

Table of Contents	Page#
Part Numbers Affected .....	1
Minimum System Requirements .....	1
New Features .....	1
Issues Fixed .....	2
Known Issues .....	3
Upgrade Procedure .....	10
Restoring InfraStruXure Central using ISO Format .....	11
Creating a bootable USB Key (Windows or Linux machine) .....	12

## Part Numbers Affected

<b>AP9465</b>
<b>AP9470</b>
<b>AP9475</b>

## 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 2000 SP6, Microsoft Windows XP (SP1,SP2 or SP3), or Microsoft Vista, Red Hat Enterprise Linux v4.0 or higher
- Java Runtime Environment (JRE) 1.5.0\_06
- At least 512MB of RAM
- Screen resolution should be set to at least 1024 x 768.

## New Features

InfraStruXure Central 5.0.0 has the following new features:

- Improved Usability
  - New user interface to match Change and Capacity Manager
  - Cohesive look and feel
  - Superior usability over current user interface
- Scalability
  - Increased maximum node count (currently 1025)
  - Standard Up to 2025
  - Enterprise Up to 4025
- New Functions
  - Mass firmware updates of APC Network Management Cards
  - Remote Monitoring Service Support
  - Vastly improved alerting (speed and configuration)

- New, Low Cost, Entry InfraStruXure Central platform
  - ISX Central Basic – matches ISX Manager entry price point
  - All the same great ISX Central features
  - Up to 525 nodes
  - Optional Surveillance add on for 15 cameras
- Localized User Interface
  - Japanese
  - German
  - Russian
  - Simplified Chinese
  - Korean
  - French
  - Spanish
  - Italian
  - Portuguese (Brazil)

## Issues Fixed

The following are InfraStruXure Central v4.x issues fixed in InfraStruXure Central v5.0.0:

- When a monitored device, such as a camera, is set up with an older date than the server, the disk on the server no longer fills up, and the client is no longer unable to log on.
- An HTTP 404 error no longer occurs when generating a Certificate Signing Request (CSR).
- Changing the Server Locale in Time Settings to Portuguese (Brazil) no longer deletes the public and private network settings.
- Sensor data always written to the repository as expected now.
- APC devices no longer report receiving an IP address from BOOTP server 0.0.0.0 while on the InfraStruXure Central private LAN.
- A discovery process no longer adds NetBotz Appliances as SNMP nodes.
- Virtual NetBotz devices cannot be selected for pod sharing now.
- An upgrade now informs the customer how a long it can take to complete.
- An SNMP NMC device with DES encryption enabled for SNMPv3 support now propagates data to the InfraStruXure Central server.
- E-mailed graph data always reflects correct historical values of numeric alerts now.
- 100% CPU usage on client when viewing surveillance with Direct Connect for camera images enabled no longer an issue – InfraStruXure Central supports Direct Connect for audio only.
- The way the average is calculated in a Graph view has been updated to include start and stop times when averaging graph values.
- DHCP no longer gives invalid IP address (ending in .255).
- Removing a camera now causes surveillance thumbnail view to get updated.
- Console performance no longer becomes sluggish when connected using IP in SSL mode.
- When installing an InfraStruXure Central server, the License Agreement no longer takes up to 30 seconds to load.
- Having the InfraStruXure Central console open while upgrading the client no longer causes a corrupt installation.
- NetBotz surveillance: licensing an already-licensed appliance no longer switches the appliance to the new InfraStruXure Central without warning.
- Security/User Groups with Active Directory are now supported.
- Authenticated E-mail: spaces in passwords now supported
- External ports on unplugged pods no longer report that they are unplugged as well.
- Editing newly created e-mail Alert Actions on multiple NetBotz 500 series devices is no longer a problem.
- Generic SNMP device icons are still used for some APC devices, but this is no longer considered to be a notable issue.

The following are InfraStruXure Central v4.x issues that no longer exist because the UI redesign for InfraStruXure Central server v5.0.0 changed how the features are accessed and used:

- Mass Configuration of unplugged sensors no longer results in those sensors reporting invalid values.
- Removing Users from User Groups will no longer require deleting the user from the InfraStruXure Central server.
- Larger clips at 8x or 16x speed on slower console systems may play slow or may not show frame updates at real-time speeds.

