

User Guide: Sybari Enterprise Manager



COPYRIGHT

Copyright © 1998-2005 by Sybari Software, Inc. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Sybari Software, Inc.

TRADEMARK NOTICES

Sybari Enterprise Manager, Advanced Spam Manager, Sybari Spam Manager, Antigen, Antigen File Filtering, Antigen Worm Purge, and Antigen Central Manager, are trademarks of Sybari Software, Inc. All other products or services mentioned in this document are identified by the trademarks or service marks of their respective companies or organizations. All trademarks are the property of their respective owners.

FEEDBACK

Sybari appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligations whatsoever. Please address your feedback to: Sybari Software, Inc., 353 Larkfield Road, East Northport, NY 11731, or send email to info@sybari.com.

Issued November 2004/Sybari Enterprise Manager v 1.1

Written by Michel LaFantano, Sybari Software Inc.

Table of Contents

Chapter 1 - Introduction	4
The Sybari Enterprise Manager	4
System Requirements	4
Chapter 2 – Installation.....	5
Uninstalling.....	6
Uploading the SEM License File	7
Chapter 3 - Client Overview	8
Chapter 4 - Getting Started	11
Configuring the Global Settings	11
Configuring SEM User Accounts	12
Configuring Managed Servers	13
Configuring Server Groups.....	14
Configuring Engine Signature Updates	15
Chapter 5 - The Deployment Job	19
Installing Antigen on Remote Servers	19
Creating the Deployment Package	19
Configuring the Install Deployment Job	23
Deploying Antigen Template Files on Remote Servers.....	24
Creating the Template Package.....	24
Configuring the Template Deployment Job	24
Deploying the Antigen License File on Remote Servers	25
Creating the License Package	25
Configuring the License Deployment Job.....	26
Chapter 6 – Reports.....	27
Detection Reports	27
Traffic Reports.....	27
Engine Versions.....	27
Configuring and Running Reports	28
Saving SEM Reports.....	31
Scheduled e-Mail Reports.....	32
Chapter 7 – Alert Management.....	34
Configuring Alerts	34
Chapter 8 - Getting Help.....	37

Chapter 1 - Introduction

The Sybari Enterprise Manager

The Sybari Enterprise Manager (SEM) is a centralized management tool designed to provide IT Administrators a way to manage Sybari software solutions on all of the servers in their enterprise. Through a web-based management UI, the SEM will provide administrators with centralized:

- Deployment
- Reporting
- Management (**Please Note:** Available in a future SEM release. These tasks can currently be handled using templates that can be deployed using the SEM.)

Centralized Deployment will allow administrators to deploy new products, product upgrades, hot fixes and patches, templates files, and signature files to all or selected servers in an enterprise. The deployment functionality will also include the ability to deploy to machines without pre-existing software, live Exchange server updates (no restart necessary), server driven signature file updates to centralize the update procedure, and the ability to deploy templates for configuration management.

Reporting will provide a way for administrators to more closely monitor the servers in their enterprise and evaluate the effectiveness of their anti-virus software. The SEM will collect statistics from all the servers under its management and store them in a central repository for analysis. The statistics will also be used by the SEM to alert administrators to potential problems by monitoring event thresholds and looking for statistical anomalies that may indicate a problem.

Reports will provide information about the trends in virus, spam, filter, and update activity for each server or the entire enterprise.

Data used by the SEM can be stored in MSDE (a scaled down version of SQL Server) or an existing SQL server—locally or remotely—using SQL or Windows authentication.

System Requirements

Minimum Server Requirements:

- Windows 2000
or Windows 2000 Server/Advanced Server
or Windows 2003.
- 128 MB of available memory
- 183 MB of available disk space for pre-requisites listed below
- 65 MB of available disk space for the SEM

Pre-requisites:

- IIS 5.0 or higher
- .net Runtime v. 1.1
- ASP.net v. 1.1
- Microsoft Message Queue and MSMQ Triggers
- MSDE or SQL Server

Please Note: The SEM uses bi-directional DCOM to communicate information between SEM and the Agents located on remote machines. In environments where internal firewalls are present, the firewall configuration must be configured to allow the DCOM protocol.

Chapter 2 – Installation

This release of the Sybari Enterprise Manager supports local installs on Windows 2000 and/or 2003. **(Please Note:** The SEM cannot be installed on a server that is used as a Domain Controller.)

SEM's setup wizards can be used to install the product to a local Windows 2000/2003 machine. The following information should be gathered prior to installation:

- The Administrator Account and Password for the machine on which the SEM is being installed.
- If you are installing SEM on a Windows 2000 server, you will need the Windows 2000 server install CD available during the install process. The install wizard will need this disk while installing the Windows server components if necessary.

To begin the installation procedure, run SETUP.EXE from the directory containing the SEM installation files. Follow the steps below to complete the installation:

1. The install wizard will first check for the required system components and then ask if you would like the SEM install wizard to install any that are missing. Click "Yes" to have the install wizard install missing components or "No" if you prefer to install the components manually.
Please Note: IIS is an install pre-requisite, however, for security reasons this must be installed and patched manually by an administrator.
2. On Windows 2000, you may be asked to reboot the machine after the required components are installed. If so, you will need to run SETUP.EXE again after you log back in to continue the installation.
3. You will be prompted to select the type of database you would like to use with SEM. Select MS SQL Server 2000 Desktop Engine (MSDE) or Existing SQL Server.

For MSDE Installations:

1. The License will be displayed. Click "I Accept the terms in the license agreement" and then Click Next. (If you do not accept the terms of the license agreement, the install will terminate.)
2. User Information will be displayed. Modify if necessary. Click Next.
3. The install destination folder will be displayed. Modify if necessary. Click Next.
4. Click "Install" to begin the installation.
5. Install status is displayed. Click "Finish" to complete the installation.

For SQL Installations:

To install SEM to an existing SQL Server, the user can run through the same install program as above for MSDE installations. Before starting the install, however, the administrator must have:

- The name of the SQL Server they intend to access.
- A database created for:

SybariEnterpriseManager

SybariEnterpriseManagerReports
- A username and password (SQL Authentication or Windows).

Important: Both SybariEnterpriseManager and SybariEnterpriseManagerReports databases must have granted the specified user access to the database and the db_owner permission. If the user is database owner these rights are automatically granted.

The install wizard will prompt you for the following information:

- **Authentication Type** – Select Windows integrated security or SQL Authentication. The remote SQL server administrator will be able to tell the user how their system was setup. If the wrong Authentication type is selected, the install will fail to logon.

Please Note: If you are using Windows Integrated Security with a remote server, the SEM Server requires credentials accessible to both SEM and the remote SQL box. This is only supported using SEM & SQL in a domain/AD environment.
- **Server** – This is the local or remote SQL server to install to. The dropdown box will display all the SQL Servers that could be discovered in the client's environment. The user is not limited to this list and can manually type a server name.
- **Domain** – This field can be ignored if you are using a local SQL server with integrated security and a local account or using SQL authentication. If you are using integrated security to connect to a remote SQL server, enter the domain in which SQL and SEM are located.
- **User** – Enter the name of the user with access to the SQL repository.
- **Password** – Enter the user's password.

After providing the necessary credentials, the user must test the login, using the test logon button, before proceeding to the next step of the SQL install.

In the final stage of the SQL part of the install, you will be asked to specify the target databases in the SQL Server. These are the databases created by your SQL Administrator prior to the SEM install. As mentioned above, we recommend "SybariEnterpriseManager" and "SybariEnterpriseManagerReports."

If you are using SQL authentication, you can use the dropdown boxes to browse by name (Windows authentication doesn't allow this.). Before progressing to the next step both "Check Database" buttons must be pressed to confirm database access on the remote server.

Once the SQL server steps are completed, the install continues as described above for MSDE installations..

The installation is complete. To run the Enterprise Manager, open an internet browser and enter the server name followed by "semconsole."

Example: http://servername/semconsole

If you are connecting to the local machine, enter: http://localhost/semconsole

When connecting remotely to the SEM console, you will be prompted to log in using the credentials used to originally install the SEM.

Uninstalling

To uninstall SEM, you may either use the Windows "Add/Remove Programs" function or run setup.exe and select the "Remove" option. Follow the on-screen instructions to complete the removal process.

When using either method to uninstall SEM, you will be asked the following question:

“Would you like to delete the SEM database information and revoke associated login rights?” Select “Yes” or “No.”

Sybari suggests deleting old SEM databases when removing the product. If they are left in place, any new SEM installations will attempt to connect to the old database, but the administrator will be prompted before SEM connects to an old database, because if the old database is corrupted or was created with a different version of SEM, it may not function properly.

Uploading the SEM License File

When upgrading from an evaluation install of SEM or updating your license at the end of your subscription period, the SEM provides an easy way to upload the new license files (license.cfg) to the install folder.

1. Click on Upload New License File in the left navigation panel. The New License File work panel will open.
2. Enter the path or browse to the new license file (cfg).
3. Click Upload New License File. The new license file will be uploaded to the install folder and initialized.

Chapter 3 - Client Overview

The Sybari Enterprise Manager User Interface provides administrators with an easy way to deploy Antigen, disseminate engine updates, and create reports about virus and spam activity on their network(s).

The SEM console is used for all configuration and deployment tasks, but the client console does not need to remain open when jobs are running. The SEM runs constantly regardless of the status of the Console window. Once a job has been initiated or scheduled, the SEM console may be closed without affecting the operation of SEM components.

The UI is divided into two main areas as shown in the image below:

SYBARI Enterprise Manager At a Glance...

• At a glance...

SEM Administration:

- Users
- Servers
- Server Groups
- Global Configuration

Job Management:

- Packages
- Jobs

Reports:

- Detections
- SMTP Traffic
- Engine Versions

Alert Management:

- Alerts

Event Logs:

- Alerts
- Deployment
- Redistribution

Welcome to the Sybari Enterprise Manager. Below is a summarized view of what has happened in your enterprise in the last 24 hours.

