Exemplo de Configuração do SSO SAML do Unity Connection versão 10.5

Contents

Introduction

Este documento descreve como configurar e verificar o SSO (Single Sign-on, login único) do SAML (Security Assertion Markup Language) para o UCXN (Cisco Unity Connection).

Prerequisites

Requirements

Configuração do Network Time Protocol (NTP)

Para que o SSO SAML funcione, você deve instalar a configuração NTP correta e certificar-se de que a diferença de tempo entre o Provedor de identidade (IdP) e os aplicativos de comunicações unificadas não exceda três segundos. Para obter informações sobre a sincronização de relógios, consulte a seção Configurações do NTP no Guia de Administração do Sistema Operacional do Cisco Unified Communications.

Configuração do Domain Name Server (DNS)

Os aplicativos de Comunicações Unificadas podem usar DNS para resolver nomes de domínio totalmente qualificados (FQDNs) para endereços IP. Os provedores de serviços e o IdP devem ser resolvidos pelo navegador.

O Ative Diretory Federation Service (AD FS) Versão 2.0 deve ser instalado e configurado para tratar solicitações SAML.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- AD FS Versão 2.0 como IdP
- UCXN como provedor de serviços
- Microsoft Internet Explorer versão 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.

Informações de Apoio

SAML é um formato de dados baseado em XML e de padrão aberto para troca de dados. É um protocolo de autenticação usado por provedores de serviços para autenticar um usuário. As informações de autenticação de segurança são passadas entre um IdP e o provedor de serviços.

O SAML é um padrão aberto que permite que os clientes se autentiquem contra qualquer serviço de colaboração habilitado por SAML (ou Comunicação unificada), independentemente da plataforma do cliente.

Todas as interfaces da Web do Cisco Unified Communication, como Cisco Unified Communications Manager (CUCM) ou UCXN, usam o protocolo SAML Versão 2.0 no recurso SSO SAML. Para autenticar o usuário do Lightweight Diretory Access Protocol (LDAP), o UCXN delega uma solicitação de autenticação ao IdP. Essa solicitação de autenticação gerada pelo UCXN é uma solicitação SAML. O IdP autentica e retorna uma Asserção SAML. A Asserção SAML mostra Sim (autenticado) ou Não (falha na autenticação).

O SSO SAML permite que um usuário LDAP faça login em aplicativos cliente com um nome de usuário e senha que se autentica no IdP. Um usuário que se conecta a qualquer um dos aplicativos da Web suportados em produtos do Unified Communication, depois de habilitar o recurso SSO SAML, também obtém acesso a esses aplicativos da Web no UCXN (além do CUCM e CUCM IM e Presence):

Usuários do Unity Connection	Aplicativos da Web
Usuários LDAP com direitos de administrador	• Administração de UCXN • Capacidade de serviço do Cisco UCXN • Cisco Unified Serviceability • Assistente pessoal de comunicações da Cisco • Caixa de Entrada da Web • Caixa de Entrada da Web (versão do desktop)
Usuários LDAP sem direitos de administrador	• Assistente pessoal de comunicações da Cisco • Caixa de Entrada da Web • Caixa de Entrada da Web (versão do desktop) • Clientes Cisco Jabber

Configurar

Diagrama de Rede

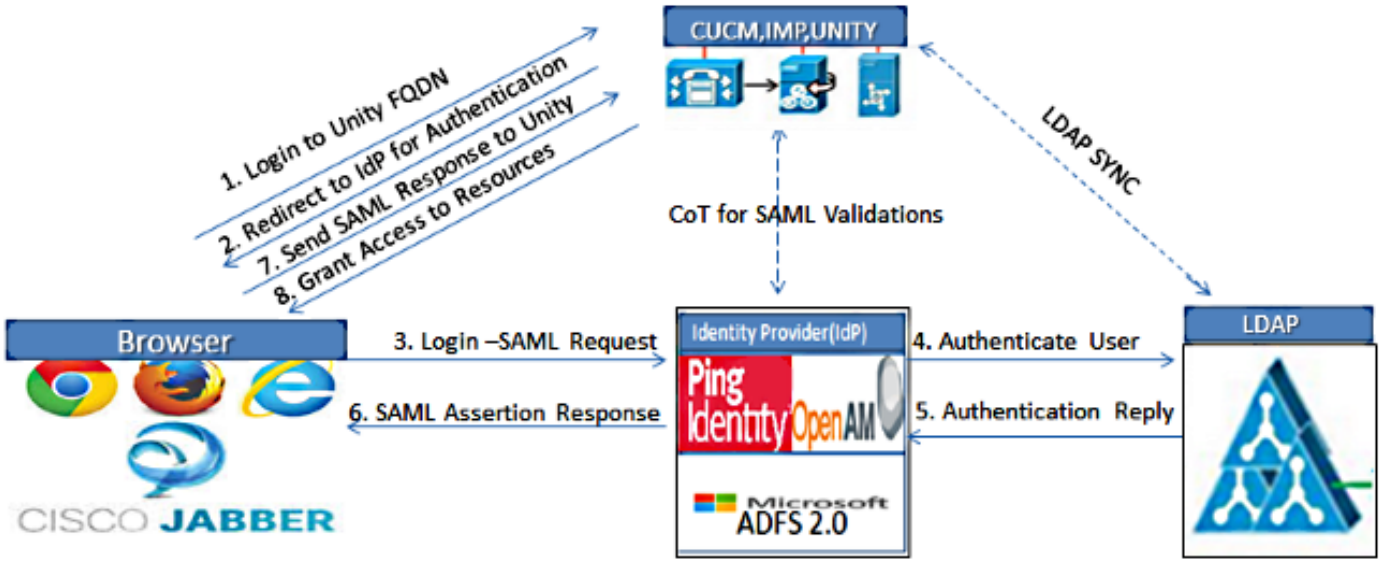
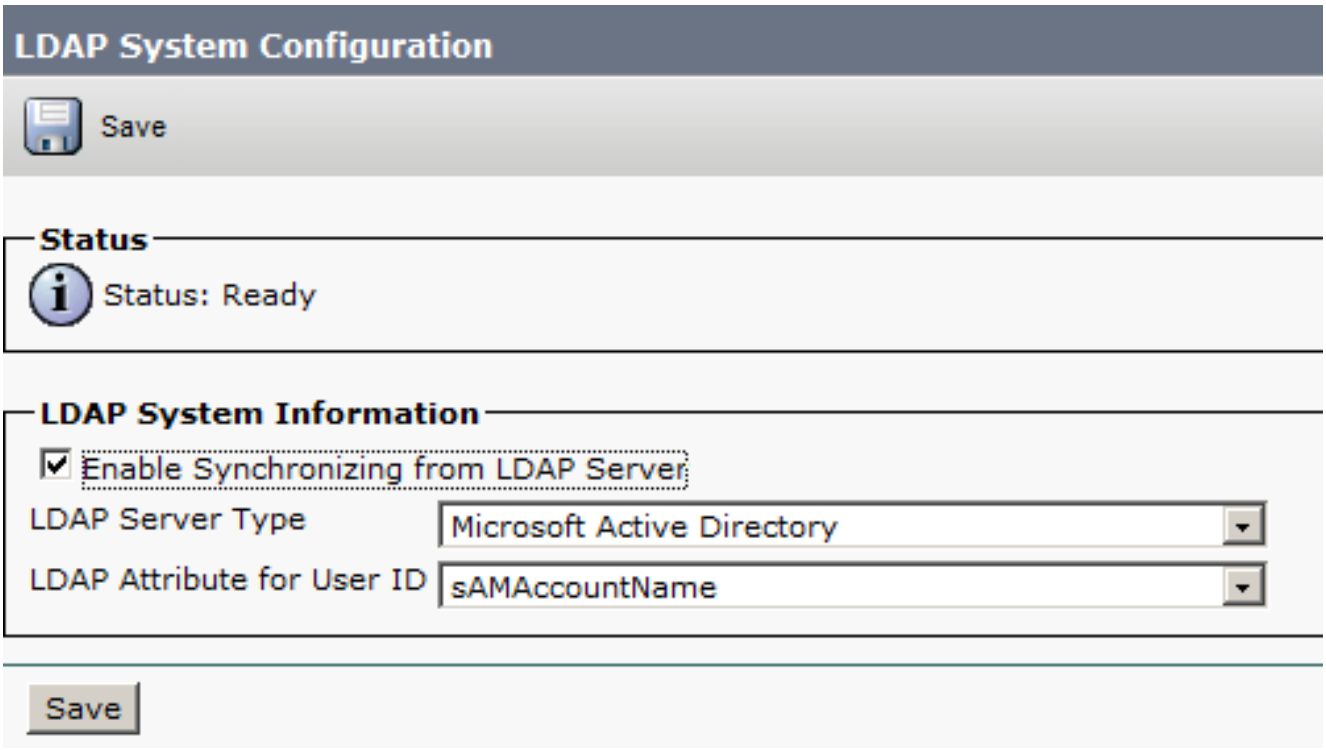


