InfraStruxure® Central 6.2 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 6.2 New Features

The following features are available in the 6.2.0 release of InfraStruxure Central:

- **InfraStruxure Manager Migration Utility**
  InfraStruxure Central v6.2 provides a utility used to migrate settings and other important data from an InfraStruxure Manager v4.7 to an InfraStruxure Central v6.2 server. When migration is complete, the InfraStruxure Central server will manage devices previously managed by the InfraStruxure Manager.

  Migration of a fully configured InfraStruxure Manager, monitoring the maximum number of nodes, can take over twenty-four hours to complete when the InfraStruxure Manager data log is included in the migration. When the data log is not included, migration can take up to one hour. When a migration that includes devices on the private LAN is complete, the InfraStruxure Manager will be turned off.

Rev 2/16/2011

- **Enhanced Alarm Configuration**
  Users can now modify device alarm configurations, changing the default values to better comply with their IT management policies.

- **New Reports perspective**
  Predefined summary reports and user-customized sensor history reports are now in one Reports perspective. Users can now create graph-format, summary-format, or table-format custom sensor history reports, modify the report criteria, and export or save these reports. Additionally, users can generate pre-defined graph-format snapshot reports for the devices or device groups the InfraStruxure Central server monitors, and export them as HTML, CSV (comma delimited), or PDF.

- **Trending and Analytics**
  Users can now include a trend line on a graph-format report to predict future sensor values based on past data sets when all numeric sensors included in the report use the same unit of measure.
  The trend is calculated using a linear regression model and the ordinary least squares estimation method. All the available data returned by the InfraStruxure Central server for the sensors selected, and the time range specified for the report, are considered in the model. The data are extended for twice the specified time range to create the trend line.

- **Client Preferences**
  Users can now open a browser in a view inside the InfraStruxure Central client to automatically logon to the user interface of devices that use basic authentication.

- **License Keys**
  Users can now view information about installed license keys and copy it to a document.

- **Open LDAP Authentication**
  The InfraStruxure Central server now requires OpenLDAP for secure communication with a Linux authentication server.

- **Server SSL Certificates**
  The user can now import SSL certificates used for secure communication with an SMTP server, Active Directory or OpenLDAP server, or a NetBotz Appliance. The STARTTLS extension is required to communicate with SMTP servers using the Secure SMTP protocol.

- **Storage Settings Purge Option**
  Users can now manually purge alarm history data.

- **Rack Access Configuration**
  Users can now configure Rack Access Users settings in the APC SNMP Device Configuration wizard “Configure Device Settings” display.

- **Surveillance Settings**
  Users can now access configuration options in a right-click menu in the Camera view.

- **Macros**
  Additional alarm action macros are now available.
  Identification macros:
  ${SERVERIP}: The dotted-decimal IP address of the InfraStruxure Central server.
  ${SERVERHOSTNAME}: The hostname of the InfraStruxure Central server.
  ${SERVERMODEL}: The model of the InfraStruxure Central server.
  Alarm macros:
  ${ALERTTYPENAME}: The ${ALERTTYPE} value, displayed in the language appropriate for the InfraStruxure Central server locale.
  ${ALERTSEVNAME}: The ${ALERTSEV} value, displayed in the language appropriate for the InfraStruxure Central server locale.
  ${DEVICELABEL}: The label of value of the device that either contains the sensor that reported the alarm or to which the sensor is connected.

InfraStruxure Central 6.1 New Features

The InfraStruxure Central v6.1 release supports new features in InfraStruxure Operations v6.1 only. There are no new features available in InfraStruxure Central v6.1. APC recommends updating to InfraStruxure Central v6.1 to support InfraStruxure Operations v6.1 only.

InfraStruxure Central 6.0.2 New Features

The following features are available in the 6.0.2 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 v6.2.0:

- Total power is reported for Symmetra PX devices.
- Per-phase output power VA is reported for MGE UPS devices.
- IP address fields in the APC SNMP Device Configuration wizard now accept hostnames.
- A column in the Device View now displays the MAC address of monitored devices.
- Piller UPS devices are now a UPS device type.
- Chloride UPS devices now a UPS device type.
- Notifications for Modbus device threshold alarms contain the IP address of the Modbus gateway.
- Web Services reports the correct sensor types for environmental sensors on the Network Management Card.
- The Device Sensor Report sensor table correctly sorts numerical values containing commas.
- The Current Reading for NetBotz Appliance thresholds now displays the latest sensor value.
- When both primary and secondary SMTP servers are specified on the InfraStruxure Central server, only one InfraStruxure Operations email notification is now sent.

The InfraStruxure Central v6.1 release supports issues fixed in the new InfraStruxure Operations v6.1 release only. No InfraStruxure Central issues were addressed in InfraStruxure Central v6.1.

