TREND MICRO™
Damage Cleanup Services™ 3

Administrator's Guide

TREND MICRO™

Document Part No. DCEM32236/50331

Release Date: October 2006

Patents Pending

The user documentation for Trend Micro Damage Cleanup Services is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software is available in the online help file and online Knowledge Base at the Trend Micro Web site. To contact Trend Micro technical support, go to the *Contacting Trend Micro* section of this document.

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

www.trendmicro.com/download/documentation/rating.asp

Contents

Chapter 2: Installing Damage Cleanup Services

Chapter 3: Getting Started with Damage Cleanup Services

List of Figures

List of Tables

Preface

Welcome to the *Trend Micro™ Damage Cleanup Services 3.2 Administrator's Guide*. This book contains information about the tasks you need to do to install and configure Damage Cleanup Services™. This book is intended for novice and experienced users of Damage Cleanup Services who want to quickly configure, administer, and use the product.

The Damage Cleanup Services package includes the Trend Micro Solutions CD for Damage Cleanup Services.

This preface discusses the following topics:

Damage Cleanup Services Documentation

The Damage Cleanup Services (DCS) documentation consists of the following:

Online Help—Web-based documentation that is accessible from the DCS management console by clicking the Help icon ( ).

Administrator's Guide—PDF documentation that is accessible from the Trend Micro Solutions CD for Damage Cleanup Services and is downloadable from the Trend Micro Web site.

This guide contains detailed instructions on how to configure and administer Damage Cleanup Services, as well as explanations of DCS concepts and features. See *About This Administrator's Guide* on page 4 for a brief description of the chapters in this book.

Readme File—Contains information about known issues, bug fixes from earlier releases, system requirements, installation, release history, Trend Micro contact information, and license agreement.

About This Administrator's Guide

The Damage Cleanup Services (DCS) Administrator's Guide, which is in Adobe Acrobat format (PDF), provides the following information:

Product Overview

Overview of the product and its features, and a discussion of The Agentless Cleanup Strategy employed by Damage Cleanup Services (*Understanding Damage Cleanup Services* on page 1-1)

Installation

Guidelines on installing and updating Damage Cleanup Services 3 and on activating the DCS license (*Installing Damage Cleanup Services* on page 2-1 and *Getting Started with Damage Cleanup Services* on page 3-1)

Configuring and Administering Scans

Procedures to configure and administer scans and notifications from the Damage Cleanup Services Web-based management console and guidance on keeping Damage Cleanup Services up to date (*Configuring Scans* on page 4-1)

Creating Scans

Detailed instructions on how to create scheduled and one-time scans for malware and spyware/grayware, including guidance on using the Manual Damage Cleanup Tool (*Using the Manual Damage Cleanup Tool* on page 5-10)

Managing Logs

Detailed instructions on managing logs and reports (*Logs and Reports* on page 6-1)

Troubleshooting

Assistance on troubleshooting and technical support, including Frequently Asked Questions (*Troubleshooting and Technical Support* on page A-1)

Glossary

Glossary of relevant terms (*Glossary* on page B-1)

Audience

The Damage Cleanup Services ™ documentation is written for IT managers and network administrators. The documentation assumes the reader has a basic knowledge of network security systems and has some familiarity with other Trend Micro products.

Document Conventions

To help you locate and interpret information easily, the Damage Cleanup Services 3 documentation uses the following conventions.

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

TABLE 1. Conventions used in the DCS documentation

Chapter 1

Understanding Damage Cleanup Services

This chapter includes the following topics:

Features and Benefits

Damage Cleanup Services (DCS) is a comprehensive service that helps assess and clean system damage without installing software on client computers in a network. It removes network viruses that can re-attack the network. It performs the following activities:

- Removes unwanted registry entries created by worms or Trojans
- Removes memory-resident worms or Trojans
- Removes active spyware/grayware
- Removes rootkits
- Removes garbage and viral files dropped by viruses
- Assesses a system to decide whether it is infected or not
- Returns the system to an active and clean state
- Can register to Cisco™ Incident Control Server™
- Can act on cleanup requests from Trend Micro InterScan Web Security Suite™ and the new Trend Micro InterScan Web Security Appliance™
- Enhanced spyware/grayware detection

Client Machines That DCS Can Scan

Damage Cleanup Services can deploy cleanup and assessment tasks to the following client machines:

- Windows 2000 Professional/Server/Advanced Server
- Windows XP Professional
- Windows Server 2003 (Web, Standard, or Enterprise Edition)
- Windows Server 2003 R2 (Standard or Enterprise Edition)

What's New in Damage Cleanup Services 3.2

Best-of-Breed Spyware/Grayware Detection and Cleanup

DCS 3.2 comes with a greatly improved spyware scanning and cleanup engine. This new engine and pattern can detect and clean more spyware/grayware than ever before, with fewer false positives.

This version of DCS also includes a new component for detecting and removing rootkits. Currently on the rise, rootkits corrupt regular operating system functions that application programs assume are valid to gain a great deal of control on the user's computer. Rootkits are extremely hard to remove without rebuilding the machine.

The improved Spyware Scan Engine includes the following features:

- Anti-rootkit Driver component that can be updated separately through ActiveUpdate
- Can automatically take action on self-resuscitating spyware
- Can delete spyware remnant files after system restart
- Can scan running processes
- Can scan known bad IP addresses in a Hosts file
- Deletes more references to bad files for better spyware cleanup

Changes in Component Names

Components available in the previous version have been renamed but will still function as before.

- From Damage Cleanup template to Virus Cleanup Template
- From Spyware Cleanup template to Spyware Pattern
- From Damage Cleanup engine to Virus Cleanup Engine
- From Spyware Scan engine to Spyware Scan Engine

Can Serve As a Stand-alone Product or Register to Trend Micro Control Manager

DCS is capable of functioning as a stand-alone product and has the following new features:

- Its own installation program
- A scalable architecture that can expand to multiple servers or to a wide area network
- Management through either Trend Micro Control Manager or through the stand-alone DCS management console
- Its own configurable administrative notifications
- Separate queries for spyware/grayware logs and malware logs

Improved Account Management Tool

DCS provides a Windows-based account management tool to allow IT managers to set the domain/machine administration account password. DCS must have administrative privileges for each client in your network in order to scan the clients. Use this tool to give DCS the access it needs.

With this release, the Account Management Tool makes it easier to add scan targets, regardless of account type. For more information, see *Using the Account Management Tool* on page 3-6.

Global Deployment Settings

You now have the option of having DCS mark all deployed files for deletion by client machines upon reboot. See *Global Deployment Settings* on page 4-2.

Global and Scan-Specific Exclusion Lists

Because not all spyware/grayware is undesirable, IT managers can mark desired spyware/grayware for exclusion from the assessment and cleanup processes. DCS provides for a global exclusion list, for spyware/grayware to be excluded from all scans (See *Global Spyware/Grayware Exclusion List* on page 4-8), and scan-specific lists, which can be tailored to any individual scan (See *Scan-Specific Spyware/Grayware Exclusion List* on page 4-8).

Three Scan Modes for Spyware/Grayware Scans

You can now choose from three spyware/grayware scan modes, based upon your IT policies.

- Quick scan (Fastest scan, but only a partial scan)
- Full scan (Slower than quick scan, but a complete scan)
- Hybrid scan (Try quick scan. If it finds any spyware/grayware, switch to full scan)

See *Spyware/Grayware Scan Types* on page 4-6 for details about these scan modes.

For a description of the term "grayware," see *What Is Grayware?* on page 1-7.

Advanced Spyware/Grayware and Malware Scan Reporting

DCS can produce a variety of spyware/grayware and malware scan reports, drilling all the way down to the level of an individual machine if desired. DCS can export these reports in Adobe Acrobat (`.PDF`) format. Users can also export database logs into .CSV files.

Enhanced Scan Target Selection

This release features a method of importing a large list of scan targets via a customized INI file. (See *Importing a List of Scan Targets* on page 4-13.) You can also input a larger range of IP addresses for your scan targets.

You can select scan targets by any of the following criteria (or any combination of them)—

- IP address
- IP range
- Network segment or subnet mask
- Machine name
- Domain name

Scheduled Updates

DCS supports manual or scheduled updates of components.

Damage Cleanup Services Basics

Trend Micro Damage Cleanup Services (DCS) helps restore your Windows system after a Trojan attack. Trojans and viruses are similar because they both attack your system. However, a Trojan cannot self-replicate, whereas a virus can.

When a Trojan runs, you will likely experience unwanted system problems in operation, and sometimes, loss of valuable data. These are indications that you should run DCS on your system.

Who Should Use Damage Cleanup Services?

DCS is designed for IT managers and administrators of medium-to-large computer networks. In order for DCS to find and clean active Trojans, worms, and spyware/grayware in memory, it is not necessary to install any software on client machines. A single DCS server can deploy its updated cleanup engine (*The Virus Cleanup Engine and the Spyware Scan Engine* on page 1-11) when needed to all of the computers in the network. Individual users need not even be aware that DCS is doing its job. In the rare case in which DCS is unable to connect to a client machine, because it is running an outdated operating system or because the login information that DCS has is incorrect, the administrator can provide the user with a simple URL that, when clicked, activates a special Manual Damage Cleanup Tool (see *Using the Manual Damage Cleanup Tool* on page 5-10) that scans and cleans that particular client and sends the resulting scan log back to the DCS server.

How Does Damage Cleanup Services Access Client Machines?

DCS uses several technologies. When preparing DCS for use, you enter the account information for all of the computers in the network into the Account Management Tool (see *Using the Account Management Tool* on page 3-6). DCS uses this tool when accessing clients. Because no DCS software is installed on client machines, only the DCS server is required to update its components, which are as follows:

- The Virus Cleanup Template, which contains patterns used to identify Trojans and network viruses
- The Spyware Pattern, which DCS uses to intelligently identify active spyware programs
- The Virus Cleanup Engine, which DCS deploys to each client machine at the time of scanning
- The Spyware Scan Engine, which DCS deploys to each client machine at the time of scanning
- The Anti-rootkit Driver, which detects and removes rootkit programs

Therefore, client machines are never required to update any software or receive pattern files.

Note: DCS uses NetBIOS protocol to resolve client machine names. If your network has NetBIOS disabled, please see page A-2 for a workaround.

DCS uses ActiveX controls to perform several tasks. For this reason, the machine on which the DCS server is installed must have Microsoft Internet Information Server (IIS) and the browser used for accessing the DCS Web console must be Microsoft Internet Explorer.

DCS uses Microsoft .NET Framework 1.1 to generate reports. For this reason, this technology is required for the DCS server.

What Is Grayware?

Your computers are at risk from potential threats other than viruses. Grayware refers to applications or files that are not classified as viruses or Trojans, but can still negatively affect the performance of the computers on your network and introduce significant security, confidentiality, and legal risks to your organization. Often, grayware performs a variety of undesired and threatening actions such as irritating users with pop-up windows, logging user key strokes, and exposing computer vulnerabilities to attack.

Types of Grayware

Damage Cleanup Services scans for several types of grayware in memory, including the following:

- **Spyware:** gathers data, such as account user names, passwords, credit card numbers, and other confidential information, and transmits it to third parties
- **Adware:** displays advertisements and gathers data, such as Web surfing preferences that could be used for targeting future advertising at the user
- **Dialers:** changes client Internet settings and forces a computer to dial preconfigured phone numbers through a modem. These are often pay-per-call or international numbers that can result in a significant cost to your organization.
- **Joke Programs:** causes a computer to behave abnormally, such as making the screen shake or modifying the appearance of the cursor.
- **Hacking Tools:** helps malicious hackers enter a computer
- **Remote Access Tools:** helps hackers remotely access and control a computer
- **Password Cracking Applications:** helps decipher user names and passwords
- **Others:** other types of programs that are potentially malicious

How Spyware and Other Grayware Get Into Your Network

Spyware and other grayware often get into a corporate network when users download legitimate software that includes grayware applications in the installation package. Grayware applications often use ActiveX controls.

Most software programs include an End User License Agreement (EULA), which the user has to accept before downloading. Often the EULA does include information about the additional grayware application and its intended use to collect personal data. However, users often overlook this information or do not understand the legal terminology describing the application.

Potential Risks and Threats

Spyware and other types of grayware on your network have the potential to intorduce the following:

- **Reduced computer performance:** To perform their tasks, grayware applications often use significant CPU and system memory resources.
- **Increased Web browser-related crashes:** Certain types of grayware, such as adware, are often designed to create pop-up windows or display information in a browser frame or bar. Depending on how the code in these applications interacts with system processes, grayware can sometimes cause browsers to crash or freeze and may even require a system reboot.
- **Reduced user efficiency:** Grayware can unnecessarily distract users from their main tasks by forcing them to close frequently occurring pop-up advertisements and deal with the negative effects of joke programs.
- **Degradation of network bandwidth:** Grayware often regularly transmits the data it collects to other applications running on your network or to locations outside of your network, using up your network bandwidth.
- **Loss of personal and corporate information:** Not all data that grayware applications collect is as simple as a list of Web sites users visited. Some grayware can also collect user names and passwords that allow access to both personal user accounts, such as a bank account, and corporate accounts on your network.
- **Higher risk of legal liability:** If computer resources on your network are hijacked, hackers may be able to utilize your computers to launch attacks or install grayware on computers outside your network. The participation of your network resources in these types of activities could leave your organization legally liable for damages incurred by third parties.

The Trend Micro Solution

This version of Trend Micro Damage Cleanup Services has the ability to scan for, detect, and remove a multitude of active spyware and other grayware processes.

For instructions on configuring Damage Cleanup Services to scan for spyware/grayware, see *Selecting Scan Action* on page 4-5.

The Agentless Cleanup Strategy

Overview

Damage Cleanup Services (DCS) is an important part of the Trend Micro overall Enterprise Protection Strategy, falling within the area of "Assessment and Restoration."

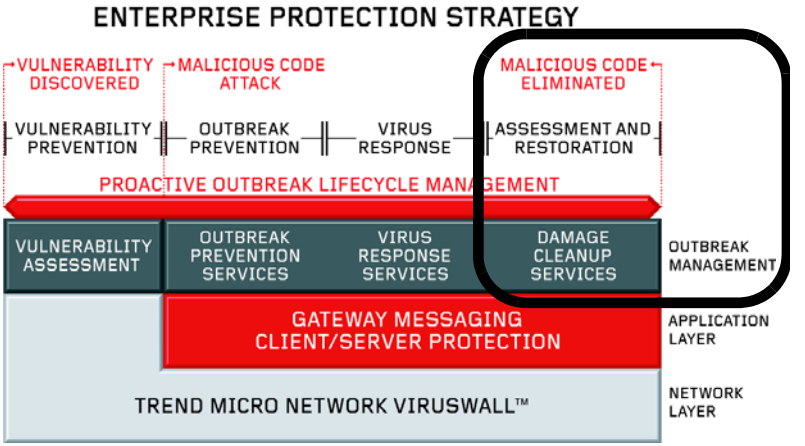


FIGURE 1-1. Where DCS fits in the Enterprise Protection Strategy

DCS enables IT managers to remotely detect viruses and other Internet threats on all of the machines in a network and clean up any damage that the threat has caused. It is extremely time-consuming and costly to clean up virus damage by manually installing and running a repair agent on each affected machine. DCS can clean machines without the need to manually install anything on any client machine.

Instead of requiring manual installation, DCS deploys the Virus Cleanup Engine to each client machine at the time of scanning. This engine scans the machine and repairs any damage that Trojans or worms have caused. The administrator is never required to manually install software on individual machines. This approach constitutes the DCS agentless cleanup strategy.

The Virus Cleanup Engine and the Spyware Scan Engine

Damage Cleanup Services makes use of two scanning and cleanup tools to protect your computers. The first, called the Virus Cleanup Engine, finds and repairs damage caused by viruses and other Internet threats. The second, the Spyware Scan Engine, can find and clean spyware and other grayware.

The Virus Cleanup Engine

The Virus Cleanup Engine is essentially a software agent that makes use of a database to find targeted machines and evaluate whether or not viruses or other Internet threats have affected them. The Virus Cleanup Engine resides on a single machine, deploys to the targeted client machines on the network at the time of scanning, and, if you select the option, can mark all deployed DCS files for removal of the Virus Cleanup Engine from each targeted machine the next time those machines reboot.

The Virus Cleanup Engine uses the Virus Cleanup Template, which contains information that Virus Cleanup Engine uses to restore damage caused by the latest known viruses or other Internet threats. DCS regularly updates these templates and patterns.

The Spyware Scan Engine

The DCS Spyware Scan Engine works in much the same way as the Virus Cleanup Engine, making use of a database and deploying to targeted client machines at the time of scanning. The Spyware Scan Engine, however, uses cutting-edge technology to find and kill active spyware programs. As with the the Virus Cleanup Engine, if you select the option, DCS can mark this component (and all deployed DCS files) for removal from targeted machines the next time those machines reboot.

Tip: When you install DCS, you are installing the versions of the Virus Cleanup Engine and the Spyware Scan Engine that were current as of the release of this product. These engines are updated frequently, however, so Trend Micro recommends that you update your components immediately after installing and activating DCS.

Chapter 2

Installing Damage Cleanup Services

This chapter includes the following topics:

Pre-Installation Considerations

Before installing Damage Cleanup Services (DCS), please take careful note of the following:

System Requirements

The only platform to which DCS can successfully install to is Microsoft Windows server. The system on which you install DCS has different system requirements than its client systems. For system requirements for client machines in your network, see *Client Machines That DCS Can Scan* starting on page 1-2 and *Using the Manual Damage Cleanup Tool* starting on page 5-10.

Minimum System Requirements

Operating system:

- Windows 2000 Server/Advanced Server SP3
- Windows 2003 Standard/Enterprise Server
- Windows Server 2003 R2 (Standard or Enterprise Edition)

WARNING! *DCS does not support Microsoft Windows NT as the DCS server machine, nor does it support SQL 7.*

Browser:

Microsoft Internet Explorer 5.5 plus SP2 (DCS uses ActiveX controls and JavaScript, and those technologies are supported by IE 5.5 + SP2.)

Web server:

- Microsoft Internet Information Server (IIS) 5.0 (with Windows 2000)
- Microsoft Internet Information Server (IIS) 6.0 (with Windows 2003)

Hardware:

- Memory: 512MB
- Processor: Pentium III, 1GHz
- Available Disk Space: 300MB

Other:

Microsoft .NET Framework 1.1 (DCS installs it if it is not present)

Recommended System Requirements

Hardware:

- Memory: 1GB
- Processor: Pentium 4, 2.4GHz or faster
- Available Disk Space: 2GB

Installing from CD

To install from the Trend Micro Enterprise CD:

1. Insert Disk [1] in the CD drive of the server where you will install Trend Micro Damage Cleanup Services. (If the CD does not automatically open, double-click the file `setup.exe` in the root directory of the CD drive.)
2. In the drop-down menu under "Already know what you are looking for?" select **Damage Cleanup Services** and click **GO.** The Damage Cleanup Services installation page appears.
3. Follow the steps under *Pre-Installation Considerations* on page 2-2 and *The InstallShield Wizard* on page 2-6.

Installing via a Web Download

To download from the Web:

1. Download or copy the Damage Cleanup Services binary archive to a temporary directory on the server where you want Damage Cleanup Services to run, and then extract the files.
2. Double-click the file `setup.exe` to begin installing (or `readme.txt` for program information).

Follow the steps under *Pre-Installation Considerations* on page 2-2 and *The InstallShield Wizard* on page 2-6

Microsoft Dot-Net Framework 1.1 Is Required for DCS Reporting

Please be aware that DCS reporting makes use of Microsoft .NET Framework 1.1. If installed on a machine running .NET 2.0 (the current Microsoft recommendation), DCS will install .NET Framework 1.1, and the two versions will co-exist peacefully on the same machine.

DCS Requires that NetBIOS Be Enabled

DCS makes use of NetBIOS to deploy and execute DCS scan agents. DCS cannot scan if NetBIOS is disabled.

Tip: Microsoft.NET Framework 1.1 cannot be installed remotely. If installing DCS on a machine that does not have .NET Framework 1.1, install it manually on your DCS server machine to ensure success.

To perform the necessary pre-installation tasks:

1. The installation program checks to see if Microsoft .NET Framework 1.1 is installed on your system. If Microsoft .NET Framework 1.1 is not already on your system, the installation program installs it for you.

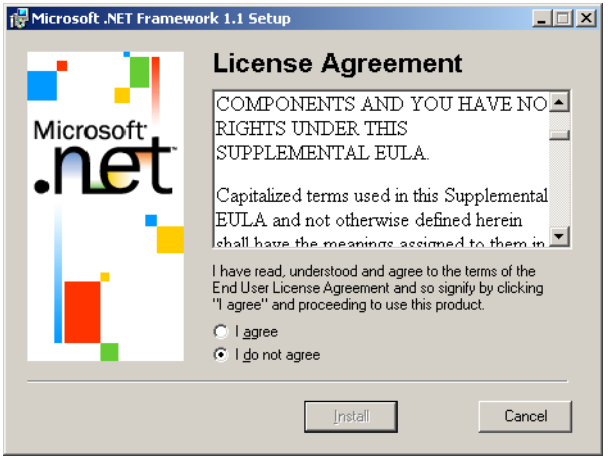


FIGURE 2-1. License Agreement screen of Microsoft .NET Framework 1.1 installation

2. Once Microsoft .NET Framework 1.1 has completed its installation, the DCS InstallShield Wizard begins.

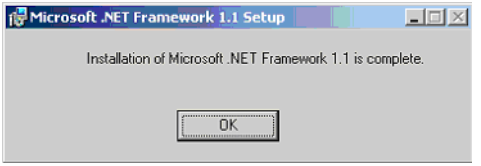


FIGURE 2-2. Microsoft .NET Framework 1.1 installation is complete

The InstallShield Wizard

The Damage Cleanup Services (DCS) Installation Wizard makes installation of DCS simple. The steps of the wizard can be broken down into four major tasks:

1. *Launching the InstallShield Wizard* on page 2-6
2. *Selecting a Database* on page 2-9
3. *Activating Damage Cleanup Services* on page 2-13
4. *Setting an Administrator Account and Installing the Program Files* on page 2-15

Launching the InstallShield Wizard

Follow the instructions below to launch the DCS InstallShield Wizard.

