SOFTWARE DOCUMENT

NiagaraAX 2013 Security Updates

In late 2013, the initial release of AX-3.8 occurs, which includes all the station security-related improvements incorporated in the earlier security-oriented 2013 *update releases* of NiagaraAX, as follows:

- AX-3.7 *update 1* release — denoted in this document as "AX-3.7u1" for 3.7.*1nn* builds.
- AX-3.6 and AX-3.5 *update 4* releases— denoted as "AX-3.6u4" for 3.6.*4nn* builds, and as "AX-3.5u4" for 3.5.*4nn* builds, respectively.

For background details on update terms above, see "Update release level from build-number" on page 16.

Note: *For proper security, we* strongly recommend *all existing jobs running AX-3.7, AX-3.6, and AX-3.5* upgrade to these update releases *as soon as they become available. Even stronger system security can be achieved in an upgrade to AX-3.8. For a related details, see "Improvements and changes in AX-3.8" on page 5.*

To increase system security, starting in the update releases, *change* were made to NiagaraAX *station password storage*. These changes affect *upgrades* of systems that transition from "pre-update NiagaraAX releases" to AX-3.8 or any update release (AX-3.7u1 or later, AX-3.6u4 or later, and AX-3.5u4 or later).

In addition, after a system is updated to these current releases, these changes can[1] affect how you should perform some *station backup*, *copy*, or *restore* operations.

This document explains these changes and also provides upgrade considerations, as well as methods to use when performing ongoing station backup, copy, and restore operations.

The following sections provide more details:

[1] Improvements were made in AX-3.8 when doing station backup, copy, and restore operations that help simplify things as compared to doing similar operations with any of the update releases (AX-3.7u1, AX-3.6u4, AX-3.5u4). These differences are noted in various sections of this document.

Improvements to the security of stored passwords

In all of the new and updated NiagaraAX releases in 2013, significant changes were made to the encoding and storage of station passwords, to stay up to date with security best practices. New and updated releases now use *three different formats* to store passwords in a station’s database (`config.bog` file):

- **Hashed**
  The safest way to deal with passwords is to not store them at all, but instead store a *hash* of the passwords created with a cryptographically-strong, one-way, algorithm (PBKDF2-HMAC-SHA256). Therefore, passwords that do not need to be transmitted to other systems, like all those for Users in the UserService, are stored as hashes.
- **Encrypted (AES-256)**
  Some station services need to store passwords in order to communicate as *clients* to other hosts, such as email servers, LDAP servers, and other NiagaraAX stations (FoxService). For these passwords, a strong, two-way encryption algorithm like AES-256 is used, where the encryption key used is stored *separately from the station database file* (`config.bog`). This way, an attacker with access to the station file cannot learn the passwords it contains.
- **Legacy**
  In select cases, station passwords are stored as in the old (pre-update release) *legacy* format.
  - First, any station database saved by an older NiagaraAX version has all passwords stored in this legacy format. However, if a host with updated NiagaraAX starts a station from that file, it immediately *converts* the passwords to the two new formats above, and then *re-saves* that file.
  - Second, when editing station database files *offline* in Workbench, any password changes made (new or updated) are stored in this legacy format. However, note that in this case too, after starting the station, it converts these passwords to the new, stronger formats.
  - Third (and in AX-3.8 only), when using the platform Station Copier to save (copy) a station, all client (encrypted) passwords are automatically *decrypted* and stored in portable format in the `config.bog` file. This provides better “portability” of the station database. Again, after starting the station, these passwords are automatically converted to the new AES-256 encryption.

Note: *Once a station converts passwords to the new, stronger, hashed or encrypted storage formats, if you save that station database and attempt to run in it an earlier NiagaraAX (pre-update) release, it will fail at startup. This happens because the older software does not understand the new password storage.*

If for some reason you do need to downgrade a station for such usage, you must edit that `config.bog` *file* offline in Workbench, *re-entering* all password values, *and then resave it.*

When upgrading systems there are related considerations you should know about (and prepare for). Also, *after* upgrading and when archiving stations for making modifications and copying back to the original host, keep in mind the following things about the passwords stored in saved files.

- User passwords are unrecoverable
- Portability of stored passwords

User passwords are unrecoverable

Because only one-way hashes are stored for station user passwords, they cannot be recovered when forgotten. However, they can be reset by admin users when the station is running, or by editing an offline copy of the station database in Workbench (and then subsequently re-installing that edited station).

Portability of stored passwords

Passwords stored in a `config.bog` as *hashes* or the *legacy* format are “portable”. This means when the `config.bog` is used by another host, these passwords continue to work as they did on the original host. Note station *users* (all User components under the station’s User Service) use password hashing.

However (*in update releases*) all "client" passwords stored in a `config.bog` in the new *encrypted* format are *not portable*. If the `config.bog` is used by a host that doesn't have the encryption key that was used to store them originally, these passwords will not be usable, at least as-is. However, if you copy (install) that station file to a new host, start the station, then re-enter those client password values, the encrypted storage is properly "re-keyed", and those passwords will then work.

Note: *In AX-3.8, improvements were made in the portability of client passwords in a station that is used in different hosts, making such operations unnecessary. See "Improvements and changes in AX-3.8" on page 5.*

The *importance* of portability arises in the two different methods to archive a station:

- **Station backup**
  This is initiated from either Workbench or a Supervisor's Provisioning mechanism, or directly from the BackupService in the station. A station backup results in a single distribution (`.dist`) file.
- **Station copy**
  This is done using the platform Station Copier tool. A station copy results in a `config.bog` file, plus typically other files, all under the station's folder (file space).

The difference is that *backup* `.dist` *files contain the key for the encrypted passwords*, whereas *station copies* (`config.bog`) files *do not*.

Caution *Be sure to keep backup* `.dist` *files in a secure location. They have always contained sensitive information, for example a station's* `config.bog` *file. They may also contain sensitive host platform information. In 2013 update releases (AX-3.7u1, AX-3.6u4, AX-3.5u4) or later, this includes files mentioned above.*

When using an *update release* to perform station archives (backups, copies) and restoring the same, you should keep this difference in mind. Note in some cases it is desirable to transfer the encryption key along with the station database (for example, restoring or replacing to the same host). Yet in other cases, this is an unacceptable weakening of security. For more details, see "Station archiving changes" on page 7.

Note: *In a AX-3.8 system working with AX-3.8 hosts, these station archiving considerations do not apply. Station backups and copies are more straightforward. See "Improvements and changes in AX-3.8" on page 5.*

Upgrade considerations

Any system with a "pre-update release" Supervisor that transitions to an update release (or AX-3.8) for the *first time* has a few extra steps involving the Supervisor station. See the following sections:

- "System-wide release level for security" on page 3
- "Upgrading a system" on page 3

System-wide release level for security

For any multi-station job to be properly secure with one of the 2013 security update releases or AX-3.8, *all hosts* must implement at least a security update release. Typically all hosts will all be at the *same* release level (recommended)—for example all at AX-3.8, or all at AX-3.7u1, or all at AX-3.6u4.

However, if for some reason a subordinate JACE needs to remain at an earlier revision level than the Supervisor, say at AX-3.5 (the *minimum* level recommended), it should be upgraded to at *least* AX-3.5u4. This provides optimum system security, while all JACEs maintain communications with the Supervisor.

Note that AX-3.8 uses the same improved station password storage as the update releases. Therefore, a system that you have already upgraded to any of these 2013 security update releases (AX-3.7u1, AX-3.6u4, or AX-3.5u4) is already "password compatible" with AX-3.8.

Upgrading a system

Except where noted, an upgrade of an existing AX-3.7, AX-3.6, or AX-3.5 job to the same-revision "update release" (AX-3.7u1, AX-3.6u4, or AX-3.5u4) should go much like any other "maintenance release" system upgrade. In this scenario, hosts should not need license upgrades.

If you are upgrading a system from a lower-revision level, say from AX-3.5 to AX-3.8 or to AX-3.7u1, the procedure is much the same, but you need to purchase *license upgrades* for all hosts before the upgrade.

