EcoStruxure™ IT Data Center Expert 9.0.0 Release Notes

Table of Contents

Part Numbers Affected

- AP9465
- AP9470
- AP9475
- AP94VMTRL

Server hardware requirements have changed in this release.
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.

New Features

Licensing transition

As part of Schneider Electric's initiative to streamline software management across all EcoStruxure IT solutions, your active DCE licenses under support contracts will be upgraded to version 9.0.
This upgrade will transition your license management into mySchneider Software Management, which simplifies license handling and provides easier access to the latest software updates.

Important: To use this new version, your DCE licenses will be moved to a new licensing model once your current support contract ends. Please note that you will be required to accept new Terms of Use as part of the upgrade process.

Once you engage with our support team, a Customer Success Manager (CSM) will contact you within 7 days to help align your system and generate updated licenses.
After installation and until an updated license is applied, DCE 9.0 will operate in trial mode for 90 days. During that time, some features, such as server upgrades, device firmware updates, and surveillance clip retrieval, will be temporarily restricted. Surveillance clips will continue to be recorded.

This release contains improvements including:

- **Increased supported device node count**
  The maximum supported node count has increased to:
  - AP9465 - DCE Basic server, supports up to 540 nodes (525 nodes + 15 cameras)
  - AP9470 - DCE Standard server, supports up to 2150 nodes (2025 nodes + 125 cameras)
  - AP9475 - DCE Enterprise server, supports up to 4275 nodes (4025 nodes + 250 cameras)

- **Notification on login when attention is required**
  A notification is shown on login when:
  - An Administrator user does not have an email address associated with their DCE credentials. Administrators can provide an email address in **System** > **Users and Device Group Access**.
  - When the DCE server does not have email settings properly configured in **System** > **Server Administration Settings** > **Email Settings**.
  - When the DCE server license is a trial, to notify the user to obtain a license.
  - When the DCE server license has expired, to notify the user to obtain a license.
  - When the password for technical support access is not set.

- **Configurable client inactivity timeout**
  You can now control how long a user session will remain connected while there is no user-initiated activity in the **System** > **Server Administration Settings** > **Session Settings** option.
  This setting applies to both the desktop client and the web client. It is disabled by default. When enabled, the default setting is 5 minutes.
  Note: Allowing more than 30 minutes of inactivity is considered a security risk and is not recommended.

- **Improved desktop client startup performance**
  The desktop client takes less time to load when a large number of devices are monitored.

- **Default file transfer protocol**
  The default file transfer protocol was changed from FTP only to SCP, Fall back to FTP. You can change the file transfer protocol in **Device** > **SNMP Device Communication Settings** > **Device File Transfer Settings**.

- **Interval offset added in Global Scan Settings**
  In SNMP and Modbus **Device Communication Settings** > **Global Scan Settings**, the next device scan time is now based on the **Scan end time** plus the **Scan interval** by default.
  Data will be displayed in sensor history at intervals that equal the amount of time the scan takes plus the scan interval. This helps optimize network traffic, particularly when monitoring large numbers of devices.
  To display data at the configured interval, select **From scan start time**.

- **Improved device scan logging**
  Logging was added for device scan start, scan end, next scheduled scan, and scan paused to diagnose issues more efficiently.

- **Increased default timeout in Device Scan Settings**
  In SNMP and Modbus **Device Communication Settings** > **Device Scan Settings**, the default timeout settings were increased from 2 seconds to 10 seconds to reduce intermittent device communication issues.

- **Web client enhancements**
  - You can now view historical and active alarm data for all monitored devices on the **Devices** > **Alarm History** page.
    Search by description, device label, device hostname, or status; filter by alarm type, severity and timeframe; and toggle to show or hide resolved and hidden alarms.
  - Logs, desktop client download, status, and help pages were updated to align with the current page design.

- **Description added in Device Group information**
  There is now a **Description** field in the Create/Edit Device Group options.

- **Improved capture server logs**
  Capture server logs now include the routing table.

- **Set backup password**
  You can now set the password used to encrypt new backup files. Go to **System** > **Server Administration Settings** > **Server Backup/Restore** and click **Change Backup Password**.

- **File names for failed and successful backups**
  All backups in progress now have a *.tmp file name until complete. To distinguish failed and successful backup files, failed backups retain the *.tmp file name; successful backups end in *.dce.

