# InfraStruxure® Central Smart Plug-in for HP Operations Manager for Windows

## Table of Contents

# Section 1: Concepts

## *Abbreviations*

- GUID - Globally Unique Identifier: A sequence of 16 bytes generated in such a way it is guaranteed to be unique, even when used across multiple computer systems
- OMW - Hewlett Packard's Operations Manager for Windows
- SPI - Smart Plug-in: A software component that extends the capabilities of OMW
- WMI - Windows Management Instrumentation: A facility common to computer systems running Windows that provides a standard interface for controlling and accessing information regarding various parts of the system

## *Smart Plug-in Overview*

The APC InfraStruxure Central server is a network appliance that collects data from and monitors status of devices that support data center critical infrastructure.

The APC InfraStruxure Central Smart Plug-in for HP Operations Manager for Windows provides a link between the physical infrastructure components monitored by InfraStruxure Central servers, such as power, cooling, and environmental devices, and the server infrastructure monitored by OMW such as servers, services, and applications.
The SPI runs as a Windows service on a machine that has the OMW agent installed. The SPI package consists of several components:

- Server Integration Components
  - Five programs:
    - A configuration utility
    - An inventory integration component that synchronizes the inventory between InfraStruxure Central and OMW
    - An alarm integration component that projects active alarms in InfraStruxure Central as messages in OMW
    - A service process that schedules the execution of the inventory and alarm components
    - A device information tool defined in OMW as a management server-based utility that displays detailed information about any InfraStruxure Central device to an operator
  - A default OMW policy set: These policies ensure the messages generated by the alarm integration component of the SPI are processed properly by OMW. The default policy

set also includes policies to monitor the SPI service process and event log entries logged by the components themselves.
    - A default configuration file set: These files contain the default SPI configuration.

- Client Integration Components
    - A set of icon files installed on each system running the OMW console: These icons are used in the visual display of services and tools in OMW.

## *Smart Plug-in Workflow*

The general workflow for the SPI is as follows:

- The SPI is installed.
- The configuration utility is run, the basic configuration is set, and at least one InfraStruxure Central server is registered.
- The integration components are run according to the configured schedule.
- The inventory integration component runs to synchronize the InfraStruxure Central inventory with OMW, and gather information required by the alarm integration component.
- The alarm integration component runs to project active alarms in InfraStruxure Central as messages in OMW. This component may run before the initial inventory based on its schedule, but it will not completely process any alarms until the inventory integration component completes for the first time.
- The configuration utility may be used to further modify the configuration based on information gathered by the inventory component, such as newly-encountered device types and device groups.

## *Projection Model for Inventory Integration*

The SPI projects the InfraStruxure Central inventory into OMW using the following model:

- All InfraStruxure Central servers registered using the configuration utility are projected into OMW as managed nodes.
- All managed nodes are in a node group named “Power and Cooling Infrastructure” by default.
- Each managed node is also projected as a service in the service tree.
- The services for InfraStruxure Central servers are under a root-level service named “Power and Cooling Infrastructure” by default.
- For each InfraStruxure Central server:
    - Each device group is projected as a service node directly under the service node of the InfraStruxure Central server itself.

- Each device for which that device group is considered the primary device group is projected as a service node directly under the service node of the device group.

*For more information regarding the determination of the primary device group and the inclusion/exclusions of devices according to their type, see the configuration section (3) of this manual.*

- Tools and Actions are created and assigned to managed nodes and services where appropriate.

*For more information regarding the operational considerations of the SPI, see the operational section (4) of this manual.*

## Caution Regarding HP OMW Impact

The default SPI configuration is designed to limit the impact on HP OMW. As the configuration of the SPI is changed, it is important to understand the effect these changes will have on OMW. The following are several items to consider:

- The default configuration specifies transaction batch size limits, a commit delay, and a batch limit designed to limit the number of adds, deletes, and changes performed in OMW in a single inventory synchronization cycle. This configuration is usually sufficient for normal use. Changes are made through the OMW WMI provider, which is not designed for a high volume of changes for a sustained time. The number of changes is usually minimal, especially after the initial inventory.
- The default configuration does not inventory any device types, and sets the default for new device types to follow the same behavior. The number of devices managed by InfraStruxure Central servers, whose type is marked for inventory in the SPI, directly relates to the number of services created in OMW. By HP's own design guidelines, any more than ten child services under any given services node begins to degrade the usability of the product. The following limitations will begin to become a factor:
  - The Map View for services becomes unreadable if there are too many services in the hierarchy, especially under a single parent.
  - The performance of operations through the WMI provider will degrade if too many services, overall, are created.
- In general, the principle of operation for OMW is to manage by policy and messages. The service tree, a relatively new addition in OMW 8, provides some measure of visual interaction with the infrastructure, but is not designed for granular modeling of large numbers of systems and components.

- The principle of operation for InfraStruxure Central includes a rich visual model. Therefore, linking the two models together requires not only that the objects be synchronized, but that the principles of operation are merged as well.
- For this reason, the SPI works equally well with or without projecting individual devices into the services tree. Each message is self-contained and is populated with Custom Message Attributes that can be used to identify the exact source of the message. The Device Information Tool also allows operators to examine the source device or sensor in detail.
- Use caution when modifying the default behavior of the SPI so the services tree is not overloaded.

# Section 2: Installation and Uninstallation

## *Installation Requirements*

- Server Installation Components
    - Disk space requirements: 50 MB
    - Memory requirements: 20 MB of memory consistently with up to 250 MB during inventory
    - Windows Version: Windows XP or 2003 or above with .NET Framework 2.0
    - HP Operations Manager for Windows
        - Server: Version 8.1 (may be on a different physical server)
        - SPI Installation Point: Agent Version 8.1
    - InfraStruxure Central server: Version 6.0 or above
- Client Installation Components
    - To install the custom icons for the objects created by the SPI:
        - HP Operations Manager for Windows: Console Version 8.1
    - To enable launching of the InfraStruxure Central client as a tool linked in OMW:
        - InfraStruxure Central: Client version matching the managed InfraStruxure Central servers
- Supported Character Sets/Locales
    - Only single byte character sets are supported. Character sets for languages that require double byte character sets are not supported through the OMW Message Stream Interface.

## *Installation Considerations*

### Security Credentials

- The installer must be run with administrative rights, whether installing the server integration components, client integration components, or both.
- The Services Controller should be installed to run as an account that has write access to the data directory specified during installation.
- If the service account is not an administrator of the system on which the service is running, some additional steps must be taken:
    - Ensure the account has the appropriate permissions to access the SPI registry key. The RegistryTool.exe utility, provided with the installation in the program directory, can be used to set the required permissions. See details about using this tool in section 4.

    - Ensure the event log sources used by the SPI are registered. The RegisterEventLogSources.exe utility, also provided with the installation in the program directory, can be used to create these. This utility takes no parameters.
- If the OMW WMI provider resides on the same server as the Services Controller, usually the case on a management server, the OMW connection must be made under this identity. Additionally, the service account needs rights to OMW (admin rights sufficient to read and write through the OMW WMI provider).
- The InfraStruxure Central credentials may be administrative or a restricted user. If a restricted user is specified, only those devices visible to that user will be inventoried.

## Data File Location

The location chosen for the SPI data files should be a reliable location included in some form of backup schedule. The data files include the following critical components of the SPI:

- The SPI configuration
- The mapping of each object from the InfraStruxure Central inventory to each object created by the SPI in OMW:
  If this file is lost, the SPI cannot link the InfraStruxure Central inventory to the existing inventory projected into OMW. The SPI will then re-create every object with new GUIDs and delete the existing objects.
- The mapping of active alarms in InfraStruxure Central projected into OMW:
  If this file is lost, the SPI cannot determine which alarms have already been projected into OMW. Every alarm will then generate a new message.

# *Installation Components*

## Server Integration Components

The server integration components are installed on the OMW management server. The server integration components consist of the following:

- SPI Executables
    - Configuration Utility
    - Inventory Integration Engine
    - Alarm Integration Engine
    - Device Information Tool
    - Services Controller
    - Support Library
    - Registry Tool
    - Tool to Register Event Log Sources

- Services Controller, installed as a Windows service, named “ApcIsxcSpiService “ with the display name "APC InfraStruxure Central SPI for HP OMW Services Controller"
- Operations Manager Policy
  - The policy may optionally be uploaded by the installer.
  - If you choose to allow the installer to upload the policy, you may optionally choose to have it backup the existing policy and/or automatically deploy the new policy to a node or node group of your choice.
  - If you prefer to inspect the policy first, the files are installed in the Policy sub-folder of the SPI program install location.
- Start Menu Program Group, from which the Uninstaller and Configuration Utility may be accessed
- Registry settings under HKLM\Software\APC\ApcIsxcSpiForHpOmw

### Client Integration Components

The client integration components are typically installed on every workstation running the OMW console. These workstations may also be running the InfraStruxure Central client.
The client integration components consist of the following:

- Icons for services and tools that are copied to the appropriate locations beneath the OMW install directory
- An environment variable named ISXCUI that the console uses to locate the InfraStruxure Central client, if it is also installed

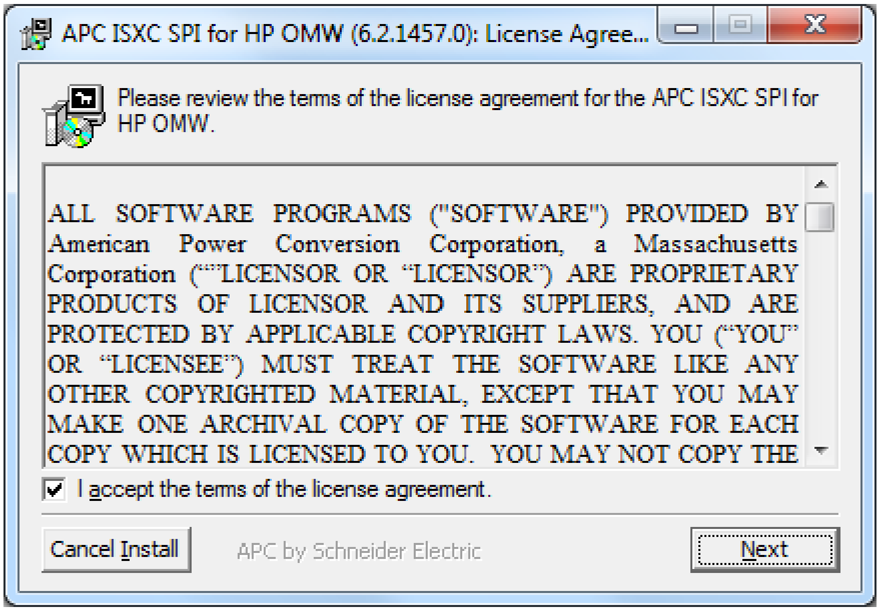
Note: The client integration components are optional. It is also possible to install either of the two components listed above separately. During the installation, if the OMW or InfraStruxure Central client install directory is not specified, the icons and environment variable, respectively, will not be implemented. The ramifications of this are as follows:

- If the icons are not installed, the OMW console will show the tools and services with the default icons instead of the custom icons supplied with the SPI.
- If the InfraStruxure Central client installation is not identified, the tool to launch the InfraStruxure Central client from a managed node, server, or message will not function properly. If the InfraStruxure Central client is not installed on a console machine or it is not desirable for certain operations workstations to have access to the InfraStruxure Central client directly, this may be the desired behavior.

## *Installation Walk-Through*

### License Agreement Acceptance

The first step in the installation is the license acceptance. The license agreement must be accepted for the installation to continue.



APC ISXC SPI for HP OMW (6.2.1457.0): License Agree...

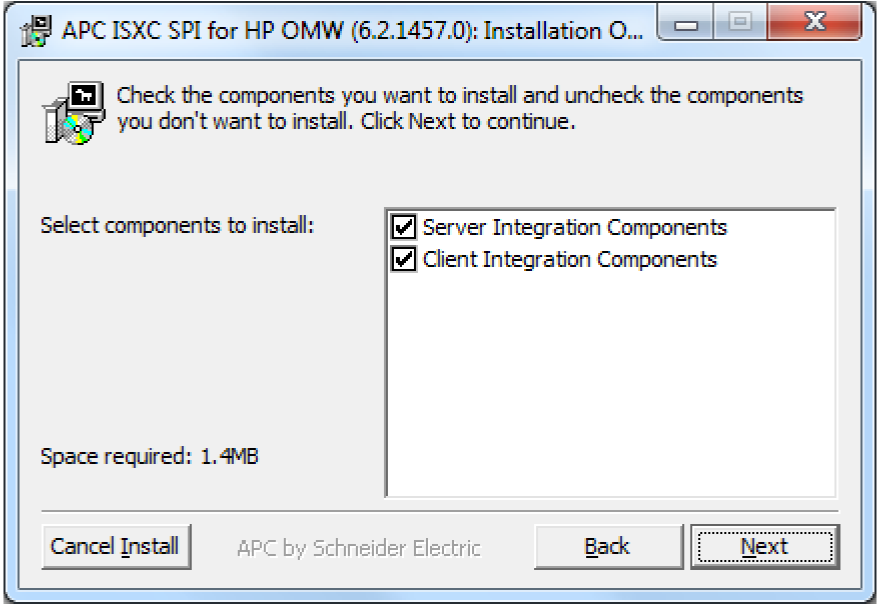
Please review the terms of the license agreement for the APC ISXC SPI for HP OMW.

ALL SOFTWARE PROGRAMS ("SOFTWARE") PROVIDED BY American Power Conversion Corporation, a Massachusetts Corporation (“"LICENSOR OR “LICENSOR”) ARE PROPRIETARY PRODUCTS OF LICENSOR AND ITS SUPPLIERS, AND ARE PROTECTED BY APPLICABLE COPYRIGHT LAWS. YOU (“YOU” OR “LICENSEE”) MUST TREAT THE SOFTWARE LIKE ANY OTHER COPYRIGHTED MATERIAL, EXCEPT THAT YOU MAY MAKE ONE ARCHIVAL COPY OF THE SOFTWARE FOR EACH COPY WHICH IS LICENSED TO YOU. YOU MAY NOT COPY THE

☑ I accept the terms of the license agreement.

## Component Selection

The next step in the installation is to select the components you wish to install. The server integration components and client integration components can be installed together or separately, depending on the requirements of the machine on which the installation is being run.



APC ISXC SPI for HP OMW (6.2.1457.0): Installation O...

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

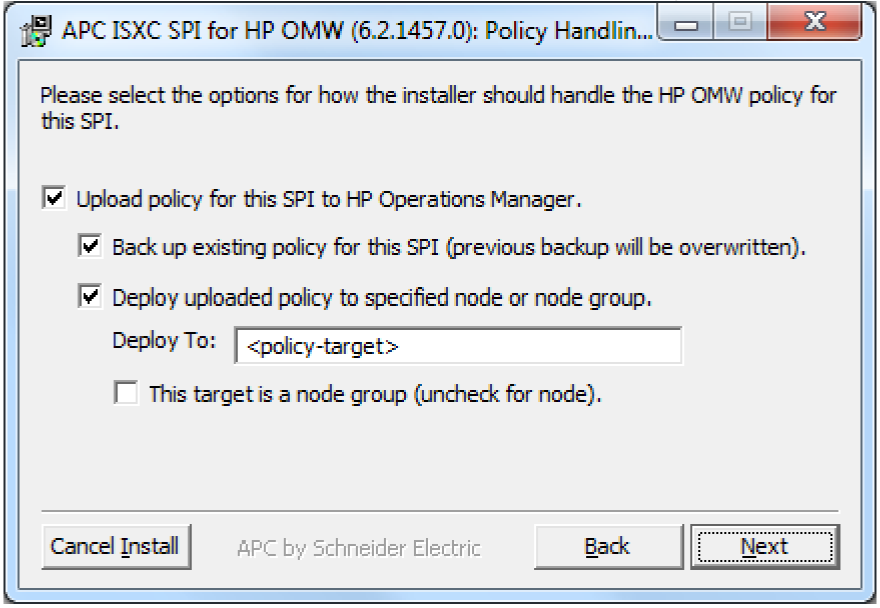
☑ Server Integration Components
☑ Client Integration Components

Space required: 1.4MB

## Policy Handling Options (Server Integration Component Only)

The following options are available when installing the Server Integration Components. These govern the behavior of the installer with respect to policy installation in OMW.

