Esempio di configurazione di Unity Connection versione 10.5 SAML SSO

Sommario

Introduzione

In questo documento viene descritto come configurare e verificare il protocollo SAML (Security Assertion Markup Language) Single Sign-on (SSO) per Cisco Unity Connection (UCXN).

Prerequisiti

Requisiti

Installazione di Network Time Protocol (NTP)

Affinché SAML SSO funzioni correttamente, è necessario installare l'installazione NTP corretta e assicurarsi che la differenza di tempo tra il provider di identità (IdP) e le applicazioni Unified Communications non superi i tre secondi. Per informazioni sulla sincronizzazione degli orologi, vedere la sezione relativa alle impostazioni NTP nel manuale Cisco Unified Communications Operating System Administration Guide.

Installazione di DNS (Domain Name Server)

Le applicazioni Unified Communications possono utilizzare il DNS per risolvere i nomi di dominio completi (FQDN) in indirizzi IP. I provider di servizi e l'IdP devono essere risolvibili dal browser.

Per gestire le richieste SAML, è necessario installare e configurare Active Directory Federation Service (ADFS) versione 2.0.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- AD FS versione 2.0 come IdP
- UCXN come provider di servizi
- Microsoft Internet Explorer versione 10

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

SAML è un formato di dati standard aperto basato su XML per lo scambio di dati. È un protocollo di autenticazione utilizzato dai provider di servizi per autenticare un utente. Le informazioni di autenticazione di protezione vengono passate tra un IdP e il provider di servizi.

SAML è uno standard aperto che consente ai client di eseguire l'autenticazione in base a qualsiasi servizio di collaborazione abilitato per SAML (o Unified Communications) indipendentemente dalla piattaforma client.

Tutte le interfacce Web di Cisco Unified Communications, quali Cisco Unified Communications Manager (CUCM) o UCXN, utilizzano il protocollo SAML versione 2.0 nella funzione SAML SSO. Per autenticare l'utente LDAP (Lightweight Directory Access Protocol), UCXN delega una richiesta di autenticazione all'IdP. Questa richiesta di autenticazione generata da UCXN è una richiesta SAML. IdP autentica e restituisce un'asserzione SAML. L'asserzione SAML visualizza Sì (autenticato) o No (autenticazione non riuscita).

SAML SSO consente a un utente LDAP di accedere alle applicazioni client con un nome utente e una password che vengono autenticati nel provider di identità. L'utente che accede a una delle applicazioni Web supportate nei prodotti Unified Communications, dopo aver abilitato la funzione SAML SSO, ottiene anche l'accesso a queste applicazioni Web in UCXN (a parte CUCM e CUCM IM e Presence):

Utenti Unity Connection	Applicazioni Web
Utenti LDAP con diritti di amministratore	• Amministrazione UCXN • Manutenzione di Cisco UCXN • Manutenzione unificata di Cisco • Cisco Personal Communications Assistant • Posta in arrivo Web • Posta in arrivo Web minima (versione desktop)
Utenti LDAP senza diritti di amministratore	• Cisco Personal Communications Assistant • Posta in arrivo Web • Posta in arrivo Web minima (versione desktop) • Client Cisco Jabber

Configurazione

Esempio di rete

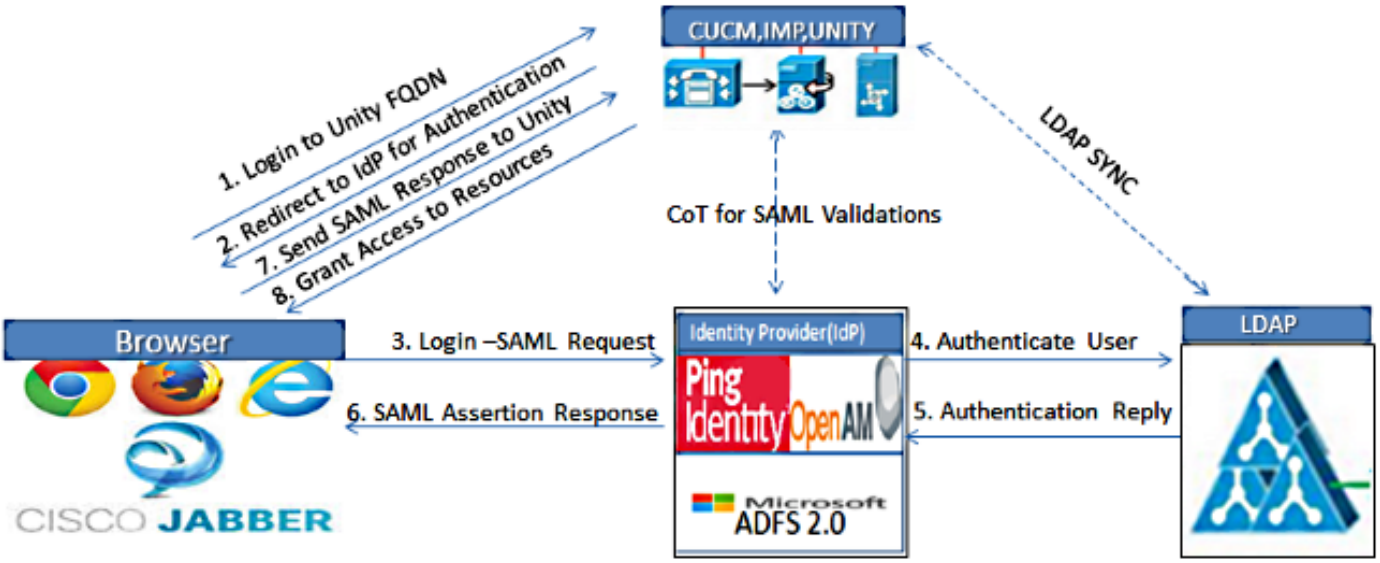
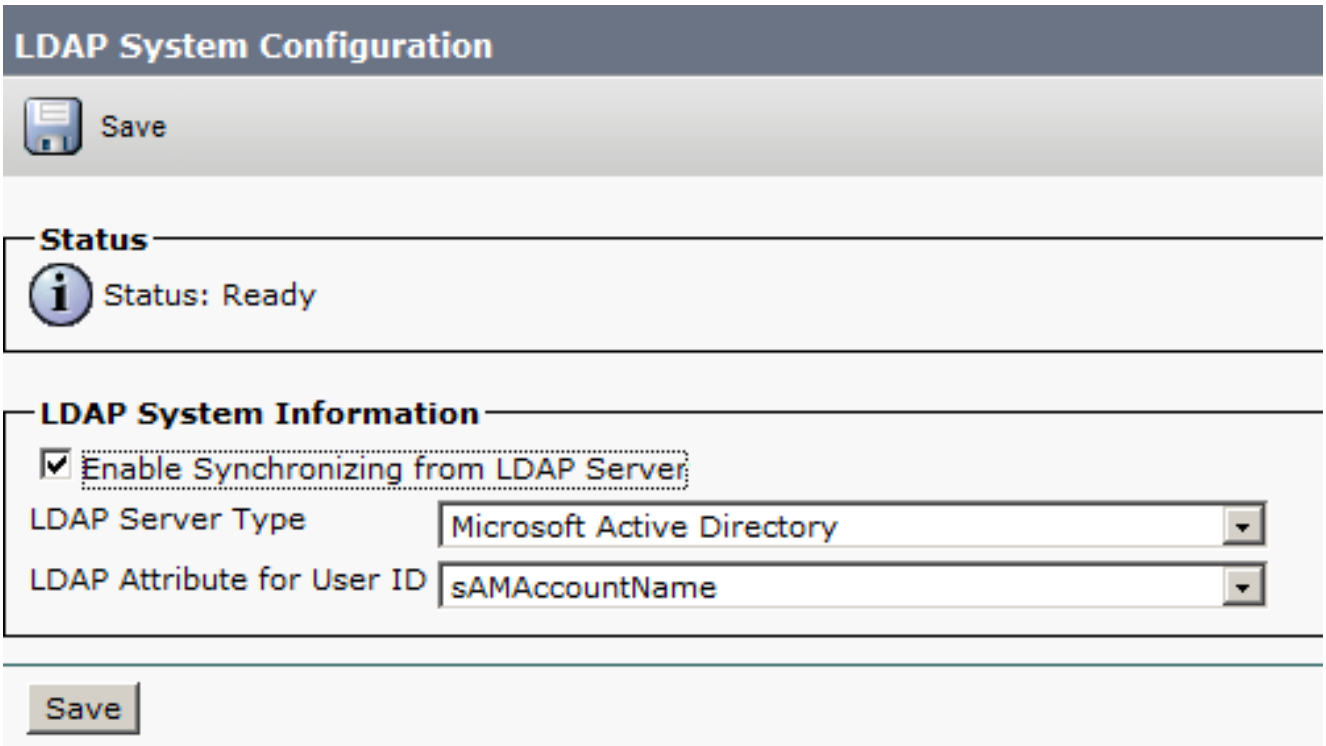