## Known Issues

- **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.

- **Non-Metric Sensor Readings Can Cause Inconsistent Alert Triggering Behavior Due to Rounding**

All sensor reading values are processed and stored using metric units. If your device is configured to report sensor readings in non-metric units, readings are converted. In the process rounding occurs which can cause inconsistent alert triggering behavior in some cases. For example, if you are using non-metric units and you configure a temperature sensor to alert if a minimum threshold is exceeded, the alert will actually be triggered if the reported value exceeds or is equal to the specified minimum value. This is because even though the reported value is equal to the specified value, the actual converted value (prior to rounding) is slightly higher than the minimum value. Note that this issue occurs only with sensor types who report units that require conversion unconverted values will cause alert conditions to occur as expected. For example, voltage sensors do not require conversion, regardless of whether metric or English units are being used. Because no rounding occurs, these sensors will trigger alert conditions only when the reading exceeds the minimum value, not when it equals or exceeds the minimum value.

- **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.

- **Launching the Browser from InfraStruXure Central to Devices Connected to the APC Private (Internal DHCP) LAN**

In order to connect with Internal DHCP LAN-connected devices using the "Launch Browser" selection in InfraStruXure Central (available by right-clicking on a device in the Map or Table Views) you must ensure that the device is configured to communicate using the same HTTP (or HTTPS, if using SSL) port as the HTTP or HTTPS proxy on the InfraStruXure Central server. The HTTP and HTTPS ports are configured on the InfraStruXure Central server using the **Settings> Server Administration Settings> Server Access> Web Server** tab. The method used to configure the HTTP or HTTPS port on individual devices is device-dependant. Please refer to your device documentation for additional information.



- **An InfraStruXure Central Server Cannot Report that an Alert that Requires User Input Has Been Resolved on Devices in Post-only Mode Until the Post-only NetBotz Appliance Posts to the InfraStruXure Central server**

When configuring NetBotz appliances to generate alerts, you can configure each threshold to require a user to manually acknowledge that the alert condition no longer exists by checking the "Return to Normal Requires User Input" check box when configuring the threshold. This will cause the alert condition to continue until the user manually resolves the alert. However if a device is configured to operate in post-only mode, an InfraStruXure Central can resolve the alerts that require user input, but it cannot report that the alert has been resolved until the post-only NetBotz Appliance posts to the InfraStruXure Central server.

- **After Replacing an InfraStruXure Manager with an InfraStruXure Central, User's Can Get Flooded with NMC Traps**

InfraStruXure Manager, during auto-discovery and configuration of APC NMC devices, sets itself as a trap receiver for all SNMP devices. After replacing the InfraStruXure Manager with an InfraStruXure Central, if the InfraStruXure Central system is set to a different internal DHCP LAN address than was previously assigned to the InfraStruXure Manager device, the InfraStruXure Central can get flooded with SNMP traps begin forwarded from the NMC devices, and will forward those traps out to the public network. This will only happen if the InfraStruXure Central private network settings range doesn't include the old InfraStruXure Manager Private network IP address. To avoid this issue, you should disable the InfraStruXure Manager's trap forwarder before replacing the unit with the InfraStruXure Central.

- **Importing Data after Adding Appliances that Have Large Amount of Externally Stored Data Can take a Long Time**

When adding an appliance that uses External Storage, and that currently has a large amount of data stored externally, to InfraStruXure Central the data import process can take a long time to complete. InfraStruXure Central will automatically begin importing data stored externally by the appliance in 24-hour increments, starting with the most recently stored data and working backward until all data has been imported. As a result, depending on how much data is stored by the appliance externally, it may take a long time for all externally stored data to be available from the InfraStruXure Central server.

- **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.

