Configurar o ASA AnyConnect VPN com o Microsoft Azure MFA por meio de SAML

Contents

Introduction

Este documento descreve como configurar a SAML (Security Assertion Markup Language) com foco no Adaptive Security Appliance (ASA) AnyConnect através do Microsoft Azure MFA.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da configuração da VPN do RA no ASA.
- Conhecimento básico do SAML e do Microsoft Azure.
- Licenças do AnyConnect ativadas (apenas APEX ou VPN).

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Uma assinatura do AD do Microsoft Azure.
- Cisco ASA 9.7+ e Anyconnect 4.6+
- Perfil de VPN do AnyConnect em funcionamento

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O SAML é uma estrutura baseada em XML para troca de dados de autenticação e autorização entre domínios de segurança. Ele cria um círculo de confiança entre o usuário, um provedor de serviços (SP) e um provedor de identidade (IdP) que permite que o usuário entre uma única vez para vários serviços. O Microsoft Azure MFA integra-se perfeitamente ao dispositivo VPN Cisco ASA para fornecer segurança adicional para os logons do Cisco AnyConnect VPN.

Componentes SAML

Metadados: É um documento baseado em XML que garante uma transação segura entre um IdP e um SP. Permite que o IdP e o SP negociem contratos.

Funções suportadas pelos dispositivos (IdP, SP)

Um dispositivo pode suportar mais de uma função e pode conter valores para uma controladora e um IdP. No campo EntityDescriptor, há um IDPSSODescriptor se as informações contidas forem para um IdP de Logon Único ou um SPSSODescriptor se as informações contidas forem para um SP de Logon Único. Isso é importante, pois os valores corretos devem ser tirados das seções apropriadas para que o SAML seja configurado com êxito.

ID da entidade: Esse campo é um identificador exclusivo de um SP ou IdP. Um único dispositivo pode ter vários serviços e pode usar diferentes IDs de entidade para diferenciá-los. Por exemplo, o ASA tem diferentes IDs de entidade para diferentes grupos de túneis que precisam ser autenticados. Um IdP que autentica cada grupo de túneis tem entradas de ID de entidade separadas para cada grupo de túneis para identificar com precisão esses serviços.

O ASA pode suportar vários IdPs e tem um ID de entidade separado para cada IdP para diferenciá-los. Se um dos lados receber uma mensagem de um dispositivo que não contém uma ID de entidade que tenha sido configurada anteriormente, o dispositivo provavelmente descartará essa mensagem e a autenticação SAML falhará. A ID da entidade pode ser encontrada no campo EntityDescriptor ao lado de entityID.

URLs de serviço: Definem a URL para um serviço SAML fornecido pelo SP ou IdP. Para os IdPs, é mais comum ser o Serviço de Logoff Único e o Serviço de Logon Único. Para os SPs, geralmente é o Assertion Consumer Service e o Single Logout Service.

A URL do serviço Single Sign-On encontrada nos metadados do IdP é usada pelo SP para redirecionar o usuário ao IdP para autenticação. Se esse valor estiver configurado incorretamente, o IdP não receberá ou não poderá processar com êxito a solicitação de

autenticação enviada pelo SP.

A URL de serviço do consumidor de asserção encontrada nos metadados da controladora de armazenamento é usada pelo IdP para redirecionar o usuário de volta para a controladora de armazenamento e fornecer informações sobre a tentativa de autenticação do usuário. Se isso for configurado incorretamente, o SP não receberá a asserção (a resposta) ou não poderá processá-la com êxito.

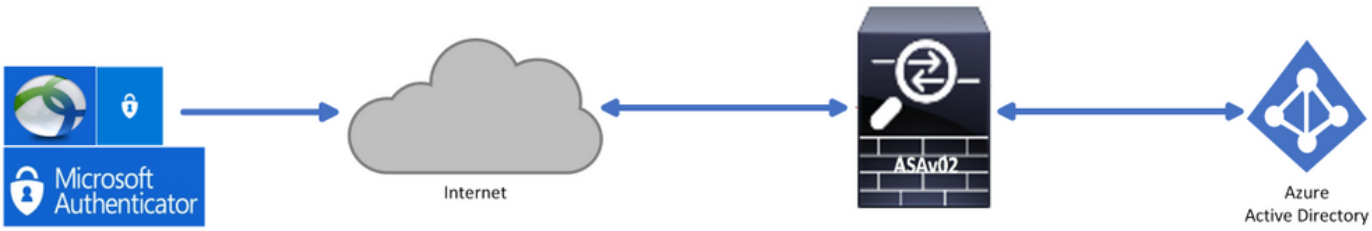
A URL do serviço de logoff único pode ser encontrada na controladora e no IdP. É usado para facilitar o logoff de todos os serviços SSO do SP e é opcional no ASA. Quando a URL do serviço SLO dos metadados de IdP é configurada na controladora, quando o usuário faz logoff do serviço na controladora, a controladora envia a solicitação ao IdP. Depois que o IdP tiver desconectado com êxito o usuário dos serviços, ele redirecionará o usuário de volta para o SP e usará a URL do serviço do SLO encontrada nos metadados do SP.

