APPENDIX C

Using CSC SSM with Trend Micro Damage Cleanup Services

Trend Micro InterScan for CSC SSM works with Trend Micro Damage Cleanup Services (DCS) as part of an enterprise protection strategy. The CSC SSM works with DCS Versions 3.1 and 3.2.

This appendix includes the following sections:

About Damage Cleanup Services

This section includes the following topics:

DCS is a comprehensive service that helps assess and clean system damage without installing software on client computers in a network. DCS removes network viruses that can re-attack the network, and performs the following functions:

- Removes unwanted registry entries created by worms or Trojans.
- Removes memory-resident worms or Trojans.
- Removes active spyware and grayware.
- Removes rootkits.
- Removes garbage and viral files dropped by viruses.
- Assesses a system to decide whether it is infected or not.

- Returns a system to a clean state.
- Can register to Cisco Incident Control Server (ICS) and Cisco Security Monitoring, Analysis and Response System (MARS).
- Can act on clean-up requests from the CSC SSM and MARS.
- Detects spyware and grayware.

Who Should Use DCS?

DCS is designed for IT managers and administrators of medium-to-large computer networks. For DCS to find and clean active Trojans, worms, and spyware or grayware in memory, you need to install required software on client machines. A single DCS server can deploy its updated clean-up engine, when needed, to all Windows PCs in the network. Individual users need not even be aware that DCS is doing its job. If 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), you can have users click a URL that activates a special manual damage cleanup tool to scan and clean a particular client, and then return the resulting scan log to the DCS server.

How Does DCS Access Client Machines?

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

- The virus cleanup template, which contains patterns used to identify Trojans and network viruses
- The spyware pattern, which DCS uses to intelligently identify active spyware programs
- The virus cleanup engine, which DCS deploys to each client machine at the time of scanning
- The spyware scan engine, which DCS deploys to each client machine at the time of scanning
- The anti-rootkit driver, which detects and removes rootkit programs

Note DCS uses the NetBIOS protocol to resolve client machine names.

Machines That DCS Can Scan

DCS can deploy cleanup and assessment tasks to the following systems:

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

Web Browser Requirements

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

DCS Documentation

This appendix gives a brief overview of how Damage Cleanup Services works with CSC SSM. To access the full documentation set for DCS, use the documentation that shipped with the product, the online help in the product, or the following link.

The complete set of print documentation for Damage Cleanup Services is available at the following URL:

http://www.trendmicro.com/download/product.asp?productid=48

Network Scenarios

This section shows network scenarios in which you can deploy DCS, and includes the following topics:

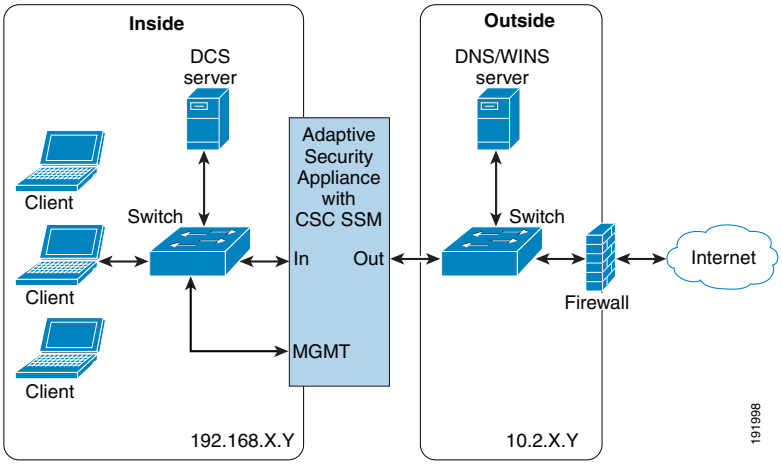
Note HTTP requests must travel through the ASA on Port 80 for CSC SSM to notice suspicious activity. Only clients on the inside network will trigger scans from CSC SSM. For information about how to trigger remote client scans, see DCS Documentation.

Most Common Network Scenario

The network scenario depicted in Figure C-1 has these physical attributes:

- Clients are in the “inside” network.
- The CSC SSM interface is on the “inside” network.
- DCS is on a server in the “inside” network.
- The DNS/WINS server is on the “outside” network.

Figure C-1 Most Common Deployment



In this scenario, note the actions and configurations described in Table C-1.

