Configura SSO FMC con Azure come provider di identità

Sommario

Introduzione

In questo documento viene descritto come configurare Firepower Management Center (FMC) Single Sign-On (SSO) con Azure come provider di identità (idP).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Informazioni di base su Firepower Management Center
- Conoscenze base di Single Sign-On

Componenti usati

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

- Cisco Firepower Management Center (FMC) versione 6.7.0
- Azure - IdP

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

Terminologie SAML

SAML (Security Assertion Markup Language) è il protocollo sottostante che rende possibile l'SSO. Un'azienda gestisce una singola pagina di accesso, dietro di essa un archivio di identità e varie regole di autenticazione. Può facilmente configurare qualsiasi app Web che supporti SAML, che consente di accedere a tutte le applicazioni Web. Offre inoltre il vantaggio della sicurezza non costringendo gli utenti a mantenere (e potenzialmente riutilizzare) le password per ogni app Web a cui hanno bisogno di accedere, né esponendo le password a quelle app Web.

La configurazione per SAML deve essere eseguita in due punti: a IdP e a SP. È necessario configurare l'IdP in modo che sappia dove e come inviare gli utenti quando desiderano accedere a uno specifico SP. È necessario configurare l'SP in modo che sia in grado di considerare attendibili le asserzioni SAML firmate dall'IdP.

Definizione di alcuni termini fondamentali per SAML:

- Provider di identità (IdP): lo strumento o il servizio software (spesso visualizzato da una pagina di accesso e/o da un dashboard) che esegue l'autenticazione; controlla nome utente e password, verifica lo stato dell'account, richiama due fattori e altre autenticazioni.

- Provider di servizi (SP) - L'applicazione Web a cui l'utente tenta di accedere.

- Asserzione SAML - Messaggio che asserisce l'identità di un utente e spesso altri attributi, inviato tramite HTTP tramite reindirizzamenti del browser

Configurazione IdP

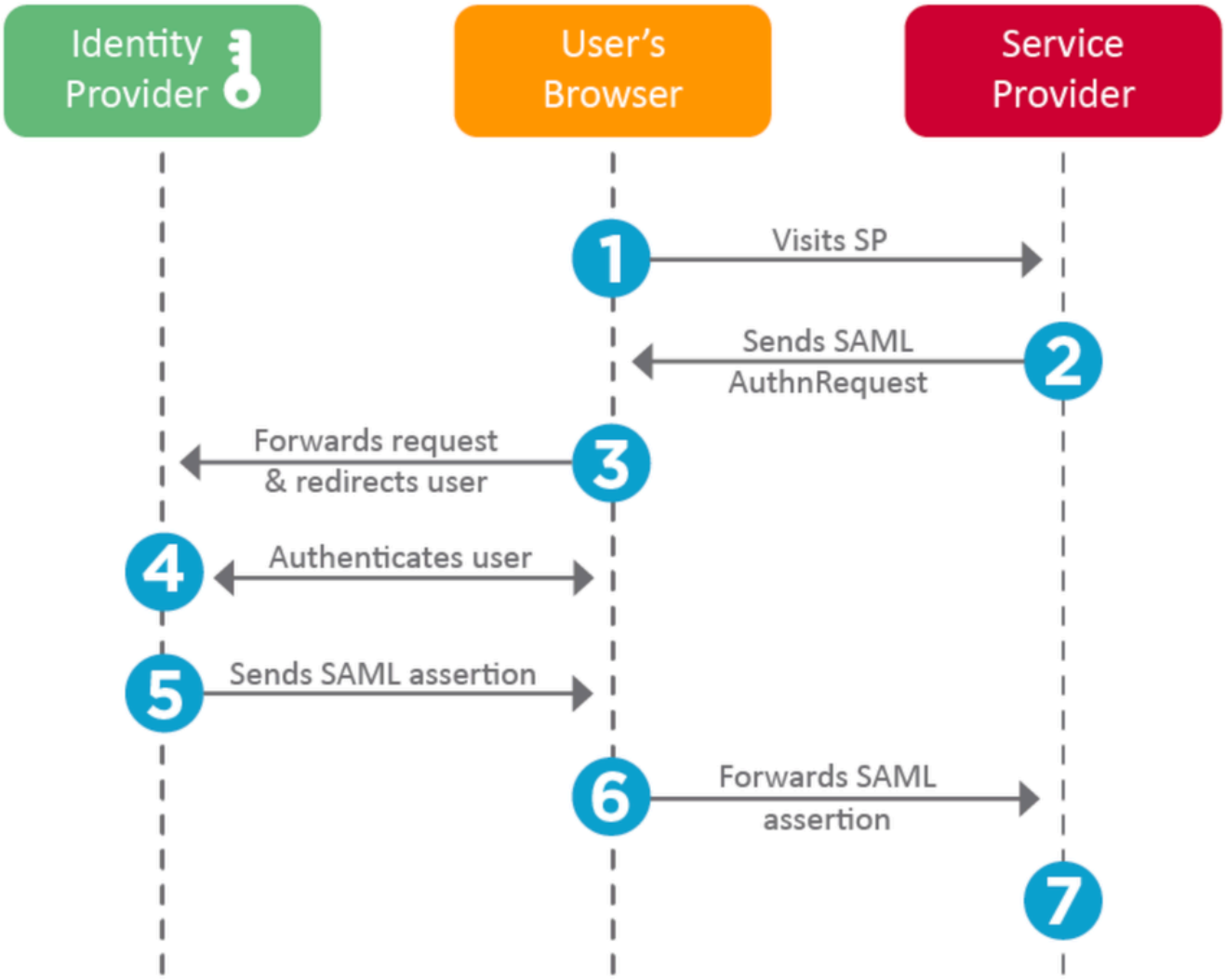
Le specifiche per un'asserzione SAML, il relativo contenuto e la modalità di formattazione vengono fornite dall'SP e impostate sull'IdP.

- EntityID: nome univoco globale per l'SP. I formati variano, ma è sempre più comune vedere questo valore formattato come URL.
  Esempio: https://<FQDN-or-IPaddress>/saml/metadata

- Assertion Consumer Service (ACS) Validator: misura di sicurezza sotto forma di espressione regolare (regex) che assicura che l'asserzione SAML venga inviata all'ACS corretto. Questa operazione viene eseguita solo durante gli accessi avviati da SP in cui la richiesta SAML contiene un percorso ACS, quindi questo validator ACS garantisce che il percorso ACS fornito dalla richiesta SAML sia legittimo.
  Esempio: https://<FQDN-or-IPaddress>/saml/acs

- Attributi: il numero e il formato degli attributi possono variare notevolmente. In genere è presente almeno un attributo, nameID, che in genere corrisponde al nome utente dell'utente che tenta di eseguire l'accesso.

- Algoritmo della firma SAML - SHA-1 o SHA-256. Meno comunemente SHA-384 o SHA-512. Questo algoritmo viene utilizzato insieme al certificato X.509.



Configurazione SP

Nella parte opposta della sezione precedente, questa sezione parla delle informazioni fornite dall'IdP e impostate sull'SP.

- URL autorità emittente: identificatore univoco del provider di identità. Formattato come un

URL contenente informazioni sull'IdP in modo che l'SP possa convalidare che le asserzioni SAML che riceve siano emesse dall'IdP corretto.