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

Impostazione directory

1. Accedere alla pagina Amministrazione UCXN e selezionare **LDAP**, quindi fare clic su **Configurazione LDAP**.

2. Selezionare **Abilita sincronizzazione dal server LDAP** e fare clic su **Salva**.



3. Fare clic su **LDAP**.

4. Fare clic su **Configurazione directory LDAP**.

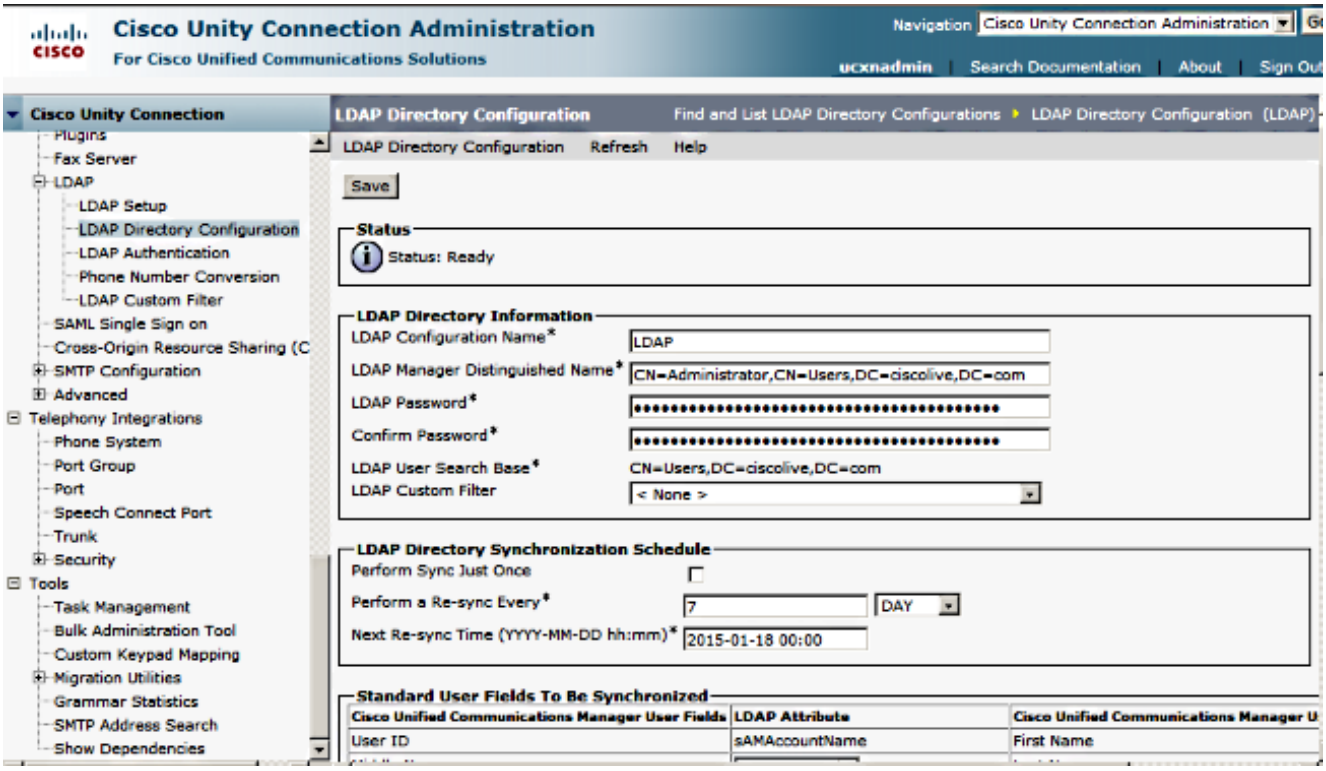
5. Fare clic su **Aggiungi nuovo**.