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

Configurando diretórios

1. Entre na página de administração UCXN e selecione **LDAP** e clique em **Configuração LDAP**.

2. Marque **Enable Synchronizing from LDAP Server (Ativar sincronização do servidor LDAP)** e clique em **Save (Salvar)**.



3. Clique em **LDAP**.

4. Clique em **LDAP Diretory Configuration**.

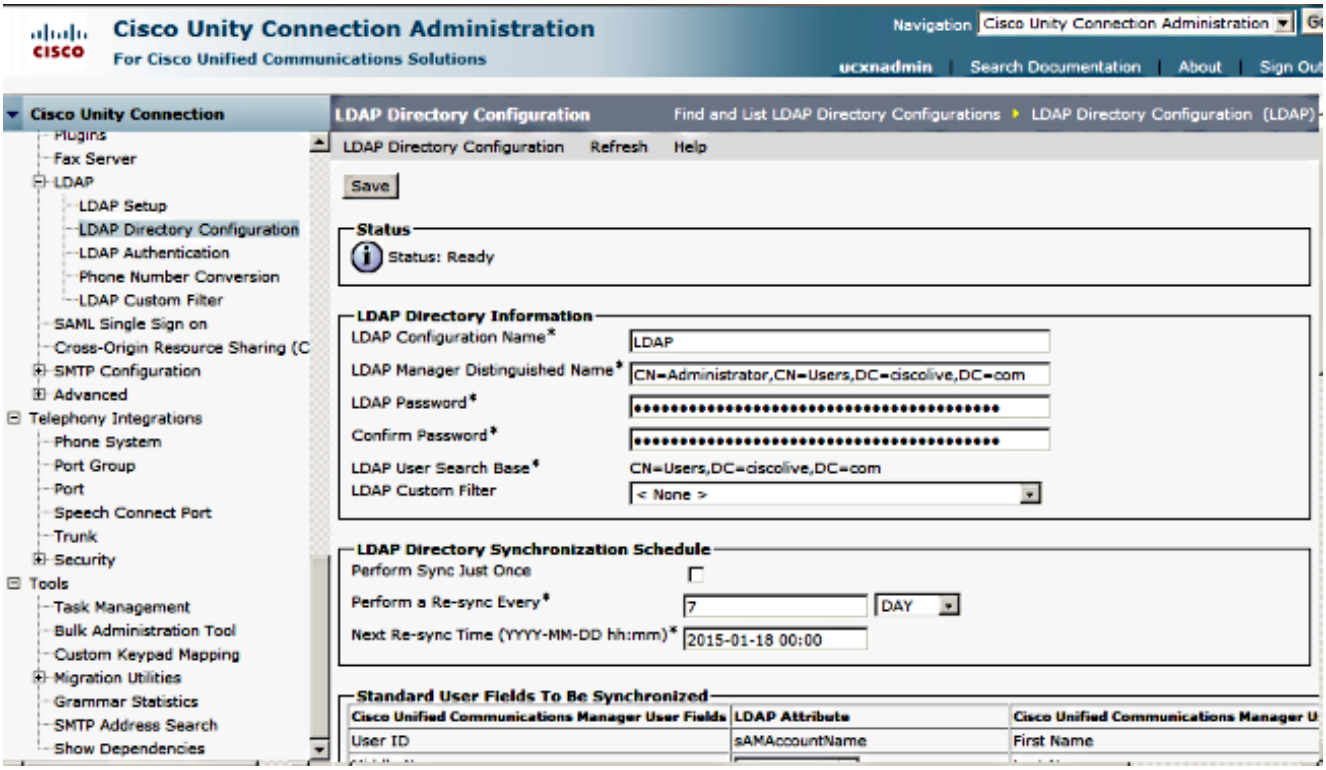
5. Clique em **Adicionar novo**.