- URL di accesso endpoint SSO SAML/provider di servizi: endpoint IdP che avvia l'autenticazione quando viene reindirizzato qui dall'SP con una richiesta SAML.
  Esempio: https://login.microsoftonline.com/023480840129412-824812/saml2
- Endpoint SLO (Single Log-Out) SAML: endpoint IdP che chiude la sessione IdP quando viene reindirizzato qui dall'SP, in genere dopo la disconnessione.
  Esempio: https://access.wristbandtent.com/logout

SAML su FMC

La funzionalità SSO in FMC è stata introdotta a partire dalla versione 6.7. La nuova funzionalità semplifica l'autorizzazione di FMC (RBAC, FMC Authorization), poiché associa le informazioni esistenti ai ruoli di FMC. Si applica a tutti gli utenti dell'interfaccia utente e ai ruoli di FMC. Per il momento, supporta la specifica SAML 2.0 e questi IDP supportati

- OKTA
- OneLogin
- IDping
- Azure AD
- Altri (qualsiasi IDP conforme a SAML 2.0)

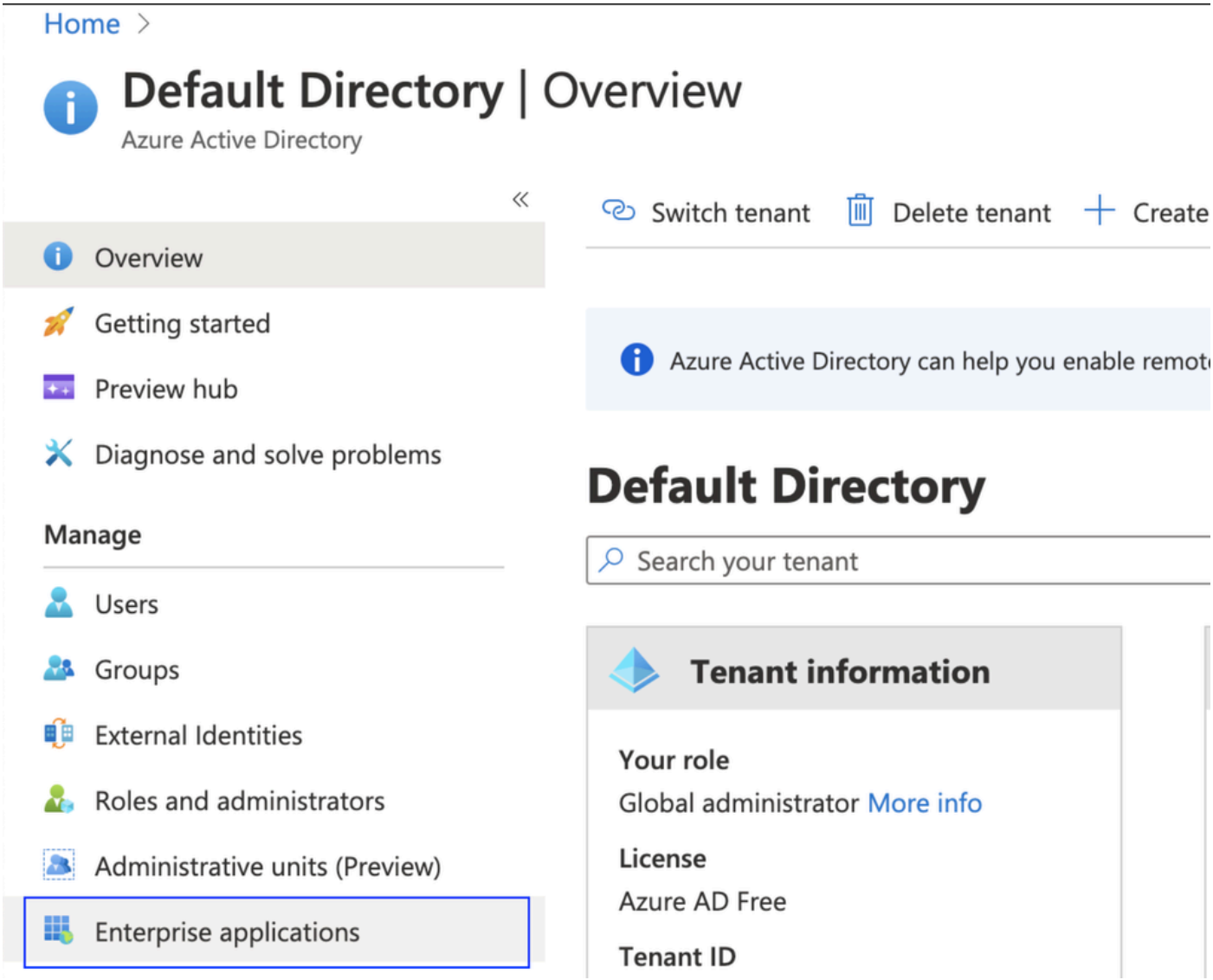
Limitazioni e avvertenze

- SSO può essere configurato solo per il dominio globale.
- I FMC in Coppia HA richiedono una configurazione individuale.
- Solo gli amministratori locali/AD possono configurare Single Sign-On.
- L'SSO avviato da Idp non è supportato.

