

Configurazione di LDAP su Expressway per l'accesso Web, API e CLI

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Configurazione LDAP](#)

[Come trovare il DN di base](#)

[Esempio di configurazione LDAP](#)

[Configurazione dei gruppi di amministratori](#)

[Opzioni di configurazione dei gruppi di amministratori in Expressway](#)

[Configurazione del gruppo di amministratori in AD](#)

[Configurazione del gruppo di amministratori in Expressway](#)

[Verifica](#)

Introduzione

In questo documento viene descritto come abilitare il protocollo LDAP (Lightweight Directory Access Protocol) sul server Expressway e come abilitare i gruppi di amministratori ad accedere a Expressway con gli utenti del dominio tramite Web, API (Application Programming Interface) e CLI (Command Line Interface).

Contributo di Jefferson Madriz e Elias Sevilla, Cisco TAC Engineers.

Prerequisiti

Requisiti

- Conoscenze base di Expressway.
- Configurazione di base di Expressway già eseguita.
- Active Directory (AD) già configurato.
- Regole del firewall pronte per consentire la comunicazione tra Expressway e il server AD.

Componenti usati

- Active Directory installato in Windows Server 2016.
- Server Expressway-C nella versione X14.0.3.

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

Configurazione LDAP

La pagina di configurazione LDAP Utenti > Configurazione LDAP viene utilizzata per configurare una connessione LDAP a un servizio directory remoto per l'autenticazione dell'account amministratore.

- Autenticazione account remoto: Questa sezione consente di abilitare o disabilitare l'utilizzo di LDAP per l'autenticazione degli account remoti.

The screenshot shows the 'Remote account authentication' section of a configuration interface. It contains two rows of settings. The first row is 'Administrator authentication source' with a dropdown menu set to 'Both' and an information icon. The second row is 'FindMe authentication source' with a dropdown menu set to 'Local' and an information icon.

- Solo locale: Le credenziali vengono verificate rispetto a un database locale memorizzato nel sistema.
- Solo remoto: Le credenziali vengono verificate rispetto a una directory esterna delle credenziali.
- Entrambi: Le credenziali vengono innanzitutto verificate rispetto a un database locale archiviato nel sistema e quindi, se non esiste corrispondenza con l'account, viene utilizzata la directory delle credenziali esterne.

- Configurazione server LDAP: questa sezione specifica i dettagli di connessione al server LDAP.

The screenshot shows the 'LDAP server configuration' section. It includes several settings: 'FQDN address resolution' with a dropdown set to 'Address record'; 'Host name and Domain' with two text input fields; 'Port' with a text input field containing '389' and a red star icon; 'Encryption' with a dropdown set to 'TLS'; and 'Certificate revocation list (CRL) checking' with a dropdown set to 'None'. Each setting has an information icon to its right.

Risoluzione indirizzo FQDN:

- Record SRV: ricerca dei record DNS (Domain Name Service).
- Record indirizzo: Ricerca record A o AAAA DNS.
- Indirizzo IP: immessi direttamente come indirizzo IP.

 Nota: Se si utilizzano record SRV, verificare che _ldap._tcp. i record utilizzano la porta LDAP standard 389. Expressway non supporta altri numeri di porta per LDAP.

Nome host e dominio:

