Client for Open Enterprise Server Phase II
Advanced Authentication Integration Behavior

VERSION 20181109.1
Intention for Behavior with Phase II Integration

Using a workstation with only the NetIQ Advanced Authentication Client for Windows installed, the credential provider experience must be able to perform a Windows account logon in response to having successfully performed an Advanced Authentication logon. The same is true on a workstation using the "Phase 1" integration with Client for Open Enterprise Server, which was made available in March 2017 starting with Client for Open Enterprise Server 2 SP4 (IR5).

In both of these cases, it is the NetIQ CredentialProvider.dll which is providing the credential provider experience. This NetIQ Advanced Authentication credential provider maintains and has access to Windows account logon information as part of the Advanced Authentication repository user data.

For an Advanced Authentication repository that is Active Directory-based, the Windows logon information is the same as the LDAP user and password. In the case of a non-Active Directory-based repository, the non-domain Windows account logon information is stored as additional user data associated with the repository user.
Intention for Behavior with Phase II Integration (continued)

For the Client for Open Enterprise Server “Phase 2” integration behavior, there will be eDirectory credential information stored as part of the Advanced Authentication user data, similar to how the stand-alone Windows workstation case is handled by Advanced Authentication.

Meaning in addition to however the Windows account logon information is being maintained for a particular Advanced Authentication user, the Client for Open Enterprise Server will save eDirectory credential data that is separate from and in addition to the Windows account logon information.

The key points here are that the Windows username and password and the eDirectory username and password need not necessarily be in sync, although they can be. Also, the administrator could turn off “Phase 2” integration behavior at any time, and the Advanced Authentication user could still be successfully used by “Phase 1” or even Advanced Authentication Client for Windows-only configurations, to perform a successful Windows-only logon using Advanced Authentication, using the Windows account information that was being maintained even during “Phase 2” behavior.
Intention for Behavior with Phase II Integration
(continued)

There are three core design goals for the “Phase 2” integration with the Client for Open Enterprise Server.

- Allow using the Client for Open Enterprise Server’s NCCredProvider for the Windows credential provider experience, instead of the NetIQ Advanced Authentication credential provider.

- Enable utilizing Advanced Authentication to perform eDirectory logins through the Client for Open Enterprise Server.

- In addition to the eDirectory logins, use NCCredProvider to continue supporting exactly the same Windows account logon that is possible using the NetIQ Advanced Authentication credential provider.

To clarify this last point, this means that a customer using “Phase 2” integration could – at any time – disable “Phase 2” behavior and return to “Phase 1” integration behavior. Or could even remove the Client for Open Enterprise Server entirely, to have only the Advanced Authentication Client for Windows installed. Or could simply use the same Advanced Authentication user, but on a workstation which is using “Phase 1” integration, or simply doesn’t have the Client for Open Enterprise Server installed at all.

And the customer would be able to continue logging into their Windows workstation using Advanced Authentication, without being re-prompted or re-saving any Windows account logon-related information. Because the Advanced Authentication information being utilized and maintained for the Windows account logon when “Phase 2” and NCCredProvider is in use intends to be exactly the same Windows account logon information the NetIQ credential provider expects to utilize and maintain, too.

Meaning the customer doesn’t need to have “a separate Advanced Authentication environment for the Client for Open Enterprise Server workstations” that intend to perform eDirectory authentication. They can create a separate repository if desired, but they are not required to.
Behavior WITHOUT Client for Open Enterprise Server (only Advanced Authentication client installed or enabled)

Before starting to describe the Client for Open Enterprise Server “Phase 2” integration behavior with Advanced Authentication, we will first describe and confirm a couple relevant behaviors of the environment when only Advanced Authentication Client for Windows is installed.

In order to then more usefully contrast and compare the Client for Open Enterprise Server integration behavior against this behavior, as presented later in the document.

