

PATROL[®]
for Microsoft Windows
Servers
Getting Started

Version 3.0

January 23, 2003



Copyright 2003 BMC Software, Inc., as an unpublished work. All rights reserved.

BMC Software, the BMC Software logos, and all other BMC Software product or service names are registered trademarks or trademarks of BMC Software, Inc. All other registered trademarks or trademarks belong to their respective companies.

THE USE AND CONTENTS OF THIS DOCUMENTATION ARE GOVERNED BY THE SOFTWARE LICENSE AGREEMENT ENCLOSED AT THE BACK OF THIS DOCUMENTATION.

Restricted Rights Legend

U.S. GOVERNMENT RESTRICTED RIGHTS. UNPUBLISHED—RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES. Use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth in FAR Section 52.227-14 Alt. III (g)(3), FAR Section 52.227-19, DFARS 252.227-7014 (b), or DFARS 227.7202, as amended from time to time. Contractor/Manufacturer is BMC Software, Inc., 2101 CityWest Blvd., Houston, TX 77042-2827, USA. Any contract notices should be sent to this address.

Contacting BMC Software

You can access the BMC Software Web site at <http://www.bmc.com>. From this Web site, you can obtain information about the company, its products, corporate offices, special events, and career opportunities.

United States and Canada

Address BMC Software, Inc.
2101 CityWest Blvd.
Houston TX 77042-2827

Telephone 713 918 8800 or
800 841 2031

Fax 713 918 8000

Outside United States and Canada

Telephone (01) 713 918 8800

Fax (01) 713 918 8000

Customer Support

You can obtain technical support by using the Support page on the BMC Software Web site or by contacting Customer Support by telephone or e-mail. To expedite your inquiry, please see “Before Contacting BMC Software.”

Support Web Site

You can obtain technical support from BMC Software 24 hours a day, 7 days a week at http://www.bmc.com/support_home.html. From this Web site, you can

- read overviews about support services and programs that BMC Software offers
- find the most current information about BMC Software products
- search a database for problems similar to yours and possible solutions
- order or download product documentation
- report a problem or ask a question
- subscribe to receive e-mail notices when new product versions are released
- find worldwide BMC Software support center locations and contact information, including e-mail addresses, fax numbers, and telephone numbers

Support by Telephone or E-mail

In the United States and Canada, if you need technical support and do not have access to the Web, call 800 537 1813. Outside the United States and Canada, please contact your local support center for assistance. To find telephone and e-mail contact information for the BMC Software support center that services your location, refer to the Contact Customer Support section of the Support page on the BMC Software Web site at www.bmc.com/support.html.

Before Contacting BMC Software

Before you contact BMC Software, have the following information available so that Customer Support can begin working on your problem immediately:

- product information
 - product name
 - product version (release number)
 - license number and password (trial or permanent)
- operating system and environment information
 - machine type
 - operating system type, version, and service pack or other maintenance level such as PUT or PTF
 - system hardware configuration
 - serial numbers
 - related software (database, application, and communication) including type, version, and service pack or maintenance level

- sequence of events leading to the problem
- commands and options that you used
- messages received (and the time and date that you received them)
 - product error messages
 - messages from the operating system, such as `file system full`
 - messages from related software

Contents

Chapter 1	Product Components and Capabilities	
	PATROL for Windows Servers Features	1-3
	Centralized Event Filtering and Notification	1-3
	Built-in Recovery Actions	1-3
	Ability to Deploy Configuration Settings	1-4
	Product Components	1-4
	PATROL KM for Microsoft Windows Operating System	1-5
	PATROL KM for Microsoft Windows Active Directory	1-6
	PATROL KM for Microsoft Windows Domain Services	1-7
	PATROL Cluster Configuration Wizard	1-7
	PATROL KM for Microsoft Cluster Server	1-8
	PATROL KM for Microsoft Network Load Balancing	1-8
	PATROL KM for Microsoft COM+	1-8
	PATROL KM for Microsoft Message Queue (MSMQ)	1-10
	PATROL KM for Log Management	1-10
	PATROL Wizard for Microsoft Performance Monitor and WMI	1-10
	PATROL KM for Event Management	1-11
	PATROL KM for History Loader	1-12
	PATROL Adapter for WBEM	1-12
	PATROL Adapter for Microsoft Office	1-12
	PATROL Agent	1-13
	Services	1-13
	Windows Logo Certification	1-13
	Related Documentation	1-14
Chapter 2	Installing and Migrating PATROL for Windows Servers	
	Installation Overview	2-3
	Verifying Installation Requirements	2-3

System	2-3
License Management	2-7
Accounts	2-7
Preloaded Files	2-10
Preparing for Installation	2-12
Determine the Version of the Installation Utility	2-13
Target Computers and Their Roles	2-14
Determining Where to Install KMs Based on Architecture	2-15
Typical and Custom Installation Types	2-16
Installing into the PATROL KMDS	2-17
Installing into a PATROL 3.3.x or 3.4.x Unix Environment	2-17
PATROL Security Levels	2-17
Installing For the First Time	2-18
To Install Using the Typical Installation Type	2-19
Upgrading from an Earlier Version	2-23
Prepare to Upgrade	2-24
Upgrade Without Saving Customizations	2-25
Upgrade and Preserve Customizations	2-32
Migrate Your Customizations	2-41
Creating and Installing Installable Images	2-46
Create an Installable Image	2-47
Install the Created Installable Image	2-48
Installing the Unix Version of the Help Browser	2-49
Additional Considerations for Using Online Help for Unix	2-49
Setting Environment Variables for the Browser	2-50
Uninstalling	2-51

Chapter 3

Loading and Configuring PATROL for Windows Servers

Preparing to Use PATROL for Windows Servers	3-3
Loading KMs	3-4
Loading the PATROL for Windows Servers KMs	3-5
Unloading PATROL for Windows Servers KMs	3-9
Configuring the PATROL KM for Windows OS	3-12
Requirements for Configuring from the PATROL Console	3-12
Configuration Tasks	3-14
Configuring Windows Event Monitoring	3-15
Configuring Registry Key Monitoring	3-17
Configuring Service Monitoring	3-19
Configuring Process Monitoring	3-21
Configuring Recovery Actions	3-24

Creating Custom Parameters	3-26
Creating and Monitoring Windows 2000 Job Objects	3-27
Monitoring Logical or Physical Disk Drives	3-28
Configuring E-Mail Notification	3-29
Command-Line Based, E-Mail Client Required	3-29
Configuring PATROL to Send E-Mail Notifications	3-30
Creating New Parameters with the	
PATROL Wizard for Microsoft Performance Monitor and WMI	3-32
Loading the PATROL Wizard for Microsoft Performance	
Monitor and WMI	3-33
Creating Performance Monitor Parameters	3-34
Creating WMI Parameters	3-36
Configuring the PATROL KM for Log Management	3-37
Selecting Log Files for Monitoring	3-38
Defining Log File Searches	3-40
Using the PATROL Adapter for Microsoft Office to View Reports	3-43
Displaying PATROL Data by Using the PATROL Adapter for	
Microsoft Office	3-44
How to Use the PATROL Adapter for Microsoft Office	3-45
Built-In Report Templates	3-45

Appendix A Accessing Menu Commands, InfoBoxes, and Online Help

Accessing KM Commands and InfoBoxes	A-2
Accessing Online Help	A-3

Appendix B Agent Configuration Variables

Managing Configuration Variables	B-2
PATROL for Windows Servers Configuration Variables	B-2
PATROL KM for Microsoft Windows OS	B-3
PATROL KM for Microsoft Windows Domain Services	B-10
PATROL KM for Microsoft Windows Message Queue	B-13
PATROL KM for Microsoft COM+	B-14
PATROL Wizard for Microsoft Performance Monitor	
and WMI	B-14

Appendix C PATROL for Windows .kml Files

PATROL for Windows Servers .kml Files	C-2
PATROL KM for Log Management	C-2
PATROL KM for Windows OS	C-3
PATROL KM for Microsoft Windows Domain Services	C-6

PATROL KM for Microsoft COM+ (Windows 2000) C-7
PATROL KM for Microsoft Message Queue C-7
PATROL Wizard for Microsoft Performance Monitor
 and WMI C-8
PATROL KM for History Loader C-8
PATROL KM for Event Management C-9

Figures

Figure 2-1	Select Products and Components to Install - Typical Install . . .	2-21
Figure 2-2	Select Products and Components to Install - Custom Install . . .	2-29
Figure 3-1	Configure Windows Event Monitoring Window	3-16
Figure 3-2	Example of Monitored Registry Key and Excluded Subkey . . .	3-18
Figure 3-3	Log File (New) Dialog Box	3-38
Figure 3-4	Select/Deselect Dialog Box	3-39
Figure 3-5	Log Template: (NEW) Dialog Box	3-41

Tables

Table 1-1	PATROL for Windows Servers Services	1-13
Table 2-1	System Requirements for Installing PATROL for Windows Servers	2-4
Table 2-2	Preloaded Files by Product	2-10
Table 2-3	Typical Installation Included Components	2-22
Table 2-4	Choosing an Upgrade Procedure	2-23
Table 2-5	PATROL Installation Directories to Back Up	2-25
Table 2-6	Versions That You Can Migrate	2-33
Table 2-7	Command Line Options for Installing in a KMDS Environment	2-35
Table 2-8	Map File Names	2-44
Table 3-1	PATROL for Windows Servers .kml Files	3-5
Table 3-2	PATROL KM for Windows OS Features that Require Local Administrator Privileges	3-12
Table 3-3	PATROL KM for Windows OS Configuration Tasks	3-14
Table 3-4	PATROL Response to Registry Activity	3-18
Table 3-5	Service Monitoring Options	3-20
Table 3-6	Process Monitoring Options	3-21
Table 3-7	Process Control Options	3-23
Table 3-8	Selecting a Recovery Action Instance	3-24
Table 3-9	Recovery Action Configuration Options	3-25
Table 3-10	PATROL Wizard for Microsoft Performance Monitor and WMI Tasks	3-32
Table 3-11	Configure Event Behavior Dialog Options	3-42
Table 3-12	Reports for PATROL KM for Microsoft Windows Operating System	3-45
Table 3-13	Reports for PATROL KM for Microsoft Windows Domain Services	3-46
Table 3-14	Reports for PATROL KM for Microsoft Message Queue	3-47

Table 3-15	Reports for PATROL for Microsoft COM+.....	3-48
Table A-1	Accessing KM Commands and InfoBoxes.....	A-2
Table A-2	Accessing Online Help.....	A-3
Table B-1	Configuration Variables for PATROL KM for Microsoft Windows OS	B-3
Table B-2	Configuration Variables for the Domain Services Component .	B-10
Table B-3	Configuration Variables for PATROL for Message Queue	B-13
Table B-4	Configuration Variables for PATROL KM for Microsoft COM+ .	B-14
Table B-5	Configuration Variables for PATROL Wizard for Microsoft Performance Monitor and WMI	B-14
Table C-1	PATROL KM for Log Management .kml File	C-2
Table C-2	PATROL KM for Windows OS NT_LOAD.kml File	C-3
Table C-4	PATROL KM for Windows OS NT_BASE.kml File	C-5
Table C-5	PATROL KM for Microsoft Windows Domain Services .kml File	C-6
Table C-6	PATROL KM for Microsoft COM+ (Windows 2000) .kml File	C-7
Table C-7	PATROL KM for Microsoft Message Queue .kml File	C-7
Table C-8	PATROL Wizard for Microsoft Performance Monitor and WMI .kml File	C-8
Table C-9	PATROL KM for History Loader .kml File	C-8
Table C-10	PATROL KM for Event Management .kml Files	C-9

Product Components and Capabilities

PATROL[®] for Microsoft Windows Servers *Getting Started* provides the necessary information and instructions for installing and configuring the *PATROL*[®] for Microsoft Windows Servers product (also referred to as *PATROL* for Windows Servers). This chapter provides a brief overview of *PATROL* for Windows Servers and covers the following topics:

PATROL for Windows Servers Features	1-3
Centralized Event Filtering and Notification	1-3
Built-in Recovery Actions	1-3
Ability to Deploy Configuration Settings	1-4
Product Components	1-4
PATROL KM for Microsoft Windows Operating System	1-5
PATROL KM for Microsoft Windows Active Directory	1-6
PATROL KM for Microsoft Windows Domain Services	1-7
PATROL Cluster Configuration Wizard	1-7
PATROL KM for Microsoft Cluster Server	1-8
PATROL KM for Microsoft Network Load Balancing	1-8
PATROL KM for Microsoft COM+.	1-8
PATROL KM for Microsoft Message Queue (MSMQ)	1-10
PATROL KM for Log Management	1-10
PATROL Wizard for Microsoft Performance Monitor and WMI	1-10
PATROL KM for Event Management	1-11
PATROL KM for History Loader	1-12
PATROL Adapter for WBEM	1-12
PATROL Adapter for Microsoft Office	1-12
PATROL Agent	1-13

Services	1-13
Windows Logo Certification	1-13
Related Documentation	1-14

PATROL for Windows Servers Features

The PATROL for Windows Servers product allows you to monitor and manage the following Windows servers:

- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows NT Server 4.0
- Microsoft Windows NT 4.0 Enterprise Edition
- Microsoft Windows NT 4.0 Terminal Server Edition
- Windows .NET Server
- Windows .NET Advanced Server
- Windows .NET Datacenter Server

Centralized Event Filtering and Notification

Built into the base PATROL product is the ability to centralize and correlate events. This ability enables you to use paging and e-mail to bring issues to the experts' attention for quick resolution. For more information, see “Configuring E-Mail Notification” on page 3-29.

Built-in Recovery Actions

PATROL for Windows Servers provides the following automated, built-in recovery actions. Recovery actions are corrective actions taken by PATROL when a parameter reaches a set value or is in a warning or alarm state.

- backing-up and clearing event logs
- clearing the temp directory
- backing-up and clearing text log
- killing a run-away process
- restarting failed services
- increasing available DFS connections when utilization is high
- increasing share connections when utilization is high
- initiating WINS scavenging when replication fails

For more information on the built-in recovery actions for a specific component, see the online Help for that component.

Ability to Deploy Configuration Settings

PATROL for Windows Servers supports the PATROL Configuration Manager, which allows you to configure and deploy KM configuration settings to other servers in your environment. To support the PATROL Configuration Manager, all PATROL for Windows Servers configuration settings are stored as agent configuration variables. For a complete list of the agent configuration variables for PATROL for Windows Servers, see “Managing Configuration Variables” on page B-2.

Product Components

The PATROL for Windows Servers product includes components and Knowledge Modules (KMs) that manage and monitor elements of your server environment. A KM is a set of instructions that the PATROL Agent uses to monitor objects in your enterprise. For modularity and convenience, these features have been grouped into smaller component pieces, shown below, that can be installed and loaded independently. For a description of each component, see the following sections.

- PATROL KM for Microsoft Windows Operating System (PATROL KM for Windows OS)
- PATROL KM for Microsoft Windows Active Directory
- PATROL KM for Microsoft Windows Domain Services
- PATROL Cluster Configuration Wizard
- PATROL KM for Microsoft Cluster Server
- PATROL KM for Microsoft Network Load Balancing
- PATROL KM for Microsoft COM+
- PATROL KM for Microsoft Message Queue
- PATROL KM for Event Management
- PATROL KM for Log Management
- PATROL Wizard for Microsoft Performance Monitor and WMI
- PATROL Adapter for Microsoft Office
- PATROL Adapter for WBEM

- PATROL Agent for Microsoft Windows
- PATROL KM for History Loader

PATROL KM for Microsoft Windows Operating System

The PATROL KM for Windows OS monitors the availability of your servers, which includes the following elements:

- disk space
- disk drive usage
- cache
- CPU usage
- memory usage
- Windows event logs
- Windows services
- registry keys
- printer status
- NTFS

With the PATROL KM for Windows OS you can also

- monitor and group processes
- monitor and manage services
- monitor and manage printers
- monitor system Stop errors and manage dump files
- create custom composite parameters that are based on existing parameters

For information on configuring these features, see “Configuring the PATROL KM for Windows OS” on page 3-12.

The PATROL KM for Windows Operating Systems also allows you to create and monitor Windows 2000 job objects. Job objects allow you to group related processes so that you can monitor and manage process and total CPU time, minimum and maximum working set (memory usage), active process count, CPU affinity (which CPUs in a multiprocessor system can run the processes) and priority class.

The KM monitors the following job objects properties:

- process control service
- changes to a process priority or affinity

By default, the KM alarms when

- job objects are created or control limits are changed
- applications shut down when they violate a process control limit

Using the The PATROL KM for Windows Operating Systems, you can create job objects on the following servers:

- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows 2000 Datacenter Server

For instructions on how to create and monitor job objects, see “Creating and Monitoring Windows 2000 Job Objects” on page 3-27. For more detailed information, see the PATROL KM for Windows OS online Help.

PATROL KM for Microsoft Windows Active Directory

The PATROL Knowledge Module for Microsoft Windows Active Directory lets you monitor and analyze your Microsoft Windows Active Directory environments. Whether you choose to monitor and analyze one environment or many, PATROL KM for Active Directory helps you

- detect and notify if Microsoft Active Directory generates errors or performs slowly
- monitor performance of system resources
- plan for capacity and availability
- monitor all domain controllers within a site
- monitor all domain controllers between sites within a single domain
- anticipate and eliminate problems before they become apparent to users of the monitored Active Directory environments

For more information, see the *PATROL Knowledge Module for Microsoft Windows Active Directory Getting Started*.

PATROL KM for Microsoft Windows Domain Services

The PATROL KM for Microsoft Windows Domain Services monitors the availability of the following Microsoft Windows NT Domain Controller resources:

- primary domain controller (PDC)
- backup domain controller (BDC)
- member servers

PATROL KM for Microsoft Windows Domain Services monitors:

- Distributed File System (DFS)
- Dynamic Host Configuration Protocol (DHCP) service availability and lease usage
- Domain Name Service (DNS)
- remote server connectivity
- Remote Access Service (RAS) and devices
- replicated directories
- shared directories
- trust relationships
- Windows Internet Naming Service (WINS)

For instructions on how to monitor these features, see the PATROL KM for Microsoft Windows Domain Services online Help system.

PATROL Cluster Configuration Wizard

The PATROL Cluster Configuration Wizard provides an easy-to-use interface with which you can configure the PATROL Agent for failover in a Microsoft Cluster Server environment. While guiding you through the process, the wizard collects the required configuration data and updates the system environment to integrate the PATROL Agent into the cluster.

Configuring the PATROL Agent for failover support allows you to record history data for a clustered application in the same history database. This feature prevents you from having to reconcile the two different history files that are normally created when an application is failed-over from one node to another. For more information, see the *PATROL KM for Windows Clustering Getting Started* and the PATROL Cluster Configuration Wizard Help.

PATROL KM for Microsoft Cluster Server

The PATROL KM for Microsoft Cluster Server monitors, analyzes, and manages activities of a Microsoft Cluster Server and its associated nodes, groups, resources, and services. With the PATROL KM for Microsoft Cluster Server, you can obtain the current status of all essential cluster objects and perform cluster operations from a central point. For more information, see the *PATROL KM for Windows Clustering Getting Started* and the PATROL KM for Microsoft Cluster Server online Help.

PATROL KM for Microsoft Network Load Balancing

The PATROL KM for Microsoft Network Load Balancing provides a central point for monitoring and administrating Microsoft Network Load Balancing clusters and nodes through the PATROL Console. It monitors and manages load balancing of internet/intranet traffic across Microsoft Network Load Balancing cluster nodes. For more information, see the *PATROL KM for Windows Clustering Getting Started* and the PATROL KM for Microsoft Network Load Balancing online Help.

PATROL KM for Microsoft COM+

The PATROL KM for Microsoft COM+ provides functionality to monitor the run-time environment for Microsoft Transaction Server (MTS) on a Windows NT 4.0 server and Microsoft COM+ (COM+) on a Windows 2000 Server.

The PATROL KM for Microsoft COM+ product performs the following actions for Windows 2000 servers:

- monitors the COM+ run-time environment
- monitors the status of COM+ applications
- manages the MS DTC service by providing the capability to start or stop the service
- monitors Windows 2000 COM+ log events
- monitors Windows 2000 log events related to the Microsoft Distributed Transaction Coordinator (MS DTC) service and monitors the MS DTC service status

The PATROL for COM+ product includes the following features for the Windows NT 4.0 servers:

- monitors and manages the Microsoft Transaction Server (MTS)
- monitors MTS package resource usage
- monitors Windows NT log events related to the Microsoft Distributed Transaction Coordinator (MS DTC) service and monitors the MS DTC service status
- manages the MS DTC service by providing the capability to start or stop the service
- monitors MTS log events

For instructions on how to monitor these features, see the PATROL KM for Microsoft COM+ KM online Help system.

PATROL KM for Microsoft Message Queue (MSMQ)

The PATROL KM for Microsoft Message Queue monitors message activity and status, which includes monitoring of

- MSMQ service
- MSMQ queues
- MSMQ messages and roundtrip message time

For instructions on how to monitor these features, see the PATROL KM for Microsoft Message Queue KM online Help system.

PATROL KM for Log Management

The PATROL KM for Log Management monitors binary and text log files in your environment. The KM provides the following statistics about log files

- size
- growth rate
- content

You can also use the PATROL KM for Log Management to

- search log files for a specified text string
- scan the last 'n' lines of a log file

For instructions on how to monitor these features, see the PATROL KM for Log Management online Help system.

PATROL Wizard for Microsoft Performance Monitor and WMI

The PATROL Wizard for Microsoft Performance Monitor and WMI is a powerful but easy-to-use tool that allows you to create new, user-defined PATROL parameters based on Microsoft's Performance Monitor counters or Windows Management Instrumentation (WMI) data. You can also set alarm and warning thresholds for each parameter you create.

This functionality allows you to monitor performance counters and WMI data that are not typically monitored by PATROL. For more information, see “Creating New Parameters with the PATROL Wizard for Microsoft Performance Monitor and WMI” on page 3-32, or the PATROL Wizard for Microsoft Performance Monitor and WMI online Help.

PATROL KM for Event Management

The PATROL KM for Event Management provides event notification, event filtering, message rewording, and centralized alert management. It includes the following features:

- provides highly scalable architecture with redundancy and automatic fail-over
- provides flexible alert configuration options
- provides the following alert settings:
 - notification procedures
 - recovery actions
 - alert message rewording and translation
 - blackout periods
 - notification targets (for example, e-mail or paging systems)
 - parameter thresholds and polling times
- provides the ability to change KM settings without changing BMC Software or third-party PATROL KMs
- checks the availability of agents and hosts
- integrates with any paging solution, compiled executable, or script and provides sample scripts
- simplifies and lowers the cost of integrating enterprise event consoles and tools

For more information, see the *PATROL KM for Event Management User Guide*.

PATROL KM for History Loader

The PATROL KM for History Loader extracts PATROL KM parameter history and loads it into your relational database management system (RDBMS). Once PATROL history data is stored in an RDBMS, you can perform complex analysis and statistical planning on all monitored activity. For more information, see the *PATROL KM for History Loader User Guide*.

PATROL Adapter for WBEM

The PATROL Adapter for WBEM component provides the tools necessary for building a PSL interface to allow PATROL Agents to access Microsoft Windows Management Instrumentation (WMI) data. The product also includes components called PATROL Providers that allow WMI clients access to PATROL data. For more information, see the following documents:

- *PATROL Adapter for WBEM User Guide*
- *PATROL Adapter for WBEM Reference Manual*

PATROL Adapter for Microsoft Office

The PATROL Adapter for Microsoft Office component allows you to connect to a PATROL Agent and gather information without a PATROL Console.

With the PATROL Adapter for Microsoft Office, you can evaluate PATROL data by using Microsoft Excel. The PATROL Adapter for Microsoft Office collects data from PATROL parameters on local or remote hosts and displays the data as a Microsoft Excel chart or graph. You also can create HTML output for Web display.

For more information, see the *PATROL Adapter for Microsoft Office User Guide*. For a list of PATROL Adapter for Microsoft Office reports, see “Displaying PATROL Data by Using the PATROL Adapter for Microsoft Office” on page 3-44.

PATROL Agent

PATROL for Windows Servers includes the PATROL Agent. The PATROL Agent monitors a system according to the instructions provided by loaded PATROL KMs. You can display the information gathered by the PATROL Agent on the PATROL Console. For more information, see the *PATROL Agent Reference Manual*.

Services

The PATROL for Windows Servers product uses the following services:

Table 1-1 PATROL for Windows Servers Services

Service	Component or KM	Installed and Runs by default?
PatrolAgent	PATROL Agent	Yes
Patrol for Windows Operating System Monitor	All PATROL KM for Windows OS application classes	Yes

Windows Logo Certification

The PATROL for Microsoft Windows Servers product has been certified for Microsoft Windows 2000 Server, Advanced Server, and Datacenter Server and has achieved *Designed for Microsoft BackOffice* status through stringent testing by VeriTest.

Related Documentation

For additional information about PATROL for Windows Servers, see the online Help for the component of interest and refer to the PATROL for Windows Servers release notes. For information about the PATROL for Windows Servers parameters, see the product Help or the *PATROL Parameter Reference Manual*. For additional information about PATROL, see the following documentation:

- Help for your PATROL Console
- PATROL Fundamentals Help
- PATROL installation guides for Windows

To view the complete PATROL documentation library, visit the support page on the BMC Software Web site at http://www.bmc.com/support_home. Log on and select a product to access the related documentation.

To log on if you are a first-time user and have purchased a product, you can request a permanent user name and password by registering at the Customer Support page. To log on if you are a first-time user and have *not* purchased a product, you can request a *temporary* user name and password from your BMC Software sales representative.

