

Table of Contents	Page #
Part Numbers Affected	1
Minimum System Requirements	1
New Features	1
Issues Fixed	3
Known Issues	4
Upgrade Procedure	6
Restoring InfraStruXure Central using ISO Format	7
Creating a bootable USB Key (Windows or Linux machine)	7

Part Numbers Affected

AP9465
AP9470
AP9475

Minimum System Requirements

The InfraStruXure Central console 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 Microsoft Windows 2003 Server (SP2), Microsoft Windows XP (SP1,SP2 or SP3), or Microsoft Vista, Red Hat Enterprise Linux version 5.0 or higher
- Java Runtime Environment (JRE) 1.6.0_11
- At least 512MB of RAM
- Screen resolution should be set to at least 1024 x 768.

New Features

InfraStruXure 5.1.1 New Features

The following features are new in InfraStruXure Central 5.1.1:

- **Operating System Upgrade**
The OS for the InfraStruXure Central server was upgraded from Fedora Core 5 to Fedora Core 9. This upgrade provided many security and performance improvements as well as any bug fixes implemented in subsequent versions.
- **Client Locale Selector**
The user interface now provides a language selector that allows the user to choose from a list of supported locales. The user interface will display text in the chosen language. By default, the user interface will display text matching the locale of the OS on the computer where the client is installed.

- **Localized Server Messages / Alerts and Device Alerts**

The user can now choose a locale for the server on the Server Administration Settings page. The InfraStruXure Central server provides localized text for the following languages:

- Brazilian Portuguese
- English
- French
- German
- Italian
- Japanese
- Korean
- Russian
- Simplified Chinese
- Spanish

- **Modbus TCP Output Module**

The InfraStruXure Central server has the ability to share data and alarms from any managed devices with a BMS system. Once the feature is enabled (with the corresponding license), the user can configure which devices (up to 247 slave devices) can be polled via Modbus TCP.

A user can also use InfraStruXure Central to configure custom register maps for each device and copy those register maps to other devices. The Modbus registers can contain device and threshold alarm information, including the severity of the alarm and the number of active alarms on the device.

- **Network Management System (NMS) Integration**

The NMS Integration feature allows users to quickly configure InfraStruXure Central to send SNMP v1 Traps and SNMP v3 Informs to an NMS. By default, Traps and Informs will be sent for each device alarm condition. Users can configure the server to only generate Traps or Informs for alarms above a chosen severity level.

- **APC SNMP Device Configuration**

The APC SNMP Device Configuration feature allows users to mass configure settings on any supported APC device. These settings can be saved as templates and used to set up future devices. The user has the option to choose all or some of the discovered devices and configure settings shared on the devices.

- **Web Services API**

The InfraStruXure Central server is equipped with a Web Services API which can be used to retrieve the following information:

- Active Alarms
- Alarm History
- Devices
- Device Groups
- Sensors
- Sensor History

Note: The Web Services API can only be used to read information from the server; users cannot edit settings or send data to the server through the API.

- **Microsoft Security Center Operations Manager 2007 Management Pack for InfraStruXure Central**

APC now provides a Management Pack for Operations Manager 2007. This Management Pack connects to InfraStruXure Central through the Web Services API, and provides the same information through the Operations Manager interface.

- **Sensor Summary Reports**

The Graphing and Reporting feature now includes a Summary Report option. Summary Reports provide a minimum, maximum, average, and current value for one or more chosen sensors over a specified date range. The algorithm used to generate the average value takes into account how long a sensor was at a given value over the specified date range.



- **Support for SCP File Transfer**
 InfraStruXure Central now allows secure SCP file transfers for customers with strict network security policies. This file transfer option applies to APC Firmware Updates and APC Device Configuration, as well as downloads of DDF files from APC 3.x devices during discovery.
- **Auto-Refresh Option for Graphs**
 An auto-refresh option was added for customers who need to generate a graph for real-time display. The graph can be refreshed automatically at intervals of 30 seconds, 1, 5, 10,15, 30, or 60 minutes.
- **Surveillance Thumbnail Configuration**
 Two additional display options were added for surveillance thumbnails. The user can now hide the thumbnail borders to increase the number of cameras that can be displayed on a page. In addition, the user can now select between two thumbnail display sizes: 160x120 pixels, or 320x240 pixels.
- **Improved User and Device Group Interface**
 The display dialogs for Users and Device Groups were redesigned to offer a more comprehensive view of users and user access. The new display uses a single dialog to show all relevant information regarding user access.
- **Advanced View Launch Option**
 The Advanced View user interface for NetBotz appliances can now be started from within the InfraStruXure Central user interface. This feature requires Advanced View 3.1.1 or later.
- **Improved Icons**
 Many icons in the ISXC user interface have been redesigned to provide a more intuitive experience while navigating the application.
- **Custom Audio Alerts**
 InfraStruXure Central now allows users to choose a custom audio file (of a supported format). This file will play if an active alert occurs on a managed device.
- **Highlighting Priority Alarms**
 Devices in error, critical, or failure states can now be highlighted in red in the Device View. This feature is disabled by default and can be accessed through the **Client Preferences > Device View Settings** dialog.
- **1 Node Base Surveillance License**
 InfraStruXure Central now ships with a 1 node base surveillance license pre-installed.

