nAppliance
application protection & acceleration

Resonate CD on IAG
Installation Guide

Release 12/03/2008

Version 1.0.3

NAPPLIANCE APPLIANCE END USER AGREEMENT

CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS. BY INSTALLING AND USING SOFTWARE AND HARDWARE INCLUDED WITH THE NAPPLIANCE APPLIANCE, YOU (THE 'END USER') ARE AGREEING TO BE BOUND BY THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, IMMEDIATELY RETURN THE NAPPLIANCE APPLIANCE TO NAPPLIANCE INC.

1. CERTAIN DEFINITIONS

1. "NAppliance Appliance" means the NAppliance hardware and software that includes, without limitation: licensed software, hardware, support, and professional services.

2. "Open Source Software" means software included in the NAppliance Appliance which is licensed and made available under the terms and conditions of the GNU General Public License version 2.

3. "Licensed Software" means NAppliance Proprietary Software and Open Source Software together.

4. "NAppliance Proprietary Software" means NAppliance proprietary software that may be included in the NAppliance Appliance, including enhancements, updates, bug fixes and upgrades thereto that may be provided to End User from time to time**.**

2. LICENSE

(a) License Grant. Subject to full payment of all applicable fees and to the terms of this end user agreement (the "Agreement"), NAppliance hereby grants to End User, a non-transferable, non-exclusive license to use the Licensed Software and related product documentation (the "Documentation") with the NAppliance Appliance for the duration of the Agreement. This license allows the End User to install the NAppliance Appliance on a network supporting the number of active nodes specified by the NAppliance Appliance Purchase Agreement. NAppliance shall have the right to conduct audits periodically upon advance notice to verify compliance with the terms of this Agreement.

(b) License Restrictions. End User may use the Licensed Software solely with the NAppliance Appliance. Except as otherwise permitted by the GNU General Public License version 2, End User agrees not to modify, translate, reverse engineer, de-compile or disassemble the Licensed Software; or to create derivative works based on the Licensed Software.

(c) Other Restrictions. End User agrees to safeguard copies of the Licensed Software against disclosure, copying or use by unauthorized persons. End User agrees that it will not use, or allow use of, the NAppliance Appliance for any improper purpose (including without limitation, testing the integrity of any network other than those it is authorized to test). End User agrees that it will not, and will not allow, reverse engineering of the hardware included in the NAppliance Appliance. End User shall ensure that the provisions of this Agreement are not violated by End User's employees, contractors or agents. End User agrees to indemnify NAppliance for any third party claims related to the breach of this or any other provision of this Agreement by End User, its agents, contractors, or employees.

(d) Open Source Software. The use distribution and modification of Open Source Software is governed by the terms and conditions of the GNU General Public License version 2 which can be viewed at http://gnu.org and which is hereby incorporated by reference. Copies of the source code for Open Source Software may be obtained by contacting NAppliance via email at source@NAppliance.com. NAppliance may charge End User a fee equal to its cost for copying and distributing such source code. Nothing in this Agreement is meant to modify or supercede any terms and conditions of the GNU General Public License version 2 and if there is a conflict between the Agreement and the GNU General Public License version 2, the terms of the GNU General Public License version 2 shall control.

3. TITLE

End User acknowledges and agrees that all right, title and interest in the Licensed Software and Documentation, including all intellectual property rights therein, is retained by NAppliance or its suppliers, subject only to the license granted to End User hereunder. This license is not a sale and does not transfer to End User any title or ownership in or to the Licensed Software or the Documentation.

4. MAINTENANCE

End User shall have the option of purchasing maintenance services from NAppliance for a fee. Maintenance may include the following:

(a) Software Updates. Software updates will be provided by NAppliance at its sole discretion to End User from time to time. Updates may include software enhancements, upgrades, minor updates, and bug fixes.

(b) Hardware Repair or Replacement. For End Users purchasing maintenance services, NAppliance will use commercially reasonable efforts to repair or replace defective hardware within two (2) business days in accordance with the terms of the hardware warranty set forth in Section 4 (b) of this Agreement. End User is responsible for returning defective hardware to NAppliance within seven (7) days of receipt of replacement hardware. If NAppliance does not receive returned defective hardware within seven days NAppliance may charge End User the cost of the replacement hardware, such charges to be invoiced by NAppliance to End User in accordance with Section 7.

(c) Support. NAppliance will provide phone and email support to End Users Monday-Friday between 7:00 a.m. and 5:00 p.m. Pacific Time. NAppliance will use commercially reasonable efforts to reply to support requests within one (1) business day.

(d) Technical Support Incidents. End Users who purchase maintenance are entitled to twelve (12) technical support incidents per year. Support for technical support incidents above twelve (12) per year will be provided on a time and materials basis.

(e) Bug Fixes. The discovery of errors in the NAppliance Appliance ("Bugs") by End user shall not be deemed a technical support incident. Bugs should be promptly reported via email by End User to NAppliance at bugs@NAppliance.com. NAppliance will use commercially reasonable efforts to fix Bugs in a timely manner.

(f) Other Technical Support. Additional technical support services are available, at NAppliance's discretion, on a time and materials basis.

5. LIMITED WARRANTY

(a) Software. NAppliance warrants to End User only that the media on which the Licensed Software is recorded shall be free from defects in materials and workmanship under normal use for a period of ninety (90) days from the date of shipment by NAppliance. End User's sole and exclusive remedy, and NAppliance's sole and exclusive liability, shall be replacement of the media in accordance with this limited warranty.

(b) Hardware.

(i) Limited Warranty. NAppliance warrants only to End User that hardware furnished to End User under this Agreement will be free from defects in materials and workmanship for a period of ninety (90) days following shipment by NAppliance. NAppliance's sole and exclusive liability and End User's sole and exclusive remedy under this section 5(b) is to, at NAppliance's sole discretion, repair or replace without charge any non-conforming hardware. NAppliance shall repair or replace such hardware within a reasonable time period. Returned hardware and parts shall become NAppliance's property. End User agrees to assist NAppliance in identifying the circumstances under which the hardware failed.

(ii) Warranty Exclusions. The warranty under this section 5(b) does not apply to any hardware that has been subjected by End User or a third party to: (a) operating or environmental conditions contrary to NAppliance's specifications, (b) damage, misuse or neglect, (c) improper installation, repair or alteration, (d) modifications, other than by NAppliance, or (e) third party software, firmware or hardware that interferes with operation of such hardware. This warranty also excludes expendable items, such as fuses or other similar parts that fail from normal use.

(c) WARRANTY DISCLAIMER.

(i) THE LICENSED SOFTWARE AND DOCUMENTATION IS PROVIDED "AS IS." EXCEPT FOR THE LIMITED WARRANTIES GRANTED IN SECTIONS 5 (a)

AND (b), NAPPLIANCE EXPRESSLY DISCLAIMS AND NEGATES ALL WARRANTIES FOR THE NAPPLIANCE APPLIANCE, WHETHER EXPRESSED, IMPLIED, STATUTORY OR OTHERWISE, AND NAPPLIANCE SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT OF INTELLECTUAL PROPERTY OR OTHER VIOLATION OF RIGHTS. NAPPLIANCE DOES NOT WARRANT THAT THE NAPPLIANCE APPLIANCE WILL MEET END USER'S REQUIREMENTS OR THAT THE OPERATION OF THE LICENSED SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE.

(iii) Some states or countries do not allow exclusion or limitation of incidental or consequential damages or limitation on how long an implied warranty lasts, so the above limitations or exclusions may not apply to End User. This warranty gives End User specific legal rights and End User may also have other rights, which vary from state to state or country to country.

6. LIMITATION OF LIABILITY AND DAMAGES

(a) IN NO EVENT SHALL NAPPLIANCE, ITS SUPPLIERS OR ITS DISTRIBUTORS BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGE, INCLUDING WITHOUT LIMITATION, LOSS OF DATA, LOST PROFITS OR COST OF COVER ARISING FROM THE USE OF THE NAPPLIANCE APPLIANCE, OR ANY DEFECT IN THE NAPPLIANCE APPLIANCE, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY. THIS LIMITATION SHALL APPLY EVEN IF NAPPLIANCE, ITS SUPPLIERS OR ITS DISTRIBUTOR SHALL HAVE BEEN ADVISED OF THE POSSIBILITY OF ANY SUCH DAMAGE. IN PARTICULAR, BUT WITHOUT LIMITATION, NAPPLIANCE, ITS SUPPLIERS AND ITS DISTRIBUTORS SHALL HAVE NO LIABILITY FOR THE LOSS OF ANY INFORMATION STORED OR COMMUNICATED OR ATTEMPTED TO BE STORED

OR COMMUNICATED WITHIN ANY SYSTEM USING THE LICENSED SOFTWARE.

(b)THE MAXIMUM AGGREGATE LIABILITY OF NAPPLIANCE AND ITS SUPPLIERS FOR ANY CLAIM ARISING OUT OF USE OF THE NAPPLIANCE APPLIANCE, OR ANY DEFECT IN THE NAPPLIANCE APPLIANCE, ON ANY AND ALL THEORIES OF LIABILITY, INCLUDING WITHOUT LIMITATION NEGLIGENCE BY NAPPLIANCE, SHALL IN ALL EVENTS BE LIMITED TO RETURN OF THE AMOUNTS ACTUALLY PAID TO NAPPLIANCE FOR THE DEFECTIVE LICENSED SOFTWARE OR HARDWARE, LESS DEPRECIATION OF SUCH AMOUNTS LINEARLY OVER A THREE-YEAR PERIOD, WHICH THE PARTIES AGREE CONSTITUTES A REASONABLE RATE OF DEPRECIATION.

7. FEES

End User shall pay to NAppliance the fees for the NAppliance Appliance in effect at the applicable delivery date requested by End User in accordance with the NAppliance Appliance Purchase Agreement, and NAppliance shall invoice End User for all such fees. NAppliance may increase fees at its discretion, provided that fee increases will not be effective until 30 days after notice to End User. All payments due hereunder to NAppliance shall be paid to NAppliance not later than thirty (30) days following the date of the applicable invoice. In addition to the fees, End User will pay all charges, including without limitation transportation charges, insurance premiums, and shall be responsible for all taxes (except NAppliance’s U.S. income taxes), duties, costs of compliance with export and import controls and regulations, and other governmental assessments.

8. TERMINATION

This agreement shall continue in effect until terminated hereunder. This Agreement may be terminated by NAppliance upon 30 days notice to End User. This Agreement shall terminate automatically if End User fails to pay fees when due and such failure is not remedied within fifteen days of the original payment due date. In addition, this agreement shall terminate automatically on End User's failure to comply with any of the restrictions and provisions herein, including without limitation any attempt to transfer this license. Upon any termination of this agreement, End User agrees promptly to destroy or return to NAppliance all copies of the Licensed Software and Documentation, including without limitation all original and archival copies thereof. No refunds shall be given for such returned materials. Notwithstanding any termination of this License, the rights and obligations set forth in section 3 (Title), section 5 (Limited Warranty), section 6 (Limitation of Liability and Damages), section 7 (Fees), section 8 (Termination) and section 9 (Miscellaneous) shall survive such termination.

9. MISCELLANEOUS

End User may not assign this Agreement without the consent of NAppliance. Any attempted assignment by End User shall be null and void. NAppliance may freely assign this Agreement. No delay, failure or waiver by either party to exercise any right or remedy under this Agreement shall operate to limit, preclude, cancel or waive any exercise of such right or remedy or the exercise of any other right or remedy. This Agreement shall be governed by and construed in accordance with the laws of the State of California without regard to conflict of laws principles or the United Nations 1980 Convention on Contracts for the International Sale of Goods. The federal and state courts of California shall have exclusive jurisdiction and venue to adjudicate any dispute arising out of this Agreement, and End User expressly consents to the personal jurisdiction of the state and federal courts of California .If any provision in this Agreement shall be found or be held to be invalid or unenforceable in any jurisdiction in which this Agreement is being performed, it shall not affect the validity of the remaining portions of the Agreement. This Agreement constitutes the entire agreement between the parties and supercedes any prior agreement, whether written or oral, relating to the subject matter of this Agreement.

TABLE OF CONTENTS

About This Guide

Document Objectives

This document describes the installation and configuration of the Resonate Central Dispatch system layered over the Microsoft Intelligent Application Gateway product.

Audience

This guide is for the IT administrators which are managing the nAppliance mIAG products with the Resonate Load Balancer options.

Feedback

nAppliance Networks appreciates any comments, complaints or suggestions. Your opinion on what is right or wrong with this document is very helpful. You can contact nAppliance directly via email at:

support@nAppliance.com

Please include the document name and version.

Chapter 1: Introduction

The Resonate Central Dispatch ™ is a software based Network Load Balancer product which provides:

- High Availability for the nAppliance mIAG products: Resonate Central Dispatch™ monitors the IAG systems, and when an IAG system fails, will automatically redirect traffic to the companion nodes.
- Load Balancing of traffic: Resonate Central Dispatch™ spreads network traffic among the IAG node cluster. Resonate CD by default will distribute traffic based on CPU usage and number of connections.
- Centrally managed – The Resonate CD manager software client can be installed on a central non-IAG system. The CD Manager configures and monitors the nodes within the cluster.

Chapter 2: Operation

The Resonate CD system is layered in front of the ISA/IAG applications, so there is no direct integration between Resonate CD and ISA or IAG. The configurations required to install Resonate CD are:

- ISA Access Rules – Resonate CD must maintain network communications with each of the other Resonate CD nodes in a cluster, so ISA access rules must be applied to allow this network traffic.
- Users interact with the IAG nodes via a VIP (Virtual IP address), so the IAG trunks must be configured with the DNS node name of the VIP address instead of the IAG External IP address.
- The IAG nodes interface with the end clients via the VIP address instead of the External IP address, so the ISA firewall needs to be configured to allow communications using the VIP address.

Traffic Flow

Resonate CD sits on the outer edge of the network interfaces, and processes the traffic before passing it to the ISA Firewall. The ISA firewall processes the network traffic then hands this to the IAG system. The IAG system will process the traffic, then pass this to the published applications.

User Client ←→ Resonate CD ←→ ISA ←→ IAG ←→ App Server

The following sections will describe this and other configurations required to install and manage the Resonate CD system in an IAG environment.

Resonate CD Components

CD Master – The CD Master is the management software which will run on one or more nodes. This software can run on a node in the cluster, or run on a separate server used for management of the CD cluster of nodes.

CD Adapter – A component of CD Master which communicates between the nodes within a CD cluster and with the CD Master GUI.

CD Agent – Windows Services software which runs on each node of a CD cluster and collects statistics on the health of each

CD Node – The CD installer option of CD Node. This installs the RXP protocol and the CD Agent onto a node. This is the required software on a node to participate into a cluster, but does not include the CD Master management system. A CD Node must be managed by a node running CD Master.

CD Scheduler – The component which handles traffic redirection. The scheduler node receives incoming IP traffic and redirects the traffic to the appropriate node to process each request.

Chapter 3: Installation

Installation and Configuration

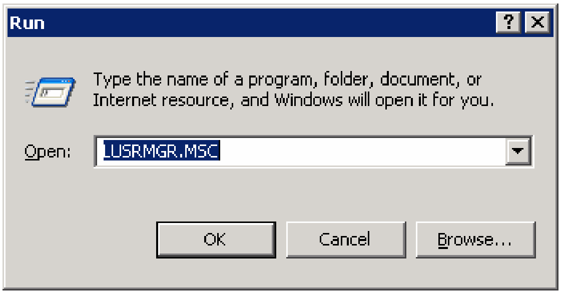
The following steps need to be performed to install the Resonate CD components onto each IAG system.

1. Create Resonate Administrator and Monitor accounts
2. Create environmental variables for persistant sessions
3. Disable ISA Spoof Detection
4. Download and install Resonate CD software
5. Create ISA access rules to allow Resonate CD nodes and components to communicate between nodes
6. Create a VIP DNS entry on your network
7. Configure Resonate CD
8. Create IAG Trunk

Note: This installation will require changes to the server network infrastructure and require reboots. This installation process will temporarily disrupt operation of this system and should not be done on a system running in production.

Create Resonate Administrator and Monitor accounts

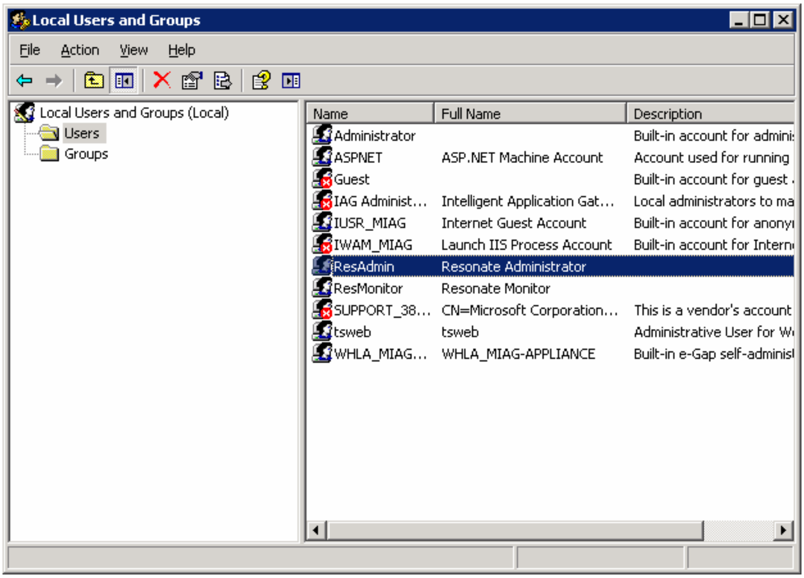
Start the user account manager snapin program to create the accounts.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: LUSRMGR.MSC

Start -> Run -> LUSRMGR.MSC



Name	Full Name	Description
Administrator		Built-in account for admini:
ASPNET	ASP.NET Machine Account	Account used for running
Guest		Built-in account for guest .
IAG Administ...	Intelligent Application Gat...	Local administrators to ma
IUSR_MIAG	Internet Guest Account	Built-in account for anonyı
IWAM_MIAG	Launch IIS Process Account	Built-in account for Interni
ResAdmin	Resonate Administrator	
ResMonitor	Resonate Monitor	
SUPPORT_38...	CN=Microsoft Corporation...	This is a vendor's account
tsweb	tsweb	Administrative User for Wi
WHLA_MIAG...	WHLA_MIAG-APPLIANCE	Built-in e-Gap self-adminis

Create accounts ResAdmin and ResMonitor.

