Getting Started Guide

Revision 1.0

Release Date: March, 2007

Contents

Chapter 1

Introducing Trend Micro HouseCall Server

Trend Micro™ HouseCall 6.6 Server Edition provides agentless scanning and cleaning for both viruses and spyware. This solution lends itself to service providers and enterprises with large extranets who want to lower support costs.

This Java-based solution supports Windows-based PCs and Linux computers with a variety of browsers including Microsoft Internet Explorer and Mozilla Firefox.

Virus infections and spyware are a particular pain point for XSPs and Enterprises. XSPs must spend time and resources answering customer calls. HouseCall also enables organizations with large extranets such as retail banks, educational institutions, and government agencies to lower support costs and increase consumer confidence in e-commerce services.

Why HouseCall?

HouseCall offers the following benefits and capabilities:

- On-demand client virus scanning and cleaning
- On-demand spyware scanning and cleaning
- On-demand vulnerability scanning
- Port scanning of remote PCs
- Integration of the Trend Micro System Cleaner(TM) into the HouseCall client
- Secure configuration via a password-protected Server Administration Tool
- Automatic updates of program components
- Automatic updates of ActiveUpdate components for scan engines and pattern files
- Configurable Reports of malware, grayware and vulnerabilities detected on HouseCall Client PCs as XML or CSV format.
- Online registration and certification
- Participation in the Trend Micro Virus Map statistics
- Web-based architecture eliminates software installation and deployment costs
- Supports both Java and ActiveX for maximum operating systems and browser compatibility
- Easy set up: simply install on your Intranet or Extranet server and then point users to the appropriate URL
- Customizable interfaces allows administrators to reflect corporate identity, enabling easy configuration of logos, page colors and links to other internal ressources.
- Compatible with anitvirus and security software from major vendors to preserve existing technology investments

HouseCall Server Illustration

The following is a conceptual model of what HouseCall Server and HouseCall Client does to protect your clients.

Main Features

HouseCall Server helps you to secure your clients with a lightweight interface at the client.

Client Features

- Detects and removes malware (Viruses, Worms, Trojans, etc.)
- Detects and removes grayware and spyware
- Detects rootkit based malware
- Restores damage caused by malware to your system
- Notifies about vulnerabilities in installed programs and connected network services
- Multi-platform support for Windows and Linux
- Easy-to-use with the following browsers: Microsoft Internet Explorer, Mozilla Firefox

Server Features

- Secure configuration via a password-protected web-based administration tool
- Scheduled updates of program components
- Status on client side scans and cleans is maintained in a SQL database, including client identification based on MAC, IP and username. An open notification API allows to attach implicit custom actions optionally (Java development required)
- Receives automatic updates from TrendLabs and each PC is updated upon access to keep users maschines current.

New Features in HouseCall Version 6.6

- HouseCall server installer
  - Online registration
  - Microsoft IIS Integration
  - Apache Derby Database Integration
  - Java Environment Integration
  - Apache Tomcat Integration
- HouseCall Launcher Application
- HouseCall Client Uninstaller
- Profile based scanning support
- Improved Client scan status
- Granular scan, Cleaning options and pattern file update functions
- Enhanced reporting options

HouseCall External Modules

VSAPI	8.3
SSAPI	5.0
DCE	5.0
ActiveUpdate	2.8
TmEngDriv (dll)	1.5
AntiRootKit (sys)	1.5

Using the Product Documentation

The documentation set for this product includes the following:

- Getting Started Guide or Administrator's Guide—This Guide helps you get "up and running" by introducing Trend Micro HouseCall 6.6 Server Edition, assisting with installation planning, implementation, and configuration, and describing the main product functions. It also includes instructions on testing your installation

using a harmless test virus. The latest version of the Guide is available in electronic form at:

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

- Online help—The purpose of the online help is to provide "how to's" for the main product tasks, usage advice, and field-specific information such as valid parameter ranges and optimal values. Online help is accessible from the HouseCall management console.
- Readme file—The Readme file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues and release history.
- Knowledge Base— The Knowledge Base is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues.

Chapter 2

Installation Planning

This chapter presents an installation planning summary and different topologies for the HouseCall Server.

Topics discussed in this chapter include:

Installation Planning Summary

As a web application, HouseCall Server Edition needs a servlet container that supports the Java Servlet and JavaServer pages technologies and also requires a database. In addition a web server can be used before the servlet container to handle incoming requests.

As for the database, the service can run locally or on the network using TCP/IP protocol.

All neccessary 3rd party software that is needed to install, configure and run the HouseCall server, is included in the HouseCall server installation setup process. No other Software is required to run the HouseCall server

The HouseCall Server requires an Activation Key to be authenticated at the Trend Micro HouseCall Root Server.

Recommended System Requirements

Install HouseCall Server Edition on a system with the following software and hardware:

Hardware:

- 1GHz Intel™ Pentium™ processor or equivalent
- 1GB RAM
- At least 5GB of available disk space for system partition
- At least 4GB of available disk space for caching (own fast and secure partition recommended - RAID5)

Operating System (Server):

- Microsoft Windows 2000 (Adv) Server and 2003 Server or,
- Linux Distributions Red Hat™ Enterprise Linux (ES, AS) 4.0, SuSE™ Linux Enterprise Server 10.x, Fedora Core 6, OpenSuSE 10.2

Software on Server Site:

- HouseCall 6.6 SE application (included in HouseCall Server installer)

Software on Client Site:

If Linux is used as the HouseCall SE Operating System with no X-Server installed, then a client PC is needed for remote validatation of the installation

- Microsoft Windows 2000 Professional with SP4 or above
- Microsoft Windows XP Home or Professional with SP1 or SP2
- Microsoft Windows XP Media Center Edition 2004, 2005
- Microsoft Windows XP Tablet PC Edition 2004, 2005
- Microsoft Windows XP 64 bit Edition
- Any GUI HTTP1.1 compliant browser

Note: Windows Resolution 1024 * 768 (XGA) and above

Network:

- HouseCall Server hostname DNS entry, for LAN name resolving
- Allow HouseCall Server listen on ports 80 and 443 for client connections or on port 8009 when IIS integration is used.
- You may specify a proxy server to allow HouseCall Server connecting to the internet
- Use a reverse proxy to improve HouseCall's performance
- Allow email notifications from HouseCall Server on your SMTP Server to be relayed, if enabled

Browser:

- Microsoft Internet Explorer 6.0 or later
- Mozilla Firefox Version 1.5 or later

Additional Notes:

- Mail Relay if HouseCall Server is not allowed to send notification emails
- Proxy Server for inbound requests to HouseCall Server from Clients is recommended HouseCall 6.6 SE Activation Key for activating the Server

Java Servlet/JSP Container

The HouseCall Server is designed as a Java Application and can optionally run on other Web Application Servers as long as they provide the Java Authentication and Authorization Service (JAAS).

Database

The database usage in HouseCall Server is designed with the JDBC technology to provide a cross-DBMS connectivity to SQL databases. If JDBC technology-enabled drivers are used, HouseCall Server can work with other SQL standard databases (e.g. PostgreSQL).

WebServer

A Web Services Adapter (JK from Apache Jakarta Project) plug-in can handle the communication between Tomcat and the Web Server.

Proxy Topology

HouseCall Server provides a choice to run in the default configuration or in an optional configuration with a Web Proxy cache in-between to the HouseCall Clients. Optionally, you can also configure an outbound proxy server to get access to the Internet.

HouseCall Server Proxy Chains

The diagram below provides an overview of how the HouseCall Server can be located between different proxy chains.

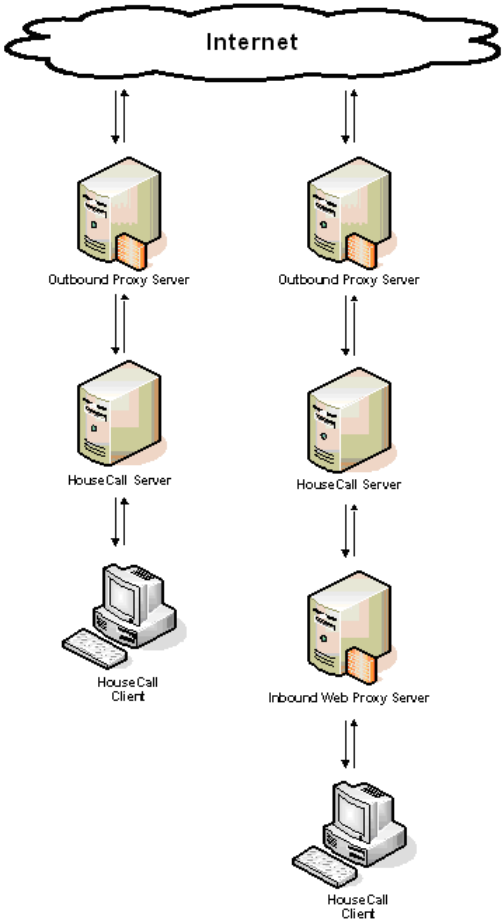


FIGURE 2-1 HouseCall Server proxy chains

Standard Configuration of the HouseCall Server

In the HouseCall Server standard configuration the HouseCall Clients connect directly to their HouseCall Server and the HouseCall Server uses direct connection or a proxy server to access the Internet and the Trend Micro HouseCall Server and ActiveUpdate Service. The database and the SMTP relay can be configured to a separate host or on the same server.

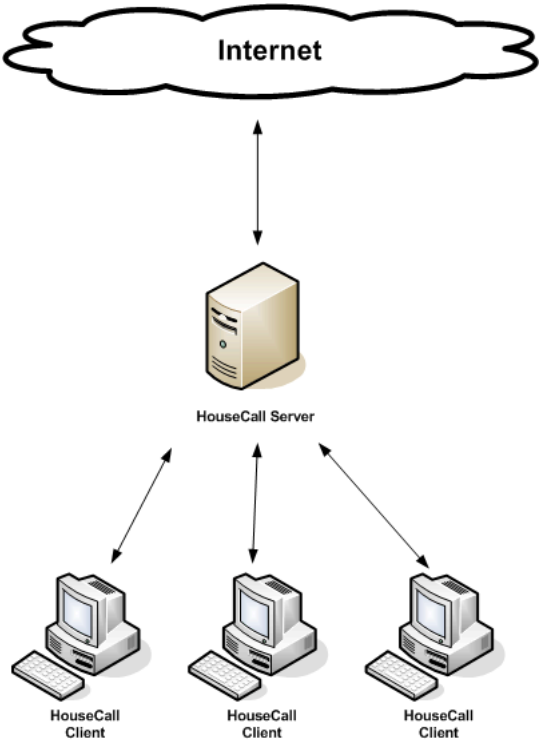


FIGURE 2-2 HouseCall Server without Web Proxy cache in-between

HouseCall Server and Web Proxy Cache

In a more complex configuration the HouseCall Server can work with a Web Proxy Cache between HouseCall Clients and HouseCall Server. The next figure shows an overview network diagram of this configuration.

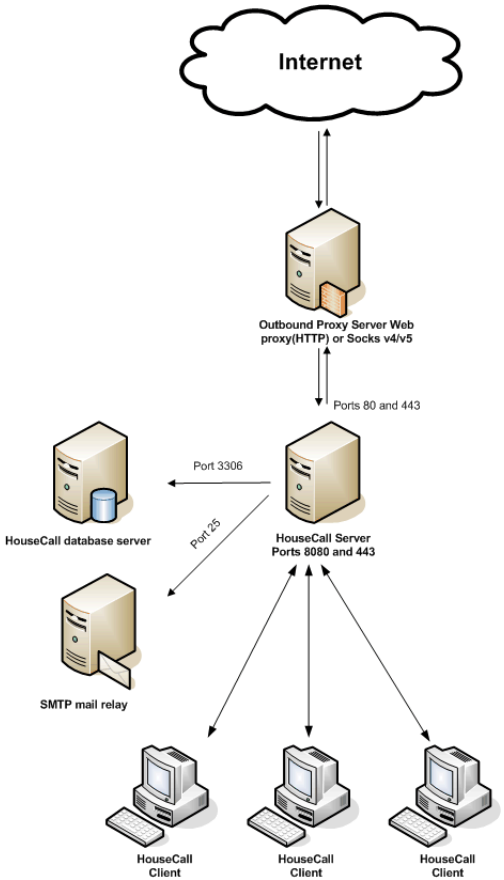


FIGURE 2-3 HouseCall Server with a web proxy server in-front

Database Setup

HouseCall Server is designed to use the database with the JDBC technology to provide cross-DBMS connectivity to SQL databases. The recommended database system is Apache Derby which will be provided and installed during the HouseCall installation process. The default database schema (housecall) and all related tables were configured during the HouseCall Server setup.

Chapter 3

Installation and Server Setup

In this chapter, you will find step-by-step instructions for installing and testing the HouseCall Server. Topics discussed in this chapter include:

Prerequisite Server Setup

Apache Derby Setup

Apache Derby is a relational database implemented completely in Java. It has a small footprint that allows it to be easily embedded into any Java application, disappearing from view and requiring no DBA administration. It also supports the more familiar client/server access model.

Install Apache Derby on Windows/Unix platforms

The Apache Derby database will be automatically installed by the HouseCall Installer program. All runtime specific settings for variables and path extensions will be performed from the installer procedure.

The HouseCall installation process uses Apache Derby as default database. If a different database already installed (e.g. PostgreSQL) and should be used to store HouseCall related data, during the setup procedure you can choose to implement an external database by selecting the “Custom Settings”.

Apache Tomcat Setup

The Trend Micro HouseCall Installer automatically installs and configures the Apache Tomcat Server Version 5.5.20 as a service on the local system. Apache Tomcat will be installed and configured, independent from any previous Tomcat version that might be already installed and/or running on the system. No configuration changes will be completed on any previously installed version. This process is necessary to prevent any software related issues while uninstalling the complete HouseCall Server environment if this is needed, including the Apache Server version supplied with HouseCall.

HouseCall Server Setup

Trend Micro recommends that you install HouseCall Server Edition on a dedicated server. To install HouseCall Server you must log on to the target server as administrator or root to have equivalent access rights.

To install HouseCall Server Edition:

- You can install HouseCall Server Edition by downloading the installation files from the Trend Micro download page on the Web. (LINK TO TREND DOWNLOAD PAGE)
- If you are downloading from the Web, download the HouseCall Server Edition binary archive to a temporary directory on the server where you want to extract the HouseCall Server Edition files.

The install can be run using the Graphical Interface (GUI) or via silent mode with a pre-configured xml file (installer properties). A xml file is included in the HouseCall software package. The information made during the installation is written into a debug log that can be viewed if necessary.

- GUI - start setup.exe and confirm the further installation points
- Silent - start setup.exe with additional parameter: setup.exe -i -silent -f <xml file path>
- Debug - start setup.exe with additional arguments: setup.exe [-i -silent -f <xml file path>] -Ddebug=true

The HouseCall Server Installer file will initialize within a Java environment. You can start the installer either from Windows or any supported Linux based system.

Standard or Custom Installation

The HouseCall server installation setup routine offers two scenarios to install and configure the server settings.

Standard Installation

The standard installation is recommended for most HouseCall installations. HouseCall installation such as Apache Derby will be installed and standard configuration parameter will be set during the installation process. Only a few, easy to configure steps have to be completed manually to install and pre configure the installation.

Custom Installation

In addition of the standard settings and configurations steps, you can choose to walk through a custom setup routine when prompted during the setup. This should only be done by experienced administrators. The custom installation allows manually configure the following steps:

- IIS Integration
- Manual Port settings
- Customized Data Storage and Log
- Integration of a custom SQL based database

HouseCall Server Standard Installation

Starting the Installation

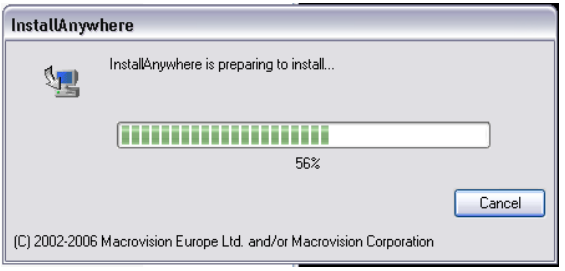


FIGURE 3-1 Install Anywhere starting screen

After you have downloaded the HouseCall Installer program file from the Trend Micro web site, you can start the installation process by double clicking on the "Setup" icon.

The HouseCall Installer is based on Macrovision InstallAnywhere. This installer shell is loading first and contains the HouseCall server setup process. You can cancel the installation any time by clicking the "Cancel" button.

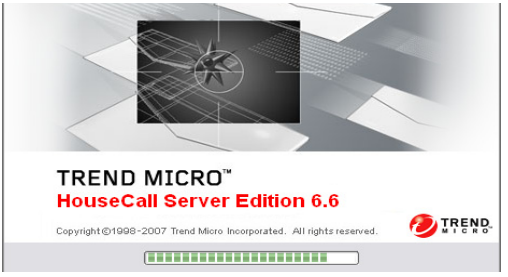


FIGURE 3-2 Trend Micro HouseCall Server Logo screen

After loading the installer shell, the Trend Micro HouseCall Server logo appears and the major setup procedure will be loaded.

Step 1 - Welcome Page

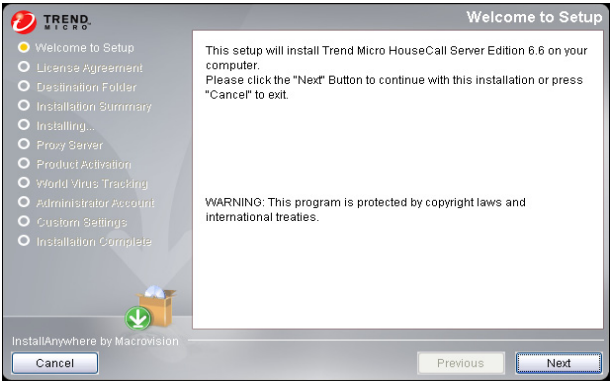


FIGURE 3-3 HouseCall Installation - Welcome Page

This is the Trend Micro HouseCall Server Welcome page. The installation steps on the left side shows you the current installation progress, marked with the yellow dot.

The grayed out items will be verified as the installation continues. Completed steps are displayed in white.

At any time during the installation process of the HouseCall server, you can cancel the installation by clicking on the “Cancel” button. Use the “Next” and “Previous” buttons to proceed with the next installation step, or move backwards to change or edit previously done settings and configuration.

Step 2 - License Agreement

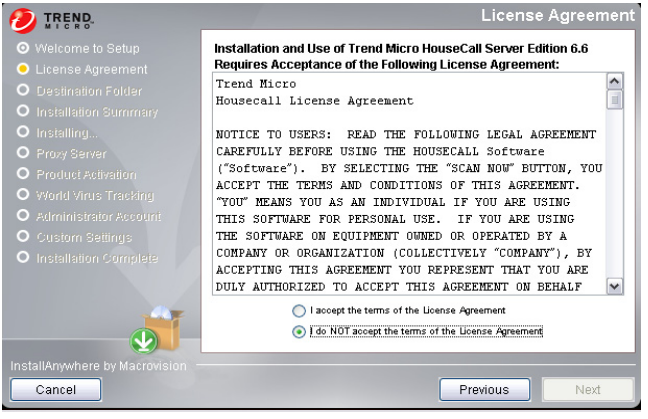


FIGURE 3-4 HouseCall Installation - License Agreement

The Installation and use of Trend Micro HouseCall Server Edition requires your acceptance of the displayed License Agreements. Please read them carefully and accept them by clicking the "I accept..." checkbox below the text frame. If you not sure of acceptance, please contact your company lawyer for assistance.

Note: As long as you have not accept the products License Agreements, the "Next" button will be inactive, and the installation process will not continue to the next configuration step.

