EcoStruxure™ IT Data Center Expert 9.2.0 Release Notes

Table of Contents

Part Numbers Affected 1
Minimum System Requirements 1
New Features 1
Issues Fixed 5
Known Issues 6
Upgrade Procedure 7
Restoring using ISO Format (Data Center Expert hardware server only) 8
Migrating a Data Center Expert hardware server to a virtual appliance 8
Creating a bootable USB Key (Windows or Linux machine) 9

Note: The 25-node 1-year subscription entitlement previously associated with Data Center Expert appliance licensing has been removed.

Part Numbers Affected

- AP9465
- AP9470
- AP9475
- AP94VMTRL

Server hardware requirements
For the list of the server appliances (AP9465, AP9470, and AP9475) supported by DCE, see
Data Center Expert 7.9.x and newer - server hardware requirements

Minimum System Requirements

The Data Center Expert desktop client is a stand-alone Java application that runs on systems that meet the following requirements:

- A PC with a 1-GHz or better AMD/Intel processor running a 64-bit operating system: Microsoft® Windows® Server 2019, 2022, and 2025; Windows 10 and 11
- At least 2 GB of RAM and 20 GB disk space
- Screen resolution should be set to at least 1024 x 768.
- Supported browsers: Microsoft Edge; Mozilla® Firefox®; Google Chrome™
  Note: See Known Issues in DCE for details about support for Internet Explorer and Edge.
- The web client requires a minimum screen width of 1024 pixels.

New Features

This release contains enhancements including:

Desktop client

- **Required passwords for backups**
  A password is now required for all backup configurations, and administrators are alerted at login to set passwords on existing backup configurations if they are not present. To configure a backup password, go to **System > Server Administrator Settings > Server Backup/Restore**.

- **Administrators can terminate other users' sessions**

© 2026 Schneider Electric. All rights reserved

Confidential

Administrators can now manage and terminate all active Desktop Client, Web Client, and REST API sessions from the **Logged On Users** view. Access this view by clicking the **User: [name]** indicator in the bottom-right status bar of the desktop client. The terminated user receives a notification and is logged out of the client.

- **Improved chained certificate imports**
  You can now import DCE server chained SSL certificates into the desktop client change certificate wizard. Go to **System > Server Administration Settings > Server Access > Change Certificate...**
  When importing a certificate chain, certificates must be provided in the correct order: **Server/Leaf Certificate** → **Intermediate Certificate(s)** → **Root Certificate**. Importing certificates in an incorrect order may prevent chain validation and can result in misleading errors, such as a private key mismatch.

Web client

- **Device Groups Tree**
  All device groups are now displayed and selectable in the **Monitoring** tab. The **Active Alarms** list and **Devices** list are automatically filtered based on the selected group.

- **Improved device list in Monitoring**
  The Devices section is now displayed as a table, making it easier to browse devices. You can filter the list, customize displayed columns, and export the device list data to CSV or TXT files.

- **Administrators can terminate other users' sessions**
  Administrators can now manage and terminate all active Desktop Client, Web Client, and REST API sessions. To access it, click the **View Status** icon in the upper-right corner of the web client and select the **Logged On Users** tab. The terminated user receives a notification and is logged out of the client.

- **Desktop notifications for alarms**
  You can now receive desktop notifications for qualifying alarms. Enable the feature in **User Preferences** and configure the minimum alarm severity for notifications. Notifications are displayed even when the application tab is active.

- **Icon notifications for new alarms**
  You can now enable icon notifications in **User Preferences**. A notification indicator is displayed on the browser tab icon when new alarms arrive while you are away from the tab. The indicator is cleared when you return and interact with the application.

- **Request device scan**
  In the **Monitoring** tab, administrators and users with writer permissions can now request a device scan from the **More actions** menu **> Request Scan**.

- **Export Reports as PNG**
  Reports can now be exported as a single image including both the chart and table.

- **Edit a device’s label and type**
  In the **Monitoring** tab, administrators and users with server admin and device admin permissions can now use **More actions > Edit Settings** to change a device's label or type, or reset either value to its default.