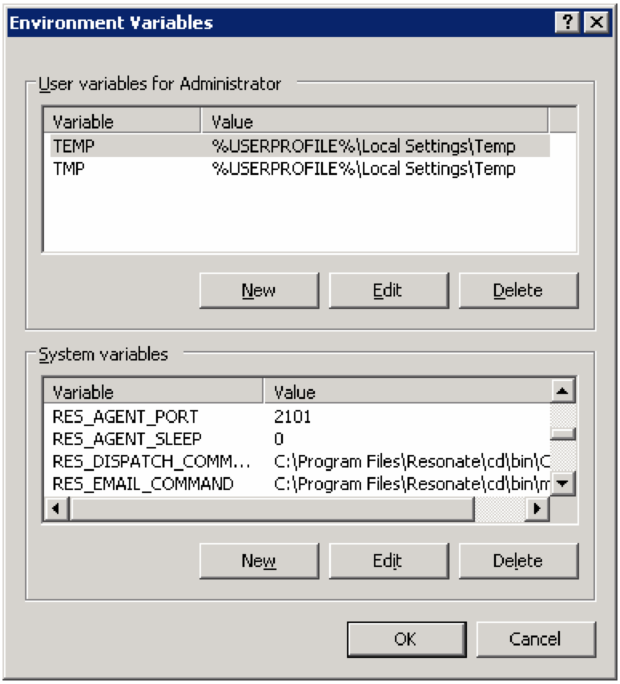
Add ResAdmin into the Administrators group.
Set the ResAdmin and ResMonitor passwords. The ResAdmin passwords and the ResMonitor passwords must be the same on each node. If the IAG systems are joined to a Windows Domain, this will be automatic. If

the IAG systems are not on a Domain, then this synconization will have to be done manually.

Note: **It is very important that the passwords be the same on each IAG node.**

Create Environmental Variables for Persistent Sessions

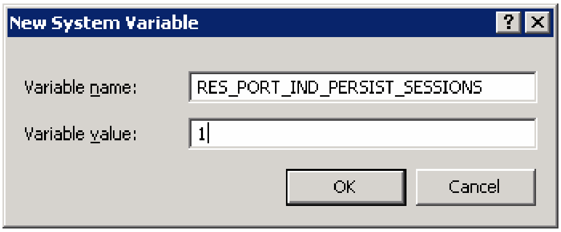
The following environmental variables need to be created to allow persistent sessions to be grouped by IP address. This allows Resonate to persist sessions for all applications on an IAG trunk. IAG maintains a session for multiple published applications, so these variables forces Resonate to peg sessions to a single IAG node instead of spreading transactions among multiple servers.



Variable	Value
TEMP	%USERPROFILE%\Local Settings\Temp
TMP	%USERPROFILE%\Local Settings\Temp

Variable	Value
RES_AGENT_PORT	2101
RES_AGENT_SLEEP	0
RES_DISPATCH_COMM...	C:\Program Files\Resonate\cd\bin\C
RES_EMAIL_COMMAND	C:\Program Files\Resonate\cd\bin\m

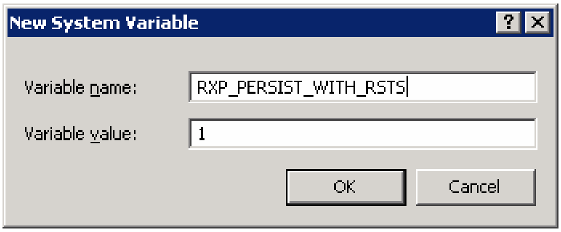
Start -> Control Panel -> System -> Advanced -> Environmental Variables



Variable name: RES_PORT_IND_PERSIST_SESSIONS

Variable value: 1

Add this variable.



Variable name: RXP_PERSIST_WITH_RSTS

Variable value: 1

Disable ISA Spoof Detection

The ISA spoof detection must be disabled to allow the intra-node traffic to be permitted. ISA will drop valid HTTP traffic that is redirected from the Resonate CD scheduler node to the actual server by the Resonate Load Balancing mechanism.

To disable ISA Spoof Detection, a registry entry will need to be updated. A script is provided to make this registry change. This script is located in the Resonate CD folder that was downloaded and unpacked.

Run the DisableSpoofDetection.bat in the Resonate CD folder.

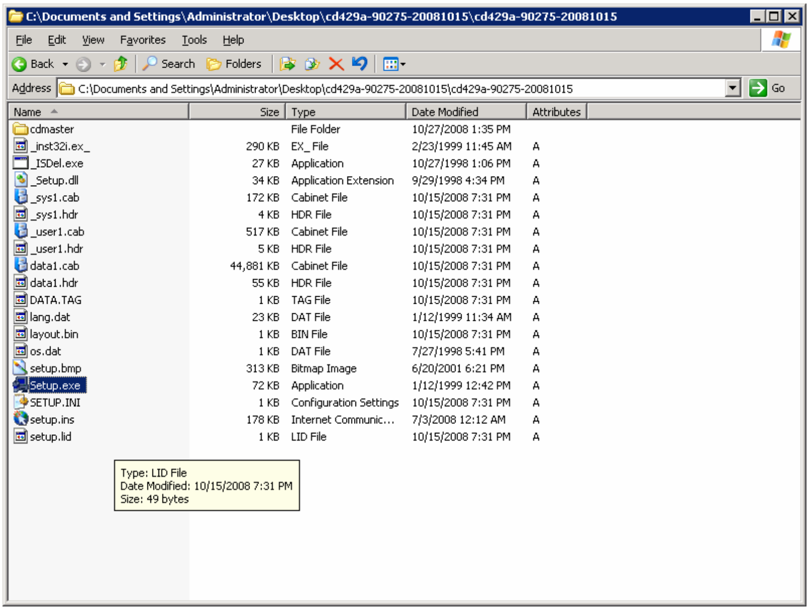
Download and Install Resonate CD software

The Resonate CD software can be downloaded from the nAppliance support site. Go to http://support.nappliance.com downloads. Select the latest version of Resonate CD.

This download will require a password. This password can be provided by the nAppliance support or sales departments. Please contact your nAppliance sales representative.

Copy this software package to your mIAG appliance. The mIAG appliance is hardened, and will not allow downloads from the Internet directly, but will allow you to mount a local Windows share.

Once the package is on your system, unzip the contents into a folder and follow the following steps.



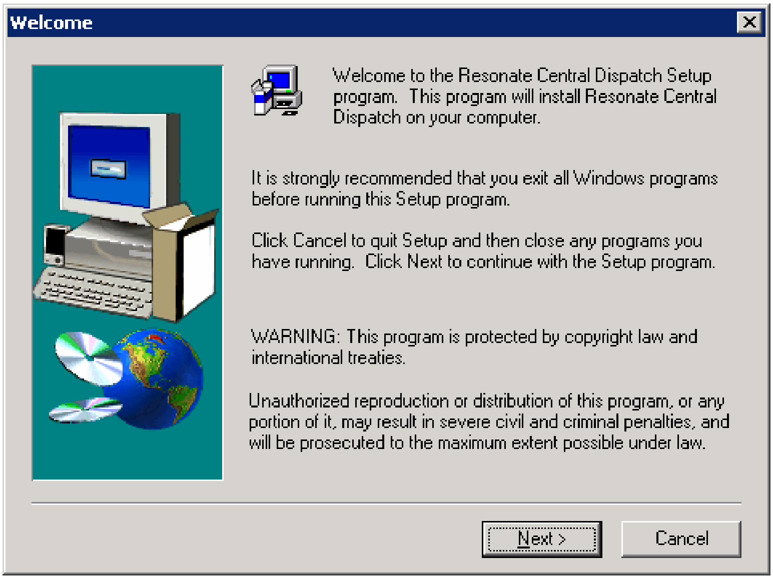
C:\Documents and Settings\Administrator\Desktop\cd429a-90275-20081015\cd429a-90275-20081015

Address C:\Documents and Settings\Administrator\Desktop\cd429a-90275-20081015\cd429a-90275-20081015

Name	Size	Type	Date Modified	Attributes
cdmaster		File Folder	10/27/2008 1:35 PM	
inst32i.ex	290 KB	EX_ File	2/23/1999 11:45 AM	A
_ISDel.exe	27 KB	Application	10/27/1998 1:06 PM	A
_Setup.dll	34 KB	Application Extension	9/29/1998 4:34 PM	A
_sys1.cab	172 KB	Cabinet File	10/15/2008 7:31 PM	A
_sys1.hdr	4 KB	HDR File	10/15/2008 7:31 PM	A
_user1.cab	517 KB	Cabinet File	10/15/2008 7:31 PM	A
_user1.hdr	5 KB	HDR File	10/15/2008 7:31 PM	A
data1.cab	44,881 KB	Cabinet File	10/15/2008 7:31 PM	A
data1.hdr	55 KB	HDR File	10/15/2008 7:31 PM	A
DATA.TAG	1 KB	TAG File	10/15/2008 7:31 PM	A
lang.dat	23 KB	DAT File	1/12/1999 11:34 AM	A
layout.bin	1 KB	BIN File	10/15/2008 7:31 PM	A
os.dat	1 KB	DAT File	7/27/1998 5:41 PM	A
setup.bmp	313 KB	Bitmap Image	6/20/2001 6:21 PM	A
Setup.exe	72 KB	Application	1/12/1999 12:42 PM	A
SETUP.INI	1 KB	Configuration Settings	10/15/2008 7:31 PM	A
setup.ins	178 KB	Internet Communic...	7/3/2008 12:12 AM	A
setup.lid	1 KB	LID File	10/15/2008 7:31 PM	A

Type: LID File
Date Modified: 10/15/2008 7:31 PM
Size: 49 bytes

Click on Setup.exe.



Welcome

Welcome to the Resonate Central Dispatch Setup program. This program will install Resonate Central Dispatch on your computer.

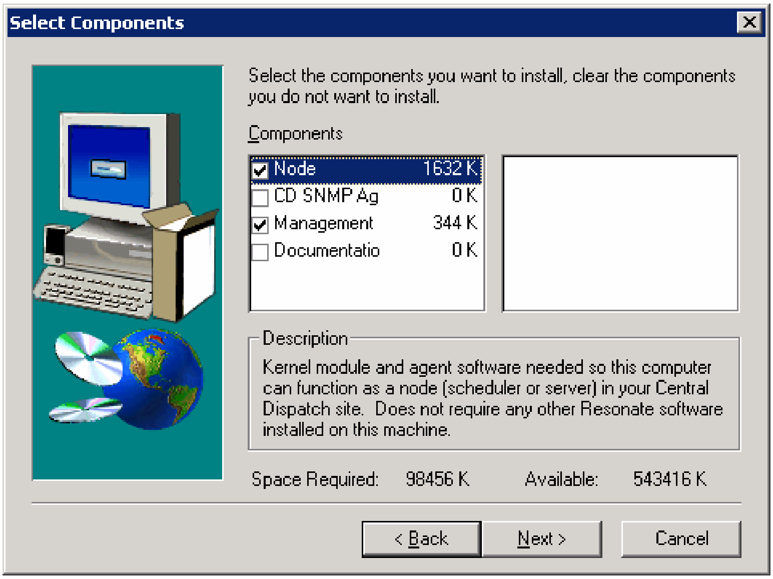
It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Click Next.



Select Components

Select the components you want to install, clear the components you do not want to install.

Components

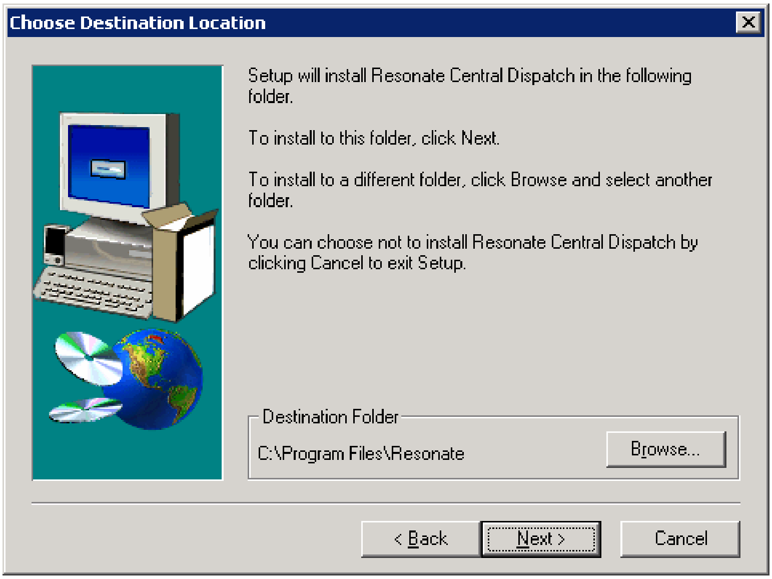
☑ Node	1632 K
□ CD SNMP Ag	0 K
☑ Management	344 K
□ Documentatio	0 K

Description

Kernel module and agent software needed so this computer can function as a node (scheduler or server) in your Central Dispatch site. Does not require any other Resonate software installed on this machine.

Space Required: 98456 K Available: 543416 K

Only select the Node and Management components.



Setup will install Resonate Central Dispatch in the following folder.

To install to this folder, click Next.

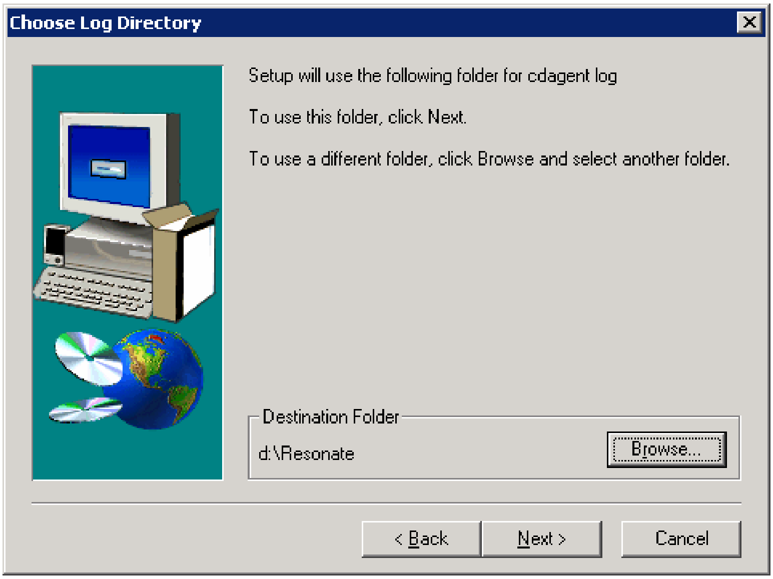
To install to a different folder, click Browse and select another folder.

You can choose not to install Resonate Central Dispatch by clicking Cancel to exit Setup.

Destination Folder

C:\Program Files\Resonate

Select the default program files folder.



Setup will use the following folder for cdagent log

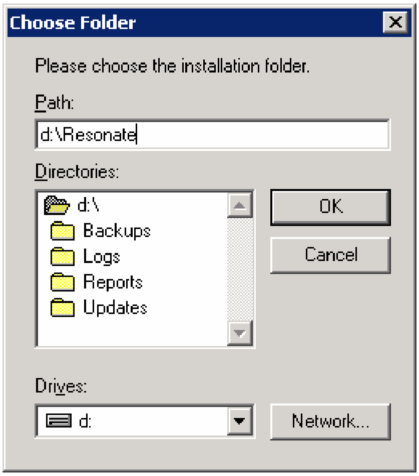
To use this folder, click Next.

To use a different folder, click Browse and select another folder.

Destination Folder

d:\Resonate

Navigate to the D: partition to write log files.

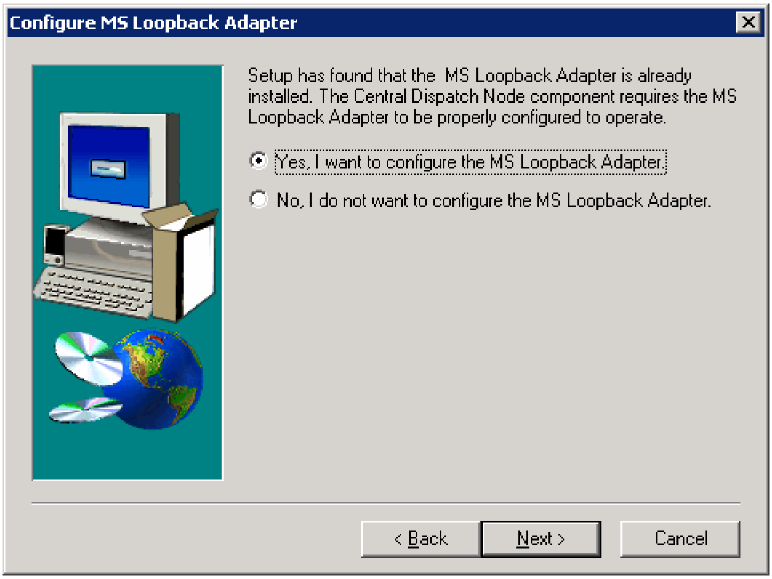


Please choose the installation folder.

