



---

Managing Your Network

## **Solstice Enterprise Manager™ 4.1**

---

Sun Microsystems, Inc.  
901 San Antonio Road  
Palo Alto, CA 94303  
U.S.A. 650-960-1300

Part No. 806-7966-10  
October 2001, Revision A

Copyright 2001 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, California 94303 U.S.A. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Solstice, Solstice Enterprise Manager, SunOS, and Solaris are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

**RESTRICTED RIGHTS:** Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a).

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

---

Copyright 2001 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, Californie 94303 Etats-Unis. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Solstice, Solstice Enterprise Manager, SunOS, et Solaris sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REpondre A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.



Please  
Recycle



Adobe PostScript

# Contents

---

## **Preface   xxv**

## **1. Introduction to Solstice Enterprise Manager   1**

- 1.1 What is Solstice EM?   1
  - 1.1.1 What You Can Manage With Solstice EM   2
  - 1.1.2 Who Uses Solstice EM?   3
- 1.2 Solstice EM Features   4
- 1.3 Solstice EM Components   4
  - 1.3.1 Solstice EM Architecture   5
  - 1.3.2 Solstice EM Network Management Tools   8
- 1.4 Basic Enterprise Manager Concepts   10
  - 1.4.1 Network Management Software   10
  - 1.4.2 Agents and Stations   10
  - 1.4.3 Management Information Servers   12
    - 1.4.3.1 More About MIS Databases   13
    - 1.4.3.2 More About the MIS Nerve Center   14
    - 1.4.3.3 More About PMI and MPAs   14
    - 1.4.3.4 Ancillary MIS Services   15
    - 1.4.3.5 More About MIS Data Access   16
    - 1.4.3.6 More About Object Orientation   16
  - 1.4.4 Network Management Protocols   17

1.4.4.1	More About RPC	18
1.4.4.2	More About MIBs	18
1.5	Solstice EM Application APIs	19
1.5.1	API Modules	20
1.5.2	Application Development Support Tools	21
1.6	Related Reading	21
1.7	Solstice EM Tools—Complete Listings	22
<b>2.</b>	<b>Getting Started With Solstice EM</b>	<b>1</b>
2.1	Overview	1
2.1.1	Related Files	2
2.1.2	Related Tasks	3
2.2	Setting Up the Solstice EM Environment	3
2.3	Starting Solstice EM	4
2.4	Starting Individual Tools	5
2.5	Reconnecting to the MIS	7
2.6	Accessing Online Documentation	7
2.7	Adding and Removing Tools	9
2.8	Modifying Tool Configurations	11
2.9	Reference	12
2.9.1	Command-Line Options	12
2.9.1.1	Options for the <code>em</code> Command	12
2.9.1.2	System Variables Used by Solstice EM	13
2.9.1.3	Solstice EM Environment Variables	14
2.9.2	Windows and Dialogs	15
2.9.2.1	The Network Tools Window	15
2.9.2.2	Network Tools Customize Dialog	17
<b>3.</b>	<b>Discovering Network Components</b>	<b>1</b>
3.1	Overview	2
3.1.1	Agents and Stations	2

3.1.2	Methods Used by Network Discovery	3
3.1.3	Network Views	3
3.1.4	Network Monitor	4
3.1.5	Related Tasks	4
3.1.6	Related Files	5
3.1.7	Further Reading	5
3.2	Getting Started With Network Discovery	5
3.3	Loading and Saving Discovery Rules	7
3.4	Deciding Which Components to Discover	8
3.5	Viewing Network Discovery Progress	12
3.6	Stopping a Network Discovery in Progress	12
3.7	Creating a New MIS Managed Object Database	13
3.8	Keeping Data Current With Network Monitor	14
3.9	Reference	17
3.9.1	Command-Line Options	17
3.9.1.1	Network Discovery Options	18
3.9.1.2	Network Discovery Monitor Options	21
3.9.2	More About Network Discoveries	22
3.9.2.1	Network Discovery Query Stage	22
3.9.2.2	Network Discovery Probe Stage	23
3.9.2.3	More About Classifying Devices	24
3.9.2.4	Discover and Network Security	25
3.9.2.5	Recovering From a Failed Discovery	25
3.9.3	More About Hop Counts	27
3.9.4	More About Ping/SNMP Optimization	27
3.9.5	More About RPC Agents and SunNet Manager Proxies	28
<b>4.</b>	<b>Viewing Network Components</b>	<b>1</b>
4.1	Overview	2
4.1.1	Basic Network Views Concepts	3
4.1.1.1	Component Representations	4

4.1.1.2	Object Properties	4
4.1.1.3	Icon Objects	5
4.1.1.4	Saved Views	6
4.1.2	Related Tasks	7
4.1.3	Related Files	7
4.1.4	Further Reading	8
4.2	Getting Started With Network Views	8
4.3	Working With Views	9
4.3.1	Populating the Network Views Window	9
4.3.2	Selecting a View	10
4.3.3	Starting Network Views in a Specific View	11
4.3.4	Displaying and Selecting Objects	12
4.3.5	Searching for an Object	12
4.3.6	Creating a Logical (Non-topological) View	13
4.3.7	Creating a Network Views Icon Object	14
4.3.8	Editing View Contents	16
4.3.9	Deleting Objects From a View	17
4.3.10	Zooming In or Out in the Current View	17
4.3.11	Navigating in Geographical Map Views	18
4.3.12	Changing Icon Size in the Current View	19
4.3.13	Changing Label Size for the Current View	19
4.3.14	Changing the Background Image for the Current View	20
4.3.15	Displaying Specific Object Types	20
4.3.16	Displaying Specific Map Layers	21
4.3.17	Saving and Loading View Settings	22
4.3.18	Viewing the Network Views Message Log	22
4.4	Configuring Object Icons and the Workspace	23
4.4.1	Configuring General Display Properties	23
4.4.2	Configuring Icon and Label Display	24
4.4.3	Configuring Zoom Settings	25

4.4.4	Customizing Color Settings	26
4.4.5	Customizing View Layout	29
4.4.6	Using Background Images	31
4.4.7	Configuring Double-click Actions	33
4.4.8	Configuring the Tools Menu	34
4.4.9	Configuring Pop-up Menus	36
4.4.10	Configuring the Object Attributes Command	36
4.4.11	Adding an Object Type to the Object Palette	37
4.5	Managing Object Properties	39
4.5.1	Getting Started With Object Properties	39
4.5.2	Viewing Object Properties	40
4.5.3	Modifying Object Properties	41
4.5.4	Creating New Managed Objects	42
4.5.5	Configuring Agent Communications	44
4.5.5.1	Configuring Default Agents	44
4.5.5.2	Manually Configuring SNMP Agents	45
4.5.5.3	Manually Configuring RPC Agents	46
4.5.5.4	Manually Configuring MIS Agents	47
4.5.5.5	Manually Configuring CMIP Agents	48
4.5.5.6	Using Multiple CMIP MPAs Over RFC1006	49
4.5.5.7	Restarting the CMIP MPA Stack	53
4.6	Working With Alarms	53
4.6.1	Viewing Object Alarms	53
4.6.2	Clearing Object Alarms	54
4.6.3	Propagating Alarm Severity	54
4.7	Working With Requests	56
4.7.1	Viewing Advanced Request Information	57
4.7.2	Viewing Basic Request Information	57
4.7.3	Creating, Modifying, and Initiating Advanced Requests	58
4.7.4	Creating, Modifying, and Initiating Basic Requests	59

<b>4.8</b>	<b>Reference</b>	<b>61</b>
4.8.1	Command-Line Options	61
4.8.1.1	Network Views Options	62
4.8.1.2	Object Properties Options	62
4.8.1.3	Network Views Layout Options	63
4.8.1.4	Basic Requests Options	64
4.8.1.5	Request Designer Options	65
4.8.2	Network Views Command and Variable Macros	65
4.8.3	More About Object Properties	67
4.8.3.1	Network Views Object Types	67
4.8.3.2	Configurable Object Type Data	70
4.8.4	More About Geographical Map Backgrounds	72
4.8.4.1	Components of Geographical Map Backgrounds	72
4.8.4.2	Adding New Geographical Maps	72
4.8.4.3	Geographical Map Configuration Files	73

## **5. Managing Alarms 1**

5.1	Overview	1
5.1.1	Functions of the Alarms Window	2
5.1.2	Alarm Severities	3
5.1.3	Alarm States	3
5.1.4	Alarm Associations	4
5.1.4.1	Attributes Used to Associate Alarms	4
5.1.4.2	Alarm That Represents the Association	5
5.1.5	Alarm Views	5
5.1.5.1	Summary View of Alarms	5
5.1.5.2	Association View of Alarms	6
5.1.6	Alarm Filters	7
5.1.7	Alarm Clearing	7
5.1.7.1	Manually Cleared Alarms	8
5.1.7.2	Automatically Cleared Alarms and Cleared Severity Events	8



5.1.8	Related Tasks	8
5.1.9	Related Files	9
5.1.10	Further Reading	9
5.2	Getting Started With the Alarms Window	9
5.3	Viewing Alarms	10
5.3.1	Viewing Alarms in Summary View	10
5.3.2	Viewing Alarm Associations and Alarm Instances	11
5.3.3	Viewing Alarms for a Specific Network Component	13
5.3.4	Viewing Alarms on a Remote MIS	14
5.3.5	Viewing a Non-default Alarm Log	14
5.3.6	Printing a List of Alarms	15
5.4	Grouping Alarms Into Associations	16
5.5	Filtering Alarms	18
5.5.1	Setting Alarm Filtering Rules	18
5.5.2	Using Filtering Rules Files	19
5.6	Performing Operations on Alarms	20
5.6.1	Acknowledging Alarms	20
5.6.2	Clearing Alarms	21
5.6.3	Hiding an Alarm in the Alarms Window	23
5.6.4	Annotating Alarms	24
5.7	Deleting Alarms From the Log	24
5.7.1	Deleting Alarms Manually	25
5.7.2	Selecting Alarms for Automatic Deletion After Clearing	25
5.7.3	Filtering Alarms for Deletion	26
5.8	Logging Alarms Management Activity	28
5.9	Graphing Alarm Data	29
5.10	Customizing the Alarms Window	29
5.11	Customizing the Tools Menu	32
5.12	Reference	33
5.12.1	The <code>em_alarmmgr</code> Command	33

5.13 Configuration Files 35

**6. Controlling User Access 1**

6.1 Overview 1

6.1.1 Understanding the Solstice EM Access Control Model 2

6.1.1.1 Security Rules 2

6.1.1.2 Policy for Enforcing Security Rules 2

6.1.1.3 About Users and Groups 4

6.1.2 Predefined Groups, Security Rules, and Object Sets 5

6.1.3 Implementation Schemes for Access Control 5

6.1.3.1 Control User Access to Tools 5

6.1.3.2 Control User Access to Managed Objects 6

6.1.4 Implementation Plan 6

6.1.5 Related Tasks 8

6.1.6 Related Files 8

6.2 Getting Started With Security 8

6.3 Turning Off Access Control 9

6.4 Preparing for Security Control 10

6.4.1 About Users, Granting All Privileges, and Root 10

6.4.2 About Privilege Groups 11

6.4.3 Getting Ready for Security Control 12

6.4.4 Turning On Security Control 13

6.4.5 Preparing for Remote Connections to the MIS 14

6.4.6 Preparing User Profiles 16

6.4.7 Granting Security Privileges 17

6.4.8 Preparing Group Profiles 18

6.4.9 Saving and Reusing Profiles 20

6.4.10 Printing Profiles 21

6.4.11 Searching for Users and Groups 21

6.4.12 Maintaining User Profiles 22

6.4.13 Maintaining Group Profiles 23

6.5	Controlling Access to Solstice EM Tools	24
6.5.1	Implementation Overview	24
6.5.1.1	About Solstice EM Tools and Tasks	25
6.5.1.2	Security Rules for Controlling Access to Tools	25
6.5.2	Getting Ready to Control Access to Solstice EM Tools	26
6.5.3	Placing Tools Under Security Control	26
6.5.4	Removing Tools From Security Control	28
6.5.5	Granting and Denying Access to Tools and Tasks	29
6.5.6	Viewing Tool Access Privileges	30
6.5.7	Updating Tool Access Privileges	30
6.6	Controlling Access to Managed Objects	31
6.6.1	Implementation Overview	31
6.6.1.1	Security Rules for Controlling Access to Managed Objects	32
6.6.1.2	Understanding Object Sets	33
6.6.2	Getting Ready to Control Access to Managed Objects	34
6.6.3	Defining Object Sets	35
6.6.4	Defining Security Rules for Object Sets	37
6.6.5	Assigning Objects and Security Rules to Groups	46
6.6.6	Viewing Access Privileges to Managed Objects	47
6.6.7	Maintaining Object Sets	48
6.6.8	Maintaining Object Privileges	49
6.6.9	Importing/Exporting Access Control Objects	50
6.7	Using the <code>em_accesscmd</code> Utility	50
6.8	Reference	54
6.8.1	Command-Line Options	54
6.8.1.1	The <code>em_accessmgr</code> Command	55
6.8.1.2	The <code>em_accesscmd</code> Utility	55
6.8.1.3	The <code>em_accesscmd</code> Commands	56
6.8.1.4	More About Object Sets	58
6.8.2	More About the Solstice <code>EM-config</code> Configuration File	60

## **7. Automating Nerve Center Requests 1**

- 7.1 Overview 1
  - 7.1.1 About Requests for Network Conditions 1
  - 7.1.2 About Nerve Center Request Templates 2
  - 7.1.3 About autoManagement Objects 2
    - 7.1.3.1 Default autoManagement Objects 3
    - 7.1.3.2 Custom autoManagement Objects 4
    - 7.1.3.3 When to Create an autoManagement Object 4
    - 7.1.3.4 Criteria Used by autoManagement Objects 5
  - 7.1.4 About the autoManagement Daemon 6
  - 7.1.5 Process of Automatic Management 6
  - 7.1.6 Related Tasks 7
  - 7.1.7 Related Files 8
- 7.2 Getting Started 8
- 7.3 Creating autoManagement Objects 8
  - 7.3.1 Creating Multiple autoManagement Objects 10
- 7.4 Manually Starting and Stopping Requests 11
- 7.5 Changing autoManagement Object Characteristics 12
- 7.6 Reference 13
  - 7.6.1 Command-Line Options 14
  - 7.6.2 AutoManagement Daemon 14
  - 7.6.3 Sample autoManagement Objects 15
    - 7.6.3.1 Entry Launching IsSnmpSystemUp Template 15
    - 7.6.3.2 Entry Launching LinkUp Template 16
    - 7.6.3.3 Entry Launching Ping-Reachable Template 17
    - 7.6.3.4 Entry Returning the Transport Address of an Agent 18

## **8. Gathering Attribute Data 1**

- 8.1 Overview 1
  - 8.1.1 How Data is Obtained in Solstice EM 3
  - 8.1.2 About Collections 4

8.1.3	Related Tasks	4
8.1.4	Related Files	5
8.1.5	Further Reading	5
8.2	Getting Started	5
8.3	Viewing Object Attributes From an SNMP Agent	7
8.4	Specifying an SNMP Device to Query	8
8.5	Working in Tables	10
8.5.1	Creating and Loading Tables	10
8.5.2	Selecting and Moving Data in Tables	11
8.5.3	Completing Tables	12
8.5.4	Clearing Tables	13
8.5.5	Printing Tables	13
8.6	Getting Attribute Data	14
8.7	Setting Attribute Data	16
8.8	Polling for Data	17
8.9	Displaying Data From Another MIS	19
8.10	Obtaining Data From a Network Component Managed by a Remote MIS	19
8.11	Updating MIS Tables With Attribute Values From Third-Party MIBs	23
8.12	Recording Data to a Collection	24
8.13	Creating Data Collections	25
8.14	Scheduling Collection Polls	26
8.15	Viewing Collected Data	27
8.16	Graphing Collected Data	28
8.17	Reference	28
8.17.1	SNMP Command-Line Options	29
8.17.2	Data Collections Command-Line Options	30
8.18	More About Data Collection	30
8.18.1	Data Collections GDMO Classes	30
8.18.2	The dataCollector GDMO class	31

- 8.18.3 The dataCollectorEntry Object GDMO Class 32
- 8.18.4 The RequestInfo Attribute 33
- 8.19 Error Messages 33

## **9. Viewing Collected Data 1**

- 9.1 Overview 1
  - 9.1.1 What Are Streams? 2
  - 9.1.2 How Are Streams Defined? 3
  - 9.1.3 What Are Reports? 3
  - 9.1.4 What Are Folders? 4
  - 9.1.5 Related Tasks 4
  - 9.1.6 Related Files 4
- 9.2 Getting Started With Results Browser 4
- 9.3 Loading Collections as Streams 5
- 9.4 Viewing Reports 6
- 9.5 Managing Reports 6
- 9.6 Selecting Streams 8
- 9.7 Displaying Streams in Grapher 10
- 9.8 Managing Folders 10
- 9.9 Customizing the Results Browser 12
  - 9.9.1 Changing the Window Position 13
  - 9.9.2 Changing the Window Size 13
  - 9.9.3 Specifying a Printer 13
  - 9.9.4 Defining an Output Size 14
  - 9.9.5 Setting the Format for Reports 14

## **10. Graphing Collected Data 1**

- 10.1 Overview 1
- 10.2 Getting Started With Grapher 2
- 10.3 Loading Data Into Grapher 3
- 10.4 Displaying Graphs 4

10.5	Selecting Streams to Display as Graphs	4
10.6	Displaying Graphical Dimensions	5
10.7	Plotting Values in Different Ways	6
10.8	Changing Viewing Angles in 3-D Graphs	6
10.8.1	Changing the X-Axis, Vertical Rotation	7
10.8.2	Changing the Y-Axis, Diagonal Rotation	7
10.8.3	Changing the Z-Axis, Horizontal Rotation	8
10.9	Setting Graph Colors	8
10.10	Changing the Display of the Plotted Data	10
10.11	Saving a Graph to a File	12
10.12	Printing a Graph	12
10.13	Replotting a Graph	13
10.14	Merging Graphs	13
<b>11.</b>	<b>Examining Log Entries</b>	<b>1</b>
11.1	Overview	1
11.1.1	Log Entries in the AlarmLog File	2
11.1.2	Related Files	2
11.1.3	Related Tasks	2
11.1.4	Further Reading	3
11.2	Getting Started With Log Entries	3
11.3	Changing the Log Entry Display	4
11.4	Viewing Log Entry Details	6
11.5	Filtering Log Entries	6
11.6	Combining Log Entries in a Single View	7
11.7	Searching for Log Entries	8
11.8	Printing and Deleting Log Entries	9
11.9	Adding and Removing Solstice EM Tools	9
11.10	Reference	10
11.10.1	Command Line Options	11

11.10.1.1	The <code>em_logview</code> Command	11
11.10.1.2	The <code>em_nnconfig</code> Utility	11
11.10.1.3	Log Entries Configuration File	12

## **A. Integrating Solstice Enterprise™ SyMON System Monitor With Solstice EM 1**

A.1	Overview	1
A.1.1	About Forwarding SyMON Events to Solstice EM	2
A.1.1.1	The SyMON System	3
A.1.1.2	The Solstice EM System	3
A.1.2	Limitations of SyMON Event Forwarding	3
A.1.3	About Adding the SyMON Monitor to the Solstice EM Interface	4
A.1.4	Related Tasks	4
A.1.5	Related Files	4
A.1.6	Further Reading	4
A.2	Setting Up the SyMON System to Forward Events	5
A.2.1	Adding an MIS Server Name to the SNMP Host List	5
A.2.2	Modifying SyMON Event Rules	6
A.2.2.1	Location of Event Rules Files	7
A.2.2.2	Determining Which Events to Forward	7
A.2.2.3	Editing the Actions of an Event Rule	7
A.2.2.4	Using the <code>snmp_trapsend</code> Utility in Event Rules	9
A.3	Setting Up Solstice EM to Receive SyMON Traps	14
A.3.1	Creating an Object Instance for the SyMON System	15
A.3.2	Mapping SyMON Traps	15
A.3.3	Creating a GDMO Document for SyMON Events	17
A.3.4	Mapping the SyMON Event Notification to an Object	20
A.4	Adding the SyMON Monitor to the Solstice EM Interface	21

## **B. Managed Object Definitions 1**

B.1	The Management Information Base	1
B.2	MIB Terminology	2



B.2.1	Organization of the MIB	2
B.2.1.1	Directory Group	2
B.2.1.2	Management Group	3
B.2.1.3	Experimental Group	4
B.2.1.4	Private Group	4
B.3	Managed Objects by Function	4
B.4	Objects and Solstice EM	5
B.4.1	Solstice EM Applications and Supported Protocols	6
B.4.2	MIBs Supported by Solstice EM	6
B.5	MIBs Supported by Solstice EM	9



# Figures

---

- FIGURE 1-1 Solstice EM Architecture Overview 7
- FIGURE 1-2 Agent Communications Overview 11
- FIGURE 1-3 Overview of Management Information Servers 13
- FIGURE 2-1 Network Tools Window 16
- FIGURE 2-2 Administration Window 16
- FIGURE 2-3 Network Tools Customize Dialog 18
- FIGURE 3-1 Network Discovery Button 6
- FIGURE 4-1 Network Component Representation in Network Views 4
- FIGURE 4-2 Network Views Button 9
- FIGURE 4-3 Network Discovery Button 10
- FIGURE 4-4 Network Views Toolbar Zoom Controls 17
- FIGURE 4-5 Network Views Map Toolbar 18
- FIGURE 6-1 Solstice EM Enforcement of Security Rules 3
- FIGURE 6-2 Rule Denying Group Access to All Objects 39
- FIGURE 6-3 Rule Denying Group Access to Specific Objects 40
- FIGURE 6-4 Rule Granting Access to All Objects 42
- FIGURE 6-5 Rule Granting Access to Specific Objects 43
- FIGURE 6-6 Default Rule 45
- FIGURE 8-1 Solstice EM Architecture as it Facilitates Network Communication 3

FIGURE 8-2 Viewing Requested Data Returned From a Host on a Remote MIS 19

FIGURE 9-1 Results Browser Window 2

FIGURE 10-1 Trends in Alarm Data Plotted in the Grapher View Dialog 2

FIGURE 11-1 Controls for Viewing Details of Log Entries 6

# Tables

---

TABLE 1-1	Common Solstice EM Tools	8
TABLE 1-2	Solstice EM API Modules	20
TABLE 1-3	Solstice EM Tools – Complete List, Sorted by Binary Name	22
TABLE 2-1	Core Solstice EM Tools	2
TABLE 2-2	Core Solstice EM Tools Executables	5
TABLE 2-3	Options for the <code>em</code> Command	12
TABLE 2-4	System Environment Variables	13
TABLE 2-5	Solstice EM Environment Variables	14
TABLE 2-6	Network Tools Menu	17
TABLE 2-7	Network Tools Customize Options	18
TABLE 3-1	Network Discovery Command-line Options	18
TABLE 3-2	Network Discovery Monitor Command-line Options	21
TABLE 3-3	Discover.conf Definitions	25
TABLE 3-4	Network Discovery Debugging Options	26
TABLE 4-1	Network Views Default Icon Object Types	5
TABLE 4-2	Common Network Views Object Icons	6
TABLE 4-3	Default Alarm Severity Color Mapping	28
TABLE 4-4	Network Views Command-line Options	62
TABLE 4-5	Object Properties Command-line Options	63

TABLE 4-6	Network Views Layout Command-line Options	64
TABLE 4-7	Basic Requests Command-line Options	64
TABLE 4-8	Advanced Requests Command-line Options	65
TABLE 4-9	Network Views Command and Variable Macros	66
TABLE 4-10	Network Views Object Icons and Types	67
TABLE 4-11	OCT Object Types and Configurable Data	70
TABLE 5-1	Color Mapping for Alarm Severity	3
TABLE 5-2	Effects of Summary and Association Settings on Alarms Window	6
TABLE 5-3	em_alarmmgr Command-Line Options	34
TABLE 5-4	Configuration Files Used by Alarms Tool	35
TABLE 6-1	Implementation Schemes	7
TABLE 6-2	Pre-defined Groups	12
TABLE 6-3	Predefined Security Rules	33
TABLE 6-4	Predefined Object Sets	34
TABLE 6-5	Security Command Options	55
TABLE 6-6	Security em_accesscmd Parameters	55
TABLE 6-7	em_accesscmd Utility Commands	56
TABLE 6-8	Criteria Defining Object Sets	58
TABLE 6-9	Security Control Variables	60
TABLE 7-1	Default autoManagement Objects Available During Installation	3
TABLE 7-2	Criteria for Automatic Management	5
TABLE 7-3	Request Controller Options	14
TABLE 7-4	Automatic Management Entry File Fields	16
TABLE 8-1	Solstice EM Tools for Data Gathering	2
TABLE 8-2	SNMP Data Command-Line Options	29
TABLE 8-3	Data Collections Command-Line Options	30
TABLE 8-4	Error Messages	33
TABLE 9-1	Type of Data Provided Per Stream	3

TABLE 9-2      Results Browser Report Stream Variables    3

TABLE 11-1    em\_logview Command Options    11

TABLE A-1      Mapping of Options for snmp\_trapsend and my\_trapsend    13

TABLE B-1      Attribute Categories in Management Group and Example Attributes    3

TABLE B-2      Solstice EM Objects Provided, Per MIB Group, For Network Management    5

TABLE B-3      Table of Protocols Accepted by Solstice EM Data Collecting Tools    6

TABLE B-4      Objects and Attributes of Solstice MIB Supported by Solstice EM Default Agent    7





# Preface

---

This guide provides step-by-step instructions and basic reference information for performing daily network management operations and for updating an existing Solstice Enterprise Manager network configuration.

---

## Who Should Use This Book

This book is intended for individuals who have the authority and the responsibility to operate and maintain medium to large area local and remote networks. This book is not aimed at people who have not yet acquired the experience and expertise in managing systems and networks.

---

## Before You Read This Book

If you have just acquired Solstice Enterprise Manager (Solstice EM) read the *Solstice Enterprise Manager Release Notes* for late-breaking information on compatibility and minimum machine and software requirements, and an inventory of the product components. Refer to online help and the books listed in Related Books for additional information about related topics.

---

# How This Book Is Organized

**Chapter 1, "Introduction to Solstice Enterprise Manager"** provides an introduction to the components of Solstice EM and their architectural relationship.

**Chapter 2, "Getting Started With Solstice EM"** provides information for setting the necessary environment variables and starting Solstice EM. The chapter includes instructions on how to add, modify, and delete Solstice EM tools to the Network Tools window for quick access.

**Chapter 3, "Discovering Network Components"** provides information on using Discover to configure the Solstice EM database with hosts, routers, networks, and Simple Network Management Protocol (SNMP) devices to be managed.

**Chapter 4, "Viewing Network Components"** provides information on the tools used to display graphical views of managed resources.

**Chapter 5, "Managing Alarms"** provides information on monitoring the alarms reports that have been sent to the MIS.

**Chapter 6, "Controlling User Access"** provides information on using Access Manager to set up groups and user accounts which control user access privileges within Solstice EM.

**Chapter 7, "Automating Nerve Center Requests"** provides information on configuring and starting/stopping the automatic management function.

**Chapter 8, "Gathering Attribute Data"** provides information on configuring and browsing the attributes of a Viewer's object.

**Chapter 9, "Viewing Collected Data"** provides information on collecting and viewing attributes from SNMP and SNM objects.

**Chapter 10, "Graphing Collected Data"** describes how to graph collected attribute data.

**Chapter 11, "Examining Log Entries"** provides the capability to browse through each log record within each log object.

**Appendix A, "Integrating Solstice Enterprise™ SyMON System Monitor With Solstice EM"** provides details on how to integrate SyMON with Solstice EM.

**Appendix B, "Managed Object Definitions"** provides explanatory and reference information about the Management Information Base (MIB), an important part of the Solstice Enterprise Manager architecture, and MIBs supported by Solstice EM.

---

## Related Books

Following is a list of related books:

- *Installation Guide*
- *Customizing Guide*
- *Troubleshooting Guide*
- *Management Information Server (MIS) Guide*
- *CORBA Gateway Administration Guide*

---

## What Typographic Changes Mean

The following table describes the typographic changes used in this book.

TABLE P-1 Typographic Conventions

Typeface or Symbol	Meaning	Example
AaBbCc123	The names of commands, files, and directories; on-screen computer output	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. <code>machine_name%</code> You have mail.
<b>AaBbCc123</b>	What you type, contrasted with on-screen computer output	<div>machine_name% <b>su</b> Password:</div>
<i>AaBbCc123</i>	Command-line placeholder: replace with a real name or value	To delete a file, type <code>rm filename</code> .
<i>AaBbCc123</i>	Book titles, new words or terms, or words to be emphasized	Read Chapter 6 in <i>User's Guide</i> . These are called <i>class</i> options. You <i>must</i> be root to do this.

---

# Shell Prompts in Command Examples

The following table shows the default system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

**TABLE P-2** Shell Prompts

Shell	Prompt
C shell prompt	machine_name%
C shell superuser prompt	machine_name#
Bourne shell and Korn shell prompt	\$
Bourne shell and Korn shell superuser prompt	#

---

# Accessing Sun Documentation Online

The docs.sun.com<sup>sm</sup> web site enables you to access Sun technical documentation on the Web. You can browse the docs.sun.com archive or search for a specific book title or subject at <http://docs.sun.com>.

Also, you can view the online documentation by pointing your browser to the following URL, `file:/opt/SUNWconn/em/docs/SEMDOCHP/index.html`

---

# Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can send your comments by email to [docfeedback@sun.com](mailto:docfeedback@sun.com).

Please include the part number of your document in the subject line of your email.

# Introduction to Solstice Enterprise Manager

---

This chapter provides introductory information designed to help you get going with Solstice Enterprise Manager software (Solstice EM) and your day-to-day network management tasks.

This chapter comprises the following topics:

- Section 1.1 “What is Solstice EM?” on page 1-1
- Section 1.2 “Solstice EM Features” on page 1-4
- Section 1.3 “Solstice EM Components” on page 1-4
- Section 1.4 “Basic Enterprise Manager Concepts” on page 1-10
- Section 1.5 “Solstice EM Application APIs” on page 1-19
- Section 1.6 “Related Reading” on page 1-21
- Section 1.7 “Solstice EM Tools—Complete Listings” on page 1-22

---

## 1.1 What is Solstice EM?

Solstice EM software is a distributed, standards-based, hierarchical, object-oriented suite of enterprise-grade network management tools, and a rich set of application programming interfaces (APIs) for developing custom network management applications. What this means is that Solstice EM is a highly flexible, totally customizable network management solution that can be scaled and configured to fit your needs. You can use any or all of the Solstice EM tools “as is,” or you can combine them with your own custom applications written to the Solstice EM API.

## 1.1.1 What You Can Manage With Solstice EM

Solstice EM provides tools for monitoring, evaluating, and refining your network. The management functions you can perform with Solstice EM include:

- **Discovering components on your network**

Automated tools let you keep track of components as they are added or removed from your network. Support for Common Management Information Protocol (CMIP), Simple Network Management Protocol (SNMP), and Remote Procedure Call (RPC) agents allow you to gather information about a wide variety of network components. Component details are stored in industry-standard relational databases on one or more management information servers.

- **Visualizing your network**

A powerful Network Views tool serves as the graphical command center of Solstice EM, from which you can organize and manage your network components as groups of icons in logical, hierarchical, and geographical *views*. You can create as many different views of your network components as you want, using whatever view is most appropriate for the task at hand. For example, you can view your network components on a cartographically accurate geographical map background—a map of the world, perhaps, or a blueprint of one of your buildings—which lets you see at a glance not only *what* component is reporting a fault but *where* that component is physically located. You can then initiate actions to correct the fault directly from the Network Views tool.

- **Configuring network components**

Solstice EM object properties editors in combination with CMIP, SNMP, and RPC agents let you configure all aspects of your network components, from general network properties to detailed component data, such as individual router interfaces. Schema- and MIB-to-GDMO compilers let you customize specific object attributes.

- **Detecting, tracking, and correcting network problems**

A sophisticated alarm manager and request template designer, in combination with data viewers, and logging, reporting, and graphing tools, let you gather detailed information about your network, configure and respond to alarms, and design dynamic request templates to automatically gather and respond to network and component conditions.

- **Managing user access to objects and applications**

The Solstice EM Security tool lets you control user access to individual Solstice EM and custom tools, as well as to specific sets of network components.

### ■ Customizing the Solstice EM interface

You can tailor Solstice EM tools in a wide number of ways, from pull-down and pop-up menus, to tool palettes, to default parameters and automatic monitoring methods. You can run almost every Solstice EM component from the UNIX command line, if you want, to create script-based maintenance routines. You can even modify Management Information Base (MIB), Abstract Syntax Notation One (ASN.1), and Guidelines for the Definition of Managed Objects (GDMO) to customize settings for the types of objects you can work with in Solstice EM.

### ■ Developing custom network management applications

Solstice EM is a standards-based, object-oriented environment that supports the Portable Management Interface (PMI) API over SNMP, CMIP, and SunNet Manager RPC, as well as full conformance with Telecommunications Management Networks (TMN) standards.

## 1.1.2 Who Uses Solstice EM?

Large companies—for example, in the telecommunications industry—use Solstice EM to manage hundreds of thousands of network nodes, with network components ranging from mainframes, subnetworks, gateways, servers, routers, and hubs, to workstations, personal computers, and agent-enabled mobile devices. Such companies use the standard suite of Solstice EM tools alongside their own custom tools developed with the Solstice EM APIs and toolkit.

Smaller companies use Solstice EM “out of the box” to manage all their network components, knowing that Solstice EM can be scaled to meet whatever needs they have as their company grows.

Any company interested in secure, high-performance management of distributed network resources—from portable handheld devices to deskbound graphical workstations—can use Solstice EM’s distributed agent-oriented technology to manage virtually any type of network component.

---

## 1.2 Solstice EM Features

Solstice EM provides the following network management features:

- Comprehensive suite of network management tools—from objects to enterprises, infrastructure to interfaces.
- Management of virtually any network-aware component, from UNIX workstations to Windows-based PCs, printers to routers, subnetworks to network interfaces.
- Graphical “point and click” CDE (Common Desktop Environment) tools and UNIX command-line interfaces allow real-time ease-of-use and script-based automation.
- Multiple concurrent user access—run anywhere, anytime with UNIX-based security and scalability.
- Distributed, hierarchical, ASN.1 object-oriented architecture utilizing an industry-standard SQL-compatible relational database (Informix™ by default).
- Customizable interfaces and support for custom third-party applications by means of the PMI API over SNMP, CMIP, RPC, and TMN protocols.
- Development support tools—a set of API modules, object development tools, compilers, and debuggers—for developing your own custom network management applications.
- Backward-compatibility with SunNet™ Manager and Solstice Site/Domain Manager data and applications.

---

## 1.3 Solstice EM Components

Solstice EM components can be divided into two categories:

- **Architecture** – The structural components underlying the Solstice EM environment.
- **Network Management Tools** – The means by which you access and manipulate the Solstice EM environment and the components on your network.

These components are described in the following sections.



## 1.3.1 Solstice EM Architecture

Network management in the Solstice EM environment is based on the exchange of information between managers and agents. It is client/server-based, hierarchical and object-oriented environment comprising:

- **Motif Applications** – The manager applications run on the Motif environment. The applications can either be custom applications or Solstice EM Tools.
- **JMA Server** – The Java Management Adapter (JMA) provides the framework for the thin client/fat server model. JMA is not exposed to end users or developers. It is a transparent component lying between services such as the JMI and the MIS. JMA provides the infrastructure for services such as JMI API, Topology API, and Alarm API to communicate seamlessly with the MIS. It is responsible for the scheduling and synchronization of all PMI calls made by each Java API. It provides an event handling mechanism, this allows clients to register their own events and servers to forward the events to the clients.
- **SEM CORBA Gateway** – SEM CORBA Gateway translates CORBA manager requests in Interface Description Language (IDL) to Solstice EM Portable Management Interface (PMI) or equivalent requests, it also translates Solstice EM PMI responses to IDL or Internet Inter-ORB Protocol (IIOP) responses, and PMI events to CORBA events. The SEM CORBA Gateway is designed to work with standard management reference models (such as SNMP/IP and CMIP/OSI). The interfaces defined and implemented by the SEM CORBA Gateway define the interaction with applications.  
Refer to the *CORBA Gateway Administration Guide* for detailed information.
- **Managed objects** – Solstice EM is centered around the concept of managed objects. A managed object is a set of programmatic services and attributes that describes a type of managed resource. In practical terms, it means that each physical component on your network is represented by one or more objects in an MIS database (see below). When you perform an action in Solstice EM on a network component for example, setting a configuration parameter or retrieving status information, you are actually performing that action on the managed object representing the network component.
- **Agent software** – Provides object-level communication methods between your network components and the rest of Solstice EM—that is, the means by which you can use Solstice EM to get and set properties on managed objects. Solstice EM supports SNMP, CMIP, and RPC agents, and includes a set of CMIP- and RPC-based Solstice™ Enterprise Agents (SEA) that support a wide variety of managed objects, including legacy objects created in SunNet Manager and Solstice Site/Domain Manager. See Section 1.4.2 “Agents and Stations” on page 1-10 for more information.

- **Management Information Server (MIS)** – A machine that hosts an SQL database containing a Metadata Repository (MDR) and a Management Information Tree (MIT), which are used by Solstice EM to maintain information about the properties and relationships, respectively, of all managed objects on your network. An MIS daemon and a set of ancillary MIS service daemons provide MIS services on the MIS host. For data security or organizational convenience, you can use multiple MIS hosts, with one MIS database on each host. Multiple MISs can be linked so that all appear as one MIS to a given user. See Section 1.4.3 “Management Information Servers” on page 1-12 for more information.
- **Application programming interfaces** – Support communication and protocol translation between one or more MISs and Solstice EM and/or custom network management tools. See Section 1.5 “Solstice EM Application APIs” on page 1-19 for more information.
- **Solstice EM and/or custom network management tools** – The tools you use to access and manipulate the Solstice EM environment and managed objects. These tools are described in Section 1.3.2 “Solstice EM Network Management Tools” on page 1-8.

The relationships between Solstice EM architectural components are illustrated in Figure 1-1, “Solstice EM Architecture Overview,” on page 7. Explanations of basic Solstice EM network management concepts are provided in Section 1.4 “Basic Enterprise Manager Concepts” on page 1-10.

Figure 1-1 provides an overview of Solstice EM architecture.

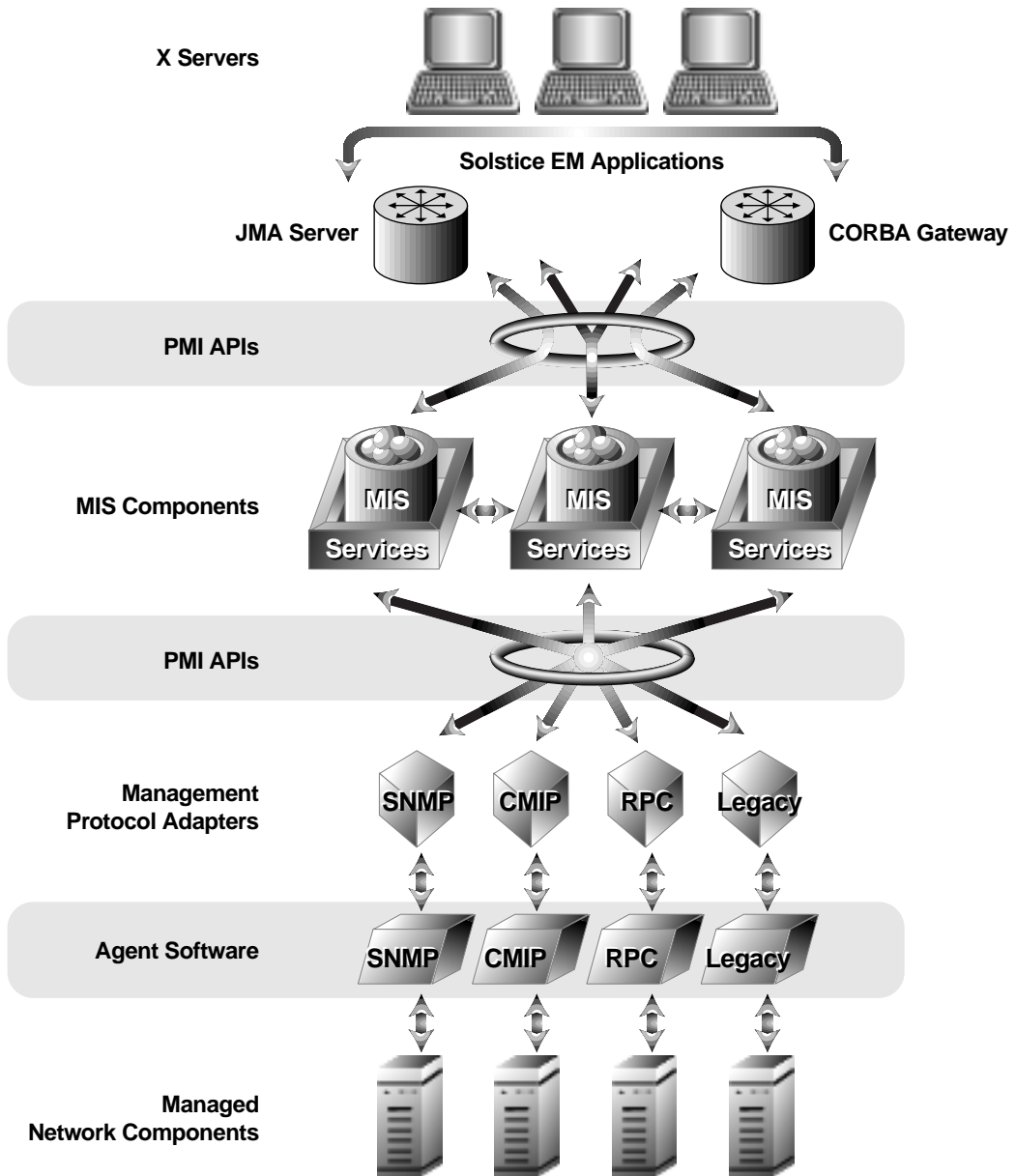


FIGURE 1-1 Solstice EM Architecture Overview

## 1.3.2 Solstice EM Network Management Tools

Solstice EM network management tools can be divided into three general categories:

- **General management** – Tools for day-to-day network management tasks—these are the tools you will use most often.
- **MIS** – Tools and services for running and managing MIS servers and databases—once MIS services have been started on one or more MIS hosts, you will use these tools for occasional MIS database maintenance chores.
- **Application customization and development** – Tools for customizing the Solstice EM environment and creating custom management applications.

The following table briefly describes the common Solstice EM tools you are likely to use often. The tools in the table are divided into two categories: general network management tools you will use on a day-to-day basis and administration tools. A quick-reference table describing all of the Solstice EM tools is provided at the end of this chapter, in Section 1.7 “Solstice EM Tools—Complete Listings” on page 1-22.

**TABLE 1-1** Common Solstice EM Tools

Tool	Description	More Information
<i>General Management Tools</i>		
Alarms	Configure, view, and respond to alarms posted against managed objects.	<i>Managing Your Network</i>
Data Collections	Create data requests to collect performance data about selected managed objects.	<i>Managing Your Network</i>
Grapher	Graph data from several Solstice EM tools.	<i>Managing Your Network</i>
Event Logs	View and manage logs and log objects.	<i>Managing Your Network</i>
Network Discovery	Automatically detect components on your network and populate the MIS with managed objects representing those components; a monitor function dynamically updates the MIS as components are added and removed from your network.	<i>Managing Your Network</i>
Network Tools	Customizable window providing access to Solstice EM and other tools; you can add and remove Solstice EM tools, third-party tools, or your own tools to this window; provides a handy starting point for Solstice EM.	<i>Managing Your Network</i>

**TABLE 1-1** Common Solstice EM Tools (*Continued*)

<b>Tool</b>	<b>Description</b>	<b>More Information</b>
Network Views	Graphical tool for visualizing, organizing, and managing your network; most other Solstice EM tools can be run directly from Network Views; provides a convenient, customizable, point-and-click way to view and respond to alarms, and configure object properties. Views of your network can be superimposed over cartographically accurate map backgrounds, making it easy to determine the physical location of network components and faults.	<i>Managing Your Network</i>
Object Properties	View, create, and modify managed objects and object properties; commonly invoked from Network Views.	<i>Managing Your Network</i>
RPC/CMIP Data	Get, set, view, and modify properties for CMIP- and RPC-managed objects.	<i>Managing Your Network</i>
<b>Administration Tools</b>		
Administration	Customizable window providing access to Solstice EM administration tools.	<i>Customizing Guide</i>
Advanced Requests	Create Nerve Center request templates; used by Solstice EM to poll for object properties or receive notifications from managed object agents, and then generate responses based on the data received.	<i>Customizing Guide</i>
Automatic Management	Configure the MIS to launch and stop event requests automatically.	<i>Managing Your Network</i>
DB Backup/Restore	Back up and restore MIS databases.	<i>Customizing Guide</i>
MIS Manager	Configure MIS communications and parameters.	<i>Customizing Guide</i>
Object Editor	View, create, and delete managed object attributes directly in the MIS.	<i>Customizing Guide</i>
Security	Manage user access to network management tools and managed objects.	<i>Managing Your Network</i>
SNMP MIB Browser	View attributes and modify SNMP attribute values for SNMP MIBs.	<i>Managing Your Network</i>
Topology Import/Export	Import or export an ASCII version of all or part of a MIS database; useful for recreating or transferring an MIS topology on another host.	<i>Customizing Guide</i>

---

## 1.4 Basic Enterprise Manager Concepts

Before you start using Solstice EM to manage the components on your network, it is useful to review some basic network management concepts as they relate to Solstice EM.

This section comprises the following topics:

- “Network Management Software” on page 1-10
- “Agents and Stations” on page 1-10
- “Management Information Servers” on page 1-12
- “Network Management Protocols” on page 1-17

### 1.4.1 Network Management Software

In the context of Solstice EM, *network management software* refers to one or more software tools, like the Solstice EM suite, that:

- Provide user interfaces through which network management tasks can be performed.
- Issue requests to network devices—that is, ask a given device to take some action, typically to provide some specific information to the manager.
- Receive responses to requests.
- Receive unsolicited information—called *notifications*—from network components concerning component status, such as problems, abnormalities, and changes in the managed environment.

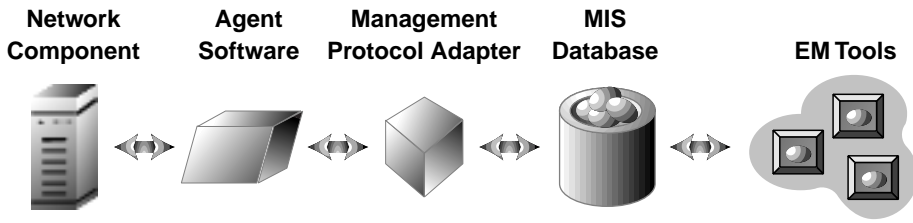
The Solstice EM tools function as network management software for various network management functions. For example, the Solstice EM Alarms tool lets you create and manage alarms for monitoring component status.

### 1.4.2 Agents and Stations

Rather than communicating directly with network components, Solstice EM communicates through software *agents*—“middlemen”—that are specifically configured to understand the particular kinds of information and settings a given network component can receive or provide.

In network management jargon, a *station* is a network management software component that communicates with one or more agents. In the case of Solstice EM, the station component is the MIS. For example, as illustrated in Figure 1-1, a Solstice

EM tool sends a request to an agent via the MIS and a Management Protocol Adapter (MPA). The agent, in turn, passes that request to the network component. On the return trip, the component's response is passed first to the agent, then to the MIS by means of the MPA, and then finally back to the Solstice EM tool. Solstice EM handles the translation between various agent protocols transparently—for most management tasks, users do not need to know what type of agent is associated with a given network component.



**FIGURE 1-2** Agent Communications Overview

Every network component managed by Solstice EM has an associated software agent. In some cases, the agent software is embedded in the component—for example, burned into a component's ROM. In most cases, however, the agent software resides on a host machine to which the component is connected, and provides services for a related set of components.

Solstice EM is based on the ISO-standard agent/station network management model. The strength of this model is that your network management software does not need to maintain configuration information for every network component available on the market. As new types of components are added or upgraded on your network, the agent software that travels with a given component is able to communicate the new configuration information to the management software.

Solstice EM supports the following common agent protocols:

- CMIP – Common Management Information Protocol
- SNMP – Simple Network Management Protocol
- SNMPv2c – Simple Network Management Protocol, version 2
- RPC – SunNet Manager Remote Procedure Call

Solstice EM also provides full conformance with Telecommunications Management Networks (TMN) standards. See Section 1.4.4 “Network Management Protocols” on page 1-17 for more information about network protocols supported by Solstice EM.

---

**Note** – Solstice EM installation includes by default a set of Solstice Enterprise Agents (SEA), which allow you to communicate with components configured for legacy SunNet/Site/Domain Manager environments. Other agents may be installed as well, depending on your package options. See the *Installation Guide* for complete information.

---

### 1.4.3 Management Information Servers

In the Solstice EM environment, a Management Information Server (MIS) is a machine hosting an object-oriented SQL database containing information about every component on your network that is managed by Solstice EM. In this model, physical network components are represented as managed objects in an MIS database.

In general terms, the MIS provides the following services:

- Access control
- Requests
- Connections
- Events and alarms
- Logging
- Object management

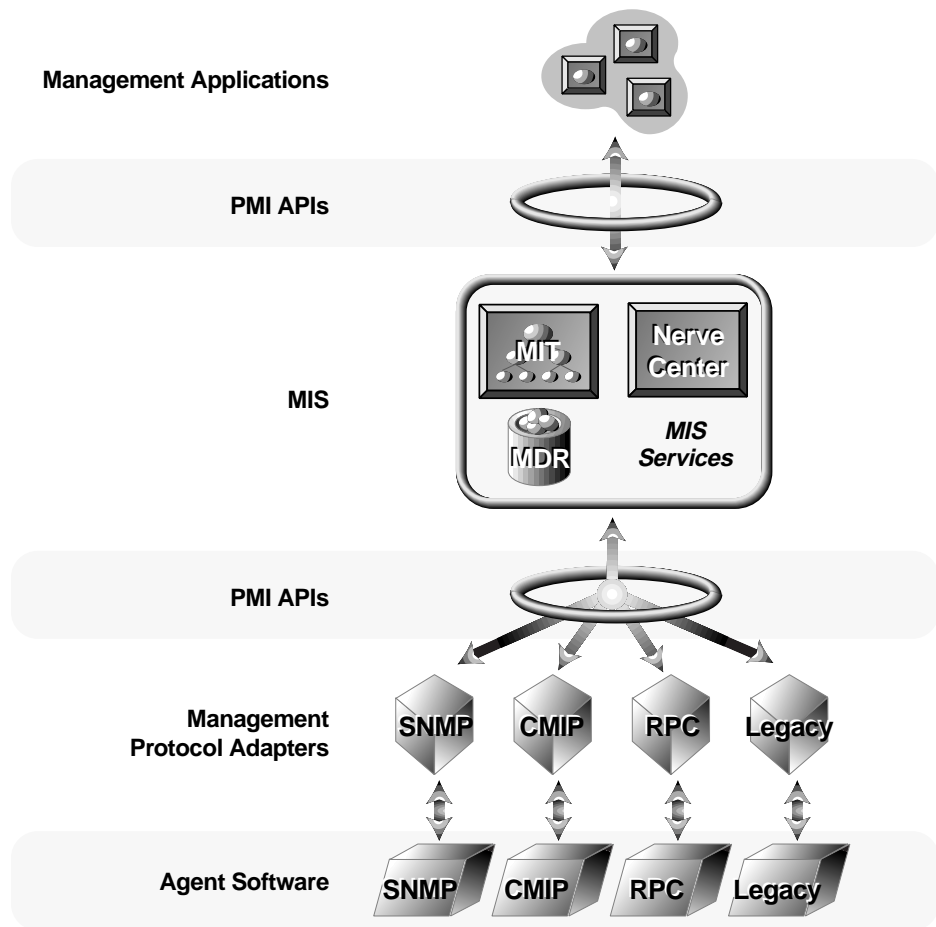
Functionally, the resources on an MIS can be divided into four general categories:

- An MIS database containing information about the components on your network.
- An MIS Nerve Center that provides the logic and methods to actually do something with the information in the MIS—that is, the Nerve Center is the source of requests and responses based on network conditions.
- Portable Management Interface (PMI) APIs and Management Protocol Adapters (MPAs).
- A set of ancillary MIS services that make the information in the MIS database available to network management applications and software agents.

For data security or logical convenience, you can use multiple MIS databases, with one MIS database on each host. Multiple MIS databases can be linked so that all appear as one database to a given user. See the *Customizing Guide* for more information about linking multiple MIS databases.

The figure Figure 1-3 depicts the layers of management information servers.





**FIGURE 1-3** Overview of Management Information Servers

### 1.4.3.1 More About MIS Databases

A Solstice EM MIS database comprises two primary components:

- **Metadata Repository (MDR)** – Maintains information about managed object attributes and properties—that is, the specific configuration settings used by network components. This data encompasses everything from the syntax required to refer to an attribute to the composition of an object package. The language used to describe network components is Guidelines for the Definition of Managed Objects (GDMO), outlined in the ITU X.722 ISO/IEC 10165-4 standard. The MIS allows for dynamic updates to the MDR.

- **Management Information Tree (MIT)** – A tree-like, hierarchical representation of the relationships between network components. For example, a network might have subnetwork branches, from which routers, switches, and hubs are parents to gateways, workstations, and printers. The MIS supports dynamic creation, maintenance, and deletion of objects in the MIT.

### 1.4.3.2 More About the MIS Nerve Center

The MIS Nerve Center provides the logic and methods to interrogate agent software for information about network components, receive notifications from agents, and initiate actions based on network conditions.

Nerve Center activities are based upon user-defined *request templates*, which are rules-based configuration files that tell Solstice EM how to interrogate for network component information, and how to respond to the information received. In this context, the term *request* should not be confused with the common object-oriented use of the term as it relates to `GET` and `SET` methods—that is, a Nerve Center request is a set of programmatic rules, whereas an object-oriented request refers to a specific set of methods for manipulating object properties.

The Solstice EM Advanced Requests tool lets you view, create, and manage Nerve Center Request templates. See the *Customizing Guide* for information about creating automated Nerve Center requests using customized templates.

### 1.4.3.3 More About PMI and MPAs

Although there are potentially many interfaces to Solstice EM, only one is required by the Solstice EM architecture. This primary interface is the high-level Portable Management Interface (PMI). The PMI defines the management protocol, services, and transport mechanisms for all Solstice EM components. Specifically, the PMI provides the following features:

- **Protocol-independent management applications** – Management applications can communicate with managed objects via the PMI regardless of the protocol used by the managed object.
- **Distributed, multi-user access** – Multiple users can access and modify objects and object definitions in the MIS.
- **Proxy agent support** – Proxy agents can use the Management Protocol Adapter (MPA) library to access managed objects over protocols other than CMIP or SNMP.

MPAs translate information between managed objects and the MIS. For example, if you have a network component that uses SNMP, then the SNMP MPA receives data from an SNMP agent, translates the data into the PMI, and sends the data to the MIS.

Solstice EM includes the following MPAs:

- CMIP – Common Management Information Protocol
- SNMP – Simple Network Management Protocol
- SNMPv2c – Simple Network Management Protocol, version 2
- RPC – SunNet/Site/Domain Manager Remote Procedure Call

Solstice EM also supports other MPAs; see the *Developer's Guide* for information about adding MPAs to your Solstice EM environment.

#### 1.4.3.4 Ancillary MIS Services

In addition to the MIS database and Nerve Center, an MIS provides ancillary services that make information about managed objects available and modifiable by network management applications and agent software. These services are invoked at MIS startup with the `em_services` command.

---

**Note** – Solstice EM MIS services are usually run on one or more of the network's workstations. It is not necessary to dedicate a machine to running MIS services, although Solstice EM requires at least one MIS to be running somewhere on the network. As mentioned previously, you can run multiple MISs on a network.

---

The Solstice EM MIS provides the following ancillary services:

- **Protocol and location transparency** – A network management tool provides a managed object name, and the Solstice EM services determine what protocol to use to access the object, and what address to use within that protocol. This means that management clients do not need to know where an object is physically located or what protocol to use to communicate with it.
- **Coordinate requests from multiple tools** – Solstice EM supports concurrent access to MIS data from multiple network management clients.
- **Persistent storage** – Data in the MIS database is not lost when an MIS host is shut down.
- **SNMP traps and events** – Event handling for SNMP traps and events, and a registry mechanism that allows applications and objects to register interest in an event.
- **Log management services** – Keep track of what is happening where on the network. Solstice EM provides detailed logging services, which are maintainable through Solstice EM's Event Logs tool.

### 1.4.3.5 More About MIS Data Access

One of the primary functions of an MIS is to make managed object data available to network management tools and agent software. A related function is to make this data transparently available across multiple MIS machines on multiple subnetworks.

In Solstice EM, all managed objects are accessed through the MIT. There is one global tree, with a single naming scheme for all data. The MIT is constructed according to the rules provided by OMNIPoint™, and has a single `root` branch. The shape of the tree descended from this root branch is arbitrary, and may vary widely from one MIS to another. The tree's structure is hierarchical and based on parent/child containment relationships—that is, below any given object are one or more related subordinate objects.

A Solstice EM MIS makes MIT data accessible both through the naming conventions that come from the managed resources it describes, and from a resource-independent naming convention, in which identifiers are specified using Fully Distinguished Names (FDNs). FDNs enable an Solstice EM MIS to provide transparent access to managed objects.

Managed objects in the Solstice EM environment may be stored *locally*, in an MIS database. However, Solstice EM also supports access to *remote* objects that are stored outside a given MIS. When representing a remote object, a Solstice EM MIS stores information about that object's physical location, along with a description of the address and protocol required to access that object. When getting or setting properties for a given object, Solstice EM handles the address and protocol resolution transparently—that is, without user intervention—whether the object is local or remote to the MIS.

### 1.4.3.6 More About Object Orientation

As mentioned previously, Solstice EM MIS services are based on an ISO-standard ASN.1 (Abstract Syntax Notation One) object-oriented architecture. Specifically, Solstice EM:

- Describes managed objects in terms of OMNIPoint and ISO terminology
- Uses C++ objects for internal storage and manipulation of network data

Some object-oriented terms as they relate to Solstice EM are:

- **Class** – C++ classes, as described in the *Annotated C++ Reference Manual* (Margaret Ellis and Bjarne Stroustrup; Addison-Wesley Publishing Co., Reading, MA; copyright 1990 by AT&T Bell Laboratories).
- **Instance** – Memory that is allocated for a C++ class according to its definition. A variable name is usually associated with a particular instance of a class.

- **Managed resource** – An actual physical device or entity that exists in a network or system. This is consistent with the OSI/Network Management Forum (NMF) definition of the term.
- **Managed Object (MO)** – A set of services and attributes that describes a type of managed resource. This is also consistent with the OSI/NMF definition of the term.
- **Managed Object Class (MOC)** – In the Solstice EM development environment, this term refers to the internal representation of a managed object, as described by the OSI/NMF. An MOC is based on the GDMO description, which could itself be a translation of an SNMP MIB or SunNet Manager schema description—that is, the MOC represents the attributes and behaviors for particular types of manageable objects. The MOC defines the type of data stored and the behaviors that can be taken, but does not represent the actual data for any managed object. The MOC is the internal representation used by the Solstice EM MIS.
- **Managed Object Instance (MOI)** – Relates to a managed object class in the same way as an instance relates to a class—that is, where the MOC determines the type of attributes and behaviors available to operate on an object of this type, and MOI refers to actual data that represents an object being managed by the MIS. An MOI is also an internal representation used by the Solstice EM MIS.

## 1.4.4 Network Management Protocols

In order to be able to pass management data from component to agent to MIS to management tool and back again, all components in the environment must agree on and understand how and what data is being exchanged. The rules that define such exchanges are called *protocols*.

As mentioned previously, Solstice EM is based on the ISO-standard agent/station network management model, and supports the following common protocols:

- CMIP – Common Management Information Protocol
- SNMPv1 – Simple Network Management Protocol
- SNMPv2c – Simple Network Management Protocol version 2
- RPC – SunNet/Site/Domain Manager Remote Procedure Call

SNMPv2c support enables the Solstice EM architecture to manage SNMPv2c agents and view SNMPv2c configured devices in the SNMP browser.

Solstice EM also provides full conformance with Telecommunications Management Networks (TMN) standards.

SNMP and RPC are network management protocols used to manage resources in a TCP/IP network environment. CMIP is the protocol used in ISO networks. Both protocols specify ASN.1 as the language used to encode and decode object request and response messages.

---

**Note** – When you install Solstice EM, you are asked if you want support for IP management, CMIP management, or both. The choice you make depends on the types of devices on your network, and the network management protocols they support. See Chapter 8 “Gathering Attribute Data” for more information about network management protocols.

---

#### 1.4.4.1 More About RPC

Solstice EM includes a suite of agents developed for the SunNet/Site/Domain Manager (SNM) platform. These agents communicate with Solstice EM using RPC protocols, and are included primarily to provide a migration path from SNM installations to Solstice EM.

In addition to migrating to Solstice EM, however, SNM agents communicating over RPC can be a useful part of your network management strategy. Specifically, SNM agents can act as *proxies* for communicating via older protocols. See the *Customizing Guide* for more information about working with RPC and SNM.

#### 1.4.4.2 More About MIBs

Part of the SNMP protocol includes attribute definition files called Management Information Base (MIBs). MIBs define:

- *Attributes* or types of data that can be supplied by an agent to a manager
- *Actions* performed by an agent that can be requested by a manager
- *Behavior* exhibited by the agent
- *Notifications*—unsolicited information—the agent can send to a manager

The ISO standards organization defines a MIB in ISO/IEC 7948-4 as follows: “The conceptual repository of management information within an open system.” A network management package normally contains management information describing each type of agent the manager is capable of managing. This information typically includes Internet MIB definitions and ISO GDMP definitions for managed objects and agents. An agent typically presents or contains management information for one type of device, although this information can include descriptions and data for several types of devices. See Appendix B and Chapter 8” for more information about MIBs.

---

## 1.5 Solstice EM Application APIs

In addition to the network management tools shipped with Solstice EM, you can define your own tools and applications to work with Solstice EM through the Application Programming Interfaces (APIs) included with Solstice EM.

If an application developer also provides access to a managed object type not previously known to the MIS, the MIS must be informed of the Managed Object Class through the use of GDMO ASN.1 documents.

The Solstice EM APIs provide a rich set of functions for the application programmer. The libraries, written in C++, contain the objects and methods necessary to communicate with the MIS and obtain information about the managed resources it controls. The APIs provide the following services:

- Initialization, including establishment of a distributed message passing interface to the MIS
- Event subscription
- Remote caching and cache control
- Local object cache management for applications
- Encoding and decoding of parameters into ASN.1
- Encoding and encapsulation of data into a format (message class) passed to the MIS

# 1.5.1 API Modules

The Solstice EM APIs consist of several different groupings or modules, as summarized in the following table. See the Solstice EM *Application Development Guide* for detailed information about developing applications that interact with Solstice EM.

TABLE 1-2 Solstice EM API Modules

API Module	Description
High-level PMI (Programming Management Interface)	For most applications, all interaction with the MIS can be handled through the high-level protocol-independent functions of the PMI. These functions hide the encoding/decoding of ASN.1 values, and provide CMIS-like messages used in communication with the MIS and managed objects (through the MIS). It also provides for initialization and for event subscription and propagation.
Low-level PMI	Used to exchange messages between the Solstice EM MIS and client services using CMIS-like messages (M-GET, M-SET, M-CREATE, M-DELETE, M-EVENT-REPORT, M-CANCEL-GET, and M-ACTION).
Application-to-Application API	Allows applications to send messages to other Solstice EM applications through an <code>emApplicationInstance</code> object.
Grapher API	Allows developers to create graphical representations of data.
Nerve Center Interface (NCI) Library	A programmatic interface for controlling Nerve Center operation. The NCI library enables applications to create, edit, and launch Nerve Center requests.
Object Services API	Allows developers to access services provided by the Solstice EM MIS to implement intra-object behaviors or specialized behaviors.
Topology API	Allows developers to create applications for the Solstice EM environment without learning the details of the MIT topology naming tree.
Viewer API	Allows applications to communicate with the Solstice EM Network Views tool to control specific Network Views features. This allows developers to leverage Network Views functionality and integrate their applications with Network Views.



## 1.5.2 Application Development Support Tools

In addition to the API classes and methods described in the preceding table, Solstice EM includes the following application development support tools:

- **Object Development Tools (ODT)** – Provide a simple and automated framework developers can use to add and write behaviors for managed objects that reside in the MIS. See the Solstice EM *Application Development Guide* for detailed information.
- **Compilers** – Required by developers and, in some cases, system administrators. The compilers provide a means by which you add new managed object definitions to the MIS. Solstice EM includes the following compilers:
  - **ASN.1** (`em_asn1`) – Compile descriptions of managed objects into the MDR. These descriptions are provided as ASN.1 documents.
  - **GDMO** (`em_gdmo`) – Compile new GDMO object descriptions and then add them to the MDR.
  - **Concise MIB** (`em_cmib2gdmo`) – Convert object descriptions written in Concise MIB format to GDMO for use in Solstice EM.
  - **Schema** (`em_snm2gdmo`) – Convert object descriptions written in SunNet Manager schema format to GDMO for use in Solstice EM.
- **em\_debug** – Solstice EM includes a dynamic debugging function that helps you track information going in to and out of the MIS.

---

## 1.6 Related Reading

Depending on what you want to do in Solstice EM, one or more of the following Solstice EM manuals may interest you:

- *Installation Guide* – Complete instructions on installing all Solstice EM components and utilities, including agent software.
- *Customizing Guide* – Detailed information about advanced Solstice EM configuration and customization.
- *Management Information Server (MIS) Guide* – Advanced information about MIS servers.
- *Developing C++ Applications Guide* – Information for developers writing custom applications that can be integrated with Solstice EM.
- *CORBA Gateway Administration Guide* – Information on installing, configuring and using the SEM CORBA ToolKit to build and package the SEM CORBA Gateways.
- *Troubleshooting Guide* – Solutions to problems you may have with Solstice EM and explanations of error messages you may encounter while using Solstice EM
- *Glossary* – A glossary of network management terms as they relate to Solstice EM

## 1.7 Solstice EM Tools—Complete Listings

The remainder of this chapter is a quick-reference table that briefly describes all of the Solstice EM network management tools, along with pointers to the books in which you can find more detailed information.

Refer to the preceding sections in this chapter for information about general Solstice EM network management concepts, and explanations of how the major Solstice EM tools work together.

The following table lists the Solstice EM tools, sorted by binary name. All tools listed here are located by default in `/opt/SUNWconn/em/bin` (`$EMHOME/bin`) directory.

