NetIQ® AppManager® for Cisco Interactive Voice Response

Management Guide

February 2009

Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

© 2010 NetIQ Corporation. All rights reserved.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Check Point, FireWall-1, VPN-1, Provider-1, and SiteManager-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

ActiveAudit, ActiveView, Aegis, AppManager, Change Administrator, Change Guardian, Compliance Suite, the cube logo design, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowledge Scripts, NetConnect, NetIQ, the NetIQ logo, PSAudit, PSDetect, PSPasswordManager, PSSecure, Secure Configuration Manager, Security Administration Suite, Security Manager, Server Consolidator, VigilEnt, and Vivinet are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the USA. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

Contents

About this Book and the Library

The NetIQ AppManager product (AppManager) is a comprehensive solution for managing, diagnosing, and analyzing performance, availability, and health for a broad spectrum of operating environments, applications, services, and server hardware.

AppManager provides system administrators with a central, easy-to-use console to view critical server and application resources across the enterprise. With AppManager, administrative staff can monitor computer and application resources, check for potential problems, initiate responsive actions, automate routine tasks, and gather performance data for real-time and historical reporting and analysis.

Intended Audience

This guide provides information for individuals responsible for installing an AppManager module and monitoring specific applications with AppManager.

Other Information in the Library

The library provides the following information resources:

Installation Guide for AppManager

Provides complete information about AppManager pre-installation requirements and step-by-step installation procedures for all AppManager components.

User Guide for AppManager Control Center

Provides complete information about managing groups of computers, including running jobs, responding to events, creating reports, and working with Control Center. A separate guide is available for the AppManager Operator Console.

Administrator Guide for AppManager

Provides information about maintaining an AppManager management site, managing security, using scripts to handle AppManager tasks, and leveraging advanced configuration options.

Upgrade and Migration Guide for AppManager

Provides complete information about how to upgrade from a previous version of AppManager.

Management guides

Provide information about installing and monitoring specific applications with AppManager.

Help

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

The AppManager library is available in Adobe Acrobat (PDF) format from the NetIQ Web site: www.netiq.com/support/am/extended/documentation/default.asp?version=AMDocumentation.

About NetIQ Corporation

NetIQ, an Attachmate business, is a global leader in systems and security management. With more than 12,000 customers in over 60 countries, NetIQ solutions maximize technology investments and enable IT process improvements to achieve measureable cost savings. The company's portfolio includes award-winning management products for IT Process Automation, Systems Management, Security Management, Configuration Audit and Control, Enterprise Administration, and Unified Communications Management. For more information, please visit www.netiq.com.

Contacting Sales Support

For questions about products, pricing, and capabilities, please contact your local partner. If you cannot contact your partner, please contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, please contact our Technical Support team.

Worldwide:	www.netiq.com/Support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, please visit http://community.netiq.com.

1 Introducing AppManager for Cisco IVR

This chapter introduces AppManager for Cisco IP Interactive Voice Response (IVR), providing a brief overview of the module and its features and benefits.

1.1   Brief Overview

Cisco IVR is an IP-powered interactive voice response (IVR) solution that provides an open, extensible, and feature-rich foundation for the creation and delivery of IVR solutions via Internet Technology. Cisco IVR automates the handling of calls by autonomously interacting with users. The IVR processes user commands to facilitate command response features such as access to checking account information or user-directed call routing. IVR also performs "prompt and collect" functions to obtain user data such as passwords or account identification. Additionally, Cisco IVR can extract and parse Web-based content and present this data to customers via a telephony interface, thus facilitating the delivery of Web-maintained information to a voice media user. Designed to operate upon the Cisco AVVID (Architecture for Voice, Video and Integrated Data) architecture, Cisco IVR is constructed specifically to exercise the power of IP-based communications.

With AppManager for Cisco IVR, administrators charged with managing IVR gain access to a new set of tools they can leverage to gather a wide range of diagnostic and management data, which can help prevent outages and keep things running smoothly.

AppManager is designed to help you gain easy access to Cisco IVR data, and to help you analyze and manage that data. The AppManager for Cisco IVR solution minimizes the cost of maintaining an IP IVR system, aids in capacity planning, and can prevent downtime.

Like AppManager, IVR is designed to run on Windows 2000 systems, and uses Microsoft SQL and IIS servers and custom application services developed by Cisco Systems. AppManager can monitor and regulate all of the services and applications that are critical to IVR performance:

- Application Editor
- Application/CRA/CRS Engine
- Step libraries
- Flow repository
- Reporting tool

AppManager for Cisco IVR includes Knowledge Scripts to create jobs that monitor the health, availability, and performance of key services, applications, and the operating system. These scripts allow you to monitor and manage any or all of these crucial Cisco IVR services at a depth unparalleled by any other solution. Each Knowledge Script can be configured to send an alert, collect data for reporting and perform automated problem management when an event occurs.

By continuously monitoring critical Cisco IP IVR services, AppManager can keep you informed anytime something changes in your IP IVR system. For example, you can configure a Knowledge Script to send an email to an administrator if the Application Editor goes down. In addition, you can configure a Knowledge Script to use the AppManager agent to restart the service.

