

## Password Management

The NetScreen Password Management option allows you to automatically relay vital password information directly to the IVE end-user. Additionally, it allows users to change their passwords when prompted to, or at will.

### Supported LDAP Directories

- Microsoft Active Directory/Windows NT
- Sun iPlanet
- Novell eDirectory
- Generic LDAP directories, such as IBM Secure Directory and OpenLDAP

### Supported Windows Servers

- Microsoft Active Directory
- Microsoft Active Directory 2003
- Windows NT 4.0

<b>Password Management Overview .....</b>	<b>1</b>
<b>Directory-Specific Information .....</b>	<b>2</b>
Microsoft Active Directory.....	2
Sun iPlanet .....	2
General.....	2
<b>Troubleshooting .....</b>	<b>2</b>
<b>LDAP Password Management Matrix.....</b>	<b>3</b>
<b>AD/NT Password Management Matrix.....</b>	<b>4</b>

### Benefits of the Combined Solution

The Password Management feature can be very helpful in environments where passwords have set expiration times, forcing users to frequently change their passwords. The Password Management feature also helps minimize tedious Help Desk calls. For example, end-users will not need to ask the Help Desk to reset their passwords because they were never informed that their passwords were about to expire.

## Password Management Overview

To enable Password Management on the IVE, either the UPG-Password Management Integration license or the Access Series Advanced license must first be applied to the IVE. Next, the Realm configuration must have the "Enable Password Management" option checked. Note: This option will only appear if the Authentication server for the Realm is of type LDAP or NT/AD.

Once enabled, the IVE performs a series of queries to determine user account information, such as when the user's password was last set, if his account is expired, and so forth. The IVE does this by using its internal LDAP or Samba client. Many servers, such as Microsoft Active Directory or Sun iPlanet, offer an Administrative Console to configure account and password options.

During login, the user may be informed if his password is expired or is about to expire. If expired, the user is prompted to change his passwords. If the password has not expired, the user may be allowed to sign in. After he has signed in, he may change his password from the Preferences page.

---

## Directory-Specific Information

The following sections list specific issues related to individual server types.

### Microsoft Active Directory

- Changes on the Active Directory domain security policy may take 5 minutes or more to propagate among AD domain controllers. Additionally, this information does not propagate to the domain controller on which it was originally configured for the same time period. This is a limitation of Active Directory.
- When changing passwords in Active Directory using LDAP, the IVE automatically switches to LDAPS, even if LDAPS is not the configured LDAP method. To support LDAPS on the Active Directory server, an SSL certificate must be installed into the server's "Personal Certificate Store". This can be done using the Microsoft Management Console (MMC) and selecting the "Certificates" Snap-In. Not only must the SSL certificate be valid and signed by a trusted CA, the CN in the certificate's "Subject" field must contain the exact hostname of the Active Directory server, for example: adsrv1.company.com.
- The "Account Expires" option in the User Account Properties tab only changes when the account expires, not when the password expires. As per the functional matrix (below), Password Expiration is calculated on-the-fly by using the Maximum Password Age and Password Last Set information retrieved from the User Policy and Domain Security Policy LDAP objects.

### Sun iPlanet

- When selecting "User must change password after reset" on the iPlanet server, the administrator must also reset the user's password before this function takes effect. This is a limitation of iPlanet.

### General

- The IVE only displays a warning about password expiry if the password will expire in 14 days or less. This message is displayed during each IVE sign in attempt. The warning message contains the remaining number of days, hours, and minutes that the user has to change his password before it expires on the server. The default value is 14 days; however, this is configurable and may be changed using the Realm → Authorization → Password configuration page.

## Troubleshooting

When troubleshooting, please provide any pertinent IVE logs, server logs, configuration information, and a TCP trace from the IVE. If LDAPS is being used, please switch to the "Unencrypted" LDAP option in the IVE LDAP server configuration while taking the LDAP TCP traces.

## LDAP Password Management Matrix

The following matrix describes the Password Management functions supported by NetScreen, their corresponding function names in the individual LDAP directories, and any additional relevant details.

Function	Active Directory	iPlanet	Novell eDirectory	Generic
Authenticate user	<b>unicodePwd</b>	<b>userPassword</b>	<b>userPassword</b>	<b>userPassword</b>
Allow user to change password if licensed and if enabled	Server tells us in bind response (uses <b>ntSecurityDescriptor</b> )	If <b>passwordChange == ON</b>	If <b>passwordAllowChange == TRUE</b>	✓
Log out user after password change	✓	✓	✓	✓
Force password change at next login	If <b>pwdLastSet == 0</b>	If <b>passwordMustChange == ON</b>	If <b>pwdMustChange == TRUE</b>	
Password expired notification	<b>userAccountControl == 0x80000</b>	If Bind Response includes OID <b>2.16.840.1.113730.3.4.4 == 0</b>	Check date/time value in <b>passwordExpirationTime</b>	
Password expiration notification (in X days/hours)	if <b>pwdLastSet - now() &lt; maxPwdAge - 14 days</b> (maxPwdAge is read from domain attributes) (IVE displays warning if less than 14 days)	If Bind Response includes control OID <b>2.16.840.1.113730.3.4.5</b> (contains date/time) (IVE displays warning if less than 14 days)	If <b>now() - passwordExpirationTime &lt; 14 days</b> (IVE displays warning if less than 14 days)	
Disallow authentication if "account disabled/locked"	<b>userAccountControl == 0x2 (Disabled)</b> <b>accountExpires</b> <b>userAccountControl == 0x10 (Locked)</b> <b>lockoutTime</b>	<b>Bind ErrorCode: 53</b> "Account Inactivated" <b>Bind Error Code: 19</b> "Exceed Password Retry Limit"	<b>Bind ErrorCode: 53</b> "Account Expired" <b>Bind ErrorCode: 53</b> "Login Lockout"	
Honor "password history"	Server tells us in bind response	Server tells us in bind response	Server tells us in bind response	
Enforce "minimum password length"	If set, IVE displays message telling user <b>minPwdLength</b>	If set, IVE displays message telling user <b>passwordMinLength</b>	If set, IVE displays message telling user <b>passwordMinimumLength</b>	
Disallow user from changing password too soon	If <b>pwdLastSet - now() &lt; minPwdAge</b> , then we disallow	If <b>passwordMinAge &gt; 0</b> , then if <b>now()</b> is earlier than <b>passwordAllowChangeTime</b> , then we disallow	Server tells us in bind response	
Honor "password complexity"	If <b>pwdProperties == 0x1</b> , then enabled. Complexity means the new password does not contain username, first or last name, and must contain characters from 3 of the following 4 categories: English uppercase, English lowercase, Digits, and Non-alphabetic characters (ex. !, \$, %)	Server tells us in bind response	Server tells us in bind response	

---

## AD/NT Password Management Matrix

The following matrix describes the Password Management functions supported by NetScreen.

Function	Active Directory	Active Directory 2003	Windows NT
Authenticate user	✓	✓	✓
Allow user to change password if licensed and if enabled	✓	✓	✓
Log out user after password change	✓	✓	✓
Force password change at next login	✓	✓	✓
Password expired notification	✓	✓	✓