Configuring DCS 3.2 with Cisco MARS

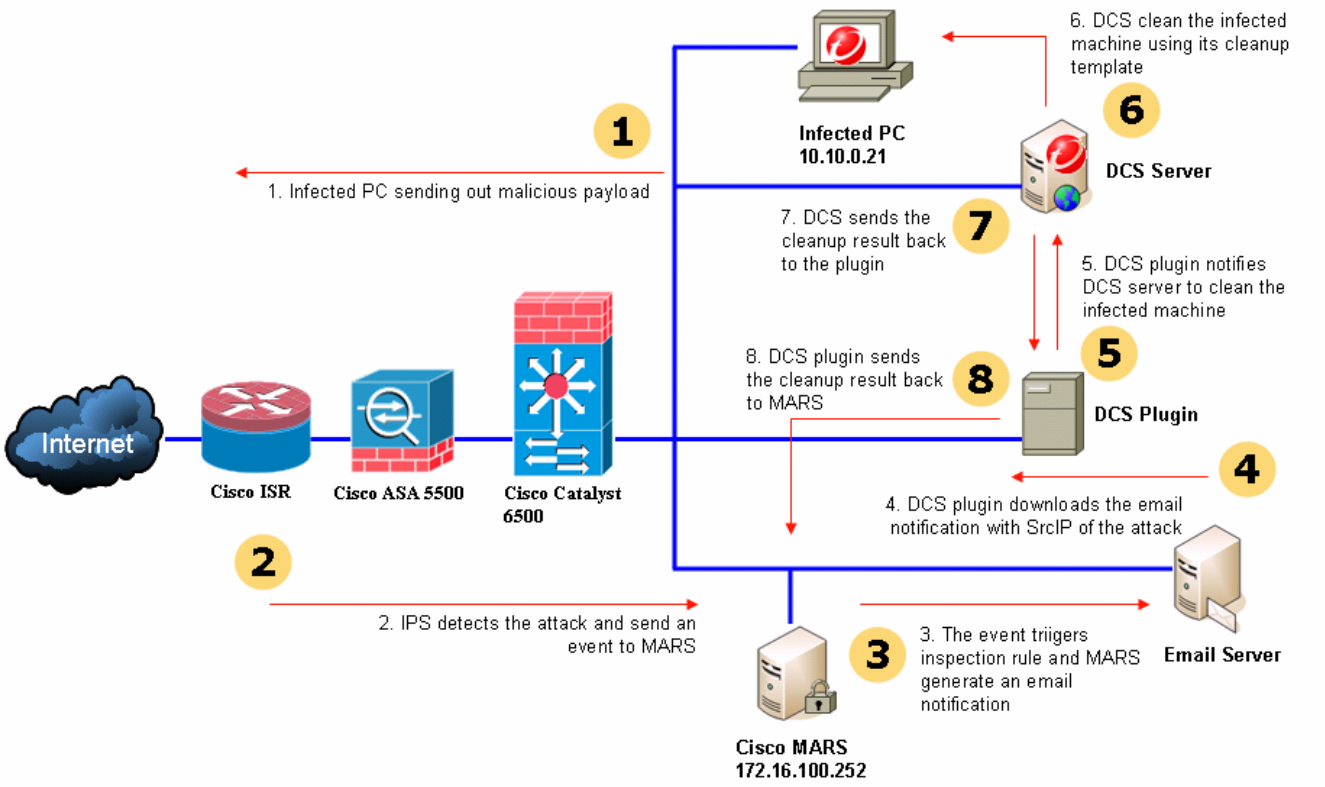
MARS-DCS 3.2 Plug-in

Table of Contents

Revision History

Change Date	Author	Description
03/14/2007	Alwin Yu	Draft
03/27/2007	Alwin Yu	Final Draft with Complete Syslog Data
04/17/2007	Alwin Yu	Version 1.0
04/26/2007	Alwin Yu	Version 1.1 – Updated Inspection Rules Section
05/07/2007	Alwin Yu	Version 1.3 – Added bug fixes section
05/30/2007	Alwin Yu	Version 1.4 – run as a service and MARS rules
06/11/2007	Alwin Yu	Version 1.5 – notes on enabling POP3 Service
06/11/2007	Alwin Yu	Version 1.6 – Included steps for DCS notification
06/22/2007	Erwin Benavidez	Version 1.6 – Convert to PDF format

1. Network Topology



MARS collects network events as well as security violation from various networking and security devices. MARS correlates all these events to come up with meaningful data and identify incidents that require administrator's attention. Trend Micro Damage Cleanup Service extends the capability of MARS not just to notify administrators of worm and spyware incidents but to also perform remediation action automatically within seconds after the incident has been identified by MARS. After DCS server completed its remediation process on the attacker's machine, the DCS action result is sent back to MARS to inform the network administrator of the result of the cleanup if it is successful, fail or an error has occurred.

2. Deployment Use Cases

2.1 LAN Deployment

Trend Micro Damage Cleanup Services and Cisco MARS can be installed on the same network segment. This scenario is applicable for customers with only one central office and one DCS server is enough to cover the cleanup requirements of the entire network. MARS upon generating an incident will trigger an SMTP notification. This SMTP notification goes into a user's mailbox that is monitored by the DCS plug-in. This email is downloaded by DCS plug-in at a pre-configured interval and appropriate cleanup request is sent to the local DCS server. DCS server must be able to connect and login with administrator's privilege to all desktop machines on network from its location in order to provide cleanup capability.

2.2 WAN Deployment

On a network that spans multiple geographic locations, the Cisco MARS device can be situated on the main office and multiple branch offices report to the single MARS device. Under this environment simply follow Cisco's recommendation how to situate the SMTP/POP3 server for Cisco MARS. The DCS plug-in is best to be installed on the same network as the SMTP/POP3 server to check for emails

generated by MARS locally. The DCS plug-in is able to notify specific DCS servers based on the IP address range of the host that requires cleanup.

You can register multiple DCS server into one DCS plug-in, but the DCS plug-in has a one to one mapping between itself and the Cisco MARS device. We recommend one DCS server for each remote office. It is required that the DCS plug-in must be able to access each DCS server via their web management port, default port is 80 in order to send the cleanup request. The DCS server also needs to send the cleanup result back to the DCS plug-in, default port is 1080. If communication between the DCS server and the DCS plug-in traverses a firewall, these 2 port numbers must be kept open for the cleanup functionality to work properly. The DCS server local to each region will be able to perform cleanup on its local network faster than any remote server could achieve. This method also in one way or the other distributes the cleanup load among multiple DCS servers.

2.3 MARS events triggering DCS cleanup

In order for DCS to cleanup machines based on incidents triggered by MARS, it is required that you configure certain Inspection Rules in MARS to trigger an SMTP notification to the pre-configured DCS mailbox. We have identified 3 levels of MARS inspection rules we can configure to send SMTP notification with XML attachment to the DCS mailbox, the Mailbox is what makes it possible for DCS plug-in to notify the DCS server which machine needs to be cleaned regardless of antivirus software installation.

These are the inspection rules in MARS you should enable SMTP notification with XML attachment. The MARS incident must at least have Source IP Address of the attacker.

1. 1st Level of Inspection Rules:

   This will require Trend Micro Control Manager to be able to send Trend Micro logs to Cisco MARS.

   - Trend Micro product Virus Incidents
     - **Trend Micro: Web_Security_Violation**
     - **Trend Micro: Virus_Found_Pass_Thru**
   - Trend Micro product Spyware Incidents
     - **Trend Micro: Grayware_Found_Pass_Thru**

2. 2nd Level of Inspection Rules:

   - Standard MARS Virus/WORM related incidents from 3rd party AV vendors
     - **System Rule: Virus Found - Not Cleaned**

3. 3rd Level of Inspection Rules:

   This set of rules pertains to events gathered from Cisco Security products as well as other behavioral monitoring products.

   - System: Client Exploits, Virus, Worm and Malware
     - **System Rule: Worm Propagation - Success Likely**
     - **System Rule: Worm Propagation – Attempt**
     - **System Rule: Network Activity: Windows Popup Spam**
     - **System Rule: Network Activity: Excessive Denies - Host Compromise Likely**
     - **System Rule: Client Exploit - Sysbug Trojan**
     - **System Rule: Client Exploit - Success Likely**
     - **System Rule: Client Exploit - Sasser Worm**
     - **System Rule: Client Exploit - Mass Mailing Worm**
     - **System Rule: Client Exploit – Attempt**
     - **System Rule: Backdoor: Spyware**
     - **System Rule: Backdoor: Covert Channel**
     - **System Rule: Backdoor: Connect**
     - **System Rule: Backdoor: Active**

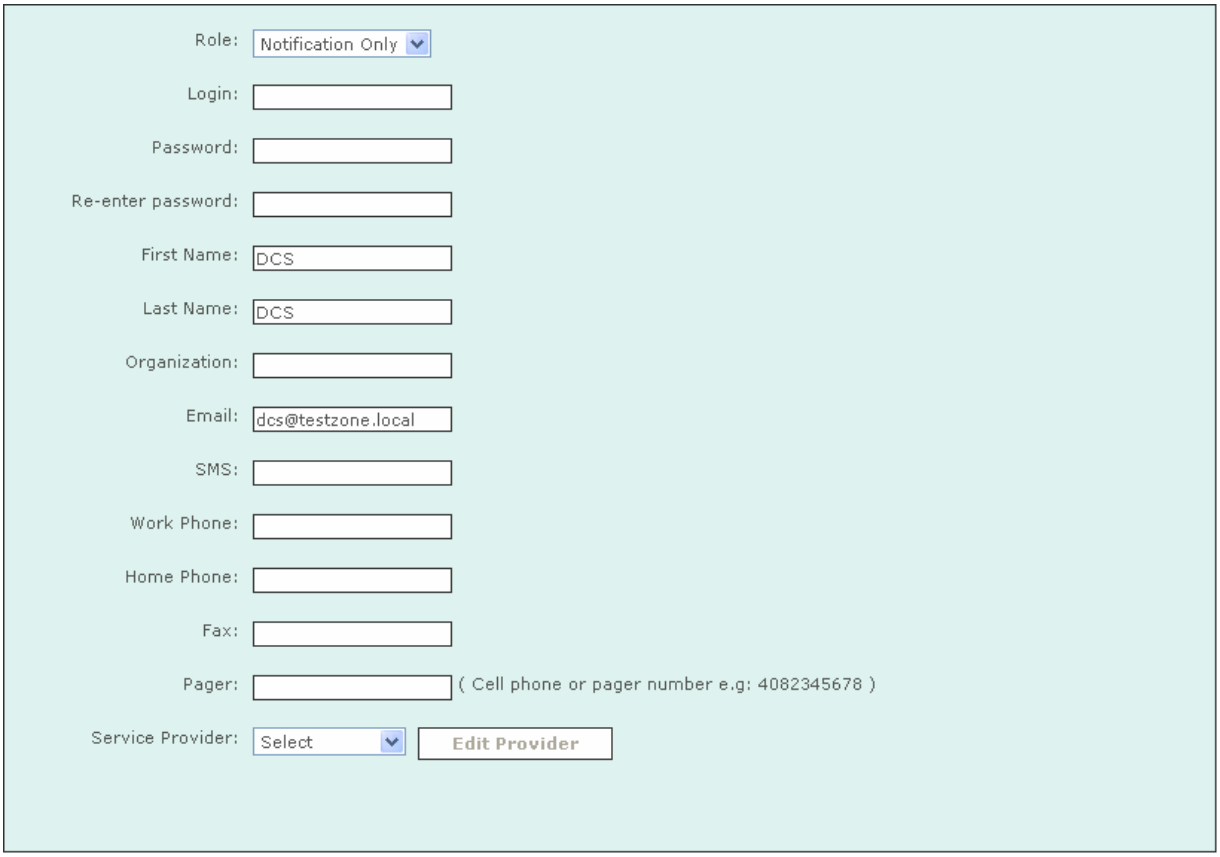
- System: Network Attacks and DoS
  - **System Rule: Sudden Traffic Increase To Port**

- System: Reconnaissance
  - **System Rule: Scans: Stealth**
  - **System Rule: Scans: Targeted**

After you have identified the rules you want to trigger DCS notification. We need to configure each rule's action to trigger an SMTP Notification with XML Attachment.

Step 1 Open the MARS web console, go to the **Management** tab → **User Management**

Step 2 Click the **Add** button to add a new user for **notification only**



Step 3 Click **Submit**

Step 4 The DCS notification user has been created

	User Name	Login	Email	Role	Organization	Groups
☐	Administrator (pnadmin)	pnadmin	root@apszone.local	Admin		Admin
☐	DCS, DCS		dcs@testzone.local			Notification

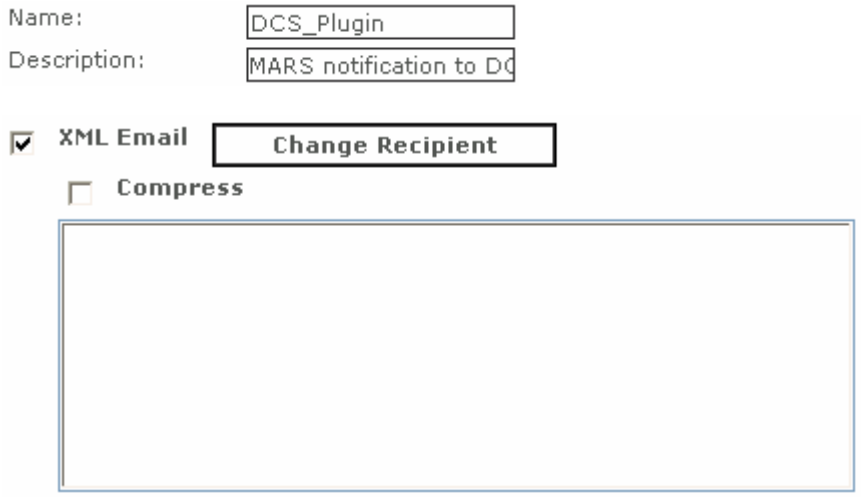
Step 5 Open the MARS web console, go to the **Rules** tab.

Step 6 Identify the rules you want to configure.

