HP OpenView Smart Plug-In for Data Network Devices

Administrator's Guide

Version A.02.00
July 2002

U.S.A.

Legal Notices

The information in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty. A copy of the specific warranty terms applicable to your Hewlett- Packard product and replacement parts can be obtained from your local Sales and Service Office.

Restricted Rights Legend. Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

HEWLETT-PACKARD COMPANY
3000 Hanover Street
Palo Alto, California 94304 U.S.A.

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Contents

Contents

Printing History

The manual printing date and version number indicate its current edition. The printing date will change when a new edition is printed. Minor changes may be made at reprint without changing the printing date. The version number will change when extensive changes are made.

Manual updates may be issued between editions to correct errors or document product changes. To ensure that you receive the updated or new editions, you should subscribe to the appropriate product support service. See your HP sales representative for details.

First Edition: January 2002

Second Edition: July 2002

1 Introducing the HP OpenView Smart Plug-In for Data Network Devices

What is the HP OpenView Smart Plug-In for Data Network Devices?

HP OpenView Smart Plug-Ins (SPIs) are ready-to-go modules that put the enterprise operations center back in control of application complexity with instant intelligence. They are pre-configured to easily install and link with the HP OpenView Operations (OVO) console to extend capabilities and more fully manage industry-leading business applications, e-commerce platforms, messaging services, databases, and Internet infrastructure.

HP OpenView Smart Plug-In for Data Network Devices (Network SPI) provides a template group with pre-configured message source templates. These templates consolidate status information from all supported and configured components and devices in the network infrastructure into a single screen. This reduces the time to isolate and repair problems in the network.

What Does the Network SPI Do?

The Network SPI allows HP OpenView Operations to instantly monitor events (SNMP traps and system error messages) that occur on a network device.

The Network SPI does the following:

- Reduces the time-to-value for HP OpenView management solutions in the operations center by providing out-of-the-box coverage of the most popular network devices
- Enriches what the IT operations staff sees in the HP OpenView operations manager console
- Consolidates management information from networks, systems, services, and applications into a single-pane-of-glass
- Reduces event overload from popular network devices by providing out-of-the-box event filters to monitor only what is important

How Does the Network SPI Work?

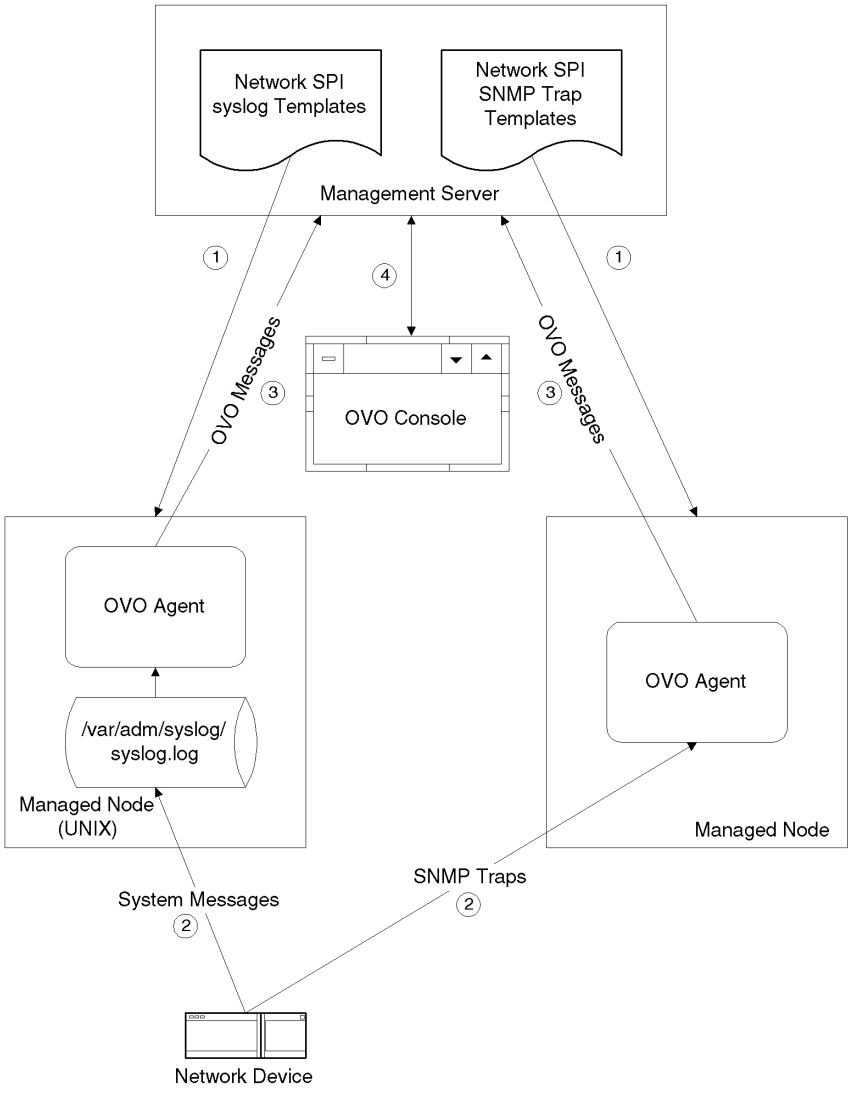
The Network SPI provides pre-configured message source templates that track events (SNMP traps and system error messages) that occur on a network device. These events appear as messages in the OVO Message Browser.

The following list refers to Figure 1-1, “How the Network SPI Works.”

1. Install the Network SPI software on your management server and configure your management server, managed node(s), and network device(s) to work with each other.
2. The OVO agent on a managed node intercepts SNMP traps and system error messages written to the `/var/adm/syslog/syslog.log` file from the network device(s).
3. The agent converts this information into OVO messages and forwards them to the management server.
4. The OVO operator can monitor the events that occur using the Message Browser and react with an appropriate response.

For information on how OVO works, refer to the *HP OpenView Operations for UNIX Concepts Guide.*

Figure 1-1 How the Network SPI Works



2 Installing the HP OpenView Smart Plug-In for Data Network Devices Software

Prerequisites

HP OpenView Operations must be installed before you can use theHP OpenView Smart Plug-In for Data Network Devices (Network SPI).

Hardware/Software Requirements

Operating System	HP-UX 11.0, 11.11, Solaris 2.7, 2.8
Memory	N/A
Disk Space	1.7 Mb in `/opt/OV/OpC/integration` 1.5 Mb for the OVO database
OVO Server and Agent	version 6.0 or later

Network Devices Supported

The Network SPI supports the following network devices:

Cisco Network Devices	
AS5xxx Universal Access Server	AS5200, AS5300, AS5400, AS5800
3600 Series Router	3620, 3640, 3660
7xxx Series Router	7000, 7010, 7200, 7300, 7400, 7505, 7507, 7513, 7603, 7606, 7609
12xxx Series Internet Router	12004, 12008, 12012, 12016, 12410, 12416
Catalyst 2900 Series Switch	2900, 2926
Catalyst 2900 Series XL Switch	2912, 2924
Catalyst 3500 Series XL Switch	3512, 3524, 3548, 3524-PWR, 3508G

Cisco Network Devices	
Catalyst 3550 Series Switch	3550-24, 3550-48, 3550-12G, 3550-12T
Catalyst 4000 Series Switch	4003, 4006
Catalyst 5xxx Series Switch	5000, 5002, 5500, 5505, 5509
Catalyst 6xxx Series Switch	6006, 6009, 6506, 6509
CSS 11000 Content Services Switch	11050, 11150, 11800

f5 Network Devices	
BIG-IP	LoadBalancer

Foundry Networks Network Devices	
BigIron	4000, 8000, 15000

Juniper Networks Network Devices	
M-series Internet Router	M5, M10, M20, M40, M160

Nortel Networks Network Devices	
Alteon	180, 180e, and ACEdirector 2 and 3

Installing/Reinstalling the Network SPI Software

To install or reinstall the Network SPI software on the OVO management server, do the following:

Step 1. Mount the OVO SPI application CD. Refer to *HP OpenView Operations for UNIX Application CD-ROM Release Notes* for more information.

Step 2. Use `swinstall` to install the `B9159AA` fileset.

HP-UX

On an HP-UX system, use the `swinstall` graphical user interface:

1. Type the following: **`/usr/sbin/swinstall -s /<mount_point>/OV_DEPOT/VPO6_OVO7/11.0HPUX.sdtape`**

   The `SD Install - Software Selection` window appears.

2. Highlight `B9159AA`.
3. Select `Actions: Mark for Install` from the menu bar.
4. Select `Actions: Install (Analysis)` from the menu bar.
5. Verify that the analysis phase of the installation completes without errors by clicking on **Logfile**. This displays the `/var/adm/sw/swagent.log` log file. Correct any errors that appear.
6. Click on **OK** to continue with the installation.
7. Exit `swinstall` after the installation completes.