- **MPEG Encoding of Clips that Cover Long Time Spans Can take a Very Long Time to Complete**

The amount of time it takes for an MPEG encode to complete is proportional to the total span of time that makes up the clip. The time span is total amount of time that occurs between the time stamp of the first frame in the clip and the time stamp of the last frame in the clip, regardless of whether there are gaps in the clip (i.e. portions of the time span that do not include picture data). For example, even if a clip contains only 4 frames of picture data, if the time covered by the clip spans two hours the MPEG encoder will take an enormous amount of time (as much as several hours) creating and including "empty" image frames for all of the "blank" time in the resulting MPEG file. Note that the AVI encoder does not work this way and AVI files will encode far more quickly.

- **Devices that Have Large Amounts of Sensor Data that Are in Post-only Mode Can Generate Alerts that Do Not Specify a Triggering Sensor Type**

If you add a device to InfraStruXure Central in Post Only mode that has a particularly large amount of sensor data (for example, a large number of images associated with alerts, a large number of Surveillance data, very extensive sensor histories on NetBotz 500's with Extended Storage Systems, and so forth) it is possible for InfraStruXure Central to begin retrieving alerts and other data from the device before all of the sensor history data can be gathered and entered into the database. If this occurs, it is possible for an alert to be received from the Post Only device before InfraStruXure Central knows everything about the various sensors that are actually connected to the device. If this happens, the alert would appear in the Alerts View with the value for "Sensor Type" left blank.

In addition, if InfraStruXure Central reaches the time-out value for retrieving sensor history before all of the sensor data has been retrieved from the device it will continue to try to retrieve the sensor history each time the device posts to InfraStruXure Central. If the timeout occurs again, this process will repeat again and again until the complete sensor data is retrieved, possibly compounding the "missing sensor type" problem because more and more time will pass, increasing the chances that alerts will be generated.

Please note that this issue isn't indicative of a problem with InfraStruXure Central's ability to handle large amounts of data. Rather, the problem is caused by two concurrent events:

- InfraStruXure Central needing to download a large amount of data that will enable it to properly identify and store data associated with an device's sensors and
- Alerts being posted by the same appliance, before data is posted, InfraStruXure Central needs to "understand" the alert data has been received and processed. The complete sensor history data download (event a, above) only occurs once. After the sensor history data has been downloaded and processed all future updates are far smaller, since only changes and new information are sent. Therefore, once the complete sensor history for the device has been successfully received by InfraStruXure Central for the first time you should not encounter any more alerts that contain blank sensor type values. If you encounter this problem, try the following steps to correct it:

1. Remove the InfraStruXure Central server from the Advanced View post-only settings dialog (Tools >> Advanced >> InfraStruXure Central POST-only mode).
2. Delete the Post Only device from InfraStruXure Central.
3. Use the Advanced View to access the device and reduce the amount of sensor history that is being stored for sensors. To do this, start the appropriate Configuration task (Sensor Pod, Camera Pods, Output Relay Pods, etc.), click Sensors, highlight a sensor in the top half of the panel and click Modify. Then reduce the Sensor Value History and click OK. This will cause older data to be deleted from the device, and should help InfraStruXure Central to successfully obtain the sensor history data.
4. Now use the Advanced View to restore the device to Post Only mode. Select Tools->Advanced->InfraStruXure Central Post-Only Mode.

**Note:** If you have a NetBotz 500 that has an Extended Storage System connected, and you are saving very large amounts of sensor data, you will almost certainly have to do this. The Extended Storage System can hold up to nearly 60GB of data. If an Extended Storage System is nearly filled to capacity, it could take as much as 48 hours for the initial sensor history data to be sent to InfraStruXure Central.

- **Camera Motion Settings on 320, 420 and 500 Series Appliances**

When configuring Camera Motion settings or Surveillance Motion settings for NetBotz Appliances, the settings are shared by both the Surveillance application and the Camera Motion Sensor. Therefore, if you adjust the Camera Motion settings (such as applying a Motion Mask, or adjusting sensitivity) it will affect the motion detection and Surveillance event triggering for that device in Surveillance. This applies only to 320, 420 and 500 Series appliances.

