Esempio di configurazione di Unified Communications Manager 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 Unified Communications Manager (CUCM).

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.

In caso di mancata corrispondenza tra CUCM e IdP, viene visualizzato il seguente messaggio di errore: "Risposta SAML non valida." Questo errore potrebbe essere causato da un tempo di sincronizzazione non corretto tra i server CUCM e IdP. Affinché SAML SSO funzioni, è necessario installare la corretta configurazione NTP e assicurarsi che la differenza di tempo tra l'IdP e le applicazioni Unified Communications non superi i tre secondi.

Per informazioni su come sincronizzare gli 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.

Componenti usati

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

- Active Directory Federation Service (ADFS) versione 2.0 come IdP
- CUCM versione 10.5 come provider di servizi
- Microsoft Internet Explorer 10

> **Attenzione:** Questo documento si basa su un CUCM appena installato. Se si configura SAML SSO su un server già in produzione, potrebbe essere necessario ignorare alcuni passaggi. È inoltre necessario comprendere l'impatto del servizio se si eseguono le operazioni sul server di produzione. Si consiglia di eseguire questa procedura al di fuori dell'orario di lavoro.

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 basato su XML e basato su standard aperti che consente agli amministratori di accedere senza problemi a un insieme definito di applicazioni di collaborazione Cisco dopo aver eseguito l'accesso a una di tali applicazioni. L'SSO SAML stabilisce un Circle of Trust (CoT) quando scambia metadati come parte del processo di provisioning tra l'IdP e il provider di servizi. Il provider di servizi considera attendibili le informazioni utente dell'IdP per consentire l'accesso ai vari servizi o applicazioni.

> **Nota:** I provider di servizi non sono più coinvolti nell'autenticazione. SAML versione 2.0 delega l'autenticazione ai provider di servizi e agli IdP. Il client esegue l'autenticazione in base all'IdP e l'IdP concede un'asserzione al client. Il client presenta l'asserzione al provider di servizi. Poiché è stato stabilito un CoT, il provider di servizi considera attendibile l'asserzione e concede l'accesso al client.

Configurazione

Esempio di rete

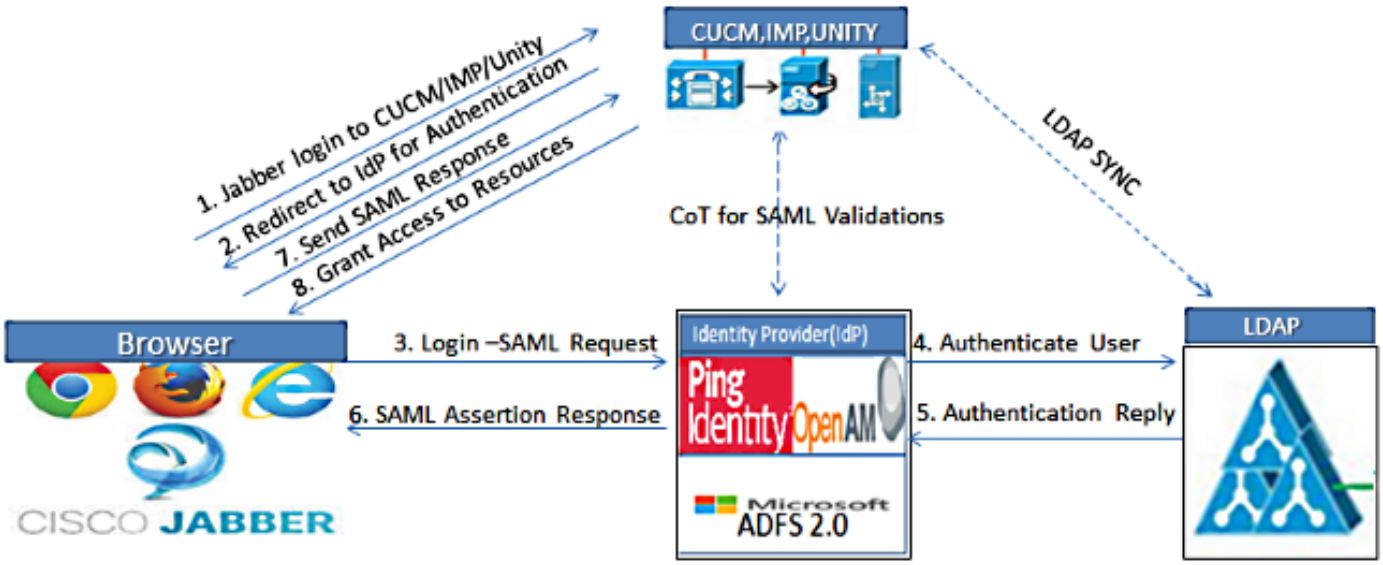
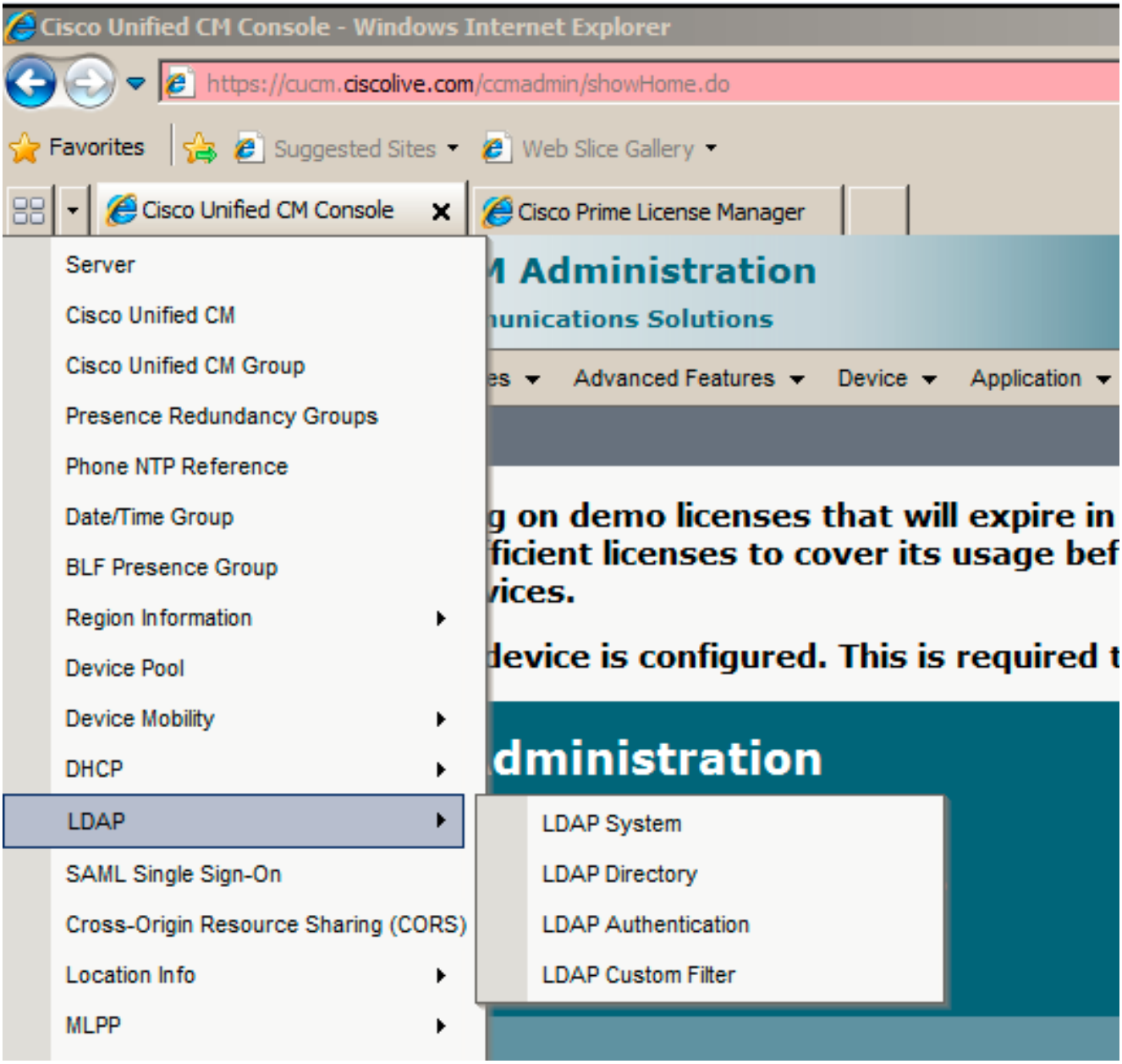