NOTE: For more information about the CiscoIVR Knowledge Scripts, see the AppManager Help for any specific script.

1.2 Features and Benefits

The following are just a few of the highlights of monitoring Cisco IVR with AppManager:

- Reduces the time that you spend diagnosing and resolving IP IVR issues
- Monitors and manages the entire Cisco IP IVR system, including the Application Editor and the Application/CRA/CRS Engine
- Automates system management issues that could affect IP IVR performance
- Pinpoints problems whether they originate at the hardware, operating system, or application level

2 Installing AppManager for Cisco IVR

This chapter provides installation instructions and describes system requirements for AppManager for Cisco IVR.

This chapter assumes you have AppManager installed. For more information about installing AppManager or about AppManager system requirements, see the *Installation Guide for AppManager*, which is available on the AppManager Documentation Web site: https://www.netiq.com/support/am/extended/documentation/default.asp.

2.1 System Requirements

AppManager for Cisco IVR has the following system requirements:

Software/Hardware	Version
NetIQ AppManager installed on the repository, agent, and console computers	7.0, at minimum
Cisco Interactive Voice Response	One of the following versions: ◆ 2.2.x ◆ 3.0.x ◆ 4.0.x ◆ 7.x

For the latest information about supported software versions and the availability of module updates, visit the AppManager Supported Products page at www.netiq.com/support/am/supportedproducts/default.asp. If you encounter problems using this module with a later version of your application, contact NetIQ Technical Support.

For more information about system requirements for the AppManager agent, repository, and management server, see the *Installation Guide for AppManager*.

2.2   Installing the Module

The setup program automatically identifies and updates all relevant AppManager components on a computer. Therefore, run the setup program only once on any computer. The pre-installation check also runs automatically when you launch the setup program.

You can install the module in one of the following ways:

- ◆ Run the module setup program, `<AM70-CiscoIVR-7.x.x.0.>.msi`, which you downloaded from the Web. Save the module setup files on the distribution computer, and then delete the older versions of the module setup files. For more information about the distribution computer, see the *Installation Guide for AppManager.*

- ◆ Use Control Center to install the module on the remote computer where an agent is installed. For more information, see Section 2.3, "Deploying the Module with Control Center," on page 12.

To install the module:

1 Run the module setup program on all AppManager repository (QDB) computers to install the Knowledge Scripts and reports.

- ◆ Run the setup program on the primary repository computer first. Then run the setup program on all other repository computers.

- ◆ For repositories running in active/active and active/passive clusters, run the setup program on the active node. Then, copy the following Registry key to the non-active node.

  `HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\AppManager\4.0`

2 Install the module on the Cisco IVR computer you want to monitor (agent computer). Use one of the following methods:

- ◆ Run the module setup program.

- ◆ Use Control Center to deploy the installation package.

3 Run the module setup program on all Operator Console and Control Center computers to install the Help and console extensions.

4 If you have not already discovered Cisco IVR resources, run the "Discovery_CiscoIVR" on page 33 Knowledge Script on all agent computers where you installed the module.

After the installation has completed, you can find a record of problems encountered in the `CiscoIVR_Install.log` file, located in the `\NetIQ\Temp\NetIQ_Debug\<ServerName>` folder.

2.3   Deploying the Module with Control Center

You can use Control Center to deploy the module on a remote computer where an agent is installed. This topic briefly describes the steps involved in deploying a module and provides instructions for checking in the module installation package. For more information, see the *Control Center User Guide for AppManager*, which is available on the AppManager Documentation Web site: https://www.netiq.com/support/am/extended/documentation/default.asp.

2.3.1   Deployment Overview

This section describes the tasks required to deploy the module on an agent computer.

To deploy the module on an agent computer:

1 Verify the default deployment credentials.

2 Check in an installation package.

3 Configure an email address to receive notification of a deployment.

4 Create a deployment rule or modify an out-of-the-box deployment rule.

5 Approve the deployment task.

6 View the results.

2.3.2 Checking In the Installation Package

You must check in the installation package, `AM70-CiscoIVR-7.x.x.0.xml`, before you can deploy the module on an agent computer.

To check in a module installation package:

1 Log on to Control Center and navigate to the Administration pane.

2 In the Deployment folder, select **Packages**.

3 On the Tasks pane, click **Check in Packages**.

4 Navigate to the folder where you saved `AM70-CiscoIVR-7.x.x.0.xml` and select the file.

5 Click **Open**. The Deployment Package Check in Status dialog box displays the status of the package check in.

2.4 Verifying Your Installed Module

To verify installation on many computers, run the ReportAM_CompVersion Knowledge Script. Ensure you discover a report-enabled agent before running this script. For more information, see the Help for the script.

To verify installation on one or only a few computers, use the Operator Console.

To verify your installed module with the Operator Console:

1 In the TreeView pane, select the computer for which you want to verify your installed module.

2 From the TreeView menu, select **Properties**. On the System tab, the System information pane displays the version numbers for all modules installed on the computer.