If the option to back up existing policy is selected, the policy will be stored in the program directory (selected in the next window) under a folder named PolicyBackup.



APC ISXC SPI for HP OMW (6.2.1457.0): Policy Handlin...

Please select the options for how the installer should handle the HP OMW policy for this SPI.

☑ Upload policy for this SPI to HP Operations Manager.

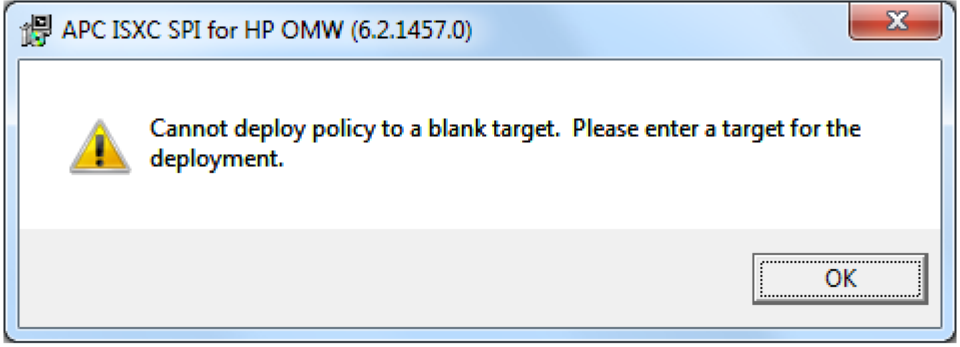
☑ Back up existing policy for this SPI (previous backup will be overwritten).

☑ Deploy uploaded policy to specified node or node group.

Deploy To: <policy-target>

☐ This target is a node group (uncheck for node).

Note the target cannot be blank, if the option to deploy is selected. Doing so will generate the following warning message:

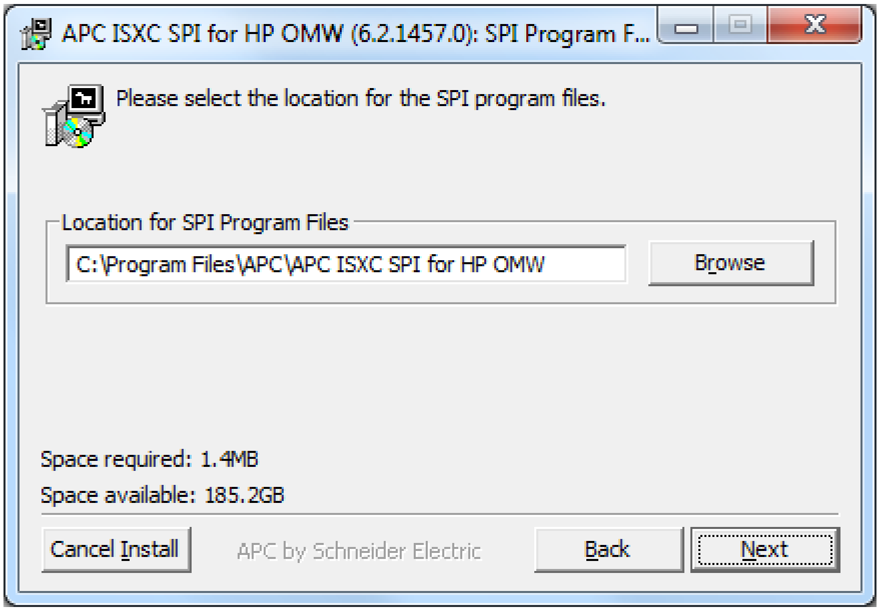


APC ISXC SPI for HP OMW (6.2.1457.0)

Cannot deploy policy to a blank target. Please enter a target for the deployment.

## Location for SPI Program Files (Server Integration Components Only)

If the server integration components are selected, you will be asked to specify the location to which the SPI program and data files will be installed. The installer chooses an appropriate default for you, but you may specify any location you choose, as follows:



APC ISXC SPI for HP OMW (6.2.1457.0): SPI Program F...

Please select the location for the SPI program files.

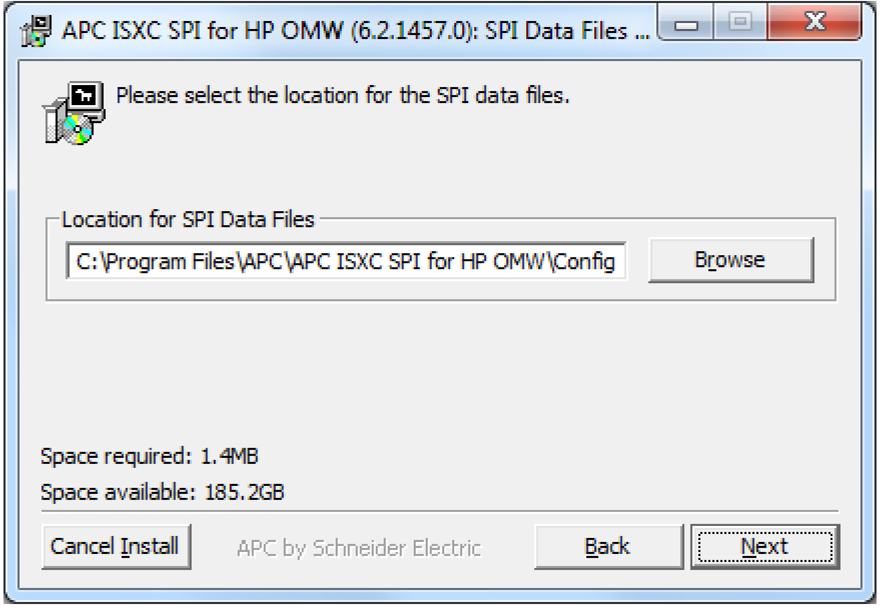
Location for SPI Program Files: C:\Program Files\APC\APC ISXC SPI for HP OMW

Space required: 1.4MB

Space available: 185.2GB

## Location for SPI Data Files (Server Integration Components Only)

After specifying the location in which to install the program files, you will be asked to specify the location in which the SPI programs will store their data files.  The initial configuration files will also be installed to this location.  The installer chooses the default location to be the **Config** subdirectory of the location you specified for the SPI programs, as follows:



APC ISXC SPI for HP OMW (6.2.1457.0): SPI Data Files ...

Please select the location for the SPI data files.

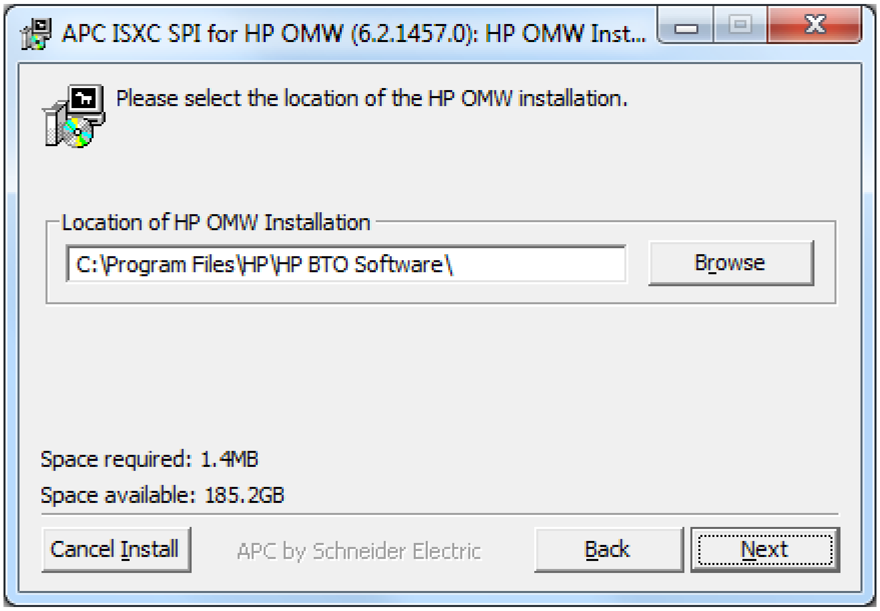
Location for SPI Data Files: C:\Program Files\APC\APC ISXC SPI for HP OMW\Config

Space required: 1.4MB

Space available: 185.2GB

## Location of the HP OMW Installation

The OMW installation must be located for (a) Server Integration Components if policy operations were requested (upload, backup, and/or deploy) or (b) Client Integration Components, which include icons that must be installed within the OMW installation tree.



APC ISXC SPI for HP OMW (6.2.1457.0): HP OMW Inst...

Please select the location of the HP OMW installation.

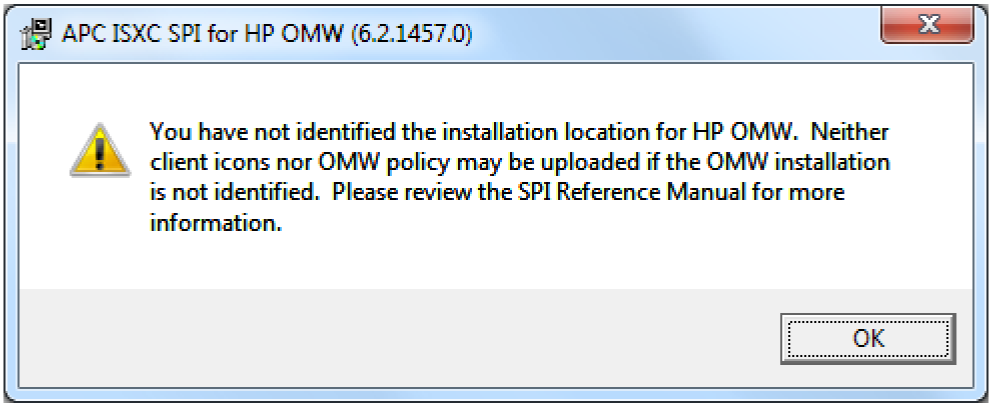
Location of HP OMW Installation

C:\Program Files\HP\HP BTO Software\

Space required: 1.4MB

Space available: 185.2GB

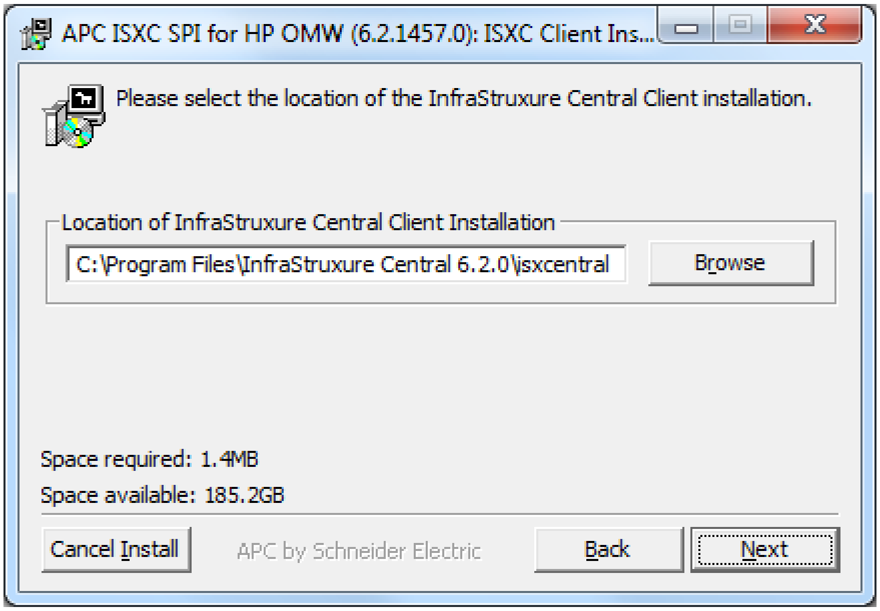
If any of the requirements are present for this location but the location is not identified, you will be warned as follows:



APC ISXC SPI for HP OMW (6.2.1457.0)

You have not identified the installation location for HP OMW. Neither client icons nor OMW policy may be uploaded if the OMW installation is not identified. Please review the SPI Reference Manual for more information.

## InfraStruxure Central Client Installation Location (Client Integration Components Only)



APC ISXC SPI for HP OMW (6.2.1457.0): ISXC Client Ins...

Please select the location of the InfraStruxure Central Client installation.

Location of InfraStruxure Central Client Installation

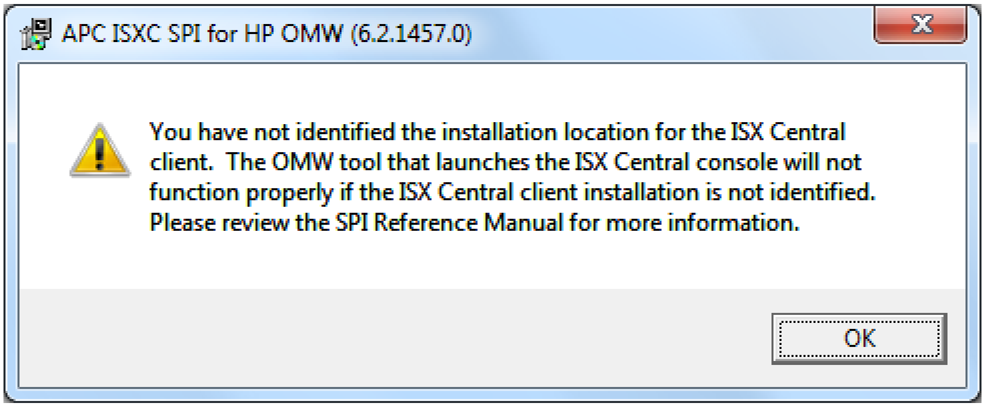
C:\Program Files\InfraStruxure Central 6.2.0\isxcentral

Space required: 1.4MB

Space available: 185.2GB

Cancel Install
APC by Schneider Electric
Back
Next

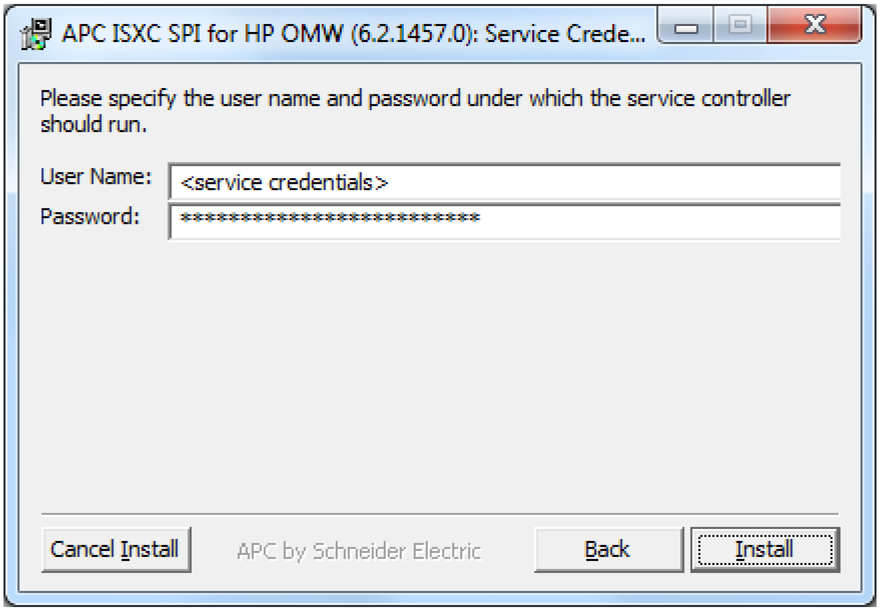
If any of the requirements are present for this location but the location is not identified, you will be warned as follows:



You have not identified the installation location for the ISX Central client. The OMW tool that launches the ISX Central console will not function properly if the ISX Central client installation is not identified. Please review the SPI Reference Manual for more information.