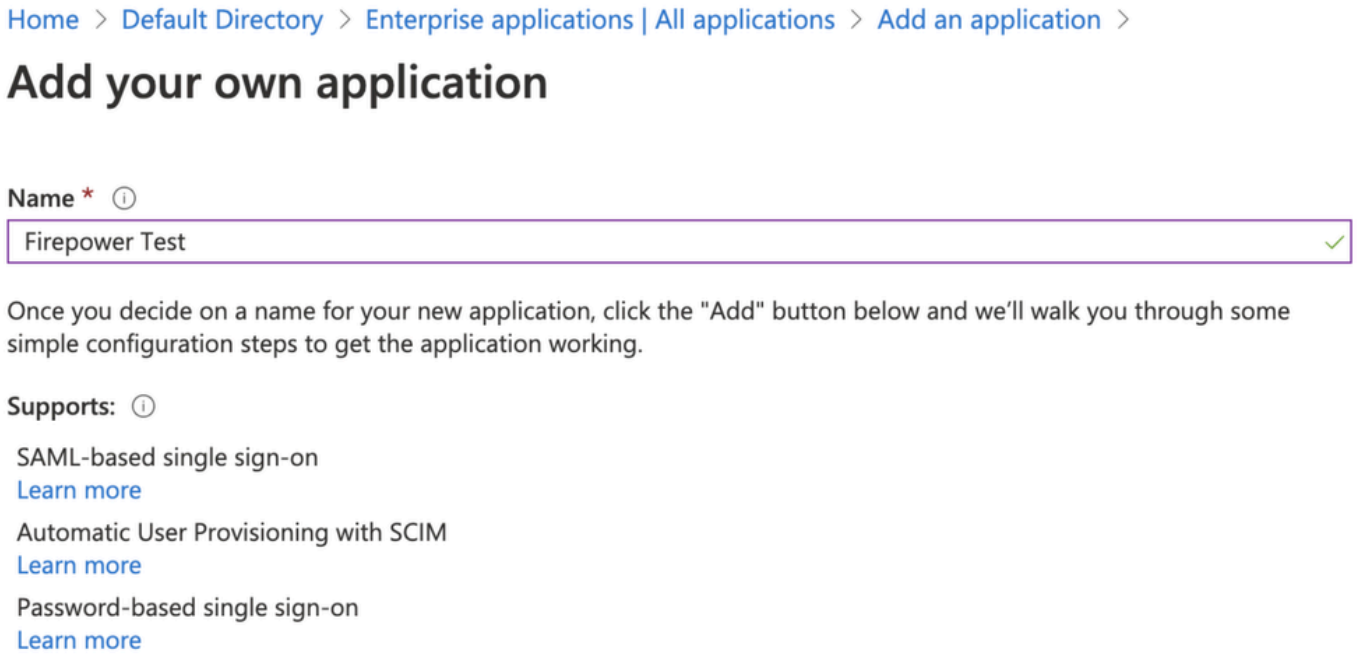
Configurazione

Configurazione sul provider di identità

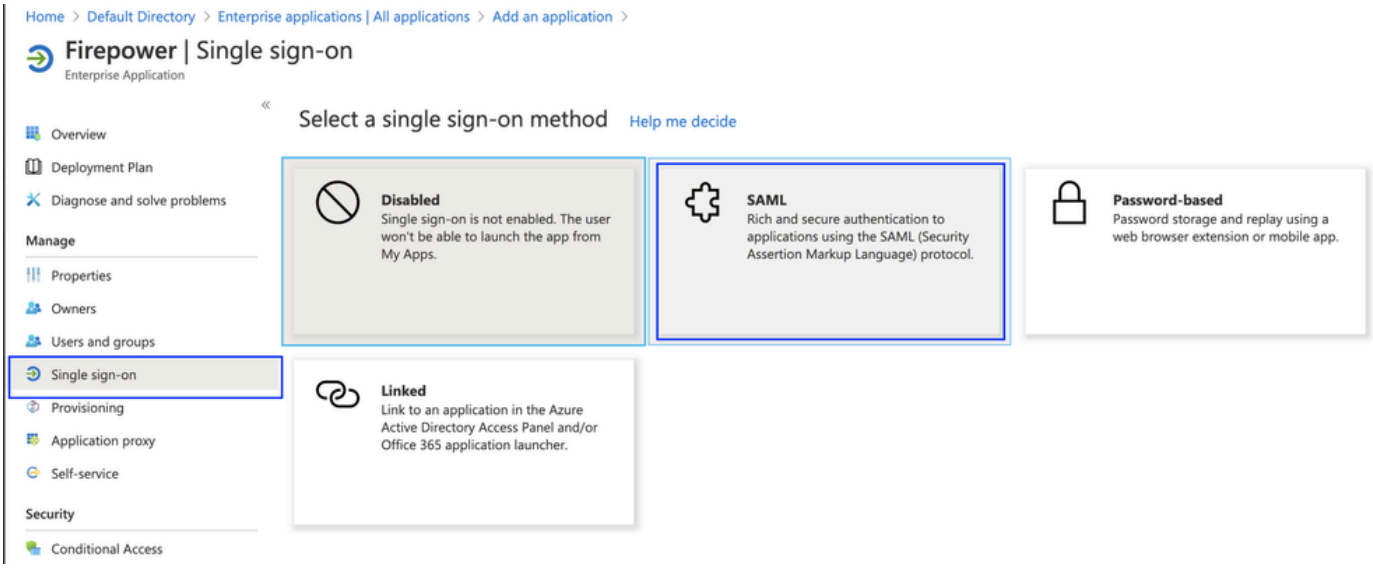
Passaggio 1. Accedere a Microsoft Azure. Passare ad Azure Active Directory > Applicazione enterprise.



- Passaggio 2. Crea nuova applicazione in Applicazione diversa da Raccolta, come mostrato nell'immagine:



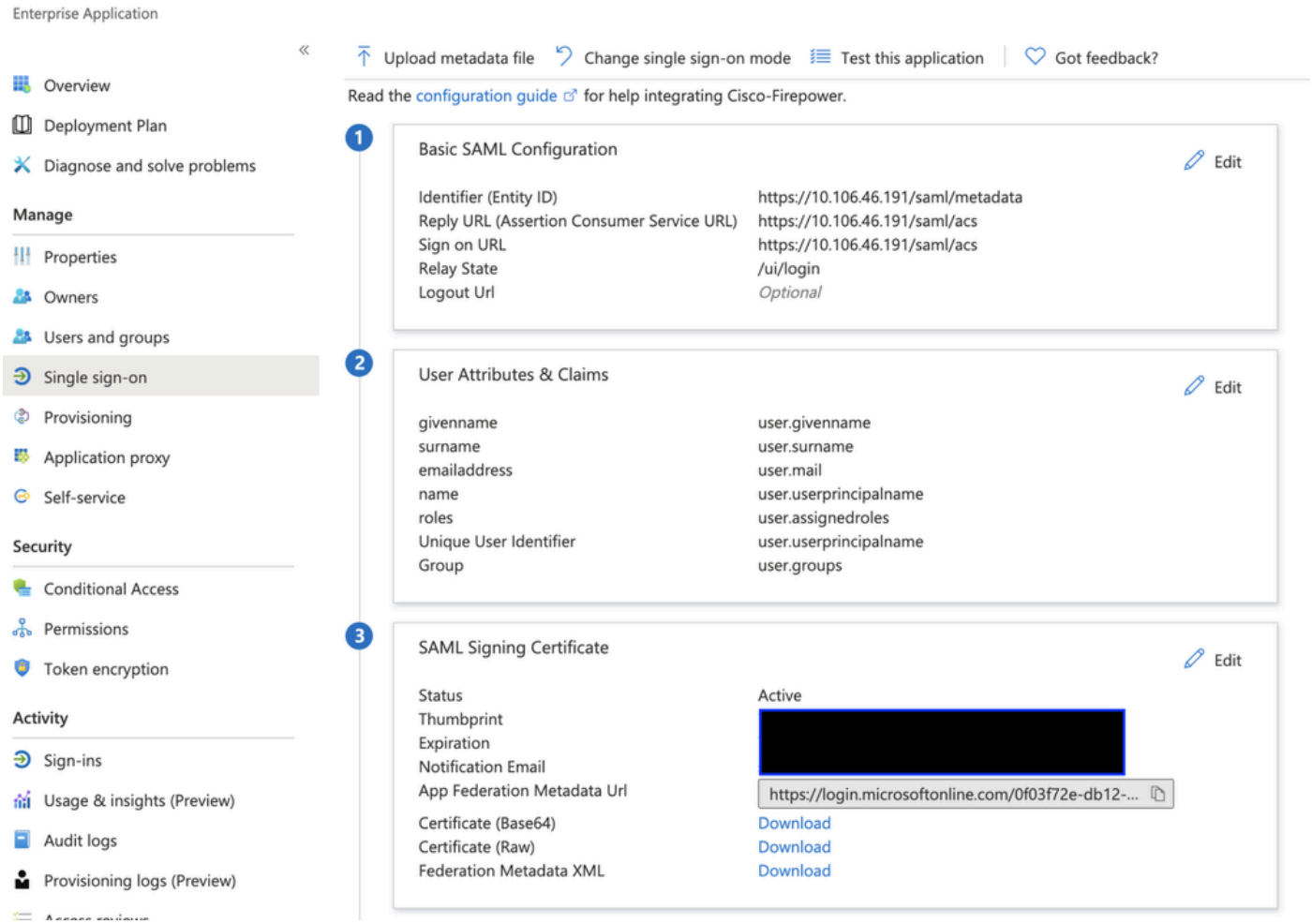
Passaggio 3. Modificare l'applicazione creata e passare a Imposta Single Sign-On > SAML, come mostrato nell'immagine.



