

Configurar o portal do patrocinador do 2.1 ISE com PingFederate SAML SSO

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Vista geral do fluxo](#)

[Configurar](#)

[Etapa 1. Prepare o ISE para usar um fornecedor externo da identidade de SAML](#)

[Etapa 2. Configurar o portal do patrocinador para usar um fornecedor externo da identidade](#)

[Etapa 3. Configurar PingFederate como um IdP para segurar pedidos de autenticação ISE](#)

[Etapa 4. Importe Metadata de IdP no perfil externo do fornecedor ISE SAML IdP](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar um server de PingFederate SAML com o 2.1 de Engine(ISE) dos serviços da identidade de Cisco para fornecer únicas capacidades de On(SSO) do sinal de patrocinar usuários.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Serviços do convidado do Cisco Identity Services Engine.
- Conhecimento básico sobre disposições de SAML SSO.

[Componentes Utilizados](#)

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

- Versão 2.1 do Cisco Identity Services Engine
- Server de PingFederate 8.1.3.0 da identidade do sibilo.
- Windows Server 2012 R2 com serviços de diretório ativo.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se sua rede está viva, certifique-se de que você compreende o impacto potencial dos comandos any.

Convenções

Refira as [convenções dos dicas técnicas da Cisco](#) para obter mais informações sobre as convenções de documento

Vista geral do fluxo

O linguagem de marcação da afirmação da Segurança (SAML) é um padrão com base em XML para trocar dados da authentication e autorização entre domínios de segurança.

A especificação de SAML define três papéis: o diretor (usuário do patrocinador), o fornecedor da identidade (IdP) (server confederado do sibilo), e o provedor de serviços (SP) (ISE). Em um fluxo típico de SAML SSO, o SP pede e obtém uma afirmação da identidade do IdP. Baseado neste resultado, o ISE pode executar decisões de política enquanto o IdP pode incluir os atributos configuráveis que o ISE pode usar durante decisões de política. Uma vez que a autenticação inicial ocorre, o usuário não deve ser alertado para credenciais outra vez alcançar o serviço enquanto a sessão da afirmação é ainda ativa no IdP.

Este é o fluxo previsto para este caso do uso:

1. As tentativas do usuário de entrar ao portal do patrocinador lançando o nome de domínio totalmente qualificado feito sob encomenda do portal configurado do patrocinador (FQDN).
2. O ISE verifica se há uma afirmação ativa associada à sessão de navegador deste cliente emitindo um rápido reorienta ao IdP. Se não há nenhuma sessão ativa, o IdP reforçará o login de usuário.
3. O IdP autentica o usuário através do LDAP e passa atributos do memberOf e do email a ISE(SP).
4. O ISE processa a resposta de IdP XML e baseado no atributo do memberOf e na configuração dos grupos do patrocinador o usuário será permitido ou rejeitado (verificação de condição da membrasia do clube para combinar um grupo configurado do patrocinador).
5. O Time to Live da sessão variará em cada solução. Neste caso do uso, o sibilo Federate será configurado com um **timeout de sessão de 60 minutos** (se não há nenhuma solicitação de login SSO do ISE em 60 minutos após a autenticação inicial, a sessão é suprimida) e um **intervalo máximo da sessão de 480 minutos** (mesmo se o IdP tem recebido solicitações de login constantes SSO do ISE para este usuário que a sessão expirará em 8 horas). Uma vez o tempo de sessão para fora, uma autenticação de novo usuário é reforçada pelo IdP.
6. Quando a sessão for ainda ativa, o usuário do patrocinador deve poder fechar o navegador e o retorno ao portal sem credenciais entrando.

Configurar

A seguinte seção discutirá as etapas de configuração para integrar o ISE com o sibilo confederado e como permitir o navegador SSO para o portal do patrocinador.