Traffic Summary

Messages Processed: 0	Files Processed: 0
-----------------------	--------------------

Virus Statistics

Skipped:	0
Cleaned:	0
Deleted:	0
Worms Purged:	0
Total:	0

Spam Statistics

Skipped:	0
Purged:	0
Identified:	0
Total:	0

Filter Statistics

Skipped:	0
Purged:	0
Identified:	0
Deleted:	0
Displaced:	0
Total:	0

Top 5 Viruses

Virus Name	Count

Most Active Servers (Based on Detections)

Server	Viruses	Spam	Filters

The left-hand column is the navigation panel for access to the various SEM configuration components and the center area of the UI is the work panel. Each navigator option is described briefly below.

At a Glance. . .:

The “At a Glance. . .” work panel provides information about the managed servers in your environment. The panel provides the following information for the previous 24 hour period:

- Traffic Summary
- Virus Statistics
- Spam Statistics
- Filter Statistics
- Top 5 Viruses
- Most Active Servers (Based on Detections)

The information in the “At a Glance. . .” screen is updated when the screen is opened or refreshed so as to always display information for the previous 24 hours.

SEM

Users:

The Manage Users work panel is used to create user accounts for people within your organization who will need access to the SEM console.

Servers:

The Manage Servers work panel is used to add or remove servers to the SEM database and deploy the SEM “Deploy Agent” that must be installed on each target server to facilitate communication between the SEM and the servers it manages.

Server Groups:

The Manage Server Groups work panel allows administrators to group servers into “Server Groups” to simplify the server management process.

Global Configuration:

The Global Configuration work panel is used to configure the SEM's global settings.

Job Management

Packages:

The Manage Packages work panel is used to create and configure SEM “packages.” SEM packages are Antigen install images or template files that are configured for deployment by the SEM to the managed servers.

Jobs:

The Manage Jobs work panel is used to create, modify, delete, or view SEM Deployment and Signature Distribution jobs.

Reports

Detections:

Detection Reports provide overall statistics on virus, spam, and filter detections including information such as detection rates, actions taken, and filter efficiency.

SMTP Traffic:

SMTP Traffic Reports provide statistical information about SMTP traffic for both messages and bytes processed.

Engine Versions:

Engine Version Reports provide a quick view of the signatures file versions deployed throughout the environment; allowing administrators to easily determine which servers are up to date and which still need updating.

Alert Management

Alerts:

The SEM provides 5 different types of alerts that can be used to monitor when virus or spam activity exceeds certain thresholds. All alerts are configured using the Configure Alerts Work Panel.

Event Logs

Alerts: The Alerts Log provides a log of all Alert events.

Deployment: The Deployment Log provides a log of all Deployment jobs.

Redistribution: The Redistribution Log provides a log of all Signature Redistribution jobs.

License:

License Configuration: The License Configuration page provides a way for administrators to update their SEM license file.

Chapter 4 - Getting Started

After installing the Sybari Enterprise Manager, administrators should configure the following settings in the order they are listed:

1. Global Settings
2. User Accounts
3. Servers
4. Engine Signature Updates

Once these settings have been configured, administrators can deploy Antigen Installs, Configuration Templates, and License Files.

Configuring the Global Settings

The SEM Global Configuration Settings include SMTP Server settings that are used for administrator notifications and the Statistics Polling settings that determine how often reporting data is collected from the managed servers.

SMTP Server Settings

To configure the SMTP server settings that the SEM will use to send notifications about events, alerts, etc., click on “Global Configuration” in the SEM area of the navigation bar. The Global Configuration work panel will open. You will need to enter the following information:

SMTP Server: Enter the name of the SMTP server to use. (Enter the machine name in the format: “machinename.domain.com” or the IP address.)

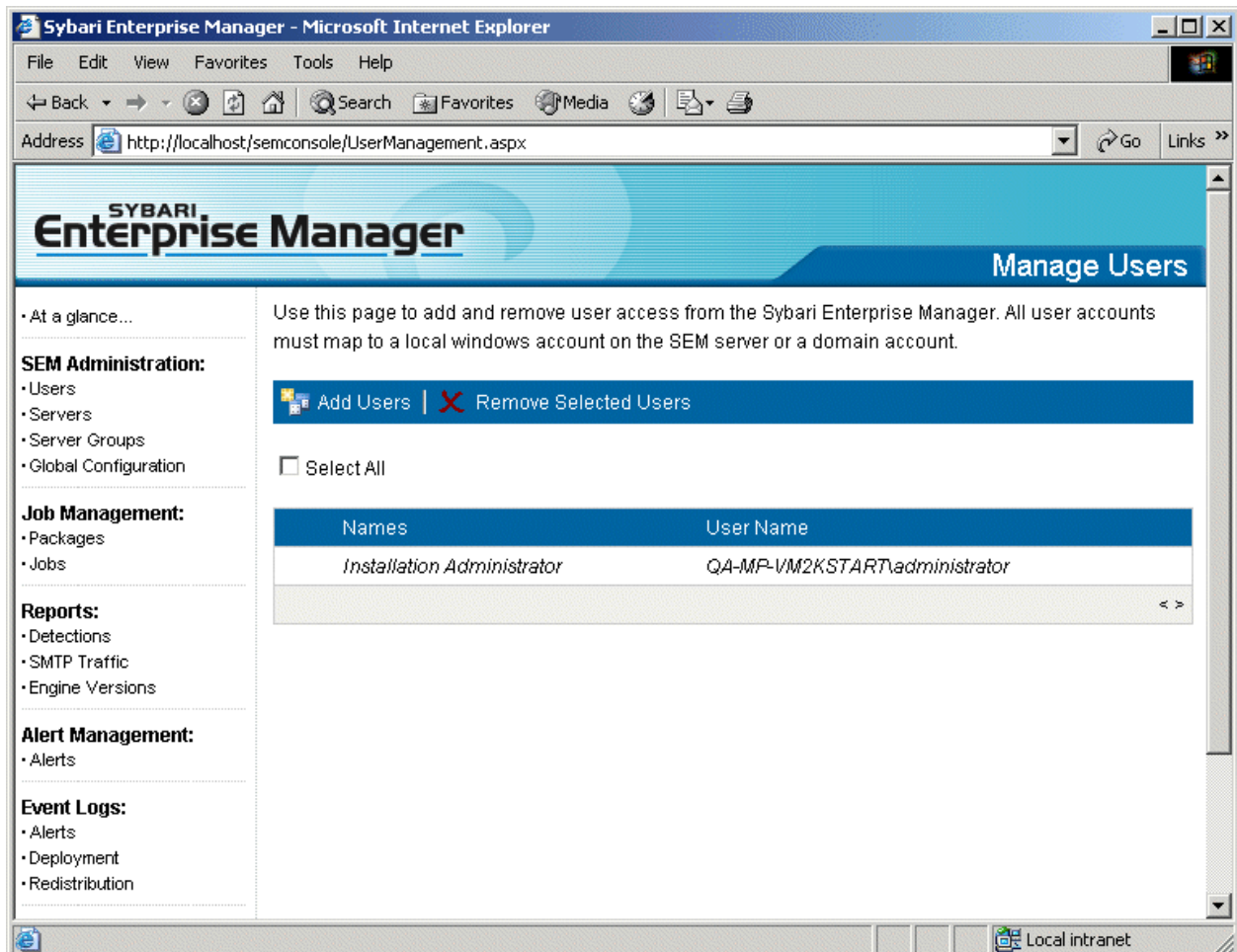
From Address: Enter a valid e-mail address that will be used in the “From” field for notifications and alerts.

Polling Interval: Set the polling interval in minutes that the SEM should use when gathering information from the managed servers for the purpose of reporting.

After you have configured all of the settings, click the Save button.

Configuring SEM User Accounts

When the SEM is installed, the User Account used to install the SEM (Named “Installation Administrator”) is automatically granted access to the SEM. Additional users who wish to use the SEM must have their NT/2000/2003 user accounts granted access to the SEM to perform management tasks. To open the Manage Users work panel, click on “Users” in the SEM area of the navigation bar. The Manage Users work panel will open as shown in the image below:



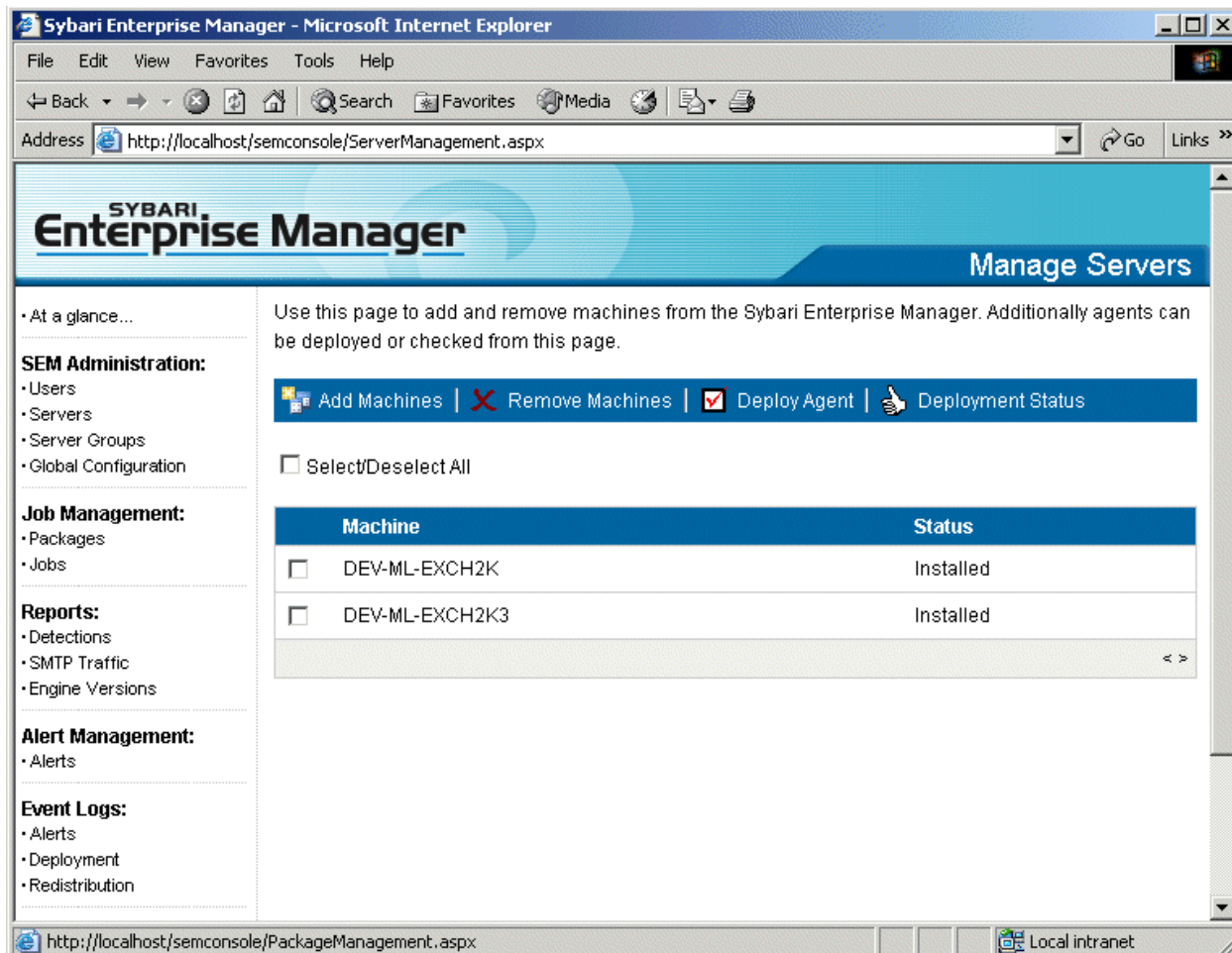
To configure User Accounts, follow the steps below:

1. Click on “Add Users.”
2. You may add local user accounts or domain accounts manually or use the “Browse” button to select and add users. For domain accounts, use the format “domain\username.” For local user accounts, simply enter the user name. Multiple user names must be separated by a semicolon.
3. After you have entered or selected all of the users you would like to add, click on the “Insert Users” button.
4. The new user will be displayed in the main Manage Users screen.

Users can be deleted by selecting the check box next to the user’s name and clicking on the “Remove Selected Users” button on the tool bar.

Configuring Managed Servers

Each server that will be managed must be configured using the SEM console. To open the Manage Servers work panel, click on the “Servers” button in the SEM area of the navigation bar. The Manage Servers work panel will open as shown in the image below:



To configure servers, follow the steps below:

1. Click on “Add Machines.”
2. Use the “Browse” button to select servers to add. After each server is added, you may click on the “Verify” button to insure that the server path has been entered correctly.
3. You may also add the selected servers to Server Groups for the purpose of managing similar machines as a single unit. See below for more information on Server Groups.
4. After you have selected all of the servers to add, click on the “Insert Machines” button.
5. The new machines will be displayed in the main Manage Servers screen.

After the servers have been added to the SEM database, you will need to install an Agent on each machine. This can be accomplished by selecting each server and clicking the “Deploy Agent” button on the tool bar. The Agent serves as the interface between the SEM and the managed server. To deploy an Agent:

1. Select a server or servers and click on the “Deploy Agent” button. You will be asked to supply a User Name and Password to access the selected machine(s). The username and

password provided must have administrative rights either as a local admin to the machine(s) or a domain admin.

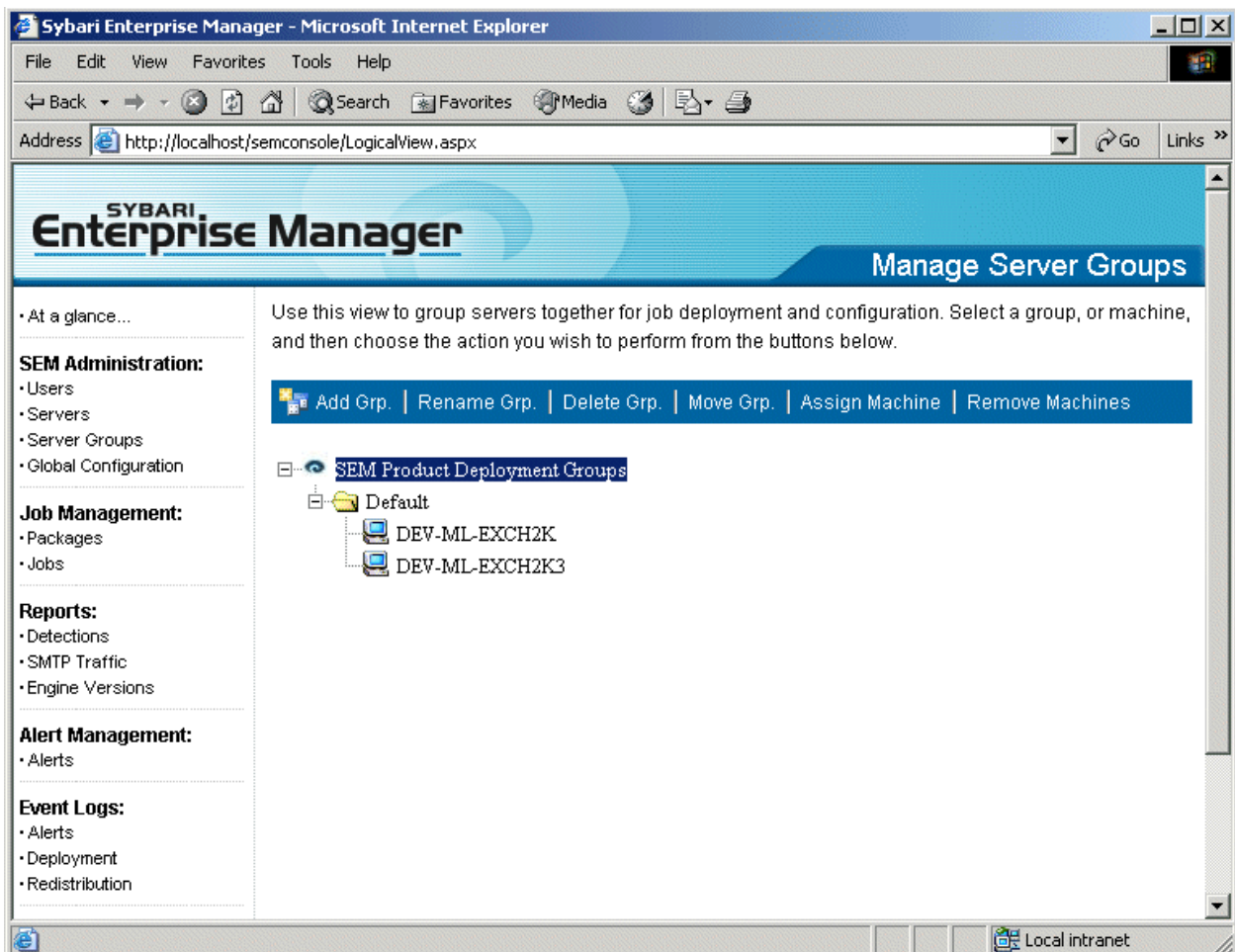
2. The SEM will install the Agent on each selected server.
3. Once the Agent has been installed, the SEM will provide a status update through a pop-up window to report if the installation was completed successfully. (To see the pop-up window, pop-up blocking software must be disabled.)

The Manage Servers screen may also be used to remove servers and to check Agent deployment status. If you choose to deploy Agents to several hundred machines, you can close the SEM console and check the Deployment Status at a later date by selecting each machine, and pressing the deployment status button.

Configuring Server Groups

Server Groups provide a way for Administrators to group servers for the purpose of deployment, engine updates, or configuration through template deployment. By default, any servers added to the SEM will be added to the "Default" folder unless the administrator specifies otherwise.

To manage Server Groups, click on Server Groups in the SEM area of the navigation bar. The Manage Server Groups work panel will open as shown in the image below:



The work panel provides a way for Administrators to Add, Rename, Delete, or Move Groups and Assign or Remove machines from groups. The various processes are described below:

Adding Groups

To add a Server Group, click on the “Add Group” button. The Add Group work panel will be displayed.

1. Name the new group and click on the “Insert” button.
2. The new group will be added to the SEM and will be displayed on the Product Groups page.

Once a new Server Group has been added, existing servers may be moved into the group using the “Assign Machine” button or new servers may be assigned to the group when they are added to the SEM.

Renaming Groups

To rename a group, highlight the group in the “Product Groups” work panel and click on the “Rename Group” button. A new work panel will open to allow you to change the group name. Click the “Rename” button when done to save the new group name.

Deleting Groups

To delete a group, highlight the group name in the “Product Groups” work panel and click on the “Delete Group” button. A new work panel will open to confirm that you would like to delete the group. Click the “Confirm” button to complete the group deletion. **Please Note:** When a server group is deleted, the servers are not deleted from the SEM.

Moving Groups

The Move Group button is used for re-organizing your group structure. This is important if you want to create a hierarchical group structure with top-level groups and sub-groups. The Move Group function allows you to move groups into or out of sub-groups or move groups that may not have been categorized correctly when created.

To move a group, highlight the group name on the Product Groups page and click the “Move Group” button. The Move Group work panel will open. Select the “target” folder where you would like the group moved and click the “Insert” button to complete the move.