Where to Go from Here

The following table suggests topics that you should read next:

If you want information on...	See...
how to install the PATROL for Windows Servers product	Chapter 2, "Installing and Migrating PATROL for Windows Servers"
how to load and configure the components using a PATROL console	Chapter 3, "Loading and Configuring PATROL for Windows Servers"
PATROL for Windows Servers agent configuration variables	Appendix B, "Agent Configuration Variables"
KMs included in each PATROL for Windows Servers .KML file	Appendix C, "PATROL for Windows .kml Files"

Installing and Migrating PATROL for Windows Servers

This chapter provides the information that you need to install PATROL for Windows Servers. For additional information about the PATROL installation process, see the *PATROL Installation Reference Manual*. The following topics are discussed in this chapter:

Installation Overview	2-3
Verifying Installation Requirements	2-3
System	2-3
License Management	2-7
Accounts	2-7
Preloaded Files	2-10
Preparing for Installation	2-12
Determine the Version of the Installation Utility	2-13
Target Computers and Their Roles	2-14
Determining Where to Install KMs Based on Architecture	2-15
Typical and Custom Installation Types	2-16
Installing into the PATROL KMDS	2-17
Installing into a PATROL 3.3.x or 3.4.x Unix Environment	2-17
PATROL Security Levels	2-17
Installing For the First Time	2-18
Upgrading from an Earlier Version	2-23
Prepare to Upgrade	2-24
Upgrade Without Saving Customizations	2-25
Upgrade and Preserve Customizations	2-32
Migrate Your Customizations	2-41
Creating and Installing Installable Images	2-46

Create an Installable Image	2-47
Install the Created Installable Image	2-48
Installing the Unix Version of the Help Browser	2-49
Additional Considerations for Using Online Help for Unix	2-49
Setting Environment Variables for the Browser	2-50
Uninstalling	2-51

Installation Overview

This chapter contains instructions for installing PATROL for Windows Servers. For additional installation instructions, see the following documents:

Component	See
<ul style="list-style-type: none">• PATROL Cluster Configuration Wizard• PATROL KM for Microsoft Cluster Servers• PATROL KM for Microsoft Network Load Balancing	<i>PATROL KM for Microsoft Clustering Getting Started</i>
PATROL KM for Microsoft Active Directory	<i>PATROL KM for Microsoft Active Directory Getting Started</i>

Verifying Installation Requirements

Before installing PATROL for Windows Servers, verify that your environment meets the following requirements:

- system
- accounts

System

Verify that the target computer meets the installation requirements listed in Table 2-1 on page 2-4. These requirements apply and supported platforms apply to all PATROL for Windows Servers components unless otherwise noted.

Table 2-1 System Requirements for Installing PATROL for Windows Servers (Part 1 of 3)

Resource	Requirements	Comments
operating systems	<ul style="list-style-type: none"> • Windows 2000 Server (SP1, SP2, and SP3 are supported) • Windows 2000 Advanced Server (SP1, SP2, SP3, and 64-bit Limited Edition are supported) • Windows 2000 Datacenter Server (SP1, SP2, SP3, and 64-bit Limited Edition are supported) • Windows NT Server 4.0 (SP6A with the security patch rollup, SP6A without the security patch rollup) • Windows NT 4.0 Enterprise Edition (SP6A with the security patch rollup, SP6A without the security patch rollup) • Windows NT 4.0 Terminal Server Edition (SP5 is supported) 	<p>The following operating systems are supported on the machine that you install PATROL console components:</p> <ul style="list-style-type: none"> • Windows NT 4.0 Workstation 4.0 (SP6A) • Windows 2000 Professional (SP1, SP2, and SP3) • Windows XP Professional 5.1 <p>PATROL for Windows Servers was built to support Microsoft .NET Server 2003 Standard, Enterprise, and Datacenter Editions (32 and 64 bit). Since .NET Server is not generally available at the time of this release, see the BMC Software Support web site for information regarding official support for .NET once .NET Server 2003 becomes generally available.</p>
PATROL products	<ul style="list-style-type: none"> • PATROL Agent 3.4x • PATROL Classic Console for Microsoft Windows 3.4x • PATROL Classic Console for Unix 3.4x or later (on Solaris and Unix platforms only) • PATROL Central Operator — Windows Edition 7.1x • PATROL Central Operator — Web Edition 7.1.x • PATROL Console Server 7.1.x 	
license	<p>You must have a valid demonstration license (typically good for 30 days) or a permanent license to run your PATROL products. If you do not have a permanent license, contact your BMC Software sales representative or the BMC Software Contract Administration department.</p>	
ports	<p>If you are installing an agent or console with PATROL for Windows Servers, you must specify the port number to connect to all the agent computers and to the Knowledge Module Deployment Server (KMDS).</p>	<p>The default port numbers are 3181 for agents and 3182 for the PATROL KMDS.</p>

Table 2-1 System Requirements for Installing PATROL for Windows Servers (Part 2 of 3)

Resource	Requirements	Comments
disk space needed to install	20 MB for an agent (without components and KMs)	More memory is required to run PATROL with larger applications.
	50 MB for a console (without components and KMs)	More memory is required to run PATROL simultaneously with other Windows applications.
	148 MB for an agent (with all solution components and KMs) (without PATROL KMDS)	
	116 MB for a console (with all solution components and KMs) (without PATROL KMDS)	
	26 MB for PATROL KMDS	Knowledge Modules installed on the PATROL KMDS require the same amount of disk space as the KMs installed on the agents and console.
Monitor (for Console)	256-color display	
	800 x 600 resolution	
File system	FAT or NTFS	HPFS is not supported.
Network	TCP/IP network protocol	
External software products (required only for the components or features listed)	Microsoft Windows NT Resource Kit, Supplement 2 or higher	The PATROL KM for Microsoft Windows Domain Services requires the following Microsoft Windows NT Resource Kit files: <ul style="list-style-type: none"> • dhcpcmd.exe and dhcpsapi.dll for the DHCP Lease Report available on the NT_DHCP application class • dnscmd.exe for the NT_DNS application class, which discovers only on Windows NT 4.0

Table 2-1 System Requirements for Installing PATROL for Windows Servers (Part 3 of 3)

Resource	Requirements	Comments
External software products (required only for the components or features listed)	Java Runtime Environment (JRE) v1.4.0_02 or later	When using PATROL Classic Console for Unix to configure the PATROL KM for Windows OS or the PATROL Wizard for Microsoft Performance Monitor and WMI, you must install the JRE version shown. In addition, if you install JRE in a directory other than %PATROL_HOME%\lib\JRE , you must also set the environment variable \$JAVA_HOME\$ to the full directory path where you installed JRE. On all other consoles besides PATROL Classic Console for Unix, the JRE is automatically installed in %PATROL_HOME%\lib\JRE and no action is required.
	Netscape Navigator version 3.01–4.78	To use online Help with PATROL Classic Console for Unix, you must install this browser. For more information, see “Installing the Unix Version of the Help Browser” on page 2-49.
	SNMP service	To monitor network protocols and to use the following domain monitoring parameters and management features, you must have the SNMP service installed: <ul style="list-style-type: none"> • NT_DHCP parameters • WpReplicationFailures parameter • executing a WINS database scavenge
	command-line based e-mail client	To use the PATROL KM for Event Management to send e-mail notifications when PATROL alarms, you must have a command-line based, e-mail client that is installed and operational.
	WMI	To use the PATROL Wizard for Microsoft Performance Monitor and WMI on Windows NT, you must have WMI installed. WMI is installed by default on Windows 2000 and Windows XP.
	<ul style="list-style-type: none"> • Microsoft Excel 97 (SR1 or SR2) • Microsoft Excel 2000 (SR1) • Microsoft Excel Office XP 	To use PATROL Adapter for Microsoft Office, you must load one of these versions of Microsoft Excel on the console machine.

License Management

OneKey license management software controls BMC Software product licenses, thereby reducing the time and attention that you must devote to administering licenses and passwords.

The OneKey software collects information about the usage of BMC Software products that are OneKey enabled. Individual computers send information to the OneKey Server. You can then produce reports about BMC product usage.

In the current release of PATROL for Windows Servers, the OneKey license management software is not required, although it will be in the future, so BMC Software strongly recommended that you install OneKey when installing PATROL for Windows Servers.

For additional information about OneKey, see the

- *OneKey Licensing Guide*
- *OneKey Server Installation and Administrator Guide*

Accounts

This section describes how to set up a PATROL installation account for Windows and Unix platforms.

Windows Environment

PATROL requires a dedicated user account, known as the PATROL default account, in the Windows environment. The PATROL default account must be created before you install PATROL. The PATROL default account can be either a local or a domain account.

Stand-alone workgroup servers must use a local user account as a PATROL default account. Servers that are trusted members of a domain may use either a local or domain account. In each case, the PATROL default account must be a member of the local Administrators group of the computer where the agent will reside.

PATROL default accounts on domain controllers should be only domain accounts. The account on a domain controller must be a member of the domain Administrators group.

Although you can use an existing Windows user account, BMC Software recommends that you create a separate Windows user account for PATROL.

Warning

Do not use a built-in Windows domain or local Administrator account as the PATROL default account. Such account usage causes files created by PATROL to be owned by the Administrator, which could result in security or file access problems.

Console Connection Accounts

BMC Software recommends that you create a separate account, in addition to the PATROL default account, for PATROL console operators who don't need administrative privileges. Operators can use this account to connect the console to the agent. If you want to configure KMs from the console, however, the console connection account may need administrative rights. For more information, see "Requirements for Configuring from the PATROL Console" on page 3-12.

Unix Environments

BMC Software recommends that the Unix account that you create meet the following conditions:

- The account **.login**, **.profile**, **.cshrc**, and **.kshrc** files should contain as little user customization as possible. Specifically, be sure that the account has no aliases and that no commands in these files can change the unmask setting. The recommended umask setting for the installation account is 022. In addition, verify that the prompt is set to the default.
- Do not use the root account to install PATROL products because this may create security risks.

- Ensure that the account has permission to create directories in the directory where you will install PATROL products.
- Ensure that the computers on which you want to install PATROL have ftp and telnet enabled.

PATROL configuration requires permissions usually reserved for the system administrator. These permissions include access to a root account on the computer where you want to install PATROL.

BMC Software recommends that you install PATROL on local partitions, not on NFS-mounted partitions. If you do install PATROL on NFS-mounted partitions, the root account must have been granted root access permissions on the NFS server.

The account that you use to install PATROL must have permission to write the installation logs to the **\$HOME** and **/tmp** directories on the computer where you are installing products.

Your PATROL product may have other restrictions with regard to the logon accounts and the default PATROL account. Check with your developers for text that more fully describes the logon and PATROL account requirements for your product. Many products require, for example, that the default PATROL account have the same rights as the third-party product that your KM monitors.

Preloaded Files

During the installation, each PATROL for Windows Servers component will automatically preload a basic set of application classes on the PATROL Agent. The preloaded application classes are shown in Table 2-2. For a complete list of application classes by product, see See “PATROL for Windows Servers .kml Files” on page C-2.

Table 2-2 Preloaded Files by Product (Part 1 of 2)

Component	Preloaded .kml File	Application Classes
PATROL KM for Microsoft Windows Operating Systems	NT_BASE.kml	NT.km NT_OS.km NT_CACHE.km NT_CPU.km NT_MEMORY.km NT_PAGEFILE.km NT_SYSTEM.km NT_LOGICAL_DISKS_CONTAINER.km NT_LOGICAL_DISKS.km NT_NTFS_MOUNT_CONTAINER.km NT_NTFS_MOUNT.km NT_NTFS_QUOTA_CONTAINER.km NT_NTFS_QUOTA.km NT_NTFS_JOURNAL.km NT_HEALTH.km INET_NTS.km PATROL_NT.km
PATROL KM for Microsoft COM+	COM.kml	COM_PLUS.km COM_APPLICATIONC.km COM_APPLICATION.km COM_DTC.km MTS_MTS.km MTS_PACKAGEC.km MTS_PACKAGE.km MTS_DTC.km

Table 2-2 Preloaded Files by Product (Part 2 of 2)

Component	Preloaded .kml File	Application Classes
PATROL KM for Microsoft Message Queue	MSMQ.kml	MQ_CONTAINER.km MQ_SERVER.km MQ_QUEUEESC.km MQ_QUEUEES.km MQ_IS.km MQ_ROUNDTRIP.km MQ_SESSIONSC.km MQ_SESSIONS.km
PATROL Wizard for Microsoft Performance Monitor and WMI	NT_PERFMON_WIZARD.kml	NT_PERFMON_WIZARD.km NT_PERFMON_OBJECT.km NT_PERFMON_INSTANCE.km NT_PERFMON_COUNTER.km NT_WMI.km NT_WMI_PARAMETER.km
PATROL KM for Microsoft Windows Domain Services	NTD.kml	NT_DFS_LINK.km NT_DFS_LINK_REPLICA.km NT_DFS_ROOT.km NT_DFS_ROOT_REPLICA.km NT_DHCP.km NT_DHCP_SCOPE.km NT_DNS.km NT_DNS_2000.km NT_DOMAIN.km NT_MEMBER_SERVER.km NT_RAS.km NT_RAS_DEVICE.km NT_REMOTE_SERVERS.km NT_REPL_DIR.km NT_REPL_SVR.km NT_REPLICATION.km NT_SHARES.km NT_TRUST.km NT_USER_ACCOUNTS.km NT_USERS.km NT_WINS.km NT_WINS_PARTNER.km
PATROL KM for Event Management	EVENT_MANAGEMENT.kml	AS_EVENTSRING.km AS_AVAILABILITY.km AS_EVENTSRING_ALL_COMPUTERS.km

Preparing for Installation

BMC Software recommends that you first install PATROL for Windows Servers on a limited number of development or test machines, then configure and test PATROL for Windows Servers before installing it onto production machines.

Note

If you want to install a KM into the PATROL KMDS, *do not launch the installation utility from the installation CD*. See “Upgrade and Preserve Customizations” on page 2-32 for information about how to install into the PATROL KMDS.

The installation utility installs only to a local computer. The installation utility cannot perform remote installations. You must install PATROL for Windows Servers and a PATROL Agent locally on each computer that you want to monitor. You also must install PATROL for Windows Servers and a PATROL Console locally on each computer from which you want to view results.

Note

The installation utility provides you with the ability to create an installable image of the products that you select during install. After you create the installable image, you can export it to a shared **BMC Software** directory to install the package on all computers that share the same **BMC Software** product installation directory, PATROL default logon, PATROL Agent port number, PATROL 3.x product directory, PATROL 7.x product directory, and security option. For more information about creating and exporting installation packages, see “Creating and Installing Installable Images” on page 2-46.

Before you install, you must

- make sure you are using the appropriate version of the installation utility (page 2-13)
- understand target machines and their roles (page 2-14)

- choose between typical and custom installation options (page 2-16)
- choose among PATROL security options (page 2-17)
- (if you are using PATROL KMDS) learn how to install into the KMDS (page 2-32)

Determine the Version of the Installation Utility

The installation instructions contained in this version of PATROL[®] for Microsoft Windows Servers Getting Started pertain to version 7.3.10 of the PATROL Installation Utility. This version of the installation utility might be different from the version included on another product CD or from a version that you downloaded from the BMC Software Electronic Product Download (EPD) site. If you use a version of the PATROL Installation Utility other than version 7.3.10, the instructions in this manual will not accurately describe what you see on your screen.

To determine the version of an installation utility, perform the following steps:

- Step 1** Open a command prompt.
- Step 2** Navigate to the directory where the installation utility is located.
- Step 3** Enter one of the following commands:
- `setup.exe -v` (Windows)
 - `setup.sh -v` (Unix)

A message box displays the version of the installation utility.

Note

If you are using version 7.3.10, the message box displays the version as **7.3.1.0**.

Target Computers and Their Roles

The PATROL installation utility prompts you to select the roles performed by the computer that you are installing BMC Software products on (the target computer). Before beginning the installation process, review the following definitions of the roles that are presented in the installation utility and decide which of these roles is performed by each computer in your environment.

- **Console Systems** (also referred to as console computers) host user desktop applications such as consoles, user interfaces, viewers, console KMs, and browsers. Select this option if the computer to which you are installing will perform any of the following roles:
 - monitor, manage, and develop KMs on Windows by using a PATROL Classic Console for Windows (PATROL 3.x architecture)
 - monitor, manage, and develop KMs on Unix by using a PATROL Classic Console for Unix (PATROL 3.x architecture)
 - monitor and manage on Unix or Windows by using a PATROL Central Operator – Web Edition console (PATROL 7.x architecture)
 - monitor and manage on Windows by using a PATROL Central Operator – Microsoft Windows Edition console (PATROL 7.x architecture)
- **Managed Systems** (also referred to as agent computers) host software that manages the resources on the computer, such as a PATROL Agent, PATROL Knowledge Modules, and Service Reporting Retrievers. Select this option if the computer to which you are installing will perform any of the following roles:
 - host a PATROL Agent 3.5 (works with both the PATROL 3.x and PATROL 7.x architecture)
 - host KMs and components that contain the knowledge that PATROL uses to monitor the resources on this computer

- **Common Services** (new with PATROL 7.x architecture) computers host services that are shared among managed systems and console systems. You can install each of these common services on any computer in the network. Select this option if the computer to which you are installing will perform any of the following roles:
 - host the PATROL Central Operator – Web Edition (PATROL 7.x architecture) Web server
 - host the PATROL Console Servers
 - host the RTservers

If you choose this option, you must install KMs to the selected computer. For more information about where to install KMs, see “Determining Where to Install KMs Based on Architecture” on page 2-15.

For more information about these products, see *PATROL Console Server and RTserver Getting Started*, *PATROL Central Operator – Web Edition Getting Started*, and PATROL Central Operator – Web Edition online Help.

Determining Where to Install KMs Based on Architecture

PATROL 3.x and PATROL 7.x architectures differ as to which target computers store Knowledge Modules and how much KM information is required by each type of system. During installation, ensure that you select the appropriate types of systems according to the following information:

PATROL 3.x

Install KM packages to Managed Systems and Console Systems.

PATROL 7.x

For PATROL Central Operator – Microsoft Windows Edition, install KM packages to Console Systems, Common Services Systems, and Managed Systems.

For PATROL Central Operator – Web Edition, install KM packages to Common Services Systems and Managed Systems.

Typical and Custom Installation Types

The PATROL installation utility prompts you to select one of the following installation types:

- Use the **Typical** installation type in any or all of the following instances:
 - You are new to the product you want to install.
 - You are performing a first-time installation (you are not upgrading).

The Typical installation type installs some components by default when you select other components.

- Use the Custom installation type in any or all of the following instances:
 - You want to install individual components
 - You are upgrading PATROL for Windows Servers from a previously installed version.
 - You are installing into a PATROL 3.3.x or 3.4.x environment.

With each installation type, you can deselect any components that you don't want to install. For more information about what components are installed with each type, see Table 2-3 on page 2-22.

Installing into the PATROL KMDS

If you want to install PATROL for Windows Servers into the PATROL KMDS, you must launch the installation utility from the command line as described in “Migrating Customizations Using the KMDS” on page 2-34.

Installing into a PATROL 3.3.x or 3.4.x Unix Environment

If you are installing PATROL for Windows Servers into a *Unix* environment that has PATROL 3.3.x or PATROL 3.4.x installed, you must launch the installation utility from the command line using the `-releaseversion` option as described in “Upgrading from an Earlier Version” on page 2-23.

PATROL Security Levels

You can secure the data passed between PATROL components and restrict unauthorized users from accessing your data by implementing PATROL security. PATROL contains five *security policy* levels in a predefined set of security configurations that you can select from when you install PATROL.

Basic security (level 0) is a minimal level of security with no configuration requirements. At the highest level of advanced security (4), all communicating components must authenticate with each other and key databases must validate connection requests.

High security requires more configuration of the communicating components (the agent and the console) and is more difficult to use than lower levels of security. You can select the security level that best balances the ease of use with your need for security.

All components in a system, including agents and consoles, must operate at the same level of security in order to communicate with each other. This requirement is ensured when you install PATROL with basic security (the default level of 0).

Review the security level definitions in the PATROL Security User Guide before installing PATROL to determine the appropriate security level for your system needs. If you want to implement a new security level after having previously installed PATROL security, see the PATROL Security User Guide for instructions.

For more information about implementing and using PATROL security, see the following documentation:

- *PATROL Security User Guide*
- *PATROL Security Release Notes*

How PATROL Security Affects the PATROL for Windows Servers

PATROL security is installed as part of the agent and console. KMs inherit the security policy from the agent and console on which they are installed.

Installing For the First Time

The PATROL Installation utility offers two types of installations: Typical and Custom. For a description of the two types of installations, please see “Typical and Custom Installation Types” on page 2-16. BMC Software recommends using the Typical installation type in the following situations:

- if you are new to PATROL and you want to use default product configuration values

- if you are installing PATROL for Windows Servers for the first time into an existing PATROL environment, and you are installing into the default product installation directories as listed in the following table:

PATROL Version	BMC Products Installation Directory	PATROL Product Subdirectory
3.4	<i>homedrive:\Program Files\BMC Software</i> (Windows)	PATROL3-4 (Windows)
	user's home directory (Unix)	PATROL3.4 (Unix)
3.5	<i>homedrive:\Program Files\BMC Software</i> (Windows)	Patrol3 (Windows and Unix)
	<i>/opt/bmc</i> (Unix)	

Note

By default, the Typical installation type configures the PATROL Agent to connect through port 3181. If you want to connect the agent from a different port, you must use the Custom installation type. See “Upgrading from an Earlier Version” on page 2-23 for instructions about using the Custom installation type.

Before You Begin

You first should install on a limited number of machines in the test environment, test the installation thoroughly, and then install in your production environment.

To Install Using the Typical Installation Type

- Step 1** From the installation CD or from an electronically downloaded installation (EPD) image, run **setup.exe** (Windows) or **setup.sh** (Unix).
- Step 2** In the Welcome to the Installation Utility window, click **Next** to begin your installation.

Step 3 Review the license agreement, select **Accept**, and click **Next** to continue.

Step 4 In the Select Installation Option window, select one of the following options:

- If you want to install the products without creating an installable image, select **I want to install products on this computer now** and click **Next** to continue.
- If you want to create an installable image that you can use to install the products on this computer and other computers later, select **I want to create an installable image to be installed later**, enter the directory where you want to store the installable image, and click **Next** to continue.

Note

If you select to create an installable image, all of the computers where you plan to use the installable image must share the same **BMC Software** product installation directory, PATROL default logon, PATROL Agent port number, platform, and security option. For more information, see “Creating and Installing Installable Images” on page 2-46.

Step 5 In the Select Type of Installation window, select **Typical** and click **Next** to continue.

Step 6 In the Specify Installation Directory window, accept the default directory and click **Next** to continue.

Step 7 In the Select System Roles window, select **Managed Systems**, **Console Systems**, or both to indicate the components you want to install and click **Next**.

- Select **Console Systems** if you are installing to a computer that hosts or will host a PATROL Console.
- Select **Managed Systems** if you are installing to a computer that hosts or will host a PATROL Agent.

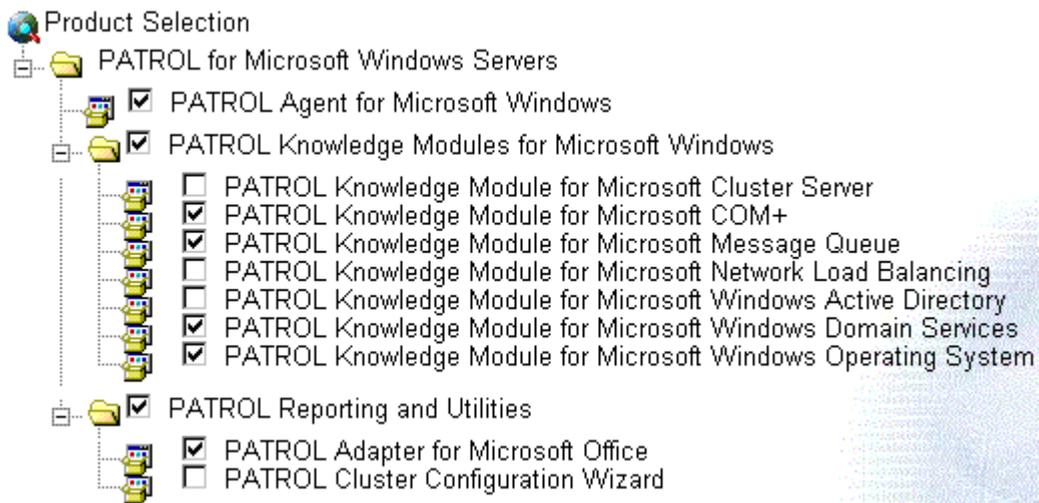
For more information, see “Target Computers and Their Roles” on page 2-14.

Note

For more information about the PATROL consoles, PATROL Console Server, or RT Server, see the *PATROL Central Operator – Web Edition Getting Started* and the *PATROL Console Server and RTserver Getting Started*.

- Step 8** From the Select Products and Components to Install window, select components that you want to install (see Figure 2-1 on page 2-21 and Table 2-3 on page 2-22) and click **Next**.

Figure 2-1 Select Products and Components to Install - Typical Install



When you select the products or components shown in Table 2-3, the components listed are installed automatically.

Table 2-3 Typical Installation Included Components

Selectable Product or Component	Included Components
PATROL Knowledge Module for Microsoft Windows Operating System	<ul style="list-style-type: none"> • PATROL Knowledge Module for Event Management • PATROL Knowledge Module for Log Management • PATROL Knowledge Module for OneKey Usage • PATROL Wizard for Microsoft Performance and WMI
PATROL Adapter for Microsoft Office	PATROL Adapter for Microsoft Office—Server Report Templates
PATROL Reporting and Utilities	PATROL Service Reporting History Retriever

Step 9 In the PATROL Default Account Properties window, enter the user name and password that you want to use for your PATROL default account and click **Next**. You should have created this account manually before you began to install PATROL. (For more information about the PATROL Account, see “Accounts” on page 2-7.)

Step 10 Complete the remaining windows. The number and content of the windows depend on your KM selections and your inputs to the windows. Click **Help** as needed to complete the windows.