6. Configure estes itens:

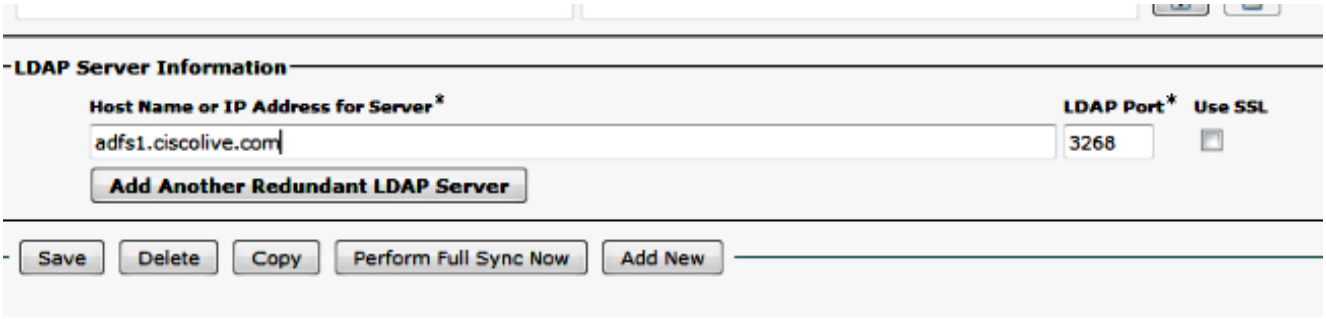
   Configurações de conta de diretório LDAPAtributos de usuário a serem sincronizadosAgenda de sincronizaçãoNome de host do servidor LDAP ou endereço IP e número de porta

7. Marque **Usar SSL** se quiser usar SSL (Secure Socket Layer) para se comunicar com o diretório LDAP.

   Tip: Se você configurar LDAP sobre SSL, faça upload do certificado de diretório LDAP para CUCM. Consulte o conteúdo do diretório LDAP no Cisco Unified Communications Manager SRND para obter informações sobre o mecanismo de sincronização de conta para produtos LDAP específicos e as práticas recomendadas gerais para sincronização LDAP.



8. Clique em **Executar sincronização completa agora**.



Note: Certifique-se de que o serviço **Cisco DirSync** esteja habilitado na página da Web Serviceability antes de clicar em Salvar.

9. Expanda **Users** e selecione **Import Users**.

10. Na lista **Localizar usuários finais do Unified Communications Manager**, selecione **Diretório LDAP**.

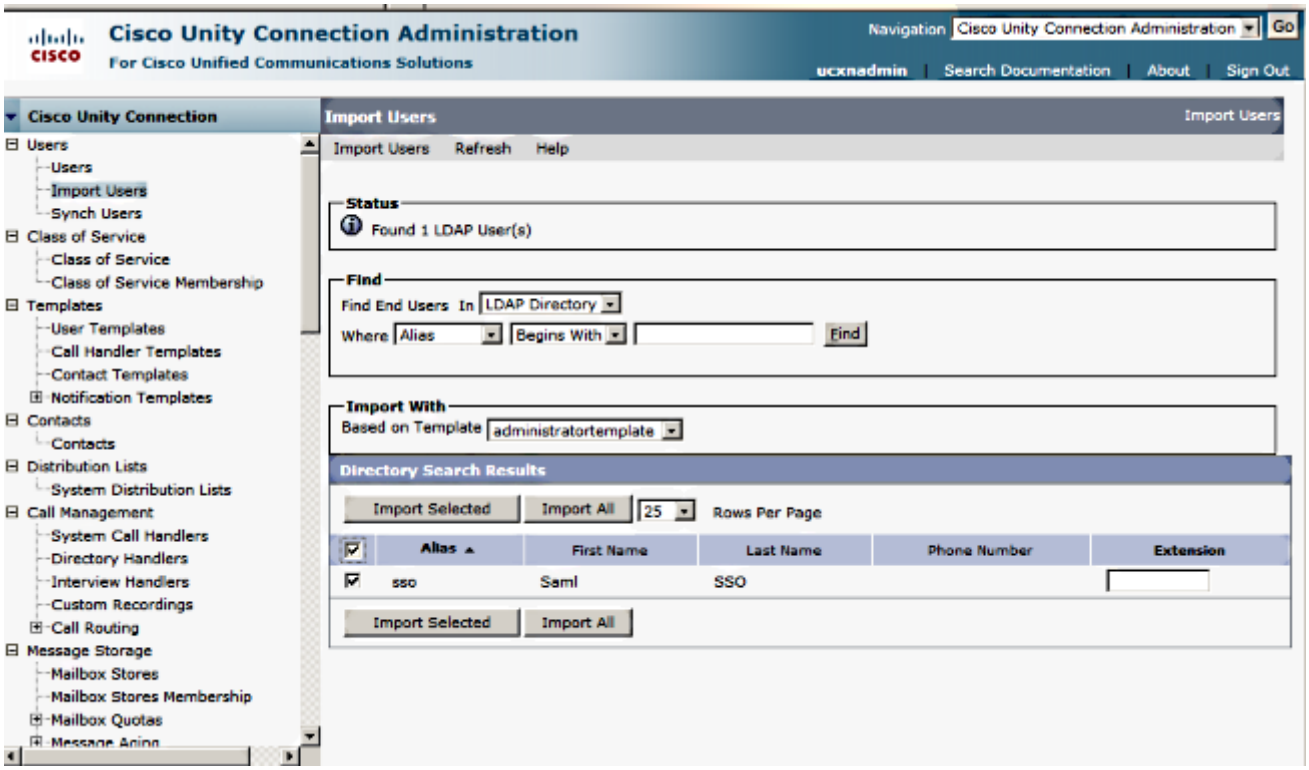
11. Para importar apenas um subconjunto dos usuários no diretório LDAP com o qual você integrou o UCXN, insira as especificações aplicáveis nos campos de pesquisa.

12. Selecione **Localizar**.

13. Na lista Baseado em modelo, selecione o **modelo de administrador** que deseja que o UCXN use quando criar os usuários selecionados.

    Caution: Se você especificar um modelo de administrador, os usuários não terão caixas de correio.

