NetIQ®

SecureLogin 8.8

Security Guide

December, 2019

Legal Notice

Contents

About this Book and the Library

The *Security Guide* is intended to help the SecureLogin administrators with several configurations guidelines. These guidelines can be used to enhance the security of a SecureLogin deployment.

It is recommended that the administrators frequently consult the SecureLogin Documentation (https://www.netiq.com/documentation/securelogin) and keep up to date on patches and versions of both SecureLogin and the host operating system.

Intended Audience

This book is intended for SecureLogin administrators. It is assumed that you have knowledge of the following:

- Certificate Authority (CA)
- Microsoft Active Directory
- Microsoft Management Console (MMC)
- Microsoft Group Policy Object Management Console (GPMC)
- Microsoft Windows operating systems
- Lightweight Directory Access Protocol (LDAP)
- Secure Socket Layer/Transport Layer Security (SSL/TLS)

1 Deployment Considerations

This section includes the following topics that explain basic considerations to make the SecureLogin deployment more secure.

- "Installing SecureLogin In Network Firewall" on page 7
- "Using AES for SSO Encryption" on page 7
- "Enabling Passphrase" on page 7

Installing SecureLogin In Network Firewall

SecureLogin can be installed within the network firewall as well as outside the network firewall.

Using AES for SSO Encryption

You should select the AES for the SSO data encryption. AES is more advanced and secure than 3DES.

Enabling Passphrase

A SecureLogin passphrase is a question and response combination used as an alternative form of identity verification. Passphrase functionality protects SecureLogin credentials from unauthorized access and enables users to access SecureLogin in offline mode. Passphrases can also be used as a substitute authentication mode if, for example, a user forgets his or her password. Depending on your preferences, SecureLogin passphrase questions can be generated by the administrator and, or the user.

IMPORTANT: Enabling passphrase provides the following benefits:

1. It disables administrators to impersonate users and gain access to their secret data. Hence, the **Passphrase Hidden** must be used only when the LAN administrators are highly trusted, as getting access to users' secret data may provide them access to other corporate systems.
2. It provides data encryption between the client and the LDAP server. Without the passphrase feature, the only protection available is ACL protection provided by the Directory server.

During installation, the passphrase security is enabled to enforce passphrase setup during the initial login. You can disable the passphrase policy by deselecting **Use Passphrase Policy** option in the **Advanced Settings** pane of the Administrative Management utility. If a passphrase has previously been configured, this dialog box does not display and the installation is complete.

On initial login to SecureLogin, all users are requested to save a passphrase response. It is important that this response is easy to recall because it cannot be viewed by anyone.

WARNING: Remember the passphrase answer. You cannot access the answer if you forget it.

To set up a passphrase:

1. Specify a question in the **Enter a question** field.
2. Specify an answer in the **Enter the answer** field.
3. Specify the answer again in the **Confirm the answer** field.
4. Click **OK**. Your passphrase is saved and SecureLogin is installed on the administration workstation.

2 Strengthening Certificates

This section provides information on how to install SecureLogin in the LDAP mode with or without the root CA certificates.

- "Installing SecureLogin In LDAP Mode With Root CA Certificate" on page 9

Installing SecureLogin In LDAP Mode With Root CA Certificate

Perform the following steps to install SecureLogin in the LDAP mode with root CA certificate. For detailed information see "Installing, Configuring, and Deploying in an LDAP Environment" in the "*SecureLogin Installation Guide*".

1. Log in to the workstation as an administrator.
2. Run the `NetIQSecureLogin.exe` file.
3. Accept the license agreement and click **Next**.
4. Select **NetIQ eDirectory with LDAP** as the datastore.
5. Click **Next**.
6. Click **Install**.
7. Click **Next**.
8. In the Custom Setup window, select the features you want to install.
9. Click **Next**.
10. In the **LDAP Server Information** window, specify the server address, port, and the root CA certificate path.