Passaggio 4. Modificare la configurazione SAML di base e fornire i dettagli FMC:

- URL FMC: https://<FMC-FQDN-or-IPaddress>
- Identificatore (ID entità): https://<FMC-FQDN-or-IPaddress>/saml/metadata
- URL risposta: https://<FMC-FQDN-or-IPaddress>/saml/acs
- URL di accesso: https://<FMC-QDN-or-IPaddress>/saml/acs

- RelayState:/ui/login

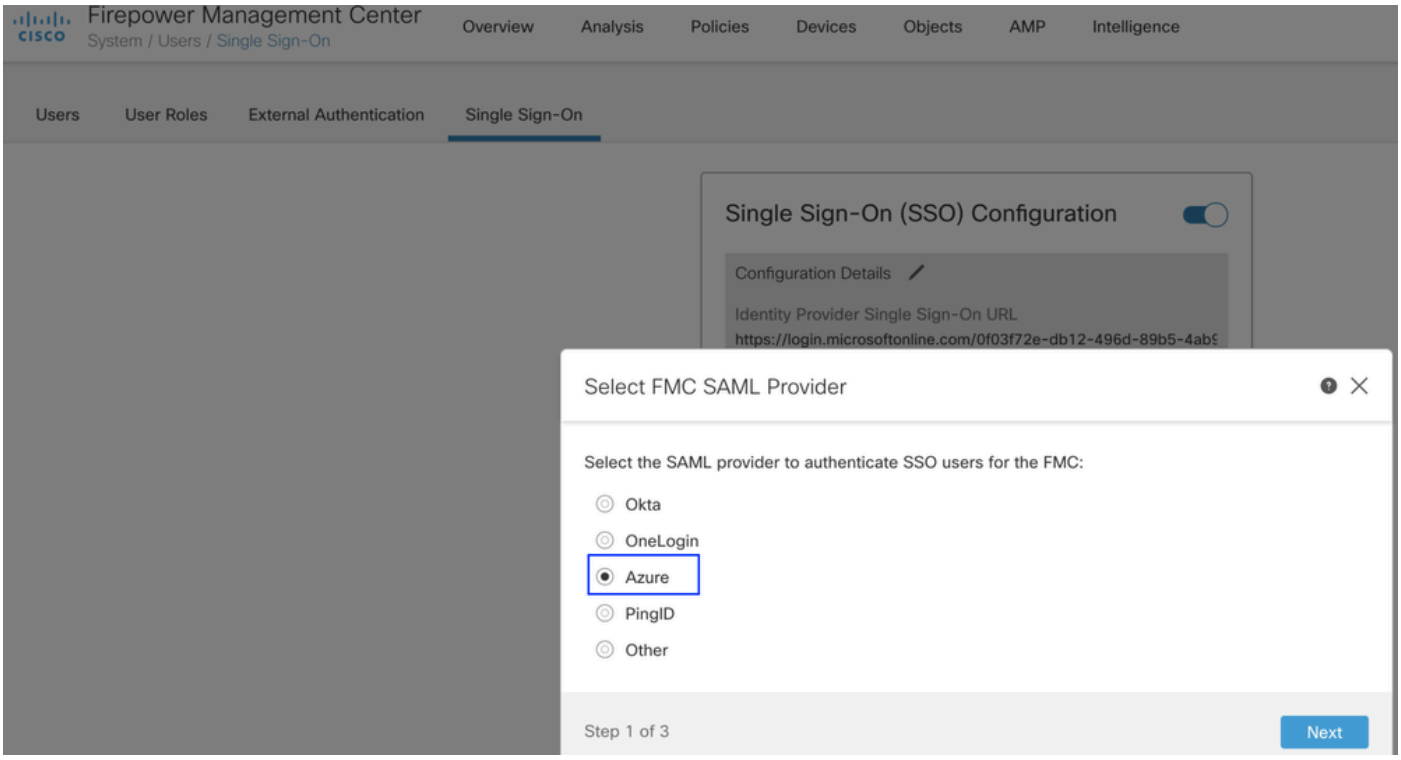


Mantenere il resto come predefinito: questo argomento viene ulteriormente descritto per l'accesso basato sui ruoli.

Indica la fine della configurazione del provider di identità. Scaricare il file XML dei metadati federativi utilizzato per la configurazione di FMC.

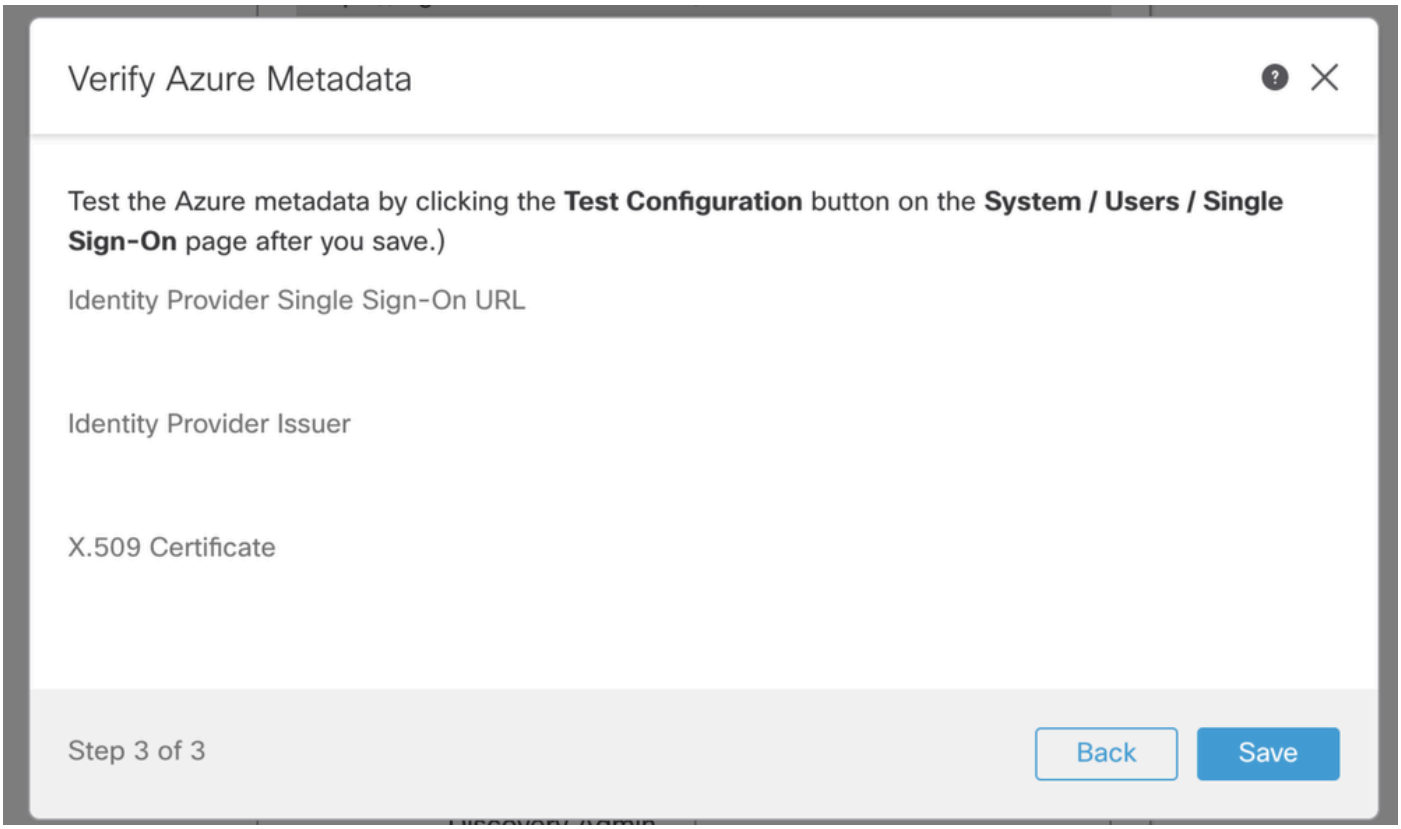
Configurazione su Firepower Management Center