Or on an HP-UX system, use the command line:

1. Type the following: **`/usr/sbin/swinstall -s /<mount_point>/OV_DEPOT/VPO6_OVO7/11.0HPUX.sdtape B9159AA`**
2. Check the `/var/adm/sw/swagent.log` log file and correct any errors that appear.

Solaris

On a Solaris system, use the command line:

1. Type the following: **`/usr/sbin/swinstall -s /<mount_point>/OV_DEPOT/VPO6_OV07/SOLARIS.sdtape B9159AA`**
2. Check the `/var/adm/sw/swagent.log` log file and correct any errors that appear.

3 Configuring the HP OpenView Smart Plug-In for Data Network Devices

To configure the HP OpenView Smart Plug-In for Data Network Devices (Network SPI), do the following:

1. Install the OVO agent on the managed node(s).
2. Assign the Network SPI template group to the managed node(s).
3. Distribute the Network SPI templates to the managed node(s).
4. Configure your network device(s) to report to your managed node(s).
5. Add your network device(s) to the net_devices node group.
6. Assign OVO user responsibilities.

Installing the OVO Agent

The first task in configuring the Network SPI is to install the OVO agent on the managed node(s). Refer to the *HP OpenView Operations for UNIX Administrator's Reference, Volume I* for information on how to install the OVO agent on a managed node.

Assigning the Network SPI Template Groups

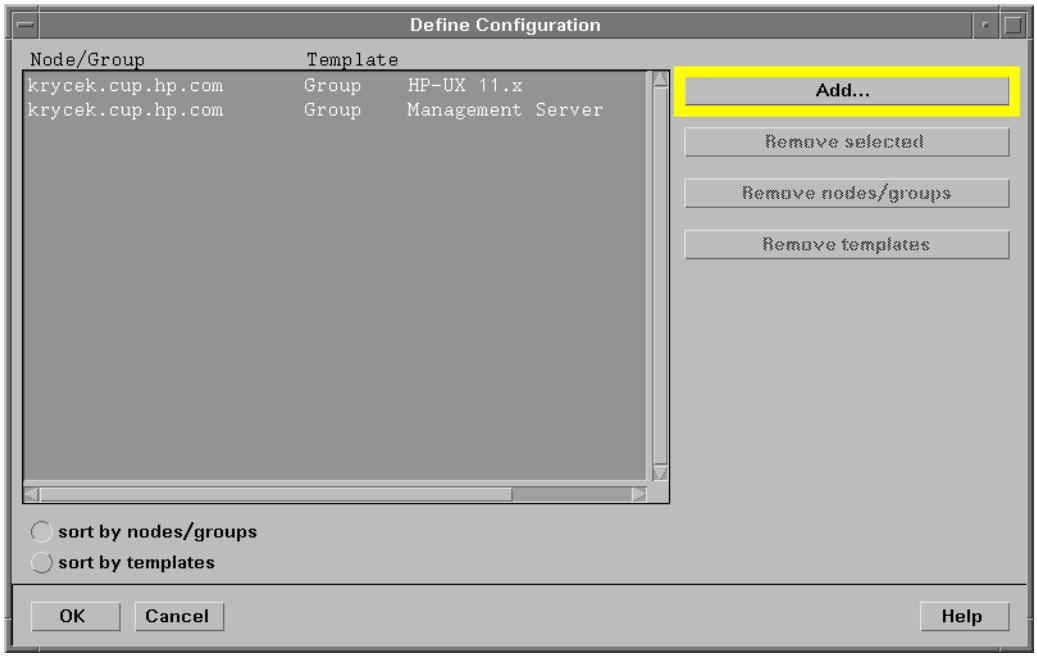
The second task in configuring the Network SPI is to assign templates to the managed node(s) that will be running the Network SPI.

Step 1. As the OVO administrator, open the Node Bank window.

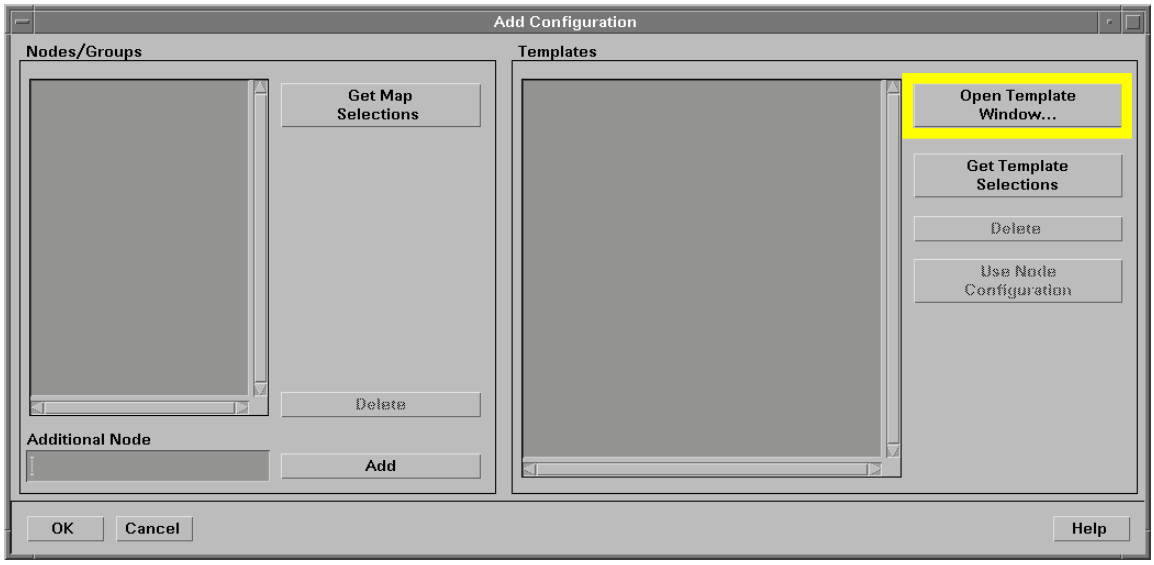
Step 2. Choose the managed node(s) that will be running the Network SPI.

Step 3. Select `Actions: Agents -> Assign Templates` from the menu bar to open the Define Configuration window.

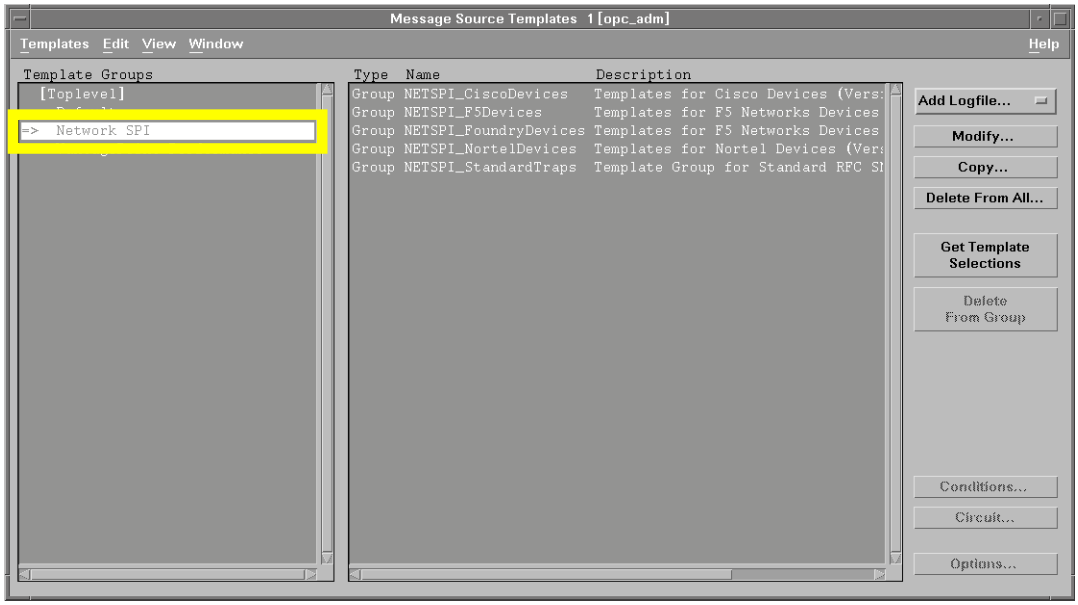
Step 4. Click on **Add** to open the Add Configuration window.



Step 5. Click on **Open Template Window** to open the Message Source Templates window.



Step 6. From the Message Source Templates window, select `Network SPI` from the Template Groups list.



Step 7. From the Add Configuration window, click on **Get Template Selections**. The Group Network SPI template appears under the Templates list.

Step 8. From the Add Configuration window, click **OK**.

Step 9. Close the Message Source Templates window.

Step 10. From the Define Configuration window, click **OK**.