Full Credential Provider Experience at Logon
The Advanced Authentication Client for Windows credential provider (NetIQ’s CredentialProvider.dll) asks for an Advanced Authentication username only:
Behavior WITHOUT Client for Open Enterprise Server
(only Advanced Authentication client installed or enabled)

Full Credential Provider Experience at Logon
(continued)

The Advanced Authentication Client for Windows credential provider then presents the Advanced Authentication factor(s) required for that user.

Upon a successful Advanced Authentication logon, the credential provider performs a Windows-only logon using a Windows account name and Windows account password stored and associated with the Advanced Authentication identity.

When an Active Directory-based user repository is being used by Advanced Authentication, and the Windows workstation is a member of the Active Directory domain, then there is not any additional prompting expected for the Windows account logon.

The Advanced Authentication user identity DN is the Active Directory user DN in this case, and the LDAP password known to Advanced Authentication is the Active Directory user’s password.
Behavior WITHOUT Client for Open Enterprise Server
(only Advanced Authentication client installed or enabled)
(continued)

Full Credential Provider Experience at Logon
(continued)

For stand-alone Windows workstations (meaning the non-Active Directory-joined machines), or when using a non-Active Directory-based user repository, the Advanced Authentication client must simply store a user-specified Windows user account name and user-specified Windows user account password.

This is the Windows username and password that will be retrieved in response to a successful Advanced Authentication logon, as opposed to the inherent Active Directory-specific user association that occurs in the Active Directory use case.

If during logon the Advanced Authentication client determines that the Windows password or account name stored by the Advanced Authentication client is no longer the correct username or password for logging into Windows, or if the Windows account information has never been stored before by the Advanced Authentication client, then the user will be prompted to supply the current Windows account name and password.
Behavior WITHOUT Client for Open Enterprise Server  
(only Advanced Authentication client installed or enabled)  
(continued)

CredUI Experience from User's Desktop

This usage mode of the credential provider occurs when prompting for Windows account credentials for a mapped drive or when elevating an application under UAC. Because an Advanced Authentication logon is required in order to retrieve the Windows account credentials, the CredUI scenario must also present an Advanced Authentication logon.

When handling the CredUI scenario, the NetIQ CredentialProvider prompts for an Advanced Authentication username only, and upon successfully passing the authentication factors for the specified user, retrieves the same Windows credentials that would have been retrieved during a workstation logon.

Unlike the full credential provider experience at logon where the Advanced Authentication factor user interfaces are shown full-screen by the credential provider, in the CredUI case the Advanced Authentication factor user interfaces are shown in a desktop window.
Behavior WITHOUT Client for Open Enterprise Server (only Advanced Authentication client installed or enabled) (continued)

Change Password Experience

Invoking the CTRL-ALT-DEL “Change Password” option causes the Advanced Authentication credential provider to first present the “login” experience, in order to verify that the interactive user is the person who controls the account for which the password is about to be changed.

The user must successfully complete all the authentication factors for the Advanced Authentication user in order to proceed with the password change attempt.
Behavior WITHOUT Client for Open Enterprise Server (only Advanced Authentication client installed or enabled) (continued)

Change Password Experience (continued)

Once the Advanced Authentication login factors have been successfully completed, the user is prompted to provide the new password and to confirm the new password.

The “old password” is not required, because the existing password on the Windows account has been provided by the Advanced Authentication login.

After providing the new password and confirming the new password, the credential provider performs the password change and confirms the results.

Upon successfully changing the Windows account password, not only has the actual Windows account password been changed, but the Windows account information enrolled with Advanced Authentication has been updated to reflect the new password as well.
Behavior with Client for Open Enterprise Server
Phase 2 Advanced Authentication Integration

Full Credential Provider Experience at Logon

The Client for Open Enterprise Server credential provider (NCCredProvider) will prompt for the eDirectory ("Network") username as the primary username the user must specify.

