General Antivirus Guidelines

Antivirus Guidelines

Antivirus applications have numerous configuration options that allow granular control of what data is scanned, and how the data is scanned on a server.

With any antivirus product, configuration is a balance of scanning versus the performance of the server. The more you choose to scan, the greater the potential performance overhead. The role of the system administrator is to determine what the optimal configuration requirements are for installing an antivirus application within a particular environment. Refer to your particular antivirus product documentation for more detailed configuration information.

You can use third-party antivirus software products that adhere to the guidelines in this chapter. For a list of antivirus software products that are tested by Cisco, see the *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

For more information about the Cisco Guidelines on third-party software product, see the *Cisco Customer Contact Software Policy for Use of Third-Party Software Bulletin* at https://www.cisco.com/c/en/us/products/collateral/customer-collaboration/unified-ip-interactive-voice-response-ivr/prod_bulletin09186a0080207fb9.html.

Warning Often, the default AV configuration settings increase CPU load and memory and disk usage, adversely affecting software performance. Cisco tests specific configurations to maximize product performance. It is critical that you use the following guidelines for using AV software with Unified ICM/Unified CCE.

Viruses are unpredictable and Cisco cannot assume responsibility for the consequences of virus attacks on mission-critical applications. Take particular care for systems that use Microsoft Internet Information Server (IIS).

The following list highlights some general guidelines:

- Ensure that your corporate Antivirus strategy includes specific provisions for any server that is positioned outside the corporate firewall or subject to frequent connections to the public Internet.

- Refer to the *Contact Center Enterprise Compatibility Matrix* for the application and version that is qualified and approved for your release of Unified ICM/Unified CCE.
- Update AV software, and definition files regularly, following your organization's policies.
- Upgrade to the latest supported version of the third-party antivirus application. Newer versions improve scanning speed over previous versions, resulting in lower overhead on servers.

  Avoid scanning of any files that are accessed from remote drives (such as network mappings or UNC connections). Where possible, ensure that each of these remote machines has its own antivirus software installed, thus keeping all scanning local. With a multitiered antivirus strategy, scanning across the network and adding to the network load is not required.
- Schedule full scans of systems by AV software **only** during scheduled maintenance windows, and when the AV scan cannot interrupt other Unified ICM maintenance activities.
- Do not set AV software to run in an automatic or background mode for which all incoming data or modified files are scanned in real time.
- Heuristics scanning has higher overhead over traditional antivirus scanning. Use this advanced scanning option only at key points of data entry from untrusted networks (such as email and internet gateways).
- Real-time or on-access scanning can be enabled, but only on incoming files (when writing to disk). This approach is the default setting for most antivirus applications. Implementing on-access scanning on file reads yields a higher impact on system resources than necessary in a high-performance application environment.
- On-demand and real-time scanning of all files gives optimum protection. However, this configuration has the overhead of scanning files that cannot support malicious code (for example, ASCII text files). Exclude files or directories of files, in all scanning modes, that you know present no risk to the system.
- Schedule regular disk scans only during low-usage times and at times when application activity is lowest.
- Disable the email scanner if the server does not use email.

  Also, set the AV software to block IRC ports and block port 25 to block any outgoing email.
- If your AV software has spyware detection and removal, then enable this feature. Clean infected files, or delete them (if these files cannot be cleaned).
- Enable logging in your AV application. Limit the log size to 2 MB.
- Set your AV software to scan compressed files.
- Set your AV software to not use more than 20% CPU utilization at any time.

  When a virus is found, the first action is to clean the file, the second to delete or quarantine the file.
- If it is available in your AV software, enable buffer overflow protection.
- Set your AV software to start on system startup.

Unified ICM/Unified CCE Maintenance Parameters

A few parameters control the application activity at specific times. Before you schedule AV software activity on Unified ICM/Unified CCE Servers, ensure that Antivirus software configuration settings do not schedule "Daily Scans," "Automatic DAT Updates," and "Automatic Product Upgrades" during critical times.

Logger Considerations

Do not schedule AV software activity to coincide with the time specified in the following Logger registry keys:

- 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

Distributor Considerations

Do not schedule AV software activity to coincide with the time specified in the following Distributor registry keys:

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

CallRouter and PG Considerations

On the CallRouter and Peripheral Gateway (PG), do not schedule AV program tasks:

- During times of heavy or peak call load.
- At the half hour and hour marks, because Unified ICM processes increase during those times.

Other Scheduled Tasks Considerations

You can find other scheduled Unified ICM process activities on Windows by inspecting the Scheduled Tasks Folder. Ensure that scheduled AV program activity does not conflict with those Unified ICM scheduled activities.

File Type Exclusion Considerations

Several binary files that are written to during the operation of Unified ICM processes have little risk of virus infection.

Omit files with the following file extensions from the drive and on-access scanning configuration of the AV program:

- *.hst applies to PG
- *.ems applies to ALL
- *.repl
- *.localrepl

Note If you are using Outbound High Availability replication, the **repl** directory, which is at `/icm/<cust>/la` or `lb/repl` should be excluded from antivirus scanning.

Note Exclude the *c:\icm* folder from all antivirus scans.