Note: Embora as várias opções e possibilidades existam quando você autentica usuários do patrocinador, não todas as combinações estão descritas neste documento. Contudo, este exemplo fornece-o a informação necessária compreender como alterar o exemplo à

configuração que precisa você quer conseguir.

Etapa 1. Prepare o ISE para usar um fornecedor externo da identidade de SAML

1. Em Cisco ISE, navegue à **administração > ao Gerenciamento de identidades > fontes externos da identidade > identificação de SAML fornecedores**.
2. O clique adiciona
3. Sob o tab geral, dê entrada com um nome do fornecedor identificação e clique a **salvuarda**. O resto da configuração nesta seção dependerá dos metadados que precisa de ser importada do IdP.

Etapa 2. Configurar o portal do patrocinador para usar um fornecedor externo da identidade

1. Navegue aos **centros de trabalho > ao acesso do convidado > configuram > portais do patrocinador**
2. Clique sobre o **portal do patrocinador (padrão)** ou crie um portal novo.
3. Sob **ajustes portais** incorpore um nome de domínio totalmente qualificado feito sob encomenda (FQDN) ligado a este portal do patrocinador.
4. Selecione da **sequência que da fonte da identidade SAML** externo IdP definiu previamente.
5. Verifique que o diagrama de fluxo representa **salvuarda a seguinte** e do clique:

Etapa 3. Configurar PingFederate como um IdP para segurar pedidos de autenticação ISE

1. Navegue à **administração > ao Gerenciamento de identidades ISE > fontes externos da identidade > identificação de SAML fornecedores > PingFederate**
2. Clique a aba da **informação do provedor de serviços** e clique a **exportação**
3. Salvar e extraia o arquivo zip gerado. O arquivo XML contido aqui será usado ao criar o perfil em PingFederate.
4. Abra o portal de PingFederate admin (tipicamente <https://ip:9999/pingfederate/app>).
5. Sob a seção do **guia de configuração IDP > das conexões SP** seleta crie novo.
6. Sob o **tipo de conexão** clique **em seguida**
7. Sob **opções de conexão** clique **em seguida**
8. Sob **Metadados da importação**, o **arquivo** seleta, escolheu o arquivo e seleciona o arquivo XML exportado previamente do ISE.
9. Sob o **sumário dos Metadados**, clique sobre **em seguida**.
10. Na página da informação geral, sob o **nome de conexão** dê entrada com um nome (IE. ISEsponsorPortal) e clica **em seguida**.
11. Sob o clique do **navegador SSO configurar o navegador SSO** e sob a verificação dos **perfis de SAML** estas opções e clique-o **em seguida**:
12. Na **vida da afirmação** clique **em seguida**

13. No clique da **criação da afirmação** configurar a criação da afirmação

14. Sob o **padrão** e o clique seletos do **mapeamento da identidade em seguida**

SP Connection | Browser SSO | Assertion Creation

Identity Mapping

Attribute Contract

Authentication Source Mapping

Identity mapping is the process in which users authenticated by the IdP are associated to the SP. This mapping may affect the way that the SP will look up and associate the user to a specific local account.



STANDARD: Send the SP a known attribute value as the name identifier. The

15. No **contrato do atributo** > **estenda o contrato** incorporam o **correio dos atributos** e o **memberOf** e o clique **adicionam**. Em seguida, clique em **Avançar**.

Note: Este é um passo crítico como o ISE confia nestes atributos para o mapeamento correto do grupo do patrocinador e igualmente envia por correio eletrónico é necessário para funções corretas da notificação.

16. Sob o **exemplo novo do adaptador do mapa do clique do mapeamento da fonte da autenticação**.

17. No **exemplo do adaptador** selecione o **adaptador do formulário HTML**. Clique em **Next**.

18. Sob o **método do mapeamento** selecione a segunda opção e clique-a **em seguida**

19. No **atributo as fontes &** o clique da **consulta do usuário adicionam** a caixa da **fonte do atributo**.

20. Sob a **loja dos dados** incorpore uma descrição, a seguir selecione-a dos **dados ativos armazenam** seu exemplo da conexão ldap e definem que tipo de serviço de diretório este é. Se não há nenhuma loja dos dados configurada contudo clique sobre **lojas dos dados Manage** para adicionar o novo citam como exemplo.

