Configurare le federazioni

NetApp Console setup and administration

NetApp
January 13, 2026

Sommario

Configurare le federazioni

Federare la NetApp Console con Active Directory Federation Services (AD FS)

Federa i tuoi servizi di federazione di Active Directory (AD FS) con la NetApp Console per abilitare l'accesso singolo (SSO) per la NetApp Console. Ciò consente agli utenti di accedere alla Console utilizzando le proprie credenziali aziendali.

Ruoli richiesti

Il ruolo di amministratore della federazione è necessario per creare e gestire le federazioni. Il visualizzatore della Federazione può visualizzare la pagina della Federazione."Scopri di più sui ruoli di accesso."

Puoi federarti con il tuo IdP aziendale o con il sito di supporto NetApp . NetApp consiglia di scegliere l'una o l'altra opzione, ma non entrambe.

NetApp supporta solo SSO avviato dal provider di servizi (SP). Per prima cosa, configura il provider di identità in modo che consideri attendibile la NetApp Console come provider di servizi. Quindi, crea una connessione nella Console utilizzando la configurazione del tuo provider di identità.

È possibile configurare la federazione con il server AD FS per abilitare l'accesso Single Sign-On (SSO) per NetApp Console. Il processo prevede la configurazione di AD FS in modo che consideri attendibile la Console come fornitore di servizi e quindi la creazione della connessione nella NetApp Console.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare **Federazione** per visualizzare la pagina **Federazioni**.
3. Selezionare **Configura nuova federazione**.
4. Inserisci i dettagli del tuo dominio:
   a. Scegli se vuoi utilizzare un dominio verificato o il tuo dominio di posta elettronica. Il dominio di posta elettronica è il dominio associato all'account con cui hai effettuato l'accesso.
   b. Inserisci il nome della federazione che stai configurando.
   c. Se scegli un dominio verificato, seleziona il dominio dall'elenco.
5. Selezionare **Avanti**.
6. Per il metodo di connessione, seleziona **Protocollo** e poi seleziona **Active Directory Federation Services (AD FS)**.
7. Selezionare **Avanti**.
8. Crea un trust della relying party nel tuo server AD FS. È possibile utilizzare PowerShell o configurarlo manualmente sul server AD FS. Per informazioni dettagliate su come creare un trust relying party, consultare la documentazione di AD FS.
   a. Creare il trust utilizzando PowerShell utilizzando il seguente script:

```
(new-object Net.WebClient -property @{Encoding = [Text.Encoding]
::UTF8}).DownloadString("https://raw.github.com/auth0/AD FS-
auth0/master/AD FS.ps1") | iex
AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-
cloud-account.auth0.com/login/callback"
```

b. In alternativa, è possibile creare manualmente il trust nella console di gestione di AD FS. Utilizzare i seguenti valori NetApp Console durante la creazione del trust:

   - Quando si crea il Relying Trust Identifier, utilizzare il valore **YOUR_TENANT**: `netapp-cloud-account`
   - Quando selezioni **Abilita supporto per WS-Federation**, usa il valore **YOUR_AUTH0_DOMAIN**: `netapp-cloud-account.auth0.com`

c. Dopo aver creato il trust, copia l'URL dei metadati dal tuo server AD FS o scarica il file dei metadati della federazione. Questo URL o file ti servirà per completare la connessione nella Console.

NetApp consiglia di utilizzare l'URL dei metadati per consentire alla NetApp Console di recuperare automaticamente la configurazione AD FS più recente. Se scarichi il file dei metadati della federazione, dovrai aggiornarlo manualmente nella NetApp Console ogni volta che vengono apportate modifiche alla configurazione di AD FS.

9. Torna alla Console e seleziona **Avanti** per creare la connessione.
10. Creare la connessione con AD FS.
    a. Inserisci l'URL di AD FS copiato dal server AD FS nel passaggio precedente oppure carica il file dei metadati di federazione scaricato dal server AD FS.
11. Seleziona **Crea connessione**. La creazione della connessione potrebbe richiedere alcuni secondi.
12. Selezionare **Avanti**.
13. Seleziona **Test connessione** per testare la tua connessione. Verrai indirizzato a una pagina di accesso per il tuo server IdP. Accedi con le tue credenziali IdP. Dopo aver effettuato l'accesso, torna alla Console per abilitare la connessione.

    Quando si utilizza la Console in modalità limitata, copiare l'URL in una finestra del browser in incognito o in un browser separato per accedere al proprio IdP.

14. Nella Console, seleziona **Avanti** per rivedere la pagina di riepilogo.
15. Imposta le notifiche.

    Scegli tra sette giorni o 30 giorni. Il sistema invia notifiche di scadenza tramite e-mail e le mostra nella Console a tutti gli utenti con i seguenti ruoli: Super amministratore, Amministratore organizzazione, Amministratore federazione e Visualizzatore federazione.