    NOTE: SecureLogin supports the following certificate formats:

    1. BASE64 (*.b64)
    2. PEM (*.pem)

    IMPORTANT: It is mandatory to specify the root CA certificate path when installing SecureLogin in the LDAP mode. Specifying the root CA certificate is also mandatory when migrating to the LDAP mode using `slMigrationHelper.exe`. Although, it is not recommended if you do not wish to specify the root CA certificate path, see "Installing SecureLogin in the LDAP Mode Without Root CA Certificate" on page 10 to install SecureLogin without a certificate.

Installing SecureLogin in the LDAP Mode Without Root CA Certificate

WARNING: Installing SecureLogin without a root CA certificate makes SecureLogin and the LDAP server open to security threats. It is not recommended to install SecureLogin without the root CA certificate.

Perform one of the following methods to install SecureLogin in the LDAP mode without the root CA certificate.

- "Installing SecureLogin in the LDAP Mode Without the Root CA Certificate Using Command Line" on page 10
- "Installing SecureLogin in the LDAP Mode Without the Root CA Certificate Using Response.ini (Silent Installation)" on page 11

Installing SecureLogin in the LDAP Mode Without the Root CA Certificate Using Command Line

Perform the following steps to install the SecureLogin in the LDAP mode without the root CA certificate:

1. Log in as an administrator.
2. Launch the command prompt.
3. Navigate to the location where the SecureLogin installer package is saved.
4. Run the `NetIQSecureLogin.exe` installer file with the `INSTALLWITHOUTCACERT=Yes` parameter. For example:

   ```
   NetIQSecureLogin.exe INSTALLWITHOUTCACERT=Yes
   ```

   NOTE: You can use the `INSTALLWITHOUTCACERT=Yes` parameter and continue the remaining installation with the GUI installer. For example, NetIQSecureLogin.exe /install INSTALLWITHOUTCACERT=Yes.

5. Perform the following steps to modify the registries. The registry modification is necessary to prevent SecureLogin to check for the root CA certificate.

   5a Click **Start > Run** to open the **Run** dialog box.

   5b Specify `regedit` and click **OK** to open **Registry Editor**.

   5c Navigate to the **HKEY_LOCAL_MACHINE > SOFTWARE > Novell > Login > LDAP** key.

   5d Right click and click **New > DWORD**.

   5e Rename the **DWORD** to **CACertNotProvided**.

   5f Edit the `CACertNotProvided` value to 1.

For more information on how to install SecureLogin using command line, see "Installing through the Command Line" in the "*SecureLogin Installation Guide*".

Installing SecureLogin in the LDAP Mode Without the Root CA Certificate Using Response.ini (Silent Installation)

IMPORTANT: Upgrading SecureLogin using the `response.ini` file is not supported.

Perform the following steps to install the SecureLogin in the LDAP mode without the root CA certificate using the `response.ini` file:

1. Log in as an administrator.
2. Specify `INSTALLWITHOUTCACERT=YES` in the `response.ini` file.
3. Launch the command prompt.
4. Navigate to the location where the SecureLogin installer package is saved.
5. To install SecureLogin on all the target machines with the `response.ini` file, run the following command.

   ```
   NetIQSecureLogin.exe /install X_PRIMARYSTORE=LDAP
   PATHTOISS="c:\temp\response.ini" /quiet
   ```

6. Perform the following steps to modify the registries. The registry modification is necessary to prevent SecureLogin to check for the root CA certificate.

   6a Click **Start > Run** to open the **Run** dialog box.

   6b Specify `regedit` and click **OK** to open **Registry Editor**.

   6c Navigate to the **HKEY_LOCAL_MACHINE > SOFTWARE > Novell > Login > LDAP** key.

   6d Right click and click **New > DWORD**.

   6e Rename the **DWORD** to **CACertNotProvided**.

   6f Edit the `CACertNotProvided` value to `1`.