Verify that the version number from the *AppManager for Cisco IVR Readme* matches the version number shown in the System information pane.

2.5 Propagating Knowledge Script Changes

This release of AppManager for Cisco IVR may contain updated Knowledge Scripts. You can propagate script changes to jobs that are running and to Knowledge Script Groups, including recommended Knowledge Script Groups.

Before propagating script changes, verify that the script parameters are set to your specifications. Customized script parameters may have reverted to default parameters during the installation of the module. New parameters may need your attention.

You can propagate only properties (specified in the Schedule, Values, Actions, and Advanced tabs), only the script (which is the logic of the Knowledge Script), or both. Unless you know specifically that changes affect only the script logic, you should propagate both properties and the script.

For more information about propagating Knowledge Script changes, see the "Running Monitoring Jobs" chapter of the *Operator Console User Guide for AppManager*.

2.5.1 Propagating Changes to Running Jobs

You can propagate the properties and the logic of a Knowledge Script to running jobs started by that Knowledge Script. Corresponding jobs are stopped and restarted with the Knowledge Script changes.

To propagate changes to running Knowledge Script jobs:

1 In the Knowledge Script pane, select the Knowledge Script for which you want to propagate changes.

2 On the KS menu, select **Properties propagation**, and then select **Ad Hoc Jobs**.

3 Select the components of the Knowledge Script that you want to propagate to associated running jobs:

Select	To propagate
Script	The logic of the Knowledge Script.
Properties	The Knowledge Script properties, including schedule, monitoring values, actions, and advanced options.

4 Click **OK**.

2.5.2 Propagating Changes to Knowledge Script Groups

You can propagate the properties and logic of a Knowledge Script to corresponding Knowledge Script Group members.

After you propagate script changes to Knowledge Script Group members, you can propagate the updated Knowledge Script Group members to associated running jobs. For more information, see Section 2.5.1, "Propagating Changes to Running Jobs," on page 14.

To propagate Knowledge Script changes to Knowledge Script Groups:

1 In the Knowledge Script pane, select the Knowledge Script for which you want to propagate changes.

2 On the KS menu, select **Properties propagation**, and then select **Knowledge Script Group Members**.

3 Select the components of the Knowledge Script that you want to propagate to associated Knowledge Script Groups:

Select	To propagate
Script	The logic of the Knowledge Script.
Properties	The Knowledge Script properties, including schedule, monitoring values, actions, and advanced options.

4 Click **OK**.

2.6   Launching IVR Administration Web Pages

You can launch Cisco IVR administrative Web pages from the AppManager Operator Console.

To launch administrative Web pages:

1 In the TreeView pane, select the IVR resource for which you want to launch administrative Web pages.

2 On the Extensions menu, click Cisco IVR Administration.

3 Select the Web page that you want to launch and then click OK. The Web page is displayed in your Web browser.

3 Cisco IVR Knowledge Scripts

AppManager provides the following Knowledge Scripts for monitoring Cisco IVR resources. From the Knowledge Script view of Control Center, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help**. In the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
IIS_CpuHigh	Monitors CPU usage for IIS processes.
IIS_HealthCheck	Monitors the queue length for blocked I/O requests and the up-and-down status of IIS services and Web sites.
IIS_KillTopCPUProcs	Monitors the CPU usage of the dllhost and MTX processes. Can automatically stop a process that exceeds the threshold.
IIS_MemoryHigh	Monitors memory usage and memory pool usage for IIS application processes.
IIS_RestartServer	Restarts an IIS server.
IIS_ServiceUpTime	Monitors Web sites and Web services uptime.
IVR_CpuHigh	Monitors the CPU resource consumption for IVR processes.
IVR_EventLog	Scans the Event Log for Cisco IVR errors and status events.
IVR_HealthCheck	Monitors the status of Cisco IVR services. Can automatically restarts any service that is down.
IVR_MemoryHigh	Monitors the memory consumption for IVR processes. If a process is not found, it assumes that the process is not running, and reports zero as the memory result.
IVR_RestartService	Schedules an IVR service to stop and then restart after a specified interval.
IVR_SystemUsage	Monitors the CPU usage and memory for the Cisco IVR process and for system processes.
Report_ServicesAvailability	Summarizes the average availability of IVR services.
Report_SystemUsage	Summarizes the average CPU and memory usage per IVR server.
"Discovery_CiscoIVR" on page 33	Discovers Cisco IVR (Interactive Voice Response) resources and configuration.

3.1 IIS_CpuHigh

Use this Knowledge Script to monitor CPU usage for IIS application processes. This script raises an event if CPU usage exceeds the threshold you set. In addition, this script generates data streams for CPU usage.

3.1.1 Resource Object

CISCOIVR_IIST_Server

3.1.2 Default Schedule

By default, this script runs every five minutes.

