

Technical Document

JACE-9000 Backup and Restore Guide

niagara

JACE-9000 backup and restore overview

You can backup a JACE-9000 in several ways. This topic provides an overview of the backup and restore procedure options that are available. Other topics in this document provide information that can help you understand the different specific backup and restore processes.

Following are options for backup:

- Automatic backup with microSD card
- Manual backup with microSD card using Serial Shell connection
- Manual backup to a Supervisor platform using Platform Administration connection.

Following are options for restore:

- Restoring from a microSD card backup
- Restoring from a backup .dist file
- Restoring backup from Niagara Cloud management portal. For more information refer to Niagara Recover chapter of *Niagara Cloud Suite (NCS) Partner Guide*.

Backup to the microSD card

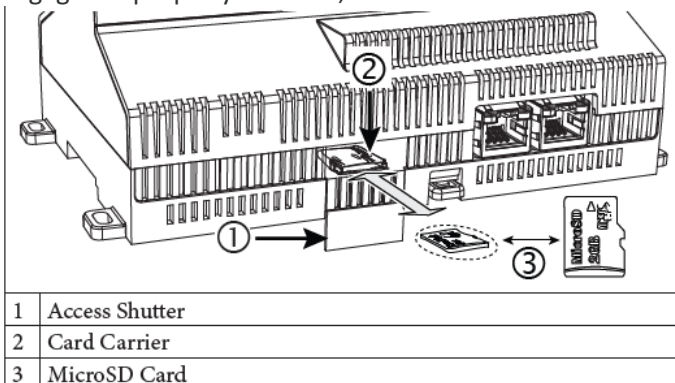
The JACE-9000 allows you to backup the entire controller platform and station to a microSD card without requiring access to the backup functions of Workbench.

- Only Tridium- configured microSD cards are supported.
- If you install a non-Tridium microSD card in the unit, the system will not generate a Host ID and Niagara will not run.
- If you insert or remove a microSD card from a JACE-9000 the Host ID will change for that controller.

Preparing for backup and restore

Note: Always remove power from the controller before installing or removing a microSD card.

To insert the microSD card into the controller, slide it into the card carrier, label side up, until the spring catch engages. If properly inserted, the card is behind the **Access Shutter** track.



The manual backup procedure uses a serial connection to the controller **DEBUG** port. This connection must be established before any backup or restore steps occur. The **DEBUG** port is a USB-C port for serial debug communications to the controller. You can use a serial terminal program (for example: PuTTY) with the **DEBUG** port to access the controller's system shell menu.

- **About Host ID**

Unlike other controllers, the ATLAS-1B22-B800-1CD8-A54B has a Host ID that can change based on the presence or absence of a MicroSD card. It is important to understand the role of the MicroSD card and its part in the creation of the controller Host ID, which is unique and essential for licensing the controller.

- **Validating the MicroSD card's Host ID**

The JACE-9000 Host ID depends on the presence of a MicroSD card. This ties the license file to the Host ID on an MicroSD card and makes it portable. All MicroSD cards are programmed with the Tridium secret, which validates the authenticity of the MicroSD card-based Host ID established using Card Identification (CID) values. The CID number is a unique identifier or serial number created on the MicroSD card at the time of manufacturing.

About Host ID

Unlike other controllers, the ATLAS-1B22-B800-1CD8-A54B has a Host ID that can change based on the presence or absence of a MicroSD card. It is important to understand the role of the MicroSD card and its part in the creation of the controller Host ID, which is unique and essential for licensing the controller.

- To support portability between JACE-9000 devices, the Host ID of a JACE-9000 will change to reflect presence of MicroSD card. This ties the license file to the Host ID on the SD card and makes it portable.
- For a JACE-9000 without an MicroSD card, the Host ID is derived from the CPU ID. It takes the format: ATLAS-1B22-B800-1CD8-A54B.
- For a JACE-9000 with a MicroSD card, the Host ID is derived from data on the MicroSD card. It takes the format: ATLAS-SD-F93E-14C2-6345-D321

Parent topic: [JACE-9000 backup and restore overview](#)

Validating the MicroSD card's Host ID

The JACE-9000 Host ID depends on the presence of a MicroSD card. This ties the license file to the Host ID on an MicroSD card and makes it portable. All MicroSD cards are programmed with the Tridium secret, which validates the authenticity of the MicroSD card-based Host ID established using Card Identification (CID) values. The CID number is a unique identifier or serial number created on the MicroSD card at the time of manufacturing.

The controller is plugged into the wall outlet with its power off.

