

Configuração do objeto de autenticação LDAP no sistema FireSIGHT

Contents

[Introduction](#)

[Configuração de um objeto de autenticação LDAP](#)

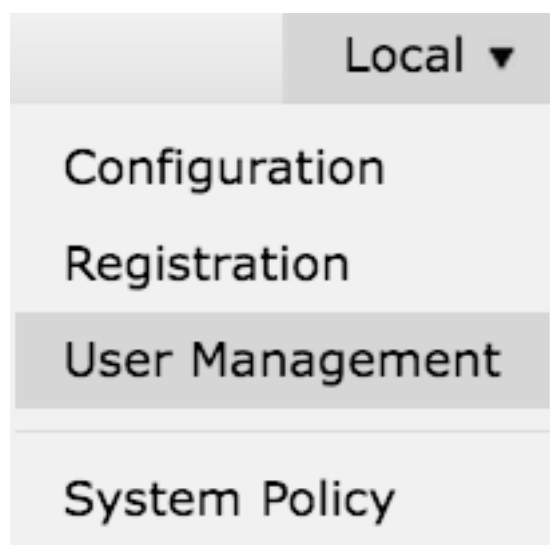
[Documento relacionado](#)

Introduction

Os Objetos de Autenticação são perfis de servidor para servidores de autenticação externos, contendo configurações de conexão e configurações de filtro de autenticação para esses servidores. Você pode criar, gerenciar e excluir objetos de autenticação em um FireSIGHT Management Center. Este documento descreve como configurar o objeto de autenticação LDAP no sistema FireSIGHT.

Configuração de um objeto de autenticação LDAP


1. Faça login na interface de usuário da Web do FireSIGHT Management Center.
2. Navegue até **Sistema > Local > Gerenciamento de Usuário**.



Selecione a guia **Autenticação de login**.



Clique em **Create Authentication Object**.

 Create Authentication Object

3. Selecione um **Método de Autenticação** e um **Tipo de Servidor**.

- **método de autenticação:** LDAP
- **Nome:** <Nome do objeto de autenticação>
- **Tipo de servidor:** MS Ative Directory

Note: Os campos marcados com asteriscos (*) são obrigatórios.

Authentication Object

Authentication Method	LDAP
Name *	<input type="text"/>
Description	<input type="text"/>
Server Type	MS Active Directory

4. Especifique o Nome do Host ou o Endereço IP do Servidor Primário e de Backup. Um servidor de backup é opcional. No entanto, qualquer controlador de domínio dentro do mesmo domínio pode ser usado como um servidor de backup.

Note: Embora a porta LDAP seja o padrão para a porta **389**, você pode usar um número de porta não padrão que o servidor LDAP esteja escutando.

5. Especifique os **Parâmetros Específicos do LDAP** conforme mostrado abaixo:

Tip: Os atributos de usuário, grupo e OU devem ser identificados antes da configuração de **parâmetros específicos de LDAP**. Leia [este documento](#) para identificar os atributos de objeto LDAP do Ative Directory para a configuração do objeto de autenticação.

- **DN base** - DN de domínio ou UO específico
- **Base Filter** - O DN de grupo do qual os usuários são membros.
- **Nome de Usuário** - Conta de representação para o DC
- **Senha:** <password>
- **Confirmar senha:** <password>

Opções avançadas:

- **Criptografia:** SSL, TLS ou Nenhum
- **Caminho de Carregamento do Certificado SSL:** Carregar a certificação CA (opcional)
- **Modelo de nome de usuário:** %s
- **Tempo limite (segundos):** 30

LDAP-Specific Parameters

Base DN * ex. dc=sourcefire,dc=com

Base Filter ex. (cn=jsmith), (|cn=jsmith), (&(cn=jsmith)((cn=bsmith)(cn=csmith*)))

User Name * ex. cn=jsmith,dc=sourcefire,dc=com

Password *

Confirm Password *

Show Advanced Options ▼

Encryption SSL TLS None

SSL Certificate Upload Path ex. PEM Format (base64 encoded version of DER)

User Name Template ex. cn=%s,dc=sourcefire,dc=com

Timeout (Seconds)

Na Configuração de política de segurança de domínio do AD, se o **requisito de assinatura do servidor LDAP** estiver definido como **Exigir assinatura**, SSL ou TLS deverá ser usado.