3.1.3 Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Raise event if CPU usage exceeds threshold?	Set to **y** to raise an event if the threshold is exceeded. The default is y.
Collect data for CPU usage?	Set to **y** to collect data about CPU usage for reports and graphs. The default is n.
Process names	Sepcify the names of the application processes you want to monitor. Separate multiple entries with commas. For example: inetinfo,dllhost. The default is inetinfo. **NOTE**: Do not append .exe to the process names.
Threshold - Maximum CPU usage	Specify the maximum percentage of CPU resources the selected process can use before an event is raised. The default is 60%.
Event severity when CPU usage exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event inwhich CPU usage exceeds the threshold you set. The default is 8.

3.2 IIS_HealthCheck

Use this Knowledge Script to check IIS servers, Web site status, and the queue length for blocked I/O requests. This script raises an event if any server or Web site is not running. In addition, you can choose to automatically restart the IIS server or Web site. This script also raises an event if the blocked I/O queue length is longer than the specified threshold.

This script monitors only Web sites (servers), not FTP sites, NNTP sites, or SMTP sites.

3.2.1 Resource Objects

- CISCOIVR_IIST_Server
- CISCOIVR_IIST_FTPSRV

- CISCOIVR_IIST_W3SRV
- CISCOIVR_IIST_WebInst

3.2.2 Default Schedule

By default, this script runs every five minutes.

3.2.3 Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Auto-start monitored server(s)?	Set to **y** to automatically restart servers that are down. The default is y.
Event severity when auto-start fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which a server is down and AppManager cannot restart it. The default is 5.
Event severity when auto-start succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which a server was down and AppManager successfully restarted it. The default is 25.
Event severity when auto-start is set to "n"	Set the severity level, from 1 to 40, to indicate the importance of an event in which a server is down and AppManager has not been set to restart the service. The default is 18.
Event severity for blocked I/O requests	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the threshold is exceeded. The default is 5.
Threshold - Maximum blocked I/O requests	Specify the maximum queue length for blocked I/O requests. The default is 0 requests.
Monitor IIS server?	Set to **y** to monitor the IIS server. The default is y.
Monitor FTP server?	Set to **y** to monitor the FTP server. The default is n.

3.3 IIS_KillTopCPUProcs

Use this Knowledge Script to monitor the CPU usage for the IIS dllhost and mtx processes. This script raises an event if one or both processes exceed the CPU usage threshold you set. You can set this script to automatically stop a process that exceeds the CPU usage threshold.

3.3.1 Resource Object

CISCOIVR_IIST_Server

3.3.2 Default Schedule

By default, this script runs every three minutes.

3.3.3 Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Raise event if kill is successful or unsuccessful?	Set to **y** to raise an event when a process is successfully or unsuccessfully stopped. The default is y.
Kill CPU intensive processes?	Set to **y** to automatically stop any process that exceeds the threshold. The default is n.
Threshold - Maximum CPU usage	Specify the maximum percentage of CPU that can be used by the `dllhost` and `mtx` processes before an event is raised. The default is 90%.
Event severity when CPU usage exceeds threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which CPU usage exceeds the threshold you set. The default is 10.
Event severity when kill fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot stop a process. The default is 10.
Event severity when kill succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stops a process. The default is 20.

3.4 IIS_MemoryHigh

Use this Knowledge Script to monitor memory usage for IIS applications. This script raises an event if memory usage exceeds the threshold. In addition, this script generates data streams for memory usage.

3.4.1 Resource Object

CISCOIVR_IIST_Server

3.4.2 Default Schedule

By default, this script runs every five minutes.

3.4.3 Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Raise event if threshold is exceeded? ?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data about memory usage for reports and graphs. The default is n.

Parameter	How To Set It
Process names	Specify the names of the application processes you want to monitor. Use a comma to separate multiple entries — do not use spaces. For example: `inetinfo,dllhost`. The default is inetinfo. **NOTE**: Do not append .exe to the process names.
Threshold - Maximum memory usage	Specify the maximum amount of memory the selected process can use before an event is raised. The default is 10000000 bytes.
Threshold - Maximum memory pool usage	Specify the maximum amount of memory pool the selected process can use before an event is raised. The default is 5000000 bytes.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 8.

3.5 IIS_RestartServer

Use this Knowledge Script to restart an IIS server. This script raises an event if the server either successfully restarts or fails to restart.

3.5.1 Resource Object

CISCOIVR_IIST_Server

3.5.2 Default Schedule

By default, this script runs once.

3.5.3 Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Wait N seconds before restarting	Specify the number of seconds to wait after the server is stopped before attempting to automatically restart the server. The default is 5 seconds.
Event severity when stop fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot stop the server. The default is 5.
Event severity when restart fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot restart the server. The default is 5.
Event severity when status of server is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot determine the status of the server. The default is 10.
Event severity when stop succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stops the server. The default is 25.

Parameter	How To Set It
Event severity when restart succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully restarts the server. The default is 25.

3.6 IIS_ServiceUpTime

Use this Knowledge Script to monitor the uptime for Web sites and services. This script raises an event if the amount of time the sites and services are running is less than the threshold you set. In addition, this script generates data streams for uptime.

NOTE: This script supports IIS version 5 and later.

3.6.1 Resource Objects

- ◆ CISCOIVR_IIST_WebInst
- ◆ CISCOIVR_IIST_FTPInst

3.6.2 Default Schedule

By default, this script runs every hour.

