



# **Management Utilities**

V5.15

User Manual

June 2014

© 2014 SyAM Software, Inc.

All rights reserved. SyAM Software and the SyAM Software logo are trademarks of SyAM Software, Inc.  
All other trademarks are the property of their respective owners.

Information contained in this document is assumed to be accurate at the time of publishing. SyAM Software reserves the right to make changes to the information contained in this document at any time without notice.

For additional information, sales, or technical support, contact SyAM Software

[www.syamsoftware.com](http://www.syamsoftware.com)



**This icon represents - Important information to note**



**This icon represents – Here is an example**

## Contents

Chapter 1 - Getting Started .....	6
System Requirements .....	6
User Account Control .....	7
Network Shares .....	8
Firewall and Network Configuration for Windows Client Systems .....	8
Logging Into Management Utilities.....	12
Product Terms.....	14
User Interface Panels .....	14
Groups .....	15
Details Panel .....	16
System Detail Data.....	17
Copy / Move Systems.....	18
Remove Systems .....	19
Copy / Remove Systems from the SyAM Groups .....	19
System Actions (Right-Click Menu) .....	20
The Shutdown Task.....	21
Active Directory Management.....	21
Chapter 2 – Configuring General Settings.....	24
Defining Paths to the Network Shares Used for Deployment .....	24
Setting History Retention .....	24
Adding and Editing Users .....	25
Restricted Access List .....	28
Blackout Calendar .....	29
Wake on LAN URL List.....	30
My Settings .....	33
Chapter 3 – Network Discovery.....	35
Chapter 4 – Using the Unattended Installation Wizard .....	40
Chapter 5 – Client Deployment and Configuration .....	46
Authentication Settings Template - Windows.....	46
Authentication Settings and User Account Control .....	47
Authentication Settings Template – Macintosh OSX.....	48
Authentication Settings Template – Linux and VMWare ESXi .....	49

Client Deployment Template - Windows .....	50
Client Deployment and User Account Control.....	51
Client Deployment Template - Macintosh .....	52
Client Deployment Template - Linux.....	53
Client Deployment Template – VMWare ESXi .....	54
Discovery Template.....	55
Location and Function Template.....	57
Notification Settings Template .....	58
Power Settings Template.....	59
Remote Console Settings Template .....	61
Area Manager IP Address Template.....	62
System Alert Matrix Template.....	63
Wake on LAN Template .....	64
Chapter 6 – Managing Job Templates and Creating Scheduled Jobs .....	66
Configuring a Job Template.....	66
Adding Tasks to a Job .....	67
Configuring a Schedule .....	69
Copying a Job Template.....	72
Running a Scheduled Job on Target Systems .....	73
Job Filtering Options.....	75
Creating a Scheduled Wake On LAN Job.....	76
Chapter 7 – Microsoft Patch Management .....	80
On-Demand Vulnerability Scan.....	80
Automated Patch Management .....	84
Windows Update Agent .....	91
Chapter 8 - Third Party Application Deployment.....	92
Silent Install Parameters for Third Party Application Deployment Templates .....	95
Chapter 9 - Viewing Scheduled Job Status and History .....	96
Scheduled Jobs.....	96
Job Status .....	97
View History – Audit Trail.....	98
View History – Job Status.....	98
Chapter 10 – Power Auditor .....	99

Discovery Template.....99

Power On Hours Template .....101

Power Audit Wizard .....102

Daylight Saving Time.....103

Groups Section.....104

Power Charts.....105

Reports.....107

At A Glance .....114

Administration Settings.....114

## Chapter 1 - Getting Started

Management Utilities provides IT administrators the ability to automate tasks to sets of systems across the network, enabling them to perform more tasks efficiently and remotely with fewer resources.

- System Client deployment
- Silent deployment of third party applications to groups of systems across the network
- Vulnerability scanning and patch management
- Group Change Management
- User definable scheduling of jobs
- BIOS update deployment to target systems across the network

## System Requirements

To successfully install, configure and use SyAM Management Utilities you will need a system that has the following requirements met:

### Operating System

- Windows 2008 Server / 2008R2
- Windows 2012 Server / 2012R2
- Windows 7 Professional / Enterprise
- Windows 8 Professional / Enterprise

### Hardware Platform (x86 or x64)

- 2GB Memory (Recommended 4GB or above)
- 100GB Disk Space
- Ethernet Adapter
- Networking
- Static IP on Local Area Network (LAN)

### Locale and Language

- Language chosen during installation must be the default language for the locale setting of the system on which Management Utilities is being installed

### Database and Web Server

- Microsoft SQL or SQL Express 2008R2 or 2012
- Microsoft Internet Information Server 7 or 8

### Web Browser Support

- Microsoft Internet Explorer 8 or 9
- Mozilla Firefox 7 or newer



**Please note that .NET Framework 3.5 SP1 must be installed before configuring SQL and IIS.**



**Please note that IIS must be cleared of any current web sites to be able to use ports 80 and 443 for Management Utilities before starting the installation procedure.**



The user installing Management Utilities must have administrative rights on the system Management Utilities is to be installed on and must also be a SQL Administrator.



Please note that if you are using SQL Server 2012 or SQL 2012 Express, you must add an additional user, System, to the list of SQL Administrators.

The screenshot shows the 'SQL Server 2012 Setup' window, specifically the 'Database Engine Configuration' step. The window title bar reads 'SQL Server 2012 Setup'. The main heading is 'Database Engine Configuration' with a subtitle 'Specify Database Engine authentication security mode, administrators and data directories.' On the left is a navigation pane with options: Setup Support Rules, Feature Selection, Installation Rules, Instance Configuration, Disk Space Requirements, Server Configuration, Database Engine Configuration (selected), Error Reporting, Installation Configuration Rules, Installation Progress, and Complete. The main area has four tabs: 'Server Configuration' (selected), 'Data Directories', 'User Instances', and 'FILESTREAM'. Under 'Server Configuration', it says 'Specify the authentication mode and administrators for the Database Engine.' There are two radio buttons for 'Authentication Mode': 'Windows authentication mode' (unselected) and 'Mixed Mode (SQL Server authentication and Windows authentication)' (selected). Below this, it says 'Specify the password for the SQL Server system administrator (sa) account.' with two password fields: 'Enter password:' and 'Confirm password:', both containing seven dots. A list box titled 'Specify SQL Server administrators' contains two entries: 'WIN-GO9AEOP54EG\Administrator (Administrator)' and 'NT AUTHORITY\SYSTEM (SYSTEM)'. To the right of the list box is a note: 'SQL Server administrators have unrestricted access to the Database Engine.' At the bottom of the list box are three buttons: 'Add Current User', 'Add...', and 'Remove'. At the very bottom of the window are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.



Detailed information on configuring IIS and SQL before installing Management Utilities is provided in the Getting Started document.

## User Account Control

In environments where Windows machines have User Account Control enabled, some Management Utilities features (including Client Deployment and Third Party Software Deployment) require that the Management Utilities service be run by a domain administrator, rather than by Local System which is the default. To set this configuration on the Management Utilities server, after Management Utilities is installed:

1. Open Administrative Tools – Services

2. Find the service SyAM Management Utility
3. Stop the service
4. Right-click the service and choose Properties
5. Go to the Log On tab
6. Check This account
7. Enter the account name (e.g. MYDOMAIN\Administrator) and password
8. Click OK
9. Start the service

Please refer to the SyAM Tool Tip on Management Utilities Configuration for UAC Environments for further information.

## Network Shares

Network shared directories are used to deploy SyAM System Client, third party applications, and Windows updates. The same credentials used to access client machines must be valid for the network shares. Shares may be located on the Management Utilities server, but this is not required except for Macintosh client deployment. Default path names for applications and for Windows patches are specified on the Administration Settings page. All users should have read and write permissions, as follows:

- Administrator: Read/Write
- Administrators: Owner
- Domain Users: Read/Write
- Everyone: Read/Write

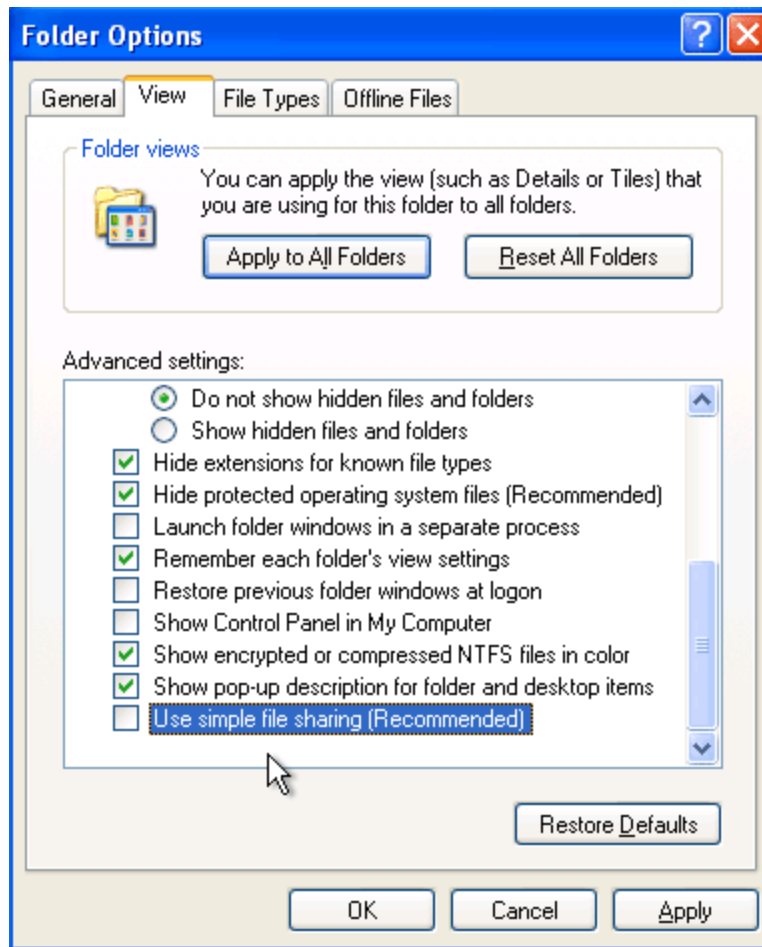
## Firewall and Network Configuration for Windows Client Systems

To install the System Client on Windows XP and Windows 7 systems, the Windows firewall and network settings on the target machines must be configured to allow Management Utilities to discover the systems and deploy the client software.

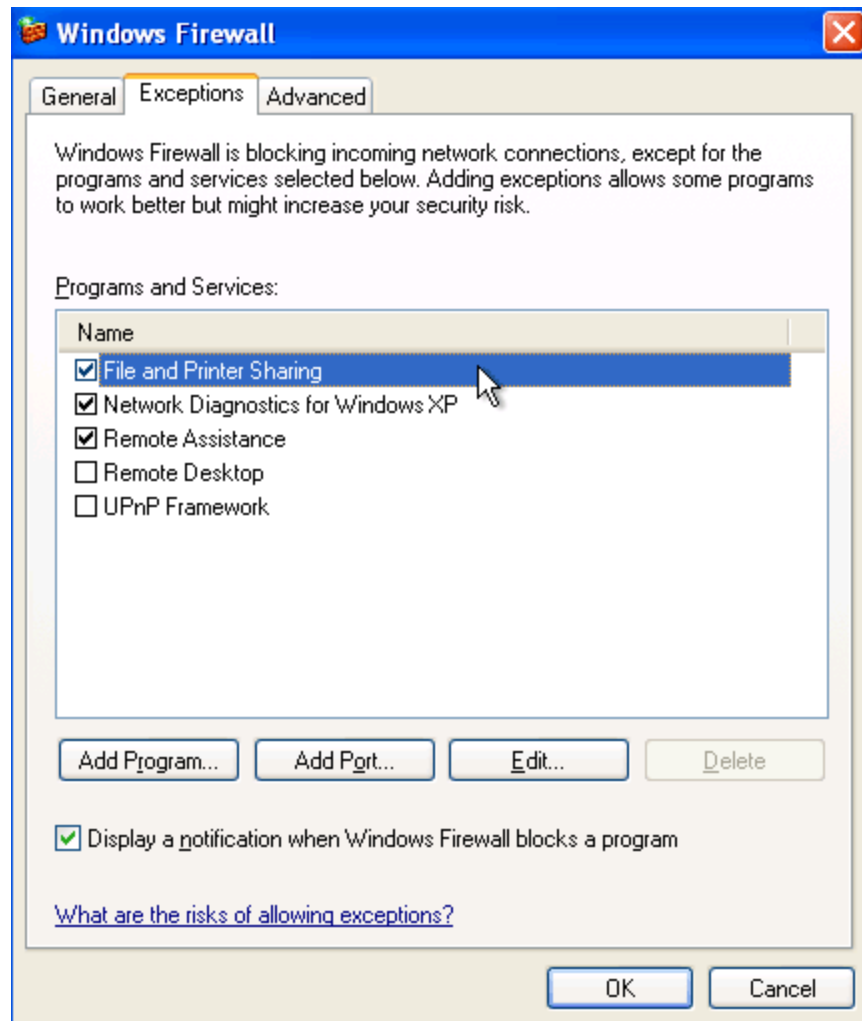
### Windows XP

The Simple File Sharing feature of Windows XP is not supported by Management Utilities, and must be disabled on all XP systems. To disable this feature, choose My Computer from the Start menu or the Windows XP desktop. Go to Tools - Folder Options. Click the View tab and find "Use Simple File Sharing (Recommended)" in the list of advanced settings. It should be at or near the bottom of the list. If the feature is enabled, click to clear the checkbox. Click OK to close the Folder Options dialog.





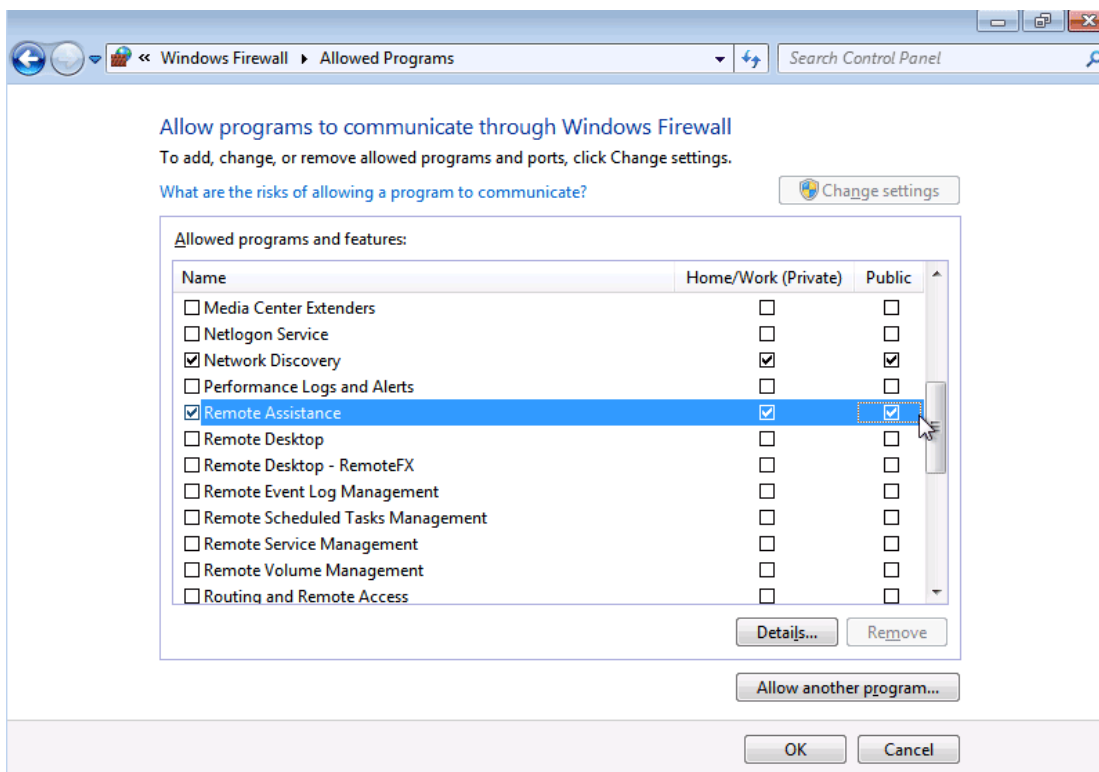
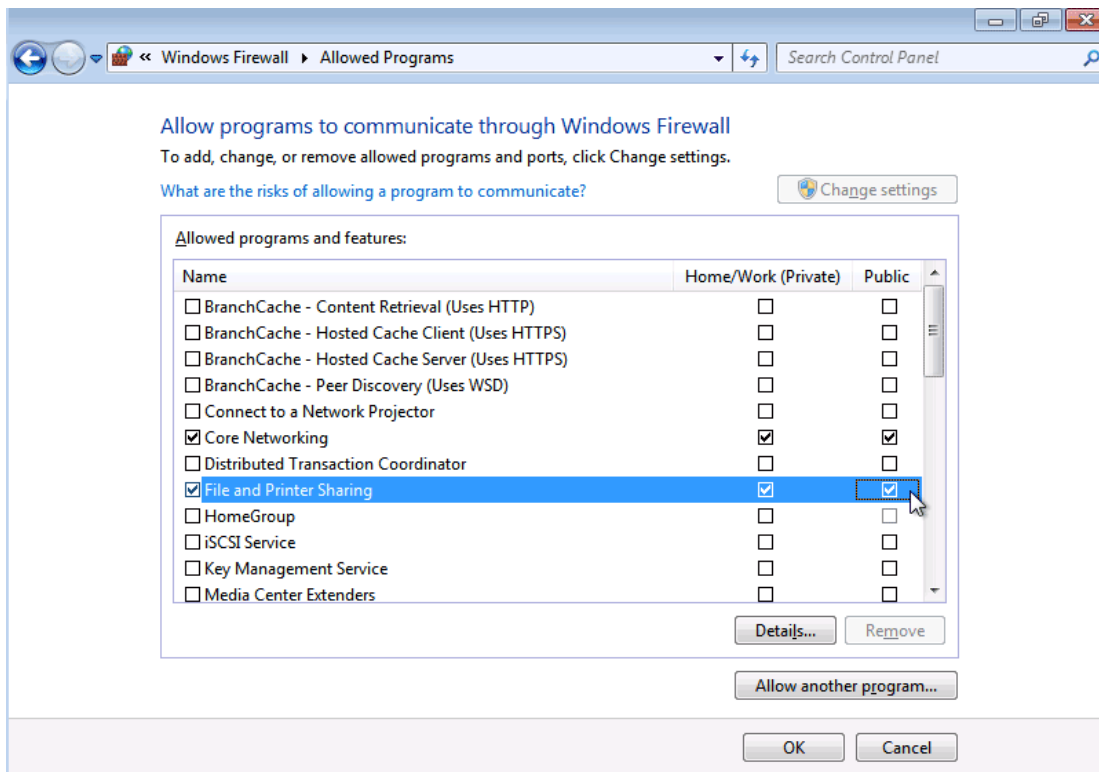
To configure the Windows firewall, choose Control Panel from the Start menu. In Control Panel, go to Windows Firewall. The Windows Firewall dialog will be displayed. If the firewall is enabled, you will need to add exceptions. Click the Exceptions tab. Check the box for File and Printer Sharing. Click OK to close the Windows Firewall dialog.



## Windows 7 - 8

To configure the Windows firewall, choose Control Panel from the Start menu. In Control Panel, go to Windows Firewall. If the firewall is enabled, you will need to allow features through the firewall. On the sidebar at the left of the Windows Firewall screen, click Allow a program or feature through Windows Firewall. Enable these features for the private and public networks: Core Networking, File and Printer Sharing, Network Discovery, and Remote Assistance. Click OK to close the configuration screen. The illustrations are for a Windows 7 system; the procedure is the same for Windows 8.

User Account Control must be disabled. To do this on a domain, or in a non-Active Directory environment, please refer to the SyAM Tool Tip Disabling User Account Control.



## Logging Into Management Utilities

The Management Utilities browser based interface can be accessed across the network from a system using a supported web browser.

Open up the browser and type in

- http or https
- IP Address or name of the system running Management Utilities
- Port number used – leave blank if using the default port 80



Example <http://192.168.100.63>

You will be presented with a Windows Authentication box. Enter the username and password that are valid on your Windows network



**The first user to log into the Management Utilities will be created as the administrator and primary username. Additional users can be set up by this user for accessing Management Utilities.**



**To browse to Management Utilities from a Windows 8 system, install Firefox and browse from the Desktop. V5.13 Management Utilities may not support all functions of Internet Explorer 10 and greater.**

Upon logging into Management Utilities for the first time, you will be presented with an Authentication Template which must be completed and saved before you can continue.

Enter a Template Name, Username, and Password (and Domain, if using a domain administrator account), then press Save to save your template. Click on the top right hand corner X to close the window and continue.



**This user must be an administrator on your Windows network and have access to the target systems you will be deploying software to.**

## Product Terms

- **Group:** A collection of systems that have been discovered in your network. Some groups are organized automatically, but user-defined groups are also available.  
*Example: An IP scan range of 192.168.100.1 to 192.168.100.25*
- **Template:** A collection of settings that specify how a given task will operate.  
*Example: Power Off Systems at 5 PM each weekday*
- **Task:** A single operation that is configured by one or more templates.  
*Example: Apply Power Template*
- **Job:** An ordered list of tasks that are performed on one or many systems or groups. Jobs can be scheduled or on-demand.  
*Example: Apply the Power Template to the group Accounting Systems*

## User Interface Panels

### Groups:

Shows the breakdown of discovered systems in your network. The Function, Location and Operating System groups are automatically organized, but the user may also define their own custom groups.

### Functions:

Provides options to modify templates, create jobs or configure settings for using the software.

### Details:

Shows the details of all the systems in the group that has been selected in the group panel.

### Status:

Displays a brief overview of the results from jobs that have been run.

### Scheduled Jobs:

Displays jobs that have been scheduled, are in progress, have completed today, or have been suspended.

The screenshot displays the SYAM Management Utilities web interface. The top navigation bar includes the SYAM logo, the title "Management Utilities", and user information: "Logout", "Management Utility", and "Logged In As: administrator".

The interface is divided into four main sections:

- Groups:** A sidebar on the left lists categories like "SyAM - Function", "SyAM - Location", "SyAM - Operating System", "Job Errors", "test-lab local", and "Patch Scans".
- Functions:** A sidebar on the left lists various management tasks such as "Administration Settings", "Configure Templates", "Authentication", "Client Deployment", "Discovery", "Location/Function", "Notifications", "Patch Management", "Remote Console Settings", "Area Manager IP Address", "System Alert Matrix", "Third Party", "Wake On LAN", "Manage Job Templates", "Network Discovery Wizard", "My Settings", "Unattended Installation Wizard", and "View History".
- Details:** The central panel titled "All Systems with Client" shows a table of discovered systems. The table has columns for IP, MAC, Name, OS, Client, Type, Mgt, Area, Manager, Power, and Power Template Set. It lists various systems like "RUS-SP3-RETAIL", "RUS-WIN7X86", "DENVER DESKTOPS", etc.
- Status:** A panel at the bottom showing the results of recent jobs. It includes a "View Details" link and a summary of job execution, such as "Patch Scan Now in Job 'administrator: 11/19/2013 2:12 PM'. Job started on 11/19/2013 2:13:26 PM. The containing job is still in progress."

Red text labels are overlaid on the image to identify these sections: "Groups", "Functions", "Details", and "Status".

## Groups

There are four types of groups shown in the Groups window.

**SyAM – Function / Location / Operating System** - These are the groups of systems discovered by the Management Utilities that are running the System Client. They are organized by the SyAM Client programmed fields for Function, Location, and Operating System.

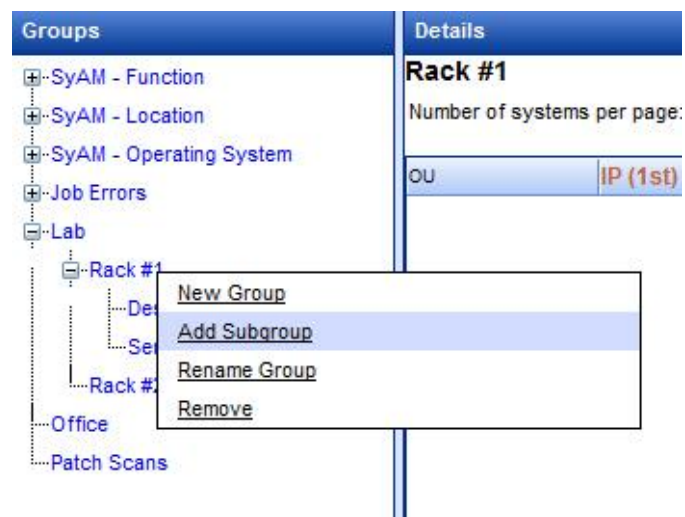
**Job Errors** – A client system that is the target of a job run by the Management Utilities can be copied to these groups when a job error is reported. Job error subgroups are organized by error codes and by the jobs that reported errors.

**User Defined Groups** – These are the groups that users create either through a Discovery Template or manually by right clicking the mouse button and choosing New Group, or by clicking on a group name and then right clicking the mouse button and choosing Add Subgroup.