Associações SAML para URLs de Serviço: As vinculações são o método que o SP usa para transferir informações para o IdP e vice-versa para serviços. Isso inclui Redirecionamento HTTP, POST HTTP e Artefato. Cada método tem uma maneira diferente de transferir dados. O método de vinculação suportado pelo serviço está incluído na definição desses serviços. Por exemplo: SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://saml.example.com/simplesaml/saml2/idp/SSOService.php"/ >. O ASA não oferece suporte à associação de Artefato. O ASA sempre usa o método Redirecionamento HTTP para solicitações de autenticação SAML, por isso é importante escolher a URL do Serviço SSO que usa a associação Redirecionamento HTTP para que o IdP espere isso.

Certificados para operações de assinatura e criptografia

Para fornecer confidencialidade e integridade para as mensagens enviadas entre o SP e o IdP, o SAML inclui a capacidade de criptografar e assinar os dados. O certificado usado para criptografar e/ou assinar os dados pode ser incluído nos metadados para que a extremidade que recebe possa verificar a mensagem SAML e garantir que ela vem da fonte esperada. Os certificados usados para assinatura e criptografia podem ser encontrados nos metadados em KeyDescriptor use="signing" e KeyDescriptor use="encryption", respectivamente, depois em X509Certificate. O ASA não oferece suporte à criptografia de mensagens SAML.