3.6.3 Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Raise event if uptime falls below threshold?	Set to **y** to raise an event when uptime falls below the threshold. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. If set to y, the script returns how long a service has been running. The default is n.
Threshold - Minimum uptime	Specify the minimum amount of time that discovered Web sites, Web services, FTP sites, and FTP services are required to be up during any interval to prevent an event from being raised. If the sites and services up time is less than this threshold, an event is raised. The default is 10000 seconds.
Event severity when uptime falls below threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which uptime falls below the threshold. The default is 5.

3.7 IVR_CpuHigh

Use this Knowledge Script to monitor the CPU resource consumption for IVR processes. This script raises an event if CPU utilization exceeds the thresholds you set. The script monitors CPU usage for each IVR process and the total CPU usage for all processes. If a process is not found, the script assumes that the process is not running and reports zero as the CPU result.

3.7.1 Resource Object

CISCOIVR

3.7.2 Default Schedule

By default, this script runs every 15 minutes.

3.7.3 Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for graphs and reports. The default is n.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 15.
Threshold - Maximum CPU usage for Cisco Application/CRA/CRS Engine	Specify the maximum amount CPU that can be used by the Cisco Application/CRA/CRS Engine before an event is raised. Set to **0** if you do not want to monitor this process. The default is 20%.
Threshold - Maximum CPU usage for Cisco AVVID Alarm Service	Specify the maximum CPU usage for Cisco AVVID Alarm Service that can be detected before an event is raised. Set to **0** if you do not want to monitor this process. The default is 20%
Threshold - Maximum CPU usage for Cisco Syslog Collector	Specify the maximum CPU usage for Cisco Syslog Collector that can be detected before an event is raised. Set to **0** if you do not want to monitor this process. The default is 20%.

3.8 IVR_EventLog

Use this Knowledge Script to monitor the event log entries from Cisco IVR during the past *n* hours. This script raises an event if log entries are detected. In addition, this script generates datastreams for log entries.

3.8.1 Resource Object

CISCOIVR

3.8.2 Default Schedule

By default, this script runs every 10 minutes.

3.8.3 Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Raise event for log entries?	Set to **y** to raise an event when the log contains entries for which you have filtered. The default is y.
Collect data?	Set to **y** to collect data about log entries for charts and graphs. The default is n.
Separate data?	Set to **y** to separate events entries from different log files into different data streams. If set to **n**, all event entries matching your filtering criteria are placed in the same data stream and the data detail message may include event entries from multiple log sources. The default is n. For example, if you are monitoring both the System and Application logs, you may want to set this parameter to **y** so that events in the System log are tracked separately from events in the Application log.
Log source	Specify the event log you want to monitor. Separate multiple entries by commas. For example: `System,Application`. The default is Application.
Events in past N hours	Enter the number of hours of log file entries through which the script will search for events that match the criteria you specify. For instance, if you enter 15, then the script will search through the last 15 hours of log file entries. If you enter **0** (which is the default), no past events are looked at during the first iteration of the Knowledge Script job. During subsequent iterations, the script will look through and filter only the new events that have been created in the Windows event log.
Type: Error	Set to y to monitor for error events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for the Collect data? parameter. The default is y.
Type: Warning	Set to y to monitor for warning events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for the Collect data? parameter. The default is y.
Type: Information	Set to y to monitor for information events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for the Collect data? parameter. The default is n.
Type: Success Audit	Set to y to monitor for success audit events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for the Collect data? parameter. The default is n.
Type: Failure Audit	Set to y to monitor for failure audit events. If you set to n, this entry does not raise an event, is not returned in an event detail message, and is not collected as data if you specified y for the Collect data? parameter. The default is n.

Parameter	How To Set It

Instructions for filters: To limit the types of entries that raise events and the type of data that is collected, enter a search string that filters the following fields in the event log. The search string can contain criteria used to include entries, exclude entries, or both.·

- ◆ Separate include and exclude criteria with a colon (:). For example, `net:logon`.

- ◆ Separate multiple include or exclude entries with commas. For example, `finance,sales:corp00,HQ`.

- ◆ If you are specifying only include criteria, the colon is not necessary. For example, `SQL`.

- ◆ If you are specifying only exclude criteria, start the search string with a colon. For example, `:defragmentation,cleanup`.