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

Impostazione directory

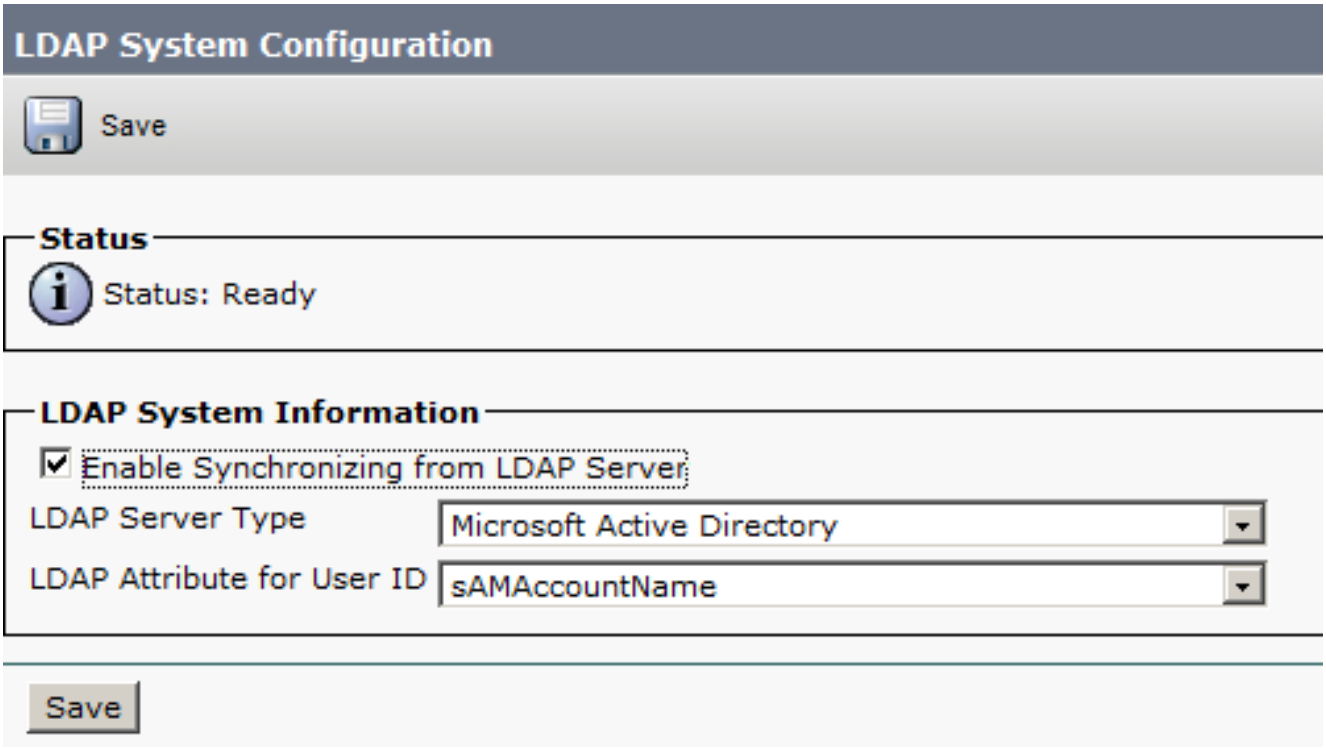
1. Scegliere **Cisco Unified CM Administration > System > LDAP > LDAP System.**



2. Fare clic su **Aggiungi nuovo**.

3. Configurare il tipo e l'attributo del server Lightweight Directory Access Protocol (LDAP).

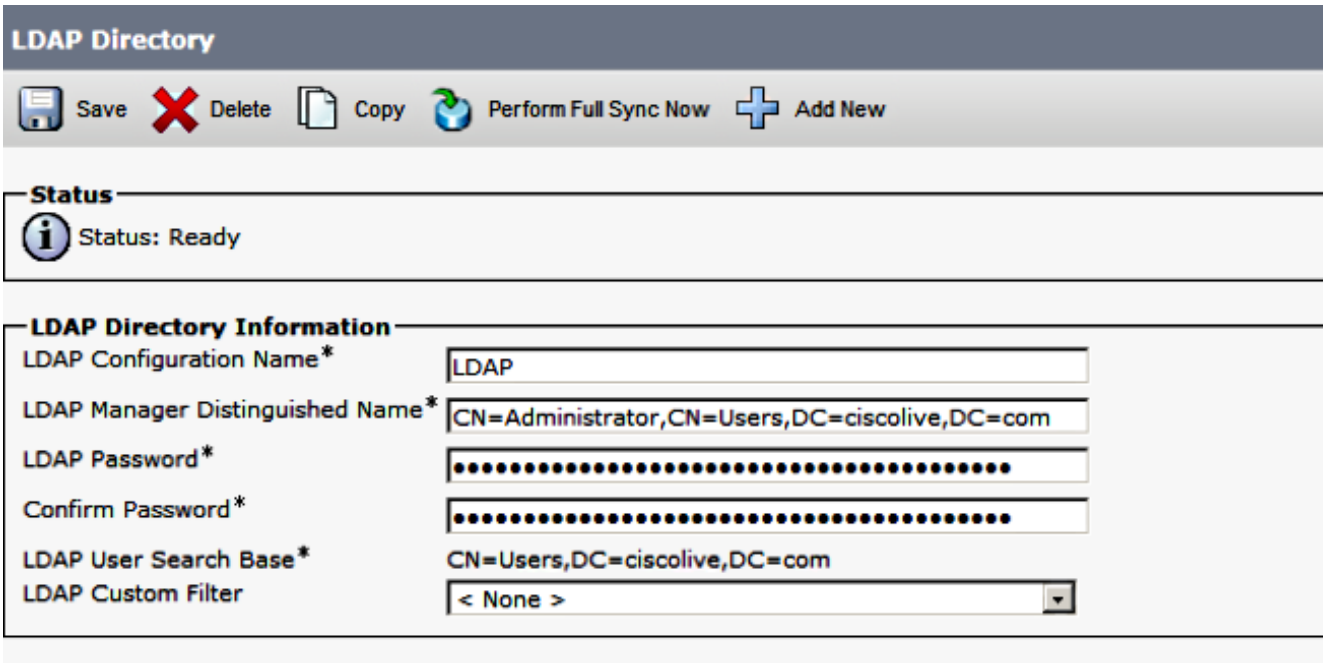
4. Scegliere **Abilita sincronizzazione dal server LDAP**.