## Service Credentials (Server Integration Components Only)

The next step of the installation is to provide the credentials under which the SPI service controller will run.



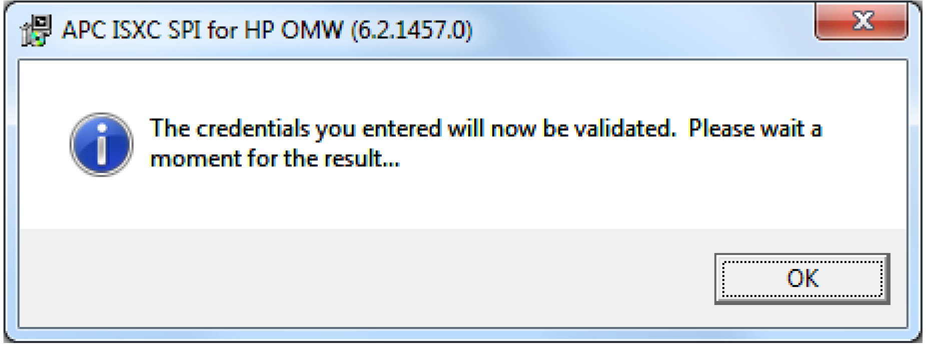
APC ISXC SPI for HP OMW (6.2.1457.0): Service Crede...

Please specify the user name and password under which the service controller should run.

User Name: <service credentials>

Password: ****************************

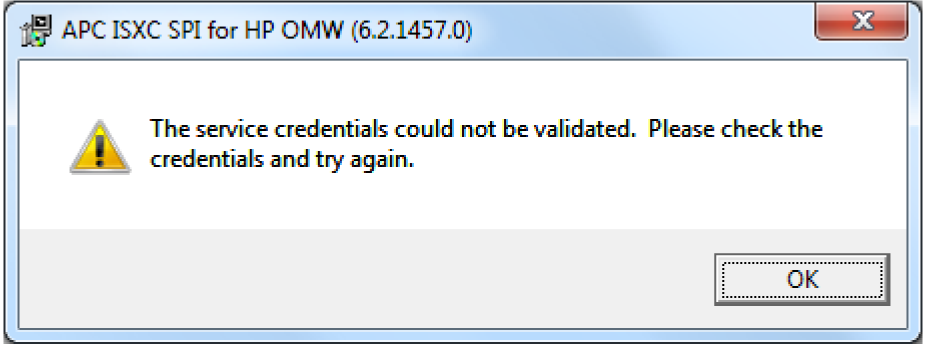
After the credentials are entered, they will be verified:



APC ISXC SPI for HP OMW (6.2.1457.0)

The credentials you entered will now be validated.  Please wait a moment for the result...

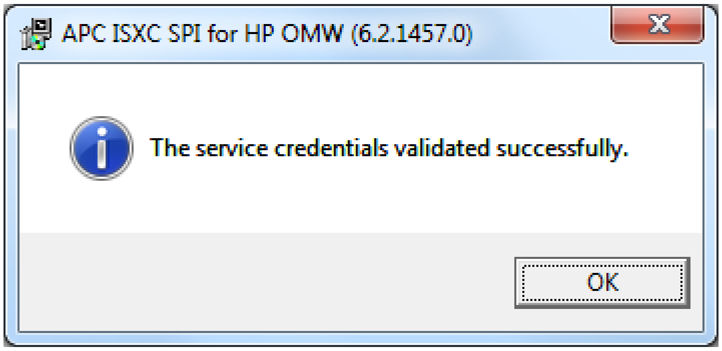
The results of the validation will be displayed.  Credentials that cannot be verified must be corrected before the installation can continue, as indicated by the following warning:



APC ISXC SPI for HP OMW (6.2.1457.0)

The service credentials could not be validated.  Please check the credentials and try again.

If the credentials are successfully validated, you will receive the following confirmation:

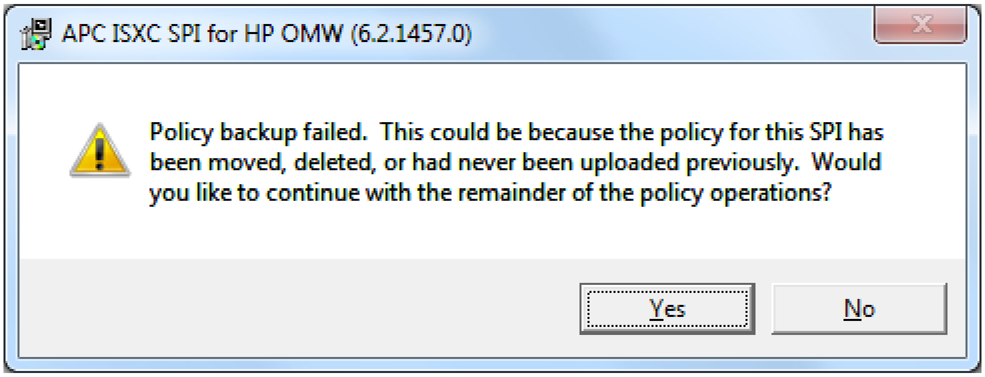


APC ISXC SPI for HP OMW (6.2.1457.0)

The service credentials validated successfully.

## Issues During Install – Policy Operations

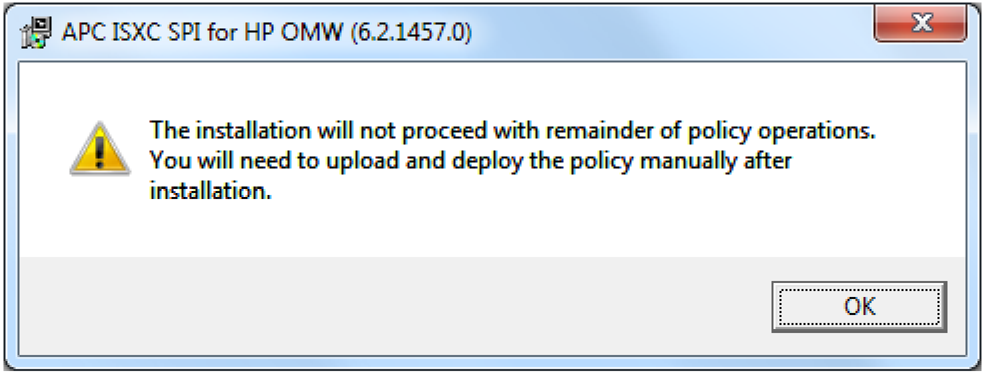
If any of the policy operations encounter issues, you will be warned accordingly. Note that the policy backup may fail if it is selected and the policy cannot be backed up (e.g. if the SPI policy never existed, has been moved, or has been deleted). This is the only issue with policy operation that provides you with the option of continuing with the remainder of the policy options.



APC ISXC SPI for HP OMW (6.2.1457.0)

Policy backup failed. This could be because the policy for this SPI has been moved, deleted, or had never been uploaded previously. Would you like to continue with the remainder of the policy operations?

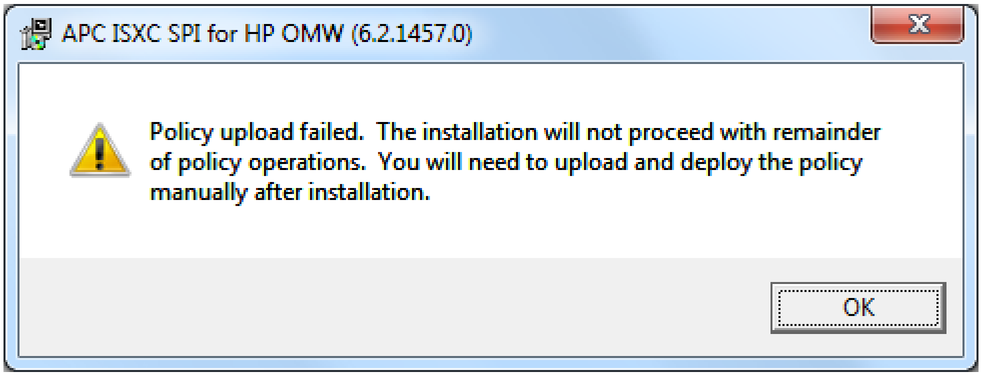
If you choose not to continue, the installation will continue, but you will be warned of the consequences, as follows:



APC ISXC SPI for HP OMW (6.2.1457.0)

The installation will not proceed with remainder of policy operations. You will need to upload and deploy the policy manually after installation.

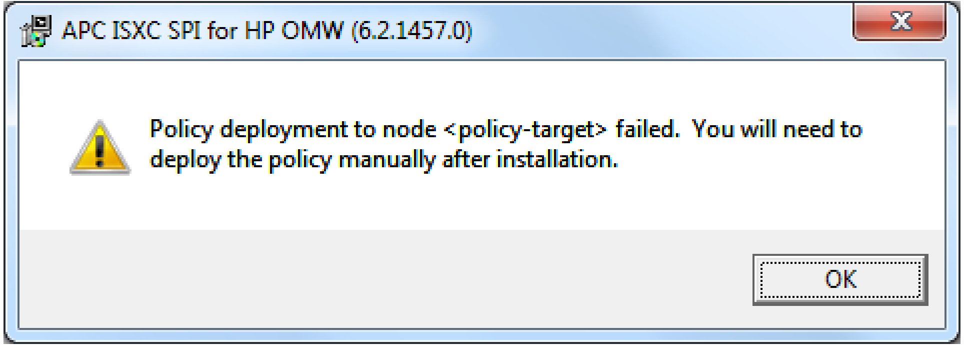
The next policy operation is the policy upload. If this fails, you will be notified, but the remainder of the policy operations cannot continue (deployment).



APC ISXC SPI for HP OMW (6.2.1457.0)

Policy upload failed. The installation will not proceed with remainder of policy operations. You will need to upload and deploy the policy manually after installation.

If the upload succeeds, the deployment may fail (especially if the target does not exist or is misspelled). You will be warned accordingly, as follows:



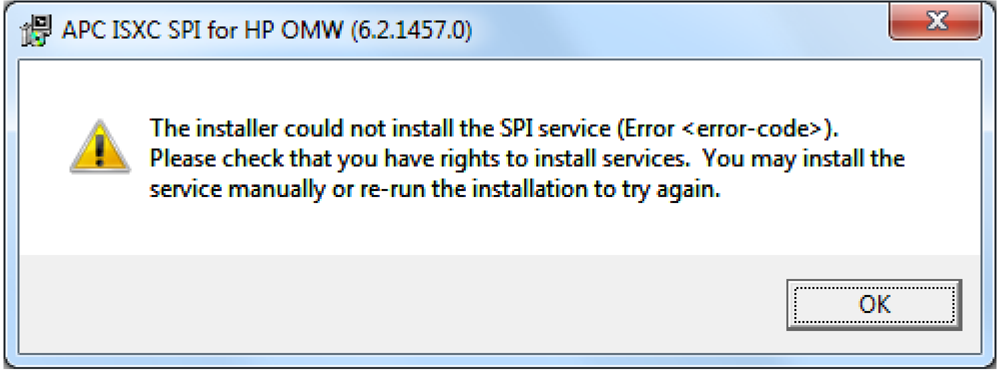
APC ISXC SPI for HP OMW (6.2.1457.0)

Policy deployment to node <policy-target> failed. You will need to deploy the policy manually after installation.

If any policy operations fail, it is strongly recommended that you complete those tasks manually. The policy is installed in the program folder under the folder named Policy.

## Issues During Install –Services Controller Installation

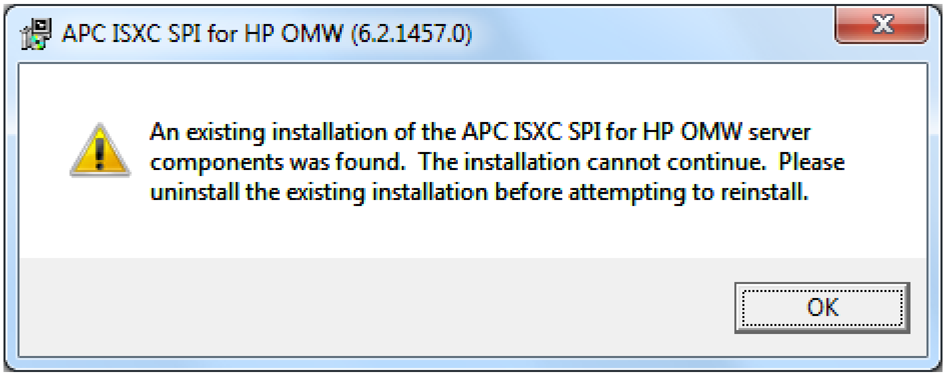
If the Services Controller cannot be installed, you will be warned as such:



APC ISXC SPI for HP OMW (6.2.1457.0)

The installer could not install the SPI service (Error <error-code>). Please check that you have rights to install services. You may install the service manually or re-run the installation to try again.

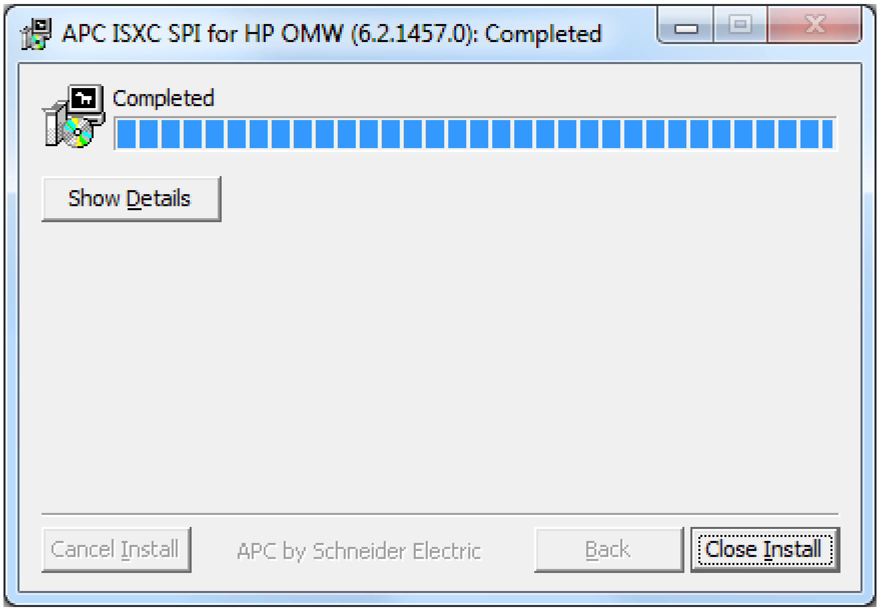
You may install the service manually (using the Windows sc.exe utility) or re-run the installation. No executables will be scheduled if the Services Controller is not installed.
If you attempt to install the SPI services when they are already installed, you will be warned as follows and the installation will be aborted:


APC ISXC SPI for HP OMW (6.2.1457.0)

An existing installation of the APC ISXC SPI for HP OMW server components was found. The installation cannot continue. Please uninstall the existing installation before attempting to reinstall.

