NetIQ SecureLogin 8.7 Release Notes

December 2018

NetIQ SecureLogin 8.7 enhances the product capability and resolves several previous issues.

Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure that our products meet all your needs. You can post feedback in the NetIQ SecureLogin forum on NetIQ Communities, our online community that also includes product information, blogs, and links to helpful resources.

The documentation for this product and the latest Release Notes are available on the NetIQ website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at the NetIQ SecureLogin documentation page. To download this product, see the NetIQ Downloads website.

1 What’s New?

This release includes the following:

1.1 SecureLogin Installation With the 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.

From SecureLogin 8.7 onwards, as part of security enhancement, SecureLogin LDAP server certificate validation is mandatory and it requires valid certificate configured on eDirectory server. Also, you must provide a valid root CA certificate on every workstation during SecureLogin installation. The installation fails if the valid root CA certificate is not specified. However, if you want to install SecureLogin without the root CA certificate, see Installing SecureLogin in the LDAP Mode Without Root CA Certificate in the *NetIQ SecureLogin Installation Guide*.

1.2 SecureLogin Is VMware Ready Certified

From this release, SecureLogin is a VMware certified application. SecureLogin works with VMWare virtual machine to deliver a more efficient, simple, and reliable single sign-on solution. It provides a single login experience to users accessing VMWare ESXi virtual machines and other VDI environments. The following list contains the supported VMware products:

- vSphere Hypervisor (ESXi)
- Horizon (with View)

For more information, see the SecureLogin Solution (https://marketplace.vmware.com/vsx/solutions/securelogin-8-6?ref=company) on VMware Solution Exchange.

1.3 SecureLogin Includes SHA256 As Default Hashing Algorithm

From this release 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. After you install SecureLogin 8.7 that includes SHA256, you cannot downgrade to 8.6.x which includes SHA1. For more information, see Section 3, “Installing or Upgrading,” on page 7 before you upgrade to SecureLogin 8.7.

NOTE: 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.

1.4 Support For Dynamic Control

From this release, SecureLogin provides successful single sign-on to windows that includes dynamic controls. The dynamic controls are the UI elements that can change their order or place of appearance in a window. These controls include check box, radio button, text fields or any UI element that require user interaction.

For more information on Dynamic Control Support, see Support for Dynamic Controls in *NetIQ SecureLogin Application Definition Guide*

1.5 Web Wizard Enhancements

From this release, the SecureLogin web wizard supports the following capabilities:

- The wizard automatically specifies `-noform` when applications do not contain a form ID or form name
- The wizard successfully differentiates between the name element and the ID element
- The wizard identifies the hidden element and appends them
- The wizard identifies the URLs on a page and click them.

1.6 Software Fixes

This release includes the following software fixes:

1.6.1 The SecureLogin Tray Does Not Open When Workstation Is Offline

Issue: When the **Password protect the system tray icon** option is enabled and workstation is offline then the SecureLogin tray does not open. The SecureLogin tray does not open even if you specify the correct password. This issue does not occur when workstation is connected to a network. (`Bug 1068129`)

Fix: With this release, the check condition for authentication in the offline mode is modified to fix this issue.

1.6.2 SecureLogin Does Not Display Directory Authentication Messages In Local Languages

Issue: SecureLogin displays the authentication failure/successful messages only in English language. These messages are displayed in English language even when the Windows language is not English. (`Bug 1091148`) (`Bug 1091874`)

Fix: In this release, the messages are translated to the system language.

1.6.3 SecureLogin Events Are Not Displayed In Proper Format

Issue: In the Event Viewer, the SecureLogin application events are displayed in unidentified format. This issue occurs because SecureLogin event logs are in UTF-8 format and Event Viewer requires UTF-16 format. In this case, Event Viewer converts the UTF-8 format logs to ANSI and displays. (`Bug 1091150`)

Fix: In this release, `slEventMessages.dll` is modified to convert the log inputs in correct format.

