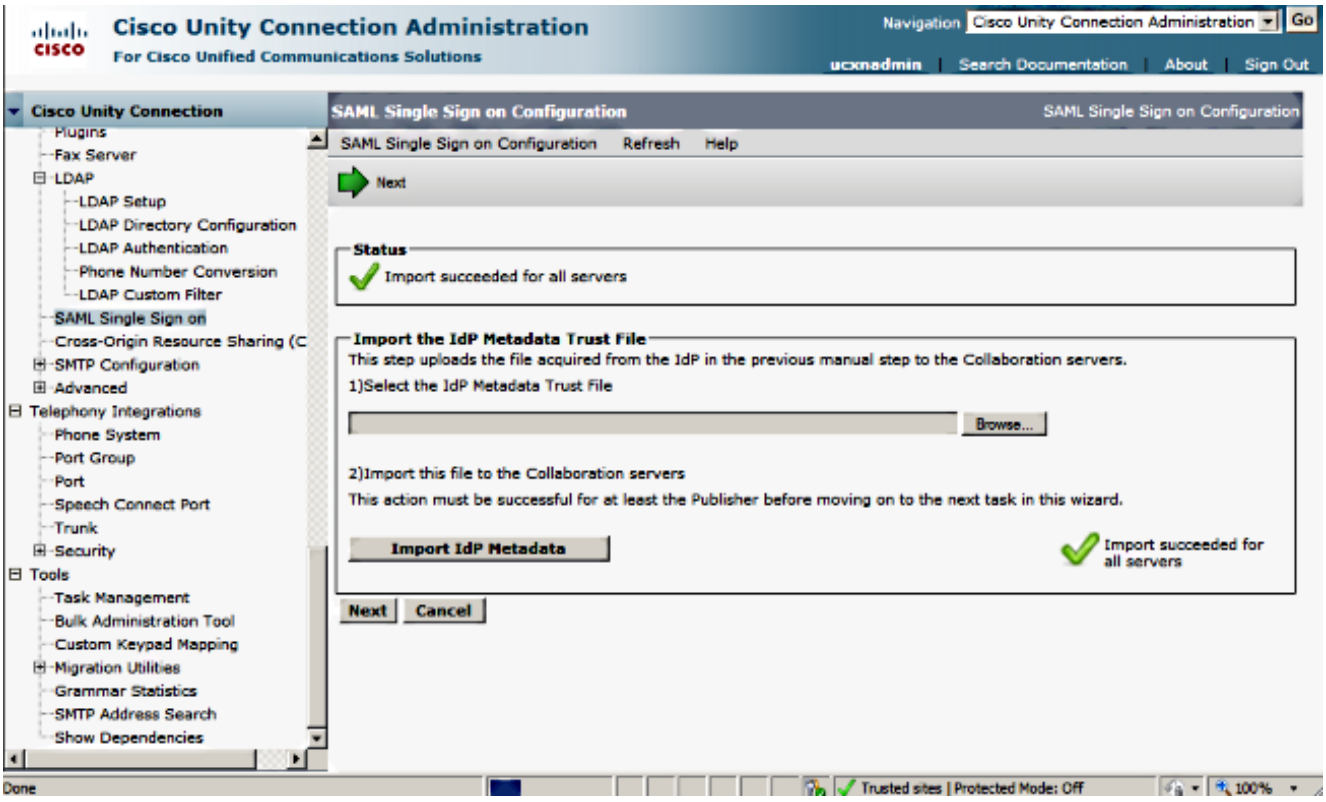
4. En la ventana Restablecer advertencia, haga clic en **Continuar.**



