TREND MICRO™

Intrusion Defense Firewall 1.1

for OfficeScan Client/Server Edition

Deployment Guide

Endpoint Security

Document part number: OSEM83589/80317
Release Date: May 2008

Table Of Contents

About Intrusion Defense Firewall

Intrusion Defense Firewall for OfficeScan Client/Server Edition is an intrusion defense system that 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.

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, and log forwarding for event correlation with other systems.
- Ability to save multiple dashboard layouts.

Monitoring Tools

Monitoring tools include event viewers for Firewall, IPS, 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 the Intrusion Defense Firewall.

Security Profiles

Security profiles are policy templates that let you configure and specify the security rules that 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.

IPS (Intrusion Prevention System) Filters

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

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

Stateful Configurations

The 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

The 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.

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 RAM 512 MB (1 GB recommended)
- **Disk Space:** Minimum 1.5 GB (6 GB recommended)
- **Web Browser:** Internet Explorer 6+ (cookies enabled)
- **Operating System:** Microsoft ® Windows ® Server 2003 (SP1 or higher), Microsoft Storage Server 2003 (SP1 or higher), Microsoft Cluster Server 2003 (SP1 or higher), Microsoft Windows 2000 Server (SP4 or higher)
- **Pre-requisites:**
  - **Windows 2000:** MDAC 2.81, Windows Installer 3.1 and Microsoft .NET Framework 2.0 or higher (Required for SQL Server 2005 Express Installation)
  - **Windows 2003:** Microsoft .NET Framework 2.0 or higher (Required for SQL Server 2005 Express Installation)

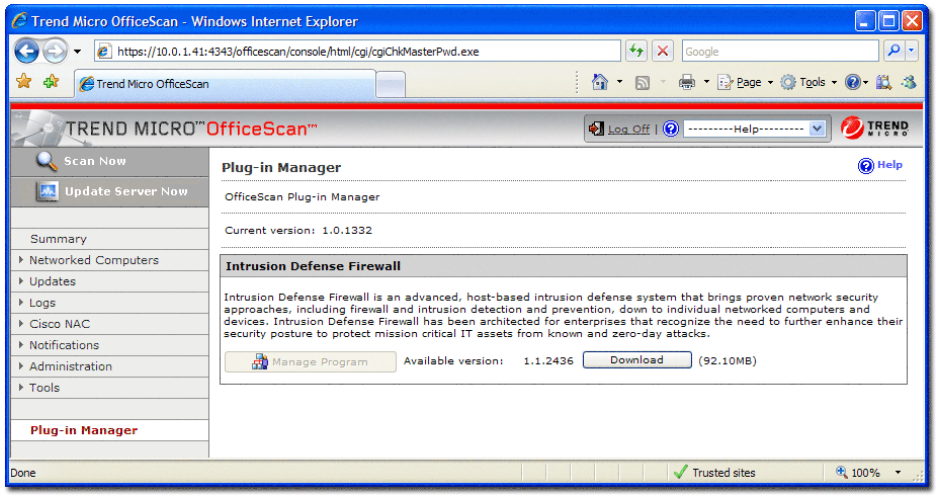
The Server Plug-in automatically installs Microsoft ® SQL Server 2005 Express ®.

Client Plug-in

- **Memory:** Minimum RAM 128 MB
- **Disk Space:** Minimum 50 MB (100 MB recommended, primarily for logging)
- **Operating System:** Windows 2000 (32-bit), Windows XP (32- and 64-bit), Windows 2003 (32- and 64-bit), Vista (32- and 64-bit)

Installation

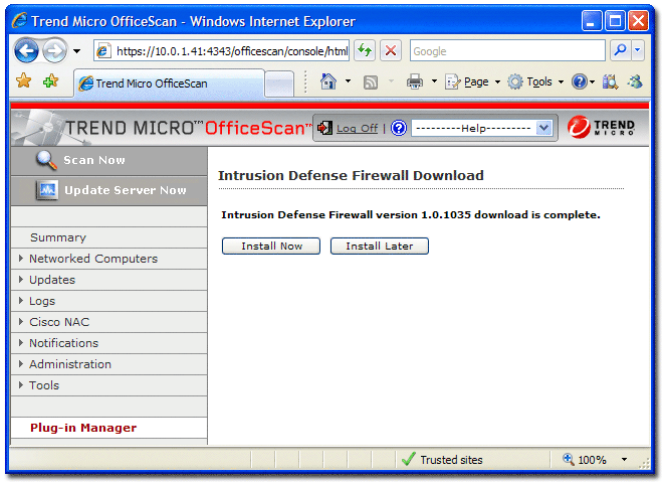
1. Download the Intrusion Defense Firewall



