ePolicy Orchestrator® 3.5
Easy steps to set up ePolicy Orchestrator and try out new features in a test environment

McAfee®
System Protection
Industry-leading intrusion prevention solutions
Contents

Introduction: Before You Begin  4
Step 1: Install the ePolicy Orchestrator server and console  8
Step 2: Create your Directory of managed computers  10
  1. Add computers to your Directory  11
  2. Organize computers into groups for servers and workstations  15
Step 3: Push agents to the clients in your Directory  16
  1. Configure the agent policies before deploying  17
  2. Initiate an agent installation to the computers in your site  18
Step 4: Install agent manually on client computers  19
Step 5: Set VirusScan Enterprise 8.0i policies before deploying  20
Step 6: Deploy VirusScan Enterprise to clients  29
Step 7: Run a report to confirm your coverage  32
Step 8: Update DAT files with a client update task  33
Step 9: Schedule automatic repository synchronization  35
  1. Schedule a pull task to update master repository  35
  2. Schedule a replication task to update your distributed repository  36
  3. Schedule a client update task to update DATs daily  37
Step 10: Test global updating with SuperAgents  38
  1. Deploy a SuperAgent to each subnet  38
  2. Enable global updating on ePolicy Orchestrator server  39
Step 11: Where to go from here?  40

Feature Evaluations  41
ePolicy Orchestrator Notification  41
  1. Configure agent policy to upload events immediately  41
  2. Configure Notifications  42
Step 3: Creating a rule for any VirusScan Enterprise event  44
Step 4: Providing a sample virus detection  46
Rogue System Detection  46
  1. Configure Rogue System Detection sensor policy  47
  2. Deploy the Rogue System Detection sensor  48
  3. Configure an automatic response  50
  4. Rogue detection and remediation  51
Introduction: Before You Begin

This evaluation guide demonstrates how you can install and deploy ePolicy Orchestrator in a test environment. It provides easy steps that gets you up and running quickly with a test deployment of ePolicy Orchestrator 3.5, and illustrates important features.

This guide is divided into two sections:

- Installation and Setup
- Maintaining and Monitoring your Environment

Install ePolicy Orchestrator and deploy VirusScan Enterprise in ten easy steps

The steps covered in this evaluation guide are:

1. Install the ePolicy Orchestrator server and console.
2. Create your Directory of managed computers.
4. Set up master and distributed repositories.
5. Set VirusScan Enterprise 8.0i policies before deploying.
6. Deploy VirusScan Enterprise to clients.
7. Run a report to confirm your coverage.
8. Update DAT files with a client update task.
9. Schedule automatic repository synchronization.
10. Test global updating with SuperAgents.

What is covered in this guide

This evaluation guide describes how to deploy ePolicy Orchestrator 3.5 in a small lab environment consisting of one ePolicy Orchestrator server and a small number of client computers. The demonstrates the basic steps required to deploy ePolicy Orchestrator in this environment quickly and test its most important features.

What is not covered in this guide

This document does not cover everything that ePolicy Orchestrator can do, including many advanced features or installation scenarios typical in real-world deployments. While you can follow many of these basic steps for your live deployment, this guide may not cover everything you will need. For complete information on all aspects of the product, including advanced features, refer to the ePolicy Orchestrator 3.5 Product Guide.
Before you begin installing and testing ePolicy Orchestrator, you must first create a safe test network. Planning and testing a live deployment in your organization may take weeks or even months, especially if your organization is very large. However, you should be able to create a small test environment within several hours, or identify several existing computers on your network for testing within even less time.

At the very least, this environment should contain one server computer to host the ePolicy Orchestrator server, and one or more client computers, which can be either servers or workstations, to which you deploy agents and VirusScan Enterprise 8.0i. See the ePolicy Orchestrator 3.5 Installation Guide and VirusScan Enterprise 8.0i Installation Guide for complete software and hardware requirements for the ePolicy Orchestrator server, the agent, and VirusScan Enterprise 8.0i.

As you set up your test environment, ensure your network is correctly configured for ePolicy Orchestrator by considering:

1 **Create a network user account with administrator privileges.** If you plan to use the ePolicy Orchestrator server to push agents to computers, the server must have administrator credentials. You can configure ePolicy Orchestrator to use these credentials when you install the server, or you can specify them when you push the agent. Either way, you will need an administrator user name and password to deploy agents from the ePolicy Orchestrator console.

2 **Create trusted domain connections to any remote NT domains.** If you plan to test deploying agents to computers located outside the local NT domain where the ePolicy Orchestrator server resides, you must create a trusted connection between the domains. This connection is required to allow the server to deploy agents and install software on these remote clients. See your Microsoft Windows documentation for information on how to do this. Furthermore, you must have a user account with administrator rights in the remote domain for the ePolicy Orchestrator server to be able to deploy agents to those clients.
3 **Ping client computers from the ePolicy Orchestrator server.** From the computer where you plan to install the ePolicy Orchestrator server, ping client computers to which you plan to deploy agents to test network connectivity. To do this from your server, open a command window by selecting **Start** | **Run** and typing `cmd` at the run prompt. Then type ping commands, using the syntax below. Test both computer name and IP address:

```
ping MyComputer
ping 192.168.14.52
```

4 **Confirm that client NT Admin$ share folders are accessible from the server.** From the computer on which you plan to install your ePolicy Orchestrator server, test access to the default Admin$ share folder on each client computer. The ePolicy Orchestrator server service requires access to this shared folder to install agents and other software, such as VirusScan Enterprise. This test also confirms your administrator credentials, because you cannot access remote Admin$ shares without administrator rights. To access client Admin$ shares from the ePolicy Orchestrator server, do the following:

   a  Select **Start** | **Run**.

   b  At the run prompt, type the path to the client Admin$ share by specifying either computer name or IP address:

```
\MyComputer\Admin$
\192.168.14.52\Admin$
```

If the computers are properly connected over the network, your credentials have sufficient rights, and the Admin$ shared folder is present, you should see a Windows Explorer dialog box.

5 **Install Microsoft updates on any Windows 95, Windows 98, or Windows ME client computers.** If you include clients running Windows 95, Windows 98, or Windows ME in your test, download VCREDIST.EXE and DCOM 1.3 updates from the Microsoft web site and install them on these clients as required. ePolicy Orchestrator agents will not run on these clients without them. See the ePolicy Orchestrator 3.5 Installation Guide or the following links for information:

```
  support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q259403
  www.microsoft.com/com/dcom/dcom95/dcom1_3.asp
```

6 **Enable File and Print Sharing on Windows 95, Windows 98, or Windows ME client computers.** If you plan to deploy the agent to Windows 95, Windows 98, or Windows ME clients, you must first enable File and Print Sharing on those clients. This is only required if you plan to **push** agents to these clients. If you install the agent manually or through some other method, such as a logon script, this is not required. Once you have pushed the agent to these Windows 95, Windows 98, Windows ME clients, you can disable File and Print Sharing again and still manage agent policies on those clients with ePolicy Orchestrator.

**About the lab environment used in this guide**

The lab environment used in this guide consists of one NT domain and one Active Directory container, each containing several servers and several workstations.
Having multiple NT domains or Active Directory containers in your lab environment is not required to use this guide or test ePolicy Orchestrator.

### Table 1 Computers in Domain1 (IP addresses 192.168.14.1-255)

<table>
<thead>
<tr>
<th>Computer</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>ePO Server</td>
<td>Windows 2000 Server SP 4 running SQL Server 2000 SP 3. This computer hosts the ePolicy Orchestrator server, console, database, and master software repository.</td>
</tr>
<tr>
<td>4 clients</td>
<td>Running Windows 2000 Professional.</td>
</tr>
</tbody>
</table>

### Table 2 Computers in Domain2 (IP addresses 192.168.15.1-255)

<table>
<thead>
<tr>
<th>Computer</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 clients</td>
<td>Running Windows 2000 Professional.</td>
</tr>
</tbody>
</table>

**Get installation files from McAfee**

Before you start installing, get the installation files for ePolicy Orchestrator and VirusScan Enterprise from the McAfee web site or your product CD, if you have one. If you want to use the 30-day evaluation versions for your tests, download them from the McAfee web site. The files you need are:

- **EPO350EML.ZIP** The installation files necessary for installing the ePolicy Orchestrator 3.1 server, console, and database.
- **VSE800EEN.ZIP** The VirusScan Enterprise 8.0i installation files, including the PkgCatalog.z package file required to deploy VirusScan Enterprise through ePolicy Orchestrator.
- **VSC451Lens1.ZIP** The VirusScan 4.5.1 installation files and PkgCatalog.z file. You only need VirusScan 4.5.1 if you have client computers running Windows 95, Windows 98, or Windows ME, because VirusScan Enterprise 8.0i does not run on these operating systems.

To download the files from the McAfee web site:

1. From the computer on which you plan to install the ePolicy Orchestrator server and console, open a web browser and go to:  
2. Select ePolicy Orchestrator Enterprise Edition 3.5 from the list and click the TRY link.
3. Fill out the form and follow directions to download the EPO350EML.ZIP file.
4. Extract the contents of the EPO350EML.ZIP to a temporary folder, such as C:\ePOTemp.
5. Repeat these steps to download the VSE80iEVAL.ZIP evaluation version of VirusScan Enterprise 8.0i and the VSC451Lens1.ZIP of VirusScan 4.5.1.
6. Extract the contents of the downloaded .ZIP files into a temporary folder on the computer you plan to use as your test ePolicy Orchestrator server.

You need to access files in these folders at various times during the deployment process covered in this guide.
**STEP 1**

**Install the ePolicy Orchestrator server and console**

Install the ePolicy Orchestrator server, console, and database on the computer you plan to use as your ePolicy Orchestrator server. In the examples used in this guide, we install the ePolicy Orchestrator server to the computer called `ePOServer` that is running the Windows 2000 Server operating system.

To install the ePolicy Orchestrator console and server:

1. Locate and start the `SETUP.EXE` file located in the root of the `ePOTemp` folder where you extracted the `EPO350EML.ZIP`.