Requisito de assinatura do servidor LDAP

- **Nenhum:** A assinatura de dados não é necessária para vincular ao servidor. Se o cliente solicitar a assinatura de dados, o servidor a suportará.
- **Exigir assinatura:** A menos que TLS\SSL esteja sendo usado, a opção de assinatura de dados LDAP deve ser negociada.

Note: O lado do cliente ou o certificado da CA (certificado da CA) não é necessário para LDAPS. No entanto, seria um nível extra de segurança do certificado de CA carregado no Objeto de autenticação.

6. Especificar Mapeamento de Atributos

- **Atributo de acesso à interface do usuário:** sAMAccountName
- **Atributo de acesso do shell:** sAMAccountName

Attribute Mapping

UI Access Attribute *

Shell Access Attribute *

Tip: Se você encontrar a mensagem Usuários sem suporte na saída do teste, altere o **Atributo de acesso à interface do usuário** para userPrincipalName e verifique se o modelo Nome de usuário está definido como %s.

Unsupported Admin Users

The following administrator shell access users (3) were found with this filter but are invalid because their format is not supported for this appliance:

secadmin1 , secadmin2 , secadmin3

Unsupported Users

The following users (3) were found with this filter but are invalid because their format is not supported for this appliance:

secadmin1 , secadmin2 , secadmin3

*Required Field

7. Configurar Funções de Acesso Controlado por Grupo

Em **ldp.exe**, navegue para cada grupo e copie o DN do grupo correspondente para o Objeto de autenticação, como mostrado abaixo:

- **DN do Grupo <Nome do Grupo>: <group dn>**
- **Atributo de membro do grupo:** sempre deve ser **membro**

Exemplo:

- **DN do Grupo de Administradores:** CN=administradores de DC,CN=Grupos de segurança,DC=VirtualLab,DC=local
- **Atributo de membro do grupo:** membro

Um grupo de segurança do AD tem um atributo de **membro** seguido pelo DN de usuários membros. O número que precede o atributo **member** indica o número de usuários membros.

```
3> member: CN=secadmin3,CN=Users,DC=VirtualLab,DC=local; CN=secadmin2,CN=Users,DC=VirtualLab,DC=local; CN=secadmin1,CN=Users,DC=VirtualLab,DC=local;
```

8. Selecione **Mesmo que o Filtro Base** para o Filtro de Acesso Shell ou especifique o atributo **memberOf** como indicado na etapa 5.

Filtro de acesso Shell: (memberOf=<DN do grupo>)

Por exemplo,

Filtro de acesso Shell: (memberOf=CN=Usuários Shell,CN=Grupos de segurança,DC=VirtualLab,DC=local)

9. Salve o Objeto de Autenticação e execute um teste. Um resultado de teste bem-sucedido se parece com o seguinte:



Info



Administrator Shell Test:

3 administrator shell access users were found with this filter.

See Test Output for details.



Info



User Test:

3 users were found with this filter.

See Test Output for details.



Success



Test Complete: You may enter a test user name to further verify your Base Filter parameter.

Admin Users

The following administrator shell access users (3) were found with this filter:

secadmin1, secadmin2, secadmin3

Users

The following users (3) were found with this filter:

secadmin1, secadmin2, secadmin3

*Required Field

Save

Test

Cancel

10. Depois que o Objeto de Autenticação passar no teste, habilite o objeto na Política do Sistema e replique a política ao seu equipamento.

Documento relacionado

- [Identificar Atributos de Objeto LDAP do Ative Directory para Configuração de Objeto de](#)

Autenticação