**TABLE 1-3** Solstice EM Tools – Complete List, Sorted by Binary Name

Binary Name	Tool Name	Description	More Information
build_oid	Build Object IDs	SunNet Manager (SNM) SNMP utility; creates an Object ID Database ( <code>/var/usr/SUNWconn/snm/oid.dbase</code> ).	<i>Customizing Guide</i>
build_tt	Build Textual Convention Types	Builds the textual convention types database; used by the <code>mib2schema</code> utility to look for new IMPORT definitions local to a MIB.	<i>Developing C++ Applications Guide</i>
create_admin	Create EM Administrator	Internal utility to create an EM administrator accounts. EM administrators are accounts other than <code>root</code> that can run <code>em_services</code> to start and stop EM MIS services.	<i>Management Information Server (MIS) Guide</i>
db_services	Initialize Database Services	Initializes MIS database services; usually run as part of the <code>em_services</code> command.	<i>Management Information Server (MIS) Guide</i>
em	Network Tools	Primary EM tools window; EM and custom network tools can be started, added, and removed from this window.	This Guide
em_accesscmd	Access Control – command line interface	Command-line Access Control tool; lets you manage user access to EM tools and objects.	This Guide

**TABLE 1-3** Solstice EM Tools – Complete List, Sorted by Binary Name *(Continued)*

Binary Name	Tool Name	Description	More Information
em_accessmgr	Access Control – graphical interface	Graphical Access Control tool.	This Guide
em_add_db_server	Add Database Server	Lets you specify an MIS database server to use instead of or in addition to the default.	<i>Management Information Server (MIS) Guide</i>
em_admintool	Administration	Access advanced administration functions; for example, MIS connections and parameters, database backup and restore, request template designer, etc.	<i>Customizing Guide</i>
em_alarmmgr	Alarms	View and manage object alarms.	This Guide
em_asn1	ASN.1 Compiler	ASN.1 object compiler.	<i>Management Information Server (MIS) Guide</i>
em_autod	Automatic Management Daemon	Automatic management daemon; monitors creation and deletion of MIS objects; starts and stops requests when objects are added and deleted.	<i>Management Information Server (MIS) Guide</i>
em_autoexd	Database Table Extender	MIS daemon that automatically extends database tables when they get full.	<i>Management Information Server (MIS) Guide</i>
em_automgr	Request Controllers	Automatic management configuration tool; used in conjunction with em_autod.	<i>Management Information Server (MIS) Guide</i>
em_auxdb	MIS External Database Access daemon	Internal daemon acting as a co-processor for the em_mis process to set up database access control permissions on user exposed tables.	<i>Management Information Server (MIS) Guide</i>
em_clear_alarms	Clear Alarms – command line interface	Command-line utility for clearing alarms against a specified range of toponodes.	This Guide
em_cmib2gdmo	Concise MIB Compiler	Converts MIB files in Concise MIB format to GDMO and ASN.1 formats.	<i>Management Information Server (MIS) Guide</i>
em_cmip	CMIP Management Protocol Adapter	Implements CMIP MPA functions; starts during product installation.	<i>Management Information Server (MIS) Guide</i>

**TABLE 1-3** Solstice EM Tools – Complete List, Sorted by Binary Name *(Continued)*

Binary Name	Tool Name	Description	More Information
em_cmipautoreg	CMIP Autoregistration	Automatically registers CMIP agents in the MIS.	<i>Management Information Server (MIS) Guide</i>
em_compose_all	Compose/Load GDMO Bindings	Compose and load all name bindings from a GDMO file.	<i>Management Information Server (MIS) Guide</i>
em_compose_oc	Instantiate Volatile Class	Instantiates a new MIS object class with volatile data storage.	<i>Management Information Server (MIS) Guide</i>
em_compose_poc	Instantiate Persistent Class	Instantiate a new MIS object class with persistent data storage.	<i>Management Information Server (MIS) Guide</i>
em_datacollector	Data Collections	Create and manage data collection entry objects, and display data gathered from requests.	This Guide
em_datad	Data Collection Daemon	Daemon used in conjunction with em_datacollector.	This Guide
em_dataviewer	RPC/CMIP Data	View and manage RPC, CMIP, and SNM managed objects.	
em_db_abort	Abort Database	Script to abort an Informix database on the specified MIS.	<i>Management Information Server (MIS) Guide</i>
em_db_create	Create Database	Script to create a new Informix database on the specified MIS	<i>Management Information Server (MIS) Guide</i>
em_db_drop	Drop Database Tables	Script to drop log or non-log tables from an Informix database on the specified MIS.	<i>Management Information Server (MIS) Guide</i>
em_db_start	Start Database Server	Script to start a database server on the specified MIS.	<i>Management Information Server (MIS) Guide</i>
em_db_stop	Stop Database Server	Script to stop the database server on the specified MIS.	<i>Management Information Server (MIS) Guide</i>
em_dbarchive	Database Backup/Restore	Graphical administration tool for backing up and restoring MIS databases.	<i>Management Information Server (MIS) Guide</i>

**TABLE 1-3** Solstice EM Tools – Complete List, Sorted by Binary Name *(Continued)*

Binary Name	Tool Name	Description	More Information
em_dbbackup	Database Backup – command-line interface	Command-line interface for MIS database backup.	<i>Management Information Server (MIS) Guide</i>
em_dbrestore	Database Restore – command-line interface	Command-line interface for MIS database restore.	<i>Management Information Server (MIS) Guide</i>
em_debug	EM Debugging Tool	Command-line debugging tool that supports the EM remote dynamic debugging feature.	<i>Cooperative Consoles Administration Guide</i>
em_discover	Network Discovery	Discover components on your network and update the MIS database.	This Guide
em_edc	Event Distribution System	Distributes events from event sources to event listeners.	<i>Management Information Server (MIS) Guide</i>
em_gdmo	GDMO Compiler	GDMO compiler; lets you extend EM capabilities with new GDMO object class descriptions.	<i>Customizing Guide</i>
em_grapher	Grapher	Create graphs from alarm and agent data.	This Guide
em_help	Help	EM help system.	<i>Online Help</i>
em_imex	Log File Import/Export	Import and export log objects from and to ASCII files.	This Guide
em_java2gdmo	Java GDMO Compiler	Compile Java classes in GDMO format.	<i>Customizing Guide</i>
em_jdmk_config	Configure Java Agents	Configure EM to work with Java-based agents.	<i>Customizing Guide</i>
em_jdmkfwd	Forward Java Events	Forwards Java events to the EM MIS for processing.	<i>Management Information Server (MIS) Guide</i>
em_layout	Network Views Layout	Define how object views are laid out in Network Views; commonly invoked from Network Views.	This Guide
em_load_name_bindings	Load Name Bindings	Loads object name bindings; allows the MIS to resolve MIT object names.	<i>Management Information Server (MIS) Guide</i>

**TABLE 1-3** Solstice EM Tools – Complete List, Sorted by Binary Name *(Continued)*

Binary Name	Tool Name	Description	More Information
em_load_nc_templates	Load Nerve Center Templates	Script that invokes the <code>em_ncimport -file</code> command; loads EM Nerve Center templates.	<i>Management Information Server (MIS) Guide</i>
em_loaddefs	Load Object Definitions	Load MIB, GDMO, and SunNet Manager schema files into the MIS.	<i>Management Information Server (MIS) Guide</i>
em_log	Initialize Log Server	Initializes log server MPA functions.	<i>Customizing Guide</i>
em_log2hist	Save Log Entries	Saves logs in history files.	This Guide
em_log2rdb.ifmx	Transfer Log Histories Daemon – Informix	Daemon that reads and transfers log histories to an Informix database.	This Guide
em_log2rdb.orcl	Transfer Log Histories Daemon – Oracle	Daemon that reads and transfers log histories to an Oracle database.	This Guide
em_log2rdb.sybs	Transfer Log Histories Daemon – Sybase	Daemon that reads and transfers log histories to an Sybase database.	This Guide
em_login	Login Daemon	Listens for EM connection requests for password authentication.	<i>Management Information Server (MIS) Guide</i>
em_logmgr	Event Logs	Create, modify, and delete log objects.	This Guide
em_logview	View Logs	View logs and log objects.	This Guide
em_mis	MIS Services Core	Primary EM services; commonly invoked from the <code>em_services</code> command.	<i>Management Information Server (MIS) Guide</i>
em_mismgr	MIS Manager	Manage MIS parameters and connections.	<i>Management Information Server (MIS) Guide</i>
em_mpa_jdmk	Initialize JDMK MPA functions.	Initializes JDMK MPA functions on the MIS.	<i>Management Information Server (MIS) Guide</i>
em_mpa_rpc	Initialize RPC MPA functions.	Initializes RPC MPA functions on the MIS.	<i>Management Information Server (MIS) Guide</i>

**TABLE 1-3** Solstice EM Tools – Complete List, Sorted by Binary Name *(Continued)*

Binary Name	Tool Name	Description	More Information
em_mpa_snmp	Initialize SNMP MPA functions.	Initializes SNMP MPA functions on the MIS.	<i>Management Information Server (MIS) Guide</i>
em_ncam	Nerve Center Daemon	Daemon that handles nerve center actions, such as sending email or executing UNIX commands.	<i>Customizing Guide</i>
em_ncexport	Nerve Center Export	Export Nerve Center templates to an ASCII file.	<i>Customizing Guide</i>
em_ncimport	Nerve Center Import	Import Nerve Center templates that have been previously exported with em_ncexport.	<i>Customizing Guide</i>
em_nnadd	Global Nickname Service Addition	Enable a global nickname server on the MIS; generally started with em_services.	<i>Developing C++ Applications Guide</i>
em_nnconfig	Global Nickname Configuration	Populate the global nickname translation server.	<i>Developing C++ Applications Guide</i>
em_nnmpa	Global Nickname Service Daemon	Starts the global nickname translation server.	<i>Developing C++ Applications Guide</i>
em_ns_server	Debug Nickname Services	Debug global nickname translation services.	<i>Developing C++ Applications Guide</i>
em_obcodegen	Object Code Generator	Used to generate object behavior code from GDMO and ASN.1 definitions.	<i>Developing C++ Applications Guide</i>
em_obed	Object Editor	View and edit objects in the MIT; see also em_oct.	<i>Customizing Guide</i>
em_objop	Object Operations Utility	Command-line utility for sending CREATE, SET, DERIVE, and DELETE requests; primarily used by init_platform to create and modify MIS objects at MIS startup.	<i>Management Information Server (MIS) Guide</i>
em_oct	Network Views Object Configuration Tool	View, modify, and create managed objects; commonly run from a Network Views window; see also em_obed.	This Guide
em_panel	Network Tools	Starting point for EM general network management applications; usually invoked with the em command or em -host <i>hostname</i>	This Guide

**TABLE 1-3** Solstice EM Tools – Complete List, Sorted by Binary Name *(Continued)*

Binary Name	Tool Name	Description	More Information
em_purged	Alarm Deletion Daemon	Periodically deletes alarms based on severity, stat, time, etc.	This Guide
em_purgemgr	Alarm Deletion Controller	Sets up conditions for em_purged to delete alarms.	This Guide
em_reqedit	Request Template Designer	View, modify, create, and delete Nerve Center request templates.	<i>Customizing Guide</i>
em_restart	Restart MIS Services	Restart MIS services.	<i>Management Information Server (MIS) Guide</i>
em_services	Initiate MIS Services	Initiate MIS services; starts the MIS server and several related daemons.	<i>Management Information Server (MIS) Guide</i>
em_simplerequests	Network Views Basic Requests	View, modify, and create simple MIS request templates; generally invoked from Network Views.	This Guide
em_snm2gdmo	SNM Schema to GDMO Compiler	Convert SNM schema files to GDMO descriptions.	<i>Customizing Guide</i>
em_snm_type_import	Import SNM Object Types	Import SNM object types into the EM environment.	<i>Customizing Guide</i>
em_snmdb_import	Import SNM Topology	Imports SNM topology databases into an EM MIS.	<i>Management Information Server (MIS) Guide</i>
em_snmfwd	Forward SNM Events	Forwards SNM events to the EM MIS for processing.	<i>Management Information Server (MIS) Guide</i>
em_snmp-trap	Listen for SNMP Traps Daemon	Daemon that listens on port 162 for SNMP traps.	<i>Management Information Server (MIS) Guide</i>
em_snmpbrowser	SNMP Data	Get, set, view, and modify SNMP agent attributes.	This Guide
em_sql	Log In to SQL Database	Login process for SQL databases.	<i>Customizing Guide</i>
em_srm	Simple Request System daemon	Internal Simple Request system daemon; dispatches simple requests on behalf of the user.	<i>Customizing Guide</i>
em_startup	Start MIS Server	Start the MIS server; usually invoked as part the em_services command.	<i>Management Information Server (MIS) Guide</i>



**TABLE 1-3** Solstice EM Tools – Complete List, Sorted by Binary Name (*Continued*)

Binary Name	Tool Name	Description	More Information
em_topo_args	Modify Toponodes	Command-line interface for modifying topoNode objects.	<i>Customizing Guide</i>
em_topoimex	Topology Import/Export	Import or export MIT topology information.	<i>Management Information Server (MIS) Guide</i>
em_topoimex_BC	Convert Legacy Topology Information	Converts topology information from prior versions of EM.	<i>Customizing Guide</i>
em_trapd	Initialize Topology Services	Initializes topology services on the MIS; commonly invoked as part of em_services.	<i>Customizing Guide</i>
em_viewer	Network Views	View, organize, modify, and create managed objects.	This Guide
emenv.csh	Environment Configuration – C Shell	Source this file to configure EM environment variables, such as \$EMHOME, license server, etc.; C Shell environment only.	This Guide
emenv.sh	Environment Configuration – Korn/Bourne Shell	Source this file to configure EM environment variables, such as \$EMHOME, license server, etc.; Korn or Bourne shell.	This Guide
get_local_host	Find Local MIS Host	Display the name of the current local MIS host.	<i>Customizing Guide</i>
hyperhelp	Help Viewer	Bristol HyperHelp™ Viewer; EM online help is in HyperHelp format.	This Guide
jme_jre	JME Services helper script	Helper script for jme_services; do not invoke directly.	<i>MIS Guide</i>
jme_services	JME Services	Start and stop EM Java daemons	<i>MIS Guide</i>
mib2schema	SNMP MIB to SNM Schema compiler	Convert SNMP MIB files to SNM scheme format.	<i>Customizing Guide</i>
snm_br	Results Browser	List RPC, CMIP, or SNMP data collected with the Data Collections tool.	<i>Customizing Guide</i>
snm_cmd	Manage SNM Agents – command-line interface	Command- line manager for Site/ SunNet/Domain Manager agents.	<i>Customizing Guide</i>
snm_cmdtool	Run Command from SNM Session	Run an UNIX command from an SNM session.	<i>Customizing Guide</i>

**TABLE 1-3** Solstice EM Tools – Complete List, Sorted by Binary Name *(Continued)*

Binary Name	Tool Name	Description	More Information
snm_exec	Execute command via EVAL from SNM	Uses the Bourne shell's eval to execute an UNIX command from an SNM session.	<i>Customizing Guide</i>
snm_gr	Grapher	Display and graph SNM data.	<i>Customizing Guide</i>
snm_kill	Stop SNM Agent Requests	Stop one or more SNM agent requests.	<i>Customizing Guide</i>
snm_version	SNM Version Information	Displays information about the current version of SunNet Site/Domain Manager software.	
v2mib2schema	SNMP2 MIB to Schema Compiler	Convert SNMP2 MIBs to SNM schema format.	<i>Customizing Guide</i>
var-install	Install EM Packages on Remote	Install EM packages on another machine.	<i>Installation Guide</i>
var-obj-install	Install EM object Definitions	Install EM object definitions.	<i>Customizing Guide</i>

# Getting Started With Solstice EM

---

The Solstice Enterprise Manager™ (Solstice EM) Network Tools window is the launchpad from which you start all Solstice EM management tools for monitoring your network components. By default, Network Tools is displayed when you start Solstice EM.

This chapter comprises the following topics:

- Section 2.2 “Setting Up the Solstice EM Environment” on page 2-3
- Section 2.3 “Starting Solstice EM” on page 2-4
- Section 2.4 “Starting Individual Tools” on page 2-5
- Section 2.5 “Reconnecting to the MIS” on page 2-7
- Section 2.6 “Accessing Online Documentation” on page 2-7
- Section 2.7 “Adding and Removing Tools” on page 2-9
- Section 2.8 “Modifying Tool Configurations” on page 2-11

---

## 2.1 Overview

Network Tools provides access to the Solstice EM tools you will use most often for configuring, updating, and managing your network. You can, however, add and remove other Solstice EM and custom-developed network management tools to meet your specific needs.

By default, the core tools described in the following table can be started from the Network Tools window.

**TABLE 2-1** Core Solstice EM Tools

Tool Name	Description
Network Views	Monitor and control network and system components.
Alarms	Create and monitor event alarms for Solstice EM managed resources.
Network Discovery	Discover the physical and logical resources on your network.
Event Logs	Create Data Collection Entry objects.
Data Collections	Create Data Collection Entry objects.
Administration	<p>Provide access to the following administrative tools:</p> <ul style="list-style-type: none"><li>• MIS Connections – Set up communication between local and remote MIS servers.</li><li>• MIS Parameters – Configure system parameters for protocol adapters, MIS-to-protocol adapters, access control, and Alarm Manager.</li><li>• Database Backup/Restore – Create and restore backup copies of the MIS.</li><li>• Security – Control user access to applications and managed objects.</li><li>• Request Controllers – Define, start, and stop agents to monitor network resources.</li><li>• Network View Import/Export – Export and import topology information to and from an ASCII file.</li><li>• Automatic Management – Configure the MIS to launch and stop event requests automatically.</li><li>• Design Advanced Requests – Create query requests for monitoring managed objects on your network.</li></ul> <p>Load Data Definitions – Convert data definitions, such as SNM schema and MIB files, to GDMO format and load the data definitions into the MIS.</p>
Documentation	Access the complete Solstice EM documentation suite.

## 2.1.1 Related Files

- `/opt/SUNWconn/em/config/em_panel.cf` – Solstice EM configuration file.
- The `emenv` script – To set all necessary environment variables.
- The `em_login` daemon – UNIX process for connecting to the MIS servers.

## 2.1.2 Related Tasks

- Chapter 3 "Discovering Network Components"
- Chapter 4 "Viewing Network Components"
- Chapter 5 "Managing Alarms"
- Chapter 6 "Controlling User Access"
- Chapter 7 "Automating Nerve Center Requests"
- Chapter 8 "Gathering Attribute Data"
- Chapter 9 "Viewing Collected Data"
- Chapter 10 "Graphing Collected Data"
- Chapter 11 "Examining Log Entries"
- Appendix A "Integrating Solstice Enterprise™ SyMON System Monitor With Solstice EM"
- Appendix B "Managed Object Definitions"

---

## 2.2 Setting Up the Solstice EM Environment

Before starting and using Solstice EM, you may need to set certain environment variables that are used by the system. An easy way to set all the environment variables is to run the `emenv` script.

You can also start Network Tools and connect to a remote MIS by setting the `$EM_SERVER` environment variable to the name of the remote host where the MIS is running. Then at the command line, enter the `em` command with no options.

---

**Note** – Environment variables cannot be set from Network Tools. If your third party or custom-developed application requires certain environment variable settings, you can set these from a script and then start Network Tools from that script.

---

If you will be running any of the Solstice EM executables that reside in the `/opt/SUNWconn/em/bin` directory individually, you should run the `emenv` script first.

At a system prompt, execute the following command:

- For C-shell users: `source /opt/SUNWconn/em/bin/emenv.csh`
- For shell or Korn shell users: `. /opt/SUNWconn/em/bin/emenv.sh`

---

## 2.3 Starting Solstice EM

All Solstice EM tools rely on a connection with the kernel—called the Management Information Server or MIS—for their data. All Solstice EM tools can connect to a MIS on a local or remote machine. When reading the descriptions of the tools in this manual, keep these facts in mind:

- A tool must have a connection to a running MIS.
- A MIS can be on a local or remote machine.

If you invoke an application without the `-host` option and with the `EM_SERVER` variable not set, the application attempts to connect to a MIS on the local machine.

Users need a connection access right to connect to a MIS. The connection access rights are stored in the user profiles in the MIS. The MIS checks the user's privileges to determine whether or not to grant or deny the connection. The `em_login` daemon on the MIS server is the UNIX process that listens to all MIS connection requests for password authentication. The user's password is verified when starting any Solstice EM tool. Users are not prompted to enter their login password under the following conditions:

- The connection is to the local MIS server
- The user is logged in as root
- The user has security trustee status

### ▼ To Use Solstice EM

---

**Note** – Throughout this guide, C-shell syntax is used for specifying the environment variable. Use the syntax appropriate for your shell.

---

**1. Type of the following command at a system prompt:**

```
em [-host remote_MIS_machine]
```

For example: `em -host zircon`

**2. If prompted, type your user name and password.**

The Network Tools window is displayed.

**3. Click any tool icon to start the tool and perform any network management operation.**

If Security was enabled either during installation, or when configuring Solstice EM for deployment in your company, and you are not logged in as root, you may have restricted access to some of the tools and managed objects, depending on your access privileges controlling access to the Solstice EM tools.

**4. Click File->Exit when you have finished working with Solstice EM.**

**See Also:**

- “Starting Individual Tools” on page 2-5
- “System Variables Used by Solstice EM” on page 2-13
- “Solstice EM Environment Variables” on page 2-14
- “The Network Tools Window” on page 2-15

---

## 2.4 Starting Individual Tools

In most cases, you start the Solstice EM tools from the Network Tool window. However, there may be circumstances—such as executing scripts—when you want to start individual Solstice EM tools. The following table lists the executable tools you may want to start individually.

**TABLE 2-2** Core Solstice EM Tools Executables

Tool Name	Description
Alarms	em_alarmmgr
Database Backup/Restore	em_dbbackup and em_dbrestore
Data Collections	em_datacollector
Design Advanced Requests	em_reqedit
Network Discovery	em_discover
Event Logs	em_logmgr
MIS Connections	em_mismgr
Network View Import/Export	em_imex
Network Views	em_viewer

**TABLE 2-2** Core Solstice EM Tools Executables

Tool Name	Description
Load Data Definitions	em_loaddefs
Security (command)	em_accessmgr (command) and em_accesscmd (utility)
Database Backup/Restore	em_dbbackup and em_dbrestore

Other Solstice EM executables can be found in the `/etc/SUNWconn/em/bin` directory.

## ▼ To Start Individual Tools

1. **Execute the following command at a system prompt:**

```
em [-host remote_MIS_machine] toolexecutable
```

where *toolexecutable* is one of the executables listed in Table 2-1 on page 2-2.

For example: `em -host zircon em_viewer` will start Solstice EM, connect to the MIS on the `zircon` server and start the Network Views tool.

2. **If prompted, enter your user name and password.**



---

## 2.5 Reconnecting to the MIS

If Network Tools fails to connect to the MIS, or the connection breaks, the tool icons in the Network Tools window are unavailable.

If you previously established a successful connection under access control, you will not be asked for user ID and password when reconnecting to the MIS.

### ▼ To Reconnect to the MIS

- **In the Network Tools window, click Actions->Reconnect.**

**See Also:** For information about remote MIS connections:

- “Preparing for Remote Connections to the MIS” on page 6-14

---

## 2.6 Accessing Online Documentation

The Solstice EM documentation is available as HTML documents and can be viewed in a browser. The online documentation is shipped on the product CD-ROM and can be found in `/opt/SUNWconn/em/docs`. Each book has its own subdirectory. Display the `index.html` file in a browser to gain access to the entire Solstice EM documentation set.

Depending on your Solstice EM installation, the online Solstice EM documentation may or may not be accessible from Network Tools. If the Solstice EM documentation set is not accessible from the Network Tools window, you can add an icon to the Network Tools window and gain access to the documentation set.

### ▼ To Access Online Documentation

- **In the Network Tools window, click Documentation.**

A new instance of your browser starts and opens the Solstice EM documentation page.

## ▼ To Add Access to Online Documentation

1. **In the Network Tools window, click File->Customize to display the Network Tools Customize dialog.**
2. **In Path To Executable, type the path name of your browser.**
3. **In Path To Icon field, type the path name for the icon graphic file.**
4. **In Icon Name, type the string to be used as the icon label.**  
For example, EM 3.0 Online\nDocumentation. The “\n” causes a line break so that the entry appears on two lines.
5. **Select No to specify the browser is not an Solstice EM tool.**
6. **Click Add.**  
The icon you added now appears in the Network Tools window.
7. **Click Save.**  
Changes are saved in the `em_panel.cf` configuration file.
8. **To start the browser, click the icon you just added.**
9. **Open the `/opt/SUNWconn/em/docs/index.html` file.**

---

## 2.7 Adding and Removing Tools

Network Tools displays an icon for each tool or custom-developed application accessible from the Network Tools window. You can use the Network Tools Customize dialog to add, modify, or delete icons and tools from Network Tools.

Solstice EM does not check the validity of your entries in the Network Tools Customize dialog. Errors are detected when you attempt to start a tool.

If you are adding custom-developed tools to Network Tools, you must first add the tool under Solstice EM control using the `createApplication` command of the `em_accesscmd` utility. See “The `em_accesscmd` Utility” on page 6-55 for more information about the command.

### ▼ To Add Tools to the Network Tools Window

1. **In the Network Tools window, click File->Customize to display the Network Tools Customize dialog.**
2. **In Number Of Columns, specify the number of icon columns you want displayed in the Network Tools window.**
3. **In Path To Executable, type the path name for the executable.**

For example, `$EM_HOME/bin/em/em_viewer -host EM_MIS`

4. **In Path To Icon field, type the path name for the icon graphic file.**

For example, `/opt/SUNWconn/em/glyphs/em_viewer.pm`. By default, Solstice EM glyph files are located in `/opt/SUNWconn/em/glyphs`.

5. **In Icon Name, enter the string to be used as the icon label.**

For example, `Network Views`. To create a multi-line entry, add “`\n`” where you want the line to break. For example: `Network \nViews`.

6. **Specify (Yes/No) whether the tool is a Solstice EM tool.**

7. **In Solstice EM Tool Name, enter the connection name that the tool uses to connect to the MIS.**

The Solstice EM tool name is often the same as the executable used to run the tool. For example, the Solstice EM tool name for Network Views is `em_viewer`, which is also the name of the executable. If you do not know a tool’s name, use the Security tool to look up the tool names by selecting View->Privilege Components->Applications List.

### **8. Click Add.**

The icon you added appears in the Network Tools window.

### **9. Click Save.**

Changes are saved in the `.em_panel.cf` configuration file. If you are logged in as root, the `.em_panel.cf` configuration file is put in the root directory `/`. In other cases, the configuration file is placed in the user's home directory. The original configuration file is installed as `/opt/SUNWconn/em/config/em_panel.cf` (without the initial dot.)

## **▼ To Remove Tools From the Network Tools Window**

### **1. In the Network Tools window, click File->Customize to open the Network Tools Customize dialog.**

### **2. In the Applications list box, select the tool to be removed.**

The fields in the Application Information area should now reflect the information for your selection.

### **3. Click Delete.**

### **4. (Optional) Click Save to open a standard Select File dialog.**

### **5. Type the path and file name where you want to save the modified configuration.**

The default file is `~/em_panel.cf`.

---

## 2.8 Modifying Tool Configurations

From time to time, it may be necessary to change the configuration settings of the tools accessible from the Network Tools window. Tools may be moved to other systems, replaced by other tools, and so on.

### ▼ To Modify Tool Configurations

1. **In the Network Tools window, click File->Customize to display the Network Tools Customize dialog.**
2. **In the Applications list box, select the tool and application name.**
3. **Type your modifications.**
4. **Click Change and then click Save.**  
The default configuration file is `~/em_panel.cf`.
5. **Click OK.**

**See Also:** “Network Tools Customize Dialog” on page 2-17 for more information on the dialog options.

---

## 2.9 Reference

Reference information is provided for the following:

- “Command-Line Options” on page 2-12
- “Windows and Dialogs” on page 2-15

### 2.9.1 Command-Line Options

Reference information is provided for the following:

- “Options for the `em` Command” on page 2-12
- “System Variables Used by Solstice EM” on page 2-13
- “Solstice EM Environment Variables” on page 2-14

#### 2.9.1.1 Options for the `em` Command

The `em` command invokes the executable script for starting Solstice EM and displaying the Network Tools window. The `em` command executes the `emenv.sh` script to set up the correct environment before running the `em_panel` executable.

**TABLE 2-3** Options for the `em` Command

Options	Description
<code>-help</code>	Displays a list of the options with descriptions for the <code>em</code> command.
<code>-host &lt;hostname&gt;</code>	Specifies the name of a remote MIS Server

## 2.9.1.2 System Variables Used by Solstice EM

The following table describes the system environment variables and how they are used by Solstice EM.

**TABLE 2-4** System Environment Variables

Environment Variable Name	Default Setting	Description
DISPLAY	<i>localhost:0</i>	Set to your local machine when displaying an application from a remote machine. (Is not set by the <code>emenv.sh</code> script.)
LD_LIBRARY_PATH	<code>/opt/SUNWconn/em/lib</code>	Shared object library path. (Is set by the <code>emenv.sh</code> script.)
OPENWINHOME	<code>/usr/openwin</code>	Directory where Open Windows is located. (Is set by the <code>emenv.sh</code> script. For CDE, <code>/usr/dt</code> is used.)
PATH	<code>\${EM_HOME}/bin:\${EM_HOME}/etc:\${EM_DB_HOME}/bin:\${PATH}</code>	Search path for executable files. (Is set by the <code>emenv.sh</code> script.)
XFILESEARCHPATH	<code>/opt/SUNWconn/em/config/%N</code> is postpended.	Search path for X files. (Is set by the <code>emenv.sh</code> script.)

### 2.9.1.3 Solstice EM Environment Variables

The following table describes the Solstice EM environment variables.

TABLE 2-5 Solstice EM Environment Variables

Environment Variable Name	Default Setting	Description
EM_HOME	/opt/SUNWconn/em	Used by the tools to identify where the SUNWemapp package is installed. (Is set by the emenv.sh script.)
EM_CMIP_MPA_DEFAULT_HOST	localhost	Used by the MIS to identify the machine where the default CMIP MPA is located. (Is not set by the emenv.sh script.)
EM_CMIP_MPA_DEFAULT_PORT	5557	Used by the MIS to identify the port number used by the default CMIP MPA. (Is not set by the emenv.sh script.)
EM_MAPPATH	\$EM_HOME/mapdata	Used by the Viewer to determine where vector map info is located. (Is not set by the emenv.sh script.)
EM_MIS_DEFAULT_HOST	localhost	Used by the CMIP MPA to identify the name of the machine where the MIS is located. (Is not set by the emenv.sh script.)
EM_MIS_DEFAULT_PORT	5557	Used by the CMIP MPA to identify the port number the MIS is using to communicate with it. (Is not set by the emenv.sh script.)
EM_MIS_HOME	/opt/SUNWconn/em	Used by the MIS to identify where the SUNWemmis package is installed. (Is set by the emenv.sh script.)



**TABLE 2-5** Solstice EM Environment Variables (*Continued*)

Environment Variable Name	Default Setting	Description
EM_MIS_PORT	5555	Used to specify the TCP/IP port number the MIS uses to communicate with tools. (Is not set by the <code>emenv.sh</code> script.)
EM_RUNTIME	<code>/var/opt/SUNWconn/em</code>	Used by the MIS to identify where the runtime environment is installed. (Is set by the <code>emenv.sh</code> script.)
EM_SERVER	<i>localhost</i>	Used by the tools to identify the name of the machine where the MIS is running. (Is not set by the <code>emenv.sh</code> script.)
GRAPHER_PATHNAME	<code>/opt/SUNWconn/em/bin/em_grapher</code>	The path to the grapher for tools that use the Grapher API. (Is set by the <code>emenv.sh</code> script.)

## 2.9.2 Windows and Dialogs

Reference information is included for:

- “The Network Tools Window” on page 2-15
- “Network Tools Customize Dialog” on page 2-17

### 2.9.2.1 The Network Tools Window

When you invoke Network Tools, the main window displays as shown in FIGURE 2-1. Initially, Network Tools provides access only to the core Solstice EM tools you use for configuring and managing your network components. You can, however, add and remove other Solstice EM and third-party Solstice EM applications to and from Network Tools.

Click any of the Network Tools icons in the window to launch the corresponding Solstice EM tool.



FIGURE 2-1 Network Tools Window

Click Administration to display the Administration window from which you start the Solstice EM administrative tools.



FIGURE 2-2 Administration Window

The following table describes the menu bar and menu items on the Network Tools window.

**TABLE 2-6** Network Tools Menu

File	Customize	Displays the Network Tools Customize dialog to add and remove tools and application to and from Network Tools. See “Network Tools Customize Dialog” on page 2-17 for more information.
	Exit	Exits the Network tool while keeping the tools and applications that were started from the Network tool running.
Actions	Reconnect	After successfully connecting to the MIS, the menu item is greyed out. The option changes to Reconnect when the connection to the MIS is broken. If Network Tools successfully connected to the MIS, the menu item is greyed out. When reconnecting, you will not be prompted for your user ID and password if Network Tools previously connected successfully under security control.
Help		Displays the online help.

**See Also:** For tasks that use the Network Tools window:

- “Starting Solstice EM” on page 2-4
- “Reconnecting to the MIS” on page 2-7

### 2.9.2.2 Network Tools Customize Dialog

The Network Tools Customize dialog enables you to specify the tools that can be started from the Network Tools window.

Use this dialog to add and remove tools and to specify or update the path and file names for the executables and the graphic files for the icons of Network Tools.

- **To display the Network Tools Customize dialog, click File->Customize from the Network Tools window.**

FIGURE 2-3 illustrates the Customize dialog and the following table provides more information about configuration options.



**FIGURE 2-3** Network Tools Customize Dialog

**TABLE 2-7** Network Tools Customize Options

Options	Description
Applications	Lists the tools and applications that can be started from Network Tools. To view information about a tool, select it's name from this list.
Number of Columns	Specifies the number of columns in which to display the icons.
Path to Executable	Specifies the complete path name for the executable, including any arguments.
Path to Icon	Specifies the complete path name for the icon graphic to display for this tool.
Icon Name	Specifies the text string to use as the button label. For multi-line labels, use the characters \n to force a line break.

**TABLE 2-7** Network Tools Customize Options *(Continued)*

Options	Description
EM Tool (Yes) (No)	Specifies whether or not the tool is a Solstice EM tool.
EM Tool Name	Specifies the name of the executable of the tool that is used to connect to the MIS. It must be the same as the name you specified when setting up access control with the <code>createApplication</code> command of the <code>em_accesscmd</code> utility. If the name is incorrect and the tool is under access control, the icon is unavailable when a user without superuser status starts Network Tools. If a super user or root starts Network Tools, the field is ignored, the icon is available and the tool can be started.
Clear	Clears all data entry fields.
Load button	Enables to load a Network Tools configuration file previously saved using the Save button.

Settings in this Network Tools Customize dialog are saved to the following configuration files:

- `/.em_panel.cf`, if you are logged in as root.
- `~/.em_panel.cf` in your home directory, if you are logged in as a regular user.

**See Also:** For tasks that use the Network Tools Customize dialog:

- “Adding and Removing Tools” on page 2-9
- “Modifying Tool Configurations” on page 2-11



## Discovering Network Components

---

Network Discovery is an automated tool for finding the components on your network and creating a managed object database representing those components on an MIS. The database created by Network Discovery is stored on a local or remote MIS as either a logical or topological (hierarchical) map that you can view with the Network Views tool. After using Network Discovery, you can use the Network Monitor tool to automatically update your managed object databases at intervals you specify.

See Section 3.1 “Overview” on page 3-2 for more information on Network Discovery and Network Monitor. Step-by-step instructions for using these tools begin from Section 3.2 “Getting Started With Network Discovery” on page 3-5. Detailed command-line reference information is provided in Section 3.9 “Reference” on page 3-17.

This chapter comprises the following topics:

- Section 3.2 “Getting Started With Network Discovery” on page 3-5
- Section 3.3 “Loading and Saving Discovery Rules” on page 3-7
- Section 3.4 “Deciding Which Components to Discover” on page 3-8
- Section 3.5 “Viewing Network Discovery Progress” on page 3-12
- Section 3.6 “Stopping a Network Discovery in Progress” on page 3-12
- Section 3.7 “Creating a New MIS Managed Object Database” on page 3-13
- Section 3.8 “Keeping Data Current With Network Monitor” on page 3-14

---

## 3.1 Overview

Before you can use Solstice Enterprise Manager (Solstice EM) to manage the various components on your network, you must first determine what those components are. More specifically, before you perform any management tasks in Solstice EM, you must populate at least one Solstice EM Management Information Server (MIS) database in your Solstice EM environment with a map of your network components.

You can use the Network Discovery tool to perform two types of functions:

- **Discovery** – The primary means of finding network components and populating the MIS with managed objects representing those network components; can be initiated from the GUI or from the command line. Numerous options are available for defining the scope and range of the Network Discovery process, and for defining the way managed objects are represented in the MIS. Refer to Section 3.9 “Reference” on page 3-17 for more information about these options.
- **Monitoring** – Provides the means to conveniently schedule through the GUI automated periodic updates to MIS entries for specific subsets of network components. The Monitor function uses the settings you specify for the Discover function, and also provides options for specifying what and when you want to monitor; refer again to Section 3.9 “Reference” on page 3-17 for more information.

### 3.1.1 Agents and Stations

The Network Discovery tool uses the industry-standard *agent/station* model to provide a simple, automated way to find the hosts, workstations, PCs, routers, networks, subnetworks, links, and other SNMP devices on your network. When Network Discovery finds a network component, it creates a managed object to represent the component in an MIS database.

In the agent/station model of network management, network components run locally, or are accessible by, software *agents*. These agents make available to network management *station* applications information about the network component with which the agent is associated. Station applications request information from one or more agents, and return this information either directly to the user or to other network management applications.



## 3.1.2 Methods Used by Network Discovery

By default, Discover and Monitor use a combination of Ping, SNMP, and RPC methods to find SNMP network components. You can modify these methods directly through the Network Discovery tool, and add support in your MIS for other protocols using the various MIS tools described in the *Customizing Guide*. More information about Network Discovery Tool methods is provided later in this chapter, in Section 3.9 “Reference” on page 3-17.

## 3.1.3 Network Views

Network components discovered by Network Discovery are stored as managed objects in the MIS under a root container or view you specify, in either a *hierarchical* or *logical* format. Briefly, these two formats are as follows:

- **Hierarchical** – Network components are represented in a topographical format, based on physical parent/child relationships. For example, a hierarchical view of a network may progress, tree-style, from networks, to routers, to subnetworks, to hosts. This is the default format created by Network Discovery.
- **Logical** – Network components are all represented at the same level under the root (or other specified) container in the MIS. This format is not recommended for large networks.

When running Network Discovery on your network, you can specify the name of the root container object under which you want to store your discovery results in the MIS, as well as the format in which you want to store the object data. This format—that is, hierarchical or logical—is important, because it affects the basic way in which your object data is recorded in the MIS, and you cannot change the format after the network discovery is completed. The default container is “Root.” If you use a container other than Root, the container you specify is created at the root level, and new objects are created in logical format.



---

**Caution** – By default, Network Discovery only adds objects to the MIS for newly discovered network components—that is, if an object reference to a network component already exists in the MIS, Network Discovery will not overwrite it. If you save the results of your network discovery first in, say, hierarchical format, and then do a subsequent discovery saving the results in logical format, you will create a condition in which you will not see all your components in a given view—for example, some components will be visible in your logical views, but not in your hierarchical views. The only way to recreate your MIS database, and thereby be assured that you will later be able to see all your components in a given view, is to start the MIS services with a new database. Instructions for doing this are provided later in Section 3.7 “Creating a New MIS Managed Object Database” on page 3-13.

---

See Chapter 4 “Viewing Network Components” for more information about creating and working with Network Views. Refer to the *MIS Guide* for more information about working directly with the MIS.

## 3.1.4 Network Monitor

The Network Discovery Monitor function provides a convenient set of controls for automatically updating some or all of your MIS at periodic intervals. Use the Monitor function instead of, or in addition to, any script-based automation you may already use to maintain updated object data in your MIS.

For example, you may use a `cron` script that runs Network Discovery to completely rebuild your MIS every two weeks. Depending on your goals for this rebuild, you may find that the Monitor function adequately suits your needs, is faster than a complete rebuild and, at the same time, is simpler and more straightforward to use.

See Section 3.8 “Keeping Data Current With Network Monitor” on page 3-14 for more information about using Network Monitor.

## 3.1.5 Related Tasks

Before using Network Discovery, you must:

- Install or configure network agent software as needed on or for the network components you want to discover—Solstice EM installation may or may not have installed such agent software automatically for you. See the *Installation Guide* for more information.
- Use the `em_services` command to start the MIS daemons on the host that manages the MIS you want to populate. See the *MIS Guide* for more information.

If your network uses CiscoWorks, Optivity, or other components, you must add managed object definitions for such devices to your MIS before running a Network Discovery. See the *MIS Guide* for information about adding object definitions to your MIS.

After using the Discover tool to create a managed object database of the components on your network, you may want to:

- Use the Monitor function to automate updates to your MIS. Refer to Section 3.8 “Keeping Data Current With Network Monitor” on page 3-14 for more information.
- Use the Network Views tool to view and manage the components on your network. See Chapter 4” for more information.

- Use the various object viewing tools to view detailed information about the objects in your MIS. See Chapter 9” for more information.
- Use the Alarms tool to configure or respond to alerts and alarms generated by one or more network components. See Chapter 5” for more information.

### 3.1.6 Related Files

- `$EM_HOME/config/discover.conf` – Network Discovery configuration file
- `/tmp/em_discover_pid.log` – Discover log file
- `/tmp/em_monitor_pid.log` – Monitor log file

### 3.1.7 Further Reading

Refer to the *Solstice EM Customizing Guide* for more information about configuring network agents and your MIS. Also refer to the *MIS Guide* for more information about MIS configuration options.

---

## 3.2 Getting Started With Network Discovery

Network Discovery can be run from either a simple graphical interface or from the command line. The command-line interface is particularly useful if you want to run Network Discovery as part of an automated script. This is important, because the Discovery process can be more or less time-consuming depending on the number of network components being discovered.

---

**Note** – By default, the Network Discovery process starts from the machine on which it is run, not the machine on which the MIS is located. While you can tell Network Discovery to locate whatever components you want, this default behavior could be significant if the machine on which Network Discovery is run and the machine on which the MIS is located are on different subnetworks.

---

Refer to Section 3.8 “Keeping Data Current With Network Monitor” on page 3-14, for instructions on using Network Monitor.

The following procedures provide information about:

- Starting the Network Discovery tool
- Starting a Network Discovery using default settings
- Initiating a Network Discovery using rules from a file
- Stopping a Network Discovery

## ▼ To Start the Network Discovery Tool

Start the Network Discovery tool in one of the following ways:

- In the Network Tools window, click Network Discovery.



FIGURE 3-1 Network Discovery Button

- Using other Solstice EM tools, click Tools->Network Discovery.
- Using the UNIX command-line, type:

`em_discover -options`

Refer to TABLE 3-1 on page 3-18 for a complete list of Network Discovery command-line options. After starting Network Discovery from either the Network Tools window or the Tools->Network Discovery menu item, the Network Discovery window is displayed. The Network Discovery window is *not* displayed when you use the command-line interface unless you specify the `-T` option.

---

**Note** – Network Discovery cannot be run from the command line by any user other than `root` if Solstice EM is installed in a directory other than the default (`/opt`). Non-root users can still run Network Discovery from the Network Tools window even if Solstice EM is installed in a non-default location. The command-line restriction only exists when Solstice EM is installed in a non-default location.

---

## ▼ To Start a Network Discovery Using Default Settings

- In the Network Discovery window, click **Start** to initiate the Network Discovery process using the default settings.

## ▼ To Start a Network Discovery Using Saved Settings

1. Click **Actions->Discover Network** to display the **Discover Network** dialog box.
2. Select the various **Discover** options you want to use, or load an existing **Network Discovery rules file**.

Refer to the subsequent procedures in this chapter, and to Section 3.9 “Reference” on page 3-17, for complete information about these options.

3. Click **Start** to initiate the discover process.

## ▼ To Stop a Network Discovery

- When the discovery process is complete, click **File->Exit** to close the **Network Discovery** window.

---

## 3.3 Loading and Saving Discovery Rules

When you use the Network Discovery graphical interface (but not when you use the command-line interface), you can save and load all your settings—components to discover, discovery methods, and logging options—in a Network Discovery *rules file*. Rules files are plain ASCII text, and provide a convenient means for recalling your Network Discovery settings for use at a later time or by another person.

## ▼ To Load an Existing Discovery Rules File

1. In the Network Discovery window, click **Actions->Discover Network** to display the Discover Network dialog box.
2. Click **Load**, and then enter the name of the rules file you want to use.
3. Click **Start** to start the Network Discovery process.

## ▼ To Save a Discovery Rules File

1. In the Network Discovery window, click **Actions->Discover Network** to display the Discover Network dialog box.
2. Specify your Network Discovery settings, as described in the subsequent procedures in this chapter.
3. Click **Save**.
4. Enter a name and location for your rules file.

---

## 3.4 Deciding Which Components to Discover

The Network Discovery tool lets you specify:

- **Types of components to discover**—Specify multiple or single networks, a specific list of IP addresses, a single device, specific object types, and so forth. You can also specify how you want discovered components to be represented in the MIS.
- **Ports to use for discovery**—Select from a list of available ports to use for discovery.
- **Discover by**—Specify whether to discover by services, topotypes, or both. Choose the services to discover for.

- **Discover methods**—Specify settings for Ping, SNMP, RPC, and SunNet Manager agents and proxies.
- **Logging options**—Enable and disable logging, and specify location of log files generated by the Network Discovery process.

---

**Note** – The procedures below describe how to specify Network Discovery options using the graphical Network Discovery window. If you are using the command-line interface, simply enter the desired options at the command line. Refer to TABLE 3-1 on page 3-18 for complete descriptions of Network Discover command-line options.

---

## ▼ To Select Components to Discover

1. In the Network Discovery window, click **Actions->Discover Network** to display the **Discover Network** dialog box.
2. Select the **Network Discovery** tab, if it is not already selected.
3. Select the type of discovery you want to perform from the **Types of Discovery** group.

The selection you make here constrains most of the other options on this tab.

4. In the **Display of Newly Discovered Objects** group, specify how you want discovered objects to be represented in the MIS.

You can specify the name of the default view to use when representing the results of your discovery in the Network Views window, and whether you want these results saved in the MIS in topographical (hierarchical) or logical formats. The default is Root. If you use a container other than Root, the container you specify is created at the root level, and new objects are created in logical format.

---

**Note** – When a discover is completed, the time and date stamp, number of objects discovered, in addition to the time required for discovery are printed on the discovery report.

---

5. On machines with multiple network interfaces, you can select which interfaces to use for discovery.
6. Continue on to specify a discovery method, as described in the next procedure.

## ▼ To Select Interface(s) for Discovery

1. On the **Network Discovery** tab, select any interfaces from the list of **Selected Ports** to add or remove the interface from the discovery.
2. Click **Remove** or **Restore** to set the interfaces for discovery.

## ▼ To Specify Discovery by Services and TopoTypes

1. In the **Discover Network** dialog, select the **Services/TopoTypes** tab.
2. Set the **Discover by Services** option to **Off**.  
All services will be grayed out.  
*or*
2. Set the **Discover by Services** option to **On**.  
This action makes the available services active.
3. Click to select available service protocols or you can enter a new service.
4. Click the **All Topotypes** checkbox to select the topotypes to discover.  
By default, all topotypes are discovered.
5. Select the topotype from the list.
6. Click **Add** to add selections to the discovery list.
7. Click **Remove** to remove selections from the discovery list.

## ▼ To Specify Discovery Methods

1. In the **Discover Network** dialog, select the **Ping/SNMP/RPC** tab.
2. Specify **Ping** and **SNMP** optimization parameters, depending on the characteristics of your network.
3. Specify if you want to discover agents.

---

**Note** – If there are any agents, this will significantly increase the discovery time.

---

4. Type the names of any **SNMP read community strings** to use.

You can specify up to five read community strings, separating each string with a colon, no spaces; for example, `public:floor2`. The default read string is `public`.



5. **Type the name of an SNMP write community string to use, if desired.**  
You can only specify one write community string. The default write community string name is `private`. Note that this setting only affects the recording of object data in the MIS; that is, it does not issue any `SNMP SET` requests.
6. **Specify whether you want to use automatic RPC configuration.**
7. **Specify any specific RPC agents you want to use in addition to those used by the automatic RPC configuration option.**
8. **Click Start to initiate the Discover process, or continue on to specify Logging options, as described in the next procedure.**

## ▼ To Specify Logging Options

1. **In the Discover Network dialog box, select the Logging tab.**
2. **Specify whether you want to turn logging on or off.**  
If you choose to enable logging, select the name of a log file to use. If desired, specify one or more addresses to which you want to email the log file. Separate multiple addresses with a semicolon.
3. **Specify the level of detail you want to capture in the log file.**

---

**Note** – Executing Debug in verbose mode will process a multitude of data that is unnecessary for most users.

---

4. **Click Start to initiate the Discover process.**  
The Network Discovery window displays the status of the discovery process, and this output is also directed to the log file you specified. If you want to save your settings in a Network Discover rules file, refer to Section 3.3 “Loading and Saving Discovery Rules” on page 3-7.

---

## 3.5 Viewing Network Discovery Progress

The Network Discovery window displays a running log and progress counter of the Network Discovery currently in progress. This information remains available after the Discovery process has been completed, but is lost when you close the Network Discovery window—that is, if you close and restart Network Discovery, this information will be lost. Use a log file to view progress information after Network Discovery has been completed and you have closed the Network Discovery window. Creating Network Discovery log files is described in the preceding procedure, “To Specify Logging Options” on page 3-11.

### ▼ To View a Network Discovery in Progress

- **Look in the Network Discovery window.**

You can print the text in this window, or select text and paste it into another application, such as a text editor. Note that you cannot insert text into the Network Discovery window.

---

## 3.6 Stopping a Network Discovery in Progress

You can stop a Network Discovery in progress without causing any damage to your existing MIS. Network Discovery only adds new objects to your MIS, and does not overwrite any existing objects.

### ▼ To Stop a Network Discovery in Progress

- **Click Stop in the Network Discovery window.**

---

## 3.7 Creating a New MIS Managed Object Database

By default, as described in Section 3.1.3 “Network Views” on page 3-3, Network Discovery only adds object references to your MIS for newly discovered objects. If an object reference already exists in the MIS, Network Discovery does not overwrite it.

There will likely be occasions when you want to recreate your MIS database from scratch. For example, you may want to recreate the database for periodic maintenance purposes, or to change the object format from logical to hierarchical or vice versa.

Recreating your MIS is accomplished by an MIS services command-line option, and not by any specific option in Network Discovery. While most MIS commands are beyond the scope of this guide, the command to create a new MIS database is fundamental to using Network Discovery, and so it is described here. For complete information about working with MIS object data, refer to the *MIS Guide*.



---

**Caution** – Use extreme caution when creating a new MIS database! Creating a new MIS database destroys all data in the old MIS database. Refer to the *Management Information Server (MIS) Guide* for information about using the Topology Import/Export tool to save and restore MIS topology information. See the *MIS Guide* for information about creating and restoring backups of your MIS database.

---

### ▼ To Create a New MIS Managed Object Database

1. On the host on which you want to create the new MIS, stop the currently running MIS services, if any, by executing the following command at an UNIX command prompt:

```
em_services -stop
```

2. Start (or restart) the MIS services by executing the following command:

```
em_services -init
```

You are warned that proceeding will destroy all data in the current MIS.

3. Enter **y** to continue, or **n** to cancel.

A new MIS database is created, and the MIS services are reinitialized.

4. Run Network Discovery to create a new MIS database.

---

## 3.8 Keeping Data Current With Network Monitor

The Network Discovery Monitor function provides a convenient set of controls for automatically updating some or all of your MIS at periodic intervals. Specifically, Network Monitor updates the MIS with managed objects for newly discovered network components, and marks as down components that are unreachable. Use the Monitor function instead of, or in addition to, any script-based automation you may already use to maintain the currency of object data in your MIS.

For example, you may use a `cron` script that runs Network Discovery to completely rebuild your MIS every two weeks. Depending on your goals for this rebuild, you may find that the Monitor function adequately suits your needs, is faster than a complete rebuild and, at the same time, is simpler and more straightforward to use.

The Monitor function uses the current settings specified for the Discover function. In addition, Monitor provides options for specifying what you want to monitor, and for scheduling when you want Monitor to run.

### ▼ To Use Network Discovery Monitor

**1. Start the Network Discovery tool in one of the following three ways:**

- From the Network Tools window, click Network Discovery.
- From the Network Views window, click Tools->Network Discovery.
- From an UNIX command prompt, execute:

```
em_discover -M options
```

See TABLE 3-2 on page 3-21 for a complete list of Network Discovery Monitor command-line options.

After starting Network Discovery from either the Network Tools window or the Tools->Network Discovery menu, the Network Discovery window is displayed. The Network Discovery window is *not* displayed when you use the command-line interface unless you specify the `-T` option.

- 2. From the Network Discovery window, click Actions->Monitor Network to display the Monitor Network dialog box.**
- 3. Select the various Monitor options you want to use, or load an existing discovery rules file.**

4. **In the Network Monitor window, click Start to start the Monitor process.**

Make sure that you are in the Network Monitor window when you click Start; clicking Start in the main Network Discovery window starts the Discover process, not the Monitor process.

5. **Click File->Exit to close the Network Discovery window.**

## ▼ To Load an Existing Monitor Rules File

1. **In the Network Discovery window, click Actions->Monitor Network to display the Monitor Network dialog box.**
2. **Click Load.**
3. **Enter the name of the rules file you want to use.**
4. **Click Start to start the Network Monitor process.**

## ▼ To Save a Monitor Rules File

1. **In the Network Discovery window, click Actions->Monitor Network to display the Monitor Network dialog box.**
2. **Specify your Network Monitor settings, as described in the subsequent procedures in this section.**
3. **Click Save.**
4. **Enter a name for your rules file.**

## ▼ To Specify Which Objects to Monitor

1. **In the Network Discovery window, click Actions->Monitor Network to display the Monitor Network dialog box.**
2. **Select the Monitor tab, if it is not already selected.**
3. **Specify the container names for objects you want to monitor from the Objects to Monitor group.**

The container names you specify here are those that you have defined with the Network Views tool.

**4. Specify the objects you want to exclude from the monitor process.**

You can specify device names or IP addresses.

**5. Specify Time Between Cycles.**

This setting refers to the frequency of Monitor cycles; the default is 15 minutes.

**6. Specify a Holding Container to use for newly discovered objects.**

The default is “Root,” which means that newly discovered objects are added to the topology in the Root container. If you use a container other than Root, the container you specify is created at the root level, and new objects are created in logical format.

**7. Select a Generate Event if Object is Down option—that is, whether a communications alarm of a specified `perceivedSeverity` should be generated if an object is unreachable.**

By default, this option is set to No. If you select Yes, you can then also specify a severity level for the alarm. Choose from Critical, Major, Minor, or Warning. When a previously unreachable host becomes reachable, Monitor generates an alarm with `perceivedSeverity` set to “Cleared.”

**8. Select the Ping/SNMP/RPC tab, and then specify discovery methods to use in the Monitor process, if desired.**

The discovery methods you can specify here are exactly the same as those described earlier in this chapter for the Discover process, in “To Start the Network Discovery Tool” on page 3-6.

**9. Click Start to start the Monitor process, or continue on to specify Schedule/Logging options, as described in the next procedure.**

## ▼ To Set Up Monitor Schedules and Logging

**1. In the Monitor tab of the Monitor Network dialog box, select the Schedule tab.**

**2. Specify Start Time and Stop Time.**

If you specify a start time that is in the future, Network Monitor will not start automatically; you must then click Start to start the process after completing the other fields on this tab.

**3. Specify Start Date and Stop Date.**

The start and stop dates indicated takes affect only if the daily or weekly option is selected.

**4. Select if you want Monitor to run daily or weekly, and if weekly, on what day.**

Monitors daily / weekly (day of the week) for the specified time interval given by start time & stop time.

5. **Select the Logging tab.**
6. **Specify whether you want to enable logging.**  
Logging is Off by default.
7. **Specify the name of the file in which you want to save logging information.**
8. **Specify one or more email addresses to which you want to send log information at the end of each Monitor cycle.**
9. **Click Start to start the Monitor process.**

---

## 3.9 Reference

The remainder of this chapter provides detailed reference information about Network Discovery and Monitor command-line options, and conceptual background material to help you understand more about how Network Discovery works. This section covers the following topics:

- “Command-Line Options” on page 3-17
- “More About Network Discoveries” on page 3-22
- “More About Hop Counts” on page 3-27
- “More About Ping/SNMP Optimization” on page 3-27
- “More About RPC Agents and SunNet Manager Proxies” on page 3-28

For detailed information about dialogs, menus, and other user interface elements, refer to the Solstice EM Online Help. To access Online Help, click the Help button on any dialog box or select options from the Help menu located in the upper right corner of each Solstice EM tool window.

### 3.9.1 Command-Line Options

TABLE 3-1 describes the Network Discovery command line options, and TABLE 3-2 describes the Network Discovery Monitor options.

### 3.9.1.1 Network Discovery Options

The general form for the Network Discovery command line is:

```
em_discover -options
```

The various Network Discovery command-line *options* are described in the following table. Step-by-step instructions for using the Network Discovery graphical interface begin in Section 3.2 “Getting Started With Network Discovery” on page 3-5.

---

**Note** – Network Discovery cannot be run from the command line by any user other than `root` if Solstice EM is installed in a directory other than the default (`/opt`). Non-root users can still run Network Discovery from the Network Tools window even if Solstice EM is installed in a non-default location. The command-line restriction only exists when Solstice EM is installed in a non-default location.

---

**TABLE 3-1** Network Discovery Command-line Options

Option	Description
-agent [ <i>:agent</i> ]	Specify the name(s) of a SunNet Manager (SNM/RPC) agent to configure (for example, <code>snmp</code> , <code>diskinfo</code> , or <code>hostperf</code> ). The following example would configure the device <code>augusta</code> to be manageable by <code>diskinfo</code> : <code>em_discover -agent diskinfo -device augusta</code> . Separate multiple agent names with a colon (:).
-contain <i>container</i>	Put discovered objects in the specified container. If you use a container other than <code>Root</code> , the container you specify is created at the root level, and new objects are created in logical (flat) format.
-cr <i>string</i> [ <i>:string</i> ]	Specify up to five SNMP read community strings. This limits the discovery to only those devices that have the specified community names. The default is “public.” Use a colon, no spaces, to separate multiple community strings. Using multiple community strings can significantly increase the time of the discovery process.
-cw <i>string</i>	Enter one SNMP write community string. The default string is <code>private</code> . Note that the SNMP Write Community string is used to configure an option in the MIS that can be used by other Solstice EM tools; Network Discovery itself does not use this string to send SNMP <code>SET</code> requests.
-D e n	Debugging options, expert or novice. Refer to TABLE 3-4 on page 3-26 for more information.
-D c s t	Component-level debugging options <code>config</code> , <code>snmp</code> , <code>tracer</code> . Refer to TABLE 3-4 on page 3-26 for more information.



**TABLE 3-1** Network Discovery Command-line Options (*Continued*)

Option	Description
-device <i>device_name</i>	Discover only the specified device; use a device name or IP address.
-file [include exclude] <i>hosts_file</i>	Discover/exclude specified hosts in the specified <i>hosts_file</i> .
-flat	Create objects in a logical hierarchy. See Section 3.1.3 “Network Views” on page 3-3 for more information.
-g [only] <i>gateways</i>	Specify the gateway(s) to be used in the discovery process. You can enter multiple gateway names, separated by a colon. If the keyword “only” is entered, only the networks found at the listed gateways are probed.
-help	Display command-line help for Network Discovery.
-hop <i>n</i>	Specify the maximum number of hops from the manager that Network Discovery will extend. The default is 0, which restricts the discovery to the local subnetwork. Enter -1 to instruct Network Discovery to not limit its discovery. See Section 3.9.3 “More About Hop Counts” on page 3-27 for more information.
-host <i>hostname</i>	Specify the name of the host machine on which the MIS is running.
-int <name>	Interface to use for discovery on a multi-homed machine.
-lf <i>file</i>	Direct output to a log history file.
-lh	Direct output to log history.
-M	Start Network Discovery Monitor.
-m <i>name</i>	Email log history file to specified <i>name</i> .
-mask <i>n</i>	Specify the netmask to be used in the discovery.
-nc [b x t][+ -]	Specify network characteristics for purposes of discovery optimization. See Section 3.9.4 “More About Ping/SNMP Optimization” on page 3-27 for more information.
-net <i>network</i>	Specify a network address or name to start a discover from. Defaults to the net/subnet where discover is currently run from.
-objects <i>objects</i>	Specify the types of objects you want to discover. Valid values are: snmp, host, network, router, and link. Separate multiple values with a colon. By default, Network Discovery finds all types of objects. Certain types of objects are necessarily discovered in conjunction with other types.

**TABLE 3-1** Network Discovery Command-line Options (*Continued*)

Option	Description
<code>-of [i w e d]</code>	Output filter to display only the selected types of messages.
<code>-pb</code>	Use a broadcast method of pinging subnetworks. This option creates a heavy network load and is not recommended for use with Monitor or for discoveries with <code>-hop</code> greater than 0.
<code>-pfn num</code>	Specify the maximum number of outstanding simultaneous fast pings per interval specified by the <code>-pft</code> option. The default value is 10.
<code>-pfr num</code>	Specify the number of times Network Discovery tries to contact a device using ICMP (ping) when the fast ping method is used.
<code>-pft seconds</code>	Specify the frequency between transmissions of ICMP echo requests (in seconds) when the fast ping method is used.
<code>-pr num</code>	Specify the number of times an attempt is made to contact a device using ICMP (ping). Increase this value for very busy or long-haul networks. However, increasing this value slows down the discovery process.
<code>-ps</code>	Use serial ping to discover components.
<code>-r from:to</code>	Specify a range of host addresses to ping for each network/subnet specified, for example <code>1:2048</code> . The 'from' range should be $\geq 1$ and the 'to' range should be $\geq \text{inverse of netmask} - 1$ . This option should be used with <code>-net</code> option for a specific subnet/non-subnet network.
<code>-rc device   array   container</code>	Create unmapped routers as RouterArray, RouterContainer, or Device.
<code>-Sr n</code>	Specify the number of tries when sending SNMP requests to devices. Increase this value for a very busy or long-haul network.
<code>-St n</code>	Specify the timeout value in seconds when sending SNMP requests to devices.
<code>-T</code>	Bring up the Network Discovery graphical user interface; use with the <code>-M</code> option to display the Monitor Network window.
<code>-tune</code> <code>fping ping ssnmp csnmp</code> <code> rpc port trace:min max</code> <code>x ret:n: tune timeout</code> <code>parameters</code>	Tune timeout parameters, depending on your network environment.

**TABLE 3-1** Network Discovery Command-line Options (*Continued*)

Option	Description
-v	Verbose output.
-wait	Wait for a platform connection at startup.
-www	Notify when discovered device is a WWW server (uses ports 80 and 8080).

### 3.9.1.2 Network Discovery Monitor Options

The general form for the Network Discovery Monitor command line is:

```
em_discover -M -options
```

The various Network Discovery Monitor command-line *options* are described in the following table. Step-by-step instructions for using the Network Discovery Monitor graphical interface begin in Section 3.8 “Keeping Data Current With Network Monitor” on page 3-14.

**TABLE 3-2** Network Discovery Monitor Command-line Options

Option	Description
-ct <i>time</i>	Specify the amount of time (in minutes) between each time Monitor is run.
-dw <i>day</i>	Specify the day of the week to run Monitor. Valid values are sun, mon, tue, wed, thu, fri, and sat.
-w <i>week</i>	Specify to run Monitor weekly.
-h <i>holding_area</i>	Specify the name of the holding area into which all newly discovered objects are placed.
-fc <i>container</i>	Limit Monitor’s discovery operations and reach ability testing to devices in the container(s) specified. Separate multiple container names with a colon.
-i <i>device-name</i>	Ignore the devices specified in <i>device-name</i> . Separate multiple device names with a colon. Use this option to instruct Monitor not to ping for devices that have been taken down or removed from the network, but which are still in the MIS database.
-mevt	Monitor generate event.
-sev <i>event_severity</i>	Monitor event severity.
-start <i>hh:mm</i>	Specify the start time in the format <i>hh:mm</i> .
-stop <i>hh:mm</i>	Specify the stop time in the format <i>hh:mm</i> .

**TABLE 3-2** Network Discovery Monitor Command-line Options (*Continued*)

Option	Description
-startd <i>mm:dd:yy</i>	Specify the start date in the format <i>mm:dd:yy</i> .
-stopd <i>mm:dd:yy</i>	Specify the stop date in the format <i>mm:dd:yy</i> .
-t <i>n</i>	Monitor non-response timeout.
-w	Run Monitor weekly.

## 3.9.2 More About Network Discoveries

Network Discovery interrogates the network using the following Internet protocols:

- Simple Network Management Protocol (SNMP)
- Internet Control Message Protocol (ICMP)

### ▼ To Select an Interface for a Discovery

1. **On the Network Discovery tab, select any interfaces from the list of Selected Ports to add or remove the interface from the discovery.**
2. **Click Remove or Restore to set the interfaces for discovery.**

After identifying the local configuration—network and subnet, netmask, host interfaces, and routing table—Network Discovery interrogates the network in a two-stage process: *Query* and *Probe*.

### 3.9.2.1 Network Discovery Query Stage

During the Query stage, Network Discovery builds an internal hierarchical model of the network topology and adds one entry for each Class A, B, or C network it discovers. Each entry contains a list of subnets and a list of directly connected networks. If the network has no subnets, then each entry contains a list of directly connected hosts.

To build the hierarchical model of the network topology, Network Discovery:

- Accesses the local routing table to find the location of the subnetwork's default router.
- Retrieves the default router's interface table using SNMP.
- Retrieves the interface tables from all next hop gateways.
- Jumps from gateway to gateway as it retrieves the interface table from each "next hop" gateway.

- Continues to retrieve interface tables of “next hop” gateways until the Hop Count set in the Discover Network dialog box is reached (by default, Hop Count is set to 0 and the discovery process is limited to the local subnetwork).

In all the discovery methods, the routers and the hosts found within the hop count are added to the MIS. The only difference is in the way they ping the entire subnet to find the rest of the hosts.

- **Default** – The pings are sent in batches and get the responses by waiting for the specified timeout value. The batch number and timeout value can be changed using the `pfn` and `pft` command line options.
- **Serial Ping** – The pings are sent one after another in series for the entire subnet range. The timeout value to wait for the response can be specified using the command-line `icmp timeout`. Note that this option is only available from the command line with the `em_discover -ps` command; it is not available through the Network Discovery graphical interface.
- **Broadcast Ping** – This can be specified only through a command line. Here the pings for the entire subnet range are sent at the same time. This method is recommended only for the local subnets, since the routers do not forward broadcast pings. Note that this option is only available with the `em_discover -pb` command; it is not available through the Network Discovery graphical interface.

---

**Note** – It is only possible to explicitly specify these three Ping methods from the Network Discovery command line, as described in TABLE 3-1. The Ping/SNMP optimization settings on the Discover Network Ping/SNMP/RPC tab can automatically configure optimal Ping and timeout parameters based on the characteristics of your network. Refer to Section 3.9.4 “More About Ping/SNMP Optimization” on page 3-27.

---

### 3.9.2.2 Network Discovery Probe Stage

For the devices found in the Query stage, above, Network Discovery attempts to obtain relevant information by:

- Sending an ICMP echo request (ping) to check for reachability of the device
- Determining if the object is an SNMP device and, if so, find out its interfaces, system table, `iftable`, and `ifstatus`.
- Using the `ipAddrTable` to determine the number of interfaces, determining the data link protocol of these interfaces (Ethernet, FDDI, Token Ring), and obtaining the MAC addresses.
- Testing for a match in the OID to object mapping table in `discover.conf`.
- Testing for a match in the `sysDescr` to object mapping table in `discover.conf`.

Once the above tests are completed and the relevant information is obtained, Network Discovery classifies and creates an object for the device in the MIS, if one does not already exist. The information obtained from the tests is used to set the attributes of the object.

### 3.9.2.3 More About Classifying Devices

The `discover.conf` file allows you to classify devices based on Object ID (OID), and then further classify each device based on system description. The OID must be specified using the keyword “OID” and subsequent lines should contain the system description and device type. The format is as follows:

OID	sysobject_id_of_the_device
system_desc_1	device_type_1
system_desc_2	device_type_2
system_desc_3	device_type_3

The `discover.conf` file is located at `$EM_HOME/config/discover.conf`. A line beginning with the “#” character designates a comment and is therefore not processed.

The format for Probe\_OIDs is as follows:

PROBE_OID	IIMCCISCO-MIB	1.3.6.1.4.1.9
PROBE_OID	IIMCECSV2-MIB	1.3.6.1.4.1.43
PROBE_OID	IIMCRETIX-MIB	1.3.6.1.4.1.72
PROBE_OID	IIMCSUN-MASTER-AGENT-MIB	1.3.6.1.4.1.42.2.15
PROBE_OID	IIMCHOST-RESOURCES-MIB	1.3.6.1.2.1.25
MIB	Bridge	IIMCCISCO-MIB
MIB	Bridge	IIMCECSV2-MIB
MIB	Bridge	IIMCRETIX-MIB
MIB	Host	IIMCSUN-MASTER-AGENT-MIB

The following table lists the definitions associated with a Probe\_OID.