Upgrading a system to a Security Update release (or AX-3.8)

The basic steps in performing this upgrade are as follows:

Step 1 Using your existing Workbench, backup all stations including the Supervisor.

Step 2 Stop the Supervisor station.

Step 3 Install the new updated Workbench to your PC and also Supervisor.

Select the install option for "this Workbench to be used as an installation tool".

Note: *In the Workbench install options, be sure to select "Copy Settings from Latest Version Installed". If for some reason you do not see this option, see the section "Copying items from previous install" on page 4.*

Step 4 Start the new update Workbench and start the Supervisor.

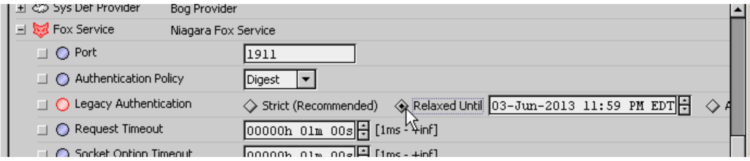
Note: *In AX-3.8 Workbench, all* **`Open Platform`** *and* **`Open Station`** *choices default to "open with SSL". In most cases, you need to change the connection "Type" to regular (non-SSL), unless an upgrade from an initial AX-3.7 release where SSL was previously configured. Following any upgrade to AX-3.7u1 or later, SSL configuration is highly recommended. For related details, see the* SSL Connectivity Guide.

Step 5 In Workbench, open the running Supervisor station (Fox connection).

Step 6 In the Supervisor station, open the property sheet of its **`NiagaraNetwork`**. (**`Config`** > **`Drivers`** > **`NiagaraNetwork`**).

Step 7 Expand the **`FoxService`** and look for a new property **`Legacy Authentication`**.

Step 8 Change **`Legacy Authentication`** from the default "Strict" to "Relaxed Until" (shown below) and then **`Save`**. For further details, see "Fox Service properties" in the NiagaraAX *Drivers Guide*.



⊞ Sys Def Provider — Bog Provider
⊟ Fox Service — Niagara Fox Service
□ ○ Port — 1911
□ ○ Authentication Policy — Digest ▼
□ ○ Legacy Authentication — ◇ Strict (Recommended) ◆ Relaxed Until 03-Jun-2013 11:59 PM EDT ◇ A
□ ○ Request Timeout — 00000h 01m 00s [1ms - +inf]
□ ○ Socket Option Timeout — 00000h 01m 00s [1ms - +inf]

Note: *This should be a* temporary setting only. *Reset this to "Strict" in the Supervisor's FoxService after you finish upgrading NiagaraAX in the subordinate JACE hosts (represented in the Supervisor's NiagaraNetwork).*

Typically you use the platform Commissioning Wizard to update these JACEs, as described in the next step.

(Background): Relaxed authentication in the Supervisor's FoxService allows its subordinate JACEs to continue to communicate with the Supervisor until they have been upgraded. This is necessary to continue operations like remote alarming, archiving histories, and so on.

However, you should not leave the Supervisor in this state, as this negates much security (see Caution).

⚠ **Caution** *Unless set to "Strict", either "Relaxed" option is effectively the same as setting the FoxService property* Authentication Policy *to "Basic", as this is the only "common ground" authentication between a legacy Fox client (Workbench or another station) and this update release station. Thus, passwords for client connections to this station are passed in clear text. Obviously, this is not a desired operating state. For this reason, you should seldom (if ever) set the* Legacy Authentication *property to "Always Relaxed".*

Step 9 For each of the subordinate JACE hosts, open a platform connection in Workbench. Run the platform **`Commissioning Wizard`**, selecting to "Install/upgrade core software from distribution files", and also to "upgrade all out-of-date software modules".

After each JACE reboots and its station starts, verify that its communications to the Supervisor are still functional (in upgraded JACEs, you should not need to change any FoxService properties).

Step 10 After all JACEs are upgraded to the update release level, open the Supervisor station in Workbench.

In the Supervisor's NiagaraNetwork, FoxService, reset the **`Legacy Authentication`** property to "Strict", and then **`Save`**.

Step 11 Verify that NiagaraNetwork communications between the Supervisor and JACE stations are OK, and make new backups of all stations.

Copying items from previous install

When you choose the Workbench install option to "Copy settings from Latest Version Installed (version)", the contents of the following folders are copied from the older NiagaraAX Workbench release folder (`!`) to the new NiagaraAX Workbench release folder (`!`):

- `!backups`
- `!certificates`
- `!certManagement` (new folder in AX-3.8)
- `!daemon`
- `!jre/lib/security/krb5.conf` (if it exists - used for LDAP with Kerberos)
- `!licenses`
- `!modules` -> `!sw/inbox`
- `!security`

- `!sedona/kits` (if it exists)
- `!sedona/manifests` (if it exists)
- `!sedona/platforms` (if it exists)
- `!stations` (except for `!stations/demo` and `!stations/demoAppliance`)
- `!sw`
- `!users` (in an AX-3.8 installation, user credentials are not included)
- `!workbench`

If necessary, you can manually copy these files.

Note: *If upgrading Workbench or a Supervisor from the original AX-3.7 release to either AX-3.7u1 (or AX-3.8), the contents of these folders have special significance:*

- `!security`
- `!workbench/security`

This is especially important if SSL is implemented, as these contain related certificates, exemptions, and trusted root certificates.

To copy the `!sw` folder for Workbench, you can alternatively use the platform **`Software Manager`** after starting Workbench and making a local platform connection. Select "**`Software Import`**", "Import software from directory", and navigate to the old `!sw` folder. For details, see "Software Import" in the *Platform Guide*. Note that backup `.dist` files have exact dependencies, such that prior saved backups are likely dependent upon modules in the older software database (`!sw`) folder.

Improvements and changes in AX-3.8

Much of this document applies to systems running NiagaraAX *update releases* of AX-3.7, AX-3.6, and AX-3.5 (AX-3.7u1, AX-3.6u4, AX-3.5u4), but *not* to AX-3.8 systems. In particular, the following sections describe possible station archiving modifications that are typically *unnecessary* in AX-3.8:

- "Station archiving changes" on page 7
  - "Use case: station backups" on page 8
  - "Use case: replicated stations (system image)" on page 8
- "Making modifications to archived station files" on page 9
  - "Editing the station database (config.bog) file" on page 9
  - "Creating a "system image" distribution file from a backup .dist file" on page 12

For background details, see "Station archive portablility improvements in AX-3.8" on page 7.

In addition to AX-3.8 improvements in *station* credentials storage and archiving, security was also improved for *platform* credentials. However, note these improvements may affect behavior when you restore station backups. See "Platform credentials improvements" on page 5.

Finally, note that *browser access* of any AX-3.8 station using "Web Workbench" (WbApplet in Java), now requires the *browser client PC* to have Java "Unlimited Strength Policy Files" installed, otherwise the WbApplet does not launch—an error popup appears instead. These unlimited strength policy files are not included in a Java Standard Edition (SE) install, or Java SE update, but are available for download from Oracle. For complete details, see "Additional AX-3.8 client-side Java installation steps" on page 6.

Platform credentials improvements

In AX-3.8, security improvements were also made in *platform credentials* for *digest* authentication—where digest authentication is the *only* authentication method for any QNX-based JACE host, and an option for a Windows or Linux based host. Digest platform credentials in AX-3.8 now use the strong, two-way AES-256 encryption against the unique keyring and key material file of each JACE host.

Digest platform credentials were also *relocated* to a more secure location in the *registry* of AX-3.8 JACEs (or with Windows hosts, relocated in the Windows registry).

Station backup and restore changes

For the most part, AX-3.8 platform credentials improvements are transparent. However, be aware of this when restoring an AX-3.8 station backup:

- Platform credentials are *no longer included* in a station backup `.dist` of an AX-3.8 host (unlike in a backup `.dist` file for any AX-3.7u1 or earlier release JACE).