1. Insert a MicroSD card into the card slot.
2. Turn the power on.

If no MicroSD card is present, the device uses a CPU-based Host ID. When the MicroSD is present at boot time, the MicroSD card is checked for authenticity using the Tridium secret. The Host ID's authenticity will be verified. If the MicroSD card fails authentication, the Host ID is considered invalid. If the MicroSD card passes authentication, the MicroSD card-based Host ID will be used.

Parent topic: [JACE-9000 backup and restore overview](#)

Backup procedures

You may back up a controller automatically or manually using the system shell or the Workbench's **PlatformAdministration** feature.

- [Creating an automatic backup to an SD Card](#)
You may create a backup while a station is running or stopped.
- [Creating a manual backup to an SD Card](#)
The serial menu option Create SD backup manually creates a backup.
- [Backing up a station using Platform Administration](#)
The **Platform Administration** view performs a complete backup of the connected controller, saved as a .dist file on your PC. The backup dist contains the entire station folder, the specific NRE config used by the platform, license(s), certificate(s), pointers to the appropriate NRE core, Java VM, modules, OS and the TCP/IP configuration of the host.
- [Resetting platform credentials \(JACE-9000\)](#)
Occasionally a situation will arise where you have a functional JACE-9000 controller but no valid credentials or system passphrase. This could be due to a change in building ownership or control contractors. The Platform Account Recovery feature provides you with a secure method of regaining access to the controller without losing station data and configuration.

Creating an automatic backup to an SD Card

You may create a backup while a station is running or stopped.

You have a microSD card.

1. Confirm that the controller's power is off.
2. Insert the microSD card.
3. Apply power to the controller.
The system initiates an automatic backup at 02:00 local time daily. The most recent three backups are stored on the microSD card. The system removes older versions.

Parent topic: [Backup procedures](#)

Creating a manual backup to an SD Card

The serial menu option Create SD backup manually creates a backup.

You have installed Niagara and commissioned the controller with up-to-date core software.

1. Start the controller.
2. Make a serial connection from your PC to controller's Debug serial port.
3. Run the shell command to display **ATLAS System Shell** using the controller's platform credentials.

```
ATLAS System Shell
```

```
-----  
hostid: ATLAS-SD-F93E-14C2-6345-D321  
serial number: 0  
system time: Tue May  2 14:17:37 EDT 2023  
niagara daemon port: https 5011  
  
en0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP gr  
oup  
default qlen 1000  
link/ether 00:01:f0:96:41:8d brd ff:ff:ff:ff:ff:ff
```

```

    inet 172.31.67.86/22 brd 172.31.67.255 scope global noprefixroute
en0
    valid_lft forever preferred_lft forever
    inet6 fe80::201:f0ff:fe96:418d764 scope link
    valid_lft forever preferred_lft forever
en1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOW
N
    group default qlen 1000
    link/ether 00:01:f0:96:41:8c brd ff:ff:ff:ff:ff:ff
-----

```

```

1  Update System Time
2  Update Network Settings
3  Ping Host
4  System Diagnostic Options
5  Change Current User Password
6  Change System Passphrase
7  Create SD Backup
8  Restore SD Backup
9  Reboot
L  Logout

```

Enter Choice : 7

4. To start the manual backup , enter option no 7 Create SD Backup.
The shell prompts you to confirm this action.

Do you want to start backup now? [y/N]? y

5. To start the backup, type y.
The backup procedure starts and, when finished, displays “Backup Successful.”

```

Backup Started,
Please wait for backup to complete...
Backup Successful


```

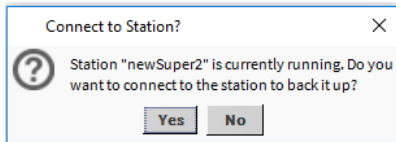
Parent topic: [Backup procedures](#)

Backing up a station using Platform Administration

The **Platform Administration** view performs a complete backup of the connected controller, saved as a .dist file on your PC. The backup dist contains the entire station folder, the specific NRE config used by the platform, license(s), certificate(s), pointers to the appropriate NRE core, Java VM, modules, OS and the TCP/IP configuration of the host.

You are working in Workbench and are connected to the Supervisor or remote controller.

1. Expand the **Platform** node in the Nav tree or double-click **Platform**.
The contents of the Nav Container View opens in the tree or in the main view.
2. Double-click the  **Platform Administration**.
The **Platform Administration** view opens.
3. Click the **Backup** button.
If the station is running, Workbench asks you to confirm that you intend to connect to the station to back it up.

