



## **Xcalibur W Administration Guide**

**September 2013  
Document version 1.0**

## Document Information

### People Involved in the Preparation of this document

Function	Name
<i>Chip PC France Technical Manager</i>	Romain DUCHENE

### Review List

Reviewed by	Date

### Change History

Version	Date	Revision Description
1.0	September 2013	Initial version.

# Table of Contents

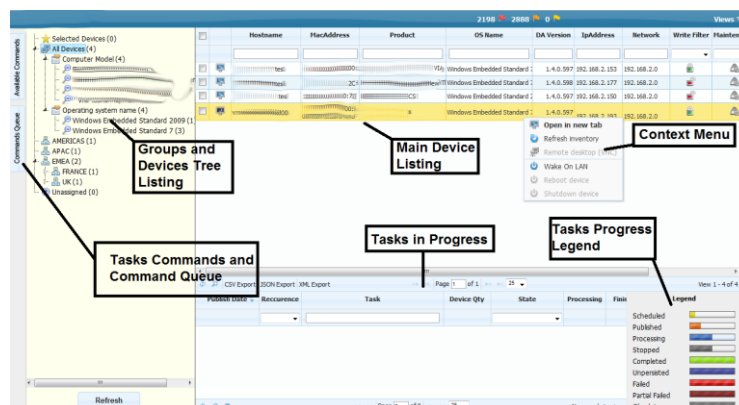
1	Main concepts .....	5
1.1	Main Screen.....	5
1.2	Main devices Listing .....	5
1.3	Context Menu .....	5
1.4	Task List and Progress Legend.....	6
1.4.1	Task Progress Legend.....	7
1.4.2	Task Commands & Command Queue .....	7
1.5	Groups and Devices Tree Listing .....	8
2	Enrolling Client Devices .....	9
2.1	Client Access Licenses.....	9
2.1.1	Applicable Licenses types .....	9
2.1.2	Registering New Client Licenses.....	9
2.2	Discovering New Clients.....	10
2.2.1	Automatic Discovery over the Network.....	10
2.2.2	Manually Configure the Client.....	11
2.2.3	DHCP-Provided Server Address .....	13
2.3	Enrolling Client Devices.....	19
2.3.1	Manual Enrollement .....	19
2.3.2	Automatic Enrollement.....	20
3	Manage Devices.....	22
3.1	Groups and Device Grouping .....	22
3.1.1	Default Groups .....	22
3.1.2	Static and Automatic Groups .....	22
3.1.3	Use TAGs for custom Grouping.....	24
3.1.4	Filtering and Searching Devices .....	26
3.2	Single Device View .....	26
3.3	Tasks and Creating Tasks.....	27
3.3.1	Available Commands Tab.....	28
3.3.2	Command Queue .....	28
3.4	Publishing Tasks .....	29
3.4.1	Scheduling .....	29
3.4.2	Recurrency.....	30
3.4.3	Progress Legend.....	30
3.5	Tasks and Commands Board.....	30
3.5.1	Task Level View .....	30
3.5.2	Command View .....	31
4	Commands Glossary.....	33

4.1	Commands to Multiple Devices.....	33
4.1.1	Toolbox .....	33
4.1.2	Monitor .....	33
4.1.3	Interact .....	34
4.1.4	Agent Administration.....	36
4.1.5	Device Security .....	39
4.1.6	Device Configuration.....	43
4.1.7	User Experience .....	46
4.1.8	Image Management .....	46
4.2	Commands to Single Device .....	48
4.2.1	Monitor .....	48
4.2.2	Apps Configuration .....	50
4.2.3	User Experience .....	51

# 1 Main concepts

## 1.1 Main Screen

Once you have logged in you will see the main Xcalibur-W Server window, the Device List as we will refer to it from now on.



The Device List window has several sections to it and these are detailed below starting in a clockwise manner beginning at the top:

- Main Device Listing
- Context Menu
- Groups and Devices Tree Listing
- Task Commands and Command Queue
- Tasks Progress Legend

## 1.2 Main devices Listing

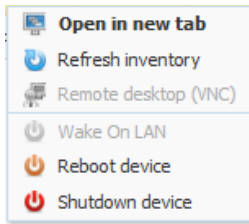
This is the main area where you can view the devices currently controlled by Xcalibur-W Server. Depending on the device tree level that you have clicked, you will find the appropriate devices listed in the Main Devices Listing.

	Hostname	MacAddress	Product	OS Name	DA Version	IpAddress	Network	Write Filter	Maintenance	Last Check In
<input type="checkbox"/>	test	00:0C:29:00:00:00	Windows Embedded Standard 7	Windows Embedded Standard 7	1.4.0.597	192.168.2.153	192.168.2.0			6/18/2013 12:17:06 PM
<input type="checkbox"/>	test	00:0C:29:00:00:00	Windows Embedded Standard 7	Windows Embedded Standard 7	1.4.0.598	192.168.2.177	192.168.2.0			6/18/2013 12:16:48 PM
<input type="checkbox"/>	test	00:0C:29:00:00:00	Windows Embedded Standard 7	Windows Embedded Standard 7	1.4.0.597	192.168.2.150	192.168.2.0			6/18/2013 12:16:57 PM
<input type="checkbox"/>	test	00:0C:29:00:00:00	Windows Embedded Standard 7	Windows Embedded Standard 7	1.4.0.597	192.168.2.193	192.168.2.0			6/17/2013 8:55:58 AM

You will also note that the listing comprises various columns and these may be sorted in ascending or descending order. There is also a checkbox on the leftmost column provided for selection of single or multiple devices for the purpose of task deployment.

## 1.3 Context Menu

If you should right click on a device listing you will be presented with a device Context Menu that allows you to perform various tasks on that particular device.



### **Open in New Tab**

This opens a new browser tab within which you can examine the current settings of the device. You can also change settings from within this configuration section.

### **Refresh Inventory**

Selecting this option will instruct the device agent to upload its inventory to the Xcalibur-W Server. An inventory essentially comprises of all the settings and configurations that are stored within the Xcalibur-W Server

### **Remote Desktop (RVNC)**

On occasions you will wish to connect and shadow a device. Selecting this option will open a new RVNC window. Please see later in this user guide for details of how RVNC works.

### **Wake On Lan**

This option, when selected will send a Magic Packet specifically for this device instructing it to wake up to take instructions.

### **Reboot Device**

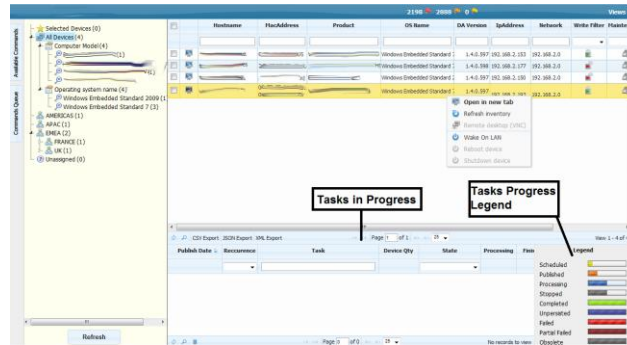
As the title suggests, this option will cause the device to reboot.

### **Shutdown Device**

Using this option you can remotely shutdown the device, or multiple devices.

## **1.4 Task List and Progress Legend**

---



### 1.4.1 Task Progress Legend

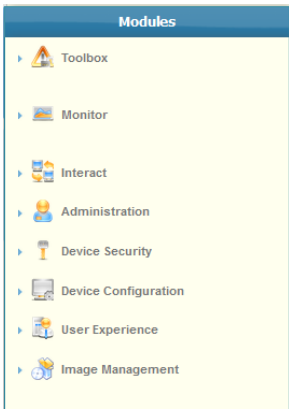
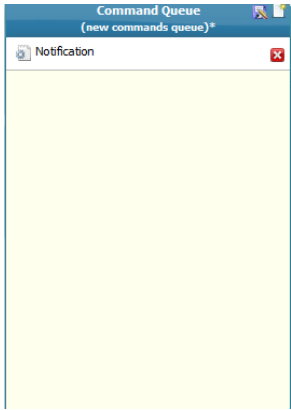
The task progress legend pictured on the right of the picture above is a reference indicator to show what progress the task has reached. This is extremely useful when you are sending tasks down to devices and need to know if they have completed.

All Xcalibur-W Server agents are bi-directional and report back the progress of any task that has been sent to them. The task progress list itself will show each individual task that has been sent down to the various devices and indicate what stage each task is at.

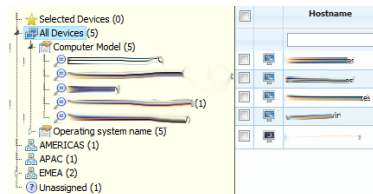
Scheduled		Task is planned but not yet published ; the start date is later than now
Published		Task is published ; the start date is over but no agent has collected the task yet
Processing		Task is processing ; at least one agent did collect the task
Stopped		Task has been stopped ; no more agent will collect the task anymore
Completed		Task is over ; all agents did execute the task without any error
Unpersisted		Task is over ; all agents did execute the task without any error but the Write Filter was not deactivated
Failed		Task has failed ; at least one error occurred
Partial Failed		Task has failed ; at least one error occurred but the Write Filter was not deactivated
Obsolete		Task is over ; the End date is over

### 1.4.2 Task Commands & Command Queue



This section consists of two vertical tabs that allow you to configure commands and add them to the Command Queue. This is detailed in further depth in the section: Tasks and Creating Tasks.

Task Commands	Command Queue
	

## 1.5 Groups and Devices Tree Listing



In order to manage your devices in a structured fashion, Xcalibur-W Server provides the ability to construct groups, both logical and automatic. You can move devices into logical groups

(aka  Static Groups) using drag and drop, while dynamic groups (aka  Automatic Groups) are created using data based logic.



Note that a Device can only belong to one Static Group while same Device can belong to several Automatic Groups



## 2 Enrolling Client Devices

### 2.1 Client Access Licenses


#### 2.1.1 Applicable Licenses types

Xcalibur-W Server uses Client Access Licenses to manage Devices. License Management section is available within the Discovery and Enrollment page.

The screenshot shows the 'Discovery and Enrollment' page with a sidebar on the left containing 'Discovery' and 'Device Enrollment'. The main content area is titled 'License Grants' and shows details for 'DEMO\_WFR\_LICENSES'. It includes fields for 'Name', 'Total number of seats' (5), 'Number of used seats' (3), and 'Number of available seats' (2). Below this is an 'Add License' section with 'Name' and 'License Key' input fields and a 'Submit' button. At the bottom, there is a table with columns: 'License Key', 'Type of License', 'Total seat', and 'Date'. One row is visible with the license key '4250820711', type 'Thin Client', total seat '5', and date '6/6/2013 9:52:10 AM'.

License Key	Type of License	Total seat	Date
4250820711	Thin Client	5	6/6/2013 9:52:10 AM

A Client Access License is defined by:

License Key Number	10-Digit Number
Type of Licenses	Version of the Softw are granted by the License Key. The Type of License can restrain to certain class of Client Devices and can exclude the use of extra fonctionnalities (Ex: Monitoring etc)
Number of Seats	Maximum number of devices that can be enrolled by on the server
 By definition, Client Access Licenses are Transferable Licenses. Therefore, Administrator can un-enroll an Out-Of-Service device in order to use its license on a replacement device.	

#### 2.1.2 Registering New Client Licenses

Licenses are entered onto Xcalibur-W Server using the Submit button of the License section of Discovery & Enrollment page.

License Grants	
Name	DEMO_NFR_LICENSES
Total number of seats	5
Number of used seats	3
Number of available seats	2

Add License  
Name   
License Key

License Key	Type of License	Total seat	Date
4250820711	Thin Client	5	6/6/2013 9:52:10 AM

Once entered, the server will displayed the total number of Client Access Licenses granted by the Keys (aka Seats), the number of Licenses already used and the remaining available Licenses.

## 2.2 Discovering New Clients

### 2.2.1 Automatic Discovery over the Network

Xcalibur-W Server employs a methodology of discovery and enrollment to register and make devices available for management by Xcalibur-W Server. This process can be automated as well as be handled using manual intervention – which one you decide to use will depend mainly on your security policies.

The Discovery is mainly used in LAN Environments. It enables to send packets onto the network so as to identify Devices that have the Xcalibur-W Device Agent installed.

From the **Discovery / Enrollement** section, you can access to **Discovery** page as follows

**Discovery and Enrollement**  
Licensess  
Discovery  
Device Enrollment

**Current Discover**  
Number of devices detected 6  
Number of devices enrolled 4

Settings  
Auto Enroll at first discovery ☐  
Enrollement port 9999

Discover  
☒ by Broadcast  
☐ by Network address  

from   
to   
☐ by Address/Hostname  
Host

The **Enrollement port** is by default set to TCP 9999. This the listening port for the devices.

Settings  
Auto Enroll at first discovery ☐  
Enrollement port 9999

The Discovery supports the following methods:

- **Broadcasting**

Discover

☒ by Broadcast

- **IP Scan**

☒ by Network address

from  
to

- **Direct Device contact**

☐ by Address/Hostname

Host

The Discovery may takes some seconds before returning results. Once done, you will be automatically directed to the **Device Enrollment** page. All the Devices newly discovered are added to the device list in **Not Enrolled** state.

	Hostname	MacAddress	Product	DA Version	IpAddress	Network	First Discovery	Last Check In	State
				1.4.0.597	192.168.2.153	192.168.2.0	6/14/2013 10:27:57 PM	6/18/2013 3:07:42 PM	Enrolled
			C/S	1.4.0.598	192.168.2.177	192.168.2.0	6/14/2013 10:31:21 PM	6/18/2013 3:07:51 PM	Enrolled
		00:10:00:08		1.3.2.516	192.168.204.1	192.168.204.0	6/15/2013 2:15:59 PM	6/17/2013 2:19:27 PM	Not Enrolled
		10:10:00:08		1.4.0.597	192.168.2.150	192.168.2.0	6/14/2013 10:06:17 PM	6/18/2013 3:07:31 PM	Enrolled
		00:10:00:08		1.3.11.594	192.168.2.166	192.168.2.0	6/17/2013 9:24:13 AM	6/18/2013 3:07:47 PM	Not Enrolled
				1.4.0.597	192.168.2.193	192.168.2.0	6/14/2013 10:20:14 PM	6/17/2013 8:55:58 AM	Enrolled

## 2.2.2 Manually Configure the Client

Xcalibur-W Device Agent can be manually configured to connect to its Management Server. By opening up the Web Interface, you can access the Agent Configuration in the Administration menu.

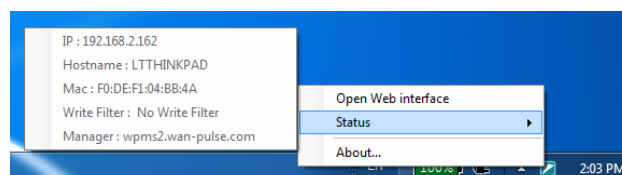
When not enrolled, the **Manager Handler URL** is set to <http://localhost>. By entering the IP Address or URL of the Management Server, the Agent will then connect and register onto Xcalibur-W Server. A reboot will be needed to complete the operation.



The Address shall be provided in HTTP mode if there is no local SSL certificate installed on the unit prior. Once the Device is enrolled by Xcalibur-W Server, then the SSL certificate will be downloaded from the Server to the Client and the communication will turn automatically to HTTPS

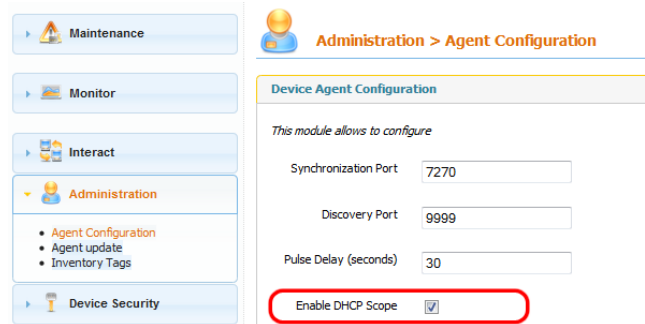
If you wish to set the Manager Address to HTTPS, you can use the SSL Certificate upload module to store the certificate locally on the Client Device.