Sometimes, this may be confusing. For example, say you have an AX-3.8 JACE running with platform credentials unique to a job, and you make a station backup. The backup `.dist` for that JACE does *not contain* these platform credentials, as stated above. This applies whether an "online backup" via a station's BackupService (or Supervisor's provisioning), or an "offline backup" with the station stopped, via a platform connection and from the Platform Administration view.

- Now say you have another AX-3.8 JACE running that has been commissioned with *different* unique (non-default) platform credentials. If you restore the backup `.dist` described above to this JACE, it will reboot with the same platform credentials that it had *before* restoring the backup.
- Or, in the case where you install a "clean dist" file in a JACE first, note that when the JACE reboots from the cleaning, it will be using *factory default* platform credentials (set by the cleaning operation).
  - If you restore the AX-3.8 backup `.dist` file at this point, following the restore the AX-3.8 JACE reboots with *factory default* platform credentials.
  - If (after the cleaning) you first *change* the platform credentials in the JACE to non-defaults, *then restore* the AX-3.8 backup `.dist` file, following the restore the AX-3.8 JACE cannot use the credentials you previously entered—again, it reboots with *factory default* platform credentials.

  In particular, this can lead to confusion—and you should never leave a JACE running in this state. In either case, always reopen a platform connection and change the platform credentials to non-default values, via the "Update Authentication" choice in the **`Platform Administration`** view.

For details, see "Downgrading a JACE (Clean Dist)" and "Update Authentication" in the *Platform Guide*.

Note: *Backup and restore changes described here are dependent on the NiagaraAX release level of the target backup* host *(JACE), and not the release level of the Workbench client. In other words, if you use AX-3.8 Workbench to backup a JACE that is running an earlier release (e.g. AX-3.7u1, AX-3.6u4), when you restore that backup, the JACEs will reboot with the platform credentials from that backup* `.dist` *file.*

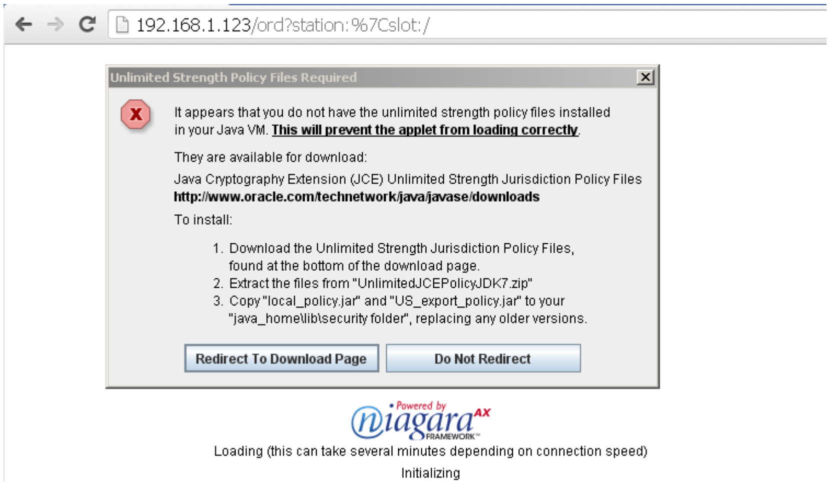
Additional AX-3.8 client-side Java installation steps

Note: *These steps are required on any* client computer *that needs to access any AX-3.8 station using a browser, where "Web Workbench" access is being used (WbApplet in Java browser plugin). In addition, be aware that following a future "Java SE update" install on that computer, you may need to* repeat *these steps—as these installed files may be* overwritten *by the Java update with "standard strength" policy files.*

Because of core AX-3.8 changes to support stations that may need to run in "FIPS mode" (a separately licensed feature), accessing any AX-3.8 station via a browser with a Wb Web profile (Web Workbench, using the WbApplet) now requires the JCE (Java Cryptography Extension) "Unlimited Strength Jurisdiction Policy Files" to run. This allows the JCE to use the stronger cryptography required in AX-3.8.

If your browser client PC does not have these policy files installed, you are prompted to do so at the first browser access of an AX-3.8 station, after login as a user with a Wb Web profile. See Figure 1.

Figure 1 *Unlimited Strength Policy Files Required warning (and download link)*



192.168.1.123/ord?station:%7Cslot:/

Unlimited Strength Policy Files Required

It appears that you do not have the unlimited strength policy files installed in your Java VM. **This will prevent the applet from loading correctly**.

They are available for download:

Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files
http://www.oracle.com/technetwork/java/javase/downloads

To install:

1. Download the Unlimited Strength Jurisdiction Policy Files, found at the bottom of the download page.
2. Extract the files from "UnlimitedJCEPolicyJDK7.zip"
3. Copy "local_policy.jar" and "US_export_policy.jar" to your "java_home\lib\security folder", replacing any older versions.

Loading (this can take several minutes depending on connection speed)

Initializing

As shown above, the popup provides basic instructions as well as a link to the Oracle download page (once there, scroll to look for the "JCE Unlimited Strength Jurisdiction Policy Files 7" download link). These steps are also outlined below:

Installing Unlimited Strength Policy Files for browser WbApplet access

Step 1 Download the policy files. Either follow the "**`Redirect To Download Page`**" link in the popup, scrolling down find this download, or else use the following link (current at the time of this document):

http://www.oracle.com/technetwork/java/javase/downloads/index.html

Step 2 Look for the "JCE Unlimited Strength Jurisdiction Policy Files 7" download link, and download it.

Step 3 Extract the files from the downloaded archive, perhaps to a `temp` folder.

Step 4 From the extracted files, copy these two files to the browser PC's `java_home/lib/security` folder:

- `local_policy.jar`
- `US_export_policy.jar`

Overwrite any existing files with the same name.

Note: *This is not the NiagaraAX installation's `java_home`, but instead the Java installation on the PC used by browser clients—for example to connect to Niagara stations using "Web Workbench" (WbApplet). For many Windows PCs, this may be something similar to:*

`C:\Program Files (x86)\Java\jre7\lib\security`

Once you have copied the policy files to Java's security folder, the WbApplet should run in the browser. Note that the station's (server) `java_home`, installed with NiagaraAX, *already includes* these policy files.

Station archive portablility improvements in AX-3.8

This document's sections "Station archiving changes" on page 7 and "Making modifications to archived station files" on page 9 do not apply if using AX-3.8—modifications are *unnecessary*. Why? In an AX-3.8 station archive (station save via platform **`Station Copier`**, or station backup via Workbench, the station's BackupService, or a Supervisor's provisioning mechanism), the station `config.bog` file or backup `.dist` file is "more portable" than a file made from a prior *update release* platform.

- In AX-3.8, when you copy a station using the platform **`Station Copier`**, any encrypted (client) passwords are automatically decrypted and stored in a portable format in the `config.bog` file for that station. This means you can reinstall that station in a different AX-3.8 host with all stored passwords working. Upon station startup, client passwords are re-encrypted to the keyring and key material unique to the new host, and then resaved. Thus (and often unlike in update releases), any re-entering of client passwords is unnecessary.
- In AX-3.8, when a station backup is initiated, the keyring (used against encrypted passwords) is automatically *decrypted* during the backup, and stored in the backup `.dist` file.
  - As always, you can restore the backup `.dist` back to the *same* AX-3.8 host, using the platform **`Distribution File Installer`**. The "key material" file used in encryption is unchanged.
  - You can also use the backup as a "system image" to install in *other* AX-3.8 hosts, for example same model JACEs. When using the **`Distribution File Installer`** to install the backup `.dist` file in this case, the stored keyring is automatically *re-encrypted* to the key material file unique to each JACE, ensuring adequate security for all encrypted passwords.

In either case upon installation all the station's client passwords are operational and maintain good security practices. Manual modifications to station archive files should not be necessary.

Note: *A station's `config.bog` file contained (compressed) inside a backup `.dist` of an AX-3.8 host contains client passwords that are* still encrypted*. This is mentioned because this `config.bog` is not "portable" like the `config.bog` produced by a station copy (save) using the AX-3.8* **`Station Copier`**.

