

# Technical Document

## **JACE-9000 Backup and Restore Guide**

**July 15, 2023**

niagara<sup>4</sup>

# JACE-9000 Backup and Restore Guide

## **Tridium, Inc.**

3951 Westerre Parkway, Suite 350  
Richmond, Virginia 23233  
U.S.A.

## **Confidentiality**

The information contained in this document is confidential information of Tridium, Inc., a Delaware corporation ("Tridium"). Such information and the software described herein, is furnished under a license agreement and may be used only in accordance with that agreement.

The information contained in this document is provided solely for use by Tridium employees, licensees, and system owners; and, except as permitted under the below copyright notice, is not to be released to, or reproduced for, anyone else.

While every effort has been made to assure the accuracy of this document, Tridium is not responsible for damages of any kind, including without limitation consequential damages, arising from the application of the information contained herein. Information and specifications published here are current as of the date of this publication and are subject to change without notice. The latest product specifications can be found by contacting our corporate headquarters, Richmond, Virginia.

## **Trademark notice**

BACnet and ASHRAE are registered trademarks of American Society of Heating, Refrigerating and Air-Conditioning Engineers. Microsoft, Excel, Internet Explorer, Windows, Windows Vista, Windows Server, and SQL Server are registered trademarks of Microsoft Corporation. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Mozilla and Firefox are trademarks of the Mozilla Foundation. Echelon, LON, LonMark, LonTalk, and LonWorks are registered trademarks of Echelon Corporation. Tridium, JACE, Niagara Framework, and Sedona Framework are registered trademarks, and Workbench are trademarks of Tridium Inc. All other product names and services mentioned in this publication that are known to be trademarks, registered trademarks, or service marks are the property of their respective owners.

## **Copyright and patent notice**

This document may be copied by parties who are authorized to distribute Tridium products in connection with distribution of those products, subject to the contracts that authorize such distribution. It may not otherwise, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior written consent from Tridium, Inc.

Copyright © 2023 Tridium, Inc. All rights reserved.

The product(s) described herein may be covered by one or more U.S. or foreign patents of Tridium.

# Contents

<b>About this Guide .....</b>	<b>5</b>
Document change log .....	5
Related documentation .....	5
<b>Chapter 1 JACE-9000 backup and restore overview.....</b>	<b>7</b>
About Host ID .....	8
Validating the MicroSD card's Host ID .....	8
<b>Chapter 2 Backup procedures.....</b>	<b>9</b>
Creating an automatic backup to an SD Card.....	9
Creating a manual backup to an SD Card.....	9
Backing up a station using Platform Administration.....	10
<b>Chapter 3 Restore procedures.....</b>	<b>13</b>
Restoring from a microSD card backup.....	13
Restoring a backup distribution file .....	14
Restoring factory defaults (JACE-9000) .....	18



## About this Guide

This topic contains important information about the purpose, content, context, and intended audience for this document.

### Product Documentation

This document is part of the Niagara technical documentation library. Released versions of Niagara software include a complete collection of technical information that is provided in both online help and PDF format. The information in this document is written primarily for Systems Integrators. To make the most of the information in this book, readers should have some training or previous experience with Niagara software, as well as experience working with JACE network controllers.

### Document Content

This document includes topics that describe how to create USB backups and restore them to your controller. Also included are instructions for recovering factory defaults, and safely shutting down a controller.

## Document change log

Updates and changes to the document are listed in this topic.

### July 15, 2023

Initial release publication.

## Related documentation

Additional related information is available in the following document(s).

- *JACE-9000 Controller (15885) Mounting and Wiring Guide*
- *JACE-9000 Install and Startup Guide*
- *Niagara Platform Guide*



# Chapter 1 JACE-9000 backup and restore overview

## Topics covered in this chapter

- ◆ About Host ID
- ◆ Validating the microSD card's Host ID

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 Supervisorplatform using Platform Administration connection.

