NetIQ SecureLogin 8.5 Release Notes

October 2016

NetIQ SecureLogin 8.5 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?

SecureLogin 8.5 release includes the following:

NOTE: From this release onwards, the support for Secure Workstation is discontinued. Hence, you can use Desktop Automation Service (DAS) to perform any of the Secure Workstation functionalities.

1.1 Enhanced SecureLogin Single Sign-On Extension for Google Chrome

This release introduces version 8.5.0.0 of SecureLogin SSO extension for Google Chrome. The extension, **NetIQ SecureLogin SSO Extension** can be installed from the Chrome web store. You must use this extension to enable single sign-on for the applications launched through Chrome. For more details about installing the extension refer, Installing SecureLogin Browser Extensions.

1.2 Application Definition Wizard Support for Google Chrome

From this release, you can use Application Definition Wizard to add application definition for the applications launched in Google Chrome. However, you must have the **NetIQ SecureLogin SSO Extension** installed in Chrome to automatically detect and add application definition for single sign-on applications.

1.3 Generic Mozilla Firefox SSO Plug-In

From this release, there will not be a separate plug-in for every version of Mozilla Firefox. Instead there will be a generic Mozilla Firefox SSO plug-in which can be downloaded from the NetIQ product download site. For more information about installing the Mozilla Firefox plug-in refer, Installing SecureLogin Browser Extensions

This release supports only Mozilla Firefox version 50 or later.

1.4 Advanced Authentication Enhancements

- Support for the latest version of Advanced Authentication AA 5.4.
- Support for SecureLogin Advanced Authentication kiosk login in eDirectory mode.
- Support for second factor skipping feature of advanced authentication.
- Support to distinguish between Desktop Automation Service (DAS) tap off and the re-authentication tap in.
- Support for single tap to switch user in kiosk mode instead of double tap. To enable this feature, TapCardSwitchUser attribute value must be set to true. For more information about this attribute refer, DAS Actions and Descriptions

1.5 Password Recovery Support in DAS Environment

From this release, a forgotten password link is added to the DAS login screen for resetting the SecureLogin user password. To reset the password using this link, you must install Client Login Extension in your workstation.

1.6 Display the Logged in User Name on the Task Bar

You can identify the user who is currently logged into the SecureLogin with the help of the user name displayed in the task bar. This feature is useful in identifying the logged in user in the kiosk mode. Also, you can enable, disable and customize the user name displayed in the task bar by modifying the general preferences. For more information refer, Display SecureLogin User Name on the Task Bar.

1.7 Windows 10 Toast Notification

In windows 10 toast messages are used to notify the user of any SecureLogin actions instead of balloon notification.

1.8 Software Fixes

This release of NetIQ SecureLogin includes the following software fixes:

1.8.1 Single Sign-On Fails for Some Applications That Are Launched Through Google Chrome

Issue: Single sign-on for some web applications fails to work in Google Chrome, when SecureLogin has the DHTML monitor option enabled in the web preferences. But it is working as expected in Internet Explorer.(`Bug 1000566`)

Fix: This issue is fixed in this release.

1.8.2 Application Scripts That Are Generated in Internet Explorer Do Not Work in Google Chrome

Issue: When you launch an application in Google Chrome after generating the application definition script in Internet Explorer, SecureLogin enters the credentials and does not proceed with the submit operation. But this script works as expected in Internet Explorer.(`Bug 990949`)

Fix: This issue is fixed in this release.

1.8.3 SecureLogin Does Not Detect Excel Embedded Web Application

Issue: SecureLogin does not detect excel embedded web application for SSO.(`Bug 988075`)

Fix: Excel embedded web applications are supported in this release.

1.8.4 SecureLogin Does Not Detect the Check Box in the Right-Fax Web Application

Issue: When you Single Sign-on to Right-Fax web application with the wizard generated script, it does not uncheck the check box in the web page as expected. This prevents the SecureLogin from injecting the credentials.(`Bug 940858`)

Fix: This issue is fixed in this release.

1.8.5 The `Get Text` Command Returns Additional Information That Breaks the Script Execution

Issue: The `Get Text` command returns additional information from the web page along with the required text, which breaks the script execution.(`Bug 977332`)

Fix: With this release, the `Get Text` command is working as expected.

1.8.6 An Error is Displayed When Logging Into SecureLogin in AD or ADAM Mode.

Issue: In AD or ADAM mode, when user logs into SecureLogin `Unable to determine Cryptographic Service Provide from Security Preferences` error is displayed. This error occurs because SecureLogin by default is looking for a smart card instead of the credentials.(`Bug 978660`)

Fix: This issue is fixed in this release.

1.8.7 SecureLogin Is Unresponsive When Authenticating a User in Windows Terminal Server

Issue: In Windows terminal server, SecureLogin fails to detect the smart card for authentication and becomes unresponsive. You can continue to use SecureLogin only after deleting the SSO details of the user.(`Bug 968117`)

Fix: With this release, SecureLogin is working as expected.