Once the Agent is configured with a Manager Address, then the Address can be checked within the Agent Tray in the Windows Task Bar such as shown below.



## 2.2.3 DHCP-Provided Server Address

Xcalibur-W Device Agent can use DHCP as a mean of automatically obtaining the IP Address or URL of its Management Server. For that purpose, the option Enable DHCP Scope Option shall be activated as shown below.



There are three different data that can be provisioned by the DHCP server:

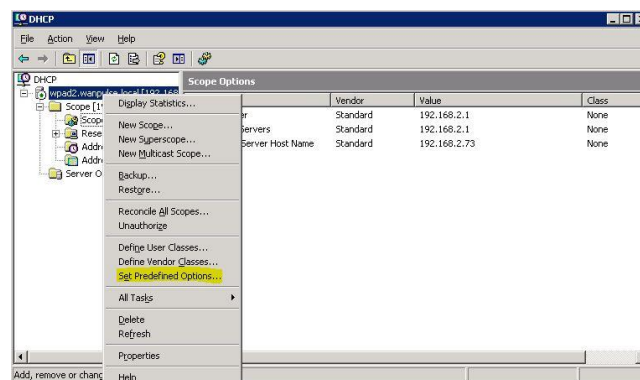
Description	Option Number
FTP Server settings for the Agent Update	Scope Option 230
Agent TAGs	Scope Option 231
Xcalibur-W Server Manager Address	Scope Option 232

Depending of you DHCP server type, you will need to use instructions in the following sections

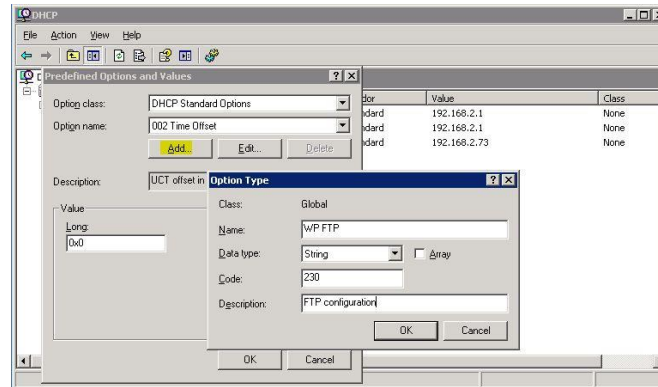
### 2.2.3.1 DHCP Options settings for Windows

#### 2.2.3.1.1 DHCP settings - Add options

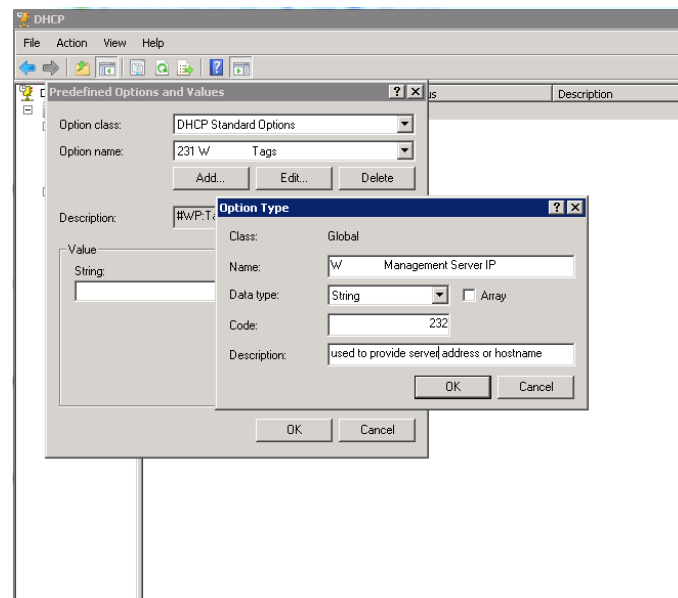
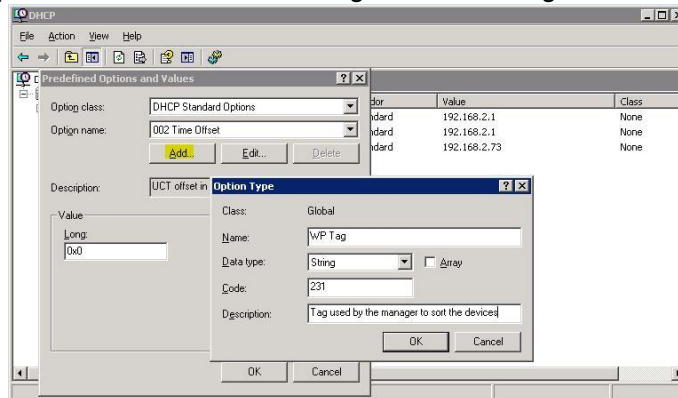
The setting for the DHCP scope options follows a well defined logic. The following example illustrates the configuration of DHCP on a windows server 2003. Make a right click on the server node, and then “Set Predefined Options...”



Click on “Add...” then fill in the fields as below, and then “OK”

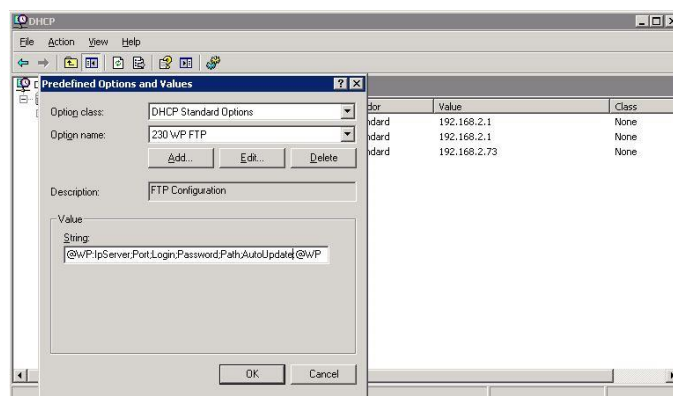


Redo the previous sequence for the Xcalibur-W Tag and the Manager Address



### 2.2.3.1.2 DHCP Option 230 - XcaliburW FTP Update

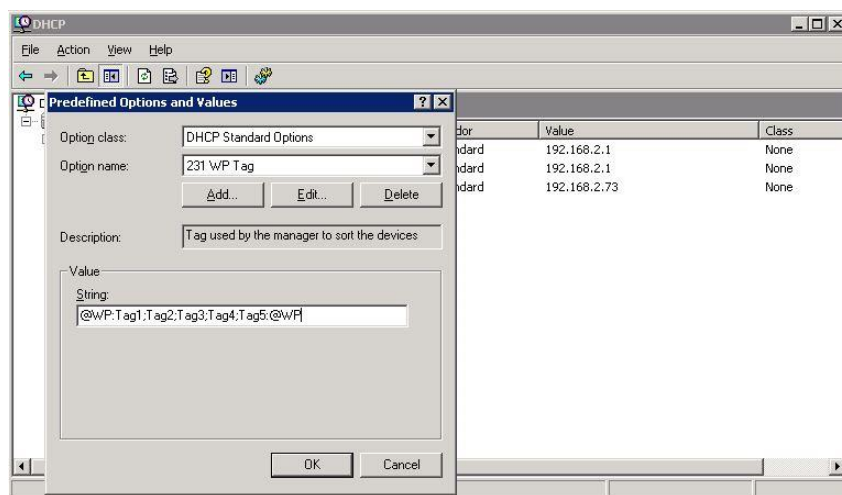
Select the 230 option in the drop-down list and fill in the fields as below



Parameters	Description
@WP:	Start of tag
IpServer	Ip address of the FTP server
;	Mandatory parameter separator
Port	Port number of the FTP server
;	Mandatory parameter separator
Login	Login used for the connection to the FTP server
;	mandatory parameter separator
Passw ord	Passw ord used for the connection to the FTP server
;	Mandatory parameter separator
Path	full path to the file InfoVersion.xml
;	Mandatory parameter separator
AutoUpdate	Boolean indicating w hether or not the automatic update by FTP is active. Possible values are "true" OR "false"
:@WP	End of tag

### 2.2.3.1.3 DHCP Option 231 - WP Tags

Do the same for the option 231



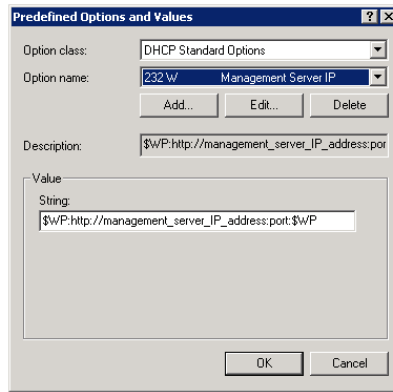
Parameters	Description
#WP:	Start of tag
Tag1	Tag1 entry
;	Mandatory parameter separator
Tag2	Tag2 entry
;	Mandatory parameter separator
Tag3	Tag3 entry
;	Mandatory parameter separator
Tag4	Tag4 entry
;	Mandatory parameter separator
Tag5	Tag5 entry
:#WP	End of tag

#### 2.2.3.1.4

#### 2.2.3.1.5 DHCP Option 232 - Manager Address

Add in the DHCP option 232.



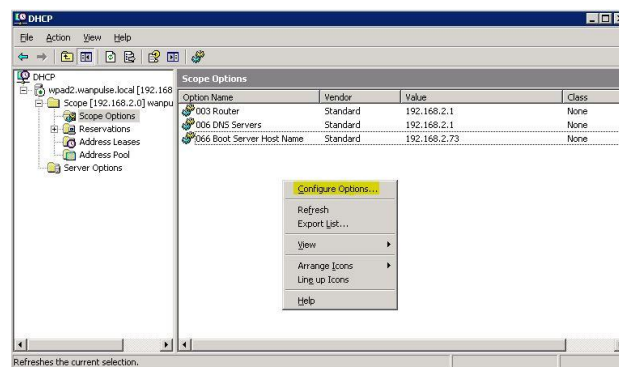


Parameters	Description
#WP:	Start of Manager Address
http://management_server_IP_address:port	Address of the Manager
:#WP	End of Manager Address

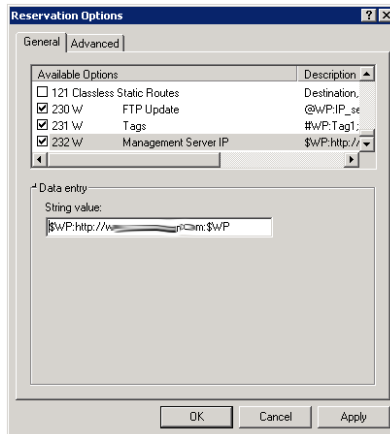
#### 2.2.3.1.6

#### 2.2.3.1.7 Enable Scope Options

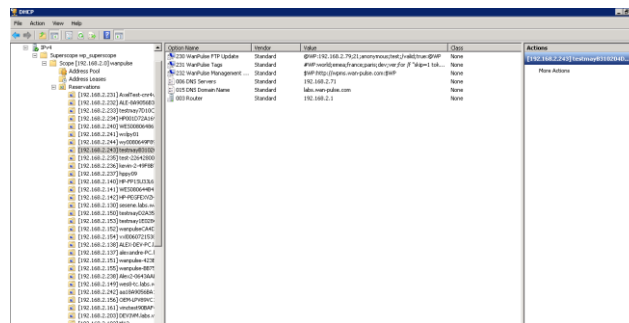
Click on the node corresponding to the scope covered by the tag, right click then “Configure options...”



Select 230, 231 and 232 then validate.



The configuration is completed, you can see the 3 new options appearing.



### 2.2.3.2 DHCP Options settings for Linux

Edit dhcp file settings: /etc/dhcp/dhcpd.conf and add follow ing lines for Xcalibur-W DHCP Scopes Options:

on main section:

```
option WP_FTP_Update code 230 = string; option WP_Tag code 231 = string;
```

on "subnet" section:

```
option WP_FTP_Update
"@WP:IPServer;Port;Login;Password;Path;AutoUpdate(True/False):@WP"; option WP_Tag
"#WP:Tag1;Tag2;Tag3;Tag4;Tag5:#WP";
```

Example:

```
option subnet-mask 255.255.255.0; option broadcast-address 192.168.1.255; option
routers 192.168.1.254; option domain-name-servers 192.168.1.1, 192.168.1.2; option
domain-name "xcaliburw.com"; option ntp-servers 192.168.1.254; option WP_FTP_Update
code 230 = string; option WP_Tag code 231 = string;
```

```
subnet 192.168.1.0 netmask 255.255.255.0 { option WP_FTP_Update
"@WP:192.168.1.79;21;anonymous;test;/ftupdate;true:@WP"; option WP_Tag
"#WP:world;emea;france;paris;dev:#WP"; range 192.168.1.10 192.168.1.100; range
192.168.1.150 192.168.1.200; }
```

## 2.3 Enrolling Client Devices

### 2.3.1 Manual Enrollement

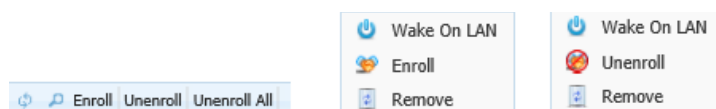
Enrolling Devices can be performed using the Manual Enrollment. From the **Device Enrollement** page, you can select which devices you wish to enroll. Of course, if you had many thousands of devices you may find it difficult to find the device, and so we have provided a filter system for displaying un-enrolled devices.

Hostname	MacAddress	Product	DA Version	IpAddress	Network	First Discovery	Last Check In	State
			1.4.0.597	192.168.2.153	192.168.2.0	6/14/2013 10:27:57 PM	6/18/2013 3:07:42 PM	Enrolled
		C6	1.4.0.598	192.168.2.177	192.168.2.0	6/14/2013 10:31:21 PM	6/18/2013 3:07:51 PM	Enrolled
		10iSD-CE	1.3.2.516	192.168.204.1	192.168.204.0	6/15/2013 2:15:59 PM	6/17/2013 2:19:27 PM	Not Enrolled
			1.4.0.597	192.168.2.150	192.168.2.0	6/14/2013 10:06:17 PM	6/18/2013 3:07:31 PM	Enrolled
			1.3.11.594	192.168.2.166	192.168.2.0	6/17/2013 9:24:13 AM	6/18/2013 3:07:47 PM	Not Enrolled
		UTM45	1.4.0.597	192.168.2.193	192.168.2.0	6/14/2013 10:20:14 PM	6/17/2013 8:55:58 AM	Enrolled

Enrollment Status allows three different **States** :

- Enrolled means the unit is already Enrolled
- Not Enrolled means the unit is not yet Enrolled
- Waiting enrollement means the Enrollment process is ongoing

You can select the devices you wish to enroll and click the enroll button located on the bottom status bar. You can also use the right-click context menu.





Enrollment takes a couple of minutes and this is due to the inventory of the device being registered. In addition, enrollment also uses up one license from the license pool.

Once Enrolled, the Device is automatically added to the Device List page and can then be managed.

Be aware that before being fully functional, the Device will need to create its first inventory. This process may take some minutes. During this timeline, some data will be missing and therefore the corresponding line in the Device List will feature some empty fields as shown below.