Step 11 In the Review Selections and Install or the Review Selections and Create Installable Image window, review the selections carefully to make sure they are correct.

- If you want to change your selections, click **Back** and make those changes.
- If the selections are correct, select **Start Install** to start installing or **Create Image** to start exporting the image to the directory you entered in Step 4 on page 2-20.

A status window opens that contains current messages, current milestones and percent complete.

Note

If you selected to create an installable image to install on several computers or on the local computer at a later time, see “Creating and Installing Installable Images” on page 2-46.

Step 12 When the status window reports that the installation is 100% complete, click **Next** to view the results window. (*Next* does not appear until the installation is 100% complete.)

Step 13 In the results window, click **View Log** to review the details of the installation or click **Exit** to close the installation utility.

Upgrading from an Earlier Version

If you have a previous version of PATROL for Windows Servers installed on the target computer, you have two options for upgrading to the new version of PATROL for Windows Servers. Use Table 2-4 to help you choose an upgrade procedure.

Table 2-4 Choosing an Upgrade Procedure

Choose This Procedure	If You Have This Situation
Upgrade Without Saving Customizations	<ul style="list-style-type: none">• have not made any customizations to your previous version of PATROL for Windows Servers• want to overwrite your customizations with the default values of the new version of PATROL for Windows Servers• have a currently installed version of PATROL for Windows Servers that cannot be migrated (See “Versions That You Can Migrate” on page 2-33)
Upgrade and Preserve Customizations	made customizations to your previously installed version of PATROL for Windows Servers and want to save those customizations and migrate them to the new version of PATROL for Windows Servers

Whether you choose to save and migrate your KM customizations or not, the customizations you have made to agents and consoles are preserved and incorporated into the new version automatically. Only customizations to Knowledge Modules must be migrated.

Note

Throughout this section, all references to *PATROL_HOME* represent *\$PATROL_HOME* in Unix and *%PATROL_HOME%* in Windows; all references to *PATROL_CACHE* represent *\$PATROL_HOME/patrol* in Unix and *%PATROL_CACHE%* in Windows.

Prepare to Upgrade

Whether you are upgrading and migrating customizations or simply upgrading, you must first

- back up the current installation
- remove PATROL for Windows Servers files from *PATROL_CACHE*

Back Up the Current Installation

Whether you are upgrading and migrating any customizations or simply upgrading, back up the current PATROL installation before starting to install. Follow these steps to back up the current installation:

- Step 1** Shut down any PATROL Agents, Consoles, and related services that are currently running.
- Step 2** Ensure that no one is accessing any PATROL files or directories.

- Step 3** Perform a full backup of the two directories where PATROL executables and data are typically stored. These directories are listed in Table 2-5.

Table 2-5 PATROL Installation Directories to Back Up

Operating System	Directory
Windows	%PATROL_HOME% for agent and console installation directories %PATROL_CACHE% for the console working cache
Unix	\$PATROL_HOME for agent and console installation directories \$PATROL_CACHE for the console working cache
Linux	\$PATROL_HOME for agent and console installation directories \$PATROL_CACHE for the console working cache

Remove PATROL for Windows Servers Files from *PATROL_CACHE*

You must remove the current PATROL for Windows Servers files from the *PATROL_CACHE* directory for the console. If you do not, old product files in *PATROL_CACHE* are loaded instead of the newly installed files from *PATROL_HOME*.

Delete all PATROL for Windows Servers files with the following naming patterns from *PATROL_CACHE\knowledge* and *PATROL_CACHE\psl*:

- NT_*
- BSK*
- COM*
- MQ*
- MSDM*
- DT*
- WEBM*

Upgrade Without Saving Customizations

Use this procedure in the following circumstances:

- you have performed the procedures in “Prepare to Upgrade” on page 2-24

- you want to install PATROL for Windows Servers into an existing PATROL environment
- you want to install individual components
- you want to upgrade PATROL for Windows Servers, but do not want to migrate existing customizations to PATROL for Windows Servers

Step 1 If you are installing into PATROL 3.3.x or 3.4.x in a *Unix* environment, follow these steps to start the installation utility. If you are installing into PATROL 3.3.x or 3.4.x in a Windows environment or into PATROL 3.5 in a Unix or Windows environment, skip to Step 2.

- 1.A** Open a command line prompt.
- 1.B** Change to the drive where the installation CD is located.
- 1.C** At the Unix command line prompt, enter **setup.sh -releaseversion *v.r*** where *v.r* is the version of the PATROL environment into which you are installing.
- 1.D** Skip to Step 3.

Step 2 From the installation CD or from an electronically downloaded installation (EPD) image, run **setup.exe** (Windows) or **setup.sh** (Unix).

Step 3 In the Welcome to the Installation Utility window, click **Next** to begin your installation.

Step 4 In the Review License Agreement window, review the license agreement, select **Accept**, and click **Next** to continue.

Step 5 In the Select Installation Option window, select one of the following options:

- If you want to install the products without creating an installable image, select **I want to install products on this computer now** and click **Next** to continue.

- If you want to create an installable image that you can use to install the products on this computer and other computers later, select **I want to create an installable image to be installed later**, enter the directory where you want to store the installable image, and click **Next** to continue.

Note

If you select to create an installable image, all of the computers where you plan to use the installable image must share the same **BMC Software** directory, PATROL default logon, PATROL Agent port number, platform, and security option. For more information, see “Creating and Installing Installable Images” on page 2-46.

Step 6 From the Select Type of Installation Window, select **Custom** and click **Next**.

Step 7 In the Specify Installation Directory window, enter the correct information based on your installation scenario and click **Next**.

Installation Option	Directory	Example
PATROL for Windows Servers into an existing PATROL 3.4 environment	the directory path up to the PATROL product directory	To install PATROL into D:\Program Files\BMC Software\PATROL3-4 , enter D:\Program Files\BMC Software in the Specify Installation Directory window.
PATROL for Windows Servers into an existing PATROL 3.4 environment where previously installed PATROL products are in a top-level directory such as C:\PATROL3-4	the full directory path to your previously installed products	To install into the previously installed directory C:\PATROL3-4 , enter C:\PATROL3-4 in the Specify Installation Directory window.

Installation Option	Directory	Example
PATROL for Windows Servers into an existing PATROL 3.5 environment	the directory path up to the PATROL product directory	To install PATROL into D:\Program Files\BMC Software\Patrol3 , enter D:\Program Files\BMC Software in the Specify Installation Directory window.
PATROL for Windows Servers into an existing PATROL 3.5 environment where previously installed PATROL products are in a top-level directory such as C:\PATROL3-5	the full directory path to your previously installed products	To install into the previously installed directory C:\PATROL3-5 , enter C:\PATROL3-5 in the Specify Installation Directory window.

The PATROL product directory is appended to the path that you enter in this step. You will specify the PATROL installation directory in Step 10 on page 2-29.

Step 8 In the Select System Roles window, select **Managed System, Console System**, or both and click **Next**.

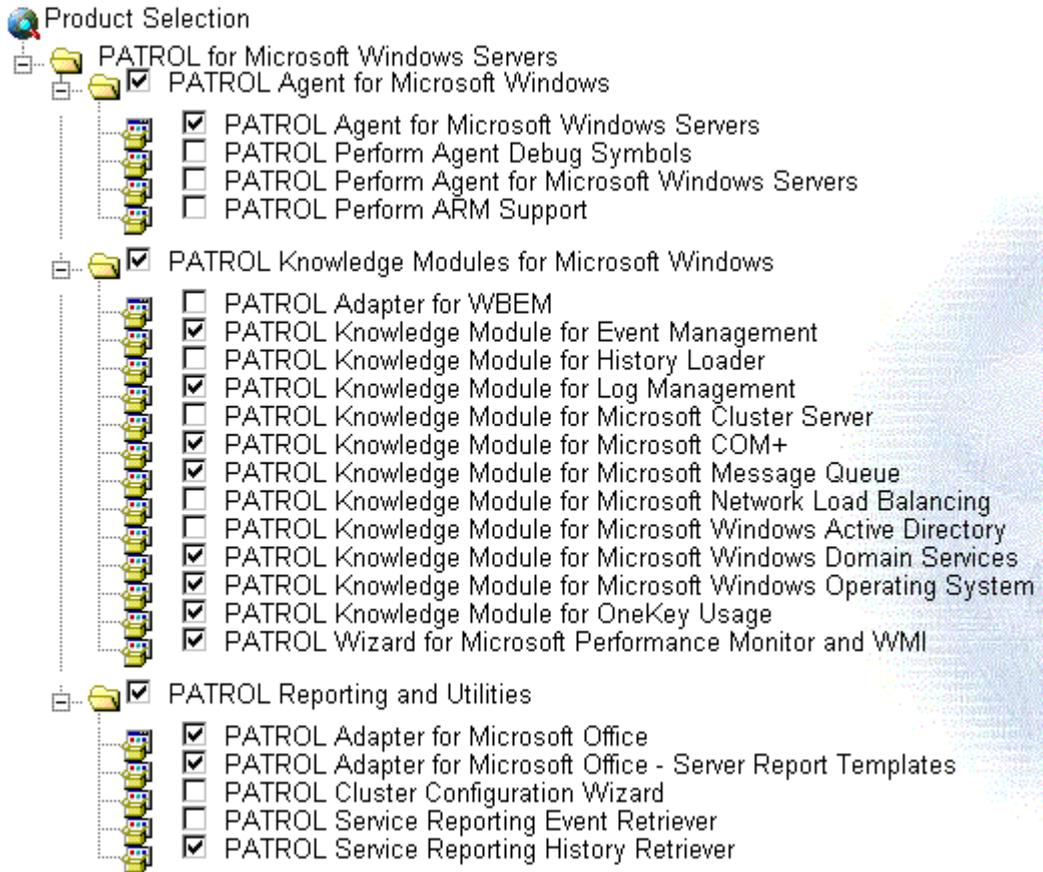
- Select **Console System** if you are installing to a computer that hosts or will host a PATROL Console.
- Select **Managed System** if you are installing to a computer that hosts or will host a PATROL Agent.
- Select **Common Services** if you are installing services that are shared among managed systems and console systems. This may include KM files. For more information, see “Determining Where to Install KMs Based on Architecture” on page 2-15 and “Target Computers and Their Roles” on page 2-14.

Note

For more information about the PATROL consoles, PATROL Console Server, or RT Server, see the *PATROL Central Operator – Web Edition Getting Started* and the *PATROL Console Server and RTserver Getting Started*.

Step 9 In the Select Products and Components to Install window, select the KMs that you want to install (see Figure 2-2) and click **Next**.

Figure 2-2 Select Products and Components to Install - Custom Install



Note

Depending on which components you select, a screen is displayed asking you if you want to install the Perform Agent. This product is optional. For more information, see the Perform documentation on the PATROL for Windows Servers documentation CD.

Step 10 In the Provide the PATROL 3.x Product Directory window, enter the directory where you want to install PATROL for Windows Servers as

appropriate for your installation scenario. Use the following table as a guide.

Install option	Directory	Example
PATROL for Windows Servers into an existing PATROL 3.4 environment	the PATROL product directory	To install PATROL into D:\Program Files\BMC Software\PATROL3-4 , enter PATROL3-4 in the PATROL 3.x Product Directory field.
PATROL for Windows Servers into an existing PATROL 3.5 environment	the PATROL product directory	To install PATROL into D:\Program Files\BMC Software\Patrol3 , enter Patrol3 in the PATROL 3.x Product Directory field.
PATROL for Windows Servers into an existing PATROL 3.4 environment where previously installed PATROL products are in a top-level directory such as C:\PATROL3-4	do not enter anything; delete any defaults in this field	To install into the previously installed directory C:\PATROL3-4 , do not enter anything in the PATROL 3.x Product Directory field.
PATROL for Windows Servers into an existing PATROL 3.5 environment where previously installed PATROL products are in a top-level directory such as C:\PATROL3-5	do not enter anything; delete any defaults in this field	To install into the previously installed directory C:\PATROL3-5 , do not enter anything in the PATROL 3.x Product Directory field.

This directory is appended to the base directory path that you entered in Step 7 on page 2-27.

Step 11 In the PATROL Default Account Properties window, enter the user name and password that you want to use for your PATROL default account and click **Next**. You should have created this account manually before you began to install PATROL. (For more information about the PATROL Account, see “Accounts” on page 2-7.)

Step 12 Complete the Confirm BMC Startup Information window:

12.A In the **Specify the Current Agent Port Number** field, enter the port number you want the PATROL Agent to use. The default is 3181.

Note

If your previous installation used a different port number, change the default to the current port number for the PATROL Agent.

12.B In the **Restart the PATROL agent automatically?** field, select **Yes** or **No**:

- If you want the installation utility to restart the PATROL Agent after the installation is complete, select **Yes**.
- If you want to restart the PATROL Agent after the installation is complete, select **No**.

Step 13 In the RTServers Variable Properties window, if you do not have any PATROL 7.x consoles or RTServers, accept the default options. When you upgrade to PATROL 7.x, you can change these values using the RTServers environment variable.

Step 14 Complete the remaining windows. The number and content of the windows depend on your KM selections and your inputs to the windows. Click Help as needed to complete the windows.

Step 15 In the Review Selections and Start Install or in the Review Selections and Create Installable Image window, review the selections carefully to make sure they are correct.

- If you want to change your selections, click **Back** and make those changes.
- If the selections are correct, select **Start Install** to start installing or **Create Image** to start exporting the image to the directory you entered in Step 4 on page 2-20.

A status window opens that contains current messages, current milestones and percent complete.

Note

If you selected to create an installable image to install on several computers or on the local computer at a later time, see “Creating and Installing Installable Images” on page 2-46.

- Step 16** When the status window reports that the installation is 100% complete, click **Next** to view the results window. (*Next* does not appear until the installation is 100% complete.)
- Step 17** In the results window, click **View Log** to review the details of the installation or click **Exit** to close the installation utility.

Upgrade and Preserve Customizations

Use the appropriate procedure in this section if you want to upgrade to the new version of PATROL for Windows Servers and you want to preserve any customizations you have made to the previous version of PATROL for Windows Servers.

After you have finished this procedure, see “Migrate Your Customizations” on page 2-41 for instructions about incorporating your customizations into the new version. You should complete this process on a limited number of machines in the test environment first, test the merged KMs thoroughly, and then deploy them to your production environment.

Note

To upgrade and preserve customizations, you must either migrate your customizations manually or use the PATROL Migration Tools version 3.5 (no KMDS required), or have the latest version of KMDS installed as well as any available patches.

Determine Whether You Can Migrate

Before migrating customizations, you must determine whether or not the customizations to the previous version of PATROL for Windows Servers that you have installed can be migrated to the new version of PATROL for Windows Servers. See Table 2-6 to determine whether migration is supported for your current version of each PATROL for Windows Servers component.

If migration is supported, choose one of the following installation procedures to migrate your customizations:

Migration Procedure	Page
"Migrating Customizations Using the PATROL Migration Tools Version 3.5"	2-34
"Migrating Customizations Using the KMDS"	2-34
"Migrating Customizations Manually"	2-36

Table 2-6 Versions That You Can Migrate

Component	Version
PATROL for Windows Servers	2.1.01 and up
PATROL KM for Windows Operating System	3.5.06, 3.6.00, 3.6.05, 3.7.00, 3.7.01
PATROL KM for Windows Domain Services	1.1.00, 1.1.03, 1.2.00, 1.2.01, 1.3.00, 1.4.00, 1.4.01
PATROL Knowledge Module for History Loader	1.4.00, 1.4.01, 1.4.02, 1.4.03, 1.4.05
PATROL KM for Microsoft Message Queue	1.1.00, 1.2.00, 1.3.00, 1.3.01
PATROL KM for Microsoft COM+	1.2.00, 1.2.02, 1.2.03
PATROL Wizard for Microsoft Performance Monitor and WMI	No migration is supported; however, if you created .km files and parameters using an older version of this component, they will continue to work, even after loading the new KM.

Migrating Customizations Using the PATROL Migration Tools Version 3.5

The process of migrating KM customizations from a PATROL 3.x environment to PATROL 3.5 no longer depends on the PATROL KMDS. Because the PATROL Migration Tools version 3.5 copy the new product files directly from the product CD rather than from KMDS, you do not have to install the new version of PATROL for Windows Servers. Just ensure that the product CD is accessible when you are running the migration tools.

For specific instructions and detailed information about using the PATROL Migration Tools version 3.5, see the *PATROL Migration Tools User Guide*.

Migrating Customizations Using the KMDS

Note

Ensure that you have installed the latest version of PATROL KMDS, including any available patches.

If you want to install PATROL for Windows Servers into the KMDS so that you can migrate the customizations that you have made to the currently installed version of PATROL for Windows Servers to the new version of PATROL for Windows Servers, you must follow these steps to run the installation utility in KMDS mode:

- Step 1** Open a command line prompt.
- Step 2** Change to the drive where the installation CD is located.
- Step 3** Enter the correct command for your operating system (Table 2-7 describes the command line options):
 - At the Windows command line prompt, enter **setup.exe -kmds [-kmdsportnum *portnum*]**

- At the Unix command line prompt, enter
`setup.sh -kmds [-kmdsportnum portnum] [-releaseversion v.r]`

Table 2-7 Command Line Options for Installing in a KMDS Environment

KMDS Installation Options	Description
<code>-kmdsportnum <i>portnum</i></code>	optional; use only if you are not using the default KMDS port number 3182
<code>-releaseversion <i>v.r</i></code>	optional; use only if you are installing to a <i>Unix</i> PATROL 3.3.x or PATROL 3.4.x environment. <i>v.r</i> designates the version number of the PATROL environment into which you are installing (for example, <code>-releaseversion 3.4</code>).

The installation utility opens in KMDS mode.

- Step 4** In the Welcome to the Installation Utility window, click **Next** to begin your installation.
- Step 5** In the Review License Agreement window, review the license agreement, select **Accept**, and click **Next** to continue.
- Step 6** In the Select Installation Option window, select one of the following options:
- If you want to install the products without creating an installable image, select **I want to install products on this computer now** and click **Next** to continue.

- If you want to create an installable image that you can use to install the products on this computer and other computers later, select **I want to create an installable image to be installed later**, enter the directory where you want to store the installable image, and click **Next** to continue.

Note

If you select to create an installable image, all of the computers where you plan to use the installable image must share the same **BMC Software** directory, PATROL default logon, PATROL Agent port number, platform, and security option. For more information, see “Creating and Installing Installable Images” on page 2-46.

- Step 7** In the Specify KMDS directory window, enter the full path to the directory in which the KMDS is installed and click **Next**.
- Step 8** From the Select Products and Components to Install window, select the KMs that you want to install and click **Next**.
- Step 9** In the Review Selections and Install window, review the selections carefully to make sure they are correct.
- To change your selections, click **Back** and make those changes.
 - If the selections are correct, click through the rest of the windows in the installation utility to install PATROL for Windows Servers into the KMDS.

Migrating Customizations Manually

After you have performed the procedures in “Prepare to Upgrade” on page 2-24 and reviewed the information in “Determine Whether You Can Migrate” on page 2-33, use this installation procedure *if you do not want to use the PATROL Migration Tools version 3.5 or the PATROL KMDS* to migrate the customizations that you have made to the currently installed version of PATROL for Windows Servers.

- Step 1** If you are installing into PATROL 3.3.x or 3.4.x in a *Unix* environment, follow these steps to start the installation utility. If you are installing into PATROL 3.3.x or 3.4.x in a Windows environment or into PATROL 3.5 in a Unix or Windows environment, skip to Step 2.
- 1.A** Open a command line prompt.
 - 1.B** Change to the drive where the installation CD is located.
 - 1.C** At the Unix command line prompt, enter **setup.sh -releaseversion v.r** where *v.r* is the version of the PATROL environment into which you are installing.
 - 1.D** Skip to Step 3.
- Step 2** If you have already installed PATROL 3.5 or PATROL 7.x, or you are installing to a Windows environment, start the installation utility by running **setup.exe** (Windows) or **setup.sh** (Unix) from the installation CD or from an electronically downloaded (EPD) installation image.
- Step 3** In the Welcome to the Installation Utility window, click **Next** to begin your installation.
- Step 4** In the Review License Agreement window, review the license agreement, select **Accept**, and click **Next** to continue.
- Step 5** In the Select Installation Option window, select one of the following options:
- If you want to install the products without creating an installable image, select **I want to install products on this computer now** and click **Next** to continue.

- If you want to create an installable image that you can use to install the products on this computer and other computers later, select **I want to create an installable image to be installed later**, enter the directory where you want to store the installable image, and click **Next** to continue.

Note

If you select to create an installable image, all of the computers where you plan to use the installable image must share the same **BMC Software** directory, PATROL default logon, PATROL Agent port number, platform, and security option. For more information, see “Creating and Installing Installable Images” on page 2-46.

Step 6 From the Select Type of Installation Window, select **Custom** and click **Next**.

Step 7 In the Specify Installation Directory window, enter the correct information based on your installation scenario and click **Next**. Use the information in the table below as a guide.

Installation Option	Directory	Example
PATROL for Windows Servers into an existing PATROL 3.4 environment	the directory path up to the PATROL product directory	To install PATROL into D:\Program Files\BMC Software\PATROL3-4 , enter D:\Program Files\BMC Software in the Specify Installation Directory window.
PATROL for Windows Servers into an existing PATROL 3.4 environment where previously installed PATROL products are in a top-level directory such as C:\PATROL3-4	the full directory path to your previously installed products	To install into the previously installed directory C:\PATROL3-4 , enter C:\PATROL3-4 in the Specify Installation Directory window.

Installation Option	Directory	Example
PATROL for Windows Servers into an existing PATROL 3.5 environment	the directory path up to the PATROL product directory	To install PATROL into D:\Program Files\BMC Software\Patrol3 , enter D:\Program Files\BMC Software in the Specify Installation Directory window.
PATROL for Windows Servers into an existing PATROL 3.5 environment where previously installed PATROL products are in a top-level directory such as C:\PATROL3-5	the full directory path to your previously installed products	To install into the previously installed directory C:\PATROL3-5 , enter C:\PATROL3-5 in the Specify Installation Directory window.

The PATROL product directory is appended to the path that you enter in this step. You will specify the PATROL installation directory in Step 10 on page 2-29.

Step 8 From the Select System Roles window, select **Managed System, Console System, Common Services**, or both, using the information provided in “Target Computers and Their Roles” on page 2-14, and click **Next**.

Note

For more information about the PATROL consoles, *PATROL Console for Unix User Guide*, *PATROL Console for Microsoft Windows User Guide*, *PATROL Console Server*, or *RTserver*, see *PATROL Central Operator – Web Edition Getting Started*, *PATROL Central Operator – Microsoft Windows Edition Getting Started*, and *PATROL Console Server and RTserver Getting Started*.

Step 9 From the Select Products and Components to Install window, select the KMs that you want to install and click **Next**.

Note

If your previous installation used a different port number, change the default to the current port number for the PATROL Agent.

Step 10 In the Provide the PATROL 3.x Product Directory window, enter the correct information based on your installation scenario and click **Next**. For more information, use the following table as a guide.

Install option	Directory	Example
PATROL for Windows Servers into an existing PATROL 3.4 environment	the PATROL product directory	To install PATROL into D:\Program Files\BMC Software\PATROL3-4 , enter PATROL3-4 in the PATROL 3.x Product Directory field.
PATROL for Windows Servers into an existing PATROL 3.5 environment	the PATROL product directory	To install PATROL into D:\Program Files\BMC Software\Patrol3 , enter Patrol3 in the PATROL 3.x Product Directory field.
PATROL for Windows Servers into an existing PATROL 3.4 environment where previously installed PATROL products are in a top-level directory such as C:\PATROL3-4	do not enter anything; delete any defaults in this field	To install into the previously installed directory C:\PATROL3-4 , do not enter anything in the PATROL 3.x Product Directory field.
PATROL for Windows Servers into an existing PATROL 3.5 environment where previously installed PATROL products are in a top-level directory such as C:\PATROL3-5	do not enter anything; delete any defaults in this field	To install into the previously installed directory C:\PATROL3-5 , do not enter anything in the PATROL 3.x Product Directory field.

Step 11 In the PATROL Default Account Properties window, enter the user name and password that you want to use for your PATROL default account and click **Next**. You should have created this account manually before you began to install PATROL. (For more information about the PATROL Account, see “Accounts” on page 2-7.)

Step 12 Complete the Confirm BMC Startup Information window:

12.A In the Specify the Current Agent Port Number field, enter the port number you want the PATROL Agent to use. The default is 3181.

Note

If your previous installation used a different port number, change the default to the current port number for the PATROL Agent.

12.B In the Restart the PATROL agent automatically? field, select Yes or No:

- If you want the installation utility to restart the PATROL Agent after the installation is complete, select **Yes**.
- If you want to restart the PATROL Agent after the installation is complete, select **No**.

Step 13 Complete the remaining windows. The number and content of the windows depend on your KM selections and your inputs to the windows.

Step 14 Proceed to “Migrate Your Customizations” on page 2-41.

Migrate Your Customizations

Customizations made to PATROL for Windows Servers may include changes to the parameter alarm ranges, recovery actions, states, or other parameter properties.

You can migrate customizations manually or through the KMDS. Migration of **.km** files through the KMDS is automated, with the following exceptions:

- modified PSL code, whether it is embedded in **.km** files or in **.psl** files
- parameter overrides done with a PATROL Operator Console (3.3.00 and later)

- new Knowledge Modules that you created

Note

Even if you are not using the PATROL KMDS, you can use the PATROL migration tools to help you migrate customizations. For more information about the PATROL migration tools, see the *PATROL Migration Tools User Guide*.

Preparing to Migrate

Before you migrate the customizations from the previously installed version of PATROL for Windows Servers to the newly installed version of PATROL for Windows Servers, you remove any obsolete KMs from the list of preloaded KMs on each PATROL Agent. See the *PATROL Agent Reference Manual* for instructions on removing KMs from the preload list.

