

Table of Contents

Getting Started	1
Client Server Architecture	2
System Requirements	3
Licensing and Registration	4
Tutorials	5
Console	2
Object Explorer	6
Groups	7
Enabling and Disabling Objects	10
Options	11
Service	2
Service Connections	12
Server Manager Properties	13
Changing the Service Logon As Credentials	14
Viewing the Service Log File	15
Running the Service in Verbose Mode	16
Configuring Active Directory Connections	17
Configuring Email Server Connections	18
Configuring Web Proxy Server Settings	19
Tray Icon	20
Computers, Devices and Hosts	21
Adding Computers, Devices and Hosts	21
Mapping Computers, Devices and Hosts	22
Importing a Host List	23
Importing a Disk List	24
Computer, Device and Host Properties	25
Browse Active Directory	26
Browse Network	27
Searching for Computers, Devices and Hosts	28
Selecting Multiple Computers, Devices and Hosts	29
Assigning Logon As Credentials	30
Batch Assign Logon As Credentials	31
Templates	32
Adding Templates	33
Selecting a Template Type	34
Template Properties	37
Selecting Multiple Templates	38
Reports	39
Adding Reports	40
Selecting a Report Type	41
Report Properties	42
Selecting Multiple Reports	43
Duplicate Files Reports	44
File and Directory Access Permissions Reports	45
File Extension Reports	46
Largest Files Reports	47
Least Accessed Files Reports	48
Recently Accessed Files Reports	49
Temporary Files Reports	50
Schedules	51

Configuring Day and Time Exclusions	53
Actions	54
Desktop Actions, Alerts and Notifications	56
Action Tags	57
HTML and Email Templates	58
File Output Options	59
Filters	60
Auto Configurators	61
Adding Auto Configurators	62
Auto Configurator Properties	63
Selecting Multiple Auto Configurators	64
Select Active Directory Organizational Unit	65
Signing Files	66
Creating a Filename Mask	67
Troubleshooting	68
Access Denied	68
Quota Violation	70
The RPC Server is Unavailable	71
Viewing the Service Log File	15
Running the Service in Verbose Mode	16
Terminology	72

Corner Bowl Server Manager Help

Corner Bowl Server Manager is an enterprise-wide systems and application monitoring software package enabling both small business and large enterprise System Administrators to proactively manage their networks and fulfill compliance requirements.

Consolidates, archives and monitors logs such as:

- Windows Event Logs
- Syslogs
- Text logs

Includes Security Event Log Reports such as:

- Failed Logon Attempts
- Successful Logons
- Account Management
- Account Lockout

Monitors resources such as:

- Disk space
- CPU load over time
- Memory load over time

Monitors and controls applications and services such as:

- Websites
- Email servers
- Databases
- Windows Services and Processes

Monitors Internet connectivity and throughput.

Includes extensive disk and directory monitoring and analysis functions and reports

How it Works? Server Manager...

- Installs to a single server then remotely manages computers, devices and hosts.
- Is configured through a client user interface which can be installed to any Windows computer at any location.
- Fires alerts and notifications through email, SMS, remote desktop popups, SNMP traps and more.
- Automatically publishes systems and network status to your web server for remote access via your iPhone or Android.
- Generates reports to HTML, text and CSV.

For more information see:

[Client/Server Architecture](#)

[Object Explorer](#)

[System Requirements](#)

Client Server Architecture

Server Manager is implemented using client/server architecture. The server, referred to as the Server Manager Service, runs as a Windows service and is responsible for all monitor and report execution. The client, referred to as the Server Manager Console, runs on any Windows supported platform and is responsible for all configuration and management. The tray icon, also a client, is responsible for desktop notifications (e.g. message box and sound alerts). You can install the console and tray icon on as many computers as necessary.

The client/server interface is implemented using TCP port 6766 by default. The TCP interface authenticates all incoming connections using Windows authentication. Access will only be granted if the user accessing the service belongs to the Administrator group. For secure environments the TCP interface can be configured to encrypt all packets using private keys.

To configure the TCP port and encryption options and settings see [Server Manager Properties](#).

To configure the console or tray icon to connect to a remote service installation see [Service Connections](#).

NOTE: Server Manager is deployed through a single installer that always installs the service, console and tray icon. If you only plan to use the console and/or tray icon, disable the Corner Bowl Server Manager service via the Windows Service Control Manager.

System Requirements

Supported Operating Systems

Windows Server 2008 R2, Server 2008, Server 2003, 7, Vista, or XP.

Supported CPUs (64-Bit / 32-Bit)

Server Manager is offered in both 64-bit and 32-bit Windows installers. Be sure to install the 64-bit installer when targeting 64-bit hardware as the 64-bit installer includes 64-bit binaries.

Memory

2 GBs of available memory, 4 GBs suggested for large networks.

Microsoft .NET Framework 3.5 Service Pack 1

The installation detects if the .Net Framework 3.5 Service Pack 1 is already installed. If not, the framework is automatically downloaded from Microsoft and then installed. Please note the framework may take a significant amount of time to install. Please be patient while the installation completes.

Domain Administrator Account

To access and manage remote resources Server Manager requires domain administrator rights. If off-domain, local administrator rights. The first time the application is run, you will be prompted to assign administrator credentials to the service.

Windows Management Instrumentation (client and server)

Many functions within Server Manager utilize Microsoft's Windows Management Instrumentation (WMI) API (e.g. Event Log management, CPU, memory, services, processes, Access Permissions Reports, SMART). If unavailable, the dependent functions will not be available.

Optional Components

Microsoft's SNMP Service

SNMP traps are exposed through Microsoft's SNMP Service.

Licensing and Registration

Server Manager is licensed by the number of addressable hosts. An addressable host is defined as an IP address or other application layer access identifier (e.g. SQL Server database instance names).

Licensing is further broken into 3 template categories:

- Disk Monitoring
- Log Management
- Network Application Monitoring

At any time these categories may be expanded or customized per user requirements. A single license key may be purchased for each category or set of categories per user requirements.

The management user interface, Server Manager Console, and the notification tray icon are free to install on as many computers as necessary.

A simple licensing sample

If monitoring a single physical server called cornerbowl that hosts a web server (www.cornerbowl.com) and mail server (mail.cornerbowl.com) 3 host licenses will be required. One for each addressable name:

- cornerbowl
- www.cornerbowl.com
- mail.cornerbowl.com

You, however, can apply as many templates (e.g. CPU, memory, disk space, web content, etc.) to each host as necessary.

Registering your license

Upon purchasing a license from Corner Bowl Software you will receive a license key or set of keys via email.

From the Edit menu item select Server Manager Properties.

Once the Server Manager Properties page loads select the Licensing tab then click Register License.

Specify the email address used when purchasing the license and the license key then click *Submit*.

NOTE: If the installation is at a secure location please email the target MAC address along with the license key you wish to assign to sales@cornerbowl.com.

Resetting your license

If you need to move a license to another computer, you can reset your own license for registration on the new system.

From the Edit menu item select Server Manager Properties.

Once the *Server Manager Properties* page loads select the *Licensing* tab.

From the *Installed Licenses* pane select the license to return then click *Return License*.

NOTE: If the installation is at a secure location please email the target MAC address along with the license key you wish to assign to sales@cornerbowl.com.

Tutorials

Under construction

Object Explorer

The *Object Explorer* is the central navigation view that contains all of Server Manager’s configurable objects. Use the *Object Explorer* to create objects, assign objects, update objects, view object detail and delete objects.

These objects include:

Tree Nodes	Description
Root	Each configured Server Manager connection is added to the root.
Computers, Devices and Hosts	Contains all of the managed hosts and their monitors. This includes physical computers, hardware devices and network addressable applications (e.g. web sites and SQL Server instances).
Monitors	From within the Computers, Devices and Hosts tree node when viewing a host, assigned Templates appear under each host. Assigned Templates are referred to as Monitors. Monitors are a representation of a host-template assignment or the result of a host group or template group-template assignment.
Templates	Contains monitor definitions.
Reports	Contains informational type monitors (e.g. daily summary email reports and largest files reports).
Schedules	Contains the frequency to execute monitors, reports and Auto Configurators.
Actions	Contains the actions, alerts and notifications,
Auto Configurators	Contains the Auto Configurators.
Filters	Contains Active Directory and log monitoring filters.

For more information see:

[Groups](#)

Groups

The need for groups

Systems management is made easier through grouping. Grouping provides you with the ability to group similar or related objects into smaller more manageable collections while also offering inheritance (e.g. when assigning a host to a host group, all templates assigned to the host group as applied to the host). Server Manager supports hierarchical grouping as well as multi-assignment.

