

Acesso portal administrativo ISE com exemplo de configuração das credenciais AD

Índice

[Introdução](#)

[Pré-requisitos](#)

[Componenets usou-se](#)

[Configurar](#)

[Junte-se ao ISE ao AD](#)

[Selecione grupos do diretório](#)

[Permita o acesso administrativo para o AD](#)

[Configurar o admin group ao mapeamento do grupo AD](#)

[Ajuste permissões RBAC para o admin group](#)

[Alcance o ISE com credenciais AD](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve um exemplo de configuração para o uso do microsoft active directory (AD) como uma loja externo da identidade para o acesso administrativo ao Gerenciamento GUI do Cisco Identity Services Engine (ISE).

Pré-requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de versões 1.1.x ou mais recente de Cisco ISE
- Microsoft AD

Componenets usou-se

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

- Versão 1.1.x de Cisco ISE
- Liberação 2 de Windows Server 2008

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 a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Use esta seção a fim configurar para o uso de Microsoft AD como uma loja externo da identidade para o acesso administrativo ao Gerenciamento GUI de Cisco ISE.

Junte-se ao ISE ao AD

1. Navegue à **administração > ao Gerenciamento de identidades > fontes externos > diretório ativo da identidade**.
2. Dê entrada com o nome da loja do Domain Name e da identidade AD, e o clique **junta-se**.
3. Incorpore as credenciais da conta AD que pode adicionar e fazer mudanças aos objetos do computador, e clique a **configuração da salvaguarda**.

Selecione grupos do diretório

1. Navegue à **administração > ao Gerenciamento de identidades > > Add da identidade das fontes externas > do diretório ativo > dos grupos > diretório seletor do formulário dos grupos**.
2. Importe pelo menos um grupo AD a que seu administrador pertence.

Permita o acesso administrativo para o AD

Termine estas etapas a fim permitir a autenticação senha-baseada para o AD:

1. Navegue à **administração > ao sistema > ao acesso > à autenticação Admin**.
2. Da aba do **método de autenticação**, selecione a **senha baseada** opção.
3. Selecione o **AD** do menu suspenso da **fonte da identidade**.
4. Clique **mudanças da salvaguarda**.

Configurar o admin group ao mapeamento do grupo AD

Defina um admin group de Cisco ISE e trace-o a um grupo AD. Isto permite a autorização determinar as permissões baseadas papel do controle de acesso (RBAC) para o administrador baseado na membrasia do clube no AD.

1. Navegue à **administração > ao sistema > ao acesso Admin > aos administradores > aos grupos Admin**.
2. O clique **adiciona** no encabeçamento da tabela a fim ver a placa nova da configuração do admin group.

3. Dê entrada com o nome para o admin group novo.
4. No tipo campo, verifique a caixa de verificação **externo**.
5. Do menu suspenso dos **grupos externos**, selecione o grupo AD a que você quer este admin group traçar, como definido no diretório seletor agrupe a seção.
6. Clique **mudanças da salvaguarda**.

Ajuste permissões RBAC para o admin group

Termine estas etapas a fim atribuir permissões RBAC aos grupos Admin criados na seção anterior:

1. Navegue à **administração > ao sistema > ao acesso > à autorização > à política Admin**.
2. Do menu suspenso das **ações na política nova da inserção** direita, seleta **abaixo** a fim adicionar uma política nova.
3. Crie uma regra nova chamada **ISE_administration_AD**, trace-a com o admin group definido no acesso administrativo da possibilidade para a seção AD, e atribua-lhe permissões. Nota: Neste exemplo, o admin group chamado **Super Admin** é atribuído, que é equivalente à conta admin padrão.
4. **A salvaguarda do clique muda**, e a confirmação das mudanças salvar é indicada no canto inferior direito do GUI.

Alcance o ISE com credenciais AD

Termine estas etapas a fim alcançar o ISE com credenciais AD:

1. Saída do GUI administrativo.
2. Selecione **AD1** do menu suspenso da **fonte da identidade**.
3. Incorpore o nome de usuário e senha do base de dados AD, e do início de uma sessão.

Nota: Os padrões ISE à loja do usuário interno caso o AD for inacessível, ou as credenciais da conta usadas não existem no AD. Isto facilita o início de uma sessão rápido se você usa a loja interna quando o AD estiver configurado para o acesso administrativo.

Verificar

A fim confirmar que sua configuração trabalha corretamente, verifique o nome de usuário autenticado no canto superior direito do ISE GUI.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta

configuração.

Informações Relacionadas

- [Guia do Usuário do Cisco Identity Services Engine, liberação 1.1 - Controlando o acesso de Identities e Admin](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)