1.6.4 SecureLogin Stops Working And Does Not Start Again

Issue: SecureLogin stops working and fails to start again. SecureLogin starts only when the user deletes the single sign-on data. This issue occurs when users use a new smart card or a smart card with new certificate. This issue is fixed in this release. (`Bug 968117`)

1.6.5 Single Sign-on Script Is Case Sensitive In Internet Explorer

Issue: When using external variables in the single sign-on script for Internet Explorer, the variable name must be of same case as specified in the script. If the cases do not match, single sign-on fails. (`Bug 1104255`)

Fix: In this release, `slbroker.exe` is modified to fix this issue.

1.6.6 slWinSSO.exe Utilizes More CPU In Windows 10

Issue: In Windows 10, `slWinSSO.exe` utilizes more CPU for applications that generates large number of `WM_COMMAND` messages. This issue occurs even if the application is specified in the `exclude.ini` file. (`Bug 1108379`)

Fix: From this release, the debug binaries do not process the applications that are specified in the `exclude.ini` file.

1.6.7 SecureLogin Closes The Application And Displays An Error Message

Issue: When credentials are deleted for an application, SecureLogin prompts for credentials. When credentials are specified, the application stops working. This issue occurs because the `CRITICAL_SECTION` objects are not initialed before the `Lock` and `Unlock` operations. (`Bug 1108180`)

Fix: In this release, `IESSOWizardWorker.cpp` and `IESSOWizardWorker.h` files are modified to fix this issue.

1.6.8 The Type Command Does Not Process Strings That Contain Escape Sequences

Issue: If the username or password contains an escape sequence then the `Type` command of SecureLogin does not type the username or password correctly. (`Bug 1107118`)

Fix: In this release, the `strReplace` command is added to fix this issue. For more information on the `StrReplace` command, see StrReplace in *NetIQ SecureLogin Application Definition Guide*.

1.6.9 The SecureLogin Tray Does Not Open And An Error Message Is Displayed

Issue: When `slTray.exe` is opened, SecureLogin displays the `SecureLogin Datastore Broker has stopped working` error message. In the event viewer, `slBroker.exe` is listed as the faulty application for this issue. `slBroker.exe` stops working while obtaining profile and username from `moses.dll`. (`Bug 1106106`)

Fix: From this release, the destination buffer length calculations are corrected to fix this issue.

1.6.10 slWinSSO.exe Stops Working In Windows Server 2008 R2

Issue: The `slBroker.exe` service stops working while processing the Group Policy (GPO) data. (`Bug 1105642`)

Fix: From this release, the GPO data processing is re-factored and load functions are used to handle exceptions.

1.6.11 SecureLogin Displays Error Messages When Encrypted From 3DES to AES

Issue: SecureLogin displays error message when the encryption is changed from 3DES to AES. This issue occurs when a user is logged in to multiple systems simultaneously. (`Bug 1041755`)

Fix: From this release, `slBroker.exe` attempts multiple instantiations with sleep intervals.

1.6.12 SecureLogin Displays Error Message on Windows Start Up

Issue: SecureLogin displays the `Unable to Instantiate scriptbroker Error 80080005` message during Windows start up. This issue occurs when COM object instantiation awaits for user's HKCU availability. (`Bug 1095645`)

Fix: From this release, `slBroker.exe` attempts multiple instantiations with sleep intervals.

1.6.13 SecureLogin Stops Working In LDAP Secret Store Mode

Issue: SecureLogin stops working when installed in LDAP eDirectory mode with the Secret Store option enabled. The outdated libraries of Secret Store causes this issue. (`Bug 1047795`)

Fix: In this release, the `nsss.dll` Secret Store binary is modified to fix this issue.