A simple real-world sample

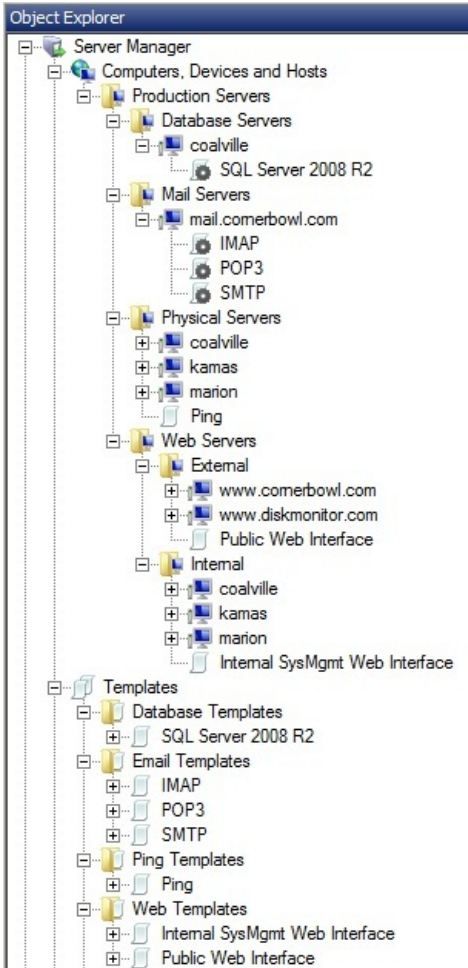
Here is a simple grouping example. Let's say we have 3 servers (coalville, kamas, and marion) of which all provide internal HTTP interfaces on port 8080. A SQL Server database is hosted on coalville, kamas provides public HTTP interfaces for www.cornerbowl.com and www.diskmonitor.com and marion provides SMTP, IMAP and POP3 interfaces for mail.cornerbowl.com.

In this example the goal is to ping all physical machines and monitor all HTTP, database and email interfaces. To implement these monitoring requirements:

- Create 4 groups: Database Servers, Mail Servers, Physical Servers and Web Servers. Within the Web Server group I created 2 sub-groups named External and Internal.
- Add coalville to the Database Servers group.
- Add mail.cornerbowl.com to the Mail Servers group.
- Add coalville, kamas and marion to the Physical Servers group.
- Add www.cornerbowl.com and www.diskmonitor.com to the Web Servers -> External group.
- Add coalville, kamas and marion to the Web Servers -> Internal group.
- Create the database, email, ping, external HTTP and internal HTTP templates.
- Assign the database template to coalville.
- Assign the email templates to mail.cornerbowl.com.
- Assign the ping template to the Physical Servers group.
- Assign the public HTTP templates to the External group.
- Assign the internal HTTP templates to the Internal group.

NOTE: Assign generic templates (e.g. ping) to groups and host specific templates (e.g. templates that contain logon as information) directly to the appropriate host.

When you have completed adding and assigning the objects the *Object Explorer* should look something like the screenshot below:



How to group

To create a group

From the *Object Explorer*, navigate to the object collection node (e.g. 'Computers, Devices and Hosts', 'Templates' or any user defined groups), right click then select *New Group*.

From the *New Group* dialog type the group name then click *OK*.

To add objects to groups

From the *Object Explorer* use drag and drop.

To move an object, drag using the left mouse button.

To link an object, drag using the right mouse button. When dropped you are prompted with 3 choices:

Move	Unassigns the object from the current object moves it to the target object.
Link	Links the object to the target object creating a membership to multiple objects.
Cancel	Cancels the drag and drop operation.

To assign templates to Hosts, Host Groups and Template Groups

From the *Object Explorer* navigate to the target template then right click and select *Properties*.

From the *Template Properties* page use the *Template Assignments* combo-boxes to select the groups you would like to assign the template.

To assign Summary Reports to Hosts, Host Groups and Template Groups

From the *Object Explorer* navigate to the target report then right click and select *Properties*.

From the *Report Properties* page use the *Report Assignments* combo-boxes to select the groups you

would like to assign the template.

To batch move or assign multiple hosts to another group

From the *Edit* menu item select *Batch -> Assign Hosts to Group*.

From the Select Multiple Computers, Devices and Hosts dialog select the target hosts.

From the Assign Multiple Computers, Devices and Hosts to Group dialog choose to:

- move or link hosts,
- the target group type: Host Group or Template Group,
- the target group

Once you have selected the options click *Assign*.

Enabling and Disabling Objects

When using Server Manager you will likely find times you need to disable a monitor or report. For example, if you would like to shutdown all monitoring on a particular server while you apply operating system patches you can disable the host for a pre-determined period of time such as the next 30 minutes. Server Manager enables you to temporarily or permanently disable hosts, templates, reports and Auto Configurators.

To disable an object

From the *Object Explorer* navigate to the target object (e.g. host group, host or template) then right click and select *Disable*.

Once the *Enable/Disable Properties* dialog loads use the controls to either temporarily or permanently disable or re-enable the select object.

To batch enable or /disable multiple objects

From the *Edit* menu item select *Batch -> Update...*

Once the *Select Multiple Objects* dialog loads check the target objects then click *OK*.

Once the object specific properties dialog opens use the controls within the dialog to batch enable or disable the target objects.

For more information, see:

[Configuring Day and Time Exclusions](#)

[Schedules](#)

Options

The Options Dialog enables you to set user preferences for the Server Manager Console (e.g. automatically displaying the dashboard at startup).

To view the Options Dialog

From the *Tools* menu item select *Options*.

The following options are available:

- Display the *Dashboard* when a new connection is established
- Display the *Service Output* when a new connection is established
- Proxy WMI calls through the Server Manager Service
- Disable the tray icon

Note: If you would like to set Service options such as:

- Email server settings
- Backend database connections
- Directory services
- Automatically publishing system status to your web server
- HTML templates

Please see [Server Manager Properties](#).

Service Connections

Server Manager is implemented using [client/server architecture](#).

To add a new service connection

From the *File* menu item select *New Service Connection*.

Specify a connection name, the network addressable hostname or IP address and the TCP port.

Specify the Windows username, password and domain. If the service is installed on an off-domain computer or within a workgroup either clear the domain field or within the domain field specify the computer name the service is installed.

Choose to encrypt packets. If you enable encryption, specify the private key.

NOTE: If you would like to encrypt packets you must first enable encryption within the [Server Manager Properties](#) page.

Server Manager Properties

The Server Manager Properties view enables you to configure the Server Manager Service (e.g. configure email server settings and backend database connections).

To view the Server Manager Properties View

From the Edit menu item select Server Manager Properties.

The following tab pages are available:

- Dashboard
- Error Report
- Email
- Databases
- Active Directory
- Web Server
- HTML Templates
- TCP Server Settings
- Licensing

Please see each tab page for detailed help.

NOTE: If you would like to set Console options such as:

- Display the *Dashboard* when a new connection is established
- Display the *Service Output* when a new connection is established
- Proxy WMI calls through the Server Manager Service
- Disable the tray icon

Please see [Options](#).

Changing the Service Logon As Credentials

The Server Manager Service executes all configured functionality using the account the service is logged on as. In order for the service to access network resources (e.g. CPU load, disk space, sending email through Exchange Server or connecting to SQL Server databases that require Windows Authentication) it must run with either domain or local administrator credentials.

To change the service logon as credentials

From the computer the service is installed open the console.

From the *Service* menu item select *Change Service Logon*.

Specify a domain administrator username, password and domain. If the computer the service is installed is not a member of a domain specify a local administrator account. Click the *Next* button.

The service will be restarted using the specified credentials. If the service fails to start because of a logon failure, check the credentials and try again.

For more information, see:

[Access Denied](#)

Viewing the Service Log File

The Server Manager Service logs errors, triggers, general activity and [verbose output](#) to a text log file called cbsmsrv.log. To verify activity or trouble-shoot the system you can view the log file from within the console or manually with any text editor.

To tail the service log file

From the *View* menu item select *Service Output*.

To review the entire log file

From the *Service* menu item select *View Service Log*.

To manually open the log file using notepad

From the computer the service is installed open Notepad then select File -> Open.

Navigate to then open the following file:

Server 2008/7/Vista	C:\programdata\cornerbowl\server manager\cbsmsrv.log
Server 2003/XP	C:\documents and settings\all users\application data\cornerbowl\server manager\cbsmsrv.log

For more information see

[Running the Service in Verbose Mode](#)

Running the Service in Verbose Mode

The Server Manager Service logs errors, triggers and general activity to a text log file called cbsmsrv.log. If you are not receiving the results you expect and have already reviewed the service log file you may be able to gain insight by temporarily running the service in verbose mode. When run in verbose mode, the service logs additional debug messages enabling you to identify executing functions (e.g. executing monitors and schedule updates).

To run the service in verbose mode

From the computer the service is installed open the console.

From the *Service* menu item select *Stop* then *Start Verbose*.

NOTE: If the computer the Server Manager Service is installed on is rebooted the service will restart normally.