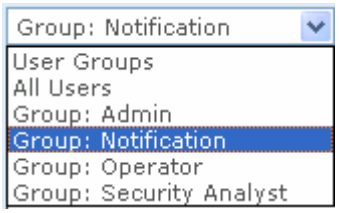
Step 7 Click on the value next to "**Action:**"

Step 8 You will need to create your action profile. Click on **Add** button

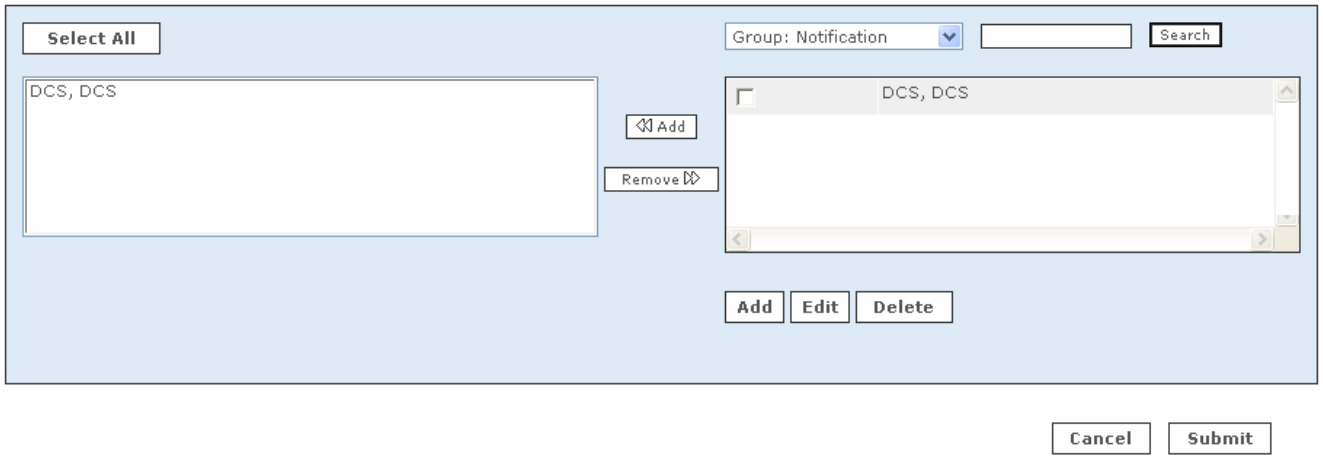
Step 9 Provide a **name** and **description** for the Action profile. **Enable XML Email** and click on **Change Recipient** button



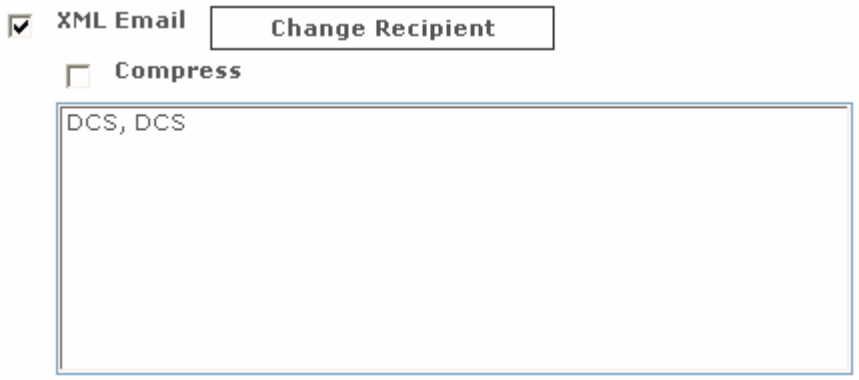
Step 10 Select **Group: Notification**.



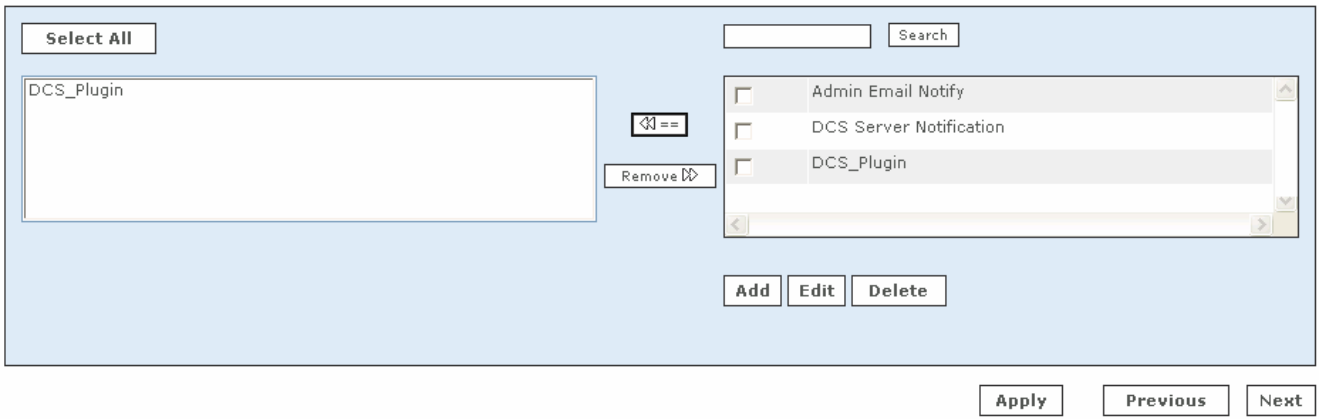
Step 11 Add the **DCS mailbox** to the Email recipients and click **Submit**.



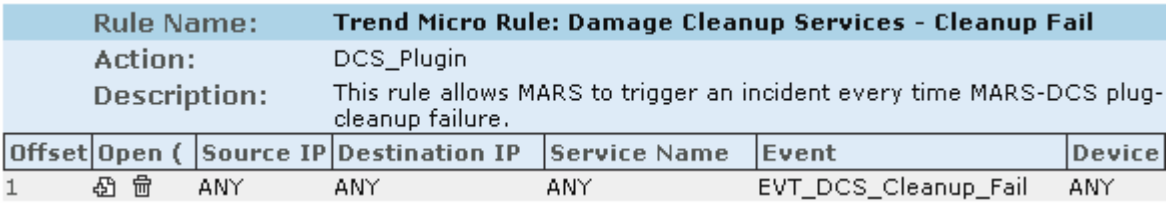
Step 12 Verify the DCS Notification has been correctly added. Click **Submit**.



Step 13 Select the newly created Notification Profile and add it to the right hand side. Click **Apply** button.

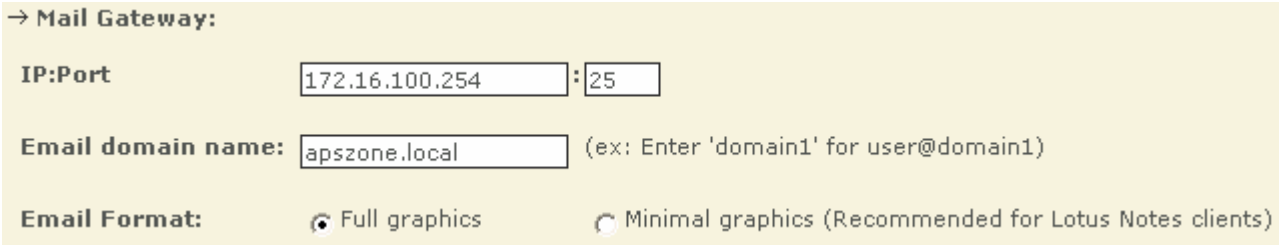


Step 14 Verify the rule and click the **Submit** button

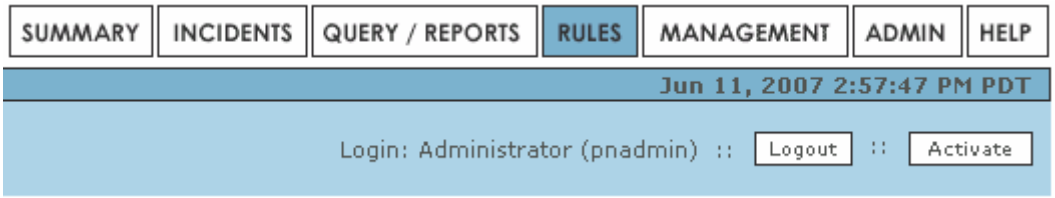


Step 15 Go to the **MARS Console → Admin Tab → System Setup → Configuration Information**

Step 16 Supply the correct value for **Mail Gateway IP** and **Port** information.



Step 17 Click **Activate** button for the new settings to take effect.



3. Installing and Configuring DCS Server

3.1 Installing the DCS server

Step 1 Download the DCS server installer from the Trend Micro website.

- http://www.trendmicro.com/download/product.asp?productid=48
- Filename: DCS32_1023_Repack3.zip (134MB)

Step 2 Obtain an Activation Key for DCS, the beta kit will provide an Activation Key valid for 30 days.

Step 3 Copy the DCS 3.2 installer to your Windows 2000/2003 server.

Step 4 Run the **setup.exe** installation file to start the DCS server installation

Step 5 The Trend Micro DCS welcome page appears. Click **Next**

Step 6 Select **I accept** under Trend Micro License Agreement. Click **Next**

Step 7 The installation checks for your minimum system requirements. Click **Next**

Step 8 The database information settings screen appears. Select **Install Microsoft SQL Server Desktop Engine**, under the **Password field**, supply a secure password, under the **Database field**, use the default database name **DCS**. Click **Next**

Step 9 The proxy connection settings screen appears. If you do not require proxy configuration to connect to the internet simply click **Next**, otherwise specify the proxy port information.

Step 10 The product activation screen appears, enter the Trend Micro DCS activation key provided. Click **Next** button.

Step 11 Supply the DCS console password, click **Next**

Step 12 Click the **Install** button to start DCS server installation.

Step 13 Click **Finish** to close the Install Shield wizard screen.

Step 14 Select **No** when prompted to install Trend Micro Control Manager agent for DCS

3.2 Configuring the DCS server's Account Management Tool

Step 15 After the DCS server has been successfully installed. Go to the start menu → All Programs → Trend Micro Damage Cleanup Services → Account Management Tool

Step 15 Enter the password you have used during the DCS server installation, click **Log On** button

Step 16 On the Trend Micro Account Management Tool screen, click the **Add** button

Step 17 Select **Machine account** and proceed to supply information to the following fields:

- Machine Name
- Administrator account
- Password
- Confirm Password

Provide an account that has either Local Admin or Domain Admin privilege

Step 18 Click **Verify Account** button. Confirm if you have received the message "**Connectivity to client verified**", click **OK**

Step 19 Click the **OK** button to save your configuration. Confirm you have received the message "**New account information saved**", click **OK**

Step 20 Check your new machine account information correctly display on the utility, click the **Close** button

4. Installing and Configuring DCS Plug-in for MARS

4.1 Installing software required by the DCS plug-in

Step 1 The DCS plug-in uses third party applications to perform its function. You may find them on the Beta Kit or download them from this URL.

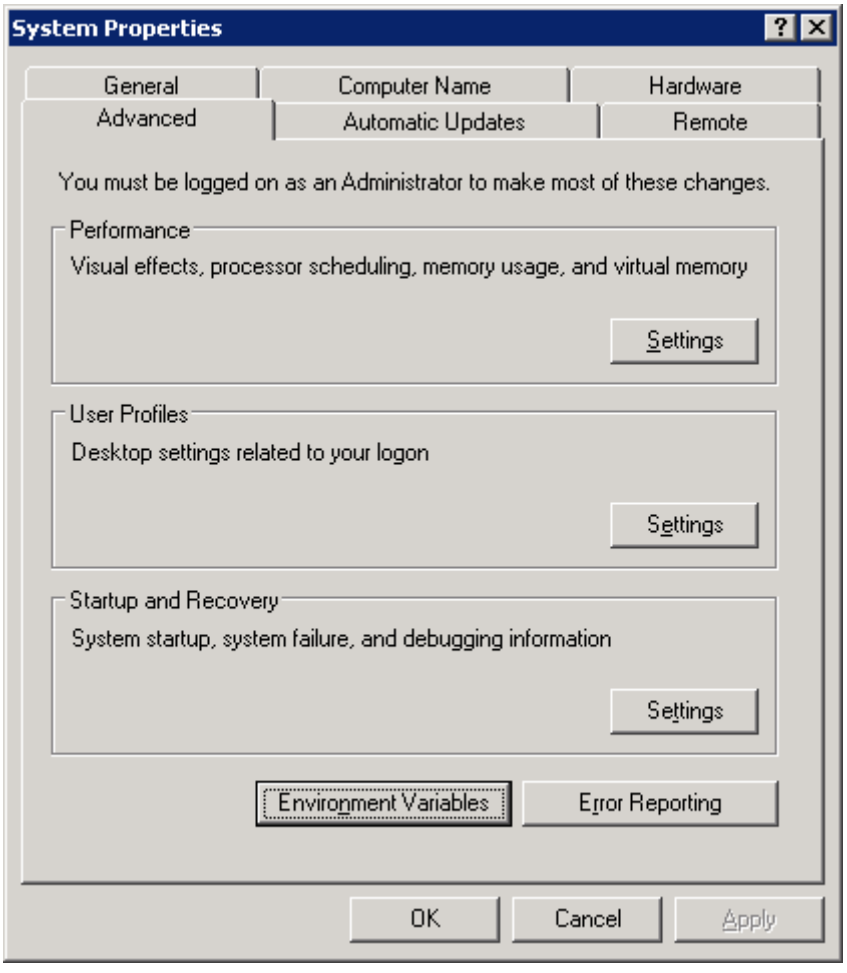
- http://www.python.org/download/
- http://www.baremetalsoft.com/wintail/

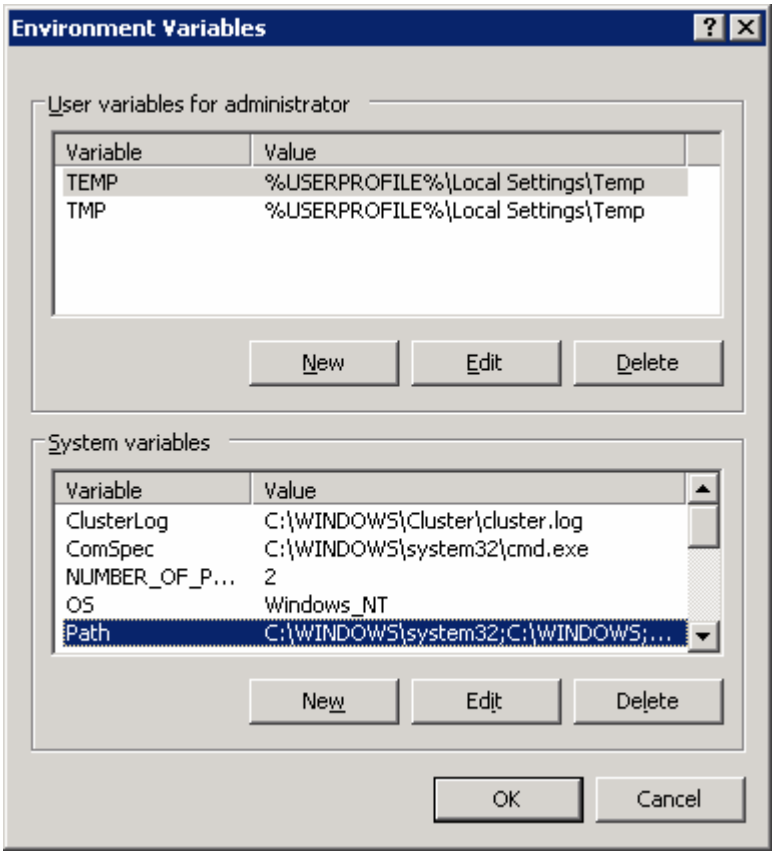
Step 2 Download the file **python-2.5.msi** to the machine running the DCS plug-in. Install the python MSI package. The python installation by default goes into C:\Python25

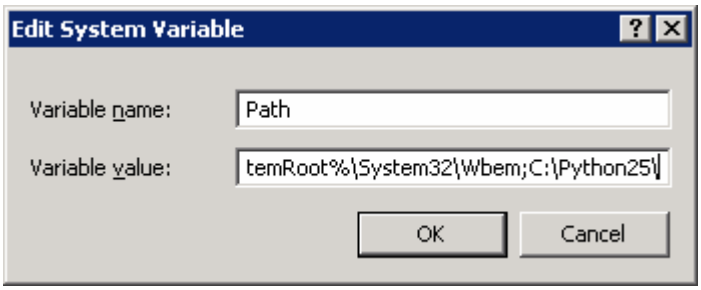
Step 3 After the Python has been installed, add the Python.exe executable to the %PATH% environment variables.