Parameter	How To Set It
Event source filter	Specify one or more text strings to look for; separate multiple strings with commas. If your valid text string includes a comma, replace the comma with a tilde. For example: `Cisco Systems~ Inc. CRS` The Knowledge Script will convert the tilde to a comma at runtime.
Event category filter	Specify one or more text strings to look for; separate multiple strings with commas.
Event ID filter	Specify a single event ID or a range of event IDs; separate multiple entries by commas. For example: `1094,1404-1463`
Event user filter	Specify a single or multiple user names to look for; separate multiple entries by commas. For example: `Pat,Chris,Alex`
Computer filter	Specify a single or multiple computer names to look for; separate multiple entries by commas. For example: `SHASTA,MARS`
Event description filter	Specify a detail description or keywords in the description. The string can contain spaces, underscores, and periods; separate multiple entries with commas. For example: `data loss during system failures,corrupt indices,Inter-Site Transport objects failed`
Threshold - Maximum number of entries per event report	Specify the maximum number of Application log events that can be returned in each event report. For example, if this value is set to 30 and 67 Application log events are found, then three event reports are raised: two reports containing 30 events and one report containing seven events. The default is 30. The Message column on the **Events** tab in the Operator Console displays the number of events in each event report, the type of log the events are from, and the event report batch number. The batch number is the sequential number of the event report. Batch numbers start at 1 for each Knowledge Script iteration.
Event severity for log entries	Set the event severity level, from 1 to 40, to indicate the importance of an event in which log entries are detected. You may want to adjust the severity depending on the types of events for which you are checking. The default is 15.

3.9 IVR_HealthCheck

Use this Knowledge Script to monitor Cisco IVR services. This script raises an event if any service is not running, and can automatically re-start any service that is not running. To make the most of the data collected by this script, run Report_ServicesAvailability.

3.9.1 Using Recommended Knowledge Scripts

This script is a member of the CiscoIVR Recommended Knowledge Script Group (KSG). As part of a KSG, these scripts have their parameters already set to recommended values. To run all of the recommended scripts at one time, click the RECOMMENDED tab and then run the **CiscoIVR** group on a Cisco IVR resource.

- IVR_HealthCheck
- IVR_SystemUsage

3.9.2 Resource Object

CISCOIVR

3.9.3 Default Schedule

By default, this script runs every minute.

3.9.4 Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Collect data?	Set to **y** to collect data for reports and graphs. The default is y.
Auto-start monitored services?	Set to **y** to auto-start any of the services that you choose to monitor. The default is y.
Event severity when auto-start fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and AppManager cannot restart it. The default is 5.
Event severity when auto-start succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service was down and AppManager successfully restarted it. The default is 25.
Event severity when auto-start is set to "n"	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a service is down and AppManager has not been set to restart the service. The default is 18.
Event severity when service does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a monitored service does not exist. The default is 15.
Monitor the Cisco Application/CRA/CRS Engine service?	Set to **y** to monitor the Cisco Application/CRA/CRS Engine service. The default is y.

Parameter	How To Set It
Monitor the Cisco AVVID Alarm service?	Set to **y** to monitor the Cisco AVVID Alarm service. The default is y.
Monitor the Cisco Syslog Collector service?	Set to **y** to monitor the Cisco Syslog Collector service. The default is n.

3.10 IVR_MemoryHigh

Use this Knowledge Script to monitor the memory consumption for IVR processes. This script checks the memory used by each IVR process individually, and the total memory used by all processes. If a process is not found, the script assumes that the process is not running, and reports zero as the memory result.

This script raises an event if any value exceeds the threshold you set.

3.10.1 Resource Object

CISCOIVR

3.10.2 Default Schedule

By default, this script runs every five minutes.

3.10.3 Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for graphs and reports. The default is n.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 15.
Monitor Cisco Application/CRA/CRS Engine memory usage?	Set to **y** to monitor the memory usage of the Cisco Application/CRA/CRS Engine. The default is y.
Threshold - Maximum memory usage for Cisco Application/CRA/CRS Engine	Specify the maximum amount of memory that can be used by the Cisco Application/CRA/CRS Engine before an event is raised. The default is 200000 KB.
Threshold - Maximum memory pool usage for Cisco Application/CRA/CRS Engine	Specify the maximum amount of memory pool that can be used by the Cisco Application/CRA/CRS Engine before an event is raised. The default is 5000 KB.
Monitor Cisco AVVID Alarm Service memory usage?	Set to **y** to monitor the memory usage of Cisco AVVID Alarm Service. The default is y.
Threshold - Maximum memory usage for Cisco AVVID Alarm Service	Specify the maximum amount of memory that can be used by the Cisco AVVID Alarm Service before an event is raised. The default is 200000 KB.

Parameter	How To Set It
Threshold - Maximum memory pool usage for Cisco AVVID Alarm Service	Specify the maximum amount of memory pool that can be used by the Cisco AVVID Alarm Service before an event is raised. The default is 5000 KB.
Monitor Cisco Syslog Collector memory usage?	Set to **y** to monitor the memory usage of Cisco Syslog Collector. The default is y.
Threshold - Maximum memory usage for Cisco Syslog Collector	Specify the maximum amount of memory that can be used by the Cisco Syslog Collector before an event is raised. The default is 200000 KB.
Threshold - Maximum memory pool usage for Cisco Syslog Collector	Specify the maximum amount of memory pool that can be used by the Cisco Syslog Collector before an event is raised. The default is 5000 KB.

3.11   IVR_RestartService

Use this Knowledge Script to schedule an IVR service to stop and then restart after a specified interval. This script raises an event when a stop or restart fails, when service status is unavailable, and when a stop or restart succeeds.

3.11.1   Resource Object

CISCOIVR

3.11.2   Default Schedule

By default, this script runs every hour.

