EcoStruxure™ IT Data Center Expert 9.1.1 Release Notes

Table of Contents

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

The DCE 9.1.1 release addresses an issue that caused historical numeric sensor data to be represented as zero during lost communication events.
The data was stored correctly in the database, but was translated incorrectly when pulled from the system, for example via the API or reports.

Data Center Expert 9.1.0

The DCE 9.1.0 release contains enhancements including:

- **Increased maximum supported node count for SNMPv3 devices**
  The maximum supported node count for SNMPv3 devices is now the same as for SNMPv1 devices.

Total supported node count:

- AP9465 - Basic server, supports up to 540 nodes (525 nodes + 15 cameras)
- AP9470 - Standard server, supports up to 2150 nodes (2025 nodes + 125 cameras)
- AP9475 - Enterprise server, supports up to 4275 nodes (4025 nodes + 250 cameras)

See the DCE sizing guide for additional guidance.

- **Increased trial version node count**
  DCE software trial versions for both the server appliance and the VM now support 100 nodes.

- **Desktop client features restricted after trial expires**
  After the trial software license expires, access to features available in the DCE desktop client is restricted by a dialog displayed after login.

  Access is limited to:
  - License, Network Settings, Server Access, and Server SSL Certificate
  - Users and Device Group Access
  - About DCE

  Once a new subscription license file is uploaded, full access to the desktop client is available.

  Note: Access to web client features is not affected.

- **Launch to device using an external browser**
  The **Device Launch Settings** right-click option in the **Device view** and **Map view** now includes a setting to **Always use the external browser.**
  This setting at the device level overrides the internal browser setting configured in File > Client Preferences.

- **Launch to multiple devices at once**
  It is now possible to select and launch to up to ten devices at the same time.

- **Retrieve sensors by type in REST API**
  The ISXCSensorType call was added to the Rest API.

- **Maintenance Mode in REST API**
  The REST API now supports Maintenance Mode.

- **Device info includes MAC address in REST API**
  The REST API includes the device MAC address in the device list. Search by MAC address is now supported.

- **Improved Device Scan Settings dialog**
  The Device Scan Settings dialog for SNMP and Modbus devices now includes a column for **Scan interval**.

- **Server hostname in syslog messages**
  The DCE server hostname is now sent in syslog messages.

- **Improved SNMP Device Configuration dialog**
  The number of target devices selected is now displayed in the **Select Destination Devices** dialog.

- **Improved backup success messages**
  Backup successful or failed messages in the event log, email, and nb log now include the backup file name.

- **Event log absolute time option**
  The absolute time option persists after the browser is refreshed.

Web client

- **Rack access control**
  Administrator users and users with appropriate permissions can lock and unlock rack doors in the web client.
  Note: You configure rack access settings in the desktop client.

  All the doors on both the NetBotz appliance and the Rack Access Pods are named Door 1 and Door 2 by default. DCE cannot determine which appliance or pod the doors are associated with.
  It is recommended that you assign unique names to the doors on each NetBotz appliance and Rack Access Pod 170/175.

- **Outlet control**
  Administrator users and users with appropriate permissions can control outlets in the web client.
  Note: When a command is performed at an outlet that is part of an outlet group, that command will be executed at all outlets in the group.

- **Maintenance Mode**
  Administrator users and users with appropriate permissions can use Maintenance Mode in the web client to enable or disable notifications immediately or on a schedule.

- **Export event log data**
  Event log data can be exported from the web client as a CSV or TXT file.

- **Export graphs**
  Graphs can be exported from the web client as a CSV or PDF file.

- **Sensor history reports**
  You can now generate, manage, save, run, export, and view sensor history reports on the new **Reports** page in the web client.
  Sensor history reports now include trendlines, auto-refresh, a summary view, and state sensor graphing.

- **Feature announcements**
  See announcements about new features directly in the web client. New announcements are shown the first time you log in. Click the megaphone icon in the upper right to view announcements again.

- **Dark mode**
  The user preferences page in the web client includes an **Appearance** option to choose light or dark mode.

- **Inactivity timeout message**
  The session inactivity timeout message in the web client is dismissed after login as expected.

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

Server operating system

Server OS: Proprietary Rocky Linux 8.10 (RHEL derivative)

Java Version: OpenJDK-headless-17.0.18.0.8-1.el8

Windows desktop client

Java version: Adoptium 8u472-b08

Software vulnerabilities fixed in DCE 9.1.0

The security vulnerabilities addressed in this release include:

- CVE-2025-13957

This release includes various component updates to improve overall security.

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

Issues Fixed

The following issues were fixed in DCE 9.1.1:

- This release addresses an issue that caused historical numeric sensor data to be represented as zero during lost communication events.

  The data was stored correctly in the database, but was translated incorrectly when pulled from the system, for example via the API or reports.

The following issues were fixed in DCE 9.1.0:

- The **Restore from Backup** button in the **System** > **Server Administration Settings** > **Server Backup/Restore** option is now grayed out when a backup is running.
- Failed backups on high latency networks or networks with a high degree of packet loss no longer stay running and fail will gracefully.
- When a synchronized backup fails, the file now reverts to the last successful synchronized backup.
- The **System** > **Server Administration Settings** > **Network settings** option now accepts a .local domain.
- Guidance in the Surveillance view was improved to state that a subscription license is required to view clips.
- User roles update as expected after a change in permissions.
- Information is now logged by the server at shutdown as expected.
- All NetBotz 750/755 surveillance data is now fully purged when the device is deleted.
- Duplicate devices no longer appear in the Unassigned list after a reboot.
- Duplicate devices no longer appear in the device list after the MAC address of the VM is changed.
- Device Administrator users can now comment on alarms in the web client.
- The web client now displays progress as expected when restoring from backup.
- The web client now displays progress as expected during a server update.
- The web client now displays server starting progress messages on the login page as expected.
- The web client search display was improved.
- Event log messages for IT Advisor SOAP API failed login and DCE desktop client failed login were updated for clarity.
- The event log now includes entries for session timeout events.
- The web client now displays a *No data available* message when a saved report is run that contains no devices or sensors.
- Dashboards in the web client now load as expected and show a *No data to display* message when gadgets contain no devices or sensors.

Known Issues

- 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 DCE

Release notes for older versions of Data Center Expert

Upgrade Procedure

The following steps are necessary to upgrade Data Center Expert 9.1.0 to Data Center Expert 9.1.1.

The Data Center Expert 9.1.1 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 9.1.1. If you are downloading Data Center Expert 9.1.1, 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 9.1.0 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.**

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 9.1.1 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.

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_9.1.1.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_9.1.1.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	