

Esempio di configurazione dell'accesso al portale di amministrazione ISE con credenziali AD

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Partecipa ad ISE e AD](#)

[Seleziona gruppi di directory](#)

[Abilita accesso amministrativo per AD](#)

[Configurare il mapping tra il gruppo di amministratori e il gruppo AD](#)

[Impostare le autorizzazioni RBAC per il gruppo Admin](#)

[Accesso ad ISE con credenziali AD](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive un esempio di configurazione per l'utilizzo di Microsoft Active Directory (AD) come archivio identità esterno per l'accesso amministrativo all'interfaccia utente di gestione di Cisco Identity Services Engine (ISE).

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di Cisco ISE versione 1.1.x o successive
- Microsoft AD

Componenti usati

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

- Cisco ISE versione 1.1.x

- Windows Server 2008 release 2

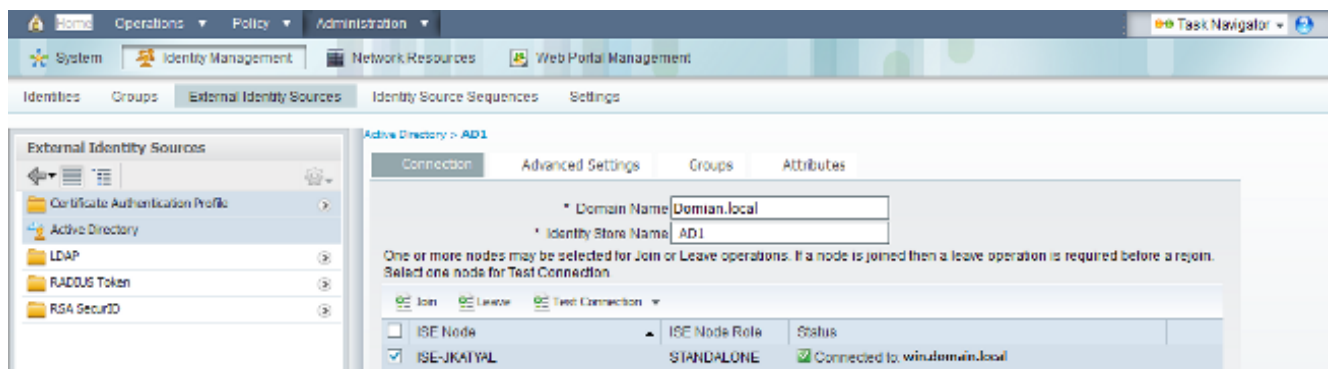
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Configurazione

Utilizzare questa sezione per configurare l'uso di Microsoft AD come archivio identità esterno per l'accesso amministrativo all'interfaccia utente grafica di gestione di Cisco ISE.

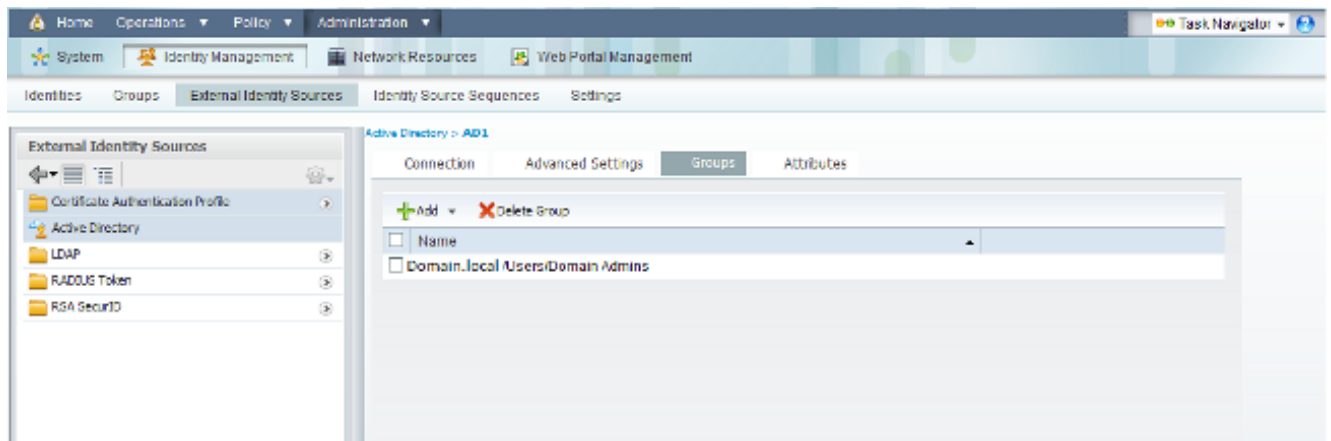
Partecipa ad ISE e AD

1. Passare a **Amministrazione > Gestione delle identità > Origini identità esterne > Active Directory**.
2. Immettere il nome del dominio Active Directory e il nome dell'archivio identità e fare clic su **Partecipa**.
3. Immettere le credenziali dell'account AD che possono aggiungere e modificare gli oggetti computer e fare clic su **Salva configurazione**.