21. Sob a **busca do diretório LDAP** defina a **base DN** para a consulta do usuário LDAP no domínio e clique-a em seguida.

Note: Isto é importante porque definirá a base DN durante a consulta do usuário LDAP. A base incorretamente definida DN conduzirá a um erro "objeto não encontrado no esquema LDAP".

22. Sob o **filtro LDAP** adicionar a corda **sAMAccountName=\$ {username}** e clique-a **em seguida**.

23. Sob a **realização do contrato do atributo** selecione estas opções e clique-as **em seguida**

24. Verifique a configuração na **seção sumária** e clique-a **feito**.

25. Suporte clique na **consulta das fontes & do usuário do atributo em seguida**.

26. Sob a **fonte à prova de falhas do atributo** clique **em seguida**.

27. Sob a **realização do contrato do atributo** selecione estas opções e clique-as **em seguida**:

27. Verifique a seção e o clique da configuração em resumo **feitos**.

28. Suporte no clique do **mapeamento da fonte da autenticação em seguida**.

29. Uma vez que a configuração foi verificada sob o clique da **seção sumária feito**.

30. Suporte no clique da **criação da afirmação em seguida**.

31. Sob o clique das **configurações de protocolo configurar configurações de protocolo**.

Neste momento deve haver 3 entradas já povoadas. Clique **em seguida**

32. Sob **SLO preste serviços de manutenção** ao clique **URL em seguida**

33. **Em emperramentos permissíveis de SAML** desmarcar as opções **PRODUTO MANUFATURADO** e **SABÃO** e clique-as **em seguida**.

34. Sob a **política da assinatura** clique **em seguida**.

35. Sob a **política de criptografia** clique **em seguida**.

36. Reveja a configuração na **página de sumário** e clique-a **feito**.

37. Suporte no **navegador SSO** > clique das **configurações de protocolo em seguida**, valide a configuração e clique-a **feito**. Isto trará para trás a aba do **navegador SSO**. Clique em Next.

38. Sob o clique das **credenciais configurar credenciais** e escolha o certificado de assinatura a ser usado durante IdP às comunicações ISE e verifique a opção **incluem o certificado na assinatura**. Em seguida, clique em Avançar.

Note: Se não há nenhum Certificados configurado, o clique **controla Certificados** e segue as alertas para gerar um certificado auto-assinado a ser usado para assinar IdP às comunicações ISE.

39. Valide a configuração sob a **página de sumário** e clique-a **feito**.

40. Suporte no clique da aba das **credenciais em seguida**.

41. Sob a **ativação & o sumário** seletos no **ACTIVE do status de conexão**, valide o resto da configuração e clique a **salv guarda**.

1. Sob o console de gerenciamento de PingFederate, navegue à **configuração do servidor > às funções administrativas > à exportação dos Metadata** se o server esteve configurado para papéis múltiplos (IdP e SP) seleciona a opção que **eu sou a identidade Provider(IdP)**. Clique em **seguida**

2. Sob o modo dos **Metadata** seletor “**selecione a informação para incluir manualmente nos Metadata**”. Clique em Next.

3. Sob o **protocolo** clique **em seguida**.

4. **No contrato do atributo** clique **em seguida**.

5. Sob a **chave de assinatura** selecione o certificado configurado previamente no perfil de conexão. Clique em Next.

6. Sob a **assinatura dos Metadata** selecione o certificado de assinatura e a verificação **inclui a chave pública deste certificado no elemento de informação chave**. Clique em Next.

7. Sob o clique do **certificado da criptografia XML em seguida**. A opção para reforçar a criptografia aqui é até a rede Admin.