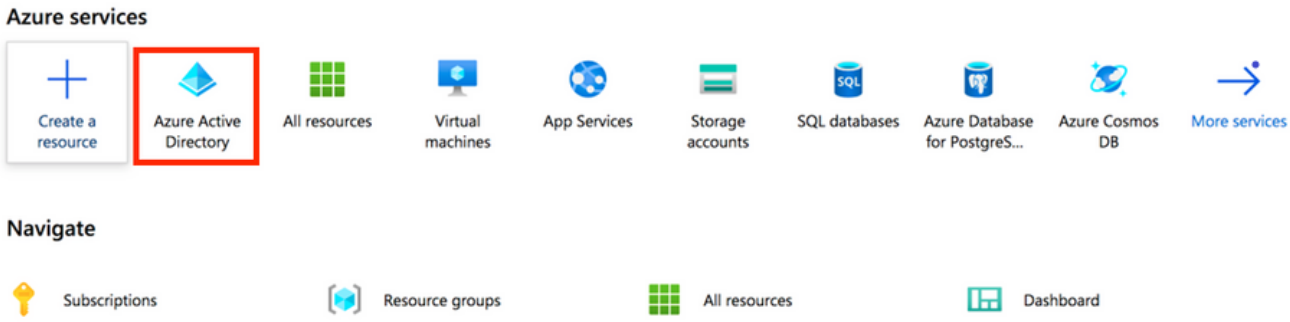
Diagrama de Rede



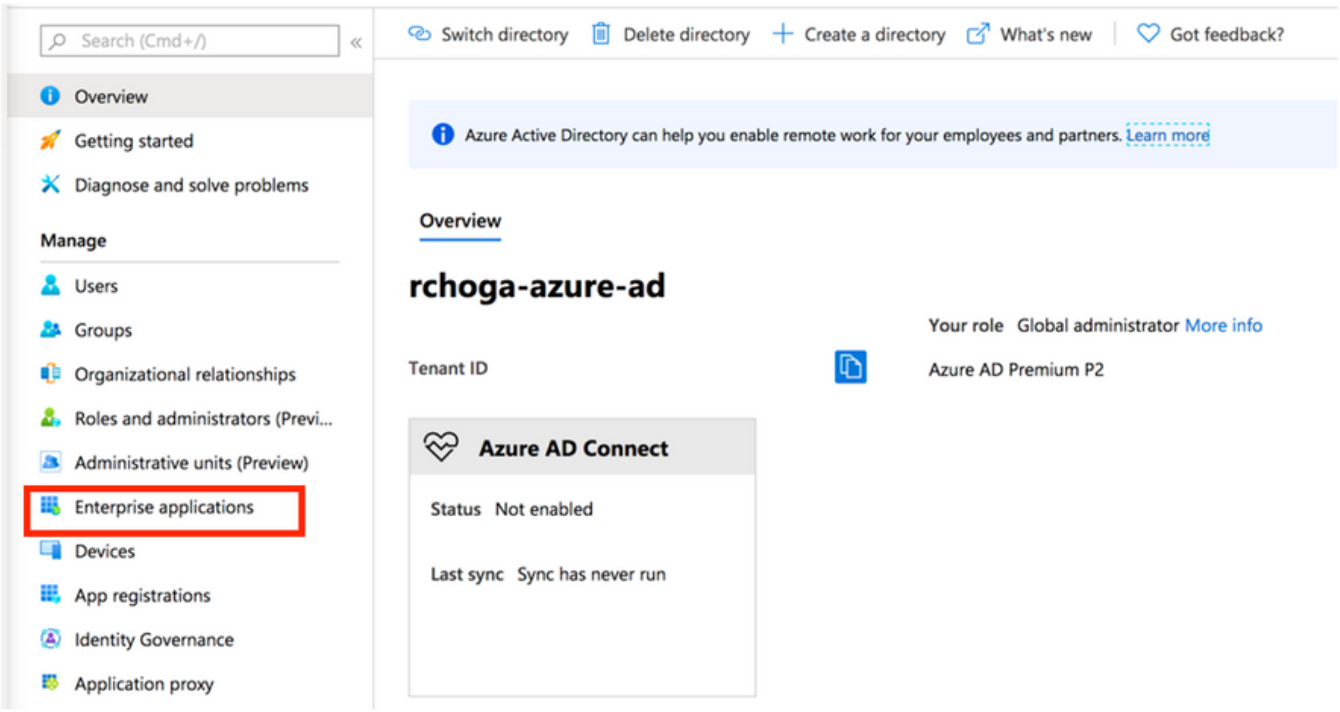
Configurar

Adicionar o Cisco AnyConnect da Galeria de aplicativos da Microsoft

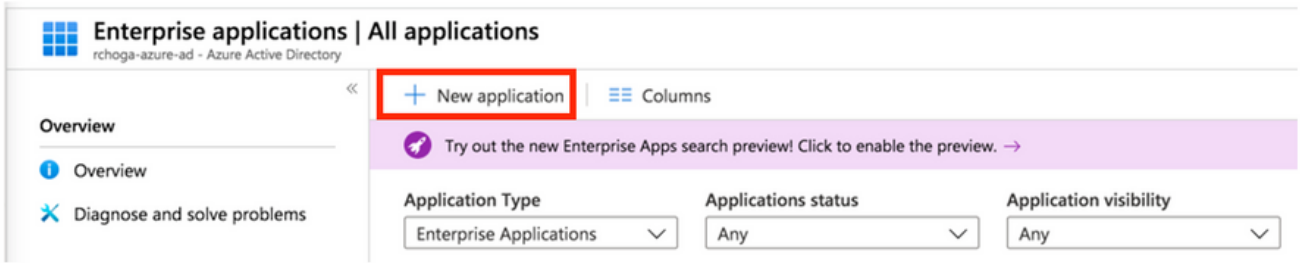
Etapa 1. Faça logon no Portal do Azure e selecione Ative Diretory do Azure.



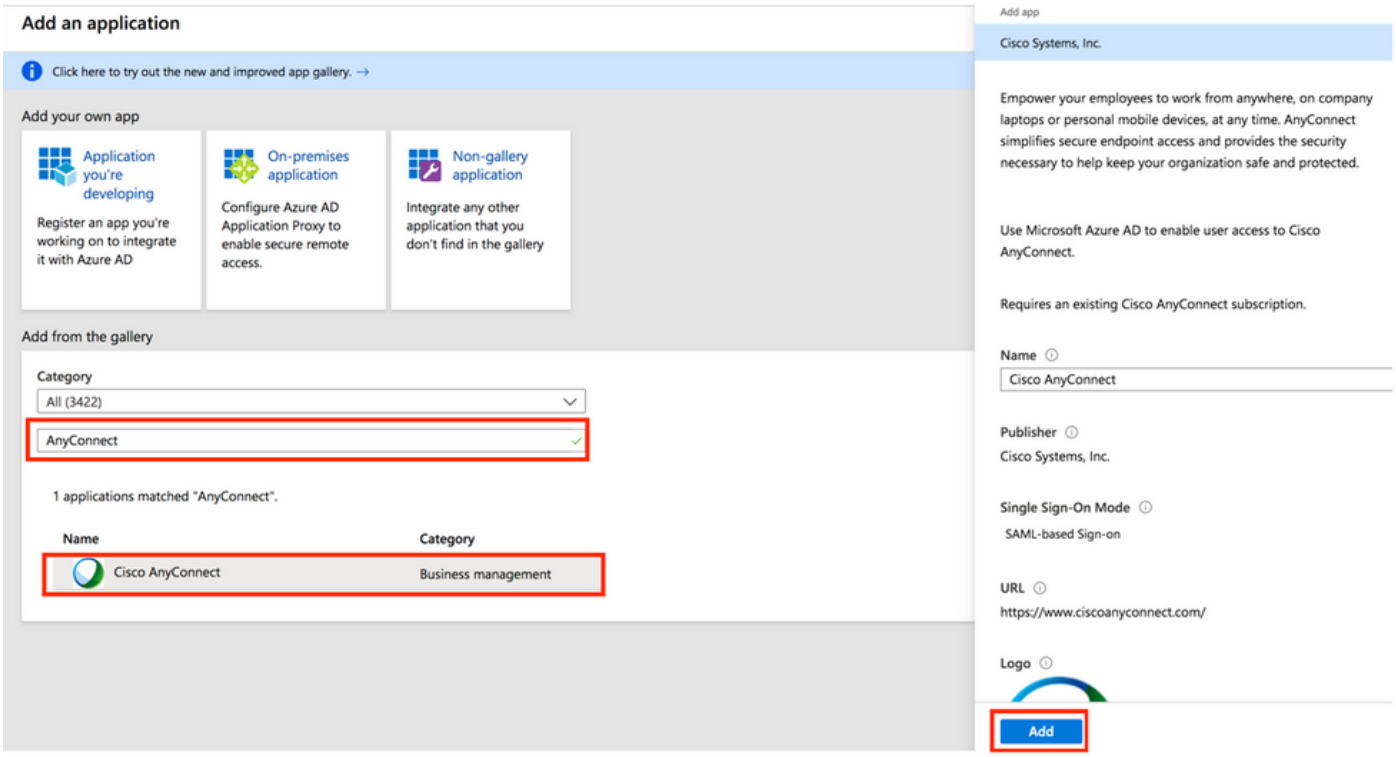
Etapa 2. Como mostrado nesta imagem, selecione **Enterprise Applications**.