16. Rivedi i dettagli della federazione e seleziona **Abilita federazione**.
17. Selezionare **Fine** per completare il processo.

Dopo aver abilitato la federazione, gli utenti accedono alla NetApp Console utilizzando le proprie credenziali aziendali.

Federare la NetApp Console con l'ID Microsoft Entra

Federati con il tuo provider IdP Microsoft Entra ID per abilitare l'accesso Single Sign-On (SSO) per NetApp Console. Ciò consente agli utenti di accedere utilizzando le proprie credenziali aziendali.

Ruoli richiesti

Il ruolo di amministratore della federazione è necessario per creare e gestire le federazioni. Il visualizzatore della Federazione può visualizzare la pagina della Federazione."Scopri di più sui ruoli di accesso."

Puoi federarti con il tuo IdP aziendale o con il sito di supporto NetApp . NetApp consiglia di scegliere l'una o l'altra opzione, ma non entrambe.

NetApp supporta solo SSO avviato dal provider di servizi (SP). Per prima cosa è necessario configurare il provider di identità in modo che consideri attendibile NetApp come fornitore di servizi. Quindi, è possibile creare una connessione nella Console che utilizzi la configurazione del provider di identità.

È possibile impostare una connessione federata con Microsoft Entra ID per abilitare l'accesso Single Sign-On (SSO) per la Console. Il processo prevede la configurazione del tuo ID Microsoft Entra in modo che consideri attendibile la Console come fornitore di servizi e quindi la creazione della connessione nella Console.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare **Federazione** per visualizzare la pagina **Federazioni**.
3. Selezionare **Configura nuova federazione**.

Dettagli del dominio

1. Inserisci i dettagli del tuo dominio:
   a. Scegli se vuoi utilizzare un dominio verificato o il tuo dominio di posta elettronica. Il dominio di posta elettronica è il dominio associato all'account con cui hai effettuato l'accesso.
   b. Inserisci il nome della federazione che stai configurando.
   c. Se scegli un dominio verificato, seleziona il dominio dall'elenco.
2. Selezionare **Avanti**.

Metodo di connessione

1. Per il metodo di connessione, seleziona **Provider** e poi seleziona **Microsoft Entra ID**.
2. Selezionare **Avanti**.

Istruzioni di configurazione

1. Configura il tuo ID Microsoft Entra per considerare NetApp attendibile come fornitore di servizi. Devi eseguire questo passaggio sul tuo server Microsoft Entra ID.
   a. Utilizzare i seguenti valori durante la registrazione dell'app Microsoft Entra ID per considerare attendibile la console:
      - Per l'URL di reindirizzamento, utilizzare `https://services.cloud.netapp.com`

- Per l'**URL di risposta**, usa `https://netapp-cloud-account.auth0.com/login/callback`

b. Crea un segreto client per la tua app Microsoft Entra ID. Per completare la federazione sarà necessario fornire l'ID client, il segreto client e il nome di dominio ID Entra.

2. Torna alla Console e seleziona **Avanti** per creare la connessione.

Crea connessione

1. Crea la connessione con Microsoft Entra ID
   a. Inserisci l'ID client e il segreto client creati nel passaggio precedente.
   b. Inserisci il nome di dominio dell'ID Microsoft Entra.
2. Seleziona **Crea connessione**. Il sistema crea la connessione in pochi secondi.

Testare e abilitare la connessione

1. Selezionare **Avanti**.
2. Seleziona **Test connessione** per testare la tua connessione. Verrai indirizzato a una pagina di accesso per il tuo server IdP. Accedi con le tue credenziali IdP. Dopo aver effettuato l'accesso, torna alla Console per abilitare la connessione.

   Quando si utilizza la Console in modalità limitata, copiare l'URL in una finestra del browser in incognito o in un browser separato per accedere al proprio IdP.

3. Nella Console, seleziona **Avanti** per rivedere la pagina di riepilogo.
4. Imposta le notifiche.

   Scegli tra sette giorni o 30 giorni. Il sistema invia notifiche di scadenza tramite e-mail e le mostra nella Console a tutti gli utenti con i seguenti ruoli: Super amministratore, Amministratore organizzazione, Amministratore federazione e Visualizzatore federazione.

5. Rivedi i dettagli della federazione e seleziona **Abilita federazione**.
6. Selezionare **Fine** per completare il processo.

Dopo aver abilitato la federazione, gli utenti accedono alla NetApp Console utilizzando le proprie credenziali aziendali.