For more information see

[Viewing the Service Log File](#)

Configuring Active Directory Connections

Active Directory connections are used by the *Browse Active Directory* dialog and more importantly Auto Configurators. Auto Configurators enable you to scan OUs for computers. Once discovered, computers are filtered, added then templates and reports assigned.

By default Server Manager discovers your Active Directory server; however, if the computer Server Manager is running is off-domain or you would like to connect to multiple Active Directory Servers you must configure the connections..

To configure Active Directory connections

From the *Edit* menu item select *Server Manager Properties* , Once the properties view loads, select the *Active Directory* tab. Use this tab to add or modify existing connections.

NOTE: When scanning multiple domains, create a connection for each domain's OU and specify the appropriate domain administrator credentials. When the Auto Configurator runs the specified credentials are assigned to all newly added computers.

For more information see:

[Auto Configurators](#)

[Browse Active Directory](#)

Configuring Email Server Connections

In order to email alerts, notifications and reports you must configure the connection to the email server you would like to send email through.

To configure email server connections

From the *Edit* menu item select *Server Manager Properties* then select the *Email* tab.

Specify the settings then click the *Test* button.

To use a backup email server when the primary email server is down

From the *Edit* menu item select *Server Manager Properties* then select the *Email* tab.

Check the Use a backup email server... option then click Configure Backup.

Specify the settings then click the *Test* button.

NOTE: When sending email through Microsoft Exchange Server if no username is specified email is sent from the account the Server Manager Service is logged on as.

Configuring Web Proxy Server Settings

For security purposes, many organizations require all HTTP/S packets to pass through a web proxy server. If your organization implements a web proxy server you can configure Server Manager to forward all HTTP requests to the proxy server.

You can configure the web proxy server settings when registering your license or creating an HTTP monitor.

To configure when registering your license

From the *Edit* menu item select *Server Manager Properties* then select the *Licensing* tab.

Click *Register License*

Once the *Register License Key* dialog loads, click *Configure Web Proxy*.

Once the *Web Proxy Server Properties* dialog loads see instructions below.

To configure when creating a new HTTP monitor

Select *File -> New Template*.

Once the *Select Template Type* dialog loads, select an *HTTP* template type.

Once the *Enter URL* dialog loads, type the URL to monitor.

Once the *Template Properties* dialog loads, select the *Monitor* tab then click *Configure Web Proxy*.

Once the *Web Proxy Server Properties* dialog loads see instructions below.

Using the Web Proxy Server Properties dialog

Check the option to proxy web server requests.

Specify proxy server's hostname or IP address and port.

If the proxy server requires you to authenticate, check the *Authenticate* check box and type the appropriate credentials.





If you are unsure about any of the settings, contact your systems administrator.

Tray Icon

The Server Manager Tray Icon is client application that enables your Windows desktop to display system status, receive [desktop notifications](#) (e.g. message box alerts, sound alerts and optionally interactive file execution) and launch the Server Manager Console.

The tray icon can be installed on any Windows computer then configured to connect to the Server Manager Service (multiple if necessary). Once connected, your desktop is ready to display the system status, message box alerts and play sound alerts.

The tray icon displays the following system status icons:

	The tray icon has connected to the service and there are no triggers.
	The tray icon has connected to the service and there is at least one warning trigger.
	The tray icon has connected to the service and there is at least one critical trigger.
	There is at least one network related error.

To configure your workstation, laptop or home computer to receive desktop notifications

See [Desktop Actions, Alerts and Notifications](#)

To open Server Manager from the tray

Double-click the tray icon or right click and select *Open Corner Bowl Server Manager Console* .

NOTE: If the tray icon is displaying a trigger or error icon, the console will open the last triggered monitor.

To clear the tray icon alert icon

From the tray icon, right click and select *Clear Tray Alert* .

To view the message box alert history

From the tray icon, right click and select *View Message Box Alert History* .

To temporarily close the tray icon

From the *Tools* menu item select *Close Tray Icon* or from the tray icon right click and select *Exit*.

NOTE: Desktop actions will no longer fire.

To restart the tray icon

From the *Tools* menu item select *Start Tray Icon*.

To permanently disable or re-enable the tray icon

From the *Tools* menu item select *Options*.

From the *User Preferences* tab check the option to disable or un-check to re-enable.

For more information see:

[Client/Server Architecture](#)

[Desktop Actions, Alerts and Notifications](#)

Adding Computers, Devices and Hosts

Computers, devices (e.g. switches and routers) and hosts (e.g. www.cornerbowl.com, mail.cornerbowl.com) can be added to Server Manager in several ways.

- Browsing your Windows network
- Browsing your Active Directory tree
- Typing the identifier
- [Importing](#) a list of computers, devices and hosts from a text or CSV file.

To browse your Windows network, Active Directory tree or type the hostname

From the *Object Explorer* select the target [host group](#). If a target group is not selected, new hosts are added to the root.

From the *File* menu item select *New Computer, Device or Host* .

Once the *Add Computers, Devices and Hosts* dialog loads choose a method to select multiple hosts or type the identifier (e.g. 10.1.0.100 or mail.cornerbowl.com) then click Add.

Available Methods	Description
Browse Network	Browse your Windows network. This method is similar to viewing your network within Windows Explorer.
Browse Active Directory	When logged onto a domain, this method enables you to scan and search your Active Directory tree.
Map a Computer, Device or Host	Provides a means to add a computer that requires logon as credentials or cannot be discovered within the Windows network.
Select Localhost	Select the local computer.

For more information, see:

[Browse Active Directory](#)

[Browse Network](#)

[Groups](#)

[Importing a Host List](#)

[Mapping Computers, Devices and Hosts](#)

[Searching for Computers, Devices and Hosts](#)

[Selecting Multiple Computers, Devices and Hosts](#)

Mapping Computers, Devices and Hosts

When managing Windows servers or workstations in multi-domain or non-domain environments DNS may not be able to resolve some computers names. This scenario typically results in a 'The RPC server is Unavailable' or 'The network path was not found' error.

Another error commonly seen, 'Access Denied', occurs when the account the service is running under or the account the user is logged in as does not have the required access permissions to execute WMI functions or discover administrator disk shares (e.g. c\$, d\$ and e\$).

Finally, some server names are complex or un-informative (e.g. SRV0001UT). Mapping hosts enables you to create your own alias for either a hostname or IP address. In the example above, SRV0001UT, you could assign an alias such as 'Prod Utah Database Server'. Once assigned, all displays of SRV0001UT within the *Object Explorer* and properties pages are replaced with the alias.

To map a host

From the *File* menu item select *New -> Computer, Device or Host* .

From the combo box select *Map Computer, Device or Host* .

Once the *Map Computer, Device or Host* dialog loads specify the addressable hostname or IP address, Windows username, password and domain that enables you to access the remote computer. If accessing an off-domain server or workstation either clear the domain combo-box or specify the remote computer name.

For more information see

[Adding Computers, Devices and Hosts](#)

[Access Denied](#)

[Batch Assign Logon As Credentials](#)

[The RPC Server is Unavailable](#)

Importing a Host List

If you have a list of computers, devices and/or hosts in a spreadsheet, CSV (comma separated values) or text file you can import your list into Server Manager. When imported you have the option of assigning logon as credentials, host groups, template groups, templates, report groups and reports.

NOTE: If you have a list of disks or shares you would like to import see [Importing a Disk List](#).

To import a host list

From the *File* menu item select *Import -> Host List*

Follow the instructions found within the wizard.

For more information see:

[Adding Computers, Devices and Hosts](#)

Importing a Disk List

If you have a list of disks or shares in a spreadsheet, CSV (comma separated values) or text file you can import your list into Server Manager. When imported disk monitor templates are created and assigned to each computer. You have the option of creating a single template per computer or a template for each disk or share listed in your file.

NOTE: If you have a list of computers, devices and/or hosts you would like to import see [Importing a Host List](#).

To import a disk list

From the *File* menu item select *Import -> Disk List*

Follow the instructions found within the wizard.

Computer, Device and Host Properties

The *Computer, Device and Host* properties dialog enables you to assign logon as credentials, enable or disable monitors, configure WMI quotas and configure SNMP connectivity.

To view or edit a host's properties

From the *Object Explorer* select the target host or [host group](#) then right click and select *Properties*.

Or

From the *Edit* menu item select *Batch -> Update Computers, Devices and Hosts*. Once the *Select Multiple Computers, Devices and Hosts* dialog loads check the target hosts then click *OK*.

Once the *Computer, Device and Host Properties* dialog loads, select the target tab.

Tab	Description
Logon As	Use this page to assign logon as credentials or provide a hostname or IP address alias.
Enable/Disable	Use this page to enable or disable the host.
WMI	Use this page to increase the WMI quota settings.
SNMP	Use this page to configure Simple Network Management Protocol (SNMP) connectivity.

For more information see:

[Groups](#)

[Selecting Multiple Computers, Devices and Hosts](#)

Browse Active Directory

The *Browse Active Directory* dialog enables you to navigate and search through your Active Directory tree to select computers.