**TABLE 3-3** Discover.conf Definitions

Term	Description
Probe OID	Discover term for Object Identifier (OID) that identifies a MIB.
MIB	Management Information Base; contains the structural definition of all information stored by an agent about a device type.
Object Identifier	Sequence of numbers that identifies a particular MIB.

Another feature is the “\_ALL\_ROUTER\_” keyword which can be used in the system description field. This feature sets all routers that match the OID to be the device type specified OID in the device type field. This saves you the trouble of having to list all the different system descriptions for each router, assuming that they are all intended to be classified as the same device type.

Additionally, you can use wildcard characters such as “\*” in the system description field for mapping objects with the specified OID.

### 3.9.2.4 Discover and Network Security

By default, Network Discovery probes the network by using the following ports:

- 161 – Network Discovery uses this port to communicate with the SNMP daemon (snmpd) on a remote device.
- 32768+666 – Network Discovery uses this port to determine the hop distance to a device. If the Gateway as Boundary List option is used, port 32768+666 is not probed.
- 80 , 8080 – If the command line option, -www, is used, Discover probes these ports to determine whether or not a WWW server is running on the machine.

When discovering a device based on its supported services, ANY port number specified by the user can be probed.

### 3.9.2.5 Recovering From a Failed Discovery

The Network Discovery debugging options are only available when running Network Discovery from the command line. Use these debugging options if you experience difficulties in completing the discovery process, or if you are receiving a large number of error messages.

Two categories of Network Discovery debugging options are available:

- **Current Detail** – Run and receive information about the current, “real” discovery process; part of this process includes connecting to and updating the MIS.
- **Component Detail** – Debug specific software modules that are components of Network Discovery; does not establish an MIS connection or make any changes to the MIS.

Network Discovery debugging information is always printed to standard output—that is, in most cases, to your screen.

## ▼ To Use Network Discovery Debugging Options

- **Start Network Discovery from the command line with the following parameters:**

`em_discover -D [options]`

The table below lists Network Discovery debugging options.

**TABLE 3-4** Network Discovery Debugging Options

Option	Description
<i>Current Detail (connection made to MIS)</i>	
-D e	Prints debugging information in a format that assumes Internet-specific expertise.
-D n	Prints debugging information in a format that is understandable to the average user.
<i>Component Detail (no connection made to MIS)</i>	
-D c	Starts Network Discovery Configuration module, which prints information about the host on which Network Discovery is running, such as local routing table, ARP table, interfaces, default routers, network number, subnet number, and netmask.
-D s <i>hostname</i>	Starts Network Discovery SNMP module, which takes <i>hostname</i> as its target host, does a one-time SNMP query of the specified device, and prints the information to standard output.
-D t <i>hostname</i>	Starts Network Discovery Traceroutes module, which executes the <code>traceroutes</code> code with <i>hostname</i> as target, and prints to standard output the route to the specified host and the gateways used to reach it.



### 3.9.3 More About Hop Counts

Hop Count, set in the Discover Network dialog, is a measure of how far Network Discovery will extend when attempting to discover new network components. Specifically, for any given route from the machine running Network Discovery (or from the subnetwork specified with the Network option, also in the Discover Network dialog), Hop Count specifies the maximum number of routers that the packets sent by Network Discovery can traverse. The default setting is 0 hops, which means that discoveries are restricted to the local subnetwork. Specifying -1 for Hop Count causes Network Discovery to not limit its discovery.

---

**Note** – Depending on the size of your network, setting Hop Count to any value above 0 may result in very long discoveries. An alternative would be to limit the discovery to subnets, links, and routers for discoveries with a hop count greater than 0.

---

#### ▼ To Perform a Multihop Discovery On a Remote Network

1. In the Discover Network window, select the From Network toggle button in Types of Discovery.
2. In the Network field, enter the network name from which to initiate the discovery.
3. Select the number of hops, from the Hop Count menu, to set the boundary to discover for.
4. Click Start to begin the discovery.

### 3.9.4 More About Ping/SNMP Optimization

Setting optimal Network Discovery ping and timeout parameters, based on your network characteristics and the objects for which you are discovering, can have significant performance and reliability implications for the discovery process. To put it another way: if you set these parameters optimally, your network discovery will proceed smoothly and relatively quickly, but if your ping and timeout settings are wrong for your particular network, network discovery can take an extremely long time and/or not find all the components on your network.

The Network Discovery tool uses a set of ping, SNMP, and timeout algorithms that automatically optimize your Network Discovery ping and timeout settings based on the characteristics of your network and the components you are discovering. To use

this feature, select the Ping/SNMP optimization settings on the Discover Network Ping/SNMP/RPC tab that most closely match your network characteristics, and then Network Discovery will do the rest. Refer to Section 3.4 “Deciding Which Components to Discover” on page 3-8 for more instructions on setting Ping/SNMP options.

While it is possible to manually set Ping and timeout values from the `em_discover` command line, it is not always so easy to get these settings right. Moreover, the automatic Ping/SNMP algorithms dynamically vary these settings based on the network components you are discovering.

### 3.9.5 More About RPC Agents and SunNet Manager Proxies

SunNet Manager (SNM) RPC-based agents and proxy agents deployed on devices in your network can be used by Solstice EM as part of your strategy for managing network resources. The resource may be a machine, a component in a machine (such as a router interface card), or some other resource. The SNM agent may be local to or remote from that resource. For more information about using RPC agents in general, refer to the *Customizing Guide*.

## Viewing Network Components

---

The power of Solstice Enterprise Manager (Solstice EM) resides in one or more distributed Management Information Server (MIS) databases containing information about every component on your network. To use this power, though, you need a way to consolidate access to your MIS databases, and to design meaningful views of the information they contain.

Network Views is a graphical tool for viewing and working with the information in your MIS databases. You can create and save custom views of your network, in geographical or logical formats, and access the other Solstice EM tools through menu commands and point-and-click interaction with your managed objects. Think of Network Views as a convenient place from which you can visualize your network and initiate all of your day-to-day management functions.

With the Network Views tool, you can:

- View the managed objects on your network in geographical or logical formats
- Create and modify managed objects
- Launch requests against managed objects
- Receive data, reports, events, and traps from managed network components
- Monitor your network
- Display selected subsets of objects
- Switch among any number of customizable views
- Search for managed objects in the current view or across multiple views
- Launch other Solstice EM tools, either through menus or direct interaction with objects

This chapter provides background information about the Network Views tool, step-by-step instructions for using Network Views, and detailed reference information.

This chapter comprises the following topics:

- Section 4.2 “Getting Started With Network Views” on page 4-8
- Section 4.3 “Working With Views” on page 4-9
- Section 4.4 “Configuring Object Icons and the Workspace” on page 4-23
- Section 4.5 “Managing Object Properties” on page 4-39
- Section 4.6 “Working With Alarms” on page 4-53
- Section 4.7 “Working With Requests” on page 4-56

---

## 4.1 Overview

Every managed object in a Solstice EM MIS can be represented as a icon in a Network Views window. These icons can include representations of physical network components, such as routers, hubs, switches, gateways, and hosts, and logical constructs, like universes, subnetworks, and domains.

You can point and click on these Network Views icons to initiate actions on the managed objects they represent. For example, by default, double-clicking on an object icon opens the Solstice EM Alarms tool, and right-clicking displays a pop-up menu, from which you can display the Object Properties dialog box and modify properties for the managed object. You can change the default behaviors of mouse clicks and menus to suit your needs, and you can define custom views to display whatever groupings of icons you want.

Before using Network Views, it is important to understand a few basic Network Views concepts and to have a sense of the kind of tasks you can perform from the Network Views window. Basic Network Views concepts are explained in the following section.

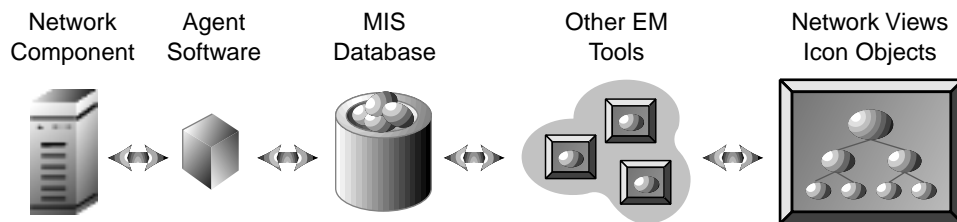
## 4.1.1 Basic Network Views Concepts

There are seven basic items with which you work in a Network Views window:

- **Component Representations** – The Network Views tool shows you *snapshots*, or instances, of the resources on your network—not the resource itself. Put another way, there are several layers of abstraction between what you see in a Network Views window and the actual network component being managed. Intrinsic to this concept are software *agents*, which intercede between your network components and the rest of Solstice EM. See Section 4.1.1.1 “Component Representations” on page 4-4, below, for more information.
- **Object Properties** – An important component of the Network Views tool is the Object Properties dialog box, from which you can create managed objects, and get and set object properties on all managed objects in the MIS. See Section 4.1.1.2 “Object Properties” on page 4-4 for an introduction to object properties concepts.
- **Icon Objects** – There are seven general types of Network Views icon objects, each representing a different type of network component or logical construct; these are described in Section 4.1.1.3 “Icon Objects” on page 4-5.
- **Saved Views** – Defined sets of icons representing sets of managed objects let you look at your network in any number of different ways according to your needs. Network views are described more in Section 4.1.1.4 “Saved Views” on page 4-6.
- **Object Alarms** – Alarms generated by managed network components can be propagated to object icons in a Network Views window. For example, if a router fails, the alarm generated by that event can be represented by changing the color of the Network Views icon object associated with the component. The specific color used can vary depending on the alarm severity. You can clear alarms or launch the Alarms tool directly from the Network Views window. See Section 4.6 “Working With Alarms” on page 4-53 for more information.
- **Advanced Requests** – You can configure Solstice EM to take various actions based on status information obtained or received from managed objects. Such sets of actions are defined by means of *request templates*—rules for the kind of object information to obtain or accept, and what to do in response. See Section 4.7.1 “Viewing Advanced Request Information” on page 4-57 for general instructions on using the Requests tool through the Network Views tool. See the *Customizing Guide* for more detailed information about working with automated requests and request templates.
- **Basic Requests** – You can perform customized performance and fault monitoring of managed objects by using the Basic Requests tool. See Section 4.7.2 “Viewing Basic Request Information” on page 4-57 for general instructions on using the Basic Requests tool. See the *Customizing Guide* for more detailed information about configuring and working with basic requests.

### 4.1.1.1 Component Representations

When you view or manipulate icons in a Network Views window, you are, in fact, working with *representations* of the managed objects in your MIS, not the network components themselves. You could, for example, use several different icons to represent a single MIS managed object, depending on the kinds of management tasks you want to perform. Everything you do in Network Views—retrieve and set object properties, clear alarms, launch other tools, and so forth—acts upon the managed objects in your MIS.



**FIGURE 4-1** Network Component Representation in Network Views

Managed objects in the MIS, in turn, are representations of software *agents* that interact with the real, physical components on your network—that is, you could have several managed objects in the MIS all referring to the same physical network component.

When you finally get down to the real, physical component level, software agents associated with a given component are what actually perform most management functions. Moreover, the capabilities of the agent object associated with a component will constrain what you can see or do with that component in the Network Views window, and the results of any management action performed on a given component depend on the interaction of other management objects and agents associated with that component.

### 4.1.1.2 Object Properties

Every managed object definition includes a set of attributes on which the object's programmatic methods can act. The behavior of a given real world network component depends on the properties—that is, the specific attribute values—used for the managed object instance representing that component.

To put it another way, every physical network component can be represented by one or more particular types of managed objects. The type of managed object used to represent a component has associated with it a set of attributes that define what kind

of information and settings can be gathered from, or applied to, the component. In Solstice EM, object properties refer to the specific values used for a given set of attributes for a given object type.

For example, a Printer Device object provides attributes for host name, printer type, and IP address, among others, whereas a Router Device provides attributes for IP address, port number, and so forth. The values you specify for a given object's attributes are referred to collectively as the object's *properties*.

See Section 4.5 “Managing Object Properties” on page 4-39 for more information about working with object properties.

### 4.1.1.3 Icon Objects

As views, or access points, into MIS managed objects, Network Views icon objects represent two related groups of MIS objects:

- A topology object (topoNode object), the attributes of which specify an object's location in a network topology.
- One or more agent objects internal to the MIS that inform the MIS which protocol to use to manage a given network component.































Network Views lets you work with several different icon object *types*. The following table briefly describes the default Network Views icon object types.

**TABLE 4-1** Network Views Default Icon Object Types

Object Type	Description
Array	Contains groups of objects in a compact array; object names are displayed in the array cells.
Bus	Multisegmented line; links objects that are connected to it.
Container	Contains other objects, such as views, networks, and subnetworks.
Device	Physical components, such as hosts, routers, hubs, and printers.
Link	Connects two other objects; link containers can contain other links.
Monitor	Container object divided into one or more sections; each section contains a view of one of the objects contained in the monitor.
RouterArray	Allows to use this object type as an array; each array cell contains an object name.
RouterContainer	Allows to use this object type as a container; contains the objects in the router.
Vendor-specific	Custom or platform-specific objects; for example, Sun hardware.

Within each category of icon object type are one or more object icons representing a particular component or logical construct. The table Table 4-2 shows the standard object icons with which you will work most often.

**TABLE 4-2** Common Network Views Object Icons

					
Array	Bridge	BSC	BTS	Bus	Bus Container
					
Circle	Container	Device	Hexagon	Hexagon120	HLR
					
Host	Hub	Interface	Java	Link	MSC
					
Network	OMC	Omnisector	PC	Printer	Router
					
Server	SPARC	Subnetwork	Universe	VLR	XCDR

You can define additional object icons and object icon types as needed for your environment. See Section 4.4.11 “Adding an Object Type to the Object Palette” on page 4-37 for more information about adding object types to your Solstice EM environment.

#### 4.1.1.4 Saved Views

In the Network Views tool, a *view* is a named collection of icons representing a set of managed objects or logical constructs. Views themselves are represented as a kind of container object in the MIS.

The Network Views window displays one view at a time. You can easily switch back and forth among different views, and you can also run multiple instances of the Network Views tool so you can display multiple views simultaneously.



You can display two general types of views:

- **Logical** – Logical views can contain other logical views. An example of a hierarchically branched view of logically related network components is a network containing multiple subnetworks. The network could be one view, and each subnetwork within it could have its own view. In this case, the primary network view would contain the subnetwork views. An example of a non-topological view distinct from your network topology is one that shows all your administration building routers in one view and all your campus file servers in another view. Logical views emanate from the `root` view separately from your topological views.
- **Geographical** – A view of network components mapped in a representation of their physical location. The user can place nodes at longitudinal and latitudinal coordinates on this geographical map.

## 4.1.2 Related Tasks

- Discovering Network Components – Chapter 3
- Managing Alarms – Chapter 5
- Managing User Access – Chapter 6
- Viewing CMIP, SNMP, and RPC Data – Chapter 9

## 4.1.3 Related Files

- `$EM_HOME/bin/em_viewer` – Network Views executable
- `$EM_HOME/bin/em_oct` – Object Properties executable
- `$EM_HOME/bin/em_layout` – Network Views Layout executable
- `$EM_HOME/bin/em_simplerequests` – Simple Requests executable
- `$EM_HOME/bin/em_layout` – Requests Editor executable
- `$EM_HOME/config/em_viewer.cf` – Network Views user preferences file
- `$EM_HOME/config/em_viewer.ad` – Network Views resource file
- `$EM_HOME/config/em_viewer.access.cf` – Network Views application access control file
- `$EM_HOME/config/EM_viewer` – Network Views shared EM application resource file
- `$EM_HOME/config/em_oct.ad` – Object Properties resource file
- `$EM_HOME/config/EM_oct` – Object Properties shared Solstice EM application resource file

---

**Note** – By default, `$EM_HOME` is the `/opt/SUNWconn/em` directory.

---

## 4.1.4 Further Reading

- *MIS Guide for Solstice EM* – Provides information about working with MIS databases
  - *Customizing Guide for Solstice EM* – Provides information about configuring the Solstice EM environment
- 

## 4.2 Getting Started With Network Views

You can start the Network Views tool from the command line, the Network Tools window, or the Tools menu in one of the other Solstice EM tools. Unlike most of the other Solstice EM tools, Network Views is a purely graphical tool—no matter how you start it, you will always get the Network Views graphical interface.

As with other Solstice EM tools, before running Network Views, you must configure your environment settings with `emenv.csh` or `emenv.sh`, as described in Chapter 2.”

Having said this, it is important to note that one of the components of Network Views, the Object Properties window, is actually a separate binary from Network Views itself—that is, the Network Views binary is `em_viewer`, and the Object Properties binary is `em_oct`. Unlike Network Views, you *can* run `em_oct` directly from the command line, bypassing the graphical interface, and separately from Network Views. This can be especially useful if you want to use a script or a custom application to automate the creation or modification of managed objects.

Finally, you can only display one view at a time in a Network Views window, but you can run multiple instances of Network Views and display a different view in each window.

If you start Network Views without first running at least one Network Discovery to populate the MIS, Network Views displays only an empty `Root` view with no object icons. See Section 4.3.1 “Populating the Network Views Window” on page 4-9 for information about running a Network Discovery for the first time. See Chapter 3 “Discovering Network Components” for complete information about using the Network Discovery tool.

## ▼ To Use Network Views

1. **Start the Network Views tool in one of the following three ways:**
  - From the Network Tools palette, click Network Views.



FIGURE 4-2 Network Views Button

- From another Solstice EM tool, click Tools->Network Views.
- From an UNIX command prompt, execute:

```
em_viewer -options
```

See TABLE 4-4 on page 4-62 for a complete list of Network Views command-line options. After starting Network Views in any of the above ways, the Network Views window is displayed.

2. **From the Network Views window, perform one or more tasks, as described in this chapter.**

Refer to the subsequent procedures in this chapter and to Section 4.8 “Reference” on page 4-61 for complete information about the various Network Views tasks and tools.

3. **Click File->Exit to close the Network Views window.**

---

## 4.3 Working With Views

This section provides step-by-step instructions for getting around in the Network Views window, creating views, and viewing, selecting, and searching for objects.

### 4.3.1 Populating the Network Views Window

If you start Network Views without first running at least one Network Discovery to populate the MIS, Network Views displays only an empty `Root` view with no object icons. While you can manually create managed objects using the Object Properties dialog, as described in Section 4.5.4 “Creating New Managed Objects” on page 4-42, the fastest and easiest way to populate the Network Views window is to run a Network Discovery.

## ▼ To Populate the Network Views Window

### 1. Start the Network Discovery tool in one of the following three ways:

- From the Network Tools window, click Discover/Monitor.



FIGURE 4-3 Network Discovery Button

- From the Network Views window, click Tools->Network Discovery.
- From an UNIX command prompt, type:

`em_discover -options`

Refer to TABLE 3-1 on page 3-18 for a complete list of Network Discovery command-line options.

- ### 2. From the Network Discovery window, select the various Discover options you want to use, or load an existing Network Discovery rules file, and then initiate the discovery process.
- ### 3. When the discovery process is complete, click File->Exit to close the Network Discovery window.

See Chapter 3 "Discovering Network Components" for complete information about using the Network Discovery tool.

## 4.3.2 Selecting a View

Each view in a Network Views window lets you look at a selected subset of your network. The Available Views pane on the left side of the Network Views window displays a branched tree list of the views available to you, starting from the topmost view, called `Root`. The specific views available depends on the views that have been defined. You can only display one view at a time in a Network Views window, but you can switch between views any time you want.

---

**Note** – You can run multiple instances of Network Views, each showing a different view, to display multiple views simultaneously.

---

## ▼ To Select a View

- **Use any one of the following six methods to select a view:**
  - Double-click an object in the Available Views pane on the left side of the Network Views window.
  - Double-click a container object (this default behavior can be changed).
  - Select the view you want from the Visited Views drop-down list, located just beneath the Network Views toolbar.
  - Right-click a container object or any object in the Available Views pane, and then click Display View from the pop-up menu.
  - Click View->View List to display the View List dialog, and then choose the name of the view you want to display.
  - Type the view name in the Find by Name field at the top of the Network Views window.

### 4.3.3 Starting Network Views in a Specific View

By default, Network Views displays the `Root` view on startup. You can temporarily override this default behavior or specify a new default behavior to display whatever view you want when you start Network Views.

## ▼ To Temporarily Override the Default View Setting

- **Start Network Views from the command line using the `-view` option; that is:**  

```
em_viewer -view viewname
```

where *viewname* refers to the view you want to display. View names are case-sensitive, and you can only specify one view at a time. The *viewname* you specify is only used for the instance of Network Views being invoked; it is not saved as a new default for subsequent instances of Network Views.

## ▼ To Specify a New Default View

1. In the Network Views window, click **File->Customize->Display Settings** to display the Display Settings dialog box.
2. Select the **Display** tab, if it is not already selected.
3. Type the name of the view you want to use as the new default in the **Default View** field, and then click **OK**.

You can also modify the command line used to invoke Network Views from the various Solstice EM Tools menu, and the Network Views button in the Network Tools window, so that Network Views always starts with the view of your choice. See Section 4.4.8 “Configuring the Tools Menu” on page 4-34 for instructions on configuring the Network Views Tools menu. These instructions apply to configuring the Tools menu in other Solstice EM tools in general. Also see Section 2.8 “Modifying Tool Configurations” on page 2-11 for detailed instructions on configuring the Network Tools window.

## 4.3.4 Displaying and Selecting Objects

You can display objects by opening the view in which the object is located, or by using one of the Network Views search methods described in the next section, “Searching for an Object” on page 4-12.

Once an object is displayed, you can select it and perform management functions with it. For example, you could manage alarms, view or modify object properties, or copy objects to other views.

### ▼ To Display and Select an Object Within a View

- 1. Open the view in which the object is located.**

If you do not know where the object is located, use the search methods described in the next section.

- 2. Click once on the object to select it; use Control-click to select multiple objects.**

Alternatively, you can select multiple objects by clicking and dragging to draw a bounding box around a group of objects.

## 4.3.5 Searching for an Object

Network Views provides two ways to search for objects in the current view or across multiple views:

- Directly typing the name of the object in the Find by Name field.
- Using the Actions->Find dialog.

## ▼ To Search for an Object Using Find by Name

1. **In the Network Views main window, type the name of the object you want to find in the Find by Name field, just below the Network Views toolbar, and then press Enter.**

If only one such object exists, the view in which the object is located is opened and the object is selected. If multiple objects exist, the Multiple Views dialog is displayed, listing all instances of the object.

2. **In the Multiple Views dialog, select the object you want to view, and then click Go to View.**

## ▼ To Search for an Object Using the Find Dialog

1. **In the Network Views window, click Actions->Find to display the Find dialog.**
2. **Select the name of the MIS in which you want to search.**

By default the MIS loaded when you started Network Views is selected.

3. **Select the object type and/or type the name of the object for which you want to search.**

You can use either or both of these options. Separate multiple object names with spaces.

4. **Click Find to initiate the search.**
5. **In the Results pane, select the object you want to view.**
6. **Click Go to View to display the view containing the object.**

### 4.3.6 Creating a Logical (Non-topological) View

You can create logical views—also known as non-topological views—that are based on logical relationships you define, rather than on physical network hierarchy. For example, you could create a view showing all your administration building routers in one view and all your campus file servers in another view.

The process of creating or modifying a logical view involves two general steps:

1. Select the objects you want to include in the logical view.
2. Add the selected objects to the new or existing logical view.

These steps are described in more detail below.

---

**Note** – By default, when you run a Network Discovery, a topological view is created—that is, a hierarchical view that directly corresponds to your physical network topology. You can override this behavior in the Network Discovery tool, so that newly discovered object will be added to a logical view. See Section 3.7 “Creating a New MIS Managed Object Database” on page 3-13 for more information.

---

## ▼ To Create a Logical View

1. **In the Network Views window, click Actions->Find to display the Find dialog.**
2. **Select the name of the MIS in which you want to search for objects.**  
By default the MIS loaded when you started Network Views is selected.
3. **Select the object type and/or type the name(s) of the object(s) for which you want to search.**  
You can use either or both of these options. Separate multiple object names with spaces.
4. **Click Find to initiate the search.**
5. **In the Results pane, select the object(s) you want to include in the logical view.**
6. **Click Add to View to display the Add To dialog.**  
Alternatively, you can drag-and-drop with the middle mouse button to drop the selected objects into the current view.
7. **Type a new or existing view name to which you want to add the selected objects, and then click Save.**
8. **Repeat Steps 2 through 7, if desired, to add other objects to the logical view; when you are finished, click Close to exit the Find dialog and return to the Network Views window.**

### 4.3.7 Creating a Network Views Icon Object

You can create new Network Views icon objects in any one of three ways:

- With the Actions->Create menu
- From the Tools->Object Palette
- From the View->Create View menu

Note that the last method, using the View->Create View menu, only lets you create new view objects—that is, a container object of some type.



## ▼ To Create an Icon Object With the Actions->Create Menu Item

- **In the Network Views window, click Actions->Create->*object type*, where *object type* is the type of object you want to create.**

The Object Properties dialog is displayed (same as invoking `em_oct` from the command line), from which you can specify various properties for the new icon object. See Section 4.5.4 “Creating New Managed Objects” on page 4-42 for more information.

## ▼ To Create an Icon Object From the Object Palette

1. **In the Network Views window, click Tools->Object Palette to display the Network Views Object Palette.**
2. **Select the desired subset of object types to display in the palette, if desired, by selecting the type you want from the Object Types drop-down list.**
3. **Double-click the icon representing the type of object you want to create.**

The Object Properties dialog is displayed (same as invoking `em_oct` from the command line), from which you can specify various properties for the new icon object. See Section 4.5.4 “Creating New Managed Objects” on page 4-42 for more information.

Alternatively, you can drag-and-drop with the middle mouse button to drop the selected objects from the object palette into the current view. This method does not open the Object Properties dialog.

## ▼ To Create a View Object with the View->Create View Menu Item

- **In the Network Views window, click View->Create View->*object type*, where *object type* is the type of container object you want to create.**

The Object Properties dialog is displayed (same as invoking `em_oct` from the command line), from which you can specify various properties for the new view object. See Section 4.5.4 “Creating New Managed Objects” on page 4-42 for more information.

## 4.3.8 Editing View Contents

You can copy and paste icon objects from one view to another. This can be a convenient way to build custom views. Alternatively, you can use the Actions->Find dialog to add selected objects to a view.

### ▼ To Copy and Paste Objects From One View to Another

1. **Display the view containing the object(s) you want to copy.**
2. **Select the object(s) you want to copy.**
3. **Click Edit->Copy.**
4. **Switch to the view into which you want to copy the object(s).**
5. **Click Edit->Paste to paste the objects into the current view.**

### ▼ To Add Objects to a View With the Find Dialog

1. **In the Network Views window, click Actions->Find to display the Find dialog.**
2. **Select the name of the MIS containing the object(s) you want to add to a view.**  
By default the MIS loaded when you started Network Views is selected.
3. **Select the object type and/or type the name(s) of the object(s) for which you want to search.**  
You can use either or both of these options. Separate multiple object names with spaces.
4. **Click Find to initiate the search.**
5. **In the Results pane, select the object(s) you want to include in a different view.**
6. **Click Add to View to display the Add To dialog.**
7. **Type the name of the view to which you want to add the selected objects, and then click Save.**

If you specify a new view name here, a view is created as a container object of the type `Subnet` in the Root view.

## 4.3.9 Deleting Objects From a View

You can delete objects from individual views or from all views in which they may be located.

---

**Caution** – Deleting icon objects from a view also deletes that object from the MIS. If you delete all instances of an object in all views, you will have also completely deleted that object from the MIS.

---

### ▼ To Delete Objects From a View

1. Display the view containing the object(s) you want to delete.
2. Select the object(s) you want to delete.
3. Click **Actions->Delete**.

If the object exists in more than one view, you are asked whether you want to delete it in just the current view or in all views.

## 4.3.10 Zooming In or Out in the Current View

Network Views provides several zoom controls that let you adjust the magnification of a view or view region for the current view. Specifically, you can:

- Zoom in and out
- Zoom in on an area
- Reset the zoom level to 100%
- Move backward and forward through your zoom history
- Set the zoom increment

The Network Views zoom controls are available from the **View->Zoom** menu and from the Network Views toolbar, both of which are in the Network Views main window.



**FIGURE 4-4** Network Views Toolbar Zoom Controls

The zoom level you set with the View->Zoom command applies to the current view only. To set zoom parameters for Network Views in general, use the procedures described in Section 4.4.3 “Configuring Zoom Settings” on page 4-25.

## ▼ To Use View Zoom Controls

- In the Network Views main window, use either of the two following methods:
  - Click the toolbar button for the zoom function you want to use
  - Click View->Zoom, and then choose the zoom function you want to use

### 4.3.11 Navigating in Geographical Map Views

When you use a geographical map background in a view, the Network Views main window displays three additional Map toolbar buttons to the right of the Zoom controls. You can use these buttons to center the map in the view window, and pan across the map to see objects beyond the window edge.

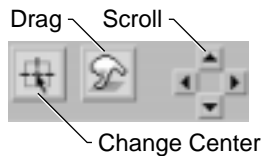


FIGURE 4-5 Network Views Map Toolbar

See Section 4.4.6 “Using Background Images” on page 4-31 for information about configuring geographical map backgrounds.

## ▼ To Navigate in a Geographical Map View

- In the Network Views main window, click the button on the Map Toolbar for the navigational function you want to perform:
  - To center the map in the view window, click the map centering button.
  - To pan across the map, click the pan button, and then drag the mouse in the direction you want to view.
  - To scroll the map, use the scroll buttons on the toolbar.

Alternatively, you can use the commands on the View->Background menu in the Network Views main window.

---

**Note** – The Map Toolbar and the View->Background menu are only enabled if you have configured Network Views to use a geographical map background. See Section 4.4.6 “Using Background Images” on page 4-31 for more information.

---

## 4.3.12 Changing Icon Size in the Current View

You can change the size of icons in the current view by using the View->Icon Size command in the Network Views main window.

The icon size you set with the View->Icon Size command applies to the current view only. To set icon size parameters for Network Views in general, use the procedures described in Section 4.4.2 “Configuring Icon and Label Display” on page 4-24.

### ▼ To Set the Icon Size in the Current View

- **In the Network Views main window, click View->Icon Size, and then select the relative percentage you want to use to display icons.**

## 4.3.13 Changing Label Size for the Current View

You can change the size of icon labels and view labels in the current view by using the View->Label Size command in the Network Views main window. Sizes are expressed as points in the current font.

The label size you set with the View->Label Size command applies to the current view only. Also, you can only change the label size with this command, and not the label font. To set label size and font parameters for Network Views in general, use the procedures described in Section 4.4.2 “Configuring Icon and Label Display” on page 4-24.

### ▼ To Set the Label Size in the Current View

- **In the Network Views main window, click View->Label Size, and then select the point size you want to use to display labels.**

## 4.3.14 Changing the Background Image for the Current View

If a particular view is configured to use a background image, you can change the image that is used by modifying the container object's properties with the Object Properties tool.

---

**Note** – These instructions describe only how to *change* the background image used for a view. To use these instructions, you must configure the object and the Network Views tool to use background images, as described later in this chapter, in Section 4.4.6 “Using Background Images” on page 4-31.

---

### ▼ To Change the Background Image for the Current View

1. **Right-click the container object for which you want to change the background image, and click Properties from the pop-up menu.**
2. **In the Object Properties dialog, select the Display tab.**
3. **Type or browse for the name of the background image or geographical map background you want to use.**
4. **Click Apply.**

## 4.3.15 Displaying Specific Object Types

Each of the Network Views object types—for example, Links, Hosts, Routers, Networks, and so forth—are stored in distinct logical layers. By default, all of these logical layers are displayed in any given view. If a large number of objects are in a single view, you may want to suppress the display of selected object types to make it easier to sort through the view.

---

**Note** – The Object Layers selection you make applies to all views in the current instance of Network Views. You can run multiple instances of Network Views, with each using a different Object Layers setting.

---

## ▼ To Display Only Specific Object Types

1. In the Network Views main window, click **File->Customize->Object Type Layers** to display the Object Type Layers dialog box.
2. Select **Selected Object Layers** option.
3. Select the Object Layers you want to display.
4. Click **OK**.

### 4.3.16 Displaying Specific Map Layers

If you are using a geographical map for a view background, you can use the **View->Background->Layers** dialog to display only specific map layers. Similar to displaying specific object type layers, described above, this option can be useful for working with large or complex views.

See Section 4.4.6 “Using Background Images” on page 4-31 for instructions on configuring views to use background images, including geographical maps.

## ▼ To Display Only Specific Map Layers

1. Ensure that the display of geographical map backgrounds is enabled, as described in Section 4.4.6 “Using Background Images” on page 4-31.
2. In the Network Views main window, click **View->Background->Layers** to display the Map Layers dialog.
3. In the Map Layers dialog, enable the **Selected Map Layers** option.
4. Select the map layers you want to display.
5. Click **OK**.

The specific map layers available depend on the map file you are using.

## 4.3.17 Saving and Loading View Settings

You can save your view settings—icon location, zoom area, icon and label sizes—so that when you restart viewer, these settings are used by default. Similarly, after moving icons, changing zoom levels, and resizing icons and labels, you can restore your initial view settings to get back to where you started.

When you exit Network Views, if any of your view settings have changed, you are prompted to save the changes.

### ▼ To Save View Settings

1. **Arrange your view to your liking.**  
For example, Layout, Icon Size, Label Size, Zoom.
2. **Click View->Save Initial Values to View to display the Save to View dialog.**
3. **Select the location and zoom/size options, as desired.**
4. **Click Save.**

### ▼ To Restore View Settings

- **Click View->Load Initial Values from View.**

## 4.3.18 Viewing the Network Views Message Log

The Network Views Message Log displays system messages returned by Network Views. For example, viewing object properties spawns the `em_oct` process; this action, along with the parameters passed to `em_oct`, are displayed in the Network Views Message Log.

### ▼ To View the Network Views Message Log

- **In the Network Views main window, click Tools->Message Log.**



---

## 4.4 Configuring Object Icons and the Workspace

This section provides step-by-step instructions for configuring the Network Views workspace, menus, and default behaviors.

You may also want to refer to the following sections for information about other Network Views tasks:

- Section 4.2 “Getting Started With Network Views” on page 4-8
- Section 4.3 “Working With Views” on page 4-9
- Section 4.5 “Managing Object Properties” on page 4-39
- Section 4.6 “Working With Alarms” on page 4-53
- Section 4.7 “Working With Requests” on page 4-56

### 4.4.1 Configuring General Display Properties

The Network Views window can be configured to display object information in a variety of ways with the settings on the Display tab in the File->Customize->Display Settings dialog. Specifically, the general Display settings are:

- Canvas Layout
- Default View
- Alarm Severity Relationships
- Show Severity on Label Background
- Display Background Image

The settings you choose are used for all views in the current instance of Network Views. Subsequent instances of Network Views also inherit the settings.

Many display options can also be used on a per object basis. For example, you can specify background image and alarm severity propagation for an individual container object. See Section 4.5.3 “Modifying Object Properties” on page 4-41 for instructions on modifying individual object properties.

### ▼ To Configure General Display Properties

1. In the Network Views main window, click File->Customize->Display Settings to display the Display Settings dialog box.
2. Select the Display tab, if it is not already selected.

**3. Select a Canvas Layout option.**

- **Logical** – Default setting; displays hierarchical or logical view.
- **Geographical** – Lets you associate objects with a position on a geographical map.

**4. Type the name of a Default View.**

See Section 4.3.3 “Starting Network Views in a Specific View” on page 4-11 for more information about default views.

**5. Enable or disable the display of Alarm Severity Relationships.**

Enabling this option displays peer to peer propagation relationships drawn as dashed lines from node to node in the relationship. An arrow indicates the direction of propagation. Enabling this option causes Network Views to display the associated alarm severity color on the label in addition to the icon. The colored icon objects and labels give the node’s condition greater visibility. For objects without children, this color is the same as that for Propagated Alarm Severity. See Section 4.6.3 “Propagating Alarm Severity” on page 4-54 for more details.

**6. Enable or disable the Show Severity on Label Background option.**

Enabling this option colors icon labels based on alarm severities, as described in Section 4.4.4 “Customizing Color Settings” on page 4-26.

**7. Enable or disable the Display Background Image option.**

Enabling this option causes the currently selected background image to be displayed. See Section 4.4.6 “Using Background Images” on page 4-31 for more information.

**8. Click OK to apply your settings and exit the Display Settings dialog, or click Apply if you want to modify other settings in the dialog before exiting.**

## 4.4.2 Configuring Icon and Label Display

You can separately configure the display of icons and icon labels in Network Views windows. Specifically, you can specify default size, scaling and font sizes with the settings on the Icon/Label tab in the File->Customize->Display Settings dialog box.

Icon and icon label colors are specified on the Colors tab in the same dialog box, as described in Section 4.4.4 “Customizing Color Settings” on page 4-26.

## ▼ To Configure Icon and Label Display

1. **In the Network Views main window, click File->Customize->Display Settings to display the Display Settings dialog box.**
2. **Select the Icon/Label tab, if it is not already selected.**
3. **Select a default Icon Size.**

Icon sizes are displayed in terms of percentages of icon size, as defined in given file. Icon files are stored by default in the `$EM_HOME/glyphs` directory.
4. **Select Icons always display using this value, if desired.**

Selecting this option causes all icons to be displayed at the same size, regardless of zoom level or any previously saved view settings. Selecting this option disables the View->Icon Size command in the Network Views main window.
5. **Select an icon Label Font.**

This is the font that will be used to display all icon labels.
6. **Select an icon Label Size.**
7. **Select Labels always display using these values, if desired.**

Selecting this option causes all icon labels to be displayed at the same size, regardless of zoom level or any previously saved view settings. Selecting this option disables the View->Label Size command in the Network Views main window.
8. **Click OK to apply your settings and exit the Display Settings dialog, or click Apply if you want to modify other settings in the dialog before exiting.**

### 4.4.3 Configuring Zoom Settings

You can specify how icons and icon labels are scaled, zoom increments, and the zoom level at which icon labels are suppressed, by using the settings on the Zoom tab in the File->Customize->Display Settings dialog.

---

**Note** – The settings on this tab are only used if either or both the “Icons always display using this value,” or “Labels always display using these values” options are left unselected on the Icon/Label tab, described above.

---

## ▼ To Configure Zoom Settings

1. In the Network Views main window, click **File->Customize->Display Settings** to display the Display Settings dialog box.
2. Select the **Zoom** tab, if it is not already selected.
3. Click **Modify**, if you want to specify icon and icon label maximum and minimum scaling settings.

The Variable Icon/Label Size dialog is displayed.

- a. Select the **minimum icon size to display**.
- b. Select the **minimum zoom level at which the minimum icon size will be displayed**.

Icon sizes will not scale any smaller than the minimum size at the minimum zoom level.

- c. Select the **maximum icon size to display**.
  - d. Select the **maximum zoom level at which the maximum icon size will be displayed**.
- Icon sizes will not scale any larger than the maximum size at the maximum zoom level.

#### 4. Select a Zoom Increment.

The percentage you specify is used each time you click one of the Network Views zoom tools, described in Section 4.3.10 “Zooming In or Out in the Current View” on page 4-17.

5. Select a percentage below which the display of icon labels will be suppressed.
6. Click **OK** to save your settings and exit the Display Settings dialog, or click **Apply** if you want to modify other settings in the dialog.

## 4.4.4 Customizing Color Settings

You can use the options on the Colors tab in the File->Customize->Display Settings dialog box to specify colors for general presentation purposes and to indicate alarm status. Specifically, you can control colors for:

- **Alarm Status** – Specify whether you want the icon status color source to be based on alarm severity, propagated alarm severity, or some user-defined color definitions.
- **Presentation** – Specify colors to use for the viewer background (canvas), selected objects, and object label text.

## ▼ To Specify Alarm Status Color

1. In the Network Views main window, click File->Customize->Display Settings to display the Display Settings dialog box.
2. Select the Colors tab, if it is not already selected.
3. In the Icon Status Color Source group, select the color source option you want to use:

- **Alarm Severity** – Icons are colored based on the most severe outstanding alarm posted against their associated object (topoNode). See TABLE 4-3, below, for a list of the default alarm severity colors used by Network Views.
- **Propagated Alarm Severity** – Icons are colored based on the most severe propagated severity or all objects contained within a given object. For objects without children, this is the same as Alarm Severity. For container objects, the propagated severity is the most severe outstanding alarm posted against the container and all its children. This severity is evaluated recursively for all containers within containers. This is the default setting.
- **User-defined** – An advanced option that allows you to specify the name of a script or program containing color data and alarm mapping logic. Icon color is based on values set in the `topoNodeDisplayStatus` attribute for MIS objects. This attribute contains a list of tag/value pairs, for example:

```
{ { "Netload", 4 }, { "MySeverity", 3 } }
```

Typically, you would write your own client/daemon program which would update the `topoNodeDisplayStatus` based on your criteria. Note that in order for the tag values (for example, `Netload` and `MySeverity`) to display in the User-Defined option menu, you must add the tags to the `topoAllStatus` attribute of the `topoNodeDB=NULL` object; for example:

```
{ "Netload", "MySeverity" }
```

The same color mapping used for severities is used for the user-defined values; consequently, the values must be between 0 and 5. You can add more color mappings, as well. This requires using the Object Properties tool to add more objects.

4. Click OK to save your settings and exit the Display Settings dialog, or click Apply if you want to modify other settings in the dialog.

The following table lists the default alarm severity mapping used by Network Views.



**TABLE 4-3** Default Alarm Severity Color Mapping

Color	Alarm Severity
Red	Critical
Orange	Major
Cyan	Minor
Yellow	Warning
Blue	Indeterminate

## ▼ To Set Network Views Presentation Colors

1. In the Network Views main window, click **File->Customize->Display Settings** to display the Display Settings dialog box.
2. Select the **Colors** tab, if it is not already selected.
3. In the **Presentation** group, select the item you want to modify, and then click **Modify** to open the Color Chooser dialog box.

You can modify the colors for Viewer Canvas (background), Object Selection, and Object Label Text.

- a. Grab a color, if desired, from another item on your desktop, by clicking **Grab Color** and then clicking on the item with the desired color.
  - b. Use the Color Editor controls, if desired, to create a custom color.
    - **R, G, and B** – Red, green, and blue color values
    - **Hue** – Color balance
    - **Saturation** (  ) – Color purity
    - **Brightness** (  ) – Dark/light value
  - c. Click **OK** to save the color and return to the Display Settings dialog.
4. Repeat Step 3 for each item you want to modify.
  5. Click **OK** to save your settings and exit the Display Settings dialog, or click **Apply** if you want to modify other settings in the dialog.

## 4.4.5 Customizing View Layout

You can arrange the icons in your views in four general ways by using the View->Layout command in the Network Views main window. The four general layout patterns are as follows:

- **Tile**
- **Tree**
- **Mesh**
- **Cluster**

Following immediately below is the general procedure for customizing your view layout. Each layout style has its own set of options; refer to the subsequent procedures in this section to set options for the layout style you want to use.

The View->Layout command spawns the `em_layout` binary, if desired, you can run `em_layout` directly from the command line, outside of Network Views. See Section 4.8.1.3 “Network Views Layout Options” on page 4-63 for more information about the `em_layout` command.

### ▼ To Customize Your View Layout

1. **In the Network Views main window, click View->Layout to display the Layout dialog box.**
2. **Select the Layout Style you want to use from the drop-down list.**
3. **Specify the desired options for the layout style you have selected.**  
Refer to the procedures immediately below for more information.
4. **Click Apply to update the current view with the options you have selected without exiting the Layout dialog.**

---

**Note** – Your modifications affect only the current view in the current instance of Network Views. If you add icons to the current view after modifying the layout settings, the new icons do not automatically align according to your settings; you must use the Layout dialog again to apply layout settings to the new icons.

---

5. **Click View->Save Initial Values to View to save the new layout options.**
6. **Click OK to update the view and exit the dialog.**

## ▼ To Set Tile Layout Options

1. In the View->Layout dialog, select Tile from the Layout Style list.
2. Specify horizontal and vertical spacing values, as desired.
3. Specify whether you want the view to contain a fixed number of columns.  
If yes, the view will contain the number of columns you specify; otherwise the number of columns will vary according to window size.
4. Click OK or Apply to update the view with your settings.

## ▼ To Set Tree Layout Options

1. In the View->Layout dialog, select Tree from the Layout Style list.
2. Specify whether you want the tree orientation to be horizontal or vertical.
3. Specify whether you want objects at the same hierarchical level to be top-aligned, center-aligned, or bottom-aligned.
4. Specify horizontal and vertical spacing values, as desired.
5. Specify the minimum slope for connecting lines between icons.  
Depending on the number of objects in your view, this option can affect the width or height of the displayed object tree.
6. Click OK or Apply to update the view with your settings.

## ▼ To Set Mesh Layout Options

1. In the View->Layout dialog, select Mesh from the Layout Style list.
2. Select mesh options, as desired.
3. Click OK or Apply to update the view with your settings.

## ▼ To Set Cluster Layout Options

1. In the View->Layout dialog, select Cluster from the Layout Style list.
2. Select Cluster options, as desired.
3. Click OK or Apply to update the view with your settings.



## 4.4.6 Using Background Images

You can configure your Network Views container objects to display a background image. This image can either be a simple bitmap or a geographical map based on real-world latitude and longitude coordinates. For example, you could use a geographical map that displays a blueprint of your building with the location of servers and printers.

The procedure for using background images involves three general steps:

1. **Configure Object Properties** – You use the Object Properties dialog to specify the simple bitmap and/or geographical map you want to use for a container object background image.
2. **Enable the display of background images** – You can enable or disable the display of background images with the Display Background Image option on the Display tab in the File->Customize->Display Settings dialog.
3. **Enable either a logical or geographical image** – You can associate both a simple bitmap and geographical map with an object. The background image that is displayed depends on the Canvas Layout option you select on the Display tab in the File->Customize->Display Settings dialog. If you select Logical for the Canvas layout option, the simple bitmap is used; if you specify Geographical, the geographical map is used.

The procedures for using background images are described below. Please note that the instructions in this section describe the Object Properties dialog and the Display Settings dialog only to the extent required to configure background images. You may also want to refer to the following sections:

- Complete instructions for using the Object Properties dialog begin in Section 4.5 “Managing Object Properties” on page 4-39.
- Instructions for using the Display Settings dialog begin in Section 4.4.1 “Configuring General Display Properties” on page 4-23.
- Detailed information about the structure of geographical map backgrounds, including instructions for adding map backgrounds to your Network Views environment, are provided in Section 4.8.4 “More About Geographical Map Backgrounds” on page 4-72.

### ▼ To Use a Simple Bitmap Background

1. **In the Network Views main window, select the container object for which you want to use a background image.**

---

**Note** – Network Views supports Sun Raster files for background images.

---

2. **Right-click on the object to display the pop-up menu, and then click Properties to display the Object Properties dialog.**
3. **In the Object Properties dialog, select the Display tab.**
4. **Type or browse for the name of the Background Image you want to use.**
5. **Click Apply.**  
By default, background images are installed in the `$EM_HOME/images` directory.
6. **In the Network Views main window, click File->Customize->Display Settings to open the Display Settings dialog.**
7. **Select the Display tab, if it is not already selected.**
8. **Select Logical for the Canvas Layout option.**
9. **Select On for the Display Background Image option.**
10. **Click Apply or OK to update the selected view with the background image.**

## ▼ To Use a Geographical Map Background

1. **In the Network Views main window, select the container object for which you want to use a geographical map background.**

You can only use map backgrounds with container objects, like networks and subnetworks. You cannot use map backgrounds with non-container objects, like devices and links.

---

**Note** – Several sample geographical map files are provided with your Solstice EM distribution. To install the maps, refer to the instructions in the Solstice EM *Installation Guide*. The sample map data, if installed, is located by default in `$EM_HOME/mapdata` directory.

---

2. **Right-click on the object to display the pop-up menu, and then click Properties to display the Object Properties dialog.**
3. **In the Object Properties dialog, select the Display tab.**
4. **Type or browse for the name of the Geographical Map you want to use and then click Apply.**  
By default, geographical maps are installed in the `$EM_HOME/mapdata` directory.
5. **In the Network Views main window, click File->Customize->Display Settings to open the Display Settings dialog.**

6. Select the **Display** tab, if it is not already selected.
7. Select **Geographical** for the **Canvas Layout** option.
8. Select **On** for the **Display Background Image** option.
9. Click **Apply** or **OK** to update the selected view with the geographical map.  
See Section 4.3.11 “Navigating in Geographical Map Views” on page 4-18 for instructions on moving around in views that use a geographical map background.

## 4.4.7 Configuring Double-click Actions

You can use the **File->Customize->Double Click Action** command to configure the action that occurs when you double-click an object in the Network Views window. By default, double-clicking on container objects switches to the associated object view, whereas clicking on non-container objects, such as devices and links, opens the Alarms tool (`em_alarmmgr`).

You can configure a unique double-click action for each object type in your Network Views environment. For example, you can configure different actions for hubs and routers.

### ▼ To Configure Double-click Actions

1. In the Network Views main window, click **File->Customize->Double Click Action** to display the **Configure Double Click Action** dialog.
2. Select the object type for which you want to configure an action.
3. In the **Command** field, type the command you want to use for the double-click action, and then click **Apply**.  
See Section 4.8.2 “Network Views Command and Variable Macros” on page 4-65 for a list of the commands you can use in this field.
4. Repeat Steps 2 and 3 to configure additional double-click actions, if desired.

## 4.4.8 Configuring the Tools Menu

You can use the File->Customize->Tools Menu to add, modify, or remove commands from the Network Views Tools menu.

### ▼ To Add a Tools Menu Entry

1. **In the Network Views main window, click File->Customize->Tools Menu to display the Configure Tools dialog.**
2. **In the Applications list, select the name that precedes the list location where you want to insert the new application.**

For example, to insert a new tools menu entry after an existing application named “Application A,” select “Application A.”

3. **Type a new name in the Application Name field.**

This is the name that will be displayed on the Tools menu.

---

**Note** – If the Application Name field has not been changed before clicking Add, the user will receive the error message: “Add Failed: Duplicate Application Name.”

---

4. **In the Path to Executable field, type the path and name of the executable you want to associate with the menu entry.**

For example, if you wanted to add the Network Discovery tool (em\_discover) to the menu, you would type:

```
$EM_HOME/bin/em_discover
```

5. **In the Arguments field, type any command line arguments you want to pass to the executable.**

For example, if you wanted to run the Network Discovery GUI and connect to the default MIS, you would type:

```
-host EM_MIS -T
```

See Section 4.8.2 “Network Views Command and Variable Macros” on page 4-65 for a complete list of Network Views commands and variables.

6. **Click Add to post the new entry.**
7. **Click Apply to update the Tools menu.**
8. **Click Cancel to close the Configure Tools dialog.**

## ▼ To Modify a Tools Menu Entry

1. In the Network Views main window, click **File->Customize->Tools Menu** to display the **Configure Tools** dialog.
2. In the **Applications** list, select the name of the application you want to modify.
3. Enter modified parameters, as desired, in the **Application Name**, **Path to Executable**, and **Arguments** fields.

See Section 4.8.2 “Network Views Command and Variable Macros” on page 4-65 for a complete list of Network Views commands and variables.

4. Click **Change** to accept the modified entry.
5. Click **Apply** to update the **Tools** menu.
6. Click **Close** to close the **Configure Tools** dialog.

## ▼ To Delete a Tools Menu Entry

1. In the Network Views main window, click **File->Customize->Tools Menu** to display the **Configure Tools** dialog.
2. In the **Applications** list, select the name of the application you want to delete from the **Tools** menu.
3. Click **Delete**.
4. Click **Apply** to update the **Tools** menu, and then click **Close** to close the **Configure Tools** dialog.

## 4.4.9 Configuring Pop-up Menus

You can use the File->Customize->Pop-up Menus command to configure the menu that displays when you right-click an object in the Network Views window.

You can configure a unique pop-up menu for each object type in your Network Views environment. For example, you can configure different pop-up menus for hubs and routers.

### ▼ To Configure Pop-up Menus

1. **In the Network Views main window, click File->Customize->Pop-up Menu to display the Configure Pop-up Menu dialog.**

2. **Select the Device Type for which you want to configure a pop-up menu.**

The existing menu entries, if any, for the selected object type are displayed in the Menu Options list.

3. **If desired, select an Object Type from which you want to copy a menu configuration.**

Copying an existing menu configuration from another object type is often the easiest way to create or modify a pop-up menu. In many cases, you may find that similar devices—say a SPARC10 and SPARC20 workstation—can use the same pop-up menu configuration.

4. **Add, change, or delete Menu Options, as desired.**

See Section 4.8.2 “Network Views Command and Variable Macros” on page 4-65 for a list of Network Views commands.

5. **Click Apply to update your pop-up menus, and then click Close to close the Configure Pop-up Menu dialog.**

## 4.4.10 Configuring the Object Attributes Command

When you select an object in a Network Views window, and then click Actions->Properties, Network Views opens the Object Properties tool (`em_objt`) by default. You can configure Network Views to use another object editor, if desired, with the Misc tab in the File->Customize->Display Settings dialog.

## ▼ To Configure the Object Attributes Command

1. In the Network Views main window, click **File->Customize->Display Settings** to open the Display Settings dialog.
2. Select the **Misc** tab, if it is not already selected.
3. Type the command you want to use to handle object properties.

The default command is:

```
$EM_HOME/bin/em_oct -host EM_MIS
```

This command opens the Object Properties tool and connects to the MIS from which Network Views is running.

4. Click **Apply** or **OK** to update the Actions menu.

### 4.4.11 Adding an Object Type to the Object Palette

The Tools->Object Palette command displays all object types defined in your Network Views environment. The objects displayed here are also those that are available to the View->Create View and Actions->Create commands.

You can add new objects to the Object Palette by editing the Solstice EM `init_user` file. This is an advanced procedure done outside the Network Views interface, and involves instantiating objects in the MIS, and in some cases restarting the MIS.

## ▼ To Add an Object Type to the Object Palette

1. Determine the class of the object type (Device, Link, Container, and so forth) you want to add.

As an example, in this procedure, you will add a new Container class object called `Satellite`.

**2. Edit the `$EM_HOME/conf/init_user` file to provide the pertinent information.**

For example, to add Satellite as a new Container class, modify `init_user` to include the following entry (note exact punctuation):

```
CREATE
{
OC = topoType
SOI = 'topoTypeDBId=NULL'
topoTypeId = Satellite
topoTypeDerivedFrom = '{ "Container" }'
topoTypeDrawMethod=circle
topoTypeDefaultLayer = Default
}
```

By default, your Solstice EM installation includes this example in the `init_user` file, but the lines are commented out.

**3. Configure the new object type so it can be displayed in its own layer.**

To do this, the `topoTypeDefaultLayer` attribute needs to be changed to match the `topoTypeId` attribute. For example:

```
CREATE
{
OC = topoType
SOI = 'topoTypeDBId=NULL'
topoTypeId = SpecialView
topoTypeDerivedFrom = '{ "Container" }'
topoTypeDrawMethod=circle
topoTypeDefaultLayer = SpecialView
}

SET
{
OI = 'topoNodeDBId=NULL'
topoAllLayer += '{ "SpecialView" }'
}
```

**4. Create an icon for the Satellite Container class object and save it to the following file:**

`$EM_HOME/glyphs/Satellite.pm`

Network Views will look for the `Satellite.pm` file to obtain the icon associated with the `Satellite` object class. This icon must be in X pixmap format (xpm). Other formats may be incompatible with Network Views.



5. Use either of the following two methods to instantiate the `Satellite` object in the MIS.

- If you want to make the new object type available in the Object Palette without restarting the MIS, type the following command at a system prompt:

```
em_objop -f init_user
```

---

**Caution** – The following action will erase all existing information contained in the MIS.

---

- If you want to use the `em_services` command, you must restart the MIS using the `-i` option, which erases all existing information in the MIS, but preserves the `init_user` file:

```
em_services -i
```

When you restart Network Views, the new object type will be available from the Object Palette.

---

## 4.5 Managing Object Properties

This section provides step-by-step instructions for creating and deleting managed objects, and for viewing and modifying object properties.

You may also want to refer to the following sections for information about other Network Views tasks:

- Section 4.2 “Getting Started With Network Views” on page 4-8
- Section 4.3 “Working With Views” on page 4-9
- Section 4.4 “Configuring Object Icons and the Workspace” on page 4-23
- Section 4.6 “Working With Alarms” on page 4-53
- Section 4.7 “Working With Requests” on page 4-56

### 4.5.1 Getting Started With Object Properties

You can run the Object Properties tool as an integrated Network Views component, or as a standalone application. For example, by default, when you right-click a managed object, and then click Properties from the pop-up menu, the Object Properties dialog is displayed. You can also, if you wish, run Object Properties outside of Network Views, from the UNIX command line with the `em_oct` command.

You can use Object Properties to:

- View properties for an existing managed object
- Modify properties for an existing managed object
- Configure SNMP, CMIP, RPC, and MIS agent interaction with managed objects
- Create a new managed object

## ▼ To Run Object Properties From the Command Line

- **Type the following command at an UNIX prompt:**

```
em_oct -options
```

See Section 4.8.1.2 “Object Properties Options” on page 4-62 for a complete list of Object Properties command-line options.

## 4.5.2 Viewing Object Properties

The easiest way to view properties for an existing managed object is to use the Network Views graphical interface. You can also use the command line, if desired, with one or more of the options listed in Section 4.8.1.2 “Object Properties Options” on page 4-62. The procedure provided here is for viewing object properties from the Network Views interface.

## ▼ To View Properties for an Existing Object

- **In the Network Views main window, use either of the following two methods to display the Object Properties dialog:**
  - Right-click any object to display the object’s pop-up menu, and then click Properties.  
See Section 4.4.9 “Configuring Pop-up Menus” on page 4-36, if desired, for information about changing the default pop-up menus associated with different object types.
  - Select an object and then click Actions->Properties.

### 4.5.3 Modifying Object Properties

The easiest way to modify properties for an existing managed object is to use the Network Views graphical interface to invoke the Object Properties tool, and then modify the object properties as desired. You can also use the `em_oct` command line, if desired, with one or more of the options listed in Section 4.8.1.2 “Object Properties Options” on page 4-62.

The specific properties that you can modify may vary, depending on the type of object you want to modify. For example, the properties for a container object, like a network or subnetwork, are different than those for a device, like a workstation or a router.

Tasks for modifying object properties can be divided into six general categories:

- **Object Identification** – Object name and, in the case of container object, the list of all objects with which the object is associated.
- **Object Type** – Type of object; this option is restricted based on the category of object—that is, Container, Device, Monitor, and so forth—being modified.
- **Agent Communications** – Agent types and parameters for interactions between Solstice EM and SNMP, CMIP, RPC, and MIS agents.
- **Display** – How the managed object is displayed, including background images and related objects, in a Network Views window.
- **Coordinates** – Where the object is displayed in a Network Views window.
- **Stored Data** – Detailed information about the object; for example, IP address, description, and so forth.

The procedure below provides a high-level overview of the general steps required to modify managed objects. Subsequent procedures provide more detailed step-by-step instructions for configuring specific object properties. Please note that the instructions here describe how to modify object properties from within the Network Views interface.

#### ▼ To Modify a Managed Object

1. **In the Network Views main window, use any of the following methods to open the Object Properties dialog with the object you want to modify:**
  - Right-click any object and then click Properties from the pop-up menu.
  - Select an object and then click Actions->Properties.

If desired, you can also select multiple objects that share the same properties, and modify them all at once in the Object Properties dialog.

## 2. Modify the Object Identification fields, as desired.

- **Name** – The name of the managed object; this is the name that is displayed in Network Views windows.
- **Available Objects** – Use the Add and Delete buttons to add or remove objects from the available objects list. The objects in this list can be modified individually or as a group within the current instance of the Object Properties dialog.

## 3. Modify the Object Type, if desired.

You can only change the Object Type within the specific category already defined for the object. For example, if the object you are modifying is a Bridge (Device category), you can change the object to another type of Device, but all other categories will be unavailable.

## 4. Modify the Detailed Information fields, if desired.

- **Agents** – Create and modify SNMP, CMIP, RPC, and MIS agent communications. See Section 4.5.5 “Configuring Agent Communications” on page 4-44, later in this section for instructions.
- **Display** – How the managed object is displayed in a Network Views window, including background images and related objects. The settings here are related to the various Network Views display settings, descriptions for which begin in Section 4.4.1 “Configuring General Display Properties” on page 4-23.
- **Coordinates** – Logical or geographical coordinates specifying the position of the managed object icon in a Network Views window, including its position on a bitmap image or geographical map background. The settings here are related to those described in Section 4.4.6 “Using Background Images” on page 4-31.
- **Stored Data** – Detailed configurable data for object; for example, IP address, description, and so forth. The specific data you can configure varies according to the object.

## 5. When you are done, click Apply or OK to save your changes.

# 4.5.4 Creating New Managed Objects

The easiest way to create new managed objects is to run a Network Discovery, as described in Chapter 3.” You can, however, create managed objects one at a time by using the Object Properties tool.

The procedure for creating a managed object is almost exactly the same as that for modifying an existing object; the primary difference being the ways in which you can start Object Properties. As with modifying existing objects, the specific settings available for your new object depend on the type of object you want to create.

The procedure below provides a high-level overview of the general steps required to create managed objects. Subsequent procedures provide more detailed step-by-step instructions for configuring specific object properties. Please note that the instructions here describe how to create an object from within the Network Views interface.

## ▼ To Create a Managed Object

1. **In the Network Views main window, use any of the following methods to open the Object Properties dialog with the object you want to modify:**

- Click View->Create View->*category*->*type*.

*category*->*type* is the cascading menu pick for the category and type of object you want to create. Category and type will be restricted to containers.

- Click Actions->Create->*category*->*type*.

Again, *category*->*type* is the cascading menu pick for the category and type of object you want to create. You can create any object categories and types including container views.

- Click Tools->Object Palette, to display the Object Palette, and then double-click an object type.

The specific objects available on the Object Palette depends on your Solstice EM configuration. See Section 4.4.11 “Adding an Object Type to the Object Palette” on page 4-37 for more information.

2. **Enter a name for the object in the Object Identification field.**

3. **Specify an Object Type.**

You can only change the Object Type within the specific category you specified when you invoked Object Properties to create the new object. For example, if you clicked Actions->Create->Device->Printer in the Network Views window, the only Object Types available in this instance of Object Properties would be Devices.

4. **Modify the Detailed Information fields, if desired.**

- Agents
- Display
- Coordinates
- Stored Data

5. **When you are done, click Apply or OK to save your changes.**

## 4.5.5 Configuring Agent Communications

You can use the options on the Agents tab in the Object Properties dialog to configure parameters for SNMP, CMIP, RPC, and MIS agents. You can use the default agent for a given object with a single click of a button, or you can manually configure agents as needed.

The specific agent options available depend on the type of agent you want to configure. The procedures below describe how to automatically configure default agents in general, and how to manually configure each of the four types of agents supported by Solstice EM.

### 4.5.5.1 Configuring Default Agents

You can configure an object to communicate with a default SNMP, RPC, MIS agent. The default managed object name is the same name as the device you are configuring. The Managed Object Remote Distinguished Name (MO RDN) indicates the relative position in the Management Information Tree (MIT) at which the management information for a given device is located. The default MO RDN is always the base of the agent.

---

**Note** – CMIP agents cannot be configured with the default agent function, and must be configured manually.

---

#### ▼ To Configure a Default Agent

1. In the Object Properties dialog, select the Agents tab.
2. Select the type of agent you want to configure from the Protocol drop-down list.
3. Click Configure Default.
4. Select the new agent from the Configured Agents list, and then click Change to display the configuration dialog box for that agent type.
5. Modify configuration information as desired, and then click OK to return to the Object Properties dialog.

See the procedures below for instructions on modifying various agent options.

### 4.5.5.2 Manually Configuring SNMP Agents

You can manually configure SNMP agents from the Object Properties dialog, or from the UNIX command line with the `em_oct -snmp` command.

#### ▼ To Manually Configure SNMP Agents from the Object Properties Dialog

1. In the Object Properties dialog, select the Agents tab.
2. Select SNMP from the Protocol drop-down list.
3. Click Configure Manually to open the SNMP Configuration dialog.
4. Enter values for each of the fields in the SNMP Configuration dialog:
  - **Agent Host** – Name of the network component on which the agent is hosted.
  - **Object Path** – Distinguished Name (DN) of the agent host; use the Browser button open the Object Browser window, from which you can select a path.
  - **Protocol Version** – Select SNMP V1 or SNMP V2C.
  - **IP Address** – IP address of the agent host.
  - **Port** – Port number used by the agent host; default is 161.
  - **Read Community** – SNMP read community string; default is `Public`.
  - **Write Community** – SNMP write community string; default is `Private`.
5. Specify the SNMP MIBs you want to use:
  - a. Click Add to display the Add SNMP MIBs dialog.
  - b. Use the Add and Remove buttons to specify the MIBs you want to use in the SNMP MIBs to Add list.
  - c. When you have finished selecting MIBs, click OK to save your selections and return to the SNMP Configuration dialog.
6. Click Apply or OK to save your configuration and return to the Object Properties dialog.

#### ▼ To Configure SNMP Agents From the Command Line

1. Execute the following command at an UNIX prompt to display the SNMP Configuration dialog:

```
em_oct -snmp
```
2. Complete the fields as described in the procedure above.

### 4.5.5.3 Manually Configuring RPC Agents

You can manually configure RPC agents from the Object Properties dialog, or from the UNIX command line with the `em_oct -rpc` command.

#### ▼ To Manually Configure RPC Agents From the Object Properties Dialog

1. In the Object Properties dialog, select the Agents tab.
2. Select RPC from the Protocol drop-down list.
3. Click Configure Manually to open the RPC Configuration dialog.
4. Enter values for each of the fields in the RPC Configuration dialog:
  - **Agent Host** – Name of the network component on which the agent is hosted.
  - **Object Path** – Distinguished Name (DN) of the agent host; use the Browser button open the Object Browser window, from which you can select a path.
  - **Read Community** – SNMP read community string; default is `Public`.
  - **Write Community** – SNMP write community string; default is `Private`.
5. Add or remove RPC agents, proxy agents, and SunNet Manager (SNM) schemas, as desired:
  - a. Click Add to display the Add RPC Agents dialog.
  - b. Use the Add and Remove buttons to specify the RPC agents, proxy agents, and SNM schemas you want to use in the RPC Agents to Add list.
  - c. When you have finished selecting agents, click OK to save your selections and return to the RPC Configuration dialog.
6. Click Apply or OK to save your configuration and return to the Object Properties dialog.

#### ▼ To Configure RPC Agents From the Command Line

1. Execute the following command at an UNIX prompt to display the RPC Configuration dialog:

```
em_oct -rpc
```
2. Complete the fields as described in the procedure above.



#### 4.5.5.4 Manually Configuring MIS Agents

You can manually configure MIS agents from the Object Properties dialog, or from the UNIX command line with the `em_oct -mis` command. You can configure two types of relationships between an MIS agent and one or more associated objects:

- **One-to-one** – Created when you click Configure Default; one agent is created for each object in the Name field.
- **One-to-many** – Created by default when you run `em_oct` from the command line, or when you click Configure Manually.

##### ▼ To Manually Configure MIS Agents From the Object Properties Dialog

1. In the Object Properties dialog, select the **Agents** tab.
2. Select **MIS** from the Protocol drop-down list.
3. Click **Configure Manually** to open the MIS Configuration dialog.
4. Enter values for each of the fields in the MIS Configuration dialog:
  - **MIS Host** – Type the name of the MIS host, or click the down arrow and choose a host name from the drop-down list.
  - **Object Path** – Distinguished Name (DN) of the MIS; use the Browser button to open the Object Browser window, from which you can select a path.
  - **Port** – Port number used to communicate with the MIS; default is 5555.
5. Click **Apply** or **OK** to save your configuration and return to the Object Properties dialog.

##### ▼ To Configure MIS Agents From the Command Line

1. Execute the following command at an UNIX prompt to display the MIS Configuration dialog:

```
em_oct -mis
```

2. Complete the fields as described in the procedure above.

### 4.5.5.5 Manually Configuring CMIP Agents

You can manually configure CMIP agents from the Object Properties dialog, or from the UNIX command line with the `em_oct -cmip` command.