Step 3 - Destination Folder

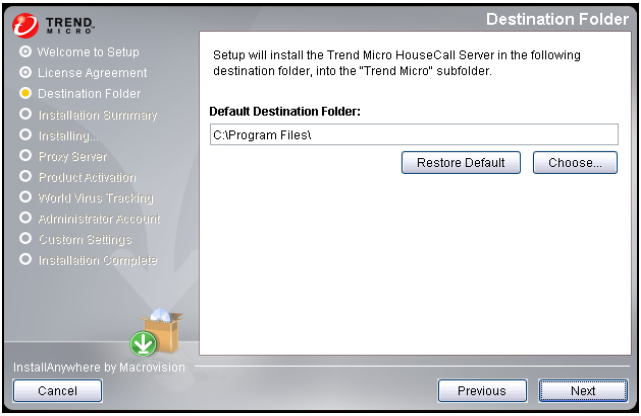


FIGURE 3-5 HouseCall Installation - Destination folder

Please select a destination folder to install the HouseCall server files. By default, the server directories and files will be installed under the local “C:\Program Files\” folder.

You can select to use a custom drive and directory by clicking on the “Choose” button, or restore the default folder settings by a click on the “Restore Default” button.

After you select the installation path and folder, the installer program validates your entries by checking the destination folder for existence and to ensure sufficient disk space to install the HouseCall server files.

Click on the “Next” button to start the validation and proceed to the “Step 4 - Installation Summary“ screen.

Default Folders:

- Windows - %PROGRAMFILES%\Trend Micro\HouseCall Server Edition 6.6
- Linux - /opt/trend/HouseCallSE66

Step 4 - Installation Summary

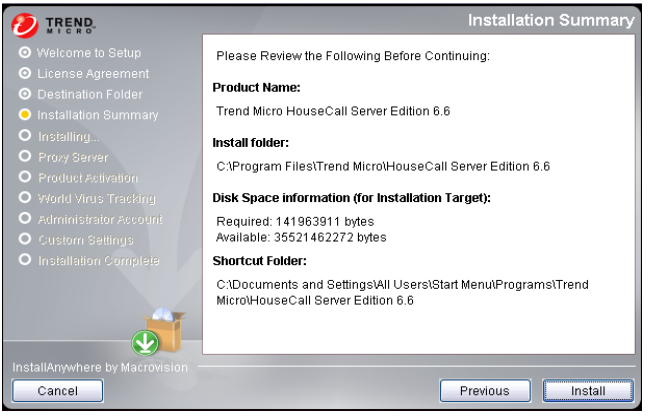


FIGURE 3-6 HouseCall Installation - Installation summary

The summary screen shows the settings and the result of the disk space validation process from the installation path provided on the previous screen.

If there is not sufficient disk space available on the selected drive or folder to install the HouseCall server, please return to the previous installation step and configure a different installation location.

Step 5 - Installation Progress

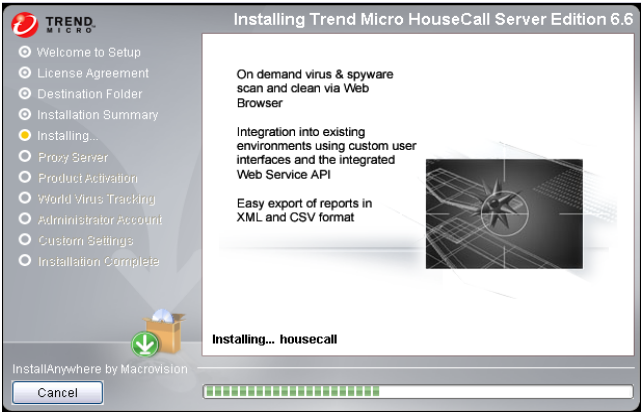


FIGURE 3-7 HouseCall Installation - Installation Progress

All necessary program files will now be installed into the selected location. This may take some time, depending on your local systems capability. After the file copy process, the next screen will appear to start configuring the basic settings for the HouseCall server.

Step 6 - Proxy Server

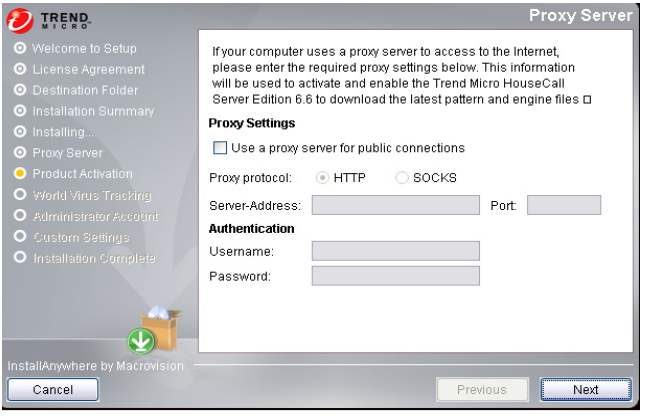


FIGURE 3-8 HouseCall Installation - Proxy Settings

This configuration step is needed to establish a connection to the internet. This connection is required to validate and register your HouseCall server and to retrieve the latest pattern and Engine files to ensure your server and it´s components are up-to-date.

If you **do not use a proxy server** to connect to the internet, no settings are required to be configured. You may proceed with the next installation step.

If you **use a proxy server** to connect to the internet, please activate the checkbox and fill in the required connection information. If your proxy uses authentication, please type in a valid user account name and password.

If you are not sure if you are using a proxy server or not sure of the required settings, please ask your network administrator for help. After the settings have been completed, click “Next” to proceed. The connection settings will now be validated. If no connection can be established, you will be notified with a pop up message and will need to verify your proxy settings.

Note: HouseCall supports Proxy and SOCKS connection without authentication.

Step 7 - Product Activation

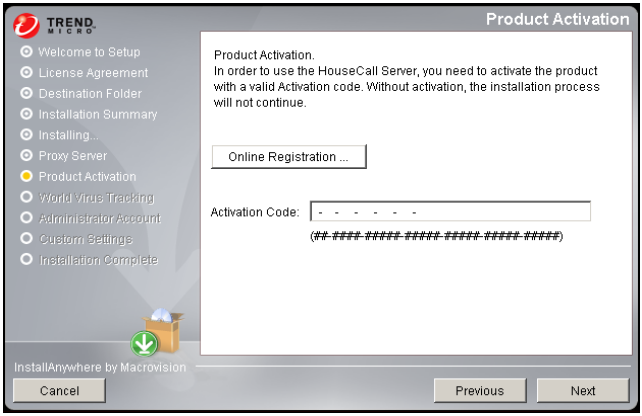


FIGURE 3-9 HouseCall Installation - Product Activation

In order to use the HouseCall Server, you need to activate the product with a valid Activation code. Without activation, the installation process will not continue. If you enter an invalid activation key or a wrong syntax, the following screen will be shown. Please assure that your activation key is valid and you enter the correctly.

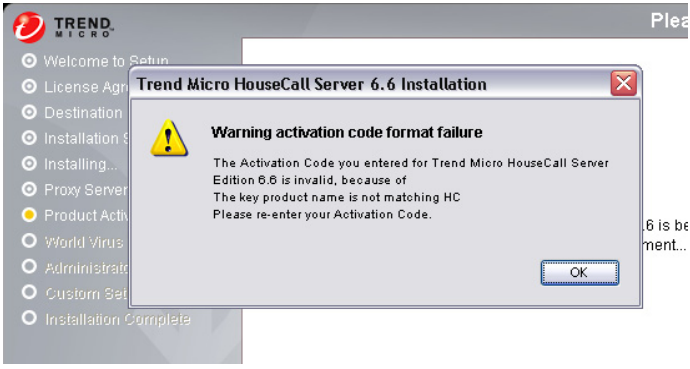


FIGURE 3-10 HouseCall Installation - Product Activation - Invalid

If you **do not have an Activation code**, first click on the “Online Registration” button to connect to the Trend Micro Registration web page and register your product. After successful registration, you will receive an Activation code which allows you to proceed with the installation.

If you already have a **valid Activation code** from Trend Micro, you can skip “Step 1" to register your product first. Continue to type in the code and ensure the correct syntax is used as shown in the screen below in the “Activation Code” input field.

After you entered the Activation Code and click on the “Next” button, the code will be validated (Figure 3-11) by Trend Micro. If the code is not valid for any reason, please check the correct syntax has been used. If you still have problem to validate the Activation code, please ask your Trend Micro sales representative for help. After successful validation, the Installer automatically proceeds to the next installation step.

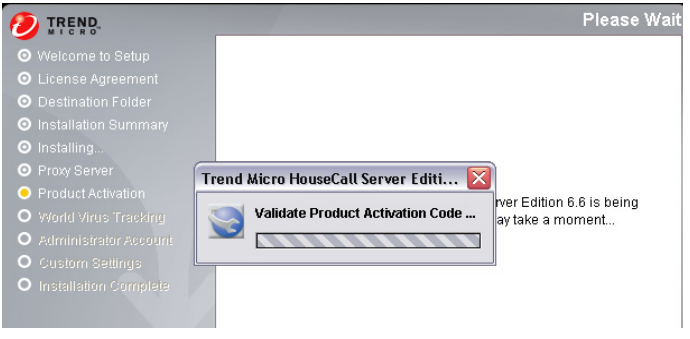


FIGURE 3-11 HouseCall Installation - Product Activation - Validation

Note: Please ensure that the server date is correct as SSL validation will fail and the installation program will be cancelled. The date has to be in the range of the SSL.

Step 8 - WTC Settings

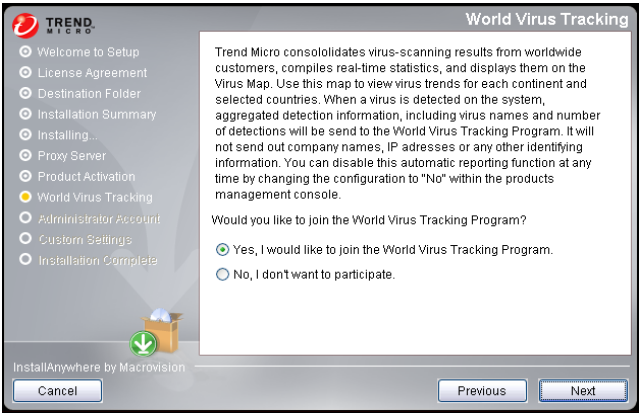


FIGURE 3-12 HouseCall Installation - World Virus Tracking Program

Participating in the World Virus Tracking Program, allows your HouseCall server to send specific data about infections and vulnerabilities to be collected by Trend Micro for statistical reasons. Trend Micro use this data to create a dynamic map to analyze worldwide virus trends in real time.

If you would like to participate in this program, select the “Yes ...“ checkbox, or “No ...“ if you do not like to participate.

Trend Micro consolidates virus-scanning results from worldwide customers, compiles real-time statistics, and displays them on the Virus Map. Use this map to view virus trends for each continent and selected countries.

When a virus is detected on the system, aggregated detection information, including virus names and number of detections will be send to the World Virus Tracking Program. It will not send out company names, IP addresses or any other identifying information.

Note: You can disable this automatic reporting function at any time by changing the configuration to “No” within the products management console.

Step 9 - Administrator

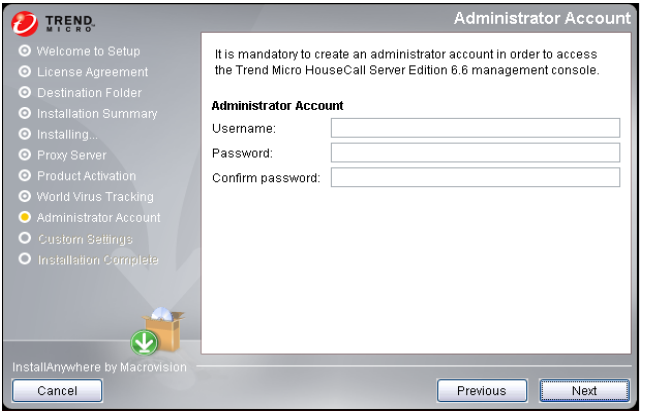


FIGURE 3-13 HouseCall Installation - Administrator Account

In order to login to your HouseCall server web console to configure your server, you have to create an administrators login account. Type in an username and password and confirm your entries. After the HouseCall server is successfully installed and you enter the server web console for the first time, you have to login with these settings.

You can modify this account at any time later on the server web console.

Note: On the web console, it is only allowed to change to password. The username remains as defined during the installation and is not changeable.

Step 10 - Custom Setup

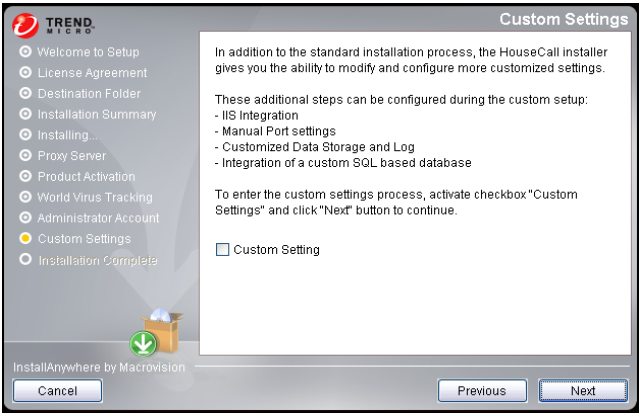


FIGURE 3-14 HouseCall Installation - Custom Setup

Choosing to configure “Custom Settings” will lead you to some additional installation screens, where you can configure environment specific settings to customize your HouseCall server. For more detail on the custom settings, please see *HouseCall Server Custom Installation* on page 3-19 later in this chapter.

Step 11 - Installation Complete

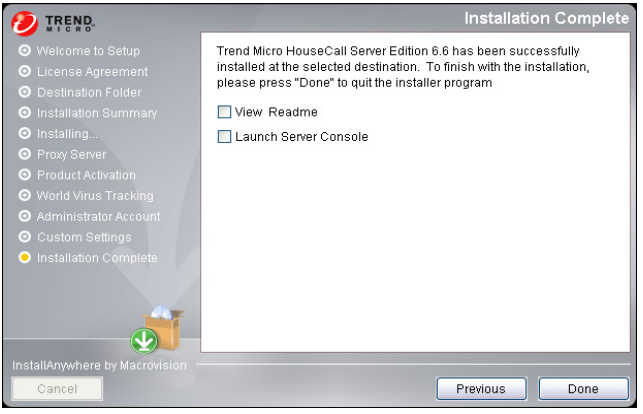


FIGURE 3-15 HouseCall Installation - Installation Complete

This is the final screen of the installation routine. If all settings are correct and the server is successfully installed, you will see the “Installation Complete” window.

After clicking on the “Done” button, you can click on the checkbox to either to view the readme file, or to automatically launch the HouseCall web server console.

If you choose to automatically launch the HouseCall server, a browser window opens the HouseCall server web console where you can configure your server settings, accounts, reporting and other server related tasks as described in “Chapter 4: HouseCall Server Web Console” later in this manual.

HouseCall Server Custom Installation

About Custom Installation

In Addition to the standard installation process, the HouseCall installer gives you the ability to modify and configure more customized settings. These additional options allows you to integrate and customize the HouseCall server into an existing local environment to meet your company profile.

These additional steps can be configured during the custom setup.

- IIS Integration
- Manual Port settings
- Customized Data Storage and Log
- Integration of a custom SQL based database

To enter the custom settings process, activate checkbox “Custom Settings” at Custom Settings screen and click “Next” button to continue.

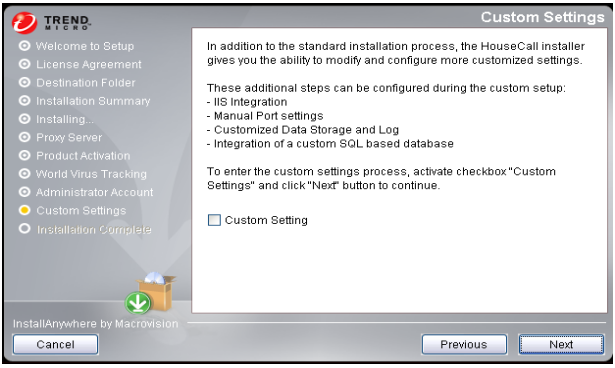


FIGURE 3-16 Custom Settings - Activate Checkbox

Custom - Server Integration

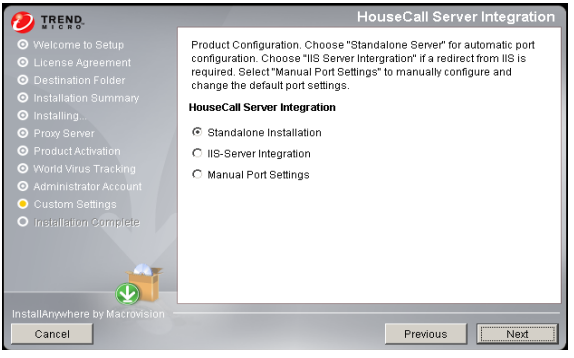


FIGURE 3-17 Custom Settings - Server Integration

Choose “Standalone Server” if you don’t have an IIS web server in front of the HouseCall server and you will use the standard configured port 80 as listener port. A preconfigured server will be installed where Log and Storage paths can be specified. Also remote access to internal Derby database and including external PostgreSQL.

If you are using an IIS server in front of the HouseCall server, you can configure the HouseCall server web API to retrieve data coming from the IIS. Choosing “IIS Integration” from the menu, the port where HouseCall listens for incoming communication from the web, this will be automatically set to the next free open port (e.g. port 81 for HTTP). This will be defined as listener port for incoming data from the IIS. HouseCall creates a redirection rule from IIS to HouseCall on the local server where Log and Storage Path can be specified.

If you like to configure your server to listen on a different port, you need to choose “Manual Port Settings” from the menu and customize your port settings.

Custom - Manual Port Settings

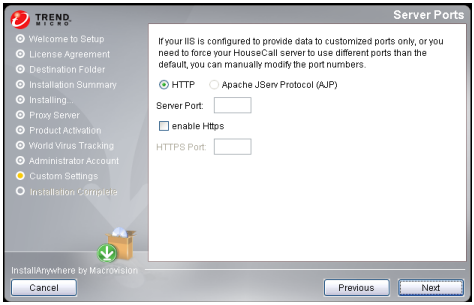


FIGURE 3-18 Custom Settings - Manual Server Ports

If you need to force your HouseCall server to use different listener ports than the default, you can manually modify the port numbers of the HouseCall server to support your local environment.

In case you plan to locate the HouseCall server behind any Web Server that supports the AJP protocol (e.g. Apache / IIS), you have to modify the ports to enable this protocol.

Three different ports can be configured:

- HTTP Port (default 80)
- HTTPs Port - Enable and set (default 443)
- AJP (Apache JServ protocol) Port (default 8009) - is needed for IIS Integration. Can only be enabled if IIS is installed on local system.

The following ports were automatically checked for availability by the HouseCall installer:

- *For HTTP* : Ports 80, 8080 - 8442
- *For HTTPs*: Ports 443, 8443 - 8888
- *For IIS*: Ports 8009, 8010 - 8079

Note: Server Certificates can be displayed if HTTPs is used.

Custom - Certificates

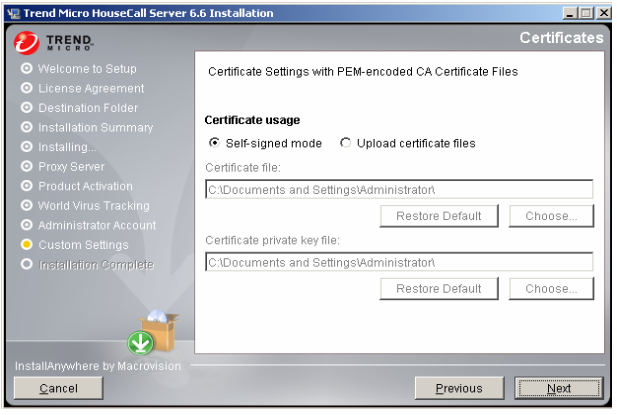


FIGURE 3-19 Custom Settings - Certificates

Server Certificate Information is needed for HTTPs using. HouseCall delivers certification and private key.