Table C-1 Common Deployment Actions and Configurations

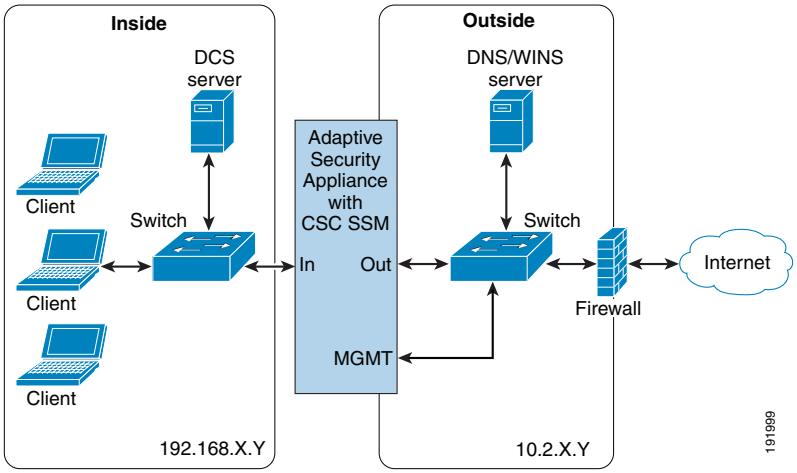
Action	Special Configuration
Registering or unregistering CSC SSM to DCS	None
Remote client cleanup	Requires that the target PCs belong to a Windows domain. An additional configuration file must be manually added to DCS to map client IP addresses to domains. See Adding the ExtraMachineDomainList.ini File, page C-7 for details. In addition, the configuration of the Windows firewall on client PCs must allow file and printer sharing and ICMP echo.
Client redirect to the manual cleanup page	None
DCS transmissions of scan results to the CSC SSM	None

Network Scenario Alternative 2

Network scenario alternative 2, depicted in Figure C-2, has the following physical attributes.

- Clients are in the “inside” network.
- The CSC SSM is “outside.”
- DCS is “inside.”
- The DNS/WINS server is “outside.”

Figure C-2 Alternative #2



In this scenario, note the actions and configurations in Table C-2.

Table C-2 Network Scenario #2 Actions and Configurations

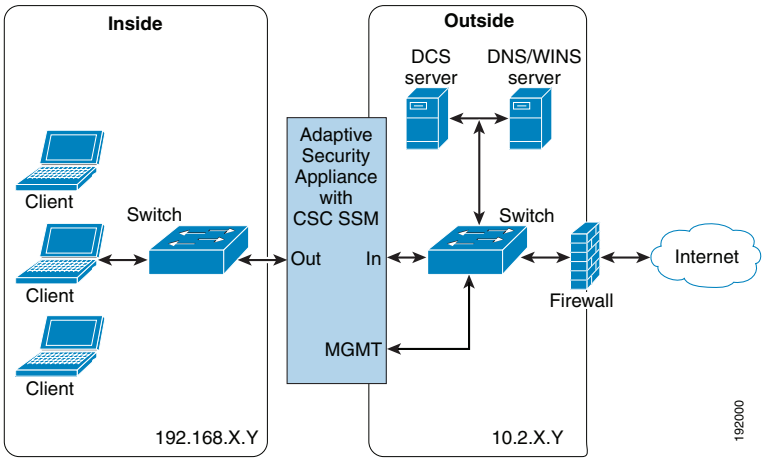
Action	Special Configuration
Registering or unregistering CSC SSM to DCS	A forwarding rule must be added to the security appliance to allow access from outside to DCS GUI on the inside.
Remote client cleanup	A forwarding rule must be set up to allow registration. Has the same restrictions as the most common deployment.
Client redirect to the manual cleanup page	The forwarding rule must be set up to allow registration.
DCS transmissions of scan results to the CSC SSM	The forwarding rule must be set up to allow registration.

Network Scenario Alternative 3

Network scenario alternative 3, depicted in Figure C-3, has the following physical attributes.

- Clients are in the “inside” network.
- The CSC SSM is in the “outside” network.
- DCS is in the “outside” network.
- The DNS/WINS server is in the “outside” network.

Figure C-3 Alternative #3



In this scenario, note the actions and configurations in Table C-3.

Table C-3 Network Scenario #3 Actions and Configurations

Action	Special Configuration
Registering or unregistering CSC SSM to DCS	None
Remote client cleanup	Will not work. The DCS does not see the client IPs at all and cannot use the mapping file to match them to a domain.
Client redirect to the manual cleanup page	None
DCS transmissions of scan results to the CSC SSM	None

Getting Started

The following tasks must be completed for CSC SSM to register to DCS.

