Getting Started

SNMPc Enterprise

Version 10, March 2017

Castle Rock
Computing

Castle Rock Computing
Saratoga, CA, USA

Phone: 408-366-6540
Email: sales@castlerock.com
WEB: www.castlerock.com

Printed in the United States of America

Contents

Using this Document

This document provides a tutorial description of the most commonly used SNMPc Enterprise features. It is not an exhaustive reference document and most areas are not completely described. But the examples provide insight into SNMPc Enterprise usage and should be enough to get started with SNMPc Enterprise.

For a complete description of SNMPc Enterprise, please use the ***Help/Help Topics*** menu to show the Online Help system. The Online Help system includes a high level ***Table of Contents***, as well as an ***Index*** and ***Keyword Search*** mechanism. You can also press the ***F1 key*** at any time to show ***Context Sensitive Help*** for a currently displayed dialog or for the most recently activated console window.

This document is available in Adobe PDF format at the ***Products*** page of *www.castlerock.com* and in the SNMPc Enterprise ***Help/Getting Started*** menu.

> This document and the SNMPc Enterprise Help system assume that you have a good working knowledge of the Simple Network Management Protocol (SNMP). We recommend that you read and understand one of the many available books that describe SNMP before working with SNMPc Enterprise.

Getting Technical Support and Updates

SNMPc Enterprise includes free technical support via email and web downloadable updates for a period of three months from purchase. An unconditional full refund is also available during this period. With technical support, you can get help when installing or using SNMPc Enterprise. We do not provide telephone support or training.

For continued technical support and downloadable updates you must purchase an Extended Software Updates license on a yearly basis. Please go to the Sales page at www.castlerock.com for more information.

For technical support, please go to the ***Support*** page at *www.castlerock.com*. Press "Click Here to Create a New Account" to register at our HelpDesk system.

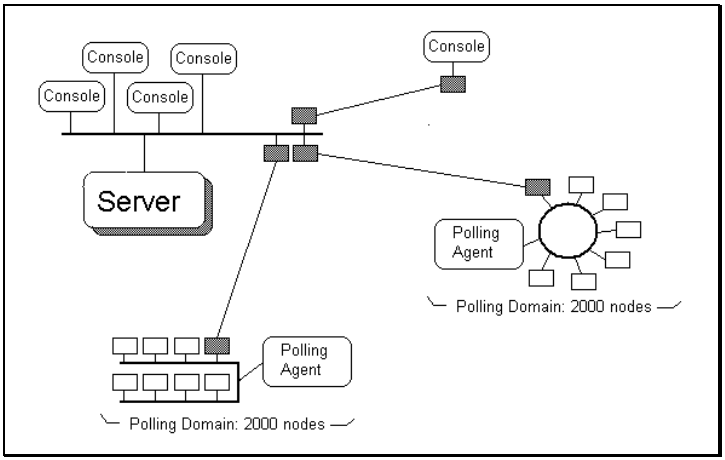
After creating your HelpDesk account, log on and click the "Support Tickets" link. Then use the Post link in the upper right of the page to add a new support ticket.

Once you have created a HelpDesk account you can also send email to *support@castlerock.com.*

Architecture Overview

SNMPc Enterprise is a general-purpose Distributed Network Manager offering the following benefits over a standalone product:

- By using ***Polling*** and ***Server*** components that run on multiple computers, SNMPc Enterprise can be scaled to manage very large networks.
- By using multiple ***Remote Consoles***, SNMPc Enterprise encourages sharing of management information by many people.
- SNMPc Enterprise is cost-effective because a collection of components costs less than an equivalent number of standalone managers.



SNMPc Enterprise uses the popular SNMP management protocol to poll and configure devices, workstations and servers over IP networks. Along with all the features expected in any SNMP management station, SNMPc Enterprise also includes the following advanced features:

- Secure SNMP Version 3 support
- Supports Internet Protocol Version 6 (IPv6) addressing
- Scalable to 25,000 managed devices.
- Supports a manager-of-managers architecture
- Redundant Backup Server support
- Remote Consoles and JAVA Web access.
- Event forwarding and email/pager notifications.
- Audit events for user actions (login/editing)
- Application Service (TCP) polling
- Integrates with SNMPc OnLine Reporting and Web Interface
- Custom MIB Tables with Derived MIB Expressions.
- RMON-I user interface application.
- Web Map Service (WMS) support for Geographic map views.
- GUI Device Support development tools.
- Application programming interfaces with samples.

SNMPc Workgroup Edition

SNMPc is also available to large OEM and U.S. Government entities as a standalone Workgroup edition. SNMPc Workgroup has the same interface as SNMPc Enterprise but with some limited functionality.

The following table shows the differences between the Enterprise and Workgroup editions:

FEATURE	ENTERPRISE	WORKGROUP
Device Limit	25,000	1000
Distributed Scalable Architecture	Yes	
Backup Server Support	Yes	
Remote Poller Included	Yes (10)	
Remote Consoles Included	Yes	
JAVA Console Included	Yes	
SNMPc OnLine Web access	Yes	
Netflow Device Reporting	Yes (10)	
Automatic ODBC Export	Yes	

SNMPc System Requirements

The following table lists the minimum *recommended* system requirements.

PARAMETER	MINIMUM REQUIREMENT
CPU	Intel 2 GHz
Memory	8 GB
Disk Free	100 GB
Windows Operating System	10, 8, 2012, 7, 2008R2

Device Access Modes

SNMPc Enterprise supports various device access modes including TCP only, ICMP (Ping), SNMP V1, SNMP V2c and SNMP V3. Each mode is briefly described below.

None (TCP Only)

Null access is used for polling TCP services only, where ICMP/SNMP access is restricted by a firewall.

ICMP (Ping)

ICMP (Ping) mode is used for devices that do not support SNMP but can still be *Pinged* to see if they are responding. This may include servers and workstations.

SNMP V1 and V2c

SNMP V1 and SNMP V2c are very similar SNMP Agent protocols that are used by most currently deployed network devices. Any device that supports V2c will generally also support V1. SNMPc Enterprise uses automatic intelligence to switch from one mode to the other as needed. So in most cases you will always select ***SNMP V1*** as the device access mode for any SNMP device.

Since SNMP V1 and V2c are the most common and simplest SNMP protocols, this guide will only show you how to use these protocols.

SNMP V3

SNMP V3 is a secure SNMP Agent protocol that supports authentication and privacy (encryption). The use of SNMP V3 is considered an advanced topic. As such, this guide does not describe V3 in any detail. For more information about using V3, please use the ***Help/Help Topics*** menu and search for ***Setting Device Access Modes*** in the Index.

Internet Protocol Version 6 (IPv6) Addressing

This version of SNMPc Enterprise supports IPv6 addressing of polled devices only and reception of traps from IPv6 addressed devices.

At this time all communication between SNMPc Enterprise server, poller and console components is only supported with IPv4 addresses. Every system that runs SNMPc Enterprise components must reside on an IPv4 network and be addressable using IPv4.

Use an IPv6 hexadecimal address or a DNS name that resolves to an IPv6 address in the Address field of any map Device, Link, or Network type object.

DNS address lookup can return multiple addresses that match the same name, including IPv4 and IPv6 addresses. By default SNMPc Enterprise will choose the IPv4 address. To force SNMPc Enterprise to use the IPv6 address, surround the DNS name in square braces, for example “[name]” instead of “name”.

Please note the following caveats:

- To use the Windows SNMP agent with IPv6 you must set an IPv6 address as an accepted host in the Security tab of the SNMP Service Properties dialog. Alternatively you can allow all hosts access. The default is 127.0.0.1.

- There is a new set of IPv6 menus but not all devices that support IPv6 will support these tables. Specifically, Windows does not support any of them.

- SNMPc Enterprise components (server, poller, console) communicate with each other using IPv4 only. Therefore, when using IPv6 SNMPc Enterprise must be installed on a system that supports both IPv6 and IPv4 networks.

- When using a link local address with scope identifier (scope id) (%nn in fe80:...%nn) it is important to understand that scope id's are local to the computer sending a packet (i.e., SNMPc Enterprise server) and represent the interface number the packet will be sent out from.

  For example, if you want to poll computer AA from SNMPc Enterprise at computer BB and use *ipconfig* on AA to get the address to use, the scope id you see will not be valid on BB. You need to use the scope id of the network interface on BB that AA is connected to. Note that the scope id on AA <<MAY>> be the same as the correct value, but it is not guaranteed. Scope identifiers are ONLY valid on the sending computer.

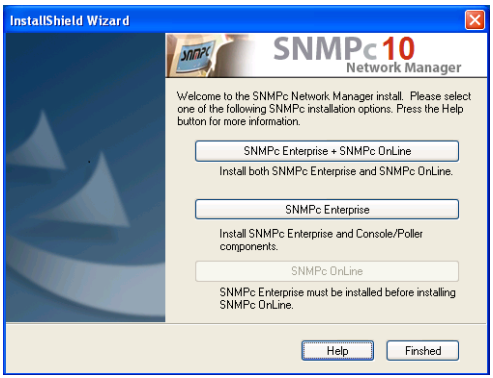
  An interesting side effect of using link local addresses with scope id's in SNMPc Enterprise is that the scope id you use will become invalid if you change the interface your computer is using, for example from a hardwired network to a wireless connection, or vice-versa.

  If your computer only has one network card then you can use a link local address without specifying the scope identifier.

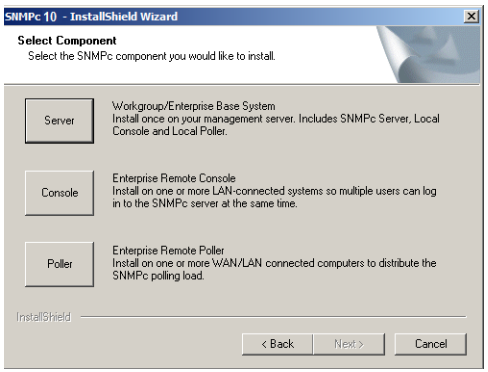
Installing the SNMPc Enterprise Server and Local Console

SNMPc Enterprise is sold as a bundle with the SNMPc OnLine web based reporting engine as the ***SNMPc Network Manager***. Use the SNMPc Network Manager installation package to install SNMPc Enterprise components.

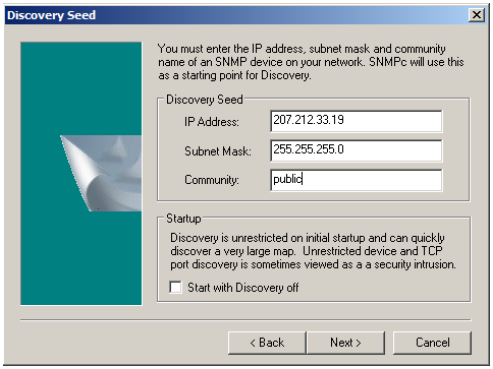
- Log on to Windows with Administrator permission.
- Insert the SNMPc Network Manager CDROM into the CDROM drive.
- Use the ***Windows Start/Run*** menu and enter *d:\setup*, where *d:* is the CDROM drive.
- The install program will show three buttons to optionally install SNMPc Enterprise, SNMPc OnLine, or both applications. Select one of the buttons marked as installing SNMPc Enterprise.



- The SNMPc Enterprise installation program will show a dialog with three buttons for the installable SNMPc Enterprise options. On your main SNMPc Enterprise system, you only need to install the Server component, as this includes a local console and polling agent.
- Press the **Server** button.



- You will be prompted for the installation directory next, and then the ***Discovery Seed*** dialog will be displayed. You must enter valid information at this dialog or network discovery will not work properly.
- Enter the IP Address of an SNMP *Seed Device* on your network, preferably a router.
- Enter the Subnet mask for the Seed Device.
- Enter the SNMP V1 ***Read Community*** for the seed device.
- The install program will proceed to install SNMPc Enterprise on your hard drive. After the installation is complete, logoff Windows and restart your computer.



Installing the Air Messenger Pro Paging Software

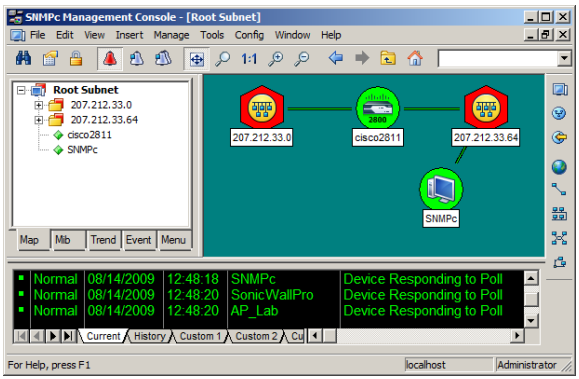
SNMPc Enterprise includes a copy of the ***Air Messenger Pro*** paging application. This software is required if you want SNMPc Enterprise to page you when an event occurs. Air Messenger Pro is not installed as part of the regular SNMPc Enterprise installation.

To install the Air Messenger Pro paging application, use the Windows ***Start/Programs/SNMPc Network Manager/Install Air Messenger Pro*** menu. In Windows 8, use the Search charm to bring up the application list, then use the ***Install Air Messenger Pro*** icon under the SNMPc Network Manager section. Follow the installation instructions.

After you have installed Air Messenger Pro you can configure SNMPc Enterprise to notify your pager when an event occurs. Please refer to the ***Emailing or Paging the Administrator on an Event*** section in this guide for further instructions.

Starting the SNMPc Enterprise Server and Local Console

To control SNMPc Enterprise tasks, you must be logged on to Windows with Administrator permission.



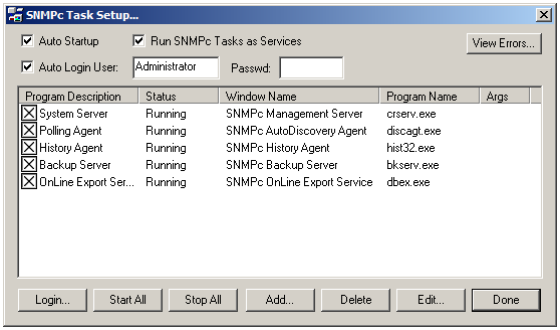
After installation of the SNMPc Enterprise Server component, you will be asked to reboot the Windows system.

When the system has rebooted and you logon to Windows, the SNMPc Enterprise Server and Console applications will be automatically started and you will be automatically logged on.

Disabling Automatic Console Login

To disable automatic console startup and login, go to the Windows Start menu and use the ***Programs/SNMPc Network Manager/Configure Tasks*** menu.

Disable the ***Auto Login User*** check box and press the ***Done*** button.



Starting a Local Console Session

Go to the Windows Start menu and use the ***Programs/SNMPc Network Manager/Login Console*** menu. At the login prompt, enter localhost as the Server Address. Enter the username and password and press OK. Initially there is only one user named Administrator with no password.