---

**Note** – Unlike other agent protocols in Solstice EM, there is no option to configure default CMIP agents; if you want to use CMIP, you must configure the agents manually.

---

#### ▼ To Manually Configure CMIP Agents From the Object Properties Dialog

1. In the Object Properties dialog, select the **Agents** tab.
2. Select CMIP from the Protocol drop-down list.
3. Click **Configure Manually** to open the CMIP Configuration dialog.
4. Specify an Entity Name for the MIS with which you want the CMIP agent to communicate.
5. Select the **Basic** tab, if it is not already selected, and then enter values for the following:
  - **MO DN** – Managed Object Distinguished Name for the topmost MIT node(s), if any, that you want to add to the Agent DN list.
  - **Presentation Address** – Address of the CMIP agent; comprises the following:
    - Presentation Selector
    - Session Selector
    - Transport Selector
    - Network SAP

The values you enter here must match those defined when the CMIP agent was installed.
6. Select the **Advanced** tab, and then enter values for the following:
  - **Name Translation** – Specify whether the CMIP should use LDN, FDN, or None (the default) for translating requests between the agent and MIS.
  - **MPA Address** – Specify the IP address and port number used by the CMIP agent. Selecting Default uses the values specified in the `EM_CMIP_MPA_DEFAULT_HOST` and `EM_CMIP_MPA_DEFAULT_PORT` environment variables. Select custom if you want to specify an address and port other than the default.
7. Click **Apply** or **OK** to save your configuration and return to the Object Properties dialog.

## ▼ To Configure CMIP Agents From the Command Line

1. Execute the following command at an UNIX prompt to display the CMIP Configuration dialog:

```
em_oct -cmip
```

2. Complete the fields as described in the procedure above.

### 4.5.5.6 Using Multiple CMIP MPAs Over RFC1006

You can configure multiple CMIP Management Protocol Adapters (MPAs) over RFC1006. RFC1006 is an Internet Engineering Task Force (IETF) specification for “ISO Transport Service on top of the TCP.” This section provides instructions for configuring CMIP MPAs on local and remote MIS hosts.

---

**Note** – Before starting additional CMIP MPAs, make certain that the CMIP stack on the host machine is configured for RCD1006. See the *Solstice EM MIS Guide* for more instructions. If you just need to restart the CMIP MPA stack, follow the instructions in this chapter, in Section 4.5.5.7 “Restarting the CMIP MPA Stack” on page 4-53.

---

The general procedure for starting multiple CMIP MPAs over RFC1006 is as follows:

1. Set the CMIP environment variables.
2. Verify that the appropriate ancillary MIS processes are running.
3. Run a CMIP MPA configuration script on the MIS host.

These procedures are described in more detail below.

## ▼ To Set CMIP Environment Variables

1. Set variables for the MIS host and port number, as follows:

```
EM_MIS_DEFAULT_HOST=localhost  
EM_MIS_DEFAULT_PORT=5555
```

2. Set the variable for the CMIP MPA TCP port number, as follows:

```
EM_CMIP_MPA_DEFAULT_PORT=5558
```

3. Set variables for the OSI address for the CMIP MPA, as follows:

```
EM_CMIP_MPA_PSEL=rfc2  
EM_CMIP_MPA_SSEL=Prs  
EM_CMIP_MPA_TSEL=CMIP  
EM_CMIP_MPA_NSAP=0x8192b81d
```

## ▼ To Verify if Ancillary MIS Processes are Running

- **Type the following commands to verify that the `rk6d` and `osimcsd` processes are running on the MIS host:**

```
ps -ef | grep rk6d  
ps -ef | grep osimcsd
```

## ▼ To Run a CMIP MPA Configuration Script

### 1. Run a CMIP MPA configuration script as root on the MIS host.

The following is an example of a shell script that will start two additional CMIP MPAs on the local MIS host.

```
#!/bin/sh

# start additional MPA 1

EM_MIS_DEFAULT_HOST=localhost
EM_MIS_DEFAULT_PORT=5555
EM_CMIP_MPA_DEFAULT_PORT=5558

EM_CMIP_MPA_PSEL=rfc2
EM_CMIP_MPA_SSEL=Prs
EM_CMIP_MPA_TSEL=CMIP
EM_CMIP_MPA_NSAP=0x8192b81d

export EM_CMIP_MPA_PSEL EM_CMIP_MPA_SSEL EM_CMIP_MPA_TSEL
EM_CMIP_MPA_NSAP
export EM_MIS_DEFAULT_HOST
export EM_MIS_DEFAULT_PORT
export EM_CMIP_MPA_DEFAULT_PORT

echo "Starting CMIP MPA for port 5558"
/opt/SUNWconn/em/bin/em_cmip &

# start additional MPA 2

EM_MIS_DEFAULT_HOST=localhost
EM_MIS_DEFAULT_PORT=5555
EM_CMIP_MPA_DEFAULT_PORT=5559

EM_CMIP_MPA_PSEL=rfc3
EM_CMIP_MPA_SSEL=Prs
EM_CMIP_MPA_TSEL=CMIP
EM_CMIP_MPA_NSAP=0x8192b81d

export EM_CMIP_MPA_PSEL EM_CMIP_MPA_SSEL EM_CMIP_MPA_TSEL
EM_CMIP_MPA_NSAP
export EM_MIS_DEFAULT_HOST
export EM_MIS_DEFAULT_PORT
export EM_CMIP_MPA_DEFAULT_PORT

echo "Starting CMIP MPA for port 5559"
/opt/SUNWconn/em/bin/em_cmip &
```

## ▼ To Start Additional CMIP MPAs Over RFC1006 Remotely

1. **Run a CMIP MPA configuration script as root on the machine from which you want to start a CMIP MPA on a remote machine.**

The following is an example of a shell script that will start a remote CMIP MPA.

```
#!/bin/sh

EM_MIS_DEFAULT_HOST=greco  ## host name on which MIS is running
EM_MIS_DEFAULT_PORT=5555
EM_CMIP_MPA_DEFAULT_PORT=5560

EM_CMIP_MPA_PSEL=rem1
EM_CMIP_MPA_SSEL=Prs
EM_CMIP_MPA_TSEL=CMIP
EM_CMIP_MPA_NSAP=0x8192b812

export EM_CMIP_MPA_PSEL EM_CMIP_MPA_SSEL EM_CMIP_MPA_TSEL
EM_CMIP_MPA_NSAP
export EM_MIS_DEFAULT_HOST
export EM_MIS_DEFAULT_PORT
export EM_CMIP_MPA_DEFAULT_PORT

#quarkqal 0x8192b812

echo "Starting remote CMIP MPA for port 5560"
/opt/SUNWconn/em/bin/em_cmip
```

2. **Start \$EM\_HOME/bin/em\_cmip in the background from the script.**

You will be prompted for a password if access control is enabled on the MIS and the host from which you ran the script is not on the MIS host's trusted host list.

### 4.5.5.7 Restarting the CMIP MPA Stack

If communication is not working properly between the CMIP agents and your newly added CMIP MPAs, you need to restart the CMIP MPA stack.

#### ▼ To Restart the CMIP MPA Stack

##### 1. Shut down the current CMIP MPA stack:

```
/etc/rc2.d/S98cmipmpa stop  
/etc/rc2.d/S97osimcs stop  
/etc/rc2.d/S90rk6 stop
```

##### 2. Restart the stack:

```
/etc/rc2.d/S90rk6 start  
/etc/rc2.d/S97osimcs start
```

---

## 4.6 Working With Alarms

This section provides step-by-step instructions for basic viewing and responding to alarm data. Specifically, the following tasks:

- Viewing Object Alarms—page 4-53
- Clearing Object Alarms—page 4-54
- Propagating Alarm Severity—page 4-54

Complete information about configuring and managing alarms is provided in Chapter 5 "Managing Alarms."

You may also want to refer to the following sections for information about other Network Views tasks:

- "Getting Started With Network Views" on page 4-8
- "Working With Views" on page 4-9
- "Configuring Object Icons and the Workspace" on page 4-23
- "Managing Object Properties" on page 4-39
- "Working With Requests" on page 4-56

### 4.6.1 Viewing Object Alarms

You can view alarm data for objects that have been configured to generate alarms in the Alarms tool by double-clicking non-container objects, clicking Alarms on the object's pop-up menu, or by selecting the object and clicking Actions->Alarms. All of these actions open the Alarms tool, from which you can view alarm data.

## ▼ To View Alarm Data for an Object

- **In the Network Views main window, use any of the following three methods to open Alarm Manager and display alarm data for an object:**
  - Double-click the object.
  - Right-click the object, and then click Alarms from the object's pop-up menu.
  - Select the object, and then click Actions->Alarms.

You can also open the Alarms tool without selecting an object by clicking Tools->Alarms. This opens the Alarms tool without any object preselected in the Alarms window.

### 4.6.2 Clearing Object Alarms

You can clear all outstanding alarms against a managed object by clicking Clear All Alarms on the object's pop-up menu, or by selecting an object and clicking Actions->Clear All Alarms.

---

**Note** – Clearing alarms on a container object will not clear the alarms of the objects within that container.

---

## ▼ To Clear Alarms for an Object

- **In the Network Views main window, use either of the following two methods to clear all alarms for an object:**
  - Right-click the object, and then click Clear All Alarms from the object's pop-up menu.
  - Select the object, and then click Actions->Clear All Alarms.

### 4.6.3 Propagating Alarm Severity

You can configure a managed object so that its alarm severity data is passed to any parent object in which it is contained. This makes it possible to view in a parent container object the alarm severity states for one or more child objects. For example, you could have managed objects for several printers contained in a network object; by propagating alarm severity from the printer objects, you could monitor alarm status for all of the printers by watching just the parent network object.



You can propagate alarm severity for individual objects, or for an entire view; the methods for propagating alarms for individual managed objects and for views differ slightly from each other. In all cases, though, you must verify that the display of propagated alarm severities is enabled in the Network Views window.

## ▼ To Verify if Propagated Alarm Severities are Enabled in Network Views

1. In the Network Views main window, click **File->Customize->Display Settings** to open the Display Settings dialog.
2. In the Display Settings dialog, select the **Display** tab, if it is not already selected.
3. Select **On** for the **Alarm Severity Relationships** option.
4. Select the **Colors** tab.
5. Select **Propagated Alarm Severity for the Icon Color Source**, if it is not already selected.
6. Click **OK** to exit the Display Settings dialog.

See Section 4.4.1 “Configuring General Display Properties” on page 4-23 and Section 4.4.2 “Configuring Icon and Label Display” on page 4-24 for more information about the various Network Views display options associated with propagated alarm severities.

## ▼ To Propagate Alarm Severity From an Individual Child Object to a Parent Object

1. In the Network Views main window, select the child object.
2. Click **Actions->Properties** to open the Object Properties dialog.
3. In the Object Properties dialog, select the **Display** tab, if it is not already selected.
4. Select **On** for the **Propagate Severity** option, and then click **OK** to save the setting and exit the Object Properties dialog.

## ▼ To Propagate Alarm Severity for Peer Objects

1. In the Network Views main window, switch to the view for which you want to propagate alarm severity.
2. Click Actions->Propagate Severity.

## ▼ To Remove Severity Propagation for Peer Objects

1. In the Network Views main window, select the object or view for which you want to remove severity propagation.
2. Click Actions->Remove Severity Propagation.

---

## 4.7 Working With Requests

This section provides step-by-step instructions for creating, modifying, and starting object requests, and for performing get and set requests. Specifically, this section describes the following tasks:

- Viewing Advanced Request Information—page 4-57
- Viewing Basic Request Information—page 4-57
- Creating, Modifying, and Initiating Advanced Requests—page 4-58
- Creating, Modifying, and Initiating Basic Requests—page 4-59

You may also want to refer to the following sections for information about other Network Views tasks:

- “Getting Started With Network Views” on page 4-8
- “Working With Views” on page 4-9
- “Configuring Object Icons and the Workspace” on page 4-23
- “Managing Object Properties” on page 4-39
- “Working With Alarms” on page 4-53

You can work with two general types of requests in Network Views, both of which are accessible from the Network Views Tools menu:

- **Advanced Requests** – Opens the Requests dialog, from which you can view the status of Nerve Center requests on the current MIS. From this dialog, you can also open the Design Advanced Requests tool (`em_reqedit`), which provides functions for creating and modifying advanced Nerve Center requests, request templates, and autoManagement objects.
- **Basic Requests** – Spawns the Basic Requests tool (`em_simplerequests`), which provides functions for starting, stopping, and managing fault and performance monitoring for RPC and SNMP objects.

See the *Customizing Guide* for more detailed information about working with advanced Nerve Center requests, advanced request templates, and basic requests. See Chapter 7 "Automating Nerve Center Requests" for information about automating advanced Nerve Center requests.

## 4.7.1 Viewing Advanced Request Information

You can view detailed information about all active Nerve Center requests in the current MIS by clicking Tools->Advanced Requests from the Network Views main window.

### ▼ To View Advanced Request Information

1. **In the Network Views main window, click Tools->Advanced Requests to display the Requests dialog.**  
All available and active requests are displayed in the two lists at the top and bottom of the dialog.
2. **In the Active Requests list, select the request for which you want to view detailed information, and then click Examine to open the Request Examine dialog.**

## 4.7.2 Viewing Basic Request Information

You can view fault and performance information about RPC and SNMP (via RPC proxy) managed objects by clicking Tools->Basic Requests from the Network Views main window.

## ▼ To View Basic Agent Request Information

1. In the Network Views main window, select an object for which you want to display basic request information, and then click Tools->Basic Requests to open the Basic Requests tool.
2. In the Basic Requests dialog, click View->Requests or View->Request Groups to view available or active requests, or request groups, as desired.  
A list of active requests, available requests, or request groups is displayed, according to your choice.
3. Select the request or request group for which you want more information, and then click Actions->Properties to display detailed information.

### 4.7.3 Creating, Modifying, and Initiating Advanced Requests

You can use the Network Views Requests dialog to start and stop requests based on existing request templates. You can also use the Requests dialog to open the Request Designer tool, from which you can perform a full range of request management tasks. Complete information about using the Request Designer is provided in the *Customizing Guide*.

## ▼ To Initiate an Advanced Request

1. In the Network Views main window, click Tools->Advanced Requests to display the Requests dialog.
2. Select the request you want to start from the Available Requests list.
3. Select the target object(s) in the current view, and then click Start.  
Alternatively, you can use the middle mouse button to drag a request from the Available Requests list and drop it on an object in the Network Views window.
4. Repeat Steps 2 and 3 for each request you want to initiate, or click Close to exit the Requests dialog.

## ▼ To Halt an Advanced Request

1. In the Network Views main window, click Tools->Advanced Requests to display the Requests dialog.
2. Select the request you want to halt from the Active Requests list.
3. Click Delete.

The request template itself is not deleted from the MIS; only the particular request object instance based on the request template is deleted.
4. Repeat Steps 2 and 3 for each request you want to halt, or click Close to exit the Requests dialog.

## ▼ To Create or Modify an Advanced Request

1. In the Network Views main window, click Tools->Advanced Requests to display the Requests dialog.
2. In the Requests dialog, do either of the following:
  - If you want to **modify** a request, select the request from the Available Requests lists, and then click Modify.
  - If you want to create a request, click Create.

In both cases, the Request Designer (`em_reqedit`) is opened.
3. In the Request Designer, modify or create requests or request templates as desired.

Follow the instructions in the Solstice EM *Customizing Guide* for complete information about using the Solstice EM Request Designer.

## 4.7.4 Creating, Modifying, and Initiating Basic Requests

You can use the Basic Requests tool start, stop, create, and modify basic requests and request groups. Complete instructions for using the Basic Requests tool are provided in the *Customizing Guide*.

## ▼ To Initiate a Basic Request

1. In the Network Views main window, select an object for which you want to initiate a basic request, and then click Tools->Basic Requests to open the Basic Requests tool.
2. Click View->Requests->Active Requests, or View->Request Groups to view active requests or request groups, as desired.
3. Select the request you want to initiate, and then click Actions->Start.

## ▼ To Halt a Basic Request

1. In the Network Views main window, select an object for which you want to halt a basic request, and then click Tools->Basic Requests to open the Basic Requests tool.
2. Click View->Requests->Active Requests, or View->Request Groups to view active requests or request groups, as desired.
3. Select the request you want to halt, and then click Actions->Stop.

## ▼ To Create a Basic Request or Request Group

1. In the Network Views main window, select an object for which you want to create a basic request, and then click Tools->Basic Requests to open the Basic Requests tool.
2. Click Actions->Create->Request or Actions->Create->Request Group, as desired, to open the Create Request or Create Group dialog.
3. Specify Request or Request Group options as needed.

See the *Customizing Guide* for complete information about the Create Request and Create Request Group options.

## ▼ To Modify a Basic Request or Request Group

1. In the Network Views main window, select an object for which you want to modify a basic request, and then click Tools->Basic Requests to open the Basic Requests tool.

2. **Click View->Requests or View->Request Groups to view available or active requests, or request groups, as desired.**

A list of active requests, available requests, or request groups is displayed, according to your choice.

3. **Select the request or request group you want to modify, and then click Actions->Properties to display detailed information.**

If you selected a request group, the Group Properties dialog is displayed. If you selected an individual request, the Request Properties dialog is displayed.

4. **Specify Request or Request Group options as needed.**

See the *Customizing Guide* for complete information about the Request Properties and Group Properties dialogs.

---

## 4.8 Reference

The remainder of this chapter provides detailed information about command-line options for the various executable files discussed in one or more procedures earlier in the chapter, as well as menu and dialog box options, and other general reference information. Specifically, this reference section includes the following topics:

- “Command-Line Options” on page 4-61
- “Network Views Command and Variable Macros” on page 4-65
- “More About Object Properties” on page 4-67
- “More About Geographical Map Backgrounds” on page 4-72

For detailed information about dialogs, menus, and other user interface elements, refer to the Solstice EM Online Help. To access Online Help, Click the Help button on any dialog box or select options from the Help menu located in the upper right corner of each Solstice EM tool window.

### 4.8.1 Command-Line Options

This section describes the command-line options for the following tools:

- “Network Views Options” on page 4-62
- “Object Properties Options” on page 4-62
- “Network Views Layout Options” on page 4-63
- “Basic Requests Options” on page 4-64
- “Request Designer Options” on page 4-65

### 4.8.1.1 Network Views Options

The Network Views command (`em_viewer`) displays the primary Network Views interface. The general form for the Network Views command is:

```
em_viewer -options
```

The various Network Views command-line *options* are described in the following table. Step-by-step instructions for using the Network Views tool begin in Section 4.2 “Getting Started With Network Views” on page 4-8.

**TABLE 4-4** Network Views Command-line Options

Option	Description
-help	Print descriptions of <code>em_viewer</code> options.
-host <i>hostname</i>	Specify the remote machine on which the MIS you want to use is located. By default, Network Views uses the local MIS on the machine from which it is invoked. You can specify a DNS name or an IP address.
-init_requests	Initialize requests subsystem.
-no_labels	Suppress the display of object icon labels.
-no_move	Prevent movement of object icons.
-view <i>view</i>	Specify the name of view you want to display when Network Views starts.

### 4.8.1.2 Object Properties Options

The Object Properties command (`em_oct`) displays the Object Properties dialog, from which you can create and modify managed objects, and view managed object properties. The Object Properties dialog can also be displayed from the Network Views main window, as described earlier in this chapter. The general form for the Object Properties command is:

```
em_oct -options
```



The various Object Properties command-line *options* are described in the following table. Step-by-step instructions for using the Object Properties function begin in Section 4.5 “Managing Object Properties” on page 4-39.

**TABLE 4-5** Object Properties Command-line Options

Option	Description
-bus_locations <i>x:y:z...</i>	Specify coordinates for a bus object you want to create or modify.
-cmip	Configure a CMIP agent; displays the CMIP Configuration dialog.
-help	Print descriptions of <i>em_oct</i> options.
-host <i>hostname</i>	Specify the remote machine on which the MIS you want to use is located. By default, <i>em_oct</i> uses the local MIS on the machine from which it is invoked. You can specify a DNS name or an IP address.
-id <i>id...</i>	Specify topology IDs; separate multiple IDs with a space.
-link <i>id1 id2</i>	Create a link between <i>id1</i> and <i>id2</i> .
-mis	Configure an MIS agent; displays the MIS Configuration dialog.
-name <i>name...</i>	Specify the name of an object; separate multiple names with a space.
-parent <i>parent_id</i>	Specify the parent of the object being created or modified
-rpc	Configure an RPC agent; displays the RPC Configuration dialog.
-snmp	Configure an SNMP agent; displays the SNMP Configuration dialog.
-type <i>type</i>	Specify the type of object you want to create.
-visible_children <i>id...</i>	Specify the children of a container object being created or modified; separate multiple IDs with a space.

### 4.8.1.3 Network Views Layout Options

The Network Views command (*em\_layout*) displays the Network Views Layout dialog, from which you can modify Tree, Tile, Mesh, and Cluster layout options. The Layout dialog can also be displayed by clicking View->Layout in the Network Views main window. The general form for the Network Views Layout command is:

*em\_layout -options*

The various Layout command-line *options* are described in the following table. Step-by-step instructions for using the Layout options begin in Section 4.4.5 “Customizing View Layout” on page 4-29.

**TABLE 4-6** Network Views Layout Command-line Options

Option	Description
<code>-app_id viewer_instance</code>	Specify the application ID of the instance of Network Views to which you want to connect. You can determine a list of Network Views instances by using the Message Log in the instance.
<code>-help</code>	Print descriptions of <code>em_layout</code> options.
<code>-host hostname</code>	Specify the remote machine on which the MIS you want to used is located. By default, <code>em_oct</code> uses the local MIS on the machine from which it is invoked. You can specify a DNS name or an IP address.

#### 4.8.1.4 Basic Requests Options

The Basic Requests command (`em_simplerequests`) displays Basic Requests dialog, from which you can start, stop, and manage fault and performance monitoring of RPC and SNMP (via RPC proxy) managed objects. The Basic Requests dialog can also be displayed by clicking Tools->Basic Requests in the Network Views main window. The general form for the Basic Requests command is:

`em_simplerequests -options`

The various Basic Requests command-line *options* are described in the following table. Step-by-step instructions for using the Basic Requests options begin in Section 4.7.2 “Viewing Basic Request Information” on page 4-57. Detailed information about Basic Requests is provided in the *Customizing Guide*.

**TABLE 4-7** Basic Requests Command-line Options

Option	Description
<code>-help</code>	Print descriptions of <code>em_simplerequests</code> options.
<code>-host hostname</code>	Specify the remote machine on which the MIS you want to use is located. By default, Network Views uses the local MIS on the machine from which it is invoked. You can specify a DNS name or an IP address.
<code>-viewer id</code>	Specify the viewer process to which you want to return request information.

**TABLE 4-7** Basic Requests Command-line Options (*Continued*)

Option	Description
-id <i>id...</i>	Specify topology IDs; separate multiple IDs with a space.
-ar	Show available requests on startup.
-rr	Show running requests on startup.
-rg	Show request groups on startup.

### 4.8.1.5 Request Designer Options

The Request Designer command (`em_reqedit`) opens the Request Designer tool, from which you can manage advanced requests. The Request Designer is an integral part of the Network Views Request Services function, which is initiated by clicking Tools->Advanced Requests in the Network Views main window. The Request Designer can be displayed from the Network Views Requests dialog by clicking Create or Modify. The general form for the Advanced Requests command line is:

```
em_reqedit -options
```

The various Request Designer command-line *options* are described in the following table. Basic step-by-step instructions for using the Request Designer options begin in Section 4.7.3 “Creating, Modifying, and Initiating Advanced Requests” on page 4-58. Detailed information about using the Request Designer is provided in the Solstice EM *Customizing Guide*.

**TABLE 4-8** Advanced Requests Command-line Options

Option	Description
-help	Print descriptions of <code>em_reqedit</code> options.
-host <i>hostname</i>	Specify the remote machine on which the MIS you want to use is located. By default, Network Views uses the local MIS on the machine from which it is invoked. You can specify a DNS name or an IP address.
-template <i>template</i>	Specify the name of a request template to load.

## 4.8.2 Network Views Command and Variable Macros

You can customize the Network Views Tools menu, pop-up menu, and double-click actions to perform a wide range of functions. The procedures for configuring these items are described earlier in this chapter, beginning with Section 4.4.7 “Configuring Double-click Actions” on page 4-33.

The configuration procedure for each of these items includes specifying a command line to execute when a given action is performed. For example, you can define a command to execute when an object is double-clicked. The table below lists the Network Views command and variable macros you can use when configuring command lines for Tools menu, pop-up menu, and double-click actions.

**TABLE 4-9** Network Views Command and Variable Macros

Macro	Description
<b>Command Macros</b>	
EM_GOTOVIEW	For double-click actions and pop-up menus, changes the current view to the associated object. An error will result if assigned to an object that is not a view (for example a Container or Monitor).
EM_VIEWERCONFIG	Launches <code>em_oct</code> (Object Properties tool).
<b>Variable Macros</b>	
EM_OBJNAME	For double-click actions and pop-up menus, substitutes the name of the associated object. For the Tools menu, substitutes the name of the selected object. If more than one object is selected, the object used is arbitrary.
EM_OBJNAMES	For double-click actions and pop-up menus, substitutes the name of the associated object. For the Tools menu, substitutes the names of all selected objects.
EM_OPTIONAL_UNIQUE_IDS	Same as <code>EM_UNIQUE_ID</code> , except the substitution of object identifiers occurs only if object identifiers are specified, otherwise the variable is ignored.
EM_UNIQUE_ID	Same as <code>EM_OBJNAME</code> , except the unique object identifier <i>system-name: id</i> is substituted instead of the object name. Use this to integrate with other EM applications that accept the <code>-id</code> command line option.
EM_UNIQUE_IDS	Same as <code>EM_OBJNAMES</code> , except the unique object identifier <i>system-name: id</i> is substituted instead of the object name. Use this to integrate with other EM applications that accept the <code>-id</code> command line option.
EM_VIEW	Substitutes the name of the current view.
EM_VIEW_UNIQUE_ID	Same as <code>EM_VIEW</code> , except the unique object identifier <i>system-name: id</i> is substituted instead of the object name. Use this to integrate with other EM applications that accept the <code>-id</code> command line option.
EM_MIS	Substitutes the name of the MIS system to which the current instance of Network Views is connected.

# 4.8.3 More About Object Properties










This section provides detailed tabular listings for:

- Network Views Object Types—page 4-67
- Configurable Object Type Data—page 4-70















## 4.8.3.1 Network Views Object Types

The table below provides descriptions of the various types of Network Views objects you can create, along with their default associated icons.









TABLE 4-10 Network Views Object Icons and Types

Object Name	Object Type	Default Icon	Description
Array	Array		Contains a group of objects in a compact array. The object names are displayed in the array cells.
Bridge	Device		Device object representing a network bridge.
BSC	Device		Device object representing a base station controller
BTS	Device		Device object representing a base transceiver station
Bus	Bus		A free-standing multisegmented line; links objects that are connected to it. Any links attached to the bus will be connected along the shortest path.
Bus Container	Bus		Same as a Bus object, above, but can also contain other Bus objects.
Circle	Multimonitor		Container object with up to 360 object view sections; each section represents a view of one of the objects contained within it.
Container	Container		Basic container object; often used for logical constructs, like views, networks, and subnetworks.
Device	Device		Represents an object that cannot contain another object—used for physical components, like hosts, routers, and hubs. Devices are connected by link and bus objects.

**TABLE 4-10** Network Views Object Icons and Types *(Continued)*

Object Name	Object Type	Default Icon	Description
Hexagon	Multimonitor		Container object with six object view sections; each section represents a view of one of the objects contained within it.
Hexagon120	Multimonitor		Container object with three object view sections; each section represents a view of one of the objects contained within it.
HLR	Device		Device object representing a home location register.
Host	Device		Device object representing a host machine.
Hub	Device		Device object representing a network hub.
Interface	Device		Device object representing an interface that connects two or more hosts or other network devices.
Java	Sun (Device)		Platform-specific object representing a Sun Javastation.
Link	Link		Link object connecting two other objects; a link container can also contain other objects.
MSC	Container		Container object representing a mobile switching center.
Network	Container		Container object representing a network.
OMC	Device		Device object representing an operations and maintenance center.
Omnisector	Multimonitor		Container object with a single object view section representing a view of the object it contains.
PC	Device		Device object representing a PC.
Printer	Device		Device object representing a printer.

**TABLE 4-10** Network Views Object Icons and Types *(Continued)*

Object Name	Object Type	Default Icon	Description
Router	Device		Device object representing a network router.
RouterArray	Device		Device object representing a network router array.
RouterContainer	Device		*placeholder for description and icon
Server	Device		Device object representing a server machine.
SPARC	Sun (Device)		Platform-specific object representing a Sun SPARCstation.
Subnetwork	Container		Container object representing a subnetwork.
Universe	Container		Enterprise-wide container object representing multiple local and wide area networks.
VLR	Device		Device object representing a visitor location register.
XCDR	Device		Device object representing a network transcoder.
Vendor-specific	Varies (Device)	Varies	Custom or platform specific objects; for example Sun devices. See the <i>Customizing Guide</i> for information about adding object definitions and icons to the Network Views Object Palette.

### 4.8.3.2 Configurable Object Type Data

The table below lists the data you can configure in the Object Properties dialog for each of the Network Views object types.

TABLE 4-11 OCT Object Types and Configurable Data

Object Type	Array	Configurable Data
Bus	Bus Container	defaultData, snm-busdotethernetData
Container	Network	networkData, snm-viewdotbuildingData, snm-viewdotnetworkData, snm-viewdotstarData, snm-viewdotringData, snm-viewdotbusData
	Subnetwork	subnetData, snm-viewdotsubnetData, snm-viewdotcampusData
	Universe	defaultData



**TABLE 4-11** OCT Object Types and Configurable Data (*Continued*)

Object Type	Array	Configurable Data
Device	Bridge	defaultData, snm-componentdotbridgeData
	Host	hostData, snm-componentdotss1Data, snm-componentdotss2Data, snm-componentdotss5Data, snm-componentdotipcData, snm-componentdotipxData, snm-componentdotlxDData, snm-componentdotss10Data, snm-componentdotss20Data, snm-componentdotsun3Data, snm-componentdotsun4Data, snm-componentdotsun470Data, snm-componentdotgenwsData, snm-componentdotworkstationData, snm-componentdotgenhostData, snm-componentdotlaptopData, snm-componentdotxhynterminalData, snm-componentdotlanboxData
	Hub	defaultData, snm-componentdothubData
	Interface	defaultData
	Pc	hostData, snm-componentdotsun386Data, snm-componentdotpcData
	Printer	hostData, snm-componentdotlaserwriterData, snm-componentdotprinterData, snm-componentdotnewsprinterData
	Router	routerData, snm-componentdotrouterData
	Server	defaultData, snm-componentdotsunhynserverData, snm-componentdotsc1000Data, snm-componentdotsc2000Data, snm-componentdotss330Data, snm-componentdotss370Data, snm-componentdotserverData, snm-componentdottermsrvrData
	Sunws	hostData. snm-componentdotsunhynworkstationData, snm-componentdotsunhyndesksideData
Link	Link Container	linkData, snm-connectiondotlinkData, snm-connectiondotrs232Data
Monitor	Circle	defaultData

**TABLE 4-11** OCT Object Types and Configurable Data (*Continued*)

Object Type	Array	Configurable Data
	Hexagon	defaultData
	Hexagon120	defaultData
	OmniSector	defaultData

## 4.8.4 More About Geographical Map Backgrounds

Network Views lets you use geographical maps as background images for container objects. The procedures for doing this are provided earlier in this chapter, in Section 4.4.6 “Using Background Images” on page 4-31. This section describes geographical map backgrounds in more detail, and describes what you need to do to add new map backgrounds to the Network Views environment.

### 4.8.4.1 Components of Geographical Map Backgrounds

Geographical map backgrounds in Network Views comprise two components:

- **Cartographically accurate Map Data (MD) files** – These are the actual map data files that represent your buildings, city, state, country, the world, or whatever your mapping needs may require. Network Views includes a sample set of maps, located in `$EM_HOME/mapdata`. You can order additional geographical maps from the ESRI Corporation at (909)793-2853.
- **Geographical Map Configuration (GMC) files** – These are ASCII configuration files that list the component geographical map files and any other format files to be used to construct the map background. By default, geographical map configuration files have the extension `.gmc`.

By default, MD files and GMC files are stored in `$EM_HOME/mapdata`. If desired, you can store the MD files in a separate directory from the GMC files, because GMC files contain an absolute path description of the location of their associated MD files.

### 4.8.4.2 Adding New Geographical Maps

To add a geographical map background to the Network Views environment, you must first obtain a suitable MD file, and then create an associated GMC file. See Section 4.8.4.3 “Geographical Map Configuration Files” on page 4-73 for an explanation of the GMC file structure.

### 4.8.4.3 Geographical Map Configuration Files

GMC files consist of three sections:

- Absolute path to the associated MD files
- Relative path to any style sheet or symbol files
- Relative path list of any component MD files

Each of these sections is described in more detail below, followed by an example of the three sections put together in a sample GMC file.

#### *Section 1 – Absolute Path to MD Files*

Specify the absolute path to the MD files. Use the following format:

<code>TvFileDir</code>	<i>absolute_pathname</i>
------------------------	--------------------------

`TvFileDir` indicates the absolute path to the directory containing the MD files.

#### *Section 2 – Relative Path to Style Sheets and Symbol Files*

Specify the relative path—that is, relative to the `TvFileDir`, above—to any style sheet or symbol files to be used when generating the geographical map background. Use the following format:

<code>TvStyleSheet</code>	<i>relative_pathname</i>
<code>TvSymbols</code>	<i>relative_pathname</i>

### Section 3 – Relative Path List of Component MD Files

Specify the relative path to the component MD files to be used when generating the geographical map background. Each component MD file represents a map layer in the Network Views window. Use the following format:

Y   N	<i>relative_pathname</i>	<i>"label"</i>
-------	--------------------------	----------------

- Y | N – Specify whether the given map layer should be displayed by default. You can also change the display of layers in the Network Views window later by using the File->Customize->Object Type Layers command.
- *relative\_pathname* – Specify the name of the MD file to use for the given map layer.
- *"label"* – Specify the name of the map layer as it should appear in the Network Views Layers dialog.

### Sample GMC File

A sample GMC file containing the three sections described above is as follows:

TvFileDir	/opt/SUNWconn/em/mapdata/so-ca	
TvStyleSheet	TvStyleSheet	
TvSymbols	TvSymbols	
Y	Apodj.tv	"DCW: Areas - Political & Ocean"
Y	Appdj.tv	"DCW: Areas - Populated Places"
Y	Ldndj.tv	"DCW: Areas - Rivers & Lakes"
Y	Lpodj.tv	"DCW: Lines - Ocean Features"
Y	Lrddj.tv	"DCW: Lines - Roads"
Y	Lrrdj.tv	"DCW: Lines - Railroads"
Y	Ltsdj.tv	"DCW: Lines - Bridges & Tunnels"
Y	Lutdj.tv	"DCW: Lines - Pipelines & Power Lines"
Y	Pdndj.tv	"DCW: Lines - Rivers & Lakes"
Y	Pdsdj.tv	"DCW: Lines - Misc. Rivers & Lakes"
Y	Pofdj.tv	"DCW: Point - Ocean Features"
Y	Ppodj.tv	"DCW: Point - Political & Ocean"
Y	Pppdj.tv	"DCW: Point - Populated Places"
Y	Tdndj.tv	"DCW: Text - Rivers & Lakes"
Y	Tpodj.tv	"DCW: Text - Political & Ocean"
Y	Tppdj.tv	"DCW: Text - Populated Places"
Y	Trddj.tv	"DCW: Text - Roads"
Y	Tutdj.tv	"DCW: Text - Pipelines & Power Lines"

# Managing Alarms

---

The Alarms window in Solstice Enterprise Manager™ (Solstice EM) provides information about alarms received by the Management Information Server (MIS). An alarm notifies the network administrator that an unsolicited message has been received from an agent running on a network device. The message indicates a problem or condition detected on the device. These messages are known as event notifications (in CMIP terminology) or traps (in SNMP terminology).

This chapter comprises the following topics:

- Section 5.2 “Getting Started With the Alarms Window” on page 5-9
- Section 5.3 “Viewing Alarms” on page 5-10
- Section 5.4 “Grouping Alarms Into Associations” on page 5-16
- Section 5.5 “Filtering Alarms” on page 5-18
- Section 5.6 “Performing Operations on Alarms” on page 5-20
- Section 5.7 “Deleting Alarms From the Log” on page 5-24
- Section 5.8 “Logging Alarms Management Activity” on page 5-28
- Section 5.9 “Graphing Alarm Data” on page 5-29
- Section 5.10 “Customizing the Alarms Window” on page 5-29
- Section 5.11 “Customizing the Tools Menu” on page 5-32

---

## 5.1 Overview

Alarms originate as event notifications or SNMP traps are sent to the MIS from managed network components. Some types of event notifications and SNMP traps are translated into log records and collected by the AlarmLog. By default, the AlarmLog collects alarms for all events that provide a perceived severity attribute, such as the following default event types:

- communicationAlarm
- environmentalAlarm
- equipmentAlarm

- qualityofServiceAlarm
- processingErrorAlarm
- SNMP traps that are mapped to event notifications:
  - coldStartTrap
  - warmStartTrap
  - linkUpTrap
  - linkDownTrap
  - egpNeighborLossTrap
  - authenticationFailureTrap
  - enterpriseSpecificTrap

Event notifications for object creation and deletion, attribute value change, SNM alarm events, and state change are *not* logged to the AlarmLog. These types of events may be collected by another log, depending on how Event Logs is configured. See the *Customizing Guide* for information about Event Logs.

You use the Alarms window to monitor and manage alarms in Solstice EM's AlarmLog, by default. You can also use the Alarms window to manage alarms collected by other logs you may have created with Event Logs. In this chapter, the term alarms refers only to those alarms that are collected by the AlarmLog.

You can find more information about logs in Chapter 11."

## 5.1.1 Functions of the Alarms Window

The Alarms window lets you:

- View summary information about all alarms or the details of an individual alarm.
- Change the state of an alarm as work progresses on resolving problems that trigger an alarm. Alarm states are explained in the next section, Section 5.1.3 "Alarm States" on page 5-3.
- Group alarms of a certain type into an association so that actions can be taken on the group as a whole. Alarm associations are explained in Section 5.1.4 "Alarm Associations" on page 5-4.
- Filter alarms to further refine the type of alarms you want to look at.
- Delete alarms from the AlarmLog.
- Graph alarm information.

---

**Tip** – You can use Alarms to monitor alarm logs other than the AlarmLog, if any. See the *Customizing Guide* for information about creating other alarm logs.

---

## 5.1.2 Alarm Severities

The perceived severity is an attribute of each alarm, indicating the seriousness of the problem. Severity is indicated in the Alarms window by the Severity column and by the color shown in the first column in the Alarms window. The colors match the colors used to indicate severity in the Viewer window. The default color mapping is shown in the following table.

**TABLE 5-1** Color Mapping for Alarm Severity

Severity	Color
Cleared	Gray
Indeterminate	Blue
Warning	Yellow
Minor	Cyan
Major	Orange
Critical	Red

This table lists the severities from lowest to highest severity. Alarms with the highest severity -- critical, are shown in red.

Color mapping for severities cannot be changed in the Alarms tool.

## 5.1.3 Alarm States

The state of an alarm helps network operators keep track of the status of network problems. Alarms may exist in three possible states:

- Open – the alarm has been received by the MIS and added to the AlarmLog, but not yet acted upon by an operator.
- Acknowledged – the alarm has been seen by an operator who has marked it to indicate that the alarm is being investigated.
- Cleared – the problem causing the alarm has been fixed.

In the Alarms tool, an alarm may be marked Acknowledged or Cleared, or both. An Open alarm is neither acknowledged nor cleared.

See Section 5.1.7 “Alarm Clearing” on page 5-7 for more information about clearing alarms.

## 5.1.4 Alarm Associations

Alarm associations are groupings of alarms with equivalent values for one or more selected attributes, such as event type and object instance. Associations make it easier to manage large numbers of alarms generated for the same network problem, or problems in related areas.

The Alarms window allows you to change your view of Alarms from an individual alarm view to an associations view, and vice versa. When you switch your view mode to Associations, an alarm listed in the table of alarms actually represents a group of similar alarms. The alarm selected to represent the group is either of the highest severity, or the most recent. You determine the criteria used to select the representative alarm when you specify the association rules.

Any action you take on an alarm while viewing associations applies to all the alarms in the group associated with that alarm. For example, if you acknowledge an alarm while viewing alarm associations, all alarms in the same association are changed to an acknowledged state. You cannot take action on any individual alarm within an association.

### 5.1.4.1 Attributes Used to Associate Alarms

Alarms have a number of attributes whose values are determined when the alarm is generated. You can use combinations of the following attributes to group alarms into associations:

- Object instance – the name of the device generating the alarm
- Event type – the class of the event, such as `communicationAlarm`, or `nerveCenterAlarm`
- Probable cause – the likely cause of the alarm, such as `adapterError`
- Specific problem – information more specific to the problem
- Additional Text – additional textual information provided in the notification
- Additional Information Identifier – indicator of the type of information included in the Additional Information attribute
- Additional Information – other additional information provided in the notification

Individual alarms are in the same association if they have the same values for the selected attributes. For example, if you select object instance as the attribute of association, all alarms for the same device are grouped into an association.

By default, when you enable associations, the Alarms tool uses all the available parameters to group alarms. Alarms may have null values for the attributes for Specific Problem, Additional Text, Additional Information Identifier, and Additional



Information. Generally, Object Instance, Event Type, and Probable Cause are the attributes most likely to create meaningful associations. You can experiment with different association criteria to determine what best suits your needs.

#### 5.1.4.2 Alarm That Represents the Association

When you view associations in the Alarms window, you are actually viewing data for one alarm that is chosen to represent each alarm association. You can specify in the Association Rules whether the representative alarm should be the one of highest severity or the most recent. If you use the highest severity, you realize one important advantage to grouping alarms into associations: to quickly convey the highest severity alarm that is related to a single problem area.

### 5.1.5 Alarm Views

You can choose to view alarms in several ways:

- By summary or all individual instances
- By Associations

An important difference between grouping alarms by associations and by summary is that associations are a means to view and *manage* groups of alarms, while summary view is a means to view groups of alarms or groups of associations that have only their severity or object instance in common.

#### 5.1.5.1 Summary View of Alarms

The Alarms window allows you to choose between a summary view of alarms, or viewing all alarms at once. The summary view shows a table of alarms grouped either by severity or by object instance, depending on your preference. You can specify how to summarize in the Summary Rules dialog.

If you summarize by severity, the main Alarms window displays one row for each of the severity levels: critical, major, minor, warning, and indeterminate. If there are no alarms of a given severity, no row exists for that severity. Each row indicates how many alarms exist for each severity.

If you summarize by object instance, the main Alarms window displays one row for each device that has generated an alarm. Each row indicates how many alarms exist for each object instance.

# 5.1.5.2 Association View of Alarms

Associations share a common severity or object instance.

The main Alarms window, by default, has both Summary and Associations turned on; the main window shows a summary of associations.

The following table may help you understand the relationship between associations and summary view in the Alarms main window.

TABLE 5-2 Effects of Summary and Association Settings on Alarms Window

If Associations are ...	And Summary is ...	Summarized by...	Alarms Window Displays
On	On	Severity	A summary of the alarm associations, showing the number of associations that contain alarms of each severity level.
		Object Instance	A summary of the alarm associations, showing the number of associations that contain alarms generated by the same object instance (device).
Off	On	Severity	A summary of the individual alarms, showing the number of alarms of each severity level.
		Object Instance	A summary of the individual alarms, showing the number of alarms generated by each different object instance (device).
On	Off	N/A	A listing of the alarm associations, organized only according to the sort order specified in the Alarm Summary Rules. The non-summary listing of associations includes much more information about the representative alarm than is available in summary view.
Off	Off	N/A	A listing of all alarms in the MIS, organized only according to the sort order specified in the Alarm Summary Rules. The the non-summary listing may include more information about the alarms than is available in summary view.

Associations and summary view can be toggled easily in the Alarms window, as explained in Section 5.3 “Viewing Alarms” on page 5-10.

## 5.1.6 Alarm Filters

To further refine your view of alarms, you can filter alarms to select only those that match criteria you specify. You might, for example, use filtering to find all acknowledged alarms or all alarms that were generated on a certain date.

You can define up to eleven filters, using the following attributes:

- Managed object instance – device triggering the alarm
- Managed object class – type of device or resource generating alarms
- Alarm state – whether the alarm is in an open, acknowledged, or cleared state
- Alarm severity – alarm’s perceived severity (critical, major, minor, warning, indeterminate, normal)
- Event type – type of event, such as communications, Internet, Nerve Center
- Date and time – occurring on the current day at a specific time, or after a certain date and time
- Acknowledgment operator – user name of the operator who acknowledged an alarm
- Acknowledgment date – date when an alarm was acknowledged
- Clear operator – user name of the operator who cleared an alarm
- Clear date – date when an alarm was cleared
- Problem code – numeric or textual ID of the probable cause of an alarm

Filters are cumulative, therefore all specified filters are used in selecting alarms.

## 5.1.7 Alarm Clearing

Similar alarms are defined as those alarms that are identical in all respects except for the log ID and the date/time stamp. For example, if you received 150 identical alarms from the same network device about the same problem, these alarms would be considered similar. If you cleared one of the alarms, all 150 would be cleared. However, if some of the alarms were related to the same problem on the same device, but the value of the `probableCause` attribute was different, the alarms having the different value for `probableCause` would *not* be cleared automatically.

To look at it another way, suppose you have ten `linkDown` alarms from two different hosts (five identical alarms from each host). If you select all ten alarms with the mouse and clear them at once, you can expect to receive two cleared-severity alarms. Of the ten alarms selected, two were unique and the rest were essentially duplicates of one of the two.

If you select a large number of dissimilar alarms and clear them, you can expect to receive a potentially large number of cleared-severity alarms in response.

---

**Note** – If you clear the alarm representing an association, thus clearing all the alarms in the association, Solstice EM does *not* generate cleared-severity events for the cleared alarms.

---

If you do not want this alarm-clearing functionality, deselect the Clear Event Required option in the Alarms Properties. Only the selected alarms will be cleared, and Solstice EM will not generate cleared-severity events.

### 5.1.7.1 Manually Cleared Alarms

Once a network problem has been resolved, you can clear the alarm(s) associated with the problem. You can clear alarms one at a time, or clear multiple events at once. You can clear multiple events in the following ways:

- Select multiple alarms with the mouse in the Alarms window and choose Actions -> Clear.
- Clear one alarm while Associations are on – this clears all the alarms in the association. See Section 5.6.2 “Clearing Alarms” on page 5-21 for more information about clearing alarms.
- Clear one alarm and let Solstice EM clear all similar alarms – this action causes Solstice EM to generate a new alarm with severity specified as *cleared*. Section 5.1.7.2 “Automatically Cleared Alarms and Cleared Severity Events” on page 5-8 explains more about this feature.

### 5.1.7.2 Automatically Cleared Alarms and Cleared Severity Events

By default, Solstice EM is set up with the Clear Event Required option enabled in the Alarms Properties dialog. This causes Solstice EM to do the following:

- Clear similar events automatically.
- Generate an event (and subsequently an alarm, by default) with severity specified as cleared. The purpose of the alarm is to notify operators that multiple alarms were automatically cleared.

### 5.1.8 Related Tasks

- Chapter 11 “Examining Log Entries”
- Chapter 6 “Controlling User Access”

## 5.1.9 Related Files

Alarms configuration files, see Section 5.13 “Configuration Files” on page 5-35.

## 5.1.10 Further Reading

You may find it helpful to read about the Alarm Service in;

- *Customizing Guide*
- *Management Information Server (MIS) Guide*

---

# 5.2 Getting Started With the Alarms Window

This section describes how to start and exit the Alarms window.

## ▼ To Use the Alarms Window

### 1. Start Alarms in one of the following ways:

- **From the Network Tools window, double-click Alarms.**
- **From the Viewer window, click Tools -> Alarms.**
- **From the Viewer window, select a network component, right-click, and select Alarms.**

This shows alarms specific to the device.

- **From an operating system prompt, execute:**

```
em_alarmmgr
```

See Section 5.12.1 “The em\_alarmmgr Command” on page 5-33 for a list of options to be used with the em\_alarmmgr command.

### 2. Perform any of the tasks discussed in this chapter.

### 3. Click File -> Exit when you have finished your tasks.

**See Also:** “The em\_alarmmgr Command” on page 5-33.

---

## 5.3 Viewing Alarms

The Alarms window provides flexibility in viewing information about alarms. The default view is a summary view of alarms. You can change your initial view of alarms to use your preferred view. Section 5.3.2 “Viewing Alarm Associations and Alarm Instances” on page 5-11 describes how the Associations and Summary settings change the view of alarms.

You can quickly switch your view of alarms between instance and association, and between details and summary, as explained in the following procedures.

---

**Tip** – When you exit Alarms, you can save your Alarms properties so your preferred view is the one you see when first starting the Alarms window.

---

### 5.3.1 Viewing Alarms in Summary View

The main Alarms window view can be toggled to show alarms in summary view.

In summary view, the main window shows a subset of the available information about alarms, and groups alarms by severity or by the device generating the alarm. When summary is off, the main window shows more information about the individual alarms, or alarm associations if associations are on. Section 5.3.2 “Viewing Alarm Associations and Alarm Instances” on page 5-11 explains the effects of toggling Associations and Summary in the main window.

You can determine what attributes are shown in the more detailed non-summary view, as well as their order of appearance, using the Alarm Summary Rules dialog. See Section 5.10 “Customizing the Alarms Window” on page 5-29 for more information.

## ▼ To View Alarms in Summary View

- **Click View -> Summary to toggle the view of the main Alarms window between detailed and summary format.**

If you are viewing details, the view changes to show a summary. If you are viewing a summary, the view changes to show more details.

---

**Note** – If both summary view and associations are off, the main window shows all alarm instances.

---

### 5.3.2 Viewing Alarm Associations and Alarm Instances

The main Alarms window view can be toggled to alternately display alarm associations and alarm instances.

## ▼ To View Alarm Associations or Instances

- **Click View -> Associations to toggle the view in the main Alarms window.**

If you are viewing associations, the view changes to show alarm instances. If you are viewing instances, the view changes to show alarm associations. See Section 5.4 “Grouping Alarms Into Associations” on page 5-16 for information about creating associations.

---

**Note** – If both summary and associations are off, the main window shows all alarm instances.

---

## ▼ To View Alarm Instances in an Association When Summary is On

1. **Open the Alarm Associations window from the main Alarms window in one of the following ways:**
  - Double-click the association summary you are interested in.
  - Select the association summary you are interested in and click Actions -> Alarm Associations.
2. **From the Alarm Associations window, open the Alarm Instances window in one of the following ways:**
  - Double-click the association you are interested in.
  - Select the association you are interested in and click Actions -> Alarm Instances.

## ▼ To View Alarm Instances in an Association When Summary is Off

- **Open the Alarm Instances window from the main Alarms window in one of the following ways:**
  - Double-click the association you are interested in.
  - Select the association you are interested in and click Actions -> Alarm Instances.

## ▼ To View Details of an Alarm

1. **Open the Alarm Instances window, as explained in the two previous procedures.**

If you have turned off summary and associations, you are already viewing alarm instances.
2. **Open the Alarm Details window in one of the following ways:**
  - Double-click the alarm in the table.
  - Select the alarm and click Actions -> Alarm Details.



## ▼ To View Details of the Alarm Representing an Association

- **With associations turned on, open the Alarm Details window in one of the following ways:**
  - Double-click the alarm in the table.
  - Select the alarm and click Actions -> Alarm Details.

### 5.3.3 Viewing Alarms for a Specific Network Component

If you are interested in seeing only the alarms for one specific network component, you can either use filtering, as described in Section 5.5 “Filtering Alarms” on page 5-18, or you can use the Viewer window to do this quickly and easily, as described in the following procedure.

## ▼ To View Alarms for a Specific Network Component

1. **In the Viewer, select the network component whose alarms you want to see.**
2. **Right-click to open the pop-up menu, and select Alarms.**

The Alarms window is displayed, showing the alarms (or associations) for the selected device.

## 5.3.4 Viewing Alarms on a Remote MIS

You can view alarms on a remote MIS instead of the local MIS if you modify the Alarms Properties as described in the following procedure.

### ▼ To View Alarms on a Remote MIS

1. **Set up a trusted host relationship between your host and the remote MIS host.**  
See Chapter 6 "Controlling User Access" for information about trusted host relationships.
2. **On the local MIS, click File -> Customize -> Properties to open the Alarms Properties dialog.**
3. **In the MIS field near the center of the dialog, type the name of the MIS whose alarms you want to view.**
4. **In Available Alarm Logs, select AlarmLog and click Display.**  
Display Alarm Logs lists the *remote-MIS-name: AlarmLog*.
5. **(Optional) In Display Alarm Logs, select *local-MIS-name:AlarmLog* and click Remove.**  
This removes from view the alarms from the local MIS.
6. **Click OK or Apply.**

## 5.3.5 Viewing a Non-default Alarm Log

If the MIS is collecting alarms in a log other than the default AlarmLog, you can use the Alarms Properties dialog to select the log that contains the alarms you want to view. (The Event Logs tool is used to create logs and determine what objects are collected in the log.)

### ▼ To View a Log Other than AlarmLog

1. **Click File -> Customize -> Properties to open the Alarms Properties dialog.**
2. **In the lower half of the dialog, select the log you want to view from the list of Available Alarm Logs.**

3. Click **Display** to move the log name to the **Display Alarm Logs** list.

The Alarms window will display alarms from all logs listed in **Display Alarm Logs**.

4. If you do not want to view a log listed in **Display Alarm Logs**, select the log name and click **Remove** to move the log name to the **Available Alarm Logs** list.
5. Click **OK**.

## 5.3.6 Printing a List of Alarms

You can print the list of alarms currently displayed in the Alarms window as described in the following procedure.

### ▼ To Print a List of Alarms

1. In the Alarms window, click **File -> Print** to open the **Print** window
2. Select the appropriate print options:
  - **Print to file** – Select this and type a file name for printing to a file. The file is created in the directory from which you started Solstice EM or the Alarms tool. You can also browse to another directory.
  - **Printer** – Select this and type or select a printer name.
  - **Copies** – Select the number of copies to print. This option is available only when printing to a printer.
  - **Banner Page Title** – Type an optional title to print on the title page of the printout. This option is available only when printing to a printer.
  - **Text/Table** – select **Text** to print the alarms in ASCII text, or select **Table** to print a PostScript version that looks similar to the table shown in the Alarms window.
3. Click **Print**.

---

## 5.4 Grouping Alarms Into Associations

The Alarms tool allows you to group alarms with similar attributes into associations, which are described in “Alarm Associations” on page 5-4. This section describes how to set association rules to:

- Select the alarm for the association
- Specify attributes to associate alarms
- Save association rules
- Load association rules

By setting rules for alarm associations, you determine which attributes will be used to group alarms into associations. You also specify whether to use the highest priority alarm or the most recent alarm as a representative for the group to display in the Alarms window. The following procedures show you how to do this.

### ▼ To Select the Alarm to Represent the Association

1. Click **View -> Association Rules** to display the **Alarm Association Rules** dialog.
2. For the setting **Get Alarm Data From**, select an option as follows:
  - Select **Highest Severity Alarm** if you want the alarm with highest severity to be displayed as the representative alarm for the association. Making this choice ensures that the highest severity alarm for a single problem area is conveyed quickly to the operator.
  - Select **Most Recent Alarm** if you want the most recent alarm to represent the association.
3. Click **OK**.

### ▼ To Specify Attributes Used to Associate Alarms

1. Click **View -> Association Rules** to display the **Alarm Association Rules** dialog.
2. For the setting **Associate By**, select the attributes that should be used to group alarms into associations.

**3. Click OK or Apply.**

When you exit Alarms, you are prompted to save properties. If you are logged in as root and you save properties, the alarm association rules will be saved in the file `em_alarmmgr_ap.cf` in the / (root) directory. If you are logged in as another user, properties are saved in `.em_alarmmgr_ap.cf` in your home directory. The rules will be used each time you start Alarms, until you change the rules.

## ▼ To Save Association Rules to a File

- 1. Click View -> Association Rules to display the Alarm Association Rules dialog.**
- 2. Make your selections.**
- 3. Click Save to open a Select File dialog and specify the name of the file in which to save the association rules.**

You can provide any name to the file. You can load this file to use these association rules again as explained in the following procedure.

## ▼ To Load Existing Association Rules

- 1. Click View -> Association Rules to display the Alarm Association Rules dialog.**
- 2. Click Load to open a Select File dialog and select the file containing association rules you want to use.**
- 3. Click OK in the Select File dialog to load a rules file.**
- 4. Click OK or Apply in the Alarm Association Rules dialog to put the association rules into effect.**

---

## 5.5 Filtering Alarms

You can select particular attributes of alarms you want to view, thereby creating a subset of alarms relevant to you. You specify the attributes you are interested in by setting alarm filtering rules. See Section 5.1.6 “Alarm Filters” on page 5-7 for information about filters.

### 5.5.1 Setting Alarm Filtering Rules

This section tells you how to specify rules for filtering alarms and how to deselect a rule for a filter.

#### ▼ To Set Alarm Filtering Rules

1. **Click View -> Filtering Rules to display the Alarm Filtering Rules dialog.**
2. **At the first Include list, select a filter attribute to include.**  
Options allow you to specify the value of the attributes for which you want to filter alarms.
3. **Specify values for the filter attribute.**  
For example, the Only Object Instances filter allows you to type the instance names you are interested in and click Add.
4. **If you want to specify additional filters, scroll down to the next Include list and select another filter attribute.**  
As you define filters, additional Include lists are added to the dialog.
5. **Click OK when you have defined all the filters you want to use.**  
The Alarms window is updated to display the filtered alarms.

#### ▼ To Deselect a Filter Rule

1. **Click View -> Filtering Rules to display the Alarm Filtering Rules dialog.**
2. **At the Include list for the filter you no longer want to use, select the blank item at the top of the list.**
3. **Click OK or Apply.**

## 5.5.2 Using Filtering Rules Files

If you want to use combinations of filters at various times to select filters having different attributes, you can save filtering rules to a file and reuse them at another time. You can also print filtering rules. The following tasks describe these options.

### ▼ To Save Alarm Filtering Rules

1. Click **View -> Filtering Rules** to display the **Alarm Filter Rules** dialog.
2. Make your selections.
3. Click **Save** to open a **Select File** dialog and specify the name of the file in which to save the filtering rules.

You can name the file any name you like. You can load this file to use these filtering rules again as explained in the following procedure.

### ▼ To Load Existing Filtering Rules Files

1. Click **View -> Filtering Rules** to display the **Alarm Filtering Rules** dialog.
2. Click **Load** to open a **Select File** dialog and select the file containing filtering rules you want to use.
3. Click **OK** in the **Select File** dialog to load a rules file.
4. Click **OK** in the **Alarm Filtering Rules** dialog to put the filtering rules into effect.

### ▼ To Print Filtering Rules

1. Click **View -> Filtering Rules** to display the **Alarm Filtering Rules** dialog.
2. Set the filters you want to use, or load an existing filter rules file.
3. Click **Print**.

The **Print** dialog is displayed, allowing you to print to a file or a specific printer and, optionally, specify a banner title.

The printout shows which filters have been selected and their assigned values.

---

## 5.6 Performing Operations on Alarms

You can perform the following operations on alarms:

- Acknowledge an alarm – Mark the alarm to indicate that you have seen it.
- Undo an acknowledgment – Remove the acknowledgment from an alarm.
- Clear an alarm – Mark the alarm to indicate that the problem is fixed.
- Undo a clear – Remove the clear indication from an alarm.
- Hide an alarm from the display – Make an alarm disappear from the Alarms window, although the alarm is still contained in the log.
- Annotate an alarm – Add to an alarm text that will be displayed with the alarm in the Alarms window.

You can perform operations on individual alarms or alarm associations.

---

**Note** – If you have associations on, and are looking at alarm instances within an association, you cannot perform any actions on an alarm instance in that association. Actions can be taken against individual alarms *only* when associations are off.

---

### 5.6.1 Acknowledging Alarms

When an operator acknowledges an alarm, the implication is that the operator is taking care of the problem. The Ack Opr and Ack Date fields are updated to indicate the user ID for the operator acknowledging the alarm and the time that it was acknowledged. Acknowledging changes the state of the alarm.



## ▼ To Acknowledge an Alarm

**1. In the main window, select the alarm you want to acknowledge.**

**2. Do one of the following:**

- Click the Ack check box in the alarm row.

or

- Click Actions -> Acknowledge.

The user ID of the person who acknowledges the alarm is listed in the Ack Opr column in the row for the alarm. The timestamp of the acknowledgment is displayed in the Ack Date column. You may have to use the horizontal scroll bar to see these fields in the Alarms window.

If you have associations on, all alarms in the association are marked acknowledged. If you have associations off, only the alarm instance is marked acknowledged.

## ▼ To Undo an Alarm Acknowledgment

**1. In the main window, select the alarm you do not want to acknowledge.**

**2. Do one of the following:**

- Click the Ack check box in the alarm row.

or

- Click Actions -> Undo Acknowledge.

If you have associations on, all alarms in the association are no longer marked acknowledged. If you have associations off, only the alarm instance is no longer marked acknowledged.

## 5.6.2 Clearing Alarms

When you clear an alarm, the implication is that the network problem that caused the alarm to be generated has been fixed. You can clear one alarm at a time, select multiple alarms and clear them, or set up Solstice EM to clear multiple related alarms when you clear only one. In the latter case, Solstice EM generates a new event to indicate that several related alarms have been cleared. See Section 5.1.7.2 “Automatically Cleared Alarms and Cleared Severity Events” on page 5-8 for more information about this feature.

## ▼ To Clear Alarms

**1. In the main window, select the alarm(s) you want to clear.**

**2. Do one of the following:**

- Click the Clear check box in the alarm row.

or

- Click Actions -> Clear.

The user ID of the person who clears the alarm is listed in the Clear Opr column in the row for the alarm. The timestamp of the clear is displayed in the Clear Date column.

If you have associations on, all alarms in the association are marked cleared. If you have associations off, only the alarm instance is marked cleared.

## ▼ To Undo an Alarm Clear

**1. In the main window, select the alarm you do not want to clear.**

**2. Do one of the following:**

- Click the Clear check box in the alarm row.

or

- Click Actions -> Clear.

If you have associations on, all alarms in the association are no longer marked cleared. If you have associations off, only the alarm instance is no longer marked cleared.

## ▼ To Automatically Clear Similar Alarms

1. Click **File -> Customize -> Properties** to open the Alarm Properties dialog.
2. Select **Clear Event Required**.
3. Click **OK** in the Alarm Properties dialog.
4. In the Alarms window, select an alarm you want to clear.
5. Do one of the following:
  - Click the Clear check box in the alarm row.

or

- Click **Actions -> Clear**.

The alarm and all similar alarms are marked cleared. Similar alarms are those that are identical in all attribute values except time and log record ID. Solstice EM then generates an event having the same attribute values as the cleared alarms, except for the severity attribute, which is Cleared. The event is displayed as an alarm in the Alarms window.

### 5.6.3 Hiding an Alarm in the Alarms Window

If you want an alarm or association to be displayed in the Alarms window, but you do not want to delete the alarm, you can hide it from view.

---

**Note** – Once an alarm or alarm association is hidden from the Alarms display, you cannot get it to redisplay unless you use the MIS Objects tool to modify the `displayState` attribute of the alarm's log record. See the *Customizing Guide* for more information about the MIS Objects tool.

---

## ▼ To Hide an Alarm in the Alarms Window

1. In the main window, select the alarm(s) you want to remove from the display.
2. Click **Actions -> Hide**.

The selected alarm is removed from the display, but it remains in the log.

## 5.6.4 Annotating Alarms

You can annotate an alarm to add notes or comments to provide additional information about the alarm. The annotation, or display text attribute, can only be seen through the Alarm Details window. See Section 5.3.2 “Viewing Alarm Associations and Alarm Instances” on page 5-11 for more information about viewing alarm details.

### ▼ To Annotate an Alarm

1. **In the main Alarms window, select the alarm you want to annotate.**
2. **Click Actions -> Annotate to open the Display Text dialog.**
3. **In the Display Text box, type the text you want to be displayed with the alarm.**

Useful annotations include the status of the problem, when it might be fixed, who is working on it, and so on.

If associations are on, all alarms in the selected association are annotated.

---

## 5.7 Deleting Alarms From the Log

You can delete alarms from the log in several ways.

- **Manually** – Select an alarm or alarm association in the Alarms main window, and delete it. See Section 5.7.1 “Deleting Alarms Manually” on page 5-25 for more information.
- **Automatically** – Have alarms deleted once they have been cleared by an operator and meet specified criteria (such as a certain severity level) or once they have been in the log for a specified period of time. See Section 5.7.2 “Selecting Alarms for Automatic Deletion After Clearing” on page 5-25 for more information.
- **Using Alarm Deletion Controllers** – Set up filters to select alarms to delete. See Section 5.7.3 “Filtering Alarms for Deletion” on page 5-26 for more information.

## 5.7.1 Deleting Alarms Manually

In the Alarms window, you can delete from the alarm log specific alarm instances or alarm associations.

### ▼ To Delete an Alarm From the Log Manually

1. **In the main window, select the alarm or association you want to delete.**
2. **Click Actions -> Delete to remove the alarm from the log permanently.**

Deleted alarms cannot be retrieved.

## 5.7.2 Selecting Alarms for Automatic Deletion After Clearing

You can set up Alarms to automatically delete from the log an alarm that has been cleared. You can select only alarms that meet certain criteria to be deleted in this fashion. For instance, you can specify that only alarms having minor severity or less, and which are older than five days be deleted automatically. The Alarm Properties dialog allows you to do this, as explained in the following procedure.

### ▼ To Select Alarms for Automatic Deletion After Clearing

1. **Click File -> Customize -> Properties to open the Alarm Properties dialog.**
2. **Select Delete on Manual Clear.**
3. **For the setting Alarms of Severity or Below, select the highest severity level alarm that you want to be automatically deleted after being cleared.**

For example, if you choose critical, the highest severity, alarms of any severity will be deleted. If you choose minor, only alarms having severity levels of minor, warning, or indeterminate will be deleted.

4. **For the setting Alarms Older Than, select the number of days, hours, and minutes an alarm must exist before being deleted.**

Alarms must meet both the severity level and time criteria before being deleted after being cleared.

5. **Click OK or Apply.**

## 5.7.3 Filtering Alarms for Deletion

The Alarm Deletion Controllers window allows you to create controllers used to select alarms to delete from the MIS. The alarm deletion controllers can be used to delete alarms from any log in the MIS, including the AlarmLog. This section describes creating controllers for deleting alarms from the AlarmLog.

---

**Note** – Before alarms can be deleted using controllers, the purge daemon (`em_purged`) must be running. To start the purge daemon, you must set the `EM_ENABLEPURGE` environment variable to `TRUE` and restart the MIS with the `em_services -start` command.

---

### ▼ To Create Alarm Deletion Controllers for Deleting Alarms Automatically

**1. Open the Alarm Deletion Controllers window in one of the following ways:**

- Click Tools -> Alarm Deletion Controllers in the Alarms window.
- From a command line, type the following command:

```
em_purgemgr [-host hostname]
```

where *hostname* is the name of a remote MIS.

**2. In the Alarm Deletion Controllers window, click Actions -> Create to open the Alarm Deletion Controllers Create dialog.**

**3. In the MIS field, specify the MIS on which you want to delete alarms.**

By default, the local MIS is displayed, but you can specify a remote MIS instead. The system from which you are running Solstice EM must have a trusted host relationship with the remote MIS.

**4. In the Controller Name field, type a name for the filter you are creating.**

**5. At the Deletion item, select Enabled to enable this controller.**

**6. In the Log Name field, select AlarmLog.**

If you use another log to collect alarms, you can select it from the list.

**7. In the Conditions area, make selections for the following options:**

- Alarm Severity – Select the severities of alarms that you want to delete.
- Alarm State – Select the cleared and acknowledged status of alarms you want to delete.