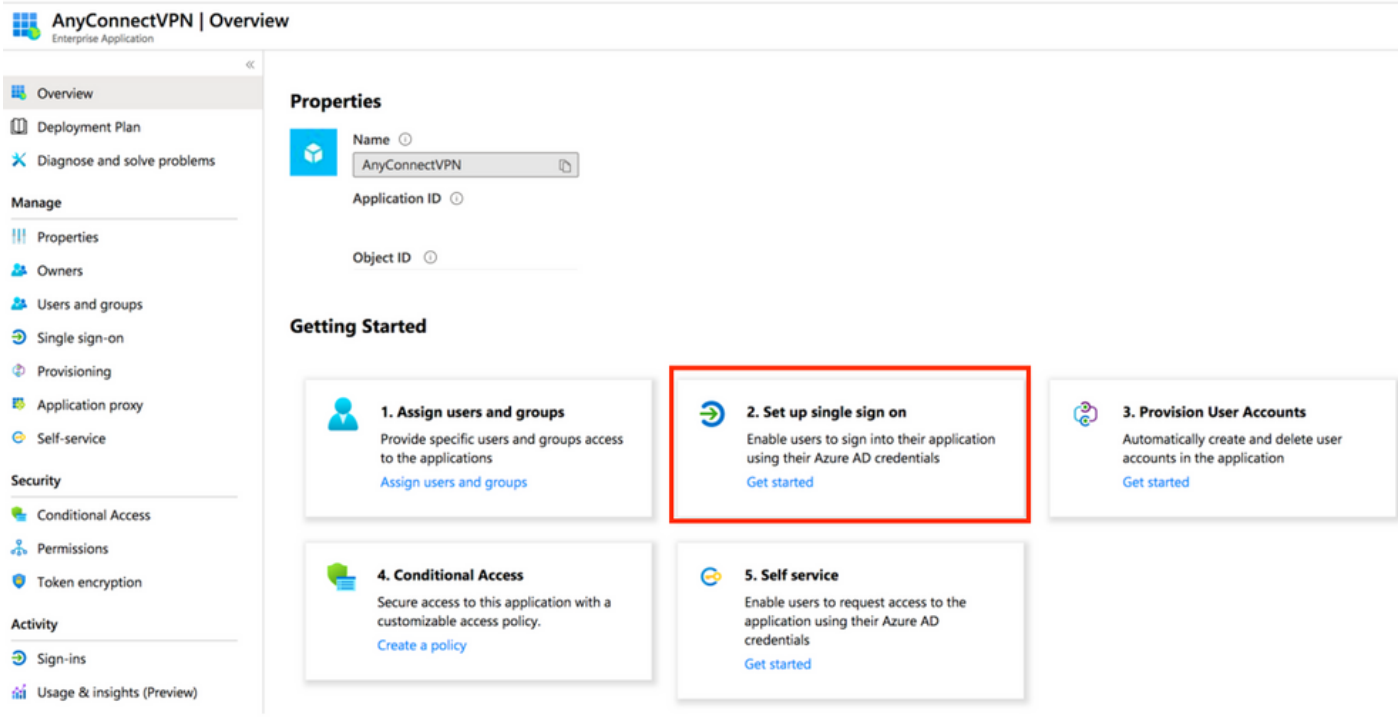
Etapa 3. Agora selecione **New Application**, conforme mostrado nesta imagem.



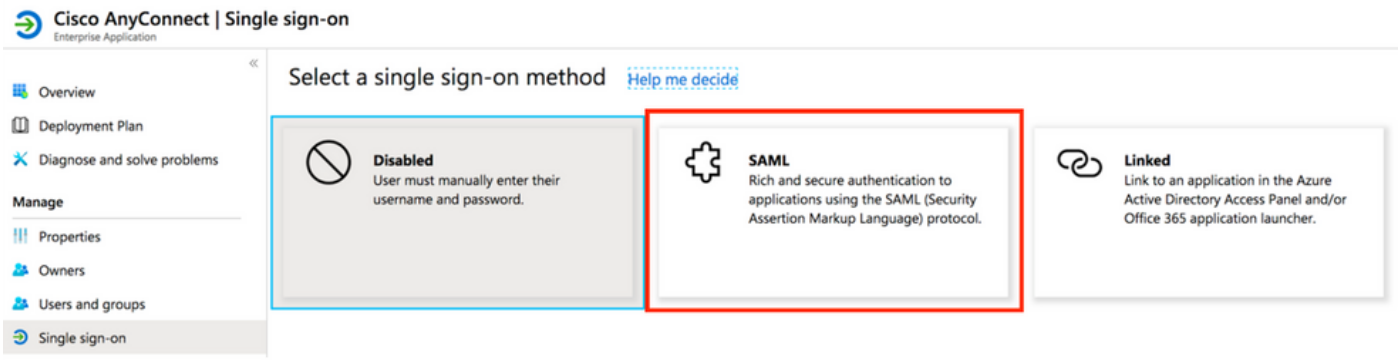
Etapa 4. Na seção **Adicionar da galeria, digite AnyConnect na caixa de pesquisa, selecione Cisco AnyConnect no painel de resultados e adicione o aplicativo.**



Etapa 5. Selecione o item de menu **Sign-on único**, conforme mostrado nesta imagem.