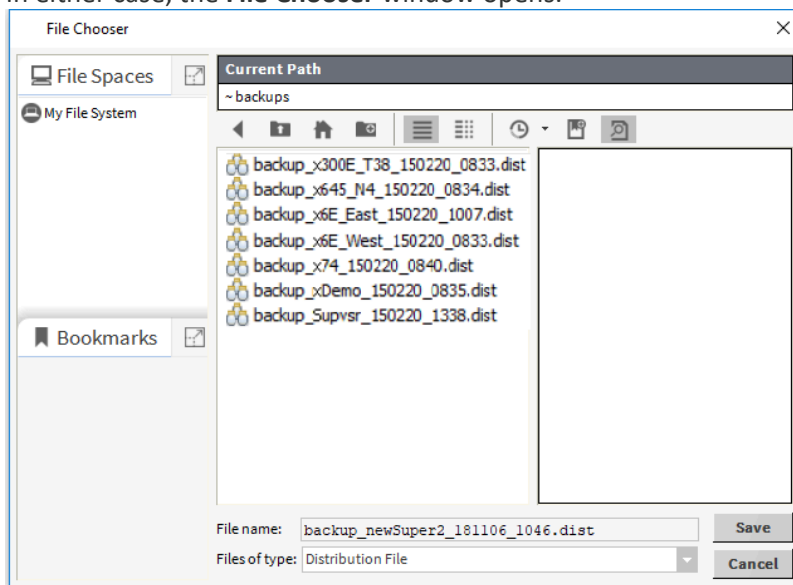


You can perform a backup with a station running on the target host, or when no station is running.

4. If you choose to stop the station, click **No**, double-click the **Application Director**, select the station, click **Stop**, then go back and click **Platform Administration > Backup**.
If no station is running on the controller, the platform daemon performs its own offline backup or you may log in as a station user.

If the station is running, Workbench uses the station's **BackupService** to perform an online backup.

In either case, the **File Chooser** window opens.



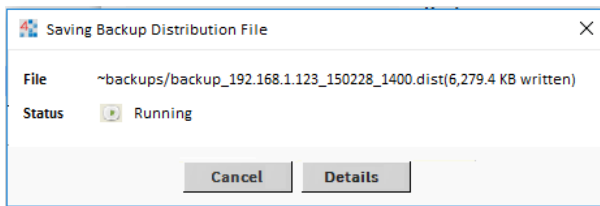
The Current Path defaults to ~backup and the File name property defaults to the current station. The ~ in the path name represents the path to a folder under the file system's Workbench User Home. For example: C:\Users\<user>\<Niagara version>\tridium\backups where:

- <user> is your user folder.
- <Niagara version> is your installed version.

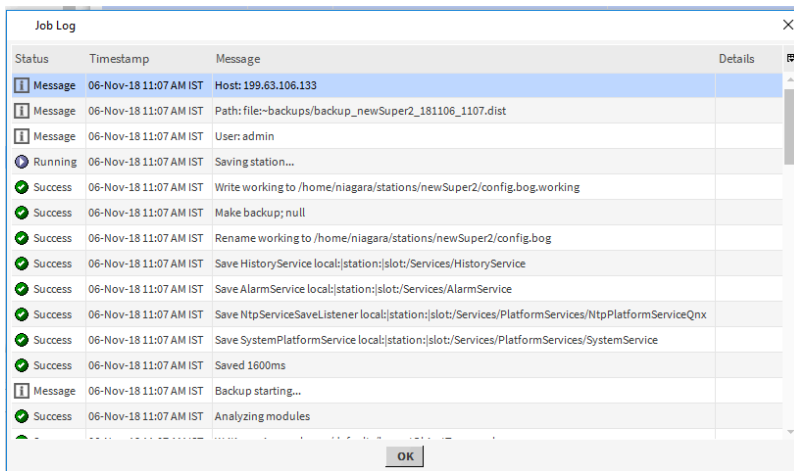
5. Navigate to a target location to save the backup file, rename it if desired, and click **Save**.
By default, the backup function automatically creates (if not already present) a backups subdirectory under your Workbench User Home. The default file name for a backup file uses a format of:
backup_stationName_YYMMDD_HHMM.dist

If the station is running, the system performs a Fox Backup job and a notification popup opens in the lower right of your display when the backup is done. This job is recorded in the station's **BackupService** and is visible in that component's **Backup Manager** view. Details are also available by accessing the job in the station's **Job Service Manager**.

If you perform an offline backup (no station running), the platform daemon provides another progress window during the backup to the .dist file.



Upon completion, you can click **Close** to return to the **Platform Administration** view, or click **Details** to see another popup with a log of actions performed in the backup.



