Trend Micro® Endpoint Security Platform Console

Administrator's Guide

Version 8.0

August 2010

Trend Micro Endpoint Security Platform Suite

Document Part No.: APEM84654/100908

Release Date: September 2010

Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Please evaluate this documentation on the following site:
http://www.trendmicro.com/download/documentation/rating.asp

IMPORTANT NOTICE AND LIMITATION

Your use of the Trend Micro Endpoint Security Platform is limited to supporting the Trend Micro Core Protection Module and other BigFix Products purchased from Trend Micro only as expressly described in and permitted by this user guide.

You are only authorized and licensed to use the software distribution capabilities of the Trend Micro Endpoint Security Platform to distribute the Trend Micro Core Protection Module and other BigFix Products purchased from Trend Micro, but you are not authorized or licensed to use the Trend Micro Endpoint Security Platform to distribute any other Trend Micro, BigFix, or any third party software

You are authorized and licensed to use the Trend Micro Endpoint Security Platform only to customize the Fixlets that are provided with the Trend Micro Core Protection Module and other BigFix Products purchased from Trend Micro, but you are not authorized to create completely new Fixlets unrelated to such software purchased from Trend Micro.

However, you may at any time purchase an upgrade from Trend Micro which permits you to use the full and complete software distribution capabilities of the Trend Micro Endpoint Security Platform with any software application (any Trend Micro, BigFix, or third party software) and to create new Fixlets that are unrelated to the software purchased from Trend Micro.

Contents

CONTENTS

Part One

Introduction

The **Trend Micro® Endpoint Security Platform (ESP)** aims to solve the increasingly complex problem of keeping your critical systems updated, compatible, and free of security leaks. It uses patented Fixlet® technology to identify vulnerable computers in your enterprise. Then, with just a few mouse-clicks you can remediate them across your entire network from a central Console. Fixlet messages are flexible and customizable. Utilizing Fixlet technology, you can:

- Analyze vulnerabilities (patched or insecure configurations)
- Easily and automatically remediate all your networked endpoints
- Establish and enforce configuration policies across your entire network
- Distribute and update software packages
- View, modify and audit properties of your networked client computers

Fixlet technology allows you to analyze the status of configurations, vulnerabilities, and inventories across your entire enterprise and then enforce policies automatically in near real-time. In addition, administrators can create or customize their own Fixlet solutions and Tasks to suit their specific network needs.

ESP is easy to install and has built-in public/private-key encryption technology to ensure the authenticity of Fixlet messages and actions. ESP is designed to grant maximum power to you as the administrator, with a minimal impact on network traffic and computer resources. ESP is capable of handling hundreds of thousands of computers in networks spanning the globe.

Once ESP is installed, you will find it easy to keep your networked computers properly configured, updated, and patched, all from a central ESP Console. You can track the progress of each computer as updates or configuration policies are applied, making it easy to gauge the level of compliance across your entire enterprise. In addition to downloads and security patches, you can also examine your managed computers by specific attributes, allowing you to group them for action deployments, ongoing policies or asset management. You can log the results to keep an audit trail and chart your overall activity with a convenient web-based reporting program.

Audience

This guide is meant for Administrators and IT managers who want to install and administer the Endpoint Security Platform. It details the system requirements for each of the components and provides licensing and installation instructions that will enable you to deploy ESP in your environment. It also includes information on configuring and maintaining ESP. Please refer to the ***ESP Console Operator's Guide*** for operating instructions and further information about the performance of the various suite components, including ESP Servers, Relays and Agents.

Versions

The document includes the functionality introduced in ESP Version 8.0.

Overview of the ESP System

The ESP system has the following main components:

- **ESP Agents**, also called Agents, are installed on every computer you wish to manage under ESP. They access a collection of Fixlet messages that detects security holes, improper configurations and other vulnerabilities. The ESP Agent is then capable of implementing corrective actions received from the ESP Console through the ESP Server. The ESP Agent is designed to run undetected by end users using a minimum of system resources. However, ESP also allows the administrator to provide screen prompts for those actions that require user input. ESP Agents are capable of encrypting their upstream communications, protecting sensitive information. ESP Agent software can run under Windows, Linux, Solaris, HPUX, AIX and Macintosh operating systems.
- **ESP Servers** offer a collection of interacting services, including application services, a web server and a database server, forming the heart of the ESP system. It coordinates the flow of information to and from individual computers and stores the results in the ESP database. The ESP Server components operate quietly in the background, without any direct intervention from the administrator. ESP Servers also include a built-in **Web Reporting** module to allow authorized users to connect via a web browser to view all the information about computers, vulnerabilities, actions, and more. ESP supports multiple servers, adding a robust redundancy to the system.
- **ESP Relays** increase the efficiency of the system. Instead of forcing each networked computer to directly access the ESP Server, relays spread the load. Hundreds to thousands of ESP Agents can point to a single ESP Relay for downloads, which in turn makes only a single request of the server. ESP Relays can connect to other relays as well, further increasing efficiency. An ESP Relay does not need to be a dedicated computer – the software can be installed on any Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Red Hat Enterprise Linux 4/5/6, or Solaris 10, computer with the ESP Agent installed. As soon as you install an ESP Relay, the ESP Agents on your network have the ability to automatically discover and connect to them.
- **ESP Consoles** tie all these components together to provide a system-wide view of all the computers on your network, along with their vulnerabilities and suggested remedies. The ESP Console allows an authorized user to quickly and simply distribute fixes to each computer that needs them without impacting any other networked computers. The ESP Console can be run on any Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2 computer that has network access to the ESP Server. ESP Consoles for large deployments are often hosted from Terminal Servers or Citrix Servers.

Using this Guide

The process of getting ESP up and running varies, depending on your network environment and your security policies. This guide focuses on a standard ESP deployment, which applies to workgroups and to enterprises within a single administrative domain. For the sake of readability and generality, this guide assumes these restrictions:

- The ESP Servers are able to make connections to the Internet on port 80. The ESP Server can be set up to use a proxy, which is a common configuration. Alternatively, an air-gap can be used to physically separate the ESP Server from the Internet Fixlet Server (for more information, see the article on air-gaps at the ESP support site).
- Each ESP Server must have access to the SQL server, located locally on the ESP Server machine or remotely on a separate SQL Server.
- Each ESP Console operator can make an ODBC connection to the database and an HTTP connection to the ESP Server.
- Each ESP Agent computer in the network must be able to make an HTTP connection to an ESP Server or an ESP Relay on the specified port (the default port is 52311 but any available port will serve).

Some enterprises will violate one or more of these conditions, but ESP can still be deployed in these environments – the section titled **Deployment Scenarios** (page 98) shows you how. If your network configuration does not match any of the scenarios in that chapter, talk to a Trend Micro support technician for more options.

The initial deployment of a minimal ESP system (ESP Server, ESP Console, and a few ESP Agents) should take roughly an hour to complete.

When you are ready to install the full system, you will want to pay extra attention to the sections in this document on ESP Agent and ESP Relay deployment, to ensure an efficient rollout.

Several steps in the ESP installation depend on the completion of prior steps. For this reason, it is recommended that you follow this guide in the order presented.

ESP Operating Requirements

ESP has been designed to run efficiently using minimal server, network and agent resources. The requirements for the ESP Agent programs are not stringent. The hardware required by the ESP Server and the ESP Console will depend on the number of computers that are administered and the total number of ESP Consoles. The distributed architecture of ESP allows a single ESP Server to support hundreds of thousands of computers.

ESP Server Requirements

The ESP Server is supported on Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2. The supported versions of SQL Server are SQL Server 2005, SQL Server 2008, and SQL Server 2008 R2.

SQL 2005 Express Edition is not recommended for use in production deployments of ESP. For more information, see the knowledge-base article on MSDE at the Trend Micro support site.

A 2-3 GHz CPU with 1 GB RAM is sufficient for a few hundred ESP Agents, but the requirements scale with the number of computers. To support 200,000 computers, you would likely need 8 cores and 16 GB RAM.

A minimum of 5 GB free disk space is needed by the database, data files, and the file caches to run ESP. However, an additional 20-50 GB of disk space can be useful for database backups and further growth. To support more than a couple hundred ESP Agents, you will need RAID Arrays. For 200,000 computers, you will need about 3 Arrays (RAID 10). For optimal performance, the disk cache should be set to 50/50 read/write.

The exact hardware requirements for the ESP Servers will vary depending on how many ESP Agents are attached. The latest references on ESP Servers can be found at the Trend Micro support site. Consult with your support technician for more information about the ESP Server requirements.

The following network configuration is recommended for security and performance reasons:

- All internal network communication will be on one specified port (52311 is the default) to allow for simplicity and flexibility of deployment. TCP/IP and UDP on this port must be completely unblocked at all internal routers and internal firewalls (you can optionally disable UDP but that may negatively affect performance).
- The ESP Server should connect to the network at 100 mbps or higher.
- The ESP Consoles must be able to make connection to the SQL Server database using ODBC. ESP Consoles should have high speed connections to the ESP Server (100 mbps or higher)
- The Windows Firewall must be turned off on the ESP Server machine.
- The ESP Agent must be installed on the ESP Server machine.

These networking recommendations are typically easy to satisfy for most organizations maintaining a moderate security posture. If these requirements cannot be met in your organization, see **Configuring the ESP Components** (page 60). For information on larger installations, see **Deployment Scenarios** (page 98).

The ESP Server requirements and performance may also be affected by other factors in addition to the number of ESP Agents. These include:

- **The number of ESP Console Operators.** Multiple ESP Console operators can connect to the ESP Server(s) at the same time to manage subsets of the networked computers – some deployments may have hundreds of operators. If you plan on having more than 30 operators, you may want to have a more powerful ESP Server to support the additional load.
- **ESP Relays.** ESP Relays should be used to lighten the load on the ESP Server(s) by accepting connections from ESP Agents and then forwarding the data to an ESP Server. In most deployments, very few ESP Agents report directly to the main ESP Server.
- **The number and type of Retrieved Properties and Analyses.** Custom Retrieved Properties and Analyses can provide extremely useful data. But if custom properties are poorly implemented or overused, they can also create undue load on the system by requiring too much bandwidth or too many ESP Agent resources. For instance, it would be unwise to create a custom retrieved property that returned the names of every file on every computer, due to the load on the client computers and the network.

For more information about these performance issues, please consult the Trend Micro support site.

ESP Console Requirements

To install the ESP Console, you must have a computer that meets the following minimum requirements:

- **Hardware:** Intel Pentium III–class processor with 512 MB RAM. Larger deployments will require more capable computers.
- **Software:** Windows XP, 2003 Vista, 2008, 7, or 2008 R2 with Internet Explorer version 7.0 or better.

The ESP Console can be installed on a laptop or any moderately powerful computer. However, as the number of computers that you are managing with the ESP Console grows, you may need a more powerful computer. The latest ESP Console recommendations can be found at the Trend Micro support site.
The ESP Console also requires a high bandwidth connection (LAN speeds work best) to the ESP Server due to the amount of data that needs to be transferred to the ESP Console. If you need to remotely connect to the ESP Server across a slow bandwidth connection, it is recommended that you use a remote control connection to a computer (such as a Citrix server or Terminal Services computer) with a high-speed connection to the ESP Server. Contact your support technician for more information about ESP Console scaling requirements.

Note: The ESP Console is the primary interface to ESP and manages a great deal of information about the ESP Agents. If the ESP Console computers are underpowered or on a slow connection, it can adversely impact performance.

ESP Agent Requirements

The ESP Agent can run on computers that meet the following minimum requirements:

- **Hardware:** x86-based computers, Mac or SPARC with 32 MB RAM and 20 MB free hard disk space. Extra temporary disk space may be required for some patches.
- **Software:** Windows 2000, Server 2003, XP, Vista, 2008, 7, 2008 R2 Red Hat Linux 8.0, & 9.0, Red Hat Linux Enterprise 3/4/5/6, Red Hat Fedora Core 3.0, 4.0 & 5.0, Solaris 8, 9 & 10, HPUX 11.00 & 11.11, AIX 5.1, 5.2 & 5.3, SUSE 8, 9 & 10, Mac OS X 10.3 & 10.4.

New versions of the ESP Agent are always in development so please check with your support technician for more details. For Windows platforms, IE 5 or greater must be installed.
You can find the latest ESP Agent at the Trend Micro support site.

Database Requirements

ESP requires SQL Server 2005, 2008, or 2008 R2, which will store all of the data retrieved from the ESP Agents.

Security Requirements

The ESP system authenticates all Fixlet messages and actions using secure public-key infrastructure (PKI) signatures. PKI uses public/private key pairs to ensure authenticity.

Before you can install ESP, you must use the ESP Installer to generate your own **private key** and then apply to ESP for a signed certificate containing your **public key**. Your private key (which only exists on your computer and is unknown to anyone else, including ESP) is encrypted by a password of your choosing, so if someone steals it, they still need to know your password in order to use it. Nevertheless, you should guard it well. ***Anyone who has the private key and password for your site, access to the server and a database login will be able to apply any action to your ESP Agent computers.***

Treat your private key just like the physical key to your company's front door. Do not leave it lying around on a shared disk. Instead, store it on a removable disk or a secured location – and ***do not lose it***. In the physical world, if you lose your master key you have to change all the locks in the building. Similarly, if you lose your digital key, you will need to do a migration to a new authorization key or a fresh install of the entire system (including all the ESP Agents). It is not unreasonable to store a backup copy of your site level key files in a secured safe deposit box.
As the ESP Site Administrator, you will authorize trusted people within your enterprise to deploy, or publish, remedial Fixlet actions across the network. These ESP Console operators will have publishing rights, and they must sign all the actions they publish with their own private key. Like the ESP Site Administrator, they have a password to encrypt their private key. Both the password and the key should be carefully guarded for each authorized operator.

Whenever operators issue an action, it must be signed by their private publisher key. Then when the ESP Agent receives the action, it validates the signature using the public key information. If the signature validation fails on the ESP Agent, the operator's action is discarded. This prevents unauthorized personnel from using the ESP Console to propagate actions.

Fixlet messages are also digitally signed. The Fixlet site author signs each message with a key that can be traced back to the ESP root for authentication. This signature must match the Fixlet site's masthead, which is placed in the ESP Agent install folder upon subscribing to the site. This procedure prevents spoofing and man-in-the-middle attacks, and guarantees that the Fixlet messages you receive are from the original certified author.

There are a few other security-related issues to address before installing ESP in your organization:

- Make sure the ESP Server computer is running Windows Server 2003+ with the latest Service Pack available from Microsoft.
- Make sure that the SQL Server is secured with the latest security-related patches.
- Verify that your network firewall forbids inbound and outbound traffic on the specified port (default 52311) so that ESP-related traffic will not be able to flow into or out of your network.

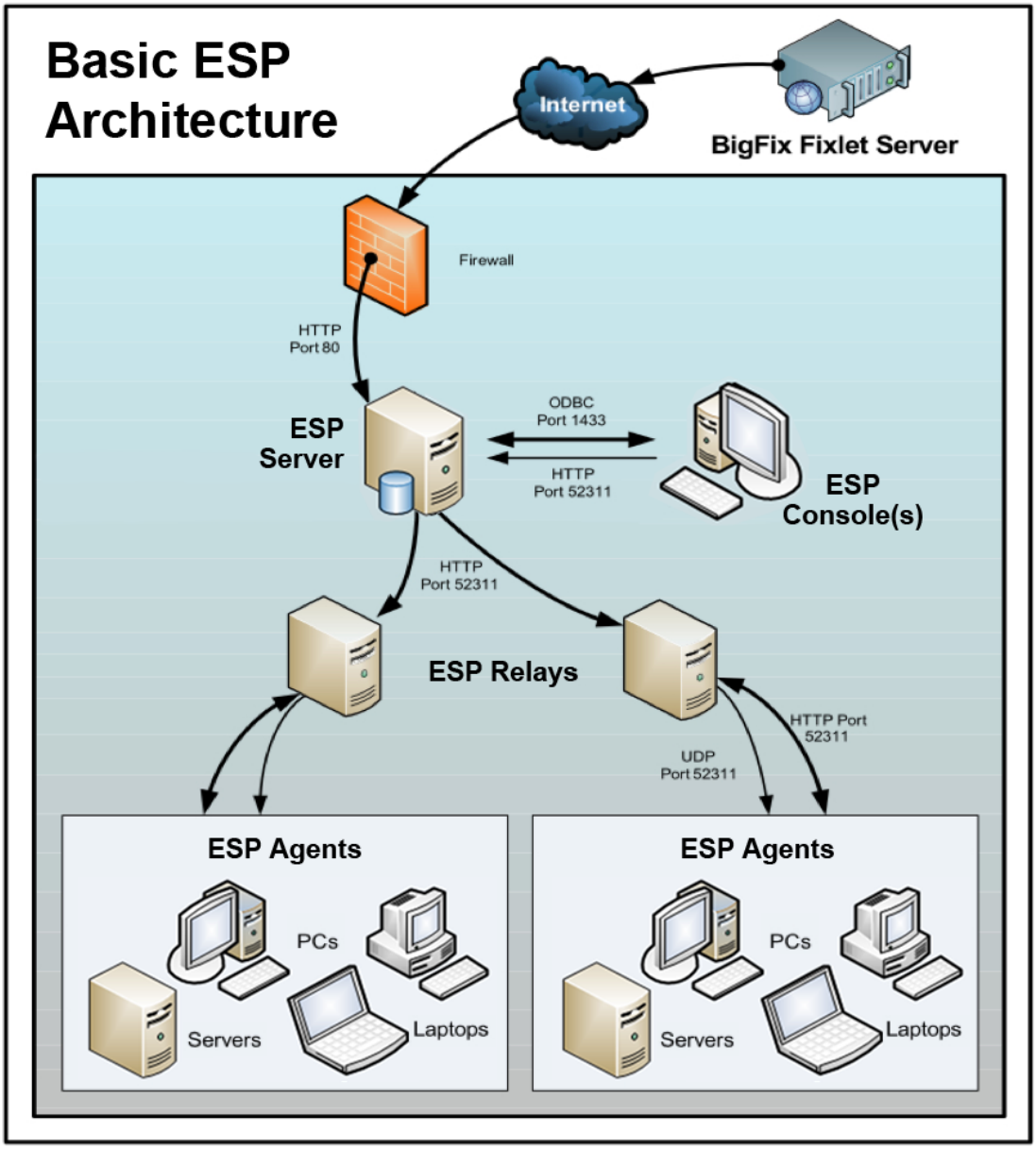
  It is possible to administer roaming laptops by opening this port on your firewall. However, a better technique is to use message-level encryption to route the relay through a non-default port and avoid opening this port altogether.
- Make sure that TCP/IP and UDP on the specified port (default 52311) is completely unblocked at all internal routers and internal firewalls.
- Verify with your network administrator that you can allow the ESP Server to access the Internet via port **80**. The ESP Gather service is the only component of the ESP Server that accesses the Internet and by default it runs as the Windows SYSTEM account. If the SYSTEM account cannot reach the Internet because of proxy or firewall restrictions, then you will need to set the ESP Gather service to logon as a user with Internet and administrative access on the ESP Server computer. Detailed instructions on how to configure the server are available from the knowledge base at the Trend Micro support site.

  It is also possible to maintain a physical disconnect from the Internet with an air-gapped implementation as described in the KB article at the Trend Micro support site.
- You should secure the ESP Server computers and the SQL or SQLite database using company or industry-wide standards. Contact your network administrator or database administrator for more information.

Note: Certain rare lockdown procedures may cause the ESP Servers to function improperly. Contact your support technician if you have any specific questions about lockdown procedures.

A Basic Installation

A simplified ESP deployment resembles the diagram below. There is at least one ESP Server that gathers Fixlet messages from the Internet where they can be viewed by the ESP Console operator and distributed to the ESP Relays. Each ESP Agent inspects its local computer environment and reports any relevant Fixlet messages back to the ESP Relay, which compresses the data and passes it back up to the server(s).



The ESP Console oversees all this activity. It connects to the ESP Server(s) and periodically updates its displays to reflect changes or new knowledge about your network.

The ESP Console operator can then target actions to the appropriate computers to fix vulnerabilities, apply configuration policies, deploy software, etc. The progress of the

actions can be followed in near real-time as they spread to all the relevant computers and, one by one, address these critical issues.
This diagram labels all the default ports used by ESP, so you can see which ports need to be open and where. These ports were selected to avoid conflict, but if you are currently using any of these ports, they can be customized upon installation.

Note: The arrows in the diagram are intended to illustrate the flow of information throughout the enterprise. The arrows from the Fixlet Server to the ESP Server(s) represent the flow of Fixlet messages into your network. ESP Agents gather Fixlet messages and action information from ESP Relays. They then send small amounts of information back to the ESP Server(s) through the ESP Relays. The UDP packets from the ESP Relay to the ESP Agents are small packets sent to each ESP Agent to inform them that there is new information to be gathered. The UDP messages are not strictly necessary for ESP to work properly. Please view the article on network traffic at the Trend Micro support site, or ask your support technician for more details.

ESP Message Level Encryption (MLE) Overview

Message Level Encryption (MLE) allows your ESP Agents to encrypt upstream data using a combination of an RSA public/private key-pair and an AES session key.
The RSA key-pair can be of 2048- or 4096-bit key length, with longer keys offering additional security but requiring more processing power for decryption at the server. The AES session key uses the maximum FIPS-recommended length of 256 bits. You can configure your ESP relays to reduce the load on the ESP Server by decrypting and repackaging the Agent data before relaying it.
The RSA public key encrypts the session key and adds it to the AES-encrypted report. At the ESP Server (or a decrypting ESP Relay) the corresponding RSA private key is used to decrypt the AES session key which is then used to decrypt the ESP Agent report.
There are three levels of report encryption:

- **Required:** Agents require encryption of reports and uploads. The client will not report or upload files if it cannot find an encryption certificate or if its parent relay does not support receipt of encrypted documents.
- **Optional:** Agents prefer, but do not require encryption of reports and uploads. If encryption cannot be performed, reports and uploads are done in clear-text.
- **None:** Agents do not encrypt, even if an encryption certificate is present.

A Typical Installation

Although the basic installation discussed above shows many of the specific ports needed to establish the ESP network, it does not illustrate two important aspects of many ESP deployments: a DMZ and direct connections. In the DMZ example, an office connected by a VPN can share the content from an ESP Relay or Server. In the direct connection, home PCs and laptops can connect directly to the Internet for content from ESP Fixlet servers through their own private firewalls. For the sake of clarity, these extra connections may not be shown in all diagrams, but they are generally present in most deployments.

A Multiple Server Installation

ESP includes the important ability to add multiple, fully redundant ESP Servers – a feature called Distributed Server Architecture (DSA). Each Server maintains a replica of the ESP database and can be positioned anywhere in the world. In the case of a network fracture, these Servers continue to provide uninterrupted service to the local network. As soon as the connection is re-established, the Servers automatically reconnect and sync up. The ESP Relays and Agents are also capable of gracefully recovering from such a disconnect. DSA provides the following capabilities:

- Continued service availability on both sides of a network split (automatic failover).
- Continued availability in the event of a server outage.
- Distribution of Console database load during normal operation.
- Automatic failback upon reconnection.

To take advantage of this functionality, you will need one or more additional servers with a capability at least equal to your primary server. All ESP servers in your deployment must run the same version of SQL Server. If your existing ESP Server is running SQL 2005, your new servers must run SQL 2005 as well.

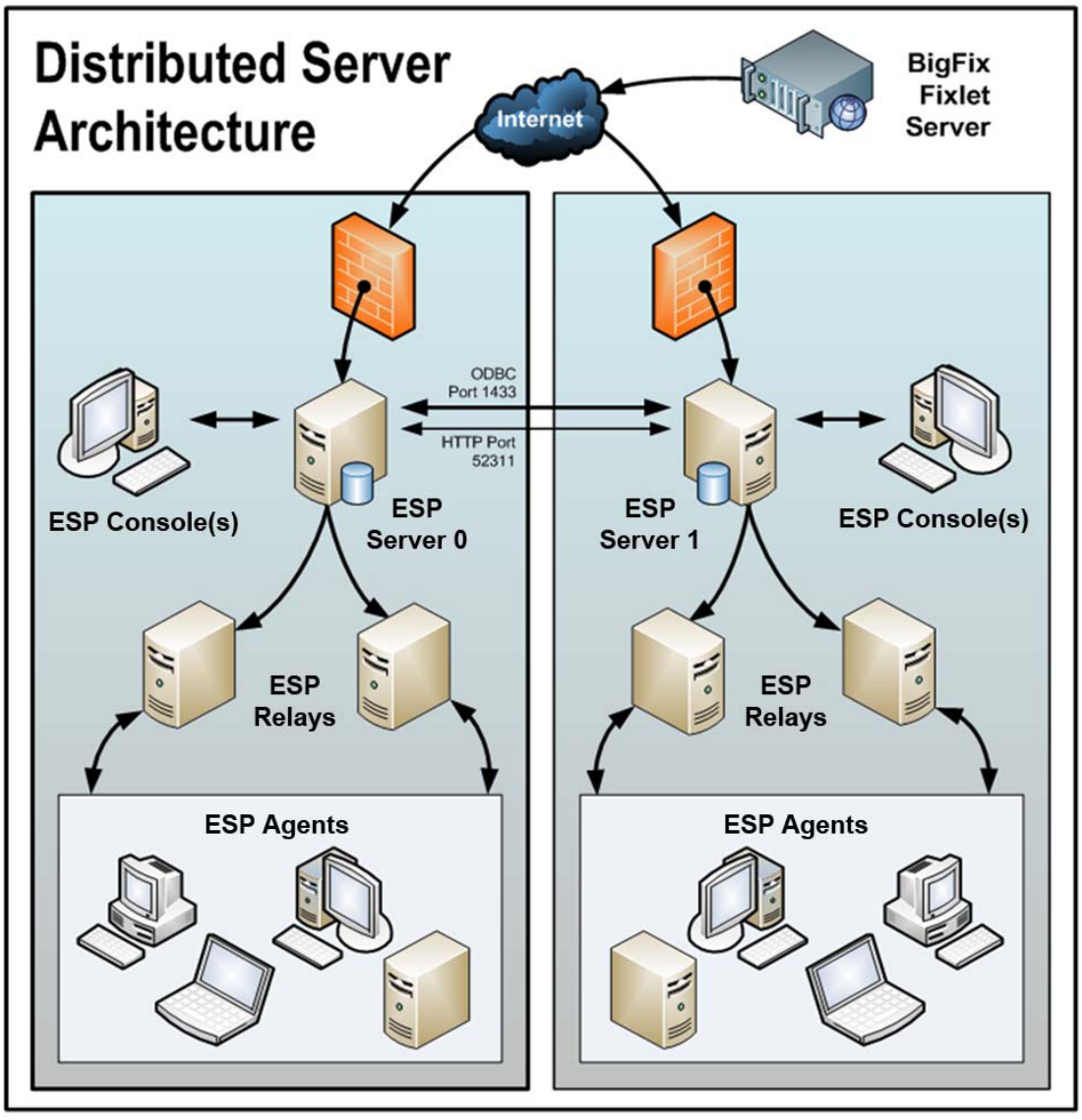
Understanding Replication

Additional servers help to distribute the work load and create a redundant system that is hardened to outages. Knowing how it accomplishes this can help you to create the most efficient deployment for your particular network. Here are some of the important elements of multi-server installations:

- Servers communicate on a regular schedule to replicate their data. You review the current status and adjust the replication interval through **ESP Administration > Replication**.
- When each server goes to replicate from the other servers in the deployment, it calculates the shortest path to every other server in the deployment. Primary links are assigned a length of 1, secondary links 100, and tertiary links 10,000. Links which resulted in a connection failure the last time they were used are considered to be non-connected.
- When an outage or other problem causes a network split, it is possible to for a custom Fixlet or a retrieved property to be modified independently on both sides of the split. When the network is reconnected, precedence will go to the version on the server with the lowest ESP Server ID.
- If multiple copies of **Web Reports** are installed, they will operate independently. Each Web Report Server can connect to the ESP Server that is most convenient, since they all contain equivalent views of the database.
- By default, server 0 (zero) is the master server. **ESP Administration** will only allow you to perform certain administrative tasks (such as creating and deleting users) when connected to the master server.
- If you want to switch the master to another server, you can do so with a setting. For more information, see the section on **Managing Replication** (page 72).