This is the same behavior Client for Open Enterprise Server has when Advanced Authentication integration is not enabled. This is different from the Advanced Authentication Client for Windows credential provider (NetIQ's CredentialProvider), which prompts for the Advanced Authentication username as the primary username the user must specify.

With “Phase 2” integration enabled, the password field normally shown by the Client for Open Enterprise Server credential provider is disabled by default, because an Advanced Authentication login is about to be performed, and may or may not involve a password at all. This is the same behavior as the Advanced Authentication Client for Windows credential provider, which does not show a password field.
In the “Show Advanced Options” dialog, the “eDirectory” tab continues to allow for the user to specify whichever eDirectory tree and user context they intend to login with. This is the same Client for Open Enterprise Server behavior that exists even without Advanced Authentication integration enabled.

A new tab, the “Advanced Authentication” tab, allows the user to specify the specific Advanced Authentication user they intend to use to perform their Advanced Authentication logon.

Similar to the “Windows” tab behavior, if the user never visits the “Advanced Authentication” tab or never specifies a specific username, the Advanced Authentication username will default to being the same as the eDirectory username that was specified.

A default “Repository:” can be saved in the login profile, and a default for new users can be saved in the “Default” system login profile, similar to when a specific default eDirectory tree name is desired for new users.
Proceeding with the credential provider logon attempt, the next experience the user will see are the user interface(s) of the Advanced Authentication factor(s) that are required for the Advanced Authentication user logon.

This portion of the logon process, although now being initiated by the Client for Open Enterprise Server’s credential provider (NCCredProvider), will be similar to the full screen Advanced Authentication factor user interfaces presented by the NetIQ CredentialProvider.

The Advanced Authentication logon must succeed in order to proceed on to the actual eDirectory and Windows logon attempts.
Behavior with Client for Open Enterprise Server Phase 2 Advanced Authentication Integration (continued)

Full Credential Provider Experience at Logon (continued)

When the eDirectory login information stored by Advanced Authentication for the specified eDirectory user is already up to date, then the eDirectory login will proceed immediately and transparently after the successful Advanced Authentication logon, without any additional eDirectory-related prompting.

If the eDirectory password stored by Advanced Authentication no longer represents the correct password, or if the eDirectory password for the specified eDirectory user simply has never been stored before by Advanced Authentication, then the user will be prompted to supply the current eDirectory password.

```
 eDirectory Password Required

 The eDirectory password must be synchronized.
Enter the current eDirectory user password.

 OK  Cancel
```

Again, this is similar to the scenario with the Advanced Authentication Client for Windows when supporting stand-alone Windows workstations, and the Windows account logon information has changed or has never been stored before.
Behavior with Client for Open Enterprise Server Phase 2 Advanced Authentication Integration (continued)

Full Credential Provider Experience at Logon (continued)

When an Active Directory-based user repository is being used by Advanced Authentication, and the Windows workstation is a member of the Active Directory domain, then there is not any additional prompting expected for the Windows account logon, and it will proceed transparently.

For stand-alone Windows workstations, or when using a non-Active Directory user repository, if the Windows account name or password stored by Advanced Authentication is no longer the correct username or password, or if the Windows account information has never been stored before by Advanced Authentication, then the user will be prompted to supply the current Windows account name and password.

This is similar to the prompt that occurs for Client for Open Enterprise Server in non-Advanced Authentication scenarios, whenever the eDirectory account password is not successful for performing the Windows account logon and the user must be prompted to enter the correct Windows account password.

The Windows credentials entered here to complete a successful Windows account logon will also become enrolled with Advanced Authentication. Such that they are automatically supplied for transparent Windows account logon during future Advanced Authentication logins.
Behavior with Client for Open Enterprise Server Phase 2 Advanced Authentication Integration (continued)

**eDirectory-only Login from User Desktop**

Invoking an eDirectory-only login from the user’s desktop will present the Client for Open Enterprise Server’s traditional eDirectory login dialog. In addition to the standard “eDirectory” tab, the “Advanced Authentication” tab will be present in the same manner that the credential provider “Show Advanced Options” had presented this new tab.