- Device that has not yet finished its Inventory

	win7-58	00:0C:29:3E:95:81			1.3.11.594	192.168.2.166	192.168.2.0			6/18/2013 5:40:01 PM
--	---------	-------------------	--	--	------------	---------------	-------------	--	--	----------------------

- Device that has finished its Inventory

	testmayD2A35DCE	10:78:D2:A3:5D:CE	ECS - 945GSED-ITX	Windows Embedded Standard 7	1.4.0.597	192.168.2.150	192.168.2.0			6/18/2013 5:59:06 PM
--	-----------------	-------------------	-------------------	-----------------------------	-----------	---------------	-------------	--	--	----------------------

### 2.3.2 Automatic Enrollment

The task of enrolling can be made fully automatic by simply ticking **Auto Enroll at first discovery** checkbox on the page below.

<b>Discovery and Enrollment</b> Licenses <b>Discovery</b> Device Enrollment	<b>Current Discover</b> Number of devices detected: 6 Number of devices enrolled: 5
	<b>Settings</b> Auto Enroll at first discovery <input checked="" type="checkbox"/>
	Enrollment port: 9999
	Save

When enabled, all the devices will initiate their enrollment process without requiring any further action.



Note that this feature applies to all new devices discovered by the server and all new devices that register themselves onto the server (using DHCP Scope options, DNS Name or IP Address set into their configuration file).

Once enrollment process is started, it follows the same process than the Manual Enrollment.



## 3 Manage Devices

---

### 3.1 Groups and Device Grouping

---

The concept of grouping devices was designed in order to make life easier for system administrators who need to access devices in a logical manner and manage them.

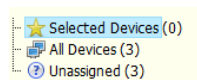
Xcalibur-W Server has a hierarchical method of grouping and administrators can create two different levels of groups: Static and Automatic. Once created groups can be populated manually or automatically, depending on the group type.




The following sections will drive you through the Best Practices

#### 3.1.1 Default Groups

---

By default, there are three built-in Groups that displayed in the Device Tree. These Groups are systems groups and therefore they can not be deleted nor modified.



	Selected Devices	The devices that have been already ticked, and to which the tasks will apply
	All Devices	The entire list of Enrolled Devices
	Unassigned	The devices that have not yet been assigned to any Static group

At first time use, Administrator will want to create specific Groups that will reflect its network topology, its geographical locations or its business organization. This is made possible using the Static and Automatic Groups.

#### 3.1.2 Static and Automatic Groups

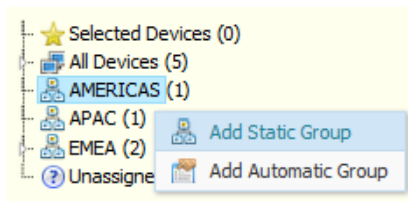
---

##### 3.1.2.1 Static Groups

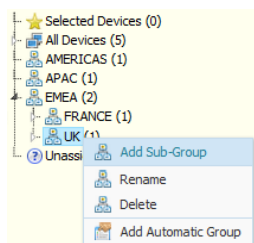
---

A static group is one which contains an exclusive list of devices : devices within a static group cannot exist within any other static group. It is intended for showing devices that are contained

within a static location such as country, region etc. To create a static group you right click on the All Devices entry within the Device Tree and select Add Static Group.



You can add Static Groups to the root (All Devices) or as a Sub Group within an already created group.



You can have as many nested static sub-groups as you wish, but take care not to make the structure too unwieldy. You can see an example of a static sub-group in the picture above.

#### 3.1.2.1.1 Adding Devices to a Static Group

When devices are enrolled onto Xcalibur-W Server they will normally join the Unassigned Group located at the bottom of the Devices tree. From there you will need to assign them to a group that is appropriate. You can do this by dragging and dropping the devices onto the target group. If you wish to move multiple devices you will need to select them first by ticking the check box and then dragging.

#### 3.1.2.1.2 Removing Devices from a Static Group

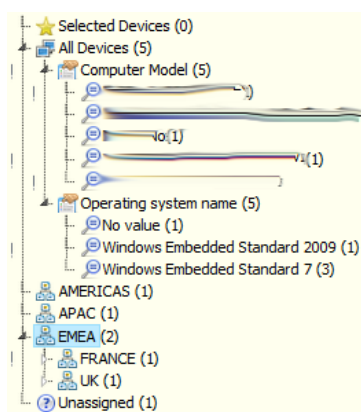
There is no method of deleting devices from a static group. You need to move them to the Unassigned Group or un-enrol them from Xcalibur-W Server. The process of un-enrolment will remove the devices from all groups.

### 3.1.2.2 Automatic Groups

There are the obvious limitations with static groups that can be a hindrance to the administrator. Static groups are intended for static locations such as countries, regions etc. However, administrators have a need for organizing devices within different types of groupings such as network subnet, operating system type, write-filter state etc. For this, Xcalibur-W Server provides the Automatic Group system. You can create automatic groups based on a number of pre-defined criteria as indicated in the table below :

*Computer Manufacturer	*Processor Model
*Computer Model	*XW Agent Version
*Network Address/Subnet	*Write Filter State
*DHCP	*Write Filter Type
*Operating System & Service Pack	*Auto Tags 1 to 2
*Processor Architecture	*Tags 1 to 5
*Processor Cores	

When a dynamic group is created using one of the choices above, the group will contain segment with the appropriate devices pre-populated. This allows the administrator to auto create groups based on these parameters. An example of this is shown below.



### 3.1.3 Use TAGs for custom Grouping

Xcalibur-W Server allows you to apply TAGs to your devices in order to ease the grouping. This feature is available within the **Single View** of your device. Click on **Administration** section and then **Inventory Tags** page.



There are two types of TAG :

- **Static** - The above fields can be used to manually entered data such as Location, Dates, Numbers that are relevant for sorting purpose.

Tag N° 1

Tag N° 2

Tag N° 3

Tag N° 4

Tag N° 5



Please note that the TAGs can also be provided by the mean of a DHCP Server. For further details, please refer to DHCP Scope Options.

- **Calculated** - One of the coolest things about Xcalibur-W Server's dynamic grouping technology is its ability to run DOS or WMIC commands on the device and return back the values generated by the operating system. This means that you can create dynamic groups based on say, the time zone or display resolution being used etc. In order to do this you need to populate the Auto Tags of which there are two with the appropriate entries.

*In the above example, we query for the version of the installed OS.*

Tag auto N° 1  Command

Tag auto N° 2  Command



Be careful how you use this as it can populate the Dynamic Group name with a lot of data. Further information on these WMIC are available in the WMIC Commands Glossary

### 3.1.4 Filtering and Searching Devices

All administrators need to occasionally search and locate specific devices within the estate. This can be very tedious if there are literally thousands of devices present. Xcalibur-W Server provides administrators with a very simple and effective way to find devices within the infrastructure. You will note that on the top of the devices list there are a number of text entry fields and some drop down lists. You can use these to filter and find devices you wish to locate.

	Hostname	MacAddress	Product	OS Name	DA Version	IpAddress	Network	Write Filter	Maintenance	Last Check In
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	testmay1E028C35	00:1F:1E:02:8C:35	VIA Technologies Ltd. - VX80	Windows Embedded Standarc	1.4.0.597	192.168.2.153	192.168.2.0			6/19/2013 5:09:47 PM
	testmayD2A35DCE	10:78:D2:A3:5D:CE	ECS - 945GSED-ITX	Windows Embedded Standarc	1.4.0.597	192.168.2.150	192.168.2.0			6/19/2013 4:45:37 PM

The text fields use standard wildcard methods. So if you wish to filter for any device with the term LNV within the hostname then you simply enter \*Test\* in the text field in the hostname column. If you wish to locate a device with the first four digits of the MAC ID equal to 01:0F then enter the term \*01:0F\* in the field within the MAC ID column. The drop down lists for columns such as Write Filter and Maintenance also provide you with options for listing. You can also use multiple columns filtering to provide you with a better result, for example you can filter on the Device Agent version and FBWF enabled.

### 3.2 Single Device View

The Single Device View can be accessed when double-clicking on any device from the Device Listing. The page is displayed within a new tab and is related to the selected device only.

Connected to: testmay1E028C35 | Up Time: 0d 03h07min03sec | Write Filter state: | Maintenance State: | Last pulse: 6/20/2013 3:47:46 PM | Last Inventory: 6/20/2013 3:47:46 PM

Maintenance

Monitor

Interact

Administration

Device Security

Device Configuration

Apps Configuration

User Experience

Image Management






Home


Home section isn't available.

The top bar of the screen provides useful information regarding the device status, this includes the Hostname, the Uptime, the Write Filter State and the Maintenance State.


Connected to: testmay1E028C35 | Up Time: 0d 03h07min03sec | Write Filter state: | Maintenance State: | Last pulse: 6/20/2013 3:47:46 PM | Last Inventory: 6/20/2013 12:13:28 PM

The table below describes all items available within the top bar and their expected values.

Connected to	Hostname of the Device
Uptime	Uptime since last bootup
Write Filter	 =No Write Filter Installed  =Write Filter Installed but not enabled  = Write filter installed and enabled
Maintenance	 = Device is out of Maintenance Mode  = Device is under Maintenance
Last Pulse	Last connection from the client to the Management Server
Last Inventory	Last time Inventory has been sent to the Management Server

In order to update the Inventory Information, you can press the  which request the Client to send new inventory.

Whenever a function is used to execute a command within the Single View , then a Task containing one command - and applied to this device only - will be published on the Management Server.

Publish Date	Reccurence	Task	Device Qty	State	Processing	Finished	Failed
6/21/2013 10:11:07 AM		Launch shell command - vxd0060722804A5	1		0	0	0

Details of all available commands and functions are listed in the Commands to Single Device section.

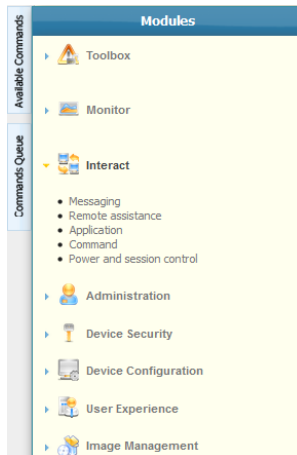
### 3.3 Tasks and Creating Tasks

One of the mainstream capabilities all management softw are needs to possess is the ability to send a single command or a series of commands to devices in order for them to perform certain tasks, be they simple or complex in nature. Xcalibur-W Server is fully equipped to do just such a thing. The functions, commands and command queues that can be constructed within Xcalibur-W Server can be saved as tasks that can be used in isolation or as recurring tasks intended to deliver actions on a repetitive basis.

Tasks can be simple affairs such as asking a series of devices to change their display wallpaper. Or, they can be slightly more involved such as joining a domain and they can also be highly detailed such as running scripts to engage an application to install.

The administrator can choose commands from the Available Commands Tab located on the left of the main Device Listing display. The Available Command Tab is activated when the mouse is hovered over the tab area and consists of a number of main level 1 functions with commands within. The figure below shows an example of the level 1 function and command set available within the Command Tab.

### 3.3.1 Available Commands Tab



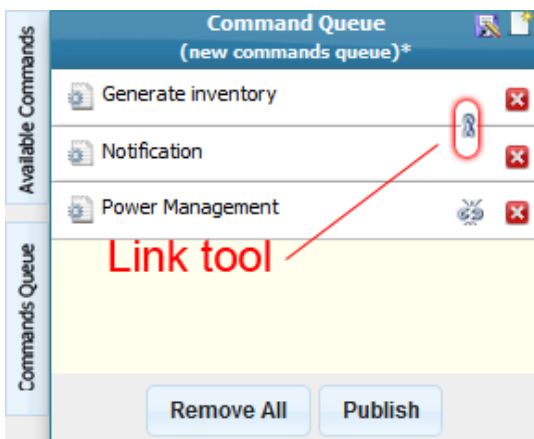
Whenever you wish to build a new Command Queue and then convert that into a task or recurring task, you need to access the available commands by using the Available Commands Tab. There are a variety of commands available within the Available Command Tab and these are described in further depth in Glossary of Functions and Commands.


By clicking on any module, the corresponding section will pop up in a separate window allowing you to define the parameters and save the command.


### 3.3.2 Command Queue


As you configure commands within the Available Commands Tab, these are added sequentially to the Command Queue.

Once you have completed building the Command Queue, you can then edit it as required by



moving the command object by using drag and drop, or deleting command object within the queue by clicking on the  symbol.

By default, all commands will be run concurrently once sent to the device. However, there are circumstances in which you will need to run commands in a serial manner, with one command following when the previous has finished. This can be done using the Link capability within Xcalibur-W Server's Command Queue. Notice the Link icon  and an example of linked commands within the image on the left.

You can then save the Command Queue as a Task Template by clicking the Save icon located on the top orange bar (). When clicked, Xcalibur-W Server will present you with a dialog requesting the name of the Task Template. Once you provide an appropriate name and click the Save Template button, the Command Queue will be saved in the Library's Tasks section.

If you wish to publish the Command Queue as a task to devices, you can click the Publish button and choose to make it an immediate task or a repetitive task.

## 3.4 Publishing Tasks

By pressing the Publish button from the Command Queue, Xcalibur-W Server will display the Publish Task window.

**Publish Task**

Choose a name for the task, then set parameters for execution

Task Name

Publish Start  (UTC +02)

Expected execution date on client device depending on its time zone

Publish End

☐ Wake On Lan selected devices

☒ Recurring Task

Recurrence Settings

Recurrence Unit

Frequency

**Publish**

Administrator can choose to enter a friendly name for the Task so as to ease the understanding in the logs.

Additionally, the Wake-On-Lan option can be enabled. If at least one unit is powered on in the pool of target device, then this unit will send a Wake-On-Lan network event to the other units of the pool.

### 3.4.1 Scheduling

The Task can be set to be executed immediately or at a later time. For that purpose, the **Publish Start** field can be modified.

The Administrator can also choose to define an End date using the **Publish End** field

- If leave empty, then the Task will remain active until all the agents collect and process the Task.
- If a date is defined, then the Task will be stopped after the specified date ensuring that no other devices process the Task after the date. ***If at least one agent did not collect and process the Task within the execution period, then the Task will turn to Obsolete status.***



When managing units that are not in the same Timezone, it is sometimes difficult to figure out at what time the Task is performed by the remote device. For that purpose, the **Expected Execution Date** is provided for information purpose based on the device timezone.

Please modify the timezone according to your remote device's timezone


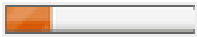







### 3.4.2 Recurrency

---

When Publishing a Task, Administrator can also choose to set the Task as recurrent Task. The option is activated using the corresponding checkbox. Once published the Task is stored within the Library in the Recurring Task section. Xcalibur-W Server will then automatically create and publish occurrences of the Task according to the recurrency settings that have been defined.

### 3.4.3 Progress Legend

---

Scheduled		Task is planned but not yet published ; the start date is later than now
Published		Task is published ; the start date is over but no agent has collected the task yet
Processing		Task is processing ; at least one agent did collect the task
Stopped		Task has been stopped ; no more agent will collect the task anymore
Completed		Task is over ; all agents did execute the task without any error
Unpersisted		Task is over ; all agents did execute the task without any error but the Write Filter was not deactivated
Failed		Task has failed ; at least one error occurred
Partial Failed		Task has failed ; at least one error occurred but the Write Filter was not deactivated
Obsolete		Task is over ; the End date is over

## 3.5 Tasks and Commands Board

---

One of the fundamental aspects of any management solution is the ability to perform tasks and make note of events. The Device Task Board described below is used to record and archive the tasks that have been performed as a part of the management process. The Device Task Board is also used to examine the tasks on a granular basis when required to indicate why tasks may have failed or part failed.

### 3.5.1 Task Level View

---

The task level view is used by administrators to list the tasks that have taken place. Tasks are listed in chronological order with the Task Level View with the most recent at the top.