Windows 2003 Server

- Right Click on **My Computer** → **Properties** → **Advanced Tab** → Click on **Environment Variables** → Under System Variables, locate and highlight **Path** → Click on the **Edit** button → Add **C:\Python25** into the variable value field delimited by a semi-colon







Example:
%SystemRoot%\system32;%SystemRoot%;C:\Python25\

Step 4 The **wintail.exe** goes into the same directory as the DCS plug-in files.

Note: The MARS-DCS plug-in **requires a Mail Server that supports the POP3 protocol** to download MARS email notification to trigger DCS cleanup.

4.2 Installing the DCS plug-in

Step 5 Create a directory for Plug-in software (e.g. C:\DCS_Plugin)

Step 6 Unzip the archive "**dcsplugin_x.x.x .zip**" into this directory. You should see 13 python byte code files (.pyc), an XML configuration file and the wintail.exe utility.

List of DCS Plugin Files:

- dcs_plugin.pyc
- dcsp_config.pyc
- dcsp_dcs_interface.pyc
- dcsp_inet.pyc

- dcsp_list_mgmt.pyc
- dcsp_log_listener.pyc
- dcsp_log_module.pyc
- dcsp_main.pyc
- dcsp_network_utils.pyc
- dcsp_pop_client.pyc
- dcsp_syslog.pyc
- dcsp_unregister.pyc
- dcsp_url_utils.pyc
- WinTail.exe
- dcsp_config.xml

4.3 Configuring and customizing the DCS plug-in

Step 7 Open the file dcsp_plugin.xml using notepad or other text editor. Configure the behavior of DCS plug-in to match the requirements on your network

Step 8 Configuring **Logging_Info**

- **log_file** (default value: dcsp_log.txt)
  specify the name of the log file generated by the DCS plug-in. The log file by default is created on the same directory where you have run the DCS plug-in

- **log_level** (default value: info)
  supports the following log level: critical, error, warning, info, debug. Depending on your needs, the beta script requires you to run the plug-in in debug level.

- **use_wintail** (default value: yes)
  When you start the plug-in, this allows the plug-in to load a debug screen to see real-time activities done by the plug-in.

Step 9 Configuring **Product_Info**

- **Product_Name_Mars_Syslog** (default value: DamageCleanupServices)
  This is part of the syslog message sent by the plug-in to MARS.

- **Enable_CCA** (default value: yes)
  Offer services to CCA to redirect users to DCS manual cleanup page.

Step 10 Configuring **DCS_Server_List**

You may define multiple entries under this section. Each entry represents one DCS server on your network. The **ip_net** and **ip_mask** represents the network to be protected by the DCS server specified under **server_name** and the DCS port number **server_port**. It is mandatory to have **ip_net=0.0.0.0** and **ip_mask=0.0.0.0** this represents the default DCS server cleanup will be assigned if no match has been found.

Example given:

Events from 10.30.0.0/16 network will be cleaned by DCS server 10.30.1.11, remaining events will always go to DCS server 172.16.100.253.

```
<DCS_Server
    ip_net="10.30.0.0"
    ip_mask="255.255.0.0"
    server_name="10.30.1.11"
    server_port="80" />

<DCS_Server
        ip_net="0.0.0.0"
```

ip_mask="0.0.0.0"
server_name="172.16.100.253"
server_port="80" />

Step 11 Configuring **Clean_Exception_List**

This list is the highest priority. Entries in this list are never cleaned (max 50)

Example given:

<Exception_IP value="172.16.100.1" />
<Exception_IP value="172.16.100.2" />

Step 12 Configuring **Internal_Network_List**

DCS cleanup will be performed only for computers on these networks. A max of 10 are allowed

Example given:

<Network ip_net="10.30.0.0" ip_mask="255.255.0.0" />
<Network ip_net="172.16.100.0" ip_mask="255.255.255.0" />
<Network ip_net="192.168.0.0" ip_mask="255.255.255.0" />

Step 13 Configuring **MARS_Event_Info**

MARS sends SMTP notification to this email account on this mail server, DCS plug-in uses the parameters defined here to download email via pop3. Download frequency is specified under **email_check_frequency** in seconds

Example given:

<email_server_name value="172.16.100.254" />
<email_acct_username value="dcs_admin" />
<email_acct_password value="password" />
<email_check_frequency value="5" />

Step 14 Configuring **MARS_Server_Info**

Plug-in sends cleanup result back to MARS using this information. The port value only supports UDP port number 514.

Example given:

<mars_syslog_server value="172.16.100.252" />
<mars_syslog_port value="514" />

Step 15 Configuring **DCS_Log_Listener** (default value: 1080)

The DCS plug-in listens on this port to receive cleanup result back from the DCS server. This port number can be any port that is not in use currently by the machine where the DCS plug-in is running.

Step 16 Configuring **DCS_Cleanup_Params**

- **min_damage_free_time** (default value: 60)
  Specify here the number of minutes after a machine has already cleaned and no infection found to inform DCS server not to clean this machine again until the elapse time has passed. This allows damage on the machine un-cleanable by DCS to inform MARS that machine is still sending out attacks and has to be cleaned manually.

Note: The plug-in requires POP3 be enabled on your mail server, if you are unable to enable this service or if your mail server does not support POP3 see **Section 11** for instructions.

Configuring the MARS-DCS plug-in to run as a service

Step 1 Stop the plug-in if it is running.

Step 2 Install Windows 2000 or Windows 2003 **Resource Kit** (or copy the 2 binaries **instsrv.exe** and **srvany.exe**). You can download the free kit from Microsoft's website.

- http://www.microsoft.com/downloads/details.aspx?familyid=9D467A69-57FF-4AE7-96EE-B18C4790CFFD&displaylang=en

Step 3 Open a command prompt and run **instsrv** to install **srvany.exe** as a service with the name "**DCS Plugin**"

- C:\> "C:\Program Files\Resource Kit Tools\instsrv" "DCS Plugin" "C:\Program Files\Resource Kit Tools\srvany.exe"

Step 4 Go to **Control Panel** → **Administrative Tools** → **Computer Management** → **Services**. Ensure that "**DCS Plugin**" is listed as a service and the startup type is "**automatic**".

Step 5 Create **registry** entries for the DCS Plugin service

Step 6 Go to **Start** → **Run** → **regedit**. Go to the registry key hive **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DCS Plugin**

Step 7 Add new key called "**Parameters**"

Step 8 Add these three values (all string values) under the **Parameter** key

- "Application"="C:\Python25\pythonw.exe"
- "AppDirectory"="C:\DCS_Plugin"
- "AppParameters"="C:\DCS_Plugin\dcs_plugin.pyc"

Note: Make sure to set the directory names according to your installation.

Step 9 Open the file dcsp_config.xml and set parameters **<use_wintail value="no">** and **<Run_As_Service value="yes" />**. This is needed for the plug-in to run as a service.

Step 10 Perform a test by starting and stopping the "**DCS Plugin**" service in **Computer Management** → **Services**.

Verification Procedure:
The service is running and if the MARS-DCS plug-in is set to run in debug mode, you will be able to check the file dcsp_log.txt that the service is checking for emails every few seconds based on your defined time intervals. This is a sign the utility is operational.

4.4 Starting and stopping the DCS plug-in

Step 16 Go to **Start Menu** → **Run Window** → Type **CMD**

Step 17 On the command prompt, change directory to the DCS_Plugin

Step 18 To start the DCS plug-in, type the command: **python dcs_plugin.pyc**

- C:\DCS_Plugin>python dcs_plugin.pyc

Step 19 The DCS plug-in upon starting will automatically register itself to the pre-configured DCS servers.

Step 20 To stop the DCS plug-in, simply type **quit** then press enter.

Note: Any modification to the dcsp_config.xml file requires restarting the plug-in for the change to take effect.

Note: After the plug-in has stopped, the wintail debug window has to be closed manually.

4.5 Un-registering DCS plug-in from a DCS server

When "http_listen_port" value is modified in dcsp_plugin.xml, the plug-in has to un-register with the DCS servers first and then re-register for the new port number to take effect.

Step 1 Stop the DCS plug-in

Step 2 Run the command: python dcsp_unregister.pyc all

Step 3 Start the DCS plug-in

5. Configuring MARS Custom Devices

When you want to add a custom device into MARS, you must define a custom device and its corresponding log parser. When you are defining an instance of the custom device, you are required to specify the reporting method. You are prompted to select either SYSLOG or SNMP as the device type. It is this designation that determines what kind of traffic MARS is expecting to receive from the reporting device. The coverage of this document is SYSLOG method only.

5.1 Adding User Defined Log Parser Templates

MARS allows the user to enter any SYSLOG or SNMP device into the network topology, configure it to report data to the MARS and query the data using free-form query.

User needs to specify the incoming data format so that MARS can parse and retrieve session information from arbitrary logs.

Note: While the raw message for an event does include the header information, MARS removes the header prior to sending the payload to the custom parser. When writing a parser log template, do not include the header fields.

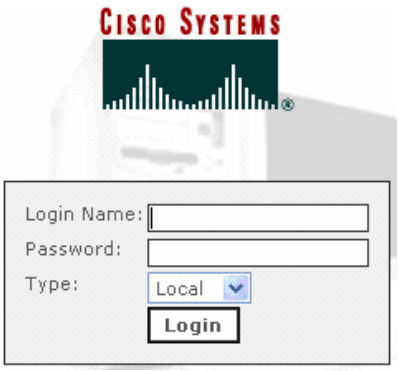
To add a user-defined log parser template, you must perform the following tasks:

1. **Add a custom Device or Application type**. See Define a Custom Device/Application Type Damage Cleanup Services
2. **Add a log parser template**. See Add Parser Log Templates for the Custom Device/Application Damage Cleanup Services.
3. **Add device with the above custom Device or Application type**. See Add Custom Device or Application as Reporting Device.

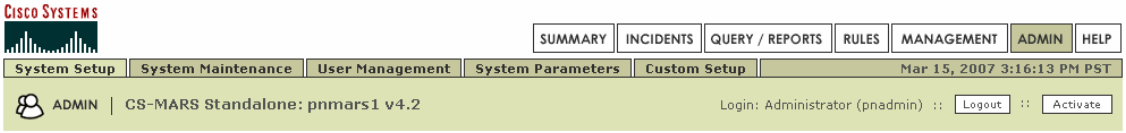
Until each of these tasks is completed, MARS is unable to parse the logs from the reporting device, even if it is receiving those events.

5.1.1 Define a Custom Application Type Damage Cleanup Services

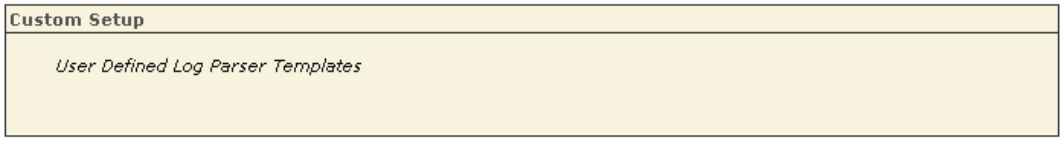
Step 1 **Login** to Cisco MARS web console.



Step 2 Go to **Admin** → **Custom Setup** Tab



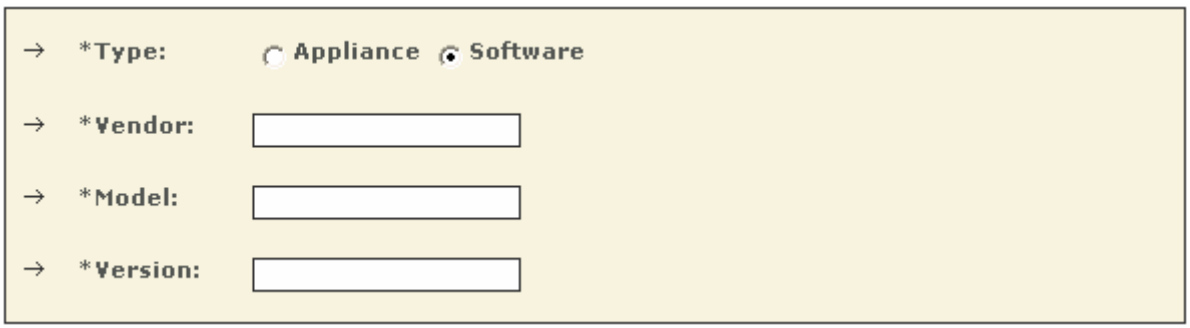
Step 3 Click the **User Defined Log Parser Templates**.



Step 4 Click **Add** button which is located next to the Device/Application type list.

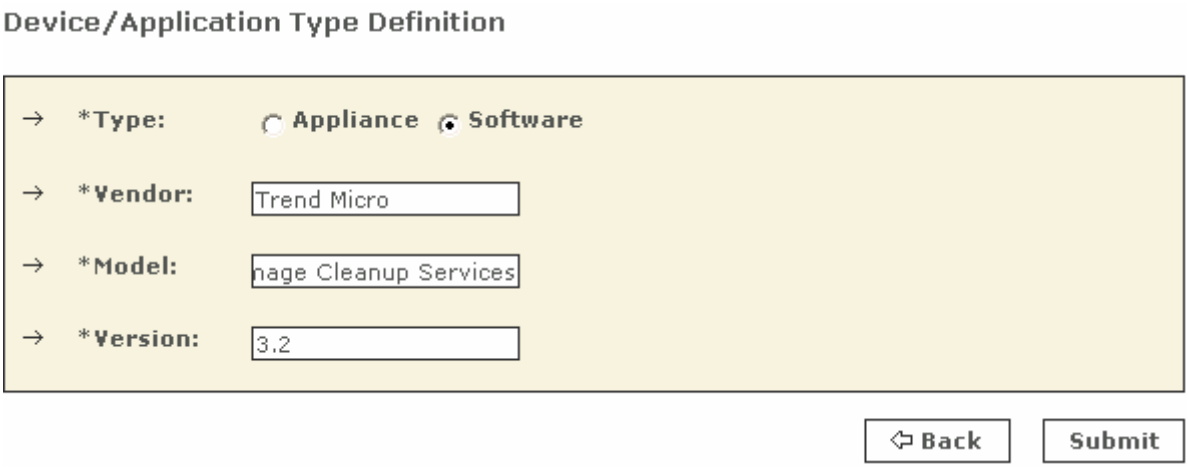
Step 5 Choose the Type - Appliance or Software. Select **Software** for our Damage Cleanup Services custom parser.