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

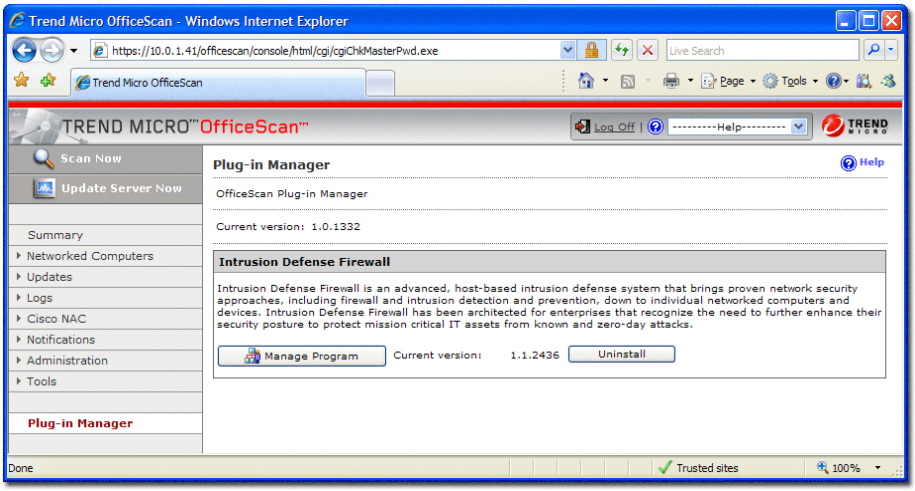
In the dialog box, click "OK" to confirm the download, and wait for the download to complete.

2. Install the 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 to the license agreement. Read and accept the license agreement to continue.

The installation will take several minutes.



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

> 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 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. (It checks once a day.) 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, click **Upgrade** to upgrade your Server Plug-in.

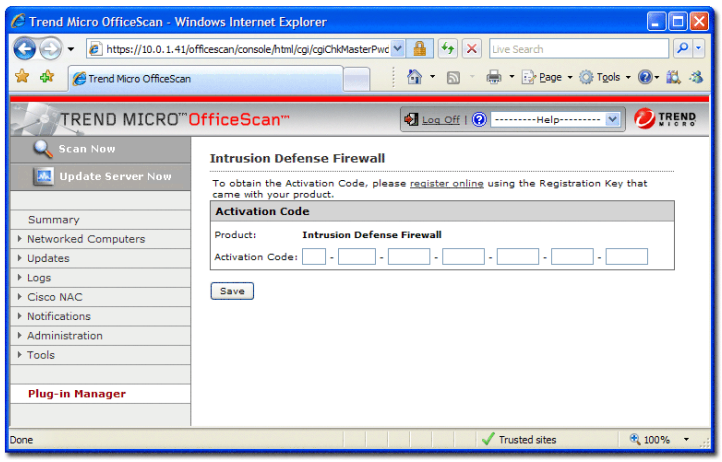
Activating the Intrusion Defense Firewall Server Plug-in

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.

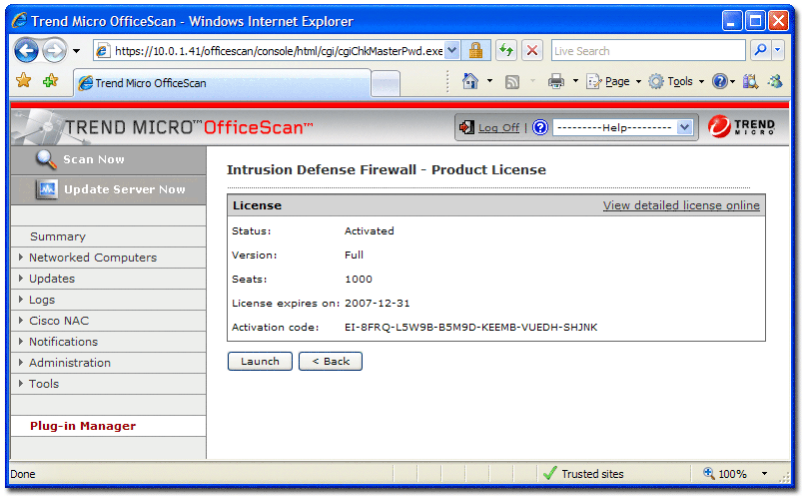
Click **View Certificate**, and then on the Certificate Information screen, click **Install Certificate**. In the Certificate Import Wizard, follow the instructions to import the certificate into the certificate store.

2. Enter your Activation Code



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

> 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 the Intrusion Defense Firewall.

Installing the Intrusion Defense Firewall 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.