## Completing the Installation

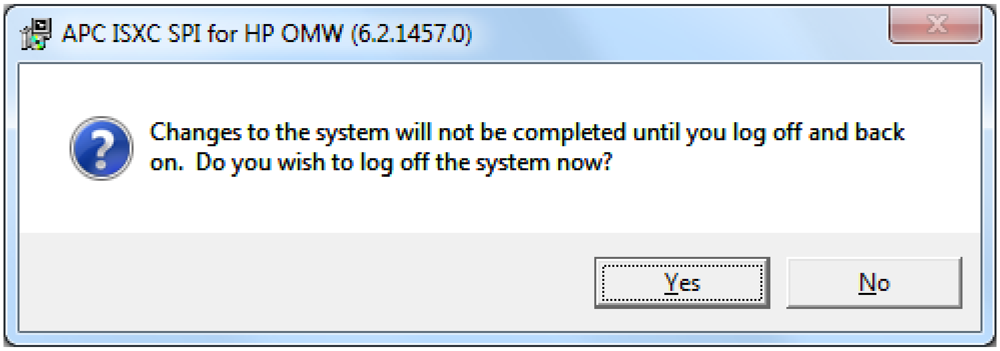
After the installation completes, you may close the installer or press **Show Details** to see a log of the individual actions taken by the installer. The final installer window:


APC ISXC SPI for HP OMW (6.2.1457.0): Completed

Completed

## Post-Install Tasks

If the install included the client components, you will be asked to log off and back on. This is to allow the changes to the environment variables to take effect.

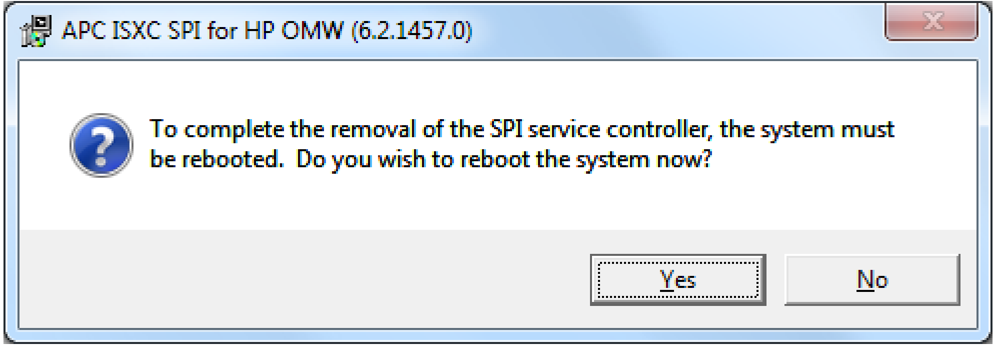


APC ISXC SPI for HP OMW (6.2.1457.0)

Changes to the system will not be completed until you log off and back on.  Do you wish to log off the system now?

## Post-Uninstall Tasks

If the uninstaller detected that the SPI service controller was installed, it will have stopped and removed the service from the system.  In this case, the uninstaller will prompt you to reboot the system.  This is to complete the removal of the SPI service controller.

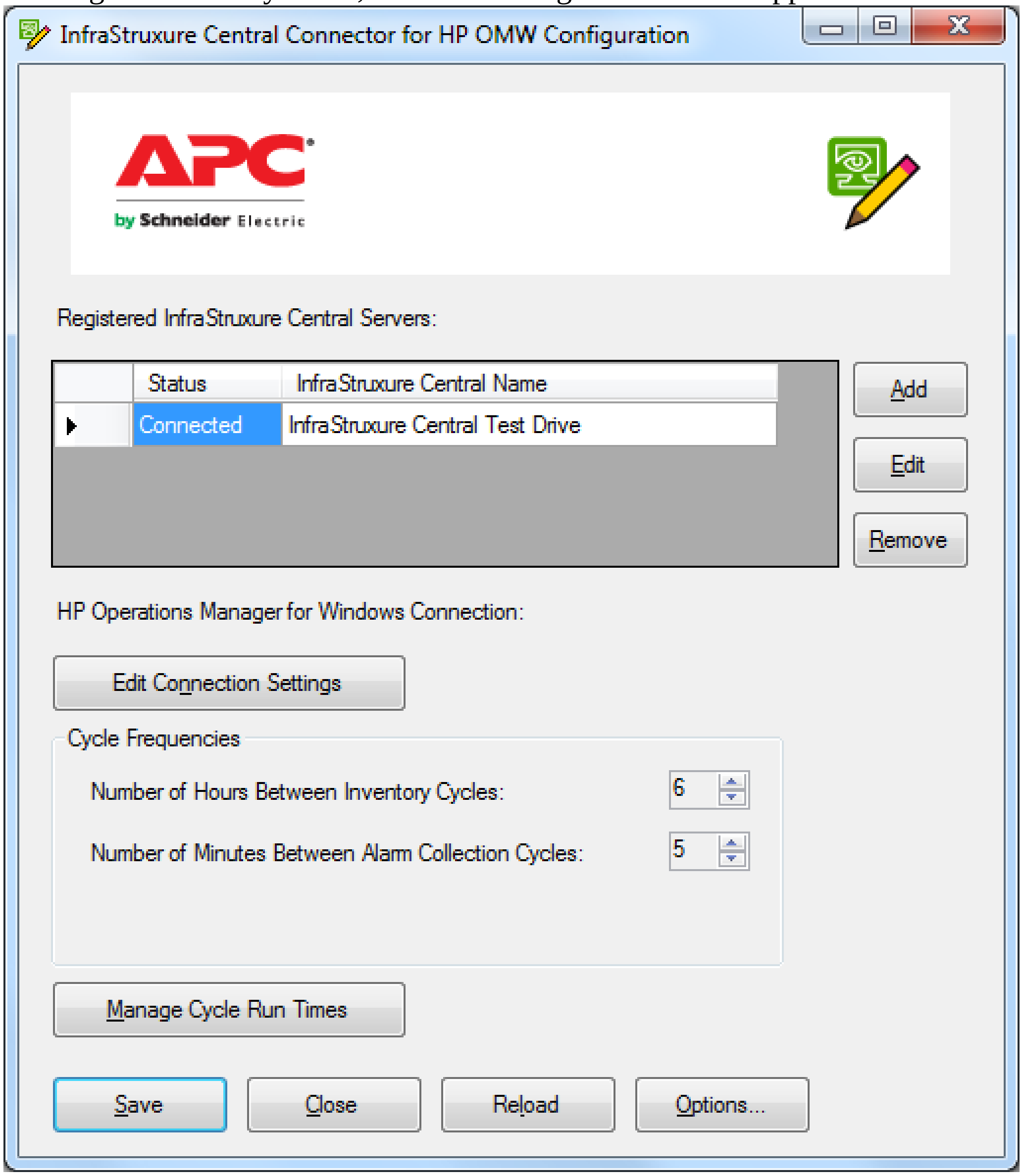


APC ISXC SPI for HP OMW (6.2.1457.0)

To complete the removal of the SPI service controller, the system must be rebooted.  Do you wish to reboot the system now?

# Section 3: Configuration

When the configuration utility is run, the main configuration screen appears.


InfraStruxure Central Connector for HP OMW Configuration
APC by Schneider Electric
Registered InfraStruxure Central Servers:
Add
Edit
Remove
HP Operations Manager for Windows Connection:
Edit Connection Settings
Cycle Frequencies
Manage Cycle Run Times
Save
Close
Reload
Options...

| | Status | InfraStruxure Central Name |
|---|---|---|
| ▶ | Connected | InfraStruxure Central Test Drive |

Number of Hours Between Inventory Cycles: 6

Number of Minutes Between Alarm Collection Cycles: 5

*Figure 1: The main configuration screen.*

## *The Main Configuration Screen*

### General

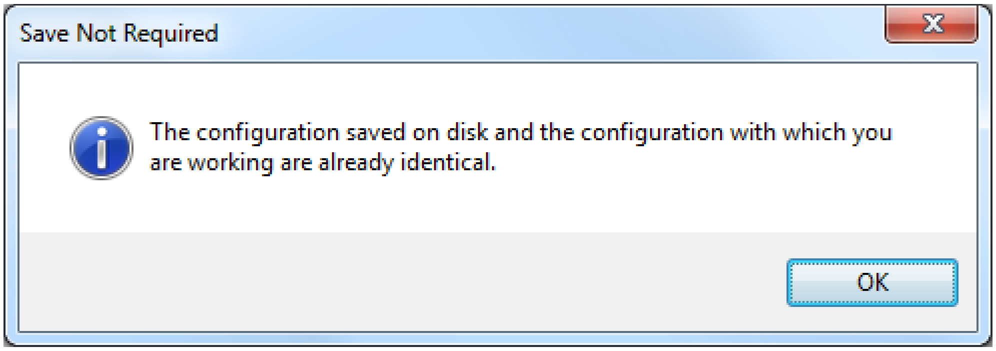
The **Save** button will save the current configuration. Up to nine previous versions of the configuration files are kept in the data file location chosen during install. Note that no changes are saved to the files unless the **Save** option is selected on this main form. Changes to the OMW connection, registered InfraStruxure Central servers, device groups, and device types are all saved together when this option is selected.

The **Close** button will exit the configuration utility. Unsaved changes will generate a warning, providing you the opportunity to save them before exiting.

The **Reload** button will reload the configuration from the underlying files. This is useful if an inventory has recently completed and you would like to make changes to the latest device group and device type configuration for the registered InfraStruxure Central servers.

Note the configuration can be in four states, which affect the warning displayed when saving, closing, reloading, or changing run times:

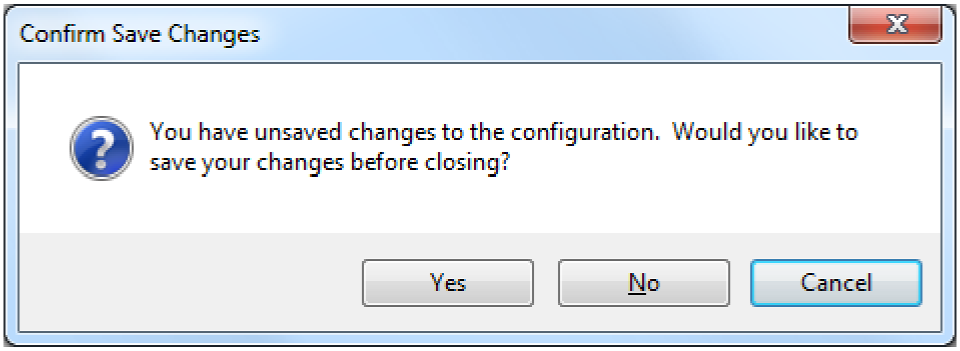
- The configuration has not been modified. The following warning identifies this state (example taken after pressing **Save**):



Save Not Required

The configuration saved on disk and the configuration with which you are working are already identical.

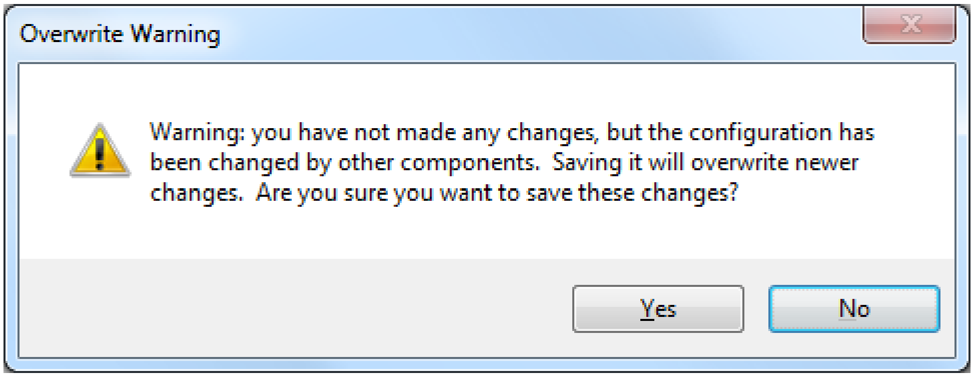
- The configuration has been modified by you using the configuration utility, but has not been saved. The following warning identifies this state (example taken after pressing **Close**):



Confirm Save Changes

You have unsaved changes to the configuration. Would you like to save your changes before closing?

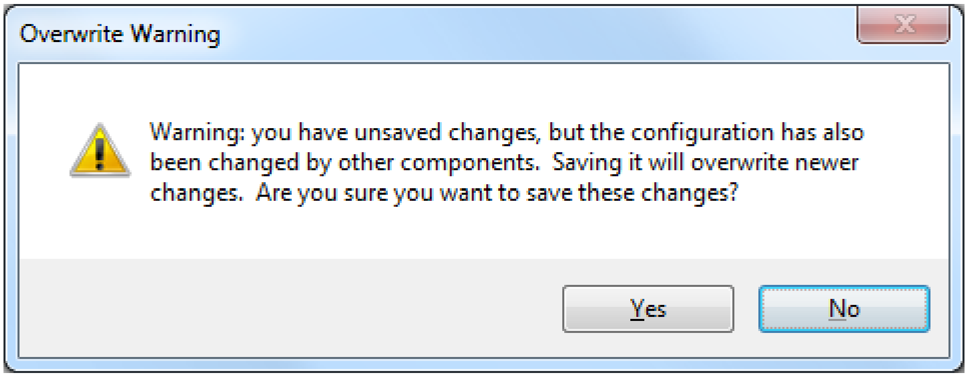
- The configuration has been modified external to the configuration utility (such as an inventory run). The following warning identifies this state (example taken after pressing Save):



Overwrite Warning

Warning: you have not made any changes, but the configuration has been changed by other components. Saving it will overwrite newer changes. Are you sure you want to save these changes?

- The configuration has been modified by both you and externally. The following warning identifies this state (example taken after pressing Save):



Overwrite Warning

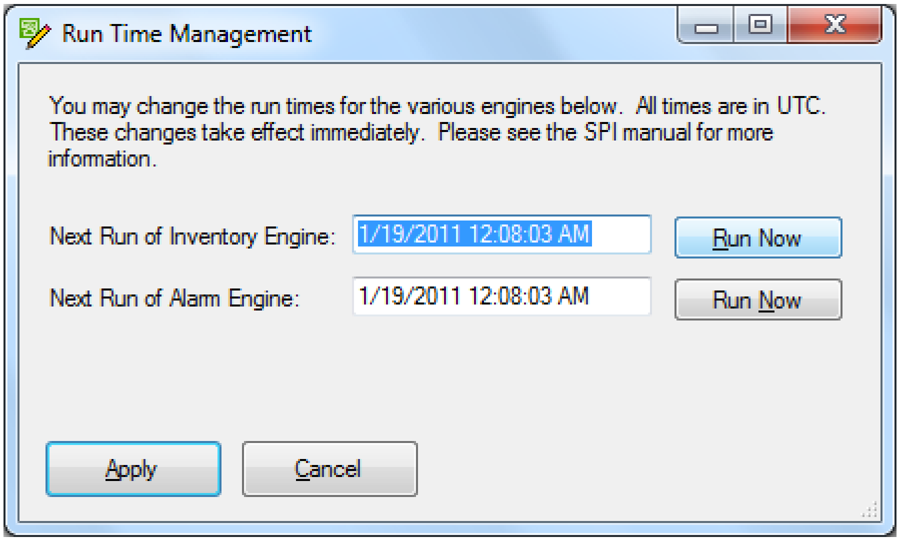
Warning: you have unsaved changes, but the configuration has also been changed by other components. Saving it will overwrite newer changes. Are you sure you want to save these changes?