- **State Unchanged Since** – Specify the amount of time that an alarm must not have had a change in state (clear/acknowledge) before deleting.

**8. Click OK.**

The controller is displayed in the table in the Alarm Deletion Controllers window.

## ▼ To Modify an Existing Alarm Deletion Controller

- 1. In the Alarm Deletion Controllers window, select the filter you want to change, and click Actions -> Properties.**

You can also double-click the filter to open the Properties dialog.

- 2. Make the modifications to the filter.**

- 3. Click OK or Apply.**

## ▼ To Disable an Alarm Deletion Controller

- 1. In the Alarm Deletion Controllers window, select the filter you want to disable, and click Actions -> Properties.**

You can also double-click the filter to open the Properties dialog.

- 2. At the Deletion field, click Disabled.**

- 3. Click OK or Apply.**

The controller is marked Disabled in the Alarm Deletion Controller window. The controller will not be used for deleting alarms unless you enable it.

## ▼ To Delete an Alarm Deletion Controller

- 1. In the Alarm Deletion Controllers window, select the controller you want to delete, and click Actions -> Delete.**

- 2. Click OK.**

## ▼ To Display Alarm Deletion Controllers on a Remote MIS

1. In the Alarm Deletion Controllers window, click View -> Controller Selection.

2. In the MIS field, type the name of a MIS whose alarm deletion controllers you want to display.

You can enter more than one MIS if you want to connect to more than one MIS at a time to view their alarm deletion controllers.

3. In the Available Controllers field, select one or more MIS names and click the Show button to move the MIS name to the Shown Controllers field.

4. Click OK or Apply.

---

## 5.8 Logging Alarms Management Activity

The actions taken by network operators can be logged to a file. You can determine whether to log activity, and which activities to log using the Alarms Security dialog. The information is logged in a text file, located in the directory from which the Alarms tool was started.

### ▼ To Log Alarms Management Activity

1. Click File -> Customize -> Security to open the Alarms Security dialog.

2. In the MIS field, type the name of the MIS whose alarms activity you want to monitor.

3. Click Log the Operators Actions.

4. Select the activities you want to log.

5. Click OK.



---

## 5.9 Graphing Alarm Data

You can represent alarm data in graphical form to observe trends in areas of your network that are generating alarms. You can use alarm summary data or alarms from specific devices, and plot the alarm type or severity of alarms. You can also choose to do a static plot of current alarms in the log, or do a dynamic plot of data polled at an interval you specify.

### ▼ To Graph Alarm Data

1. **Select Tools -> Grapher to open the Graph dialog.**
2. **Specify a name for your graph.**
3. **Select options for Input, Plot, and Type.**
4. **Click OK.**

The Grapher window opens, displaying the name of your graph.

5. **Double-click the name of the graph to view it.**

**See also** Chapter 10 "Graphing Collected Data."

---

## 5.10 Customizing the Alarms Window

The organization and format of the information displayed in Alarms can be customized according to your preferences. Most of the settings you can change are contained in the Alarm Summary Rules dialog, although many of the settings apply only when summary view is off.

You can save the customization settings to a file and load them at a later time. If you save properties when you exit Alarms, the settings you choose in the Alarm Summary Rules dialog are saved in the `.em_alarmmgr_vp.cf` configuration file in your home directory and used by default each time you start Alarms. If you run Solstice EM as root and save properties, the settings are saved in `em_alarmmgr_vp.cf` in the `/` (root) directory.

The settings you can customize in the Alarm Summary Rules dialog include:

- Show duplicate alarms
- Scroll to the newest alarms automatically

- Display object name as fully distinguished name or system name
- Apply alarm color to entire row or only the first column
- Display attribute name using default name or one you define
- Show or hide selected attributes
- Display column order
- Sort order

## ▼ To Customize the Alarms Window Display

1. Click **View -> Summary Rules** to open the **Alarm Summary Rules** dialog.
2. Make your selections for displaying the alarm attributes.
3. Click **OK**.

## ▼ To Specify Alarm Attributes to Display

1. Click **View -> Summary Rules** to open the **Alarm Summary Rules** dialog.
2. In the **Hidden Attributes** list, select the attributes you want to display.  
You can select multiple attributes by pressing the Control key while you click, or select a range of attributes by pressing the Shift key while clicking the first and last attribute in the range.
3. Click **Show** to move the selected attributes to the **Shown Attributes** list.
4. In the **Shown Attributes** list, select any attributes you do not want to display.  
You can select multiple attributes by pressing the Control key while you click, or select a range of attributes by pressing the Shift key while clicking the first and last attribute in the range.
5. Click **Hide** to move the selected attributes to the **Hidden Attributes** list.
6. Select attributes in the **Shown Attributes** list and use the **Move Up** and **Move Down** buttons to place the attributes in the order in which you want the attribute columns displayed in the **Alarms** window.  
The attribute at the top of the list is displayed in the left most column and the attribute at the bottom of the list is displayed in the right most column.
7. Click **OK**.

## ▼ To Change Attribute Labels

1. Click **View -> Summary Rules** to open the **Alarm Summary Rules** dialog.
2. In the **Display Attribute Names** item, select **User Defined Name**.
3. Click **Label Names** to open the **Alarm Label Names** dialog.
4. In the **User Defined** column, select the row of the attribute you want to change.
5. Type the name you want displayed for the selected attribute in the **Alarms** window.
6. Click **OK**.

## ▼ To Change the Alarm Sort Order

1. Click **View -> Summary Rules** to open the **Alarm Summary Rules** dialog.
2. Click **Sort Order**, located between the attribute lists in the lower half of the dialog.

The Sort Order dialog is displayed.
3. In the **All Attributes** list, select the attributes you want to use for sorting alarms.

You can select multiple attributes by pressing the Control key while you click, or, select a range of attributes by pressing the Shift key while clicking the first and last attributes in the range.
4. Click **Add** to move the attributes to the **Sort Order** list.
5. In the **Sort Order** list, select any attributes you do not want to use for sorting alarms.

You can select multiple attributes by pressing the Control key while you click, or, select a range of attributes by pressing the Shift key while clicking the first and last attributes in the range.
6. Click **Remove** to move the attributes to the **All Attributes** list.
7. Select attributes in the **Sort Order** list and use the **Move Up** and **Move Down** buttons to place the attributes in the order you want them used for sorting.

For example, suppose you have chosen the attributes **Received On**, **Severity**, and **From**. If you want to sort by severity first, date received second, and object instance third, you must list the attributes in the order **Severity**, **Received On**, and **From**.
8. Click **OK**.

---

## 5.11 Customizing the Tools Menu

The Tools menu enables you to start other tools from the Alarms window. You can add, modify, and remove names of Solstice EM tools on the Tools menu. By default, only Grapher and Alarm Deletion Controller are listed in the menu. You can add other tools that you might find useful to access from the Alarms window, such as Log Entries and Event Logs.

You can save the customization settings to a file and load them at a later time. If you save properties when you exit Alarms, the settings you make in the Customize Tools dialog are saved in the `.em_alarmmgr_tp.cf` configuration file in your home directory and used by default each time you start Alarms. If you run Alarms as root and save properties, the settings are saved in `em_alarmmgr_tp.cf` in the `/` (root) directory.

---

**Note** – You cannot remove Grapher from the Tools menu.

---

### ▼ To Add or Change a Tool on the Tools Menu

1. Click **File -> Customize -> Tools Menu** in the Alarms main window to open the **Configure Tools Menu** dialog.
2. If you want to change an existing entry on the Tools menu, select the tool in the **Applications** list.
3. In the **Application Name** field, type or edit the name you want to appear in the Tools menu.
4. In the **Absolute Path to Executable** field, type or edit the complete path to the command used to start the application.  
For Event Logs, the default path is `/opt/SUNWconn/em/bin/em_logmgr`. For Log Entries, the default path is `/opt/SUNWconn/em/bin/em_logview`.
5. In the **Arguments** field, type the options you want to use with the command line.  
See the appropriate chapter for information on command line options for starting the tool.

**6. Do one of the following:**

- Click Add to add the tool to the list of applications on the Tools menu.
- Click Change to modify an existing entry.

**7. Click OK.**

## ▼ To Remove a Tool From the Tools Menu

- 1. Click File > Customize -> Tools Menu in the Alarms main window to open the Configure Tools Menu dialog.**
- 2. In the Applications list, select the tool you want to remove.**
- 3. Click Delete.**
- 4. Click OK.**

---

## 5.12 Reference

This section provides technical reference information about command-line options for working with alarms.

For detailed information about dialogs, menus, and other user interface elements, refer to the Solstice EM Online Help. To access Online Help, Click the Help button on any dialog box or select options from the Help menu located in the upper right corner of each Solstice EM tool window.

### 5.12.1 The `em_alarmmgr` Command

The `em_alarmmgr` command starts the Alarms tool. Before using this command, you must set appropriate environment variables by running one of the environment scripts in `/opt/SUNWconn/em/bin`.

If you use the Bourne shell, type:

```
source /opt/SUNWconn/em/bin/emenv.sh
```

If you use the C shell, type

```
source /opt/SUNWconn/em/bin/emenv.csh
```

The `em_alarmmgr` command uses the following syntax:

`em_alarmmgr [options]`

If you start Alarm Manager from the command line, and you are a non-root user, you are required to supply a password if password authentication is turned on.

Access to Alarms functions depends on the permissions granted to you through Security.

The optional parameters for the `em_alarmmgr` command are described in the following table.

**TABLE 5-3** `em_alarmmgr` Command-Line Options

Option	Description
<code>-help</code>	Displays a list of options (with descriptions) for the <code>em_alarmmgr</code> command.
<code>-host hostname</code>	Host name of a remote MIS; you can also specify an IP address as the host name.
<code>-device device-name</code>	Device name for which you want to view alarms. For a host, the device name is the <code>systemId</code> name, such as <code>platinum</code> . The device name is the name you would use to ping a network node of any kind.
<code>-device_fdn device-fdn</code>	Fully distinguished name of the device, for example <code>systemId=name:"zirconium" / agentTableType="CMIP" / agentId=id:"platinum"</code>
<code>-refresh refresh-rate</code>	Screen refresh rate in milliseconds.
<code>-log MIS-name:log-name</code>	Log name, which must include the MIS name, for example <code>silicon:AlarmLog</code> .
<code>-file config-file</code>	Path to the <code>.em_alarmmgr_fp.cf</code> filter configuration file.
<code>-id MIS-name:toponodeId</code>	ID of the topology node, which must include the MIS name; for example, <code>silicon:25</code> . See Chapter 4 "Viewing Network Components" for information about determining a device's topology node ID.

## 5.13 Configuration Files

The Alarms tool creates configuration files if you save properties when you exit the Alarms window. The table lists the configuration files and the names of the dialogs used to set the values within the files.

When the Alarms tool starts, it looks for the configuration files in your home directory, or in the / (root) directory if you use Solstice EM as root. If the files do not exist, the Alarms tool looks in the `$EM_HOME/config` directory. (The file names used in the `config` directory do not include an initial dot.) If the configuration files are not found in either location, the default properties are used.

Manual editing of these files (except the `em_alarmmgr_i18n.cf` file) is not recommended. You should use the Alarms dialogs to change the properties..

**TABLE 5-4** Configuration Files Used by Alarms Tool

Configuration File	Dialog Used to Set the Values
<code>.em_alarmmgr_fp.cf</code>	Alarms Filtering Rules
<code>.em_alarmmgr_vp.cf</code>	Alarm Summary Rules
<code>.em_alarmmgr_ap.cf</code>	Alarm Association Rules
<code>.em_alarmmgr_tp.cf</code>	Alarm Tools Properties
<code>.em_alarmmgr_i18n.cf</code>	No dialog associated, used for Internationalization.

The information displayed in the alarms data table changes dynamically, and cannot be internationalized by the operating system localization facility. However, you can use the internationalization properties configuration file to explicitly define localized aliases for certain strings that might display in the table. The file contains the replacement strings for these items.

The i18n Properties Configuration file (`.em_alarmmgr_i18n.cf`) has the following format:

```
"major"  "majeur"  
"minor"  "mineur"  
"critical" "critique"
```

Each line in the file consists of a pair of strings. For each pair, the first string is the string to be replaced, and the second string is the user-defined replacement. To define a replacement string, edit or add the appropriate pair in this file.

The characters in each line must begin at the left edge, and each statement must begin on a separate line.



# Controlling User Access

---

With the Security tool you can control user access to Solstice Enterprise Manager (Solstice EM) tools and managed objects. Based on the needs and responsibilities of system administrators, operators, and other users managing the components of your network, you can determine who may use any of the Solstice EM tools, and which managed objects they are allowed to access and manipulate for monitoring purposes.

This chapter comprises the following topics:

- Section 6.1 “Overview” on page 6-1
- Section 6.2 “Getting Started With Security” on page 6-8
- Section 6.3 “Turning Off Access Control” on page 6-9
- Section 6.4 “Preparing for Security Control” on page 6-10
- Section 6.5 “Controlling Access to Solstice EM Tools” on page 6-24
- Section 6.6 “Controlling Access to Managed Objects” on page 6-31
- Section 6.7 “Using the `em_accesscmd` Utility” on page 6-50

---

## 6.1 Overview

Controlling user access to Solstice EM tools and managed objects is an option.

Without access control, anyone can access all Solstice EM tools and manipulate the managed objects. The risks of this approach can be devastating when individuals without the proper authority or expertise alter or delete important components of the Solstice EM configuration and object attributes.

By controlling user access, you can prohibit unwanted access to critical applications and network components. By controlling user access, users are allowed to access only those applications and objects they need based on their network management responsibilities and other relevant criteria.

## 6.1.1 Understanding the Solstice EM Access Control Model

The access control model used by Solstice EM is based on the X.741 Recommendation issued by the International Telecommunications Union (ITU). This model uses *rules* and a *logic* in which these rules are enforced as a mechanism to control user access.

### 6.1.1.1 Security Rules

The basis for denying or granting users access to tools and managed objects are *security rules*. Security rules are controls that identify the *user groups* to which access controls are to be applied, the *tools* or *managed objects* for which access is to be denied or granted, and the *policy* to determine if access is to be denied or granted.

As such, the tasks outlined in this chapter involve working with users, tools and managed objects, and creating security rules.

What differentiates security rules from each other is the range of access granted or denied to the user groups.

### 6.1.1.2 Policy for Enforcing Security Rules

---

**Note** – Security rules that deny access to tools and managed objects are always enforced *before* security rules that grant access.

---

---

**Note** – When users derive their access privileges from multiple security rules, only one of these security rules will be enforced and determine the user's access to tools and managed objects.

---

The preceding notes contain the two fundamental principles to remember for determining an individual user's access. The principles and the policy logic are the same for controlling user access to Solstice EM tools and managed objects. The following graphic illustrates the logic of the policy that is used.

The policy logic used to enforce the security rules is a process of elimination, done in a hierarchical manner. When multiple security rules define an individual user's access privileges, only one of these rules will determine what the user can and cannot do.

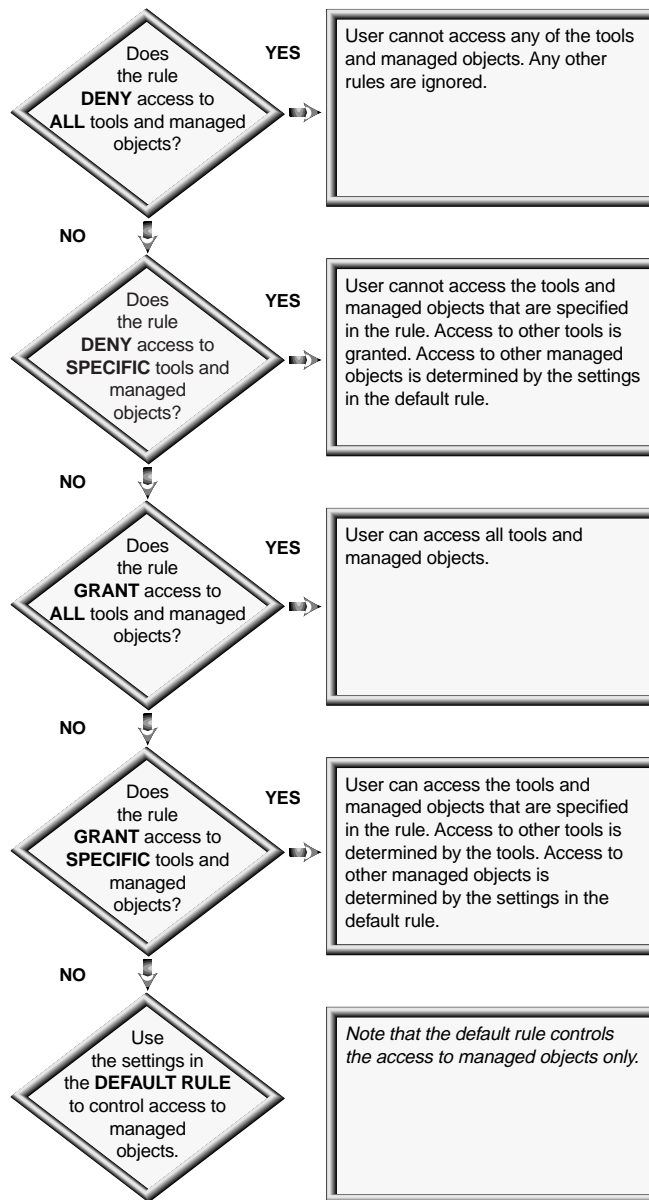


FIGURE 6-1 Solstice EM Enforcement of Security Rules

### 6.1.1.3 About Users and Groups

In the Solstice EM control model, security rules are not set for individual users but for a group of users. This requires using existing user groups, or creating new groups and assigning individual users to such groups.

The identity of individual users and the groups to which they belong needs to be known to the MIS to which they connect. User identity is recorded in an access control list. User group data is recorded in profiles. (See Section 6.4.6 “Preparing User Profiles” on page 6-16 for more information on user profiles.)

The control model used by Solstice EM allows individual users to belong to more than one group. This can result in situations where several seemingly conflicting rules control the access privileges of an individual user. In reality there is no conflict because of the policy logic in which the rules are enforced. The following scenario best illustrates the point.

**Example**– User John Doe is an operator monitoring alarms exclusively pertaining to routers. As such, John belongs to two user groups: the Operators group and the Routers group.

Users of the Operators group derive their privileges from one rule which denies them access to the Event Logs tool. Users of the Routers group derive their privileges from one rule which grants all users of that group access to all Solstice EM tools.

The question is: “Can John Doe start and use the Event Logs tool, say for creating or editing log files?” The answer is *NO* because rules that deny access are always enforced before rules that grant access. John, however, does have access to any of the other Solstice EM tools.

---

**Tip** – The preceding example illustrates the importance of ensuring that you do not assign Solstice EM users to user groups whose access to tools and managed objects would be denied due to conflicting security rules. Thorough advance planning and good record keeping should help avoid access problems.

---

#### See Also:

- The Implementation Overview section in “Preparing for Security Control” on page 6-10 for more information about users, groups, and profiles.
- The Implementation Overview section in “Controlling Access to Solstice EM Tools” on page 6-24 for more details about the type of rules to use for controlling user access to applications.
- The Implementation Overview section in “Controlling Access to Managed Objects” on page 6-31 for more details about the type of rules to use for controlling user access to managed objects.

## 6.1.2 Predefined Groups, Security Rules, and Object Sets

The Solstice EM installation procedure provides you with a minimum of predefined privilege groups, security rules and sets of objects to get you started.

- **Predefined privilege groups** – Full Access, Operators, and View Only. The use of the predefined and custom-created privilege groups is required when you want to control user access to the tools, managed objects, or both.
- **Predefined security rules** – Full Access, DenyAccessControlObjectsChange, and View Only. Use the predefined security rules as a starting point for controlling user access to managed objects.
- **Predefined object sets** – DenyAccessControlObjectsChange, Connection, and View Only. Use the predefined object sets as a starting point to control user access to managed objects.

The installation procedures give you the opportunity to enable or disable (default) access control. If you choose to enable access control, you are also given the opportunity to create user profiles and to assign users to one of the three default privilege groups provided by the Solstice EM installation.

## 6.1.3 Implementation Schemes for Access Control

When you want to control user access, you can opt for the following schemes:

- **Control user access to tools.** This scheme is best suited when you are new to Solstice EM. It is also a stepping stone toward the more complex task of controlling user access to managed objects.
- **Control user access to managed objects.** This scheme is best accomplished after you have acquired expertise in controlling user access to Solstice EM tools and tasks.

### 6.1.3.1 Control User Access to Tools

This scheme enables you to specify for a group of users the tools and tasks to which they are granted and denied access. The term *tool* means any Solstice EM tool such as Network Views, Network Discovery, Alarms, Security, and so on, as well as any custom-developed or third party application integrated using the Solstice EM API. The term *task* means any application features supported by the tool, such as create, edit, delete, and so on.

For example, network administrators should be able to create log files and alter the events that are to be recorded, while operators may only need the capability to view log records. In this instance, you would grant your network administrators the privilege to start and use the Event Logs tool to create and specify the contents of log files. In contrast, operators would be denied access to the Event Logs tool but would be able to use the Log Entry tool to look at log records.

### 6.1.3.2 Control User Access to Managed Objects

This scheme enables you to specify the managed objects to which a group of users is granted and denied access. The term *managed object*, and any of its variations such as *object sets*, are the representations of network components such as routers, hubs, bridges, logical and hierarchical views of the network, alarms, and so on.

Assume your company has regional headquarters in Boston and San Francisco. The two regional system administrators should only be able to manage the network components pertaining to their respective areas. By controlling access to managed objects, you can create access controls that exclude the Boston system administrators from seeing and manipulating network components pertaining to the San Francisco headquarters and vice versa.

## 6.1.4 Implementation Plan

Implementing an access control scheme requires that you put the necessary framework in place. You need to perform a number of preparatory tasks to set the stage for setting access controls to tools only, or to tools and managed objects.

This chapter is organized according to the implementation schemes discussed in Section 6.1.3 “Implementation Schemes for Access Control” on page 6-5.

- Section 6.1 “Overview” on page 6-1 provides information that is pertinent to controlling user access to Solstice EM tools and managed objects.
- Section 6.4 “Preparing for Security Control” on page 6-10 provides an overview and preparatory tasks that need to be performed when you want to control user access to both Solstice EM tools and managed objects.
- Section 6.5 “Controlling Access to Solstice EM Tools” on page 6-24 provides an overview and tasks for controlling user access to tools.
- Section 6.6 “Controlling Access to Managed Objects” on page 6-31 provides an overview and tasks for controlling user access to managed objects.

The following table identifies the major tasks to be accomplished for each of the implementation schemes and the sections in this chapter where the information can be found.

**TABLE 6-1** Implementation Schemes

Implementation Scheme	Implementation Guidelines
<p><b>No access control.</b></p> <p>All users have full and equal access to all applications and managed objects.</p>	<ul style="list-style-type: none"> <li>• If you chose to disable security control during the installation procedure, no other tasks need to be performed.</li> <li>• If you chose to enable security control during the installation procedure, but do not want to implement security control after all, then turnoff access control as explained in Section 6.3 “Turning Off Access Control” on page 6-9.</li> </ul> <p>No other access control tasks discussed in this chapter need to be performed. See <i>Chapter 2</i> of the <i>Installation Guide</i> for more information about enabling or disabling security during installation.</p>
<p><b>Tool access control</b></p>	<ul style="list-style-type: none"> <li>• If security control was disabled during the installation procedure, turn on access control as explained in Section 6.4.4 “Turning On Security Control” on page 6-13.</li> <li>• Perform the tasks as explained in Section 6.4 “Preparing for Security Control” on page 6-10.</li> <li>• Follow the directions of Section 6.5 “Controlling Access to Solstice EM Tools” on page 6-24.</li> </ul>
<p><b>Managed object access control</b></p>	<p>If you did <i>not</i> implement any application access controls:</p> <ul style="list-style-type: none"> <li>• Turn access control on as explained in Section 6.4.4 “Turning On Security Control” on page 6-13.</li> <li>• Prepare for access control as explained in Section 6.4 “Preparing for Security Control” on page 6-10.</li> <li>• Control user access to Solstice EM tools as explained in Section 6.5 “Controlling Access to Solstice EM Tools” on page 6-24.</li> <li>• Control user access to managed objects as explained in Section 6.6 “Controlling Access to Managed Objects” on page 6-31.</li> </ul> <p>If you implemented access controls to tools:</p> <ul style="list-style-type: none"> <li>• Control user access to managed objects as explained in Section 6.6 “Controlling Access to Managed Objects” on page 6-31.</li> </ul>

Each section starts with an overview that provides details about concepts and other information appropriate for the tasks to be performed.

## 6.1.5 Related Tasks

See the Chapter 5 in the *Customization Guide* for information on creating log files.

## 6.1.6 Related Files

- /opt/SUNWconn/em/build/acct/EM-config
- /opt/SUNWconn/em/build/acct/init\_access\_privileges
- /opt/SUNWconn/em/build/acct/init\_access\_user\_apps
- /opt/SUNWconn/em/build/acct/init\_user
- The em\_login daemon

---

# 6.2 Getting Started With Security

All access control operations are performed in the Solstice EM Security window which is displayed when you start the Security tool.

You can start the Security tool from the following places:

- The Administration window accessible from Network Tools
- The operating system command line

When logged in as root or users with permission to grant All Privileges start Security, they always have the right to connect to the MIS without user ID and password authentication.

Users belonging to less privileged user groups can connect to the MIS with user ID and password authentication when security rules allow them to do so.



## ▼ To Use Security

### 1. Start Security in one of the following ways:

- From the Network Tools window, click Administration, and then click Security.
- From an operating system prompt, enter the following command:

`em_accessmgr` (to connect to a local MIS server)

or

`em_accessmgr [-help] [-host hostname] &`

For example: `em_accessmgr -host omega` to connect to the MIS on the server `omega` and start the Security tool.

The Security window is displayed.

### 2. Perform any of the tasks discussed in this chapter.

### 3. Click File->Exit when you are finished.

**See Also** Section 6.8.1.1 “The `em_accessmgr` Command” on page 6-55 for more information about the command options.

---

## 6.3 Turning Off Access Control

When you turn off access control, you are giving all Solstice EM users complete access to applications, managed objects, and the operations for manipulating the objects. Any Solstice EM user can add and remove applications, add and remove managed objects, and change object attributes.

Turning off access control can be done either during or after the installation procedure. If you turned off access control during installation, no further tasks need to be performed. You can always turn on access control later when you want to control user access.

In the event access control had previously been turned on, either during installation or at a later point in time, you can override it by disabling access control. If you do, any security rules that were put in place before disabling access control will no longer control the users' actions.

Turning off access control requires you to disable access control.

## ▼ To Turn Off Access Control

1. **Start the Security tool in one of the following ways:**

- From the Administration window, click Security.
- From the command line, execute the following command line at an operating system prompt:

```
em_accessmgr
```

or

```
em_accessmgr -host MIS_Server_Name
```

2. **In the Security window, click Actions->Security Defaults to display the Defaults dialog.**

3. **Verify that the Security option at the top of the dialog is “Off.”**

4. **Click OK.**

---

## 6.4 Preparing for Security Control

As explained in “Understanding the Solstice EM Access Control Model” on page 6-2, individual users derive their access privileges from *security rules* that are applied to the *privilege group* to which they belong. The chapter overview also explained that users can belong to more than one group. In such event, users derive their access privileges from all the groups to which they belong.

Whether you want to control user access to Solstice EM tools and tasks only, or also to managed objects, you need to perform a number of preparatory tasks to ensure the necessary framework is in place. The section “Getting Ready for Security Control” on page 6-12 in this chapter takes you through the tasks in the sequence that they need to be performed.

### 6.4.1 About Users, Granting All Privileges, and Root

All Solstice EM users must have UNIX accounts which you create using the UNIX administration tools available for this purpose, such as `admintool` from Solaris. In addition, the identity of the users must be recorded in an access control list. This is done by using Solstice EM. Solstice EM makes a distinction between users who are logged in as root, users who can grant all privileges, and regular users.

Users who are logged in as root or users who can grant all privileges always enjoy the following access privileges:

- Full access to all the Solstice EM tools, managed objects, and the `em_accesscmd` utility, even if they belong to a group controlled by restrictive rules.
- Create and modify Solstice EM user information and group profiles.
- Access to remote MIS servers.

Users not logged in as root or who cannot grant All Privileges in Security tool cannot change security access controls. However, they can access tools and manipulate managed objects based only on their access privileges to tools and managed objects.

## 6.4.2 About Privilege Groups

Solstice EM privilege groups—also referred as *groups*—are a collection of Solstice EM users having the same security privileges. Solstice EM privilege groups have no relationship to UNIX user groups. Privilege groups can have one or more members. There is no limit to the number of users you can assign to a group. Also, users can belong to more than one group.

Security rules are set for the groups. When users belong to several privilege groups, they derive their security privileges from all the rules that control the groups to which they belong. As such, users may have seemingly contradictory privileges. Refer to Section 6.1.1 “Understanding the Solstice EM Access Control Model” on page 6-2 for more information about how Solstice EM determines user access.

Group details such as membership, tools, and/or managed objects that group members can access based on the access privileges, are recorded in *profiles*. These profiles are represented as objects in the management information base.

A Solstice EM installation provides the following predefined groups.

**TABLE 6-2** Pre-defined Groups

User Group Name	Description
Full Access	Users belonging to this group can access all Solstice EM tools, create, modify, and delete all Solstice EM tools and managed objects according to any existing rules or the settings of the default rule. Users will not be able to update the security access controls. This is <i>not</i> quite the same as turning off access control. When access control is turned off, no existing rules limit the user's access to applications and managed objects.
Operators	Users belonging to this group can access specific tools and modify specific managed data.
View Only	Users belonging to this group can view a restricted set of controlled object data, but they cannot modify the data. Users in this group have access to a restricted set of tools to use for viewing data to which they have access.

### 6.4.3 Getting Ready for Security Control

Getting ready for security control requires you to carry out several preparatory tasks. The following outlines the tasks to be performed if you want to control user access to either Solstice EM tools or to managed objects.

1. Log in as root or as super user, create UNIX accounts for all Solstice EM users.
2. If not enabled during installation, turn on access control.  
Follow the instructions in “Turning On Security Control” on page 6-13.
3. If multiple management information servers are used, prepare for remote connections to the MIS.  
Follow the instructions in “Preparing for Remote Connections to the MIS” on page 6-14.

4. Prepare user profiles, if you did not do so during the installation. If you did and need not add any other profiles, skip this step. If you prepared some user profiles during installation, but need to add more, then execute this step.

- a. Follow the instructions in “Preparing User Profiles” on page 6-16.

Note that at this stage of preparing user profiles you cannot yet specify group membership. You will be able to assign users to groups when you prepare the group profiles.

- b. If specific users need the ability to grant all privileges, follow the instructions in “Granting Security Privileges” on page 6-17.

5. Prepare group profiles.

Follow the instructions of “Preparing Group Profiles” on page 6-18.

At this stage you will be able to complete the user profile by assigning group membership.

Note that group profiles will be completed with information about the list of tools, and the rules for controlling user access to tools, when you perform the tasks described in “Controlling Access to Solstice EM Tools” on page 6-24.

Similarly, the group profiles will be completed with information about the managed objects, and the rules for controlling user access to the objects, when you perform the tasks described in “Controlling Access to Managed Objects” on page 6-31.

## 6.4.4 Turning On Security Control

When you enable access control, you can grant or deny user access to the tool itself and to the operations that can be performed with these tools. Regarding access to managed objects, you can determine which users have access to which objects, and the operations they can perform on these objects.

Turning on access control requires you to do the following:

- Enable the Security option
- Edit the security controls in the Solstice EM configuration file
- Restart the MIS

### ▼ To Turn On Security Control

1. In the Security window, click Actions->Security Defaults to display the Defaults dialog.

**2. Enable or disable access control:**

- To enable access control, verify that the Security option at the top of the dialog is On (default).
- To disable access control, verify that the option is Off.

**3. Click OK.**

**4. Edit the assignments for the following access control variables in the `$EM_HOME/build/acct/EM-config` configuration file:**

- `EM_ACCESS_PASSWORD_CONTROL`
- `EM_ACCESS_CONNECTION_CONTROL`
- `EM_ACCESS_BACKWARD_COMPATIBILITY`

**5. For each of these variables, use TRUE to enable and FALSE to disable the variable.**

The following is an example of access control settings in an EM-config file.

```
#####  
# Access control configuration variables  
#####  
EM_ACCESS_PASSWORD_CONTROL:      TRUE  
EM_ACCESS_CONNECTION_CONTROL:    TRUE  
EM_ACCESS_BACKWARD_COMPATIBILITY: FALSE  
#####
```

The two TRUE statements indicate that access to Solstice EM will be controlled and that user password will be required and verified. the FALSE statement indicates that objects created using Solstice EM V2.1 will not be accessible. See the *Developing Applications* guide for details concerning this configuration file.

**6. Restart the MIS after turning on Security by executing this command at an UNIX system prompt:**

```
em_services -reload
```

## 6.4.5 Preparing for Remote Connections to the MIS

To connect to a remote MIS server, the following must be set up:

- The names of the systems connecting to the MIS server must be added to the list of trusted hosts on the system where the MIS resides.
- If the users connecting to the MIS need the capability to set and change object attributes or access controls, you must enable the “Grant All Privileges” option for each of these users.

When users connect to a remote MIS server, the machine from which they are connecting must be recognized as a *trusted host* by the server on which the MIS resides. For example, when John Doe connects from the machines called `alpha`, `beta`, and `gamma`, to a remote MIS server called `omega`, then the systems `alpha`, `beta`, and `gamma` must be known as a trusted host to establish a connection to `omega`. You accomplish this by adding the names of the `alpha`, `beta`, and `gamma` systems to the list of trusted hosts in the Security Defaults dialog on the `omega` server.

With an established trusted host relationship, users can connect to a remote MIS but cannot make any changes. To connect to a remote MIS with the intention of changing object attributes, or application access, or both, users must be able to grant all privileges, or be able to log in as root. See “Granting Security Privileges” on page 6-17 for step-by-step instructions.

## ▼ To Allow Connections to a Remote MIS Server

1. In the Security window, click **Actions->Security Defaults** to display the Defaults dialog.
2. Next to **Trusted Hosts** at the bottom of the dialog, type the name of the MIS server and click **Add**.  
Repeat this step for every MIS server to which the users who can grant all privileges should be able to connect to.
3. Click **OK**.

## ▼ To Prevent Connections to a Remote MIS Server

1. In the Security window, click **Actions->Security Defaults** to display the Defaults dialog.
2. Select the MIS server from the list of trusted hosts and click **Delete**.  
Repeat this step for every MIS server to which users who can grant all privileges should no longer be able to connect to.
3. Click **OK**.

## 6.4.6 Preparing User Profiles

When access control is turned on, Solstice EM requires that the identity of users be known to the management information server. User profile information is recorded in a Solstice EM access control list. In addition to the profile information, Solstice EM requires that all users have UNIX accounts.

---

**Note** – It is imperative that the UNIX accounts be created before you create the user profiles. Failing to do so will result in your inability to prepare user profiles and an error message will be displayed.

---

When access control is turned off, UNIX accounts are still needed but no Solstice EM user profiles need to be created.

To prepare user profiles you will need the following information:

- User ID of the user's UNIX account.
- The individual's first and last names.
- Whether the user will be able to grant all privileges. See Section 6.4 "Preparing for Security Control" on page 6-10 and Section 6.4.7 "Granting Security Privileges" on page 6-17 for more information.

User profiles are prepared using either the Security tool or the command line. Using the Security tool, you create new user profiles in one of the following two ways:

- Completing the User Create dialog
- Duplicating an existing user profile

For preparing user profiles from the command line, see Section 6.7 "Using the em\_accesscmd Utility" on page 6-50.

### ▼ To Prepare User Profiles

1. In the Security window, click Actions->Create to display the Create dialog.
2. On the Identity tab, in User Login, type the user ID.

For example: `jdoe`. The user ID must be a valid login ID for the host on which the current MIS is running. What you type in this field is what is listed in the User Login column in the Security window.

3. In Full Name, type the user's first and last names.



4. **For users who will be entrusted with security management, click Grant All Privileges.**

See Section 6.4.7 “Granting Security Privileges” on page 6-17 for more information on the privileges associated with the option of Granting All Privileges.

5. **Click Apply to continue adding other users, or click OK when you have finished.**

The user ID is immediately added to the list of users and groups, and an empty user profile object for that individual is added to the MIS.

Group membership cannot be assigned until group profiles have been prepared. Once group profiles have been prepared, you can assign group membership.

## ▼ To Prepare User Profiles by Duplication

1. **In the Security window, click the Users tab to list the existing users.**
2. **Select the user whose profile you want to use for creating a new one.**
3. **Click Actions->Duplicate to display the Duplicate dialog.**
4. **On the Identity tab, type the user login for the user profile you want to create.**
5. **Enter the user’s first and last names.**
6. **Click any of the other tabs and update the information as necessary.**
7. **Click OK.**

## 6.4.7 Granting Security Privileges

When access control is turned on, users who can grant all privileges—regardless of the groups to which they belong—are automatically granted update privileges to controlled applications and managed objects.

The option Granting All Privileges enables any user to use all Solstice EM tools, to manipulate and update managed objects and access privileges to which they normally do not have access. Users who can grant all privileges may update user records and group profiles *except their own*, change security rules, change access controls to applications, and update object attributes.

The privilege of granting all privileges can be given to any user when you prepare the user’s profile or later as the need arises.

---

**Note** – Note that users who are member of the Full Access group do not automatically have the ability to grant all privileges.

---

## ▼ To Grant Security Privileges

1. In the Security window, click the Users tab to display all Solstice EM users.
2. Click the user record to select it and then click Actions->Properties to display the Properties dialog for the selected user.
3. Click Grant All Privileges.  
When selected, the option displays a check mark.
4. Click OK.

### 6.4.8 Preparing Group Profiles

When access control is turned on, group identities, just like user identities, need to be recorded in profiles that are stored in the management information database as objects. Group profiles also identify the security rules that determine whether or not the group members are granted or denied access to the specified tools and the managed objects.

To prepare group profiles you need to have the following information on hand:

- The name to be given to the group
- The IDs of the users who will become members of the group

Group profiles will be completed when you carry out the task for controlling user access to applications and managed objects.

Group profiles are created using the Solstice EM graphical user interface or from the command line. Using the graphical user interface, you create group profiles in one of the following two ways:

- Completing the Group Create dialog
- Duplicating an existing group profile

For preparing group profiles from the command line, see Section 6.7 “Using the em\_accesscmd Utility” on page 6-50.

---

**Tip** – Use the Full Access users group (or any other existing group) as the basis for creating (by duplication) group profiles for new users groups; then, modify the access controls for the newly created group as needed.

---

## ▼ To Prepare Group Profiles by Duplication

1. In the Security window, select the Privilege Groups tab to display the list of existing privilege groups.
2. Select the group you want to use as the basis for creating a new privilege group.
3. Click Actions->Duplicate to display the Group Duplicate dialog.  
This dialog is identical to the Create Privilege Group dialog. A duplicate of that group is created and the group information is loaded into the dialog.
4. On the Identity tab, type the name of the new privilege group
5. Type a group description.
6. Move from tab to tab and modify the existing group information to meet the requirements for the new group.
7. Click OK.

## ▼ To Prepare Group Profiles

1. In the Security window, select the Privilege Groups tab.
2. Click Actions->Create to display the Create Group dialog.
3. On the Identity tab, in Privilege Group Name, type the group's name.
4. Type a group description.  
For example, if the group will contain the names of operators monitoring the routers in your network, "Router Operators" might be a suitable name.
5. On the Members tab, specify the group members as follows:
  - Select one or more users from the Managed Users list on the left and click Add.
  - To select all users, click Select All and then click Add.

The rest of the group profile will be completed when you carry out the tasks outlined in Section 6.5 "Controlling Access to Solstice EM Tools" on page 6-24 and Section 6.6 "Controlling Access to Managed Objects" on page 6-31.

## 6.4.9 Saving and Reusing Profiles

After defining profiles for the Solstice EM users and groups, you may want to save the profile information to a file of your choice. This file can then be loaded back into the system after an upgrade or a re-installation of Solstice EM.

When importing a file, the file to be imported must have been created using the Export command. The imported access information is created in the current MIS. This information is appended to any pre-existing information. No information is removed.

### ▼ To Save Profiles

1. In the Security window, click **File->Export** to display the **Export dialog**.
2. Select one of the following options:
  - **All Access Control Objects** – Select this option to save the access control data of all users, groups, and trusted hosts, applications, targets, rules, and security default information for the current MIS.
  - **Users, Groups, Trusted Hosts, and Application List** – Choose this option to save information for the current MIS.
  - **Targets, Rules, and Security Defaults** – Select this option to save control access data information for the current MIS.
3. In **File Name**, type a directory path name and file name for saving the profiles.

If you do not know the directory path name, click **Browse** to select a directory path name. Use the \* wildcard and click **Filter** to filter the contents of the selected directory. For example, `/home/user1/EM_EXPORTS/*` will display the contents of this directory; from this list, select the file to which the data should be saved. If the file does not exist, type a file name.
4. Click **OK**.

### ▼ To Reuse Saved Profiles

1. In the Security window, click **File->Import** to display a standard **Select File dialog**.
2. Enter the directory path and file name, or click **Browse** to search for and select an existing profile file.
3. Click **OK**.

## 6.4.10 Printing Profiles

You can print the list of Solstice EM users and groups in two formats:

- **Text format** – Prints the existing user groups and their members in plain ASCII format.
- **Table format** – Creates an encapsulated PostScript file of the table listing the user groups in the Security window.

### ▼ To Print Profiles

1. In the Security window, click **File->Print** to display the **Print** dialog.
2. Select **Print to File or Printer** as print destination.  
If you select **Print to File**, click the [...] button to display a file selection dialog from which you select the profile to be printed.
3. Select either **Text** or **Table** format.
4. Click **Print**.

## 6.4.11 Searching for Users and Groups

Solstice EM provides a search mechanism for finding existing Solstice EM users and groups based on search criteria that you specify.

### ▼ To Search for Users and Groups

1. In the Security window, click **Action->Find** to display the **Find** dialog.
2. Select **User or Privilege Group** from the **Find** options.
3. Select the type of match.
4. Specify whether or not to use case sensitivity when searching.
5. (Optional) Enter the search string.
6. Click **Find** to start searching.
7. Click **Close** to exit.

## 6.4.12 Maintaining User Profiles

Maintaining user profiles includes the following activities:

- Modifying the profile properties of existing users
- Assigning users to other groups
- Deleting user profiles

The above tasks can be performed using the Security tool as explained below, or from the command line as explained in Section 6.7 “Using the `em_accesscmd` Utility” on page 6-50.

### ▼ To Update User Profiles

1. In the Security window, click the Users tab to display the existing users.
2. Select the user from the list, and click Actions->Properties to display the Properties dialog for the selected user.
3. Move from tab to tab and enter your changes.
4. Click Apply to change and keep the dialog open, or click OK to change and exit.

### ▼ To Assign Users to Other User Groups

1. In the Security window, click the Users tab to list the existing users.
2. Select the user from the list and click Actions->Properties to display the Properties dialog for the selected user.  
Alternatively, double-click on the user's name.
3. Select the Privilege Groups tab.
4. To add the user to another privilege group, select the privilege group from the list on the left and click Add.
5. If necessary, to remove the user from a privilege group to which the user currently belongs, select the privilege group from the list on the right and click Remove.
6. Click Apply or OK.

## ▼ To Delete User Profiles

1. In the Security window, click the Users tab to list all existing users.
2. Select the name of the user to be deleted.
3. Select Actions->Delete.
4. Click OK.

### 6.4.13 Maintaining Group Profiles

Maintaining group profiles includes the following activities:

- Updating the properties of groups, such as the changing the group's members, the group's privileges to applications and database objects
- Deleting groups

The above tasks can be performed using the Security tool as explained below, or from the command line as explained in Section 6.7 “Using the em\_accesscmd Utility” on page 6-50.

## ▼ To Update Group Profiles

1. In the Security window, click the Privilege Groups tab to list the existing groups.
2. Select the privilege group whose profile is to be updated and click Actions->Properties to display the Group Properties dialog.  
Alternatively, double-click the privilege group.  
The dialog is identical to the Group Create dialog.
3. Moving from tab to tab, update the group's properties as necessary.
4. Click OK.

## ▼ To Delete Group Profiles



---

**Caution** – Deleting groups by deleting group profiles irrevocably and immediately removes the corresponding group profile objects from the MIS.

---

1. In the Security window, click the Privilege Groups tab to list the existing groups.
2. Select the privilege group you want to delete and click Actions -> Delete.

---

## 6.5 Controlling Access to Solstice EM Tools

This section of the guide discusses the tasks you need to perform to control user access to Solstice EM tools.

The tasks involved in controlling access to tools are easy to accomplish. As such, controlling user access to Solstice EM tools can be considered a stepping stone toward building the expertise you need to control user access to managed objects.

---

**Note** – Before you carry out any of the tasks outlined in this section of the chapter, you must have accomplished all the required preparatory tasks outlined in Section 6.4 “Preparing for Security Control” on page 6-10.

---

### 6.5.1 Implementation Overview

This overview expands the concepts introduced in the chapter overview and discusses them in more detail.

This Implementation Overview provides more details about the following:

- Definition of Solstice EM tools and tasks
- Security rules for controlling access to tools
- Guidelines for controlling access to tools



### 6.5.1.1 About Solstice EM Tools and Tasks

Solstice EM enables you to control access at the tool level and at the task level.

As used in this guide, *tool* means any Solstice EM tool and any custom-developed application developed using the Solstice EM API; *tasks* mean any of the tool features supported by the tool, such as edit, create, delete, and so on.

Before you can proceed with setting access controls, all tools must be placed under Solstice EM Security control.

### 6.5.1.2 Security Rules for Controlling Access to Tools

As explained in “Overview” on page 6-1, security rules are at the heart of Solstice EM for controlling user access. User access to tools can be controlled by creating security rules that deny or grant access in the following ways:

- **Deny members of identified groups access to all Solstice EM tools** – Use this type of rule when you want to exclude specific users from accessing any Solstice EM and all of the Solstice EM tools. When no specific groups are identified, the rule applies to all groups.
- **Deny members of identified groups access to specific Solstice EM tools** – Use this type of rule when you want to ensure that specific users do not have the capability to run specific tools. For example, denying operators the right to create log files using Solstice EM’s Event Logs tool.
- **Deny members of identified groups the ability to perform specific tasks when using Solstice EM tools** – This type of rule allows specific users to run the tools but they are denied access to specific tool features, such as the edit or delete function provided by the tool. For example, allowing operators to view log records using Solstice EM’s Log Entries tool, but denying them the capabilities of editing the log records in the log file, or deleting them using the Log Entries tool edit and delete functions.

The logic used for controlling user access is explained in Section 6.1.1 “Understanding the Solstice EM Access Control Model” on page 6-2.

Access to the tool is enforced by the tool itself. The MIS only stores the list of features that can be accessed for each application.

## 6.5.2 Getting Ready to Control Access to Solstice EM Tools

The tasks in this section need to be carried out if you want to control user access to Solstice EM tools and tasks. The following outline is a high-level overview of the tasks to be performed.

1. Make sure you have accomplished all preparatory tasks.

See Section 6.4.3 “Getting Ready for Security Control” on page 6-12.

2. If necessary, add custom-developed applications to Solstice EM.

Follow the instructions in Section 6.5.3 “Placing Tools Under Security Control” on page 6-26.

3. Define the privileges for accessing tools and tasks.

Follow the instructions in Section 6.5.5 “Granting and Denying Access to Tools and Tasks” on page 6-29.

## 6.5.3 Placing Tools Under Security Control

Before you can specify access controls to applications and tasks, you must ensure that any custom-developed applications for which you want to control user access are under Solstice EM control.

If you plan on controlling user access at the task level for custom-developed applications, you will need to obtain the following:

- The name of the application’s executable(s).
- The exact name of the application tasks to which access will be controlled. The task name must be the name recognized by the application. For example, if you want to control user access to the delete function of the XYZ application, you need to know that the developer named that function “XYZDelete.”

Once the tools are added to Solstice EM, tasks supported by the tools appear as a list of options from which you make your selections.

## ▼ To Place Tools Under Security Control

1. In the Security window, click **Actions->Privilege Components->Applications List** to display the Applications dialog.
2. Click **Add** to display the Application Create dialog.
3. In **Application Name**, type the name of the application to be added.  
You can choose either the name of the executable or the commercial name.
4. In **Description**, type a description of the application.
5. (Optional) At the bottom of the dialog, type the description for the Application Task.  
Enter the description for an application task *before* adding the task name to the list. For example, if the task is delete, type: `Delete`.  
Attempting to add a description to an existing task results in a duplicate task name displaying in the list. If you have done this, delete the undescribed task name from the list, leaving only the described version of the task.
6. Still at the bottom of the dialog, enter the application task.  
For example, if the name of the task is “XYZDelete”, then type: `XYZDelete`. If the application developer named the task “XYZ-delete”, then type: `XYZ-delete`. The syntax of the task must match the task name as defined by the application developer.  
Note the Task and Description list display table in the center of the Application Add dialog. This is a display/selection list only. To add a task to this list, enter the task name in the Application Task field below the table, and then click **Add**. The feature name must be the name recognized by the application (for example, the Viewer application task “Move Object” is listed as “MoveObject”).
7. Click **Apply**.
8. Keep adding tool tasks and descriptions until you have added all the features to be controlled.
9. Click **OK** when you are finished.

## ▼ To Place Tools Under Security Control by Duplication

1. In the Security window, click **View->Privilege Components->Applications List** to display the Applications dialog.
2. Select the application you want to use for creating a new one, and click **Duplicate** to display the Application Duplicate dialog.

3. **Enter the application name.**
4. **Change the application's description.**
5. **Make any necessary modifications as follows:**
  - To delete a feature from the list, select it and then click Delete.
  - To modify a feature description or name, first delete the existing feature from the list, and then re-add it with the new description.
6. **Click Apply for each change.**
7. **Click OK when you are finished.**

## 6.5.4 Removing Tools From Security Control

When specific tools are no longer to be used under Solstice EM, you should remove them. Removing tools from Solstice EM control results in deleting the objects which represent these tools in the MIS.

If the tool to be removed is a custom-developed application for which you had specified access controls at the task level, removing it will result in losing task information which may have been time consuming to collect.

You cannot restore a tool that was removed. If the application is a Solstice EM tool, your only option is to reinstall Solstice EM. If the tool to be removed is a custom-developed application, you will need to add it again under Solstice EM as explained in Section 6.5.3 "Placing Tools Under Security Control" on page 6-26.

### ▼ To Remove Tools From Security Control

1. **In the Security window, click Actions->Privilege Components->Applications List to display the Applications dialog.**
2. **Select the tool name from the list and click Delete.**
3. **Click Close.**

## 6.5.5 Granting and Denying Access to Tools and Tasks

After making sure that all applications are under Solstice EM control, you can proceed by specifying the rules that will determine the group access privileges to tools and tool tasks.

You both grant or deny access at the tool level and at the task level at the same time.

### ▼ To Grant and Deny Access to Tools and Tasks

1. In the Security window, click the Privilege Groups tab.
2. Select the group and click Actions->Properties to display the Properties dialog for the selected group.
3. On the Tasks tab, select Task Access by Application and click Edit to display the Edit Task Access By Application dialog.
4. In Application Names, select the application.  
Solstice EM tools are listed by the names of their executables. For example, the Security tool is listed as `em_accessmgr`.
5. Specify the level of access by selecting No Access, Full Access or Specify Tasks.
  - **No Access** – Denies the members of the group any access to the tool. Users will not be able to start and run the tool.
  - **Full Access** – Grants the members of the group complete access to the tool and its tasks. Users will be able to start and run the tool and perform all tasks supported by the tool.
  - **Specify Task** – Grants the members of the group access to the tool but denies and grants access to specific tool tasks. Users will be able to start and run the tool. If, for example, you denied access to the Delete task, users will not be able to perform any delete operations.
6. If you selected Specify Tasks, select the tasks from the list of available tasks.  
The list of tasks available for selection is determined by the selected application.
7. Click Apply to continue, or click Close when you have finished to return to the Properties dialog.
8. Click OK.

The group profile data in the MIB is updated to include the rules that determine access to the tools and tasks.

## 6.5.6 Viewing Tool Access Privileges

When security control is enabled, individual Solstice EM users can view the privileges that control their access to tools and tasks.

### ▼ To View Tool Access Privileges

1. In the Security window, click the Users tab to list the users.
2. Select a user.
3. Click Actions->Properties to display the Properties dialog for the selected user.
4. Click the Tasks tab to view access privileges information.

The information shown is for viewing only and cannot be changed. See Section 6.5.5 “Granting and Denying Access to Tools and Tasks” on page 6-29 for instructions on granting and denying access to tools.

5. Click Cancel to close the dialog.

## 6.5.7 Updating Tool Access Privileges

Organizational or other changes affecting the Solstice EM configuration may require you to update the access controls to tools and tasks.

---

**Note** – To make any changes, you must either be a user who can grant all privileges, or be logged in as root. If necessary, follow the instructions in Section 6.4.7 “Granting Security Privileges” on page 6-17 before making any of the desired changes. You cannot change your own privileges; to do so, log in as root.

---

### ▼ To Update Tool Access Privileges

1. In the Security window, click Actions->Privilege Components->Applications List to display the Applications dialog.
2. Select the application you want to modify and click Edit to display the Applications Edit dialog.
3. Enter your changes.

- To change the tool name or tool task, click in the Description field box and type your changes.
- To delete a task from the list, select it and click Delete.
- To modify a task description or task name, type the new task description or task name.

4. Click OK.

---

## 6.6 Controlling Access to Managed Objects

This section of the guide discusses the tasks you need to accomplish to control user access to managed objects.

The tasks involved in controlling access to managed objects are complex and require a solid understanding of the Solstice EM configuration as well as experience in controlling user access to Solstice EM tools. As such, controlling user access to managed objects should only be considered after you have acquired expertise in controlling user access to Solstice EM tools and tasks.

---

**Note** – Before you carry out any of the tasks outlined in this section of the chapter, you must have accomplished all the required preparatory tasks outlined in Section 6.4 “Preparing for Security Control” on page 6-10 and the tasks outlined in Section 6.5 “Controlling Access to Solstice EM Tools” on page 6-24.

---

### 6.6.1 Implementation Overview

This overview expands the concepts introduced in the chapter overview and discusses them in more detail to successfully set up security controls to managed objects.

This Implementation Overview provides more details about the following:

- Security rules for controlling access to managed objects
- Definition of object sets
- Guidelines for controlling access to managed objects

### 6.6.1.1 Security Rules for Controlling Access to Managed Objects

As explained in Section 6.1 “Overview” on page 6-1, security rules are the foundation for controlling user access.

User access to managed objects can be controlled by creating rules that deny or grant access in the following ways:

- **Deny members of specific groups access to all managed objects** – Use this type of rule when you want to exclude the members of specific groups from accessing all objects in the MIS. When no specific groups are identified, the rule applies to all groups. This rule is sometimes referred to as the *global deny rule*.
- **Deny members of specific groups access to specific managed objects** – Use this type of rule when you want to exclude the members of specific groups from accessing specific objects. For example, members of the “Routers Operators” group should not have any access to managed objects representing bridges which are monitored by members of the “Bridge Operators” group. This rule is sometimes referred to as the *item deny rule*.
- **Grant members of specific groups access to all managed objects** – Use this type of rule when you want to ensure that all members of specific groups have access to all the managed objects. For example, members of the “SysAdmin” group should have access to all managed objects in the MIS. This rule is sometimes referred to as the *global grant rule*.
- **Grant members of specific groups access to specific managed objects** – Use this type of rule when you want to ensure that all members of specific groups have access to specific managed objects. For example, members of the “Boston SysAdmin” group have access to all objects representing the Boston network components in the management information database. This rule is sometimes referred to as the *item grant rule*.
- **Grant and/or deny members of all groups access to managed objects** – When none of the above rules apply, Solstice EM will use this type of rule—sometimes referred to as *the default rule*—to determine user access as follows:
  - To managed objects that are not included in a list of managed objects to which access is either specifically granted or denied.
  - To managed objects where there are no rules that specifically deny or grant user groups access to managed objects.

For example, user Jane Smith is a member of the “Router Operator” group whose access privileges are defined by a rule that grants the group members access to managed objects of the `router` type in the MIS.

In addition, there are *no* rules that specifically deny the group members access to objects of a type other than `router`.

Jane Smith’s access to managed objects that are not of the `router` type, will be determined by the default rule settings.



The logic used for controlling user access is explained in Section 6.1.1 “Understanding the Solstice EM Access Control Model” on page 6-2.

The installation provides you with the following predefined security rules.

**TABLE 6-3** Predefined Security Rules

Rule Name	Description
Full Access	Grants the users of the “Operators” and “Full Access” groups access to all Solstice EM tools and managed objects.
DenyAccessControlObjects Change	Denies the users of the “Operator” group access to change object attributes.
View Only	Grants the users of the “View Only” group access to the following objects named: <ul style="list-style-type: none"><li>• “View Only” which allows the users to view data but not to change it.</li><li>• “Connection” which allows them to connect to a MIS to view data.</li></ul>

The MIS enforces the access control policy as defined by the security rules.

Before you proceed in setting access controls to managed objects, you must have completed all preparatory tasks as explained in “Preparing for Security Control” on page 6-10 and “Controlling Access to Solstice EM Tools” on page 6-24.

## 6.6.1.2 Understanding Object Sets

An *object set* is a group of managed objects protected by the same access rule. Object sets identify managed objects within the security domain. An object set can be one or more of the following:

- Any managed object type or class
- One or more specific instances of an object.
- All objects below that object in the Management Information Tree (MIT)
- One or more subtrees below an object, including or not including the object itself
- One or more attributes of an object

The following are some examples of object sets:

- All Solstice EM log files, except AlarmLog
- topoNodes contained in the 129.146.0.0 network
- “Set” operations on objects of the type “router”

A default Solstice EM installation provides the following predefined object sets.

**TABLE 6-4** Predefined Object Sets

Name of Object Set	Description
DenyAccessControl ObjectsChange	Pointer for the object /em-name="accessControlContainer"
Connection	Pointer for the instance of the object subsystemid='EM-MIS' which is of type emApplicationinstance
View Only	Pointer to the root directory of the Management Information Tree (MIT)

See Section 6.8.1.4 “More About Object Sets” on page 6-58 for more information.

## 6.6.2 Getting Ready to Control Access to Managed Objects

The tasks in this section of the chapter need to be carried out if you want to control user access to managed objects. The following outline is a high-level overview of the tasks to be performed.

1. Make sure you have accomplished all preparatory tasks.  
See Section 6.4.3 “Getting Ready for Security Control” on page 6-12.
2. If you are not already controlling user access to Solstice EM tools, define access controls to Solstice EM tools.  
See Section 6.5 “Controlling Access to Solstice EM Tools” on page 6-24.
3. Define the object sets.  
Follow the instructions in Section 6.6.3 “Defining Object Sets” on page 6-35.
4. Define the security rules for the object sets.  
Follow the instructions in Section 6.6.4 “Defining Security Rules for Object Sets” on page 6-37.
5. Assign the objects sets and rules to the appropriate groups.  
Follow the instructions in Section 6.6.5 “Assigning Objects and Security Rules to Groups” on page 6-46.

## 6.6.3 Defining Object Sets

---

**Note** – To define object sets, you must be logged in as root or a user with “grant all” privileges.

---

To complete the tasks pertaining to specifying object sets, you will need to have the following information on hand:

- The object class of the objects
- The name of the object instance in the MIS
- The access scope in the topology
- Target filters
- Available CMIS filter(s)
- The operations that can be performed on the objects

Using the graphical user interface, you add sets of objects in one of the following ways:

- Using the Object Set Create dialog
- Duplicating an existing definition

### ▼ To Define Object Sets

1. **In the Security window, click Actions->Privilege Components->Object Sets to display the Object Sets dialog.**
2. **Click Create to display the Object Set Create dialog.**  
The Object Sets Create dialog is organized in the following two groups: Objects and Operations.
3. **In Object Set Name, enter a name for the object set as you want to see it listed in the Object Sets dialog.**
4. **Specify the types of objects to be included in the object set as follows:**
  - Click Types, select an object type from the list, click Add, and then click Close.
  - Alternatively, type in the name of the object type in the text field next to the Types button.
5. **Specify object instances to be included in the object set as follows:**
  - Click Instances, select an object instance from the list, click Add, and then click Close.
  - Alternatively, type in the name of the object instance in the text field next to the Instances button.

The Object Instances do not bear any relationship to the Object Types.

#### **6. Specify the Scope (Base Object).**

Click the scope selection box to display the available options. If you select either Base to the Nth Level or Nth Level, you must also specify the level in the number field next to the selection list. Use the up and down arrows to select the correct level.

#### **7. (Optional) Define a CMIS filter by clicking Filter to display the CMIS Filter dialog.**

Using the CMIS Filter dialog, you can create and save a new CMIS filter definition, or load an existing filter. See CMIS Scoping and Filtering in the *Developing Applications* guide for more information.

#### **8. On the Operations Group tab, select either All Operations, or select the operations individually.**

#### **9. (Optional) Create a CMIS filter by clicking Event Discriminator to display the CMIS Filter dialog.**

#### **10. Click OK.**

### **▼ To Define Object Sets by Duplication**

#### **1. In the Security window, click Actions->Privilege Components->Object Sets to display the Object Sets dialog.**

#### **2. Select an object set in the list and click Duplicate to display the Object Sets Duplicate dialog.**

#### **3. Enter the name of the new object set.**

#### **4. Make any other changes as necessary.**

#### **5. Click OK.**

### **▼ To Create CMIS Filters**

#### **1. In the Security window, click Object->Object Sets to display the Object Sets [Create] dialog.**

See CMIS Scoping and Filtering in the *Developing Applications* guide for more information.

#### **2. Click Filter to display the CMIS Filter dialog.**

#### **3. Enter the filter definition as follows:**

##### **a. Click Item to display the CMIS Filter Item dialog.**

- b. Select the Operator for the item.
  - c. Type the Attribute ID.
  - d. Click Search to display the CMIS Filter Item Search dialog.
  - e. Type the Attribute Value.
  - f. Add the item to the CMIS filter definition.
  - g. Click OK to add the item to the filter definition and return to the CMIS Filter dialog.
- 4. (Optional) Click Save to name and save the filter.
  - 5. Click OK.

## 6.6.4 Defining Security Rules for Object Sets

When you do not want to give all users the same level of access to managed objects, you can use the predefined rules and add your own. With security rules you can refine user access to the object level and exclude specific users from accessing designated objects.

---

**Note** – Individual users derive their privileges from the group to which they belong. Security rules only apply to users belonging to user groups. Users who do not belong to any groups (an unlikely event) derive their access privileges from the default rule.

---

As explained in Section 6.6.1.1 “Security Rules for Controlling Access to Managed Objects” on page 6-32 you can control user access in the following ways.

Using the Object Access Rule dialog:

- Deny groups access to all sets of objects.
- Deny groups access to specific objects.
- Grant groups access to all sets of objects.
- Deny groups access to specific sets of objects.

Using the Defaults dialog specify access defaults applicable to all users when no other access rule prevails.

Detailed steps for creating these security rules are provided in the following sections.

If necessary, see Section 6.1.1 “Understanding the Solstice EM Access Control Model” on page 6-2 for information about security rules and the logic used for enforcing them.

## ▼ To Deny Groups Access to All Sets of Objects

This type of rule is also referred to as the *global deny rule*.

1. **In the Security window, click Actions->Privilege Components->Object Access Rules to display the Object Access Rule dialog.**
2. **Click Create to display the Object Access Rule Create dialog.**
3. **In Rule Name, type the name of the custom access rule.**
4. **In Privilege Groups Using Rule, click Edit List to display the Edit Privilege Groups List dialog.**
5. **Select one, several, or all user groups listed in All Groups and click Add.**
6. **Click OK to return to the Rule Create dialog.**
7. **Do not specify any sets of objects.**
8. **Select one of the three Deny options.**
9. **When finished creating rules, click OK, otherwise click Apply.**



**FIGURE 6-2** Rule Denying Group Access to All Objects

FIGURE 6-2 Illustrates a rule that denies the members of the groups “Group\_A” and “Group\_B” access to all objects. When users attempt to access the objects, an informational message will be displayed.

## ▼ To Deny Groups Access to Specific Sets of Objects

This type of rule is also referred to as the *item deny rule*.

1. In the Security window, click Actions->Privilege Components->Object Access Rules to display the Object Access Rule dialog.
2. Click Create to display the Object Access Rule Create dialog.
3. In Rule Name, type the name of the custom access rule.
4. In Privilege Groups Using Rule, click Edit Group List to display the Edit Privilege Groups List dialog.
5. Select one, several, or all user groups listed in All Groups and click Add.

6. Click OK to return to the Rule Create dialog.
7. In Objects Sets Affected By Rule, click Edit List to display the Edit Object Sets List dialog.
8. In All Object Sets, select the objects to which access is to be denied and click Add.
9. Click OK to return to the Rule Create dialog.
10. Select one of the three Deny options.
11. When finished creating rules, click OK, otherwise click Apply.



**FIGURE 6-3** Rule Denying Group Access to Specific Objects

FIGURE 6-3 Illustrates a rule that denies the members of the groups “Group\_A” and “Group\_B” access to the objects “Object\_A” and “Object\_B”. When attempting to access these two objects, no informational message will be displayed.



## ▼ To Grant Groups Access to All Sets of Objects

This type of rule is sometimes referred to as the *global grant rule*.

1. In the Security window, click Actions->Privilege Components->Object Access Rules to display the Object Access Rule dialog.
2. Click Create to display the Object Access Rule Create dialog.
3. In Rule Name, enter the name of the custom access rule.
4. In Privilege Groups Using Rule, click Edit Group List to display the Edit Privilege Groups List dialog.
5. Select one, several, or all user groups listed in All Groups and click Add.
6. Click OK to return to the Rule Create dialog.
7. In Objects Sets Affected By Rule, click Edit List to display the Edit Object Sets List dialog.
8. Click Select All and then click Add.
9. Click OK to return to the Rule Create dialog.
10. Select Allow.
11. When finished creating rules, click OK, otherwise click Apply.



**FIGURE 6-4** Rule Granting Access to All Objects

FIGURE 6-4 Illustrates a rule that grants the members of the groups “Group\_A” and “Group\_B” access to all objects.

## ▼ To Grant Groups Access to Specific Sets of Objects

This type of rule is sometimes referred to as the *item grant rule*.

1. In the Security window, click Actions->Privilege Components->Object Access Rules to display the Object Access Rule dialog.
2. Click Create to display the Object Access Rule Create dialog.
3. In Rule Name, type the name of the custom access rule.
4. In Privilege Groups Using Rule, click Edit Group List to display the Edit Privilege Groups List dialog.
5. Select one, several, or all user groups listed in All Groups and click Add.

6. Click OK to return to the Rule Create dialog.
7. Click Edit Target List to display the Edit Targets List dialog.
8. In All Object Sets, select the objects to which access is to be granted and click Add.
9. Click OK to return to the Rule Create dialog.
10. Select Allow.
11. When finished creating rules, click OK, otherwise click Apply.



**FIGURE 6-5** Rule Granting Access to Specific Objects

FIGURE 6-5 Illustrates a rule that grants the members of the groups “Group\_A” and “Group\_B” access to the objects “Object\_A” and “Object\_B”.

## ▼ To Create Security Rules by Duplication

1. In the Security window, click **Actions->Privilege Components->Object Access Rules** to display the **Object Access Rules** dialog.
2. Select the rule to duplicate and click **Duplicate** to display the **Object Access Rule Duplicate** dialog.
3. In **Name**, type the name of the new custom access rule.
4. (Optional) Enter your modifications.
5. Click **OK**.

## ▼ To Specify Default User Access

This type of rule is sometimes referred to as the *default rule*.

1. In the Security window, click **Actions->Security Defaults** to display the **Defaults** dialog.
2. Verify that **Security** is turned on.
3. Define the access defaults for each operation type.
4. Choose the desired access level for the logging of security and audit events.
5. If users will access remote MIS servers, add the names of these servers and click **Add**.
6. Click **OK**.