Passaggio 1. Accedere a FMC, selezionare Impostazioni > Utenti > Single Sign-On e Abilita SSO. Selezionare Azure come provider.



Passaggio 2. Caricare qui il file XML scaricato da Azure. Vengono automaticamente inseriti tutti i dettagli necessari.

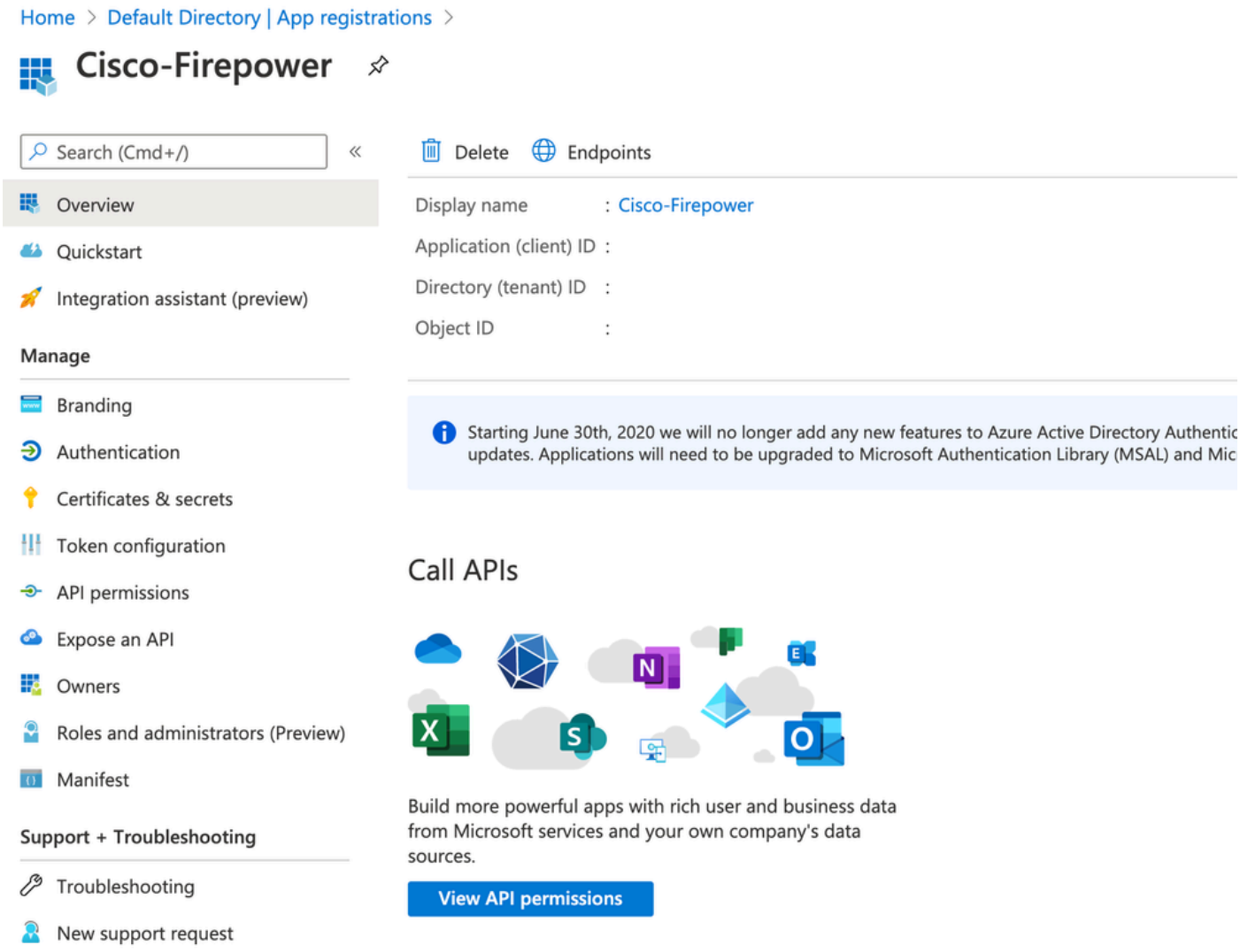
Passaggio 3. Verificare la configurazione e fare clic su Save (Salva), come mostrato nell'immagine.