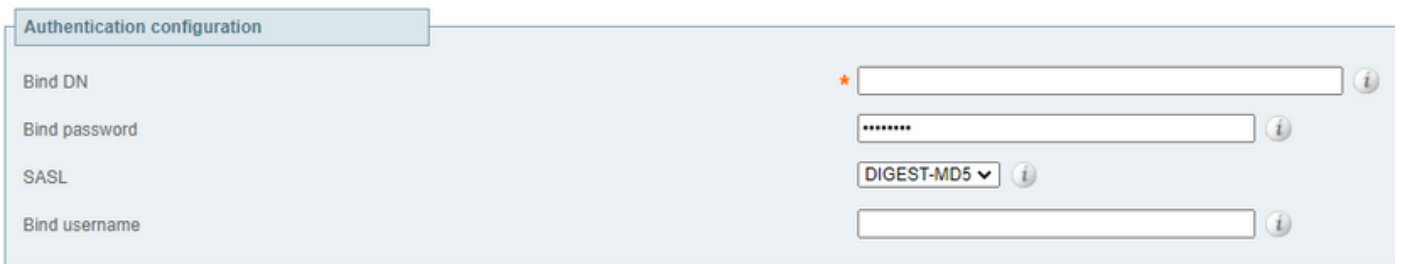
- Record SRV: è necessaria solo la parte Domain dell'indirizzo del server.
- Record indirizzo: immettere il nome dell'host e il dominio. Questi elementi vengono quindi combinati per fornire l'indirizzo completo del server per la ricerca dei record di indirizzo DNS.
- Indirizzo IP: l'indirizzo del server viene immesso direttamente come indirizzo IP.

Port:

- La porta IP da utilizzare sul server LDAP.

Crittografia:

- TLS: utilizza la crittografia TLS (Transport Layer Security) per la connessione al server LDAP.
- Spento: non viene utilizzata alcuna crittografia.
- Configurazione dell'autenticazione: questa sezione specifica le credenziali di autenticazione di Expressway da utilizzare per il binding al server LDAP.



Authentication configuration	
Bind DN	ⓘ
Bind password	ⓘ
SASL	DIGEST-MD5 ▼ ⓘ
Bind username	ⓘ

DN binding: Nome distinto (DN), senza distinzione tra maiuscole e minuscole, utilizzato da Expressway per l'associazione al server LDAP. È importante specificare il DN nell'ordine cn=, quindi ou= e infine dc=

 Nota: L'account di binding è in genere un account di sola lettura senza privilegi speciali.

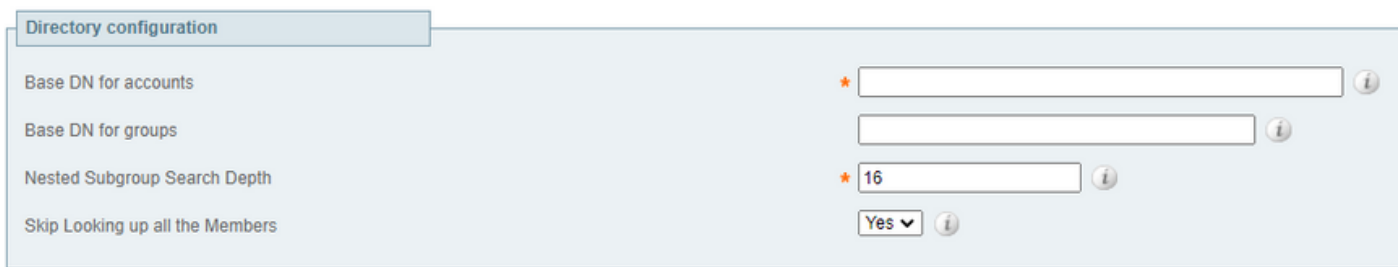
Password binding: La password (con distinzione tra maiuscole e minuscole) utilizzata da Expressway per eseguire il binding al server LDAP.

SASL: Meccanismo SASL (Simple Authentication and Security Layer) da utilizzare per il binding al server LDAP

- Nessuna: non viene utilizzato alcun meccanismo.
- DIGEST-MD5: viene utilizzato il meccanismo DIGEST-MD5.

Nome utente di binding: Nome utente dell'account utilizzato da Expressway per accedere al server LDAP (con distinzione tra maiuscole e minuscole).

- Configurazione directory: In questa sezione vengono specificati i nomi distinti di base da utilizzare per la ricerca di nomi di account e gruppi.



Directory configuration

Base DN for accounts *

Base DN for groups *

Nested Subgroup Search Depth * 16

Skip Looking up all the Members Yes

DN di base per gli account: definizione dell'unità organizzativa e del controller di dominio del nome distinto in cui viene avviata la ricerca di account utente nella struttura del database (senza distinzione tra maiuscole e minuscole).