Following are options for restore:

- Restoring from a microSD card backup
- Restoring from a backup `.dist` file

## Backup to the microSD card

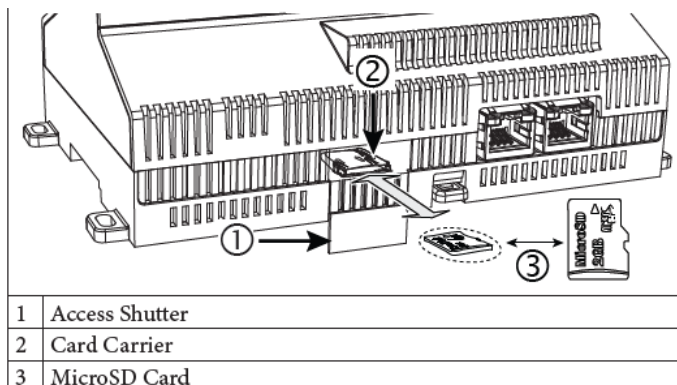
The JACE-9000 allows you to backup the entire controller platform and station to a microSD card without requiring access to the backup functions of Workbench.

- 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 JACE 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`

## 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.

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

**Step 1** Insert a MicroSD card into the card slot.

**Step 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.



# Chapter 2 Backup procedures

## Topics covered in this chapter

- ◆ Creating an automatic backup to an SD Card
- ◆ Creating a manual backup to an SD Card
- ◆ Backing up a station using Platform Administration

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.

**Prerequisites:** You have a microSD card.

**Step 1** Confirm that the controller's power is off.

**Step 2** Insert the microSD card.

**Step 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.

## Creating a manual backup to an SD Card

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

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

**Step 1** Start the controller.

**Step 2** Make a serial connection from your PC to controller's Debug serial port.

**Step 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 group
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:fe96:418d/64 scope link
    valid_lft forever preferred_lft forever
en1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN
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