Device Task Board	Publish Date	Recurrence	Task	Device Qty	State	Processing	Finished	Failed	Ack
Task level view									No
Command level view	6/20/2013 4:28:49 PM		Power Management - vx0060722804A5	1	<div></div>	0	1	0	
	6/20/2013 4:28:46 PM		Write Filter FBWF - vx0060722804A5	1	<div></div>	0	1	0	
	6/20/2013 3:57:16 PM		Notification - testmay1E028C35	1	<div></div>	0	1	0	
	6/20/2013 3:52:20 PM		Monitoring rule	6	<div></div>	0	6	0	
	6/20/2013 3:50:08 PM		Monitoring rule	6	<div></div>	0	6	0	
	6/20/2013 3:39:25 PM		Monitoring rule	7	<div></div>	0	7	1	
	6/20/2013 3:33:19 PM		Monitoring rule	7	<div></div>	0	7	0	
	6/20/2013 3:28:31 PM		Monitoring rule	3	<div></div>	0	3	0	
	6/20/2013 3:26:58 PM		Task	7	<div></div>	0	7	0	
	6/20/2013 3:26:05 PM		Task	7	<div></div>	0	7	0	
	6/20/2013 3:17:19 PM		Task	7	<div></div>	0	7	0	
	6/20/2013 2:28:28 PM		test sleep	8	<div></div>	0	8	0	
	6/20/2013 1:10:02 PM		reboot toute les 30 mins	4	<div></div>	0	0	0	
	6/20/2013 1:09:24 PM		maintenance + inventaire + diag	4	<div></div>	0	0	0	
	6/20/2013 12:40:02 PM		reboot toute les 30 mins	4	<div></div>	0	4	0	
	6/20/2013 12:10:02 PM		reboot toute les 30 mins	4	<div></div>	0	3	0	

As can be seen from the image above, tasks lists are generated with full details of the task description, date, the number of devices, state the task finished at as well as the number of sub-tasks that completed. In addition the failed tasks are clearly indicated in red. You can drill down into a task by double-clicking on its listing or by examining the entire set within the Command View.

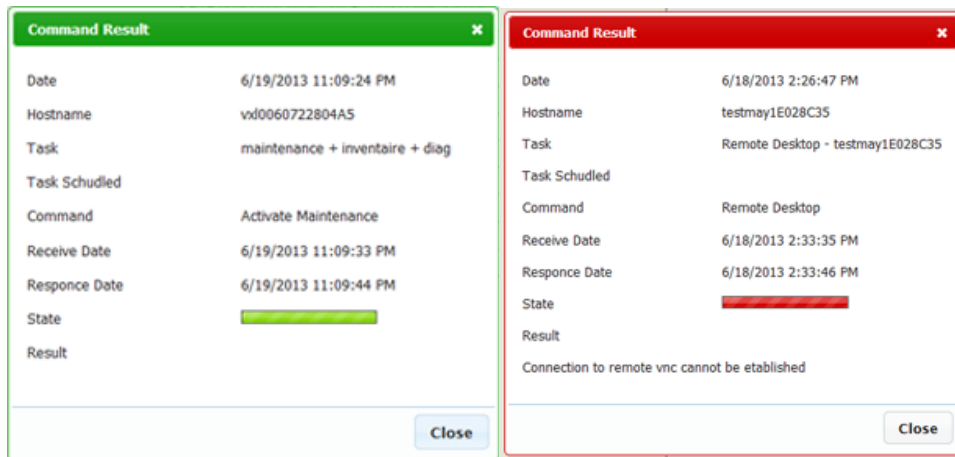
### 3.5.2 Command View

The Command Level view shows the administrator which of the task's individual commands have completed and to what level. As can be seen from the example below, several commands have not completed and their state is indicated by the colored status bar.

Device Task Board	Date	Hostname	Ip Address	Task	Command	Receive Date	Response Date	State
Task level view								
Command level view	6/19/2013 11:09:24 PM	vx0060722804A5	192.168.2.193	maintenance + inventaire + diag	Activate Maintenance	6/19/2013 11:09:33 PM	6/19/2013 11:09:44 PM	<div></div>
	6/19/2013 11:09:24 PM	vx0060722804A5	192.168.2.193	maintenance + inventaire + diag	Generate inventory	6/19/2013 11:10:03 PM	6/19/2013 11:10:38 PM	<div></div>
	6/19/2013 11:09:24 PM	vx0060722804A5	192.168.2.193	maintenance + inventaire + diag	Diagnostic report	6/19/2013 11:10:03 PM	6/19/2013 11:11:46 PM	<div></div>
	6/19/2013 11:09:24 PM	vx0060722804A5	192.168.2.193	maintenance + inventaire + diag	Deactivate Maintenance	6/19/2013 11:10:03 PM	6/19/2013 11:11:58 PM	<div></div>
	6/19/2013 11:09:24 PM	testmay1E028C35	192.168.2.153	maintenance + inventaire + diag	Activate Maintenance	6/19/2013 11:11:47 PM	6/19/2013 11:12:00 PM	<div></div>
	6/19/2013 11:09:24 PM	testmay1E028C35	192.168.2.153	maintenance + inventaire + diag	Generate inventory	6/19/2013 11:12:19 PM	6/19/2013 11:13:26 PM	<div></div>
	6/19/2013 11:09:24 PM	testmay1E028C35	192.168.2.153	maintenance + inventaire + diag	Diagnostic report	6/19/2013 11:12:19 PM	6/19/2013 11:17:55 PM	<div></div>
	6/19/2013 11:09:24 PM	testmay1E028C35	192.168.2.153	maintenance + inventaire + diag	Deactivate Maintenance	6/19/2013 11:12:19 PM	6/19/2013 11:18:06 PM	<div></div>
	6/19/2013 11:09:24 PM	testmay02A35DCE	192.168.2.150	maintenance + inventaire + diag	Activate Maintenance			<div></div>

Further double clicking on the command results in the Status Info being displayed for that particular task.

Should the command have run successfully the status info windows will be similar to that shown below on the left:



How ever if the command was not successful the status window will indicate the failure and its reasons. See above right image.



## 4 Commands Glossary

---

### 4.1 Commands to Multiple Devices

---

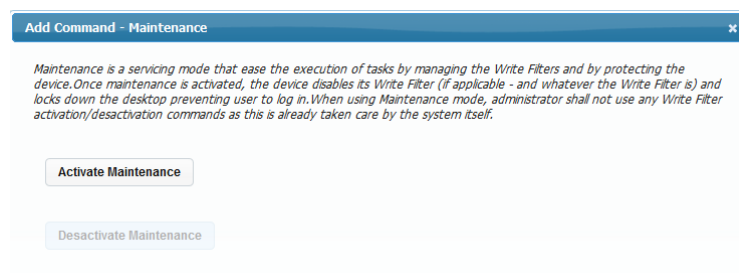
#### 4.1.1 Toolbox

---

##### 4.1.1.1 Maintenance

---

There are occasions when the administrator will need to perform tasks on the device and they require the protective Write Filters to be disabled. It is not advisable to allow users to use the device in any manner as it may interfere with the management process. In order to accommodate such circumstances, we have provided the **Maintenance** command.



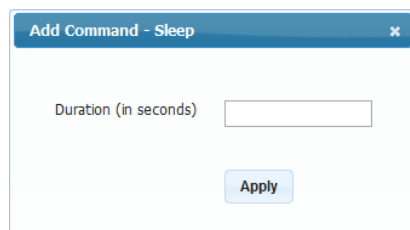
When Maintenance is activated the device agent places the device into a maintenance mode. This locks out all keyboard and mouse activity from the user thereby rendering any interference impossible. The maintenance mode also disengages the Write Filter (FBWF or EWF) so that any maintenance tasks performed are persistent in nature.

When the Maintenance mode is deactivated the FBWF or EWF is switched on and the device is rebooted.

##### 4.1.1.2 Sleep

---

The **Sleep** command enables to create a pause during a sequence of commands. The Agent will execute the next command only once the time elapsed. The duration shall be set in seconds.



##### 4.1.2 Monitor

---

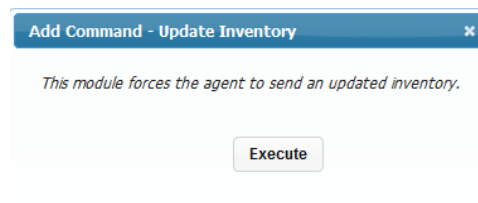
The Monitor command consists of two further Level 2 commands: Inventory and Diagnostics.

#### 4.1.2.1 Inventory

---

When the Inventory command is run via the Command Queue instructs the devices in the selection to update their inventory to the Xcalibur-W Server. This inventory update can also be done on the startup of every device if required.

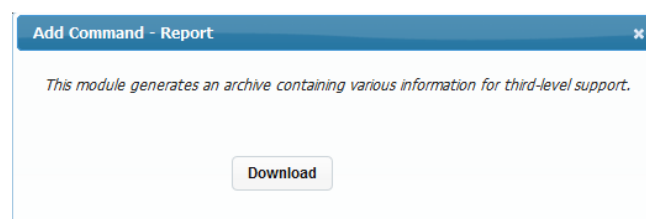
If you wish to view the inventory of a particular device, simply double click on its device listing entry.



#### 4.1.2.2 Diagnostics

---

The Diagnostic command sends an instruction down to the client(s) to upload the diagnostic log to the server. This diagnostic log is in an XML format and can be sent to the support department for assistance. The diagnostic files are then downloaded to the library as compressed archives.



#### 4.1.3 Interact

---

The Interact command section contains commands that allow you to interact with users via the device.

##### 4.1.3.1 Messaging

---

**Add Command - Messaging**

This module allows you to send a message to the user logged on the system. The message displayed as a Windows message box.

Title:

Message:

Message Type: ☒ Information message box ☐ Question message box

Display Time:

Messaging allow s you to send a message to one or many devices. The messages can be interactive ones or simple notifications. Messages like any other command can be scheduled for later delivery.

### 4.1.3.2 Remote Assistance

Remote Assistance allow s you to open a VNC session, to control the devices. Just enter the passw ord, and the Administrator passw ord if you w ant the full rights on the device.

**Add Command - Remote assistance**

This module enables to start a VNC session on the remote device. Your web browser must have Java enabled to execute the VNC session.

Settings

Enable remote connection ☐

Enable access password ☐

Access Password:

Confirm Password:

Enable Administration password ☐

Administration Password:

Confirm Password:

Query Local User ☐

### 4.1.3.3 Application

**Add Command - Application**

This module allows to launch any local application stored into the remote system.

Application's path:   
Example: C:\Windows\System32\calc.exe or calc

Parameters:

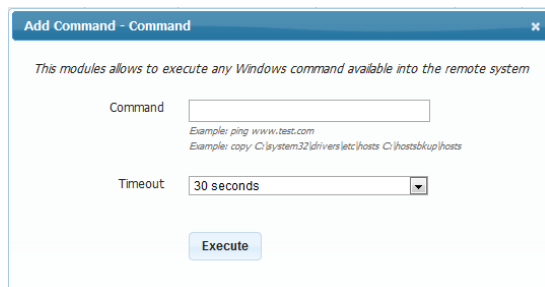
☐ Warn user

There are times w hen administrators are required to run applications on the local server. In order to achieve this you need to use the Application command.

In order to use the Application command enter the full path to the application and any runtime parameters that are needed. You can also w arn the user by sending a message. Click the Launch button and you're done.

#### 4.1.3.4 Command

---



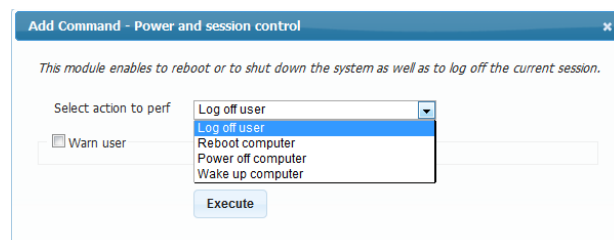
In order to run any commands on the local device you will need to use the Command function. This allows you to specify the command name or path and execute it on the device(s).

#### 4.1.3.5 Power and Session Control

---

The Power and Session Control function allows administrators to perform a number of low level commands that determine the user's session. These are:

- Log Off
- Reboot
- Shutdown
- Wake Up Computer



#### 4.1.4 Agent Administration

---

The Administration command set consists of commands that are required for the device's agent configuration.

##### 4.1.4.1 Device Agent Configuration

---

Although the Device Agent installed in the device is configured for the optimum performance, administrators may need to reconfigure the agent to operate within the restrictions or rules of the network.

**Add Command - Device Agent Configuration**

Warning, this form will be applied with all the values below.

This module allows to configure

Synchronization Port

Discovery Port

Pulse Delay (seconds)

Enable DHCP Scope ☒

Randomize the sending of inventory over (seconds)

Update Inventory at each device startup ☒

**Apply**

## Synchronization Port

When clients connect to the Xcalibur-W Server over a local area network or a routed wide area network using MPLS for example, the pulse synchronization system uses port 7270 by default to inform the client agent that there is a Command Queue waiting for it.

When operating across a WAN that is not routed the server awaits the pulse sent from the client and then sends the task to it.

## Discovery Port

This is the port used by the Xcalibur-W Server when receiving and sending discovery signals.

## Pulse Delay

The pulse or heartbeat is sent by the client agent on a regular basis to inform the Xcalibur-W Server that it is present and online. It is also used by the server to determine that there are jobs waiting for the client in a WAN managed scenario. The entry represents the number of seconds in between each pulse.

## Enable DHCP Scope

As mentioned earlier in the Discovery section of this guide, the client agent uses DHCP as a means of obtaining the IP address or the host name of the Xcalibur-W Server. You can choose if this method is enabled or not by toggling the checkbox. The default state is enabled.

## Randomize the Sending Inventory (Seconds)

Every client agent will send the inventory of the device when it is powered on. As you will appreciate, if there are several hundreds or even thousands of devices powering on at approximately the same time there will be a sizeable network load generated when the

information is sent. This setting enables the device to randomize the sending time of the inventory to reduce network loads.

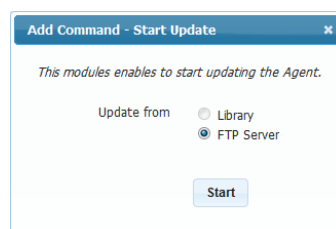
### Update Inventory at each device startup

If required the “Update Inventory at each device startup” can be disabled using the Client Agent settings described later.

#### 4.1.4.2 Agent Update

---

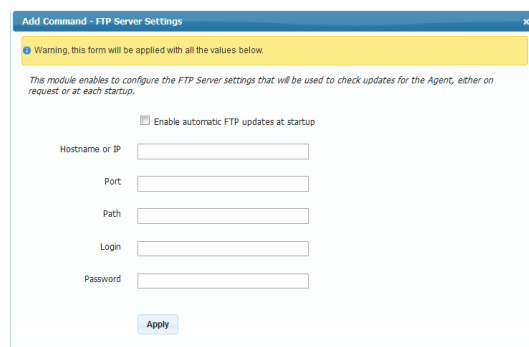
You can choose how to update your Agent, either with the Library or the FTP server.



The dialog box titled "Add Command - Start Update" contains the text "This module enables to start updating the Agent." Below this, there are two radio buttons for "Update from": "Library" and "FTP Server". The "FTP Server" option is selected. At the bottom right, there is a "Start" button.

#### 4.1.4.3 FTP Server Settings for Agent Update

---



The dialog box titled "Add Command - FTP Server Settings" contains a warning message: "Warning, this form will be applied with all the values below." Below this, it states: "This module enables to configure the FTP Server settings that will be used to check updates for the Agent, either on request or at each startup." There is a checkbox labeled "Enable automatic FTP updates at startup" which is checked. Below the checkbox are five input fields: "Hostname or IP", "Port", "Path", "Login", and "Password". At the bottom left, there is an "Apply" button.