The following are InfraStruxure issues fixed in InfraStruxure Central v6.0.2:

- Devices in the All Devices group now stay visible in Map View when a device state change occurs.
- The Device Label now updates after a device's SNMP Scan Settings are changed.
- Average sensor values for a specified date range are calculated correctly in Sensor Reports.
- The most recently recorded sensor values for a specified date range now appear in Sensor Reports when the start date is in a year prior to the end date.
- Enterprise server RAID utility logging is now more efficient.
- Help for importing firmware updates has correct procedure.

The following are InfraStruxure issues fixed in InfraStruxure Central v6.0.1:

- 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 v6.0.0:

- 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

- **Limitation in Windows Operating System for Large Images Used as Custom Backgrounds**
  Bitmap images used for custom backgrounds in Map View cannot exceed 48MB when the InfraStruxure Central client is installed on a Windows operating system.

- **Limitation on Private LAN (LAN2)**
  The InfraStruxure Central server is not a multihomed server. The private LAN (LAN2) is a private network used to communicate with devices monitored by the InfraStruxure Central server only. Integration with other network configurations, such as routing to a public LAN or redundant links, is not supported.

- **Alarm Sensor Values are Displayed in the Locale Specified on the InfraStruxure Central Server**
  In the InfraStruxure Central client, sensor values for alarms are displayed in the format of the InfraStruxure Central server locale, not the format of the locale specified in the InfraStruxure Central client.

- **Units in Graphs Included in Alarm Notifications are Displayed in English**
  When an email, HTTP POST, or FTP alarm notification includes a graph, the units are displayed in English. The body of the email and the sensor data are displayed in the language for the locale specified in the alarm action.

- **Limitations on Requests for Data Using Web Services**
  Data requests via Web Services exceeding 3.5MB return no data.

- **Web Services Sends Two Clearing Events**
  When an alarm clears on the InfraStruxure Central server, two clearing events are sent via Web Services.

- **Web Services v2_0 API Incorrectly Reports Sensor Status as Unplugged**
  The getMultiplePeakSensorData method can report a sensor value as Unplugged if no sensor value change has been recorded between the start time and end time parameters of the query.

- **InfraStruxure Central Server Reboots While Using the InfraStruxure Manager Migration Utility**
  The InfraStruxure Central server will reboot while migrating settings and data from InfraStruxure Manager v4.7 to the InfraStruxure Central v6.2 server when the InfraStruxure Manager data log is included in the migration, or the time settings on the InfraStruxure Central server change because of the migration.

- **Priority Scanning is Disabled on Some Devices After Using the InfraStruxure Manager Migration Utility**
  When the InfraStruxure Manager Migration Utility is used to migrate settings and data from InfraStruxure Manager v4.7 to the InfraStruxure Central v6.2 server, priority scanning settings can be disabled on devices managed with the APC Web/SNMP Management card (AP9606). Users can manually enable priority scanning in the InfraStruxure Central client after the migration is completed.

- **The APC IP Gateway for Analog KVM (AP5456) is Not Migrated from InfraStruxure Manager**
  The InfraStruxure Central server does not support the APC IP Gateway for Analog KVM (AP5456).
  When the InfraStruxure Manager Migration Utility is used to migrate settings and data from InfraStruxure Manager v4.7 to the InfraStruxure Central v6.2 server, the APC IP Gateway for Analog KVM (AP5456) is not migrated.

- **Devices Briefly Appear in the Unassigned Group After Migrating from InfraStruxure Manager**
  After the InfraStruxure Manager Migration Utility is used to migrate settings and data from InfraStruxure Manager v4.7 to the InfraStruxure Central v6.2 server, the Device Groups view in the InfraStruxure Central Monitoring perspective might briefly display some migrated devices in both the device group to which they are assigned and the Unassigned group. The Device Groups view updates to display the devices in the correct groups within a few minutes.

- **Product Upgrade Can Take Up to Twelve Hours When Certain Rack PDU Devices are Monitored**
  A product upgrade to InfraStruxure Central 6.2.0 can take up to 12 hours when monitored Dell PDU versions DELL66xx or DELL68xx, or APC rack PDU versions AP86xx, AP88xx, or AP89xx have extensive sensor history.

- **Threshold Descriptions are Truncated After Product Upgrade**
  Custom descriptions for alarm thresholds are limited to 256 characters on the InfraStruxure Central v6.2 server. After a product upgrade to InfraStruxure Central 6.2.0, descriptions longer than 256 characters are truncated.

- **Device Launch with Automatic Login Requires Internal Browser for Some APC SNMP Devices**
  You can provide credentials to automatically log in to the web interfaces of APC SNMP devices. You must select **Use the Internal Web Browser when Launching to Devices** in the **Client Preferences** option to automatically login to the web interface of devices that use basic authentication.
  Note: You cannot automatically login to the web interfaces of APC SNMP devices monitored by NetBotz Appliance versions 320, 420, and 500.

- **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.

- **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.

- **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 6.x to 6.2.0.

Note 1: You must have a valid software support contract in order to receive the 6.2.0 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 6.0.0 in order to upgrade to version 6.2.0. If you are downloading version 6.2.0 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 6.0 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.

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_6.2.0.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_6.2.0.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	