## Cycle Frequency

These values govern how frequently each of the two SPI engines is run. These values are measured relative to the previous run.

## *Managing Cycle Run Times*

Clicking the **Manage Cycle Run Times** button results in the following window (sample data shown):


Run Time Management

You may change the run times for the various engines below. All times are in UTC. These changes take effect immediately. Please see the SPI manual for more information.

Next Run of Inventory Engine: 1/19/2011 12:08:03 AM

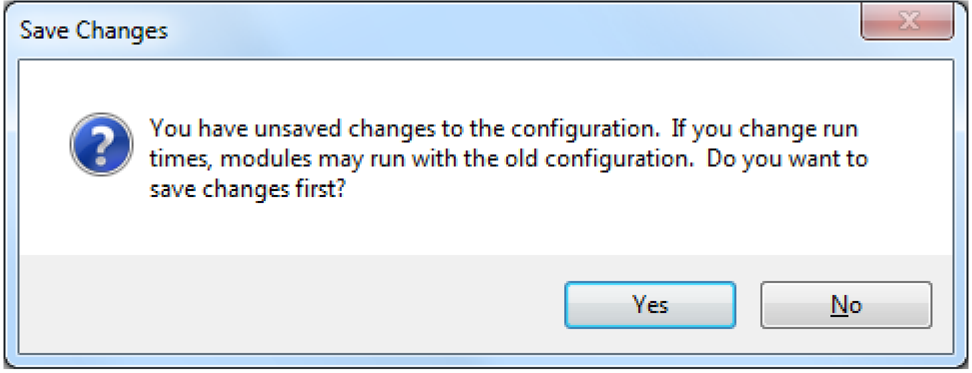
Next Run of Alarm Engine: 1/19/2011 12:08:03 AM

The “next run” values are the current values stored in the registry that the scheduler is using to determine when next to run each particular component. You may change these values here and click **Apply**. *Note the values are in UTC.* You may also click **Run Now** to insert the current date and time in UTC into the text box.

It is important to note if the Services Controller is not running when these values are changed, when it starts, it will consider any “next run” value that has already passed as being a missed run. It will not run immediately, but adjust the “next run” value per the run intervals configured to be a future date and time. Especially for the inventory module, this can be several hours into the future.

If the Services Controller is running, a “next run” value that has already passed will be considered differently, causing the component to be run immediately. Therefore, ensure the Services Controller is running before using this window to schedule an immediate run.

Because this function can be used to request an immediate run, it is likely changes to the configuration have been made, prompting the request for the immediate run. Therefore, if there are unsaved changes when you select this function, you will be warned as follows:


Save Changes

You have unsaved changes to the configuration. If you change run times, modules may run with the old configuration. Do you want to save changes first?

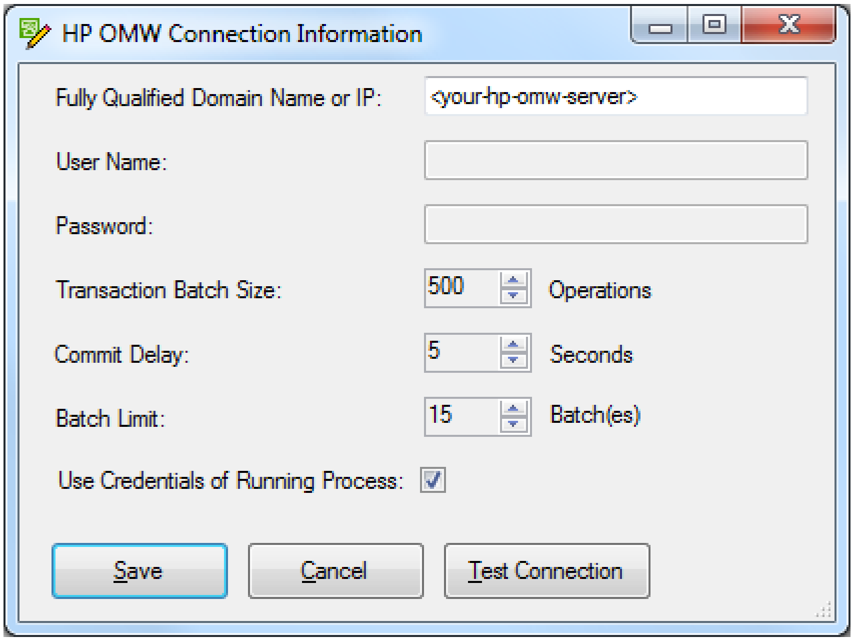
You may also use this window to change the “next run” values to a specific date and time to ensure a predictable run time. The scheduler always selects the next “next run” value based on the current “next run” value, incrementing evenly by the run intervals configured. Therefore, for example, if you configure inventory to run every 6 hours, you can use this window to set the next run to today at 1:30 PM (UTC). This will cause the inventory module to run at UTC 1:30 PM, UTC 7:30 PM, UTC 1:30 AM, and UTC 7:30 AM every day.

## *Registered InfraStruxure Central Servers*

This is the list of the InfraStruxure Central servers registered with the SPI to be integrated into OMW. The current status of each registered InfraStruxure Central is also shown.
You may **Add** a registration for a new InfraStruxure Central server, or select one of the existing InfraStruxure Central servers and **Edit** or **Remove** it.
Important: InfraStruxure Central servers are assigned a unique identifier (GUID) when they are first registered. This GUID is essential to the mapping of objects between an InfraStruxure Central server and OMW. If you remove an InfraStruxure Central server and re-add it with exactly the same parameters, the GUID will still be different. This will cause all objects in OMW to be deleted and re-created, since their underlying GUID will have changed. Instead, consider changing the status of an InfraStruxure Central server until you are certain that you will not need it again.

## *HP Operations Manager for Windows Connection*

From the main configuration screen, pressing the **Edit Connection Settings** button for the OMW connection shows the screen depicted in figure 2. The following settings govern the connection the SPI services make to the OMW server:



HP OMW Connection Information

Fully Qualified Domain Name or IP: <your-hp-omw-server>

User Name:

Password:

Transaction Batch Size: 500 Operations

Commit Delay: 5 Seconds

Batch Limit: 15 Batch(es)

Use Credentials of Running Process: ☑

*Figure 2: The HP OMW Connection Information screen.*

## OMW Server Location and Credentials

Enter the fully qualified domain name or IP address of the OMW server. This should be the name of the server on which the OMW WMI provider is running. For clusters, enter an IP or Network Name that is in the OMW resource group such that it will follow the active node. Authentication may be via a user name/password entered explicitly or set to use the credentials of the running process. The "running process" will be the account under which the SPI control service runs on the managed node. Ensure that this account has access to OMW.

Note: If you are running the configuration tool as a user other than the user as which the actual SPI services will run, the Test Connection button will verify the accessibility of the OMW provider as the user as which the configuration utility is being run. This user may or may not have the same access as the user as which the actual SPI services run.

Important: If the SPI services are running on the same machine as the OMW provider, the **Use credentials of running process** option must be checked.

## Transaction Limiting

All changes to the OMW inventory are made in the context of a transaction. Three connection settings govern the behavior of the SPI regarding transactions. This only affects the inventory component of the SPI.

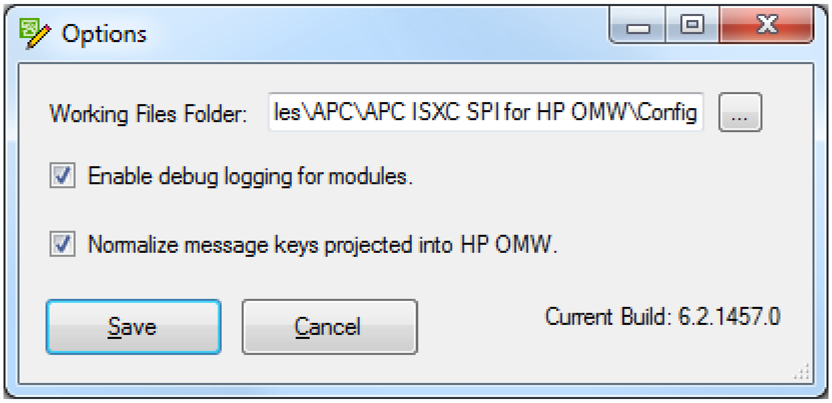
- **Batch Size**: The maximum number of operations (adds, deletes, or changes) performed by the SPI processes before the active transaction is committed and a new one is started.
- **Commit Delay**: The number of seconds the SPI will pause before starting the next transaction.
- **Batch Limit**: The maximum number of full transactions committed during one inventory run. After this limit is reached, the inventory cycle will end.

Note: With batch limiting in place, several runs of the inventory cycle could be required to completely synchronize the inventory. This is especially applicable for the registrations of new InfraStruxure Central servers with many devices. Consider the number of hours configured between inventory cycles, the batch size, and batch limit, and the size of your environment when evaluating how to set these parameters, and when evaluating the behavior of the SPI and the immediacy of changes appearing in OMW. These parameters are designed to limit the impact on OMW at the expense of currency of the inventory.

## Accepting Changes

You may select **Test Connection**, **Save** or **Cancel**. The **Save** button saves the changes but does not commit them to the configuration files until the **Save** button on the main window is clicked.

## *General SPI Options*



Working Files Folder: les\APC\APC ISXC SPI for HP OMW\Config

☑ Enable debug logging for modules.

☑ Normalize message keys projected into HP OMW.

Current Build: 6.2.1457.0

## Working Files Folder

The **Working Files Folder** is where the SPI components will access configuration files. The SPI processes need read and write access to this folder. Even though the configuration utility is used to register InfraStruxure Central servers, each component also uses this folder for any files that may be required for its work. For example, the alarm component uses this folder to store the list of active alarms that have already been projected as messages in OMW. The inventory component uses this folder to store the object map that is used to link InfraStruxure Central inventory to OMW objects.

If you change this folder, the utility will attempt to move the configuration files from the existing folder to the new folder. This will happen immediately after clicking **Save**. If you have made unsaved changes to the configuration, these are unaffected. You will be prompted to save those changes upon exiting the configuration utility, at which point the files would be saved to the new location.

Use this option to move the configuration files to a different location, for example, to a disk managed by a cluster if the SPI services will be moved to a clustered environment.

Notes:

- Ensure no components are currently running before changing this value.
- Do not use a mapped drive. UNC paths will also not function unless the user as which the SPI service is running has the appropriate access to the network resource specified in the UNC path.

## Debug Logging

If **Enable debug logging for modules** is checked, the SPI components will write debug logs to the **Working Files Folder**. It is likely this option will be used at the request of APC Support. Debug logs are always appended to. If this option remains checked for a long period, the debug logs will grow to a significant size, as they are designed to be very verbose. Use this option with caution.

## Normalizing Message Keys

- With this option turned off (unchecked):
    - The message key that will be generated for the message projected into OMW will be unique *for each instance* of any alarm.
    - For example: an alarm reporting a temperature threshold violation for device A, temperature sensor B will generate a unique message key every time the alarm is raised and cleared.
    - OMW will never consider these messages duplicates.
- With this option turned on (checked):
    - The message text for each alarm that is processed from InfraStruxure Central is checked against a set of normalization patterns.
    - If no pattern in the set matches the message text, the alarm is processed just as described above (as if the option was turned off).
    - If a pattern in the set matches the message text, the message key that will be generated for the message projected into OMW will be unique *for the source and pattern* of the alarm.
    - For example:
        - If a pattern is defined that matches “temperature threshold” in the text, the alarm in the previous example will generate a message key that is unique to that pattern and source (“device A, temperature sensor B”).
        - If this alarm later clears and is raised again, the message key for the new message will be the same as the previous message (i.e. *not* unique to the instance, but unique to the source and pattern.) The new message will be considered a duplicate by OMW.
        - If another sensor on device A or a completely different device generates the same alarm, the message key will be unique to the same pattern, but a different device and/or sensor.
    - Because the message key will be unique to the pattern and the source, the normalization functionality is directly affected by the granularity of the source identified in the alarms that come from InfraStruxure Central. InfraStruxure Central, in turn, directly reflects the granularity of alarms that come from the devices it manages.
    - There may be cases where multiple alarms match the same pattern, are from different logical sources, but are not completely differentiated. For example, on a device with multiple fans, a “fan failure” alarm may be identified only by the device from which it comes and not by the specific fan to which it applies. The alarm text may reference the source with additional granularity, but the alarm attributes may not include these details. In such cases, like alarms may be treated as duplicates. This only applies to the

specific type of situation exemplified here. Alarms are always differentiated at least by device.

- The pattern set may be modified to suit your specific needs. See Section 4 for more details.

Note: If you choose to turn message normalization on, you may wish to remove the policy item that automatically acknowledges messages generated when an alarm is no longer active. This will allow OMW operators to see the message sequence in the active message browser, but will require the operators to acknowledge the messages manually. This represents a trade-off, but it is something that should be considered for your installation. See the section describing the default OMW policy set in Section 4 for more information.

### Current Build

The current build is displayed on this screen to provide an indication of the currently installed version and build of the integration.

## *General Information Regarding InfraStruxure Central Integration*

### Device Type Filtering

To control the number of objects that are represented in OMW, each InfraStruxure Central can be configured to handle devices of different types in different ways. There are two levels to this:

1. A particular device type can be selected or deselected for inventory. If a device type is selected for inventory, the objects for that device will be created in OMW. If a device type is not selected for inventory, any child devices of devices of that type will also be omitted, regardless of the setting for their individual type.
2. If a device type is omitted from the inventory, alarms raised for devices of that type (or their child devices or sensors) can be rolled up or discarded. If alarms are rolled-up, sensor alarms will be rolled up to the parent device, device alarms will be rolled up to the parent device, etc., up to and including rolling the alarm up to the InfraStruxure Central itself.

In addition, the handling of default types and newly encountered types is as follows:

1. When an InfraStruxure Central is first registered, settings for specific device types are loaded from an XML file (see Section 4). The standard device types are set to inventory. This file may be reviewed and edited as required.
2. When an InfraStruxure Central is first registered, the default action for new device types is **Do Not Inventory but Roll-Up Alarms**. This means that any new device types encountered during inventory that are not already on the list will be added to the list, but devices of these types will not be projected into OMW as individual objects. Alarms will be rolled-up accordingly, however.

3. If you change the default for an InfraStruxure Central, new device types encountered after that change will be added to the list with the default options, as set at the time they are added. Existing types will remain unchanged (that is, standard types, types subsequently added with the previous default options, and types edited manually).
4. While editing an InfraStruxure Central registration, you may add, remove, and modify the behavior of any existing type.
   Note: If a type is removed and encountered again, it will be re-added with the default options in effect at the time it is encountered again.