- *Appliance* - A hardware device that can send logs to the MARS Appliance
- *Software* - An application running on a host and the host can be configured to send logs to the MARS Appliance.



Step 6 Enter the Vendor, Model and Version for the Device or Application.

Fields	Value
Vendor	Trend Micro
Model	Damage Cleanup Services
Version	3.2



Step 7 Click **Submit**. Trend Micro Damage Cleanup Services becomes available on the drop down menu.

Verification Procedure:
The application type Trend Micro Damage Cleanup Services 3.2 has been successfully created.

5.1.2 Add Parser Log Templates for Custom Device/Application Damage Cleanup Services

DCS Events

Log ID: TM_DCS_CLEAN_SUCCESS	
Log Description: Trend Micro DCS successfully cleaned an infection	
Mapped to Event Type: EVT_DCS_Cleanup_Success	
• **Event ID:**	EVT_DCS_Cleanup_Success
• **Description:**	EVT_DCS_Cleanup_Success
• **Severity:**	Green
• **CVE Name:**	
Regular Expressions:	
• **Received Time**	DCS_Cleanup_Success .* Event time="
• **Destination Address**	.* Infection destination IP="

Log ID: TM_DCS_CLEAN_FAIL	
Log Description: Trend Micro DCS was unable to clean an infection	
Mapped to Event Type: EVT_DCS_Cleanup_Fail	
• **Event ID:**	EVT_DCS_Cleanup_Fail
• **Description:**	EVT_DCS_Cleanup_Fail
• **Severity:**	Red
• **CVE Name:**	
Regular Expressions:	

• **Received Time**	DCS_Cleanup_Fail .* Event time="
• **Destination Address**	.* Infection destination IP="

Log ID: TM_DCS_LOGIN_FAILURE	
Log Description: Trend Micro DCS was unable to log into the machine	
Mapped to Event Type: EVT_DCS_Cleanup_Fail	
• **Event ID:**	EVT_DCS_Cleanup_Fail
• **Description:**	EVT_DCS_Cleanup_Fail
• **Severity:**	Red
• **CVE Name:**	
Regular Expressions:	
• **Received Time**	DCS_Login_Failure .* Event time="
• **Destination Address**	.* Infection destination IP="

Log ID: TM_DCS_NO_INFECTION_FOUND	
Log Description: Trend Micro DCS did not find any infection	
Mapped to Event Type: EVT_DCS_No_Infection_Found	
• **Event ID:**	EVT_DCS_No_Infection_Found
• **Description:**	EVT_DCS_No_Infection_Found
• **Severity:**	Yellow
• **CVE Name:**	
Regular Expressions:	
• **Received Time**	DCS_No_Infection_Found .* Event time="
• **Destination Address**	.* Infection destination IP="

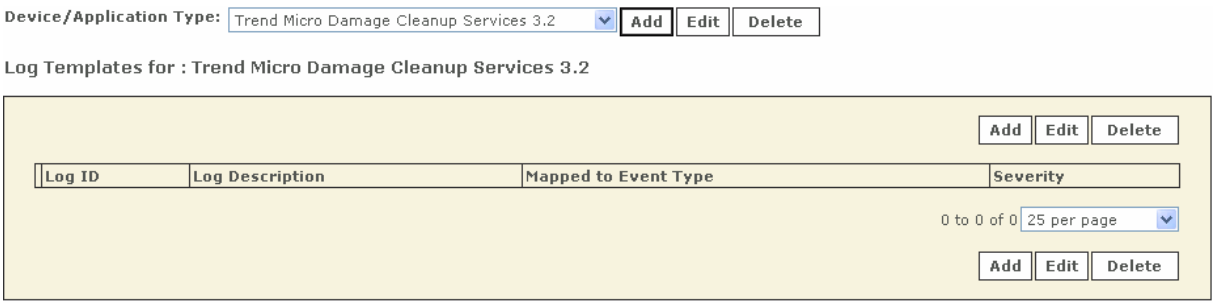
Log ID: TM_DCS_SCAN_REQUEST_ON_CLEANED_HOST	
Log Description: Trend Micro DCS cleaned the machine but the machine continues to trigger MARS alert	
Mapped to Event Type: EVT_DCS_ SCAN_REQUEST_ON_CLEANED_HOST	
• **Event ID:**	EVT_DCS_ SCAN_REQUEST_ON_CLEANED_HOST
• **Description:**	EVT_DCS_ SCAN_REQUEST_ON_CLEANED_HOST
• **Severity:**	Red
• **CVE Name:**	
Regular Expressions:	
• **Received Time**	DCS_MANUAL_CLEAN_NEEDED .* Event time="
• **Destination Address**	.* Infection destination IP="

Sample Event: TM_DCS_CLEAN_SUCCESS

Step 1 Go to the **Admin > Custom Setup** tab.

Step 2 Click the **User Defined Log Parser Templates.**

Step 3: Select the newly created/existing Device/Application from the Device/Application Type list **Trend Micro Damage Cleanup Services 3.2**.



Step 4 To add a log template, click **Add**.

Note A log template ties directly to the particular message that you want to parse. A log template is composed of one or more Event Types that describe the contents of the message. Using the Event Types, MARS parses the message when it is received.

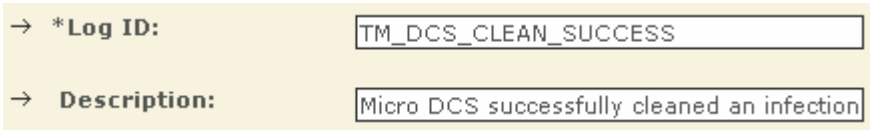
Step 5 Enter a value in the **Log ID** field. This value is a unique string value that identifies the log message.

- **Log ID**: TM_DCS_CLEAN_SUCCESS

Note The Log ID field provides an opportunity to map this message number or another moniker used by the device to the custom event type that you are developing. You can use this value to clarify the device messages for which you have developed custom event types.

Step 6 Enter **Description** - A description of the log message.

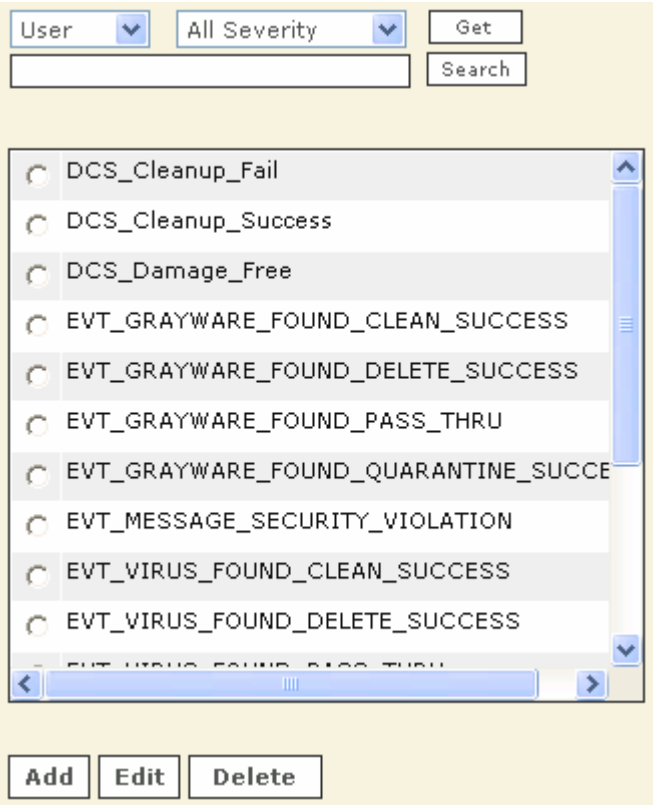
- **Description**: Trend Micro DCS successfully cleaned an infection



Step 7 Map the new log **TM_DCS_CLEAN_SUCCESS** to an Event Type.

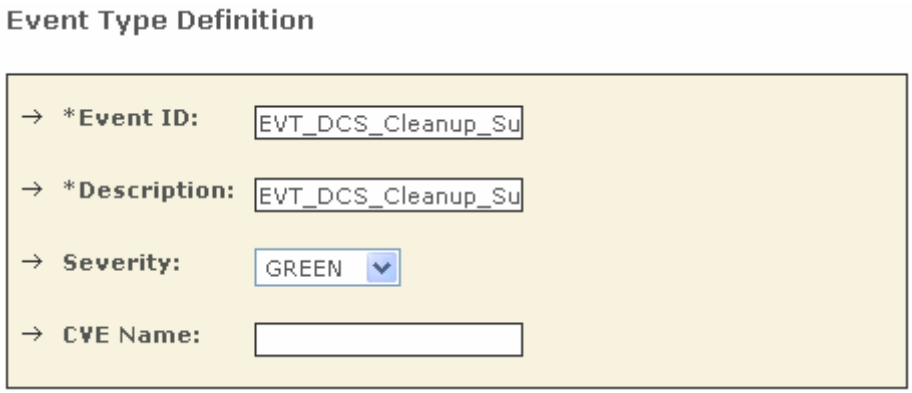
Note The MARS Appliance comes with a number of predefined Event Types. For this guide we want to create our own events.

Step 8 To add a new event type, click **Add** below the **Map to Event Type** area.



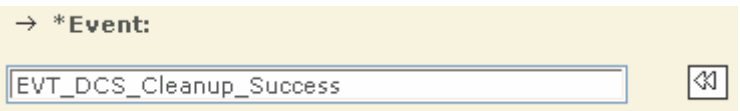
Step 9 Use the following information:

Fields	Value
Event ID	EVT_DCS_Cleanup_Success
Description	EVT_DCS_Cleanup_Success
Severity	GREEN
CVE Name	



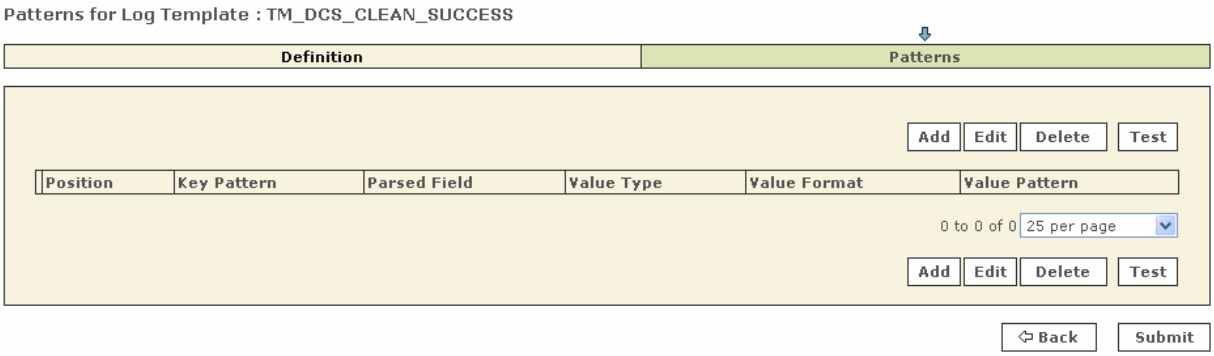
Step 10 Click **Submit.**

Step 11 Select the newly created event type and then click the icon: To move the event type to the left hand pane.



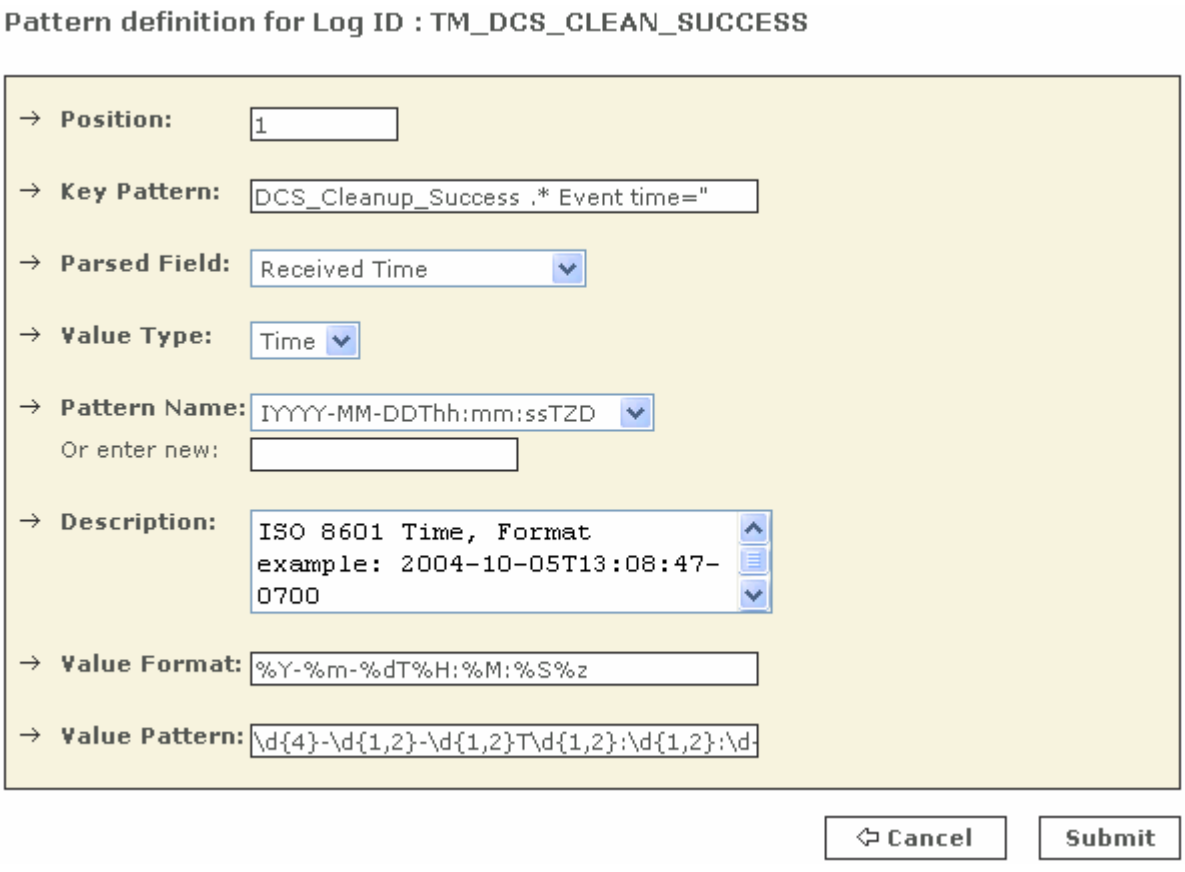
Step 12 Click **Apply** button, the **Patterns** link will now become enabled.