Assigning and Removing Machines

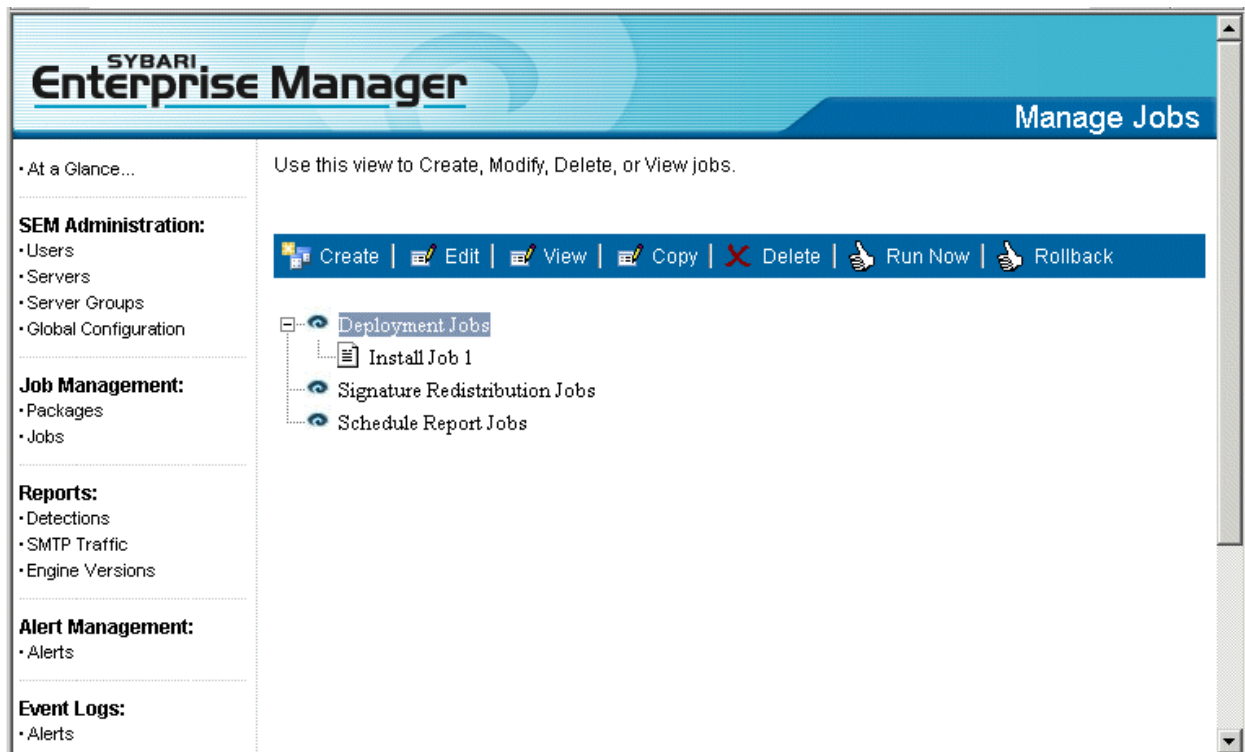
To assign a machine to a group, highlight a group name and click on the “Assign Machine” button. A new work panel will open that will allow you to select machines that should be assigned to the group. Click on the “Insert” button to save your changes.

To remove a machine from a group, highlight a machine name and click on the “Remove Machines” button. The Remove Machine work panel will open to allow you to confirm that you would like to remove the machine from the group. Click on the “Confirm” button to save your changes. **Please Note:** When a machine is removed, the machine is not deleted from the SEM.

Configuring Engine Signature Updates

The Signature Redistribution job is used to provide anti-virus and anti-spam signature updates to all of the servers in an environment by downloading the engine updates to a single staging server that is then used as the retrieval point for all other servers in the environment. It is important to configure the Signature Redistribution before using the SEM to install Antigen in the environment because Antigen will attempt to retrieve updates from the SEM server immediately after install.

To open the Signature Redistribution job work panel, click on “Jobs” in the Job Management area of the navigation bar. The Manage Jobs work panel will open as shown in the image below:



To configure the Signature Redistribution job, follow the steps below:

1. Highlight "Signature Redistribution Jobs" and click on the "Create Job" button.
2. Name the job. Example: Engine Updates
3. Set the update schedule. This setting controls when and how often the SEM will poll the Sybari website for new signature file updates. To schedule the job, you will need to deselect the "Don't Schedule Deployment" check box and then click on the button to the right of the "Schedule" field that will open the Schedule Dialogue Box shown below:

Modify Schedule - Microsoft Internet Explorer

SYBARI Enterprise Manager

Occurs Daily

Daily Every day(s)

Weekly

Monthly

Daily Frequency

Occurs once at: : :

Occurs every: Hours starting at: : : ending at: : :

Duration

Start Date: ... End Date: ...

No End Date

- A. Select a daily, weekly, or monthly update schedule.
 - B. If you would like the SEM to check for updates every day, click on the "Daily" radio button and enter "1" in the field to the right.
 - C. Set the daily frequency. Polling for updates can occur as often as you like.
 - D. Set the Duration of updates. Enter the start date and end date if desired or set "No End Date" to have the SEM check for updates as long as it is installed.
 - E. Click OK to save your settings.
4. Enter the "Number of Retries" if desired. This setting enables the SEM to poll the Sybari site again if it encounters a problem during a download. You will also need to set the "Retry Delay," which is the number of minutes the SEM will wait before attempting a download again.
 5. Enter the Download Location information. The Sybari FTP site is entered by default. You may change this to the Sybari HTTP site or another site if desired.
 6. Proxy Server Settings: If your server accesses the internet through a Proxy Server, enter the proxy server settings including a User Name and Password if necessary.
 7. Enter an e-mail address where update notifications can be sent by the SEM. These will notify the recipient of the success or failure of an update job.
 8. Click "Next" to continue.
 9. Select the engine signature updates you wish to download. You may update all of your licensed engines using one job or create individual jobs for each engine.
 10. Click "Finish." The new job will be displayed in the main Manage Jobs panel under Signature Redistribution Jobs.

11. Since this is the first time you are scheduling the job, highlight the job from the main screen and select “Run Now.” This will force the SEM to do a download and update from the server.

Once you have configured a Signature Redistribution Job, you can use the Manage Jobs panel to Run, Edit, or Delete the job. If the Signature Redistribution job is scheduled, it will start automatically at the scheduled time. If it is not scheduled, you must click on the “Run Job” button to start the selected job.

You can also copy jobs if you want to create multiple jobs that are similar. For example, if you want to create a Redistribution Job for each engine, you can configure one and then copy and modify the job for each engine.

Please Note: When using the Signature Redistribution job to update Antigen’s scan engines, you should disable the Scheduled Updates in Antigen so that Antigen is not updating the scan engines twice. Scheduled Engine updates can be disabled using the Antigen UI or by using the ACM to deploy the File Scanner Template for each engine with the “Scheduler” field set to “disabled.” See Chapters 11 and 18 in the Antigen for Exchange User Guide for more information about scheduled updates.

The Rollback Button

The “Rollback” button can be used to rollback your engine signatures to the previous signature file in the event of a problem with a newly distributed signature package.

Chapter 5 - The Deployment Job

The Deployment Job provides a way for Administrators to:

- Remotely deploy full Antigen Installs or Hotfixes to managed servers.
- Deploy Antigen configuration templates to managed servers.
- Deploy Antigen license files to managed servers.

Creating these Deployment Jobs involves two major steps: 1) Creating the Deployment “Package,” and 2) Creating and running the Deployment Job. Each Deployment Job is described below.

Installing Antigen on Remote Servers

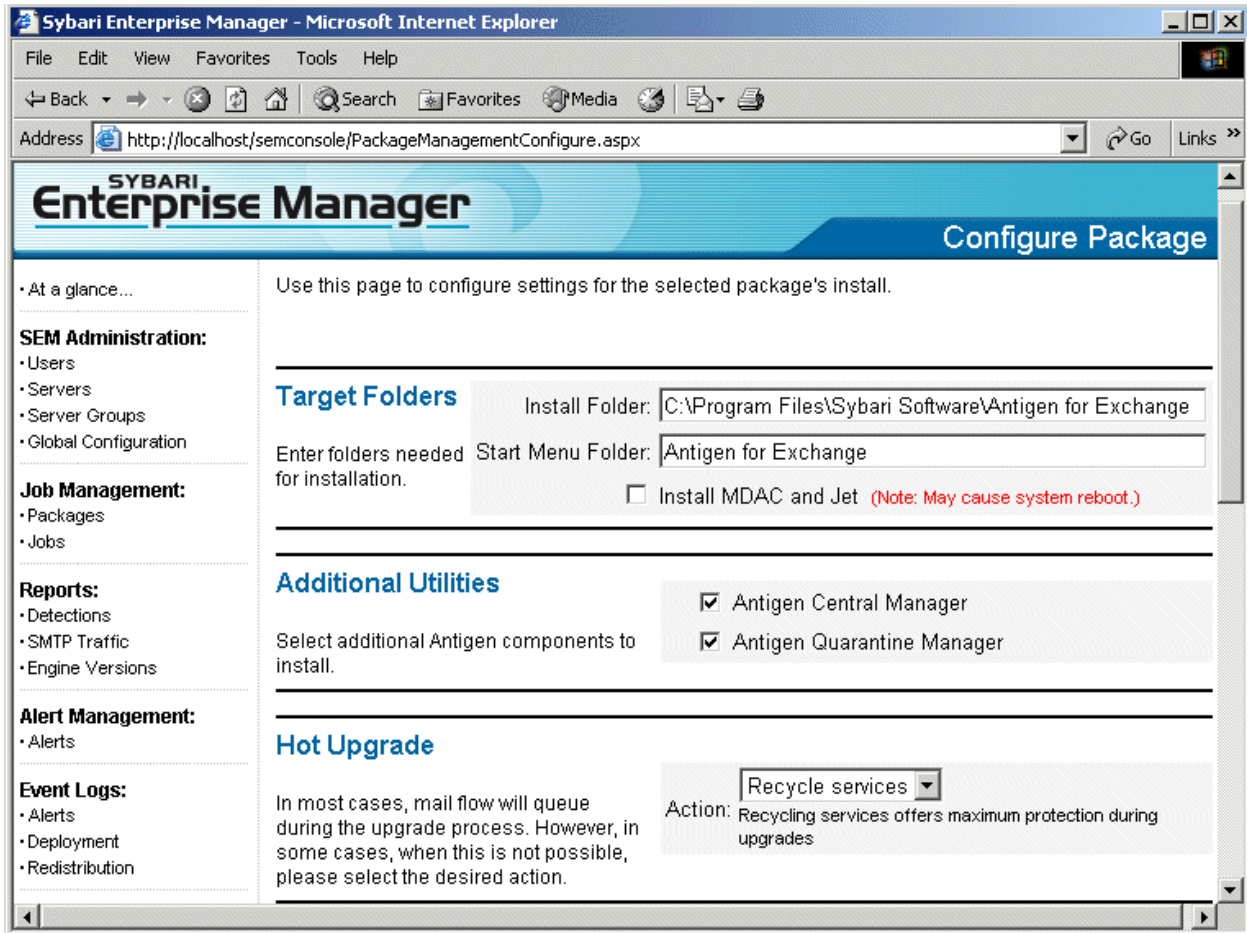
To deploy Antigen to remote servers, you will need to configure the Install Package and create and run a Deployment Job for the target server(s). Each step is described below.

