TREND MICRO™
Damage Cleanup Services™ 3

Administrator's Guide

TREND MICRO™

Document Part No. DCEM32236/50331

Release Date: June 2005

Patents Pending

The Administrator's Guide 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.

For technical support, please refer to Appendix A: Troubleshooting and Technical Support for technical support information and contact details. Detailed information about how to use specific features within the software is available in the online help file and online Knowledge Base at Trend Micro's Web site.

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

Chapter 3: Getting Started with Damage Cleanup Services—continued

Chapter 4: Configuring Damage Cleanup Services

Chapter 5: Running Scans

Chapter 6: Logs and Reports

Appendix A: Troubleshooting and Technical Support

Appendix B: Glossary

Index

Preface

Welcome to the *Trend Micro™ Damage Cleanup Services 3 Administrator's Guide*.This book contains information about the tasks you need 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 ii 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 PDF, provides the following information:

- 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)
- Guidelines on installing and updating Damage Cleanup Services 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)
- Procedures to configure and administer scans and notifications from the Damage Cleanup Services Web-based management console and instructions on using the *Using the Account Management Tool* (*Configuring Damage Cleanup Services* on page 4-1)
- Detailed instructions on how to create scheduled and one-time scans for malware and spyware/grayware, including guidance on using the *Using the Manual Damage Cleanup Tool* (*Running Scans* on page 5-1)

- Detailed instructions on managing logs and reports (*Logs and Reports* on page 6-1)
- Assistance on troubleshooting and technical support, including *Frequently Asked Questions* (*Troubleshooting and Technical Support* on page A-1)
- 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 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 Damage Cleanup Services 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 garbage and viral files dropped by viruses
- Repairs system file configurations (such as system.ini), after they have been altered or infected by malicious code
- 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™

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

- Windows NT Server and Workstation
- Windows 2000 Professional/Server/Advanced Server
- Windows XP Professional
- Windows 2003 Web/Standard/ Enterprise server

What's New in Damage Cleanup Services 3.0

With this release Trend Micro launches Damage Cleanup Services™ (DCS) as a standalone product, instead of a component of Trend Micro Control Manager™ (TMCM).

A Standalone Product

Because DCS is now a standalone product, it has the following new features:

- Its own installation program
- Scalable architecture allows it to expand to multiple servers or to a wide area network
- Its own management console
- Its own configurable administrative notifications
- Separate queries for spyware/grayware logs and malware logs

Account Management Tool

DCS provides a Windows-based account management tool to allow IT managers to set the domain/machine administration account password. Use this tool to give DCS the access it needs to scan the clients targeted in your network.

Advanced Spyware/Grayware and Malware Scan Reporting

DCS can produce a variety of spyware/grayware reports 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

You can now 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

Spyware/Grayware Detection and Cleanup

DCS can now detect and remove unwanted spyware/grayware. Because not all spyware/grayware is undesirable, however, IT managers can mark desired spyware/grayware for exclusion from the cleanup process. For a description of the term "grayware," see *What Is Grayware?* on page 1-5. See *Choosing Spyware/Grayware to Exclude from Scans* on page 4-13.

Scheduled Updates

DCS supports manual or scheduled updates of damage cleanup templates, spyware/grayware patterns, and versions of the Damage Cleanup Engine.

Damage Cleanup Services Basics

Trend Micro Damage Cleanup Services 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 Trend Micro Damage Cleanup Services on your system.

Who Should Use Damage Cleanup Services?

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 (*Introducing the Damage Cleanup Engine* on page 1-9) 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 5-9) 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 makes use of several technologies to do its work. When preparing DCS for use, the administrator enters account information for all of the computers in the network in to the DCS Account Management Tool (see *Using the Account Management Tool* on page 4-2). DCS uses this tool when running its scans and cleanup up clients. Because no DCS software is installed client machines, only the DCS server is required to update its components (the Damage Cleanup template, which contains patterns used to identify Trojans, network viruses, and active spyware/grayware, and the Damage Cleanup engine, which DCS deploys to each client machine at the time of scanning). Client machines therefore are never required to update any software or receive pattern files.

DCS deploys the Damage Cleanup engine by making use of ActiveX technology. For this reason, the machine on which the DCS server is installed must have Microsoft Internet Information Server 5.0 and the Microsoft .NET Framework 1.1.

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:** change client Internet settings and can force a computer to dial preconfigured phone numbers through a modem. These are often pay-per-call or international numbers that can result it a significant cost to your organization.
- **Joke Programs:** cause a computer to behave abnormally, such as making the screen shake or modifying the appearance of the cursor.
- **Hacking Tools:** help malicious hackers enter a computer
- **Remote Access Tools:** help malicious hackers remotely access and control a computer
- **Password Cracking Applications:** help decipher account 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 introduce 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

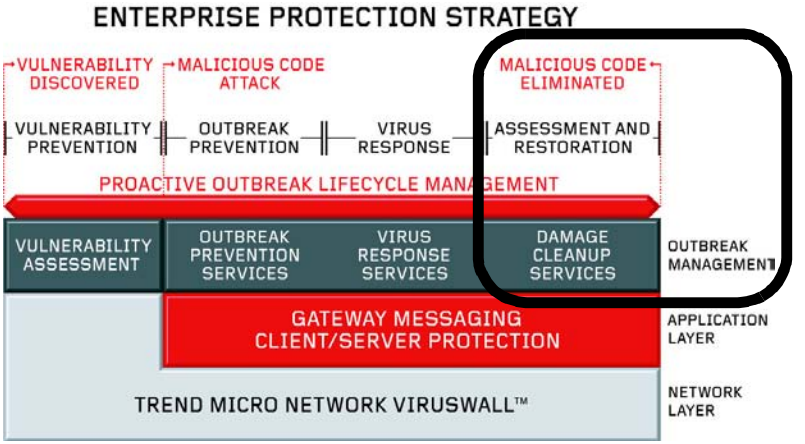
This version of Trend Micro Damage Cleanup Services has the ability to scan for, detect, and remove a multitude of active spyware and other grayware processes.

For instructions on configuring Damage Cleanup Services to scan for spyware/grayware, see *Selecting Scan Action* on page 4-12.

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."



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 Damage 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.

Introducing the Damage Cleanup Engine

Damage Cleanup Services (DCS) makes use of a scanning and cleanup tool called the Damage Cleanup Engine (DCE) to find and repair damage caused by viruses and other Internet threats. The Damage Cleanup Engine can find and clean both spyware/grayware and malware. DCE is essentially a software agent that makes use of a database to find targeted machines and evaluate whether or not viruses, spyware/grayware, or other Internet threats have affected them. DCE resides on a single machine and deploys to the targeted client machines on the network at the time of scanning.

The Damage Cleanup Engine uses damage cleanup templates and spyware/grayware patterns that contain information that DCE uses to restore damage caused by the latest known viruses, spyware/grayware, or other Internet threats. DCS regularly updates these templates and patterns. When you install DCS, you are installing the version of the Damage Cleanup Engine that was current as of the release of this product. This engine is updated frequently, therefore, Trend Micro recommends that you update your components immediately after you have installed and activated Damage Cleanup Services.

Chapter 2

Installing Damage Cleanup Services

This chapter includes the following topics:

System Requirements

The only platform to which Damage Cleanup Services can successfully install to is Microsoft Windows server. The system on which you install DCS has different system requirements than its client systems.

Minimum System Requirements

Operating systems:

- Windows 2000 Server/Advanced Server SP3
- Windows 2003 Standard/Enterprise Server

Note: Damage Cleanup Services does not support Microsoft Windows NT.