Distributing the Network SPI Templates

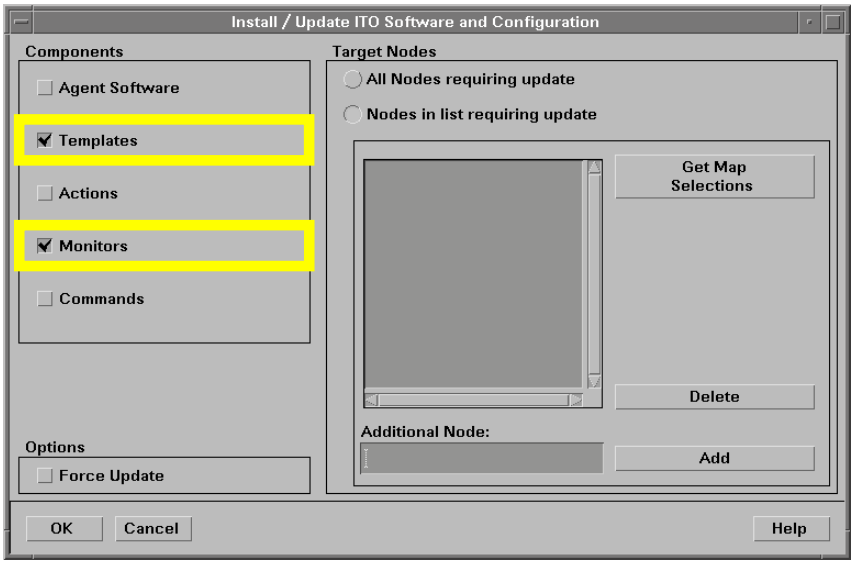
The third task in configuring the Network SPI is to install the Network SPI templates on the management server and distribute them to the managed node(s).

Step 1. From the Node Bank window, choose the managed node(s) that will be running the Network SPI.

Step 2. Select `Actions: Agents -> Install/Update SW & Config` from the menu bar to open the Install/Update ITO Software and Configuration window.

Step 3. Select the checkboxes of the following components:

- Templates
- Monitors



Step 4. Click on **OK**.

Step 5. From the Node Bank window, select `Window: Message Browser` from the menu bar to open the Message Browser window. When the following message appears, the Network SPI templates have been distributed to the managed node(s).

```
The following configuration information was successfully
distributed: Templates Monitors
```

Configuring the Network Device(s)

The fourth task in configuring the Network SPI is to configure your network device(s) to report to the managed node(s). You must direct SNMP traps and syslog messages from the network device(s) to the managed node(s).

To direct SNMP traps from the network device(s) to the managed node(s), do the following:

Step 1. Set the SNMP trap destination on your network device(s) to the managed node(s).

Step 2. Enable all SNMP traps on your network device.

Step 3. If Network Node Manager (NNM) is *not* installed on your managed node(s), add the following to the `/opt/OV/bin/OpC/install/opcinfo` file:

```
SNMP_SESSION_MODE NO_TRAPD
```

To direct syslog messages from the network device(s) to the managed node(s), do the following:

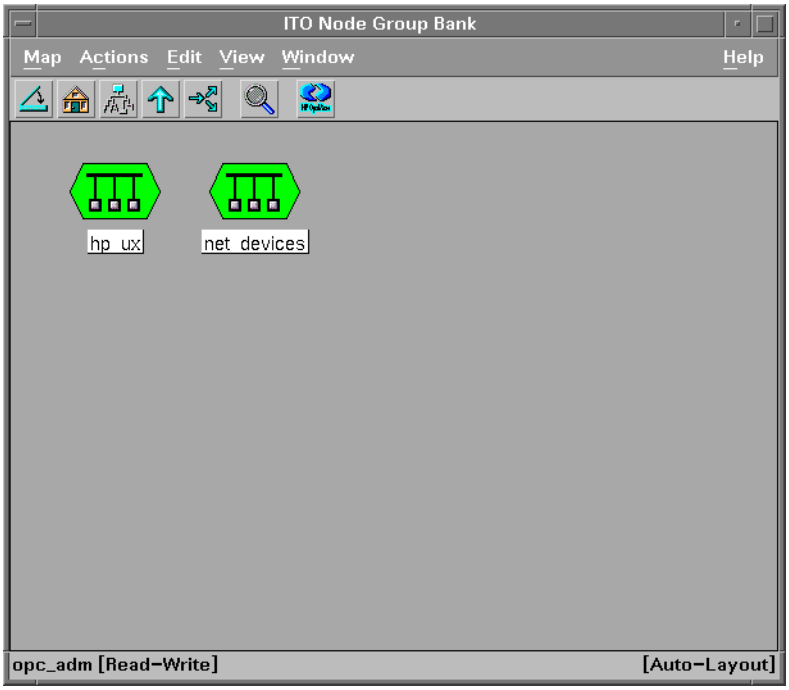
Step 1. Designate a managed node (this managed node must be a UNIX system) to receive syslog messages from your network device(s). Refer to your network device documentation for more information. syslog messages *must* be directed to `/var/adm/syslog/syslog.log` (for example, on a Solaris system, create a link from `/var/adm/messages` to `/var/adm/syslog/syslog.log`).

Step 2. From the Node Bank window, add this managed node as a controlled node. Refer to the online help and/or the “Adding Nodes” section in the *HP OpenView Operations for UNIX Concepts Guide* for more detailed information about adding nodes

Adding the Network Device(s) to the net_devices Node Group

The fifth task in configuring the Network SPI is to add the network device(s) to the net_devices Node Group.

Step 1. Open the Node Group Bank window.



Step 2. Double-Click on `net_devices` to open the NodeGroup: net_devices window.

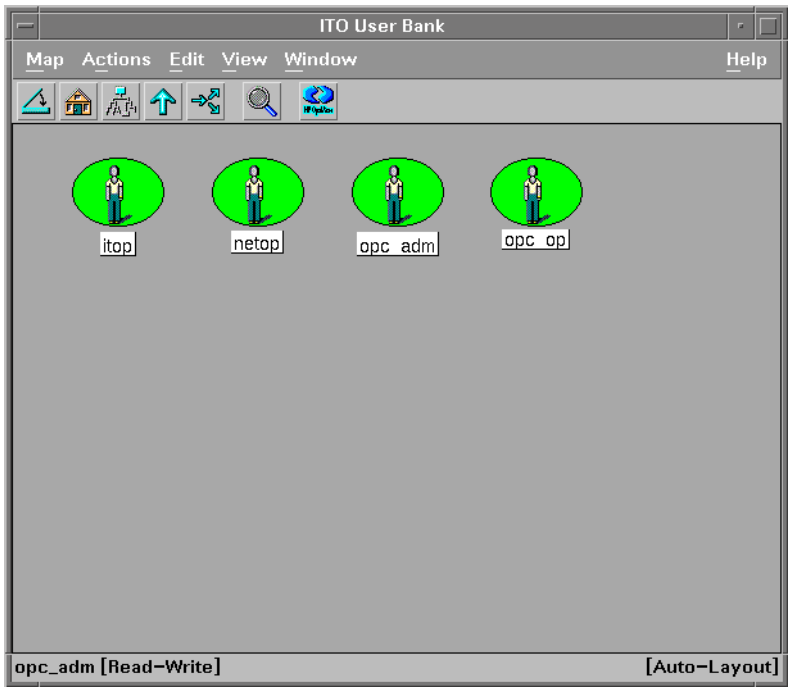
Step 3. Select `Actions: Node -> Add` from the menu bar to add your network device(s)

Refer to the online help and/or the “Adding Nodes” section in the *HP OpenView Operations for UNIX Concepts Guide* for more detailed information about adding nodes.

Assigning User Responsibilities

The final task in configuring the Network SPI is to assign user responsibilities by assigning the Network message group to the net_devices node group for a selected user.

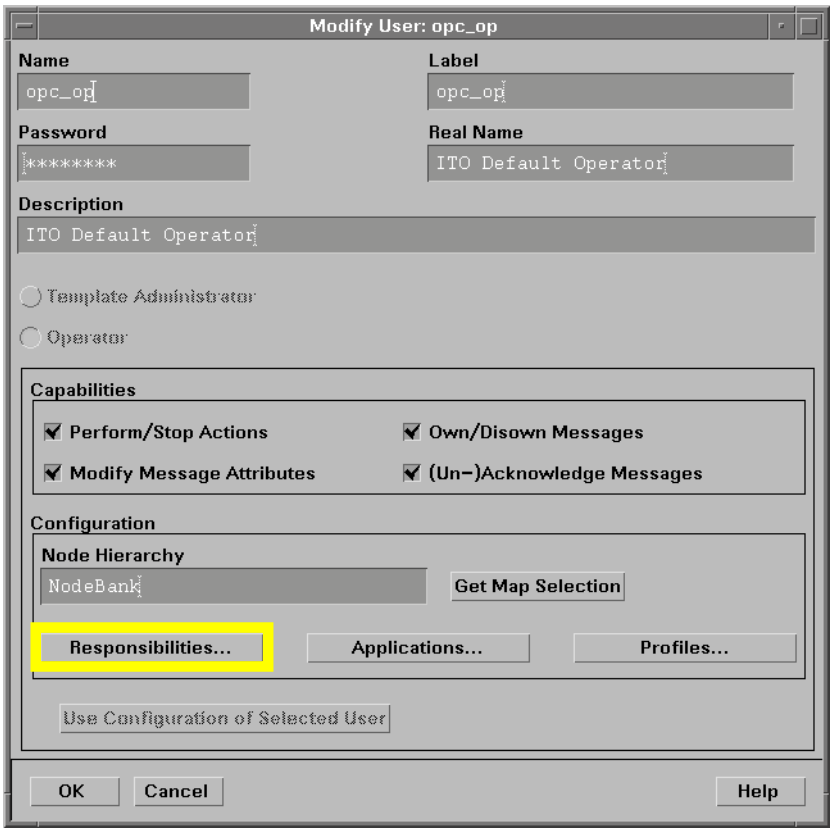
Step 1. As the OVO administrator, open the User Bank window.