Etapa 6. Selecione **SAML, conforme mostrado na imagem.**

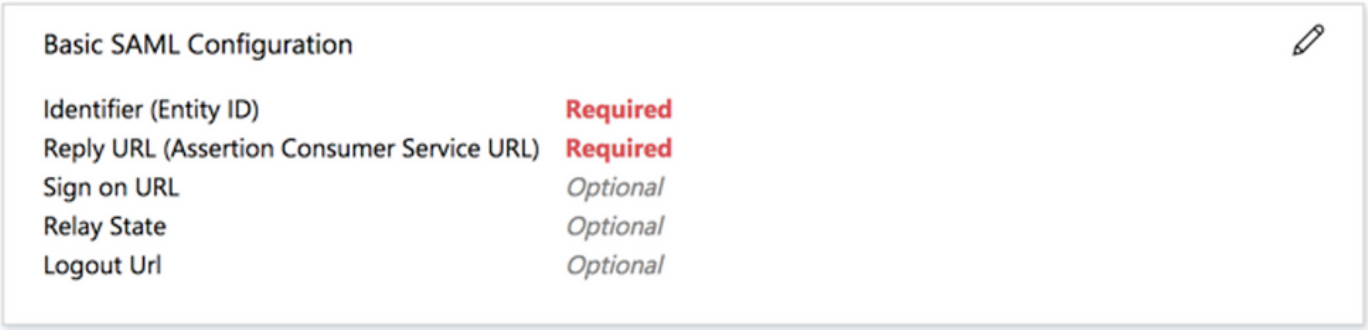


Etapa 7. Edite **a Seção 1 com esses detalhes.**

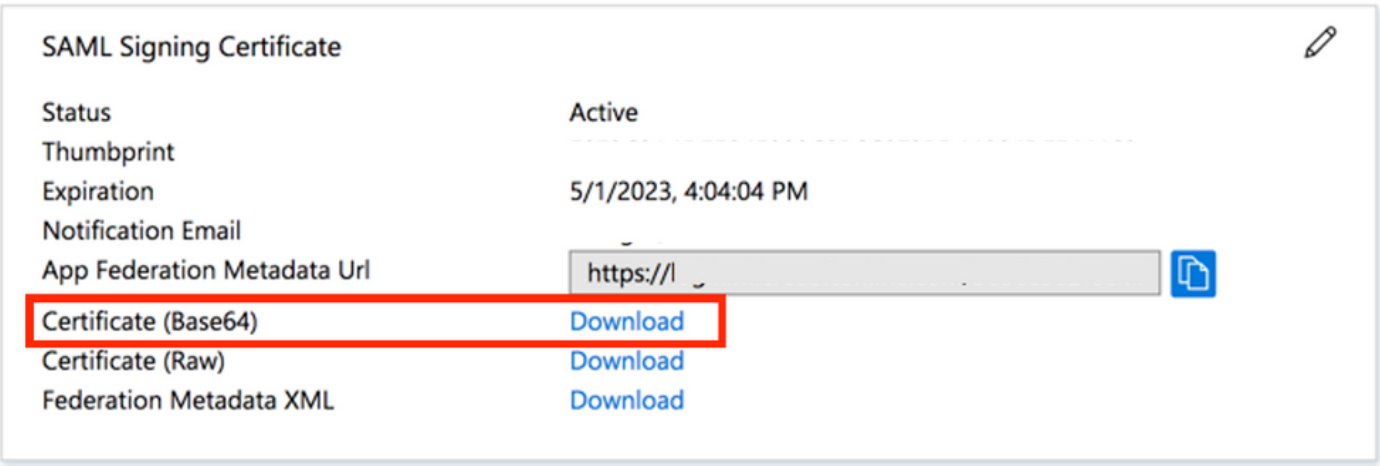
```
 a. Identifier (Entity ID)  - https://<VPN URL>/saml/sp/metadata/<TUNNEL-GROUP NAME>

 b. Reply URL (Assertion Consumer Service URL) - https://<VPN
URL>/+CSCOE+/saml/sp/acs?tgname=<TUNNEL-GROUP NAME>

 Example: vpn url called asa.example.com and tunnel-group called AnyConnectVPN-1
```