Microsoft Internet Explorer 5.5 plus SP2
(DCS uses ActiveX controls and JavaScript, and those technologies are supported by IE 5.5 + SP2.)
Microsoft Internet Information Server (IIS) 5.0
Microsoft .NET Framework 1.1 (DCS installs it if it isn't present)
Memory: 512MB
Processor: Pentium III, 1GHz
Available Disk Space: 300MB

Recommended System Requirements

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

Installation Procedures

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 the **Damage Cleanup Services** and click **GO.** The Damage Cleanup Services installation page appears.
3. Follow the steps under *Pre-Installation Tasks* on page 2-4 and *The InstallShield Wizard* on page 2-5.

Installing via a Web Download

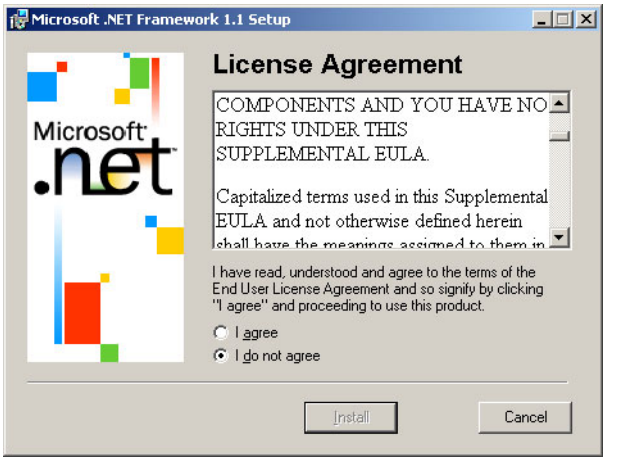
To download from the Web:

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).
3. Follow the steps under *Pre-Installation Tasks* on page 2-4 and *The InstallShield Wizard* on page 2-5

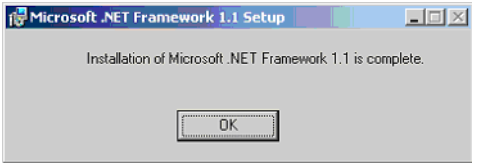
Pre-Installation Tasks

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.



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



The InstallShield Wizard

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

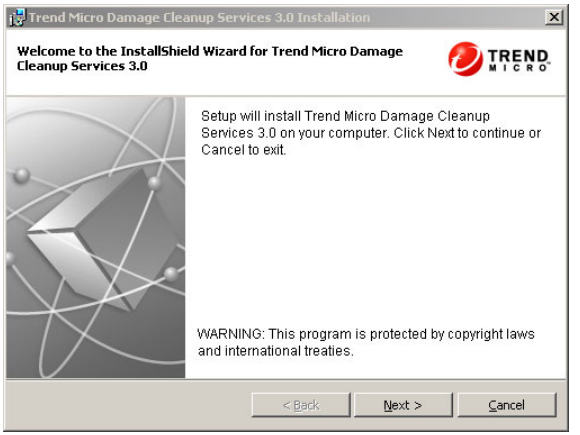
1. *Launching the InstallShield Wizard* on page 2-5
2. *Selecting a Database* on page 2-7
3. *Activating Damage Cleanup Services* on page 2-10
4. *Setting an Administrator Account and Installing the Program Files* on page 2-12

Launching the InstallShield Wizard

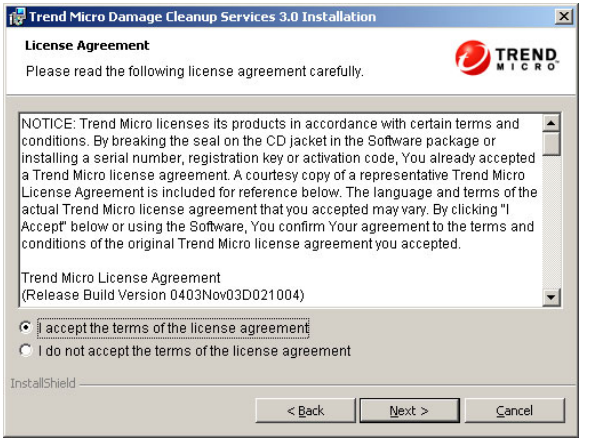
Follow the instructions below to launch the Damage Cleanup Services InstallShield Wizard.

To launch the Damage Cleanup Services InstallShield Wizard:

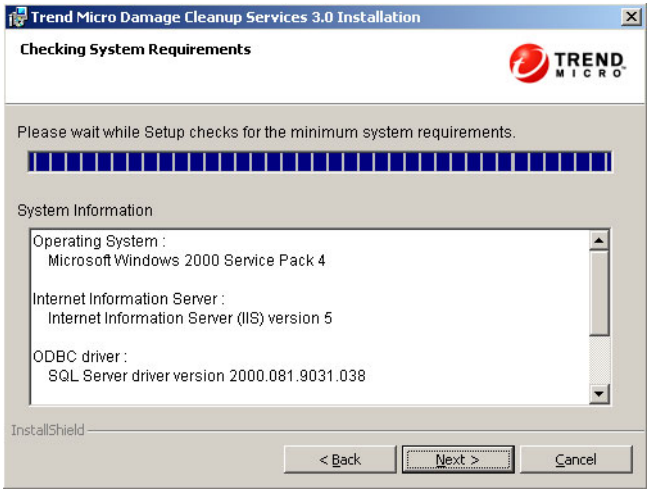
1. Launch the InstallShield Wizard by double-clicking the file `setup.exe` on your Trend Micro Damage Cleanup Services CD (or on your hard disk, if you have downloaded it). The InstallShield Welcome screen appears.



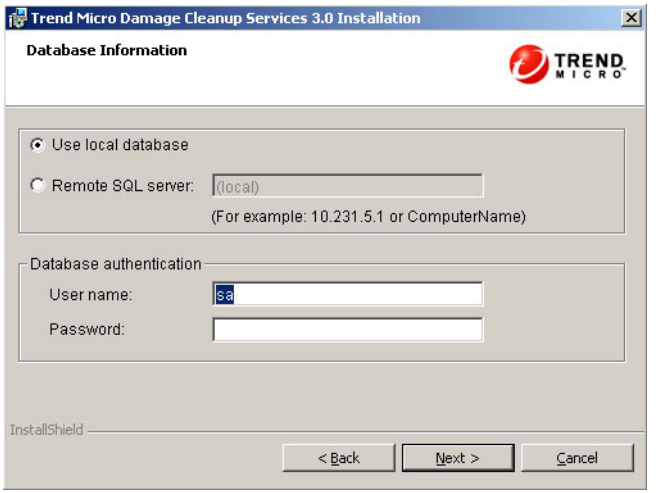
2. Click **Next** from the initial InstallShield screen to start the installation. The License Agreement screen appears.