Creating the Deployment Package

The “Deployment Package” consists of the Antigen Install Image files and the install parameters as configured by the SEM. Click on the “Packages” button in the Job Management area of the navigation bar to begin. The Manage Packages work panel will open. Follow the steps below to create the Deployment Package:

1. Click on the “Add Package” button. The “Add Package” screen will be displayed.
2. Enter a name for the Package. (We usually suggest that you use a name that contains the build number as well, such as Antigen for Exchange 8.0.1414.1).
3. Enter the path where the .exe or .zip image downloaded from Sybari’s web site can be found. You can also browse to the folder on your local machine using the Browse button.
4. Click on the “Add Package” button. The Install files are uploaded to the SEM database. **(Please Note:** This may take several minutes since the file has to be uploaded to the SEM database through your local web browser. The upload time will be increased if you are working from a remote machine. Depending on network speed and server usage, the time may vary.)

Once the Install Package has been uploaded, the “Configure Package” work panel will open as shown below:



The SEM recognizes the install image and will ask for information relevant to that package. You will need to complete the following information to complete the Deployment Package:

Antigen for Exchange and SMTP Install Packages:

Target Folders

Install Folder: Enter the path to the Install Folder to be used on the Target Server(s) or use the default folder provided. (These paths are only used for clean installs, not upgrades.)

Start Menu Folder: Enter the path to the Start Menu Folder to be used on the Target Server(s) or use the default folder provided. (These paths are only used for clean installs, not upgrades.)

Install MDAC and Jet: Click on the selection box if you would like the Antigen install wizard to install MDAC and Jet on the Target Server(s).

Additional Utilities Select if you would like to install the Antigen Central Manager (ACM) and/or the Antigen Quarantine Manager (AQM) as part of your install/upgrade.

Hot Upgrade

Action: Sybari's Hot Upgrade technology allows the SEM and Antigen to perform most product upgrades without the need to stop or recycle the Exchange services. During the upgrade, mail is queued to prevent mail from being delivered unscanned. When this is not possible, you will need to select the action the SEM should take. The options are: "Recycle Services," "Disable Scanning," or "Abort Upgrade." Sybari recommends selecting "Recycle Services" so that no mail will be delivered unscanned.

Exchange 2000/2003

Mode: Select ESE or VSAPI mode for the installation on the Target Server(s).

Exchange 5.5

Mailbox Name: Enter the Mailbox name that Antigen will use for e-mail notifications.

Mailbox Server: Enter the Server name that Antigen will use for e-mail notifications.

MAPI Profile: Enter the MAPI profile that Antigen will use for e-mail notifications.

Username & Password: Enter the User Name and Password of a logon account that has Administrative Rights to MS Exchange on the Target Server(s). This is necessary to allow Antigen to register the Antigen Services.

Advanced Spam Manager:

Web Root Folder: Enter the file path to the Web Root folder on the Target Server(s) or use the default path provided.

Sybari Junk Mail Folder: Enter the folder name where the Sybari Junk Mail application will be installed or use the default provided.

Additional Fields for Antigen for SharePoint Installs:

SharePoint Login: In order to install into SharePoint SEM requires a username and password with administrative rights to the server.

Additional Fields for Antigen for IM Installs:

SMTP Notification Settings: IM provides notifications via SMTP e-mail to administrators. These settings allow you to specify which server to relay messages through, as well as credentials used to logon. You will need to provide the SMTP server name, the User Name and Password, and the Product name (IM).

Install Type: Select if you are installing Antigen on Microsoft LCS or IM Logic IM Manager.

LCS Notification Agent Settings: When configuring Antigen for IM, Antigen requires a user account that sends notifications to clients when items such as viruses are detected during transfers or filters are matched. The credentials specified here allow Antigen to send notifications to the user via IM. You will need to provide a User Name, Password, URI, Homeserver name, and Protocol type

After you have completed all of the information, click on “Finish” to complete the Package Configuration. The Deployment Package will be added to the “Manage Packages” screen under the “Package Names” field. Packages can be Renamed or Deleted by selecting the package and clicking on the appropriate button above.

Configuring the Install Deployment Job

After the Deployment Package has been created, click on “Jobs” in the Job Management area of the navigation bar. The Manage Jobs work panel will open. Highlight “Deployment Jobs” and click on the “Create” button. The “Add Deployment Job” work panel will open as shown below:

The screenshot shows a web browser window with the address `http://localhost/semconsole/DepJobModify.aspx`. The page title is "SYBARI Enterprise Manager" and the page content is titled "Add Deployment Job". The interface includes a navigation sidebar on the left with sections: "SEM Administration" (Users, Servers, Server Groups, Global Configuration), "Job Management" (Packages, Jobs), "Reports" (Detections, SMTP Traffic, Engine Versions), "Alert Management" (Alerts), "Event Logs" (Alerts, Deployment, Redistribution), and "Help". The main content area contains the following sections:

- Job Name:** A text input field containing "Install Job 1".
- Select Package:** A dropdown menu for "Package Name" showing "Deployment Package 1" and an "Add Package" button. Below it is the instruction: "Select the package you want to deploy, or upload a new package for installation".
- Schedule Install:** A section with "Schedule Options:" where the checkbox "Don't Schedule Deployment" is checked. It includes a "Start Date" field with "5/14/2004" and a "Start Time" field set to "12 : 00 : AM". Below it is the instruction: "Select the time you want the agent to begin installing the package on the target machine."
- eMail Notification:** An "eMail Recipients:" field with an "Add" button.

Follow the steps below to configure the Deployment Job:

1. Name the Deployment Job
2. Select the Package. Either select a Package that you have already configured from the drop down list or upload and configure a new Package.
3. Schedule the Install if desired. If you don't schedule the install, you will have to manually start the Deployment Job after you have completed the configuration.
4. Enter the e-mail address that should receive the success/failure notification(s) following the deployment of the job.
5. Click “Next.” The “Assign Job” work panel will open.
6. Assign the job by selecting the Target Server(s) or deployment group.
7. Click “Finish” to complete the job configuration.

After you have completed configuring the Deployment Job, it will be added to the “Manage Jobs” work panel under the “Deployment Jobs” section. If you have not scheduled the job, you can run the job by highlighting the job and clicking on the “Run Now” button. You may also edit, copy, or delete the job from the “Manage Jobs” work panel.

Deploying Antigen Template Files on Remote Servers

To deploy Antigen Template files to remote servers, you will need to configure the Template Package and create and run a Deployment Job for the target server(s). Each step is described below.

Creating the Template Package

The “Template Package” consists of the Antigen Template Files (template.adb). You will need to configure your template.adb file using the Antigen Client UI on a local server. See the Antigen for Exchange, SMTP, or SharePoint User Manual for more information about configuring Template files. Click on the “Packages” button in the Job Management area of the navigation bar to begin. The Manage Packages work panel will open. Follow the steps below to create the Template Package:

1. Click on the “Add Package” button. The “Add Package” screen will be displayed.
2. Enter a name for the Package.
3. Enter the path to the template.adb file or use the Browse button to navigate to the file.
4. Click on the “Add Package” button. The Template file is uploaded to the SEM database.

Once the Template Package has been uploaded, the SEM will provide the following Template install options, which allow administrators to deploy all or selected Antigen templates:

- Select All
- Update Scan Job and Anti-Virus Settings
- Update File Filter Settings
- Update Notification Settings
- Update File Scanner Updates Path and Proxy Server Settings
- Update Content Filter Settings
- Update Filter Lists

Check “Select All” to upload all of the Antigen templates or select the individual templates as needed. You may select multiple options.

Click “Finish” and the new package will be added to the “Package Names” list in the Manage Packages work panel.

Configuring the Template Deployment Job

After the Template Package has been created, click on “Jobs” in the Job Management area of the navigation bar. The Manage Jobs work panel will open. Highlight “Deployment Jobs” and click on the “Create” button. The “Add Deployment Job” work panel will open as shown below:

SYBARI Enterprise Manager Add Deployment Job

• At a glance...

SEM Administration:

- Users
- Servers
- Server Groups
- Global Configuration

Job Management:

- Packages
- Jobs

Reports:

- Detections
- SMTP Traffic
- Engine Versions

Alert Management:

- Alerts

Event Logs:

- Alerts
- Deployment
- Redistribution

• Help

Use this page to add deployment jobs to the Sybari Enterprise Manager.