Issues Fixed

The following are InfraStruXure Central v5.0, 5.0.1, and 5.1 issues fixed in InfraStruXure Central v5.1.1:

- Remote backups configured in InfraStruXure Central v5.1.0 will be written to the local InfraStruXure Central server file system, if they fail to complete due to network or remote share issues.
- Internal InfraStruXure Central v5.1.0 backups are written daily to the local file system without rotation. These backups were not accessible to customers and have been disabled in InfraStruXure Central v5.1.1.
- Customers who upgraded from InfraStruXure Central v4.1.1, and had configured NetBotz Appliance Pod labels in that version, could experience errors in the InfraStruXure Central user interface due to incorrect string labels carried over from the v4.1.1 settings. These incorrect string labels are deleted upon upgrade to InfraStruXure Central v5.1.1.
- Historical Alarms are now sorted correctly by clicking the "Time Occurred" column header.
- Active Directory and LDAP users with the special characters (!@#%&*()_) in their username or password can now log into InfraStruXure Central successfully.
- Users can now restore a server using an external USB DVD drive.
- The InfraStruXure Central Private Proxy no longer allows network spoofing.
- Surveillance Posts no longer fail after using NetBotz Post Alert Data Settings to push a valid IP / Hostname to a NetBotz Appliance.
- An InfraStruXure Central Backup entry with an underscore(_) in the hostname can be restored properly.



- Blank Passwords can no longer be set to NetBotz Appliances from InfraStruXure Central.
- Users can now export graphs as images from the InfraStruXure Central Linux client.
- The InfraStruXure Central DHCP server now hands out IP addresses sequentially on the Private LAN.
- Users can now view camera movie clips in their entirety without having to resize the clip player dialog.
- Users can now multi-select and configure other state/other numeric thresholds of the same type.
- Exported Reports can now use either English or Metric units.
- Active Directory and LDAP Users/Groups added to InfraStruXure Central are now sorted alphabetically.
- Server backups can now be scheduled at the same time and complete successfully.

Known Issues

- **Limitations of Graphing Refresh Intervals**

A graph with a high amount of data points needs a certain amount of time to run before it can be successfully refreshed.

- If your graph has less than 50,000 data points, you can use any refresh interval
- If your graph has 50,000 or more data points, the graph will not refresh unless you set the refresh interval to 5 minutes or greater. (Higher intervals may be needed for higher data point totals.)
- If your graph has more than 200,000 data points, the graph will not refresh.

- **Help For Importing Firmware Updates Has Incorrect Procedure**

On the Help page for **Apply Firmware Updates**, the procedure for downloading the firmware updates is incorrect. The corrected procedure is:

1. Access the Software/Firmware download page (<http://apc.com/tools/download>).
2. In the **Filter by Hardware** list, select **InfraStruXure Central**, then select your Model Number and click **Submit**.
3. Choose the appropriate InfraStruXure Central Device Firmware Catalog File and click **Download**.

- **Loading Alert Threshold Configuration and NetBotz Appliance Configuration May Take a Long Time if Managing Many Devices**

If you are using InfraStruXure Central and are managing large numbers (1000's) of devices, it can take a significant amount of time to perform any activity requiring the selection and configuration of multiple data values. It is recommended that you configure your devices in small groups, less than 100 devices at a time, and use the provided filter capabilities to reduce the total time it will take to select and configure your devices.

- **Toggling the Private Side Network Ranges with APC NMC Devices**

If you have APC NMC devices connected to your internal DHCP LAN and you change internal DHCP LAN network IP address range settings, you may (depending on the NMC network settings) need to reset each NMC in order for them to obtain a new, valid IP address.