Path:

d:\Resonate

You will need to create the Resonate folder.



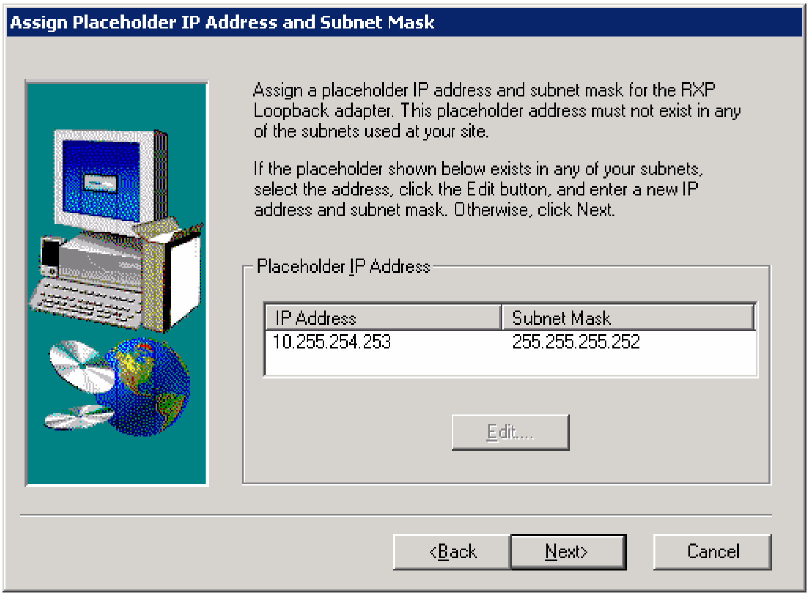
Configure MS Loopback Adapter

Setup has found that the MS Loopback Adapter is already installed. The Central Dispatch Node component requires the MS Loopback Adapter to be properly configured to operate.

● Yes, I want to configure the MS Loopback Adapter.

○ No, I do not want to configure the MS Loopback Adapter.

Configure the Loopback.



Assign Placeholder IP Address and Subnet Mask

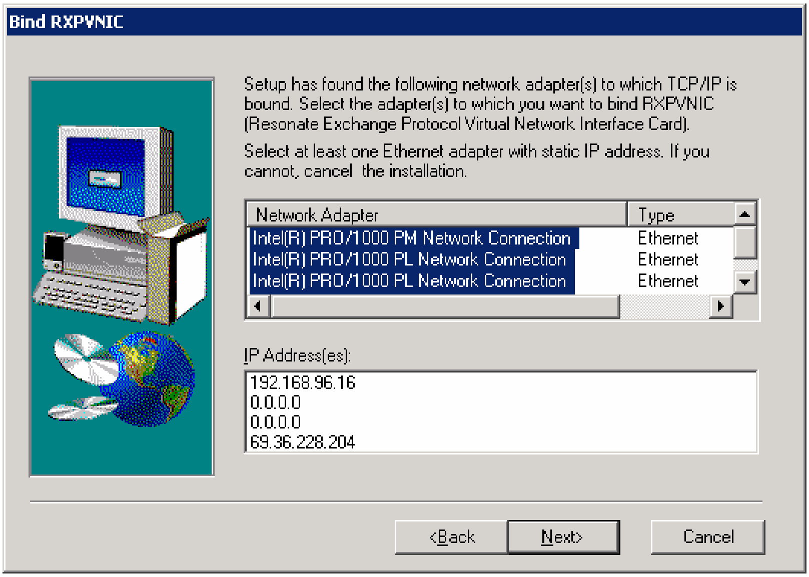
Assign a placeholder IP address and subnet mask for the RXP Loopback adapter. This placeholder address must not exist in any of the subnets used at your site.

If the placeholder shown below exists in any of your subnets, select the address, click the Edit button, and enter a new IP address and subnet mask. Otherwise, click Next.

Placeholder IP Address

IP Address	Subnet Mask
10.255.254.253	255.255.255.252

Take the default values here.



Bind RXPVNIC

Setup has found the following network adapter(s) to which TCP/IP is bound. Select the adapter(s) to which you want to bind RXPVNIC (Resonate Exchange Protocol Virtual Network Interface Card).

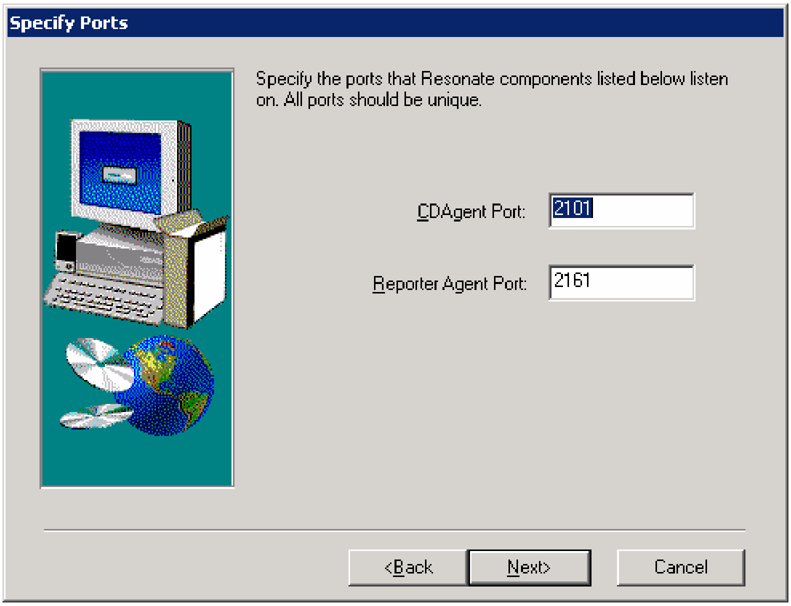
Select at least one Ethernet adapter with static IP address. If you cannot, cancel the installation.

Network Adapter	Type
Intel(R) PRO/1000 PM Network Connection	Ethernet
Intel(R) PRO/1000 PL Network Connection	Ethernet
Intel(R) PRO/1000 PL Network Connection	Ethernet

IP Address(es):

192.168.96.16
0.0.0.0
0.0.0.0
69.36.228.204

Configure the RXP protocol on every interface.



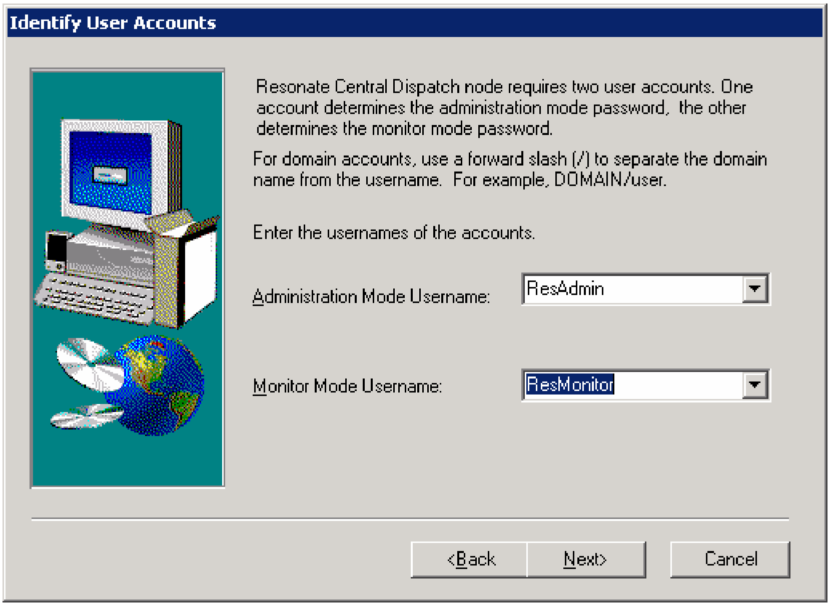
Specify Ports

Specify the ports that Resonate components listed below listen on. All ports should be unique.

CDAgent Port: 2101

Reporter Agent Port: 2161

Use the default ports. If these are changed, be sure to change the ISA access rules to match the new values.



Identify User Accounts

Resonate Central Dispatch node requires two user accounts. One account determines the administration mode password, the other determines the monitor mode password.

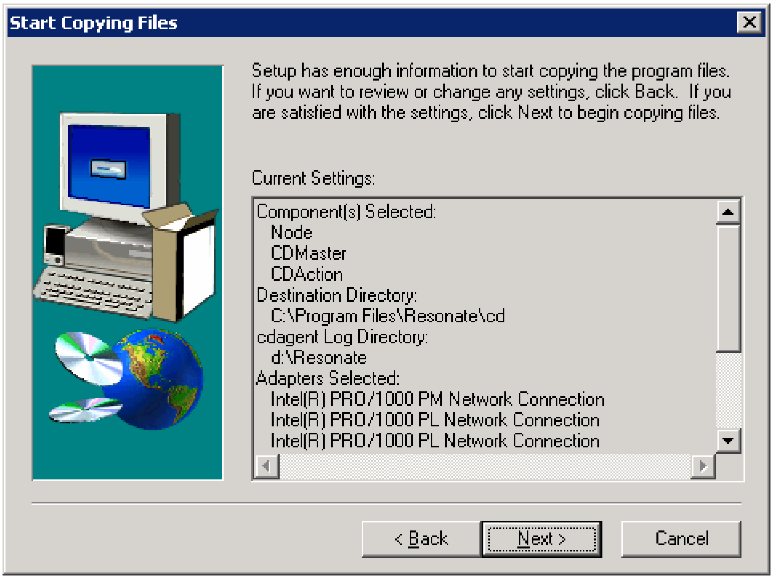
For domain accounts, use a forward slash (/) to separate the domain name from the username. For example, DOMAIN/user.

Enter the usernames of the accounts.

Administration Mode Username: ResAdmin

Monitor Mode Username: ResMonitor

Select the user accounts created earlier.



Start Copying Files

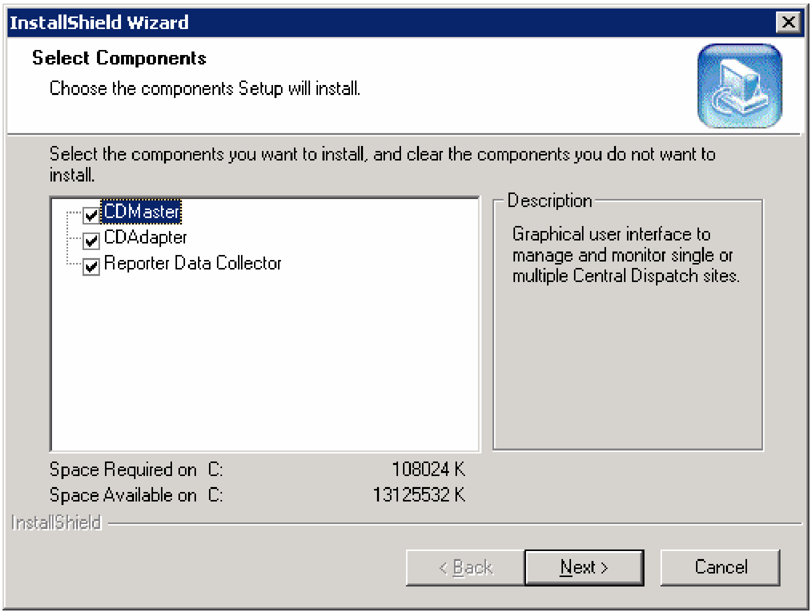
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

```
Component(s) Selected:
   Node
   CDMaster
   CDAction
Destination Directory:
   C:\Program Files\Resonate\cd
cdagent Log Directory:
   d:\Resonate
Adapters Selected:
   Intel(R) PRO/1000 PM Network Connection
   Intel(R) PRO/1000 PL Network Connection
   Intel(R) PRO/1000 PL Network Connection
```

The installation will now install the software.

Next the installation process will launch a configuration wizard.



InstallShield Wizard

Select Components

Choose the components Setup will install.

Select the components you want to install, and clear the components you do not want to install.

- ☑ CDMaster
- ☑ CDAdapter
- ☑ Reporter Data Collector

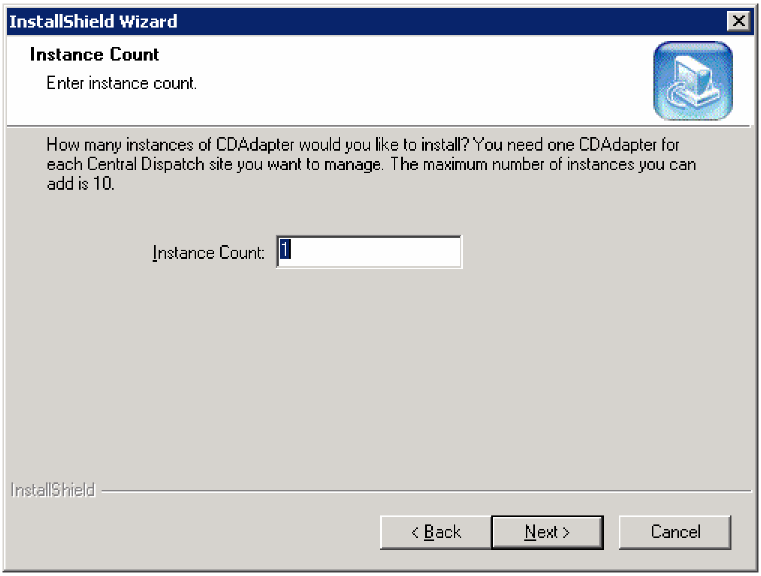
Description

Graphical user interface to manage and monitor single or multiple Central Dispatch sites.

Space Required on C: 108024 K

Space Available on C: 13125532 K

Select all the above components for each IAG node.


InstallShield Wizard

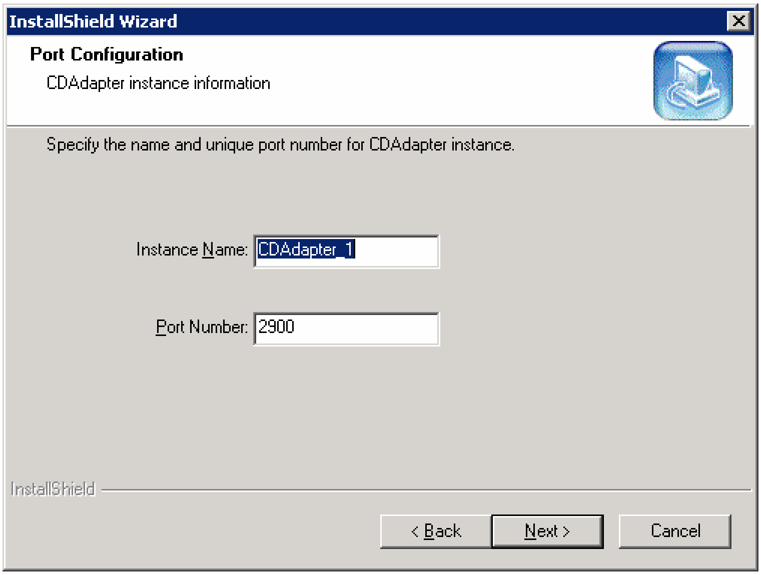
Instance Count

Enter instance count.

How many instances of CDAdapter would you like to install? You need one CDAdapter for each Central Dispatch site you want to manage. The maximum number of instances you can add is 10.

Instance Count: 1

A typical IAG cluster implementation only needs 1 instance.


InstallShield Wizard

Port Configuration

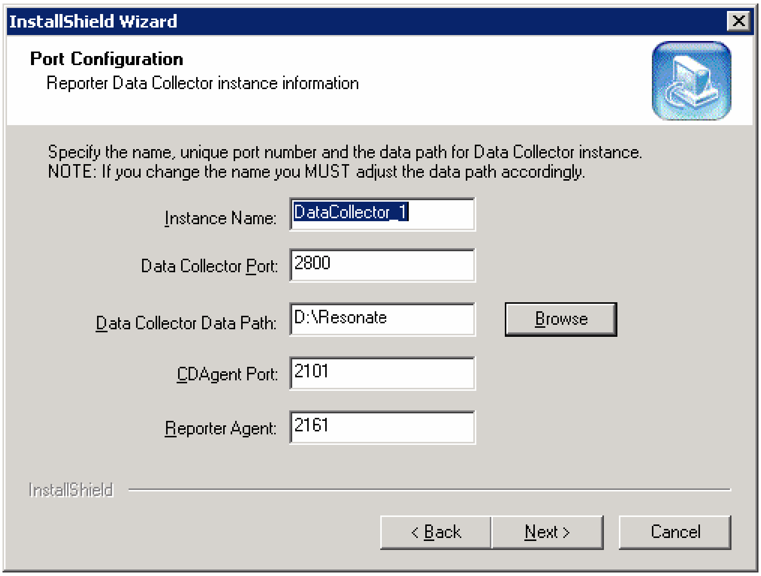
CDAdapter instance information

Specify the name and unique port number for CDAdapter instance.

Instance Name: CDAdapter_1

Port Number: 2900

Select the default values.