**FIGURE 6-6** Default Rule

FIGURE 6-6 Illustrates the default rule that applies to groups in the absence of any other security rules, and to users who do not belong to any groups.

As shown, users are allowed to do the following:

- From the Action setting – Request an agent to invoke a specific behavior that is supported by the managed object that receives the request.
- From the Get setting – Request information from an agent.
- From the Filter setting – Request an agent to perform a test on a managed object before carrying out a request.
- From the Events setting – To request an agent to send event report messages.
- From the Multiple Object Selection – Request an agent to send a single request to several managed objects.

- Users logging in from the `dugout` and `zirconium` systems can, for example, connect to the server on which the MIS resides.

Users are not allowed to do the following:

- From the Create setting – Request an agent to create a managed object.
- From the Delete setting – Request an agent to delete one or more managed objects.
- From the Set setting – Request an agent to change attribute values of a managed object.
- From the Security Logging setting – Request an agent to generate service or mechanism violation notifications or events to allow the logging of all security violations.
- From the Audit Logging setting – Request an agent to generate Service Report notifications or events to log all authorized access to management information at the object level.

## 6.6.5 Assigning Objects and Security Rules to Groups

After you have defined object sets and created security rules, you are ready to assign these objects and rules to the appropriate user groups.

### ▼ To Assign Objects and Security Rules to Groups

1. **In the Security window, click the Privilege Groups tab.**
2. **Select the group and click Actions->Properties to display the Properties dialog for the selected group.**
3. **On the Object Access Rules tab, specify the group's security rules as follows:**  
From the All Rules list, select one, several or all security rules that will apply to the group and its members, and then click Add.
4. **On the Database Objects tab, specify the managed objects accessible to the group folder as follows:**  
From the All Database Object list, select one, several or all database objects, and then click Add. The selected objects are listed in Group Database Objects on the right.
5. **Click OK.**
6. **Repeat steps 2 to 5 for every group until you are finished.**

The group profiles in the MIS are automatically updated with the object sets and security rules.

## 6.6.6 Viewing Access Privileges to Managed Objects

Individual Solstice EM users can view the privileges that control their access to managed objects.

Users whose access to managed objects is controlled view their privileges as follows:

- On the Access Rules tab of the Properties dialog, when rules that deny or grant access to managed objects are put in place.
- In the Defaults dialog, when rules that deny or grant access to managed objects have not been put in place, or for any managed objects not governed by any grant or deny rules.

Users who do not belong to any groups view their access privileges to managed objects in the Defaults dialog.

### ▼ To View Privileges to Managed Objects

1. In the Security window, click the Groups tab.
2. Select the user or the group whose properties are to be viewed.
3. Click Actions->Properties to display the Properties dialog for the selected group.
4. Click the Object Access Rules tab to view the list of rules that control the group's access to managed objects.
5. Click the Database Object tab to view the managed objects subject to access control.
6. Click OK if changes were made, otherwise click Cancel.

### ▼ To View Privileges From the Default Rule

1. In the Security window, click View->Security Defaults to display the Default dialog.
2. Click Cancel when you are finished.

## 6.6.7 Maintaining Object Sets

Maintaining object sets includes the following activities:

- Updating object sets
- Deleting object sets

The dialogs for creating and updating object sets are identical, except for their titles. As such, the procedures for creating and modifying objects are very similar.



---

**Caution** – Security does not display warning messages when you delete object sets. Deleting object sets removes the instances representing the object sets from the MIS immediately and irrevocably.

---

To make any changes you must be a user who can grant all privileges, or be logged in as root.

### ▼ To Update Object Sets

1. In the Security window, click **Actions->Privilege Components->Object Sets** to display the Object Sets dialog.
2. Select an object set in the list and click **Edit** to display the Object Sets (Edit) dialog.
3. Enter your changes.
4. Click **OK**.

### ▼ To Delete Object Sets

1. In the Security window, click **Actions->Privilege Components->Object Sets** to display the Object Sets dialog.
2. Continue as follows:
  - To delete an object set listed in the Object Sets dialog, select it and click **Delete**.
  - To delete object types and instances associated with a selected object set, click **Edit** to display the Target Edit dialog.



3. **Working in the Object Set Edit dialog, continue as follows:**
  - To delete an object type, select it in the Objects list and click Delete.
  - To delete an object instance, select it in the Instances list and click Delete.
4. **Click OK.**

## 6.6.8 Maintaining Object Privileges

Maintaining privileges for managed objects includes the following activities:

- Updating security rules
- Deleting security rules

The dialogs for creating and updating privileges are identical, except for their titles. As such, the procedures for creating and modifying custom security rules are very similar.

### ▼ To Update Object Privileges

1. **In the Security window, click Actions->Privilege Components->Object Access Rules to display the Rules dialog.**
2. **Select a rule from the list and click Edit to display the Object Access Rule Edit dialog.**
3. **Make the necessary changes.**
4. **Click OK.**

### ▼ To Delete Object Privileges

1. **In the Security window, click Actions->Privilege Components->Object Access Rules to display the Rules dialog.**
2. **Select the rule to delete and click Delete.**
3. **Click Close.**

## 6.6.9 Importing/Exporting Access Control Objects

Use previously configured access control files and parameters for the following:

- Importing object files
- Exporting object files

### ▼ To Import Access Control Objects

1. In the Security Window, click File->Import to display the Import dialog.
2. Enter the filename to import.
3. Click OK.

### ▼ To Export Access Control Objects

1. From the Security Window, click File->Export to display the Export dialog.
2. Choose from the following export options:
  - All Access Control Objects
  - Users, Groups, Trusted Hosts and Application List
  - Targets, Rules and Security Defaults
3. Enter a filename in the field to export a file.
4. Click OK.

---

## 6.7 Using the em\_accesscmd Utility

A number of tasks pertaining to access control can be performed from the command line. This is particularly useful when you want to automate security tasks by loading existing files.

Solstice EM provides the `em_accesscmd` utility for the purpose of performing the most important security tasks.

Instructions for the following tasks are provided in this section:

- Creating user profiles
- Creating group profiles
- Assigning users to groups
- Deleting user profiles
- Deleting group profiles
- Adding applications under Solstice EM control
- Assigning user access to application features
- Exporting files

For a complete list of `em_accesscmd` commands see Section 6.8.1.3 “The `em_accesscmd` Commands” on page 6-56

## ▼ To Create User Profiles

1. **Start the `em_accesscmd` utility by executing the following command at a system prompt:**

```
em_accesscmd [-help] [-host hostname]
```

2. **Enter the following command:**

```
createUser login_name "full_name"
```

For example: `createUser jdoe "Jane Doe"`

## ▼ To Create Group Profiles

1. **Start the `em_accesscmd` utility by executing the following command:**

```
em_accesscmd [-help] [-host hostname]
```

2. **Create the user group by entering the following command:**

```
createGroup group_name "group_description"
```

For example: `createGroup OmegaSysAdmins "System Administrations of host omega"`

## ▼ To Assign Users to Other Groups

1. **Start the `em_accesscmd` utility by executing the following command:**

```
em_accesscmd [-help] [-host hostname]
```

2. **Add the user to another group by executing the following command:**

```
addMembers "group_name" login_name
```

For example, to add Jane Doe to the Operators group, enter: `addMembers "Operators" jdoe`

3. **If necessary, remove the user from another user group by executing the following command:**

```
removeMembers "group_name" login_name
```

For example: `removeMembers "Operators" jdoe`

## ▼ To Delete User Profiles

1. **Start the `em_accesscmd` utility by executing the following command:**

```
em_accesscmd [-help] [-host hostname]
```

2. **Delete the user by executing the following command:**

```
deleteUser login_name
```

For example: `deleteUser jdoe`

## ▼ To Delete Group Profiles

1. **Start the `em_accesscmd` utility by executing the following command:**

```
em_accesscmd [-help] [-host hostname]
```

See "The `em_accessmgr` Command" on page 6-55 for more information.

2. **Delete the privilege group by executing the following command:**

```
deleteGroup "group_name"
```

For example: `deleteGroup "Boston_SysAdmins"`

## ▼ To Place Tools under Solstice EM Control

1. **Start the `em_accesscmd` utility by executing the following command from a system prompt:**

```
em_accesscmd [-help] [-host hostname]
```

2. **Add the application by executing the following command from a system prompt:**

```
createApplication "app_name" "app_description"
```

For example: `createApplication "Wizbang" "Monitor Wiz"`

## ▼ To Specify Tool Tasks

1. **Start the `em_accesscmd` utility by executing the following command from a system prompt:**

```
em_accesscmd [-help] [-host hostname]
```

2. **Specify a tool task by executing the following command:**

```
createFeature "app_name" "task_name" "task_description"
```

For example: `createFeature "Wizbang" "feature_add" "Add Wizbang objects"`

## ▼ To Assign Tool Tasks to a Group

1. **Start the `em_accesscmd` utility by executing the following command from a system prompt:**

```
#em_accesscmd [-help] [-host hostname]
```

2. **Assign a tool task to a group by executing the following command:**

```
assignAppFeatures "privilege_group_name" "app_name" ["task_name"]  
"<task_description>"
```

For example: `assignAppFeatures "BostonAdmins" "Wizbang" "feature_add" "Add Wizbang objects to Boston network views"`

## ▼ To get a list of Authorized Tasks for a User

1. **Start the `em_accesscmd` utility by executing the following command from a system prompt:**

```
em_accesscmd [-help] [-host hostname]
```

2. **Get the list by executing the following command from a system prompt:**

```
getAuthFeatures login_name [ "app_name" + ] ]
```

For example: `getAuthFeatures jdoe "Wizbang"`

## ▼ To Get a List of Authorized Tools for a User

1. **Start the `em_accesscmd` utility by executing the following command from a system prompt:**

```
em_accesscmd [-help] [-host hostname]
```

2. **Get the list by executing the following command from a system prompt:**

```
getAuthApps [login_name]
```

For example: `getAuthApps jdoe`

## ▼ To Export Access Control Objects

1. **In the Administration window, click Security to start the Security tool.**
2. **Click File->Export to use the Export dialog.**
3. **Select from the following options:**
  - All Access Control Objects
  - Users, Groups, Trusted Hosts and Application List
  - Targets, Rules and Security Defaults
4. **Enter a file name to export.**
5. **Click OK.**

---

## 6.8 Reference

This section provides reference information about command-line options for security operations.

For detailed information about dialogs, menus, and other user interface elements, refer to the Solstice EM Online Help. To access Online Help, click the Help button on any dialog box or select options from the Help menu located in the upper right corner of each Solstice EM tool window.

### 6.8.1 Command-Line Options

Reference information is available for the following:

- Section 6.8.1.1 “The `em_accessmgr` Command” on page 6-55
- Section 6.8.1.2 “The `em_accesscmd` Utility” on page 6-55

### 6.8.1.1 The em\_accessmgr Command

The `em_accessmgr` command is the executable to start the Security tool.

```
em_accessmgr [-help] [-host hostname]
```

For example: `em_accessmgr -host omega`. This command connects to the MIS on the server `omega` and starts the Security application.

**TABLE 6-5** Security Command Options

Option	Description
<code>-help</code>	Print the list of options with descriptions for the <code>em_accessmgr</code> command.
<code>-host</code>	Specify the connection to a remote MIS.
<i>hostname</i>	Specifies the name of the MIS server.

### 6.8.1.2 The em\_accesscmd Utility

The `em_accesscmd` utility is the command-line interface for creating security access profiles for users, privilege groups, and tools. You enter this command and its parameters to create users, user groups, assign users to user groups, add applications, specify access controls for tool tasks, and so on.

When adding third-party applications to Solstice EM, you first must use `em_accesscmd` to define the application in the MIS. Once the application is defined, you can use either `em_accesscmd` or the Security tool to create access control objects and assign user access privileges.

The `em_accesscmd` command uses the following syntax:

```
em_accesscmd [-help] [-host hostname] [-import filename]  
[-exportall/-exportapp/-export filename].
```

**TABLE 6-6** Security `em_accesscmd` Parameters

Option	Description
<code>-host <i>hostname</i></code>	Specifies the <code>&lt;hostname&gt;</code> of a remote MIS.

**TABLE 6-6** Security em\_accesscmd Parameters (*Continued*)

Option	Description
-help	Prints a descriptive list of options for the em_accesscmd command.
-import <i>filename</i>	Imports a file containing a set of commands to be executed by the Access Control tool. If you start the tool without using the -import option, you must create access control objects and assign privileges from the command line.
-exportall <i>filename</i>	Exports a file containing all Access Control object.
-exportapps <i>filename</i>	Exports application level objects.
-exportobj <i>filename</i>	Exports object level objects.

### 6.8.1.3 The em\_accesscmd Commands

After you start Security from the command line, you can use any of the commands documented in the following table. You can call these commands either from a file to be imported with the -import option, or directly on the em\_accesscmd command line.

Please note the following:

- No quotes are required for the *login\_name* option or the :ALL option. Quotes are required for all other options.
- The + character following an option means you can enter multiple instances of that option. The delimiter is a space.

**TABLE 6-7** em\_accesscmd Utility Commands

Commands	Description
createUser <i>login_name</i> " <i>full_name</i> "	Creates a user.
createGroup " <i>group_name</i> " " <i>description</i> "	Creates a group.
createApplication " <i>app_name</i> " " <i>description</i> "	Adds a tool. You cannot control access privileges for a tool unless it has been created.
createFeature " <i>app_name</i> " " <i>feature_name</i> " " <i>description</i> "	Creates a tool task.
addMembers " <i>group_name</i> " <i>login_name</i> +	Adds users to a group. You can specify one or more login names separated by spaces. <i>Do not</i> use quotes to delineate the login names.



**TABLE 6-7** em\_accesscmd Utility Commands (*Continued*)

Commands	Description
assignApps "group_name" [ :ALL   "app_name"+ ]	Defines tool access for a group. If you specify :ALL, then access is granted to all tools. Otherwise, you must specify one or more tools. Access is granted implicitly to all tasks (if any) of the specified tools.
assignAppFeatures "group_name" "app_name" [ "feature_name" ]+	Defines access to tool tasks for a group. The <i>feature_name</i> option defaults to all tool tasks if none is entered.
deleteUser login_name	Deletes a user. You must first remove the user from all groups to which the user belongs.
deleteGroup "group_name"	Deletes a group. This command does not delete the users belonging to the group.
deleteApplication "app_name"	Deletes a tool. You cannot delete a tool unless you first delete all tool tasks (if any).
deleteFeature "app_name" "feature_name"	Deletes a tool task.
removeMembers "group_name" login_name+	Removes users from a group. The users are not deleted.
deassignApps "group_name" [ :ALL   "app_name"+ ]	Denies a group access to a tool. If you specify :ALL, then group access will be denied for all tools. Otherwise, you must specify one or more tools. Access is denied to the group for all tool tasks (if any) of deassigned tools.

**TABLE 6-7** em\_accesscmd Utility Commands (*Continued*)

Commands	Description
deassignAppFeatures "group_name" "app_name" [ "feature_name" ] +	De assigns access to specified tool tasks for a group. The <i>feature_name</i> option defaults to all tool tasks if none are entered.
getAuthFeatures [ login_name [ "app_name" + ] ]	Gets the list of authorized tool tasks for the given user and the given tools.  If you do not specify a login, then the user currently logged in is assumed and you can not specify any tools. If you specify a login name, then you can specify any number of tool names. If you do not specify any tools, then the authorized tool tasks for all tools are listed.
getAuthApps [ login_name ]	Gets the list of authorized tools for the specified user. If no login name is specified, then the current user is assumed.

### 6.8.1.4 More About Object Sets

The following table provides detailed descriptions about object sets.

**TABLE 6-8** Criteria Defining Object Sets

Criteria	Description
Object Classes	Defines a specific type of managed object. GDMO object types are identified in the GDMO files shipped with the product. For a list of object types, see the Developing Applications guide.
Object Instances	The representations in the MIS of a specific object in the Management Information Tree. For example, the Object Type <i>router</i> defines what elements constitute an object of type <i>router</i> as recognized by the MIS. Suppose there exists a router called <i>Router_A</i> , and <i>Router_A</i> is declared to be of Object Type <i>router</i> , and thereby described to and registered in the MIS. The abstract representation of <i>Router_A</i> in the MIS is the Object Instance of that particular physical object. Objects instances are also objects in the MIS.
Scope	Specifies the level within the topology to which an object operation can apply.

**TABLE 6-8** Criteria Defining Object Sets *(Continued)*

Criteria	Description
(Object) Filter	Allows you to further refine the criteria used to evaluate to a set of objects to which access will be controlled. For example, after enumerating the list of Object Types in the Object Set Create dialog, you can use a CMIS filter to exclude objects with a given attribute value. The remaining objects will comprise the object set to which access is controlled. For example, if you choose the object type to be <code>toponode</code> , then you can use a filter to specify that only those <code>toponodes</code> with IDs greater than a certain value are to be protected.
Operations (Get, Set, Action, Create, Delete, Filter, and Multiple Object Selection)	Actions you can perform against the target currently being defined. Multiple Object Selection on an object means that the object is being selected as a result of some scoped operation. Get includes all variations of GET, including Multiple Object Selection and Filter.
Event Discriminator	Support CMIS filtering for access control, as well as for the Solstice EM components and applications PMI and the Log Manager Application. You use CMIS filters to define event discriminators. A CMIS filter consists of an assertion about the presence or values of attributes in objects being tested. If a CMIS filter contains more than one assertion, the assertions can be grouped using the AND, OR, and NOT operators. Filters can be complex, because you can nest filters within filters.

6.8.2

More About the Solstice EM-config Configuration File

When turning on security for the purpose of controlling user access, the assignments for the access control variables in the `#EM_HOME/build/acct/EM-config` configuration file needs to be edited. The following table describes the variables.

TABLE 6-9 Security Control Variables

Variable Name	Description	Enable	Disable
EM_ACCESS_PASSWORD_CONTROL	A TRUE value will prompt the users to enter their login password.	TRUE	FALSE
EM_ACCESS_CONNECTION_CONTROL	A TRUE value will grant the non-privileged users access to the MIS server.	TRUE	FALSE
EM_ACCESS_BACKWARD_COMPATIBILITY	A TRUE value allows users to connect to an Solstice EM MIS with applications linked with Solstice EM libraries. You must be running the applications as root on a trusted host.	TRUE	FALSE

You can also modify the access control variables in the `/var/opt/SUNWconn/em/conf/EM-config` configuration file. When you run `em_services -r`, your changes will not be saved, and the access control settings revert to the assignments in `$EM_HOME/build/acct/EM-config`.

See the *Developing C++ Applications* guide for details concerning this configuration file.

# Automating Nerve Center Requests

---

Automating a Solstice Enterprise Manager™ (Solstice EM) network involves precise interworking of pre-programmed Nerve Center request templates, autoManagement objects, and an autoManagement daemon, `em_autod`. Nerve Center requests are inquiries programmed into Nerve Center request templates and issued to agents for data about the status of the network components that the agents support.

Through automation of Nerve Center requests, you can manage any network component configured with an agent, regardless of protocol, without having to manually check conditions. For example, you can launch a Nerve Center request that probes to determine whether a host is up and running or down. See Section 7.6 “Reference” on page 7-13 for sample requests or refer to any of the following tasks.

This chapter comprises the following topics:

- Section 7.2 “Getting Started” on page 7-8
- Section 7.3 “Creating autoManagement Objects” on page 7-8
- Section 7.4 “Manually Starting and Stopping Requests” on page 7-11

---

## 7.1 Overview

By setting up predefined and customizable Nerve Center request templates, autoManagement objects, and the autoManagement daemon, `em_autod`, you can automate the management of components that exist in the topology of your network.

### 7.1.1 About Requests for Network Conditions

The Nerve Center is a module of the MIS that detects the current conditions of a type of object and responds by taking appropriate actions. Solstice EM provides scripts that, when run, send requests to the Nerve Center. The Nerve Center responds, and the ensuing chain of events results in the automation of network management tasks.

## 7.1.2 About Nerve Center Request Templates

The scripts that enable the automation of Solstice EM network management tasks are referred to as Nerve Center request templates, or request templates for short. You can customize the templates using Advanced Requests, accessible from the Tools menu of Network Views, or from the command line. For information about customizing default request templates, see the *Customizing Guide*.

Request templates comprise a finite number of states and transitions between states. States represent the anticipated conditions of a network component, as indicated by information available to the request. Specifying transitions in request templates involves providing conditions that define when a transition is likely to occur.

For example, if you want to determine whether a device is up and running or down, the states up and down are included in the request template as possible states. Request templates also indicate how a transition from one state to another should occur following an evaluation of the conditions of the network component. In this example, the request template could contain a transition to indicate the transition from the up state to the down state, or from the down state to the up state, or both.

## 7.1.3 About autoManagement Objects

Solstice EM provides autoManagement objects, which use preset criteria to determine the status of specific network components and to indicate the Nerve Center request templates to be launched against each instance of a type of network component. AutoManagement objects are represented online in the Request Controllers tool by the template name and type of object that they specify. Like request templates, the autoManagement object also is associated with a script, called an entry file, which defines its characteristics. Solstice EM provides a set of default autoManagement objects that you can customize using the Request Controllers tool.

### 7.1.3.1 Default autoManagement Objects

During installation, you have the opportunity to start the two default autoManagement objects, described in the following table.

**TABLE 7-1** Default autoManagement Objects Available During Installation

autoManagement Object	Description
admin_oper_status_up. autoentry	Correlates the RPC_MibII_InterfaceStatus request template with the type of object, or TopoType, router.  Enables you to monitor the status of router device interfaces.
device_reachable_ping. autoentry	Correlates the AutoManageDecayReachablePing request template with the TopoType host.  Checks hosts in the topology to ensure that they are reachable by the Ping command.

**Note** – The autoManagement objects listed in the preceding table are specified by their entry file name, which uses the .autoentry extension. This extension is optional. No extension is required for an entry file. For information about creating new entry files, see Section 7.3.1 “Creating Multiple autoManagement Objects” on page 7-10.

If the two autoManagement objects described above are selected during installation, they are started automatically by the installation procedure after Solstice EM is started. If Solstice EM is stopped, you can restart the autoManagement objects if they were previously running when you bring up the MIS again using the command, `em_services`, without the `-i` or `-r` options. If you do not start the two default autoManagement objects during installation, you can manually start them later using the Request Controllers tool. For additional information about how to manually start requests, see Section 7.4 “Manually Starting and Stopping Requests” on page 7-11. For information about the `em_services` command, see Chapter 2 of the *MIS Guide*.

Solstice EM also provides another default autoManagement object, `link_up.autoentry`, which enables you to monitor the status of links, the connections between network topology objects, such as hosts and routers, networks and subnetworks. The `link_up.autoentry` object is not available during installation, but can be started manually once Solstice EM is running.

### 7.1.3.2 Custom autoManagement Objects

You can customize your own autoManagement objects as well as the Nerve Center request templates they use. For more information about customizing request templates, see the *Customizing Guide*.

### 7.1.3.3 When to Create an autoManagement Object

Create an autoManagement object when you want to automatically launch a Nerve Center request against objects of a given type. However, autoManagement objects are not mandatory if you want to run a Nerve Center request manually, on an ad-hoc basis.

The autoManagement object identifies a particular object type and correlates the object type with a specific Nerve Center request template. This correlation ensures that when a new object of the specified type is created in the topology, the autoManagement daemon automatically launches the associated Nerve Center request template against the new object. The same request template is also launched separately against every object of the specified type.

For example, if an autoManagement object specifies an autoEntryTopoType as “host,” then, as long as the autoManagement object is started (its administrativeState value displays as `unlocked` in Request Controllers), the autoManagement daemon causes a Nerve Center request to be launched against each new or pre-existing host object.

An exception to this rule exists in the case of the `device_reachable_ping.autoentry` autoManagement object, which issues only one request, against root, rather than against every host object in the topology. The autoManagement daemon then issues an `snmEventRequest` against every host in the topology to determine whether or not a network component can be reached by the ping command. The collected responses from each host are received by the single Nerve Center request. Because only one request is issued, the load is reduced on the MIS components that handle Nerve Center requests, contributing to improved MIS performance. For detailed information about the `device_reachable_ping.autoentry` object, see Section 7.6.3.3 “Entry Launching Ping-Reachable Template” on page 7-17.



### 7.1.3.4 Criteria Used by autoManagement Objects

You can set up autoManagement objects from the Request Controllers tool or from the command line. By setting up specific criteria, you set an autoManagement object to recognize specific network components from which to request status data. The following table lists and describes some criteria used in typical autoManagement objects.

**TABLE 7-2** Criteria for Automatic Management

Criterion	Description
Identity of the autoManagement object	Distinguished name or unique identifier of the autoManagement object you create. A unique identifier is required.
Template to use	Specifies the name of the template to be launched against the topology object. This template must exist in the system. Default templates are provided in the Advanced Requests tool, available in Network Views by clicking Tools -> Advanced Requests.
Type of object	Specifies the topology type of network components against which you want to launch requests for status. The type of object specified must be a valid Solstice EM definition, such as Device or Container. In Solstice EM, you can find out an object's type in Network Views by clicking Object -> Properties. The type is displayed in the Object Properties dialog.
Scope of the network request	Specifies whether or not requests are launched against all topology nodes. Possible values of this attribute are local and all. Local specifies that the request is launched only against topology nodes of the local MIS. All specifies that the request is launched against topology nodes in all available MISs.
Specific keywords	Specifies a value that must match a keyword contained in the ObjectInstance of the topoNodeMOSet. If the keyword matches, a request is launched. A keyword specification of none, the default value, causes requests to be launched without checking the topoNodeMOSet, resulting in simple autoManagement entries.

The following two criteria are backward-compatible SunNet Manager (SNM) characteristics used in creating an autoManagement object that launches requests against SNM proxy agents.

Schema	Specifies a concatenation of the SNM agent name and the group in the schema that the agent supports.
Event Request information	Specifies SNM-specific event request information, the snmEventRequest attribute, entered in the same format used for the RCL function snmEventRequest when building a Nerve Center request template. For more information, see chapter 20 in the <i>Customizing Guide</i> covering RCL functions.

## 7.1.4 About the autoManagement Daemon

The autoManagement daemon, `em_autod`, is responsible for the following tasks:

- Monitoring the creation and deletion of objects in the MIS topology
- Starting Nerve Center requests by launching request templates when new managed objects are created in the topology
- Stopping Nerve Center requests when objects are deleted from the topology

To automatically start requests for managing network components, the autoManagement daemon must be running. For a more detailed description of what the autoManagement daemon is and how it works, see Section 7.6.2 “AutoManagement Daemon” on page 7-14.

## 7.1.5 Process of Automatic Management

From a high-level perspective, the overall process of automatically managing a network component by automating Nerve Center requests can be delineated as follows:

### Your Steps—Preliminary Tasks

Before automatic management begins, you complete the following tasks.

1. In the Design Advanced Requests tool, you use or customize default Nerve Center templates or write new Nerve Center templates as needed.
2. In the Request Controllers tool, you create an autoManagement object that specifies a Nerve Center request template and the type of network component to which to send a request. If you prefer, you can create an autoManagement object from the command line in an entry file rather than use Request Controllers.

**Example**—You create an autoManagement object called `SysUpOrDown` that specifies the default Nerve Center request template `IsSnmpSystemUp` and the object type `host`. The `IsSnmpSystemUp` request template causes the Nerve Center to inquire of an agent whether the host it supports is up or down. In response to the request, the agent sends back a response about the condition of the host. If the agent itself is not running or if the device is down then the `IsSnmpSystemUp` request will send a nerve center alarm indicating that the device is down.

### The Steps of Automatic Management

After you have set up your Nerve Center template and autoManagement object, automatic management begins. The following steps occur:

1. The autoManagement daemon, `em_autod`, extracts the criteria required for gathering status data from the autoManagement object. This criteria includes the specified Nerve Center request template and the object type.
2. The autoManagement daemon then listens for notification of the creation or deletion of the specified type of object from the topology.
3. When the autoManagement daemon discovers an object of the specified type in the topology, it starts the Nerve Center request template designated by the autoManagement object.
4. The Nerve Center request starts. Following specifications in the request template, the Nerve Center sends a request for attributes to, or subscribes to events from, the agent of the specified network component.
5. The agent receives the request and sends back the appropriate response to the Nerve Center.
6. The Nerve Center listens for the agent's response or waits for an event to come from the agent.

**Example**—In the previous example, the autoManagement daemon extracts the Nerve Center request template `IsSnmppSystemUp` and the object type `host` from the `SysUpOrDown` autoManagement object.

The autoManagement daemon discovers a host computer named *wasabi* and starts up the `IsSnmppSystemUp` template.

The SNMP agent configured for *wasabi* receives the request from the Nerve Center. The request, essentially, asks “Is *wasabi* up or down?”

The SNMP agent configured for *wasabi* sends back notification that *wasabi* is down. The `IsSnmppSystemUp` request template sends a request to check if a device is up or down. If *wasabi* is down or the agent on *wasabi* is not running, the agent sends an error response that triggers the template to then send an alarm indicating that the device is down.

## 7.1.6 Related Tasks

- Complete a Discover of your network. For more information about finding out what components are located on your network, see Chapter 3 “Discovering Network Components.”
- Determine which Nerve Center request templates you want to automate. Also anticipate potential states of managed objects and transitions.
- Obtain the appropriate Nerve Center request templates in the Advanced Request tool.

## 7.1.7 Related Files

- /opt/SUNWconn/em/bin/em\_automgr
- /opt/SUNWconn/em/bin/em\_autod
- /opt/SUNWconn/em/bin/em\_services

---

## 7.2 Getting Started

This section explains how to start and exit the Request Controllers tool.

**1. Start Request Controllers in one of the following ways.**

- From Network Tools, click the Administration icon, then click the Request Controllers icon. The Request Controllers window displays.
- From an operating system prompt, execute: `em_automgr options`

where *options* include: `-help -host hostname`

For more information about the `em_automgr` command-line options, see Section 7.6.1 “Command-Line Options” on page 7-14.

**2. Perform any task discussed in this chapter.**

**3. Click File -> Exit when you are finished.**

See also Creating autoManagement Objects—page 7-8.

---

## 7.3 Creating autoManagement Objects

This section describes how to create a basic or an advanced autoManagement object using the Request Controllers tool. Basic autoManagement objects require a specification of the following:

- Nerve Center request template to launch against the specified type of object
- Type of object that exists in the network topology against which you want the autoManagement object to launch the Nerve Center request

Advanced autoManagement objects require this information as well as additional criteria, described in Section 7.1.3.4 “Criteria Used by autoManagement Objects” on page 7-5.

The following types of object creation are included:

- Basic
- Advanced
- Multiple

## ▼ To Create a Basic autoManagement Object

1. **In the Request Controllers window, click Object -> Create.**

The Request Controllers - Create dialog displays.

2. **To create a basic autoManagement object:**

- In the Template field, type or select the name of the Nerve Center request template to launch.
- In the Device field, enter the object type of network component, such as a host, container, bridge, or router in the network topology, against which you want the Nerve Center to start a request.

3. **Click OK.**

A message displays briefly to confirm that the autoManagement object was created.

## ▼ To Create an Advanced autoManagement Object

1. **In the Request Controllers - Create dialog, after you have specified the Nerve Center request template and the object type, click Advanced.**

2. **In the expanded Request Controllers - Create dialog, type the appropriate information in the following fields:**

- Scope (this can be `local` or `all`)
- Key
- Schema
- Event Request

For descriptive information about any of these details, see Section 7.1.3.4 “Criteria Used by autoManagement Objects” on page 7-5. For sample entry files that use this information, see Section 7.6.3 “Sample autoManagement Objects” on page 7-15.

3. **Click OK.**

A message displays briefly to confirm that the autoManagement object was created.

Whether you create a basic or an advanced autoManagement object, the autoManagement daemon will run the specified Nerve Center request against all objects of the specified type. Requests continue to run until the network component being monitored is deleted, or until you manually stop the request. For information about manually stopping requests, see Section 7.4 “Manually Starting and Stopping Requests” on page 7-11.

## 7.3.1 Creating Multiple autoManagement Objects

The Request Controllers tool provides a convenient and simple way to create autoManagement objects one at a time. However, when you want to create many autoManagement objects at once, it is easier to develop entry files.

Entry files are scripts that contain the specifications of autoManagement objects, including the object type and the Nerve Center request template to use—the same information that you specify in Request Controllers—but for more than one object simultaneously. You can also put additional information in entry files to develop more complex functions for autoManagement objects.

### ▼ To Create Multiple autoManagement Objects

1. **Execute the following command at an operating system prompt:**

```
em_objop -f entry-file
```

This command loads an entry file for the autoManagement objects that you want to create.

2. **Add entries to the file to describe each of the autoManagement objects you create.**

Multiple CREATE entries can be present in the entry file to load multiple autoManagement objects.

To view how the CREATE entry operates in the context of an entry file, see Section 7.6.3 “Sample autoManagement Objects” on page 7-15. For more information about using `em_objop` to create customized scripts, see Chapter 4 of the *Developing C++ Applications* Guide.

---

## 7.4 Manually Starting and Stopping Requests

When autoManagement objects are first created in the MIS, they are given an administrativeState value of unlocked, which means that the ability to automate Nerve Center requests is turned on. If you change the administrativeState value to locked, the autoManagement object is disabled and all requests launched by the autoManagement daemon for that autoManagement object are deleted. If you want to re-enable the autoManagement object, you need to change the administrativeState attribute value to unlocked. You can change the administrativeState value from the Request Controllers tool.

### ▼ To Start Request Controllers

- **After opening Request Controllers, click Object -> Start in the Request Controllers window.**

When a request is running, the autoManagement object is displayed as unlocked in the Request Controllers window. The administrative state value, unlocked, refers to the condition of the autoManagement object as being available, and permitted, to run automatically and continuously until the managed object that it affects is deleted.

### ▼ To Stop Request Controllers

- **To manually stop requests, click Object -> Stop.**

After you manually stop a request, the name of the autoManagement object is displayed as locked in the Request Controllers window. The administrative state value, locked, refers to the condition of the autoManagement object as being available, but not permitted, to run.

---

## 7.5 Changing autoManagement Object Characteristics

You can change, or edit, an autoManagement object to specify a Nerve Center request template different from the one that you originally specified, or to launch requests against another type of object. When you change an autoManagement object, the pre-existing object is deleted and replaced with a new autoManagement object containing your changes. You can also delete or change advanced criteria, for example, if the scope of the request changes.

To change an autoManagement object, you use the Request Controllers - Edit dialog, which contains the same fields as the Request Controllers - Create dialog.

### ▼ To Change a Basic autoManagement Object

1. **In the Request Controllers window, click Object -> Edit.**

The Request Controllers - Edit dialog displays, in the default manner for changing basic attributes of an autoManagement object.

2. **To change the autoManagement object:**

- In the Template field, select a different Nerve Center request template.
- In the Device field, enter the type of network component, such as a host, container, bridge, or router, against which you want the Nerve Center to start a request.

**Click OK.**

A message displays to confirm the deletion of the previous autoManagement object and the creation of the new autoManagement object which contains your changes.

### ▼ To Change an Advanced autoManagement Object

1. **In the Request Controllers - Edit dialog, click Advanced to expand the dialog.**
2. **Change the information in any of the following fields:**
  - Scope (this can be local or all)
  - Key



- Schema
- Event Request

For descriptive information about any of these details, see Section 7.1.3.4 “Criteria Used by autoManagement Objects” on page 7-5. For sample entry files that use this information, see Section 7.6.3 “Sample autoManagement Objects” on page 7-15.

### 3. Click OK.

A message displays to confirm the deletion of the previous autoManagement object and the creation of the new autoManagement object which contains your changes.

Using the new criteria in the modified autoManagement object, your requests run as specified until the network component being monitored is deleted, or until you manually stop the request. For information about manually stopping requests, see Section 7.4 “Manually Starting and Stopping Requests” on page 7-11.

## ▼ To Delete an autoManagement Object

- **In the Request Controllers window, select the autoManagement object that you want to delete, then click Object -> Delete.**

A message displays to confirm that the autoManagement object was deleted.

---

## 7.6 Reference

The following sections include information about command-line options for Request Controllers.

For detailed information about dialogs, menus, and other user interface elements, refer to the Solstice EM Online Help. To access Online Help, click the Help button on any dialog box or select options from the Help menu located in the upper right corner of each Solstice EM tool window.

## 7.6.1 Command-Line Options

The optional parameters of the `em_automgr` command are shown in the following table.

**TABLE 7-3** Request Controller Options

Option	Description
<code>-help</code>	Prints list of options (with descriptions) for the <code>em_automgr</code> command.
<code>-host hostname</code>	Specifies the <i>hostname</i> of a remote MIS.

For information about the criteria required for both Basic and Advanced autoManagement objects and for descriptions of the fields in the Request Controllers - Create dialog, see Section 7.1.3.4 “Criteria Used by autoManagement Objects” on page 7-5.

## 7.6.2 AutoManagement Daemon

The autoManagement daemon (`em_autod`) starts and stops requests launched against managed objects when the automatic management function is active. The autoManagement daemon starts automatically when the MIS is started using the command `em_services`. The daemon can also be restarted any time after start-up of the MIS using the command: `em_autod [-debug]`. The optional `-debug` parameter causes debugging information to be displayed.

The main tasks of the autoManagement daemon are to await the creation or deletion of object types specified by the autoManagement object and to launch or delete the Nerve Center requests against those created or deleted objects. To ensure that this task is completed, the object types must be created in or deleted from the same environment in which the autoManagement object exists.

As long as both conditions are met—the autoManagement daemon is running and objects of a type specified by the autoManagement object are created in the appropriate system—the autoManagement daemon registers with the MIS to receive event notifications of the creation or deletion of objects. For each autoManagement object, the autoManagement daemon retrieves from the MIS the managed objects that match the selection criteria set up in the autoManagement object. The autoManagement daemon then launches the request template specified by the autoManagement object against all objects specified in the entry file.

The autoManagement daemon is also notified by the MIS if the administrativeState value is changed for any autoManagement object, or if any managed objects are deleted. If the value of administrativeState for an autoManagement object is changed from unlocked to locked, the daemon deletes the requests that were launched against the objects selected by that entry file.

If a request launched against an object is deleted manually, you can restart automatic management for that object by first changing the administrativeState to locked, then changing it to unlocked.

---

**Note** – There can be at most one `em_autod` daemon running at one time. The MIS does not check for duplicate autoManagement daemons.

---

## 7.6.3 Sample autoManagement Objects

### 7.6.3.1 Entry Launching IsSnmppSystemUp Template

The format of `CREATE` entries is illustrated in the following example. The example entry file creates a single entry that launches the `IsSnmppSystemUp` template against all “Host” topology objects configured to manage SNMP. See TABLE 7-4 for field descriptions.

**CODE EXAMPLE 7-1** Entry Code that Launches the `IsSnmppSystemUp` Template

```
CREATE
{
  OC = autoManagementEntry
  OI = 'subsystemId="EM-MIS"/autoManagerId="TheAutoManager" /
  autoEntryId="IsSnmppSystemUp_Host" '
  autoEntryTemplate = IsSnmppSystemUp
  autoEntryScope = local
  autoEntryTopoType = Host
  autoEntryKey = 'cmipsnmp'
}
```

**TABLE 7-4** Automatic Management Entry File Fields

Entry File Field	Description
OC	The name of the object class.
OI	The identity or distinguished name of this entry. Each entry should have a unique name.
autoEntryTemplate	The name of the template you want to launch against the topology object. This template must exist in the system. To view the request templates, use Advanced Requests. For more information, consult the <i>Customizing Guide</i> .
autoEntryScope	Specifies whether or not the requests are launched against all topology nodes. The possible values for this attribute are <code>local</code> and <code>all</code> .  If the <code>autoEntryScope</code> is set to <code>local</code> , and there are multiple MISs connected, then the specified <code>autoEntryTemplate</code> is launched against only those topology nodes in the local MIS. If <code>autoEntryObject</code> is set to <code>all</code> , then the request is launched against all topology nodes in all available MISs.
autoEntryTopoType	Specifies the topology type of the objects against which you want to launch the request(s). This must be a valid topology type. All topology types in Solstice EM begin with a capital letter (for example, “Host”, not “host”).
autoEntryKey	The value specified in this field must match a keyword contained in the <code>ObjectInstance</code> in the <code>topoNodeMOSet</code> before a request is launched. If you specify ‘none’, then <code>em_autod</code> launches requests without checking the <code>topoNodeMOSet</code> . In short, requests are started on topology node creation based on topology type. This allows for very simple autoManagement Entries. The default value is ‘none.’

---

**Note** – Automatic Nerve Center requests work only for objects that exist in the topology.

---

### 7.6.3.2 Entry Launching LinkUp Template

The following `CREATE` entry creates a single autoManagement object that launches the LinkUp template against all topology objects on the local MIS of type “Link” with ‘cmipsnmp’ as part of its `topoNodeMOSet`.

### CODE EXAMPLE 7-2 Entry Code that Launches the LinkUp Template

```
CREATE
{
  OC = autoManagementEntry
  OI = 'subsystemId="EM-MIS"/autoManagerId="TheAutoManager"/
  autoEntryId="LinkUp_Link" '
  autoEntryTemplate = LinkUp
  autoEntryScope = local
  autoEntryTopoType = Link
  autoEntryKey = 'cmipsnmp'
}
```

You can also create an autoManagement object that minimizes the network traffic generally involved in polling. Management stations initiate polling by issuing SNM requests to proxy agents. By editing the autoManagement object to use the LinkUp Nerve Center request template, you can ensure that polling is completed outside the MIS by the proxy agent, thus minimizing the network traffic and polling work required of the MIS. For example, you could send a request to a proxy agent to check devices for reachability. If a device is not reachable, then that proxy agent sends out an event notification. For more information on device management using RPC agents see chapter 6 of the *Customizing Guide*.

To take advantage of this feature, add the following attributes to the CREATE entry:

- autoEntrySchema — A concatenation of the SNM agent name and the group in the schema that the agent supports.
- autoEntryEventRequest — The snmEventRequest information, entered in the same format used for the RCL function snmEventRequest when building a Nerve Center request template. For more information, see Chapter 20 of the *Customizing Guide*.

### 7.6.3.3 Entry Launching Ping-Reachable Template

The following entry file creates the device\_reachable\_ping autoManagement object. This autoManagement object issues only one request, against root. The entry file specifies the Nerve Center request template, snmEventRequest, is launched against all managed objects of the type, host, to determine whether each host in the topology can be reached by the ping command. Proxy agents handle the polling and send back error information only if the threshold specified in the request to the proxy agent is crossed, thereby reducing polling load on the MIS and improving MIS performance overall. Responses to the request are sent to the single AutoManageDecayReachablePing template, which ascertains which devices can be reached and posts alarms accordingly.

---

**Note** – The keyword *HOSTNAME* in the *autoEntryEventRequest* attribute is replaced by the name of the host against which the request is launched.

---

**CODE EXAMPLE 7-3** Entry Code That Launches the Ping-Reachable Template

```
CREATE
{
  OC = autoManagementEntry
  OI = 'subsystemId="EM-MIS"/autoManagerId="TheAutoManager"/
  autoEntryId="Ping-Reachable_Host" '
  autoEntryTemplate = AutoManageDecayReachablePing
  autoEntryScope = local
  autoEntryTopoType = Host
  autoEntryKey = RPC
  autoEntrySchema = ping-reach
  autoEntryEventRequest = 'request: {agentHost
  "HOSTNAME",agentProgram 100115, agentVersion 10,timeout
  33,interval 30, group "reach", threshold
  {"reachable",21,1,"0",high}}'
}
```

The advantage of this type of autoManagement is that you only need one template for any number of hosts. All the threshold checking is done by the SNM RPC proxy agent.

#### 7.6.3.4 Entry Returning the Transport Address of an Agent

The following file causes the transport address attribute of a CMIP or SNMP proxy agent to be returned in hexadecimal form. The line, *OPTION = 'HEX'* can be changed to *OPTION = 'OCTAL'* to have the transport address returned in octal form.

**CODE EXAMPLE 7-4** Entry Code That Returns the Transport Address in Hexidecimal Form

```
CREATE
{
OPTION = 'HEX'
OC = '"iimcMnagementProxyMIB":cmipsnmpProxyAgent'
OI = '/systemId="hostname"/internetClassId={1 3 6 1 4 1 42 2 2 2
9 2 4 1 0}/cmipsnmpProxyAgentId="agent1"'
mpaAddressInfo='default : NULL'
nameBinding='"iimcManagementProxyMIB":cmipsnmpProxyAgent-
cmipsnmpProxyTableNB
systemTitle='oid : { 1 2 3 1 }'
accessControlEnforcement='1'
accessControlMechanism='1'
adminState='unlocked'
cmipsnmpProxyAgentId='agent1'
managementProtocol='{1 3 6 1 4 1 42 2 2 2 9 99}'
opState='enabled'
snmpGetCommunityString='public'
snmpSetCommunityString='public'
supportedMIBs='{ps : "IIMCRFC1213-MIB", ps : "IIMCSZ-SZM-MIB"}
systemTitle='oid : {1 2 3 1}'
transportAddress="0X81924AD500A1'
}
```





# Gathering Attribute Data

---

Solstice Enterprise Manager (Solstice EM) provides three tools for collecting data from agents about the attributes of the network components you manage. Using the RPC/CMIP Data or SNMP Data tools, you can collect data from RPC, CMIP, or SNMP agents, respectively. Using the Data Collections tool, you create a collection, a specific set of attributes for which you obtain and save data. See Section 8.17 “Reference” on page 8-28 for more information.

This chapter comprises the following topics:

- Section 8.2 “Getting Started” on page 8-5
- Section 8.3 “Viewing Object Attributes From an SNMP Agent” on page 8-7
- Section 8.4 “Specifying an SNMP Device to Query” on page 8-8
- Section 8.5 “Working in Tables” on page 8-10
- Section 8.6 “Getting Attribute Data” on page 8-14
- Section 8.7 “Setting Attribute Data” on page 8-16
- Section 8.8 “Polling for Data” on page 8-17
- Section 8.9 “Displaying Data From Another MIS” on page 8-19
- Section 8.12 “Recording Data to a Collection” on page 8-24
- Section 8.13 “Creating Data Collections” on page 8-25
- Section 8.14 “Scheduling Collection Polls” on page 8-26
- Section 8.15 “Viewing Collected Data” on page 8-27
- Section 8.16 “Graphing Collected Data” on page 8-28

---

## 8.1 Overview

Gathering data about the network components you manage can make it easier to proactively manage faults of components or network configurations, enhance network performance, and plan for upgrades. For example, data such as CPU usage can help you optimize disk space and plan future software installations.

Solstice EM provides three tools with which to gather attribute data. Each tool serves a different purpose. SNMP Data enables you to gather, modify, and poll for data from SNMP agents. Likewise, RPC/CMIP Data enables you to gather, modify, and poll for data from RPC and CMIP agents. In both tools, the method of collection is non-persistent, which means that when data is updated, older data is replaced and not retained. However, from both tools, you can access Data Collections, the data gathering tool that enables you to create a collection, a specific group of attributes, for which values can be gathered from SNMP, RPC, or CMIP agents at specified intervals. The collected data is recorded in a log file as a set of reports that can be viewed or graphed.

**TABLE 8-1** Solstice EM Tools for Data Gathering

Tool for Data Gathering	Protocols Supported	What You Can Do
SNMP Data	SNMP	<p>Select specific attributes of network components configured with SNMP agents</p> <p>View, or get, attribute values of read-only attributes, which are identifiable as gray icons</p> <p>Modify, or set attribute values of read-write attributes, which are identifiable as white icons</p> <p>Poll for data at intervals</p> <p>Prepare for a collection of SNMP data to be retrieved and recorded in a log file</p>
RPC/CMIP Data	RPC and CMIP	<p>Select specific attributes of network components configured with RPC and CMIP agents</p> <p>View, or get, attribute values of read-only attributes, which are identifiable as gray icons</p> <p>Modify, or set, attribute values of read-write attributes, which are identifiable as white icons</p> <p>Poll for data at intervals</p> <p>Query using CMIP and SNM schemas</p> <p>Prepare for a collection of RPC or CMIP data to be retrieved and recorded in a log file</p>
Data Collections	SNMP, RPC, and CMIP	<p>Select specific attributes of network components configured with SNMP, RPC, and CMIP agents</p> <p>Create a collection which automatically polls for and records attribute data</p> <p>View attribute data in the SNM Results Browser</p> <p>Graph data trends in Grapher</p>

## 8.1.1 How Data is Obtained in Solstice EM

Regardless of the type of data that you collect or the Solstice EM tool that you use to collect it, all data is stored in a repository on a host, referred to as a Management Information Server (MIS). In Solstice EM, all MISs use the CMIP protocol to communicate.

All data regarding a network component is saved in an MIS repository. The network component is configured with an agent, a software module that enables communication with the MIS. The agent may be configured to communicate using CMIP or another protocol. If the network component uses a protocol other than CMIP, Solstice EM provides Management Protocol Adaptors (MPA) that use the Portable Management Interface (PMI) application programming interfaces (APIs) as a framework to translate one protocol into another. The following figure shows the process used to enable a network component to communicate with and gather attribute data from the MIS.

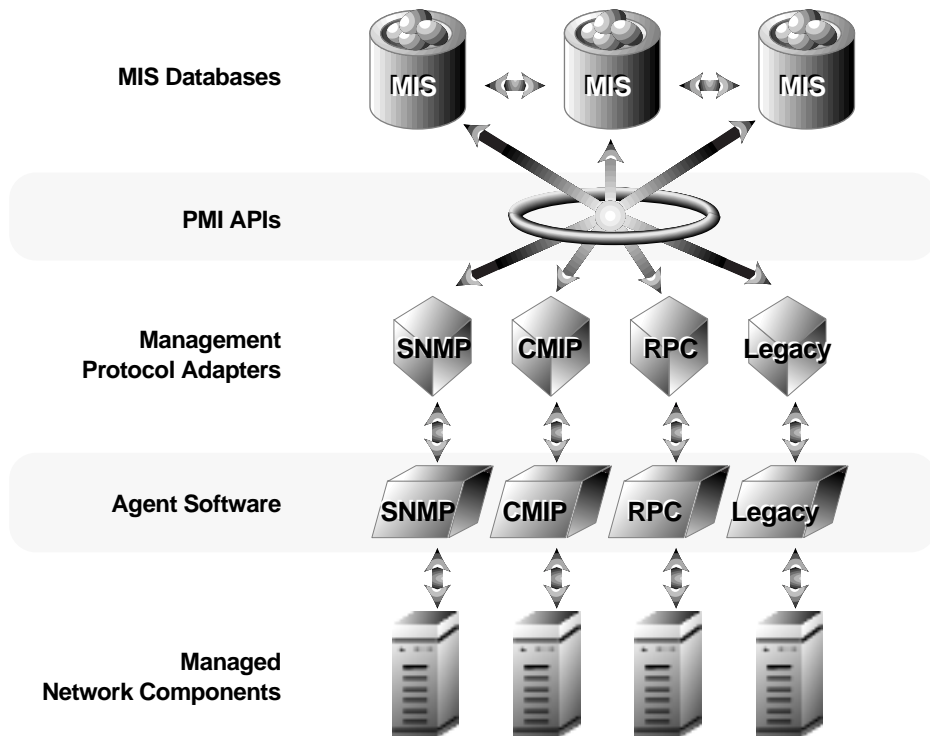


FIGURE 8-1 Solstice EM Architecture as it Facilitates Network Communication

You can think about it this way: the MIS is like an international organization that has gathered statistics about one of its member countries. The network component is like the member country, and it wants to find out the statistics that have been gathered about itself. Once it has those statistics, it can evaluate what must be done to improve its presence and performance on a global basis.

With this in mind, when you use any of the data collection tools—RPC/CMIP Data, SNMP Data, or Data Collections—you provide an agent software module, located on the network component, with a list or collection of the kind of data that you want to receive. Like a diplomat from a member country, the agent sends the request for data to the MPA, which acts as a translator between the agent and the MIS. The MPA then uses the PMI APIs—the equivalent of vocabulary lists and conjugation sheets—to translate the protocol of the network component into the protocol that the MIS understands. After receiving the request in its native CMIP protocol, the MIS retrieves the requested data, which then passes back to the network component through the same process in reverse.

## 8.1.2 About Collections

In RPC/CMIP Data and SNMP Data, you can retrieve one-time views of data about a network component. In Data Collections, you can obtain a more permanent view of data by setting up a collection, a set of object attributes for which you can poll periodically, and a file in which the returned sets of data, referred to as reports, are recorded. The benefit of creating a collection of attribute data lies in its ability to be stored, viewed sequentially in a browser, or graphed in the Grapher tool.

## 8.1.3 Related Tasks

- Complete a Discover before querying for data. For information about discovering components on your network, see Chapter 3 "Discovering Network Components."

---

**Note** – You must complete a Discover prior to getting, setting, polling, or collecting data.

---

- Ensure that appropriate access privileges have been set in Security. For information about setting user access privileges, see Chapter 6 "Controlling User Access."

## 8.1.4 Related Files

- /opt/SUNWconn/em/bin/em\_viewer
- /opt/SUNWconn/em/bin/em\_dataviewer
- /opt/SUNWconn/em/bin/em\_snmpbrowser
- /opt/SUNWconn/em/bin/em\_datacollector
- /opt/SUNWconn/em/bin/snm\_br
- /opt/SUNWconn/em/bin/em\_grapher

## 8.1.5 Further Reading

For additional data about SNMP, RPC, and CMIP agents and Management Protocol Adapters (MPA), see the *Management Information Server (MIS) Guide*.

For additional data about adding, integrating, converting, and loading managed object classes, see the *Management Information Server (MIS) Guide*.

For additional data about SNMP, RPC, and CMIP management, see Chapters 8 through 10 of the *Customizing Guide*.

---

# 8.2 Getting Started

This section explains how to start and exit the three tools provided for gathering and collecting attribute data:

- SNMP Data
- RPC/CMIP Data
- Data Collections

## ▼ To Use SNMP Data

### 1. Start SNMP Data in one of the following ways.

- From Network Views, click Tools->SNMP Data.
- From an operating system prompt, type: `em_snmpbrowser options`

where *options* include: `-help -host MIS servername -agent  
-id system toponodeid -community`

See Section 8.17.1 “SNMP Command-Line Options” on page 8-29 for more information.

2. **Perform any task discussed in this chapter.**
3. **Click File->Exit when you are finished.**

**See Also** SNMP Command-Line Options—page 8-29

## ▼ To Use RPC/CMIP Data

1. **Start RPC/CMIP Data in one of the following ways:**
  - From Network Views, click Tools -> RPC/CMIP Data.
  - From an operating system prompt, type: `em_dataviewer options`  
where *options* include the following: `-help -host MIS servername -id system toponodeid`
2. **Perform any task discussed in this chapter.**
3. **Click Close when you are finished.**

## ▼ To Use Data Collections

1. **Start Data Collections in one of the following ways.**
  - From the Network Tools window, double-click the Data Collections icon.
  - From the RPC/CMIP Data dialog or an SNMP Data - Table window, click the Data Collection button.
  - From an operating system prompt: `em_datacollector options`  
where *options* include the following: `-help -host hostname -timeout time-out`

See Section 8.17.2 “Data Collections Command-Line Options” on page 8-30 for more information.

2. **Perform any task discussed in this chapter.**
3. **Click File->Exit when you are finished.**

**See Also:**

- “Data Collections Command-Line Options” on page 8-30
- “Recording Data to a Collection” on page 8-24

---

## 8.3 Viewing Object Attributes From an SNMP Agent

By querying an agent from SNMP Data, you can get data about attributes, such as the IP status or the number of error messages of each component running an SNMP agent. Attributes are contained in attribute folders that you can display in the upper portion of the SNMP Data window. Attribute folders are contained in MIB folders that pertain to an associated MIB.

The SNMP Data window displays two default characteristics: the name of the host on which the SNMP agent is located, and the public read community. You can view the attributes of another network component by replacing the name in the Device field.

### ▼ To View Specific Attributes of an Object

1. In the Device field of the SNMP Data window, type the host name or internet address of the network component configured with the SNMP agent that you want to query.
2. Press Return.
3. (Optional) In SNMP Read Community, type the name of a group or an individual to have general read access to the attribute data. The default value is Public.
4. Press Return.
5. To view MIB variables sorted by Object Identifier (Oid) or by name, click View->Sort by Names or View->Sort by Oids to select the MIB variables view.
6. Ensure that a check mark is displayed in the View->Supported MIBs Only box to view all folders of supported management information bases (MIBs).

You can change the display of folders by clicking View->Supported MIBs Only. When a check mark is displayed in the Supported MIBs Only box, only folders of MIBs supported by the network component are displayed. Otherwise, folders of all MIBs integrated into Solstice EM are displayed.
7. Click a MIB folder to display the attribute folders pertaining to the MIB. Click the appropriate attribute folder to display its contents, the attributes.

---

**Note** – Index attributes are differentiated by color. The SNMP Browser indicates internal indexes in blue and external indexes in red.

---

**8. Click the text of the attribute you want to select.**

Attributes that are read-only appear as gray page icons. Attributes that are read-write appear as white page icons.

---

## 8.4 Specifying an SNMP Device to Query

Gathering data about the attributes of a network device entails querying an SNMP agent. The SNMP agent then sends the request for data to the network component, and the network component returns the requested data to the agent. The data is displayed in the tables of the SNMP Data tool. Although the SNMP Data tool is configured to gather data from a default SNMP agent, you can select a different agent to query and you can query multiple agents.

### ▼ To Specify an SNMP Agent

1. **In the Device field of the SNMP Data window, type the host name or IP address of the network component configured with the SNMP agent that you want to query.**
2. **Press Return.**
3. **(Optional) In SNMP Read Community, type the name of a group or an individual to have general read access to the attribute data. The default value is Public.**
4. **Press Return.**

Group folders associated with the agent are displayed in the upper portion of the SNMP Data window.



## ▼ To Select Multiple Agents Simultaneously

You can specify multiple SNMP agents using SNMP Data tables. For more information about SNMP Data tables, see Section 8.5 “Working in Tables” on page 8-10.

1. **In the Device field of the SNMP Data window, type the host name or IP address of the network component configured with the SNMP agent that you want to query.**
2. **Press Return.**
3. **(Optional) In SNMP Read Community, type the name of a group or an individual to have general read access to the attribute data. The default value is Public.**
4. **Press Return.**
5. **Ensure that a check mark is displayed in the View -> Supported MIBs Only box to show the folders of all MIBs supported by the network component for which you want to obtain attribute data.**
6. **Click a MIB folder to display the attribute folders pertaining to the MIB. Click the appropriate attribute folder to display its contents, the attributes.**
7. **Click the text of the attribute you want to select, then:**
  - a. **Click the table button (located to the right of the Add Selected to button).**
  - b. **Select the table into which you want the data to display. If no other table has been created, the only available option is New Table.**
  - c. **Click Add Selected to.**
8. **In the SNMP Data - Table window, click View->Add Device.**
9. **In the Add Device dialog,**
  - a. **In the Device field, type the host name or IP address of another network component configured with an SNMP agent.**
  - b. **Press Return.**
  - c. **In the Community field, type the name of the group or individual to have read access to the attribute data.**
  - d. **Click OK.**

The SNMP Data table is now set to query multiple agents. You can obtain data about the network components associated with these agents when you click Get in the SNMP Data - Table window.

---

## 8.5 Working in Tables

The SNMP Data tool provides tables in which you display the attribute data that you obtain from SNMP agents. In the SNMP Data window, data is displayed in rows. When data is moved into an SNMP Data - Table window, it is then displayed in columns. You can add as many attributes as you want to a table, and you can edit the arrangement of data in a table and customize the format of tables.

### 8.5.1 Creating and Loading Tables

Most available attributes are read-only. These attributes display as gray icons, and you can only view their attribute values. Read-write attributes are displayed as white icons. From the SNMP Data tool, you can change their values in the MIS by dragging them into a table and clicking Set. For more information about setting attribute values, see Section 8.7 “Setting Attribute Data” on page 8-16.

You can create and customize your own tables for organizing this data or use the default table. You can also save the structure of the tables you create, including the attribute headings across the top of the table, but you cannot save the data contained within a table when you save a table.

#### ▼ To Create Tables

- To create an empty table, in the SNMP Data window, click File->Create Table.
- To create a table filled with selected attributes and their values, in the SNMP Data window, open the appropriate MIB folder, click an attribute folder, and click the text of an attribute, then click Add Selected to->New Table.
- To save the format of a table, including the attributes that comprise the headings of columns and rows, click File->Save Table Definition.

Save the table format as a file in the Save File dialog and click OK. Table formats are generally saved in the current working directory. You can save tables to any directory to which you have write privileges.

#### ▼ To Load Existing Tables

1. In the SNMP Data window, click File->Open Table.
2. In the Load From File dialog, select the file of the table to load.

## 8.5.2 Selecting and Moving Data in Tables

You can select data and move it to other cells in the table.

### ▼ To Make Selections in Tables

- **Click a row or column label to select the desired row or column.**
- **Click Edit->Select All to select all items in a table.**
- **Click Edit->Deselect All to deselect all selected items.**

### ▼ To Move Attributes Into a Table

- 1. In the SNMP Data window, click an attribute folder or the text of an attribute and hold down the middle mouse button to drag the icon.**
- 2. In the SNMP Data - Table window, drop the icon on the Sun logo, as indicated by the message, “Drop Here: Folder or Sheet Icon.”**

For a group icon, all of the attributes for that group are added to the active table. For an attribute icon, only the selected attribute is added. You can mix agents, groups, and attributes as desired.

### ▼ To Create a Row in a Table

- 1. In the SNMP Data window, click an attribute folder or an attribute text.**
- 2. Click Add Selected To to add the MIB group and its attributes to the table.**
- 3. Click the row you want to add to the table.**
- 4. Click Agent->Add Row to create an empty row.**
- 5. Fill in the values in the empty row.**
- 6. Click Agent->Create Row.**

## ▼ To Delete a Row from a Table

1. In the SNMP Data window, click an attribute folder or an attribute text.
2. Click Add Selected To to add the MIB group and its attributes to the table.
3. Click the row you want to delete from the table.
4. Click Agent->Delete Row to delete the selected row.

### 8.5.3 Completing Tables

You can add attributes to a table and display and modify attribute values.

## ▼ To Add Attributes to Tables

1. In the SNMP Data window, display available MIB folders.  
Ensure that a check mark is displayed in the View->Supported MIBs Only box to show the folders of supported MIBs.
2. Click a MIB folder to display the attribute folders pertaining to the MIB. Click the appropriate attribute folder to display its contents, the attributes.
3. Click the text of the attribute you want to select.
4. Click the table button to the right of the Add Selected to button, and select the name of the table into which you want the attribute data to display.  
If no other table has been created, the only available option is New Table.
5. Click Add Selected to.  
The attribute data is placed in the appropriate table.

## 8.5.4 Clearing Tables

You can remove data from a table cell, delete a row or a column, and clear tables.

### ▼ To Delete Table Entries

In the SNMP Data - Table window, do any of the following:

- **Select the rows or columns to be deleted, then click View->Delete Selected.**
- **To remove all columns, click View->Delete All Columns.**
- **To clear data from the rows in the table without clearing column headings, click View->Delete All Rows.**

## 8.5.5 Printing Tables

### ▼ To Print Tables

- **Click File->Print in the table window.**

---

## 8.6 Getting Attribute Data

By querying an agent by means of the RPC/CMIP Data or SNMP Data tools, you can get data about attributes, such as the IP status or the number of error messages output, from each SNMP, RPC, or CMIP agent configured for the network component. This data is then displayed in the respective tool: either SNMP attribute values in the SNMP Data tool or RPC and CMIP attribute values in the RPC/CMIP Data tool.

SNMP Data queries can be performed using either SNMPv1 or SNMPv2c protocols. In SNMPv1, you will receive a best-effort response. If you incorrectly specify the attributes to get data about, your request will be rejected entirely. With SNMPv2c however, when an agent cannot provide values to all attributes from the request, the agent does respond to all requests that can be satisfied and rejects only the incorrect attributes.

### ▼ To Get Attribute Data From SNMP Agents

1. **Start the SNMP Data tool.**

See Section 8.2 “Getting Started” on page 8-5 for more information.

2. **In the Device field of the SNMP Data window, type the host name or internet address of the network component configured with the SNMP agent that you want to query.**

3. **Press Return.**

4. **(Optional) In SNMP Read Community, type the name of a group or an individual to have general read access to the attribute data. The default value is Public.**

5. **Press Return.**

6. **Ensure that a check mark is displayed in the View->Supported MIBs Only box to show the folders of all MIBs supported by the network component for which you want to obtain attribute data.**

7. **Click a MIB folder to display the attribute folders pertaining to the MIB. Click the appropriate folder to display its contents, the attributes.**

8. **To get data for only one attribute, click the text of the attribute.**

9. **Then, click Get in the SNMP Data window.**

---

**Note** – If a GET request is taking too much time to retrieve the requested information, you can use the “stop” button to terminate the request and continue using the application. If you want to get data for multiple attributes, click the text of one attribute, then set up a customized SNMP Data table in the following manner:

---

**a. Click the table button (located to the right of the Add Selected to button).**

If only one table has been created, click New Table.

**b. Select the table into which you want the data to display.**

**c. Click Add Selected to.**

The attribute data is displayed in an SNMP Data - Table window. To display additional attribute data in the SNMP Data - Table window, return to the SNMP Data window, click the text of another attribute, and repeat the previous procedure. You can add as many attributes to the SNMP Data table as you want.

**d. Click Get in the SNMP Data - Table window each time you want to update the data displayed.**

## ▼ To Get Attribute Data From RPC/CMIP Agents

**1. Start the RPC/CMIP Data tool.**

**2. In the Target Object field, type the host name or internet address of the network component for which you want to retrieve attribute data.**

**3. Press Return.**

In Attribute Groups, attributes from all RPC and CMIP agents configured for the network component are listed. The appropriate protocol is automatically selected. If the device supports both RPC and CMIP, you can select either RPC or CMIP to list attributes from the agents configured with either protocol.

**4. In Attribute Groups, double-click the folder of the attribute for which you want to obtain data values.**

The attribute values are displayed in the Data area of the RPC/CMIP Data tool.

You can also select an attribute and click Get to send a request for data to the component specified in the Target Object field.

## ▼ To Stop a Get Request

- **Click Stop during any get request to cancel the current request for attribute data.**  
Stop is grayed out when no request for data is being processed.

---

## 8.7 Setting Attribute Data

With the SNMP Data and RPC/CMIP Data tools, you can modify and save attribute values of an object. Although most available attributes are read-only causing them only to be viewed, some attributes, such as sysContact, are read-write and can be viewed as well as modified. In the SNMP Data tool, read-only attributes display as gray icons. Read-write attributes display as white icons.

## ▼ To Set Attribute Data With an SNMP Agent

Before you can set attribute data, you must get attribute data. This task includes procedures for getting and then setting data.

1. **In the Device field of the SNMP Data window, type the host name or internet address of the network component configured with the SNMP agent that you want to query.**
2. **Press Return.**
3. **(Optional) In SNMP Read Community, type the name of a group or an individual to have general read access to the attribute data. The default value is Public.**
4. **Press Return.**
5. **Ensure that a check mark is displayed in the View->Supported MIBs Only box to show the folders of all available MIBs from which you can select attributes.**
6. **Click the folder of the MIB to display the attribute folders.**  
The data of selected attributes is displayed in the attributes table in the lower portion of the SNMP Data window. Attributes that appear in white are read-write and can be changed. Attributes that appear in gray are read-only.
7. **Click the appropriate attribute folder to display its contents, the attributes.**
8. **Click the text of the attribute you want to select to change. Delete the value and type a new value in the field.**



**9. Click Set to send changed values back to the network component.**

You can also display attribute data in an SNMP Data - Table window by clicking the table button, selecting New Table or the appropriate table if more than one are opened, and clicking Add Selected to. Then, you can change data in the table and click Set in the SNMP Data - Table window.

## ▼ To Set Attribute Data From an RPC/CMIP Agent

**1. Start the RPC/CMIP Data tool.**

**2. In the Target Object field, type the host name or internet address of the network component for which you want to retrieve attribute data.**

**3. Press Return.**

In Attribute Groups, attributes from all RPC and CMIP agents configured for the network component are listed. The appropriate protocol is automatically selected. If the device supports both RPC and CMIP, you can select either RPC or CMIP to list attributes from the agents configured with either protocol.