To launch the Damage Cleanup Services InstallShield Wizard:

1. Launch the InstallShield Wizard by double-clicking the file `setup.exe` on your Trend Micro Damage Cleanup Services CD (or on your hard disk, if you have downloaded it). The InstallShield Welcome screen appears.

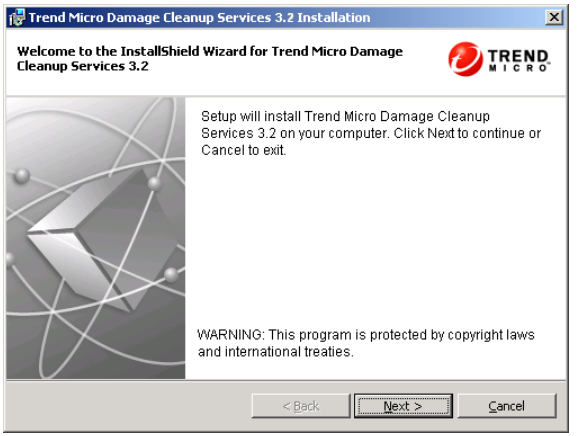


FIGURE 2-3. InstallShield Wizard splash screen

2. Click **Next** from the initial InstallShield screen to start the installation. The License Agreement screen appears.

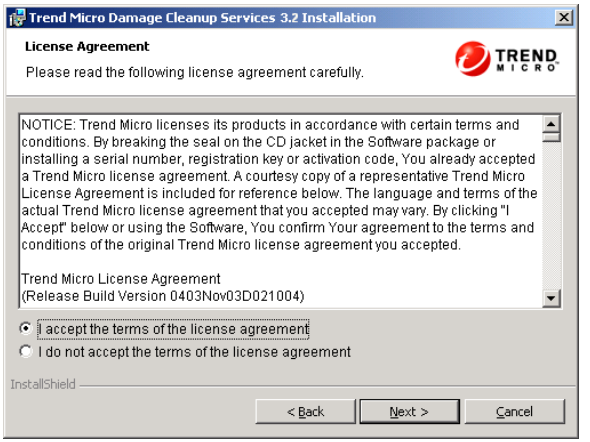


FIGURE 2-4. License Agreement screen

3. After reading the agreement text, select **I accept the terms of the license agreement** and click **Next.** The Checking System Requirements screen appears. (If you do not accept the terms of the agreement, select **I do not accept the terms of the license agreement** and click **Cancel** to cancel the installation or simply click **Cancel**).

4. The InstallShield checks your system for minimum system requirements and displays the results.

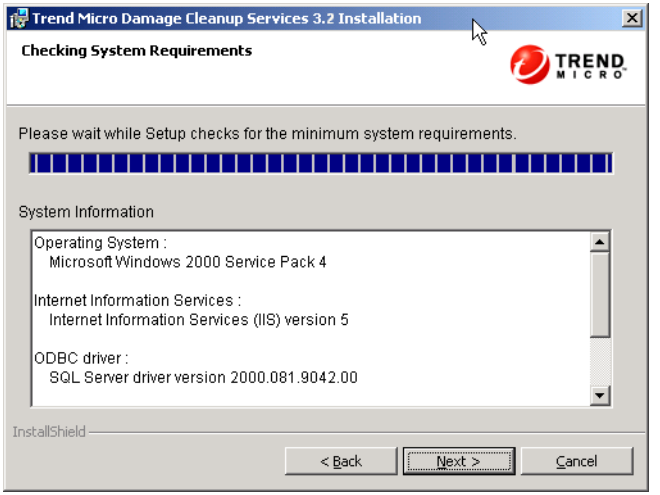


FIGURE 2-5. Checking System Requirements screen

After the InstallShield has checked system requirements, click **Next.** The Database Information screen appears.

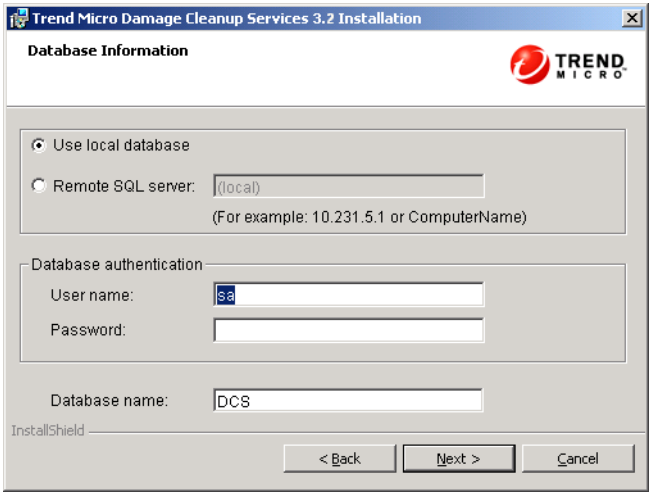


FIGURE 2-6. Database Information screen

Selecting a Database

The InstallShield first checks to see whether your machine has Microsoft SQL2000 Server installed. If SQL server has been installed on the machine, InstallShield provides two options:

- Use Local Database
- Remote SQL Server

If InstallShield finds that there is no SQL server installed on the machine, it offers the option of installing Microsoft SQL Server Desktop Engine at that time. The options it presents are:

- Install Microsoft SQL Server Desktop Engine
- Remote SQL Server

If InstallShield finds that Microsoft SQL Server is installed on the machine, but the version is older than Microsoft SQL2000 Server, it presents only one option:

- Remote SQL Server

To select a database for use with DCS:

1. Select **Install Microsoft SQL Server Desktop Engine (MSDE)** or **SQL server.** If you will be deploying to only a limited number of clients, and if you do not require the more advanced administrative options available with SQL server, you may want to use MSDE. Otherwise, choose **SQL server.**

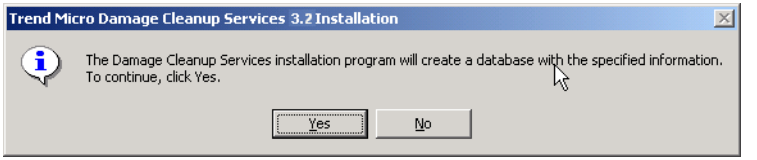


FIGURE 2-7. Message advising about the creation of a database

2. If using SQL server, type the server address.

3. If using database authentication, type the **User name** and **password.** Click **Next.** The Connection Settings screen appears.

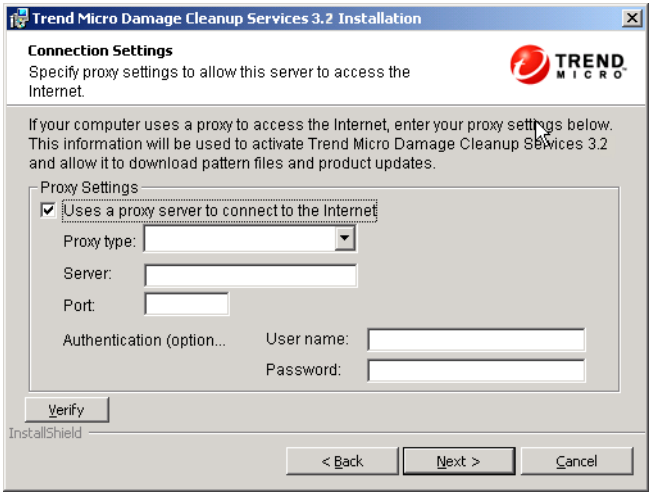


FIGURE 2-8. Connection Settings screen

4. If your computer uses a proxy server, select **Uses a proxy server to connect to the Internet**, select the **Proxy type**, and type the server name, port and (optionally) a user name and password for authentication.
5. Click **Verify** to verify that proxy server is valid. If the proxy server is valid, InstallShield displays the following information message:

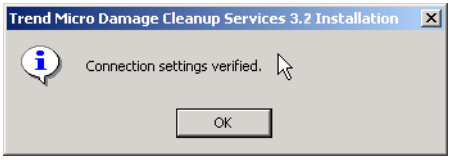


FIGURE 2-9. Connection settings verified message

6. Click **OK** to close the information message and click Next in the Connection Settings screen. The Product Activation screen appears.

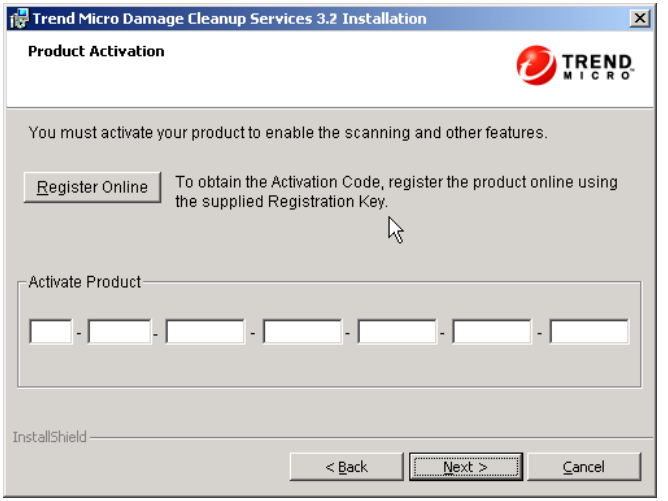


FIGURE 2-10. Product Activation screen

Activating Damage Cleanup Services

To activate Damage Cleanup Services and set installation directory:

1. If you do not have an Activation Code, click **Register Online** to register your product and obtain an Activation Code. A Web browser window opens to the Trend Micro online registration page. Follow the instructions on the Web site to obtain your Activation Code.

   Once you have the Activation Code, type it in the fields provided in the Activate Products section.

   Note: The product can still install even if you do not activate it now. You can install first and enter the Activation Code later if you like. However, the program runs only after activation.

2. Click **Next.** The Destination Folder screen appears.

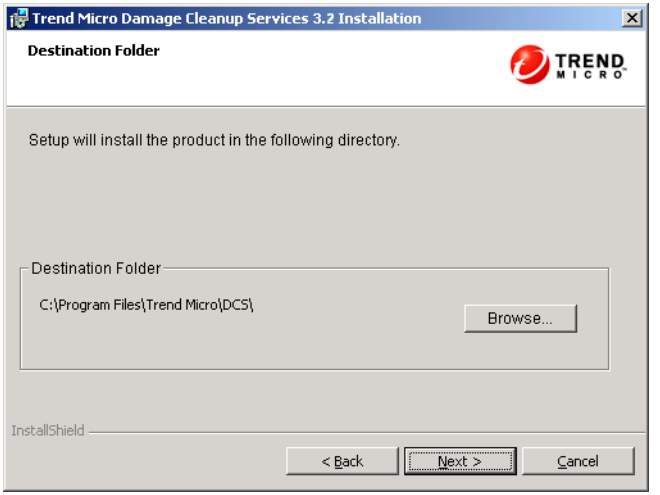


FIGURE 2-11. Destination Folder screen

3. To select a directory other than the default installation directory, click **Browse** and navigate to your preferred installation directory. Click **Next.** The Administrator Account screen appears.

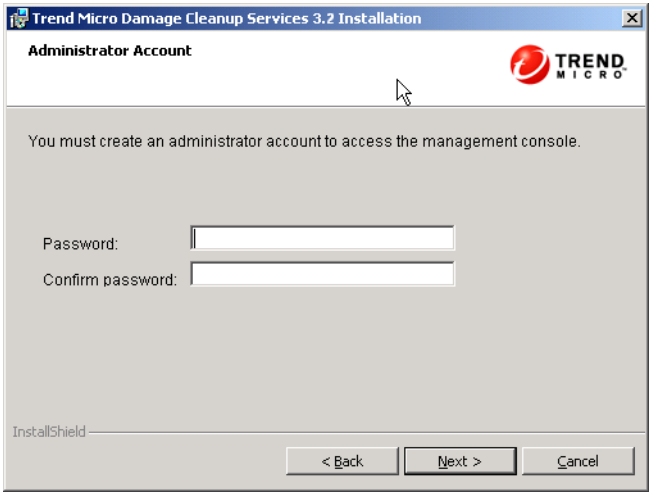


FIGURE 2-12. Administrator Account screen

Setting an Administrator Account and Installing the Program Files

To set up an administrator account and install the program files:

1. Type a password for the Administrator account that you will use with DCS and retype it in **Confirm password.** Click **Next.** A screen appears stating that you are now ready to install Trend Micro Damage Cleanup Services.

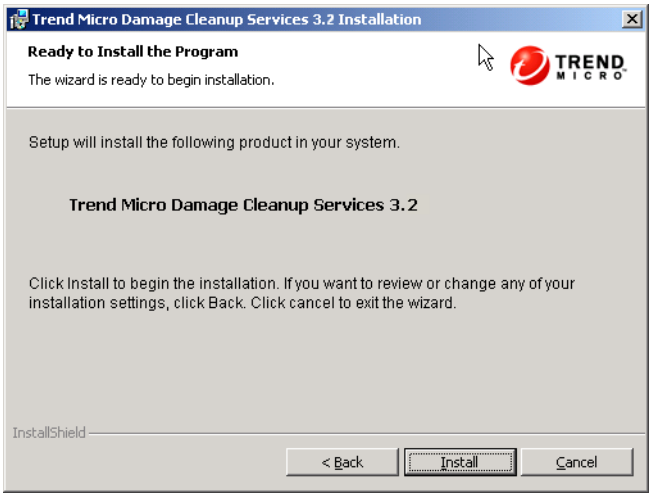


FIGURE 2-13. Ready to Install the Program screen

2. Click **Install** to install Damage Cleanup Services.

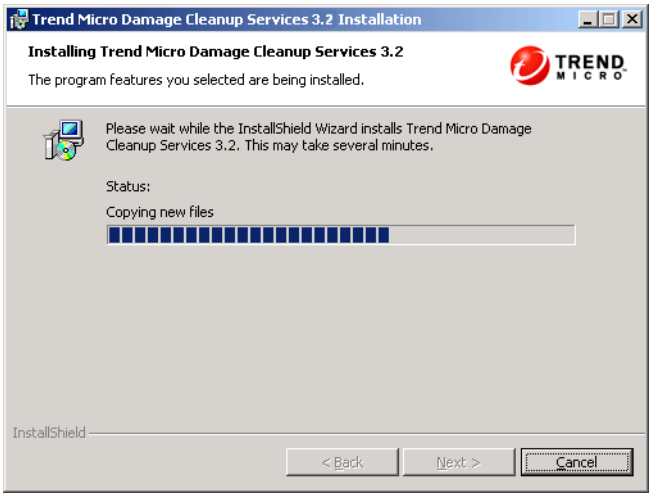


FIGURE 2-14. DCS InstallShield, progress bar screen

The InstallShield installs the program and the InstallShield Wizard Completed screen appears.

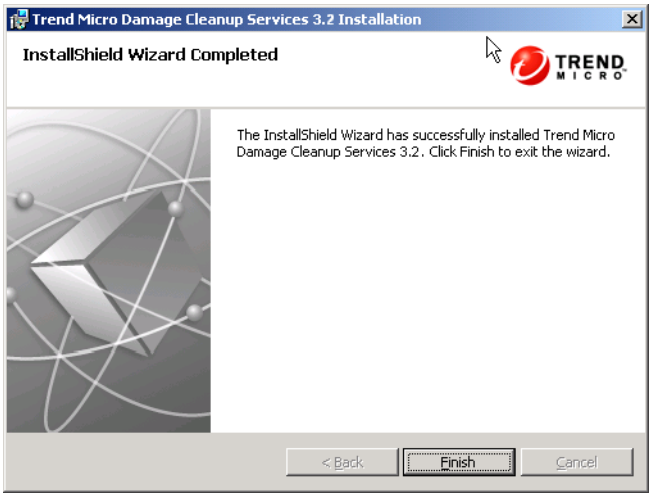


FIGURE 2-15. InstallShield Wizard Completed screen

3. Click **Finish** to exit the InstallShield Wizard.

Managing Passwords

Passwords for DCS should be at least six (6), and preferably eight (8) or more alphanumeric characters long. To make sure your environment is secure, choose a password that is difficult to guess.

The following tips can help you create a safe password:

- Include both letters and numbers in your password
- Avoid words found in the dictionary
- Intentionally misspell words
- Use phrases or combine words
- Use both uppercase and lowercase letters

You can change your DCS password via the Administration submenu.

To change your DCS password:

1. On the sidebar click **Administration** > **Password**. The Change Password screen appears.
2. Type the **Old password** and **New password** in their respective entry fields.
3. Retype the new password in the **Confirm new password** field.
4. Click **Save** to save the new password.

Managing DCS through Trend Micro Control Manager

During installation, administrators have the option to enable DCS to be managed by Trend Micro Control Manager. Choosing this option requires the installation of a Control Manager agent for DCS.

Immediately after you click Finish in the InstallShield Wizard Completed screen, a prompt appears asking if you would like to manage DCS by using Trend Micro Control Manager.

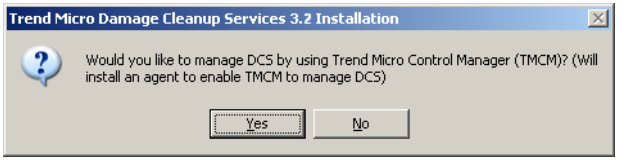


FIGURE 2-16. Message asking if Trend Micro Control Manager will manage DCS

Uninstallation Considerations

Before uninstalling DCS, there are a few issues worth considering. These issues primarily relate to preventing data loss.

Uninstalling Using a Different User Account

In DCS 3.0, the **Add/Remove program** feature for DCS and registry entries created are visible only to the user who installed DCS. In DCS 3.2 (and 3.1), these items are visible to all users. Therefore, a user who did not install the program may not be able to upgrade or remove it.

Note: When uninstalling DCS 3.0, use the same user account as the account that installed it. Other user accounts will not be able to access the **Add/Remove program** feature for DCS 3.0. If you upgrade from DCS 3.0 to 3.2 using a different account, the DCS 3.2 installation program detects the previous installation and halts.

Database Considerations

Administrators can uninstall DCS as they would any Microsoft Windows™ program. During uninstallation, the program prompts you to close any programs that have the potential to interfere with the installation. Notably, the uninstallation program asks whether you would like to keep the database:

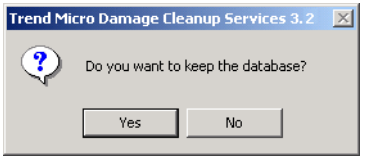


FIGURE 2-17. Message asking if you want to keep the DCS database

If it is likely that you will re-install the program, you may wish to keep the DCS database, which contains most of the information that has been entered into the DCS Web console. For example, scan settings and tasks, scan results history logs, report

history data, and the information entered using the Account Management Tool. When you re-install, you can use the same database, so that you keep all of this data.

Note: The Account Management Tool provides an export and import feature that can also provide an alternative to re-keying account information upon re-installation. (See *Importing and Exporting Account Information* on page 3-15.) Deleting the database would still delete any scan configurations and other data, however.

If you are sure that you will not re-install DCS on the same machine, Trend Micro recommends that you do not keep the database.

Chapter 3

Getting Started with Damage Cleanup Services

This chapter contains the following topics:

Activating Damage Cleanup Services

Although you are not required to enter an Activation Code (AC) while installing Damage Cleanup Services (DCS), you must register DCS before you can use its full features.

Registering and Activating Damage Cleanup Services

You need a DCS AC or Registration Key (RK) for activation. If you do not have the AC or RK, contact your Trend Micro sales representative or download an AC or RK from the Trend Micro web site. Until you input a valid Activation Code, the scan and component update functions will not work.

Trend Micro recommends that you register your product before beginning the installation process. You can register online at:

`https://olr.trendmicro.com/registration/us/en-us/login.aspx`

However, if you did not do so during installation, you can activate DCS after installation.

To activate DCS after installation:

1. On the sidebar, click **Administration** > **Product License**. The **Product License** screen appears.
2. If you do not have the AC, click **Register**. Your browser redirects to the Trend Micro registration Web site. Follow the directions on the screen and use the RK to obtain an AC.
3. Once you have the AC, type it in under **Step 2. Activate** and click **Activate**. An information screen appears notifying you of—
   - Expiration date
   - License status
   - License version
   - Date license was last updated
   - Activation Code

Within the last 60 days before your license expires, the system reminds you of how many days you have left on a daily basis.

Use this screen to update your license from evaluation to full or to re-activate your license before it expires.

Obtaining a Registration Key and an Activation Code

Registration Key

A product RK is required to complete the product registration process. This uses 22 characters, including hyphens, in the following format:

XX-XXXX-XXXX-XXXX-XXXX

Damage Cleanup Services (DCS) must be registered, using your product RK, before you receive an AC that allows you to begin using DCS.

Trend Micro recommends that you register your product before beginning the installation process.

Activation Code

An AC is required to enable scanning, receive product updates, and display the status of your license in the management console. An AC uses 37 characters, including hyphens, in the following format:

XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

After you have completed the product registration process, you will receive your Activation Code from Trend Micro.

Re-activating Damage Cleanup Services

If a license has expired but you are still within the grace period, you can still run scans and update components. Once the grace period is over, DCS locks the component update functions. To unlock this function, re-activate the license (from the sidebar click **Administration** > **Product License** > **Re-activate**).