2. Click **Next** at the initial page of the ePolicy Orchestrator 3.5.0 Setup wizard.

3. If you are installing an evaluation version, click **OK** at the Evaluation page.

4. On the license agreement, select **I accept the terms in the license agreement** and click **OK**.

5. On Installation Options, select **Install Server and Console** and click **Next**. You can also change the installation folder if desired.

6. If you see a message box stating that your server does not have a static IP address, ignore it by clicking **OK**.

   While McAfee recommends installing ePolicy Orchestrator on a computer with a static IP address in your production environment, a DHCP-assigned IP address can be used for testing purposes.

7. On the **Set Server Password** dialog box, enter the password you would like to use for the ePolicy Orchestrator server. You cannot leave this blank.

8. On the **Server Service Account** dialog box, deselect Use Local System Account.

9. In the Account Information area, enter a domain, user name and password to be used by the ePolicy Orchestrator server service.

10. Click **Next** to save the account information and continue.

   **Note**

   If the account you specified is not an administrator account, you will see a warning that you cannot use ePolicy Orchestrator to deploy agents. If you want the ePolicy Orchestrator server service to have rights so that you can deploy agents, click **OK** then **Back** and type a user account and password with administrator rights. Alternatively, you can use a non-administrator account for the ePolicy Orchestrator server service and still deploy agents by specifying administrator credentials at deployment time. Finally, you can choose not to deploy agents through ePolicy Orchestrator at all, but rather install the agent manually and use ePolicy Orchestrator only to manage policies. In this case you do not need administrator rights for your server service account.

11. On the **Select Database Server** dialog box, select **Install a server on this computer and use it**. This option installs the free MSDE database included with ePolicy Orchestrator.

12. Click **Next**.

13. On the **Database Server Account** dialog box, deselect Use the same account as the Server service, then select **This is a SQL Server account**. Type in and verify a secure password. This is the `SA` account that your ePolicy Orchestrator server service uses to access the MSDE database.

14. Click **Next** to save the database account information.
15 On the **HTTP Configuration** dialog box, change the **HTTP port for Agent communication** to 82 and the **HTTP port for Console communication** to 83.

**Figure 1 Change the HTTP ports used by agent and console if already being used**

Some HTTP ports, and ports 80 and 81 in particular, are commonly used by many HTTP applications and services. Because of this, port 80 may already be in use and not available. McAfee recommends changing the port number to avoid this conflict.

16 Click **Next** to save the port information.

If you do see a warning message saying that one or more HTTP ports are in use, click **OK** and repeat **Step 15**, this time specifying unused HTTP ports.

17 On the **Set E-mail Address** dialog box, type the e-mail address to which the default notification rules send messages once they are enabled.

This e-mail address is used by the ePolicy Orchestrator Notifications feature. This feature is covered in this guide, so enter an e-mail address that receives messages you can view.

18 On the **Ready to Install** dialog box, click **Install** to begin the installation.

The installation takes approximately 20 minutes to complete and may prompt you to reboot the computer during the installation.

19 Click **OK** when prompted to reboot and be sure to log back in when the computer reboots to allow the installation to continue.

20 When the installation is finished, click **Finish**.

Once the installation is complete, you can open the ePolicy Orchestrator console to begin deploying agents and anti-virus products to the client computers in your network.
Start the ePolicy Orchestrator console for the first time

Now your server is installed and running. Open the ePolicy Orchestrator console to begin using ePolicy Orchestrator to manage policies on your network.

To open the console from your ePolicy Orchestrator server:

1. Click the Start button, then select Programs | Network Associates | ePolicy Orchestrator 3.5.0 Console.
2. On the Start Page, click Log on to server.
3. When the Log on to Server dialog box appears, make sure the Server name displays the name of your ePolicy Orchestrator server and that the User name is administrator, then type the Password you set during the installation wizard, and click OK.
4. If you have installed an evaluation version, click OK at the Evaluation splash screen.

Wait a few moments while the ePolicy Orchestrator server initializes. You are now ready to use the ePolicy Orchestrator console.

Congratulations on a successful installation of your ePolicy Orchestrator server, console, and database!

Create your Directory of managed computers

The Directory is in the left-hand console tree of the ePolicy Orchestrator console. The Directory contains all the computers in your network that are managed by ePolicy Orchestrator. In other words, the Directory contains all the computers in your network running active ePolicy Orchestrator agents that are reporting to this server.

Before you start managing client anti-virus policies for computers on your network, you must add those computers to your ePolicy Orchestrator Directory. After installing the server, you initially have one computer in the Directory—the ePolicy Orchestrator server itself.

To organize your computers, you can group them into logical collections called sites and groups. You can create a tree hierarchy of sites and groups, much like you would create a hierarchy of folders in Windows Explorer. Grouping is useful because ePolicy Orchestrator allows you to define policies at the group level. You can group computers according to any criteria that makes sense for your organization.

This guide uses three common levels of grouping:

- **NT Domain.** Using your existing NT network domains as sites makes creating your Directory fast and easy. Having your Directory structure mirror your network structure can also mean you only have to remember one hierarchy not two.

- **Active Directory containers.** Using your existing Active Directory network containers as sites makes creating your Directory, or parts of it, fast and easy. Having your Directory structure mirror your network structure also means you only have to remember one hierarchy.
- **Servers and workstations.** You may want to configure separate policies for products like VirusScan Enterprise 8.0i, depending on whether the software is running on a server or a workstation. Dividing your **Directory** into groups is not required, especially for testing in a small lab environment. However, you can use groups to experiment with setting policies for groups of computers or for how you might want to organize your **Directory**.

Other typical methods of grouping include, but are not limited to:

- **Geographical divisions.** If you have locations in various portions of the world, or in multiple time zones, you may want to divide your ePolicy Orchestrator **Directory** according to those divisions. Some of your policy or task coordination is much easier across multiple time zones if you place these computers in such sites.

- **Security divisions.** If users have various levels of security access in your environment, creating your **Directory** structure to mirror those levels may make enforcing policy much easier.

1. **Add computers to your Directory**

   The first step in creating your **Directory** is to add computers from your network. Try one of these three methods:

   - **Option A: Automatically add entire existing NT domains to your Directory.** Very easy and fast. Very useful if you plan to deploy agents to every computer in that domain. Use this method if you organized your test client computers into domains in your lab network, as in the examples in this evaluation guide.

   - **Option B: Automatically add entire Active Directory containers to your Directory.** Very easy and fast. Very useful if all or part of your environment is controlled by Active Directory and if you want portions of your ePolicy Orchestrator **Directory** to mirror portions of your Active Directory.

   - **Option C: Manually add individual computers to your Directory.** While this may be too slow when deploying ePolicy Orchestrator in a live network, it is fast enough for adding a handful of computers in your test network.

**Option A: Automatically add entire existing NT domains to your Directory**

ePolicy Orchestrator allows you to import all computers in an NT domain into your **Directory** with just a few clicks. Use this feature if you organized your test client computers into domains in your lab network.

The examples in this guide use this method to create **Directory** sites from an NT domain on the test network, **Domain1**.

To add entire NT domains to your **Directory**:

1. Right-click the **Directory** and select **New | Site**.
2. In the **Add Sites** dialog box, click **Add**.
3. In the **New Site** dialog box, type a name for the site. Make sure the name you type matches exactly the name of your NT domain.
4. Under **Type**, select **Domain** and **Include computers as child nodes**.
5. Click **Add** under **IP Management** to specify an IP address range for the site.
6. In the IP Management dialog box, type an IP subnet mask or IP range to specify the IP address ranges of computers that belong to this site.

7. Click **OK** to save the IP settings.

8. Click **OK** to save the new site and close the **New Site** dialog box.

9. In the **Add Sites** dialog box, make sure that **Send agent package** is NOT selected and click **OK** to create and populate the sites in the **Directory**. Although you can deploy agents at this point, you will do that in a later step once we have modified the agent policies.

![Figure 2 Add Sites dialog box](image)

After a few moments, the computers are added to your **Directory**. When completed, you can see that ePolicy Orchestrator first created a site in the **Directory** with the name of your network test domain and added all the computers in that domain as children of that domain.

**Option B: Automatically add entire Active Directory containers to your Directory**

ePolicy Orchestrator allows you to import all computers in an Active Directory container, and its sub-containers, into your **Directory** with just a few clicks. Use this feature if you organized your test client computers into Active Directory containers in your lab environment.

The examples in this guide use this method to create **Directory** sites from an Active Directory container, with two sub-containers.

To use ePolicy Orchestrator software's Active Directory tools, it is important that both the ePolicy Orchestrator server and the computer running the remote console, if you are using a remote console, can reach the Active Directory server.

The **Active Directory Import** wizard is meant to be used as a tool to import Active Directory computers for the first time, while you create the entire **Directory**, or only a specific site of the **Directory**. You will use the **Active Directory Computer Discovery** task to regularly poll these Active Directory containers for any new computers.

To add Active Directory containers and sub-containers to your **Directory**:

1. Right-click **Directory**, and select **New | Site**.
2 In the Add Sites dialog box, click Add.

3 In the New Site dialog box, type a name for the site, for example Container1, then click OK.

4 Make sure that Send agent package is NOT selected, then click OK.

5 Right-click Directory, and select All Tasks | Import Active Directory Computers.

6 Click Next when the Active Directory Import wizard appears.

**Figure 3 Active Directory Import wizard**

7 On the ePolicy Orchestrator Destination Group panel of the wizard you can select the Directory root or a site of the Directory to import the Active Directory computers. For the purposes of this guide, select the site you just created from the Import to this ePO location drop-down list, then click Next.

   If you want to import your entire Active Directory structure, minus exceptions, to use as your ePolicy Orchestrator Directory, select Root from this list. This will result in the Active Directory structure, minus exceptions, being imported into the Lost&Found of the Directory root.

8 On the Active Directory Authentication panel, type Active Directory user credentials with administrative rights for the Active Directory server.

9 In the Active Directory Source Container dialog box, click Browse to select the desired source container in the Active Directory Browser dialog box, then click OK.