This denotes the FTP Server details for the management agent update system. The agent is capable of auto updating itself in the event of a version change.

This is achieved by seeking and downloading an XML file called `infoversion.xml`. The format of this file is as follows:

```
<Info>
  <Imaging>
    <Version>0.0.0</Version>
    <Path>image15032011</Path>
  </Imaging>
  <Profile>
    <Version>0.0</Version>
    <Path>Profile0.2.txt</Path>
  </Profile>
```

```

<Agent>
  <Version>1.3.11.594</Version>
  <Path>ftp://anonymous:test@ftpserver/XGWAgent_1.3.exe</Path>
</Agent>
</Info>

```

This information can also be set up for provisioning via a DHCP Scope, ID230. The format used for the scope entry is as follow s: @WP:n.n.n.n;21;Anonymous;Test;/;true:@WP

So w hat does this all mean?

- @WP: is the start of the information tag
- n.n.n.n is the IP address of the FTP Server
- 21 is the port to be used
- Anonymous is the username used to log in
- Test is the passw ord used to authenticate
- / is the path w here the infoversion.xml is kept
- True is to inform the agent that the auto-update is active.
- :@WP is the end of tag marker

#### 4.1.4.4 Inventory Tags

---

The Xcalibur-W Server is capable of enabling clients w ith inventory tags. There are tw o types of tags: Regular Tags and Auto Tags. There are five Regular Tags provided and tw o Auto Tags.

Regular Tags may consist of plain alphanumeric text w hilst Auto Tags may consist of expressions using WMIC. For example you could get the time zone of a device back to the management server by using an Auto Tag such as “WMIC TIMEZONE GET STANDARDNAME”. This w ill return something similar to GMT Standard Time.

You can use inventory tags to auto create groups. The additional pow er of WMIC commands allow s the auto-creation of groups using a much w ider set of parameters such as time zone etc.

#### 4.1.5 Device Security

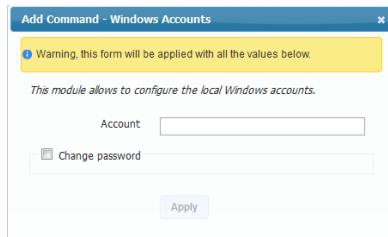
---

As the name suggests this L1 function comprises commands that are linked to the security and operable state of the device.

#### 4.1.5.1 Windows Accounts

---

The action of this command is to allow you to change the password of any given account on the



target device(s). As can be seen from the snapshot you can enter the account name in the Account field and then tick the checkbox to edit the password. The format of the password can be standard alphanumeric and symbol as Windows permits or it can be prefixed or have a suffix based on the MAC ID of the device. The latter obviously making the unit highly secure and individual.

#### 4.1.5.2 Auto Logon

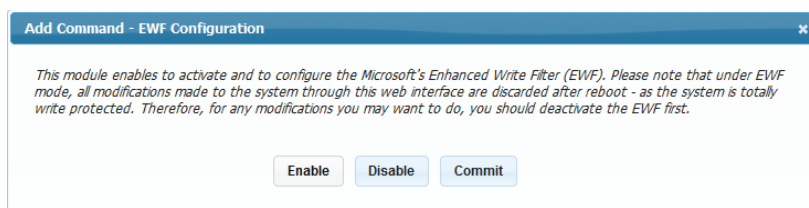
---

Windows embedded devices by default are shipped to logon locally with a username USER, whose default password is user. However in domain environments it is not normal to have a device auto logon in any manner. It is preferred to have a domain login as standard in order that single sign on works seamlessly. This command does allow you to set an auto login credential with domain name if it is required.

#### 4.1.5.3 Write Filter (EWF)

---

This command controls the behaviour of the Enhanced Write Filter (EWF) within Windows embedded devices. All Xcalibur-W Server enabled devices are configured to have File-based Write Filter (FBWF),



Activating any of the options within this command will initiate a reboot sequence within the Command Queue.



#### 4.1.5.4 Write Filter (FBWF)

---

This command allows the control of the File Based Write Filter (FBWF) within Windows embedded devices.



Whenever FBWF is used within devices there is a possibility of Low Memory alerts being displayed on the desktop device. This is a result of the threshold setting for low memory pre-programmed by Microsoft into all Windows embedded devices. The settings allow you to alter this threshold should you find any problems with this issue on your devices.

##### **Display Warning Message at %**

This field allows you to set the percentage at which the FBWF Cache will trigger a low memory warning. (Default value = 85, Minimum value = 50, Maximum value = 90)

##### **Display Critical Message and Reboot at %**

This field allows you to set the value at which the FBWF Cache has reached a critical stage and reboot of the device is required in order to flush the system in an orderly manner. This message will be displayed in conjunction with a countdown to reboot. (Default value = 95, Minimum value = 55, Maximum value = 95)

##### **Time before Auto-reboot (seconds)**

This field allows you to set the number of seconds that will elapse before the system reboots following the Critical message described previously. Operation of this command causes a reboot command being placed in the Command Queue.

#### 4.1.5.5 Write Filter Exclusion List

---

This option enables to add a new location into the list of exclusions of the FBWF Write Filter.

Dialog box titled "Add Command - FBWF Configuration". The "Settings" section is expanded, showing a "New exclusion" text input field and an "Add" button.

#### 4.1.5.6 Write Filter Cache Size

---

This option allow s to define the size of the memory cache that is dedicated to the Write filter Ram overlay.

Dialog box titled "Add Command - FBWF Configuration". The "Settings" section is expanded, showing a "Set Maximum Cache size" text input field with the value "0" and an "Apply" button.

#### 4.1.5.7 Fbwf Memory Alerts

---

This Task allow s you to enable the Low Memory Alerts. The w arning, criticals messages, and if it needs, the autoreboot of the device.

Dialog box titled "Add Command - FBWF Configuration". A yellow warning banner at the top states: "Warning, this form will be applied with all the values below." The "Low Memory Alerts" section is expanded, showing three text input fields: "Display warning message at" (value 0, recommended 85), "Display critical message and reboot at" (value 0, recommended 95), and "Time before auto reboot" (value 0, recommended 120). An "Apply" button is at the bottom.

#### 4.1.5.8 RAM drive

---

There are occasions such as installing application updates etc on the target device, w hen you need to temporarily increase the size of the RAM drive configured on the target device. The RAM drive command allow s you to do just that.

In case you decide to change the drive letter used by the RAM drive, take care though that you change other parameters that reference the RAM drive.

The default size of the RAM drive is 64MB, the recommended maximum size being 512MB.

#### 4.1.5.9 USB Ports

---

One of the key concerns of IT managers is the security of the USB ports that are present on the target devices. The USB Port command allows administrators to lock the USB ports from accessing any 'storage class' device, or make them read only.

#### 4.1.6 Device Configuration

---

The Device Configuration function consists of a series of commands specifically concerned with configuring the target device in terms of general configuration.

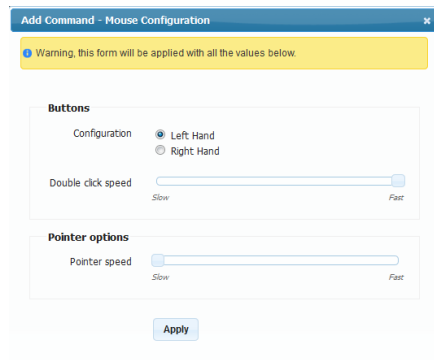
##### 4.1.6.1 Keyboard Configuration

---

Using this command the administrator can change the language of a keyboard, its character repeat delay and repeat rate.

### 4.1.6.2 Mouse Configuration

---

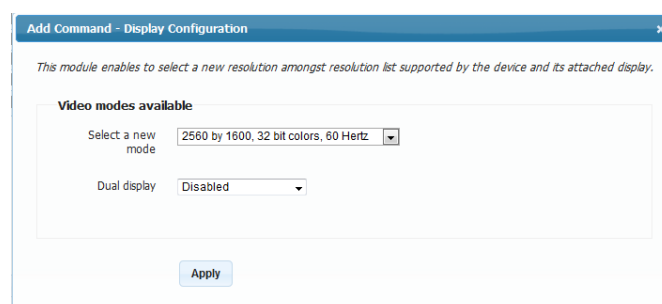


Although this is rarely done, it may be required of the administrator to configure a user's mouse for him. This command provides the administrator with the means of doing this.

### 4.1.6.3 Display

---

Although all Xcalibur-W approved target devices are configured to use DDC there are occasions when the administrator may need to set a resolution manually. There will also be the need to set displays up to use dual screen modes and orientations. The Display command empowers the administrator to carry out such functions.



The Display command dialog and the different dual screen options are shown above.

### 4.1.6.4 Network

---

You can enable DHCP, and configure a DNS for your device in this panel.

**Add Command - Network Configuration**

Warning, this form will be applied with all the values below.

Enable DHCP ☐

The configuration linked to the Ip address will not be changed.

Obtain DNS server address automatically ☐

Primary DNS

Secondary DNS

Apply

#### 4.1.6.5 Proxy

**Add Command - Proxy Configuration**

Warning, this form will be applied with all the values below.

Proxy settings apply to the system including Internet Explorer.

Use Proxy Server ☐

Server

Port

Bypass Proxy server for local address ☐

Apply

Some organizations require the configuration of target devices to use the company proxy server. The Proxy command allows these settings to be made by the Administrator using Xcalibur-W Server.

#### 4.1.6.6 System Time

You can change the date and the time in this part.

**Add Command - Date and Time Configuration**

This module enables to change the system time and date.

Date and Time

June 2013

Su	Mo	Tu	We	Th	Fr	Sa
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

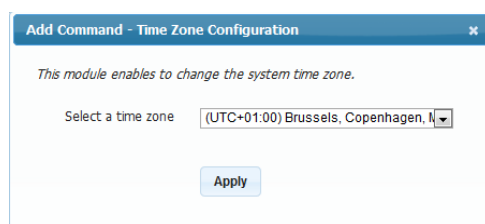
Time 15:15

Hour

Minute

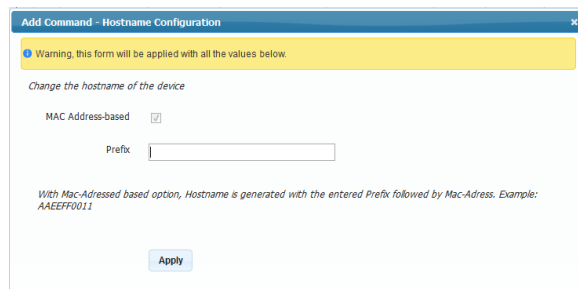
Apply

### 4.1.6.7 Time Zone



You shall go in this panel to change the Time Zone of your device.

### 4.1.6.8 Hostname

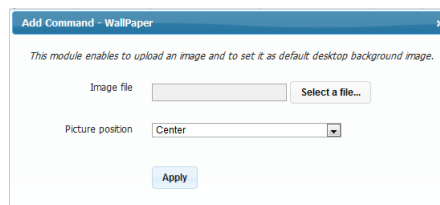


In the event that the administrator needs to change host names they can do this using the Hostname command. This command also allows you to include the MAC ID as part of the hostname.

## 4.1.7 User Experience

### 4.1.7.1 Wallpaper

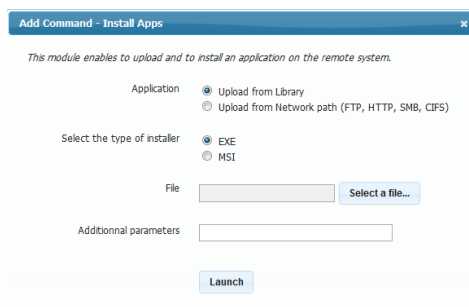
The Wallpaper command allows you to modify the wallpaper of target devices using an image of your choice.



## 4.1.8 Image Management

This set of commands concentrates on the different OS image changes that may be required from time to time, such as application updates etc.

### 4.1.8.1 Install Apps



The Install Apps command allows administrators to deploy applications from a variety of sources to the target devices. Applications can be in either EXE or MSI formats, and can be delivered via the Xcalibur-W Server Library or FTP, HTTP, SMB or CIFS locations. In addition, launch parameters can also be specified.

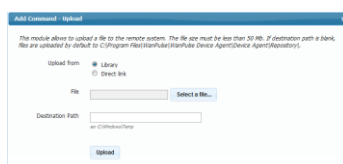


Remember that the Application shall be installed silently. MSI resources install silently whereas EXE resources may not. Administrator shall make sure required parameters and switches are properly specified to force silent installation. Please refer to the publisher documentation to get the exact application parameters

#### 4.1.8.2 Upload

---

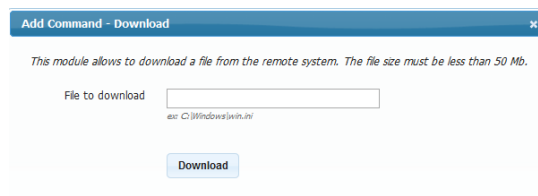
The Upload command is intended for use when you wish to upload a file or files to the target device(s).



#### 4.1.8.3 Download

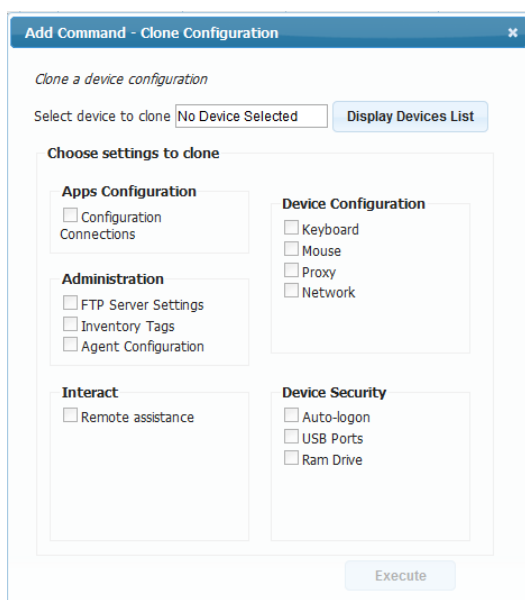
---

Whenever you have the requirement to recover a file from target devices, you can use the Download command. Files downloaded are stored in the Library under Downloads.



#### 4.1.8.4 Clone Configuration

---



When you have a network landscape comprising many hundreds or even thousands of devices, it is a challenge to distribute the same settings to multiple devices. For this reason we have provided you the ability to clone the settings of one device to many other devices.

## 4.2 Commands to Single Device

### 4.2.1 Monitor

#### 4.2.1.1 System Informations

System Informations provide an overview of **Device's** properties as well as the list of **Installed Applications** and **Security Patches**.

System Informations	
This module displays the global information of the device as well as installed application and Microsoft QFEs.	
Device	Installed Applications
Product name	FEC - MNIIC8PI
Hostname	wanpulee-4238B9
Operating system and SP	Microsoft Windows XP Professional - Service Pack 3
Operating system name	POSReady 2009
Product ID (License Microsoft)	00817-620-0054345-06839
CPU type and Speed	Intel(R) Atom(TM) CPU D525 @ 1.80GHz, 1795 Mhz
Disk Size	152 625 Mo
Disk Free	145 880 Mo
RAM Size	1 024 Mo

#### 4.2.1.2 Inventory Informations

This section lists all the **hardware specifications** of the device. By clicking on the desired grid, you can get detailed information on each element.

Get informations from the system

This module displays detailed hardware information of the device.