To Migrate Using the PATROL Migration Tools Version 3.5

The following procedure is a general workflow for using the PATROL Migration Tools version 3.5 to migrate your customizations to the new version of PATROL for Windows Servers. For detailed explanation and instruction on using the migration tools, see the *PATROL Migration Tools User Guide*.

Follow this migration procedure only after you have met the following criteria:

- completed the procedures in “Prepare to Upgrade” on page 2-24.
- installed version 3.5 of the PATROL migration tools, including the KM archive

- Step 1** Run the migration probe to locate the base version of PATROL for Windows Servers from the KM archive and the new version of PATROL for Windows Servers from the product CD.
- Step 2** Run the merge tool to merge the base and customized versions of PATROL for Windows Servers with the new version of PATROL for Windows Servers.
- Step 3** Choose one of the following methods to transfer merged KMs to your test environment:
- Copy the contents of the results directory to the /lib directory where the new version of PATROL for Windows Servers is installed.
 - Copy the contents of the packaged results to a CD image and then use that CD to install.
 - Deploy the contents of the merged results directory using a third-party deployment system.
- Step 4** Perform any additional optional migration tasks as described in the PATROL Migration Tools User Guide.

To Migrate Using the PATROL Migration Tools Version 3.4.11 and the KMDS

Note

Before beginning this procedure, ensure that you use the PATROL KMDS version 3.4.11 and apply any available patches.

After you have checked your customizations to the previous version of PATROL for Windows Servers into the KMDS, use the following steps to migrate your customizations to the new version of PATROL for Windows Servers. For detailed instructions about migrating customizations using the KMDS, see the *PATROL Migration Tools User Guide*.

- Step 1** Use the Probe and Merge tools to identify, preserve, and merge customizations from the prior version of PATROL for Windows Servers into the newly installed version of PATROL for Windows Servers. See the *PATROL Migration Tools User Guide* to run the Probe and Merge tools.
- Step 2** When prompted during the merge phase of the migration, enter the appropriate map file name as shown in Table 2-8 on page 2-44.

Table 2-8 Map File Names

Required Component	Map File Name
PATROL KM for Windows Operating System	NT_3_8_00.map
PATROL KM for Windows Domain Services Component	domain_km_1_5_00.map
PATROL KM for History Loader	histakm_1_4_05.map
PATROL KM for Microsoft Message Queue	msmq_km_1_4_00.map
PATROL KM for Microsoft COM+	complus_km_1_3_0.map

Warning

Make sure that you use the merge map file that was shipped with the *new* version of PATROL for Windows Servers. The default location is ***PATROL_HOME*\lib\migration\new\lib\kmmergemap**.

- Step 3** Use KMDS to merge.
- Step 4** After you have completed the migration of your changes, load the new version and save the configuration.

To Migrate Customizations Manually

If you do not want to use the KMDS to migrate customizations, use the following steps to migrate your customizations manually:

- Step 1** Move the old PATROL for Windows Servers to a new directory that is different from **PATROL_HOME**.
- Step 2** Identify the customizations in PATROL for Windows Servers by comparing the content of the text file of the KM in the current PATROL for Windows Servers version with the content of the text file for the customized KM that is saved in the PATROL Console cache backup directory.
- Step 3** Incorporate your customizations to the new PATROL for Windows Servers by performing the following steps:
- 3.A** Restart the PATROL Console.
 - 3.B** Load the newly installed PATROL for Windows Servers.
 - 3.C** Using a PATROL Developer Console, enter the customizations that you identified in Step 2, one by one.

To Migrate Customized PATROL Script Language Code

Customizations made to PATROL Script Language (PSL) code are not automatically migrated. These customizations may be embedded in **.km** files or stored in separate **.psl** files. Migrate these customizations manually, using the following guidelines:

- If you modified **.psl** files that were shipped by BMC Software, you must manually re-edit the PSL code in the new KM by using a PATROL Developer Console to reapply your changes.
- If you modified PSL code embedded in a KM, that code will be overwritten when you install a new version of the product. You must manually edit the **.km** files by using a PATROL Developer Console to reapply your changes.

- If you created a new PSL file (not shipped by BMC Software) outside of a **.km** file, or if you created new PSL code (not shipped by BMC Software) and embedded it in a KM that was shipped by BMC Software, use the `pslsearch` utility to search your KM for terms that you may have used that have since been adopted by BMC Software as PSL keywords. Reapply your changes by using a PATROL Developer Console. For instructions about using the `pslsearch` utility, see the *PATROL Migration Tools User Guide*.

Note

If you have a customized a PSL library that was compiled with an earlier version of the PSL compiler than the version that was provided with PATROL 3.2.09, you must manually recompile the library by using the PATROL 3.4.11 compiler.

Creating and Installing Installable Images

The PATROL installation utility installs only to a local computer. The installation utility cannot perform remote installations. You must install a PATROL Agent and PATROL for Windows Servers locally on each computer that you want to monitor. You also must install a PATROL Console and PATROL for Windows Servers locally on each computer from which you want to view results.

The installation utility does provide you with the ability to create an installable image from the products that you select during a regular local installation. If you place the installable image in a shared directory, you can use that installable image to install the selected BMC Software products on all computers that perform the same roles and have these identical requirements:

- same shared **BMC Software** directory
- same PATROL default logon
- same PATROL Agent port number
- same platform
- same security option

You can also use a distribution server to distribute the installable images that you create.

Create an Installable Image

If you selected the **I want to create an installable image to be installed later.** option in the Select Installation Option window during the installation process, then you elected to create an installation image that you can execute later on the current computer or on several computers that share the same roles and installation selections.

Once you select **Create Image** in the Review Selections and Create Installable Image window, the installation utility finishes exporting the installation image.

The installation utility creates an **install.ctl** file in the specified directory that includes all the configuration information needed to install the products that you selected in the Product Selection window.

Before you run the installation image, you might want to change the properties for the image. Read the following instructions and decide whether changing the image is appropriate for your environment:

- If you want to run the installation package more than once from the same location, change the properties on the installation image file, **install.ctl**, to **Read-Only**.

Warning

The **install.ctl** file includes the encrypted password for the account that was used during the install process. If the **install.ctl** file is set to Read-Only, ensure that the **install.ctl** file is removed from all computers to which the installation image is copied.

- If you want to distribute the installation image from a central location to multiple machines, do *not* change the properties of the **install.ctf** file to **Read-Only**.

Warning

If you do not change the **install.ctf** file to Read-Only, it is deleted after the first time you execute the installation image, and you will not be able to use the exported installation image more than once.

Install the Created Installable Image

After you create the installable image, as described on page 2-47, you can then use it to install PATROL for Windows Servers on a local computer of the same platform that performs the same roles and has the same shared **BMC Software** directory, PATROL default logon, PATROL Agent port number, and security options as the options in the installable image. Use the following steps:

Step 1 Navigate to the directory where the installable image resides.

Step 2 Run the installation utility:

- On Windows, double-click the **install.exe** file or type **install.exe** at a command prompt.
- On Unix, type **./install.sh** at a command prompt.

The installation utility executes and then creates an installation log that lists the products installed, which you can view. The text at the end of the installation log indicates whether or not the installation was successful.

Installing the Unix Version of the Help Browser

The browser required for the Unix version of PATROL Help is Netscape Navigator version 3.01 through 4.78. However, if you are running a Red Hat Linux platform, you must run Netscape Navigator version 4.x to display the online Help. Currently, PATROL Help does not support Netscape Navigator 6.0.

You must install Netscape Navigator on the computer where the PATROL Console resides. You can install Netscape anywhere on your Unix computer as long as the binary is in the path.

Netscape Navigator is supplied by Netscape Communications Corp. You can locate the browser at <http://home.netscape.com/download>.

Additional Considerations for Using Online Help for Unix

When you select Help from the PATROL Console on a Unix system, it may take a few seconds for the Help browser to launch. Two windows will be displayed. First the Netscape Navigator window is displayed as an icon, and then a browser window that contains the Help is displayed.

In addition, you must be aware of the following restrictions:

- Netscape Navigator displays warning messages when it is invoked multiple times within the same user account because of its file-locking mechanism. It will, however, continue functioning.
- By default, when Netscape Navigator starts, it uses a private color map. As a result, you might experience color flashing on your workstation. If so, you can set the value of `PATROL_BROWSER` so that the `colormap` option is not specified. However, some subsequent color requests might fail and the online Help will be improperly displayed.
- The eXceed for Windows NT X Window Server product by Hummingbird Communication Ltd. may not always display the Help files properly.

Consult your Netscape Navigator documentation for specific platform requirements and restrictions.

Setting Environment Variables for the Browser

The LANG, PATH, and PATROL_BROWSER environment variables must be set for the Help browser to run properly. The following sections describe these variables.

LANG Variable

On some platforms, the Unix LANG environment variable must be set to C so that Netscape Navigator will work properly. Otherwise, you might experience product failures.

Set your user or system **.profile** for Bourne or Korn shells as follows:

```
LANG=C
export LANG
```

For C shell users, issue the following command:

```
setenv LANG C
```

PATH Variable

The PATROL user account PATH variable must contain the location of the directory containing the Netscape files. If the directory containing the Netscape files is not on the path, add the directory to the PATROL user account path.

This requirement applies only to the PATROL user account on the same computer as the PATROL Console.

PATROL_BROWSER Variable

When PATROL starts the Help browser, it uses the command in the PATROL_BROWSER environment variable. As a default, the PATROL_BROWSER environment variable contains the following command:

```
netscape -display $DISPLAY -install -iconic
```

To use different arguments, set the value of PATROL_BROWSER to the appropriate string. For example:

```
export PATROL_BROWSER=/usr/local/bin/netscape -raise
```

Uninstalling

For instructions about uninstalling PATROL products see the *PATROL Installation Guide*.

Where to Go from Here

The following table lists other topics and where you can find them:

Topic	Source of Information
overview of the PATROL for Windows Servers features	Chapter 1, "Product Components and Capabilities"
setting up and configuring PATROL for Windows Servers	Chapter 3, "Loading and Configuring PATROL for Windows Servers," and PATROL for Windows Servers component online Help
instructions about how to access the KM menu commands, InfoBoxes and online Help	Appendix A, "Accessing Menu Commands, InfoBoxes, and Online Help"
information about PATROL for Windows Servers configuration variables	Appendix B, "Agent Configuration Variables"
listing of the KM included with each PATROL for Windows Servers component	Appendix C, "PATROL for Windows .kml Files"
step-by-step procedures and detailed descriptions of the applications, menu commands, parameters, and InfoBoxes	PATROL for Windows Servers component online Help

Loading and Configuring PATROL for Windows Servers

This chapter provides information about how to begin using and configuring the PATROL for Windows Servers components. The following topics are discussed in this chapter:

Preparing to Use PATROL for Windows Servers	3-3
Loading KMs	3-4
Loading the PATROL for Windows Servers KMs	3-5
Unloading PATROL for Windows Servers KMs	3-9
Configuring the PATROL KM for Windows OS	3-12
Requirements for Configuring from the PATROL Console	3-12
Configuration Tasks	3-14
Configuring Windows Event Monitoring	3-15
Configuring Registry Key Monitoring	3-17
Configuring Service Monitoring	3-19
Configuring Process Monitoring	3-21
Configuring Recovery Actions	3-24
Creating Custom Parameters	3-26
Creating and Monitoring Windows 2000 Job Objects	3-27
Monitoring Logical or Physical Disk Drives	3-28
Configuring E-Mail Notification	3-29
Command-Line Based, E-Mail Client Required	3-29
Configuring PATROL to Send E-Mail Notifications	3-30
Creating New Parameters with the PATROL Wizard for Microsoft	
Performance Monitor and WMI	3-32
Loading the PATROL Wizard for Microsoft Performance Monitor	
and WMI	3-33

Creating Performance Monitor Parameters	3-34
Creating WMI Parameters	3-36
Configuring the PATROL KM for Log Management	3-37
Selecting Log Files for Monitoring	3-38
Defining Log File Searches	3-40
Using the PATROL Adapter for Microsoft Office to View Reports . .	3-43
Displaying PATROL Data by Using the PATROL Adapter for Microsoft Office	3-44
How to Use the PATROL Adapter for Microsoft Office	3-45
Built-In Report Templates	3-45

Preparing to Use PATROL for Windows Servers

If PATROL for Windows Servers has not been installed, see Chapter 2, “Installing and Migrating PATROL for Windows Servers.” After installing, return to this section for information on how to configure the components.

Before configuring the PATROL for Windows Servers components, you should verify that the following software requirements are met:

- The PATROL Console version 3.4.x or later and PATROL for Windows Servers must be installed on the computer you want to use for the PATROL Console.
- The PATROL Agent version 3.4.x or later and PATROL for Windows Servers must be installed on the computer you want to monitor and manage.
- The necessary product component files must be installed on the PATROL Console computers and the PATROL Agent computers.

You should also verify that you have access to all required information about the monitored domain controllers or Windows servers.

Example

If you want to monitor your operating system, ensure that you have the PATROL Console and the PATROL KM for Windows OS installed on the console machine and the PATROL Agent and the PATROL KM for Windows OS installed on the agent machine.

Loading KMs

Before you can begin configuring and using the PATROL for Windows Servers components, you need to load the KMs on the PATROL Console. For more information, see the following topics:

Task	Page
Loading the PATROL for Windows Servers KMs	3-5
Unloading PATROL for Windows Servers KMs	3-9

Loading the PATROL for Windows Servers KMs

Summary: This section provides instructions for loading the PATROL for Windows Servers KMs on each of the PATROL consoles.

Before You Begin

Make sure you have met the following requirements:

- the components that you want to load on the agent and console computers are installed
- the agents to which you want to load components are running
- the PATROL Console is running

To Load KMs on the PATROL Console for Windows Servers

Step 1 Choose **File => Load KM** from the PATROL Console menu bar.

Step 2 Select one or more of the **.kml** files in Table 3-1 that correspond to the components that you want to load. For detailed information on the application classes that are loaded with these **.kml** files, see “PATROL for Windows Servers .kml Files” on page C-2.

Table 3-1 PATROL for Windows Servers .kml Files (Part 1 of 2)

.kml file	Component	Description
COM.kml	PATROL KM for Microsoft COM+ (Windows 2000)	loads application classes to monitor COM+ packages
HISTORY.kml	PATROL KM for History Loader	loads application classes to monitor PATROL KM parameter history
MSMQ.kml	PATROL KM for Microsoft Message Queue	loads application classes to monitor Microsoft Message Queue (MSMQ)
NT_LOAD.kml	PATROL KM for Windows OS	loads application classes to monitor your operating system
NTD.kml	PATROL KM for Windows Domain Services	loads application classes to monitor your domain controller resources

Table 3-1 PATROL for Windows Servers .kml Files (Part 2 of 2)

.kml file	Component	Description
NT_PERFMON_WIZARD.kml	PATROL Wizard for Microsoft Performance Monitor and WMI	loads application classes that are required to use the PATROL PerfMon and WMI Wizard
WBEM.kml	PATROL Adapter for WBEM	loads application classes required to use the PATROL Adapter for WBEM
EVENT_MANAGEMENT.kml	PATROL KM for Event Management	loads application classes required to configure alerts, such as e-mail or paging notifications
LOG.kml	PATROL KM for Log Management	loads application classes required to configure text log monitoring

Step 3 Click **OK**.

Note

If the icons do not appear within 10 minutes of startup, open and read the information in the PATROL system output window.

Note

Unless you are an advanced PATROL user, use the **.kml** files to load product component files. Loading individual **.km** files can break the interdependencies between the **.km** files.

To Load the KM on a PATROL Console for Unix

Step 1 Choose **File => Load KM** from the PATROL Console menu bar.

Step 2 Select one or more of the **.kml** files in Table 3-1 that correspond to the components that you want to load. For detailed information on the application classes that are loaded with these **.kml** files, see “PATROL for Windows Servers .kml Files” on page C-2.

Step 3 Click Open.

Note

If the icons do not appear within 10 minutes of startup, open and read the information in the PATROL system output window.

Note

Unless you are an advanced PATROL user, use the **.kml** files to load product component files. Loading individual **.km** files can break the interdependencies between the **.km** files.

To Load the KM on PATROL Central Operator - Windows Edition

Step 1 In the **Common Tasks** tab of the Operator Console Module Taskpad, click the **Load Knowledge Module(s)** icon.

PATROL Displays the Load Knowledge Module(s) Wizard.

Step 2 To start the wizard, click **Next**.

Step 3 From the Managed System screen, select the managed system that you want to load KMs on.

Step 4 From the Knowledge Modules screen, select the KMs that you want to load. For detailed information on the application classes that are loaded with these **.kml** files, see “PATROL for Windows Servers .kml Files” on page C-2.

Step 5 Click **Finish**.

The KMs that you selected are loaded on the managed system, added to your management profile, and displayed in the PATROL Central Operator tab.

To Load the KM on PATROL Central - Web Edition

PATROL Central - Web Edition has a Loading KMs feature that enables you to control which KMs are loaded on which computers.

Step 1 From the Monitored Systems page, click the **Load/Unload KMs** button.

The Load KMs page opens, listing each computer on which a PATROL Agent has been installed.

Step 2 Select the computers on which you want to load KMs, and click **Next**.

The Load KMs page displays a list of available **.km** and **.kml** files.

If you selected more than one computer, the only **.km** and **.kml** files that are listed are the ones that have been installed on all of the selected computers. If a particular **.km** or **.kml** file was installed only on one computer, you must choose that computer by itself to load the file.

Step 3 Select the **.km** or **.kml** files that you want to load.

Step 4 Click **Finish**.

PATROL loads the selected KMs on the selected computers.

Note

If you want to load a **.km** or **.kml** file that was not listed in Step 2, ensure that the KM is installed on the appropriate computer and select only that computer in Step 2.

Unloading PATROL for Windows Servers KMs

Summary: If you no longer want to use an application class that you previously loaded, you can unload the **.km** file so that its application class will no longer appear in your console. This section provides instructions for unloading the PATROL for Windows Servers KMs on each of the PATROL consoles.

Before You Begin

In the PATROL Console for Microsoft Windows and the PATROL Console for Unix, unloading a KM is also referred to as *deleting* a KM. However, when you unload or delete a **.km** file using a console, the file is not deleted from the **patrol\knowledge** directories on the PATROL Console on the PATROL Agent computers.

To Unload KMs with the PATROL Console for Microsoft Windows Servers

- Step 1** From the **KM** tab of the tree view, right-click the application class name that you want to delete and choose **Delete** from the pop-up menu.
- Step 2** Click **Yes** to delete the application class.

The application class is removed from your cache directory and your console session file.
- Step 3** Repeat Step 1 and Step 2 until you have deleted all of the application classes associated with the KM that you want to delete.
- Step 4** From the console menu bar, choose **File => Save KM** to save your changes.

To Unload KMs with the PATROL Console for Unix

- Step 1** From the PATROL Main window, choose **Attributes => Application Classes**.
- Step 2** From the Lists of Application Classes window, click the name of the application class that you want to delete.
- Step 3** From the List of Application Classes menu bar, choose **Edit => Delete**.

The application class is removed from your cache directory and your console session file. The PATROL Console removes the application class name from the List of Application Classes.

- Step 4** Repeat Step 2 and Step 3 until you have deleted all of the application classes associated with the KM that you want to delete.
- Step 5** From the List of Application Classes menu bar, choose **File => Save KM** to save your changes.

To Unload KMs with PATROL Central Operator - Windows Edition

- Step 1** In the Common Tasks tab of the Operator Console Module Taskpad, click the **Unload Knowledge Module(s)** icon.

PATROL displays the Unload Knowledge Module(s) Wizard.
- Step 2** To start the wizard, click **Next**.
- Step 3** From the Managed System screen, select the managed system.
- Step 4** From the Knowledge Modules screen, select the KMs that you want to unload. For a description of the PATROL for Windows Servers KMs, see “PATROL for Windows Servers .kml Files” on page 3-5.
- Step 5** Click **Finish**.

To Unload KMs with PATROL Central - Web Edition

PATROL Central - Web Edition has a feature that enables you to unload specified **.km** files from specified computers.

Step 1 From the Managed Systems page, click the **Load/Unload KMs** button.

The Load KMs page opens, listing each computer on which a PATROL Agent has been installed.

Step 2 Select the computers from which you want to unload **.km** files, and click **Next**.

The Load KMs page displays a list of **.km** files. Currently loaded **.km** files are highlighted in the list.

Step 3 Cancel the selection of the **.km** files that you want to unload.

Step 4 Click **Finish**.

The console removes the **.km** files that you specified. These **.km** files will no longer be in the current management profile.

Configuring the PATROL KM for Windows OS

The following section describes how to begin configuring key features of the PATROL KM for Windows OS. For more detailed step-by-step instructions on configuring and using the PATROL KM for Windows OS, see the PATROL KM for Windows OS online Help.

Requirements for Configuring from the PATROL Console

When using the PATROL Console to configure or manage the PATROL KM for Windows OS, verify that the console connection account, the account that you use to connect to the agent, is a member of the local Administrators group on the agent computer. If the console connection account is not a member of the local Administrators group, the features described in Table 3-2 are not available.

Table 3-2 PATROL KM for Windows OS Features that Require Local Administrator Privileges (Part 1 of 2)

Functionality	Application Class	Menu Command	Behavior
configuring Windows operating system quotas	NT_LOGICAL_DISK	Configure Operating System Quotas	The KM displays a message stating that local administrator privileges are required.
managing Windows services, such as starting and stopping services or changing service startup properties	NT_SERVICES	Manage Windows Operating System Services	The KM displays a list of services but does not allow you to change the service properties.
viewing the Windows security event log	NT_EVENTLOG	Windows Event Viewer	The KM does not display the security event log but does display other event logs.

Table 3-2 PATROL KM for Windows OS Features that Require Local Administrator Privileges (Part 2 of 2)

Functionality	Application Class	Menu Command	Behavior
managing Windows event logs or logging events	NT_EVENTLOG	Windows Event Viewer	You can view event logs, other than the security event log, but you cannot change properties or log events.
monitoring mount points and configuring quotas on an NTFS system	<ul style="list-style-type: none"> • NT_NTFS_MOUNT • NT_NTFS_QUOTA 	All	The KM does not discover or display these NTFS application classes and writes a message to the console system output window.

In addition, the console connection account must have P (PEM enabled) mode access specified in the agent configuration variable `/AgentSetup/accessControlList`. This mode is set by default. If it is removed, the following functionality is not available:

- configuring Windows event monitoring
- viewing Windows events
- configuring service monitoring
- configuring process monitoring
- configuring registry monitoring
- managing services
- configuring quotas
- enabling/disabling pagefile monitoring
- enabling/disabling logical disk monitoring
- enabling/disabling CPU monitoring

Configuration Tasks

For information about PATROL KM for Windows OS configuration tasks, see the referenced sections in Table 3-3. For more information about accessing KM menu commands, see “Accessing KM Commands and InfoBoxes” on page A-2.

Table 3-3 PATROL KM for Windows OS Configuration Tasks

Tasks	Menu Command	Page
configure Windows event monitoring	From the PATROL Console, access the NT_EVENTLOG application and choose the KM menu command Configure Windows Event Monitoring .	3-15
configure registry key monitoring	From the PATROL Console, access the NT_REGISTRY application and choose the KM menu command Configure Registry Key Monitoring .	3-17
configure service monitoring	From the PATROL Console, access the NT_SERVICES application and choose the KM menu command Configure Service Monitoring .	3-19
configure process monitoring	From the PATROL Console, access the NT_PROCESS application and choose the KM menu command Configure Process Monitoring .	3-21
configure built-in recovery actions	From the PATROL Console, access the host application and choose the KM menu command Configure Recovery Actions .	3-24
create custom parameters	From the PATROL Console, access the NT_CompositesColl application and choose the KM menu command Create Expressions .	3-26
configure Windows 2000 job objects	From the PATROL Console, access the NT_JOBS application and choose the KM menu command Job Objects Management => Process Group Execution Rules .	3-27

Configuring Windows Event Monitoring

Summary: This task describes how to configure the PATROL KM for Windows OS to monitor for specific Windows events.

Before You Begin

To monitor for specific Windows events, you must create event filters. Event filters specify the type of events to monitor and how to monitor them. You can create event filters by

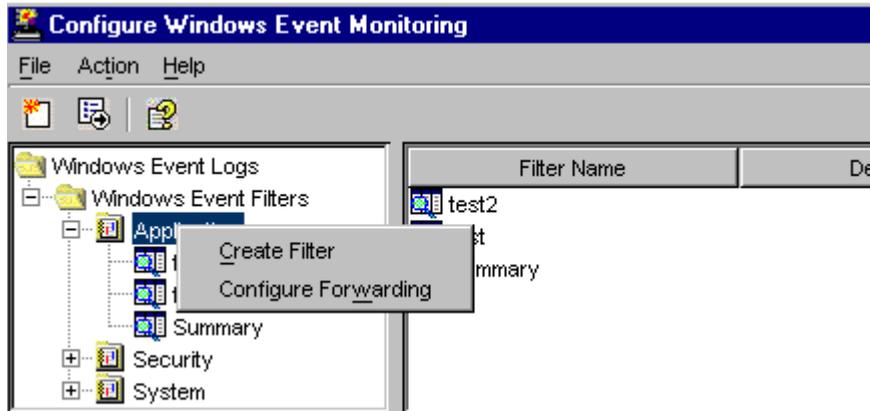
- specifying the types of events that you want to monitor based on the event's source, ID, type, and content
- selecting events to monitor directly from the Windows event viewer

The Windows event log must be monitored by PATROL before you can create an event filter. By default, all Windows event logs are monitored. To enable or disable Windows event log monitoring, access the NT_EVENTLOG application and choose the KM menu command **Enable\Disable Windows Event Log Monitoring**.

To Specify Events to Monitor

- Step 1** Access the NT_EVENTLOG application menu as described in “Accessing KM Commands and InfoBoxes” on page A-2 and choose the KM menu command **Configure Windows Event Monitoring**.
- Step 2** From the Configure Windows Event Monitoring window, right-click the event log (Application, Security, or System) in the left pane and choose the menu command **Create Filter** (See Figure 3-1 on page 3-16).