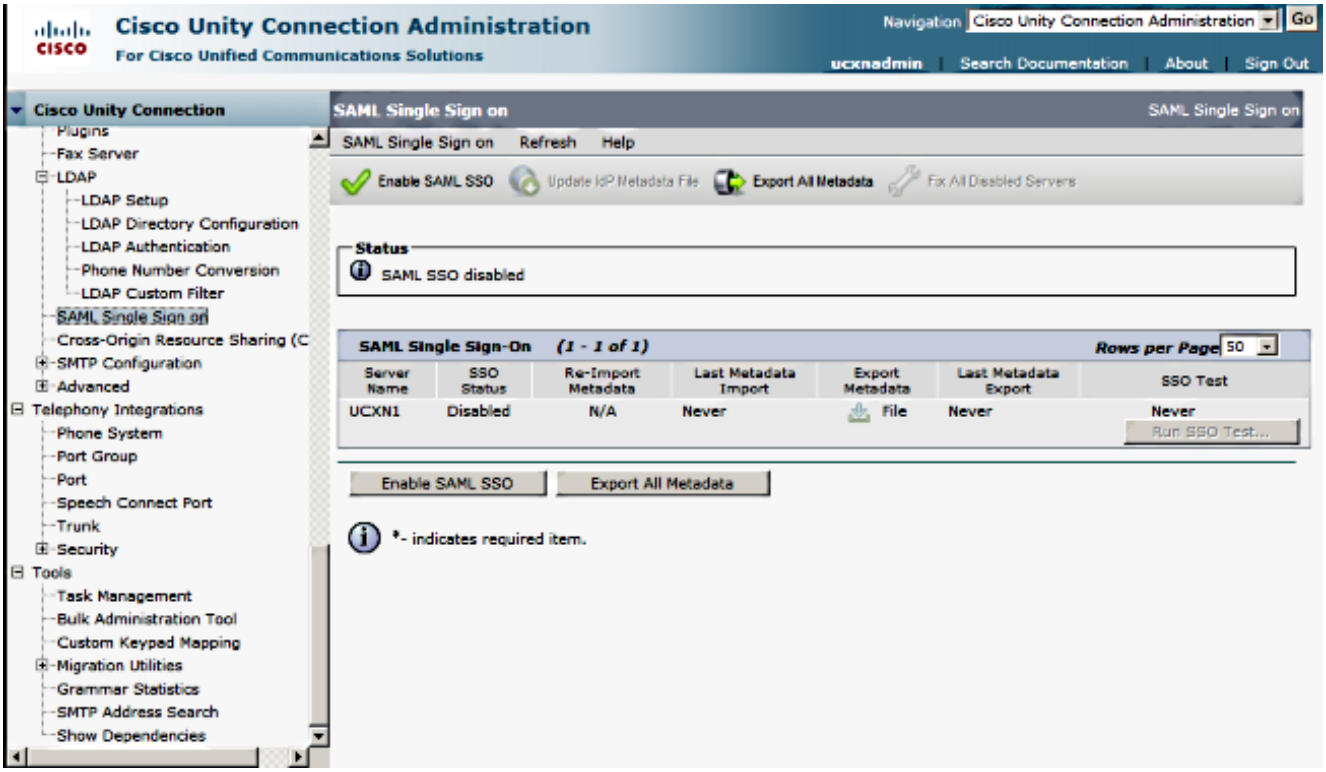
14. Marque as caixas de seleção dos usuários LDAP para os quais deseja criar usuários UCXN e clique em **Importar selecionados**.



Ativar SSO SAML

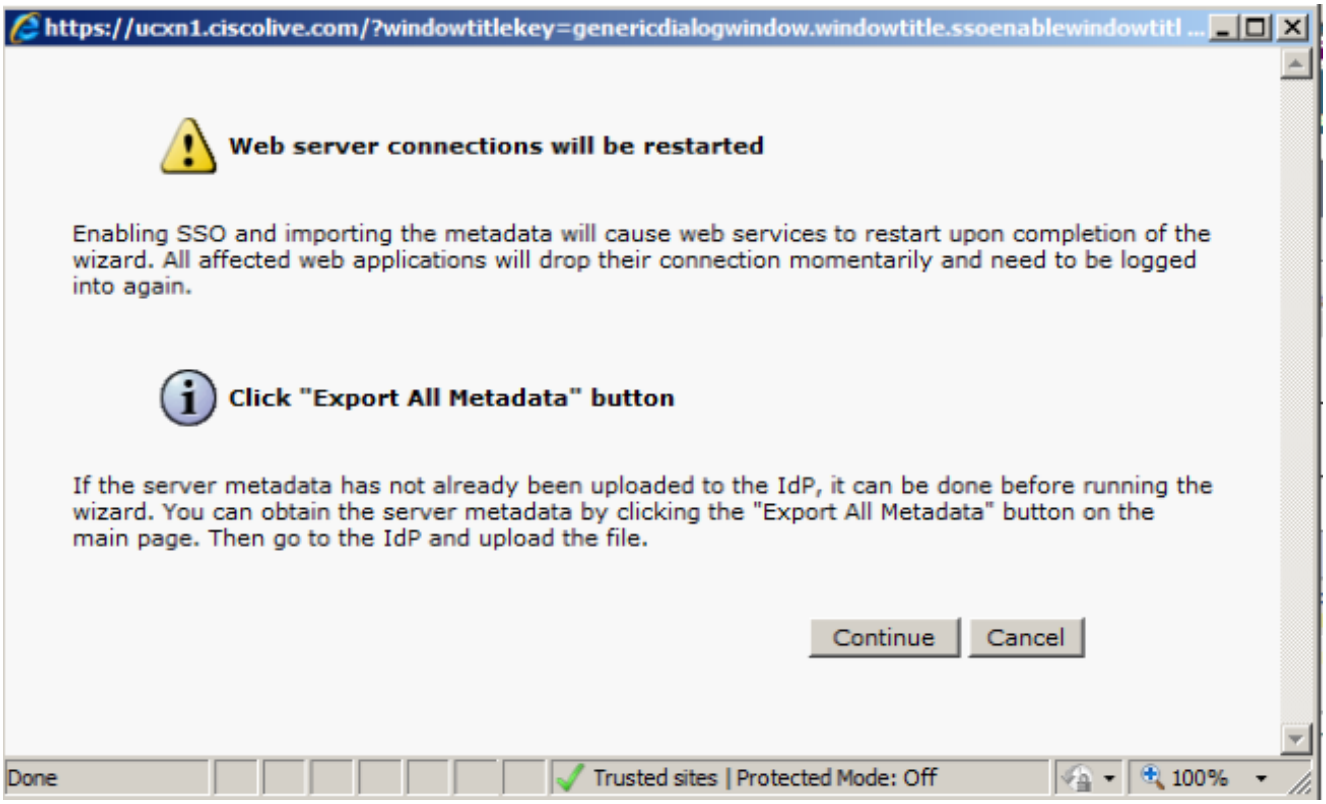
1. Efetue login na interface de usuário do UCXN Administration.