- Registration and Activation of DCS, page C-6
- Setting up Accounts, page C-7
- Adding the ExtraMachineDomainList.ini File, page C-7
- Verifying Firewall Security on Target Machines, page C-9
- Registering CSC SSM to DCS, page C-9

Registration and Activation of DCS

DCS is available at the following URL:

http://us.trendmicro.com/us/products/enterprise/damage-cleanup-services/

Registration and activation information are available in the DCS product documentation. For information about logging on using the DCS console and querying logs, see DCS Interface, page C-10.

Setting up Accounts

Using the DCS Account Management Tool, add entries for accounts on each domain that has local administrative privileges for machines to be scanned.

To add a domain or machine account, perform the following steps:

Step 1 To open the Account Management Tool, choose **Start > Programs > Trend Micro Damage Cleanup Services > Account Management Tool**.

The Login screen appears.

Step 2 Type your DCS administrative password and click **Log On**.

A list of all existing accounts appears, showing account type and the available descriptions.

Step 3 Click **Add** to add an account.

The Add Account screen appears.

Step 4 Under Select the type of account to add, select what kind of account to add by accepting the default choice of Domain account or by choosing **Machine account**.

Step 5 If the account is a domain account and you would like to use it as the default account, check the **Make this account the default account** check box.

Note If, during a scan, DCS is unable to access a remote machine using the account for that machine, DCS uses the default account to access the machine. Because only a domain account can be a default account, this option is disabled for machine accounts.

Step 6 In the Domain name field, type the name of the domain or machine account.

Step 7 Type the administrator account.

Step 8 Type the password for the administrator account, and then retype it to confirm the entry.

Step 9 (Optional) Type a description for this account (for example, Company domain 1).

Step 10 Click **Verify** to verify that DCS can connect to the domain with the information provided. If DCS can connect to the domain, a **Connectivity to client verified** message appears.

Step 11 Click **OK** to close the verification message, and click **OK** to finish adding the new domain.

The account name appears in the Name column of the Accounts table.

Step 12 Click **Close** to close the Account Management Tool.

Adding the ExtraMachineDomainList.ini File

DCS uses NetBIOS lookups to determine hostnames of PCs that have been targeted for cleanup by external applications (such as TMCM and Cisco ICS) when those applications provide only the target IP address. This method of hostname resolution may fail, particularly if the network WINS server resides on a different network segment with NAT between the WINS server and the clients (both DCS and the target PC).

If your target PCs are part of a Windows domain, you can still use remote cleanup with some additional configuration on both DCS and the clients.

To specify the domain of particular machines by IP address or IP range, place a file named ExtraDomainMachineList.ini into the DCS root folder. DCS uses the domain account type in the Account Management Tool to access those machines and scan them automatically.

Note This file is necessary for deployments using NAT.

To verify that you need to create the ExtraMachineDomainList.ini file, perform the following steps:

Step 1 On your DCS server, to resolve the client machine name using its IP address, issue the **nbtstat** command from a DOS command prompt:

```
c\: nbtstat -A [Client IP Address]
```

Step 2 If the DCS server cannot resolve the client machine name, make sure that the NetBIOS protocol over TCP/IP on the client and DCS server machines is enabled.

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

You can also place a file named ExtraDomainMachineList.ini into the DCS root folder to specify the domain of particular machines by IP addresses or IP range.

Step 3 Create a file named ExtraDomainMachineList.ini in the DCS installation directory. For example:

```
[domain_name1}
IP=10.2.2.2
IPRange=10.2.4.1-10.2.4.255
[domain_name2]
IP=10.2.2.1
```

Step 4 In the ExtraDomainMachineList.ini file, specify your Windows domains and the list of machine IP addresses that belong to each domain. Use only the top-level domain name. FQDNs are not supported. Use the format shown in Table C-4:

Table C-4 Elements Used in the ExtraDomainMachineList.ini File

Element	Description
[domain_name1]	The domain name of the IP address or IP range under this section.
IP=10.1.1.1	The IP address that is specified for the domain.
IP=10.2.2.2	Another IP address that is specified for the domain.
IPRANGE=10.1.1.1-10.1.1.255	The IP range that is specified for the domain.
IPRANGE=1.1.1.1-255.255.255.255	Another IP range that is specified for the domain.
[domain_name2]	The second domain name of the IP address or IP range under this section.
IP=10.3.3.3	The IP address that is specified for the second domain.

Table C-4 Elements Used in the ExtraDomainMachineList.ini File (continued)

Element	Description
IPRANGE=10.3.3.3-10.3.3.255	The IP range that is specified for the second domain.
IPRANGE=10.3.3.3-255.255.255.255	Another IP range that is specified for the second domain.

Verifying Firewall Security on Target Machines

DCS uses ICMP echo to verify the route to a target machine, and Windows RPC to log in and clean the targeted PC. Windows Firewall (or other software firewalls) on the target machine may interfere with this process.