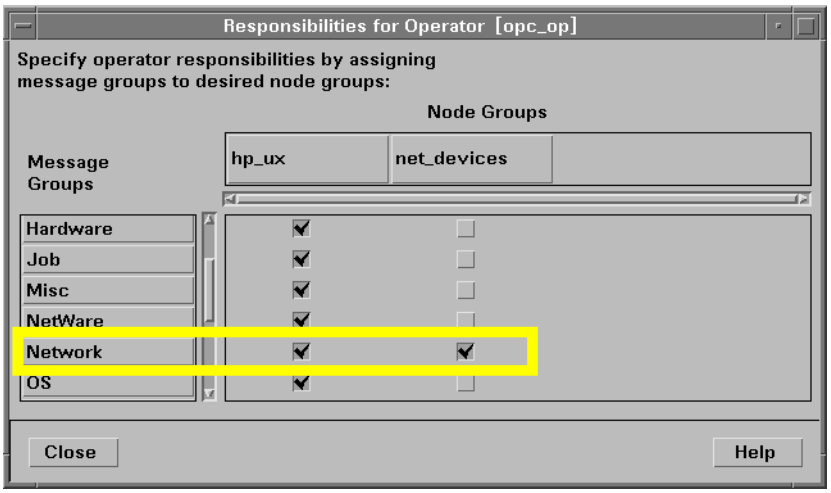
Step 2. Select a user (for example, opc_op).

Step 3. From the User Bank window, select `Actions: User -> Modify` from the menu bar to open the Modify User window.

Step 4. Click on **Responsibilities** to open the Responsibilities for Operator window.



Step 5. Scroll down the Message Group list to `Network` and select the net_devices checkbox.



Step 6. Click on **Close**.

Step 7. Click on **OK**.

Refer to the online help and/or the “Configuring and Maintaining ITO” chapter in the *HP OpenView Operations for UNIX Concepts Guide* for more detailed information about assigning user responsibilities.

4 About the HP OpenView Smart Plug-In for Data Network Devices Templates

This chapter provides the following information about the HP OpenView Smart Plug-In for Data Network Devices (Network SPI) templates:

- template name
- syslog file message types and their default severity levels
- SNMP traps monitored and their default severity levels

For information on using the templates in OVO, refer to the *HP OpenView Operations for UNIX Concepts Guide*.

For information on specific network device SNMP traps and syslog messages, refer to your network device's documentation.

Standard Templates

The following templates can be used with any network device (see “Network Devices Supported” on page 16 for a list of supported network devices):

Table 4-1 Standard Templates

Template Name	syslog Messages/SNMP Traps Monitored	Default Severity
NETSPI_BGP4-MIB	bgpEstablished bgpBackwardTransition	Normal Normal
NETSPI_BRIDGE-MIB	newRoot topologyChange	Warning Warning
NETSPI_ENTITY-MIB	entConfigChange	Minor
NETSPI_FRAME-MIB	frDLCIStatusChange	Warning
NETSPI_Generic	Authentication Failure EGP Neighbor Loss Cold Start Warm Start Link Down Link Up	Suppressed Suppressed Warning Normal Critical Normal
NETSPI_RSVP-MIB	newFlow lostFlow	Normal Normal

Templates for Cisco Network Devices

The following templates can be used with Cisco network devices (see “Network Devices Supported” on page 16 for a list of supported Cisco network devices):

Table 4-2 Templates for Cisco Network Devices

Template Name	syslog Messages/SNMP Traps Monitored	Default Severity
NETSPI_CSSMESSAGES	CHM-1 FLOWMGR-4 IPV4-4:Ipv4IfMgrCctUpdateMsg NETMAN-2 SYSSOFT-2 SYSSOFT-4	Critical Minor Minor Major Major Minor

Table 4-2 Templates for Cisco Network Devices (Continued)

Template Name	syslog Messages/SNMP Traps Monitored	Default Severity
NETSPI_IOSMessages1 NETSPI_IOSMessages2	ALIGN-3-SPURIOUS CLEAR-5-COUNTERS HD-0-NOMEMORY HD-1-BADENCAP IP-3-BADIPALIGN	Major Warning Critical Critical Minor
	IP-3-BADSROUTE IP-4-DUPADDR IPC-2-NOBUFFER IPFAST-4-RADIXDELETE IPRT-3-NOMEMORY	Minor Minor Critical Warning Major
	LANCE-1-NOMEMORY LANCE-5-COLL LANCE-5-LATECOLL NIM-2-BADSLOT OSPF-3-NOMEMORY	Critical Warning Warning Critical Major
	OSPF-4-BADLENGTH RPS-3-MULTFAIL SYS-2-BADSHARE SYS-2-CFORKMEM SYS-2-MALLOCFAIL	Warning Critical Critical Critical Critical
	SYS-3-CONFIG_NV_ERR SYS-3-CPUHOG TCPIP-0-PANIC ALL CRITICAL IOS MESSAGES ALL MAJOR IOS MESSAGES	Minor Major Critical Critical Major
	ALL MINOR IOS MESSAGES ALL WARNING IOS MESSAGES ALL NORMAL IOS MESSAGES	Minor Warning Normal
NETSPI_PIXMessages	ALL CRITICAL PIX MESSAGES ALL MAJOR PIX MESSAGES ALL MINOR PIX MESSAGES	Critical Major Minor
NETSPI_ACCOUNTING-CONTROL-MIB	acctngFileNearlyFull acctngFileFull	Warning Critical
NETSPI_ATM-SOFT-PVC-MIB	atmSoftPvcCallFailuresTrap	Warning

Table 4-2 Templates for Cisco Network Devices (Continued)

Template Name	syslog Messages/SNMP Traps Monitored	Default Severity
NETSPI_CISCO-ACCESS-ENVON-MIB	caemTemperatureNotification caemVoltageNotification	Warning Major
NETSPI_CISCO-ARROWPOINT	apTermSessionLoginFailureTrap apSnmpExtReloadTrap apFlowMgrExtDOSSynTrap apFlowMgrExtDosPingTrap apFlowMgrExtDosSmurfTrap	Major Critical Critical Critical Critical
	apSvcTransitionTrap apFlowMgrExtDosLandTrap apFlowMgrExtDosIllegalTrap	Major Critical Critical
NETSPI_CISCO-ATM-DUAL-PHY-MIB	ciscoAtmDualPhyChange	Warning
NETSPI_CISCO-CHANNEL-MIB	cipCardLinkFailure cipCardDtrBrdLink	Critical Warning
NETSPI_CISCO-CLUSTER-MIB	ccStatusMemberStatusChange	Major
NETSPI_CISCO-CONFIG-MAN-MIB	ciscoConfigManEvent	Suppressed
NETSPI_CISCO-CONTENT-ENGINE-MIB	ciscoContentEngineWriteDiskError ciscoContentEngineWriteTransFailed ciscoContentEngineOverloadBypass ciscoContentEngineDataDiskFailed ciscoContentEngineReadDiskError	Major Major Warning Major Major
NETSPI_CISCO-CONTENT-NETWORK-MIB	ccnNotifNeedsAttention ccnNotifWaitingForCdm ccnNotifOnline ccnNotifOffline	Major Major Normal Major
NETSPI_CISCO-DEVICE-EXCEPTION-REPORTING-MIB	cderMonitoredExceptionEvent	Major
NETSPI_CISCO-DSP-MGMT-MIB	cdspMIBCardStateNotification	Major
NETSPI_CISCO-DSPU-MIG	apSnmpExtReloadTrap	Major

Table 4-2 Templates for Cisco Network Devices (Continued)

