



Intrusion Defense Firewall 1.5

Advanced threat protection for Endpoints

for OfficeScan Client/Server Edition

Deployment Guide



Endpoint Security

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, review the readme files, release notes, and the latest version of the applicable user documentation, which are available from the Trend Micro Web site at:

<http://www.trendmicro.com/download>

Trend Micro, the Trend Micro t-ball logo, Intrusion Defense Firewall, OfficeScan, and TrendLabs are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright© 2011 Trend Micro Incorporated. All rights reserved.

Release Date: September 2011

Document part number: OSEM15026/110817

The Installation Guide for Trend Micro™ Intrusion Defense Firewall™ is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the online Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Evaluate this documentation on the following site:

<http://www.trendmicro.com/download/documentation/rating.asp>

Contents

Preface

| | |
|--|------|
| Audience | viii |
| Intrusion Defense Firewall Documentation | ix |
| Document Conventions | x |
| About Trend Micro | x |

Chapter 1: About Intrusion Defense Firewall

| | |
|--|-----|
| Server Plug-in | 1-1 |
| Dashboard | 1-2 |
| Monitoring Tools | 1-2 |
| List of Computers | 1-2 |
| Security Profiles | 1-2 |
| Firewall Rules | 1-2 |
| DPI (Deep Packet Inspection) Rules | 1-3 |
| Stateful Configurations | 1-3 |
| Reusable Components | 1-3 |
| Location Awareness | 1-4 |
| Bridging Attack Protection | 1-4 |
| Client Plug-in | 1-4 |
| System Requirements | 1-4 |
| Server Plug-in | 1-4 |
| Client Plug-in | 1-5 |
| What's New in Intrusion Defense Firewall 1.5 | 1-6 |
| Performance and Scalability | 1-6 |
| Automatic Computer Activation and Protection | 1-6 |
| Expanded OfficeScan Corporate Edition (OSCE) Support | 1-6 |
| Event Tagging | 1-6 |

| | |
|---|-----|
| Expanded Platform and File System Support | 1-6 |
|---|-----|

Chapter 2: Installation

| | |
|---|------|
| Installing Intrusion Defense Firewall | 2-2 |
| 1. Download Intrusion Defense Firewall | 2-2 |
| 2. Install Intrusion Defense Firewall | 2-3 |
| Upgrading the Server Plug-in | 2-4 |
| Activating the Intrusion Defense Firewall Server Plug-in | 2-5 |
| 1. Install Security Certificates | 2-5 |
| 2. Type Your Activation Code | 2-5 |
| Installing the IDF Server Components with a Local Update Source | 2-6 |
| Installing the Intrusion Defense Firewall Client Plug-in | 2-8 |
| Deploy the Client Plug-in | 2-8 |
| Optionally Use the Standalone Client Plug-in Installer | 2-8 |
| Transitioning from the OfficeScan Firewall | 2-10 |
| 1. Modify OfficeScan Firewall Configuration | 2-10 |
| 2. Assign Appropriate Security Profiles to the Computers | 2-11 |
| 3. Edit the Domain Controllers IP List | 2-12 |
| 4. Disable the Native OfficeScan Firewall | 2-12 |
| Creating Your Own SSL Authentication Certificate | 2-12 |
| Uninstalling Intrusion Defense Firewall | 2-15 |
| Client Plug-in | 2-15 |
| Server Plug-in | 2-16 |
| Scaling IDF for Large Installations | 2-16 |

Chapter 3: Troubleshooting

| | |
|----------------------|-----|
| Server Plug-in | 3-1 |
| Client Plug-in | 3-5 |

Chapter 4: Frequently Asked Questions

| | |
|--------------------|-----|
| General FAQs | 4-1 |
|--------------------|-----|

IDF Database FAQs 4-4

Index



Preface

Welcome to the *Trend Micro™ Intrusion Defense Firewall™ 1.5 Deployment Guide*. This guide helps you to get “up and running” by introducing Intrusion Defense Firewall (IDF), assisting with deployment, installation, migration (if necessary), initial configuration, and troubleshooting.

This preface describes the following topics:

- *Audience on page viii*
- *How to Use this Guide on page viii*
- *Intrusion Defense Firewall Documentation on page ix*
- *Document Conventions on page x*
- *About Trend Micro on page x*

Audience

The Intrusion Defense Firewall documentation is intended for OfficeScan Administrators who are responsible for OfficeScan management. These users are expected to have in-depth knowledge of networking, server management, and OfficeScan.

How to Use this Guide

This guide contains the information you need to understand and use Intrusion Defense Firewall.

| | |
|--|--|
| Chapter 1, <i>About Intrusion Defense Firewall</i> | This chapter introduces Intrusion Defense Firewall, system requirements, and what's new in the current version. |
| Chapter 2, <i>Installation</i> | This chapter describes how to install the application, how to activate the Server Plug-in and Client Plug-in, transitioning from the native OfficeScan Firewall to Intrusion Defense Firewall, how to create your own SSL Authentication Certificate, and uninstalling Intrusion Defense Firewall. |
| Chapter 3, <i>Troubleshooting</i> | This chapter describes how to troubleshoot the Server Plug-in and Client Plug-in installations. |
| Chapter 4, <i>Frequently Asked Questions</i> | This chapter provides answers to frequently asked questions about general deployment issues and about the IDF database. |

Intrusion Defense Firewall Documentation

Intrusion Defense Firewall documentation includes the following:

TABLE P-1. OfficeScan documentation

| DOCUMENTATION | DESCRIPTION |
|-----------------------|--|
| Deployment Guide | A PDF document that discusses requirements and procedures for installing the IDF Server Plug-in, upgrading the Server Plug-in, and installing the IDF Client Plug-in |
| Administrator's Guide | A PDF document that discusses getting started information, IDF Client Plug-in installation procedures, and IDF Server Plug-in and Client Plug-in management |
| Help | HTML files that provide "how to's", usage advice, and field-specific information. The Help is accessible from the IDF Server Plug-in user interface. |
| Readme file | Contains a list of known issues and basic installation steps. It may also contain late-breaking product information not found in the Help or printed documentation. |
| Knowledge Base | An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following Web site: http://esupport.trendmicro.com/support |

Download the latest version of the PDF documents and readme at:

<http://www.trendmicro.com/download>

Document Conventions

To help you locate and interpret information easily, the Intrusion Defense Firewall documentation uses the following conventions.

TABLE 1-1. Document Conventions

| CONVENTION | DESCRIPTION |
|-----------------|--|
| ALL CAPITALS | Acronyms, abbreviations, and names of certain commands and keys on the keyboard |
| Bold | Menus and menu commands, command buttons, tabs, options, and ScanMail tasks |
| <i>Italics</i> | References to other documentation |
| Monospace | Examples, sample command lines, program code, Web URL, file name, and program output |
| <u>Note:</u> | Configuration notes |
| <u>Tip:</u> | Recommendations |
| <u>WARNING!</u> | Reminders on actions or configurations that should be avoided |

About Trend Micro

Trend Micro, Inc. is a global leader in network antivirus and Internet content security software and services. Founded in 1988, Trend Micro led the migration of virus protection from the desktop to the network server and the Internet gateway-gaining a reputation for vision and technological innovation along the way.

Today, Trend Micro focuses on providing customers with comprehensive security strategies to manage the impacts of risks to information, by offering centrally controlled server-based virus protection and content-filtering products and services. By protecting

information that flows through Internet gateways, email servers, and file servers, Trend Micro allows companies and service providers worldwide to stop viruses and other malicious code from a central point, before they ever reach the desktop.

For more information, or to download evaluation copies of Trend Micro products, visit our award-winning Web site:

<http://www.trendmicro.com>



About Intrusion Defense Firewall

Intrusion Defense Firewall for OfficeScan Client/Server Edition provides earlier, stronger endpoint protection by supplementing highly effective OfficeScan client-level security with network-level Host Intrusion Defense.

