



Sygate Network Access Control 5.0 MR2 Quick Start Guide

*Documentation Build 9501
Published July 15, 2005*

Copyright Information

Copyright © 2005 Sygate Technologies, Inc. and its licensors. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means, electronic, mechanical, or otherwise, without prior written permission of Sygate Technologies, Inc. Information in this document is subject to change without notice and does not constitute any commitment on the part of Sygate Technologies, Inc. Sygate Technologies, Inc. may have patents or pending patent applications, trademarks, copyrights, and other intellectual property rights covering the subject matter of this document.

Furnishing of this documentation does not in any way grant you license to these patents, trademarks, copyrights, or any other intellectual property of Sygate Technologies, Inc.

Sygate, the Sygate 'S' Logo, Sygate Enterprise Protection, and Sygate Network Access Control, Host Integrity, and AutoLocation Switching are registered trademarks or trademarks of Sygate Technologies, Inc.

All other companies and product names are trademarks or registered trademarks of their respective holders.

Portions derived from Java and XSLT by Eric M. Burke. Copyright © 2001 O'Reilly & Associates.

Portions copyright © 2001-2003 INCORS GmbH - All rights reserved.

Portions include software under the following terms:

Copyright © 1995-2001 International Business Machines Corporation and others.

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS

OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

This product includes software developed by the Apache Software Foundation <<http://www.apache.org>>. Copyright © 1999, 2000 The Apache Software Foundation. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgement:

"This product includes software developed by the Apache Software Foundation <<http://www.apache.org/>>."

Alternately, this acknowledgement may appear in the software itself, if and wherever such third-party acknowledgements normally appear.

4. The names "Xerces", "The Jakarta Project", "Tomcat", and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact <apache@apache.org>.

5. Products derived from this software may not be called "Apache" nor may "Apache" appear in their names without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes software developed by the MX4J project (<http://mx4j.sourceforge.net>), copyright © 2001 MX4J. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the MX4J project (<http://mx4j.sourceforge.net>)." Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names "MX4J" and "mx4j" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact biorn_steedom@users.sourceforge.net.
5. Products derived from this software may not be called "MX4J", nor may "MX4J" appear in their name, without prior written permission of Simone Bordet.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL CARLOS QUIROZ OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright © 2005 Sygate Technologies, Inc. and its licensors. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means, electronic, mechanical, or otherwise, without prior written permission of Sygate Technologies, Inc. Information in this document is subject to change without notice and does not constitute any commitment on the part of Sygate Technologies, Inc. Sygate Technologies, Inc. may have patents or pending patent applications, trademarks, copyrights, and other intellectual property rights covering the subject matter of this document.

Furnishing of this documentation does not in any way grant you license to these patents, trademarks, copyrights, or any other intellectual property of Sygate Technologies, Inc.

Sygate, the Sygate 'S' Logo, Sygate Enterprise Protection, Sygate Network Access Control, Host Integrity, and AutoLocation Switching are registered trademarks or trademarks of Sygate Technologies, Inc.

All other companies and product names are trademarks or registered trademarks of their respective holders.

Portions copyright © 1995 Martin Schulze. For a period of three years from receipt of this notice, Sygate shall, at your request, provide a copy of the pidfile.c source code at a fee equaling Sygate's reproduction cost.

Portions include software under the following terms:

Copyright © 1995-2002 World Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. This program is distributed under the W3C's Intellectual Property License.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See W3C License <http://www.w3.org/Consortium/Legal/> for more details. This work (and included software, documentation such as READMEs, or other related items) is being provided by the copyright holders under the following license. By obtaining, using and/or copying this work, you (the licensee) agree that you have read, understood, and will comply with the following terms and conditions:

Permission to copy, modify, and distribute this software and its documentation, with or without modification, for any purpose and without fee or royalty is hereby granted, provided that you include the following on ALL copies of the software and documentation or portions thereof, including modifications:

1. The full text of this NOTICE in a location viewable to users of the redistributed or derivative work.
2. Any pre-existing intellectual property disclaimers, notices, or terms and conditions. If none exist, the W3C Software Short Notice should be included (hypertext is preferred, text is permitted) within the body of any redistributed or derivative code.
3. Notice of any changes or modifications to the files, including the date changes were made. (We recommend you provide URIs to the location from which the code is derived.)

THIS SOFTWARE AND DOCUMENTATION IS PROVIDED "AS IS," AND COPYRIGHT HOLDERS MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, WARRANTIES OF

MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

COPYRIGHT HOLDERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE SOFTWARE OR DOCUMENTATION.

The name and trademarks of copyright holders may NOT be used in advertising or publicity pertaining to the software without specific, written prior permission. Title to copyright in this software and any associated documentation will at all times remain with copyright holders.

Table of Contents

Preface	ix
Related Documentation	ix
Intended Audience.....	ix
Chapter 1. Preparing for the Installation	1
System Requirements for the Policy Manager	2
Hardware Requirements	2
Software Requirements	3
Installation Requirements	3
Database Requirements	3
Sygate Embedded Database Requirements	3
Microsoft SQL Server Requirements	3
System Requirements for the Agent Software	5
Hardware Requirements	5
Software Requirements	5
Sygate Software Installation Overview	5
Step 1: Check the Machine Prerequisites	5
Step 2: Install the Policy Manager and Configure the Database.....	6
Configuring the Policy Manager Database	6
Step 3: Set Up the Organizational Structure.....	6
Step 4: Create Security Policies.....	7
Step 5: Deploy and Install the Agent Software	7
Policy Manager Communication Ports	8
Chapter 2. Installing the Policy Manager Software	9
Using the Server Configuration Assistant	10
Configuring the Name, Port, and Data Root	11
Site Type.....	12
Database Server Choice	13
Setting Up a Microsoft SQL Database	14
Setting Up an Embedded Database	17
Setting Up Replication (Optional)	17
Logging in to the Policy Manager for the First Time	21
Understanding Administrator Accounts	21
Adding System Administrators.....	21
Getting Started with the Policy Manager.....	22
Working on the Policy Manager	23
Trees.....	24
Monitoring Tree.....	24
Policies Tree	25
Client Manager Tree.....	25
Servers Tree.....	25
Administrators Tree	26

Chapter 3. Setting Up the Organizational Structure.....	27
About Groups.....	28
Replication of Groups Between Sites	28
Adding a Group	29
About Users and Computers.....	29
Importing Users from an LDAP Server.....	30
Searching for Users on an LDAP Server	30
Importing Users from LDAP Server Search Results	32
Chapter 4. Creating Security Policies	33
About Locations.....	33
About Host Integrity Policies.....	34
Where to Develop Host Integrity Policies.....	35
Creating a Location with Default Policies	35
Creating a Policy in the Policy Library.....	38
Chapter 5. Installing Agent Machines	43
About Packages and Deploying the Agent.....	43
Exporting a Package for Deployment.....	44
Installing the Agent Software	46
Chapter 6. Enforcers (Optional)	47
Enforcer Installation Task List	47

List of Tables

Table 1.	Policy Manager Defaults: Listening Ports	8
Table 2.	LDAP Search Attributes	31

List of Figures

Figure 1.	Sygate Network Access Control Components	2
Figure 2.	Policy Manager Opening Screen.....	22
Figure 3.	Policy Manager User Interface	24
Figure 4.	Sample Group Tree Hierarchy	27

Preface

This guide is designed to walk you through the basic installation and setup of the Sygate Network Access Control software. It includes information on the installation of the Policy Manager and Agent software. There are also overviews and instructions on how to set up basic aspects of the Policy Manager such as groups, users, locations, and security settings.

Related Documentation

You have access to the following documents for additional reference:

- *Online Help*—All components of Sygate Network Access Control have help files. These help files provide the same information as the printed documentation, which is available in PDF format from Sygate. Refer to the Readme for links to the documentation.
- *Sygate Policy Manager Installation Guide*—Describes how to install the Policy Manager and set up replication (PDF format).
- *Sygate Policy Manager Administration Guide*—Describes how to configure and administer the Policy Manager and Sygate Enforcement Agent (PDF format).
- *Sygate Enforcer Installation and Administration Guide*—Describes how to install, configure, and administer the Sygate Gateway Enforcer, Sygate LAN Enforcer, and the Sygate DHCP Enforcer (PDF format).
- *Sygate Enforcement Agent User Guide*—Describes how to use the Sygate Enforcement Agent (PDF format).

Intended Audience

This document is written for anyone who needs to quickly set up a working Sygate Network Access Control system for testing. You should have a good understanding of networking and system security, and you should be familiar with the networking environment of the company.

Chapter 1. Preparing for the Installation

There are specific prerequisites for both the Policy Manager machines and the Agent machines. Make sure you have met all the system requirements and prerequisites in this chapter before you start installing the Policy Manager.

You can print the installation overview included in this chapter for use as a step-by-step list. When needed, you can refer to the other sections in this guide for additional detail about a particular step.

Sygate Network Access Control provides three main software components that work together to protect your company computers and corporate network from security threats.

- **Sygate Policy Manager**—The management center for the Sygate software, where you create policies and assign them to Agents
- **Sygate Enforcement Agents**—Software that you deploy to company computers to monitor policies and automate restoration of compliance to policies
- **Sygate Enforcers** (optional)—Software that provides additional enforcement of policy compliance by monitoring network access; there are three types available: Gateway Enforcer, LAN Enforcer, and DHCP Enforcer

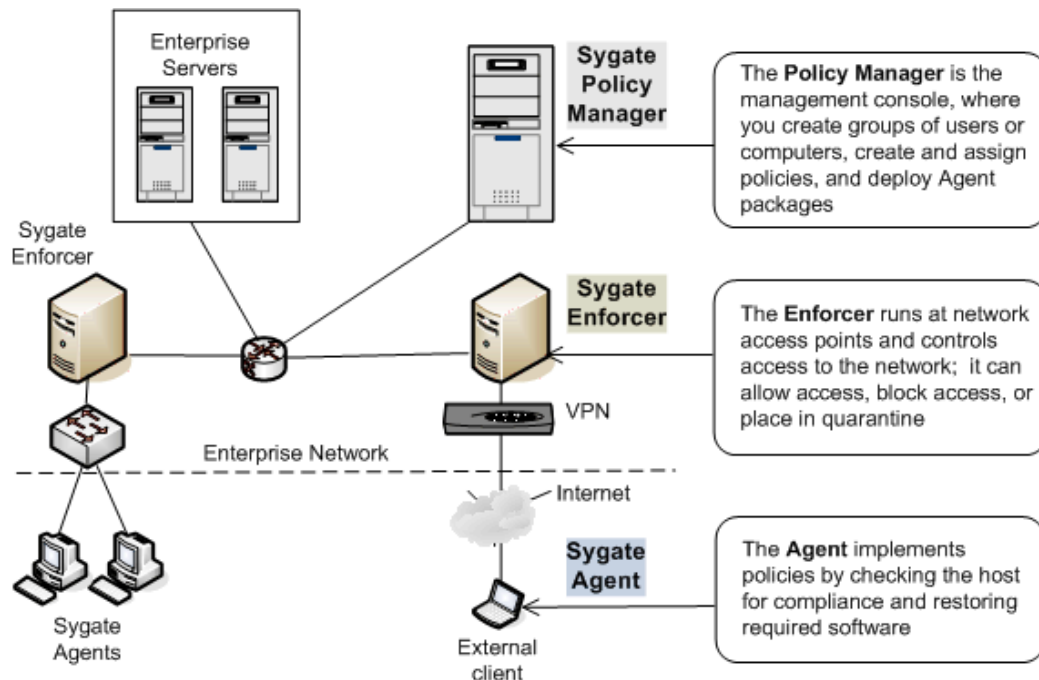


Figure 1. Sygate Network Access Control Components

System Requirements for the Policy Manager

Following are the hardware and software requirements for installing the Sygate Policy Manager.

Hardware Requirements

Following are the minimum hardware requirements for the computer on which you plan to install a Policy Manager.