So in addition to specifying a different eDirectory tree or user, a different Advanced Authentication user can be specified prior to proceeding with the login attempt.

The Advanced Authentication factor(s) user interface(s) in this case will be presented in a non-full screen window on the user’s desktop, rather than the full screen mode used during the credential provider login.
Behavior with Client for Open Enterprise Server Phase 2 Advanced Authentication Integration (continued)

eDirectory-only Login from User Desktop (continued)

When the eDirectory login information stored by Advanced Authentication for the specified eDirectory user is already up to date, then the eDirectory login will proceed immediately and transparently after the successful Advanced Authentication logon, without any additional eDirectory-related prompting.

If the eDirectory password stored by Advanced Authentication is no longer the correct password, or if the eDirectory password for the specified eDirectory user has never been stored before by Advanced Authentication, then the user will be prompted to supply the current eDirectory password.

![eDirectory Password Required]

The eDirectory password must be synchronized. Enter the current eDirectory user password.

[OK] [Cancel]

Again, this is similar to the scenario with the Advanced Authentication Client for Windows when supporting stand-alone Windows workstations, and the Windows account logon information has changed or has never been stored before.
Behavior with Client for Open Enterprise Server Phase 2 Advanced Authentication Integration (continued)

CredUI Experience from User's Desktop

With the Client for Open Enterprise Server “Phase 2” integration enabled to employ Advanced Authentication to login to eDirectory, it is still necessary to also support Advanced Authentication for Windows-only credential scenarios too, such as the CredUI prompt from Windows.

Even with the Client for Open Enterprise Server “Phase 2” integration enabled, this scenario will continue to be handled by the NetIQ CredentialProvider, same as when the Advanced Authentication Client for Windows is installed without the Client for Open Enterprise Server.

Meaning the CredUI scenario will continue to prompt for an Advanced Authentication username only, and upon successfully passing the authentication factors for the specified user, retrieves the same Windows credentials that would have been retrieved during a workstation logon.
Behavior with Client for Open Enterprise Server Phase 2 Advanced Authentication Integration (continued)

Workstation Unlock Behavior

When unlocking a workstation with Client for Open Enterprise Server Phase 2 integration behavior enabled, the credential provider will show the user credential based on their eDirectory user name, and with the password field disabled. Similar to the original workstation login to eDirectory, and also similar to the Change Password screen which will be described later.

An Advanced Authentication logon will be performed using the same Advanced Authentication user which logged this user into eDirectory, and the workstation will become unlocked using the Windows account credentials retrieved from that successful Advanced Authentication logon.
Behavior with Client for Open Enterprise Server Phase 2 Advanced Authentication Integration (continued)

Client Properties Configuration Options
The configuration options for “Advanced Authentication” in the Client for Open Enterprise Server configuration properties will be as follows.

“Enabled” means the “Phase 2” behaviors described are all enabled. The Client for Open Enterprise Server credential provider will be used. An Advanced Authentication login will be required in order to login to eDirectory and/or Windows, or to unlock the workstation, or to initiate a password change.

Alternatively, in addition to setting “Advanced Authentication” to “Enabled”, if the existing “Client Logon” parameter is set to “Off”, this means “do not use the Client for Open Enterprise Server credential provider.”

The result will be “Phase 1” behavior, where the NetIQ credential provider is presented. If the “Login with Third-Party Credential Provider” parameter is set to “On”, then a password-based eDirectory login will be performed using the Windows account password. Again, this is in line with the “Phase 1” behavior previously available.

“Disabled” means all Advanced Authentication integration behaviors are disabled.

In addition to the pre-existing “Client Logon” option referenced above, there is also now a new “Change Password Allowed” parameter.