8. Sob a salvaguarda da **exportação do** clique da **seção sumária os Metadata** arquivam gerado e clicam então **feito**.

9. Sob o ISE, navegue à **administração > ao Gerenciamento de identidades > fontes externos da identidade > identificação de SAML fornecedores > PingFederate**.

10. Clique sobre o **fornecedor da identidade o >Click da configuração que consulta** e continue importar os metadata salvar da operação da exportação dos Metadata de Pingfederate.

11. A aba seletor dos **grupos** e sob o **atributo da membrasia do clube** adiciona o **memberOf** e clica-o então **adiciona**

12. Sob o nome na **afirmação** adicionar o **nome destacado** que o IdP deve retornar para trás quando o atributo do **memberOf** é autenticação LDAP recuperada do formulário. Este grupo será ligado ao grupo do patrocinador.

Uma vez que você adiciona o DN e o “nome **APROVAÇÃO** do clique da descrição ISE”.

13. Selecione a aba dos **atributos** e o clique **adiciona**. Nesta etapa nós adicionaremos o atributo “**correio**”. Isto é contido na autenticação de SAML; resultado passado do IdP (baseado no atributo do email para esse objeto do usuário no diretório ativo).

Note: Esta etapa é por mais importante que o ISE deva poder processar o email ligado à sessão do patrocinador para poder traçar todas as contas no status pendente dos fluxos auto-registrados. Se não as contas permanecerão em um estado do limbo porque a “**pessoa que é**” email visitado não será traçada a uma sessão válida do patrocinador. É igualmente importante para a notificação de Email propõe.

14. Sob o **guia avançada** selecione os seguintes ajustes:

Note: Esta seção instruirá o ISE para incluir o atributo do email em pedidos da saída ao server do IdP. Isto é importante quando o usuário do patrocinador termina manualmente do portal.

15. Click **Save**.

16. Nesta etapa o administrador traçará o grupo do diretório ativo recuperado pelo IdP a um grupo do patrocinador. Navegue aos **centros de trabalho** > ao **acesso do convidado** > **configuram** > **patrocinador agrupa** > **ALL_ACCOUNTS** (ou selecione o grupo apropriado). Clique **membros** e selecione o **PingFederate: Agrupe-nos** traçou em etapas precedentes e adicionar-lo à coluna dos grupos de usuário selecionado. Em seguida, clique em "OK".

17. Quando o fluxo registrado auto é configurado, as contas serão durante a aprovação. Neste caso, seleto "**aprove e pedidos da vista dos convidados auto-registrados**" e selecione "**somente durante as contas atribuídas a este patrocinador**" como uma maneira fácil verificar o endereço email do objeto é AD e transferidas à identidade do patrocinador no ISE através do server de IdP usando o atributo do **correio**.

18. Click **Save**. Isto termina a configuração no ISE.

Verificar

1. Lance o portal do patrocinador usando o FQDN configurado do costume. O ISE deve reorientar o usuário ao portal da autenticação de usuário de PingFederate.
2. Incorpore credenciais do diretório ativo e sinal da batida sobre. A tela de logon de IdP reorientará o usuário ao AUP inicial no portal do patrocinador do ISE.

Neste momento o usuário do patrocinador deve ter o acesso direto ao portal.

3. Verifique o único sinal sobre. Quando "a característica do **teste URL portal**" está usada o ISE deve pedir credenciais do patrocinador todas as vezes se o SSO não é configurado.

Lance o portal do patrocinador com link portal do teste URL. O patrocinador URL ISE comutará rapidamente ao IdP URL para verificar que estado da sessão e uma vez que o token da sessão é confirmado o cliente está reorientada de volta ao portal do patrocinador sem a necessidade de incorporar credenciais.

4. Verifique que o atributo do email está passado corretamente do objeto do diretório ativo a IdP ao ISE. A maneira a mais fácil de testar é criando uma conta nova no portal do patrocinador e selecionando a opção da **notificação**. Se o email é recuperado corretamente aparecerá sob o campo do **endereço email do patrocinador**.