6. Configurare gli elementi seguenti:

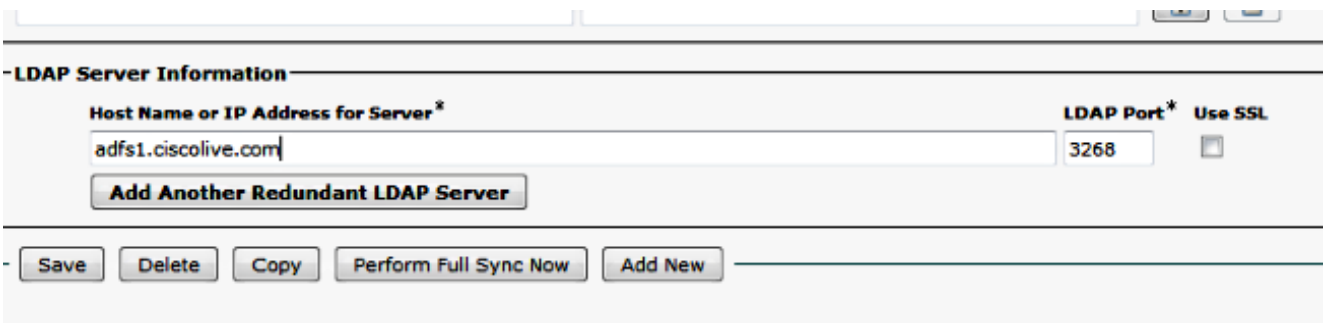
   Impostazioni account directory LDAPAttributi utente da sincronizzarePianificazione sincronizzazioneNome host o indirizzo IP del server LDAP e numero di porta

7. Selezionare **Usa SSL** se si desidera utilizzare SSL (Secure Sockets Layer) per comunicare con la directory LDAP.

   Suggerimento: Se si configura LDAP su SSL, caricare il certificato della directory LDAP in CUCM. Fare riferimento al contenuto della directory LDAP in Cisco Unified Communications Manager SRND per informazioni sul meccanismo di sincronizzazione degli account per prodotti LDAP specifici e per le best practice generali per la sincronizzazione LDAP.



8. Fare clic su **Esegui sincronizzazione completa**.



Nota: Prima di fare clic su Salva, verificare che il servizio **Cisco DirSync** sia abilitato nella pagina Web Serviceability.

9. Espandere **Utenti** e selezionare **Importa utenti**.

10. Nell'elenco **Trova utenti finali di Unified Communications Manager** selezionare **LDAP Directory**.

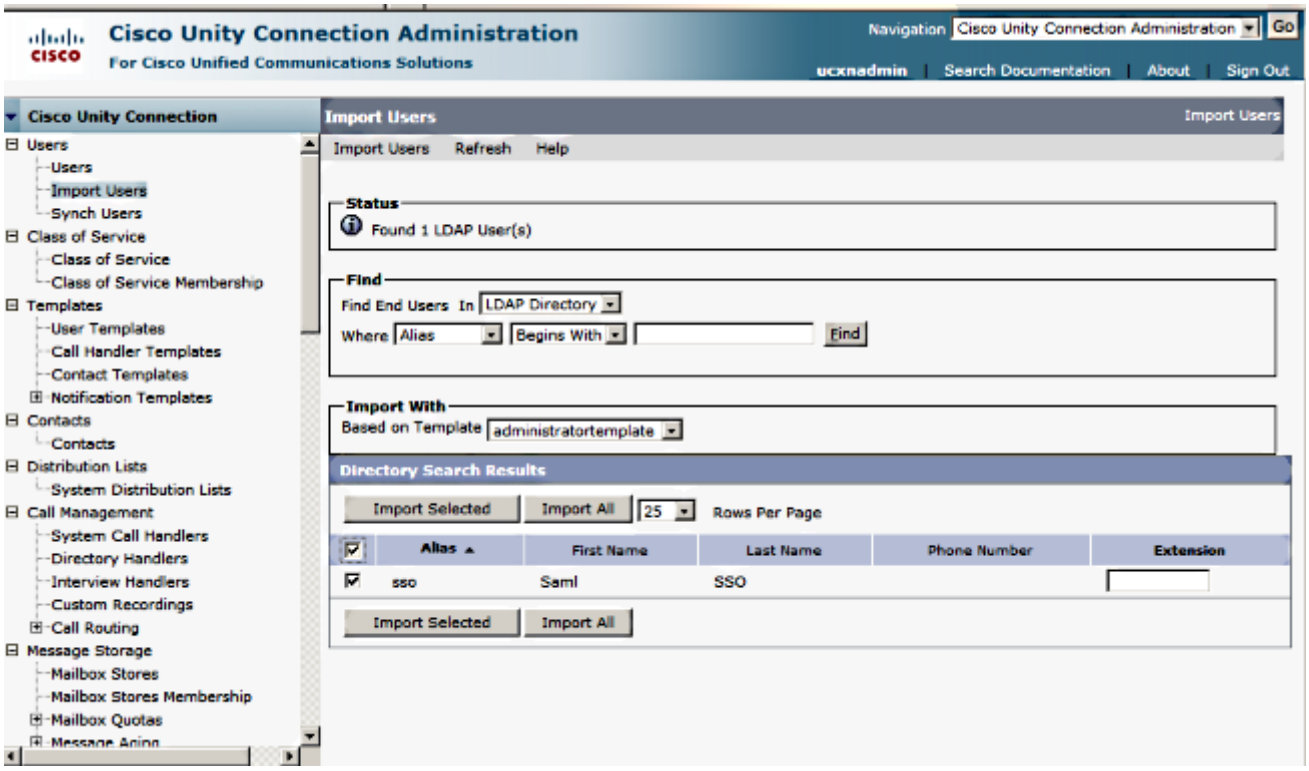
11. Se si desidera importare solo un sottoinsieme degli utenti nella directory LDAP con cui è stato integrato UCXN, immettere le specifiche applicabili nei campi di ricerca.

12. Selezionare **Trova**.

13. Nell'elenco In base a modello selezionare il **modello dell'amministratore** che si desidera utilizzare per la creazione degli utenti selezionati in UCXN.

    Attenzione: Se si specifica un modello per l'amministratore, gli utenti non disporranno di cassette postali.