Show grids

Collapse grids

Bios					
Serial Number	Manufacturer	Model	Version	Date	
To Be Filled By O.E.M.	American Megatrends Inc.	MN1C8PI	GBT - 20110528	6/28/2011 2:00:00 AM	
Controllers					
Disk					
Keyboard					
Memory					
Monitor					
Base board					
Partition					
Pointing device					
Printer					
Processor					
Sound device					
Video card					
Network					

#### 4.2.1.3 Device Performances



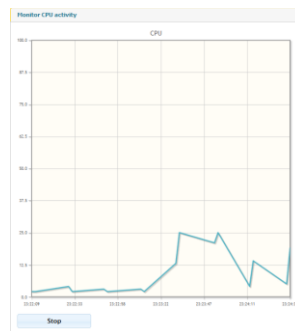
There are live information that Administrator might want to get when accessing to a particular Device. This can include the CPU performances, the list of started services or the the list of running applications. Once you click on the functions below , then the Device will send to Xcalibur-W Server a continuous flow of data so as to display these live information.



Before starting to send the data, the Device will need to receive the corresponding request from Xcalibur-W Server. The time needed for this is equal to the pulse frequency. Therefore, Administrator should expect a delay before displaying the data

#### 4.2.1.3.1 Graphics

These graphic gives an overw iew of the current RAM, CPU and T° levels.



#### 4.2.1.3.2 Application Running

The section below displays the list of applications running along with their Process ID and Memory Footprint.

Applications running			
Pid	Name	File Name	Memory (Ko)
1292	vservc	C:\Windows\System32\vservc.exe	1332
352	tvnservr	C:\Program Files\TightVNC\TVNServer.exe	7300
164	svchost	C:\Windows\system32\svchost.exe	2460
1772	KeyboardSurrogate	C:\Program Files\Common Files\Microsoft Shared\Ink\KeyboardSurrogate.exe	13212
880	csrss	[77]C:\Windows\system32\csrss.exe	1744
968	lsass	C:\Windows\system32\lsass.exe	4096
1588	EloService	C:\Program Files\Elo TouchSystems\EloService.exe	2140
1140	svchost	C:\Windows\system32\svchost.exe	2940
956	services	C:\Windows\system32\services.exe	1820
2304	svchost	C:\Windows\System32\svchost.exe	1828
1784	svchost	C:\Windows\system32\svchost.exe	2848
2196	mqdgvic	C:\Windows\system32\mqdgvic.exe	1496
3440	vmiprvse	C:\Windows\system32\wbem\vmiprvse.exe	2724
1568	clsvic	C:\Windows\system32\clsvic.exe	2552

#### 4.2.1.3.3 Services Running

The section below displays the entire list of services with their live status.

Services running				
Name	Description	Path	StartMode	Started
IPv6 Helper Service	Provides DNS name registration and automatic IPv6 connectivity	C:\Windows\system32\svchost.exe -k netvcs	Auto	✓
Alert	Notifies selected users and computers of administrative alerts. If the	C:\Windows\system32\svchost.exe -k LocalService	Disabled	✗
Application Layer Gateway Service	Provides support for 3rd party protocol plug-ins for Internet Conn	system32\alg.exe	Manual	✓
Application Management	Provides software installation services such as Assign, Publish, and	C:\Windows\system32\svchost.exe -k netvcs	Manual	✗
ASP.NET State Service	Provides support for out-of-process session states for ASP.NET. If	C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_state.e	Manual	✗
Windows Audio	Provides support for Windows Audio functions.	C:\Windows\System32\svchost.exe -k netvcs	Auto	✓
Background Intelligent Transfer S	Uses idle network bandwidth to transfer data.	system32\svchost.exe -k netvcs	Manual	✗
Computer Browser	Maintains an updated list of computers on the network and supplie	C:\Windows\system32\svchost.exe -k netvcs	Auto	✓
Indexing Service	Indexes contents and properties of files on local and remote compi	C:\Windows\system32\clbcatq.exe	Auto	✓
ClipBook	Supports ClipBook Viewer, which allows pages to be seen by remc	C:\Windows\system32\clbcatq.exe	Disabled	✗
.NET Runtime Optimization Servi	Microsoft .NET Framework NGEN	c:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe	Manual	✗
COM+ System Application	Manages the configuration and tracking of Component Object Mo	C:\Windows\system32\clbcatq.exe /Processid:{02D483F1-FD68-11	Manual	✗
Cryptographic Services	Provides key management services for this computer.	C:\Windows\system32\svchost.exe -k netvcs	Auto	✓
DCOM Server Process Launcher	Provides launch functionality for DCOM services.	C:\Windows\system32\svchost.exe -k DcomLaunch	Auto	✓
DHCP Client	Manages network configuration by registering and updating IP ad	C:\Windows\system32\svchost.exe -k netvcs	Auto	✓

#### 4.2.1.4 Tools

In order to check the network connectivity from the Device to a specific URL, Xcalibur-W Server enables to execute and to return the output of the **PING** and **TRACERT** Commands. The corresponding results are then stored within the **Command Result Window**

**Launch specific command**

*This module enables to send a Ping request or analyze the network route from the device to a remote host and to display the output on the web interface.*

Command to use ☒ ping ☐ tracert

Host

Example: www.wan-pulse.com, 192.168.2.1

Timeout

**Launch**

### 4.2.2 Apps Configuration

#### 4.2.2.1 Configuration Connections

When using Thin Client devices, Administrator is able to create connections to remote hosts using IE, RDP, ICA and VMWare clients. These connections can then be deployed to other Devices using the **Clone Configuration** function.

**Configuration Connections**

*This module enables to create connections to remote hosts using IE, RDP, ICA and VMWare clients.*

Name	Type	Auto Start	Shell
		✗	✗

**New** **Edit** **Delete**

To add a new connection, click on **New** and fill the appropriate fields in the **Connection Parameters** section.

Some optional settings are provided in order to customize the behaviour while executing the connection.

<div> <div>Configuration Connections</div> <div>This module enables to create connections to remote hosts using IE, RDP, ICA and VMware clients.</div> <div> <div>Connection Name</div> <div>RDP1</div> </div> <div> <div>Connection Type</div> <div>RDP</div> </div> <div> <div>Connection Parameters</div> <div> <div>Default</div> <div>Advanced</div> </div> <div> <div>Hostname</div> <div>RDPserver.corporate.com</div> </div> <div> <div>Port</div> <div>3389</div> </div> <div> <div>Login</div> <div>user1</div> </div> <div> <div>Password</div> <div>*****</div> </div> <div> <div>Domain</div> <div>ad.corporate.com</div> </div> </div> <div> <div>Execution Settings</div> <div> <div>Create shortcut on Desktop</div> <div><input type="checkbox"/></div> </div> <div> <div>Create shortcut in Startmenu</div> <div><input type="checkbox"/></div> </div> <div> <div>Autostart connection</div> <div><input type="checkbox"/></div> </div> <div> <div>Auto reconnect connection</div> <div><input type="checkbox"/></div> </div> <div> <div>Replace Shell</div> <div><input type="checkbox"/></div> </div> <div> <div>Fallover</div> <div></div> </div> <div> <div>Working Directory</div> <div></div> </div> <div> <div>Arguments</div> <div></div> </div> </div> <div> <div>Save</div> <div>Cancel</div> </div> </div>		<div>Create shortcut on Desktop</div> <div>The connection icon is displayed on the User's Desktop</div> <div>Create shortcut in Startmenu</div> <div>The connection icon is attached to the Window s Start Menu</div> <div>Autostart connection</div> <div>The connection w ill be started automatically w hen Device boots up</div> <div>Auto reconnect connection</div> <div>The connection w ill be restarted if/w hen it is stopped</div> <div>Replace Shell</div> <div>The Window s Shell Explorer w ill be replaced by the connection</div> <div>Failover</div> <div>When the connection stops, the connection specified in this field gets started automatically</div> <div>Working Directory</div> <div>This defines the Working Directory for the connection</div> <div>Arguments</div> <div>This allow s to specify additionnal parameters to the connection</div>
---	--	--

Once saved, the connection w ill then appear in the Connection Manager as below

Name	Type	Auto Start	Shell
RDP1	RDP	✖	✖

## 4.2.3 User Experience

### 4.2.3.1 Screen Saver

This section lists the **Screen Savers** available on the Device and enables to configure the default one.

ScreenSaver

This module enables to configure the ScreenSaver settings

Screen Saver status

☐ Enable
 ☒ Disable

Timeout (seconds)

900

Available on the device

logon.scr  
scrnsave.scr  
ss3dfo.scr  
ssbezier.scr  
ssflwbox.scr

Apply



## 5 Library

### 5.1 Task Templates

Whenever you create a new task comprising a series of commands, you have the choice to publish it immediately to devices or groups, or to save the task to the library for later use.

Library	Name	Date Created	Nb commands
Task Templates	config souris clavier	6/21/2013 10:15:11 AM	4
	task instal 1	6/21/2013 9:31:23 AM	9
Recurring Tasks	test sleep	6/20/2013 2:31:45 PM	5
Monitoring Rules	maintenance + inventaire + diag	6/18/2013 11:11:19 PM	4
Downloads	rask dir bit	6/15/2013 10:46:07 AM	1
Uploads	del dir	6/15/2013 10:46:23 AM	1
	task 2	6/14/2013 10:34:10 PM	6

Tasks stored in the library can then be published or edited at a later stage by double clicking on them or right-clicking and selecting LOAD from the context menu.

### 5.2 Recurring Tasks

This section of the library displays the recurring tasks that you have defined from the Command Queue.

Library	Status	Task	Active	Frequency	Recurrence Unit	Next Occurrence	Publish Start	Publish End
Task Templates								
Recurring Tasks		reboot toute les 30 mins	Inactive	30	Minutes		6/18/2013 11:10:02 PM	6/20/2013 8:27:36 PM
		maintenance + inventaire + diag	Active	1	Hours		6/18/2013 11:09:24 PM	6/22/2013 8:27:36 PM
Monitoring Rules		inventaire tous les jours	Inactive	1	Days		6/18/2013 9:00:28 AM	6/21/2013 8:27:36 PM
Downloads		attente	Inactive	2	Minutes		6/18/2013 9:25:23 PM	6/18/2013 9:50:29 PM
Uploads		rask dir bit	Inactive	8	Minutes		6/15/2013 10:47:43 AM	6/17/2013 6:00:00 AM
		task 2	Inactive	20	Minutes		6/15/2013 10:42:10 AM	6/17/2013 6:00:00 AM

Once a recurring task is published, then Xcalibur-W Server automatically create and publish occurrences of the task according to the recurrency settings that have been defined. Occurences of the task are displayed within the Task Board and can be identified thanks to the Recurrency icon

6/23/2013 7:24:58 PM		install chrome ext				0	4	0	
6/23/2013 6:14:58 PM		Frequency : 70 Minutes				0	4	0	
6/23/2013 5:04:58 PM		Publish Start : 6/23/2013 12:24:58 PM				0	4	0	
6/23/2013 3:54:58 PM		Publish End : 6/24/2013 7:00:00 AM				0	4	0	
6/23/2013 2:44:58 PM		Next Occurrence : 6/24/2013 5:54:58 AM				0	4	0	

All Recurring Tasks are stored within the library. They can be paused or removed manually using the context menu. The Status of the Recurring is detailed as below :

<b>Status</b>	In Progress: The task is active and has not been manually paused Paused : The task is active but has been manually paused Terminated : The task execution time window is terminated
<b>Active</b>	If Active, the task is still in its execution time window

<b>Next Occurrence</b>	Displays the expected execution time for the next occurrence of the recurring task
------------------------	--

### 5.3 Monitoring Rules

The Monitoring Rules section is the storage location within the library for the rules that have been created. From this location you can create, edit, remove the rules.

Library	Rule Name	Status	Date Created	Devices
Task Templates				
Recurring Tasks	fbwrf cache < 20Mb	Enabled	6/26/2013 2:38:25 PM	2
Monitoring Rules	esapce libre	Enabled	6/26/2013 12:13:33 PM	7
Downloads	tache cle de registre	Enabled	6/24/2013 3:34:38 PM	3
Uploads	temperature MB	Enabled	6/26/2013 11:54:48 AM	8
	test disque	Disabled	6/21/2013 11:26:11 AM	6
	test fichier test.bit	Enabled	6/20/2013 3:28:31 PM	2



For further information regarding Monitoring, please refer to the Monitoring and Preventive Maintenance chapter

### 5.4 Downloads

The Downloads section is the storage location within the library for files that have been downloaded from the devices. From this location you can choose to save the file to your local file system.

### 5.5 Uploads

We can see all the uploaded files in this part.

Library	Filename	Date Uploaded	Description	State	Size
Task Templates	SkypeSetup_6.3.0.105.msi	6/19/2013 9:36:18 PM		Available	19.6 Mb
Recurring Tasks	Eyes-with-water-creative-close-up_1680x1050.jpg	6/19/2013 9:35:58 PM		Available	598.3 Kb
Monitoring Rules	DsAtj.jpg	6/19/2013 9:35:48 PM		Available	18.3 Kb
Downloads					
Uploads					


Upload file

File to upload :

Select a file...

File description

Upload

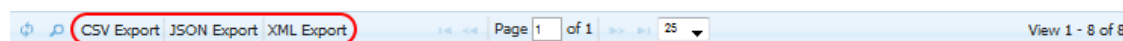
Whenever you need to upload files to devices through a task command, you will need to ensure it is first uploaded into this section of Xcalibur-W Server. To upload a file is simple. Simply click on the  icon on the status bar and you will be presented with a file upload dialog.

## 6 Reporting Services

### 6.1 Quick Export of Device List

There are occasions when Administrator wants to export Device data outside of the Software. This can be the case for Reporting or Asset management purposes.

Xcalibur-W Server allow s to quickly extract data from the current **Device List View** and export them into various file format.



There are three supported file format

<b>CSV</b>	A Comma-Separated Value (CSV) file stores tabular data (numbers and text) in plain-text form. (Opened with Excel or a similar software)
<b>JSON</b>	JSON, or JavaScript Object Notation, is a text-based open standard designed for human-readable data interchange. It is derived from the JavaScript scripting language for representing simple data structures and associative arrays, called objects.
<b>XML</b>	Extensible Markup Language (XML) is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. (Opened in a web browser)

Once you click on the Export button, then you can save the file onto your computer.

### 6.2 Create Custom Reports

Xcalibur-W Server collects and centrally store data from Devices onto its Database. These information are available within the existing views of the software, however they might not be in the desired form and format.

**Reporting Services** offers a mean to select and export Device data according to **Layouts** and **Filters**. The output of these data can be CSV, XML and JSON as for the Quick Export of Device List.

#### 6.2.1 Columns Layout

A Layout is an ordered list of items that defines the structure of data that are intended to be extracted from the database. There are 5 default layouts that are provided as templates. They can not be edited nor deleted.

Reporting Services	Entity	Locking	Layout name	Description
Columns Layouts				
Filters	Agent		Devices List	The default layout of Devices List View
File Export	Agent		Application Inventory	List the application names and versions of all enrolled devices
	Agent		Device Agent Info	List data related to Agent communication
	Agent		Enrollment List	The default layout of Enrollment List View
	Agent		Hardware Inventory	List all hardware information per device

You can add a custom layout by clicking on the button, this requires an advanced know ledge of the system.

Entity Agent

Name

Description

Fields 

Field
-------

Add field

Field

Save

Save

Cancel

## 6.2.2 Filters

A Filter is an ordered list of criteria that are used to refine the data that shall be extracted from the database. There are 5 default filters that are provided as templates. They can not be edited nor deleted.

Reporting Services	Entity	Locking	Filter name	Description
Columns Layouts				
Filters	Agent		Online Devices	Filters by Online status
File Export	Agent		Offline Devices	Filters by Offline status
	Agent		Last Inventory	Filters devices whose Inventory is solder than specific date
	Agent		Application Filter	Filters devices featuring Device Agent application (as example)
	Agent		Last Pulse Filter	Filters devices that have not contacted Management Server since specific date

You can add a custom filter by clicking on the button, this requires an advanced know ledge of the system.