5. Scegliere **Cisco Unified CM Administration > System > LDAP > LDAP Directory**.

6. Configurare gli elementi seguenti:

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



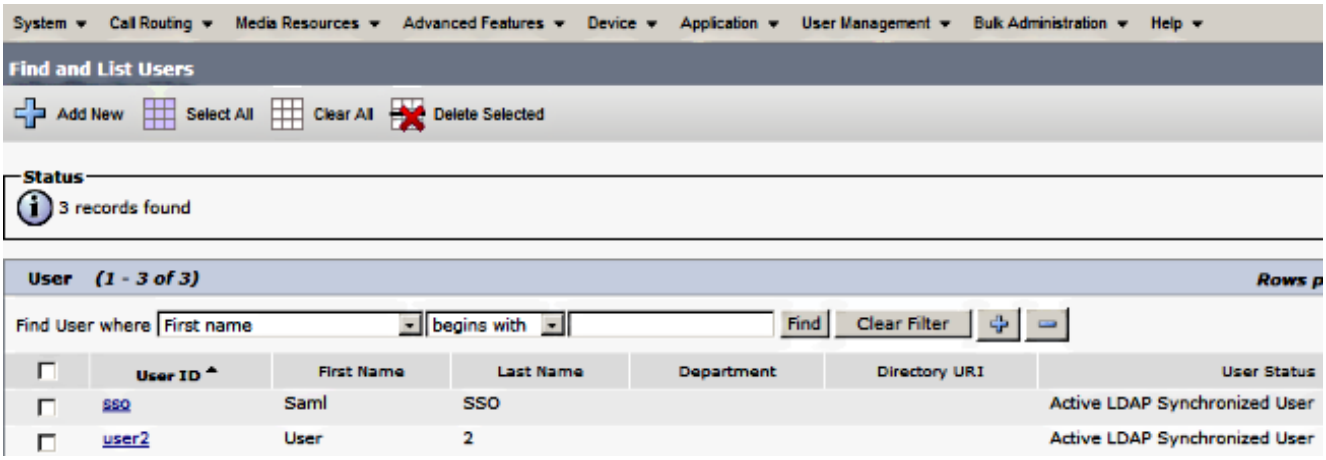
7. Deselezionare **Usa SSL** se non si desidera utilizzare SSL (Secure Sockets Layer) per comunicare con la directory LDAP.

   Suggerimento: Se si desidera configurare LDAP su SSL, caricare il certificato della directory LDAP in CUCM. Per informazioni sul meccanismo di sincronizzazione degli account per prodotti LDAP specifici e sulle best practice generali per la sincronizzazione LDAP, vedere il

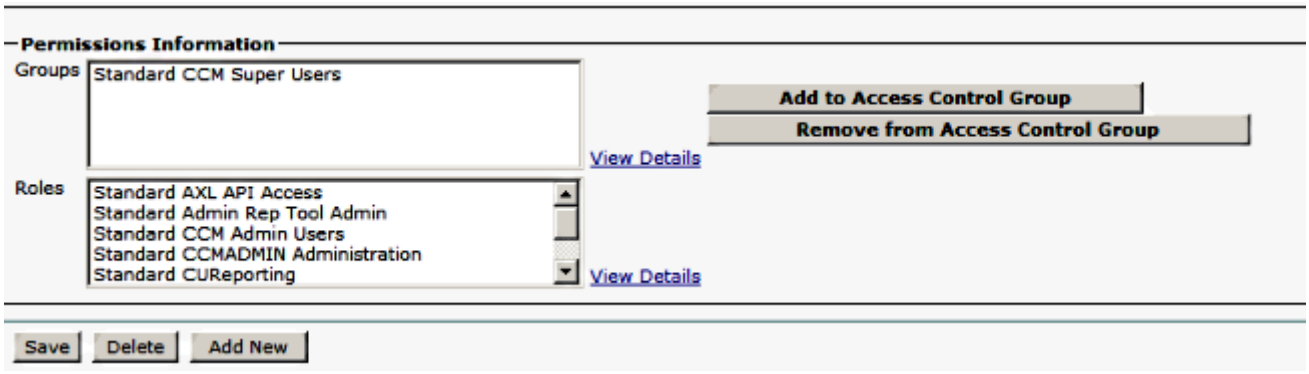
contenuto della directory LDAP in Cisco Unified Communications Manager SRND.

8. Fare clic su **Save** (Salva), quindi su **Perform Full Sync Now (Esegui sincronizzazione completa)**.
   Nota: Prima di fare clic su Salva, verificare che il servizio **Cisco DirSync** sia abilitato nella pagina Web Serviceability.

9. Passare a **Gestione utente > Utente finale** e selezionare un utente al quale si desidera assegnare il ruolo amministrativo CUCM (in questo esempio viene selezionato **SSO** utente).