Default HouseCall Path

- Certificate: %HOUSECALL_HOME%\server\conf\cert.crt
- Private Key: %HOUSECALL_HOME%\server\conf\cert.key

Custom - Data Storage and Log

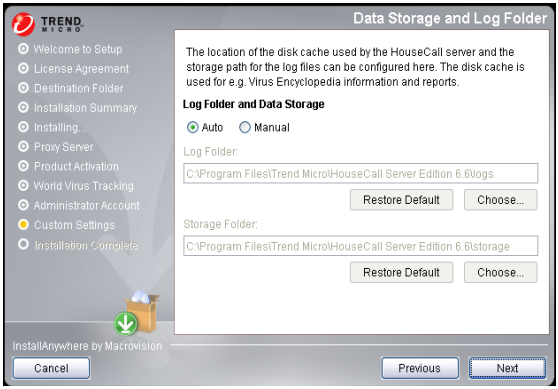


FIGURE 3-20 Custom Settings - Data Storage and Log

The location of the cache used by the HouseCall server and the storage path for the log files can be configured here. The cache is used for e.g. Virus Encyclopedia information and reports.

Usually the size reach between 50 and 100 MB of disk space, but can grow to several Gb size, dependent on the systems load (e.g. number of clients). The disk storage will be automatically organized by the HouseCall server to refresh and clean unused entries. If you set a new path for the cache, please ensure you have at least 100 MB of free disk space available.

To change the default path to store the HouseCall server log files, activate the “Manual” checkbox and edit the default pathname to a desired valid path.

The default path can be restored at any time by clicking the “Restore Default” button.

Three sub-folders will be created under the storage path.

- *cache* - stores all files and data that will be cached from the system (former “disk cache” in previous HouseCall versions)
- *attachments* - a temporary storage folder for the WebService API layer
- *database* - this folder hosts the data files for the Apache Derby database

---

Note: Please verify that there is enough disk space for the cache has remaining on your local hard drive. Please also ensure that there is enough disk space at the chosen location to store the log files. See also the recommended hardware requirements in Chapter 2 “Installation Planning“.

Custom - Database Selection

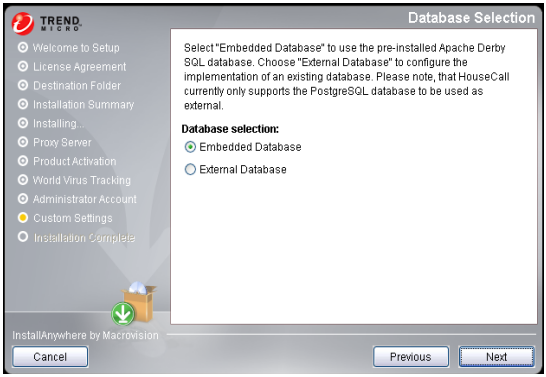


FIGURE 3-21 Custom Settings - Database Selection

Select “Embedded Database” to use the pre-installed Apache Derby SQL database. You can configure a remote account for login to the database on the next configuration setup page when you click “Next”.

If you would like to use an existing SQL database instead of the integrated Apache Derby, you need to configure HouseCall to implement this database.

Choose “External Database” to configure the implementation of an existing database.

Note: Currently only PostgreSQL database is fully supported to be used as external database by the HouseCall server

---

Embedded Database

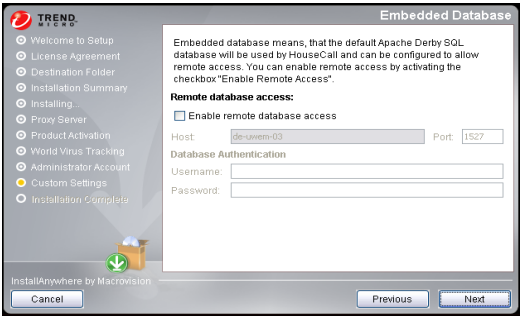


FIGURE 3-22 Custom Settings - Database Selection - Embedded

Embedded database means, that the default Apache Derby SQL database will be used by HouseCall and can be configured to allow remote access. You can enable remote access by activating the checkbox “Enable Remote Access”.

In order to use the remote access ability of the database, an account will have to be created for the remote user to login.

Type in the Username, Password and the port number (default port 1527) for the remote account and click “Next”.

This settings will be used to create an account in the database which can be used to login with from remote. When you remote login to the database, you will be asked for the database name that is used for the HouseCall server.

The default database name for Apache Derby is “housecall”. The schema that is used, is Derbys default schema "public".

To remotely login to the Apache Derby database, you need to have the DB2-ODBC drivers installed on your system. You can download the needed drivers from the IBM DB2 support web site. *(http://www-128.ibm.com/developerworks/db2/library/techarticle/dm-0409cline2/index.html)*.

If you are using the java variant of the ODBC drivers (JDBC), the syntax of the URL to connect to the database is “jdbc:derby://[hostname]:[port]/housecall”

With the required ODBC drivers installed, you will be able to connect to the database from any application that supports these type of connections, like e.g. MS-Access, Excel or Visio.

External Database

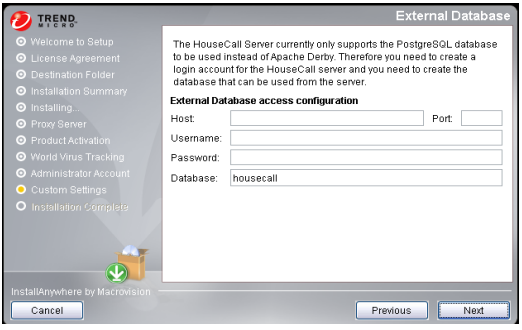


FIGURE 3-23 Custom Settings - Database Selection - External

HouseCall currently only supports the PostgreSQL database to be used instead of Apache Derby. Therefore you need to create a login account for the HouseCall server and you need to create the database schema that can be used from the server.

This schema will be used from the HouseCall server to store the data into the PostgreSQL database. Type in Host and Port where the PostgreSQL is located. Also type in the username and password for the account to allow HouseCall to be connected and login to your existing database.

Note: It is recommended to use the default schema named “public”. Please assure, that the given account for the server have full rights (create, alter, select, drop insert, update and delete) on the chosen database schema.

When the HouseCall server connects to the database and locates the default “public” schema, it will automatically create the required database tables.

This is the final custom configuration step inside the HouseCall server custom installation. The next step refers to the “Installation Complete” screen as described in section *Step 11 - Installation Complete* on page 3-18.

Migration of HouseCall Version 6.5 to Version 6.6

The previous HouseCall server Version 6.5 uses the Microsoft *MySQL* database by default to store the server related settings. To overtake the database content from MySQL to the new *Apache Derby* database, a ***Migration Tool*** was created, to transfer your previously done settings and configuration into the new database.

Follow the migration steps described below to move your configuration data into the new Apache Derby database environment.

Note: Please be aware, that while processing the migration steps, any existing data from a previously done HouseCall version 6.6 configuration will be overwritten and replaced with the configuration data from version 6.5. To avoid replacing existent database tables and content, it is recommend to migrate the configuration content from version 6.5 **before** running the version 6.6 server for the first time!

The tool can be found at the following location:

"\Program Files\Trend Micro\HouseCall Server Version 6.6\tools\migration" (or any equivalent directory you have selected to install the server files).

HouseCall 6.6 supports

- a built-in database, based on "Apache Derby" and the network interface compatible with "IBM DB2"
- an external SQL-based database (*Note*: Currently supporting "PostgreSQL" only)

Migration steps:

1) You can either start the application ("ServerMigration.jar") from the command line with "java -jar ServerMigration.jar", or simply by using the batch file "servermigration.bat" which can be found in the same location.

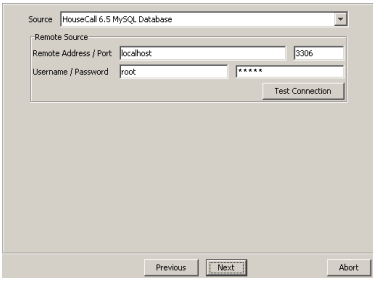


FIGURE 3-24 Migration Tool Settings

2) After passing the "Welcome" screen, the remote database source and connection information needs to be configured, in order to allow the tool to connect to any existing database and to migrate the neccessary data.

Type in the correct administrators login account information for the existing MySQL database.

To check that the tool can access the database in order to migrate the database content, click on the "Test Connection" button. The tool tries to connect to the database with the given information. If the test runs successfully, click "Next" to continue. If the tool can not connect, please review the connection information.

3) A final warning page appears and you need to confirm the migration process.

4) After your confirmation, the database content from the source database will be automatically migrate into the new Derby database structure. A log file for the migration process will be written and stored at the "\logs" directory.

5) Finalize the migration by clicking the "Finish" button. The data has now be moved from the original configured source database into the new Apache Derby and will automatically be used after a server restart. Proceed to the Server Web console to check the correctness of the migration process.

The new database credentials needs to be configured in the "config.xml" file, located in the HouseCall config directory.

To configure the **built-in** Apache Derby database:

- Set parameter "database.external" to "false"
- Enter login information to connect to the database at parameter "database.builtin.network.username" and "database.builtin.network.password"

To configure an **external** database (PostgreSQL):

- Set "database.external" to "true"
- Enter "database.external.hostname", "database.external.port", "database.external.schema", "database.external.username" and "database.external.password" to connect to the external database.

Testing HouseCall Server

After finishing the installation, the installer creates a new service entry under Windows. This service is set to automatically start after a system reboot.

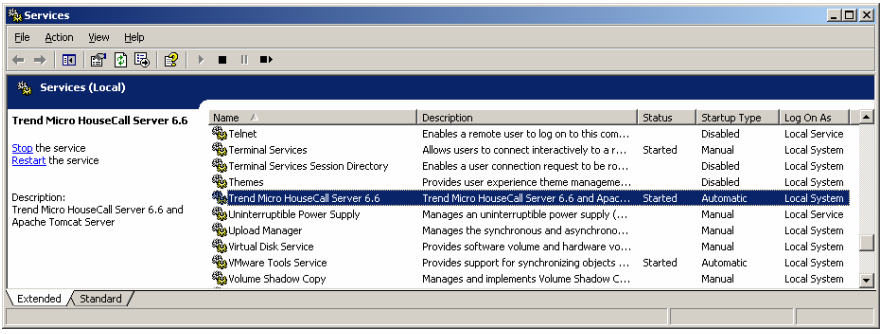


FIGURE 3-25 HouseCall service entry

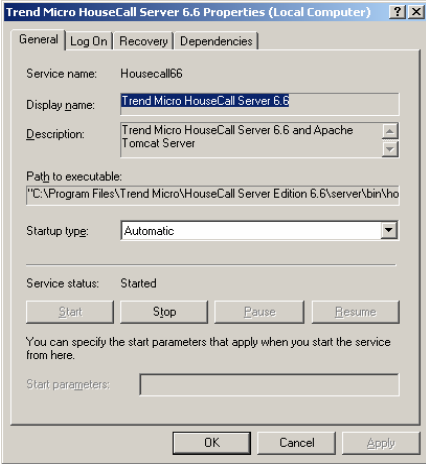


FIGURE 3-26 Service Settings

The HouseCall installer creates also a new program folder entry into the Windows Start menu.

FIGURE 3-27 Program Folder Entry

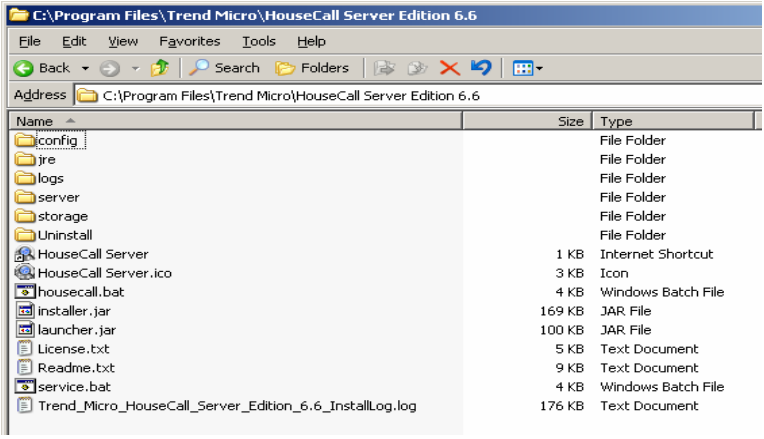


FIGURE 3-28 HouseCall Folder structure

config	Includes global configuration files.
jre	Includes JRE 1.6.
logs	Includes log files.
server	Includes TomCat 5.5 server and HouseCall folder.
storage	Includes Apache Derby 10.2.2.0 database and cache information.
Uninstall	Includes uninstaller information for HouseCall 6.6.

FIGURE 3-29 HouseCall folder legend

After completing the HouseCall Server installation, you can access the Web console by typing:

http://domain:<port>/housecall

http://<machinename>:<port>/housecall

http://123.123.123.12:<port>/housecall

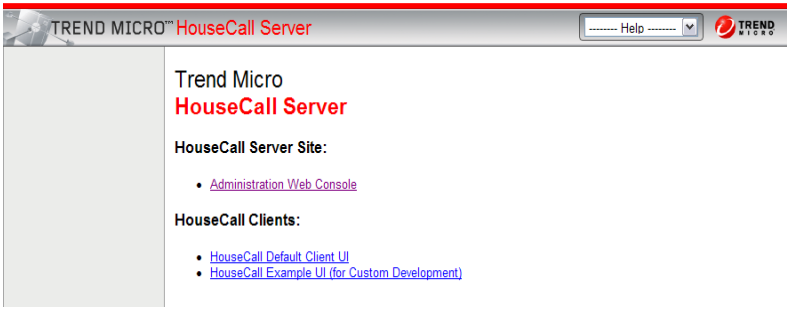


FIGURE 3-30 HouseCall Server Web Console

Clicking on **Administration Web Console** opens a login window. Login with your admin account and proceed as described in *HouseCall Server Web Console* on page 4-1.

You can start the HouseCall Client by clicking on **HouseCall Default HTML-UI**. Then proceed with *Testing HouseCall Client* on page 3-34 or *HouseCall Client* on page 3-36.

Testing HouseCall Client

Trend Micro recommends testing your product and confirming that it works by using the EICAR test script. EICAR, the European Institute for Computer Antivirus Research, developed the test script as a safe way to confirm that antivirus software is properly installed and configured. Visit the EICAR Web site at http://www.eicar.org for more information.

The EICAR test script is an inert text file with a *.com extension. It is not a virus and does not contain any fragments of viral code, but most antivirus software will react to it as if it were a virus. Use it to trigger a virus incident and confirm that email notifications, HTTP scanning, and virus logs work properly.

WARNING! *Never use real viruses to test your antivirus installation.*

To test your installation's ability to detect an infected file:

Open an ASCII text file and copy the following 68-character string to it:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
$H+H*
```

Save the file as EICAR.com to a temp directory. If there is an antivirus installation on your machine, it should immediately detect the file.

To test other computers on your network that your antivirus installation is currently protecting attach the EICAR.com file to an email message and send it to one of the computers.

Note: Trend Micro also recommends testing a zipped version of the EICAR file. Use compression software to zip the test script and perform the steps above.

To test your installation's HTTP scanning capability:

Download the EICAR.com test script from either of the following URLs:

http://www.trendmicro.com/vinfo/testfiles/
http://www.eicar.org/anti_virus_test_file.htm

Updating

Both HouseCall Server and HouseCall Client require up-to-date components. For your convenience HouseCall Clients are updated automatically. This section provides information about how HouseCall components are updated and where related information can be found.

HouseCall Server

The HouseCall Server acts as the update server for the Clients. Update components that are provided to the HouseCall Clients include the scan engine and the pattern file along with configuration settings. The HouseCall Server itself updates all program components from the HouseCall Root Server and all scan engine and pattern files from the Trend Micro ActiveUpdate Server. The update schedule can be configured on the HouseCall server web console at “Updates - Pattern & Engine“.

Where to find Update Information?

Current update information can be found on the “Summary” page at the administration web console.

HouseCall Client

The HouseCall Client uses automatic update procedure. It is updated each time it connects to the HouseCall Server.

Update Procedure

The HouseCall Client is downloaded from the HouseCall Server and updates itself and the scan engine and pattern files from the HouseCall Server.

Where to find Version Information?

Version information about HouseCall Client components, scan engine and pattern files is stored in the log file. The log file is locate under “log/housecall.log”

See *Configuration Files* on page A-1 for more details.

Upgrade HouseCall Server

The HouseCall server does only support the upgrade from the same 6.6. Version 6.6 with a new build. It does NOT support any upgrade from version 6.5 or earlier to Version 6.6. While trying to upgrade from a previous version, you will get an error message popup.

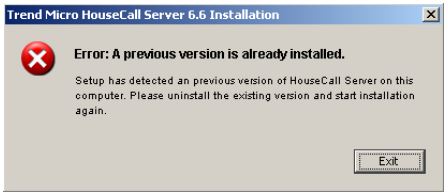


FIGURE 3-31 Upgrade Error Message

Uninstalling the HouseCall Server

The HouseCall server can be fully removed from your system by running an un-install routine from the Microsoft Windows Software Add/Remove panel.

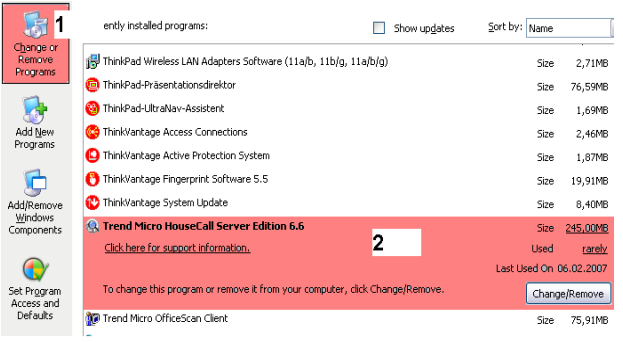


FIGURE 3-32 Uninstall HouseCall Server - Remove Program

From Software Add/Remove Panel (1), select “Trend Micro HouseCall Server Edition 6.6" (2) and click “Change/Remove” Button. This will start the removal program for the HouseCall server.

Uninstaller Program

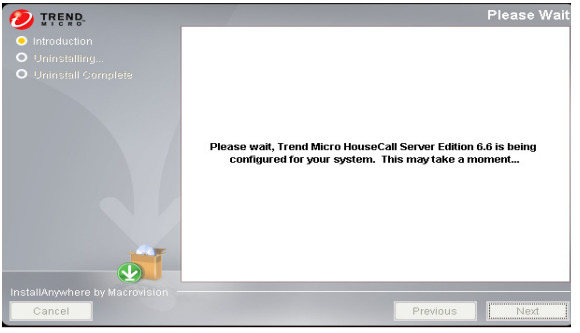


FIGURE 3-33 Uninstall HouseCall Server - Configuring

This uninstallation screen will appear and configures the files that need to be removed.

Confirm Uninstallation

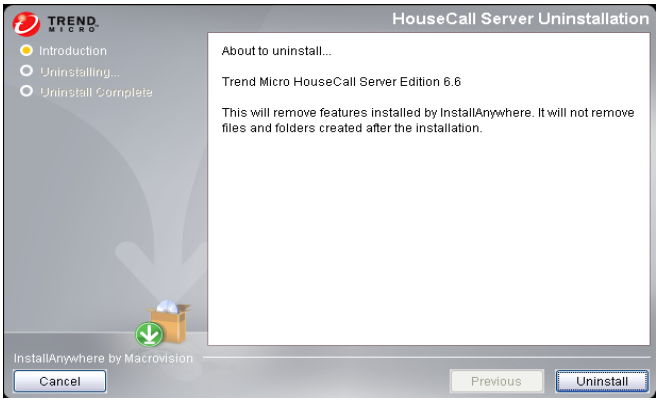


FIGURE 3-34 Uninstall HouseCall Server - Confirm

After configuration, you will be asked for the last time to assure you really want to remove the HouseCall server from your system.

Please confirm the deletion and remove the HouseCall server files by clicking the "Uninstall" button. Now the files and entries will be removed and cannot be restored.

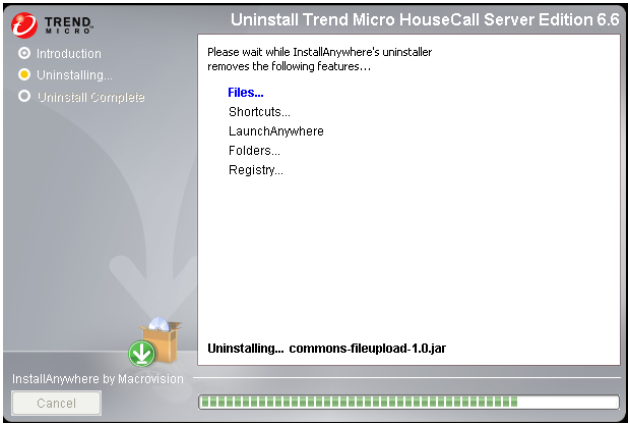


FIGURE 3-35 Uninstall proceeds

Uninstalling Complete

FIGURE 3-36 Uninstall HouseCall Server - Completed

After deleting all files and entries from your local system, click “Done” button to exit the uninstall routine. The HouseCall server program entry will now be removed from the Software list.

Chapter 4

HouseCall Server Web Console

This chapter explains how to use the HouseCall Server Web Console. Topics discussed in this chapter include:

Accessing HouseCall Server Web Console

Open a Web browser, and type the HouseCall Server URL your web server is listening to. Connect to the HouseCall Server computer using the qualified domain name, machine name, or IP address. For example,

http://<domain>/housecall

http://<machinename>/housecall

http://123.123.123.12/housecall

The following screen should appear. Click on “Administrator Web Console” link to proceed to the HouseCall server web console.

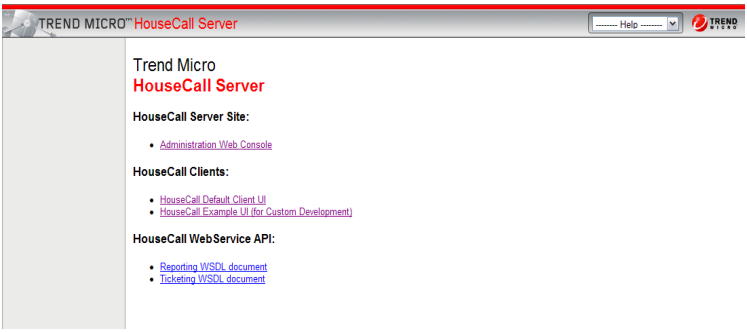


FIGURE 4-1 HouseCall Browser Link

Note: The links in the browser window are based on regular HTTP. If you like to transfer your login information more securely and encrypted, it is recommended to use a HTTPs connection if possible.

Login to Web Console

The HouseCall Server Web Console requires authentication before you can enter the configuration pages. Type in the administrator username and password as created during the HouseCall setup process to login to the web console.

FIGURE 4-2 HouseCall Login Screen

Using Help on the Web console

If you require help on any page you are working on, click on the button in the upper right corner on each page. This will open a help content window linked to the page that you require help with.

Summary (Live Status Page)

This summary page will be shown as the very first screen after you login to the server and enter the HouseCall Server Administration Web console. Here you can find important information of the servers current status, categorized in four major sections:

- Infection Summary
- Access Summary
- HouseCall Server Status and
- Update Status

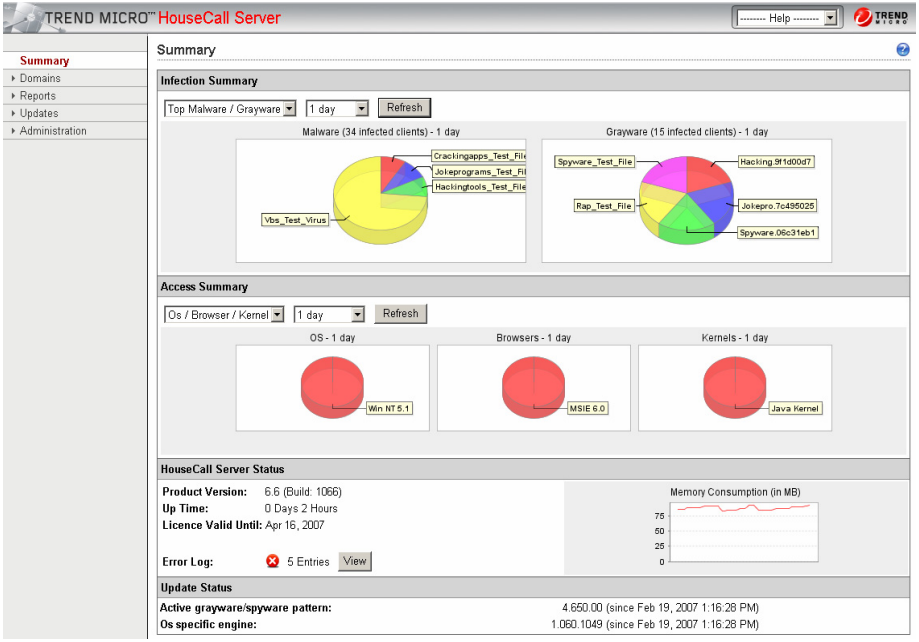


FIGURE 4-3 HouseCall Server Summary screen

Infection Summary

This section provides detailed information about malware, grayware and vulnerability detections. Select the information source to be shown from the first drop-down menu.

Any of the information can be shown in different selectable time ranges from 1 hour up to 3 months by choosing the appropriate time range from the second drop-down menu

As soon as you select any of the items from one of the drop-down menus, the screen will be refreshed automatically. To reflect the information shown, click on the "Refresh" button

Access Summary

The Access Summary section shows multiple information categories about the connected clients choose the selection to be shown from the first drop-down menu.

Selectable values are:

Load - Information about the count of connected HouseCall clients

Load w/o Hits - is the short term for "Load without Hits". As every client might produce several hundred hits which makes a graph a little bit unreadable, we have two sorts of graphs, one with hits included and one with hits filtered.

The reason to have "hits" included is because the hits will indicate the real network load and should significantly fall as soon as a reverse caching proxy is set in front of the HouseCall server.

Language / Country - Information about browser language and country settings

OS / Browser / Kernel - Summarized information about users operating system, the browser used (e.g. IE, Mozilla...) and used HouseCall client kernel (ActiveX or Java)

OS - Information about the users operating system only (e.g. Win XP, Linux...)

Browser - Information about browser usage only (e.g. IE, Mozilla Firefox...)

Kernel - Information about kernel usage only (ActiveX or Java)

Any of this information can be shown in different time ranges, selected from the second drop-down menu from “Now”, which shows the current status, up to a range for showing the last 3 month

HouseCall Server HouseCall Server Status

The summary in the HouseCall server status section shows some basic information that are also important for the administrators

Product Version - the current HouseCall program version and build number

Up Time - elapsed time since the HouseCall server was last restarted

License Valid Until - the date when your current HouseCall server license will expire

Error Log - number of entries in the current server error log. Click on “View” button to show details

Memory Consumption (in Mb) - memory used by the HouseCall server

Update Status

The Update Status gives an overview of the current active virus pattern and scan engine files and their versions. The update status is composed out of the information sent by the clients. That means the status will only change after a client reported its updated versions.

Note: Note: To prevent from outdated virus pattern or scan engine files, the range of the update interval should not be longer than 30 minutes!

Domain Configuration

HouseCall can assign separate settings on domain names used by the HouseCall clients to connect. Most of the client UI customizations or scan profile settings are maintained in the configuration.

By default the hostname of the server will be added to the domain configuration during the startup process of HouseCall server and this entry can be used to change any client options.

All clients using this hostname in their connection URL will get the settings that you applied to this entry.

For using the multiple configuration feature, you need to:

- Setup your network to make an additional FQDN point to your HouseCall server
- Add the newly created FQDN to the domain configuration inside your HouseCall server and start configuring it.

Note: The domain name entered inside the configuration must match the exact value used inside the connection URL for the clients

---

HouseCall supports a scheme of “virtual hosts” that allows to maintain multiple configurations for Scan and Clean technology and other features using a configuration interface that is sensitive to full qualified domain names (FQDN) or server hostnames that are configured inside your environment to access this HouseCall Server.

As HouseCall is designed to work in public potential unsafe networks, a domain configuration must be present if the requested or requesting hostname is not in a private IP range.

Domain - Settings

Domain usage means that one HouseCall Server can host multiple domains, each having different configuration parameters.

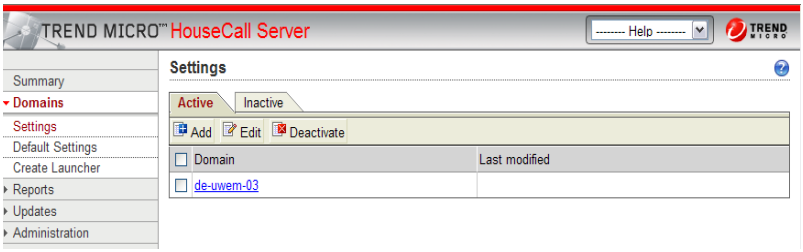


FIGURE 4-4 Domain settings

Active - Inactive Domain Folders

This overview returns a list of all currently created Active/Inactive domains that can be hosted by the HouseCall server. Click on the folder tabs to select the Active or Inactive view of the domains.

Active

The Active-Domain overview page shows a list of all created currently active domains, able to connect to the HouseCall server.

Edit - To edit any of the domain settings, double-click on the domain name or activate the dedicated checkbox leading the domain row and click the “Edit” button.

Deactivate - To deactivate (decline access) a domain, first click to the leading checkbox of the dedicated domain, then the “Deactivate” icon on top of the overview.

The name of the deactivated domain immediately disappears from the list and will be shown in the “Inactive” folder until reactivation.

Possible actions on active domains:

Add – Opens additional page to create a new domain entry

Edit – Click on any domain name to edit the domain settings

Deactivate - Select any domain name and click on “Deactivate” button.

Table legend for active domains:

- Domain - Name of the currently active domain.
- Last modified - Date of the last modification of the domain settings.

Inactive

This is the Inactive-Domain overview page.

All current inactive domains will be shown in this view. If you like to change the status of a domain from “Inactive” to “Active”, just select the dedicated row by clicking on the checkbox and click on the “Activate” icon.

The selected row disappears immediately and will be shown in the “Active” view folder.

Possible action on inactive domains:

Activate - A previously selected domain or multiple domains will switched to be active which allows the domain to connect to HouseCall server.

Domain - Create a New Domain

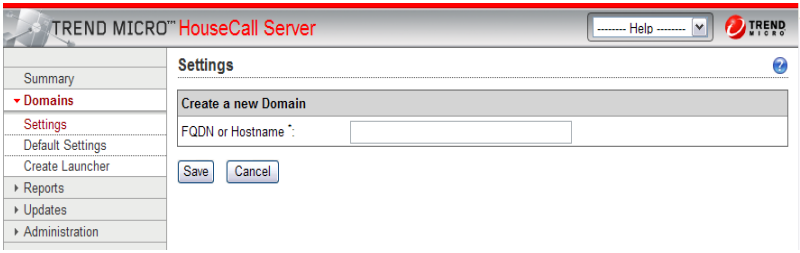


FIGURE 4-5 Create a new domain

Create a new Domain

To create a new Domain, click on the “Add” button in the Active Domain view.

Type in the FQDN or hostname of the new domain and click on “Save” button to store your settings or “Cancel” to discard.

FQDN or Hostname

Specify the FQDN or the server hostname that this host setup is bound to. Requests that are issued against the HouseCall server using this hostname or FQDN will be using the configuration that can be made on the further pages

Domain - Basic Settings

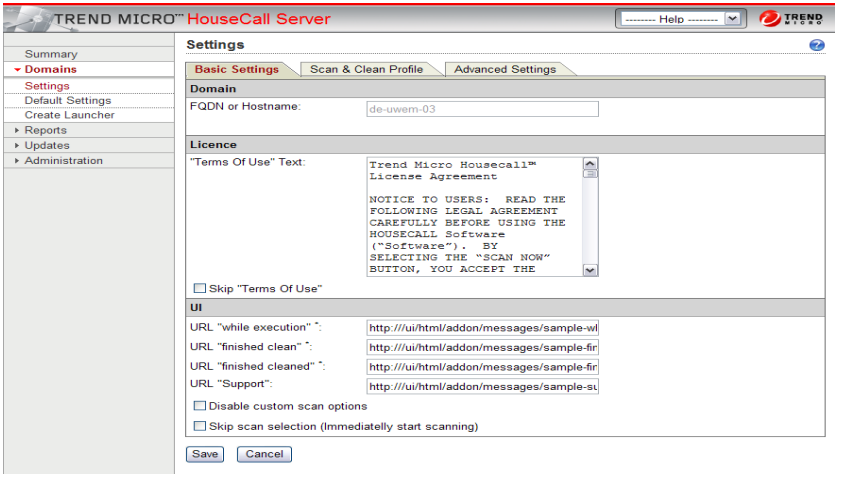


FIGURE 4-6 Basic settings

Basic Settings

Allows specifying the basic settings of this multi host configuration, showing in three major sections:

Domain - Shows FQDN or Hostname

License - "Terms Of Use" - Enter the terms of use that will be shown when HouseCall Client is started or click to activate the checkbox to Skip "Terms Of Use".

UI

Here you can configure the HouseCall clients behavior when a user executes the scanning/cleaning process.

URL "while execution" - Clientside URL pointing to the content, shown during the scan

URL "finished clean" - Clientside URL pointing to the content, shown after the scan completed and nothing was found

URL "finished cleaned" - Clientside URL pointing to the content, shown after an infected system was cleaned using HouseCall

URL "Support" - Clientside URL pointing to a support page. If this is empty, the support link is hidden

Disable custom scan options - Do not show any custom scan options inside the client ui.

Skip scan selection (Immediately start scanning) - Do not wait for the user to select a scan option. Immediately start scanning using the server side scan profile.

Note: After you have completed any modifications or changes on the domain settings, you need to store them to the HouseCall system. Click "Save" button to store or "Cancel" to discard all changes.

Domain - Scan & Clean Profile

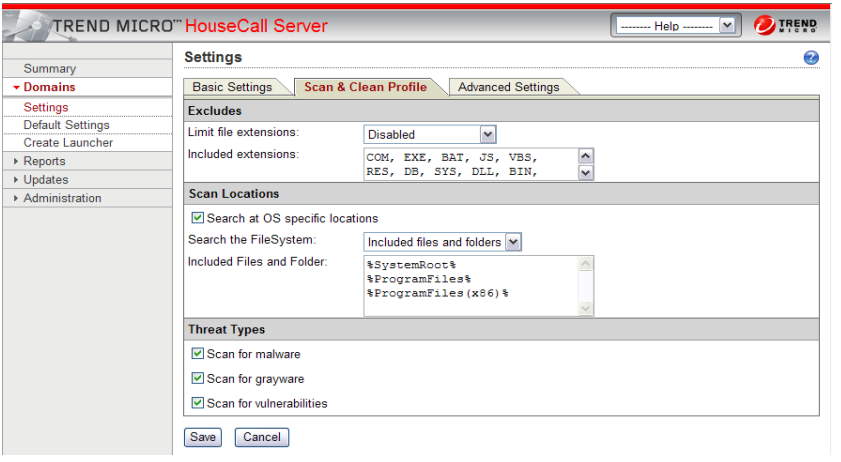


FIGURE 4-7 Scan & Clean Profile

Scan & Clean Profile

Allows configuring the recommended scan options

Excludes

Limit File Extensions - can be Disabled or Enabled to include extensions

Included extensions - This is a list of file extensions to be included in a scan operation within the recommended scan profile. The extensions are delimited by a new line or comma.

Scan Locations

Search at OS specific locations - Search at locations like the windows registry, browser caches.

Note: Please note that this option does not include the regular file system, e.g. folders like “C:\Windows” must be handled separately

---

Search the File System

This option can have three different settings:

Disabled - No files or folders will be searched.

Included Files and Folders - This refers to a list of paths that are included in a scan operation within the recommended scan profile. Environment variables like %SystemRoot% or %ProgramFiles% are fully supported. Paths are delimited either by a new line, “,” or “;”

All Files and Folders - This option includes all local files and folders

Threat Types

Three major threat types can be activated or disabled to be handled while executing this domain profile. To activate/disable the dedicated threat type, click on the leading checkbox.

Scan for malware - scans for known viruses, trojans and all kind of malware

Scan for grayware - scans for spyware, bots and all type of grayware

Scan for vulnerabilities - scans the system for vulnerabilities e.g. portscan, missing Windows patches...

Domain - Advanced Settings

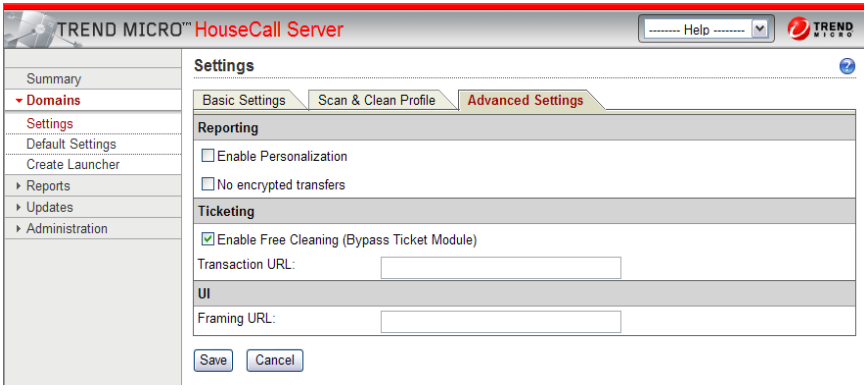


FIGURE 4-8 Advanced Settings

Advanced Settings

Allows for the configuration of advanced options.

Reporting

Enable Personalization - Enables the client to send Username and IP address. This might conflict with the license agreement, used in intranets only.

No encrypted transfers - By enabling this option, personalized data will be sent in clear text over the network (not SSL encrypted). Do not enable this option in public networks

Ticketing

Enable Free Cleaning (Bypass Ticket Module) - HouseCall Client does not show any payment, if this is set

Transaction URL - Sets the transaction URL to be called when a ticket purchase is issued using the external payment provider

UI

Framing URL - If this URL is specified, it will be used as a replacement for the default index file of the selected UI. The actual URL of the original index file for opening the UI will be transferred as the URL parameter “ui”.

Tip: If you specify “http://yourhost/frame.html” as the framing URL for example, a call to “http://server/housecall/ui/html/default/” will redirect to http://yourhost/frame.html?ui=http://server/housecall/ui/html/default/index.html.

This can be used to surround the selected client UI with your company logos, colors etc. This works even if HouseCall is started through a launcher application.

Note: Please refer to the additional “Server Integration Guide” for more detailed information on how to enable the ticket system.

Domain - Create Launcher

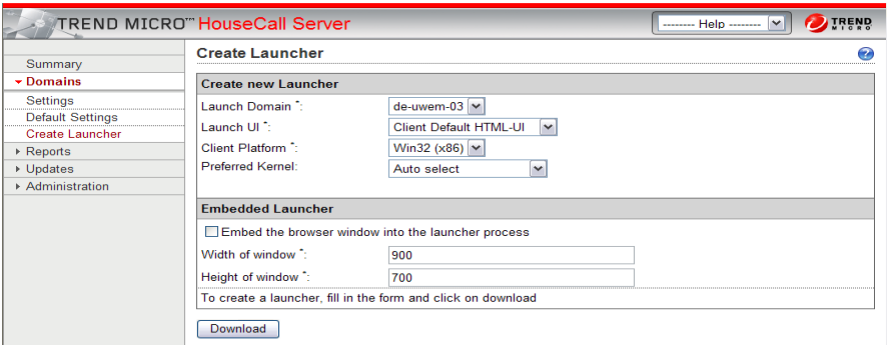


FIGURE 4-9 Create Launcher

Create Launcher

This page allows you to configure and create a small executable program called HouseCall “Launcher”. The Launcher program can be used to be executed whenever a local system starts up and should automatically launch the HouseCall Client in a browser window on the users desktop.

The “Launcher” program allows it to be integrated into local systems startup routine to be executed when the system boots up (autostart).

The Launcher program can be configured for two different behaviors:

a. Open a browser windows with a pre configured URL

b. Run HouseCall like a normal application by embedding the systems web browser into the executed launcher process.

Create new Launcher

Launch Domain - Configurable URL to get connected to the custom HouseCall Server

Launch UI - Defines the size of the embedded browser window when Launcher starts (default = 900*700)

Client Platform - Creates executable program for Windows, Linux and OSX system platforms

Preferred Kernel - Options

"*Auto Select*" uses the default kernel on the chosen operating system (Java with Windows, Linux and OSX)

"ActiveX" – forces the HouseCall client to use the ActiveX kernel by default on Windows environment

Embedded Launcher - Embed the browser window into the launcher process

---

Note: Activation of this option forces to startup the HouseCall Client in an embedded browser window. Running in embedded mode ignores the local users browser security settings and runs the ActiveX component without manual confirmation or installation.

If you select "*Auto Select*" as preferred kernel, the HouseCall Client will be configured to use the Java Kernel by default.

In this case (Auto Select and deactivated embedding) the program starts the default browser window in the regular mode instead of embedded and uses the pre-configured URL to connect to the custom HouseCall server.

Once the configuration is done and you click on the "Download"-button, the program will be automatically created.

A Pop-Up window appears, asking where to store the program onto your local system

Reports - One-time Reports

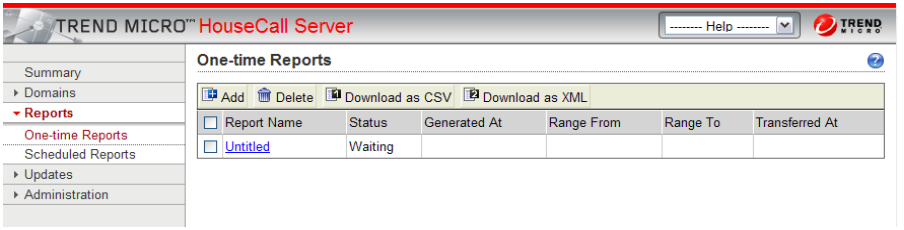


FIGURE 4-10 One-time Reports

The One-time report allows you to retrieve a single status sheet of the current system. If you like to have a continuous reporting, you need to select “Scheduled Reports” from the main menu.

Note: Any report generation process will cause additional system load while performing!

From this view, you can add a new one-time report or delete an already existing one.

To Add a report, click on the “Add” button. Another screen will be opened where you need to define your reporting options described later in this section.

Tip: When you select an existing report and click then on the “Add” button, the newly created report will overtake all settings and modifies the start and end dates in a way, that the new report starts when the previously selected ends.

To Delete one or more reports, select the dedicated report by activating the leading checkbox and then click on the “Delete” button.

Note: While clicking the “Delete” button, the selected reports will be immediately deleted and cannot be restored.

All shown reports can also be downloaded in two different formats.

As CSV file - this format is support by most text editors or

As XML file - to be used by editors that supports XML format or you like to display the report in a browser.

Example for XML Report

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE reports (View Source for full doctype...)>
- <reports created="2007-02-19 14:37:02" version="1.0">
  - <report id="r1" countryCode="DE" languageCode="de" created="2007-02-19 14:15:50" domain="w2k3-ee-en" serverName="no-
      servername">
      <identity clientUsername="" clientAddress="" clientMachine="" />
      <state selectedProfile="custom-clientside" initialContext="initial" finalContext="resolving" duration="47" />
      <environment browser="MSIE 6.0" kernel="html/java" os="Windows NT 5.1" platform="win32" architecture="x86" />
      <scanned amount="0" type="system.grayware" pattern="4.650.00" engine="1.060.1049" />
    </report>
  - <report id="r2" countryCode="DE" languageCode="de" created="2007-02-19 10:14:16" domain="w2k3-ee-en" serverName="no-
      servername">
      <identity clientUsername="" clientAddress="" clientMachine="" />
      <state selectedProfile="" initialContext="" finalContext="" duration="0" />
      <environment browser="MSIE 6.0" kernel="html/java" os="Windows NT 5.1" platform="win32" architecture="x86" />
      <scanned amount="0" type="system.grayware" pattern="4.650.00" engine="1.060.1049" />
    - <infections>
      - <remaining>
          <infection amount="2" threat="VBS_TEST_VIRUS" threatClass="malware" />
        </remaining>
      </infections>
    </report>
  - <report id="r3" countryCode="DE" languageCode="de" created="2007-02-19 10:24:10" domain="w2k3-ee-en" serverName="no-
      servername">
      <identity clientUsername="" clientAddress="" clientMachine="" />
      <state selectedProfile="" initialContext="" finalContext="" duration="0" />
      <environment browser="MSIE 6.0" kernel="html/java" os="Windows NT 5.1" platform="win32" architecture="x86" />
      <scanned amount="0" type="system.grayware" pattern="4.650.00" engine="1.060.1049" />
    - <infections>
      - <remaining>
          <infection amount="2" threat="VBS_TEST_VIRUS" threatClass="malware" />
        </remaining>
      </infections>
    - <vulnerabilities>
        <vulnerability threat="MS05-020" type="software" />
```