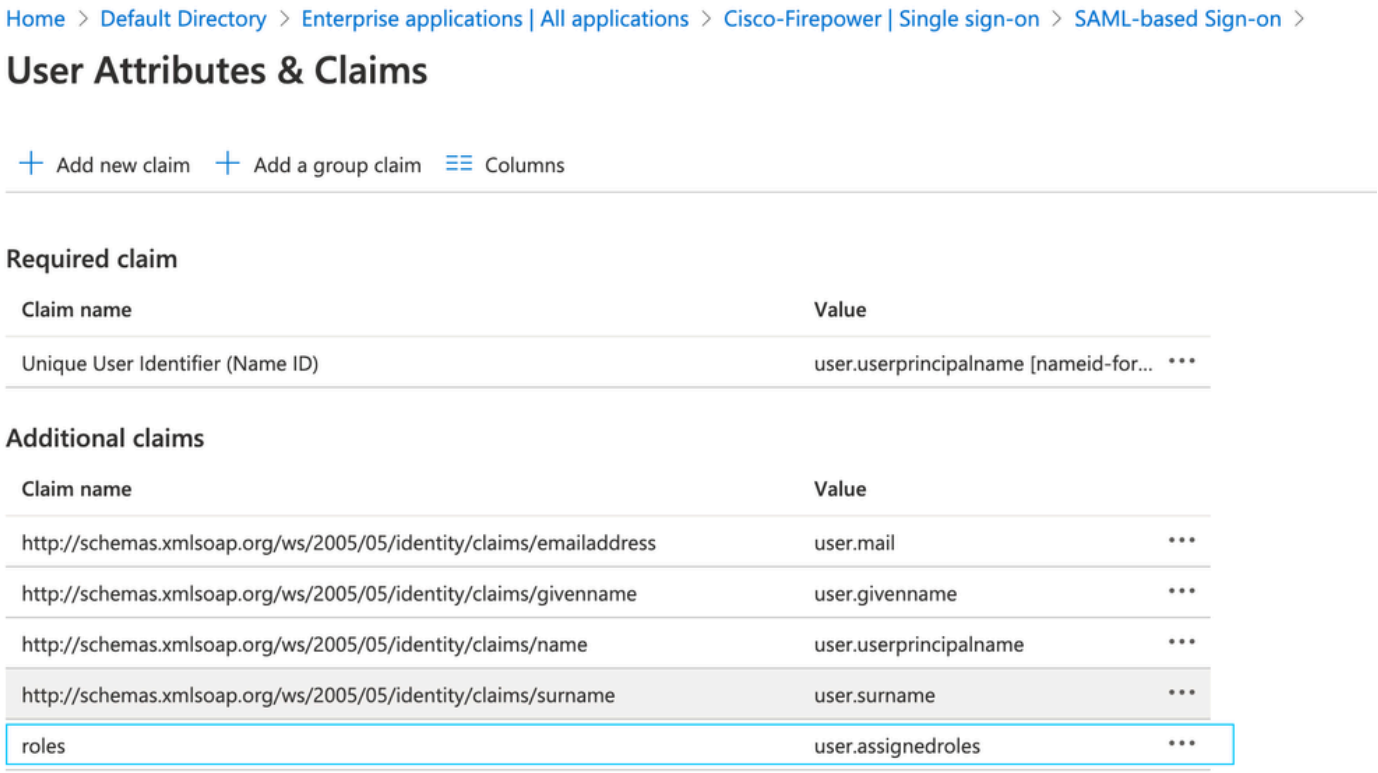
Configurazione avanzata - RBAC con Azure

Per utilizzare vari tipi di ruolo per il mapping ai ruoli di FMC, è necessario modificare il manifesto dell'applicazione in Azure per assegnare i valori ai ruoli. Per impostazione predefinita, il valore dei ruoli è Null.

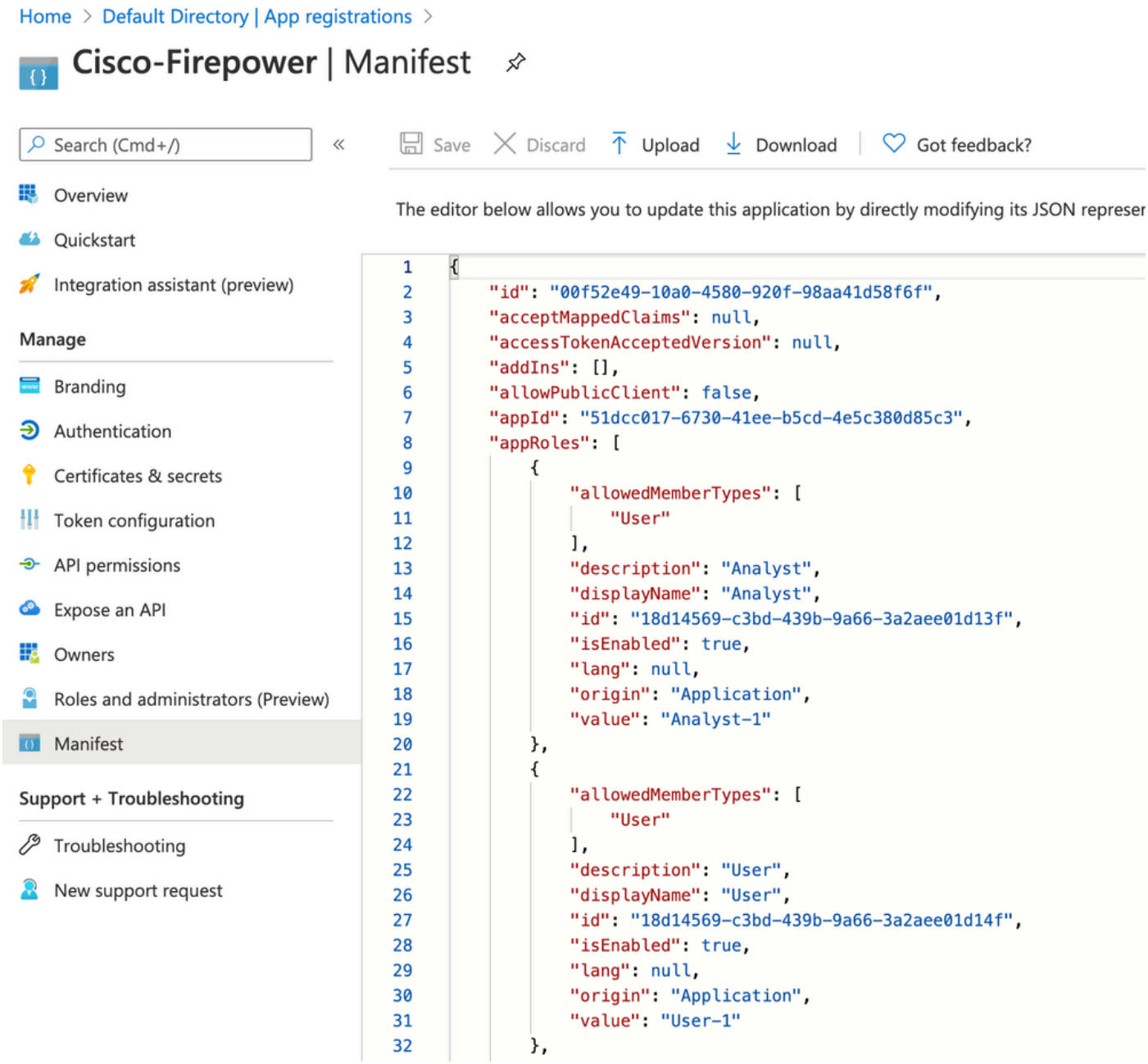
Passaggio 1. Passare all'applicazione creata e fare clic su Single Sign-On.