Step 13 Click the **Patterns** link. The pattern configuration screen comes up.



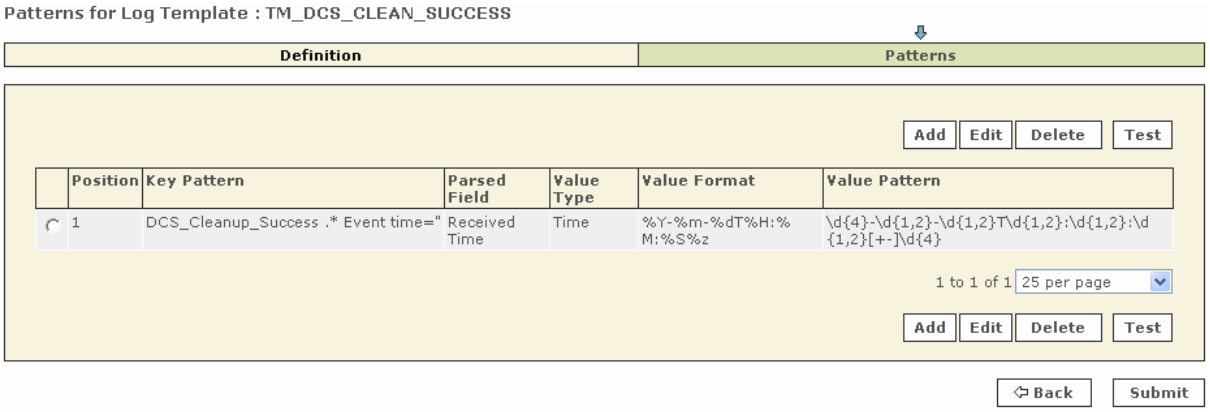
Step 14 Click **Add** button to parse our 1st value from the syslog for the **Received Time** field. Supply the fields with the value found under this table, the remaining fields will automatically populate with the correct data.

Fields	**Value**
Position	1
Key Pattern	DCS_Cleanup_Success .* Event time="
Parsed Field	Received Time
Value Type	Time
Pattern Name	IYYY-MM-DDThh:mm:ssTZD



Note: Careful when entering the Key Pattern field, one incorrect character or an additional spacing will cause the entire parsing to fail.

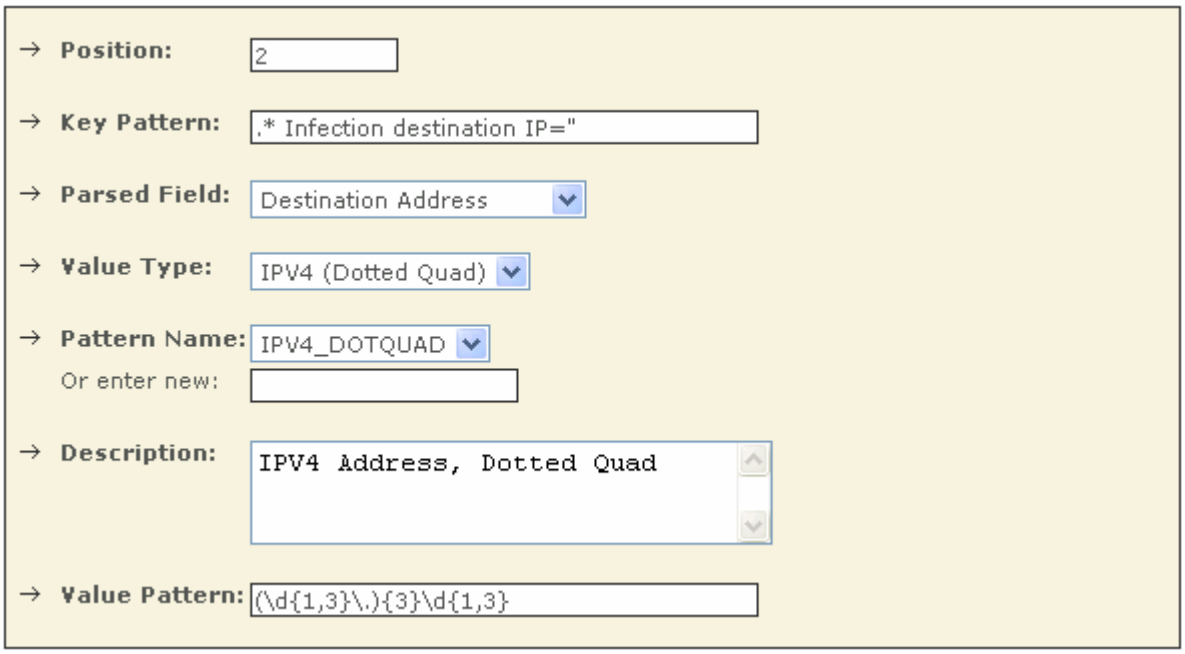
Step 15 Click **Submit**. The first parsing pattern is now created.



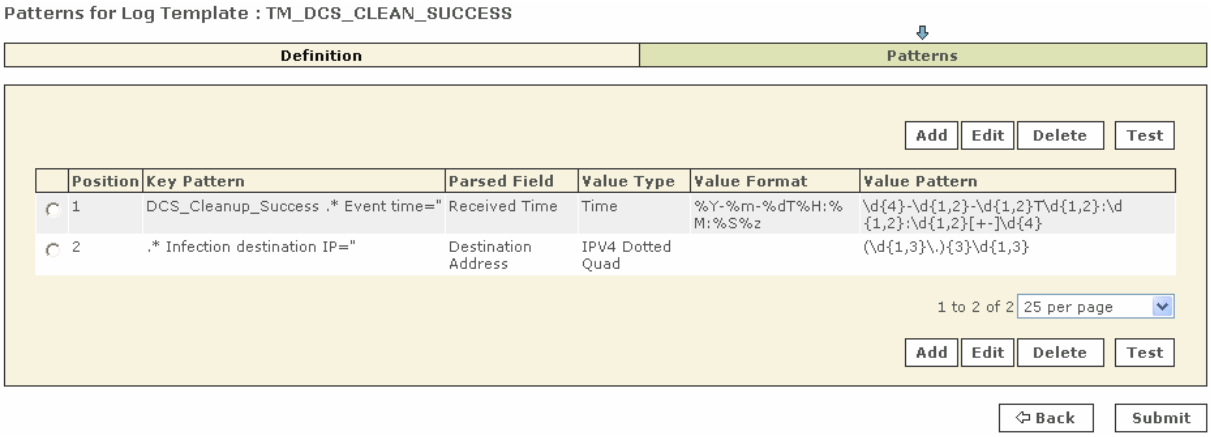
Step 16 Click **Add** button to parse the 2nd value for **Destination Address** field. Supply the fields with the value found under this table, the remaining fields will automatically populate with the correct data.

Fields	Value
Position	2
Key Pattern	.* Infection destination IP="
Parsed Field	Destination Address
Value Type	IPV4 (Dotted Quad)
Pattern Name	IPV4_DOTQUAD
Value Pattern	(\d{1,3}\.){3}\d{1,3}

.



Step 17 Click **Submit**.



Step 20 Check if the pattern is working, click **Test** button on the Pattern section, a new window will appear.

Step 21 Copy/Paste a sample log from Trend Micro Damage Cleanup Service 3.2 into the Log message box.

Note: The parsing patterns for the example above are specified to match the following example raw message reported in an event.

DCS_Cleanup_Success Security product = "DamageCleanupServices" Event time="2007-04-05T16:57:18-0800" Infection destination IP="10.10.0.21"

Step 22 Click **Submit** to verify the pattern you have created. All status for each row must show **Ok**.

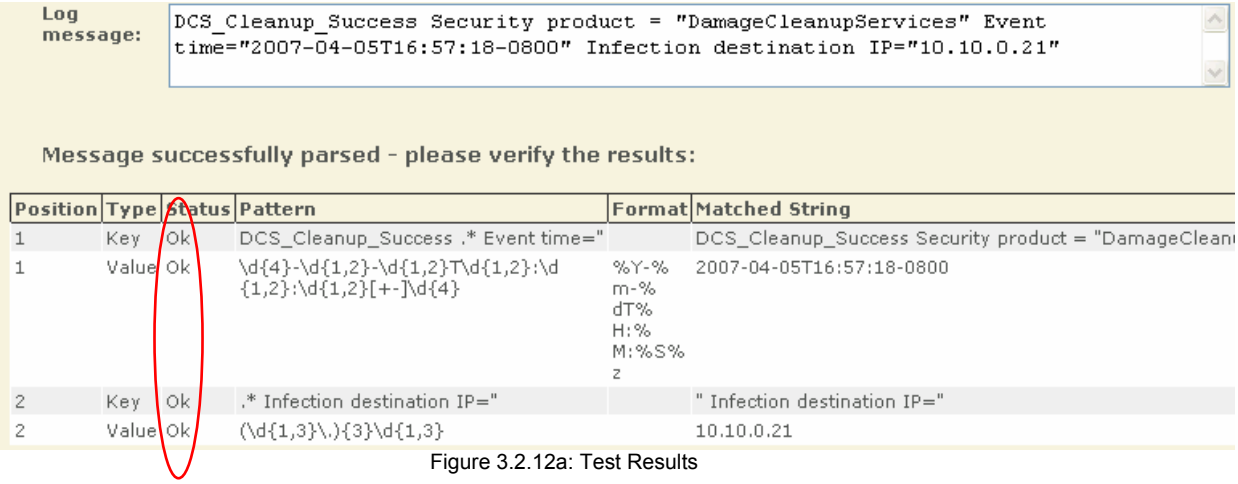
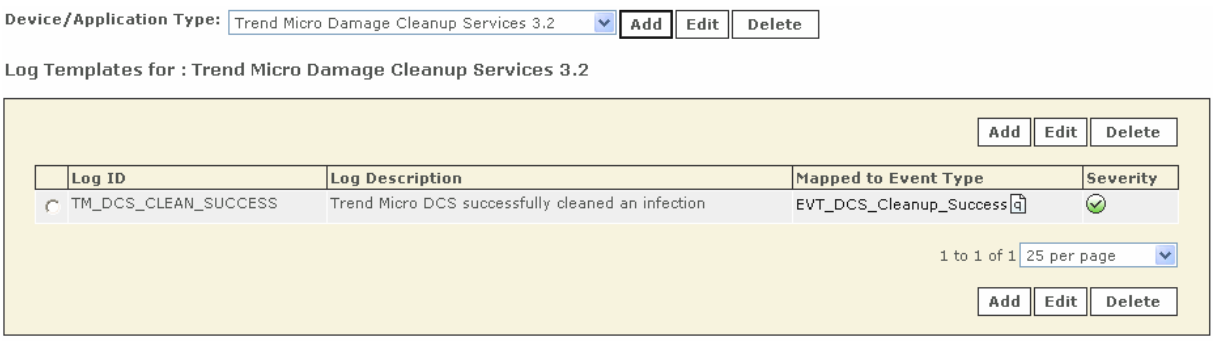


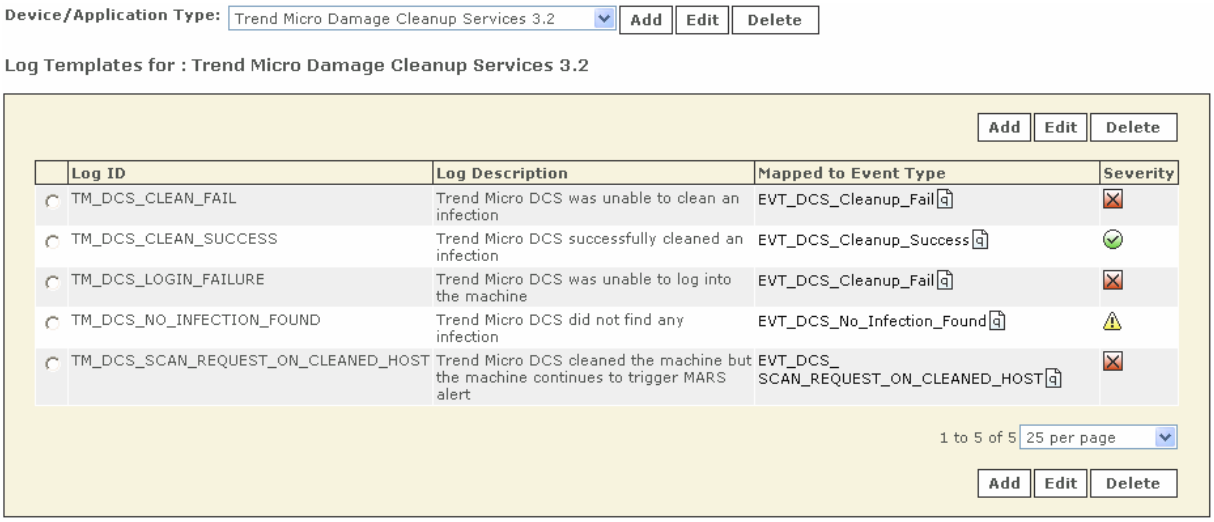
Figure 3.2.12a: Test Results

Step 23 Close the **Test Parsing Patterns** window and click **Submit** in the **Parser Patterns** window.



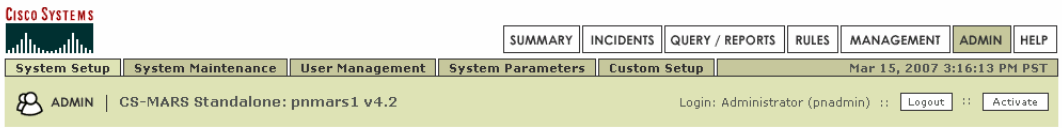
Step 24 Redo **Step 1 to 23** referring to the chart at the start of this chapter to add each of the events into MARS.

TM_DCS_CLEAN_SUCCESS
TM_DCS_CLEAN_FAIL
TM_DCS_LOGIN_FAILURE
TM_DCS_NO_INFECTION_FOUND
TM_DCS_ SCAN_REQUEST_ON_CLEANED_HOST

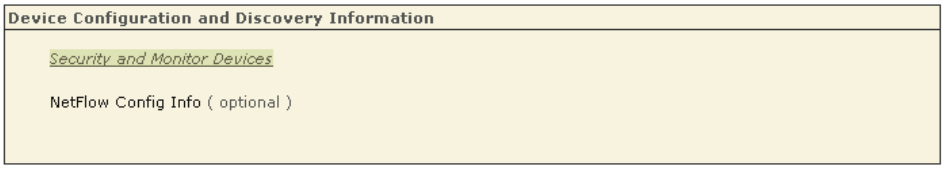


5.1.3 Add Damage Cleanup Service Application as a Reporting Device

Step 1 Go to **Admin > System Setup** Tab.