2. Escolha **System > SAML Single Sign-on** e a janela SAML SSO Configuration será aberta.

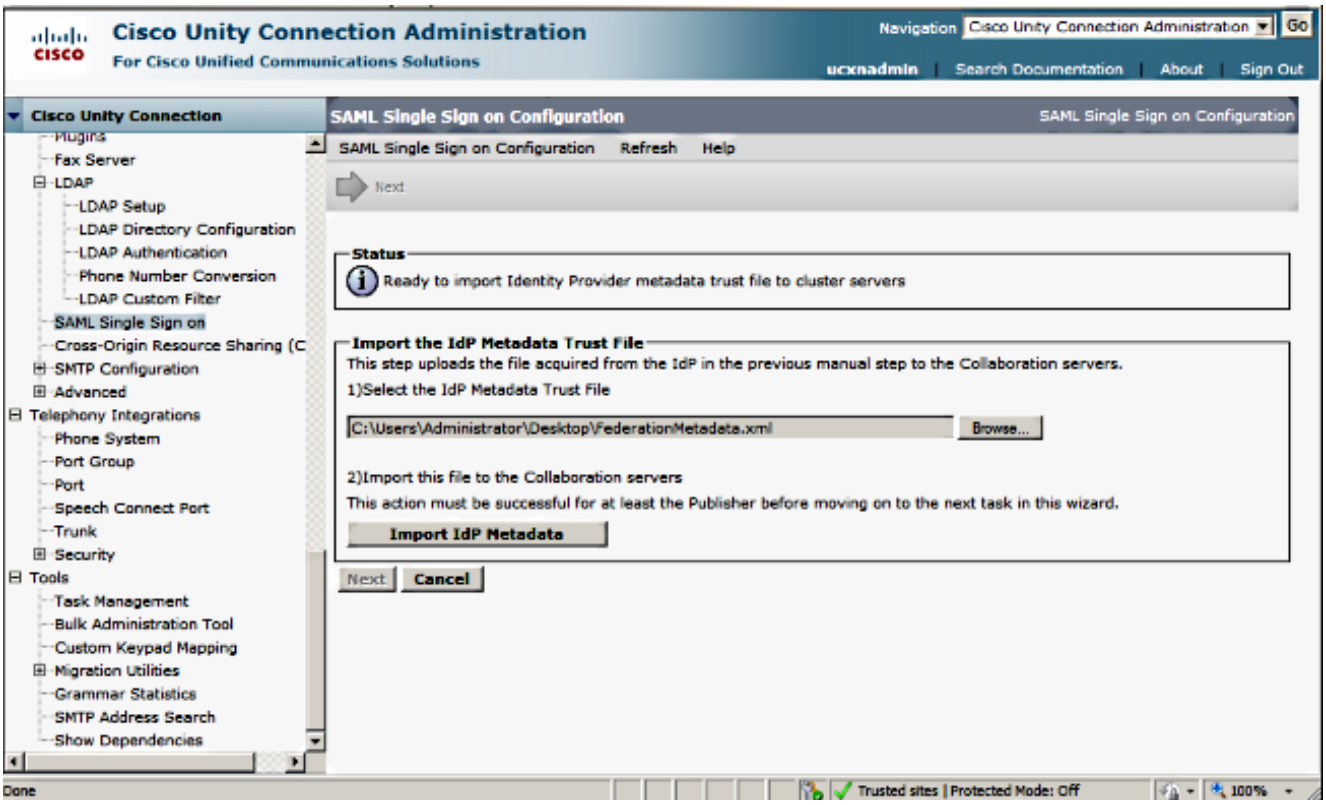


3. Para ativar o SSO SAML no cluster, clique em **Ativar SSO SAML**.

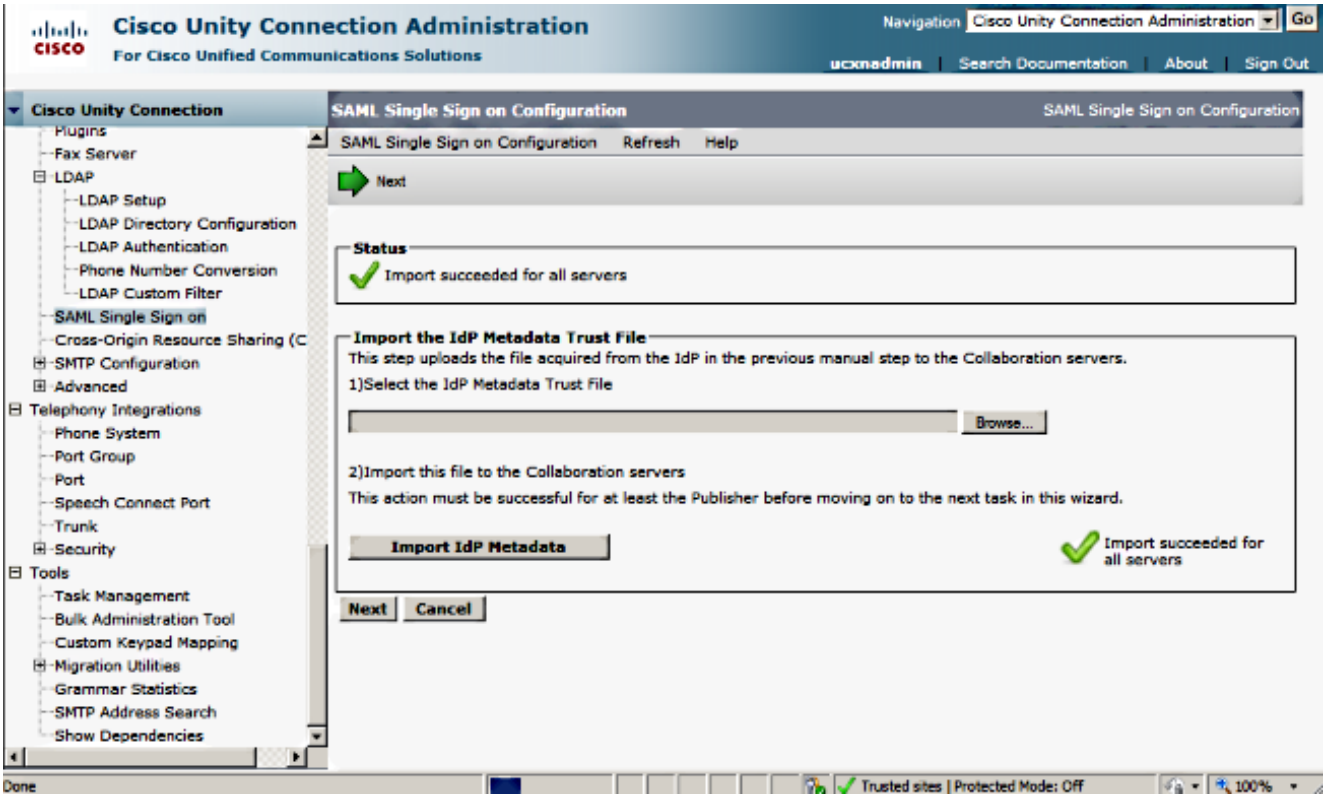
4. Na janela Redefinir aviso, clique em **Continuar.**