If needed, you can restore a backup .dist using the platform **Distribution File Installer** view. When restoring the backup, you can select to restore these settings, or retain the TCP/IP settings currently in use by the target host.
Parent topic: [Backup procedures](#)

Resetting platform credentials (JACE-9000)

Occasionally a situation will arise where you have a functional JACE-9000 controller but no valid credentials or system passphrase. This could be due to a change in building ownership or control contractors. The Platform Account Recovery feature provides you with a secure method of regaining access to the controller without losing station data and configuration.

You should have access to the following items and information before starting this task.

- A USB-C cable to connect the controller to your PC.
- A terminal emulator (system shell) program, such as PuTTY, installed on your PC.
- During the procedure, you will be prompted to provide the Host id and “proof of ownership” for this controller.

Resetting platform credentials is accomplished using a multi-step process that involves using serial shell software plus contacting your Support channel, and interacting with Tridium by phone or email in order to initiate a secure method of validating that you (the serial shell user) are authorized to reset the platform credentials and system passphrase.

Note: The controller must be rebooted to initiate this procedure. This process could take several hours to

complete, depending on your access to cell phone or internet service.

1. If the controller is running, press and hold the SHUTDOWN button until the BEAT light stops blinking (about 5 seconds).
 2. Remove power from the controller.
 3. Connect a USB-C cable from your PC to the controller DEBUG port.
 4. Open a terminal emulator (system shell) program and connect to the controller. See the “Connecting to the controller system shell” topic for details on connecting.
-
5. Important:

In this step, you need to monitor the terminal emulator window and respond to prompts using the PC keyboard.

- You have just a few seconds to press the Escape key. If you press **Esc** too late, you will not get the **Boot Options** menu and will need to repeat the reboot process.
- If you press **Esc** after the **Boot Options** menu appears, the system will ignore further input until an alphabetic character is entered (for example, the letter “a”). If this happens and the menu does not respond to input, do the following:
 - a. Enter the letter “a” (you may need to press the keyboard twice) or any other alphabetic (non-numeric) character to exit the Escape mode.
 - b. Delete the alphabetic character that you just entered and continue the process as described below.

Power up the controller and during the boot sequence, press **Esc** when you see the following message:
 Press ESC to enter boot options....
 The **Boot Options** menu displays, as shown below.

```

Boot Options
-----
1 Reset platform credentials
2.Continue with boot

Enter Choice :_
  
```

6. Type **1** in the **Enter Choice:** field to select “Reset platform credentials”, and enter **Y** to confirm and continue.
 The **Platform Access Recovery** screen displays, showing the controller’s Host id and a randomly generated Token with additional instructions, as shown.

```

*****
**** Platform Access Recovery ****
*****
Host id      : ATLAS-SD-F84C-2E6D-D888-BB87

Token       : AE85-2F72-DA11-260C

Key version: 1
  
```

Contact technical support and provide them with the hostId and token.
 Token is valid for 24 hours.

Recovery process will exit if key is not provided within 24 hours.

Would you prefer to enter key in:

- 1 Single line (best when key is copied from email)
- 2 Multiple lines (best when receiving key over voice)

Enter Choice :

7. Contact your appropriate Support channel and request credential/system passphrase reset for the Host id shown on-your screen.
8. When prompted, provide the support representative with the required “proof of ownership” for the controller.
Once proof of ownership is established the support representative will notify Tridium.
9. When prompted In the **Platform Access Recovery** screen, enter the customer name. For example, Joe NewBuildingOwner.
10. Contact Tridium (either via phone or email) and provide the generated token, the Host id, and the customer name entered in the previous step.

The Tridium representative validates your customer identity via Niagara Licensing, and generates a “Signature” for the token/Host id/customer name that includes a Reset Authorization Key. This Signature is sent to you either by phone or email.

CAUTION: The Reset Authorization Key is valid only for 24 hours from the time it is generated. If you do not enter the key in the Platform Access Recovery screen within the 24 hour period, you must start over with step 1 of this procedure to obtain another Key.

11. Once you have received the Signature, in the **Platform Access Recovery** screen indicate your preference for entering the Reset Authorization Key in the serial shell window; enter one of the following:
 - Enter **1** for Single Line (best when the Key is copied from email), and at the “Enter Key” prompt paste the Reset Authorization Key. After checking the key enter **v** to verify it (or if necessary, enter **1** to edit the key and then **v** to verify it.)
Enter choice: 1

Enter Key: aa

Please check the key & edit it if necessary

1) Edit key: aa
v) Verify key
Enter choice: v
 - Enter **2** for Multiple Line (best when receiving the Key over voice), and at the “Enter line x” prompts enter the string of characters as instructed. After checking your entries enter **v** to verify the key.