5. Verifique a função da **saída**. Isto é crucial na integração verificar que a saída do patrocinador provoca a sessão simbólica a ser terminada no lado de servidor da identidade. Assine para fora do portal do patrocinador e certifique-se de que a próxima vez que o usuário tenta alcançar o portal do patrocinador, estará reorientado de volta à tela da autenticação de IdP.

Troubleshooting

Toda a transação da autenticação de SAML será lado entrado ISE sob `ise-psc.log`. Há um componente dedicado (**SAML**) sob a **administração > registrando > debuga a configuração do log > seleciona o nó na pergunta > ajustou SAML componente ao nível de debug**.

Nós podemos alcançar o ISE com o CLI e para emitir da “uma cauda de registro de `ise-psc.log` do aplicativo mostra” e para monitorar os eventos de SAML viva, ou nós podemos transferir `ise-psc.log` para a análise mais aprofundada sob **operações > pesquisamos defeitos > logs da transferência > selecionamos o nó ISE > debugamos a aba dos logs > o clique `ise-psc.log` para transferir os logs**.

Tipicamente o log inicial da autenticação olhará como este:

```
2016-06-13 10:18:58,560 DEBUG [http-bio-14.36.157.210-8443-exec-7] []
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML request -
spUrlToReturnTo:https://torsponsor21.rtpaaa.net:8443/sponsorportal/SSOLoginResponse.action
```

```
2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7] []
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML Response:
statusCode:urn:oasis:names:tc:SAML:2.0:status:Success
```

```
2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7] []
cpm.saml.framework.impl.SAMLAttributesParser -:::- [parseAttributes] Found attribute name :
mail
```

```
2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7] []
cpm.saml.framework.impl.SAMLAttributesParser -:::- [parseAttributes] Delimiter not configured,
Attribute=<mail> add value=<antontor@rtpaaa.net>
```

```
2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7] []
cpm.saml.framework.impl.SAMLAttributesParser -:::- [parseAttributes] Found attribute name :
memberOf
```

```
2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7] []
cpm.saml.framework.impl.SAMLAttributesParser -:::- [parseAttributes] Delimiter not configured,
Attribute=<memberOf> add value=<CN=TOR,DC=rtpaaa,DC=net>
```

Após o evento do login inicial, cada vez que os acessos de usuário o portal do patrocinador nós considerarão o ISE recuperar a informação da afirmação para verificar que o token é ainda ativo. O resultado deve olhar como este:

```
2016-06-13 10:18:58,560 DEBUG [http-bio-14.36.157.210-8443-exec-7] []
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML request -
spUrlToReturnTo:https://torsponsor21.rtpaaa.net:8443/sponsorportal/SSOLoginResponse.action
```

```
2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7] []
cpm.saml.framework.impl.SAMLFacadeImpl -:::- SAML Response:
statusCode:urn:oasis:names:tc:SAML:2.0:status:Success
```

```
2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7] []
cpm.saml.framework.impl.SAMLAttributesParser -:::- [parseAttributes] Found attribute name :
mail
```

```
2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7] []
cpm.saml.framework.impl.SAMLAttributesParser -:::- [parseAttributes] Delimiter not configured,
Attribute=<mail> add value=<antontor@rtpaaa.net>
```

```
2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7] []
cpm.saml.framework.impl.SAMLAttributesParser -:::- [parseAttributes] Found attribute name :
memberOf
```



```
2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7][  
cpm.saml.framework.impl.SAMLAttributesParser -:::- [parseAttributes] Delimiter not configured,  
Attribute=<memberOf> add value=<CN=TOR,DC=rtpaaa,DC=net>
```

Informações Relacionadas

[Release Note para o Cisco Identity Services Engine, 2.1 da liberação](#)

[Guia do administrador do Cisco Identity Services Engine, 2.1 da liberação](#)