



# GUIA DE CONFIGURAÇÃO

AUTENTICAÇÃO DO PROXY COM  
ACTIVE DIRECTORY USANDO LDAP

# GUIA DE CONFIGURAÇÃO

## Autenticação do proxy com o Active Directory usando LDAP

O Proxy do Netdeep Secure pode ser configurado para realizar a autenticação em um servidor Active Directory.

Acompanhe os passos a seguir para ativar esta configuração.

### 1. Preparando o Active Directory

---

Para que o Netdeep Cop possa realizar uma busca no servidor LDAP do Active Directory, este último deve ser configurado para que aceite operações anônimas. Isto é feito ativando-se o atributo dsHeuristics.

Com o programa “**ADSI Edit**” (parte do pacote Microsoft Windows Server 2003/2008 Support Tools) abra a chave “**CN=Directory Service,CN=Windows NT, CN=Services, CN=Configuration, <Domínio>**” em “**Configuration**”.

Entre nas propriedades da chave “**CN=Directory Service**” e encontre o atributo **dsHeuristics<sup>1</sup>**, colocando como valor “**0000002**”.

Reinicie o servidor.

### 2. Crie um usuário para conexão com o Active Directory

---

Utilizando o snap in “**Usuários e computadores do Active Directory**” crie um usuário comum (por exemplo: na chave , Users, crie o usuário proxy) para conexão com o Active Directory. Ele não precisa estar em nenhum grupo especial.

### 3. Configurando o Netdeep Secure

---

Na interface de administração do Netdeep Secure vá no menu “**Serviços**” → “**Proxy Web**”. Vá ao item “**Método de autenticação**” e selecione “**LDAP**”, clique em salvar para habilitar as opções de preenchimento.

Preencha as informações:

Base DN<sup>2</sup> : O Distinguished Name base para pesquisar pelos usuários.

Ex: **dc=dominio,dc=com**

Tipo LDAP<sup>2</sup> : Active Directory

Servidor LDAP: IP do servidor do Active Directory

Porta: 389

Nome de usuário Bind DN<sup>2</sup> : O Distinguished Name do usuário criado no tópico 2.

Ex: **CN=proxy,OU=Users,DC=dominio,DC=com**

Senha Bind DN: Senha do usuário criado no tópico 2.

Clique em “**Salvar**”.

**Método de autenticação**

Nenhum
  Local
  identd
  LDAP
  Windows
  RADIUS
  KERBEROS

---

**Configuração global de autenticação**

Número de processos de autenticação:

Cache de autenticação TTL (em minutos):

Limite de endereço IP por usuário:

Cache Usuário/IP TTL (em minutos):

Requer autenticação para fonte de endereços irrestrita:

Campo de autenticação:   
 Domínios sem autenticação (um por linha):

---

**Configuração LDAP comum**

Base DN:  Tipo LDAP:

Servidor LDAP:  Porta:

---

**Configuração Bind DN**

Nome de usuário Bind DN:  Senha Bind DN:

---

**Controle de acesso baseado em grupo**

Grupo é requerido:

Este campo pode ficar vazio.

Obs.: Caso queira liberar acesso para os usuários pertencentes a um grupo específico, informe no campo **“Controle de acesso baseado em grupo”** o Distinguished Name do grupo (Ex.: CN=Internet,OU=Users,DC=dominio,DC=com).

<sup>1</sup> Mais informações sobre as flags do dsHeuristics podem ser encontradas em:

<http://msdn.microsoft.com/enus/library/ms675656%28v=vs.85%29.aspx>

<sup>2</sup> Todas estas informações podem ser coletadas pelo **ADSI Edit**

#### 4. Para saber mais

<http://www.netdeep.com.br/secure/>