**Patch Scans** – These are the groups of systems that have had a manual Microsoft Vulnerability scan performed on them.



The example below shows how to add a subgroup to the group called **Rack #1**:





## Details Panel

The Details panel displays information on all the systems in the chosen group.

Details

All Systems with Client

Number of systems per page: 25

Copy

Move

Remove

[?]

OU	IP (1st)	MAC	Name	OS	Client	Type	Mgd	Area Man...	Power	Power
	192.168.100.9	00-15-17-27-24-21	S3210SH	Microsoft(R) Window...	V4.37.12...	Server	Yes	192.168....	On	No
	192.168.100.11	00-02-B3-E9-62-30	SE7501CW2	Microsoft Windows 2...	V4.38.00...	Server	No		On	No
	192.168.100.12	00-30-05-8F-36-8D	D885GBF	Microsoft Windows X...	V4.08.80...	Desktop	No		On	No
	192.168.100.22	00-16-76-56-8E-33	NH1	Red Hat Enterprise L...	V4.08.00...	Server	Yes	192.168....	On	No
	192.168.100.25	1C-8F-65-28-8F-24	H55	Microsoft Windows 7...	V4.34.97...	Desktop	No		On	No
	192.168.100.26	6C-F0-49-ED-91-5F	P55	Microsoft Windows 7...	V4.34.97...	Desktop	Yes	192.168....	On	No
	192.168.100.28	6C-F0-49-E1-D2-35	Q57MS2H	Microsoft Windows 7...	V4.35.60...	Desktop	No		On	No
	192.168.100.41	00-24-81-E1-0E-5C	WIN-NHPJOHW8NYK	Microsoft® Windows...	V4.34.97...	Server	Yes	192.168....	On	No
	192.168.100.42	00-19-DB-A2-7A-03	NEC-SERV	Microsoft(R) Window...	V4.37.20...	Server	No		On	No
	192.168.100.43	00-24-81-E7-2F-B8	WIN-6SDTJMGUW5	Microsoft® Windows...	V4.34.97...	Server	Yes	192.168....	On	No
	192.168.100.50	00-0C-29-DA-86-07	XP-1	Microsoft Windows X...	V4.34.97...	Desktop	Yes	192.168....	On	No
	192.168.100.60	00-30-48-F4-24-1A	X8DT3	Microsoft(R) Window...	V4.34.97...	Server	Yes	192.168....	On	No
	192.168.100.93	00-0C-29-6D-CE-09	2K03-CHILD	Microsoft(R) Window...	V4.38.00...	Desktop	Yes	192.168....	On	No
	192.168.100.111	00-60-08-17-5E-4F	D845GTP-VMWARE1	Microsoft Windows X...	V4.05.30...	Desktop	Yes	192.168....	On	No
	192.168.100.132	00-22-15-C3-E3-3E	WIN-CE2ZRYAFFZP	Microsoft® Windows...	V4.34.91...	Server	No		On	No
	192.168.100.133	00-21-85-1D-37-34	P45NEO	Microsoft Windows X...	V4.35.70...	Desktop	Yes	192.168....	On	No
	192.168.100.135	00-60-08-C7-89-ED	GA-8I845GV	Microsoft Windows 2...	V3.45.10...	Desktop	No		On	No
	192.168.100.140	00-40-A7-0A-26-95	MT1310	Microsoft Windows X...	V4.08.90...	Server	Yes	192.168....	On	No
	192.168.100.151	00-1C-C0-B6-1D-84	DB43LD-2k08-X84	Microsoft® Windows...	V4.37.12...	Server	Yes	192.168....	On	No
	192.168.100.153	00-13-46-6D-2E-EE	MS-7351-W7U-X84	Microsoft Windows 7...	V4.34.97...	Desktop	Yes	192.168....	On	No

Items: 1 - 25 of 42

Page 1 of 2 Next Page

The columns can be sorted in ascending and descending order. The default sort order is IP address; this can be changed to Machine Name under the Administration Settings. Click on the column heading to go from ascending to descending; click one more time to remove it from the sorting order.

You can have 1<sup>st</sup> and 2<sup>nd</sup> column sorting; these are shown by the Amber Text and (1<sup>st</sup>) label and Green Text and (2<sup>nd</sup>) label.

Client	Type (1st) ▲	Mgd (2nd) ▲
V4.08.80...	Desktop	No
V3.45.10...	Desktop	No
V4.07.00...	Desktop	No

To change the column sorting order make the column you wish to become the 1<sup>st</sup> sorting order as the 2<sup>nd</sup> column by clicking on the column heading, then click on the 1<sup>st</sup> column header twice to remove the 1<sup>st</sup> column sorting order. This will then make the 2<sup>nd</sup> column sorting the new 1<sup>st</sup> column sorting.



## System Detail Data

The Column headings in the system details represent data collected from the systems.

Column Heading	Data
<b>OU</b>	Organizational Unit name (Active Directory)
<b>IP</b>	IP Address last obtained for that system
<b>MAC</b>	Network adapter MAC Address
<b>Name</b>	Machine Name
<b>OS</b>	Operating System (This is retrieved through the system Client)
<b>Client</b>	Version of System Client installed
<b>Type</b>	Client configuration type (Server, Desktop, Notebook, Tablet)
<b>Mgd</b>	Managed status of Client. Yes means the Client is managed by a System Area Manager; No means the Client is not managed by a System Area Manager.
<b>Area Manager IP</b>	IP Address of the System Area Manager the Client is reporting to
<b>Power</b>	Current Power Status
<b>Power Template Set</b>	Set means that SyAM System Client will perform a scheduled shutdown or restart. Set is followed by All Days (7 days a week) or Week Days (5 days a week) or Partial (individual day or days). Not Set means no shutdown or restart is scheduled. The Windows power scheme is listed for systems with 4.51 or newer client version
<b>Location</b>	The Location programmed into the Client
<b>Function</b>	The Function programmed into the Client
<b>Refreshed</b>	The date and time the system data was last refreshed by the Management Utilities



***Please note that systems must have the System Client installed, running and managed by a System Area Manager before you can perform Third Party Application Deployment or Patch Management actions to them.***

## Copy / Move Systems

Systems placed into the user created groups either manually or through a Discovery Job can be copied to other groups/subgroups, removed from a group, or moved to another group or subgroup.

Select the system or systems that you wish to take the action on, then click the Copy or Move button.

Details										
Office										
Number of systems per page: 25 ▼							Copy	Move	Remove	?
OU	IP (1st)	MAC	Name	OS	Client	Type	Mgd	Area Man...	Power	Power Ter
	192.168.200.5					Unknown	No		Off	Not Se
	192.168.200.6					Unknown	No		Off	Not Se
	192.168.200.7	00-40-05-32-06-0B	D915GUX	Microsoft Windows X...	V4.31.99...	Desktop	Yes	192.168....	On	Not Se
	192.168.200.8		LINUX-BUILD-SER			Unknown	No		Off	Not Se
	192.168.200.9	00-30-48-70-7C-EF	BUILD-SERVER	Microsoft Windows 2...	V4.31.20...	Server	No		On	Not Se
	192.168.200.10	00-30-48-88-A5-FE	SYAM-SERVER1	Microsoft(R) Window...	V4.05.30...	Server	Yes	192.168....	On	Not Se
	192.168.200.11					Unknown	No		Off	Not Se
	192.168.200.12					Unknown	No		Off	Not Se
	192.168.200.13					Unknown	No		Off	Not Se

This will then bring up a list of the groups/subgroups that you can copy or move the selected systems to. Choose the name from the list and click the OK button.

192.168.200.6						Unknown	No		Off
192.168.200.7	00-40-05-32-06-0B	D915GUX	Microsoft Windows X...	V4.31.99...	Desktop	Yes	192.168...	On	
192.168.200.8		LINUX-BUILD-SER			Unknown	No		Off	
192.168.200.9	00-30-48-70-7C-EF	BUILD-SERVER	Microsoft Windows 2...	V4.31.20...	Server	No		On	
192.168.200.10	00-30-48-88-A5-FE	SYAM-SERVER1	Microsoft(R) Window...	V4.05.30...	Server	Yes	192.168...	On	
192.168.200.11					Unknown	No		Off	
192.168.200.12								Off	
192.168.200.13								Off	
192.168.200.14								Off	
192.168.200.15								Off	
192.168.200.16								Off	
192.168.200.17								Off	
192.168.200.18								Off	
192.168.200.19					Unknown	No		Off	
192.168.200.20					Unknown	No		Off	
192.168.200.21					Unknown	No		Off	
192.168.200.22					Unknown	No		Off	
192.168.200.23					Unknown	No		Off	

Select the group to which you would like to copy the selected systems

- Lab
- Lab - Rack #1
- Lab - Rack #1 - Desktops
- Lab - Rack #1 - Servers
- Lab - Rack #2

OK Cancel

Select the group to which you would like to copy the selected systems

Lab  
Lab - Rack #1  
Lab - Rack #1 - Desktops  
Lab - Rack #1 - Servers  
Lab - Rack #2

OK Cancel

## Remove Systems

Select the system or group of systems that you wish to remove from the group, and then click the Remove button.

Details										
Office										
Number of systems per page: 25							Copy	Move	Remove	[?]
OU	IP (1st)	MAC	Name	OS	Client	Type	Mgd	Area Man...	Power	Power Ter
	192.168.200.5					Unknown	No		Off	Not Se
	192.168.200.6					Unknown	No		Off	Not Se
	192.168.200.7	00-40-05-32-06-0B	D915GUX	Microsoft Windows X...	V4.31.99...	Desktop	Yes	192.168....	On	Not Se
	192.168.200.8		LINUX-BUILD-SER			Unknown	No		Off	Not Se
	192.168.200.9	00-30-48-70-7C-EF	BUILD-SERVER	Microsoft Windows 2...	V4.31.20...	Server	No		On	Not Se
	192.168.200.10	00-30-48-88-A5-FE	SYAM-SERVER1	Microsoft(R) Window...	V4.05.30...	Server	Yes	192.168....	On	Not Se
	192.168.200.11					Unknown	No		Off	Not Se
	192.168.200.12					Unknown	No		Off	Not Se
	192.168.200.13					Unknown	No		Off	Not Se

This will then bring up a confirmation of the removal. Press the OK button to confirm the removal of the selected systems.

## Copy / Remove Systems from the SyAM Groups

Systems that are in the SyAM Groups can be copied or removed; they cannot be moved as they are placed in their group based upon the information programmed into the System Client.

Details										
All Systems with Client										
Number of systems per page: 25							Copy	Move	Remove	[?]
OU	IP (1st)	MAC	Name	OS	Client	Type	Mgd	Area Man...	Power	Power Tem
	192.168.100.9	00-15-17-27-24-21	S3210SH	Microsoft(R) Window...	V4.37.12...	Server	Yes	192.168....	On	Not Se
	192.168.100.11	00-02-B3-E9-82-30	SE7501CW2	Microsoft Windows 2...	V4.38.00...	Server	No		On	Not Se
	192.168.100.12	00-30-05-8F-35-8D	D885GBF	Microsoft Windows X...	V4.08.80...	Desktop	No		On	Not Se
	192.168.100.22	00-16-78-58-8E-33	NH1	Red Hat Enterprise L...	V4.08.00...	Server	Yes	192.168....	On	Not Se
	192.168.100.25	1C-8F-85-28-8F-24	H55	Microsoft Windows 7...	V4.34.97...	Desktop	No		On	Not Se
	192.168.100.26	6C-F0-49-ED-91-5F	P55	Microsoft Windows 7...	V4.34.97...	Desktop	Yes	192.168....	On	Not Se



Please note that when you remove a system from a SyAM group it will only be returned to that group if it is re-discovered.

## System Actions (Right-Click Menu)

Select one or more Details panel rows, then right-click to display a menu of actions that can be taken. The action is applied by default to the selected system(s) but you can choose instead to take an action on the entire group, with or without its subgroups. Further details of specific job actions are given in other sections of this manual.

The screenshot shows a web-based management interface. At the top, a blue header bar contains the word "Details". Below it, a section titled "All Systems with Client" includes a dropdown menu set to "25" for "Number of systems per page:" and three buttons: "Copy", "Move", and "Remove". To the right of these buttons is a help icon "[?]".

The main area is a table with the following columns: OU, IP (1st), MAC, Name, OS, Client, Type, Mgd, and Area M. The table lists 25 systems. A right-click context menu is open over the first few rows. The menu has three radio buttons at the top: "Apply to Selected Machines" (selected), "Apply to Group", and "Apply to Group & Subgroups". Below these are several actions, some with right-pointing arrows indicating they are disabled: "Schedule a job...", "Client Deployment", "Set Location or Function", "Set Notification Settings", "Patch Management", "Set Power Schedule", "Set Remote Console Settings", "Shutdown", "Set Area Manager IP Address", "Set System Alert Matrix", "Deploy Third Party Software", "Issue Wake On LAN Command", and "Wait". At the bottom of the menu, there are four more actions: "Patch Scan Now", "Refresh Selected Systems", "Add to Restricted Access List", and "Add to Wake On LAN URL List...".

At the bottom left of the table, it says "Items: 1 - 25 of 49". At the bottom right, there is a pagination bar showing "Page 1 of 2" and a "Next Page" link.

Adding a machine to the Restricted Access List prevents Management Utilities from taking any actions on the machine. This feature can be used to define exceptions within a discovery group's IP range or Active Directory organizational unit. The Restricted Access List can be viewed in Administration Settings, and systems can be removed from the list there as well.

The Copy Text to Clipboard option is supported only when using Internet Explorer to browse to Management Utilities. Details of selected systems are copied with the fields delimited by commas. You can paste into Notepad and save as a Comma Separated Values (.csv) file, or paste into Excel and use the Text to Columns option to format the data for your spreadsheet.



## The Shutdown Task

The Shutdown task is used to perform an immediate shutdown of selected machines. It can be run from the Groups right-click menu, or as part of a job defined in a saved job template.

## Active Directory Management

In an Active Directory environment, Management Utilities can move a machine between Organizational Units, or remove a machine from Active Directory. To access this feature, click a system in Groups, right-click to display the context menu, then choose Active Directory Management.

Details

Denver Desktops

Number of systems per page: 25

CopyMoveRemove

?

OU	IP (1st)	MAC	Name	OS	Client	Type	Mgd	Area M
			D1-MARKETING			Unknown	No	
						Unknown	No	
						Unknown	No	
Denver Desktops	192.168.100.150	00-1C-C0-D4-F7-4			.420..	Desktop	Yes	192.16
Denver Desktops	192.168.100.152	00-E0-4C-D0-4A-B			.420..	Desktop	Yes	192.16

Apply to Selected Machines

Apply to Group

Apply to Group & Subgroups

Schedule a job...

Client Deployment

Set Location or Function

Set Notification Settings

Patch Management

Set Power Schedule

Set Remote Console Settings

Shutdown

Set Area Manager IP Address

Set System Alert Matrix

Deploy Third Party Software

Issue Wake On LAN Command

Wait

Patch Scan Now

Refresh Selected Systems

Add to Restricted Access List

Add to Wake On LAN URL List...

Active Directory Management

Copy Text to Clipboard

Items: 1 - 5 of 5

Page 1 of 1

Choose a template for authentication as a domain administrator. To move a system, click the Move radio button. Click Discover Domains and select the desired domain, then click Discover Organizational Units.

Details

Active Directory Management

Manage systems in Active Directory.

Active Directory Management

Choose authentication template

Windows Domain Admin

Move

Remove

Discover Domains

Discover Organizational Units

Domain:

test-lab.local

Organizational Units:

Boston Desktops

Boston Desktops - Aardvark Group

Boston Desktops - Komodo Group

Boston Desktops - Komodo Group - Chameleon Circle

Boston Desktops - Komodo Group - Chameleon Circle - Ferret Forum

Denver Desktops

Domain Controllers

Los Angeles Desktops

Temporary

Temporary - Movedmachines

Apply

Affected Systems (1)

DG31PR-W7E-X86

Remove

Select the Organizational Unit to move the system into. If you select the first (blank) line, the system will be removed from its current OU but not placed into another one. Click the Apply button to make the change.



**It will take some time for the Management Utility Groups interface to display the system in its new OU group and for the information in the system's OU field to become current. This depends on the configuration of your Active Directory domain controller and the refresh interval of the Management Utility network discovery.**

To remove a system from Active Directory, click the system in Groups, right-click to display the context menu, and choose Active Directory Management. Then choose the domain authentication template and click the Remove radio button. Click Apply to remove the system from Active Directory.

## Active Directory Management

Manage systems in Active Directory.

Active Directory Management

Choose authentication template Windows Domain Admin ▾

☐ Move

☒ Remove

Discover Domains

Discover Organizational Units

Domain: test-lab.local ▾

Organizational Units: ▾

Apply Cancel

## Affected Systems (1)

DG31PR-W7E-X86

Remove

## Chapter 2 – Configuring General Settings

After you have created the initial Authentication Template you should configure the Network shares in the Administration Settings.

### Defining Paths to the Network Shares Used for Deployment

As the Management Utility deploys software across the network you need to configure the utility to access the network share where the applications and patches to be deployed can be stored.

Click on Administration Settings, enter the Patch and Default Application paths and press the Save Changes button.

The screenshot shows a web-based configuration window titled "Details". It has a tabbed interface with the following tabs: "Settings" (selected), "Users", "Restricted Access List", "Blackout Calendar", and "Wake on LAN URL List".

The "Settings" tab is divided into two sections:

- Build Information:**
  - Application Vendor: SyAM Software
  - Installed Version: V5.14
  - Build Number: 970
  - Build Date: 20140327
  - Database Version: 163
- Management Utility Settings:**
  - Patch Download Folder:** A text input field containing the path "\\192.168.100.158\patches".
  - Default Application Path:** A text input field containing the path "\\192.168.100.158\apps".
  - Days to keep history:** A text input field containing the value "60".

At the bottom of the window are two buttons: "Save Changes" and "Cancel".

Spaces in folder names are supported. Quotation marks should not be used.

### Setting History Retention

You can choose the number of days of Management Utility history to be retained. This refers to the information displayed on the View History page.



## Adding and Editing Users

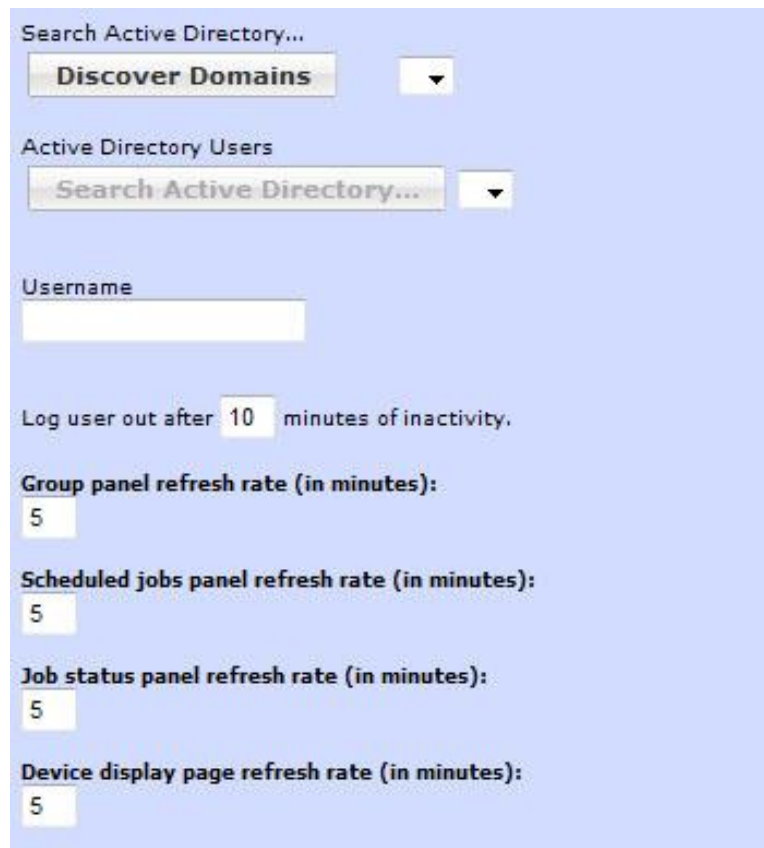
The Management Utility uses Windows authentication for all users. A username and password that is used to log into Management Utilities must be one that can log into Windows on the server running Management Utilities.

Set up the Windows user name in the Management Utility and choose which features that user has access to.

From the Users section you can:

- Create a New User
- Edit User
- Remove User
- Create SQL Login

To add a new user, click the Create User button.



The screenshot shows a user configuration interface with a light blue background. At the top, there is a section labeled "Search Active Directory..." containing a "Discover Domains" button and a dropdown arrow. Below this is a section labeled "Active Directory Users" with a "Search Active Directory..." button and a dropdown arrow. Underneath is a "Username" label followed by an empty text input box. Further down, there is a label "Log user out after" followed by a text input box containing the number "10" and the text "minutes of inactivity.". Below that are four sections, each with a label and a text input box containing the number "5": "Group panel refresh rate (in minutes):", "Scheduled jobs panel refresh rate (in minutes):", "Job status panel refresh rate (in minutes):", and "Device display page refresh rate (in minutes):".

If an Active Directory user is to be added, click the Discover Domains button. Choose the domain from the drop down menu. Once the domain has been chosen, click the Search Active Directory button to populate the drop down menu with user names. Selecting a user from the menu will populate the Username box.

Management Utilities users must have unique names. It is not permitted to have more than one user with the same name, even if they are on different domains or are local system users. The

user can be granted access to all features of Management Utilities without regard to the particular domain or non-domain login used.

To remove a user, choose the user you wish to remove and click the Remove User button.

To edit a user, choose the user you wish to edit and click the Edit User button.

The screenshot shows a software interface titled "Details". It features a tabbed menu with the following tabs: "Settings", "Users", "Restricted Access List", "Blackout Calendar", and "Wake on LAN URL List". The "Users" tab is currently selected. Below the tabs, on the left, is a "Create User" button above a list box containing the names "administrator" and "bob", with "bob" highlighted. To the right of the list box are two buttons: "Edit User" and "Remove User". Further to the right are three input fields labeled "Domain Name", "Windows User Name", and "SQL Login Name". Below these fields is a "Create SQL Login" button.

When editing a user you can modify the parameters for the user and enable/disable the features available to the user.

The screenshot displays a user configuration window for a user named 'russell'. The interface includes several sections for configuring user parameters and features.

**Username:** russell

**Log user out after:** 10 minutes of inactivity.

**Group panel refresh rate (in minutes):** 5

**Scheduled jobs panel refresh rate (in minutes):** 5

**Job status panel refresh rate (in minutes):** 5

**Device display page refresh rate (in minutes):** 5

**Power Audit dashboard refresh rate (in minutes):** 5

**Power stats at a glance panel refresh rate (in minutes):** 5

**Application to load on startup:** Power Auditor

**Default number of days in identified savings dashboard and reports:** 7 (selected), 1, 30

**Show help text:** ☒

**Number of machines to display at a time on the group page:** 25

**Default sort column on the group page:** IP Address (selected), Machine Name

**Features:**

- ☒ Administration Settings
- ☒ Configure Templates
- ☒ Unattended Installation Wizard
- ☒ My Settings
- ☒ View History
- ☒ Show Audits for All Users
- ☒ Reports
- ☒ Change system power auditing
- ☒ Network Discovery Wizard / Power Audit Wizard
- ☒ Active Directory Management

**Tasks:**

- ☒ Discovery
- ☒ Client Deployment
- ☒ Set Location or Function
- ☒ Set Power Schedule
- ☒ Set Area Manager IP Address
- ☒ Set Remote Console Settings
- ☒ Set System Alert Matrix
- ☒ Set Notification Settings
- ☒ Issue Wake On LAN Command
- ☒ Deploy Third Party Software
- ☒ Patch Management
- ☒ Wait
- ☒ Shutdown

**Buttons:** Save Changes, Cancel

Click the Save Changes button to save and apply the changes to the user. Users may configure these parameters (but not the selection of available features and tasks) by choosing My Settings from the Features menu at the bottom left of the browser page.

The Create SQL Login feature is used to add a user to SQL as an administrator.

The screenshot shows the 'Details' window with the 'Users' tab selected. The 'Create User' section is active. A list box on the left contains the text 'administrator'. To the right, there are three text input fields: 'Domain Name' with the value 'testdomain.local', 'Windows User Name' with the value 'ITadmin', and 'SQL Login Name' with the value 'ITadmin'. Below these fields are three buttons: 'Edit User', 'Remove User', and 'Create SQL Login'.

Enter the domain name, Windows user name, and SQL login name. If the Management Utilities server does not belong to a Windows domain, its machine name should be entered in place of the domain name.

## Restricted Access List

Systems that have been added to the Restricted Access List through the Groups interface are listed here. Jobs run by the Management Utility will take no action on any systems on this list. To remove a system from the list, check the box for that system, then click the Remove from Restricted Access List button.

The screenshot shows the 'Details' window with the 'Restricted Access List' tab selected. It displays a table with the following data:

<input type="checkbox"/>	Location	IP Address	Device Name
<input type="checkbox"/>	Office	192.168.100.6	DQ77MK-HYPER-V
<input type="checkbox"/>	2nd Floor Basement	192.168.100.70	THINKCENTRE

Below the table is a button labeled 'Remove from Restricted Access List'.

In the Groups area, systems on the Restricted Access List are displayed with a grey background.