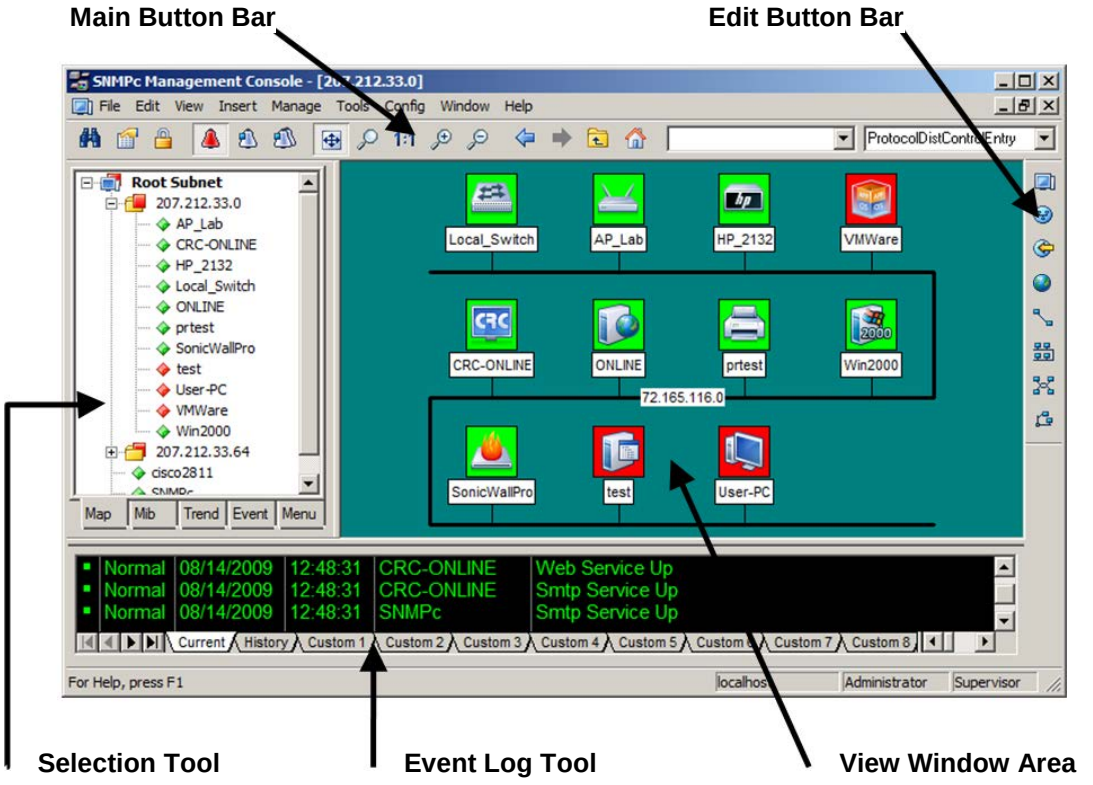
Stopping and Starting the Server

Go to the Windows Start menu and use the ***Programs/SNMPc Network Manager/Shutdown System*** menu to stop the SNMPc Enterprise Server system tasks. Use the Windows Start ***Programs/SNMPc Network Manager/Startup System*** menu to restart the SNMPc Enterprise Server system tasks. Note that any running console sessions will be logged off and you will need to exit the console applications separately.

To disable automatic startup of the SNMPc Enterprise Server system tasks, go to the Windows Start menu and use the ***Programs/SNMPc Network Manager/Configure Tasks*** menu. Disable the ***Auto Startup*** check box and press the ***Done*** button.

Using Console Elements

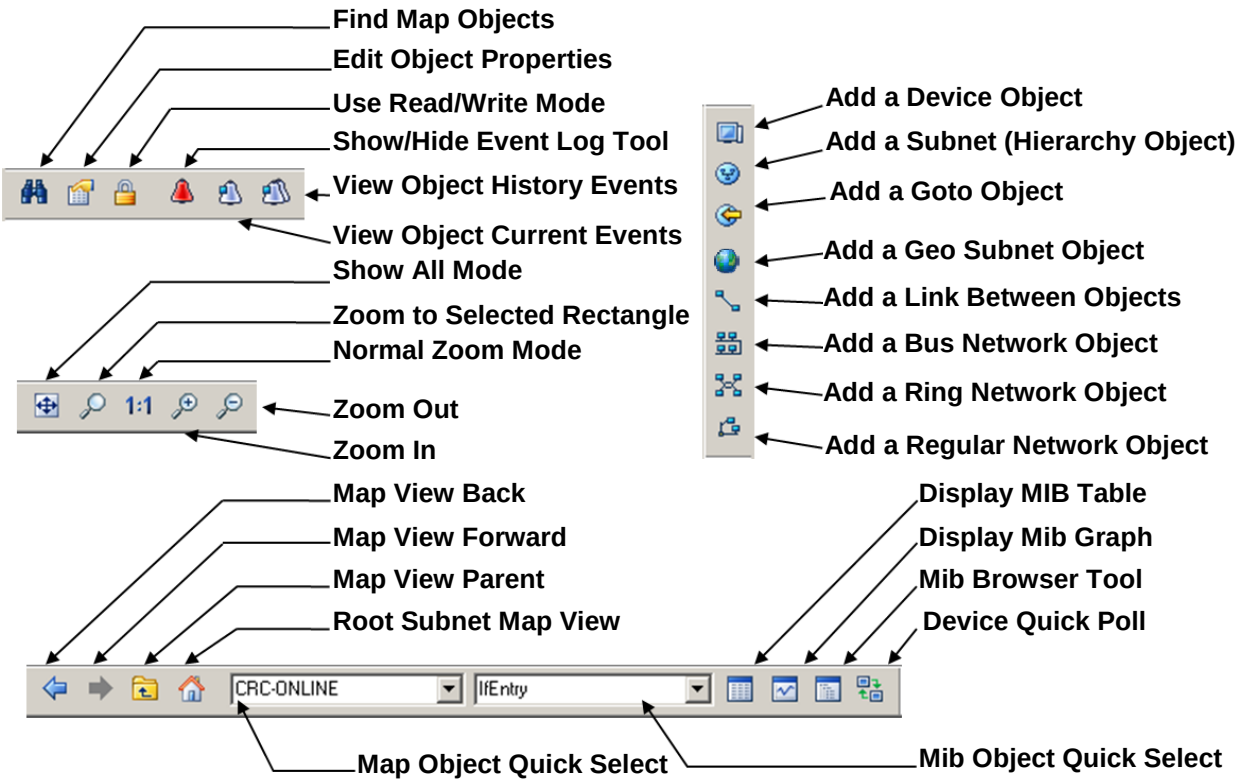
The following diagram and table below show the main elements of the SNMPc Enterprise console.



ELEMENT	FUNCTION
Main Button Bar	Buttons and controls to execute common commands quickly
Edit Button Bar	Buttons to quickly insert map elements
Selection Tool	Tabbed control for selection of objects within different SNMPc Enterprise functional modules
Event Log Tool	Tabbed control for display of filtered event log entries
View Window Area	Map View, Mib Tables, and Mib Graph windows are shown here.

Console Button Commands

The following diagram shows the function of each button in the Main Button Bar and Edit Button Bar. Each of these buttons has a corresponding main menu item.



Selection Tool

If you can't see the selection tool, use the ***View/Selection Tool*** menu to show it. Use the Selection Tool to manipulate objects from one of several databases. Use the drag control at the right of the Selection Tool to change its size. Select one of the Selection Tool tabs to display a tree control for the database. Use the ***right-click*** menu inside a selection tree for database-specific commands.

SELECTION TAB	DESCRIPTION
Map	Map Object database, including devices and subnets.
Mib	Compiled SNMP Mibs, Custom Tables and Custom Mib Expressions.
Trend	Report profiles that define long term polling procedures and scheduled reports.
Event	Event filters used to determine what happens when an event is received.
Menu	Custom menus that appear in the Manage, Tools, and Help menus.

Event Log Tool

The Event Log Tool displays different filtered views of the SNMPc Enterprise event log. If you can't see the Event Log Tool, use the ***View/Event Log Tool*** menu to show it.

- Select the ***Current*** tab to show unacknowledged (current) events. These events have a colored box at the left side of the log entry. The color of map objects is determined by the highest priority unacknowledged event for that object.
- Select the ***History*** tab to show all events, including acknowledged and unacknowledged events.
- Select one of the ***Custom*** tabs and use the right-click ***Filter View*** menu to specify what events should be displayed for that tab.
- ***Double-click*** an event entry to display a Map View window with the corresponding device icon visible.
- To quickly view events for a particular device, first select the device and then use one of the ***View Events*** buttons (or the ***View/Active Events*** and ***View/History Events*** menus). This will show the device events in a separate window in the View Windows area.
- To remove one or more events, select the events and press the ***Delete*** key.
- To acknowledge (remove current status of) an event, select the event and use the right-click ***Acknowledge*** menu.
- To completely clear the event log, use the ***File/Clear Events*** menu.

View Window Area

The View Window Area is the main interface for viewing the SNMPc Enterprise map and command results. This area uses the *Multi-Document-Interface* (MDI) specification to display multiple windows at the same time.

Use the ***Window/Cascade*** and ***Window/Tile*** menus to rearrange the windows in the View Window Area in a way that makes them all visible.

Windows in this area can be in one of several states:

- A ***Maximized*** window uses the entire area and hides any other windows behind it. If you close a maximized window, the next top-most window will still be displayed in the maximized state. You need to be careful when using maximized windows because it is easy to lose track of how many windows you have opened and there is an upper limit. Use the ***Windows*** menu to see a list of windows. Use the ***Windows/Cascade*** menu to view all windows at the same time.

- An ***Overlapped*** window does not take up the entire area. One window will be completely visible and other windows are partially hidden behind it. This is the most common situation for the View Window area because it lets you view maps, tables and graphs at the same time and quickly move between them.

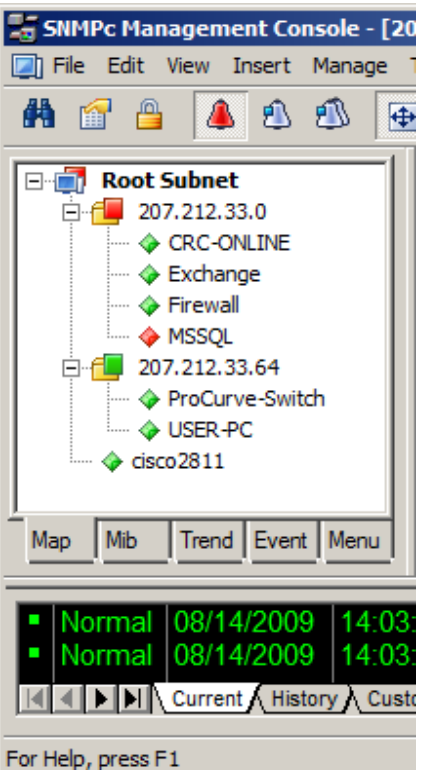
- A ***Minimized*** window is displayed as a small title bar with window open/close buttons. Windows are not typically minimized within the View Window Area because, as with the maximized case, they can easily be lost behind other windows.

Working with the Map Database

Using the Map Selection Tree

Locate the ***Selection Tool*** on the right side of the console. If you can't see the Selection Tool, use the ***View/Selection Tool*** menu to show it. Select the first tab marked ***Map***. The displayed Map Selection tree shows all icon objects in the map. This includes subnets (which contain lower map levels), devices, and goto icons. Networks and links are not shown in the map selection tree.

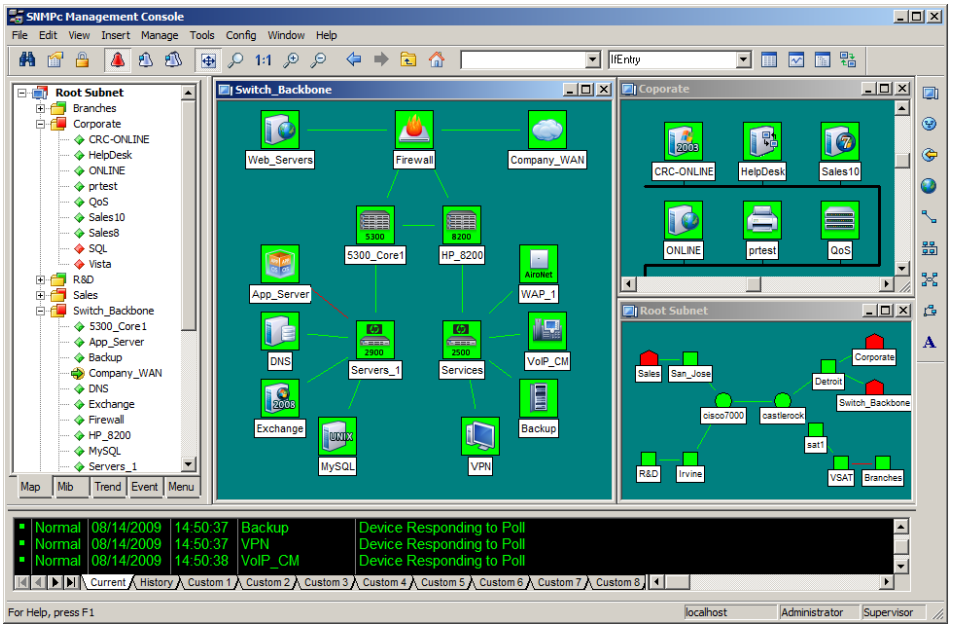
- ***Single-click*** on the small box to the left of a subnet icon (folder icon) to open or close that sublevel in the selection tree.
- ***Double-click*** on a subnet name (right of folder icon) to open that subnet level as a Map View window (see below).
- ***Left-click*** on any object name to select that object. Use the shift and ctrl keys to select multiple objects.
- Use the ***Delete*** key to remove selected objects.
- After opening two subnet levels, select multiple device names and ***drag the mouse*** to move them from one subnet to another. Note that any attached links and networks are not moved, and links will be deleted during the move (you can re-add them manually later).
- ***Right-click*** on a device icon (colored rectangle) or name to see the available ***Right-Click Menus***. Use these menus to edit the selected object properties, display tables, and run other custom menus.
- Open a subnet tree and use the ***Insert/Map Object*** menus or ***Edit Button Bar*** buttons to add icon objects to the subnet tree.



Each icon in the Map Selection Tree is colored according to the status of the represented object. Subnet icons (and the top level Root Subnet icon) show the highest priority color of all underlying objects.

Using Map View Windows

Map View windows are regular overlapping windows that are displayed in the View Window Area of SNMPc Enterprise. This is the main area where you can see the map topology as a diagram and easily manipulate the map objects (add, delete, move). Note that the View Window Area shows multiple windows and if the topmost window is maximized (takes up the entire area), any other windows will be hidden. Use the ***Windows/Cascade*** menu to show all windows within the View Window Area.