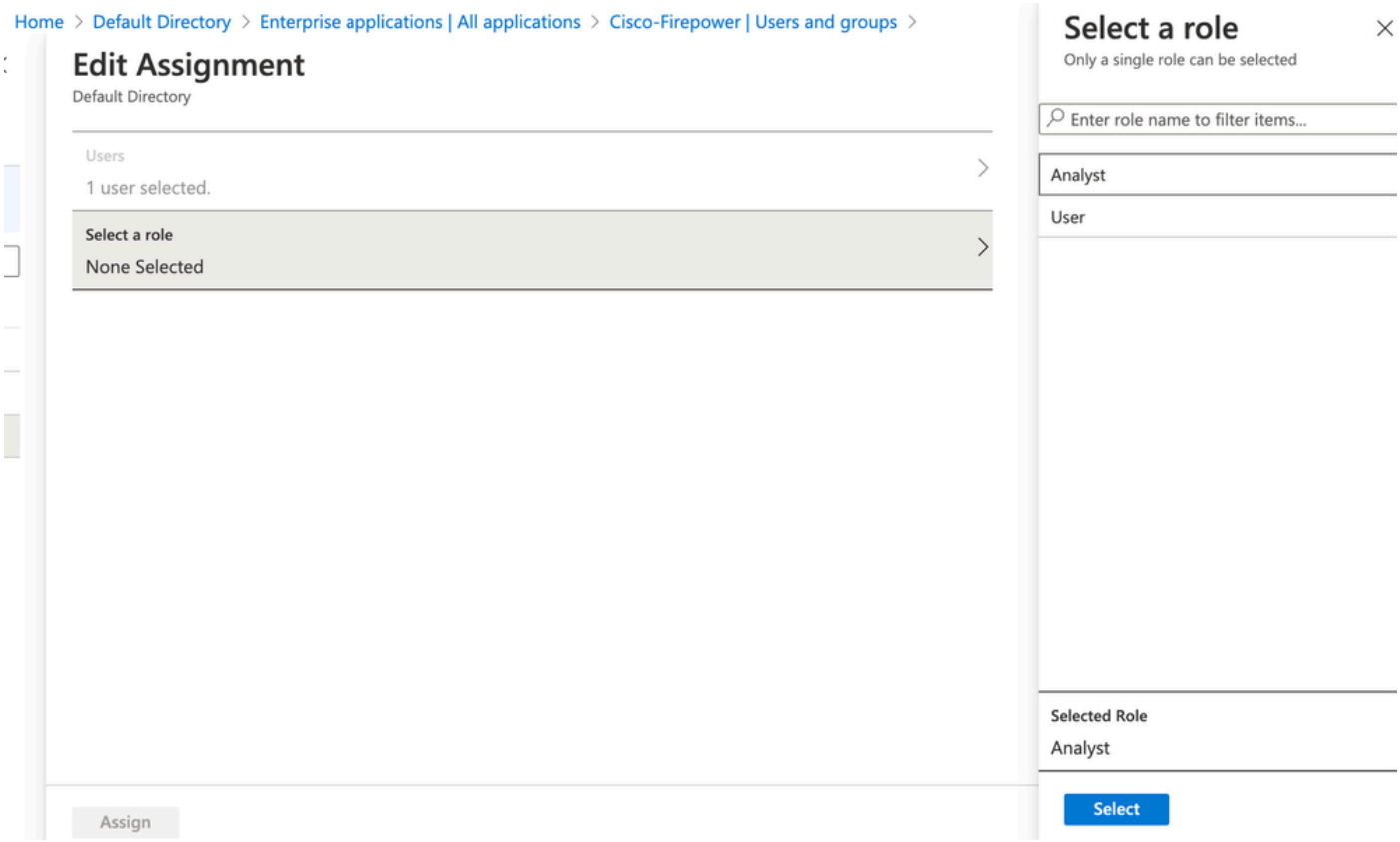
Passaggio 2. Modificare gli attributi utente e le attestazioni. Aggiungere una nuova attestazione con nome: ruoli e selezionare il valore come user.assignedroles.



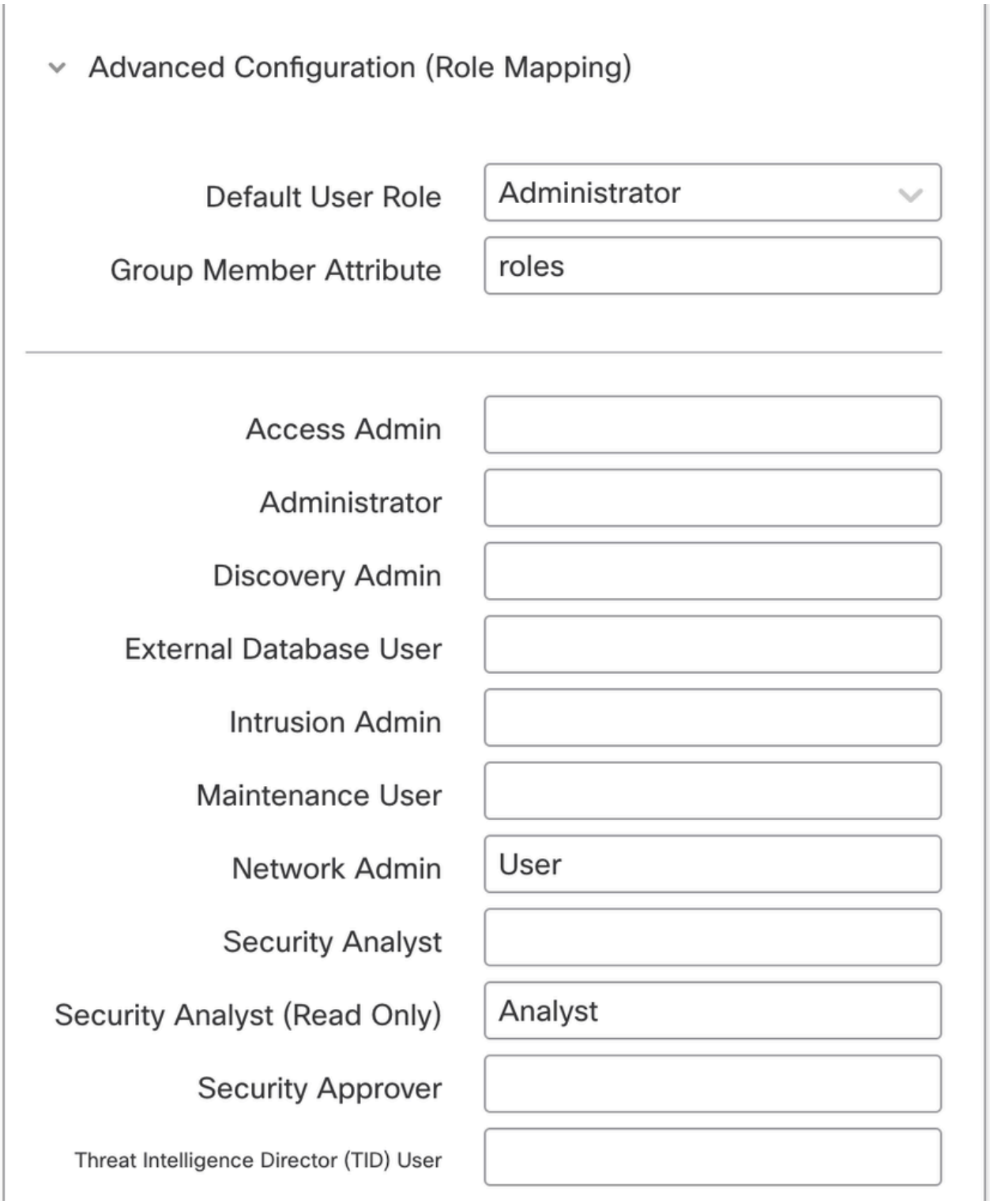
Passaggio 3. Passare a <Application-Name> > Manifesto. Modificare il manifesto. Il file è in formato JSON ed è disponibile per la copia un utente predefinito. Ad esempio, qui vengono creati 2 ruoli: Utente e Analista.