## Details

### Lab

Number of systems per page: 25 ▼

OU	IP (1st) ▲	MAC	Name	OS	Client	Type	Mgd
	192.168.100.1	00-D0-CF-02-39-73				Unknown	No
	192.168.100.2	00-1C-C0-61-52-85	MULTILANGSERVER	Microsoft Windows Ser	V4.50.570-4	Server	Yes
	192.168.100.3	00-19-DB-A2-7A-02	NEC-Server.CTTEST.lc	VMware ESXi 5.5.0	V4.52.001-4	Server	Yes
	192.168.100.4					Unknown	No
	192.168.100.5					Unknown	No
	192.168.100.6					Unknown	No
	192.168.100.7					Unknown	No
	192.168.100.8	00-0C-29-BD-62-A8	mailsrv1	Red Hat Linux release	V4.51-LINL	Server	Yes
	192.168.100.9	00-15-17-27-24-21	S3210SH	Microsoft(R) Windows(t	V4.53.520-4	Server	Yes
	192.168.100.10					Unknown	No
	192.168.100.11	00-0A-95-D1-98-8C	syams-power-mac-g5.k	Mao OS X 10.5.6	V4.50.001-4	Desktop	No
	192.168.100.12					Unknown	No
	192.168.100.13					Unknown	No

## Blackout Calendar

The Blackout Calendar allows you to define a blackout period by specifying starting and ending days. When setting up a scheduled job, select the Enforce Blackout Calendar option, and the job will not take any actions during the blackout period. The Blackout Calendar has no effect on any other jobs.

Click the button to add blackout dates.

**Configure Template**

Settings

Users

Restricted Access List

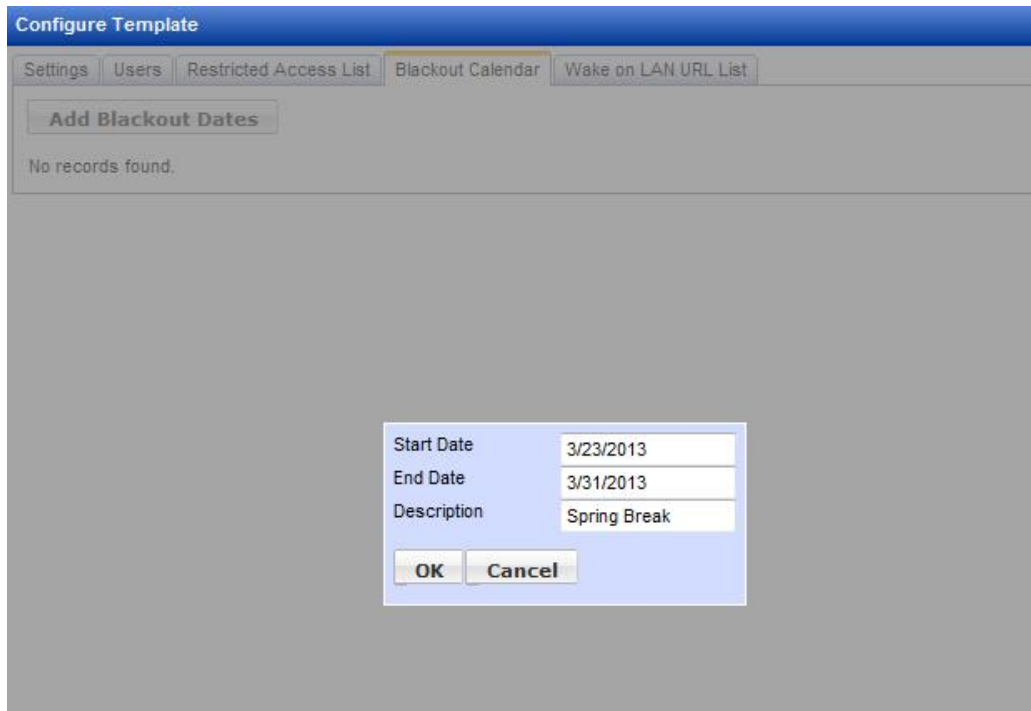
**Blackout Calendar**

Wake on LAN URL List

**Add Blackout Dates**

No records found.

Enter starting and ending dates, with a name for the calendar entry.



Existing calendar entries are displayed on the Blackout Calendar tab. They can be removed by clicking Delete.



## Wake on LAN URL List

You can create a URL that can be used to activate a supported system using Wake on LAN.

Each URL applies to an individual client machine. Highlight a system in Groups, then right-click to display the context menu. Mouse over the selection Add to Wake On LAN URL List near the bottom of the menu. Click to select the Wake on LAN template to be used. (For more information on creating the template, see the relevant section of this manual.)

**Details**  
200-94

Number of systems per page: 25

[Copy](#) [Move](#) [Remove](#) [\[?\]](#)

OU	IP (1st)	MAC	Name	OS	Client	Type	Mgd	Area M
	192.168.200.94	00-15-5D-C8-A4-00	MINI PC	Microsoft Windows V	V4.51.420...	Desktop	No	

☒ Apply to Selected Machines  
☐ Apply to Group  
☐ Apply to Group & Subgroups

[Schedule a job...](#)  
[Client Deployment](#)  
[Set Location or Function](#)  
[Set Notification Settings](#)  
[Patch Management](#)  
[Set Power Schedule](#)  
[Set Remote Console Settings](#)  
[Shutdown](#)  
[Set Area Manager IP Address](#)  
[Set System Alert Matrix](#)  
[Deploy Third Party Software](#)  
[Issue Wake On LAN Command](#)  
[Wait](#)

[Patch Scan Now](#)  
[Refresh Selected Systems](#)  
[Add to Restricted Access List](#)  
[Add to Wake On LAN URL List...](#)  
[Active Directory Management](#)  
[Copy Text to Clipboard](#)

Items: 1 - 1 of 1

Page 1 of 1

Relay 200-111

Choosing a template brings you to the Wake on LAN URL List tab of the Administration Settings area.

**Details**

[Settings](#) [Users](#) [Restricted Access List](#) [Blackout Calendar](#) [Wake on LAN URL List](#)

The default URL when enabling Remote Wakeup for a system should...

☒ Use Machine Name  
☐ Use A Randomly Generated Code

**Default Authentication Template**  
 Windows Admin


	Location IP Address	Device Name	WOL Template	WOL Authentication Template	URL	
<input type="checkbox"/>	192.168.200.88	HP-PC	Relay 200-111		http://192.168.100.158:8080/remote/wake.aspx?HP-PC	<a href="#">Edit</a>
<input type="checkbox"/>	192.168.200.29	Q57TM	Relay 200-111		http://192.168.100.158:8080/remote/wake.aspx?Q57TM	<a href="#">Edit</a>

[Remove Selected URLs](#) [Randomize Selected URLs](#)



The defaults that can be set on this page are to end the URL with the machine name or with a randomly generated code, and the default authentication template used by the Wake on LAN job. Click an entry's Edit link to change the Wake on LAN template, or the authentication template, or the ending characters of the URL. When finished editing, click Update to save changes or Cancel to discard changes. URL entries may be deleted, or changed from machine names to randomly generated characters, by using the checkboxes to select entries then clicking the Remove Selected URLs or Randomize Selected URLs buttons.

To wake a system, browse to the corresponding URL. In this example, the Management Utilities server is referred to by an internal IP address, so the URL will work on the internal network or VPN. The user will be prompted for a username and password. (Please refer to the relevant section of this manual for information on setting up Management Utilities users.)



## Management Utilities

### Remote Wake On LAN

---

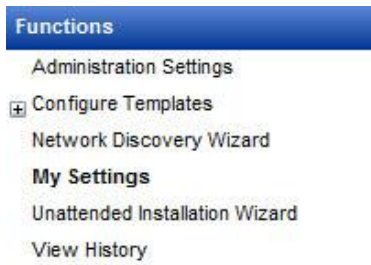
<b>Name</b>	L1-SALES
<b>IP</b>	
<b>MAC</b>	
<b>Power Status</b>	Off

Click the Power System On button. The system power status will be reported as On when the machine responds to ping, or when the System Client is initialized. If the system is still off after five minutes, it may be unavailable on the network or not properly configured for Wake on LAN.



## My Settings

The My Settings page is used to define your personal settings and preferences.



The session timeout value is the number of minutes Management Utilities will wait before logging you out of your session because of inactivity. If no value is filled in, you will never be logged out for inactivity. We strongly recommend leaving this value at the default.

The refresh rate options specify how many minutes should pass between refreshes of your content pages. Having a lower value here will keep information up-to-date, but will drastically reduce performance.

You can choose to have either Power Auditor or Management Utility loaded by default on startup, set the default number of days for the Power Auditor's dashboard and reports, and whether to expand the power chart.

Unchecking the Show help text option will suppress help messages that are typically found at the top of a window.

Default behavior of the Management Utility Groups page (machines per page, sort order) can be configured here.

## Details

Last logged in: 4/19/2011 9:40:42 AM

Log me out after  minutes of inactivity.

Group panel refresh rate (in minutes):

Scheduled jobs panel refresh rate (in minutes):

Job status panel refresh rate (in minutes):

Device display page refresh rate (in minutes):

Power Audit dashboard refresh rate (in minutes):

Power stats at a glance panel refresh rate (in minutes):

Application to load on startup:

Default number of days in identified savings dashboard and reports:

- ☐ 1  
☒ 7  
☐ 30

☒ Power Chart Expanded By Default

Show help text ☒

Number of machines to display at a time on the group page:

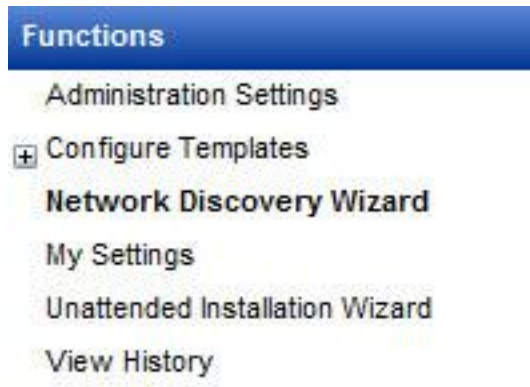
Default sort column on the group page:

- ☒ IP Address  
☐ Machine Name

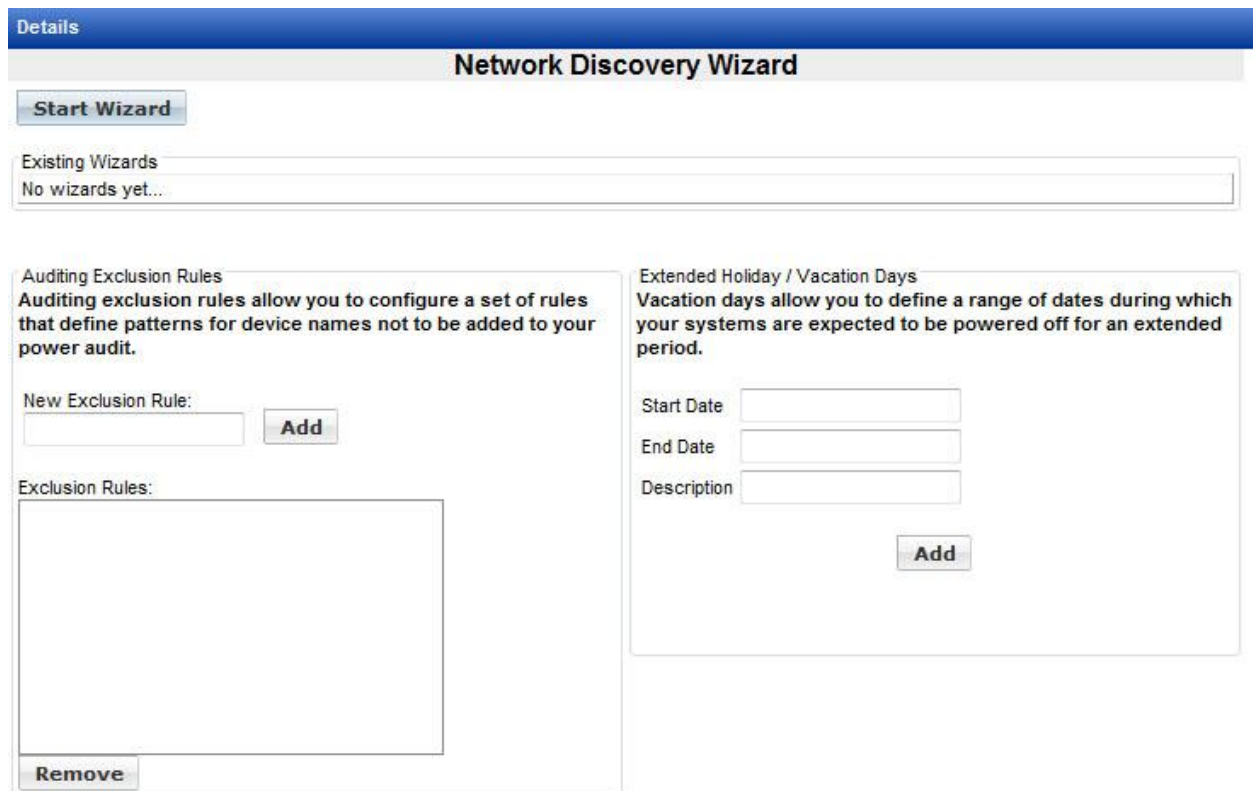
## Chapter 3 – Network Discovery

Now that our users and network shares are configured, we can discover systems using the Network Discovery Wizard.

In the Functions menu, click Network Discovery Wizard.



If there are any existing wizard jobs, they will be displayed. To create a new one, click the Start Wizard button.

A screenshot of the 'Network Discovery Wizard' configuration page. At the top is a blue header bar with the word 'Details' on the left and 'Network Discovery Wizard' in the center. Below the header is a 'Start Wizard' button. Underneath is a section titled 'Existing Wizards' with the text 'No wizards yet...'. The main area is divided into two panels. The left panel is titled 'Auditing Exclusion Rules' and contains a description, a 'New Exclusion Rule' section with a text input and an 'Add' button, an 'Exclusion Rules' list area, and a 'Remove' button at the bottom. The right panel is titled 'Extended Holiday / Vacation Days' and contains a description, 'Start Date', 'End Date', and 'Description' input fields, and an 'Add' button.

By default, the wizard is scheduled to run about 30 to 45 minutes from the time it's created, and to run at the same time every 24 hours. These settings can be changed now, or by editing the wizard after it's created.

Discovery templates define a group of machines. This can be done by specifying a range of IP addresses, with options to filter on the machine name. In an Active Directory environment, a discovery template can also use Windows domains and Organizational Units to define the group.

In the Network Discovery wizard you can choose an existing discovery template or create a new one. You can also make changes to existing templates.

Begin creating a new discovery template by entering a template name that is related to the group of machines being selected.

Enter the name of the discovery group. The group will be created in the Groups section of Management Utility, and the machines discovered using this template will be placed in the group. Note that multiple discovery templates can use the same group name.

Set your discovery range either by Domain and Organizational Unit or as an IP address range. Click on Allow Systems with duplicate information if there is a router between your Management Utilities server and the target IP range, as the router may not allow the target systems' MAC

addresses to be passed, but instead represents the MAC address as the same for all systems. If you have selected a domain, you can check the Replicate OUs box to create subgroups for all Organizational Units in the domain.

Set filter options if desired. You may configure the filter so that only machine names which meet the filter are selected, or you may enter a list to exclude machine names. Wildcards can be used (an asterisk for any number of characters, a question mark for a single character to filter based on the position of a character.)

The screenshot shows the 'Network Discovery Wizard' dialog box. The title bar is blue with a red 'X' button. The main area is white. At the top, there's a 'Start Date' section with three dropdowns for year (19), month (10), and day (2011), followed by a time dropdown (10:30). Below this is a text field for 'Number of hours between network scans' with the value '24'. The 'Starting IP address' and 'Ending IP address' fields are empty. There's a checkbox for 'Resolve IP address to host name'. Under 'Other Options', there's a checkbox for 'Only discover systems that meet the following filter:' followed by an empty text field. Below that, there's a section for 'Exclude systems that meet the following filters:' with an 'Add' button and an empty text field. At the bottom of this section is a 'Remove' button. At the very bottom of the dialog are 'Save Changes' and 'Cancel' buttons. A 'Next' button is located at the bottom right of the dialog box.

When you are finished creating or editing the Discovery Template, click the Save Changes button. In the Existing Templates box, highlight the template you wish to select for your network discovery, then click the Next button.

**Network Discovery Wizard**

Start Date: 19 10 2011 10:30

Number of hours between network scans: 24

**Discovery Template**

Define a group or range of systems to be discovered.

Template Name: Lab

Discovery Group Name: Lab

☒ Allow systems with duplicate information

**Domain Options**

☐ Scan my domain (you must be logged into the domain)

Discover Domains

Discover Organizational Units

Domain:

Organizational Units:

☐ Replicate OUs

**Network Scan**

☒ Scan IP address range

Starting IP address: 192.168.100.1

**Existing Templates**

100-99
200-111
Lab
Office

**New Template**

Copy Remove

Next

The wizard will ask you to select a Power On Hours template, which is described in the documentation for Power Auditor. If you are not using Power Auditor, select the default Power On Hours template (8AM On, 5PM Off) and then click the Save Wizard button. Power Auditor users can change these settings later, if desired.

Configure Template

Network Discovery Wizard

Start Wizard

Existing Wizards

Scan Type	Scan Range	Group Name	Power On Hours Template	Last Scanned	Next Scan					
IP	192.168.100.1 - 192.168.100.254	Lab Rack	8AM On, 5PM Off	6/19/2012 3:28:45 PM	6/19/2012 4:00:00 PM	Enabled	<a href="#">Suspend</a>	<a href="#">Update Now</a>	<a href="#">Edit</a>	<a href="#">Remove</a>
IP	192.168.200.111 - 192.168.200.111	Test	8AM On, 5PM Off	6/19/2012 3:20:43 PM	6/19/2012 4:00:00 PM	Enabled	<a href="#">Suspend</a>	<a href="#">Update Now</a>	<a href="#">Edit</a>	<a href="#">Remove</a>

Auditing Exclusion Rules

Auditing exclusion rules allow you to configure a set of rules that define patterns for device names not to be added to your power audit.

New Exclusion Rule:

Exclusion Rules:

Remove

Extended Holiday / Vacation Days

Vacation days allow you to define a range of dates during which your systems are expected to be powered off for an extended period.

Start Date

End Date

Description

Add

The newly created wizard is now listed and placed in the schedule. To run the discovery now (without changing the schedule) click the Update Now link. Existing wizards can be edited or removed. Removing a wizard will not affect the contents of the Groups area. When multiple wizards are displayed, clicking a column header will update their sort order.

Like other scheduled jobs, Network Discovery Wizards can be suspended and resumed.

Users of Power Auditor should consult the documentation for information on Auditing Exclusion Rules and Extended Holiday / Vacation Days.

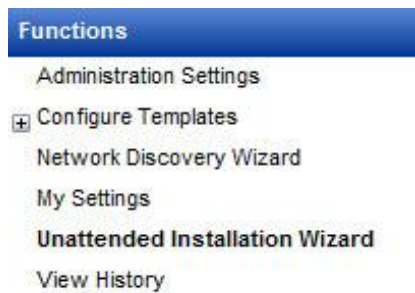


## Chapter 4 – Using the Unattended Installation Wizard

The Unattended Installation Wizard is a powerful tool for the Management Utility which allows you to configure all of the settings required to get your network up and running the System Area Manager and System Client suite. Clients are deployed and configured silently, making it easy to have a fully managed network in minutes.

The wizard guides you through discovery of systems on the network, specifying normal power on hours, client software deployment, and connection to the System Area Manager by creating new templates or using existing ones. Optionally, location, function, and power settings can also be configured through the wizard. The installation job can be set up to run on a regular schedule.

To begin, click the Unattended Installation Wizard link in the Functions menu at the lower left of the browser page. If you have already used the wizard to configure a deployment job, you can choose it, or else create a new one.



You will be prompted for Discovery, Power On Hours, Client Deployment, and System Area Manager IP Address templates. These are required for the unattended installation job. In each case, you can choose a template you have already configured, or you can create a new one.



## Unattended Installation Wizard

**Discovery Template**

Template Name:

Discovery Group Name:

☒ Allow systems with duplicate information

Domain Options

☐ Scan my domain (you must be logged into the domain)

Domain:

Organizational Units:

☐ Replicate OUs

Network Scan

☒ Scan IP address range

Starting IP address:

Ending IP address:

☒ Resolve IP address to host name

Other Options

☒ Only discover systems that meet the following filter:

Exclude systems that meet the following filters:

Existing Templates

Automation Network  
Automation Network 2K  
G4 Macs  
Replicate OUs

New Template

## Unattended Installation Wizard

**Power On Hours Template**

Define the hours that machines in your environment are typically powered on.

Template Name:

	Power On Time	Power Off Time
<b>Sunday</b>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>
0 Power On Hours		
<b>Monday</b>	<input type="text" value="08:00"/>	<input type="text" value="17:00"/>
9 Power On Hours		
<b>Tuesday</b>	<input type="text" value="08:00"/>	<input type="text" value="17:00"/>
9 Power On Hours		
<b>Wednesday</b>	<input type="text" value="08:00"/>	<input type="text" value="17:00"/>
9 Power On Hours		
<b>Thursday</b>	<input type="text" value="08:00"/>	<input type="text" value="17:00"/>
9 Power On Hours		
<b>Friday</b>	<input type="text" value="08:00"/>	<input type="text" value="17:00"/>
9 Power On Hours		
<b>Saturday</b>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>
0 Power On Hours		

Existing Templates

8AM On, 5PM Off

New Template

## Unattended Installation Wizard

**Client Deployment Template**  
Define the paths to executables used to silently deploy System Clients across your network.

Template Name:

Choose Installation Source

Choose installation source (must be System Client Version 3.3 or above):

Target Platform

☒ Windows  
☐ Linux  
☐ Mac OS X  
☐ VMWare ESXi

Select File

Select the authentication template with credentials to browse the network share entered below

Path to directory containing source executable file (depsvc.exe MUST be present in this directory):

☐ Copy this file locally to each target machine before installing (required if the above is not a network share, cannot be used with local impersonation)

☐ Install this file as a PKG.

Existing Templates

Mac 10.4 Desktop Deployment

Windows Deployment

XYZ Linux

New Template

SvAM Software Parameters

## Unattended Installation Wizard

**System Area Manager IP Address Template**  
Define the IP address of system area managers in your network.

Template Name:

System Area Manager IP Address

☒ Set agent to report to remote IP via file transfer

System Area Manager IP Address

☐ Set agent to report to this IP

Please note: this option will only work if the client is not already managed and this utility is on the same IP as the area manager.

Existing Templates

Local System Area Manager

This IP

New Template

You can set Location and Function, as well as Power Settings. These are not required for the unattended installation job, but it may be convenient to include these steps as part of your job. Again, you can use templates you've already configured, or you can create new ones.

Details

Unattended Installation Wizard

Location and Function Template

Location / Function Template:

Template Name: Office Desktop

☒ Location

Office

☒ Function

Desktop

Existing Templates

Office Desktop

New Template

CopyRemove

Save Changes

Cancel

Previous

Next

Configure Template

Unattended Installation Wizard

Template Name: Power - Windows

Timeout Settings for AC Main

Turn off monitor: After 1 Hour

Turn off hard disks: After 2 Hours

System standby: After 3 Hours

Hibernate: After 4 Hours

Hybrid Sleep (Windows 7 / 8 only): Disable

Power Management Scheduler Settings

Schedule	No Action	Shutdown	Restart	Hibernate	Execute Time
					Apply To All 17:30
Sunday	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	17:30
Monday	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	17:30
Tuesday	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	17:30
Wednesday	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	17:30
Thursday	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	17:30
Friday	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	17:30
Saturday	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	17:30

Power On Weekdays Settings  
This setting is only applicable to Macintosh systems running OSX 10.4.x and

Existing Templates

Default

Power - Mac

Power - Windows

New Template

CopyRemove

Previous

Next

You will be prompted to set a job schedule. Choose the start date and time, how often the job should run, and on which days. A job can be scheduled to run up to five times a day.

The image displays four screenshots of a job scheduling wizard interface, arranged in a 2x2 grid.

**Top Left Screenshot: "How should this job be scheduled?"**  
This screen contains three radio button options: "Select A Schedule:", "Run Immediately", and "Create A New Template...". Below these, there are two more radio button options: "Recurring" (which is selected) and "One-Time". At the bottom left, there is a checkbox labeled "Enforce Blackout Calendar". At the bottom right, there are "Next" and "Cancel" buttons.

**Top Right Screenshot: "Choose a start date."**  
This screen is for setting the start date and time. It includes a "Start Date:" field with a date picker showing "14/02/2011". Below it is a "Start Time:" dropdown menu set to "06:00". There are also buttons for "+ Add additional start times." and "- Remove last start time.". Below these are five more "Start Time" dropdown menus, labeled "Start Time 2:" through "Start Time 5:", with values "09:30", "12:30", "15:00", and "20:00" respectively. At the bottom right, there are "Previous", "Next", and "Cancel" buttons.