License Status	DCS Scan	Component Updates	DCS Cleanup	Generate Reports	Update License
License expired; still in grace period	Yes	Yes	Yes	Yes	Yes
License expired; grace period is over	Yes	No	Yes	Yes	Yes

TABLE 3-1. Standard version functionality after the license expires

DCS Scan	Component Updates	DCS Cleanup	Generate Reports
No	No	No	Yes

TABLE 3-2. Evaluation version functionality after the license expires

You can activate or re-activated DCS anytime, as long as the AC you enter is valid. In order to register DCS, however, you must have a live Internet connection, because you must type your RK at the Online Registration Web site:

`https://olr.trendmicro.com/registration/us/en-us/login.aspx`

Upgrading from DCS 3.0

When upgrading to DCS 3.2 from DCS 3.0, DCS 3.2 will migrate the previous version's settings, logs, reports and data. You can also choose to enable DCS to register to Trend Micro Control Manager (TMCM) as a managed service by installing a Control Manager agent. This agent enables DCS to be managed by TMCM. Follow the DCS 3.2 installation screens for guidance on installing the TMCM agent.

If you would prefer to manage DCS through its own Web management console, simply decline to install the Control Manager agent when prompted by the DCS 3.2 installation program.

Administrators have several options on how to manage DCS:

- As a stand-alone Web console (which does not require the installation of the TMCM agent for DCS)
- As a managed service of TMCM
- As a managed service of Cisco Incident Control Server
- In conjunction with Trend Micro InterScan Web Security Suite™
- In conjunction with the new Trend Micro InterScan Web Security Appliance (a hardware device)

Setting the Internet Proxy

The Web console uses proxy settings when connecting to the Internet for two purposes:

- Registering the product (Product Registration Server)
- Downloading updates

To set the Internet proxy:

1. On the sidebar click **Administration** > **Proxy Settings.** The Proxy Settings screen appears.
2. Select **Use a proxy server.**
3. Select the type of proxy your system uses.
4. Type the server name or IP address and its port number.
5. If your proxy server requires a password, type your user name and password in the fields provided.
6. Click **Save**.

Using the Account Management Tool

Before DCS can scan any of your client machines, it needs to be able to access them with Administrator privileges. The Account Management Tool enables you to prepare your network for scanning and cleanup by DCS by supplying DCS with the Administrator user name and password for each machine in your network.

Use this tool to record this information and to view, add, modify, or delete login credentials for the machines and domains that you wish to target for scanning. (See *Selecting Scan Targets* on page 4-10 for detailed information about the Select Scan Target screen.)

This tool is accessible only from the machine hosting the Damage Cleanup Server.

You can use the Account Management Tool to:

- Add a scan target account (see *Adding an Account* on page 3-8)
- Set a default account (see *Setting a Default Account in the Account Management Tool* on page 3-11)
- Delete a domain or machine account (see *Removing a Domain or Machine Account Using the Account Management Tool* on page 3-12)
- Modify domain or machine account information (see *Editing Domain or Machine Account Information* on page 3-13)
- Import or export Account Management Tool settings (*Importing and Exporting Account Information* on page 3-15)

Note: When using the Account Management Tool, you cannot input IP addresses.

To open the Account Management Tool:

1. Click **Start** > **Programs** > **Trend Micro Damage Cleanup Services** > **Account Management Tool.** The Account Management Tool Login screen appears.
2. A list of all existing accounts appears, showing account type and the available descriptions.

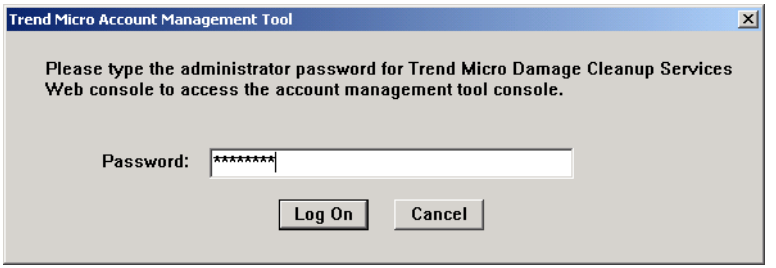


FIGURE 3-1. The Account Management Tool login screen

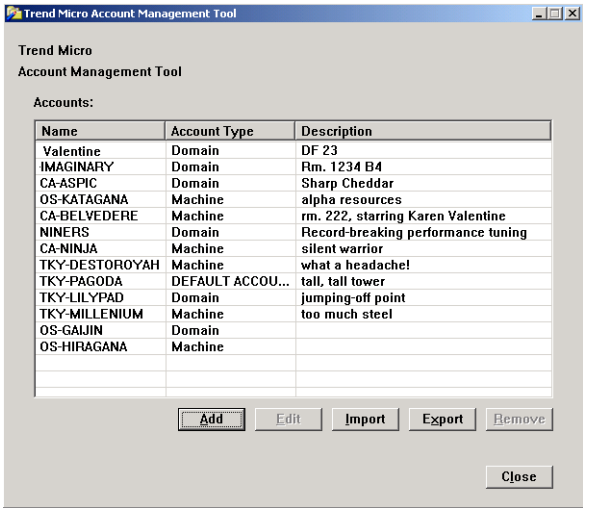


FIGURE 3-2. Use this screen to view all domain and machine accounts

To view all domains and machines currently accessible by Damage Cleanup Services:

1. Click **Start** > **Programs** > **Trend Micro Damage Cleanup Services** > **Account Management Tool** to open the Account Management Tool. The Login screen appears
2. Type your administrative password and click **Log On.** A list of all existing accounts appears, showing account type and the available descriptions.
3. Click **Close** to close the tool.

Adding an Account

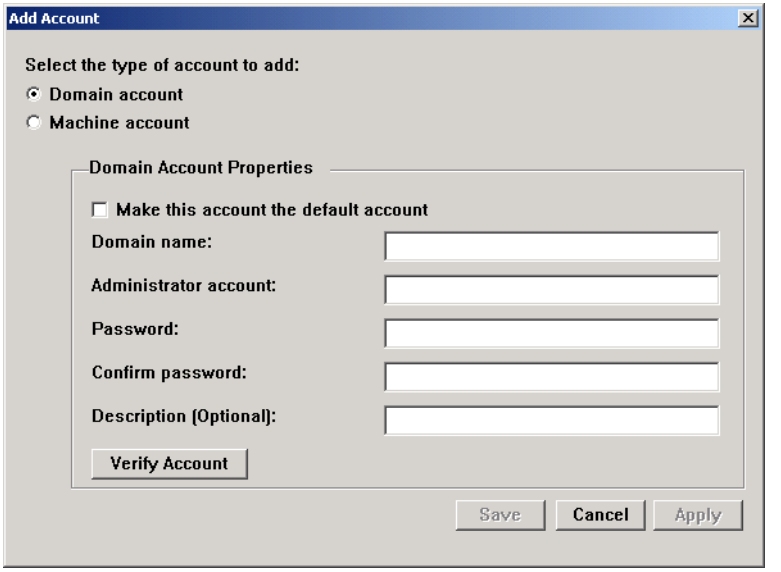


FIGURE 3-3. Account Management Tool: Add Account screen for a domain account

To add a domain account:

1. Click **Start** > **Programs** > **Trend Micro Damage Cleanup Services** > **Account Management Tool** to open the Account Management Tool.
2. Type your administrative password and click **Log On.** A list of all existing accounts, including account type and the available descriptions appears.
3. Click **Add** to add an account. The Add Account screen appears.
4. Under **Select the type of account to add,** accept the default choice of **Domain account**.
5. If this account is the default account, select **Make this account the default account**. If during a scan, DCS is unable to access a remote account, it will access the default account.
6. In **Domain name** type the Windows domain name you wish to add.
7. Type the **Administrator Account.**
8. Type the **Password** for the domain administrator account and then retype it in **Confirm Password.**
9. If desired, type a description for this account in **Description.** For example, `Company domain 1.`
10. Click **Verify** to verify that DCS can connect to the domain with the information provided. If DCS can connect to the domain, a **Successfully verified connection** message appears.
11. Click **OK** to close the verification message and click **OK** to finish adding the new domain. The domain name appears in the Name column of the Accounts table with an Account Type of **Domain.**
12. Click **Close** to close the Account Management Tool.

The procedure for adding a machine account is virtually the same as that for adding a domain account, except that the **Make this account the default account** check box is disabled, because only a domain account can serve as the default account.

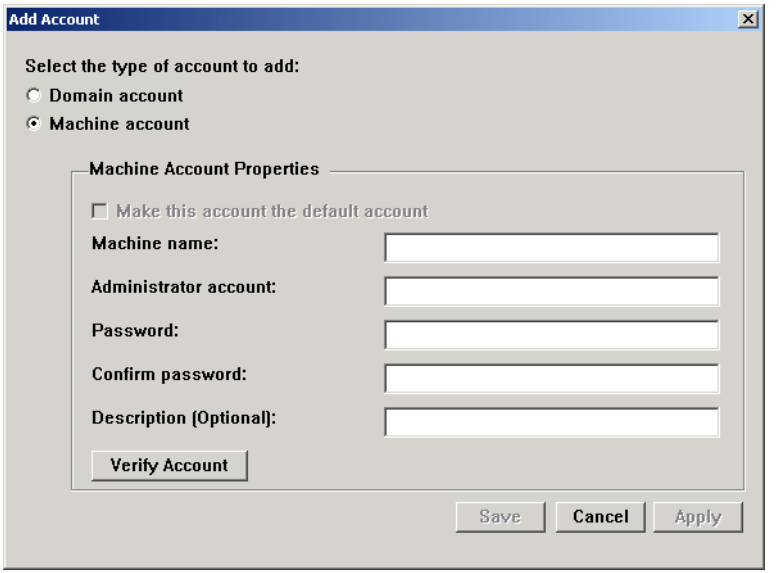


FIGURE 3-4. Account Management Tool: Add Account screen for a machine account

To add a machine account:

1. Click **Start** > **Programs** > **Trend Micro Damage Cleanup Services** > **Account Management Tool** to open the account management tool.
2. Type your administrative password and click **Log On.** A list of all existing accounts, including account type and the available descriptions appears.
3. Click **Add** to add an account. The Add Account screen appears.
4. Under **Select the type of account to add,** select **Machine account**.
5. In **Machine name** type the computer name of the client that you wish to add.
6. Type the **Administrator Account.**

7. Type the **Password** for the machine administrator account and then retype it in **Confirm Password.**
8. If desired, type a description for this account in **Description.** For example, `JSMITH02.`
9. Click **Verify** to verify that DCS can connect to the machine with the information provided. If DCS can connect to the machine, a **Successfully verified connection** message appears.
10. Click **OK** to close the verification message and click **OK** to finish adding the new machine account. The machine name appears in the Name column of the Accounts table with an Account Type of **Machine.**
11. Click **Close** to close the Account Management Tool.

Setting a Default Account in the Account Management Tool

Some network topologies make use of several subdomains branching off of one root domain. In such a topology, DCS may not be able to access a domain account deployed as a subdomain under a root domain in such a network. There is a workaround for such a scenario, however: the default account.

If, during a scan, DCS cannot find the individually targeted domain, it will use the default account to try again to locate the targeted domain. Because the problem that the default account addresses is limited to domain accounts, the default account set must be a domain account. However, one cannot set a machine account as the default account.

Tip: Trend Micro recommends creating a default account so that DCS can run a scan if the targeted domain account is located under a root domain.

To set an account as the default account, select the **Default Account** checkbox at the bottom of the Add a New Account screen.

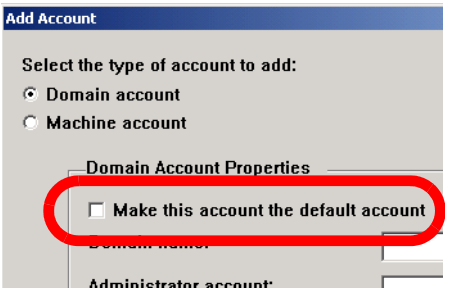


FIGURE 3-5. Location of the default account checkbox

Note: There can be only one default account, and it must be a domain account and not a machine account.

Removing a Domain or Machine Account Using the Account Management Tool

To delete a domain or machine account:

1. Click **Start** > **Programs** > **Trend Micro Damage Cleanup Services** > **Account Management Tool** to open the Account Management Tool.
2. Type your administrative password and click **Log On.** A list of all existing accounts appears, showing account type and the available descriptions.
3. Select the account that you wish to remove from the accounts list.

4. Click **Remove.** The Remove Account screen appears showing account name and administrator account.

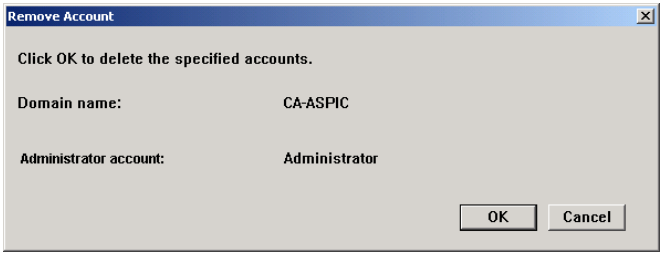


FIGURE 3-6. The Remove Account confirmation screen

5. Click **OK** to remove the account.
6. Click **OK** in the **Successfully deleted account information** message screen.

Editing Domain or Machine Account Information

To modify domain or machine account information:

1. Click **Start** > **Programs** > **Trend Micro Damage Cleanup Services** > **Account Management Tool** to open the Account Management Tool.
2. Type your administrative password and click **Log On.** A list of all existing accounts appears, showing account type and the available descriptions.
3. In the accounts list, select the domain or machine account that you wish to modify.

4. Click **Edit.** The Edit Account screen appears

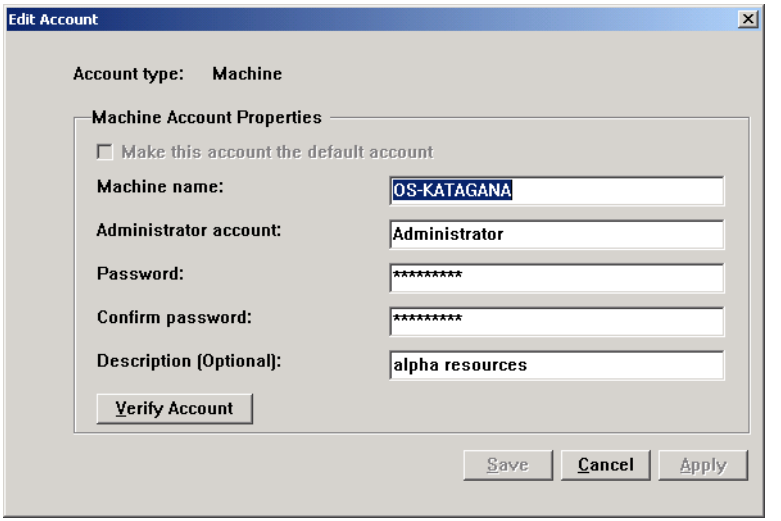


FIGURE 3-7. The Edit Account screen

5. Type the updated information in **Domain (Machine) name, Administrator account,** or **Description.**
6. If you wish to change the password, type the new password in **Password** and then retype it in **Confirm password.**
7. Click **Apply** to apply the change or **Save** to apply the change and close the Edit Account screen. A **New account information successfully modified** confirmation screen appears.
8. Click **OK.** The Trend Micro Account Management Tool screen appears, displaying the revised account information.

Importing and Exporting Account Information

You can also use the Account Management Tool to import a list of machines or domains, in comma-separated values (.CSV) format or export current settings for later use.

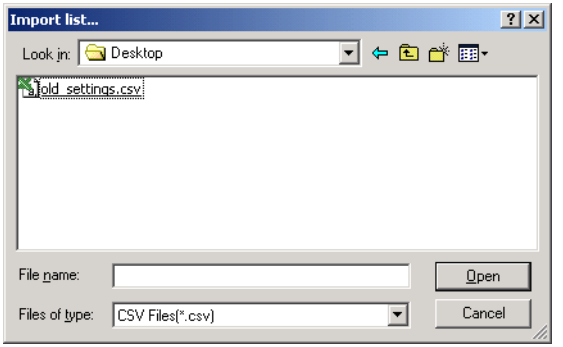


FIGURE 3-8. Importing Account Management Tool settings

To import account information:

1. Click **Start** > **Programs** > **Trend Micro Damage Cleanup Services** > **Account Management Tool** to open the Account Management Tool.
2. Type your administrative password and click **Log On.** A list of all existing accounts appears, showing account type and the available descriptions.
3. Click **Import.** An **Import list...** screen appears.
4. Navigate to your CSV file, select it, and click **Open.** If the file format is correct, the Account Management Tool imports your settings and displays an Import Completed message.
5. Click **OK** to close the Import Complete message. The settings from your import display in the Accounts table.

To export account information:

1. Click **Start** > **Programs** > **Trend Micro Damage Cleanup Services** > **Account Management Tool** to open the Account Management Tool.
2. Type your administrative password and click **Log On.** A list of all existing accounts appears, showing account type and the available descriptions.
3. Click **Export.** An **Export list...** screen appears.
4. Navigate to the location where you wish to save your settings, type a file name, and click **Save** to export your settings.
5. Click **OK** to close the Export Complete message.

Using the Damage Cleanup Services Web Management Console

Because Damage Cleanup Services (DCS) is a stand-alone product and is no longer dependent on Trend Micro Control Manager for configuration and use, DCS now has its own Web-based management console.

Logging On to the Console

After you have installed DCS, you can run the DCS console from within Windows.

To log on to the DCS Web management console:

1. Launch the DCS Web console, in one of three ways:
   a. From the Windows Start menu, click **Start** > **Programs** > **Trend Micro Damage Cleanup Services** > **Trend Micro Damage Cleanup Services**.
   b. Point your browser to the URL of your installed DCS Web console (`http://<Your_DCS_Server>/DCS/cgiDispatcher.exe`)

Tip: For convenience, you may wish to bookmark this URL in your Microsoft Internet Explorer Web browser.

---

c. Double-click the Internet shortcut file created by your installation in the default Destination Folder:
`<OS_drive>\Program Files\Trend Micro\DCS\WebUI\DCS\DCS.url`

or in the folder that you chose during installation, if this is different from the default location:
`<Destination Folder>\WebUI\DCS\DCS.url`

The DCS Web console loads in a browser window of Microsoft Internet Explorer (required because DCS makes use of ActiveX controls).

2. Type the Administrator password that you chose when installing the program and press **Enter** or click **Log On.** The DCS Web management console opens to the Summary screen.

Note: The default system timeout for DCS is 900 seconds (15 minutes). You can change the timeout setting by editing the system registry. See App. A, Troubleshooting, page A-8, for detailed instructions.

The Web Console Interface

The DCS Web management console consists of a top banner; a left-side sidebar with six major menu topics, four of which have submenus; and the main content window.

The Top Banner

The top banner displays the name of the product and contains a Log Off link and a drop-down menu listing several navigational options that, when clicked, open in a

new window. Click the **Log Off** link from within any screen at any time to log off from the console and return to the initial log on screen.

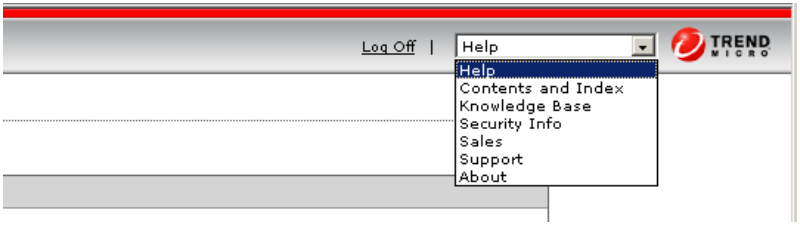


FIGURE 3-9. Navigational options in the top banner drop-down menu

Navigational options in the drop-down menu are as follows:

Help - Clicking on this option expands the drop-down menu

Contents and Index - The Damage Cleanup Services console-based Online Help (*What's New* screen)

Knowledge Base - The search page of the Trend Micro online Knowledge Base

Security Info - The latest Trend Micro advisories on malware, spyware/grayware, and other security issues

Sales - Online purchasing information from the Trend Micro Web site

Support - Information on how to get online, telephone, and email support, from the Trend Micro Web site

About - Basic version information about the current installation of Trend Micro DCS, including product version, build number, service pack version, hot fix number, component versions, and Activation Code (if one has been entered)

The Sidebar

The left-side sidebar comprises six major menu choices, five of which expand into submenus.

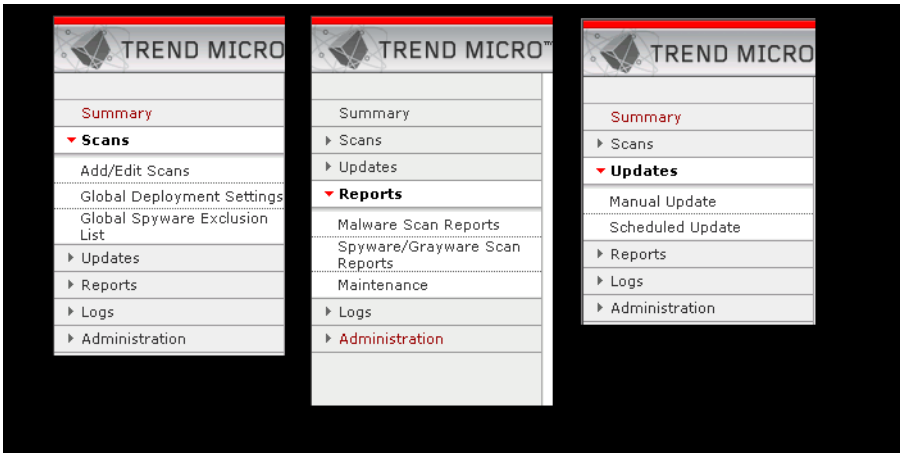


FIGURE 3-10. The Web console sidebar with various menus expanded

Summary - Opens the Summary screen in the main content window

Scans - Opens the following submenus:

Add/Edit Scans - Opens Add/Edit Scans screen showing information about existing scans with links to add, run now, copy, or delete scans

Global Deployment Settings - Opens the Global Deployment Settings screen, from which you can configure DCS to delete all deployed files from client machines after scanning.