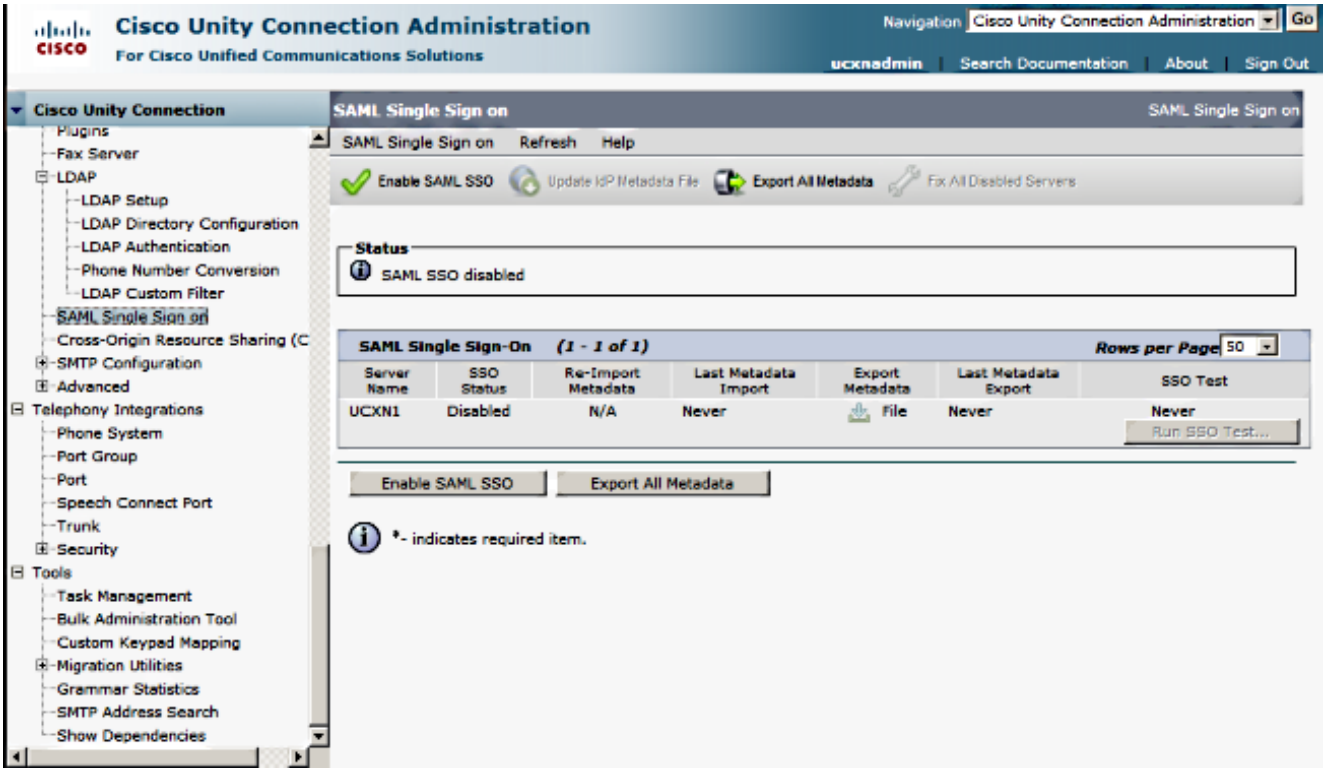
14. Selezionare le caselle di controllo relative agli utenti LDAP per i quali si desidera creare utenti UCXN e fare clic su **Importa selezionati**.



Abilita SAML SSO

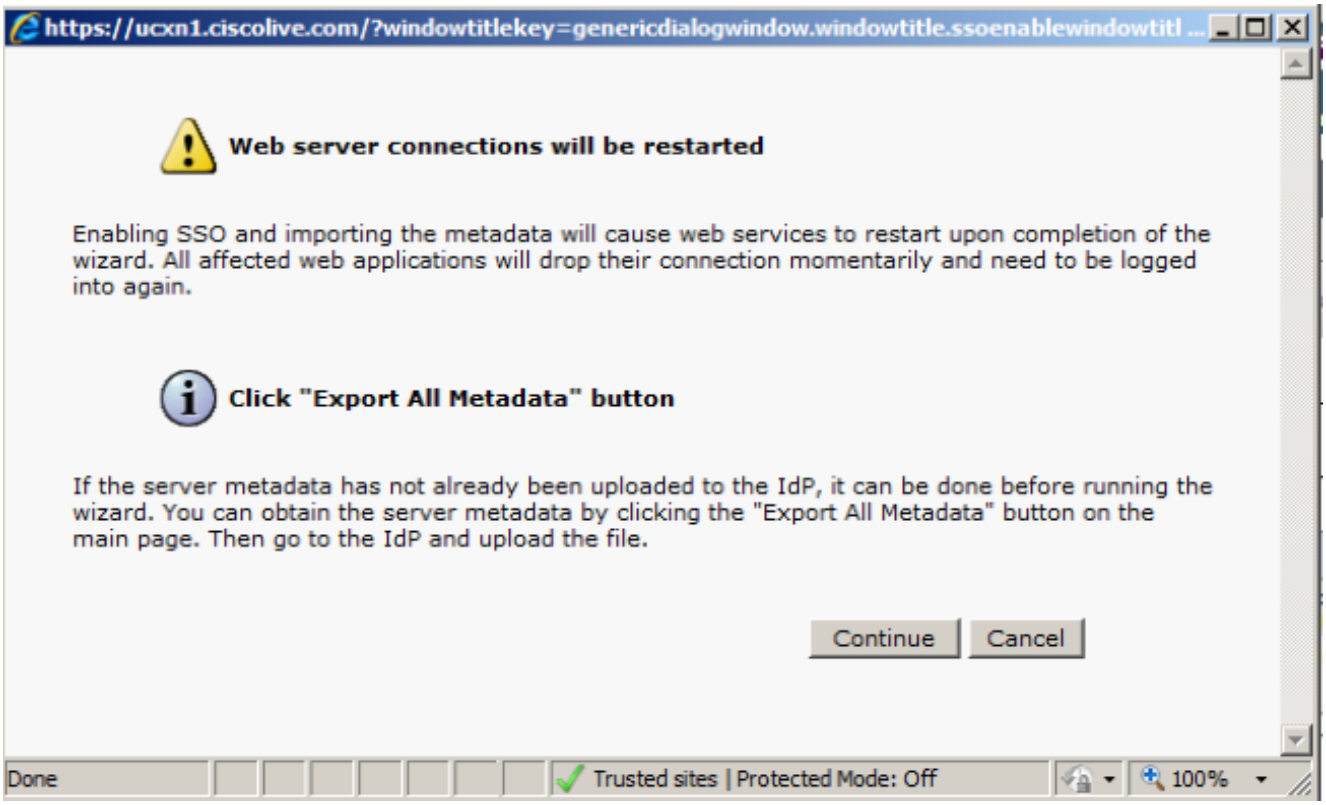
1. Accedere all'interfaccia utente di amministrazione UCXN.