- Use the ***View/Map View/Root Submap*** menu to show the top level of the SNMPc Enterprise map.
- ***Double-Click*** on any subnet name in the Map Selection Tree or subnet icon in a map view to show a map view for that subnet.
- To easily move the map view, ***Left-Click*** anywhere on the view and ***drag the mouse*** to move the view contents. You can also use the ***scroll bars***, but this is not as easy.
- Use the ***Zoom Buttons*** to see more or less of the map view. Use the ***Pan/Zoom*** button to zoom into a selected rectangle (left click and drag the rectangle). Use the ***1:1*** button to set the normal zoom mode (icon and name visible). Use the ***Zoom +/-*** buttons to manually zoom. You can also zoom the map view using the ***mouse scroll wheel***.
- Use the ***View All*** button to toggle the ***View All*** state for a selected map view. In this state, the view contents are automatically zoomed so that all icons are visible. As you change the size of the view window, the contents will change size. As the icon sizes get smaller, the icon image is hidden and then the name is hidden. If your top-level map is large and the View All state is enabled (default) you may only see small icons. Use the manual Zoom buttons to zoom in to an area of the map view.
- Use the ***Previous View*** and ***Next View*** buttons to move back and forth between different zoom levels you have selected.

Moving Map Objects

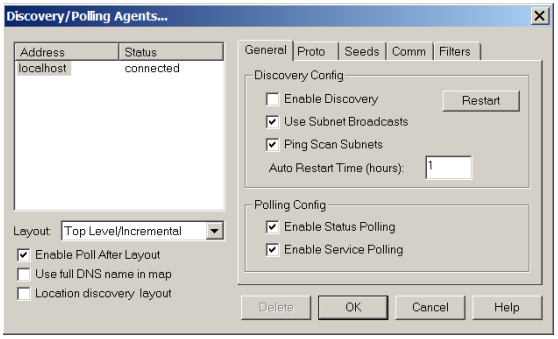
SNMPc Enterprise normally uses a discovery process to add subnets, devices, links, and networks in a logical topology that represents a two-level IP Subnet hierarchy. The top level includes all router devices and subnet icons. The second layer includes single-port devices linked to Bus Networks under the appropriate subnet icons. The top level map is automatically arranged as a star network.

Map objects are placed on the nearest **Map Grid Point** when you move them. Use the ***Config/Console Options*** menu and select the ***Show Grid*** check box to show map grid points. Set the grid size in the ***Grid Spacing*** edit box.

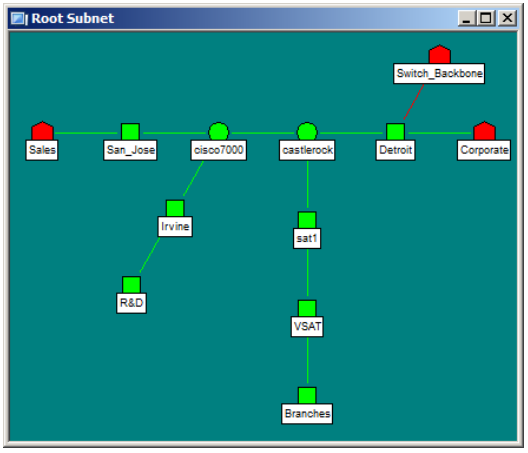
To Move Objects at the Root Level

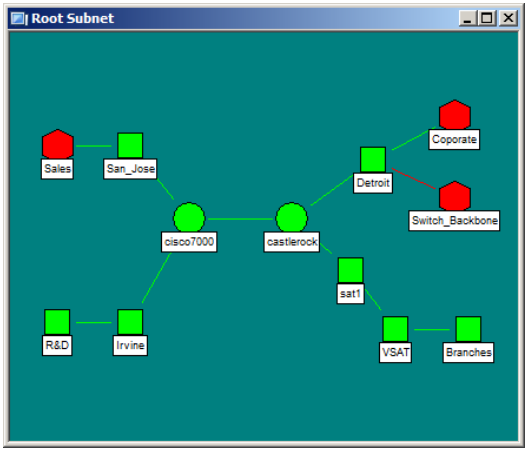
Since the discovery agent will continually arrange the top map level, before changing the root level manually you need to change the way discovery works. Use the ***Config/Discovery-Polling*** menu and then do ***one of the following:***

1. Uncheck the ***Enable Discovery*** checkbox so that discovery is completely disabled
2. Select ***Discovered Objects*** from the ***Layout*** pull-down so that any newly discovered objects are added to a separate subnet icon named Discovered Objects.
3. Select ***Top Level/Incremental*** from the ***Layout*** pull-down so that any newly discovered objects are added using an incremental layout algorithm that doesn't disturb the existing layout.



To move objects at the top level just select one or more objects in a map view and drag the mouse. The selected objects are moved to the new mouse location. The following two map views show an automatically (left) and manually (right) arranged Root Submap level:



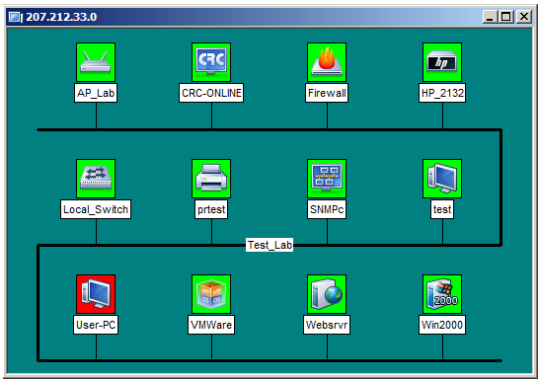


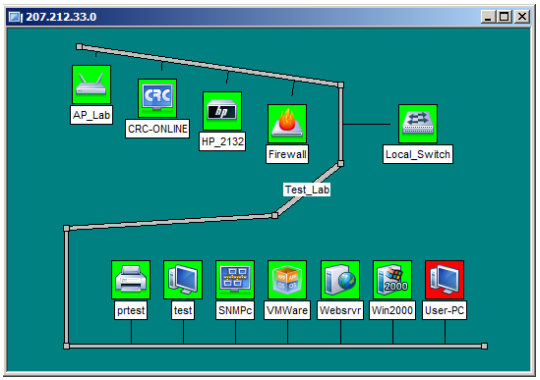
To Move Objects Inside Subnet Levels

Single port devices are added to the second map layer, below top-level subnet icons. Each subnet layer will also include a ***Bus Network*** that all devices are attached to. You can move devices around the Bus Network by selecting them and dragging them to the new position. However, the Bus Network is automatically arranged and the object will only be approximately placed where you dragged it.

If you need to positively rearrange the lower levels then it's best to change the network from a Bus to a regular ***Network***. This network will not be automatically arranged and you can move icons anywhere in the view, as well as change the network shape with the use of ***Junction Points***. You can click and drag any junction point or network segment, and add or remove junction points by double clicking on the network.

You can also disconnect objects from the Bus Network by deleting the attaching link. Then the detached object can be moved anywhere in the view. The following two map views show a subnet level that is automatically arranged (left) and manually arranged using a regular Network (right):





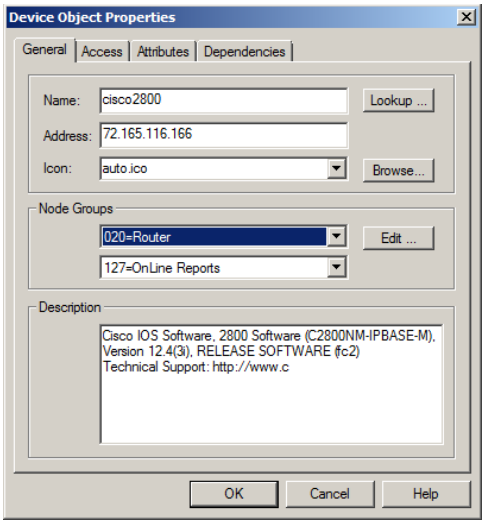
To Move Objects from One Subnet to Another

1. Use the ***Window/Close All*** menu to remove all view windows.
2. Open a map view for each of the source and target map subnets.
3. Use the ***Window/Tile Horizontal*** menu to make both windows fully visible.
4. Scroll and zoom the source map view so the objects you want to move are visible.
5. Scroll and zoom the target map view so the location where the objects will be placed is visible.
6. Select the objects (click on icon+drag or shift click on icons) in the source map view.
7. Drag the selected objects from the source to the target map view.

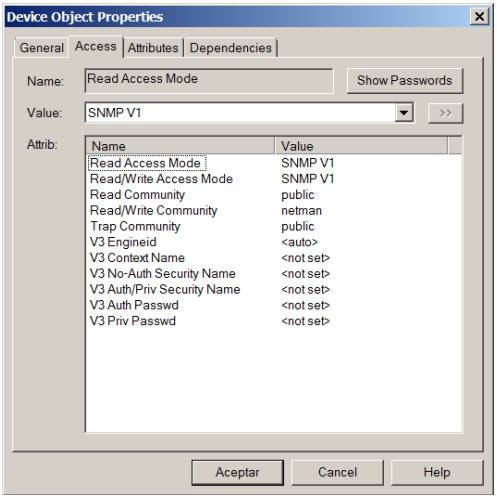
Note that any links will be deleted if you just move the attached objects. To move a network and all attached links and objects you must select all of the items. You can also use the ***Edit/Copy*** or ***Cut*** menus along with the ***Edit/Paste*** menu to move objects (or create copies) but these menus will not move link or network objects and the moved objects will not retain their relative positions.

Changing Object Properties

- Use the ***Edit/Properties*** menu to change the attributes of one or more selected objects. To edit multiple objects, all selected objects must be of the same type (subnet, device, etc.).
- Set the object name in the ***Name*** edit box.
- For Device objects, set the object IP Address in the ***Address*** edit box. This can be in dot format or a DNS name. You can also append a UDP port number to a dot-notation IP address (i.e., 198.22.11.22.***168***)
- For **Goto** objects, set the name of the subnet that the Goto jumps to in the ***Address*** edit box.
- Set alias names for groups of similar device objects in the ***Node Groups*** edit boxes.
- For icon type objects (Subnet, Device, Goto), set the icon in the ***Icon*** edit box. This is normally set to auto.ico so that an icon is selected automatically based on the device SNMP Object Identifier.



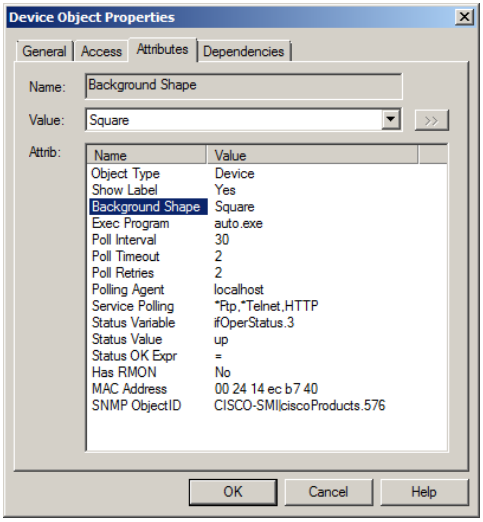
- Select the ***Access*** tab to set access parameters for a ***Device***, ***Link***, or ***Network*** object. For a description of access parameters, please see the table on the next page.
- To change an access parameter, first select the parameter name in the ***Attrib*** table. The selected parameter name is displayed in the ***Name*** box and the current value in the ***Value*** pull-down control.
- In the ***Value*** pull-down, select one of the pull-down values or type in a new value. Note that the Value pull-down does not necessarily show all possible values for the attribute.
- When editing multiple objects, any access parameter that has a different value for different objects is shown as *#####*. Changing these attributes will set the new value for all selected objects.



The following table describes the access parameters available in the ***Object Properties Access*** tab for ***Device***, ***Link***, and ***Network*** objects. Access parameters are not valid for Subnet and Goto object types.

ATTRIBUTE NAME	DESCRIPTION
Read Access Mode	The mode used for polling and SNMP Read operations. Select *ICMP (Ping)* for non-snmp devices. Select *SNMP V1* for standard SNMP devices. Select *NONE (TCP Only)* for devices that will only have TCP services polled.
Read/Write Access Mode	The mode used for SNMP Write operations. Select SNMP V1 for standard SNMP devices. You can also force this mode to be used for both Read and Write operations from your console (not polling operations) by using the Read/Write button on the SNMPc Enterprise frame button bar (3rd button from left).
Read Community	The Community name used for SNMP V1/V2c operations when the Read Access Mode is used.
Read/Write Community	The Community name used for SNMP V1/V2c operations when the Read/Write Access Mode is used.
Trap Community	The Community name expected in a received SNMP V1/V2c Trap frame. This is used to match an incoming trap to a map object.
V3 Engineid	SNMP V3 Engine Identifier (detected automatically).
V3 Context Name	SNMP V3 Context Name (normally blank).
V3 No Auth Security Name	SNMP V3 Security Name to use with the noAuth access mode (no authentication, no privacy).
V3 Auth/Priv Security Name	SNMP V3 Security Name to use with authenticated or private (encrypted) access modes.
V3 Auth Password	SNMP V3 password to use for authentication.
V3 Priv Password	SNMP V3 password to use for privacy (encryption).

- Select the ***Attributes*** tab to set type-dependent attributes. For a complete description of all type-dependent object attributes, please see the table on the next page.
- To change an attribute, first select the attribute name in the ***Attrib*** table. The selected attribute name is displayed in the ***Name*** box and the current value in the ***Value*** pull-down control.
- In the ***Value*** pull-down, select one of the pull-down values or type in a new value. Note that the Value pull-down does not necessarily show all possible values for the attribute. Use the >> button to show an expanded selection mechanism for the selected attribute value.
- When editing multiple objects, any attribute that has a different value for different objects is shown as *#####*. Changing these attributes will set the new value for all selected objects.



The following table lists each available attribute in the ***Object Properties Attributes*** tab, the object types it is valid for, and a description of the attribute.