10 If you wish to exclude a specific sub-container of the selected container, click Add under Exclude the following sub-containers, then select the desired sub-container to exclude and click OK.

11 Click Next, and view the active log for any new computers that have been imported. Verify in the ePolicy Orchestrator tree that these computers were imported.

12 Click Finish.
The Active Directory computers have been imported into the **Lost&Found** directory located under the site to which you imported them. If your Active Directory container included sub-containers, the **Lost&Found** directory retains the Active Directory hierarchy.

13 Click and drag the top of this structure from **Lost&Found**, to the site above it. (The site you selected in the wizard. For example **Container1**)

Congratulations. You have imported your Active Directory computers into a site in the ePolicy Orchestrator **Directory**.

In a production environment, once Active Directory containers have been imported, you should create an **Active Directory Computer Discovery** task. This task regularly polls administrator-specified Active Directory containers for any new computers. See the *ePolicy Orchestrator 3.5 Product Guide* for instructions. This task is beyond the scope of this guide.

**Option C: Manually add individual computers to your Directory**

When you deploy ePolicy Orchestrator in your production network, you probably want to populate the **Directory** automatically by importing your NT domains as shown in the previous section. However, for testing purposes in a small lab environment, you can also add sites and computers to your **Directory** manually. The first step, therefore, is to manually create a site. After that, you can manually add computers to it.

### Create a new site in which to group the computers

1. Right-click the **Directory** node in the console tree and select **New | Site**.
2. In the **Add Sites** dialog box, click **Add**.
3. Type a name for the site, such as **Domain1** in our example, into the **Name** field of the **New Site** dialog box.
4. Specify an IP mask or address range for the site if needed. See the previous section for details.
5. Click **OK**. The **Domain1** site is added to the **Sites to be added** list on the **Add Sites** dialog box.
6. Repeat the previous steps to create additional sites, if desired.
7. Click **OK**. ePolicy Orchestrator adds the new, empty sites to the **Directory**.

### Manually add new computers to your site

Now that you have created a site or sites, the next step is to manually add each new computer to your site. To do this:

1. In the **Directory**, right-click the site you added and select **New | Computer**.
2. In the **Add Computers** dialog box, add new computers either by clicking **Browse** to locate them in your NT Network Neighborhood, or by clicking **Add** and typing the computer’s NetBIOS name.
3. Click **OK** once you have added the names of all the computers.

ePolicy Orchestrator adds the new computers to the **Directory** beneath the site.
2 Organize computers into groups for servers and workstations

Once you’ve created sites and added computers to your Directory, it is a good idea to organize them into groups. The groups you create depend on what makes sense in your network. You may want to group computers by functional area, such as Sales, Marketing, or Development. You may want to create groups for geographic units, such as office locations. Or you may want to group computers by operating system.

The example in this guide creates groups in each site for servers and workstations. Use these groups later when setting different VirusScan Enterprise policies for servers and workstations.

To add groups to sites in your Directory and add computers to them:

1. Right-click a site that you added to the Directory and select New | Group.
2. In the Add Groups dialog box, click Add.
3. On the New Group dialog box, type the name Workstations into the Name text box.
4. If your network is designed to allow you to assign specific IP addresses to servers and workstations, create an IP range for the group. For example, in the test network shown in this guide, servers in Domain1 have IP addresses between 192.168.14.200 - 255; workstations in Domain1 have addresses 192.168.14.1 - 199.

To set an IP range for a group:

- Under IP Management on the New Group dialog box, click Add.
- In the IP Management dialog box, type an IP subnet mask or IP range to specify the IP address ranges of computers that belong to this site.
- Click OK to save the IP settings and close the IP Management dialog box.
5. Click OK to close the New Group dialog box. The group is added to the Groups to be added list.
6. Click OK on the Add Groups dialog box to add the group to your Directory.

Add computers to the new groups you created

Once the new groups appear in the Directory, drag computers from that site into the appropriate group as you would drag files in Windows Explorer. You must drag computers in the Directory one at a time; you cannot select multiple computers. Alternatively, you can use the Directory search feature (right-click the Directory and select Search) to move multiple systems at one time.
While dragging computers into groups, ignore the IP Integrity warning message if you see it by clicking OK.

Create additional groups and subgroups as needed
Repeat all these steps to create a server group for your site, as well as additional server and workstation groups for other sites, if you have them. You can also make groups within groups. For example, the test network shown in this guide has computers running both Windows 2000 and Windows 98. Due to limitations with older versions of Windows, we need to set different policies for computers running Windows 98. Creating Win98 and Win2K subgroups within our Workstation group makes setting these different policies easier.

Now your test Directory is finished. You have created sites and added computers, either manually or by importing existing NT domains on your network. And you have separated the computers in each site into separate groups for servers and different types of workstation operating systems. You’re ready for the next step—deploying agents.

---

**STEP 3**

Push agents to the clients in your Directory

Before you can do anything else to manage the client computers in your Directory, you must install an ePolicy Orchestrator agent to those client computers. The agent is a small application that resides on the client computer and periodically checks with the ePolicy Orchestrator server for updates and new instructions.

Deploying the agent from the ePolicy Orchestrator server requires the following:

- **A network account with administrator privileges.** If you specified administrator credentials when you installed your ePolicy Orchestrator server service, you will automatically be able to deploy agents; otherwise, you will need to specify appropriate credentials when you deploy.

- **Domain trusts to other NT domains, if necessary.** To deploy agents outside the local NT domain that hosts your ePolicy Orchestrator server, you must have a domain trust relationship configured between the local and target domain.

- **For Windows 95 and Windows 98 computers, install extra Microsoft updates.** Windows 95 and Windows 98 first edition require that you install additional Microsoft updates to be able to run the ePolicy Orchestrator agent. See the ePolicy Orchestrator Installation Guide for information on finding and installing these updates. You must install these updates to be able to run the agent on these systems at all, even if you do not use ePolicy Orchestrator to deploy it.

- **For Windows 95 and Windows 98 computers, turn on File and Print Sharing.** Enable File and Print Sharing on each client to which you plan to push the agent. Note that this is only a requirement to push the agent from the ePolicy Orchestrator server, not to manage policies. Once you have deployed the agent to a Windows 95 or Windows 98 computer, you can disable file and print sharing.
From the **Directory** in the ePolicy Orchestrator console, you can install the agent to all computers in a site at once. To do this, send an agent install command at the site level. Because of the concept of **inheritance**, you can specify an agent installation at the parent site (or group) level and all children, whether groups or computers, inherit the command.

In our example **Directory** containing two sites you will initiate separate agent installations to each site. These two agent installation commands install the agent to all computers in these sites.

To deploy agents to a site:

1. **Configure the agent policies before deploying.**

2. **Initiate an agent installation to the computers in your site.**

Alternatively, if you do not plan to use ePolicy Orchestrator to push the agent, you can install the agent manually from the client computer. See *Install agent manually on client computers on page 19.*

1 **Configure the agent policies before deploying**

You can deploy agents with the default policy settings. However, for testing purposes, you will modify the policy to allow the agent tray icon to display in the Windows system tray on the client computer. Not only will this expose you to setting agent policies, it also makes it easier to see when the agent has installed on your clients. When you make this policy change at the site level, it applies to all test computers that exist as children in this site. This allows you to change the policy configuration once then deploy it to all your computers in a site.

To change the agent policy so that the agent icon appears in the system tray after installation:

1. Select your site (*Domain1* in this example) by clicking it once in the **Directory** tree.

2. In the right-hand details pane, click the **Policies** tab and select **ePolicy Orchestrator Agent** | **Configuration**.

3. In the **ePolicy Orchestrator Agent** page, deselect **Inherit** to enable configuration options.

4. On the **General** tab, select **Show Agent tray icon** and click **Apply All** to save your change.
5 Repeat these steps to make the same agent policy change to other sites (Container1 in this example).

Now your policies are set and your agents are ready to deploy. The next step is to begin an agent install.

2 Initiate an agent installation to the computers in your site

Use the Install Agent feature to have ePolicy Orchestrator push agents to your client computers. Push agents to all your test computers in a site at once by initiating the agent installation at your site level in the Directory.

To initiate an agent installation for all computers in a site:

1 Right-click the site in your Directory and select Install Agent.

2 Click OK on the Install Agent dialog box to accept all default settings and begin the agent installation.

3 Repeat these steps for other sites in your Directory.

The agent installations begin immediately.

A word about deploying agents to computers running Windows 95, Windows 98, or Windows ME

When pushing agents to computers running Windows 95, Windows 98, or Windows ME you may not be able to tell that the agent has been successfully deployed until you log out of the client computer. This can include the agent icon not appearing in the system tray or the computer not showing up as managed in the ePolicy Orchestrator console Directory. If, after logging out and back into the Windows 95, Windows 98, or Windows ME clients, the agent still does not appear, try pushing it again. If that still does not work, you can install the agent manually from the client (see Install agent manually on client computers on page 19).

A word about deploying to computers outside the local NT domain

If the other site(s) contain computers residing in a different NT domain than your ePolicy Orchestrator server, you may need to specify other domain administrator credentials for the target domain.

Before initiating the agent push, deselect Use ePO server credentials on the Install Agent dialog box, and type an appropriate user name and password with domain administrator rights in the target domain.

What can I do while I’m waiting for agents to install?

It may take up to ten minutes for all the agents to be installed on all computers in your sites, and for the Directory tree to update with the new covered status. In the meantime, you can check the ePolicy Orchestrator server for events, which can alert you of failed agent installations. To view server events:

1 In the console tree of the ePolicy Orchestrator console, right-click your server and select Server Events.
2 Skim the **Server Event Viewer** for events. Successful agent installations are not displayed here, but failed installs are.

When agent deployment is complete and the agents have called back to the server for the first time, the computers in your **Directory** are marked with green checks.

If the agents have installed and the **Directory** does not reflect this, manually refresh the **Directory** by right-clicking **Directory** and selecting **Refresh**. Note that the **Directory** does not show the computers as managed until they call back to the server, usually within ten minutes. This is true even though the agent is installed and running on the clients.