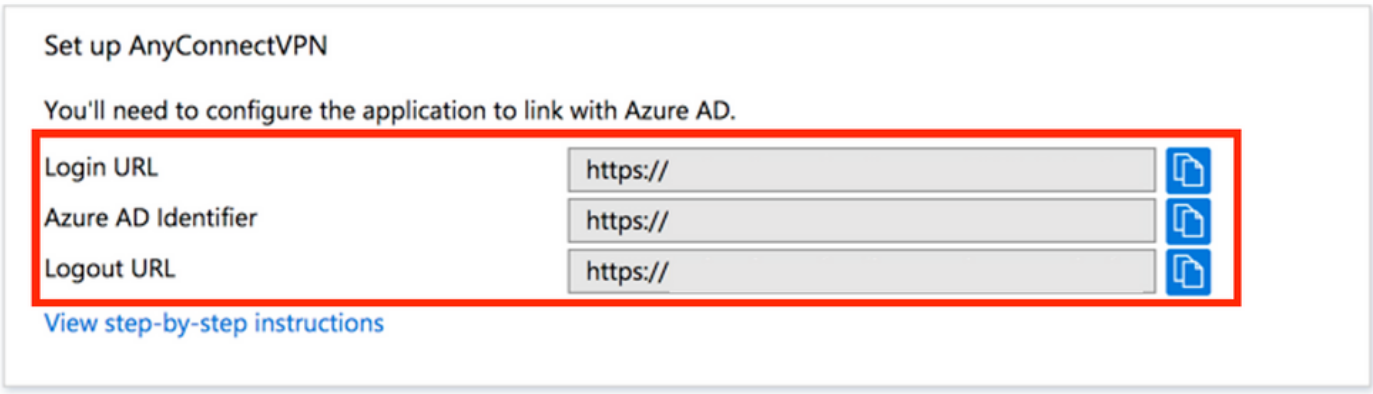


Etapa 8. Na seção **Certificado de assinatura SAML**, selecione **Download** para baixar o arquivo de certificado e salvá-lo no computador.



Etapa 9. Observe que isso é necessário para a configuração do ASA.

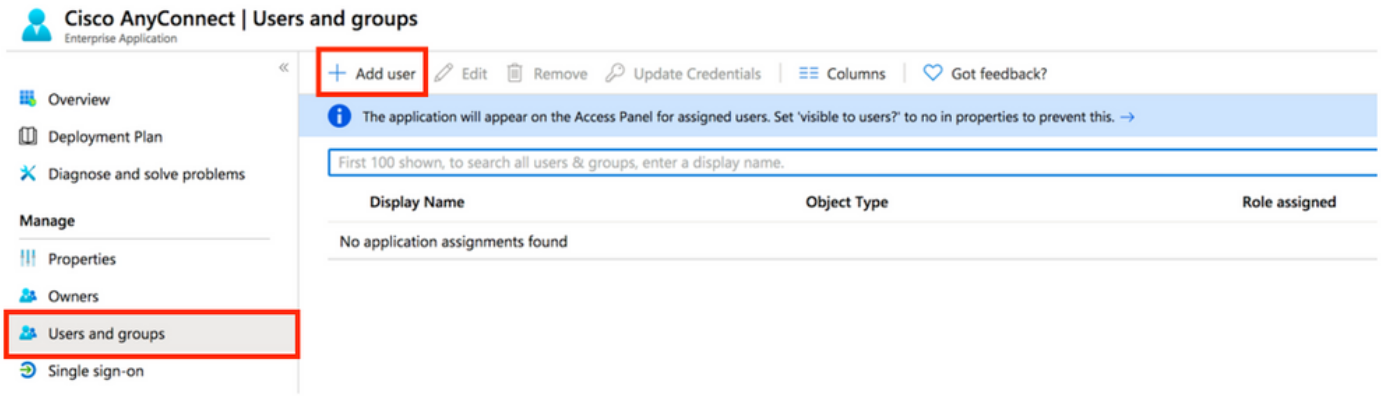
- Identificador do Azure AD - Este é o saml idp em nossa configuração VPN.
- URL de login - É a URL de entrada.
- URL de logoff - É o URL de saída.



Atribuir Usuário do Azure AD ao Aplicativo

Nesta seção, **Test1** está habilitado para usar logon único do Azure, à medida que você concede acesso ao aplicativo Cisco AnyConnect.

Etapa 1. Na página de visão geral do aplicativo, selecione **Usuários e grupos** e depois **Adicionar usuário**.



Etapa 2. Selecione **Usuários e grupos** na caixa de diálogo Adicionar tarefa.

Etapa 3. Na caixa de diálogo **Adicionar atribuição**, clique no botão **Atribuir**.

Configurar ASA para SAML via CLI

Etapa 1. Crie um ponto confiável e importe nosso certificado SAML.

```
config t
crypto ca trustpoint AzureAD-AC-SAML revocation-check none no id-usage enrollment terminal no
ca-check crypto ca authenticate AzureAD-AC-SAML -----BEGIN CERTIFICATE----- … PEM Certificate
Text you downloaded goes here … -----END CERTIFICATE----- quit
```

Etapa 2. Esses comandos provisionam seu IdP SAML.

```
webvpn

 saml idp https://sts.windows.net/xxxxxxxxxxxx/ - [Azure AD Identifier]
 url sign-in https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxx/saml2 - [Login URL]
 url sign-out https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0 – Logout URL
 trustpoint idp AzureAD-AC-SAML - [IdP Trustpoint]
 trustpoint sp ASA-EXTERNAL-CERT - [SP Trustpoint]
 no force re-authentication
 no signature
 base-url https://asa.example.com
```

Etapa 3. Aplicar a Autenticação SAML a uma Configuração de Túnel VPN.

```
tunnel-group AnyConnectVPN-1 webvpn-attributes
  saml identity-provider https://sts.windows.net/xxxxxxxxxxxx/
  authentication saml
end

write memory
```

> **Note**: Se você fizer alterações na configuração do IdP, precisará remover a configuração saml identity-provider do Grupo de Túneis e reaplicá-la para que as alterações entrem em vigor.