Station archiving changes

Note: *Archiving changes and use case issues described here* do not apply to a *AX-3.8* system, *but do apply to a system running an update release (AX-3.7u1 or later, AX-3.6u4 or later, AX-3.5u4 or later). See "Station archive portablility improvements in AX-3.8" on page 7.*

Historically, NiagaraAX users have made archives of stations using two basic methods:

- Using the **`Station Copier`** platform tool
  This can be used to both *save* a station to the Workbench PC (including most folders and files under that station's file space) as well as *install* (copy) that station to a remote host, typically a JACE. Such a station copy includes a station folder with a `config.bog` file, and optionally other files.
- Using a station's **`BackupService`**, which provides a **`Backup Manager`** view, plus a right-click "Backup Station" command on the station (FoxSession) as it appears in the Workbench Nav tree. Or, a similar backup is available from a Supervisor's Provisioning extension, or directly from a platform connection to the station's host. Collectively, these methods are considered "BackupService" tools. All such station backups are saved as a single backup "`.dist`" (distribution) file, which can be restored by using the platform **`Distribution File Installer`** tool.

As explained in the section "Portability of stored passwords" on page 2, when running an *update release* of NiagaraAX, the difference is now a `config.bog` from a **`Station Copier`** save contains some passwords that are *not portable* (do not work if copied to another host other than the original one).

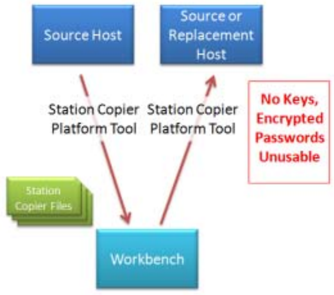
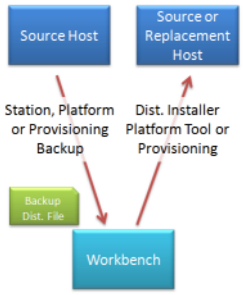
And although a backup `.dist` file *does* contain all portable passwords, in any “replicated station” scenario (if using an update release) this is often *undesirable*, as a security risk—as all hosts then use identical encryption key files.

Consider these two use cases for archiving and reinstalling a station:

- “Use case: station backups” on page 8
- “Use case: replicated stations (system image)” on page 8

Use case: station backups

(Issues not applicable to AX-3.8) When making backups of Niagara stations to restore a station back to its current state, you have the option of either the **`Station Copier`** or the **`BackupService`** tools.

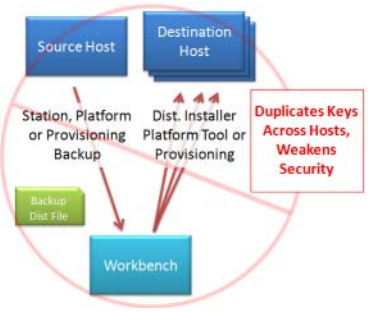
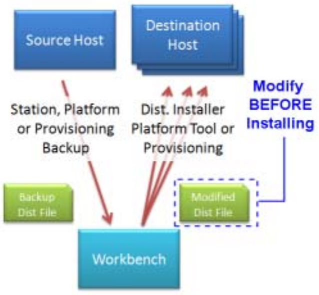
Using **`Station Copier`**	Using **`BackupService`** and **`Distribution File Installer`**
 Source Host Source or Replacement Host Station Copier Platform Tool Station Copier Platform Tool No Keys, Encrypted Passwords Unusable Station Copier Files Workbench	 Source Host Source or Replacement Host Station, Platform or Provisioning Backup Dist. Installer Platform Tool or Provisioning Backup Dist. File Workbench
User passwords are usable, but client (account) passwords are not.	Both User passwords and client passwords are usable, but encryption keys are identical.
NOTE: Issues do not apply to AX-3.8. See “Improvements and changes in AX-3.8” on page 5.	

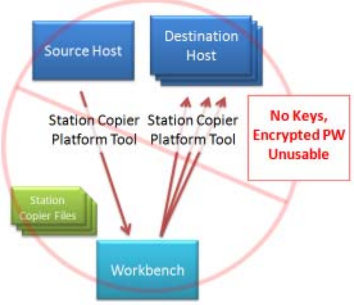
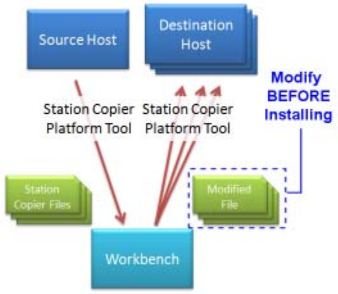
Now, you must keep in mind if the original source host (JACE hardware) needs to be replaced, the backup files archived using the **`Station Copier`** (above left) do not contain the key used for encrypting “client passwords”. So those passwords will not be usable after the copy is restored back to the new hardware. (You could, however, copy that station back to the original source host without issues—providing a “clean dist” (cleaning) file has not been installed beforehand. A clean dist removes the `!security` folder from the host, and new set of encryption keys are generated upon station startup).

Whereas, the backup `.dist` file made using the **`BackupService`** tools (above right) *does* contain the host’s security (encryption) key. If needed, you could successfully install that dist file to new JACE hardware. So, a backup `.dist` is a *more reliable* way to ensure that the system can be recovered.

Use case: replicated stations (system image)

(Issues not applicable to AX-3.8) Backups of a Niagara system are often used to make a copy to *replicate* an identically-configured station to use on many different hosts (sometimes called a “system image”).

Replicated stations, Backup dist and **`Distribution File Installer`**		Dist file modifications:
 Source Host Destination Host Station, Platform or Provisioning Backup Dist. Installer Platform Tool or Provisioning Duplicates Keys Across Hosts, Weakens Security Backup Dist File Workbench	 Source Host Destination Host Station, Platform or Provisioning Backup Dist. Installer Platform Tool or Provisioning Modify BEFORE Installing Backup Dist File Modified Dist File Workbench	- keys removed, - modified manifest, - modified config.bog, - only legacy encoded passwords, - only default passwords
Weakened security from identical encryption key files on all hosts.	Modifications (at right) keep security strong in all hosts.	
NOTE: Issues above and below are not in AX-3.8. See “Improvements and changes in AX-3.8” on page 5.		

Replicated stations, using **Station Copier**		Config.bog file modifications:
 Source Host Destination Host Station Copier Platform Tool Station Copier Platform Tool No Keys, Encrypted PW Unusable Station Copier Files Workbench	 Source Host Destination Host Modify BEFORE Installing Station Copier Platform Tool Station Copier Platform Tool Station Copier Files Modified File Workbench	- only legacy encoded passwords, - only default passwords
Client (account) passwords unusable.	Modifications (at right) make all passwords usable.	

For this replicated station use case, you must take care that:

- The same encryption key is not installed to different hosts, as this weakens overall security strength.
- If any passwords need to be part of the copy, that they are encoded with the portable legacy format, and not the new (non-portable) encrypted format.

To do this you must *modify* the `config.bog` file, and if using the backup dist method (above, top) also make changes to *other* items contained in the `.dist` file. Moreover, you should also be sure to *test these modifications* before relying on them for jobs or sharing with customers or clients.

Caution *As with regular backup dist files, keep these modified files (`config.bog`, `.dist`) in a* secure location *as well. Or for best security, consider* deleting them *after installing in the the intended target platforms.*

Making modifications to archived station files

Note: *File modifications described here* do not apply to a *AX-3.8* system, *but only on a system running an update release (AX-3.7u1 or later, AX-3.6u4 or later, AX-3.5u4 or later). See "Station archive portablility improvements in AX-3.8" on page 7.*

- To modify a station `config.bog` file, you open the file *offline* in Workbench, then *resave*. See the section "Editing the station database (config.bog) file" on page 9.
- To modify a station backup `.dist` file, you must use a zip editing tool (a `.dist` file is a zip compressed file) and do *several* operations on its contents. Typically, *one* of these includes modifying its `config.bog` file (after extracting it) using the method above—then placing it back in the backup `.dist` file. A number of *other* operations are usually needed as well. See the section "Creating a "system image" distribution file from a backup .dist file" on page 12.