You can also watch the installation from any of your client computers. The default policy suppresses the installation interface (which we did not change when we set agent policies in this example). So you cannot see the installation interface. However, you can open the Task Manager on the client computer and watch the CPU usage spike briefly as the installation begins. Once the agent is installed and running, two new services appear in the **Processes** window: **UPDATERUI.EXE** and **FRAMEWORKSERVICE.EXE**. Also, because of how we modified the agent policies before deploying, the **Icon** appears in the system tray after installing and reporting back to the server for the first time.

---

**Install agent manually on client computers**

Rather than use ePolicy Orchestrator to push the agent, you may want to install it manually from the client. Some organizations may want to install software on clients manually and use ePolicy Orchestrator to manage policies only. Or, maybe you have many Windows 95 or Windows 98 clients and do not want to enable print and file sharing on them. In these cases, you can install the agent from the client instead.

Use the **FRAMEPKG.EXE** file located on your ePolicy Orchestrator server to install the agent. The **FRAMEPKG.EXE** file is automatically created when you install the ePolicy Orchestrator server. It contains address information for your ePolicy Orchestrator server to allow the new agent to communicate with the server immediately.

By default, **FRAMEPKG.EXE** is located in the following folder on your ePolicy Orchestrator server:

```
C:\Program Files\Network Associates\ePO\3.5.0\DB\Software\Current\EPOAGENT3000\Install\0409
```

To install the agent manually:

1 **Copy** the **FRAMEPKG.EXE** file to the local client or network folder accessible from the client.

2 **Run** **FRAMEPKG.EXE** by double-clicking it. Wait a few moments while the agent installs.

At some random interval within ten minutes, the agent reports back to the ePolicy Orchestrator server for the first time. At this point, the computer is added to the **Directory** as a managed computer. If you specified IP address filtering for your **Directory** sites and groups, the client is added to the appropriate site or group for its IP address. Otherwise, the computer is added to the **Lost&Found** folder. Once the computer is added to the **Directory**, you can manage its policies through the ePolicy Orchestrator console.
You can bypass the ten-minute callback interval and force the new agent to call back to the server immediately. You do this from any computer on which an agent has just been installed.

To manually force the initial agent callback:

1. From the client computer where you just installed the agent, open a DOS command window by selecting **Start | Run**, type `command`, and press **Enter**.

2. In the command window, navigate to the agent installation folder containing the `CMDAGENT.EXE` file.

3. Type the following command (note the spaces between command line options):
   
   `CMDAGENT /p /e /c`

4. Press **Enter**. The agent calls back to the ePolicy Orchestrator server immediately.

5. From the ePolicy Orchestrator console on your server, refresh the **Directory** by clicking **F5**. The new client computer on which you have just installed the agent should now appear in your **Directory**.

---

**STEP 4**

### Set up master and distributed repositories

Now you have agents installed on your clients, but what can they do? The purpose of an agent is to allow you to manage client security software policies centrally through ePolicy Orchestrator. But until you have anti-virus software installed on the client computers, your agents have nothing to do. The next step is to use ePolicy Orchestrator to deploy VirusScan Enterprise 8.0i anti-virus software to your client computers.

Software to be deployed with ePolicy Orchestrator is stored in software repositories. There are many ways to set up your repositories. This guide demonstrates a typical example that you can use in your test environment.

See the following sections for details on how to do this. The steps covered here are:

1. **Add VirusScan Enterprise to the master repository.**

2. **Pull updates from McAfee source repository.**

3. **Create a distributed repository.**

### About using master and distributed repositories in your test network

ePolicy Orchestrator uses repositories to store the software that it deploys. This guide illustrates using both master and distributed repositories for deploying software and updating. Repositories store the software, such as the agent or VirusScan installation files, and updates, such as new DAT files, that you plan to deploy to clients. The master repository is located on the ePolicy Orchestrator server, and is the primary storehouse for your software and updates. Distributed repositories are copies of the master that can reside in other parts of your network, such as other network NT domains or other Active Directory containers. Computers in those other parts of your network can update more quickly from local servers than across a WAN to your ePolicy Orchestrator server.
Domains and Active Directory containers can be geographically separated and connected via a WAN. In this case, create a distributed repository, which is simply a copy of the master repository, on a computer in the remote location. Computers in that location, Container1 in our example, can update from the distributed repository instead of having to copy updates across the WAN.

Computers in the Domain1 site receive updates and product deployments directly from the master repository, located on the ePolicy Orchestrator server (ePOServer). Computers located in the Container1 site, however, receive them from a distributed repository located on a server.

The VirusScan Enterprise 8.0i NAP file
Policy pages, or NAP files, are used to configure client software from your ePolicy Orchestrator console. ePolicy Orchestrator 3.5 installs with several NAP files, including the VirusScan Enterprise 8.0 NAP.

1 Add VirusScan Enterprise to the master repository

The VirusScan Enterprise 8.0i policy pages, or NAP file, allow you to manage VirusScan Enterprise 8.0i policies once it has been installed on client computers in your network. However, to be able to first use ePolicy Orchestrator to push, or deploy, VirusScan Enterprise 8.0i to those client computers, you must also check in the VirusScan Enterprise deployment, or installation, package to the master software repository. The deployment package file is called PkgCatalog.z and is contained in the VSE80iEVAL.ZIP you downloaded from McAfee (see Get installation files from McAfee on page 7).

To check in the VirusScan Enterprise package to your master repository:

1 From the ePolicy Orchestrator console, select Repository in the console tree.
2 Select Check in Package from the right-hand Repository details pane.
3 When the Check in package wizard opens, click Next.
4 On the second page of the wizard, select Products or updates and click Next.

Figure 4 Check in Package wizard
5 Browse to your temporary folder containing your VirusScan Enterprise 8.0i installation files.

6 Locate and select the PkgCatalog.z package file in your VirusScan Enterprise temporary folder.

7 Click Next to continue.

8 At the final wizard page, click Finish to begin the package check-in.

Wait a few moments while ePolicy Orchestrator uploads the package to the repository.

**Check in the VirusScan 4.5.1 package if you have Windows 95, Windows 98, or Windows ME clients**

VirusScan Enterprise 8.0i does not run on Windows 95, Windows 98, or Windows ME. If you have clients in your test network running these versions of Windows, as is the case in the examples in this guide, you must deploy VirusScan 4.5.1 to these systems. To be able to do this, repeat the same procedure above to check in the VirusScan 4.5.1 deployment package to the software repository. The 4.5.1 package is also called PkgCatalog.z and is located in your temporary folder to which you have extracted the VirusScan 4.5.1 installation files.

2 **Pull updates from McAfee source repository**

Use the McAfee HTTP or FTP site as your source repository, from which you can update your master repository with the latest DAT, engine, and other updates. Initiate a repository pull from the source repository to your master repository to

- Test that your ePolicy Orchestrator server can connect over the Internet to the source repository.
- Update your master repository with the latest DAT files.

DAT files are updated often, and the DAT files included in your VirusScan Enterprise installation files are not the latest. Pull the latest DAT files from the source repository before deploying VirusScan Enterprise to your network.

**Configure proxy settings through Internet Explorer or in ePolicy Orchestrator**

Your ePolicy Orchestrator server must be able to access the Internet to pull updates from the McAfee source repository. All other computers on your network do not require Internet access—they pull updates either from your master repository or distributed repository on your network (which we will set up in the next step).

ePolicy Orchestrator by default uses your Internet Explorer proxy settings. If you have not yet done so, configure your LAN connection for Internet Explorer. Be sure to select the Use proxy for all protocols (both FTP and HTTP) and select Bypass proxy for local addresses options.

Alternatively, you can manually specify proxy server information using the Configure proxy settings option. Refer to the ePolicy Orchestrator 3.5 Product Guide for information on how to do this.

**Initiate manual pull from the McAfee source repository**

To manually pull updates from the source repository to your master repository:

1 From the console tree, click Repository.

2 Select Pull Now from the right-hand Repository details pane.
3 When the Pull Now wizard opens, click Next at the first wizard page.

4 On the next page, select NAIHttp and click Next. You can also select the default NAFtp, but HTTP is often more reliable.

**Figure 5 Pull Now wizard**

5 If you are managing older products, such as VirusScan 4.5.1 for Windows 95 or 98 computers, be sure to select Support legacy product update.

6 Click Finish at the last page to accept all defaults on this page and begin the pull.

   Wait several minutes while the pull task executes.

7 Click Close when the pull is complete.

Now you have checked in VirusScan Enterprise to your master repository and also updated the master repository with the latest DAT and engine files from the McAfee source repository. The computers located in the same domain as your ePolicy Orchestrator server, those computers in your Domain1 site in the Directory in this example, get VirusScan Enterprise from the master repository.

But where do other computers get their software and updates? If these computers are located in different subnets or a WAN-connected location, it may be more efficient to create a distributed repository, or a copy of the master repository, that is more easily accessible to these computers.

3 **Create a distributed repository**

Now we need to create a distributed repository in Container1 so that those computers can update from there. Your test network, with only a few clients and one ePolicy Orchestrator server, is small enough to not require an elaborate distributed repository structure. However, you can use the distributed repository examples in this guide to simulate a probable real-world scenario. Such a scenario could include computers in remote domains that cannot update efficiently over a WAN-connected master repository on the ePolicy Orchestrator server.
You can use FTP, HTTP, or UNC to replicate data from the master repository to your distributed repositories. This guide describes creating a UNC share distributed repository on one of the computers in the Container1 site.

To do this:

1. **Create a shared folder on a computer to be a repository.**
2. **Add the distributed repository to the ePolicy Orchestrator server.**
3. **Replicate master repository data to distributed repository.**
4. **Configure remote site to use the distributed repository.**

1. **Create a shared folder on a computer to be a repository**

Before you add the UNC distributed repository to ePolicy Orchestrator, you must first create the folder to use. In addition, you must set the folder to enable sharing across the network so that your ePolicy Orchestrator server can copy files to it.