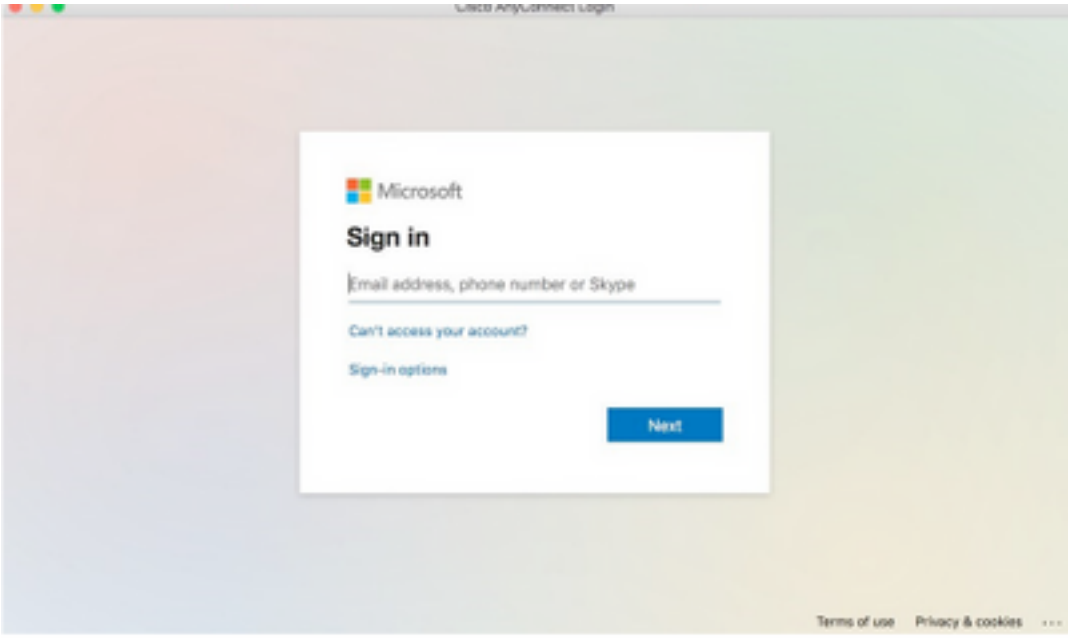
Verificar

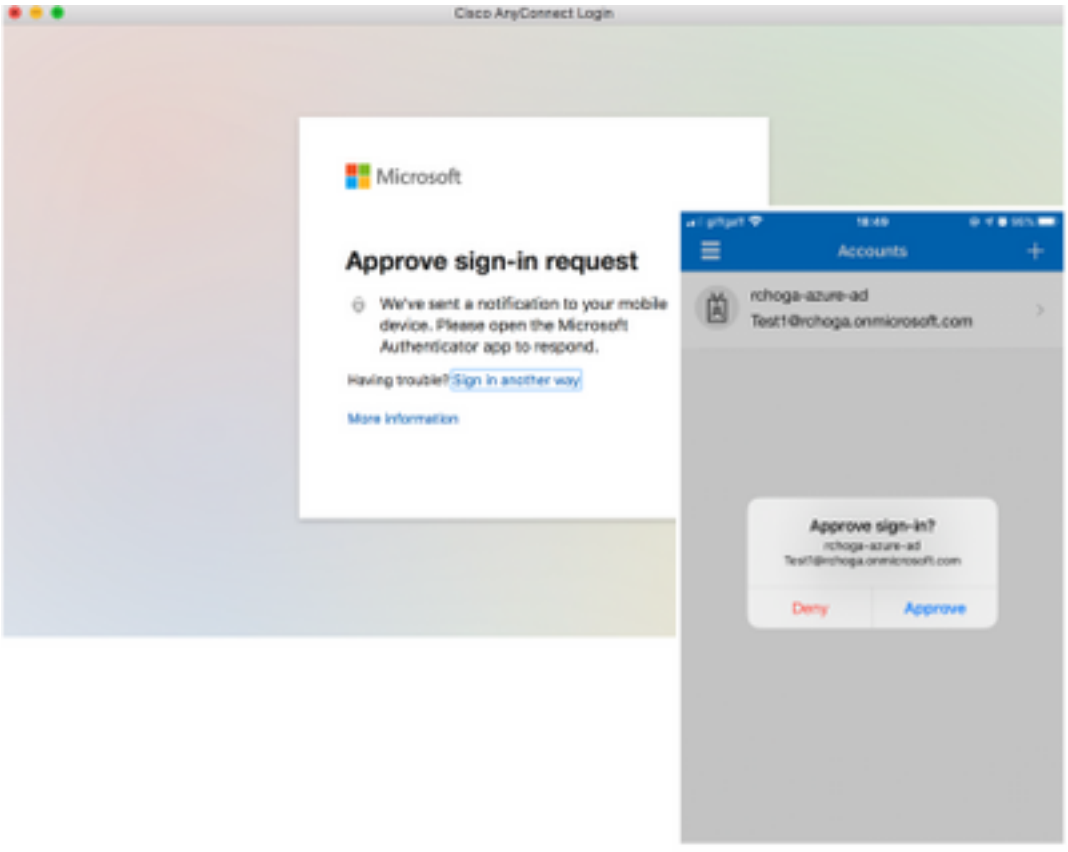
Testar AnyConnect com Autenticação SAML

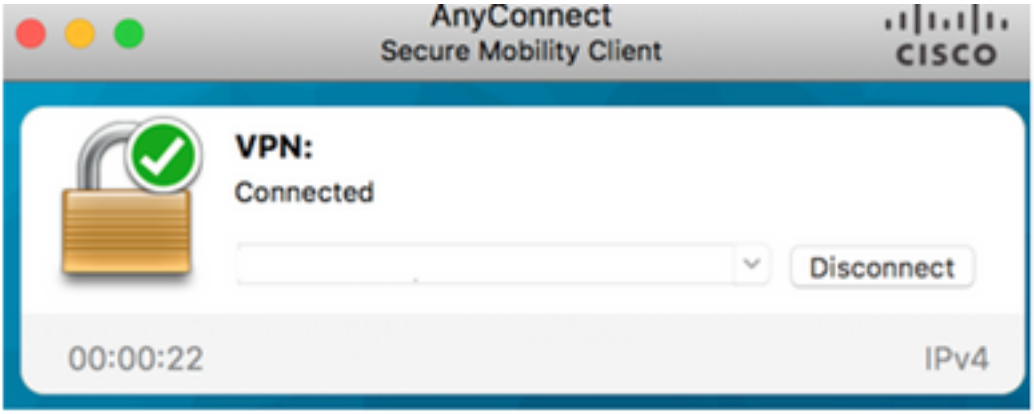
Etapa 1. Conecte-se à sua URL VPN e insira seus detalhes de logon do Azure AD.

Etapa 2. Aprovar solicitação de entrada.

Etapa 3. O AnyConnect está conectado.







Problemas comuns

Incompatibilidade de ID de entidade

Exemplo de depuração:

[SAML] consume_assertion: O identificador de um provedor é desconhecido para #LassoServer. Para registrar um provedor em um objeto #LassoServer, você deve usar os métodos lasso_server_add_provider() ou lasso_server_add_provider_from_buffer().

Problema: Geralmente, significa que o comando **saml idp [entityID]** na configuração webvpn do ASA não corresponde à ID de entidade do IdP encontrada nos metadados do IdP.

Solução: Verifique a ID da entidade do arquivo de metadados do IdP e altere o comando **saml idp [entity id]** para corresponder a isso.

Incompatibilidade de horário

Exemplo de depuração:

[SAML] NotBefore:2017-09-05T23:59:01.896Z NotOnOrAfter:2017-09-06T00:59:01.896Z tempo limite: 0

[SAML] consume_assertion: a asserção expirou ou não é válida

Problema 1. O tempo VMR não foi sincronizado com o tempo do IdP.

Solução 1. Configure ASA com o mesmo servidor NTP usado pelo IdP.

Problema 2. A declaração não é válida entre o tempo especificado.

Solução 2. Modifique o valor de tempo limite configurado no ASA.

Certificado de Assinatura IdP Incorreto Usado

Exemplo de depuração:

[Lasso] func=xmlSecOpenSSLEvpSignatureVerify:file=signatures.c:line=493:obj=rsa-sha1:subj=EVP_VerifyFinal:error=18:os dados não correspondem:a assinatura não corresponde

[SAML] consume_assertion: O perfil não pode verificar uma assinatura na mensagem

Problema: O ASA não pode verificar a mensagem assinada pelo IdP ou não há assinatura para o ASA verificar.

Solução: Verifique o certificado de assinatura IdP instalado no ASA para certificar-se de que ele corresponde ao que é enviado pelo IdP. Se isso for confirmado, verifique se a assinatura está incluída na resposta SAML.