Seleziona gruppi di directory

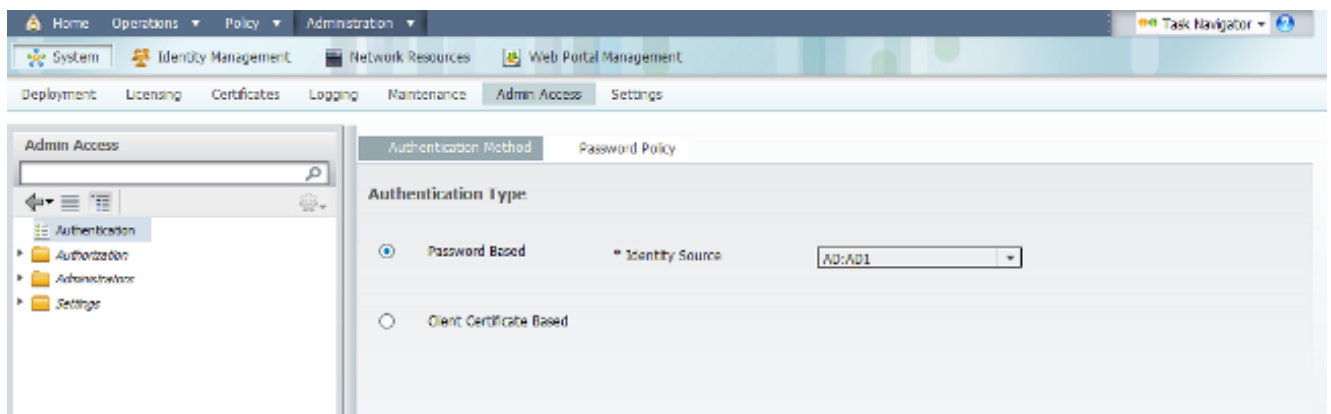
1. Passare a **Amministrazione > Gestione delle identità > Origini identità esterne > Active Directory > Gruppi > Aggiungi > Seleziona gruppi dalla directory**.
2. Importare almeno un gruppo AD a cui appartiene l'amministratore.



Abilita accesso amministrativo per AD

Completare questa procedura per abilitare l'autenticazione basata su password per AD:

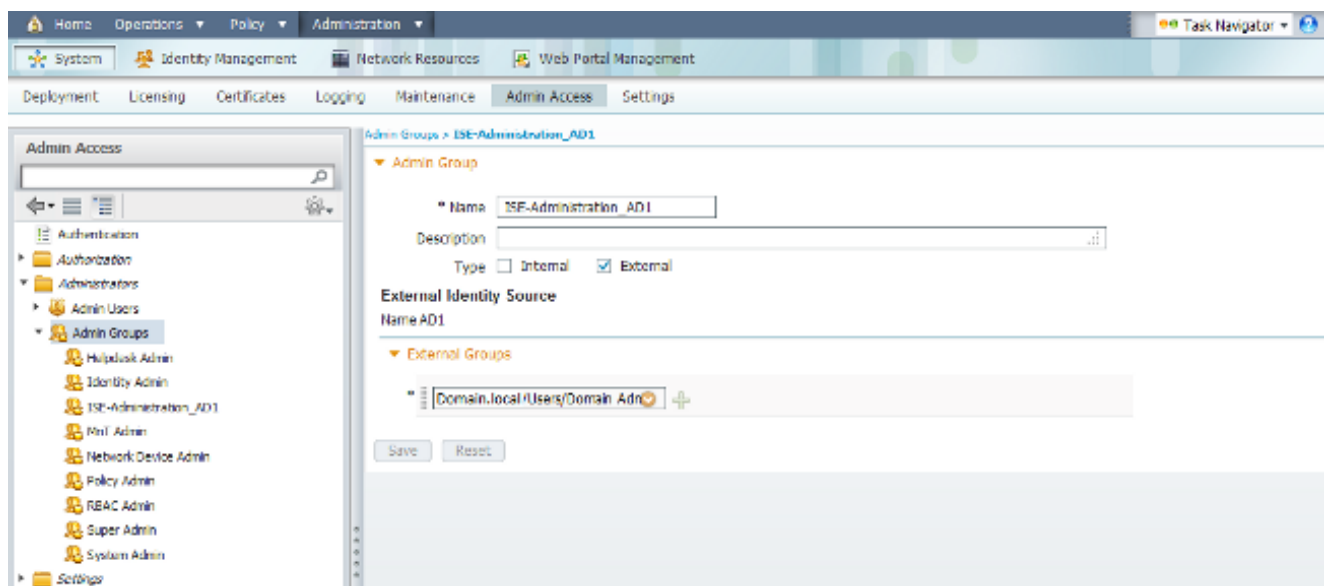
1. Selezionare **Amministrazione > Sistema > Accesso amministratore > Autenticazione**.
2. Nella scheda **Metodo di autenticazione** selezionare l'opzione **Basato su password**.
3. Selezionare **AD** dal menu a discesa **Origine identità**.
4. Fare clic su **Salva modifiche**.