1.8.8 An Error Is Displayed When You Close the Re-authentication Dialog Box

Issue: When the user clicks the close button on the top right corner of the SecureLogin re-authentication dialog box, a popup appears with the error message `Object reference not set to an instance of an object`. The user can ignore this error screen and continue to use the application without re-authentication.(`Bug 1001529`)

Fix: With this release, the close button in the SecureLogin re-authentication dialog box is removed.

1.8.9 Re-Authentication Fails When Using the PKI Generated Shared Key Pair

Issue: SecureLogin re-authentication fails with the error message `Signature verification failed` when using the generate keypair option during the PKI enrollment. This error occurs since SecureLogin does not support generated keypair.(`Bug 1001938`)

Fix: With this release, generate shared keypair is supported.

1.8.10 Fingerprint Authentication Fails When Using ISO Fingerprint Format

Issue: SecureLogin fingerprint re-authentication fails when using the Lumidigm Fingerprint device. The issue occurs because SecureLogin does not support the ISO fingerprint format. (`Bug 1003503`)

Fix: With this release, the ISO fingerprint format is supported.

1.8.11 Keyboard Actions Are Not Restricted When Work Station Is Locked in DAS Environment

Issue: In a DAS environment, even when the workstation is locked, user can switch focus away from the SecureLogin dialog box using keyboard actions. (`Bug 911504`)

Fix: With this release, Keyboard actions in the locked workstation is restricted.

1.8.12 DAS Stops Working When the `Kill-App` Action Has a Large Exception list

Issue: The DAS stops workings when the `except-app` attribute of the `kill-app` action has a long list.(`Bug 910181`)

Fix: With this release, you can have large exception list in `kill-app` action.

1.8.13 SecureLogin Allows Launching Application When There Is No User Logged Into SecureLogin

Issue: In a DAS environment, you can launch any application in the workstation even when no user is logged into SecureLogin. (`Bug 910184`)

Fix: With this release, SecureLogin will automatically kill any application that is launched when there is no active SecureLogin user in the DAS environment.

2 System Requirements

For more information about hardware requirements, supported operating systems, and browsers, see the NetIQ SecureLogin Quick Start Guide.

3 Installing or Upgrading to SecureLogin 8.5

You can either upgrade from the previous versions of SecureLogin or perform a new installation. For more information about upgrading from previous release, see Upgrading SecureLogin. For more information on installing SecureLogin, see NetIQ SecureLogin Installation Guide.

4 Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support.

4.1 SecureLogin Does Not Support Some of the Advanced Authentication Features

Issue: SecureLogin 8.5 does not support the following Advanced Authentication features:

1. Advanced Authentication offline feature and SecureLogin offline login in the Kiosk environment.
2. Advanced Authentication LDAP v3 support.
3. Citrix and Terminal server support with Advanced Authentication Device based login. (`Bug 1004420`)
4. Linked Authenticators.
5. HTTP Proxy Server support.
6. Non-Domain Joined Client support.

Workaround: No workaround is available.

4.2 SecureLogin Repair Operation Doesn't Resolve the Corrupted Advanced Authentication Endpoint Registry

Issue: SecureLogin repair operation doesn't resolve Advanced Authentication registry corruption.(`Bug 976540`)

Workaround: Run the SecureLogin modify operation to un-install and re-install the Advanced Authentication component.

4.3 SecureLogin Modify Operation Does Not Modify the Advanced Authentication Configuration If Advanced Authentication Was Installed Already

Issue: SecureLogin modify operation doesn’t change the Advanced Authentication configurations if it was already installed. (`Bug 976564`)

Workaround: Execute the SecureLogin modify operation to remove Advanced Authentication feature, and then run the SecureLogin modify operation again to add this feature to include the new configuration.

4.4 SecureLogin Advanced Authentication Integration Does Not Work with the SecureLogin Re-Authentication <Default> Method

Issue: SecureLogin Advanced Authentication integration does not work with the SecureLogin re-authentication <default> method. (`Bug 977163`)

Workaround: Select the Advanced Authentication listed methods.

4.5 Re-Authentication Issues when Users Have the Same Username in Multiple Advanced Authentication Repositories

Issue: For users who have the same username in different Advanced Authentication repositories, re-authentication fails and displays the message `Methods are not enrolled`. (`Bug 974768`)

Workaround: Select configured repository and make that the default Advanced Authentication repository.

4.6 Closing SecureLogin Kiosk Login Prompt Does Not Clear the SecureLogin Sys Tray Footprints

Issue: When a user cancels the SecureLogin kiosk login prompt, SecureLogin sys tray footprints are not cleared from the Windows notification panel. (`Bug 977561`)

Workaround: Hover the mouse on the footprints.

4.7 Google Chrome Does Not Allow Domain Authentication

Issue: When users access an application located on a specific domain by using Google Chrome, SecureLogin does not allow single sign-on to those applications. Users are required to manually provide the credentials. (`Bug 935212`)

Workaround: To workaround this issue, either enter the credentials manually or use Mozilla Firefox or Internet Explorer.