## Device Group Ordering

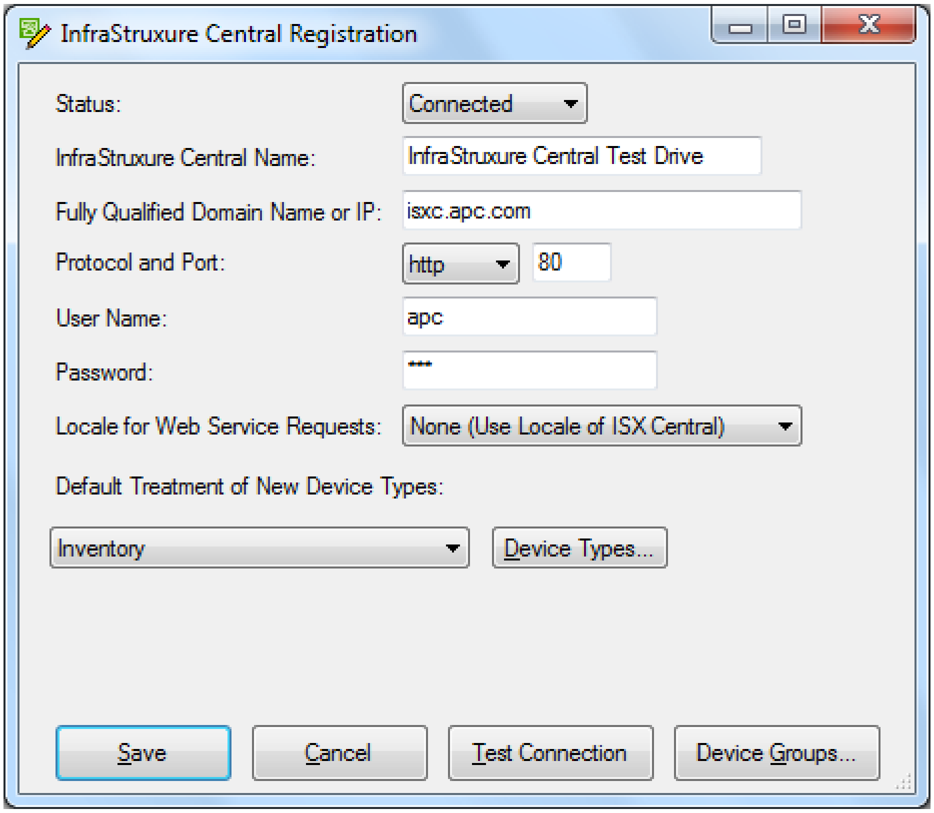
InfraStruxure Central permits a device to be in multiple device groups. OMW allows any given service to be the child of one and only one service. Since device groups and devices are represented as services in OMW, only one of these membership relationships can be represented. By default, device groups are processed in alphabetical order with any nested (child) device groups being considered before the parent. The first device group encountered of which a device is a member will be considered the "primary" device group for that device. The primary device group will be the parent in OMW. No other memberships will be represented for that device.

As soon as a new device group is inventoried, its order is fixed at the time of discovery. This applies to the initial inventory of the InfraStruxure Central server when all device groups are considered new. Any device groups that are discovered on subsequent runs will be processed in the same manner (i.e. in alphabetical order with nested groups considered before parents); however, they will all be appended to the end of the order. This means a group that would naturally be listed before another group, had they been discovered together, will be placed at the end of the order on subsequent discoveries. This is to prevent unintended shuffling of the location of devices in the OMW service tree.

Since these mechanisms may not correctly determine which device groups are of primary importance to your installation, they can be re-ordered manually. When editing a registered InfraStruxure Central server, the discovered ordering of device groups can be altered, ensuring that groups moved up in the order are considered first in determining which group is the primary group for any given device.

The **Device Group Order Management** window is covered in more detail in the next section.

## *Adding or Editing an InfraStruxure Central Registration*



Status: Connected

InfraStruxure Central Name: InfraStruxure Central Test Drive

Fully Qualified Domain Name or IP: isxc.apc.com

Protocol and Port: http 80

User Name: apc

Password: ***

Locale for Web Service Requests: None (Use Locale of ISX Central)

Default Treatment of New Device Types:

Inventory

*Figure 3: The InfraStruxure Central Registration screen.*

### Status

A registered InfraStruxure Central server can be in one of three states:

1. **Connected**: The InfraStruxure Central server will be inventoried and its inventory synchronized with OMW. InfraStruxure Central alarms will be projected into OMW.
2. **Disconnected**: The InfraStruxure Central server will not be inventoried or synchronized. InfraStruxure Central alarms will not be projected. The inventory and alarms already in OMW will be preserved as is.
3. **Removed**: The InfraStruxure Central server will not be inventoried or synchronized. InfraStruxure Central alarms will not be projected. The inventory in OMW will be removed, just as if the registration itself were removed. This option is useful because it preserves the registration configuration, GUID, device types, device group ordering, and InfraStruxure Central-to-OMW mapping configuration.

### InfraStruxure Central Name

This name is for reference only and can be any name chosen by the user.

## Fully Qualified Domain Name of IP

Provide the network information used to connect to the InfraStruxure Central server.

## Protocol and Port

HTTP (unencrypted) or HTTPS (encrypted) communication can be selected for access to this InfraStruxure Central server. The standard ports for HTTP and HTTPS are 80 and 443, respectively. These can be changed to match the InfraStruxure Central server. Note: The protocol and port must match the setup of the InfraStruxure Central.

## User Name and Password

Provide a user name and password that has access to the InfraStruxure Central web services. If a user name is provided that has restricted access to devices, it will function, but will only have visibility into the InfraStruxure Central inventory (i.e. device groups) to which it has access.

## Locale for Web Service Requests

Each web service call can be issued with a desired locale (language). Where possible, responses will be localized to the locale specified. The default is to request responses in the default locale of the InfraStruxure Central server itself.

## Default Treatment of New Device Types

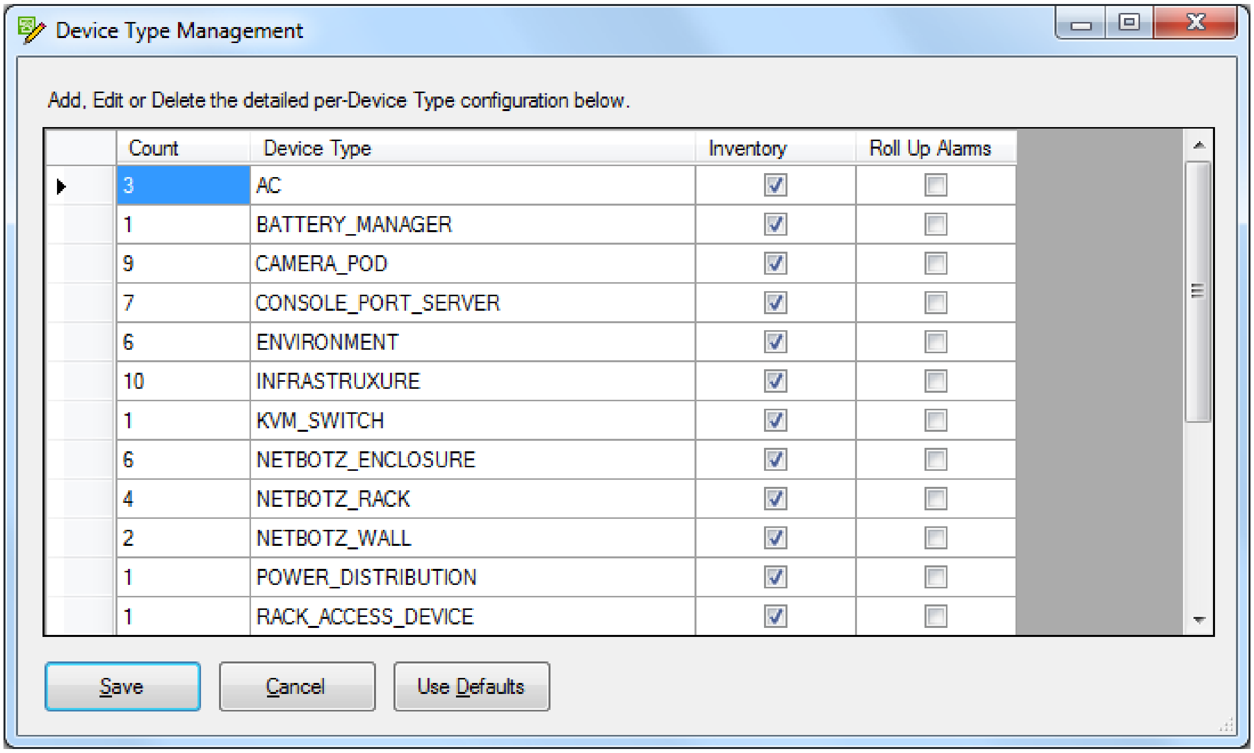
Select the default treatment of newly-encountered device types. See the section titled *General Information Regarding InfraStruxure Central Integration* for more information. The possible treatments are:

- **Do Not Inventory and Discard Alarms**
- **Do Not Inventory but Roll Up Alarms**
- **Inventory**

## Modifying Device Types

Pressing the **Device Types…** button will display the **Device Type Management** window for the selected InfraStruxure Central server.

When an InfraStruxure Central server is first registered, a list of device types for that server is copied from the standard types configuration file (if any). After the first inventory, the list of device types for each InfraStruxure Central server is augmented to include any additional device types present on at least one device in the current inventory, but not currently in the list. These will be added and behave according to the default behavior for new device types configured for that InfraStruxure Central server, as set at the time of that inventory. Individual device types may be edited using these screens thereafter.



Device Type Management

Add, Edit or Delete the detailed per-Device Type configuration below.

| | Count | Device Type | Inventory | Roll Up Alarms |
|---|---|---|---|---|
| ▶ | 3 | AC | ☑ | ☐ |
| | 1 | BATTERY_MANAGER | ☑ | ☐ |
| | 9 | CAMERA_POD | ☑ | ☐ |
| | 7 | CONSOLE_PORT_SERVER | ☑ | ☐ |
| | 6 | ENVIRONMENT | ☑ | ☐ |
| | 10 | INFRASTRUXURE | ☑ | ☐ |
| | 1 | KVM_SWITCH | ☑ | ☐ |
| | 6 | NETBOTZ_ENCLOSURE | ☑ | ☐ |
| | 4 | NETBOTZ_RACK | ☑ | ☐ |
| | 2 | NETBOTZ_WALL | ☑ | ☐ |
| | 1 | POWER_DISTRIBUTION | ☑ | ☐ |
| | 1 | RACK_ACCESS_DEVICE | ☑ | ☐ |

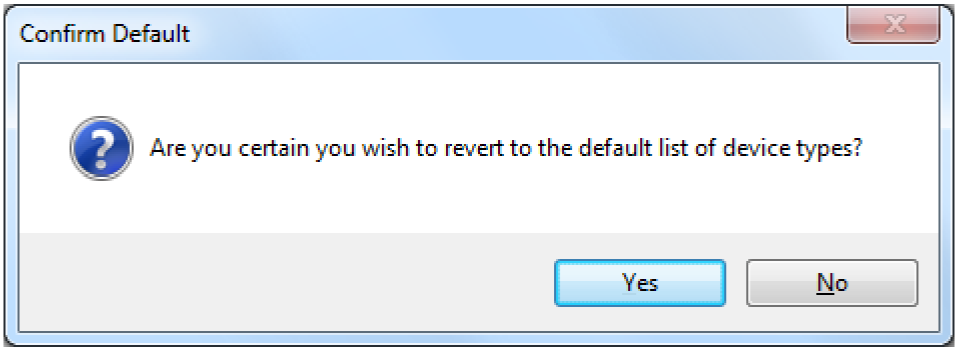
*Figure 4: The Device Type Management window.*

You can edit type names, change the per-type options by checking or un-checking the appropriate column for a given device type, or add a new device type. New device types can be added at the bottom of the list. Blank types are not permitted.

Note only certain combinations of options are meaningful. If **Inventory** is checked, **Roll-Up Alarms** will be cleared automatically. If **Roll-Up Alarms** is checked, **Inventory** will be cleared automatically. Invalid combinations are corrected on save.

The **Count** column is read-only and reflects the number of objects for the given type encountered during the last inventory run. This number is subject to change between runs, but is provided to help scope the number of devices that would be affected by any change to the type definition.

The **Use Defaults** button will clear the current device types list and re-load from the standard types file. Note: During the next inventory run, any device types on in the standard types file will be discovered again and assigned the default behavior, as discussed in the section titled *General Information Regarding InfraStruxure Central Integration*.

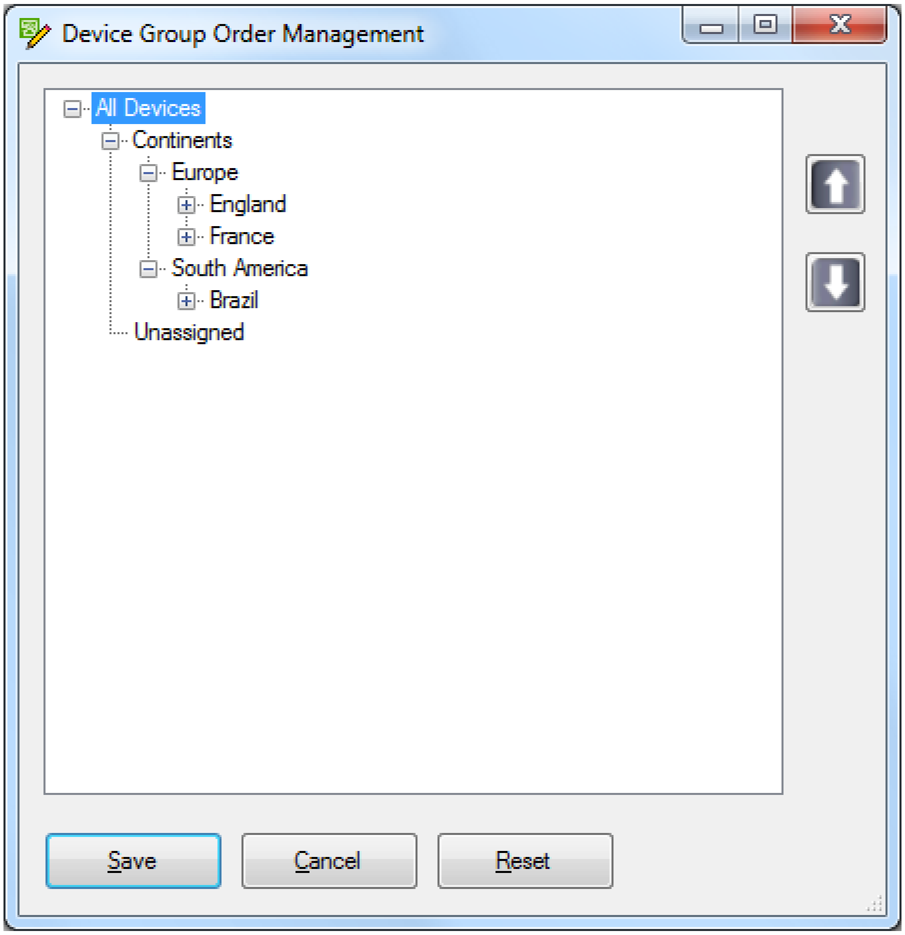


Are you certain you wish to revert to the default list of device types?

## Modifying Device Group Ordering

Clicking **Device Groups…** opens the Device Group Order Management window. To modify device group ordering, select a group, and use the up and down arrows to adjust the device group order. The order can only be changed within its own level of the hierarchy; children can be re-ordered only within parents, which is standard for this type of list.