**Bottom Left Screenshot: "How often should this job run?"**  
This screen is for setting the frequency of the job. It has two radio button options: "Every Week" (selected) and "Every Month". Below this, it says "This job should run on..." and lists days of the week with checkboxes: "All Days", "Week Days" (selected), "Sunday", "Monday", "Tuesday", "Wednesday", "Thursday", "Friday", and "Saturday". At the bottom right, there are "Previous", "Next", and "Cancel" buttons.

**Bottom Right Screenshot: "Schedule Summary..."**  
This screen provides a summary of the configured schedule. It lists: "Frequency: Every Day", "Intelligent Removal Once Completed Successfully: Disabled", "Start Date: Monday, February 14, 2011", "Run Time: 06:00, 09:30, 12:30, 15:00, 20:00", and "Days: Monday, Tuesday, Wednesday, Thursday, Friday". At the bottom right, there are "Previous", "Finish", and "Cancel" buttons.

Finally, you will be prompted to review the tasks and schedule before saving the job. By default, the wizard does not attempt to deploy the client on devices with blank names. To override this, check Allow Blank Device Names.

**Add / Edit A Job...**

Create a job that will run one or more times using templates that you have created.

**Job Details**

Job Name:

☐ Allow Blank Device Names

☐ Create groups for failure codes

**Schedule Summary...**

**Frequency:** Every Day

**Intelligent Removal Once Completed Successfully:** Disabled

**Start Date:** Thursday, March 07, 2013

**Run Time:** 06:00, 09:00, 12:30, 15:00, 20:00

**Days:** Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday

[Configure Schedule](#)

Task Name	Template Name				
Discovery	Automation Network 2K	↑	↓	<a href="#">Edit</a>	<a href="#">X</a>
Client Deployment	Windows Deployment	↑	↓	<a href="#">Edit</a>	<a href="#">X</a>
Wait		↑	↓	<a href="#">Edit</a>	<a href="#">X</a>
Set Area Manager IP Address	Local System Area Manager	↑	↓	<a href="#">Edit</a>	<a href="#">X</a>
Wait		↑	↓	<a href="#">Edit</a>	<a href="#">X</a>
Set Location or Function	Windows Location and Function	↑	↓	<a href="#">Edit</a>	<a href="#">X</a>
Set Power Schedule	Power - Windows	↑	↓	<a href="#">Edit</a>	<a href="#">X</a>

[+ Add Task](#)

[Save Changes](#) [Cancel](#)

**(Please note** that in an environment where User Account Control is enabled on target machines, you will need to click the blue Edit links for Client Deployment and Set Area Manager IP Address to change the authentication template to the one for local administrator. For further details, please refer to the SyAM Tool Tip on Management Utilities Configuration for UAC Environments.)

When you have reviewed the wizard configuration, click the Save Changes button to add the installation job to the schedule.

Once a wizard job has been created, clicking the Unattended Installation Wizard link will display a list of wizard jobs.

Configure Template					
<a href="#" style="background-color: #f0f0f0; padding: 2px 5px;">Start Wizard</a>					
Wizard Name	Status				
Unattended Installation Wizard - Lab Network	Enabled	<a href="#">Suspend</a>	<a href="#">Edit</a>	<a href="#">Copy</a>	<a href="#">Remove</a>
Unattended Installation Wizard - Office Network - Windows	Enabled	<a href="#">Suspend</a>	<a href="#">Edit</a>	<a href="#">Copy</a>	<a href="#">Remove</a>

Here you can edit, copy, or delete a wizard job. A job may also be suspended or resumed.

## Chapter 5 – Client Deployment and Configuration

A key function of the Management Utilities is the automated deployment and configuration of the System Client.

The templates used for client deployment and configuration are:

- Authentication
- Client Deployment
- Discovery
- Location/Function
- Notifications
- Power Settings
- Remote Console Settings
- Area Manager IP Address
- System Alert Matrix
- Wake on LAN

### Authentication Settings Template - Windows

The first time you access Management Utility you will be prompted to create an Authentication template, which is used to store the username and password to access the server share and target systems for silently deploying applications and configuring the system Client. Enter a Template Name, Username and Password (and Domain, if using an Active Directory login.) Press Save to save your template, then click on the top right hand corner X to close the window and continue.

**Authentication Settings Template**

Define administrator usernames / passwords used in your network.

**No Authentication Settings Templates found. Please create a template before proceeding.**

Template Name:

☐ Install as local system (the file must be copied to each system before installation) - (UAC)

**Impersonation**

Install impersonating this user on each target machine

User name:

Password:

Domain:

☒ Grant this user "logon as service" permissions (required unless the account already has this privilege).

☒ Remove "logon as service" permissions when finished (this will remove the privilege from the account, even if it was not granted by this program).

☒ Impersonate this user locally (required if you are not logged in as the above user). This user **MUST** exist on the local system, and copying locally cannot be enabled!

**Mac Authentication**

Enter Mac administrator authentication information

User name:

Password:

**Linux / VMWare ESXi Authentication**

Enter Linux administrator authentication information

User name:

Password:

**Existing Templates**

**New Template**

Copy Remove



**This user must be an administrator on your Windows network and have access to the target systems you will be deploying software to.**



## Authentication Settings and User Account Control

When configuring Management Utilities for an environment where User Account Control is enabled on Windows systems, features such as Client Deployment and Third Party Software Deployment require an additional authentication template. The Local Admin template uses the same authentication as the normal Domain Admin template, but the Install as local system option is checked, and three other options (Grant logon as service, Remove permissions when finished, Impersonate this user locally) must be unchecked. (It is also necessary to configure the Management Utilities server so that the Management Utilities service is run by a domain administrator rather than by Local System. Please refer to the SyAM Tool Tip on Management Utilities Configuration for UAC Environments.)

Configure Template

Authentication Settings Template

Define administrator usernames / passwords used in your network.

Template Name:

☒ Install as local system (the file must be copied to each system before installation) - (UAC)

Impersonation

Install impersonating this user on each target machine

User name:

Password:

Domain:

☐ Grant this user "logon as service" permissions (required unless the account already has this privilege).

☐ Remove "logon as service" permissions when finished (this will remove the privilege from the account, even if it was not granted by this program).

☐ Impersonate this user locally (required if you are not logged in as the above user). This user MUST exist on the local system, and copying locally cannot be enabled!

Mac Authentication

Enter Mac administrator authentication information

User name:

Password:

Linux / VMWare ESXi Authentication

Enter Linux administrator authentication information

User name:

Password:

Existing Templates

Windows Domain Admin

Windows Local Admin

New Template



## Authentication Settings Template – Macintosh OSX

For deploying to Mac systems you keep the Windows administrator information to access the Windows share where the Mac apps are stored for deployment, then enter the username and password that is a system admin on each of the Mac target systems.

Configure Template

Authentication Settings Template

Define administrator usernames / passwords used in your network.

Template Name:

☐ Install as local system (the file must be copied to each system before installation)

Impersonation

Install impersonating this user on each target machine

User name:

Password:

Domain:

☒ Grant this user "logon as service" permissions (required unless the account already has this privilege).

☒ Remove "logon as service" permissions when finished (this will remove the privilege from the account, even if it was not granted by this program).

☒ Impersonate this user locally (required if you are not logged in as the above user). This user MUST exist on the local system, and copying locally cannot be enabled!

Mac Authentication

Enter Mac administrator authentication information

User name:

Password:

Linux / VMWare ESXi Authentication

Enter Linux administrator authentication information

User name:

Password:

Save Changes

Cancel

Existing Templates

Windows Admin

Windows Admin - Copy

Windows Domain Admin

New Template

Copy

Remove

## Authentication Settings Template – Linux and VMWare ESXi

For deploying to Linux systems you keep the Windows administrator information to access the Windows share where the Linux apps are stored for deployment, then enter the username and password that is a system admin on each of the Linux target systems. You can use the same authentication template for VMWare ESXi if the authentication credentials are the same, or you can create a separate template.

Configure Template

Authentication Settings Template

Define administrator usernames / passwords used in your network.

Template Name:

☐ Install as local system (the file must be copied to each system before installation)

Impersonation

Install impersonating this user on each target machine

User name:

Password:

Domain:

☒ Grant this user "logon as service" permissions (required unless the account already has this privilege).

☒ Remove "logon as service" permissions when finished (this will remove the privilege from the account, even if it was not granted by this program).

☒ Impersonate this user locally (required if you are not logged in as the above user). This user MUST exist on the local system, and copying locally cannot be enabled!

Mac Authentication

Enter Mac administrator authentication information

User name:

Password:

Linux / VMWare ESXi Authentication

Enter Linux administrator authentication information

User name:

Password:

Save Changes

Cancel

Existing Templates

Macintosh

Windows Admin

Windows Admin - Copy

Windows Domain Admin

New Template

Copy

Remove

## Client Deployment Template - Windows

Select the target OS and the corresponding authentication template, then type the path to the directory that contains the client executable. Click the Find Files button to populate the drop down menu where you can choose the correct executable file.

**Configure Template**

**Client Deployment Template**

Define the paths to executables used to silently deploy System Clients across your network.

Template Name:

**Choose Installation Source**  
**Choose installation source (must be System Client Version 3.3 or above):**

**Target Platform**  
☒ Windows  
☐ Linux  
☐ Mac OS X  
☐ VMWare ESXi

**Select File**  
Select the authentication template with credentials to browse the network share entered below

**Path to directory containing source executable file (depsvc.exe MUST be present in this directory):**  
  
**Find Files...**

☐ Copy this file locally to each target machine before installing (required if the above is not a network share, cannot be used with local impersonation)  
☐ Install this file as a PKG.

**SyAM Software Parameters**  
☐ Agent with Local Interface  
☒ Agent only  
Client Version (ex 4.32):   
Computer Type:   
Preferred Language:   
☐ Enable SSL  
Install Directory:   
Timeout (Minutes):

**Save Changes** **Cancel**

**Existing Templates**  
  
**New Template**  
**Copy** **Remove**

When specifying the path to the directory containing installation files, or to the installation directory on the client machine, quotation marks should not be used. Spaces in folder names are supported.

## Client Deployment and User Account Control

For UAC environments, the Client Deployment template should specify the normal domain authentication template, and the Copy this file locally option must be checked. When running a job using this template, configure the job to use the local admin authentication. For further information, please refer to the SyAM Tool Tip on Management Utilities Configuration for UAC Environments.

**Configure Template**

**Client Deployment Template**

Define the paths to executables used to silently deploy System Clients across your network.

Template Name:

Choose Installation Source

**Choose installation source (must be System Client Version 3.3 or above):**

Target Platform

☒ Windows  
☐ Linux  
☐ Mac OS X  
☐ VMWare ESXi

Select File

Select the authentication template with credentials to browse the network share entered below

Path to directory containing source executable file (depsvc.exe MUST be present in this directory):

☒ Copy this file locally to each target machine before installing (required if the above is not a network share, cannot be used with local impersonation)

☐ Install this file as a PKG.

SyAM Software Parameters

☐ Agent with Local Interface  
☒ Agent only

Client Version (ex 4.32)

Computer Type:

Preferred Language:

☐ Enable SSL

Existing Templates

**New Template**

## Client Deployment Template - Macintosh

When deploying to Mac OSX, the client installation files must be stored on a local drive of the Management Utilities server, and the path name must be a local drive path such as c:\apps instead of specifying a Windows network share. The option to copy the file locally before installation must be checked (this is typically done automatically when Mac options are selected). The Client Version will need to be entered, as the field is not automatically populated as it is for Windows clients.

If you install using the Mac package file (with the pkg.zip extension) check the “Install this file as a PKG” box. For installations using install.sh do not check this box.

**Configure Template**

**Client Deployment Template**

Define the paths to executables used to silently deploy System Clients across your network.

Template Name:

Choose Installation Source

Choose installation source (must be System Client Version 3.3 or above):

Target Platform

☐ Windows

☐ Linux

☒ Mac OS X

☐ VMWare ESXi

Select File

Select the authentication template with credentials to browse the network share entered below

Path to directory containing source executable file (depsvc.exe MUST be present in this directory):

☒ Copy this file locally to each target machine before installing (required if the above is not a network share, cannot be used with local impersonation)

☒ Install this file as a PKG.

SyAM Software Parameters

☐ Agent with Local Interface

☒ Agent only

Client Version (ex 4.32)

Computer Type:

Preferred Language:

☐ Enable SSL:

Install Directory:

Timeout (Minutes):

Existing Templates

New Template

## Client Deployment Template - Linux

Select the target OS and the corresponding authentication template, then type the path to the directory that contains the client executable. Click the Find Files button to populate the drop down menu where you can choose the correct executable file. The Client Version will need to be entered, as the field is not automatically populated as it is for Windows clients.

**Configure Template**

**Client Deployment Template**  
Define the paths to executables used to silently deploy System Clients across your network.

Template Name:

**Choose Installation Source**  
**Choose installation source (must be System Client Version 3.3 or above):**

**Target Platform**  
☐ Windows  
☒ Linux  
☐ Mac OS X  
☐ VMWare ESXi

**Select File**  
Select the authentication template with credentials to browse the network share entered below  
  
  
Path to directory containing source executable file (depsvc.exe MUST be present in this directory):

☒ Copy this file locally to each target machine before installing (required if the above is not a network share, cannot be used with local impersonation)  
☐ Install this file as a PKG.

**SyAM Software Parameters**  
☐ Agent with Local Interface  
☒ Agent only  
Client Version (ex 4.32):   
Computer Type:   
Preferred Language:   
☐ Enable SSL:  
Install Directory:   
Timeout (Minutes):

**Existing Templates**  
Linux Client 4.52  
Mac Client 4.52  
Windows Client 4.52  
  
**New Template**



## Client Deployment Template – VMWare ESXi

When deploying to ESXi systems, the client installation files must be stored on a local drive of the Management Utilities server, and the path name must be a local drive path such as c:\apps instead of specifying a Windows network share. The option to copy the file locally before installation must be checked (this is typically done automatically when ESXi options are selected). The Client Version will need to be entered, as the field is not automatically populated as it is for Windows clients.

Configure Template

Client Deployment Template

Define the paths to executables used to silently deploy System Clients across your network.

Template Name: ESXi Client 4.52

Choose Installation Source

Choose installation source (must be System Client Version 3.3 or above):

Target Platform

☐ Windows

☐ Linux

☐ Mac OS X

☒ VMWare ESXi

Select File

Select the authentication template with credentials to browse the network share entered below

ESXi

Path to directory containing source executable file (depsvc.exe MUST be present in this directory):

c:\apps

Find Files... syam-v4.52-0001.tgz

c:\apps\syam-v4.52-0001.tgz

☒ Copy this file locally to each target machine before installing (required if the above is not a network share, cannot be used with local impersonation)

☐ Install this file as a PKG.

SyAM Software Parameters

☐ Agent with Local Interface

☒ Agent only

Client Version (ex 4.32)

4.52

Computer Type:

Desktop

Preferred Language:

English (US)

☐ Enable SSL:

Install Directory:

C:\SyAM

Timeout (Minutes):

10

Existing Templates

ESXi Client 4.52

Linux Client 4.52

Mac Client 4.52

Windows Client 4.52

New Template

Copy

Remove

Save Changes

Cancel



## Discovery Template

The Discovery Template is discussed in the section on the Network Discovery Wizard. Whether you are using the interface in Configure Templates, or the Network Discovery Wizard, or the Unattended Installation Wizard, the same options are available for creating, editing or removing a Discovery Template.

Configure Template

Discovery Template

Template Name: Office

Discovery Group Name: Office Network

☒ Allow systems with duplicate information

Domain Options

☐ Scan my domain (you must be logged into the domain)

Discover Domains Discover Organizational Units

Domain:

Organizational Units:

☐ Replicate OUs

Network Scan

☒ Scan IP address range

Starting IP address: 192.168.200.1

Ending IP address: 192.168.200.254

☒ Resolve IP address to host name

Other Options

☐ Only discover systems that meet the following filter:

Exclude systems that meet the following filters: Add

Remove

Save Changes Cancel

Existing Templates

Automation Network 2K

G4 Macs

Office

Replicate OUs

New Template

Copy Remove



In this example we have defined a template called Office. The group name is Office Network and the discovery is through an IP Scan of IP addresses 192.168.200.1 to 192.168.200.254 with no filtering on machine name, and allowing systems with duplicate information.

Filtering for discovery templates is based on machine names. A single filter can be used to include systems; multiple filters can be used to exclude systems. Wildcards can be used in filters. A question mark substitutes a single character, an asterisk for an indefinite number of characters.

The screenshot shows the 'Configure Template' window for a 'Discovery Template'. The window has a blue header bar with the text 'Configure Template' and a white sub-header bar with the text 'Discovery Template'.

**Template Name:** Finance OU

**Discovery Group Name:** Finance

☒ Allow systems with duplicate information

**Domain Options**

☒ Scan my domain (you must be logged into the domain)

**Discover Domains** **Discover Organizational Units**

**Domain:** TESTDOMAIN.local

**Organizational Units:** Finance

☐ Replicate OUs

**Network Scan**

☐ Scan IP address range

**Starting IP address:**

**Ending IP address:**

☐ Resolve IP address to host name

**Other Options**

☒ Only discover systems that meet the following filter: \*xp\*

**Exclude systems that meet the following filters:**

**Add**

**Remove**

**Existing Templates**

Automation Network 2K

Finance OU

G4 Macs

Replicate OUs

**New Template**

**Copy** **Remove**

**Save Changes** **Cancel**



In this example we have defined a template called Finance OU. The group name is Finance and the discovery is of the Organizational Unit called Finance on the Domain called TESTDOMAIN with filtering set to only show machines where the machine name contains **xp**.



**For all template types, you can select multiple existing templates to copy or remove.**

## Location and Function Template

You can specify locations and functions for your systems. Location and function may be set separately, or together. Choose a template name that reflects what the template does.

Up to ten templates can be created on one page.

Details	
Location and Function Template	
<div>Location / Function Template:</div> <div>Template Name: <input type="text" value="Sales Office"/></div> <div><input checked="" type="checkbox"/> Location <input type="text" value="Sales Office"/></div> <div><input checked="" type="checkbox"/> Function <input type="text" value="Sales Notebook"/></div>	<div>Existing Templates</div> <div></div> <div>New Template</div> <div><input type="button" value="Copy"/> <input type="button" value="Remove"/></div>
<div>Location / Function Template:</div> <div>Template Name: <input type="text" value="Support Workstation"/></div> <div><input type="checkbox"/> Location <input type="text"/></div> <div><input checked="" type="checkbox"/> Function <input type="text" value="Support Workstation"/></div>	
<div>Location / Function Template:</div> <div>Template Name: <input type="text" value="1 Main St 3rd Floor"/></div> <div><input checked="" type="checkbox"/> Location <input type="text" value="1 Main St 3rd Floor"/></div> <div><input type="checkbox"/> Function <input type="text"/></div>	
<div>Location / Function Template:</div> <div>Template Name: <input type="text"/></div> <div><input type="checkbox"/> Location <input type="text"/></div> <div><input type="checkbox"/> Function <input type="text"/></div>	
<div>Location / Function Template:</div> <div>Template Name: <input type="text"/></div>	

## Notification Settings Template

System alert notifications (see System Alert Matrix, below) can be sent via email or abbreviated email to your cell phone (SMS). Specify the addresses for these notifications, and enter authentication information for your mail server to allow the emails to be sent. You can also specify an IP address where you monitor SNMP traps.

Configure Template

### Notification Settings Template

Define notification settings for systems in your network.

Template Name:

Notification Settings

Email Address	<input type="text" value="server-support@company.com"/>
SMS / Pager Address	<input type="text"/>
Username	<input type="text" value="admin@company.com"/>
Sender's Email Address	<input type="text" value="admin@company.com"/>
Sender's Email Password	<input type="password" value="•••••"/>
Mail Server	<input type="text" value="mailserver.company.com"/>
SNMP Trap Receiver	<input type="text"/>

Existing Templates

New Template

## Power Settings Template

Create a Power Settings Template to configure power management for client machines. A daily shutdown, restart, or hibernate can be scheduled for each day of the week. SyAM System Client checks for recent keyboard or mouse activity to insure that scheduled actions do not interfere with system users. A template may also include a list of applications that, if found to be running at the time a shutdown or other scheduled action is to occur, will prevent that scheduled action.

Timeouts can be set to turn off the monitor or hard disks, place the system in standby, hibernation, or (for Windows 7 or 8) hybrid sleep mode, after a specified period of inactivity.

The Power On Weekdays option is available for Macintosh OSX 10.4 or later.

Forced log off or screen lock after a period of keyboard and mouse inactivity can be configured by the Power Settings Template.



***Scheduling a hibernation action will leave the system in that state until it is powered back on.***



***To use hibernation mode, set a timeout or schedule a hibernation action. Enabling both on the same machine is not recommended.***

## Configure Template

## Power Settings Template

Template Name:

Weekdays 6 PM

## Timeout Settings for AC Main

Turn off monitor: After 5 Minutes ▼

Turn off hard disks: Never ▼

System standby: Never ▼

Hibernate: Never ▼

Hybrid Sleep (Windows 7 / 8 only): Disable ▼

## Power Management Scheduler Settings

Schedule	No Action	Shutdown	Restart	Hibernate	Execute Time
					Apply To All 18:00 ▼
Sunday	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	00:00 ▼
Monday	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	18:00 ▼
Tuesday	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	18:00 ▼
Wednesday	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	18:00 ▼
Thursday	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	18:00 ▼
Friday	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	18:00 ▼
Saturday	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	00:00 ▼

## Power On Weekdays Settings

This setting is only applicable to Macintosh systems running OSX 10.4.x and above

No Action Power On

Weekdays ☒ ☐ 00:00 ▼

## Advanced Power Management (requires V4 client or above)

Check for Activity Timer 15 Minutes ▼

Shutdown Countdown Timer 2 Minutes ▼

Wait Period before rechecking 15 Minutes ▼

Number of attempts to shutdown 4 ▼

Application	
<input checked="" type="radio"/>	payroll.exe

Remove Application

Enter application executable name:

Add Application

## System Security - User Log Off / Lock Screen Settings

If a defined application is running the screen will be locked.

Check for User Inactivity

15 Minutes ▼

Force Log Off Lock Screen



Save Changes

Cancel

## Existing Templates

Weekdays 6 PM

## New Template

Copy

Remove

## Remote Console Settings Template

You can configure systems to accept or deny remote console connections. Settings can be applied according to bandwidth and security requirements.

Configure Template

### Remote Console Settings Template

Define remote console settings for systems in your network.

Template Name:

Incoming Connections

☒ Accept Incoming Connections

Password (limited to 8 characters):

Update Handling

☐ Poll Full Screen (recommended for x64 targets)

☒ Poll Foreground Window

☐ Poll Window Under Cursor

Accept Remote Console Connection Options

☐ Display Connection Window

☒ AutoAccept

☐ AutoReject

Timeout (seconds):

Connection Settings

☐ Disable Remote Keyboard and Pointer

☐ Remove Desktop Wallpaper

Existing Templates

New Template

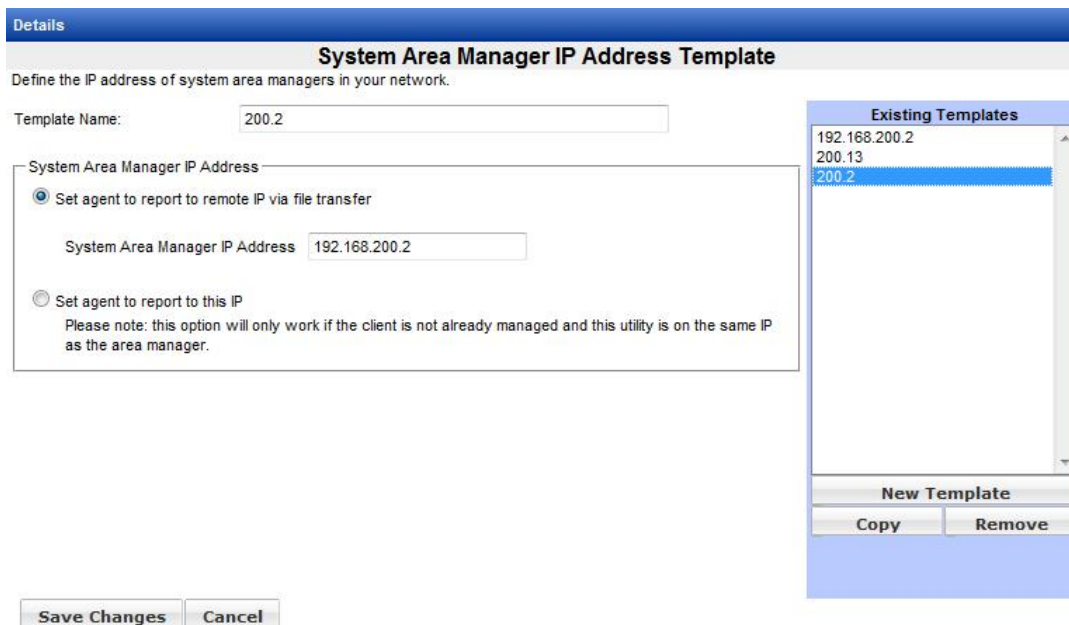
CopyRemove

Save ChangesCancel



## Area Manager IP Address Template

Systems can be assigned to be managed by your System Area Manager. The first method, using file transfer, can be used to connect to an Area Manager at any IP address.



