Configurare le federazioni

BlueXP setup and administration

NetApp
August 18, 2025

This PDF was generated from https://docs.netapp.com/it-it/bluexp-setup-admin/task-federation-adfs.html on August 18, 2025. Always check docs.netapp.com for the latest.

Sommario

Configurare le federazioni

Federare BlueXP con Active Directory Federation Services (AD FS)

Federa i tuoi Servizi Federazione di Active Directory (AD FS) con BlueXP per abilitare il Single Sign-On (SSO) per BlueXP. Questo consente agli utenti di accedere a BlueXP utilizzando le proprie credenziali aziendali.

Ruoli richiesti

Per creare e gestire le federazioni è necessario un amministratore dell'organizzazione o della federazione. 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'uno o l'altro, ma non entrambi.

NetApp supporta solo l'SSO avviato dal provider di servizi (SP). Innanzitutto, configura il provider di identità affinché consideri attendibile BlueXP come provider di servizi. Quindi, crea una connessione in BlueXP 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 BlueXP. Il processo prevede la configurazione di AD FS in modo che consideri attendibile BlueXP come provider di servizi e la successiva creazione della connessione in BlueXP.

Prima di iniziare

- È richiesto un account IdP con privilegi amministrativi. Contatta l'amministratore del tuo IdP per completare la procedura.
- Identifica il dominio che desideri utilizzare per la federazione. Puoi utilizzare il tuo dominio email o un dominio diverso di tua proprietà. Se desideri utilizzare un dominio diverso dal tuo dominio email, devi prima verificarlo in BlueXP. Puoi farlo seguendo i passaggi descritti nella sezione "Verifica il tuo dominio su BlueXP" argomento.

Fasi

1. Nella parte superiore destra della console di BlueXP , selezionare > **Gestione identità e accessi**.
2. Selezionare la scheda **Federazione**.
3. Selezionare **Configura nuova federazione**.
4. Inserisci i dettagli del tuo dominio:
    a. Scegli se desideri utilizzare un dominio verificato o il tuo dominio email. Il dominio email 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 tra relying party nel tuo server AD FS. Puoi utilizzare PowerShell o configurarlo manualmente sul tuo server AD FS. Consulta la documentazione di AD FS per dettagli su come creare un trust tra relying party.

   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 BlueXP 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 server AD FS o scarica il file dei metadati della federazione. Questo URL o file sarà necessario per completare la connessione in BlueXP.

   NetApp consiglia di utilizzare l'URL dei metadati per consentire a BlueXP di recuperare automaticamente la configurazione AD FS più recente. Se scarichi il file dei metadati della federazione, dovrai aggiornarlo manualmente in BlueXP ogni volta che si verificano modifiche alla configurazione AD FS.

9. Ritorna a BlueXP e seleziona **Avanti** per creare la connessione.
10. Creare la connessione con AD FS.

    a. Immetti l'URL di AD FS copiato dal server AD FS nel passaggio precedente oppure carica il file di metadati della 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 per completare il test e torna a BlueXP per abilitare la connessione.
14. Selezionare **Avanti**.
15. Nella pagina **Abilita federazione**, rivedi i dettagli della federazione e poi seleziona **Abilita federazione**.
16. Selezionare **Fine** per completare il processo.

Dopo aver abilitato la federazione, gli utenti potranno accedere a BlueXP utilizzando le proprie credenziali aziendali.

Federare BlueXP con Microsoft Entra ID

Federati con il tuo provider IdP Microsoft Entra ID per abilitare il Single Sign-On (SSO) per BlueXP. Questo consente agli utenti di accedere utilizzando le proprie credenziali

aziendali.

Ruoli richiesti

Per creare e gestire le federazioni è necessario un amministratore dell'organizzazione o della federazione. 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'uno o l'altro, ma non entrambi.

NetApp supporta solo l'SSO avviato dal provider di servizi (SP). È necessario innanzitutto configurare il provider di identità affinché consideri NetApp attendibile come provider di servizi. Successivamente, è possibile creare una connessione in BlueXP che utilizzi la configurazione del provider di identità.