- **New dashboard drawer**
  In the **Dashboards** tab, click **Show Dashboard List** to search for dashboards. Dashboards now display a scope indicator icon, with a multi-user icon for global dashboards and a single-user icon for personal dashboards.

- **Filter alarms by device or group**
  In the **Alarms** tab, you can now filter the alarms list without leaving the page. Open the **Filter alarms by device or group** drawer from the toolbar to choose which devices and groups to include.

- **New reports table view**
  Saved Reports can now be browsed in a table view, allowing you to sort and filter reports by criteria such as name, sensors, start date, and end date.

© 2026 Schneider Electric. All rights reserved

Confidential

- **Larger sensor result sets in Reports**
  Added selectable sensor result page sizes (25, 50, 100, 200, and 500), making it easier to generate reports for large sensor sets.

- The event log now includes entries for backup/restore password changes.

General

- **Device scan and upgrade events added to event log**
  Device scans initiated through **Request Device Scan** and DCE server upgrades now generate dedicated event log entries. This makes it easier to identify device scan activity and distinguish upgrade-related restarts from expected or unexpected restart events.

- **REST API best practices**
  Added REST API best practices to the Help documentation in the web client to improve guidance on API usage and integration.

- **Improved subscription expiration warning emails**
  Subscription license expiration notifications sent 90, 60, and 30 days before expiry now identify the functionality affected by license expiration, including software updates, device firmware updates, and camera clip retrieval and export capabilities.

- **Added support for SNMP Opaque OID types for float and double values**
  Note: If your device requires Opaque SNMP OIDs, any existing third-party DDFs may need to be updated to support them. If updates are needed, submit a DDF request through the following link https://app.ecostruxureit.com/request/.

Visit the EcoStruxure IT Help Center for more information about Data Center Expert.

© 2026 Schneider Electric. All rights reserved

Confidential

Server operating system

Server OS: Proprietary Rocky Linux 8.10 (RHEL derivative)

Java Version: java-21-openjdk-headless-21.0.11.0.10-1

Windows desktop client

Java version: Adoptium 8u492-b09

Software vulnerabilities fixed in DCE 9.2.0

The security vulnerabilities addressed in this release include:

- CVE-2026-8044
- CVE-2026-19233

This release includes various component updates to improve overall security.

See the Data Center Expert Security section in the Help Center for more information.

© 2026 Schneider Electric. All rights reserved

Confidential

Issues Fixed

The following issues were fixed in DCE 9.2.0:

- Added WebSocket proxy support for Galaxy NMC4 devices, enabling private-network device launches from an external browser across public/private networks. **Note:** The internal browser does not support WebSockets. NMC4 launches requiring WebSocket connectivity must use an external browser.
- Chained certificates can now be imported through the desktop client, with each certificate in the chain displayed individually in the **Web Server** tab. To access it, go to **System > Server Administration Settings > Server Access**.
  Note: Chained certificate files must be ordered as **Server/Leaf Certificate → Intermediate Certificate(s) → Root Certificate**. Importing certificates in an incorrect order may prevent chain validation and can result in misleading errors, such as a private key mismatch.
- Improved user messaging for backup password configuration.
- Improved session inactivity timeout behavior in the web client.
- The **Save As** option in **Reports** in the web client now creates a copy of the current report instead of renaming it.
- Restoring from backup to the same server will no longer clear the license file.
- In the **Monitoring** page under **Devices**, view-only users can now see the full breadcrumb when viewing a group.
- When users generate sensor history reports, devices in a lost communication state now return null sensor readings, ensuring that minimum, maximum, average, and delta values remain unaffected.
- The report start time in the web client is now accurately preserved when using the refresh button or auto-refresh.
- Report refresh options are now available in the web client for reports using absolute date ranges that end on the current day.
- The text in **Active Alarms** cards on **Dashboards** no longer overflows when the user interface is resized.
- Improved reliability of the GET /v1/devices/sensors endpoint on large-scale deployments, reducing 503 errors through sensor cache optimizations.
- Improved **Monitoring** and **Alarms** responsiveness during large-scale alarm clear/update events, preventing user interface stalls and reducing delays in refreshing alarm data.