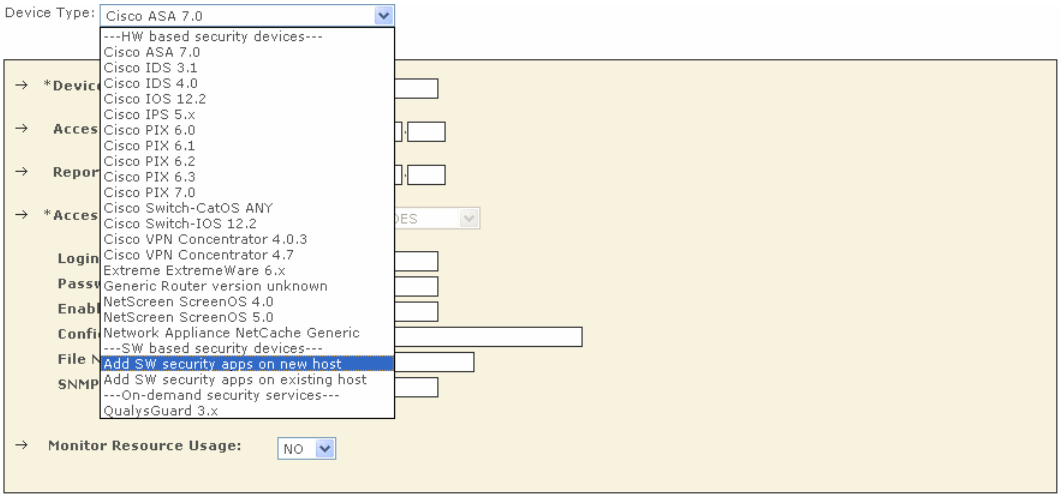


Step 2 Click the **Security and Monitor Devices**.



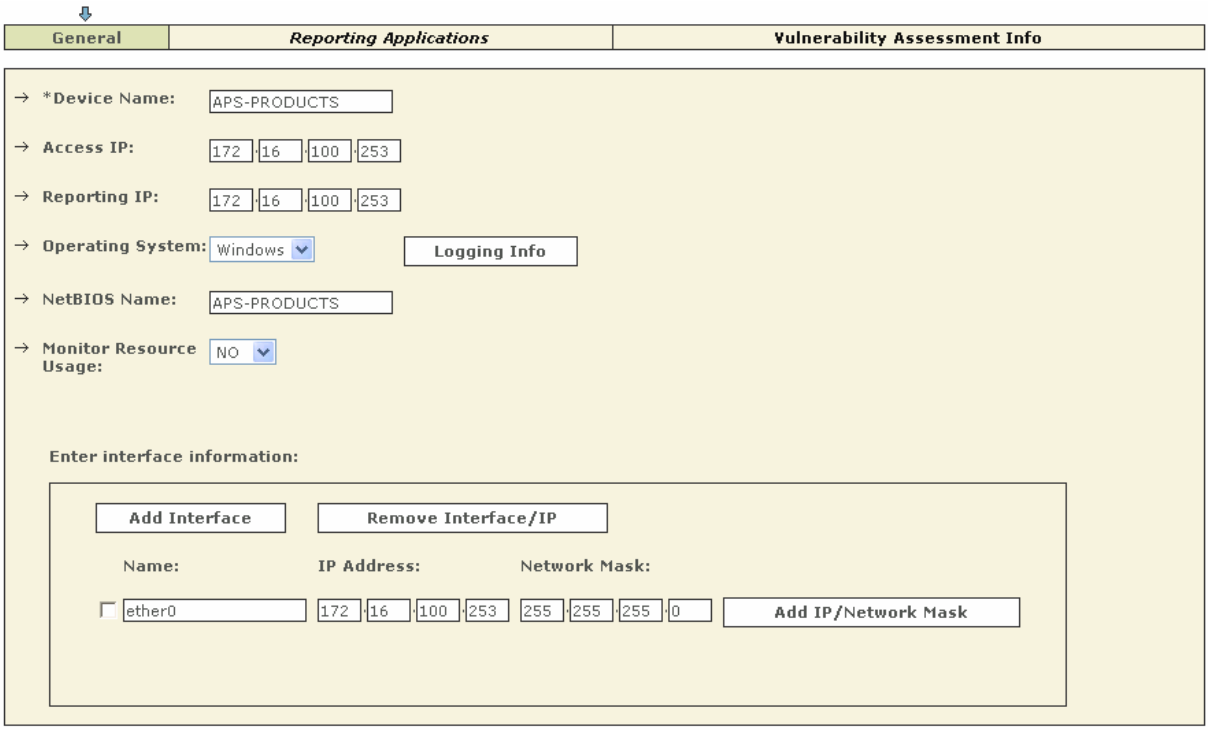
Step 3 Click **Add** to add a new device.

Step 4 From the **Device Type** list, select **Add SW security apps on new host**.

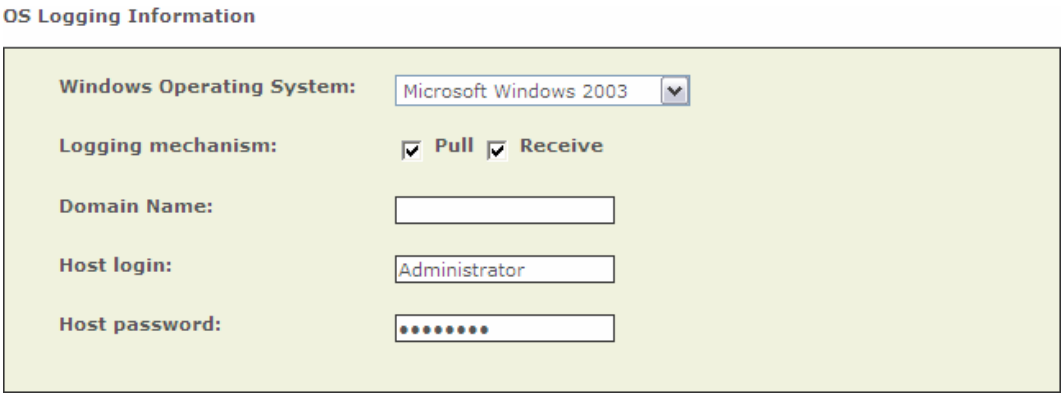


Step 5 Fill in the name and other host details of the server running the MARS-DCS plug-in. Click on the Logging Info button and supply the necessary information. Click **Apply**.

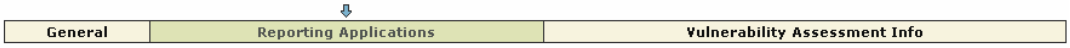
Fields	**Value**
Device Name	ServerName
Access IP	172.16.100.253
Reporting IP	172.16.100.253
Operating System	Windows
Netbios Name	ServerName
Monitor Resource Usage	No
Interface Information: Name	Ether0
Interface Information: IP Address	172.16.100.253
Interface Information: Network Mask	255.255.255.0



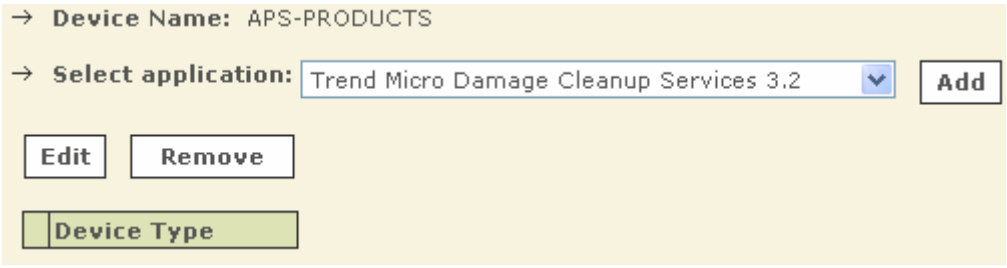
Logging Info Button	
Fields	**Value**
Windows Operating System	Microsoft Windows 2003
Logging Mechanism	Pull and Receive (check both)
Domain Name:	
Host Login	Administrator
Host Password	password



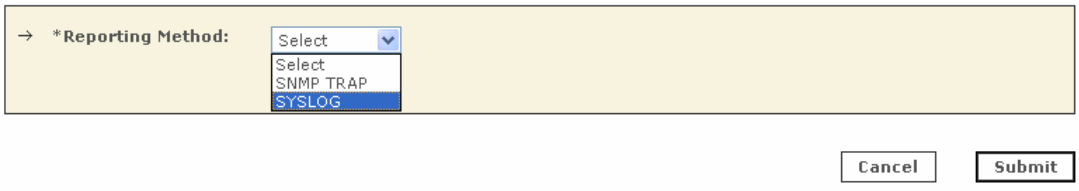
Step 6 Click the **Reporting Applications** tab.



Step 7 Select **Application** (Trend Micro Damage Cleanup Service 3.2) from the list and click **Add**.



Step 8 Select **SYSLOG** as the Reporting Method and click **Submit**. This option determines the type of logs that will be processed by the custom log parser



Step 9 Click **Done** button and the MARS-DCS plug-in service has been added into MARS.

Verification Procedure:
The server with the MARS-DCS plug-in has been successfully added to MARS

5.2 Adding User Defined Inspection Rules

DCS Rules

Rule Name: Trend Micro Rule: Damage Cleanup Services - Cleanup Success	
Rule Description: This rule allows MARS to trigger an incident every time MARS-DCS plug-in sends a syslog notification to the MARS device that is related to cleanup success.	
• **Sources**	ANY
• **Destination**	ANY
• **Service**	ANY
• **Event Types**	EVT_DCS_Cleanup_Success

• **Reporting Devices**	ANY
• **Reported User**	ANY
• **Keywork**	ANY
• **Severity**	ANY
• **Count**	1

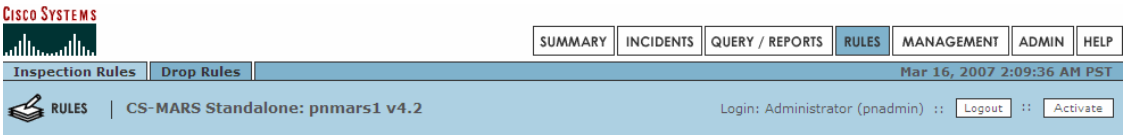
Rule Name: Trend Micro Rule: Damage Cleanup Services - Cleanup Fail	
Rule Description: This rule allows MARS to trigger an incident every time MARS-DCS plug-in sends a syslog notification to the MARS device that is related to cleanup failure.	
• **Sources**	ANY
• **Destination**	ANY
• **Service**	ANY
• **Event Types**	EVT_DCS_Cleanup_Fail
• **Reporting Devices**	ANY
• **Reported User**	ANY
• **Keywork**	ANY
• **Severity**	ANY
• **Count**	1

Rule Name: Trend Micro Rule: Damage Cleanup Services – No Infection Found	
Rule Description: This rule allows MARS to trigger an incident every time MARS-DCS plug-in sends a syslog notification to the MARS device that is related to no infection found.	
• **Sources**	ANY
• **Destination**	ANY
• **Service**	ANY
• **Event Types**	EVT_DCS_No_Infection_Found
• **Reporting Devices**	ANY
• **Reported User**	ANY
• **Keywork**	ANY
• **Severity**	ANY
• **Count**	1

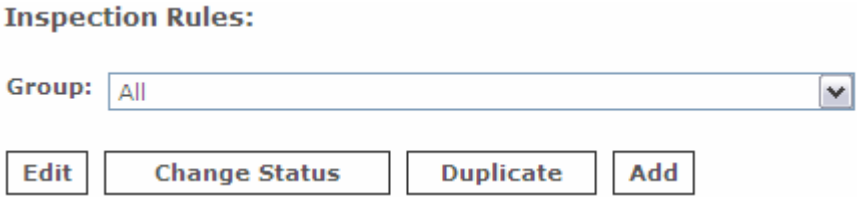
Rule Name: Trend Micro Rule: Damage Cleanup Services - Repetitive Cleanup Request	
Rule Description: This rule allows MARS to trigger an incident every time MARS-DCS plug-in sends a syslog notification to the MARS device that is related to MARS-DCS plug-in attempt to clean a machine that has already been scanned before but no infection was found. The machine is still in violation of security policy and must be examined.	
• **Sources**	ANY
• **Destination**	ANY
• **Service**	ANY
• **Event Types**	EVT_DCS_ SCAN_REQUEST_ON_CLEANED_HOST
• **Reporting Devices**	ANY
• **Reported User**	ANY
• **Keywork**	ANY
• **Severity**	ANY
• **Count**	1

Sample Rule: Trend Micro Rule: Damage Cleanup Services - Cleanup Success

Step 1 Go to **Rules** Tab.

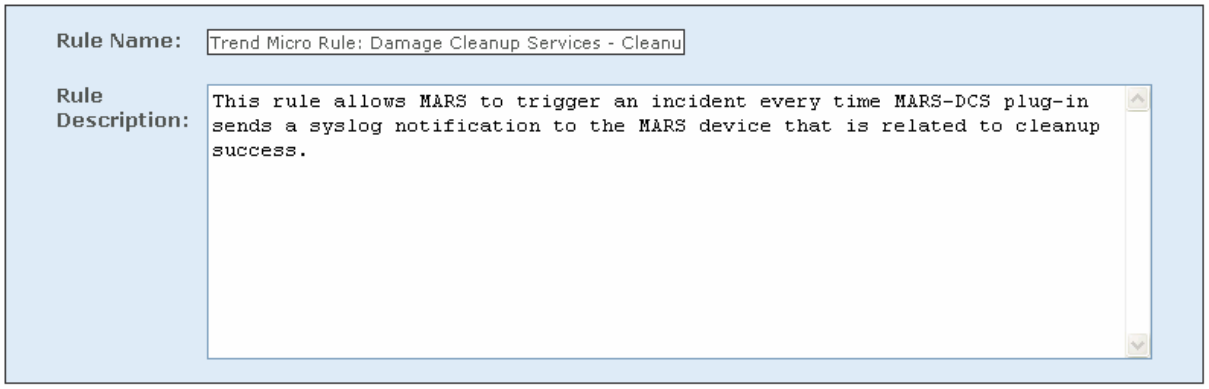


Step 2 Click the **Add** button.



Step 3 Enter a name and description for the rule and click **Next**.

- **Rule Name**: Trend Micro Rule: Damage Cleanup Service – Cleanup Success
- **Description**: This rule allows MARS to trigger an incident every time MARS-DCS plug-in sends a syslog notification to the MARS device



Step 4 Select **Source IP Address (ANY)** and click the **Next** button.