Global Spyware Exclusion List - Opens the Global Spyware/Grayware Exclusion List screen, from which you can select spyware/grayware that you wish to exclude from all scans

Updates - Opens the following submenus:

Manual Update - Opens the Manual Update screen showing latest component versions available, current versions in use, recommended action, and an input screen for setting the download source

Scheduled Update - Opens the Scheduled Update screen showing input fields to enable scheduled update, to choose which components to update, to set an update schedule, and to specify download source

Reports - Opens the following submenus:

Malware Scan Reports - Opens the Malware Scan Reports page displaying a list of malware scan report templates if any have been created

Spyware/Grayware Scan Reports - Opens the Spyware/Grayware Scan Reports page displaying a list of spyware/grayware scan report templates if any have been created

Maintenance - Opens the Report Maintenance screen, which allows you to set the maximum number of reports to keep

Logs - Opens the following submenus:

Malware Logs - Opens the Log Query for Malware Add/Edit Scans screen, from which you can perform simple or advanced queries of malware scan logs

Spyware/Grayware Logs - Opens the Log Query for Spyware/Grayware Add/Edit Scans screen, from which you can perform simple or advanced queries of spyware/grayware scan logs

Maintenance - Opens the Log Maintenance screen, which allows you to set the maximum number of days to keep malware and spyware/grayware scan logs

Administration - Opens the following submenus:

Cisco ICS Registration - Opens the Cisco Incident Control Server (Cisco ICS) Registration screen, from which you can enter settings to enable DCS and Cisco ICS to work together

Notifications - Opens the Notifications screen, from which you can select the events that will trigger notifications, the methods of notifying recipients, and necessary settings for the various notification media

Password - Opens the Change Password screen

Proxy Settings - Opens the Proxy Settings screen, from which you can add or modify proxy settings for the DCS Web console

Product License - Opens the Product License screen, from which you can register and activate DCS if you have not already done so

The Main Content Window

The main content window is the main window by which the Trend Micro Damage Cleanup Services Web console displays its information and accepts new information.

Note that every main content screen contains a link to page-level help at the top right. Click the question mark icon ( ) from any screen to access DCS context-sensitive help.

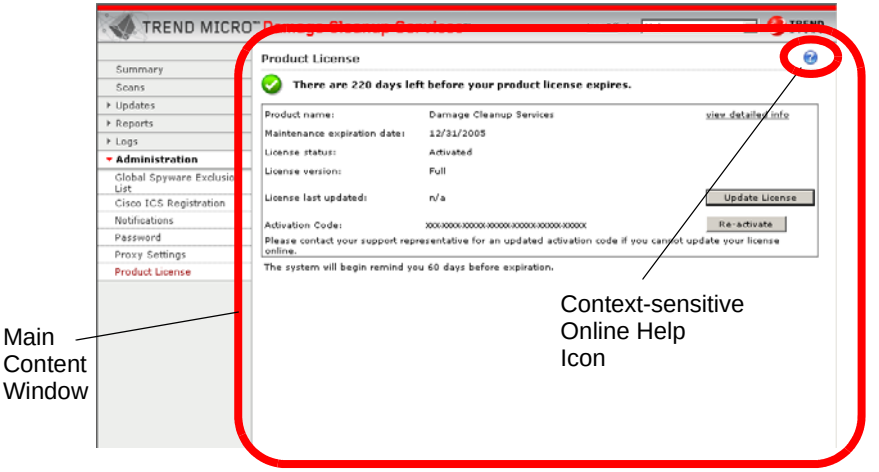


FIGURE 3-11. DCS Web management console main content window

Icons Used in the Web Console

Icon	Web Console Screen	Meaning
	Scan Result for Malware (or Spyware/Grayware)	Click to clean one or more selected machines in the Scan Result for Malware (or Spyware/Grayware) table.
	Summary, Product License screen	Warning note about how many days are left before license expires
	All screens	Click to open DCS context-sensitive Online Help.
	Summary, Manual Update screens	Click to update DCS component.
	Summary, Current Running Scan screens	Next to **Refresh** link. Click to refresh data on page. **WARNING!** *Do not use the Refresh button on your browser to refresh this page. Doing so during a running scan return will halt the display of live data and will return to the default view of the Summary screen.*
	• Add/Edit Scans screen • Add Scan screen • Malware (or Spyware/Grayware) Scan Reports screen	• Next to **Add Scan** link. Click to add a new scan to list of scans. • Next to **Add/Edit Scan Target** link. Click to edit scan targets for existing scan • Next to **Add Report Template** link. Click to add a new report template.
	Add/Edit Scans screen	Next to **Run Now** link. Click to run one or more selected scans immediately.
	Add/Edit Scans screen	Next to **Copy** link. Click to copy an existing scan in order to use it as a base for creating a new, similar scan.
	• Add/Edit Scans screen • Malware (or Spyware/Grayware) Scan Reports screen	• Next to **Delete** link. Click to delete one or more selected scans. • Next to **Delete** link. Click to delete one or more selected report templates.

TABLE 3-3. Icons used in the Web console, locations and meaning

Icon	Web Console Screen	Meaning
	Manual Update, Scheduled Update screens	Click to browse directory tree for UNC path to download source.
	• Log Query for Malware (or Spyware/ Grayware) Scan screen • Add Scan screen, Step 3 of 4: Set Schedule	• Click to open a small popup calendar from which to choose a date range for use with creating a log query. • Click to open a small popup calendar from which to choose a date for a one-time scan.
	Edit Report Template screen	Mouse over icon for additional, brief Help information.
	Log Query for Malware (or Spyware/Grayware) Scan screen	Next to **Export to CSV** link. Click to export log query results in comma-separated value format.
	Enabling and Disabling Malware (or Spyware/Grayware) Scan Report Templates screen	Indicates that a specific scan report template is enabled. Click to disable a malware or spyware/grayware scan report template. DCS disables the template and replaces the green check mark icon with a red X icon.
	Enabling and Disabling Malware (or Spyware/Grayware) Scan Report Templates screen	Indicates that a specific scan report template is disabled. Click to enable a malware or spyware/grayware scan report template. DCS enables the template and replaces the red X icon with a green check mark icon.

TABLE 3-3. Icons used in the Web console, locations and meaning

Using DCS with Cisco Incident Control Server

If you are using the Cisco Incident Control Server (Cisco ICS), you may be interested to know that DCS can now integrate with Cisco ICS. When Cisco ICS is integrated with DCS, Cisco ICS redirects the lower part of its console to the DCS user interface. DCS also sends malware scan logs to Cisco ICS upon scan completion, so that Cisco ICS can use them when generating a consolidated log report.

Registering DCS to Cisco ICS

You can register DCS to Cisco ICS from within the DCS management console.

To register DCS to Cisco ICS:

1. From the DCS management console, select **Administration** > **Cisco ICS Registration.** The Cisco ICS Registration screen appears.
2. Type the server name or IP address in **Server name/IP address.**
3. Select the http protocol you would like to use for communication between DCS and Cisco ICS. The options are **HTTP** and **HTTPS.**
4. Select the port number of the Cisco ICS server. The defaults are 8080 for HTTP and 4343 for HTTPS.
5. Type the virtual directory of the Cisco ICS CGI program in **Virtual directory.**
6. Type the update directory for Cisco ICS in **Update directory.**
7. Select the **DCS Notification URL host** from the drop-down box.
8. Click **Register Now.** DCS registers itself to the Cisco ICS server.

You can unregister DCS from either Cisco ICS or the DCS management console. For instructions on unregistering from Cisco ICS, consult your Cisco ICS documentation. For instructions on unregistering from the DCS management console, see below.

To unregister DCS from Cisco ICS:

1. From the DCS management console, select **Administration** > **Cisco ICS Registration.** The Cisco ICS Registration screen appears.
2. Click **Unregister Now.** DCS unregisters with Cisco ICS.

Updating Components from Cisco ICS

When you are using DCS in conjunction with Cisco ICS, Cisco ICS downloads any necessary updates from the Trend Micro ActiveUpdate server and then notifies DCS that an update is available. DCS can then obtain the updated components from Cisco ICS.

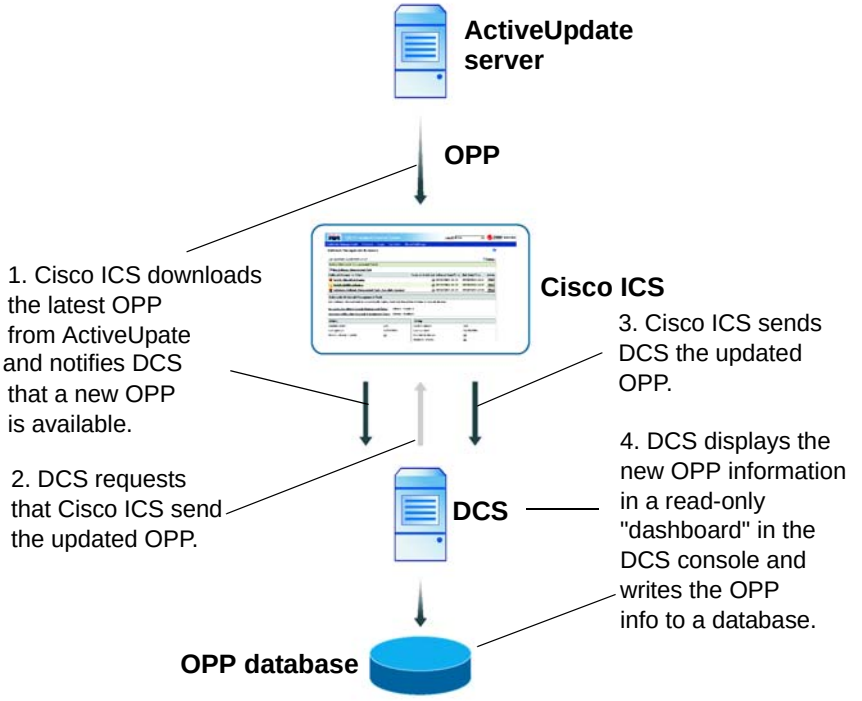


FIGURE 3-12. Delivery of OPP from ActiveUpdate through Cisco ICS to DCS

Cisco ICS and Outbreak Prevention Services

When DCS and Cisco ICS are working together, Cisco ICS obtains the Outbreak Prevention Policy (OPP) from the Trend Micro ActiveUpdateserver and notifies DCS of any new OPP. DCS can then request the OPP from Cisco ICS (see *Delivery of OPP from ActiveUpdate through Cisco ICS to DCS* on page 3-25). If there is an outbreak alert, DCS displays it in the OPP "dashboard" in the DCS management console (shown below). You can then run a manual damage cleanup to address the outbreak.

FIGURE 3-13. Outbreak Protection Policy Outbreak Alert from Cisco ICS displayed in DCS console Summary Screen

---

Note: DCS can also work with Trend Micro InterScan Web Security Suite (IWSS) and Trend Micro InterScan Web Security Appliance (IWSA). IWSS and IWSA can request a cleanup from DCS. See your IWSS or IWSA documentation for more information.

Getting Summary Information

After you log in to the DCS management console (or click **Summary** in the sidebar at any time), the Summary screen appears. Here you can view a summary of the following:

Component Update Status

View the following component update details for Virus Cleanup Template, Spyware Pattern, Anti-rootkit Driver, Virus Cleanup Engine and Virus Cleanup Engine:

Current Version: The version number of the latest component version installed

Latest Version: The version number of the latest component version available

Status: Success or failure of last update attempt and its time and date. If the last update attempt failed, DCS displays a link with the time and date of the failed attempt. Click this link to see a more detailed error message as to the reason that the update did not succeed.

Scan Results for Malware or Spyware/Grayware

View the following results details for malware or spyware/grayware scans:

Scan Name: The descriptive name of the scan

Completion Date/Time: Date and time last scan was completed. Shows percent complete if scan is in progress.

Malware (or Spyware/Grayware) Scan Action: Description of what action was taken after the last scan

Damage Found: For scans done in Assessment Only mode, shows the number of machines on which the scan found damage; otherwise, shows **n/a**

Cleanup Successful: For scans done in Assessment with Cleanup mode, shows the number of machines the scan successfully cleaned; otherwise, shows **n/a**

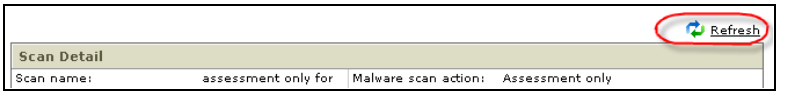
Cleanup Unsuccessful: For scans done in Assessment with Cleanup mode, shows the number of machines that the scan could not clean; otherwise, shows **n/a**

Damage Free: The number of client machines that were found to be free of damage

Unresponsive: The number of client machines that did not respond to the DCS server

Total: The total number of client machines that DCS attempted to deploy to.

Note: The screen refreshes automatically every 30 seconds. Click the **Refresh** link at the top right of the Scan Detail table to allow DCS to retrieve and display the very latest data for this screen.



You can also right-click on the screen and select Refresh from the pop-up window to refresh the data.

WARNING! *Do not click **Refresh** on your browser to refresh the data in this screen. Doing so will return halt the display of live data and will return to the default view of the Summary screen.*

Chapter 4

Configuring Scans

This chapter covers the following topics:

Global Deployment Settings

By default, Damage Cleanup Services (DCS) does not remove some deployed files on client machines. The files that remain are inconsequential to client machines but help to increase the speed of future scans. For a description of these files, see Table 4-1, "Files deployed to DCS clients," on page 4-2.

Trend Micro recognizes that some IT strategies call for zero deployed files to remain on client machines. Therefore, you can choose a deployment option that marks all deployed DCS files for removal from each targeted machine the next time those machines reboot.

Deployed File	*Description*
RMAgentService.exe	The service program that is installed to target machines. DCS server starts the service to perform the task.
RMAgent.exe	This agent is launched by the Risk Management Agent service. It executes TSC and sends the scan/clean result to the server.
RMAgentOutput.dll	This is the plug-in DLL for TSC to collect the detailed scan/clean information. It generates the results and reports to the files RM_REPORT.DAT and RM_RESULT.DAT.
TSC.exe	Virus Cleanup Engine
TSC.ini	An INI file used for configuring scanning options
TSC.ptn	Virus Cleanup Template
psapi.dll	Process status helper for Windows systems

TABLE 4-1. Files deployed to DCS clients

Deployed File	*Description*
ssapiptn.da5	Spyware Pattern
ssapi32.dll	Spyware Scan Engine
tmcomm.sys	Anti-rootkit Driver
TmEngDrv.dll	The library for Anti-rootkit Driver
unicows.dll	A DLL used for client machines that do not support Unicode
usrwl.dat	Lists spyware/grayware for exclusion from scanning

TABLE 4-1. Files deployed to DCS clients

To set DCS to mark all deployed files for removal upon next client reboot:

1. On the left-side panel, click **Scans** > **Global Deployment Settings.** The Global Deployment Settings screen displays.
2. Select **Yes, I want to remove all deployed files.**
3. Click **Save.** Client machines scanned while DCS is operating with this option will remove all deployed DCS files the next time the client machine reboots.

Note: When DCS operates with the **Yes, I want to remove all deployed files** option, deployed files will remain on a client machine until that machine reboots.

Adding a Scan

Using the DCS Add Scan screen, you can customize scan name and description, scan action, scan target, schedule, and notification.

To open the Add Scan screen:

1. Select **Scans** from the sidebar. The Scans submenu opens.
2. Click **Add/Edit Scans.** The Add/Edit Scans screen appears.
3. Click the **Add Scan** link. The Add Scan screen appears.

There are four steps to creating a scan:

- *Step 1 of 4: Select Scan Action* (see *Selecting Scan Action* on page 4-5)
- *Step 2 of 4: Select Scan Target* (see *Selecting Scan Targets* on page 4-10)
- *Step 3 of 4: Set Schedule* (see *Setting Scan Schedules* on page 4-15)
- *Step 4 of 4: Notification* (see *Setting Notifications of Scan Completion* on page 4-16)

Selecting Scan Action

To customize scan name and description:

1. Type a scan name in the **Scan name** field.
2. Type a description of the scan in the **Description** field.
3. Select **Enable the scan.**

Note: You must complete the steps under *Selecting Scan Targets* on page 4-10**,** *Setting Scan Schedules* on page 4-15**,** and *Setting Notifications of Scan Completion* on page 4-16 before you can save your changes.

To select scan action:

1. Select **Scans** from the sidebar. The Add/Edit Scans screen appears.
2. Click **Add Scan**. The Add Scan screen appears.
3. Select **Enable malware scan** to scan for Trojans and worms.
4. In the drop-down menu in the Malware Scan section, select **Assessment only** to limit your scan to finding Trojans and worms in memory or select **Assessment with cleanup** to both find and clean these threats.

Note: The DCS malware scan looks for Internet worms, which are Trojans and worms residing in computer memory and not in files.

---

5. Select **Enable spyware/grayware scan** to scan for spyware/grayware programs.
6. In the drop-down menu in the Spyware/Grayware Scan section, select **Assessment only** to limit your scan to finding active spyware/grayware or select **Assessment with cleanup** to both find and clean these programs.

Note: The DCS spyware/grayware scan only looks for active spyware/grayware programs.

---

7. Specify the scan mode for the spyware/grayware scan. Choose from—
   - Quick scan: Fastest scan, but only a partial scan
   - Full scan: Slower than quick scan, but a complete scan
   - Hybrid scan: Try quick scan. If it finds any spyware/grayware, switch to full scan. (For a more detailed description of these three scan types, see *Spyware/Grayware Scan Types* on page 4-6.)
8. If there are any spyware/grayware items that you would like keep, you can exclude them from scanning by selecting **Enable spyware/grayware exclusion list** and clicking the **spyware/grayware exclusion list** link or the drop-down arrow to create or manage a list of spyware programs for the scan to disregard. (See *Choosing Spyware/Grayware to Exclude from Scans* on page 4-7.)

Spyware/Grayware Scan Types

As mentioned in *Selecting Scan Action* starting on page 4-5, there are three types of spyware/grayware scans that you can choose from—

- Quick scan (Fastest scan, but only a partial scan)
- Full scan (Slower than quick scan, but a complete scan)
- Hybrid scan (Try quick scan. If it finds any spyware/grayware, switch to full scan)

This section provides details as to what DCS scans when using the various spyware/grayware scan types.

Quick Scan

This scan is the fastest of the three scan types, but it is only a partial scan.

When using quick scan mode, DCS scans the following:

- Memory
- File system
- Registry
- Cookies
- Shortcut links

Full Scan

Full scan mode offers the most complete scan, but it takes the longest time.

Tip: If your deployment scenario involves a smaller network, or if your IT security strategy places the value of completeness higher than scan speed, Trend Micro recommends using full scan mode.

In full scan mode, DCS scans all of the items listed above in Quick Scan and also scans all files on the hard disk.

For very large networks, if length of scan time is an issue, it may be preferable to use either the quick scan or hybrid scan modes.

Hybrid Scan

As summarized above and in the UI, in hybrid scan mode, DCS performs a Quick Scan first, and if that scan finds any spyware/grayware, DCS switches to full scan mode.

Scan speed in hybrid scan mode can be either fast or slow, depending on such variables as—

- How many machines you have targeted for scanning
- Whether or not DCS finds any spyware/grayware in the initial, quick scan mode

Choosing Spyware/Grayware to Exclude from Scans

Not all spyware or grayware is undesirable. For this reason DCS allows you to create a list of spyware/grayware that you would like to exclude from spyware/grayware scans. There are two kinds of spyware/grayware exception lists: scan-specific lists and a global list.

Global Spyware/Grayware Exclusion List

You can set a spyware/grayware exclusion list that every scan can use.

To create a global spyware/grayware exclusion list:

1. Access the Global Spyware/Grayware exclusion list through either of two ways:
   a. On the Add Scan screen (**Scans** > **Add/Edit Scan, Add Scan** link), click the **global spyware/grayware exclusion list** link in the Spyware/Grayware Scan section of *Step 1 of 4: Select Scan Action.*
   b. On the left-side panel, select **Scans > Global Spyware Exclusion List.**

   The Global Spyware/Grayware Exclusion List screen appears.
2. Type the name that Trend Micro uses to identify the spyware/grayware program that you wish to add (for example, ***SPYW_GATOR.C***) to the exclusion list. If you are unsure of this name, visit the Trend Micro Web site to find it:

   `www.trendmicro.com/vinfo/grayware/`
3. Click **Add>.** The spyware/grayware item appears in the Spyware/Grayware to exclude table.
4. Click **Save** to save your changes.

Scan-Specific Spyware/Grayware Exclusion List

You can also set a unique spyware/grayware exclusion list when adding or editing any scan. This scan-specific list applies only to the scan you are creating.

To create a scan-specific spyware/grayware exclusion list:

1. On the Add Scan screen (**Scans** > **Add/Edit Scan, Add Scan** link), click the exclusion list link in the Spyware/Grayware Scan section of *Step 1 of 4: Select Scan Action.* The Spyware/Grayware Exclusion List screen appears.
2. Type the name that Trend Micro uses to identify the spyware/grayware program that you wish to add (for example, ***SPYW_GATOR.C***) to the exclusion list. If you are unsure of this name, visit the Trend Micro Web site to find it:

   `www.trendmicro.com/vinfo/grayware/`

3. Click **Add>.** The spyware/grayware item appears in the Spyware/Grayware to exclude table.
4. Click **Save** to save your changes.