3.11.3   Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Collect data?	Set to **y** to collect data for graphs and reports. The default is n.
Wait N seconds before restarting	Specify the number of seconds that should elapse before the service is restarted. The default is 5 seconds.
Event severity when stop fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot stop the service. The default is 5.
Event severity when restart fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot restart the service. The default is 5.
Event severity when status of service is unavailable	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager cannot determine the status of the service. The default is 10.
Event severity when stop succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully stops the service. The default is 25.

Parameter	How To Set It
Event severity when restart succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which AppManager successfully restarts the service. The default is 25.
Restart Cisco Application/CRA/CRS Engine service?	Set to **y** to restart the Cisco Application/CRA/CRS Engine. The default is y.
Restart Cisco AVVID Alarm service?	Set to **y** to restart the Cisco AVVID Alarm. The default is n.
Restart Cisco Syslog Collector service?	Set to **y** to restart the Cisco Syslog Collector. The default is n.

3.12   IVR_SystemUsage

Use this Knowledge Script to monitor CPU usage and memory for the Cisco IVR process. This script raises an event if a threshold is exceeded. To make the most of the data collected by this script, run Report_SystemUsage.

3.12.1   Using Recommended Knowledge Scripts

This script is a member of the CiscoIVR Recommended Knowledge Script Group (KSG). As part of a KSG, these scripts have their parameters already set to recommended values. To run all of the recommended scripts at one time, click the RECOMMENDED tab and then run the **CiscoIVR** group on a Cisco IVR resource.

- ◆ IVR_HealthCheck
- ◆ IVR_SystemUsage

3.12.2   Resource Object

CISCOIVR

3.12.3   Default Schedule

By default, this script runs every five minutes.

3.12.4   Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Raise event if threshold is exceeded?	Set to **y** to raise an event if a threshold is exceeded. The default is y.
Collect data?	Set to **y** to collect data for reports and graphs. The default is y.
Event severity when threshold is exceeded	Set the severity level, from 1 to 40, to indicate the importance of an event in which a threshold is exceeded. The default is 15.
Threshold - Maximum IVR server CPU usage	Specify the maximum amount of IVR CPU that can be in use before an event is raised. The default is 75%.

Parameter	How To Set It
Threshold - Maximum total CPU usage	Specify the maximum amount of total CPU that can be in use before an event is raised. The default is 90%.
Threshold - Maximum IVR server memory usage	Specify the maximum amount of IVR memory that can be in use before an event is raised. The default is 75%.
Threshold - Maximum total memory usage	Specify the maximum amount of total memory that can be in use before an event is raised. The default is 90%.

3.13   Report_ServicesAvailability

Use this Knowledge Script to summarize the average availability of each IVR service within a time frame that you specify. This script uses the data collected by the IVR_HealthCheck script.

3.13.1   Using Recommended Knowledge Scripts

This script is a member of the CiscoIVR Recommended Knowledge Script Group (KSG). As part of a KSG, these scripts have their parameters already set to recommended values. To run all of the recommended scripts at one time, click the RECOMMENDED tab and then run the **CiscoIVR_Report** group on a Report agent.

- ◆ Report_ServicesAvailability
- ◆ Report_SystemUsage

3.13.2   Resource Object

Report agent

3.13.3   Default Schedule

By default, this script runs once.

3.13.4   Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Data Source	
Select data wizard	Select which computers to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Select Knowledge Script(s)	Select the Knowledge Scripts that you want to include in the report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Report Settings	

Parameter	How To Set It
Decimal accuracy for % values	Specify the number of decimal places that you want to see in the values displayed in this report. The default is 3.
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of data stream values in the report. The default is y.
Include chart?	Set to **y** to include a chart of data stream values in the report. The default is y.
Select chart style	Define the graphic properties for the charts in your report. The default style is Bar.
Select output folder	Set parameters for the output folder. The default folder name is CiscoIVRServicesAvailability.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n.
	The job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set the report properties as desired. The default report name is Cisco IVR Services Availability.
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated.
	Adding a time stamp is useful for running consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report is successful?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report is successful. The default is 35.
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of an event in which the report fails. The default is 5.

3.14   Report_SystemUsage

Use this Knowledge Script to summarize the average CPU and memory usage per IVR server within a time frame that you specify. This script uses the data collected by the IVR_SystemUsage script.

3.14.1   Resource Object

Report agent

3.14.2 Default Schedule

By default, this script runs once.