**Step 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

**Step 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

```

## 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.

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

**Step 1** Expand the **Platform** node in the Nav tree or double-click **Platform**.

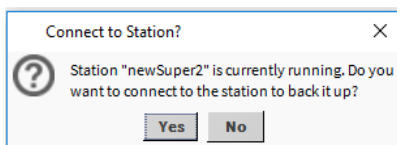
The contents of the Nav Container View opens in the tree or in the main view.

**Step 2** Double-click the  **Platform Administration**.

The **Platform Administration** view opens.

**Step 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.



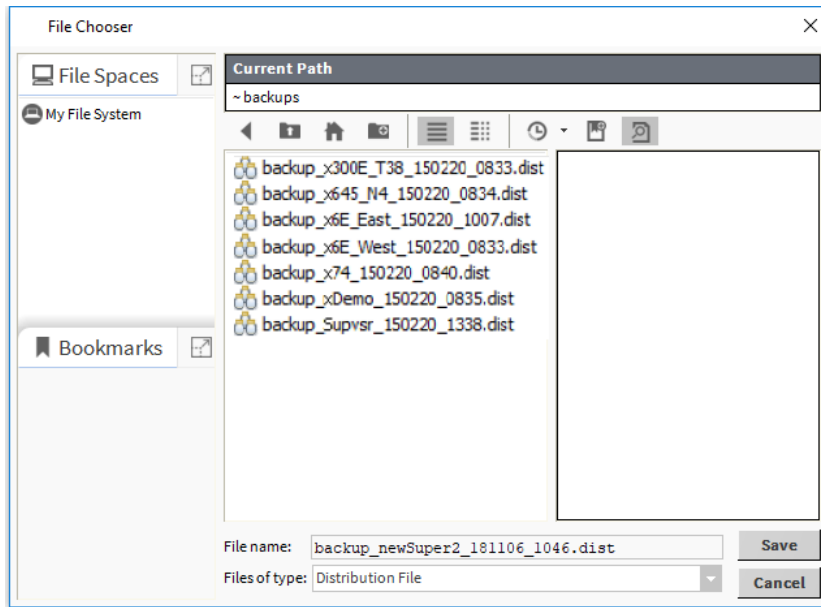
You can perform a backup with a station running on the target host, or when no station is running.

**Step 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.

Workbench uses the 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:

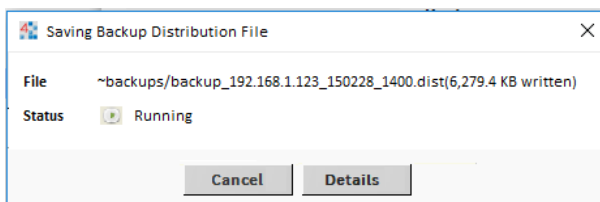
- `<user>` is your user folder.
- `<Niagara version>` is your installed version.

**Step 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.

| Job Log |                        |                                                                                                   |         |    |
|---------|------------------------|---------------------------------------------------------------------------------------------------|---------|----|
| Status  | Timestamp              | Message                                                                                           | Details |    |
| Message | 06-Nov-18 11:07 AM IST | Host: 199.63.106.133                                                                              |         |    |
| Message | 06-Nov-18 11:07 AM IST | Path: file:~backups/backup_newSuper2_181106_1107.dist                                             |         |    |