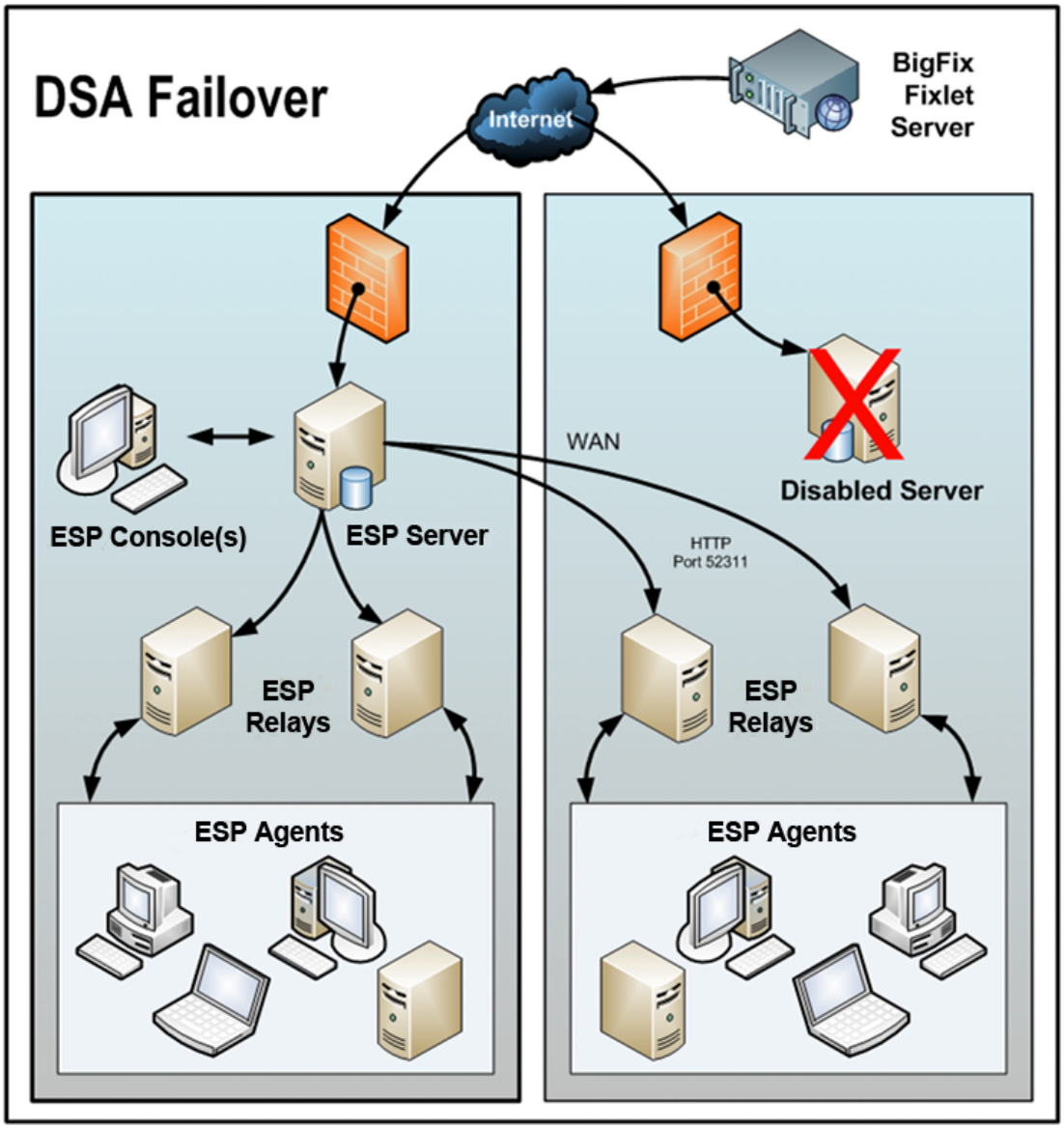
Distributed Server Architecture (DSA)

The following is a diagram of a typical DSA setup with two servers. Each ESP Server is behind a firewall, possibly in a separate office, although it is easy to set up multiple servers in a single office as well. It is important that the ESP Servers have high-speed connections to replicate the ESP data (generally LAN speeds of 10-100MBPS are required). The ESP Servers will communicate over ODBC and HTTP protocols. This DSA configuration provides automatic failover and failback services, minimizing loss of data.



Automating Failover and Failback

If an ESP Server goes down, whether due to disaster or planned maintenance, the DSA deployment reconfigures itself (hot failover) as the orphaned ESP Relays find a new server connection. When the disabled server comes back online, its data will automatically be merged with the data on the healthy server.



Administrative Roles

To install and maintain ESP typically requires the cooperation of several administrators and operators:

- **The Network Administrator.** This person will need to allow the ESP Server to connect to the Internet through the existing proxy server (if applicable) as well as resolve any network-specific issues that may prevent ESP from working properly. The network administrator will also provide information about WAN link connection speeds and subnet addresses if necessary. When starting a deployment of ESP, it is best to make the Network Administrator aware of how ESP uses the network by reviewing the page on network traffic at the Trend Micro support site.
- **The Database Administrator.** This person will be responsible for setting up and maintaining the SQL Server 2005+ database for the ESP Server.
- **The ESP Site Administrator.** This person will install and maintain the ESP software, including the ESP Server, ESP Console, and the ESP Agent programs. The Site Administrator will also be responsible for creating, distributing, and revoking publisher keys and management rights that allow ESP Console operators to deploy actions. The Site Administrator is the only person in an organization who can authorize new ESP Console Operators or Master Operators (see next bullet). A Site Administrator holds this position by virtue of having administrative access to the ESP Server computer as well as access and the password to the site-level signing keys.
- **ESP Console Master Operators.** These people are operators with access to all the ESP computers with the added authority to assign management rights to other ESP Console operators. Master Operators can do most of what you can do as the Site Administrator. In fact, Master Operators are often referred to as administrators. However, only the ESP Site Administrator can create new operators and a Master Operator can only create custom content with permission from the Site Administrator.
- **ESP Console Operators.** These people will manage the day-to-day operation of ESP, including Fixlet management and action deployment, typically on a subset of computers subject to the management rights assigned by an ESP Site Administrator or Master Operator.

Often these administrative roles will overlap and one person may be assigned multiple duties. The network and database duties are limited to minimal setup procedures, which are covered in this document. The ESP Console Operators (including Master Operators) should read the separate ***ESP Console Operator's Guide***.

Duties of the ESP Site Administrator

This ESP Site Administrator has the following primary responsibilities:

- **Obtaining and securing the Action Site Credentials.** In order to install ESP, the ESP administrator needs to generate a private key, receive a license certificate from ESP, and create a masthead with the digital signature and configuration information.
- **Certifying Users.** The ESP Site Administrator must create an account and private key files for each operator. You should avoid using the same login information for site-level and user-level accounts. This practice increases confusion about context and can lead to errors.
- **Preparing the ESP Server**. The ESP Server must be properly set up to communicate externally with the Internet and internally with the ESP Agents. The ESP Server also needs to be configured to host the ESP database (or another computer can be used as the SQL Server database).
- **Installing the various** ESP Components. The ESP Site Administrator will install the ESP Agent, Server, Relay and Console modules.
- **Assigning Management Rights.** ESP Master Operators can assign management rights to the ESP Console operators. These rights constrain operators to specific computers. You can also grant or revoke the right to make custom content or to view unmanaged assets.
- **Maintaining the ESP Server**. The ESP Server runs a SQL Server database and many ESP specific services. Standard maintenance tasks like upgrades or fixes will be managed using Fixlet technology or may be performed manually by the ESP Site Administrator.
- **Maintaining security**. The ESP system is protected by password-encrypted private keys. The ESP Site Administrator controls access to these and can create new private publisher keys or revoke them as the need arises. ESP authentication uses public key infrastructure (PKI) technology with key lengths of up to 4096 bits.

Each of these administrative duties is described fully in the following sections of this guide.

Part Two

Getting Started

Now that you understand the terms and the administrative roles, it's time to actually get authorized and install the programs. This guide goes through each step in detail, but the process is typically straightforward and speedy.

Getting Authorized

Because ESP is powerful, you will want to limit access to trusted, authorized personnel only. ESP operates from a central repository of Fixlet actions called the **Action site**, which uses public/private key encryption to protect against spoofing and other unauthorized usage. To get started, you need authorization from Trend Micro, Inc.

If you have not yet purchased a license to use ESP, please Sales (+1 (800) 228-5651) or visit the Trend Micro Website at http://us.trendmicro.com/us/about/contact/.

The sales agent will want to know how many ESP Agents you intend to install. Based on this, the agent will create, sign and email you an **ESP License Authorization** file which will have a name like "CompanyName.ESPLicenseAuthorization".

The Installer program will collect further information about your deployment and then create a file called the **action site masthead**. This file establishes a chain of authority from the ESP root all the way down to the ESP Console operators in your organization. The masthead combines configuration information (IP addresses, ports, etc.) and license information (how many ESP Agents are authorized and for how long) along with a public key used to verify the digital signatures. To create and maintain the digital signature keys and masthead, you will use the **ESP Installer**, which you can download from Trend Micro, Inc.

> **Note:** If you are using an evaluation version of ESP, you may skip the following section. During installation, the ESP Evaluation Generator will create your signing keys through an expedited process, and the generation of separate publisher keys will not be necessary.

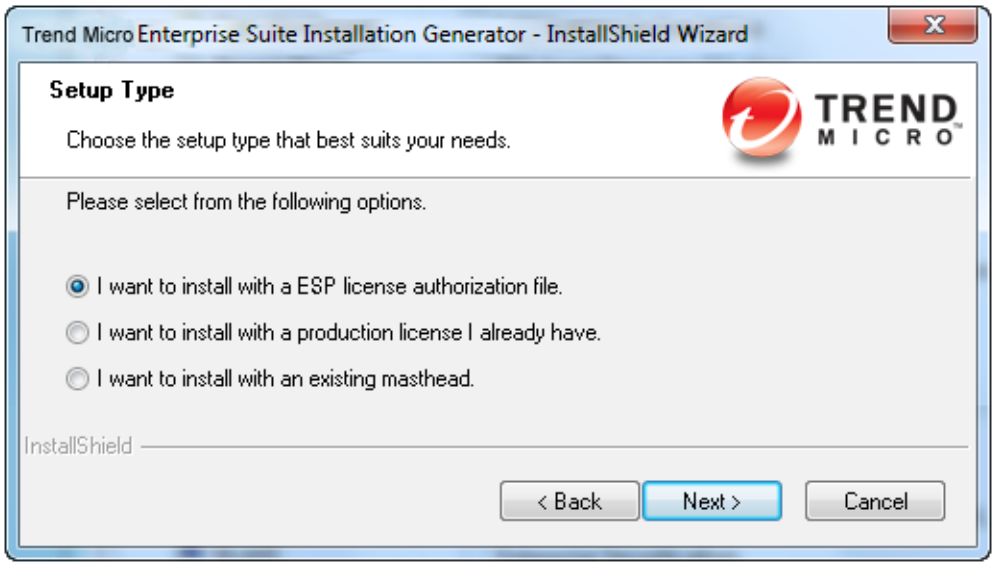
Creating the Action Site Masthead

Before you perform the steps below, you must have purchased a license and received an ESP License Authorization File (see previous section).

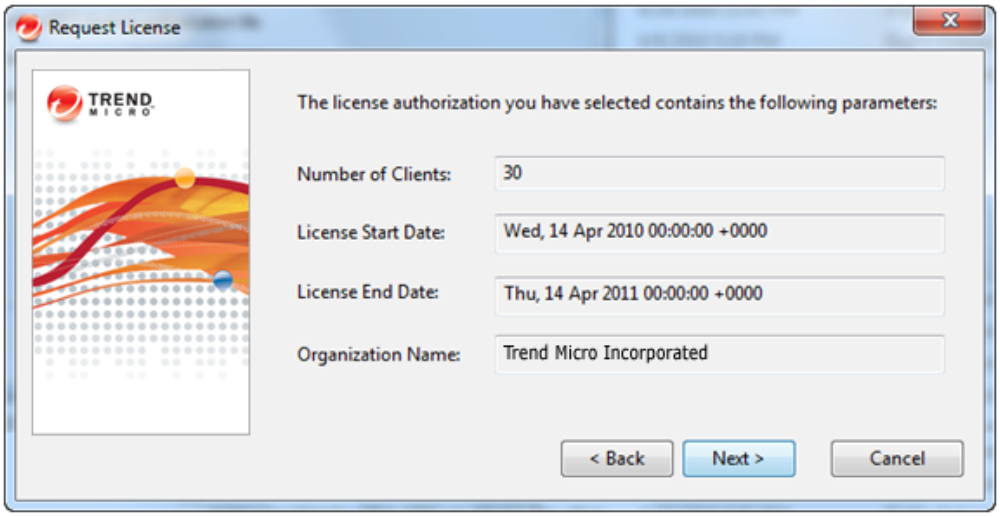
Once you have your license authorization file, you are ready to create a personalized **action site masthead** that will, in turn, allow you to install and use ESP. The masthead includes URLs for the ESP Server CGI programs and other site information in a signed MIME file. The masthead is central to accessing and authenticating your action site. To create the masthead and activate your site, follow these steps:

1. Run the ESP Installer that you downloaded from the Trend Micro site (www.trendmicro.com). At the welcome screen, click **Next**.
2. You will see a dialog offering to install the Evaluation or Production version of ESP. Select **Production** and click **Next**.

3. After reading the License Agreement, click **Yes** to accept it and continue. The **Setup Type** dialog appears.



4. Select the choice to **install using the License Authorization file from Trend Micro, Inc.**, then click **Next**.
5. The ESP Action Site Masthead Creation Wizard launches. It asks you for the location of your license authorization file. Click the **Browse** button to bring up a standard Windows open-file dialog. Navigate to your license authorization file, which has a name like CompanyName.ESPLicenseAuthorization. Select the file and click **Open.**
6. A dialog appears displaying the current contents of your license authorization.



Click **Next**.

7. The next screen in the Wizard prompts you for the **DNS name** or **IP address** of your ESP Server. Type this in and click **Next**.

8. Note: The DNS/IP address that you choose becomes a permanent part of your deployment and must never change. For the sake of flexibility, we strongly recommend using a DNS name instead of a static IP address.
9. The next screen in the Wizard prompts you for a site-level **password** so you can create a site admin key for your deployment. Type in your password twice (for verification), and specify a key size (from 2K- to 4K-bits) for the public/private key pair. Click **Next**.
10. From the **Save As** dialog, find a folder to save your private key file (license.pvk) to a secure location, such as a PGPDisk on a USB drive. Click **Save**.
11. The next screen in the Wizard prompts you to submit your masthead request to ESP. This request consists of your original authorization, your server DSN name and your public key, all packaged into a single file. Typically, you will select the first choice, **submit request**, to post the request via the Internet. Click **Next**. The Wizard will then retrieve your certificate (license.crt) from the Trend Micro License Server.

    (Alternatively, the Wizard will let you save the request as a file named request.ESPLicenseRequest. Then you can visit the Trend Micro website, post your request and download your certificate.)
12. Upon a successful request submission, the Wizard retrieves your license (license.crt) and prompts you to save it. Click **Save**. This action completes the Wizard, returning you to the **Setup Type** dialog. You are now ready to install the programs with your new production license.
13. Keep in mind that the private key (license.pvk) to your action site authorizes you, as the ESP Site Administrator, to create ESP Console operators with publisher credentials. This key is *not* sent to ESP during the creation process, and should be carefully protected. For the highest level of security, it is recommended that you save the ESP Credentials to an encrypted disk, such as a PGPDisk on a USB key or other removable media.

Warning!

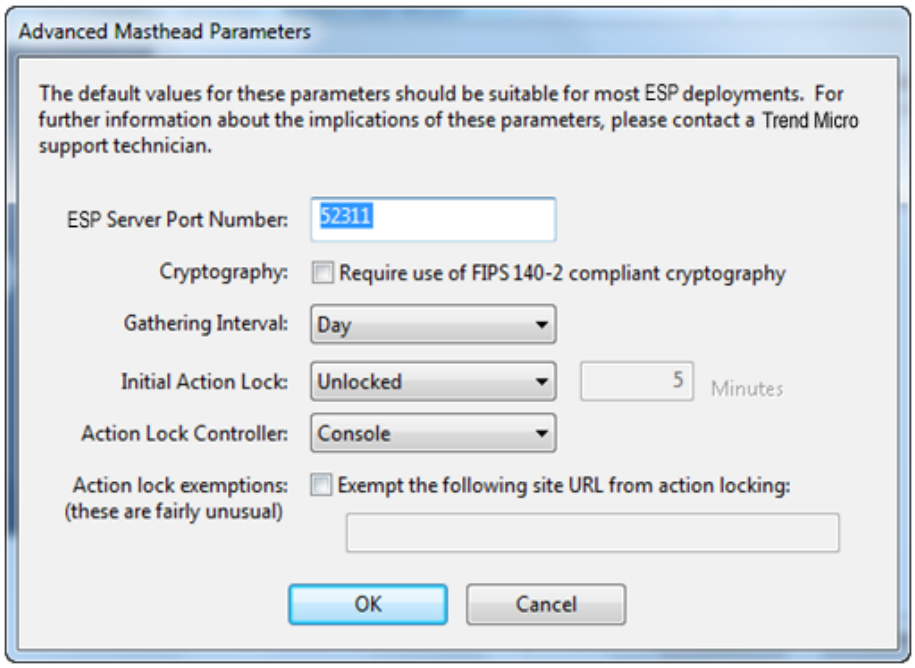
If you lose your site credential files or password, then no one – not even Trend Micro – can recover your keys or your password. You will need to ***reinstall the entire system***, including all the ESP Agents, with a freshly generated key.

If the main ESP Server is lost, you may also lose your encryption key file. For disaster recovery you have two options: you can back up your encryption key now, so you can restore it after recreating the ESP Server, or you can generate a new encryption key after recreating the ESP Server.

Installing the Programs

Once you have your license and/or your action site masthead, you are ready to install the programs. Here is how:

1. If the installer is not already running, launch it. From the **Setup Type** dialog, select the second choice to **Install with a production license**. Click **Next**.
2. Browse to the location of your license key and click **Open**.
3. A dialog appears, prompting you for your private **site signing key** (license.pvk). This is typically stored in the same folder as the license.crt file. Browse to it and click **Open**.
4. A dialog prompts you for the **Site Admin Private Key Password**. Enter the password you selected to protect your private key (see the previous section) and click **OK**.
5. The program prompts for a server port number that ESP will use for all its data transmissions. The default port is **52311**.



This is the recommended port number, but you may choose a different port if that is more convenient for your particular network. Typically, you would choose a port from the IANA range of private ports (49152 through 65535). You could use a reserved port number (ports 1-1024), but it is not considered best practice because it inhibits the ability to monitor or restrict traffic properly and it defeats the idea of port numbers for specific applications. The lock options in this dialog typically do not need to be changed unless you want a computer to automatically be locked after installation. There is also a checkbox if you want to apply FIPS 140-2 Cryptography. Click **OK** when you are done.

You should accept the default settings on this page unless you have a specific reason

to change them. Improper settings can cause ESP to work in a sub-optimal fashion. Consult with a support technician for more details.

6. A standard Windows **Save As** dialog prompts you to save the **Masthead**. This is a public file that does not require protection. Navigate to the desired folder, name the file (e.g. actionsite.afxm), and click **Save**.
7. You are now ready to generate the **Endpoint Security Platform installation components**. Select the default directory (ESP Installers) or click **Browse** to choose a different folder. Click **Next**.
8. The Install Wizard will then generate and save various ESP installation components. After saving the files, a dialog appears confirming the installation and reminding you of their location. Click **Finish** to exit and start the **ESP Installation Guide**.

Running the Component Installers

So far, you have created a private key, requested and received a certificate, used the certificate to create a masthead and then generated the various ESP installation components, including the **ESP Installation Guide**. When the components have been saved, the **ESP Installation Guide** automatically launches. You may also run it at any time by selecting it from the Start Menu.

To install the three major components of ESP (ESP Server, Console, and Agent), follow these steps:

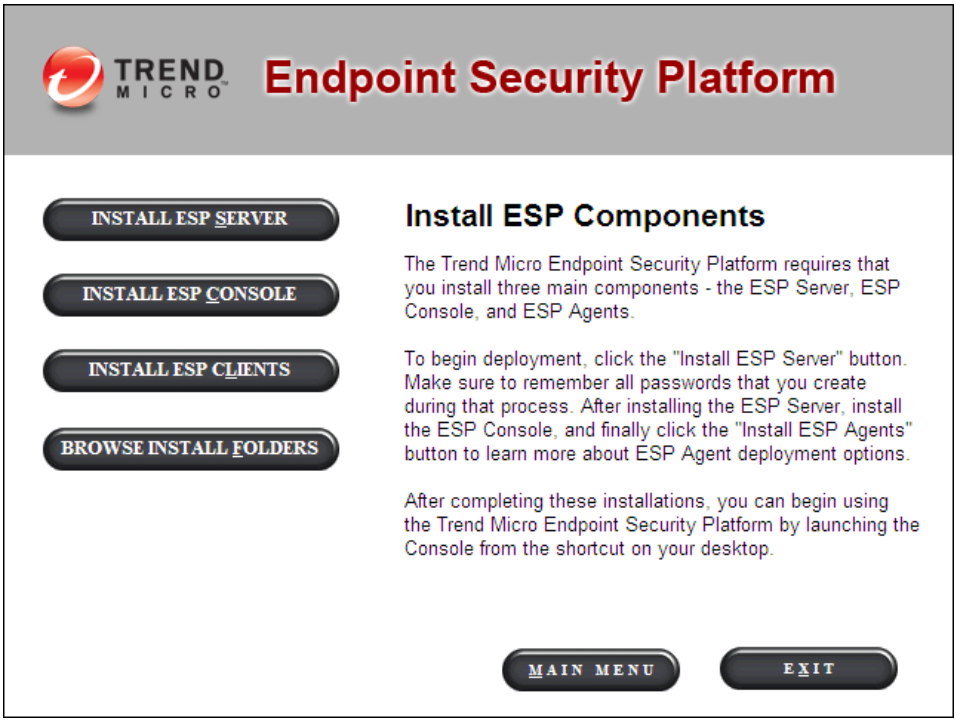
1. If it is not already running, launch the ESP Installation Guide (**Start > Programs > ESP Enterprise > ESP Installation Guide**).
2. Select the button labeled **Install ESP Components**.
3. A dialog box appears, prompting you to select an ESP component to install. Click the buttons on the left, in order from top to bottom, to install the ESP components. The component installers include:
   - Install ESP Server
   - Install ESP Console
   - Install ESP Agents
   - Browse Install Folders
4. The ESP Server, Console and Agents all have their own installers. Follow the instructions for each, as described in the following sections.

Installing the Primary ESP Server

The ESP Server is the heart of the ESP System. It runs on a server-class computer on your network that should have direct Internet access as well as direct access to all the ESP Agent computers in your network. Make sure your server meets the requirements outlined in the **ESP Server Requirements** section (page 11). Also, you can consult the knowledge-base article on server requirements at the Trend Micro support site.

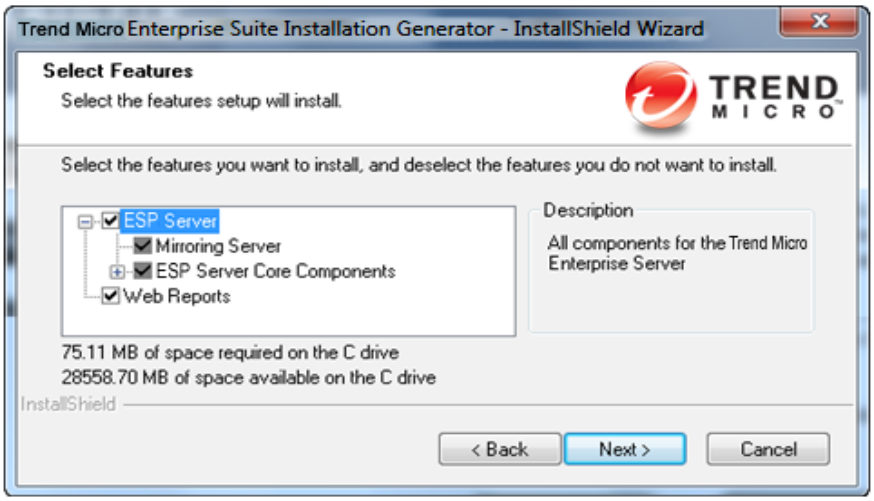
To install the ESP Server, follow these steps:

1. If you have not already done so, run the ESP Installation Guide (**Start > Programs > ESP Enterprise > ESP Installation Guide**). Click the button labeled **Install ESP Components**.
2. A new screen appears.



   Click the top button labeled **Install ESP Server.** The ESP Server Install Wizard presents a welcome screen. Click **Next** to continue.
3. After reading the **License Agreement**, click **Yes** to accept it and continue.
4. A dialog prompts you to choose a **Master** or **Replicated** database. Click the first button to create a Master database for later replication – or if you only need a **Single** database in your deployment. Click the second button to create a Replica of an existing Master. If this is your initial installation, click the top button.
5. A dialog prompts you to select a **Local** or **Remote** database. If you want to use another computer to host the ESP Database, it must have a SQL Server already installed. The most common choice is to use the local database.

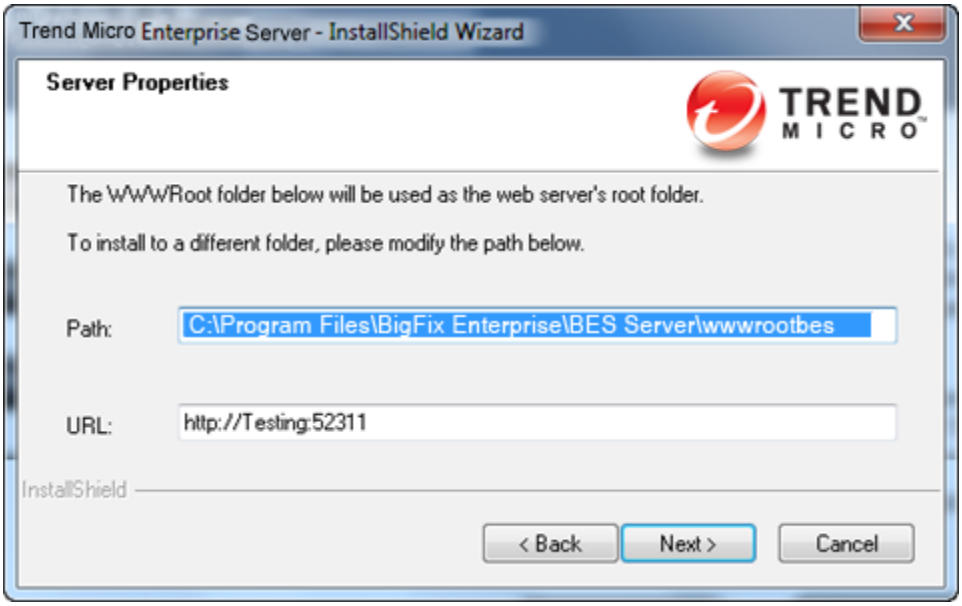
6. A dialog displays a list of the ESP Server components about to be installed.



In general, you should accept the default components and click **Next**.

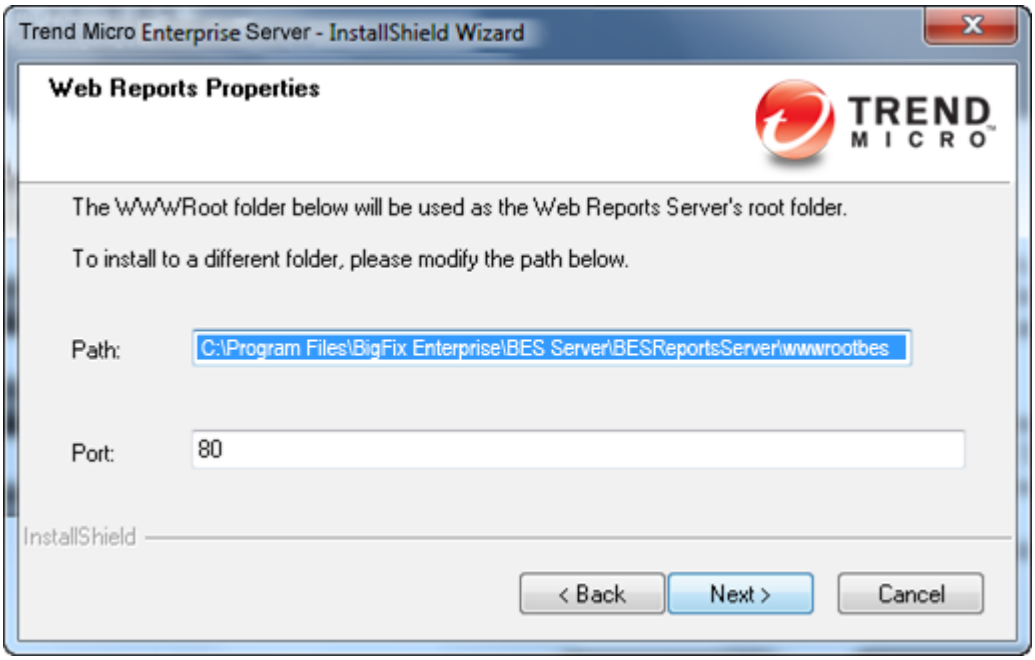
7. The installer prompts you for the desired destination of the ESP Server components. The default location is **C:\Program Files\BigFix Enterprise\BES Server**, but you can specify a different location by clicking the **Browse** button. Once you have decided on the destination, click **Next**.