Enter choice: 2

Enter line 1: xxxxxxxxxxxx

Enter line 2: xxxxxxxxxxxx

Enter line 3: xxxxxxxxxxxx

Enter line 4: xxxxxxxxxxxx

Please check the entries & edit them if necessary

1) Edit line 1: xxxxxxxxxxxx

2) Edit line 2: xxxxxxxxxxxx

3) Edit line 3: xxxxxxxxxxxx

4) Edit line 4: xxxxxxxxxxxx

v) Verify key

Enter choice:v

The controller uses the previously installed `tridium` certificate to verify that this Signature was generated by private key for the given token/Host id/customer name values. Afterwards, the system software generates the factory default username/password credentials and default system passphrase.

The serial shell window displays the following text and reboots after the specified amount of time:

```
Verification Passed
```

```
System user credentials are reset  
Shutdown in 10 seconds
```

12. Make a serial or platform connection to the controller. On detecting default credentials, the system prompts you to change the default credentials and default system passphrase before completing the platform connection.

On completion, you can login and access the station data and configuration as you normally would.

Parent topic: [Backup procedures](#)

Restore procedures

The following sections describe how to restore a JACE-9000 from a backup.

Below enhancements are implemented in JACE-9000:

- To move a backup to a new JACE-9000 requires that the controller is connected to your PC serial port using a serial shell program, such as Putty. This is true even if both the old and new controller have the same passphrase.
- A microSD card is formatted as a FAT32 partition and you use a system passphrase to encrypt backups. Therefore, if you have a backup of a system and the passphrase, you can extract the station data using a Linux or Windows PC.
- [Restoring from a microSD card backup](#)
Restoring from a microSD card backup returns the controller to the state it was in when the system made the backup. You may restore to a controller other than the one on which the backup was made, provided that the target controller is the same model. The restore procedure does not require access to Workbench. Launch the System Shell and use the shell menu to initiate a back up the data to the microSD card from the controller's Embedded MultiMediaCard (eMMC), where it is stored.
- [Restoring a backup distribution file](#)
This procedure restores a controller to a factory default state.
- [Restoring factory defaults \(JACE-9000\)](#)
The process of recovering factory defaults deletes all platform and station data, and returns the controller to the state it was in when it shipped from the factory. If you cannot commission the controller because you made an error when entering the default platform daemon credentials or passphrase, you can restore factory defaults and start again. Also, when decommissioning a controller, a best practice is to recover the factory defaults, which removes the platform and station data from the controller. This procedure uses a terminal emulator program to access the controller's system shell menu.

Restoring from a microSD card backup

Restoring from a microSD card backup returns the controller to the state it was in when the system made the backup. You may restore to a controller other than the one on which the backup was made, provided that the target controller is the same model. The restore procedure does not require access to Workbench. Launch the System Shell and use the shell menu to initiate a back up the data to the microSD card from the controller's Embedded MultiMediaCard (eMMC), where it is stored.

You have a MicroSD card with a backup.

1. Connect your PC to the Debug serial port using a USB-C cable.
2. Log in to System Shell menu.
The **Restore Menu** opens. If more than one backup exists, the **Restore Menu** lists the files.

```
Restore Menu
-----
1. backup-20230502141937-v1
Select Backup file for Restore from list(Eg: 1) : 1
Selected backup file for restore: backup-20230502141937-v1
```

3. Select the backup file to restore from the list and press **Enter**.
The System Shell displays the file to restore and prompts with:

```
Is backup passphrase same as the system passphrase [Y/n]? n
Enter the passphrase used to encrypt the backup :
```

Confirm passphrase :

4. Do one of the following:

- Enter Y if the backup passphrase is the same as the system passphrase.
- Enter n if the backup passphrase is not the same as the system passphrase.

The restore operation resets the controller to its factory state, then restores the backup.

Restore operation will take several minutes and performs a few reboots when required

Restore operation will initiate after reboot

Waiting for device to reboot

Press ENTER to continue

Importing Backup

Snapshot backup imported

Snap backup imported

System Configuration backup imported

Restore operation is ongoing

Wait for system installation to complete

<-NOTE: There is currently a long wait with no user feedback after this step

Restoring snapshot of core20

Restoring snapshot of hbt-imx-kernel

Restoring snapshot of network-manager

Restoring snapshot of snapd

Restoring snapshot of tridium-atlas-gadget

Restoring snapshot of tridium-atlas-protod

Restoring snapshot of tridium-atlas-updatemgr

Restoring snapshot of tridium-niagara

Restoring snapshot of tridium-usermgr

Restoring system configuration

Restore Succeeded

Rebooting system

After the backup is restored, the system reboots. This process can take up to five minutes or longer.

