



# Using CSC-SSM 6.2 with Trend Micro Damage Cleanup Services

Setup Guide

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes, and the latest version of the applicable user documentation, which are available from the Trend Micro Web site at:

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

Trend Micro, the Trend Micro logo, and Damage Cleanup Services are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 1995-2008 Trend Micro Incorporated. All rights reserved.

## Abstract

This document describes how to configure CSC-SSM 6.2 Content Security to work with Trend Micro's Damage Cleanup Services.

## Document Modifications

Revision	Name	Date	Comments
1	<i>Erwin Benavidez</i>	<i>9/06/07</i>	<i>CSC 6.2 with DCS</i>

# Contents

Contents .....	3
Required Resources .....	4
Exercise 1: Equipment Verification .....	5
1.1: Document Conventions .....	5
1.2: Network Layout .....	5
Exercise 2: Registration and Activation of DCS .....	6
Exercise 3: Setting Up DCS Accounts .....	6
Exercise 4: Registering CSC-SSM to DCS .....	9
Un-registering CSC-SSM from DCS .....	10

## Required Resources

The following are required to perform/complete this exercise.

### Software Requirements:

- Cisco Adaptive Security Appliance software version 7.1 (2)
- CSC-SSM version 6.2 (Build# 1599)
- Operating system and applications:
  - o MS Windows 2003 Server Standard Edition SP1 with the latest hot fixes  
**or** MS Windows XP Professional Edition SP2 with the latest hot fixes
  - o Windows Internet Explorer 6.0 (or higher)
  - o Cisco ASDM launcher version 1.4 (7)
  - o Trend Micro DCS

### File Requirements:

- DCS32\_1023\_Repack3.zip

### Hardware Requirements:

- 1 Unit Cisco Adaptive Security Appliance ASA5510 with Content Security and Control (CSC) - Security Services Module SSM10
- 2 Units personal computer/laptop each with:
  - o 256 MB or RAM or higher
  - o 1 Fast Ethernet LAN adapter
  - o 2 Gig free disk space
  - o At least 256 color screen and a minimum of 800x600 pixels of resolution
  - o Keyboard and mouse
- Unit layer-2 Fast Ethernet switch (4 ports at least)
- 3 Sets (straight-through) Ethernet cables
- 1 Set (crossover) Ethernet cable
- 1 Set rollover (console patch) cable with DB9 serial connector
- One of the PCs must have a serial communications port

# Exercise 1: Equipment Verification

## 1.1 Document Conventions

This document presumes that you will be installing your Cisco ASA appliance in a test network laboratory with the device settings illustrated in Figure 1, and that your Cisco ASA has working PIX and ASDM images in it. Where your IP addresses and other system configuration settings differ from this example, you will need to replace settings in the PIX and InterScan configuration commands with your system parameters. Command fields surrounded by < > braces indicate field variables that require values corresponding to your system's settings.

## 1.2 Network Layout

The PIX firewall will be configured to allow all outgoing TCP, UDP and ICMP traffic. The ASA inside network interface will have an IP address of 192.168.0.2/24 and a single PC attached to it (through a Fast Ethernet switch) with an IP address of 192.168.0.11/24. The DCS server will be installed and configured later into the machine in the internal network using the DCS configuration guide that can be downloaded from <http://www.trendmicro.com/download/product.asp?productid=48>. The ASA outside network interface will have an IP address of 10.0.0.1/24 and a single PC attached to it with an IP address of 10.0.0.10/24. The SSM management port will connect to the Fast Ethernet switch in the inside network and will have an IP address of 192.168.0.6/24. The ASA console port will be connected with a rollover cable (with a DB9 connector) to the serial port (COM) of the PC attached to the inside network.