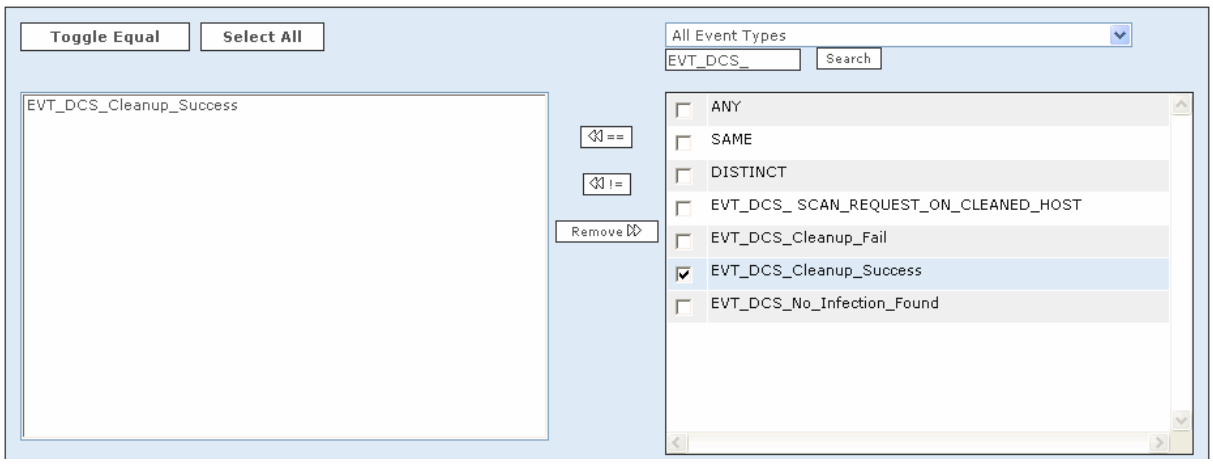
Step 5 Select **Destination IP Address (ANY)** and click the **Next** button.

Step 6 Select **Service Name (ANY)** and click the **Next** button.

Step 7 On the right pane of the **Event Types**, choose **All Event Types** from the drop down menu. Type the keyword EVT_DCS_ and click the **Search** button.

Step 8 Add the following events to the left hand pane and click **Next** button.

- **EVT_DCS_Cleanup_Success**



Step 8 Select **Device (ANY)** and click the **Next** button.

Step 9 Select **Reported User (ANY)** and click the **Next** button.

Step 10 Select **Keyword (ANY)** and click the **Next** button.

Step 11 Select **Severity (ANY)** and **Counts (1)** then click the **Next** button.

Step 12 Click **YES,** when prompted with the question "Are you done refining the rule conditions?"

Step 13 On the **Action** section. Click **Next.**

Step 14 On the **Time Range (no change)**. Click **Next**.

Step 15 Click **Submit**.

Step 16 Redo **Step 1 to 15** referring to the chart at the start of this chapter to add each of the DCS rules into MARS.

Trend Micro Rule: Damage Cleanup Services - Cleanup Success
Trend Micro Rule: Damage Cleanup Services - Cleanup Fail
Trend Micro Rule: Damage Cleanup Services – No Infection Found
Trend Micro Rule: Damage Cleanup Services - Repetitive Cleanup Request

Step 17 Click the **Activate** button on the top right corner of the MARS console to apply all the configuration changes made.

6. Configuring MARS reporting for DCS related events

On this example we are creating a report for all DCS events. It is also possible to generate reports only for specific DCS events like cleanup successful or clean fail events.

6.1 Adding User Defined Reports

Step 1 Click the **Query/Reports** tab.

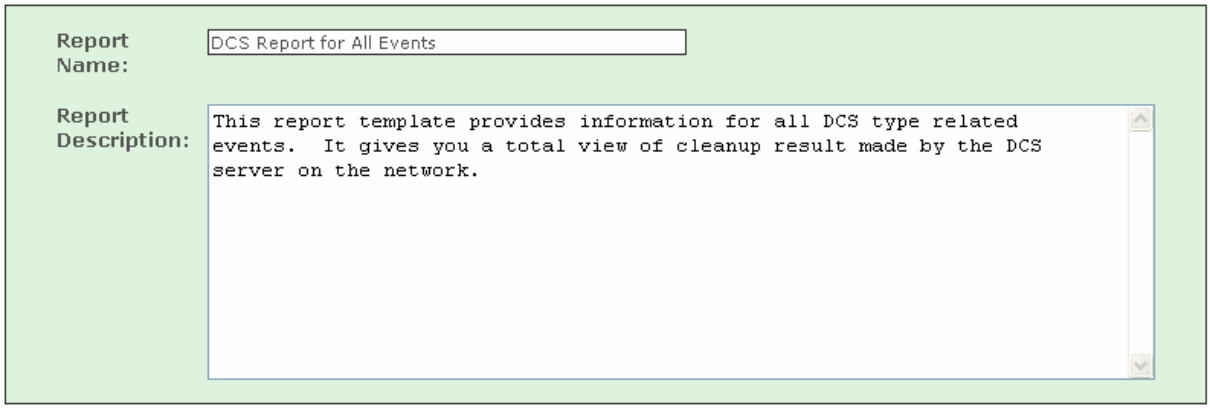
Step 2 Click **Report**

Step 3 Under **Report Selection** section, select **User Reports** by the **Group** drop down box

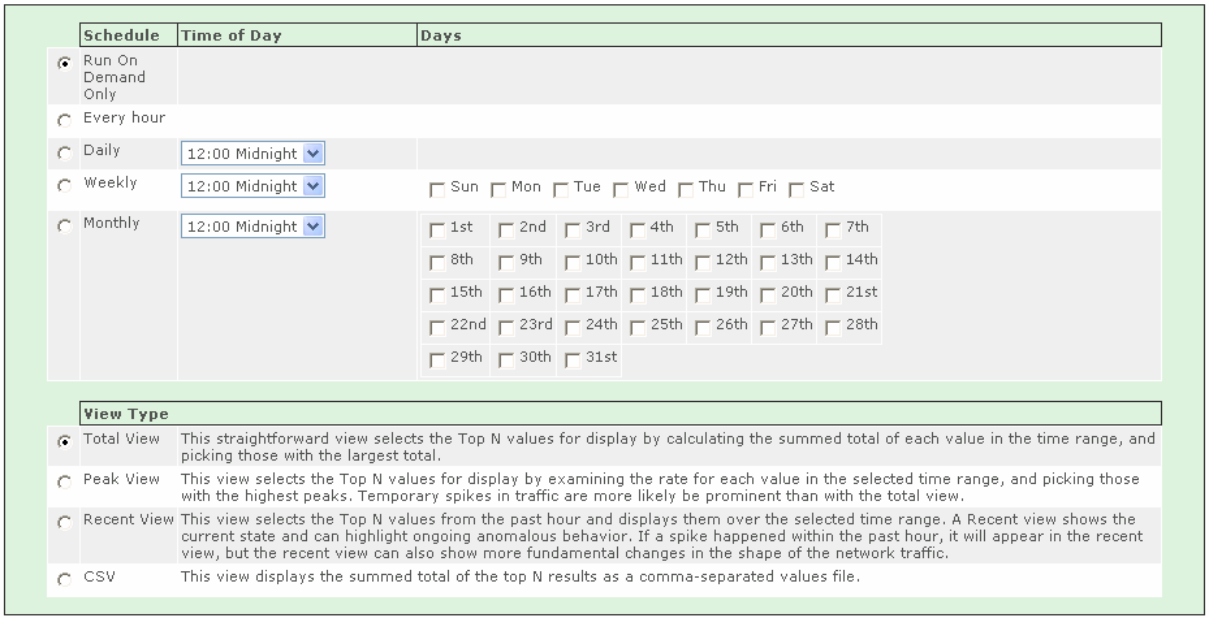
Step 4 Click **Add**

Step 5 Enter the **name** and **description** of the report. Click **Next**

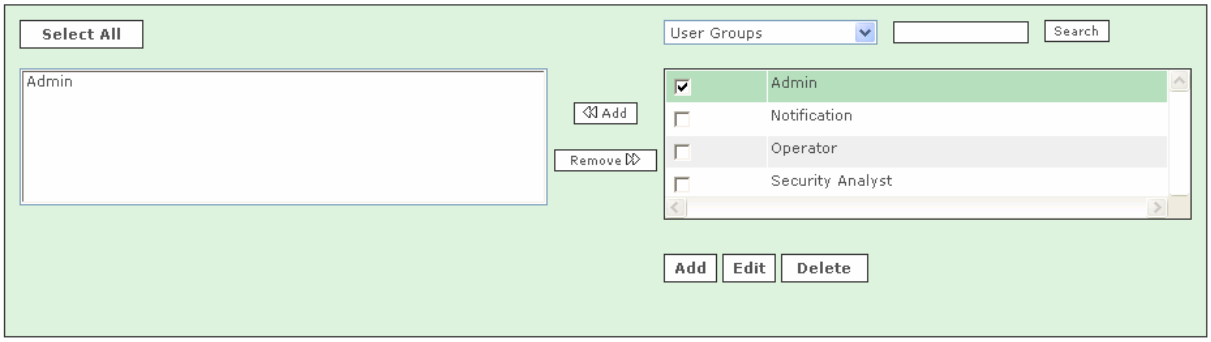
Name	**Description**
DCS Report for All Events	This report template provides information for all DCS type related events. It gives you a total view of cleanup result made by the DCS server on the network.



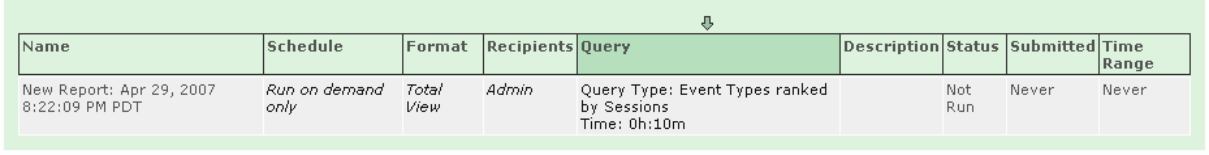
Step 6 Select **Run on Demand Only** and **Total View**. Click **Next**



Step 7 Add your preferred **user accounts** to the list of **recipients**, click **next**

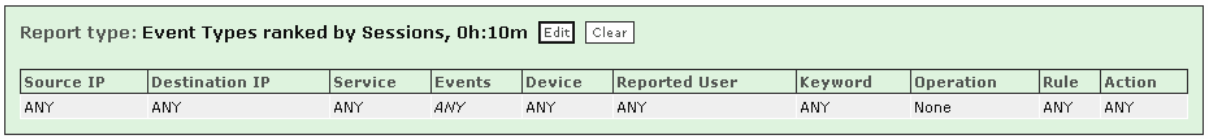


Step 8 You are now on the query section.



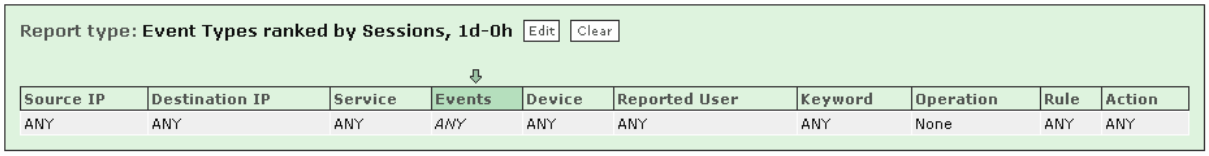
Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
New Report: Apr 29, 2007 8:22:09 PM PDT	*Run on demand only*	*Total View*	*Admin*	Query Type: Event Types ranked by Sessions Time: 0h:10m		Not Run	Never	Never

Step 9 Under **Query Event Data**, click on **Edit** button



Step 10 Modify the **Filter by Time** to **Last 1 Day(s) 0 Hours 0 Minutes**, click **Apply**

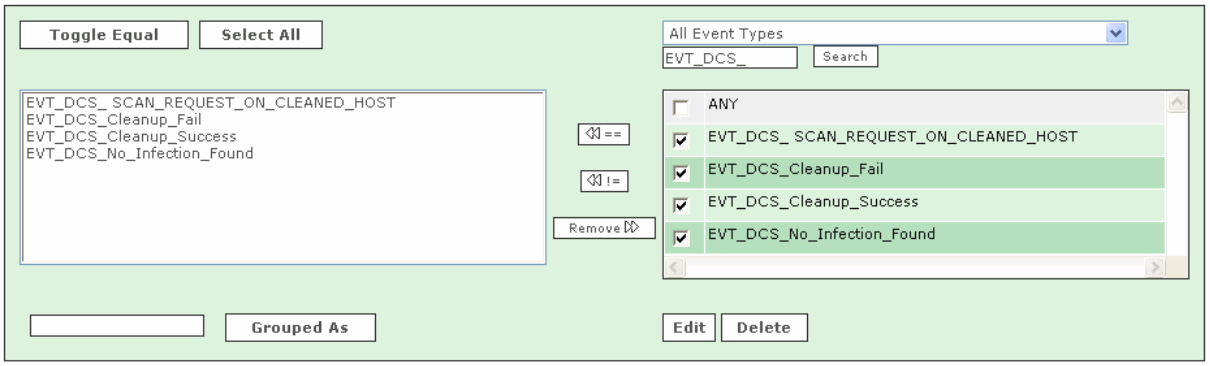
Step 11 Click on the link **ANY** under **Events**



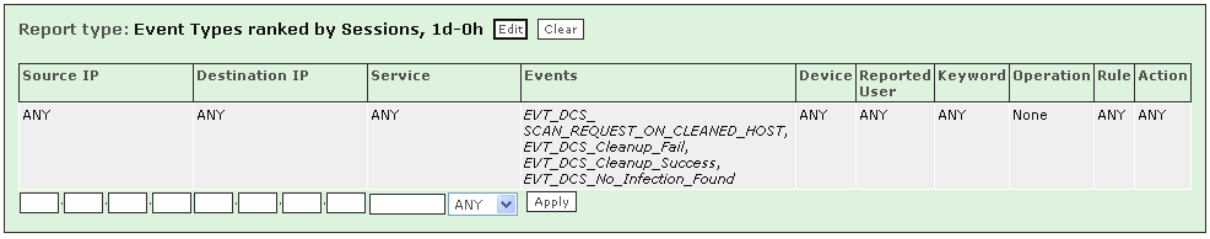
Step 12 On the right pane of the **Event Types**, choose **All Event Types** from the drop down menu. Type the keyword EVT_DCS_ and click the **Search** button.

Step 13 Remove **ANY** and add **DCS type events** to the left hand pane. Click **Apply**.