3.14.3 Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Data Source	
Select data wizard	Select the computers that you want to include in the report. You can select computers by category: View, Server Group, or Computer. The default is View.
Select Knowledge Script(s)	Select the Knowledge Scripts that you want to include in the report.
Select time range	Select a **Specific** or **Sliding** date/time range from which the report should pull data. The default is Sliding.
Charts	
Include % CPU chart?	Set to **y** to include a chart that details the CPU usage for the selected cluster. The default is y.
Include memory usage chart?	Set to **y** to include a chart that details the memory usage for the selected cluster. The default is y.
% CPU chart threshold	Specify the CPU percentage threshold to display on the charts in the report. The default is 0%.
Memory usage chart threshold	Specify the physical memory threshold to display on the charts in the report. The default is 0 KB.
Chart size	Select the size of the rendered chart. Choose from Large, Medium, and Small. The default is Medium.
Chart color scheme	Select a color scheme template. The default is NetIQ1.
Report Settings	
Include parameter help card?	Set to **y** to include a table in the report that lists parameter settings for the report script. The default is y.
Include table?	Set to **y** to include a table of information in the report. The default is y.
Select output folder	Locate and select the output folder. The default folder name is CiscoIVRSystemUsage.
Add job ID to output folder name?	Set to **y** to append the job ID to the name of the output folder. The default is n.
	The job ID is helpful for making the correlation between a specific instance of a Report script and the corresponding report.
Select properties	Set the report properties as desired. The default report name is Cisco IVR System Usage.

Parameter	How To Set It
Add time stamp to title?	Set to **y** to append a time stamp to the title of the report, making each title unique. The default is n. The time stamp is made up of the date and time the report was generated.
	Adding a time stamp is useful for running consecutive iterations of the same report without overwriting previous output.
Event Notification	
Raise event when report is successful?	Set to **y** to raise an event when the report is successfully generated. The default is y.
Event severity when report succeeds	Set the severity level, from 1 to 40, to indicate the importance of the event when the report is successful. The default is 35.
Event severity for report with no data	Set the severity level, from 1 to 40, to indicate the importance of the event when the report contains no data. The default is 25.
Event severity when report fails	Set the severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

3.15 Discovery_CiscoIVR

Use this Knowledge Script to discover Cisco IVR resources and configuration for Cisco IVR versions 4.x and earlier.

3.15.1 Resource Object

NT_MachineFolder

3.15.2 Default Schedule

By default, this script runs once.

3.15.3 Setting Parameter Values

Set the following parameters as necessary:

Parameter	How To Set It
Raise event if discovery succeeds	This script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event if the job succeeds. The default is y.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery succeeds. The default is 25.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery fails. The default is 5.
Event severity when discovery partially succeeds	Set the event severity level, from 1 to 40, to reflect the importance of an event in which discovery returns some data but also generates warning messages. The default is 10.

4 Using the Module Effectively

This chapter provides details about functions within AppManager that are unique to monitoring Cisco IVR. Review the following topics to improve your management of critical services.

- Section 4.1, "Launching IVR Administration Web Pages," on page 35
- Section 4.2, "Using Monitoring Policies," on page 35
- Section 4.3, "Using Recommended Knowledge Scripts," on page 35

NOTE: For information about using AppManager for non-IVR-specific functions, see the AppManager *User Guide*.

4.1 Launching IVR Administration Web Pages

You can launch Cisco IVR administrative Web pages from the AppManager Operator Console.

To launch administrative Web pages:

1 In the TreeView pane, select the IVR resource for which you want to launch administrative Web pages.

2 Click Extensions > Cisco IVR Administration. The Select the Cisco IVR Administration application dialog box is displayed.

3 Select the Web page that you want to launch and then click OK. The Web page is displayed in your Web browser.

4.2 Using Monitoring Policies

A monitoring policy uses a set of pre-configured Knowledge Scripts, such as the group of recommended scripts for Cisco IVR, to automatically monitor resources as they appear in the TreeView. With a monitoring policy, you can efficiently and consistently monitor all of the resources in your environment.

If you use monitoring policies for your Knowledge Script jobs, ensure that the `sqlserveragent` service is running. Monitoring policies use SQL jobs to ensure that all monitoring policies have the environments they need in order to run properly.

For more information about monitoring policies, see the AppManager *User Guide*.

4.3 Using Recommended Knowledge Scripts

NetIQ recommends using at least the following Knowledge Scripts to ensure optimal monitoring of Cisco IVR processes. For more information about these and other Knowledge Scripts, see the AppManager Help for any particular script.

4.3.1 Monitoring Scripts

You can find these scripts in a group on the RECOMMENDED tab of the Knowledge Script pane, or individually on the CiscoIVR tab.

- IVR_HealthCheck. Monitors the status of Cisco IVR services and automatically restarts any service that is down.
- IVR_SystemUsage. Monitors the CPU usage and memory for the Cisco IVR process and for system processes.

As part of a Knowledge Script group, these scripts have their parameters already set to recommended values. To run all of the recommended scripts at one time, simply click on the RECOMMENDED tab, and then drag and drop the **CiscoIVR** group onto an IVR resource in the TreeView pane.

4.3.2 Report Scripts

You can find these scripts in a group on the RECOMMENDED tab of the Knowledge Script pane, or individually on the CiscoIVR tab.

- Report_ServicesAvailability. Displays the average availability of IVR-related services.
- Report_SystemUsage. Displays average CPU and memory usage.

As part of a Knowledge Script group, these scripts have their parameters already set to recommended values. To run all of the recommended scripts at one time, simply click on the RECOMMENDED tab, and then drag and drop the **CiscoIVR_Reports** group onto a Report Agent in the TreeView pane.