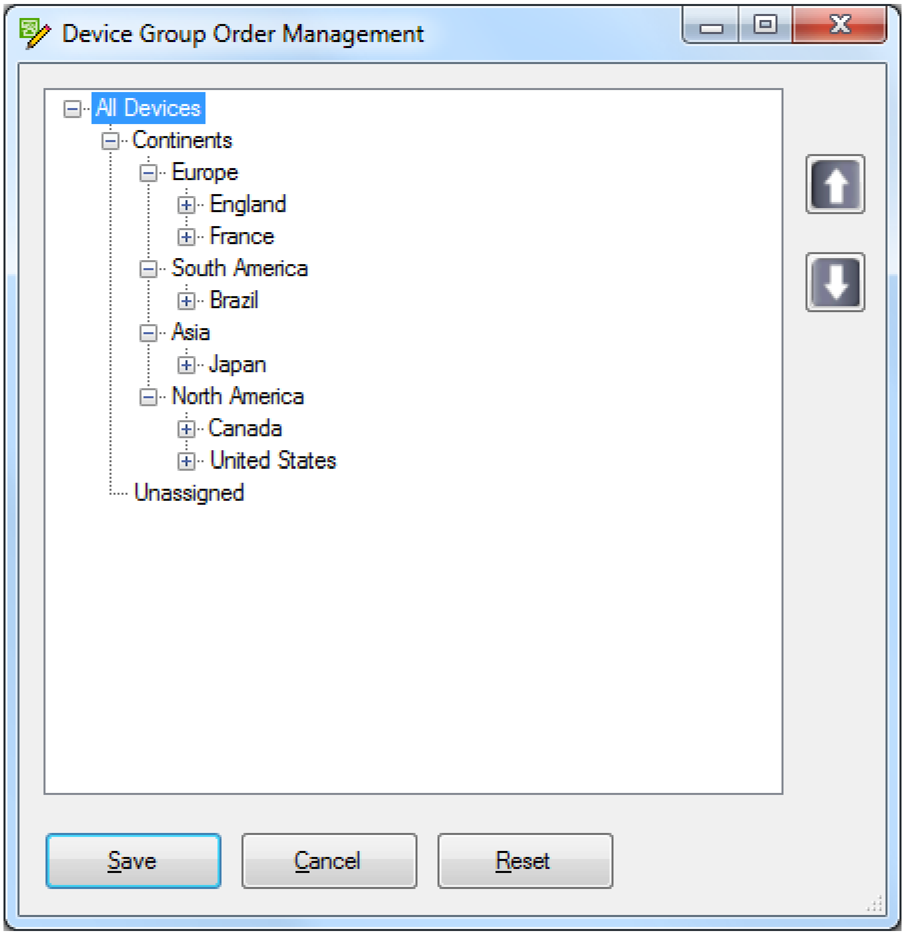
Example 1: The device groups after the initial inventory of an exemplar InfraStruxure Central



The initial inventory has produced a hierarchical list of device groups sorted alphabetically. The primary device group for devices will be chosen in this order.

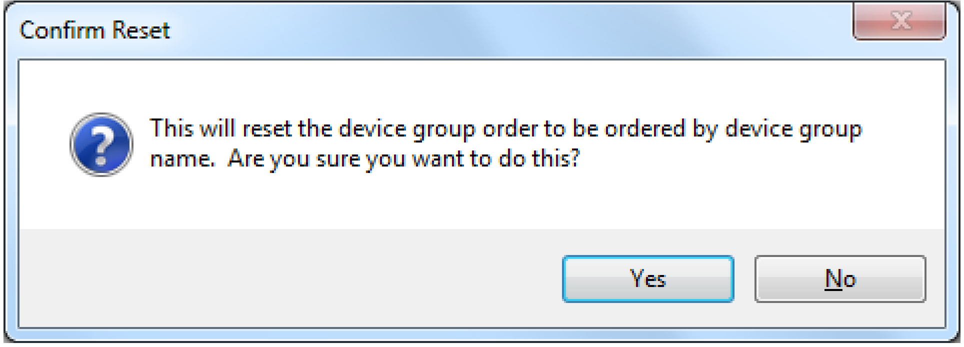
Example 2: The device groups after the second inventory of the same InfraStruxure Central server

Note the new device groups have been added to the hierarchy, and are listed after any previously discovered device groups, regardless of their alphabetical order.



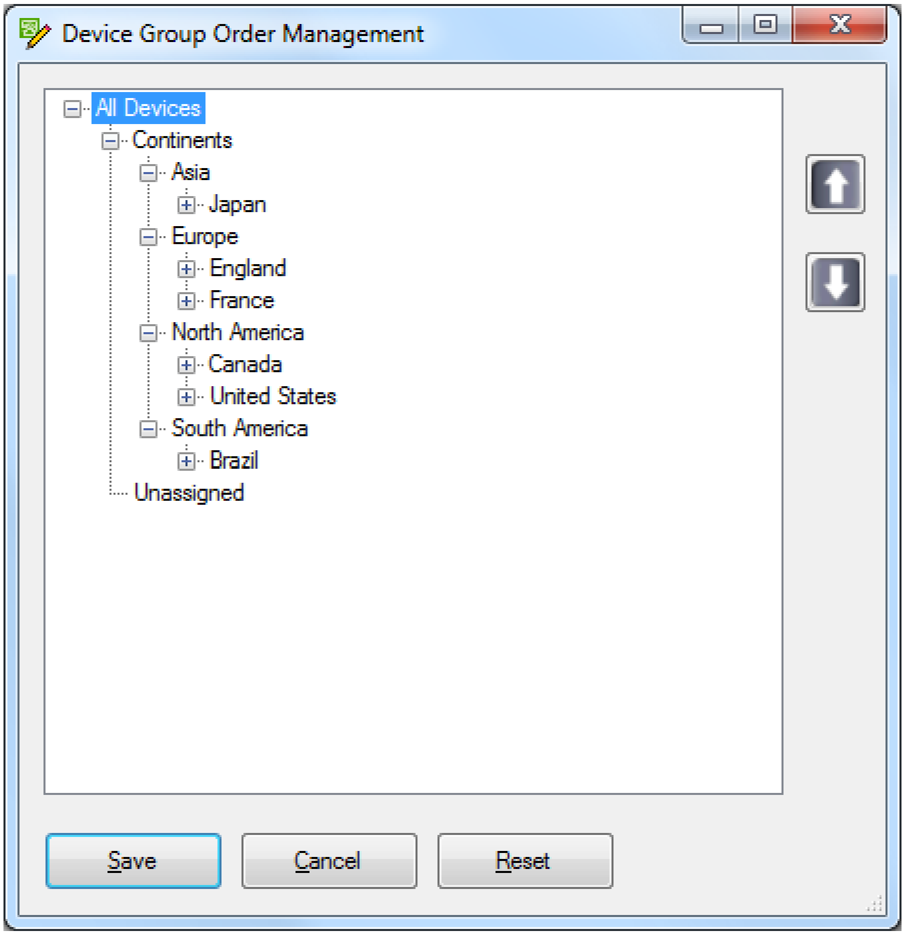
The **Reset** button resets the order to be alphabetical, considering all inventoried groups. This is useful when groups are inventoried over multiple runs and the order becomes fragmented. See the section titled *General Information Regarding InfraStruxure Central Integration* under the subsection titled *Device Group Ordering* for more details on how device groups are added to the order over multiple inventory runs.

The following shows the confirmation you will receive when you click **Reset**:

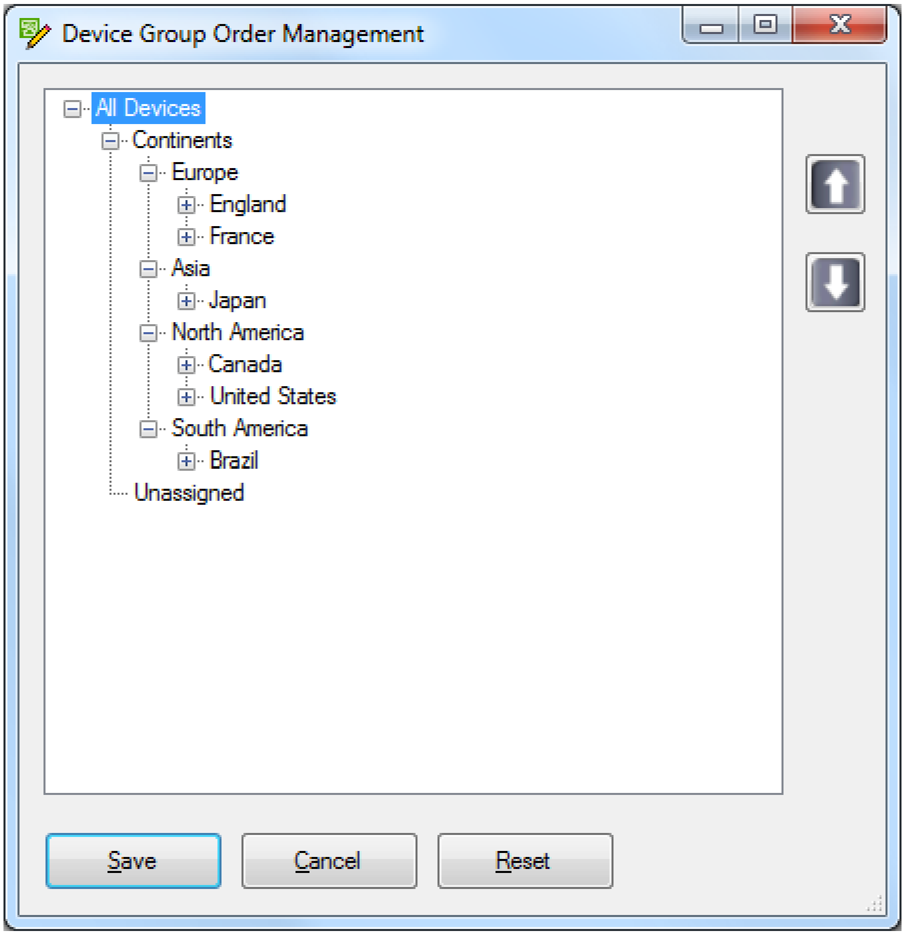


This will reset the device group order to be ordered by device group name. Are you sure you want to do this?

After resetting, the resultant device group hierarchy is as follows:



Finally, if we consider that in a particular infrastructure, the European data center is the central management point for the global infrastructure, we may always wish to consider the European groups as the primary device group for devices. Clicking the Europe node and pressing the up arrow results in the following hierarchy:



Finally, note that promotion and demotion may occur only within the underlying parent/child relationship of the groups. That is, France may be moved above England, but Japan will always be below Asia. Since Asia is below Europe, Japan could not be moved above anything in Europe.

## Testing the Connection

Select this option to test the connection to the InfraStruxure Central server.

## Saving Changes

Click **Save** to save the changes to the InfraStruxure Central. This includes the general settings for the InfraStruxure Central, device types, and device group ordering. This does not commit the changes to the configuration files until the **Save** option on the main configuration window is selected.

# *Advanced Configuration*

## Special Configuration Files

Several configuration files are installed with the SPI and are not modified by the components or the configuration utility.  Certain advanced configuration changes can be made to these files directly.  The following is a description of the files and the reasons you may wish to edit them.  Note: These files are standard XML files.  You should be familiar with editing XML files and ensure that your edits do not break the XML validation rules or the schema of the file.  The schema is implicitly defined by the as-installed contents of the file.  The XML validation rules are more strictly defined and may be validated by opening the modified XML file with any XML-compliant tool, such as Internet Explorer.  If the tool can open the file as a standard XML file, no basic syntax errors have been introduced.  Be sure to examine the original file and your modified version to ensure the schema is also intact.

- Root Objects (InfraStruxure CentralentralConnectorForHPOMW-RootObjects.xml)
    - This file contains the definition of the root node group and service node under which all managed nodes and service nodes for InfraStruxure Central servers, respectively, are created.  If you wish to rename these groups, localize their names, or change the icon for these objects, you may edit this file.
    - This file also contains the definition of the tool group and actions used by the SPI.  If you wish to modify the names, icons, parameters, or object mappings for these actions, you may edit this file.
    - For actions that represent executables, you may embed the token {APCSPI} within the command or the parameters definition.  This will be replaced with the SPI program install location when the action is created or updated during inventory.  The token is replaced with the trailing backslash character (\), so "{APCSPI}SomeProgram.exe" would be correct whereas "{APCSPI}\SomeProgram.exe" would result in a double backslash.  Remember to enclose such references in quotes to account for spaces in the location path.
    - Note that you may add tool groups and/or actions to the list and map them to the object types the SPI handles.  The following targets are valid for actions:
        - **Server**:  The InfraStruxure Central server itself
        - **DevGroup**:  Device groups
        - **DevPriv/SenPriv**:  Devices and sensors on the InfraStruxure Central private network
        - **DevPub/SenPub**:  Devices and sensors on the InfraStruxure Central public network

*For **DevPriv**, **SenPriv**, **DevPub**, and **SenPub**, you may also further restrict the assignment to a particular device or sensor type by appending the type in parenthesis, for example:*
***SenPriv(DEVICE_STATUS)***
***DevPriv(UPS)***

- Standard Types (InfraStruxure CentralentralConnectorForHPOMW-StandardTypes.xml)
  - When a new InfraStruxure Central server is registered, these device and sensor types are listed by default.
  - The **DeviceTypes** group lists device types by name.  It is assumed that these will be inventoried, which implies that the alarms will not be rolled up.
  - The **SensorTypes** group lists sensor types by name.  It is assumed that these will be inventoried, which also implies that the alarms will not be rolled up.  Each type has an attribute to determine whether data will be collected for this type or not.
  - It is assumed unlisted types will follow the default for the InfraStruxure Central, defined in the main configuration file.

- Type Icons (InfraStruxure CentralentralConnectorForHPOMW-TypeIcons.xml)
  - This file maps the appropriate icon file to each type.
  - The **BaseTypeIcons** section contains only two entries and maps the icon files for InfraStruxure Central server and device group service nodes.
  - The **DeviceTypeIcons** section maps the icon file for each device type.  The last entry, "*", applies to any unlisted device type encountered.
  - The **SensorTypeIcons** section maps the icon file for each sensor type.  The last entry, "*", applies to any unlisted sensor type encountered.

- Normalization Regular Expressions (InfraStruxure CentralentralConnectorForHPOMW-NormRegEx.xml)
  - This file contains the list of patterns used for alarm normalization.
  - These patterns should be written as standard regular expressions.
  - The patterns are processed in the order they are listed.
  - For this reason, though not technically required, it is recommended that patterns be ordered by length, with the longer patterns appearing first in the file.

## Advanced Scheduling

- The Services Controller included with the SPI uses a simple scheduling algorithm to run the various components. It essentially uses the last run time and a run interval setting to schedule the executables.
- For more advanced scheduling such as multiple schedules or day of week exclusions, the individual executables may be scheduled using the Windows Task Scheduler.
- In this case, you may stop and disable the Services Controller and schedule the individual executables manually.
- The only two executables that need to be scheduled are:
  - The alarms executable. Run this as often as you want active or inactive alarms to be projected into OMW as messages.
  - The inventory executable. Run this as often as you want changes to the InfraStruxure Central inventory to be projected into OMW.
- No parameters are required for these executables, but you may optionally specify “-debug” as a command line parameter, which is essentially the parameter the Services Controller uses when that option is turned on in the configuration. The same warning regarding the size of the debug logs applies.
- The executables may also be run from the command line or Windows Explorer.

# Section 4: Operational Considerations

## *The Central Role of the Inventory Component*

The Inventory Component is central to the operation of the SPI.

- It synchronizes the inventory between InfraStruxure Central and OMW.
  - It creates the root node group, service nodes, tools, and actions.
  - It creates the managed nodes and service nodes for each registered InfraStruxure Central server.
  - It creates the service nodes for each InfraStruxure Central server's device groups and devices.
  - It ensures the inventory stays up-to-date by processing new inventory; updating inventory that may have changed, such as captions, descriptions, and icons; and by deleting inventory from OMW that is no longer present in the InfraStruxure Central inventory.
- It updates configuration information that may be further customized using the configuration utility.
  - It augments the device type list with any newly-encountered device types. New entries are added using the configured defaults.
  - It augments the device group list with any newly-encountered device groups.
- It collects information required by the other components.
  - It calculates the proper target for alarms generated by sensors and devices, considering device types that are configured for alarm discard and/or alarm roll up. This is required by the alarm integration component.
  - It determines the mapping between devices in the InfraStruxure Central inventory and managed nodes and service nodes in the OMW inventory. This is required by the alarm integration component.