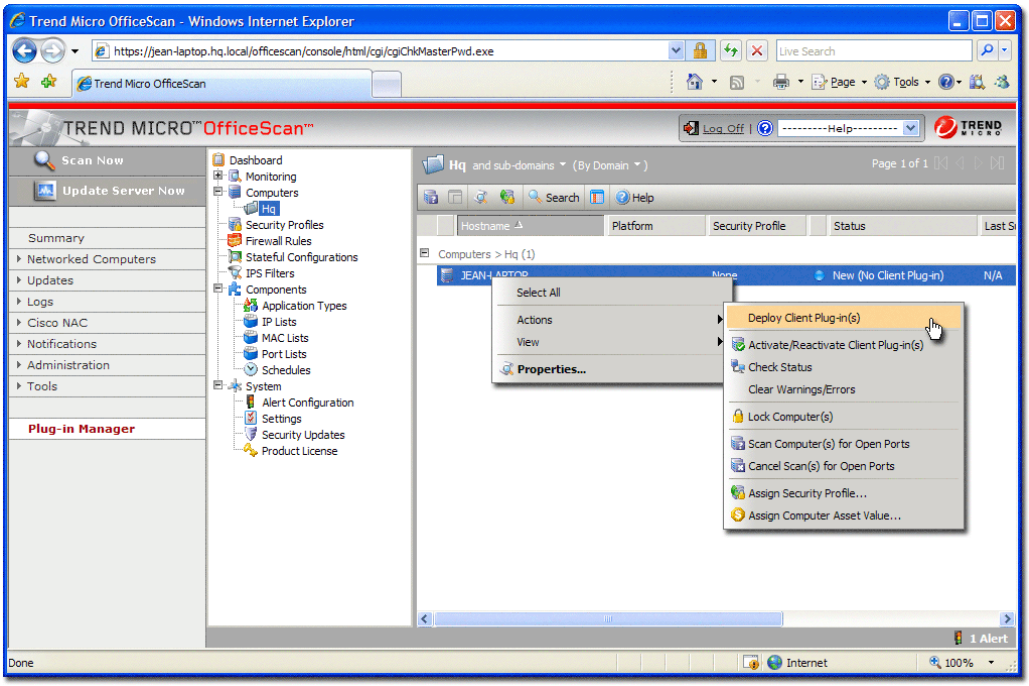
To specify a local update source for OfficeScan:

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 Plug-in on the OfficeScan server.
6. After the installation is completed, click **Manage Program** to access the configuration screens for the Intrusion Defense Firewall.
7. Type the Activation Code to register the product. After product registration is completed successfully, the Getting Started Page for the Intrusion Defense Firewall Plug-in is displayed.

Installing the Intrusion Defense Firewall Client Plug-in

Deploy Client Plug-in

From the Intrusion Defense Firewall management console, go to **Computers** and right-click the computer (or Domain, or Workgroup) 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(s) are being deployed.

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

Transitioning from the Native OfficeScan Firewall to the Intrusion Defense Firewall

The Intrusion Defense Firewall firewall and the native OfficeScan Firewall are two distinct firewalls and only one should be used at a time. The following instructions tell you how to switch from the OfficeScan firewall to the Intrusion Defense Firewall firewall without leaving your computers exposed during the transition.

> Some users may wish to only make use of the Intrusion Defense Firewall's IPS (Intrusion Prevention System) or IDS (Intrusion Detection system) functionality and continue using the native OfficeScan firewall. In this case, the following steps must still be carried out (except the last one: disabling the native OfficeScan firewall) so that the Server Plug-in can communicate with the Client Plug-in.

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 an 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 the Intrusion Defense Firewall

2. Assign Appropriate Security Profiles to the Computers

The Intrusion Defense Firewall comes with three pre-defined Security Profiles: Windows Laptop profile, Windows workstation Profile, and OfficeScan Server Profile.

> Security Profiles are composed of sets of Firewall Rules, IPS Filters, and Stateful Configurations (see "About Intrusion Defense Firewall", above). 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 filters, rules, 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 three 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.

Uninstalling Intrusion Defense Firewall

For instruction on Uninstalling the Intrusion Defense Firewall Client and Server Plug-ins, see the **How To...** section of the Administrator's Guide.

Server Plug-in Installation Troubleshooting

Error Message: “Unable to proceed. The Trend Micro Plug-in Manager must be version 1.0.1332 or greater.”
Solution: Please check the version of Trend Micro Plug-in Manager and contact support if you are unable to download and install version 1.0.1332 or higher. The Plug-in Manager must be upgraded before the 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 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 3.1 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 or higher is required.”
Solution: Download and Install Microsoft .NET 2.0 using Windows Update or from the following location: http://www.microsoft.com/downloads/details.aspx?familyid=0856eacb-4362-4b0d-8edd-aab15c5e04f5&displaylang=en

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: Please 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 please consult the logs referred to in the error message. If the SQLSetup?_?_Core(Local).log file contains an error similar to:

"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. The .NET installation is likely corrupt. If that does not remedy the situation please contact support.

For other SQL Errors please contact support and send them the log files in the directory referred to in the error message.

Error Message: “Installation of the Intrusion Defense Firewall failed. Check the logs in ? and ?”
Solution: A general unexpected error has occurred. Please 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 does not exist 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