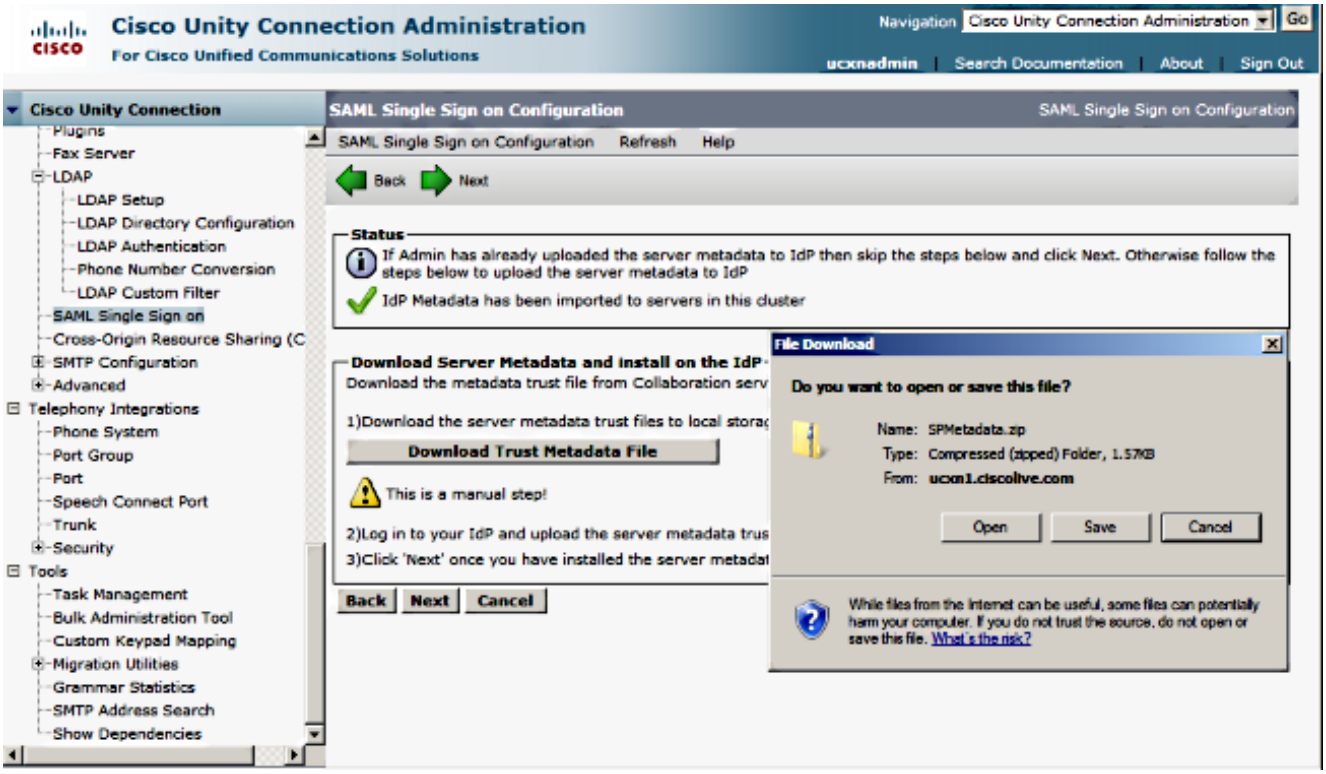
5. En la pantalla SSO, haga clic en **Examinar** para importar el archivo XML de metadatos **FederationMetadata.xml** con el paso **Descargar metadatos Idp**.