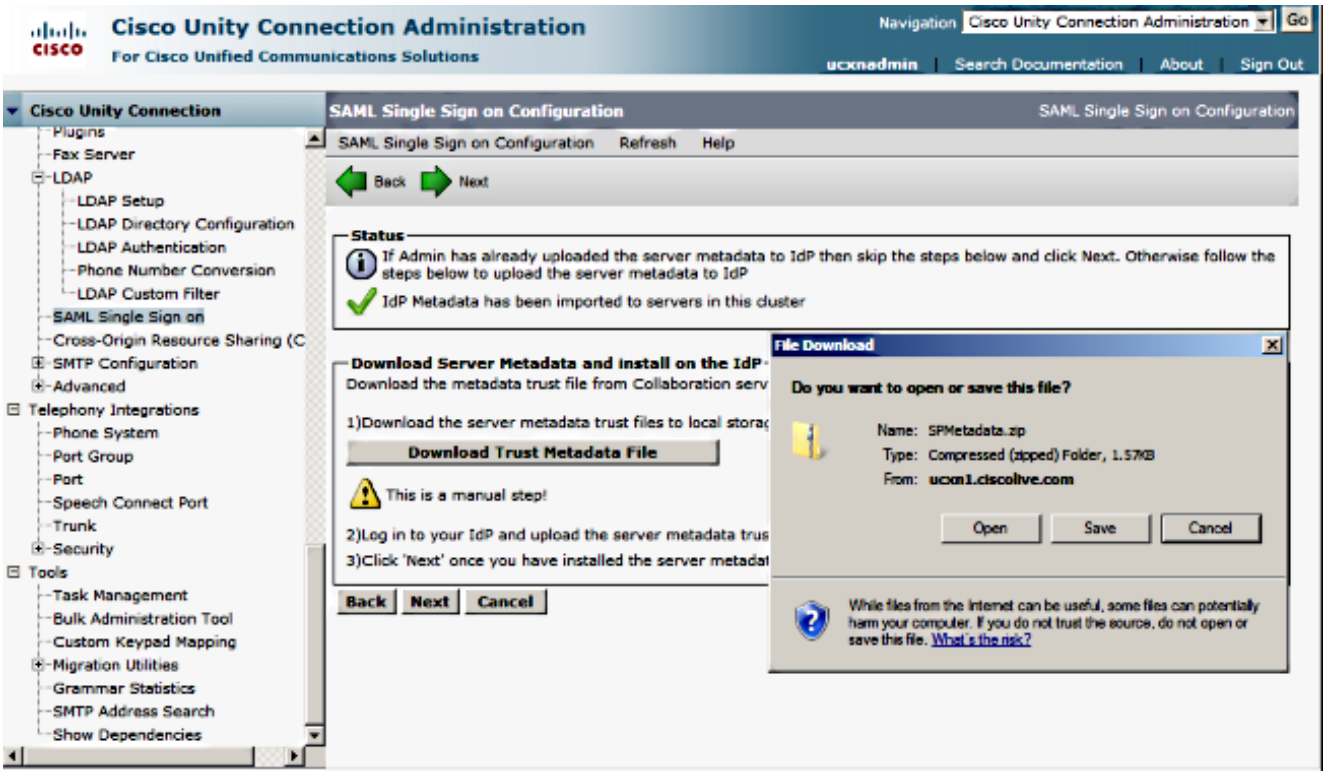
5. Na tela SSO, clique em **Procurar** para importar o arquivo XML de metadados **FederationMetadata.xml** com a etapa **Download Idp Metadata**.



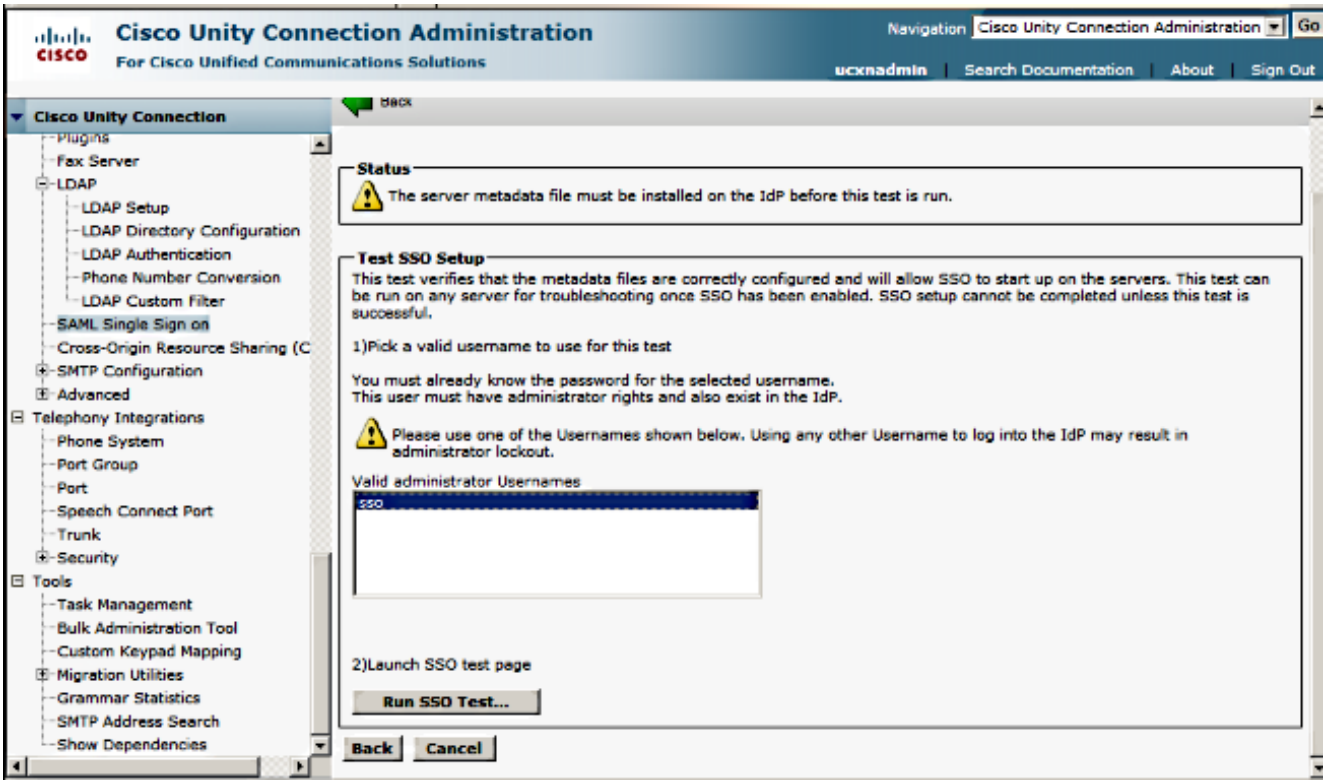
6. Depois que o arquivo de metadados for carregado, clique em **Importar Metadados do IdP** para importar as informações do IdP para o UCXN. Confirme se a importação foi bem-sucedida e clique em **Avançar** para continuar.