Editing the station database (config.bog) file

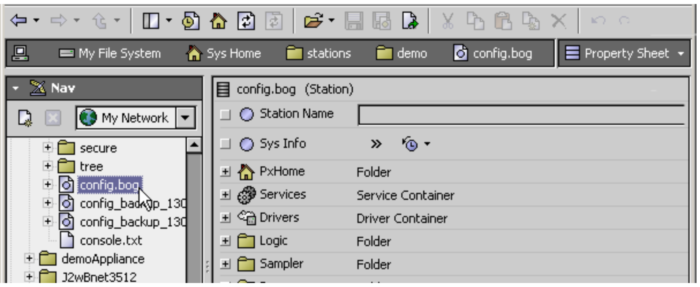
Whether the station database file (`config.bog`) is considered to be a station backup or whether it is part of a replicated station (system image) backup dist, the suggested modifications to it are the same.

Note: *Be sure to keep unmodified copies of `config.bog` files (from Station Copier) or saved backup `.dist` files before making modifications. Work from copies of these files.*

Test your changes — be sure your modifications accomplish what you intend. This is especially important if you will be relying on them for jobs or sharing with customers or clients.

To modify, you open the file offline in Workbench.

Figure 2 *Edit config.bog file offline in Workbench*



My File System › Sys Home › stations › demo › config.bog — Property Sheet

Nav — My Network
- secure
- tree
- config.bog
- config_backup_130
- config_backup_130
- console.txt
- demoAppliance
- J2wBnet3512

config.bog (Station)

Station Name	
Sys Info	
PxHome	Folder
Services	Service Container
Drivers	Driver Container
Logic	Folder
Sampler	Folder

Note: *Modifications described here* do not apply to a *AX-3.8* system*, but only on a system running an update release (AX-3.7u1 or later, AX-3.6u4 or later, AX-3.5u4 or later). See "Station archive portablility improvements in AX-3.8" on page 7.*

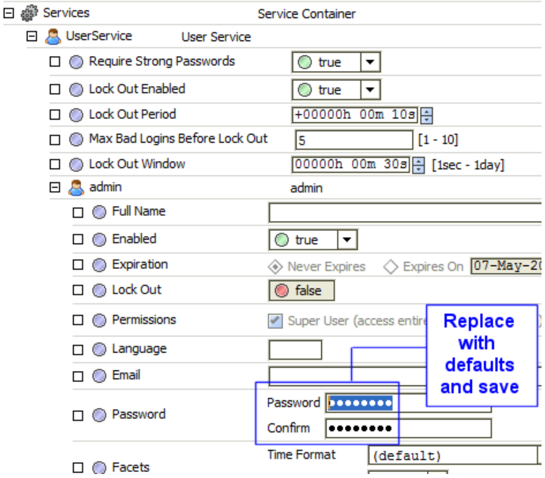
The following modifications are recommended:

1. Remove any User passwords that were changed from defaults
2. Set "Force Reset At Next Login" for all Users (AX-3.7 and later only, recommended in many cases)
3. Convert any encrypted passwords
4. Revert any automated configuration
5. Save the BOG file changes

Remove any User passwords that were changed from defaults

In some cases by logging into a template station to verify a "known good" configuration, you can be forced to change passwords from defaults (particularly true if an AX-3.7 station).

Figure 3 *Changing password back to defaults*



Services	Service Container
UserService	User Service
Require Strong Passwords	true
Lock Out Enabled	true
Lock Out Period	+00000h 00m 10s
Max Bad Logins Before Lock Out	5 [1 - 10]
Lock Out Window	00000h 00m 30s [1sec - 1day]
admin	admin
Full Name	
Enabled	true
Expiration	◆ Never Expires ◇ Expires On 07-May-20
Lock Out	false
Permissions	☑ Super User (access entir
Language	
Email	
Password	Password ●●●●●●●● Confirm ●●●●●●●●
	Time Format (default)
Facets	

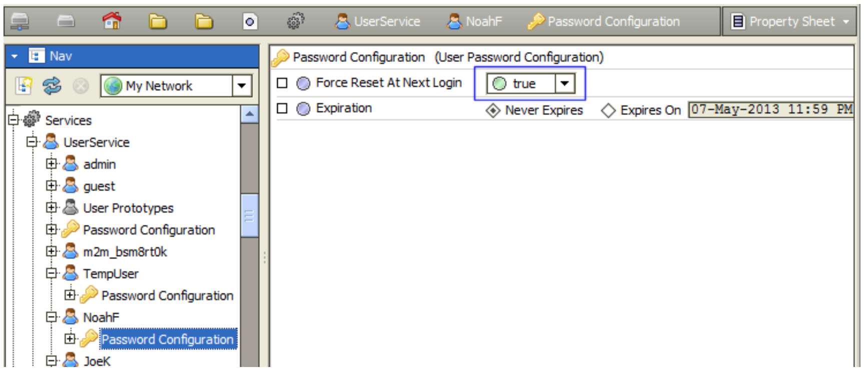
Replace with defaults and save

In an image, you'll want to change such User passwords back to defaults.

Set "Force Reset At Next Login" for all Users

If using AX-3.7 or later, in many cases it is recommended that you set each User's "Force Reset At Next Login" property (under `Password Configuration`) to true.

Figure 4 *Set "Force Reset At Next Login" to true for every user*



Password Configuration (User Password Configuration)

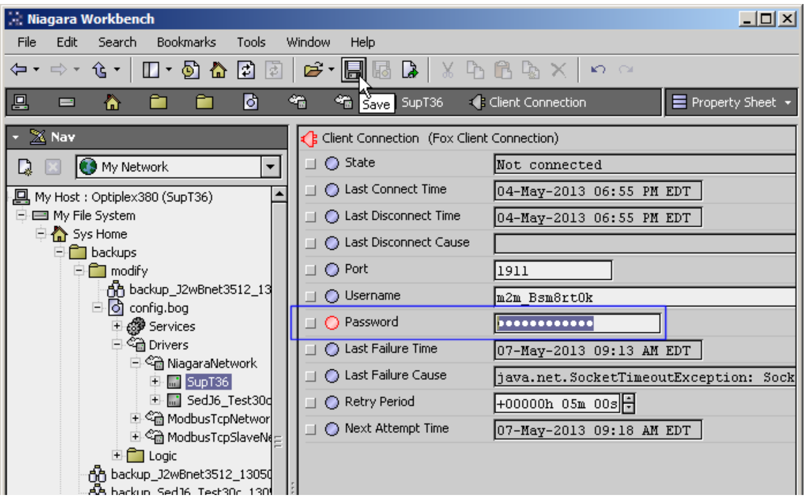
Force Reset At Next Login	true
Expiration	◈ Never Expires ◇ Expires On 07-May-2013 11:59 PM

An exception to this may be if these are replicated JACE stations to be installed in a NiagaraNetwork where "network users" are configured. In this scenario, sometimes you may wish to reserve this setting for only the (source) network Users in the Supervisor station.

Convert any encrypted passwords

If you need client credentials in an image, they won't work in a target host because of new encryption techniques. Your offline edit of a station `config.bog` should replace any "new format" encoded passwords with *legacy* passwords. Figure 5 shows such an offline edit in progress.

Figure 5 *Editing a client password in offline config.bog file*



Client Connection (Fox Client Connection)

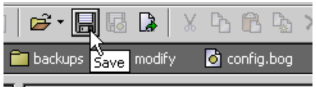
State	Not connected
Last Connect Time	04-May-2013 06:55 PM EDT
Last Disconnect Time	04-May-2013 06:55 PM EDT
Last Disconnect Cause	
Port	1911
Username	m2m_Bsm8rt0k
Password	••••••••••••
Last Failure Time	07-May-2013 09:13 AM EDT
Last Failure Cause	java.net.SocketTimeoutException: Sock
Retry Period	+00000h 05m 00s
Next Attempt Time	07-May-2013 09:18 AM EDT

Note you may have to overtype the password with an incorrect password, save, then correct it and save again to ensure that it gets stored correctly.