- EVT_DCS_ SCAN_REQUEST_ON_CLEANED_HOST
- EVT_DCS_Cleanup_Fail
- EVT_DCS_Cleanup_Success
- EVT_DCS_No_Infection_Found

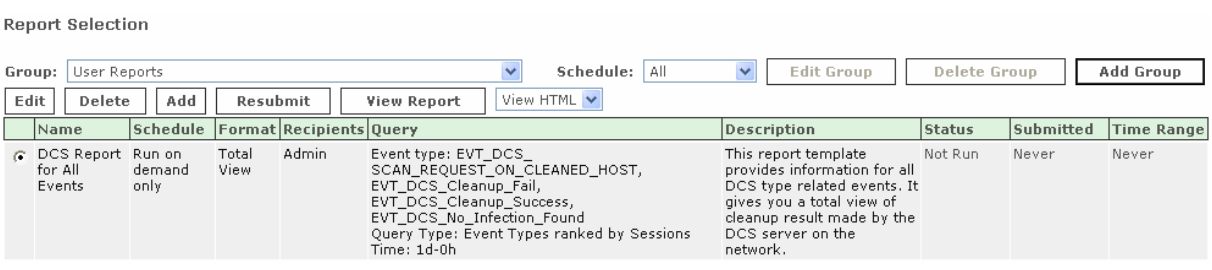


Step 14 You have completed the query type configuration. Click **Next**



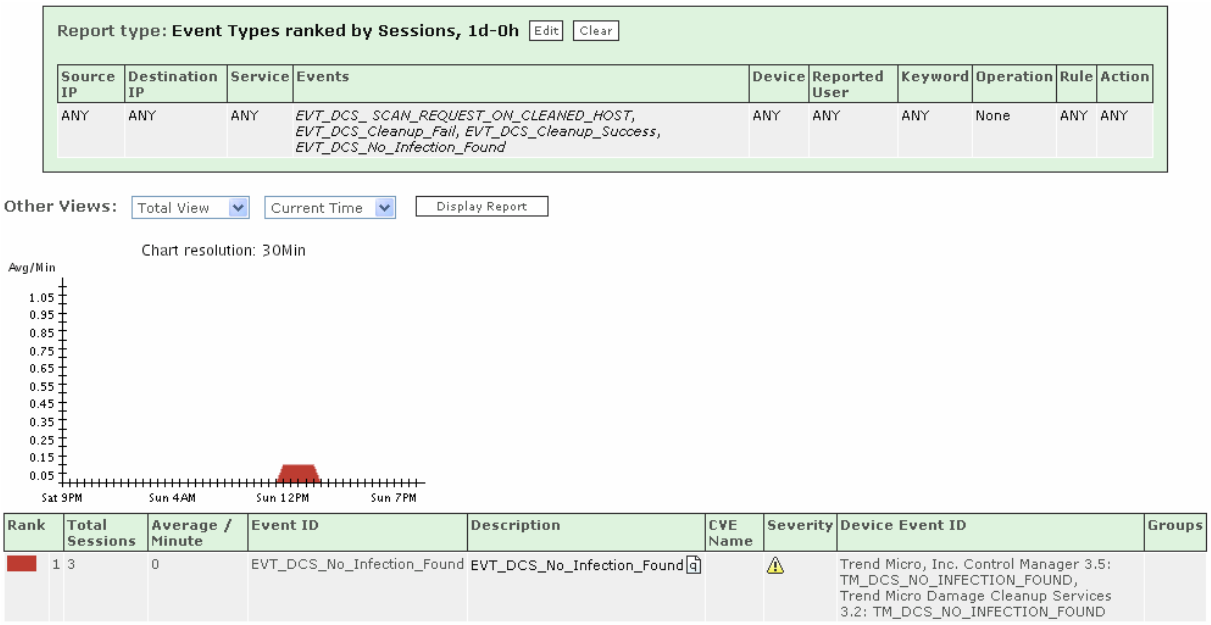
Step 15 Click **Submit** to create the report template.

Step 16 Go back to the **Query / Reports → Reports** Tab. Select the new report and click **Resubmit** button



Step 17 Go back to the **Query / Reports → Reports** Tab. Select the new report and click **Resubmit** button

Step 18 After the report finished generating itself. Select the report and click **View Report** and see the DCS cleanup result for the day.



Report type: **Event Types ranked by Sessions, 1d-0h** Edit Clear

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	*EVT_DCS_ SCAN_REQUEST_ON_CLEANED_HOST, EVT_DCS_Cleanup_Fail, EVT_DCS_Cleanup_Success, EVT_DCS_No_Infection_Found*	ANY	ANY	ANY	None	ANY	ANY

Other Views: Total View | Current Time | Display Report

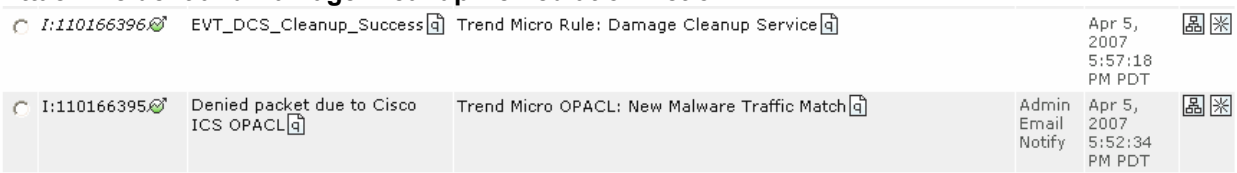
Chart resolution: 30Min

Rank	Total Sessions	Average / Minute	Event ID	Description	CVE Name	Severity	Device Event ID	Groups
1	3	0	EVT_DCS_No_Infection_Found	EVT_DCS_No_Infection_Found		⚠	Trend Micro, Inc. Control Manager 3.5: TM_DCS_NO_INFECTION_FOUND, Trend Micro Damage Cleanup Services 3.2: TM_DCS_NO_INFECTION_FOUND	

7. Verify Damage Cleanup Service and MARS configuration

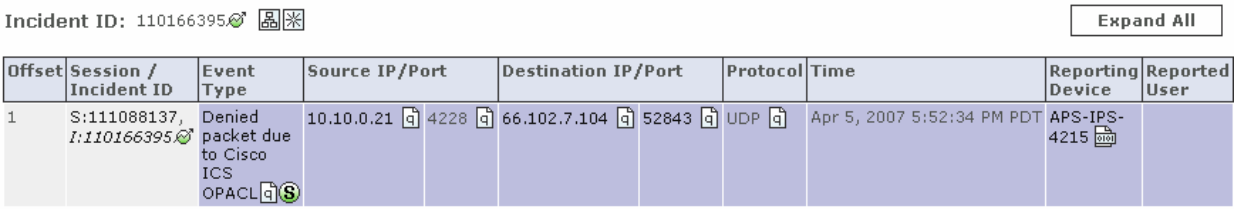
Follow the beta test script documentation to validate if the MARS-DCS plug-in is working properly on your environment.

Attack Incident and Damage Cleanup Remediation Action



I:110166396	EVT_DCS_Cleanup_Success	Trend Micro Rule: Damage Cleanup Service		Apr 5, 2007 5:57:18 PM PDT	
I:110166395	Denied packet due to Cisco ICS OPACL	Trend Micro OPACL: New Malware Traffic Match	Admin Email Notify	Apr 5, 2007 5:52:34 PM PDT	

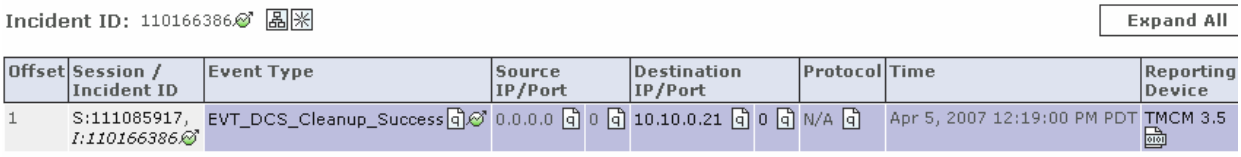
Detailed View of an Incident with Source and Destination IP of the attack:



Incident ID: 110166395 Expand All

Offset	Session / Incident ID	Event Type	Source IP/Port		Destination IP/Port		Protocol	Time	Reporting Device	Reported User
1	S:111088137, *I:110166395*	Denied packet due to Cisco ICS OPACL (S)	10.10.0.21	4228	66.102.7.104	52843	UDP	Apr 5, 2007 5:52:34 PM PDT	APS-IPS-4215	

Detailed View of an Incident of the cleanup action done by Damage Cleanup Service:



Incident ID: 110166386 Expand All

Offset	Session / Incident ID	Event Type	Source IP/Port		Destination IP/Port		Protocol	Time	Reporting Device
1	S:111085917, *I:110166386*	EVT_DCS_Cleanup_Success	0.0.0.0	0	10.10.0.21	0	N/A	Apr 5, 2007 12:19:00 PM PDT	TMCM 3.5

8. Appendixes

==========
Caveats
==========

- When plug-in is stopped, wintail window (if configured) is not killed. It has to be killed manually. Otherwise the listening port use by the MARS-DCS plug-in will not be released.

- The generated log file dcsp_log.txt grows continuously in this version. This has to be deleted manually if it grows too big. In the next version of plug-in, the size will be capped at the file will be recycled once the limit is reached.

- The contents of the log file dcsp_log.txt are deleted on every plug-in restart.

- Plugin does not check for duplicate entries in the config file in the lists
    - Clean_Exception_List
    - Internal_Network_List
    - DCS_Server_List

==========
Dealing with configuration changes
==========

- All the configuration changes are pickup by the Plugin when it is restarted with the exception of the following.
    - When "http_listen_port" value is modified, the plug-in has to un-register with the DCS servers first and then re-register. So, the sequence of steps is:
        1. Stop the plug-in
        2. Run the command "python dcsp_unregister.pyc all"
        3. Start the plug-in

==========
Other notes on configuration parameters
==========

- A maximum of 50 entries are allowed in "Clean_Exception_List" Excess entries are ignored.

- A maximum of 10 entries are allowed in "Internal_Network_List" Excess entries are ignored.

- A maximum of 10 entries are allowed in "DCS_Server_List" Excess entries are ignored.

- The config parameter "use_hostname_in_dcs_req" (set to "no" by default) allows the plug-in to send IP addresses of the infected machines in the cleanup requests even if MARS reports hostname in the notification. This is because DCS Server doesn't seem to like the hostnames (it doesn't send anything back).

- Recommended log level setting is "info" (this is also the default)

9. Bug Fixes

==========
Version 1.0.2
==========

- Check if the MARS-DCS plug-in listening port is already in use or not, if the port is available it will then register to Trend Micro DCS server.

- The MARS-DCS plug-in will no longer initiate a cleanup to an invalid IP, network address or broadcast address.

==========
Version 1.0.3
==========

- Daylight Saving Time can now be properly recognized and syslog notification will now be able to send the correct time to MARS.

- Properly handle emails with attachments that are receive by the DCS mailbox. "invalid attachments", "valid but not mars notifications", and "any other attachments" are now gracefully ignored by the MARS-DCS plug-in

- Broadcast addresses in MARS xml attachment will now be ignored by the MARS-DCS plug-in

- In the plug-in configuration file dcsp_config.xml, empty strings for value attribute are no longer allowed.

    - e.g. The following will result in an error during plug-in initialization because ip_net is empty.
    - <DCS_Server ip_net="" ip_mask = "0.0.0.0" server_name = "10.2.42.212" server_port = "80" />

- Disallow invalid IP address and netmask where ever applicable in the dcsp_config.xml

10. Configuring the MARS-DCS plug-in to run as a service

Step 1 Stop the plug-in if it is running.

Step 2 Install Windows 2000 or Windows 2003 **Resource Kit** (or copy the 2 binaries **instsrv.exe** and **srvany.exe**). You can download the free kit from Microsoft's website.

- http://www.microsoft.com/downloads/details.aspx?familyid=9D467A69-57FF-4AE7-96EE-B18C4790CFFD&displaylang=en

Step 3 Open a command prompt and run **instsrv** to install **srvany.exe** as a service with the name "**DCS Plugin**"

- C:\> "C:\Program Files\Resource Kit Tools\instsrv" "DCS Plugin" "C:\Program Files\Resource Kit Tools\srvany.exe"

Step 4 Go to **Control Panel** → **Administrative Tools** → **Computer Management** → **Services**. Ensure that "**DCS Plugin**" is listed as a service and the startup type is "**automatic**".

Step 5 Create **registry** entries for the DCS Plugin service

Step 6 Go to **Start** → **Run** → **regedit**. Go to the registry key hive **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DCS Plugin**

Step 7 Add new key called "**Parameters**"

Step 8 Add these three values (all string values) under the **Parameter** key

- "Application"="C:\Python25\pythonw.exe"
- "AppDirectory"="C:\DCS_Plugin"
- "AppParameters"="C:\DCS_Plugin\dcs_plugin.pyc"

Note: Make sure to set the directory names according to your installation.

Step 9 Open the file dcsp_config.xml and set parameters **<use_wintail value="no">** and **<Run_As_Service value="yes" />**. This is needed for the plug-in to run as a service.

Step 10 Perform a test by starting and stopping the "**DCS Plugin**" service in **Computer Management** → **Services**.

Verification Procedure:
The service is running and if the MARS-DCS plug-in is set to run in debug mode, you will be able to check the file dcsp_log.txt that the service is checking for emails every few seconds based on your defined time intervals. This is a sign the utility is operational.

11. Enabling of POP3 Service on a Windows 2003 Server

The DCS plug-in for CS-MARS requires POP3 be enabled on your mail server. If you are unable to enable POP3 on your existing mail server the following procedure will enable POP3 and SMTP on another server to allow you to use the plug-in without modifying your existing mail server.

In the MARS device, you can only specify one SMTP server, all notifications from MARS will be sent to this server, and we can then relay messages from your existing server to the new mail server that is setup for the DCS plug-in.

Step 1 Log into the machine using an account with administrative privileges.

Step 2 Go to **Control Panel** and open **Add/Remove Programs**

Step 3 Click on Add/Remove **Windows Components**

Step 4 Under Components, enable **E-mail Services**

Step 5 Click **next** and finish the installation

Step 6 2 services will be added to your machine. **Simple Mail Transfer Protocol (SMTP)** and **Microsoft POP3 Service**

Step 7 Go to **Start** >> **All Programs** >> **Administrative Tools** >> **POP3 Service.** At the POP3 service console, beneath your **server name icon**, create a **new domain** . This can be either a stand-alone mail only domain, or part of your Windows Active Directory structure.

Step 8 After you have created the **domain name**, highlight the **domain name** and create a user mailbox called DCSMail. The mailbox will be created, if you selected an Active Directory integrated domain in the previous step a user account will also be created on your domain.

Step 9 This mailbox is now able to receive emails and emails can be downloaded from this server via the POP3 protocol.

Step 10 In the MARS-DCS plug-in configuration file set the mail server to the IP/FQDM of the machine selected above.

Step 11 On your existing mail server configure the mailbox that will receive notifications from MARS to forward them to the email account created in **Step 8**.

.

Note: We do not want to reconfigure MARS to point directly to the new POP3 server, although this will work and allow the MARS-DCS plug-in to work as intended, but notification from MARS to email accounts that do not exist on our POP3 server will no longer be relayed to their intended destination.

If anyone has questions regarding Trend-Cisco solutions, email:
Alliance_Support@trendmicro.com