To create a shared folder for a UNC distributed repository:

1. From the computer on which you plan to host the distributed repository, create a new folder using Windows Explorer.
2. Right-click the folder and select **Sharing**.
3. On the **Sharing** tab, select **Share this folder**.
4. Click **OK** to accept all other defaults and enable sharing for this folder.

Caution: Creating a UNC share in this way could be a potential security problem in a production environment, because it allows everyone on your network access to the share. If creating a UNC folder in a production environment, or if you are not sure that your network test environment is secure, be sure to take extra security precautions as necessary to control access to the shared folder. Client computers only require read access to retrieve updates from the UNC repository, but administrator accounts, including the account used by ePolicy Orchestrator to replicate data, require write access. See your Microsoft Windows documentation on how to configure security settings for shared folders.
2 Add the distributed repository to the ePolicy Orchestrator server

Once you have created the folder to use as the UNC share, add a distributed repository to the ePolicy Orchestrator repository and point it at the folder you created.

To add the distributed repository:

1 From the console tree, click Repository.

2 Select Add distributed repository from in the details pane Repository pane.

3 Click Next at the first page of the wizard.

4 Type a name into the Name field. Note this is how the distributed repository name appears in the repository list in the ePolicy Orchestrator console. It does not have to be the name of the share folder that actually hosts the repository.

5 Select Distributed Repository from the Type drop-down list.

6 Select UNC for the repository configuration and click Next.
7 Type the path of the shared folder you created. Be sure to type a valid UNC path. The example in this guide would be: `\BU06\ePOshare` where BU06 is the name of a computer in Container1 and ePOshare is the name of the UNC shared folder.

8 Click Next.

9 On the download credentials page, deselect Use Logged On Account.

10 Type appropriate domain, user name, and password credentials that client computers should use when downloading updates from this distributed repository.

11 Click Verify to test the credentials. After a few seconds, you should see a confirmation dialog box confirming that the share is accessible to clients.

If your site is not verified, check that you typed the UNC path correctly on the previous wizard page and that you configured sharing correctly for the folder.

12 Click Next.

13 Enter replication credentials by typing a domain, user name and password in the appropriate text boxes.

The ePolicy Orchestrator server uses these credentials when it copies, or replicates, DAT files, engine files, or other product updates from the master repository to the distributed repository. These credentials must have administrator rights in the domain where the distributed repository is located. In our examples, these can be the same credentials used to deploy the agent. See Initiate an agent installation to the computers in your site on page 18.

14 Click Verify to test that your ePolicy Orchestrator server can write to the shared folder on the remote computer. After a few seconds, you should see a confirmation dialog box confirming that the server can do this.

15 Click Finish to add the repository. Wait a few moments while ePolicy Orchestrator adds the new distributed repository to its database.

16 Click Close.

3 Replicate master repository data to distributed repository

Now you have created a UNC share on a computer to host a distributed repository, and added the repository location to your ePolicy Orchestrator database. Now the only thing missing in the new repository is data. If you browse to your share folder you created, you can see that it is still empty.

Use the Replicate now feature to manually update your distributed repositories with the latest contents from your master repository. Later, we'll schedule a replication task so this happens automatically.

To initiate replication manually:

1 From the console tree, click Repository.
2 On the Repository page, click Replicate now to open the Replicate Now wizard.

3 Click Next at the first page of the wizard.

4 From the list of available distributed repositories, select the distributed repository you have created and click Next.

5 Select Incremental replication.

Because this is a new distributed repository, and this is the first time you are replicating to it, you could also select Full replication. However, for future replications, it is recommended to use incremental replication to save time and bandwidth.

6 Click Finish to begin replication. Wait a few minutes for replication to finish.

7 Click Close to close the wizard window.

If you browse to your ePOShare folder now, you can see that it now contains subfolders for agents and software.

4 Configure remote site to use the distributed repository

Since you have created a distributed repository, why not make sure it gets used? As stated earlier, your test network is too small to really require distributed repositories. But for the sake of simulating how they work, we can configure your updating to force computers in one site in your Directory to update only from the distributed repository instead of the master.

To simulate this in your test, let’s configure the agent policies for one of the sites in your Directory to use only the new distributed repository. In our example network used in this guide, this is the Container1 site, which is where the Win2KServer computer hosting your newly-created distributed repository resides.

To configure the ePolicy Orchestrator agent policy for the Container1 site to use the distributed repository for updating:

1 From the Directory in the console tree, select the site that you want to use the distributed repository.

2 In the right-hand policies pane, click the Policies tab.

3 Expand the ePolicy Orchestrator Agent and select Configuration.

4 Click the Repositories tab of the ePolicy Orchestrator Agent policy page.

5 Deselect Inherit to enable repository options.

6 Under Repository selection, select User defined list.

7 In the Repository list, deselect all repositories until only your distributed repository is selected.

8 Click Apply All at the top of the page to save all the changes.

Now, when the computers in this site require updates, they retrieve them from the distributed repository.
Again, forcing updates from certain repositories is shown here only for the purposes of simulating distributed repositories in a lab network. This is not something you would do in a production environment, where you would want to have some repository redundancy available for fail-over. Due to faster local network connections, client computers would likely update from a local distributed repository, rather than over a WAN to the master repository, even if not specifically configured to do this. On the other hand, if the distributed repository were unavailable for any reason, the client could still update from other repositories on the network if necessary.

**STEP 5**

**Set VirusScan Enterprise 8.0i policies before deploying**

Now that you have created your repositories and added the VirusScan Enterprise deployment package to them, you are almost ready to deploy VirusScan Enterprise to your clients. Before deploying VirusScan Enterprise, however, let’s modify the policies slightly. Remember the NAP file you checked in? We can use it to configure how VirusScan Enterprise functions once it is installed on the client computer. To demonstrate how to do this, we’ll use a simple example: changing the policies for workstations to install VirusScan Enterprise 8.0i with minimal user interface. Servers keep the default policy, which is to display the full interface.

This could be a potentially useful implementation in your real network, where you may want to hide the system tray interface on your workstations to prevent end-users from easily changing policies or disabling features.

To set these policies, we’ll use the Workstations groups created when you made your Directory. You can change the policy once for each workstation group (within Domain1 and Container1) to have it inherit to all computers within those groups. For servers, we can leave the default policy, which installs VirusScan Enterprise with the full menu options available in the system tray.

To change the VirusScan Enterprise policies for workstations:

1. From the console tree, click your Workstations group within a site.
2. In the details pane, click the Policies tab and select VirusScan Enterprise 8.0i.
3. Select the User Interface Policies.
4. Select **Workstation** from the **Settings for** drop-down list at the top of the page.

The **Settings for** drop-down list allows you to set separate policies for servers and workstations without using **Directory** groups. ePolicy Orchestrator detects the operating system on the client computer and applies the right policy. However, for testing purposes, it can be useful to create server and workstation groups.

5. Deselect **Inherit** to enable user interface policy options.

6. Select **Show the system tray icon with minimal menu options**.

7. Click **Apply** to save the changes.

8. Repeat these steps for other **Workstations** groups in your **Directory**.

---

**STEP 6**

**Deploy VirusScan Enterprise to clients**

Now you have created master and distributed repositories, added the VirusScan Enterprise 8.0i PKGCATALOG.Z file to your master repository, and replicated this to a new distributed repository. Your computers are added to your **Directory** and they all have ePolicy Orchestrator agents installed on them. You’ve defined your VirusScan Enterprise policies for servers and workstations. You are now ready to have ePolicy Orchestrator deploy VirusScan Enterprise on all the clients in your test network.

Unlike deploying agents, which must be done at the site, group, or computer level, you can deploy VirusScan Enterprise from the **Directory** level to install it on all the computers in your **Directory** at once. Note that whatever policies you have set for specific sites or groups within your **Directory**, such as the **Servers** and **Workstations** groups in this example, still apply when VirusScan Enterprise is installed to clients within those groups. Alternatively, you can deploy VirusScan Enterprise to sites, groups, or individual computers—you can use the steps in this section to deploy at any level in your **Directory**.
To deploy VirusScan Enterprise 8.0i to all computers in your Directory:

1. In the console tree, select Directory.

2. In the details pane, select the Task tab and then double-click the Deployment task in the task list.

3. Once the ePolicy Orchestrator Scheduler opens, click the Task tab and deselect Inherit under Schedule Settings.

![Figure 10 ePolicy Orchestrator Scheduler dialog box](image)

4. Under Schedule Settings, select Enable (scheduled task runs at specified time).

5. Click the Settings button.

6. On the Deployment page, deselect Inherit to enable product deployment options.

7. Set the Action for the VirusScan Enterprise 8.0i deployment task to Install.

8. Click OK to save the product deployment options and return to the ePolicy Orchestrator Scheduler dialog box.

9. On the ePolicy Orchestrator Scheduler dialog box, click the Schedule tab.

10. Deselect Inherit to enable scheduling options.

11. From the Schedule Task drop-down list, select Run Immediately.

12. Click OK to save your changes.

In the task list on the Tasks tab of the details pane, the Enabled status for the deployment task is set to True.

You have now configured your default deployment task to install VirusScan Enterprise on all client computers in your test site. The deployment occurs the next time the agents call back to the ePolicy Orchestrator server for updated instructions. You can also initiate an agent wakeup call to have the deployment occur immediately. See Send an agent wakeup call to force agents to call back immediately on page 31.
Deploy VirusScan 4.5.1 to Windows 95, Windows 98, or Windows ME computers

If you have any Windows 95, 98, or ME computers in your test network, as this example does, you can repeat the steps in this section to deploy VirusScan 4.5.1 to these computers only. Make sure you have already checked the VirusScan 4.5.1 deployment package into the repository (see Check in the VirusScan 4.5.1 package if you have Windows 95, Windows 98, or Windows ME clients on page 22). Deploying VirusScan 4.5.1 to several computers is easiest if you have organized your Windows 95, Windows 98, or Windows ME computers into a group in your Directory, but you can also run the deployment task for individual computers too.