Template Name	syslog Messages/SNMP Traps Monitored	Default Severity
NETSPI_CISCO-ENVMON-MIB	ciscoEnvMonRedundantSupplyNotification ciscoEnvMonShutdownNotification ciscoEnvMonVoltageNotification ciscoEnvMonTemperatureNotification ciscoEnvMonFanNotification	Major Critical Major Major Major
NETSPI_CISCO-FLASH-MIB	ciscoFlashCopyCompletionTrap ciscoFlashPartitioningCompletionTrap ciscoFlashMiscOpCompletionTrap cisocFlashDeviceChangeTrap	Normal Normal Normal Normal
NETSPI_CISCO-FLOWMGREXT-MIB	apFlowMgrExtDosSynTrap apFlowMgrExtDosLandTrap apFlowMgrExtDosIllegalTrap apFlowMgrExtDosPingTrap apFlowMgrExtDosSmurfTrap	Critical Critical Critical Critical Critical
NETSPI_CISCO-GATEKEEPER-MIB	ciscoGatekeeperEvent	Minor
NETSPI_CISCO-HSRP-MIB	cHsrpStateChange	Warning
NETSPI_CISCO-ICSUDSU-MIB	ciscoICsuDsuT1LoopStatusNotification ciscoICsuDsuSw56kLoopStatusNotification	Minor Minor
NETSPI_CISCO-IETF-ATM2-PVCTRAP-MIB	atmIntfPvcFailuresTrap	Major
NETSPI_CISCO-IF-THRESHOLD-MIB	cifthTemplateIfStatusChange cifthIfThresholdCleared cifthIfThresholdFired	Major Normal Warning
NETSPI_CISCO-IP-ENCRYPTION-MIB	cieTestCompletion	Normal
NETSPI_CISCO-LOCAL-DIRECTOR-MIB	ciscoLocalDirectorFailoverCableChange ciscoLocalDirectorFailoverUnitStatus ciscoLocalDirectorExVrtualStateChange ciscoLocalDirectorERealStateChange ciscoLocalDirectorFailoverEnablechange	Normal Warning Warning Warning Normal

Table 4-2 Templates for Cisco Network Devices (Continued)

Template Name	syslog Messages/SNMP Traps Monitored	Default Severity
NETSPI_CISCO-NETWORK-REGISTRAR-MIB	ciscoNetRegServerStart ciscoNetRegDNSQueueTooBig ciscoNetRegOtherServerNotResponding ciscoRegDuplicateAddress ciscoNetRegAddressConflict	Normal Major Warning Warning Minor
	ciscoNetRegOtherServerResponding ciscoNetRegFailoverConfigMismatch ciscoNetRegServerStop ciscoNetRegFreeAddressHigh ciscoNetRegFreeAddressLow	Normal Major Normal Warning Warning
NETSPI_CISCO-PIM-MIB	ciscoPimInvalidJoinPrune ciscoPimInvalidRegister ciscoPimInterfaceDown ciscoPimInterfaceUp	Warning Warning Warning Normal
NETSPI_CISCO-SLB-MIB	ciscoSlbRealStateChange ciscoSlbVirtualStateChange	Warning Warning
NETSPI_CISCO-STACK-MIB	ipPermitDeniedTrap lerAlarmOn lerAlarmOff moduleUp moduleDown chassisAlarmOn chassisAlarmOff	Suppressed Warning Normal Normal Major Warning Normal
NETSPI_CISCO-STP-EXTENSIONS-MIB	stpxInconsistencyUpdate stpxRootInconsistencyUpdate	Warning Warning
NETSPI_CISCO-SVCEXT-MIB	apSvcTransitionTrap	Major
NETSPI_CISCO-SYSLOG-MIB	N/A	
NETSPI_CISCO-VLAN-MEMBERSHIP	vmVmpsChange	Warning
NETSPI_CISCO-VOICE-DIAL-CONTROL-MIB	cvdcPoorQoVNotification	Minor

Table 4-2 Templates for Cisco Network Devices (Continued)

Template Name	syslog Messages/SNMP Traps Monitored	Default Severity
NETSPI_CISCO-VTP-MIB	vtpConfigRevNumberError vtpConfigDigestError vtpServerDisabled vtpMtuTooBig vtpVlanRingNumberConfigConflict vtpVersionOneDeviceDetected vlanTrunkPortDynamicStatusChange	Warning Warning Warning Warning Warning Warning Warning
NETSPI_CISCO_SNMPEXT-MIB	apSnmpExtReloadTrap	Major
NETSPI_CISCO_TERMINALMGMT-MIB	apTermSessionLoginFailureTrap	Warning

Templates for f5 BIG-IP Network Devices

The following templates can be used with f5 BIG-IP network devices (see “Network Devices Supported” on page 16 for a list of supported f5 BIG-IP network devices):

Table 4-3 Templates for f5 BIG-IP Network Devices

Template Name	syslog Messages/SNMP Traps Monitored	Default Severity
NETSPI_F5-3DNS-TRAPMessages	POOL YELLOW TO GREEN ECV RED TO GREEN ECV GREEN TO RED POOL GREEN TO YELLOW VIRTUAL SERVER RED TO GREEN	Normal Normal Critical Minor Normal
	SERVER RED TO GREEN CRC FAILURE SERVER GREEN TO RED ACTIVE TO STANDBY STANDBY TO ACTIVE VIRTUAL SERVER GREEN TO RED	Normal Critical Critical Warning Normal Critical
NETSPI_F5Messages	ABORT MESSAGE SHUTDOWN MESSAGE NODE UP MESSAGE NODE DOWN MESSAGE SERVICE UP MESSAGE SERVICE DOWN MESSAGE	Critical Warning Normal Critical Normal Critical
NETSPI_3DNS-MIB	threednsTrapVSRedToGreen threednsTrapServerRedToGreen threednsTrapServerGreenToRed threednsTrapCRCFailure threednsTrapStandbyToActive	Normal Normal Critical Critical Normal
	threednsTrapActiveToStandby threednsTrapPoolGreenToYellow threednsTrapPoolYellowToGreen threednsTrapECVGreenToRed threednsTrapECVRedToGreen threednsTrapVSGreenToRed	Minor Minor Normal Critical Normal Critical

Table 4-3 Templates for f5 BIG-IP Network Devices (Continued)

Template Name	syslog Messages/SNMP Traps Monitored	Default Severity
NETSPI_BIG-IP-MIB	loadBalTrapMisc loadBalTrapServiceDown loadBalTrapServiceUP loadBalTrapReset loadBalTrapDenial	Major Critical Normal Normal Major
	loadBalTrapLogin loadBalTrapRemoveUnit loadBalTrapAddUnit	Normal Major Normal

Templates for Foundry Networks Network Devices

The following templates can be used with Foundry Networks network devices (see “Network Devices Supported” on page 16 for a list of supported Foundry Networks network devices):

Table 4-4 Templates for Foundry Networks Network Devices

Template Name	syslog Messages/SNMP Traps Monitored	Default Severity
NETSPI_FOUNDRYMessages	CRITICAL MESSAGES MAJOR MESSAGES WARNING MESSAGES	Critical Major Warning

Table 4-4 Templates for Foundry Networks Network Devices (Continued)

Template Name	syslog Messages/SNMP Traps Monitored	Default Severity
NETSPI_FOUNDRY-MIB	snTrapChasPwrSupply snTrapChasPwrSupplyFailed snTrapChasFanFailed snTrapTemperatureWarning snTrapDuplicateIp	Critical Critical Minor Critical Major
	snTrapL4MaxSessionLimitReached snTrapL4TcpSynLimitReached snTrapL4RealServerUp snTrapL4RealServerDown snTrapL4RealServerPortUp	Major Major Normal Major Normal
	snTrapL4RealServerPortDown snTrapL4RealServerMaxConnectionLimitReached snTrapL4BecomeStandby snTrapL4BecomeActive snTrapL4GslbRemoteUp	Major Major Warning Normal Normal
	snTrapL4GslbRemoteDown snTrapL4GslbRemoteControllerUp snTrapL4GslbRemoteControllerDown snTrapL4GslbHealthCheckIpUp snTrapL4GslbHealthCheckIpDown	Major Normal Major Normal Major
	snTrapL4GslbHealthCheckIpPortUp snTrapL4GslbHealthCheckIpPortDown snTrapL4FirewallBecomeStandby snTrapL4FirewallBecomeActive snTrapL4FirewallPathUp	Normal Major Major Normal Normal
	snTrapL4FirewallPathDown snTrapL4ContentVerification	Minor Normal

Templates for Juniper Network Devices

The following templates can be used with Juniper network devices (see “Network Devices Supported” on page 16 for a list of supported Juniper network devices):

Table 4-5 Templates for Juniper Network Devices

Template Name	syslog Messages/SNMP Traps Monitored	Default Severity
NETSPI_DCD-SYSLOGMessages	DCD_CLOSE_SOCKET_FAILED DCD_FW_PARSE_ERROR DCD_MALLOC_FAILED DCD_OPEN_SOCKET_FAILED DCD_PARSE_EMERGENCY DCD_PARSE_ERROR DCD_AS_ROOT	Critical Critical Critical Critical Critical Critical Critical
NETSPI_RPD-SYSLOGMessages	RPD_ISIS_ADJUP RPD_ISIS_LSPCKSUM RPD_ISIS_OVERLOAD RPD_ISO_SYSIDDUP RPD_OSPF_NBRDOWN RPD_OSPF_NBRUP RPD_RDISC_NOMULTI RPD_ISIS_ADJDOWN	Normal Critical Critical Critical Major Critical Critical Critical