Intrusion Defense Firewall enables you to create and enforce security policies that protect sensitive data, applications, computers, or network segments. The server component (“Server Plug-in”) is installed on the OfficeScan server. It deploys and manages the client component (“Client Plug-in”) on OfficeScan clients.

This chapter describes the following:

- *Server Plug-in on page 1-1*
- *Client Plug-in on page 1-4*
- *System Requirements on page 1-4*
- *What's New in Intrusion Defense Firewall 1.5 on page 1-6*

Server Plug-in

The Server Plug-in is a management system embedded within the OfficeScan Web console. It allows administrators to create and manage comprehensive intrusion defense security policies, track threats, and log preventive actions taken in response to these threats.

Dashboard

The Server Plug-in Dashboard provides:

- Extensive system, event and computer reporting, with drill-down capabilities.
- Graphs of key metrics with trends, with drill-down.
- Detailed event logs, with drill-down.
- Ability to save multiple dashboard layouts.

Monitoring Tools

Monitoring tools include event viewers for Firewall, Deep Packet Inspection (DPI), and System Events as well as a selection of reports summarizing recent activity.

List of Computers

The client tree structure on the Computers screen and on the OfficeScan Web console's Networked Computers screen are the same. The list displayed in the Server Plug-in is the list used to apply the various rules, filters, and stateful configurations of Intrusion Defense Firewall.

Security Profiles

Security profiles are policy templates that let you configure and specify the security rules that are applied to one or more computers. These compact, manageable rule sets make it simple to provide comprehensive security without the need to manage thousands of rules. Default security profiles provide the necessary rules for a range of common computer configurations, ensuring rapid deployment.

Firewall Rules

A sophisticated, bi-directional stateful firewall provides complete support for all network protocols, including TCP, UDP and ICMP. Firewall Rules are fully configurable to allow or deny traffic on a per-interface basis, and restrict communication to allowed IP or MAC addresses.

DPI (Deep Packet Inspection) Rules

Deep-packet inspection, which examines application data to and from the computer, shields software vulnerabilities from attack. DPI Rules allow, block, log, or edit data based on its content. DPI Rules protect vulnerabilities from known and unknown attacks by defining expected application data, and blocking malicious data based on its content.

Security Updates: Ongoing DPI Rule updates automatically provide the most current, comprehensive protection against known and unknown attacks.

Stateful Configurations

Intrusion Defense Firewall's Stateful Configuration mechanism analyzes each packet in the context of traffic history, correctness of TCP and IP header values, and TCP connection state transitions. In the case of stateless protocols like UDP and ICMP, Intrusion Defense Firewall implements a pseudo-stateful mechanism based on historical traffic analysis. The stateful mechanism handles packets as follows:

- A packet is passed to the stateful routine if it has been allowed through by the static Firewall Rule conditions,
- The packet is examined to determine whether it belongs to an existing connection by checking a connection table created by the stateful mechanism for matching end points, and
- The TCP header is examined for correctness (for example, sequence numbers and flag combinations.)

Reusable Components

Intrusion Defense Firewall makes use of independent sets of Application Types, IP Lists, MAC Address Lists, and Port Lists. These components can be used by multiple elements of the Intrusion Defense Firewall system (Firewall Rules, IPS Filters, Security Profiles, and so on) so that the same information does not have to be entered each time a new rule, filter, or profile is created.

Location Awareness

Rule Contexts are a powerful way of implementing different security policies depending on the Computer's network environment. Intrusion Defense Firewall uses Rule Contexts to create Security Profiles which apply different Firewall Rules to Computers (usually mobile laptops) depending on whether that Computer is in or away from the office.

Bridging Attack Protection

The Restricted Interfaces feature allows you to force a Computer to use only one network interface at any one time. This feature gives you the ability to prevent attackers from bridging between a wireless and a wired VPN connection and tunneling into your enterprise.

Client Plug-in

The Client Plug-in is a high performance, small footprint, software component installed on a Computer that has OfficeScan client installed. It applies the Security Profile (deployed by the Server Plug-in) to incoming and outgoing network traffic and monitors for protocol deviations or contents that might signal an attack. When necessary, the Client Plug-in intervenes and neutralizes the threat by either blocking or correcting the traffic.

System Requirements

Server Plug-in

- Memory: Minimum 2GB (4GB recommended)
- Disk Space: 1.5GB for install files, 4GB to 40GB for database
- Web Browser: Microsoft™ Internet Explorer™ 7+ (cookies enabled)
- Operating System: Microsoft Windows Server™ 2008 (32- and 64-bit), Microsoft Windows Server™ 2003 SP2 (32- and 64-bit), Microsoft Windows Server™ 2003 R2 (32- and 64-bit), Microsoft Windows Server™ 2003 R2 SP2 (32- and 64-bit), Microsoft Storage Server™ 2003 (SP2 or higher) (32- and 64-bit)

- Pre-requisites:
 - Trend Micro OfficeScan Server™ Corporate Edition 8.0+
 - Trend Micro OfficeScan Plug-in Server Plug-in™ 1.0 Patch 2 (build 1.0.3151) or later
 - Microsoft SQL Server™ 2005 (All Service Packs), Microsoft SQL Server™ 2008 (All Service Packs), Microsoft SQL Server™ 2008 R2 (All Service Packs), Microsoft SQL Server™ 2012 (All Service Packs)
 - Windows 2003: Microsoft .NET Framework™ 2.0 SP2 or higher and Microsoft Windows Installer 4.5 (Required for Microsoft SQL Server 2008 R2 Express™ Installation)
 - Windows 2008: Microsoft .NET Framework 2.0 SP2 or higher and Microsoft Windows Installer 4.5 (Required for SQL Server 2008 Express Installation)
 - Adobe™ Acrobat Reader™ 5+ (Required to read deployment guide)
-

Note: The Server Plug-in automatically installs the Microsoft SQL Server 2005/2008 Express provided within OfficeScan.

Note: Ports 4119 and 4120 must be open on the Server Plug-in machine.

Client Plug-in

- Memory: 384MB
- Disk Space: 100MB (200MB recommended, primarily for logging)
- Operating System: Microsoft™ Windows 7™ (32- and 64-bit), Windows 2008™ (32- and 64-bit), Windows 2008™ R2 (64-bit), Vista™ (32- and 64-bit), Windows Server 2003 R2™ (32- and 64-bit), Windows Server 2003 R2 SP2™ (32- and 64-bit), Windows XP™ (32- and 64-bit)

What's New in Intrusion Defense Firewall 1.5

Performance and Scalability

Intrusion Defense Firewall 1.5 brings increased overall performance and scalability by significantly improving the speed and efficiency of security update deployments, heartbeats, recommendation scans, memory usage, and the IDF Server Plug-in user interface.

Automatic Computer Activation and Protection

Tasks now let you automatically and conditionally activate and/or assign Security Profiles to computers that are added via Client Plug-in-initiated activation.

Expanded OfficeScan Corporate Edition (OSCE) Support

Intrusion Defense Firewall 1.5 supports the following OSCE features:

- OSCE 10.6 and PLM 2.0
- OSCE dashboard widgets
- OSCE mash-up widgets

Event Tagging

Event Tagging allows you to manually tag events with predefined or custom labels, which enables specialized views of events, dashboards, and reports that can be applied to a single event, similar events, or even to all future similar events.

Expanded Platform and File System Support

Intrusion Defense Firewall 1.5 supports the following client and server platforms:

- 32- 64-bit clients and servers
- Separate 32- and 64-bit client deployment
- FAT32 file system
- Multi-Language Support

- Operating System: Microsoft™ Windows 7™ (32- and 64-bit), Windows 2008™ (32- and 64-bit), Windows 2008™ R2 (64-bit), Vista™ (32- and 64-bit), Windows Server 2003 R2™ (32- and 64-bit), Windows Server 2003 R2 SP2™ (32- and 64-bit), Windows XP™ (32- and 64-bit)

Intrusion Defense Firewall 1.5 is available in multiple language versions. Please contact Trend Micro to find out what languages are available.