È possibile configurare una connessione federata con l'ID Microsoft Entra per abilitare l'accesso Single Sign-On (SSO) per BlueXP. La procedura prevede la configurazione dell'ID Microsoft Entra per considerare BlueXP attendibile come fornitore di servizi e la successiva creazione della connessione in BlueXP.

Prima di iniziare

- È richiesto un account IdP con privilegi amministrativi. Contatta l'amministratore del tuo IdP per completare la procedura.
- Identifica il dominio che desideri utilizzare per la federazione. Puoi utilizzare il tuo dominio email o un dominio diverso di tua proprietà. Se desideri utilizzare un dominio diverso dal tuo dominio email, devi prima verificarlo in BlueXP. Puoi farlo seguendo i passaggi descritti nella sezione "Verifica il tuo dominio su BlueXP" argomento.

Fasi

1. Nella parte superiore destra della console di BlueXP , selezionare > **Gestione identità e accessi**.
2. Selezionare la scheda **Federazione**.
3. Selezionare **Configura nuova federazione**.

Dettagli del dominio

1. Inserisci i dettagli del tuo dominio:
   a. Scegli se desideri utilizzare un dominio verificato o il tuo dominio email. Il dominio email 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 server del tuo ID Microsoft Entra.

a. Utilizza i seguenti valori quando registri la tua app Microsoft Entra ID per considerare attendibile BlueXP:
   - 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 client secret per la tua app Microsoft Entra ID. Dovrai fornire il client ID, il client secret e il nome di dominio dell'ID Entra per completare la federazione.

2. Ritorna a BlueXP 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 creerà 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 per completare il test e torna a BlueXP per abilitare la connessione.
3. Selezionare **Avanti**.
4. Nella pagina **Abilita federazione**, rivedi i dettagli della federazione e poi seleziona **Abilita federazione**.
5. Selezionare **Fine** per completare il processo.

Dopo aver abilitato la federazione, gli utenti potranno accedere a BlueXP utilizzando le proprie credenziali aziendali.

Federate BlueXP con PingFederate

Federati con il tuo provider IdP PingFederate per abilitare il Single Sign-On (SSO) per BlueXP. Questo consente agli utenti di accedere utilizzando le proprie credenziali aziendali.

Ruoli richiesti

Per creare e gestire le federazioni è necessario un amministratore dell'organizzazione o della federazione. 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'uno o l'altro, ma non entrambi.

NetApp supporta solo l'SSO avviato dal provider di servizi (SP). È necessario innanzitutto configurare il provider di identità affinché consideri NetApp attendibile come provider di servizi. Successivamente, è possibile creare una connessione in BlueXP che utilizzi la configurazione del provider di identità.

È possibile configurare una connessione federata con PingFederate per abilitare il Single Sign-On (SSO) per

BlueXP. Il processo prevede la configurazione del server PingFederate in modo che consideri BlueXP attendibile come provider di servizi e la successiva creazione della connessione in BlueXP.

Prima di iniziare

- È richiesto un account IdP con privilegi amministrativi. Contatta l'amministratore del tuo IdP per completare la procedura.
- Identifica il dominio che desideri utilizzare per la federazione. Puoi utilizzare il tuo dominio email o un dominio diverso di tua proprietà. Se desideri utilizzare un dominio diverso dal tuo dominio email, devi prima verificarlo in BlueXP. Puoi farlo seguendo i passaggi descritti nella sezione "Verifica il tuo dominio su BlueXP" argomento.

Fasi

1. Nella parte superiore destra della console di BlueXP , selezionare > **Gestione identità e accessi**.
2. Selezionare la scheda **Federazione**.
3. Selezionare **Configura nuova federazione**.
4. Inserisci i dettagli del tuo dominio:
   a. Scegli se desideri utilizzare un dominio verificato o il tuo dominio email. Il dominio email 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 attendibile come fornitore di servizi. Devi eseguire questo passaggio sul tuo server PingFederate.
   a. Utilizzare i seguenti valori quando si configura PingFederate per considerare attendibile BlueXP:
      - 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 del pubblico/entità sarebbe `urn:auth0:netappcloud-account:fed-example-com-pingfederate` .
   b. Copia l'URL del server PingFederate. Questo URL ti servirà per creare la connessione in BlueXP.
   c. Scarica il certificato X.509 dal tuo server PingFederate. Deve essere in formato PEM con codifica Base64 (.pem, .crt, .cer).
9. Ritorna a BlueXP e seleziona **Avanti** per creare la connessione.
10. Crea la connessione con PingFederate
    a. Inserisci l'URL del server PingFederate 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 creerà 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 per completare il test e torna a BlueXP per abilitare la connessione.
14. Selezionare **Avanti**.
15. Nella pagina **Abilita federazione**, rivedi i dettagli della federazione e poi seleziona **Abilita federazione**.
16. Selezionare **Fine** per completare il processo.