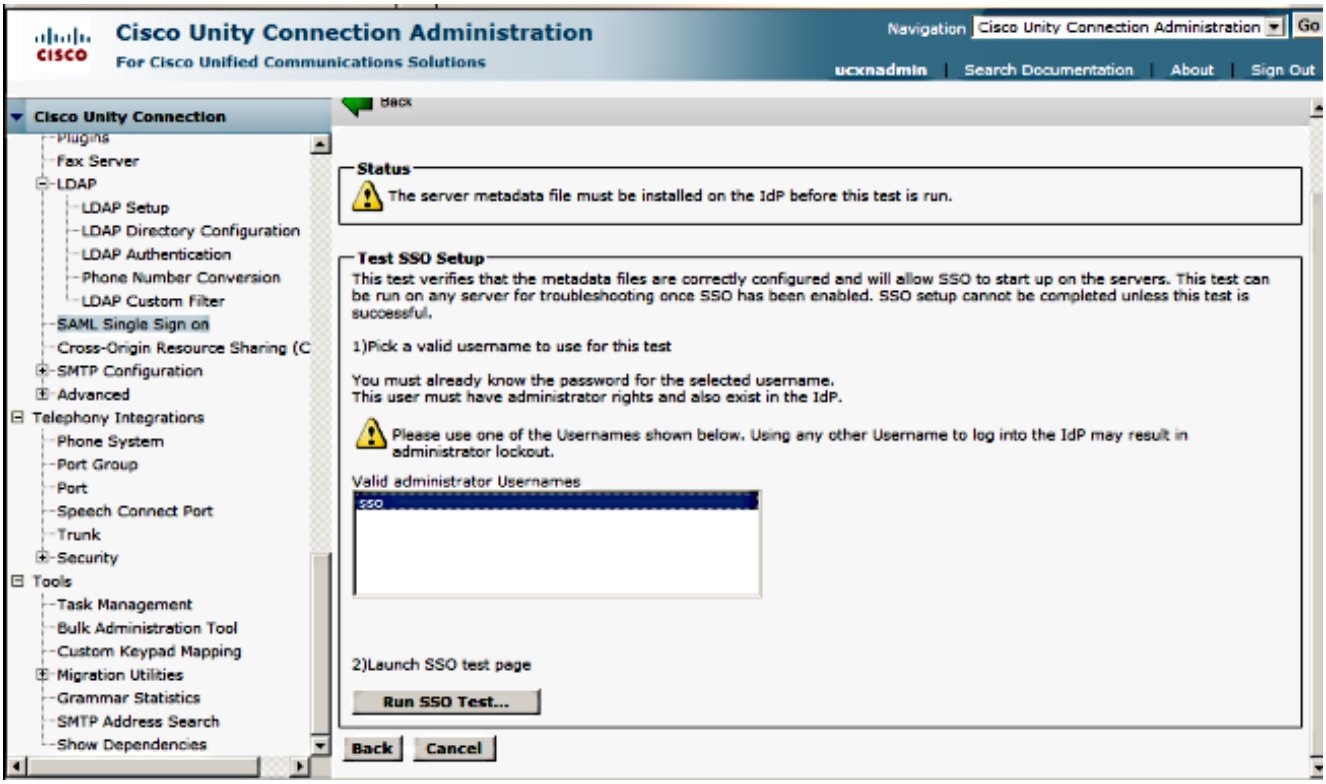
6. Una vez cargado el archivo de metadatos, haga clic en **Importar metadatos IdP** para importar la información de IdP a UCXN. Confirme que la importación se ha realizado correctamente y haga clic en **Siguiente** para continuar.