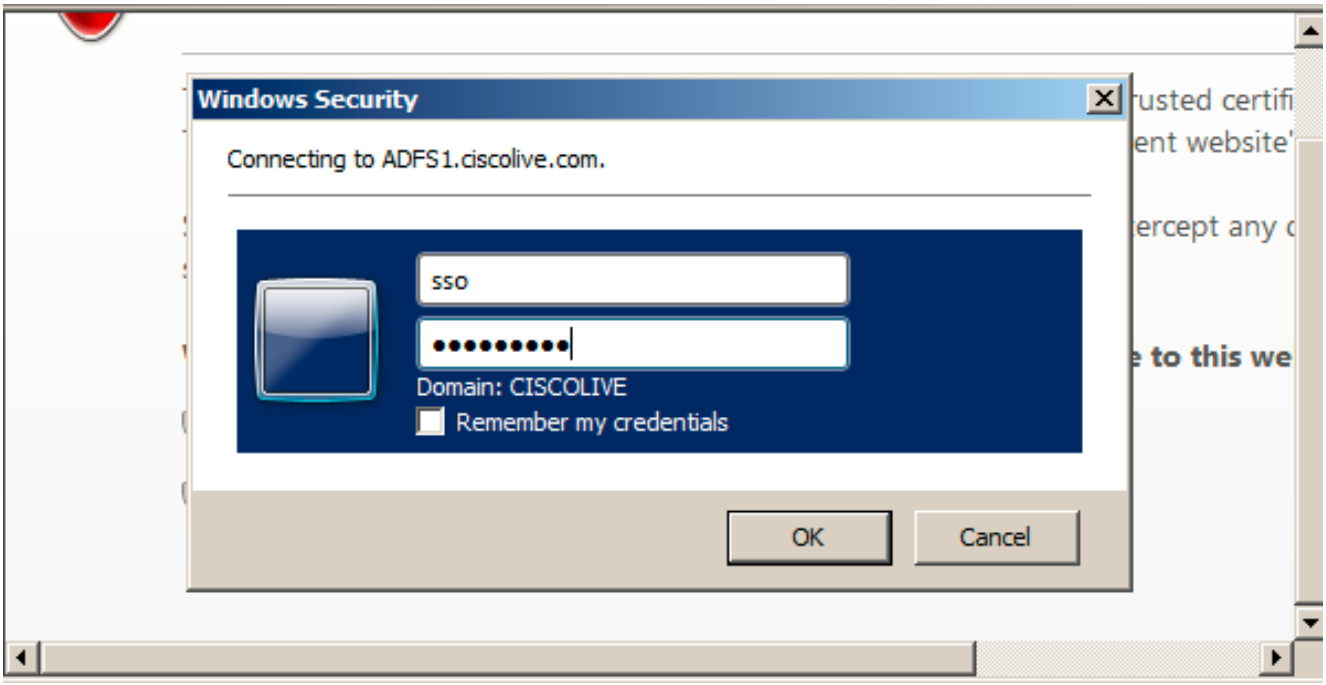
7. Clique em **Download Trust Metadata Fileset** (faça isso somente se você ainda não configurou o ADFS com metadados UCXN) para salvar os metadados UCXN em uma pasta local e vá para Add UCXN as Relay Party Trust. Quando a configuração do AD FS for concluída, vá para a Etapa 8.



8. Selecione **SSO** como o usuário administrativo e clique em **Executar teste SSO**.

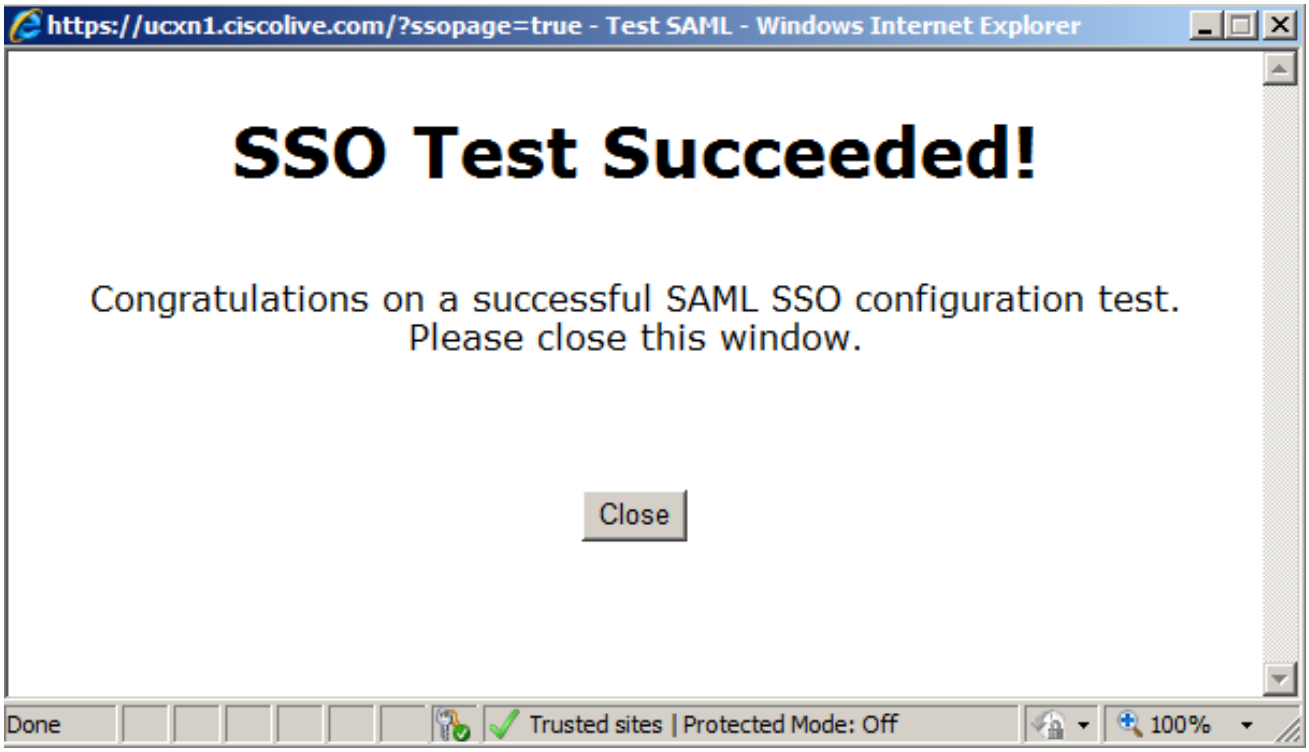


9. Ignore os avisos de certificado e continue. Quando você for solicitado a fornecer credenciais, digite o nome de usuário e a senha do SSO do usuário e clique em **OK**.