Audiência de Asserção Inválida

Exemplo de depuração:

[SAML] consume_assertion: audiência de asserção inválida

Problema: O IdP define o público incorreto.

Solução: Corrija a configuração de Audiência no IdP. Ele deve corresponder à ID da entidade do ASA.

URL incorreta para o Serviço de Consumidor de Asserção

Exemplo de depuração: Não é possível receber depurações após o envio da solicitação de autenticação inicial. O usuário pode inserir credenciais no IdP, mas o IdP não redireciona para o ASA.

Problema: O IdP está configurado para a URL incorreta do Serviço de Consumidor de Asserção.

Solução(ões): Verifique a URL base na configuração e certifique-se de que esteja correta. Verifique os metadados ASA com show para certificar-se de que a URL do Assertion Consumer Service esteja correta. Para testá-lo, procure-o. Se ambos estiverem corretos no ASA, verifique o IdP para certificar-se de que o URL está correto.

Alterações de configuração SAML que não têm efeito

Exemplo: Depois que uma URL de logon único é modificada ou alterada, o certificado SP, o SAML ainda não funciona e envia as configurações anteriores.

Problema: O ASA precisa regenerar seus metadados quando houver uma alteração de configuração que o afete. Ele não faz isso automaticamente.

Solução: Depois que as alterações forem feitas, no grupo de túneis afetado, remova e reaplique o

comando saml idp [entity-id].

Troubleshoot

A maioria das soluções de problemas SAML envolve uma configuração incorreta que pode ser encontrada quando a configuração SAML é verificada ou quando as depurações são executadas. debug webvpn saml 255 pode ser usado para solucionar a maioria dos problemas, no entanto, em cenários onde essa depuração não fornece informações úteis, depurações adicionais podem ser executadas:

```
debug webvpn saml 255
debug webvpn 255
debug webvpn session 255
debug webvpn request 255
```

Informações Relacionadas

- Logon único SAML para aplicativos locais com Proxy de Aplicativo