Revert any automated configuration

Certain NiagaraAX services can configure themselves based on available hardware when their station is first run. You may wish to investigate for this. If found, revert any such configuration during your offline edit of the station `config.bog`.

Save the BOG file changes



When finished modifying, remember to *save* `config.bog` file changes!

Creating a “system image” distribution file from a backup .dist file

Note: *Modifications described here* do not apply to a *AX-3.8* system*, but only on a system running an update release (AX-3.7u1 or later, AX-3.6u4 or later, AX-3.5u4 or later). See “Station archive portablility improvements in AX-3.8” on page 7.*

The BackupService includes contents in a backup distribution file that are appropriate for restoring the original source system to its current state. However, some contents are inappropriate for “system images” used to replicate the same station to many different hosts. You can modify the backup `.dist` file to remove or replace those contents.

Note: *Be sure to keep unmodified copies of saved backup* `.dist` *files or* `config.bog` *files (from* **`Station Copier`**) *before making modifications. Work from copies of these files.*

Test your changes — be sure your modifications accomplish what you intend. This is especially important if you will be relying on them for jobs or sharing with customers or clients.

Each distribution file is zip archive that contains certain system files and a manifest file that describes system and software dependencies, with rules for installing the system files. Because it is a zip archive, you can modify it with common tools such as 7-Zip, WinZip, and recent versions of Microsoft Windows.

To modify a backup `.dist` file to be suitable for use as a system image, you need to remove the (encryption) key files, and typically also make edits to its manifest file and modify its station database (`config.bog`) file.

The following `.dist` file modifications are typical:

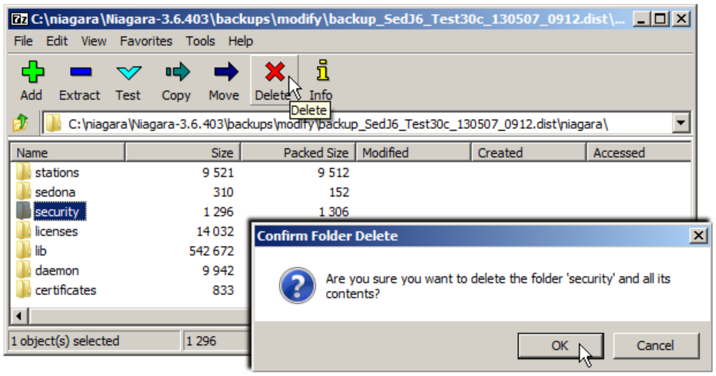
1. Remove the security folder (recommended)
2. Edit the distribution manifest (optional)
3. Modify the station database (config.bog) file (typical)

Remove the security folder

In the backup `.dist` file, the `security` folder contains encryption key data that is unique to this device. If the same folder was copied to many different hosts, overall system security would be weakened.

Note: *This underscores the importance of properly securing backup dist files! If someone obtains a copy of the backup dist file, they would have this encryption key data. See the related Caution on page 3.*

Figure 6 *Remove security folder inside backup .dist file*


C:\niagara\Niagara-3.6.403\backups\modify\backup_SedJ6_Test30c_130507_0912.dist\...
File
Edit
View
Favorites
Tools
Help
Add
Extract
Test
Copy
Move
Delete
Info
Delete
C:\niagara\Niagara-3.6.403\backups\modify\backup_SedJ6_Test30c_130507_0912.dist\niagara\
Confirm Folder Delete
OK
Cancel

Name	Size	Packed Size	Modified	Created	Accessed
stations	9 521	9 512			
sedona	310	152			
security	1 296	1 306			
licenses	14 032				
lib	542 672				
daemon	9 942				
certificates	833				

1 object(s) selected 1 296

Are you sure you want to delete the folder 'security' and all its contents?

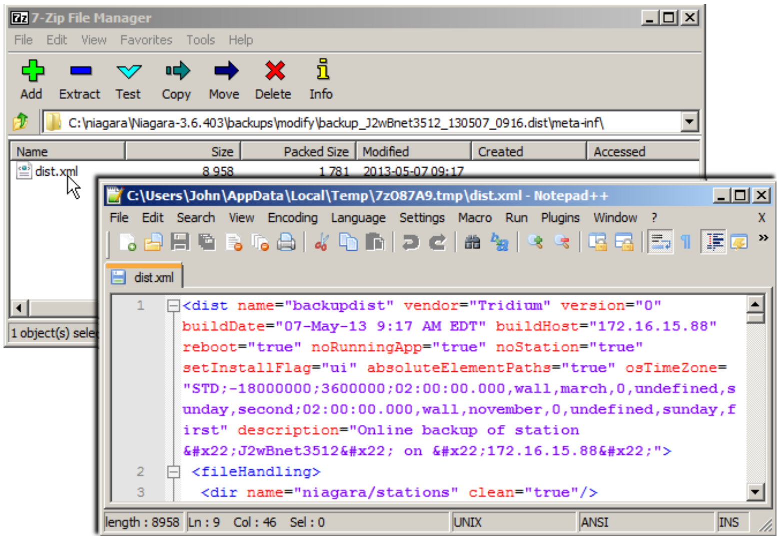
Delete the `security` folder. Figure 6 shows this being done using 7-Zip.

Note this also underscores the importance of saving *unmodified copies* of backup `.dist` files, again in a *secure location*. Once the folder shown above is deleted, all the client (encrypted) passwords in the associated station database file (`config.bog`) will no longer work.

Edit the distribution manifest

The distribution manifest is an XML file, stored as `meta-inf/dist.xml` in the distribution. Its format is documented in the *Niagara Developer Guide* (docDeveloper) in a "Distributions" section.

Figure 7 *Accessing/opening the distribution manifest (dist.xml) file in a backup .dist file*


7-Zip File Manager
File Edit View Favorites Tools Help
Add
Extract
Test
Copy
Move
Delete
Info
File Edit Search View Encoding Language Settings Macro Run Plugins Window ? X
dist.xml
length : 8958 Ln : 9 Col : 46 Sel : 0 UNIX ANSI INS

C:\niagara\Niagara-3.6.403\backups\modify\backup_J2wBnet3512_130507_0916.dist\meta-inf\

Name	Size	Packed Size	Modified	Created	Accessed
dist.xml	8 958	1 781	2013-05-07 09:17		

1 object(s) sele

C:\Users\John\AppData\Local\Temp\7z087A9.tmp\dist.xml - Notepad++

```
<dist name="backupdist" vendor="Tridium" version="0"
buildDate="07-May-13 9:17 AM EDT" buildHost="172.16.15.88"
reboot="true" noRunningApp="true" noStation="true"
setInstallFlag="ui" absoluteElementPaths="true" osTimeZone=
"STD;-18000000;3600000;02:00:00.000,wall,march,0,undefined,s
unday,second;02:00:00.000,wall,november,0,undefined,sunday,f
irst" description="Online backup of station
&#x22;J2wBnet3512&#x22; on &#x22;172.16.15.88&#x22;">
 <fileHandling>
  <dir name="niagara/stations" clean="true"/>
```

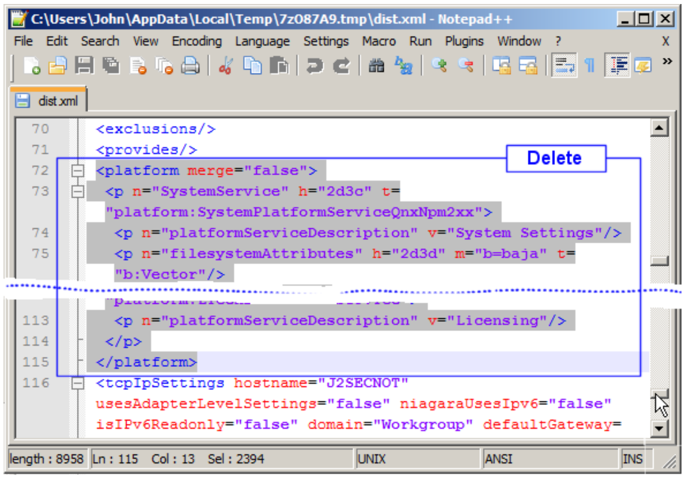
Note: *Some zip editing tools don't support editing files in place very well. To use these, you will need to extract the `dist.xml` file to your system, make your edits, then add the file back to the dist with the zip tool.*

The manifest in a backup `.dist` file contains elements or attributes you may wish to delete in many cases, including the following:

- platform (element)
- tcpIpSettings (element)
- rel (attribute of dependency elements)

platform (element) The `platform` element in the `dist.xml` file will not be appropriate if the target hosts can have different hardware configurations. If this is the case, remove that element.