To display the Browse Active Directory dialog

From the *Object Explorer* select the target [host group](#). If a target group is not selected, new hosts are added to the root.

From the *File* menu item select *New Computer, Device or Host* .

Once the *Add Computers, Devices and Hosts* dialog loads from within the combo box select *Browse Active Directory*.

To search your AD Tree for specific computers

From the *Browse Active Directory* dialog click [Search](#).

For more information see:

[Adding Computers, Devices and Hosts](#)

[Configure Active Directory Connections](#)

[Groups](#)

[Searching for Computers, Devices and Hosts](#)

Browse Network

The *Browse Network* dialog enables you to you to navigate and search through your network to select computers.

To display the Browse Network dialog

From the *Object Explorer* select the target [host group](#). If a target group is not selected, new hosts are added to the root.

From the *File* menu item select *New Computer, Device or Host* .

Once the *Add Computers, Devices and Hosts* dialog loads from within the combo box select *Browse Network*.

To search your network for specific computers

From the *Browse Network* dialog click [Search](#).

For more information see:

[Adding Computers, Devices and Hosts](#)

[Groups](#)

[Searching for Computers, Devices and Hosts](#)

Searching for Computers, Devices and Hosts

The *Search for Computers, Devices and Hosts* dialog enables you to search your network or Active Directory tree for computer selection.

To display the *Search for Computers, Devices and Hosts* dialog

From the *File* menu item select *New Computer, Device or Host* . Once the *Add Computers, Devices and Hosts* dialog loads choose *Browse Network* or *Browse Active Directory*.

Or

From the *Edit* menu item select *Batch -> Update/Delete Computers, Devices or Hosts* .

From one of the *Browse* dialogs click *Search*.

From the *Search for Computers...* dialogs specify your search criteria and optionally create and assign an Active Directory computer property filter. Once you have set your search criteria click *Search*. To select all results click *Select Computers* otherwise multi-select the computers of interest then click *Select Computers*.

What are Active Directory computer property filters?

Active Directory computer property filters enable you to search your AD tree and filter each discovered computer for specific criteria (e.g. only pass computers that have the word 'Server' embedded in the 'operatingSystem' property).

For more information see:

[Adding Computers, Devices and Hosts](#)

[Browse Active Directory](#)

[Browse Network](#)

Selecting Multiple Computers, Devices and Hosts

Server Manager provides you with the ability to quickly re-configure and delete multiple hosts at the same time (e.g. resetting logon as credentials, setting WMI quotas or assigning templates).

To update multiple hosts

From the *Edit* menu item select *Batch -> Update Computers, Devices and Hosts*.

Once the *Select Multiple Computers, Devices and Hosts* dialog loads see instructions below.

To assign a template, template group, report or report group to multiple hosts

From the *Object Explorer*, right click on the object to assign then select *Assign Computer, Device or Host*.

Once the *Select Multiple Computers, Devices and Hosts* dialog loads see instructions below.

To delete multiple hosts

From the *Edit* menu item select *Batch -> Delete Computers, Devices and Hosts*.

Once the *Select Multiple Computers, Devices and Hosts* dialog loads see instructions below.

Using the *Select Multiple Computers, Devices and Hosts* dialog

The *Select Multiple Computers...* dialog enables you to select from a list of configured hosts. The dialog includes search and add functions.

- To search then automatically check hosts, click [Search](#).
- To add a new host, click [Add](#).
- To select multiple hosts, check each host then click *OK*.
- To select a single host, double-click the host.

If updating hosts, the [Computer, Device and Host Properties](#) dialog will load.

For more information see:

[Adding Computers, Devices and Hosts](#)

[Searching for Computers, Devices and Hosts](#)

[Computer, Device and Host Properties](#)

Assigning Logon As Credentials

When managing Windows servers or workstations in multi-domain or non-domain environments users are often prompted with 'Access Denied' errors. An 'Access Denied' error occurs when the account the service is running under or the account the user is logged in as does not have the required access permissions to execute WMI functions (e.g. downloading Event Logs or monitoring CPU load) or discover administrator disk shares (e.g. c\$, d\$ and e\$).

To add a new computer and assign logon as credentials

From the *File* menu item select *New -> Computer, Device or Host*.

From the Choose a method to select hosts combo box select Map Computer, Device or Host.

Once the *Map Computer, Device or Host* dialog loads see the instructions below.

To update or add logon as credentials to an already existing computer

From the *Object Explorer*, navigate to the target computer, right click then select *Properties*.

Once the *Map Computer, Device or Host* dialog loads see the instructions below.

Using the Map Computer, Device or Host dialog

From the *Map Computer, Device or Host* dialog specify the addressable hostname or IP address, Windows username, password and domain that enables you to access the remote computer. If accessing an off-domain server or workstation either clear the domain combo-box or specify the remote computer name.

For more information see

[Access Denied](#)

[Batch Assign Logon As Credentials](#)

Batch Assign Logon As Credentials

When accessing multiple Windows servers on another domain you will likely need to periodically update the logon as credentials.

NOTE: It is only necessary to assign credentials when accessing computers on another domain or within a workgroup.

To batch update logon as credentials

From the Edit menu item select Batch -> Assign Logon As Credentials.

Once the *Select Multiple Computers, Devices and Hosts* dialog loads check the target computers or click [Search](#) to scan the tree for specific computer names or computers that match specific Active Directory computer properties (e.g. operatingSystem contains 'Server'). When you have finished selecting the target computers, click *OK*.

Once the *Computer, Device and Host Properties* dialog loads from the *Logon As* tab specify the logon as credentials. To set credentials for a single computer contained in the list select the target computer from the *Host* combo-box found at the top of the dialog then specify the logon as credentials.

For more information see

[The RPC Server is Unavailable](#)

[Access Denied](#)

[Batch Assign Logon As Credentials](#)

Templates

A template is defined as an assignable configuration object that defines properties for an executable function with the purpose of executing against each assigned host (e.g., a Ping template that defines the failure rate prior to triggering or an HTTP template that sends an email alert when any assigned website is down).

Templates can be assigned to hosts, host groups, template groups and summary reports.

Templates are [groupable](#).

In the example above, a single Ping or HTTP template is created then assigned to each host or group of hosts.

To create a new Template

From the *File* menu item select *New -> Template*.

To batch update existing Templates

From the *Edit* menu item select *Batch -> Update Templates*.

For more information, see:

[Adding Templates](#)

[Groups](#)

[Template Properties](#)

Adding Templates

To add a new template

From the *File* menu item select *New Template*.

Once the *Select a Template Type* dialog loads, select the target type.

NOTE: Unlicensed template types appear in gray text.

Once the [Template Properties](#) dialog loads, use the controls to configure the properties, assign target hosts, host groups and template groups.

For more information, see:

[Templates](#)

[Template Properties](#)

[Selecting a Template Type](#)

Selecting a Template Type

When adding a new template you are prompted to select a template type (e.g. Ping Monitor, CPU Monitor or Event Log Consolidation). Unlicensed template types appear in gray text. If you would like to create a template that is not currently licensed, please visit www.CornerBowl.com and upgrade your license.

The following template types are available:

Type	Description	Licensing
Event Log Backup	Backup, archive, compress, encrypt and sign Event Log files (.evt and .evtx files).	Log Manager
Event Log Consolidation	Download, consolidate, filter and alert on Windows Event Log entries.	Log Manager
Event Log Monitor	Real-Time monitor mission critical Event Logs for specific entries.	Log Manager
File Size Monitor	Monitor a file for maximum size.	Log Manager
Idle File Monitor	Monitor application text log files for inactivity.	Log Manager
Syslog Backup	Backup, archive, compress, encrypt and sign consolidated syslog entries.	Log Manager
Syslog Consolidation	Consolidate syslog messages.	Log Manager
Syslog Monitor	Monitor syslog messages for specific entries.	Log Manager
Text Log Backup	Backup, archive, compress, encrypt and sign text log files.	Log Manager
Text Log Consolidation	Consolidate application text log files.	Log Manager
Text Log Monitor	Monitor application text log files for specific entries.	Log Manager
Defragment Disks	Schedule the service to remote execute disk defragmentation.	Disk Monitor
Delete Temporary Files	Delete old temporary files.	Disk Monitor
Directory Cleaner	Delete old files.	Disk Monitor
Directory Size Monitor	Monitor a directory's size.	Disk Monitor
Directory Watcher	Monitor, log and trigger alerts when a directory or file is created, modified, renamed or deleted.	Disk Monitor
Disk Space Monitor	Monitor free disk space.	Disk Monitor
File Count Monitor	Monitor the number of files	Disk Monitor