Job Name Template Deployment 1

Select Package Package Name: Template Package 1 [Add Package]

Select the package you want to deploy, or upload a new package for installation

Schedule Install Schedule Options: Don't Schedule Deployment

Start Date: 5/18/2004

Start Time: 12 : 00 : AM

Select the time you want the agent to begin installing the package on the target machine.

eMail Notification eMail Recipients: [Add]

Follow the steps below to configure the Template Deployment Job:

1. Name the Deployment Job
2. Select the Package. Either select a Package that you have already configured from the drop down list (In this case the Template file that you uploaded previously.) or you can upload it now by clicking on the “Add Package” button.
3. Schedule the deployment if desired. If you don't schedule the deployment, you will have to manually start the Template Deployment Job after you have completed the configuration.
4. Enter the e-mail address that should receive the success/failure notification(s) following the deployment of the job.
5. Click “Next.” The “Assign Job” work panel will open.
6. Assign the job by selecting the Target Server(s) or deployment group.
7. Click “Finish” to complete the job configuration.

After you have completed configuring the Template Deployment Job, it will be added to the “Manage Jobs” work panel under the “Deployment Jobs” section. If you have not scheduled the job, you can run the job by highlighting the job and clicking on the “Run Now” button. You may also edit, copy, or delete the job from the “Manage Jobs” work panel.

Deploying the Antigen License File on Remote Servers

To deploy the Antigen License file (license.cfg) to remote servers, you will need to configure the License Package and create and run a Deployment Job for the target server(s). Each step is described below.

Creating the License Package

The “License Package” consists of the Antigen License File (license.cfg). Click on the “Packages” button in the Job Management area of the navigation bar to begin. The Manage Packages work panel will open. Follow the steps below to create the License Package:

1. Click on the “Add Package” button. The “Add Package” screen will be displayed.
2. Enter a name for the Package.
3. Enter the path to the license.cfg file or use the Browse button to navigate to the file.
4. Click on the “Add Package” button. The license file is uploaded to the SEM database.

Click “Finish” and the new package will be added to the “Package Names” list in the Manage Packages work panel.

Configuring the License Deployment Job

After the License Package has been created, click on “Jobs” in the Job Management area of the navigation bar. The Manage Jobs work panel will open. Highlight “Deployment Jobs” and click on the “Create” button. The “Add Deployment Job” work panel will open.

Follow the steps below to configure the License Deployment Job:

1. Name the Deployment Job
2. Select the Package. Either select a Package that you have already configured from the drop down list (In this case the License package that you uploaded previously.) or you can upload it now by clicking on the “Add Package” button.
3. Schedule the deployment if desired. If you don’t schedule the deployment, you will have to manually start the License Deployment Job after you have completed the configuration.
4. Enter the e-mail address that should receive the success/failure notification(s) following the deployment of the job.
5. Click “Next.” The “Assign Job” work panel will open.
6. Assign the job by selecting the Target Server(s) or deployment group.
7. Click “Finish” to complete the job configuration.

After you have completed configuring the License Deployment Job, it will be added to the “Manage Jobs” work panel under the “Deployment Jobs” section. If you have not scheduled the job, you can run the job by highlighting the job and clicking on the “Run Now” button. You may also edit, copy, or delete the job from the “Manage Jobs” work panel.

The Rollback Button

The Rollback Button on the Manage Jobs work panel serves two functions. For Install Deployment jobs, it will uninstall Antigen. For Signature Redistribution Jobs, it will rollback to the previous engine. To use the Rollback Button, highlight the job you would like to roll back and click the Rollback button.

Chapter 6 – Reports

The Sybari Enterprise Manager can collect information from all of the managed servers and generate reports on a variety of Antigen related topics. There are four main Report categories:

- Detection Reports
- SMTP Traffic Reports
- Engine Versions

The SEM regularly polls all of the servers it manages to collect data about scanner activity, engine versions, and SMTP traffic. The polling interval is set in the Global Configuration work panel as described in Chapter 4 above. If you are running reports manually, you should first open the Global Configuration work panel and click the “Poll Now” button to ensure that the SEM has the most recent data from the servers it manages.

The reports available in each category are described below.

Detection Reports

Detection Reports are used to collect and present data about the number of viruses, filter matches, and spam incidents detected during a certain period on selected or multiple Exchange servers running Antigen. The report options include:

- Virus Detection Report
- Virus Detection Summary
- Virus Action Report
- Virus Action Summary
- Top N Viruses Found
- Spam Detection Report
- Spam Detection Summary
- Spam Action Report
- Spam Action Summary
- Content Filter Report
- Content Filter Summary
- File Filter Report
- File Filter Report Summary
- Filter Action Report
- Filter Action Summary
- Filter Statistics
- Filter Statistics for all servers.

Traffic Reports

Traffic Reports are used to collect and present data about the amount of activity on selected SMTP servers running Antigen. The report options include:

- SMTP Messages Processed
- SMTP Messages Processed Summary
- SMTP Bytes Processed
- SMTP Bytes Processed Summary

Engine Versions

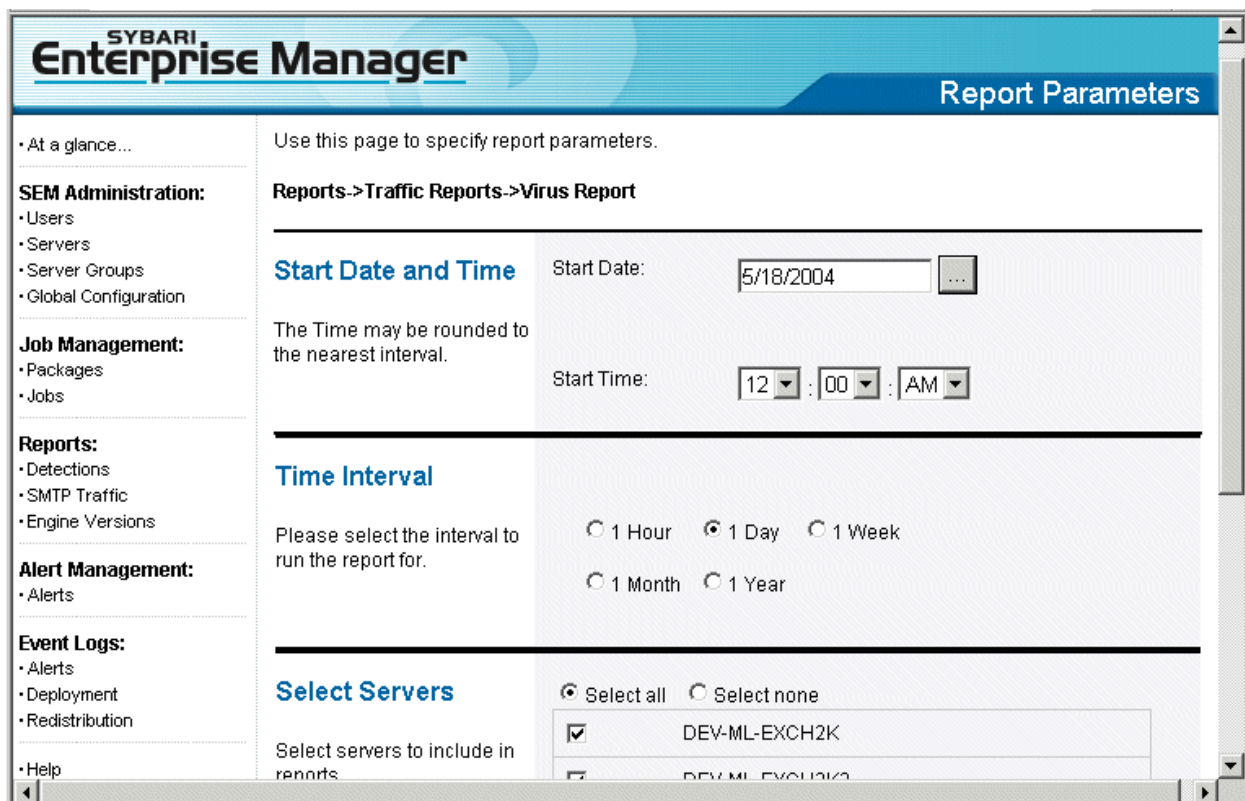
Engine Version Reports are used to collect and present data about the anti-virus and anti-spam engine versions on selected or multiple Exchange servers running Antigen. The report options include:

- o Engine Versions Report

Configuring and Running Reports

To run any of the reports, open the desired category by clicking on the category name in the Reports area of the navigation bar, then click on the Report that you would like the SEM to generate. Follow the steps below to configure and run the selected report: (The Virus Detection report will be configured in the steps below as an example. All reports are configured and run following the same basic steps, with the exception of Engine Version reports that are described later.)

1. Click on Detection Reports in the Reports area of the Navigation bar. The Detection Reports work panel will open.
2. Click on "Virus Detection Reports" in the reports list. The Report Parameters work panel will open as shown in the image below:



3. Complete the following information:

Select Products: Select which products to include in the report. Your choices include Antigen for Exchange, IM, and/or SharePoint.

Start Date and Time: Enter the start date and time. This date and time indicates the Starting point of the data collection.

Time Interval: Enter the time period that the report should cover. The options are: 1 Hour, 1 Day, 1 Week, 1 Month, and 1 Year. **For example:** If you

want to collect information for the past week, you would a start date of one week previous and select 1 Week as the interval.