**4. In Attribute Groups, click the attribute for which you want to display data values to modify.**

**5. In the Data field, click in the field of the attribute data that you want to modify. Delete the current value from the field and type a new value.**

For example, if you want to change the name of the system administrator responsible for a particular component, delete the value of the `sysContact` attribute and type a new name.

You can change the read/write attribute values of every agent configured for the network component.

**6. Click Set to send changed values back to the network component.**

---

## 8.8 Polling for Data

Polling for data enables you to continually monitor details that affect network performance at specified intervals. You can set polling intervals after initially getting attribute values.

## ▼ To Poll an SNMP Agent

1. **After getting attribute values for selected attributes, display the data in a new or existing SNMP Data - Table window.**

For information about getting attribute values, see Section 8.6 “Getting Attribute Data” on page 8-14. For information about creating an SNMP Data table, see Section 8.5.1 “Creating and Loading Tables” on page 8-10.

2. **In the SNMP Data - Table window, click Poll.**
3. **In the Poll dialog, click All or Selected Only to specify whether to query all agents noted in the table or only the agents that you have selected.**
4. **In the Rate field, drag the marker to specify the interval, in seconds, between queries.**
5. **Click Close to close the Poll dialog.**

Querying occurs automatically, at the intervals you specified.

## ▼ To Poll an RPC/CMIP Agent

1. **In the RPC/CMIP dialog, get values of the attributes for which you want data.**

For information about getting attribute values, see Section 8.6 “Getting Attribute Data” on page 8-14.

2. **Click Poll.**
3. **In the Poll dialog, set polling to occur in time intervals of seconds, minutes, or hours.**
4. **In the Frequency field, set the number of seconds, minutes, or hours to pass between polls.**
5. **Click Start.**

Polling begins. The data in the Data field is updated at the specified intervals.

---

**Note** – As data is updated in the SNMP Data and RPC/CMIP Data tools, older data is replaced by newer data. However, you can open Data Collections to set up a collection of attributes which you can poll at intervals and retain in a log file. See the following section, “Recording Data to a Collection,” for more information.

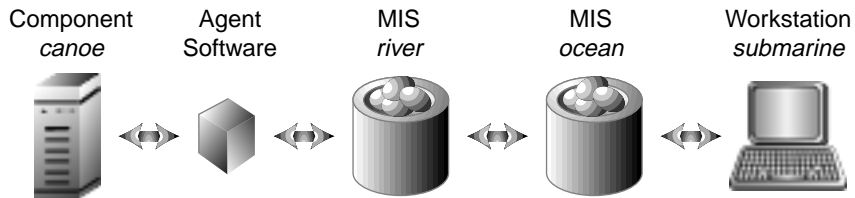
---

---

## 8.9 Displaying Data From Another MIS

When MIS-to-MIS communication has been established, you can manage a network component from another MIS. For example, in the following illustration, the host *canoe* is configured with an SNMP agent and is managed by the MIS located on the host, *river*. The host *submarine* is managed by the MIS located on the host, *ocean*.

When MIS-to-MIS communication is configured between the two MISs, located respectively on the hosts *river* and *ocean*, you can use the SNMP Data tool on *submarine* to manage *canoe*. Likewise, if you want to obtain RPC or CMIP data, you can use the RPC/CMIP Data tool to manage a component on another MIS.



**FIGURE 8-2** Viewing Requested Data Returned From a Host on a Remote MIS

Before you can manage a component on another MIS, you need to set MIS-to-MIS communication between the two servers. Setting up MIS-to-MIS communication involves specifying the trusted host and setting up an MIS-to-MIS connection. For information on setting up trust relationships between MIS hosts, see Chapter 6 "Controlling User Access." For information about setting up MIS-to-MIS connections, refer to the *MIS Guide*.

---

## 8.10 Obtaining Data From a Network Component Managed by a Remote MIS

Every component on your network that is integrated into Solstice EM as a managed object is assigned a unique, numeric identifier called a *toponodeID*. If you know the *toponodeID* of a network component managed by a remote MIS, and if you have previously initiated MIS-to-MIS communication with the remote MIS, you can open the SNMP Data or RPC/CMIP Data tools from the command line or the Network Views tool to display the attribute data of all agents configured for the network

component. For information about using Network Views to view a network component managed by a remote MIS, see Chapter 4 "Viewing Network Components."

## ▼ To Obtain the toponodeID of a Network Component

1. In Network Tools, click Administration.
2. In the Solstice EM - Administration window, click MIS Objects.
3. In the MIS Objects (object editor) window, select the folder of the network component for which you want the toponodeID.

For example, if you want the toponodeID of a host named `sparks`, look for the folder labeled as follows: `systemId=name:"sparks"`

---

**Note** – If the folder is not already open, click the plus sign to the left of the folder.

---

4. Select the `topoNodeDBId=NULL` folder under the `systemId=name:<hostname>`.
5. Click Object->Action->topoNodeGetByName.
6. In the Parameter field of the MIS Objects - Action dialog, type the name or internet address of the host for which you want to obtain the toponodeID.
7. Click OK.

In this example, you would enter `sparks` in the Parameter field and click OK.

The MIS Objects - Output Window is displayed containing the toponodeID of the specified network component set in braces.

## ▼ To Obtain Data From a Network Component Managed by Another MIS

- Obtain SNMP data from all agents configured for a network component on a remote MIS by typing the following command at an operating system prompt:

```
em_snmpbrowser -host hostname -id name:toponodeID
```

where:

<code>em_snmpbrowser</code>	Specifies that you want to gather SNMP data using the SNMP Data tool
<code>-host <i>hostname</i></code>	Refers to the name of the local MIS
<code>-id <i>name</i></code>	Refers to the name of the remote MIS, which may be in a subordinate or equal position to the local MIS depending upon the configuration
<code><i>toponodeID</i></code>	Refers to the toponodeID of the network component managed by the remote MIS

for example:

```
em_snmpbrowser -host river -id canoe:25
```

where:

<code>em_snmpbrowser</code>	Specifies that you want to gather SNMP data using the SNMP Data tool
<code>-host <i>river</i></code>	Is the name of the host on which the local MIS resides
<code>-id <i>canoe</i></code>	Is the name of the host on which the remote MIS resides
<code><i>25</i></code>	Is the toponodeID of a device managed by the remote MIS

- Obtain RPC or CMIP data from all agents configured for a network component on a remote MIS by typing the following command at an operating system prompt:

```
em_dataviewer -host hostname -id name:toponodeID
```

where:

<code>em_dataviewer</code>	Specifies that you want to gather RPC or CMIP data using the RPC/CMIP Data tool
<code>-host <i>hostname</i></code>	Refers to the name of the host on which the local MIS resides
<code>-id <i>name</i></code>	Refers to the name of the host on which the remote MIS resides
<code><i>toponodeID</i></code>	Refers to the toponodeID of the network component managed by the remote MIS

For example:

```
em_dataviewer -host river -id canoe:25
```

where:

<code>em_dataviewer</code>	Specifies that you want to gather RPC or CMIP data using the RPC/CMIP Data tool
<code>-host <i>river</i></code>	Is the name of the host on which the local MIS resides
<code>-id <i>canoe</i></code>	Is the name of the host on which the remote MIS resides,
<code><i>25</i></code>	Is the toponodeID of a device managed by the remote MIS

---

## 8.11 Updating MIS Tables With Attribute Values From Third-Party MIBs

SNMP Data accommodates the functionality provided by certain third-party applications to update MIS tables with new values of third-party MIB attributes. In the SNMP Data tables, a set of menu items, Add Row and Delete Row, enable you to update or remove the value of a third-party MIB attribute directly within your customized SNMP Data table.

### ▼ To Update MIS Tables With Attribute Values

1. **In an SNMP Data - Table window, select a row of data by clicking the heading of the row.**
2. **Click Agent->Add Row.**

A new empty row will be added below the selected row.

3. **Select Agent->Create Row from the Table window menu bar.**

A request to fill the row with the appropriate attribute values is sent to the agent. If the request is granted, the new values are displayed in the row.

### ▼ To Remove an Attribute Value From an MIS Table

1. **In an SNMP Data - Table window, select a row of data by clicking the heading of the row.**
2. **Click Agent->Delete Row.**

The row is removed from the SNMP Data table. Simultaneously, the attribute values are also removed from the MIS tables.

---

## 8.12 Recording Data to a Collection

Solstice EM enables you to create a collection, a set of attributes which you can continually poll for new sets of attribute values. Collections are saved in log files that are considered part of the collection.

Solstice EM provides the Data Collections tool for setting up a collection. From both the SNMP Data and RPC/CMIP Data tools, you can invoke the Data Collections tool and create a collection in which to store the attribute sets that you select when you query an agent for SNMP, RPC, or CMIP data.

### ▼ To Record SNMP Data

**1. From the SNMP Data - Table window, click Data Collection.**

The Data Collections tool opens, and the Create dialog is displayed. The dialog automatically has been updated with the attributes that you previously selected in the SNMP Data tool. By saving these attributes to a collection, you can schedule the same set of attributes to be polled for data continuously at set intervals.

**2. Set up the collection.**

For information about creating and using data collections, see Section 8.12 “Recording Data to a Collection” on page 8-24.

### ▼ To Record RPC/CMIP Data

**1. From the RPC/CMIP Data dialog, click Data Collection.**

The Data Collections tool opens, and the Create dialog is displayed. The dialog automatically has been updated with the attributes that you previously selected in the SNMP Data tool. By saving these attributes to a collection, you can schedule the same set of attributes to be polled for data continuously at set intervals.

**2. Set up the collection.**

For information about creating and using data collections, see Section 8.12 “Recording Data to a Collection” on page 8-24.



---

## 8.13 Creating Data Collections

The following task explains how to create a collection of attributes that you can then schedule to be polled continuously at set intervals.

### ▼ To Create a Collection

**1. In the Data Collections window, click Actions->Create Collection to display the Create dialog.**

**2. In the Create dialog, click Objects Browser to specify the object to search for.**

**3. In the Object Browser dialog, click the folder icon of an object.**

**4. Click Add to select an object.**

The selected object displays in Managed Objects.

There may be a brief delay after clicking a folder in the Object Browser dialog.

**5. Click Close to close the Objects Browser dialog.**

**6. Click Attributes Browser.**

**7. In the Attribute List dialog, select attributes of the object to include in the collection.**

**8. Click OK to close the dialog.**

The attributes display in the Attributes list.

**9. Set the properties of the collection.**

**a. Type the name of the collection in the Collection Name field.**

**b. Click the ellipsis (. . .) button of the Directory Name field to open the Collection Directory Name dialog for setting a location for the collection.**

**c. Click OK to close the dialog.**

**d. Type a value or click the up or down arrows of the Max File Size field to specify the size, in megabytes, of data that you want the file to hold. Ultimately, this measurement determines the size of the log file of the collection.**

- e. Click the appropriate button of the File Wrapping field to turn file wrapping on or off.

In the File Wrapping field, the default is Yes. When the log file of the collection reaches the Max File Size you specify, file wrapping occurs in the log file. New data writes over old data.

- f. In Log Format, click EM or SNM to specify whether you want to format your file using Enterprise Manager or SunNet Manager format.
  - g. In Write MIB Name, select Yes or No to specify whether or not to record the MIB name before each attribute value listed in the log file of the collection.
  - h. In Write Attribute Name, select Yes or No to specify whether or not to log the attribute name before each attribute value listed in the log file of the collection.
10. Click OK to create the collection with the selected parameters.

---

## 8.14 Scheduling Collection Polls

You can schedule to poll a collection in the Schedule section of the Create dialog. After you set the schedule, querying occurs automatically. You can schedule collection times during the creation of the collection. You can also change polling intervals and start and stop times for an existing collection.

### ▼ To Schedule Polling

1. In the Schedule section of the Create dialog:
  - a. Click the Start Time box to select the time when you want data collection to start.
  - b. Click AM or PM.
  - c. In the Date field, type the date on which you want to start data collection. Use the format *mm/dd/yyyy*.
  - d. Click the Stop Time box to select the time when you want to end data collection.
  - e. Click AM or PM.
  - f. In the Data field, type the date on which you want to end data collection. Use the format *mm/dd/yyyy*.

- g. Click the arrows of the Poll Interval option to increase or decrease the amount of time to pass before the agent polls the object for data.**

The default poll interval is 60 seconds between polls.

- 2. Click OK.**

Data collection automatically begins according to the time intervals you set. Data retrieved from the object is automatically recorded in the log file of the collection.

---

## 8.15 Viewing Collected Data

When you want to view data obtained in a collection formatted in the SNM format, you can use the SNM Results Browser. To view data formatted in the Solstice EM format, open the log file in which the data is contained.

### ▼ To View Data in a Collection of SNM Format

- 1. In the Data Collections window, select the log file of the collection that contains the data you want to view.**
- 2. Click Actions->SNM Results Browser.**
- 3. In the SNM Results Browser, click File ->Load.**
- 4. In the Load dialog, select the path of the log file that you want to open.**
- 5. Click Load.**

The log file you selected is displayed in the SNM Results Browser as a sequence of data referred to as a stream.

---

## 8.16 Graphing Collected Data

When you poll for data over a long period of time, you can graph trends in the Solstice EM-Grapher tool.

### ▼ To Graph Trends in the Grapher Tool

1. **In the SNM Results Browser, select the streams that you want to graph.**
2. **Right-click in the upper portion of the SNM Results Browser.**
3. **In the Streams menu.**
4. **Click Graph.**
5. **From the list of attributes, select an attribute to be graphed.**

The data is displayed in the Grapher tool.

---

## 8.17 Reference

The following sections provide command-line options for SNMP Data Browser.

For detailed information about dialogs, menus, and other user interface elements, refer to the Solstice EM Online Help. To access Online Help, click the Help button on any dialog box or select options from the Help menu located in the upper right corner of each Solstice EM tool window.

## 8.17.1 SNMP Command-Line Options

The following table describes the command options and parameters for the `em_snmpbrowser` command, which is used to start SNMP Data.

**TABLE 8-2** SNMP Data Command-Line Options

Option	Parameter	Description
-help		Prints list of options (with descriptions) for the <code>em_snmpbrowser</code> command.
-host	<i>hostname</i>	Specifies the <i>hostname</i> of a remote MIS.
-agent	<i>agentname</i>	Specifies the default agent name. If omitted, default is the name of the MIS host. If <code>-id topo_id</code> is also specified, <code>-id topo_id</code> take precedence.
-community	<i>string</i>	Specifies the default community string. If omitted, default is "public" For example: <code>em_snmpbrowser -community syseng</code> specifies that only the systems engineering group will have read privileges to the returned values of a query
-id	<i>topo_id</i>	Specifies the <code>toponodeId</code> . If <code>-agent agentname</code> is also specified, <code>-id topo_id</code> takes precedence. For example: <code>em_snmpbrowser -host zack -id zeb:42</code> specifies a query for data on a host located on the remote MIS <code>zeb</code> via the local MIS <code>zack</code> , and 42 represents the <code>toponodeID</code> of the network component that is a child object to the remote MIS

## 8.17.2 Data Collections Command-Line Options

The following table describes the command options and parameters for the `em_datacollector` command, which is used to start Data Collections.

**TABLE 8-3** Data Collections Command-Line Options

Option	Parameter	Description
<code>-help</code>		Prints list of options (with descriptions) for the <code>em_datacollector</code> command.
<code>-host</code>	<i>hostname</i>	Specifies the <i>hostname</i> of a remote MIS For example: <code>em_datacollector -host silicon</code>
<code>-timeout</code>	<i>time-out</i>	Specifies the amount of time that the Data Collections tool waits for a connection to the MIS before being prompted for Wait Again or Exit responses. This option is referred to as the initialization time-out. For example: <code>em_datacollector -timeout 10</code>

---

## 8.18 More About Data Collection

### 8.18.1 Data Collections GDMO Classes

The following persistent GDMO classes are defined to enhance data collection:

- `dataCollector`—This is defined to represent data collection locations.
- `dataCollectorEntry`—This is defined to represent data collection requests.

## 8.18.2 The dataCollector GDMO class

This managed object class is defined as the container class for Data Collection Entry objects. The dataCollector object is defined by the GDMO class shown in the following code example.

**CODE EXAMPLE 8-1** Data Collections GDMO class

```
dataCollector MANAGED OBJECT CLASS
    DERIVED FROM "Rec. X.721 | ISO/IEC 10165-2 : 1992" : top;
    CHARACTERIZED BY
        dataCollectorPackage;
    REGISTERED AS { em-data-collector-class 1 };
dataCollectorPackage
    BEHAVIOUR dataCollectorPackageDefinition BEHAVIOUR DEFINED AS
        !The managed object class represents a data
collector object!
ATTRIBUTES
        dataCollectorId GET,
        "Rec. X.721 | ISO/IEC 10165-2 : 1992":
administrativeState;
    NOTIFICATIONS
        objectCreation,
        objectDeletion,
        attributeValueChange
    ;
```

## 8.18.3 The dataCollectorEntry Object GDMO Class

The dataCollectorEntry object is defined by the GDMO class in the following code example.

**CODE EXAMPLE 8-2**

```
dataCollectorEntry MANAGED OBJECT CLASS
    DERIVED FROM "Rec. X.721 | ISO/IEC 10165-2 : 1992" : top;
    CHARACTERIZED BY
        dataCollectorEntryPackage;
    REGISTERED AS { em-data-collector-class 2};
dataCollectorEntryPackage
    BEHAVIOUR dataCollectorEntryPackageDefinition BEHAVIOUR
DEFINED AS
    !The managed object class represents a data request!
ATTRIBUTES
    dataCollectorEntryId GET,
    requestInterval GET-REPLACE,
    requestInfo GET-REPLACE,
    requestStart GET-REPLACE,
    requestStop GET-REPLACE,
    logFile GET-REPLACE,
    logFileMaxSize GET-REPLACE,
    requestState GET-REPLACE,
    "Rec. X.721 | ISO/IEC 10165-2 : 1992":
administrativeState;
    NOTIFICATIONS
        objectCreation,
        objectDeletion,
        attributeValueChange
;
;
```



# 8.18.4 The RequestInfo Attribute

The syntax for the requestInfo attribute is shown in the following code example.

CODE EXAMPLE 8-3

```
RequestInfo ::= SET OF RequestData
    RequestData ::= SEQUENCE {
        objects ObjectInstance,
        attrs SET OF Attributed
    }
```

# 8.19 Error Messages

The following is a translation of error message from SNMP to CMIP, as seen in the browser.

TABLE 8-4 Error Messages

Version	SNMP Request	Agent SNMP Error	CMIS Error	Comments
2	ALL	tooBig	Complexity Limitation	
2	ALL	noSuchName	No Such Attribute	
1	ALL	badValue	Processing Failure	For CMIS GET request errorId should be snmpBadValue errorInfo should be variable binding identified by the error-index For CMIS DELETE request errorId should be cannotDelete errorInfo should be variable binding identified by the error-index.

**TABLE 8-4** Error Messages

Version	SNMP Request	Agent SNMP Error	CMIS Error	Comments
1		readOnly	Processing Failure	For CMIS GET request errorId should be snmpReadOnly errorInfo should be variable binding identified by the error-index For CMIS DELETE request errorId should be accessDenied errorInfo should be variable binding identified by the error-index.
1/2	ALL	genError	Processing Failure	errorId should be snmpGenErr errorInfo should be variable binding identified by the error-index
2	Set	noAccess	Invalid Operation	
2	Set	wrongType	Invalid Attribute Value	
2	Set	wrongLength	Invalid Attribute Value	For CMIS CREATE and SET requests
2	Set	wrongLength	Processing Failure	For CMIS DELETE request
2	Set	wrongEncoding	Processing Failure	
2	Set	wrongValue	Invalid Attribute Value	
2	Set	noCreation	Invalid Object Instance	
2	Set	inconsistentValue	Invalid Attribute Value	For CMIS CREATE and SET requests

**TABLE 8-4** Error Messages

Version	SNMP Request	Agent SNMP Error	CMIS Error	Comments
2	Set	inconsistentValue	Processing Failure	For DELETE request
2	Set	resourceUnavailable	Resource Limitation	
2	Set	commitFailed	Processing Failure	
2	Set	undoFailed	Processing Failure	
2	ALL	authorizationError	Access Denied	
2	Set	notWritable	Invalid Operation	
2	Set	inconsistentName	Processing Failure	



## Viewing Collected Data

---

The Results Browser enables you to view data obtained in a collection if the log file of the collection has been formatted in the SunNet Manager (SNM) format. For information about creating a collection and saving it in either Solstice EM or SNM format, see Chapter 8 "Gathering Attribute Data."

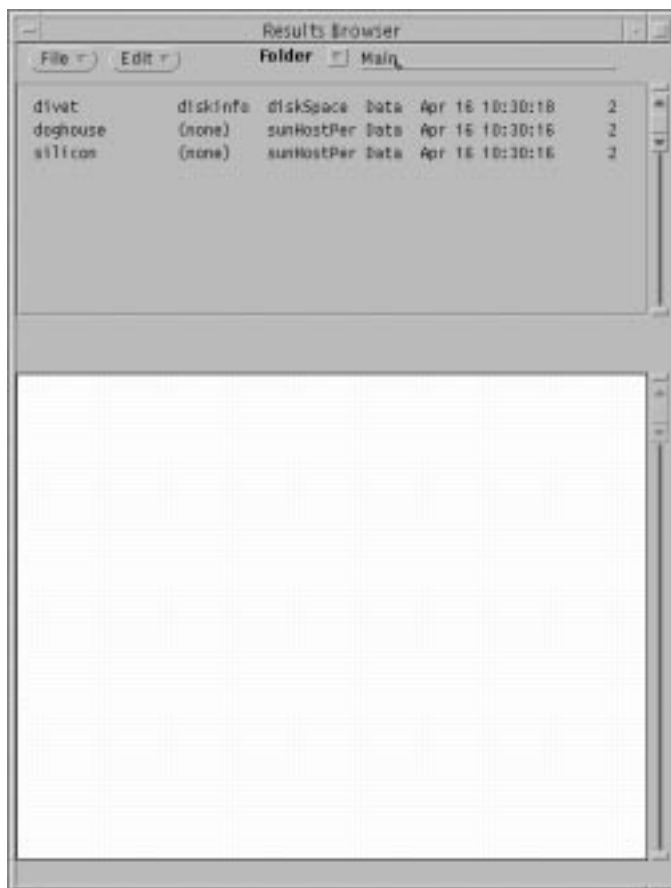
This chapter comprises the following topics:

- Section 9.2 "Getting Started With Results Browser" on page 9-4
- Section 9.3 "Loading Collections as Streams" on page 9-5
- Section 9.4 "Viewing Reports" on page 9-6
- Section 9.5 "Managing Reports" on page 9-6
- Section 9.6 "Selecting Streams" on page 9-8
- Section 9.7 "Displaying Streams in Grapher" on page 9-10
- Section 9.8 "Managing Folders" on page 9-10
- Section 9.9 "Customizing the Results Browser" on page 9-12

---

### 9.1 Overview

After collecting attribute data from an agent, you can view the information in the Results Browser if the log file of the collection was formatted in the default SNM format. You can view information about managed objects that you retrieved in the Data Collections tool. In the Results Browser, the content of each collection displays as a stream, a visual display of the native characteristics of the collection, such as the date and time on which the collection was created. Streams are organized in the Results Browser by type, including data and error streams. The following figure shows three data streams displayed in the Results Browser window.



**FIGURE 9-1** Results Browser Window

## 9.1.1 What Are Streams?

Streams are collections of the reports generated by a query in the Data Collections tool. Every time you query an agent for attribute data, this information is recorded in the log file of the collection that you created in the Data Collections tool. When you query again, the new information is appended to the log file of the collection. Each of these recordings of new attribute data is referred to as a report.

The Results Browser distinguishes streams by report type (data, event, error, and so on). For example, if a file contains both data reports and error reports resulting from an individual request, the data reports are listed in a separate stream from the error reports.

## 9.1.2 How Are Streams Defined?

Each stream is defined in the following format in the upper portion of the Results Browser window:

**TABLE 9-1** Type of Data Provided Per Stream

<i>system</i>	<i>agent</i>	<i>group</i>	<i>type</i>	<i>date</i>	<i>number of reports</i>
---------------	--------------	--------------	-------------	-------------	--------------------------

The following table defines each of the types of information provided in a stream.

**TABLE 9-2** Results Browser Report Stream Variables

Variable	Description
<i>system</i>	Name (up to 15 characters) of the target system, the host where the managed object resides
<i>agent</i>	Name of the agent
<i>group</i>	Name of the attribute group
<i>type</i>	Type of report (data, event, trap, error)
<i>date</i>	Time stamp of the original request from the manager
<i>number_of_reports</i>	Number of reports in the stream

## 9.1.3 What Are Reports?

Reports are the separate recordings of attribute data contained in a collection each time the collection is started. When you load a collection into the Results Browser, information about the file is displayed as a stream in the upper portion of the Results Browser window. When you double-click on a particular stream, it is displayed in bold font in the upper portion of the window. The individual reports derived from an agent comprise the content of each stream. When you select a stream, these reports are displayed in the lower portion of the Results Browser window in the order in which they were recorded in the collection. Thus, the first report of the stream appears as the topmost list item in a list of the collected attribute data that resulted from a query of an agent. You can specify a particular report to view, or you can scroll through all reports to view attribute data.

The list of attribute data, the content of a report, is displayed in the lower portion of the Results Browser window. Each report shows the values of the specific attributes for which you queried. For information about viewing reports, see Section 9.4 “Viewing Reports” on page 9-6.

## 9.1.4 What Are Folders?

Solstice Enterprise Manager provides folders into which streams are stored. A folder is a temporary place in which you can logically group streams and store them for reference. When you load a collection into the Results Browser, it is saved automatically into the default folder `Main`. You can also create other folders to contain groups of streams, and you can specify how streams will be grouped. See Section 9.8 “Managing Folders” on page 9-10 for more information.

## 9.1.5 Related Tasks

- Creating Data Collections—page 8-25
- Loading Data Into Grapher—page 10-3

## 9.1.6 Related Files

- `/opt/SUNWconn/em/bin/snm_br`

---

# 9.2 Getting Started With Results Browser

The Results Browser can be started from Data Collections or from the command line.

## ▼ To Use the Results Browser

### 1. Start the Results Browser in one of the following ways:

- From the Data Collections tool, select one or more SNM-formatted collections, then click **Actions->Results Browser**.
- From an operating system prompt, set environment variables specified in the `emenv.csh` or `emenv.sh` file, depending on your shell, by typing the following command:

```
source /opt/SUNWconn/em/bin/emenv.csh
```

Then, start the Results Browser by typing the following command:

```
/opt/SUNWconn/em/bin/snm_br filename1 filename2 ..
```

specifying the explicit path to each *filename*.



When you start the Results Browser from the command line, you can optionally specify files to be automatically loaded into the Results Browser. File names may include wildcards. When invoked without any file names specified, the Results Browser displays an empty Results Browser window.

2. **Perform any task discussed in this chapter.**
3. **Double-click the button in the upper-left corner of the Results Browser title bar when you are finished.**

---

## 9.3 Loading Collections as Streams

After retrieving information about the attributes of managed objects and saving this information in a collection in the Data Collections tool, you can load the collection in the Results Browser. All collections must be loaded in SNM or Solstice EM format, the formats native to SunNet Manager and Enterprise Manager, respectively. Once the file is loaded, its native characteristics, such as the server from which it originated, and the date and time it was created, are displayed as a horizontal flow of information referred to as a stream.

### ▼ To Load a File

1. **Click File->Load.**  
A dialog is displayed in which you can select a file.
2. **Click a file, or specify the path of the file you want to select in the dialog.**
3. **Click Load.**

The file is loaded into the Results Browser as a stream. To load another file, repeat these steps. You can load multiple files into the Results Browser, one at a time; however, you cannot specify wildcards in any file name.

---

**Note** – Because the Results Browser keeps open every file it reads, there is a limit to the number of files you can load in a Results Browser session. This limit is determined by the number of file descriptors allowed by the C-shell to a single process; the default is 64. You can increase this number up to 256 by using the `limit` command in the C-shell. You can also run multiple Results Browser sessions at the same time.

---

---

## 9.4 Viewing Reports

When you load a collection into the Results Browser, the native characteristics of the collection, such as the date and time when the collection was created, are automatically organized into a flow of information referred to as a stream. Streams are displayed in the upper portion of the Results Browser window. When more than one stream is displayed, the window provides a scroll bar.

### ▼ To View Reports

- **Double-click the stream that contains the reports you want to view.**

The first report of the stream is displayed in the lower portion of the Results Browser window.

### ▼ To View a Specific Report

- **Using the Report Line, type the number of a report in the Report field.**
- **Press Return.**

The report of the specified number is displayed in the lower portion of the Results Browser.

- **Using the Horizontal Scroll Bar, click and drag the rectangle of the horizontal scroll bar to select a number.**

The report of the selected number is displayed.

---

## 9.5 Managing Reports

In the Grapher tool, you can copy or clone, delete, and print the reports contained in a stream. You can also print all reports in a stream, and you can specify which reports to print.

## ▼ To Clone a Report

1. **Select the contents (the headers and attribute list) of the report you want to clone.**
2. **Right-click in the lower portion of the Results Browser window.**

The Report menu is displayed.

3. **Click Clone.**

The cloned report is displayed in a pop-up window. You can compare the report with other reports in the Results Browser.

## ▼ To Delete a Report

1. **Select the content of the report you want to delete.**
2. **Right-click in the lower portion of the Results Browser window.**

The Report menu is displayed.

3. **Click Delete.**

The report is deleted. To verify that the report is deleted, view the number of reports in the associated stream. If you had 375 reports initially, you have 374 reports after deleting the most recent report.

## ▼ To Print a Report

1. **Right-click in the lower portion of the Results Browser window.**

The Report menu is displayed.

2. **Click Print. Select Report from the Print menu.**

---

**Note** – From this menu, you also can print all reports in the stream by clicking Entire Stream, and you can print all reports in the stream beginning with the currently displayed stream by clicking Stream From Here.

---

---

## 9.6 Selecting Streams

You can select a stream or multiple streams by system, agent group, or report type. For example, you can select all streams of the same report type, such as the data streams type of report, simultaneously. You select one or more streams to:

- Select a single stream, multiple streams, or a group of similar streams
- Delete a stream
- Print a stream

### ▼ To Select Streams

- In the upper portion of the Results Browser window, click a single stream to select it.
- Click additional streams to select multiple streams at once.

### ▼ To Select All Streams of a Particular System, Group, or Report Type

1. Right-click in the upper portion of the Results Browser window.
2. Click Select in the Streams menu.
3. Select the option to use for selecting streams:
  - a. **By System**—Enables you to simultaneously select all streams that were derived from collection files created on the same system.
  - b. **By Agent Group**—Enables you to simultaneously select all streams that received information from the same agent.
  - c. **By Report Type**—Enables you to simultaneously select all streams of the same type: Data, Error, Event, Set, or Trap.

When you have made your selection, the selected streams are highlighted in the upper portion of the Results Browser window. To change your selection, for example, if three streams are selected but you only want to select two, click the stream that you do not want to select.

## ▼ To Delete a Stream

1. **Select the stream you want to delete.**

You can also select multiple streams to delete.

2. **Right-click in the upper portion of the Results Browser window.**
3. **Click Streams -> Delete.**

The stream is deleted.

## ▼ To Clear All Choices

You can clear all selected streams to make a different selection or to deselect a large series of streams rather than clicking one at a time.

1. **Right-click in the upper portion of the Results Browser window**
2. **Click Streams -> Clear All Choices.**

Selected streams are deselected.

## ▼ To Print a Stream

*To Print An Entire Stream*

1. **Select the stream you want to print.**
2. **Right-click in the lower portion of the Results Browser window.**
3. **In the Report menu, click Print -> Entire Stream.**

The selected stream is printed.

*To Print a Partial Stream From the Current Report*

1. **Right-click in the lower portion of the Results Browser window.**
2. **In the Report menu, click Print -> Stream From Here.**

All reports, from the current one to the final report of the stream, are printed.

---

## 9.7 Displaying Streams in Grapher

After viewing information in the Results Browser, you can plot it as a graph in the Grapher tool. You can graph multiple streams and merge information from more than one stream into one graph. See Chapter 10 "Graphing Collected Data" for more information about the tasks you can complete using the Grapher tool.

### ▼ To Display Streams in Grapher

1. Select the streams you want to graph.
2. Right-click in the upper portion of the Results Browser window.
3. In the Streams menu, click Graph and select one of the listed attribute names.

---

## 9.8 Managing Folders

A folder is a *temporary* place to logically group streams and store them for reference during a Results Browser session. Solstice EM provides the default folder `Main` for storage of report streams. When you load a file into the Results Browser, you automatically load it into `Main`. You can also create folders of your own and manage multiple folders using the following procedures.

---

**Note** – The default folder `Main` cannot be renamed.

---

## ▼ To Create a New Folder

1. Click **Edit->New Folder** in the **Results Browser** window.
2. Click the down arrow in the **Folder** field and select **New Folder** from the menu.  
A folder named “New Folder” is created.

## ▼ To Rename a Folder

After creating a folder, you can rename it.

1. Delete the default name **New Folder** in the **Folder** field.
2. Type a new name for the folder.
3. Press **Return**.  
Your folder is renamed.

## ▼ To Load Files Into a Folder

1. Click **File->Load** in the **Results Browser** window.
2. Select the path to the file you want to load.
3. Click **Load**.

## ▼ To Copy a Stream to a Folder

1. Select the stream you want to copy.
2. Right-click in the upper part of the **Results Browser** window.
3. In the **Streams** menu, click **Copy To** and select the folder to which you want to copy the stream.

## ▼ To Empty a Folder of All Its Streams

- Click **Edit->Empty Folder**.

## ▼ To Delete a Folder

- **Click Edit->Delete Folder.**

Folder names and their contents are no longer displayed.

---

**Note** – The default folder `Main` cannot be deleted. It can be emptied.

---

## ▼ To Save the Contents of a Folder

When you save the contents of a folder, you save the folder as a file.

1. **Click File->Save Folder.**

A dialog prompts for a path to the file in which you want to save the folder contents.

2. **Select a path and file name, and then click Save.**

In a future Results Browser session, you can load this file to view and manage the same set of streams.

---

**Caution** – Do *not* attempt to save the contents of a folder into a file that contains reports that are currently loaded into the Results Browser. This will corrupt the file. Because collection files may be large, individual reports are not kept in memory. Instead, pointers to the files are maintained. Therefore, if a file is overwritten while it is open, the file is destroyed and the pointers to the file become corrupted.

---

---

## 9.9 Customizing the Results Browser

You can customize the Results Browser in the following ways:

- Change the position of the Results Browser window when it opens on your desktop
- Change the size of the Results Browser window
- Specify where to print the contents of a stream
- Define an output size for report streams
- Specify the format and layout of a report



## 9.9.1 Changing the Window Position

The window position defines the location (in pixels) where the Results Browser window is displayed on your screen when you start the tool. Default values are 300 and 100 for X and Y locations, respectively.

### ▼ To Change the Window Position

1. Click **Edit->Tool Properties**.
2. In the **Properties** dialog, type a number or click the up and down arrows in the **Window Position** fields to set the X and Y values of the window coordinates.
3. Click **Save** to change default settings.

## 9.9.2 Changing the Window Size

The window size defines the dimensions (in pixels) of the Results Browser window. Default values are 512 and 640 for X and Y dimensions, respectively.

### ▼ To Change the Window Size

1. Click **Edit -> Tool Properties**.
2. In the **Properties** dialog, type a number or click the up and down arrows in the **Window Size** fields to set the X and Y values of the window coordinates.
3. Click **Save** to change default settings.

## 9.9.3 Specifying a Printer

You can specify a default printer, including the printer name and the print commands.

---

**Note** – `lpr` is the default print command for Solaris 1.1 installations and compatible versions. `lp` is the default print command for Solaris 2.0 installations and compatible versions.

---

## ▼ To Specify a Printer

1. Click Edit -> Tool Properties.
2. In the Properties dialog, type the print command and the printer name to which you want to print in the Print Option field. For example: `lpr -P printer filename`
3. Click Save to change default settings.

### 9.9.4 Defining an Output Size

For streams of 100 kilobytes (KBytes) or more, you can define a maximum output size for printing streams. For any output that exceeds the specified size, you will be asked to confirm whether you want to print the reports.

## ▼ To Define an Output Size

1. Click Edit -> Tool Properties.
2. In the Properties dialog, type either type a numeric value or click the up and down arrows to set a number of kilobytes in the Verify Printing More Than \_\_\_\_ Kilobytes field.
3. Click Save to change default settings.

### 9.9.5 Setting the Format for Reports

You can define the appearance and contents of reports in the lower portion of the Results Browser window. By toggling on or off the buttons in the Report Format field of the Properties dialog, you control the display of the following stream characteristics:

- Stream name
- Time requested
- Time sent
- Time logged
- Status codes
- Attributes

By default, all of these choices are selected, which causes all report information to be displayed in the report window. You can also choose to display attribute names left- or right-justified. By default, attribute names are displayed right-justified.

## ▼ To Set Report Formats

1. Click **Edit->Tool Properties**.
2. In the **Properties** dialog, click the buttons of the **report formats** field to select or deselect a characteristic to display.
3. Click **Left** or **Right** in the **Justified** field to select whether reports will be listed as left or right justified.

---

**Note** – When the buttons appear as gray color darker than that of the dialog, the buttons are selected. The selected format characteristics will be displayed in the lower portion of the Results Browser window. When the buttons appear as a color of gray the same color as the dialog, and when they appear to be raised, the buttons are deselected. The selected format characteristics will not be displayed in the lower portion of the Results Browser window.

---



# Graphing Collected Data

---

Solstice Enterprise Manager (Solstice EM) provides the Grapher tool for graphing trends in attribute or alarm data. The graphs are useful for viewing trend data and identifying areas for improvement over time.

This chapter comprises the following topics:

- Section 10.2 “Getting Started With Grapher” on page 10-2
- Section 10.3 “Loading Data Into Grapher” on page 10-3
- Section 10.4 “Displaying Graphs” on page 10-4
- Section 10.5 “Selecting Streams to Display as Graphs” on page 10-4
- Section 10.6 “Displaying Graphical Dimensions” on page 10-5
- Section 10.7 “Plotting Values in Different Ways” on page 10-6
- Section 10.8 “Changing Viewing Angles in 3-D Graphs” on page 10-6
- Section 10.9 “Setting Graph Colors” on page 10-8
- Section 10.10 “Changing the Display of the Plotted Data” on page 10-10
- Section 10.11 “Saving a Graph to a File” on page 10-12
- Section 10.12 “Printing a Graph” on page 10-12
- Section 10.13 “Replotting a Graph” on page 10-13
- Section 10.14 “Merging Graphs” on page 10-13

---

## 10.1 Overview

Using the Grapher tool, you can plot attribute or alarm data as two-dimensional line graphs or three-dimensional bar graphs. The following figure shows an example of a trend plotted as a 3-D graph.

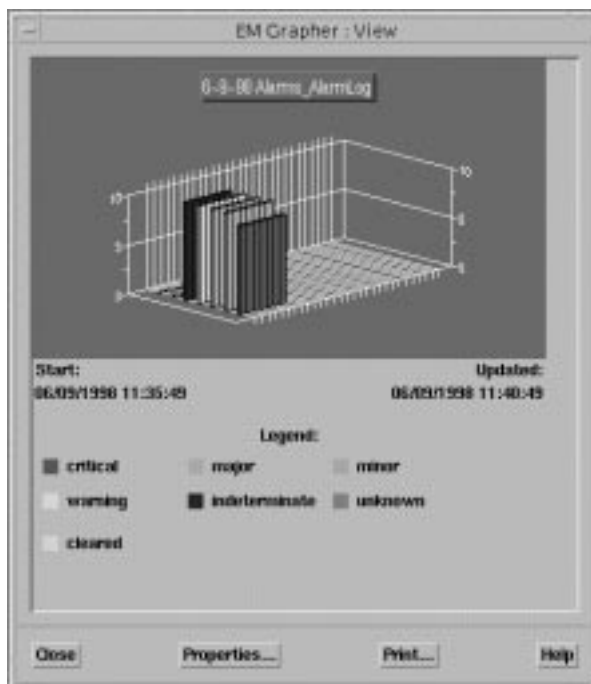


FIGURE 10-1 Trends in Alarm Data Plotted in the Grapher View Dialog

---

## 10.2 Getting Started With Grapher

To display a graph of data in the Grapher, you must have already collected attribute data in Data Collections and displayed it in the SNM Results Browser.

## ▼ To Use Grapher

### 1. Start Grapher in one of the following ways:

- In the SNM Results Browser, right-click in the upper region, then click Graph in the Streams menu.
- In the Alarm Manager window, click Tools->Grapher. In the Alarms - Graph dialog:
  - In the Name field, type a name for the graph.
  - In the Input field, select whether you want to graph alarm summary data or data about selected devices.
  - In the Plot field, select whether you want to graph data by alarm type as a function of count or severity as a function of count.
  - In the Type field, select whether you want the graph to be a static display of current data or a dynamic display that changes according to a specified time interval as data is updated.
  - If you choose to create a dynamic graph, the Update interval field becomes active and you can specify a time interval, in minutes, for updating the graph.

Click OK. The Grapher window displays, listing all graphs that you created. Double-click the name of the graph you want to view or select the name and click Object->View. The Grapher: View dialog displays the graph according to your specifications.

- From an operating system prompt, execute: `em_grapher`

### 2. Perform any task discussed in this chapter.

### 3. Click File->Close in the Grapher window when you are finished.

---

## 10.3 Loading Data Into Grapher

When you start the Grapher tool from the SNM Results Browser, the attributes you want to graph display as a stream. By starting the Grapher from the command line, you need to import the file that you want to graph.

## ▼ To Load a File

- Click File->Import and, in the Import Graph dialog, select the file to be graphed.

---

## 10.4 Displaying Graphs

Once you have loaded the streams of information that you want to view as graphs, you can graph the information by double-clicking the stream.

### ▼ To Display a Graph

1. **Click the attribute stream that you want to plot.**
2. **Click Object->View.**

The View dialog displays containing the graph.

---

## 10.5 Selecting Streams to Display as Graphs

You can select one or more graphs to display, you can deselect any selections, and you can delete streams listed in the Grapher window.

### ▼ To Select All Streams

- **Click Edit->Select All in the Grapher window.**

### ▼ To Deselect All Streams

- **When all streams are selected, click Edit->Deselect All to deselect them.**

### ▼ To Delete a Selected Stream

- **Click Edit->Delete in the Grapher window.**



---

## 10.6 Displaying Graphical Dimensions

In the Grapher, you can select to display your graphs as two-dimensional line graphs or three-dimensional bar graphs. The default setting is three dimensions.

You can also set the features of the graph including the colors of the graph, and the mode in which to view the graph, whether you use absolute, cumulative, or delta values for plotting.

### ▼ To Display a Graph in 2-Dimensions

1. After displaying a graph, click **Properties in the View dialog**.

2. Move the **Properties dialog adjacent to the View dialog**.

In this way, you can compare selections that you make in the Properties dialog with their effect on the graph in the View dialog.

3. Click the **2-D button in the Display in field in the Properties dialog**.

4. Click **Apply to view the change in the appearance of the graph**.

5. Click **OK to accept the change**.

### ▼ To Display a 2-Dimensional Graph in 3-Dimensions

1. After displaying a graph, click **Properties in the View dialog**.

2. Move the **Properties dialog adjacent to the View dialog**.

In this way, you can compare selections that you make in the Properties dialog with their effect on the graph in the View dialog.

3. Click the **3-D button in the Display in field of the Properties dialog**.

4. Click **Apply to view the change in the appearance of the graph**.

5. Click **OK to accept the change**.

---

## 10.7 Plotting Values in Different Ways

In the Grapher tool, you can plot information in three ways:

- Absolute
- Cumulative
- Delta

Absolute plots all current values. Cumulative plots, in increments, data that has been obtained over time. Delta plots the difference between the current value and the previous value.

### ▼ To Plot Values in Different Ways

1. **After displaying a graph, click Properties in the View dialog.**
2. **Move the Properties dialog adjacent to the View dialog.**

In this way, you can compare selections that you make in the Properties dialog with their effect on the graph in the View dialog.

3. **Select the option in the Plot Value field to select Absolute, Cumulative, or Delta. Notice the differences in how the data is plotted in the graph.**
4. **Click Apply to view the change.**
5. **Click OK to accept the change.**

---

## 10.8 Changing Viewing Angles in 3-D Graphs

To view the information displayed in 3-D graphs from different angles, you can rotate the graph:

- Vertically along the X-axis
- Diagonally along the Y-axis
- Horizontally along the Z-axis

## 10.8.1 Changing the X-Axis, Vertical Rotation

Rotating the graph along the X-axis causes the graph to turn vertically toward you. You can look down at the graph from the top between 80 and 90 degrees, or up into the graph from the bottom between 270 and 280 degrees, or you can set the X-axis to 0 degrees for a two-dimensional representation of the bar graph. The default setting of the X-axis is 15 degrees.

### ▼ To Change the Vertical Rotation

1. **After displaying a graph, click Properties in the View dialog.**
2. **Move the Properties dialog adjacent to the View dialog.**  
In this way, you can compare selections that you make in the Properties dialog with their effect on the graph in the View dialog.
3. **Drag the scroll bar left or right in the X-Axis field of the Properties dialog to change settings.**
4. **Click Apply to view the change in the appearance of the graph.**
5. **Click OK to accept the change.**

## 10.8.2 Changing the Y-Axis, Diagonal Rotation

Rotating the graph on the Y-axis causes the graph to turn diagonally away from you. The default setting of the Y-axis is 0 degrees.

### ▼ To Change the Diagonal Rotation

1. **After displaying a graph, click Properties in the View dialog.**
2. **Move the Properties dialog adjacent to the View dialog.**  
In this way, you can compare selections that you make in the Properties dialog with their effect on the graph in the View dialog.
3. **Drag the scroll bar left or right in the Y-Axis field of the Properties dialog to change settings.**
4. **Click Apply to view the change in the appearance of the graph.**
5. **Click OK to accept the change.**

## 10.8.3 Changing the Z-Axis, Horizontal Rotation

Rotating the graph on the Z-axis causes it to turn horizontally. Side views of the graph, which show all lines plotted on a 3-D graph, can be seen at 90 degrees and 270 degrees. At 180 degrees, you view the graph from the back. The default setting of the Z-axis is 45 degrees.

### ▼ To Change the Horizontal Rotation

1. **After displaying a graph, click Properties in the View dialog.**
2. **Move the Properties dialog adjacent to the View dialog.**  
In this way, you can compare selections that you make in the Properties dialog with their effect on the graph in the View dialog.
3. **Drag the scroll bar left or right in the Z-Axis field of the Properties dialog to change settings.**
4. **Click Apply to view the change in the appearance of the graph.**
5. **Click OK to accept the change.**

---

## 10.9 Setting Graph Colors

The Data Area and the Background are charcoal gray by default. The Mesh is light gray by default. The Foreground is white by default. The Grapher tool assigns default colors for each attribute plotted as a line or a bar on the graph.

You can change the color of the graphical display in the Grapher tool, which consists of four colored regions:

- Background, which consists of the area behind the graph and attribute heading
- Foreground, which consists of the axis lines, demarcation lines, measurements, and name heading that serves as the title of the graph
- Data Area, which refers to the area within the perimeter of the graph
- Mesh, which refers to the vertical increment lines that form a mesh with the horizontal increment lines

## ▼ To Change the Background Color

1. After displaying a graph, click **Properties** in the **View** dialog.
2. Move the **Properties** dialog adjacent to the **View** dialog.  
In this way, you can compare selections that you make in the **Properties** dialog with their effect on the graph in the **View** dialog.
3. Click **Background Color** in the **Properties** dialog.
4. Click a square in the **Background Color** dialog to select a background color.
5. Click **Apply** to view the change in the appearance of the graph.
6. Click **OK** to accept the change.

## ▼ To Change the Foreground Color

1. After displaying a graph, click **Properties** in the **View** dialog.
2. Move the **Properties** dialog adjacent to the **View** dialog.  
In this way, you can compare selections that you make in the **Properties** dialog with their effect on the graph in the **View** dialog.
3. Click **Foreground Color** in the **Properties** dialog.
4. Click a square in the **Foreground Color** dialog to select a foreground color.
5. Click **Apply** to view the change in the appearance of the graph.
6. Click **OK** to accept the change.

## ▼ To Change the Color of the Data Area

1. After displaying a graph, click **Properties** in the **View** dialog.
2. Move the **Properties** dialog adjacent to the **View** dialog.  
In this way, you can compare selections that you make in the **Properties** dialog with their effect on the graph in the **View** dialog.
3. Click **Data Area Color** in the **Properties** dialog.  
The **Data Area Color** dialog displays.
4. Click a square in the **Data Area Color** dialog to select a color for the data area.

5. Click **Apply** to view the change in the appearance of the graph.
6. Click **OK** to accept the change.

## ▼ To Change the Mesh Color

1. After displaying a graph, click **Properties** in the **View** dialog.
2. Move the **Properties** dialog adjacent to the **View** dialog.  
In this way, you can compare selections that you make in the **Properties** dialog with their effect on the graph in the **View** dialog.
3. Click **Mesh Color** in the **Properties** dialog.
4. Click a square in the **Mesh Color** dialog to select a color for the mesh increment lines.
5. Click **Apply** to view the change in the appearance of the graph.
6. Click **OK** to accept the change.

---

## 10.10 Changing the Display of the Plotted Data

You can change how the plotted data displays in the graph by specifying which attribute information to display and designating the color of plotted lines and bars.

## ▼ To Plot a Specific Attribute

1. After displaying a graph, click **Properties** in the **View** dialog.
2. Move the **Properties** dialog adjacent to the **View** dialog.  
In this way, you can compare selections that you make in the **Properties** dialog with their effect on the graph in the **View** dialog.
3. Click an attribute to plot in the **Dataset** field.

---

**Note** – In the **Dataset** field, you select attributes one at a time.

---

4. Click **Yes** in the **Visible** field to display the attribute.

5. Click **Apply** to view the change in the appearance of the graph.
6. Click **OK** to accept the change.

## ▼ To Remove Plotted Information

1. After displaying a graph, click **Properties** in the **View** dialog.
2. Move the **Properties** dialog adjacent to the **View** dialog.  
In this way, you can compare selections that you make in the **Properties** dialog with their effect on the graph in the **View** dialog.
3. In the **Dataset** field, click a plotted attribute to remove from the graph.

---

**Note** – In the **Dataset** field, you select attributes one at a time.

---

4. Click **No** in the **Visible** field to remove the displayed attribute from the graph.
5. Click **Apply** to view the change in the appearance of the graph.
6. Click **OK** to accept the change.

## ▼ To Select a Color for the Plotted Data

1. After displaying a graph, click **Properties** in the **View** dialog.
2. Move the **Properties** dialog adjacent to the **View** dialog.  
In this way, you can compare selections that you make in the **Properties** dialog with their effect on the graph in the **View** dialog.
3. Click an attribute in the **Dataset** field.
4. Ensure that **Yes** is selected in the **Visible** field to display the attribute in the graph.
5. Click **Color**.  
The **Data Set Color** dialog displays.
6. Click a square in the **Data Set Color** dialog to select a color for the attribute that you want to display on the graph.
7. Click **Apply** to view the change in the appearance of the graph.
8. Click **OK** to accept the change.

---

## 10.11 Saving a Graph to a File

When you have finished working on a graph, you can save it to a file.

- **Click File->Export and, in the Export Graph dialog, select the file to which you want to save the graph.**

---

## 10.12 Printing a Graph

You can print any graph you create to a PostScript® file or to a printer.

### ▼ To Print a Graph to a PostScript File

1. **Click Print in the View dialog.**
2. **In the Print dialog:**
  - a. **Click the button of the Print to file field.**
  - b. **Type the path and name of the file to which you want to save.**
  - c. **Click OK.**or
  - a. **Click the ellipsis (...) button.**
  - b. **Select a path and file from the File Selection dialog.**
  - c. **Click OK.**
3. **Click OK in the Print dialog.**

The information is sent to the PostScript file you specified.



## ▼ To Send a Graph to the Printer

1. Click **Print** in the **View** dialog.
2. Click the button of the **Printer** field.
3. Select a configured printer by clicking the down arrow of the **Printer** field.
4. Click **OK**.

The graph is sent to the printer you specified.

---

## 10.13 Replotting a Graph

You can replot a graph at any time by clicking **Object->View**.

---

## 10.14 Merging Graphs

You can superimpose graphs on one another by selecting more than one stream in the **Grapher** window and clicking **Object->View** to graph them.



## Examining Log Entries

---

By using Solstice Enterprise Manager (Solstice EM) Log Entries tool, you can browse the contents of log files and view the details of log entries. Log Entries gives you detailed information on events that have occurred on your network. Log files and log entries are an important network management tool, particularly in the areas of configuration, alarm, and security management.

This chapter comprises the following topics:

- Section 11.2 “Getting Started With Log Entries” on page 11-3
- Section 11.3 “Changing the Log Entry Display” on page 11-4
- Section 11.4 “Viewing Log Entry Details” on page 11-6
- Section 11.5 “Filtering Log Entries” on page 11-6
- Section 11.6 “Combining Log Entries in a Single View” on page 11-7
- Section 11.7 “Searching for Log Entries” on page 11-8
- Section 11.8 “Printing and Deleting Log Entries” on page 11-9
- Section 11.9 “Adding and Removing Solstice EM Tools” on page 11-9

---

### 11.1 Overview

Log files are software entities that collect data of events that occurred on your network. Agents that monitor the network components create event notifications when they detect a change in the state of a managed resource. When such event notifications arrive at the MIS, a filtering test—called a *discriminator construct*—is performed on the event notification to determine whether or not to discard it. If the event notification passes the filtering test, Solstice EM writes the event notification in the designated log file.

The Solstice EM installation provides you with the `AlarmLog` file. This default log file may be sufficient for your needs. If not, Solstice EM’s Event Logs tool enables you to create any number of log files to meet your specific needs. Depending on

your Solstice EM configuration, you may have more than one log file. Using Log Entries, you can examine the log entries file by file, or you can combine the log records in a single view. No log size limitation forces old records to be removed.

See the *Customizing Guide* for more information about using Event Logs to create log files and about log attributes.

### 11.1.1 Log Entries in the AlarmLog File

By default, the AlarmLog will record the following events:

- SNMP trap notifications (alarms forwarded from remote SNM managers by Cooperative Consoles)
- Nerve Center alarms
- OSI standard alarms

The following events and attributes are, by default, explicitly excluded from AlarmLog:

- SNM event notifications generated by SNM RPC agents
- attributeValueChange
- objectCreation
- objectDeletion
- stateChange

If you wish to view SNM RPC event notifications plus the above event attributes, you should create log files using Solstice EM's Event Logs tool.

Although the log records and the attributes you see in the Log Entry window depend upon what was specified during the creation of the log files using the Event Logs tool, Log Entries enables you to specify display and filtering properties to facilitate the examination of log entries.

### 11.1.2 Related Files

The `.em_logview.cf` configuration file – The Log Entries configuration file in your home directory or in the `$EM_HOME/config` directory.

### 11.1.3 Related Tasks

- “Event Logs” chapter in the *Customizing Guide*
- Chapter 5 “Managing Alarms”
- Chapter 6 “Controlling User Access”

## 11.1.4 Further Reading

See the *Customizing Guide* and *API Development Guide* for related information.

---

## 11.2 Getting Started With Log Entries

All operations pertaining to viewing log records are performed in the Log Entries window which displays when you start Solstice EM's Log Entries tool.

You start the Log Entries tool from any of the following places:

- Network Views window
- Network Tools window
- Event Log window
- The operating system command line.

If Solstice EM Security has been enabled, your access privileges determine your ability to run Log Entries, look at log entry data, and purge the log files. See Chapter 6 "Controlling User Access" for more information on defining user access.

### ▼ To Use Log Entries

#### 1. Start Log Entries in one of the following ways

- From the Network Views window, click Tools->Log Entries.
- From the Network Tools window, click Log Entries.
- From the Event Logs window, click Tools->Log Entries, or double-click a specific log.
- From an operating system prompt, enter the following command: `em_logview`.  
See Section 11.10.1.1 "The `em_logview` Command" on page 11-11 to ensure the configuration settings are correct.

#### 2. Perform any of the tasks discussed in this chapter.

#### 3. Click File->Exit.

##### See Also:

- "Command Line Options" on page 11-11
- Chapter 5 on event logs in the *Customizing Guide*

---

## 11.3 Changing the Log Entry Display

You can customize the way you view log records in the Log Entry window. By default, the Log Entry window shows the log records sorted by log record number, and identifies them by the following attributes:

- Event type
- Date at which the events were recorded in the log file
- Agent that sent the event

Solstice EM enables you to customize the default view to suit your personal needs and preferences, such as:

- Including and excluding log entry attributes from the display
- Changing the column order
- Organizing the order in which log entries are shown
- Customizing the column labels in the Log Entries window

These viewing properties can be set individually or all at once.

### ▼ To Include and Exclude Log Entry Attributes

1. **Click View->Column Headings to display the Column Headings dialog.**

Hidden Attributes lists the log entry attributes not currently shown in the Log Entry window, while Shown Attributes lists the attributes displayed in the window.

2. **Proceed as follows:**

- To exclude attributes from the window display, select one or several attributes in Shown Attributes and click Hide.
- To include attributes not currently shown, select one or several attributes in Hidden Attributes and click Show.

3. **Click OK.**

### ▼ To Change the Column Order

1. **Click View->Column Headings to display the Column Headings dialog.**
2. **In Shown Attributes, select the attribute you wish to be shown as the first column from the left and click either Move Up or Move Down so that it is in first position.**

3. Select the attribute you wish to be shown as the second column and, again, click Move Up or Move Down until it is in second position.
4. Repeat steps 2 or 3 as necessary.
5. Click OK.

## ▼ To Organize the Sort Order of Log Entries

1. Click View->Column Headings to display the Column Headings dialog.
2. Click Sort Order to display the Sort Order dialog.
3. Define the attributes that should be used for the sort order:
  - To remove attributes, select them in Sort Order and click Remove.
  - To include attributes, select them in All Attributes and click Add.

The Sort Order box now lists all the attributes to be included in the sort order.
4. Specify the priority of the sort order:
  - a. In the Sort Order box, select the first attribute and click Move Up or Move Down.
  - b. Still in Sort Order, select the second attribute and click Move Up or Move Down.
  - c. Repeat as often as necessary.
  - d. Click OK to return to the Column Headings dialog.
5. Click OK.

## ▼ To Customize the Column Labels

1. Click View->Column Headings to display the Column Headings dialog.
2. In Display Column Headings, select User Defined Headings, and click Edit Names to display the Edit Names dialog.

Default Name shows the current label names of the columns.
3. In User Defined Name, type the new column name.
4. Click OK to return to the Column Headings dialog.
5. Click OK.

---

## 11.4 Viewing Log Entry Details

By default, the Log Entry window comes up in its basic form, showing only a minimum of log record details. The window can be expanded to reveal all attribute values pertaining to a specific log entry.

### ▼ To View Log Entry Details

1. Select a log entry in the main window and click **Record Details**.
2. Move the sash up or down to reveal more or less of the log entry details.



FIGURE 11-1 Controls for Viewing Details of Log Entries

---

## 11.5 Filtering Log Entries

Log files typically contain a lot of log entries which makes viewing the records a cumbersome effort. Solstice EM enables you to temporarily remove log entries from the Log Entry window display so that you can concentrate on those of interest.

You can filter log entries based on the following:

- Object instances
- Object classes
- Event types
- Alarms

When setting filter criteria, before you exit the Filter dialog, you can save filter criteria to a file. Saved filter criteria can then be reused whenever necessary. You can also print the filter criteria to a file or to a printer.



## ▼ To Filter Log Entries

1. Click **View->Filter Properties** to display the Log Filter dialog.
2. Click the **Include** list box to reveal the filter options, and select a filter option.
3. Click **Apply**.
4. (Optional) Click **Save** to Save the current filter criteria.
5. (Optional) Click **load** to reuse a previously saved filter file and apply the criteria to the current display.
6. (Optional) Click **Print** to print the current filter criteria.
7. When done, click **OK**.

---

## 11.6 Combining Log Entries in a Single View

When looking at log entries, you can examine the log entries from individual log files, or merge the log entries from several log files into one single view, as if the log entries were recorded in one file. When log entries from several log files are combined into a single you, you then use filter criteria to remove certain log entries temporarily from the display to facilitate your examination of the log entries.

## ▼ To Combine Log Entries in a Single View

1. Click **View->Log Selection** to open the Log Selection dialog.  
See Section 11.5 “Filtering Log Entries” on page 11-6 for more information about the dialog options.
2. **Proceed as follows:**
  - To add log entries from available log files, in Available Logs select the log file and click **Display**.
  - To remove log entries from open log files, in Available Logs select the log file and click **Remove**.
3. Click **OK**.

**See Also** “Filtering Log Entries” on page 11-6

---

## 11.7 Searching for Log Entries

Solstice EM provides you with a search mechanism to quickly find the log entries of interest.

The case-sensitive text string you type must match in whole or in part any of the attributes shown in the Log Entry window. For example, you are looking for records pertaining to changes in attribute values recorded by *attributeValueChange*. If you type `valueChange`, `value` or `Change`, Solstice EM will find any log entries that reported changes in attribute values. However, if you type `value change` (lowercase characters and space between the words), `value` or `change`, Solstice EM will not find the log entries and display a “Text not found” message. Other strings can be any number, for example, 95.

### ▼ To Search for Log Entries

1. Click **Actions->Find** to display the Find dialog.
2. In **Find Text**, type the case-sensitive text string to be used for searching.
3. **Start the search as follows:**
  - Click **Find** to start a forward search.
  - Click **Find** again to continue the forward search.
  - Click **Previous** to change the search direction and find the previous log entry.
4. Click **Close**.

---

## 11.8 Printing and Deleting Log Entries

Delete log entries when you have finished examining them. Remember that you can always keep a record of the log entries by printing them or saving them to a file. Solstice EM will remove any data of the deleted log entries from the log file in the MIS.

### ▼ To Print Log Entries

1. Select one or more log entries in the Log Entries window.
2. To look at the log entry details of selected log entries, click Record Details to expand the Log Entries window.
3. Click Print to display a Print dialog.
4. Choose to print to a file or to a printer.
5. Click Print.

### ▼ To Delete Log Entries



---

**Caution** – Deleted log entries cannot be retrieved from the MIS.

---

1. Select one or more log entries in the Log Entries window.
2. Select Actions->Delete.

---

## 11.9 Adding and Removing Solstice EM Tools

Solstice EM enables you to add to the Tools menu any tools and other custom-developed applications that you either use frequently with Log Entries, or to which you wish to have quick access from any Solstice EM tool. At any point in time you can remove any tools added to the Tools menu.

Step-by-step procedures for adding and removing tools to the Tools menu follow.

## ▼ To Add Tools to the Tools Menu

1. **Click File -> Customize Tools Menu to display the Log Entries Customize Tools Menu dialog.**
2. **In Application Name, type a name that will enable you to recognize the tool, such as the name of the tool's executable or its commercial name.**  
For example, `em_logview` or `Log Entries tool`.
3. **In Path To Executable, type the path name of the tool's executable file.**  
The default is `/opt/SUNWconn/em/bin/em_logview`.
4. **In Arguments, type any desired command variables associated with and recognized by the tool's executable.**
5. **Click Add.**  
The tool's name is added to the list of tools at the top of the dialog.
6. **Click OK.**

## ▼ To Remove Tools From the Tools Menu

1. **Click File->Customize Tools Menu to display the Log Entries Customize Tools Menu dialog.**
2. **In Applications at the top of the dialog, select the tool you want to remove.**
3. **Click Delete.**
4. **Click OK.**

---

## 11.10 Reference

This section provides technical reference information about command-line options for log entry operations.

For detailed information about dialogs, menus, and other user interface elements, refer to the Solstice EM Online Help. To access Online Help, click the Help button on any dialog box or select options from the Help menu located in the upper right corner of each Solstice EM tool window.

## 11.10.1 Command Line Options

Reference information is available for the following:

- The `em_logview` Command—page 11-11
- The `em_nnconfig` Utility—page 11-11

### 11.10.1.1 The `em_logview` Command

The `em_logview` command is the executable to start the Log Entries tool. Before you start Log Entries from the command line, make sure the `$XFILESEARHPATH` environment variable is set. If you installed Solstice EM in the default location, it should point to `/opt/SUNWconn/em/config`. If this environment variable is not set, the fonts, colors, and backgrounds may not display correctly.

The command syntax is: `em_logview [options]`

The following table describes the command options.

**TABLE 11-1** `em_logview` Command Options

Option	Description
<code>-help</code>	Print a descriptive list of command options for the <code>em_logview</code> command.
<code>-host hostname</code>	Specify the name of a remote MIS server. For example: <code>em_logview -host omega</code> . Instead of a host name, you can specify an IP address as the host name. For example: <code>em_logview -host 123.345.678.900</code> .
<code>-c filename</code>	Specify the file name of the configuration file. For example: <code>em_logview -c .em_mylogview.cf</code> .
<code>-logobj fdn</code>	Display the log records of the specified log file in the main window summary table. For example: <code>em_logview snmp_router_log</code>

### 11.10.1.2 The `em_nnconfig` Utility

The `em_nnconfig` utility enables you to create and map nicknames to an object's Full Distinguished Name.

See Chapter 4 of the *Developing C++ Applications Guide* for related information.

### 11.10.1.3 Log Entries Configuration File

Upon start-up, the Log Entries tool looks for the `.em_logview.cf` configuration file in your home directory; otherwise, it looks for the `em_logview.cf` configuration file in the `$EM_HOME/config` directory. If the configuration file is not found, Log Entries uses the default properties.

The alphanumeric characters in each line of the configuration file must begin at the left edge. Each statement must be on a separate line. The configuration file has the following format.

```
display_name=fdn
label_name=default_name
show_doc_names=show
show_oids=oid
attr_name=logRecordId
logRecordId.name=Record #
logRecordId.position=1
logRecordId.displayed=true
logRecordId.width=7
attr_name=eventTime
eventTime.name=Event Time
eventTime.position=2
eventTime.displayed=true
eventTime.width=11
attr_name=eventType
eventType.position=3
eventType.displayed=true
eventType.width=14
attr_name=managedObjectClass
managedObjectClass.name=Class
managedObjectClass.position=4
managedObjectClass.displayed=true
managedObjectClass.width=12
attr_name=managedObjectInstance
managedObjectInstance.name=Instance
managedObjectInstance.position=5
managedObjectInstance.displayed=true
managedObjectInstance.width=45
```

The information in this file corresponds to the selections made in the Column Headings and Log Filter dialogs.

# Integrating Solstice Enterprise™ SyMON System Monitor With Solstice EM

---

This chapter describes how to set up the Solstice Enterprise™ SyMON™ system monitor and Solstice Enterprise Manager (Solstice EM) so that events generated by the SyMON monitor will be received by Solstice EM. It also describes how to add the ability to launch the SyMON monitor from within Solstice EM.

---

**Note** – The instructions are valid only for versions 1.4 and 1.5 of SyMON system monitor.

---

This appendix comprises the following topics:

- Section A.2.1 “Adding an MIS Server Name to the SNMP Host List” on page A-5
- Section A.2.2 “Modifying SyMON Event Rules” on page A-6
- Section A.3.1 “Creating an Object Instance for the SyMON System” on page A-15
- Section A.3.2 “Mapping SyMON Traps” on page A-15
- Section A.3.3 “Creating a GDMO Document for SyMON Events” on page A-17
- Section A.3.4 “Mapping the SyMON Event Notification to an Object” on page A-20
- Section A.4 “Adding the SyMON Monitor to the Solstice EM Interface” on page A-21

---

## A.1 Overview

The Solstice SyMON system monitor is a tool that collects hardware and system status information about a server system and displays it through a graphical user interface. Much of the information the SyMON monitor gathers about a system is

useful to network administrators. In particular, events generated in response to conditions on the system would be helpful when brought to an administrator's attention.