8. The Server Properties dialog prompts you to enter a location for the ESP Server web root folder (if different from the default). This is where downloaded files for the ESP Agents will be stored. The default URL is also available for editing, should you wish to change it.

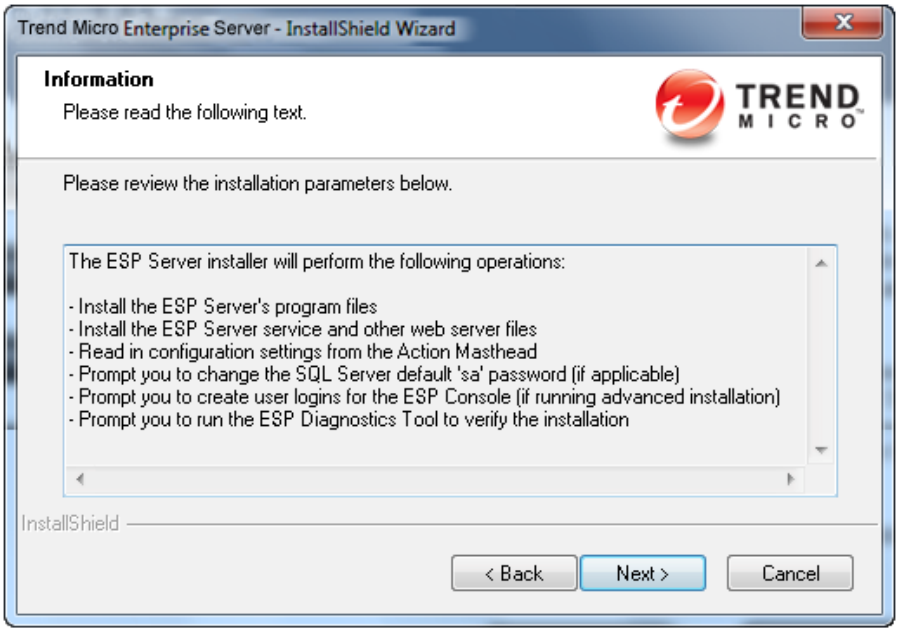


Note: No other application should be listening on the ESP port or errors will occur.

9. Next a dialog prompts you for a location and port number for ESP Web Reports. By default, it will use port 80. If IIS is installed, it will instead choose port 52312.



10. The ESP Server installer then presents a window displaying the selected inventory of server components to be installed as well as some other installation programs to run.

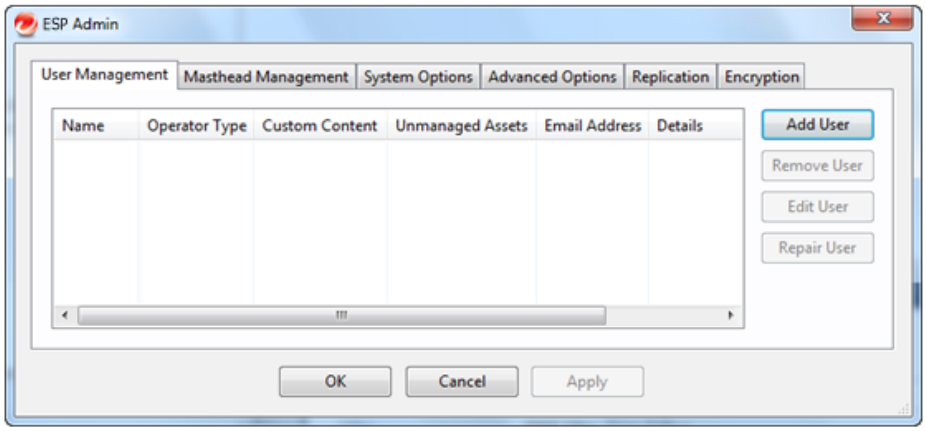


Click **Next** to continue the installation.

11. When the files have been properly installed, the program prompts you for specific information, depending on your installation parameters. The program will ask you to

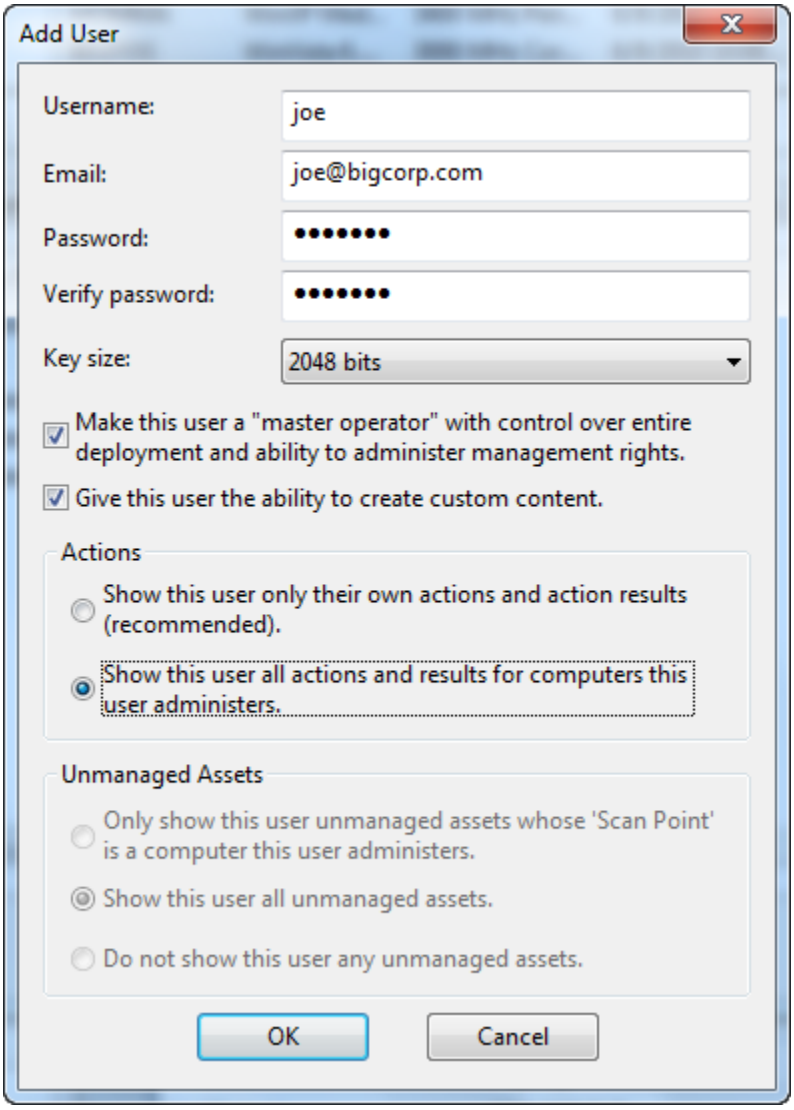
set a default ‘sa’ password if the ‘sa’ password for the SQL Server database is currently blank (this is done for security reasons).

12. The program then prompts you to locate the **Action Site Masthead**. Click **OK** to continue. At the Windows Open dialog, navigate to the folder where you stored your masthead, select it and click **Open**.
13. The program may prompt you for the location of your **license certificate**. Click **OK** to continue. At the Windows Open dialog, navigate to the folder where you stored your license (license.crt), select it and click **Open**.
14. Next, the program may prompt you for the location of your private key (license.pvk). Accept the default path (if specified) or click the **Browse** button to find a different location. Finally, enter your password to initialize the database.
15. The program then prompts you to create an administrative user. Click **OK** to open the **ESP Enterprise User Management** dialog.



Click **Add User** to enter each desired user.

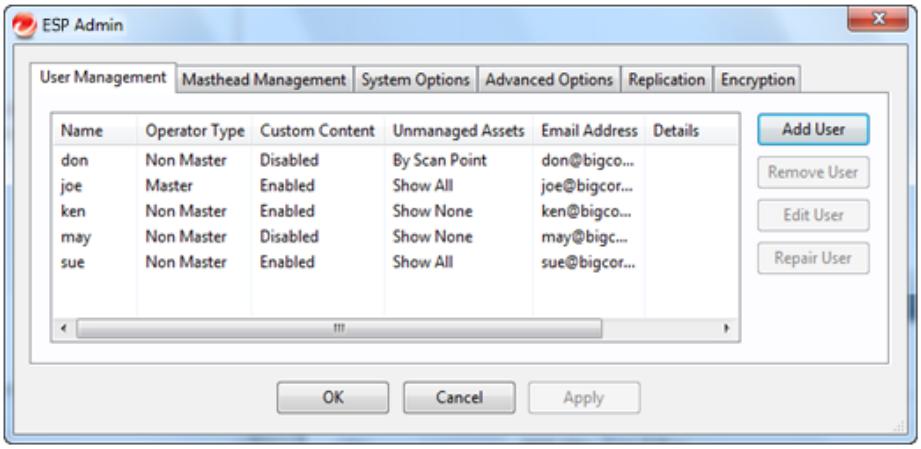
For each user, enter the name, email, password and various permissions.



You do not need to add all your users at this point; you will be able to add more users by running the **ESP Administration Tool** later. Enter the name of the ESP operator (no spaces allowed), the email address and a password for this user. Indicate whether you want to allow this user to **administer management rights** or to **create custom content**.

You must grant administrative rights to at least one user, typically yourself. You can limit user rights to view **unmanaged assets**. You can also limit users to their specific domain (using Scan Point), allow unfettered access or disallow all access. Click **OK** when done.

16. When you have finished entering users, click **Done**.



The program prompts you for your site admin password in order to propagate the ESP Operator information.

17. The ESP Server installation is now complete. As the program exits, it gives you a chance to assess the installation. Make sure the box labeled **Run the ESP Diagnostic Tool** is checked and then click **Finish**. Click the **Full Interface** button to run the ESP Diagnostics in order to ensure that the installation is functioning properly and to present a complete analysis for your inspection. For more information on this dialog, refer to the section labeled **Running the ESP Diagnostics Tool** later in this guide.

Authenticating Additional Servers (DSA)

Multiple servers can provide a higher level of service for your ESP installation. If you choose to add Distributed Server Architecture (DSA) to your ESP installation, you will be able to recover from network and systems failures automatically while continuing to provide local service. To take advantage of this functionality, you will need one or more additional servers with a capability at least equal to your primary server. Because of the extra expense and installation involved, you should carefully think through your needs before committing to DSA.

First, you must decide how you want your ESP Servers to communicate with each other. There are three inter-server authentication options: the first two are flavors of NT and the third is SQL. Because it is more secure, Trend Micro recommends NT Authentication. You cannot mix and match; all ESP Servers must use the same authorization.

Using NT Authentication with Domain Users/User Groups

With this technique, each ESP Server uses the specified domain user or a member of the specified user group to access all other ESP Servers in the deployment. To authenticate your ESP Servers using Domain Users/User Groups, follow these steps:

1. Create a service account user or user group in your domain. For a user group, add authorized domain users to your ESP Servers. You may need to have domain administration privileges to do this.
2. On the Master ESP Server, use SQL Server Management Studio to create a login for the domain service account user or user group, with a default database of **BFEnterprise**, and give this login System Admin (sa) authority or the DBO (DataBase Owner) role on the BFEnterprise and master databases.
3. On the Master ESP Server, change the **LogOn** settings for the ESP FillDB service to the domain user or member of the user group created above, and restart the service.

Using NT Authentication with Domain Computer Groups

With this technique, each ESP Server is added to a specified domain computer group and each server accepts logins from members of that domain group. To authenticate your ESP Servers using Domain Computer Groups, follow these steps:

1. Create a Global Security Group in your domain containing each desired ESP Server. You may need to have domain administration privileges to do this.
2. After creating the group, each server will need to be rebooted in order to update its domain credentials.
3. On the Master ESP Server, use SQL Server Management Studio to create a login for the domain group, with a default database of BFEnterprise, and give this login System Admin (sa) authority or the DBO (DataBase Owner) role on the BFEnterprise and master databases.

Using SQL Authentication

With this technique, each ESP Server is given a login name and password, and is configured to accept the login names and passwords of all other ESP Servers in the deployment. Be aware that the password for this account is stored in clear-text under the HKLM branch of the registry on each ESP Server. To authenticate your ESP Servers using SQL Authentication, follow these steps:

1. Choose a single login name (for example, 'besserverlogin'), and a single password to be used by all servers in your deployment for inter-server authentication.
2. On the Master ESP Server, use SQL Server Management Studio to create a SQL Server login with this name. Chose SQL Server Authentication as the authentication option and specify the password. Change the default database to BFEnterprise and grant it System Admin (sa) authority or the db_owner role for the BFEnterprise and master databases.
3. On the Master ESP Server, add the following String values under the key

   HKLM\Software\BigFix\Enterprise Server\FillDB:
   ReplicationUser = <login name>
   ReplicationPassword = <password>
4. Restart the ESP FillDB service.

> **Note:** This choice must be made on a deployment-wide basis; you cannot mix domain-authenticated servers with SQL-authenticated servers. Also, all ESP servers in your deployment must be running the same version of SQL Server.

Installing Additional Servers (DSA)

Before proceeding with this section, determine your authentication method and complete the appropriate steps in the **Authenticating Additional Servers (DSA)** section discussed previously.

For each additional ESP Server you wish to add to your deployment, make sure they are communicating with each other, and then follow these steps:

1. Install the same SQL Server version being used by the Master ESP Server.
2. Run the **ESP Server installer** on each machine that you wish to configure as an additional ESP Server. You should use the same domain administration that you used for the local SQL Server install (so you have sa authority).
3. If you are extracting the server installer from the ESP Installation Generator, select **Production Deployment**, and **I want to install with an existing masthead**. Specify the masthead.afxm file from the Master ESP Server. Otherwise, use the Server install package from the ESPInstallers folder on the Master ESP Server.
4. On the **Select Database Replication** page of the server installer, select **Replicated Database**.
5. On the **Select Database** page, select **Local Database** to host the database on the server (typical for most applications).
6. Proceed through the installer screens as usual until the installer gets to **Configuring your new installation** and prompts you with a **Database Connection** dialog box.

Enter the hostname of your master server, and the credentials for an account that can log into the master server with DBO permissions on the BFEnterprise database.

7. The Replication Servers window shows you the ESP Server configuration for your current deployment. By default, your newly installed ESP Server should be configured to replicate directly from the master server every 5 minutes. You can adjust this as necessary.
8. For large installations, the initial database replication can take several minutes and may get interrupted. If you experience this problem, you can discuss it with your Trend Micro technical contact.
9. Use SQL Server Management Studio to create the same SQL Server login you created earlier on the Master ESP Server with BFEnterprise as the default database and System Admin (sa) authority or the DBO role on the BFEnterprise and master databases.
10. For NT Authentication via Domain User/User Group, change the LogOn settings for the ESP FillDB service to the domain user or member of the user group created above, and restart the service.
11. For SQL Authentication, add the following string values to the FillDB registry keys, and restart the ESP FillDB Service.
12. HKLM\Software\BigFix\Enterprise Server\FillDB:
    ReplicationUser = <login name>
    ReplicationPassword = <password>
13. On the newly-installed server, run the **ESP Administration Tool** and select the **Replication** tab to see the current list of servers and their replication periods. Select the newly installed server from the pull-down menu, and verify in the list below that it is successfully connected to the master server. Then select the master server in the server dropdown, and verify that is properly connected to the new server. You may need to wait for the next replication period before both servers show a successful connection.
14. Note: The initial replication may take several hours depending on the size of your database. Wait for the replication to complete before taking any actions from a Console connected to the replica ESP Server.
15. You can see a graph of the servers and their connections by clicking the **Edit Replication Graph** button. You can change the connections between servers by simply dragging the connecting arrows around.

Connecting the ESP Console to a Different Server

When an ESP Console is installed on an ESP Server, you will have the option to connect to the local ESP Server via the bfenterprise connection and the Master ESP Server via the EnterpriseServer connection, by default. All standalone Consoles will only connect to the Master ESP Server via the EnterpriseServer connection. To enable standalone Consoles and the Master ESP Server Console to connect to the new replica ESP Server, a new ODBC System DSN must be created:

1. From **Control Panel > Administrative Tools > Data Sources (ODBC)**, select the **System DSN** tab, and click Add.
2. Select the **SQL Server** driver, and click **Finish**.
3. Specify the following information on the subsequent dialog:

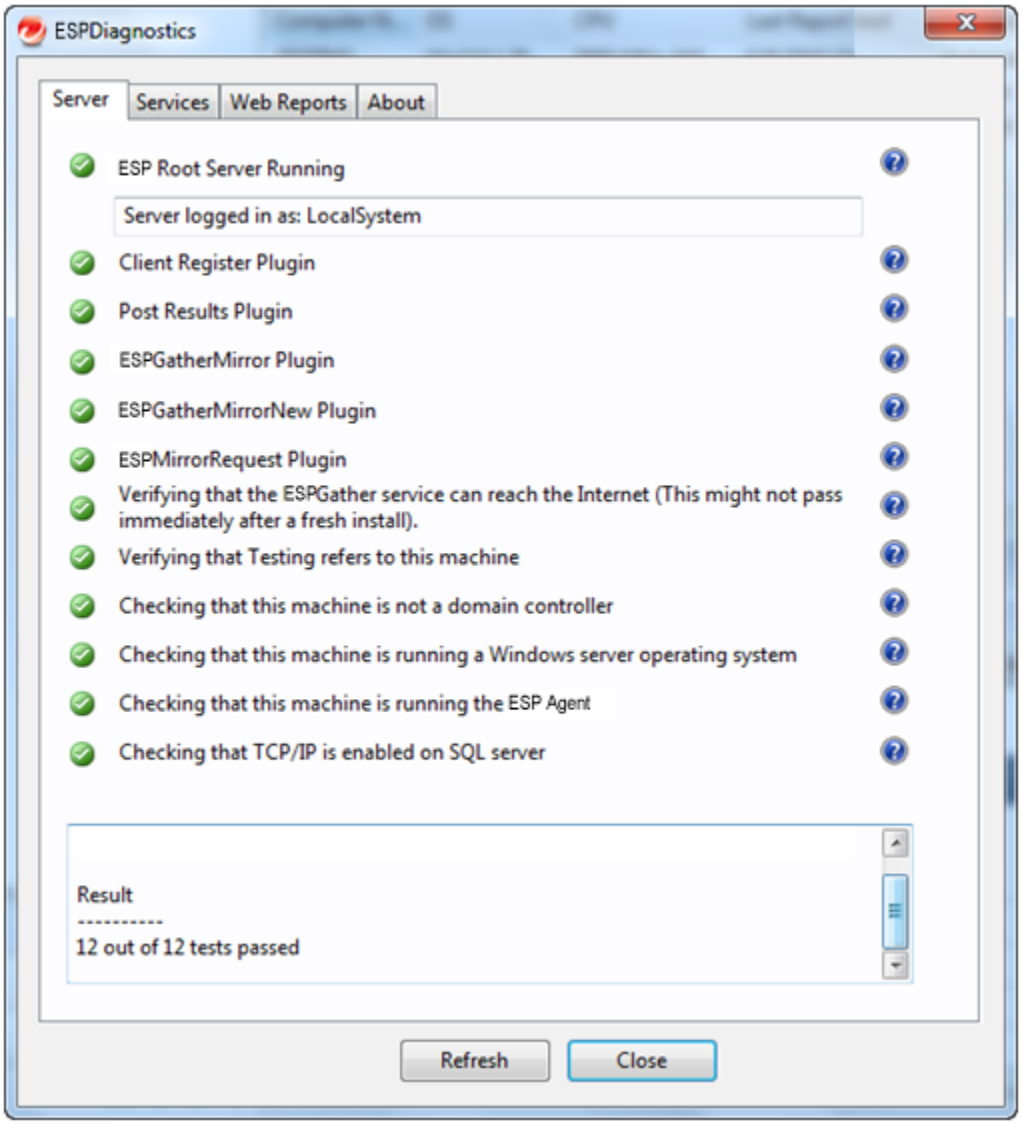
   Enter bes_<servername> for the Name, and <servername> for the Server, where <servername> is the hostname of the new replica ESP Server. Click **Next**.
4. On the following dialog, specify **NT Authentication** or **SQL Authentication** as appropriate for your deployment. If unsure, use SQL Authentication. Uncheck the box to **Connect to SQL Server** to obtain default settings. Click **Next**.
5. Check the top box and change the default database to **BFEnterprise**. Click **Next**, and on the following screen, click **Finish**.

Now when the Console is started, the drop-down menu will offer you the choice between **EnterpriseServer** (to connect to the Master ESP Server), <**servername**> (to connect to the new replica ESP Server) and, on ESP Servers only, **bfenterprise** (to connect to the local ESP Server).

Running the ESP Diagnostics Tool

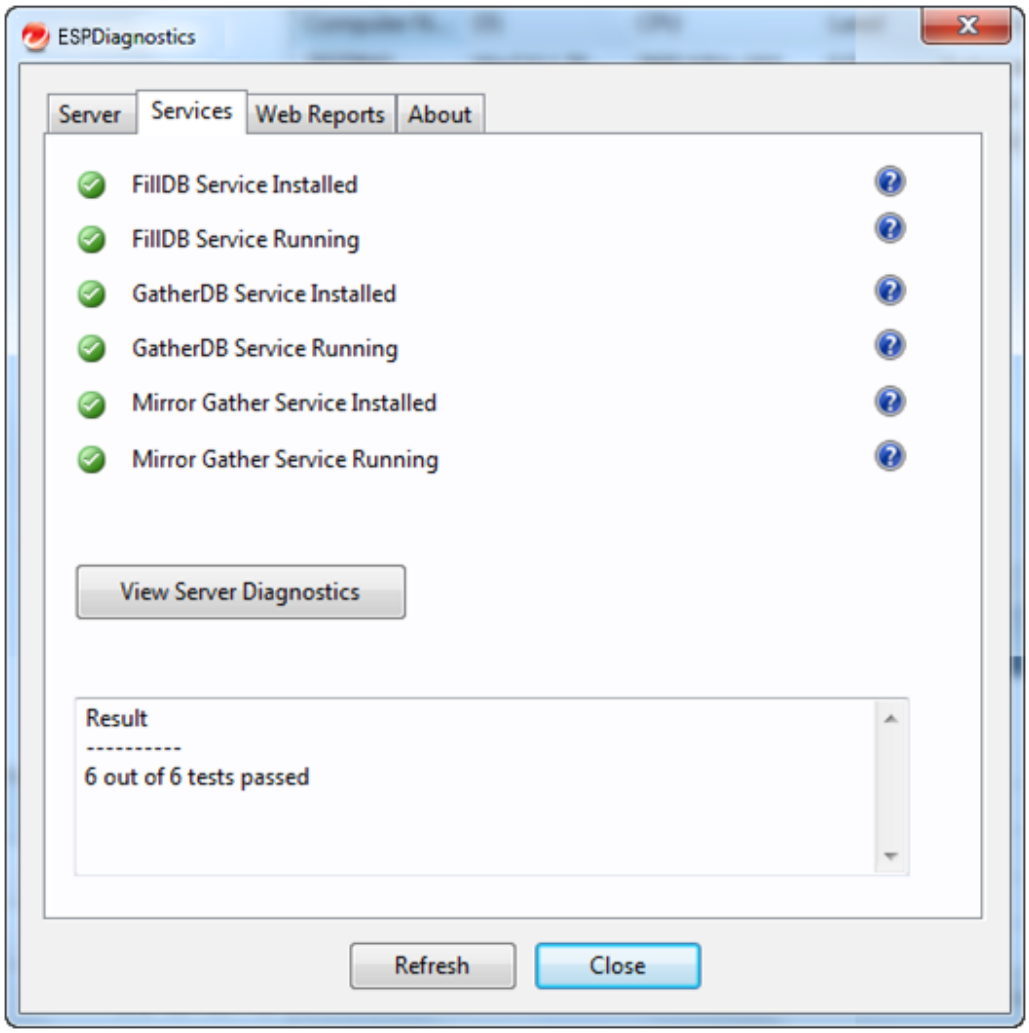
The ESP Diagnostics tool verifies the proper functioning of the ESP Server components. It identifies components that are incorrectly configured or non-functional and displays the results. To run the diagnostics, follow these steps:

1. If you have just installed the ESP Server, the ESP Diagnostics Tool should already be running. Otherwise, log on to the ESP Server as an administrator and launch the program (**Start > Programs > ESP Enterprise > ESP Diagnostics Tool**). The program analyzes the server components and creates a report.
2. For more in-depth information, click the **Full Interface** button. The ESP Diagnostic control panel is displayed. This window has tabs corresponding to the categories of server diagnostics, including **Services** and **Web Reports.**



Note that if you have not yet installed the Agent, a warning light will appear. It will register green as soon as you install the Agent.

3. The **Services** tab shows you if the database and gathering services are properly installed and running.



If a red light is glowing next to an item, it indicates a failure of that component. You must address the stated problem before you can be sure that the ESP Server is functioning properly. Similarly, there is a tab to diagnose the **Web Reports** Server.

4. To find out more information, click the question mark button to the right of any item. These buttons link to knowledge-base articles at the Trend Micro support site.
5. If all the buttons are glowing green, click **Close** to exit the Diagnostic**.**

Note:	If the ESP Server computer is a member of a domain, but you are logged in as a local user, the ESP Diagnostics Tool will sometimes improperly report that permissions are incorrect. If you see your permissions tests are incorrectly failing, you can safely ignore the diagnostics warnings.

Understanding the ESP Server Components

The ESP Server is now successfully installed. It will respond to messages and requests from the ESP Relay, Agent and Console computers using a variety of components. To better understand what the ESP Server does, here is a list of some of the components along with a short description:

- **Agent Registration Component.** When the ESP Agent is installed on a new computer, it registers itself with the client registration component of the ESP Server and the ESP Agent is given a unique ID. If the computer's IP address changes, the ESP Agent will automatically register the new IP address with the client registration component.
- **Post Results Server Component.** When an ESP Agent detects that a Fixlet has become relevant, it reports to the Post Results server component using an HTTP POST operation. It identifies the relevant Fixlet along with the registered ID of the ESP Agent computer. This information is passed on to the ESP database through the FillDB service and then becomes viewable in the ESP Console. Also, other state changes are periodically reported by the clients to the server directly or through ESP Relays.
- **Gather Server Component.** This component watches for changes in Fixlet content for all the Fixlet sites to which ESP is subscribed. It downloads these changes to the ESP Server and makes them available to the GatherDB Component.
- **FillDB Component.** This component posts ESP Agent results into the database.
- **GatherDB Component.** This component gathers and stores Fixlet downloads from the Internet into the database.
- **Download Mirror Server Component.** The Download Mirror Server Component hosts Fixlet site data for the ESP Relays and ESP Agents. This component functions as a simplified download server for ESP traffic.

Installing the ESP Console

The ESP Console lets the operator monitor and fix problems on all managed computers across the network. It can be installed on any computer that can make a network connection via ODBC port **1433** to the ESP Server. Except in testing or evaluation environments, it is not a good idea to run the ESP Console on the ESP Server computer itself due to the performance and security implications of having the publisher key credentials on a computer that is running a database and/or web server.

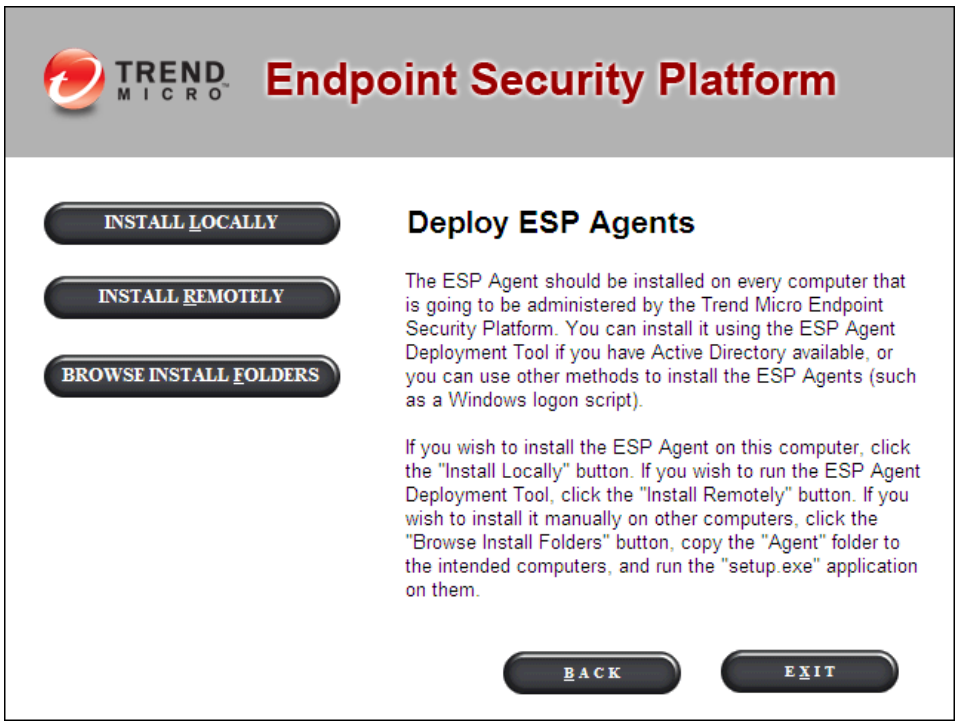
To install the ESP Console, follow these steps:

1. Run the ESP Installation Guide (Start > Programs > ESP Enterprise > ESP Installation Guide). Click the button labeled Install ESP Components.
2. From the next screen, click **Install ESP Console**.
3. After a welcome screen, you will see the ESP Console license agreement. After reading the agreement, click **Yes** to accept the terms and continue the installation.
4. From the **Select Features** dialog, you can select specific features to install. Typically, however, you will accept the default settings. Click **Next**.
5. The next screen prompts you for an installation location for the ESP Console. The default location is C:\Program Files\ESP Enterprise\ESP Console. To choose another destination, click **Browse** and navigate to the desired location. Click **Next** to continue.
6. After the files are installed, click **Finish** to complete the installation. At this point, you can choose to launch the ESP Console, or continue to the next section to install the ESP Agents.