**Details**

### System Area Manager IP Address Template

Define the IP address of system area managers in your network.

Template Name:

System Area Manager IP Address

☒ Set agent to report to remote IP via file transfer

System Area Manager IP Address

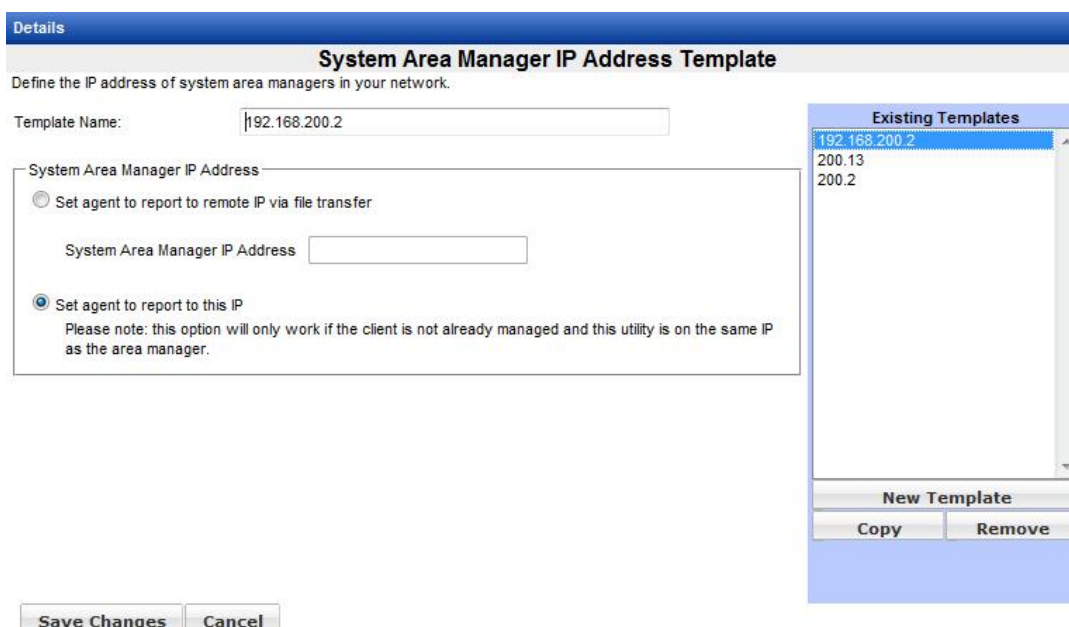
☐ Set agent to report to this IP  
Please note: this option will only work if the client is not already managed and this utility is on the same IP as the area manager.

**Existing Templates**

- 192.168.200.2
- 200.13
- 200.2

**New Template**

The second method does not require a file to be transferred, so it may be used when network settings do not allow the first method. This method requires that the client is not already managed and reporting to an Area Manager. It also requires that the Area Manager is at the same IP address as the Management Utilities.



**Details**

### System Area Manager IP Address Template

Define the IP address of system area managers in your network.

Template Name:

System Area Manager IP Address

☐ Set agent to report to remote IP via file transfer

System Area Manager IP Address

☒ Set agent to report to this IP  
Please note: this option will only work if the client is not already managed and this utility is on the same IP as the area manager.

**Existing Templates**

- 192.168.200.2
- 200.13
- 200.2

**New Template**

## System Alert Matrix Template

The System Alert Matrix defines how systems will be monitored and what types of notification alerts will be sent. Choose which alerts will be generated (email, SMS text, etc.) for each physical or logical sensor, or choose the No Monitoring option if no alerts are needed. For CPU and memory, the reporting thresholds, sample periods, and reset periods can be configured. Different templates can be set up to be applied according to the type of system (workstation, notebook, server) or for any other defined groups. When you have made your selections, scroll down and click the Save Changes button.

Configure Template

System Alert Matrix Template

Define system alert matrix settings for systems in your network.

Template Name:

Physical Sensors

Description	No Alerts		Warning Alerts					Critical Alerts					
	No Monitoring	Email	SMS / Pager	System Area Manager	Local Alerting	SNMP Trap	System Event Log	Email	SMS / Pager	System Area Manager	Local Alerting	SNMP Trap	System Event Log
Physical Security	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>						
Fans (RPM)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Temperature (°C)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Thermal Controlled Fan	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Voltages (v)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Power Unit	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>						

Existing Templates

New Template

Copy Remove

Logical Sensors

Description	Threshold	No Alerts		Warning Alerts					Intervals	
		No Monitoring	Email	SMS / Pager	System Area Manager	Local Alerting	SNMP Trap	System Event Log	Sample Period	Reset Period
Network Adapters		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
Physical Disks		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
Logical Disks (%)	90	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	8 Hr	168 Hr
Managed RAID Controllers		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
CPU Utilization (%)	95	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	4 Min	240 Min
Memory Utilization (%)	95	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	4 Min	240 Min
Memory Error Rate	2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	24 Hr	24 Hr
Hardware Asset Change		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
Software Asset Change		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		

Save Changes Cancel

## Wake on LAN Template

Wake on LAN can be configured to wake client systems on the network. This feature must be supported by the client system hardware.

To wake systems on the same subnet as the Management Utilities server, select Local Subnet Broadcast and enter the broadcast subnet IP address.

The screenshot shows a web-based configuration interface for a 'Wake On LAN Template'. The main title is 'Configure Template' with a subtitle 'Wake On LAN Template'. Below the subtitle is a description: 'Define the settings for wake on LAN commands issued to systems in your network.' The 'Template Name' field is set to 'Local Subnet'. Under 'Wake On LAN Settings', there are three radio button options: 'Local Subnet Broadcast' (selected), 'Unicast packet to target system in another subnet', and 'Relay broadcast to another subnet'. A 'Broadcast Subnet' field is set to '255.255.255.0'. On the right, an 'Existing Templates' list shows 'Local Subnet' and 'Relay 200 Network'. Below this list are 'Copy' and 'Remove' buttons. At the bottom left are 'Save Changes' and 'Cancel' buttons.

Configure Template	
Wake On LAN Template	
Define the settings for wake on LAN commands issued to systems in your network.	
Template Name:	Local Subnet
<b>Wake On LAN Settings</b> Please select one of the options below:	
<input checked="" type="radio"/> Local Subnet Broadcast	
<input type="radio"/> Unicast packet to target system in another subnet	
<input type="radio"/> Relay broadcast to another subnet	
Broadcast Subnet	255.255.255.0
<b>Existing Templates</b>	
Local Subnet	
Relay 200 Network	
<b>New Template</b>	
Copy	Remove
<b>Save Changes</b> <b>Cancel</b>	

Because routers do not normally forward broadcast packets, two features are available to wake systems on another subnet. A unicast packet can be sent to a target system. The nearest router to the target system must have a static entry in its ARP table for that system.

Configure Template

Wake On LAN Template

Define the settings for wake on LAN commands issued to systems in your network.

Template Name:

Unicast Packet

Wake On LAN Settings

Please select one of the options below:

☐ Local Subnet Broadcast

☒ Unicast packet to target system in another subnet

☐ Relay broadcast to another subnet

The closest router to the target system MUST have a corresponding static entry in the ARP table.

Save Changes

Cancel

Existing Templates

Local Subnet

Relay 200 Network

New Template

Copy

Remove

The Broadcast Relay feature sends a wake packet through a relay system on the target subnet. The relay system must be running the System Client and must be managed by the System Area Manager. To configure a template using broadcast relay, enter the broadcast subnet IP and the name or IP address of the relay system.

Configure Template

Wake On LAN Template

Define the settings for wake on LAN commands issued to systems in your network.

Template Name:

Relay 200 Network

Wake On LAN Settings

Please select one of the options below:

☐ Local Subnet Broadcast

☐ Unicast packet to target system in another subnet

☒ Relay broadcast to another subnet

Broadcast Subnet

255.255.255.0

System must have the client installed and managed, be powered on, and in the same physical LAN segment as the target systems.

☐ Name

☒ IP Address

192.168.200.29

Save Changes

Cancel

Existing Templates

Local Subnet

Relay 200 Network

New Template

Copy

Remove

## Chapter 6 – Managing Job Templates and Creating Scheduled Jobs

Job templates are a convenient way to define and run recurring jobs, either on demand or following a schedule.



By default, the template name is based on the current date and time. For a saved job template, choose a name that reflects the template's functionality.

### Configuring a Job Template



Click the button to create a new job template. The Add / Edit A Job interface will be displayed.

## Configure Template

### Add / Edit A Job...

Create a job that will run one or more times using templates that you have created.

#### Job Details

Job Name: 11/12/2012 4:28:17 PM

☐ Create groups for failure codes

#### Schedule Summary...

No schedule configured... Job will run immediately by default.

**Intelligent Removal Once Completed Successfully:** Disabled

**Configure Schedule**

**+ Add Filter**

No tasks assigned yet...

**+ Add Task**

**+ Add Task Group**

**Save Job as New Template**

**Cancel**

## Adding Tasks to a Job

Add tasks to the job template by clicking the Add Task button. In this example, we start by deploying the System Client, using the templates we've already created. The Wait parameter allows time for all processes associated with a task to complete before starting the next task.

**New Task...**

Task: Client Deployment ▼

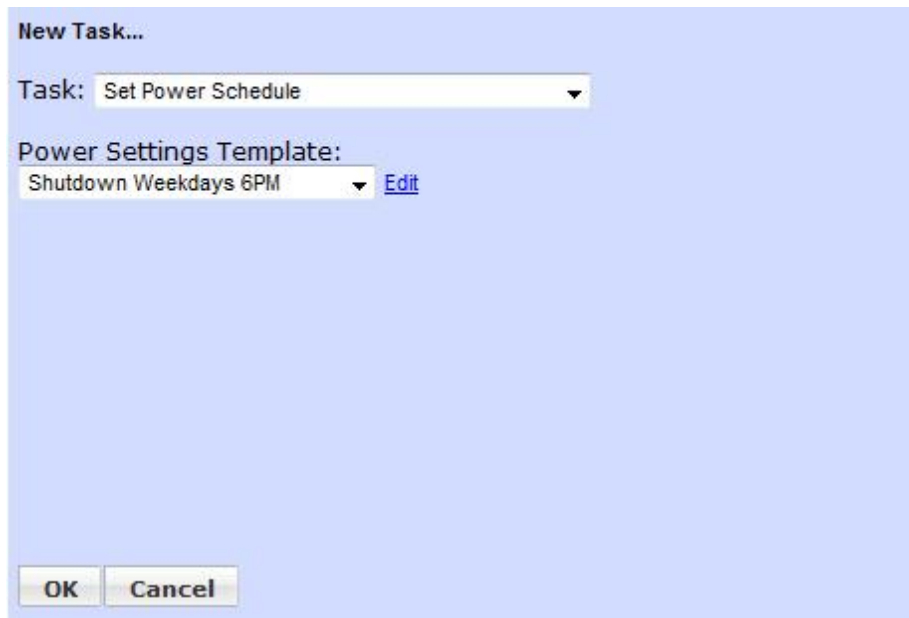
Authentication Template:  
Windows Admin ▼ [Edit](#)

Client Deployment Template:  
Windows Client 4.47 ▼ [Edit](#)

Wait (minutes):  
5

**OK** **Cancel**

The next task will configure the systems' power settings.



The screenshot shows a 'New Task...' dialog box with a light blue background. At the top, the title 'New Task...' is displayed. Below it, the 'Task:' dropdown menu is set to 'Set Power Schedule'. Underneath, the 'Power Settings Template:' section shows 'Shutdown Weekdays 6PM' selected in a dropdown, with an 'Edit' link to its right. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

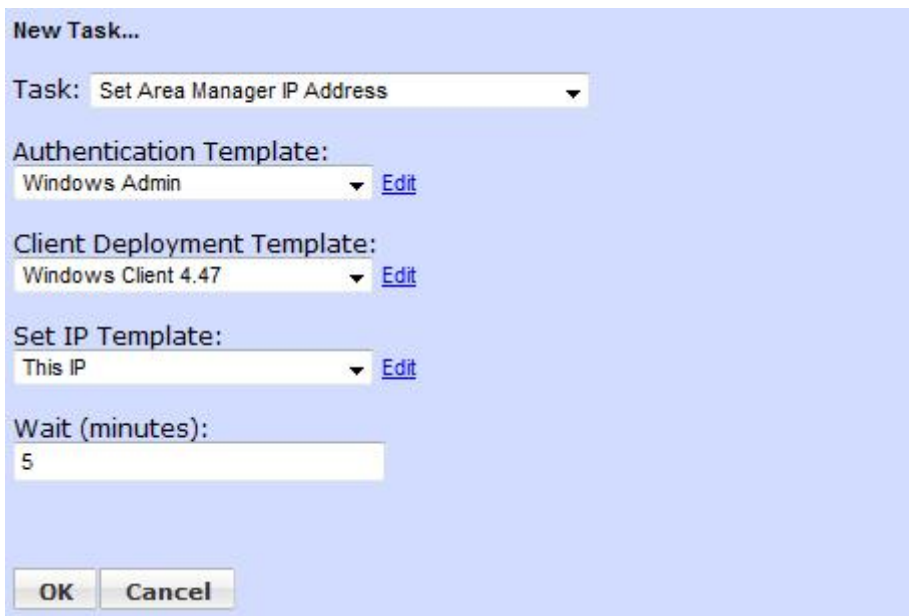
New Task...

Task: Set Power Schedule ▼

Power Settings Template:  
Shutdown Weekdays 6PM ▼ [Edit](#)

OK Cancel

Finally, we'll set the IP address for our System Area Manager.



The screenshot shows a 'New Task...' dialog box with a light blue background. The 'Task:' dropdown menu is set to 'Set Area Manager IP Address'. Below this, there are three template sections: 'Authentication Template:' with 'Windows Admin' selected and an 'Edit' link; 'Client Deployment Template:' with 'Windows Client 4.47' selected and an 'Edit' link; and 'Set IP Template:' with 'This IP' selected and an 'Edit' link. Below these templates is a 'Wait (minutes):' section with a text input field containing the number '5'. At the bottom are 'OK' and 'Cancel' buttons.

New Task...

Task: Set Area Manager IP Address ▼

Authentication Template:  
Windows Admin ▼ [Edit](#)

Client Deployment Template:  
Windows Client 4.47 ▼ [Edit](#)

Set IP Template:  
This IP ▼ [Edit](#)

Wait (minutes):  
5

OK Cancel



Choose an appropriate name for the job template.

Configure Template

Add / Edit A Job...

Create a job that will run one or more times using templates that you have created.

Job Details

Job Name:

☐ Create groups for failure codes

Schedule Summary...

No schedule configured... Job will run immediately by default.

Intelligent Removal Once Completed Successfully: Disabled

Configure Schedule

+ Add Filter

Task Name	Template Name				
Client Deployment	Windows Client 4.47	⬆	⬇	<a href="#">Edit</a>	✖
Wait		⬆	⬇	<a href="#">Edit</a>	✖
Set Power Schedule	Shutdown Weekdays 6PM	⬆	⬇	<a href="#">Edit</a>	✖
Set Area Manager IP Address	This IP	⬆	⬇	<a href="#">Edit</a>	✖
Wait		⬆	⬇	<a href="#">Edit</a>	✖

+ Add Task

+ Add Task Group

Save Job as New Template

Cancel

## Configuring a Schedule

For jobs that will be run on a regular schedule, click the Configure Schedule button. The option to enforce the blackout calendar is set by default. Uncheck the box if you want the job to run even on days that fall within a blackout period. You may also choose to have the job remove systems from the affected systems list when the job is successfully completed for that system. When this option is selected, a recurring job will not attempt to run on target systems where it has already succeeded.

**How should this job be scheduled?**

☐ Select A Schedule:

☐ Run Immediately

☒ Create A New Template...

---

☒ Recurring

☐ One-Time


☐ Intelligently remove systems from affected systems list after all tasks have completed successfully

☒ Enforce Blackout Calendar

Next Cancel

Choose the start date and the time of day the job will run. A job may run up to five times per day.

**Choose a start date.**

Start Date:    

Start Time:  ▼

Add additional start times.  Remove last start time.

Previous Next Cancel

Select the day or days when the job will run.

A screenshot of a software dialog box for scheduling a job. The dialog has a light blue background and a thin border. It contains two sections of radio buttons. The first section, titled "How often should this job run?", has two options: "Every Week" (selected with a blue dot) and "Every Month" (unselected). The second section, titled "This job should run on...", has two radio buttons at the top: "All Days" (unselected) and "Week Days" (unselected). Below these are seven checkboxes for the days of the week: Sunday, Monday (checked with a blue checkmark), Tuesday, Wednesday, Thursday, Friday, and Saturday. At the bottom right of the dialog are three buttons: "Previous", "Next", and "Cancel".

**How often should this job run?**

☒ Every Week  
☐ Every Month

**This job should run on...**

☐ All Days  
☐ Week Days

☐ Sunday  
☒ Monday  
☐ Tuesday  
☐ Wednesday  
☐ Thursday  
☐ Friday  
☐ Saturday

Previous Next Cancel

Review the schedule summary, then click Finish if everything is correct.

A screenshot of a software dialog box showing a schedule summary. The dialog has a light blue background and a thin border. It lists several configuration details: "Frequency: Every Day", "Intelligent Removal Once Completed Successfully: Disabled", "Enforce Blackout Calendar", "Start Date: Monday, November 12, 2012", "Run Time: 07:00", and "Days: Monday". At the bottom right of the dialog are three buttons: "Previous", "OK", and "Cancel".

**Schedule Summary...**

**Frequency:** Every Day

**Intelligent Removal Once Completed Successfully:** Disabled

**Enforce Blackout Calendar**

**Start Date:** Monday, November 12, 2012

**Run Time:** 07:00

**Days:** Monday

Previous OK Cancel

The schedule information is now displayed. Be sure to click the Save Job as New Template button in order to save the schedule as part of the template.

Configure Template

Add / Edit A Job...

Create a job that will run one or more times using templates that you have created.

Job Details

Job Name: Deploy Client Set Power + IP

☐ Create groups for failure codes

Schedule Summary...

Frequency: Every Day

Intelligent Removal Once Completed Successfully: Disabled

Enforce Blackout Calendar

Start Date: Thursday, March 07, 2013

Run Time: 07:00

Days: Monday

Configure Schedule

+ Add Filter

Task Name	Template Name				
Client Deployment	Windows Client 4.47	↑	↓	<a href="#">Edit</a>	<a href="#">×</a>
Wait		↑	↓	<a href="#">Edit</a>	<a href="#">×</a>
Set Power Schedule	Shutdown Weekdays 6PM	↑	↓	<a href="#">Edit</a>	<a href="#">×</a>
Set Area Manager IP Address	This IP	↑	↓	<a href="#">Edit</a>	<a href="#">×</a>
Wait		↑	↓	<a href="#">Edit</a>	<a href="#">×</a>

+ Add Task

+ Add Task Group

Save Job as New Template

Cancel

## Copying a Job Template

Clicking the Copy link to the right of a job template name will make an identical copy of the template. You can then edit the copied job template to change its name and other details as desired. This feature is useful when you need to create a new job that is similar to an existing one, but with only a few changes.

Details

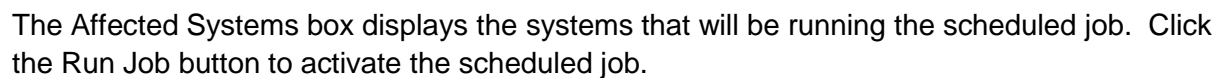
Manage Job Templates

Define jobs that can be applied to groups of systems more than once. Jobs defined here will be available from the context menu on the group page.

Create a new job template

Template Name			
Deploy Client Set Power + IP	<a href="#">Edit</a>	<a href="#">Copy</a>	<a href="#">Remove</a>
Deploy Client Set Power + IP - Copy	<a href="#">Edit</a>	<a href="#">Copy</a>	<a href="#">Remove</a>

Start the scheduled job for selected machines, or for an entire group, by right-clicking a selected system in Groups.



Details

Add / Edit A Job...

Create a job that will run one or more times using templates that you have created.

Job Details

Job Name:

☐ Save Job as Template (after running job)
 ☐ Remove devices from the following group upon successful completion: Lab
 ☐ Create groups for failure codes

Schedule Summary...

**Frequency:** Every Day  
**Intelligent Removal Once Completed Successfully:** Disabled  
**Enforce Blackout Calendar**  
**Start Date:** Thursday, March 07, 2013  
**Run Time:** 07:00  
**Days:** Monday

Configure Schedule

+ Add Filter

Task Name	Template Name				
Client Deployment	Windows Client 4.47	↑	↓	Edit	×
Wait		↑	↓	Edit	×
Set Power Schedule	Shutdown Weekdays 6PM	↑	↓	Edit	×
Set Area Manager IP Address	This IP	↑	↓	Edit	×
Wait		↑	↓	Edit	×

+ Add Task

+ Add Task Group

Run Job Cancel

Affected Systems

Lab

The job will be displayed in Scheduled Jobs.

Scheduled Jobs

▶ Remaining Today

▼ Daily
 

▶ Deploy Client Set Power +

▶ Monthly

▶ In Progress

▶ Completed Today

▶ Suspended

You may wish to create a group of systems that require a job to be run on them, and then run the job with the Remove devices from the group option enabled. Once the job has successfully completed on a system, it will be removed from the group if the option is enabled.

When the Create groups for failure codes option is selected, any target system on which a task fails will be copied into the Job Errors group. This group contains subgroups called Grouped by

Code and Grouped by Job. This allows you to find all the systems reporting failures for a particular job, or for a specific error code.

## Job Filtering Options

Management Utility jobs support filtering by machine name, IP address, and client version. To use filtering, click the Add Filter button.

**Details**

**Add / Edit A Job...**

Create a job that will run one or more times using templates that you have created.

**Job Details**

Job Name: Deploy Client Set Power + IP

☒ Save Job as Template

☐ Create groups for failure codes

**Schedule Summary...**

Frequency: Every Day

Intelligent Removal Once Completed Successfully: Disabled

Enforce Blackout Calendar

Start Date: Thursday, March 07, 2013

Run Time: 07:00

Days: Monday

**Configure Schedule**

Filter (Required)	Template Name				
+ Add Filter					
Machine Name	Windows Client 4.47	↑	↓	Edit	×
IP Address	Shutdown Weekdays 6PM	↑	↓	Edit	×
Client Version (ex 4.32)	This IP	↑	↓	Edit	×
Wait		↑	↓	Edit	×
Set Power Schedule		↑	↓	Edit	×
Set Area Manager IP Address		↑	↓	Edit	×
Wait		↑	↓	Edit	×

+ Add Task

+ Add Task Group

Save Template Changes Cancel

Up to three filters can be set for each task group. Multiple filters are ANDed together, so all conditions must be satisfied for a machine to be selected as a target. The Machine Name filter can select machines with an exact name, or machines with names that contain a specified substring. The IP Address filter selects a specific IP or a range from lower to higher. The Client Version filter can select machines where the installed SyAM System Client is less than, greater than, or equal to a particular version, or between a lower and a higher version.

Select a filter type, then a logical operator, then fill in the entry field:

- **Machine Name =** (Exact name of machine)
- **Machine Name Contains** (Substring of machine name)
- **IP Address =** (IP Address of machine)
- **IP Address Between** (Lower IP of range) (Higher IP of range)



- **Client Version <** (Filter selects clients lower than this version)
- **Client Version >** (Filter selects clients higher than this version)
- **Client Version =** (Filter selects this client version)
- **Client Version Between** (Lower version of range) (Higher version of range)

Note that the Client Version is specified with two digits after the decimal point, for example 4.49.

Click the Add Task Group button to define an additional group of tasks using different filter options. For example, an IP address range may contain a mix of teacher and student systems that can be identified by machine names containing “teacher” or “student”. If you would like to apply different power settings to each type of system, you can set up a single job to do that by using filtering options. In this example there are two task groups, and the differences between them are in the filter setting and the template used by the Set Power Schedule task.

Filter (Required) Machine Name Contains teacher

+ Add Filter

Task Name	Template Name				
Client Deployment	Windows Client 4.49	↑	↓	<a href="#">Edit</a>	✖
Wait		↑	↓	<a href="#">Edit</a>	✖
Set Area Manager IP Address	This IP	↑	↓	<a href="#">Edit</a>	✖
Wait		↑	↓	<a href="#">Edit</a>	✖
Set Power Schedule	Power Settings - Teachers	↑	↓	<a href="#">Edit</a>	✖

+ Add Task

Filter (Required) Machine Name Contains student

+ Add Filter

Task Name	Template Name				
Client Deployment	Windows Client 4.49	↑	↓	<a href="#">Edit</a>	✖
Wait		↑	↓	<a href="#">Edit</a>	✖
Set Area Manager IP Address	This IP	↑	↓	<a href="#">Edit</a>	✖
Wait		↑	↓	<a href="#">Edit</a>	✖
Set Power Schedule	Power Settings - Students	↑	↓	<a href="#">Edit</a>	✖

+ Add Task

+ Add Task Group

## Creating a Scheduled Wake On LAN Job

Systems that support the Wake On LAN feature can be activated through Management Utilities. Create a Wake On LAN Template following the instructions in the last chapter.

Configure Template

Wake On LAN Template

Define the settings for wake on LAN commands issued to systems in your network.