Entity:

Name:

Description:

Criteria:

Field	Operator	Inverse	Value
<div> <div>Add criterion</div> <div>Field: <input type="text"/></div> <div>Operator: <input type="text" value="Equals"/></div> <div>Inverse: <input type="checkbox"/></div> <div>Value: <input type="text"/></div> <div>Save</div> </div>			

Save Cancel



You can refer to Advanced Reporting section in order to get a better understanding of Layout and Filter syntax

## 6.2.3 File export

Entity:

Select Layout:

Select Filter:  ☐ Limit to Enrolled Devices

Export format:

File Name:

WebService URL:

Export

By selecting the required Layout and/or Filter, you can generate the output file in the desired format. By default, the output is restricted to Enrolled Devices. However, by unselecting the checkbox, you can extend the Un-enrolled Devices.

Once you click on **Export** button, you will be prompted to open or save the file.

## 6.3 Advanced Reporting with Webservices

Xcalibur-W Server provides a Web Service in **REST** format for data collection over the network. The Web Service allows to use requests that can be used by a third-party software (including Excel).

Entity:

Select Layout:

Select Filter:  ☐ Limit to Enrolled Devices

Export format:

File Name:

WebService URL:

Export

When exporting a file using the Custom Exports, the corresponding Web Service request is automatically displayed within the URL field. Thus, the request can be used "as is" or modified.



Please note that WebServices shall be properly configured on the IIS Server to be functional. Refer to Setting Up WebServices Section for more details

The Web Service syntax is described below .

**https://<manager-ip> : <webservice-port> /ws/ <entity> . <export-format>  
?projections=<projections-list> &orders=<orders-list> &groups=<groups-list> &  
<criteria-list>**

manager-ip	Xcalibur-W Server IP adress or DNS name
w ebservice-port	Port used by the w ebservice in the Xcalibur-W Server
entity	Request's entry point
export-format	Export format of the request
projections-list	Projections list separated by commas
orders-list	order-by list separated by commas
groups-list	group-by list separated by commas
criteria-list	criteria list with a criteria = an URL parameter



You can modify the request directly in the URL field. Below is an example where we are changing the value of the filter for the Last Pulse date.

Example :

- **Original:** the output list will only feature the Devices that **have not contacted** Xcalibur-W Server since 14/06/2013 (Last Pulse Date):  
https://srv1.xcaliburw.com:444/ws/agents.csv?projections=IsOnline,MachineName,Networks.MacAddress,Inventory.Computer.Model,Inventory.OperatingSystem.OsName,DeviceAgentVersion,Networks.IpAddress,Networks.NetworkAddress,WriteFilter,IsInPersistence,LastPulse&LastPulse=LessThan(14/06/2013 21:54:45)&EnrollementState=1
- **Modified,** the output list will only feature the Devices that **have contacted** Xcalibur-W Server since 14/06/2013 (Last Pulse Date):  
https://srv1.xcaliburx.com:444/ws/agents.csv?projections=IsOnline,MachineName,Networks.MacAddress,Inventory.Computer.Model,Inventory.OperatingSystem.OsName,DeviceAgentVersion,Networks.IpAddress,Networks.NetworkAddress,WriteFilter,IsInPersistence,LastPulse&LastPulse=GreaterThan(15/06/2013 21:54:45)&EnrollementState=1

## 7 Monitoring and Preventive Maintenance




### 7.1 Overview

Xcalibur-W Server feature a powerful and flexible **monitoring engine** - based on Rules and Triggers - which is executed on Client Devices. Rules enable to generate Alerts that are sent to the Management Server whenever a specific event occurs on the Client Device. Therefore, Administrator gets automatically informed of any dysfunctions on the equipments.

Additionally, Xcalibur-W Server is able to execute Preventing Tasks once an Alert is received eliminating the need to perform manual interventions.

From the **Device List View**, Administrator can see a counter of raised alerts.

These Alerts are classified using color code reflecting the event's severity.

High Level Alert	Normal Level Alert	Low Level Alert
		

Monitoring Rules are stored within the library. Administrator will need to create rules first and then deploy them to target Devices.

### 7.2 Rules and Creating Rules

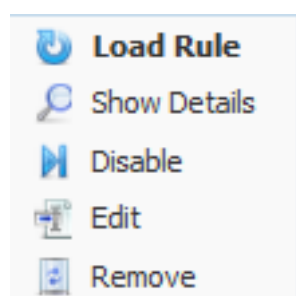
#### 7.2.1 Monitoring Rules View and Context Menu

From the Library, within the **Monitoring Rules** section, you see all the rules already created.


Library	Rule Name	Status	Date Created	Devices
Task Templates				
Recurring Tasks				
Monitoring Rules	fbwif cache < 20Mb	Enabled	6/26/2013 2:38:25 PM	2
	espace libre	Enabled	6/26/2013 12:13:33 PM	7
	tache cle de registre	Enabled	6/24/2013 3:34:38 PM	3
Downloads	temperature MB	Enabled	6/26/2013 11:54:48 AM	8
Uploads	test disque	Disabled	6/21/2013 11:26:11 AM	6
	test fichier test.txt	Enabled	6/20/2013 3:28:31 PM	2

This page lists the Rule Name, the status (Enabled or Disabled), the date of creation, and lastly the number of devices to which this rule applies.

You can access **Context Menu** by right-clicking on any of the rule:



- **Load Rule** : Allows to assign the rule to a selection of devices. The Monitoring Rule is then loaded in the Command Queue as for any Task and can be publish to devices
- **Show Details** : Display the rule details including the triggers, the polling frequency, the list of devices to w ho this rule applies...


**Rule Details - test 1**

Status :

Enabled

Devices :

2

Polling frequency :

2 Minutes

Maintenance Task :

None

Trigger	Operator	Invert	Value	Parameters
sys.reg.key	=	false	test1	HKEY_LOCAL_MACHINE\
sys.partition.freespace	<	true	10%	c

Hostname

Ip Address

testC27D7524916	192.168.2.177
testmayB310204D	

Page 1 of 1

25

View 1 - 2 of 2

- **Disable** : Disables the rule for all the devices to who this rule applies
- **Edit** : Allow s to modify the parameters of the rule
- **Remove** : Deletes the rule

### 7.2.2 Create new Monitoring Rule

You can create a new Monitoring Rule by clicking on the  button, in the bottom of the screen.

Create new Monitoring Rule

Rule Name

Conditions list

Trigger	Operator	Invert	Value	Parameters

Severity

Polling frequency  Minutes

Maintenance Task

Enabled ☒

Creating the rule requires to define trigger(s) which shall be used. You can choose and combine several **triggers** which form all together the Conditions list. All available triggers are detailed in the **Triggers Glossary**.

As an option, Xcalibur-W Server allows to assign a maintenance task to a particular rule. This feature enables to automatically execute a task once an alert is raised. A **Maintenance Tasks** can be any of the tasks in the Task

Templates section.

### 7.2.3 Load Rule

To assign a rule to devices, you shall load it in the Command Queue by clicking on **Load Rule** from Context Menu, or just double-clicking on the rule. A new Command named **Monitoring Rule** is added to Command Queue and you then just have to publish this Task to your selection of devices. More informations on **Publishing Tasks**.



The Rules are stored within the filesystem of the device, within an unprotected area - part of the FBWF Exclusions List.



As for any Tasks, if your devices are protected by an EWF Write Filter, you need to activate/deactivate Maintenance mode in your Task, otherwise the Rule may not persist onto the devices

## 7.3 Triggers Glossary

---

The list below describes all available triggers that can be monitored on the Client Device.

### 7.3.1 sys.reg.key

---

#### **Definition**

This trigger allows to monitor the registry key name

#### **Operator**

= ; Contains

#### **Value**

The new name of the registry key

#### **Parameters**

Specify the path of the existing registry key

#### **Example**

I would like to be notified when 'my\_key' will be renamed 'my\_new\_key'.

*Operator : = Value : 'my\_new\_key' Parameters :  
'HKEY\_LOCAL\_MACHINE\Software\my\_key'*

### 7.3.2 sys.reg.value

---

#### **Definition**

This trigger allows to monitor the value of a specified registry key.

#### **Operator**

= ; Contains

**Value**

String value

**Parameters**

Specify the path of the registry key

**Example**

I would like to be notified when 'HKEY\_LOCAL\_MACHINE\Software\my\_key\one\_value' takes for value 'XYZ'

```
Operator : = Value : XYZ Parameters :  
HKEY_LOCAL_MACHINE\Software\my_key\one_value
```

### 7.3.3 sys.regedit

---

**Definition**

This trigger allows to monitor whether a specified registry key exists or not

**Operator**

=, Contains

**Value**

True for existing, False for unexisting

**Parameters**

Specify the path of the registry key

**Example**

I would like to be notified when the registry key 'my\_key' exists.

```
Operator : = Value : true Parameters :  
HKEY_LOCAL_MACHINE\Software\WanPulse\my_key
```

### 7.3.4 sys.gen.result

---

**Definition**

This trigger allows to monitor the output of a shell command, may it be a windows command or a custom script

**Operator**

= ; Contains

**Value**

String value

**Parameters**

Specify the command to use

**Example**

I would like to be notified when a Ping command doesn't lose any packets

*Operator : Contains Value : 0% Loss Parameters : ping www.google.fr*

### 7.3.5 sys.serv.started

---

**Definition**

This trigger allows to monitor the current state of a specified service (Started/Stopped).

**Operator**

= ; Contains

**Value**

True for started, False for stopped

**Parameters**

Specify the name of the service

**Example**

I would like to be notified when the Windows Audio service is started

*Operator : = Value : True Parameters : Windows Audio*

### 7.3.6 sys.partition.freespace

---

**Definition**

This trigger allows to monitor the freespace of a specified disk partition

**Operator**

All applicable

**Value**

Numerical value followed by the unit %, Kb, Mb or Gb

**Parameters**

Specify the partition letter

**Example**

I would like to be notified when the freespace on C: partition is lesser than 10% of the total partition size

*Operator : < Value : 10% Parameters : C*

### 7.3.7 sys.diskdrive.health

---

**Definition**

This trigger allows to monitor the health of Smart-enabled hard disk drive

**Operator**

= ; Contains

**Value**

OK ; Error ; Degraded ; PredFail

**Parameters**

Not Applicable

**Example**

I would like to be notified when the health of hard disk drive is degraded

*Operator : Contains Value : Degraded Parameters :*

### 7.3.8 sys.temperature

---

**Definition**

This trigger allows to monitor the motherboard system temperature

**Operator**

All applicable

**Value**

Numerical value followed by the unit °C (default) or °F

**Parameters**

Not Applicable



**Example**

I would like to be notified when the motherboard temperature is greater than 50°C

*Operator : > Value : 50°C Parameters :*

### 7.3.9 file.create

---

**Definition**

This trigger allows to monitor the creation of a specified file or directory

**Operator**

= ; Contains

**Value**

The location of specified file or directory

**Parameters**

Specify the path of the file or directory

**Example**

I would like to be notified when the file 'xcaliburw.txt' is created on C:\

*Operator : Contains Value : C:\xcaliburw.txt Parameters : C:\*

### 7.3.10 file.size

---

**Definition**

This trigger allows to monitor the size of a specified file

**Operator**

All Applicable

**Value**

Numerical value followed by the unit Kb, Mb or Gb

**Parameters**

Specify the path of the file

**Example**

I would like to be notified when the file size of my\_file.txt is greater than 1 Gb

*Operator : > Value : 1 Gb Parameters : c:\Users\Admin\Desktop\my\_file.txt*

### 7.3.11 file.exist

---

**Definition**

This trigger allows to monitor whether a specified file or directory exists or not

**Operator**

= ; Contains

**Value**

True for existing, False for unexisting

**Parameters**

Specify the path of the file or directory

**Example**

I would like to be notified if the file c:\Windows\explorer.exe does not exist

*Operator : = Value : false Parameters : c:\Windows\explorer.exe*

### 7.3.12 writefilter.cachesize.current

---

**Definition**

This trigger allows to monitor the cache size of the FBWF Write Filter

**Operator**

All applicable

**Value**

Numerical values followed by the unit %, Kb, Mb or Gb

**Parameters**

Not applicable

**Example**

I would like to be notified when the cache size exceeds 90 Mb

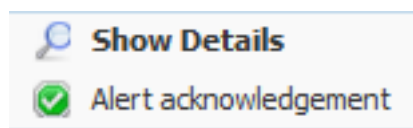
*Operator : >  
Value : 90 Mb  
Parameters :*

## 7.4 Alerts

The **Alerts View** within the **Monitoring** section provides an instant access of all Alerts logs. Each Alert is summarized with date, severity, device affected, rule name, task performed if exists.

Monitoring	Alert Date	Severity	Hostname	Rule Name	Task	Ack
Alerts view						No
	6/30/2013 9:43:13 AM		testmay7D10C755	temperature MB		
	6/30/2013 9:39:12 AM		testmay7D10C755	temperature MB		
	6/30/2013 9:35:10 AM		testmay7D10C755	temperature MB		
	6/30/2013 9:31:10 AM		testmay7D10C755	temperature MB		
	6/30/2013 9:27:09 AM		testmay7D10C755	temperature MB		
	6/30/2013 9:23:07 AM		testmay7D10C755	temperature MB		

Alert can be acknowledged by right-clicking and selecting **Alert acknowledgement**.



By double clicking, you can get details on the alert including the triggers, the values and parameters as well as the reported result.

As an example, the screenshot below describes an Alert on Device Temperature which exceeds the 40°C threshold.

Alert Details - temperature MB - 6/30/2013 9:35:10 AM			
Hostname :	testmay7D10C755	Ip Address :	192.168.2.233
Polling frequency :	4	Maintenance Task :	None
Conditions		Result	
Trigger :	sys.temperature	48°C	
Operator :	>		
Invert :	False		
Value :	40°C		

## 8 Manager Options

### 8.1 Settings

The Settings section within the Manager Options allows administrators to set specific parameters that may be required within the organization. A selection of these is shown below.

**Options**

**Settings**

**Users**

**Current Settings**

Temporary Folder: Temp

Type of Authentication: Local

**General**

Temporary Folder: Temp

Apply

**SSL Certificate**

Name	Devices	Serial Number	Expiration	Status
	8/8	64A1D6247A67E8A94ADD5EF4861BF8F8	8/25/2022 10:24:50 AM	✓
vxl.net	0/8	0C1E2C	6/21/2014 12:47:19 PM	

**Authentication**

☒ Local

☐ Active Directory

Apply

**VNC Proxy**

VNC Proxy automatic close (in min) [0 : disabled]: 0

**Range of ports (Java Viewers)**

Start port: 5900

End port: 5919

**Range of ports (Agents connections)**

Start port: 5980

End port: 5999

Remove all VNC sessions Apply

#### 8.1.1 General

The General panel contains the following parameter fields.

**General**

Temporary Folder: Temp

Apply

**SSL Certificate**

Name	Devices	Serial Number	Expiration	Status
	8/8	64A1D6247A67E8A94ADD5EF4861BF8F8	8/25/2022 10:24:50 AM	✓
vxl.net	0/8	0C1E2C	6/21/2014 12:47:19 PM	

#### Temporary Folder

Specifies the location where temporary files will be stored. The default setting is: TEMP.

