
Considerations When Upgrading IVE version 2.x to 3.0

IVE version 3.0 introduces a new process for authenticating and authorizing users. IVE version 3.0 supports the 2.x authentication and authorization (AA) process as a **legacy mode**. By default, when you upgrade an existing 2.x IVE system to 3.0, the IVE continues to use the 2.x AA process. We strongly encourage existing customers, however, to migrate to the new authentication and authorization process introduced in 3.0, which is the **standard mode** of 3.0. This document describes what happens to your system data when you run IVE version 3.0 in standard mode and what to expect during the upgrade process. This document is intended for use by customers with existing 2.x deployments.

Changes to system data	1
Upgrading to the 3.0 service package.....	2
Verifying user accessibility to the IVE	3

Changes to system data

Just like in the version 2.x AA process, the version 3.0 AA process requires administrators to define servers against which user credentials are authenticated and groups which define the resources and tasks users are authorized to access and perform. Even so, the 3.0 Administrator Console menus have changed somewhat and there are some differences in the functionality of servers, groups, and local users. Before upgrading a 2.x IVE to version 3.0, read about these differences in Chapter 2, “Upgrading IVE version 2.x to 3.0,” in the 3.0 *Administration Guide* manual. In particular, note the following about what happens to system data when you change from legacy to standard mode:

- All system configuration data is retained. System configuration data includes all system settings, authentication server settings, and network settings.
- All Administrators group data is retained. Administrator data includes local records, authentication settings, and group authorization settings defined for the Administrators group.
- All authorization group data is retained. Authorization group data includes session, access control list, feature, bookmark, messaging, and application data.
- All **local user records created for the Users group or a subgroup are *not* retained in the standard mode**. These records are preserved in legacy mode, however, so if you switch back to this mode, the IVE has access to the records.

In 2.x, local user records exist within the context of IVE authorization groups—local users are considered “members” of the Users group and other subgroups. In 3.0, IVE authorization groups do not include members; rather the IVE dynamically maps verified users to an authorization group per session according to the authentication server instance settings. For more information about this behavior, read Chapter 5, “Administering IVE Authentication and Authorization,” in the 3.0 *Administration Guide* manual.



- All **user preference, bookmark, and cookie data is *not* retained in the standard mode.** This data is preserved in the legacy mode, however, so if you switch back to this mode, the IVE has access to this data.

Important: To continue using a local database for user authentication, you must re-create each user record within an IVE local authentication database. See Chapter 5, "Administering IVE Authentication and Authorization," in the 3.0 *Administration Guide* manual for details. A future release of the IVE will enable you to import local user records as you can in version 2.x.

Upgrading to the 3.0 service package

The process for upgrading your IVE to version 3.0 is the same as installing any other service package with the following caveats:

1. The time it takes to install the service package varies and can be quite long.
2. The URL to access the Administrator Console after installing the service package must be appended with /admin.

To upgrade your IVE to the 3.0 service package and run the IVE in standard mode:

1. Download the 3.0 service package and corresponding release notes from the Neoteris Support Site: <https://support.neoteris.com>.
2. Review the release notes to become familiar with any current issues related to the upgrade process.
3. Begin monitoring the IVE so that you can track its status during installation.

To monitor the IVE, open a command prompt and ping the IVE using the -t switch, which causes the ping command to repeat until stopped, in the format:
ping a.b.c.d -t, where a.b.c.d is the IVE machine IP address.

The IVE replies to this ping while it is online. When the service package installation begins, the IVE becomes unreachable, which is shown in the command prompt. When the installation completes, the IVE services restart, and when the IVE is back online, it replies to the ping command.

We strongly recommend that you also monitor the upgrade process via the IVE serial console. By doing so, you will see exactly when the IVE reboots and other activity. If the upgrade is successful, the main menu that allows you to modify system settings displays. If the upgrade fails, you will see other information that can be used by Neoteris Support to help determine where the failure occurred.

4. Install the service package through the Administrator Console. Wait until the service package is installed before continuing.
5. After the service package installation completes, go to a browser and enter the IVE URL followed by /admin to access the administrator sign-in screen. The URL is in the format: <https://a.b.c.d/admin>, where a.b.c.d is IVE machine IP address.
6. In the sign-in screen, enter the your administrator username click **Sign In**. The Administrator Console appears.



7. Navigate to the **System > Settings > General** page and verify that the 3.0 service package was installed by reviewing the version information shown in the **System Software Pkg Version** field. If the 3.0 service package is not listed, repeat the service package installation process and continue to monitor the IVE through a command prompt.
8. If you obtained a new license, navigate to the **System > Settings > License** page, enter your company name and license code in the appropriate fields, and click **Enter**.
9. Navigate to the **System > Settings > Sign-In Options** page, clear the **Enable legacy mode** checkbox, and then click **Save Changes**. The Administrator Console begins running the 3.0 user interface.

Verifying user accessibility to the IVE

After you install service package 3.0 and disable legacy mode, you should verify that users can still access the IVE. End-users who are authenticated by an external authentication server may sign in to the IVE from the same URL. Any local users that were defined in the 2.x Users group or a subgroup will no longer be able to sign in unless you re-create their local user records within a local IVE authentication database. See Chapter 5, "Administering IVE Authentication and Authorization," in the 3.0 *Administration Guide* manual for details.

To verify user accessibility in version 3.0:

1. Navigate to the **Authentication & Authorization > Authentication Servers** page. From the drop-down list, select **IVE Local Authentication** and then click **Create**. The **New IVE Local Authentication Server** page appears.
2. In the **Name** field, enter **test** and then click **Save Changes**. The **Group Mapping** and **User** tabs appear.
3. Select the **Users** tab and then click **New**. The **New Local User** page appears.
4. Create a test user by entering a username and a password, and then click **Create User**. The test user is added to the IVE local authentication database called "test."
5. Go to a desktop workstation and enter the IVE URL in a browser. The URL is `https://a.b.c.d`, where a.b.c.d is the IVE machine IP address. When prompted with the security alert to proceed without a signed certificate, click Yes. The Neoteris IVE sign-in screen for end-users appears.
6. Enter the username and password you created for the test user and then click **Sign In**. The IVE home page appears.
7. Under **Browse Web**, enter a URL and click **Browse** to make sure users can access the IVE.
8. In the main menu, click **Windows Files** and then browse to a share and try to download and upload a file. For more information, click the **Help** link at the top of the IVE home page.

After verifying user accessibility, your Neoteris IVE is operational! Sign in to the Administrator Console again to finish configuring your IVE system, including verifying authentication server configurations, reviewing authorization group and access control settings, and re-creating local user records, if needed. Make sure to consult *Administration Guide* version 3.0, which is available from the Administrator Console (version 3.0) **Help** link and as part of the 3.0 service package on the Neoteris Support site.