InstallShield Wizard

Port Configuration

Reporter Data Collector instance information

Specify the name, unique port number and the data path for Data Collector instance.
NOTE: If you change the name you MUST adjust the data path accordingly.

Instance Name: DataCollector_1

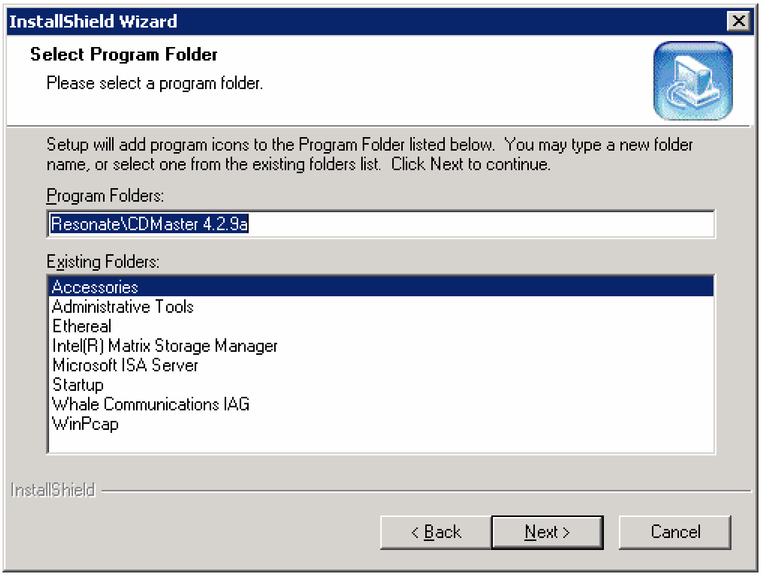
Data Collector Port: 2800

Data Collector Data Path: D:\Resonate

CDAgent Port: 2101

Reporter Agent: 2161

Select the default values except change the Data Collector Path to D:\Resonate which was created above.



InstallShield Wizard

Select Program Folder

Please select a program folder.

Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing folders list. Click Next to continue.

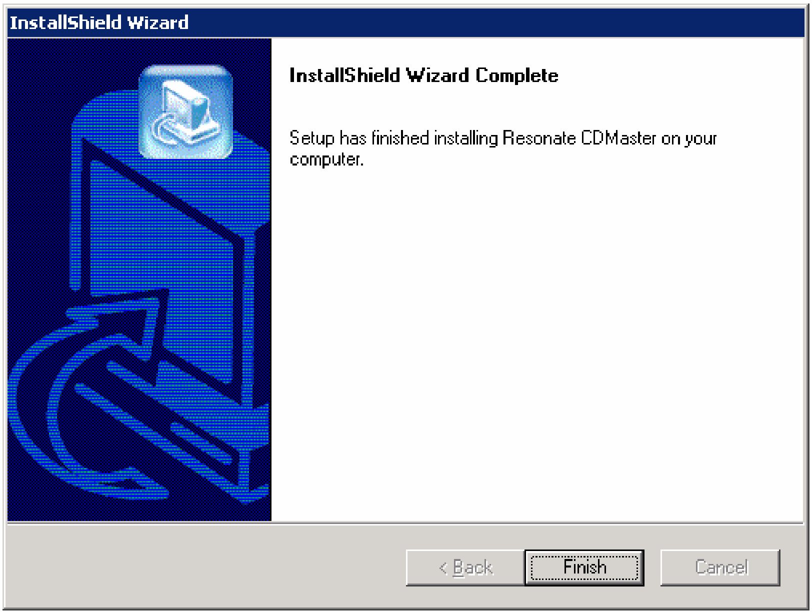
Program Folders:

Resonate\CDMaster 4.2.9a

Existing Folders:

- Accessories
- Administrative Tools
- Ethereal
- Intel(R) Matrix Storage Manager
- Microsoft ISA Server
- Startup
- Whale Communications IAG
- WinPcap

Select the defaults.

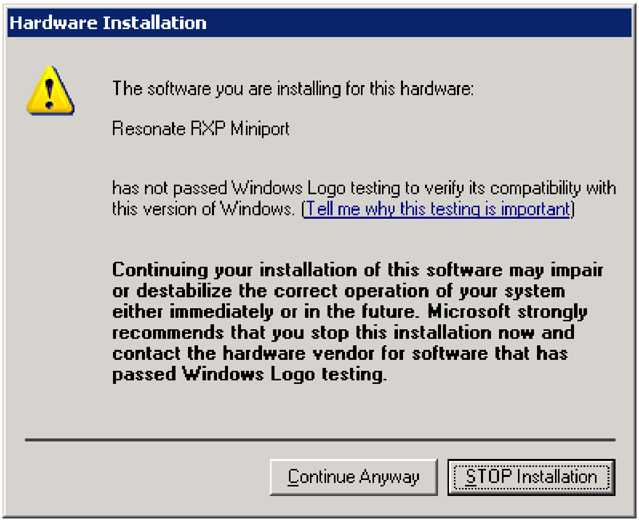


InstallShield Wizard

InstallShield Wizard Complete

Setup has finished installing Resonate CDMaster on your computer.

Click Finish.



Hardware Installation

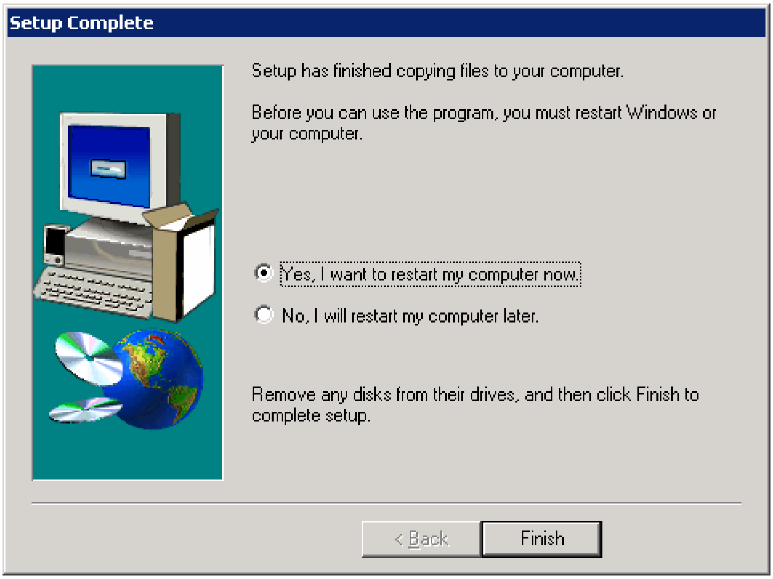
The software you are installing for this hardware:

Resonate RXP Miniport

has not passed Windows Logo testing to verify its compatibility with this version of Windows. (Tell me why this testing is important.)

Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.

The following warning will appear several times. Click “Continue Anyway” and continue. This installation could take a few moments at this stage.



Setup Complete

Setup has finished copying files to your computer.

Before you can use the program, you must restart Windows or your computer.

● Yes, I want to restart my computer now.

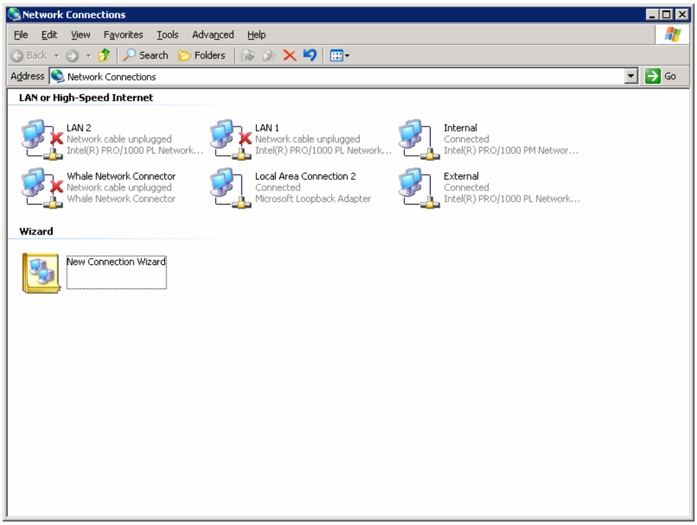
○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

A reboot is required at this stage.

Checking the Install

After the reboot, the following changes should be visable.


Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections
Go

LAN or High-Speed Internet

LAN 2
Network cable unplugged
Intel(R) PRO/1000 PL Network...

LAN 1
Network cable unplugged
Intel(R) PRO/1000 PL Network...

Internal
Connected
Intel(R) PRO/1000 PM Networ...

Whale Network Connector
Network cable unplugged
Whale Network Connector

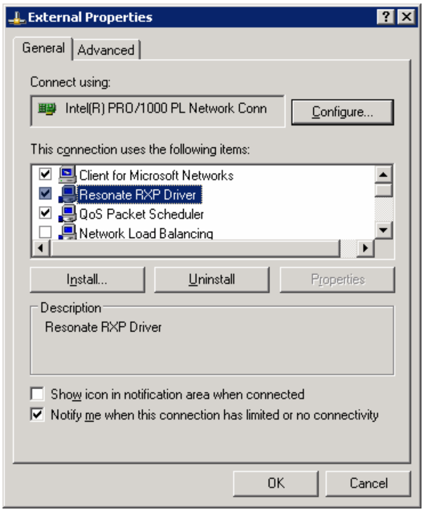
Local Area Connection 2
Connected
Microsoft Loopback Adapter

External
Connected
Intel(R) PRO/1000 PL Network...

Wizard

New Connection Wizard

Select any of your physical interfaces.



Connect using:

Intel(R) PRO/1000 PL Network Conn

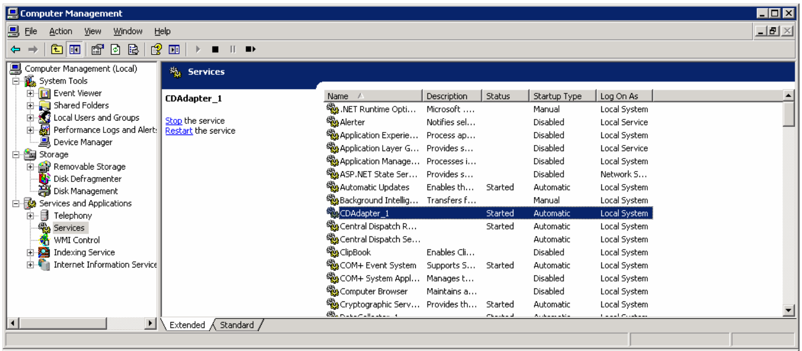
This connection uses the following items:

☑ Client for Microsoft Networks
☑ Resonate RXP Driver
☑ QoS Packet Scheduler
□ Network Load Balancing

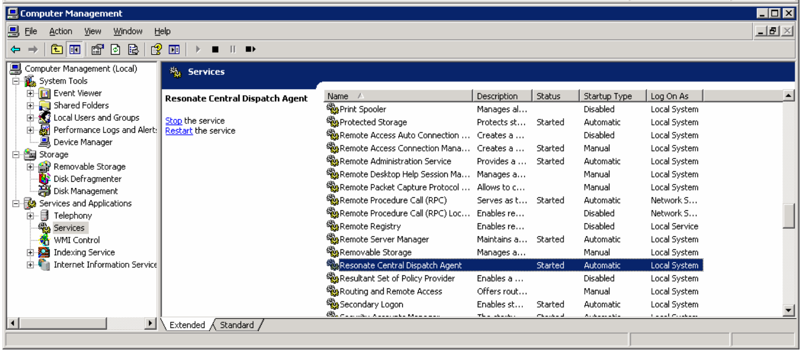
Description
Resonate RXP Driver

□ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

The Resonate RXP Driver will now be installed.

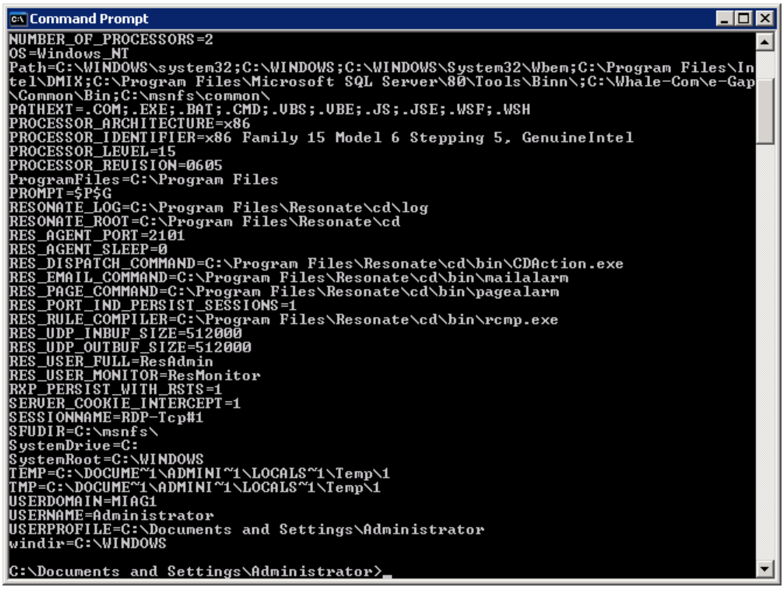


Name	Description	Status	Startup Type	Log On As
.NET Runtime Opti...	Microsoft		Manual	Local System
Alerter	Notifies sel...		Disabled	Local Service
Application Experie...	Process ap...		Disabled	Local System
Application Layer G...	Provides s...		Disabled	Local Service
Application Manage...	Processes i...		Disabled	Local System
ASP.NET State Ser...	Provides s...		Disabled	Network S...
Automatic Updates	Enables th...	Started	Automatic	Local System
Background Intellig...	Transfers f...		Manual	Local System
CDAdapter_1		Started	Automatic	Local System
Central Dispatch R...		Started	Automatic	Local System
Central Dispatch Se...			Automatic	Local System
ClipBook	Enables Cli...		Disabled	Local System
COM+ Event System	Supports S...	Started	Automatic	Local System
COM+ System Appl...	Manages t...		Disabled	Local System
Computer Browser	Maintains a...		Disabled	Local System
Cryptographic Serv...	Provides th...	Started	Automatic	Local System



Name	Description	Status	Startup Type	Log On As
Print Spooler	Manages al...		Disabled	Local System
Protected Storage	Protects st...	Started	Automatic	Local System
Remote Access Auto Connection ...	Creates a ...		Disabled	Local System
Remote Access Connection Mana...	Creates a ...	Started	Manual	Local System
Remote Administration Service	Provides a ...	Started	Automatic	Local System
Remote Desktop Help Session Ma...	Manages a...		Manual	Local System
Remote Packet Capture Protocol ...	Allows to c...		Manual	Local System
Remote Procedure Call (RPC)	Serves as t...	Started	Automatic	Network S...
Remote Procedure Call (RPC) Loc...	Enables re...		Disabled	Network S...
Remote Registry	Enables re...		Disabled	Local Service
Remote Server Manager	Maintains a...	Started	Automatic	Local System
Removable Storage	Manages a...		Manual	Local System
Resonate Central Dispatch Agent		Started	Automatic	Local System
Resultant Set of Policy Provider	Enables a ...		Disabled	Local System
Routing and Remote Access	Offers rout...		Manual	Local System
Secondary Logon	Enables st...	Started	Automatic	Local System

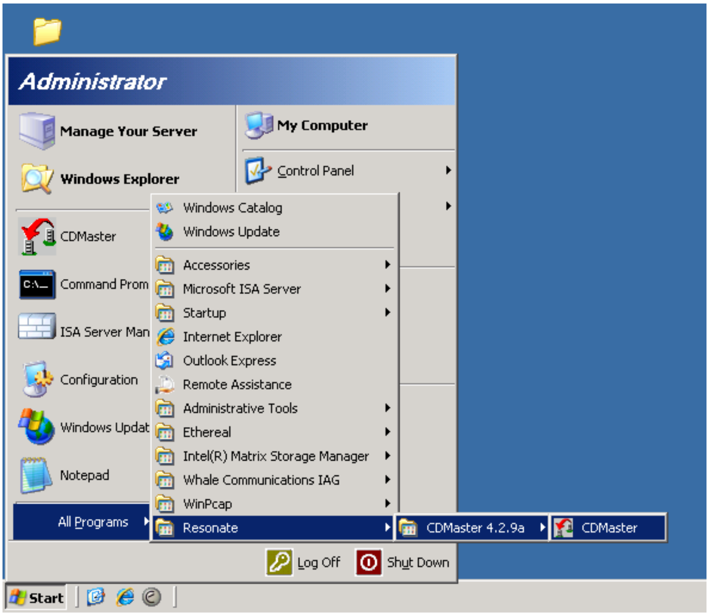
Several Resonate services and a service called CDAdapter_1 will be running.



```
NUMBER_OF_PROCESSORS=2
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\Program Files\In
tel\DMIX;C:\Program Files\Microsoft SQL Server\80\Tools\Binn\;C:\Whale-Com\e-Gap
\Common\Bin;C:\msnfs\common\
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 15 Model 6 Stepping 5, GenuineIntel
PROCESSOR_LEVEL=15
PROCESSOR_REVISION=0605
ProgramFiles=C:\Program Files
PROMPT=$P$G
RESONATE_LOG=C:\Program Files\Resonate\cd\log
RESONATE_ROOT=C:\Program Files\Resonate\cd
RES_AGENT_PORT=2101
RES_AGENT_SLEEP=0
RES_DISPATCH_COMMAND=C:\Program Files\Resonate\cd\bin\CDAction.exe
RES_EMAIL_COMMAND=C:\Program Files\Resonate\cd\bin\mailalarm
RES_PAGE_COMMAND=C:\Program Files\Resonate\cd\bin\pagealarm
RES_PORT_IND_PERSIST_SESSIONS=1
RES_RULE_COMPILER=C:\Program Files\Resonate\cd\bin\rcmp.exe
RES_UDP_INBUF_SIZE=512000
RES_UDP_OUTBUF_SIZE=512000
RES_USER_FULL=ResAdmin
RES_USER_MONITOR=ResMonitor
RXP_PERSIST_WITH_RSTS=1
SERVER_COOKIE_INTERCEPT=1
SESSIONNAME=RDP-Tcp#1
SFUDIR=C:\msnfs\
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1
TMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1
USERDOMAIN=MIAG1
USERNAME=Administrator
USERPROFILE=C:\Documents and Settings\Administrator
windir=C:\WINDOWS

C:\Documents and Settings\Administrator>_
```

Resonate specific environmental variables will be set.