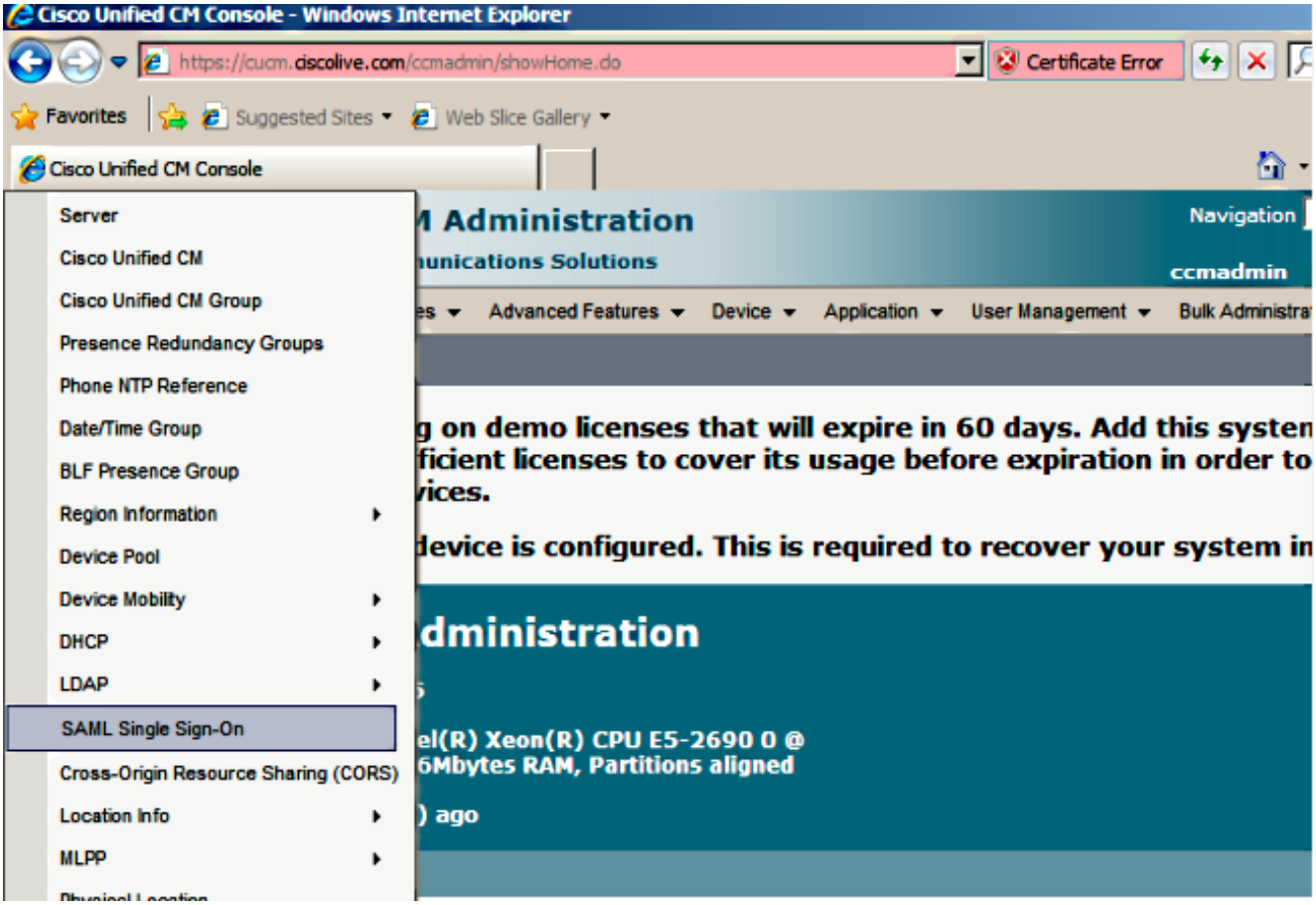
10. Scorrere fino a visualizzare le informazioni sulle autorizzazioni e fare clic su **Aggiungi a gruppo di controllo di accesso**. Selezionare **Utenti privilegiati CCM standard**, fare clic su **Aggiungi selezionati**, quindi fare clic su **Salva**.



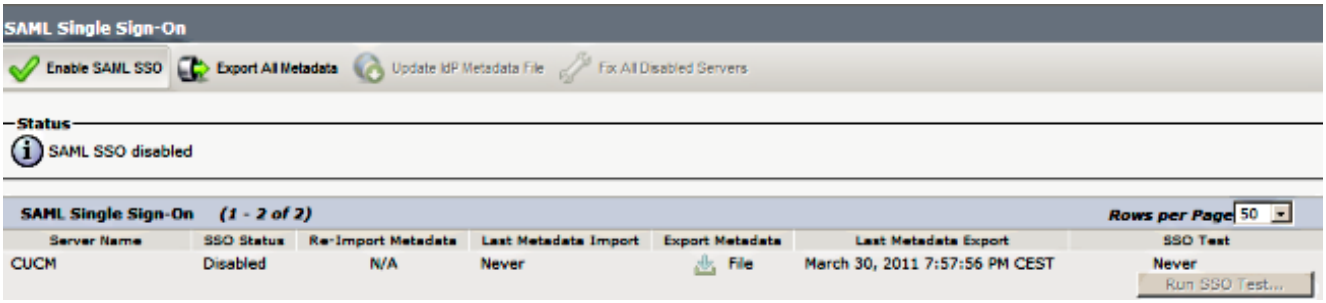
Abilita SAML SSO

1. Accedere all'interfaccia utente di amministrazione CUCM.

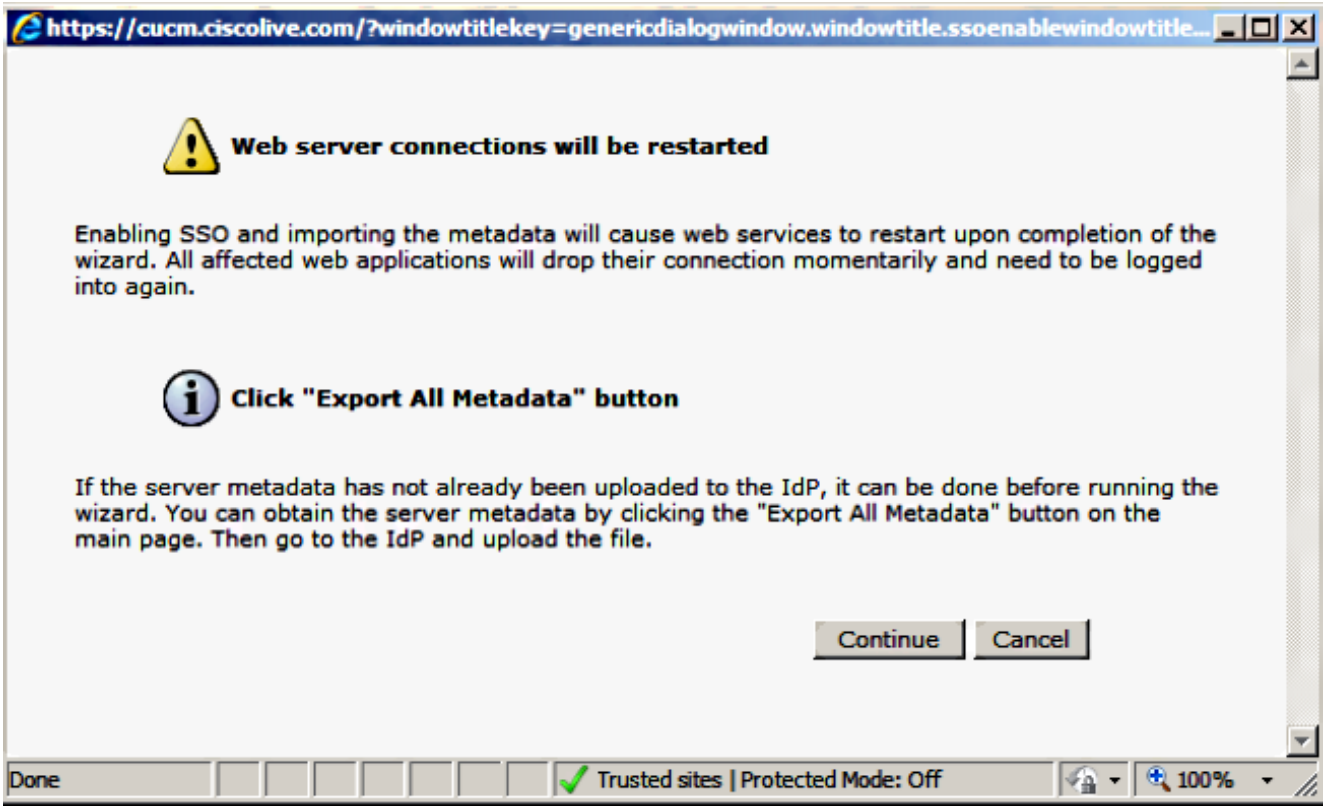
2. Scegliere **Sistema > SAML Single Sign-On** e viene visualizzata la finestra Configurazione SAML Single Sign-On.