Il DN di base per conti e gruppi deve essere uguale o inferiore al livello DC (includere tutti i valori dc= e ou= se necessario). L'autenticazione LDAP non esamina gli account dei controller di dominio secondari, ma solo i livelli di unità organizzativa e di riquadro comune (CN) inferiori.

DN di base per i gruppi: la definizione dell'unità organizzativa e del controller di dominio del nome distinto da cui deve iniziare la ricerca di gruppi nella struttura del database (senza distinzione tra maiuscole e minuscole).

Se non viene specificato alcun DN di base per i gruppi, il DN di base per i conti viene utilizzato sia per i gruppi che per i conti.

Profondità di ricerca sottogruppi nidificati: utilizzata per limitare la profondità dei gruppi per la ricerca LDAP.

Ignora ricerca di tutti i membri: consente di disabilitare o abilitare la ricerca dei membri di un gruppo di amministratori durante il processo di ricerca dell'autenticazione. Il valore predefinito è Sì - ignora la ricerca di membri.

Come trovare il DN di base

Sul server AD, aprire Prompt dei comandi (CMD) come amministratore ed eseguire il comando: **dsquery user -name**

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>dsquery user -name exp
'CN=exp,CN=Users,DC=apolo,DC=local'
C:\Users\Administrator>
```

Esempio di configurazione LDAP