Configurare il mapping tra il gruppo di amministratori e il gruppo AD

Definire un Cisco ISE Admin Group e mapparlo a un gruppo AD. In questo modo viene concessa l'autorizzazione per determinare le autorizzazioni RBAC (Role Based Access Control) per l'amministratore in base all'appartenenza ai gruppi in Active Directory.

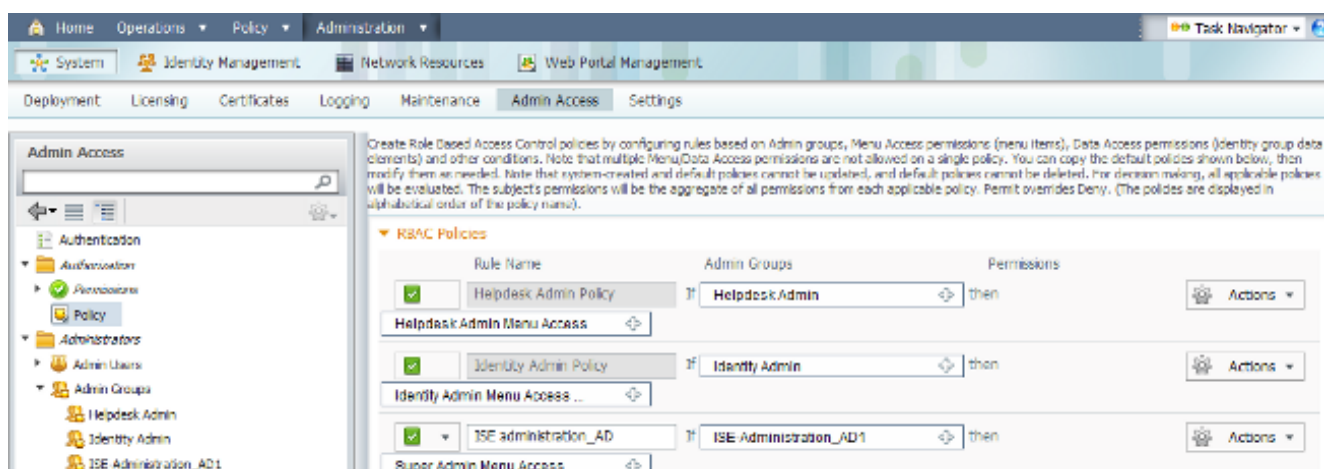
1. Passare a **Amministrazione > Sistema > Accesso amministratore > Amministratori > Gruppi amministratori**.
2. Fare clic su **Add** nell'intestazione della tabella per visualizzare il nuovo riquadro di configurazione del gruppo di amministratori.
3. Immettere il nome del nuovo gruppo Amministratore.
4. Nel campo **Tipo** selezionare la casella di controllo **Esterno**.
5. Dal menu a discesa **Gruppi esterni**, selezionare il gruppo AD a cui si desidera mappare questo gruppo amministrativo, come definito nella sezione **Seleziona gruppi di directory**.
6. Fare clic su **Salva modifiche**.



Impostare le autorizzazioni RBAC per il gruppo Admin

Completare questi passaggi per assegnare le autorizzazioni RBAC ai gruppi amministrativi creati nella sezione precedente:

1. Selezionare **Amministrazione > Sistema > Accesso amministratore > Autorizzazione > Criteri**.
2. Dal menu a discesa **Azioni** a destra, selezionare **Inserisci nuovo criterio sotto** per aggiungere un nuovo criterio.
3. Creare una nuova regola denominata **ISE_administration_AD**, mapparla al gruppo Admin definito nella sezione Abilitare l'accesso amministrativo per AD e assegnarle le autorizzazioni. **Nota:** In questo esempio viene assegnato il gruppo Admin denominato **Super Admin**, equivalente all'account admin standard.
4. Fare clic su **Save Changes** (Salva modifiche). Nell'angolo inferiore destro dell'interfaccia grafica viene visualizzata la conferma delle modifiche salvate.



Accesso ad ISE con credenziali AD

Per accedere ad ISE con le credenziali di AD, completare la procedura seguente:

1. Uscire dalla GUI amministrativa.
2. Selezionare **AD1** dal menu a discesa **Origine identità**.
3. Immettere il nome utente e la password del database di Active Directory ed eseguire l'accesso.



Nota: Per impostazione predefinita, ISE utilizza l'archivio utenti interno nel caso in cui AD non sia raggiungibile o le credenziali dell'account utilizzate non esistano in AD. Ciò semplifica l'accesso rapido se si utilizza l'archivio interno mentre AD è configurato per l'accesso amministrativo.

Verifica

Per verificare che la configurazione funzioni correttamente, verificare il nome utente autenticato nell'angolo in alto a destra della GUI di ISE.



Risoluzione dei problemi

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

Informazioni correlate

- [Guida dell'utente di Cisco Identity Services Engine, versione 1.1 - Gestione delle identità e dell'accesso degli amministratori](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)