	a directory contains.	
SMART Status Monitor	Monitor SMART Predictive Failure status.	Disk Monitor
Active Directory Monitor	Verify your Active Directory is up and running.	Internet Server Monitor
CPU Monitor	Monitor CPU load over time.	Internet Server Monitor
Create Process	Schedule a process or batch file to run.	Internet Server Monitor
DNS Monitor	Check the availability of a DNS server and the accuracy of a record.	Internet Server Monitor
Domain Expiration	Check a domain's expiration date.	Internet Server Monitor
FTP Monitor	Verify the availability of an FTP server.	Internet Server Monitor
HTTP/S Monitor	Verify a website is available and returning the expected content.	Internet Server Monitor
IMAP Monitor	Verify the availability of an IMAP email server.	Internet Server Monitor
Memory Monitor	Monitor memory load over time.	Internet Server Monitor
MySQL Monitor	Verify a MySQL database is available and able to execute a select statement.	Internet Server Monitor
ODBC Monitor	Verify an ODBC database is available and able to execute a select statement.	Internet Server Monitor
Oracle Monitor	Verify an Oracle database is available and able to execute a select statement.	Internet Server Monitor
Ping Monitor	Use ICMP to ping a remote host.	Internet Server Monitor
POP3 Monitor	Verify the availability of a POP3 email server.	Internet Server Monitor
Process Monitor	Monitor a process.	Internet Server Monitor
SMTP Monitor	Verify an SMTP email server is available and able to send email.	Internet Server Monitor
SNMP Get Monitor	Monitor SNMP variables.	Internet Server Monitor
SQL Server Monitor	Verify a SQL Server database is available and able to execute a select statement.	Internet Server Monitor
SSL Certificate Expiration	Check an SSL certificate's expiration date.	Internet Server Monitor

TCP Port Monitor	Verify a TCP port is accepting connections and optionally returning a packet.	Internet Server Monitor
Throughput Monitor	Uploads and downloads a file to an FTP server then calculates and saves the throughput information.	Internet Server Monitor
Windows Service Monitor	Verify a Windows Service is either running or stopped.	Internet Server Monitor

Once the *Template Properties* dialog loads, use the controls to configure the properties and assign target hosts, host groups and template groups.

For more information, see:

[Adding Templates](#)

Template Properties

The *Template Properties* page enables you view and modify templates and assignments.

To view or edit a Template

From the *Object Explorer* select the target template then right click and select *Properties*.

Or

From the *Edit* menu item select *Batch -> Update Templates*. Once the *Select Multiple Templates* dialog loads check the target templates then click *OK*.

Common Configuration Objects

Templates include the following common configuration objects:

Configuration Object	Description
Name	The friendly name of the object.
Description	A user description of the object.
Enabled	Enables scheduled and real-time execution.
Temporarily disabled	Temporarily disables scheduled and terminates real-time execution.
Retain History	The number of days to retain the monitor execution history. NOTE: Monitor data is not saved to the history database.
Automatically Open	If checked the console automatically opens all monitors when the console connects to the service. NOTE: The console will only open a maximum of 20 monitors.
Host Assignment	The assigned hosts.
Host Group Assignment	The assigned host groups. Assigns all hosts linked to the host group or child host group.
Template Group Assignment	The assigned template groups. Assigns all hosts linked to the template group or child template group.

For more information see:

[Templates](#)

[Groups](#)

[Selecting Multiple Templates](#)

Selecting Multiple Templates

Server Manager provides you with the ability to quickly re-configure and delete multiple templates at the same time (e.g. assign a different schedule or trigger action).

To update or delete multiple templates

From the *Edit* menu item select *Batch -> Update Templates*.

Once the *Select Multiple Templates* dialog loads see instructions below.

To assign a multiple templates to a host or host group

From the *Object Explorer*, right click on the target host or host group then select *Assign Template*.

Once the *Select Multiple Templates* dialog loads see instructions below.

Using the *Select Multiple Templates* dialog

The *Select Multiple Templates* dialog enables you to select from a list of configured templates. The dialog includes a template type filter, an *Add* button and a *Delete* button.

- To filter by template type, select the type from the *Filter* combo box
- To add a new template, select the target group then click [Add](#).
- To delete a template, check each template then click *Delete*.
- To select multiple templates, check each template then click *OK*.
- To select a single template, double-click the template.

If updating templates, the [Template Properties](#) dialog will load.

For more information see:

[Adding Templates](#)

[Template Properties](#)

Reports

A report is defined as a configuration object that defines properties for an executable function that optionally targets multiple hosts (e.g. a weekly Failed Logon report that returns failed logon attempts from 3 domain controllers or a Duplicate Files report that scans directories on 3 different servers).

To create a new Report

From the *File* menu item select *New -> Report*.

To batch update existing Reports

From the *Edit* menu item select *Batch -> Update Reports*.

For more information, see:

[Adding Reports](#)

[Groups](#)

[Report Properties](#)

Adding Reports

To add a new report

From the *File* menu item select *New Report*.

Once the *Select a Report Type* dialog loads, select the target type.

NOTE: Unlicensed report types appear in gray text.

Once the [Report Properties](#) dialog loads, use the controls to configure the properties.

For more information, see:

[Reports](#)

[Report Properties](#)

[Selecting a Report Type](#)

Selecting a Report Type

When adding a new report you are prompted to select a template type (e.g. Failed Logons or Largest Files). Unlicensed report types appear in gray text. If you would like to create a report that is not currently licensed, please visit www.CornerBowl.com and upgrade your license.

The following report types are available:

Type	Description	Licensing
Summary	Displays details for a list of monitors.	None Required
File and Directory Access Permission	Displays user access permissions (e.g. read, write) for directories and optionally files and sub-directories.	Disk Monitor
Duplicate Files	Displays a list of duplicate files.	Disk Monitor
Largest Files	Displays a list of the largest files.	Disk Monitor
Recently Accessed Files	Displays a list of recently accessed files.	Disk Monitor
Least Accessed Files	Displays a list of the least accessed files.	Disk Monitor

Once the *Report Properties* dialog loads, use the controls to configure the properties.

For more information, see:

[Adding Reports](#)

[Reports](#)

Report Properties

The *Report Properties* page enables you view and modify reports and when applicable assignments.

To view or edit a Report

From the *Object Explorer* select the target report then right click and select *Properties*.

Or

From the *Edit* menu item select *Batch -> Update Reports*. Once the *Select Multiple Reports* dialog loads check the target reports then click *OK*.

Common Configuration Objects

Templates include the following common configuration objects:

Configuration Object	Description
Name	The friendly name of the object.
Description	A user description of the object.
Enabled	Enables scheduled and real-time execution.
Temporarily Disabled	Temporarily disables scheduled and terminates real-time execution.
Execution Frequency	The scheduled frequency to execute the report.
Retain History	The number of days to retain the report execution history. NOTE: Monitor data is not saved to the history database.
Automatically Open	If checked the console automatically opens the report when the console connects to the service.

For more information see:

Selecting Multiple Reports

Server Manager provides you with the ability to quickly re-configure and delete multiple reports at the same time (e.g. assign a different schedule or complete action).

To update or delete multiple reports

From the *Edit* menu item select *Batch* -> *Update Reports*.

Using the *Select Multiple Templates* dialog

The *Select Multiple Reports* dialog enables you to select from a list of configured reports. The dialog includes a report type filter, an *Add* button and a *Delete* button.

- To filter by report type, select the type from the *Filter* combo box
- To add a new report, select the target group then click [Add](#).
- To delete a report, check each report then click *Delete*.
- To select multiple reports, check each report then click *OK*.
- To select a single report, double-click the report.

If updating reports, the [Report Properties](#) dialog will load.

For more information see:

[Adding Reports](#)

[Report Properties](#)

Duplicate Files Reports

Duplicate Files Reports list all files that have the same name, and/or are the same size, and/or have the same modified date. You have the option to scan a single directory or multiple directories contained on the same or multiple computers. All scans are recursive.

To display a report

From the *Object Explorer* navigate to the target computer and find the assigned disk or directory monitor template. If one does not exist, first create and assign a new *Disk Space Monitor* template.

Right click on the assigned template and select *Explore*.

Once the monitor detail loads select the *Explorer* tab.

From the *Explorer* tab select the target disk, share or directory then right click and select *Duplicate Files Report*.

To schedule a report

From the *File* menu item select *New Report*.

Once the *Select Report Type* dialog loads expand the *Disk Monitor* tree node then select *Duplicate Files*.

File and Directory Access Permissions Reports

File and Directory Access Permissions Reports are comprised of a list of directories, files, users, and assigned permissions (e.g. read, write, delete). You have the option to scan a single directory or multiple directories contained on the same or multiple computers. Scans can optionally recursively scan all sub-directories. When recursively scanned the report can optionally show detail for each file or summarize by concatenating permissions. The report can optionally validate users against the domain's Active Directory. Users not validated are removed from the report.

When run on-demand within the console, once complete, you can filter by directory and user, print the report, export the report to a file and re-run with different options.

To display a report

From the *Object Explorer* navigate to the target computer and find the assigned disk or directory monitor template. If one does not exist, first create and assign a new *Disk Space Monitor* template.