WARNING! *Spyware/grayware names entered into the spyware/grayware exclusion list must follow the Trend Micro naming convention. DCS ignores mistyped or nonstandard names added to the list.*

To remove a spyware/grayware item from an exclusion list:

1. Click the name of a scan in the Scan Name column of the scans table on the Add/Edit Scans screen. The Edit Scan screen appears.
2. In the Spyware/Grayware Scan section of *Step 1 of 4: Select Scan Action* click the link for the kind of list you wish to modify (**global spyware/grayware exclusion list**, link, for the global list or **exclusion list** link, for a scan-specific list).
3. In the **Spyware/Grayware to exclude** table, click the trash can icon () next to the spyware/grayware item that you wish to remove from the exclusion list.
4. Click **Save** to save your changes.

Editing a Scan

You can edit an existing scan or copy an existing scan to modify it and save it as a new scan.

To edit an existing scan:

1. Click **Scans > Add/Edit Scans** in the sidebar. The Add/Edit Scans screen appears.
2. Under the **Scan name** column, click the name of the scan you wish to edit. The Edit Scan screen appears showing the current settings for the scan.
3. Make any changes you wish, following the procedures you used when adding a new scan (see *Adding a Scan* on page 4-3).
4. Click **Save** to save your changes.

You can also use an existing scan as a basis from which to create a new scan. Follow the instructions below to copy a scan and then modify it to create a new scan.

To copy a scan for modification:

1. Select **Scans** > **Add/Edit Scans** from the sidebar. The Add/Edit Scans screen appears.
2. Select the scan or scans you wish to copy.
3. Click  **Copy.** The copy of the selected scan appears in a new row in the table. The scan names appear like the original, but appended with "**_COPY_**" and an incrementing number (for example, "**_COPY_1**").
4. Click the linked name of the copied scan that you wish to modify. The Edit Scan screen appears.
5. Edit the scan.

Selecting Scan Targets

You can select scan targets in two basic ways:

- By adding scan targets manually (click **Add/Edit Scan Target**), or
- By importing a list of scan targets (click **Import Target**)

Adding Scan Targets Manually

DCS allows you to set scan targets by IP address, IP range, network segment and subnet mask, machine name, or network domain. Selecting scan targets is the second step in a four-step process.

Select Scan Target by Machine Name

In some cases, an IT manager may wish to select scan targets by machine name or network domain.

To add one or more machines to the scan list by machine name:

1. Click **Add/Edit Scan Target.** The Select Scan Target screen appears.
2. Under **Select machines** select **By machine name.** A list of available machines appears on the left, and a list of selected machines appears on the right.

3. To add the entire list of available machines, click **Add All>>** (Add All >>). The entire list of machines appears in the Selected machines table.
4. To expand the domain or workgroup tree, double-click a domain or workgroup name. A list of all machines in the domain or workgroup appears.
5. To add a single machine or network domain, click its name and click **Add>** (Add >). That machine or domain appears in the Selected machines list.
6. To add several—but not all—machines or domains to the list, use the Microsoft Windows **Shift-mouse** or **Ctrl-mouse** conventions for multiple selection to select the machines to add, and then click **Add>** (Add >). The newly selected machines appear in the Selected machines table.
7. Click **Save** to save your changes.

Note: Alternatively, you can type the name of the machine to add in the **Computer Name** field and then click **Add>.**

To remove one or more machines from the scan list by name:

1. Under *Step 2 of 4: Select Scan Target* click **Add/Edit Scan Target.** The Select Scan Target screen appears.
2. Under **Select machines** select **By machine name.** A list of available machines appears on the left, and a list of selected machines appears on the right.
3. To remove the entire list of available machines, click **<< Remove All** (<< Remove All). The entire list of machines in the **Selected machines** table disappears.
4. To remove a single machine or network domain, click its name in the **Selected machines** list and click **<Remove** (< Remove). That machine or domain disappears from the **Selected machines** list.
5. To remove several—but not all—machines or domains from the list, use the Microsoft Windows **Shift-mouse** or **Ctrl-mouse** conventions for multiple selection to select the machines to remove, and then click **<Remove** (< Remove). The machines or domains selected for removal disappear from the **Selected machines** table.
6. Click **Save** to save your changes.

Select Scan Target by IP Address

DCS allows you to set scan targets by IP address or by IP range.

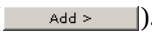
To select scan target by IP range:

1. Click **Add/Edit Scan Target.** The Select Scan Target screen appears.
2. Under **Select machines** select **By IP address.**
3. To enter an IP range, type the IP addresses in the **From** and **To** fields under the **IP range** section.
4. Click **Add>** ( **).** The new IP address range appears in the table to the right of the IP range section.
5. Click **Save** to save your change.

To select scan target by IP address:

1. Click **Add/Edit Scan Target.** The Select Scan Target screen appears.
2. Under **Select machines** select **By IP address.**
3. To enter an IP address, type it under the **IP address** section.
4. Click **Add>** ( **).** The new IP address appears in the table to the right of the IP address section.
5. Click **Save** to save your change.

To select scan target by network segment and subnet mask:

1. Click **Add/Edit Scan Target.** The Select Scan Target screen appears.
2. Under **Select machines** select **By IP address.**
3. Type a network segment in the **Segment** fields.
4. Type the subnet mask in the **Mask** fields.
5. Click **Add>** (). The new network segment/subnet mask appears in the table to the right of the IP address section.
6. Click **Save** to save your change.

To delete an IP address or range:

1. Click **Add/Edit Scan Target.** The Select Scan Target screen appears.
2. Under **Select machines** select **By IP address.**
3. In the IP Type/Identification table on the right side of the **Select machines** section, click the trash can icon () in the Delete column next to the IP range or IP address that you wish to delete. The entry disappears from the table.
4. Click **Save** to save your change.

Importing a List of Scan Targets

Trend Micro understands that most users of DCS use the product on large networks that may have a large and complex list of clients for DCS to scan (scan targets). For this reason, we have provided an option to import a list of scan targets by way of a specially formatted `.INI` file.

In the **Step 2 of 4: Select Scan Target** section of the Add Scan screen, you can choose to add or edit scan targets manually (click the **Add/Edit Scan Target** link or icon) or by importing a preformatted list of scan targets (click the **Import Target** link or icon).

Import List Sections

The DCS target import list `.INI` format has five independent sections for scan targets:

- By single IP
- By IP range
- By IP segment
- By domain name
- By host name

Each of the five sections uses the same basic syntax:

```
LIST.{key number}
```

...where "key number" represents the numerical order (starting at 1 for each section) of that list of machines, grouped by the category in which that list resides. See Table 4-2, “Scan target import list .ini file section names, target notation, and sample

entries, by grouping," on page 4-14 for `.INI` file section names, target notation, and sample entries.

Grouping	*Section name*	*Target notation*	*Sample entries*
Single IP	[IP]	{standard_IP}	[IP] LIST.1=10.1.2.3;10.112.3.4;192.128.11.1 LIST.2 = 20.4.55.32
IP range	[RANGE]	{starting_IP}-{ending_IP}	[RANGE] LIST.1 = 10.1.2.3-10.1.2.211;10.112.3.4-10.112.3.128; LIST.2 = 20.4.55.32-20.4.55.80 LIST.3 = 192.111.12.1-192.111.12.36
IP segment	[SEGMENT]	{IP}({IP_mask})	[SEGMENT] LIST.1 = 10.1.2.3(255.255.0.0);10.112.3.4(255.255.128.0) ; LIST.2 = 20.4.55.32(255.255.255.0)
Domain name	[DOMAIN]	{domain_name}	[DOMAIN] LIST.1 = MyCompany;test-domain; LIST.2 = test1;test2;test3;
Host	[HOST]	{domain_name}*\{client_name} *optional	[HOST] LIST.1 = COMPANY\pc-test;test-domain; LIST.2 = test1;test2;AAA\test3;

TABLE 4-2. Scan target import list .ini file section names, target notation, and sample entries, by grouping

Import List Format Details

For one key, you can separate target machines with a semicolon (;) as shown below:

```
LIST.1 = 10.1.2.3;10.112.3.4;192.128.11.1
```

The maximum size of the value string is 4096 bytes. If there is not room in a single numbered list item for all of the machines that you need to target, simply add another, consecutively numbered list item:

```
LIST.1 = 10.1.2.3;10.112.3.4;192.128.11.1
LIST.2 = 185.126.12.2;185.126.9.3;185.126.11.4
```

A few points to remember:

- Use of a semicolon at the end of an entry is optional; DCS will successfully import the value whether or not there is a terminal semicolon.
- Key names are not case-sensitive (List.1, list.1, and LIST.1 are all acceptable).
- List items must be added in sequential order, starting with `LIST.1`. DCS cannot import items that are not listed in sequential order.

Setting Scan Schedules

You can schedule scanning in DCS:

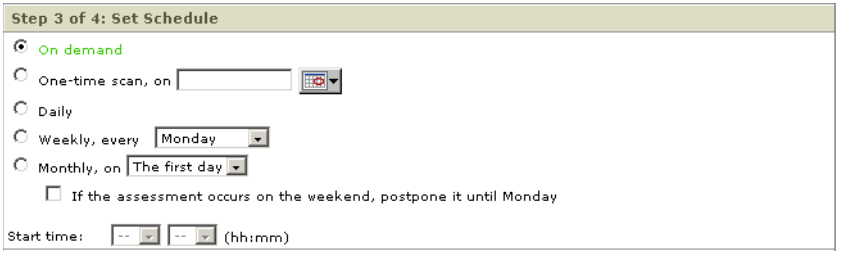


FIGURE 4-1. Setting a scanning schedule

To set scan scheduling:

1. Select **Scan > Add/Edit Scans** in the sidebar. The Add/Edit Scans screen appears.
2. Click the **Add Scan** link above the table. The Add Scan screen appears.

3. In *Step 3 of 4: Set Schedule*, choose one of the following options:
   - On demand - Allow user to scan at will
   - One-time scan - Set a single date and time for the next scan
   - Daily
   - Weekly (select day of the week)
   - Monthly (on the x day of the month)
4. If setting a monthly schedule and you wish to prevent scanning on the weekend, check **If the assessment occurs on the weekend, postpone it until Monday.**
5. Select a **Start time** (hour and minute).
6. Proceed to *Step 4 of 4: Notification*. (See *Setting Notifications of Scan Completion* on page 4-16.)

Setting Notifications of Scan Completion

Damage Cleanup Services (DCS) can send an email notification to the administrator or any other recipients after a scan is complete. You can customize the content of this notification. You can have it sent to one or to several recipients.

WARNING! *To use email notifications, first specify an email server for DCS to use. If you have not yet set up an SMTP server, please do so under the **Administration** > **Notifications** > **Settings** tab. Otherwise, DCS will not be able to send emails.*

To customize the scan results notification message:

1. Click **Scans > Add/Edit Scans** in the sidebar. The Add/Edit Scans screen appears.
2. Click the **Add Scan** link above the table. The Add Scan screen appears.
3. In *Step 4 of 4: Notification*, select **Notify administrator after the scan.**
4. Type the email address(es) of the recipient(s) in the **To** field. (Separate multiple addresses with semicolons.)
5. You can customize the subject line in the **Subject** field. (The default is *Trend Micro Damage Cleanup Services: [<%scan name%>] scan result summary.*)

6. The information in the message body can also be customized by editing the **Message** field. For details, see *Customizing Notification Messages with Variables* on page 4-22.
7. Click **Save** to save your changes.

Note: You can restore the default settings of the Message and Subject fields by clicking **Set to Default.**

Setting Administrative Notifications

With Damage Cleanup Services (DCS), you can specify which events trigger an administrative notification. You can also fine-tune the methods by which notifications go out.

Note: By default, no notifications are selected, so you must configure administrative notifications if you would like to notify anyone of DCS events.

To configure administrative notifications:

1. Click **Administration** > **Notifications**. The Notifications screen appears.
2. Follow the procedures below to—
   - Set events that trigger notifications (see *To select events to trigger notifications:* on page 4-18)
   - Select the method(s) by which each notification type goes out
   - Set the content for various notification types (see *Setting Notification Content* on page 4-18)
   - Configure the various notification methods

Setting Events to Trigger Notifications

To select events to trigger notifications:

1. Click **Administration** > **Notifications** > **Events**. The **Specify the notifications** screen appears.
2. Select any combination of the following notification types for notifications upon successful and unsuccessful completion of **Pattern update, Engine update** and **Scan process**:
   - Email
   - SNMP
   - Event Log
   - Pager
   - MSN Messenger
3. Select any combination of the five notification types listed above for notification when DCS receives an **Outbreak alert.**
4. Click **Save** to save your changes.

Setting Notification Content

To configure notification content:

1. Click **Administration** > **Notifications** > **Events.** The **Specify the notifications screen** appears.
2. Click the link identifying the notification trigger for—
   - **Pattern update**: Successful and Unsuccessful
   - **Engine update**: Successful and Unsuccessful
   - **Scan process**: Successful and Unsuccessful, or
   - **Outbreak alert**: There is only one choice: "When being activated"

   An Edit Message screen appears.

Note: For **Scan process,** "Unsuccessful" means that DCS was unable to complete the scan because of a system crash or some other unforeseen problem. If DCS completes a scan and the scan contains all unresponsive machines, the scan status is still "Successful," not "Unsuccessful," because the scan itself successfully completed.

3. The subject line of the message can be modified. The default is **Trend Micro Damage Cleanup Services: [Event type].**
4. The message body content can be modified. See *Customizing Notification Messages with Variables* on page 4-22.
5. Click **Save** to save your changes.

Note: If you wish to restore content to the defaults, click **Set to Default.**

Setting Notification Method

Setting email notifications settings only enables DCS to use your email server; it does not identify email recipients. If you want to use email notification, you must also specify email recipients when creating a scan, in *Step 4 of 4: Notification.* See *Setting Notifications of Scan Completion* on page 4-16.

To set email notifications for reports, you must specify email recipients in the Add Report Template screen. See the respective instructions for creating malware report templates (*Creating Malware Scan Report Templates* on page 6-3) and spyware/grayware report templates (*Creating Spyware/Grayware Scan Reports Templates* on page 6-7). Email settings made here will not automatically apply to notifications for scans or reports.

To configure notification methods:

1. Click **Administration** > **Notifications > Settings.** The Settings screen appears.
2. Follow the relevant procedure below to configure any of the four notification methods you would like to use with your notifications:
   - Email
   - SNMP
   - Pager
   - MSN Messenger

Configure email notification settings to set up DCS to use your email server so that DCS can send out notifications via email.

Configuring Email Notification Settings

To configure email notification settings:

1. Click **Administration** > **Notifications** > **Settings.** The Settings screen appears.
2. In the Email Setting section, type the email address(es) for one or more recipients.
3. Type the **Sender's email address.**
4. Type the **SMTP server name or IP address.**
5. Type the **Port number.** (This is the SMTP port number.)
6. Click **Save** at the bottom of the screen to save your changes.

Configuring SNMP Settings for Notifications

To configure SNMP settings:

1. Click **Administration** > **Notifications** > **Settings.** The Settings screen appears.
2. In the SNMP setting section type the **Community name.**
3. Type the **Server IP address.**
4. Click **Save** at the bottom of the screen to save your changes.

Configuring Pager Settings for Notifications

To configure pager settings:

1. Click **Administration** > **Notifications** > **Settings.** The Settings screen appears.
2. Type the **Pager COM port.**
3. Type the **Pager number** or numbers. (Separate multiple entries with semicolons.)
4. Click **Save** at the bottom of the screen to save your changes.

Configuring MSN Messenger Settings for Notifications

To configure MSN Messenger settings:

1. Click **Administration** > **Notifications** > **Settings.** The Settings screen appears.
2. In the MSN™ Messenger Setting section, type the **Sender's MSN email address.**
3. Type the sender's MSN password.
4. Type the email address(es) of one or more recipients.
5. If you use a proxy server, select **Use a proxy server** and follow the procedures set out in *To set MSN Messenger proxy server settings:* on page 4-21.
6. Click **Save** at the bottom of the screen to save your changes.

To set MSN Messenger proxy server settings:

1. Follow the procedures set out in *To configure MSN Messenger settings:* on page 4-21, to activate the fields below **Use a proxy server.**
2. Select the **Proxy type** from the drop-down menu.
3. Type the **Server name or IP address.**
4. Type the **Port number.** (This is the proxy server port number.)
5. If the proxy server requires authentication, type the proxy server user name and password.
6. Click **Save** at the bottom of the screen to save your changes.

Customizing Notification Messages with Variables

Notification messages provide valuable update, scan, and outbreak alert information to administrators. An administrator can customize these messages to suit the company's needs. The Subject and Message fields on the Edit Message screen are editable for this purpose. The administrator can type text and DCS variables into these fields. Trend Micro has provided a subset of system variables that an administrator can use for each type of notification. The tables below list for each notification type these variables and their descriptions.

Tip: Although the variables appear in the tables below in mixed case for readability purposes, they are, in fact, case-insensitive. It is not necessary to type them using the exact same capitalization style. (DCS will interpolate these variables correctly regardless of case.)

Variables for Notification of Individual Scan Completion

Variable	Description
<%Date/Time%>	Time and date of scan completion
<%Scan Name%>	Name of the scan that DCS executed. Whether the execution was successful or unsuccessful makes no difference.
<%Malware Scan Action%>	Type of malware scan performed: Assessment Only and Assessment With Cleanup
<%Spyware Scan Action%>	Type of spyware/grayware scan performed: Assessment Only and Assessment With Cleanup
<%Scan Target%>	Name of the machine group a scan acts upon
<%Machine Total%>	Total no. of machines targeted in this scan
<%Schedule%>	Scan schedule that user set
<%Scan Time%>	Time and date of a scan
<%Malware Damage%>	No. of machines with malware damage
<%Malware Cleanup Successful%>	No. of machines successfully cleaned
<%Malware Cleanup Unsuccessful%>	No. of machines that could not be cleaned
<%Malware Damage Free%>	No. of malware-free machines
<%Malware Unresponsive%>	No. of machines that DCS could not contact in a malware scan
<%Malware Total%>	Total no. of machines targeted for a malware scan
<%Spyware Damage%>	No. of machines with spyware/grayware damage
<%Spyware Cleanup Successful%>	No. of machines successfully cleaned
<%Spyware Cleanup Unsuccessful%>	No. of machines that could not be cleaned
<%Spyware Damage Free%>	No. of machines free of spyware/grayware
<%Spyware Unresponsive%>	No. of machines that DCS could not contact in a spyware/grayware scan
<%Spyware Total%>	Total no. of machines targeted for a spyware/grayware scan

TABLE 4-3. Variables available for customizing notifications of type: Individual Scan Completion

Variables for Successful Pattern Update Notification

Variable	Description
<%Date/Time%>	The time and date of an update
<%DCT Current Version Number%>	The version number of the Virus Cleanup Template in use by DCS
<%DCT Latest Version Number%>	The version number of the latest Virus Cleanup Template available for download by DCS
<%DCT Status%>	The update status of the Virus Cleanup Template in use by DCS
<%Spy Current Version Number%>	The version number of the Spyware Pattern in use by DCS
<%Spy Latest Version Number%>	The version number of the latest Spyware Pattern available for download by DCS
<%Spy Status%>	The update status of the Spyware Pattern in use by DCS

TABLE 4-4. Variables available for customizing notifications of type: Successful Pattern Update

Variables for Unsuccessful Pattern Update Notification

Variable	Description
<%Date/Time%>	The time and date of an update
<%DCT Current Version Number%>	The version number of the Virus Cleanup Template in use by DCS
<%DCT Latest Version Number%>	The version number of the latest Virus Cleanup Template available for download by DCS
<%DCT Cause%>	An error message that provides users with a description of the error that DCS encountered when attempting to update the Virus Cleanup Template, the reason for the error, and the Trend Micro recommended action to correct the error
<%DCT Status%>	The update status of the Virus Cleanup Template in use by DCS
<%Spy Current Version Number%>	The version number of the Spyware Pattern in use by DCS
<%Spy Latest Version Number%>	The version number of the latest Spyware Pattern available for download by DCS
<%Spy Status%>	The update status of the Spyware Pattern in use by DCS
<%Spy Cause%>	An error message that provides users with a description of the error that DCS encountered when attempting to update the Spyware Pattern, the reason for the error, and the Trend Micro recommended action to correct the error

TABLE 4-5. Variables available for customizing notifications of type: Unsuccessful Pattern Update

Variables for Successful Engine Update Notification

Variable‘	Description
<%Date/Time%>	The time and date of an update
<%DCE Current Version Number%>	The version number of the Virus Cleanup Engine in use by DCS
<%DCE Latest Version Number%>	The version number of the latest Virus Cleanup Engine available for download by DCS
<%DCE Status%>	The update status of the Virus Cleanup Engine in use by DCS
<%SSE Current Version Number%>	The current version number of the Spyware Scan Engine (or SSAPI)
<%SSE Latest Version Number%>	The version number of the Spyware Scan Engine available for download
<%SSE Status%>	The update status of the Spyware Scan Engine
<%ROOTKIT Current Version Number%>	The version number of the Anti-rootkit Driver in use by DCS
<%ROOTKIT Latest Version Number%>	The version number of the latest Anti-rootkit Driver available for download by DCS
<%ROOTKIT Status%>	The update status of the Anti-rootkit Driver in use by DCS

TABLE 4-6. Variables available for customizing notifications of type: Successful Engine Update

Variables for Unsuccessful Engine Update Notification

Variable‘	Description
<%Date/Time%>	The time and date of an update
<%DCE Current Version Number%>	The version number of the Virus Cleanup Engine in use by DCS
<%DCE Latest Version Number%>	The version number of the latest Virus Cleanup Engine available for download by DCS
<%DCE Status%>	The update status of the Virus Cleanup Engine in use by DCS
<%DCE Cause%>	An error message that provides users with a description of the error that the Virus Cleanup Engine encountered, the reason for the error, and the Trend Micro recommended action to correct the error
<%SSE Current Version Number%>	The current version number of the Spyware Scan Engine (or SSAPI)
<%SSE Latest Version Number%>	The version number of the Spyware Scan Engine available for download
<%SSE Status%>	The update status of the Spyware Scan Engine
<%SSE Cause%>	An error message that provides users with a description of the error that the Spyware Scan Engine encountered, the reason for the error, and the Trend Micro recommended action to correct the error
<%ROOTKIT Current Version Number%>	The version number of the Anti-rootkit Driver in use by DCS
<%ROOTKIT Latest Version Number%>	The version number of the latest Anti-rootkit Driver available for download by DCS
<%ROOTKIT Status%>	The update status of the Anti-rootkit Driver in use by DCS
<%ROOTKIT Cause%>	An error message that provides users with a description of the error that the Anti-rootkit Driver encountered, the reason for the error, and the Trend Micro recommended action to correct the error

TABLE 4-7. Variables available for customizing notifications of type: Unsuccessful Engine Update

Variables for Successful Scan Completion, Global Notification

Variable	Description
<%Scan Name%>	The name of the scan that DCS executed. Whether the execution was successful or unsuccessful makes no difference.
<%Date/Time%>	The time and date of a scan
<%Malware Scan Action%>	The type of malware scan performed. Types include: Assessment Only and Assessment With Cleanup
<%Spyware Scan Action%>	The type of spyware/grayware scan performed. Types include Assessment Only and Assessment With Cleanup
<%Scan Target%>	The name of the machine group a scan acts upon
<%Machine Total%>	Total number of machines targeted in this scan
<%Schedule%>	The scan schedule the user sets in the Set Schedule screen

TABLE 4-8. Variables available for customizing notifications of type: Successful Scan Completion, Global

Variables for Unsuccessful Scan Completion Global Notification

Variable	Description
<%Scan Name%>	The name of the scan that DCS executed. Whether the execution was successful or unsuccessful makes no difference.
<%Date/Time%>	The time and date of a scan
<%Malware Scan Action%>	The type of malware scan performed. Types include: Assessment Only and Assessment With Cleanup
<%Spyware Scan Action%>	The type of spyware/grayware scan performed. Types include Assessment Only and Assessment With Cleanup
<%Scan Target%>	The name of the machine group a scan acts upon
<%Machine Total%>	Total number of machines targeted in this scan
<%Schedule%>	The scan schedule the user sets in the Set Schedule screen
<%Cause%>	An error message that provides users with a description of the error that DCS encountered when attempting to complete a scan, the reason for the error, and the Trend Micro recommended action to correct the error

TABLE 4-9. Variables available for customizing notifications of type: Unsuccessful Scan Completion, Global

Click **Set to Default** to reset the notification message to the default message provided with DCS upon installation.