FIGURE 4-11 Example XML Report

Reports - Add a One-time Report

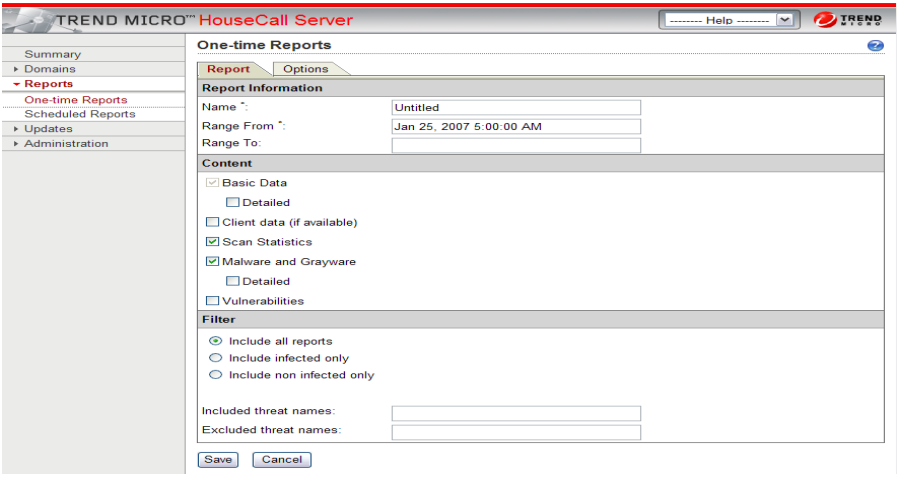


FIGURE 4-12 Add a One-time Report

Add/edit a One-time Report

Report Information

Name - Type in a name of the report

Range From - Starting time from where the data should collect

Range To - Last time for the collected data (e.g.: Sep 01, 2007 13:15:00 PM) The time setting is optional. With no time specified, all data of the chosen day from 00:00 AM to 11:59 PM will be collected.

Content

Basic Data - Only Information and Warnings will be shown in the report.

Detailed - Available status information will be reported.

Client data (if available) - Personalized information including login names, IP and Mac addresses

Scan Statistics - This provides a statistical analysis of the scan processes from the selected time range.

Malware and Grayware - Provides basic information on found Malware/Grayware during the scan processes

Detailed - Reports more detailed information about Malware/Grayware

Vulnerabilities - Provides information about possible system vulnerabilities found during the scans

Filter

Filter rules that can be activated to retrieve specific data only.

Include all reports – Report will be created with all settings above.

Include infected only – Report will only be created if any infection can be found on the system

Include non infected only – Report will only be created if no infection can been found on the system

Included threat names - A comma separated list of threat names that must be included in a single report entry. The wildcard character "*" is allowed to be used in the beginning and at the end of a name. E.g. "WORM*, TROJ*" will select all report entries containing worms and trojan infections while "*BAEGLE*" would match any BEAGLE malware.

Excluded threat names - Has the same features as "Included Thread names" but inverts the rule.

Note: Once the configuration is made, click on "Save" button to store your settings or "Cancel" to discard.

Reports - One-time Report - Options

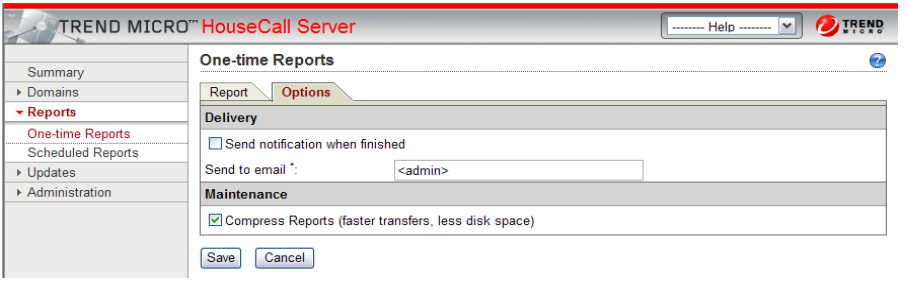


FIGURE 4-13 Options on One-time Report

Options

With the one-time report options page, you can specify the delivery and maintenance of the created report.

Delivery

Send notification when finished - Sends out a notification mail about the finishing state of the report.

Send to email * - A valid E-mail address to send the notification message. By default the administrators mail address will be used to receive report notification messages.

Maintenance

Compress Reports (faster transfers, less disk space) - By default this option is enabled. It compresses the output of the report to save diskspace and faster delivery because of the reduced file size.

Note: When reports are compressed, the XML file is also sent compressed to the browser. In very rare situations this might be a problem. If customers expect any issues downloading the XML, disabling this option might solve the problem. However it's really recommended to keep it enabled.

Reports - Scheduled Reports

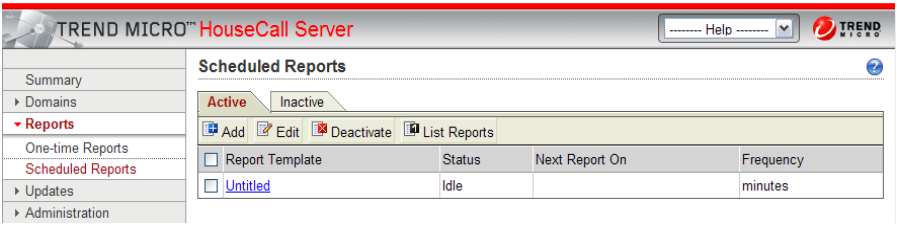


FIGURE 4-14 Scheduled Reports

Scheduled Reports

With the "Scheduled Reports" option, you can specify an interval on which a series of reports should be created. Therefore you can create a template which will be used to start your specific report generation based on your settings.

Note: Any report generation process will cause additional system load while performing!

Active

The active report overview page shows a list of all created currently active reports, able to run on a dedicated schedule to retrieve report data from the HouseCall domains.

To edit any of the report settings, double-click on the reports name.

To deactivate a report, first click to the leading checkbox of the dedicated line, then click the "Deactivate" icon on top of the overview. The name of the deactivated report immediately disappears from the list and will be shown in the "Inactive" folder until reactivation.

Actions:

Add – opens a page to create a new report entry

Edit – Click on any report name to edit the report settings

Deactivate - Sets status of the selected report to "Inactive"

List Reports - Lists all reports from the same reporting template or schedule

Reports - Add/Edit a Scheduled Report

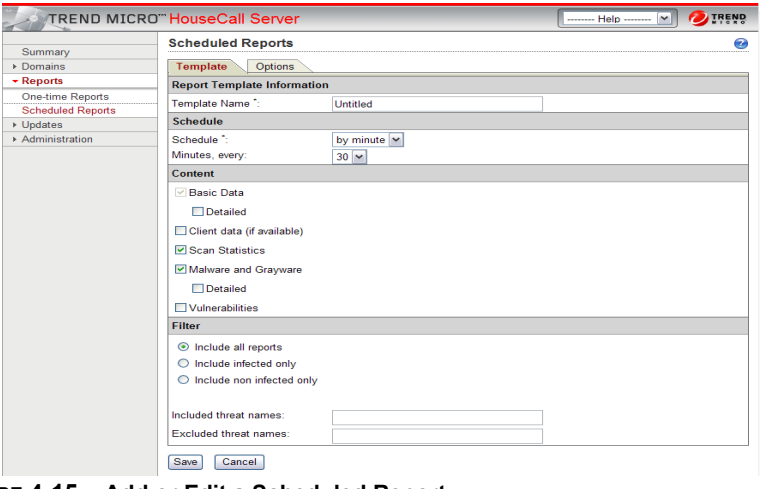


FIGURE 4-15 Add or Edit a Scheduled Report

Add or Edit a Scheduled Report

Report Template Information

Template Name - Type in a name to store with the template

Schedule

Schedule - Choose either to schedule the report “by minute”, if you like to have multiple reports in a one hour range, or “by hour” if you like to have multiple reports during a day.

Minutes, every - Select the range of minutes to start a report again (only active if you select “by minute” as schedule)

Hours, every - Select the range of hours to start a report again (only active if you select “hourly” as schedule)

Days, every - Select the range of days to start a report again (only active if you select “daily” as schedule)

Weeks, every - Select the range of weeks to start a report again (only active if you select “weekly” as schedule)

Content

Basic Data - Only Information and Warnings will be shown in the report.

Detailed - available status information will be reported.

Client data (if available) - Personalized information including login names, IP and Mac addresses

Scan Statistics - Provides a statistical analysis of the scan processes from the selected time range.

Malware and Grayware - Provides basic information on found Malware/Grayware during the scan processes

Detailed - Reports more detailed information about Malware/Grayware

Vulnerabilities - Provides information about possible system leaks found during the scans

Filter

Filter rules that can be activated to retrieve specific data only.

Include all reports – Report will be created with all settings above.

Include infected only – Report will only be created if any infection can be found on the system

Include non infected only – Report will only be created if no infection can been found on the system

Included threat names - A comma separated list of threat names that must be included in a single report entry. The wildcard character "*" is allowed to be used in the beginning and at the end of a name. E.g. "WORM*, TROJ*" will select all report entries containing worms and trojan infections while "*BAEGLE*" would match any BEAGLE malware.

Excluded threat names - Has the same features as "Included Thread names" but inverts the rule.

Reports - Scheduled Report - Options

FIGURE 4-16 Scheduled Report Options

Options

With the scheduled report options page, you can specify the delivery and maintenance of the created report.

Delivery

Send notification when finished - Sends out a notification mail about the completed state of the report.

Send to email * - A valid eMail address to send the notification message. By default the administrators email address will be used to receive report notification messages.

Maintenance

Compress Reports (faster transfers, less disk space) - By default this option is enabled. It compresses the output of the report to save diskspace and faster delivery because of the reduced file size.

*Number of Reports to keep *:* - Default is 50. You can specify the numbers of scheduled reports using this template to be stored on the server. If the limit is reached, the oldest report will be deleted and the latest will be stored.

Note: Once the configuration is made, click on “Save” button to store your settings or “Cancel” to discard.

Updates - Pattern & Engine

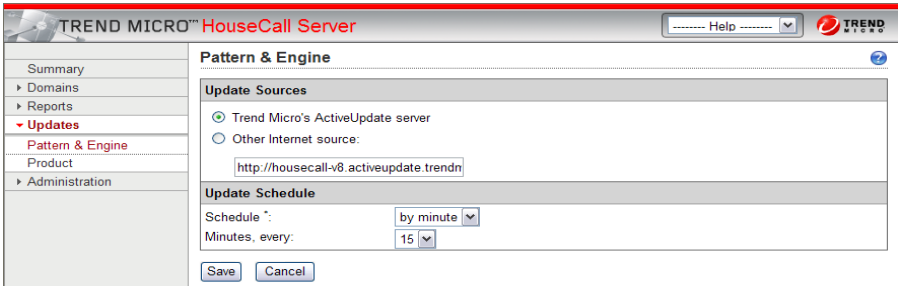


FIGURE 4-17 Update Pattern & Engine

Update Pattern & Engine

It is recommended to save a schedule profile to assure an automatic update for virus pattern, scan engine and Spam engine files. The HouseCall server is able to retrieve all updates from the Trend Micro ActiveUpdate server to ensure always to work with the latest available up-to-date pattern and engine versions.

Update Sources

In this section you can choose your update source to be used to retrieve the latest engine and pattern file information.

Trend Micro's ActiveUpdate server - Default (Recommended)

Other Internet source: - If you have a custom Active Update server running or like to select a different source to keep your pattern and engine files up-to-date, select this option. You need to manually type in the URL to connect to retrieve the files.

Note: Note: Please ensure the availability of any custom ActiveUpdate source, otherwise your pattern and/or engine files can be outdated which can cause serious problems, because the latest malware and vulnerabilities can not be detected.

Update Schedule

This setting describes the interval of the HouseCall server to retrieve the defined data from the chosen update source.

Schedule - Choose either to schedule the ActiveUpdate “by minute”, if you like to have multiple updates in a one hour range, or “by hour” if you like to have multiple updates during a day.

Minutes, every - Select the range of minutes to start an update again (only active if you select “by minute” as schedule)

Hours, every - Select the range of hours to start an update again (only active if you select “hourly” as schedule)

Days, every - Select the range of days to start an update again (only active if you select “daily” as schedule)

Weeks, every - Select the range of weeks to start an update again (only active if you select “weekly” as schedule)

Note: Once the configuration is made, click on “Save” button to store your settings or “Cancel” to discard.

Updates - Product Modules

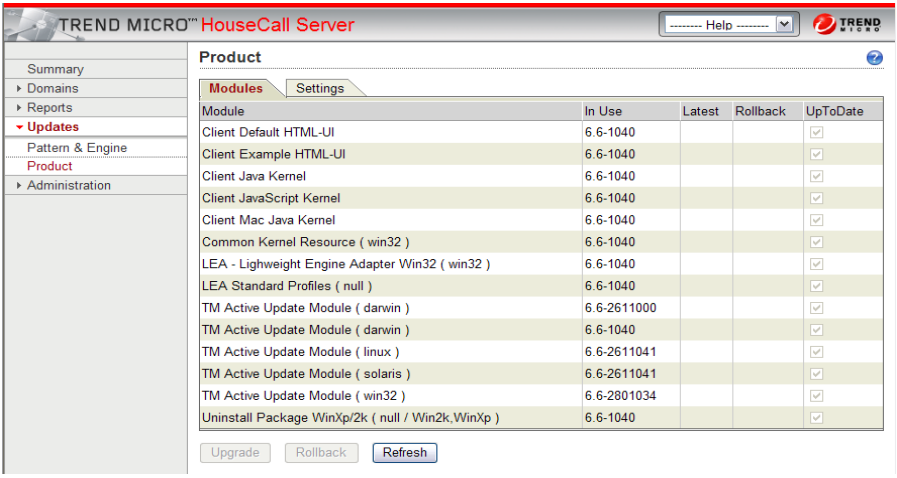


FIGURE 4-18 Update/Rollback on Product Modules

The various components used by the HouseCall server, are called “modules”.

This summary gives you an overview on the current modules in use by the HouseCall server. Also the latest available version, located on the ActiveUpdate server will be shown if available.

To upgrade a module, if any newer version is shown as available, click on the “Upgrade” Button below the view.

To rollback any module to the previous version, choose the module and click on “Rollback” button to activate to rollback process.

Note: It is highly recommended to always use the latest available versions of the HouseCall server modules. Only rollback module if facing issues after upgrading them into the local environment. The rollback action should be used to restore the previous version.

With the “Refresh” button, the view will be updated to show the current available information.

Product Modules view

Module - Name of the module in use

In Use - Shows the current version number of the module in use.

Latest - If any later version of an module is available from the ActiveUpdate server, it will be shown here.