See the ***ESP Console Users Guide*** for more details on using the Console program.

Installing the ESP Agents

The ESP Agent should be installed on every computer in your network that you want to administer with ESP – including those computers running the ESP Server and the ESP Console. That allows those computers to receive important Fixlet messages (like security patches, configuration files or ESP upgrades).
If you are running the ESP Installer, you can select **Install ESP Components > Install ESP Agents > Install Locally**, which will install the Agent on your local machine in the directory you specify.



There are several different techniques for installing the ESP Agent on remote computers, including the **ESP Agent Deploy Tool**, login scripts, third-party utilities and manual installation. Once the ESP Agents are installed, upgrades and other maintenance tasks can be automated with Fixlet messages.

Using the ESP Agent Deploy Tool

On smaller networks (less than about 5,000 computers) connected to Active Directory or NT Directory domains, you can use the ESP Agent Deploy Tool to install Windows ESP Agents. For larger networks, you may find it easier to use other deployment methods. This is an easy way to roll out clients, but there are some requirements and conditions:

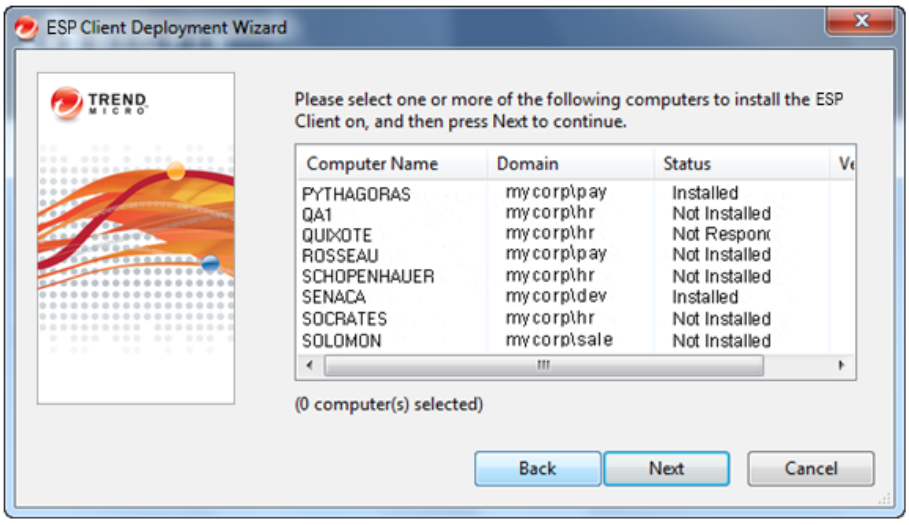
- You must have an Active Directory or NT Directory domain (there is also an option to deploy to a list of computers if you have an administrator account on the computer).
- The ESP Agent Deploy Tool can only target computers running Windows 2000, XP, Server 2003, Vista, Server 2008, 7, or Server 2008 R2.

- The computer running the ESP Agent Deploy Tool must be connected to the domain, but should not be the domain controller itself.
- The Service Control Manager (SCM) and the Remote Procedural Call (RPC) services must be running on the target machines.
- There must be no security policy on the computer that would prevent either a remote connection to the SCM or the issuance of a Remote Procedural Call.
- The dnsName property of every target computer in the Active Directory must be properly defined.

The Agent Deploy Tool is designed to make it easier to push the ESP Agent to computers, but is not a full-featured enterprise-class software distribution tool. If you already have a software distribution tool, it is recommended that you use the existing software distribution tool instead.
The ESP Agent Deploy Tool starts by getting a list of computers from the Active Directory server and remotely connecting to the computers (accessing 100 computers at a time) to see if the ESP Agent service is already installed on each computer. If so, it reports **Installed** along with the status of the ESP Agent service such as **Running**, **Stopped**, etc. If it cannot determine the status due to a permissions problem or for any other reason, it will report **Status Unknown**. Otherwise it reports **Not Installed** – unless it cannot communicate with the computer at all, in which case it reports **Not Responding**. If the ESP Agent is not yet installed, the tool provides interfaces that allow you to issue a Remote Procedural Call that accesses the shared installer and – with the proper domain administration credentials – runs it silently, with no end user interaction. Here is how to use the tool:

1. The ESP Agent Deploy Tool is created by the ESP Installation Generator. You can launch the tool from the ESP Installation Guide (click the **Install ESP Components > Install ESP Agents > Install Remotely** button) or launch it directly from **Start > Programs >ESP Enterprise > ESP Agent Deploy**.
2. The resulting dialog offers three ways to deploy the ESP Agents:
   - **Find computers using Active Directory**. The ESP Agent Deploy tool contacts the Active Directory server to get a list of all of the computers in the domain. It checks each of the computers to see if the ESP Agent is already installed and displays this information in a list.
   - **Find computers using NT 4.0 Domains**. All the computers in the domain are listed with a status flag indicating whether the ESP Agent has been installed or not.
   - **Find computers specified in a list**. Based on how your network resolves computer addresses, you will need to provide a list of computer names, IP address ranges, or hostnames. The list must have one name / IP address range / hostname per line. Using this option, the ESP Agent Deploy Tool will not attempt to discover any computers, but instead will attempt to install directly to all the listed computers.
3. Type in a **username** and **password** that has administrative access to the desired computers. In most cases, this is a domain administrator account. If you are using

the computer list option, you can specify a local account on the remote computers (such as the local administrator account) that have administrative privileges. The rest of the client deployment process will use this username/password, so if the account does not have the appropriate access on the remote computers, you will receive access denied errors.



4. When the list of computers is displayed, shift- and control-click to select the computers you want to administer with ESP. Click **Next.**
5. You will see a list of the computers you have selected. The default options are usually sufficient, but you may want to select **Advanced Options** to configure the following installation parameters:
   - **File Transfer:** You can elect to **push** the files out to the remote server for installation or to have the files **pulled** from the local computer. Unless there are security policies in place to prevent it, for most cases pushing the files to the remote computer works best.
   - **Connection Method:** There are two ways to connect to the remote computers. Using the **Service Control Manager** (SCM) is recommended, but you may also use the **task scheduler** if the SCM does not work.
   - **Installation Path:** Specify a path for the Agent, or accept the default (recommended).
   - **Verification:** Check this box to verify that the ESP Agent service is running after waiting for the installation to finish, which will allow you to know if the installation completed successfully.
   - **Custom Setting:** Add an ESP Custom Setting to each ESP Agent deployed, in the form of a Name / Value pair.

6. To begin the installation, click **Start**.
7. When completed, a log of successes and failures is displayed. Simply retrying can resolve some failures; use advanced options if that does not work. For more information, see the article on Agent deployment at the Trend Micro support site.

Installing the ESP Agent Manually

The ESP Agent can always be installed by manually running the ESP Agent installer on each computer. This is a quick and effective mechanism for installing the ESP Agent on a small number of computers.

1. There are at least two ways to install the client:
   - Log on to the desired computer with administrator privileges and copy the **ESP Installers\Agent** folder from the ESP installation computer to the local hard drive.
   - Or run the ESP Installation Guide (available at **Start > Programs > ESP Enterprise > ESP Installation Guide**) and click the button marked **Browse Install Folders**. It opens the **ESP Installers** folder and displays the **Agent** folder.
2. Once you have copied the Agent folder to the target computer, double-click on **setup.exe** from that folder to launch the installer.
3. After the welcome screen, you will be prompted for a location to install the software. You may accept the default, or click **Browse** to select a different location.
4. After the files have been moved, click **Done** to exit the installer. The ESP Agent application is now installed and it will automatically begin working in the background.
5. Repeat this process on every computer in your network that you want to place under ESP administration.

Installing the ESP Agent with MSI

You can use the Microsoft Installer (MSI) version of the ESP Agent to interpret the package and perform the installation automatically. This MSI version of the client (BESClientMSI.msi) is stored in the BESInstallers\ClientMSI folder. You can run this program directly to install the client or you can call it with arguments. Here are some sample commands, assuming that the MSI version of the Client is in the C:\Program Files\BigFix Enterprise\BES Installers\ClientMSI folder:

- msiexec.exe /i c:\BESInstallers\ClientMSI\BESClientMSI.msi/qn
  The \qn command performs a silent install.
- msiexec.exe /i c:\BESInstallers\ClientMSI\BESClientMSI.msi INSTALLDIR="c:\myclient"
  This command will install the program to the given directory.

You can find the full list of installation options at the Microsoft site: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/command_line_options.asp.
With the MSI version of the client installer, you can create a Group Policy Object (GPO) for BESClientMSI deployments. For more information on Group Policies, see the Microsoft knowledge base article: http://support.microsoft.com/kb/887405.

Using Software Distribution Tools

If you have access to a software distribution tool such as Microsoft SMS, IBM's Tivoli, CA Unicenter, or Novell's ZENworks, and all the intended computers have the tool enabled, you can use the tool to deploy an installation package for the ESP Agent. **This is the most effective way to deploy to an enterprise because the infrastructure and deployment procedure is already in place**.

Using Group Policies

It is possible, using Active Directory Group Policy Objects (GPO), to define a policy insisting that the ESP Agent should be installed on every machine in a particular group (Organizational Unit, Domain, etc.). This policy is applied every time a user logs into the specified domain, making it a very effective way to deploy the client if GPO is enabled. Consult your Active Directory administrator for more details.

Using Login Scripts

In an NT or AD domain, login scripts can be written that check for the presence of the ESP Agent. When the computer logs in and finds the ESP Agent missing, it can automatically access the ESP Agent installer from a specified location on a global file share. The Trend Micro support site has a knowledge-base article with a sample login script (Keywords: example login script) and instructions on how to use login scripts to install the ESP Agent.

If your network will be adding new computers from time-to-time, this approach can be very convenient, ensuring that the ESP Server will discover and manage new machines automatically. However, in some networks using Windows 2000 or XP, users must log in with administrator privileges for this technique to work.

These scripts pass arguments to the Windows Installer based setup. For more information about command line options for setup.exe, please refer to InstallShield's support web site at http://kb.flexerasoftware.com/doc/Helpnet/isxhelp12/IHelpSetup_EXECmdLine.htm. Here are some examples of command line switches for the ESP Agent installer that can be used in a login script:

- To install the ESP Agent silently while writing a log to the C:\, execute a DOS command of the form:

  ```
  setup.exe /s /v/l*voicewarmup
  \"C:\besclientinstall.log\" SETUPEXE=1 /qn”
  ```

- To change the default installation location, the appropriate form of the command is:

  ```
  setup.exe /s /v/l*voicewarmup
  \"C:\besclientinstall.log\"
  INSTALLDIR=\”<InstallPath\” SETUPEXE=1 /qn”
  ```


Where <InstallPath> is the full windows path to the folder where the ESP Agent should be installed.

Note: The Windows user running setup.exe must have Administrative privileges on the computer and must be able to write a log file to the same folder that contains the "setup.exe" file, otherwise the installation will fail and a log file will not be created.

Embedding in a Common Build

If your organization employs a specific build image or common operating environment (COE) on a CD or image that is used to prepare new computers, you can include the ESP Agent in this build. To create the image, follow these directions:

For Windows

1. Install the ESP Agent on the computer to be imaged.
2. The ESP Agent will immediately attempt to connect to the ESP Server. If it successfully connects to the ESP Server, it will be assigned a **ComputerID**. This ComputerID is unique to that particular computer, so it should ***not*** be part of a common build image. The next steps will delete this ID.
3. Open the Windows services dialog and stop the **ESP Agent service**.
4. Open the registry to **HKLM\Software\BigFix\EnterpriseClient\GlobalOptions** and delete the values ComputerID, RegCount, and ReportSequenceNumber.
5. The ESP Agent is now ready to be imaged.

Note: If the ESP Agent is started again for any reason (*including a system restart*), it will re-register with the server and **you will need to perform steps 3-4 again.** The ESP Server has built-in conflict detection and resolution so if for any reason you fail to delete the ID, the ESP Server will notice that there are multiple ESP Agents with the same ComputerID and force the ESP Agent to re-register and everything will work normally. However, we do recommend you perform the steps above to avoid having a grayed-out ESP Agent (the first imaged computer) in the computer list in the ESP Console.

For Macintosh and Linux

1. Let the client register.
2. Stop the ESP Agent in the approved way, using **sudo systemstarter stop BESClient.exe**.
3. If they exist, remove **RegCount**, **ReportSequenceNumber**, and **ComputerID** from the client preferences folder: /Library/Preferences/com.bigfix.besagent.plist. (On Linux systems edit the .config file in this location).
4. Delete the __BESData folder. The default location is \Library\Application Support\BigFix\BES Client.
5. The ESP Agent is now ready to be imaged.

Note: If the ESP Agent is started again for any reason (*including a system restart*), it will re-register with the server and **you will need to perform steps 2-4 again.** On a Windows system, the data in the folder simply overwrites the old install. On Unix systems, however, the ESPData folder acts as a registry and must be deleted before imaging.

Using Email

You can send users an e-mail containing a URL and asking them to use it to install the ESP Agent when they log in to the network. This is an effective technique for Win9x computers since there are no limitations on user rights on those platforms. However, where administrative rights are enforced, this method requires users to log in with administrator privileges.

Enabling Encryption on ESP Agents

Once installed, you can set up your ESP Agents to encrypt all outgoing reports to protect data such as credit card numbers, passwords and other sensitive information.

> **Note:** You must have encryption enabled for your ESP deployment before enabling it for your Agents. In particular, for the required option, your clients will go silent if you enable them without first setting up your deployment.

To enable encryption, follow these steps:

1. From the **ESP Management** Domain, open the **Computer Management** folder and click the **Computers** node.
2. Select the computer or set of computers that you want to employ encryption.
3. From the right-click context menu, select **Edit Computer Settings**.
4. From the **Edit Settings** dialog, click **Add**.
5. In the **Add Custom Setting** dialog, enter the setting name as

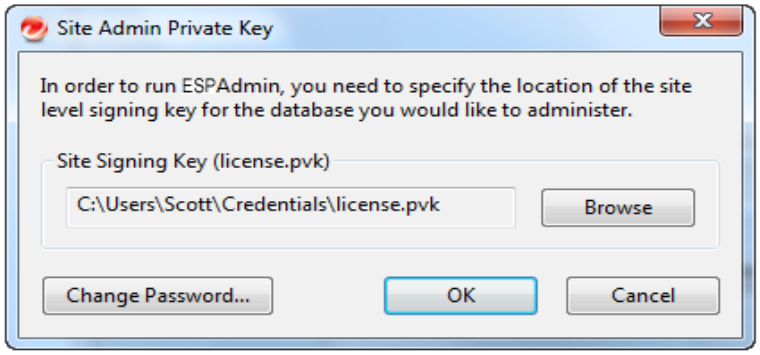
   _ESPClient_Report_Encryption (note the double underline starting the name).

   There are three possible values for this setting:
   - **required:** causes the ESP Agent to always encrypt. In the event that there is no encryption certificate available in the masthead or if the target computer (ESP Relay or Server) cannot accept encryption, the ESP Agent will not send reports.
   - **optional:** the ESP Agent encrypts if it is able, otherwise it sends its reports in clear-text.
   - **none:** No encryption will be done, even if an encryption certificate is present. This allows you to turn off encryption after you enable it.

6. Click **OK** to accept the value and **OK** again to complete the setting. You will need to enter your private key password to deploy the setting action.

Running the ESP Administration Tool

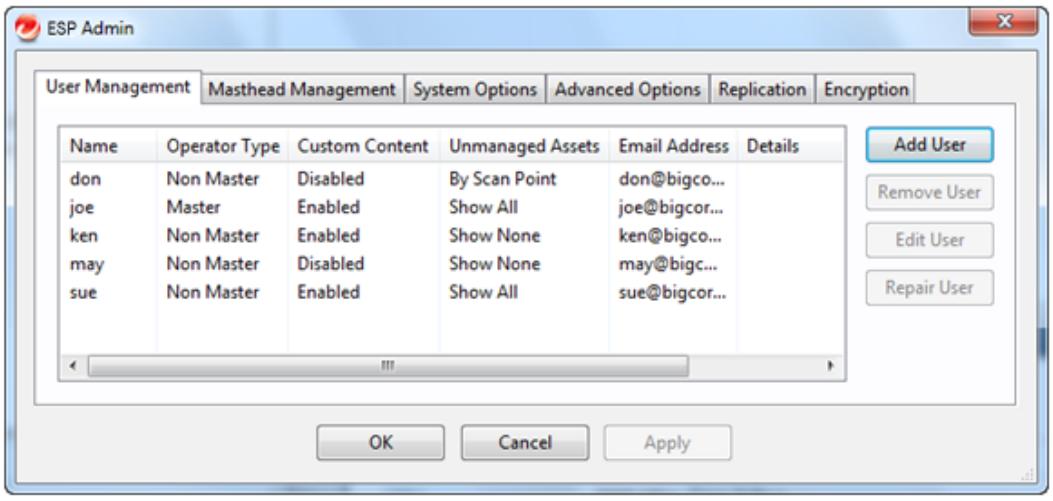
The Installer automatically creates the ESP Administration Tool (also called ESP Admin), when it installs the other components of the Console program. This program operates independently of the ESP Console and is intended for Administrative Operators only. You can find it from the Start menu: **Start > All Programs > ESP Enterprise > ESP Administration Tool.** To run the program, you must first browse to the signing key (license.pvk):



Note that you can also change your administrative password through this interface. Once you have selected the signing license, click OK to continue. You will need to supply your private key password to proceed.

User Management

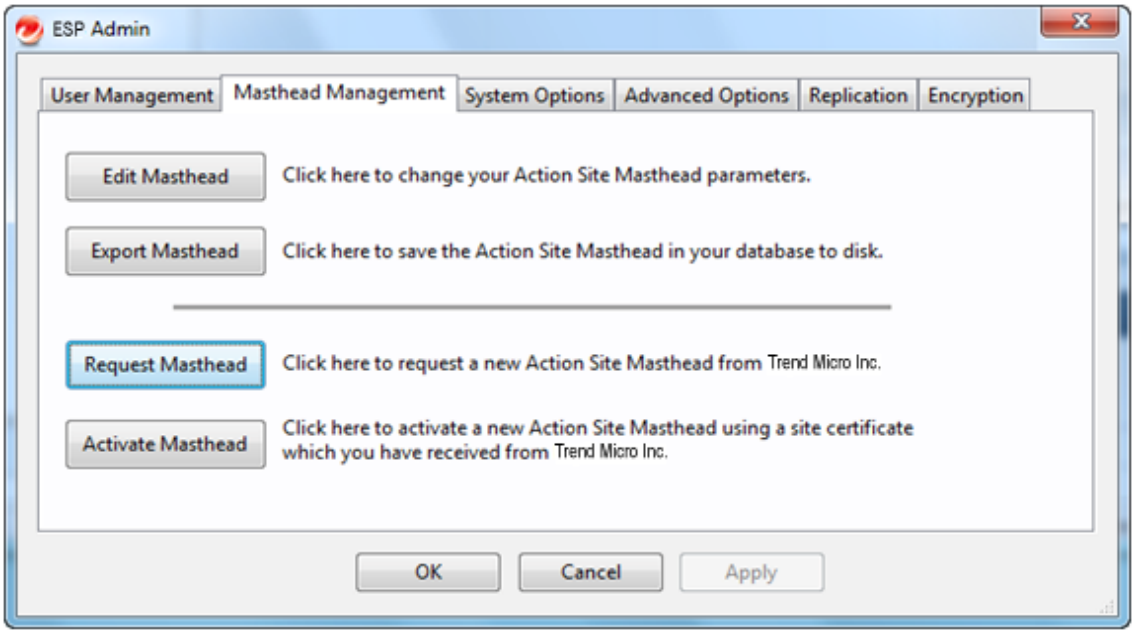
If this is the first time you have run the program, the Administration Tool will provide you with a blank slate of users. Click **Add User** to include new ESP Operators. This is where you will return when you want to add, remove or edit the management rights of your users.



You can find out more about how to assign management rights in the section titled **Adding New Operators and Master Operators** (page 82).

Masthead Management

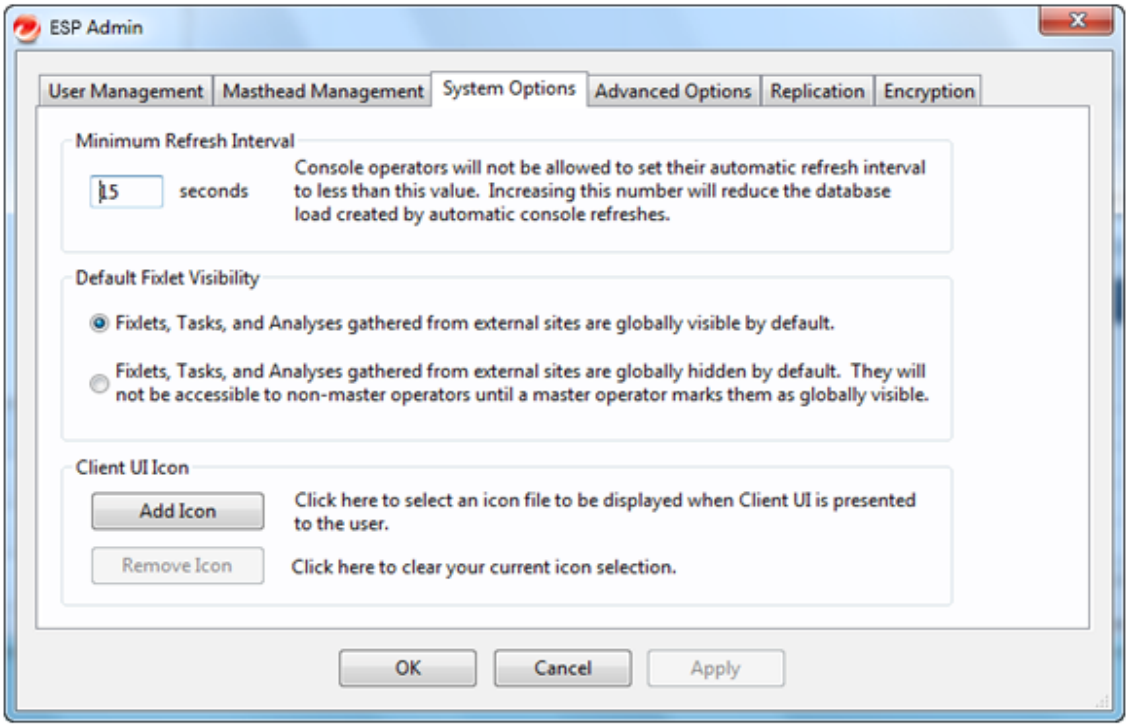
Click the second tab to view the **Masthead Management** dialog.



If you don't yet have a masthead, which is required to run the ESP Console, this dialog provides an interface to **Request** and subsequently **Activate** a new masthead. If you have an existing masthead, you can edit it to change gathering intervals and locking. For more information on managing your masthead, see the section named **Editing the Masthead** (page 91). You can also export your masthead, which can be useful if you want to extend your ESP network to other servers.

System Options

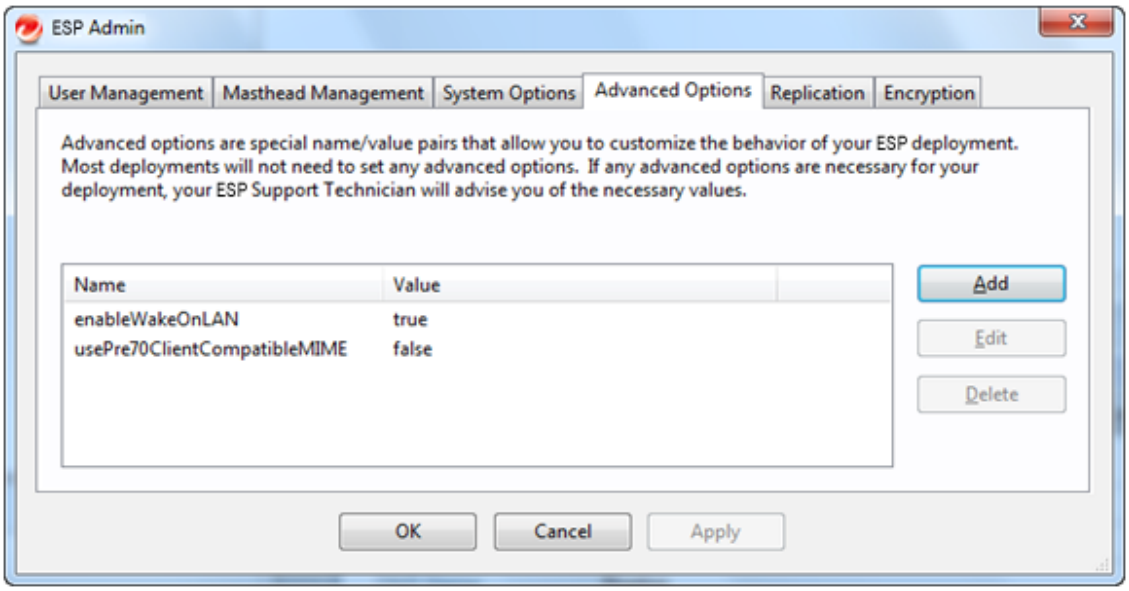
The third tab opens the **System Options** dialog. The first option sets a baseline minimum for refresh intervals. This refers to the Fixlet list refresh period specified in the Preferences dialog of the ESP Console. The default period is 15 seconds, but if you feel that your network can handle the bandwidth, you can lower this number to make the Console more responsive. Conversely, if your network is strained, you may want to increase this minimum.



This dialog also lets you set the default visibility of external sites. These are, by default, globally visible to all Console operators. To give you extra control, you can set the visibility to hidden, and then adjust them individually through the Console. You must be an administrator or a master operator to make these hidden sites become visible.
This dialog also lets you add your own logo to any content that is presented to the user through the ESP Agent. Branding can be important to reassure your users that the information has corporate approval.

Advanced Options

The fourth tab opens the **Advanced Options** dialog. This dialog lists any global settings that apply to your particular ESP installation.



These options are name/value pairs, and are typically supplied by your ESP Support Technician. As an example, if you are subscribed to the Power Management site, one of these options would allow you to enable the WakeOnLAN functionality.

Replication

The fifth tab opens the **Replication** dialog. This dialog helps you to visualize your replication servers. For more information, see the section titled **Managing Replication** (page 72).

Encryption

The final tab opens the **Encryption** dialog. This dialog allows you to generate a new encryption key or to disable encryption altogether. For more information, see the section titled **Managing Agent Encryption** (page 85).

Understanding Operator Rights

ESP Console users, also known as publishers or operators, can be in charge of flexibly defined groups of computers with varying degrees of freedom. As the Site Administrator, you are in charge of each operator's domain and the specific rights they have over that domain. You can manage your team of operators and administrators by using the **ESP Administration Tool**. This program is usually found in the start menu, under **Programs > ESP Enterprise > ESP Administration Tool**.

There are three basic classes of users: Site Administrators, Master Operators and ordinary (Non-Master) Operators. They each have different responsibilities and restrictions, described below.

Site Administrators

As a Site Administrator, you are the caretaker of the site-level key. This is a special key and should only be used for site-level tasks, and never for ESP Console operations. For day-to-day operations, you must create a Master Operator key. Only use your Site Administrator key when performing top-level management tasks, including the following:

- **Creating/Modifying/Deleting** Users with the ESP Administration Tool.
- **Setting global system options** including the Minimum Refresh Interval, Default Fixlet Visibility, and the Agent UI Icon with the ESP Administration Tool.
- **Editing Mastheads.**
- **Administering Distributed Server Architecture** (DSA) configurations. This includes setting the replication rate and the linkage between Replication Servers.