L'origine dell'autenticazione dell'amministratore è impostata su Both e SASL è impostata su None in questo esempio.

Cisco Expressway-C

Status > System > Configuration > Applications > Users > Maintenance >

LDAP configuration

Remote account authentication

Administrator authentication source: Both ⓘ

FindMe authentication source: Local ⓘ

LDAP server configuration

FQDN address resolution: Address record ⓘ

Host name and Domain: ad-apollo . apollo.local ⓘ

Port: * 389 ⓘ

Encryption: Off ⓘ

Certificate revocation list (CRL) checking: None ⓘ

Authentication configuration

Bind DN: * cn=exp,cn=Users,dc=apollo,dc=local ⓘ

Bind password: ⓘ

SASL: None ⓘ

Bind username: exp ⓘ

Directory configuration

Base DN for accounts: * cn=Users,dc=apollo,dc=local ⓘ

Base DN for groups: ⓘ

Nested Subgroup Search Depth: * 16 ⓘ

Skip Looking up all the Members: Yes ⓘ

Save

Status (last updated: 15:27:47 CDT)

State: Available

Verifica stato LDAP

Convalida stato connessione server LDAP:

- Disponibile: Non viene visualizzato alcun messaggio di errore
- Operazione non riuscita: Vengono visualizzati messaggi di errore. [Messaggi di errore LDAP](#)

Configurazione dei gruppi di amministratori

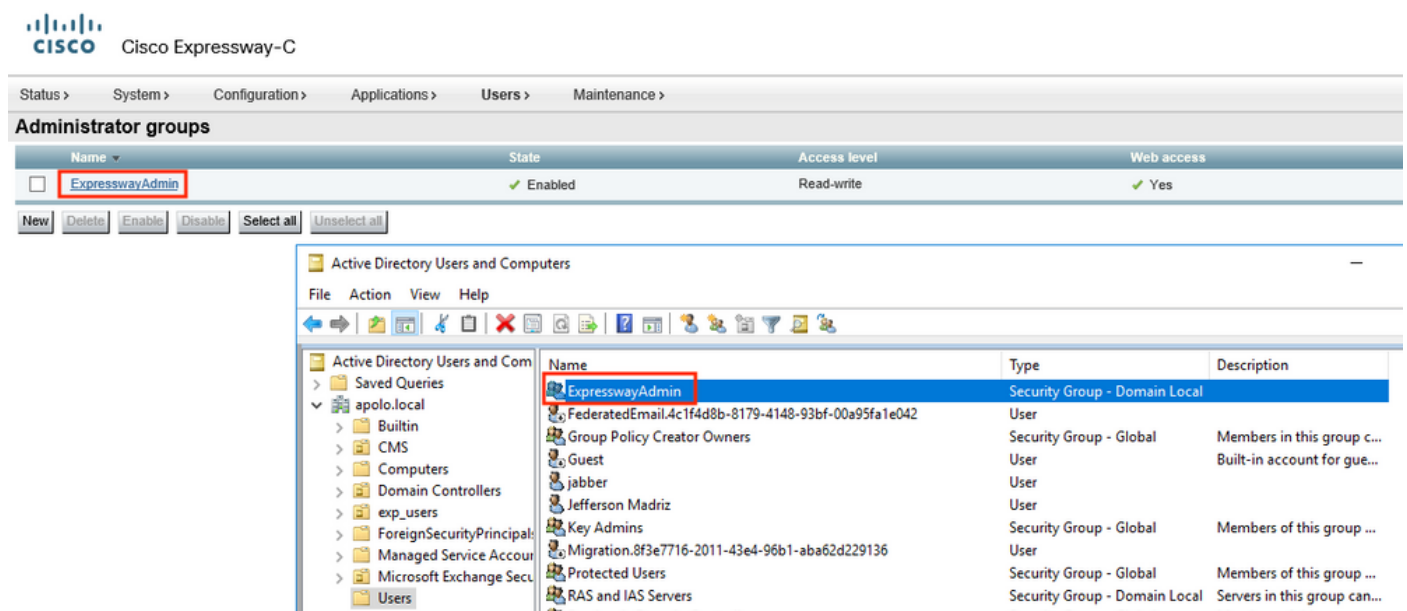
La pagina Gruppi amministratori Utenti > Gruppi amministratori elenca tutti i gruppi di amministratori configurati in Expressway e consente di aggiungere, modificare ed eliminare i gruppi.