- **Added endpoints in the REST API**
  A minimum value endpoint and a peak value endpoint were added to the REST API to support the Sensor Summary report.

- **Password required for server access by technical support**
  A password is now required for technical support to access the DCE server to assist with advanced troubleshooting. You must log in to the DCE server console using the *apcsetup* account to set the support password. You provide that password to the technical support agent if access to the server is required for troubleshooting.

- **Event log enhancements**
  The event log now includes:
  - Dashboard activity messages when users create, modify, or delete dashboards
  - Authentication server messages when users are added or removed
  - Improved web client access messages when users log in or out

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-17.0.15.0.6-2.el8

Windows desktop client

Java version: Adoptium 8u452-b09

Software vulnerabilities fixed in DCE 9.0.0

The security vulnerabilities addressed in this release include:

- CVE-2025-50125
- CVE-2025-50124
- CVE-2025-50123
- CVE-2025-50122
- CVE-2025-50121
- CVE-2025-6438

Schneider Electric Security Notification

The following third-party components were updated to address these specific cybersecurity vulnerabilities:

- CVE-2025-50302 - Linux Kernel
- CVE-2025-27363 - FreeType
- CVE-2024-53150, CVE-2024-53197 - USB audio
- CVE-2024-53104 - UVC Driver
- CVE-2024-8176 - libexpat

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 9.0.0:

- The capture logs now include all new events as expected.
- Documentation for **System** > **Server Administration Settings** > **Storage Settings** > **Purge Settings** was updated to accurately describe the percentage of total capacity that will cause the purge to end. Depending on how data is stored, the actual percentage may be below the configured value.
- The reset button on the User Preferences page now resets changes to the graph line style as expected.
- The URL in the *Report from* line in scheduled email exports is now https://…
- Test Export in the **Reports** > **Manage Export Scheduling** > **Export Action Configuration** wizard now validates the export settings as expected.
- DCE requires multiple binds to Active Directory or LDAP systems on login. This can now be reduced for individual users if the AD or LDAP instance utilizes *memberOf*. If the user is part of a group that is added to DCE, multiple binds are still required.
- DDF filename formats are now validated during import to prevent server issues caused by unsupported characters.
- Historical alarms and events are now included in automatic purge.
- When HTTP is enabled without enabling HSTS on the DCE server, a message advising the user to connect using HTTPS is now displayed.
  Note: If HTTP is not needed, you can modify HTTP and HTTPS settings in the desktop client on the **System** > **Server Administration Settings** > **Server Access** > **Web Server** tab.
- In French and Spanish locales, graphs are now displayed correctly in the web client when decimal values use commas.
- LDAP group members with Administrator privileges can now add or assign dashboards in the web client.
- The line graph gadget in the web client now handles permission changes correctly.

Known Issues

- The **Change server** and **Reboot** options do not relaunch the desktop client on Windows 11 and Windows Server 2025.
- Launch to device from the DCE desktop client may not work as expected. Some modern web UI frameworks are not supported by the internal desktop client browser.
- Launch to device to NMC3.devices with 3.2.x and 3.3.x firmware does not automatically log in the user.
- The web client does not show progress as expected when restoring from backup. A message is displayed, *Please wait while Data Center Expert initializes.* Do not reboot the server while the restore is in progress.
- If an AD/LDAP user provides a bad password and their system is configured to lock users out after X failed attempts, make sure that X is greater than 3 to account for 3 bind attempts by DCE. This prevents users from being locked out on a single bad attempt.
- The DCE 9.0 server cannot be updated to the next version while the server is in FIPS mode. Go to **System** > **Server Administration Settings** > **Server Access** > **Security Policy** and choose a policy other than FIPS before applying the update. **Note**: The server will reboot after you change the policy.

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 8.3.0 to Data Center Expert 9.0.0.

The Data Center Expert 9.0.0 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: You must have a valid software support contract to receive the Data Center Expert 9.0.0 upgrade.

Note 2: Data Center Expert must be at a minimum of version 8.3.0 to upgrade to Data Center Expert 9.0.0. If you are downloading Data Center Expert 9.0.0, you will need access to the Internet.

Note 3: 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 or contact Technical Support for assistance: http://www.apc.com/support/index.cfm.

   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 8.3.0 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: http://www.apc.com/support/index.cfm.
    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 9.0.0 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** 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_9.0.0.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_9.0.0.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	