Rollback - In case of any issues with a dedicated module version, the former version that can be roll backed will be shown here

UpToDate - An activated checkbox declares the currently used module as up-to-date

Updates - Product Modules - Settings

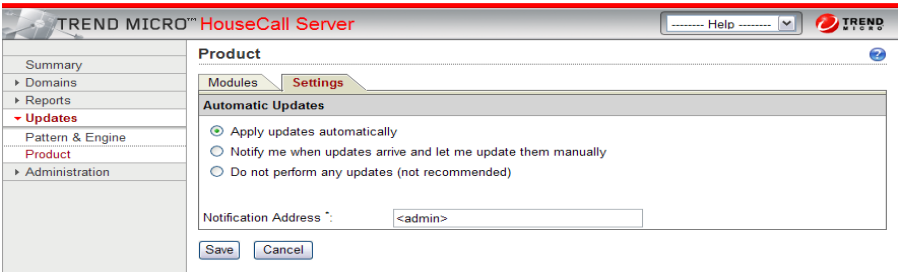


FIGURE 4-19 Updates Product Modules - Settings

In this view, the update options and notification address can be configured.

Automatic Updates

You can manually choose between three different options to perform an automatic update on the HouseCall modules.

Apply updates automatically - will retrieve always the latest modules if available without any user or admin interaction needed.

Notify me when updates arrive and let me update them manually - Sends a notification that new modules are available, but needs manual interaction to update

Do not perform any updates (not recommended) - No updates and no notification will be send.

Notification Address - Type in a valid email address to send out a notification mail when new updates are available. (Only if you choose to be notified from above selection). By default the notification will be send to the administrators address.

Note: Once the configuration is made, click on “Save” button to store your settings or “Cancel” to discard.

Administration

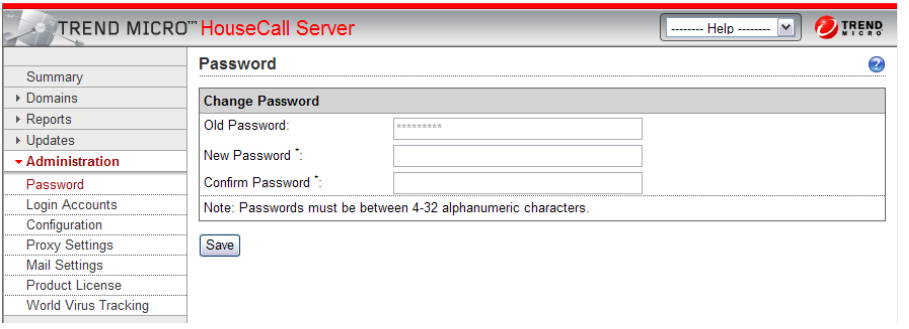


FIGURE 4-20 Administration - Password Setting

Administration Password Setting

On this page, you can change the HouseCall server administrator password. This is the password you have to type in to get access to the HouseCall server administration web console and configuration pages.

It is highly recommended to change this password once the installation of the HouseCall server has finished!

Change Password

Old Password - Type in your existing administrator password.

New Password - Type in your new password. This password must have a minimum length of 4 and a maximum of 32 characters.

Confirm Password - Confirm the new password by typing in again.

Once the password is set, click on the “Save” button to store the new information.

From the next time you login to the HouseCall administration pages, you will be asked for the new password.

Administration - Login Accounts

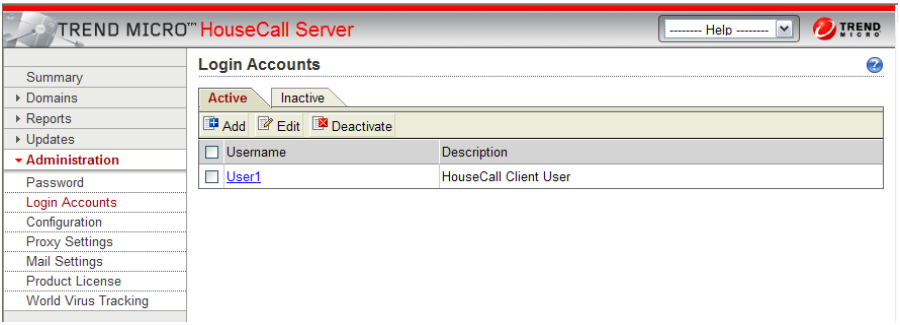


FIGURE 4-21 Administration - Login Accounts - Active

Active Login Accounts

On this page, you will get an overview on the existing active and inactive Login Accounts on your HouseCall server.

Active view

There are three different actions you can perform on the active accounts by clicking the checkbox in the dedicated row.

Actions:

Add - Add a new Login account for a user

Edit - Select an account by clicking the checkbox first. Then the click on edit and all information about the chosen user account will be shown that can be edited.

Deactivate - Choose an account to be deactivated first by clicking the checkbox, then click on the “Inactivate” icon. The chosen account disappears from the Active folder and appears in the Inactive folder at the same time. This user account is now disabled and can not longer login to the HouseCall server.

Inactive Login Accounts

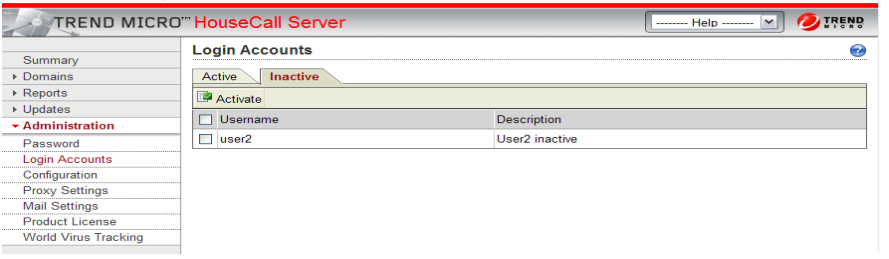


FIGURE 4-22 Administration - Login Accounts - Inactive

Inactive view

This is the “Inactive” folder view of the existing Login Accounts on your HouseCall server. All current inactive accounts will be shown in this view.

If you like to change the status of an account from “Inactive” to “Active”, just select the dedicated row by clicking on the leading checkbox and click on the “Activate” icon.

The selected row disappears immediately and will be shown in the “Active” view folder.

The selected account can be used to login to the HouseCall server after activation.

Action:

Activate - Activates a previously selected account

Administration - Add/Edit Login Accounts

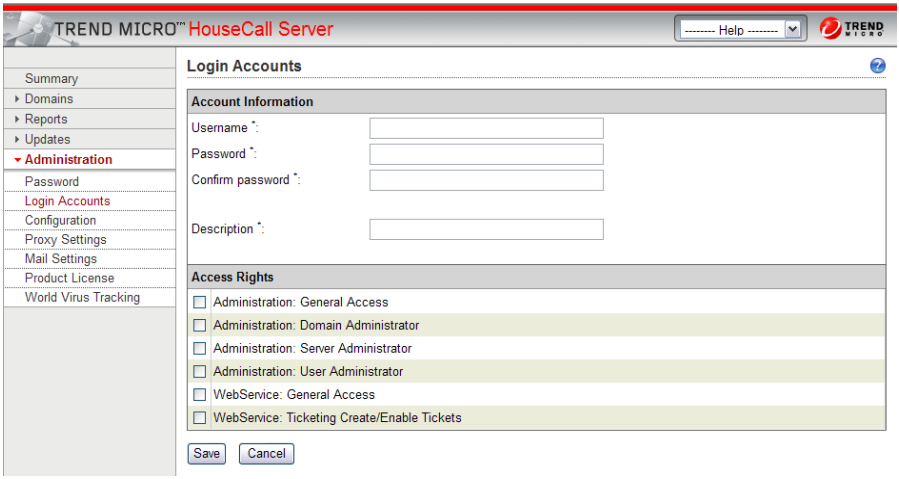


FIGURE 4-23 Administration - Add Login Accounts

Add/Edit

To add a new user or modify existing user settings in the configuration area, you need to configure the **Username,** the **Password** a **Brief Description** and the **Access Rights** of that user. These **Access Rights** have different kind of privileges so that almost all configuration tasks can be assigned to different users or administrators.

Account Information

Username - Type in a Username for this account.

Password - Password the this user account.

Confirm Password - Type in again the Password to be confirmed

Description - Add a brief description to describe this account.

Access Rights

Administration: General Access - Unlimited Access to all function of the HouseCall Server

Administration: Domain Administrator - All access rights on a dedicated domain or list of domains

Administration: Server Administrator - All access rights on a dedicated server or list of servers

Administration: User Administrator - All privileges to Add, Edit, Activate and Deactivate users on the server

WebService: General Access - General access rights to all web services used with the HouseCall server

WebService: Ticketing Create/Enable Tickets - Can create and enable tickets if a ticketing system is used

Administration - Configure Inbound Network Options

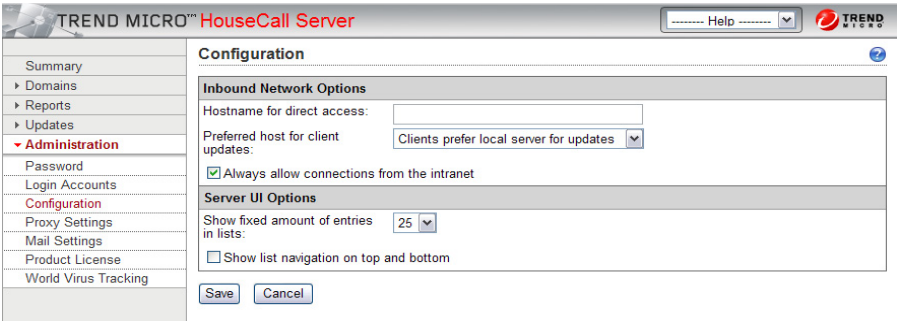


FIGURE 4-24 Administration - Inbound Network Options

Inbound Network Options

The HouseCall server configuration must be set, to personalize your local HouseCall server installation

Inbound Network Options

Hostname for direct access - Enter a valid full qualified hostname for the HouseCall server. This hostname must be known by a DNS server entry inside your domain. This entry is optional and only for configuring special environment needs like "Reverse proxy in front of HouseCall"

Preferred host for client updates - Choose local or public server from where the connected clients should receive their files to update the virus pattern and scan engine information.

Always allow connections from the intranet - By enabling this option, HouseCall clients that are located within the intranet can always connect to the HouseCall Server even when no domain setting is created.

Server UI Options

Show fixed amount of entries in lists - Number of lines to be shown.(Default = 25)

Show list navigation on top and bottom - Default = disabled. List navigation will only be shown on top of the list. you can enable this option if the list entries requires scrolling and you can navigate either from top or bottom.

Administration - Proxy Settings

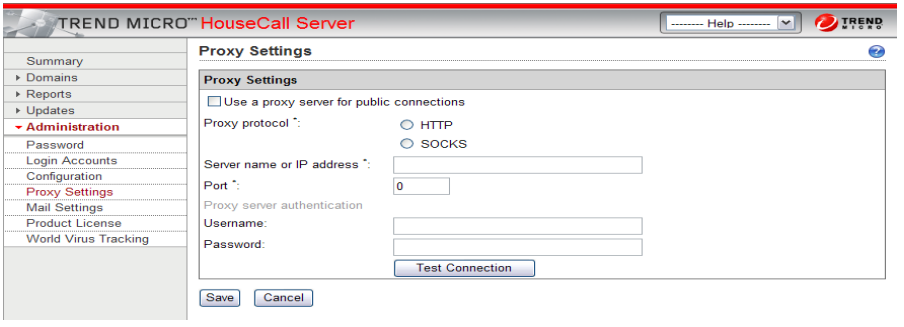


FIGURE 4-25 Administration - Proxy Settings

Proxy Settings

If your environment uses a proxy server to connect to the internet, you need to specify your proxy settings in order to allow the HouseCall server to retrieve update information from an external update source.

Proxy Settings

Use a proxy server for public connections - Activate the proxy settings by enabling this checkbox. If the checkbox is not activated, no proxy server will be used to connect to the internet.

Proxy protocol - Choose the used Proxy protocol either HTTP or SOCKS by clicking on the dedicated selection.

Server name or IP address - Type in a valid servername or IP address of a valid proxy server

Port - Portnumber where the proxy server can be connected

Proxy Authentication

Username - If your proxy server requires authentication, please type in the Username with the equivalent rights

Password - Type in the password to access the proxy

Test Connection - After you configured the proxy server settings, click on the “Test Connection” button. The HouseCall server will now try to open an internet connection to verify your settings. If the connection can not be established, an error message appears with a possible reason. Please check your proxy settings again to assure they are correct. If you need further help setting up the proxy connection, please contact your local Proxy or Firewall administrator.

Note: Once the configuration is made, click on “Save” button to store your settings or “Cancel” to discard.

Administration - Mail Settings

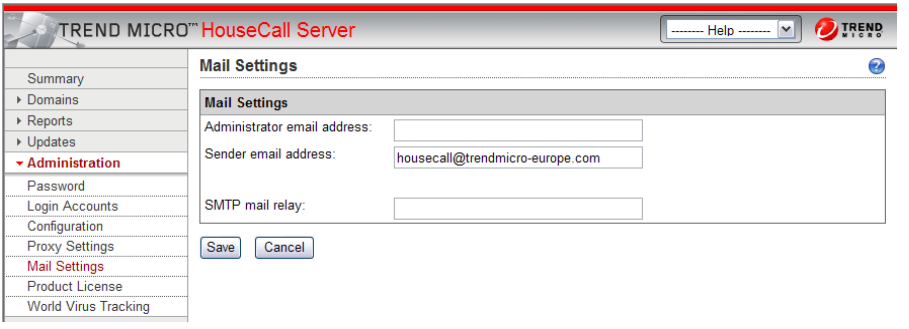


FIGURE 4-26 Administration - Mail Settings

Mail Settings

Here you can specify an email account on where system notification messages should be delivered.

Mail Settings

Administrator email address - Enter the full qualified administrator email address

Sender email address - Enter an email address to be displayed as sender address in the notification header (e.g. servername), Default = HouseCall server email address.

SMTP mail relay - If a specific server will act as mail relay, please enter the full qualified servername in this field. All notifications will be send through this server.

Administration - Product License

FIGURE 4-27 Administration - Product License

Product License

In order to receive a valid activation code for your HouseCall server, you need to register successfully your copy of the HouseCall server at Trend Micro. After you have successfully registered, you will receive an activation code.

With this code you can activate your HouseCall server. You need to proceed through the following two Steps to finally register and activate your license key.

Step 1 - Register

Click on the “Register” button. This will proceed you to the Trend Micro registration website, where you have to fill out a specific registry form with your personal information. After you filled out the registration form successfully, Trend Micro will send an activation key to the registered email address.

Step 2 - Activate

Activation Code - Type in the activation key manually (or copy & paste) into the “Activation Code” field. Ensure that you have entered the correct syntax of the key and click on “Activate” button once. Now your copy of the HouseCall server has been successfully activated.

Administration - World Virus Tracking

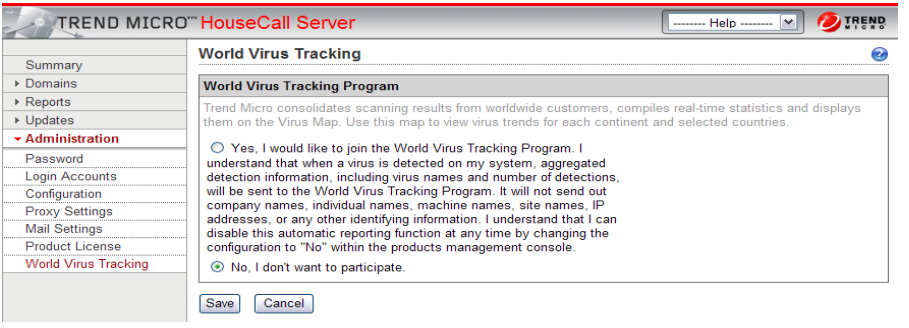


FIGURE 4-28 Administration - World Virus Tracking

World Virus Tracking Program

Trend Micro consolidates scanning results from worldwide customers, compiles real-time statistics and displays them on the Virus Map. Use this map to view virus trends for each continent and selected countries. In order to participate to this program, you need to commit your participation.

Note: After your selection, click on “Save” button to store your settings or “Cancel” to discard.

Server Logs and Configuration

The default Log paths are:

HouseCall Server Log

%HOUSECALL_HOME%\Trend_Micro_HouseCall_Server_Edition_6.6_InstallLog.log

%HOUSECALL_HOME%\logs\3rdparty.log

%HOUSECALL_HOME%\logs\housecall.log

TomCat Server Log

%HOUSECALL_HOME%\server\logs\jakarta_service_<20070219>.log

%HOUSECALL_HOME%\server\logs\stderr_<20070219>.log

%HOUSECALL_HOME%\server\logs\stdout_<20070219>.log

Apache Derby Log

%HOUSECALL_HOME%\storage\database\derby.log

Configuration files

HouseCall Server Config

- %HOUSECALL_HOME%\config\config.xml

  XML file includes all information which admin has set during the installation. If admin needs to modify any configuration entries this file is the file that needs to be modified.

- %HOUSECALL_HOME%\server\webapps\housecall\META-INF\housecall-config.xml

  When HouseCall is started the HouseCall launcher reads all information from config.xml and updated this xml file. That is the reason to modify only the config.xml instead of the housecall-config.xml.

Chapter 5

The HouseCall Client

This chapter describes you how to use the HouseCall Client Web Service. The topics discussed in this chapter include:

Client Usage

The clients appearance is divided in three major sections to provide all necessary information and to give the best options for usage.

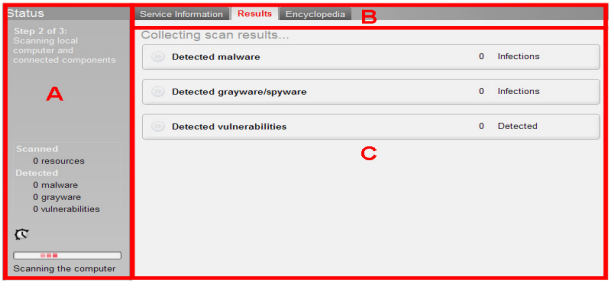


FIGURE 5-1 HouseCall Client usage

A - The status section always provides the current progress on the selected action (e.g. Update, Download, Scanning...).

B - The folder tabs on top of the client screen gives the ability to select different screens to show and configure (Encyclopedia, Results, Service Information)

C - The main screen of the client. It is at this location, you can select and configure the action that should be performed by the HouseCall client.

HouseCall Kernel

HouseCall Kernel refers to the technology that allows to scan computers for malicious code such as viruses, worms, and other malware or spyware/grayware and display the results in a browser window.

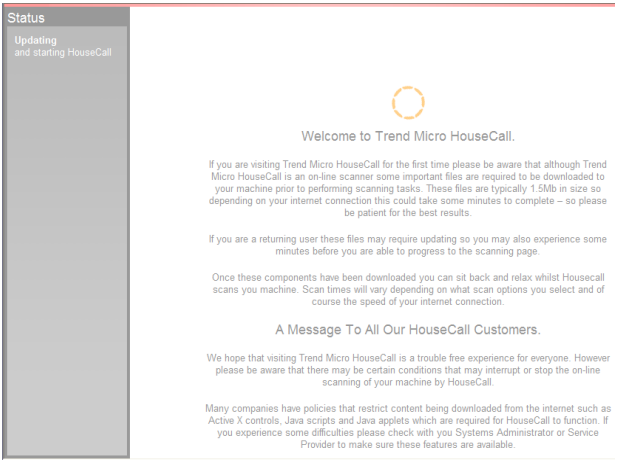
Since there are many different types of computers, which in turn use different browsers and operating systems, it is necessary to provide different HouseCall kernels.

If the system detection identifies more than one possible kernel, you may select according to your preferences, as each kernel offers the same overall features.