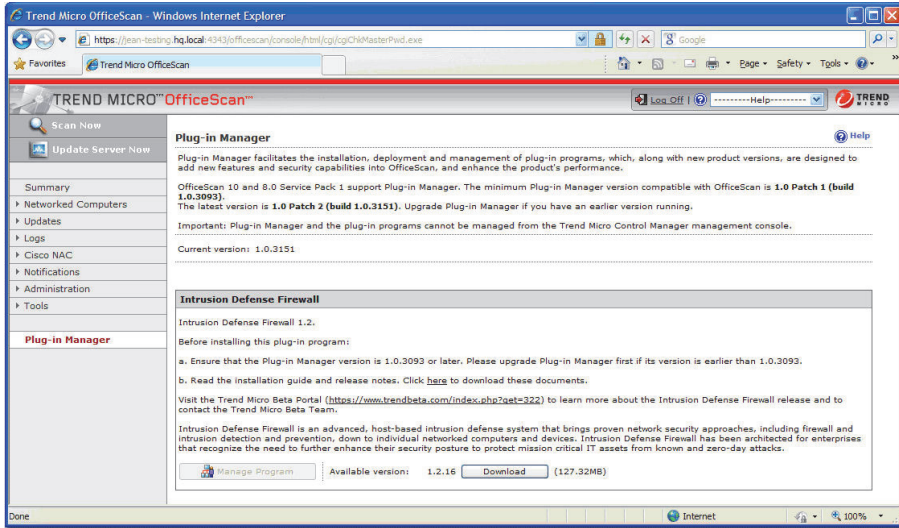
Installation

This chapter explains the following:

- *Installing Intrusion Defense Firewall on page 2-2*
- *Activating the Intrusion Defense Firewall Server Plug-in on page 2-5*
- *Installing the IDF Server Components with a Local Update Source on page 2-6*
- *Installing the Intrusion Defense Firewall Client Plug-in on page 2-8*
- *Transitioning from the OfficeScan Firewall on page 2-10*
- *Creating Your Own SSL Authentication Certificate on page 2-12*
- *Uninstalling Intrusion Defense Firewall on page 2-15*

Installing Intrusion Defense Firewall

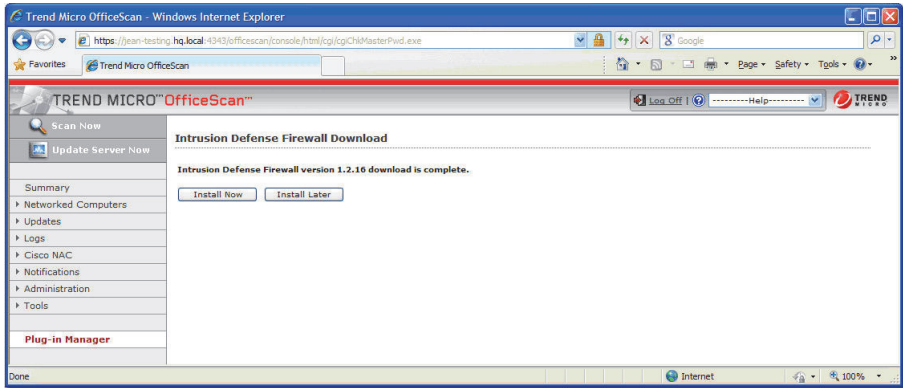
1. Download Intrusion Defense Firewall



From the OfficeScan Plug-In Manager, select **Intrusion Defense Firewall** and click **Download**.

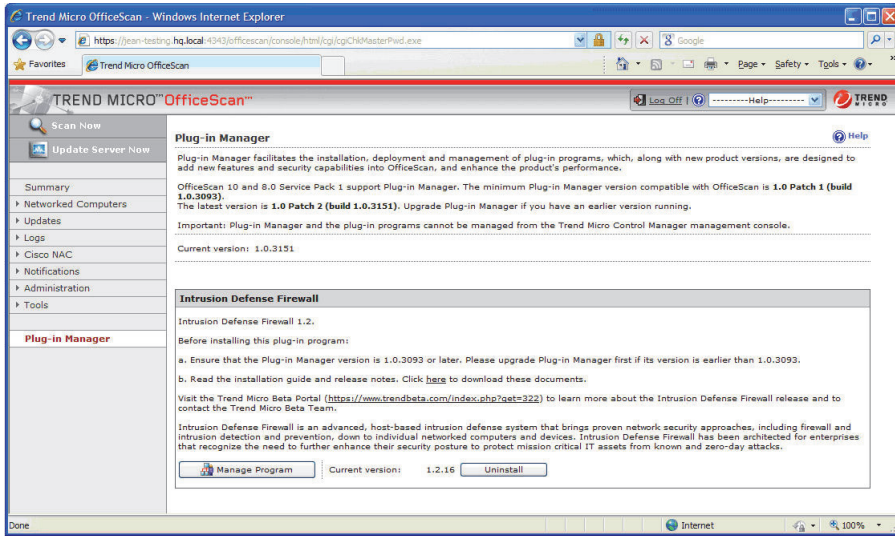
In the dialog box, click **OK** to confirm the download, and wait for the download to complete.

2. Install Intrusion Defense Firewall



Click **Install Now**. If you are performing a fresh install or renewing your license with a new Activation Code, you will be asked to accept the license agreement. Read and accept the license agreement to continue.

Note: The installation will take several minutes.



When the installation of Intrusion Defense Firewall Server Plug-in is complete, click **Manage Program** to activate Intrusion Defense Firewall.

Note: The first time you run the Intrusion Defense Firewall Server Plug-in, you may receive a certificate warning. This is because the Server Plug-in runs on a different Web server than the OfficeScan server. It is safe to accept this certificate. When the warning appears, click the **Install Certificate...** button and install to the default location.

Upgrading the Server Plug-in

The Plug-in Manager screen will inform you if a new version of the Intrusion Defense Firewall Server Plug-in is available. The new version will be listed above the current version. To upgrade to the new version, click the **Download** button. When the new version has finished downloading, the button will change to **Upgrade**. Click **Upgrade** to upgrade your Server Plug-in.

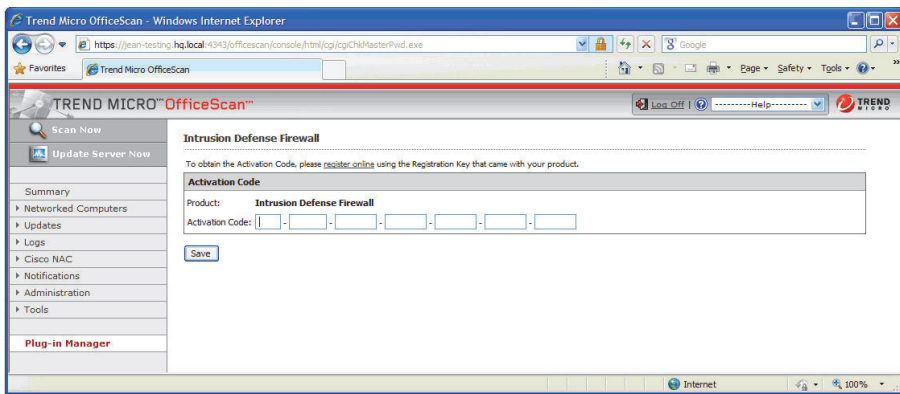
Activating the Intrusion Defense Firewall Server Plug-in

1. Install Security Certificates

The first time that you activate the Intrusion Defense Firewall Server Plug-in, you may see a Microsoft Security certificate alert.