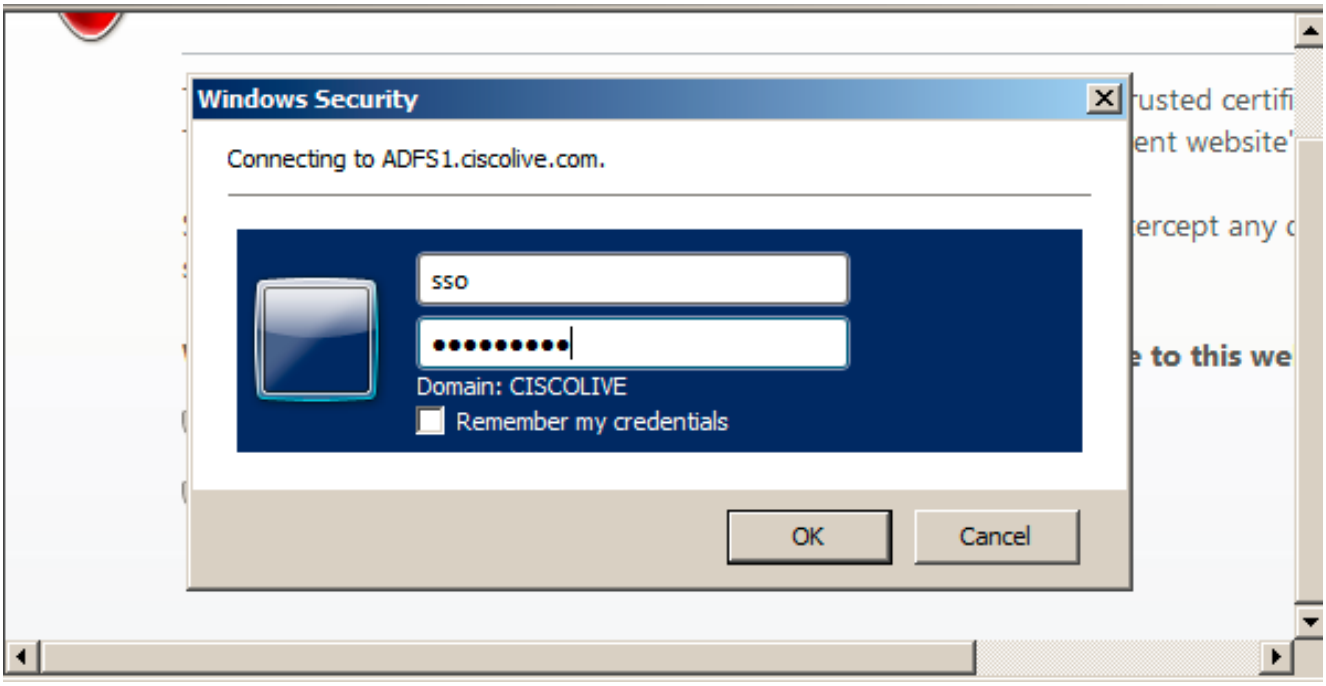
7. Haga clic en **Descargar conjunto de archivos de metadatos de confianza** (sólo si no ha configurado el ADFS ya con metadatos UCXN) para guardar los metadatos UCXN en una carpeta local y vaya a Agregar UCXN como confianza de parte reactiva. Una vez completada la configuración de AD FS, continúe con el paso 8.