Administrator
Manage Your Server
Windows Explorer
CDMaster
Command Prom
ISA Server Man
Configuration
Windows Updat
Notepad
All Programs
My Computer
Control Panel
Windows Catalog
Windows Update
Accessories
Microsoft ISA Server
Startup
Internet Explorer
Outlook Express
Remote Assistance
Administrative Tools
Ethereal
Intel(R) Matrix Storage Manager
Whale Communications IAG
WinPcap
Resonate
CDMaster 4.2.9a
CDMaster
Log Off
Shut Down
Start

Create ISA access rules to allow Resonate CD nodes and components to communicate between nodes

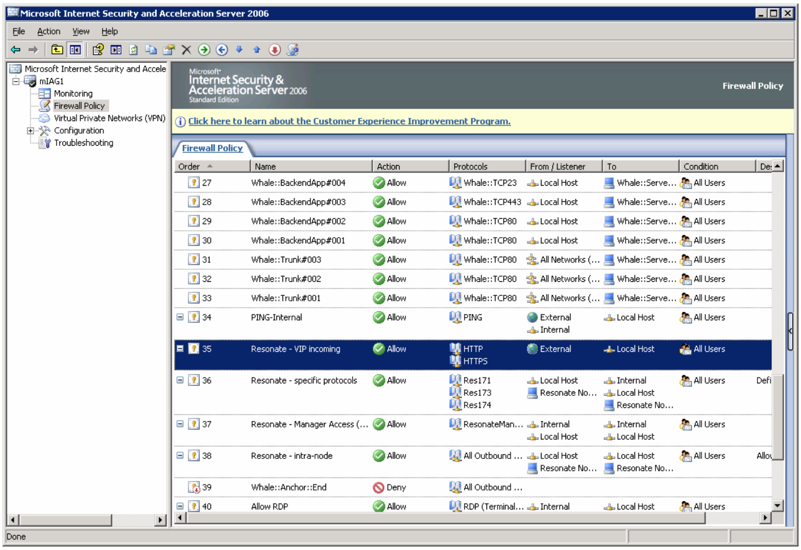
Several ISA access rules will have to be created to allow Resonate CD to communication between nodes.

The communicates paths specific to ISA rules are:

1. Inter-node communicates between Resonate components
2. VIP to node traffic, where ISA must allow traffic from a VIP address. IAG defines ISA access rules to allow traffic from the External address, and since the VIP address is different than the IAG External address, additional rules are required.
3. CD Master management traffic – where the CD Master management software communicates with the CD Adapter node on port 2900. This management software may be on an external node to the IAG cluster, or running on any of the IAG nodes.

The ISA rules defined below must be added to every node in the IAG cluster. Once these rules are created on a single node, the Resonate rules can be exported, then imported on the other IAG systems. For this import/export to work correctly, when defining the "Resonate Node x" entries, add all the nodes to each rule, including the node where the rule is defined. Adding the current node entry with the foreign nodes into an access rule makes the export/imports transportable among all the nodes without having to customize the rules per node.

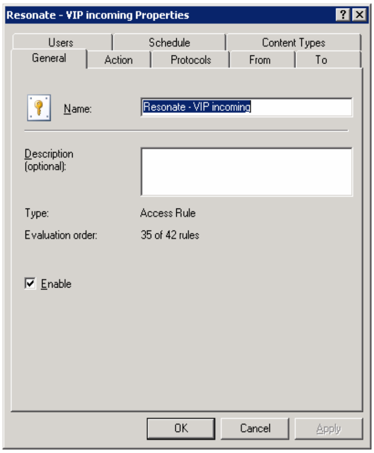
Resonate VIP Access Rules


Microsoft Internet Security and Acceleration Server 2006
File
Action
View
Help
Microsoft Internet Security and Accele
mIAG1
Monitoring
Firewall Policy
Virtual Private Networks (VPN)
Configuration
Troubleshooting
Microsoft Internet Security & Acceleration Server 2006 Standard Edition
Firewall Policy
Click here to learn about the Customer Experience Improvement Program.
Firewall Policy
Done

Order	Name	Action	Protocols	From / Listener	To	Condition	De:
27	Whale::BackendApp#004	Allow	Whale::TCP23	Local Host	Whale::Serve...	All Users	
28	Whale::BackendApp#003	Allow	Whale::TCP443	Local Host	Whale::Serve...	All Users	
29	Whale::BackendApp#002	Allow	Whale::TCP80	Local Host	Whale::Serve...	All Users	
30	Whale::BackendApp#001	Allow	Whale::TCP80	Local Host	Whale::Serve...	All Users	
31	Whale::Trunk#003	Allow	Whale::TCP80	All Networks (...	Whale::Serve...	All Users	
32	Whale::Trunk#002	Allow	Whale::TCP80	All Networks (...	Whale::Serve...	All Users	
33	Whale::Trunk#001	Allow	Whale::TCP80	All Networks (...	Whale::Serve...	All Users	
34	PING-Internal	Allow	PING	External Internal	Local Host	All Users	
35	Resonate - VIP incoming	Allow	HTTP HTTPS	External	Local Host	All Users	
36	Resonate - specific protocols	Allow	Res171 Res173 Res174	Local Host Resonate No...	Internal Local Host Resonate No...	All Users	Defi
37	Resonate - Manager Access (...	Allow	ResonateMan...	Internal Local Host	Internal Local Host	All Users	
38	Resonate - intra-node	Allow	All Outbound ...	Local Host Resonate No...	Local Host Resonate No...	All Users	Allov
39	Whale::Anchor::End	Deny	All Outbound ...				
40	Allow RDP	Allow	RDP (Terminal...	Internal	Local Host	All Users	

The access rule name “Resonate – VIP incoming” screens are shown below.

Follow the screens below to create the access rule.


Resonate - VIP incoming Properties

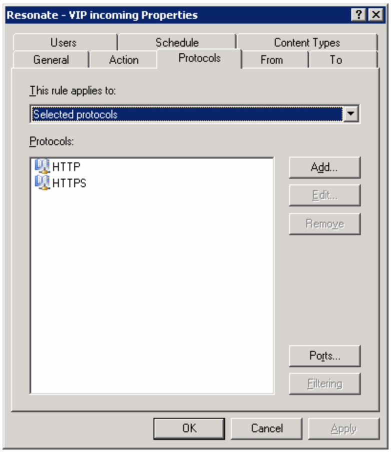
Name: Resonate - VIP incoming

Description (optional):

Type: Access Rule

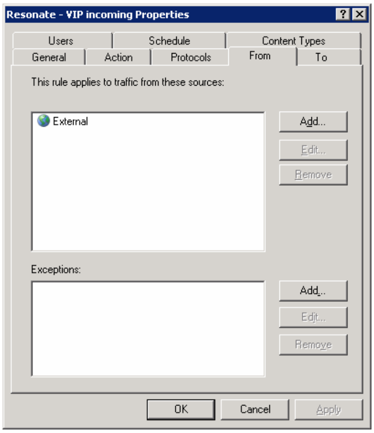
Evaluation order: 35 of 42 rules

☑ Enable


Resonate - VIP incoming Properties

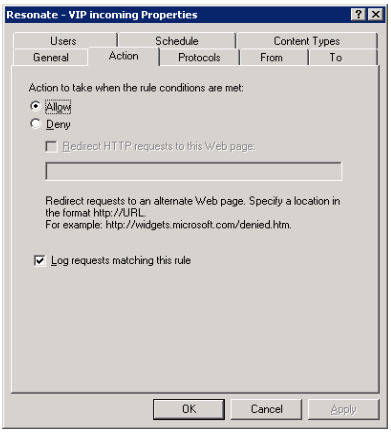
This rule applies to: Selected protocols

Protocols:
HTTP
HTTPS


Resonate - VIP incoming Properties

This rule applies to traffic from these sources:
External

Exceptions:


Resonate - VIP incoming Properties

Action to take when the rule conditions are met:

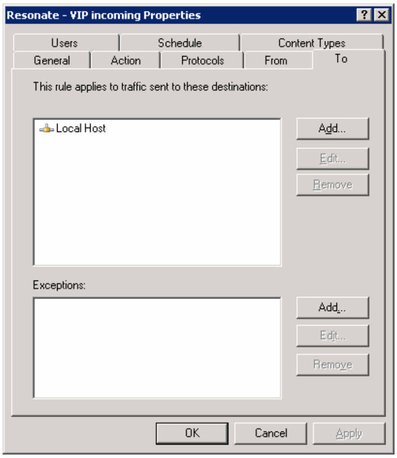
● Allow

○ Deny

□ Redirect HTTP requests to this Web page:

Redirect requests to an alternate Web page. Specify a location in the format http://URL.
For example: http://widgets.microsoft.com/denied.htm.

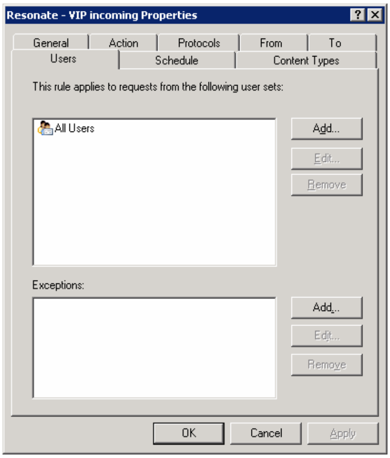
☑ Log requests matching this rule



This rule applies to traffic sent to these destinations:

Local Host

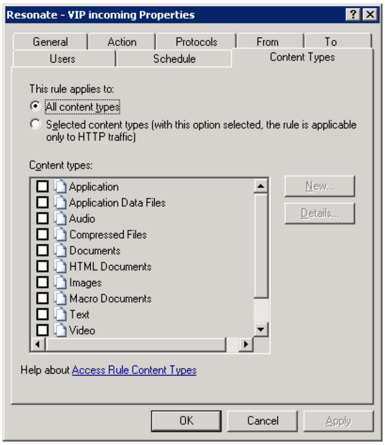
Exceptions:



This rule applies to requests from the following user sets:

All Users

Exceptions:



This rule applies to:

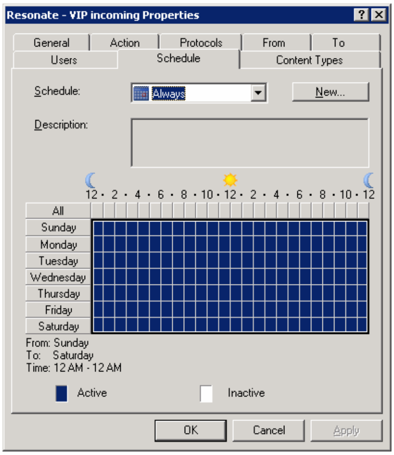
● All content types

○ Selected content types (with this option selected, the rule is applicable only to HTTP traffic)

Content types:

- □ Application
- □ Application Data Files
- □ Audio
- □ Compressed Files
- □ Documents
- □ HTML Documents
- □ Images
- □ Macro Documents
- □ Text
- □ Video

Help about Access Rule Content Types



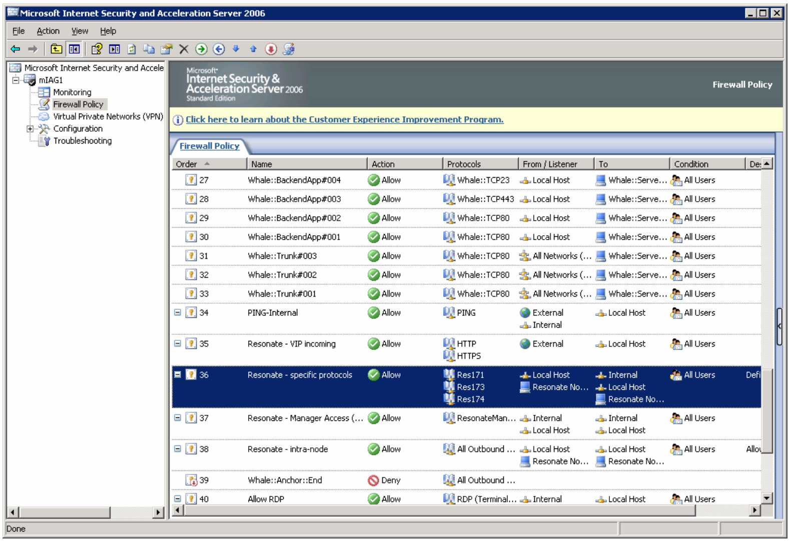
Schedule: Always

Description:

From: Sunday
To: Saturday
Time: 12 AM - 12 AM

■ Active □ Inactive

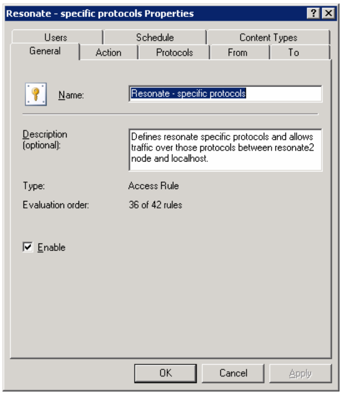
Resonate Specific Protocols Access Rule


Microsoft Internet Security and Acceleration Server 2006
File Action View Help
Microsoft Internet Security and Accele
mIAG1
Monitoring
Firewall Policy
Virtual Private Networks (VPN)
Configuration
Troubleshooting
Microsoft Internet Security & Acceleration Server 2006 Standard Edition
Firewall Policy
Click here to learn about the Customer Experience Improvement Program.
Firewall Policy
Done

Order	Name	Action	Protocols	From / Listener	To	Condition	De:
27	Whale::BackendApp#004	Allow	Whale::TCP23	Local Host	Whale::Serve…	All Users	
28	Whale::BackendApp#003	Allow	Whale::TCP443	Local Host	Whale::Serve…	All Users	
29	Whale::BackendApp#002	Allow	Whale::TCP80	Local Host	Whale::Serve…	All Users	
30	Whale::BackendApp#001	Allow	Whale::TCP80	Local Host	Whale::Serve…	All Users	
31	Whale::Trunk#003	Allow	Whale::TCP80	All Networks (…	Whale::Serve…	All Users	
32	Whale::Trunk#002	Allow	Whale::TCP80	All Networks (…	Whale::Serve…	All Users	
33	Whale::Trunk#001	Allow	Whale::TCP80	All Networks (…	Whale::Serve…	All Users	
34	PING-Internal	Allow	PING	External Internal	Local Host	All Users	
35	Resonate - VIP incoming	Allow	HTTP HTTPS	External	Local Host	All Users	
36	Resonate - specific protocols	Allow	Res171 Res173 Res174	Local Host Resonate No…	Internal Local Host Resonate No…	All Users	Defi
37	Resonate - Manager Access (…	Allow	ResonateMan…	Internal Local Host	Internal Local Host	All Users	
38	Resonate - intra-node	Allow	All Outbound …	Local Host Resonate No…	Local Host Resonate No…	All Users	Allo
39	Whale::Anchor::End	Deny	All Outbound …				
40	Allow RDP	Allow	RDP (Terminal…	Internal	Local Host	All Users	

Resonate uses specific protocols (IP number 171, 173 and 174). This access rule defines these protocols and the access rules necessary.

The following screens define the Resonate – specific protocols rule. During this rule creation, the system will prompt to create protocol and node definitions which do not yet exist. Screen shots to create these are shown below.



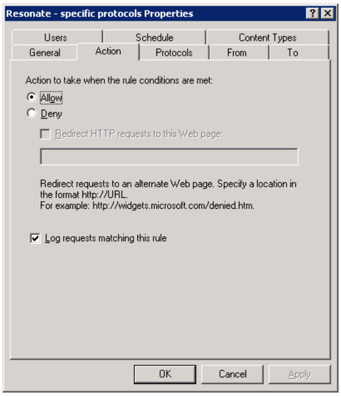
Name: Resonate - specific protocols

Description (optional): Defines resonate specific protocols and allows traffic over those protocols between resonate2 node and localhost.

Type: Access Rule

Evaluation order: 36 of 42 rules

☑ Enable



Action to take when the rule conditions are met:

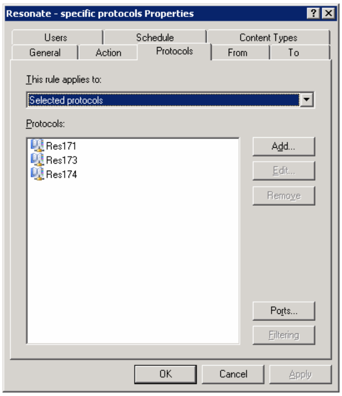
● Allow

○ Deny

□ Redirect HTTP requests to this Web page:

Redirect requests to an alternate Web page. Specify a location in the format http://URL.
For example: http://widgets.microsoft.com/denied.htm.