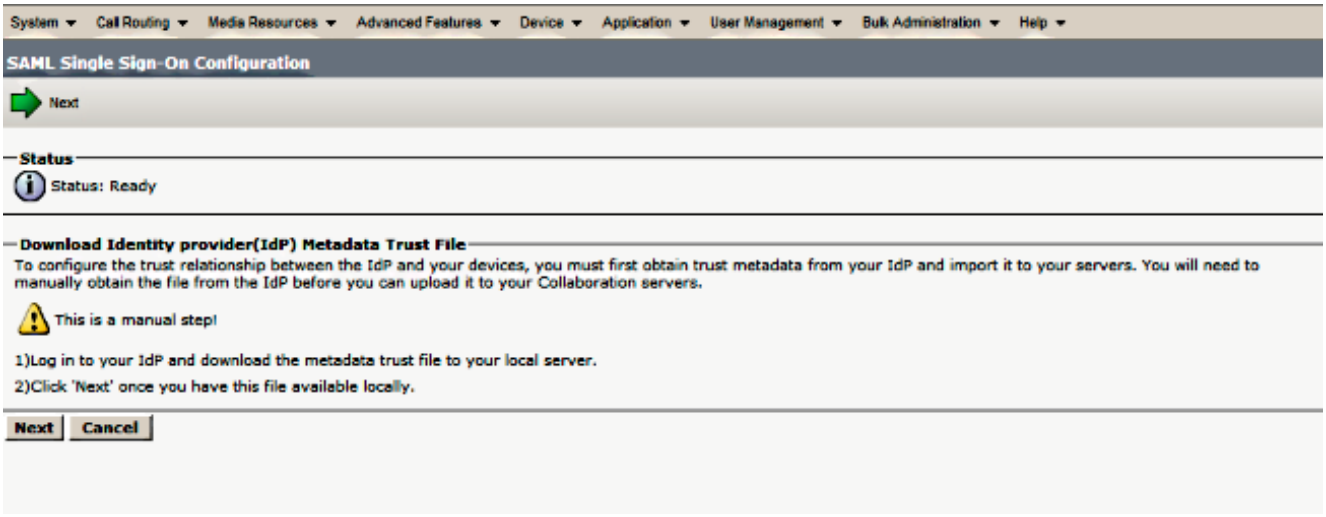
3. Per abilitare l'SSO SAML nel cluster, fare clic su **Abilita SSO SAML**.



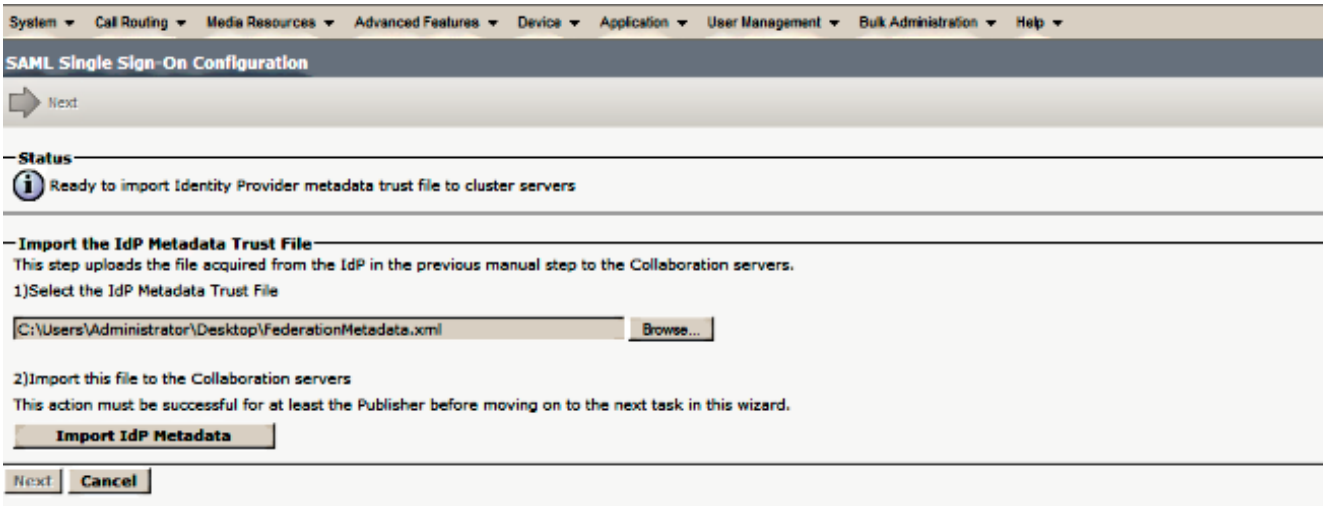
4. Nella finestra Reimposta avviso fare clic su **Continua**.