Master Operators

Master Operators can perform all of the functions of ordinary operators. In addition, they can also:

- **Edit the management rights** settings for other operators. This allows you to divide up the computers on your network among various operators so they each see a smaller subset of client computers.
- **Create new computer settings**, which monitor and control ESP Agent behavior and hold various labeled values for filtering. For more information, see the article on configuring BigFix settings at the support site.
- **Create or edit global retrieved properties**, which are used to filter and sort computers and can be used to create reports.
- View all unmanaged assets.
- Change the ESP Agent heartbeat, to optimize ESP performance.
- Subscribe or unsubscribe from Fixlet sites.

- Create new custom Fixlet sites.
- **Designate operators** to be custom site owners, writers and readers.
- **Globally hide or unhide** Fixlet messages.
- **Audit all Actions** taken in the ESP Console.
- Manage External Fixlet Site subscriptions.

Operators

Ordinary operators can perform various management functions on computers under their control depending on the management rights that are delegated to them by master operators. They can:

- **Deploy Actions.**
- **Create custom content**, including Fixlet messages, Tasks, Baselines and Analyses. The Site Administrator can grant or revoke this right from the ESP Administration Tool.
- **Change or delete computer settings**, which monitor and control ESP Agent behavior and hold various labeled values that can be used for sorting and filtering.
- **View unmanaged assets** according to each Operator's scope (as defined by Scan Points). The Site Administrator can grant or revoke this right from the ESP Administration Tool.
- **Be custom site owners**, writers, and readers if granted the privilege by Master Operators.

Operators and Analyses

Operators have various rights and restrictions when it comes to activating and deactivating analyses:

- Ordinary operators cannot deactivate an analysis activated by other operators on computers they administer.
- Master Operators cannot directly activate custom analyses authored by ordinary operators. They can, however, make a copy of an analysis and activate the copy.

This chart summarizes the privileges and abilities of both types of Console Operator:

User Privileges	Master Operator	Operator
Initialize Action Site	Yes	No
Manage Fixlet Sites	Yes	No
Change ESP Agent heartbeats	Yes	No
Create Fixlets	Requires Custom Authoring	Requires Custom Authoring
Create Tasks	Requires Custom Authoring	Requires Custom Authoring
Create Analyses	Requires Custom Authoring	Requires Custom Authoring
Create Baselines	Requires Custom Authoring	Requires Custom Authoring
Create Groups	Yes	Manual Groups Only
Activate/Deactivate Analyses	All	Administered
Take Fixlet/Task/Baseline Action	All	Administered
Take Custom Action	Requires Custom Authoring	Requires Custom Authoring
Stop/Start Actions	All	Administered
Manage Administrative Rights	Yes	No
Manage Global Retrieved Properties	Yes	No
View Fixlets	All	Administered
View Tasks	All	Administered
View Analyses	All	Administered
View Computers	All	Administered
View Baselines	All	Administered
View Computer Groups	All	Administered
View Unmanaged Assets	Administered by ESP Admin	Administered by ESP Admin
View Actions	All	Administered
Make Comments	All	Administered
View Comments	All	Administered
Globally Hide/Unhide	Yes	No
Locally Hide/Unhide	Yes	Yes
Use Wizards	Requires Custom Authoring	Requires Custom Authoring
Remove computer from database	All	Administered
Create Manual Computer Groups	Yes	Yes
Delete Manual Computer Groups	Yes	No
Create Automatic Computer Groups	Yes	Requires Custom Authoring
Delete Automatic Computer Groups	Yes	Requires Custom Authoring and Administered
Create Custom Site	Yes	No
Modify Custom Site Owners	Yes	No
Modify Custom Site Readers/Writers	Yes	Site Owners

Administered: The operator must own or have permissions

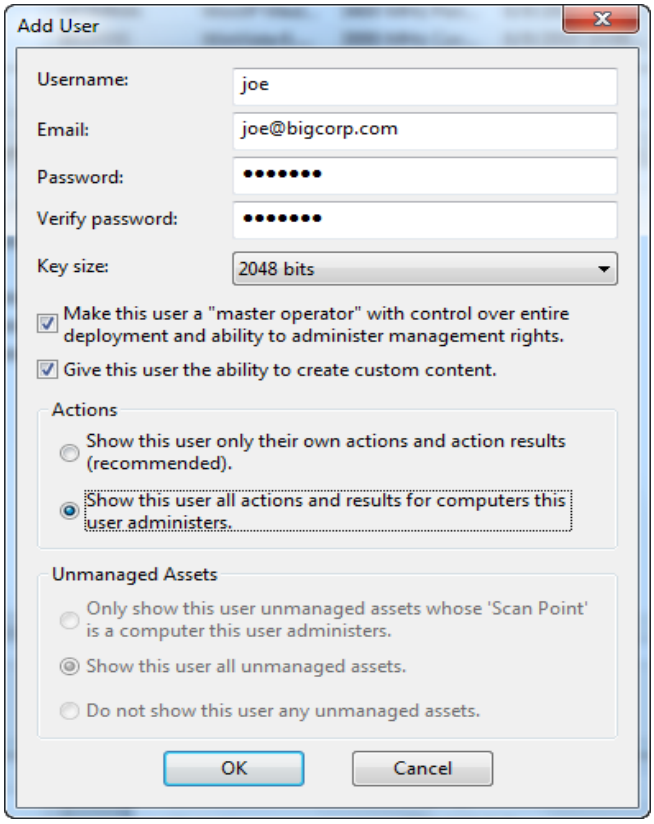
Requires Custom Authoring: Granted by the Site Administrator through ESP Admin

Administered by ESP Admin: Granted by the Site Administrator through ESP Admin

Adding ESP Console Operators

As the ESP Site Administrator, you must create accounts for each new ESP Console operator, allowing them to view the database using the ESP Console. For security purposes, a password-protected public/private key is also generated so the new operator can properly create and sign actions. To add a new operator, use the ESP Administration Tool.

1. When you install the ESP Server, the ESP Admin Tool is automatically run so you can add new operators. However, you may add operators at any time by launching **Start > Programs > ESP Enterprise > ESP Administration Tool**.
2. If not already displayed, browse to your **site signing key** (license.pvk) and select it. Click **OK**.
3. Click the **User Management** tab. Click **Add User** to start adding new ESP Console operators with publishing credentials. For each operator/publisher you add, you will fill out data in the **Add Publisher** dialog:



4. Enter the **Username** and **Email** address of the person you want to designate as a publisher, or operator. Start with yourself, making sure you grant yourself management rights.
5. Create a **Password** and retype it for confirmation. Once you hand the keys over to your operators, they can change their passwords if they wish.
6. Enter a **Private Key Length** from the pull-down menu, or accept the default.
7. Check the first box if you want this operator to **administer management rights**, making them a Master Operator. As the ESP administrator, you should check this box when you add yourself to the user list.

8. Check the second box if you want this operator to be able to **create custom content** such as custom Fixlet messages, Tasks and Baselines. The availability of this feature depends on the license granted you by Trend Micro, Inc. By default, operators only see actions and action results for actions that they have issued. This is recommended for better Console performance. However, you can also choose to have the operator see all actions and action results that were taken against computers that the operator administers.

   WARNING!

   Custom actions grant the user the ability to create and deploy custom actions to any computer the operator manages with just a few mouse clicks. Use good judgment when granting these rights to operators.

   .

9. At this point, you can also grant rights to view **unmanaged assets**. You can grant all-or-none access, or limit users to their personal Scan Point scope. Make note of this operator and password in a safe place and then click **OK**.
10. A dialog will appear prompting you to choose a location in which to create a new folder that will contain the operator's credentials. You will need to choose both the parent folder and the name for the new folder, which will default to the operator's name. Consider using a removable disk for additional security. You will hand this folder, along with the password, to the designated ESP Console operator.
11. ESP will ask you for the **Site Admin Private Key Password** (this is the password you created when you first installed ESP) to authenticate you as the ESP Site Administrator. Type it in and click **OK**. Note that you will have opportunities later to change this password.
12. Repeat this process for each operator you wish to authorize as an ESP Console operator. These operators will then have a personal folder that acts as their key to the ESP Console. They should take care to protect the disk containing this folder, which holds the following files:
    - **publisher.pv**k: the private key created for each authorized operator/publisher. As with the key to the front door, the operator must understand the responsibility of caring for this file.
    - **publisher.crt:** the signed certificate authorizing each operator/publisher to issue actions. This file is also stored in the database.

13. Once you have granted publishing rights to all your designated ESP Console operators, click **APPLY** and provide your site level password again.
14. The ESP Administration Tool must propagate the action site – with the new operator information – throughout your network. Click **Yes** to send the updated user information to all the ESP Agents. At any time, you can add new authorized operators by running the ESP Administration Tool again.

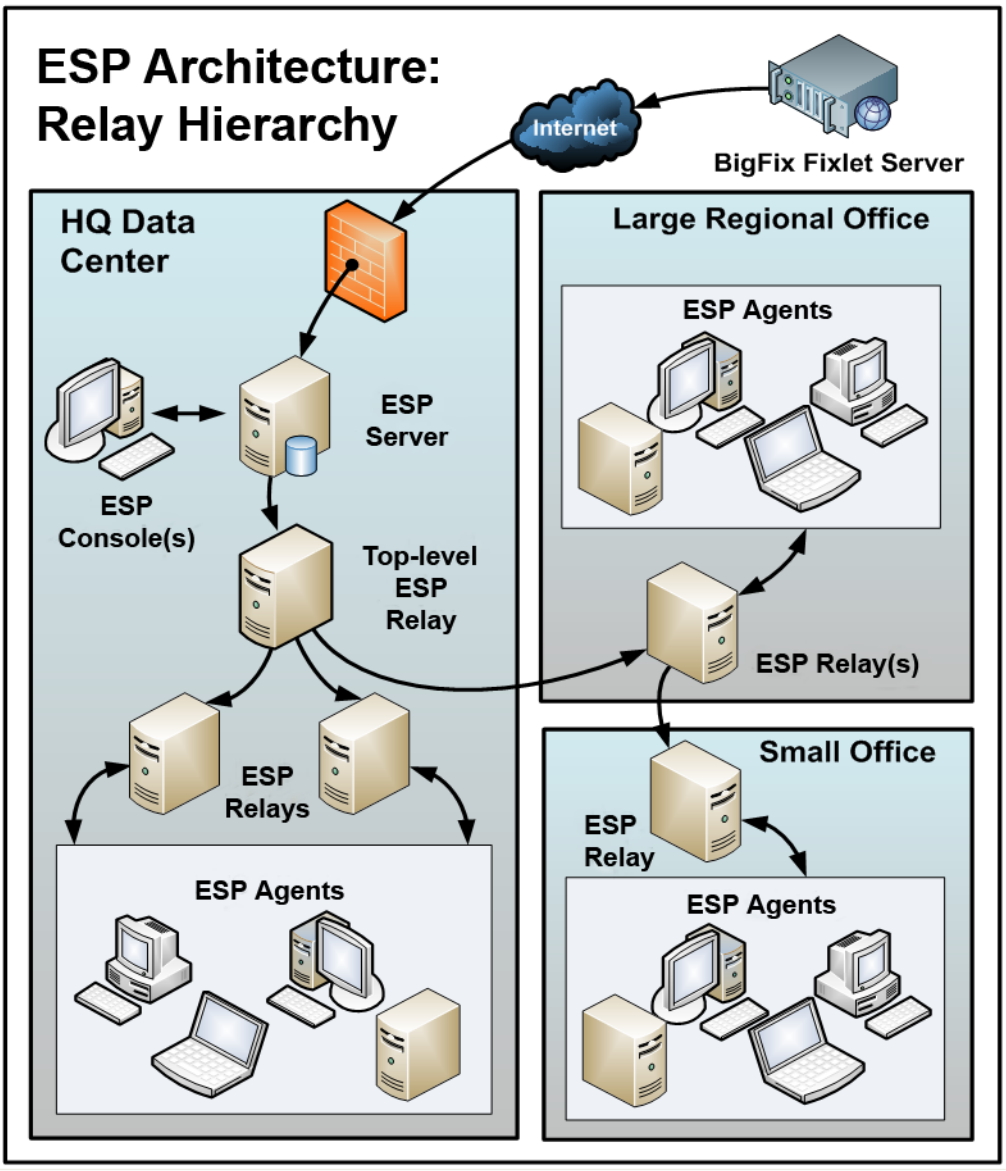
Notes on Operators:

- You should propagate the action site whenever you change any operator information, especially when you revoke operators.
- If two operators were created prior to ESP Version 7.0 with the same email address, their signing certificates may conflict with each other and they will not be able to use the custom site functionality until one of them is deleted and reissued. Such users will be highlighted in red in ESP Admin – clicking on **repair** will pop up a message box explaining the problem.
- A user's status as Operator or Master Operator is permanently associated with the username and cannot be changed.
- To be on the safe side, Site Administrators would be wise to create users with a default password and store a backup copy of the console key files with those default passwords. Console operators who forget their password can be provided with the saved copy.

Part Three

Configuring the ESP Components

Now that the ESP components have been installed, you can configure your system for greater efficiency or to support larger or non-standard deployments.
The picture below represents a large and fairly complex deployment of ESP. Study the picture to understand how the system communicates. In particular, notice that all information flows into the ESP Server in the HQ/Data Center, that there are multiple levels of ESP Relays, and that all communications flow through the relay chain back to the server.



Using ESP Relays

ESP Relays can significantly improve the performance of your ESP installation. ESP Relays are designed to lighten both upstream and downstream burdens on the ESP Server. Rather than communicating directly with an ESP Server, ESP Agents can instead be instructed to communicate with designated ESP Relays, considerably reducing both server load and client/server network traffic. ESP Relays work by:

- **Relieving Downstream Traffic**. The ESP Server has many duties, one of the most taxing of which is distributing files, such as patches or software packages, and Fixlet messages to the ESP Agents. ESP Relays can be set up to ease this burden, so that the ESP Server does not need to distribute the same file to every ESP Agent. Instead, the file is sent once to the ESP Relay, which in turn distributes it to the ESP Agents. In this model, the ESP Agent connects directly to the ESP Relay and does not need to connect to the ESP Server.
- **Reducing Upstream Traffic**. In the upstream direction, ESP Relays can compress and package data (including Fixlet relevance, action status and retrieved properties) from the ESP Agents for even greater efficiencies.
- **Reducing Congestion on Low-Bandwidth Connections**. If you have an ESP Server communicating with computers in a remote office over a slow connection, designate one of those computers as an ESP Relay. Then, instead of sending patches over the slow connection to every ESP Agent independently, the ESP Server only sends a single copy to the ESP Relay (if it needs it). That ESP Relay, in turn, distributes the file to the other computers in the remote office over its own fast LAN. This effectively removes the slow connection bottleneck for remote groups on your network.
- **Reducing the Load on the ESP Server**. The ESP Server has many duties including handling connections from ESP Agents and ESP Relays. At any given instant, the ESP Server is limited in how many connections it can effectively service. ESP Relays, however, can buffer multiple ESP Agents and upload the compressed results to the ESP Server. ESP Relays also distribute downloads to individual ESP Agents, further reducing the workload of the ESP Server and allowing ESP to operate faster and more efficiently.

ESP Relays are an absolute requirement for any network with slow links or more than a few thousand ESP Agents. Even with only a few hundred ESP Agents, ESP Relays are recommended: they make downloads faster by distributing the load to several computers rather than being constricted by the physical bandwidth of the ESP Server. ESP is quite powerful; it is easy to deploy an action causing hundreds of thousands of ESP Agents to download very large files all at once. Windows XP SP2 alone is more than 200MB and it is not uncommon to distribute software packages that are gigabytes in size. Without ESP Relays, even network pipes as fast as T1 (or faster) lines can be overwhelmed by many ESP Agents requesting large, simultaneous file downloads. Establishing the appropriate ESP Relay structure is one of the most important aspects of deploying ESP to a large network. When ESP Relays are fully deployed, an action with a

large download can be quickly and easily be sent out to tens of thousands of computers with minimal WAN usage.
In an effort to ease deployment burdens and reduce the total cost of ownership of ESP, the ESP Relays are designed to run on shared servers such as file/print servers, domain controllers, SMS servers, AV distribution servers, etc. As a consequence, a typical ESP installation will have less than 1% of its relays running on dedicated computers.
For the most part, the ESP Relay uses minimal resources and should not have a noticeable impact on the performance of the computer running it (see the next section ESP Relay requirements). The ESP Agents can be set to automatically find their closest ESP Relay. These features allow for significant savings in both hardware and administrative overhead.

Note: If the connection between an ESP Relay and ESP Server is unusually slow, it may be beneficial to connect the ESP Relay directly to the Internet for downloads. More information about ESP Relay can be found by visiting the Trend Micro support site, or by talking to your Trend Micro sales engineer or support technician.

ESP Relay requirements

An ESP Relay takes over most of the download duties of the ESP Server. If several ESP Agents simultaneously request files, the ESP Relay may consume a fair amount of bandwidth to serve them up. Generally, however, the duties of the ESP Relay are not too demanding. When many actions are being deployed at once, CPU and disk usage can spike, but typically for only a short duration. The primary resource constraint for the ESP Relay will be disk space.
The requirements for an ESP Relay computer vary widely depending on a number of factors. Here are some requirements for the ESP Relays:

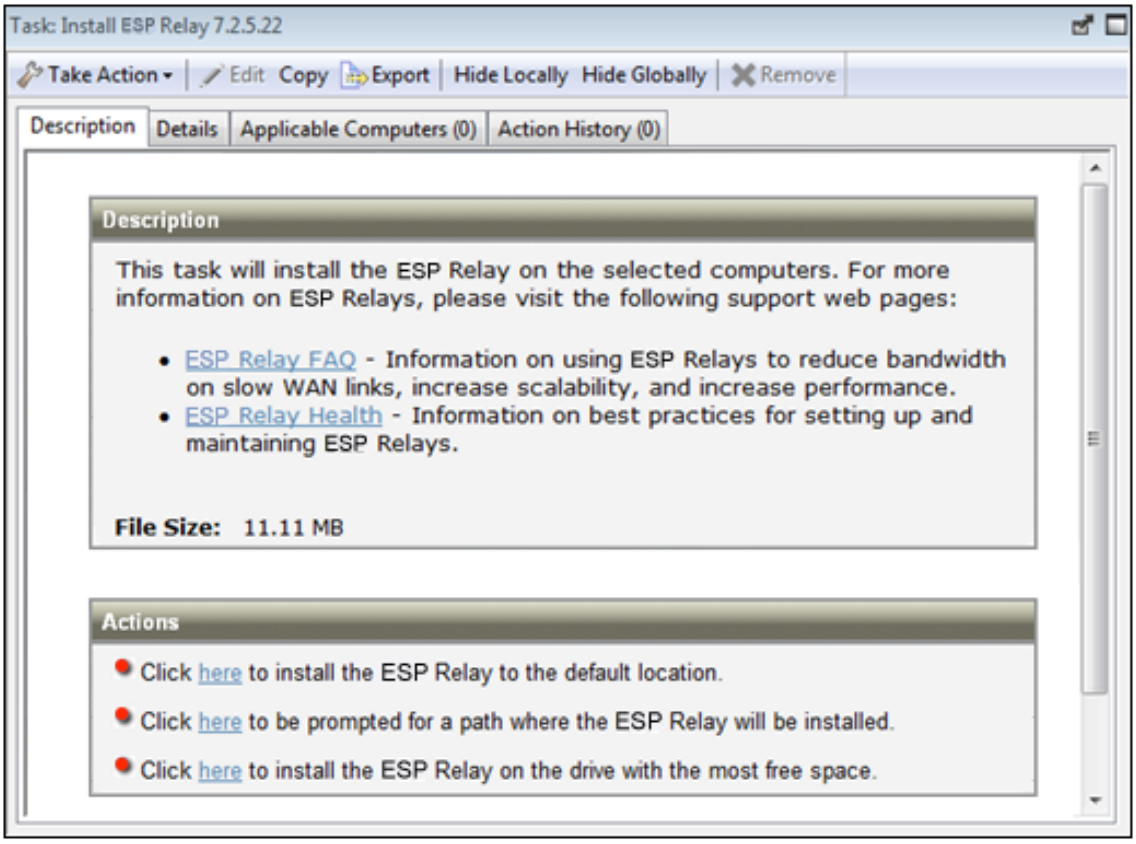
- The ESP Relay must have a two-way TCP connection to its parent (which can be an ESP Server or another ESP Relay).
- The ESP Relay can be installed on an ordinary workstation, but if many ESP Agents simultaneously download files, it may slow the computer down. Also, for the ESP Relay to work properly, the computer must be powered on. That means workstations that are commonly powered off are poor choices for ESP Relays.
- Workgroup file servers, print servers, SMS servers, AntiVirus servers, domain controllers, test servers, and other server-quality computers that are always turned on are good candidates for installing an ESP Relay. ESP Relays were designed to be installed on an existing shared server to reduce the total hardware cost of deploying ESP. Most companies already have partially utilized servers in the appropriate places throughout their networks. Fortunately, should you need to purchase a new computer for the task, the ESP Relay requirements are low. An inexpensive workstation-class computer or bottom-of-the-line server should suffice.
- ESP Relays must be installed on Windows 2000, XP, Server 2003, Vista, Server 2008, 7, Server 2008 R2, Red Hat Enterprise Linux 4/5/6, or Solaris 10 computers.

- Due to the fact that older versions of Internet Explorer used outdated network libraries, the computers running the ESP Relays must have at least Internet Explorer 4.0 or above to work properly.
- More information about ESP Relay can be found at the Trend Micro support site.
- The ESP Relay cache size is configurable but is set to 1GB by default. It is recommended that you have at least 2 GB available for the ESP Relay cache to prevent hard drive bottlenecks.

Designating an ESP Relay

To set up an ESP Relay, you need to designate a Windows 2000, XP, Server 2003, Vista, Server 2008, 7, Server 2008 R2, Red Hat Enterprise Linux 4/5/6, or Solaris 10 computer that is running an ESP Agent to act as the ESP Relay. The ESP Agents on your network will detect the new Relays and automatically connect to them. To create an ESP Relay, use the ESP Console, and follow these steps:

1. In the ESP Console, click the **Tasks** icon in the Navigation treeto bring up a tree/list of all Tasks.
2. Find the Task with the title **Install ESP Relay** (it may include a version number after it). This Task will be relevant as long as there is at least one ESP Agent that meets the requirements for the ESP Relay.



3. Choose your deployment option by choosing one of the actions in the Task. You can target single or multiple computers with this action.

Automatically Discovering Relays

Once you have set up your ESP Relays, you are almost done. If they are configured to perform automatic relay selection, the ESP Agents will automatically find the relay that is the fewest hops away and point to that computer instead of the server. This is the recommended technique, since it dynamically balances your system with minimal administrative overhead. To make sure your ESP Agents are set up to automatically discover relays:

1. Start up the ESP Console and select the **ESP Management** Domain. From the Computer Management folder, click the **Computers** node to bring up a list of ESP Agents in the list panel.
2. Shift- and ctrl-click to select the set of computers you want to automatically detect ESP Relays. Press **Ctrl-A** to select the entire set of ESP Agents.
3. Right-click on this highlighted set and choose **Edit Computer Settings** from the pop-up menu. Depending on whether you selected one or more computers, the dialog boxes are slightly different. Typically, you will have selected all the ESP Agents in your network, so you will see the multiple-select dialog.
4. Check the box marked **ESP Relay Selection Method**.
5. Click the button marked **Automatically Locate Best ESP Relay**.
6. Click **OK**.

Defaulting to Automatic Relay Discovery

As you install ESP Agents, you may want them to automatically discover the closest ESP Relay by default. Here is how to set this up:

1. As described in the previous section, open the **Edit Computer Settings** dialog
2. Select the **Target** tab.
3. Click the button labeled **All computers with the property**.
4. In the window below, select **All Computers**.
5. Select the **Constraints** tab.
6. Uncheck the **Expires On** box.
7. Click **OK**.

Now as new ESP Agents are installed, they will automatically find and connect to the closest ESP Relay without any further action.

Notes about Automatic Relay Discovery

The ESP Agents use a sophisticated algorithm to figure out which ESP Relay is the closest on the network. The algorithm uses small ICMP packets with varying TTLs to discover and assign the most optimal relay. If multiple optimal relays are found, the algorithm automatically balances the load. If a relay goes down, the Agents will perform an auto-failover. This represents a major improvement over manually specifying and optimizing relays. However, there are a few important notes about automatic relay selection:

- ICMP must be open between the ESP Agent and the ESP Relays. If the ESP Agent cannot send ICMP messages to the ESP Relays, it will be unable to find the optimal ESP Relay (in this case it would use the failover relay if specified or pick a random relay).
- Sometimes fewer network hops are not a good indication of higher bandwidth. In these cases, ESP Relay Auto-selection may not work properly. For instance, a datacenter may have an ESP Relay on the same high-speed LAN as the ESP Agents, but an ESP Relay in a remote office with a slow WAN link is fewer hops away. In a case like this, you should manually assign the ESP Agents to the appropriate optimal ESP Relays.
- ESP Relays will use the DNS name that the operating system reports. This name must be resolvable by all ESP Agents otherwise they will not find the ESP Relay. This DNS name can be overridden with an IP address or different name using a Task in the ESP Support site.
- ESP Agents can report the distance to their corresponding relays. This information is valuable and should be monitored for changes. Computers that abruptly go from one hop to five, for instance, may indicate a problem with their relays.
- More information about ESP Relays, automatic relay selection, and troubleshooting ESP Relay can be found at the Trend Micro support site.

Using Relay Affiliation

ESP Relay Affiliation is intended to provide a more sophisticated control system for automatic relay selection. The feature is very flexible and may be used in many different ways but the primary use case is to allow the ESP infrastructure to be segmented into separate logical groups. A set of ESP Agents and ESP Relays can be put into the same affiliation group such that the ESP Agents will only attempt to select the ESP Relays in their affiliation group. This feature is built on top of automatic relay selection and you should understand that process (see the previous section) prior to implementing ESP Relay Affiliation.

ESP Relay Affiliation only applies to the automatic relay selection process. The manual relay selection process (see next section) is unaffected even if computers are put into ESP Relay Affiliation groups.

Creating ESP Agent Affiliation Groups

ESP Agents are assigned to one or more Relay Affiliation groups through the ESP Agent setting:

`_BESClient_Register_Affiliation_SeekList`

This ESP Agent setting should be set to a semi-colon (;) delimited list of relay affiliation groups, for example:

```
AsiaPacific;Americas;DMZ
```

Creating ESP Relay and Server Affiliation Groups

ESP Relays and ESP Servers can be assigned to one or more Affiliation groups through the ESP Agent setting:

```
_BESRelay_Register_Affiliation_AdvertisementList
```

This ESP Agent setting should also be set to a semi-colon (;) delimited list of relay affiliation groups, for example:

```
AsiaPacific;DMZ;*
```

Note: ESP Relays and ESP Servers are not required to have a SeekList setting. The SeekList is only used by the ESP Agent.

ESP Relay Affiliation List Information

There are no pre-defined relay affiliation group names; you are free to pick group names that are logical to your deployment of ESP. There are some naming rules you should observe:

- Do not use special characters (including ".") when picking names

- Group names are not case sensitive
- Leading and trailing whitespaces are ignored in comparisons

The ordering of Relay Affiliation groups is important for the ESP Agent. The asterisk (*) has a special meaning in a Relay Affiliation list: it represents the set of unaffiliated computers. Unaffiliated computers are ESP Agents or ESP Relays which do not have any relay affiliation group assignments or have the asterisk group listing.
For more information on ESP Relay Affiliation, see the article at the Trend Micro support site.

Manually Selecting Relays

You may have a reason to manually specify exactly which ESP Agents should connect to which ESP Relay. You can do that too. Here is how:

1. Start up the ESP Console and select the **ESP Management** Domain. From the Computer Management folder, click the **Computers** node to bring up a list of ESP Agents in the list panel.
2. Shift- and ctrl-click to select the set of computers you want to attach to a particular ESP Relay.
3. Right-click on this highlighted set and choose **Edit Computer Settings** from the pop-up menu. As with creating the relays (above), the dialog boxes are slightly different if you have selected one or multiple computers.
4. Check the box labeled **Primary ESP Relay** and then select a computer name from the drop-down list of available ESP Relay servers.
5. Similarly, you can assign a **Secondary ESP Relay**, which will be the backup whenever the Primary Relay Server is unavailable for any reason.
6. Click the **OK** button**.**

Viewing ESP Relay Selections

To see which ESP Agents are selecting which ESP Relays:

1. Start up the ESP Console and select the **ESP Management** Domain.
2. From the **Computer Management** folder, click the **Computers** node to bring up a list of ESP Agents.
3. Look under the **Relay** column in the List Panel (this column may be hidden; if so you may need to right-click on the column headings and make sure **Relay** is checked). The ESP Relay columns show information including the ESP Relay method, service and computer.