- **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
  
- **Surveillance Event Time/Date Stamps Do Not Match other InfraStruXure Central Event Time/Date Stamps**  
The time and date associated with Surveillance events is determined by the time/date settings on the NetBotz Appliance that generates the event, as opposed to other InfraStruXure Central events (which are determined by the time/date settings on the InfraStruXure Central appliance). To ensure that the time/date stamps on your Surveillance events are consistent with other InfraStruXure Central events, make sure your NetBotz Appliances are using NTP to synchronize their clocks.
  
- **NetBotz Appliance Upgrade Fails without Error Notification**  
Your InfraStruXure Central server must have proper authorization (Supervisor or Administrator access) in order for the appliance to perform upgrades on a NetBotz Appliance. If you attempt to upgrade a NetBotz Appliance for which you do not have adequate authorization, the appliance will not report an error and the upgrade will not occur.
  
- **Deleting a NetBotz 500 with Extended Storage from InfraStruXure Central Can Cause Database Server Log Errors**  
If you delete a NetBotz 500 with Extended Storage from the InfraStruXure Central server, that server can take as long as 3-4 hours to delete the large amount of data associated with the NetBotz 500.
  
- **LDAP Users that Are Part of 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.
  
- **User Interface Refresh Is Slow when Deleting Large Numbers of Devices**  
If you delete more than 500 devices at a time, it may take up to 10 minutes for the UI to refresh the device list in the Devices View. Closing and re-opening the InfraStruXure Central client will expedite this update.
  
- **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 side.
  
- **InfraStruXure Central will allow the creation of a network share with incorrect credentials if a user has already created share on the target server with valid credentials**  
For performance reasons, once a successful share has been mounted on a target server, InfraStruXure Central will create a session ID for the user and target server associated with the created share. For all other requests by the user to create a share on the target server, InfraStruXure Central will use the validated session ID instead of the entered credentials. This allows the user to type invalid credentials and still successfully mount the new share. If either the user or the target server is changed, the entered credentials will be validated.



- **When Upgrading to InfraStruXure Central v5.0 from v4.1.x, Surveillance Clips Tagged with the Same Text Will Show up as a Single Clip**  
 When searching for clips by tag or description after an upgrade to v5.0, groups of clips that have been tagged with the same text will show up as a single clip. If you search by range or relative time, the individual clips will be shown.
- **SELinux Configurations May Cause the InfraStruXure Central Client Startup to Fail**  
 To insure the successful loading of the InfraStruXure Central console on Linux systems running SELinux, configure SELinux as follows:

  1. Select system->Administration->SELinuxManagement
  2. Select "Boolean" from the left menu
  3. Expand the "Memory protection group"
  4. Check item labeled "Allow all unconfined executable to use libraries requiring text relocation..."
- **E-mail Test for NetBotz Appliances in Post Only Mode Always Reported as Successful Immediately**  
 The test e-mail takes place the next time the NetBotz appliance posts to the InfraStruXure Central server. After the post cycle occurs, you will need to validate that the e-mail was sent successfully.
- **Attempting to Restore a Backup File for a Post Only NetBotz Appliance Using an Invalid Password Fails without Notifying the User**  
 The restore will appear to succeed, but no restore actually occurs. Check your credentials, and try again.
- **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).
- **If the InfraStruXure Central Private LAN Address Is Changed, NetBotz Appliances Will Need to Be Deleted and Rediscovered**  
 The Post Alert Settings IP Address is not dynamically updated, so if the Private network settings change, any NetBotz Appliances on the Private LAN need to be deleted and re-discovered in order to update to a new address. (Note: any stored sensor data for a NetBotz Appliance will be deleted when the appliance is deleted from the InfraStruXure Central server.)
- **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 3<sup>rd</sup>-Party Devices**  
 The trap registration option available during SNMP device discoveries can be used for APC devices only.
- **If a Monitored Device Uses HTTP instead of HTTPS, Attempting to Use Secure Socket Layer (SSL) to Launch to that Device Can Result in the Password Sent as Clear Text**  
 When both HTTP and HTTPS are enabled for the InfraStruXure Central server's web-based communication using the **Settings> Server Administration Settings> Server Access> Web Server** tab, the InfraStruXure Central server will use HTTP for web communication, regardless of whether you want to use HTTPS, when that device is defined as using HTTP. To insure a secure connection when InfraStruXure Central server launches to the web

interface at a device, HTTPS must be selected for that device's web communication using its right-click "Device Launch Settings" option.

