InfraStruxure® Central 6.0.1 Release Notes

Table of Contents

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), Windows Vista, or Windows 7, Red Hat® Enterprise Linux® version 5.0 or higher
- At least 1 GB of RAM
- Screen resolution should be set to at least 1024 x 768.
- Supported browsers: Microsoft Internet Explorer® 8, Mozilla® Firefox® 3.5.x

New Features

InfraStruxure Central 6.0 New Features

The following features are available in the 6.0.0 release of InfraStruxure Central:

- **Improved Icons**
  Many icons in the ISXC user interface have been redesigned to provide a more intuitive experience while navigating the application.

- **Updated Menu Options**
  Redesigned the contents of the menu bar for additional clarity and functionality.

- **Modbus TCP Device Support**
  InfraStruxure Central can now discover and monitor devices that use the Modbus TCP protocol and Modbus RTU devices that are connected to a Modbus RTU to Modbus TCP gateway.

- **New Perspectives**
  InfraStruxure Central now provides three new perspectives to help manage your devices:
  Alarm Configuration – Modbus and SNMP device alarm configuration is now handled in the Alarm Configuration perspective. Users can create thresholds, notification policies, and alarm actions. NetBotz devices are handled in the same manner as previous releases.

  Summary Reports – Five pre-defined reports are available in the Summary Reports perspective. By default, two views appear in the Summary Reports perspective. These views allow you to generate, view, print, and export reports in HTML, CSV (comma-delimited), or PDF format for the device groups selected.
    - **All Reports View**: lists the Available Reports for the devices the InfraStruxure Central server monitors, and allows you to generate those reports for selected device groups.
    - **Report View**: displays the reports generated for the device groups selected, and allows you to print and export those reports.

  Power Management – InfraStruxure now supports the PowerLogic™ ION Enterprise™ server. When the ION Enterprise integration is enabled through the InfraStruxure Central user interface, and the client is rebooted, the Power Management perspective will be enabled. This allows users to access the ION Enterprise view.

- **Custom Property Support**
  Users can now create custom properties that can appear as columns in the Monitoring perspective views and the Device Sensors display. Custom properties are created in a new view, the Custom Properties Editor.

- **Maintenance Mode**
  InfraStruxure Central now has a way to disable notifications for a device or device group. Enabling "Maintenance Mode" for a device or device group will disable any notifications from those devices until the mode is disabled again.

- **Trend Lines in Graphs and Reports**
  Graphs and reports in InfraStruxure Central now have the option to show trend lines, which track the moving average value of the chart data.

- **Device Launch with Automatic Log In**
  You can provide credentials to automatically log in to the web interfaces of APC SNMP devices with the following Network Management Card and firmware revisions:
    - rPDU with Network Management Card firmware revision 3.7.1 and higher.
    - APC SNMP devices with a Network Management Card (AP9617, AP9618, or AP9619) with firmware revision 3.7.0 and higher.
    - APC SNMP devices with a Network Management Card (AP9630, AP9631, AP9635) with firmware revision 5.1.0 and higher.

- **Support for Static IPs on the Private LAN**
  InfraStruxure Central now supports two private LAN sectors (Network A and Network B) that can be used to separate devices that use DHCP address assignment and static IPs. Devices which require static IPs can be added to the Network B LAN. When devices are reset on the DHCP Discovery tab, the IPs of devices on Network B will not be reset.

- **InfraStruxure Central Server Can Now Be Used As Standalone NTP Server**
  Users can now set the InfraStruxure Central Server as an NTP server without syncing with an external NTP server.

- **New Communication Link Status Threshold**
  Users can configure a new threshold – "Communication Link Status" – for SNMP and Modbus devices in the Alarm Configuration perspective. This threshold is triggered when communication is lost with the device, and replaces the off-line alarm configuration capability in previous releases.

Issues Fixed

The following are InfraStruxure issues fixed in InfraStruxure Central v 6.0.1:

- Enterprise servers no longer log Fedora information by default (restores prior behavior).
- Map view backgrounds and icon positions are displayed correctly after upgrading from 5.1.
- Map view icons are displayed correctly when a device is added or removed from the map.

The following are InfraStruxure issues fixed in InfraStruxure Central v 6.0.0:

- The Schedule Updates Check now checks for NetBotz Appliance updates
- SSH settings are now carried over when restoring from a backup.
- Remove button now works properly in Server Proxy Settings when removing multiple entries in succession from the "Do not use proxy server for the following addresses" list.
- When new sensors are added to a device, they will now automatically show up in the "Device Sensors" window without having to reopen the window.
- Users can now map device sensor values to multiple Modbus registers for sensor values that are too large to fit in a single 16-bit register.
- SNMPv3 discoveries of private side devices using ranges or wildcards now discover all devices.
- If the user had a saved report with more than 1026 datapoints in InfraStruxure Central 4.1.1, the report would not be saved after editing it in the "Edit Report Scheduling" dialog, but the user was never prompted to reduce the data points. The user is now prompted that they must reduce the number of data points before they can save the changes to the report.
- Selecting multiple devices and making changes in the "Device Launch Settings" dialog will now apply the changes to all selected devices.
- Performing a test of the Server Proxy Settings will now notify the user if the Username and Password are invalid.
- Exporting a Modbus Register Map for a device configured in the Building Management Settings window will now include the plaintext sensor name.
- The user is now able to access to devices on the private network via the Private Proxy when DHCP is disabled on the private network.
- When HTTP access on the server is disabled, and HTTPS access is enabled, the user is now able to web launch to devices on the private network that are configured to use HTTPS.
- E-mails containing double-byte characters in the subject line are now encoded correctly.
- In certain situations, a sudden loss of utility power the server could cause corruption of the server's filesystem. In these situations, the integrity of the filesystem is now preserved.
- Running a firmware update for devices without correct credentials stored in the "Device File Transfer Settings" dialog no longer causes the firmware update to hang at "Transferring AOS Settings".
- Restoring a server backup will now restore the server's Private LAN IP Address.
- In some situations, backing up a server with large amounts of data would fail. These backups will now succeed.
- Scheduled reports now correctly obey the server's 24-hour mode setting
- Restoring a server backup when the network share user's password contains special characters will now successfully complete.
- The "Label" field in the Surveillance perspective now uses the Netbotz "Camera Label" instead of the "Pod Label" to support internal device cameras without Pod Labels.