- If the APC NMCs are set to "BootP Only" or "BootP/DHCP" ("BootP/DHCP" is the default setting), you can use the Reset APC devices button to reset the NMC addresses, as long as the NMC is on the network and if private SNMP community names are properly set. Otherwise, you will have to manually reboot each NMC for the NMC to pick up a new valid private side IP address.
- If the APC NMCs are set to "DHCP Only", all NMC devices will properly reset to the new private network IP addresses.

- **Loading Large Clips that Contain Audio Data May Seem Slow, May Appear to Cause Console to Hang**

When opening a large clip with audio, the Clip Player might take a few minutes to load. If the Clip Player is closed before the loading is complete, the InfraStruXure Central console appears to hang or freeze. However, after 15-20 seconds the console should become responsive again.



- **Loading Large, Remotely Stored Clips that Contain Audio Can take Several Minutes**
Large clips with audio can take several minutes to load if the clips are currently stored on the management device instead of on the InfraStruXure Central server

- **SSL Certification Requests: Certificate Signing Request Generation Tips**
Certificate signing and authentication services are strict about the format in which CSR data is submitted. Here are some guidelines you should follow when using the Server Security task to generate a CSR:
 - Common Name: Use the fully qualified hostname of your server
 - Organization: Use your company name (such as “American Power Conversion.”). (Note: do not use commas.)
 - Organizational Unit: Use your department name (such as “Engineering”)
 - Locality: Use the name of your city, town, village, hamlet, etc. (such as “West Kingston”)
 - State: Your state name. Use the full name of the state, not an abbreviation (for example “Rhode Island,” not “RI”)
 - Country: Your country
 - E-Mail: A standard e-mail address

- **LDAP Users In an LDAP Group Will Not Receive E-mails When a NetBotz Appliance Goes Offline**
LDAP users must be explicitly added to the InfraStruXure Central user list in order for e-mail notifications to work successfully.

- **ISXC Private Proxy of Web Launch for Java-based Interfaces Will Not Allow Them to Launch from the Private to Public Side**
The “Launch to Device” functionality is limited to web-based interfaces if the InfraStruXure Central client and the target device reside on different InfraStruXure Central server LANs. Devices with a native Java user interface or command line interface, such as APC’s Console Port Server or IP KVM, will need to reside on the same LAN as the requesting console (Private or Public) for the “Launch to Device” to be successful.

- **Nothing to Indicate Idle Motion in Surveillance Clips**
There is no visual clue except for an optional time stamp. The motion idle time is set to 10 seconds on the server.

- **When Multiple Servers Are Added to the Same Remote Repository, each Server Overwrites the repository.id file**
Make sure each InfraStruXure Central server uses its own remote repository. If you assign an InfraStruXure Central server to use a remote repository that is already used by another InfraStruXure Central server, the repository.id file is overwritten, and may cause unexpected behavior for the original InfraStruXure Central server.

- **Schedule Updates Check Does Not Check for NetBotz Appliance Updates**
This feature only checks the APC website for Firmware Updates for managed devices enabled with an APC Network Management Card. To check for available Firmware Updates for the NetBotz Appliance, do the following:
 1. Select “Apply Firmware Updates” in the Updates menu.
 2. Select the “NetBotz Appliance Update” radio button.
 3. Click “Check Updates” button (available updates will be displayed in the Update section).

- **Maximum SNMP device Scanning Settings Cause Performance Degradation**
It is recommended that the default 5-minute scanning rate be used for SNMP devices, and only adjusted for small subsets of critical devices.

- **The InfraStruXure Central Server Cannot Use Priority Scanning with 3rd-Party Devices**
The trap registration option available during SNMP device discoveries can be used for APC devices only.

- **An Attempt to Add a Remote User with the Same Name as a Local User Does Not Result in an Error Message**

Username must be unique on the InfraStruXure Central server. If you attempt to add an Active Directory or LDAP user to your InfraStruXure Central server, and a local user exists with the same username, the Active Directory/LDAP user will not be added and you will not be notified.

Upgrade Procedure

The following steps are necessary to upgrade InfraStruXure Central 5.0, 5.0.1, or 5.1 to version 5.1.1.

Note 1: The customer must have a valid software support contract in order to receive the 5.1 upgrade. If the customer does not, then they will need to purchase one in order to receive the upgrade.

Note 2: InfraStruXure Central must be at a minimum of version 5.0 in order to upgrade to version 5.1.1. If you are downloading version 5.1.1 you will need access to the Internet. APC recommends backing up the InfraStruXure Central Configuration file by going to Settings>>Server Administration Settings >>Server Backup/Restore, create a backup entry and then hit Start.