OBJECT [1]	ATTRIBUTE NAME	DESCRIPTION
D,L,N,S,G	Show Label	Show or hide the object name.
S, G, D	Background Shape	Icon background, one of Square, Circle, Hexagon, Octagon, or Diamond.
S	Bitmap	Background bitmap image.
S	Bitmap Scale	Background bitmap image scaling factor (bigger number expands).
Sg	Map Server	Geographic Map Service profile name.
L	Show Link Name	Link names normally hidden.
D	Exec Program	Double-click program for devices. Include any of the following special program arguments: $a – IP Address, $n –` node name, $g – Read Community; $s – Set community, $w – console window number.
D, L, N	Poll Interval	Seconds between poll sequences.
D, L, N	Poll Timeout	Seconds to wait for a response after a poll is sent.
D, L, N	Poll Retries	Number of times to retry a failed poll during a single poll sequence.
D, L, N	Polling Agent	IP Address of the Polling Agent system that performs regular and trend statistics polling for this object. Unless you are using Remote Polling Agents, this is set to *localhost*.
D, L, N	Service Polling	List of services to poll (TCP or custom service polling)
D, L, N	Status Variable	An SNMP variable with instance that is polled to determine device status (as opposed to just polling for device response). For example, ifOperStatus.3.
D, L, N	Status Value	The number to be compared to the returned Status Variable value.
D, L, N	Status OK Expr	The expression to use when comparing the Status Value to the returned Status Variable to determine if the status is OK (<, >, <=, >=, =, !=).
D, L, N	HasRMON	Set to TRUE to enable the RMON tool.
D, L	MAC Address	Primary device MAC address or link MAC address, if known.
D, L, N	SNMP ObjectID	Read-Only. The System Object Identifier of an SNMP object.

Note 1: D = Device, L = Link, N = Ring, Bus, Network, S = Subnet, Sg = Geo Subnet, G = Goto

Adding Map Objects

SNMPc Enterprise supports several object types, including subnets, devices, links, and networks. To add objects, first open a map view window and then use one of the ***Insert/Map Object*** menus or the *Edit Button Bar* buttons. After adding icon objects, you need to move them to the desired location. If you can't see the new object, use the ***View All*** button. The following table describes the different object types:

TYPE	DESCRIPTION
Device	A Device icon represents a polled device, including SNMP and Ping polled devices. • When adding a device object, you need to set the device Address in the displayed Properties dialog box. You can append an optional UDP port to the address as x.x.x.Port. • Then select the Access tab and set the Read Access Mode and Read/Write Access Mode parameters. Use *ICMP (Ping)* for non-SNMP devices (or *NONE* where you only want to poll TCP services), and use *SNMP V1* for regular SNMP devices. For SNMP V1 devices, you must also set the Read Community and Read/Write Community parameters to valid community names. • Finally, select the Attributes tab and set appropriate values for the Poll Interval, Poll Timeout, and Poll Retries attributes.
Subnet	A Subnet icon contains other map layers, possibly including other subnets. • Double-click on a subnet icon to open a view window for the next layer down. • Use the Parent Window button to go up one layer to the parent subnet view. Use the Root Subnet button to open the top map level view.
Geo Subnet	A Geo Subnet icon is the same as a Subnet icon but displays a geographic map background dynamically imported from an external map service.
Goto	A Goto object is like a subnet in that you can double-click on it to open a new map view window. However, a Goto object displays the map subnet that is named in the Address field. To make a Goto that opens the Root Submap, leave the Address field blank.
Link	A link object is a line between two icon objects (subnet, device, goto). Link objects can be polled so you can optionally set an IP Address and Access/Polling attributes as with the Device Object. However, by default link the Poll Interval for links is set to zero so it is not polled. To add one or more link objects, first select two or more device objects and optionally a single subnet or network object, then press the Add Link button from the Edit Button Bar.
Network	There are several types of Network objects which have different layout styles. • A Bus Network automatically arranges the network and attached links/icons in a bus configuration. • A Ring Network automatically arranges the attached objects in a ring. • A regular Network object can be manually shaped. Double-click on a Regular Network object to create a junction point. Double-click on an existing junction point to remove it. Click on a junction object or network segment and drag it to move it in the map view. • Network objects can also be polled but the Poll Interval is set to zero (non-polled) by default. Use one of the Add Network buttons from the Edit Button Bar to add a network. If you first select several icon objects, SNMPc Enterprise will also add links between the icons and the new network.
Text	A static text box.

Using Geographic Subnet Map Views

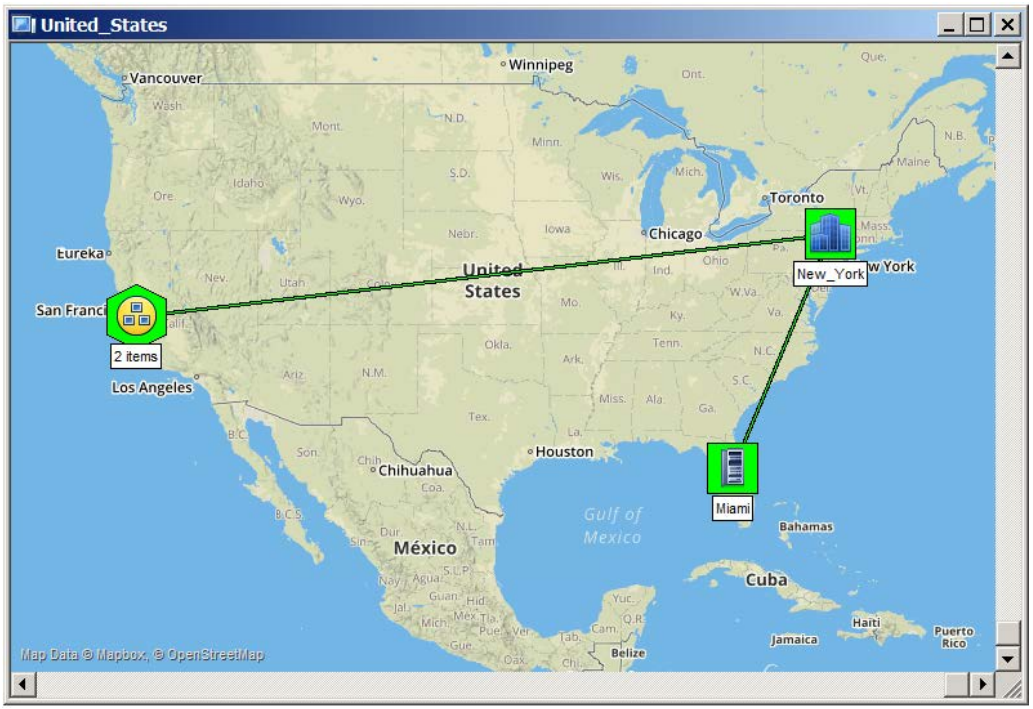
A Geographic Subnet object is the same as a Subnet Object but uses an external ***Web Map Service (WMS)*** to dynamically display a geographic map view instead of a static bitmap background.

Use the ***Insert/Map Objects/Geo Subnet*** menu to add a new Geo Subnet object to a map view.

The default Map Server is set to ***CastleRockStreet***, which provides street style maps using the *map.castlerock.com* WMS provider. Note that access to *map.castlerock.com* map data is restricted to users with a current *Software Updates* license. If your software license is older than three months please configure your *Software Update*s license key using the ***Config/Software Keys*** menu.

To change to a different map service or style right click on the Geo Subnet icon or on the background within the Geo Subnet icon and use the ***Edit/Object Properties*** menu. Select the ***Attributes*** tab and then select a different style from the ***Map Server*** attribute.

The following shows a sample Geo Subnet map view:

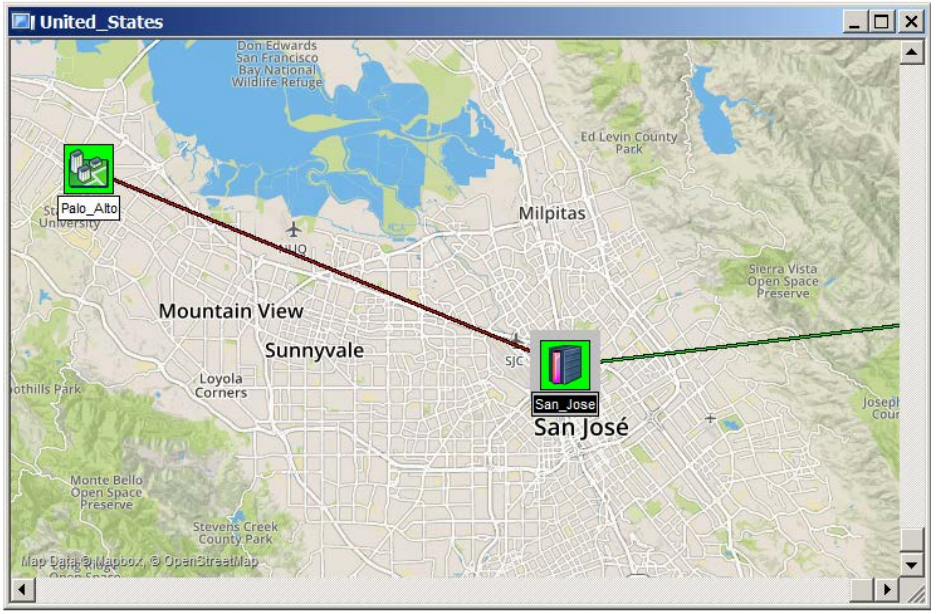


As you zoom out of a Geo Subnet view, when multiple objects get too close together they are merged into a single Group icon. Click on any group icon to zoom into a view that shows the topmost separated set of objects (which may contain other object groups).

Use the ***left mouse button*** to pan (drag) a Geo Subnet map view.

Use the ***mouse scroll wheel*** to zoom in or out of a Geo Subnet map view.

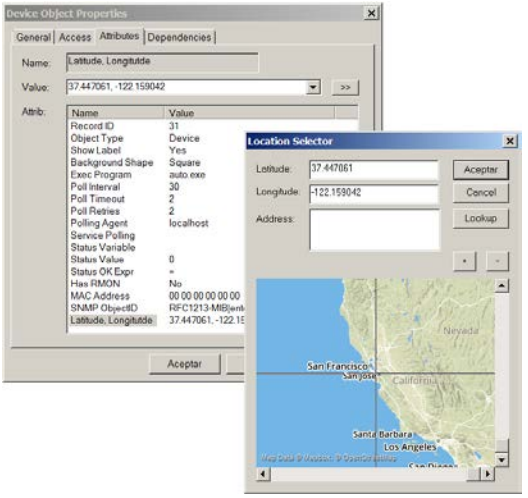
The following shows the previous sample Geo Subnet map view after clicking on the group icon at San Francisco:



Use the ***Latitude, Longitude*** attribute of the ***Object Properties*** dialog to move any device object within a Geo Subnet map view to a specific GPS or street address location.

Use the ***Browse (>>)*** button to show the ***Location Selector*** dialog box then enter a new ***Latitude, Longitude*** coordinates or a street address in the supplied edit boxes.

You can only use a street address when your selected Geo Subnet Map Server supports address lookups (also known as Geocode requests).



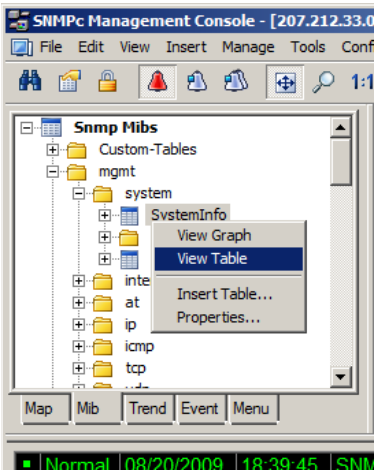
Objects on Geo Subnet map views are always fixed size. To change the size use the ***Config/Console Options*** menu and select a different size from the ***Geo Icon Size*** pulldown.

For information about customizing the Geo Subnet map servers used by SNMPc please refer to the *Geomaps.doc* MS Word document in the SNMPc ***SDK/DOCS*** Windows subdirectory.

Viewing Device Mib Data

Using the Mib Selection Tree

- First select one or more SNMP device objects.
- Locate the Selection Tool at the left of the console window. If you can't see it, use the ***View/Selection Tool*** menu to show it. Press the ***Mib*** tab to activate the MIB Selection Tree. This tree shows all compiled standard and private Mibs.
- Open the ***Mgmt*** subtree to show standard Mib elements. Open the ***Private*** subtree to show vendor-specific Mib elements. Note that each device supports a subset of the standard and private Mibs. It's up to you to determine if a device supports a particular Mib table.
- Open subtree elements until you see one or more table grid icons listed. These are the Mib table definitions that you will be mostly working with.
- Right-Click on one of the table names and use the ***View Table*** or ***View Graph*** menus to display the contents of the table for the selected devices as a form or graph.



Using Manage Menus

Select one or more SNMP devices objects and use the ***Manage*** or ***Right-Click*** menus to display common SNMP MIB tables in several formats. Note that not all devices implement all tables in these menus so in some cases the menus will fail to show a result. It's up to you to determine if the table specified in the menu is supported.

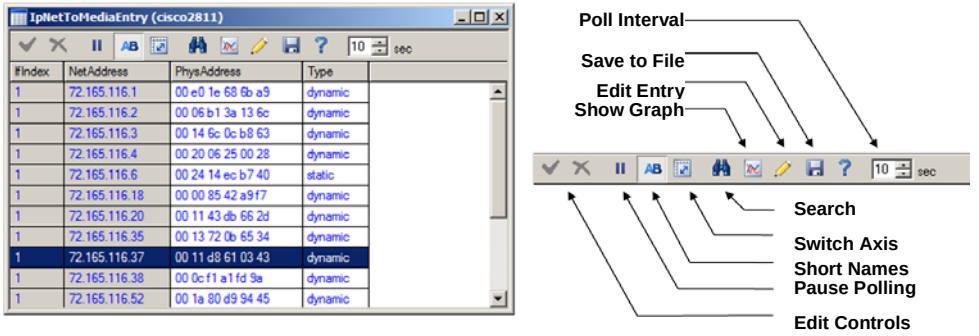
- Use the ***List*** <***tablename***> menus to display a single entry table.
- Use the ***Edit*** <***tablename***> menus to show an edit dialog for a single entry table.
- Use the ***Display*** <***tablename***> menus to display a multi-entry table.
- Use the ***Graph*** <***tablename***> menus to display a graph for all instances in the table. You can also start a graph after selecting some elements in a displayed table.

Using Custom Menus

Manage menus are actually built-in custom menus from an external configuration file. You can also add custom menus to display particular tables. For example, if you have only a few device types in your network you probably should add custom menus to display the vendor specific tables for those devices. You can then display Mib information using the Right-Click menus instead of searching for Mib tables in the Mib Selection Tree. For more information about custom menus, select the ***Menu*** tab of the ***Selection Tool*** and press the ***F1 key***.