1.6.14 SecureLogin Does Not Provide Login

Issue: SecureLogin specifies the username and password in the respective fields and displays the following error:

```
Operation failed. Invalid user ID or password
```

This issue occurs because AngularJS applications do not recognize the inputs received from SecureLogin. (`Bug 1103751`) (`Bug 998861`)

Fix: From this release, `slIESSO.exe` is modified and it notifies the changes to the AngularJS applications.

1.6.15 slWinSSO.exe Stops Working When An Existing Script Is Used

Issue: `slWinSSO.exe` stops working and does not provide single sign-on when an existing script is used. The existing script works on previous versions of SecureLogin. This issue occurs when the argument order is changed. (`Bug 1092375`)

1.6.16 SecureLogin Does Not Provide Single Sign-on When Control IDs Are Changed

Issue: SecureLogin fails to provide single sign-on to Windows that includes dynamic controls. Controls are the UI elements that require user interaction, for example, check box, radio button, text fields etc. (`Bug 1056459`)

Fix: In this release, new commands are added to create single sign-on scripts that fix this issue. For more information on Dynamic Control Support, see Support for Dynamic Controls in *NetIQ SecureLogin Application Definition Guide*.

1.6.17 slWinSSO.exe Stops Working While Processing eDirectory Attributes

Issue: `slWinSSO.exe` stops working when SecureLogin executes a script that contains eDirectory attributes. (`Bug 1098619`)

Fix: If you are using an attribute in the script, you must define the attributes in the user object. For more information, see Directory Attribute Variables in *NetIQ SecureLogin Application Definition Guide*.

1.6.18 Performance Issues With SecureLogin

Issue: The following issues occurred while using SecureLogin with ActivClient 7.1: (`Bug 1099610`)

1. SecureLogin stops working after selecting the correct Dynamic-link library file for Public Key Cryptography Standards.
2. `slBroker.exe` stops working while obtaining the certificate details.
3. `slDotnetSSO` binaries keep running in background even when SecureLogin is closed. It prevents SecureLogin to restart.
4. SecureLogin stops working without any error message.

Fix: In this release, several SecureLogin executables are modified to fix these performance issues.

1.6.19 SecureLogin Does Not Process the PIN Prompt Window

Issue: In Windows 10, SecureLogin does not process some windows. This issue occurs when the dialog is not ready for processing and `slDotNetSSO.exe` attempts to find UI elements on the window. (`Bug 1110187`)

Fix: In this release, a small processing time delay is added to fix this issue.

1.6.20 SecureLogin Prompts Users For Credentials In A Loop

Issue: In Internet Explorer, SecureLogin keeps prompting users to provide credentials.This issue occurs when application name stored in `setplat <app name>` is in different case than the application name stored in local cache. (`Bug 1110169`)

Fix: From this release, the `setplat` command is not case sensitive.

1.6.21 SecureLogin Wizard Does Not Differentiate Between Name and ID Inputs

Issue: The SecureLogin wizard does not differentiate between `name` and `ID` of input fields. It uses `ID` for `name`. (`Bug 920303`)

Fix: From this release, the SecureLogin wizard differentiates between `name` and `ID` of input fields. It uses `ID` over `name` only when `name` is not available.

2 System Requirements

For information about hardware requirements, supported operating systems, and browsers, see System Requirements for SecureLogin in *NetIQ SecureLogin Quick Start Guide*.

3 Installing or Upgrading

You can either upgrade from the previous versions of SecureLogin or perform a new installation. For information about how to install and how to upgrade, see NetIQ SecureLogin Installation Guide.

IMPORTANT: Ensure that you test SecureLogin 8.7 in your test environment before you upgrade from a previous version to the SecureLogin 8.7 version in your production environment. The downgrade from 8.7 to lower versions is not supported because SecureLogin 8.7 uses SHA256 for the single sign-on data encryption. If you downgrade from SecureLogin to 8.7 to a previous version, one of the following issue will occur:

1. If the passphrase is enabled, the lower version of SecureLogin will prompt you to specify the passphrase. After you specify passphrase, SecureLogin will stop working.
2. If the passphrase is disabled, the lower version of SecureLogin will stop working after the initial start.
3. If a user is logged on multiple systems with different versions of SecureLogin and one of the systems is upgraded to SecureLogin 8.7 then the lower versions of SecureLogin will stop working.