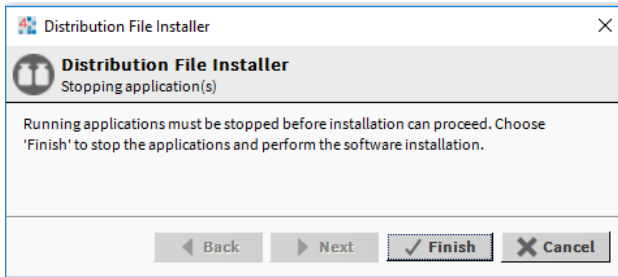
Parent topic: [Restore procedures](#)

Restoring a backup distribution file

This procedure restores a controller to a factory default state.

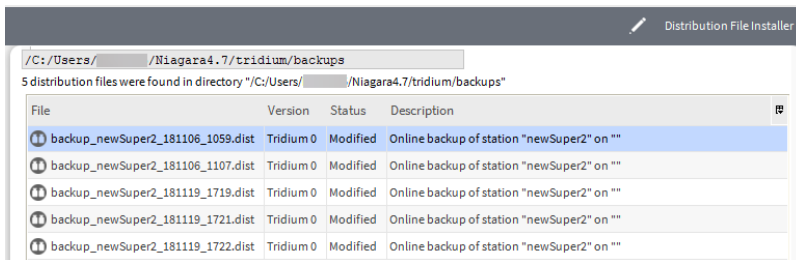
- A backup .dist file of the station on the target controller exists.
- The software database of your niagara4 installation includes matching versions of all software modules used by the station when the station backup was made. Without these modules, restoring the backup .dist will fail.
- Any controlled equipment, which might be adversely affected by the station stopping (and the removal of software) is put in a manually controlled state.
- If the .dist file is protected with a file passphrase, you know this passphrase.

1. Using Workbench, open a platform connection to the remote host.
2. If a station is already running on the remote host, use the **Applications Director** to stop the station.



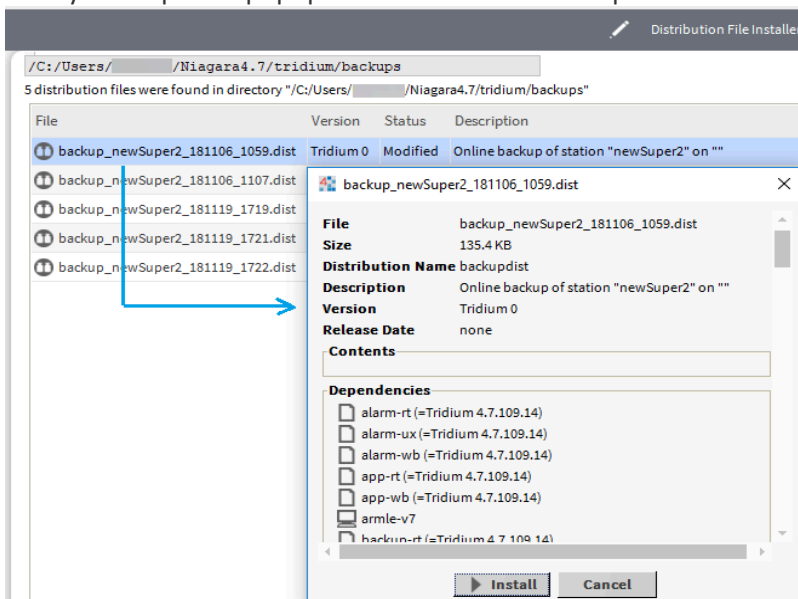
3. To locate the .dist file, do one of the following:
 - In the **Distribution File Installer** click the **Backups** button (📁). This opens the `!/backups` folder.
 - Click the **Choose Directory** button to point to another backup .dist file location.

The Installer parses through the distribution files, and makes selectable only those files that are compatible with the opened platform. When done parsing, available backup .dists open in a list.



Distribution files that are inappropriate, for example those that are for a different target platform or have unmet dependencies, are dimmed and the **Install** button does not become active if you select one of them.