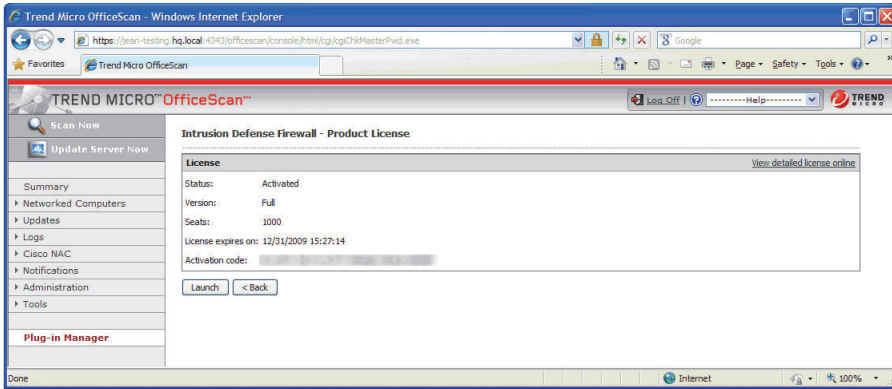
If you cannot open the IDF Server console, see *Why can't I open the IDF Server console using IE7? on page 4-2.*

2. Type Your Activation Code



Type the Intrusion Defense Firewall Activation Code and click **Save** to complete the registration.

Note: To enter your complete Activation Code quickly, right-click in the first code entry box, then paste your full Activation Code. If you do not have an Activation Code, please contact your Trend Micro representative or support provider.



Click **Launch** to start Intrusion Defense Firewall.

Installing the IDF Server Components with a Local Update Source

If the OfficeScan server is unable to connect to the Internet, you need to install the Intrusion Defense Firewall components on the OfficeScan server (localhost) and specify local update sources for OfficeScan.

Note: Before you continue, obtain the installation package from Trend Micro. The installation package will contain the setup files for Intrusion Defense Firewall components.

To install Intrusion Defense Firewall with a local update source:

1. On the OfficeScan server, create a virtual directory “IDF”.
 - If you are using IIS Web server, open the Internet Information Services (IIS) Manager screen and right-click Default Web Site. Then click New > Virtual Directory.
 - If you are using Apache Web server, specify the new virtual directory in the httpd.conf file and restart the Apache service. The following shows an example of the virtual directory section for “IDF” in the httpd.conf file:

```
#IDF Plug-in Active Update
Alias /IDF "C:/TmUpdate/IDF/"
<Directory "C:/TmUpdate/IDF">
    Options None
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
```

2. Extract the installation package from Trend Micro.
3. Copy the folders “activeupdate” to the virtual directory. If prompted, accept to overwrite any existing folders in the directory.

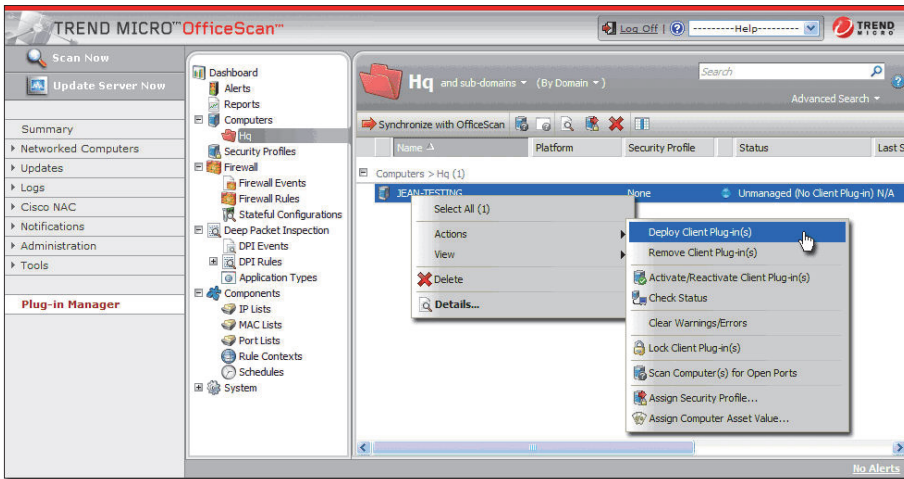
To specify a local update source for OfficeScan:

1. Log on to the OfficeScan Web console and click **Updates > Update Source**. The Server Update Source screen displays.
2. Select **Other update source** and type:
"http://localhost:8080/IDF/activeupdate" in the field provided. Click **Save**.
3. Restart the OfficeScan Plug-in Manager service to make the changes take effect.
4. Log on to the OfficeScan Web console again and click Plug-in Manager.
5. Follow the on-screen instruction to download and install the Intrusion Defense Firewall Server Plug-in on the OfficeScan server.
6. After the installation is completed, click **Manage Program** to access Intrusion Defense Firewall's configuration screens.
7. Type the Activation Code to register the product. After product registration is completed successfully, the Getting Started Page for the Intrusion Defense Firewall Server Plug-in is displayed

Installing the Intrusion Defense Firewall Client Plug-in

Deploy the Client Plug-in

From the Intrusion Defense Firewall Server Plug-in interface, go to **Computers** and right-click the computer (or Domain) to which you want to install the Client Plug-in(s). From the **Actions** menu, select **Deploy Client Plug-in(s)**.



Wait while the Client Plug-in is deployed to the selected Computer(s). During this process, the Computer Status column will display messages that the Client Plug-in is being deployed.

When the Client Plug-in deployment has completed, the Computer's Status column will read "Managed (Online)".

Optionally Use the Standalone Client Plug-in Installer

The IDF Standalone Client Plug-in Installer package is a self-extracting .msi file which is run on the client computer and is available from Trend Micro support upon request. The client computer must already have the OSCE client installed on it. The Client

Plug-in will perform automatic agent-initiated activation after installation but Client Plug-in Initiated Activation must be enabled from the IDF Server Plug-in console for automatic activation to work. (**System > System Settings > Computers**)

The standalone installer uses the OSCE Client to perform the installation of the IDF Client Plug-in, and assumes that the OSCE Client is already installed in the default location:

```
C:\Program Files\Trend Micro\OfficeScan Client
```

To use the Standalone Client Plug-in Installer:

1. For the 32-bit platform, double-click IdfClient-1.5.0.xxxx-en.i386.msi. For the 64-bit platform, double-click IdfClient-1.5.0.xxxx-en.x86_64.msi. (xxxx is the internal build number.)
2. If you need logging, do the following:
 - a. Open a command window.
 - b. Navigate to the folder containing the standalone msi.
 - c. Run the following command:

```
msiexec /i IdfClient-1.5.0.xxxx-en.i386.msi /l*v  
idf_standalone.log
```

The log file is named idf_standalone.log.
3. Verify the client is listed on the **Computers** screen and that its status is “Managed”.

Note: Because the standalone installer will briefly interrupt the client's network connection, the installer **must** be run locally on the host computer.

Transitioning from the OfficeScan Firewall

Trend Micro recommends using only one firewall at a time. Perform the following procedure to switch from using the OfficeScan firewall to the IDF firewall while keeping computers protected during the transition.

- Step 1: Modify OfficeScan Firewall Configuration
- Step 2: Assign Appropriate Security Profiles to the Computers
- Step 3: Edit the Domain Controllers IP List
- Step 4: Disable the Native OfficeScan Firewall

To use the IDF Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) features with the OfficeScan firewall, perform the same procedure except the last step. Steps 1 to 3 are required to maintain the communication between the Server Plug-in and the Client Plug-in.

Note: Running both OfficeScan firewall and Intrusion Defense Firewall, regardless of whether IDF is active, may lead to unpredictable behavior on some Windows XP/2003 systems. Trend Micro recommends uninstalling the OfficeScan firewall driver to resolve the issue. For more information, see <http://esupport.trendmicro.com/solution/en-us/0122179.aspx>.