| Message | 06-Nov-18 11:07 AM IST | User: admin                                                                                       |         |    |
| Running | 06-Nov-18 11:07 AM IST | Saving station...                                                                                 |         |    |
| Success | 06-Nov-18 11:07 AM IST | Write working to /home/niagara/stations/newSuper2/config.bog.working                              |         |    |
| Success | 06-Nov-18 11:07 AM IST | Make backup; null                                                                                 |         |    |
| Success | 06-Nov-18 11:07 AM IST | Rename working to /home/niagara/stations/newSuper2/config.bog                                     |         |    |
| Success | 06-Nov-18 11:07 AM IST | Save HistoryService local: station: slot: Services/HistoryService                                 |         |    |
| Success | 06-Nov-18 11:07 AM IST | Save AlarmService local: station: slot: Services/AlarmService                                     |         |    |
| Success | 06-Nov-18 11:07 AM IST | Save NtpServiceSaveListener local: station: slot: Services/PlatformServices/NtpPlatformServiceQnx |         |    |
| Success | 06-Nov-18 11:07 AM IST | Save SystemPlatformService local: station: slot: Services/PlatformServices/SystemService          |         |    |
| Success | 06-Nov-18 11:07 AM IST | Saved 1600ms                                                                                      |         |    |
| Message | 06-Nov-18 11:07 AM IST | Backup starting...                                                                                |         |    |