Table 4-5 Templates for Juniper Network Devices (Continued)

Template Name	syslog Messages/SNMP Traps Monitored	Default Severity
NETSPI_UI-SYSLOGMessages	UI_CMDLINE_READ_LINE UI_COMMIT_ROLLBACK_FAILED UI_DAEMON_ACCEPT_FAILED UI_DAEMON_CHILD_EXITED UI_DAEMON_CHILD_SIGNALED	Normal Critical Critical Critical Critical
	UI_DAEMON_CHILD_STOPPED UI_DAEMON_SELECT_FAILED UI_DAEMON_SOCKET_FAILED UI_DBASE_ACCESS_FAILED UI_DBASE_CHECKOUT_FAILED	Critical Critical Critical Critical Critical
	UI_DBASE_EXTEND_FAILED UI_DBASE_LOGIN_EVENT UI_DBASE_LOGOUT_EVENT UI_DBASE_MISMATCH_ENDIAN UI_DBASE_MISMATCH_MAJOR	Critical Normal Normal Critical Critical
	UI_LOST_CONN UI_MGD_DAEMON_NOT_ME UI_MGD_TERMINATE UI_LOAD_EVENT UI_DBASE_REOPEN_FAILED	Critical Critical Critical Normal Critical
	UI_DBASE_RECREATE UI_DBASE_REBUILD_SCHEMA_FAILED UI_DBASE_OPEN_FAILED UI_DBASE_MISMATCH_SIXE UI_SCHEMA_MISMATCH_MINOR	Critical Critical Critical Critical Critical
	UI_DBASE_MISMATCH_SEQUENCE UI_DBASE_MISMATCH_MINOR UI_AUTH_INVALID_CHALLENGE	Critical Critical Critical
NETSPI_Juniper-CHASSIS-MIB	jnxFanFailure jnxOverTemperature jnxRedundancySwitchover jnxPowerSupplyFailure	Minor Minor Critical Critical

Table 4-5 Templates for Juniper Network Devices (Continued)

Template Name	syslog Messages/SNMP Traps Monitored	Default Severity
NETSPI_Juniper-MPLS-MIB	mplsLspChange mplsLspDown mplsLspUp	Normal Critical Normal

Templates for Nortel Networks Network Devices

The following templates can be used with Nortel Networks network devices (see “Network Devices Supported” on page 16 for a list of supported Nortel Networks network devices):

Table 4-6 Templates for Nortel Networks Network Devices

Template Name	syslog Messages/SNMP Traps Monitored	Default Severity
NETSPI_WEBOSMessages	CRITICAL WEBOS MESSAGES MAJOR WEBOS MESSAGES	Critical Major
NETSPI_Alttrap	altSwRedunPowerSupplyFailure altSwDefGwInService altSwDefGwNotInService altSwSlbRealServerUp altSwSlbRealServerMaxConnReached	Major Normal Major Normal Critical
	altSwSlbBkupRealServerAct altSwSlbBkupRealServerDeact altSwSlbBkupRealServerActOverflow altSwSlbBkupRealServerDeactOverflow altSwSlbFailoverStandby	Major Minor Critical Normal Normal
	altSwSlbRealServerServiceUp altSwSlbRealServerServiceDown altswfltFilterFired altSwFailoverSwitchUp altSwSlbFailoverSwitchDown	Normal Critical Suppressed Normal Critical
	altSwSlbFailoverActive altSwRealServerDown altSwDefGwUp altSwDefGwDown altSwPrimaryPowerSupplyFailure	Critical Major Normal Major Major

5 Removing the HP OpenView Smart Plug-In for Data Network Devices

To completely remove the HP OpenView Smart Plug-In for Data Network Devices (Network SPI), do the following:

1. Delete the Network SPI templates and template groups from the management server.
2. Delete the Network SPI application bank from the management server.
3. Delete the Network SPI templates from the managed node(s).
4. Remove the Network SPI software from the management server.

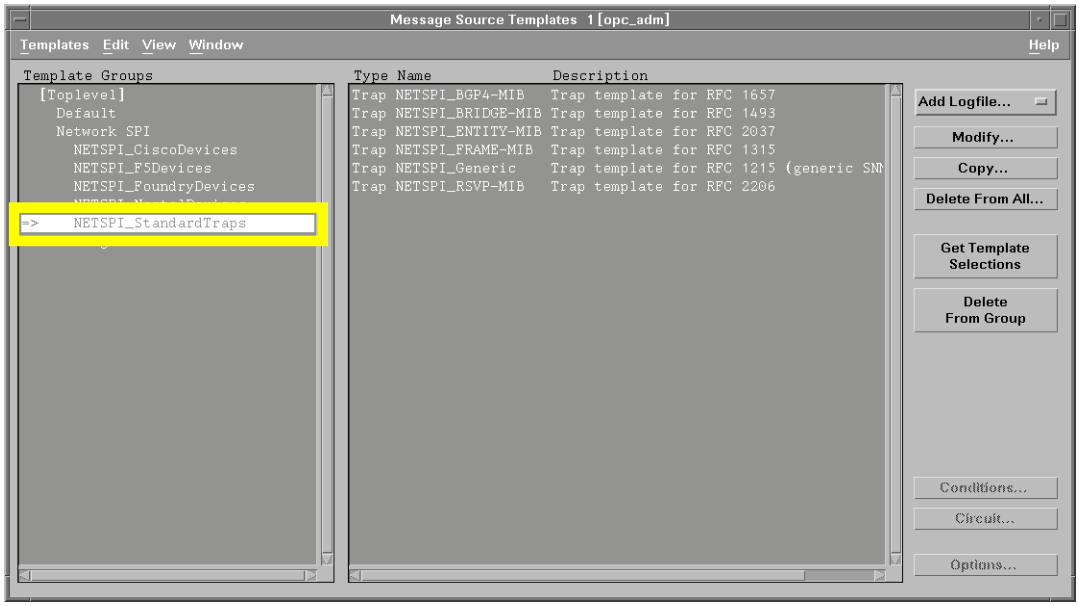
Deleting the Network SPI Templates and Template Group

To delete the templates and template groups from your management server, do the following:

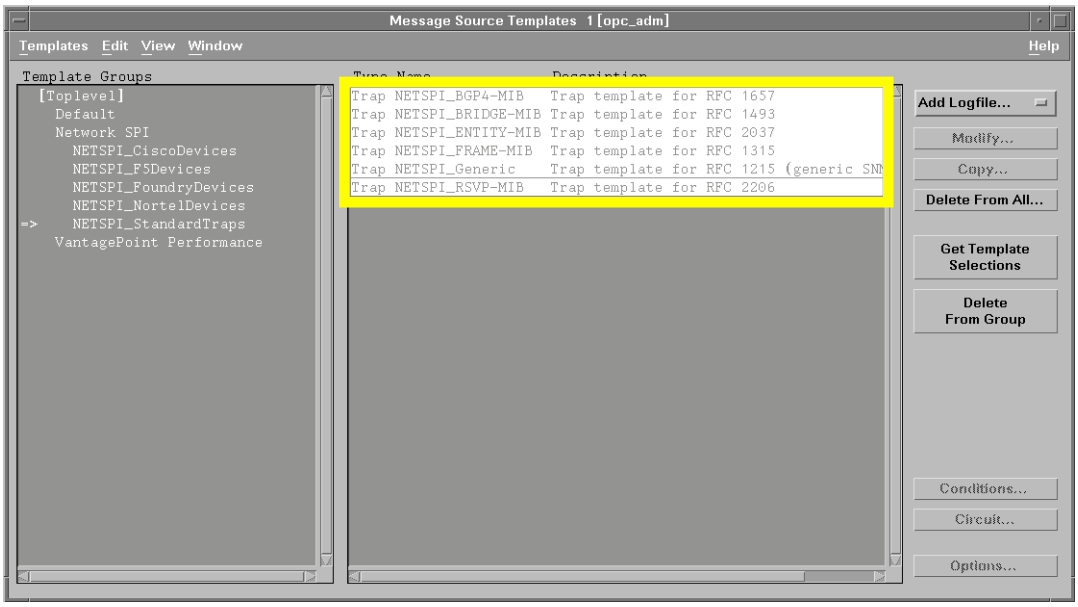
Step 1. As the OVO administrator, open the Message Source Templates window.

Step 2. Double-Click on the `Network SPI` template group.