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



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:

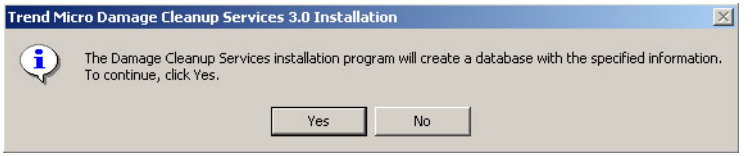
- Install Microsoft SQL Server Desktop Engine
- Remote SQL Server

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:

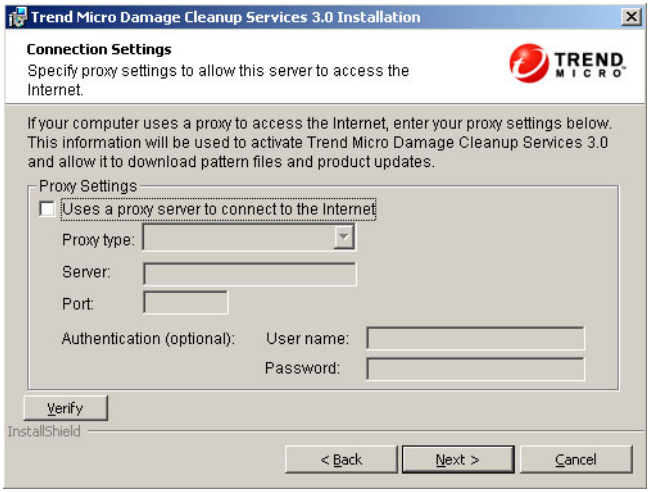
- Remote SQL Server

To select a database for use with Damage Cleanup Services:

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.**

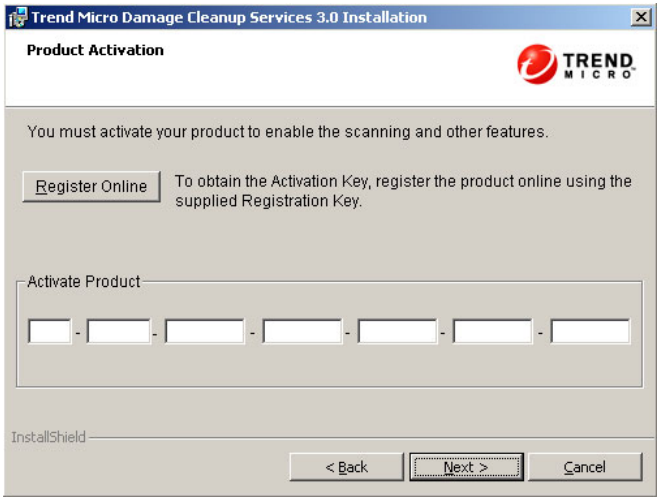


2. If using SQL server, type the server address.
3. If using database authentication, type the **User name** and **password.** Click **Next.** The Connection Settings screen appears.



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:

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



Activating Damage Cleanup Services

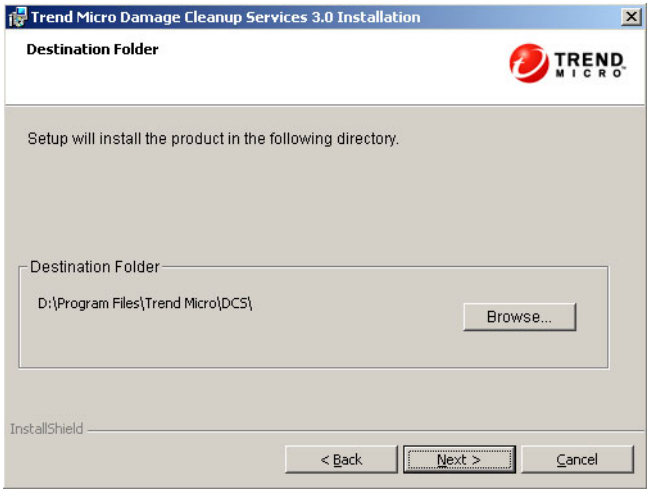
To activate Damage Cleanup Services and set installation directory:

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.

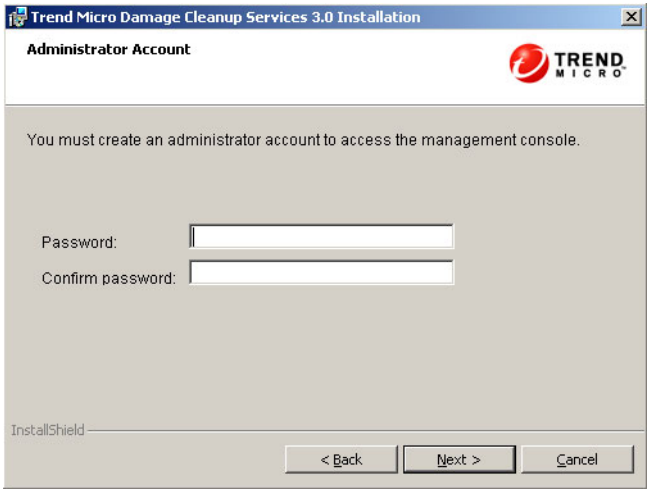
   Once you have the Activation Code, type it in the fields provided in the Activate Products section.

   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.



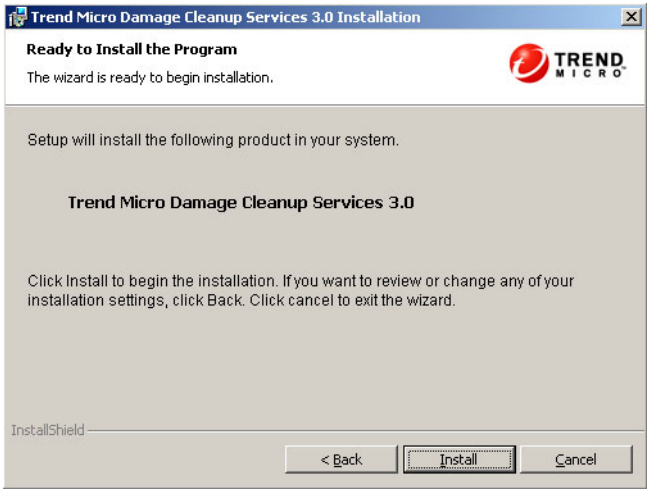
3. To select a directory other than the default installation directory, click **Browse** and navigate to your preferred installation directory. Click **Next.** The Administrator Account screen appears.


Trend Micro Damage Cleanup Services 3.0 Installation
Administrator Account
TREND MICRO
You must create an administrator account to access the management console.
Password:
Confirm password:
InstallShield
< Back
Next >
Cancel

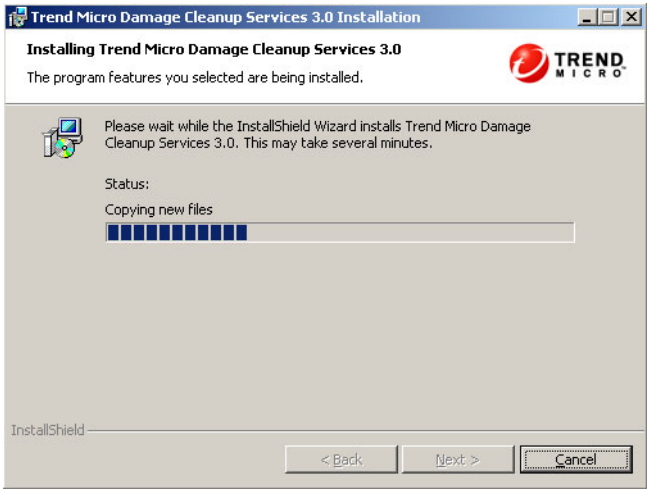
Setting an Administrator Account and Installing the Program Files

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

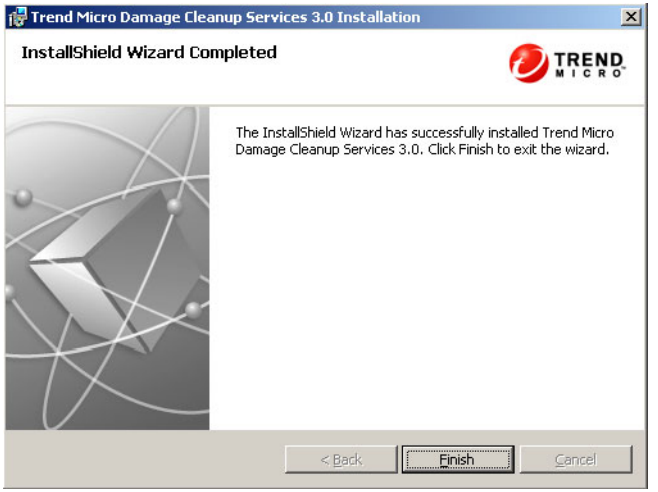
1. Type a password for the Administrator account that you will use with DCS and retype it in **Confirm password.** Click **Next.** A screen appears stating that you are now ready to install Trend Micro Damage Cleanup Services.