Figure 3-1 Configure Windows Event Monitoring Window



Step 3 In the **General** tab **Name** field, enter a name for the event filter.

Step 4 Select monitoring options for the filter. For more information about the monitoring options, click the **Help** button.

Step 5 When you finish selecting the monitoring options, click **Apply**.

PATROL creates an application instance for the filter beneath the NT_EVENTLOG application on the PATROL Console.

To Select Events to Monitor from the Windows Event Viewer

Step 1 Access the NT_EVENTLOG application menu as described in “Accessing KM Commands and InfoBoxes” on page A-2 and choose the KM menu command **Windows Event Viewer**.

Step 2 From the Windows Event Viewer window, select (highlight) the event(s) that you want to monitor and then click the right mouse button and choose the menu command **Create Filter with Event Viewer**.

PATROL creates an event filter based on the properties of the events that you selected.

Step 3 Verify that the filter properties are appropriate and then click **Apply**. For more information about the filter options, click the **Help** button.

Configuring Registry Key Monitoring

Summary: This task describes how to configure the PATROL KM for Windows OS to monitor registry key activity.

Before You Begin

With the PATROL KM for Windows OS, you can monitor the Windows registry keys to determine when the following key activities occur:

- key is changed
- key is created
- key is removed
- key value is changed

For each configuration, you must specify the following information:

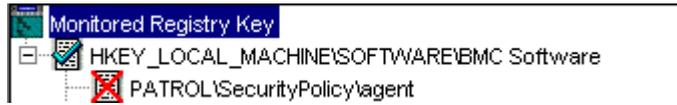
- registry key that you want to monitor (required)
- subkeys that you want to exclude from monitoring (optional)

To Configure Registry Key Monitoring

- Step 1** Access the NT_REGISTRY application menu as described in “Accessing KM Commands and InfoBoxes” on page A-2, and choose the KM menu command **Configure Registry Key Monitoring**.
- Step 2** From the Configure Registry Key Monitoring window, right-click the Monitored Registry Keys folder and select **Create Registry Filter**.
- Step 3** To select the registry key that you want to monitor, click **Add Key**.
- Step 4** From the Add Key dialog box, select the registry key and click **OK**.
- Step 5** To exclude from monitoring any subkeys of the selected key, click **Exclude Subkeys**.
- Step 6** From the Exclude Subkeys dialog, select the keys that you want to exclude and click **OK**.

The keys that you chose to exclude are shown beneath the monitored registry key, as shown in Figure 3-2:

Figure 3-2 Example of Monitored Registry Key and Excluded Subkey



Step 7 From the **Monitoring Options** tab select the following options:

- registry activity that you want to monitor
- how PATROL responds to the registry activity

For more information about specifying the PATROL response to registry activity, see Table 3-4.

Table 3-4 PATROL Response to Registry Activity

Option	When to Use	Default (Yes/No)
Display warnings and alarms until they are acknowledged	You want to be notified and manually acknowledge the alarm, if the registry key activity occurs. If you select this option, PATROL generates an alarm when the registry activity occurs and stays in alarm even if the registry activity does not occur during the next collection period.	No
Don't display warnings or alarms, but continue to log registry activity in agent history	You want to keep a record of registry activity but you don't want PATROL to generate alarms.	No

Step 8 To apply your changes to the PATROL Agent, click **Apply**.

PATROL applies your changes to the PATROL Agent and creates an application instance for the configuration beneath the NT_REGISTRY application on the PATROL Console.

Configuring Service Monitoring

Summary: This task describes how to configure PATROL to monitor Windows services.

Before You Begin

To monitor a service, you select it from a list of services running on the machine. You can monitor a service using the default settings or you can change the settings if you want to specify how the service is monitored.

Note

To configure service monitoring, the console account that you use to connect to the PATROL Agent on the monitored system must have local administrator rights on the monitored system.

To Select a Service to Monitor

Step 1 Access the NT_SERVICES application menu as described in “Accessing KM Commands and InfoBoxes” on page A-2 and choose the KM menu command **Configure Service Monitoring**.

PATROL displays the Configure Service Monitoring window that allows you to select the services that you want to monitor and configure how the service is monitored.

Services that are currently monitored are displayed in the left tab, beneath the Monitored Services folder.

Step 2 To monitor a new service, choose the menu command **Action => Add New Service to be Monitored**.

Step 3 Select the service that you want to monitor and click **OK**.

The service is added to the list of monitored services.

To Configure Service Monitoring

Step 1 From the left tab of the Configure Service Monitoring window, select the service that you want to configure.

Step 2 From the Service Monitoring Configuration dialog, select the appropriate monitoring options, described in Table 3-5.

Table 3-5 Service Monitoring Options

Option	Description	Default?
Restart service when stopped	If you select this option, PATROL automatically attempts to restart the service when it is stopped.	Yes
Generate a PATROL Alarm/Warn when the service is stopped	<p>By default, when a service is stopped, PATROL generates an Alarm. However, for a particular service, you can specify a Warning instead.</p> <p>If you choose Warning instead of Alarm, PATROL will not restart the service when it is stopped even if you select the option Restart service when stopped. In addition, the service's ServiceStatus alarm ranges and status levels are changed. For more information, see the PATROL KM for Windows OS online Help.</p>	Yes (Alarm)
Enable process monitoring for this service	When monitoring services, PATROL monitors only whether the service is available. To monitor how much memory and CPU a service executable consumes, enable process monitoring for the service. When you enable process monitoring, PATROL monitors the service executable process and displays the monitored process beneath the NT_PROCESS application.	No
Use specified command to check status of non responsive service	<p>If you select this option, you must supply an executable that checks that status of the service and returns the following result:</p> <ul style="list-style-type: none">• 0 = the service is OK• 1 = the service is not responding <p>This feature is for advanced users who have developed custom executables that determine the status of a service. If the custom executable determines that the service is not responding, the following parameters enter an alarm state:</p> <ul style="list-style-type: none">• SvcNotResponding• SvcStatus	No

Step 3 To apply your changes to the PATROL Agent, click **Apply**.

Configuring Process Monitoring

Summary: This task describes how to configure PATROL to monitor processes.

Before You Begin

With PATROL for Windows Servers you can configure process monitoring using the methods shown in Table 3-6.

Table 3-6 Process Monitoring Options

Method	When to Use
Manual process monitoring	You want to select or specify the processes to monitor and you want to customize how PATROL monitors them.
Automatic process monitoring	You want to monitor a process only if it exceeds a specified CPU utilization percentage.

To Configure Manual Process Monitoring

- Step 1** Access the NT_PROCESS application menu as described in “Accessing KM Commands and InfoBoxes” on page A-2, and choose the KM menu command **Configure Process Monitoring**.
- Step 2** From the Configure Process Monitoring window, right click the Processes folder and choose the menu command **Configure Manual Process Monitoring**.
- Step 3** Select (highlight) the process that you want to monitor or, if the process is not currently running, enter the process name and any appropriate command-line arguments.
- Step 4** Select one of the following options:
- monitor the process(es) only when it is running with the command line arguments shown
 - monitor any occurrence of the selected process(es), regardless of the command-line arguments

Step 5 Click **Apply**.

PATROL performs the following actions:

- The processes you selected are removed from the list of running processes and are added to the list of monitored processes that are shown on the left pane of the Configure Process Monitoring window.
- The processes you selected are added to the PATROL console, beneath the NT_PROCESS application.
- The PATROL Agent begins monitoring the process.

To configure how the process is monitored and managed, see “To Configure Process Control” on page 3-23.

To Configure Automatic Process Monitoring

Step 1 Access the NT_PROCESS application menu as described in “Accessing KM Commands and InfoBoxes” on page A-2, and choose the KM menu command **Configure Process Monitoring**.

Step 2 From the Configure Process Monitoring window, right-click the Processes folder and choose **Configure Automatic Process Monitoring**.

Step 3 Change the length of time specified for high CPU.

PATROL defines high CPU as a value higher than the alarm threshold specified by the NT_PROCESS\PROCProcessorTimePercent parameter. To change this threshold, access the PROCProcessorTimePercent parameter and change the default alarm ranges. For more information about changing parameter default values, see the documentation for your console.

Step 4 Click **Apply**.

When any process consumes high CPU for a period longer than what you specified, PATROL begins monitoring the process and adds the process to the PATROL console, beneath the NT_PROCESS application.

To Configure Process Control

- Step 1** Access the NT_PROCESS application menu as described in “Accessing KM Commands and InfoBoxes” on page A-2 and choose the KM menu command **Configure Process Monitoring**.
- Step 2** From the Configure Process Monitoring window, select the monitored process that you want to configure.
- Step 3** Select the appropriate options, described in Table 3-7, and then click **Apply**.

Table 3-7 Process Control Options

Option	Description	Default (Yes/No)
Restart the process using the specified command when the process is stopped	If you check this option, you must supply the path to an executable that restarts the process and you must include any appropriate command-line arguments.	No
Terminate the process when the process CPU% utilization exceeds the defined PATROL threshold	<p>If you check this option, PATROL terminates the process when it appears to be in a “run away” state. This state is defined by the following criteria:</p> <ul style="list-style-type: none"> • the CPU% utilization exceeds the threshold specified by the NT_CPU PROCProcessorTimePercent parameter • the process exceeds this threshold for the specified length of time <p>To change the CPU utilization threshold, access the PROCProcessorTimePercent parameter and change the default alarm ranges.</p> <p>When the process exceeds the threshold for the specified length of time, the process is terminated during the next collection cycle, whose scheduling is determined by the parameter PROCProcessColl. By default, PROCProcessColl collects data every 5 minutes.</p>	No
Generate a PATROL Alarm when the process is terminated	If you select this option, the PATROL NT_PROCESS parameters PROCStatus and PROCDown will be in alarm when the process is terminated.	Yes
Generate a PATROL Alarm when the process is started	If you select this option, the PATROL NT_PROCESS parameter PROCStatus will be in an alarm state when the process is started.	No

Configuring Recovery Actions

Summary: This task describes how to configure the PATROL for Windows Servers built-in recovery actions, which are corrective actions taken by PATROL when a parameter reaches a set value or is in a warning or alarm state.

Before You Begin

The recovery actions that are available depend on the KMs that you have loaded on the host.

To Configure Recovery Actions

- Step 1** Access the host application menu as described in “Accessing KM Commands and InfoBoxes” on page A-2 and choose the KM menu command **Configure Recovery Actions**.
- Step 2** From the list of recovery actions, highlight the desired recovery action and click **Accept**.
- Step 3** From the list of recovery action instances, highlight the instance and click **Edit**. For information about which instance to select, see Table 3-8.

Table 3-8 Selecting a Recovery Action Instance

Purpose	Recovery Action to Select
configure the recovery action for a specific instance (for example, a monitored process)	the recovery action instance that displays the name of the application instance in the INSTANCE column
configure the recovery action for all instances (for example, all monitored processes)	the recovery action that displays an asterisk (*) in the INSTANCE column

Step 4 From the Edit Recovery Action dialog box, choose from the settings described in Table 3-9.

Table 3-9 Recovery Action Configuration Options

Setting	Description
Run automatically	If you select this mode, PATROL runs the recovery action automatically, without prompting you.
Run only with operator confirmation	If you select this mode, PATROL prompts you before running the recovery action. Note: If you select this option, be sure to keep a console connected to the PATROL Agent on the managed machine. If you have no console connection, PATROL is unable to prompt you.
Do Not Execute	If you select this mode, PATROL does not perform the recovery action.
Suspend Recovery Action	If you select this option, PATROL temporarily pauses the recovery action. When you resume the recovery action (by deselecting this check box), the previous recovery action settings take effect.
Attended Mode Dialog Timeout	If the recovery action is configured in Run Attended mode, this setting specifies the amount of time PATROL waits for confirmation to run the recovery action. If you do not provide confirmation within the allotted time, PATROL does not run the recovery action.

Note

For more information on the recovery action and its configuration options, click the **Help** button.

Step 5 To save your changes, click **Accept**.

Creating Custom Parameters

Summary: This topic describes how to create composite parameters, which are parameters whose values are dependent on one or more existing PATROL parameters.

Before You Begin

Composite parameters give you the capability to create parameters whose values are dependent on one or more existing PATROL parameters. You can then use PATROL alarm settings and recovery actions on the newly created parameters in the same way that you use alarm settings and recovery actions on other parameters.

You can enter and edit composite parameter expressions manually or by using the expression entry wizard.

To Create Custom Parameters using the Expression Entry Wizard

- Step 1** Access the NT_CompositesColl application menu as described in “Accessing KM Commands and InfoBoxes” on page A-2, and choose the KM menu command **Create Expressions**.
- Step 2** From the Create Expressions dialog box, enter a name for the expression (parameter).
- Step 3** Follow the instructions provided in the wizard. For more information, click the **Help** button.

After you complete the wizard, the new composite parameter is displayed on the console beneath the NT_Composites application.

Creating and Monitoring Windows 2000 Job Objects

Summary: This section describes how to create and monitor Windows 2000 job objects. Job objects are a feature provided with Windows 2000 that allow you to group related processes for monitoring and management.

With Windows 2000 job objects, you can apply the following resource constraints to a group of processes:

- process and total CPU usage
- process and total memory usage
- maximum number of processes
- which CPUs in a multiprocessor system can run the processes
- process priority and scheduling class

Using the PATROL KM for Windows OS, you first create the job object (also referred to as a process group) and then you specify the processes included in the group.

To Create a Process Group

- Step 1** Access the NT_JOBS application menu as described in “Accessing KM Commands and InfoBoxes” on page A-2 and choose the KM menu command **Job Objects Management => Process Group Execution Rules**.
- Step 2** In the Process Group Name field, enter a name for the process group.
- Step 3** Select the **Create** radio button and then click **Apply**.
- Step 4** From the Define Process Group Execution Rules dialog box, select the process group configuration options and then click **Apply**. For more information, click the **Help** button.

The process group is created and automatically monitored by PATROL as an instance beneath the NT_JOBS application.

To Specify Processes for the Process Group

- Step 1** Access the NT_JOBS application menu as described in “Accessing KM Commands and InfoBoxes” on page A-2 and choose the KM menu command **Job Objects Management => Process Execution Rules**.
- Step 2** In the Select a Process Group field, click the job object.
- Step 3** Select the **Define Process Execution Rules** radio button and then click **Apply**.
- Step 4** Specify processes using one of these methods:
- Highlight the process name and argument in the **Unselected Processes** list.
 - Enter data in the **Specify Process Name** and **Arguments** fields.
- Step 5** Select the **Add** radio button and then click **Apply**.

The processes are added to the process group and the process group execution rules are applied.

Monitoring Logical or Physical Disk Drives

If no data appears for the NT_LOGICAL_DISK application class, run one of the following diskperf commands from a command-line window to ensure that the Microsoft diskperf counters are enabled:

- **diskperf -ye** for Windows NT
- **diskperf -yv** for Windows 2000

Microsoft requires you to restart your system before the **diskperf** command takes effect. This behavior is documented in Microsoft's Knowledge Base article, “How to Monitor Disk Performance with Performance Monitor.”

Configuring E-Mail Notification

With the PATROL KM for Event Management, you can configure PATROL to send e-mail or paging notifications when a PATROL parameter enters an alarm state. This section describes how to configure the PATROL KM for Event Management to send an e-mail notification.

Command-Line Based, E-Mail Client Required

Before configuring e-mail notification, verify that your system has a command-line based e-mail client, such as Blat, which is a public domain utility that sends the contents of a file in an e-mail message by using the SMTP protocol. The instructions that follow assume that you are using Blat. If you are using a different command-line based, e-mail client, additional steps are required. For more information, see the *PATROL KM for Event Management User Guide*.

Downloading and Installing Blat

If you choose to use Blat as your command-line e-mail client, you can download it at <http://www.interlog.com/~tcharron/blat.html>.

Install Blat in the **C:\Blat** directory. If Blat is not installed in the **C:\Blat** directory, you must edit the file **AS_EVSLocalAlertNotify.bat**, located in **%PATROL_HOME%\lib\psl** directory, and replace **C:\Blat** with the actual installation path.

To configure Blat to send e-mail from the command line, follow the instructions provided with the Blat documentation.

Testing Blat

Before configuring PATROL e-mail notification, verify that you can use Blat to send a test message from the command line.

Configuring PATROL to Send E-Mail Notifications

Summary: This task describes how to configure PATROL to send e-mail notifications when parameters enter an alarm state.

Before You Begin

This procedure assumes that you are using Blat as your command-line e-mail client. Before proceeding, verify the following information:

- Blat is located in the C:\Blat directory. If Blat is not located in the C:\Blat directory, see “Downloading and Installing Blat” on page 3-29.
- Blat is functioning properly. To test Blat, send a test message from the command line.

Note

A command-line e-mail client is not required on each agent machine. With the PATROL KM for Event Management, you can configure a notification server that routes e-mail notifications and other alerts from remote agents. For more information, see the *PATROL KM for Event Management User Guide*.

To Configure PATROL to Send E-Mail Notifications

Step 1 From the PATROL Console, access the host menu commands as described in “Accessing KM Commands and InfoBoxes” on page A-2 and choose the KM menu command **Event Management => Quick Config => Notification Server**.

Note

If this menu command is not available, load the **EVENT_MANAGEMENT.kml** file in the PATROL Console.

Step 2 From the QUICK CONFIG - NOTIFICATION SERVER dialog, specify the default e-mail account that will receive the e-mail notifications.

Step 3 Accept the default notification command.

Note

By default, PATROL uses the batch file `AS_EVSLocalAlertNotify.bat` as the notification command. If you are using a command-line e-mail notification program other than Blat, you must edit this batch file. For more information, see the *PATROL KM for Event Management User Guide*.

Step 4 In the **Perform Alert Test** field, select **Yes**.

Step 5 Click **Accept**.

PATROL displays a message in the system output window indicating if the e-mail notification is configured successfully.

When *any* PATROL parameter enters an alarm state, PATROL sends an e-mail notification to the default e-mail account that you specified. However, you can customize your e-mail notification by specifying which parameters generate notifications. You can also use multiple e-mail accounts and specify that certain accounts receive only certain types of notifications. For more information, see the *PATROL KM for Event Management User Guide*.

Creating New Parameters with the PATROL Wizard for Microsoft Performance Monitor and WMI

The PATROL Wizard for Microsoft Performance Monitor and WMI allows you to quickly create your own parameters based on Microsoft's Performance Monitor (PerfMon) counters or Windows Management Instrumentation (WMI) data. You may want to create a new parameter if you are interested in monitoring something for which no PATROL parameter currently exists.

The tasks associated with the PATROL Wizard for Microsoft Performance Monitor and WMI are listed in Table 3-10.

Table 3-10 PATROL Wizard for Microsoft Performance Monitor and WMI Tasks

Task	Page
Loading the PATROL Wizard for Microsoft Performance Monitor and WMI	3-33
Creating Performance Monitor Parameters	3-34
Creating WMI Parameters	3-36

Loading the PATROL Wizard for Microsoft Performance Monitor and WMI

Summary: Before you can create new parameters by using the PATROL Wizard for Microsoft Performance Monitor and WMI, you must load the KM files on your PATROL console.

- » Load the **NT_PERFMON_WIZARD.kml** file as described in the “Loading KMs” on page 3-4.

The Performance Monitor Wizard and WMI Wizard application icons appear in the console.

Note

After you have created new parameters on a particular PATROL Agent, other PATROL console users will not be able to see the new parameters that you created until they load the **NT_PERFMON_WIZARD.kml** file.

Creating Performance Monitor Parameters

Summary: With the Performance Monitor Wizard, you can create new, user-defined parameters based on Microsoft Performance Monitor counters.

Step 1 Access the Performance Monitor Wizard application menu as described in “Accessing KM Commands and InfoBoxes” on page A-2.

Step 2 Choose the **Create New Parameters** menu command to display the Create Performance Monitor parameter dialog box.

Step 3 From the Create Performance Monitor Parameter dialog box, choose a **Performance Object** from the drop-down list box.

Counters and instances for the selected performance object display in the **Available Counters** and **Available Instances** tables.

Step 4 Select the counters you want to monitor from the **Available Counters** table by clicking the counter names.

Selected counters appear highlighted.

Step 5 Select the instances you want to monitor from the **Available Instances** table by clicking the instance names.

Selected instances appear highlighted.

Step 6 Click one of the following:

- Click **Next >** to set alarm thresholds for the parameters you are creating.

The Set Alarm Thresholds dialog box displays. Continue with Step 7.

- Click **Finish** to create the parameters without setting Alarm Thresholds.

The dialog box closes and PATROL creates your new parameters. You can set alarm thresholds later.

Step 7 Check the Set Alarm Thresholds dialog box and decide which parameters need warning and alarm thresholds. For the parameters that need thresholds:

- Type the lower-bound warning value in the **Warning Min** field.
- Type the upper-bound warning value in the **Warning Max** field.
- Type the lower-bound alarm value in the **Alarm Min** field.
- Type the upper-bound alarm value in the **Alarm Max** field.

Step 8 Click one of the following:

- **< Back** returns you to the previous dialog box (Creating Performance Monitor parameters).
- **Finish** creates the parameters according to your selections and closes the dialog box.
- **Cancel** closes the dialog box without applying your changes.

Creating WMI Parameters

Summary: With the WMI Wizard, you can create new, user-defined parameters based on WMI data.

- Step 1** Access the WMI Wizard application menu as described in “Accessing KM Commands and InfoBoxes” on page A-2.
- Step 2** Choose the **Create New Parameters** menu command to display the Create WMI Parameter dialog box.
- Step 3** Type a name for the WMI-based parameter you want to create in the **Parameter Name** field.
- Step 4** Type a valid select statement in the **Please enter WMI Query in WQL Syntax** field.

The query must return a numerical value.

Example

```
select NumberOfProcesses from Win32_OperatingSystem
or
select CurrentSize from Win32_Registry
```

- Step 5** Click **Test Query** to make sure that your WQL query returns valid data.
- Step 6** Click one of the following:
- **Next >** sets alarm thresholds for the parameter you are creating.
- The Set Alarm Thresholds dialog box displays. Continue with Step 7.
- **Finish** creates the parameter according to the SQL Query you entered and closes the dialog box.
 - **Cancel** closes the dialog box without applying your changes.

Step 7 Check the Set Alarm Thresholds dialog box and decide if your parameter needs warning and alarm thresholds. If it does:

- Type the lower-bound warning value in the **Warning Min** field.
- Type the upper-bound warning value in the **Warning Max** field.
- Type the lower-bound alarm value in the **Alarm Min** field.
- Type the upper-bound alarm value in the **Alarm Max** field.

Step 8 Click one of the following:

- **<Back** returns you to the previous dialog box (Create WMI Parameter dialog box).
- **Finish** creates the parameter according to the SQL Query you entered and closes the dialog box.
- **Cancel** closes the dialog box without applying your changes.

Configuring the PATROL KM for Log Management

This section describes how to configure the PATROL KM for Log Management so you can begin monitoring log files in your environment. The following table lists the topics covered in this section.

Task	Page
Selecting Log Files for Monitoring	3-38
Defining Log File Searches	3-40

Selecting Log Files for Monitoring

Summary: This section describes how to set up log files for monitoring.

Before You Begin

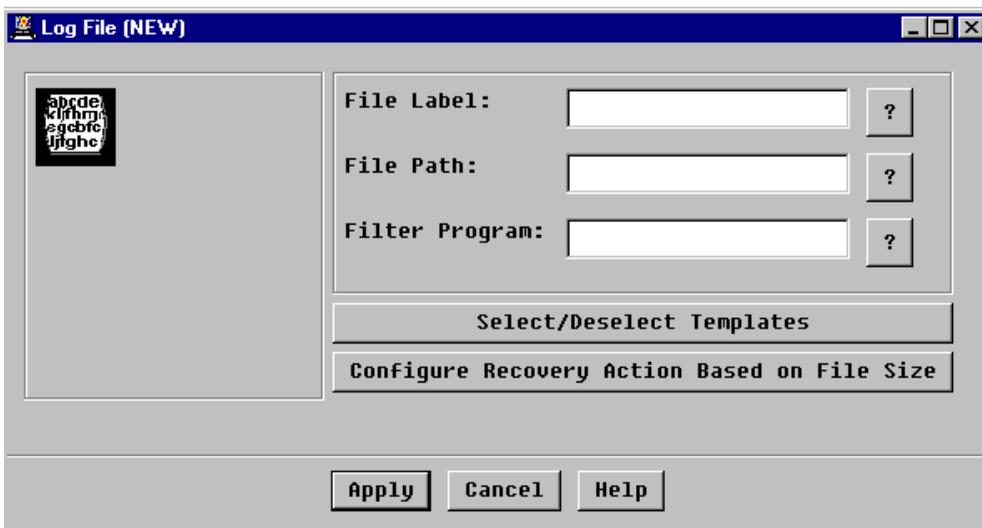
This task provides basic information about setting up a log file for monitoring. To set up log files with automatic recovery actions, see the PATROL KM for Log Management online Help.

To Monitor a Log File

- Step 1** Access the LOG application menu as described in “Accessing KM Commands and InfoBoxes” on page A-2.
- Step 2** Choose **Manage List of Monitored Files**.
- Step 3** From the Log Files dialog box, select the **ADD** radio button and then click **Apply**.

PATROL displays the Log File (New) dialog box (Figure 3-3).