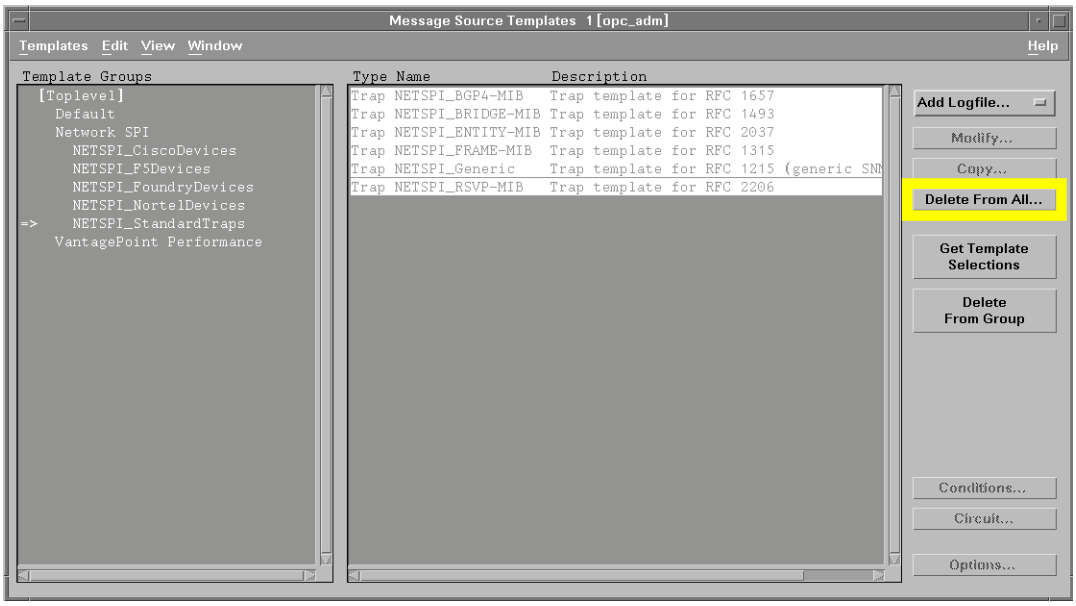
Step 3. Select one of the NETSPI template groups.



Step 4. Highlight all the logfile and trap templates listed in the right window.



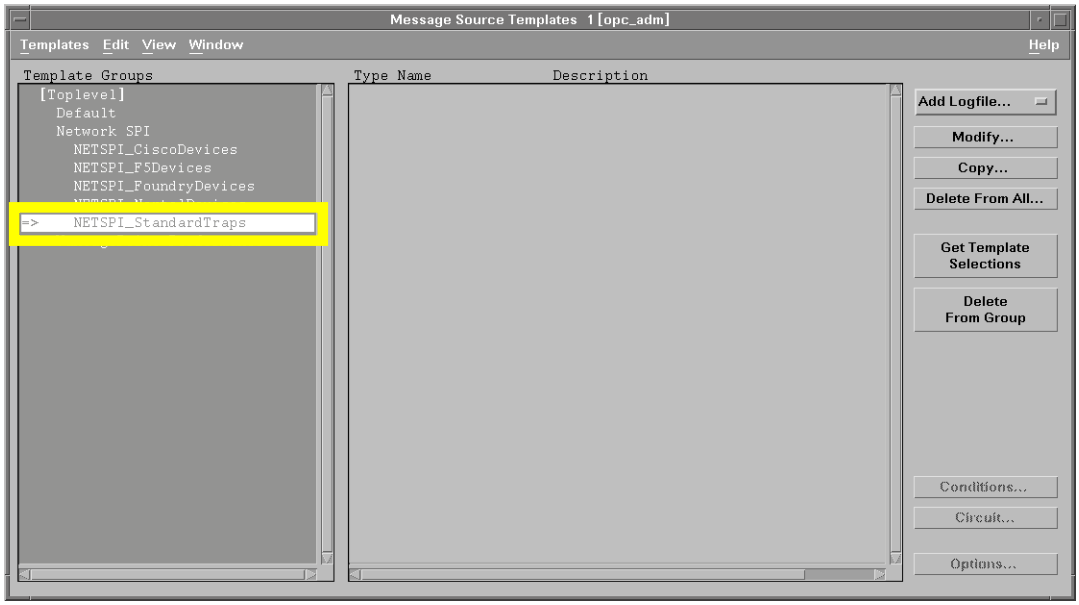
Step 5. Click on **Delete from All** to delete the templates.



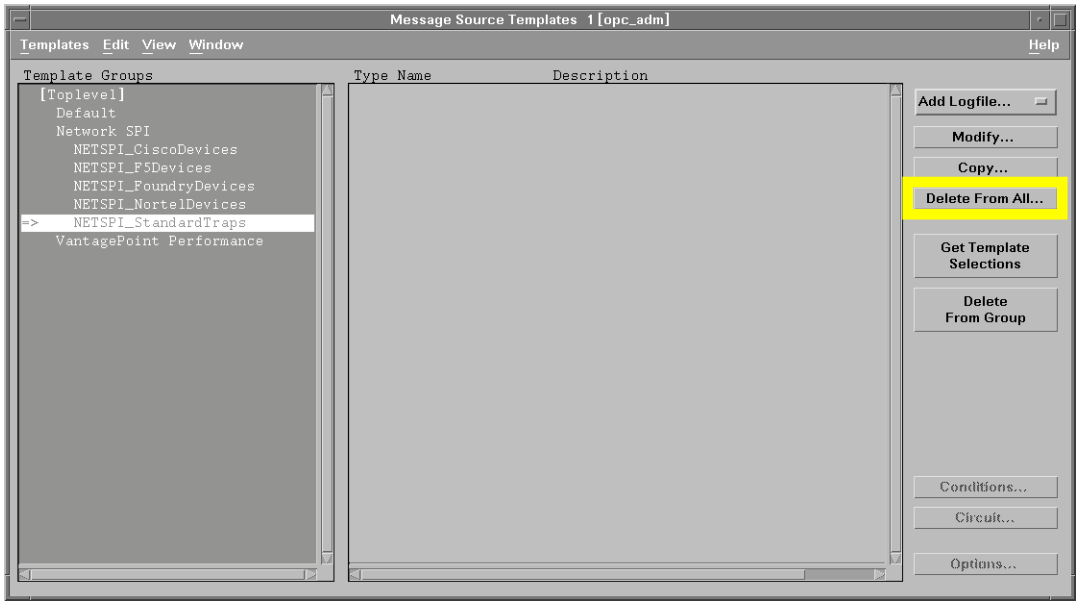
Step 6. Click on **Yes** at the `Do you really want to delete the template(s)?` prompt.

Step 7. Repeat steps 3 - 6 for each NETSPI template group.

Step 8. Select one of the NETSPI template groups.



Step 9. Click on **Delete from All** to delete the template group.



Step 10. Click on **Yes** at the `Do you really want to delete the template(s)?` prompt.

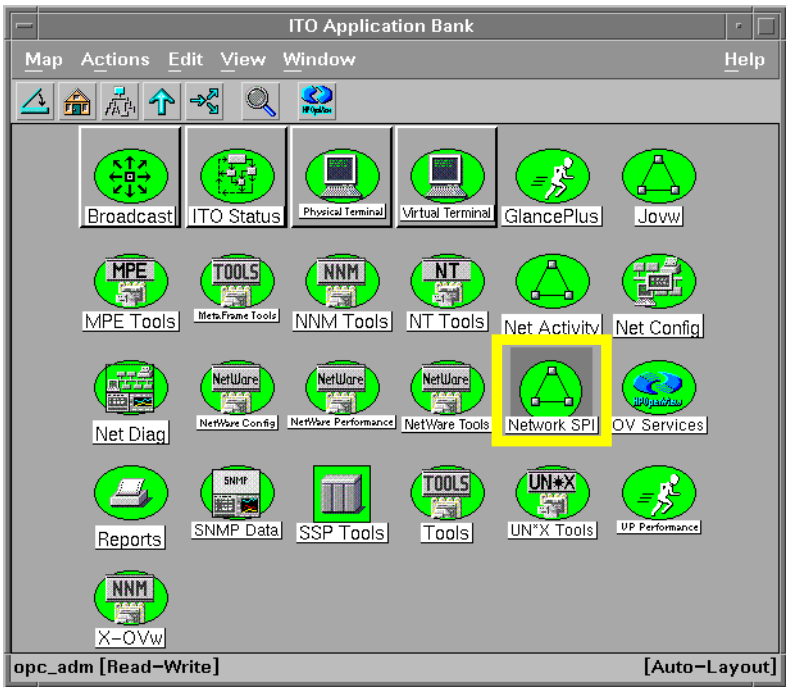
Step 11. Repeat steps 8 - 10 for each NETSPI template group and the `Network SPI` template group.

Deleting the Network SPI Application Bank

To delete the application bank from your management server, do the following:

Step 1. As the OVO administrator, open the Application Bank window.

Step 2. Select the Network SPI icon.



Step 3. Select `Actions: Application -> Delete` from the menu bar.

Step 4. Click on **Yes** at the `Do you really want to delete the applications application groups?` prompt.