Variables for Notification that an Outbreak Alert Has Been Activated

Variable	Description
<%Date/Time%>	The date and time at which the outbreak policy was activated.
<%Virus Name%>	The name of the virus related to the outbreak.
<%Threat Information%>	Detailed information about the outbreak.

TABLE 4-10. Variables available for customizing notifications of type: Outbreak Alert Has Been Activated

Keeping Damage Cleanup Services Up to Date

Virus writers and makers of spyware/grayware are constantly inventing new ways to compromise your systems. For this reason, it is essential to keep your installation of Damage Cleanup Services (DCS) up to date with the very latest pattern files so that DCS can always be aware of the very latest threats and potential threats. Follow the guidelines in this section to ensure that DCS is always protecting your network from the very latest malware and spyware/grayware.

Things To Consider When Setting an Update Schedule

As of the time of this release of DCS 3.2, Trend Micro, Inc. is updating the Virus Cleanup Template about once a week.

If you are using DCS 3.2 with Cisco Incident Control Server or with Trend Micro Control Manager version 3.x, DCS is taking advantage of Trend Micro Outbreak Prevention Services, which supplies automatic updates when there is an Internet threat outbreak. Therefore, it is not necessary for networks using these products with DCS 3.2 to set scheduled updates more than once a week.

Note: DCS 3.2 can act as a stand-alone product or as a component of Trend Micro Control Manager 3.x.

Configuring Scheduled Updates for Damage Cleanup Services

Configure DCS to regularly check the update server and automatically download any available updates. Using scheduled updates is an easy and effective way to ensure that your protection against viruses and other Internet threats is always current.

To configure automatic updates:

1. On the sidebar, click **Updates** > **Scheduled**. The Scheduled Update screen appears.
2. Select **Enable scheduled update**.
3. In the Component box, select the components that you wish to update.
   Component

- Virus Cleanup Template and Spyware Pattern
- Virus Cleanup Engine and Spyware Scan Engine
- Anti-rootkit Driver

4. Under Update Schedule, specify how often to perform scheduled updates. First, choose the unit of time to base your schedule on and then select a frequency.
5. Select the **Start time** for your scheduled updates. The update begins according to your schedule at the **Start time** that you set. See Table 4-11, "Description of frequency options for scheduled updates," on page 4-31 for a description of the available options.

Option	Frequency	Description
Minutes, every:	Every *X* minutes	Runs within the minute you specify, at the start time
Hours, every:	Every *X* hours	Runs within the hour you specify, at the start time
Days, every:	Every *X* days	Runs within the day you specify, at the start time
Weekly, every:	Once a week, on *X*day	Runs weekly, on the day you specify, at the start time

TABLE 4-11. Description of frequency options for scheduled updates

6. Under Download Source, select the location from which you want to download the update. Select the **Trend Micro ActiveUpdate server**, **Other update source** (and type in the source's URL) or an **Intranet location containing a copy of the current file**.
7. If you have chosen an Intranet location, type in the **UNC path,** including domain name or machine name, and a user name and password if necessary.

Note: The UNC path must include the domain name or machine name as the root of the path, for example, "`\\machine-name\<share_folder>.`" Input format for user name is "`machine-name\<account>`" (if specifying a machine account) or "`domain-name\<domain_account>`" (if specifying a domain account).

8. Click **Save** to save your settings.

Updating Damage Cleanup Services Manually

There are five components of DCS that an IT manager will want to update:

- Virus Cleanup Template
- Spyware Pattern
- Virus Cleanup Engine
- Spyware Scan Engine
- Anti-rootkit Driver

An IT manager may wish to update these components immediately after installing DCS, to ensure that DCS is making use of the latest components. Although you can configure a variety of update schedules, DCS also allows you to update manually.

To update DCS manually:

1. On the sidebar, click **Updates** > **Manual Update.** The Manual Update screen appears, showing your current components, their version numbers, and the most recent update status.
2. Under **Download Source**, choose whether to receive updates from the **Trend Micro ActiveUpdate server**, from another Internet source (**Other update source)**, or from an **Intranet location containing a copy of the current file**. If you have selected **Other update source**, type the source URL. If you have selected **Intranet location containing a copy of the current file**, type the UNC path and, if necessary, a **User name** and **Password**.

FIGURE 4-2. Selecting a download source for Trend Micro ActiveUpdate server

3. Click **Save.**
4. Click **Update Now** in the Action column of the components that you wish to update. The server checks the update server for updated components. If there are available updates, the server updates the components.

To check if you have specified a download schedule, click **Updates** > **Scheduled** on the sidebar.

Chapter 5

Scanning and Cleanup

This chapter contains the following topics:

Scanning Manually

Damage Cleanup Services (DCS) can run one or several scans whenever you choose to run them.

To run a scan manually:

1. Click **Scans** > **Add/Edit Scans** in the sidebar. The Add/Edit Scans screen appears.
2. Select the scan that you wish to run.
3. Click **Run Now** ( ). The Current Running Scan screen appears, showing scan details and progress of the scan. (See Figure 5-2, "Current Running Scan screen, Scan Status table detail showing the scan progress bar," on page 5-4).
4. To stop the scan after it has begun, click **Stop the Scan.**

The second-to-last column of the table on the Add/Edit Scans screen shows the enabled or disabled status of the scan.

Note: The screen refreshes automatically every 30 seconds. Click the **Refresh** link near the top of the Summary screen to allow DCS to retrieve and display the very latest data for this screen.

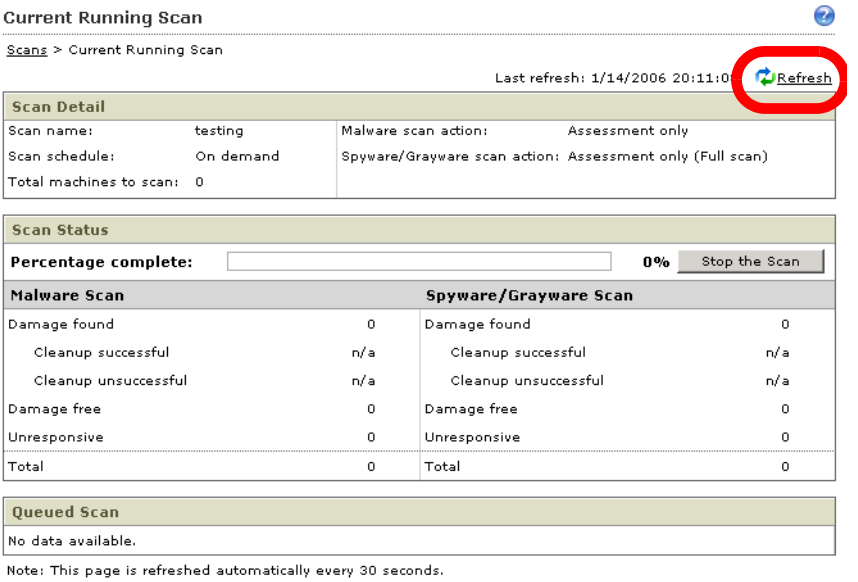


FIGURE 5-1. The Current Running Scan screen showing the DCS Refresh link

To run two or more scans manually:

1. Click **Scans > Add/Edit Scans** in the sidebar. The Add/Edit Scans screen appears.
2. Select the scans that you wish to run. To select all scans listed, select the checkbox in the table header row (to the left of Scan Name).
3. Click **Run Now** ( ). DCS runs the first scan and queues the remaining scans. The Current Running Scan screen appears, showing scan details, progress of the scan, and a list of any scans in the queue.
4. To stop a scan after it has begun, click **Stop the Scan.**

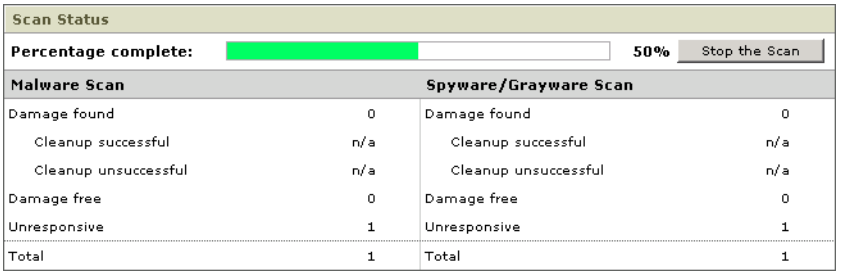


FIGURE 5-2. Current Running Scan screen, Scan Status table detail showing the scan progress bar

Note: DCS cannot run more than one scan simultaneously. If two or more scheduled scans have the same start time, DCS begins one scan and places the rest in a queue.

By default, DCS enables scans upon creation.

Viewing the Scan Results Summary

When you open the DCS management console, the Summary screen appears. The bottom half of the screen displays a table showing scan results.

To enable a disabled scan:

1. Click **Scans** in the sidebar. The Scans screen appears.
2. Click the red X icon in the second-to-last (Status) column. The screen refreshes and displays a green checkmark icon in the column, indicating that the scan is now enabled.

To disable an enabled scan:

1. Click **Scans** in the sidebar. The Scans screen appears.
2. Click the green checkmark icon in the second-to-last (Status) column. The screen refreshes and displays a red X icon in the column, indicating that the scan is now disabled.

To view scan results:

1. Click **Summary** in the sidebar. The Summary screen appears.
2. Click the tab for the type of scan results desired (**Scan Results for Malware** or **Scan Results for Spyware/Grayware)**. On either tab, you can view the following details for scan results for malware or spyware/grayware (there is a separate tab for each):

   Scan Name: The descriptive name of the scan

   Completion Date/Time: Date and time last scan was completed. Shows percent complete if scan is in progress.

   Malware Scan Action: Description of what action was taken after the last scan

   Damage Found: For scans done in Assessment Only mode, shows the number of machines on which the scan found damage; otherwise, shows **n/a**

   Cleanup Successful: For scans done in Assessment with Cleanup mode, shows the number of machines the scan successfully cleaned; otherwise, shows **n/a**

   Cleanup Unsuccessful: For scans done in Assessment with Cleanup mode, shows the number of machines that the scan could not clean; otherwise, shows **n/a**

   Damage Free: The number of client machines that were found to be free of damage

   Unresponsive: The number of client machines that did not respond to the DCS server

   Total: The total number of client machines that DCS attempted to deploy to.

Viewing Scan Results Details

DCS provides several different ways to access details about a malware or spyware/grayware scan.

Summary View

From the Scan Results for Malware (Spyware/Grayware) tabs in the Summary screen:

- By clicking on a pending scan in the Completion Date/Time column

- By clicking on a completed scan in the Completion Date/Time column
- By clicking on the number in any of these columns:
  - Damage Found
  - Cleanup Successful
  - Cleanup Unsuccessful
  - Damage Free
  - Unresponsive
  - Total

While a Scan Is Running

You can view scan details while a scan is running if the scan was done manually:

1. In the sidebar, click **Scans.** The Add/Edit Scans screen appears
2. Select a scan from the list and click **Run Now** ( ). The Current Running Scan screen appears, showing three tables:
   - Scan Detail
   - Scan Status
   - Queued Scan

After a Scan Is Finished

The Add/Edit Scans screen displays different information about a completed scan once the scan is finished. The sections below explain this information in detail.

The Scan Detail Table

This table displays if the selected scan is complete. It shows the following information:

Scan name: The scan name that the administrator entered when creating the scan

Completion time: Date, hour, and minute that the scan completed

Total scan time: The time it took for the scan to run, in hours and minutes

Malware scan action: "Assessment only" or "Assessment with cleanup" (only appears if the scan included malware assessment)

Spyware/grayware scan action: "Assessment only" or "Assessment with cleanup" (only appears if the scan included spyware/grayware assessment)

Scan schedule: The frequency of scheduled scans (if set), including start time

The Scan Result for Malware (Spyware/Grayware) Table

This table displays when you click on a number in any of these columns in the Scan Results for Malware (Spyware/Grayware) table on the Summary screen:

Damage Found: For scans done in Assessment Only mode, shows the number of machines on which the scan found damage; otherwise, shows **n/a**

Cleanup Successful: For scans done in Assessment with Cleanup mode, shows the number of machines the scan successfully cleaned; otherwise, shows **n/a**

Cleanup Unsuccessful: For scans done in Assessment with Cleanup mode, shows the number of machines that the scan could not clean; otherwise, shows **n/a**

Damage Free: The number of machines that the scan found to be free of any damage

Unresponsive: The number of machines that DCS could not scan

Total: The total number of machines targeted for scanning

This table shows a list of computers falling into one of the above categories. The table shows the following information about each computer:

Machine Name: The name of the computer

IP Address: The computer's IP address

MAC Address: The computer's MAC address

Scan Result: (displays the name(s) of any malware or spyware/grayware found or, if scan did not find any, displays *Damage free*.)

Malware (Spyware/Grayware) Detected: The Trend Micro name for the specific malware or spyware/grayware program found (displays *n/a* if the machine status is *Unresponsive*)

You can use this screen to manually clean any machine found with damage if its Scan Result status is *damage found* or *cleanup unsuccessful*.

Note: In the Scan Result for Malware screen, any scan that you clean with the **Clean Up Now** feature will clean only malware. Likewise, in the Scan Result for

Spyware/Grayware screen, any scan that you clean with the **Clean Up Now** feature will clean only spyware/grayware.

To manually clean a Damage Found or Cleanup Unsuccessful machine:

1. Select the machine or machines that you would like to manually clean.
2. Click **Clean Up Now.** Damage Cleanup Services runs a manual scan on the selected machines.

Note: **Clean Up Now** cannot clean machines whose status is *unresponsive.*

Results for Pending Scans

The Scan Status Table

This table displays if a scan is still running. It shows the same basic information as the Scan Results for Malware (Spyware/Grayware) table on the Summary screen does, except that it also displays Percentage complete (the completion status of a scan, in percent), which includes a Stop the Scan button.

The Queued Scan Table

This table displays when more than one scan is set to run. It shows the following information:

Scan Name: The scan name that the administrator typed when creating the scan

Malware Scan: "Assessment only" or "Assessment with cleanup"

Spyware/grayware Scan: "Assessment only" or "Assessment with cleanup"

Viewing Scan Results by Machine

You can get detailed scan results information about an individual machine for completed scans if the scanned status of that machine is **Damage Found, Cleanup successful, Cleanup unsuccessful, Damage-Free,** or **Unresponsive.**

To display scan result details for an individual machine:

1. Click **Summary** in the sidebar. The Summary screen appears.
2. Click the linked **Completion Date/Time** in the Scan Results for Malware (Spyware/Grayware) table. The Scan Result for Malware (Spyware/Grayware) screen appears.

   Note: You can sort data in this table by any column whose head displays as linked text. To sort, click the linked column head.

3. In the Machine Name column of the Scan Result for Malware (Spyware/Grayware) table, click the linked name of the machine you wish to get more detailed information about. The Scan Result for <$Machine Name> screen appears, showing the following data:
   - Machine name
   - IP address
   - MAC address
   - Scan Result
   - Task Tracking information: Shows a list of messages as to what actions the scan took, for example, `Successfully deleted the following process [winconfig.exe]`

Using the Manual Damage Cleanup Tool

The Manual Damage Cleanup tool allows users of individual client machines to perform a cleanup task on a Microsoft Windows-based machine upon demand. Users can assess and cleanup their machine(s) without the system administrator's intervention. This ability could be useful if Damage Cleanup Services cannot access a machine because of network problems or because a machine is running an unsupported operating system (for example, Windows 95/98 or other operating systems that don't support remote login).

You can run the Manual Damage Cleanup tool from a client machine running the following Microsoft Windows platforms:

- Windows 2000 Professional/Server/Advanced Server with Service Pack 3
- Windows XP Home/Professional
- Windows 2003 Server Standard/Enterprise Edition
- Windows Server 2003 R2 (Standard or Enterprise Edition)

To give a user access to the Manual Damage Cleanup Tool, supply the user with this URL:

```
<Your_DCS_Web_host>/DCS/cgiDCSX.exe
```

FIGURE 5-3. The Manual Damage Cleanup Tool screen

To use the Manual Damage Cleanup tool:

1. Click **Start Damage Cleanup** to run a cleanup task on the local machine. The cleanup progress status bar appears displaying the name of the target machine and the status of the cleanup task.
2. If you wish to interrupt the task, click **Stop.**

When the cleanup task is complete, you can view the result under Damage Cleanup Result. If Damage Cleanup Services finds any damage, it displays the type of malware or spyware/grayware.

Note: The security settings in your browser must be set to medium for Internet and Medium-low for local intranet (the default settings for Internet Explorer 6) to allow ActiveX controls to download.

To customize Internet Explorer 6 security settings to allow ActiveX controls:

1. Click **Tools** > **Internet Options** > **Security.**
2. Click **Local intranet** and set the security level to **Medium-low.**
3. Click **Internet** and set the security level to **Medium.**
4. For both zones do the following:
   - Click **Custom Level.**
   - Under *Initialize and script ActiveX controls not marked as safe,* select **Enable** or **Prompt.**
5. Click **Apply.**
6. Click **OK.**

Chapter 6

Logs and Reports

This chapter contains the following topics:

Setting the Number of Logs to Keep

To keep the size of your logs from occupying too much space on your hard disk, you can configure Damage Cleanup Services (DCS) to limit the number of recent logs to save.

To perform log maintenance:

1. On the sidebar, click **Logs** > **Maintenance.** The Log Maintenance screen appears.
2. Under Malware Scan Logs, select **Maximum number of days to keep** and, in the accompanying field, specify the number of days to keep malware scan logs. The default value is 90 days.
3. Under Spyware/Grayware Scan Logs, select **Maximum number of days to keep** and, in the accompanying field, specify the number of days to keep spyware/grayware scan logs. The default value is 90 days.
4. Click **Save** to save your changes.

Setting the Number of Reports to Keep

To keep the size of your reports from occupying too much space on your hard disk, you can configure DCS to limit the number of recent reports to save. You can set DCS to purge reports based on a set maximum number of reports, on how long ago the reports were generated, or on a combination of the two (in which case, DCS would purge the specified older reports when either condition is met).

To perform report maintenance:

1. On the sidebar, click **Reports** > **Maintenance.** The Report Maintenance screen appears.
2. Select the **Enable malware scan report purge** check box to set conditions for purging older malware scan reports. The fields in that section become active.
3. Accept the defaults or type the maximum number of days and maximum number of reports in the **Keep no more than** and the **Delete reports older than** fields, respectively. The default values are 500 reports and 90 days.

4. For spyware/grayware reports, follow steps 2 and 3 above but select the **Enable spyware/grayware scan report purge** check box instead.
5. Click **Save** to save your changes. DCS will purge reports based on the conditions you have set.