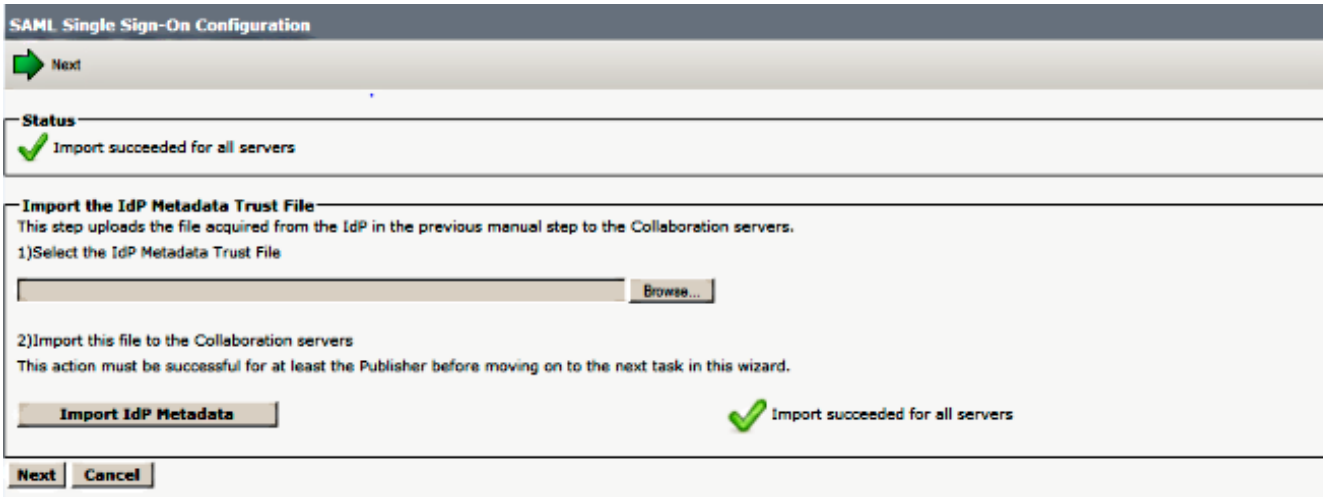


5. Nella schermata SSO fare clic su **Sfoglia** per importare il file XML dei metadati IdP (**FederationMetadata.xml**) con il passaggio **Download IdP Metadata**.

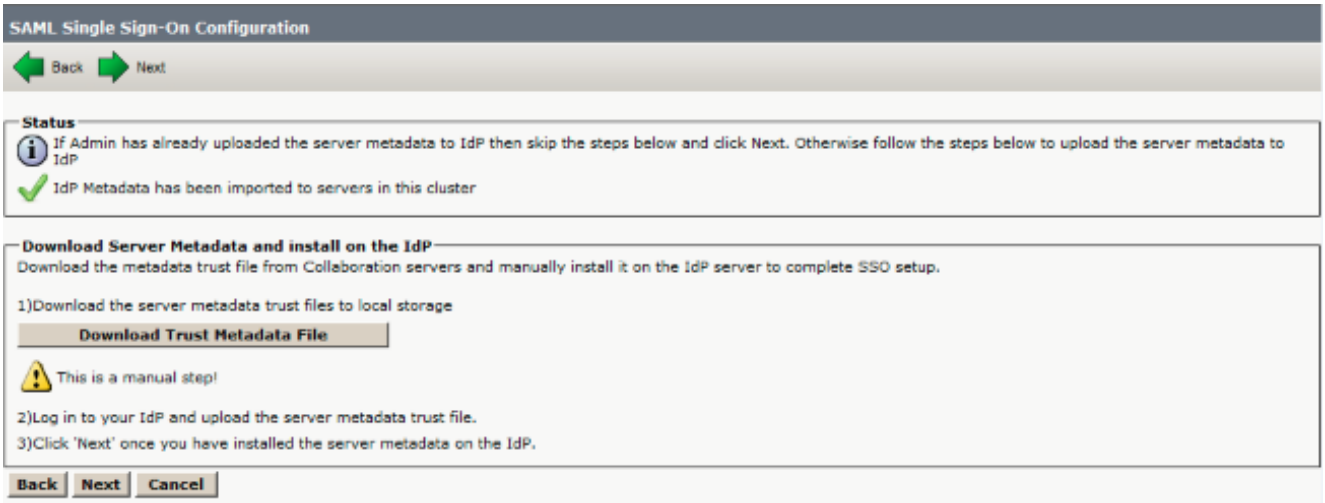


6. Una volta caricato il file di metadati, fare clic su **Import IdP Metadata** per importare le informazioni IdP in CUCM. Confermare che l'importazione è stata completata e fare clic su **Avanti** per continuare.