Template Name:

Office Network

Wake On LAN Settings

Please select one of the options below:

☒ Local Subnet Broadcast

☐ Unicast packet to target system in another subnet

☐ Relay broadcast to another subnet

Broadcast Subnet

255.255.255.0

Save Changes

Cancel

Existing Templates

Office Network

New Template

Copy

Remove

Create a new job template in Manage Job Templates. Set the desired schedule, and then save changes when finished.

Configure Template

Add / Edit A Job...

Create a job that will run one or more times using templates that you have created.

Job Details

Job Name: Wake on LAN - Office Network

☐ Create groups for failure codes

Schedule Summary...

Frequency: Every Day

Intelligent Removal Once Completed Successfully: Disabled

Enforce Blackout Calendar

Start Date: Thursday, March 07, 2013

Run Time: 07:00

Days: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday

Configure Schedule

+ Add Filter

Task Name	Template Name				
Issue Wake On LAN Command	Office Network			Edit	

+ Add Task

+ Add Task Group

Save Job as New Template

Cancel

Right click on a system in Groups to schedule the job for a single system, for selected machines, or for the entire group.

[illegible]

Click the Run Job button to place the job in the schedule.

Details

Add / Edit A Job...

Create a job that will run one or more times using templates that you have created.

Job Details

Job Name: Wake on LAN - Office Network

- ☐ Save Job as Template (after running job)
- ☐ Remove devices from the following group upon successful completion: Lab
- ☐ Create groups for failure codes

Schedule Summary...

Frequency: Every Day  
Intelligent Removal Once Completed Successfully: Disabled  
Enforce Blackout Calendar  
Start Date: Thursday, March 07, 2013  
Run Time: 07:00  
Days: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday

[Configure Schedule](#)

+ Add Filter

Task Name	Template Name				
Issue Wake On LAN Command	Office Network	↑	↓	<a href="#">Edit</a>	<a href="#">×</a>

+ Add Task

+ Add Task Group

[Run Job](#) [Cancel](#)

Affected Systems (1)

WIN8ENTERX64

[Remove](#)

## Chapter 7 – Microsoft Patch Management

The Management Utility allows you to perform Microsoft vulnerability scans and execute patch management silently to systems across your network, either on demand or through an automated process.



**Please note that systems must have the System Client installed, running and managed by a System Area Manager before you can perform Patch Management actions to them.**

### On-Demand Vulnerability Scan

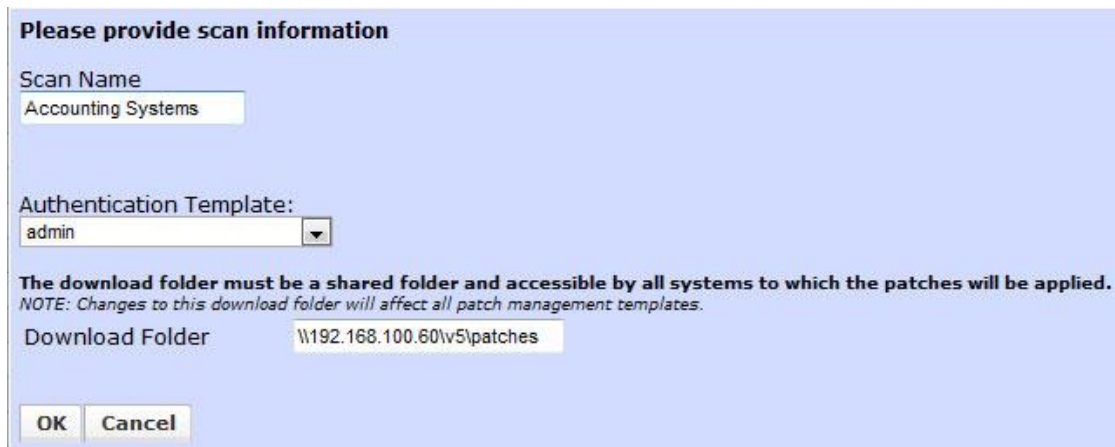
To perform on-demand vulnerability select the systems that you wish to scan, press the right mouse button and choose the Patch Scan Now option.

The screenshot shows the 'Details' view of the Management Utility for an 'Office' group. A table lists various systems with columns for OU, IP (1st), MAC, Name, OS, Client, Type, Mgd, and Area M. A right-click context menu is open over the table, showing options like 'Apply to Selected Machines', 'Apply to Group', 'Apply to Group & Subgroups', 'Schedule a job...', 'Client Deployment', 'Set Location or Function', 'Set Notification Settings', 'Patch Management', 'Set Power Schedule', 'Set Remote Console Settings', 'Shutdown', 'Set Area Manager IP Address', 'Set System Alert Matrix', 'Deploy Third Party Software', 'Issue Wake On LAN Command', 'Wait', 'Patch Scan Now' (highlighted), 'Refresh Selected Systems', 'Add to Restricted Access List', 'Add to Wake On LAN URL List...', 'Active Directory Management', and 'Copy Text to Clipboard'. The 'Patch Scan Now' option is highlighted in blue. The bottom of the window shows 'Page 1 of 11' and 'Next Page' and 'Next Block' buttons.

OU	IP (1st)	MAC	Name	OS	Client	Type	Mgd	Area M
			GATEWAY-7450R			Unknown	No	
						Unknown	No	
					[Linux]	Desktop	No	
						Unknown	No	
			SITEMGR-BUILD	Microsoft Windows X...	V4.50.550...	Desktop	Yes	19
						Unknown	No	
			CVS	Microsoft Windows X...	V4.49.000...	Desktop	Yes	0.0
						Unknown	No	
			Linux-Build-Server	Red Hat Linux releas...	V4.51-LIN...	Server	Yes	19
						Unknown	No	
			SYAMAPPLIANCE3	Microsoft Windows 7 ...	V4.51.500...	Desktop	Yes	19
			SYAM-BIGSERVER	Microsoft Windows S...	V4.51.500...	Server	Yes	19
						Unknown	No	
			WORKSTATION-NT2	Microsoft Windows 7 ...	V4.50.710...	Desktop	Yes	19
						Unknown	No	
			TFSSERVER			Unknown	No	
						Unknown	No	
			ROBERTS-DESKTOP	Microsoft Windows 7 ...	V4.51.500...	Desktop	Yes	19

This brings up a window that allows you to define the scan name and authentication template to be used to access the target systems and to set the network shared path to the folder where you wish to store the identified patches. Change the settings as required and press the OK button to perform the scan. (**Please note** that for environments where User Account Control is

enabled on Windows systems, patch scans and deployments should use the local admin authentication template.)



The screenshot shows a dialog box titled "Please provide scan information" with a light blue background. It contains the following fields and controls:

- Scan Name:** A text input field containing the text "Accounting Systems".
- Authentication Template:** A dropdown menu with "admin" selected.
- Download Folder:** A text input field containing the path "\\192.168.100.60\\v5\\patches".
- Buttons:** "OK" and "Cancel" buttons at the bottom left.

Below the Authentication Template field, there is a warning message: "The download folder must be a shared folder and accessible by all systems to which the patches will be applied." followed by a note: "NOTE: Changes to this download folder will affect all patch management templates."

You can view the scan results by expanding the Patch Scans heading and the Groups window and then clicking on the Scan Name.

## Details

## Accounting Systems

Patch Types

All

		Update for Windows 7 (KB2552343)	Update for Windows 7 (KB2616676)	Update for Windows 7 for x64- based Systems (KB2345688)	Update for Windows 7 for x64- based Systems (KB2506014)	Update for Windows 7 for x64- based Systems (KB2533552)	Update for Windows 7 for x64- based Systems (KB2552343)	Update for Windows 7 for x64- based Systems (KB2616676)	Update for Windows 7 for x64- based Systems (KB971033)	Update for Windows Media Format 11 SDK for Windows XP (KB929399)	Update for Windows Media Player 11 for Windows XP (KB939683)	Update for Windows Server 2008 x64 Edition (KB2345688)
Name	IP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
B1-P4SBA-XP	192.168.100.152	<input checked="" type="checkbox"/>									<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DB43LD-2K08-X64	192.168.100.151	<input checked="" type="checkbox"/>										<input checked="" type="checkbox"/>
DG31PR-W7E-X86	192.168.100.150	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>									
MS-7351-W7U-X64	192.168.100.153	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			

Select the authentication template with credentials to browse the network share entered below

Authentication Template: Windows

**The download folder must be a shared folder and accessible by all systems to which the patches will be applied.**

NOTE: Changes to this download folder will affect all patch management templates.

Download Folder \\192.168.100.151\patches

☐ Copy every patch locally to each target machine before installing (cannot be used with local impersonation).

Deploy Patches Now

Cancel



This screen provides a list of all identified patches missing from the systems scanned. You can filter the type of patches being displayed on screen by clicking on the Patch Type drop down menu. This menu allows you to select the following filters:

- Critical Updates
- Feature Packs
- Security Updates
- Service Packs
- Update Rollups
- Updates
- Windows Defender



For example, we set the filter Patch Types to view the Critical Updates only.

Details											
Accounting Systems											
Patch Types											
Critical Updates											
Name	IP	Update for Windows 7 for x64-based Systems (KB2345688)	Update for Windows 7 for x64-based Systems (KB971033)	Update for Windows 7 for x64-based Systems (KB976902)	Update for Windows Server 2008 for x64-based Systems (KB955020)	Update for Windows Server 2008 x64 Edition (KB951978)	Update for Windows Server 2008 x64 Edition (KB952287)	Update for Windows Server 2008 x64 Edition (KB955302)	Update for Windows Server 2008 x64 Edition (KB968389)	Update for Windows Server 2008 x64 Edition (KB973887)	Update for Windows Server 2008 x64 Edition (KB973917)
AMT7	192.168.100.29	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DB43LD-2k08-X64	192.168.100.151	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

You can perform patching on demand from this screen by checking off which patches you wish to deploy.

By default all check boxes are chosen but you can select and unselect specific patches by clicking the appropriate check box.

- You can select all or deselect all for a specific system by clicking on the check box next to the system name.
- You can select all or deselect all for a patch by clicking on the check box next to the patch name.

Once you have chosen the patches you wish to deploy, click on the Deploy Patches Now button and it will schedule the Patch Management Job for you to run immediately.



**Please Note that the Management Utility downloads the identified patch files automatically from Microsoft if it does not find them already stored on the network share defined for storing the patches.**

Once the Patch Management job has completed you can view the details in the Status window.

<b>Task:</b>	Patch Management
<b>Job Name:</b>	Accounting Systems
<b>Date Started:</b>	9/28/2010 9:10:39 AM
<b>Status:</b>	The containing job finished running at 9:12:22 AM.
<b>Successful Attempts:</b>	1
<b>Failed Attempts:</b>	0
<b>Unavailable Systems:</b>	0
<b>Total Systems Attempted:</b>	1

IP Address	Machine Name	Description	Details
192.168.200.81	HP-VPRO	Microsoft SQL Server 2008 Service Pack 1 (KB968369)	Succeeded

OK

## Automated Patch Management

Patch Management can be automated and scheduled using the Management Utility.

In order to schedule a job we need to create a Patch Management Template which will define the types of patches you wish to scan and deploy.

To access the Management Templates, expand the Configure Templates option within the Functions Window, and then click on Patch Management.

This will open up the Patch Management template screen.

Create a new Template or edit an existing template

Enter a Template name and check which types of patches are to be scanned and deployed when using that template.

Configure Template

Patch Management Template

Define automatic patch management settings for systems in your network.

Template Name:

Patch Types

Select the types of patches to apply...

☒ Critical Updates

☐ Security Updates

☐ Service Packs

☐ Update Rollups

☐ Feature Packs

☐ Updates

☐ Windows Defender

The download folder must be a shared folder and accessible by all systems to which the patches will be applied.

NOTE: Changes to this download folder will affect all patch management templates.

Download Folder

☐ Copy every patch locally to each target machine before installing (cannot be used with local impersonation).

Save Changes

Cancel

Existing Templates

All Patches

Critical Patches

New Template

Copy

Remove



This example shows a template which will just scan and patch Critical updates

Now that we have this template created we can apply the Critical Patches template against a system or systems at any time. Select the systems, right click and choose Patch Management.

**Details**  
**Office**

Number of systems per page: 25

[Copy](#) [Move](#) [Remove](#) [?](#)

OU	IP (1st)	MAC	Name	OS	Client	Type	Mgd	Area M
			ix-Build-Server	Red Hat Linux releas...	V4.51-LIN...	Server	Yes	19
						Unknown	No	
			MAPPLIANCE3	Microsoft Windows 7 ...	V4.51.500...	Desktop	Yes	19
			M-BIGSERVER	Microsoft Windows S...	V4.51.500...	Server	Yes	19
						Unknown	No	
			RKSTATION-NT2	Microsoft Windows 7 ...	V4.50.710...	Desktop	Yes	19
						Unknown	No	
			SERVER			Unknown	No	
						Unknown	No	
			BERTS-DESKTOP	Microsoft Windows 7 ...	V4.51.510...	Desktop	Yes	19
						Unknown	No	
						Unknown	No	
						Unknown	No	
						Unknown	No	
						Unknown	No	
						Unknown	No	
						Unknown	No	

Items: 1 - 25 of

Page 1 of 11 Next Page Next Block

☐ Apply to Selected Machines  
☒ Apply to Group  
☐ Apply to Group & Subgroups

[Schedule a job...](#)  
[Client Deployment](#)  
[Set Location or Function](#)  
[Set Notification Settings](#)  
[Patch Management](#)  
[Set Power Schedule](#)  
[Set Remote Console Settings](#)  
[Shutdown](#)  
[Set Area Manager IP Address](#)  
[Set System Alert Matrix](#)  
[Deploy Third Party Software](#)  
[Issue Wake On LAN Command](#)  
[Wait](#)

[Patch Scan Now](#)  
[Refresh Selected Systems](#)  
[Add to Restricted Access List](#)  
[Add to Wake On LAN URL List...](#)  
[Active Directory Management](#)  
[Copy Text to Clipboard](#)

This brings up the Patch Management Job window. Choose the authentication template that will be required to access the target systems and the Patch Management template that you wish to run on the target systems.

**New Task...**

Task: Patch Management

Authentication Template:  
Windows Admin [Edit](#)

Patch Management Template  
Critical Patches [Edit](#)

[OK](#) [Cancel](#)

Click the OK button and then on the Add/Edit Job window click the Run Job button to perform the patch management job.

You can automate the critical patching of systems by creating and scheduling a job that runs the Patch Management Template.

Click Manage Job Templates, then click Create a new job template.

Give your job a template name. Use a name that tells you what that job is doing and when it runs.

Click on Configure Schedule, create a new template, and set to recurring, but do not check the Intelligently remove option, as even if we successfully deploy patches to systems we wish to check for other patches every week on the systems. Set the start date and the time the job is to run, and set which days to run the job.

The image displays four screenshots of a software configuration wizard for scheduling a job. The first screenshot, titled "How should this job be scheduled?", shows three radio button options: "Select A Schedule:", "Run Immediately", and "Create A New Template...". The "Create A New Template..." option is selected. Below these, there are checkboxes for "Recurring" (selected), "One-Time", "Intelligently remove systems from affected systems list after all tasks have completed successfully", and "Enforce Blackout Calendar" (checked). The second screenshot, titled "Choose a start date.", shows a date picker set to 20/11/2012 and a time dropdown set to 19:00. It includes buttons to "Add additional start times" and "Remove last start time". The third screenshot, titled "How often should this job run?", shows "Every Week" selected under frequency, and "Tuesday" selected under "This job should run on...". The fourth screenshot, titled "Schedule Summary...", provides a summary of the configuration: Frequency: Every Day, Intelligent Removal Once Completed Successfully: Disabled, Enforce Blackout Calendar, Start Date: Tuesday, November 20, 2012, Run Time: 19:00, and Days: Tuesday.

**How should this job be scheduled?**

☐ Select A Schedule:  
☐ Run Immediately  
☒ Create A New Template...

---

☒ Recurring  
☐ One-Time  
☐ Intelligently remove systems from affected systems list after all tasks have completed successfully  
☒ Enforce Blackout Calendar

Next Cancel

**Choose a start date.**

Start Date: 20 11 2012  
Start Time: 19:00  
+ Add additional start times. - Remove last start time.

Previous Next Cancel

**How often should this job run?**

☒ Every Week  
☐ Every Month

**This job should run on...**

☐ All Days  
☐ Week Days  
☐ Sunday  
☐ Monday  
☒ Tuesday  
☐ Wednesday  
☐ Thursday  
☐ Friday  
☐ Saturday

Previous Next Cancel

**Schedule Summary...**

Frequency: Every Day  
Intelligent Removal Once Completed Successfully: Disabled  
Enforce Blackout Calendar  
Start Date: Tuesday, November 20, 2012  
Run Time: 19:00  
Days: Tuesday

Previous OK Cancel

Once you have finished configuring the schedule click Add task, choose Patch Management, and then choose the Authentication Template and Patch Management template you wish to use for this job.

Details

Add / Edit A Job...

Create a job that will run one or more times using templates that you have created.

Job Details

Job Name: Critical Patching Tuesday 7pm

☐ Create groups for failure codes

Schedule Summary...

Frequency: Every Day

Intelligent Removal Once Completed Successfully: Disabled

Enforce Blackout Calendar

Start Date: Thursday, March 07, 2013

Run Time: 19:00

Days: Tuesday

Configure Schedule

+ Add Filter

Task Name	Template Name				
Patch Management	Critical Patches	↑	↓	Edit	×

+ Add Task

+ Add Task Group

Save Job as New Template

Cancel

Then click Save Job as New Template to save the job.



In our example we named the job Critical Patching Tuesday 7pm so we know exactly what this job will do and when it's scheduled to run.

Now that we have the Critical Patch Job template set we can apply the job template to systems that have Clients and are managed by the System Area Manager.

Select the systems or group that you wish to apply the Critical Patch job to, right click and choose Schedule a job, then choose the job template you saved called Critical Patching Tuesday 7pm.

The screenshot shows a web-based interface for managing a network. At the top, a blue header bar contains the word "Details". Below it, the title "Test Automation Network" is displayed. To the right of the title are buttons for "Copy", "Move", and "Remove", along with a help icon "[?]". Below the title, a dropdown menu shows "Number of systems per page: 25".

The main area contains a table with the following columns: OU, IP (1st), MAC, Name, OS, Client, Type, Mgd, and Area M. The table lists several systems, including WINXPSP3, WIN7X64, and WIN7X86, all running Microsoft Windows 8 or 7.

A context menu is open over the table, showing options for applying the job to selected machines, the group, or the group and subgroups. Below these options is a list of actions: "Schedule a job...", "Client Deployment", "Set Location or Function", "Set Notification Settings", "Patch Management", "Set Power Schedule", "Set Remote Console Settings", "Shutdown", "Set Area Manager IP Address", "Set System Alert Matrix", "Deploy Third Party Software", "Issue Wake On LAN Command", and "Wait".

At the bottom of the context menu, there is a section for "Patch Scan Now" with options: "Refresh Selected Systems", "Add to Restricted Access List", "Add to Wake On LAN URL List...", "Active Directory Management", and "Copy Text to Clipboard".

At the bottom of the interface, there is a status bar showing "Items: 1 - 4 of 4" and a pagination control showing "Page 1 of 1".

You can modify the details of the job if needed. Click the Run Job button to schedule the Critical Patching job to the group called Test Automation Network.



Details

Add / Edit A Job...

Create a job that will run one or more times using templates that you have created.

Job Details

Job Name: Critical Patching Tuesday 7pm
☐ Save Job as Template (after running job)
☐ Remove devices from the following group upon successful completion: Test Automation Network
☐ Create groups for failure codes

Schedule Summary...

Frequency: Every Day  
Intelligent Removal Once Completed Successfully: Disabled  
Enforce Blackout Calendar  
Start Date: Thursday, March 07, 2013  
Run Time: 19:00  
Days: Tuesday

Configure Schedule

+ Add Filter

Task Name	Template Name				
Patch Management	Critical Patches	⬆	⬇	Edit	✖

+ Add Task

+ Add Task Group

Run Job

Cancel

Affected Systems

Test Automation Network

The scheduled job will now appear in the Daily section of Scheduled Jobs.

Scheduled Jobs

- ▶ Remaining Today
- ▼ Daily
  - ▶ Critical Patching Tuesday 7pm
  - ▶ Discovery (Lab)
  - ▶ Discovery (Office)
- ▶ Monthly
- ▶ In Progress
- ▶ Completed Today
- ▶ Suspended

You can apply the job template to multiple groups of systems.

## Windows Update Agent

The first time a patch scan or deployment is attempted on a client system, you may get an error to let you know that the operation failed because a current version of Windows Update Agent was not present on the client system. Windows Update Agent can be downloaded from Microsoft. There are separate versions for x86 (32-bit) and x64 (64-bit) systems:

WindowsUpdateAgent30-x86.exe: <http://go.microsoft.com/fwlink/?LinkID=100334>

WindowsUpdateAgent30-x64.exe: <http://go.microsoft.com/fwlink/?LinkID=100335>

The Third Party Software Installation feature of Management Utility can be used to install Windows Update Agent. Please refer to the chapter in this document entitled Third Party Application Deployment. For either version of Windows Update Agent 3.0, the command-line parameters for silent installation are:

`/quiet /norestart /wuforce`

You may also wish to refer to the SyAM Tool Tip “Installing Windows Update Agent”.

## Chapter 8 - Third Party Application Deployment

The Management Utilities enable you to deploy applications to target systems silently as a scheduled job or on demand.

Starting with Management Utilities V5.12 it is no longer required that target systems have System Clients installed and connected to a System Area Manager.

To deploy an application you must configure a Third Party Template.

Give the template a name, choose your target operating system, and then choose the authentication template that will be used to install the software on the target systems. Enter the path to where the application exe is stored; it will automatically point to the network share that you have set up in Administration Settings.

Enter the silent installation parameters specific for the application you are going to install, then press the Add button to confirm the settings. You can enter more information and add again if your application has multiple programs to run to complete the installation.

The screenshot shows the 'Configure Template' dialog box for a 'Third Party Deployment Template'. The title bar is blue with the text 'Configure Template'. Below it, the main title is 'Third Party Deployment Template' in bold. A subtitle reads: 'Define the paths to executables used to deploy third party software across your network.'

The 'Template Name' field contains 'Silverlight'.

The 'Third Party Executable Details' section includes:

- Target Platform:** Three radio buttons are present: 'Windows' (selected), 'Linux', and 'Mac OS X'.
- Authentication:** A dropdown menu shows 'Windows Admin'.
- Path to directory:** A text field contains '\\192.168.100.156\\apps'. Below it, a 'Find Files...' button is next to a field containing 'Silverlight.exe'.
- Resulting Path:** The text '\\192.168.100.156\\apps\\Silverlight.exe' is displayed.
- Timeout (minutes):** A text field contains '10'.
- Parameters:** A text field contains '/q'.
- Checkboxes:** A checkbox labeled 'Do not check for process completion (for BIOS updates)' is unchecked.
- Buttons:** An 'Add' button is at the bottom of this section.

Below the 'Add' button, there is a checkbox for 'Copy these files locally to each target machine before installing (required if the above is not a network share, cannot be used with local impersonation)'. It is unchecked.

A status bar at the bottom of the main area says 'No files have been added yet.'

At the very bottom are 'Save Changes' and 'Cancel' buttons.

On the right side, there is a vertical panel titled 'Existing Templates' with a large empty box. Below it is a 'New Template' section with 'Copy' and 'Remove' buttons.

Click the Save Changes button to save your template.

Add

☐ Copy these files locally to each target machine before installing (required if the above is not a network share, cannot be used with local impersonation)

File Path	Parameters	Timeout	Ignore Process Completion	Platform	
\\192.168.100.156\apps\Silverlight.exe	/q	10	No	Windows	<a href="#">Edit</a> <a href="#">Delete</a>

Save Changes

Cancel



In our example we are installing the Microsoft Silverlight executable using the /q silent installation parameter.

For environments where User Account Control is enabled on target machines, Third Party templates should use the normal domain admin authentication, and the Copy locally option must be checked. Then, when running the deployment job, choose the local admin authentication template. For further information please refer to the SyAM Tool Tip on Management Utilities Configuration for UAC Environments.

## Third Party Deployment Template

Define the paths to executables used to deploy third party software across your network.