By default, the ESP Agents will attempt to find the closest ESP Relay (based on the fewest number of network hops) every six hours. More information on ESP Relays can be found at the Trend Micro support site.

Monitoring ESP Relay Health

ESP allows you to monitor your ESP Agent/Relay setups to ensure they are working optimally. Before deploying a large patch, you may want to check the status of your ESP Relays to guarantee a smooth rollout.

Here are some suggestions for monitoring your ESP Relay deployment:

- Click on the **ESP Management** domain and the **Analyses** node and activate the ESP Relay Status analysis. This Analysis contains a number of properties that will give you a detailed view of the ESP Relay health.
- Click on the **Results** tab for the analysis to monitor the Distance to ESP Relay property in the ESP Relay Status Analysis to get a sense of what is normal in your network. If your topology suddenly changes, or you notice that some of your ESP Agents are using extra hops to get to the server, it could indicate the failure of an ESP Relay.
- Try to minimize the number of ESP Agents reporting directly to the ESP Server because it is generally less efficient than using ESP Relays. You can see which computers are reporting to which ESP Relays by studying this Analysis.

Optimizing the ESP Server(s)

ESP is designed to operate efficiently, with minimal impact on network resources. However, there may be installations that stretch the recommended configurations, where there just seem to be too many ESP Agents for the allotted server power. The best solution is to properly spec your server for your environment; you may be able to modify some preferences to get better performance. Most of these optimizations involve a trade-off between throughput and responsiveness, so proceed with caution. Your Trend Micro support technician has more information about which modifications might be best for your particular deployment.

Here are some possible optimization techniques:

- Deploy **ESP Relays** to reduce the load on the server. This is by far the most effective way to increase the performance and responsiveness of ESP. Generally, the more ESP Relays, the better the performance (as a rule of thumb, one ESP Relay for 500-1000 ESP Agents is a good choice, although it can be much higher for a dedicated computer).
- Slow down the **ESP Agent heartbeat** from **File > Preferences**. This decreases the frequency of messages that are regularly dispatched by the ESP Agents to update their retrieved properties. Reducing this frequency will reduce the amount of network traffic generated, but also decreases the timeliness of the retrieved properties. However, regardless of the heartbeat settings, the ESP Agents always send up their latest information whenever they receive a refresh ping from the ESP Server or when they notice that a Fixlet is relevant.
- Slow down the **Fixlet List Refresh** rate from **File > Preferences**. This decreases the update frequency for the information displayed in the ESP Console. If there are many ESP Agents or Consoles simultaneously connected or the database is very large, reducing this frequency can substantially reduce the load on the ESP Server. If multiple ESP Console operators are going to be simultaneously using the ESP Console, you should set the refresh rate to be something higher than the default (15 seconds) to reduce the load on the ESP database. Consider changing it to 60-120 seconds or more if there are many ESP Console operators. The ESP Admin tool on the ESP Server will allow you to set a global minimum refresh rate.
- Your database administrator may be able to help you with the following optimizations:
  - Change the SQL Server Recovery Model for the BFEnterprise database to **Simple** rather than **Full** which is the default.
  - Reduce the percentage of memory allocated to SQL Server from 100% to 85%, to ensure that the web server and operating system are not starved for memory.
- More performance recommendations can be found at the Trend Micro support site.

Optimizing the ESP Console(s)

To be responsive, the ESP Console requires reasonable CPU power, memory and cache space. If you have an ESP Console that is taking a long time to load or that is performing sluggishly, there are several techniques you can use to speed it up:

- **Make sure you have sufficient memory**. The ESP Console benefits greatly from capacious memory to speed up the viewing, filtering and sorting of content (Fixlet messages, Tasks, Actions, etc.). If your computer does not have enough physical memory, the ESP Console will run noticeably slower. You can check memory usage from the Task Manager (Ctrl-Shift-ESC). Select the Performance tab and refer to the Physical Memory section. If the available memory is less than 10% of the total memory, you are running low on RAM and can benefit from adding more.
- **Use high-speed network connections** between your ESP Consoles and Servers, preferably with LAN connections of at least 100 MBPS. The ESP Database can be sizeable for a large network, so running the ESP Console from a computer with a slow connection will often result in very long load times.
- **Use remote control software**. With so much data to load and display, operating the ESP Console in a remote office over a slow link can be tedious. In situations like this, you may be able to benefit from solutions such as Citrix, Terminal Services or other remote control software. Set up the remote control server on a computer with fast access to the ESP Server. Allow that machine to present instances of the ESP Console and let the branch office run these Consoles remotely. The database stays in the main office, and the remote office enjoys optimal performance. For more information, see the section on **Remote Citrix / Terminal Services Configuration** (page 109).
- **Delete old actions**. The ESP database stores information about old actions which the ESP Console loads in at startup and saves out at shutdown. If you do not need to track these old actions, you can delete them, allowing the ESP Console to load and close faster. Note that deleted actions continue to exist in the database, but are simply not loaded into the ESP Console or Web Reports and can be undeleted if necessary.
- More information about enhancing the performance of ESP is available at the Trend Micro support site.

Managing Replication (DSA)

Replication servers are simple to set up and require minimal maintenance. You may wish to tweak the interval or allocate your ESP Servers differently. Most of these changes are done through the ESP Administration Tool. Here you can see the current settings for your ESP Servers and make the appropriate changes.

Change the Replication Interval

1. Start up the **ESP Administration Tool**.
2. Select the **Replication** tab.
3. Select the desired server from the drop-down menu. Using longer replication intervals will mean that the servers will need to replicate data less often, but they will have more data to transfer each time. Note that replication intervals can be different for “replicating from” and “replicating to” a server.
4. Select the desired replication interval from the menu at the right.
5. Click **OK**.

Switching the Master Server

By default, server 0 (zero) is the master server. ESP Administration will only allow you to perform certain administrative tasks (such as creating and deleting users) when you are connected to the master server. If you wish to switch the master to another server, you must set the deployment option **masterDatabaseServerID** to the desired ID. Here is how:

1. Start up the **ESP Administration Tool.**
2. Select the **Advanced Options** tab and click the **Add** button.
3. Type masterDatabaseServerID as the name, and then enter the desired ID as the value.
4. Click **OK**.

Once that value has successfully replicated to the new server, it will become the master server. If a server suffers a failure while it is the master, another server will need to be made the master server by direct manipulation of the ADMINFIELDS table in the database. The details of this are beyond the scope of this guide, but broadly speaking, you might use a tool like SQL Enterprise Manager to view and alter the ADMINFIELDS table. Set the variable name masterDatabaseServerID to the desired value.

Uninstalling a Replication Server

To uninstall a replication server, you will have to call the database-stored procedure **delete_replication_server**, which removes the specified ID from the replication set. Be careful not to delete the wrong server, or you may lock yourself out. The details of this procedure are beyond the scope of this guide, but basically you must log into the database with SQL Server Management Studio. You can call the procedure with something like:

```
dbo.delete_replication_server( 1 )
```

This would delete the ESP Server with ID=1.

The steps involved in completely deleting the server are beyond the scope of this guide, but the full procedure is available in a KB article at the Trend Micro support site.

Managing Bandwidth

File downloads consume the bulk of the bandwidth in a typical ESP Installation. You can control this bandwidth by throttling, which limits the number of bytes per second. You can specify the bandwidth throttling on either the ESP Server or on the ESP Agent or on both (in which case the lower of the two values is used). This can be important whenever you have bandwidth issues, as in the following situations:

- A remote office with a thin channel
- Remote dial-in users or users on a slow connection
- A shared channel with higher-priority applications
- A WAN or LAN that is already saturated or has stringent load requirements

Bandwidth throttling settings (and other ESP Relay, ESP Server, and ESP Agent settings) can be set using the Tasks from the ESP Support site. Select the **ESP Management** domain and select the **ESP Component Management** node in the Navigation treeto see the entire task list.
For more information About ESP Relay, please visit the Trend Micro support site.

Dynamic Throttling

When a large download becomes available, each link in your ESP deployment may have unique bandwidth issues. There are server-to-client, server-to-relay and relay-to-client links to consider, and each may require individual adjustment. As explained in the previous section, it is possible to simply set a maximum value (throttle) for the data rates, and for this there are broad-based policies you can follow. You might, for instance, throttle an ESP Agent to 2Kb/s if it is more than three hops from an ESP Relay. However, the optimal data rates can vary significantly, depending on the current hierarchy and the network environment.

A better technique is to use **dynamic bandwidth throttling**, which monitors and analyzes overall network capacity. Whereas normal throttling simply specifies a maximum data rate, dynamic throttling adds a “busy time” percentage. This is the fraction of the bandwidth that you want to allocate when the network is busy. For instance, you could specify that ESP downloads should not use any more than 10% of the available bandwidth whenever ESP detects existing network traffic. Dynamic throttling also provides for a minimum data rate, in the case the busy percentage is too low to be practical.

When you enable dynamic throttling for any given link, ESP monitors and analyzes the existing data throughput to establish an appropriate data rate. If there is no competing traffic, the throughput is set to the maximum rate. In the case of existing traffic, ESP will throttle the data rate to the specified percentage or the minimum rate, whichever is higher.

You control dynamic bandwidth throttling with computer settings. There are four basic settings for each link:

- **DynamicThrottleEnabled:** This setting defaults to zero (disabled). Any other value enables dynamic throttling for the given link.
- **DynamicThrottleMax:** This setting usually defaults to the maximum unsigned integer value, which indicates full throttle. Depending on the link, this value sets the maximum data rate in bits or kilobits per second.
- **DynamicThrottleMin:** This setting defaults to zero. Depending on the link, this value sets the minimum data rate in bits or kilobits per second. This value places a lower limit on the percentage rate given below.
- **DynamicThrottlePercentage:** This setting defaults to 100%, which has the same effect as normal (non-dynamic) throttling. It represents the fraction of the maximum bandwidth you wish to use when the network is busy. It typically has a value between five and ten percent, to prevent it from dominating existing network traffic. (A zero for this setting is the same as 100%.)

As with any other setting, you can create or edit the dynamic bandwidth settings by right-clicking on an item (or group of items) in any computer list and choosing Edit Computer Settings from the context menu.

The specific variable names include the **ESP Server/Relay settings:**

```
_BESRelay_HTTPServer_DynamicThrottleEnabled
```



```
_BESRelay_HTTPServer_DynamicThrottleMaxKBPS
_BESRelay_HTTPServer_DynamicThrottleMinKBPS
_BESRelay_HTTPServer_DynamicThrottlePercentage
```

The **ESP Agent settings:**

```
_BESClient_Download_DynamicThrottleEnabled
_BESClient_Download_DynamicThrottleMaxBytesPerSecond
_BESClient_Download_DynamicThrottleMinBytesPerSecond
_BESClient_Download_DynamicThrottlePercentage
```

The **ESP Gathering settings:**

```
_BESGather_Download_DynamicThrottleEnabled
_BESGather_Download_DynamicThrottleMaxBytesPerSecond
_BESGather_Download_DynamicThrottleMinBytesPerSecond
_BESGather_Download_DynamicThrottlePercentage
```

Note: For any of these settings to take effect, you must restart the affected services (ESP Server, Relay or Agent).

If you set an ESP Server and its connected ESP Agent to differing maximums or minimums, the connection will choose the smaller value of the two.

Creating Agent Dashboards

You can create custom Agent Dashboards, similar to those in the ESP Console. Dashboards are HTML files with embedded Relevance clauses that can analyze the local computer and print out the current results. ESP Agents with a dashboard have an extra tab to display the resulting report.

To create an Agent Dashboard, you must create a new folder named __UISupport (note the leading underlines) in the __BESData folder. This is a subfolder of the BES Client folder, so the final pathname looks like:

Program Files/BigFix Enterprise/BES Client/__BESData/__UISupport

Place the Dashboard file (named _dashboard.html) and any accompanying graphics files into this folder. The next time the Agent starts up, it will incorporate these files into its interface, adding to the **Dashboard** tab. When the user clicks on this tab, the Dashboard will calculate the latest values of each Relevance clause and display them.

The Relevance statements are embedded in the HTML inside special tags with the form:

```
<?relevance statement ?>
```

For instance, to find and print the time, use the following:

```
<?relevance now ?>
```


When the ESP Agent displays the page containing this statement, the ESP Agent evaluates the Relevance clause “now” and substitutes the value for the tag. The following sample HTML prints out the word “Date:” and then the current date and time:

```
<html>
 <body>
 Date: <?relevance now ?>
 </body>
</html>
```

To allow the user to refresh the Relevance evaluation, add this line to the file:

```
<html>
 <body>
 Date: <?relevance now ?>
 <A href="cid:load?page=_dashboard.html"> Refresh </A>
 </body>
</html>
```

This link, labeled **Refresh**, causes the page to reload. When it does, it reevaluates the relevance clauses. It is easy to see how you would add other Relevance expressions to this page.
For instance, to print out the OS and the computer name, add these two lines:

```
<html>
 <body>
 Date: <?relevance now ?>
 Operating System: <?relevance name of operating system ?>
 Computer Name: <?relevance computer name ?>
 <A href="cid:load?page=_dashboard.html"> Refresh </A>
 </body>
</html>
```

You can use style sheets to format the output. You can even use the default style-sheet, **offer.css** for some preset formatting. Here is an example of a Dashboard with a title, a header, a refresh link and a section of retrieved property values:

```
<html>
 <head>
   <link type="text/css" rel="stylesheet"
href="offer.css"></link>
   <title>BigFix Dashboard Example</title>
 </head>
 <body>

   <div class="header">
```



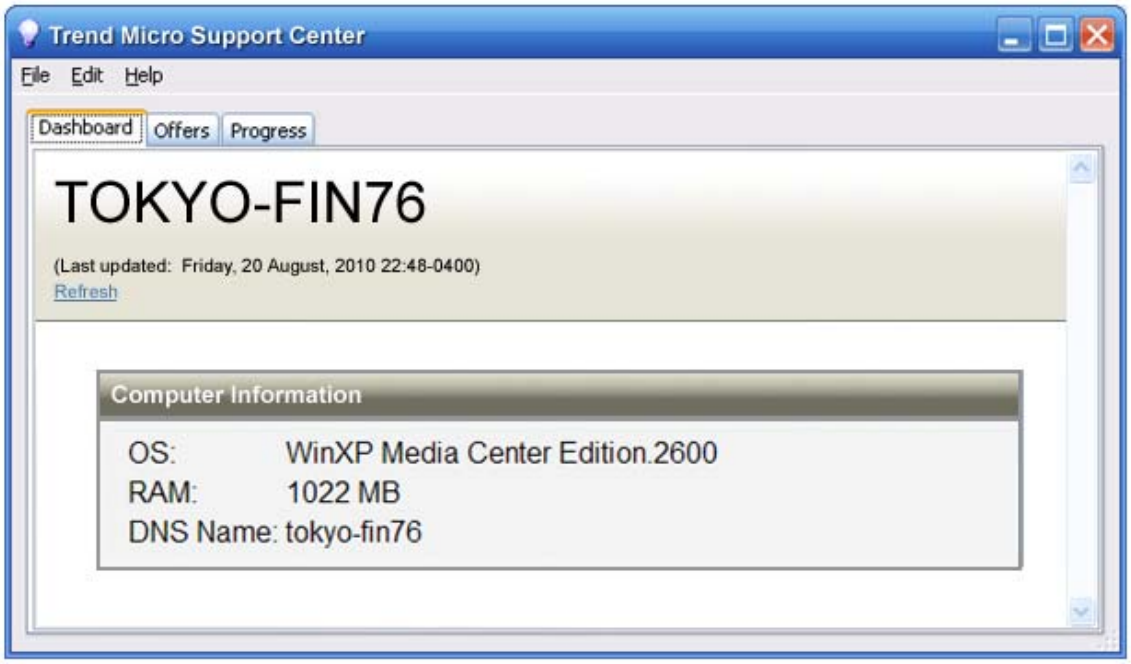
```
    <div class="headerTitle">
     <font size="6"><?relevance computer name
?></font></div>
    <div class="headerCategory">
     <font size="1">(Last updated: <?relevance now
?>)</font><BR>
     <div><font size="1">
      <a
href="cid:load?page=_dashboard.html">Refresh</a></font>
     </div>
    </div>
   </div>

   <div class="section">
    <div class="sectionHeader">Computer Information</div>
    <div class="subsection">
     <table>
      <tr> <td valign="top">OS: </td>
        <td><?relevance operating system ?></td></tr>
      <tr> <td valign="top">RAM: </td>
        <td><?relevance (size of ram)/1048576 ?>
MB</td></tr>
      <tr> <td valign="top">DNS Name: </td>
        <td><?relevance dns name ?></td></tr>
     </table>
    </div>
   </div>
  </body>
</html>
```

For the offer.css to work correctly the following graphics files should be copied to the __UISupport directory from the ESP Agent directory:

```
bodyBg.jpg,
bodyHeaderBg.jpg
bullet.gif
sectionHeaderBG.gif
```

When executed from the ESP Agent, this dashboard will produce the following output:



To learn more about Relevance expressions, see the ***BigFix Relevance Language Reference***.

Geographically Locating ESP Agents

Since the ESP Agents are often deployed in remote offices, it is useful to create a property that lets the ESP Agents report their own location. You can create a location property in ESP using the **Location Property Wizard**.

1. In the ESP Console, go to the **ESP Management** domain, click on the **Computer Management** folder node, and then click on the **Location Property Wizard** node. A wizard document will open.
2. The wizard creates a named property allowing the ESP Agents to identify themselves based on their subnet, IP range, or other information. Read the instructions in the wizard to create the property.

Viewing Reports over the Web

The **ESP Web Reports** component of the ESP Server can monitor, print or analyze the status of the local database. It also has the ability to read the databases of other ESP Servers and include their data. That offers the administrator a top-level view of a large or far-flung enterprise with multiple database servers and hundreds of thousands of managed computers.

ESP Web Reports can be viewed at any time from **Start > Programs > ESP Enterprise > ESP Web Reports** or from the ESP Console under **Tools > View Web Reports**.

Aggregating Multiple ESP Servers into One Web Reports Server

Any ESP Web Report server can be set up to include data from any other ESP Server. In order to do so, the program must be able to connect to the other databases using ODBC communications over TCP/IP (i.e., the computers must be on the same LAN or connected by VPN, etc.).

To set up the ESP Web Reports using a SQL Server authenticated account, perform the following steps:

1. From the ESP Console, open the ESP Web Reports page under **Tools > View Web Reports**.
2. Log into the ESP Web Reports as an administrator.
3. Click on **Administration**, then **Database Settings**, and then click on the **Add New Database** link.
4. Enter a Server Name that will identify this database. If connecting through a DSN (Data Source Name), enter the **DSN name**. If connecting through an IP address, select **Use a default DSN-less connection** and type in the IP address of the ESP Server you wish to include (e.g., 192.168.100.123 or besserver1.acme.com).
5. There are two ways to provide authentication for your database. The first option is **Windows Authentication**, which is convenient if you have access to the Microsoft SQL Server Enterprise Manager and the servers are in the same domain.
6. Alternatively, you can choose the option labeled **Use Username and Password to login**. With this option, you need to enter the **Username** and **Password** of a user with access to the desired database. You can use your ESP Console username and

password, or you can use the Microsoft **SQL Server Enterprise Manager** to create a new user who has *total* access to the **AggregatedBy** table and *read* access to all other tables in the BFEnterprise database.

7. Confirm or edit the Web Reports Server **URL**, which will be inserted into this database as an identifier.

Logging Web Reports

You can keep track of your Web Reports usage of by setting up a log file. The name of the log file is stored in the registry. Here is how to set or access the name:

8. Run Regedit and find the **HKey Local Machine\Software\BigFix\Enterprise Server\BESReports** key. You will see some variables and pathnames used by Web Reports. You need to add two values to this key; one for the logging flag, and one for the filename.
1. Create a new DWORD value named LogOn and set it to 1 to turn on logging.
2. Create a new string value named LogPath and set it to the full pathname of your desired log file, e.g. “C: \fullpath\file.txt".

The next time you launch Web Reports, a log of the session will be saved to the specified file.

HTTPS Configuration

To provide more security to Web Reports, you can use HTTPS instead of HTTP to make your browser connection. To use HTTPS, you must have a proper SSL certificate. The SSL certificate should be in standard OpenSSL PKCS7 (.pem) file format. If the certificate meets all of the trust requirements of the connecting browser, then the browser will connect without any interventions by the user. If the certificate does not meet the trust requirements of the browser, then the user will be prompted with a dialog asking if it is OK to proceed with the connection, and provided with access to information about the certificate. Typically, a trusted certificate is one which is signed by a trusted authority (e.g., Verisign), contains the correct host name, and is not expired. The .pem file is your SSL certificate, which you must obtain through your favorite CA. If you don't require authentication back to a trusted root, you can also generate a self-signed certificate with the OpenSSL utilities (see the Trend Micro support site for more information). Once you have a certificate, place it on the computer running web reports (usually the ESP Server) and follow these directions:

1. Run **regedit** and locate

   HKEY_LOCAL_MACHINE\Software\BigFix\EnterpriseClient\Settings\Client

   You need to add or modify three subkeys; one for the HTTPS flag, one for the location of the SSL certificate, and one for the HTTPS port number.

   For x64 systems, the key will be here:

   HKEY_LOCAL_MACHINE\Software\Wow6432Node\BigFix\EnterpriseClient\Settings\Client
2. Create a new sub-key of **Client** called _WebReports_HTTPServer_UseSSLFlag (it may already exist).
3. Create a new string value (reg_sz) for the key _WebReports_HTTPServer_UseSSLFlag called **value** and set it to 1 to enable HTTPS.
4. Create a new sub-key of **Client** called _WebReports_HTTPServer_SSLCertificateFilePath (it may already exist).
5. Create a new string value (reg_sz) for the key _WebReports_HTTPServer_SSLCertificateFilePath called **value** and set it to the full path name of the SSL certificate (cert.pem).
6. Create a new sub-key of **Client** called _WebReports_HTTPServer_PortNumber (it may already exist).
7. Create a new string value (reg_sz) for the key _WebReports_HTTPServer_PortNumber called **value** and set it to port number you would like to use (typically 443).
8. Update the Web Reports URL to use https:// instead of http:// and Port 443 instead of Port 80. You can do this by editing the URL string within Web Reports. To do this, from the Overview page select the **Databases** link. Then select the **Edit Database** link under the appropriate database. Then you can modify the entry for **Web Reports URL**.
9. Restart the **ESPWebReports** Service.

Part Four

Managing and Maintaining ESP

Now that you have installed the ESP components and customized the configuration to suit your own needs, this section explains how to maintain and manage your ESP installation.

Adding New Operators and Master Operators

There are two classes of operator for the ESP Console: Ordinary Operators and Master Operators.

- **Ordinary Operators** manage a subset of the ESP Agents based on their management rights and have restricted privileges to administer ESP functions.
- **Master Operators** have the ability to manage all the ESP Agents and can also assign management rights to other operators.

The Site Administrator has the most important primary key (license.pvk), and can do anything a Master Operator can. However, it is bad practice to use your site key for ordinary operations. Instead, create a Master Operator account and use that key (publisher.pvk) exclusively for Console operations. To add new Operators and Master Operators to the ESP system, simply repeat the steps outlined in **Adding New Operators and Master Operators** (page 82).

Assigning Management Rights

In a typical ESP deployment, there will be anywhere from a couple hundred to a couple hundred thousand computers reporting to a single ESP Server. At these scales, it is often important to separate out which computers can be controlled by different ESP Console operators for organizational and security reasons.

ESP allows you to break down management rights into separate sections based upon geography, department, computer type (servers vs. workstations), or any other property. Each ESP Console operator can be assigned management rights to the appropriate computers. All of this is done by assigning computers to operators based on computer properties. For instance, you could allow a member of a server team to control all computers that have server-based operating systems in the company datacenter. First specify which subnets are in the datacenter, then any computer in that subnet with a server OS will be managed by the given operator.

Using this approach, the operators can see a subset of computers and will not be able to see information or change anything on computers that they do not manage. When they view the ESP Console or ESP Web Reports, it appears to them that they have their own ESP Server with no other computers.

Because different operators can be assigned to overlapping groups of computers, any kind of configuration is possible. ESP Console operators only receive information from their assigned computers, improving manageability and responsiveness.

Here is how to **Add** or **Delete** management rights:

1. Log in to the ESP Console as a Master Operator.
2. Click on the **ESP Management** domain and click on the **Operators** node (if this choice is not available, you may not have the proper authorization to perform this command). You will see a list of ESP Console operators.
3. Right-click on a single operator from the list and select **Assign User Management Rights** from the pop-up menu.
4. If user rights have already been set for this user, you will see them here. Click the **Add** button to assign management rights to the selected operator. (You can also *revoke* specific management rights using this dialog box by clicking on the **Delete** button.)
5. Use the filter panel on the left to narrow down the computers you want to assign to this operator. By shift- or ctrl-clicking on items in the **Retrieved Properties** or **Group** folders, you can specify a set of computers that share common properties or settings. As new computers are added to the network, they will automatically be classified by their retrieved properties or group, and the proper ESP Console operators will automatically be assigned to manage them.

   Note: If you grant a user access to computers with a specific retrieved property value and the property value changes, then the user will no longer have access to those computers. For instance, if you assign a user permissions on a certain subnet and a laptop moves to a different location with a different subnet, the user will no longer be able to administer the laptop unless it comes back to the original office.
6. Click the **OK** button.

Changing a Publisher Password

Any console operator can change their publisher credential password from the ESP Console:

1. Select **Manage Signing Keys** from the **Tools** menu.
2. Click the **Change Password** button at the bottom of the dialog.
3. Type in your old password to authenticate yourself, then enter your new password and confirmation.

Note that the publisher password and database passwords are normally created as the same password, but they can be different if desired.

Changing an ESP Database Password

You can change your database password from the ESP Console.

1. Select **Change Database Password** from the **File** menu (you must have the proper permissions to select this item).
2. Type in your old password to authenticate yourself, and then enter your new password and confirmation.

Note that the publisher password and database passwords are normally created as the same password, but they can be different if desired.

Removing an ESP Console Operator

When an employee leaves, you will want to delete their access rights to the ESP database. This is done with the **ESP Administration Tool**:

1. Launch the program by selecting **Start > Programs > ESP Enterprise > ESP Administration Tool**.
2. Select a user from the list, and click **Remove User**.
3. When you have deleted the desired operator, click **OK.** This will remove that operator's privileges from the database, stop all of the user's pending actions and notify the ESP Agents that the private keys from that user are no longer valid.
4. You will be prompted to propagate the action site masthead to reflect the user changes. Click **Yes** to continue.
5. Enter your private key password and click **OK**.

Using NT Authentication

By default, ESP Consoles create an ODBC connection to the SQL database, and the DSN is set to use SQL authentication. You can change this DSN to use NT authentication through the Windows ODBC Data Source Administrator. Doing so will cause the ESP Console to ask the current Windows user to authenticate with the SQL Server. For more information, see the article on NT authentication at the Trend Micro support site.

Managing Agent Encryption

Server and Relay-bound communications from ESP Agents can be encrypted to prevent unauthorized access to sensitive information. To enable it, you must generate a key and provide a setting value. The setting is accomplished in the ESP Console and is described elsewhere in the section labeled **Enabling Encryption on ESP Agents**. The key is generated from the **Encryption** tab of the ESP Administration Tool:

1. Launch the ESP Administration Tool by selecting Start > Programs > ESP Enterprise > ESP Administration Tool.
2. Select the **Encryption** tab.

At the top of the dialog is a statement of the current state (in this example: **Report encryption is currently DISABLED**). ESP Agent encryption has four states, Disabled, Pending, Enabled and Pending Rotation:

- **Disabled**: This state indicates that no encryption certificate is included in your deployment masthead, which means that Agents cannot encrypt their reports even if they are told to do so. Click on **Generate Key** to create an encryption certificate (and the corresponding private key which can be used to decrypt reports at the receiving end). This will cause you to enter the **Pending** state.
- **Pending**: In this state, an encryption certificate has been generated and is ready for deployment, but the private key has not yet been distributed to all necessary decrypting relays and servers. Once you have manually distributed the private key, click on the **Enable Encryption** button to embed the certificate in the masthead and send it out to all clients. At that point, you will enter the Enabled state. You can also click **Cancel** to return to the Disabled state.
- **Enabled**: In this state, an encryption certificate has been found in your deployment masthead, which means that you are able to turn on encryption (using the setting discussed previously) for any of the Agents in your

deployment. At any time, you can click on **Generate new key** to create a new encryption certificate. This is useful if you have a key rotation policy or if your encryption key is ever compromised (see next section). Generating a new key returns you to the Pending state (unless you elect to deploy immediately as described in the next section). You can also click **Disable** to move back to the Disabled state.