Right click on the assigned template and select *Explore*.

Once the monitor detail loads select the *Explorer* tab.

From the *Explorer* tab select the target disk, share or directory then right click and select *File and Directory Access Permissions Report*.

To schedule a report

From the *File* menu item select *New Report*.

Once the *Select Report Type* dialog loads expand the *Disk Monitor* tree node then select *File and Directory Access Permissions*.

To display a report from a disk monitor

File Extension Reports

File Extension Reports list the present extensions, total size and file count. Once complete you can drill down into a directory structure to see to which sub-directory file types of interest reside, print the report and export to a file.

To display a report

From the *Object Explorer* navigate to the target computer and find the assigned disk or directory monitor template. If one does not exist, first create and assign a new *Disk Space Monitor* template.

Right click on the assigned template and select *Explore*.

Once the monitor detail loads select the *Explorer* tab.

From the *Explorer* tab select the target disk, share or directory then right click and select *File Extension Report*.

Largest Files Reports

Largest Files Reports list the largest files on a disk within a directory structure. You have the option to scan a single directory or multiple directories contained on the same or multiple computers. All scans are recursive.

To display a report

From the *Object Explorer* navigate to the target computer and find the assigned disk or directory monitor template. If one does not exist, first create and assign a new *Disk Space Monitor* template.

Right click on the assigned template and select *Explore*.

Once the monitor detail loads select the *Explorer* tab.

From the *Explorer* tab select the target disk, share or directory then right click and select *Largest Files Report*.

To schedule a report

From the *File* menu item select *New Report*.

Once the *Select Report Type* dialog loads expand the *Disk Monitor* tree node then select *Duplicate Files*.

Least Accessed Files Reports

Least Accessed Files Reports list files that have not been recently accessed. Although not required by Windows applications, some applications update a file's last accessed time value whenever the application opens a file. This report scans a directory and sorts all files ascending by last accessed time. The top results are displayed. When run on-demand within the console, you can print the report, export the report to a file and re-run with different options.

You have the option to scan a single directory or multiple directories contained on the same or multiple computers. All scans are recursive.

To display a report

From the *Object Explorer* navigate to the target computer and find the assigned disk or directory monitor template. If one does not exist, first create and assign a new *Disk Space Monitor* template.

Right click on the assigned template and select *Explore*.

Once the monitor detail loads select the *Explorer* tab.

From the *Explorer* tab select the target disk, share or directory then right click and select *Least Accessed Files Report*.

To schedule a report

From the *File* menu item select *New Report*.

Once the *Select Report Type* dialog loads expand the *Disk Monitor* tree node then select *Least Accessed Files*.

Recently Accessed Files Reports

Recently Accessed Files Reports list recently accessed files. Although not required by Windows applications, some applications update a file's last accessed time value whenever the application opens a file. This report scans a directory and sorts all files descending by last accessed time. The top results are displayed. When run on-demand within the console, you can print the report, export the report to a file and re-run with different options.

You have the option to scan a single directory or multiple directories contained on the same or multiple computers. All scans are recursive.

To display a report

From the *Object Explorer* navigate to the target computer and find the assigned disk or directory monitor template. If one does not exist, first create and assign a new *Disk Space Monitor* template.

Right click on the assigned template and select *Explore*.

Once the monitor detail loads select the *Explorer* tab.

From the *Explorer* tab select the target disk, share or directory then right click and select *Recently Accessed Files Report*.

To schedule a report

From the *File* menu item select *New Report*.

Once the *Select Report Type* dialog loads expand the *Disk Monitor* tree node then select *Recently Accessed Files*.

Temporary Files Reports

Temporary Files Reports list all System and User temporary directories on any target Windows computer. The total size, file count, and sub-directory count is summed and listed. Once complete you can drill down into sub-directories to view the details within each temporary directory, delete temporary directory contents including files and sub-directories directly from within the report, print the report and export the report to a file.

Server Manager also enables you to configure the service to automatically delete all temporary files not locked and optionally older than a configurable number of days.

To display a report

From the *Object Explorer* navigate to the target computer right click and select *Temporary Files Report*.

To schedule temporary files to be deleted

From the *File* menu item select *New Template*.

Once the *Select Template Type* dialog loads expand the *Disk Monitors* tree node then select *Delete Temporary Files*.

Once the [Template Properties](#) dialog loads, use the controls to configure the properties, assign target hosts, host groups and template groups.

Schedules

A schedule is defined as an assignable configuration object that defines the frequency to execute a function (e.g. daily at 6:00 AM or every 5 minutes). Templates, reports and Auto Configurators all require schedule assignment.

During the installation a number of sample schedules are created. You have the option of using these schedules, modifying them or if prefer removing all of them and defining your own.

Load Balancing and Range Scheduling

Imagine a mid-size environment with 100 servers. Your task is to consolidate Event Log entries to a SQL Server database while also monitoring uptime. If you configure Server Manager to download daily at 2:00 AM and each server contains 3 logs of interest, at 2:00 AM Server Manager will create 300 threads and commence downloading of the Event Log entries. Understandably the consolidation database will more than likely bottleneck and timeout while attempting to commit the Security Event Log entries.

To alleviate the pressure on the consolidation database as well as the server hosting Server Manager, Server Manager includes range scheduling, a very powerful function to evenly distribute download, monitor and report execution over time. You can enable range scheduling by setting a schedule's type to *Range*.

Schedule Types Defined

Fixed	Defines a specific time which to execute (e.g. every hour at 30 minutes past the hour). Supports, seconds, minutes, hourly, daily, weekly and monthly.
Range	<p>Defines a range of available times which to execute (e.g. at any time but at minimum once an hour).</p> <p>Example: 3 HTTP monitors www.cornerbowl.com, www.diskmonitor.com and www.networkeventviewer.com with a schedule of once every 15 minutes would result in the following monitor executions:</p> <p style="padding-left: 40px;">www.cornerbowl.com: Executing at 0:00, 0:15, 0:30 and 0:45</p> <p style="padding-left: 40px;">www.diskmonitor.com: Executing at 0:05, 0:20, 0:35 and 0:50</p> <p style="padding-left: 40px;">www.networkeventviewer.com: Executing at 0:10, 0:25, 0:40 and 0:55</p> <p>Supports minutes, hourly, daily and weekly. Seconds and monthly frequencies are not supported.</p>

To add a new schedule

From the *File* menu item select *New -> Schedule*.

Once the *Schedule Properties* dialog loads see instructions below.

To modify an existing schedule

From the *Object Explorer*, navigate to the schedule then right click and select *Properties*.

Once the *Schedule Properties* page loads see instructions below.

Configuring a schedule

The *Schedule Properties* page enables you to set the schedule type, frequency and apply [maintenance windows](#) or other days or time ranges to exclude from the schedule.

From the *Type* combo-box select the schedule type: *Fixed* or *Range*.

From the *Frequency* combo-box select the frequency. Depending on the type of frequency selected,

different configuration controls will be provided. Set the control values as appropriate.

When applicable to the schedule type and frequency use the *Day of Week and Time of Day Exclusions* controls to add maintenance windows as well as any other days or time ranges you want to exclude from the schedule.

When you have finished configuring the schedule, you have the option of applying an auto-generating name based on the schedule you have just configured (e.g. Every 4 hours). To auto-generate a name click the *Generate* button.

To delete a schedule

From the *Object Explorer* navigate to the target schedule then right click and select *Delete*.

For more information, see:

[Configuring Day and Time Exclusions](#)

[Enabling and Disabling Objects](#)

Configuring Day and Time Exclusions

When configuring execution schedules some frequency types support day and time exclusions (e.g. execute every hour excluding Sunday between 2 AM and 4 AM). Day and time exclusions enable you to configure maintenance windows into the software.

Using day and time exclusions you can also create multiple monitors for each shift operator (e.g. create a ping monitor for 12 AM – 12 PM which emails system administrator A then create a ping monitor for 12 PM - 12 AM which emails system administrator B).

To add an day or time range exclusion

From the *Object Explorer* navigate to the target schedule then right click and select *Properties*.

From the *Schedule* properties page any frequency that supports exclusion periods will include a list control titled *Day of Week and Time of Day Exclusions* . From this control click the *Add* button.

From the *Exclusion Period* dialog select the day of week or time ranges to exclude.

To edit, delete or clear existing day and time range exclusions

From the *Object Explorer* navigate to the target schedule then right click and select *Properties*.

From the *Schedule* properties page any frequency that supports exclusion periods will include a list control titled *Day of Week and Time of Day Exclusions* . From this control click the *Edit, Delete and/or Clear* button to achieve the desired results.