Setting “Change Password Allowed” to “Off” when “Client Logon” is “On” will prevent the Client for Open Enterprise Server credential provider from offering the ability to change the eDirectory or Windows password.

Enabling such an option would only be appropriate to prevent users from initiating password change from the Windows workstation. Which presumes that the network environment has some other portal or method by which the eDirectory and Windows account password changes should be managed.
Behavior with Client for Open Enterprise Server Phase 2 Advanced Authentication Integration (continued)

Change Password Behavior

With Advanced Authentication set to “Enabled”, the behavior of the CTRL-ALT-DEL “Change Password” option will be changed. The fields for entering the existing and new passwords will not shown, and the user will simply hit “Submit” to begin the password change process for the eDirectory user shown.

An Advanced Authentication logon will be performed, and is required, in order to proceed with the Change Password process. Once the Advanced Authentication logon is successfully completed, then the user will be presented with the Client for Open Enterprise Server “Change Password” dialog that allows for changing the eDirectory password and/or Windows account password.
Behavior with Client for Open Enterprise Server Phase 2 Advanced Authentication Integration (continued)

Installation Behavior

The installation behavior has effectively not changed as compared to the Client for Open Enterprise Server's “Phase 1” integration behavior with Advanced Authentication.

Which means when starting with the “Custom Installation” pathway:

In the “Custom Installation” pathway, in addition to the previous NMAS-related options that already existed, there are two Advanced Authentication component options.

All components are dependent on the previous component. Meaning you can not install Advanced Authentication Device Services without installing the Advanced Authentication Client; you can not install the Advanced Authentication Client without installing NMAS; etc.
Behavior with Client for Open Enterprise Server
Phase 2 Advanced Authentication Integration
(continued)

Installation Behavior
(continued)

Note that the new Advanced Authentication options will NOT be selected by default during an interactive installation. But their selection and installation can be controlled using the INSTALL.INI in the Client for Open Enterprise Server installation set, same as the NMAS and NICI options.

When “Advanced Authentication Client” has been selected, an additional configuration screen will be provided:

The first selection will be “credential provider.” If “Client for Open Enterprise Server credential provider” is selected, this corresponds to Client settings of “Advanced Authentication” set to “Enabled” and “Client Logon” set to “On”. Which is “Phase 2” behavior.

If “NetIQ Advanced Authentication credential provider” is selected, this corresponds to Client settings of “Advanced Authentication” set to “Enabled”, “Client Logon” set to “Off”, and “Login with Third-Party Credential Provider” set to “On”. Which is “Phase 1” behavior.

If a specific Advanced Authentication server DNS name is specified on this screen, it will be written to the config.properties for the Advanced Authentication Client. This configuration file is stored under "C:\ProgramData\NetIQ\Windows Client\config.properties".

The Advanced Authentication logon will obtain its configuration from the config.properties file setting, or will fall back to attempting automatic DNS-based discovery if the config.properties is not configured.

A specific Advanced Authentication event name can also be specified for the config.properties configuration, in case an event other than the default “Windows logon” even needs to be specified.
Known Issues and Limitations
for Client for Open Enterprise Server (IR11 Beta 20181108a) build

1. Setting "Advanced Authentication" back to "Disabled" in the Client Properties after having installed Advanced Authentication support during SETUP.EXE will currently result in an undefined behavior. Leaving "Advanced Authentication" enabled once it has been turned on is recommended. Switching "Client Logon" between "Off" and "On" is supported, and provides control of the "Use Client for Open Enterprise Server credential provider" (On) versus "Use NetIQ Advanced Authentication credential provider" (Off) behavior outside of SETUP.EXE.

2. Computer Only Logon "Change Password" case is showing an empty "Old Password" field, rather than having the Advanced Authentication-enrolled Windows account password populated.

3. The “Change Password Allowed” parameter in Client Properties does not control the offering of Change Password behavior at this time. Changing this setting will not have any effect.