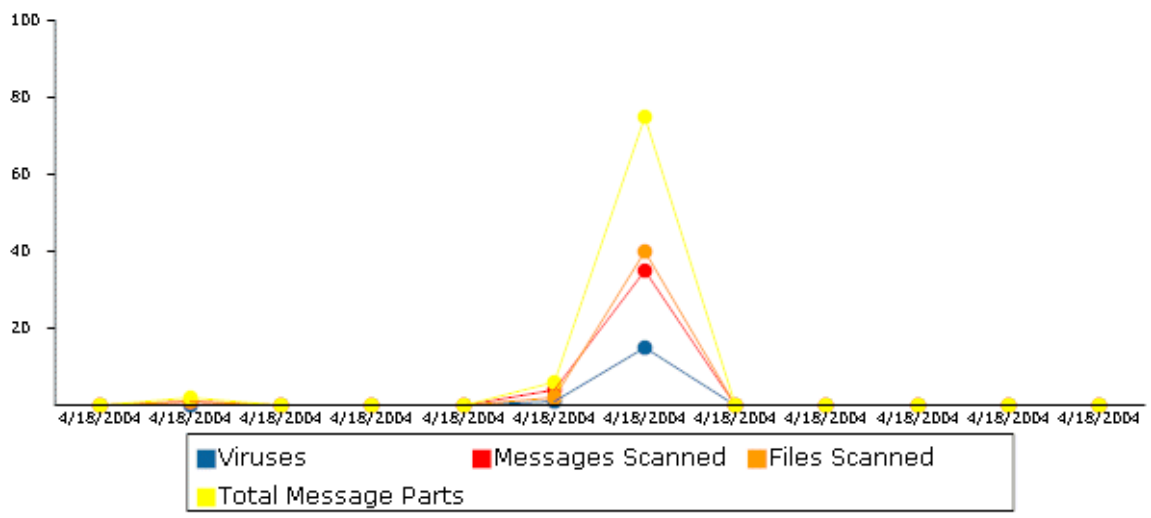
Select Servers: Select the servers that should be included in the report.

After you have completed all fields, click on the OK button to generate the report. The report will be displayed in a separate window. A sample report is shown below:

SYBARI Enterprise Manager

Virus Detection Report
 for the period from
4/18/2004 12:00:00 AM
 to
4/19/2004 12:00:00 AM

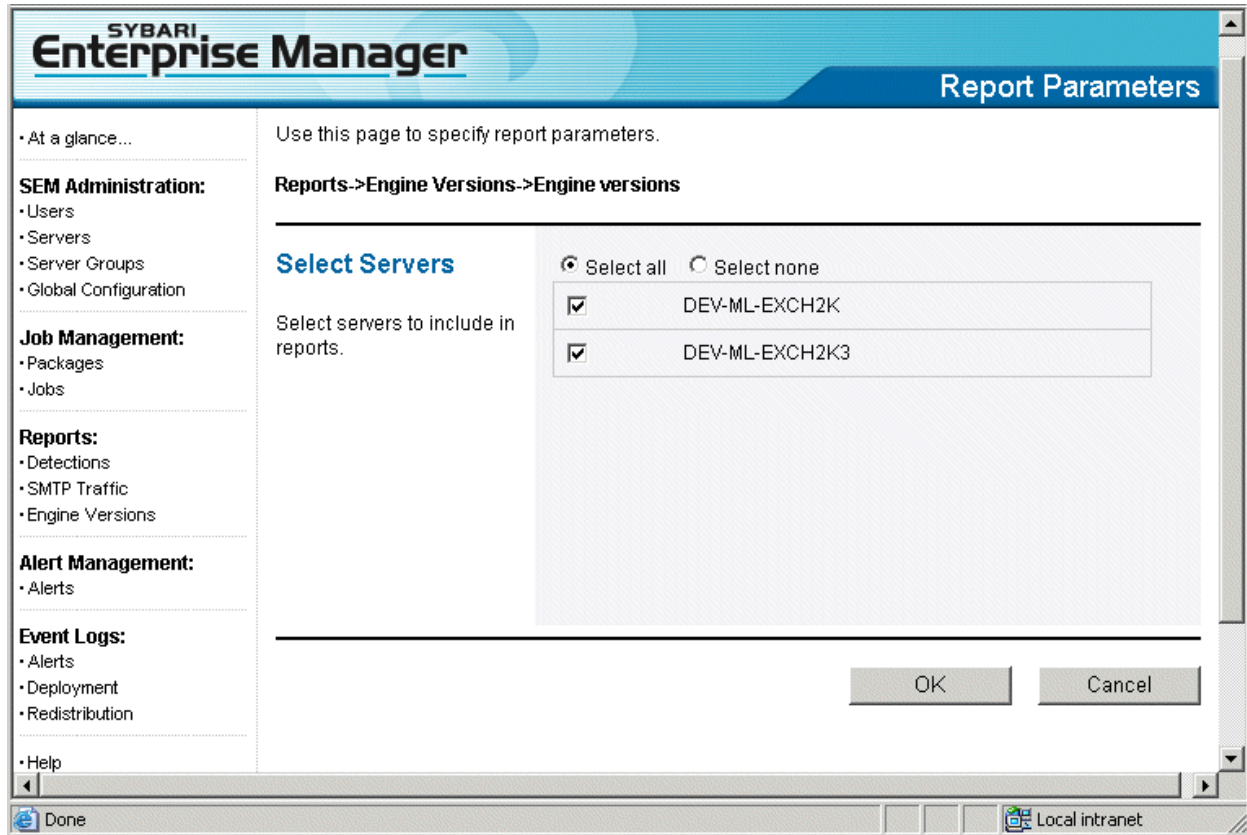
Server list processed
 qa-vm-greeceex1; qa-vm-greeceex2



Dates	Viruses	Messages Scanned	Files Scanned	Total Message Parts
4/18/2004 12:00:00 AM-4/18/2004 2:00:00 AM	0	0	0	0
4/18/2004 2:00:00 AM-4/18/2004 4:00:00 AM	0	1	1	2
4/18/2004 4:00:00 AM-4/18/2004 6:00:00 AM	0	0	0	0
4/18/2004 6:00:00 AM-4/18/2004 8:00:00 AM	0	0	0	0
4/18/2004 8:00:00 AM-4/18/2004 10:00:00 AM	0	0	0	0
4/18/2004 10:00:00 AM-4/18/2004 12:00:00 PM	1	4	2	6
4/18/2004 12:00:00 PM-4/18/2004 2:00:00 PM	15	35	40	75
4/18/2004 2:00:00 PM-4/18/2004 4:00:00 PM	0	0	0	0
4/18/2004 4:00:00 PM-4/18/2004 6:00:00 PM	0	0	0	0
4/18/2004 6:00:00 PM-4/18/2004 8:00:00 PM	0	0	0	0
4/18/2004 8:00:00 PM-4/18/2004 10:00:00 PM	0	0	0	0
4/18/2004 10:00:00 PM-4/19/2004 12:00:00 AM	0	0	0	0

Configuring and Running the Engine Versions Report

The only report that is configured differently is the Engine Versions report. When this job is selected, the Report Parameters screen shown below will be displayed:



To configure this report, select the servers from which to collect version data and click on the OK button.

Saving SEM Reports

Reports generated by the SEM can be saved for later use. SEM reports can be saved as HTM or MHT files. Follow the directions below to save report files:

1. Run the desired report.
2. The report window that is displayed has a menu. Choose "File"-> "Save As."
3. Give the file a name and a location, then hit "Save." (For Location, we recommend creating a new folder for each report.)

The report is now saved. If you are saving the report as an HTM file, the SEM will create a sub-directory to store image files used in the report. If you copy the report file to another location, the SEM will automatically copy the associated image directory.

If you are saving the report as an MHT file, the report will be saved as an individual HTML archive with all the graphics in-line to the message. This simplifies the e-mailing and sending of reports, as they are completely self-contained.

Scheduled e-Mail Reports

Administrators can also schedule reports in the SEM that will be e-mailed to an administrator configured list of recipients. Reports are sent as mht archive files and can be viewed using IE, MS Word, MS Outlook, and other MS products.

Follow the steps below to configure a scheduled report:

Click on “Jobs” in the Job Management area of the left navigation panel and then select “Schedule Report Job.” The Schedule Report Job work panel will open as shown in the image below:

The screenshot shows the 'Schedule Report Job' configuration page in the Sybari Enterprise Manager. The page is divided into a left navigation pane and a main configuration area. The navigation pane includes sections for SEM Administration (Users, Servers, Server Groups, Global Configuration), Job Management (Packages, Jobs), Reports (Detections, SMTP Traffic, Engine Versions), Alert Management (Alerts), and Event Logs (Alerts, Deployment, Redistribution). The main configuration area contains the following sections:

- Job Name:** A text input field containing 'Detection Report'.
- Schedule Report:** A section with a description: 'Select Report Interval that you want SEM Server to send the reports.' It includes a 'Report Interval' field set to '12' with a 'Hours' dropdown, a 'Don't Schedule Reports' checkbox, and a 'Start Time' field set to '12 : 00 : AM'.
- E-mail Notification:** A section with a description: 'Select an e-mail address to send success or failure notices to. (These are in addition to the defaults specified in the distribution heirarchy.)' It includes an 'eMail Subject' field with 'Sybari SEM Schedule Report', an 'eMail Body' text area with the text 'This is an auto email from Sybari SEM Schedule Report. Please do not reply to this message.', and an 'eMail Recipients' field with an 'Add' button. Below the recipients field is a blue bar labeled 'destination addresses'.

Complete the following fields:

- Job Name:** Name the Report Job.
- Schedule Report:** Set the interval for the SEM to send the reports (in hours).
- E-mail Notifications:** Enter the Subject Line, e-mail body text, and e-mail recipients.
- Select Report:** Select the report you would like SEM to run. You may only schedule one report at a time. Multiple reports must be scheduled individually.
- Select Products:** Select the products you would like to include in the report.
- Time Interval:** Select the time interval for the report. You can choose one day, one week, one month, or one year.

Select Servers: Select the servers that should be included in the report.

Click "Finish" to save your Scheduled Report. The report will run at the scheduled time and be sent to the e-mail addresses configured eMail Recipients field.