2. Scegliere **Sistema > SAML Single Sign-on** e viene visualizzata la finestra Configurazione SAML SSO.

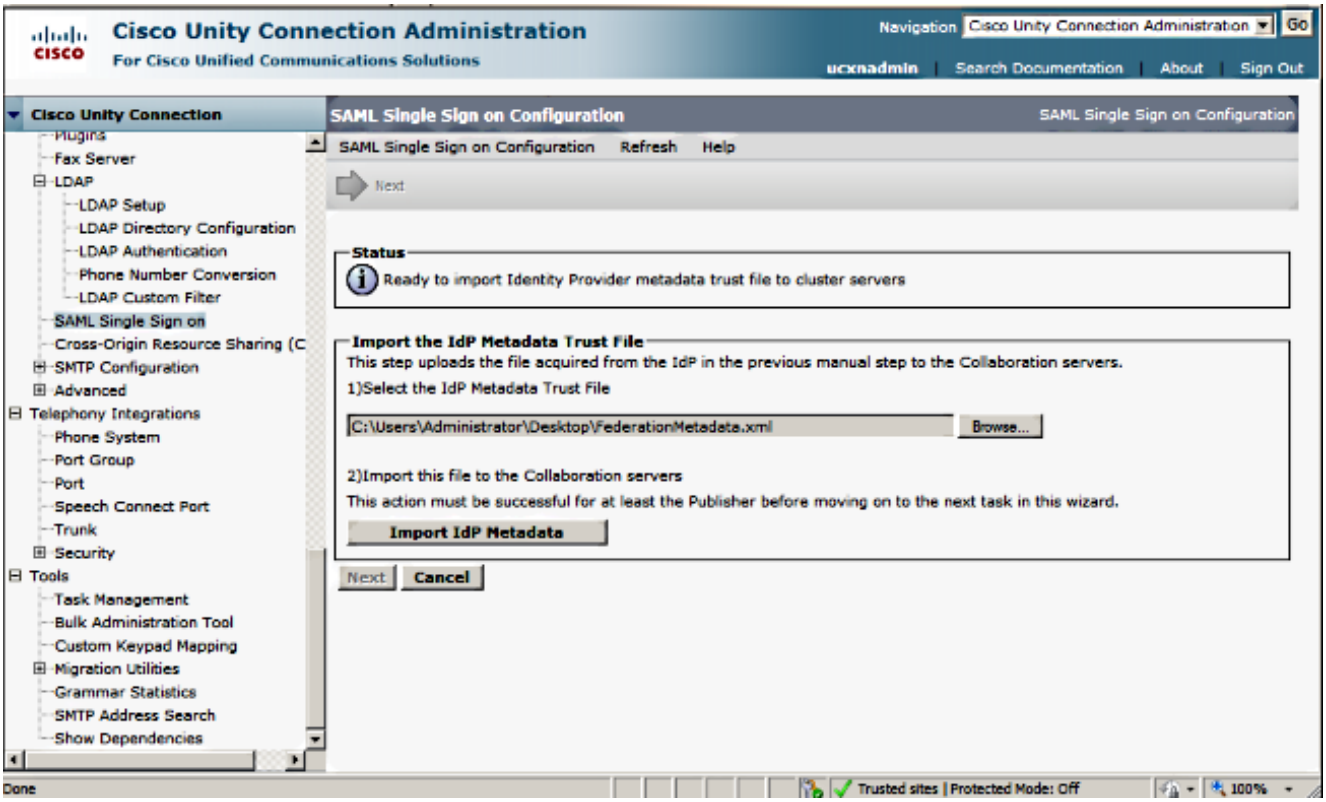


3. Per abilitare l'SSO SAML nel cluster, fare clic su **Abilita SSO SAML**.

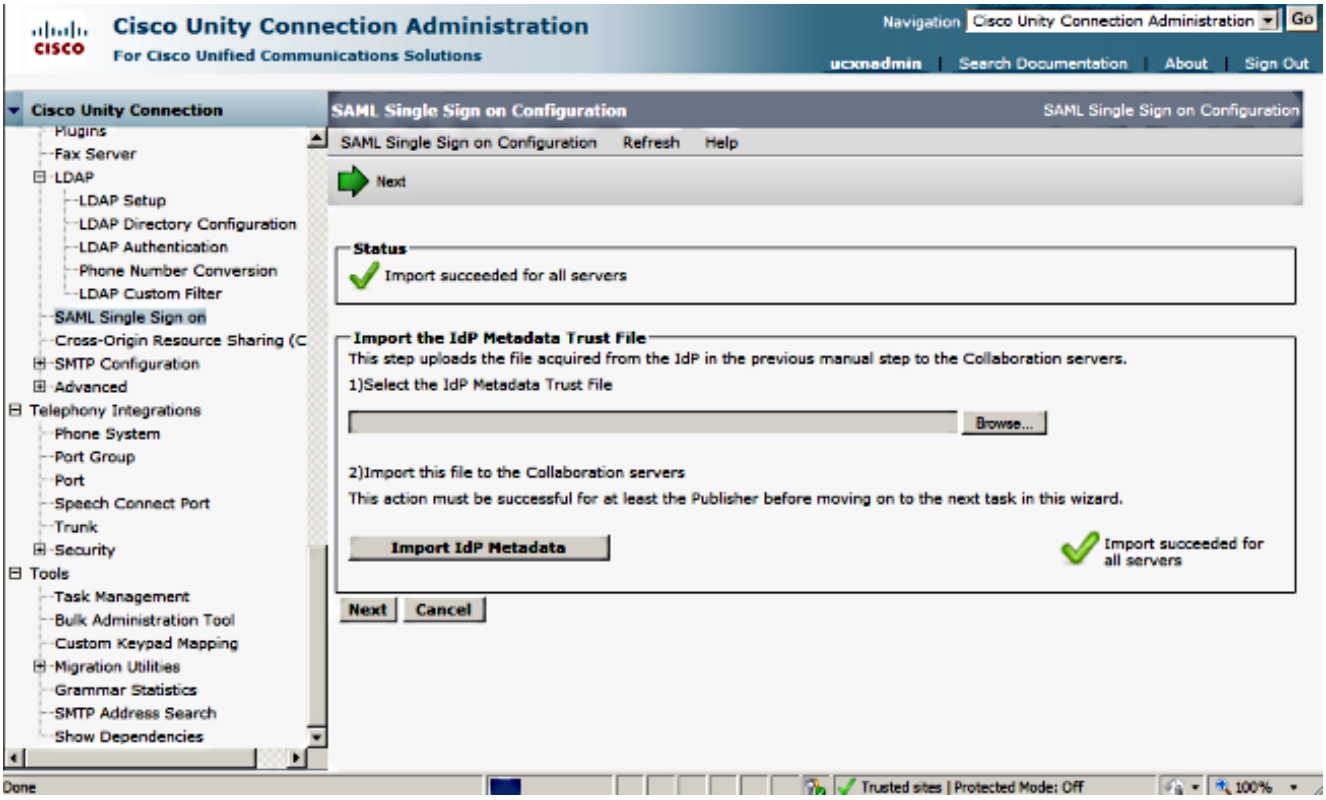
4. Nella finestra Reimposta avviso fare clic su **Continua.**