Table Display Elements

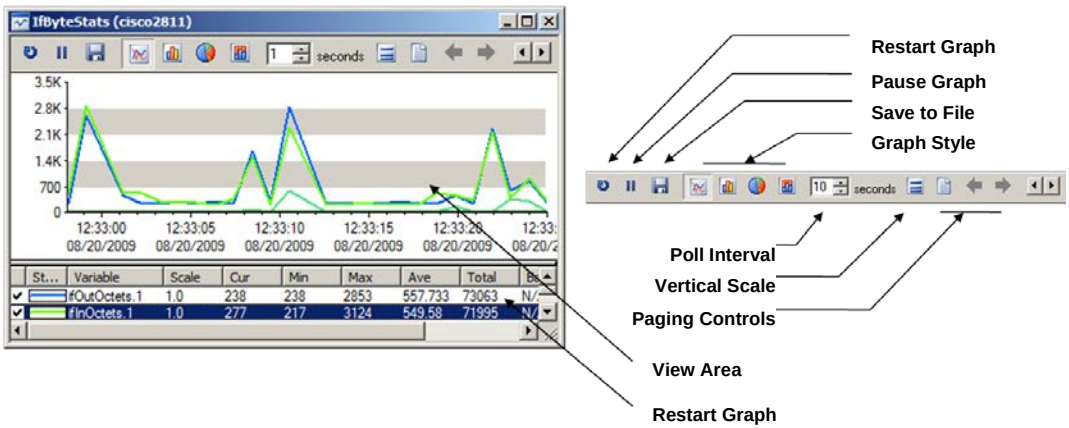
The following diagram shows a sample table display and describes the function of table controls.



- To start a graph display, first select one or more cells (rows, columns, or individual cells), then use the ***Show Graph*** button.
- To change a table cell and do a ***Set Operation*** to the device, first locate settable cells (those displayed in blue). ***Double-click*** the cell to move into the *Edit Mode*. Enter the new value directly into the cell (or select from the pull-down if it is displayed). Then press the ***Check Edit Control*** button. To cancel a Set operation in progress, press the ***Cross Edit Control*** button.

Graph Display Elements

The following diagram shows a sample graph display and the function of graph controls.



Graph Styles

The following diagram shows sample displays of the four graph styles: ***Line***, ***Bar***, ***Distribution***, and ***Pie***. Note that the Bar and Pie show Average values.

Graph Paging Controls

The graph is difficult to view with many variables at the same time. Use the ***Page Controls*** to enable blocks of variables. Use the ***Paginate*** button (paper sheet icon) to enable all variables or just the first page (8 variables). Use the ***Prev Page*** and ***Next Page*** buttons to enable the previous or next page of variables.

Graph Legend Control

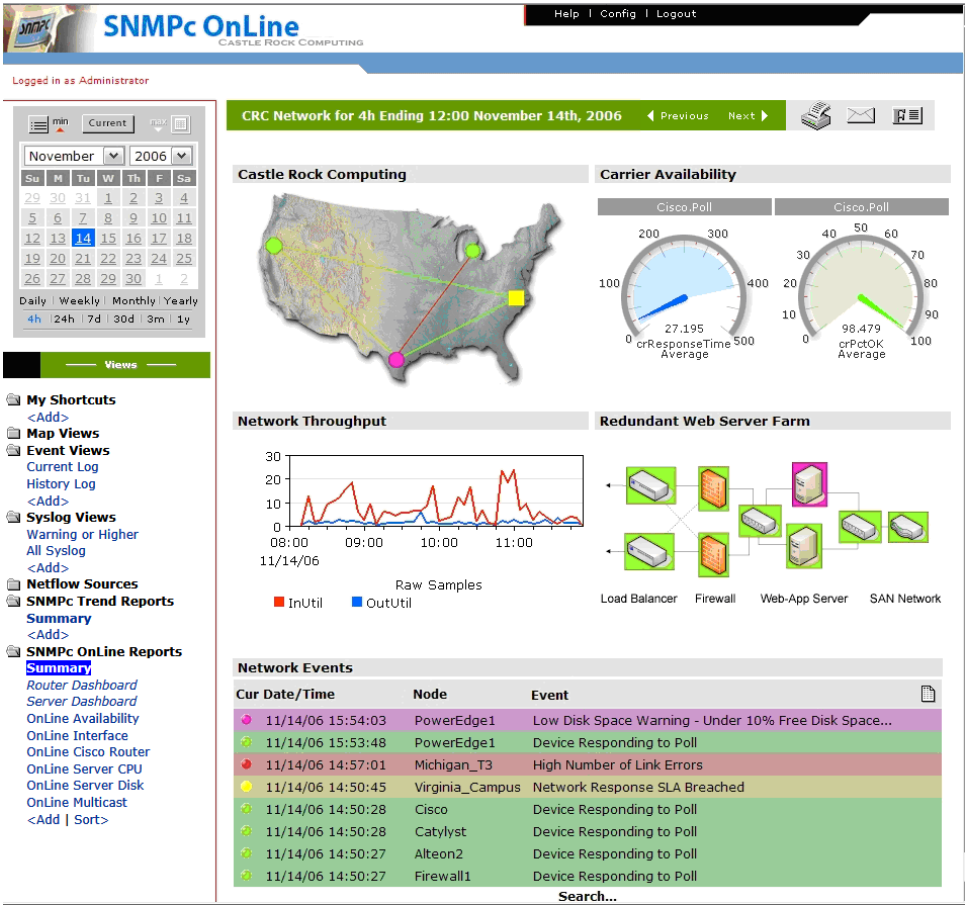
The Legend Control displays all variable names and a data summary, including the Current, Minimum, Maximum, and Average values.

- Drag the bar at the top of the Legend Control to make the control bigger or smaller.
- ***Double-click*** the check mark at the left to enable or disable of a variable.
- Use the ***Right-Click Properties*** menu to set line properties and scaling for a variable.
- ***Double-Click*** on the Graph View area to show or hide the Legend Control.

Saving Long Term Statistics

SNMPc Enterprise Trend Reports save long term statistics for any SNMP table and also Service Polling pseudo-tables. Each report saves data for one table and up to ten devices. You can set manual threshold alarms for any variable instance to generate an event when a variable reaches a specific value. Data is saved in a private format database at one or more polling agent systems. Data can be downloaded and viewed in a regular graph window for a specified date period.

SNMPc Enterprise Trend Report data is automatically exported to an SQL database and viewed from a web browser by the separate SNMPc OnLine module. The following diagram shows a sample SNMPc OnLine web based view.

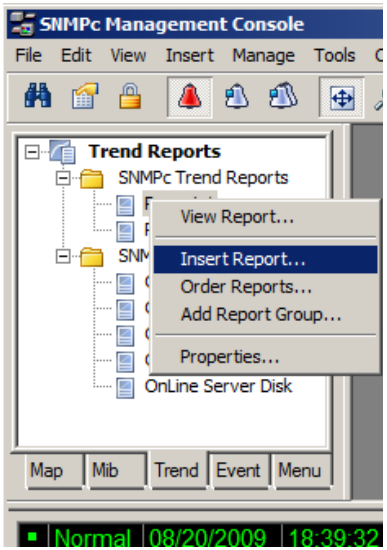


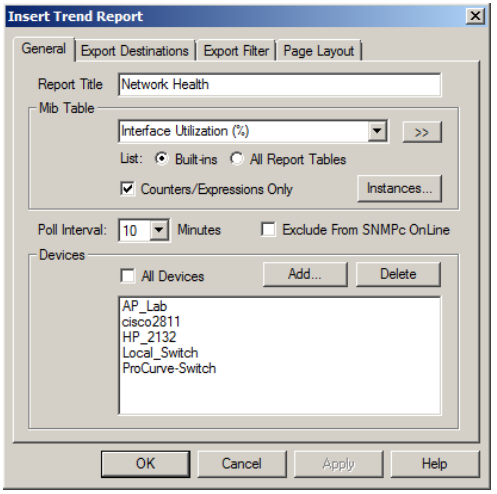
Please refer to the SNMPc OnLine Getting Started Guide for instructions on configuration and web based viewing of SQL exported trend report data.

The remainder of this section describes how to configure trend report creation, polling and alert generation within SNMPc Enterprise.

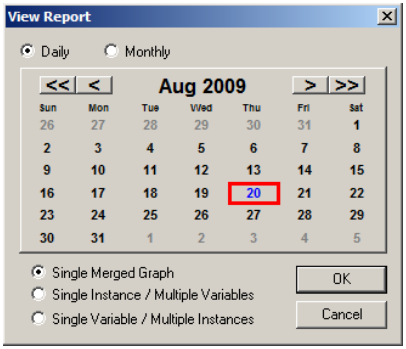
To Create A New Report

- First select one or more device objects using the ***Map Selection Tree*** or a ***Map View*** window.
- Locate the ***Selection Tool*** at the left of the console. If you can't see the Selection Tool, use the ***View/Selection Tool*** menu to show it.
- Select the ***Trend*** tab and open the ***Trend Reports*** group name.
- Use the Right-Click ***Insert Report*** menu to add a new report.
- Enter a name for the new report.
- Select one of the built-in table names from the ***Mib Table*** pull-down. You can also press the >> button to select any standard or private Mib table.
- For initial test purposes, set the ***Poll Interval*** to 1 minute. We recommend that you use a 10 minute poll interval if you have several reports.
- Press OK to save the report using standard settings.





Viewing Trend Data in a Graph Window

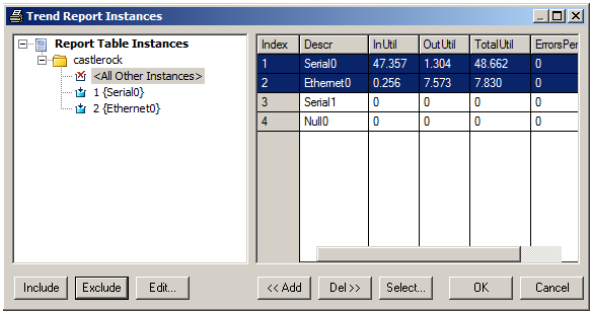


- Assuming you set a 1 minute poll interval, wait about 10 minutes to save some data.
- Right-click on the new report name in the Trend Report Selection Tree and use the ***Properties*** menu.
- Use the ***View Report*** menu.
- Select the current day and *Single Merged Graph* to see all data on one graph.
- Press OK. Some progress dialogs will be displayed and then the report data will be displayed in a regular SNMPc Enterprise graph window.

Irrespective of the report poll interval, all ***Counter*** variables shown in a trend report graph window are normalized to per-second values.

Limiting Saved Instances

The polling agent normally polls all available instances for each variable in a trend report table. To limit polled instances, select the report name in the ***Trend Selection Tree*** and use the Right-Click ***Properties*** menu, then use the ***Instances*** button.



- Select one or more rows in the displayed table and press the ***Add*** button to add them to the ***Instances Tree*** at left.
- In the Instances Tree, select one or more labels (including *<All Other Instances>*) and press the ***Include*** or ***Exclude*** button.
- For each included instance, use the ***Edit*** button to set textual instance names and manual threshold alarms

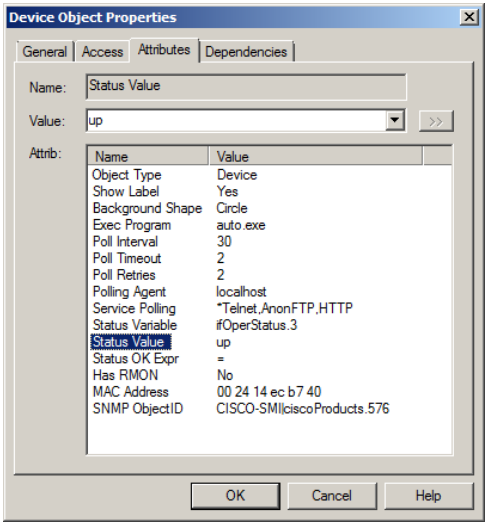
Setting Threshold Alarms

You can generate a Threshold Alarm when a polled SNMP variable value meets certain criteria. SNMPc Enterprise supports three distinct mechanisms for generating Threshold Alarms as described in the following table.

ALARM TYPE	DESCRIPTION
Status Variable Polling	Use the Object Properties dialog to set a single SNMP variable plus instance that is polled in real time (Poll Interval attribute seconds). Use this for Emergency Status Polling. For example, poll for UPS battery failure, disk full, or link down conditions.
Automatic Trend Baseline	SNMPc Enterprise automatically determines a baseline value for all variables in any trend reports that you add. The baseline is set after a learning period and periodically adjusted. The polling agent will generate alarms if a polled value exceeds the baseline by a preset percentage.
Manual Trend Threshold	Use manual threshold alarms in trend reports to specify a particular condition to test. This is commonly used to monitor line utilization variables. In this case the alarm condition is well known to the user and involves a longer polling period (e.g., 80% over 10 minutes).

Setting Status Variable Polling

- Using the *Map Selection Tree* or a *Map View Window*, ***Right-Click*** on an SNMP Device, Link, or Network object and use the ***Properties*** menu.
- Make sure the ***Address*** field is set to a valid IP address. You can optionally append a UDP port number to the address as x.x.x.x.*Port.*
- Select the ***Access*** tab.
- For a regular SNMP V1 device, set ***Read Access Mode*** to ***SNMP V1*** and set ***Read Community*** to a valid community name.
- Select the ***Attributes*** tab.
- Set ***Poll Interval*** to the number of seconds between successive polls.
- Set ***Status Variable*** to the name of an Integer SNMP variable including an instance (e.g., ifOperStatus.3). Make sure you enter a full variable instance.
- Set ***Status Value*** to the Numeric value for your comparison (or one of the pull-down aliases).
- Set ***Status OK Expr*** to the test performed to determine if the status test passes. Use the ***Value*** pull-down list for possible tests.



Note: For variables that have a textual instance part, you can use the form ***statusVar."text instance"*** rather than full SNMP dot notation.

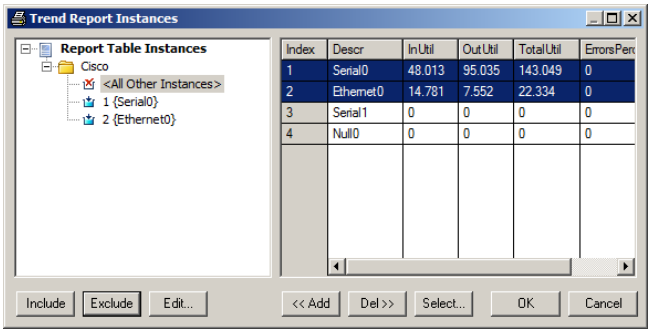
Configuring Automatic Alarms

Use the ***Config/Trend Reports*** menu and select the ***Automatic Alarms*** tab. You can set various parameters of the automatic alarm algorithm in this dialog. Generally the default settings are adequate and the main thing you might want to do is disable automatic alarms by unchecking the ***Enable Automatic Alarms*** checkbox.