1. Modify OfficeScan Firewall Configuration

If you are currently using the native OfficeScan firewall with a Medium or High security level, you must open the following client ports to the Server Plug-in. This will permit the Intrusion Defense Firewall Server Plug-in to communicate with the Intrusion Defense Firewall Client Plug-in while the OfficeScan firewall is still in effect:

TCP 4118 (The port for the Client Plug-in for communication from the Server Plug-in)

TCP 4119 (The port for the Server Plug-in Web Console)

TCP 4120 (The port for the Server Plug-in for communication from the Client Plug-in)

To modify OfficeScan firewall configuration:

1. Create a new OfficeScan Firewall policy named Intrusion Defense Firewall policy. (Refer to the OfficeScan online help for details about creating OfficeScan firewall policy and profile.)
2. Add a new exception to the policy:
 - Name:** Intrusion Defense Firewall exception
 - Action:** Allow network traffic
 - Direction:** Inbound and Outbound
 - Protocol:** TCP
 - Port(s):** Specific port numbers:
 - **4118** (The port for the Client Plug-in for communication from the Server Plug-in)
 - **4119** (The port for the Server Plug-in Web Console)
 - **4120** (The port for the Server Plug-in for communication from the Client Plug-in)
 - IP Address:** The IP address of the OfficeScan Server
3. Create a new OfficeScan firewall profile named Intrusion Defense Firewall policy
 - Set the policy to Intrusion Defense Firewall profile
 - The profile should apply to all computers that will be switched over to Intrusion Defense Firewall

2. Assign Appropriate Security Profiles to the Computers

Intrusion Defense Firewall comes with pre-defined Security Profiles including: Windows Laptop Profile, Windows Workstation Profile, and OfficeScan Server Profile.

Note: Security Profiles are composed of sets of Firewall Rules, DPI Rules, and Stateful Configurations (see *About Intrusion Defense Firewall* starting on page 1-1). You can examine a Security Profile's properties by double clicking on a Security Profile in the Security Profiles screen. By clicking on the available tabs, you can see which rules, configurations etc. the Security Profile is applying.

Security Profiles are designed to be re-used by multiple computers with similar needs. The example Security Profiles can be duplicated (right-click on a Security Profile and select “Duplicate”) and then customized to meet the needs of your organization. Intrusion Defense Firewall comes with example Security Profiles as a secure starting point.

Now go through your list of Computers and assign appropriate Security Profiles (Using the **Actions > Assign Security Profile...** function in the right-click menu).

3. Edit the Domain Controllers IP List

If you are using a Windows domain, you must edit the properties of the Domain Controller(s) IP List to include the IP addresses of all of your domain controllers. Go to **Components > IP Lists** and double-click on the **Domain Controllers** IP List. Add the IP addresses of your domain controllers.

4. Disable the Native OfficeScan Firewall

You can now safely disable the native OfficeScan firewall.

To disable the OfficeScan firewall:

1. Open the OfficeScan Web console.
2. Go to **Administration > Product License**.
3. Under **Additional Services**, click the **Disable** button.
4. Log off and then log on to the OfficeScan Web console to view the correct firewall status.

Creating Your Own SSL Authentication Certificate

Intrusion Defense Firewall creates a 10-year self-signed certificate for the Web browser-to-IDF connections. If required, this certificate can be replaced with a real certificate. (The certificate is maintained on Intrusion Defense Firewall upgrades.)

Note: More information on generating the certificate can be found at [Thawte Tomcat Support](#).

Once generated, the certificate should be imported into the keystore in the root of the Intrusion Defense Firewall installation directory and have an alias of “tomcat”. Intrusion Defense Firewall will then use that certificate.

To create your SSL authentication certificate:

1. Go to the Intrusion Defense Firewall installation directory (C:\Program Files\Trend Micro\ Intrusion Defense Firewall) and make a new folder called “Backupkeystore”.
2. Copy the keystore and configuration.properties to the newly created folder Backupkeystore.
3. Open the command prompt and go to the following location:
C:\Program Files (x86)\Trend
Micro\OfficeScan\Addon\Intrusion Defense Firewall\jre\bin
4. Run the following command which will create a self-signed certificate:
C:\Program Files (x86)\Trend
Micro\OfficeScan\Addon\Intrusion Defense
Firewall\jre\bin>keytool -genkey -alias tomcat -keyalg RSA
-dname cn=dmsserver
5. Choose password: changeit

Note: -dname is the common name of the certificate your CA will sign. Some CA require a particular cn to sign the Certificate signing request (CSR). Please consult your CA Admin to see if you have that particular requirement.

6. There is a new keystore file created under the user home directory. If you are logged in as “Administrator”, you will see the .keystore file under C:\Documents and Settings\Administrator
7. View the newly generated certificate using the following command:
C:\Program Files (x86)\Trend
Micro\OfficeScan\Addon\Intrusion Defense
Firewall\jre\bin>keytool -list -v
8. Run the following command to create a CSR for your CA to sign:

```
C:\Program Files (x86)\Trend
Micro\OfficeScan\Addon\Intrusion Defense
Firewall\jre\bin>keytool -certreq -keyalg RSA -alias tomcat
-file certrequest.csr
```

9. Send the certrequest.csr to your CA to sign. In return you will get two files. One is a certificate response and the second is the CA certificate itself.

10. Run the following command to import the CA cert in JAVA trusted keystore:

```
C:\Program Files (x86)\Trend
Micro\OfficeScan\Addon\Intrusion Defense Firewall\jre\bin
>keytool -import -alias root -trustcacerts -file cacert.crt
-keystore " C:/Program Files (x86)/Trend
Micro\OfficeScan/Addon/Intrusion Defense
Firewall\jre/lib/security/cacerts"
```

11. Run the following command to import the CA cert in your keystore:

```
C:\Program Files (x86)\Trend
Micro\OfficeScan\Addon\Intrusion Defense
Firewall\jre\bin>keytool -import -alias root -trustcacerts
-file cacert.crt
```

(say yes to warning message)

12. Run the following command to import the certificate response to your keystore:

```
C:\Program Files (x86)\Trend
Micro\OfficeScan\Addon\Intrusion Defense
Firewall\jre\bin>keytool -import -alias tomcat -file
certresponse.txt
```

13. Run the following command to view the certificate chain in you keystore:

```
C:\Program Files (x86)\Trend
Micro\OfficeScan\Addon\Intrusion Defense Firewall\jre\bin
>keytool -list -v
```

14. Copy the .keystore file from your user home directory C:\Program Files (x86)\Trend Micro\OfficeScan\Addon\Intrusion Defense Firewall\

15. Open the configuration.properties file in folder C:\Program Files (x86)\Trend Micro\OfficeScan\Addon\Intrusion Defense Firewall.

It will look something like:

```
keystoreFile=C:\\\\Program Files (x86)\\\\Trend
Micro\\\\OfficeScan\\\\Addon\\\\Intrusion Defense
```

```
Firewall\\\.keystore port=4119
keystorePass=$1$2dc445b08c0af7a34f8b3757009b3662b32b9a3bc5aa
d698154ae2bff42ac4d9716ac3aee09b57550d884ef76a0cefbb969e894b
126e39b4a308f2c9c84b0d74 commandExe=idf_c installed=true
serviceName=Intrusion Defense Firewall
```

16. Replace the password in the following string:
keystorePass=xxxx
where “xxxx” is the password you supplied in step five.
17. Save and close the file.
18. Restart the Intrusion Defense Firewall service.
19. Connect to Intrusion Defense Firewall with your browser and you will notice that the new SSL certificate is signed by your CA.