 Nota: I gruppi di amministratori sono validi solo se è abilitata l'autenticazione dell'account remoto tramite LDAP.

Quando si accede all'interfaccia Web di Expressway, le credenziali vengono autenticate in base al servizio directory remoto e all'utente vengono assegnati i diritti di accesso associati al gruppo a cui appartiene.

Opzioni di configurazione dei gruppi di amministratori in Expressway

Nome: Il nome del gruppo di amministratori. I nomi dei gruppi definiti in Expressway devono corrispondere ai nomi dei gruppi impostati nel servizio directory remoto per gestire l'accesso di amministratore a Expressway.



The screenshot shows the Cisco Expressway web interface. The top navigation bar includes Status, System, Configuration, Applications, Users, and Maintenance. The 'Administrator groups' section is active, displaying a table with columns: Name, State, Access level, and Web access. The 'ExpresswayAdmin' group is listed with a checked checkbox, 'Enabled' state, 'Read-write' access level, and 'Yes' for web access. Below the table are buttons for New, Delete, Enable, Disable, Select all, and Unselect all. An inset window titled 'Active Directory Users and Computers' shows the 'Users' folder expanded, with the 'ExpresswayAdmin' group highlighted in the list.

Name	State	Access level	Web access
☒ ExpresswayAdmin	✓ Enabled	Read-write	✓ Yes

Livello di accesso:

- Read-Write: Consente di visualizzare e modificare tutte le informazioni di configurazione. In questo modo si ottengono gli stessi diritti dell'account amministratore predefinito.
- Read-Only: Consente di visualizzare e non modificare le informazioni di stato e configurazione. Alcune pagine, ad esempio la pagina Aggiorna, sono bloccate per gli account di sola lettura.
- Revisore: Consente di accedere solo alle pagine Registro eventi, Registro configurazione, Registro di rete, Avvisi e Panoramica.
- Nessuna: Nessun accesso consentito

Accesso Web: Determina se i membri di questo gruppo possono accedere al sistema tramite l'interfaccia Web.

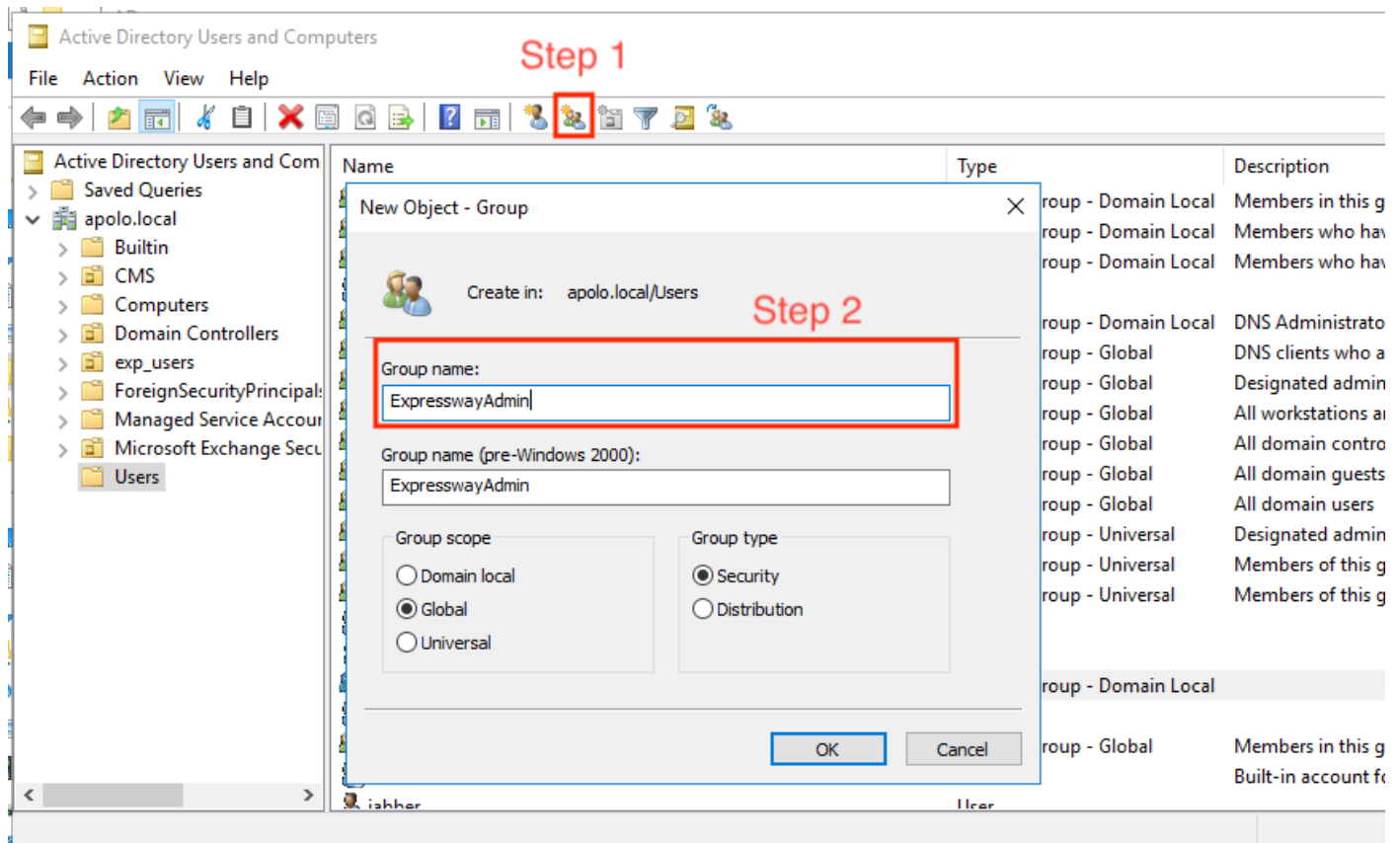
Accesso API: Determina se ai membri di questo gruppo è consentito accedere allo stato e alla configurazione del sistema con l'API.

Accesso CLI: Determina se ai membri di questo gruppo è consentito accedere al sistema tramite CLI.

State: Indica se il gruppo è abilitato o disabilitato.

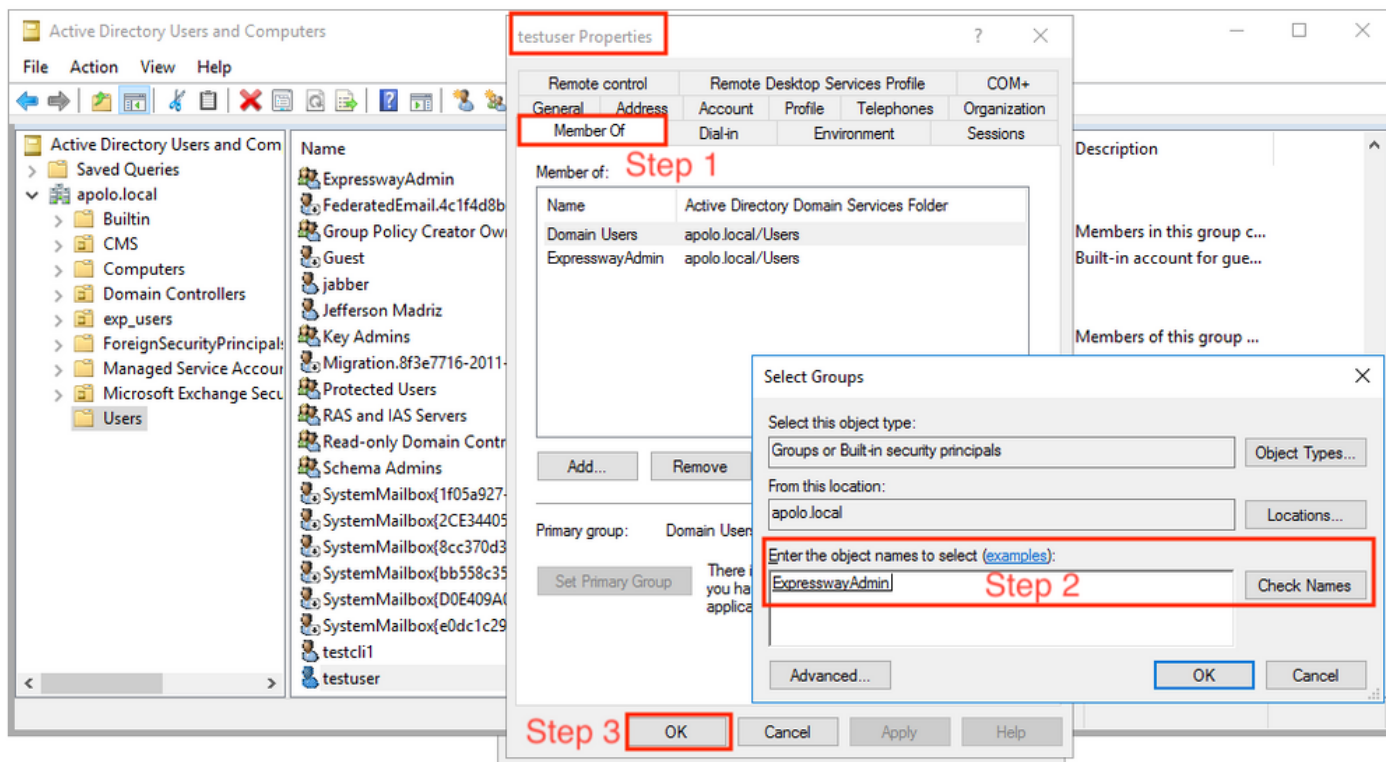
Configurazione del gruppo di amministratori in AD

1. Creare un nuovo Object Group, nella cartella in cui si desidera memorizzare gli utenti.
2. Assegnare un nome al Nome gruppo.

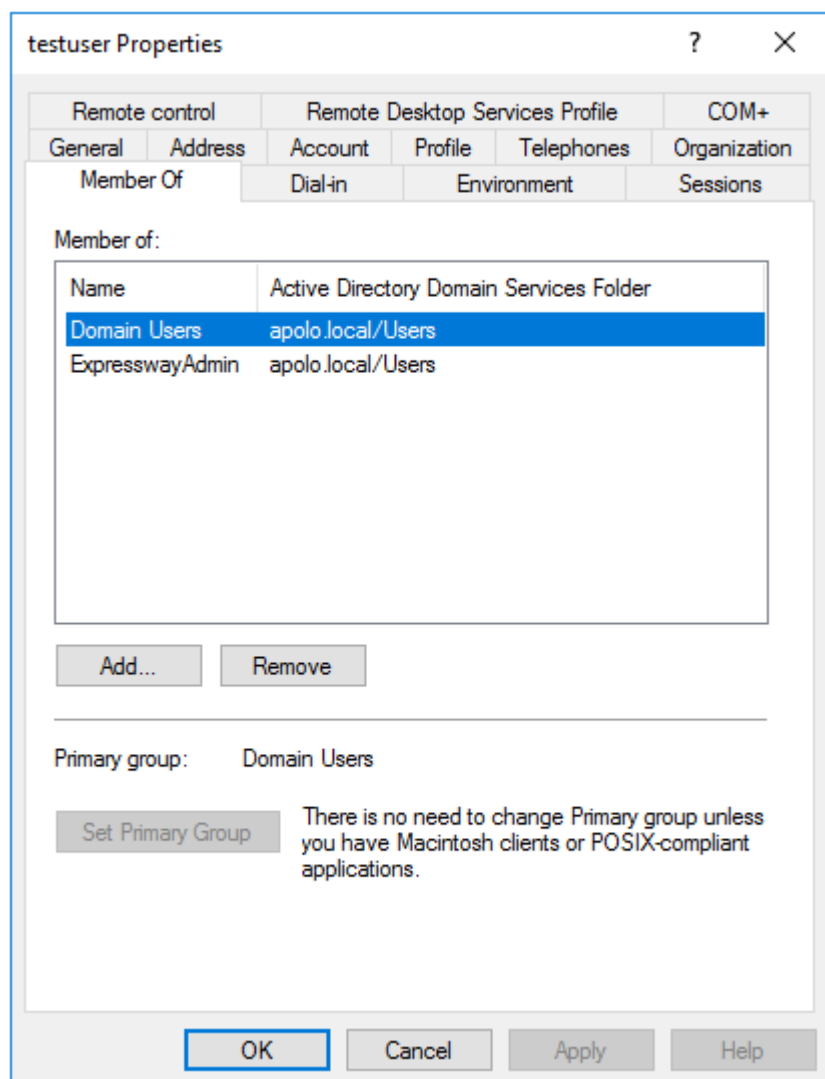


Assegnare il gruppo configurato all'utente o agli utenti che devono accedere a Expressways tramite Web, API o CLI. In questo caso l'utente è testuser.