This issue occurs because the lower versions of SecureLogin can process only the SHA1 encryption. The lower versions do not process the SHA256 encrypted single sign-on data. Also, downgrade to a lower version does not resolve this issue because lower versions cannot decrypt the single sign-on data back to SHA1. Perform the following steps to workaround this issue:

1. Ensure that you have a SecureLogin backup from an older version before you perform this workaround.
2. Uninstall SecureLogin 8.7.
3. Delete the SecureLogin 8.7 user cache file.
4. Delete the user data in the object.
5. Install the desired older version of SecureLogin.
6. Restore the user data from an existing backup.

---

4 Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently researched. For release specific issues, see previous releases' release notes. If you need further assistance with any issue, please contact Technical Support.

4.1 SecureLogin LDAP Connection Does Not Restore and Single Sign-on Fails

Issue: When the connection between SecureLogin and the LDAP server is terminated, the following performance issues are observed: (Bug 1119284)

1. Right click on the SecureLogin tray icon and click **Advanced > Refresh cache**. After the cache refresh, the tray icon stops working and subsequent single sign-on attempts fail.
2. This issue occurs only when LDAP CA certificate is configured and the cache is refreshed when network is disconnected.

3. When the connection to the LDAP server is restored, the tray icon and single sign-on starts working.
4. This issue does not occur for other operations of the SecureLogin tray.

Workaround: There is no workaround for this issue.

4.2 SecureLogin Does Not Switch To A Working LDAP Server During Re-Authentication

Issue: When the connection between SecureLogin and the LDAP server is terminated, the following performance issues are observed: (`Bug 1116443`)

1. When the re-connection is established between SecureLogin and LDAP server and if the server to which initial connection was established in unavailable then SecureLogin does not connect to the other available server.
2. When SecureLogin is running and the primary LDAP server is not reachable then the LDAP re-bind during cache refresh fails.

Workaround: There is no workaround for this issue.

4.3 SecureLogin Does Not Delete Volatile Keys

Issue: If the web browser plug-ins are active when SecureLogin is upgraded, installed or uninstalled, then SecureLogin does not clear the volatile keys after a Citrix session is terminated successfully. These volatile keys are encrypted but contains sensitive data. (`Bug 1118878`)

Workaround: There is no workaround for this issue.

4.4 SecureLogin Displays Error Messages During Upgrade or Uninstall

Issue: When the web browser plug-ins are active during SecureLogin upgrade, install or uninstall, SecureLogin displays error message. (`Bug 1117726`)

Workaround: Do not use browsers or disable the plug-ins during upgrade/install/uninstall.Using browser plug-ins during installation process can cause error messages especially when DHTML preferences are enabled.

4.5 SecureLogin Displays Incorrect Error Messages In LDAP Mode

Issue: When SecureLogin in installed in the LDAP mode without a root CA certificate using the `INSTALLWITHOUTCACERT=YES` parameter, SecureLogin displays the following error: (`Bug 1118454`)

You are not logged into directory and SecureLogin unable to find any cached user data

In this scenario, SecureLogin must display a root CA certificate related error but it displays an incorrect error.

Workaround: There is no workaround to display the correct error message. However, users can successfully login to directory after they complete the configuration required to install SecureLogin without root CA certificate. For more information, see Installing SecureLogin in the LDAP Mode Without Root CA Certificate in the *NetIQ SecureLogin Installation Guide*

5 Legal Notices

For information about NetIQ legal notices, disclaimers, warranties, export and other use restrictions, U.S. Government restricted rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/. All third-party trademarks are the property of their respective owners.