| Success | 06-Nov-18 11:07 AM IST | Analyzing modules                                                                                 |         |    |
|         |                        |                                                                                                   |         | OK |

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.

# Chapter 3 Restore procedures

## Topics covered in this chapter

- ◆ Restoring from a microSD card backup
- ◆ Restoring a backup distribution file
- ◆ Restoring factory defaults (JACE-9000)

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 backup up the data to the microSD card from the controller's Embedded MultiMediaCard (eMMC), where it is stored.

**Prerequisites:** You have a MicroSD card with a backup.

**Step 1** Connect your PC to the Debug serial port using a USB-C cable.

**Step 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

**Step 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 :

**Step 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.

## Restoring a backup distribution file

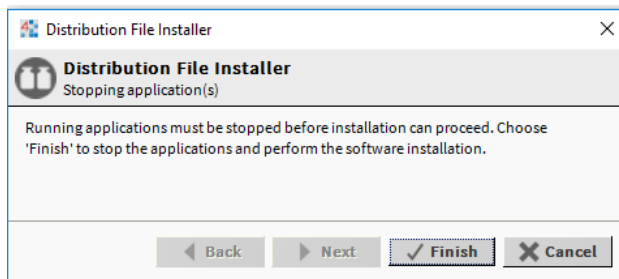
This procedure restores a controller to a factory default state.

### Prerequisites:

- A backup **.dist** file of the station on the target controller exists.
- The software database of your Niagara 4 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.

**Step 1** Using Workbench, open a platform connection to the remote host.

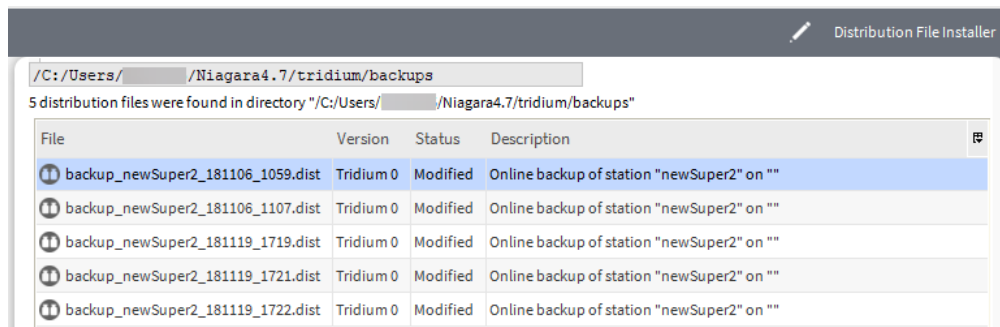
**Step 2** If a station is already running on the remote host, use the **Applications Director** to stop the station.



**Step 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.

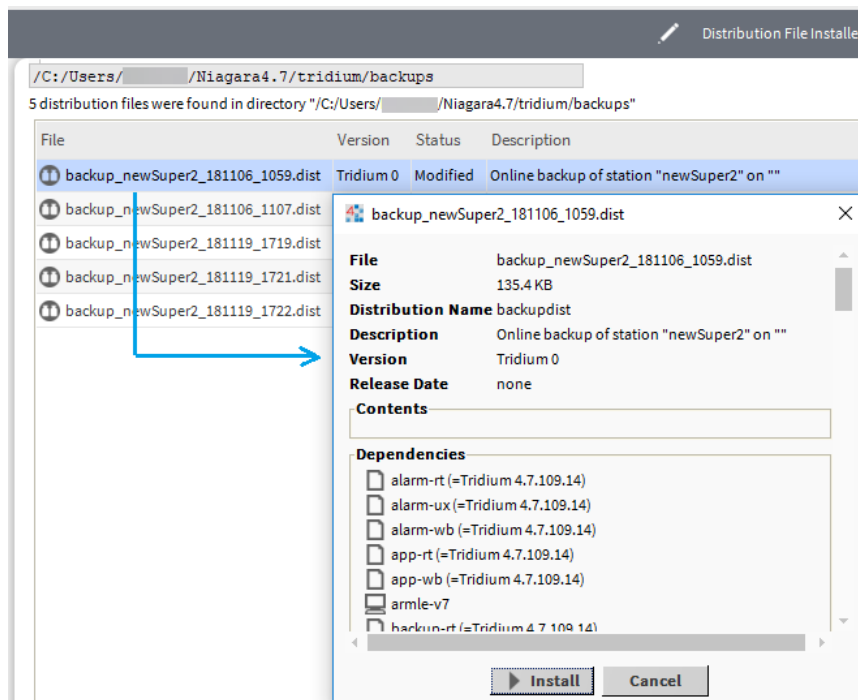