- Pentium 4 2.4 GHz
- 512 MB RAM (2.0 GB RAM if the Policy Manager and database are installed on the same computer)*
- 400 MB hard disk space (note that the system temp folder requires at least 100 MB to hold temporary files)
- Additional disk space (approx. 1 GB) for storing logs and backups (actual disk requirements depend on the number of logs and length of time the logs are kept)
- One (1) Ethernet adapter with TCP/IP installed
- Monitor display: 1024x768 resolution or better

* 768 MB RAM is recommended and more RAM is recommended if you have a large number of users (2000 or more)

Note: If you are installing the Policy Manager on the same computer where a RADIUS server is installed, both the RADIUS server and the Policy

Manager use port 1812 and there may be a conflict. The Policy Manager requires “listen port 1812” to communicate with Enforcers.

Software Requirements

Following are the software requirements for the system on which you plan to install a Policy Manager:

- Windows Server 2003, Standard or Enterprise Edition fully patched
- Internet Information Server (IIS) 5.0 or 6.0 (with World Wide Web services installed)

Note: The Policy Manager requires IIS to be up and running to stay online. If IIS is stopped during maintenance procedures or updates, the Policy Manager service will stop. It will need to be restarted after you restart IIS.

Installation Requirements

If you are installing a Policy Manager, make sure that you have done the following:

- Assigned a static IP address to the computer on which you plan to install a Sygate Policy Manager (strongly recommended)
- Decided whether to install the Policy Manager on the same computer as the database server or a separate one
- Synchronized the system time of any other Policy Managers and database servers

Database Requirements

The Policy Manager uses a database to store information such as security policies, logs, and configuration settings.

Sygate Embedded Database Requirements

If using the Sygate Embedded Database, it has no special requirements. It is installed on the same computer as the Policy Manager.

Microsoft SQL Server Requirements

If you want to create an SQL database to hold data, you will need:

Hardware Requirements

- 1 GB RAM (2 GB RAM if Policy Manager is installed on the same computer)
- 2 GB hard disk space after SQL Server is installed

Software Requirements

- Microsoft SQL Server 2000, Standard or Enterprise Edition (installed locally or remotely) and patched to SP3a
- Microsoft SQL Client (installed locally)

If Microsoft SQL Server is installed on a separate computer from the Policy Manager, you need to install the Microsoft SQL Client on the same computer as the Policy Manager.

Configuration Requirements

These are the SQL Server configuration requirements:

- Select **SQL Server and Windows** authentication (on the Security tab of SQL Server Properties or choose **Mixed Mode** during installation)
- Include TCP/IP as an enabled protocol (SQL Server Network Utility and SQL Server Client Network Utility)
- Set up SQL Server Agent service so it runs automatically upon start up

Enabling Mixed Authentication During SQL Server Installation

Follow the instructions in the Microsoft SQL Database Server documentation to install the Microsoft SQL 2000 Database Server. To work with Sygate, only one setting differs from the default install settings, the Mixed Mode (Windows Authentication and SQL Server Authentication) in the Authentication Mode dialog box.

You must select **Mixed Mode** during the installation of the Microsoft SQL installation. Otherwise, the Policy Manager will not be able to connect to the Policy Manager database on the SQL Server after you complete the installation.

Enabling Mixed Authentication After SQL Server Installation

To enable Mixed Authentication on the SQL Server:

1. Choose **Start | Programs | Microsoft SQL Server | Enterprise Manager**.
2. Expand the tree and select the SQL Server—typically called (local)(Windows NT) in the SQL Server Group.
3. Right-click and choose **Properties**.
4. Select the Security tab.
5. Select **SQL Server and Windows**.
6. Click **OK**.
7. Close the Enterprise Manager (**File | Exit**).

System Requirements for the Agent Software

Below are the minimum hardware and software requirements necessary to successfully run the Sygate Enforcement Agent software on a computer.

Hardware Requirements

- Pentium II 500 MHz or faster
- 128 MB RAM
- 40 MB available hard disk space
- One (1) Ethernet adapter (with TCP/IP installed)

Software Requirements

One of the following operating systems:

- Windows 2000 Professional (with or without SP1-SP4)
- Windows 2000 Server, Advanced Server, and Data Center (with or without SP1-SP4)
- Windows XP Home Edition or Professional (with or without SP1-SP2)
- Windows Server 2003 (with or without SP1)

Sygate Software Installation Overview

Many tasks are involved in successfully setting up Sygate software.

The high-level steps are:

1. Check that all machines meet prerequisites.
2. Install the Policy Manager and configure the database.
3. Set up the organizational structure.
4. Create security policies.
5. Deploy the Agent software on desktops.

The remainder of this Quick Start guide walks you through these steps, which are summarized below.

Step 1: Check the Machine Prerequisites

There are specific prerequisites for both the Policy Manager machines and the Agent machines. You can refer to these sections earlier in this chapter for more information.

- System Requirements for the Policy Manager
- System Requirements for the Agent Software

Step 2: Install the Policy Manager and Configure the Database

Before you begin installing a Policy Manager:

- Be sure you can access the license file provided with the software.
- Log on as a user with **Administrator** privileges.

Follow the instructions in “Installing the Sygate Policy Manager.” The installation wizard walks you through the complete installation.

If using replication, you need the IP address or host name of the Policy Manager on that site. Follow the instructions in “Installing the Sygate Policy Manager.” where you can then skip to “Setting Up Replication” during the installation.

Configuring the Policy Manager Database

Smaller organizations may choose to use the Embedded Database feature that requires no previous set up and is installed on the Policy Manager machine. Many companies, however, will use an SQL server. If you are using SQL, it is required that you install the SQL Server before installing the Policy Manager. You do not need to have installed the database at this point, but you must install SQL Server.

The Microsoft SQL 2000 database and the Microsoft SQL Server software can be physically located locally or remotely. If it is remote, the Microsoft SQL Client must be installed on the same computer as the Policy Manager. You set up the database from the same computer on which you installed the Policy Manager. This is part of the Policy Manager installation.

For details, see:

- “Setting Up a Microsoft SQL Database”
- “Setting Up an Embedded Database”

Step 3: Set Up the Organizational Structure

You can begin Policy Manager configuration by setting up groups for users and computers.

To complete this step, you need a good idea of how you want to set up your groups and users. Many companies mimic their organizational structure, or, import this information from an LDAP server directly. You can learn more about setting up groups, users, and computers by reading the following sections:

- About Organizational Structures
- About Groups
- Adding a Group
- About Users and Computers
- Importing Users from an LDAP Server

Step 4: Create Security Policies

Once you have your group structure in place, you can set up locations and security policies and apply them to the groups.

Customizing policies can be a major task, although you can quickly implement policies using the default policies and templates provided.

The chapter on creating security policies explains how to implement default policies when creating locations as well as add policies to a Policy Library for re-use in multiple locations.

Step 5: Deploy and Install the Agent Software

Once the Policy Manager is installed, you can deploy the Agent software to machines. This is a two step process that includes

- Creating and exporting an installation package(s)
- Running the install package(s) on all Agent machines

The Agent software is deployed by creating an installation package using the Policy Manager. This installation package is exported from the Policy Manager to an install point of your choosing.

Once you create an installation package, you can use your own method to deploy the software on Agent machines. Some companies use tools such as Microsoft's Systems Management Server (SMS) and others create links on a web server where users go to install the software manually.

You can read more about creating packages, exporting packages, and installing the Agent by reviewing these topics.

- About Agents
- About Packages and Deploying the Agent
- Exporting a Package for Deployment
- Installing the Agent Software

Policy Manager Communication Ports

The Policy Manager uses the following communication ports by default.

Table 1. Policy Manager Defaults: Listening Ports

Port Number	Port Type	Description
80	TCP	Communication between the Policy Manager and Agents and Enforcers. Initiated by the Agents.
443	TCP	Optional secured HTTPS communication between a Policy Manager and Agents and Enforcers. Initiated by the Agents.
1433	TCP	Communication between a Policy Manager and a Microsoft SQL Database Server if they reside on separate computers. Initiated by the Policy Manager.
1812	UDP	Communication between a Policy Manager and Enforcers for authenticating unique ID information with the Enforcer. Initiated by the Enforcer.
2638	TCP	Communication between the Embedded Database and the Policy Manager. Initiated by the Policy Manager.
8443	TCP	HTTPS communication between a remote Policy Management Console and the Policy Manager. All login information and administrative communication takes place using this secure port. Initiated by the remote Java or web console.
9090	TCP	Initial HTTP communication between a remote Policy Management Console and the Policy Manager (to display the login screen only). Initiated by the remote web console.
39999	UDP	Communication between the Agents and the Enforcer. This is used to authenticate Agents by the Enforcer. Initiated by the Enforcer.

Chapter 2. Installing the Policy Manager Software

Before you begin installing a Policy Manager:

- Have the Policy Manager connected to a network.
- Be sure you can access the license file provided with the software.
- Log on as a user with Administrator privileges.

To install a Policy Manager:

1. Double-click `snac50.exe` to begin the installation by extracting files. The Welcome screen appears.
2. Click **Next**. The License Agreement appears.
3. Read through the License Agreement. Click **Yes** if you agree with the terms of the license. (If you click **No**, the installation is terminated.) The Choose Destination Location dialog box appears.
4. Choose **Browse** to select a destination folder and click **Next** to continue, or simply click **Next** to accept the default location: `C:\Program Files\Sygate\Sygate Policy Manager`. The Select Program Folder dialog box appears.
5. Choose your program folder or use the default (Sygate Policy Manager). Click **Next** to continue. The Setup Status dialog box appears. It indicates the progress of the installation.
6. When the installation is finished, an information message appears saying the system needs to reboot. Click **OK**. The InstallShield Wizard Complete dialog box appears.
7. Select **Yes, I want to restart my computer now** or **No, I will restart my computer later**. Then click **Finish**.

After the system reboots, the Server Configuration Assistant starts up automatically helping you complete the installation.

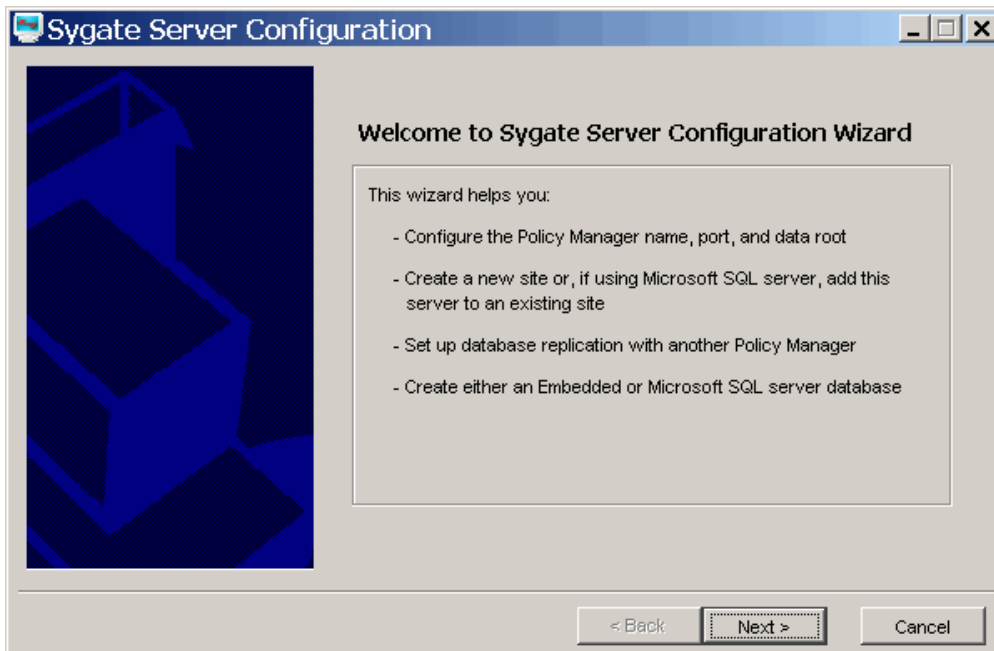
Caution: The installation of the Policy Manager will not be complete until you run the Server Configuration Assistant.

Using the Server Configuration Assistant

Once the Policy Manager is installed and the machine re-boots, it runs the Server Configuration Assistant.