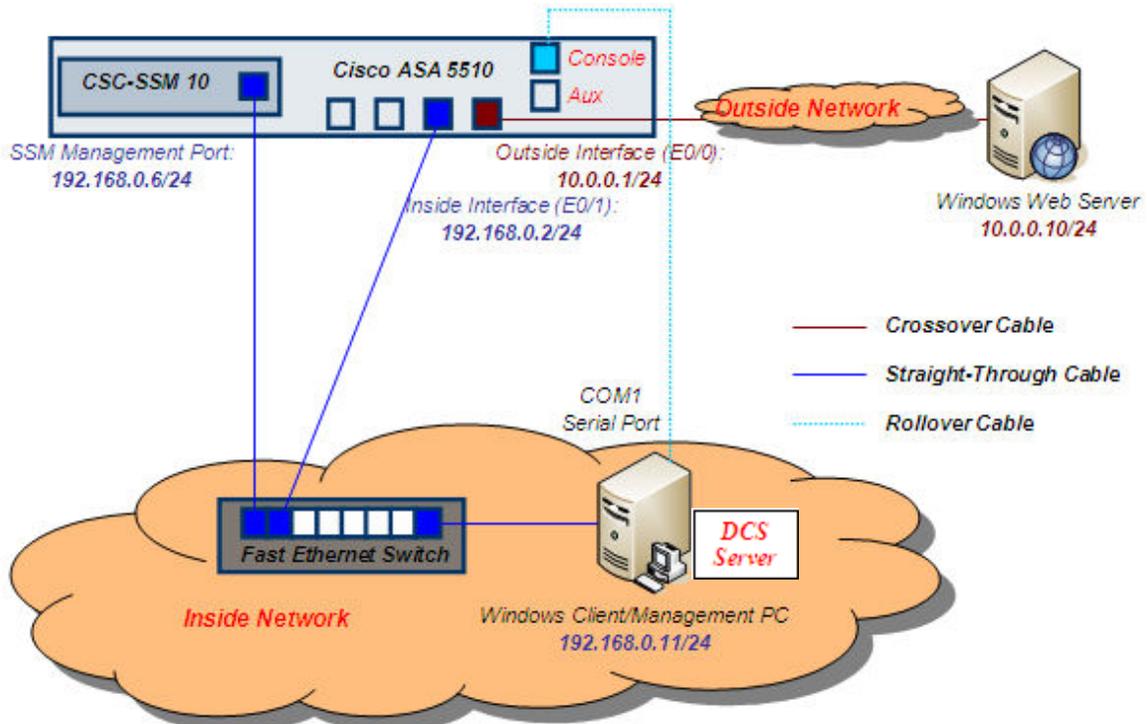


Figure 1: ASA with CSC-SSM Sample Network Layout

## Exercise 2: Registration and Activation of DCS

DCS is available at the following link:

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

Registration and activation information are available in the DCS product documentation.

## Exercise 3: Setting Up DCS 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.

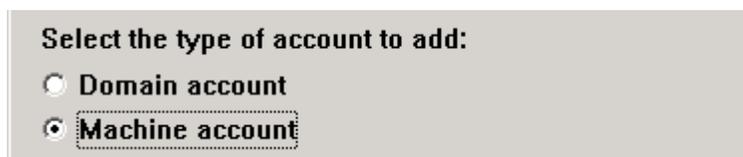


**Step 2. Type your DCS administrative password and click Log On.**

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



**Step 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.



Select the type of account to add:

Domain account

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.

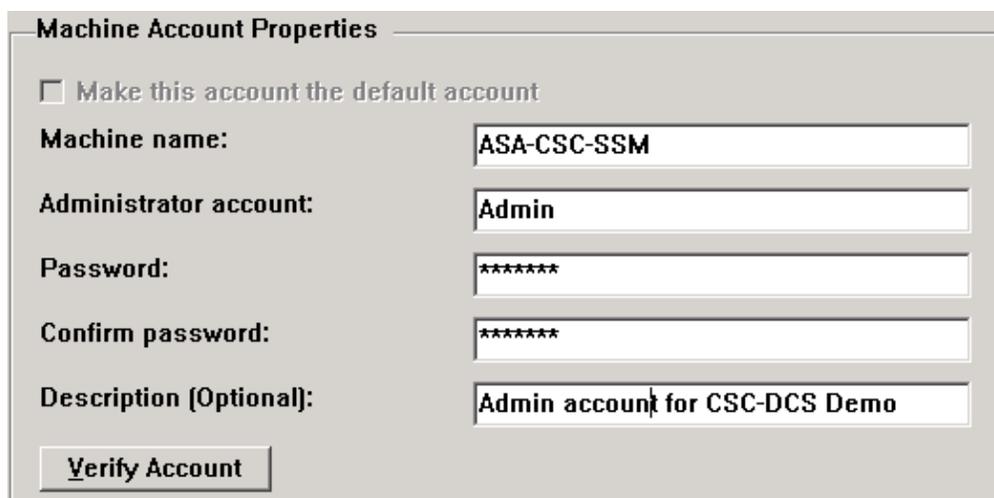
Note: If, during a scan, DCS is unable to access a remote machine using the account for that machine, DCS uses the default account to access the machine. Because only a domain account can be a default account, this option is disabled for machine accounts.