Managing Malware Scan Reports

You can use DCS to generate different kinds of reports. DCS allows you to create, edit, and delete report templates and to delete, view, and download the reports that these templates generate.

Follow the guidelines below for using report templates and reports:

Malware Report Templates

- *Creating Malware Scan Report Templates* on page 6-3
- *Deleting Malware Scan Report Templates* on page 6-5
- *Enabling and Disabling Malware Scan Report Templates* on page 6-5

Malware Reports

See *Viewing or Downloading Malware Scan Reports* on page 6-6

Note: You can edit an existing report template at any time by clicking the name of the report template (first column) on the Malware Scan Reports screen.

Creating Malware Scan Report Templates

In order to create a Malware Scan Report template, first specify the report type and then the report details. DCS generates reports in Adobe PDF format (`*.PDF`).

To specify a malware report type:

1. Click **Reports** > **Malware Scan Reports.** The Malware Scan Reports screen appears.
2. Click **Add Report Template.** The Add Malware Scan Report screen appears.
3. Type the **Report template name.**

4. Under *Step 1 of 2: Report Type*, select a scan name from the drop-down menu.

Note: If you want to create a report for a scan run using the Manual Damage Cleanup Tool, select **Manual Cleanup Tool scans** from the list. Manual scan reports produce only a **Technical Report** type. Selecting **Manual Cleanup Tool scans** disables the **Executive summary, One-time report** and **Scheduled report** options, including the **Select a scan date** drop-down list.

Manual Cleanup Tool scan reports are consolidated reports that use as their time basis the 30 days prior to the date you generate the report.

---

5. Choose **One-time report** or **Scheduled report.** DCS can generate one-time or scheduled reports for any scan that has run at least once. DCS generates scheduled reports after completing the selected scan.
6. If you have selected **One-time report**, select a scan date from the drop-down menu.

Note: DCS does not save your changes until you click **Save** at the bottom of the screen.

To specify malware report details:

1. Under *Step 2 of 2: Report Details*, select **Executive summary, Technical report,** or both (which is the default).
2. In the Recipients section, type all the email addresses of the people (up to 100 recipients) to whom you want to send the report when it generates. (Separate multiple entries with semicolons.)
3. Click **Add>.** The additional recipients appear in the field on the right.
4. To delete one or more recipients, highlight their email address(es) in the right-side text area field and then click **Delete.** The selected names disappear from the list.
5. Click **Save** to save your changes. The Malware Scan Reports screen appears with the newly created template listed.

Note: You can edit an existing report template at any time by clicking the name of the report template (first column) on the **Malware Scan Reports** screen.

Deleting Malware Scan Report Templates

To delete a malware scan report template:

1. Click **Reports** > **Malware Scan Reports.** The Malware Scan Reports screen appears.
2. Select the report template or templates that you wish to delete.
3. Click **Delete**. DCS deletes the selected report template and all of its associated reports.
4. To delete all malware scan report templates, select the check box in the gray header row, next to the column head, "Template Name," and then click **Delete.**

Enabling and Disabling Malware Scan Report Templates

By default, DCS enables malware scan report templates upon creation. For scheduled reports, you can use the DCS management console to disable a malware scan report template or to enable one that has been disabled.

To disable a malware scan report template:

1. Click **Reports** > **Malware Scan Reports.** The Malware Scan Reports screen appears.
2. Click the green check mark icon in the last (Status) column in the row of the report template you wish to disable. The screen refreshes and a red X icon appears where the check mark icon was, indicating that the template has been disabled.

To enable a disabled malware scan report template:

1. Click **Reports** > **Malware Scan Reports.** The Malware Scan Reports screen appears.
2. Click the red X icon in the last (Status) column in the row of the report you wish to enable. The screen refreshes and a green check mark icon appears where the red X icon was, indicating that the report has been enabled.

Note: Only scheduled reports have the enable/disable function. One-time reports display "n/a" in the status column.

Viewing or Downloading Malware Scan Reports

To view or download malware scan reports:

1. Click **Reports** > **Malware Scan Reports.** The Malware Scan Reports screen appears. A table displays the following malware scan report information:
   - Template name
   - Scan selected
   - Report frequency
   - Date the report was last generated
   - Status
2. Click **View** in the **Report List** column in the row of the kind of report (that is, "report template") you wish to view. The **Report List for** screen appears, listing reports for that template.
3. To download an individual report, click the linked report name (for example, 1/1/2006 22:32:57) in the **Report Generated On** column. A download window opens.

Adobe Acrobat reports are named in the following pattern:

```
{Scan type}_{report type}_{report template}_yyyy-mm-dd-hh-mm-ss.pdf
```

For example—

```
Malware_executive_production_machines_2006-01-14-22-32-57.pdf
```

Note: Although DCS generates reports only in Adobe Acrobat `.PDF` format, if DCS generates reports of two types at the same time, it compresses them for download, and so the downloaded file will have a `.ZIP` extension.

Managing Spyware/Grayware Scan Reports

You can use Damage Cleanup Services (DCS) to generate different kinds of reports. DCS allows you to create, edit, and delete report templates and to delete, view, and download the reports that these templates generate.

Follow the guidelines below for using report templates and reports:

Spyware/Grayware Report Templates

- *Creating Spyware/Grayware Scan Reports Templates* on page 6-7
- *Deleting Spyware/Grayware Scan Report Templates* on page 6-9
- *Enabling and Disabling Spyware/Grayware Scan Report Templates* on page 6-9

Spyware/Grayware Reports

See *Viewing or Downloading Spyware/Grayware Scan Reports* on page 6-10

Note: You can edit an existing report template at any time by clicking the name of the report template (first column) on the Spyware Scan Reports screen.

Creating Spyware/Grayware Scan Reports Templates

In order to create a Spyware/Grayware Scan Report template, specify the report type and then the report details. DCS generates reports in Adobe PDF format (*.PDF).

To specify a spyware/grayware report type:

1. Click **Reports** > **Spyware/Grayware Scan Reports** in the submenu. The Spyware/Grayware Scan Reports screen appears.
2. Click **Add Report Template.** The Add Report Template screen appears.

3. Type the **Report template name.**
4. Under *Step 1 of 2: Report Type*, select a scan name from the drop-down menu.

Note: If you want to create a report for a scan run using the Manual Damage Cleanup Tool, select **Manual Cleanup Tool scans** from the list. Manual Cleanup Tool scan reports produce only a **Technical Report** type. Selecting **Manual Scan** disables the **Executive summary, One-time report** and **Scheduled report** options, including the **Select a scan date** drop-down list.

Manual Cleanup Tool scan reports are consolidated reports that use as their time basis the 30 days prior to the date you generate the report.

---

5. Choose **One-time report** or **Scheduled report.** DCS can generate one-time or scheduled reports for any scan that has run at least once. DCS generates scheduled reports after completing the selected scan.
6. If you have selected **One-time report,** select a scan date from the drop-down menu.

Note: DCS does not save your changes until you click **Save** at the bottom of the screen.

To specify spyware/grayware report details:

1. Under *Step 2 of 2: Report Details*, select **Executive summary, Technical report,** or both (which is the default setting).
2. In the Recipients section, type all the email addresses of the people (up to 100 recipients) to whom you want to send the report when it generates.(Separate multiple entries with semicolons.)
3. Click **Add>.** The additional recipients appear in the field on the right.
4. To delete one or more recipients, highlight their email address(es) in the right-side text area field and then click **Delete.** The selected names disappear from the list.
5. Click **Save** to save your changes. The Spyware/Grayware Scan Reports screen appears with the newly created template listed.

Note: You can edit an existing report template at any time by clicking the name of the report template (first column) on the **Spyware/Grayware Scan Reports** screen.

Deleting Spyware/Grayware Scan Report Templates

To delete a spyware/grayware scan report template:

1. Click **Reports** > **Spyware/Grayware Scan Reports.** The Spyware/Grayware Scan Reports screen appears.
2. Select the report template(s) you wish to delete.
3. Click **Delete.** Damage Cleanup Services deletes the selected report template and all of its associated reports.
4. To delete all spyware/grayware report templates, select the check box in the gray header row, next to the column head, "Template Name," and then click **Delete.**

Enabling and Disabling Spyware/Grayware Scan Report Templates

By default, DCS enables spyware/grayware scan report templates upon creation. For scheduled reports you can use the DCS management console to disable a spyware/grayware scan report template or to enable one that has been disabled.

To disable a spyware/grayware scan report template:

1. Click **Reports** > **Spyware/Grayware Scan Reports.** The Spyware/Grayware Scan Reports screen appears.
2. Click the green check mark icon in the last (Status) column in the row of the report you wish to disable. The screen refreshes and a red X icon appears where the check mark icon was, indicating that the report has been disabled.

To enable a disabled spyware/grayware scan report template:

1. Click **Reports** > **Spyware/Grayware Scan Reports.** The Spyware/Grayware Scan Reports screen appears.
2. Click the red X icon in the last (Status) column in the row of the report you wish to enable. The screen refreshes and a green check mark icon appears where the red X icon was, indicating that the report has been enabled.

Note: Only scheduled reports have the enable/disable function. One-time reports display "n/a" in the status column.

Viewing or Downloading Spyware/Grayware Scan Reports

To view or download spyware/grayware scan reports:

1. Click **Reports** > **Spyware/Grayware Scan Reports** in the submenu. The Spyware/Grayware Scan Reports screen appears. A table displays the following spyware/grayware scan report information:
   - Template name
   - Scan selected
   - Report frequency
   - Date the report was last generated
   - Status
2. Click **View** in the **Report List** column in the row of the kind of report (that is, "report template") you wish to view. The **Report List for** screen appears, listing reports for that template.
3. To download an individual report, click the linked report name (for example, 1/1/2006 22:32:57) in the **Report Generated On** column. A download window opens.

Adobe Acrobat reports are named in the following pattern:

```
{Scan type}_{report type}_{report template}_yyyy-mm-dd-hh-mm-ss.pdf
```

For example—

```
Spyware_executive_production_machines_2006-01-14-22-32-57.pdf
```

Note: Although DCS generates reports only in Adobe Acrobat `.PDF` format, if DCS generates reports of two types at the same time, it compresses them for download, and so the downloaded file will have a `.ZIP` extension.

Generating or Deleting a Report Manually

IT managers can use DCS to generate many different kinds of reports. In addition to setting scheduled reports, you can also generate or delete a report manually.

Manually Generating a Scan Report

The steps for generating a malware scan report or a spyware/grayware scan report are virtually identical.

To generate a malware or spyware/grayware scan report:

1. Click **Reports** > **Malware Scan Reports** (or **Spyware/Grayware Scan Reports**). The Malware (Spyware/Grayware) Scan Reports screen appears.
2. In the Report List (second-to-last) column, click **View** in the row of the report template you wish to generate. The **Report List for <your template name>** screen appears.
3. Click **Generate Report,** above the table. The **Generate Report for <your template name>** screen appears.
4. The **Select a scan date** drop-down menu contains a list of past scans, showing date and time run. Select the scan that you want a report for.
5. In the Recipients section type one or more email addresses for those to whom you want to send the report. Click **Add>.** The new email addresses appear in the email address list.
6. If you wish to delete an email address, select it in the email list box to the right of the **Add>** button and click **Delete.** The selected email address disappears from the list.
7. Click **Generate** to generate your report.

Note: You can sort the data by any hyperlinked column head by clicking on the link.

Manually Deleting Scan Reports

You can also manually delete one or more generated malware or spyware/grayware scan reports. To set up DCS to purge older reports automatically, see *Setting the Number of Reports to Keep* on page 6-2. To delete individual reports manually, follow the procedure below. The steps for both malware and spyware/grayware are identical. In the procedure below, replace {report_type} with *spyware/grayware* or *malware* as needed.

To delete one or more generated reports manually:

1. On the left-side panel, click Malware Scan (Spyware/Grayware) Reports. The Malware (Spyware/Grayware) Scan Reports screen appears, showing a list of all existing generated {report_type} scan reports.
2. In the **Report list** column, click the View link. The Report List for {report_type} screen appears, listing all of the {report_type} reports that have not been purged.
3. Select the check box next each of the individual report to delete. You can select all of the reports on the screen by selecting the check box in the gray header row (next to the Report Generated on link).
4. Click the trash can icon () or the Delete link next to the Generate Report link just above the table. A confirmation screen appears.
5. Click **OK** to delete the selected reports.

Analyzing Your Protection Using Logs

DCS keeps comprehensive logs about virus incidents and events. Use these logs to assess your organization's virus protection policies and to identify devices that are at a higher risk of infection. This section discusses the logs that you can query from the DCS Web management console. (For information on logs to check for the device-server connection and to verify that updates deployed successfully, see *Working with Debug Logs* on page A-11.)

Querying Logs

Whether running a log query for malware or for spyware/grayware, the process is virtually identical.

To run a simple log query:

1. In the sidebar click **Logs** > **Spyware/Grayware** or **Logs** > **Malware** to choose the kind of log you wish to query. A Log Query Criteria screen appears.
2. Next to **Log format,** select **View details** or **View summary data.**
3. Select the scan name (or **All DCS Web console scans**) from the **Scan name** drop-down menu.

Note: In the **View details** view the **Scan name** drop-down menu may include up to two entries that do not represent scans run by DCS.

The **Scans from other programs** option targets the query to results from scans run by Cisco Incident Control Server, Trend Micro InterScan Web Security Suite or Trend Micro InterScan Web Security Appliance if these programs are registered with DCS.

The **Manual Cleanup Tool scans** option targets scan results generated from clients' use of the Manual Damage Cleanup Tool.

---

4. Select a date range for the scans to query as follows:
   *For **View details** format:*
   Select beginning and end dates from the **From** and **To** fields by clicking on the calendar icon next to each field () and the individual date. The date you clicked appears in the respective From or To field in the correct format.

   *For **View summary data** format:*
   By default, the date and time of the most recent scan appear in the **From** and **To** fields of Scan dates. Accept the defaults or select beginning and ending dates from the drop-down menu of the **From** and **To** fields.
5. Select the number of logs per page that you wish to display.
6. Click **Search.** A Query Result table appears.

Note: To export your query results to a .CSV file, click the **Export to CSV** link.

To run an advanced log query:

1. Follow the steps listed above in the procedure for running a simple log query to choose the kind of log to query, log format, scan name, and scan dates.
2. Click the **More Searching Criteria** link. Additional detailed input fields appear.
3. Refine your search by selecting any combination of the following:
   - Scan result
     - Damage found
     - Damage free
     - Unresponsive
     - Cleanup successful
     - Cleanup unsuccessful
   - Machine name
   - IP address (or range)
   - MAC address
   - Malware (Spyware/Grayware) name
4. Select the number of logs per page that you wish to display.
5. Click **Search.** A Query Result table appears.

Exporting Log Query Results

You can export the data shown in any completed scan results table into comma-separated-values (.CSV) format for importing into any number of database or spreadsheet programs.

To export table data:

1. In the sidebar click **Logs** > **Spyware/Grayware** or **Logs** > **Malware**. The Log Query Criteria screen appears.
2. Run your specified query as instructed in the above procedures. The Query Result table appears.
3. Click  **Export to CSV** at the top of the Query Result table. DCS generates a .CSV file for you to download.

Appendix A

Troubleshooting and Technical Support

Troubleshooting

Scan Failure

If a scan could not find a targeted client machine and the cause is not readily apparent, you may be able to identify the problem by performing the following actions:

1. Ping the client machine's IP address and machine name to determine the connection status between the DCS server and client machine.

   Command: `Ping [Client IP Address or Machine Name]`

   If the DCS server cannot connect to the machine, it cannot scan the machine. Fix the network problem and then try scanning again.

2. Verify if there are firewall applications on the client or DCS server machines.

   a. If there is a firewall application on the client machine and it is enabled, the firewall may block the scan task and cause scanning to fail.

   b. If there is a firewall application on the DCS server machine and it is enabled, the firewall may block the scan result that the client machine is sending to the server.

Check and open TCP ports 139 and 445 and UDP ports 137 and 138 or enable *File and Printer sharing* in the exception list in Windows Firewall. DCS makes use of these ports to communicate with clients.

3. Use the `nbtstat` command to resolve the client machine name using its IP address.

Command: `nbtstat -A [Client IP Address]`

If the command cannot resolve the client machine name, make sure that:

a. NetBIOS over TCP/IP protocol on the client and DCS server machines is enabled.

DCS makes use of the NetBIOS protocol to resolve the machine names. If the NetBIOS protocol is disabled on the server side, the server cannot enumerate any client machines. If NetBIOS is disabled on the client side, then the client will not be enumerated and will not appear in the scan result.

Aside from enabling NetBIOS over TCP/IP protocol, you can also place an `ini` file named `ExtraMachineDomainList.ini` into the DCS root folder to specify the domain of particular machines by IP address or IP range. DCS will use the domain account type in the Account Management Tool to access those machines and scan them automatically. The format of `ExtraMachineDomainList.ini` is as follows:

[DomainName1]	The domain name of the IP address or IP range under this section.
IP=10.1.1.1	IP address that is specified to the domain.
IP=10.2.2.2	Another IP address that is specified to the domain.
IPRANGE=10.1.1.1-10.1.1.255	IP range that is specified to the domain.
IPRANGE=1.1.1.1-255.255.255.255	Another IP range that is specified to the domain.

TABLE A-1. Format of ExtraMachineDomainList.ini

b. The WINS server in the network is working properly.

c. The DNS server in the network is working properly.

4. Check if the administrator accounts used to scan the client machines are entered. Open the DCS Account Management Tool, view the account list to see if the accounts for the specific machines or domains exist.
5. Use the UNC path to log on to the client machine's default shared folder and then drop a file to that machine.

   Command: `\\[Client Machine Name]\c$`

   If the DCS server cannot log on to the client machine and drop a file, check the account privilege and the security policy settings of the machine or domain.
6. Enable the ICMP protocol. DCS uses ICMP protocol to detect the existence of a client machine. If the ICMP protocol has been blocked, then DCS cannot find the client.

DCS Scan Timeout Problem

DCS provides three kinds of spyware/grayware scans:

- Quick Scan
- Hybrid Scan
- Full Scan

The default scan timeout for Quick Scan is 1,800 seconds and the default scan timeout for Hybrid and Full Scan is 7,200 seconds. Sometimes the scan result for specific machines may time out because there are more files on the machine than DCS is designed to scan.

Solution.—If you always encounter the scan timeout problem and it is not caused by a firewall or other issue, you can manually extend the scan timeout limit by editing the value of the registry key shown below:

For Quick Scan:

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\DCS\Server\HVA\DeployTimeout
Second
```

For Hybrid Scan or Full Scan:

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\DCS\Server\HVA\
DeployTimeoutForFullScan
```

Scan Failure Due to DEP (Data Execution Prevention)

Problem.— DCS sometimes fails to scan a client machine if the client machine has enabled Data Execution Prevention (DEP).

Note: DE is a Windows feature available only in Windows XP Service Pack 2, Windows XP Tablet PC Edition 2005, and Windows Server 2003 with Service Pack 1.

Solution 1.— Add the DCS client agent, `RMAgent.exe` in the `/temp/` folder into the DEP exception list. To get to the DEP exception list, follow the procedure below.

To add RMAgent.exe to the DEP exception list:

1. While logged on to the client computer as Administrator, click **Start** > **Run** and type **sysdm.cpl** and click **OK.** The System Properites multi-tabbed window appears.
2. On the Advanced tab, under Performance, click **Settings.** The Performance Options window appears.
3. Click the **Data Execution Prevention** tab and select the **Turn on DEP for all programs and services except those I select:** radio button. The field below the option and the **Add...** button below it activate.
4. Click **Add....** A file manager window appears.
5. Navigate to the location of the `RMAgent.exe` file on the client machine and click that filename. A checkbox with a green check in it appears next to the name `RMAgent.exe` in the field above the **Add...** button.
6. Click **OK** two times

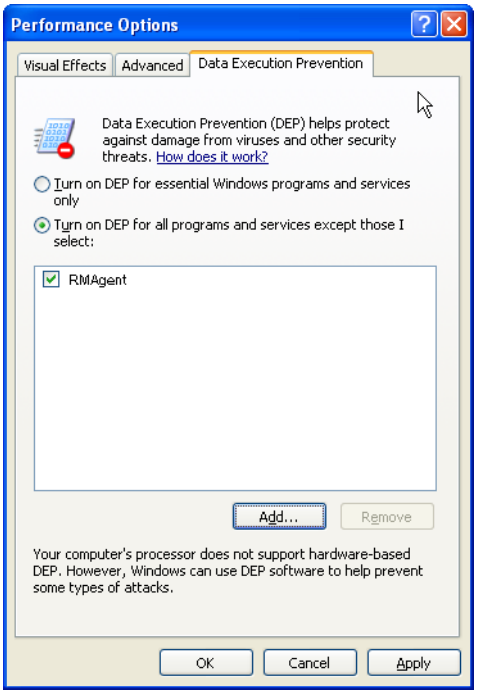


FIGURE A-1. Setting RMAgent in the Microsoft Windows XP DEP exception list

Solution 2.—Download Microsoft Application Compatibility Toolkit and apply its compatibility fix, DisableNX, to DCS client agent (`RMAgent.exe`). Save the fix as an `sdb` file and deploy the fix to machines that need it by one of the following methods:

- **Email attachment.** The custom database can be sent through email to the users who require the fixes. If users are running Windows XP, they can simply choose to run the attachment.
- **Floppy disk.** The "Sneaker Net" approach—copy the database file onto removable media and use that media to install the database on multiple machines. (Obviously, best suited to a small number of machines in close walking distance.)
- **Network folder.** Users of client machines can manually install the compatibility database from a shared network location.