During this process you perform the following actions:

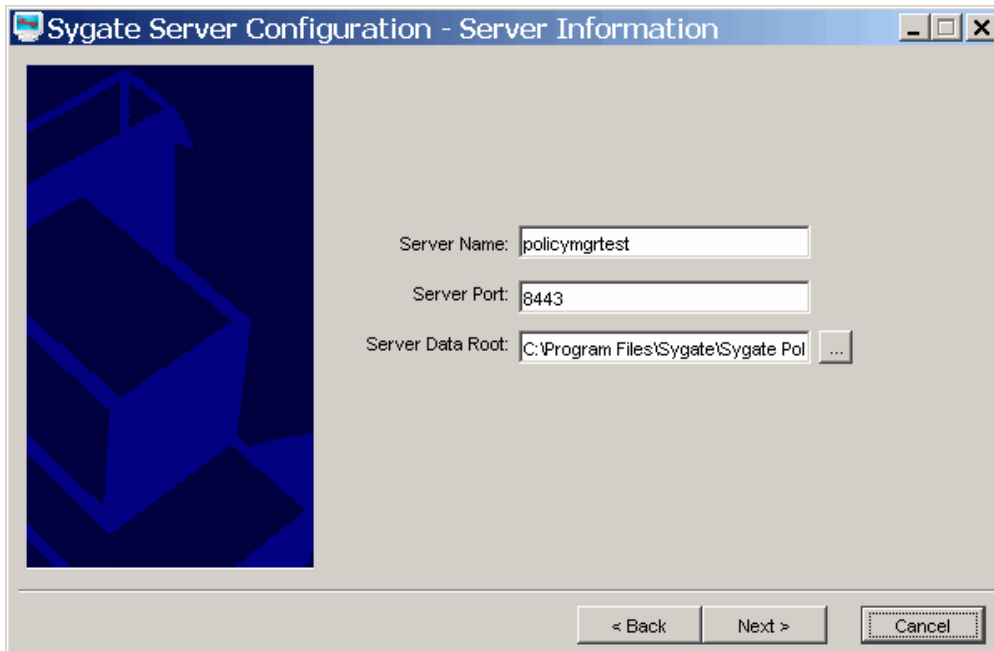
- Configure the name, port, and data root
- Create a new site, or, if using Microsoft SQL Server, add this server to an existing site
- Set up database replication with another Policy Manager if desired
- Navigate to and install the correct license file
- Create either an Embedded or Microsoft SQL database



From the Welcome Screen, click **Next** to continue the configuration.

Configuring the Name, Port, and Data Root

The next dialog box to appear is the Server Information dialog box. You can change the default information in the fields to match your configuration, or, accept the defaults, then click **Next**.



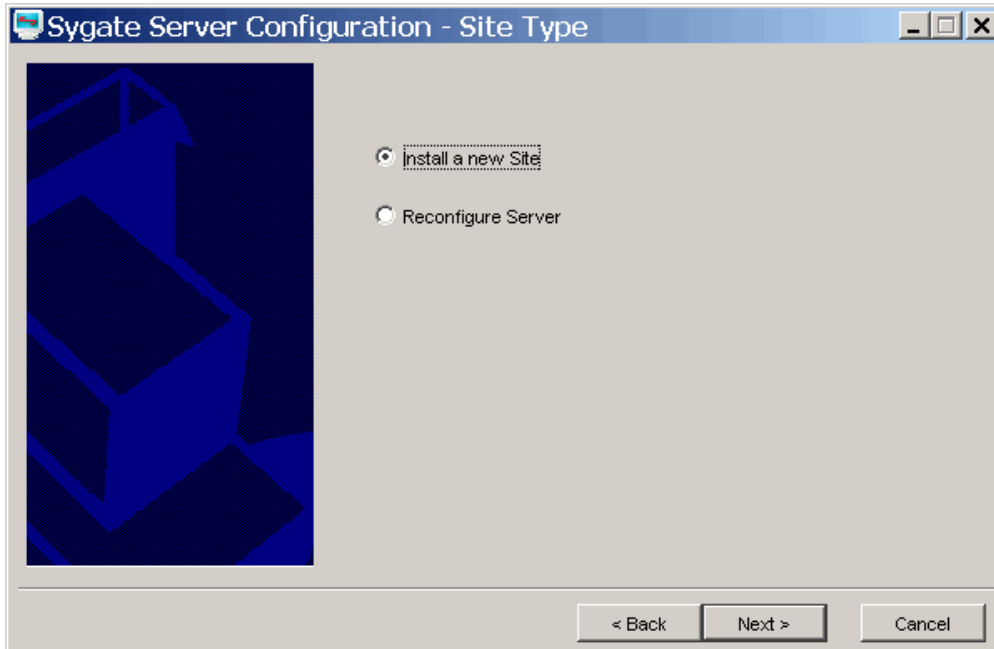
Server Name: Type the name of the computer on which the Policy Manager is installed (default: <local host name>).

Server Port: Type the HTTPS port number the Policy Manager will be listening on (default: 8443).

Server Data Root: Type the root folder where the Policy Manager will place data files such as backups and replication. If you want a customized path, you can browse to the new location. (default: C:\Program Files\Sygate\Sygate Policy Manager\data)

Site Type

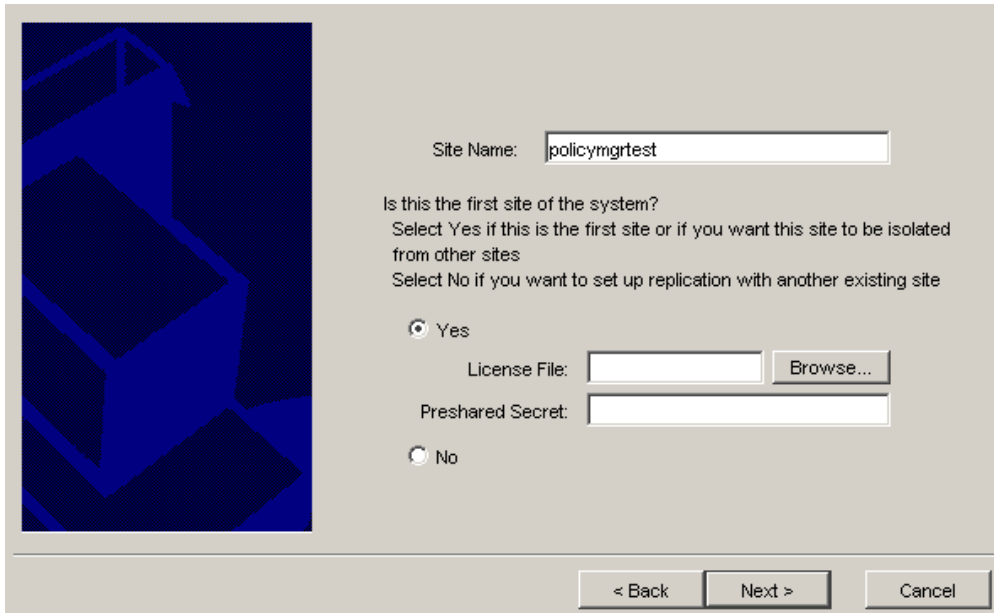
Sygate allows for the creation of multiple sites. You can create a new site when you install the Policy Manager, or, you can add this Policy Manager to an existing site.



Choose “**install a new Site**” and click **Next**.

Note: If you are going to set up replication, skip to “Setting Up Replication” and finish the Configuration Wizard from there.

The Site Information screen appears.



Site Name:

Is this the first site of the system?
Select Yes if this is the first site or if you want this site to be isolated from other sites
Select No if you want to set up replication with another existing site

Yes

License File:

Preshared Secret:

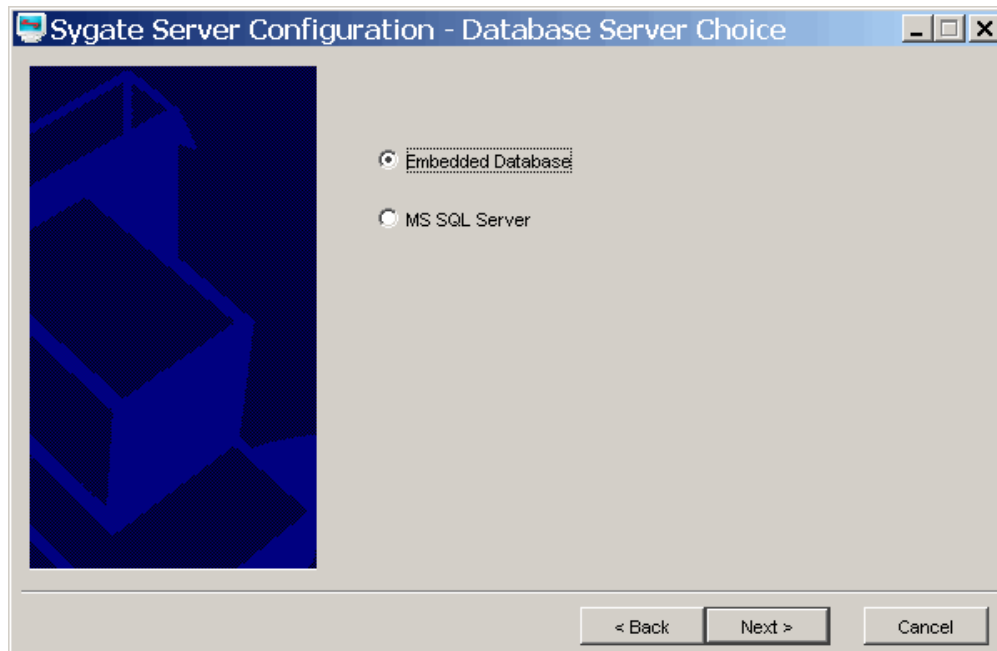
No

< Back Next > Cancel

1. Type in a name for the site.
2. Click **Yes** to create a new site.
3. Navigate to the location where the license file resides to select the file. The Preshared Secret is not required.
4. Click **Next**.

Database Server Choice

Sygate supports two database options. You can use an embedded database, or, you can use a Microsoft SQL database.



From the Database Server Choice dialog box, select your database.

- If you chose a SQL database, go to “Setting Up a Microsoft SQL Database” to finish the wizard.
- If you chose an Embedded database, go to “Setting Up an Embedded Database” to finish the wizard.

Setting Up a Microsoft SQL Database

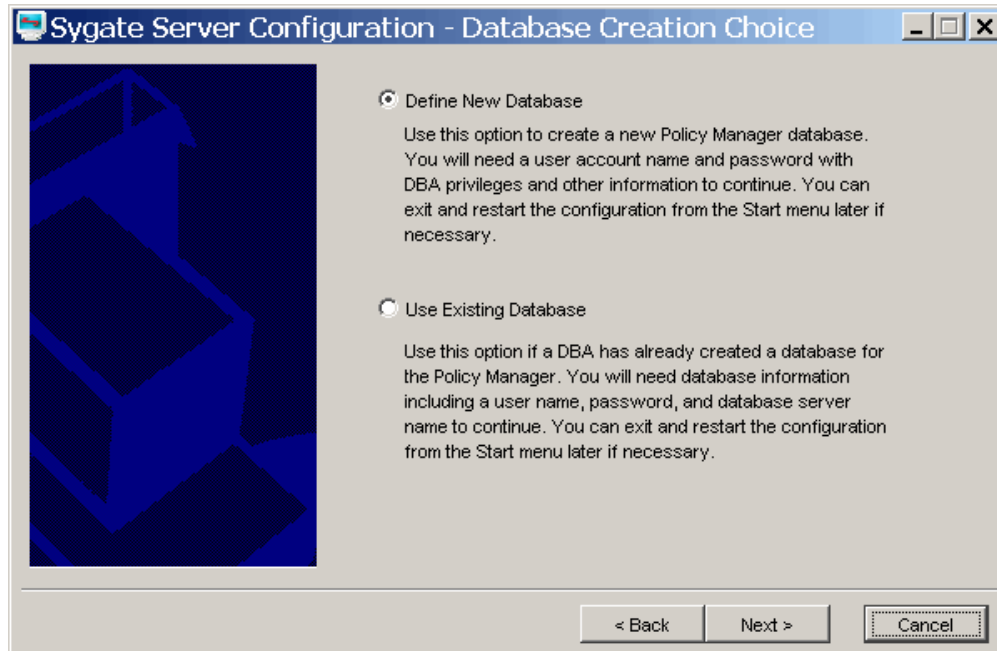
The Microsoft SQL Server can be located on the same computer as the Policy Manager (local) or on another computer (remote). If it is remote, the Microsoft SQL Client must be installed on the same computer as the Policy Manager. You set up the database on the same computer on which you installed the Policy Manager.