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



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



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

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.

You need a DCS Activation Code or Registration Key for activation. If you do not have the Activation Code (AC) or Registration Key (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 do not work.

Trend Micro recommends that you register your product before beginning the installation process. However, you can activate DCS after installation if you did not do so during installation.

To activate Damage Cleanup Services after installation:

1. On the sidebar click **Administration** > **Product License**. The **Product License** screen appears.
2. If you do not have the Activation Code, click **Register**. Your browser redirects to the Trend Micro registration Web site. Follow the directions on the screen and use the Registration Key to obtain an Activation Code.
3. Once you have the Activation Code, 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 Registration Key is required to complete the product registration process.

A Registration Key uses 22 characters, including hyphens, in following format:

`XX-XXXX-XXXX-XXXX-XXXX`

Damage Cleanup Services (DCS) must be registered, using your product Registration Key, before you receive an Activation Code that allows you to begin using DCS.

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

Activation Code

An Activation Code is required to enable scanning, receive product updates, and display the status of your license in the management console. An Activation Code 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 scan and component update functions. To unlock these functions, 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. DCS functionality of standard version after license is expired

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

TABLE 3-2. DCS functionality of evaluation version

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.

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 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`)

      Note: 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`

      or in the folder that you chose during installation, if different than the default location:
      `<Destination Folder>\WebUI\DCS\DCS`

   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 Trend Micro Damage Cleanup Services Web management console opens to the Summary screen.

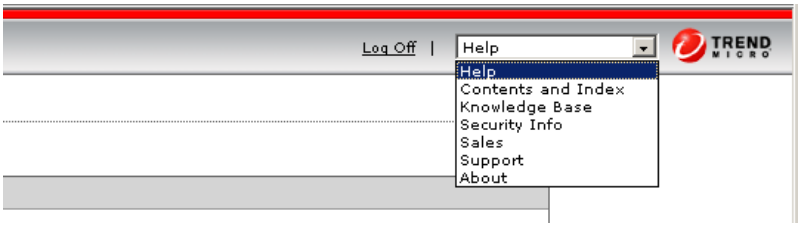
Note: The default system timeout for DCS is 900 seconds (15 minutes). You can change the timeout setting by editing the system registry. See **App. A, Troubleshooting**, page A-3, for detailed instructions.

The Web Console Interface

The Trend Micro Damage Cleanup Services 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.



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 Damage Cleanup Services, including product version, build number, Damage cleanup engine version number, Damage Cleanup template version, Spyware/Grayware pattern number, and Activation Code (if one has been entered)

The Sidebar

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

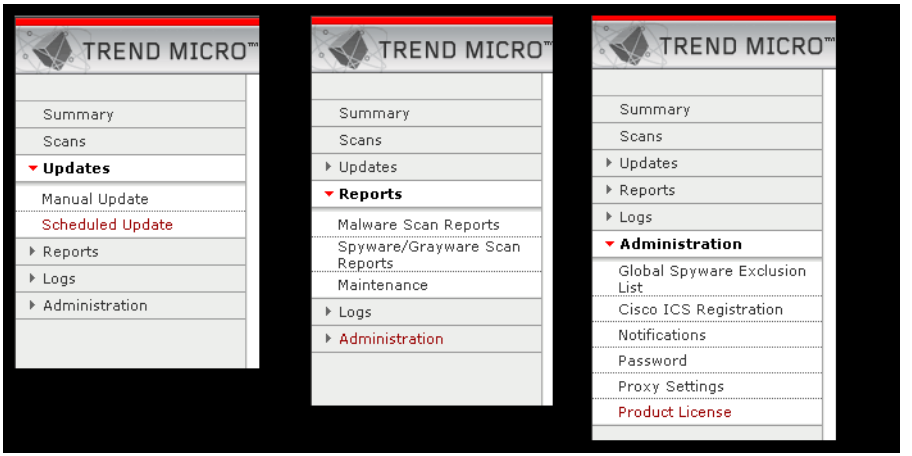


FIGURE 3-1. The DCS Web console sidebar with various menus expanded

- **Summary** - Opens the Summary screen in the main content window
- **Scans** - Opens the Scans screen showing results of any scans that have been run
- **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 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 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:
    - **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
    - **Cisco ICS Registration** - Opens the Cisco Incident Control Server (Cisco ICS) Registration screen, from which you can enter settings to allow 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.

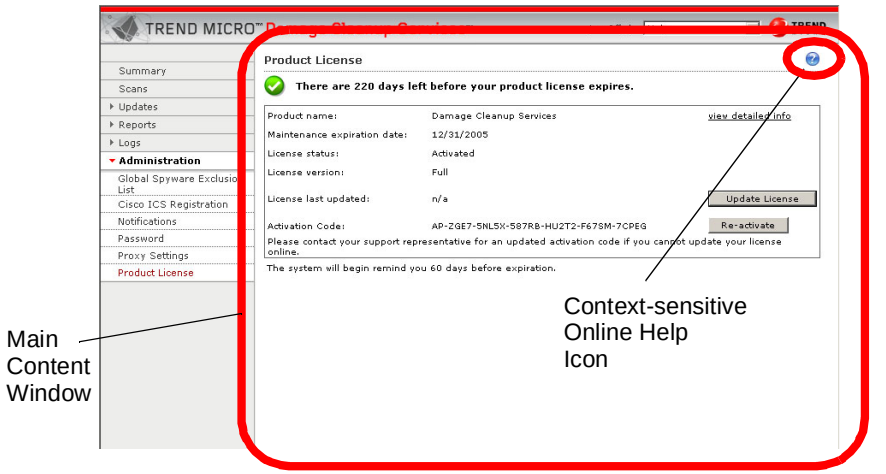


FIGURE 3-2. DCS Web management console main content window

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 Damage Cleanup Services 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 80 for HTTP and 443 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 Incident Control Server, 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.

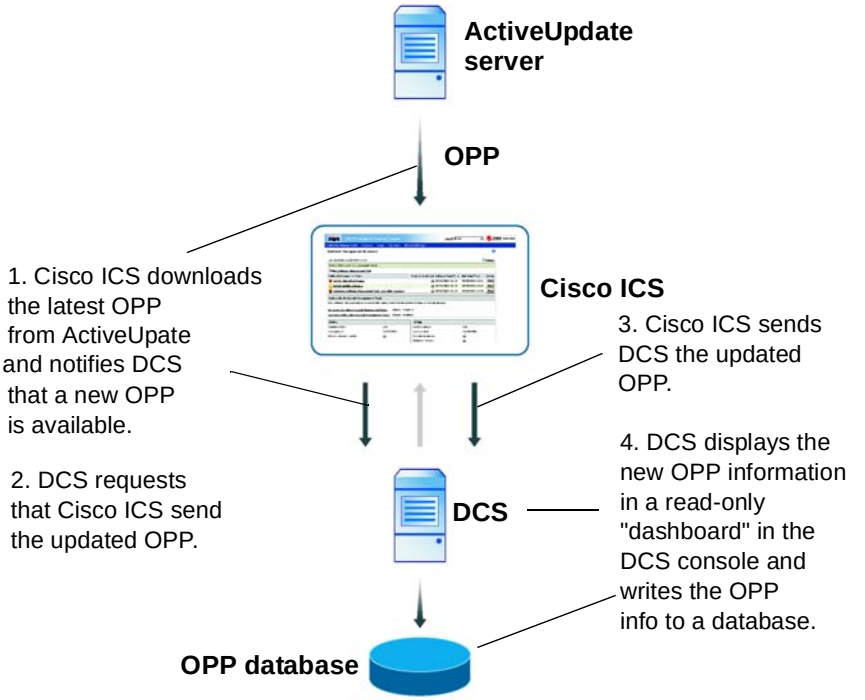


FIGURE 3-3. Delivery of OPP from ActiveUpdate through Cisco ICS to DCS

Cisco ICS and Outbreak Prevention Services

When DCS and Cisco ICS are working together, Cisco ICS obtains the outbreak prevention policy (OPP) from Trend Micro ActiveUpdate 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 3-12). 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 3-4. Outbreak Protection Policy Outbreak Alert from Cisco ICS displayed in DCS console Summary Screen