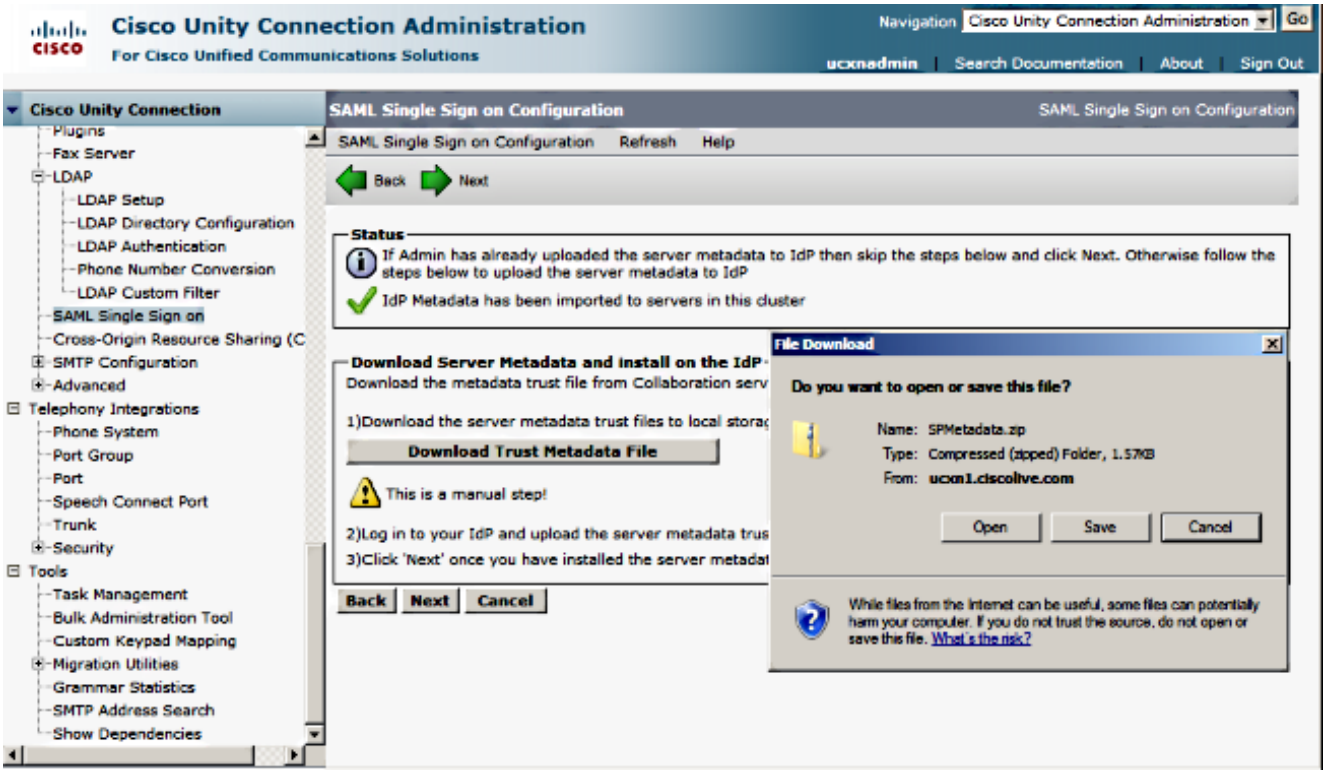
5. Nella schermata SSO fare clic su **Sfoglia** per importare il file XML dei metadati **FederationMetadata.xml** con il passaggio **Download metadati IP**.



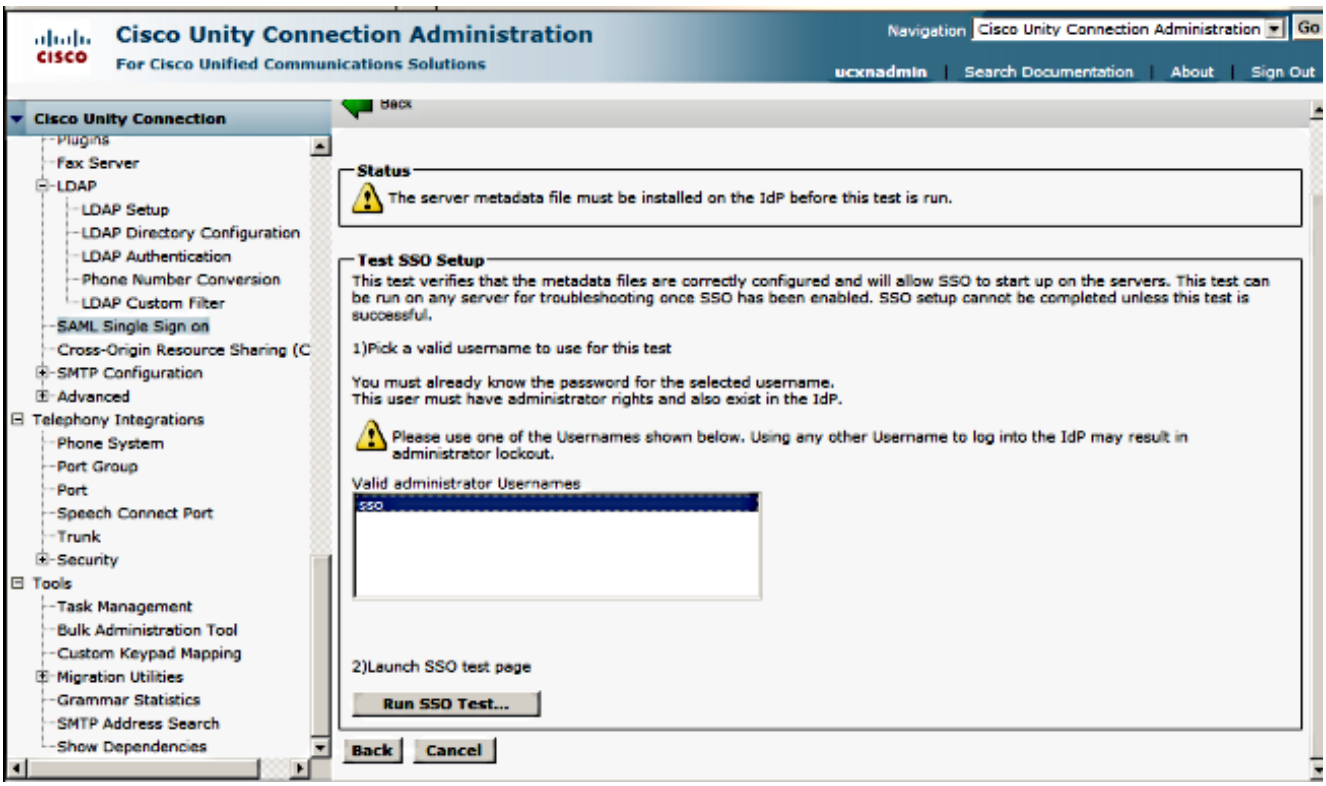
6. Una volta caricato il file di metadati, fare clic su **Import IdP Metadata** per importare le informazioni IdP in UCXN. Confermare che l'importazione è stata completata e fare clic su **Avanti** per continuare.