For more information, see:

[Schedules](#)

[Enabling and Disabling Objects](#)

Actions, Notifications and Alerts

Actions, notifications and alerts are executed when:

- A monitor is triggered, recovers and in some cases is complete (e.g. Delete Temporary Files and Create Process monitors)
- A report is complete or errors
- An Auto Configurator is complete or errors

The following actions are available:

Database	When monitoring log entries, writes each filtered log entry to a user defined database table. Please note error and recovery alerts are not supported.
Email	Sends a simple text message or a detailed HTML message. Both text messages and HTML messages can be customized using Actions Tags or by creating your own HTML Templates.
Event Log	Writes a custom entry to the Event Log of your choice. When monitoring log entries, writes each filtered log entry. The Event Log Source field supports the following Action Tags: {HOST}, {IPv4}, {IPv6}
File	Saves results to file. When monitoring log entries, writes each filtered log entry. Supports: CSV, EVT, HTML and TXT.
Manage a Process	Restarts, stops or starts a Windows process. The arguments field supports the following Action Tags: {HOST}, {IPv4}, {IPv6}, {MESSAGE} When monitoring log entries, to start a process for each log entry, include one of the following tags within the arguments field: {HOST}, {IPv4}, {IPv6}, {MESSAGE}. These fields are replaced with the appropriate values within each entry prior to the process being started.
Manage a Service	Restarts, stops or starts a Windows Service.
Message Box	Displays a message box on any computer that has the Server Manager Tray Icon installed. Requires TCP port 6766 . For more information see Desktop Actions .
SMS (Pager)	Sends a text message using one of several web SMS online gateway services.
SNMP Trap	Sends a SNMP trap via Microsoft's SNMP Service.
Sound	Plays a sound on any computer that has the Server Manager Tray Icon installed. Requires TCP port 6766 . For more information see Desktop Actions .
Syslog Message	Writes a message to any syslog server. When monitoring log entries, writes each filtered log entry.

For more information see:

[Action Tags](#)

[Desktop Actions, Alerts and Notifications](#)

[HTML and Email Templates](#)

Desktop Actions, Alerts and Notifications

Desktop actions are defined as actions that are executed within a user's Windows desktop (e.g. message box alerts, sound alerts and optionally interactive file execution).

Server Manager enables you to receive desktop notifications from any Windows computer that has network access to the Server Manager Service.

To configure your workstation, laptop or home computer to receive desktop notifications

From the target computer, install Server Manager.

Once installed select *File -> New Server Manager Connection* .

Once the *Connect to Service* dialog loads, specify a connection name.

From the *Server name* text box type the routable hostname or IP address the service is installed.

Specify credentials that provide administrator access to the server the service is installed.

Click *Connect*.

Once connected, from the *Object Explorer* navigate to the target desktop action then right click and select *Properties* or create a new action.

From the *Action Properties* page locate the *Target* list box and command buttons. Click the *Add Computer* button.

Once the *Add Computers, Devices and Hosts* dialog loads, from the combo-box select *Localhost* then click *OK*.

From the *Action Properties* page click *Apply* or *OK* to save your changes.

Finally, click the *Test* button. You should now see the test message box or hear the sound alert on the target computer as well as all other computers assigned to the action. If the connection fails due to a network error, be sure to open [TCP port 6766](#) on your organization's firewall.

For more information see:

[Client/Server Architecture](#)

[Tray Icon](#)

Action Tags

Under construction

File Consolidation

The following item tags are available:

PATH	The target path
FILE_COUNT_COPIED	The number of files copied
FILE_SIZE_COPIED	The size of the files copied
FILE_COUNT_DELETED	The number of files deleted
FILE_SIZE_DELETED	The size of the files deleted
DIRECTORY_SIZE	The size of the directory

HTML and Email Templates

Under construction

File Output Options

When running on-demand reports (e.g. failed logon attempts or largest files), you have the option to save the report results to file. The following file formats are supported:

- HTML
- Text
- CSV

When saved, previously generated reports can be:

Overwritten	Deletes the old file and replaces with the new file.
Backed up	Moves the previously generated file to a backup sub-directory and renames the file using a combination of the current filename and current date.
Appended to	Text and CSV only. Appends the report to the previous file.

By default, HTML and Text files are saved using UTF8 encoding meaning any language will display as expected, however, if your primary language requires Unicode (e.g. Japanese or Chinese), reports may be reduced in size by saving to Unicode format.

Microsoft Excel requires CSV files be saved in UTF7 (ASCII) encoding. To minimize interface requirements with Excel, CSV files are saved using UTF7 encoding. If your language requires UTF8 (e.g. non-English based languages) save CSV files to Unicode. When opened in Excel, you will be prompted to define the column delimiters.

Filters

Under construction

Auto Configurators

An Auto Configurator is defined as a configuration object that enables Server Manager to automatically monitor new servers and workstations. When utilized in large environments, Auto Configurators can be a very powerful tool enabling Server Manager to automatically monitor new and renamed servers without any interaction between yourself and Server Manager.

How it works...

When executed an Auto Configurator scans your Active Directory tree or targeted organizational unit for computers. Once found, each computer is filtered through an optional property filter (e.g. operatingSystem contains Server) and an exclusion list. Once filtered, each computer is then added to the system. Finally, targeted templates and reports are assigned to each computer.

NOTE: When executed any computer that has already been added to Server Manager will be updated with the latest template, report and group assignments assigned to the Auto Configurator. Previous assignments are left unmodified. For example, if you have previously configured a server and have modified the Auto Configurator to include a new template such as a Disk Space Monitor template, the template will be assigned to all computers that reside in both the Active Directory tree and Server Manager.

To create a new Auto Configurator

From the *File* menu item select *New -> Auto Configurator*.

To batch update existing Auto Configurators

From the *Edit* menu item select *Batch -> Update Auto Configurators*.

For more information see:

[Adding Auto Configurators](#)

[Auto Configurator Properties](#)

[Configure Active Directory Connections](#)

Adding Auto Configurators

To add a new Auto Configurator

From the *File* menu item select *New Auto Configurator* .

From the *Select Active Directory Organizational Unit* dialog select the target organizational unit.

Once the [Auto Configurator Properties](#) dialog loads, use the controls to configure the properties and assign target groups, templates and reports.

For more information, see:

[Auto Configurators](#)

[Select Active Directory Organizational Unit](#)

Auto Configurator Properties

The *Auto Configurator Properties* page enables you view and modify the Auto Configurators.

To view or edit an Auto Configurator

From the *Object Explorer* select the target Auto Configurator or [Auto Configurator group](#) then right click and select *Properties*.

Or

From the *Edit* menu item select *Batch -> Update Auto Configurators*. Once the *Select Multiple Auto Configurators* dialog loads check the target Auto Configurators then click *OK*.

Configuration Objects

Auto Configurators include the following configuration objects:

Configuration Object	Description
Name	The friendly name of the object.
Description	A user description of the object.
Active Directory path	The full path to the target organizational unit.
Recurs OU	Option to recursively scan the organizational unit.
Append domain name	Option to append a domain name so computers can be accessed using their FQDN.
Enabled	Enables the scheduled execution.
Temporarily disabled	Temporarily disables scheduled execution.
Execution frequency	The frequency to execute.
Object assignment	The groups and objects to assign discovered computers (e.g. templates).
Exclusion filters	Complex Active Directory computer property filters (e.g. operatingSystem contains 'Server') and computer name exclusion list with import function.
History retention policy	The number of days to retain execution results in the history database.
Complete actions	Actions and notifications to execute when complete (e.g. receive a daily report that shows a detailed list of updates).
Error actions	Actions, alerts and notifications to fire when there is an execution error (e.g. the Active Directory path cannot be found).

For more information see:

[Auto Configurators](#)

[Groups](#)

[Selecting Multiple Auto Configurators](#)

Selecting Multiple Auto Configurators

Server Manager provides you with the ability to quickly re-configure multiple Auto Configurators at the same time (e.g. assign a different schedule or complete action).

To update multiple Auto Configurators

From the *Edit* menu item select *Batch -> Update Reports*.

Using the *Select Multiple Auto Configurators* dialog

The *Select Multiple Auto Configurators* dialog enables you to select from a list of configured Auto Configurators. The dialog includes an *Add* button.

- To add a new Auto Configurator, select the target group then click [Add](#).
- To select multiple Auto Configurators, check each Auto Configurator then click *OK*.
- To select a single Auto Configurator, double-click the Auto Configurator.

Once selected, the [Auto Configurator Properties](#) dialog will load.

For more information see:

[Adding Auto Configurators](#)

[Auto Configurator Properties](#)

Select Active Directory Organizational Unit

When adding a new Auto Configurator you are prompted to select an organizational unit within your Active Directory tree. The *Select Active Directory Organizational Unit* dialog enables you to select an Active Directory organizational unit (ou).

To select an organizational unit

From the *Active Directory connection* combo-box select the target Active Directory connection.

From the tree view navigate to the target organizational unit then click *Select*.

To edit an existing Active Directory connection or create a new connection

Click the *Edit* button.