Uninstalling Intrusion Defense Firewall

Note: Neither the IDF Server Plug-in nor the IDF Client Plug-in can be uninstalled using the Control Panel Add or Remove Programs applet.

Client Plug-in

To uninstall the IDF Client Plug-in:

1. Using the IDF Server Plug-in, go to the **Computers** screen.
2. Right-click on the computer from which you want to remove the Client Plug-in.
3. Select **Actions > Remove Client Plug-in**.

If you cannot use the Server Plug-in to communicate with the Client Plug-in, use the following procedure.

To manually uninstall the Client Plug-in:

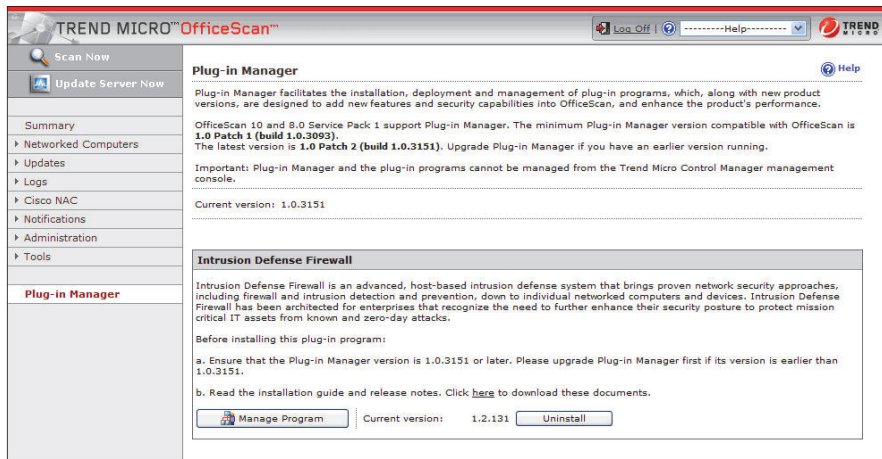
1. On the client machine, open a command prompt window (**Start > Run > cmd.exe**)
2. For 32-bit Windows, type the following and press **Enter**:
rundll32 "C:\Program Files\Trend Micro\IDF
Client\IdfClientAgent.dll",Uninstall

- For 64-bit Windows, type the following and press **Enter**:

```
rundll32 "C:\Program Files (x86)\Trend Micro\IDF
Client\IdfClientAgent.dll",Uninstall
```

Server Plug-in

To uninstall the IDF Server Plug-in, go to the OfficeScan Plug-in Manager and click **Uninstall** in the “Intrusion Defense Firewall” panel.



Scaling IDF for Large Installations

To improve the performance of the IDF Server Plug-in's for installations with a large number of managed computers, the following upgrades are suggested to enhance processing speed:

- Upgrade the server hardware—for example, upgrading to 64-bit dual node 8-core processors, greatly enhances processing speed.
- Upgrade to Microsoft SQL Server 2008.
- Use an external database. For information on upgrading the database, see the *Managing the IDF Server Plug-in* chapter of the *Trend Micro™ Intrusion Defense Firewall™ 1.5 Administrator's Guide*.



Chapter 3

Troubleshooting

This chapter describes the following:

- *Server Plug-in on page 3-1*
- *Client Plug-in on page 3-5*

Server Plug-in

Error Message: “Unable to proceed. The Trend Micro Plug-in Manager must be version 1.0.3151 or greater.”

Solution: Check the version of Trend Micro Plug-in Manager and contact support if you are unable to download and install version 1.0.3151 or higher. The Plug-in Manager must be upgraded before Intrusion Defense Firewall is installed.

Error Message: “Unable to proceed. A minimum of 1500 MB of free disk space is required and only ? MB is available.”

Solution: Free up additional disk space and re-try the installation. (The disk space must be available on the same drive that OfficeScan Server is installed on.)

Error Message: “Windows Installer Version 4.5 or higher is required.”

Solution: Run Windows Update and ensure you have the latest version of Windows Installer.

Error Message: “Microsoft Data Access Components (MDAC). Version 2.81 or higher is required.”

Solution: Download and Install MDAC from Microsoft using the following location:
<http://www.microsoft.com/downloads/details.aspx?familyid=78CAC895-EFC2-4F8E-A9E0-3A1AFBD5922E&displaylang=en> (MDAC is not installed or updated during Windows Update)

Error Message: “Microsoft .NET Framework. Version 2.0 SP2 or higher is required.”

Solution: Download and Install Microsoft .NET 2.0 SP2 using Windows Update or from the following location:
<http://www.microsoft.com/download/en/details.aspx?id=1639>

Error Message: “Unable to proceed. The system directory could not be located.”

Solution: Please contact support. They will assist you in collecting a log that will be used to diagnose the problem.

Error Message: “Unable to write to the add-on registry key '?. Please check the registry permissions before trying again.”

Solution: Check the permissions of the Plug-in Manager service and make sure it has the privileges required to write to the registry.

Error Message: “SQL installation failed. Check the logs in C:\Program Files\Microsoft SQL Server\90\Setup Bootstrap\LOG\Files”

Solution: Ensure your system meets the hardware and software requirements for SQL Server Express 2005:

<http://msdn2.microsoft.com/en-us/library/ms143680.aspx>

If your system meets the requirements, consult the logs referred to in the error message. If the SQLSetup?_?_Core(Local).log file contains an error similar to the following the .NET installation is likely corrupted:

```
"C:\Program Files\Microsoft SQL Server\90\Setup
Bootstrap\LOG\Files\SQLSetup0004_D-A-13_.NET Framework 2.0.log"
to cab file : "C:\Program Files\Microsoft SQL Server\90\Setup
Bootstrap\LOG\SqlSetup0004.cab" Error Code : 2"
```

Re-install Microsoft .NET Framework 2.0. If that does not remedy the situation please contact support. For other SQL Errors contact support and send them the log files in the directory referred to in the error message.

Error Message: “Installation of Intrusion Defense Firewall failed. Check the logs in ? and ?“

Solution: A general unexpected error has occurred. Consult the logs referred to in the error message and contact support if required. It is possible that even though Intrusion Defense Firewall failed to install, the SQL Server Express 2005 installation completed successfully and is still installed on your system. Subsequent attempts to install Intrusion Defense Firewall will use this first instance SQL Server Express. If you do not plan to install Intrusion Defense Firewall again and would like to remove this instance of SQL, manually uninstall the database instance by executing the following command:

```
"C:\Program Files\Trend
Micro\OfficeScan\PCCSRC\Admin\Utility\SQL\sql.exe" /qn
REMOVE=SQL_Engine INSTANCENAME=IDF
```

After the database has been removed, verify that the following directory either has been removed or that the IDF.mdf file has been removed (If needed delete IDF.mdf and IDF_log.LDF) located in:

```
C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data
```

Also ensure that the following directory has been removed (delete it if needed):

```
C:\Program Files\Trend Micro\OfficeScan\Addon\Intrusion Defense
Firewall
```

Problem: The Server Plug-in machine is having connectivity problems.

Solution: Ports 4119 and 4120 must be open on the Server Plug-in machine to allow the Client Plug-ins to communicate with it and to allow users access to the Web based user interface.

Problem: The IDF Server Plug-in fails to start.

Solution: In some environments, various system DLLs will be loaded in such a way that they do not allow the IDF Server process to receive all the initial contiguous RAM it requests during startup (1GB). In these environments the IDF Server process can be tuned to request less contiguous RAM, and hence be able to start.

IDF Server uses a Sun Java Virtual Machine. The JVM's memory can be tuned by adding a special file into the main IDF directory. Create and add the following file to the IDF Server directory (typically <OSCE>\AddOn\Intrusion Defense Firewall):

```
Intrusion Defense Firewall.vmptions
```

Use a text editor to edit the file and add the exact text below:

```
-Xmx950m
```

Restart the IDF Server service. If the service still does not start, you can step down the amount of memory to the highest possible amount, and continually restart the service until a value works:

```
-Xmx950m
```

```
-Xmx900m
```

```
-Xmx850m
```

```
...
```

For the IDF Server to function properly, it is important that it has access to as much RAM as possible (up to 1GB), hence this stepping down process.

