NetIQ SecureLogin 9 Release Notes

June, 2021

NetIQ SecureLogin 9 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 SecureLogin forum on our community website that also includes product information, blogs, and links to helpful resources. You can also share your ideas for improving the product in Ideas Portal.

For more information about this release and the latest release notes, see the NetIQ SecureLogin documentation page. Note that SecureLogin 9 documentation is available on the Micro Focus domain. For SecureLogin documentation versions prior to 9, see NetIQ Documentation.

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.

NetIQ SecureLogin 9 Overview

SecureLogin streamlines user authentication by providing a single secure login experience for all your desktop applications. For more information about SecureLogin, see *NetIQ SecureLogin Overview Guide*.

SecureLogin 9 introduces support for single sign-on and multi-factor authentication to enterprise workstations and applications. This release provides a new component, ***SecureLogin Advanced Edition*** and support for Windows Hello for Business, to serve this purpose. With this feature, SecureLogin extends advanced capabilities, such as public cloud adoption and hybrid deployments. It helps to provide multi endpoint support in the future.

Windows Hello and Windows Hello for Business integrations enable organizations to provide password-less workstations and multi-factor authentication to end-users for a seamless single sign-on experience.

This release leverages the Risk Service feature of NetIQ Advanced Authentication to strengthen the security for SecureLogin kiosk and application logins.

What's New

This release includes the following new features and enhancements:

- SecureLogin Advanced Edition
- Support for Windows Hello for Business
- Context-aware SecureLogin Kiosk and Re-authentication

SecureLogin Advanced Edition

This release introduces the SecureLogin server, SecureLogin Advanced Edition, to use Azure Active Directory (Azure AD) as an identity provider. As organizations are moving towards cloud-based identity providers, Advanced Edition is developed to support Azure AD. Advanced Edition will also be capable of supporting other cloud-based identity providers in the future. Using Advanced Edition, you can seamlessly migrate from an Active Directory environment to an Azure AD environment.

Advanced Edition is also useful when you are deploying SecureLogin for the first time and want to use Azure AD as the identity provider.

For more information Advanced Edition and how to deploy it, see *SecureLogin 9 Advanced Edition Installation and Configuration Guide*.

Support for Windows Hello for Business

Windows Hello for Business replaces passwords with multi-factor authentication on users' devices. It consists of an authentication method that is tied to the device and uses a biometric or PIN. SecureLogin 9 supports integrating Windows Hello for Business. After the integration, you can use the Windows Hello for Business method to protect the SecureLogin icon and re-authenticate applications.

With this release, SecureLogin is enhanced to access the datastore using a biometric or PIN. When Windows Hello for Business is configured in you environment, SecureLogin provides users a seamless single sign-on experience to their devices.

For more information, see "Support for Windows Hello for Business" in the *NetIQ SecureLogin 9.0 Administration Guide*.

Context-aware SecureLogin Kiosk and Re-authentication

If SecureLogin is installed with Advanced Authentication, you can use the risk policy configured in Advanced Authentication to login using SecureLogin kiosk and re-authenticate users when they access applications containing sensitive data. The risk policy evaluates the risk level during each access attempts using contextual information. For example, contextual information can be IP address and device information.

You can define an appropriate action for each risk level, such as granting access with simple authentication or asking for additional multi-factor authentication.

For more information, see “Using the Risk Policy of Advanced Authentication” in the *NetIQ SecureLogin 9.0 Administration Guide*.

Known Issues

The following issues are currently being researched for SecureLogin 9.0:

- Seamless Login Fails in Windows Hello for Business Certificate Trust Model When a User Tries to Log in with Password
- Seamless Login Fails After a Password Change or Password Reset on Windows Hello for Business Integrated Machines
- Windows Hello for Business Does Not Work if a User Tries to Log In from Multiple Devices
- Password Authentication Does Not Work in the Offline Mode on Windows Hello for Business Integrated Machines
- SecureLogin Fails to Load with the Passphrase Prompt When the Password Is Expired or Changed
- Object-based Search Does Not Work in SLManager
- (SecureLogin Advanced Edition) The ?syspassword Variable Does Not Get Updated After Changing the Password Through Ctrl+Alt+Del

Micro Focus strives to ensure that our products provide quality solutions for your enterprise software needs. If you need assistance with any issue, visit Micro Focus Support, then select the appropriate product category.

Seamless Login Fails in Windows Hello for Business Certificate Trust Model When a User Tries to Log in with Password

If a passphrase is configured for a user, and the user tries to log in using the password, the following issue occurs in the certificate trust model of authentication:

- **On the devices integrated with Windows Hello for Business and passphrase enabled:** Seamless login fails, and SecureLogin prompts to enter the PIN followed by the passphrase.
- **On the devices integrated with Windows Hello for Business and passphrase disabled:** Seamless login fails, and SecureLogin prompts to enter the PIN.

Seamless Login Fails After a Password Change or Password Reset on Windows Hello for Business Integrated Machines

When a PIN, biometric, or Windows Hello for Business method is configured, and users log in using their password, SecureLogin prompts them to enter the PIN followed by the passphrase. This issue occurs only in the certificate trust model of authentication.

Use a method configured for Windows Hello for Business.