During the configuration, you need the following information:

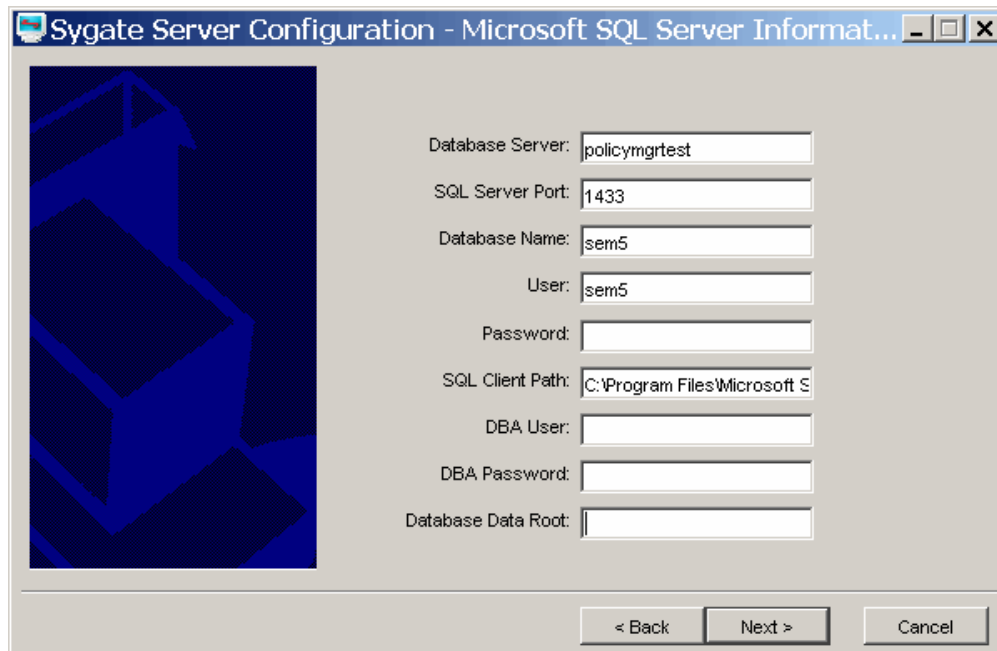
- Host name and IP address of the Microsoft SQL Server.
- Database administrator Login ID and password for the Microsoft SQL Database Server—The Policy Manager needs to create a database on the SQL Server. You will need the Login ID and password during server configuration.
- Database name, user name, and password for the Policy Manager database and database user account that will be automatically created during server configuration.

To set up an SQL database:

1. At the Database Server Choice dialog box, select **MS SQL Server** as the database type.
2. Click **Next**. The Database Creation Choice dialog box appears.



3. Select **Define New Database** to create a new SQL database or **Use Existing Database** to connect to a database that was previously created.
4. Click **Next**. The Microsoft SQL Server Information dialog box appears.



5. In the Microsoft SQL Server Information dialog box, enter:
 - **Database Server:** Host name or IP address of database server where SEM server will save application data. Default: <local host name>
 - **SQL Server Port:** The port configured by Microsoft SQL Server for accepting connections. Default: 1433
 - **Database Name:** The name of SQL database where the Policy Manager will store application data. Default: sem5
Note: If you clicked Define New Database, this database cannot already exist on the SQL Server.
 - **User:** Name of the user responsible for the Policy Manager database; user name is added to the SQL Server. Default: sem5
 - **Password:** Password for the Policy Manager database user.
 - **SQL Client Path:** SQL client bin folder that contains bcp.exe (for example, C:\Program Files\Microsoft SQL Server\80\Tools\Binn).
 - **DBA User:** Database administrator user name (for example, sa); configured on the SQL Server.
 - **DBA Password:** Password of the database administrator; configured on the SQL Server.
 - **Database Data Root:** (for example, C:\Program Files\Microsoft SQL Server\MSSQL\Data).
6. Click **Next**. The Policy Manager database is then created on the SQL Server. This takes a few minutes during which a Configuring database message will appear.
7. On the Configuration Completed dialog, you can choose to **Start Sygate Policy Manager** and **Start Management Console**. These options are selected by default.
8. Click **Finish**. This completes the configuration of the Policy Manager database. The last screen asks if you want to run the Policy Manager. When you launch the Policy Manager you get a log in screen. For details on logging on, see “Logging on to the Policy Manager for the First Time.”

When you have finished setting up the Policy Manager database, you can log on to the Policy Manager, create an organizational structure, and deploy Agents.

Setting Up an Embedded Database

Before you can start the Policy Manager, you must configure a database. Sygate's embedded database is included with the Policy Manager. This is an alternative to using a Microsoft SQL Database.

To set up an embedded database:

1. At the Database Server Choice dialog box in the Configuration Assistant, select **Embedded Database** as the database type (the default) then click **Next**. The Embedded Database Server Information dialog box appears.
2. In the Embedded Database Server Information dialog box, all of the fields are filled in (and can't be changed) except the password field:
 - **Database Server:** Host name or IP address of database server where the Policy Manager will save application data. Set to localhost.
 - **Database Server Port:** The port configured for accepting connections. Set to 2638.
 - **Database Name:** The name of the database where the Policy Manager will store application data. Set to sem5.
 - **User:** Name of the user responsible for the Policy Manager database. Set to DBA.
 - **Password:** Password for the Policy Manager database. Type the DBA password you want to use.
3. Click **Next**. The Policy Manager database is then created on the Policy Manager. This takes a few minutes after which a Configuration Completed dialog appears.
4. On the Configuration Completed dialog, you can choose to **Start Sygate Policy Manager** and **Start Management Console**. These options are selected by default.
5. Click **Finish**. This completes the configuration of the Policy Manager database. The last screen asks if you want to run the Policy Manager. When you launch the Policy Manager you get a log in screen. For details on logging on, see "Logging on to the Policy Manager for the First Time."

When you have finished setting up the Policy Manager database, you can log on to the Policy Manager, create an organizational structure, and deploy Agents.

Setting Up Replication (Optional)

You set up replication during the server configuration phase of the installation. Another site including a Policy Manager must have previously been installed and configured before you can set up replication by adding a new site to the site farm. If you want to add a replication partner between two sites on a site farm, see "Adding Replication Partners." in the Policy Manager online help.

Before you begin, you need to have the following information:

- Name or IP address of the site with which you want to partner
- Administrator name and password of the other site
- Port number of the Policy Manager with which you want to communicate

To set up replication:

1. Go to the computer that you want to set up as a replication partner with an existing Policy Manager.
2. Install the Policy Manager as explained in “Installing the Sygate Policy Manager.”
3. Run the Server Configuration Assistant (started automatically at the end of the Policy Manager installation) or from Windows by selecting **Programs | Sygate Policy Manager | Server Configuration Assistant** on the computer where the Policy Manager is installed. The Server Configuration Welcome dialog appears.
4. Click **Next** to begin the configuration.
5. In the Server Information dialog box, enter:
 - **Server Name:** Type the name of the computer on which the Policy Manager is installed (default: localhost).
 - **Server Port:** Type the HTTPS port number the Policy Manager is listening on (default: 8443).
 - **Server Data Root:** Type the root folder where the Policy Manager places data files including replication and other Policy Manager files or browses to the location. For example, C:\Program Files\Sygate\Sygate Policy Manager\data.
6. Click **Next**.
7. In the Site Type dialog box, select **Install a new site** because replication occurs between two distinct sites.
8. Click **Next**. The Site Information dialog box appears.
9. In the Site Information dialog box, enter:
 - **Site Name:** Specify a name for the site.
 - Click **No** to indicate that this is not the first site being installed on the network.
10. Click **Next**. The Replication Information dialog box appears.
11. Enter the following information to identify the remote site that you want to set up as a replication partner:
 - **Replication Server Name:** Type the host name or IP address of the remote Policy Manager with which you want to replicate data.
 - **Replication Server Port:** Specify the HTTPS port of the remote Policy Manager (8443 by default). This is specified during installation.

- **Administrator Name:** Type the user name of the administrator on the remote Policy Manager.
 - **Password:** Type the administrator password of the remote Policy Manager.
12. Click **Next**. The Database Server Choice dialog box appears.
13. Select the type of database you want to create on the local Policy Manager (**Embedded Database** or **MS SQL Server**).
14. If you selected **Embedded Database**, in the Embedded Database Server Information dialog box, enter (some information will be automatically filled in for you):
- **Database Server:** Host name or IP address of database server where the Policy Manager will save application data. Information is automatically entered into this field and it cannot be modified.
 - **Database Server Port:** The port configured by Microsoft SQL Server for accepting connections. Default value: 1433. Information is automatically entered into this field and it cannot be modified.
 - **Database Name:** The name of SQL database where the Policy Manager will store application data. Information is automatically entered into this field and it cannot be modified.
 - **User:** Name of the user responsible for this Policy Manager database. Information is automatically entered into this field and it cannot be modified.
 - **Password:** Password for the Policy Manager database user.
15. If you selected MS SQL Database, in the SQL Database Server Information dialog box, enter (some information will be automatically filled in for you):
- **Database Server:** Host name or IP address of database server where the Policy Manager will save application data.
 - **SQL Server Port:** The port configured by Microsoft SQL Server for accepting connections. Default value: 1433.
 - **Database Name:** The name of SQL database where the Policy Manager will store application data.
 - **User:** Name of the user responsible for this Policy Manager database; the user name is added to the SQL Server.
 - **Password:** Password for the Policy Manager database user.
 - **SQL Client Path:** SQL client bin folder that contains bcp.exe (for example, C:\Program Files\Microsoft SQL Server\80\Tools\Binn).
 - **DBA User:** Database administrator user name (for example, sa); configured on the SQL Server.
 - **DBA Password:** Password of the database administrator that is configured on the SQL Server.
 - **Database Data Root:** (for example, C:\Program Files\Microsoft SQL Server\MSSQL\Data)

16. Click **Next**. If you are creating an embedded database, the database is created. It takes a few minutes to create the database. Skip step 17 and continue with step 18.
17. If you are creating an MS SQL database, the Database Creation Choice dialog box appears:
 - Select **Define New Database** to create a new SQL database on the SQL Server or **Use Existing Database** to connect to a database that was previously created.
 - Click **Next**. The Microsoft SQL Server Information dialog box appears.
 - In the SQL Database Server Information dialog box, enter:
 - **Database Server:** Host name or IP address of database server where the Policy Manager will save application data.
 - **SQL Server Port:** The port configured by Microsoft SQL Server for accepting connections. Default value: 1433.
 - **Database Name:** The name of the SQL database where the Policy Manager will store application data.
 - **User:** Name of the user responsible for the Policy Manager database; user name is added to the SQL Server.
 - **Password:** Password for the Policy Manager database user.
 - **SQL Client Path:** SQL client bin folder that contains bcp.exe (for example, C:\Program Files\Microsoft SQL Server\80\Tools\Binn).
 - **DBA User:** Database administrator user name (for example, sa); configured on the SQL Server.
 - **DBA Password:** Password of the database administrator; configured on the SQL Server.
 - **Database Data Root:** (for example, C:\Program Files\Microsoft SQL Server\MSSQL\Data)
 - Click **Next**. The Policy Manager database is then created on the SQL Server. This takes a few minutes after which a message appears.
18. On the Configuration Completed dialog, you can choose to **Start Sygate Policy Manager** and **Start Management Console**. These options are selected by default.
19. Click **Finish**. This completes the configuration of the Policy Manager database. If you kept the start options selected, the Sygate Policy Management Console login is displayed. You must use the login information for the remote Policy Manager to log in to the new Policy Manager.

Notes

- When logged onto the Policy Management console of either Policy Manager, you can see the other partner listed on the **Servers** tab under Replication Partners. You can select the site to view information about it and edit replication properties.
- For details on administering replication partners, see “Managing Replication Partners.” in the Policy Manager Administration Guide.