Deleting the Network SPI Templates from the Managed Node(s)

To delete the templates from your managed node(s), do the following:

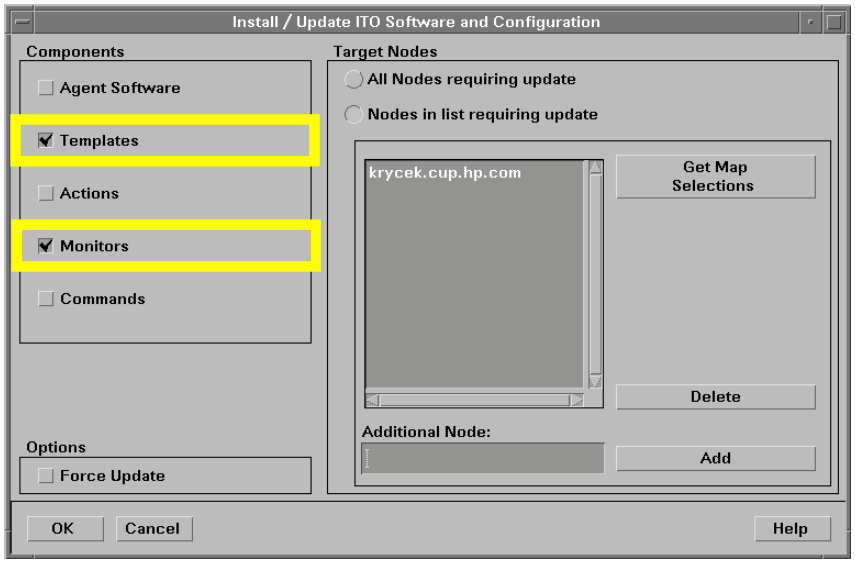
Step 1. As the OVO administrator, open the Node Bank window.

Step 2. Select the managed node(s).

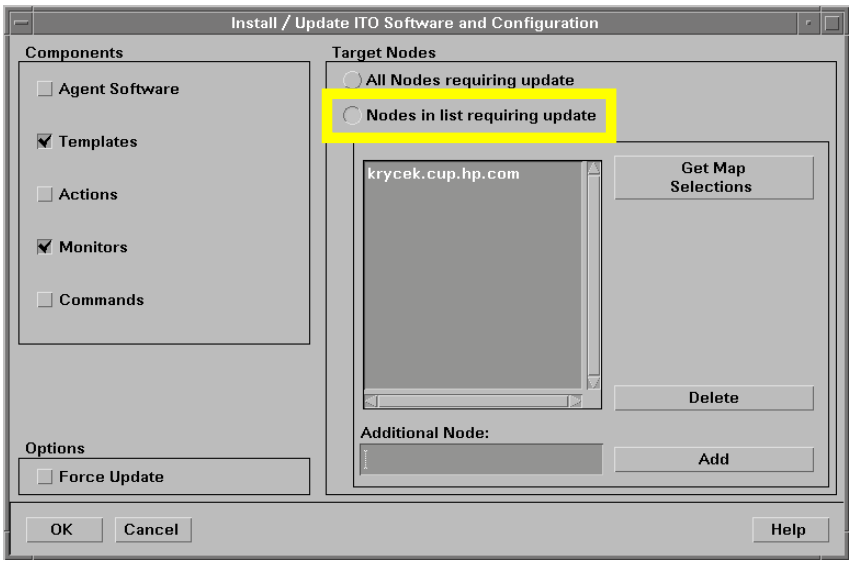
Step 3. Select `Actions: Agents -> Install/Update SW & Config` from the menu bar.

Step 4. Select the checkboxes of the following components:

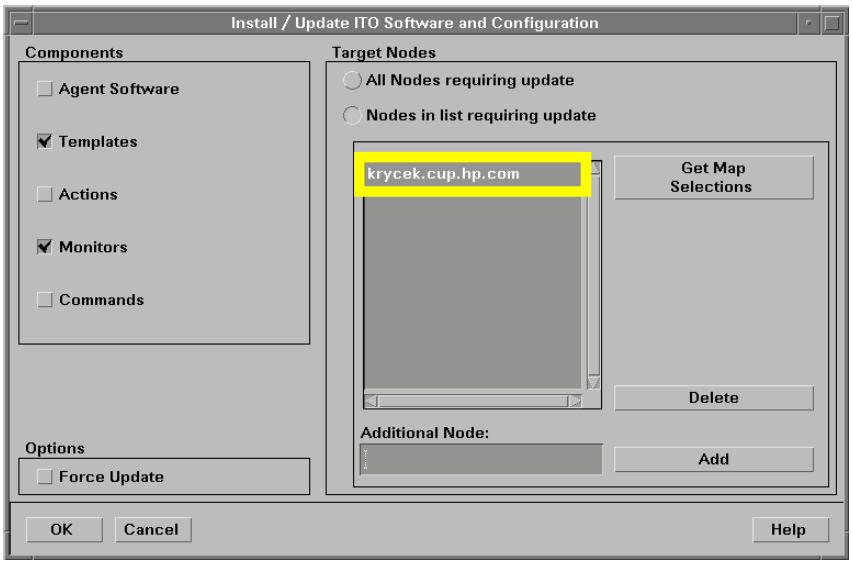
- Templates
- Monitors



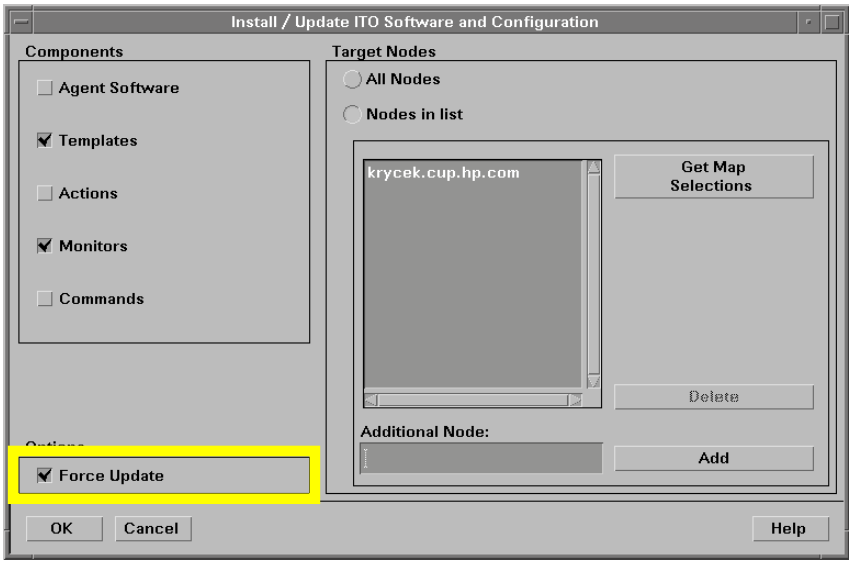
Step 5. Select `Nodes in list requiring update`.



Step 6. Make sure all the managed nodes appear in the Target Node Listbox.



Step 7. Click on **Force Update**.



Step 8. Click on **OK**.

Step 9. Open the Message Browser window. When the following message appears, the Network SPI templates have been deleted from your managed node(s).

```
The following configuration information was successfully
distributed: Templates Monitors
```

Removing the Network SPI Software

To remove the Network SPI software from the management server, do the following:

Step 1. Use `swremove` to remove the software.

Type the following: **`/usr/sbin/swremove B9159AA`**

6 Troubleshooting the HP OpenView Smart Plug-In for Data Network Devices

If you are having problems with the HP OpenView Smart Plug-In for Data Network Devices (Network SPI), check the following:

- ❏ OVO is installed and running on the management server. Refer to the following manuals for more information on OVO: *HP OpenView Operations for UNIX Concepts Guide*, *HP OpenView Operations for UNIX Installation Guide for the Management Server*, *HP OpenView Operations for UNIX Administrator's Reference Volume I*, *HP OpenView Operations for UNIX Administrator's Reference Volume II*, *HP OpenView Operations for UNIX Error Message Reference*, and *HP OpenView Operations for UNIX Software Release Notes*.
- ❏ The Network SPI template group is assigned to the managed node(s). Refer to "Assigning the Network SPI Template Groups" on page 24 for more information.
- ❏ The Network SPI templates are distributed to the managed node(s). Refer to "Distributing the Network SPI Templates" on page 27 for more information.
- ❏ SNMP traps from your network device(s) are directed to the managed node(s). Refer to "Configuring the Network Device(s)" on page 29 for more information.
- ❏ syslog messages from your network device(s) are directed to the managed node(s). Refer to "Configuring the Network Device(s)" on page 29 for more information.
- ❏ If Network Node Manager is *not* installed on your managed node, the `/opt/OV/bin/OpC/install/opcinfo` file has been updated. Refer to "Configuring the Network Device(s)" on page 29 for more information.
- ❏ The syslog daemon (`syslogd`) is up and running on the managed node(s) that are receiving the syslog messages.
- ❏ System error messages are being logged to the `/var/adm/syslog/syslog.log` file on the managed node(s).
- ❏ The network device(s) have been added to the net_devices node group. Refer to "Adding the Network Device(s) to the net_devices Node Group" on page 30 for more information.
- ❏ OVO user responsibilities are assigned. Refer to "Assigning User Responsibilities" on page 31 for more information.

For more information about troubleshooting OVO, refer to *HP OpenView Operations for UNIX Administrator's Reference Volume I*.