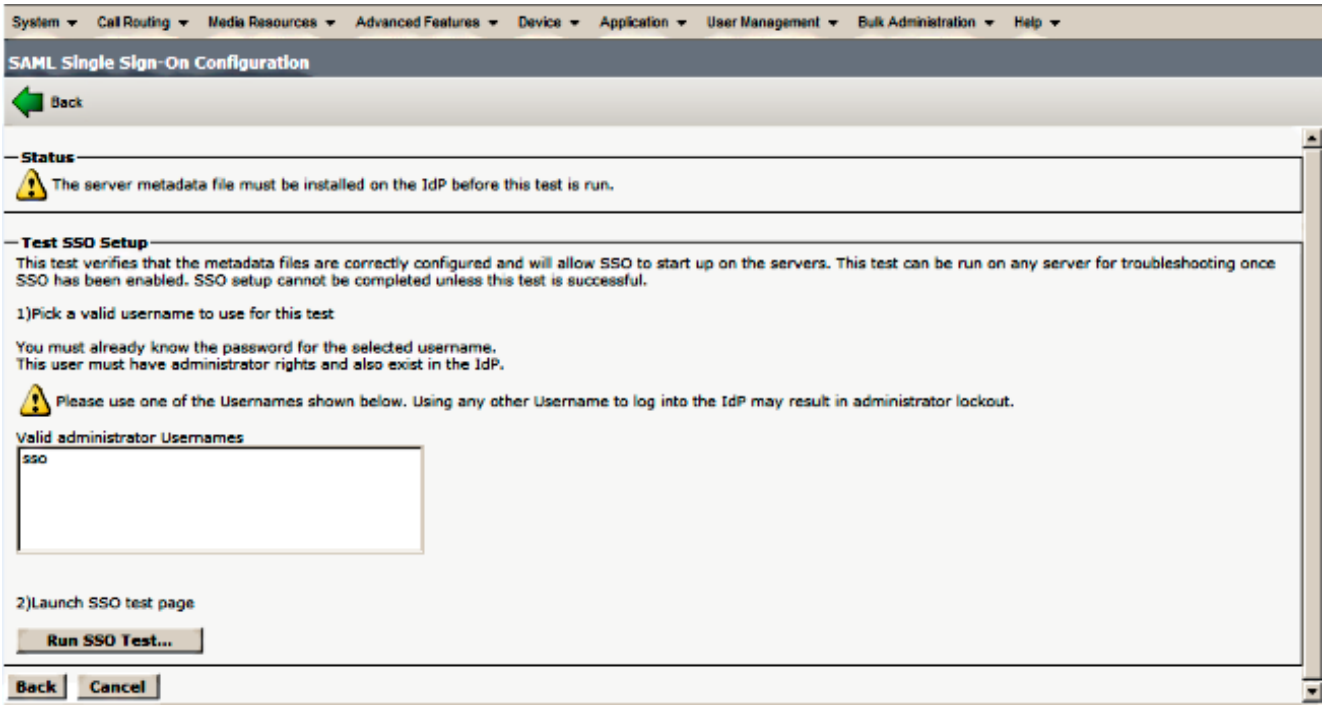




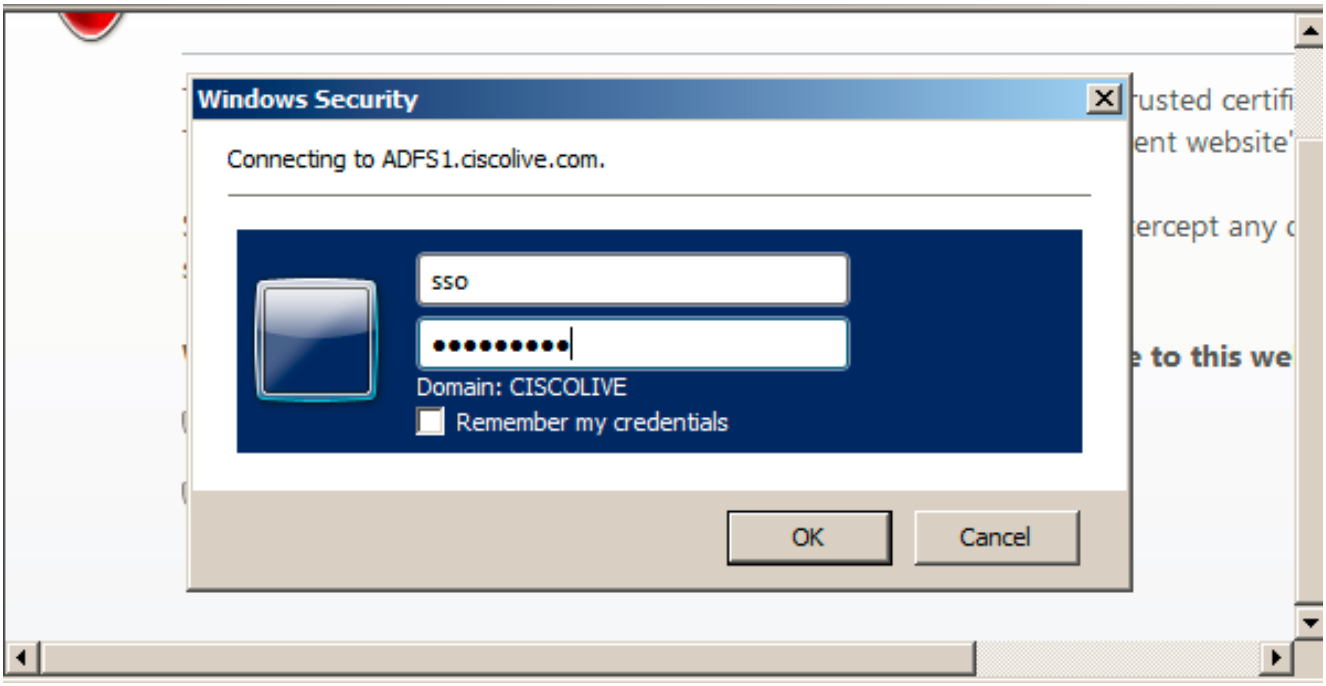
7. Fare clic su **Scarica file metadati di trust** (facoltativo) per salvare il CUCM e i metadati CUCM IM e Presenza in una cartella locale e passare a Aggiungi CUCM come attendibilità componente. Al termine della configurazione di AD FS, andare al passaggio 8.



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



9. Ignorare gli avvisi relativi ai certificati e continuare. Quando vengono richieste le credenziali, immettere il nome utente e la password per l'**SSO** utente e fare clic su **OK**.



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

10. Dopo il completamento di tutti i passaggi, il "Test SSO riuscito!" viene visualizzato un messaggio. Fare clic su **Close** (Chiudi) e su **Finish** (Fine) per continuare. Le attività di configurazione necessarie per abilitare l'SSO in CUCM con ADFS sono state completate.

11. Poiché CUCM IM e Presence funzionano come il sottoscrittore CUCM, è necessario configurare Aggiungi CUCM IM e Presenza come attendibilità componente e quindi eseguire **Esegui test SSO** per abilitare l'SSO SAML dalla stessa pagina SAML SSO CUCM.

    Nota: Se si configurano i file XML dei metadati di tutti i nodi su IdP e si abilita l'operazione SSO su un nodo, l'SSO SAML viene abilitato su tutti i nodi del cluster.

    AD FS deve essere configurato come relaying party per tutti i nodi di CUCM, CUCM IM e Presenza in un cluster.

    Suggerimento: È inoltre necessario configurare Cisco Unity Connection, CUCM IM e Presence per SAML SSO se si desidera utilizzare l'esperienza SAML SSO per i client Cisco Jabber.

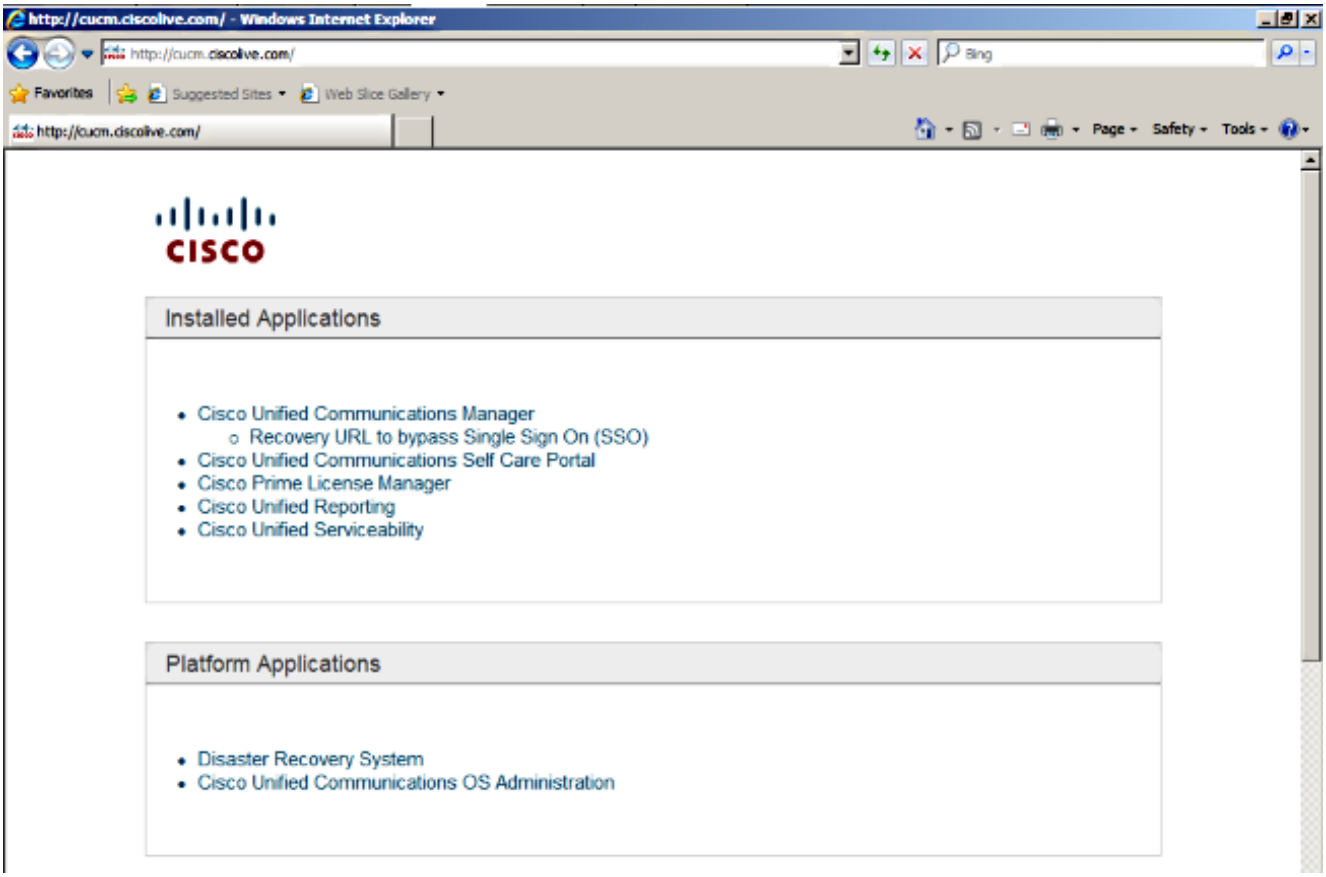
Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