For more information on how to install SecureLogin using command line, see "Installing SecureLogin in the LDAP Mode Without the Root CA Certificate Using Responsefile.ini (Silent Installation)" in the "*SecureLogin Installation Guide*".

3 Securing the Administration Access

This section provides information on how administrators can make the SecureLogin deployment more secure by restricting end users' access to administrative rights. The following table list the default and the recommended preferences for a more secure deployment. To access these configurations, open SecureLogin and click **Preferences**.

Table 3-1

Preferences	Default Value	Recommended
Add application prompts for WindowsAutomation (DotNet) applications	Yes	No
Allow "Close" option via system tray	Yes	No
Allow "Refresh Cache" option via system tray	Yes	No
Allow "Log Off" option via system tray	Yes	No
Allow "Work Offline" option via system tray	Yes	No
Allow application definition to be modified by users	Yes	No
Allow application definition to be viewed by users	Yes	No
Allow credentials to be deleted by users through the GUI	Yes	No
Allow credentials to be modified by users through the GUI	Yes	No
Allow users to (de) activate SSO via system tray	Yes	No
Allow users to backup/restore	Yes	No
Allow users to change passphrase	Yes	No
Allow users to modify names of Applications and Logins	Yes	No
Allow users to view and change Preferences	Yes	No
Allow users to view and modify API preferences	Yes	No

Preferences	Default Value	Recommended
Password protect the system tray icon	No	No
Provide API Access	Yes	No
Wizard mode	Yes	No
Add application prompts for Internet Explorer	Yes	No
Add application prompts for Mozilla Firefox	Yes	No
Add application prompts for Google Chrome	Yes	No
Add application prompts for web pages on mutation	No	No

4 Securing Single Sign-on Data

This section includes the following topic:

- "Securing SSO Data In Local Cache" on page 15
- "Securing SSO Data In Directory" on page 15

Securing SSO Data In Local Cache

Securing the Single Sign-on (SSO) data in local cache has the following three aspects:

1. The local cache file must have a sufficiently restrictive Access Control List (ACL).
2. When SecureLogin is installed with default cache file path, the ACL would be explicitly set under `%LOCALAPPDATA%`.
3. In case of a custom cache file path, the administrator must configure ACL for the custom path.

Securing SSO Data In Directory

SecureLogin stores sensitive data under directory attributes of the user object. Sufficiently restrictive ACL must be configured at the Directory level.

5 Strengthening TLS/SSL Settings

It is recommended to use TLS v1.2 and above for the SecureLogin communication with the following components.

1. Directory (Active Directory, eDirectory or LDAP compliant directory)
2. Advanced Authentication server
3. Privileged Account Manager server
4. Syslog server

SecureLogin initiates the SSL connection by default with TLS v1.2 protocol. You must configure the same TLS version on the corresponding server.

6 Restoring Previous Security Level After Upgrade

All protocols, ciphers, and configurations in all components are highly secure by default in SecureLogin 8.7 and later. If your SecureLogin deployment is configured with less secure settings, upgrading it to higher and then downgrading it back is not supported. The following are a few example scenarios.

- Downgrading the SSO data from AES to 3DES is not supported. Once the SSO data is encrypted to AES, downgrading it to 3DES may lead to data loss.
- From SecureLogin 8.7, SHA1 is replaced by SHA256 as the default hashing algorithm. SHA256 is more secure and trustworthy. SHA1 to SHA256 is a seamless migration and is available only if you were already using the default AES encryption.

  IMPORTANT: If you are using 3DES encryption then upgrading to SecureLogin 8.7 will not encrypt single sign-on data to SHA256. It remains in SHA1.

- After you install SecureLogin 8.7 that includes SHA256, you cannot downgrade to lower SecureLogin version which includes SHA1. If you downgrade from SecureLogin 8.7 to a previous version, SecureLogin will stop working. This issue occurs because the lower versions of SecureLogin can only process the SHA1 encryption, it does not process the SHA256 encrypted single sign-on data.