8. Seleccione **SSO** como usuario administrativo y haga clic en **Ejecutar prueba SSO**.

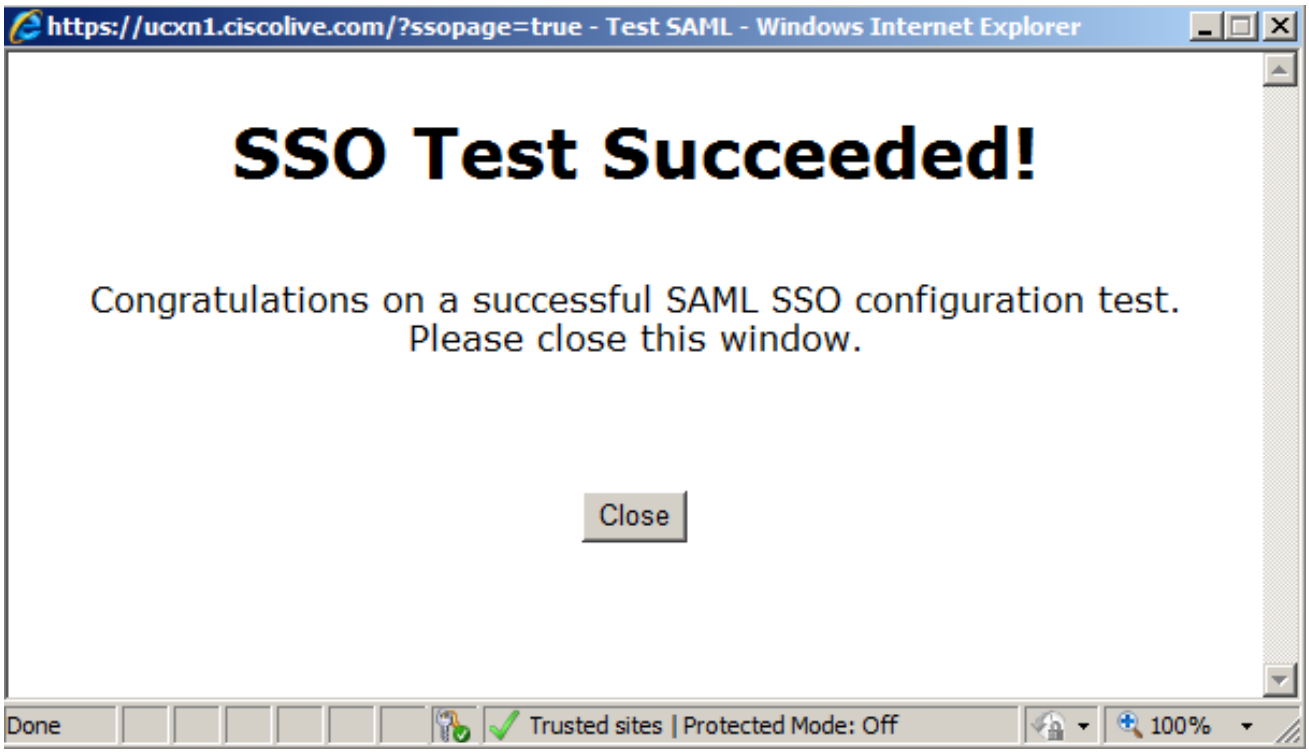


9. Ignore las advertencias del certificado y continúe. Cuando se le pida las credenciales, ingrese el nombre de usuario y la contraseña del SSO del usuario y haga clic en **Aceptar**.



Nota: Este ejemplo de configuración se basa en certificados autofirmados UCXN y AD FS. En caso de que utilice certificados de autoridad certificadora (CA), deben instalarse los certificados adecuados tanto en AD FS como en UCXN. Refiérase a Administración y Validación de Certificados para obtener más información.

10. Después de completar todos los pasos, recibirá la "Prueba de SSO satisfactoria". mensaje. Haga clic en **Cerrar** y **Finalizar** para continuar.



Ya ha completado correctamente las tareas de configuración para habilitar SSO en UCXN con AD FS.