Refer to the table below for available kernels on individual operating systems

Operating System	Java Kernel	Browser Plug-in Kernel
Windows XP, Service Pack 1 or 2	YES	YES
Windows 2000, Service Pack 4	YES	YES
Windows 2003, or with SP1	YES	YES
Windows MCE 2005	YES	YES
Linux, libc6	YES	NO

Client Startup and Welcome



During the client startup, some required files will be downloaded and installed on the local system. This process can take some time, depending on your connection speed and download ability. While this is in progress, you will see a moving yellow circle and a welcome message that gives you some more detailed information about the system requirements and some functional capacities of the HouseCall client.

This screen will disappear once all files are downloaded and stored locally and the client is ready to start. If you are installing the HouseCall client for the first time, it can take several minutes until all files have been downloaded.

If you are a returning user with the HouseCall client, the program only needs to update the existing files.

License Agreements

The “Welcome to HouseCall” screen including the Trend Micro License Agreements, this is the first screen after the download of all necessary files has been completed and the client can now be configured with your preferences to scan your local system.

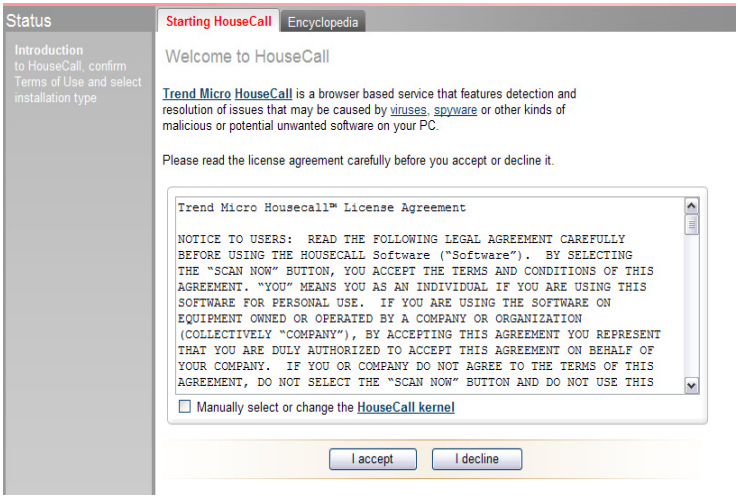


FIGURE 5-2 HouseCall License Agreements

In order to use the HouseCall client, you have to accept the License Agreements first. Click on “I accept” button to agree, or on “I decline” to decline. If you choose to decline, the HouseCall client window will be closed and the scan precess will be stopped.

You can also activate the checkbox below the License Agreements, to manually select or change the kernel that should be used to scan your local system. The HouseCall clients will always try to start with the ActiveX kernel by default provided, it is the supported by the operating system. This is the recommended kernel for most of the Microsoft Windows based environments.

If you use a Linux system or older Windows operating systems or your company has restrictions that do not allow the use of ActiveX components, click the checkbox to manually select the Java kernel on the next screen.

Manual Kernel Selection

If you have chosen to manually select the kernel used to scan your local system, the HouseCall client tests your system to detect, what kernel is able to run in this environment. After a short test, the result is shown to select one of both, Java or ActiveX.

If both kernels are able to run, they will be shown and a manual selection is required before proceeding. If only one kernel is detected by the test, click on the “Next” button to proceed to the configuration page.

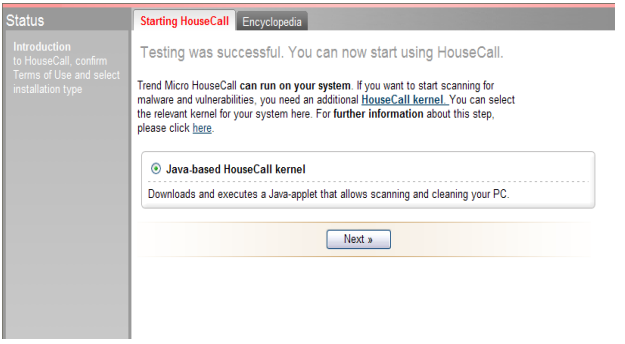


FIGURE 5-3 Manual kernel select

Client Update

Each time the HouseCall Client starts, the core components such as the scan engine and pattern files will be automatically updated from the HouseCall server, no further action is required. This process ensures, that all components that will be used to scan and clean your local system are up-to-date.

During the update procedure, displaying information will be shown on the main screen. The status section shows the current update progress. As soon as all required updates are completed, the client will automatically proceed to the next configuration page.

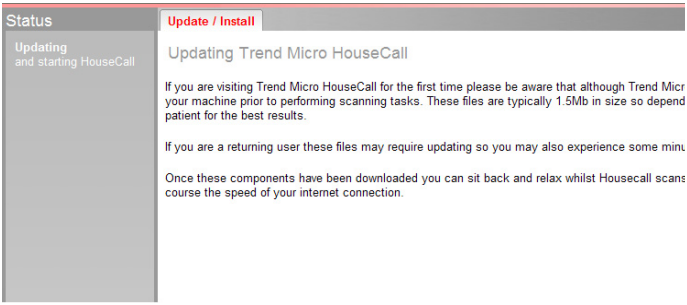


FIGURE 5-4 Updating the core components

Selecting Scan Options

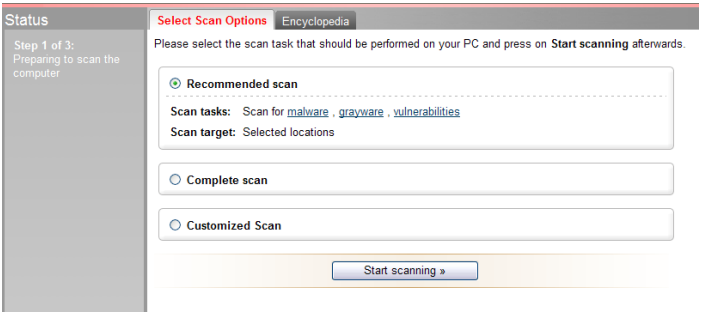


FIGURE 5-5 Client Scan Options

There are three general scanning options that can be selected from the main screen.

- *Recommended scan* - Scans based on the settings defined as the server-side custom profile.
- *Complete scan* - Scans ALL folders and files on all supported drives connected to your local system for malware, grayware and vulnerabilities.
- *Customized scan* - Scans manually selected supported drives and folders with specific scanning options (scan tasks) that can be configured.

After you have selected the option you like to use to scan your system, click on “Start scanning” button to run the scanning process. Depending on the systems performance, size and number of items to scan, this can take from a few seconds up to a number of hours.

Note: If you remove "Vulnerability" scan in the server administrator web console, the client UI will only show malware and grayware, so the display here is dynamic.

Customized Scan Options

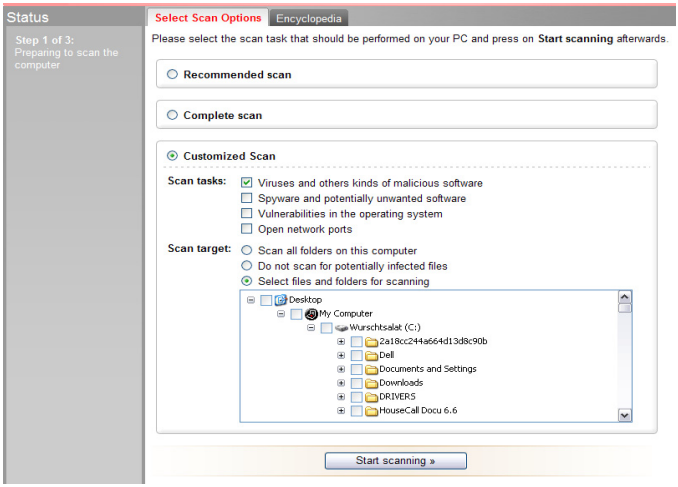


FIGURE 5-6 Customized Scan Options

Here you can configure the most powerful scanning procedure of the HouseCall client. Choosing the “Customized scan” gives you the ability to select dedicated *Scan tasks* and *Scan targets*.

Note: The Scan tasks will be displayed dynamically. Depending the users operating system, the number of selectable scan tasks can differ. On Unix system, in general it is not possible to scan for operating system vulnerabilities. On most of the Windows based operating systems, all four possible scan tasks should be displayed.

Scan tasks options

- *Viruses and other kinds of malicious software* (default) - enables the scan for known malware (e.g. viruses, trojan, worms...) and vulnerabilities
- *Spyware and potentially unwanted software* - enables the scan for spyware, grayware, adware and suspicious cookies.
- *Vulnerabilities* - scans for potential vulnerabilities on the current operating system.
- *Open network ports* - scans for system ports that are potentially unsecured and could be used to compromise the local machine.

Scan target options

- *Scan all folders on this computer* (default) - scans all files and folders on the local system with the previously customized scanning options.
- *Do not scan for potentially infected files* - in addition to the previously configured scan options, scans operating system *Registry* file for potential risks.
- *Select files and folders for scanning* - opens a Java based windows where the user can select the drives, folders and files that should be scanned with the previously customized options.

After you finished configuring the options for your customized scan process, click on "Start scanning" to perform the selected action.

Scanning process

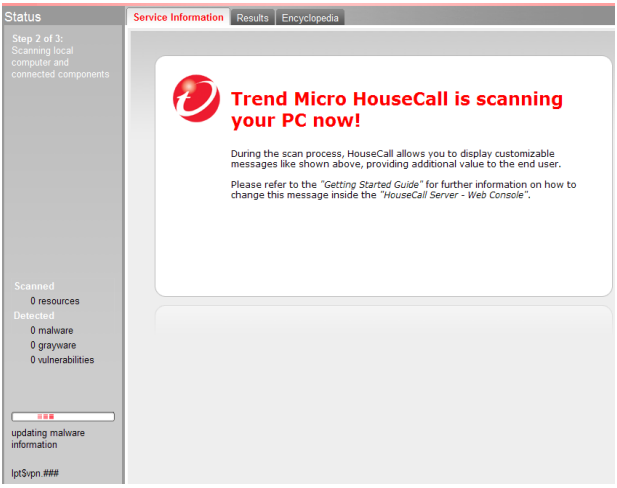


FIGURE 5-7 Scanning Process

After you have selected your scanning option and start the scan operation, the HouseCall client starts the scan task. During this step, you will see the progress of the scan procedure in the Status bar on the left side of the screen.

The number of detected scan result will be displayed, the file names and folders that are currently being scanned. As long as the scan procedure is running, a moving bar informs about the ongoing activity. To review the detailed results of the scan, change the view by clicking on the “Results” tab.

After the scan has completely finished, the “Results” tab will automatically be displayed to review the details of the scan on the different selected scan tasks.

Scan Results

After the scan has completely finished, the scan result screen will be displayed to allow further action on the detected issues during the scan.

The result are divided in three different sections

- *Detected malware* - shows detected viruses, worms, trojan and known types of malware.
- *Detected grayware/spyware* - shows detected malware, grayware, cookies and other items that may contain a potential risk to your system
- *Detected vulnerabilities* - shows vulnerabilities on your operating system and open ports that may contain a potential risk to your local system

You will see the number of detected issues on the different sections and can expand each section to see more detailed description, by clicking on the button.

The possible "Cleanup options" will be shown in each section and can be selected to perform a specific action.

Action on Scan Results

If HouseCall detects an infection, following similar result page will be displayed.

The information provided includes:

- Name, numbers and details of infection
- File name and path of the infected file
- Type of possible cleaning action

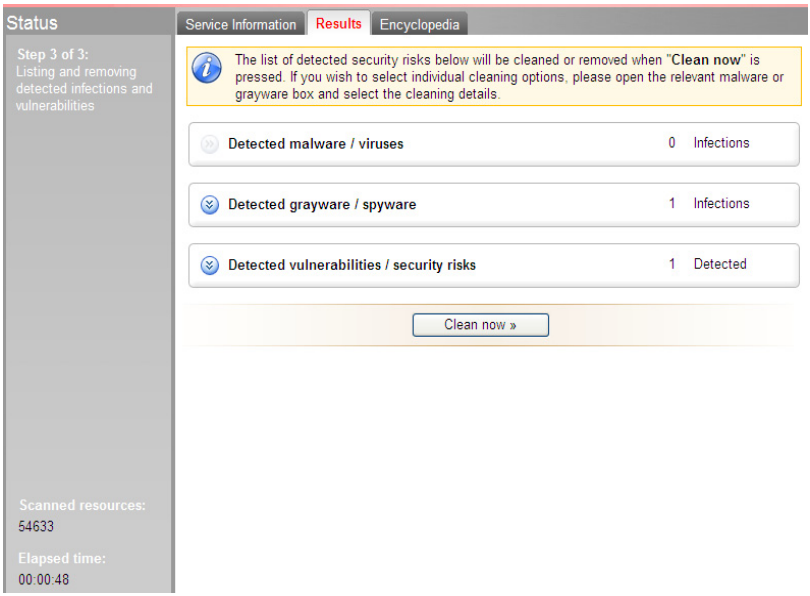


FIGURE 5-8 Action on Scan Results

To perform an action on any of the detected items, select the detection result to expand. Detailed information on any of the found items will be shown.

Action on detected malware

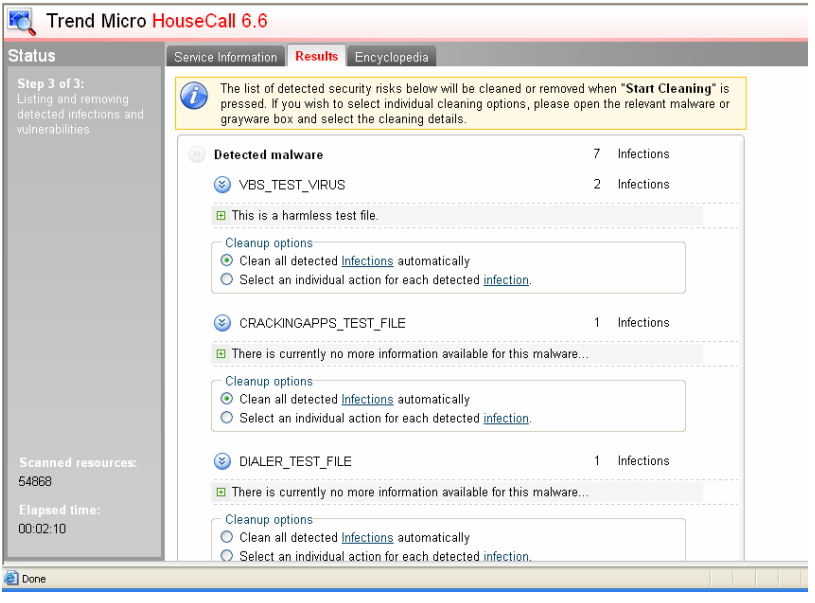


FIGURE 5-9 Action on detected malware

This is a sample screen after HouseCall detects different types of malware on the local system. Expanding the detected threats shows more details on the found infection. Select either "Clean" or an individual action on any of the found detections.

If more detailed information on any of the found detection is available, just click on the Plus ⊞ sign. The content shown will be retrieved from the Trend Micro Virus Encyclopedia.

Action on detected grayware/spyware

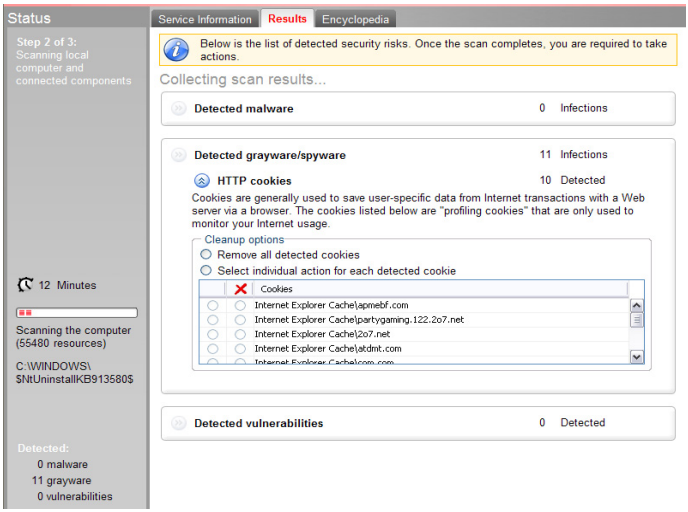


FIGURE 5-10 Action on grayware/spyware

You can either select to remove all detected items at once, or individually select every item to keep or remove by activating the leading checkbox.

	Click on this button to expand the current view/item and get more details
	Selected items in this column are marked to be cleaned from the system
	Selected items in this column will be removed from the system

Action on detected vulnerabilities

After selecting actions on the items, click on the “Clean now” button to perform.

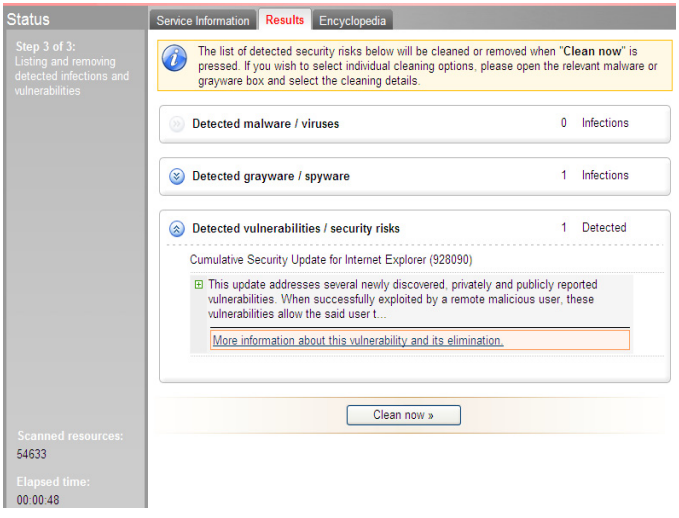


FIGURE 5-11 Action on Vulnerability

The "More information..." link refers to the Microsoft Windows Update site to give more details on the found vulnerability. After downloading and installing the latest available patches dependend on the detected vulnerability, while performing the next scan, the list of vulnerabilites should be empty.

Log Files

The HouseCall Client **Log** files provide information about important events during usage.

These events can be categorized as follows:

1. **ActiveUpdate** logs — information about scan engine and pattern file updates

   a. For Windows XP/2000/2003/MCE2005:

   ```
   C:\Documents and Settings\UserName\Application
   Data\HouseCall 6.6\AU_Data\AU_Log
   ```

   b. Linux:

   ```
   ~/HouseCall 6.6\AU_Data\AU_Log
   ```

2. HouseCall Client logs — information about communication with the Server, infections, **backup**, **quarantine**, **cleaning** and product **warnings** or **errors**

   a. For Windows XP/2000/2003/MCE2005:

   ```
   C:\Documents and Settings\UserName\Application
   Data\HouseCall 6.6\log
   ```

   b. Linux**:**

   ```
   ~/HouseCall 6.6/log
   ```

Uninstalling the HouseCall Client

To uninstall the HouseCall client, open the Software Add/Remove panel from your operating system and select “Trend Micro HouseCall Client Version 6.6". Click on the “Remove” button and the uninstall program for the client will be executed.

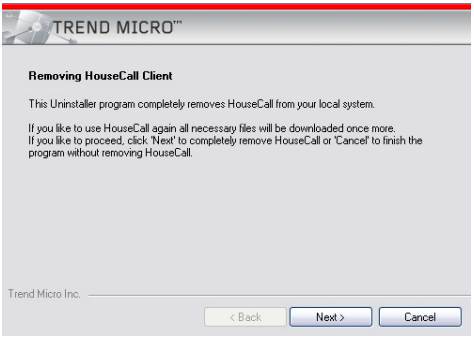


FIGURE 5-12 Uninstalling the HouseCall client

Click on “Next” button to continue the uninstallation process, or “Cancel” to exit the uninstallation and keep the clients files on the system.

No further questions will be asked while remove all HouseCall related files and folders. Clicking “Next” will show you the progress of the uninstallation.

Finish Uninstall

FIGURE 5-13 HouseCall Client uninstall finished

After the removal of the HouseCall client files and folders, this is the final screen that will be displayed. Click on the “Finish” button to close the application and the entry in the Software Add/Remove panel will disappear. The uninstallation process has completed.