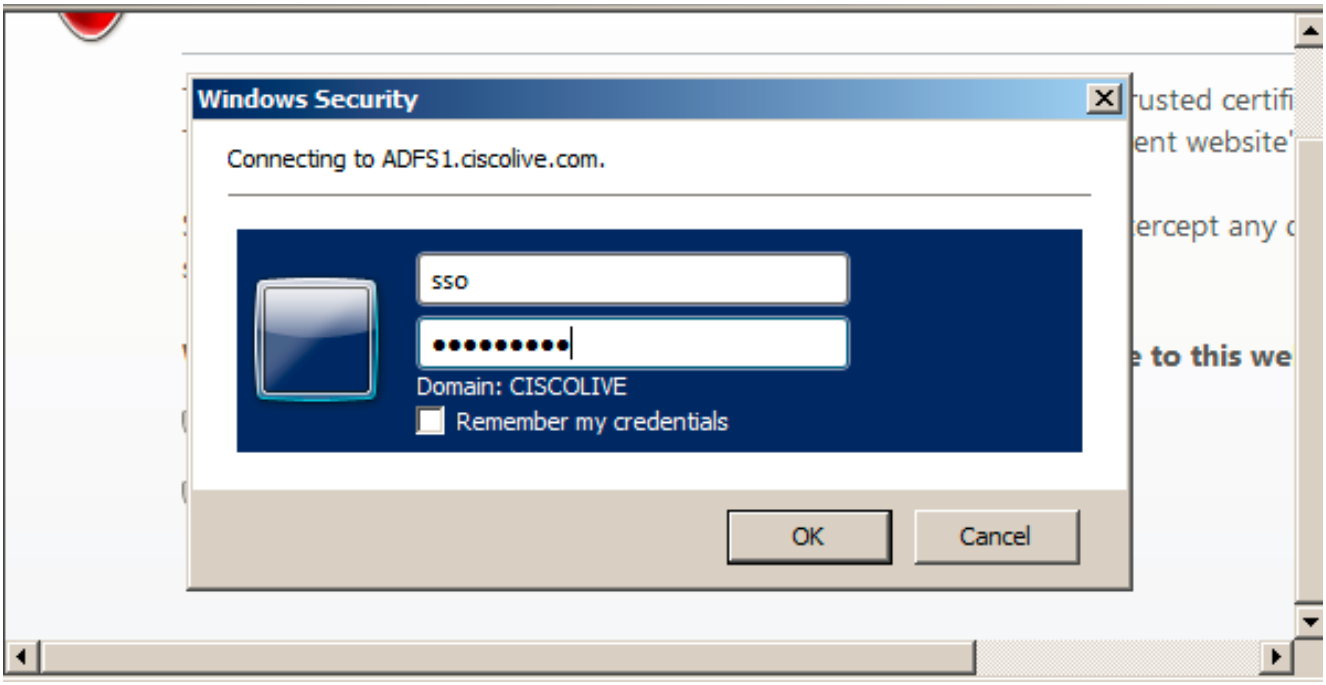
7. Fare clic su **Scarica set di file di metadati di attendibilità** (eseguire questa operazione solo se ADFS non è già stato configurato con i metadati UCXN) per salvare i metadati UCXN in una cartella locale e passare a Aggiungi UCXN come attendibilità parte di inoltro. Al termine della configurazione di AD FS, andare al passaggio 8.



8. Selezionare **SSO** come utente amministrativo e fare clic su **Esegui test SSO**.

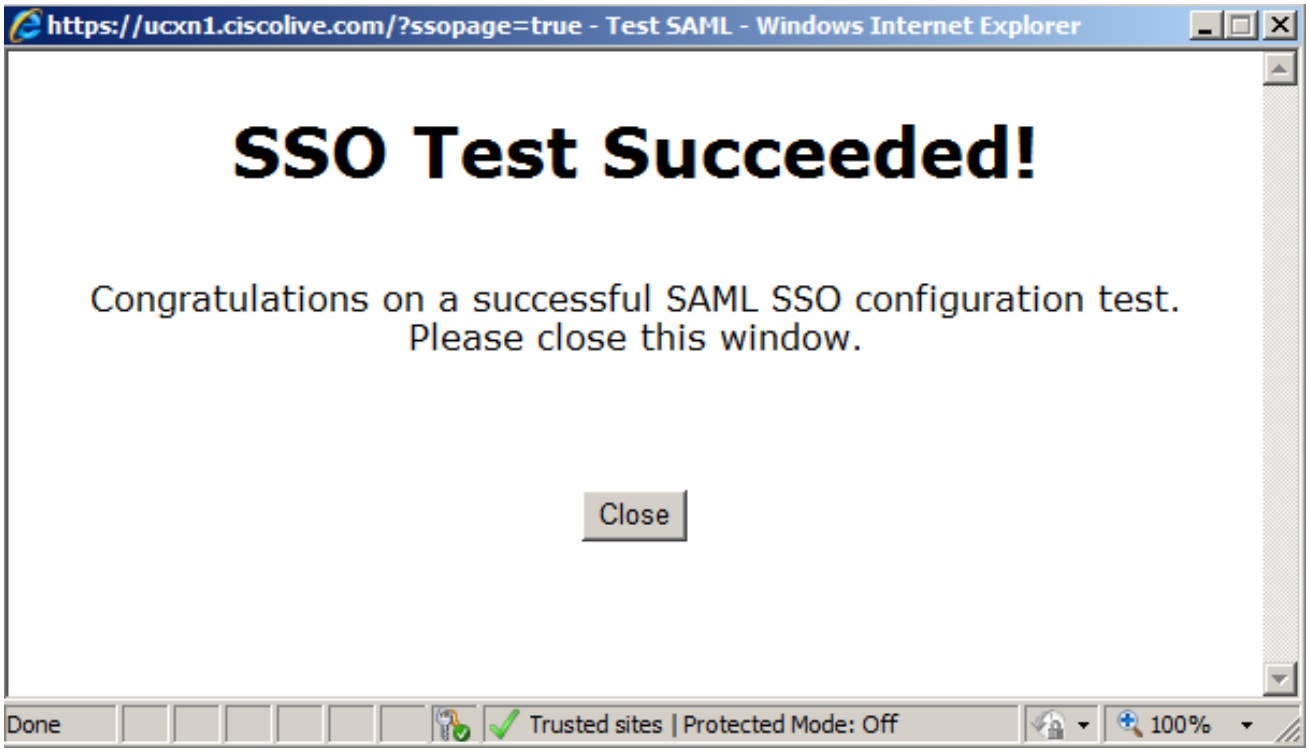


9. Ignora avvisi certificato e continua. Quando vengono richieste le credenziali, immettere il nome utente e la password di SSO utente e fare clic su **OK**.