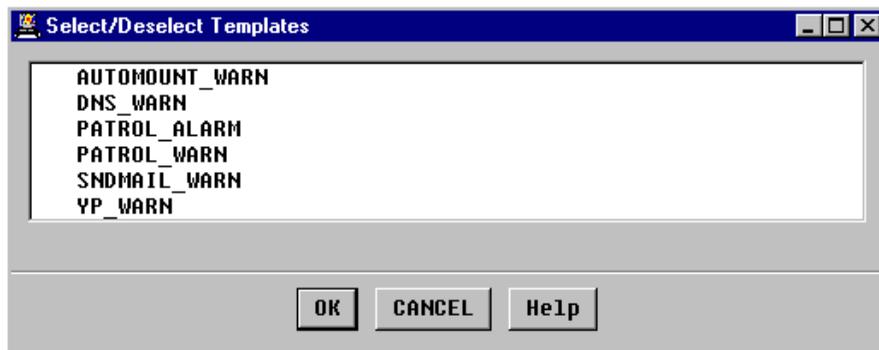
Figure 3-3 Log File (New) Dialog Box



The screenshot shows a dialog box titled "Log File (NEW)". On the left side, there is a small graphic containing a grid of letters: 'abcde', 'klfhj', 'sghbf', 'ijghe'. On the right side, there are three input fields with labels: "File Label:", "File Path:", and "Filter Program:". Each input field has a question mark button to its right. Below these input fields are two buttons: "Select/Deselect Templates" and "Configure Recovery Action Based on File Size". At the bottom of the dialog are three buttons: "Apply", "Cancel", and "Help".

- Step 4** Enter the file name and full path of the log file that you want to monitor in the **File Label** and **File Path** field.
- Step 5** To monitor a binary log file, enter the name of the program that translates the file to ASCII in the **Filter Program** field.
- Step 6** Associate a log file search template with the log file (Figure 3-4).
- If you have previously created a template to use on this log file, from the **Select/Deselect Templates** list, select a log file search template.
 - If you have not created a log file search template that applies to this log file, finish the steps in this task, and then create a template. To create a template, see “Defining Log File Searches” on page 40.

Figure 3-4 Select/Deselect Dialog Box



Step 7 For information about using an automated recovery action that reduces the log file size when it exceeds a specified limit, click the **Help** button.

Step 8 Click **Apply**.

Step 9 From the confirmation dialog, click **ACCEPT** to monitor the listed file.

PATROL displays the Log Files dialog box with the new log file name in the **List of Monitored Files** and adds a LOGMON instance icon for this log file in the LOGS container.

Step 10 Click **Close** to close the Log Files dialog box.

Defining Log File Searches

Summary: This task describes how to create search templates that can be associated to monitored log files. With search templates, you can define what type of messages PATROL should search for and how PATROL should respond when it locates a specified message.

The templates can be set up to search for text strings and regular expressions within monitored log files.

Before You Begin

- When you run a search on a log file, PATROL places a LOGTEMP instance icon in the container window of each log instance to which the template is applied. If PATROL finds a match, PATROL sets the icon for the log instance to the Alert Severity that you specified in the template. It also sets the values of the LOGSearchString parameter, which displays the number of matches found during the last search, and the LOGMatchString parameter, which displays the strings that contained matches.
- Once you define a template and associate it with a log file, the KM monitors the log for the
 - text string or pattern specified in the template
 - number of string matches per scan of the log file
 - corresponding alert severity (OK, WARN, or ALARM) when the specified string or pattern is found

To Define a Log File Search

Step 1 Access the LOGMON application menu as described in “Accessing KM Commands and InfoBoxes” on page A-2.

Step 2 Select **Manage List of Templates**.

PATROL displays the Log Search Templates dialog box.

Step 3 Select the **Add** check box and click **Apply**.

PATROL displays the Log Template: (NEW) dialog box (Figure 3-5).

Figure 3-5 Log Template: (NEW) Dialog Box

The dialog box is titled "Log Template: (NEW)". It features a preview area on the left with a small icon. The main area contains the following fields and controls:

- Template Name:** A text input field.
- Search String:** A section containing three rows, each with a NOT, a text input field, and an AND button with a question mark.
- Alert Severity:** A dropdown menu currently showing "OK".
- Buttons:** "Apply this Template to Logfile(s)", "Configure Event Behavior", "Apply", "Cancel", and "Help".

Step 4 Define the search by typing a name for the template in the **Template Name** field.

Template names are limited to 20 alphanumeric characters, hyphens (-), and underscores (_). The first character must be alphabetic or an underscore.

Step 5 Type a search string or regular expression in the **Search String** field.

You can search for a literal word or phrase or you can search for a type of message that has an identifiable format or pattern. For more information about searching based on patterns, see the PATROL KM for Log Management online Help.

Step 6 Choose how you want the LOGMON instance icons to react when the PATROL finds the search string or matches the regular expression. Click the **Alert Severity** drop-down list.

1 OK—do not change

2 WARN—place the icon into the warning state (yellow icon base)

3 ALARM—place the icon into the alarm state (red, flashing base)

Step 7 To select the log files that you want to search using this template, click the **Apply this Template to Log File(s)**.

Log files with an asterisk (*) are currently being monitored with this template.

Note

If you select (highlight) a log file with an asterisk (showing that it was previously selected) and click **Apply**, PATROL will no longer monitor that log file.

Step 8 To define the behavior when PATROL finds a match, click the **Configure Event Behavior** button.

Step 9 From the Configure Event Behavior dialog box, select the appropriate options and then click the **OK** button. For more information, see Table 3-11.

Table 3-11 Configure Event Behavior Dialog Options (Part 1 of 2)

Action	Purpose
Return to OK if Search String is Not Found in Next Scan	Select this option button to indicate that PATROL should return the log file instance to an OK state if the template does not find a match.
Do Not Generate Additional Alerts For Poll Cycles	Select this option and type a value in the provided field to indicate that PATROL should not re-send an alert for an event that has already been generated. PATROL will not send an alert for the event until the designated number of polling cycles has passed.

Table 3-11 Configure Event Behavior Dialog Options (Part 2 of 2)

Action	Purpose
Unless Search String Match Count Exceeds	Type a value in this field to indicate how many times the template must return a match before the timeout set in the prior field is ignored. For example, you can specify that if the template returns a text string match more than five times before the timeout period has expired, PATROL should send another alert to the console.
Custom Event Message	Type a customized message in this field. The customized message displays when PATROL generates an event for the template.

Step 10 From the Log Template dialog box, click **Apply** to apply your changes.

PATROL adds the template to the list of templates in the Log Search Templates dialog box and begins monitoring the log file for the search string or regular expression that you specified in the template.

Using the PATROL Adapter for Microsoft Office to View Reports

If you install the PATROL Adapter for Microsoft Office, you can display PATROL data in Microsoft Excel through the PATROL Adapter for Microsoft Office wizard. For more information, see the following topics:

Task	Page
Displaying PATROL Data by Using the PATROL Adapter for Microsoft Office	3-44
How to Use the PATROL Adapter for Microsoft Office	3-45
Built-In Report Templates	3-45

Displaying PATROL Data by Using the PATROL Adapter for Microsoft Office

Summary: This task describes how to start the PATROL Adapter for Microsoft Excel so that you can view server-based PATROL reports.

Before You Begin

To use PATROL Adapter for Microsoft Office, you must have one of the following versions of Microsoft Excel loaded on the console machine:

- Microsoft Excel 97 (SR1 or SR2)
- Microsoft Excel 200 (SR1)
- Microsoft Excel Office XP

To Start the PATROL Adapter for Microsoft Office from Microsoft Excel

- Step 1** Start Microsoft Excel.
- Step 2** Choose **File => New**.
- Step 3** Choose the **Spreadsheet Solutions** tab.
- Step 4** Choose the **Patrol Report.xlt** template.
- Step 5** Click **OK**.

The **New** dialog box is dismissed and the Microsoft Excel macros message appears.

- Step 6** Click **Enable Macros**.

To run the wizard, the Microsoft Excel security level must be either Low or Medium. If the security level is High, the wizard does not run and displays no error messages. To change the Microsoft Excel security level, start Excel and choose **Tools => Macro => Security**.

- Step 7** See the *PATROL Adapter for Microsoft Office User Guide* for instructions on generating a report.

How to Use the PATROL Adapter for Microsoft Office

For more information on how to use the PATROL Adapter for Microsoft Office, see the *PATROL Adapter for Microsoft Office User Guide*.

Note

History reports are not available for PATROL Agents that are version 3.2.09. Please see the *PATROL Adapter for Microsoft Office User Guide* for more information regarding requirements and limitations of PATROL Adapter for Microsoft Office.

Built-In Report Templates

Several products have predefined reports that you can use immediately. For a list of these predefined reports, see the following sections.

PATROL KM for Microsoft Windows Operating System

If you are using the PATROL KM for Windows OS, the predefined report templates in Table 3-13 are available when you use the PATROL Adapter for Microsoft Office.

Table 3-12 Reports for PATROL KM for Microsoft Windows Operating System

Report Name	Description
CPU Util - Weekly History CPU Util - Daily History	percentage of time that a processor is busy executing the threads of a process (the value reported by the parameter CPUprcrProcessorTimePercent)
Logical Disk - Weekly History Logical Disk - Daily History	percentage of free space available on the selected logical disk drive (the value reported by the parameter LDldFreeSpacePercent)
Memory - Weekly History Memory - Daily History	number of megabytes of physical memory currently available to processes (the value reported by the parameter MEMmemAvailableBytes)

PATROL KM for Microsoft Windows Domain Services

If you are using the PATROL KM for Microsoft Windows Domain Services, the predefined report templates in Table 3-13 are available when you use the PATROL Adapter for Microsoft Office.

Table 3-13 Reports for PATROL KM for Microsoft Windows Domain Services (Part 1 of 2)

Report name	Description
<ul style="list-style-type: none">• DHCP Lease Availability Daily History Report• DHCP Lease Availability Monthly History Report• DHCP Lease Availability Weekly History Report	NT_DHCP reports regarding the percent of DHCP leases available each day, week, or month
<ul style="list-style-type: none">• DHCP Server Utilization Daily History Report• DHCP Server Utilization Monthly History Report• DHCP Server Utilization Weekly History Report	NT_DHCP reports regarding the daily, weekly, or monthly server utilization of the DHCP service
<ul style="list-style-type: none">• DNS Server Response Time Daily History Report• DNS Server Response Time Monthly History Report• DNS Server Response Time Weekly History Report	NT_DNS reports regarding daily, weekly, or monthly server response times for the Domain Name Service (DNS)
<ul style="list-style-type: none">• DNS Server Utilization Daily History Report• DNS Server Utilization Monthly History Report• DNS Server Utilization Weekly History Report	NT_DNS reports regarding daily, weekly, or monthly server utilization of the DNS service
<ul style="list-style-type: none">• Remote Servers Connect Response Time Daily History Report• Remote Servers Connect Response Time Monthly History Report• Remote Servers Connect Response Time Weekly History Report	NT_REMOTE_SERVERS reports regarding daily, weekly, or monthly connection response times of remote domain servers
<ul style="list-style-type: none">• Remote Servers Connection Status Daily Outage Report• Remote Servers Connection Status Monthly Outage Report• Remote Servers Connection Status Weekly Outage Report	NT_REMOTE_SERVERS reports regarding daily, weekly, or monthly connection outages of remote domain servers
<ul style="list-style-type: none">• Shares Disk Usage Daily History Report• Shares Disk Usage Monthly History Report• Shares Disk Usage Weekly History Report	NT_SHARES reports regarding daily, weekly, or monthly usage of network shares on the managed server

Table 3-13 Reports for PATROL KM for Microsoft Windows Domain Services (Part 2 of 2)

Report name	Description
<ul style="list-style-type: none"> Trust Domain Connectivity Daily Outage Report Trust Domain Connectivity Monthly Outage Report Trust Domain Connectivity Weekly Outage Report 	NT_TRUST reports regarding daily, weekly, and monthly connection outages between trusted and trusting domains
<ul style="list-style-type: none"> WINS Server Utilization Daily History Report WINS Server Utilization Monthly History Report WINS Server Utilization Weekly History Report 	NT_WINS reports regarding daily, weekly, and monthly utilization of the Windows Internet Naming Service (WINS) on Windows NT servers

PATROL KM for Microsoft Message Queue

If you are using the PATROL KM for Microsoft Message Queue, the predefined report templates in Table 3-14 are available when you use the PATROL Adapter for Microsoft Office.

Table 3-14 Reports for PATROL KM for Microsoft Message Queue

Report name	Description
MSMQ Message Rate - Daily History Report	current rate that messages are received during a 24-hour period
MSMQ Service Availability - Weekly History Report	current rate that messages are received during a 7-day period
MSMQ Sessions - Daily History Report	number of MSMQ sessions that occur during a 24-hour period
MSMQ Sessions - Weekly History Report	number of MSMQ sessions that occur during a 7-day period
MSMQ Total Msgs. Waiting - Weekly History Report	total number of messages that waited for processing during a 7-day period

PATROL KM for Microsoft COM+

If you are using the PATROL KM for Microsoft COM+, the predefined report templates in Table 3-15 are available when you use the PATROL Adapter for Microsoft Office.

Table 3-15 Reports for PATROL for Microsoft COM+.

Report name	Description
Process Count Daily Summary	total number of processes run during a 24-hour period
Package Status Daily Summary	line graph of the current status of a package (active or in-active) during a 24-hour period
Package Status 30-Day Summary	line graph of the current status of a package (active or inactive) during a 30-day period
Active Packages Daily Summary	total number of packages active during a 24-hour period
Aborted Transaction Daily Summary	total number of transactions aborted during a 24-hour period
Aborted Transaction 30-Day Summary	total number of transactions aborted during a 30-day period

Accessing Menu Commands, InfoBoxes, and Online Help

BMC Software offers several PATROL consoles from which you can view a PATROL Knowledge Module (KM). Because of the different environments in which these consoles run, each one uses a different method to display and access information in the KM. This appendix provides instructions for accessing the KM menu commands, InfoBoxes, and online Help on each of the PATROL consoles. See the PATROL for Windows Servers online Help for more detailed information about navigation in the PATROL Consoles.

Accessing KM Commands and InfoBoxes.	A-2
Accessing Online Help.	A-3

Accessing KM Commands and InfoBoxes

Table A-1 provides information about how to access KM commands and InfoBoxes from the various PATROL consoles.

Table A-1 Accessing KM Commands and InfoBoxes

Console	To access menu commands	To access InfoBoxes
PATROL Console for Microsoft Windows Servers	In either the Desktop tree tab or work area, right-click a computer or application icon and choose KM Commands from the pop-up menu.	In either the Desktop tree tab or the work area, right-click an application class or parameter icon and choose InfoBox from the pop-up menu.
PATROL Console for Unix	In the work area, right-click a computer or application icon to display a pop-up menu that contains KM-specific commands.	With the middle mouse button, click an application class or parameter icon.
PATROL Central Operator - Windows Edition	In the navigation pane, right-click a managed system or application icon and choose Knowledge Module Commands from the pop-up menu.	In the navigation pane, right-click a PATROL object and choose InfoBox from the pop-up menu.
PATROL Central Operator - Web Edition	In the tree view area, right-click an application icon and choose Knowledge Module Commands from the pop-up menu.	In the tree view area, right-click a PATROL object and choose Infobox from the pop-up menu.

Accessing Online Help

Table A-2 provides information about how to access Help from each console.

Note

If you are trying to access Help from a Unix console, see the *PATROL Installation Reference Manual* for specific instructions about installing and setting up a browser in the Unix environment.

Table A-2 Accessing Online Help (Part 1 of 2)

Console	To access product help	To access application class help	To access parameter help
PATROL Console for Microsoft Windows Servers	From the console menu bar, choose Help => Help Topics => PATROL Knowledge Modules .	Double-click an application class in the KM tab of the console. From the Application Properties dialog box, click the Help tab. Then click Show Help .	<ul style="list-style-type: none"> • Right-click a parameter icon and choose Help On from the pop-up menu. • Double-click a parameter icon; click the ? icon or Help button in the parameter display window. • Double-click a parameter in the KM tab of the console; from the properties dialog box, click the Help tab; then click Show Help.
PATROL Console for Unix	From the console menu bar, choose Help On => Knowledge Modules .	Choose Attributes => Application Classes and double-click the application name. Click Show Help in the Application Definition dialog box.	Right-click a parameter icon and click Help On .

Table A-2 Accessing Online Help (Part 2 of 2)

Console	To access product help	To access application class help	To access parameter help
PATROL Central Operator - Windows Edition	From the console menu bar, choose Help => Help Topics . In the Contents tab, click the name of your product.	In the Operator tab of the navigation pane, select an application icon and press F1 .	In the Operator tab of the navigation pane, select a parameter icon and press F1 .
PATROL Central Operator - Web Edition	In the upper right corner of PATROL Central, click Help and choose PATROL KM Help .	In the tree view, right-click an application class and choose Help .	In the tree view, right-click a parameter and choose Help .

Agent Configuration Variables

The variables described in this section are PATROL for Windows Servers agent configuration variables that are set in the PATROL Agent. To view these variables, use the wpconfig utility or the PATROL Configuration Manager.

Warning

Changing any of these variables can prevent some functions from working properly and can affect your entire installation. Before you change a variable, make a record of the original setting.

Managing Configuration Variables	B-2
PATROL for Windows Servers Configuration Variables	B-2
PATROL KM for Microsoft Windows OS	B-3
PATROL KM for Microsoft Windows Domain Services	B-10
PATROL KM for Microsoft Windows Message Queue	B-13
PATROL KM for Microsoft COM+	B-14
PATROL Wizard for Microsoft Performance Monitor and WMI	B-14

Managing Configuration Variables

BMC Software recommends that you set agent configuration variables by using a console to configure PATROL for Windows Servers KMs. Use the PATROL Configuration Manager or the wpcnfig utility only to view variable settings or deploy them to others machines.

Warning

Do not use the wpcnfig utility or PATROL Configuration Manager to remove variables or add new variables. Doing so may prevent some functions from working properly and can affect your entire installation.

PATROL for Windows Servers Configuration Variables

The following sections lists the agent configuration variables associated with each PATROL for Windows Servers component.

Note

For information about the PATROL KM for Event Management agent configuration variables, see the *PATROL KM for Event Management User Guide*.

PATROL KM for Microsoft Windows OS

Table B-1 lists the PATROL KM for Microsoft Windows OS component variable settings.

Table B-1 Configuration Variables for PATROL KM for Microsoft Windows OS (Part 1 of 8)

Variable	Description	Location	Type
ForceMigration	forces KMs to migrate the configuration from registry to agent configuration file This value is used internally.	all sub keys of /NTOSKM	Boolean
ForceRefresh	forces KMs to reread the agent configuration file This value is used internally.	all sub keys of /NTOSKM	Boolean
RefreshInterVal	number of discovery cycles to reread the agent configuration file This value is used internally.	all sub keys of NTOSKM	integer
AutoMigration	allows KMs to automatically migrate configuration data from registry to agent configuration file This value is used internally.	NTOSKM	Boolean
Page File Variables			
page_bad_config_switch	determines whether to enable the PAGEBadConfiguration parameter	NTOSKM/PageFile	string
Event Log Management Variables			
AutoDisableELMEvFileFreeSpacePercent	allows NT_EVENTLOG KM to disable the parameter ELMEvFileFreeSpacePercent	NTOSKM/PWKNTEventLog	Boolean
UseCheckPoint	specifies that if the agent is restarted, the NT_EVENTLOG KM will process the events from checkpoint. Otherwise, it processes only newly logged events. Events logged while agent is down are ignored.	NTOSKM/PWKNTEventLog	Boolean

Table B-1 Configuration Variables for PATROL KM for Microsoft Windows OS (Part 2 of 8)

Variable	Description	Location	Type
CollectorType	weather to use WMI or win32api to collect data The default behavior is as follows: <ul style="list-style-type: none"> on W2K system and English system: WMIBoolean other systems: Win32Api 	NTOSKM/PWKNTE ventLog	string
Monitor All Eventlogs	whether to monitor all Windows event logs	NTOSKM/PWKNTE ventLog	string
Recovery Action All Eventlogs	whether to enable, for all event logs, the recovery action that backs up and purges an event log	NTOSKM/PWKNTE ventLog	string
Event Filter Monitoring Variables			
AcknowledgeBy	indicates how event filter alarms are acknowledged	NTOSKM/PWKNTE ventLog/event_log/E ventFilters/filter_name	string
Annotation	whether to annotate the PATROL parameter graphs associated with the event filter with information about the event	NTOSKM/PWKNTE ventLog/event_log/E ventFilters/filter_name	Boolean
ConsolidateEventTypes	whether to use one parameter to represent all of the event types that are monitored by the event filter	NTOSKM/PWKNTE ventLog/event_log/E ventFilters/filter_name	Boolean
ConsolidateNumber	the number of events that PATROL reports as a single event when the events occur within the length of time specified by the ConsolidateTime variable	NTOSKM/PWKNTE ventLog/event_log/E ventFilters/filter_name	integer
ConsolidateTime	the length of time within which the multiple events specified by the ConsolidateNumber variable are reported as a single event	NTOSKM/PWKNTE ventLog/event_log/E ventFilters/filter_name	integer
EventReport	whether to writes details about the events that occur during each collection cycle to a parameter	NTOSKM/PWKNTE ventLog/event_log/E ventFilters/filter_name	Boolean

Table B-1 Configuration Variables for PATROL KM for Microsoft Windows OS (Part 3 of 8)

Variable	Description	Location	Type
EventType	event types monitored by the event filter	NTOSKM/PWKNTEventLog/event_log/EventFilters/filter_name	integer
FilterDescription	a description of the event filter supplied by the user	NTOSKM/PWKNTEventLog/event_log/EventFilters/filter_name	string
IncludeAllCategories	whether to include all event categories in the event filter	NTOSKM/PWKNTEventLog/event_log/EventFilters/filter_name	Boolean
IncludeAllEventIDs	whether to include all event IDs in the event filter	NTOSKM/PWKNTEventLog/event_log/EventFilters/filter_name	Boolean
IncludeAllSources	whether to include all application sources in the event filter	NTOSKM/PWKNTEventLog/event_log/EventFilters/filter_name	Boolean
IncludeAllStrings	whether to include all event text strings in the event filter	NTOSKM/PWKNTEventLog/event_log/EventFilters/filter_name	Boolean
IncludeAllUsers	whether to include all users in the event filter	NTOSKM/PWKNTEventLog/event_log/EventFilters/filter_name	Boolean
RetainEventDescriptions	information about event filter events that you can use in recovery actions This information is available only if you select the option Use event details for a recovery action when configuring the event filter.	NTOSKM/PWKNTEventLog/event_log/EventFilters/filter_name	Boolean
StatusSortKey	when displaying process status, how to sort the display	NTOSKM/PWKNTProcess	string

Table B-1 Configuration Variables for PATROL KM for Microsoft Windows OS (Part 4 of 8)

Variable	Description	Location	Type
EnableAlarmIfProcessDown	whether to generate an alarm when the process goes down	NTOSKM/PWKNTProcess/ProcessConfigurationList/object	string
EnableAlarmIfProcessStarts	whether to generate an alarm when the process starts	NTOSKM/PWKNTProcess/ProcessConfigurationList/object	string
ProcessName	the name of the monitored process	NTOSKM/PWKNTProcess/ProcessConfigurationList/object	string
StartupCommand	path to an executable command, including any appropriate command-line arguments, used to start the process when the process goes down	NTOSKM/PWKNTProcess/ProcessConfigurationList/object	string
TimeLimitForKillRunAwayProcess	length of time that the process appears to be in a "run-away" state, before PATROL terminates the process A run away state is defined by the following criteria: <ul style="list-style-type: none"> the CPU% utilization exceeds the threshold specified by the NT_CPU\PROCProcessorTimePercent parameter the process exceeds this PROCProcessorTimePercent alarm threshold for the specified length of time 	NTOSKM/PWKNTProcess/ProcessConfigurationList/object	integer
UserDefinedProcess	whether the process is selected from the list of running processes or manually entered	NTOSKM/PWKNTProcess/ProcessConfigurationList/object	string
Service Monitoring Variables			
AutoRestartAutomaticStartupServices	indicates whether PATROL automatically restarts a service is stopped for services that are configured to start automatically at system startup	NTOSKM/PWKNTService	string
AutoRestartManualStartupServices	whether PATROL automatically restarts a service when it is stopped for services that are configured for manual startup	NTOSKM/PWKNTService	string

Table B-1 Configuration Variables for PATROL KM for Microsoft Windows OS (Part 5 of 8)

Variable	Description	Location	Type
EnableAlarmForAutomaticStartupServices	whether PATROL generates an alarm when a service that is configured to start automatically at system startup is stopped	NTOSKM/PWKNTS ervice	string
EnableAlarmforManualStartupServices	whether PATROL generates an alarm when a service that is configured for manual startup is stopped	NTOSKM/PWKNTS ervice	string
Monitor All Automatic Startup Services	whether PATROL automatically monitors all services that are configured to start automatically at system startup	NTOSKM/PWKNTS ervice	string
Monitor All Disabled Services	whether PATROL automatically monitors disabled services	NTOSKM/PWKNTS ervice	string
Monitor All Manual Startup Services	whether PATROL automatically monitors all services that are configured for manual startup	NTOSKM/PWKNTS ervice	string
Blue Screen Monitoring Variables (NT_BSK)			
BskCabFile	whether to compress the crash dump file and generated reports into a self-extracting executable file	BlueScreenKM	Boolean
BskDiagReport	whether to save a diagnostic report for the monitored computer after a Stop error has occurred	BlueScreenKM	Boolean
BskCompName	name of the computer or FTP server (IP address are not allowed) that you want to use to save the generated reports and crash dump files	BlueScreenKM	string
BskDirName	name of an existing Windows NT or Windows 2000 network share or the name of a directory on the FTP server By default, PATROL stores the generated reports and crash dump files in the directory designated by the local %PATROL_TEMP% environment variable. If the %PATROL_TEMP% environment variable does not exist or the location it specifies does not exist, the generated report and crash dump files are saved to the system temporary directory.	BlueScreenKM	string

Table B-1 Configuration Variables for PATROL KM for Microsoft Windows OS (Part 6 of 8)