Client Plug-in

Error Message: “Update Failed” on client computer.

Solution: In rare cases an IDF Client Plug-in deployment or upgrade will succeed, but the Computer in the IDF Server Plug-in console will go into an error state of “Update Failed”. This may be due to the driver being successfully installed, but having no bindings to any network adapters on the host.

If the network bindings are NOT present (i.e. the checkboxes are not checked in Windows Control Panel > Network Connections > Properties) during installation, then they must have been disabled in the past, or something unexpected occurred during the upgrade/install. (The IDF Client Plug-in “preserves” the existing state bindings on upgrade.)

In order to resolve this issue locally, manually enable the bindings (make sure the checkboxes associated with “TB-IM DSA Filter Driver” of a network adapter are selected, i.e. Local Area Connection > Properties). To resolve remotely, remove, and then re-deploy the Client Plug-in. The uninstall should remove the driver entirely, and the fresh install should re-instate the bindings.

Problem: Interpreting the “last error code” from a “Client Plug-in Installation Failed” message.

Solution: The last error code is a Windows Installer Error message.

The following error may occur if an earlier version of an IDF Client Plug-in is not completely uninstalled or has been corrupted so that it cannot be uninstalled: Client Plug-in installation failed (reason: Install Failed state: 7, last error code: 1603). The resolution is to install “Windows Installer Cleanup Utility” and manually uninstall the “Trend Micro Intrusion Defense Firewall” entry.

(<http://support.microsoft.com/kb/290301>)

The following error occurs when another MSI installation is already in progress during the IDF deployment: Client Plug-in installation failed (reason: Install Failed state: 7, last error code: 1618). The resolution is to complete the other installation and then re-deploy the IDF Client Plug-in. If the problem still exists you may need to reboot and/or run the Windows Installer Cleanup Utility as above.

Error Message: “Unable to open engine \\.\Global\TBIMDSA” (Client Plug-in)

Solution: To install the IDF Client Plug-in driver in the Microsoft network stack you need to use tools that have been provided through the msi installer tools set.

For the installation to be successful, the msi installer (or other programs called by the msi installer) needs to be able to lock the network configuration, as well as some files that are associated with the network stack. If these files cannot be locked, then the driver cannot be installed and bound to the network interface. In some cases the driver will be installed but not bound, leading to the situation where you will see the TBIMDSA Filter driver listed in the Network Connections, Properties without a check mark. In some cases, manually checking that box will allow the driver to be bound to the network interface, but in some cases a reboot may be required.

There are three workarounds that can be tried when this error shows up:

1. Remove and redeploy the agent from the IDF console.
2. Manually check the TBIMDSA filter driver checkbox in the Network Connections, Properties for the interface in question
3. Reboot the machine.

Problem: During an IDF Client Plug-in uninstall, what should I do if the process seems to hang?

Solution: The computer sometimes loses network connection completely if IDF un-installation hangs. From process explorer, you can see that rundll32.exe is hanging. The resolution is to restart the machine and remove the IDF Client Plug-in again.

Problem: During an IDF Client Plug-in upgrade, the upgrade of the IDF driver may not have completed but the IDF Server Plug-in shows “Managed”.

Solution: The IDF driver install/upgrade may need a reboot but in rare cases it does not show the Reboot Required warning message to the user. The IDF Client Plug-in continues to use the previous driver until rebooted. The resolution is to reboot the computer.

Problem: When creating a diagnostic package, I get an IE popup warning message.

Solution: The popup by IE to warn about unsafe download content is part of the default “Trusted Site” security level. This does NOT stop the download, only means it will prompt.

If you do not want to be prompted, go to **IE > Tools > Internet Options > Security** tab, select **Trusted Sites**, and change to a custom level. Set **Downloads > Automatic prompting for file downloads** to “Enable”. The prompt will no longer appear.



Chapter 4

Frequently Asked Questions

This chapter describes the following:

- *General FAQs on page 4-1*
- *IDF Database FAQs on page 4-4*

General FAQs

Which version of Trend Micro Plug-in Manager is required for IDF 1.5?

Before installing IDF 1.5, make sure you have PLM 1.0.3151 installed. (This means you must be using OSCE 8.0 SP1 or newer).

Note that even if PLM 1.0.3151 is installed on the OSCE server, some clients may not be updated to this version. Make sure that the OfficeScan clients have been updated to this version of the PLM.

How do I update the Plug-in Manager on a client?

On OfficeScan Server, Client Management, select the client and from the Settings menu, select Privileges and Other Settings. Then, on the Other Settings tab, clear the “Clients can update components but not upgrade the client program or deploy hot fixes” option. The OfficeScan Server will push upgrades to the clients.

In the event that any clients do not get upgraded to the correct version of PLM after clearing this option, you need to update the OfficeScan client before deploying IDF. You can do this manually at the client by right-clicking the OfficeScan icon in the system tray, and selecting Update Now from the menu. (To confirm you have the correct version installed, the file `\Program Files\Trend Micro\OfficeScan Client\CNTAoSMgr.exe` lists the current version.)

Can I install IDF to a FAT32 Partition?

Yes, IDF 1.5 now supports FAT32 file systems.

Can I change the installation directory for the IDF Client Plug-in?

No. The location is fixed as `<PROGRAM FILES>\Trend Micro\IDF Client`.

Where the `<PROGRAM FILES>` folder is from Windows (typically `C:\Program Files`)

Can I upgrade from IDF 1.2 to IDF 1.5?

Yes - See the instructions in this Deployment Guide.

Before upgrading IDF Server Plug-in, make sure that you have already installed the required minimum version of OfficeScan and Plug-in Manager. (The required minimum PLM version is always displayed on the Intrusion Defense Firewall section of the Plug-in Manager screen.)

Is there a Standalone install package for IDF 1.5 Client Plug-in?

Yes. See the installation instructions in this guide or in the *Trend Micro Intrusion Defense Firewall Administrator's Guide*.

Why can't I open the IDF Server console using IE7?

In some cases, the IDF Server console will not open in some installations of IE7 (typically on Vista). This is caused by a certificate error and the error may happen on other IE versions. The following are workarounds for this issue:

1. Add the OfficeScan server address to the list of IE "Trusted Sites":
 - a. Open IE, go to **Tools >Internet Options**.
 - b. Select the **Security** tab, and click **Trusted Sites**.

- c. Add the OfficeScan server site to the list—for example, `https://myofficescan:4343/`
 - d. Go back to the OfficeScan web console and attempt to access IDF Server.
 2. Import the IDF certificate. It is important to note that this is the IDF Server certificate, and NOT the OfficeScan certificate. To access the IDF Server certificate, the follow these steps:
 - a. Log in to the OfficeScan web console. Go to Plug-in Manager and enter the IDF server console.
 - b. Open a browser and connect to `https://<hostname>:4119/Application.screen`
 - c. Click **Certificate Error**.
 - d. Click **View Certificates**.
 - e. Install the certificate.
 - f. Place all certificates in the following store: “Trusted Root Certification Authorities”.
 - g. Go back to the OfficeScan web console and attempt to access IDF Server.

How long does it take to deploy IDF Client Plug-in over a large network with thousands of clients?

Multiple clients are deployed concurrently (by the OfficeScan server, not the IDF Server Plug-in). It takes a minute or two per client. The number of concurrent deployments depends on the OfficeScan Plug-in Manager but you should expect an average of approximately five clients per minute.

How long does it take to push a Security Update out to Clients?