Known Issues

- **Devices Will Not Be Discovered If Timeout is Longer Than 60 Seconds**
  If the timeout and retry settings for SNMP device discovery result in a time of more than 60 seconds, the discovery process will fail. The formula for figuring out whether your discovery settings are above sixty seconds is: ([Retries] + 1) * [Timeout]. If the total exceeds 60 seconds, the InfraStruxure Central server will fail to discover devices, even if the timeout and retry values are reduced.

  The discovery entry must be deleted and a new one created in order for the devices to be discovered.

- **Limitation on Global Device Scan Intervals**
  Users cannot set their global device scan settings to less than five minutes if there are more than 2026 devices discovered on their InfraStruxure Central Enterprise server. This restriction is not enforced on device-specific scan settings, but APC recommends that the same policy be applied to these settings.

  For servers monitoring fewer than 2025 devices, it is recommended that the default 5-minute scanning rate be used for SNMP devices, and only adjusted for small subsets of critical devices.

- **Threshold-specific E-Mail Addresses Not Supported**
  InfraStruxure Central now uses Notification Policies to control which e-mail addresses are notified when a threshold is violated. E-mail addresses assigned to sensor thresholds in earlier versions of the product are no longer supported, and that information is not kept during the upgrade procedure. Existing Alert Profiles are automatically assigned to a Notification Policy – only the e-mail addresses entered directly in a threshold are affected by the change.

- **Contextual Help Does Not Display in Report View After Report Generated (Linux)**
  After a report is generated in Report View, the contextual help system will not display. If all generated reports are closed, or no report is open, the help will display properly. If the help system is opened before a report is generated, the correct help page is shown.

- **Modbus Sensors With Non-Standard Units Appear in "Other Numeric Sensors" Grouping**
  When adding thresholds to sensors on Modbus devices, sensors that do not use our default units of measurement are grouped under the "Other Numeric Sensors" heading, rather than the appropriate headings for the type of sensor.

- **Server E-Mails are Sent to All InfraStruxure Users**
  When a NetBotz appliance goes offline, all users are sent a notification e-mail.

- **RMS Access Relies on DNS Information**
  In order to connect to the Remote Monitoring Service (RMS), the InfraStruxure server must have its DNS settings configured correctly.

- **Device Launch with Automatic Login Does Not Work with AP9606 Web/SNMP Cards.**
  You can provide credentials to automatically log in to the web interfaces of APC SNMP devices with the following Network Management Card and firmware revisions:
  - rPDU with Network Management Card firmware revision 3.7.1 and higher.
  - APC SNMP devices with a Network Management Card (AP9617, AP9618, or AP9619) with firmware revision 3.7.0 and higher.
  - APC SNMP devices with a Network Management Card (AP9630, AP9631, AP9635) with firmware revision 5.1.0 and higher.

  Note: You cannot automatically log in to the web interface of any APC SNMP device monitored by a NetBotz Appliance.

- **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**.

- **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 serve

- **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.

- **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.

- **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**
  Usernames 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 5.1 or 5.1.1 to version 6.0.0.

Note 1: You must have a valid software support contract in order to receive the 6.0 upgrade. If you do not, then you will need to purchase one in order to receive the upgrade.

Note 2: InfraStruxure Central must be at a minimum of version 5.1 in order to upgrade to version 6.0. If you are downloading version 6.0 you will need access to the Internet.

Warning: Before beginning an upgrade, remember to run a full backup on your InfraStruxure Central by going to Settings>>Server Administration Settings >>Server Backup/Restore, create a backup entry and then hit Start.

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 7 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 5.1 or later 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 between 15 and 45 minutes depending on the amount of sensor data and events that are stored on the server. 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 7.
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 2GB (or larger) USB key into your system.
2. Extract the following file to a temporary directory:
   ApcIsxCentralUsbFlashRestore_Win_6.0.0.zip
3. Open a command prompt to the temporary directory and run mkIsxCentralRestoreUsbKey.bat <iso image filename>. For example: mkIsxCentralRestoreUsbKey.bat c:\tmp\restore.iso
4. Answer the prompts as appropriate.

Instructions for a Linux machine:

1. Insert a 2GB (or larger) USB key into your system.
2. Extract the following file to a temporary directory:
   ApcIsxCentralUsbFlashRestore_Linux_6.0.0.tar.gz
3. Open a command prompt to the temporary directory and run mkIsxCentralRestoreUsbKey.sh <iso image filename>. For example: mkIsxCentralRestoreUsbKey.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	X	