Cisco ICM/IPCC Enterprise and Hosted Anti-Virus Software Guidelines

Introduction

This document provides guidelines for implementing anti-virus software in a Cisco ICM/IPCC Enterprise (or Hosted) solution.

Caution Cisco CCBU does not formally certify anti-virus software products; the guidelines in this document are based on the experience of Cisco CCBU QA test laboratory environments and customers who have successfully implemented anti-virus software with Cisco software solutions.

Viruses can be unpredictable; Cisco cannot assume responsibility for consequences of virus attacks on mission-critical applications.

The guidelines in this document apply to the following CCBU software products:

- Cisco Intelligent Contact Management (ICM) Enterprise
- Cisco ICM Hosted
- Cisco IPCC Enterprise
- Cisco IPCC Hosted
- All CCBU components of these solutions

Of these products, particular care should be taken for systems that use Microsoft Internet Information Server (IIS): Web Collaboration Option, Cisco Media Blender, E-Mail Manager Option, and Cisco WebView / WebView II. In addition, your corporate anti-virus strategy should include specific provisions for any server positioned outside the corporate firewall or subject to frequent connections to the Public Internet.

Cisco CCBU QA test laboratories currently use the following anti-virus software products:

- Network Associates (McAfee) NetShield 4.5.1 service pack 1 (Full Mode)
- McAfee ScanEngine 4.2.60 (upgraded weekly)
- McAfee Virus Definitions 4.0.4285 (updated nightly)

Note ScanEngine and Virus Definition versions as of August 13, 2003.

Anti-Virus Software Caveats

Please take note the following caveat before running anti-virus software on systems installed with CCBU software products:

- Many default anti-virus software configuration settings can adversely affect the performance of the Cisco CCBU products listed on page 1. This performance degradation is a result of increased CPU load and memory use by the anti-virus software program.
- The anti-virus software should not be set to run in an “automatic” or “background” mode where all incoming data or modified files are scanned in real time.
- Full scans of systems by the anti-virus software should be set to run **only** during scheduled maintenance windows.
- Anti-virus software scanning engines and definition files should be updated on a regular basis, following your organization’s current security/anti-virus policy.

Anti-Virus Software Configuration Guidelines

Before scheduling anti-virus software activity on Cisco ICM nodes, it is important to note a few parameters that control the application’s activity at specific times. Anti-virus software configuration settings should avoid scheduling “Daily Scans,” “Automatic DAT Updates,” and “Automatic Product Upgrades” during the times specified as described below.

Note Beginning with Release 5.0 of Cisco ICM, the Recovery process in the Logger and Distributor no longer perform the Update Statistics operation. Therefore, it is important to take into consideration the schedule specified in the Update Statistics registry keys.

- **Logger.** Check the Schedule settings for the Purge and Update Statistics registry keys on the ICM Logger:
  - Logger registry keys, **Release 5.0**:

    HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<*inst*>\Logger<*A/B*>\Recovery\CurrentVersion\Purge\Schedule\Schedule
    Value Name: Schedule

    HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<*inst*>\Logger<*A/B*>\Recovery\CurrentVersion\UpdateStatistics\Schedule
    Value Name: Schedule
  - Logger registry keys, **Release 4.6.2**:

    HKLM\SOFTWARE\GeoTel\ICR\<*inst*>\Logger<*A/B*>\Recovery\CurrentVersion\Purge\Schedule\Schedule
    Value Name: Schedule

    HKLM\SOFTWARE\GeoTel\ICR\<*inst*>\Logger<*A/B*>\Recovery\CurrentVersion\UpdateStatistics\Schedule
    Value Name: Schedule

- **Distributor.** Check the Schedule settings for the Purge and Update Statistics registry keys on the Distributor nodes:
  - Distributor registry keys, **Release 5.0**:

    HKLM\SOFTWARE\Cisco Systems, Inc. \ICM\<*inst*>\Distributor\RealTimeDistributor \CurrentVersion\Recovery\CurrentVersion\Purge\Schedule\Schedule
    Value Name: Schedule

    HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<*inst*>\Distributor\RealTimeDistributor \CurrentVersion\Recovery\CurrentVersion\UpdateStatistics\Schedule
    Value Name: Schedule
  - Distributor registry keys, **Release 4.6.2**:

    HKLM\SOFTWARE\GeoTel\ICR\<*inst*>\Distributor\RealTimeDistributor\CurrentVersion \Recovery\CurrentVersion\Purge\Schedule\Schedule
    Value Name: Schedule

    HKLM\SOFTWARE\GeoTel\ICR\<*inst*>\Distributor\RealTimeDistributor\CurrentVersion \Recovery\CurrentVersion\UpdateStatistics\Schedule
    Value Name: Schedule
- **Router/PG.** On the ICM Router and Peripheral Gateway (PG), do not schedule anti-virus program tasks:
  - During times of heavy or peak call load.
  - At the *half hour* and *hour* marks, as ICM processes increase during those times.
- **All Nodes.** Other scheduled ICM processes activities can be found on Windows 2000 servers by inspecting the Scheduled Tasks Folder. In Windows NT 4.0, running an application such as WinAT (or typing **AT** at the command prompt) will reveal the scheduled activity and actions. Scheduled anti-virus program activity should not conflict with those ICM scheduled activities.
- **File Exclusions**. There are a number of binary files that are written to during the operation of ICM processes which have little risk of virus infection. Files with the following file extensions can be safely omitted from the drive and on-access scanning configuration of the anti-virus program:

File Type	ICM Node
*.hst	PG
*.ems	ALL

Anti-Virus Software Configuration Example

This section shows an example of the Network Associates (McAfee) NetShield software configuration found on a typical Cisco CCBU QA test laboratory system. Figure 1 shows a screen capture of the NetShield AntiVirus Console; Table 1 describes the property settings for each console task.

Figure 1 NetShield AntiVirus Console

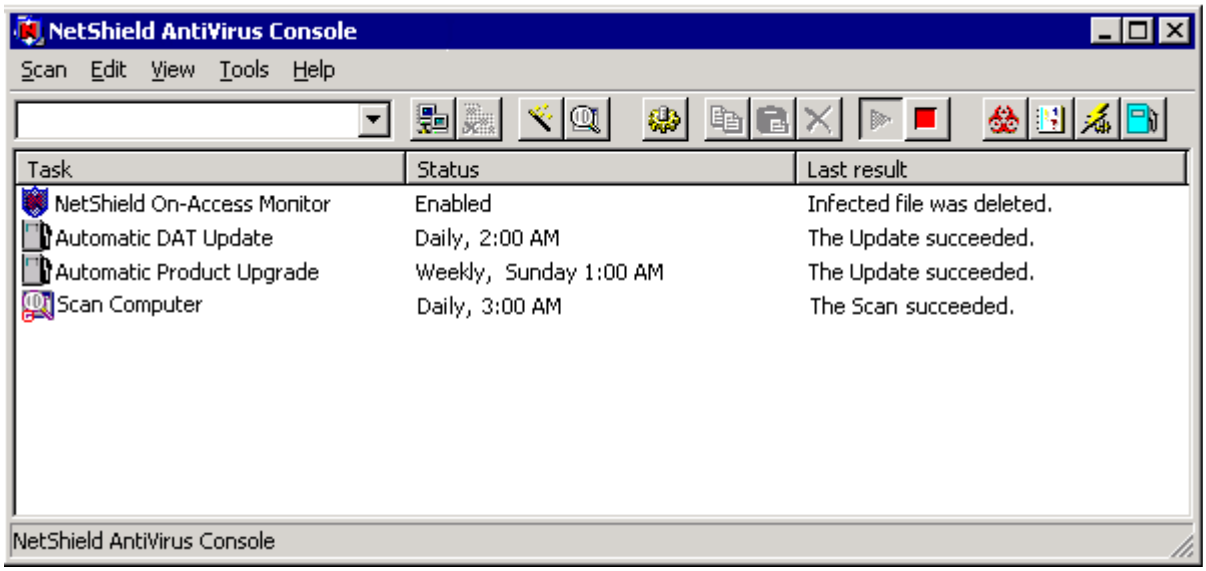

Table 1 Example Antivirus Settings (NetShield AntiVirus Console)