Note: Este exemplo de configuração é baseado em certificados autoassinados UCXN e AD FS. Caso você use certificados da autoridade de certificação (CA), os certificados apropriados devem ser instalados no AD FS e no UCXN. Consulte Gerenciamento e Validação de Certificados para obter mais informações.

10. Depois que todas as etapas estiverem concluídas, você receberá o "Teste SSO bem-sucedido!" mensagem. Clique em **Fechar** e **Concluir** para continuar.



Agora você concluiu com êxito as tarefas de configuração para ativar SSO no UCXN com AD FS.

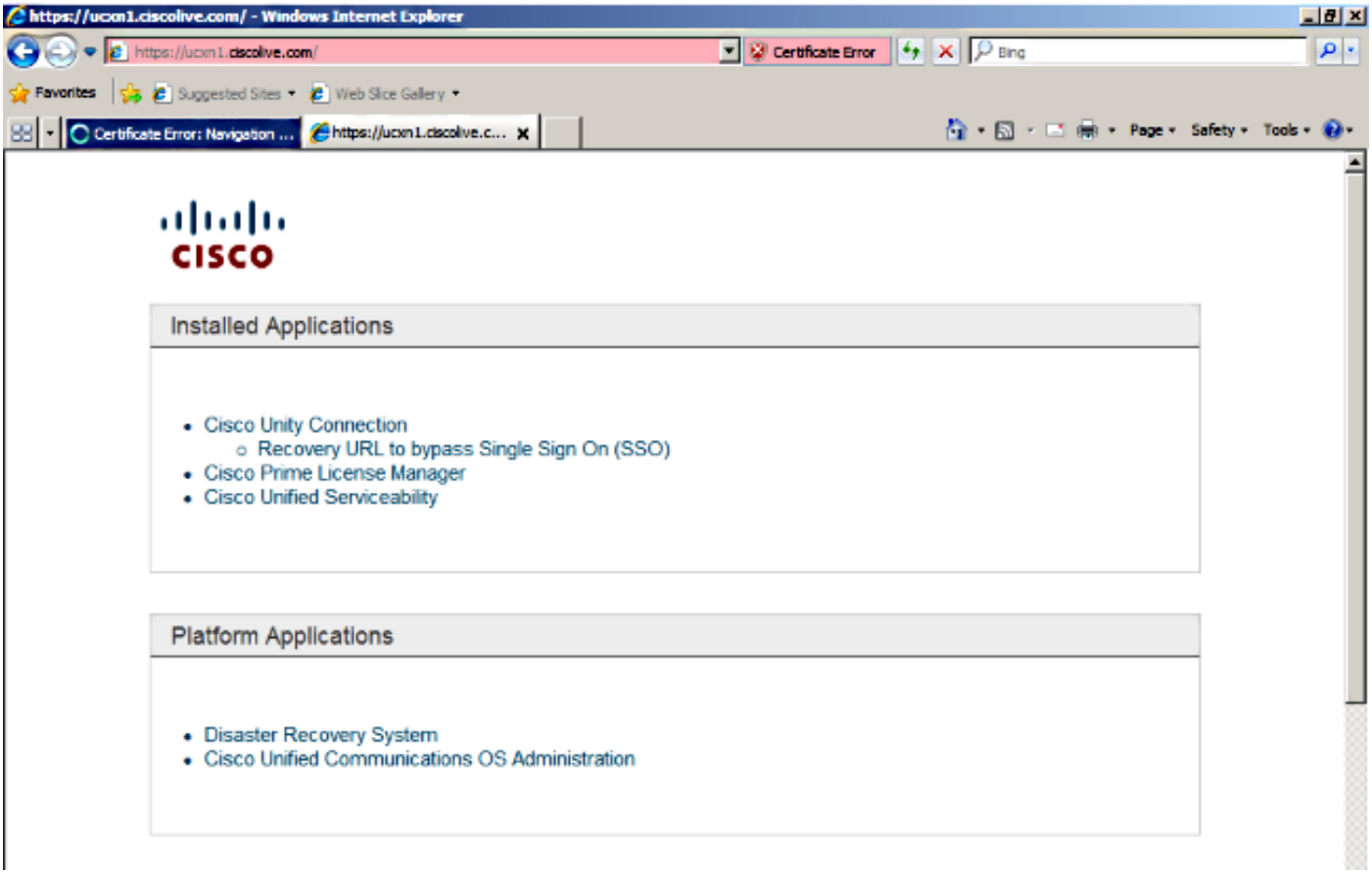
Nota obrigatória: Execute o Teste SSO para assinante UCXN se for um cluster para ativar o SSO SAML. O AD FS deve ser configurado para todos os nós do UCXN em um cluster.

Tip: Se você configurar os arquivos XML de metadados de todos os nós no IdP e começar a ativar a operação SSO em um nó, o SSO SAML será ativado automaticamente em todos os nós no cluster.

Você também pode configurar o CUCM e o CUCM IM e Presence para SAML SSO se quiser usar o SAML SSO para Cisco Jabber Clients e fornecer uma verdadeira experiência SSO aos usuários finais.

Verificar

Abra um navegador da Web e insira o FQDN do UCXN, e você verá uma nova opção em Aplicativos instalados, chamada **URL de recuperação para ignorar o SSO (Single Sign-on, login único)**. Depois de clicar no link **Cisco Unity Connection**, você será solicitado a fornecer credenciais pelo AD FS. Depois de inserir as credenciais do SSO do usuário, você será conectado com êxito na página Unity Administration, página Unified Serviceability.



Note: O SSO SAML não permite o acesso a estas páginas:
- Prime Licensing Manager
- Administração do SO
- Sistema de recuperação de desastres

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Consulte Troubleshooting SAML SSO para Produtos de Colaboração 10.x para obter mais informações.