The Installer parses through the distribution files, and makes selectable only those files that are compatible with the opened platform. When done parsing, available backup .dist's open in a list.



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.

**Step 4** For details on any .dist file, double-click it.

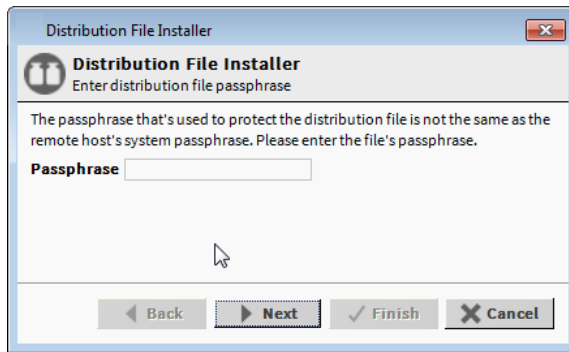
The system opens a popup that includes a list of dependencies.



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

**Step 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.

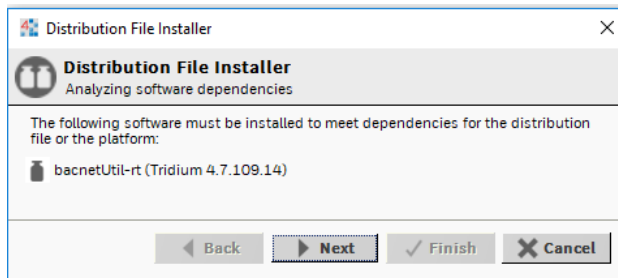


**NOTE:** If prompted for the `.dist` file passphrase and you do not know it, you cannot install the file.

**Step 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.

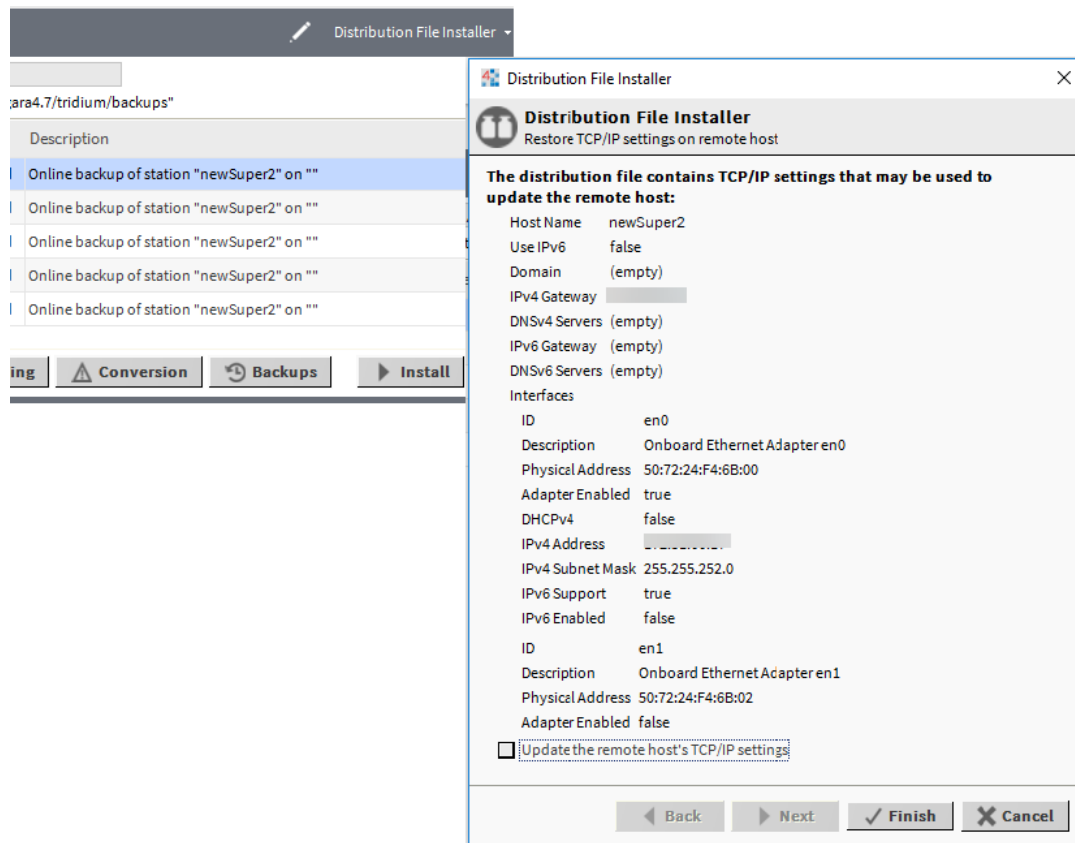
If the station backup `.dist` file contains software modules that are different from (or in addition to) those already installed in the remote host, another window opens:



**Step 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.

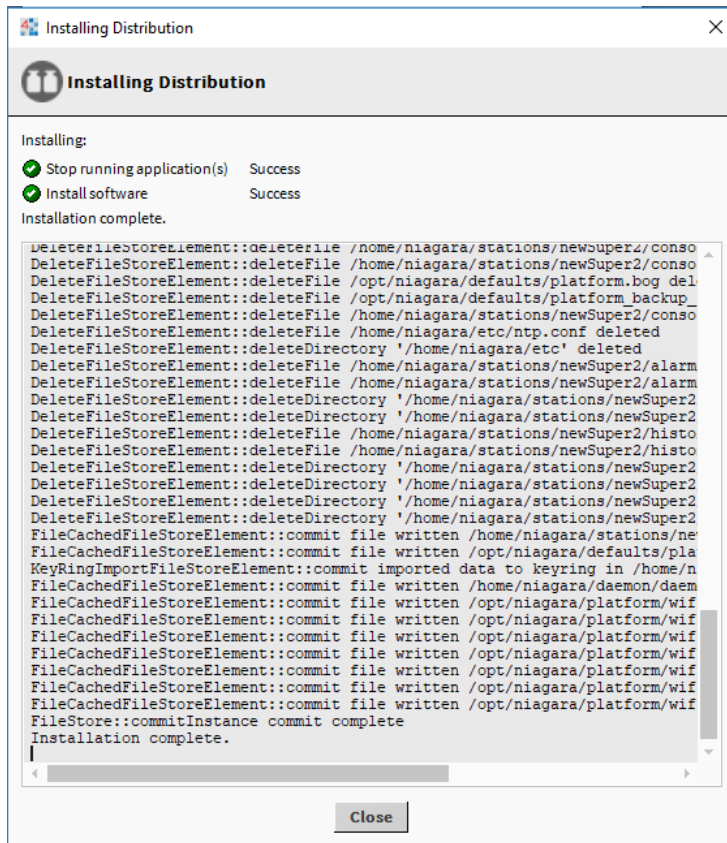
**Step 8** Do one of the following:

- 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.

**Step 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.

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

## 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.

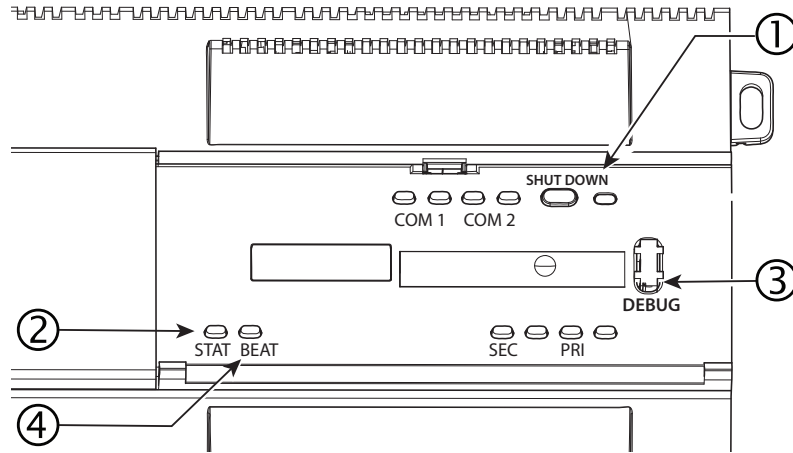
### Prerequisites:

- 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-micro USB cable.
  - Power is currently applied to the controller.
  - You are logged into 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:

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



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

**Step 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.

**Step 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.