Warning: Before beginning an upgrade, remember to run a full backup on your InfraStruXure Central system.

1. Download the upgrade.zip file, or contact InfraStruXure Central Technical Support at 877-908-2688 for assistance.

Note: The restore.iso file may be needed for later use if a re-installation is required. See Restoring InfraStruXure Central using ISO Format on page 11 for instructions for restoring your data from a restore.iso file from the ISO format.

2. Extract/expand the upgrade zip file into a separate directory on the hard drive of the system that will be running the InfraStruXure Central Console.
3. Login to your InfraStruXure Central 5.0, 5.0.1, or 5.1 server with full administrative access. Now select **Updates** from the menu bar then **Apply Server Update**.
4. Click on **Import** and look into the subdirectory where extracted files are placed. The structure of the extracted fields should contain two folders, "BW" and "NBCCore", and an index file, "nbcpkg.lst".
5. Select the "nbcpkg.lst" file and click "Open".
6. The Upgrade/New Packages table will update indicating that there is an update available for the InfraStruXure Central appliance. Check the "Install/Upgrade" option for the package(s) you wish to upgrade. Click the **Install Selected** button to start the upgrade for the selected package(s). You will be prompted to confirm if you would like to proceed with the upgrade. Click **Install Update** to start the upgrade process.

Warning: The upgrade procedure may take as long as 45 minutes. Do not manually reboot the server during the upgrade process.

7. When the file transfer completes, InfraStruXure Central will restart and disconnect your console connection. You may point a web browser to the InfraStruXure Central server for status.
8. When the update is complete, reconnect the InfraStruXure Central Console to the server and you will be prompted to upgrade. Follow the directions and install the new client.
9. Start the new InfraStruXure Central client, and the upgrade is complete.

Restoring InfraStruXure Central using ISO Format

Warning: Only perform the steps in this section if directed to do so by an APC Support technician.

Before You Restore: A system restore will wipe away all data, and restore the InfraStruXure Central 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, or contact InfraStruXure Central Technical Support at 877-908-2688 for assistance, used to create a bootable DVD or USB flash key.
 - a. For creating a DVD, use the instructions for your DVD Writer/Burner software to create a DVD from an ISO image.
 - b. For a USB Flash Key, follow the instructions provided in Creating a bootable USB Key (Windows or Linux machine) on page 12.
2. Place the InfraStruXure Central Recovery DVD in the DVD-ROM drive, or the USB flash key in the USB port of your InfraStruXure Central appliance.
3. Reboot InfraStruXure Central. Since this is a restore, you may cycle power switch to InfraStruXure Central to start restore process.
4. When the appliance restarts the system restore process begins automatically. This process takes approximately 10 minutes for the 1U InfraStruXure Central Basic, 15 minutes for 1U InfraStruXure Central Standard or 25 minutes for 2U InfraStruXure Central Enterprise. When the restore is complete, if you are restoring via a DVD, the system will eject the Restore DVD automatically and restart itself. If you are restoring via a USB flash key, you will be prompted to remove the USB flash key and hit enter to reboot the server.
5. Once InfraStruXure Central has restarted, you may configure the InfraStruXure Central network settings per instructions in the InfraStruXure Central Installation Guide.

Creating a bootable USB Key (Windows or Linux machine)

Instructions for a Windows machine:

1. Insert a 1GB (or larger) USB key into your system.
2. Extract the following file to a temporary directory:
`ApclsxCentralUsbFlashRestore_Win_5.1.1.zip`
3. Open a command prompt to the temporary directory and run `mklsxCentralRestoreUsbKey.bat <iso image filename>`.
For example: `mklsxCentralRestoreUsbKey.bat c:\tmp\restore.iso`
4. Answer the prompts as appropriate.

Instructions for a Linux machine:

1. Insert a 1GB (or larger) USB key into your system.
2. Extract the following file to a temporary directory:
`ApclsxCentralUsbFlashRestore_Linux_5.1.1.tar.gz`
3. Open a command prompt to the temporary directory and run `mklsxCentralRestoreUsbKey.sh <iso image filename>`.
For example: `mklsxCentralRestoreUsbKey.sh /tmp/restore.iso`
4. Answer the prompts as appropriate.

Third-party USB flash key scripts:

The USB flash 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 application downloaded from http://student.northpark.edu/pemente/sed/	X	