Logging in to the Policy Manager for the First Time

After running the Configuration Assistant, the last screen asks if you want to run the Policy Manager.

When you launch the Policy Manager you get a log in screen. During the installation of the Policy Manager, a default System Administrator account is created with a default password. For security reasons, the initial log on screen has been set to use a default user name and password for this account. The defaults are:

user name: admin

password: admin

Log in using the defaults and you will be asked to change the password. Once you have changed the password, the Policy Manager console appears. Later in this chapter “Getting Started with the Policy Manager” takes you on a quick tour of the console to orient you to the Policy Manager user interface.

Before you take the tour, however, it is always good practice to make your first step after installing the Policy Manager to create your own Administrator account for security reasons, although the Policy Manager will continue to function using the default account.

Understanding Administrator Accounts

There are two types of administrators: system administrators and domain administrators. System administrators can view and modify the entire system, while domain administrators can view and modify only aspects of their domain. You manage administrator accounts from the Administrators tab in the Policy Manager console.

The Policy Manager is initially installed with a default system administrator account called “admin.” You can keep this account, or, you can delete it and create your own administrator accounts.

One important property you can set is the Login Attempt Threshold which is set from the Administrators tab. This feature allows you to lock an administrator account if a set number of unsuccessful log in attempts are made. By default, this protection is not enabled. It is recommended that you set it somewhere between two and four.

Adding System Administrators

If you would like to add another administrator account, follow these instructions.

1. Click the **Administrators** tab.
2. In the tree, select either **Administrators** or **System Administrators**.

3. Click **Add System Administrator**. The Add System Administrator dialog box appears.
4. Enter the **Administrator Name** in the first field.
5. Optionally enter the **Full Name** of the system administrator
6. Enter a **Password** of six or more characters for this system administrator. Enter the password again in the **Confirm Password** field.
7. Click **OK**.

Notes

- Passwords must be at least six characters long and may not be blank.
- You can also add a System Administrator by selecting **System Administrators** in the tree, right-clicking, and choosing **Add System Admin**.

Getting Started with the Policy Manager

From the Policy Manager, you can manage protection policies on Sygate Enforcement Agents. You can also monitor policy enforcement. The easiest way to get started is to click the tabs and see what's available to you. Refer to online Help when you have questions.

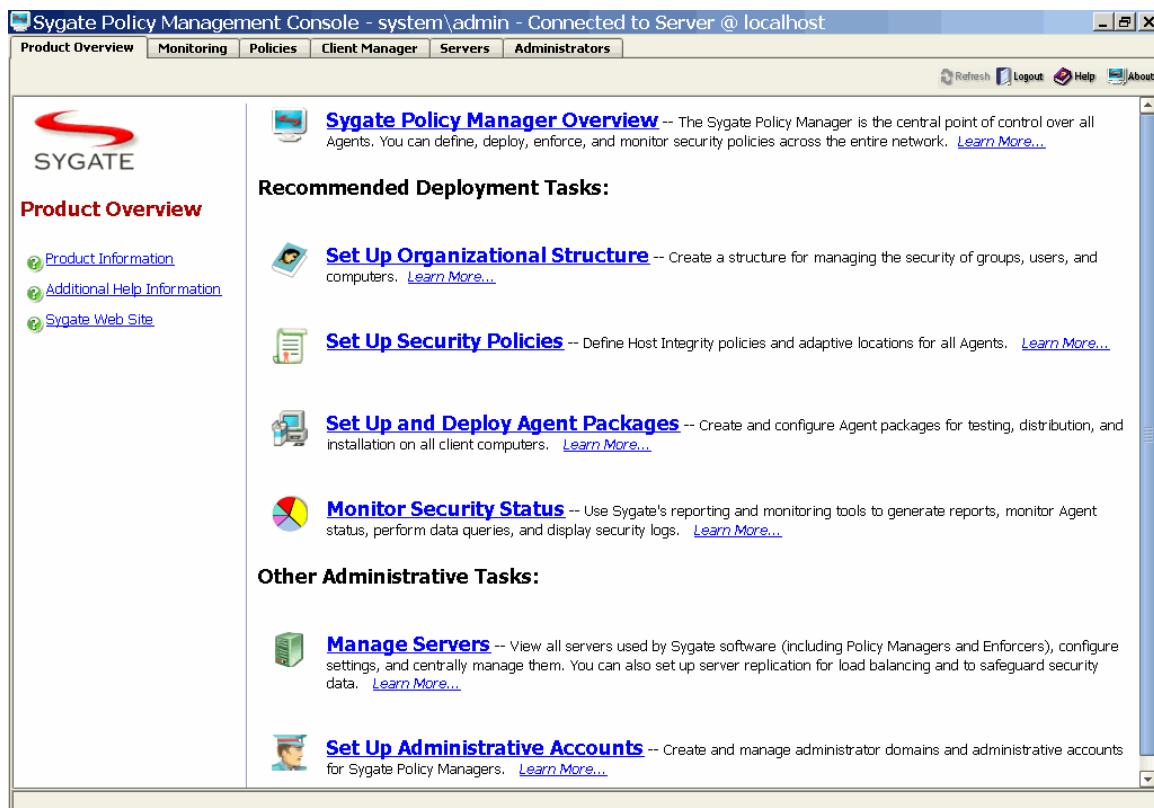


Figure 2. Policy Manager Opening Screen

You administer the security of your enterprise from the Sygate Policy Management Console. It is organized into several tabs. Tasks you can do on the Policy Manager are located on these tabs:

- **Product Overview:** The starting point that lists your main tasks and will take you to the appropriate tab where you can do your work.
- **Monitoring:** Generate reports, query the database for security details, or view security logs.
- **Policies:** Create Host Integrity policies for Agent groups and locations.
- **Client Manager:** Create Agent packages for deployment and set up organizational structure including groups, users, and computers.
- **Servers:** Manage servers (including Policy Managers and Enforcers) and sites, set up replication partners, control log settings and external logging (such as Syslog and third party logging), and maintain Sygate licenses. Administrators limited to one domain cannot see this tab.
- **Administrators:** Create administrator accounts and domains (or divisions) to allow administrative access to limited areas of the enterprise network.

Working on the Policy Manager

Except for the **Product Overview** tab, each tab is organized in a similar way:

- Tabs on top
- Tree on the left
- Task list in the center
- Information area on the right

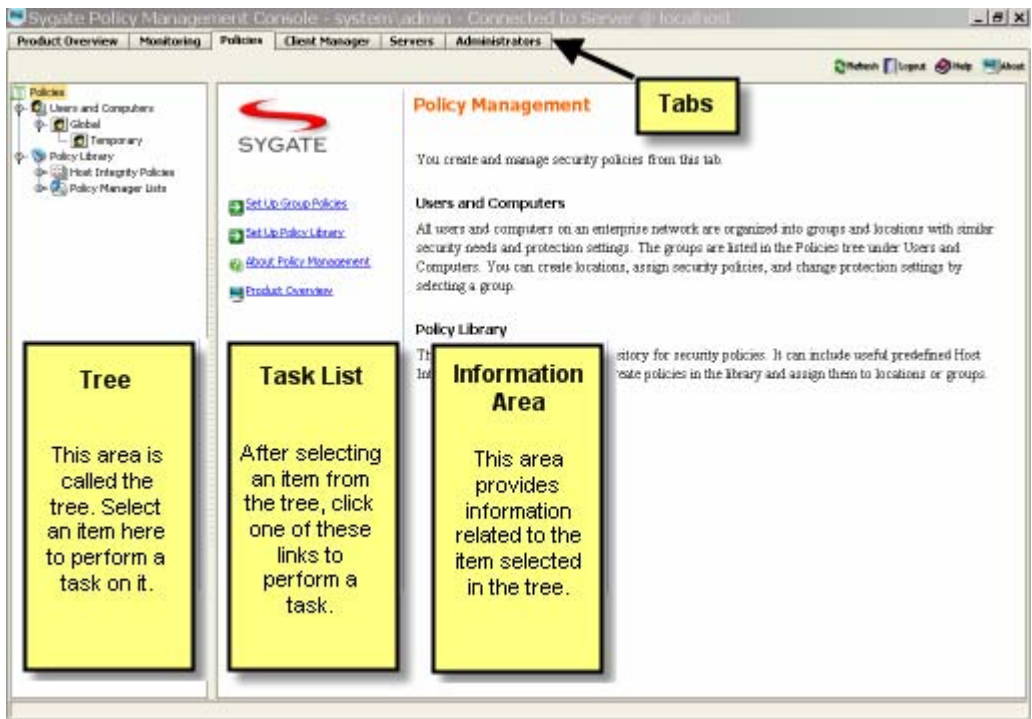
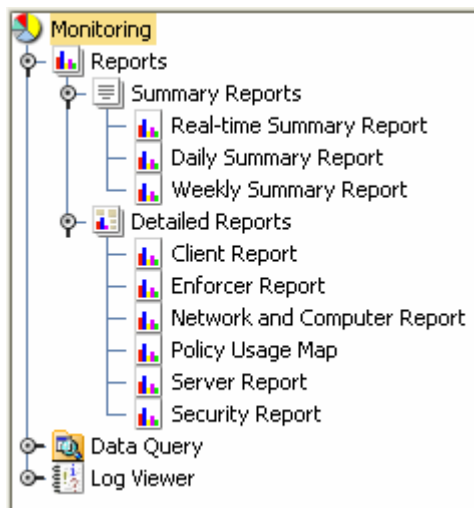


Figure 3. Policy Manager User Interface

Trees

Each of the five main tabs has a tree on the left. Selecting different items in the tree changes the task list, what you can work on, and what appears in the information area.

Monitoring Tree



View reports, query the database, or look at Server (Policy Manager), Agent, or Enforcer logs by selecting them in the Monitoring tree.

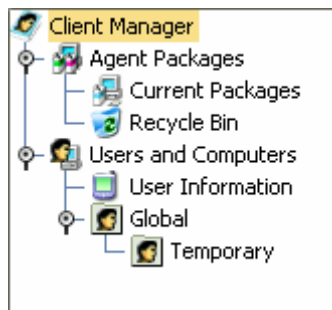
Policies Tree



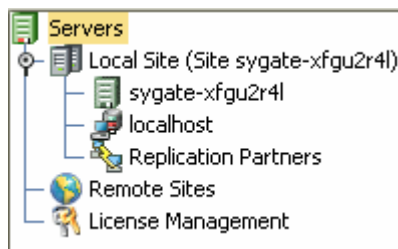
You create and manage security policies from the Policies tree. Groups are organized under Users and Computers and policies can be added to locations at the group level. You can also create policies in the Policy Library and apply them to one or more groups. Tools are provided to query which network applications are used by Agents in specific groups or locations.

Client Manager Tree

From the Client Manager tree, you can manage groups, users, and computers. You can also create Agent packages, and collect and review user information. You can also create Agent packages and collect and review user information.



Servers Tree



In the Servers tree, you can select different items to look at the properties of your server (Policy Manager), its database (called localhost), see Enforcers set up at your site (none shown here), set up other Policy Managers as replication partners, see remote sites, and manage Sygate licenses for Policy Managers, Enforcers, Agents, number of sites, and special features such as Host Integrity and AutoLocation Switching (also called Adaptive Locations).

Administrators Tree



In the Administrators tree, you can add and manage system administrators, and create and manage domains and domain administrators. Domains are separate areas that can be administered by domain administrators who see only the domain for which they are authorized and who see no Servers tab. System administrators can view and modify all domains and have access to the Servers tab.

Chapter 3. Setting Up the Organizational Structure

The organizational structure for Sygate client management consists of groups, users, and computers. The idea of groups is central to setting up your structure. It is very similar to the concept of user groups in Windows. You can create and organize the groups into a hierarchical tree structure to represent the structure of your business. The group is the only entity to which you can assign a security policy. Therefore, the creation of groups is one of the first things administrators do when configuring the Sygate system. You can then define security policies based on the security need of each group and apply them using the Policy Manager.

The figure below shows a sample group tree hierarchy. You can create groups based on location, department, or any other classification that meets your business needs.