Template Name:

## Third Party Executable Details

## Target Platform

- ☒ Windows  
☐ Linux  
☐ Mac OS X

Select the authentication template with credentials to browse the network share entered below

Path to directory containing source executable file (depsvc.exe MUST be present in this directory):

## Timeout (minutes)

## Parameters

☐ Do not check for process completion (for BIOS updates)

## Existing Templates

## New Template

☒ Copy these files locally to each target machine before installing (required if the above is not a network share, cannot be used with local impersonation)

## Silent Install Parameters for Third Party Application Deployment Templates

Application	Silent Parameters
Adobe Acrobat	Refer to SyAM Tool Tip "Deploying Acrobat or Reader with Adobe Customization Wizard"
Adobe Flash Player 11	-install
Adobe Reader 10	Refer to SyAM Tool Tip "Deploying Acrobat or Reader with Adobe Customization Wizard"
Apple Quicktime	Batch File cd \windows\system32 msiexec.exe /i \\192.168.200.113\apps\quicktime\Quicktime.msi /qbmsiexec.exe /i \\192.168.200.113\apps\quicktime\AppleApplicationSupport.msi /qbexit
Audacity	/SP- /VERYSILENT
Firefox	-ms
Java Runtime Environment	/s REBOOT=Suppress
Microsoft Internet Explorer 9	/quiet /norestart
Microsoft Silverlight	/q
Microsoft Office 2007 / 2010	/adminfile officeconfigfilename.msp Refer to SyAM Tool Tip "Deploying Microsoft Office 2007 or 2010"
Microsoft Windows Update Agent 3.0	/quiet /norestart /wuforce
OpenOffice.org 3.2 with default settings	-qn
OpenOffice.org 3.2 selected modules	Refer to SyAM Tool Tip "Deploying OpenOffice 3.2 using SyAM Management Utilities"



**Please check with the application vendor on the silent parameters specific to the version of the application that you are deploying as parameters may change by version.**

## Chapter 9 - Viewing Scheduled Job Status and History

### Scheduled Jobs

The status of the scheduled job can be viewed on the right hand pane called “Scheduled Jobs” in the Management Utility Interface.

This will provide a breakdown and status of the jobs that are scheduled to run, currently running or have completed.

By clicking on the heading you get a detailed view of that section, by clicking on the job you open up the job details.



**Remaining Today** – This is a list of recurring jobs that are scheduled to run later that day.

**Daily** – This is a list of recurring jobs that are scheduled to run each day or on a day each week.

**Monthly** – This is a list of recurring jobs that are scheduled to run once a month.

**In Progress** – This is a list of the jobs that are currently running.

**Completed Today** – This is a list of the jobs that have completed today.

**Suspended** – This is a list of the jobs that have been suspended. The job interface allows the job to be resumed.



## Job Status

At the bottom of your main window, you will see a **Job Status Panel**. This panel is used to inform you of the progress of jobs in progress and jobs recently finished. Only the last fifty jobs are displayed; older jobs can be queried from the **View History** page. To view the status and details of the job you click on the View Details section in the Status window of the job you wish to view.

**Status**

[View](#)  
[Details](#)

Discovery in Job "10/19/2010 8:33:45 AM". Job started on 10/19/2010 8:34:35 AM. The containing job finished running at 8:35:39 AM. 254 IPs scanned, 24 systems powered on.

This will then open up a window with the details specific to that job

**Task:** Discovery  
**Job Name:** 10/19/2010 8:33:45 AM  
**Date Started:** 10/19/2010 8:34:35 AM  
**Status:** The containing job finished running at 8:35:39 AM.

IP Address	Machine Name
192.168.200.1	
192.168.200.2	
192.168.200.3	
192.168.200.4	SITEMGR-BUILD
192.168.200.5	
192.168.200.6	
192.168.200.7	D915GUX
192.168.200.8	LINUX-BUILD-SER
192.168.200.9	BUILD-SERVER
192.168.200.10	SYAM-SERVER1
192.168.200.11	

OK

## View History – Audit Trail

The Audit Trail will provide a list of the actions that have been taken by your user and all users when the checkbox for Show Audit Information for All Users is chosen.

Details	
Audit Trail   Job Status	
<input type="checkbox"/> Show Audit Information For All Users	
Date	Audit Details
10/19/2010 10:04:14 AM	User "administrator" created a job.
10/19/2010 10:04:04 AM	User "administrator" created a discovery template.
10/19/2010 10:03:32 AM	User "administrator" created a job.
10/19/2010 9:55:27 AM	User "administrator" modified a power settings template.
10/19/2010 9:55:19 AM	User "administrator" created a power settings template.
10/19/2010 9:55:03 AM	User "administrator" created a location / function template.
10/19/2010 8:33:48 AM	User "administrator" created a job.
10/19/2010 8:33:42 AM	User "administrator" created a discovery template.
10/19/2010 8:32:47 AM	User "administrator" created a new user.
10/19/2010 8:32:24 AM	User "administrator" created a new user.
10/19/2010 8:18:04 AM	User "administrator" created an Area Manager IP template.
10/19/2010 8:17:44 AM	User "administrator" created an authentication template.

## View History – Job Status

The Status window shows the most recent 50 jobs that have run; to view jobs that are no longer shown in the Status window choose View History and Job Status. This will allow you to view all jobs that have been executed on the Management Utilities.

Click on the View Details to open up the window with the details of that job

Details	
Audit Trail   Job Status	
<a href="#">View Details</a>	Discovery in Job "Discover Lab Network". Job started on 10/19/2010 10:04:34 AM. The containing job finished running at 10:05:59 AM. 254 IPs scanned, 52 systems powered on.
<a href="#">View Details</a>	Discovery in Job "10/19/2010 8:33:45 AM". Job started on 10/19/2010 8:34:35 AM. The containing job finished running at 8:35:39 AM. 254 IPs scanned, 24 systems powered on.

The number of days to keep history data can be configured in Administration Settings, in the Functions menu.

## Chapter 10 – Power Auditor

With Power Auditor, IT administrators can identify cost savings to be achieved through power management. Power Auditor collects data on the actual number of hours that machines are left running. Savings are calculated based on the desired power on/off hours, with configurable settings for power consumption and cost. Power management templates can be created to enforce the desired policies, and achieved savings calculated.

Select Power Auditor from the drop down menu in the top right corner of the browser page. (Either Power Auditor or Management Utility can be loaded on startup by configuring the option on the My Settings page.)



### Discovery Template



Machines on the network can be discovered based on IP address ranges or Active Directory domains and Organizational Units.

Configure Template
Discovery Template

Template Name:
Office

Discovery Group Name
Office Network

☒ Allow systems with duplicate information

Domain Options

☐ Scan my domain (you must be logged into the domain)

Discover Domains
Discover Organizational Units

Domain:
Organizational Units:

☐ Replicate OUs

Network Scan

☒ Scan IP address range

Starting IP address:
192.168.200.1

Ending IP address:
192.168.200.254

☒ Resolve IP address to host name

Other Options

☐ Only discover systems that meet the following filter:

Exclude systems that meet the following filters:
Add

Remove

Save Changes

Cancel

Existing Templates

Automation Network 2K  
G4 Macs  
Office  
Replicate OUs

New Template

Copy

Remove

When using Active Directory, clicking the Discover Domains button will populate the Domain drop-down menu. Then, for a selected domain, clicking the Discover Organizational Units button will populate the OU drop-down. This information is retrieved from your domain controller. The server running Power Auditor must be logged into the domain.

For Active Directory you can also choose a domain, then check Replicate OUs to create subgroups based on the domain's Organizational Units.

Discovery Templates are shared by Power Auditor and Management Utility, and can be created through either one. In Power Auditor, a machine will appear in only one group, so that machines will not be double-counted for cost savings calculations.

## Power On Hours Template

Functions

Administration Settings

Configure Templates

Discovery

**Power On Hours**

Power Audit Wizard

My Settings

Reports

View History

The Power On Hours Template specifies the hours that a group of machines should be powered on. Use the default template or create your own. The easiest way may be to copy the default template and then make any desired changes.

Details

**Power On Hours Template**

Define the hours that machines in your environment are typically powered on.

Template Name:

	Power On Time	Power Off Time
<b>Sunday</b>	00:00	00:00
0 Power On Hours		
<b>Monday</b>	08:00	17:00
9 Power On Hours		
<b>Tuesday</b>	08:00	17:00
9 Power On Hours		
<b>Wednesday</b>	08:00	17:00
9 Power On Hours		
<b>Thursday</b>	08:00	17:00
9 Power On Hours		
<b>Friday</b>	08:00	17:00
9 Power On Hours		
<b>Saturday</b>	00:00	00:00
0 Power On Hours		

Existing Templates

8AM On, 5PM Off

New Template

CopyRemove

Copy Into Power Template

Idle Desktop Wattage	80
Idle Server Wattage	120
Idle Notebook Wattage	26
Idle Tablet Wattage	0
Idle Monitor Wattage	25

Save Changes

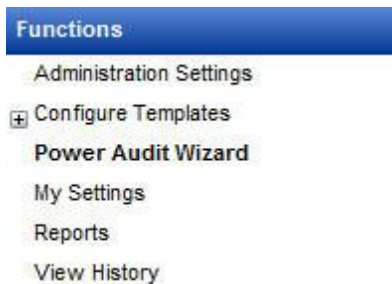
Cancel

The topmost drop down menus for Power On Time and Power Off Time will change the settings for all days of the week.

The Copy Into Power Template button creates a Power Management Template with the same name and settings in Management Utility. The Power Management Template can then be used to enforce power settings on managed systems.

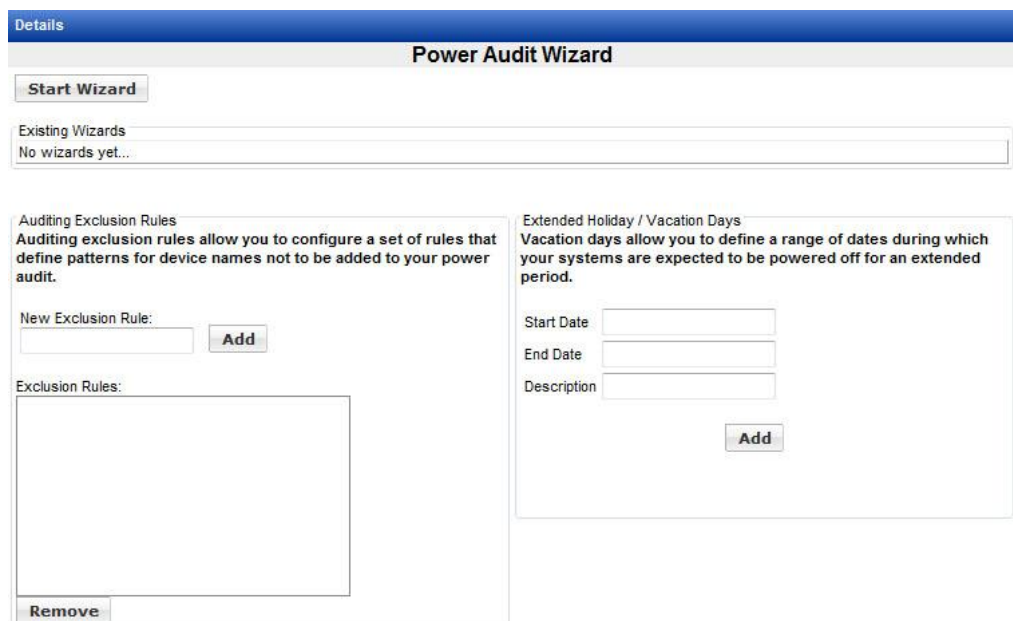
Power consumption calculations are based on wattage settings in this template. Defaults are supplied, to be changed as desired.

## Power Audit Wizard



A vertical navigation menu with a blue header bar labeled "Functions". Below the header, the following items are listed: "Administration Settings", "Configure Templates" (with a plus icon), "Power Audit Wizard" (highlighted in bold), "My Settings", "Reports", and "View History".

The Power Audit Wizard lets you define a power audit based on a Discovery Template, a Power On Hours Template, and a schedule. You can edit existing templates, or create new ones, in the wizard. Jobs created using the Network Discovery Wizard in Management Utility will appear here in the Power Audit Wizard, and vice versa. The results of a wizard job (such as how systems are displayed in Groups) may be different for Power Auditor than for Management Utility, but using the wizard is the same through either interface. Whether an action is taken through Power Audit Wizard or through Network Discovery Wizard, the results are the same.



The screenshot shows the "Power Audit Wizard" configuration page. At the top is a blue "Details" header. Below it is a "Start Wizard" button. A section titled "Existing Wizards" shows "No wizards yet...". The main area is divided into two panels. The left panel, "Auditing Exclusion Rules", explains that these rules define patterns for device names not to be added to the power audit. It includes a "New Exclusion Rule:" section with a text input and an "Add" button, and an "Exclusion Rules:" section with a large empty box and a "Remove" button. The right panel, "Extended Holiday / Vacation Days", explains that these days allow defining a range of dates during which systems are expected to be powered off. It includes "Start Date", "End Date", and "Description" text inputs, and an "Add" button.



Auditing Exclusion Rules allow you to exclude systems from power auditing based on machine name or IP address. Wildcards are allowed (a question mark for a single character, an asterisk for an unspecified number of characters). Systems are added to the list when they are selected and then removed from an audit in Power Audit Groups. Removing a group or subgroup does not add the systems to the Exclusion Rules list. The list is also not affected by removing systems from Groups in Management Utility.

For holidays and vacation periods you can set a range of dates in Extended Holiday / Vacation Days. On any day specified here, a system that is powered off all day will not be included in savings calculations. A system that is powered on for any part of the day will be included.

Details

Power Audit Wizard

Start Wizard

Existing Wizards

Scan Type	Scan Range	Group Name	Power On Hours Template	Last Scanned	Next Scan					
IP	192.168.100.1 - 192.168.100.254	Lab Rack	8AM On, 5PM Off		6/19/2012 4:45:00 PM	Enabled	<a href="#">Suspend Now</a>	<a href="#">Update Now</a>	<a href="#">Edit</a>	<a href="#">Remove</a>

Auditing Exclusion Rules

Auditing exclusion rules allow you to configure a set of rules that define patterns for device names not to be added to your power audit.

New Exclusion Rule:

Add

Exclusion Rules:

192.168.300.\*  
SYSTEM-SRRTSG

Remove

Extended Holiday / Vacation Days

Vacation days allow you to define a range of dates during which your systems are expected to be powered off for an extended period.

Start Date

End Date

Description

Add

Start Date	End Date	Description	
10/24/2012	10/28/2012	Fall Vacation	<a href="#">Remove</a>

## Daylight Saving Time

Power Auditor calculations are made on the basis of full 24-hour days, with adjustments made wherever Daylight Saving is observed. In the fall, when the clocks move back one hour, the repeated hour is not tracked in the power auditor. In the spring, when the clocks move forward one hour, the omitted hour is filled in using the power on/off statuses of devices for the hour prior to the one missing.



## Groups Section

Once an audit has been created and machines in the group have been polled, the group name will appear in the Groups section. Click the group name to see all machines in the group. Identified savings will be calculated when the audit has been running during the entire preceding day, and updated automatically.

Groups

Summary

Lab

Office

Details

Identified Savings: Lab

10/18/2011 - 10/24/2011

Move

Remove

[?]

Number of systems per page: 25

OU	IP (1st)	Name	Total Hours On	Hours To Be Saved	kWh To Be Saved	Amount To Be Saved	MAC
	192.168.100.9		0.0	0.0	0.00	0.00	00-15-17-27-24-21
	192.168.100.10	D915GVBW	0.0	0.0	0.00	0.00	00-11-11-56-33-DA
	192.168.100.11	SE7501CW2	0.0	0.0	0.00	0.00	00-02-B3-E9-62-30
	192.168.100.12	ZD865GBF	0.0	0.0	0.00	0.00	00-30-05-6F-36-6D
	192.168.100.14	NAS1000R	0.0	0.0	0.00	0.00	00-0E-0C-4E-41-2A
	192.168.100.22	NH1	0.0	0.0	0.00	0.00	00-16-76-56-6E-33
	192.168.100.24	WIN-Y4YMLDCE78P	0.0	0.0	0.00	0.00	00-13-20-8D-43-26
	192.168.100.26	DQ965WC-1	0.0	0.0	0.00	0.00	00-16-76-8F-9D-7A
	192.168.100.39	DQIZERUM	0.0	0.0	0.00	0.00	00-13-20-6F-01-E3
	192.168.100.52	H8DM8	0.0	0.0	0.00	0.00	00-30-46-7C-1B-34
	192.168.100.60	X8DT3	0.0	0.0	0.00	0.00	00-30-48-F4-24-1A
	192.168.100.92	2K03-SQL2005	0.0	0.0	0.00	0.00	00-0C-29-52-3C-9D
	192.168.100.99	DQ43AP	0.0	0.0	0.00	0.00	00-1C-C0-DF-5A-9A
	192.168.100.133		0.0	0.0	0.00	0.00	00-E0-81-62-14-39
	192.168.100.134	AUTOTESTER	0.0	0.0	0.00	0.00	00-0C-29-77-0F-88
	192.168.100.150	DG31PR-W7E-X86	0.0	0.0	0.00	0.00	00-1C-C0-D4-F7-43
	192.168.100.151	DB43LD-2K08-X84	0.0	0.0	0.00	0.00	00-1C-C0-B6-1D-84
	192.168.100.152	B1-P4SBA-XP	0.0	0.0	0.00	0.00	00-E0-4C-D0-4A-B6
	192.168.100.153	MS-7351-W7U-X84	0.0	0.0	0.00	0.00	00-13-46-8D-2E-EE
	192.168.100.154	G4-OSX411-PPC.local	0.0	0.0	0.00	0.00	00-30-65-C1-E9-5A
	192.168.100.155	G4-OSX39-PPC	0.0	0.0	0.00	0.00	00-30-65-68-0C-C8
	192.168.100.158	X3466-2K03-X84	0.0	0.0	0.00	0.00	00-11-11-E2-AD-A6

Functions

Administration Settings

Configure Templates

Power Audit Wizard

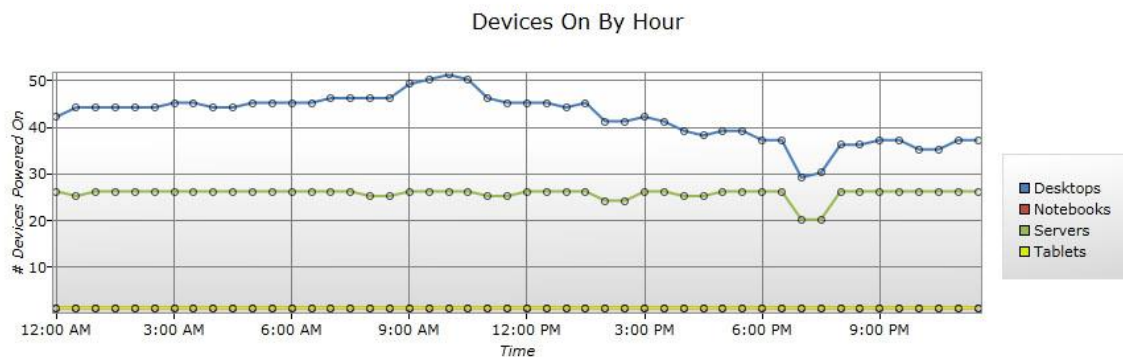
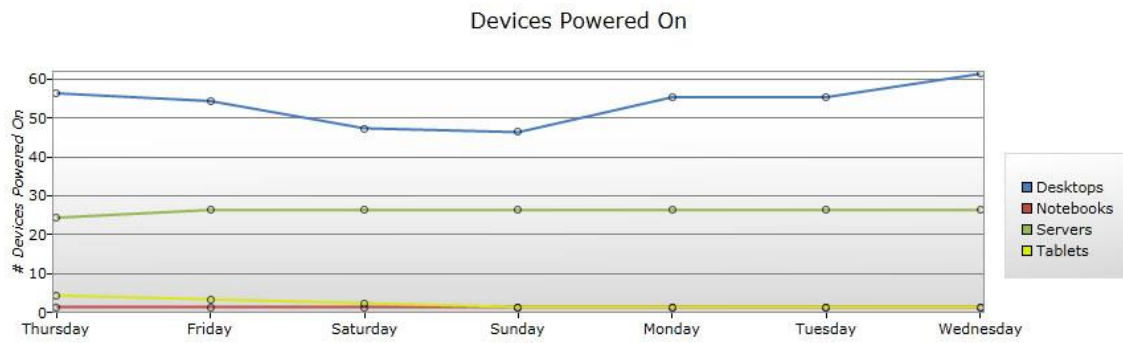
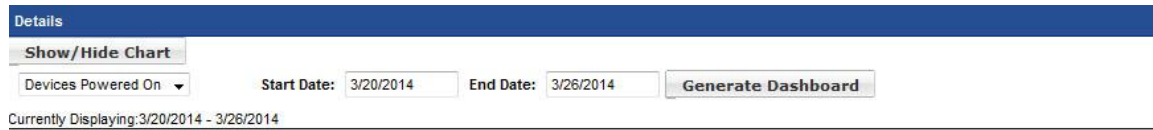
My Settings

Reports

View History

## Power Charts

The Devices Powered On chart shows the number of desktops, notebooks, and servers that are powered on for each day over a range of days, or by hour over the course of a single day.



The kWh Used chart shows the number of kilowatt-hours used per day (for a range of days) or per hour (for a 1-day chart).

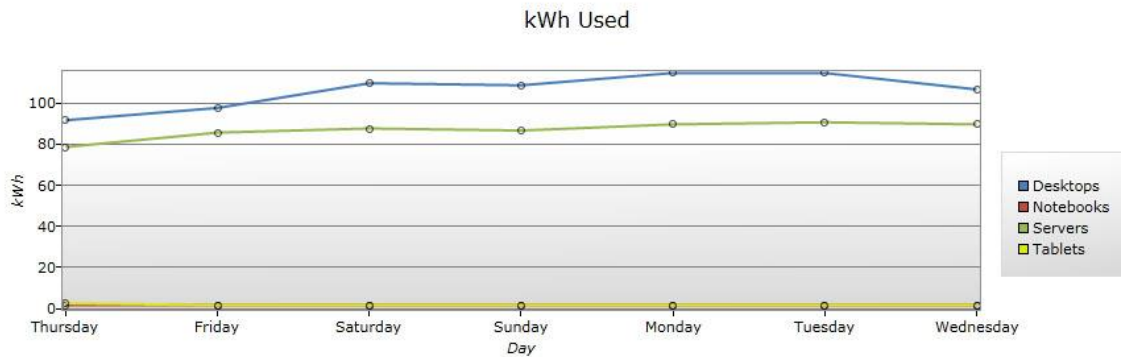
Details

Show/Hide Chart

kWh Used

Start Date: 3/20/2014 End Date: 3/26/2014 Generate Dashboard

Currently Displaying: 3/20/2014 - 3/26/2014



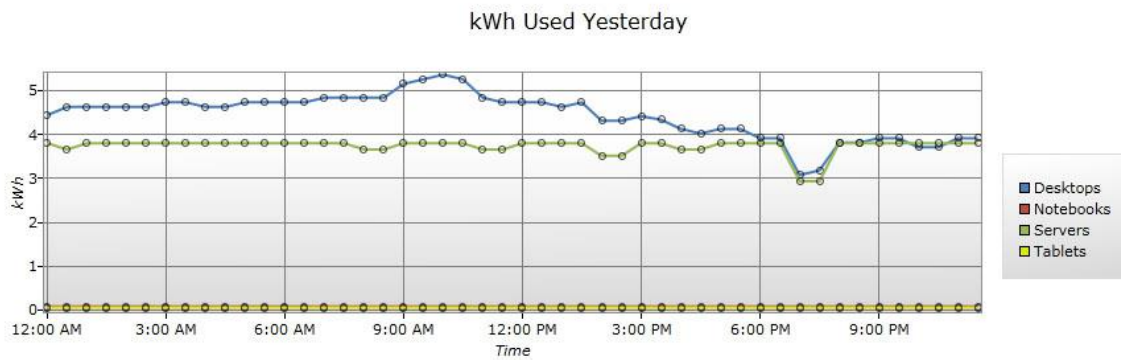
Details

Show/Hide Chart

kWh Used

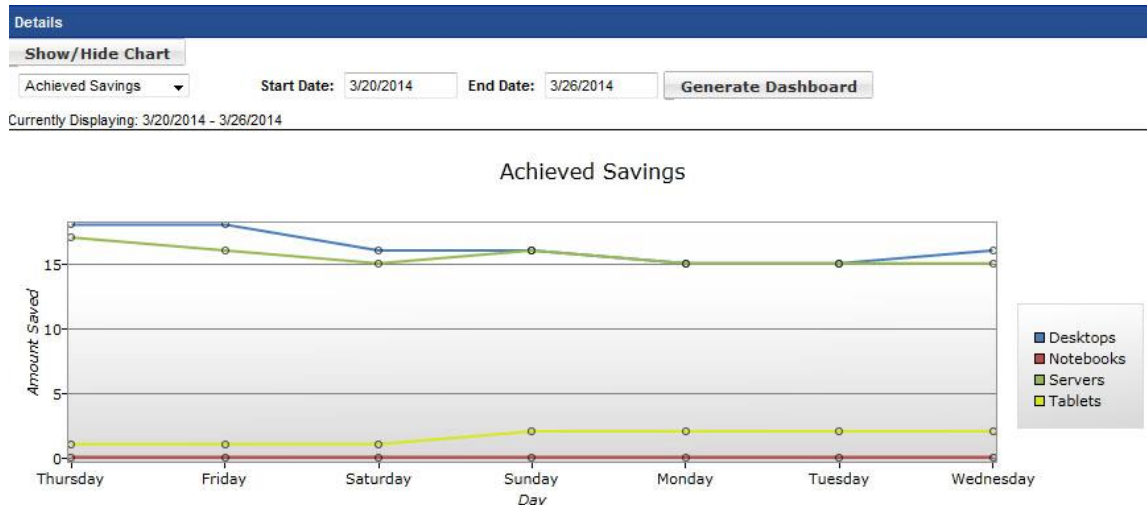
Start Date: 3/26/2014 End Date: 3/26/2014 Generate Dashboard

Currently Displaying: 3/26/2014 - 3/26/2014



Select the chart type, start date and end date, then click the Generate Dashboard button. You can choose whether to display charts by clicking the Show/Hide Chart button. There is a default setting for displaying charts on the My Settings page.