Passaggio 4. Passare a <Application-Name> > Utenti e gruppi. Modificare l'utente e assegnare i nuovi ruoli creati, come mostrato in questa immagine.



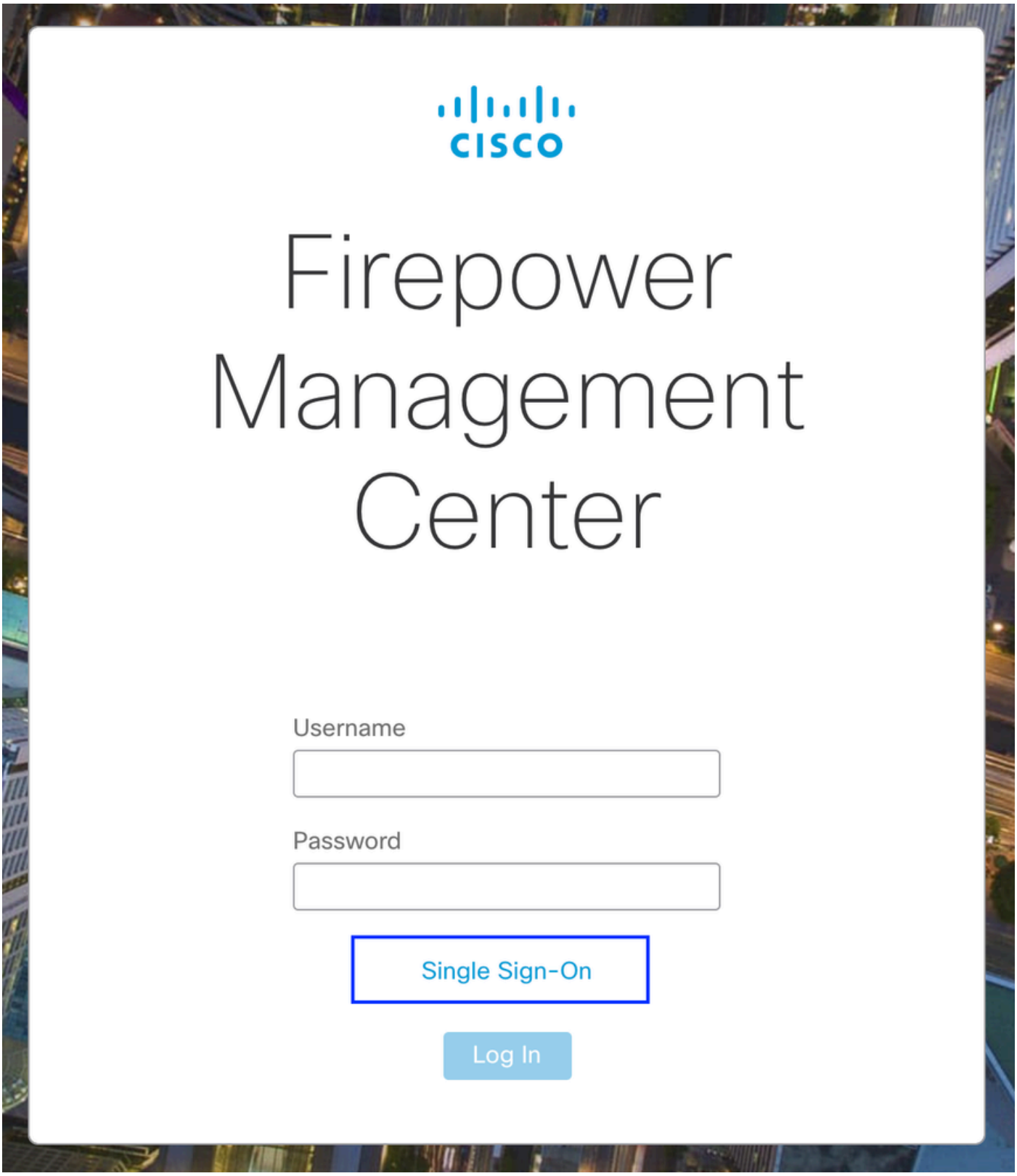
Passaggio 4. Accedere a FMC e modificare la configurazione avanzata in SSO. Attributo membro gruppo, ad esempio: assegnare ai ruoli il nome visualizzato specificato nel manifesto dell'applicazione.



Al termine, è possibile accedere al ruolo designato.

Verifica

Passaggio 1. Accedere all'URL FMC dal browser: https://<URL FMC>. Fare clic su Single Sign-On, come illustrato nell'immagine.



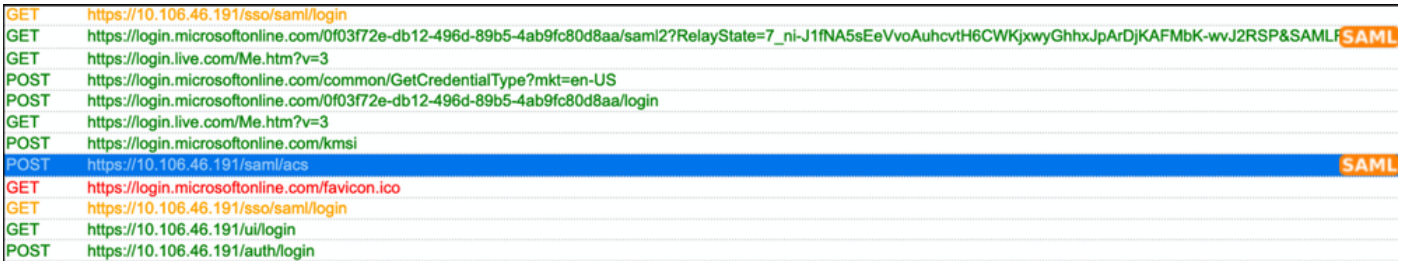
L'utente viene quindi reindirizzato alla pagina di accesso a Microsoft e l'accesso riuscito restituirà la pagina predefinita di FMC.

Passaggio 2. In FMC, selezionare System > Users (Sistema > Utenti) per visualizzare l'utente SSO aggiunto al database.

Risoluzione dei problemi

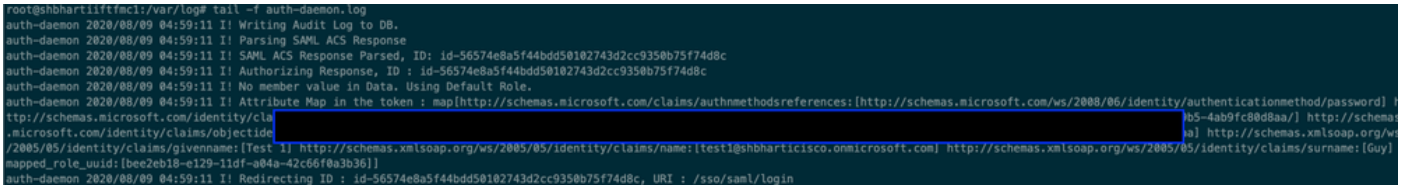
Verificare l'autenticazione SAML e questo è il flusso di lavoro ottenuto per la riuscita dell'autorizzazione (questa immagine è di un ambiente lab):

Log SAML browser



Registri SAML FMC

Verificare i log SAML su FMC all'indirizzo/var/log/auth-daemon.log



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).