Federare la NetApp Console con PingFederate

Federati con il tuo provider IdP PingFederate per abilitare l'accesso singolo (SSO) per la NetApp Console. Ciò consente agli utenti di accedere utilizzando le proprie credenziali aziendali.

Ruoli richiesti

Il ruolo di amministratore della federazione è necessario per creare e gestire le federazioni. Il visualizzatore della Federazione può visualizzare la pagina della Federazione."Scopri di più sui ruoli di accesso."

Puoi federarti con il tuo IdP aziendale o con il sito di supporto NetApp . NetApp consiglia di scegliere l'una o l'altra opzione, ma non entrambe.

NetApp supporta solo SSO avviato dal provider di servizi (SP). Per prima cosa è necessario configurare il provider di identità in modo che consideri attendibile NetApp come fornitore di servizi. Quindi, è possibile creare una connessione nella Console che utilizzi la configurazione del provider di identità.

È possibile impostare una connessione federata con PingFederate per abilitare l'accesso singolo (SSO) per la Console. Il processo prevede la configurazione del server PingFederate in modo che consideri attendibile la Console come fornitore di servizi e quindi la creazione della connessione nella Console.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare **Federazione** per visualizzare la pagina **Federazioni**.
3. Selezionare **Configura nuova federazione**.
4. Inserisci i dettagli del tuo dominio:
   a. Scegli se vuoi utilizzare un dominio verificato o il tuo dominio di posta elettronica. Il dominio di posta elettronica è il dominio associato all'account con cui hai effettuato l'accesso.
   b. Inserisci il nome della federazione che stai configurando.
   c. Se scegli un dominio verificato, seleziona il dominio dall'elenco.
5. Selezionare **Avanti**.
6. Per il metodo di connessione, seleziona **Provider** e poi seleziona **PingFederate**.
7. Selezionare **Avanti**.
8. Configura il tuo server PingFederate in modo che consideri NetApp affidabile come fornitore di servizi. Devi eseguire questo passaggio sul tuo server PingFederate.
   a. Utilizzare i seguenti valori quando si configura PingFederate per considerare attendibile la NetApp Console:
      - Per l'URL di risposta o l'URL del servizio consumatori di asserzione (ACS), utilizzare `https://netapp-cloud-account.auth0.com/login/callback`
      - Per l'URL di disconnessione, utilizzare `https://netapp-cloud-account.auth0.com/logout`
      - Per **ID pubblico/entità**, utilizzare `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` dove <fed-domain-name-pingfederate> è il nome di dominio della federazione. Ad esempio, se il tuo dominio è `example.com` , l'ID Pubblico/Entità sarebbe `urn:auth0:netappcloud-account:fed-example-com-pingfederate` .
   b. Copia l'URL del server PingFederate. Questo URL sarà necessario quando si crea la connessione nella Console.
   c. Scarica il certificato X.509 dal tuo server PingFederate. Deve essere in formato PEM codificato in Base64 (.pem, .crt, .cer).
9. Torna alla Console e seleziona **Avanti** per creare la connessione.
10. Crea la connessione con PingFederate
    a. Inserisci l'URL del server PingFederate che hai copiato nel passaggio precedente.
    b. Carica il certificato di firma X.509. Il certificato deve essere in formato PEM, CER o CRT.
11. Seleziona **Crea connessione**. Il sistema crea la connessione in pochi secondi.
12. Selezionare **Avanti**.
13. Seleziona **Test connessione** per testare la tua connessione. Verrai indirizzato a una pagina di accesso

per il tuo server IdP. Accedi con le tue credenziali IdP. Dopo aver effettuato l'accesso, torna alla Console per abilitare la connessione.

> Quando si utilizza la Console in modalità limitata, copiare l'URL in una finestra del browser in incognito o in un browser separato per accedere al proprio IdP.

14. Nella Console, seleziona **Avanti** per rivedere la pagina di riepilogo.
15. Imposta le notifiche.

    Scegli tra sette giorni o 30 giorni. Il sistema invia notifiche di scadenza tramite e-mail e le mostra nella Console a tutti gli utenti con i seguenti ruoli: Super amministratore, Amministratore organizzazione, Amministratore federazione e Visualizzatore federazione.

16. Rivedi i dettagli della federazione e seleziona **Abilita federazione**.
17. Selezionare **Fine** per completare il processo.

Dopo aver abilitato la federazione, gli utenti accedono alla NetApp Console utilizzando le proprie credenziali aziendali.

Federare con un provider di identità SAML

Federati con il tuo provider IdP SAML 2.0 per abilitare l'accesso Single Sign-On (SSO) per la console NEtApp. Ciò consente agli utenti di accedere utilizzando le proprie credenziali aziendali.