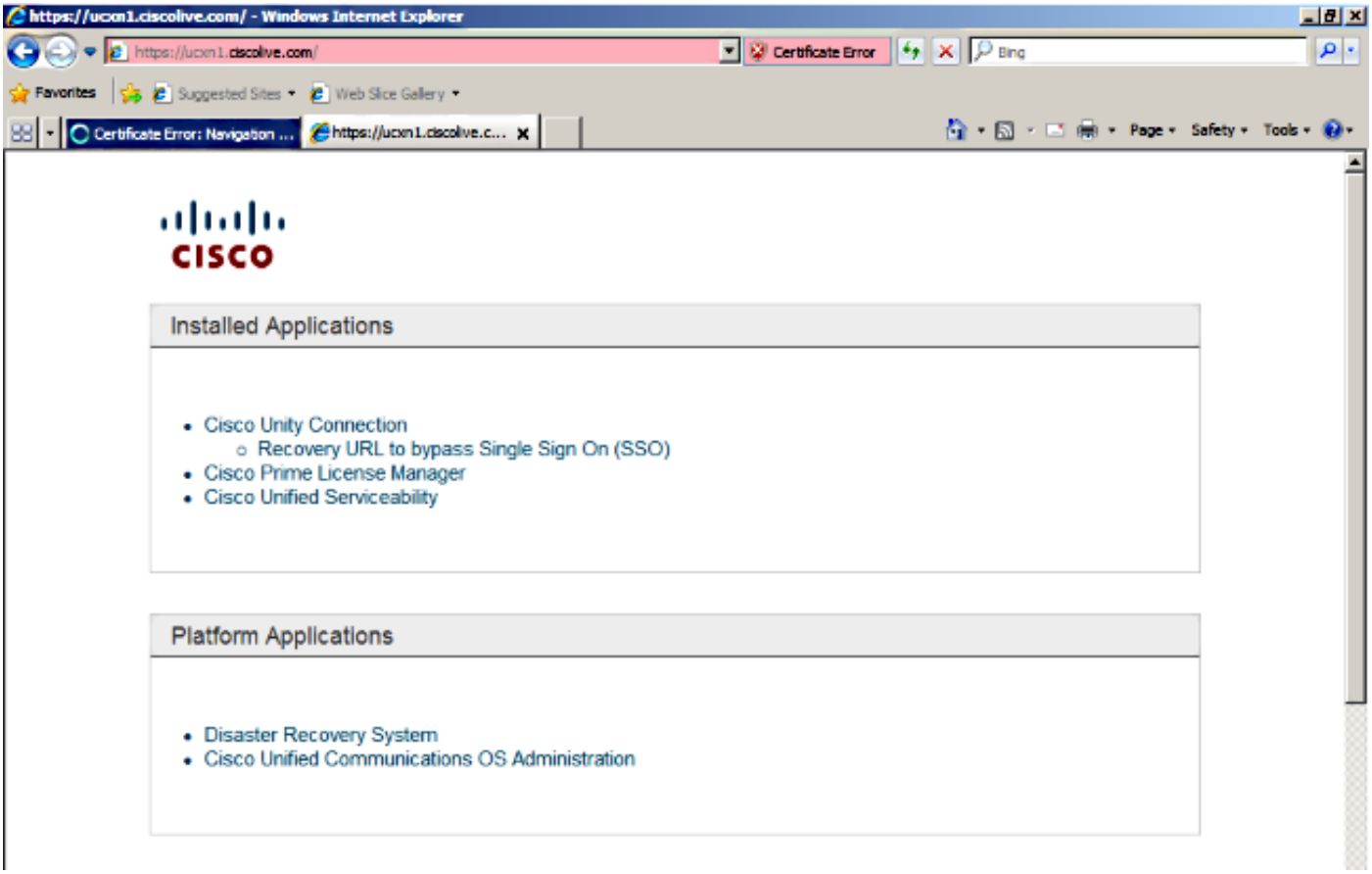
Nota obligatoria: Ejecute la prueba SSO para el suscriptor UCXN si es un clúster para habilitar SAML SSO. AD FS se debe configurar para todos los nodos de UCXN en un clúster.

Consejo: Si configura los archivos XML de metadatos de todos los nodos en IdP y comienza a habilitar la operación SSO en un nodo, SAML SSO se activará automáticamente en todos los nodos del clúster.

También puede configurar CUCM y CUCM IM and Presence para SAML SSO si desea utilizar SAML SSO para clientes Cisco Jabber y ofrecer una verdadera experiencia de SSO a los usuarios finales.

Verificación

Abra un navegador web e introduzca el FQDN de UCXN y verá una nueva opción en Aplicaciones instaladas llamada **URL de recuperación para omitir el inicio de sesión único (SSO)**. Una vez que haga clic en el enlace **Cisco Unity Connection**, el AD FS le solicitará las credenciales. Después de ingresar las credenciales del usuario SSO, se conectará correctamente a la página Unity Administration (Administración de Unity), página Unified Serviceability (Serviciabilidad unificada).



Nota: SAML SSO no permite el acceso a estas páginas:
- Prime Licensing Manager
- Administración del SO
- Sistema de recuperación ante desastres

Troubleshoot

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

Refiérase a Troubleshooting de SAML SSO para Productos de Colaboración 10.x para obtener más información.