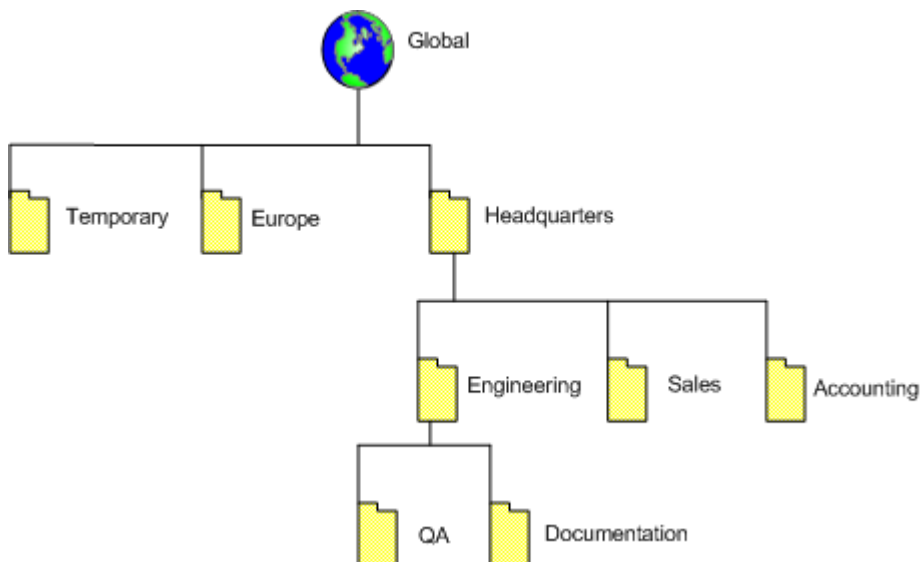


Figure 4. Sample Group Tree Hierarchy

About Groups

The Global group is the root of the tree structure. Below it, you can add groups and sub-groups to suit your organization's structure. It also includes, by default, the Temporary group. This is the default group that is assigned if users and computers do not have a predefined group when they try to register themselves for the first time with the Policy Manager. No sub groups can be created under the Temporary group.

The group structure you define will most likely match the organizational structure of your company. Users and computers with similar computing needs and network access requirements can be grouped together. You manage groups from the Client Manager tab in the Policy Manager. There are three tabs associated with managing groups: Group Management, Users/Computers Management, and Software Package Management. The tabs are located along the bottom of the Policy Manager window. When managing groups, each of these tabs provides different options.

You can also import organizational units from an LDAP server. Once imported, these groups are not managed on the Policy Manager. So, you cannot add, delete, or move groups within an imported organizational unit. You can assign security policies to the organizational unit and you can copy users from an organizational unit to other groups on the Policy Manager. The policy in groups outside the organizational unit has priority. So, if a user is in both the organizational unit and an outside group, the policy of the outside group will have priority.

Replication of Groups Between Sites

If you are planning to have more than one site and want to replicate your group structure between sites, it is important to set up your group structure before you install the Agent software on the Agent machines. All Agents that are installed without an assigned group are assigned the Temporary group. In a replicated environment, there is only one Temporary group. That group resides on the Policy Manager for the first site. So, if you do not set up your group structure for each site first, and then create installation packages based on the individual site, all the Agents will end up in the Temporary group on the first site.

More information on replication is available in your Policy Manager Installation Guide.

Adding a Group

You can use the following procedure to add a group:

Group names may be up to 256 characters and descriptions 1024 characters long. They may consist of any character except the following: ” / \ * ? < > | :

To add a group:

1. Click the **Client Manager** tab in the Policy Manager.
2. From the **Client Manager** tree, select the location of the new group. If you are adding the first group to your site, select **Global** in the tree.
3. Click **Add Group** from the task list.
4. Type the group name and a description.
5. Click **OK**.

Note: You can't add groups to the Temporary group.

About Users and Computers

A core concept in the Sygate software is the concept of users and computers. Similar to any Windows environment where you define user and computer profiles, you can create and add users and computers to any of the defined groups. Once a user or computer is added to a group, that user or computer takes on the security policy of the assigned group. The security policies for groups are set from the Policies tab in the Policy Manager.

You can specify through the Client Manager the mode in which the Agent software on the computer will run. Agents can run in two different modes; computer-based mode or user-based mode. Computer-based mode always takes precedence over user-based mode. Most machines are set to user-based mode. That way, the group to which the person logging on belongs controls the machine. Administrators use computer-based mode when there is a computer located in an unsecured area, such as a lobby. That way, they can always control what security policies are in effect on that machine because the log in user group does not go into effect. The group the computer belongs to always controls the machine.

For example, if Robin, who belongs to a policy group with lots of privileges, logs onto a computer that is in computer-based mode, she still only gets the limited policy for the group the computer belongs to. However, if she logs onto a computer that is in user-based mode, she will always get the policies assigned to the group where she belongs.

You can add, delete, and move users and computers.

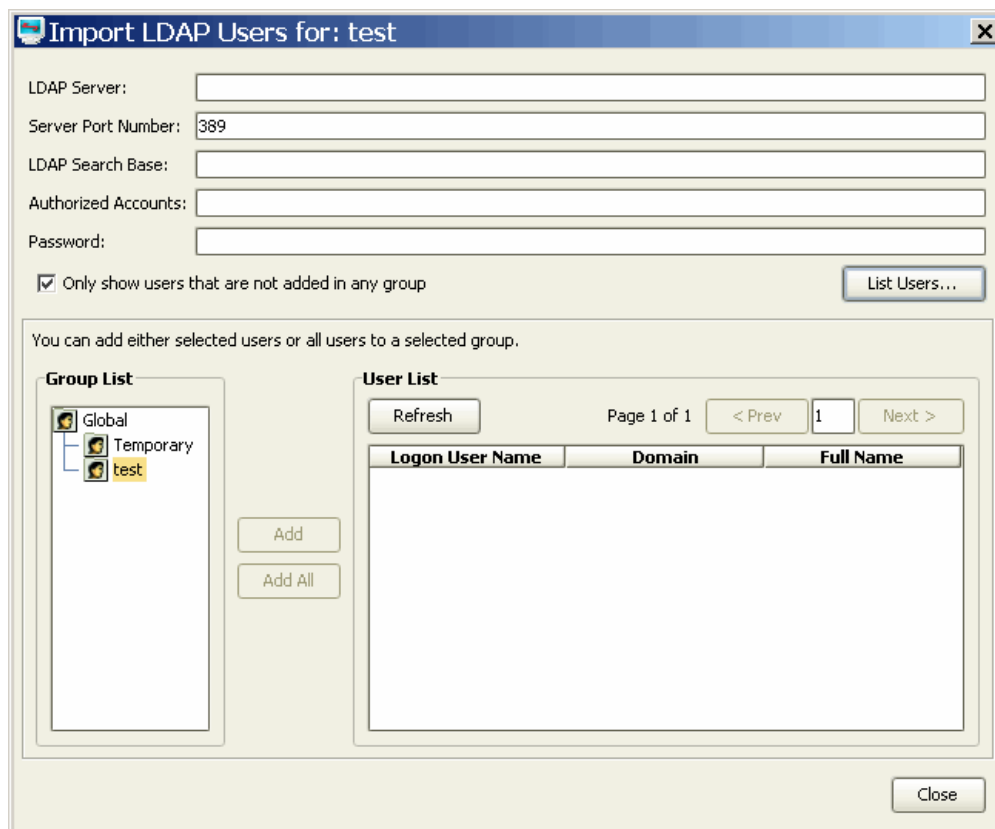
Importing Users from an LDAP Server

Administrators can import user and computer accounts from an LDAP directory server using LDAP protocol. This is a two step process which consists of searching the LDAP server and then importing the users.

Searching for Users on an LDAP Server

To search for users on an LDAP server:

1. Click the **Client Manager** tab.
2. Select the group you want to import users into from the Client Manager tree.
3. Select **Import Active Directory or LDAP Users** from the task list. The Import LDAP Users dialog box appears.



4. After **LDAP Server**, type the IP address of the LDAP server or Active Directory server from which you want to import users.
5. Specify the port number of the LDAP server or Active Directory server after **Server Port Number**. The default is 389.

6. You can list the users by clicking the **List Users** button. You can also type an LDAP query in the **LDAP Search Base** box to locate the names of users that you want to import.

The following table lists query options that you can use in the **LDAP Search Base** field as attribute=value pairs separated by commas.

Table 2. LDAP Search Attributes

Key	Description
CN	CommonName
DC	DomainComponent
L	LocalityName
ST	StateOrProvinceName
O	OrganizationalName
OU	OrganizationalUnitName
C	CountryName
STREET	StreetAddress

Note: Not all LDAP servers support all options. For example, Microsoft Active Directory does not support O.

The order in which you specify the attribute=value pairs is important because it indicates the location of the entry in the LDAP directory hierarchy.

For example, if during the installation of a directory server, you specified a DNS-type domain name of `itsupport.sygate.com` (`itsupport` is a typical NT NetBIOS domain name), you can use it to query a directory server. For this example, you would specify the LDAP search base in this order:

```
CN=Users, DC=itsupport, DC=sygate, DC=com
```

You can use wild cards or regular expressions in the search base. For example:

```
CN=a*, CN=Users, DC=itsupport, DC=sygate, DC=com
```

This query returns all the user names starting with the letter a.

Another example represents organizations within which you may want to perform a structural directory search, such as:

```
mycorp.com -> engineering.mycorp.com or sales.mycorp.com
```

You can specify either option contingent upon where you want to start searching the LDAP directory.

`o=mycorp.com` or `o=engineering.mycorp.com`

You can specify a logical comparison using `>` or `<` in a LDAP search string.

Note: An LDAP query that provides more than 1,000 results may fail. Be sure to set up the search base so fewer than 1,000 users are reported.

7. After **Authorized Accounts** type the name of the LDAP user account.
8. Type the password of the LDAP user account in the **Password** box.
9. Click **List Users** to display a list of users on the LDAP server.

Note: If the box “Only show users that are not added in any group” is checked, only those users that have not already been added will display.

Importing Users from LDAP Server Search Results

Use the following procedure to import users from the search results list.

Note: You can sort the search results by field in ascending or descending order. Click the field name to sort using that column.

1. In the **Group List** tree, select the group to which you want to add users from the **LDAP** server. You can add all the users by clicking the **Add All** button, or select specific users from the list and then click the **Add** button.
2. Select one or more users from the **User List** area. You can use standard Windows selection keys such as the CTRL key to select non-contiguous users.
3. Click **Add**. The names of new users appear in the group tree.
4. Click **Close**.

Repeat this process adding users to other groups, as necessary, until you have added all new users to appropriate groups.

Chapter 4. Creating Security Policies

A *security policy* is a set of security rules and settings that computers or users must comply with to access the enterprise network. Sygate Network Access Control provides you with the ability to create customized security policies for protecting all network entry points including internal networks, VPN, wireless, and Remote Access Service (RAS) dial-up servers. These security policies, called *Host Integrity* policies, can check for the presence of firewalls, antivirus, anti-spyware, patches, service packs, or other required applications.

You can create security policies and apply them globally, to specific groups, or make them adapt depending on the network environment. Because a user may connect to the enterprise network from different locations, such as the office or home, a different security policy can be applied depending on the location. You can create distinct locations for each type of network connection (VPN, dial-up, wireless, or Ethernet) and apply unique security policies to each.

Different Host Integrity policies can be applied to different groups or locations. You can maintain the policies in the Policy Library and apply them to groups or locations, or you can create policies for a specific location.

This chapter covers general procedures for creating and applying Host Integrity policies. For more detailed instructions, see the Policy Manager online help.

About Locations

Because security settings often need to differ based on where a user is located when they log on to the corporate network, you can create different locations to accommodate this. You can have many locations such as:

- Office (working within a corporate office)
- Remote Office (working at a remote corporate facility)
- VPN (VPN in from an outside location)
- Home (working from a home location through an internet service provider)

You can customize the security policy of each location according to specific criteria appropriate to that location. For example, the security policies for the Office location are

probably not as strict as the security policies for the VPN or Home locations because the office location is used when the user is already behind your corporate firewall.

You add locations once you have added a group. So, each group could have different locations if your security strategy required that.