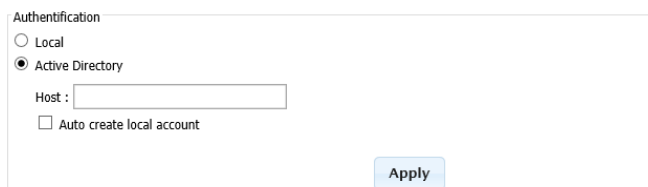
#### SSL Certificate

This tab should be populated with the license number of your SSL certificate(s) as stored and used within IIS. The serial number can be found by going to the SSL Certificate area within IIS and double clicking on the certificate listing.

### 8.1.2 Authentication

---

This panel contains the settings that concern authentication systems used for administrator access to Xcalibur-W Server.



The Authentication panel shows two radio buttons: 'Local' and 'Active Directory'. 'Active Directory' is selected. Below it is a 'Host' text field and an 'Auto create local account' checkbox. An 'Apply' button is at the bottom right.

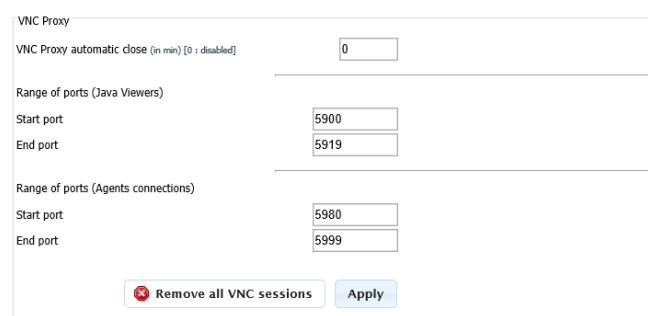
When you enter the IP address of the AD server into the Host field all authentication is done toward the AD server. However, if the account name does not exist on the local database the authentication is rejected even though it may be correct in terms of password.

So when you need to use Active Directory as the means of authentication the best method is to tick the Auto Create Local Account checkbox and ask your Xcalibur-W Server users to log in. Once they have successfully logged in you can then untick this box. The result of this action is to add the AD user name to the local database but not store any password information. Instead it is used as a reference to ensure that the AD user is allowed to authenticate on Xcalibur-W Server.

### 8.1.3 VNC Proxy

---

The VNC Proxy panel contains a number of settings that allow you to manipulate how the VNC system used to shadow desktops for remote assistance. For more details of how Reverse VNC Proxy works please see the appropriate section.



The VNC Proxy panel includes a 'VNC Proxy automatic close (in min) [0 : disabled]' field set to 0. It also has two sections for port ranges: 'Range of ports (Java Viewers)' with start port 5900 and end port 5919, and 'Range of ports (Agents connections)' with start port 5980 and end port 5999. At the bottom are 'Remove all VNC sessions' and 'Apply' buttons.

#### VNC Proxy Automatic Close

This setting is used to set the number of minutes that the VNC Proxy connection will be allowed to stay open once the VNC session has been closed. A setting of 0, the default will keep the proxy connection open indefinitely.

## Range of Ports (Java Viewers)

Use this setting to customize the port range used by Java VNC viewers that will be launched by your browser when you initiate a reverse VNC session. The default values are Start=5900 and End=5919.

## Range of Ports (Agent Connection)

Use these settings to determine what port range will be used when the Device Agent connects to the Xcalibur-W Server in order to set up the Reverse VNC Proxy connection. The default values are Start=5980 and End=5999.

## 8.2 Users

The Xcalibur-W Server has the capability to allow a number of users to connect to it in order that they may manage devices. Users can be defined locally or Xcalibur-W Server can connect to Active Directory to allow AD authenticated login.

Options	Users Name	First Name	Last Name	Email	Create Date	State
Settings	admin	System User		admin@local.domain	6/14/2013 9:54:45 PM	Enable
Users	demomanager	System User		admin@local.domain	6/14/2013 9:54:45 PM	Enable
	demouser	System User		admin@local.domain	6/14/2013 9:54:45 PM	Enable




### 8.2.1 Adding a User

To add a user click the ADD button located on the status line at the bottom of the right side of the Users page. The right hand panel will change to something similar to the image below :

You will have noticed that you can provide a level of granular permissions to the user you are adding. These permission levels allow you to restrict the level of access that the user is provided with. Fill in the details as per your requirements and click the SAVE button.

### 8.2.2 Deleting a User

To delete a particular user simply right click on the user entry and select Delete from the context menu.

Options	Users Name 	First Name	Last Name	Email	Create Date	State
	admin	System User		admin@local.domain	6/14/2013 9:54:45 PM	Enable
	demomanager	System User		admin@local.domain	6/14/2013 9:54:45 PM	Enable
	demouser	System User		admin@local.domain	6/14/2013 9:54:45 PM	Enable
	<div><div> Manage</div><div> Delete</div></div>					

## 9 Advanced

---

### 9.1 Update Client Agent

---

In the current Xcalibur-W Server version, the Client Update is being done using an external FTP server which acts as repository for Client Agent update instructions. The repository shall contain at least the XML infoversion file which specifies the target version and the exact path to the new Client Agent. The new Client Agent binary can be stored on the same FTP server, or can be stored on a remote server (SMB, HTTP, FTP...).

#### 9.1.1 Things to know

---

##### When the Device is not enrolled:

- If there is **no Write Filter** activated then the update of Device Agent is done silently for the user without any reboot
- If protected by a **FBWF Write Filter**, then a message pops up informing the user that the Device will turn automatically into Maintenance Mode to start the update, thus will reboot.



Due to Writer Filter protection, the Agent Update will not work on a Device that has EWF activated

##### When the Device is enrolled:

- If there is **no Write Filter** activated, then the update of Device Agent is done silently for the user without any reboot
- If protected by **EWF or FBWF Write Filter**, then the device shall be turned into the Maintenance state.

#### 9.1.2 Preparing FTP Server

---

The FTP Server shall contain the infoversion.xml file. Infoversion.xml file shall be written as shown below :

```
<?xml version="1.0" encoding="UTF-8"?>
  <Info>
    <Imaging>
      <Version>0.0.0</Version>
      <Path>image15032011</Path>
    </Imaging>
    <Profil>
      <Version>0.0</Version>
      <Path>Profil0.2.txt</Path>
    </Profil>
    <Agent>
```



```

<Version>1.3.6.572</Version>
<Path>ftp://anonymous:test@192.168.1.10/DeviceAgent_1.3.6.572.exe</Path>
</Agent>
</Info>

```

<b>Version</b>	Specifies the new Client Agent version. If installed version is new er than the specified one, then the update w ill not be executed
<b>Path</b>	Specifies the exact path to the new Client Agent

### 9.1.3 Preparing Device Agent

As it uses FTP as a mean for the update, Device agent shall be configured with the FTP server address and credentials. This can be done either by manually entering the settings onto the Agent or using the DHCP Scope options.

#### 9.1.3.1 FTP Server settings provided by DHCP

FTP Server settings can be provided by the mean of the DHCP using Scope Option 230. For more information about the DCHP Option, you can refer to the DHCP Scope Options section.

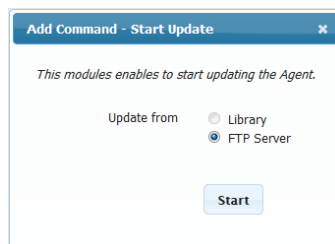
In Device Agent, you shall go in **Administration / Agent Configuration** section in order to allow the DHCP Scope Option by ticking the corresponding checkbox.

#### 9.1.3.2 FTP Server settings provided Manually

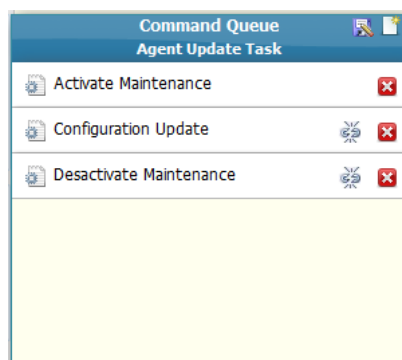
Manual settings can be entered from the **Administration, Agent Update** section. Additionnaly, You can to tick the **Enable automatic FTP updates at startup** in order to check for updates of the Agent at each startup.

### 9.1.4 Starting the Update

The update can be started using the **Agent Update** command.



When executing the update on Write Filter protected devices, then Administrator shall **Activate the Maintenance Mode prior to execute the update** as shown in the Task Template below .



## 9.2 WMIC Command Glossary

<b>baseboard</b>	get Manufacturer, Model, Name, PartNumber, slotlayout, serialnumber, poweredon
<b>bios</b>	get name, version, serialnumber
<b>bootconfig</b>	get BootDirectory, Caption, TempDirectory, Lastdrive
<b>cdrom</b>	get Name, Drive, Volumename
<b>computersystem</b>	get Name, domain, Manufacturer, Model, NumberofProcessors, PrimaryOwnerName, Username, Roles, totalphysicalmemory /format:list
<b>cpu</b>	get Name, Caption, MaxClockSpeed, DeviceID, status
<b>datafile</b>	where name='c:\\boot.ini' get Archive, FileSize, FileType, InstallDate, Readable, Writeable, System, Version
<b>dcomapp</b>	get Name, AppID /format:list
<b>desktop</b>	get Name, ScreenSaverExecutable, ScreenSaverActive, Wallpaper

	/format:list
<b>desktopmonitor</b>	get screenheight, screenwidth
<b>diskdrive</b>	get Name, Manufacturer, Model, InterfaceType, MediaLoaded, MediaType
<b>diskquota</b>	get User, Warninglimit, DiskSpaceUsed, QuotaVolume
<b>environment</b>	get Description, VariableValue
<b>fsdir</b>	where name='c:\\windows' get Archive, CreationDate, LastModified, Readable, Writable, System, Hidden, Status
<b>group</b>	get Caption, InstallDate, LocalAccount, Domain, SID, Status
<b>idecontroller</b>	get Name, Manufacturer, DeviceID, Status
<b>irq</b>	get Name, Status
<b>job</b>	get Name, Owner, DaysOfMonth, DaysOfWeek, ElapsedTime, JobStatus, StartTime, Status
<b>loadorder</b>	get Name, DriverEnabled, GroupOrder, Status
<b>logicaldisk</b>	get Name, Compressed, Description, DriveType, FileSystem, FreeSpace, SupportsDiskQuotas, VolumeDirty, VolumeName
<b>memcache</b>	get Name, BlockSize, Purpose, MaxCacheSize, Status
<b>memlogical</b>	get AvailableVirtualMemory, TotalPageFileSpace, TotalPhysicalMemory, TotalVirtualMemory
<b>memorychip</b>	get BankLabel, Capacity, Caption, CreationClassName, DataWidth, Description, DeviceLocator, FormFactor, HotSwappable, InstallDate, InterleaveDataDepth, InterleavePosition, Manufacturer, MemoryType, Model, Name, OtherIdentifyingInfo, PartNumber, PositionInRow, PoweredOn, Removable, Replaceable, SerialNumber, SKU, Speed, Status, Tag, TotalWidth, TypeDetail, Version
<b>netclient</b>	get Caption, Name, Manufacturer, Status
<b>netlogin</b>	get Name, Fullname, ScriptPath, Profile, UserID, NumberOfLogons, PasswordAge, LogonServer, HomeDirectory, PrimaryGroupID
<b>netprotocol</b>	get Caption, Description, GuaranteesSequencing, SupportsBroadcasting, SupportsEncryption, Status
<b>netuse</b>	get Caption, DisplayType, LocalName, Name, ProviderName, Status
<b>nic</b>	get AdapterType, AutoSense, Name, Installed, MACAddress, PNPDeviceID, PowerManagementSupported, Speed, StatusInfo
<b>nicconfig</b>	get MACAddress, DefaultIPGateway, IPAddress, IPSubnet, DNSHostName, DNSDomain
<b>nicconfig</b>	get MACAddress, IPAddress, DHCPEnabled, DHCPLeaseExpires, DHCPLeaseObtained, DHCPServer
<b>nicconfig</b>	get MACAddress, IPAddress, DNSHostName, DNSDomain, DNSDomainSuffixSearchOrder, DNSEnabledForWINSResolution, DNSServerSearchOrder

<b>nicconfig</b>	get MACAddress, IPAddress, WINSPRIMARYSERVER, WINSSecondaryServer, WINSEnableLMHostsLookup, WINSHostLookupFile
<b>ntdomain</b>	get Caption, ClientSiteName, DomainControllerAddress, DomainControllerName, Roles, Status
<b>nvent</b>	where (LogFile='system' and SourceName='W32Time') get Message, TimeGenerated
<b>nvent</b>	where (LogFile='system' and SourceName='W32Time' and Message like '%timesource%') get Message, TimeGenerated
<b>nvent</b>	where (LogFile='system' and SourceName='W32Time' and EventCode!='29') get TimeGenerated, EventCode, Message
<b>onboarddevice</b>	get Description, DeviceType, Enabled, Status
<b>os</b>	get Version, Caption, CountryCode, CSName, Description, InstallDate, SerialNumber, ServicePackMajorVersion, WindowsDirectory /format:list
<b>os</b>	get CurrentTimeZone, FreePhysicalMemory, FreeVirtualMemory, LastBootUpTime, NumberOfProcesses, NumberOfUsers, Organization, RegisteredUser, Status
<b>pagefile</b>	get Caption, CurrentUsage, Status, TempPageFile
<b>pagefileset</b>	get Name, InitialSize, MaximumSize
<b>partition</b>	get Caption, Size, PrimaryPartition, Status, Type
<b>printer</b>	get DeviceID, DriverName, Hidden, Name, PortName, PowerManagementSupported, PrintJobDataType, VerticalResolution, HorizontalResolution
<b>printjob</b>	get Description, Document, ElapsedTime, HostPrintQueue, JobID, JobStatus, Name, Notify, Owner, TimeSubmitted, TotalPages
<b>process</b>	get Caption, CommandLine, Handle, HandleCount, PageFaults, PageFileUsage, ParentProcessId, ProcessId, ThreadCount
<b>product</b>	get Description, InstallDate, Name, Vendor, Version
<b>qfe</b>	get description, FixComments, HotFixID, InstalledBy, InstalledOn, ServicePackInEffect
<b>quotasetting</b>	get Caption, DefaultLimit, Description, DefaultWarningLimit, SettingID, State
<b>recoveros</b>	get AutoReboot, DebugFilePath, WriteDebugInfo, WriteToSystemLog
<b>Registry</b>	get CurrentSize, MaximumSize, ProposedSize, Status
<b>scsicontroller</b>	get Caption, DeviceID, Manufacturer, PNPDeviceID
<b>server</b>	get ErrorsAccessPermissions, ErrorsGrantedAccess, ErrorsLogon, ErrorsSystem, FilesOpen, FileDirectorySearches
<b>service</b>	get Name, Caption, State, ServiceType, StartMode, pathname
<b>share</b>	get name, path, status
<b>sounddev</b>	get Caption, DeviceID, PNPDeviceID, Manufacturer, status

<b>startup</b>	get Caption, Location, Command
<b>sysaccount</b>	get Caption, Domain, Name, SID, SIDType, Status
<b>sysdriver</b>	get Caption, Name, PathName, ServiceType, State, Status
<b>systemenclosure</b>	get Caption, Height, Depth, Manufacturer, Model, SMBIOSAssetTag, AudibleAlarm, SecurityStatus, SecurityBreach, PoweredOn, NumberOfPowerCords
<b>systemslot</b>	get Number, SlotDesignation, Status, SupportsHotPlug, Version, CurrentUsage, ConnectorPinout
<b>tapedrive</b>	get Name, Capabilities, Compression, Description, MediaType, NeedsCleaning, Status, StatusInfo
<b>timezone</b>	get Caption, Bias, DaylightBias, DaylightName, StandardName
<b>useraccount</b>	get AccountType, Description, Domain, Disabled, LocalAccount, Lockout, PasswordChangeable, PasswordExpires, PasswordRequired, SID