Signing Files

Under construction

Creating a Filename Mask

Directory Cleaner

Directory Watcher

Under construction

Access Denied

An “Access Denied” error is typically thrown by the local WMI Service when an attempt is made to access WMI functions from a computer that is either not logged into the domain or when the Corner Bowl Log Manager Service is not running with domain administrator credentials.

To quickly verify the error using built-in Microsoft tools already installed on your server or workstation open a command-prompt and type:

```
wbemtest
```

Once loaded, click the *Connect* button. From the *Namespace* text box type \\SERVERNAME\root\cimv2 where SERVERNAME is the name of the remote server throwing the RPC server is unavailable error. If either computer resides on a different domain or within a workgroup specify administrator credentials that reside on the remote computer or domain. When you are finished, click *Connect*. You should receive the *Access Denied* error.

Solutions

1. Select *Service | Change Service Logon*. Specify domain administrator credentials then click *OK*. The service will be automatically restarted using the credentials you specified. If the service fails to start, check the credentials and try again.
2. If either the local computer or the target computer are not logged into the domain, specify logon as credentials. From the *Configuration Explorer*, select *Group by Log Type*, navigate to the computer of interest, right click and select *De-Select All*. Right click again and select *Log Monitor Properties Wizard*. Once the *Event Log Management Wizard* opens click *Next*. Check the *Logon As* option then specify the credentials. When specifying credentials that reside directly on the target computer (rather than a domain administrator account), specify the computer name in the Domain combo-box.

Other things to look at

1. Ensure WMI permissions have been set correctly. From the remote computer throwing the error, open a command-prompt and type: *wmimgmt.msc*. Right click on the *WMI Control (local)* node and select *Properties*. Select the *Security* tab and navigate to *root/CIMV2*. Click the *Security* button. Grant the account you and the service are using to access logs *Remote Enable* and *Read Security* rights.
2. If access is denied to a Windows Server 2003 log, grant the account you are logged in as and the account the service is running under access to each event log. For more information read the following MSDN article: [How to set event log security locally or by using Group Policy in Windows Server 2003](#)
3. When accessing a Windows 7 or Vista computer that has joined a workgroup rather than a domain, the remote computer must disable User Access Control (UAC). To disable UAC on a Windows 7 or Vista computer, search for *Turn UAC off* within the Windows help system.
4. If the remote computer is running Windows XP Pro, make sure remote logons are not being coerced to the GUEST account. From the computer you are unable to download logs from, open a command-prompt and type *secpol.msc*. Expand the *Local Policies* node and select *Security Options*. Scroll down to the setting titled *Network access: Sharing and security model for local accounts*. If this is set to *Guest only*, change it to *Classic* and restart your computer.
5. From the computer you are unable to download logs from, open a command-prompt and type *dcomcnfg*. Expand the *Component Services/Computers/My Computer* node. Right click *My Computer* and then select *Properties*. Select the *COM Security* tab. From the *Launch and Activation Permissions*, select *Edit Limits*. Add the appropriate account and assign all permissions.
6. Check that DCOM is enabled on both the local and the remote computer. Check the following registry value on both computers: Key: HKLM\Software\Microsoft\OLE, value: EnableDCOM, should be set to 'Y'
7. Check that WMI is installed on both the local and remote computer. WMI is present by default in all flavors of Windows 2000 and later operating systems, but must be installed manually on NT4 systems. To check for the presence of WMI, open a command-prompt and type *wbemtest*. If the WMI Tester application starts up, WMI is present, if not, it must be installed. Consult Microsoft for more information.
8. Verify the Windows Management Instrumentation is running on both the local and target computers.

Quota Violation

A “Quota Violation” is thrown by the WMI Service running on the target machine when Log Manager requests the contents of a large Event Log. We typically see a quota violation thrown when downloading a remote Security Event Log that is approximately 400 MBs in size for the first time. You have 3 options to resolve this error:

1. Increase the WMI Quota settings.
2. Backup and clear the Event Log.
3. Limit the download to a smaller date range such as 1 day.

Increasing the WMI Quota

From the *Object Explorer* navigate to the computer throwing the Quota Violation error then right click and select *Properties*.

Once the *Host Properties* dialog loads, select the *WMI* tab.

Double the *Memory per host* value. If the *Memory per host* is the same value as *Memory all hosts* value, double both the *Memory per host* and the *Memory all hosts* values. Click *Apply* to save your changes. For more information read the following Microsoft article: [WMI Error: 0x8004106C Description: Quota violation, while running WMI queries](#)

Backing-up and Clearing

From the *Configuration Explorer*, navigate to the log of interest, right click and select *De-Select All*. Right click again and select *Properties*. Select the *Windows Event Log* tab and select *Clear Log*.

Limiting the Download Date Range

From the *Configuration Explorer*, navigate to the log of interest, right click and select *De-Select All*. Right click again and select *Properties*. Select the *Log Consolidation* tab then set the initial download to a lesser value such as 1 day.

The RPC Server is Unavailable

A “The RPC server is unavailable” is thrown by the local WMI Service when an attempt is made to access WMI functions from a computer that is blocking WMI requests or has a firewall between the computers.

To quickly verify the error using built-in Microsoft tools already installed on your server or workstation open a command-prompt and type:

```
wbemtest
```

Once loaded, click the *Connect* button. From the *Namespace* text box type \\SERVERNAME\root\cimv2 where SERVERNAME is the name of the remote server throwing the RPC server is unavailable error. If either computer resides on a different domain or within a workgroup specify administrator credentials that reside on the remote computer or domain. When you are finished, click *Connect*. You should receive the *RPC server is unavailable* error.

Solutions

1. Open TCP port 135 and all TCP ports above 1024. For more information read the following Microsoft article: [Connecting to WMI Remotely Starting with Windows Vista](#)

NOTE: Many virus protection solutions such as McAfee and Symantec contain their own firewalls and may offer a function to allow WMI packets.

2. Configure the WMI Service on each Server 2008, Windows 7 or Vista computer to run on a specific port then open TCP port 135 and the specified port. Please note this is not an option for Server 2003 or Windows XP computers. For more information read the following Microsoft article: [Setting Up a Fixed Port for WMI](#)

3. Install Log Manager on each sub-net then push Event Log entries directly to a central database. Please note this requires you to open the necessary database ports. In the case of SQL Server this is TCP port 1433 by default.

Other things to look at

1. When accessing a Windows 7 or Vista computer that has joined a workgroup rather than a domain, the remote computer must disable User Access Control (UAC). To disable UAC on a Windows 7 or Vista computer, search for *Turn UAC off* within the Windows help system.
2. If the remote computer is running Windows XP Pro, make sure remote logons are not being coerced to the GUEST account. From the computer you are unable to download logs from, open a command-prompt and type *secpol.msc*. Expand the *Local Policies* node and select *Security Options*. Scroll down to the setting titled *Network access: Sharing and security model for local accounts* . If this is set to *Guest only*, change it to *Classic* and restart your computer.
3. From the computer you are unable to download logs from, open a command-prompt and type *dcomcnfg*. Expand the *Component Services/Computers/My Computer* node. Right click *My Computer* and then select *Properties*. Select the *COM Security* tab. From the *Launch and Activation Permissions*, select *Edit Limits*. Add the appropriate account and assign all permissions.
4. Check that DCOM is enabled on both the local and the remote computer. Check the following registry value on both computers: Key: HKLM\Software\Microsoft\OLE, value: EnableDCOM, should be set to 'Y'
5. Check that WMI is installed on both the local and remote computer. WMI is present by default in all flavors of Windows 2000 and later operating systems, but must be installed manually on NT4 systems. To check for the presence of WMI, open a command-prompt and type *wbemtest*. If the WMI Tester application starts up, WMI is present, if not, it must be installed. Consult Microsoft for more information.
6. Verify the Windows Management Instrumentation is running on both the local and target computers.

Terminology

Term	Definition
Action	Actions are defined as functions that execute in response to a monitor or report completing, triggering or erroring (e.g. sending an email or displaying a message box alert).
Desktop Action	Desktop actions are defined as actions that are executed within a user's Windows desktop (e.g. message box alerts, sound alerts and optionally interactive file execution)
Host	The term <i>host</i> is used by Server Manager to refer to either a computer, a device (e.g. switch, router or firewall) or a host (e.g. www.CornerBowl.com).
Schedule	An assignable configuration object that defines the frequency to execute a function (e.g. daily at 6:00 AM).
Server Manager Console (console)	The client application that enables you to configure the service and manually execute monitors, reports and Auto Configurators.
Server Manager Service (service)	The server application responsible for executing monitors, reports and Auto Configurators.
Server Manager Tray Icon (tray icon)	The client application that enables your Windows desktop to display system status, receive desktop notifications (e.g. message box alerts, sound alerts and optionally interactive file execution) and launch the console.
Template	An assignable configuration object that defines properties for an executable function (e.g. a Ping template that defines the failure rate prior to triggering or an HTTP template that sends an email alert when any assigned website is down).