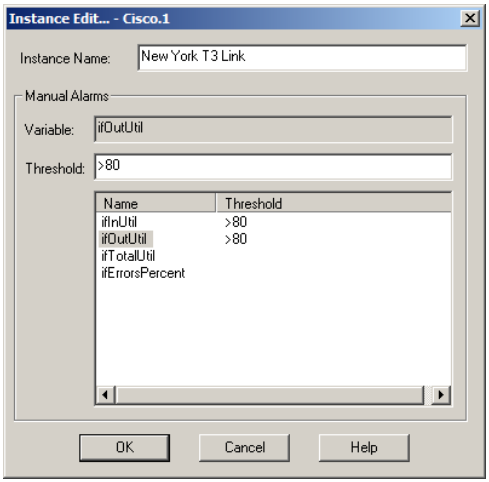
Setting Manual Threshold Alarms

You must first create a trend report for a set of devices and an SNMP Mib Table. Please refer to the earlier section, ***Saving Long Term Statistics*** for a description of creating trend reports.

Select the report name in the ***Trend Selection Tree*** and use the Right-Click ***Properties*** menu, then use the ***Instances*** button.



- Select one or more rows in the displayed table and press the ***Add*** button to add them to the ***Instances Tree*** at left.
- In the Instances Tree, select one or more labels (including *<All Other Instances>*) and press the ***Include*** or ***Exclude*** button.
- For each included instance, use the ***Edit*** button to alarms for each variable



- Select a variable name from the list at the bottom of the Instance Edit dialog.
- Enter a simple expression at the ***Threshold*** edit box. This is an operator (>, <, =, >=, <=, !=) and a numeric constant.
- You can also optionally enter a name for this variable instance in the ***Instance Name*** edit box. This makes it easier to determine what the threshold alarm refers to.
- Press OK. You will see a red exclamation mark next to the icon in the Instances Tree for any instances that have manual alarms.

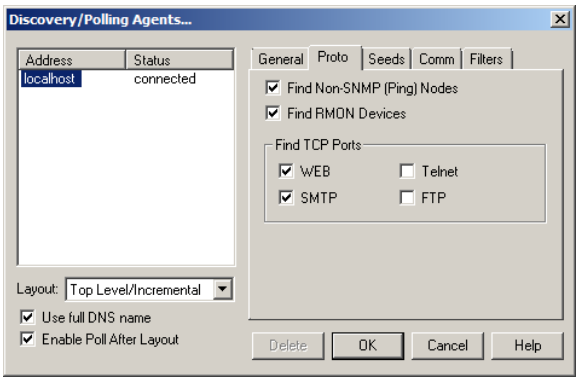
Please keep in mind that for ***Counter*** variables, the values you set in the manual threshold will be compared against a polled sample. The polled sample will be larger or smaller depending on the trend report poll interval. For example, a link that shows 100K bytes in one minute might show 1000K bytes in 10 minutes. This is different than what you see in trend graph, in which the samples are normalized to per-second values.

Polling Application Services

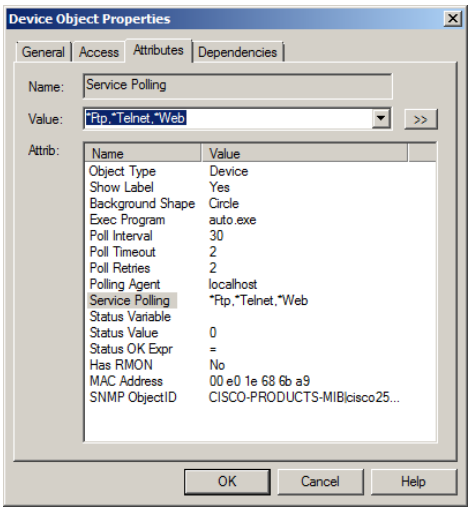
SNMPc Enterprise supports customized polling of any TCP application service, simplified polling of four built-in TCP application services (FTP, SMTP, WEB, and TELNET), and external polling of non-TCP services by custom applications. This section describes how to poll TCP services. For more information about external program polling, please use the ***Help/Help Topics*** menu, open the ***Customizing SNMPc*** link and then open the ***Developing Service Polling Applications*** link.

SNMPc Enterprise polling agents can automatically check for the existence of the built-in TCP services on discovered devices and configures these services to be polled.

Use the ***Proto*** tab of the ***Config/Discovery-Polling*** dialog to enable discovery of the four built-in TCP services.



To enable service polling for a device, right-click the device object in a map view and use the ***Properties*** menu then select the ***Attributes*** tab. Select the ***Service Polling*** attribute.



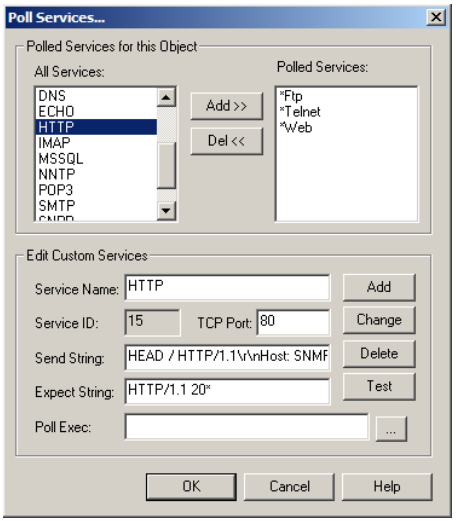
- Use the ***Value*** pulldown list to select one of the available services (*Ftp, *Telnet, *Smtp, *Web and custom names).
- To select multiple services for the device, type in the service names in the ***Value*** edit box, separated by commas. For example: "*Ftp,*Web".
- Alternatively, double-click the ***Service Polling*** attribute, or use the **">>"** button, to select multiple services.

Custom Service definitions allow more flexible and powerful polling of your application servers:

- You can optionally send a text string to a TCP service and compare the reply to a text pattern.
- Each map object can poll up to 16 different Custom Services.
- There is no limit on the total number of Custom Service definitions that can be created.
- You can optionally run an external custom application to poll the service.

Double-click the ***Service Polling*** attribute, or use the **">>"** button, to edit Custom service definitions. The ***Poll Services*** dialog is displayed.

Use the controls in the upper ***Polled Services for this Object*** section to manage polling for the selected device.



To enable polling of a service for the device:

- Select the service name in the ***All Services*** list.
- Press the ***Add***>> button

To disable polling of a service for the device:

- Select the service name in the ***Polled Services*** list.
- Press the ***Del***<< button.

Use the controls in the lower ***Edit Custom Services*** section to add, delete and change Custom Service definitions.

To add a new TCP Custom Service definition:

- Enter a new name in the ***Service Name*** edit box.
- Enter a TCP port number for a TCP service in the ***TCP Port*** edit box.
- Optionally enter a short string to transmit to a TCP service in the ***Send String*** edit box.
- Optionally enter a pattern string to match against a TCP service response in the ***Expect String*** edit box. You may use ASCII text and asterisk wildcards ('*').
- Press the ***Add*** button.

After adding a new service definition, you need to press the ***Add***>> button if you want this service to be polled for the currently selected device.

To delete an existing Custom Service definition:

- Select the service name in the ***All Services*** list.
- Press the ***Delete*** button.

To modify an existing Custom Service definition:

- Select the service name in the ***All Services*** list.
- Make changes to the ***Service Name***, ***TCP Port***, ***Send String***, ***Expect String***, or ***Poll Exec*** fields.
- Press the ***Change*** button.

Note that service names prepended by an asterisk are built-in and cannot be changed or deleted. These services are *Ftp, *Telnet, *Smtp, and *Web. These services use a simplified connect-only form of polling.

Emailing or Paging the Administrator on an Event

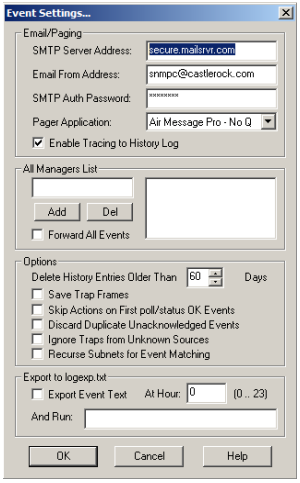
This section shows you how to dial a pager or send email to the SNMPc Enterprise Administrator user when a selection of devices goes down.

Step 1: Add the Administrator user to Air Messenger Pro

To use paging you must first install Air Messenger Pro by using the Windows ***Start/Programs/SNMPc Network Manager/Install Air Messenger Pro*** menu. Start Air Messenger Pro and add a user (not a group) named Administrator. Configure and test the Air Messenger Pro modem/pager settings and make sure you can send pages.

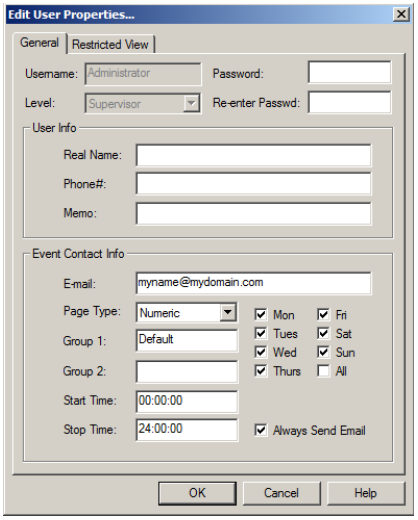
Step 2: Set the Email/Paging global event options

- Use the ***Config/Event Options*** menu.
- Set the ***SMTP Server Address*** to the IP Address of your email server in dot notation (a.b.c.d).
- Set the ***Email From Address*** to an email address that is valid at your server (e.g., SNMPc Enterprise@castlerock.com).
- Select the ***Pager Application*** (Air Messenger Pro or Notify!Connect).
- Enable the ***Enable Tracing to History Log*** checkbox. Later, when you have verified that email works you can disable this option.



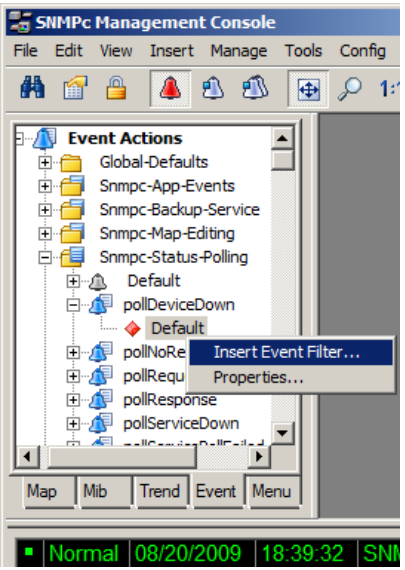
Step 3: Set the Administrator Contact Info

- Use the ***Config/User Profiles*** menu.
- Select the ***Administrator*** user and press ***Modify***.
- Set your email address in the ***E-mail*** edit box.
- Select the ***Pager Type*** (numeric or alphanumeric).
- Set the days and times you want to be emailed and paged.
- You can use the ***Group1*** and ***Group2*** edit boxes to set two alias names for multiple users. For now, leave ***Group1*** set to Default.



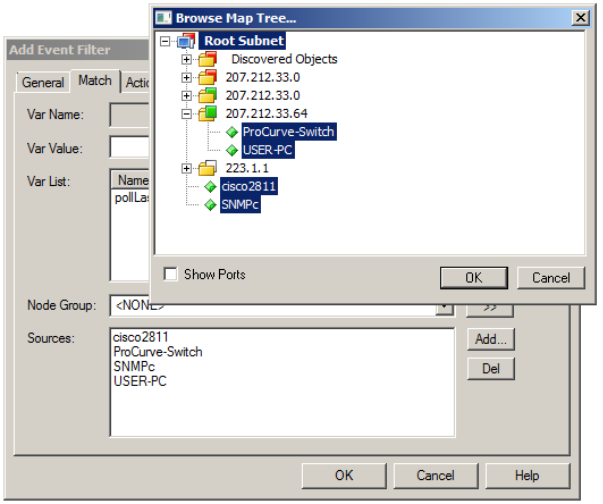
Step 4: Add an Event Filter for the pollDeviceDown event

- Locate the SNMPc Enterprise ***Selection Tool*** at the left side of the console. If it isn't there, use the ***View/Selection Tool*** to show it.
- Select the ***Event*** tab on the Selection Tool.
- Open the ***SNMPc-Status-Polling*** subtree, which contains all polling related event actions.
- Open the ***pollDeviceDown*** subtree, which contains all event filters for the Device Down event.
- Right-click on the ***Default*** event filter and use the ***Insert Event Filter*** menu to add a new event filter.
- The ***Add Event Filter*** dialog will be displayed. Enter an ***Event Name*** for the new event filter at the ***General*** tab. For example, set the name to *Primary Router Down*.



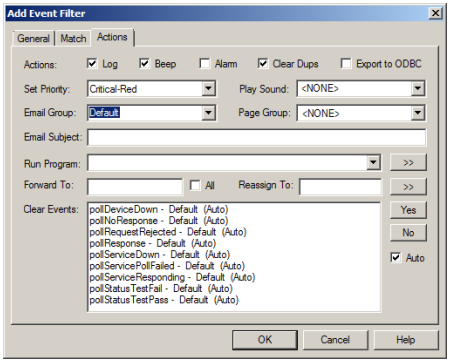
Step 5: Select the devices to match the Event Filter

- Select the ***Match*** tab of the displayed Add Event Filter dialog.
- Press the ***Add*** button.
- Use the tree control to select one or more device names and press OK.
- The matching device names are displayed in the ***Sources*** list box.



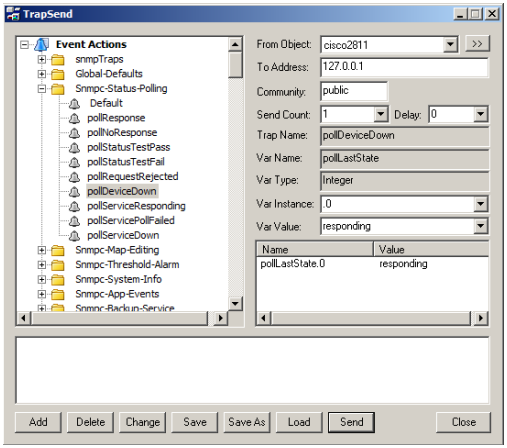
Step 6: Set the Email/Page event actions

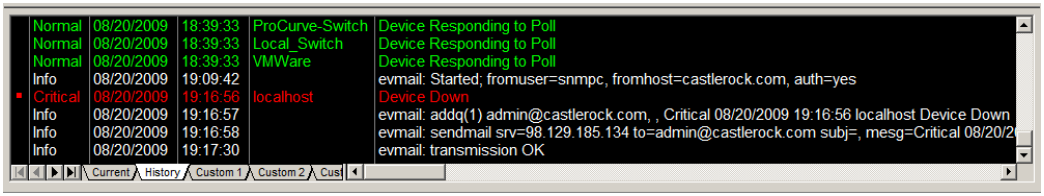
- Select the ***Actions*** tab of the displayed ***Add Event Filter*** dialog.
- Select ***Default*** from the ***Page Group*** pull-down to send a page to all users with a *Group1* or *Group2* alias set to *Default* (i.e., the Administrator user).
- Select ***Default*** from the ***Email Group*** pulldown to send email to all users with a *Group1* or *Group2* alias set to *Default* (i.e., the Administrator user).
- Press OK to save the new filter.