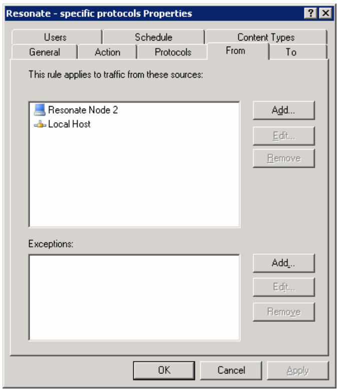
☑ Log requests matching this rule



This rule applies to: Selected protocols

Protocols:

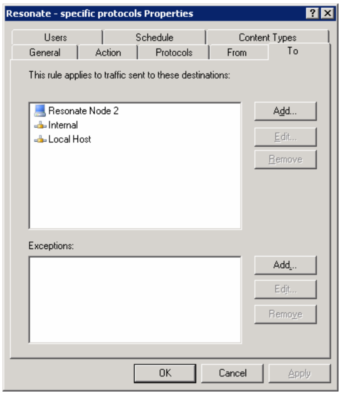
- Res171
- Res173
- Res174



This rule applies to traffic from these sources:

- Resonate Node 2
- Local Host

Exceptions:



This rule applies to traffic sent to these destinations:

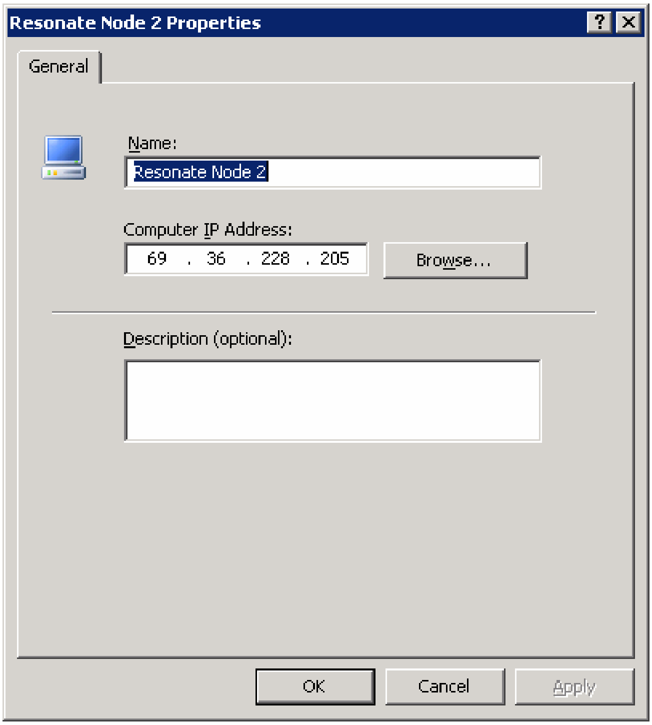
- Resonate Node 2
- Internal
- Local Host

Exceptions:

For tabs not shown above, select the defaults.

In the example above, only one node is defined in the rule. Add each cluster node in this rule. This will allow you to export and import these access rules into each node of the cluster using the same rule definitions.

Create a node definition for each of the nodes in the IAG Resonate cluster.



Resonate Node 2 Properties

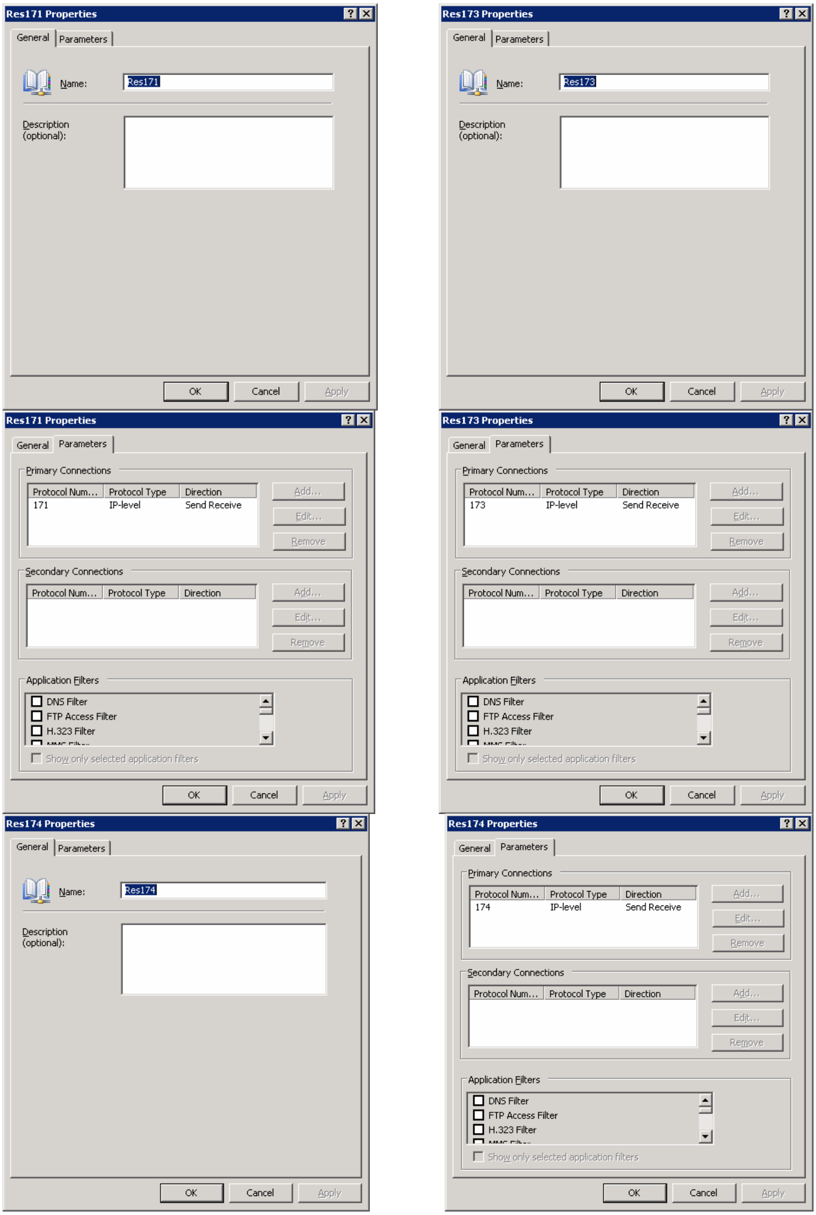
General

Name: Resonate Node 2

Computer IP Address: 69 . 36 . 228 . 205

Description (optional):

Add the specific interface address for the External Interface. The above screen defines a single node. This intra-node traffic is using the External Interfaces for this example. Any of the Windows Ethernet interfaces can be used, but the defintions within ISA and Resonate CD must be consistent.



Res171 Properties (General)

Name: Res171

Description (optional):

Res171 Properties (Parameters)

Primary Connections

Protocol Num...	Protocol Type	Direction
171	IP-level	Send Receive

Secondary Connections

Protocol Num...	Protocol Type	Direction

Application Filters

- □ DNS Filter
- □ FTP Access Filter
- □ H.323 Filter
- □ MMS Filter

□ Show only selected application filters

Res173 Properties (General)

Name: Res173

Description (optional):

Res173 Properties (Parameters)

Primary Connections

Protocol Num...	Protocol Type	Direction
173	IP-level	Send Receive

Secondary Connections

Protocol Num...	Protocol Type	Direction

Application Filters

- □ DNS Filter
- □ FTP Access Filter
- □ H.323 Filter
- □ MMS Filter

□ Show only selected application filters

Res174 Properties (General)

Name: Res174

Description (optional):

Res174 Properties (Parameters)

Primary Connections

Protocol Num...	Protocol Type	Direction
174	IP-level	Send Receive

Secondary Connections

Protocol Num...	Protocol Type	Direction

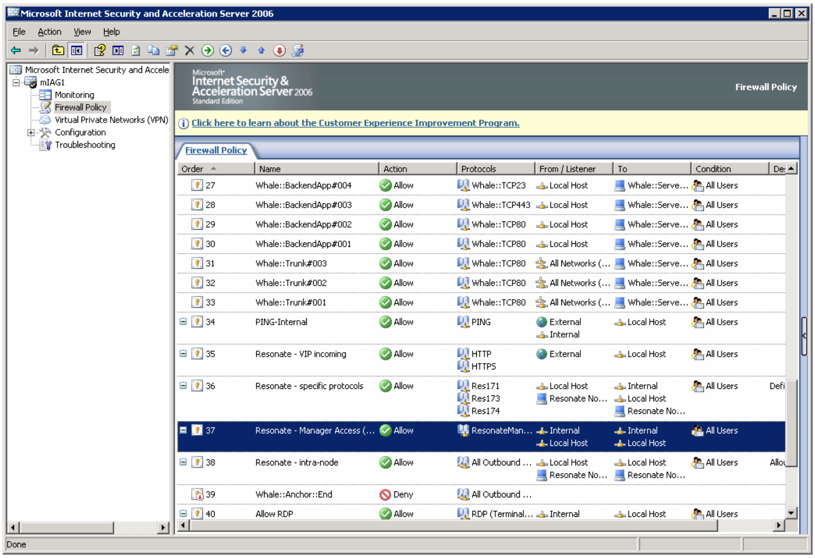
Application Filters

- □ DNS Filter
- □ FTP Access Filter
- □ H.323 Filter
- □ MMS Filter

□ Show only selected application filters

The Resonate internal IP protocol definitions.

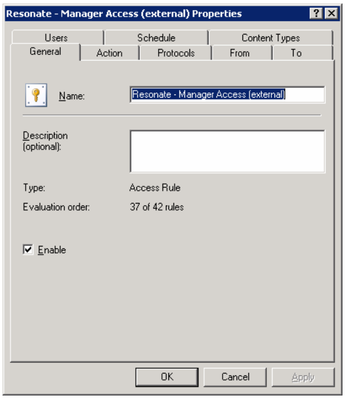
Resonate Specific Protocols Access Rule



Microsoft Internet Security and Acceleration Server 2006
File Action View Help
Microsoft Internet Security and Accele
mIAG1
Monitoring
Firewall Policy
Virtual Private Networks (VPN)
Configuration
Troubleshooting
Microsoft Internet Security & Acceleration Server 2006 Standard Edition
Firewall Policy
Click here to learn about the Customer Experience Improvement Program.
Firewall Policy
Done

Order	Name	Action	Protocols	From / Listener	To	Condition	De:
27	Whale::BackendApp#004	Allow	Whale::TCP23	Local Host	Whale::Serve...	All Users	
28	Whale::BackendApp#003	Allow	Whale::TCP443	Local Host	Whale::Serve...	All Users	
29	Whale::BackendApp#002	Allow	Whale::TCP80	Local Host	Whale::Serve...	All Users	
30	Whale::BackendApp#001	Allow	Whale::TCP80	Local Host	Whale::Serve...	All Users	
31	Whale::Trunk#003	Allow	Whale::TCP80	All Networks (...	Whale::Serve...	All Users	
32	Whale::Trunk#002	Allow	Whale::TCP80	All Networks (...	Whale::Serve...	All Users	
33	Whale::Trunk#001	Allow	Whale::TCP80	All Networks (...	Whale::Serve...	All Users	
34	PING-Internal	Allow	PING	External Internal	Local Host	All Users	
35	Resonate - VIP incoming	Allow	HTTP HTTPS	External	Local Host	All Users	
36	Resonate - specific protocols	Allow	Res171 Res173 Res174	Local Host Resonate No...	Internal Local Host Resonate No...	All Users	Defi
37	Resonate - Manager Access (...	Allow	ResonateMan...	Internal Local Host	Internal Local Host	All Users	
38	Resonate - intra-node	Allow	All Outbound ...	Local Host Resonate No...	Local Host Resonate No...	All Users	Allo
39	Whale::Anchor::End	Deny	All Outbound ...				
40	Allow RDP	Allow	RDP (Terminal...	Internal	Local Host	All Users	

The Resonate Manager Access rule defines the manager node access to the nodes in the cluster. This uses port 2900.


Resonate - Manager Access (external) Properties

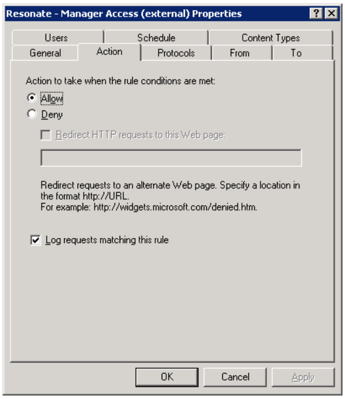
Name: Resonate - Manager Access (external)

Description (optional):

Type: Access Rule

Evaluation order: 37 of 42 rules

☑ Enable


Resonate - Manager Access (external) Properties

Action to take when the rule conditions are met:

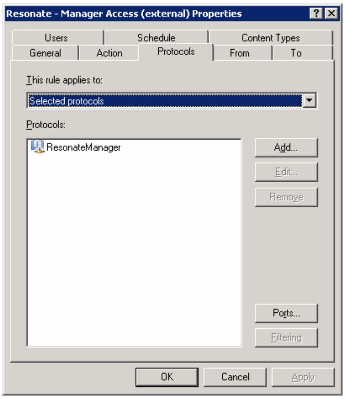
● Allow

○ Deny

□ Redirect HTTP requests to this Web page:

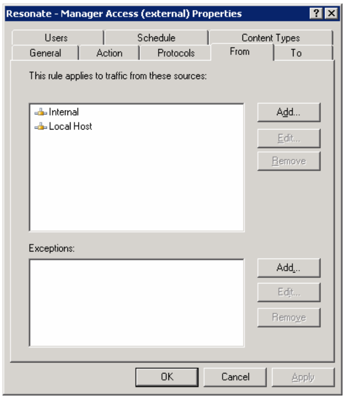
Redirect requests to an alternate Web page. Specify a location in the format http://URL.
For example: http://widgets.microsoft.com/denied.htm.

☑ Log requests matching this rule


Resonate - Manager Access (external) Properties

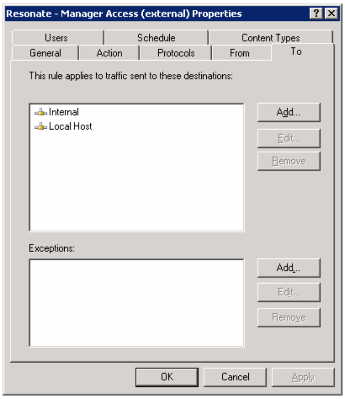
This rule applies to: Selected protocols

Protocols:
ResonateManager


Resonate - Manager Access (external) Properties

This rule applies to traffic from these sources:
Internal
Local Host

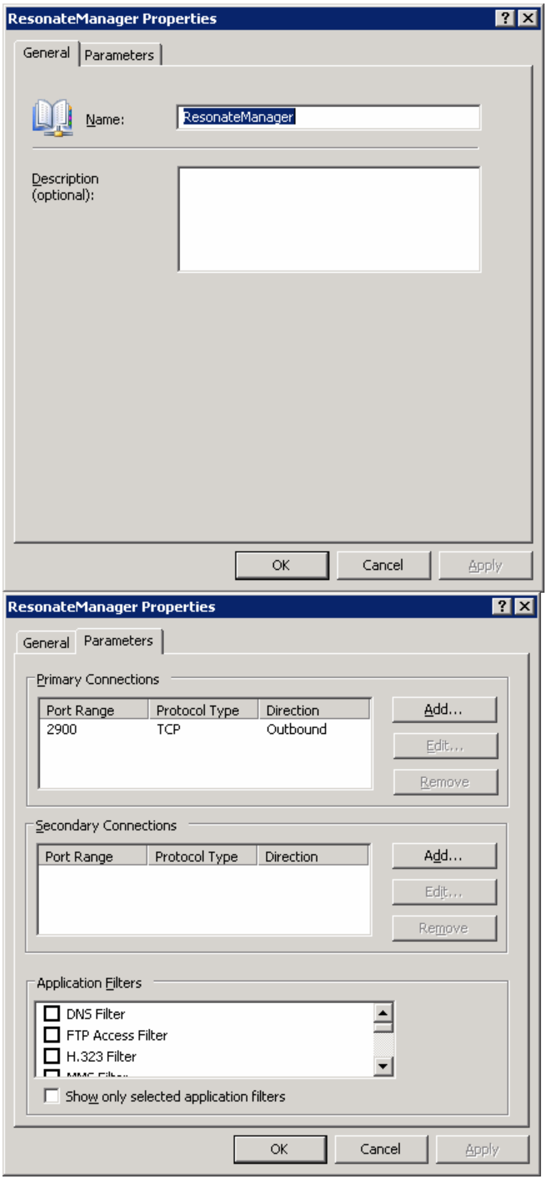
Exceptions:


Resonate - Manager Access (external) Properties

This rule applies to traffic sent to these destinations:
Internal
Local Host

Exceptions:

Define the rule using the above screens. Any screens not shown, use the system defaults. The system will prompt for a protocol defintion not defined yet, this is show below.