Because of these functions, consider the following sequence of events that illustrate the central role of the inventory component:

- An InfraStruxure Central server is registered. Only the standard device types are listed.
- The inventory runs for the first time and performs all of the actions discussed above.
- The configuration utility is run to make the following changes:
  - Certain new device types should be inventoried, but they were added with the default of **Do Not Inventory and Discard Alarms**.

  - Certain other new device types should not be inventoried, but you would like their alarms to be rolled-up to their parent.
  - You use the **Device Type Management** window to ensure the desired types are set to inventory or roll up, as required.
  - Some determinations regarding the primary device group for certain devices are not correct, and you would like to adjust the order in which device groups are considered.
  - You use the **Device Group Order Management** window to adjust the order.
- You open the OMW console, but the device group assignments are the same.
- The alarm component runs, but messages are not being generated for active alarms for the new device types. In addition, active alarms are still being generated for devices whose types are now set to roll up.
- After you run the inventory component again, all of these changes are implemented and the alarm component begins to behave as expected. This is because the OMW inventory is now synchronized, including the updated device type parameters and the new device group ordering; the alarm targets have been recalculated per the modified inventory and roll-up parameters; and the mapping has been updated to include the new devices and sensors, which is used by the alarm component.

The general rule is that the inventory component must run to fully implement configuration changes.

## *Important Note on Requirement of Multiple Inventory Runs*

Some conditions may cause the inventory module to need two or more runs to complete the synchronization between InfraStruxure Central and OMW. This includes (but is not limited to):

- If you make changes that significantly alter the structure of the InfraStruxure Central device group hierarchy.
- If you change between InfraStruxure Central user accounts that have access to different groups within InfraStruxure Central
- If you make other such changes that will require the inventory component to replace objects (which amount to “remove” and “add”). At least two runs will be required because object removal will be initiated by the inventory component, but completed by OMW server itself asynchronously. On the second run, the inventory component may process the “add” phase of the replacement.
- If the inventory integration component needs to make more changes than the transaction batch size and batch limit allow (configured in the **HP OMW Connection Information** window of the configuration utility).

If any of these conditions are true, the inventory component may need to be run more than once to complete all changes.  It is advisable to check the OMW console after the inventory run for (a) a correct reflection of the InfraStruxure Central inventory, or (b) any warning from the inventory module regarding duplicate objects encountered, indicating the "add" phase could not be completed immediately due to pending asynchronous "removes" by the OMW server, or because the transaction batch limit was reached.

## *Events Generated by SPI Components (Windows Application Event Log)*

**Event Source: ApcIsxcSpiInventory**

| Severity | Event Number | Text Template |
|---|---|---|
| Info | 1002 | The inventory engine has committed {0} change(s) to HP OMW. This is transaction #{1} for this run. |
| Warn | 2000 | Exception encountered in inventory module: {0} |
| Warn | 2001 | (PerformCentralInventory: {0}) Encountered exception while performing Central inventory: {1} |
| Warn | 2002 | (InventoryDevices: {0}) Encountered exception while performing inventory of devices: {1} |
| Warn | 2003 | (InventorySensors: {0}, {1}) Encountered exception while performing inventory of sensors: {2} |
| Warn | 2004 | (InventoryDeviceGroups: {0}) Encountered exception while performing inventory of device groups: {1} |
| Warn | 2005 | InventoryDeviceGroupMembers: {0}, {1}) Encountered exception while performing inventory of device group members: {2} |
| Warn | 2006 | Encountered exception while creating OV_ManagedNode and OV_Service instances for ISX Central {0} in HP OMW: {1} |
| Warn | 2007 | Encountered exception while creating OV_Service instance for Device Group {0} in HP OMW: {1} |
| Warn | 2008 | Encountered exception while creating OV_Service instance for Device {0} in HP OMW: {1} |
| Warn | 2009 | Encountered exception while creating OV_Service instance for Sensor {0} in HP OMW: {1} |
| Warn | 2010 | The transaction batch limit ({0}) for changes to HP OMW has been reached.  The synchronization has not been completed, but the inventory engine will stop until the next scheduled run.  It may be run sooner by managing the next run time using the configuration tool. |
| Warn | 2011 | Device {0} ({1}) has no primary device group, but neither the unassigned nor root device group could be found. |

|  |  |  |
|---|---|---|
| Warn | 2012 | The inventory for {0} has been aborted due to an error that was encountered.  Details of the error may be found in the event that was logged previously. |
| Warn | 20001 | (SoapRequest1: {0}, {1}) Encountered exception trying to connect to the web service: {2}, XML: {3} |

**Event Source: ApcIsxcSpiAlarms**

| Severity | Event Number | Text Template |
|---|---|---|
| Info | 1002 | Initiated {0} new message(s) for ISX Central {1}. |
| Info | 1003 | Acknowledged {0} message(s) for ISX Central {1}. |
| Warn | 2010 | Encountered an exception processing alarms for ISX Central {0}: {1} |
| Warn | 2011 | Encountered an exception processing alarms: {0} |
| Warn | 20001 | (SoapRequest1: {0}, {1}) Encountered exception trying to connect to the web service: {2}, XML: {3} |

**Event Source: ApcIsxcSpiDeviceInfo**

| Severity | Event Number | Text Template |
|---|---|---|
| Warn | 20001 | (SoapRequest1: {0}, {1}) Encountered exception trying to connect to the web service: {2}, XML: {3} |

**Event Source: ApcIsxcSpiService**

| Severity | Event Number | Text Template |
|---|---|---|
| Info | 1011 | The Services Controller has received the START command. |
| Info | 1012 | The Services Controller has completed processing the START command. |
| Info | 1021 | The Services Controller has received the STOP command. |
| Info | 1022 | The Services Controller has completed processing the STOP command. |
| Info | 1031 | The Services Controller scheduler thread has started. |
| Info | 1032 | The Services Controller scheduler thread is exiting. |
| Info | 1033 | The Services Controller scheduler thread current directory is {0}. |
| Info | 1034 | The Services Controller scheduler thread is sending the Services Controller a STOP command. |
| Info | 1035 | Requesting exit of all running processes... |
| Info | 1036 | Initial run configuration: Inventory Every {0} Hour(s), Next Run UTC {1}; Alarms Every {2} Minute(s), Next Run UTC {3}; Data Every {4} Minute(s), Next Run UTC {5}" |

| | | |
|---|---|---|
| Info | 1037 | The Services Controller scheduler thread will run components from {0}. |
| Warn | 2031 | There is no configuration set.  The Services Controller scheduler thread will not perform any actions until the configuration is set. |
| Warn | 2032 | The Services Controller scheduler thread encountered an exception: {0}. |
| Info | 1041 | Starting Inventory Process [{0}]; Next Run UTC {1} |
| Info | 1042 | Starting Alarms Process [{0}]; Next Run UTC {1} |
| Info | 1043 | Starting Data Process [{0}]; Next Run UTC {1} |
| Info | 1051 | Inventory Process has ended.  Run time: {0} second(s). |
| Info | 1052 | Alarms Process has ended.  Run time: {0} second(s). |
| Info | 1052 | Data Process has ended.  Run time: {0} second(s). |
| Warn | 2061 | Inventory Process was scheduled to run but is already running; Next Run {0} |
| Warn | 2062 | Alarms Process was scheduled to run but is already running; Next Run {0} |
| Warn | 2063 | Data Process was scheduled to run but is already running; Next Run {0}, NextRunData |

### Default OMW Policy Set

The default OMW policy set is divided into three policies:

- A message policy that matches messages for (a) active alarms that are critical, warning, informational, or of unknown severity; and (b) alarms that are no longer active.  This policy:
    - Maps the message option variables to custom message attributes (CMAs).
    - Map the message object to the message key for correlation and duplicate processing.
    - Forwards critical and warning messages to the active message browser.
    - Forwards normal messages and messages of any other severity to the acknowledged message browser.
    - Forwards messages for alarms that are no longer active to the acknowledged message browser.  This policy item will also automatically acknowledge the original message sent when the alarm became active.
- An event log policy that forwards warning and critical messages from the SPI components themselves to the active message browser.
- A service policy that monitors the state of the Services Controller and generates a message if the service stops.

## *The Registry Preparation Tool*

A registry preparation tools installs with the SPI programs on the management server.

- This is especially required if the Services Controller and associated engines do not run as an administrator, as you will need to prepare the registry to allow the service account to access the appropriate key (referring to the "init" option).
- This tool is also useful to initialize, back up, and restore the cryptographic keys used by the SPI. These keys are used to encrypt user names and passwords in the configuration files.

The following examples show the command line options of this tool. Running the tool with no arguments also shows a help screen that describes these options.

```
Usage:
      RegistryTool [command] [arguments]

Examples:
      RegistryTool init
            Initialize the cryptographic keys in the registry.

      RegistryTool backup [<keyfile>]
            Backup the cryptographic key to the specified file
            (defaults to ApcIsxcSpiForHpOmwKeys.bin).

      RegistryTool restore <keyfile>
            Restore the cryptographic key from the specified file
            (defaults to ApcIsxcSpiForHpOmwKeys.bin).

      RegistryTool allow <username@domain>
      (or) RegistryTool allow <domain\\username>
            Allow the specified user "change" access to the
            registry key required by the SPI.
```

## *Tools and Actions Implemented in OWM*

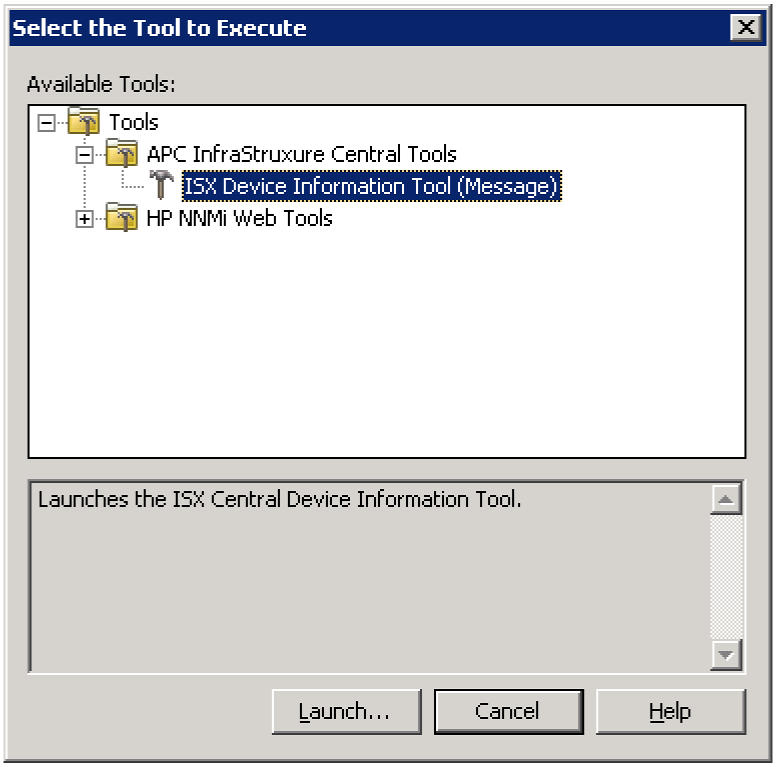
The SPI integrates four tools in OMW. Images of the appearance of these tools are given below. The four tools are:

- **Launch ISX Central**. From a managed node or service, this tool will launch the InfraStruxure Central client, provided the client was installed, and was identified when the client integration components were installed. This tool automatically populates the name of the InfraStruxure Central server when it launches the client. The password must still be entered.
- **Launch Device Console**. From a service that represents a device in InfraStruxure Central, this tool will launch a web browser to the device itself. Note two properties of this tool:
    - First, this tool cannot determine whether a device has a web console available. If the device does not support a web console, the web browser will launch and will behave exactly as it would if handling any other nonexistent web site.
    - Second, this tool has two variants: a public and a private.

    - The difference is the URL formed to access the device console.
    - The InfraStruxure Central server can manage devices on its “public” LAN (i.e. the LAN shared with the rest of the infrastructure) and on its own “private” LAN (i.e. the LAN that is only shared between the InfraStruxure Central server and the devices it manages, if you have so structured your infrastructure).
    - The “public” variant of this tool launches a web browser to the IP or host name of the device directly. It is assumed since it is on the “public” LAN, the workstation on which the browser is launched can access it directly.
    - The “private” variant of this tool launches a web browser to the InfraStruxure Central server itself using a URL specially constructed to direct the InfraStruxure Central to proxy the web requests through to the appropriate device on its “private” LAN.
    - When launching the “public” variant of this tool, you will be prompted to log into the device through whatever mechanism the device’s web interface requires.
    - When launching the “private” variant of this tool, you will be prompted to log into the InfraStruxure Central first (authenticating to the proxy) and will then be (by proxy) connected to the device itself. At that point, you will be prompted to log into the device through whatever mechanism the device’s web interface requires. This will usually result in two logins to access a device on the “private” LAN.
- **Launch Device Information Tool**. This launches a tool that runs on the management server that collects information about the specified device and its sensors. The information output by this tool is captured for review by the operator. This tool has two variants: one that runs against messages and one that runs against services. The only difference is the manner in which the parameters are supplied, since services and messages have different properties in which the information required by the tool is stored.

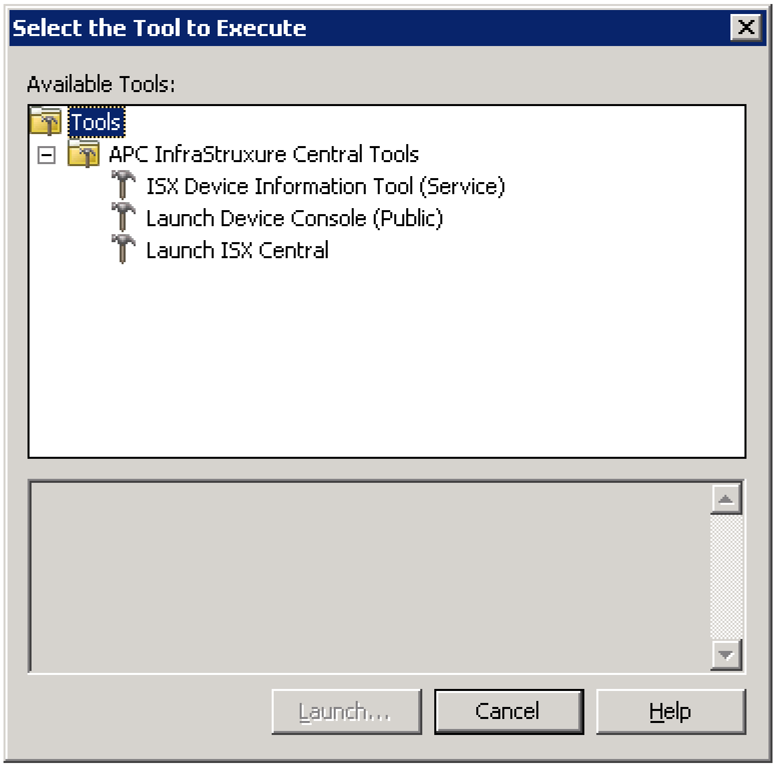
The following images show the appearance of the tools in the OMW tool context menu:

## OMW Tools for a Message


Select the Tool to Execute
Available Tools:
Tools
APC InfraStruxure Central Tools
ISX Device Information Tool (Message)
HP NNMi Web Tools
Launch...
Cancel
Help

Launches the ISX Central Device Information Tool.

## OMW Tools for a Service or Managed Node



Select the Tool to Execute

Available Tools:

- Tools
  - APC InfraStruxure Central Tools
    - ISX Device Information Tool (Service)
    - Launch Device Console (Public)
    - Launch ISX Central