Step 8: Test the new Event Filter

- Select the ***Map*** tab of the ***Selection Tool*** and select one of the devices you matched in the ne event filter.
- Use the ***Tools/Trap Sender*** menu.
- The ***TrapSend*** tool shows an Event Actions tre on the left side. Open the ***SNMPc-Status-Polling*** subtree and select the ***pollDeviceDown*** event.
- Press the **Send** button.
- Close the TrapSend tool and look at the SNMP Enterprise ***Event Log Tool*** (at the lower part of the console). If you can't see the Event Log Tool, use the ***View/Event Log Tool*** menu to show it.
- Select the ***History*** tab in the ***Event Log Tool***. You will see a red Device Down event for the selected node and some white diagnostic messages about the Email operation.





Using Other Event Types

We have used the ***pollDeviceDown*** event as an example for this section. The mechanism is the same for other types of events, including those generated for ***Status Variable*** and ***Manual Threshold Alarms***. The following table shows common SNMPc Enterprise events and when they occur.

EVENT SUBTREE	TRAP NAME	DESCRIPTION
SNMPc-Status-Polling	pollDeviceDown	Device has not responded for three consecutive poll sequences[1].
	pollNoResponse	Device failed to respond to one poll sequence[1].
	pollRequestRejected	Device rejected the sysObjectId.0 or the user-set status polling variable.
	pollResponse	Device responded to a poll sequence[1].
	pollServiceDown	Could not connect to the TCP port after three consecutive attempts.
	pollServiceNoResponse	Could not connect to the TCP port after one attempt.
	pollServiceResponding	Connection to TCP port OK.
	pollStatusTestFail	Status variable test failed.
	pollStatusTestPass	Status variable test passed.
SNMPc-System-Info	pollAgentConnect	SNMPc polling agent connection to server established.
	pollAgentDisconnect	SNMPc polling agent connection to server lost.
SNMPc-Threshold-Alarm	alarmAutoThresholdExpand	Trend auto-baseline moved higher.
	alarmAutoThresholdReduce	Trend auto-baseline moved lower.
	alarmAutoThresholdSet	Trend auto-baseline initially set.
	alarmAutoThresholdTrigger	Trend auto-baseline exceeded,
	alarmManualThresholdTrigger	Trend manual alarm passed threshold.
	alarmManualThresholdReset	After being triggered, a trend manual alarm no longer passes the threshold test.
snmp-Traps	authenticationFailure	Trap generated by a device on an illegal access (bad community name).
	coldStart	Trap generated by a device after it restarts.
	linkDown	Trap generated by a device when a link fails.
	linkUp	Trap generated by a device when a link that was down recovers.

Note 1: A *poll sequence* occurs repeatedly every ***Poll Interval*** seconds. During each poll sequence, a poll is sent and a reply expected within the ***Poll Timeout*** period. If no response is received during the timeout period, the poll is sent again immediately (retried). Up to ***Poll Retries*** attempts will be made during a single poll sequence. If the retries all fail then the poll sequence fails. The Poll Interval must then elapse before another poll sequence is attempted.

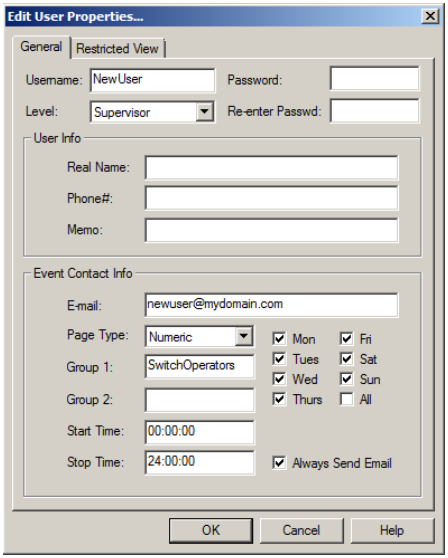
Emailing or Paging Multiple Users

This section shows how to email or page two users when a selection of devices goes down. Please read and understand the previous section before reading this one.

Step 1: Add a grouped set of SNMPc Enterprise users

- Use the ***Config/User Profiles*** menu.
- Press the ***Add*** button.
- Enter the ***Name*** of the new user.
- Set the user ***Email*** address.
- Set the user ***Pager*** type.
- Set the email/page days and times.
- Set the ***Group1*** user alias to ***SwitchOperators*** (this can be any text).
- Press ***OK*** to save the new user.

- Repeat this process for a different user name, making sure to set the ***Group1*** value to ***SwitchOperators,*** so that both users have the same value for ***Group1*** (i.e., they have the same alias).



Step 2: Add the users to Air Messenger Pro

To use paging, start the Air Messenger Pro application and add two users with the same names as those you added to SNMPc Enterprise. Do not use Air Messenger Pro groups and do not use the SNMPc Enterprise *Group1* name. Each SNMPc Enterprise user must have a matching user name in Air Messenger Pro. Setup the paging/modem options and make sure that you can send pages for each of the two new users.

Step 3: Add an Event Filter for the selected devices

Following steps 4 through 7 of the previous section, add a new event filter for a set of devices. In the ***Action*** tab, select ***SwitchOperators*** in the ***Page*** pull-down to page the two new users. Select ***SwitchOperators*** in the ***Email*** pull-down to send email to the two new users.

In the ***Match*** tab of the Add Event Filter dialog, make sure that you match different devices than those used in the previous section (emailing the Administrator). Otherwise, this new filter will not be unique and it will not match any incoming events.

Don't forget to set the ***Auto-Clears*** flags for any matching events.

Troubleshooting Network Discovery

Duration of Network Discovery

During the SNMPc Enterprise Server installation you entered the address, netmask, and community name for one SNMP V1 discovery seed device. This is normally enough information to discover most of your network. When you first start SNMPc Enterprise it will take ***several minutes*** for discovery to start adding objects to the map. Use the ***Root Subnet*** button to display the top-level map view.

If you used the ***Disable Discovery on Startup*** option of the installation, discovery will not be running when you first start SNMPc Enterprise. In this case, you need to set discovery filters before proceeding. Please refer to the *Limiting Discovery* section below before reading this section.

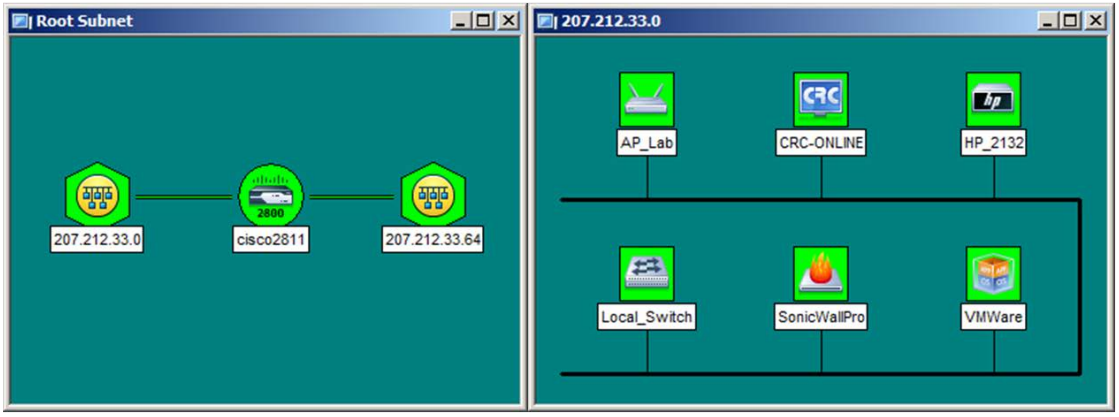
Normal Discovery Map Layout

Discovery creates a two-level IP Subnet based topology. At the top-level, discovery adds any multi-port devices (routers) and subnet icons for each IP Subnet. Link objects are added between each router and the subnets it is connected to. The map is automatically arranged in a star configuration.

All single-port SNMP devices and ICMP (Ping) devices are added to the second level under each subnet icon, based on the device IP address and subnet mask. A single Bus Network is added to each subnet level, and all devices in the subnet are linked to this network.

Use the ***Root Subnet*** button to display the top-level map view. You should see a mixture of SNMP device icons and subnet icons, connected by links in a star configuration. ***Double-click*** on one of the subnet icons. You should see a Bus Network with devices linked to it in a grid configuration.

The following diagram shows a sample top-level and subnet map view for a small network. Note that some devices have vendor-specific icons while others have generic icons. Each generic device icon is marked as SNMP or ICMP (Ping), which is important in determining discovery problems.

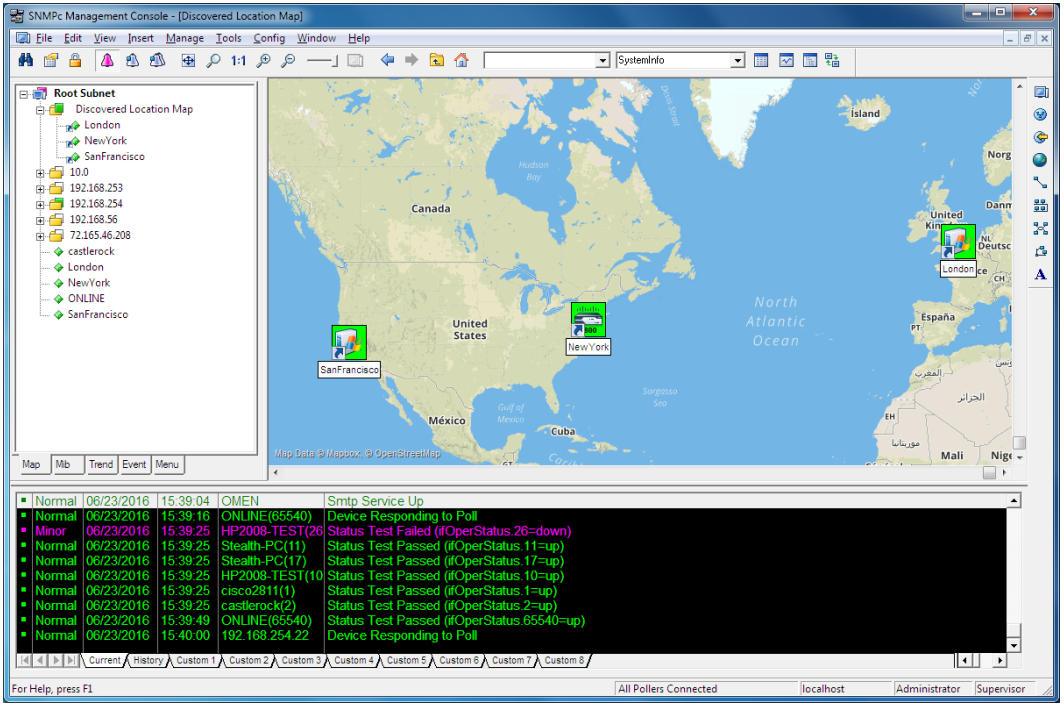


Geographic Map Layout

Discovery can optionally create a geographic map layout for devices that include position location information in the SNMP ***sysLocation*** variable. To enable geographic discovery use the ***Config/Discovery-Polling*** menu and select the ***Location Discovery and Layout*** checkbox at the bottom left of the Discovery/Polling Agents

When geographic layout is enabled Discovery will create a new Geo Subnet named ***Discovered Location Map*** and will add a ***Device Shortcut*** object for every discovered device that has position location information. A *Device Shortcut* object is similar to a *Goto* icon but links to a device instead of a subnet.

The following shows a sample ***Discovered Location Map*** view:



Failure Symptoms and Solutions

The discovery agent uses a heuristic algorithm to find network devices. That means it is somewhat non-deterministic and will show different results from one run to another. There are many reasons for this, including lost broadcast responses (buffer overflows, collisions), lost polls, slow responses, etc. This is completely normal. However, there are some permanent failure cases that you can resolve. The following symptoms are typical of a discovery failure:

1. Nothing added to the map (*after a suitable wait period of several minutes*).
2. Top-level map only or mostly contains subnet icons, with no links.
3. Some or all SNMP devices are added to lower level subnets as Ping icons.
4. Not all expected network devices are discovered.

The following sections describe solutions to these problems.

Discovery Agent Fails to Connect to the Server

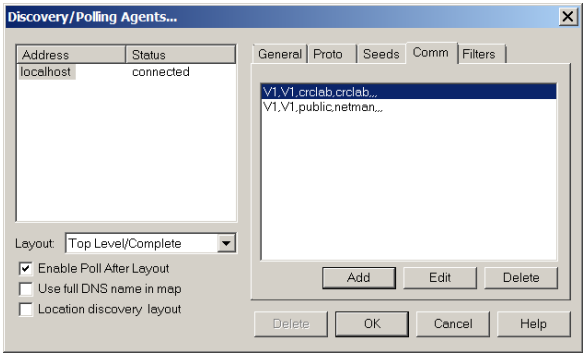
Look at the ***Current*** tab of the ***Event Log Tool***. If you can't see the Event Log Tool, use the ***View/Event Log Tool*** to show it. Scroll to the top of the event log. You should see an entry that says *Discovery/Status Agent Connected To Server*. Also, use the ***Config/Discovery-Polling*** menu. You should see an entry in the list at the left for your system IP address and the status should be *connected*. If these two things are not true then the discovery agent has not properly connected to the server.

SNMPc Enterprise uses TCP/IP to communicate between different components. This can conflict with other software running on your system. Look for any other management applications or Windows services and stop them (e.g., ***Windows SNMP Trap Service***). Try installing on a different system that has less software installed to help identify the conflicting software. This is a rare failure case.

Incorrect or Missing Community Names

Each SNMP V1 device uses a Read Community password for SNMP access. This is typically set to ***public*** when the device is installed but in most cases your network administrator has changed the community name. Furthermore, many different community names may be in use on your network.

- Determine what community names are used in your network devices.
- Use the ***Config/Discovery-Polling*** menu.
- Select your system address in the agents list.
- Press the ***Comm*** tab.
- For each community name, press the ***Add*** button. Set ***the Read Access Mode*** and ***Read/Write Access Mode*** to ***SNMP V1*** and set ***Read Community and Read/Write Community*** to valid community names
- Press the OK button.
- Use the ***File/Reset*** menu to delete the discovered map and restart discovery.



SNMP Device Access Control List

Many SNMP devices have an *Access Control List (ACL)*. An ACL is a list of IP addresses from which the device accepts SNMP requests. This is a vendor-specific security feature that is configured at the device using a terminal or Telnet session. At a minimum, you need to go to each ***Discovery Seed*** device and check if it has an ACL and that your SNMPc Enterprise system address is in the list. For complete network discovery you must add your system address to any ACLs in your network.