When you create a location, it applies to the group you created it for and any child or subgroups. Therefore locations that you intend to apply to all end users should probably be created at the Global group level. Locations specific to a particular group can be created at the subgroup level. For example, in most companies, all users generally require an Office location that is added by default to the Global group. However, not all users require a VPN connection. Those who do could be organized in a group called Telecommuter and the VPN location added to that group in addition to the Office location. Members of that group would be able to use either the Office or Telecommuter locations.

When creating locations for the groups, you also specify when the location will take effect. For example, you can set the feature to detect a particular IP address or type of connection. This feature is called AutoLocation Switching. For more information on AutoLocation Switching, see “Locations and AutoLocation Switching” in the Policy Manager online help.

If AutoLocation switching is not set up, the client can choose the location manually if multiple locations are available.

If an administrator changes the security policy, it is updated automatically from the Policy Manager during the next heartbeat. If the current location is not valid after the update, then the same location selection logic applies: the Agent will switch to another location that is valid or use the default location.

About Host Integrity Policies

A Host Integrity policy sets the requirements for firewalls, antivirus, anti-spyware, patches, service packs, or other required applications on client computers.

Each Host Integrity policy is composed of:

- One or more requirements covering:
 - What conditions should be checked for (such as the presence and update status of antivirus, firewall, anti-spyware, patches, and services packs)
 - What actions (such as downloads and installs) the Agent takes in response to the condition
- General settings, such as when and how often the Agent runs a Host Integrity check (to verify that requirements are met), how many times a user can cancel a restoration action, and so on

When specifying Host Integrity requirements, you can choose from predefined or template requirements or create custom requirements.

Where to Develop Host Integrity Policies

As explained in “Creating a Location with Default Policies” in this chapter, you can quickly implement a baseline Host Integrity policy by selecting a default antivirus enforcement requirement and a default firewall enforcement requirement while creating a location.

In addition, you can develop policies in the Policy Library and apply them to specific groups or locations, as explained in “Creating a Policy in the Policy Library” in this chapter.

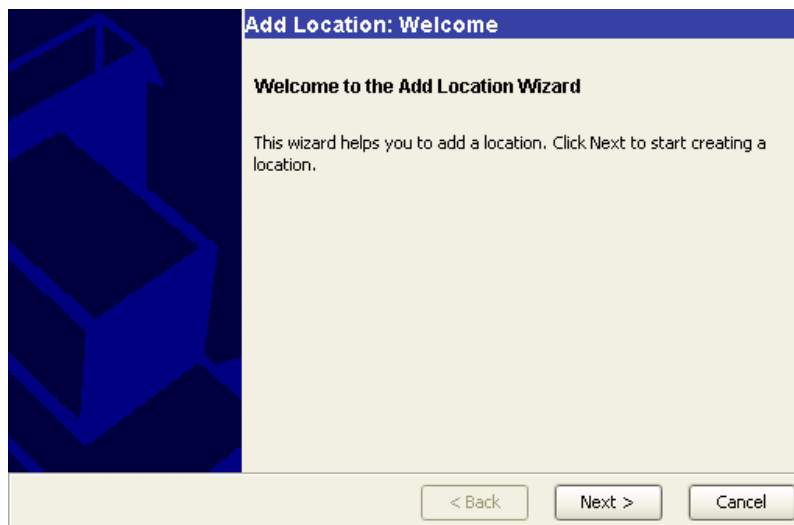
If you are using replication, you need to understand what happens if Host Integrity policies are created and modified on multiple sites in the site farm. See “Understanding the Impact of Replication” in the Policy Manager online help.

Creating a Location with Default Policies

When creating a location, you can easily implement the default Host Integrity policies while creating the location. The following procedure demonstrates how to do this by adding the Home location to a group.

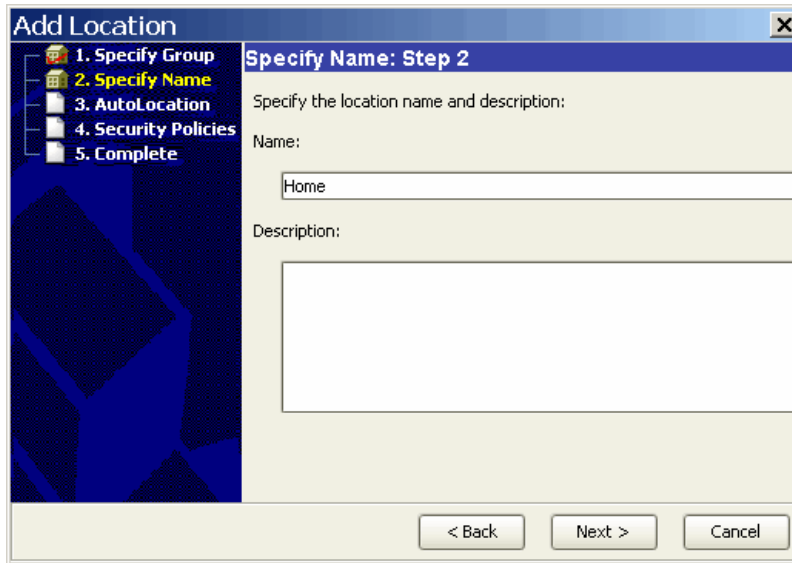
To add the Home location to a group:

1. Click the **Policies** tab.
2. In the Policies tree, select a group you created earlier or the Global group. (You can always delete the location later if using it only for testing.)
3. Click **Add Location**. The Add Location wizard appears.

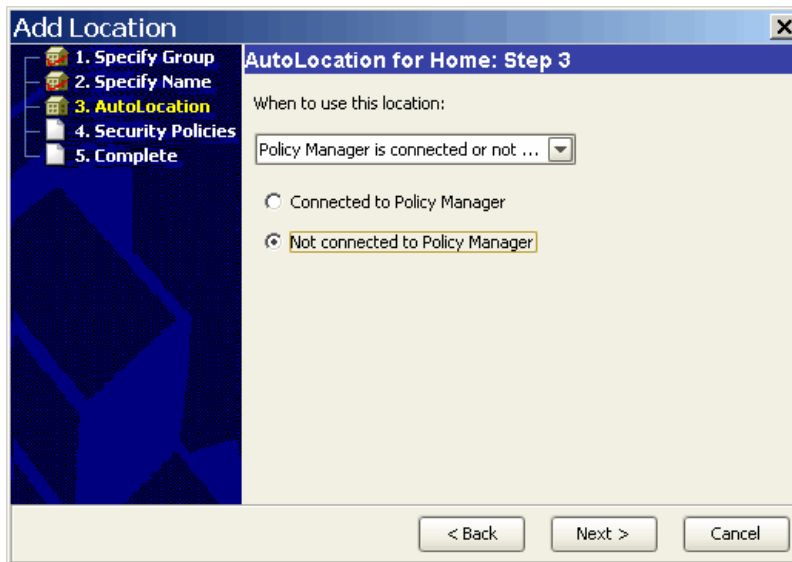


4. Click **Next**.

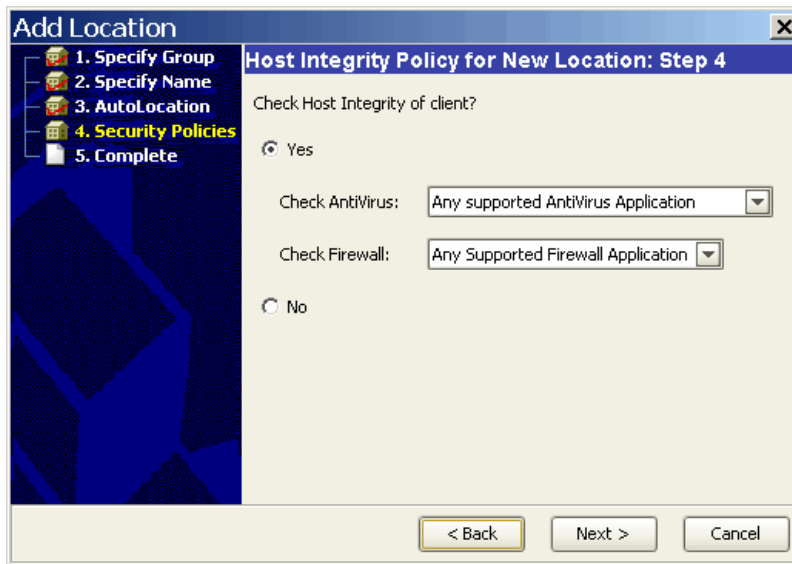
5. After **Name** type Home (you can leave the Description blank), and then click **Next**.



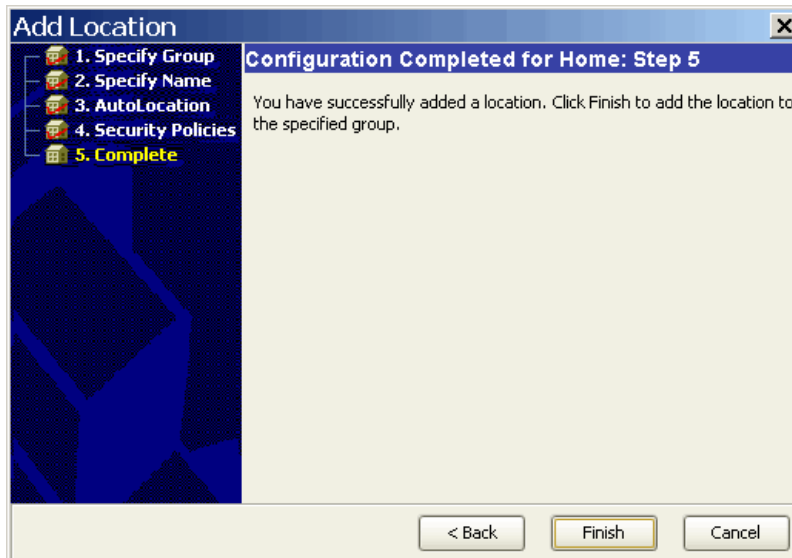
6. Specify the AutoLocation condition under which the Agent will change to this location and click **Next**. For example, for Home, you may want the following selections:
 - o Select **Policy Manager is connected or not**.
 - o Select Not connected to Policy Manager.



7. Click **Yes** to create a Host Integrity policy for this location and select from the choices for antivirus enforcement and firewall enforcement. For example, you could make the following selections for Home:
 - After Check Antivirus select **Any Supported AntiVirus Application**.
 - After Check Firewall select **Any Supported Firewall Application**.
 - Click **Next**.



8. On the Configuration Completed screen, click **Finish**.



9. A message states that the Home location has been added to the group. Click **OK**.

Now you will see the new location, Home, listed on the right in the Location Overview area. You can click **Edit** next to Host Integrity Rule to see the Host Integrity policy contents.

Creating a Policy in the Policy Library

Generally, it is a good idea to keep widely used policies in the Policy Library. That way you can edit and replace the policy in all groups and locations that use it.

The general procedure for adding policies to the library is similar for each type of policy, although the specific settings that you configure as part of the policy are different.

Creating a Host Integrity policy in the library has the following main steps.

Step 1: Add the policy and basic information

Step 2: Add the requirements

Step 3: Specify advanced settings

Step 4: Save the policy

Step 5: Apply the policy (optional)

The following procedure walks you through these main steps. You do not have to complete these steps all at one time—you can stop at any point after naming the policy and save it, and then later edit it to complete it.

Step 1: Add the Policy and Basic Information

1. Click the **Policies** tab.
2. In the Policies tree, click to expand **Host Integrity Policies**.
3. Click **Add a Policy**. The Host Integrity Setting dialog box appears, with the **Requirements** tab on top.

Host Integrity Setting - Policy Library

Requirements **Advanced Settings**

Policy name: New Host Integrity Policy

Description:

When should Host Integrity scripts be run on the client?