- **Pending Rotation**: In this state, an encryption certificate is included in your deployment masthead, and a new certificate has been generated and is ready to replace the existing certificate.

Generating a New Encryption Key

Should your private key be compromised or if you have a policy of rotating keys, you can easily generate a new key from the **ESP Administration Tool**. Here is how:

1. Launch the ESP Administration Tool by selecting **Start > Programs > ESP Enterprise > ESP Administration Tool**.
2. Select the **Encryption** tab.

3. Click the **Generate key** button. The Create Encryption Credentials dialog opens.

4. From this dialog, select the key size. The default is 2048, which is adequate for most purposes. Check the box to use this key immediately. However, if you have established ESP Relays that use encryption, you should leave this box unchecked until you can distribute the new key to those Relays.
5. Click **OK** to distribute this new key to your ESP Agents. You must provide your Site Admin Private Key to propagate the Action. A final dialog will ask for confirmation. For more information on encryption key sizes and server requirements, see the knowledge-base article on server requirements at the Trend Micro support site.

Creating Top-level Decrypting ESP Relays

When an Action is deployed, thousands of ESP Agents may report back in a short time-frame, typically to an ESP Relay. If you have elected to encrypt these reports, the Relay will bundle the reports together and pass them up to the ESP Server, which must then split up and decrypt each one of them. With many thousands of ESP Agents, this can impose a significant computational burden on the ESP Server.

To improve performance, you can lighten the load on your ESP Server by allowing your top-level ESP Relays to do the bulk of the decryption. If you have over 50,000 ESP Agents, you may be able to substantially reduce the load on your ESP Server by moving decryption down into the relay chain. If the ESP Relay has its own decryption key, it can first decrypt the Agent messages into plain text and then bundle thousands of them into a single archive. This can then be compressed, encrypted and passed up to the ESP Server. At that point, the server can perform a single decryption on the entire archive, noticeably reducing its overhead.

To spread the decryption duties, you simply need to distribute your encryption keys to your top-level ESP Relays. For normal server-level encryption, ESP creates an encryption key for you and places it in the ESP program folder:

`C:\Program Files\BigFix Enterprise\BES Server\Encryption Keys`

To allocate the load to your top-level ESP Relays, place the encryption key in the equivalent ESP Relay directory:

`C:\Program Files\BigFix Enterprise\BES Relay\Encryption Keys`

These top-level ESP Relays will decrypt all the documents received, bundle them together and then re-sign them with a single signature. You can put as many keys as you want in the folder and the ESP Relay will attempt to use each of them when it gets an encrypted Agent report. Agents encrypt against the key found in the masthead file which should be the last key created. However, it is possible that an ESP Agent will transmit a report with an older version of the masthead (and thus a different encryption key) if it hasn't gathered the latest Action site for any reason.

There are a few considerations:

- You must manually transfer the key file from the server to the relay every time you create a new encryption key.
- During the transfer process, it is important not to expose your private key file. This means you shouldn't just move the key over the internet because anyone listening might be able make a copy of your private key file. Therefore it is best to physically transfer the key from one computer to another, for instance with a USB key.
- During the encryption key creation process, you have the option to create the private key file but not propagate it out in the masthead. This step allows you time to transfer the new key file to the ESP Relays before Agents start posting encryption messages with that key.

Managing Downloads

ESP uses several methods to ensure that downloads are efficient and make the best use of available bandwidth. Among other techniques, caching is used extensively by all the ESP elements, including Servers, Relays and Agents.

When an Action on an ESP Agent needs to download a file, the local cache is checked first. If the Agent can't find it locally, it requests the file from its parent, typically an ESP Relay. When the file is requested, the Relay checks it own cache. If it finds the file, it immediately sends it down to the requesting Agent. Otherwise, it passes the request up to its parent, which may be another ESP Relay and the process continues. Ultimately, an ESP Server retrieves the file from an internal server or the Internet, caches it and then passes it back down the chain. After receiving the file, each Relay in the chain caches it, and continues to forward it down to the original ESP Agent, which also caches it.

Each cache retains the file until it runs out of room. At that point, the cache is purged of the least-recently used (LRU) files to provide more space. You can view the ESP Relay cache size and other ESP Relay information by activating the **ESP Relay Cache Information** Analysis available from the ESP Support Fixlet site. The default cache size is 1 GB, but it can be changed by using the **ESP Relay/ESP Server Setting: Download Cache Size Task**, also from the ESP Support Fixlet site.

There may be situations that require files to be manually downloaded and cached, typically because such files are not publicly available, in which case you must download the files directly from the source. You can pre-populate the download cache by copying files to the download cache location. You can also clear these files out manually if you wish.

The caches are stored as subfolders of the BigFix Enterprise folder, which is created by default at **C:\Program Files\BigFix Enterprise**. The Server download cache is **BES Server\wwwrootbes\bfmirror\downloads\sha1**, and the Agent download cache is found at **BES Client__BESData__Global__Cache\Downloads**. For security purposes, each file you save must be named with the sha1 hash value of the file. If the filename doesn't match the sha1, the file will be ignored.

As well as the download cache, ESP Relays maintain an Action cache (also 1 GB) holding all the files needed for each Action, and ESP Agents maintain a Utility cache.

For information about troubleshooting Relays, including bandwidth and downloading, see the KB article on relay health at the Trend Micro support site.

Dynamic Download White-lists

Dynamic downloading extends the flexibility of Action scripts, adding the ability to use relevance clauses to specify URLs.

As with static downloads, dynamic downloads must specify files with the confirmation of a size or sha1. However, the URL, size, and sha1 are allowed to come from a source outside of the Action script. This outside source may be a manifest containing a changing list of new downloads. This technique makes it easy to access files that change quickly or on a schedule, such as antivirus or security monitors.

This flexibility entails extra scrutiny. Since any Agent can use dynamic downloading to request a file, it creates an opportunity for people to use your server to host files indiscriminately. To prevent this, dynamic downloading uses a white-list. Any request to download from a URL (that isn't explicitly authorized by use of a literal URL in the action script) must meet one of the criteria specified in a white-list of URLs on the ESP server, located at **<ESP Server Install Path>\Mirror Server\Config\DownloadWhitelist.txt**. This file contains a newline-separated list of regular expressions using a Perl regex format, such as the following:

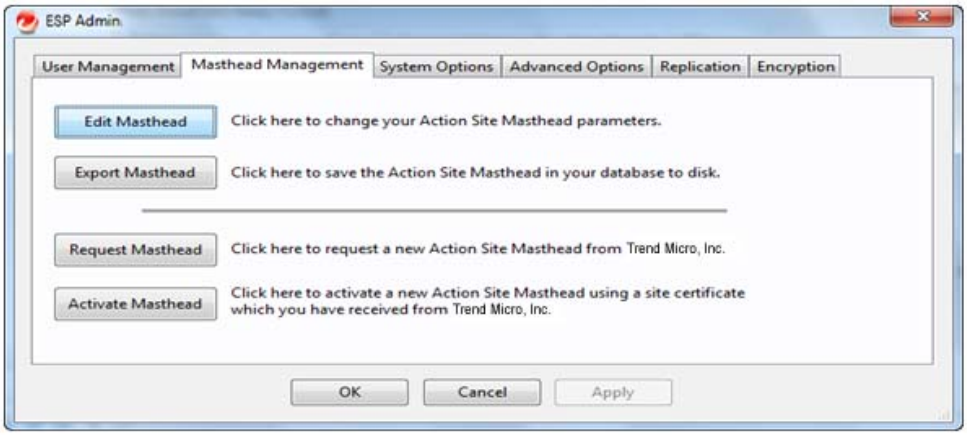
```
http://.*\.site-a\.com/.*
http://software\.site-b\.com/.*
http://download\.site-c\.com/patches/JustThisOneFile\.qfx
```

The first line is the least restrictive, allowing any file at the entire site-a domain to be downloaded. The second line requires a specific domain host and the third is the most restrictive, limiting the URL to a single file named "JustThisOneFile.qfx". If a requested URL fails to match an entry in the white-list, the download immediately fails with status NotAvailable. A note is made in the Relay log containing the URL that failed to pass. An empty or non-existent white-list will cause all dynamic downloads to fail. A white-list entry of ".*" (dot star) will allow any URL to be downloaded.

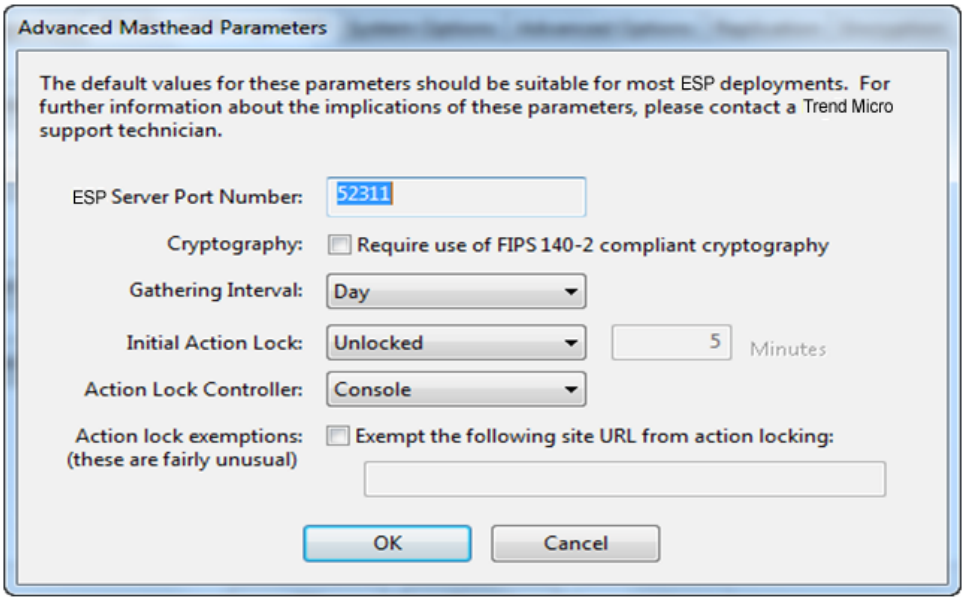
Editing the Masthead

You can change certain default parameters stored in the masthead for the ESP system by using the **ESP Administration Tool**. Here is how:

1. Launch the program from Start > Programs > ESP Enterprise > ESP Administration Tool.
2. Browse to the location of your site license and click **OK**.
3. Select the **Masthead Management** tab and Click the **Edit Masthead** button.



4. The Edit dialog appears.



> **Note:** It is recommended you keep the default settings on this page unless you have a specific reason to change them. Improper settings can cause ESP to work in non-optimal ways. Consult with a support technician for more details.

5. The parameters you can edit include:
   - **ESP Server Port Number:** In general, you will not want to change this number. In addition, if you decide to change this number *after* deploying the ESP Agents, ESP will not work correctly. See

- **Modifying Port** Numbers, in the next section.
- **Cryptography:** Check this box to implement the Federal Information Processing Standard on your network. This changes the masthead so that every ESP component attempts to go into FIPS mode. By default, the Agent will continue in non-FIPS mode if it fails to properly enter FIPS, which may be a problem with certain legacy operating systems. Be aware that checking this box can add 3-4 seconds to the ESP Agent startup time.
- **Gathering Interval:** This option determines how long the ESP Agents will wait without hearing from the ESP Server before they check whether new content is available. In general, whenever the ESP Server gathers new content, it attempts to notify the ESP Agents that the new content is available through a UDP connection, circumventing this delay. However, in situations where UDP is blocked by firewalls or where network address translation (NAT) remaps the IP address of the ESP Agent from the ESP Server's perspective, a smaller interval becomes necessary to get timely response from the ESP Agents. Higher gathering rates will only slightly affect the performance of the ESP Server, because only the differences are gathered – an ESP Agent does not gather information it already has.
- **Initial Lock state:** You can specify the initial lock state of all ESP Agents. Locked ESP Agents will report which Fixlet messages are relevant for them, but will not apply any actions. The default is to leave them unlocked and to lock specific ESP Agents later on. However, you may wish to start with the ESP Agents locked and then unlock them on an individual basis in order to give you more control over newly installed ESP Agents. Alternatively, you can set them to be locked for a certain period of time (in minutes).
- **Action Lock Controller:** This parameter determines who can change the action lock state. The default is **Console**, which allows any ESP Console operator with management rights to change the lock state of any ESP Agent in the network. If you wish to delegate control over locking to the end user, you may select **Agent**, but this is not recommended.
- **Action Lock Exemptions:** In rare cases, you may need to exempt a specific URL from any locking actions. Check this box and enter the exempt URL.

6. Click **OK** to enter the changes.
7. Enter your site password at the prompt.

Note: The masthead changes do NOT affect ESP Agents that are already deployed, but you can export the masthead using the ESP Admin tool and replace the masthead in the ESP Server so that ESP Agents deployed with the new masthead will use these changes.

Modifying Port Numbers

The ESP Console and ESP Server communicate using ODBC, which operates on port **1433** by default. For more information about changing this port please ask your database administrator.

By default, the ESP Server uses port **52311** to communicate with the ESP Agents, but any port number can be chosen (although you should avoid the reserved ports between 1-1024 because of potential conflicts and difficulty managing network traffic).

Your choice of the ESP Server Port Number is factored into the generation of the masthead, which specifies URLs for the action, registration, reporting, and mirror servers. As a consequence, you must finalize your port number ***before installation***.

Modifying Global System Options

The ESP Admin Tool allows you to modify a few basic system defaults, such as the minimum refresh, Fixlet visibility and the Agent UI Icon. Here is how:

1. Launch the ESP Admin Tool from Start > Programs > ESP Enterprise > ESP Administration Tool.
2. Select the **System Options** tab.
3. At the top, you can set the global **Minimum Refresh**. The default is 15 seconds, which is a good trade-off between responsiveness and low network load. If you find that ESP communications are impacting your network, you can raise the minimum to 60 seconds or more.
4. External sites are visible to all Console operators by default, but you can change that in the section marked **Default Fixlet Visibility**. Click the lower button to make external content invisible to all but Master Operators.
5. You can customize the Agent User Interface with your own logo. You can use any graphic you choose, but because it is a global setting, corporate branding is typical. When you present your ESP Agents with a message or an offer, they will see the icon you supply in the title bar, as well as the tray and task bar. The icon file should have several images of different sizes. The first image in the file should be a 64 x 64 image with transparency and will be used in the body of the dialogs. The title bar and task bar icons are chosen by size, targeting the size indicated by system metrics SM_CXICON and SM_CYICON. These are typically 16 or 32. The icon file should be created according to Microsoft's procedure for creating a Windows XP icon with transparency. Click the **Add Icon** button to browse for an appropriate icon (.ico) file.

Scheduling Replication

If you have multiple ESP Servers in your deployment, you can schedule when each will replicate. The default is five minutes, but you can shorten the time for greater recoverability or increase it to limit network activity. Here is how:

1. Launch the ESP Admin Tool from Start > Programs > ESP Enterprise > ESP Administration Tool.
2. Select the **Replication** tab.
3. Click the Refresh button to see the latest **Replication Graph**.
4. Select the IP Address of an ESP Server and then choose the desired replication time.

Extending the ESP License

When you first request your action site license, your query is archived with Trend Micro, Inc. and you are issued a license for a specific period of time. Before your license expires, ESP will warn you, giving you sufficient time to renew your license. When you are coming close to the expiration date, ESP will notify you using a Fixlet message. Similarly, if you start to exceed the number of ESP Agents allocated by your license, ESP will alert you. To extend your license expiration or add new ESP Agent licenses to your installation, follow these steps:

1. Notify your ESP support technician (if you have not paid for the extended license, you will need to talk to your sales person or reseller to buy an extended license).
2. Your server will check daily for a new version of your license. If you would like to force your server to check right away, go in the ESP Console to the **ESP Management** domain, click on the **License Overview** node, and click the **Check for license update** button.

Recreating Site Credentials

Private/public key encryption creates a chain of signing authority from the ESP root down through the ESP Site Administrator and including each ESP Console operator. If you lose your site credential or change the IP address of your ESP Server, the chain is broken. The consequences are serious: you must start over with a new request to Trend Micro, Inc. for a site certificate. Then you must re-install the entire system, including all the ESP Agents (contact your support technician for details on how you might migrate your ESP Agents to a new ESP Server) and re-create all the users. If this happens, please contact your support technician. To protect your site certificate, obey these important rules:

- **Do not lose the private key for your site** (saved in the file named **license.pvk**). Follow standard procedures for backing up and securing critical confidential information.
- **Do not change the IP address/hostname or port number of the ESP Server**, since it is the primary identifier for your site certificate. Any change to the IP address or port number that was specified when the license was requested negates the license and will necessitate a fresh installation of the ESP system. If you plan to decommission an ESP Server, be sure to apply the same IP address and port number to the replacement server.
- **Do not forget your password.** Follow your corporate standards for noting and storing your password.

Note: The ESP Site Administrator can change the password of the site-level key, provided he or she knows the current password.

Updating the ESP Software

Like the other software installations in your enterprise, the ESP program itself will need to be maintained and updated on occasion. Fortunately, that capacity is built into the system. To guarantee that you are running the latest version of ESP, be sure to install the ESP Agent on all ESP Server and ESP Console computers. Whenever an update is issued, a Fixlet message will be delivered to you with everything you need to install the update. If, for whatever reason, you do not wish to use the Fixlet messages to automatically update the ESP components, you can choose to manually update each ESP component. Instructions on how to do this will be included in the upgrade Fixlet message or will be available from your support technician.

ESP Announcements

ESP maintains a mailing list to announce new products, updates, informational notices, and other information useful to ESP Administrators. ESP highly recommends that all ESP customers subscribe to the ESP Administrator announcements mailing list at: http://bigmail.bigfix.com/mailman/listinfo/besadmin-announcements.

Changing the Agent Icon

By default, the icon in the upper left corner of the Agent UI is the ESP logo. This same icon appears in the tray when an Action is pending and in the task bar when the program is running. You can change this icon to help you clarify to your end users who is the source of the action, and also to comply with corporate branding and trademark requirements. Here is how to change the icon:

1. Run the ESP Administration Tool (**Start > Program Files > ESP Enterprise > ESP Administration Tool**).
2. Click the **System Options** tab.
3. Click the **Change Icon** button and use the **Open** dialog to browse for your icon (.ico) file.
4. The Administration Tool will immediately propagate this graphic to the Agents, but it will not be incorporated into the interface until the Agent restarts. After that, when a Agent interface appears (in response to an action, a dashboard or an offer), it will include the graphic icon you specified.

Maintaining and Troubleshooting ESP

If you are subscribed to the Patches for Windows site, you will be able to ensure that you have the latest upgrades and patches to your SQL Server database servers. That means that you must install the ESP Agent on all your computers, including the ESP Server and ESP Console computers. In addition, you may want to take advantage of these other tools and procedures:

- If you have the SQL Server installed, you should become familiar with the **MS SQL Server Tools**, which can help you keep the database running smoothly.
- It is standard practice to back up your database on a regular schedule, and the ESP database is no exception. It is also wise to run the occasional error-check to validate the data.
- If you start to notice any performance degradation, check for fragmentation. ESP writes out many temporary files, which may create a lot of disk fragmentation, so defragment your drive when necessary. Of course, regular maintenance also involves running the occasional error-check on your disk drives as well.
- The **ESP Diagnostics Tool** performs a complete test on the server components and can be run any time you experience problems. See the section on **Running the ESP Diagnostics Tool** (page 39).
- Check the **ESP Management** domain often. There are a number of Fixlets available that can detect problems with any of your ESP components. This can often head off problems before they ever affect your network.
- Check the ESP Knowledge Base at http://support.bigfix.com/. This site is continually updated, and if you cannot find an existing knowledge-base article about your question, you can find information on how to submit a question to a Trend Micro support technician.
- Add ESP Relays to improve the overall system performance and pay close attention to them. Healthy ESP Relays are key to a healthy ESP deployment.
- Review the **Deployment Health Checks** dashboard in the **ESP Management** domain for optimizations and failures.
- Set up monitoring activities on the ESP Server(s) to notify you in the event of a software or hardware failure, including:

    - ESP Server powered off or unavailable
    - Disk failure
    - Event log errors about ESP Server applications
    - ESP Server services states
    - FillDB buffer directory data back-up situations

Part Five

Resources

Deployment Scenarios

The next few pages contain deployment scenarios that illustrate some basic configurations taken from actual case studies. Your organization will look similar to one of the examples below, depending on the size of your network, the various bandwidth restrictions between clusters and the number of Relays and Servers. The main constraint is not CPU power, but bandwidth.

Pay careful attention to the ESP Relay distribution in each scenario. Relays provide a dramatic improvement in bandwidth and should be thoughtfully deployed, especially in those situations with thin pipes.

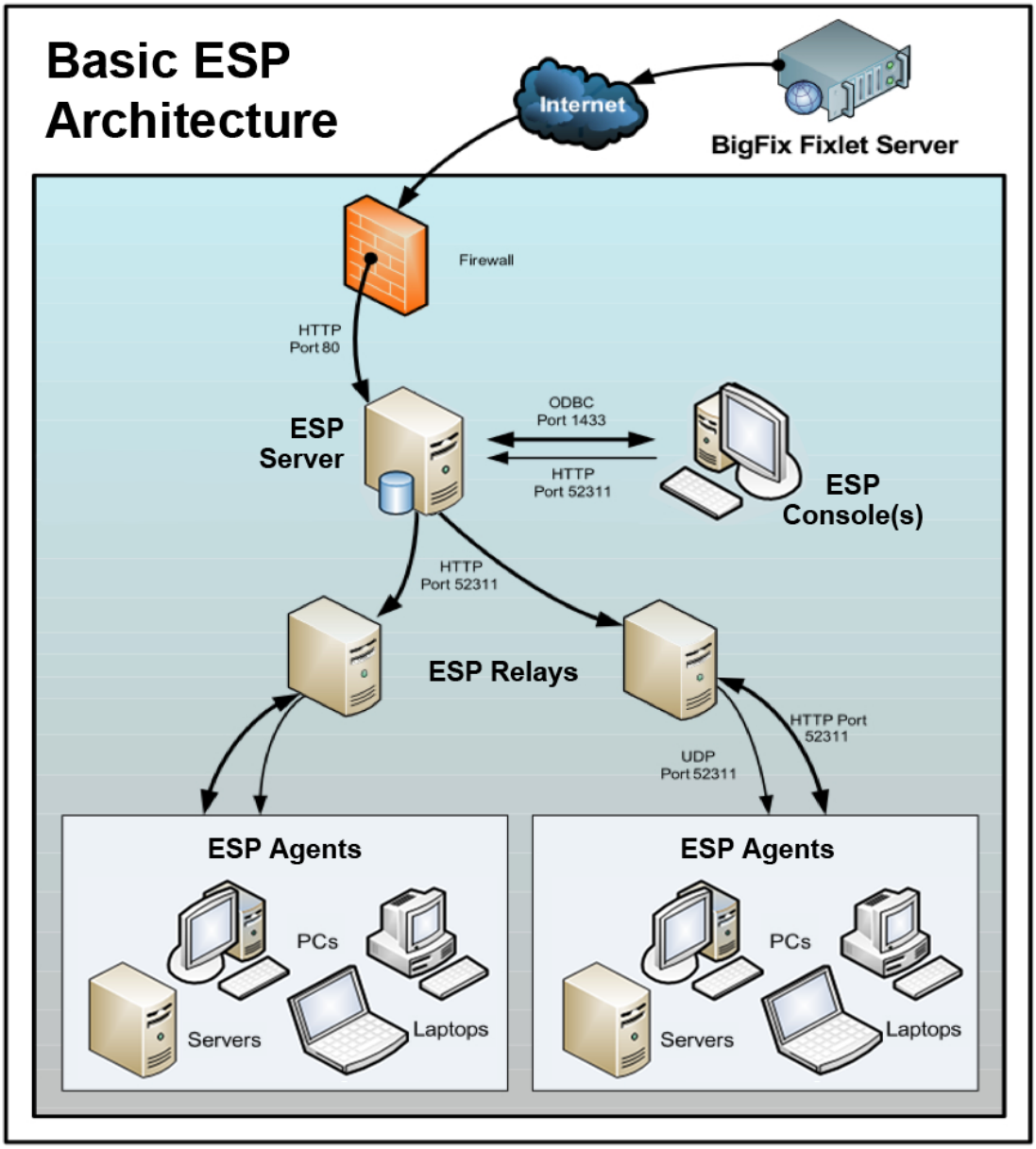
ESP Relays are generally most efficient in fairly flat hierarchies. A top-level ESP Relay directly eases the pressure on the ESP Server, and a layer under that helps to distribute the load. But hierarchies greater than two tiers deep may be counterproductive and must be carefully deployed. Multiple tiers are generally only necessary when you have more than fifty ESP Relays. In such a case, the top tier ESP Relays would be deployed on dedicated servers which would service anywhere from 50-200 second-tier ESP Relays. The following examples will help you deploy the most efficient network layout.

Notice that additional ESP Servers can also add robustness to a network, by spreading the load and supplying redundancy. Using redundant ESP Servers allows failbacks and failovers to be automated, providing minimal data loss, even in catastrophic circumstances.

With the proper deployment of ESP Servers and ESP Relays, networks of any size can be accommodated. Beyond the examples we present here, your ESP support technician will be happy to help you with other configurations.

Basic Deployment

This is a vastly simplified deployment designed to point out the basic hierarchy and the ports used to connect the components.



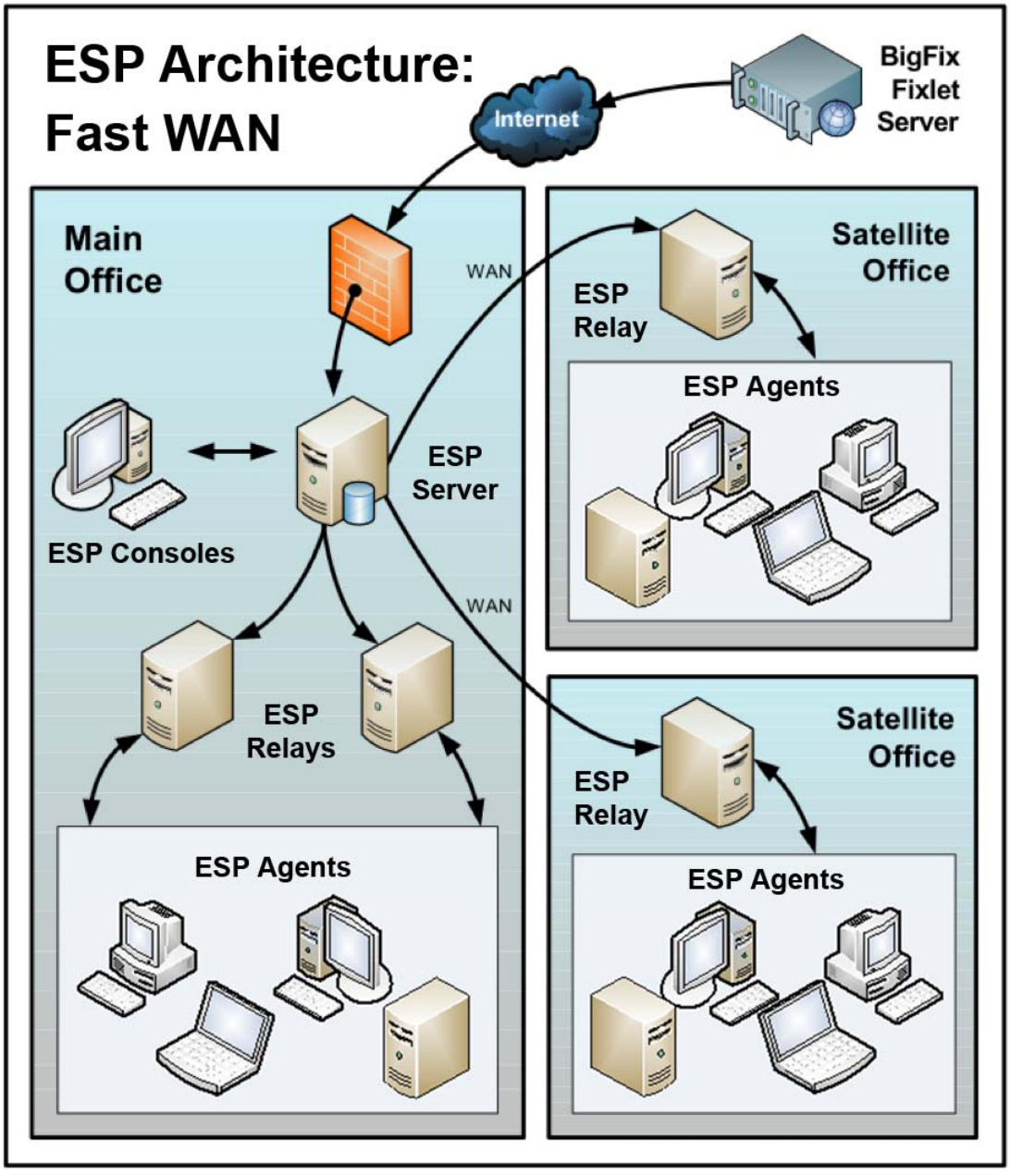
Note the following about the diagram:

- Port 80 is used to collect Fixlet messages over the Internet from Fixlet providers such as Trend Micro.
- A dedicated port (defaulting to 52311) is used for HTTP communications between ESP Servers, Consoles, Relays and Agents.
- You need both an ODBC and an HTTP connection to run the ESP Console.
- ESP Relays are used to share the server load. This diagram only shows two ESP Relays, but you can use dozens or even hundreds of ESP Relays in a similar flat hierarchy. Typically an ESP Relay is deployed for every 500-1,000 computers.
- The ESP Relays require an HTTP port (defaulting to 52311) to communicate with the ESP Agents.
- The ESP Relays can also take advantage of a UDP port to alert the ESP Agents about updates, but this is not strictly necessary.
- The ESP Agents are typically PCs or Workstations, but can include other servers, dockable laptops and more. Any device that can benefit from patches and updates is a candidate to include in the ESP deployment.