The Server Plug-in will update up to 25 Client Plug-ins at the same time. Each update takes a few seconds to complete. You can estimate the amount of time it will take to deploy an update by multiplying 0.5 seconds * number of Client Plug-ins.

Ex: 1000 clients * 0.5 seconds = 8 minutes 20 seconds

The time required can be influenced by network congestion, the resources of the Server Plug-in's Computer, and the direction of the communication between the Client Plug-in and the Server Plug-in. (By default IDF is configured so that both the client and the server can initiate communication. This is the most efficient configuration.)

Note: The manager will update up to 25 Client Plug-ins concurrently. Each update takes 2-3 seconds to complete, however because of the time-savings of the concurrency it averages 0.5 seconds/host.

What is the maximum number of IDF Clients that can be supported from one IDF Server?

- 5000 endpoints supported per OSCE server assuming the embedded MS SQL Express database is being used.
- 20,000 endpoints supported per OSCE server assuming MS SQL Server 2005/2008 (installed on a separate machine) is being used.

Does IDF work in a NAT environment?

In the scenario where the IDF Server is outside the NAT and Clients are inside the NAT, does IDF Server/Client communication work properly?

Yes, you should set the Computer Communication Direction to Client Plug-in-initiated. See more on this in the “Communication Direction” section of the *Trend Micro Intrusion Defense Firewall Administrator's Guide*.

IDF Database FAQs

Which version of SQL Server does IDF Install?

And will it conflict with other SQL Server instances already installed?

IDF installs a named instance of SQL Server 2005 Express. This should prevent it from conflicting with any other default instance or named instance on the host.

This database as installed will not conflict with any of the following:

- MSDE
- SQL Server 2000 under the default instance

- SQL Server 2000 under a named instance
- SQL Server 2005 under the default instance
- SQL Server 2005 under a named instance

The database has a limitation of 4GB, is there a way we could increase this database capacity?

It is not possible to increase the database capacity for SQL Server Express.

It is possible to migrate to a database that has no space constraints such as SQL Server database. A set of migration steps have been established. See “Migrating to a Larger Database” in the *Trend Micro Intrusion Defense Firewall Administrator’s Guide*. Please contact your Trend Micro support provider for assistance.

How can I archive the logs for a couple of years?

This is not possible. IDF uses SQL Server Express which is capped at a maximum of 4GB of data. This makes it unsuitable for archive. For audit/compliance, it is recommended that database backups be employed. The *Trend Micro Intrusion Defense Firewall Administrator’s Guide* includes information on creating scheduled backups.

How can IDF use less Database space?

IDF Server stores events in the database and automatically purges events when they reach a certain age. The maximum age of these events is fully configurable from IDF Server. This allows an administrator to tune how long they want to keep certain types of events in IDF Server, and hence allows an administrator to effectively tune how their database space is utilized.

Prune settings are configured in IDF Server by going to **System >Settings**, selecting the **System** tab, and then editing the settings within the “Prune” section. Changes to these settings are effective immediately, but it will take IDF Server up to an hour to do the actual pruning, as it is done every hour.

To decide what prune settings would benefit from being shortened, you can use a SQL Server database tool to inspect your database and find out which tables are taking up the majority of the space.

<http://www.microsoft.com/downloads/details.aspx?familyid=C243A5AE-4BD1-4E3D-94B8-5A0F62BF7796&displaylang=en>

If you use the tool mentioned above, install it on the IDF Server host, launch the tool and login to the IDF instance, expand the “IDF” database, view the tables, and then fetch the properties of the tables listed below to determine their size. Considering that SQL Server Express has a maximum size of 4GB, you should consider any table below that is over 1GB to be “too large”, and its pruning settings should be lowered if possible.

The following tables are included in the “Firewall/DPI events” prune settings:

```
packetlogs  
payloadlogs  
payloadlogdatas
```

The following tables are included in the “system/client plug-in events” prune settings:

```
systemevents  
agentevents
```

The following tables are included in the “counters” prune settings:

```
counter3s  
counter3ports  
counter3ips
```

Can I shrink the size of the IDF database?

The IDF Server uses a SQL Server Express database. It, by default, has a maximum size for data of 4GB, but its database log file (IDF_Log.mdf) can grow as large as needed. In some extreme cases it can grow up to the size of the main database file, so 4GB.

In some situations it may be helpful to shrink the database so it consumes less actual disk space.

The only way to perform this operation on the IDF database is by using a SQL Server tool. This can be done using the SQL Server Express Management tool, or via a similar command line tool - both tools are provided free from Microsoft:

```
http://www.microsoft.com/downloads/details.aspx?familyid=C243A5AE-4BD1-4E3D-94B8-5A0F62BF7796&displaylang=en
```

```
http://www.microsoft.com/Downloads/details.aspx?familyid=FA87E828-173F-472E-A85C-27ED01CF6B02&displaylang=en
```

After installing the latter tool on the IDF Server machine, the following command will shrink the database:

```
sseutil -shrink name=IDF -server .\IDF -m
```

Usually the shrink is performed on the logical logs - they grow more rapidly than the database and sometimes they are not flushed. Do the following to release logical log space:

1. Perform full backup
2. Perform logical logs backup
3. Run the following two SQL queries to release the space.

```
USE idf
GO
Checkpoint
USE idf
DBCC SHRINKFILE(idf_log, 1)
BACKUP LOG WITH TRUNCATE_ONLY
DBCC SHRINKFILE(idf_log, 1)
```

Note: Another option that is discouraged by Microsoft, but is still technically an option to keep the files small is to turn the IDF database into “Auto-Shrink” mode. You can do this using the latter GUI tool mentioned above by selecting the Databases->IDF node, right click and select Properties, choose Options, and then configuring the “Auto-Shrink” mode to be “True”.

How can I migrate IDF data from the bundled SQL Server Express onto another database?

A set of migration steps have been established. See “Migrating to a Larger Database” in the *Trend Micro Intrusion Defense Firewall Administrator’s Guide*. Please contact your Trend Micro support provider for assistance.

Index

A

activation code 2-5
automatic activation 1-6

B

bridging attack protection 1-4

C

Client Plug-in 1-4
 deploying 2-8
 installation 2-8
 standalone installer 2-8
 troubleshooting 3-5
 uninstalling 2-15
Components 1-3
computers 1-2

D

Dashboard 1-2
database 4-4
Deep Packet Inspection Rules 1-3

E

Event tagging 1-6
expanded OCSE support 1-6

F

file system support 1-6
Firewall Rules 1-2
frequently asked questions
 database 4-4
 general 4-1

I

installation
 Client Plug-in 2-8
 components 2-6
 Server Plug-in 2-2

L

location awareness 1-4

O

OfficeScan Firewall 2-10
OSCE 1-6

P

performance and scalability 1-6
platforms 1-6

S

scaling 2-16
security certificates 2-5
Security Profiles 1-2
Server Plug-in 1-1, 2-4
 activating 2-5
 bridging attack protection 1-4
 Components 1-3
 components 2-6
 computers 1-2
 Dashboard 1-2
 Deep Packet Inspection Rules 1-3
 Firewall Rules 1-2
 location awareness 1-4
 Security Profiles 1-2
 Stateful Configurations 1-3
 system requirements 1-4

- troubleshooting 3-1
- uninstalling 2-16
- upgrading 2-4
- SSL authentication certificate 2-12
- Standalone Client Plug-in Installer 2-8
- Stateful Configurations 1-3
- system requirements 1-4
 - Client Plug-in 1-5
 - Server Plug-in 1-4

T

- Tags 1-6
- troubleshooting
 - Client Plug-in 3-5
 - Server Plug-in 3-1

U

- uninstalling 2-15
 - Client Plug-in 2-15
 - Server Plug-in 2-16
- upgrading 2-4

W

- what's new in IDF 1.5 1-6