Never do Host Integrity checking

Always do Host Integrity checking

Only do Host Integrity checking through the Gateway or DHCP Enforcer

Only do Host Integrity checking when connected to the Policy Manager

Requirements:

Enable	Name
--------	------

Add... Template... Edit... Delete Move Up Move Down

Help OK Cancel

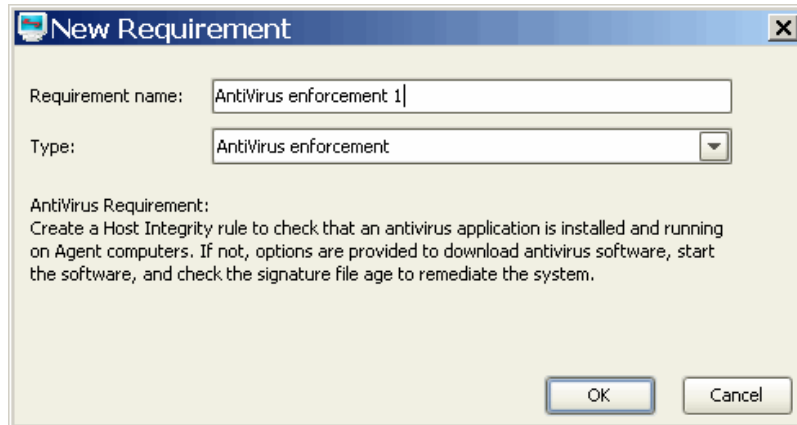
4. After **Policy name**, type the name of the policy (it shows New Host Integrity Policy by default).
5. Optionally, type a description of the new policy.
6. Choose the condition under which you want the Host Integrity check to occur (never, always, only through the Enforcer, only when connected to the Policy Manager). An additional setting, on the **Advanced** tab, allows you to specify the frequency of the checking.

Step 2: Add the Requirements

When you add Host Integrity requirements, you can use any of the following: predefined requirements, custom requirements, or requirements from templates.

To add either predefined or custom requirements:

1. Click the **Add** button. The New Requirements dialog box appears.



2. Type the requirement name. The requirement name can appear in the Agent GUI, notifying the user that the requirement passed or failed or prompting the user to download the software.
3. Select a requirement type from the **Type** list and click **OK**. You can choose from:
 - Antivirus enforcement
 - Anti-spyware enforcement
 - Patch enforcement
 - Service pack enforcement
 - Firewall enforcement
 - Custom requirement
4. Select the settings for the requirement. For more information, see the Policy Manager online help.

To add a requirement from a template:

1. Click the **Template** button. Any new templates are downloaded. The Host Integrity Online Updating dialog box is then displayed.
2. View the available templates and click the **Add** button next to each template you want to add.
3. Click **Import**.

Each new requirement is added to the bottom of the Requirements table. You can now do the following optional steps:

- Click to select or clear the **Enable** check box in order to enable or disable the requirement (the default is enabled). You may want to disable the requirement, for example, if you are adding it for possible future use.
- Change the position of requirements in the Requirements table to determine the order in which they are executed. This can be important when downloading software that requires a reboot after installation; you would try to ensure that requirements requiring a reboot for restoration are performed last. To change the order in which requirements are executed, select a requirement in the table and use the **Move Up** or **Move Down** buttons to move it up or down in the table.

Step 3: Specify Advanced Settings

Optionally, change the default settings on the **Advanced Settings** tab.

The screenshot shows the 'Advanced Settings' tab of a configuration window. At the top, there are two tabs: 'Requirements' and 'Advanced Settings'. The 'Advanced Settings' tab is selected. Below the tabs, the 'Host Integrity Checking Frequency' is set to 2 minutes. A section titled 'Cancelable Restoration Options' contains 'Minimum Time' set to 2 minutes, 'Maximum Time' set to 4 weeks, and 'Only allow user to cancel Host Integrity restoration' set to 1 times. Below this is a text input field for 'Add additional text to user restoration pop-up dialog box:' with a 'Set Additional Text...' button. A larger text box explains that 'Host Integrity "Pass" results are maintained for the time shown below if a user changes location or takes an action that might affect their system integrity. At that point, Host Integrity is checked again.' Below this text box, 'Maintain Host Integrity result for' is set to 30 days. There are two checkboxes: 'Continue to execute requirements after one fails. Note that the Host Integrity check will still fail. However, other restoration actions may be attempted if required.' (unchecked) and 'Show verbose Host Integrity Logging' (checked). A section titled 'Pop-up Message Display Options' contains two checkboxes: 'Display pop-up Message when Host Integrity check fails' (unchecked) and 'Display pop-up Message when Host Integrity passes after previously failing' (unchecked). Each has a 'Specify additional text for message box:' label and a 'Set Additional Text...' button. At the bottom of the window are 'Help', 'OK', and 'Cancel' buttons.

Step 4: Save the Policy

Click **OK** on the Host Integrity Setting dialog box. The dialog box is closed and the new Host Integrity Policy is saved and added to the Policy Library.

Step 5 (Optional): Apply the Policy

The Host Integrity policy is now available for use by any group. Before it can be used, you must select the groups and locations to which you want to apply this policy.

Policies can be applied at the Global group level, a root or head group, and they can be inherited by subgroups on the Policy Manager. You can apply one policy (with multiple rules) to a group. Not only can you apply a separate policy to each group of users or computers, but you can also apply separate security policies to each group's location, if a group has been assigned multiple locations.

If you want to apply the policy now:

1. With the policy selected in the tree, click **Apply this Policy**.
2. In the Apply Policy dialog box, select the groups or locations to which you want to apply the policy and click **Apply**.

Chapter 5. Installing Agent Machines

An Agent software package is deployed to each computer within the network. You manage Agent installation packages from the Client Manager tab in the Policy Manager.

About Packages and Deploying the Agent

Sygate refers to the bundle of installation files for the Agent software as a *package*. You will see this term used throughout the Client Manager tasks on the Policy Manager.

When deploying the Agent software for the first time, you must first export the files to an install point on a server. From there, you can install the files on each computer in the network using a variety of methods. After initial installation, the Agent software can be updated from the Policy Manager directly.

Before you export the Agent files for installation, there are three things to consider: deployment method, single or multiple file distribution, and whether you will include security policies.

The choice you make regarding the deployment method of the Agent files affects the way you may choose to export the files.

You can select from any of the following distribution methods to distribute packages:

- **Internet**—You distribute the software by pointing users to a particular location on an Internet Web site. Then the users download a single executable file and run it. It unzips application files and runs the `Setup.exe` program to install the Agent.
- **Network Install**—You distribute the software by copying the `Setup.exe` program to a network server from which users can copy the files
- **Server login script**—You distribute the software by writing a login script that automatically runs the `Setup.exe` program or the compressed Agent file and then installs the software.
- **Image file**—You distribute the software by creating image files of the operating system and all applications, including the Agent when you set up new computers. In this case, you actually go through the entire installation process with one Agent on the machine that will be cloned for the image file.

Note: Do not connect the Agent that you are using for your image to a Policy Manager. An Agent is given a unique GUID when it successfully connects to the Policy Manager. Thus, if you connect the Agent that is to be cloned to the Policy Manager, it will get that unique GUID. If you then clone that image, all Agents built with that image file will have the same GUID which will produce unintended results.

- **CD-ROM distribution**—You distribute the software by copying the Agent package to a CD-ROM, probably with other software, and send the CD to users. You may use this form of distribution for users who do not have high-speed access.
- **Software management tools**—You distribute the software by using a tool such as Microsoft System Management Software, IBM Tivoli, or HP OpenView, and distribute the Agent through that tool.

The second decision is whether you will use an install point that includes all the software files, or, are you going to use a single .exe file? Your delivery method will probably dictate whether to use all the files or a single file.

- **Individual Installation files**—This type of package is appropriate for most methods of distribution. Once the package files are exported to a directory, you can use your chosen deployment method to install the Agent.
- **Single executable file**—This type of package is best used when bandwidth is an issue as is the case with Web downloads. When created, there will be one file named SEA.exet.

The third decision is whether to include custom security settings with the software. Your deployment strategy can be designed to address the software and security policies separately, or in combination. It is entirely up to you.

Exporting a Package for Deployment

When deploying Agent software for the first time, you must first export the files to an install point on a server. You can either create and export a single executable for deployment, or, export all the files to an install point.

From the export directory you can collect the files and distribute them via any one of the possible distribution methods. You can also install directly from the export directory by running the setup.exe file. While in the export dialog box, you can also set some additional features. From the export task you can:

- Define an export directory on the Policy Manager server
- Decide to create a single .exe file for installation
- Specify a Policy Manager list
- Choose the group policies to apply to the exported package

To export an installation package:

1. From the **Client Manager** tab, select **Current Packages**, and then select a package from the list on the right.
2. Click **Export Package**.
3. Enter a directory where you want the Policy Manager to create the package.
4. Make your selections in the Export Package dialog box.

Export Directory:

Enter a location to export the source files. If there is already a package in the destination directory, it will be overwritten. The path for the exported files is:

[Export Path]\Export\SEA

For a package with group settings: [Export Path]\Group Name\SEA

Create a single .EXE for this package:

Mark this box if you want to create a single executable file for the installation.

If you plan to deploy using Microsoft SMS, Active Directory server, or auto-upgrade using the Sygate Policy Manager, single .exe files can't be used with these deployment methods.

Export default package without security policies:

You can choose to export the package without any group security policies.

Specify a Sygate Policy Manager list:

Specify a Policy Manager list to indicate the Policy Manager server(s) the Agent will connect to after installation. The drop down list box shows all Policy Manager lists that are available in the Policy Library plus an option to not connect to a server. If you choose **Do not connect to any server**, the Agent will never connect to a Policy Manager.

Export package with specified security policies and Policy Manager list:

If you want to export the package with policies from a specific group, then, select a group or groups from the group tree.

5. Click **OK**. The package is exported.

Note: The export feature can also be accessed by right clicking on any of the packages in the Current Package list.

Once the installation files are exported, you can proceed to installing the Agent software on the computers in your network.

Installing the Agent Software

Once the export package is complete, you can install the Agent software to your network machines.

To install an Agent package that has been exported:

1. Double-click the Setup.exe file (if you exported a set of files) or if you created a single executable: SEA.exe. The **Welcome** screen appears.
2. Click **Next**. The **User License Agreement** dialog box appears.
3. The user can scroll through the agreement to make sure they agree with the policies. They then click **Yes** to agree. The **Choose Destination Location** dialog box appears.
4. Click **Next** to accept the default location for the Agent files or click **Browse** to select a different location.
5. Select a Program folder from the list for the display of Agent icons (in the Start menu).
6. Click **Next**. The files are now copied.
7. Select both checkboxes to launch the Agent and display the product Readme.txt file.
8. Click **Finish**.

The machine requires a re-boot upon completion of the Agent installation.

Chapter 6. Enforcers (Optional)

In this chapter you will find an Enforcer installation checklist.

For more detail on installing Enforcers, see the *Sygate Enforcer Installation and Administration Guide*. The Enforcer documentation is also included in the Policy Manager online help.

Enforcer Installation Task List

Here is the suggested order of tasks for installing the Enforcer.

1. Determine where to set up Enforcers. See the planning information for the type of Enforcer you are installing.
2. Install a Policy Manager.
3. Verify that you have installed any other software and hardware components needed for Enforcer operation. See “Installation Prerequisites (Gateway or DHCP Enforcer)” or “Installation Prerequisites (LAN Enforcer)” in the Enforcer documentation.
4. Verify that system requirements are met on the computer on which you are installing the Enforcer.
5. Install a minimal Linux system as described in your Linux documentation. See also “Linux Installation Recommendations” in the Enforcer documentation.
6. Install the Enforcer software.
7. Specify the settings for the Policy Manager connection on the Enforcer local console.
8. Select the NIC configuration on the local console. See “Selecting NIC Configuration (Gateway or DHCP Enforcer)” or “Selecting NIC Configuration (LAN Enforcer)” in the Enforcer documentation.
9. Finish configuring the Enforcer from the Policy Manager. Once the Enforcer connects to the Policy Manager, you can perform additional configuration tasks on the Policy Manager web console. See “Enforcer Configuration Tasks after Connecting to the Policy Manager” in the Enforcer documentation.

10. Set up an Enforcer for failover **(Optional)**: Install and configure standby Enforcers for each Enforcer that you want to have availability. See “Setting Up Gateway or DHCP Enforcers for Failover” or “Setting Up a LAN Enforcer for Failover” in the Enforcer documentation.