4.8 SecureLogin Manager Fails to Load the eDirectory Users and Objects After Changing the LDAP Secure/ Non-secure port in eDirectory

Issue: SecureLogin Manager fails to load the eDirectory users and objects when the following conditions are true:

- If SecureLogin is installed in the eDirectory LDAP mode
- If the value of the LDAP secure, and unsecure port is not set to default in eDirectory

This issue occurs because SecureLogin uses the default LDAP ports to get access to eDirectory. So, if the value of the LDAP port is changed in eDirectory, SecureLogin cannot access eDirectory data.

Workaround: To workaround this issue, change the port number in the registry at `HKCU\Software\Protocom\SecureLogin\LDAP Settings\NonSecureLDAPPort`.

4.9 The Novell Client Service Fails to Start When Logging in to Windows with Default Context to the Novell Client Credential Provider

Issue: When you log in to Windows by using the Novell Client credential provider and if the eDirectory context is set to `root`, Novell Client fails to load and displays an error. This happens only when SecureLogin is installed on your computer. (`Bug 948184`)

Workaround: To workaround this issue, you must select the appropriate context of the user to log in to Windows.

4.10 SecureLogin Displays an Error in Standalone Mode When the System Password is reset By Using Manage User Accounts

Issue: In standalone mode SecureLogin displays the error, `Incorrect PIN/ Password`. This issue occurs when the **Password Protect system tray** preference is enabled in the standalone mode and when you reset your user account password by using the **Manage User Accounts** option. (`Bug 920964`)

Workaround: To avoid error and data loss, it is recommended to change the password using the Ctrl+Alt+Del keys. This ensures that SecureLogin decrypts the updated password.

4.11 slmanager Allows You to Add Duplicate User-Defined Passphrase Questions

Issue: SecureLogin does not display error when you add duplicate user-defined passphrase questions in the slmanager. However, when you relaunch slmanager it will not display the duplicate entries. (`Bug 992575`)

Workaround: You can ignore this duplication, it does not affect the functionality of SecureLogin.

4.12 slmanager Does Not Display the Tree With User Objects and Domain Names When Using eDirectory 9.0

Issue: SecureLogin with eDirectory 9.0 launches the slmanager successfully, but does not display the tree with all the user objects and domain names. This is due to an issue in eDirectory 9.0. (`Bug 1005832`)

Workaround: There is no workaround for this issue at this time.

4.13 DAS Configuration File is Replaced With the Default Template File After Upgrade

Issue: When you upgrade SecureLogin, the DAS configuration file (action.xml) is replaced with the default DAS template file. Since the configuration file is replaced, you will lose all the customization made in the file. (`Bug 1006120`)

Workaround: To workaround this issue, you need to take a backup of the existing DAS `action.xml` file from the location `C:\Program Files\NetIQ\SecureLogin\Desktop Automation Services` and restore it after upgrading SecureLogin.

4.14 `Initializing LDAP` Error Appears in slmanager

Issue: When you uninstall SecureLogin in LDAP mode and reinstall SecureLogin in Active Directory or Novell Client mode, the error `Error Initializing LDAP` appears in the slmanager.This error occurs because the system registry content is not deleted properly during reinstallation. (`Bug 1006583`)

Workaround: To workaround this issue, delete the registry settings at `HKEY_LOCAL_MACHINE\SOFTWARE\Protocom` and install SecureLogin in AD or Novell Client mode.

4.15 Cannot Log Into SecureLogin When installed in eDirectory LDAP Mode with SecretStore

Issue: In Windows 10 and Windows 2012 R2, you cannot use SecureLogin when you have installed secureLogin in eDirectory LDAP mode with SecretStore. (`Bug 1005177`)

Workaround: There is no workaround for this issue at this time.

4.16 SecureLogin Does Not Perform Submit Operation for Specific Applications in Internet Explorer

Issue: When SecureLogin is performing single sign-on for some applications in Internet Explorer, after injecting the login credentials secureLogin does not perform the submit operation. The submit operation is not performed because the submit field is not identified by the SecureLogin.(`Bug 1006700`)

Workaround: To workaround this issue, modify the application definition to identify the submit button using key strokes. For information about modifying the application definition refer, Using the Application Definition Wizard to Modify an Application Definition

4.17 The SecureLogin Performance Is Affected When Performing Single Sign-On for Specific Web Applications In Google Chrome

Issue: When performing single sign-on for web applications which has many advertisements and DHTML events in Google chrome, multiple SecureLogin chrome processes (slnativehost.exe) are created which maximizes the CPU usage and affects the SecureLogin performance. (`Bug 1005177`)

Workaround: To workaround this issue, you must disable the DHTML monitor option in the SecureLogin web preferences or use a third party ad-blockers to block the advertisements.

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/.