To deploy VirusScan 4.5.1:

1. In the console tree, select your group or computer in your Directory.
2. In the details pane, click the Tasks tab. Follow the steps in the previous section to configure the deployment as you would for VirusScan Enterprise 8.0i.
3. When you get to the Deployment settings page, set VirusScan 4.5.1 to Install.
   - You can also set VirusScan Enterprise 8.0i to Ignore, but this is not necessary. VirusScan Enterprise can detect that these computers are running an older version of Windows and will not install.
4. Complete the steps to configure the deployment. ePolicy Orchestrator deploys VirusScan 4.5.1 the next time the agents on these computers call back to the server.

Send an agent wakeup call to force agents to call back immediately

If you want, you can send the agents an immediate agent wakeup call. This forces the agents to check in immediately with the ePolicy Orchestrator server, rather than wait for the next regularly scheduled agent callback, which by default could be as long as 60 minutes. When the agents call back, they see that the VirusScan Enterprise deployment is set to install rather than ignore. The agents then pull the VirusScan Enterprise PkgCatalog.z file from the repository and install VirusScan Enterprise. Note that each agent pulls the PkgCatalog.z file from whichever repository it is configured to. In our example test network, the computers in the Domain1 site pull from the master repository and computers from Container1 pull from the distributed repository we created.

You can send an agent wakeup call to any site, group, or individual computer in your Directory. Since we want to wake up all computers in the Directory, we’ll initiate one wakeup call for each site, which inherit down to groups and computers within that site.

To send an agent wake-up call to begin VirusScan Enterprise deployment immediately:

1. Right-click the target site in the console tree and select Agent Wakeup Call.
2. Set the Agent randomization to 0 minutes.
3 Click OK to accept all other defaults and send the wakeup call.

4 Repeat these steps for other sites in your Directory.

The agents call back immediately, retrieve the new deployment policy changes, and begin installing VirusScan Enterprise. Wait a few minutes while VirusScan Enterprise 8.0i is deployed and installed.

You can check that it has successfully installed on clients in several ways. From the client computer, check that:

- The MCSHIELD.EXE process is running and visible in the Processes tab of your Windows Task Manager.
- A VirusScan folder is added to your Program Files/Network Associates folder.
- As long as you did not change the policy to hide it, the VShield icon appears in the system tray next to the agent icon. You may need to reboot to display the system tray icon. Note that VirusScan is active and running even if the VShield icon has not yet displayed in the system tray.

**STEP 7**

**Run a report to confirm your coverage**

Another way to confirm that your VirusScan Enterprise deployment was successful is to use one of the reports that comes with ePolicy Orchestrator. Run a Product Protection Summary report to confirm that your VirusScan Enterprise deployment was successful. Note that you may need to wait an hour before the database has been updated with the new status.

To run a Product Protection Summary report:

1 From the left-pane console tree, select Reporting | ePO Databases | ePO_ePOServer. ePOServer is the name of the ePolicy Orchestrator database used in this example.
If you are prompted to log in to the database, type your MSDE sa user name and password that you created when installing the console and database.

Select Reports | Anti-Virus | Coverage | Product Protection Summary.

Select No when prompted to set a data filter. Wait a moment while ePolicy Orchestrator generates the report.

Once the report has generated, the results should show the number of servers and workstations on which VirusScan 4.5.1 and VirusScan Enterprise 8.0i are currently installed. If you later deploy other products, such as McAfee Desktop Firewall, they show up in this report as well. In our example, you can see that VirusScan Enterprise 8.0i and VirusScan 4.5.1 have installed on all of the computers in our test network.

Update DAT files with a client update task

One of the most common things you will want to do with ePolicy Orchestrator is to update DAT virus definition files. VirusScan Enterprise by default performs an update task immediately after installing. So, if you followed the steps in this evaluation guide to configure your repositories and pulled the latest DAT files to your master repository before deploying, VirusScan Enterprise will be up-to-date shortly after being deployed.

Once VirusScan Enterprise is installed, however, update DAT files frequently. Your anti-virus software is only as good as its latest DAT files, so it is essential to keep them up-to-date. In a later section in this evaluation guide, you will see how to schedule a regular automatic client update task to occur regularly, such as daily or weekly. For now, let’s assume you want to initiate an immediate DAT file update. You will likely be required to do this at some point; for example, if McAfee releases updated DAT files in response to a newly-discovered virus and you want your clients to update without waiting for their regularly scheduled task.

To do this, create and run a client update task from your ePolicy Orchestrator console. This forces all your client anti-virus software to perform an update task.

Before you run a client update task, make sure you have first pulled any updated DAT or engine files into your master and distributed repositories, if you have them. See Set up master and distributed repositories on page 20.

To create and run a client update task:

1. In the console tree, right-click the Directory and select Schedule task.
2. In the Schedule Task dialog box, type a name into the New Task Name field, such as Update client DATs.
3. In the software list, select ePolicy Orchestrator Agent | Update for the task type.
4. Click OK.
5. Press F5 to refresh the console and make the new task appear in the list in the Task tab.
Note that it is scheduled to run daily at the current day and time. Also note that the Enabled flag is set to False—we now need to set this to True and run it immediately.

6 Right-click the new task in the task list and select Edit Task.

7 Deselect Inherit under the Schedule Settings section of the ePolicy Orchestrator Scheduler dialog box.

8 Select Enable.

9 Click Settings, then deselect Inherit on the Update tab.

10 Ensure that This task updates only the following components is selected. This selection allows you to specify which components you want to update. Specifying these allows you to save network resources by limiting which updates are distributed in your environment.

11 Leave the default selections under Signatures and Engines.

12 Under Patches and Service Packs, select VirusScan Enterprise 8.0, then click OK.

13 Click the Schedule tab and deselect Inherit.

14 Set the Schedule Task option to Run Immediately and click OK.

15 Initiate agent wakeup calls to all sites in your Directory so your agents call in immediately to pick up the agent update task. See Send an agent wakeup call to force agents to call back immediately on page 31.

How can I tell that VirusScan Enterprise has actually updated to the latest DATs?
First, check the DAT version that is currently checked into your master repository. These are the DATs that should now be on your client computers after they updated. To do this:

1 From the console tree, select Repository | Software Repositories | Master. The details pane displays the list of packages currently checked in to the master repository.

2 Scroll to the bottom of the Packages list and locate the Current DAT version, which will be a 4-digit number like 4306.
Next, check the DAT versions used by client software, such as VirusScan Enterprise, from the ePolicy Orchestrator console. Note that the console does not show the updated status until the next time the agent calls into the server as part of its regular agent-to-server communication. To do this:

1. In the ePolicy Orchestrator console, select any computer in your Directory that has recently been updated.
2. In the details pane, select the Properties tab.
3. In the Properties page, select VirusScan Enterprise 8.0i | General to expand the list of general properties.
4. Check the DAT Version number. It should match the latest DAT version in your master software repository.

**Schedule automatic repository synchronization**

Well, you’ve certainly come a long way! In just a few hours, you now have a fully-functional installation of ePolicy Orchestrator deployed in your test network. You have agents deployed to client computers, and these agents are active and calling back to the server for updated instructions regularly. You’ve also used ePolicy Orchestrator to deploy VirusScan Enterprise to your client computers, and have created a small software repository that you can use to push updates and additional software to your client computers.

The next step is to schedule regular pull and replication tasks to synchronize your source, master, and distributed repositories so that all your repositories are up-to-date. Then create a scheduled client update tasks to make sure client software such as VirusScan Enterprise checks regularly for updated DAT and engine files.

To do this:

1. **Schedule a pull task to update master repository daily.**
2. **Schedule a replication task to update your distributed repository.**
3. **Schedule a client update task to update DATs daily.**

1. **Schedule a pull task to update master repository daily**

   Pull tasks update your master software repository with the latest DAT and engine updates from the source repository. By default, your source repository is the McAfee web site. Let’s create a scheduled pull task to pull the latest updates from the McAfee web site once per day.

   To schedule a pull task:

   1. In the console tree, select Repository.
   2. In the Repository page, select Schedule pull tasks to open the Configure Server Tasks page.
   3. Select Create task to open the Configure New Task page.
4 Type a name into the Name field, such as Daily Repository Pull task.

5 Select Repository Pull from the Task type drop-down menu.

6 Make sure Enable task is set to Yes.

7 Select Daily from the Schedule Type drop-down list.

8 Expand the Advanced schedule options and schedule the day and time for the task to run.

9 Click Next at the top of the page.

10 Select NAIHttp in the Source repository drop-down list.

11 Leave the destination branch set to Current.

12 If you have older versions of McAfee products, such as VirusScan 4.5.1, in your test network, select Support Legacy product update.

13 Click Finish. Wait a moment while the task is created.

The new pull task is added to the Configure Server Tasks page.

2 **Schedule a replication task to update your distributed repository**

Using your new pull task, your ePolicy Orchestrator server is configured to automatically update the master repository with the latest updates from the source repository on the McAfee web site. The task runs once a day and keeps your master repository current.
But an up-to-date master repository won’t be of any use to those client computers on your network that get their updates from a distributed repository, such as the computers in the Container1 site in our sample test network. The next step, therefore, is to make sure the updates added to your master repository are also automatically replicated out to your distributed repository. To do this, create an automatic replication task and schedule it to occur every day one hour after the scheduled pull task you already created.

To schedule an automatic replication task:

1. In the console tree, select Repository.
2. In the Repository page, select Schedule pull tasks to open the Configure Server Tasks page.
3. Select Create task to open the Configure New Task page. This is the same page that you used to schedule your automatic pull task.
4. Type a name into the Name field, such as Daily Distributed Repository Replication task.
5. Select Repository Replication from the Task type drop-down menu.
6. Make sure Enable task is set to Yes.
7. Select Daily from the Schedule Type drop-down list.
8. Expand the Advanced schedule options and schedule the day and time for the task to run. Set the time for an hour after your scheduled pull task begins. This should give the pull task enough time to complete. Depending on your network and Internet connections, your pull task may require more or less time, so set your replication task start time accordingly.
9. Click Next at the top of the page.
10. Select Incremental replication and click Finish. Wait a moment while the task is created.

The new replication task appears in the Configure Server Tasks table along with your scheduled pull task.