© 2026 Schneider Electric. All rights reserved

Confidential

Known Issues

- **Firefox may display "What's New" content from a previous version after an upgrade**
  After upgrading to version 9.2.0, Firefox may display outdated **What's New** content or show translation errors in the monitoring user interface. Clearing the Firefox browser cache resolves the issue.

- The **Change server** and **Reboot** options do not relaunch the desktop client on Windows 11 and Server 2025.

- In the **System** > **Server Administration Settings** > **Server SSL Certificates** > **Certificate** view, there is a slash at the end of some fields when the server is in FIPS mode. This is cosmetic and does not affect functionality.

- Moving a device to a group with multiple nested device groups generates separate event log messages for every parent group above the device.

- Signed server update files do not parse when the DCE server is in FIPS mode. To update the server:

  1. Change the security policy to a policy other than FIPS in the desktop client **System** > **Server Administration Settings** > **Server Access** > **Security Policy** option.
  2. Reboot the server.
  3. Apply the server update.
  4. Go to the **System** > **Server Administration Settings** > **Server Access** > **Security Policy** option and change the security policy back to FIPS.

- When the DCE subscription license expires, the **Surveillance** > **Thumbnails** view shows the camera license as Expired. This can be disregarded.
  Cameras continue to function as licensed cameras, and clips are stored as expected. Cameras are shown as Licensed in **Device** > **Surveillance Settings**.

- Users who have a combination of Device Administrator or View and Control access for some devices and View access for other devices may see an error saving a future maintenance schedule in the web client if they have only View access for any selected devices.
  If **Now** is selected instead of a future time, only devices the user has permission to control will be placed in Maintenance mode. No error is generated.
  View access only devices will be removed from the web client **Maintenance Schedules** view in a future release.

Complete list of known issues in Data Center Expert

Release notes for older versions of Data Center Expert

© 2026 Schneider Electric. All rights reserved

Confidential

Upgrade Procedure

The following steps are necessary to upgrade Data Center Expert 9.1.x to Data Center Expert 9.2.0.

The Data Center Expert 9.2.0 update performs a data migration that takes under an hour for most systems. The data migration can take up to four hours if the system has thousands of devices and years of history.
Do not reboot the server during the update.

Note 1: *Data Center Expert must be at a minimum of version 9.1.0 to upgrade to Data Center Expert 9.2.0. If you are downloading Data Center Expert 9.2.0, you will need access to the Internet.*

Note 2: *Verify the apcsetup, apcinfo, and apcreset passwords before you begin the upgrade.*

NOTICE: Before beginning an upgrade, remember to run a full backup on your Data Center Expert. Go to **System** > **Server Administration Settings** > **Server Backup/Restore**, create a backup entry, and then click **Start**.

It is recommended that you perform the server upgrade when you upload the upgrade file to your DCE server. The upgrade will be performed automatically if the server reboots after the upgrade file is uploaded.

1. Download the upgrade.zip file. DCE software download links

   You must have an active software subscription license for full access to Data Center Expert features. Manage your DCE subscription license on the mySchneider Software Management website.

   Note: The restore.iso file may be needed for later use if a re-installation is required. See Restoring using ISO Format for instructions for restoring your data from a restore.iso file from the ISO format.
2. Log in to your Data Center Expert 9.1.x server with full server access. Select **Updates** > **Apply Server Update**.
3. Click **Import** to import the upgrade.zip file.

   Note: Only the zipped upgrade file is accepted.
4. The Upgrade/New Packages table will update indicating there is an update available for the Data Center Expert server. Check the "Install/Upgrade" option for the package(s) you want to upgrade. Click **Install Selected** to start the upgrade for the selected package(s). You will be prompted to confirm you want to proceed with the upgrade. Click **Install Update** to start the upgrade process.

   Do not reboot the server during the upgrade process.
5. When the file transfer completes, Data Center Expert will restart and disconnect the desktop client. You can point a web browser to the Data Center Expert server for status.
6. When the update is complete, point a web browser to the Data Center Expert server, and select **Download Client.**

© 2026 Schneider Electric. All rights reserved

Confidential

Restoring using ISO Format (Data Center Expert hardware server only)

NOTICE: Only perform the steps in this section if directed to do so by a technical support technician.