Note: Damage Cleanup Services can also work with Trend Micro InterScan Web Security Suite (IWSS). IWSS can request a cleanup from DCS. See your IWSS documentation for more information.

Getting Summary Information

After you log in to the Damage Cleanup Services (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 Damage Cleanup template, Spyware/Grayware pattern, and Damage Cleanup engine:

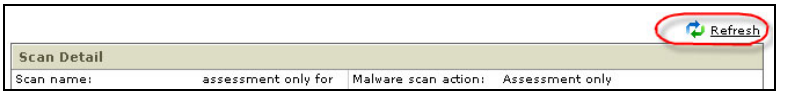
- **Current Version:** The version number of the latest component version installed
- **Latest Version:** The version number of the latest component version available
- **Status:** Success or failure of last update attempt and its time and date. If the last update attempt failed, DCS displays a link 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 2 minutes. 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 you to the default view of the Summary screen.*

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 Damage Cleanup Services (version 3.0), Trend Micro, Inc. is updating the Damage Cleanup Template about once a week.

If you are using version 3.0 with Cisco Incident Control Server or with Trend Micro Control Manager version 5, 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 3.0 to set scheduled updates to more frequently than weekly.

However, if you are using DCS 3.0 without the benefit of Trend Micro Outbreak Prevention Services, you may wish to set your update schedule to once a day or more frequently. See *Configuring Scheduled Updates for Damage Cleanup Services* on page 3-16.

Note: DCS 3.0 is a stand-alone product and is not a component of Trend Micro Control Manager version 3 (TMCM 3). If you are using TMCM 3 or earlier, DCS 3.0 is not making use of Outbreak Prevention Services.

Configuring Scheduled Updates for Damage Cleanup Services

Configure Damage Cleanup Services 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
   - Damage Cleanup template and Spyware/Grayware pattern
   - Damage Cleanup engine
4. Under Update Schedule, specify how often to perform scheduled update. 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 3-3, "Description of frequency options for scheduled updates," on page 3-16 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 3-3. 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 three components of DCS that an IT manager will want to update:

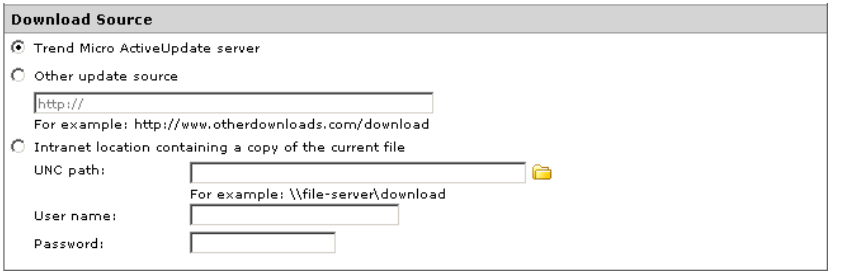
- Damage Cleanup template
- Spyware/Grayware pattern
- Damage Cleanup engine

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

To update Damage Cleanup Services 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**.



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 4

Configuring Damage Cleanup Services

This chapter covers the following topics:

Using the Account Management Tool

Use this tool to view, add, modify, or delete login credentials for the target machines and domains you wish to add in 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 domain account (see *Adding a Domain Account* on page 4-4)
- Add a machine account (see *Adding a Machine Account* on page 4-5)
- Set a default account
- Delete a domain or machine account
- Modify a domain or machine account information
- Import or export Account Management Tool settings

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. Type your administrative password and click **Login.** A list of all existing domains and the available descriptions appears.

FIGURE 4-1. The Account Management Tool Login screen

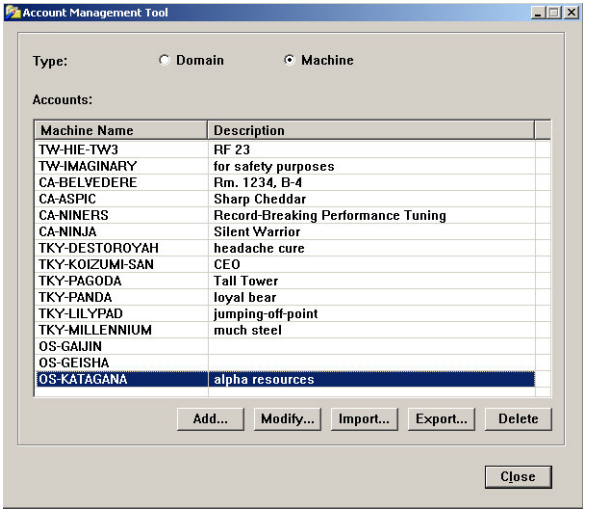


FIGURE 4-2. Use this screen to view all domain and machine accounts

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 **Login.** A list of all existing domains and the available descriptions appears.
3. For **Account type** select **Domain** or **Machine** (the default is Domain). A list of all existing domains or machines and the available descriptions appears.
4. Click **Close** to close the tool.

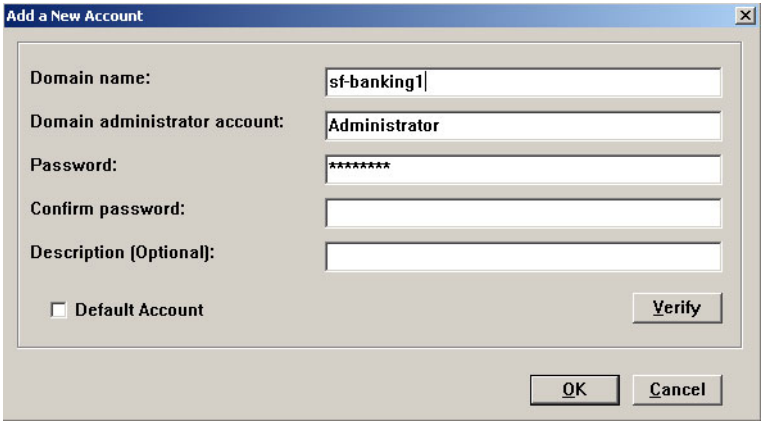


FIGURE 4-3. Account Management Tool: Add a New Domain Account

Adding 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 **Login.** A list of all existing domains and the available descriptions appears.
3. For **Account type** select **Domain** (the default choice).
4. Click **Add...** to add a domain. The Add a New Account screen appears.
5. In **Domain name** type the Windows domain name you wish to add.
6. Type the **Administrator Account.**
7. Type the **Password** for the domain administrator account and then retype it in **Confirm Password.**
8. If desired, type a description for this account in **Description.** For example, `Company domain 1.`
9. If this account is the default account, select **Default Account**. If during a scan DCS is unable to access a remote account, it will access the default account.