Variable	Description	Location	Type
BskMoveFtp	where to save generated reports and crash dump files	BlueScreenKM	integer
BskRegReport	whether to save the registry contents of the monitored computer after a Stop error occurs	BlueScreenKM	Boolean
BskFound6008Time	used internally to monitor when an a Stop error alarm is acknowledged Do not modify this variable.	BlueScreenKM	string
Registry Monitoring Variables			
ChangeStateToOK	when displaying a warning or alarm when the configuration criteria is met, whether to stay in warning or alarm until manually acknowledged	PWKNTRegistry/Instances/object	integer
CreateKeyInstances	this variable is obsolete as of version 3.8.00 of the PATROL KM for Windows OS	PWKNTRegistry/Instances/object	integer
InstanceName	name of the registry monitoring configuration	PWKNTRegistry/Instances/object	string
Label	label used to identify the registry monitoring configuration	PWKNTRegistry/Instances/object	string
RequestType	types of registry key activity monitored by the registry-monitoring configuration Possible registry activity include: <ul style="list-style-type: none"> • keys are created • keys are deleted • values are set or modified • values are deleted 	PWKNTRegistry/Instances/object	integer
RootKeyIndex	root registry key where the monitored key is located	PWKNTRegistry/Instances/object	Boolean
ToggleAlarm	whether the registry-monitoring warnings or alarms are acknowledged	PWKNTRegistry/Instances/object	Boolean
List (Exclude)	the registry subkeys that are not being monitored by the registry-monitoring configuration	PWKNTRegistry/instances/object/ExcludeKeyList	string

Table B-1 Configuration Variables for PATROL KM for Microsoft Windows OS (Part 7 of 8)

Variable	Description	Location	Type
List (Include)	the registry key that is being monitored by the registry-monitoring configuration	PWKNTRegistry/instances/object/ExcludeKeyList	string
Printer Monitoring Variables			
AlarmDayLimit	specifies the length of time a print job can be in the queue before generating an alarm	PWKNTPrinter/Time Limit	integer
AlarmEnabled	whether to generate an alarm when a print job is in the queue for more than the specified length of time	PWKNTPrinter/Time Limit	Boolean
AlarmHourLimit	specifies the length of time a print job can be in the queue before generating an alarm	PWKNTPrinter/Time Limit	integer
AlarmMinuteLimit	specifies the length of time a print job can be in the queue before generating an alarm	PWKNTPrinter/Time Limit	integer
AlarmSecondLimit	specifies the length of time a print job can be in the queue before generating an alarm	PWKNTPrinter/Time Limit	integer
WarningDayLimit	specifies the length of time a print job can be in the queue before generating a warning	PWKNTPrinter/Time Limit	integer
WarningEnabled	whether to generate a warning when a print job is in the queue for more than the specified length of time	PWKNTPrinter/Time Limit	Boolean
WarningHourLimit	specifies the length of time a print job can be in the queue before generating a warning	PWKNTPrinter/Time Limit	integer
WarningMinuteLimit	specifies the length of time a print job can be in the queue before generating a warning	PWKNTPrinter/Time Limit	integer
WarningSecondLimit	specifies the length of time a print job can be in the queue before generating a warning	PWKNTPrinter/Time Limit	integer
Monitor All	whether to monitor all detected printers	PWKNTPrinter/Time Limit	Boolean

Table B-1 Configuration Variables for PATROL KM for Microsoft Windows OS (Part 8 of 8)

Variable	Description	Location	Type
Windows 2000 Job Object Monitoring Variables			
ChangeStateToOK	whether to automatically acknowledge job processes that have alarmed	NTOSKM/PWKNTJobObjectsMonitoring	integer
IncludeAll	whether to monitor all jobs	NTOSKM/PWKNTJobObjectsMonitoring	Boolean
MonitorChildProcesses	whether to automatically monitor all child processes of the processes within a job	NTOSKM/PWKNTJobObjectsMonitoring	integer
MonitorProcessInProcessGroup	whether to monitor the processes that are in the job	NTOSKM/PWKNTJobObjectsMonitoring	integer

PATROL KM for Microsoft Windows Domain Services

Table B-2 lists PATROL KM for Microsoft Windows Domain Services component variable settings.

Table B-2 Configuration Variables for the Domain Services Component (Part 1 of 3)

Variable	Description	Location	Type
SCOPEADD	raises a PATROL event when a DHCP Scope is added	/DomainKM/DHCP/Events/SCOPEADD	Boolean
SCOPEDEL	raises a PATROL event when a DHCP Scope is removed	/DomainKM/DHCP/Events/SCOPEDEL	Boolean
DHCPBAK	raises a PATROL event when the DHCP database is backed up	/DomainKM/DHCP/Events/DHCPBAK	Boolean
IterationCount	the number of times to perform a DNS test	/DomainKM/DNS/IterationCount	string
ResolveTestList	comma-separated list of IP addresses to attempt during DNS test	/DomainKM/DNS/ResolveTestList	string
ServerIPAddress	IP address for DNS Server	/DomainKM/DNS/ServerIPAddress	string
ServerPortNumber	port of DNS Server	/DomainKM/DNS/ServerPortNumber	string

Table B-2 Configuration Variables for the Domain Services Component (Part 2 of 3)

Variable	Description	Location	Type
TCPorUDP	protocol for DNS Test 1 = TCP 0= UDP	/DomainKM/DNS/ TCPorUDP	Boolean
MBREL	raises a PATROL event when a new master browser is elected	/DomainKM/Domain/ MBREL	Boolean
MBRADD	raises a PATROL event when a member server is added to the domain	/DomainKM/Domain/ MBRADD	Boolean
MBRDEL	raises a PATROL event when a member server is removed from the domain	/DomainKM/Domain/ MBRDEL	Boolean
BDCADD	raises a PATROL event when a BDC server is added to the domain	/DomainKM/Domain/ BDCADD	Boolean
BDCDEL	raises a PATROL event when a BDC server is removed from the domain	/DomainKM/Domain/ BDCDEL	Boolean
DHCPADD	raises a PATROL event when a DHCP server is added to the domain	/DomainKM/Domain/ DHCPADD	Boolean
DHCPDEL	raises a PATROL event when a DHCP server is removed from the domain	/DomainKM/Domain/ DHCPDEL	Boolean
WINSADD	raises a PATROL event when a WINS server is added to the domain	/DomainKM/Domain/ WINSADD	Boolean
WINSDEL	raises a PATROL event when a WINS server is removed from the domain	/DomainKM/Domain/ WINSDEL	Boolean
IdleServerTime	the number of minutes a server is inactive before it is considered idle	/DomainKM/Server/ IdleServerTime	string
ServerExcludeList	comma-separated list of domain servers that should not be discovered by NT_REMOTE_SERVERS	/DomainKM/ RemoteServers/ ServerExcludeList	string
MaxShares	the maximum number of shares that can be discovered by NT_SHARES Note: Increasing this value above 300 may affect PATROL Agent performance.	/DomainKM/Shares/ MaxShares	string

Table B-2 Configuration Variables for the Domain Services Component (Part 3 of 3)

Variable	Description	Location	Type
ShareExcludeList	comma-separated list of shared directories that should not be discovered by NT_SHARES	/DomainKM/Shares/ ShareExcludeList	string
TrustExcludeList	comma-separated list of trust relationships that should not be discovered by NT_TRUST	/DomainKM/Trust/ TrustExcludeList	string
MaxUsers	the maximum number of user accounts that can be discovered by NT_USERS Note: Increasing this value above 300 may affect PATROL Agent performance.	/DomainKM/Users/ MaxUsers	string
UserExcludeList	comma-separated list of user accounts that should not be discovered by NT_USERS	/DomainKM/Users/ UserExcludeList	string

PATROL KM for Microsoft Windows Message Queue

Table B-3 provides PATROL KM for Microsoft Message Queue variable settings.

Table B-3 Configuration Variables for PATROL for Message Queue

Variable	Description	Location	Type
TotalMessageCountThreshold	the number of messages currently managed by the MSMQ service	/MQ_SERVER/ QueueMsgCount Threshold	integer
TotalMessageSizeThreshold	the size of all message queues managed by the MSMQ service	/MQ_SERVER/ QueueMsgThreshold	integer
MessageQueueCountThreshold	the number of messages currently in the queue	/MQ_QUEUES/ QueueMsgCount Threshold	integer
MessageQueueSizeThreshold	the number of kilobytes used by all messages in the queue	/MQ_QUEUES/ QueueMsgSize Threshold	integer
JournalQueueCountThreshold	the number of messages in the journal queue	/MQ_QUEUES/ JournalMsgCount Threshold	integer
JournalQueueSizeThreshold	the size of all messages in the journal queue	/MQ_QUEUES/ JournalMsgSize Threshold	integer
ScheduleRountTripMsg. Time	a string which specifies the scheduled servers and their respective scheduled interval	/MQ_SERVER/ ScheduledServers	string

PATROL KM for Microsoft COM+

Table B-4 provides PATROL KM for Microsoft COM+ variable settings.

Table B-4 Configuration Variables for PATROL KM for Microsoft COM+

Variable	Description	Location	Type
COM+ Application List	a comma-separated list of COM+ applications that are discovered by COM_APPLICATION	/COM_PLUS/Application List	string

PATROL Wizard for Microsoft Performance Monitor and WMI

Table B-5 provides the PATROL Wizard for Microsoft Performance Monitor and WMI variable settings.

Table B-5 Configuration Variables for PATROL Wizard for Microsoft Performance Monitor and WMI (Part 1 of 2)

Variable	Description	Location	Type
Performance Counter Wizard (NT_PERFMON_WIZARD)			
Name	lists the NT_PERFMON_WIZARD application class name	/Perfmon/NT_PERFMON_WIZARD/Name	string
Objects	comma-separated list of objects to monitor	/Perfmon/NT_PERFMON_WIZARD/Objects	string
Counters	comma-separated list of counters monitored for the object	/Perfmon/NT_PERFMON_WIZARD/object/Counter s	string
Instances	comma-separated list of instance of the object to monitor	/Perfmon/NT_PERFMON_WIZARD/object/Instanc es	string
AlarmMax	the upper-level alarm threshold for a specific counter instance	/Perfmon/NT_PERFMON_WIZARD/object/counter/ AlarmMax	integer
AlarmMin	the lower-level alarm threshold for a specific counter instance	/Perfmon/NT_PERFMON_WIZARD/object/counter/ AlarmMin	integer

Table B-5 Configuration Variables for PATROL Wizard for Microsoft Performance Monitor and WMI (Part 2 of 2)

Variable	Description	Location	Type
WarnMax	the upper-level warning threshold for a specific counter instance	/Perfmon/NT_PERFMON_WIZARD/object/counter/WarnMax	Integer
WarnMin	the lower-level warning threshold for a specific counter instance	/Perfmon/NT_PERFMON_WIZARD/object/counter/WarnMin	Integer
WMI Wizard (NT_WMI)			
Parameters	comma-separated list of NT_WMI parameters	/Perfmon/NT_WMI/Parameters	string
Query	WQL query used in the created NT_WMI parameter	/Perfmon/NT_WMI/name/Query	string
AlarmMax	the upper-level alarm threshold for a specific NT_WMI parameter	/Perfmon/NT_WMI/name/AlarmMax	integer
AlarmMin	the lower-level alarm threshold for a specific NT_WMI parameter	/Perfmon/NT_WMI/name/AlarmMin	integer
WarnMax	the upper-level warning threshold for a specific NT_WMI parameter	/Perfmon/NT_WMI/name/WarnMax	integer
WarnMin	the lower-level warning threshold for a specific NT_WMI parameter	/Perfmon/NT_WMI/name/WarnMin	integer

PATROL for Windows .kml Files

This section contains a list of the KM files that are included in each of the PATROL for Windows Servers .kml files.

PATROL for Windows Servers .kml Files	C-2
PATROL KM for Log Management	C-2
PATROL KM for Windows OS	C-3
PATROL KM for Microsoft Windows Domain Services.	C-6
PATROL KM for Microsoft COM+ (Windows 2000).	C-7
PATROL KM for Microsoft Message Queue.	C-7
PATROL Wizard for Microsoft Performance Monitor and WMI	C-8
PATROL KM for History Loader	C-8
PATROL KM for Event Management	C-9

PATROL for Windows Servers .kml Files

PATROL for Windows Servers uses several **.kml** files, which load specific application classes. For detailed instructions, see “Loading the PATROL for Windows Servers KMs” on page 3-5.

PATROL KM for Log Management

The PATROL KM for Log Management uses the **LOG.kml** file, which loads the application classes shown in Table C-1.

Table C-1 PATROL KM for Log Management .kml File

Component and .kml	Application Classes
PATROL KM for Log Management	LOG.km LOGMON.km LOGTEMP.km

PATROL KM for Windows OS

The PATROL KM for Windows OS uses the **NT_LOAD.kml** file, which loads the application classes shown in Table C-2:

Table C-2 PATROL KM for Windows OS NT_LOAD.kml File (Part 1 of 2)

Component and .kml	.kml and Application Classes
PATROL KM for Windows OS (uses NT_LOAD.kml and NT_BASE.kml) Note: NT_LOAD.kml includes NT_BASE.kml	NT_BASE.kml (see Table C-4, "PATROL KM for Windows OS NT_BASE.kml File," on page C-5) NT_BSK NT_EVENTLOG NT_EVLOGFILES NT_EVINSTS NT_SERVER NT_SECURITY NT_PROCESS_CONTAINER NT_PROCESS_GROUP NT_PROCESS NT_PHYSICAL_DISKS_CONTAINER NT_PHYSICAL_DISKS NT_PAGEFILE NT_NETWORK NT_NETWORK_CONTAINER NT_SERVICES_CONTAINER NT_SERVICES NT_PRINTER_CONTAINER NT_PRINTERJOB NT_PRINTERJOBS NT_PRINTER

Table C-3 Table B-11 PATROL KM for Windows OS .kml File (Part 2 of 2)

Component	Application Classes
PATROL KM for Windows OS (uses NT_LOAD.kml and NT_BASE.kml)	NT_NET_PROTOCOLS NT_NETBEUI_CONTAINER NT_IPX_CONTAINER NT_NETBIOS_CONTAINER NT_NETBEUI NT_NETBIOS NT_FTP NT_ICMP NT_IP NT_IPX NT_TCP NT_UDP NT_Composites NT_CompositesColl NT_REGISTRY NT_REGISTRY_GROUP NT_REGISTRY_GROUP_NO_ALARM NT_REGISTRY_KEYINST NT_REGISTRY_KEYINST_NO_ALARM NT_JOBS_CONTAINER NT_JOBS NT_JOBS_PROCESS_GROUP NT_JOBS_PROCESS
Note: NT_LOAD.kml includes NT_BASE.kml	

The **NT_LOAD.kml** file includes the **NT_BASE.kml** file, which loads the application classes shown in Table C-4.

Table C-4 PATROL KM for Windows OS NT_BASE.kml File

Component and .kml	Application Classes
PATROL KM for Windows OS (uses NT_LOAD.kml and NT_BASE.kml) Note: NT_LOAD.kml includes NT_BASE.kml	NT_OS NT_CACHE NT_CPU NT_CPU_CONTAINER NT_MEMORY NT_PAGEFILE_CONTAINER NT_PAGEFILE NT_SYSTEM NT_LOGICAL_DISKS_CONTAINER NT_LOGICAL_DISKS NT_NTFS_MOUNT_CONTAINER NT_NTFS_MOUNT NT_NTFS_QUOTA_CONTAINER NT_NTFS_QUOTA NT_NTFS_JOURNAL NT_HEALTH INET_NTS PATROL_NT

PATROL KM for Microsoft Windows Domain Services

The PATROL KM for Microsoft Windows Domain Services uses the **NTD.kml** file, which loads the application classes shown in Table C-5:

Table C-5 PATROL KM for Microsoft Windows Domain Services .kml File

Component and .kml	Application Classes
PATROL KM for Microsoft Windows Domain Services (uses NTD.kml)	NT_DOMAIN NT_MEMBER_SERVER NT_DFS_LINK NT_DFS_LINK_REPLICA NT_DFS_ROOT NT_DFS_ROOT_REPLICA NT_DHCP NT_DHCP_SCOPE NT_DNS NT_DNS_2000 NT_RAS NT_RAS_DEVICE NT_REMOTE_SERVERS NT_REPLICATION NT_REPL_DIR NT_REPL_SVR NT_SHARES NT_TRUST NT_USERS NT_USER_ACCOUNTS NT_WINS NT_WINS_PARTNER

PATROL KM for Microsoft COM+ (Windows 2000)

PATROL KM for Microsoft COM+ uses the **COM.kml** file, which loads the application classes shown in Table C-6.

Table C-6 PATROL KM for Microsoft COM+ (Windows 2000) .kml File

Component and .kml	Application Classes
PATROL KM for Microsoft COM+ (Windows 2000) (uses COM.kml)	COM_PLUS COM_APPLICATION COM_APPLICATIONC COM_DTC MTS_MTS MTS_PACKAGE MTS_PACKAGEC MTS_DTC

PATROL KM for Microsoft Message Queue

The PATROL KM for Microsoft Message Queue uses the **MSMQ.kml** file, which loads the application classes shown in Table C-7.

Table C-7 PATROL KM for Microsoft Message Queue .kml File

Component and .kml	Application Classes
PATROL KM for Microsoft Message Queue (uses MSMQ.kml)	MQ_CONTAINER MQ_SERVER MQ_QUEUE MQ_QUEUEC MQ_IS MQ_ROUNDTRIP MQ_SESSIONC MQ_SESSIONS

PATROL Wizard for Microsoft Performance Monitor and WMI

The PATROL Wizard for Microsoft Performance Monitor and WMI uses the **NT_PERFMON_WIZARD.kml** file, which loads the application classes shown in Table C-8.

Table C-8 PATROL Wizard for Microsoft Performance Monitor and WMI .kml File

Component and .kml	Application Classes
PATROL Wizard for Microsoft Performance Monitor and WMI (NT_PERFMON_WIZARD.kml)	NT_PERFMON_WIZARD (Performance Counter Wizard) NT_PERFMON_OBJECT NT_PERFMON_INSTANCE NT_PERFMON_COUNTER NT_WMI (WMI Wizard) NT_WMI_PARAMETER

PATROL KM for History Loader

The PATROL KM for History Loader uses the **HISTORY.kml** file, which loads the application classes shown in Table C-9.

Table C-9 PATROL KM for History Loader .kml File

Component and .kml	Application Classes
PATROL KM for History Loader (HISTORY.kml)	HISTORY_Computer HISTORY_Propagator INFORMIX_History_Loader INGRES_History_Loader MSSQLSERVER_History_Loader ORACLE_History_Loader SYBASE_History_Loader DB2CS_History_Loader BEST1_History_Loader DB2UDB_History_Loader

PATROL KM for Event Management

The PATROL KM for Event Management uses the **EVENT_MANAGEMENT.kml** file, which loads the application classes in Table C-10.

Table C-10 PATROL KM for Event Management .kml Files

Component and .kml	Application Classes
PATROL KM for Event Management (EVENT_MANAGEMENT.kml)	AS_EVENTSPRING.km AS_AVAILABILITY.km AS_EVENTSPRING_ALL_COMPUTERS.km

Index

Symbols

\$JAVA_HOME\$ 2-6
 \$PATROL_HOME/patrol 2-24
 %PATROL_CACHE% 2-24
 %PATROL_HOME% 2-24
 .kml
 COM.kml 3-5, C-7
 EVENT_MANAGEMENT.kml 3-6
 HISTORY.kml 3-5, C-8
 LOG.kml 3-6
 MSMQ.kml 3-5, C-7
 NT_BASE C-5
 NT_LOAD.kml 3-5, C-3
 NT_PERFMON_WIZARD.kml 3-6
 NTD.kml 3-5, C-6
 WBeM.kml 3-6
 .map files 2-44
 .NET Server 2-4
 .profile 2-50

A

accessControlList variable 3-13
 accounts
 requirements 3-12
 setting up for installation 2-7

accounts, *continued*
 Unix 2-8
 Windows 2-7
 AcknowledgeBy variable B-4
 Active Directory 1-6
 adding
 Performance Monitor (PerfMon)
 counters 3-34
 processes to be monitored 3-21
 registry keys to monitor 3-17
 services to be monitored 3-19
 WMI parameters 3-36
 administrator rights 3-12
 affinity, CPU 1-5
 agent
 configuration variables B-1–B-15
 installing a KM to 2-14
 PATROL 1-13
 AlarmMax variable B-14, B-15
 AlarmMin variable B-14, B-15
 alarms, generating 3-18, 3-20, 3-23
 alert settings 1-11
 alerts, configuring 3-30
 annotating events 3-43
 Annotation variable B-4
 application classes
 NT_CompositeColl 3-26
 NT_DHCP 2-6, 3-46

application classes, *continued*

- NT_DNS 3-46
- NT_EVENTLOG 3-12, 3-15
- NT_JOBS 3-27
- NT_LOGICAL_DISK 3-12
- NT_NTFS_MOUNT 3-13
- NT_NTFS_QUOTA 3-13
- NT_PROCESS 3-21
- NT_REGISTRY 3-17
- NT_REMOTE_SERVERS 3-46
- NT_SERVICES 3-12, 3-19
- NT_SHARES 3-46
- NT_TRUST 3-47
- NT_WINS 3-47

arguments, process 3-23

AS_EVSLocalAlertNotify.bat 3-29

Attended Mode Dialog Timeout field 3-25

AutoDisableELMEvFileFreeSpacePercent
variable B-3

automatic migration of KM customizations
2-43

automatic process monitoring 3-21

AutoMigration variable B-3

AutoRestartAutomaticStartupServices
variable B-6

AutoRestartManualStartupServices variable
B-6

B

backing up files 2-24

backup domain controllers, monitoring 1-7

BDCADD variable B-11

BDCDEL variable B-11

binary log files, monitoring 3-39

blackout 1-11

Blat shareware 3-29

blue screen configuration variables B-7

Bourne shell 2-50

BskCabFile variable B-7

BskCompName variable B-7

BskDiagReport variable B-7

BskDirName variable B-7

BskFound6008Time variable B-8

BskMoveFtp variable B-8

BskRegReport variable B-8

C

C shell 2-50

certification, Windows 1-13

ChangeStateToOK variable B-8, B-10

charting PATROL data 3-43

CollectorType variable B-4

colormap option 2-49

COM+ Application List variable B-14

COM.kml 3-5, C-7

command line options 2-35

command-line arguments 3-23

complus_km_1_3_00.map 2-44

components

- KM files C-2–C-9

- PATROL Adapter for Microsoft Office
1-12

- PATROL Adapter for WBEM 1-12

- PATROL Agent for Microsoft Windows
Servers 1-13

- PATROL Cluster Configuration Wizard
1-7

- PATROL KM for Event Management
1-11

- PATROL KM for History Loader 1-12

- PATROL KM for Log Management 1-10

- PATROL KM for Microsoft Cluster
Server 1-8

- PATROL KM for Microsoft COM+ 1-8

- PATROL KM for Microsoft Message
Queue 1-10

- PATROL KM for Microsoft Network
Load Balancing 1-8

- components, *continued*
 - PATROL KM for Microsoft Windows Active Directory 1-6
 - PATROL KM for Microsoft Windows Domain Services 1-7
 - PATROL KM for Microsoft Windows OS 1-5
- composite parameters, creating 3-26
- configuration variables B-1–B-15
- configurations, component-based
 - PATROL KM for History Loader C-8
 - PATROL KM for Microsoft COM+ (Windows 2000) C-7
 - PATROL KM for Microsoft Message Queue (MSMQ) C-7
 - PATROL KM for Microsoft Windows Domain Services C-6
 - PATROL Knowledge Module for Microsoft Windows Operating System C-3
- configuring
 - composite parameters 3-26
 - custom parameters 3-26
 - e-mail notification 3-29
 - event log monitoring 3-19
 - event monitoring 3-15
 - job objects 3-27
 - monitoring of text files 3-37
 - PATROL KM for Windows OS 3-12–3-28
 - process control 3-23
 - process monitoring 3-21–3-23
 - quotas 3-12
 - recovery actions 3-24
 - registry key monitoring 3-17–3-18
 - service monitoring 3-19–3-20
 - Windows event monitoring 3-15
- consoles, description of 2-14
- ConsolidateEventTypes variable B-4
- ConsolidateNumber variable B-4

- ConsolidateTime variable B-4
- Counters variable B-14
- CreateKeyInstances variable B-8
- creating
 - custom parameters 3-26
 - job objects 3-27
 - Windows event filters 3-16
 - WMI parameters 1-10
- customizations
 - migrating 2-41
 - migrating manually 2-44
 - migrating using KMDS 2-34
 - upgrading and preserving 2-32
 - upgrading without saving 2-25
- customized PSL, migrating 2-45

D

- database, parameter history 1-12
- deleting
 - KMs 3-9
 - old version 2-25
- dependencies 3-6
- DFS (Distributed File System) 1-7
- DHCP (Dynamic Host Configuration Protocol) 1-7
- DHCP reports 3-46
- DHCPADD variable B-11
- DHCPBAK variable B-10
- dhcpcmd.exe 2-5
- DHCPDEL variable B-11
- dhcpsapi.dll 2-5
- diagnostic reports B-7
- disabling
 - event log monitoring 3-15
 - KMs 3-9
- diskperf 3-28
- displaying
 - PATROL data in Microsoft Excel 3-44
 - Windows events 3-16

- Distributed File System (DFS) 1-7
- DNS (Domain Name Service) 1-7
- DNS reports 3-46
- dnscmd.exe 2-5
- domain controllers, monitoring 1-7
- Domain Name Service (DNS) 1-7
- domain_km_1_5_00.map 2-44
- dump files B-7
- Dynamic Host Configuration Protocol (DHCP) 1-7