- **A Bind Failure Occurs when other than an SSL Certificate Signed by a Well-known Certificate Authority Is Used when Adding an Authentication Server**  
The bind failure is due to certificate validation failure because the certificate returned was unknown to the InfraStruXure Central server. To use SSL, the LDAP server must return a certificate signed by a well-known certificate authority.
- **When other than an SSL Certificate Signed by a Well-known Certificate Authority Is Used, an SMTP SSL connection will not work**  
The failure is because the certificate is unknown to the InfraStruXure Central server. SSL requires using a certificate signed by a well-known certificate authority.
- **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.
- **An Error Occurs when other than a Operating System Administrative User Attempts to Launch the InfraStruXure Central Client at a Client Machine**  
In order to run the InfraStruXure Central 5.0.0 client, you must have Operating System administrative rights on the client machine.
- **Trap Registration Option under Device Discovery Should Specify that it Can Be Used Only by APC Devices.**  
The InfraStruXure Central server can serve as a trap receiver for APC SNMP devices only.
- **Cannot Create or View Alert Thresholds for a NetBotz Sensor that is in a different device group than the parent NetBotz Appliance**  
In InfraStruXure Central server 5.0, NetBotz Appliance and its sensor pods can be separated into different device groups. In order for a user with device administrator on a device group that contains only NetBotz child devices to perform all functions available to them as device administrator, they must have at least device viewer privilege for the device group that contains the NetBotz Appliance parent device.
- **Capacity and Change Manager Roles Do Not Show Up in Users and User Groups after Restoring a Full Backup, and Users Cannot Log on to their Capacity and Change Manager Applications**  
After an InfraStruXure Central server that is licensed for Change and/or Capacity Manager is restored you must reboot that server.

## Upgrade Procedure

The following steps are necessary to upgrade InfraStruXure Central to version 5.0.0.

**Before You Upgrade:** InfraStruXure Central 5.0 does not include all the InfraStruXure Central 4.x features. Be sure to download and review the "Functional Delta between ISXC 4.0 and ISXC 5.0" document from the APC website prior to upgrading to InfraStruXure Central 5.0.0.: go to the [InfraStruXure Central Products page](http://www.apc.com/products/family/index.cfm?id=350) (<http://www.apc.com/products/family/index.cfm?id=350>) and click "User Manual & Installation Guides" to access a complete list of the available InfraStruXure Central documentation.

**Note 1:** The customer must have a valid software support contract in order to receive the 5.0.0 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 4.1, in order to upgrade to version 5.0.0. If you are downloading version 5.0.0 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.



1. Download the upgrade.zip file, or contact InfraStruXure Central Technical Support at 877-908-2688 for assistance.  
**Note:** A Recovery CD 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 creating a Recovery CD 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 4.1.x server with full administrative access. Now select "Tools" from the menu bar then "Server Administration" then "Install/Upgrade Management".
4. Click on "Browse to Files" 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 "Upgrade Server" to start 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

**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.

Start the new InfraStruXure Central Console and the update is complete.

1. Download the restore.iso file, or contact InfraStruXure Central Technical Support at 877-908-2688 for assistance, used to create a bootable CD or USB flash key.
  - a. For creating a CD, use the instructions for your CD Writer/Burner software to create a CD 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 CD in the CD-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 CD, the system will eject the Recovery CD 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.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.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	<a href="http://syslinux.zytor.com/">http://syslinux.zytor.com/</a>	X	X
7-zip	<a href="http://www.7-zip.org">http://www.7-zip.org</a>	X	
GNU sed	<a href="http://unxutils.sourceforge.net">http://unxutils.sourceforge.net</a> application downloaded from <a href="http://student.northpark.edu/pemente/sed/">http://student.northpark.edu/pemente/sed/</a>	X	