Note: The format of the default account must be `Domain\Account` or `Account@Domain`. If you select the current account as the default account, the Domain name field becomes disabled.

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 Domain Name column of the Accounts table.

Adding 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 **Login.** A list of all existing domains and the available descriptions appears.
3. For **Account type,** select **Machine.**
4. Click **Add...** to add a machine. The Add a New Account screen appears.

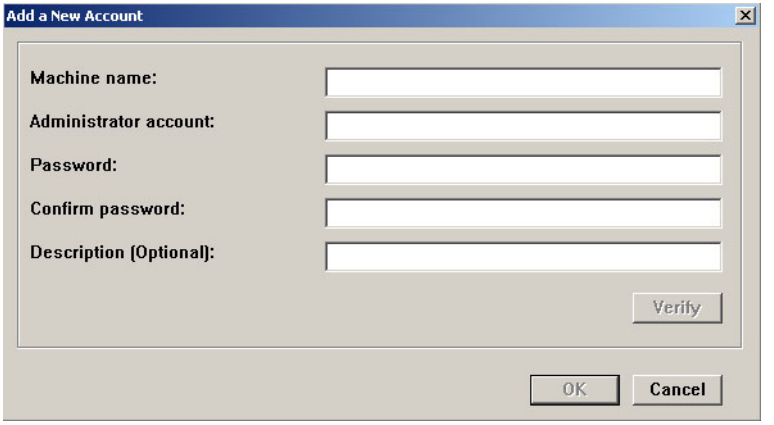


FIGURE 4-4. Account Management Tool: Add a New Machine Account

5. In **Machine name** type the machine name 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.**
9. Click **Verify** to verify that DCS can connect to the machine with the information provided. If DCS can connect to the machine, a **Connectivity verified** message appears.
10. Click **OK** to close the verification message and click **OK** to finish adding the new machine. The machine name appears in the Machine Name column of the Accounts table.

Setting a Default Account in the Account Management Tool

The Manual Damage Cleanup Tool provides for a default account. If during a scan DCS is unable to access a remote account, it will access the default account instead. Trend Micro recommends creating a default account so that DCS can run a scan even if unable to access the intended account. Using the default account in such a case

allows a scan to be completed so that the administrator can view the results of the scan and modify the scan if necessary.

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

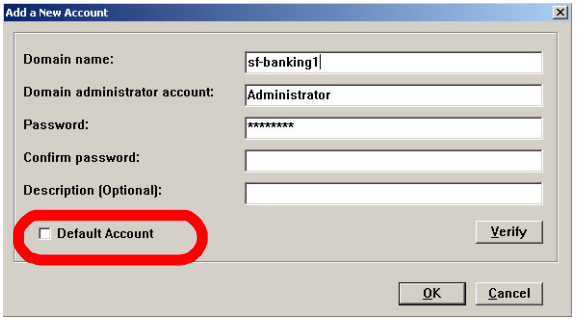


FIGURE 4-5. Location of the Default Account checkbox

Deleting 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 **Login.** A list of all existing domains and the available descriptions appears.
3. For **Account type** select **Domain** or **Machine.** A list of all existing domains or machines and the available descriptions appears.
4. Select the domain or machine you wish to remove from the accounts list.
5. Click **Delete.** The Delete Account screen appears showing name and administrator account.

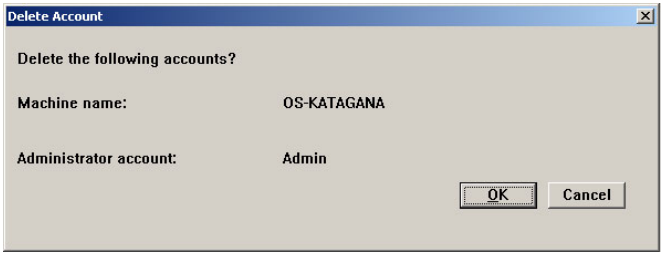


FIGURE 4-6. The Delete Account confirmation screen

6. Click **OK** to delete the account.
7. Click **OK** in the **Successfully deleted account information** message screen.

Modifying 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 **Login.** A list of all existing domains and the available descriptions appears.
3. For **Account type** select **Domain** or **Machine.** A list of all existing domains or machines and the available descriptions appears.
4. In the accounts list select the domain or machine you wish to modify.
5. Click **Modify...** The Modify Account screen appears

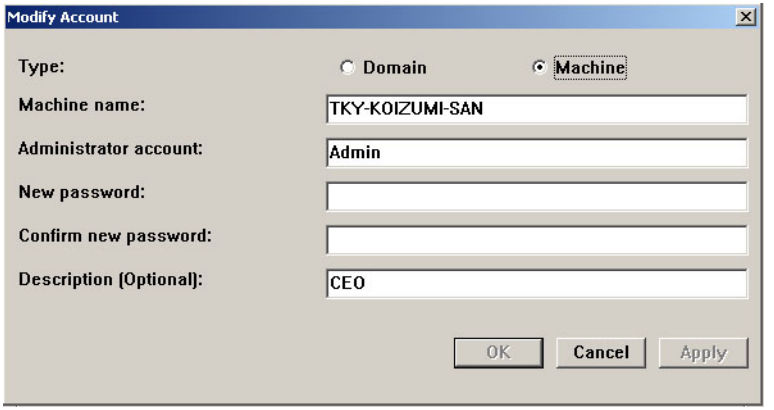


FIGURE 4-7. The Modify Account screen

6. Type the updated information in **Domain (Machine) name, Administrator account,** or **Description.**
7. If you wish to change the password, type the **New password** and then retype the new password in **Confirm new password.**
8. Click **Apply** to apply the change or **OK** to apply the change and close the Modify Account screen. The Trend Micro Account Management Tool screen appears, displaying the new information if it is in the Domain (Machine) Name or Description column.

Importing and Exporting Account Management Tool Settings

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.

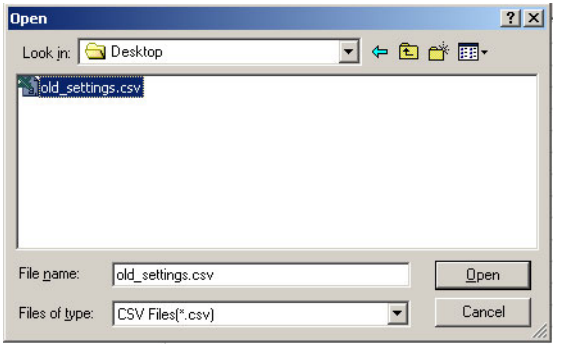


FIGURE 4-8. Importing Account Management Tool settings

To import Account Management Tool settings:

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 **Login.** A list of all existing domains and the available descriptions appears.
3. For **Account type** select **Domain** or **Machine.** A list of all existing domains or machines and the available descriptions appears.
4. Click **Import...** An Open screen appears.
5. 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.
6. Click **OK** to close the Import Complete message. The settings from your import display in the Accounts table.

To export Account Management Tool settings:

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 **Login.** A list of all existing domains and the available descriptions appears.
3. For **Account type** select **Domain** or **Machine.** A list of all existing domains or machines and the available descriptions appears.

4. Click **Export...** A Save As screen appears.
5. Navigate to the location where you wish to save your settings, type a file name, and click **Save** to export your settings.
6. Click OK to close the Export Completed message.

Managing Passwords

Passwords for Damage Cleanup Services 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 Damage Cleanup Services (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.