Before You Restore: *A system restore will erase all data and restore the Data Center Expert hardware server to its factory default settings. Please make sure you have a copy of all installed license keys and network settings prior to restore.*

1. Download the restore.iso file to create a bootable USB key or contact technical support for assistance.
    a. For a USB Key, follow the instructions provided in Creating a bootable USB Key (Windows or Linux machine.
2. Place the USB key in the USB port of your Data Center Expert server.
3. Reboot Data Center Expert.
4. To boot to USB, press F11.

    Note: Depending on the model, servers may have a different startup look, with the option to press F11 displayed earlier or later in the boot process. For more information, see the server manufacturer instructions.
5. Select the boot menu (may be called BIOS Boot Manager, BIOS boot menu, One-time boot menu, One-shot BIOS Boot Menu, One Time UEFI Boot, or similar)
6. Select your USB Device from the list.

The restore process takes approximately 10 minutes for the 1U Data Center Expert Basic, 15 minutes for 1U Data Center Expert Standard or 25 minutes for 2U Data Center Expert Enterprise. When the restore is complete, you will be prompted to remove the USB key and press Enter to reboot the server.

Once Data Center Expert has restarted, you may configure the Data Center Expert network settings per instructions in the Data Center Expert Installation Guide.

Migrating a Data Center Expert hardware server to a virtual appliance

To migrate a hardware server to a 9.2.0 virtual appliance, you must work with our Customer Success Management team. You will be connected through Schneider Electric's Customer Care Center.

1. Perform a backup of the Data Center Expert hardware server, using the **Server Backup/Restore** option, accessed from the **Server Administration Settings** option in the **System** menu.
2. Deploy the trial version and configure it using the hardware equivalents for the Data Center Expert Basic, Standard, or Enterprise server from which you are migrating. **The available disk space for the virtual appliance must be greater than the disk space used by the hardware server.** You cannot restore to a virtual appliance with fewer CPU, fewer network adapters, less RAM, or less available disk space than the hardware server. See help for Deploying and configuring a Data Center Expert virtual appliance, and Data Center Expert virtual appliance equivalent configurations.
3. Perform a restore on the virtual appliance, using the **Server Backup/Restore** option, accessed from the **Server Administration Settings** option in the **System** menu. You cannot restore to a virtual machine other than the Data Center Expert virtual appliance.
4. Log in to the Data Center Expert client. In the **License** display, accessed from the **Server Administration Settings** option in the **System** menu, click **Update license** and upload the license file you received.

© 2026 Schneider Electric. All rights reserved

Confidential

Creating a bootable USB Key (Windows or Linux machine)

Instructions for a Windows machine:

1. Insert a 4GB (or larger) USB key into your system.
2. Extract the following file to a temporary directory:
   DCExpertUsbFlashRestore_Win_9.2.0.zip
3. Open a command prompt to the temporary directory using the cd command. The command prompt working directory must be the same location as the extracted files.
4. Run mkDCExpertRestoreUsbKey.bat <iso image filename>.
   Example: mkDCExpertRestoreUsbKey.bat c:\tmp\restore.iso
5. Answer the prompts as appropriate.

Instructions for a Linux machine:

1. Insert a 4GB (or larger) USB key into your system.
2. Extract the following file to a temporary directory:
   DCExpertUsbFlashRestore_Linux_9.2.0.tar.gz
3. Open a command prompt to the temporary directory using the cd command. The command prompt working directory must be the same location as the extracted files.
4. Run mkDCExpertRestoreUsbKey.sh <iso image filename>.
   Example: mkDCExpertRestoreUsbKey.sh /tmp/restore.iso
5. Answer the prompts as appropriate.

Third-party USB key scripts:

The USB key scripts used to create USB keys utilize the following software:

Software	URL	Windows	Linux
Syslinux	http://syslinux.zytor.com/	X	X
7-zip	http://www.7-zip.org	X	
GNU sed	http://unxutils.sourceforge.net	X	

© 2026 Schneider Electric. All rights reserved

Confidential