**Step 6.** In the Machine name field, type the name of the 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).



Machine Account Properties

Make this account the default account

Machine name: ASA-CSC-SSM

Administrator account: Admin

Password: \*\*\*\*\*

Confirm password: \*\*\*\*\*

Description [Optional]: Admin account for CSC-DCS Demo

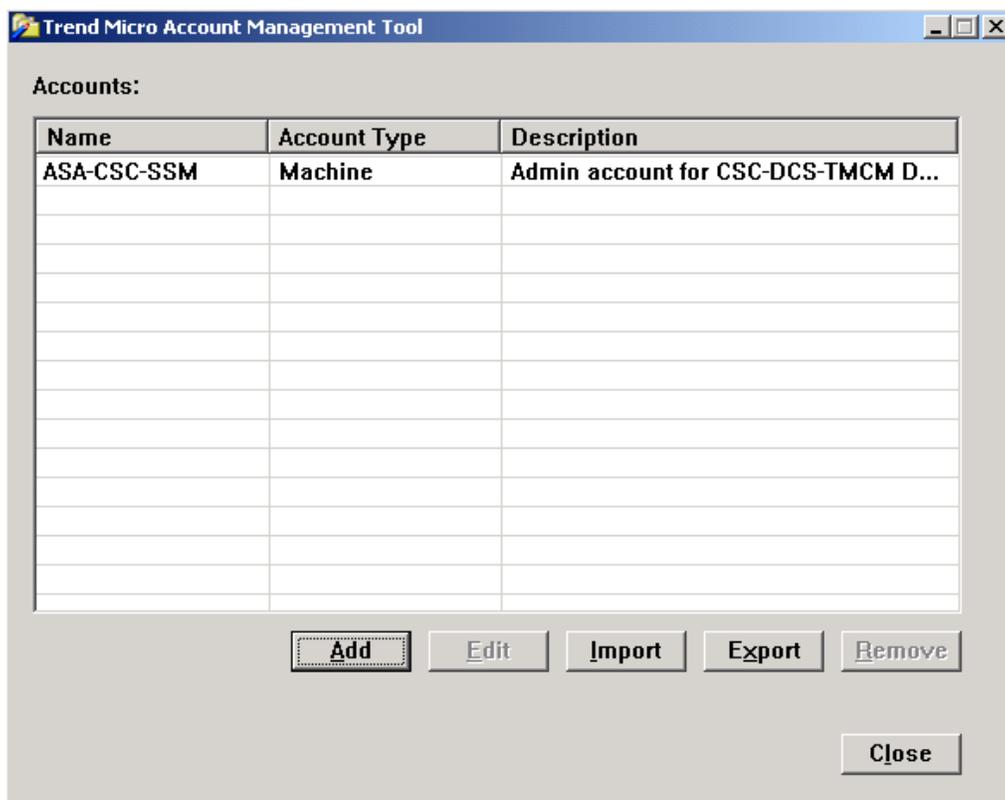
Verify Account

**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.

## Exercise 4: 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.

TREND MICRO™ InterScan™ for Cisco CSC SSM

Log Off Help

Summary

- Mail (SMTP)
- Mail (POP3)
- Web (HTTP)
- File Transfer (FTP)
- Update
- Logs
- Administration**
- Device Settings
  - Connection Settings
  - Device Failover Settings
  - Notification Settings
- Register to DCS
- Register to TCM
- Configuration Backup
- Product Upgrade
- Password
- Product License

### Damage Cleanup Services Registration

**Damage Cleanup Services**

Damage Cleanup Services: **Enabled** Disable

**Registered Server(s) / IP Address(es)**

DCS server name or IP address:  Add >

Port number:

DCS Server	Port Number	Delete
asa-csc-ssm	80	
192.168.0.11	80	

Redirect client to DCS on cleanup failure

Save Cancel

CSC-SSM is now registered to the DCS server; it can now send cleanup requests to the DCS server.

## Un-registering CSC SSM from DCS

You can un-register from DCS if your DCS server changes or if you no longer need DCS.

To un-register 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.