Chapter 7 – Alert Management

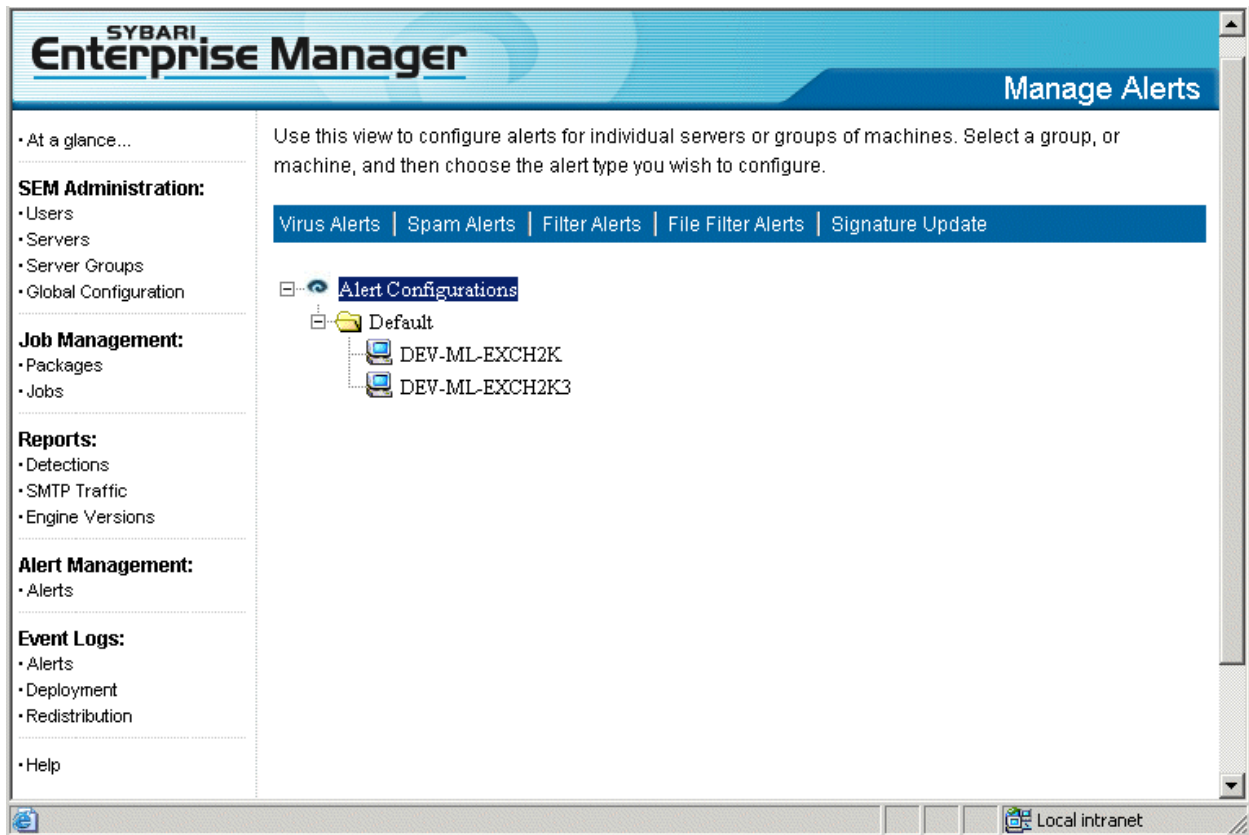
The Sybari Enterprise Manager can be configured to provide Alerts about a variety of events on the servers managed by the SEM.

Configuring Alerts

The SEM can be configured to provide the Alerts described below:

- Virus Alerts:* Used to notify administrators of possible virus outbreaks.
- Spam Alerts:* Used to notify administrators of possible spam outbreaks/attacks.
- Filter Alerts:* Used to notify administrators of unusually high or low content filtering activity (This information is based on message counts.).
- File Filter Alerts:* Used to notify administrators of unusually high or low file filtering activity (This information is based on file attachment counts.).
- Signature Update Alerts:* Used to notify administrators of the success or failure of signature file updates.

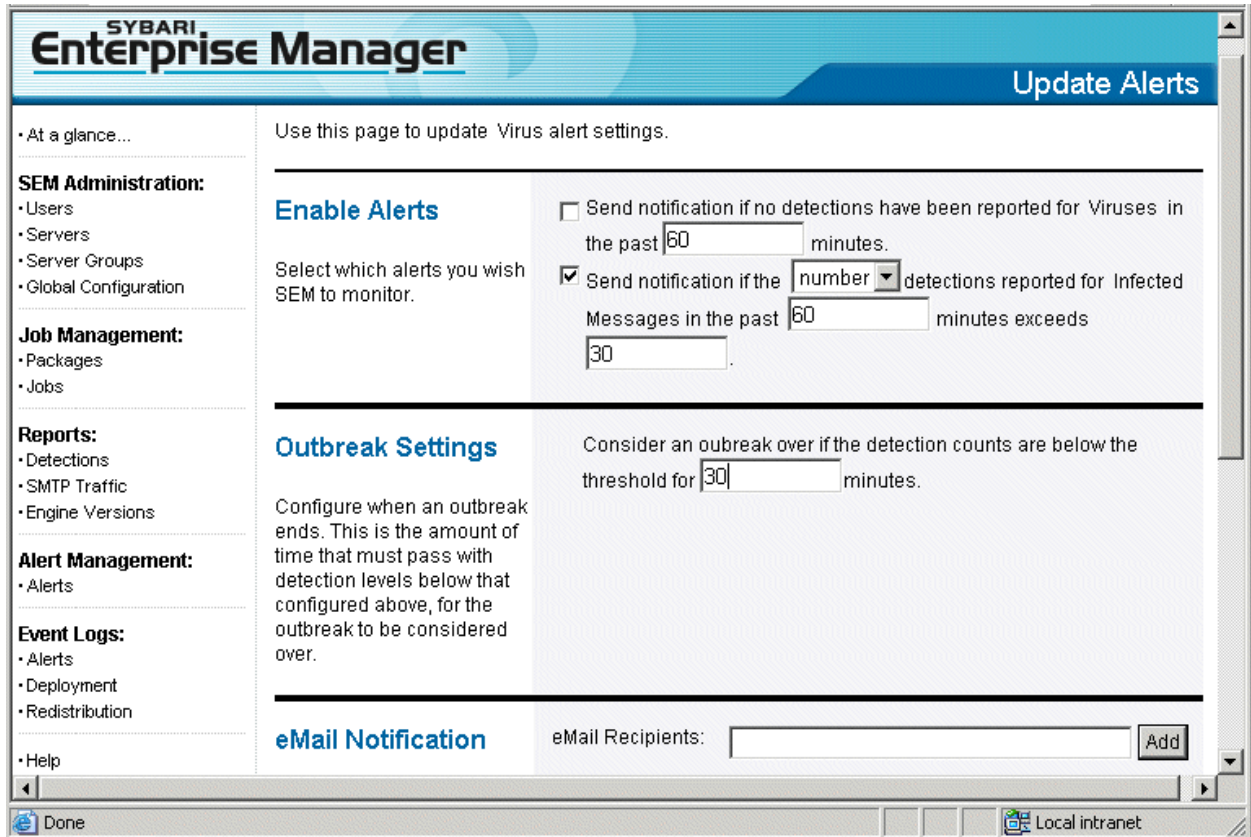
To open the Alerts work panel, click on “Alerts” in the Alert Management area of the navigation bar. The Alerts work panel will open as shown below:



To configure an alert, select the server or server group for which you would like to configure the Alert and click on the alert type button at the top of the panel. (The Virus Alert will be configured in the steps below)

as an example. All reports are configured and run following the same basic steps except for the Virus Signature Update Alert that will be described below.) Follow the steps below to configure the Alert:

1. Click on the Virus Alerts button. The Update Alerts work panel will open as shown in the image below:



2. Complete the following information:
 - a. *Enable Alerts:* Choose what events should trigger a notification. You can configure the SEM to alert you if no viruses are detected during a specified period or if the number of viruses detected surpasses a certain threshold during a specified period.
 - b. *Outbreak Settings:* This setting is used to notify the administrator when a virus outbreak has ended. Enter the length of time that the virus detection rate must be below the alert threshold after an alert has been triggered in order to consider the outbreak over.
 - c. *E-mail Notification:* Enter the e-mail addresses of administrators and others who should receive the Virus Alert notifications.
 - d. *SNMP Notification:* If you would like to receive SNMP Traps, enter the name of the server that should receive the notifications.
3. Click on the Save button to finish.

The Signature Update Alert

The Signature Update Alert is designed to alert administrators upon the success or failure of an engine signature update. To configure this alert, follow the steps below:

1. Click on “Alerts” in the Alert Management area of the navigation bar.
2. Select the server or server group for which you would like to configure the Alert.
3. Click on the Signature Update button on the Alerts work panel. The “Update Alerts” work panel will open.
4. Complete the following information:

Enable Alerts: Check the appropriate checkboxes to configure the SEM to send alerts upon the success of a signature update or the failure of a signature update.

E-mail Notification: Enter the e-mail addresses of administrators and others who should receive the Signature Update notifications.

SNMP Notification: If you would like to receive SNMP Notifications, enter the name of the server that should receive the notifications.

5. Click on the Save button to finish.

Event Logs

The Event Logs work panel is used to review the various logs maintained by the SEM. These logs include:

Alerts Log: Log of all Alerts sent by the SEM.

Deployment Log: Log of all Deployment Job activity.

Redistribution Log: Log of all Signature Redistribution activity.

To open a Log work panel, click on appropriate log name in the Event Logs area of the navigation bar. The Log work panel will open and display current log information.

Chapter 8 - Getting Help

Sybari support technicians are available to answer questions and help solve problems you may be having with your software. Please contact the support office nearest to your location.

Sybari Web Site:

Visit the support area at <http://www.sybari.com> for FAQs, support submission forms & downloads.

E-mail:

North America: support@sybari.com

Europe: support.eu@sybari.com

Asia: support.APAC@sybari.com

Australia and New Zealand: support.anz@sybari.com

Phone:

East Northport, NY Support Office: (631) 630-8500 option #2 (8 am – 8 pm EST)

San Jose, CA Support Office: (408) 938-9050 option #3 (8 am – 6 pm PST)

Madrid, Spain Support Office: (34) 91 296 2600 (9 am – 7 pm ECT)

Singapore Support Office: (65) 6533 3018 Ext. 16 (9 am - 6 pm Singapore Time)

Sydney, Australia Support Office: (61) 2 9495 9700 (9 am - 6 pm Sydney Time)