1. Aprire le proprietà utente, passare alla scheda Membro di, Selezionare Aggiungi
2. Cercare il Nome gruppo creato in precedenza.
3. Quindi selezionare OK.



A questo punto l'utente è membro di Domain Users e ExpresswayAdmin.

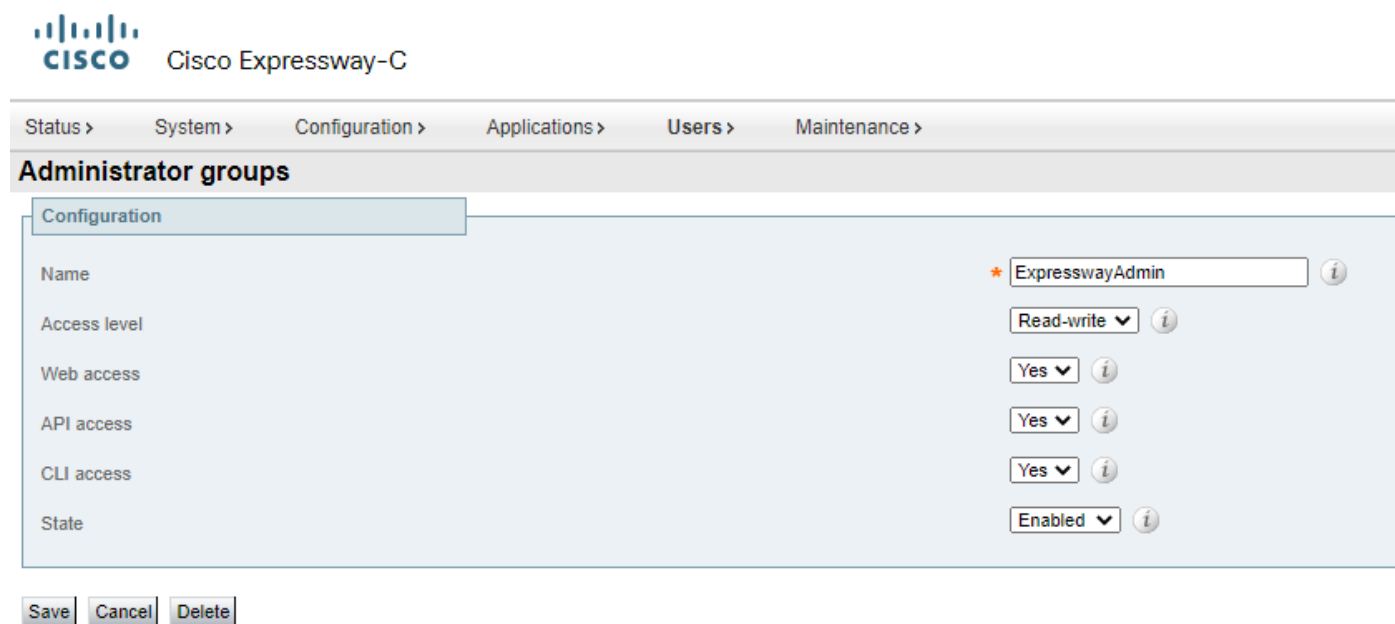


Configurazione del gruppo di amministratori in Expressway

Una volta completata la configurazione, in Expressway passare a Utenti > Gruppi amministratori, selezionare Nuovo

Nome: deve corrispondere al nome del gruppo configurato e associato all'utente LDAP che deve accedere a Expressway. In questo esempio il nome del gruppo è ExpresswayAdmin, quindi il nuovo nome del gruppo Administrator è ExpresswayAdmin.

Questo gruppo dispone di tutte le autorizzazioni e l'accesso disponibili.



The screenshot shows the Cisco Expressway-C web interface. At the top is the Cisco logo and the text "Cisco Expressway-C". Below this is a navigation bar with tabs: Status >, System >, Configuration >, Applications >, Users >, and Maintenance >. The "Users >" tab is selected, and the "Administrator groups" section is active. On the left, there is a "Configuration" tab. The main area shows the configuration for a group named "ExpresswayAdmin". The fields are: Name (ExpresswayAdmin), Access level (Read-write), Web access (Yes), API access (Yes), CLI access (Yes), and State (Enabled). Each field has an information icon (i) to its right. At the bottom, there are three buttons: Save, Cancel, and Delete.