Adding a Scan

Using the Damage Cleanup Services 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 screen appears.
2. Click **Add Scan**. 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 4-12)
- *Step 2 of 4: Select Scan Target* (see *Selecting Scan Targets* on page 4-16)
- *Step 3 of 4: Set Schedule* (see *Setting Scan Schedules* on page 4-19)
- *Step 4 of 4: Notification* (see *Setting Notifications of Scan Completion* on page 4-19)

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 4-16**,** *Setting Scan Schedules* on page 4-19**,** and *Setting Notifications of Scan Completion* on page 4-19 before you can save your changes.

To select scan action:

1. Select **Scans** from the sidebar. The 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 Damage Cleanup Services 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 Damage Cleanup Services spyware/grayware scan looks for active spyware/grayware programs only.

7. If you would like to exclude from scanning any spyware/grayware that you would like to keep, select **Enable exclusion list** and click the exclusion list link to create or manage a list of spyware/grayware programs for the scan to ignore. (See *Choosing Spyware/Grayware to Exclude from Scans* on page 4-13.)

Choosing Spyware/Grayware to Exclude from Scans

Not all spyware or grayware is undesirable. For this reason Damage Cleanup Services 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 Scan**), 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 **Administration** > **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 Scan**), 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. Damage Cleanup Services 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 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** in sidebar. The 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 4-12).
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** from the sidebar. The 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

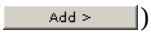
Damage Cleanup Services allows you to set scan targets by IP address, IP range, network segment and subnet mask, machine name, or network domain. Selecting scan targets is the second step in a four-step process.

Select Scan Target by Machine Name

An IT manager in some cases 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>>** (

). 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>** (

). 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>** (

). 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

Damage Cleanup Services 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>** (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>** (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:

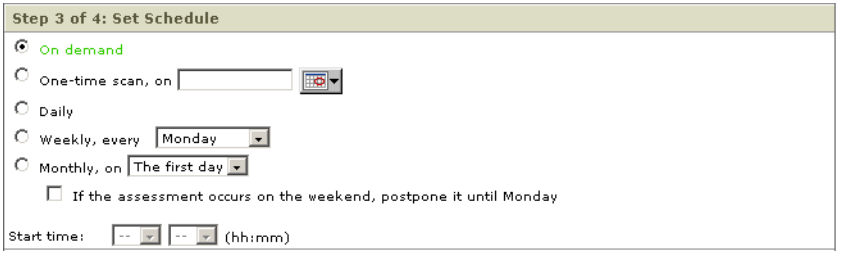
1. Click **Add/Edit Scan Target.** The Select Scan Target screen appears.
2. Under **Select machines** select **By IP address.**
3. Type a network segment in the **Segment** fields.
4. Type the subnet mask in the **Mask** fields.
5. Click **Add>** (Add >). The new network segment/subnet mask appears 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.

Setting Scan Schedules

Damage Cleanup Services allows you to set scheduled scanning.



To set scan scheduling:

1. Click **Scan** in the sidebar. The 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 4-19.)

Setting Notifications of Scan Completion

Damage Cleanup Services 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.

To customize the scan results notification message:

1. Click **Scans** in the sidebar. The 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. Customize the subject line if you like in the **Subject** field. (The default is *Trend Micro Damage Cleanup Services: [<%scan name%>] scan result summary.*)
6. Customize the information in the message body if you like, by editing the **Message** field. For details, see *Customizing Notification Messages with Variables* on page 4-25.
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 4-21)
   - Select the method(s) by which each notification type goes out

- Set the content for various notification types (see *To configure notification content:* on page 4-21)
- 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 **Damage Cleanup pattern update, Damage Cleanup 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 activates 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—
   - **Damage Cleanup pattern update**: Successful and Unsuccessful
   - **Damage Cleanup 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. If you like, modify the subject line of the message. The default is **Trend Micro Damage Cleanup Services: [Event type].**
4. If you like, modify the content of the message body. See *Customizing Notification Messages with Variables* on page 4-25.
5. Click **Save** to save your changes.

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

Setting Notification Method

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.

Note: 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 4-19.

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.

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 Page 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 4-24.
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 4-24, 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 Damage Cleanup Services 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.

Variables for Notification of Individual Scan Completion

Variable	Description
<%date/time%>	The time and date of scan completion
<%scan name%>	The name of the scan that DCS executed. Whether the execution was successful or unsuccessful makes no difference.
<%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
<%scan time%>	The time and date of a scan
<%malware damage%>	The number of machines with damage from malware
<%malware cleanup successful%>	The number of machines successfully cleaned
<%malware cleanup unsuccessful%>	The number of machines that could not be cleaned
<%malware damage free%>	The number of machines found to be free of malware
<%malware unresponsive%>	The number of machines that DCE could not contact
<%malware total%>	The total number of machines targeted for a malware scan
<%spyware damage%>	The number of machines with damage from spyware/grayware
<%spyware cleanup successful%>	The number of machines successfully cleaned
<%spyware cleanup unsuccessful%>	The number of machines that could not be cleaned
<%spyware damage free%>	The number of machines found to be free of spyware/grayware
<%spyware unresponsive%>	The number of machines that DCE could not contact
<%spyware total%>	The total number of machines targeted for a spyware/grayware scan

TABLE 4-1. 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 Damage Cleanup template in use by DCS
<%dct latest version number%>	The version number of the latest Damage Cleanup template available for download by DCS
<%dct status%>	The update status of the Damage Cleanup template in use by DCS
<%spy current version number%>	The version number of the spyware/grayware pattern in use by DCS
<%spy latest version number%>	The version number of the latest spyware/grayware pattern available for download by DCS
<%spy status%>	The update status of the spyware/grayware pattern in use by DCS

TABLE 4-2. 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 Damage Cleanup template in use by DCS
<%dct latest version number%>	The version number of the latest Damage 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 Damage Cleanup template, the reason for the error, and the Trend Micro recommended action to correct the error
<%dct status%>	The update status of the Damage Cleanup template in use by DCS
<%spy current version number%>	The version number of the spyware/grayware pattern in use by DCS
<%spy latest version number%>	The version number of the latest spyware/grayware pattern available for download by DCS
<%spy status%>	The update status of the spyware/grayware 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/grayware pattern, the reason for the error, and the Trend Micro recommended action to correct the error

TABLE 4-3. 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 Damage Cleanup engine in use by DCS
<%dce latest version number%>	The version number of the latest Damage Cleanup engine available for download by DCS
<%dce status%>	The update status of the Damage Cleanup engine in use by DCS

TABLE 4-4. 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 Damage Cleanup engine in use by DCS
<%dce latest version number%>	The version number of the latest Damage Cleanup engine available for download by DCS
<%dce status%>	The update status of the Damage Cleanup engine in use by DCS
<%dce cause%>	An error message that provides users with a description of the error that the Damage Cleanup engine encountered, 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 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 4-6. 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 4-7. 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 Damage Cleanup Services 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 4-8. Variables available for customizing notifications of type: Outbreak Alert Has Been Activated

Chapter 5

Running Scans

This chapter contains the following topics:

Running a Scan 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** in the sidebar. The 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.
4. To stop the scan after it has begun, click **Stop the Scan.**

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

To run two or more scans manually:

1. Click **Scans** in the sidebar. The 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.**

Note: Damage Cleanup Services 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.

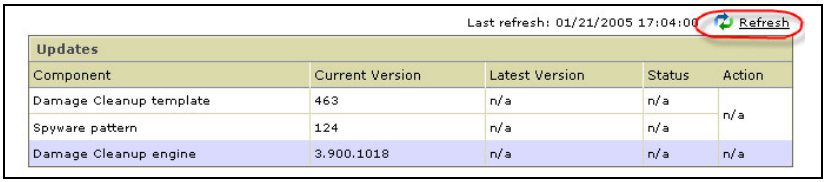
Viewing the Scan Results Summary

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

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.