To verify firewall security on targets machines, perform the following steps:

Step 1 Verify the firewall applications that are installed on the client or DCS server machine.

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

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

Step 2 Check and open TCP ports 139 and 445 and UDP ports 137 and 138, or enable File and Printer sharing in the exception list on the Exceptions tab in Windows Firewall. DCS makes use of these ports to communicate with clients.

Step 3 If your target PCs have Windows Firewall enabled, be sure that **Allow incoming echo request** check box is checked in the ICMP Settings dialog box on the Advanced tab of the Windows Firewall configuration dialog box.

Registering CSC SSM to DCS

For CSC SSM to acknowledge DCS, the CSC SSM must register to DCS.

To register CSC SSM to DCS, perform the following steps:

Step 1 In the CSC SSM console, go to **Administration > Register to DCS**.

Step 2 Click **Enable**.

Step 3 Enter the DCS server name or IP address in the appropriate field, and then click **Add**.

Step 4 Enter the port number.

Step 5 If a cleanup failure occurs, you can redirect the client to DCS by checking the check box near the bottom of the screen.

Unregistering CSC SSM from DCS

You can unregister from DCS if your DCS server changes or if you no longer need DCS.

To unregister the CSC SSM from DCS, perform the following steps:

Step 1 In the CSC SSM console, go to **Administration > Register to DCS**.

Step 2 In the registration table, click the **Delete** icon beside the registered DCS server name or IP address.

DCS Interface

This section describes the DCS interface, and includes the following topics:

Managing DCS through TMCM

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

Immediately after you click **Finish** in the InstallShield Wizard Completed screen, a prompt appears, asking if you want to manage DCS by using Trend Micro Control Manager. Click **Yes** to allow Trend Micro Control Manager to manage DCS.

Accessing DCS

DCS can serve as a stand-alone product, and no longer depends on Trend Micro Control Manager for configuration and use. DCS has its own web-based management console.

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

To log on to the DCS web management console, perform the following steps:

Step 1 Launch the DCS web console in one of the following three ways:

- From the Windows Start menu of the host on which DCS is installed, choose **Start > Programs > Trend Micro Damage Cleanup Services > Trend Micro Damage Cleanup Services**.
- Go to the URL of your installed DCS web console: (http://<Your_DCS_Server_Machine>/DCS/cgiDispatcher.exe)

Tip For convenience, you may want to add this URL to your Favorites list in Microsoft Internet Explorer web browser.

- Double-click the Internet shortcut file created by your installation in the default Destination Folder:

  <OS_drive>\Program Files\Trend Micro\DCS\WebUI\DCS\DCS.url

  or in the folder that you chose during installation, if this is different from the default location:

  <Destination Folder>\WebUI\DCS\DCS.url

The DCS web console opens in a Microsoft Internet Explorer browser window.

Step 2 Type the Administrator password that you chose when installing the program, and press **Enter** or click **Log On**.

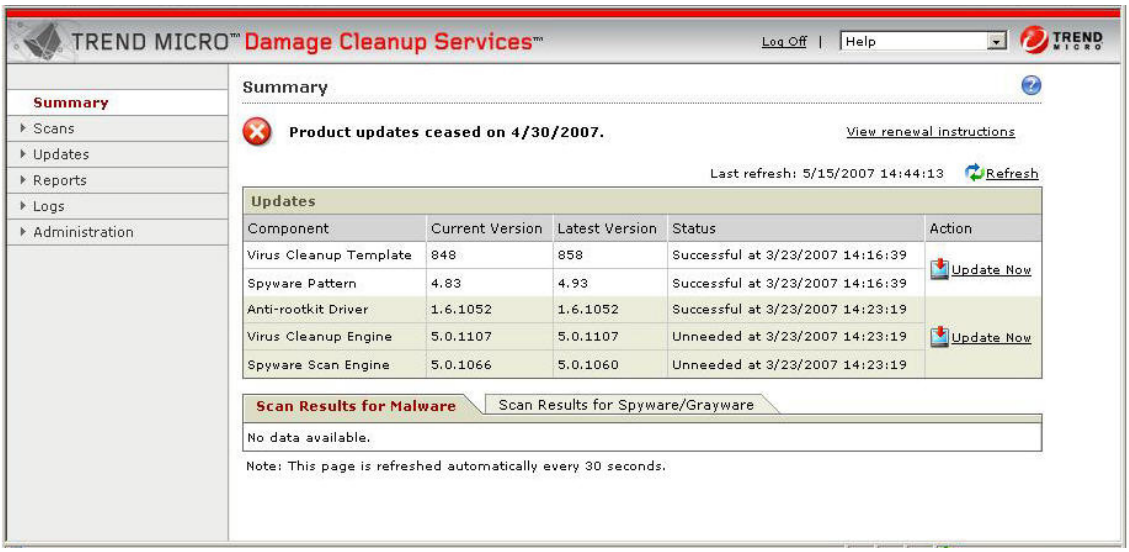
The Trend Micro Damage Cleanup Services web management console opens to the Summary screen.