Selezionare Salva.

Administrator groups					
Name	State	Access level	Web access	API access	CLI access
☐ ExpresswayAdmin	✓ Enabled	Read-write	✓ Yes	✓ Yes	✓ Yes

Verifica

Disconnettersi e provare ad accedere tramite Web con l'utente LDAP a cui è associato il gruppo degli amministratori. In questo esempio l'utente creato è testuser.

Administrator login

Username

testuser

Password

.....

Login

È possibile confermare questa condizione selezionando Status > Event log (Stato > Registro eventi):

Status > System > Configuration > Applications Users > Maintenance >

Event Log You are here: [Status](#)

Filter

Contains all of the words: [more options](#)

Filter

Reset

Configure log settings |

Download this page

1 2 3 4 5 6 ... Last | Next

Go to page Go

Results

2021-10-20T12:56:44.135-05:00	php: web: User="testuser" Event="Admin Session Start" Src-ip="10.15.13.30" Src-port="64705" UTCtime="2021-10-20 17:56:44"
2021-10-20T12:56:44.131-05:00	taa-chkpasswd: Event="pam" Module="pam_unix(taa-chkpasswd-webadmin:session)" Level="INFO" Detail="session opened for user testuser by (uid=2)" UTCtime="2021-10-20 17:56:44"

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).