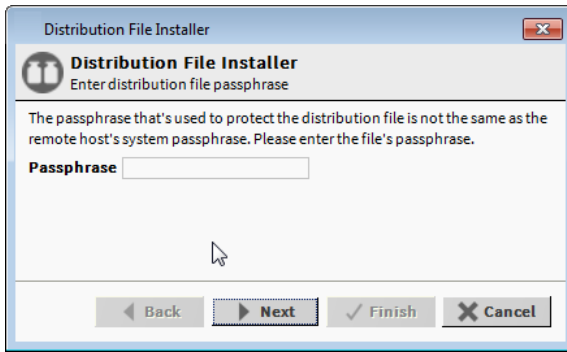
4. For details on any .dist file, double-click it.
The system opens a popup that includes a list of dependencies.



The details window provides information about the selected distribution file, including all contents and any dependencies.

5. To restore any selected backup, click **Install**.

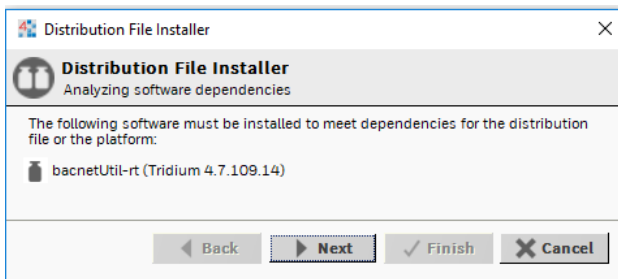
When you click **Install**, the system attempts to validate the file's passphrase. If the file passphrase and system passphrase are the same, the process continues without prompting for a file passphrase. If the file passphrase and system passphrase are different, the distribution file installer prompts you for the passphrase.



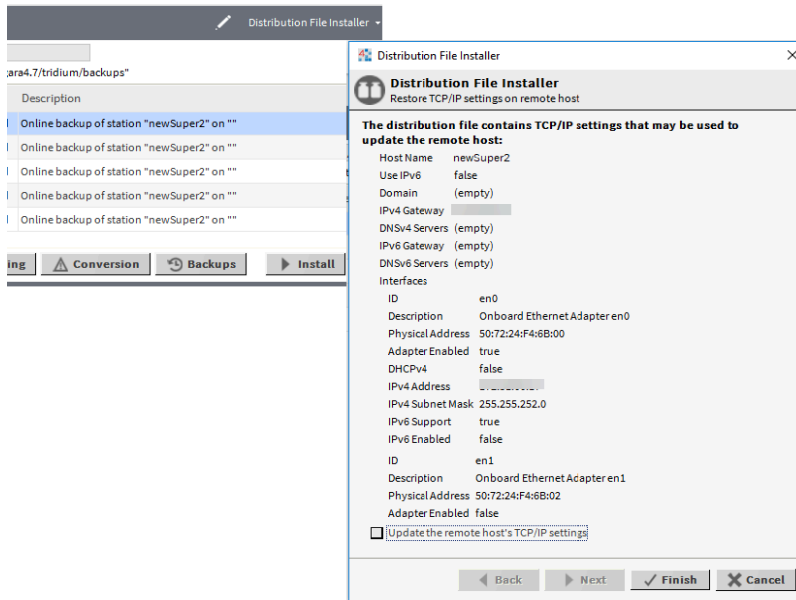
Note: If prompted for the .dist file passphrase and you do not know it, you cannot install the file.

6. If you are prompted for the Passphrase, enter it and click **Next**.
If the host is already running a station, a window opens telling you that the station must be stopped.

If the station backup .dist file contains software modules that are different from (or in addition to) those already installed in the remote host, another window opens:



7. To continue, click **Next**.
Another window asks if you wish to restore the TCP/IP settings stored in the .dist file (as displayed) into the remote host.

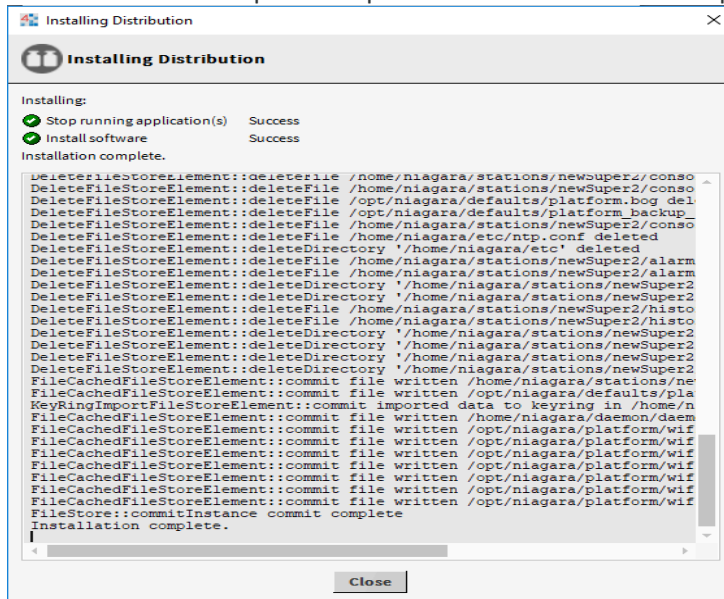


The TCP/IP settings contained in the .dist file are listed, and by default, the check box Update the remote host's TCP/IP settings is cleared.