Note: The screen refreshes automatically every 2 minutes. 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.



Viewing Scan Results Details

Damage Cleanup Services 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 when you run a scan manually:

1. In the sidebar, click **Scans.** The 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 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 machines to scan:** The total number of machines intended for scanning
- **Malware scan action:** "Assessment only" or "Assessment with cleanup"
- **Spyware/grayware scan action:** "Assessment only" or "Assessment with cleanup"
- **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:** (appears in the table linked to from the Total number only; not applicable for others, because Scan Result is the criteria that divides the above categories.)
- **Malware (Spyware/Grayware) Detected:** The Trend Micro name for the specific malware or spyware/grayware program found (appears in all tables except that generated by the Unresponsive link)

You can use this screen to manually clean any machine found with damage if its Scan Result status is Cleanup Unsuccessful or Unresponsive.

Note: In the Scan Result for Malware screen, any scan that you clean with the **Cleanup Now** feature will clean only malware. Likewise, in the Scan Result for Spyware/Grayware screen, any scan that you clean with the **Cleanup Now** feature will clean only spyware/grayware.

To manually clean up a machine listed in this table:

1. Select the machine or machines that you would like to manually clean.
2. Click  **Cleanup 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

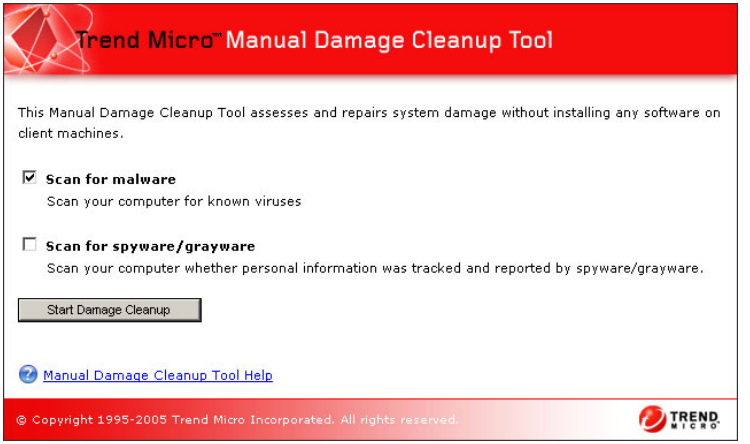
The Manual Damage Cleanup tool allows users of individual client machines to perform a cleanup task on a Microsoft Windows-based machine upon demand. Users can assess and cleanup their machine(s) without the system administrator's intervention. This ability could be useful if Damage Cleanup Services 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).

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

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

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

- Windows 95
- Windows 98
- Windows ME
- Windows NT 4 Server/Workstation with Service Pack 6
- Windows 2000 Professional/Server/Advanced Server with Service Pack 3
- Windows XP Home/Professional
- Windows 2003 Server Standard/Enterprise Edition



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 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 Damage Cleanup Services to limit the number of recent reports to save.

To perform report maintenance:

1. On the sidebar, click **Reports** > **Maintenance.** The Report Maintenance screen appears.
2. Under Malware Scan Report, select **Maximum number of reports to keep** and in the accompanying field specify the number of most recent reports to keep. The default value is 500 reports.
3. Under Spyware/Grayware Scan Report, select **Maximum number of reports to keep** and in the accompanying field specify the number of most recent reports to keep. The default value is 500 reports.
4. Click **Save** to save your changes.

Managing Malware Scan Reports

You can use Damage Cleanup Services (DCS) to generate many 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 Generated 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 scans 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 the email address of all 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**. Damage Cleanup Services 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 checkmark 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 checkmark 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 checkmark 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 Generated 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, 2005/01/04 12:00:00) in the **Report Generated On** column. A download window opens.

Note: Although DCS generates reports only in Adobe Acrobat `.PDF` format, if DCS generates two or more reports 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 many 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 6-8
- *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 6-9

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, first 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 the email address of all 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 checkmark 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 checkmark 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 checkmark 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, 2005/01/04 12:00:00) in the **Report Generated On** column. A download window opens.

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

Generating a Report Manually

IT managers can use Damage Cleanup Services to generate many different kinds of reports. In addition to setting scheduled reports, you can also generate a report manually.

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.

Analyzing Your Protection Using Logs

Damage Cleanup Services keeps comprehensive logs about virus incidents, events, and updates. Use these logs to assess your organization's virus protection policies and to identify devices that are at a higher risk of infection. Also use these logs to check the device-server connection and verify that updates deployed successfully.

Running Log Queries

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 or Trend Micro InterScan Web Security Suite 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 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.
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. 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 or Trend Micro InterScan Web Security Suite 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 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.
5. Click the **More Searching Criteria** link. Additional detailed input fields appear.
6. 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
7. Select the number of logs per page that you wish to display.
8. Click **Search.** A Query Result table appears.

Exporting Log Queries

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. Damage Cleanup Services generates a .CSV file for you to download.

Appendix A

Troubleshooting and Technical Support

Frequently Asked Questions

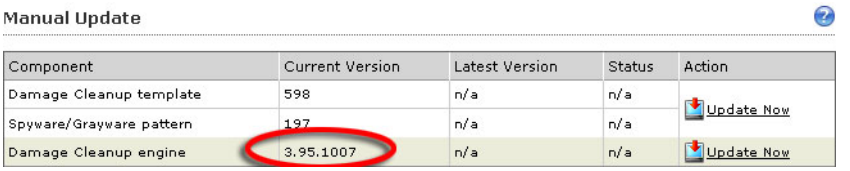
Review these frequently asked questions for insight into issues that many users ask about.

Product Information, Updating, and Compatibility

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

To determine the product version of your Damage 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 Damage 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?

No, you cannot. This release of Damage Cleanup Services is a standalone product. It does not communicate with Trend Micro Control Manager 3. See *What's New in Damage Cleanup Services 3.0* on page 1-3 for more information.

Installation and Initial Settings

Can I install DCS 3.0 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 5-9.

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.

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

scan and component update functions. To unlock these functions, 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-1. DCS functionality of standard version after license is expired

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

TABLE A-2. DCS functionality of evaluation version

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.

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** > **Debug** > **Server**
4. Double-click **ClientDebugLevel.** The **Edit DWORD Value** screen opens.
5. In **Value** data type **1**.
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` 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
```

Default Locations of Debug Logs

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

Debug log	Location
DCS engine	<OS drive>:\<DCSDir>\<DCS server name>\Debug\TSCDebug.log
DCS service	<DCSDir>\DebugLog\
Account Management Tool	<DCSDir>\DebugLog\
Web User Interface	<DCSDir>\WebUI\DebugLog\
Deploy engine	<DCSDir>\DebugLog\rm_HVAEngine.log
Manual Assessment	<WinDir>\RMXDebug.log on client machines
ActiveUpdate download	<DCSDir>\AU_Log\
DCS installation and uninstallation	<OS drive>:\\DCS_Install.log and <OS drive>:\\DCS_Uninstall.log
MSDE installation	<OS drive>:\\DCS_MSDE_Setup.log

TABLE A-3. 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:

`kb.trendmicro.com/solutions/`

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

- Asia/Pacific
- Australia and New Zealand
- Europe
- Latin America
- United States and Canada

Follow the instructions for contacting support in your region.

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 ACS server 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 programs, 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 are also often installed in tandem with spyware programs. Both programs feed off of each other's functionalities - 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 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 OfficeScan client 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 Devices.

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 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 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

N

O

P

R

S