- **Push install.** You can include the custom database in an installation package that you deploy through push technology. Possible solutions include Microsoft Systems Management Server (SMS) or Group Policy within Active Directory domains.
- **Logon script.** (Does not require user interaction and can be custom-tailored for different groups of users based on the logon script that they receive.)

As an example of how a logon script might be used, consider the following:

```
if not exist %systemroot%\apppatch\RMAgentFix.sdb sdbinst.exe –q
\\server1\compat\RMAgentFix.sdb
```

Report generation issue in an SQL Server 2005 environment

Report generation may fail if using SQL Server 2005 as the DCS 3.2 database because Microsoft disabled the SQL Server 2005 TCP/IP protocol for security concerns. DCS uses TCP/IP to connect to the database to generate reports.

To solve this problem, manually change the SQL server connection method by changing to "1" the value of the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\DCS\Server\SQLConn
ectType
```

Frequently Asked Questions

Review these frequently asked questions for insight into issues that many users ask about.

Product Information, Updating, and Compatibility

How can I find out the version of my Virus Cleanup Engine?

To determine the product version of your Virus Cleanup Engine:

1. In the sidebar click **Updates** > **Manual.** The Manual Update screen appears.
2. The Current Version column lists the product version in the Virus Cleanup Engine row.

After installing Service Pack 2 for Windows XP on a machine that is targeted for scanning in my network, the task that runs Damage Cleanup Services (DCS) on that machine does not work.

Resolve this issue by doing the following on the Windows XP machine:

1. Click **Start** and then click **Control Panel.**
2. In Control Panel, click **Windows Security Center.**
3. Click **Windows Firewall.**
4. In the Windows Firewall window, click the **Exceptions** tab.
5. Select **File and Print Sharing** and click **OK.**
6. Retry running the task for Damage Cleanup Services.

Can I manage Damage Cleanup Services through Trend Micro Control Manager 3?

Yes, you can do so after applying DCS 3.0 Service Pack 1 or after installing DCS 3.2 and the Control Manager agent that is included in the release. See *What's New in Damage Cleanup Services 3.2* on page 1-3 for more information.

Installation and Initial Settings

Can I install DCS 3.2 on a machine that has DCS 2.0 installed on it?

Yes, you can. The previous version and the new version are different Trend Micro products. However, owing to performance and server loading issues, Trend Micro suggests that you install the new version on a separate machine than the previous version.

Must I activate the product with an Activation Code during installation?

No, it is not necessary to activate the product during installation. You can activate the product after installing by using the Product License screen of the management console (**Administration** > **Product License**). To skip activation during installation, leave the Activation Code field blank in the Activate Products section of the Product Activation screen and click **Next** to continue.

Is it possible to keep the database when uninstalling DCS?

Yes, it is. During uninstallation, the system asks you whether you would like to keep the database. During installation, if DCS detects an existing DCS database on the system, DCS gives you the option of using it or overwriting it.

Why does DCS often ask me to log on again if the system has been idle a while? Is there a way to extend the timeout setting?

The default system timeout for DCS is 900 seconds (15 minutes). You can change the timeout setting by editing the system registry.

To edit the DCS timeout setting:

1. In Windows click **Start** > **Run** to open the Run screen.
2. Type **regedit** and click **OK.** The Windows Registry Editor application opens.
3. Navigate to **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **TrendMicro** > **DCS** > **Web.**
4. Double-click **Timeout.** The Edit DWORD Value screen appears.
5. In the Base section, click **Decimal** to change the numerical base to decimal. The default hexadecimal entry in the Value data field changes from 384 (hex) to 900 (decimal).
6. In the **Value data** field type your preferred timeout value, in seconds.
7. Click **OK** to apply your change.
8. Close the registry editor.

Running and Scheduling Scans

What Is the Manual Damage Cleanup Tool, and How Can I Trigger a Manual Damage Cleanup?

The Manual Damage Cleanup Tool allows clients to scan for malware and spyware/grayware voluntarily without having to wait for the DCS server to deploy tasks. The DCS server records the results from such scans. For detailed guidance on using the Manual Damage Cleanup Tool, see *Using the Manual Damage Cleanup Tool* on page 5-10.

Can two scans run at the same time?

No, they cannot. DCS performs one scan at a time. When two scans (either scheduled or manual) are have the same start time and the time arrive, DCS puts one scan in a queue. The scan that you created first runs first.

To verify how many scans are queuing, click **In progress… (dd%)** in the Completion Time column on the Summary screen. The Current Running Scan screen appears.

How can I cancel a scan while it is running or waiting in the queue?

To cancel a scan that is running, click **Stop the Scan** next to **Percentage complete** in the Scan Status table of the Current Running Scan screen. DCS does not allow the removal of a scan that is already queued.

Is there any way to adjust the default frequency that the Current Running Scan screen refreshes?

Yes, you can adjust the default refresh interval for this screen by changing the value of the following key in the Windows registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\DCS\Web\RefreshTimer
```

The maximum value is 100 (seconds) and the minimum value is 5 seconds.

Can I add more than one instance of a scan to the scan queue?

No, you cannot. DCS does not support multiple instances of a single scan in the queue.

Can I modify or delete scan details while a scan is running or in the queue?

No, you cannot. When a scan is running or in the queue, no one can modify its scan details.

Reports, Logs, and Notifications

In what file formats can DCS generate reports? Do I need special software to view them?

DCS generate reports in Adobe Acrobat (.PDF) format. To view PDF files, you need the Adobe Acrobat Viewer (www.adobe.us/products/acrobat/readstep2.html).

Every scan has its own notification, but there is also a global notification for all scans. Will I receive two notifications if I enable both notifications?

Yes, you will receive both notifications: scan result summary and scan successful notification. DCS only sends a scan result summary when a scan completes successfully.

What if my office network does not support MSN messaging?

MSN can be implemented in two ways: connect to MSN by specific port or HTTP protocol. If your IT setup blocks the specific port, you cannot use MSN notification, because DCS does not support HTTP protocol.

I set the number of days to keep logs at 5 days. Why aren't there results for scans run on the fifth day?

The number of days to keep logs includes today. If you want to keep logs for five days plus today, set the number of days to keep logs at 6.

Product Licensing

What happens to DCS if the Activation Code is not activated or if the license expires?

Until you input a valid Activation Code, the scan and component update functions do not work. If a license has expired but you are still within the grace period, you can still run scans and update components. Once the grace period is over, DCS locks the

component update function. To unlock this function, re-activate the license (Click **Administration** > **Product License** > **Re-activate**).

License Status	DCS Scan	Component Updates	DCS Cleanup	Generate Reports	Update License
License expired; still in grace period	Yes	Yes	Yes	Yes	Yes
License expired; grace period is over	Yes	No	Yes	Yes	Yes

TABLE A-2. Standard version functionality after the license expires

DCS Scan	Component Updates	DCS Cleanup	Generate Reports
No	No	No	Yes

TABLE A-3. Evaluation version functionality after the license expires

Can I activate DCS by entering the Activation Code when the DCS server is not connected to the Internet?

Yes, you can activate or re-activated DCS anytime, as long as the Activation Code you enter is valid. In order to register DCS, however, you must have a live Internet connection, because you must type your registration key at the Online Registration Web site:

`https://olr.trendmicro.com/registration/us/en-us/login.aspx`

Working with Debug Logs

Before contacting your support provider, it is often helpful to turn on debugging and try to replicate the error that you are going to report. Providing your support technicians with a debug log can help speed up resolution of the technical problem encountered.

WARNING! *Trend Micro strongly recommends that you do not turn on debugging unless you are working with Technical Support. DCS debug logs do not truncate by*

default, and an overly large debug file could slow performance. It is very important to turn off debugging after a short period of time.

To turn on debugging in Damage Cleanup Services:

1. In Windows click **Start** > **Run** to open the Run screen.
2. Type **regedit** and click **OK.** The Windows Registry Editor application opens.
3. Navigate to **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **TrendMicro** > **DCS** > **Debug.**
4. Double-click **Enable.** The Edit DWORD Value screen opens.
5. In **Value data** type **1.**

To set the debugging level:

1. In Windows click **Start** > **Run** to open the Run screen.
2. Type **regedit** and click **OK.** The Windows Registry Editor application opens.
3. Navigate to **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **TrendMicro** > **DCS** > **Debug.**
4. Double-click **Level.** The Edit DWORD Value screen opens.
5. In **Value data** type **1.**
6. Click **OK** to apply the change.

To set the location for where to store debug logs:

1. In Windows click **Start** > **Run** to open the Run screen.
2. Type **regedit** and click **OK.** The Windows Registry Editor application opens.
3. Navigate to **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **TrendMicro** > **DCS** > **Debug.**
4. Double-click **Path.** The Edit String screen opens.
5. In **Value data** type the full path name of the directory where you would like to store debug logs. If you do not enter an absolute path, the path will be relative to your <DCSDir> directory.

To turn on the debugging for DCS engine deployed on client machine

1. In Windows click **Start** > **Run** to open the Run screen.
2. Type **regedit** and click **OK.** The Windows Registry Editor application opens.

3. Navigate to **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **TrendMicro** > **DCS** > **Server**
4. Double-click **ClientDebugLevel.** The **Edit DWORD Value** screen opens.
5. In **Value** data type **3**.
6. Click **OK** to apply the change.

By default, DCS enables debugging for ActiveUpdate download and the Microsoft Desktop Engine (MSDE) database application installation.

Debugging for the Manual Damage Cleanup Tool is set via http query string. In order to turn on debugging for this tool, append `?q=begin&debug=3&MW=1&SW=1` to the normal Manual Damage Cleanup Tool URL. The full debug URL then, should look something like this:

```
<Your_DCS_Web_host>/DCS/cgiDCSX.exe?q=begin&debug=3&MW=1&SW=1
```

Default Locations of Debug Logs

The table below shows the default locations of debug logs for DCS.

Debug log	Location
Virus Cleanup Engine (on client machines)	<OS drive>:\temp\<DCS server name>\Debug\RMDebug.log and <OS drive>:\temp\<DCS server name>\Debug\TSCDebug.log
Spyware Scan Engine	<OS drive>:\temp\ <DCS server name>\ssapi.log
DCS service	<DCSDir>\DebugLog\
Account Management Tool	<DCSDir>\DebugLog\
Web User Interface	<DCSDir>\WebUI\DebugLog\
Deployment engine	<DCSDir>\DebugLog\rm_HVAEngine.log
Manual Assessment Tool - malware (on client machines)	<WinDir>\RMXDebug.log
Manual Assessment Tool - spyware/grayware (on client machines)	<WinDir>\DCS\ssapi.log
ActiveUpdate download	<DCSDir>\AU_Log\
Cisco ICS communication CGI	<DCSDir>\DebugLog\rm_CGIMessageReceiver.log
IWSS communication CGI	<DCSDir>\DebugLog\ rm_CGIReqReceiver.log
DCS installation and uninstallation	<OS drive>:\\DCS_Install.log and <OS drive>:\\DCS_Uninstall.log
MSDE installation	<OS drive>:\\DCS_MSDE_Install.log
DCS report module	<DCSDir>\DebugLog\TMReport.log

TABLE A-4. Default locations of DCS debug logs

Contacting Trend Micro

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

`www.trendmicro.com/en/about/contact/overview.htm`

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

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

`http://esupport.trendmicro.com`

Appendix B

Glossary

Access Control Server (ACS)

Passes authentication requests from the *Network Access Device* to the Policy Server in order to validate end-user client security posture. The ACS server also passes the *Posture token* from the Policy Server to the Network Access Device. The ACS server can also be configured to carry out actions on the end-user client via the Network Access Device.

ACS Certificate

Used to establish trusted communication between the *Access Control Server (ACS)* and the *Certificate Authority (CA)* server. The Certificate Authority server signs the ACS certificate, and it is saved on the ACS server.

ActiveX malicious code

A type of virus that resides in Web pages that execute ActiveX controls.

Additional Threats

Files and programs, other than viruses, that can negatively affect the performance of the computers on your network. These include *Spyware*, *Adware*, *Dialers*, *Joke program*, *Hacking tools*, *Remote access tools*, *Password cracking applications*, and others.

Adware

Adware is software that displays advertising banners on Web browsers such as Internet Explorer and Mozilla. While not categorized as malware, many users consider adware invasive. Adware programs often create unwanted effects on a system, such as annoying popup ads and the general degradation in either network connection or system performance.

Adware programs are typically installed as separate programs that are bundled with certain free software. Many users inadvertently agree to installing adware by accepting the End User License Agreement (EULA) on the free software.

Adware is also often installed in tandem with spyware programs. Both programs feed off of each other's functions — spyware programs profile users' Internet behavior, while adware programs display targeted ads that correspond to the gathered user profiles.

Backdoor

A Backdoor is a program that opens secret access to systems, and is often used to bypass system security. A Backdoor program does not infect other host files, but nearly all Backdoor programs make registry modifications. For detailed removal instructions please view the virus description. See virus types for an explanation of Trend Micro virus-naming conventions.

Boot sector viruses

A type of virus that infects the boot sector of a partition or a disk.

Certificate Authority (CA)

An authority on a network that distributes *Digital certificates* for the purposes of performing authentication and securing connections between computers and/or servers.

COM and EXE file infectors

A type of virus that masquerades as an application by using a .exe or .com file extension.

Cookies

Cookies are text files that are created on computers when visiting Web sites. They contain information on user browsing habits. When a user returns to a Web site, a

cookie provides information on the user's preferences and allows the site to display in customized formats and to show targeted content such as advertising. Cookies can collect user information that can then be obtained by another site or program.

Dialers

Software that changes client Internet settings and can force the client to dial pre-configured phone numbers through a modem.

Digital certificates

An attachment that is used for security. Most commonly, certificates authenticate clients with servers, such as a Web server, and contain the following: user identity information, a public key (used for encryption), and a digital signature of a *Certificate Authority (CA)* to verify that the certificate is valid.

Dynamic Host Control Protocol (DHCP)

A device, such as a computer or switch, must have an IP address to be connected to a network, but the address does not have to be static. A DHCP server, using the Dynamic Host Control Protocol, can assign and manage IP addresses dynamically every time a device connects to a network.

Dynamic IP Address (DIP)

A Dynamic IP address is an IP address that is assigned by a DHCP server. The MAC address of a computer will remain the same, however, the computer may be assigned a new IP address by the DHCP server depending on availability.

File Transfer Protocol (FTP)

FTP is a standard protocol used for transporting files from a server to a client over the Internet. Refer to Network Working Group RFC 959 for more information.

Grayware

A general classification for applications that have behavior that is undisclosed or that some may find annoying or undesirable.

Hacking tools

Tools used to help hackers enter computers, often through open ports.

Hypertext Transfer Protocol (HTTP)

HTTP is a standard protocol used for transporting Web pages (including graphics and multimedia content) from a server to a client over the Internet.

HTTPS

Hypertext Transfer Protocol using *Secure Socket Layer (SSL)*.

HTML, VBScript, or JavaScript viruses

Viruses that reside in Web pages and are downloaded through a browser.

Internet Control Message Protocol (ICMP)

Occasionally a gateway or destination host uses ICMP to communicate with a source host, for example, to report an error in datagram processing. ICMP uses the basic support of IP as if it were a higher level protocol, however, ICMP is actually an integral part of IP, and must be implemented by every IP module. ICMP messages are sent in several situations: for example, when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. The Internet Protocol is not designed to be absolutely reliable. The purpose of these control messages is to provide feedback about problems in the communication environment, not to make IP reliable.

Internet Protocol (IP)

"The internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses." (RFC 791)

Intrusion Detection System (IDS)

Intrusion Detection Systems are commonly part of firewalls. An IDS can help identify patterns in network packets that may indicate an attack on the client.

Java malicious code

Operating system-independent virus code written or embedded in Java.

Joke program

A Joke program is an ordinary executable program with normally no malicious intent. Virus authors create joke programs for making fun of computer users. They do not intend to destroy data but some inexperienced users may inadvertently perform actions that can lead to data loss (such as restoring files from an older backup, formatting the drive, or deleting files).

Since joke programs are ordinary executable programs, they will not infect other programs, nor will they do any damage to the computer system or its data. Sometimes, joke programs may temporarily re-configure the mouse, keyboard, or other devices. However, after a joke program finishes its execution or the user reboots the machine, the computer returns to its original state. Joke programs, while normally harmless, can be costly to an organization.

Malware

Malware refers to any program that executes and performs activities that are outside of the user's consent. A virus is a form of malware. Other examples of malware include Trojans, Worms, Backdoors, Denial of Service attacker agents, Joke programs, as well as several other smaller categories of malicious code.

Macro viruses

A type of virus encoded in an application macro and often included in a document.

Network Address Translation (NAT)

NAT is a function performed by gateway firewalls and routers. A table stored in the firewall or router records the IP addresses of devices on the inside of the gateway, and maps them to the external IP address of the gateway. A packet originating from within the network is stripped of its header and sent to its destination with a header containing the external IP address of the router or gateway. The destination IP address of the outbound packet is stored so that when a response arrives from the destination, the router may forward it to the correct internal IP address. In this manner, the IP addresses of devices on the internal network are hidden from the outside.

Network Access Device

Network access servers, firewalls, routers, or wireless access points that support Cisco NAC functionality.

Network virus

A network virus is a self-contained program (or set of programs) that is capable of spreading copies of itself or its segments across the network, including the Internet. Propagation often takes place via shared resources, such as shared drives and folders, or other network ports and services. Network viruses are not limited to the usual form of files or email attachments, but can also be resident in a computer's memory space alone (often referred to as Memory-only Worms).

Password cracking applications

Software that can help hackers decipher account user names and passwords.

Ping

A utility that sends an *Internet Control Message Protocol (ICMP)* echo request to an IP address and waits for a response. The Ping utility can determine whether or not the machine with the specified IP address is online or not.

Post Office Protocol 3 (POP3)

POP3 is a standard protocol for storing and transporting email messages from a server to a client email application.

Posture token

The Policy Server creates the posture token after end-user client validation. It includes information that tells the program to perform a set of specified actions, such as enabling Real-time Scan or updating antivirus components. Cisco NAC devices also use the posture token to manage network access allowed to the client by *Network Access Device*.

Remote access tools

Tools used to help hackers remotely access and control a computer.

Secure Socket Layer (SSL)

SSL is a scheme proposed by Netscape Communications Corporation to use RSA public-key cryptography to encrypt and authenticate content transferred on higher level protocols such as HTTP, NNTP, and FTP.

SSL certificate

A digital certificate that establishes secure HTTPS communication between the Policy Server and the *Access Control Server (ACS)* server.

Security posture

The presence and currency of antivirus software installed on an end-user client. The security posture of OfficeScan clients refers to whether or not the OfficeScan client program is installed and how old the antivirus component versions are.

Simple Mail Transport Protocol (SMTP)

SMTP is a standard protocol used to transport email messages from server to server, and client to server, over the internet.

SOCKS 4

A *Transmission Control Protocol (TCP)* protocol used by proxy servers to establish a connection between clients on the internal network or LAN and computers or servers outside the LAN. The SOCKS 4 protocol makes connection requests, sets up proxy circuits and relays data at the Application layer of the OSI model.

Spyware

Software that installs components on a computer for the purpose of recording Web surfing habits (primarily for marketing purposes). Spyware sends this information to its author or to other interested parties when the computer is online. Spyware often downloads with items identified as 'free downloads' and does not notify the user of its existence or ask for permission to install the components. The information spyware components gather can include user keystrokes, which means that private information such as login names, passwords, and credit card numbers are vulnerable to theft.

Stateful inspection firewall

Stateful inspection firewalls monitor all connections to a computer and remember all connection states. They can identify specific conditions in any connection, predict what actions should follow, and detect when normal conditions are violated. This significantly increases the chances that a firewall can detect an attack on a client.

Telnet

Telnet is a standard method of interfacing terminal devices over TCP by creating a "Network Virtual Terminal". Refer to Network Working Group RFC 854 for more information.

Test virus

An inert file that acts like a real virus and is detectable by virus-scanning software. Use test viruses, such as the EICAR test script, to verify that your antivirus installation is scanning properly (see Testing the client installation).

Transmission Control Protocol (TCP)

A connection-oriented, end-to-end reliable protocol designed to fit into a layered hierarchy of protocols which support multi-network applications. TCP relies on IP datagrams for address resolution. Refer to DARPA Internet Program RFC 793 for information.

TrendLabs

TrendLabs is Trend Micro's global network of antivirus research and product support centers that provide 24 x 7 coverage to Trend Micro customers around the world.

Trojan horses

A Trojan is a destructive program that comes concealed in software that not only appears harmless, but also comes in a particularly attractive form (such as a game or a graphics application). There may be instances when a Trojan does not have a destructive payload. Instead, it may contain routines that can compromise the security of your system or the entire network. These types of Trojans are often referred to as Backdoor Trojans.

Trojans are non-replicating malware – they do not replicate by themselves and they rely on the user to send out copies of the Trojan to others. They sometimes achieve this by hiding themselves inside desirable software (that is, computer games or graphics software), which novice users often forward to other users.

User Datagram Protocol (UDP)

A connectionless communication protocol used with IP for application programs to send messages to other programs. Refer to DARPA Internet Program RFC 768 for information.

Virus

A virus is a program that replicates. To do so, the virus needs to attach itself to other program files and execute whenever the host program executes.

Worm

A computer worm is a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems. The propagation usually takes place via network connections or email attachments. Unlike viruses, worms do not need to attach themselves to host programs. Worms often use email and applications, such as Microsoft™ Outlook™, to propagate. They may also drop copies of themselves into shared folders or utilize file-sharing systems, such as Kazaa, under the assumption that users will likely download them, thus letting the worm propagate. In some cases, worms also use chat applications such as ICQ, AIM, mIRC, or other Peer-to-Peer (P2P) programs to spread copies of themselves.

Index

T

U

V

W