8. Do one of the following:
 - To use the same .dist file on differently addressed hosts, leave this check box cleared.
 - To use the TCP/IP settings stored in the .dist file, enable the Update the remote host's TCP/IP settings check box.

Depending on your choice, after the .dist file installs and the host reboots, it retains its current TCP/IP settings or uses the TCP/IP settings stored in the .dist file.

9. To begin the installation, click **Finish**.
The .dist installation process opens a window that tracks its progress.



The installer automatically stops the station, then continues with the distribution file install process, which overwrites the station. After the distribution file (and modules, if selected) are installed on the platform, the controller reboots, and the progress window indicates complete.

10. To continue, click **Close** and open a new platform connection, perhaps to view output in the **Application**

Director.

Parent topic: [Restore procedures](#)

Restoring factory defaults (JACE-9000)

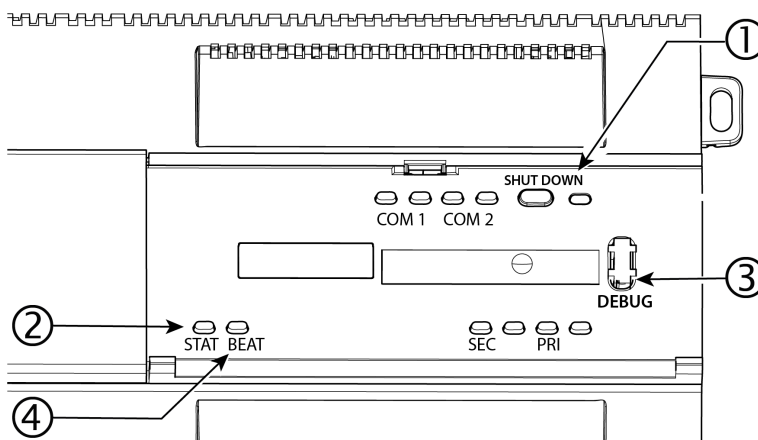
The process of recovering factory defaults deletes all platform and station data, and returns the controller to the state it was in when it shipped from the factory. If you cannot commission the controller because you made an error when entering the default platform daemon credentials or passphrase, you can restore factory defaults and start again. Also, when decommissioning a controller, a best practice is to recover the factory defaults, which removes the platform and station data from the controller. This procedure uses a terminal emulator program to access the controller's system shell menu.

- You have administrator-level platform credentials.
- You have backed up all data from the controller.
- If you are planning a “power—on” reboot using the serial shell menu
 - The controller's **DEBUG** port is connected to your PC using a USB-to-USB-C cable.
 - Power is currently applied to the controller.
 - You are logged into to the controller serial shell using a terminal emulator (system shell program), such as PuTTY and the serial shell menu is visible on your PC.

CAUTION: Recovering factory defaults removes all platform and station data from the device. Make sure this is what you intend before you follow this procedure.

To reset a JACE-9000 to factory default state:

1. With the outer panel cover open, press and hold the **SHUT DOWN** button on the JACE-9000 control panel.



- | | |
|---|--|
| 1 | SHUT DOWN shuts down the controller and serves as the factory defaults recovery button. |
| 2 | STAT (status LED) blinks during recovery of factory defaults. |
| 3 | DEBUG port is a USB-C port for serial debug communications between the controller and serial shell running in the PC. |
| 4 | BEAT (Yellow); heartbeat LED that blinks at 1Hz during normal operation. Refer to “BEAT (Heartbeat) LED” section for |

details.

2. While still pressing the **SHUT DOWN** button, reboot the controller using one of the following actions:
 - [Add power to a powered off controller.](#)
 - [Choose option 9 Reboot from the serial shell menu and enter “Y” at the confirmation prompt.](#)

Reboot is initiated.

3. Release the **SHUT DOWN** button 5 seconds after reboot is initiated.
Factory default restoration process begins.

When the **BEAT** LED blinks at normal rate the process is complete.

To setup the restored controller platform you will need to login to the serial shell using factory default credentials.

Parent topic: [Restore procedures](#)