ESP has far greater flexibility and potential than this simple case suggests. It is capable of overseeing hundreds of thousands of computers, even if they are spread out around the world. The next scenarios build on this basic deployment.

Main Office with Fast-WAN Satellites

This configuration is common in many universities, government organizations, and smaller companies with only a few geographical locations. This type of deployment is relatively easy to set up and administer because there are no (or very few) slow WAN pipes to worry about.

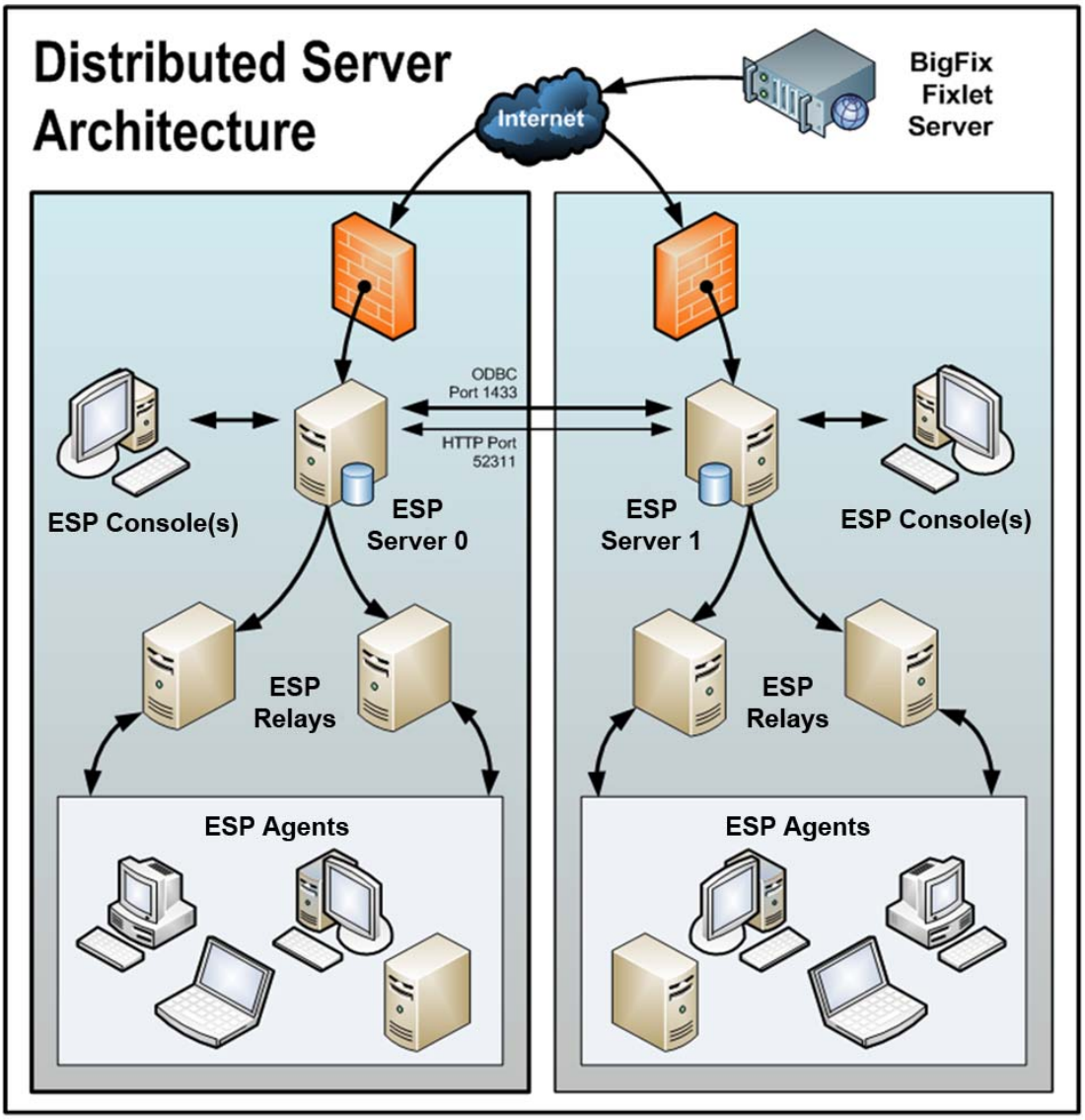


Note the following about the diagram:

- In this configuration, the ESP Relays are used both to relieve the ESP Server and to distribute the communications, optimizing the bandwidth.
- This scenario has large WAN pipes, so office relays can communicate directly to the main ESP Server. A thin WAN could force a change in the layout of the ESP Relays (see the scenarios above and below).
- The more ESP Relays in the environment, the faster the downloads and response rates.
- Because of the nature of this network, when the ESP Agents are set to **Automatically Locate Best ESP Relays**, many of the ESP Relays are the same distance away. In this scenario, the ESP Agents automatically load-balance themselves amongst all the ESP Relays that are nearby.
- For this high-speed LAN, a relatively flat hierarchy is recommended, with all ESP Relays reporting directly to the main ESP Server. Any extra levels in the hierarchy would only introduce unnecessary latency. However, if there were over 50-100 ESP Relays in this environment, another level of ESP Relays should be considered.

Distributed Server Architecture Setup

Companies with sensitive or high availability needs will want to deploy multiple, fully-redundant servers to maintain continuous operation even in the face of serious disruptions. Multiple ESP Servers also help to distribute the load and create a more efficient deployment. Here is a bare-bones diagram of how multiple servers might be set up in a single location or in two widely separated offices:

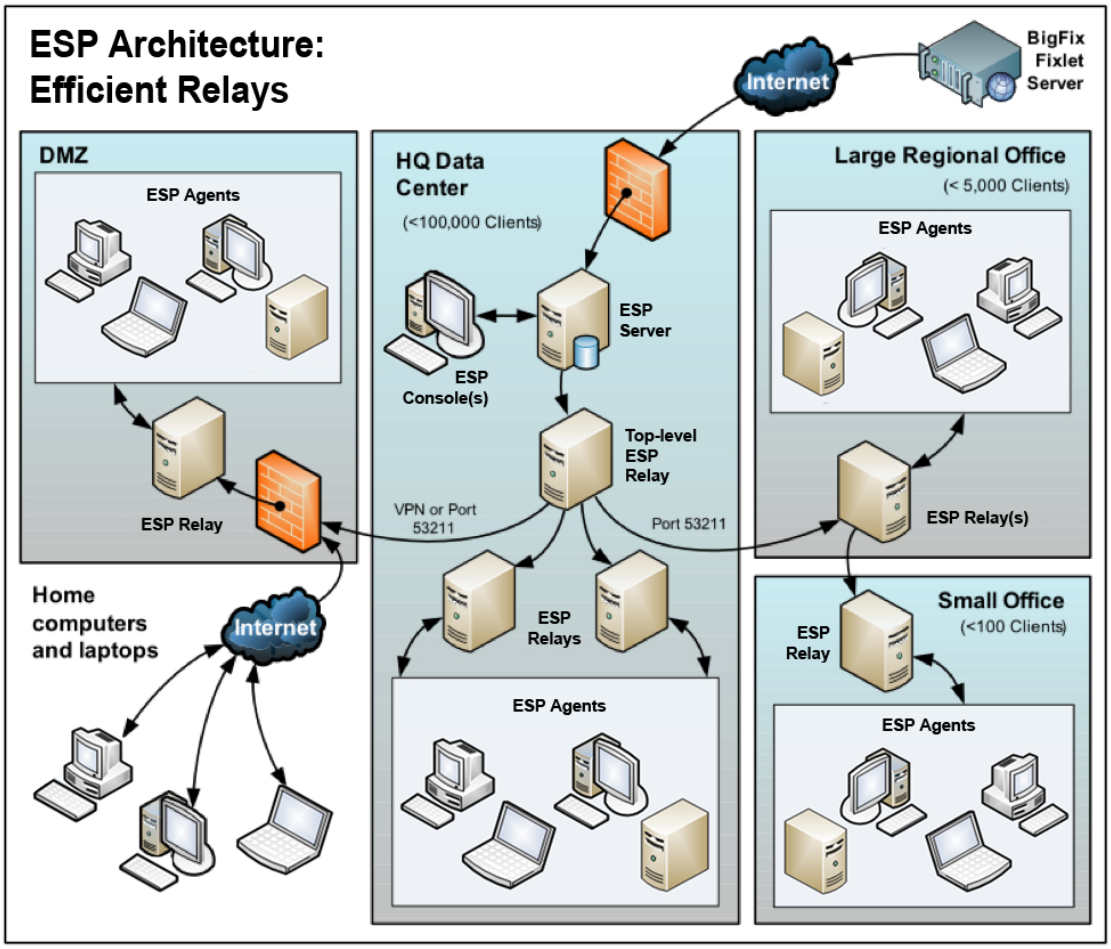


Note the following about the diagram:

- The ESP Servers are connected by a fast WAN, allowing them to synchronize several times per hour.
- The servers need both an ODBC and an HTTP link to operate and replicate properly.
- There is a primary ESP Server with an ID of 0 (zero). It is the first ESP Server that you install, and it is the default server for running ESP Administration.
- For the sake of clarity, this is a minimal configuration. A more realistic deployment would have a top-level ESP Relay and other WAN connections to regional offices.
- The ESP Servers and Relays are configured so that control can be automatically routed around a server outage (planned or otherwise), and upon failover reconnection, the databases will be automatically merged.
- The ESP Servers communicate on a regular schedule to replicate their data. You can review the current status and adjust the replication interval through ESP Administration > Replication. For the best possible performance, these pipes should be fat.
- This diagram only shows two ESP Servers, but the same basic architecture would apply to each additional server. With multiple servers, a shortest-path algorithm is used to guide the replication.
- When an outage or other problem causes a network split, it is possible to for a custom Fixlet or a retrieved property to be modified independently on both sides of the split. When the network is reconnected on failover, precedence will go to the version on the server with the lowest ESP Server ID.

Efficient ESP Relay Setup

To increase efficiency and reduce latency, this company has set up a hierarchy of ESP Relays to help relieve the server load. Each ESP Relay they add takes an extra burden off the ESP Server for both patch downloads and data uploads. Setting up ESP Relays is easy, and the ESP Agents can be set to automatically find the closest relay, further simplifying administration.

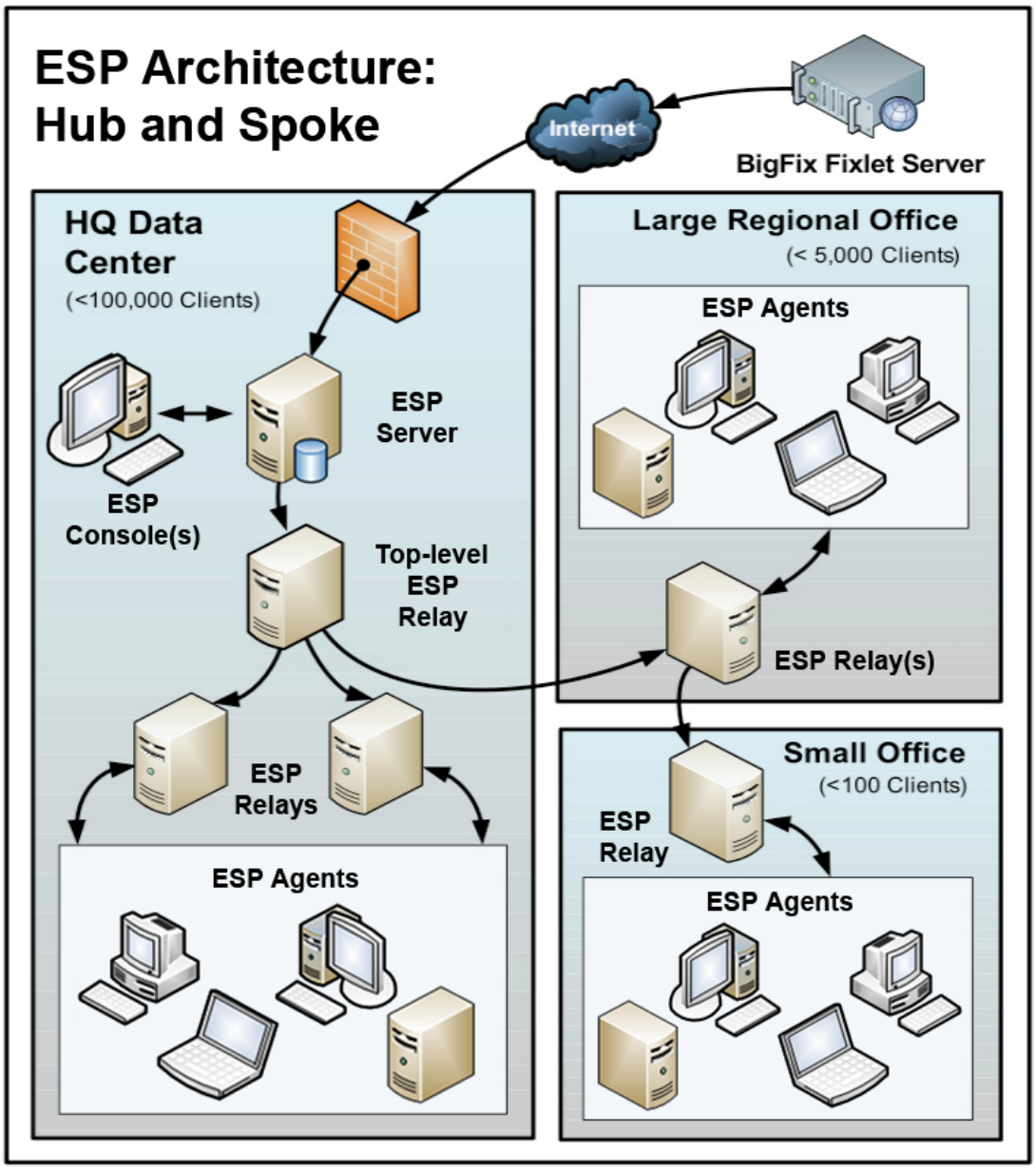


Note the following about the diagram:

- There is a dedicated server computer known as the Top-Level ESP Relay that is used to take the load off of the ESP Server computer.
- All ESP Relays are manually configured to point to either the top level ESP Relay or to another ESP Relay that is closer. The general rule for configuring ESP Relays is that you want as few levels as possible to the ESP Relays unless there is a bandwidth bottleneck. Communications over thin pipes should be relay to relay. The top-level ESP Relay will relieve the ESP Server, and the secondary ESP Relay can allow a single download to be distributed over hundreds of ESP Agents.
- There is an ESP Relay in the DMZ set up with a special trust relationship with the ESP Server. This ESP Relay will allow ESP Agents in the DMZ or on the public Internet to be managed by ESP. The DMZ places a security firewall between the ESP Relay and the set of home computers and laptops reporting in from the Internet.
- This diagram shows a single ESP Relay in the large regional office. However, for offices with more than a few hundred Agents, there will typically be multiple ESP Relays to effectively distribute the load.
- As a general rule, you should deploy at least one ESP Relay per 500-1000 ESP Agents to maximize the efficiency of the ESP Relay. See the article on relays at the Trend Micro support site for more information.

Hub and Spoke

This scenario involves a main data center, a small number of large regional offices and many small regional offices. This configuration is common in large international organizations. The ESP Agents are installed on computers in offices all around the world. Many of these locations have slow WAN connections (8 kbps-512 kbps), but there will be many offices with faster WAN connections (1mbps-45mbps).



Often these locations are configured in a hub-and-spoke arrangement. This scenario builds on the previous one, but the hub-and-spoke configuration permits more levels in the ESP Relay hierarchy.
Note the following about the diagram:

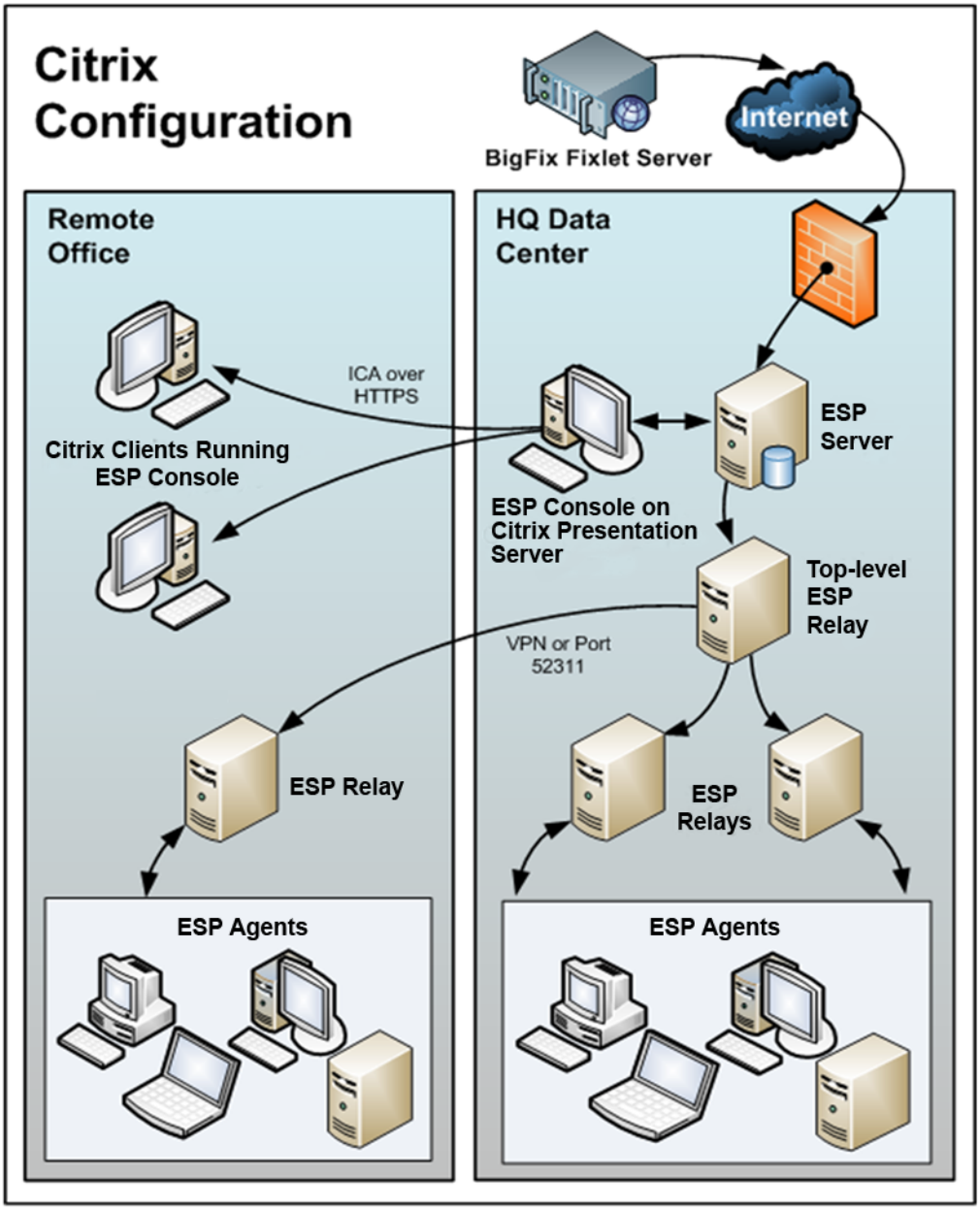
- In this scenario, the ESP Relays are carefully deployed at the proper junctions within the WAN to optimize bandwidth. Poor placement of ESP Relays can adversely impact your network performance.
- It is vital that at least one ESP Relay is installed in every location with a slow WAN connection. Often a company will already have a server in just such a spot, acting as a file server, print server, AV distribution server, SMS distribution server or domain controller, or any other computer. The ESP Relay is usually installed on these existing computers.
- To provide redundancy in a typical office, more than one ESP Relay should be installed. In case an ESP Relay fails for any reason (powered down, disconnected from the network, etc.), its attached ESP Agents can then automatically switch-over to a different ESP Relay. A redundant relay is less important in very small offices because fewer computers are affected by the failure of an ESP Relay.
- When the ESP Agents are set to **Automatically Locate Best ESP Relays**, they will choose the closest one. If any ESP Relay should fail, the ESP Agents will automatically seek out another ESP Relay. You should monitor the ESP Relay configuration after the initial automated setup (and periodically after that) to ensure that the ESP Agents are pointing to appropriate locations. Talk to your support technician for more details on how to protect against overloading WAN pipes with ESP data.
- Bandwidth throttling at the ESP Relay level is very helpful in this configuration. The ESP Relays are set up to download slowly across the WAN pipes so as not to saturate the slow links. See the article on throttling at the Trend Micro support site for more information.
- Instead of pointing to the main ESP Server, the ESP Relays are configured to point to the top level ESP Relay. This frees up the ESP Server to couple more tightly to the ESP Console and improves reporting efficiency.

The ESP Relays will be configured to manually create the optimal hierarchy. The hierarchy will have three levels (from the top down):

1. The top-level ESP Relay that connects directly to the ESP Server.
2. The regional office ESP Relays that connect to the top-level ESP Relay.
3. Multiple branch office ESP Relays that connect to specified regional office ESP Relays.

Remote Citrix / Terminal Services Configuration

Although ESP can efficiently deliver content even over slow connections, the ESP Console itself is data intensive and can overwhelm a link slower than 256 kbps. Adding more ESP Agents further increases the lag time. However, you can access the ESP Console remotely from a Citrix, Terminal Services, VNC or Dameware-style presentation server and realize excellent performance. Here is what this configuration looks like:



Note the following about the diagram:

- In the main office, the ESP Console is set up on a computer that is close to the ESP Server for fast data collection. This will be your Presentation Server.
- You must create user accounts for each remote user. These users will then be able to access the ESP Console quickly because the time-critical data loading is done at the main office over a fast link.
- Your remote connection can be over HTTPS to improve security.
- Note that running an ESP Console from a Presentation Server containing the private key is inherently less secure than if the key is stored on a removable drive.
- You may be able to benefit from load-balancing software to spread the remote accesses across multiple servers.
- The main bottleneck for an ESP Console running on Citrix is memory size. If the ESP Console runs out of memory, its performance will drop sharply. A good technique to determine the memory requirement is to open up the ESP Console as a Master Operator. Check the memory used: this will indicate the maximum memory requirement per user. Then log in as a typical operator and use this as your average memory requirement. If your Citrix server can support all concurrent users with the maximum memory then a single box will suffice. If not, then use the average memory requirement per user to determine how many extra Citrix servers you may need.
- The second constraint is CPU power. During refreshes, the ESP Console works best with a full CPU core. That means the Presentation server will be optimized with one CPU core running the ESP Console for each concurrent user.
- The final concern is disk space for the ESP Console cache. You can get a feel for the size of the cache by looking at an example on your local box: C:\Documents and Settings\<USERNAME>\Local Settings\Application Data\BigFix\Enterprise Console\ESP_bfenterprise. There should be enough disk space to provide one cache file for each ESP Console operator.

Glossary

Action Password—See ESP signing password.
ESP—See Endpoint Security Platform.
ESP Agent—Software installed on each networked computer to be managed under ESP. The Agent accesses a pool of Fixlet messages, checks the computer it is installed on for vulnerabilities, and sends the ESP Server a message when such a condition occurs.
ESP Console—A management program that provides an overview of the status of all the computers with the ESP Agent installed in the network, identifying which might be vulnerable and offering corrective actions.
ESP database—A component of the ESP system that stores data about individual computers and Fixlet messages. The ESP Server's interactions primarily affect this database, which runs on SQL Server.
ESP Generator Install folder—The directory on the installation computer where the Generator places the installation files for the ESP system.
ESP Installation Generator—An application that creates installers for the core ESP system components.
ESP Relay—This is an ESP Agent that is running special server software. Relays spare your server and the network by minimizing direct server-Agent downloads and by compressing upstream data. Relays are automatically discovered by ESP Agents, which dynamically choose the best Relay to connect to.
ESP Root Server—Refers to the HTTP or HTTPS services offered by the main ESP Server as an alternative to IIS. The ESP Root server is specially tuned to Fixlet traffic and is more efficient than IIS for this application.
ESP Server—A collection of interacting applications (web server, CGI-BIN, and database server) that coordinates the relay of information to and from individual computers in the ESP system. The server processes may be hosted by a single server computer or segmented to run on separate server computers or replicated on redundant servers.
ESP signing password—The password (specified when the ESP system was installed) used by an ESP Console operator to sign an action for deployment. It is called the *action* password in the Console interface.
ESP Site Administrator—The person in charge of installing ESP and authorizing ESP Console operators.
ESP system install folder—The directory on the ESP Server where the ESP Server and related files (including Console and Agent installers) will be installed.
BigFix Action Scripting Language—The language used for crafting action scripts. Action can be crafted in different scripting languages, including AppleScript and Unix shells.
BigFix Development Environment (BDE)—An integrated system for authoring and deploying, or publishing, Fixlet messages.
Endpoint Security Platform (ESP)—A preventive maintenance tool for enterprises that monitors computers across networks to find and correct vulnerabilities with a few simple mouse-clicks.
BigFix Relevance Language—The language in which relevance clauses are written.

Custom Site—You can create your own custom content and host it in a custom site. This can only be done by a Master Operator that has been granted the rights to create custom content (use the ESP Admin program to allocate these users).
DSA—Distributed Server Architecture. Multiple ESP Servers are linked to provide full redundancy in case of failure.
Fixlet message—A mechanism for targeting and describing a problematic situation on a computer and providing an automatic fix for it.
Fixlet servers—Web servers offering Fixlet site subscriptions. They can be either internal to the enterprise network or external to the network (if direct external web access is allowed).
Fixlet site—A trusted source from which the ESP Agent obtains Fixlet messages.
installation computer—A secure computer (separate from the ESP Server computer) that hosts and runs the ESP Installation Generator.
Management Rights—Ordinary ESP Console Operators can be limited to a specified group of computers. These limits represent the management rights for that user. Only an ESP Site Administrator or a Master Operator can assign management rights.
Master Operator—An ESP Console Operator with administrative rights. A Master Operator can do almost everything an ESP Site Administrator can do, with the exception of creating new operators.
masthead—Files containing the parameters of the ESP process, including URLs that point to where trusted Fixlet content is available. The ESP Agent brings content into the enterprise based on subscribed mastheads.
Mirror server—A server required in the ESP system if the enterprise does not allow direct web access but instead uses a proxy server that requires password-level authentication.
Operator—A person who operates the ESP Console. Ordinary operators can deploy Fixlet actions and edit certain computer settings. Master Operators have extra privileges, among them the ability to assign management rights to other operators.
signing password—See ESP signing password.
Site Administrator —The only ESP Console Operator with the right to create new Operators.
SQL server—A full-scale database engine from Microsoft that can be acquired and installed into the ESP system to satisfy more than the basic reporting and data storage needs. A step up from SQLite .
standard deployment—A deployment of ESP that applies to workgroups and to enterprises with a single administrative domain. It is intended for a setting in which all ESP Agent computers have direct access to a single internal server.
VPN—Virtual Private Network. An encrypted channel (or tunnel) that allows companies to extend their local-area networks across the world by using an inexpensive Internet connection.
WAN—Wide-area network. Many offices are connected by WAN. The bandwidth of your WAN determines the placement of ESP Relays in your deployment, with thin WANs requiring more relays to aggregate downloads and reduce overhead.

Global Support

Trend Micro offers a suite of support options to help optimize your user-experience and success with this product. Here's how it works:

- First, check the Trend Micro website Documentation page
- Next, search the ESP Knowledge Base for applicable articles on your topic
- Then check the User Forum for discussion threads and community-based support

If you still can't find the answer you need, contact Trend Micro's support team for technical assistance:

- Phone/US: +1 (408) 257-1500
- Email: support@support.trendmicro.com

Index

D

E

F

G

O

P

R

S