3 Schedule a client update task to update DATs daily

After all your repositories have been updated, schedule a client update task to make sure that VirusScan Enterprise gets the latest DAT and engine updates as soon as they are in your repositories.

You can use the client update task you created earlier after you deployed VirusScan Enterprise (see Update DAT files with a client update task on page 33). Simply modify the schedule of this task from Run Immediately to Daily and set the start time to run about an hour after your replication task begins.
**STEP 10**

**Test global updating with SuperAgents**

Global updating is a new feature in ePolicy Orchestrator 3.5 that can automatically update all your client computers every time you check new updates into your master repository. Every time you change your master repository, ePolicy Orchestrator automatically replicates the contents to any distributed repositories you have. Then it alerts all agents deployed in your network that have managed products, such as VirusScan Enterprise 8.0i, to perform an immediate update task.

The global updating feature can be very useful in a virus outbreak situation. Assume that McAfee’s AVERT team has posted updated DATs in response to a newly-discovered virus in the wild. With global updating enabled, you simply initiate a pull task from your ePolicy Orchestrator console to update your master software repository with the new DAT files. ePolicy Orchestrator’s global updating feature does the rest—updating the DATs for all computers running active, communicating agents on your network within one hour.

**Use SuperAgents to wake up all agents on network**

ePolicy Orchestrator uses something called a SuperAgent to initiate the global update. SuperAgents are ePolicy Orchestrator agents that can also wake up other agents located in the same network subnet. When you have a SuperAgent installed in each network subnet, you send a SuperAgent wakeup call to your SuperAgents, and then the SuperAgents send wakeup calls to the ePolicy Orchestrator agents in the same subnet. The regular agents can then call back to the ePolicy Orchestrator server for policy instructions and update client software.

SuperAgents can also act as distributed repositories. These SuperAgent repositories use a proprietary McAfee replication protocol called SPIPE, and can either replace or augment other HTTP, FTP, or UNC distributed repositories you have created. This evaluation guide does not cover SuperAgent repositories, however. Refer to the *ePolicy Orchestrator 3.5 Product Guide* for information on SuperAgent repositories.

To enable global updating:

1. **Deploy a SuperAgent to each subnet.**
2. **Enable global updating on ePolicy Orchestrator server.**

### 1 Deploy a SuperAgent to each subnet

You can deploy a SuperAgent to any computer in your ePolicy Orchestrator **Directory**. You can also turn any regular ePolicy Orchestrator agent into a SuperAgent. Use the ePolicy Orchestrator Agent policy pages in the ePolicy Orchestrator console to do this. Since you only need one SuperAgent per network subnet, be sure to configure SuperAgents for individual computers in your **Directory**, and not for whole groups or sites as you did when deploying regular agents or VirusScan Enterprise.

For example, in the sample test network used in this guide, we would deploy one SuperAgent to the Domain1 site.

You can deploy a SuperAgent to a computer that currently has no agent, or you can convert existing regular agents to SuperAgents. In our example, we can do this by changing the policies for an agent for one computer. To do this:

1. **Select a specific computer in the Directory.**
2 In the **Policies** tab, click **ePolicy Orchestrator Agent | Configuration** to display the agent policy page.

3 On the **General** tab, deselect **Inherit**.

4 Select **Enable SuperAgent functionality**.

You can also create a SuperAgent repository on the computer, but they are not required for global updating and are not covered in this guide. See the *ePolicy Orchestrator 3.5 Product Guide* for information on SuperAgent repositories.

5 Click **Apply All** to save the policy changes.

6 Right-click the computer in the **Directory** and select **Agent Wakeup Call**.

7 Set **Agent Randomization** to 0 and click **OK**.

8 Repeat these steps if you have computers in other network subnets.

Wait a few moments while the SuperAgent is created. Once enabled, the system tray icon on the computer hosting the SuperAgent looks slightly different.

You can use these SuperAgents to wake up other agents in the local subnet. This can save bandwidth, especially in a large network with many remote, WAN-connected sites. Send out wakeup calls to a few SuperAgents and let them wake up the other agents in the local LAN. SuperAgents are also critical for the new global updating feature.

### 2 Enable global updating on ePolicy Orchestrator server

Global updating is a feature that you can turn on or off from the ePolicy Orchestrator console. When turned on, any change to your master repository triggers an automatic replication to distributed repositories, if any, followed by a SuperAgent wakeup call to your entire **Directory**. The SuperAgents in turn wake up agents in their local subnets.

To turn on global updating:

1 In the console tree, select your ePolicy Orchestrator server.

2 In the details pane, select the **Settings** tab.
3 At the bottom of the Server Settings page, set Enable global updating to Yes.

4 For the purposes of this evaluation change the Global updating randomization interval to 1 minute.

5 Leave the default selections under Signatures and Engines.

6 Under Patches and Service Packs, select VirusScan Enterprise 8.0.

7 Click Apply Settings to save the change.

Now that you have SuperAgents deployed to subnets your network and global updating enabled, any time you change your master repository, the changes automatically replicate to your repositories. Once that replication is completed, the ePolicy Orchestrator server sends a SuperAgent wakeup call to the SuperAgents. The SuperAgents in turn send out a wakeup call to all agents in the local subnet. Those agents check in with the server and download policy changes. From checking in the changes to your master repository to your last client computer receiving its update, this process should take no longer than one hour.

STEP
11

Where to go from here?

By now you have had a chance to explore most of the major features of ePolicy Orchestrator 3.5.0. But there is also much more you can do with ePolicy Orchestrator and VirusScan Enterprise. Please refer to the ePolicy Orchestrator 3.5 Product Guide, the VirusScan Enterprise 8.0i Product Guide, and the VirusScan Enterprise 8.0i Configuration Guide for ePolicy Orchestrator 3.5 for complete information on advanced product features. These and other helpful resources are available for download from the McAfee web site.
This section of the Evaluation Guide demonstrates how you can configure and use two of the new features not covered in the previous section:

- **ePolicy Orchestrator Notification**.
- **Rogue System Detection** on page 46.

### ePolicy Orchestrator Notification

Real-time information about threat and compliance activity on your network is essential to your success.

You can configure rules in ePolicy Orchestrator to notify you when user-specified threat and compliance events are received and processed by the ePolicy Orchestrator server. The ability to set aggregation and throttling controls on a per rule basis allows you to define when, and when not, notification messages are sent.

Although you can create any number of rules to notify you of almost any threat or compliance event sent by your security programs, the focus in this guide on this feature is more narrow, centering on an e-mail notification message in response to a virus detected event.

In this section of the guide, you will:

1. **Configure agent policy to upload events immediately.**
2. **Configure Notifications.**
3. **Creating a rule for any VirusScan Enterprise event.**
4. **Providing a sample virus detection.**

#### S T E P 1

**Configure agent policy to upload events immediately**

Because the agent delivers the events to the ePolicy Orchestrator server from the managed systems, you need to configure the agent policy to deliver events immediately. Otherwise, the ePolicy Orchestrator server doesn’t receive events until the agent-to-server communication interval (ASCI).
1 Click **Directory** in the console tree, then the **Policy** tab in the upper details pane.

2 Select **ePolicy Orchestrator Agent | Configuration** in the upper details pane.

3 Select the **Events** tab in the lower details pane, then deselect **Inherit**.

4 Select **Enable immediate uploading of events**, then click **Apply All**.

Now that you’ve configured the agents to upload events to the ePolicy Orchestrator server immediately, you are ready to configure ePolicy Orchestrator Notifications.

**STEP 2**

**Configure Notifications**

Before setting up any rules, you must define who is going to receive the notification message, in which format, and what the message communicates:

1 Click **Notifications** in the console tree, then select the **Configuration | Basic Configuration** tab in the details pane.
2 Under **E-mail Server**, type the name of a mail server to which the ePolicy Orchestrator server can route, and the desired e-mail address that you want to appear in the **From** line of the message.

When you decide which e-mail address to place here you should consider the number of administrators who may receive notification messages, and whether you want these administrators to be able to send reply messages.

3 Click **Apply**, then click **E-mail Contacts** at the top of the tab. This page allows you to specify all of the addresses to include in the address book from which you will select recipients during rule creation.

There should be one contact in the list already, **Administrator**. The e-mail address provided for **Administrator** is the e-mail address you entered in the **Set E-mail Address** panel of the installation wizard. If you did not change the default address in the wizard, the address is **Administrator@example.com**. If the address for **Administrator** is one that you are not able to view the mail sent to it, then click the address and change it to one at which you can receive and view e-mail messages.

From the **Configuration** tab you can also define SNMP servers at which you’d like to receive SNMP traps and external commands that you want to run when certain events are received. These tasks are beyond the scope of this evaluation guide. For more information, see the **ePolicy Orchestrator 3.5 Product Guide**.

Now that you’ve specified an e-mail server to be used to send the message, and an address to receive the message, you are ready to create a rule to trigger on a VirusScan Enterprise event.
STEP 3

Creating a rule for any VirusScan Enterprise event

You can create a variety of rules to handle nearly any category of events that are received from your managed security products. For more information, see Chapter 9: ePolicy Orchestrator Notifications in the ePolicy Orchestrator 3.5 Product Guide.

1 Click the Rules tab, then click Add Rule to begin the Add or Edit Notification Rule wizard.

2 On the Describe Rule page, leave the default (Directory) for the Defined At text box. You can define rules for the Directory or any site within the Directory.

3 Provide a name for the rule in the Rule Name text box. For example, Virus Detected.

4 Provide a description of the rule in the Description text box. For example, Viruses detected by VirusScan Enterprise, then click Next.

5 On the Set Filters page:
   a Leave all Operating systems checkboxes selected.
   b Under Products, select VirusScan.
   c Under Categories, select Any category above the list, then click Next.

   So far the configurations you’ve made specify the rule to apply to any VirusScan event occurring on any managed system within the Directory.