Task	Properties Tab	Suggested Settings
NetShield On-Access Monitor	Detection	1. In the **Scan** section, select: – Inbound files – Boot sector(s) – Floppy during shutdown 2. In the **Files to scan** section, select: – All files
	Advanced	1. In the **Heuristics** section, select: – Find unknown program viruses – Find unknown macro viruses 2. In the **Compressed files** section, select: – Scan compressed files – Scan files in archives – Max archive scan time: 5 sec 3. In the **General section**, select: – Enable file scan caching – Enable on-access scanning at system startup

Table 1 Example Antivirus Settings (NetShield AntiVirus Console)

Task	Properties Tab	Suggested Settings
NetShield On-Access Monitor (continued)	Actions	1. In the **When a virus is found** section, select: – Clean infected files automatically
	Reports	1. In the **Log file** section, select: – Log to file – Limit size of log file – 5000 Kb 2. In the **What to log** section, select: – Virus detection – Virus cleaning – Session summary – Date and time – User name
	Exclusions	1. Click **Add**; the Add Exclusion item dialog box appears. 2. In the **File, folder, or drive to exclude** field, click **Browse** to access the folder where the *.hst and *.ems files reside. 3. Select the Include subfolders checkbox. 4. In the **Exclude from** section, select: – Inbound – Outbound
Automatic DAT Update	Update Options	1. In the **Select Transfer Method** section: – Select Get from an FTP source – Specify an value in the Enter an FTP computer name and director field (for example, ftp.nai.com/virusdefs/4.x) 2. Click **Schedule**; the Schedule dialog box appears. 3. Select the Enable scheduler checkbox. 4. In the **Run** section, select Daily. 5. In the Start At section, specify the time you want the update to begin. **Note** Scheduled time of the DAT Update must not conflict with the scheduled Cisco ICM operations. For more information, see the"Anti-Virus Software Configuration Guidelines" section on page 2.

Table 1 Example Antivirus Settings (NetShield AntiVirus Console)

Task	Properties Tab	Suggested Settings
Automatic Product Upgrade	Transfer Method	1. In the **Select Transfer Method** section: – Select Get from an FTP source – In the Enter an FTP computer name and directory field, specify the location provided by your McAfee resource. **Note** This information is available to registered users. 2. Click **Schedule**; the Schedule dialog box appears. 3. Select the Enable scheduler checkbox. 4. In the **Run** section, select Weekly. 5. In the **Start At** section, specify the time you want the update to begin.
Scan	Detection	1. In the **Item** section, select: – All local drives 2. In the **What to scan** section, select: – Include subfolders – Scan boot sector(s)
	Advanced	1. In the **Heuristics and Compressed files** section, select: – Find unknown program viruses – Find unknown macro viruses – Scan files in archives 2. In the **Scan priority** section, select: – Low – Medium (depending on scheduled time window)
	Actions	1. In the **When a virus is found** section, select: – Clean infected files
	Reports	1. In the **Log file** section, select: – Log to file – Limit size of log file – 5000 Kb 2. In the **What to log** section, select: – Virus detection – Virus cleaning – Session summary – Date and time – User name

Table 1 Example Antivirus Settings (NetShield AntiVirus Console)

Task	Properties Tab	Suggested Settings
Scan (continued)	Schedule	1. Select the Enable scheduler checkbox. 2. In the **Run** section, select Daily. 3. In the Start At section, specify the time you want the update to begin. **Note** Scheduled time of the DAT Update must not conflict with the scheduled Cisco ICM operations. For more information, see the"Anti-Virus Software Configuration Guidelines" section on page 2.
	Exclusions	1. In the **Item** section, select: – pagefile.sys 2. In the **File, folder, or drive to exclude** field, click **Browse** to access the folder where the *.hst and *.ems files reside. 3. Select the Include subfolders checkbox. 4. In the **Exclude from** section, select: – Inbound – Outbound

Note While the configuration settings in Table 1 are specific to the NetShield AntiVirus product, the principles that can be applied to most anti-virus software programs.