Figure 8 *Removing platform element in a backup .dist file's manifest (dist.xml)*


File Edit Search View Encoding Language Settings Macro Run Plugins Window ? X
dist.xml
Delete
length : 8958 Ln : 115 Col : 13 Sel : 2394 UNIX ANSI INS

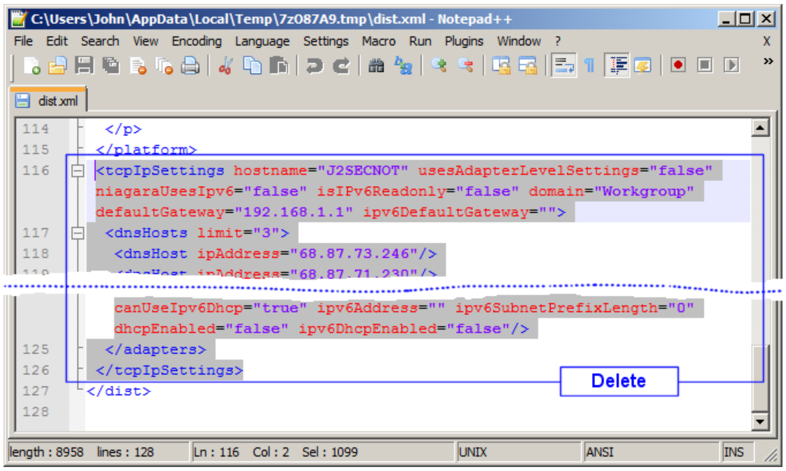
C:\Users\John\AppData\Local\Temp\7z087A9.tmp\dist.xml - Notepad++

```
<exclusions/>
<provides/>
<platform merge="false">
 <p n="SystemService" h="2d3c" t=
 "platform:SystemPlatformServiceQnxNpm2xx">
  <p n="platformServiceDescription" v="System Settings"/>
  <p n="filesystemAttributes" h="2d3d" m="b=baja" t=
  "b:Vector"/>
  <p n="platformServiceDescription" v="Licensing"/>
 </p>
</platform>
<tcpIpSettings hostname="J2SECNOT"
usesAdapterLevelSettings="false" niagaraUsesIpv6="false"
isIPv6Readonly="false" domain="Workgroup" defaultGateway=
```

As shown in Figure 8 above, all lines from `<platform merge="false">` to `</platform>` at the end should be marked for deletion.

tcpIpSettings (element) The `tcpIpSettings` element in the `dist.xml` file is not appropriate for system images. Although not critical (as the **`Distribution File Installer`** prompts if you want to install using these settings, and a Supervisor’s Provisioning extension ignores it), you can still remove it while you are already editing this file.

Figure 9 *Removing tcpIpSettings element in a backup .dist file’s manifest (dist.xml)*


C:\Users\John\AppData\Local\Temp\7z087A9.tmp\dist.xml - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
dist.xml

```
  </p>
 </platform>
<tcpIpSettings hostname="J2SECNOT" usesAdapterLevelSettings="false"
niagaraUsesIpv6="false" isIPv6Readonly="false" domain="Workgroup"
defaultGateway="192.168.1.1" ipv6DefaultGateway="">
  <dnsHosts limit="3">
   <dnsHost ipAddress="68.87.73.246"/>
   <dnsHost ipAddress="68.87.71.230"/>

   canUseIpv6Dhcp="true" ipv6Address="" ipv6SubnetPrefixLength="0"
   dhcpEnabled="false" ipv6DhcpEnabled="false"/>
  </adapters>
 </tcpIpSettings>
</dist>
```

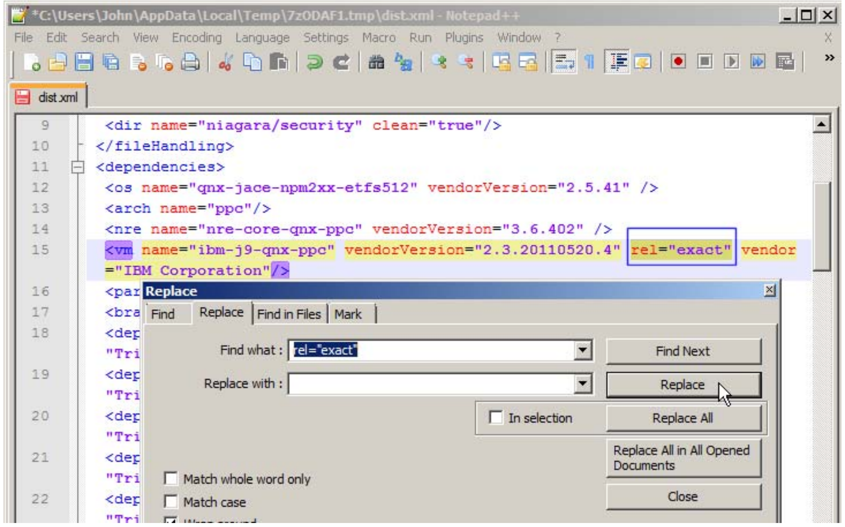
Delete

length : 8958 lines : 128
Ln : 116 Col : 2 Sel : 1099
UNIX
ANSI
INS

As shown in Figure 9 above, all lines between `<tcpIpSettings hostname="`*`value`*`" (etc)>` to the ending `</tcpIpSettings>` should be marked for deletion.

rel (attribute of dependency elements) The `rel` element in various `dependency` elements in the `dist.xml` all state `rel="exact"`. This can be a bit unforgiving when used as a “system image”, as a backup `.dist` install will fail if the exact version of a dependency isn’t available to install.

Figure 10 *Searching for rel attributes to delete in a backup .dist file’s mainfest (dist.xml), if necessary*


*C:\Users\John\AppData\Local\Temp\7z0DAF1.tmp\dist.xml - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
dist.xml

```
  <dir name="niagara/security" clean="true"/>
 </fileHandling>
 <dependencies>
  <os name="qnx-jace-npm2xx-etfs512" vendorVersion="2.5.41" />
  <arch name="ppc"/>
  <nre name="nre-core-qnx-ppc" vendorVersion="3.6.402" />
  <vm name="ibm-j9-qnx-ppc" vendorVersion="2.3.20110520.4" rel="exact" vendor
  ="IBM Corporation"/>
  <par
  <bra
  <dep
  "Tri
  <dep
  "Tri
  <dep
  "Tri
  <dep
  "Tri
  <dep
  "Tri
```

Replace
Find
Replace
Find in Files
Mark

Find what : rel="exact"

Replace with :

Find Next
Replace
Replace All
Replace All in All Opened Documents
Close

☐ In selection

☐ Match whole word only

☐ Match case

Figure 10 above shows a search and replace being used to remove the `rel` attribute from selected lines.