E

- ELMEvFileFreeSpacePercent parameter B-3
- e-mail client requirements 2-6
- e-mail notification 3-29
- EnableAlarmForAutomaticStartupServices variable B-7
- EnableAlarmforManualStartupServices variable B-7
- EnableAlarmIfProcessDown variable B-6
- EnableAlarmIfProcessStarts variable B-6
- enabling event log monitoring 3-15
- environment variables
 - LANG 2-50
 - PATH 2-50
 - PATROL_BROWSER 2-51
 - setting for Help browser 2-50
 - setting for the browser 2-50
- event filters 3-16
- EVENT_MANAGEMENT.kml 3-30, C-9
- EventReport variable B-4
- events
 - monitoring 3-15
 - PATROL, managing 1-11
- EventType variable B-5
- eXceed 2-49
- excluding registry keys from monitoring 3-17

- exported installation packages, installing 2-48
- exporting
 - installation packages 2-47
- expressions, log file 3-41

F

- failover, cluster 1-8
- FAT file system 2-5
- file systems, supported 2-5
- files, removing from PATROL_CACHE 2-25
- filter, event monitoring 3-15
- FilterDescription variable B-5
- first time installation 2-18
- ForceMigration variable B-3
- ForceRefresh variable B-3

G

- graphing PATROL data 3-43

H

- histakm_1_4_05.map 2-44
- history reports 3-45
- HISTORY.kml 3-5, C-8
- HPFS file system 2-5

I

- icons, LOGMON 3-39
- IdleServerTime variable B-11
- IncludeAll variable B-10
- IncludeAllCategories variable B-5
- IncludeAllEventIDs variable B-5

- IncludeAllSources variable B-5
- IncludeAllStrings variable B-5
- IncludeAllUsers variable B-5
- installation
 - backing up before migration 2-24
 - choosing a target machine 2-14
 - over-the-top 2-25
 - preparing for 2-12
 - setting up installation accounts 2-7
 - system requirements 2-3, 2-4
 - typical option 2-16
 - Unix account requirements 2-8
 - verifying requirements 2-3
 - Windows account requirements 2-7
- installation packages
 - exporting 2-47
 - installing 2-48
- installing
 - backing up prior to 2-24
 - clearing cache 2-25
 - exported installation packages 2-48
 - for the first time 2-18
 - into KMDS 2-34, 2-35
 - manual migration 2-36
 - upgrading from an earlier version 2-23
- InstanceName variable B-8
- Instances variable B-14
- IterationCount variable B-10

J

- Java Runtime Environment (JRE) 2-6
- job objects 1-5, 3-27
- JournalQueueCountThreshold variable B-13
- JournalQueueSizeThreshold variable B-13
- JRE (Java Runtime Environment) 2-6

K

- keys, monitoring 3-17
- KM configuration variables B-1–B-15
- KM customizations
 - migrating manually 2-44
 - migrating with KMDS 2-43
- KMDS
 - command line options for installing 2-35
 - installing into 2-34
 - using to migrate KM customizations 2-43
- KMs
 - deploying 1-4
 - determining if migratable 2-33
 - included with product C-1–C-9
 - installing QuickStart packages 2-16
 - loading 3-4–3-7
 - upgrading from an earlier version 2-23
- Korn shell 2-50

L

- Label variable B-8
- LANG environment variable 2-50
- license
 - OneKey 2-7
 - requirements 2-4
- loading KMs 3-4–3-7
- loading product components
 - PATROL Console for Unix 3-6
 - PATROL Console for Windows 3-5
 - requirements 3-3
- log file monitoring
 - automated recovery actions 3-39
 - behavior of application 3-42
 - binary files 3-39
 - log search templates 3-39
 - LOGMON instance icons 3-39

- log file templates
 - applying to log files 3-42
 - creating 3-40
 - setting alert severity 3-42
 - using regular expressions 3-41
- log file templates, naming conventions for 3-41
- log files
 - applying search templates 3-42
 - currently monitored 3-42
- LOG.kml 3-6
- logging registry activity 3-18
- logical disk drives, monitoring 3-28
- login accounts
 - requirements 2-7
 - Windows 2-7

M

- managed systems, overview 2-14
- manual
 - migration of KM customizations 2-44
 - process monitoring 3-21
- MaxShares variable B-11
- MaxUsers variable B-12
- MBRADD variable B-11
- MBRDEL variable B-11
- MBREL variable B-11
- memory requirements 2-5
- merge map file 2-44
- MessageQueueCountThreshold variable B-13
- MessageQueueSizeThreshold variable B-13
- Microsoft .NET Server 2-4
- Microsoft Cluster Server 1-8
- Microsoft Excel 2-6
- Microsoft Job Objects
 - configuring 3-27–3-28
 - monitoring features 1-5
- Microsoft Message Queue (MSMQ) 1-10
- Microsoft Network Load Balancing (NLB) 1-8
- Microsoft Transaction Server (MTS)/COM+ 1-8
- migrating
 - customizations 2-41
 - customized PSL 2-45
 - determining if KM is migratable 2-33
 - from an earlier version of the KM 2-23
 - installation procedure for 2-36
 - KM customizations manually 2-44
 - KM customizations with KMDS 2-43
 - preparing for 2-42
 - using KMDS 2-34
- migration
 - backing up current installation before 2-24
 - preparing 2-24
- Monitor All Automatic Startup Services variable B-7
- Monitor All Disabled Services variable B-7
- Monitor All Eventlogs variable B-4
- Monitor All Manual Startup Services variable B-7
- Monitor All variable B-9
- monitor requirements 2-5
- MonitorChildProcess variable B-10
- monitoring
 - Active Directory 1-6
 - backup domain controllers 1-7
 - clusters 1-7
 - domain controllers 1-7
 - events 3-15, 3-19
 - files 3-15, 3-19
 - job objects 3-27
 - log files, binary 3-39
 - log files, templates 3-39
 - logical or physical disk drives 3-28
 - logs 3-19
 - mount points 3-13

- monitoring, *continued*
 - processes 3-21, 3-27
 - registry keys 3-17
 - service executables 3-20
 - services 3-19
 - strings 3-15, 3-19
 - text files 3-37
- MonitorProcessInProgressGroup variable
 - B-10
- mount points, monitoring 3-13
- MqRoundtrip variable B-13
- MSMQ.kml 3-5, C-7
- msmq_km_1_4_00.map 2-44

N

- Name variable B-14
- naming conventions, log file template 3-41
- Netscape Navigator 2-49
- new PATROL users
 - easy install option 2-16
 - installing for the first time 2-18
- notification, e-mail 3-29
- NT 3-46
- NT_3_8_00.map 2-44
- NT_BASE.kml C-5
- NT_CompositesColl application class 3-26
- NT_DHCP application class 2-6
- NT_EVENTLOG application class 3-12, 3-15
- NT_JOBS application class 3-27
- NT_LOAD.kml 3-5, C-3
- NT_LOGICAL_DISK application class 3-12
- NT_NTFS_MOUNT application class 3-13
- NT_NTFS_QUOTA application class 3-13
- NT_PERFMON application class 3-6
- NT_PROCESS application class 3-21
- NT_REGISTRY application class 3-17
- NT_SERVICES application class 3-12, 3-19

- NTD.kml 3-5, C-6
- NTFS file system 2-5

O

- Objects variable B-14
- OneKey software 2-7
- operating system, monitoring 3-12
- over-the-top installation 2-25

P

- page_bad_config_switch variable B-3
- PAGEBadConfiguration parameter B-3
- paging 1-11
- parameters
 - composite 3-26
 - creating 1-10
 - creating e-mail notifications for 3-29
 - creating PerfMon-based 3-34
 - creating WMI 3-36
 - custom 3-26
 - customizing 3-26
 - data, storing and analyzing 1-12
 - history, viewing 3-5
 - polling time 1-11
 - PROCDown 3-23
 - PROCProcessColl 3-23
 - PROCProcessorTimePercent 3-22, 3-23
 - PROCStatus 3-23
 - ServiceStatus 3-19, 3-20
 - SvcNotResponding 3-20
 - SvcStatus 3-20
 - thresholds 1-11
- Parameters variable B-15
- PATH environment variable 2-50
- PATROL account, creating 2-7

PATROL Adapter for Microsoft Office
description 1-12
installation requirements 3-44

PATROL Adapter for WBEM 1-12

PATROL Agent
description 1-13
installing a KM to 2-14

PATROL Central - Web Edition
loading KMs on 3-8

PATROL Central Operator - Web Edition
installing 2-15

PATROL Central Operator - Windows
Edition 3-10

PATROL Cluster Configuration Wizard
description 1-7

PATROL Configuration Manager 1-4

PATROL Console
and Netscape Navigator 2-49
installing a KM to 2-14

PATROL Event Manager (PEM) 3-13

PATROL for Windows Domain Services
requirements 2-7

PATROL for Windows Operating System
Monitor service 1-13

PATROL KM for Event Management
.kml files C-9
configuring 3-29–3-31

PATROL KM for History Loader
description 1-12
KMs C-8

PATROL KM for Microsoft Cluster Server
1-8

PATROL KM for Microsoft COM+
preloaded files 2-10
report options 3-48
Windows configuration C-7

PATROL KM for Microsoft Message Queue
KMs C-7
preloaded files 2-11
report options 3-47

PATROL KM for Microsoft Network Load
Balancing 1-8

PATROL KM for Microsoft Windows Active
Directory 1-6

PATROL KM for Microsoft Windows
Domain Services
KMs C-6
network system requirements 2-5

PATROL Knowledge Module Deployment
Server (KMDS) 2-5

PATROL Knowledge Module for Microsoft
Windows Operating Systems
KMs C-3
preloaded files 2-10
requirements 2-6

PATROL security 2-17

PATROL Wizard for Microsoft Performance
Monitor and WMI
creating WMI parameters 3-36
migration 2-33

PATROL Wizard for Performance and WMI
.kml file C-8
application classes C-8
description 1-10

PATROL Wizard for Performance Monitor
and WMI
configuring 3-32
creating Performance Monitor
parameters 3-34
loading 3-33

PATROL_BROWSER environment variable
2-51

PATROL_CACHE 2-24, 2-25

PATROL_HOME 2-24

PatrolAgent service 1-13

pconfig variables B-1

PEM (PATROL Event Manager) 3-13

Performance Counter (PerfMon) Wizard
1-10

physical disk drives, monitoring 3-28

- planning, installation 2-12
- platforms, supported 2-4
- polling, parameter time 1-11
- preloaded files 2-10–2-11
- preparing
 - for installation 2-12
 - to upgrade 2-24
- priority, process 3-27
- PROCDOWN parameter 3-23
- process control, configuring 3-23
- processes
 - monitoring 3-21, 3-27
 - priority 3-27
 - restarting 3-23
 - run-away B-6
 - scheduling class 3-27
 - stopping 3-23
- ProcessName variable B-6
- PROCProcessColl parameter 3-23
- PROCProcessorTimePercent parameter 3-22, 3-23
- PROCStatus parameter 3-23
- product
 - components 1-4
 - configuration tasks 3-12
- PSL
 - migrating 2-45

Q

- Query variable B-15
- quotas, configuring 3-12

R

- RAS (Remote Access Service) 1-7
- Recovery Action All Eventlogs variable B-4
- recovery actions 3-24
 - configuring 3-24

- recovery actions, *continued*
 - log file monitoring 3-39
 - log file, behavior 3-42
- RefreshInterVal variable B-3
- registry keys
 - excluding from monitoring 3-18
 - monitoring 3-17
- registry, monitoring 3-17
- regular expressions, log file 3-41
- Remote Access Service (RAS) 1-7
- removing
 - KMs 3-9
 - registry keys from monitoring 3-17
- reports 3-45–3-48
- RequestType variable B-8
- requirements
 - e-mail client 2-6
 - log file templates, naming 3-41
 - Netscape Navigator 2-6
 - overview 2-3
 - software 3-3
 - system 2-3, 2-4
 - Unix account 2-8
 - Windows account 2-7
- ResolveTestList variable B-10
- restarting
 - monitored services 3-19
 - processes 3-23
- RetainEventDescriptions variable B-5
- RootKeyIndex variable B-8
- RTservers 2-15
- run-away processes B-6

S

- scheduling class, process 3-27
- SCOPEADD variable B-10
- SCOPEDEL variable B-10

- security
 - event log 3-12
 - overview 2-17
- ServerExcludeList variable B-11
- ServerIPAddress variable B-10
- ServerPortNumber variable B-10
- services
 - checking status of 3-20
 - monitoring 3-19
 - monitoring executables for 3-20
 - PATROL for Windows Servers 1-13
 - restarting 3-20
- ServiceStatus parameter 3-19, 3-20
- setting environment variables for Help
 - browser 2-50
- ShareExcludeList variable B-12
- shells
 - Bourne 2-50
 - C 2-50
 - Korn 2-50
- SNMP
 - requirements 2-6
- software requirements 3-3
- starting services 3-20
- startup properties, service 3-12
- StartupCommand variable B-6
- StatusSortKey variable B-5
- Stop errors B-7
- stopping
 - event log monitoring 3-15
 - monitoring of registry keys 3-17
 - processes 3-23
 - run-away processes 3-23
- sub-keys, excluding from monitoring 3-17
- Suspend Recovery Action field 3-25
- SvcNotResponding parameter 3-20
- SvcStatus parameter 3-20
- system requirements 2-3, 2-4
- system roles
 - console systems 2-14, 2-15

- managed systems 2-14
- overview of target machines 2-14

T

- TCP/IP 1-8
- TCPorUDP variable B-11
- templates
 - log file monitoring 3-39
 - log file, applying to files 3-42
 - log files, creating 3-40
 - PATROL Adapter for Microsoft Office 3-46
- terminating processes 3-23
- Test Query 3-36
- text files, monitoring 3-37
- thresholds, parameter 1-11
- TimeLimitForKillRunAwayProcess variable B-6
- ToggleAlarm variable B-8
- TotalMessageCountThreshold variable B-13
- TotalMessageSizeThreshold variable B-13
- TrustExcludeList variable B-12
- typical installation option 2-16

U

- UDP protocol B-11
- Unix
 - account requirements 2-8
 - console 3-6
- unloading KMs 3-9–3-10
- unresponsive services 3-20
- upgrading 2-23
 - backing up current installation before 2-24
 - choosing a procedure 2-23
 - from an earlier version of the KM 2-23
 - preparing 2-24

upgrading, *continued*
 removing files from PATROL_CACHE
 while 2-25
 saving customizations 2-32
 without saving customizations 2-25
UseCheckPoint variable B-3
user account 2-50
UserDefinedProcess variable B-6
UserExcludeList variable B-12

V

variables

 accessControlList 3-13
 PATROL KM for Microsoft COM+
 B-14
 PATROL KM for Windows Domain
 Services B-10–B-12
 PATROL KM for Windows Message
 Queue B-13
 PATROL KM for Windows OS B-3–B-8
 PATROL_BROWSER 2-51
 wpconfig 1-4
VeriTest 1-13
viewing
 agent configuration variables B-1
 Windows events 3-16

W

warnings, generating 3-19, 3-20, 3-23
WarnMax variable B-15
WarnMin variable B-15
WBEM.kml 3-6
Windows account requirements 2-7
Windows Event Viewer 3-16
Windows Internet Naming Service (WINS)
 1-7

Windows Management Instrumentation
 (WMI) 1-10
WINS (Windows Internet Naming Service)
 1-7
WINS reports 3-47
WINSADD variable B-11
WINSDEL variable B-11
WMI parameters, creating 3-36
WMI Wizard 1-10
wpconfig variables 1-4
WpReplicationFailures parameter 2-6
WQL 3-36

STOP!

IMPORTANT INFORMATION - DO NOT INSTALL THIS PRODUCT UNLESS YOU HAVE READ ALL OF THE FOLLOWING MATERIAL

By clicking the YES or ACCEPT button below (when applicable), or by installing and using this Product or by having it installed and used on your behalf, You are taking affirmative action to signify that You are entering into a legal agreement and are agreeing to be bound by its terms, EVEN WITHOUT YOUR SIGNATURE. BMC is willing to license this Product to You ONLY if You are willing to accept all of these terms. CAREFULLY READ THIS AGREEMENT. If You DO NOT AGREE with its terms, DO NOT install or use this Product; press the NO or REJECT button below (when applicable) or promptly contact BMC or your BMC reseller and your money will be refunded if by such time You have already purchased a full-use License.

SOFTWARE LICENSE AGREEMENT FOR BMC PRODUCTS

SCOPE. This is a legally binding Software License Agreement (“License”) between You (either an individual or an entity) and BMC pertaining to the original computer files (including all computer programs and data stored in such files) contained in the enclosed Media (as defined below) or made accessible to You for electronic delivery, if as a prerequisite to such accessibility You are required to indicate your acceptance of the terms of this License, and all whole or partial copies thereof, including modified copies and portions merged into other programs (collectively, the “Software”). “Documentation” means the related hard-copy or electronically reproducible technical documents furnished in association with the Software, “Media” means the original BMC-supplied physical materials (if any) containing the Software and/or Documentation, “Product” means collectively the Media, Software, and Documentation, and all Product updates subsequently provided to You, and “You” means the owner or lessee of the hardware on which the Software is installed and/or used. “BMC” means BMC Software Distribution, Inc. unless You are located in one of the following regions, in which case “BMC” refers to the following indicated BMC Software, Inc. subsidiary: (i) Europe, Middle East or Africa --BMC Software Distribution, B.V., (ii) Asia/Pacific -- BMC Software Asia Pacific Pte Ltd., (iii) Brazil -- BMC Software do Brazil, or (iv) Japan -- BMC Software K.K. **If You enter into a separate, written software license agreement signed by both You and BMC or your authorized BMC reseller granting to you the rights to install and use this Product, then the terms of that separate, signed agreement will apply and this License is void.**

FULL-USE LICENSE. Subject to these terms and payment of the applicable license fees, BMC grants You this non-exclusive License to install and use one copy of the Software for your internal use on the number(s) and type(s) of servers or workstations for which You have paid or agreed to pay to BMC or your BMC reseller the appropriate license fee. If your license fee entitles You only to a License having a limited term, then the duration of this License is limited to that term; otherwise this License is perpetual, subject to the termination provisions below.

TRIAL LICENSE. If You have not paid or agreed to pay to BMC or your BMC Reseller the appropriate license fees for a full use license, then, **NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THIS LICENSE:** (i) this License consists of a non-exclusive evaluation license (“Trial License”) to use the Product for a limited time (“Trial Period”) only for evaluation; (ii) during the Trial Period, You may not use the Software for development, commercial, production, database management or other purposes than those expressly permitted in clause (i) immediately above; and (iii) your use of the Product is on an **AS IS** basis, and **BMC, ITS RESELLERS AND LICENSORS GRANT NO WARRANTIES OR CONDITIONS (INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE) TO YOU AND ACCEPT NO LIABILITY WHATSOEVER RESULTING FROM THE USE OF THIS PRODUCT UNDER THIS TRIAL LICENSE.** If You use this Product for other than evaluation purposes or wish to continue using it after the Trial Period, you must purchase a full-use license. When the Trial Period ends, your right to use this Product automatically expires, though in certain cases You may be able to extend the term of the Trial Period by request. Contact BMC or your BMC reseller for details.

TERM AND TERMINATION. This License takes effect on the first to occur of the date of shipment or accessibility to You for electronic delivery, as applicable (the “Product Effective Date”). You may terminate this License at any time for any reason by written notice to BMC or your BMC reseller. This License and your right to use the Product will terminate automatically with or without notice by BMC if You fail to comply with any material term of this License. Upon termination, You must erase or destroy all components of the Product including all copies of the Software, and stop using or accessing the Software. Provisions concerning Title and Copyright, Restrictions (or Restricted Rights, if You are a U.S. Government entity) or limiting BMC’s liability or responsibility shall survive any such termination.

TITLE AND COPYRIGHT; RESTRICTIONS. All title and copyrights in and to the Product, including but not limited to all modifications thereto, are owned by BMC and/or its affiliates and licensors, and are protected by both United States copyright law and applicable international copyright treaties. You will not claim or assert title to or ownership of the Product. To the extent expressly permitted by applicable law or treaty notwithstanding this limitation, You may copy the Software only for backup or archival purposes, or as an essential step in utilizing the Software, but for no other purpose. You will not remove or alter any copyright or proprietary notice from

copies of the Product. You acknowledge that the Product contains valuable trade secrets of BMC and/or its affiliates and licensors. Except in accordance with the terms of this License, You agree (a) not to decompile, disassemble, reverse engineer or otherwise attempt to derive the Software's source code from object code except to the extent expressly permitted by applicable law or treaty despite this limitation; (b) not to sell, rent, lease, license, sublicense, display, modify, time share, outsource or otherwise transfer the Product to, or permit the use of this Product by, any third party; and (c) to use reasonable care and protection to prevent the unauthorized use, copying, publication or dissemination of the Product and BMC confidential information learned from your use of the Product. **You will not export or re-export any Product without both the written consent of BMC and the appropriate U.S. and/or foreign government license(s) or license exception(s).** Any programs, utilities, modules or other software or documentation created, developed, modified or enhanced by or for You using this Product shall likewise be subject to these restrictions. BMC has the right to obtain injunctive relief against any actual or threatened violation of these restrictions, in addition to any other available remedies. Additional restrictions may apply to certain files, programs or data supplied by third parties and embedded in the Product; consult the Product installation instructions or Release Notes for details.

LIMITED WARRANTY AND CONDITION. If You have purchased a Full-Use License, BMC warrants that (i) the Media will be, under normal use, free from physical defects, and (ii) for a period of ninety (90) days from the Product Effective Date, the Product will perform in substantial accordance with the operating specifications contained in the Documentation that is most current at the Product Effective Date. BMC's entire liability and your exclusive remedy under this provision will be for BMC to use reasonable best efforts to remedy defects covered by this warranty and condition within a reasonable period of time or, at BMC's option, either to replace the defective Product or to refund the amount paid by You to license the use of the Product. BMC and its suppliers do not warrant that the Product will satisfy your requirements, that the operation of the Product will be uninterrupted or error free, or that all software defects can be corrected. This warranty and condition shall not apply if: (i) the Product is not used in accordance with BMC's instructions, (ii) a Product defect has been caused by any of your or a third party's malfunctioning equipment, (iii) any other cause within your control causes the Product to malfunction, or (iv) You have made modifications to the Product not expressly authorized in writing by BMC. No employee, agent or representative of BMC has authority to bind BMC to any oral representations, warranties or conditions concerning the Product. **THIS WARRANTY AND CONDITION IS IN LIEU OF ALL OTHER WARRANTIES AND CONDITIONS. THERE ARE NO OTHER EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS, INCLUDING THOSE OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, REGARDING THIS LICENSE OR ANY PRODUCT LICENSED HEREUNDER. THIS PARAGRAPH SHALL NOT APPLY TO A TRIAL LICENSE.** Additional support and maintenance may be available for an additional charge; contact BMC or your BMC reseller for details.

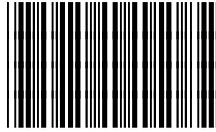
LIMITATION OF LIABILITY. Except as stated in the next succeeding paragraph, BMC's and your BMC reseller's total liability for all damages in connection with this License is limited to the price paid for the License. **IN NO EVENT SHALL BMC BE LIABLE FOR ANY CONSEQUENTIAL, SPECIAL, INCIDENTAL, PUNITIVE OR INDIRECT DAMAGES OF ANY KIND ARISING OUT OF THE USE OF THIS PRODUCT (SUCH AS LOSS OF PROFITS, GOODWILL, BUSINESS, DATA OR COMPUTER TIME, OR THE COSTS OF RECREATING LOST DATA), EVEN IF BMC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.** Some jurisdictions do not permit the limitation of consequential damages so the above limitation may not apply.

INDEMNIFICATION FOR INFRINGEMENT. BMC will defend or settle, at its own expense, any claim against You by a third party asserting that your use of the Product within the scope of this License violates such third party's patent, copyright, trademark, trade secret or other proprietary rights, and will indemnify You against any damages finally awarded against You arising out of such claim. However, You must promptly notify BMC in writing after first receiving notice of any such claim, and BMC will have sole control of the defense of any action and all negotiations for its settlement or compromise, with your reasonable assistance. BMC will not be liable for any costs or expenditures incurred by You without BMC's prior written consent. If an order is obtained against your use of the Product by reason of any claimed infringement, or if in BMC's opinion the Product is likely to become the subject of such a claim, BMC will at its option and expense either (i) procure for You the right to continue using the product, or (ii) modify or replace the Product with a compatible, functionally equivalent, non-infringing Product, or (iii) if neither (i) nor (ii) is practicable, issue to You a pro-rata refund of your paid license fee(s) proportionate to the number of months remaining in the 36 month period following the Product Effective Date. This paragraph sets forth your only remedies and the total liability to You of BMC, its resellers and licensors arising out of such claims.

GENERAL. This License is the entire understanding between You and BMC concerning this License and may be modified only in a mutually signed writing between You and BMC. If any part of it is invalid or unenforceable, that part will be construed, limited, modified, or severed so as to eliminate its invalidity or unenforceability. This License will be governed by and interpreted under the laws of the jurisdiction named below, without regard to conflicts of law principles, depending on which BMC Software, Inc. subsidiary is the party to this License: (i) BMC Software Distribution, Inc. - the State of Texas, U.S.A., (ii) BMC Software Distribution, B.V. - The Netherlands, (iii) BMC Software Asia Pacific Pte Ltd. -- Singapore (iv) BMC Software do Brazil -- Brazil, or (v) BMC Software K.K. -- Japan. Any person who accepts or signs changes to the terms of this License promises that they have read and understood these terms, that they have the authority to accept on your behalf and legally obligate You to this License. Under local law and treaties, the restrictions and limitations of this License may not apply to You; You may have other rights and remedies, and be subject to other restrictions and limitations.

U.S. GOVERNMENT RESTRICTED RIGHTS. UNPUBLISHED -- RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES. Use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth in FAR Section 52.227-14 Alt. III (g)(3), FAR Section 52.227-19, DFARS 252.227-7014 (b) or DFARS 227.7202, as amended from time to time. Contractor/Manufacturer is BMC Software, Inc., 2101 CityWest Blvd., Houston, TX 77042-2827, USA. Any contract notices should be sent to this address.

Notes



23663