Integrating the SyMON monitor into Solstice EM involves two separate tasks, which can be performed in any order:

- **Forwarding events to Solstice EM through SNMP traps** – this enables SyMON alarms to be seen by an administrator using Solstice EM. Forwarding events requires you to complete procedures on the SyMON system and on the Solstice EM system. Section A.1.1 “About Forwarding SyMON Events to Solstice EM” on page A-2 provides more information about forwarding events.
- **Adding the SyMON monitor to the Solstice EM user interface** – this enables an administrator to start the SyMON monitor while using Solstice EM. Adding the SyMON monitor to the Solstice EM user interface requires you to complete tasks only on the Solstice EM system.

More complete integration, such as managing SyMON agents from Solstice EM, is not possible.

## A.1.1 About Forwarding SyMON Events to Solstice EM

Setting up SyMON to forward events to Solstice EM is a two-stage process. The first stage sets up the SyMON system to forward the events to the Solstice EM MIS. The second stage sets up Solstice EM to monitor the machine that will be forwarding the events.

The SyMON monitor and Solstice EM may or may not run on the same server.



### A.1.1.1 The SyMON System

In a SyMON configuration, three hosts are potentially involved:

- **The monitored system**, which runs a set of agents that continuously monitor the hardware status of the monitored system. This set of agents is called the Server Subsystem.
- **The Event Generator system**, which runs the Event Generator software, comparing the data collected by the Server Subsystem to a set of event rules to determine if an event should be generated. There is one instance of Event Generator for each system being monitored. For the most effective monitoring, the Event Generator software should not be installed on the monitored system.
- **The Event Viewer system**, which runs the Event Viewer software, the user interface to the SyMON monitor. This may or may not be the same host running the Event Generator.

The changes required for the SyMON monitor to forward events to Solstice EM must take place on the system running the Event Generator. In this chapter, the system running the Event Generator is referred to as the SyMON system.

### A.1.1.2 The Solstice EM System

The Solstice EM system is a host that is running the Management Information Server (MIS). You can set up event forwarding from the SyMON monitor to more than one MIS server by repeating the tasks described in Section A.3 “Setting Up Solstice EM to Receive SyMON Traps” on page A-14 on each MIS server.

---

**Note** – SyMON integration is easier if Solstice EM is installed on the SyMON system because it enables the system monitor to use Solstice EM’s utility for sending SNMP traps.

---

## A.1.2 Limitations of SyMON Event Forwarding

SNMP events forwarded from SyMON are not as informative as those from SNMP agents communicating directly with Solstice EM. The following information is provided in an SNMP trap sent by the SyMON monitor to Solstice EM:

- Name of the machine where the trap originated
- Integer ID of the SyMON event rule that generated the trap
- Notification that the trap is from the SyMON monitor

The SyMON monitor provides descriptive information about an event within an error message associated with the event rule. This error message cannot be passed to Solstice EM. However, the information that is provided in the trap is enough to make network operators aware that they should check the SyMON monitor for a problem on the specified system. You can enable Solstice EM operators to conveniently start the SyMON monitor by adding it to the Solstice EM interface, as explained in Section A.4 “Adding the SyMON Monitor to the Solstice EM Interface” on page A-21.

## A.1.3 About Adding the SyMON Monitor to the Solstice EM Interface

You can add the SyMON monitor to the Solstice EM user interface by adding it to the Network Tools panel and the pop-up menus shown for devices in the Network Views window.

## A.1.4 Related Tasks

- Chapter 2 “Getting Started With Solstice EM”
- Chapter 4 “Viewing Network Components”

## A.1.5 Related Files

- `/opt/SUNWsymon/etc/swrules.tcl`
- `/opt/SUNWsymon/etc/event_gen.server.tcl`
- `$EM_HOME/em/conf/trap_maps`
- `$EM_HOME/etc/gdmo/snmp_traps.gdmo`
- `$EM_HOME/etc/gdmo/symon_snmp_traps.gdmo`

## A.1.6 Further Reading

- *Solstice Enterprise SyMON 1.5 User's Guide*
- *Management Information Server Guide* for Solstice EM

---

## A.2 Setting Up the SyMON System to Forward Events

Setting up the SyMON system to forward events requires you to:

1. Add the MIS server to the SNMP host list. This is the list of hosts that will receive traps forwarded by the SyMON monitor.
2. Modify the SyMON event rules. Rules determine the conditions that must be met for an event to be generated and the actions that occur when the conditions are met. You must perform the following tasks to modify the event rules:
  - a. Locate the event rules used on the SyMON system.
  - b. Determine which events you want to forward to Solstice EM.
  - c. Edit the actions of the events rules for the rules you want to forward.

These tasks are described in the following procedures.

### A.2.1 Adding an MIS Server Name to the SNMP Host List

Before Solstice EM can monitor SyMON events, you must add the name of the Solstice EM MIS server to the SyMON monitor's list of SNMP hosts. The hosts in this list receive the SNMP traps for events generated by the SyMON monitor.

#### ▼ To Add an MIS Server Name to the SNMP Host List

1. **Log in as root on the SyMON Event Generator system or become superuser.**
2. **Add the server name(s) by typing the following command:**

```
/opt/SUNWsymon/sbin/sm_confsymon -e monitored_host -P platform -S  
"list_of_snmphosts"
```

where

*monitored\_host* is the name of the host the SyMON program is monitoring,

*platform* is the server type of the monitored host. You can determine the platform using the command `uname -i` on the monitored host.

*"list\_of\_snmphosts"* is a space-separated list of hosts, contained in quotation marks.

For example, if the host being monitored is an Ultra Enterprise 1000 named *riviera* and you want to send SNMP traps to Solstice EM MIS servers *case* and *molly*, you would execute the command:

```
/opt/SUNWsymon/sbin/sm_confsymon -e riviera -P SUNW,Ultra-1 -S  
"case molly"
```

This command causes a file, *event\_gen.riviera.tcl* to be created in directories */etc/opt/SUNWsymon* and */opt/SUNWsymon/etc* and, within that file, sets a variable *snmp\_hosts* to *case molly*.

### 3. Stop and restart the Event Generator:

```
/opt/SUNWsymon/sbin/sm_control stop  
/opt/SUNWsymon/sbin/sm_control start
```

## A.2.2 Modifying SyMON Event Rules

To have SNMP traps forwarded from the SyMON monitor to Solstice EM, you must modify the SyMON monitor's event rules. The *Solstice Enterprise SyMON User's Guide* explains event rules in detail. This appendix explains only the specific changes you need to make to forward specific SyMON events to Solstice EM.

An event rule defines an event, and contains a condition and other attributes that define the state of the rule. The state of the rule indicates whether the rule is open (active), closed (inactive), or continuing (active over a period of time). A rule also may define the actions to take if a certain state is reached. For example, an event rule might define an event for swap space usage. The condition in the rule tests whether swap space usage is above a certain threshold. When usage surpasses the threshold, the rule becomes open/active, an alarm is generated and an SNMP trap is sent to the hosts on the list of SNMP hosts. The alarm and SNMP trap are the rule's actions. Your modifications of the rules will focus exclusively on the action portion of the rules.

---

**Note** – The event rules files are written in the Tcl scripting language. It is highly recommended that you are familiar with Tcl before modifying the event rules files. If you modify them incorrectly, errors or unexpected results may occur.

---

## A.2.2.1 Location of Event Rules Files

Tcl scripts for the SyMON monitor's default event rules are located in `/etc/opt/SUNWsymon` and `/opt/SUNWsymon/etc`. Your configuration may include more Tcl scripts in other locations, depending on server model, localization, additional devices the server may have, and so on. The file `event_gen.servername.tcl` sets your `TCL_SOURCE_PATH`. You should consult this file to determine possible locations for additional event rules files.

## A.2.2.2 Determining Which Events to Forward

The SyMON monitor is supplied with a number of default event rules, and you may have added rules specific to your system. You must decide which events you want to forward to Solstice EM and edit the rules for those events.

You should pay particular attention to those event rules that are already set up to generate alarms and send traps. Of the rules supplied with the SyMON monitor, the rules using the `alarm` and `snmp` functions send traps, and you should determine which might warrant forwarding to Solstice EM.

For example, the file `/opt/SUNWsymon/etc/swrules.tcl` contains software rules that monitor such things as disk wait queues, swap space, CPU swapping and paging, CPU load, and file system space. Each of these rules uses an `alarm` and `snmp` function and are thus good candidates for modification to forward events to Solstice EM.

---

**Note** – Appendix D of the *Solstice Enterprise SyMON User's Guide* lists all the default SyMON rules and specifies if they use `alarm` and `snmp` actions.

---

## A.2.2.3 Editing the Actions of an Event Rule

After deciding which rules you want to edit, you must modify each of those rules to add function calls that send traps to Solstice EM. Generally, you should send two traps per rule: the first trap notifies Solstice EM of the SyMON alarm, and the second trap clears the first trap in Solstice EM.

The first trap must be inserted after the `alarm` function, which is located in the `ON_OPEN` attribute of the SyMON rule. The `ON_OPEN` attribute specifies what actions to take when the rule is active.

The second trap must be placed after the `end_alarm` function, which may be located in the `ON_OPEN` or `ON_CLOSE` attribute of the rule. The `ON_CLOSE` attribute specifies what actions to take when the rule is no longer active. `ON_CLOSE` does not occur in all rules; some rules include all actions in the `ON_OPEN` attribute.

## Sample Rules

The following code sample shows the `ON_OPEN` and `ON_CLOSE` attributes of Rule 104, located in the `/etc/opt/SUNWsymon/swrules.tcl` file.

```
ON_OPEN { alarm YELLOW KernelReader.cpu "$r104mess" ""
          set imsg [ format "$r104msg" "$target" ]
          snmp "$imsg" }
ON_CLOSE { end_alarm }
```

### CODE EXAMPLE A-1 `ON_OPEN` and `ON_CLOSE` Attributes of Rule 104

The `ON_OPEN` attribute calls the `alarm` function, assigns to an `imsg` variable the message text for rule 104 and the host name of the server with the problem, and sends these values in an SNMP trap using the `snmp` function. The `ON_CLOSE` attribute simply ends the alarm, which closes the alarm in the SyMON monitor. This does not automatically clear the SNMP trap.

The following code sample shows the `ON_OPEN` attribute of Rule 105, also located in the `/etc/opt/SUNWsymon/swrules.tcl` file.

```
ON_OPEN {
  set lsdata      [ split $value ]
  set fsname      [ lindex $lsdata 0 ]
  set mess [ format "$r105mess" "$fsname" ]
  alarm YELLOW "" "$mess" ""
  end_alarm
  set imsg [ format "$r105msg" "$target" "$fsname" ]
  snmp "$imsg"
```

### CODE EXAMPLE A-2 `ON_OPEN` Attribute of Rule 105

The `ON_OPEN` attribute calls the `alarm` and `end_alarm` functions, which sends an alarm to the SyMON monitor and then ends the alarm. It also assigns to an `imsg` variable the message text for rule 105, the host name of the server with the problem, and the name of a file system that has become full, and sends these values in an SNMP trap using the `snmp` function.

If you left these rules as they are, events would be forwarded to the system(s) listed in the `snmp_hosts` variable (which you specified in Section A.2.1 “Adding an MIS Server Name to the SNMP Host List” on page A-5), but the information sent would not be very useful. The host name provided would be that of the system running the Event Generator rather than the monitored system. This is because the `snmp $imsg` function generates a trap with the Event Generator system as the source and uses the error message to specify the monitored system in the `$target` variable. Solstice EM can look only at the trap and not the error message, so it appears to Solstice EM that the trap originated at the Event Generator system.

To make the forwarded events more useful, you should use a different trap generator that can provide more information. Solstice EM includes a trap generator that can produce traps that are more useful to Solstice EM. Other SNMP-based products may include useful trap generators as well, which you are free to use in the event rules.

The next section explains how to use Solstice EM's `snmp_trapsend` utility to produce more useful traps.

#### A.2.2.4 Using the `snmp_trapsend` Utility in Event Rules

If both Solstice EM and the SyMON Event Generator are installed on the same server, you can use the Solstice EM `snmp_trapsend` utility, located in the `/usr/sbin` directory. The `snmp_trapsend` enables you to pass more information to Solstice EM and automatically clear traps after a problem is corrected. Using the `snmp_trapsend` utility, you can specify the following:

- Name of the host to which the SyMON monitor should forward SNMP traps (i.e., name of MIS)
- Name of the host that originated the trap
- Event rule number being sent
- Clear trap matching a trap previously sent

The `snmp_trapsend` utility may be called directly from the rule, or can be called from a program or script. You can use `snmp_trapsend` directly in the rule if you want to send the SNMP trap to only one host. If you want to forward traps to more than one host, you must use a script or program, which would enable you to use the `snmp_hosts` variable. See “Using a C Program to Call the `snmp_trapsend` Function” on page A-11 for more information.

To use the `snmp_trapsend` function in the rule, replace the `snmp "$imsg"` function with a command using the following format:

```
/usr/sbin/snmp_trapsend -h servername -i $target -g 6 -s 1  
-a "1.3.6.1.4.1.42.2.12 INTEGER (rule_number) "
```

where

<code>-h <i>servername</i></code>	Indicates the name of the host to which the SyMON monitor should forward the trap.
<code>-i \$target</code>	Is a variable the SyMON monitor uses to specify the name of the host that originated the trap.
<code>-g 6</code>	Specifies a generic trap type of 6, which indicates that this is an enterprise-specific trap.

<code>-s 1</code>	Indicates a specific trap type of 1, which does not have any defined meaning, but must match the value in <code>trap_maps</code> . To close the trap, this value must be set to 0.
<code>-a 1.3.6.1.4.42.2.12</code>	Is the object ID for the SyMON monitor, which indicates its location in the Management Information Tree.
<code>INTEGER (rule_number)</code>	Is the event rule number that was triggered, generating the trap.

## *Modifying Rule 104 to Use `snmp_trapsend`*

The following code example shows Rule 104 modified to use the `snmp_trapsend` function in the rule.

```
snmp_trapsend
inserted here to ON_OPEN { alarm YELLOW KernelReader.cpu "$r104mess" ""
send trap      → exec /usr/sbin/snmp_trapsend -h molly -i $target -g 6 -s 1
                  -a "1.3.6.1.4.1.42.2.12 INTEGER (104)"}

snmp_trapsend ON_CLOSE { end_alarm
inserted here to → exec /usr/sbin/snmp_trapsend -h molly -i $target -g 6 -s 0
clear trap      -a "1.3.6.1.4.1.42.2.12 INTEGER (104)"}

```

### **CODE EXAMPLE A-3** Rule 104 Modified to Use `snmp_trapsend`

The `ON_OPEN` attribute calls the `snmp_trapsend` to send an SNMP trap to host molly, containing the name of the effected host in `$target`, the generic trap number 6, the specific trap number 1, the object ID 1.3.6.1.4.1.42.2.12, which identifies the SyMON monitor, and the integer 104, which is the rule number.

The `set imsg` line is deleted.

The `ON_CLOSE` attribute calls the `snmp_trapsend` with identical information except for the value for the specific trap number (`-s`). This is set to 0, indicating it clears the matching trap previously sent. This causes Solstice EM to clear the alarm it created in response to the first trap sent in the `ON_OPEN`.



## Modifying Rule 105 to Use snmp\_trapsend

To use `snmp_trapsend` in Rule 105, you should edit it as shown in the following code example:

```

        ON_OPEN {
            set lsdata      [ split $value ]
            set fsname      [ lindex $lsdata 0 ]
            set mess [ format "$r105mess" "$fsname" ]
            alarm YELLOW "" "$mess" ""
            exec /usr/sbin/snmp_trapsend -h molly -i $target -g 6 -s 1
                -a "1.3.6.1.4.1.42.2.12 INTEGER (105)" }
            end_alarm
            exec /usr/sbin/snmp_trapsend -h molly -i $target -g 6 -s 0
                -a "1.3.6.1.4.1.42.2.12 INTEGER (105)" }
        }
    }
    set imsg
    and snmp lines

```

snmp\_trapsend  
inserted here to  
send trap

snmp\_trapsend  
inserted here to  
clear trap,  
replacing set  
imsg  
and snmp lines

### CODE EXAMPLE A-4 Rule 105 Modified to Use snmp\_trapsend

The `ON_OPEN` attribute calls the `snmp_trapsend` to send an SNMP trap to host `molly`, containing the name of the affected host in `$target`, the generic trap number 6, the specific trap number 1, the object ID 1.3.6.1.4.1.42.2.12, which identifies the SyMON monitor, and the integer 104, which is the rule number.

The `ON_OPEN` attribute again calls the `snmp_trapsend` with identical information with the exception of the value for the specific trap number (`-s`). This is set to 0, indicating it clears the matching trap previously sent. This causes Solstice EM to clear the alarm it created in response to the first trap sent in the `ON_OPEN`.

The `set imsg` and `snmp` lines are deleted.

## Using a C Program to Call the snmp\_trapsend Function

If you want to forward traps to more than one host, you must use a script or program, which would enable you to use the `snmp_hosts` variable.

CODE EXAMPLE A-5 shows a simple C program you can use to call the `snmp_trapsend` function if you need to forward traps to more than one MIS.

```

1  # my_trapssend.c
2  # Sample program showing use of snmp_trapssend
3  #include <stdio.h>
4  #include <string.h>
5
6  main(int argc, char *argv[])
7  {
8      char command [4096];
9      char *s2;
10
11      s2 = strtok(argv[1],",, ");
12      if(!s2)
13      {
14          exit(1);
15      }
16      while(1)
17      {
18          sprintf(command, "/usr/sbin/snmp_trapssend -h %s -i %s -g %s -s %s
19 -a \"%s\\", s2, argv[2], argv[3], argv[4], argv[5]);
20          system(command);
21          s2 = strtok((char *)0,",, ");
22          if(!s2)
23          {
24              break;
25          }
26      }
27  }

```

**CODE EXAMPLE A-5** Source Code for Sample C Program Using snmp\_trapssend

Lines 18 and 19 contain the snmp\_trapssend command. The string values replacing %s for arguments -h, -i, -g, -s, and -a are specified in the rule you are editing.

The following code example shows Rule 104 modified to execute the program that calls snmp\_trapssend.

```

my_trapssend ON_OPEN { alarm YELLOW KernelReader.cpu "$r104mess" ""
inserted here to → exec /tmp/my_trapssend $snmp_hosts $target 6 1
send trap → "1.3.6.1.4.1.42.2.12 INTEGER (104)" }
my_trapssend ON_CLOSE { end_alarm
inserted here to → exec /tmp/my_trapssend $snmp_hosts $target 6 0
clear trap → "1.3.6.1.4.1.42.2.12 INTEGER (104)" }

```

**CODE EXAMPLE A-6** Rule 104 Modified to Use Program to Call snmp\_trapssend

The parameters to /tmp/my\_trapsend are listed in TABLE A-1.

The following code example shows Rule 105 modified to execute the program that calls snmp\_trapsend.

my\_trapsend  
inserted here to  
send trap

my\_trapsend  
inserted here to  
clear trap,  
replacing set  
imsg  
and snmp lines

```
ON_OPEN {
    set lsdata      [ split $value ]
    set fsname      [ lindex $lsdata 0 ]
    set mess [ format "%r105mess" "$fsname" ]
    alarm YELLOW "" "$mess" ""
    exec /tmp/my_trapsend $snmp_hosts $target 6 1
        "1.3.6.1.4.1.42.2.12 INTEGER (105)" }
    end_alarm
    exec /tmp/my_trapsend $snmp_hosts $target 6 0
        "1.3.6.1.4.1.42.2.12 INTEGER (105)" }
```

CODE EXAMPLE A-7 Rule 105 Modified to Use Program to Call snmp\_trapsend

The parameters to /tmp/my\_trapsend are listed in the following table.

TABLE A-1 Mapping of Options for snmp\_trapsend and my\_trapsend

Options for my_trapsend	Options for snmp_trapsend	Description
\$snmp_hosts	-h	The host(s) to which to send the SNMP trap. The value of this variable is set in the event_gen.server.tcl file as explained in “Adding an MIS Server Name to the SNMP Host List” on page A-5.
\$target	-i	The host name of the server where the problem originated. The value of this variable is set automatically when one of the first rules is activated.
6	-g	An integer value indicating the standard generic SNMP trap type. The integer 6 indicates that the trap is “enterprise-specific” and that further information is indicated in the specific trap type.

**TABLE A-1** Mapping of Options for `snmp_trapsend` and `my_trapsend` (Continued)

Options for <code>my_trapsend</code>	Options for <code>snmp_trapsend</code>	Description
1 to open the trap 0 to clear the trap	-s	An integer value indicating the specific trap type. The integer is 1 to open the trap, 0 to clear the trap. The 0 value indicates the trap is cleared.
"1.3.6.1.4.1.42.2.12 INTEGER (10x)"	-a	The three values contained in quotes are: <ul style="list-style-type: none"><li>• 1.3.6.1.4.1.42.2.12 – Object ID for the SyMON monitor</li><li>• INTEGER – Object type for passing the rule number</li><li>• 10x – SyMON Rule Number, which is 104 or 105 in the examples.</li></ul>

Notice that the `exec` statement to open the trap is identical to that to clear the trap, with the exception of the value for the specific trap number. For opening the trap, it is 1, while for clearing the trap it is 0. The 0 value to close the alarm sends an SNMP trap clear to Solstice EM.

Each rule you modify should be changed exactly as shown in CODE EXAMPLE A-6, while changing the `INTEGER (10x)` to match the event rule you are modifying. For example, if you modify rule 102 change the line to read:

```
exec /tmp/my_trapsend $snmp_hosts $target 6 1 "1.3.6.1.4.1.42.2.12 INTEGER (102)"
```

## A.3 Setting Up Solstice EM to Receive SyMON Traps

Setting up Solstice EM to receive SNMP traps from the SyMON monitor requires you to do the following on the system running the MIS:

1. Create an object instance for the SyMON system, if necessary.
2. Map the SyMON traps so they can be translated into Solstice EM events.
3. Create a GDMO document for SyMON traps, compile and load it.
4. Map SyMON traps to the `Event2ObjectClass`.

## A.3.1 Creating an Object Instance for the SyMON System

If the system running the SyMON monitor does not already have an object instance in the Solstice EM MIS, you must create one before Solstice EM can receive the SNMP traps from the SyMON monitor.

The easiest way to add an object for a system new to the network is to use the Discover tool to find it.

### ▼ To Create an Object Instance for the SyMON System

1. Type one the following commands at the command-line prompt to set up your environment, depending on which shell you are running.

- For the Bourne shell (sh):

```
source $EM_HOME/bin/emenv.sh
```

- For the C shell (csh):

```
source $EM_HOME/bin/emenv.csh
```

---

**Note** – \$EM\_HOME is the directory where the Solstice EM software is installed. By default, the directory is /opt/SUNWconn/em.

---

2. Type the following command at a command-line prompt:

```
em_discover -device hostname
```

where *hostname* is the name of the SyMON system.

When Network Discovery finds the host, it automatically creates an object instance for the host in the MIS.

## A.3.2 Mapping SyMON Traps

Traps from SNMP agents are handled in Solstice EM by the SNMP trap daemon, `em_snmp-trap`, which may run on one or more machines on the network. Before Solstice EM can handle SNMP traps, the trap daemon must convert them to event notifications in CMIP format, using information in the `trap_maps` file. You can edit the `trap_maps` file on the trap daemon machine to add information about the SyMON monitor's SNMP traps so that they can be converted to useful event notifications. If Solstice EM receives an SNMP trap that is not listed in `trap_maps`,

the trap daemon converts it into a non-specific “internetAlarm” with an “indeterminate” perceived severity value. The alarm does not indicate which agent generated the trap.

You need to map only two traps for the SyMON monitor: one for the trap that is issued when a rule’s conditions are met, and one for the trap that clears the previously sent trap when a problem is fixed and a rule’s conditions are no longer met.

## ▼ To Map SyMON SNMP Traps

1. **Become superuser or log in as root.**
2. **Using a text editor, open the `trap_maps` file located on the machine running `em_snmp-trap`. The file is located in `/etc/opt/SUNWconn/em/conf`.**
3. **Insert the following lines *above* the line “enterprise 1.3.6.1.4.1”.**

```
enterprise 1.3.6.1.4.1.42
{
#Symon
#Map for SyMON traps
    GENERIC-TRAP 6
    SPECIFIC-TRAP 1
    NOTIFICATION symonSpecificTrap
    ATTRIBUTE-MAP
    probableCause=varbindvalue1;
    perceivedSeverity=warning;
    additionalText=$ALLVARS;
    FDN-MAP ;;

#Map for cleared SyMON traps
    GENERIC-TRAP 6
    SPECIFIC-TRAP 0
    NOTIFICATION symonSpecificTrap
    ATTRIBUTE-MAP
    probableCause=varbindvalue1;
    perceivedSeverity=cleared;
    additionalText=$ALLVARS;
    FDN-MAP ;;

}
```

GENERIC-TRAP must be set to 6; this indicates that the trap is enterprise-specific.

`SPECIFIC-TRAP` should be set to 1 for SyMON traps and 0 for cleared traps.

`NOTIFICATION` should be set to `symonSpecificTrap` to indicate that it originated from the SyMON monitor.

In the `ATTRIBUTE-MAP` section, setting the `probableCause` attribute to `varbindvalue1` assigns it the value of the variable that is passed with the `snmp_trapsend` command. The value passed should be the number of the event rule that triggered the alarm, such as 104, as discussed in section “Modifying SyMON Event Rules” on page A-6.

The `perceivedSeverity` attribute is set to `warning` for traps and `cleared` for cleared traps. Note that all events from the SyMON monitor will be flagged as warnings by Solstice EM. For example, CPU failures and swap space shortages would both be shown in yellow (the default color for a warning) in the Solstice EM Network Views window.

#### 4. Save the file and exit the editor.

## A.3.3 Creating a GDMO Document for SyMON Events

Before Solstice EM can convert SyMON traps to CMIP event notifications, you must create and load a new event type into the MIS. You can do this by either modifying the existing `snmp_traps.gdmo` file or creating a new `.gdmo` file defining the event type. You then use the Load Data Definitions tool to load the information into the MIS.

All `.gdmo` files must be located in the directory `$EM_HOME/etc/gdmo`. They are loaded automatically when Solstice EM starts.

In the `snmp_traps.gdmo` file, you can use the definition for `enterpriseSpecific NOTIFICATION` as a model for your definition for the SyMON monitor.

CODE EXAMPLE A-8 shows a definition that was created for SyMON events using the `enterpriseSpecific NOTIFICATION` as a model. Changes made for the SyMON monitor are labelled.

```

MODULE "SYMON Traps" ← MODULE indicates SyMON traps

symonSpecificTrap NOTIFICATION ← NOTIFICATION matches value in
    BEHAVIOUR                                trap_maps file
    enterpriseSpecificTrapBehaviour BEHAVIOUR
    DEFINED AS
    !This is a SNMP enterpriseSpecific Trap.!!!
    WITH INFORMATION SYNTAX
        SNMP-TRAP.SnmpTrapAlarmInfo

    AND ATTRIBUTE IDS
        probableCause
        "Rec. X.721 | ISO/IEC 10165-2 : 1992": probableCause,
        attributeIdList
        "Rec. X.721 | ISO/IEC 10165-2 : 1992": attributeIdentifierList,
        objectInstanceList
        "iimcManagementDoc 1": objectInstanceList,
        unknownVarBindList
        "iimcManagementProxyMIB": snmpVarBindList,
        internetTrapInfo
        "iimcManagementProxyMIB": internetTrapInfo,
        perceivedSeverity
        "Rec. X.721 | ISO/IEC 10165-2 : 1992": perceivedSeverity,
        notificationId
        "Rec. X.721 | ISO/IEC 10165-2 : 1992": notificationIdentifier,
        correlatedNot
        "Rec. X.721 | ISO/IEC 10165-2 : 1992": correlatedNotifications,
        transportDomain
        "iimcManagementDoc 1": transportDomain,
        transportAddress
        "iimcManagementProxyMIB": transportAddress,
        accessControlInfo
        "iimcManagementProxyMIB": accessControlInfo,
        additionalInformation
        "Rec. X.721 | ISO/IEC 10165-2 : 1992": additionalInformation,
        additionalText
        "Rec. X.721 | ISO/IEC 10165-2 : 1992": additionalText;

REGISTERED AS { iimcManagementNot 2050 };
END

```

← REGISTERED AS  
number must be unique.

**CODE EXAMPLE A-8** GDMO File for SyMON Traps



## ▼ To Create a GDMO Document For SyMON Event Notifications

1. **Change to the directory** `$EM_HOME/etc/gdmo`. For most installations, this will be `/opt/SUNWconn/em/etc/gdmo`.

```
cd /opt/SUNWconn/em/etc/gdmo
```

2. **Copy the** `snmp_traps.gdmo` **file to a file called** `symon_snmp_traps.gdmo`.

```
cp snmp_traps.gdmo symon_snmp_traps.gdmo
```

3. **Using a text editor, open the** `symon_snmp_traps.gdmo` **file and delete all text up to, but not including, the line:**

```
enterpriseSpecificTrap NOTIFICATION
```

4. **Make the changes shown in** CODE EXAMPLE A-8.

Briefly, you must add the `MODULE` name, change the `NOTIFICATION` name to match the `NOTIFICATION` value you specified in `trap_maps`, and change the `REGISTERED AS` number to something unique.

5. **Save the file and exit the editor.**

This file must then be compiled and loaded as explained in the next procedure.

## ▼ To Compile and Load the SyMON Monitor's GDMO Document

1. **Change to the directory** `$EM_HOME/em/etc/gdmo` **if necessary. For most installations, use the following command:**

```
cd /opt/SUNWconn/em/etc/gdmo
```

2. **Type the following command:**

```
/opt/SUNWconn/em/bin/em_gdmo -host MIS-host -file  
symon_snmp_traps.gdmo
```

You should see the following message:

```
Parsing symon_snmp_traps.gdmo completed: 3/3 elements loaded  
successfully.
```

If you get an error message, check the file to make sure you did not make any errors. It must match the code shown in CODE EXAMPLE A-8.

3. **Warn users connected to the MIS that you are about to restart Solstice EM, and then restart Solstice EM services with the following command:**

```
/opt/SUNWconn/em/bin/em_services -start
```

## A.3.4 Mapping the SyMON Event Notification to an Object

Using the Object Editor (OBED), you must add the `symonSpecificTrap` event to the list of events in the `event2ObjectClass` object. An event notification is not a persistent object, so it cannot be stored. Adding the `symonSpecificTrap` to this list tells Solstice EM that a `symonSpecificTrap` event notification must be mapped to this kind of object. Mapping to an object allows the event notifications to be recorded in the log and stored in the MIS.

### ▼ To Map the SyMON Event Notification to an Object

1. **Start the Object Editor from Network Tools or from the command line.**

To start from the command line, type:

```
/opt/SUNWconn/em/bin/em_obed
```

2. **Open the object hierarchy below, where *servername* is the MIS you are working with:**

```
/
  /systemId=name:"servername"
    /subsystemId="EM-MIS"
```

3. **Double-click `/listname="event2ObjectClass"`, or select it and choose **Object -> Get**.**

The Object Configuration dialog opens.

4. **In the “newitem” text box type the following information:**

```
{ eventtypeid "SYMON Traps":symonSpecificTrap, objectclassoid "EM-ALARM":emInternetAlarmRecord }
```

5. **Click **Set** to add the information to the list of events.**

Use the horizontal scroll bar to view the full text in the `evr2oclist` field. The text you entered in Step 4 should be at the end of the list.

6. **Stop and restart the trap daemon by entering the following commands as root.**

```
em_trapd stop
em_trapd start
```

7. **Warn users connected to the MIS that you are about to restart Solstice EM, and then restart Solstice EM services with the following command:**

```
/opt/SUNWconn/em/bin/em_services -start
```

---

## A.4 Adding the SyMON Monitor to the Solstice EM Interface

SyMON events forwarded to Solstice EM tell the operator only that the event came from the system monitor, and provide the name of the affected host and the number of the SyMON rule that was activated to send the event. To get more pertinent information, the operator must look at the event through the SyMON user interface.

Adding the SyMON monitor to the Solstice EM interface enables the operator to quickly find out more information about an event generated by the SyMON monitor.

To add the SyMON monitor to the Solstice EM interface, you must do the following:

1. Add the SyMON monitor to Network Tools.  
When you add the SyMON monitor to Network Tools, its icon is displayed with the Solstice EM tools.
2. Add the SyMON monitor to Network Views pop-up menus for selected devices.  
When you right-click a managed object in Network Views, a pop-up menu is displayed. You can add the SyMON monitor to the list of tools on the menu.

The procedures for each of these tasks follows.

### ▼ To Add the SyMON Monitor to Network Tools

1. **Select File -> Customize in the Network Tools window.**
2. **In the Path to Executable field, type the path to the SyMON program.**  
By default the path is `/opt/SUNWsymon/bin/symon`.
3. **In the Path to Icon field, type the path to a suitable icon to use for the SyMON monitor.**  
The SyMON icon is `/opt/SUNWsymon/dt/appconfig/icons/C/launcher.l.pm`. Type this path if Solstice EM and the SyMON monitor are on the same system. If Solstice EM and the SyMON monitor are not installed on the same system, you could copy this icon to the `/opt/SUNWconn/em/glyphs` directory on the Solstice EM system and specify this location.
4. **Specify the icon name for the SyMON monitor.**
5. **Select No for Solstice EM Tool.**

**6. Click Add to add the SyMON icon to Network Tools.**

**7. Click OK to close the Customize dialog.**

The SyMON icon is displayed in the Network Tools window. You can start the system monitor by clicking the SyMON icon.

## ▼ To Add the SyMON Monitor to the Network Views Popup Menu

**1. Select File -> Customize -> Pop-up Menus in the Network Views window.**

**2. In the Configure Pop-up Menus window, select a device type for the systems you will be using the SyMON monitor to monitor.**

For example, if you will be monitoring an Ultra2, select Ultra2.

**3. In the Menu Option field, type SyMON.**

**4. In the Command field, type the full path to the command.**

By default, the path is `/opt/SUNWsymon/bin/symon`.

**5. Click Add.**

**6. Select any other device types that are being monitored by the SyMON monitor and click Add to add SyMON to the popup menu for each device.**

**7. When you are finished, click Apply and then click Close.**

If you right-click on a SyMON-monitored device in Network Views, you can select SyMON to start the system monitor.

# Managed Object Definitions

---

This appendix provides explanatory and reference information about the Management Information Base (MIB), an important part of the Solstice Enterprise Manager (Solstice EM) architecture, and MIBs supported by Solstice EM.

---

## B.1 The Management Information Base

In the physical, tangible world of daily life, managed objects are generally contained in a database reserved for the storage of managed object data, including attributes and values. The definitions of the characteristics of managed objects are contained in a Management Information Base (MIB), a paper document also available online that delineates and describes each managed object and attribute. As an example of why this data is important and how it is used, when you query for data about a network device in a tool such as the Data Collections tool, and after your query, you receive a collections file filled with data, the values listed inside the file are explained in the MIB for that object. So, if you perform a query and in your collection file you find the following data:

```
ipRouteType 4
```

to understand this data, you need to know what `ipRouteType` is and the meaning of the value 4. The definition of these values is contained in the MIB that contains this attribute. In the example, the attribute `ipRouteType` is described in the RFC 1213 MIB. The definition includes its syntax, descriptions of its associated parameters, and a topical description. To find out about an attribute of a managed object, you can refer to the MIB that contains its definition.

---

## B.2 MIB Terminology

Inside the MIB, all stored data, including the attributes of objects, is referred to as an object. Consequently, from the perspective of a developer of software applications for network management, attributes, the logical representation of the characteristics of objects, are also objects. In the graphical environment of Solstice EM, however, attributes are considered to be characteristics of managed objects, and are not considered to be objects themselves.

The remainder of this appendix refers to all data contained in a subtree as an object, to remain consistent with industry terminology. At the same time, this appendix provides parallels between the objects described and the user interfaces of Solstice EM applications in which these subtree objects are represented as attributes of a network resource.

### B.2.1 Organization of the MIB

Inside the MIB, attributes are organized in groups and subsets of groups as specified in the ISO Abstract Syntax Notation One (ISO ASN.1), the document that details the syntax of a MIB. The MIB is divided into the following four groups where object data is contained:

- Directory group
- Management group
- Experimental group
- Private group

#### B.2.1.1 Directory Group

The directory group is currently not in use; it is allocated to contain future data about the OSI directory service (X.500).

## B.2.1.2 Management Group

The management group contains object data used most often. Objects used in software applications for network management are typically built upon the object data provided in this group. Eleven categories of object data are provided..

**TABLE B-1** Attribute Categories in Management Group and Example Attributes

Attribute Category	Example Attribute	Description of Data Provided
system (sys)		Specifies data about the operating system on the network resource, i.e., the operating system on a host.
	sysName	Specifies the name of the resource.
interfaces (if)		Specifies data about the availability of user interfaces on the system.
	ifAdminStatus	Specifies data about whether the system is up, down, or in a test state.
address translation (at)		Specifies mappings of internet protocol and physical, geographical addresses for a particular resource.
	atNetAddress	Specifies the internet address for a particular resource.
Internet Protocol (ip)		Specifies data about the IP attributes of an object.
	ipRouteTable	Specifies the internet protocol routing table of the device.
Internet Control Network Protocol (icmp)		Specifies ICMP protocol data.
	icmpInErrors	Specifies the rate of ICMP input errors.
Transmission Protocol (tcp)	tcpInErrors	Specifies the rate of TCP data.
		Specifies the rate of TCP input errors.
User Datagram Protocol (udp)	udpInDatagrams	Specifies UDP data. UDP is a simple protocol for the transmission of data. The UDP group contains few object attributes.
		Specifies the total number of UDP datagrams received for any given period of time.
Exterior Gateway Protocol (egp)		Specifies EGP data, Object attributes in this subtree are further divided to provide data useful to configuration, performance, and fault management.
	egpNeighAddr	Specifies the internet address of a neighboring system using EGP.
Common Management data Services (cmot)		This group is no longer used. It remains for historical significance. CMOT was designed to facilitate the transition from SNMP to CMIP/CMIS.

**TABLE B-1** Attribute Categories in Management Group and Example Attributes

Attribute Category	Example Attribute	Description of Data Provided
Transmission Media-Specific		Specifies data about the media underlying system interfaces.
Simple Network Management Protocol (snmp)	snmpInPkts	Specifies the number of SNMP errors and packets entering and leaving a system. Specifies the rate of SNMP packets entering a system.

### B.2.1.3 Experimental Group

This group contains data about experimental objects that have the potential to become future standards.

### B.2.1.4 Private Group

This group is reserved for objects developed by a company and that have a specific purpose in the network environment. For example, U.S. Robotics has its own MIB that defines data about its modems.

## B.3 Managed Objects by Function

Objects of the Management Group play an important role in Solstice EM. Polling frequently for attribute data can help you to proactively determine potential problem areas of the network; then you can set conditions to ensure that these problems do not occur. The data provided by managed objects assists you in the five main areas of network management:

- **Fault management**—Detecting and fixing network problems.
- **Configuration management**—Setting up and tweaking network resources, including routers, bridges, and hosts, to ensure that they function effectively.
- **Security management**—Setting up permissions for users and groups to access software applications and network resources.
- **Performance management**—Monitoring your network to determine the effectiveness of resources. Also, proactively making changes to hardware and software to enhance their effectiveness.
- **Accounting management**—Monitoring resources used by individuals and groups to ensure that users have appropriate versions of hardware and software and to maintain the cost effectiveness of the network installation.



The following table shows the functional areas of network management for which the MIB groups provide objects.

**TABLE B-2** Solstice EM Objects Provided, Per MIB Group, For Network Management

Management (2) Subtree Group	Functional Areas of Network Management				
	Fault Management	Configuration Management	Security Management	Performance Management	Accounting Management
sys	X	X			
if	X	X		X	X
at	Objects developed in this group are incorporated into and represented in the other groups shown in this table.				
ip	X	X		X	X
icmp				X	X
tcp	X		X	X	X
udp		X	X	X	X
egp	X	X		X	
cmot	No objects are contained in this group.				
transmission	Objects in this group pertain to the specific technology underlying the interfaces of an application. The objects in this group align with the types of technology, including Token Ring and FDDI, rather than functional areas of network management.				
snmp	X	X	X	X	X

## B.4 Objects and Solstice EM

Solstice EM provides three tools for retrieving data about attributes and attribute values of objects:

- RPC/CMIP Data
- SNMP Data
- Data Collections

## B.4.1 Solstice EM Applications and Supported Protocols

In the RPC/CMIP Data tool and the SNMP Data tool, you can poll and view non-persistent data about an object. In the Data Collections tool, you can also poll and view data. You can also record the data retrieved to a collection or graph trends in the Grapher tool. The following table lists the protocols supported by each tool.

**TABLE B-3** Table of Protocols Accepted by Solstice EM Data Collecting Tools

Application	Protocol Accepted		
	RPC	CMIP	SNMP
RPC/CMIP Data	X	X	
SNMP Data			X
Data Collections	X	X	X

## B.4.2 MIBs Supported by Solstice EM

Solstice EM supports many MIBs supporting third-party products including Cisco routers, Synoptic Token Ring and Ethernet networks, and others. The default Solstice EM agent also supports two kinds of MIBs:

- RFC 1213 MIB
- Solstice MIB

For each of these MIBs, you can retrieve data about the objects and attributes of objects contained in them. TABLE B-4 provides a listing and description of all Solstice MIB objects and attributes supported by Solstice EM. Unless specified in the table, these attributes are read-only, which means that they can be viewed in RPC/CMIP Data, SNMP Data, or Data Collections tools but cannot be modified. Read-write attributes, which can be modified, are noted in the table.

**TABLE B-4** Objects and Attributes of Solstice MIB Supported by Solstice EM Default Agent

Object	Attribute	Description
psEntry		Specifies the sequence of attributes for the Sun Processes group.
	psParentProcessID	Specifies the unique identifier of the parent process of the current process.
	psProcessCpuTime	Specifies the CPU time (including both system and user time) consumed thus far.
	psProcessID	Specifies a unique identifier for the process.
	psProcessName	Specifies the name of the process as a character string.
	psProcessSize	Specifies the combined size of the data and stack segments in kilobytes.)
	psProcessState	Specifies the run state of the process. Returns any of the following letters: R - Runnable T - Stopped P - In page wait D - Non-interruptable wait S - Sleeping (less than 20 seconds) I - Idle (more than 20 seconds) Z - Zombie
	psProcessStatus	Specifies whether or not a signal will be sent to the process. This attribute is read-write and can be modified
	psProcessTTY	Specifies the name of the terminal controlling the process
	psProcessUserID	Specifies the numeric form of the name of the user associated with this process
	psProcessUserName	Specifies the name of the user who started the process.
	psProcessWaitChannel	Specifies the reason why the process is waiting. Returns a description in the form of a character string.
sunHostPerf		The group of attributes relating to timeticks, a unit of measure equating to hundredths of a second. Attributes in this group return the value of the number of timeticks that pass during an event.
	rsDiskXfer1	No description exists for this mandatory attribute.
	rsDiskXfer2	No description exists for this mandatory attribute.
	rsDiskXfer3	No description exists for this mandatory attribute.
	rsDiskXfer4	No description exists for this mandatory attribute.

Object	Attribute	Description
sunHostPerf (continued)	rsIdleModeTime	Specifies the total number of timeticks used in idle mode since the system was last booted.
	rsIfCollisions	Specifies the number of output collisions.
	rsIfInErrors	Specifies the number of input errors.
	rsIfInPackets	Specifies the number of input packets.
	rsIfOutErrors	Specifies the number of output errors.
	rsIfOutPackets	Specifies the number of output packets.
	rsNiceModeTime	Specifies the total number of timeticks used by nice mode since the system was last booted.
	rsSystemProcessTime	Specifies the total number of timeticks used by system processes since the system was last booted.
	rsUserProcessTime	Specifies the total number of timeticks used by user processes since the system was last booted.
	rsVIntr	Specifies the number of device interrupts.
	rsVPagesIn	Specifies the number of pages read in from the disk.
	rsVPagesOut	Specifies the number of pages written to a disk.
	rsVSwapIn	Specifies the number of pages swapped in to the accepting host.
	rsVSwapOut	Specifies the number of pages swapped out to another host.
sunSystem		Specifies the system group. Attributes of the system group describe characteristics of the network systems. The implementation of this group is mandatory.
	agentDescr	Specifies the SNMP agent's description of itself.
	hostID	Specifies a unique four-byte binary string. This value is unique to Sun hardware.
	motd	Specifies the first line of /etc/motd.
	unixTime	Specifies Unix system time, measured in seconds since January 1, 1970 GMT.

---

## B.5 MIBs Supported by Solstice EM

Solstice EM supports the following MIBs developed by business units of Sun Microsystems and by other companies. You can view these MIBs and their associated objects and attributes in the SNMP Data tool by clicking View -> Show All Attributes.

- Cisco MIB
- ECSV2 MIB
- Host-Resources MIB
- Retix MIB
- Sun Master Agent MIB
- Synoptics Common MIB
- Synoptics Ethernet MIB
- Synoptics IEEE8023 MIB
- Synoptics TokenRing MIB



# Index

---

## A

access control, scope of access (security)

    defining, 35, 58

    to base object, 36

access manager, *See* security

access, data, 16

accessing remote MIS servers (security), 14

action operation (security), 45, 59

adding attributes

    SNMP Data, adding attributes, 12

administrativeState value, 15

agent communications, object

    agent communications, 44

agent/station model, 10, 2

agents

    CMIP, 48

    CMIP MPAs, 49, 51, 52

    communications, 11

    configuring, 44

    default, 44

    description, 5, 10, 2

    legacy support, 18

    MIS, 47

    MPAs, 11, 14

    protocol descriptions, 17

    RPC, 28, 46

    SNMP, 45

    SunNet Manager, 28

alarm

    configuration files, 35

    definition, 1

    instances

        viewing, 12

    security, 28

    severity, 3

    state

        overview, 3

alarm associations

    alarm representing an association, 5, 16

    and summary view, 5, 6

    attributes used to group alarms

        default, 4

        specifying, 16

    definition, 4

    definition of attributes used to group alarms, 4

    rules

        loading from a file, 17

        saving to a file, 17

        setting, 16

alarm attributes

    for grouping into associations, 4

    selecting for display in Alarms, 30

alarm deletion controllers

    creating, 26

    displaying for a remote MIS, 28

    modifying, 27

Alarm Deletion Controllers window

    using to delete alarms, 26

alarm filtering rules

    configuration file, 35

    deselecting, 18

    loading, 19

    printing, 19

    saving, 19

    setting, 18

alarm filters

    overview, 7

Alarm Manager, *See* Alarms window

## AlarmLog

- alarms collected by, 1
- alarms not collected by, 2

## alarms

- acknowledging, 21
- annotating, 24
- clearing, 54, 22
- colors, 26
- default log file, 1
- default severity colors, 28
- deleting
  - automatically, 25
  - manually, 25
  - with Alarm Deletion Controllers, 26
- filtering, 18
  - for deletion, 26
- graphing, 29
- grouping into associations, 16
- hiding, 23
- logging management activity, 28
- Network Views, in, 53 to 56
- printing a list, 15
- propagating severity, 54
- scrolling automatically, 29
- severity, 27
- showing duplicates, 29
- status, 26
- summarizing, 10
- viewing, 53, 10 to 15
  - associations, 11 to 12
  - details, 12
  - in a non-default log, 14
  - instances, 12
  - on a remote MIS, 14
  - specific network component, 13
  - summary, 10

## alarms security

- logging activities, 28

## Alarms window

- associations view, 4
- changing alarm sort order, 31
- changing attribute labels, 31
- customizing display, 29
- customizing Tools menu, 32
- functions, 2
- localized text strings, 35
- opening and exiting, 9
- overview, 1 to 9

specifying attributes displayed, 30

summary view, 5

using, 9

ancillary services, MIS, 15

APIs, 6, 19

application features, *See* tool tasks

architecture, EM, 5, 7

associations, *See* alarm associations

attribute data, tools for gathering, 2

## attributes

### alarm

for grouping into associations, 16

attributes of object sets (security), 58

attributes, object, 36

autoEntryScope field, 16

autoManagement daemon

about, 6

-debug parameter, 14

reference information, 14

starting/stopping, 14

working with customized autoManagement

Entry objects, 4

autoManagement Entry object

launching IsSnmpSystemUp Template, 15

launching LinkUp Template, 16

launching Ping-Reachable Template, 17

locked or unlocked, 14

## B

background images, 20, 31

Network Views, 18

bitmap backgrounds, 31

## C

changing log entry display, 4

changing tool description (security), 31

classifying devices, 24

clearing alarms, 54

cluster, layout, 29, 30

CMIP agents, 48

CMIP environment variables, 49

CMIP MPAs, 49, 51, 52

CMIP protocol

supported, 17

CMIS filters (security), 36



- collections, *See* data collections
- color
  - default alarm severity, 28
  - Network Views presentation, 28
  - Network Views settings, 26
  - used to indicate alarm severity, 3
- column headings (log entries), customizing, 5
- column order (log entries), changing, 4
- compilers, 21
- component representations, in Network Views, 4
- components, EM, 4
- configurable object type data, 70
- configuration files
  - em\_alarmmgr\_ap.cf, 17, 35
  - em\_alarmmgr\_fp.cf, 35
  - em\_alarmmgr\_il8n.cf, 35
  - em\_alarmmgr\_tp.cf, 32, 35
  - em\_alarmmgr\_vp.cf, 29, 35
  - em\_logview.cf, 12
  - emenv.csh, 8
  - emenv.sh, 8
- connecting to a MIS, 7
- CORBA gateway, 5
- create operation (security), 46, 59
- custom mangement applications, 20
- custom network management tools, 6

## D

- data access, in MIS, 16
- data collection tools, 4
- data collections
  - command-line options, 30
  - creating, 25
  - GDMO classes, 30
  - starting Data Collections, 6
- Data Collections tool, 24
- database, MIS, 13
- dataCollectorEntry object GDMO class, 32
- default access rule (security), 32, 37, 44
- default agents, 44
- default alarm severity colors, 28
- default folder, 10
- default object attributes command, 36
- default view, Network Views, 11
- deleting log entries, 9
- deleting objects, 17
- deleting tool tasks (security), 31

- designer, requests, 65
- devices, classifying, 24
- Discover, *See* Network Discovery
- discover.conf file, 24
- discriminator construct, 1
- display properties, general, 23
- double-click actions, configuration, 33

## E

- em command, 12
- EM objects provided per MIB group, 5
- EM tools, 22
- em\_accesscmd utility, 9, 11, 50, 55, 56
- em\_accessmgr command, 9, 10, 29, 55
- em\_alarmmgr command, 9, 33
- em\_auto daemon, *See* autoManagement daemon
- em\_datacollector command, optional
  - parameters, 30
- em\_discover command, 17
- em\_discover -M command, 21
- em\_layout command, 63
- em\_login daemon, 2, 4
- em\_logview command, 11
- em\_nnconfig utility, 11
- em\_oct command, 40, 62
- em\_purgemgr command, 26
- em\_reqedit command, 65
- em\_simplerequests command, 64
- em\_viewer command, 62
- Enterprise Manager
  - accessing online documentation, 7
  - adding tools, 9
  - basic concepts, 10
  - configuration file, 2
  - core management tools, 2
  - core management tools executables, 5
  - environment variables, 14
  - modifying tool configurations, 11
  - removing tools, 9
  - script to set environment variables, 2
  - setting environment variables, 3
  - starting, 4
  - starting individual tools, 5
  - system variables, 13
- environment variables, 14
- environment variables, CMIP, 49
- error messages, 33

error messages, SNMP to CMIP translation, 33  
event logs  
    events not recorded by default, 2  
    events recorded by default, 2

## F

fault management, proactive, 1  
features, EM, 4  
file limit in SNM Results Browser, 5  
filtering log entries, 6  
filters, alarm, *See* alarms  
finding by name, Network Views, 13  
folders  
    about, 4  
    emptying and deleting, 11  
    loading files, 11  
Full Access group (security)  
    accessing tools and objects, 33  
    default rights, 12  
    granting privileges, 18

## G

geographical maps  
    adding new, 72  
    configuration files, 73  
    layers, 21  
    more about, 72  
    navigating in, 18  
    using as background, 32  
get operation (security)  
    example of, in Defaults dialog, 45  
    option description, 59  
global deny rule, 32, 38, 39  
    *See also* security rules  
global grant rule, 32, 41  
    *See also* security rules  
GMC files, 74  
graphing alarms, 29  
graphing information trends, 1  
graphing trends  
    Grapher, 28  
graphs  
    3-D graph, 1  
    merging, replotting, 13  
    printing, 13

    starting EM - Graphs, 3  
group profiles (security)  
    access privileges of, 12, 18  
    changing members, 22  
    creating from the command line, 51  
    definition, 11  
    deleting, 24  
    deleting from the command line, 52  
    maintaining, 23  
    printing, 21  
    saving and reusing, 20  
    *See also* user profiles  
    supplied with default installation, 12  
groups (security), 12, 33  
    *See also* group profiles  
    assigning access rules to, 46  
    assigning object sets, 46  
    assigning tool tasks, 53  
    changing membership, 22  
    controlling access to tools, 24  
    definition, 11  
Full Access group  
    access to tools and objects, 33  
    default rights, 12  
    granting privileges, 18  
    minimum number of members, 11  
Operators group, 12, 33  
searching, 21  
supplied with installation, 5, 12

## H

hiding log entry attributes, 4  
hierarchical views, 3  
hop counts, Network Discovery, 27

## I

icon label size, 19  
icon objects, creating, 14  
icon size, 19  
icons, configuring display, 24  
icons, Network Views, 5  
images, background in Network Views, 18, 20, 31  
Index attributes  
    SNMP Browser, indexes, 8  
init\_user file, 38

- installation
  - predefined access rules, 33
  - predefined groups, 12
  - predefined object sets, 34
- introduction, EM, 1
- item deny rule, 32
  - managed objects, 32
  - object sets, 39
  - See also* security rules
- item grant rule, 42
  - managed objects, 32
  - object sets, 42
  - See also* security rules

## J

- JMA server, 5

## L

- labels, configuring display, 24
- labels, icon, 19
- layers, map
  - displaying map layers, 21
- layout options, 63
- layout views, 29
- legacy support, 18
- limit command, 5
- log entries
  - adding tools to menu, 10
  - AlarmLog, 1
  - changing column order, 4
  - changing sort order of log records, 5
  - combining records in single view, 7
  - command-line options, 11
  - configuration file, 2, 12
  - customizing column headings, 5
  - customizing window display, 4
  - deleting, 9
  - environment variables, 11
  - events not recorded by default, 2
  - events recorded by default, 2
  - filtering log records, 6
  - filtering test, 1
  - overview, 1
  - printing, 9
  - removing tools from menu, 10

- searching for, 8
- security privileges, 3
- showing and hiding attributes in window, 4
- starting, 3
- viewing log record details, 6
- log manager, 2
- log records, *See* log entries
- log viewer, *See* log entries
- logging
  - alarms management, 28
  - Network Discovery, 11
  - Network Views, 22
- Logging tab, 11
- logical views, 3
- logical views, in Network Views
  - creating, 13
  - definition, 7
- login privileges for root and superusers (security), 10
- login to remote MIS servers, 14

## M

- macros, Network Views, 65
- managed objects, 5
  - by function, 4
  - creating, 42
  - in Network Views, 4
  - location of, 1
  - modifying, 41
- Management Information Base, 18
- management overview, 2
- Management Protocol Adapter
  - configuring over RFC1006, 49
  - running a configuration script, 51
  - starting remotely, 52
- management tools, EM, 8
- maps, geographical, 21, 72, 73
  - adding new maps, 72
  - components of, 72
  - navigating in views, 18
  - using as background, 32
- menu, tools, 34
- menus, pop-up, 36
- mesh, layout, 29, 30
- message log, Network Views, 22
- MIB groups, 2
- MIB terminology, 2

- MIBs, 18
- MIBs supported by EM, 6
- MIS, 2
  - ancillary services, 15
  - creating, 13
  - data access, 16
  - description, 6
  - Nerve Center, 14
  - object orientation, 16
  - overview, 12
  - remote
    - viewing alarm deletion controllers, 28
    - viewing alarms on, 14
- MIS agents, 47
- MIS requests, 56 to 61
  - advanced, 58
  - basic, 59
  - viewing, 57
- modules, EM API, 20
- Monitor, Network, 14, 21
- Monitoring network components, 2
- MPA
  - communication agents, 11
  - more about, 14
  - running a configuration script, 51
  - starting remotely, 52
  - using over RFC1006, 49
- multiple instances, of Network Views, 10
- multiple object selection (security)
  - example of, in Defaults dialog, 45
  - option description, 59

## N

- navigating, in geographical maps, 18
- Nerve Center, 14
- Nerve Center request templates, 2
- NerveCenter alarms, logged in, 2
- Network Discovery
  - classifying devices, 24
  - command-line options, 17, 21
  - creating a new MIS database, 13
  - deciding what to discover, 8
  - failed, 25
  - getting started, 5
  - hop counts, 27
  - loading and saving rules, 7
  - logging, 11

- Monitor, 14, 21
  - overview, 2
  - ports, 25
  - probe stage, 23
  - protocols, 3
  - proxy agents, 28
  - queries, 22
  - reference, 17
  - related files, 5
  - related tasks, 4
  - search methods, 10, 22
  - stopping, 12
  - viewing progress, 12
- network management applications, custom, 20
- network management software, description, 10
- Network management tools, 1
- network management, protocols, 17
- Network Monitor, 14, 21
- Network Tools, 1
- Network Views, 1 to 74
  - adding geographical maps, 72
  - advanced requests, 65
  - alarm status, 26
  - alarms, 53 to 56
  - background images, 18, 31
  - basic concepts, 3
  - clearing alarms, 54
  - CMIP agents, 48
  - CMIP MPAs, 49
  - color settings, 26
  - command-line options, 61
  - component representations, 4
  - configurable object type data, 70
  - configuring double-click actions, 33
  - creating icon objects, 14
  - creating logical views, 13
  - default agents, 44
  - default view, 11
  - deleting objects, 17
  - discovering network objects, 10
  - displaying and selecting objects, 12
  - editing views, 16
  - features, 1
  - finding by name, 13
  - general display properties, 23
  - geographical maps, 18, 21, 32, 72
  - icon and label display, 24
  - icon label size, 19
  - icon objects, 5

- icon size, 19
- layout options, 63
- logical views, 7
- macros, 65
- message log, 22
- MIS agents, 47
- multiple instances, 10
- Network Discovery, 3
- Network Discovery, and, 10
- object attributes command, 36
- object palette, 15, 37
- object properties, 42, 62, 67
- object types, 20, 67
- overview, 2
- pop-up menus, 36
- presentation colors, 28
- propagating alarm severity, 54
- reference information, 61 to 74
- requests, 56 to 61, 64
- RPC agents, 46
- saved views, 6
- saving and loading settings, 22
- searching for objects, 12
- selecting a view, 10
- SNMP agents, 45
- tasks for working with views, 9
- toolbars, 18
- tools menu, 34
- variables, 65
- view layout, 29
- viewing alarms, 53
- zoom settings, 25
- zooming in and out, 17
- non-topological views, 13

## O

- object attributes command, 36
- object classes, 58
- object filters (security), 59
- object instances (security), 35, 58
- object orientation, 16
- object palette, 15, 37
- object properties
  - CMIP agents, 48
  - CMIP environment variables, 49
  - CMIP MPAs, 49, 51, 52
  - command line, 40

- configuring display, 23
- creating, 42
- getting started, 39
- MIS agents, 47
- modifying, 41
- RPC agents, 46
- SNMP agents, 45
- viewing, 40, 44
- object sets (security)
  - assigning to groups, 46
  - controlling user access, 31
  - creating, 35
  - creating CMIS filters, 36
  - criteria defining, 58
  - default access rules, 32, 44
  - definition, 33
  - deleting, 48
  - deleting access rules on, 49
  - denying access to all, 32, 38
  - denying access to specific, 32, 39
  - examples, 33
  - granting access to all, 32, 41
  - granting access to specific, 32, 42
  - implementation guidelines, 7
  - maintaining, 48
  - maintaining access rules on, 49
  - rules for controlling access to, 32
  - supplied with installation, 5, 34
  - tasks for controlling access to, 34
  - updating, 48
  - updating access rules, 49
  - viewing group access privileges, 47
  - when to control user access to, 6
- object types, 5
- objects
  - configurable data, 70
  - creating in Network Views, 14
  - deleting, 17
  - displaying and selecting, 12
  - displaying specific types, 20
  - finding by name, 13
  - searching for, 12
  - types, 37, 67
- online documentation, access to, 7
- Operators group (security), 12, 33
- OSI alarms, logged in AlarmLog, 2
- OSI standard alarms, 2
- osimcsd MIS process, 50
- overview, EM, 1

- APIs, 19
- application development support tools, 21
- complete listings, 22
- components, 4
- data access, 16
- description, 1
- features, 4
- MIS, 12
- MIS services, 15
- MPAs, 14
- Nerve Center, 14
- object orientation, 16
- PMI, 14
- protocols, 17
- task overview, 2
- tools, 8

## P

- palette, object, 15, 37
- password authentication, 4
- Ping/SNMP optimization, 27
- Ping/SNMP/RPC tab, 10
- PMI, 14
- polling
  - in RPC/CMIP Data, 17
  - intervals, 18
  - using proxy agents, 17
- pop-up menus, 36
- Portable Management Interface, 14
- ports for network discovery, 25
- printing log entries, 9
- probe, Network Discovery, 23
- Probe\_OID, 24
- propagating alarm severity, 27, 54
- properties, object
  - CMIP agents, 48
  - CMIP environment variables, 49
  - CMIP MPAs, 49, 51, 52
  - command line, 40
  - command-line options, 62
  - configurable data, 70
  - creating, 42
  - getting started, 39
  - MIS agents, 47
  - modifying, 41
  - more about, 67
  - RPC agents, 46

- SNMP agents, 45
  - viewing, 40
- protocols
  - Network Discovery, 3
  - network management, 17
- proxy agents, 28

## Q

- queries, Network Discovery, 22

## R

- reconnecting to a MIS, 7
- recording SNMP Data, 24
- remote CMIP, 52
- report formats, 14, 15
- reports
  - about, 3
  - cloning, 7
  - viewing, 6
- request templates
  - about, 2
  - customizing, 4
- requestInfo attribute, 33
- requests, 56 to 61
  - advanced, 58, 65
  - basic, 59, 64
  - designer, 65
  - stopping, 11
  - viewing, 57
- restarting CMIP MPA stack, 53
- results browser, *See* SNM Results Browser
- rk6d MIS process, 50
- root privileges (security), 10
- RPC
  - legacy support, 18
  - supported, 17
- RPC agents, 46
- RPC/CMIP Data, 1
- RPC/CMIP Data, starting, 6
- rules, Monitor, 15
- rules, Network Discovery, 7

## S

- saved views, in Network Views, 6
- scope of access, *See* access control, scope of access
- scripts, environment variables, 2
- search methods, Network Discovery, 10
- searching in Network Discovery, 22
- searching in Network Views, 12
- searching log entries, 8
- security
  - accessing remote MIS servers, 14
  - adding tools, 26
  - command-line options, 54
  - configuration files, 8
  - creating object sets, 35
  - deleting object sets, 48
  - granting privileges, 17
  - guidelines for implementing, 6
  - implementation schemes, 5
  - overview, 1
  - preparation tasks for implementing, 12
  - starting the Security tool, 8
  - superuser access privileges, 10
  - tasks for controlling access to objects, 34
  - tasks for controlling access to tools, 26
  - tasks performed from the command line, 50
- security control
  - disabling, 7
  - enabling, 13
  - managed objects, 6, 7, 31
  - preparing for, 10
  - tools, 5, 7, 24
  - user access to remote MIS servers, 14
  - using rules for, 2
- security policy, 2
- security profiles
  - creating by duplicating existing profiles, 17, 19
  - definition, 11
  - for groups, 18
  - for users, 16
  - maintaining group profiles, 23
- security reference information, 54
- security rules
  - access rules policy, 2
  - applicable to users and groups, 4
  - assigning to groups, 46
  - conflicts, 4
  - controlling access to object sets, 32
  - controlling access to tools, 25
  - creating for tools and tasks, 29
  - default access rule, 32, 44
  - deleting object rules, 49
  - denying access to all objects, 32, 38
  - denying access to specific objects, 32, 39
  - duplicating, 44
  - enforcement policy, 2
  - example of conflicting rules, 4
  - granting access to all objects, 32, 41
  - granting access to specific objects, 32, 42
  - maintaining access rules controlling objects, 49
  - supplied with installation, 5, 33
  - updating, 30
  - updating access rules controlling objects, 49
  - using, 2
  - viewing access privileges to objects, 47
  - viewing tool privileges, 30
- Services/TopoTypes tab, 10
- set operation (security), 46, 59
- severity, alarm, 28, 54, 3
- showing log entry attributes, 4
- SNM agents, 28
- SNM event notifications, 2
- SNM Results Browser
  - changing window position and size, 13
  - customizing, 12
  - defining an output size, 14
  - deleting, printing reports, 7
  - folders, 10
  - loading collections as streams, 5
  - setting report formats, 15
  - specifying a printer, 13
  - starting, 4
  - viewing reports, 6
- SNM RPC event notifications, 2
- SNMP, 12
  - MIBs, 18
  - supported, 17
- SNMP agent, specifying, 8
- SNMP Agent, viewing object attributes, 7
- SNMP agents, 45, 1
- SNMP Agents, selecting multiple, 9
- SNMP Data, 2, 5
- SNMP data
  - getting attribute data, 14
  - tables, 10
- SNMP Data Browser, 28
- SNMP Data tools, 1
- SNMP Data, creating a row, 11
- SNMP Data, displaying remote data, 19

- SNMP Data, polling an agent, 18
- SNMP Data, queries
  - SNMP Data, getting attribute data, 14
- SNMP Data, remote data, 21
- SNMP Data, setting attribute data, 16
- SNMP Data, tables, 10
- SNMP Data, window, 7
- SNMP Read Community, 7, 8
- SNMP trap notifications, logged in AlarmLog, 2
- SNMPv2c, 10
- sorting log entries, 5
- stopping Network Discovery, 12
- streams
  - about, 2, 3
  - clearing, deleting, 9
  - displaying, graphing, 10
  - organized in the SNM Results Browser, 1
  - printing, 9
  - selecting, 6, 4
  - variables, 3
  - viewing, 6
- SunNet Manager, 28
- SunNet Manager Results Browser, *See* SNM Results Browser
- support tools, for application development, 21
- system variables, 13

## T

- targets, *See* object sets
- Telecommunications Management Networks, 17
- tile, layout, 29, 30
- TMN, 17
- tool names, modifying, 31
- tool tasks (security)
  - assigning to groups, 53
  - controlling access to, 24
  - definition, 25
  - getting list for a user, 53
  - specifying from the command line, 53
- toolbars, Network Views, 18
- tools (log entries)
  - adding to log entries menu, 10
  - removing from log entries menu, 10
- tools (security)
  - adding by duplication, 27
  - adding from the command line, 52
  - adding to EM, 9, 26

- controlling access to, 24
- definition, 25
- getting list accessible to users, 53
- implementation guidelines, 7
- removing, 28
- rules for controlling access to, 25
- tasks for controlling access to, 26
- updating access rules, 30
- viewing group access privileges, 30
- when to control user access, 5
- tools menu, 34
- tools, custom application development, 21
- tools, EM, 8, 22
- tree, layout, 29, 30

## U

- UNIX accounts (security), 10, 16
- user profiles (security)
  - changing group membership, 22
  - collecting information for, 16
  - connecting to a remote MIS, 4
  - creating from the command line, 51
  - deleting, 23
  - deleting from the command line, 52
  - maintaining, 22
  - preparing, 16
  - printing, 21
  - saving and reusing, 20
- users (security)
  - accessible tools, getting list of, 53
  - accessing a remote MIS, 4
  - assigning to other groups, 51
  - authorized tool tasks, getting list of, 53
  - changing group membership, 22
  - controlling access to tools, 24
  - membership in multiple groups, 11
  - searching for users, 21
  - UNIX accounts for, 10, 16

## V

- variables, environment, 49
- variables, Network Views, 65
- view
  - dialog, 2
  - layout, 29



- log entry details, 6
- Network Discovery progress, 12
- settings, Network Views, 22
- zoom settings, 25
- zooming in and out, 17
- View Only group (security), 12, 33
- viewer, *See* Network Views
- views, editing, 16
- views, selecting in Network Views, 10

## **Z**

- zoom controls, 17
- zoom settings, 25