1. Aprire un browser Web e immettere il nome FQDN per CUCM.

2. Fare clic su **Cisco Unified Communications Manager**.

3. Selezionare l'app Web (**Amministrazione CM/Servizi unificati/Cisco Unified Reporting**) e fare clic su **Vai**, quindi verranno richieste le credenziali da ADFS. Dopo aver immesso le credenziali di **SSO** utente, si è connessi correttamente all'app Web selezionata (**pagina Amministrazione CM, pagina Manutenzione unificata, Cisco Unified Reporting***).*

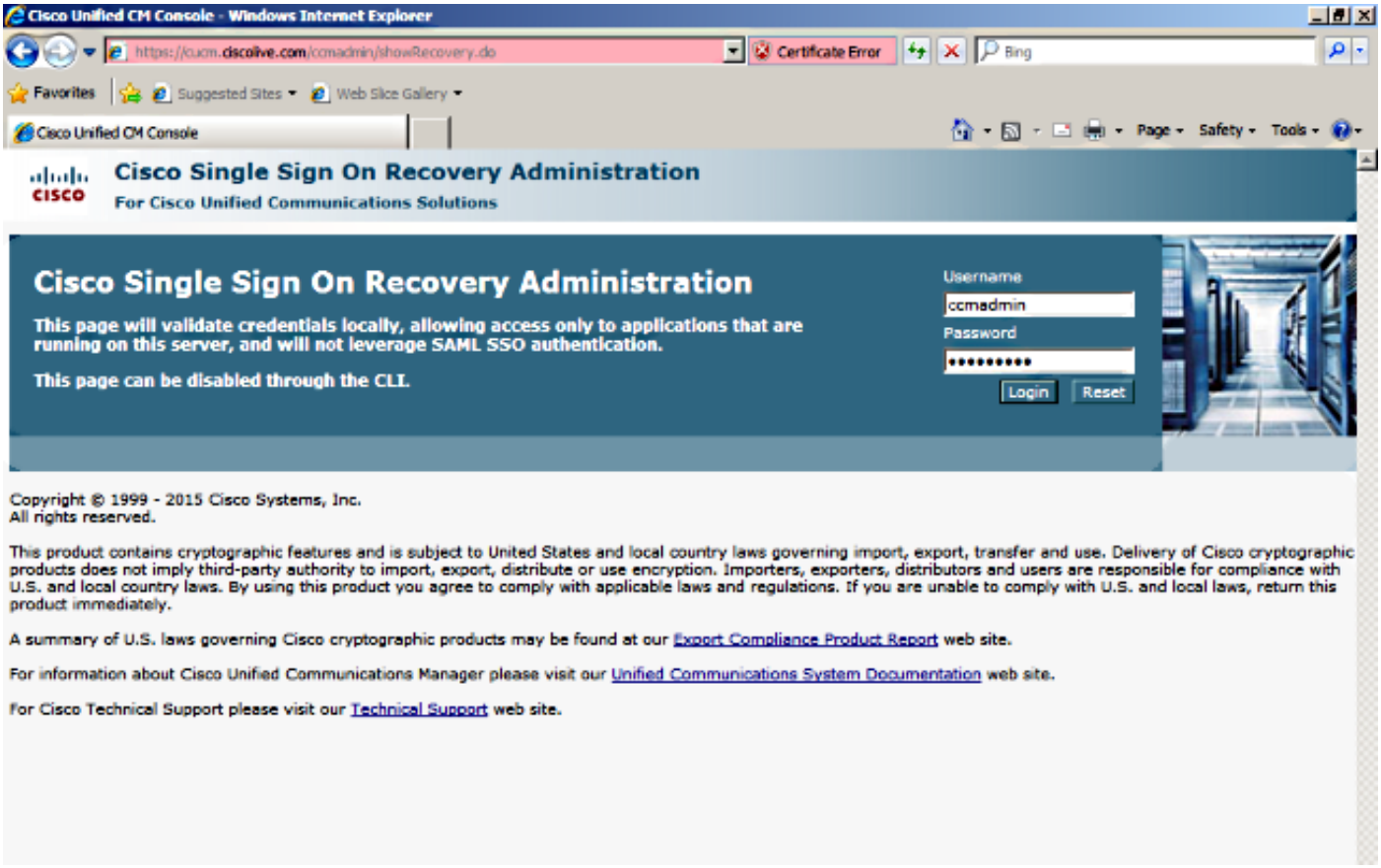


Nota: SAML SSO non consente l'accesso a queste pagine:

- Prime Licensing Manager
- Amministrazione del sistema operativo
- Sistema di disaster recovery

Risoluzione dei problemi

Se non è possibile abilitare SAML e non è possibile eseguire l'accesso, utilizzare la nuova opzione in Applicazioni installate denominata **URL di ripristino per ignorare Single Sign-On (SSO)**, che può essere utilizzata per accedere con le credenziali create durante l'installazione o con gli utenti amministrativi CUCM creati localmente.



Per ulteriori informazioni sulla risoluzione dei problemi, consultare il documento sulla risoluzione dei problemi di SAML SSO per i prodotti Collaboration versione 10.x.