Note: *This is an advanced modification—note that all listed core, config, and QNX OS distributions listed include this* `rel="exact"` *attribute, in addition to all listed software modules (.jar files).*

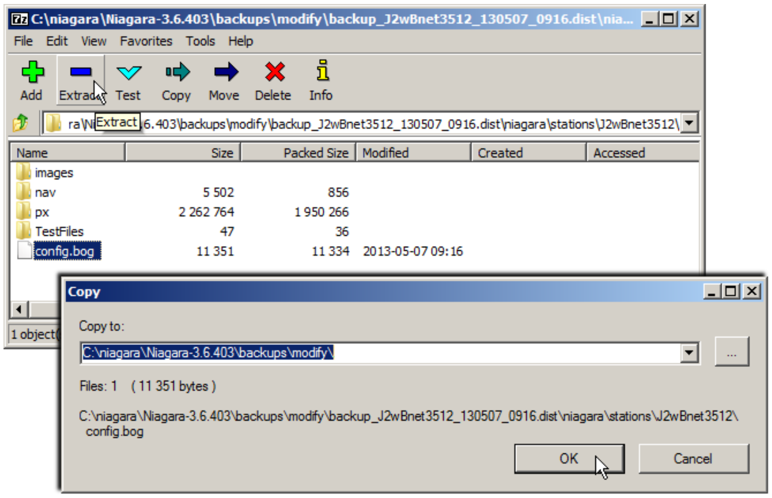
Modify the station database (config.bog) file

The station database (`config.bog` file) is included in a backup `.dist` file, stored at:

`stations/`*`stationName`*`/config.bog`

If changes are needed, you need to extract it using a zip tool, and modify it offline using Workbench.

Figure 11 *Extracting config.bog file from backup .dist file to make offline changes in Workbench*



C:\niagara\Niagara-3.6.403\backups\modify\backup_J2wBnet3512_130507_0916.dist\nia...

ra\Ni Extract 6.403\backups\modify\backup_J2wBnet3512_130507_0916.dist\niagara\stations\J2wBnet3512\

Name	Size	Packed Size	Modified	Created	Accessed
images					
nav	5 502	856			
px	2 262 764	1 950 266			
TestFiles	47	36			
config.bog	11 351	11 334	2013-05-07 09:16		

1 object(

Copy

Copy to:

C:\niagara\Niagara-3.6.403\backups\modify\

Files: 1 (11 351 bytes)

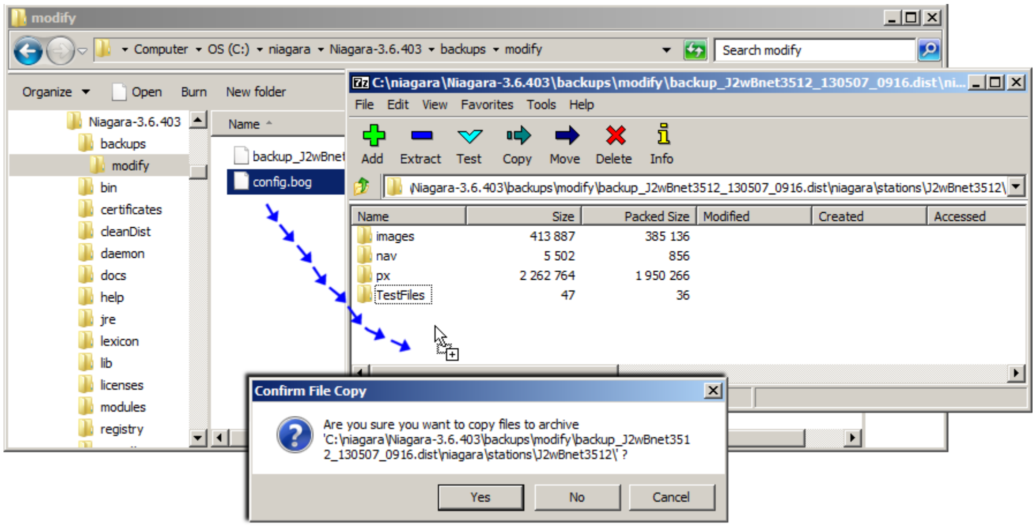
C:\niagara\Niagara-3.6.403\backups\modify\backup_J2wBnet3512_130507_0916.dist\niagara\stations\J2wBnet3512\config.bog

Figure 11 above shows the `config.bog` file being extracted (using 7-Zip) to the same folder used to modify the backup `.dist` file.

See “Editing the station database (config.bog) file” on page 9 for details on using Workbench to modify this file.

Replacing the modified config.bog file When you are finished modifying `config.bog` with Workbench (making sure to save it), you now need to *replace* the original one in the backup `.dist` file.

Figure 12 *Replacing the config.bog in a backup .dist file with a modified config.bog*



modify

Computer ▸ OS (C:) ▸ niagara ▸ Niagara-3.6.403 ▸ backups ▸ modify

Search modify

Niagara-3.6.403
backups
modify
bin
certificates
cleanDist
daemon
docs
help
jre
lexicon
lib
licenses
modules
registry

Name
backup_J2wBnet
config.bog

C:\niagara\Niagara-3.6.403\backups\modify\backup_J2wBnet3512_130507_0916.dist\ni...

\Niagara-3.6.403\backups\modify\backup_J2wBnet3512_130507_0916.dist\niagara\stations\J2wBnet3512\

Name	Size	Packed Size	Modified	Created	Accessed
images	413 887	385 136			
nav	5 502	856			
px	2 262 764	1 950 266			
TestFiles	47	36			

Confirm File Copy

Are you sure you want to copy files to archive 'C:\niagara\Niagara-3.6.403\backups\modify\backup_J2wBnet3512_130507_0916.dist\niagara\stations\J2wBnet3512\' ?

As shown in Figure 12, one way to do this (for example, using a zip tool like 7-Zip):

- *Delete* the existing `config.bog` file in the backup `.dist` file.
- Drag and drop the *modified* `config.bog` into the `stations` folder of the backup `.dist`. At the confirm file copy prompt answer **`Yes`**.

After saving, your modified backup `.dist` file should now be ready to use as a “system image”, usable to install to multiple hosts that need a replicated station.

Update release level from build-number

All Niagara builds use a numbering scheme of: *major.minor.build.patch*

For example, build 3.6.47.10 is AX (3 for major), minor release 6, build 47, patch 10. Typically, when documenting the differences between minor releases, build and patch numbers are omitted. For example, AX-3.6 and AX-3.7 are terms commonly used in NiagaraAX tech docs when discussing differences between these two minor releases.

However, any build-number of *100 or higher* also indicates that it is an *update level* build. The *leading build numeral is the update level*, such that build 3.6.305 is an “update 3” AX-3.6 build, and build 3.7.104 is an “update 1” AX-3.7 build. Any minor release *without* a build 100 or higher has had *no* update releases.

Because update releases usually provide *key fixes*, as in the case of the 2013 security-related “update 4” releases for AX-3.6 and AX-3.5 and the “update 1” release for AX-3.7, it is sometimes necessary to denote this distinction in tech docs, without citing a specific build-number (which can, and often does *change* while the document is being written).

For this reason, a term such as “AX-3.7u1” (which applies to any builds 3.7.*1nn*, such as 3.7.104 or 3.7.105) is used. In the same manner, terms “AX-3.6u4” equates to any builds 3.6.*4nn*, such as 3.6.404 or 3.6.405, and “AX-3.5u4” equates to any builds 3.5.*4nn*, such as 3.5.405 or 3.5.406.

Document change log

Updates (changes/additions) to this *NiagaraAX 2013 Security Updates* document are listed below.

- Revised: November 6, 2013
  Changes noted for differences in AX-3.8 versus using any of the update releases (AX-3.7u1, AX-3.6u4, AX-3.5u4). Included is a new main section “Improvements and changes in AX-3.8” on page 5, with subsections “Platform credentials improvements” on page 5, “Additional AX-3.8 client-side Java installation steps” on page 6, and “Station archive portablility improvements in AX-3.8” on page 7. The beginning sections “Improvements to the security of stored passwords” on page 2 and “Upgrade considerations” on page 3 were revised to include AX-3.8 changes. Various “Notes” were added in other sections about modifying station archive files (`config.bog`, backup `.dist` files) to explain that this is *unnecessary* in AX-3.8.
- Publication: May 28, 2013
  Initial document.