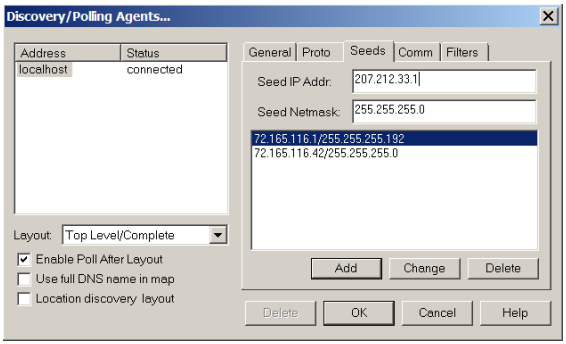
Firewalls Block SNMP Operations

Many networks use firewall devices to stop unauthorized intrusions. It is very usual for firewalls to block SNMP traffic because SNMP operations can shutdown and reconfigure devices. If you have any firewalls in your network you need to make sure that your SNMPc Enterprise system can send and receive SNMP operations through the firewalls. This is normally done with a protocol filter in combination with an Access Control List. Firewall configuration is done with a terminal or Telnet session.

Not Enough Seeds

SNMPc Enterprise uses a combination of downloaded seed device information (address, routing, arp tables) and broadcasts to discover devices. However, many devices inhibit broadcasts to networks outside of your LAN (subnet directed broadcasts). To get around this problem you need to add more seed addresses for routers around your network.

- Use the ***Config/Discovery-Polling*** menu.
- Select your system address in the agents list.
- Press the ***Seeds*** tab.
- For each new seed, enter the IP Address and Subnet mask in the supplied edit boxes and press Add.
- Press the ***General*** tab and then the ***Restart*** button.
- Press the OK button. There is no need to reset the map in this case.



Broadcast Packet Losses

In many cases network discovery mostly works but you don't see as many devices as you expect. As many devices are not represented in SNMP Arp tables they can only be discovered with broadcasts. And broadcasts responses can be lost due to buffer overflows, collisions, etc.

To get around this problem you can enable sequential polling of every possible address within a discovered subnet. Use the ***Config/Discovery-Polling*** menu and select the ***Ping Scan Subnets*** checkbox then press the ***Restart*** button.

Note that SNMPc Enterprise will not poll ranges that you specify but only discovered subnets. To discover more subnets, add more seeds as described in the previous section.

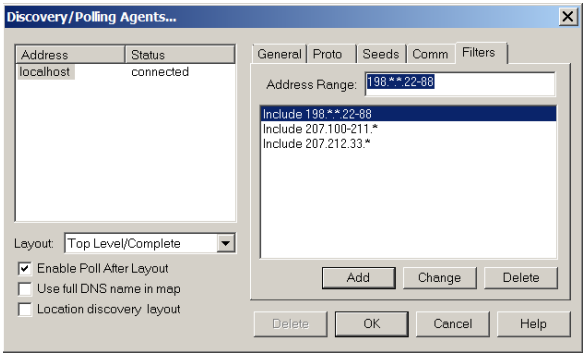
Limiting the Scope of Discovery

If you have a large network but you only want to manage a small part of it, you need to set discovery address range filters. Discovery filters only specify what should be included. So if you set any discovery filters you must set enough of them to cover any address ranges you want to discover.

Address range filters are in dot notation with optional wild-card asterisk characters and numeric range specifiers. Unless the last element is an asterisk, there must be four dot-separated elements. The following are some valid examples:

207.*
207.212.33.*
207.200-211.*
198.*.*.22-88

- Use the ***Config/Discovery-Polling*** menu.
- Select your system address from the agents list.
- Press the ***Filters*** tab.
- Enter a filter in the ***Address Range*** edit box and press ***Add***.
- Repeat for other filters.
- Press OK.
- Use the ***File/Reset*** menu to delete the current map and restart discovery with the new filters.



Stopping Discovery Auto-Layout

Left unattended, discovery will constantly rearrange your top-level map as new devices are added. This is undesirable if you want to manually change the map layout. To control discovery layout, use the ***Config/Discovery-Polling*** menu and do ***one of the following***:

1. Uncheck the ***Enable Discovery*** check box to disable further discovery.
2. Select *Discovered Objects* from the ***Layout*** pull-down to add any new objects to a subnet named Discovered Objects instead of the top-level map.
3. Select *Top Level/Incremental* from the ***Layout*** pull-down to add any new objects to the top-level using an incremental layout algorithm. The existing layout will not be disturbed.

Using a Remote Console

Once you have accustomed yourself to using SNMPc Enterprise in a standalone configuration, the first level of extension is to login from a remote workstation. You can login from any workstation that is running TCP/IP and is connected to your network in some way (e.g., over the Internet, leased line, LAN, etc.). However, the SNMPc Enterprise console has fairly heavy bandwidth requirements and will not perform adequately on low-speed dial-up lines. We recommend that you only login remotely over LAN or T1 speed lines.

Perform the following steps to install an SNMPc Enterprise Remote Console on a computer.

- Place the ***SNMPc Network Manager*** CD-ROM in the CD-ROM drive.
- From the Windows Start menu, select **Run** and enter *d:\setup.exe* (replace *d* with the drive letter for your CD-ROM drive). Press OK.
- At the ***SNMPc Network Manager*** component selection dialog, press the ***SNMPc Enterprise*** button.
- At the ***SNMPc Enterprise*** component selection dialog, press the ***Remote Console*** button.
- The setup program will proceed to install the *SNMPc Enterprise Remote Console* on your system. Once the installation is complete you can login to a running SNMPc Enterprise server. From the Windows Start menu, select the ***Programs/SNMPc Network Manager/Login Console*** menu. Enter the IP Address of the server computer and press OK. You are now logged in to the server and can perform any console operations remotely

Using the JAVA Console

JAVA Console Requirements

The JAVA Console has the following requirements:

1. The SNMPc Enterprise JAVA Console was compiled using JAVA version 1.7. You should install this, or a more recent, version of the JAVA runtime on the remote client before trying to run the console applet.

2. You must run a ***WEB Server*** on the SNMPc Enterprise server system. This is not included with SNMPc Enterprise.

3. You must use a web browser that supports Java Applets. Chrome and Microsoft Edge browsers do not support Java Applets.

Installing and Using the JAVA Console

Perform the following steps to install and use the JAVA Console:

Step 1: Install and enable a WEB Server application (not included with SNMPc Enterprise).

Step 2: Create a directory for the JAVA Console components that is accessible to your WEB Server.

Step 3: Copy the following JAVA Console components to the directory created in step 2 above:

<*SNMPc* >\java\crc.jar
<*SNMPc* >\java\default.html
<*SNMPc* >\java\manual

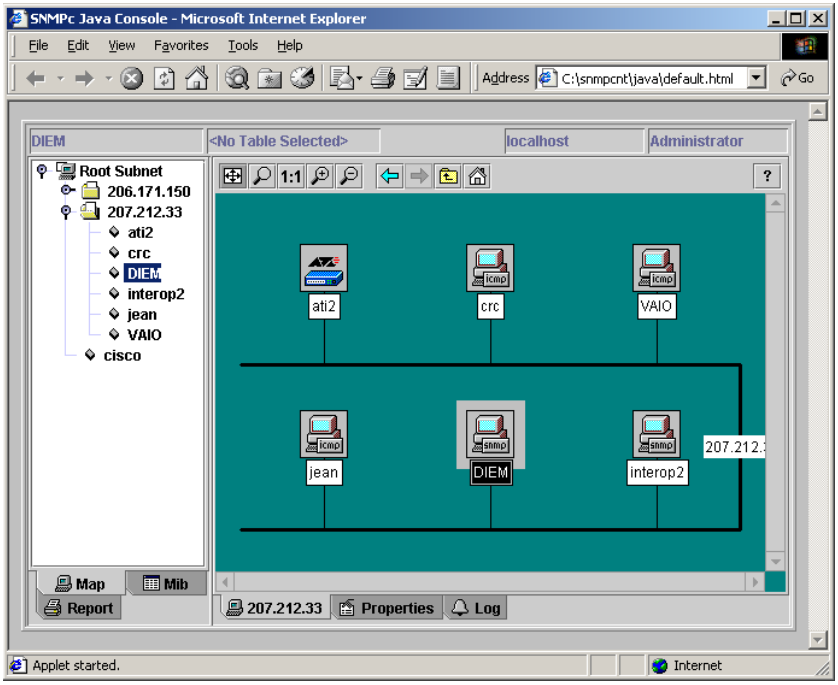
where <*SNMPc* > is the SNMPc Enterprise installation directory. *Manual* is a directory and contains all of the online documentation in HTML format.

Step 4: Using a WEB Browser from any system, enter the URL for the SNMPc Enterprise JAVA Console startup page as follows:

http://a.b.c.d/SNMPc javadir/default.html

where *a.b.c.d* is the IP address of the SNMPc Enterprise server system and *SNMPc javadir* is the directory where you placed the JAVA Console components. The JAVA Console will be executed inside the WEB browser.

The JAVA Console provides limited functionality and is read-only. It is designed for occasional use or for SNMPc Enterprise access over low-speed lines. Once you are running the JAVA Console Help menu to learn about using the JAVA user interface.



Restricting JAVA Console Access

You can limit the addresses that are allowed to connect to SNMPc Enterprise by editing the SNMPc.INI file. The SNMPc.ini file is located in the directory that SNMPc Enterprise was installed to. Add the following line to the [Server] section:

AcceptAddrs=a.b.c.d,aa.bb.cc.dd,...

where "a.b.c.d" and "aa.bb.cc.dd" are acceptable client addresses. You may add as many addresses as you like separated by commas. These must be IP Addresses. Domain names are not acceptable.

Adding a Redundant Backup Server

By using two SNMPc Enterprise servers with one designated as a Primary and the other as Backup server you can continue monitoring your network if the Primary system is disabled for any reason. The Primary SNMPc Enterprise server will automatically export its configuration files to the Backup server on a scheduled basis. It's important to do this automatically so that the Backup server is always up to date.

When the Backup server detects a failure of the Primary server it will take over all polling of the network, including instructing any remote polling agents to reconnect to the Backup server.

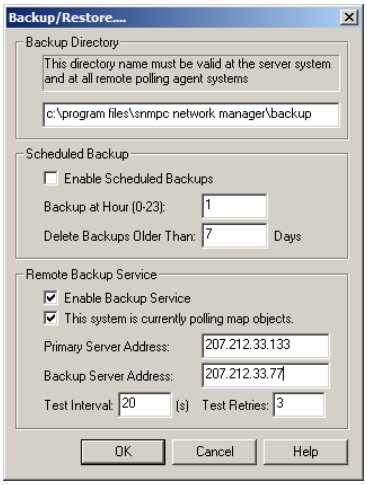
The following preconditions must exist before configuring the redundant backup server functionality:

- The password for the *Administrator* and *Remote Poller* users must be the same on both systems.
- There must be an available communication path between both systems and from each system to any remote polling agents you are using.

Use the ***Config/Backup-Restore*** menu to configure redundant backup server functionality on both the primary and backup servers.

Use the ***Enable Backup Service*** checkbox to enable or disable database export (primary server) and primary server monitoring (backup server). This check box must be enabled on both systems.

Use the ***This system is currently polling map objects*** checkbox to enable or disable map object status polling at the server you are logged on to. This checkbox is usually enabled at the primary server and disabled at the backup server.



The backup server takes over polling of all map devices by automatically setting the ***This system is currently polling map objects*** checkbox on. Once you have resolved the problem at the primary Server, disable this checkbox at the backup system to revert to the normal state.

Use the ***Primary Server Address*** and ***Backup Server Address*** edit boxes to set the IP address, in dot notation, of the corresponding server systems. These settings must be the same on both systems.

Use the ***Test Interval*** and ***Test Retries*** edit boxes to set the time between checks of the primary server by the backup server and how many times to retry before taking over polling.

Other SNMPc Enterprise Features

This document has only described some of the most commonly used SNMPc Enterprise features. SNMPc Enterprise is a full-featured distributed network management system that will meet your most demanding needs. These are some of the other features that you will find described in the Online Help system.

- Running Tasks as Windows Services
- Windows Task Bar Control Icon
- Private MIB Import
- User audit events (login and map edit)
- Manager-of-managers support
- SNMPc 4.0 Map Import
- Scheduled Backups
- ODBC Database Export
- Custom MIB Tables
- Custom MIB Expressions
- Custom Menus
- Graphical Device Views
- MIB Variable Browser
- RMON User Interface
- Alarm box event action
- Event Forwarding
- Running External Programs
- Automatic Icon/Program Selection
- Programming Interfaces

How to Buy SNMPc Enterprise

If you are using an evaluation copy of SNMPc Enterprise, the evaluation period will expire thirty days after installation. For complete pricing and purchasing information please go to the ***How to Buy*** page of *www.castlerock.com*.

If you want to buy SNMPc Enterprise after using the evaluation version, there is no need to reinstall any software components. The evaluation version you downloaded from the WEB includes the latest updates and may be newer than the CDROM you receive. To upgrade your evaluation copy, just enter your purchased license keys at the Welcome dialog when you start the SNMPc Enterprise Server.

Appendix A – Event Message/Exec Parameters

Use Event Parameters in Event Action Filters to substitute information related to a specific event. Event Parameters can be used in the ***Event Message*** and as arguments to a program in the ***Exec Program*** action. The available Event Parameters are described in the following table.

PARAMETER	EXPANSION
$$	The dollar ($) symbol
$V	Event message text (for Exec Program action).
$W	Console frame window number.
$L	License sequence number for ODBC node ID export.
$l	Log entry record number (can only be used for run program action, not in message)
$M	Server IP Address.
$R	Address of sending entity (could be the same as the target device, or Polling Agent)
$F	Event Action Filter name.
$f	Event Action Filter database record number.
$O	Trap Name as a textual string.
$o	Trap Object Identifier in dot format.
$P	Device parent submap name.
$A	Address of target device (device that the event is about)
$T	Trap Community Name.
$x	Date the event occurred, in local format at server.
$X	Time the event occurred, in time zone of server.
$@	Time the event occurred, in seconds since Jan 1, 1970.
$U	Value of sysUpTime in the event trap.
$N	The map object name of the target device.
$B	The map object MAC address of the target device
$D	The map object description of the target device
$h	The map object group number of the target device
$H	The map object group name of the target device
$i	The map database record number of the target device.
$G	The Read Community name of the target device
$S	The Set Community name of the target device.
$E	The timeout attribute, in seconds, of the target device
$Y	The max retries for the target device
$C	The number of variables in the event trap.
$z	The priority number of the associated log event.
$Z	The priority name of the associated log event.
$*	All variables as "[seq] name (type): value".
$-n	The nth variable as "name (type): value"
$+n	The nth variable as "name: value".
$n	The nth variable as “value”
$>n	All variables from the nth as "value".
$>-n	All variables from the nth as "[seq] name (type): value.
$>+n	All variables from the nth as "name: value.