Nota: Questo esempio di configurazione è basato sui certificati autofirmati UCXN e AD FS. Se si utilizzano certificati dell'Autorità di certificazione (CA), è necessario installare i certificati appropriati sia in ADFS che in UCXN. Per ulteriori informazioni, fare riferimento a Gestione e convalida certificati.

10. Al termine di tutti i passaggi, si riceve il messaggio "Test SSO riuscito!" messaggio. Per continuare, fare clic su **Close** (Chiudi) e **Finish** (Fine).



Le attività di configurazione per l'abilitazione dell'SSO su UCXN con AD FS sono state completate.

Nota obbligatoria: Eseguire il test SSO per il sottoscrittore UCXN se si tratta di un cluster

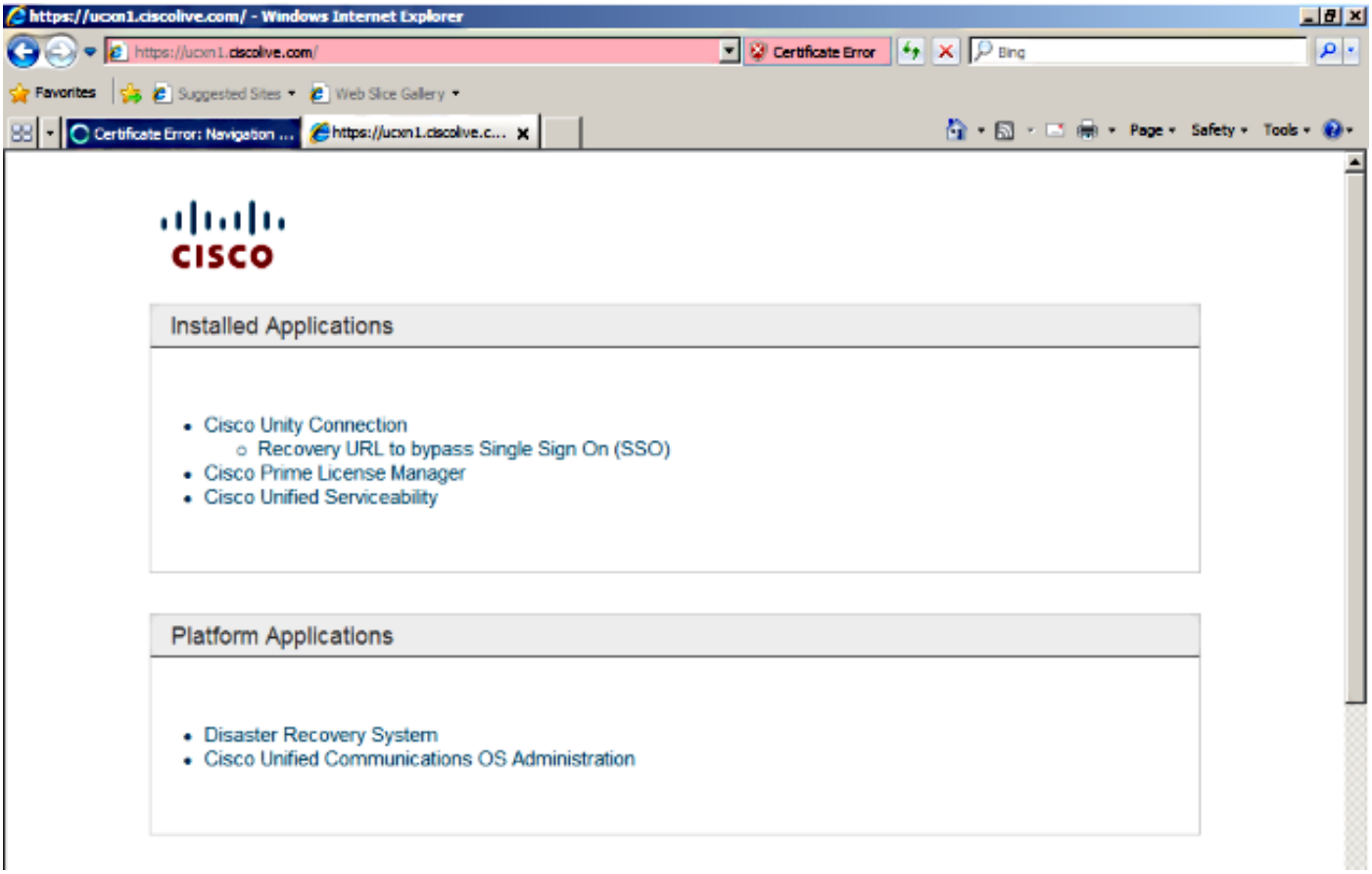
per abilitare l'SSO SAML. AD FS deve essere configurato per tutti i nodi di UCXN in un cluster.

Suggerimento: Se si configurano i file XML dei metadati di tutti i nodi in IdP e si avvia l'abilitazione dell'operazione SSO su un nodo, l'SSO SAML verrà automaticamente abilitato su tutti i nodi del cluster.

È inoltre possibile configurare CUCM e CUCM IM e Presence per SAML SSO se si desidera utilizzare SAML SSO per i client Cisco Jabber e offrire agli utenti finali un'esperienza di SSO reale.

Verifica

Aprire un browser Web e immettere il nome di dominio completo (FQDN) di UCXN. In Applicazioni installate verrà visualizzata una nuova opzione denominata **URL di ripristino per ignorare Single Sign-On (SSO)**. Dopo aver fatto clic sul collegamento **Cisco Unity Connection**, all'utente vengono richieste le credenziali da ADFS. Dopo aver immesso le credenziali dell'utente SSO, verrà eseguito correttamente l'accesso alla pagina Unity Administration, Unified Serviceability.



Nota: SAML SSO non consente l'accesso a queste pagine:
- Prime Licensing Manager
- Amministrazione del sistema operativo
- Sistema di disaster recovery

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Per ulteriori informazioni, fare riferimento a Risoluzione dei problemi di SSO SAML per i prodotti Collaboration 10.x.