Additional Note - HouseCall Client and Microsoft Vista

The HouseCall Client can also run on Micsoft Vista environment, but because of some limitations, the HouseCall client is only executable from the Client Launcher tool which allows the client to run in the Internet Explorer as an embedded application.

To run the HouseCall Client from the Vista environment, please follow the steps below.

- Login to the HouseCall Server Console
- Proceed to "Domains" > Create Launcher
- Enable checkbox "Embed the browser window ..."
- Press button "Download"
- Save executable on local disk
- Starting the EXE-file, it will be open HC Client correctly

Chapter 6

Technical Support, Security Information, and Troubleshooting

This chapter describes how to proceed while contacting the Trend Micro support in case of facing any issues with your HouseCall server or client product. The topics discussed in this chapter include:

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 threats 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.

To make this possible, TrendLabs, a global network of antivirus research and product support centers, provides continuous 24x7 coverage to Trend Micro customers around the world. TrendLabs' modern headquarters has earned ISO 9002 certification for its quality management procedures in 2000 - one of the first antivirus research and support facilities to be so accredited. We believe TrendLabs is the leading service and support team in the antivirus industry.

Trend Micro is headquartered in Tokyo, Japan, with business units in North and South America, Europe, Asia, and Australia–a global organization with more than 2,800 employees in 25 countries.

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

http://www.trendmicro.com

Contacting Trend Micro

Trend Micro has sales and corporate offices located in many cities around the globe. For global contact information, visit the Trend Micro Worldwide site at

http://www.trendmicro.com/en/about/contact/overview.htm

Note: The information on this Web site is subject to change without notice.

Contacting Technical Support

To contact Trend Micro Technical Support, visit the following URL:

http://kb.trendmicro.com/solutions/

Then, click the link for one of the following regions:

Asia/Pacific

Australia and New Zealand

Europe

Latin America

United States and Canada

Follow the instructions for contacting support in your region.

Version Information

In addition to virus pattern updates, Trend Micro also provides occasional scan engine and/or program upgrades. To find out exactly which virus pattern, spyware, or scan engine build you are running, refer to the local.conf.file in the clients program folder (C:\Documents and Settings\[username]\Application Data\HouseCall 6.6) or the Summary Page at HouseCall Server web console.

About Scan Engine Updates

By storing the most time-sensitive virus information in external data files such as the virus pattern file, the anti-spam database, and outbreak protection policies (actions deployed via Control Manager that help keep viruses from propagating), Trend Micro is able to minimize the number of scan engine upgrades while at the same time keeping protection up-to-date. Nevertheless, Trend Micro periodically makes new scan engine versions available. New engines are released, for example, when:

- New scanning and detection technologies have been incorporated into the software
- A new, potentially harmful virus is discovered that cannot be handled by the current engine
- Scanning performance is enhanced
- Support is added for additional file formats, scripting languages, encoding, and/or compression formats
- To view the version number for the most current version of the scan engine, visit:

  http://www.trendmicro.com

Knowledge Base

Trend Micro Knowledge Base is a 24x7 online resource that contains thousands of do-it-yourself technical support procedures for Trend Micro products. Use Knowledge Base, for example, if you are getting an error message and want to find out what to do. New solutions are added daily.

Also available in Knowledge Base are product FAQs, important tips, preventive antivirus advice, and regional contact information for support and sales.

Knowledge Base can be accessed by all Trend Micro customers as well as anyone using an evaluation version of a product. Visit:

http://kb.trendmicro.com/solutions/

And, if you cannot find an answer to a particular question, the Knowledge Base includes an additional service that allows you to submit your question via an email message. Response time is typically 24 hours or less.

Known Issues

Known issues are features in your Trend Micro HouseCall 6.6 Server Edition software that may temporarily require a workaround. Known issues are typically documented in section 9 of the Readme document you received with your product. Readmes for Trend Micro products can also be found in the Trend Micro Update Center:

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

Known issues can be found in the technical support Knowledge Base:

http://kb.trendmicro.com/solutions/

Trend Micro recommends that you always check the Readme text for information on known issues that could affect installation or performance, as well as a description of what's new in a particular release, system requirements, and other tips.

Sending Suspicious Code to Trend Micro

You can send your viruses, infected files, Trojans, suspected worms, spyware, and other suspicious files to Trend Micro for evaluation. To do so, visit the Trend Micro Submission Wizard URL:

http://subwiz.trendmicro.com/SubWiz

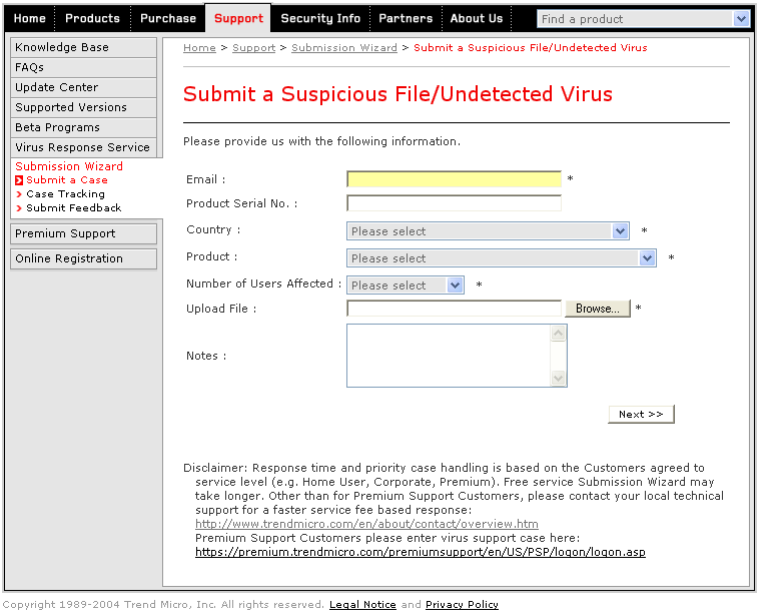


FIGURE 6-1 Submission Wizard screen

You are prompted to supply the following information:

Email: Your email address where you would like to receive a response from the antivirus team.

Product Serial No: The serial number of the product affected.

Country: The name of your country selected from the drop-down menu. This information is used to update the Virus Map.

Product: The name of the product you are currently using. If you are using multiple Trend Micro products, select the product most affected by the problem submitted, or the product that is most commonly in use.

Number of Users Affected: The number of users in your organization that are infected.

Upload File: Trend Micro recommends that you create a password-protected zip file of the suspicious file, using the word "virus" as the password—then select the protected zip file in the Upload File field.

Notes: Please include a brief description of the symptoms you are experiencing. Our team of virus engineers will "dissect" the file to identify and characterize any threats it may contain and return the cleaned file to you.

Note: Response time and the prioritization assigned to your case is based on your customer service level (Home User, Corporate, or Premium).

When you click **Next**, an acknowledgement screen displays. This screen also displays a case number for the problem you submitted. Make note of the case number for tracking purposes.

Security Information Center

Comprehensive security information is available over the Internet, free of charge, on the Trend Micro Security Information Web site at

http://www.trendmicro.com/vinfo/

Visit the Security Information site to:

- Read the Weekly Virus Report, which includes a listing of threats expected to trigger in the current week, and describes the 10 most prevalent threats around the globe for the current week
- View a Virus Map of the top 10 threats around the globe
- Consult the Virus Encyclopedia, a compilation of known threats including risk rating, symptoms of infection, susceptible platforms, damage routine, and instructions on how to remove the threat, as well as information about computer hoaxes
- Download test files from the European Institute of Computer Anti-Virus Research (EICAR), to help you test whether your security product is correctly configured
- Read general virus information, such as:

  - The Virus Primer, which helps you understand the difference between viruses, Trojans, worms, and other threats
  - The Trend Micro Safe Computing Guide
  - A description of risk ratings to help you understand the damage potential for a threat rated Very Low or Low vs. Medium or High risk
  - A glossary of virus and other security threat terminology
- Download comprehensive industry white papers
- Subscribe to Trend Micro's Virus Alert service, to learn about outbreaks as they happen, and the Weekly Virus Report
- Learn about free virus update tools available to Webmasters
- Read about TrendLabs, Trend Micro's global antivirus research and support center

TrendLabs

TrendLabs is Trend Micro's global infrastructure of antivirus research and product support centers that provide up-to-the minute security information to Trend Micro customers.

The "virus doctors" at TrendLabs monitor potential security risks around the world to ensure that Trend Micro products remain secure against emerging threats. The daily culmination of these efforts are shared with customers through frequent virus pattern file updates and scan engine refinements.

TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services. Dedicated service centers and rapid-response teams are located in Tokyo, Manila, Taipei, Munich, Paris, and Irvine, CA, to mitigate virus outbreaks and provide urgent support.

TrendLabs' modern headquarters, in a major Metro Manila IT park, has earned ISO 9002 certification for its quality management procedures in 2000—one of the first antivirus research and support facilities to be so accredited. We believe TrendLabs is the leading service and support team in the antivirus industry.

Damage Cleanup Services

Trend Micro Damage Cleanup Services (DCS) helps restore your Microsoft Windows system after an attack. DCS is designed to clean up worms, virus remnants, Trojans, and unwanted registry entries on clients. These services fall within the "Assessment and Restoration" phase of the Enterprise Protection Strategy.

As of version 2.5, DCS is a standalone product with its own management console. This product shares an installation program with Trend Micro Vulnerability Assessment 2.0, and these two products are closely related.

Version 2.5 and previous versions, which exist primarily as services of other Trend Micro products, support the following:

- Terminates malware instances in memory
- Removes malware registry entries
- Removes malware entries from system files
- Scans for and deletes malware copies in local hard drives

DCS reports show where vulnerabilities exist and track the systems that were cleaned. The standalone product can also send administrative notifications of scans to selected recipients.

Troubleshooting

HouseCall Client Logging

Two different Log levels can be configured to create a log output.

For Active update components and the update process, you can edit the “aucfg.ini” file, which can be found at “C:\Documents and Settings\[username]\Application Data\HouseCall 6.6" .

Parameter “level” can be configured from

1 - most information to

5 - less information (default)

To increase the log level of the regular client output, edit “local.conf” at location “C:\Documents and Settings\[username]\Application Data\HouseCall 6.6":

- Set/Add Logging in .housecall/local.conf
  ```
  Logging.EngineLog.Min=FINEST
  Logging.ExecutionLog.Min=FINEST
  ```
- Restart the HouseCall Client

HouseCall Server Logging

The Log level of the HouseCall server can be configured in file “config.xml” at location “C:\Program Files\Trend Micro\HouseCall Server Edition 6.6\config”

The log level can be configured from

Verbose -

Non-Verbose -

The HouseCall Log files can be found at “C:\Documents and Settings\[username]\Application Data\HouseCall 6.6\logs”

The Apache Log files can be found at “C:\Documents and Settings\[username]\Application Data\HouseCall 6.6\server\logs”

Configuration Files

There are three types of configuration files (HouseCall Server, Web Application server, including Tomcat, HouseCall Client).

HouseCall Server

For configuring HouseCall Server, logging and database access edit the following configuration file

- The main configuration file of the HouseCall Server is

  ```
  <web application server installation>/config/config.xml
  ```

- Settings for log configuration are located in

  ```
  <web application server
  installation>/config/modules/log4j.xml
  ```

Web Application Server Tomcat

- The main configuration files of Tomcat are located in

  ```
  <web application server
  installation>/config/modules/jaas.conf
  ```

HouseCall Client

The HouseCall Client stores its configuration in only one, user-related file.

- The HouseCall Client configuration file is

  ```
  <current user home directory>/Application Data/HouseCall
  6.6/local.conf
  ```

Glossary of Terms

This glossary describes special terms as used in this document or the online help.

Term	Description
Activation Key	A character code, including hyphens, that is used to identify HouseCall Server Edition.
Active Update Server	Trend Micro Update Service for scan engines and pattern files
Domain	The domain definition in HouseCall Server means that HouseCall Server is able to host several domains with configuration settings. This is the same as named-based Virtual Host support on Web Server.
Encyclopedia	In HouseCall Client an encyclopedia about viruses & Co, computer, Trend Micro and Glossary Terms is integrated
Extended Select	HouseCall Client allows for an extended selection of scans for folders and files, grayware, spyware or security checks.
HouseCall Client	Lightweight On-demand scanner that uses Trend Micros scan technology
HouseCall Root Server	Trend Micro HouseCall Server, which serves the HouseCall Child Server
HouseCall Server HouseCall Child Server	Trend Micro HouseCall Server, which provides the HouseCall Client to users for on-demand scanning and cleaning.

Platforms, Compression, and Encoding

Trend Micro has developed scan engines for all major platforms, including Windows, Unix, and DOS (individual platforms are listed below). In addition, the scan engines recognize all file types, more than 20 compression types, major encoding algorithms, Microsoft Office macros, and Web scripting languages. No known viruses or network exploits get past the engine, and there are multiple layers of analysis and protection that guard against unknown threats.

Password Protected/Encrypted Files

Since files must be opened to be scanned, password-protected or encrypted files cannot be scanned. These files are recognized as unable to be opened (and therefore un-scannable). The administrator can designate the entire class for automatic quarantine, or choose to have the scan engine ignore these files.

Platforms

- Windows 2003, 2000, Me, 95/98 and XP
- Unix, including Solaris, all major flavors of Linux, IBM AS/400, OS/390
- DOS

Encoding

- MIME
- Uuencode
- Bin/Hex

File Types

- Executables, including .exe, .com, .lnk, .bas, .reg
- Library files, including .dll,
- Others, including .hlp and.chm
- Microsoft Office files (see *Macro Scripts* below)

Compression

- Zip
- Arj
- Cab

Macro Scripts

Word Basic

VBA (Visual Basic for Applications)

VBA3

Note: Examples of applications that host Macro scripts are Microsoft Word, Excel, and PowerPoint.

Scripting Languages

- JavaScript
- VBScript

Using Ticketing in Trend Micro HouseCall 6.6

General Definition of "Ticket"

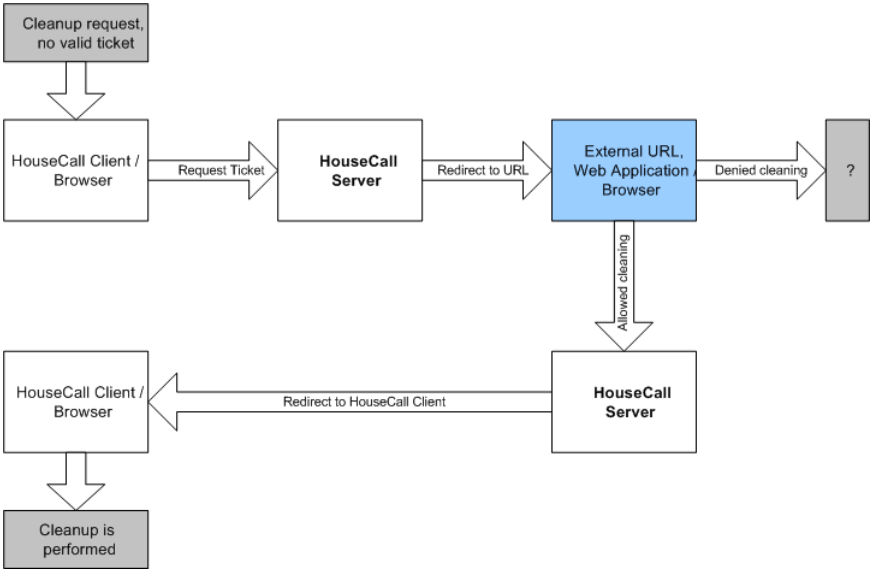
Trend Micro HouseCall 6.6 allows the cleaning of any detected infections only after a ticket code has been obtained from the HouseCall server.

Ticket codes uniquely identify a ticket. A ticket controls the access rights to cleanup sessions and is requested by the HouseCall client, in order to start cleaning any detected infections. Tickets and enforcement of the full rights are maintained on the server side and accessed through the ticket code that was provided to the client.

A ticket is necessary to request a cleanup session. Tickets need to exist on the server and must be valid.

If the client-side ticket system is enabled, a cleanup can be performed only if the client knows the ticket code of a valid ticket on the server, otherwise a new ticket needs to be requested from the server.

The following chart illustrates the complete process:



Ticket Transaction Steps

1) The transaction starts when the client requests a new ticket. The ticket obtained from the server will be in the "created" state and is not yet valid. In fact, the HouseCall Client is now waiting for the transaction to complete.

2) The transaction proceeds by opening a custom URL inside the HouseCall Client (browser) of a web application that must at least must finalize the transaction by calling a web service method on the HouseCall Server.

3) In the sample implementation attached to this appendix, the final page invokes "EnableTicketFromExternalPurchase" on the HouseCall Server.

4) This returns a URL to redirect the browser. Once the browser has been redirected, the HouseCall Client automatically starts the cleanup.

Technical background

The transaction inside the external web application is finalized by invoking a SOAP/RPC-based web service on the HouseCall Server with the following signature:

```
<URL> EnableTicketFromExternalPurchase (
<Text> isoCountryId,
       <Text> isoLanguageId,
       <Text> domain,
       <Text> ticketCode,
       <Text> ui
)
```

isoLanguageId	The language code in ISO 639 2 letter code
isoCountryId	The country code in ISO 3166 2 letter code
domain	The domain used requesting the ticket
ticketCode	The ticket code just created
ui	Optional value: The user interface to redirect the user
Return value	A URL of the location to forward the requesting client (browser) in order to finalize the transaction and start the cleanup

The WSDL location for this method is:

https://login:password@host/housecall/services/ProtectedHouseCallTicketing?WSDL

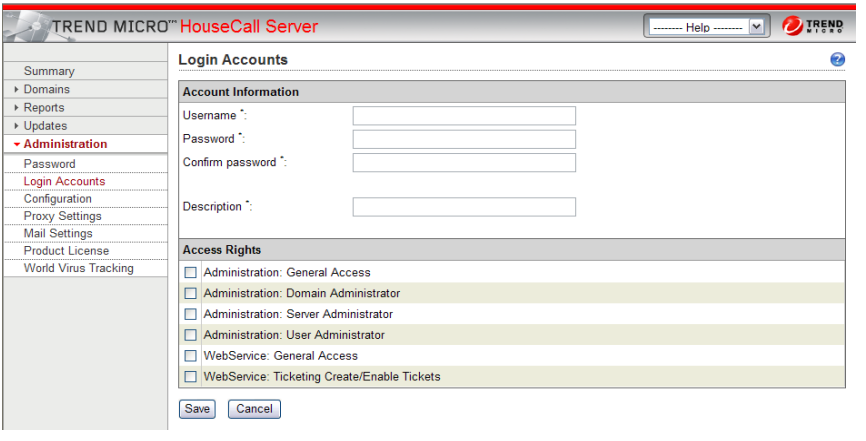
This method is login- and password-protected; the transferred data is encrypted using SSL.

Note: Tomcat needs to be configured to support SSL-secured transfers.

User accounts that allow access to the protected web service interface of the ticket system, can be configured via the Administrator Console of your HouseCall Server.

To create a new user account, log on to your HouseCall Server's Administrator Console, go to **Administration**, select **Login Accounts** and **Add a new Account**.

The following screen will display:



Enter a login name and password for the new user and assign the following two roles.

- *WebService: General Access* - Allow general access to protected web services on this server
- *WebService: Ticketing* Create/Enable Tickets

Click the "Save" button to create the new user login. Once this is done, use the login name and password you just created whenever account credentials are needed, e.g. to log on to the HouseCall server for getting the WSDL or invoking the **EnableTicketFromExternalPurchase** method.

Sample Application

A sample application implemented in the portable scripting language PHP is attached to this document to support the development of a web application that can be used for the transaction mode.

Notes on the sample application:

- The sample application contains a file called “index.php” which acts as the entrance point for HouseCall. (The transaction URL that is configured inside the Administrator Console needs to point to this file)
- Server host and user credentials are configured in the file “conf/setup.php”
- The application requires to have either PHP4 with PEAR or PHP5 installed
- The application uses sessions

Index