The Achieved Savings chart appears in the menu when Power Auditor is in Achieved Savings mode. This chart shows the amount saved, by system type, for the specified range of days.



## Reports

### Functions

Administration Settings

⊕ Configure Templates

Power Audit Wizard

My Settings

Reports

View History

Power Auditor can produce HTML or PDF reports on demand. PDF reports are stored in an archive, named either by Report Type or by the text entered in the Save Report As field. Page size for PDF reports can also be set; choose the default size on the Report Settings tab of Administration Settings. Available report types include Identified Savings (potential cost savings based on audit data) and Achieved Savings (actual savings from enforcing power settings with Management Utility power templates). Both summary and detail reports can be generated for these report types.

When Power Auditor is in Identified Savings mode, these reports are available:

- Identified Savings Summary Report
- Identified Savings Detail Report
- Devices Powered Off Detail Report
- List machines with agent but no power template
- List machines without agent installed
- Devices Not Powered On

When Power Auditor is in Achieved Savings mode, the following additional reports are available:

- Achieved Savings Summary Report
- Achieved Savings Detail Report

- Executive Report

Achieved Savings Summary Reports and Achieved Savings Detail Reports can be exported to comma-separated values (CSV) files which can be opened by a spreadsheet application. The CSV option can be selected when the report is created; there is also a button in the HTML report that will perform the export to CSV. The CSV reports are stored in the archive in the same way as PDF reports.

Details

OnDemand Reports

Report Type: Identified Savings Summary Report

Start Date: 1 Mar 2013

End Date: 7 Mar 2013

Report Format: ☐ HTML ☒ PDF ☐ CSV

Page Size: \_11X17

Save Report As...

Generate Report

Archive

Report Name • Start Date • End Date • Date Created ↑ Format • Size •

all all all all all all

Achieved Savings Summary Mar 01, 2013 Mar 07, 2013 Mar 08, 2013 .csv 0 KB

Achieved Savings Summary Report Feb 22, 2013 Feb 28, 2013 Mar 08, 2013 .pdf 55 KB

Executive Report Feb 01, 2013 Feb 28, 2013 Mar 08, 2013 .pdf 51 KB

Executive Report Jan 01, 2013 Jan 31, 2013 Mar 08, 2013 .pdf 51 KB

Total: 4

Print Close

#### Identified Savings Summary Report

3/1/2013 - 3/7/2013

Name	Device Count	Active Count	Contributing Count	Average Device Wattage	Average Monitor Wattage	Total Hours On	Hours To Be Saved	kWh To Be Saved	Amount To Be Saved
Development	15	15	13	80.00	25.00	1458.0	944.0	87.82	12.85
Marketing	10	13	13	80.00	25.00	1358.0	830.0	88.15	12.57
Sales	15	15	11	80.00	25.00	1022.0	238.0	24.99	4.78
Totals:	40	43	37	80.00	25.00	3838.0	1912.0	156.76	30.17

Powered By  
SyAM Software

Detail reports include information on individual machines in the group(s) reported on. For detail reports, check All Groups to produce a report for all groups, or check one or more individual groups. You may also choose to filter results. Click the Apply Filter radio button to configure filtering options.

## Details

### OnDemand Reports

Report Type: Identified Savings Detail Report

Start Date: 1 Mar 2013

End Date: 7 Mar 2013

Choose Group

☐ All Groups

☒ Development ☐ Marketing ☐ Sales

☐ Report on all systems. ☒ Apply filter.

Location Nashua, NH

☐ Contains

Sort by Machine Name

Report Format: ☐ HTML ☒ PDF ☐ CSV

Page Size \_11X17

Save Report As...

**Generate Report**

### Archive

Report Name	Start Date	End Date	Date Created	Format	Size
<span>all</span>	<span>all</span>	<span>all</span>	<span>all</span>	<span>all</span>	<span>all</span>
<input checked="" type="checkbox"/> Achieved Savings Summary	Mar 01, 2013	Mar 07, 2013	Mar 08, 2013	.csv	0 KB
<input checked="" type="checkbox"/> Achieved Savings Summary Report	Feb 22, 2013	Feb 28, 2013	Mar 08, 2013	.pdf	55 KB
<input checked="" type="checkbox"/> Executive Report	Feb 01, 2013	Feb 28, 2013	Mar 08, 2013	.pdf	51 KB
<input checked="" type="checkbox"/> Executive Report	Jan 01, 2013	Jan 31, 2013	Mar 08, 2013	.pdf	51 KB
<input checked="" type="checkbox"/> Identified Savings Summary Report	Mar 01, 2013	Mar 07, 2013	Mar 08, 2013	.pdf	10 KB

Total: 5

[Print](#) [Close](#) [Create Utility Group](#)

### Identified Savings Detail Report

Development

Location = Nashua, NH

3/1/2013 - 3/7/2013

Group Name	OU	IP	Name	Total Hours On	Hours To Be Saved	kWh To Be Saved	Amount To Be Saved	Type	Client	Location	Function	Power Template Set	Power On Hours Template	Device Idle Wattage	Monitor Idle Wattage
Development	142.221.51.1	Device 1	70.0	14.0	1.47	0.28	0.00	Desktop	V4.45.990-8L5162-3420-2347 (C)	Nashua, NH	Development	Set	East Coast Development	80.00	25.00
Development	142.221.51.2	Device 2	42.0	0.0	0.00	0.00	0.00	Desktop	V4.45.990-8L5162-3420-2347 (C)	Nashua, NH	Development	Set	East Coast Development	80.00	25.00
Development	142.221.51.3	Device 3	70.0	14.0	1.47	0.28	0.00	Desktop	V4.45.990-8L5162-3420-2347 (C)	Nashua, NH	Development	Set	East Coast Development	80.00	25.00
Development	142.221.51.4	Device 4	42.0	0.0	0.00	0.00	0.00	Desktop	V4.45.990-8L5162-3420-2347 (C)	Nashua, NH	Development	Set	East Coast Development	80.00	25.00
Development	142.221.51.5	Device 5	106.0	112.0	11.76	2.23	0.00	Desktop	V4.45.990-8L5162-3420-2347 (C)	Nashua, NH	Development	Not Set	East Coast Development	80.00	25.00
Development	142.221.51.1	Device B1	112.0	56.0	5.88	1.12	0.00	Desktop	V4.45.990-8L5162-3420-2347 (C)	Nashua, NH	Development	Set	East Coast Development	80.00	25.00
Development	142.221.51.1	Device B10	112.0	56.0	5.88	1.12	0.00	Desktop	V4.45.990-8L5162-3420-2347 (C)	Nashua, NH	Development	Set	East Coast Development	80.00	25.00
Development	142.221.51.2	Device B11	70.0	14.0	1.47	0.28	0.00	Desktop	V4.45.990-8L5162-3420-2347 (C)	Nashua, NH	Development	Set	East Coast Development	80.00	25.00
Development	142.221.51.3	Device B10	70.0	14.0	1.47	0.28	0.00	Desktop	V4.45.990-8L5162-3420-2347 (C)	Nashua, NH	Development	Set	East Coast Development	80.00	25.00
Development	142.221.51.4	Device B19	112.0	56.0	5.88	1.12	0.00	Desktop	V4.45.990-8L5162-3420-2347 (C)	Nashua, NH	Development	Set	East Coast Development	80.00	25.00
Development	142.221.51.2	Device B2	70.0	14.0	1.47	0.28	0.00	Desktop	V4.45.990-8L5162-3420-2347 (C)	Nashua, NH	Development	Set	East Coast Development	80.00	25.00
Development	142.221.51.5	Device B20	106.0	112.0	11.76	2.23	0.00	Desktop	V4.45.990-8L5162-3420-2347 (C)	Nashua, NH	Development	Not Set	East Coast Development	80.00	25.00
Development	142.221.51.3	Device B3	70.0	14.0	1.47	0.28	0.00	Desktop	V4.45.990-8L5162-3420-2347 (C)	Nashua, NH	Development	Set	East Coast Development	80.00	25.00
Development	142.221.51.4	Device B4	112.0	56.0	5.88	1.12	0.00	Desktop	V4.45.990-8L5162-3420-2347 (C)	Nashua, NH	Development	Set	East Coast Development	80.00	25.00
Development	142.221.51.5	Device B5	106.0	112.0	11.76	2.23	0.00	Desktop	V4.45.990-8L5162-3420-2347 (C)	Nashua, NH	Development	Not Set	East Coast Development	80.00	25.00
Development	142.221.51.1	Device B5	1456.0	944.0	67.82	12.85	0.00	Desktop	V4.45.990-8L5162-3420-2347 (C)	Nashua, NH	Development	Not Set	East Coast Development	80.00	25.00
Totals:				1456.0	944.0	67.82	12.85							80.00	25.00

Powered By  
**SyAM Software**

Identified savings reports, both on-demand and email, contain the following information (per group and totals):

- Name: The name of the Power Audit group
- Device Count: Total number of systems in the group



- Active Count: The number of systems that reported powered on status at any time during the reporting period
- Contributing Count: The number of systems that contributed to identified savings, that is, they were powered on for more hours than specified by the Power On Hours template
- Average Device Wattage: System power consumption as specified in the Power On Hours template
- Average Monitor Wattage: Display power consumption as specified in the Power On Hours template
- Total Hours On: Number of powered on hours for the entire group during the reporting period
- Hours To Be Saved: Number of powered on hours outside those specified by the Power On Hours template
- kWh To Be Saved: Total potential power saving for the group, based on wattages and hours calculated
- Amount To Be Saved: Total potential dollars saved for the group, based on kWh savings calculated and cost per kWh specified in Administration Settings

In Identified Savings mode, actual powered on hours are compared to the desired hours as defined in the Power On Hours Template. When we move into Achieved Savings mode, we are comparing the actual powered on hours with the baseline of data that was collected during the Identified Savings period. So there are some differences in achieved savings reports:

- Contributing Count: The number of systems that contributed to achieved savings, that is, they were powered on fewer hours than the baseline average
- Hours Saved: Number of powered on hours saved through power management, compared with the baseline data
- kWh Saved: Actual power saving for the group, based on wattages and hours calculated
- Amount Saved: Actual dollars saved for the group, based on kWh savings calculated and cost per kWh specified in Administration Settings
- Amount Saved by Group (pie chart)
- Amount Saved by Day (bar chart)
- kWh Saved by Day (bar chart)
- Active Systems by Day (bar chart)
- Carbon Savings summary



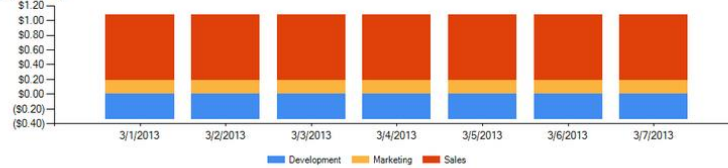
## Achieved Savings Summary Report

3/1/2013 - 3/7/2013

### Amount Saved by Group



### Amount Saved by Day



### kWh Saved by Day



### Active Systems by Day



### Carbon Savings

From 3/1/2013 to 3/7/2013, you have saved 27.09 kilowatt hours which is equivalent to 0.0 metric tons of CO2 emissions. This is the equivalent of removing 0.0 car(s) from the road. An average passenger vehicle travels 11,720 miles per year with a fuel economy of 20.4 miles per gallon. Source: <http://www.epa.gov/cleanenergy/>

Name	Device Count	Active Count	Contributing Count	Average Device Wattage	Average Monitor Wattage	Total Hours On	Hours Saved	kWh Saved	Amount Saved
Development	15	15	8	80.00	25.00	1458.0	-121.0	-12.71	-2.41
Marketing	10	13	10	80.00	25.00	1358.0	66.0	6.93	1.32
Sales	15	15	13	80.00	25.00	1022.0	313.0	32.88	6.24
Totals:	40	43	31	80.00	25.00	3838.0	258.0	27.08	5.15

Powered By  
**SyAM Software**

Other available reports include the Devices Powered Off Detail Report. This report summarizes by group the number of active devices (devices that have been powered on) and the number of devices powered off for each day in the date range. A detailed breakout of each day follows the summary, listing the active devices and whether or not they were shut down before midnight. The Devices Not Powered On report lists all devices, by group, that have not been powered on between the start date and the end date. If a device is powered on at any time during this period, it will not be listed on the report.

Reports can also be produced that list machines that do not have the agent installed, or machines where the agent has been installed but no power template has been set.

Print Close Create Utility Group

List machines without agent installed  
2/22/2011 - 2/28/2011

Group Name	IP	Name	Hours To Be Saved
Factory	192.168.100.66		19.0
Factory	192.168.100.14	NAS1000R	90.0
Factory	192.168.100.63	WIN-E2LRET2VHKA	54.0
Main Office	192.168.200.1		122.0
Main Office	192.168.200.4	SITEMGR-BUILD	0.0
Northwest Branch	192.168.100.111	D945GTP-VMWARE1	90.0
Warehouse	192.168.100.134	AUTOTESTER	90.0
Warehouse	192.168.100.191	G31MX	35.0
Warehouse	192.168.100.252	GATEWAY-7450R	90.0

For these two report types, and for all the detail reports, clicking the Create Utility Group button will copy the listed machines into a Management Utility group identified by the date and time of creation. The groups can then be used for deploying the agent and the desired power settings.

Print Close Create Utility Group

Group Created: 3/1/2011 11:17:42 AM

Details										
3/1/2011 11:17:42 AM										
Number of systems per page: 200						Copy	Move	Remove	?	
OU	IP (1st)	MAC	Name	OS	Client	Type	Mgd	Area Man...	Power	Power Template Set
	192.168.100.14	00-0E-0C-4E-41-2A	NAS1000R			Unknown	No		On	Not Set
	192.168.100.63	00-0C-29-0A-0F-37	WIN-E2LRET2VHKA			Unknown	No		On	Not Set
	192.168.100.66	00-0C-29-E1-46-70				Unknown	No		Off	Not Set
	192.168.100.111	00-60-08-17-5E-4F	D945GTP-VMWARE1			Unknown	No		On	Not Set
	192.168.100.134	00-0C-29-77-0F-88	AUTOTESTER			Unknown	No		On	Not Set
	192.168.100.191	00-22-68-60-69-ED	G31MX			Unknown	No		On	Not Set
	192.168.100.252	00-C0-9F-04-49-02	GATEWAY-7450R			Unknown	No		On	Not Set
	192.168.200.1					Unknown	No		On	Not Set
	192.168.200.4		SITEMGR-BUILD			Unknown	No		Off	Not Set

The Executive Report becomes available in Achieved Savings mode. Like the Achieved Savings summary and detail reports, it does not appear in the menu while you are still in Identified Savings mode. The Executive Report summarizes achieved savings results for the selected month and year, displaying savings by group, the trend in amount of money saved, how achieved savings compares with projected savings, and a summary of carbon savings for the month. It can be produced in HTML or PDF format.

## Executive Report Achieved Savings January 2013

This executive report visualizes the results of the energy efficiency measures implemented on your computer network using SyAM Software. The Achieved Savings of the computer network, is calculated by using the difference between actual energy usage and the estimated energy consumption that would have occurred during the same period had the efficiency measures not been implemented (the baseline).

### Achieved Savings Summary

The following information summarizes the achieved savings data for January 2013 in both kilowatt hours and amount saved. It also provides a breakdown of the types and quantities of systems being audited.

KWh Saved:	119.97	Total # of managed devices:	46
Cost Per KWh:	\$0.19	Notebooks:	0
January 2013 Savings:	\$22.79	Desktops:	46
		Servers:	0
		Unknown:	0

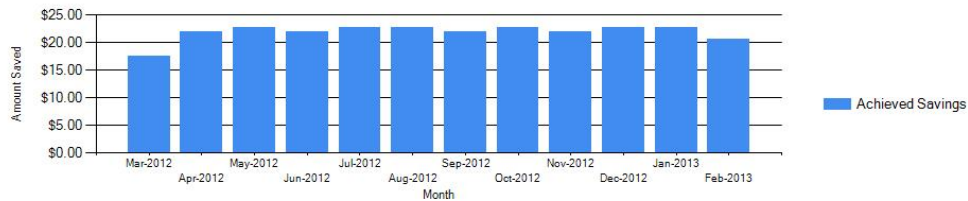
### Achieved Savings by Group

The following chart shows the percentage of each group's contribution to total savings for January 2013.



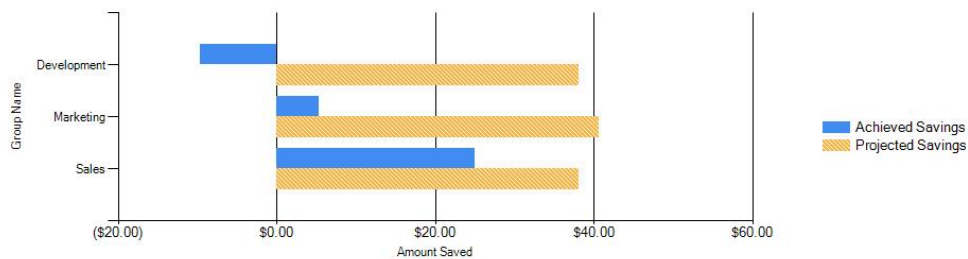
### Achieved Savings Trend

The following chart shows the amount of money saved by month over the last year or the start of achieved savings mode.



### Achieved Savings vs Projected Savings Goal

The following chart shows each group's projected savings vs actual savings.



### Carbon Savings

From 2/1/2012 to 1/31/2013, you have saved 3487.86 kilowatt hours which is equivalent to 2.4 metric tons of CO2 emissions. This is the equivalent of removing 0.5 car(s) from the road.

An average passenger vehicle travels 11,720 miles per year with a fuel economy of 20.4 miles per gallon. Source: <http://www.epa.gov/cleanenergy/>

Powered By  
**SyAM Software**

## At A Glance

This section, located on the right side of the Power Auditor browser window, displays a high-level summary of the available information. Use the Details window to drill down to specifics of groups and individual systems.

At A Glance...
<b>Achieved Savings</b> 11/5/2012 - 11/11/2012
<b>Average Wattage / System</b> Desktops: 105.00 Servers: 145.00 Notebooks: 26.00 Tablets: 0.00
<b>Average Hours On / Day</b> Desktops: 10.66 Servers: 13.25 Notebooks: 0.71 Tablets: 0.00
<b>Total # Addresses</b> Desktops: 61 Servers: 37 Notebooks: 2 Tablets: 0
<b>Total # Active Systems</b> Desktops: 53 Servers: 29 Notebooks: 1 Tablets: 0

## Administration Settings

Functions
<b>Administration Settings</b>
<input checked="" type="checkbox"/> Configure Templates
Power Audit Wizard
My Settings
Reports
View History

On the Settings page of Administration Settings, you can view the software's version information. The power cost used for Power Auditor's calculations, and the frequency with which machines are polled for data, can be changed from the default settings on this page. The currency unit can also be selected from a drop down menu.

The Remove Blank Systems button will remove any systems from your power audit that have no device name, installed System Client, or reported power on hours. Removing these systems from your power audit is important for accurate savings calculations.

Automatically Reorganize Power Audit Groups By Location will remove all existing power audit groups, creating new groups containing the same systems, categorized by location. Machines

that have the System Client installed and managed by System Area Manager, but do not have a location defined, are placed in the Ungrouped group. Systems that are not connected to System Area Manager are placed in the Unmanaged group.

Your PAL (Power Audit License) allows you to audit a specified number of systems for a specified period of time. Enter the PAL and click the Upload PAL button. License information (number of systems and starting/ending dates) will be displayed.

**Details**

SettingsUsersEmail SettingsReport SettingsAchieved Savings

**Build Information**  
**Application Vendor:** SyAM Software  
**Installed Version:** V5.14  
**Build Number:** 970  
**Build Date:** 20140327  
**Database Version:** 163

**Power Auditor Settings**  

**Currency Symbol**  
\$

**Cost Per KW/h**  
0.19

**Polling Frequency (Hours)**  
☒ 30 Minutes  
☐ 1 Hour

**Remove Blank Systems**

☐ Automatically Reorganize Power Audit Groups By Location

**Licensing Information**  
A PAL is a license that allows you to audit a number of systems for a given amount time. Please contact your administrator to obtain a copy of your PAL.

**Insert New PAL**  

**Upload PAL**

Installed Date	Quantity	Start Date	End Date
3/27/2014 12:22:09 PM	9000	3/1/2014 12:00:00 AM	4/30/2014 12:00:00 AM

**Save Changes****Cancel**

The Users tab is the same as for Management Utility. See the appropriate section of the manual for further information.

On the Email Settings tab, you can enter information about authenticating to your email server, so that Power Auditor can email an identified savings report. Send a test email to make sure the configuration is correct. This is also the place where the list of email recipients is maintained.

Details
Settings
Users
Email Settings
Report Settings
Achieved Savings

Username
audit@company.com

Password

Server
mail.company.com

Sender Email
88@company.com

Use SSL
☐

Port
25

Email an identified savings report:
☒ Daily
☒ Weekly
☒ Monthly

Report Recipient Email:
Add

richardw@company.com
Remove

Save Changes
Clear Settings
Send Test Email

Once you have moved into Achieved Savings mode, you can also select achieved savings reports to be emailed, including the Executive Report.

Details
Settings
Users
Email Settings
Report Settings
Achieved Savings

Username
audit@syamsoftware.com

Password
•••••

Server
mail.syamsoftware.com

Sender Email
autoEmailFromV5@syamsoftw

Use SSL
☐

Port
25

Email an identified savings report:
☐ Daily
☐ Weekly
☐ Monthly

Email an achieved savings report:
☐ Weekly
☐ Monthly

Email an executive report:
☐ Monthly

Report Recipient Email:
Add

cory.nickerson@syamsoftware.com
Remove

Save Changes
Clear Settings
Send Test Email

If you are using Gmail, specify the full email address as the username and smtp.gmail.com as the server. Check the box to use SSL and specify port 587.



On the Reports tab you can enter header text to be displayed on all reports. To make a logo appear on your reports, browse to a graphics file in a format that browsers can display. Also on this page is the default page size setting for PDF reports, which you can override when creating individual reports.

Here is an example of a report with header and logo.

**SyAM Power Auditor**  
Identified Savings Summary Report  
7/6/2012 - 7/12/2012

**SyAM Software**

Name	Device Count	Active Count	Contributing Count	Average Device Wattage	Average Monitor Wattage	Total Hours On	Hours To Be Saved	kWh To Be Saved	Amount To Be Saved
Development	5	5	3	80.00	25.00	392.0	140.0	14.70	2.79
Marketing	7	6	6	80.00	25.00	714.0	378.0	39.69	7.54
Sales	5	5	3	80.00	25.00	294.0	42.0	4.41	0.84
<b>Totals:</b>	<b>17</b>	<b>16</b>	<b>12</b>	<b>80.00</b>	<b>25.00</b>	<b>1400.0</b>	<b>560.0</b>	<b>58.80</b>	<b>11.17</b>

Once you have moved into Achieved Savings mode, weekly and monthly achieved savings reports will become available.

The Achieved Savings tab allows you to compare powered on hours before and after implementing your power policy. After seven days of auditing, sufficient data has been collected to establish a baseline, and at that time Achieved Savings mode is enabled.

When moving into Achieved Savings mode you will need to enter the IP address or hostname of the system(s) which are running the System Area Manager software. This will retrieve the number of licenses purchased and will allow the number of systems up to the license count to continue being monitored. Systems over the license count will not have their power audit data collected.



## Details

Settings Users Email Settings Report Settings **Achieved Savings**

Achieved Savings mode allows you to compare actual powered on and off times for devices in your network. A baseline set of data is captured and used to compare per-device usage before and after implementing a power schedule.

Once the Power Auditor has collected 7 days worth of data, you may move into Achieved Savings mode. This will allow you to compare how many hours devices were powered on before and after implementing your energy saving solution.

**Warning:** You should **NOT** implement power schedules while in identified savings. Identified savings mode is used to collect an average baseline of number of hours on for devices in your network before beginning your savings plan. Implementing power schedules while in identified savings mode will greatly reduce your achieved savings!

Your per-system baseline averages would be the following if you were to move into achieved savings today:

Device Type	Power Template	Average Hours On Per Week
Unknown	8AM On, 5PM Off	135
Unknown	Library	101
Desktop	8AM On, 5PM Off	110
Desktop	Library	130
Server	8AM On, 5PM Off	132
Server	Library	137
Server	Servers 24/7	161
Notebook	8AM On, 5PM Off	0
Notebook	Library	26
Desktop	Servers 24/7	45
Notebook	Servers 24/7	26

Area Manager IP Address

Add

Area Manager IP Address	License Count	
192.168.200.113	110	<button>Remove</button>
192.168.200.10	130	<button>Remove</button>
HP-Vpro	0	<button>Remove</button>
192.168.200.81	5	<button>Remove</button>

The button below will become active once you have reviewed an identified savings report for the last seven days.

It is strongly recommended that you closely examine the table above and the contents of the report to verify that your audit represents the usage in an average week for your environment.

[Run Report Now](#)

Go To Achieved Savings Mode