ResonateManager Properties

Name: ResonateManager

Description (optional):

ResonateManager Properties

Primary Connections

Port Range	Protocol Type	Direction
2900	TCP	Outbound

Secondary Connections

Port Range	Protocol Type	Direction

Application Filters

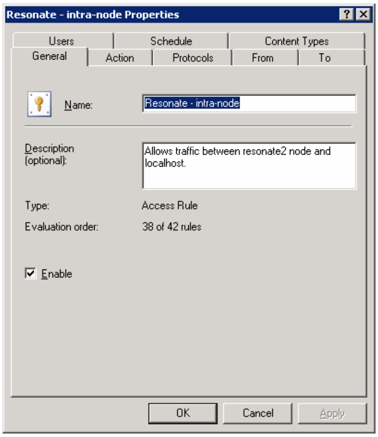
- ☐ DNS Filter
- ☐ FTP Access Filter
- ☐ H.323 Filter
- ☐ MMS Filter

☐ Show only selected application filters

The definition for the ResonateManager protocol.

Resonate Intra-Node Access Rules

This rule opens up traffic between nodes on the IAG cluster.



Resonate - intra-node Properties

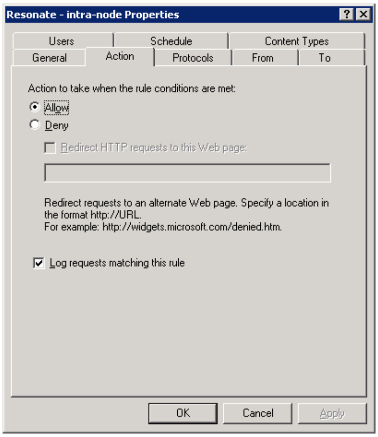
Name: Resonate - intra-node

Description (optional): Allows traffic between resonate2 node and localhost.

Type: Access Rule

Evaluation order: 38 of 42 rules

☑ Enable



Resonate - intra-node Properties

Action to take when the rule conditions are met:

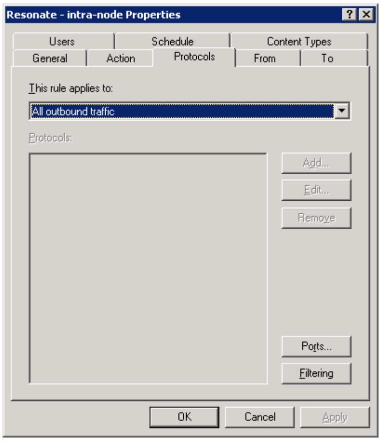
● Allow

○ Deny

□ Redirect HTTP requests to this Web page:

Redirect requests to an alternate Web page. Specify a location in the format http://URL.
For example: http://widgets.microsoft.com/denied.htm.

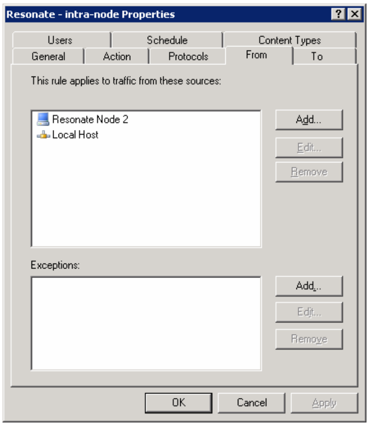
☑ Log requests matching this rule



Resonate - intra-node Properties

This rule applies to: All outbound traffic

Protocols:

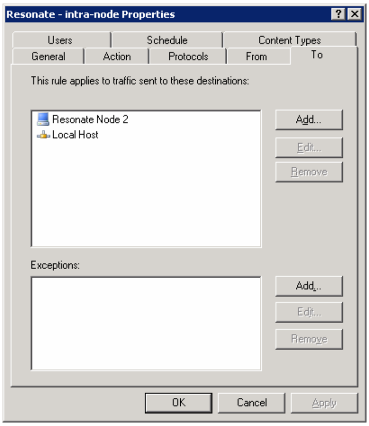


Resonate - intra-node Properties

This rule applies to traffic from these sources:

Resonate Node 2
Local Host

Exceptions:



Resonate - intra-node Properties

This rule applies to traffic sent to these destinations:

Resonate Node 2
Local Host

Exceptions:

Any screens which are not shown, take the system defaults.

Add each of the Resonate nodes of the cluster in this rule defintion. If you add the node as well as the “local host” network, you will be able to export this rule and import it into any of the other nodes in the cluster.

Create a VIP DNS entry on your network

The VIP is a virtual address which is a single address shared by all nodes on the IAG cluster. This will be the only address which is visable to remote clients which access IAG.

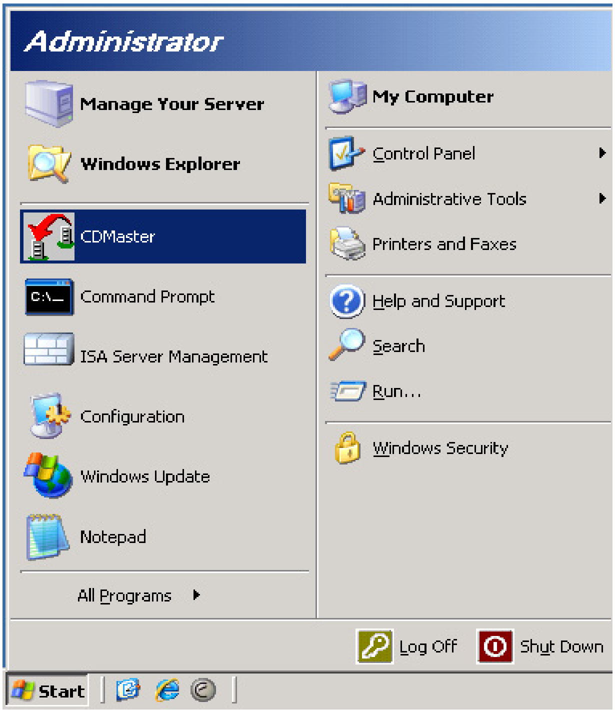
A DNS entry must be created which is available to external clients to access the IAG published applications. This DNS entry will be required for the configuration of the IAG portal trunks.

The DNS entry for the examples show is VIP.nappliance.com.

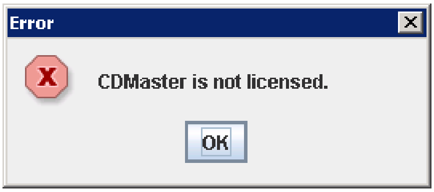
Note: you can use host file entrys for lab setups, but these host entries must be entered into each client and IAG node in your lab.

Configure Resonate CD

Select any mIAG node on the cluster, and run the CD Master program entry on the start menu.

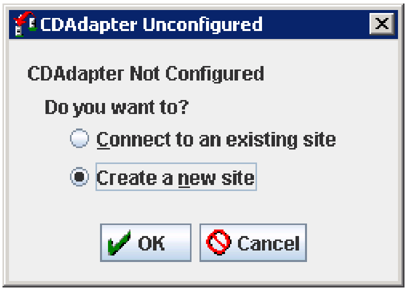


The following window will appear the first time.



CDMaster is not licensed.

Click OK to continue.



CDAdapter Unconfigured

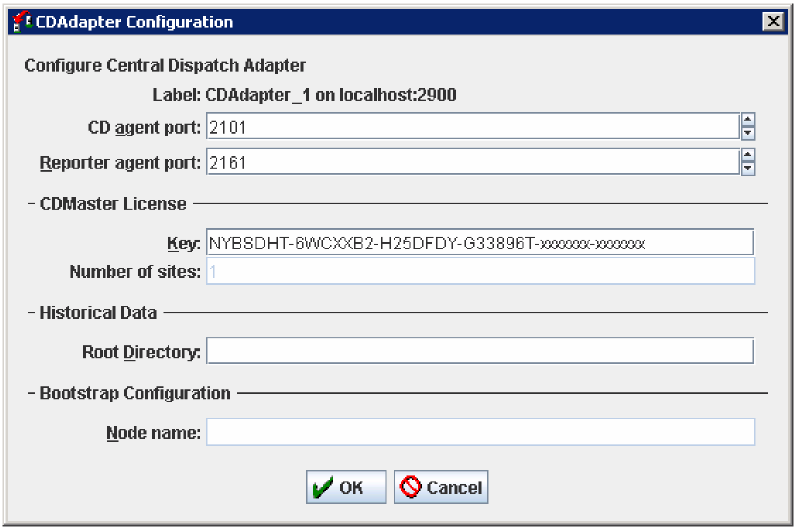
CDAdapter Not Configured

Do you want to?

○ Connect to an existing site

● Create a new site

On the next window, select “Create a new site”.



CDAdapter Configuration

Configure Central Dispatch Adapter

Label: CDAdapter_1 on localhost:2900

CD agent port: 2101

Reporter agent port: 2161

- CDMaster License

Key: NYBSDHT-6WCXXB2-H25DFDY-G33896T-xxxxxxx-xxxxxxx

Number of sites: 1

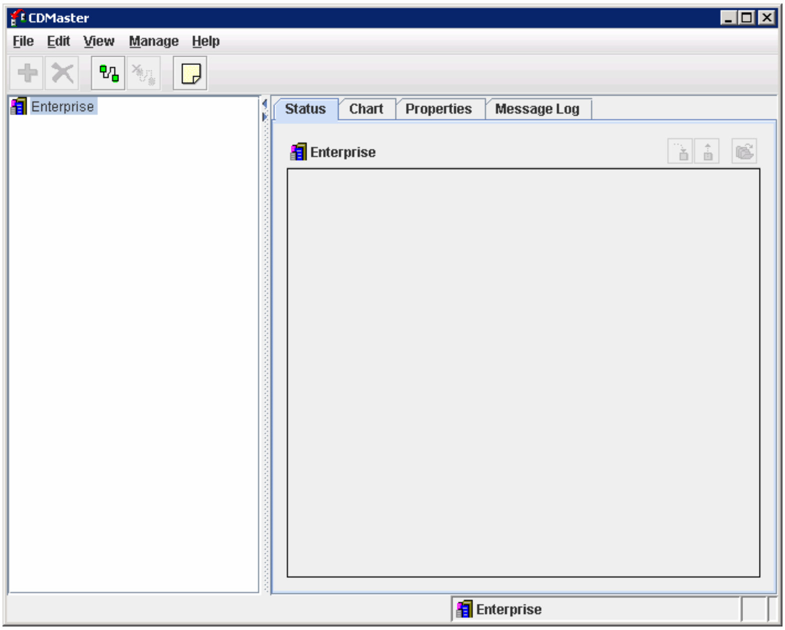
- Historical Data

Root Directory:

- Bootstrap Configuration

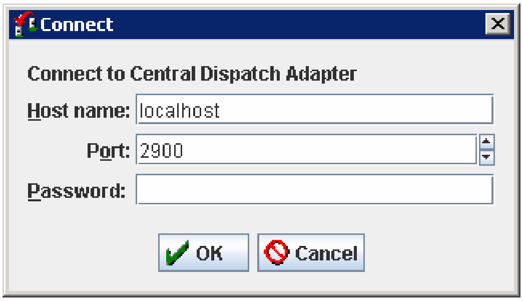
Node name:

To create the new configuration, the next window will appear. This window will require the CD Master License key. This key should have been shipped to you. If this is not available, contact your nAppliance sales representative.



The initial screen will appear. This is a CD Master management screen. You will now need to connect to a CD Adapter. There is a CD Adapter on each IAG node in the cluster. The CD Adapter syncronizes the Resonate CD configuration and statistics among each node on the cluster.

Click on the Connect Button at the top of the screen. The next screen should appear.



Connect to Central Dispatch Adapter

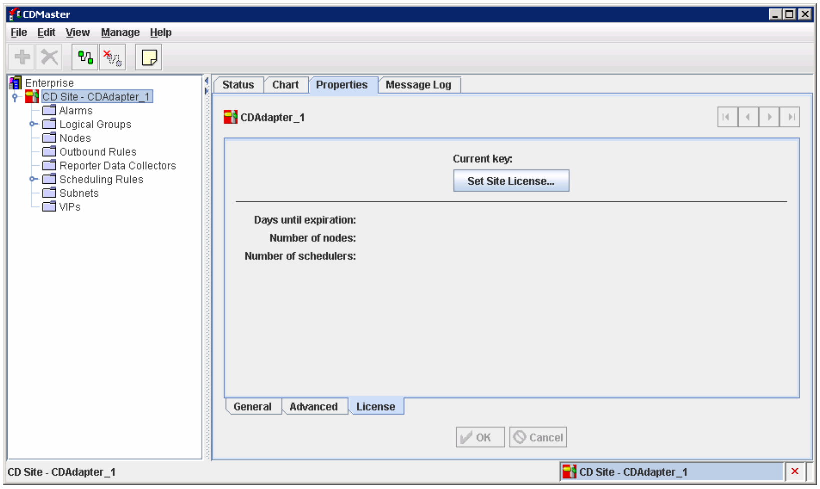
Host name: localhost

Port: 2900

Password:

Connect to the localhost on this system. Select the Password of the ResAdmin account and press OK.

Enter the site license. Each Resonate IAG cluster needs a site license key. This key should have been provided to you with the shipment. If you do not have this key, contact support@nappliance or your nAppliance sales representative.



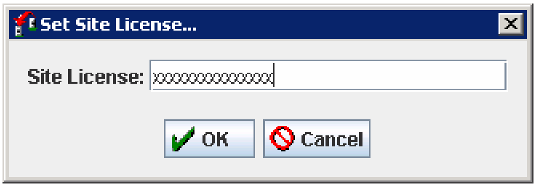
Current key:

Days until expiration:

Number of nodes:

Number of schedulers:

Select the CD Site in the panel on the left.
Select the Properties tab.
Click on the Set Site License.

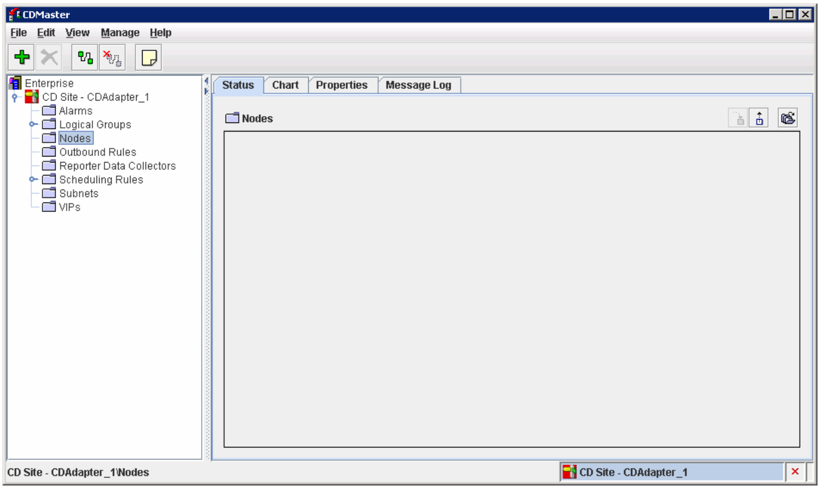


Site License: xxxxxxxxxxxxxxx

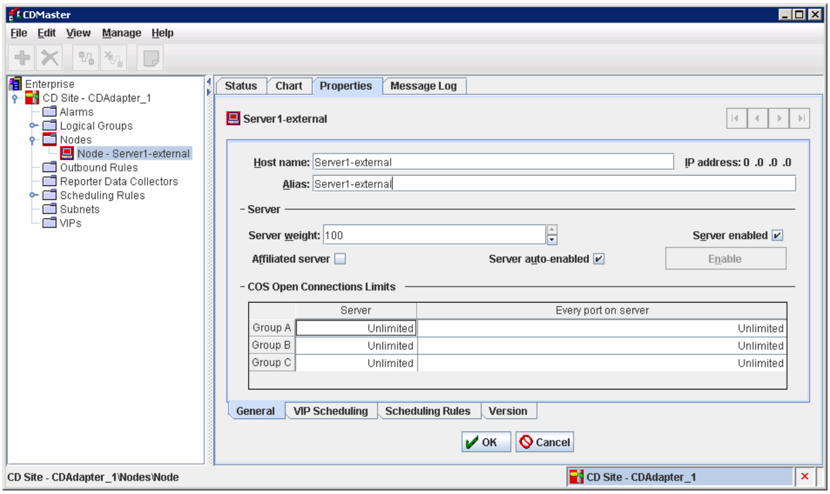
Enter the Resonate CD site license key and press OK.

The license statistics will not display correctly until later when the cluster is started.

Define each node of the IAG cluster.



Select “Nodes” on the left panel, then press the Green Plus (+) key at the top of the screen.



Host name: Server1-external IP address: 0 .0 .0 .0

Alias: Server1-external

Server

Server weight: 100

Server enabled ☑

Affiliated server □

Server auto-enabled ☑

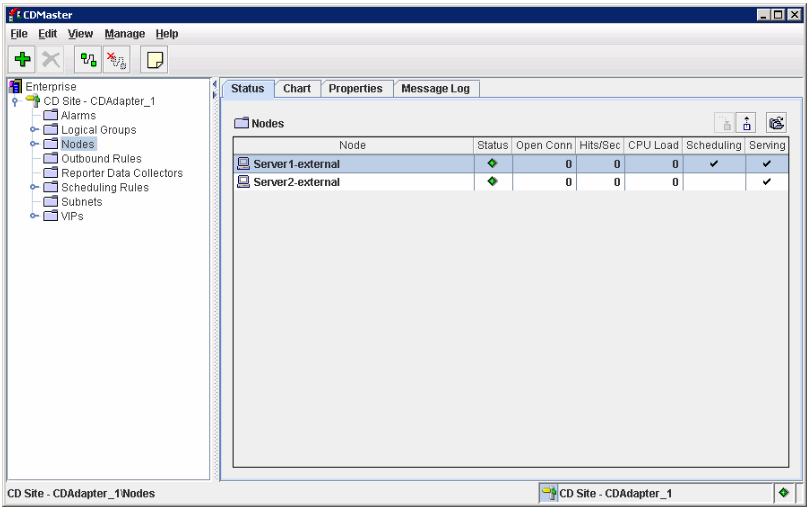
COS Open Connections Limits

	Server	Every port on server
Group A	Unlimited	Unlimited
Group B	Unlimited	Unlimited
Group C	Unlimited	Unlimited

Enter the DNS node name in the "Host name" field. Press OK.