Ruolo richiesto

Il ruolo di amministratore della federazione è necessario per creare e gestire le federazioni. Il visualizzatore della Federazione può visualizzare la pagina della Federazione."Scopri di più sui ruoli di accesso."

> Puoi federarti con il tuo IdP aziendale o con il sito di supporto NetApp . Non è possibile federarsi con entrambi.

NetApp supporta solo SSO avviato dal provider di servizi (SP). Per prima cosa è necessario configurare il provider di identità in modo che consideri attendibile NetApp come fornitore di servizi. Quindi, è possibile creare una connessione nella Console che utilizzi la configurazione del provider di identità.

È possibile impostare una connessione federata con il provider SAML 2.0 per abilitare l'accesso Single Sign-On (SSO) per la Console. Il processo prevede la configurazione del provider in modo che consideri attendibile NetApp come fornitore di servizi e la successiva creazione della connessione nella Console.

Passi

1. Selezionare **Amministrazione > Identità e accesso**.
2. Selezionare **Federazione** per visualizzare la pagina **Federazioni**.
3. Selezionare **Configura nuova federazione**.
4. Inserisci i dettagli del tuo dominio:
   a. Scegli se vuoi utilizzare un dominio verificato o il tuo dominio di posta elettronica. Il dominio di posta elettronica è il dominio associato all'account con cui hai effettuato l'accesso.
   b. Inserisci il nome della federazione che stai configurando.

c. Se scegli un dominio verificato, seleziona il dominio dall'elenco.

5. Selezionare **Avanti**.
6. Per il metodo di connessione, seleziona **Protocollo** e poi seleziona **Provider di identità SAML**.
7. Selezionare **Avanti**.
8. Configura il tuo provider di identità SAML in modo che consideri attendibile NetApp come fornitore di servizi. È necessario eseguire questo passaggio sul server del provider SAML.
   a. Assicurati che il tuo IdP abbia l'attributo `email` impostato sull'indirizzo email dell'utente. Ciò è necessario affinché la Console identifichi correttamente gli utenti:

```
<saml:AttributeStatement
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        <saml:AttributeValue
xsi:type="xs:string">email@domain.com</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

1. Utilizzare i seguenti valori quando si registra l'applicazione SAML con la Console:
   - Per l'URL di risposta o l'URL del servizio consumatori di asserzione (ACS), utilizzare `https://netapp-cloud-account.auth0.com/login/callback`
   - Per l'URL di disconnessione, utilizzare `https://netapp-cloud-account.auth0.com/logout`
   - Per **ID pubblico/entità**, utilizzare `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` dove <fed-domain-name-saml> è il nome di dominio che si desidera utilizzare per la federazione. Ad esempio, se il tuo dominio è `example.com` , l'ID Pubblico/Entità sarebbe `urn:auth0:netapp-cloud-account:fed-example-com-samlp` .
2. Dopo aver creato il trust, copia i seguenti valori dal server del tuo provider SAML:
   - URL di accesso
   - URL di disconnessione (facoltativo)
3. Scarica il certificato X.509 dal server del tuo provider SAML. Deve essere in formato PEM, CER o CRT.
   a. Torna alla Console e seleziona **Avanti** per creare la connessione.
   b. Creare la connessione con SAML.
4. Inserisci l'**URL di accesso** del tuo server SAML.
5. Carica il certificato X.509 che hai scaricato dal server del tuo provider SAML.
6. Facoltativamente, inserisci l'**URL di disconnessione** del tuo server SAML.
   a. Seleziona **Crea connessione**. Il sistema crea la connessione in pochi secondi.
   b. Selezionare **Avanti**.
   c. Seleziona **Test connessione** per testare la tua connessione. Verrai indirizzato a una pagina di accesso per il tuo server IdP. Accedi con le tue credenziali IdP. Dopo aver effettuato l'accesso, torna

alla Console per abilitare la connessione.

> Quando si utilizza la Console in modalità limitata, copiare l'URL in una finestra del browser in incognito o in un browser separato per accedere al proprio IdP.

d. Nella Console, seleziona **Avanti** per rivedere la pagina di riepilogo.
e. Imposta le notifiche.

   Scegli tra sette giorni o 30 giorni. Il sistema invia notifiche di scadenza tramite e-mail e le mostra nella Console a tutti gli utenti con i seguenti ruoli: Super amministratore, Amministratore organizzazione, Amministratore federazione e Visualizzatore federazione.

f. Rivedi i dettagli della federazione e seleziona **Abilita federazione**.
g. Selezionare **Fine** per completare il processo.

Dopo aver abilitato la federazione, gli utenti accedono alla NetApp Console utilizzando le proprie credenziali aziendali.

Informazioni sul copyright

Informazioni sul marchio commerciale