Windows Hello for Business Does Not Work if a User Tries to Log In from Multiple Devices

If a user tries to log in from multiple devices or different locations, Windows Hello for Business seamless login fails. No workaround is available.

Password Authentication Does Not Work in the Offline Mode on Windows Hello for Business Integrated Machines

When a user logs in using the password, the user is prompted to specify a passphrase. In the offline mode, even after specifying the correct passphrase, SecureLogin does not load and authentication fails. This issue happens when the user password is changed or expired and the passphrase is changed.

No workaround is available.

SecureLogin Fails to Load with the Passphrase Prompt When the Password Is Expired or Changed

SecureLogin failed to authenticate with the passphrase prompt in the following scenarios:-

- When an Azure Active directory user was created, and the user did not perform self-password change during the first login.
- The administrator changed the user password, and the user did not perform self-password change in the subsequent login

Workaround: Log in to Azure portal to change the expired password and then log in from the Windows Azure AD joined machine to load SecureLogin.

Object-based Search Does Not Work in SLManager

Perform the search using the **Search Base** and **Search Filter** fields. To view these fields, click **Configuration** and select **Display Search**.

(SecureLogin Advanced Edition) The ?syspassword Variable Does Not Get Updated After Changing the Password Through Ctrl+Alt+Del

When a user changes the Azure AD password through Ctrl+Alt+Del, a web browser console is launched as the machine is joined to Azure Active Directory. After changing the password, the `?syspassword` variable does not get updated and SSO scripts, which use the network credentials, stop working.

During the subsequent login to the machine, SecureLogin prompts for the passphrase answer (if the passphrase is enabled).

Workaround:

1. The User must log out from the machine and log in with the new password to get the SecureLogin `?syspassword` variable updated.
2. If the passphrase is enabled, the user must enter the passphrase answer for SecureLogin to unlock the SSO data and re-encrypt with the new password.

Resolved Issues

The following issues have been resolved in SecureLogin 9.0:

ID	Module	Description
228224	Single Sign-On Assistant	SecureLogin single sign-on stops working in Firefox when many instances of slNativeHost are running.
277138	Client General	After changing the password, the new one is not available when the user logs in the next time. A prompt for a failed password is displayed.
226302	Seamless Sign-on	After migrating SecureLogin from the eDirectory mode to the AD mode, the SecureLogin login scripts do not work.
268097	SSO IE	Internet Explorer 11 hangs when the **DHTML monitor on web pages** preference is enabled.
222116	Client General	Security filtering does not work when SecureLogin is configured via GPO.
220602	SmartCard	Not able to unlock the user datastore by using the smartcard. Only username and password can be used for unlocking.
226762	Client General	After enabling SecureLogin SSO, the Windows-based application becomes slow.
258190	Install	When SecureLogin is installed in the GUI mode, responsefile.ini and log.txt files are not created in the NSLFiles folder.
219967	SSO Windows	After upgrading to SecureLogin 8.7, type -raw writes only the first character ($username) to NXClient (Windows application).
220835	Client General	SecureLogin Credential Manager (SlCredman.dll) is not notified about the password change when the password is synced between eDirectory and AD through the OES client. As a result, syspassword does not pick the changed password. This issue occurs in the AD mode.
227272	Citrix Terminal Server Support	syspassword does not pick the changed password in the Citrix mode.
228199	Client General	After installing SecureLogin on Windows Server 2012R2 with administration tools, Remote Desktop Protocol (RDP) stops working. Not able to log in to the server by using RDP.
314097	Client General	When the password is changed by using Ctrl+Alt+Del, and Identity Manager is used to syncing AD password changes to the eDirectory LDAP store for SecureLogin, the SecureLogin SSO password is not updated. **Fix:** Create a SyncDelay DWORD with value '1'under `HKLM\SOFTWARE\Novell\Login\LDAP`.
301078	Client General	Seamless authentication does not work as expected when VPN is connected. After the user connects to VPN, SecureLogin prompts to specify the credentials manually for the first login attempt.

System Requirements

For information about hardware requirements, supported operating systems, and browsers, see *NetIQ SecureLogin System Requirements*.

Installing or Upgrading SecureLogin 9.0

After purchasing SecureLogin 9.0, download the software and the license from the Software License and Download (https://sld.microfocus.com/) portal. For information about how to download the product from this portal, watch the following video:

http://www.youtube.com/watch?v=esy4PTVi4wY

For information about how to install or upgrade, see *SecureLogin 9.0 Installation Guide*.

Supported Upgrade Paths

To upgrade to SecureLogin 9, you must be on one of the following versions of SecureLogin:

- 8.7
- 8.8
- 8.8.1

Upgrade or migration from SecureLogin 8.6, 8.5, 8.1, 8.0, or 7.0 might work, but it is not tested. Ensure that you test the upgrade from SecureLogin 8.6, 8.5, 8.1, 8.0, or 7.0 to SecureLogin 9.0 in your test environment before you upgrade in your production environment.

Contacting Micro Focus

For specific product issues, contact Micro Focus Support at https://www.microfocus.com/support-and-services/.

Additional technical information or advice is available from several sources:

- Product documentation, Knowledge Base articles, and videos: https://www.microfocus.com/support-and-services/
- The Micro Focus Community pages: https://www.microfocus.com/communities/

Legal Notice

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