Repeat this process for each node in your cluster.

If you select Manage -> Start from the top menu, the cluster should start at this point.

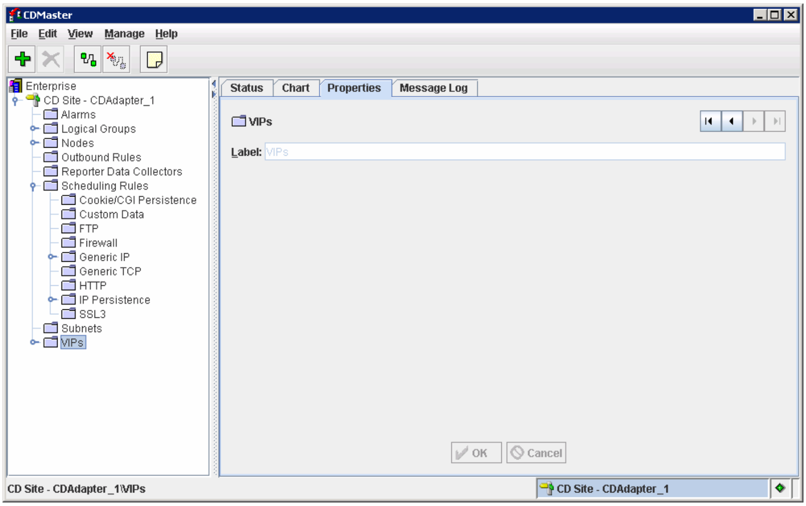


Node	Status	Open Conn	Hits/Sec	CPU Load	Scheduling	Serving
Server1-external	◆	0	0	0	✓	✓
Server2-external	◆	0	0	0		✓

If you select the “Status” tab, you should see each node in your cluster. The green status and the statistics shows that Resonate CD Agents are communicating with the CD Adapter, and you have a cluster working.

At this stage, it would be useful to check the ISA Logging mechanism to make sure each system is working and that there are not firewall Denied messages. This is a common issue. ISA rules must be working correctly for the cluster to operate.

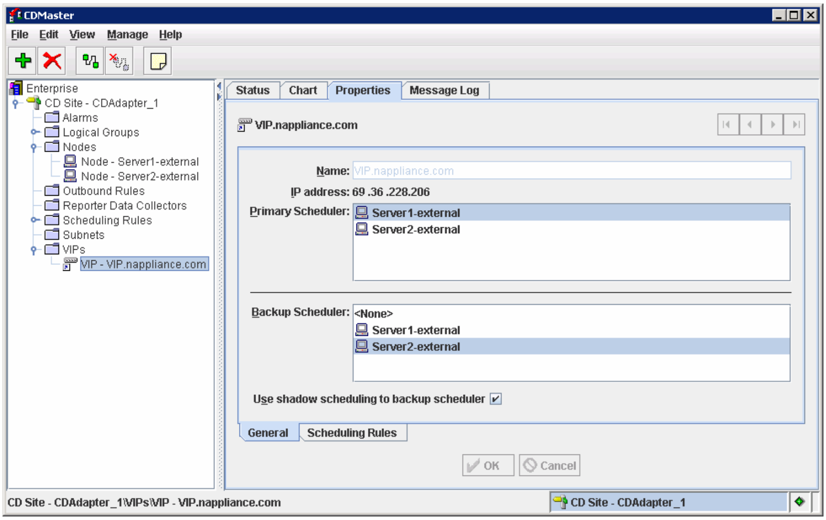
Configure the VIP entry



Label: VIPs

CD Site - CDAdapter_1\VIPs

Select the VIP entry on the left panel, and select the Properties Tab.



Name: VIP.nappliance.com

IP address: 69 .36 .228.206

Primary Scheduler: Server1-external, Server2-external

Backup Scheduler: <None>, Server1-external, Server2-external

Use shadow scheduling to backup scheduler ☑

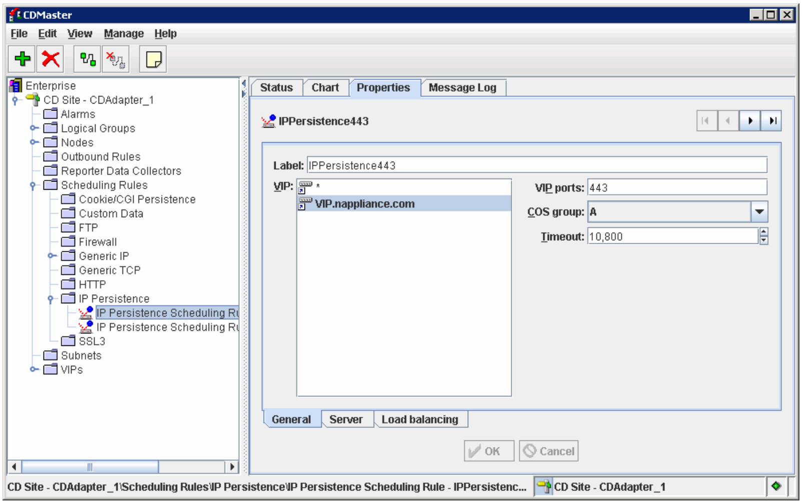
CD Site - CDAdapter_1\VIPs\VIP - VIP.nappliance.com

Define the Primary Scheduler node and the Backup Scheduler Node. The scheduler will be responsible for processing incoming traffic for all the nodes, and will dispatch this traffic to the other nodes in the cluster. Each node in the cluster will then respond back to the remote client directly, and will not communicate traffic back through the scheduler node.

The Backup scheduler will take over the scheduling operation if the primary scheduler node fails.

Press OK. Attaching nodes to the VIP is node later.

Create the IP Persistance Rule



Label: IPPersistence443

VIP: *
VIP.nappliance.com

VIP ports: 443

COS group: A

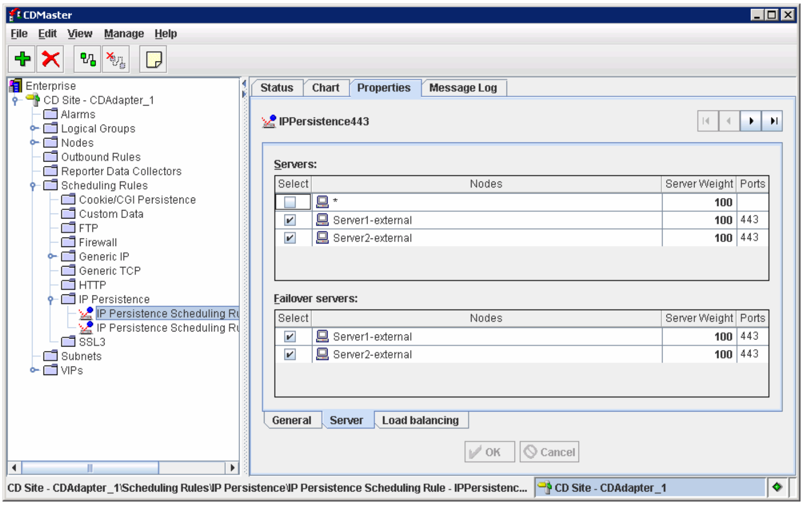
Timeout: 10,800

CD Site - CDAdapter_1\Scheduling Rules\IP Persistence\IP Persistence Scheduling Rule - IPPersistenc...

Select IP Persistence and press the Green Plus button at the top of the screen.

Next, create an IP Persistence rule for ports 80 and 443. Traffic flowing through both of these ports from a single client will be bound to the same session. If an application switches between 80 and 443 during the same HTTP session, this will persist to the same IAG node.

Create both IP Persistence rule similar to the above screen. Select a long timeout so that the IAG Session manager can manage session timeouts , and Resonate CD will not timeout the session underneath IAG.



Servers:

Select	Nodes	Server Weight	Ports
□	*	100	
☑	Server1-external	100	443
☑	Server2-external	100	443

Failover servers:

Select	Nodes	Server Weight	Ports
☑	Server1-external	100	443
☑	Server2-external	100	443

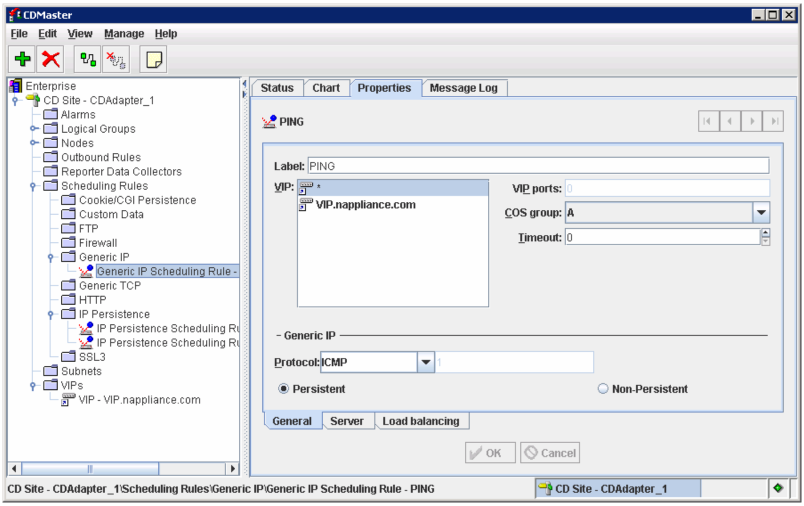
On the Server Tab (at the bottom of the right panel on the Properties tab), select all the IAG servers for both the Servers group, and for the Failover servers.

Note: All IAG nodes must be selected on the Failover servers group, or failover will not occur correctly. This is only necessary for the Persistant type sessions.

Click OK to save the IP persistent rules.

Optional PING Rule

It may be useful to create a PING rule for testing and troubleshooting connectivity.
To enable PINGS via Resonate:



Label: PING

VIP: *
VIP.nappliance.com

VIP ports: 0

COS group: A

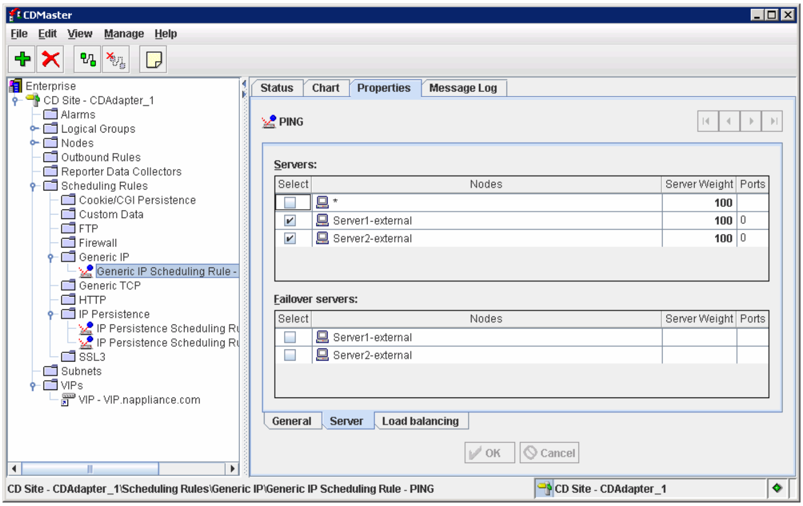
Timeout: 0

Protocol: ICMP 1

● Persistent ○ Non-Persistent

CD Site - CDAdapter_1\Scheduling Rules\Generic IP\Generic IP Scheduling Rule - PING

Select a Generic IP rule at the left, then click on the Green Plus.



Servers:

Select	Nodes	Server Weight	Ports
□	*	100	
☑	Server1-external	100	0
☑	Server2-external	100	0

Failover servers:

Select	Nodes	Server Weight	Ports
□	Server1-external		
□	Server2-external		

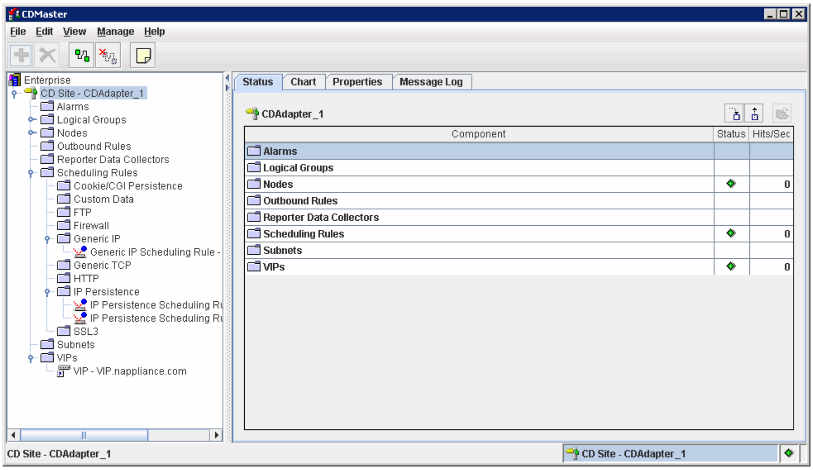
CD Site - CDAdapter_1\Scheduling Rules\Generic IP\Generic IP Scheduling Rule - PING

CD Site - CDAdapter_1

Select only the Servers in the IAG cluster and press OK.

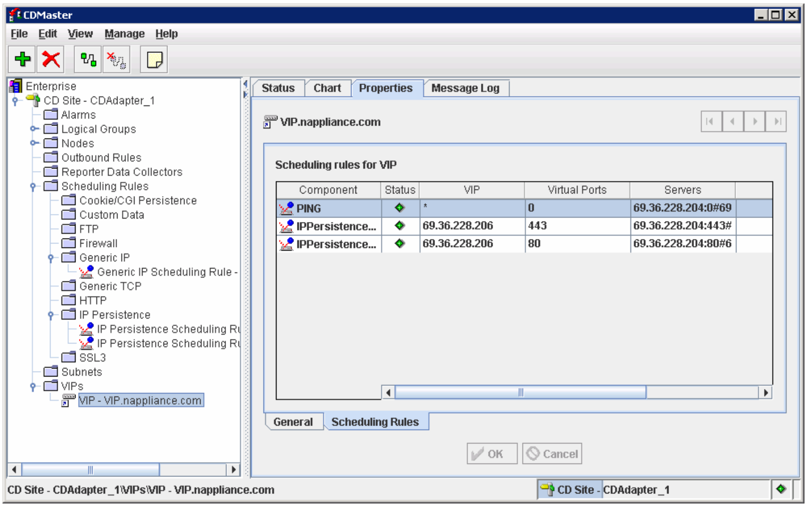
Start the CD Cluster

Select Manage then Start to start the IAG cluster (if not already started).



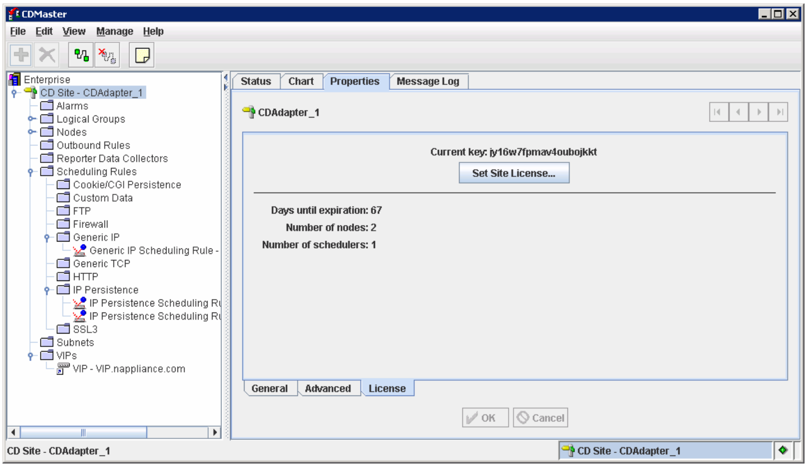
Component	Status	Hits/Sec
Alarms		
Logical Groups		
Nodes	◆	0
Outbound Rules		
Reporter Data Collectors		
Scheduling Rules	◆	0
Subnets		
VIPs	◆	0

The configured rules should show a green status and the statistics should be displayed.



Component	Status	VIP	Virtual Ports	Servers
PING	◆	*	0	69.36.228.204:0#69
IPPersistence...	◆	69.36.228.206	443	69.36.228.204:443#
IPPersistence...	◆	69.36.228.206	80	69.36.228.204:80#6

The VIP Properties should display each configured cluster rule.



Current key: jy16w7fpmav4oubojkkt

Days until expiration: 67

Number of nodes: 2

Number of schedulers: 1

The license statistics should display correctly.

Configure IAG Trunks

The IAG systems only require minor configuration.

Configure portal trunks, using the Trunk IP address as the physical IP address of the External Interface of each IAG system. The Trunk Hostname should be defined using the DNS hostname of the VIP address.

This causes IAG to communicate to client systems, which use the application URL of the VIP address, and the IAG system responds to the application, also using the correctl URL.

The client communicates with the VIP IP address, but the IAG systems interact with their respective IAG External IP interfaces, which is translated back to the VIP address by Resonate CD.