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

When you log in to DCS, the Home window appears, as shown in Figure C-4.

Note When you access a secure DCS site, it automatically sends you its certificate, and Internet Explorer displays a lock icon in the status bar.

Figure C-4 The DCS Console Home Window.



Registering DCS to Cisco ICS

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

Note For information about how CSC SSM can register to MARS, go to the following URL:

http://www.trendmicro.com/download/product.asp?productid=48

To register DCS to Cisco ICS, perform the following steps:

Step 1 From the DCS management console, choose **Administration > Cisco ICS Registration**.

The Cisco ICS Registration screen appears.

Step 2 Type the server name or IP address.

Step 3 Select the type of HTTP you would like to use for communication between DCS and Cisco ICS. The available options are HTTP and HTTPS.

Step 4 Choose the port number of the Cisco ICS. The defaults are 8080 for HTTP and 4343 for HTTPS.

Step 5 Type the virtual directory of the Cisco ICS CGI program.

Step 6 Type the update directory for Cisco ICS.

Step 7 Choose the **DCS Notification URL host** from the drop-down list.

Step 8 Click **Register Now**.

DCS registers itself to the Cisco ICS.

Unregistering DCS from Cisco ICS

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

To unregister DCS from Cisco ICS, perform the following steps:

Step 1 From the DCS management console, choose **Administration > Cisco ICS Registration**.

The Cisco ICS Registration screen appears.

Step 2 Click **Unregister Now**.

DCS unregisters with Cisco ICS.

Querying and Viewing DCS Logs in the CSC SSM

To query and view managed product logs, perform the following steps:

Step 1 From the CSC SSM console, choose **Logs > Query**.

Step 2 Choose **Damage Cleanup Services** from the Log type drop-down list.

Step 3 Choose **HTTP** from the Protocol drop-down list.

Note HTTP is the only supported protocol for DCS logging.

Step 4 Choose the time period, either **All** or a range of dates.

Step 5 Click **Display Log**.

The Damage Cleanup Services Log screen displays the results in a table.

Step 6 Using the links at the top of the screen, you can do the following:

- Initiate a new query.
- Print the current results.
- Export results in a CSV format.
- Refresh the screen.

For additional information and instructions about using DCS, see the DCS online help or the *Damage Cleanup Services Administrator's Guide*.

Troubleshooting DCS Scan Failures

If the scan cannot find a targeted client machine, and the cause is not readily apparent, try the following troubleshooting techniques.

To troubleshoot a scan failure, perform the following steps:

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

```
c\: ping [Client IP Address or Machine Name]
```

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

Step 2 Verify whether firewall applications are installed on the client or DCS server machine. For details, see Verifying Firewall Security on Target Machines, page C-9.

Step 3 Use the following command to resolve the client machine name using its IP address.:

```
c\: nbtstat -A [Client IP Address]
```

Step 4 If the command cannot resolve the client machine name, make sure that the following items have been completed:

- The NetBIOS protocol over TCP/IP on the client and DCS server machines is enabled.
- DCS makes use of the NetBIOS protocol to resolve machine names. If the NetBIOS protocol is disabled on the server side, the server cannot enumerate any client machines. If NetBIOS is disabled on the client side, then the client will not be enumerated and will not appear in the scan result.
- Aside from enabling the NetBIOS protocol over TCP/IP, you can also place a file named ExtraDomainMachineList.ini into the DCS root folder to specify the domain of particular machines by IP address or IP range. For details, see Adding the ExtraMachineDomainList.ini File, page C-7.

Note If your system uses NAT, you must create an ExtraMachineDomainList.ini file.

Step 5 Verify that the WINS server in the network is working correctly.

Step 6 Verify that the DNS server in the network is working correctly.

Step 7 Use the UNC path to log on to the client machine and access the default shared folder, and then copy a file to that machine:

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

If the DCS server cannot log on to the client machine and copy a file, check the account privilege and the security policy settings of the machine or domain.

Step 8 Enable ICMP. DCS uses ICMP to detect the existence of a client machine. If ICMP has been blocked, then DCS cannot find the client.