Dopo aver abilitato la federazione, gli utenti potranno accedere a BlueXP utilizzando le proprie credenziali aziendali.

Federarsi con un fornitore di identità SAML

Federati con il tuo provider di identità SAML 2.0 per abilitare il Single Sign-On (SSO) per BlueXP. Questo consente agli utenti di accedere utilizzando le proprie credenziali aziendali.

Ruolo richiesto

Amministratore dell'organizzazione. "Scopri di più sui ruoli di accesso."

Puoi federarti con il tuo IdP aziendale o con il sito di supporto NetApp . Non puoi federarti con entrambi.

NetApp supporta solo l'SSO avviato dal provider di servizi (SP). È necessario innanzitutto configurare il provider di identità affinché consideri NetApp attendibile come provider di servizi. Successivamente, è possibile creare una connessione in BlueXP che utilizzi la configurazione del provider di identità.

Puoi configurare una connessione federata con il tuo provider SAML 2.0 per abilitare il Single Sign-On (SSO) per BlueXP. Il processo prevede la configurazione del provider affinché consideri NetApp attendibile come fornitore di servizi e la successiva creazione della connessione in BlueXP.

Prima di iniziare

- È richiesto un account IdP con privilegi amministrativi. Contatta l'amministratore del tuo IdP per completare la procedura.
- Identifica il dominio che desideri utilizzare per la federazione. Puoi utilizzare il tuo dominio email o un dominio diverso di tua proprietà. Se desideri utilizzare un dominio diverso dal tuo dominio email, devi prima verificarlo in BlueXP. Puoi farlo seguendo i passaggi descritti nella sezione "Verifica il tuo dominio su BlueXP" argomento.

Fasi

1. Nella parte superiore destra della console di BlueXP , selezionare > **Gestione identità e accessi**.
2. Selezionare la scheda **Federazione**.
3. Selezionare **Configura nuova federazione**.
4. Inserisci i dettagli del tuo dominio:
    a. Scegli se desideri utilizzare un dominio verificato o il tuo dominio email. Il dominio email 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 NetApp attendibile come fornitore di servizi. Devi eseguire questo passaggio sul server del tuo provider SAML.
   a. Assicurati che il tuo IdP abbia l'attributo `email` Impostato sull'indirizzo email dell'utente. Questo è necessario affinché BlueXP 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>
```

   b. Utilizzare i seguenti valori durante la registrazione dell'applicazione SAML con BlueXP:
      - 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 dominio è `example.com` , l'ID del pubblico/entità sarebbe `urn:auth0:netapp-cloud-account:fed-example-com-samlp` .
   c. Dopo aver creato il trust, copia i seguenti valori dal server del tuo provider SAML:
      - URL di accesso
      - URL di disconnessione (facoltativo)
   d. Scarica il certificato X.509 dal server del tuo provider SAML. Deve essere in formato PEM, CER o CRT.
9. Ritorna a BlueXP e seleziona **Avanti** per creare la connessione.
10. Creare la connessione con SAML.
    a. Inserisci l'**URL di accesso** del tuo server SAML.
    b. Carica il certificato X.509 che hai scaricato dal server del tuo provider SAML.
    c. Facoltativamente, inserisci l'**URL di disconnessione** del tuo server SAML.
11. Seleziona **Crea connessione**. Il sistema creerà 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 per completare il test e torna a BlueXP per abilitare la connessione.
14. Selezionare **Avanti**.
15. Nella pagina **Abilita federazione**, rivedi i dettagli della federazione e poi seleziona **Abilita federazione**.
16. Selezionare **Fine** per completare il processo.

Dopo aver abilitato la federazione, gli utenti potranno accedere a BlueXP utilizzando le proprie credenziali aziendali.

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.