   Figure 3-3 Set Filters page

6 Although for this task you will leave the defaults on this page selected, the Set Thresholds page allows you to limit the number of notification messages you receive for the rule. For example, you can define any rule to send you messages only when the number of events or the number of affected computers have reached a specified number within a specified time frame (Aggregation). You can further limit the number of messages that are sent by specifying an amount of time to take place before receiving another message (Throttling). Throttling is almost always recommended by McAfee to prevent a flood of messages during an outbreak situation.
Leave **Send a notification for every event** selected, and click **Next**.

7 On the **Create Notifications** page, click **Add E-mail Message**.

8 Click **Administrator** in the box on the left of the page, then click **To** so that **Administrator** moves to the **Notification Recipient(s)** box.

   This specifies that the e-mail address you configured in Step 2: **Configure Notifications on page 42** (for the **Administrator** contact) will be sent the notification message you are about to configure.

9 Type a **Subject** for the e-mail that will be sent to **Administrator** when this rule is triggered. For example, **Threat detected by VirusScan**.

10 Type a **Body** for the e-mail message that will be sent when this rule is triggered. For example, **VirusScan detected a threat**.

11 By inserting multiple variables into the body of the message, you can have meaningful information from the event files inserted into your notification message.

   For the purpose of this section of the guide, select **Affected computer names** and click **Body**. This will place the name of the affected computer, if available from the event file, in the body of the e-mail message. Click **Save**.

   You can create multiple messages in multiple formats to send to multiple recipients, as well as choosing external commands to run, from the **Create Notifications** page. These are beyond the scope of this document. See the **ePolicy Orchestrator 3.5 Product Guide** for more information.

12 Click **Next** and verify the configurations you made to the rule you created on the **View Summary** page, then click **Finish**.
**STEP 4**

**Providing a sample virus detection**

Now that you have configured the feature and created a rule to trigger on event files from VirusScan Enterprise, you are ready to provide an event file that triggers the rule.

1. Download EICAR.COM to one of the workstation test computers. Each time you download this file, you are creating a sample detection. At press time, this file was available on the EICAR.ORG web site:

   http://www.eicar.org/anti_virus_test_file.htm

   ![This file is not a virus.]

2. The on-access scanner detects and quarantines the EICAR test virus at the same time that EICAR.COM is downloaded, and an event file capturing this information is sent to the ePolicy Orchestrator server.

3. Within minutes a notification message is created and sent to the inbox of the e-mail message recipient you provided earlier.

Congratulations! You successfully configured the product to send messages to a specific individual, created a rule to send a notification message based on events from VirusScan Enterprise, and tested the rule to ensure that it works.

---

**Rogue System Detection**

In any managed network, at any given time, there are inevitably a small number of systems that do not have an ePolicy Orchestrator agent on them. These can be computers that frequently log on and off the network, such as test servers, laptop computers, or wireless devices. End users also uninstall or disable agents on their workstations. These unprotected systems are the Achilles heel of any anti-virus and security strategy and are the entry points by which viruses and other potentially harmful programs can gain access to your network.

The Rogue System Detection system helps you monitor all the systems on your network—not only the ones ePolicy Orchestrator manages already, but the rogue systems as well. A rogue system is any computer that is not currently managed by an ePolicy Orchestrator agent but should be. Rogue System Detection integrates with your ePolicy Orchestrator server to provide real-time detection of rogue systems by means of a sensor placed on each network broadcast segment. The sensor listens to network broadcast messages and spots when a new computer has connected to the network.

When the sensor detects a new system on the network, it sends a message to the Rogue System Detection server. The Rogue System Detection server then checks with the ePolicy Orchestrator server to determine whether the newly-identified computer has an active agent installed and is managed by ePolicy Orchestrator. If the new computer is unknown to ePolicy Orchestrator, Rogue System Detection allows you to take any number of remediation steps, including alerting network and anti-virus administrators or automatically pushing an ePolicy Orchestrator agent to the computer.
In this section of the *Evaluation Guide*, you will:

2. Deploy the Rogue System Detection sensor.
3. Configure an automatic response.
4. Rogue detection and remediation.

**STEP 1**

**Configure Rogue System Detection sensor policy**

Before deploying the Rogue System Detection sensor, you should first configure the sensor policy.

These specific configurations to the sensor policy are only for the purpose of the evaluation. These are not recommended configurations for a production environment deployment of the sensor.

Once the sensor is deployed to a system in your environment, it requires one agent-to-server communication and one policy enforcement interval before it is functioning in the environment. The agent-to-server communication installs the sensor on the system in a disabled state. Then the policy enforcement retrieves policy, including security certificates. These certificates are needed by the sensor to communicate to the server directly.

The following configuration changes to the sensor policy speed up this process for this purpose of this guide.

1. Click **Directory** in the console tree, then select **Rogue System Sensor | Configuration** on the **Policy** tab of the details pane.

   ![Figure 3-5 Rogue System Sensor | Configuration](image-url)
2 Deselect Inherit, then under Communication Intervals make the following changes:
   a  Set Minimum reporting interval for each detected host to 120 seconds.
   b  Set Minimum sensor-to-server communication interval for primary sensors to 5 seconds.
3 Click Apply All.

**STEP 2**

**Deploy the Rogue System Detection sensor**

The sensor is the distributed portion of the Rogue System Detection architecture. Sensors detect the computers, routers, printers, and other network devices connected to your network. The sensor gathers information about the devices it detects, and forwards the information on to the Rogue System Detection server.

The sensor is a small Win32 native executable application. Similar to an ePolicy Orchestrator SuperAgent, you must deploy at least one sensor to each broadcast segment, usually the same as a network subnet, in your network. The sensor runs on any NT-based Windows operating system, such as Windows 2000, Windows XP, or Windows 2003.

For more information about the sensor and how it functions, see *Chapter 11: Rogue System Detection* in the *ePolicy Orchestrator 3.5 Product Guide*.

Depending on how you have your test environment set up, you may have more than one subnet represented in it. But you do have at least one.

To deploy the sensor:

1 Click Rogue System Detection in the console tree, then select the Subnets tab in the details pane to display the Subnet List.
2 Select the subnets to which you want to deploy sensors by clicking once in the checkbox for that subnet, then clicking Deploy Sensors.
3 When the Sensor Deployment: Set Preferences page appears, ensure Let me select machines manually is selected.

4 Although we are not setting criteria for ePolicy Orchestrator to use to deploy sensors automatically, the availability of this criteria allows you to save time when trying to decide on which systems to install the sensors. This way, ePolicy Orchestrator finds the best systems on each subnet to install the sensors.

5 Click Next, then select the checkbox next to the desired system to which you want to deploy a sensor, click Mark for Deployment, then Close.

6 When the Sensor Deployment: Review and Approve page appears, click Deploy Now.

The Action Progress page of the Events tab displays, indicating the progress of each sensor deployment.

7 Remember that you must wait until after one agent-to-server communication and one policy enforcement interval before the sensor calls into the server and is functioning. This can be expedited by sending agent wakeup calls.

a Right-click the computer on which you installed the sensor in the Directory of the console tree, then select Agent Wakeup Call.

b Set Agent randomization to 0, then click OK.

c Wait two minutes, then repeat.

8 Once the Action Status is Completed Successfully, the sensor has called back to the server and is functioning.

9 Select the Machines tab and select Summary to view a summary of detected systems.

Now that the sensor is deployed and installed you are ready to configure a response for the feature to take on a rogue when one is detected.

![Figure 3-6 Subnet List page](image-url)
Configure an automatic response

You can configure automatic responses for ePolicy Orchestrator to execute on rogue systems that are detected. There is a considerable amount of flexibility within this feature regarding the level of granularity available when defining the actions to take, and the conditions you can add to them. For complete information, see Chapter 11: Rogue System Detection in the ePolicy Orchestrator 3.5 Product Guide.

There are many situations where you may not want an automatic response to be taken. You can also set conditions around types of rogues where no actions are taken, or where the detected systems are simply marked for action.

For the purposes of this guide, you will configure a response that pushes an agent onto the rogue system once it has been discovered.

1. Select Rogue System Detection in the console tree, then select the Responses tab in the details pane.

2. Select the checkbox next to the default Query ePO Agent response, select Disable from the Checked responses drop-down list, then click Apply.

   This response checks the detected system for an agent of another ePolicy Orchestrator server.

3. Click Add Automatic Response to display the Add or Edit Automatic Response page.

4. Type a name for the response. For example, Push Agent.

5. Under Conditions, click Add Condition, then select Rogue Type from the Property list.
Select is for the **Comparison**, and **No Agent** for the **Value**.

Under **Actions**, change the default **Send E-mail** action to **Push ePO Agent** as the **Method**, and accept the default **Parameters**.

Click **OK**.

Select the checkbox next to the **Push Agent** automatic response when the **Automatic Responses** page reappears. Select **Enable** from the **Checked responses** drop-down list, then click **Apply**.

Now that the sensor is deployed, and a response has been created and enabled to handle rogues with no agent, you are ready to introduce such a rogue.

---

**STEP 4**

**Rogue detection and remediation**

Now you need to introduce a system into the test environment that does not have an agent. You can do this by several methods, such as joining a laptop to the test network, or by moving a computer from an outside domain to the test domain you created earlier.

1. Add a computer that does not have an ePolicy Orchestrator agent to the test network.

2. Go to the **Machine** tab, then click **List**. Once the sensor has detected a rogue system, it reports back to the server and places the system in the **Machine List**.

3. Once it appears in this list, take a five minute break to provide time for the agent installation.

4. Once the agent installation completes, the system has a **Rogue Type** of **Managed**.

You are not finished yet. You still must place the now managed system into its appropriate home in the **Directory**.
5 Once the system’s **Rogue Type** changes to **Managed**, it is placed in **Directory | Lost&Found | Rogue Systems** of the console tree.

The **Lost&Found** directory is a holding place for systems ePolicy Orchestrator has discovered, but doesn’t know where to place within the **Directory**.

6 Click and drag the system to the desired site or group in your ePolicy Orchestrator **Directory**.

Congratulations! You successfully configured the sensor, deployed the sensor, configured an automatic response which you saw taken on the rogue you introduced, and placed the newly managed system into its appropriate spot in the **Directory**.