# Sample Administering Antivirus Software

# Windows Configuration

The table below describes the configuration for systems with the Windows anti-virus agent installed.

| **Step** | **Action** |
| --- | --- |
| 1 | The agent is configured to pull the latest virus definition from the management console once per day. |
| 2 | The management console is configured to download virus definitions from the vendor’s FTP site as follows:   * Daily – scheduled to download every 60 minutes per day |
| 3 | The server is configured to continuously poll the management console then pull down any new virus definitions. |

# Windows Maintenance

The continuous pull of definitions from the console to the server plus the hourly separate downloads per day of definitions from the vendor to the console ensures virus definitions are current.

Additionally, a manual process is followed during the NOC engineers’ to verify the virus definitions are truly current. The table below describes the manual process the engineer follows.

| **Step** | **Action** |
| --- | --- |
| 1 | Navigate to the vendor’s website to conclude the most recent definition date. |
| 2 | Compare the date to the most recent definition date in the anti-virus console. |
| 3 | Document the task as completed in the production schedule. |

# Exchange Installation

The anti-virus agent is installed and configured on the server prior to going into production.However, for the Exchange/SMTP systems, depending on the purpose for the Exchange/SMTP service, the agent may not be installed when there is no risk of virus introduction while that service is enabled. This determination is made during the build.

Note:

For some systems, the implemented email functionality imposes no risk of virus. For example, automatically generated, outbound email notifications would not impose a risk of virus because the email traffic is programmatically generated, therefore reducing the ability for a virus to be propagated. Outbound email is less likely to propagate a virus than inbound email. For these types of systems, the agent may not be installed when there is no risk of virus introduction while that service is enabled.

# Exchange Configuration

The table below describes the configuration for systems with the Exchange/SMTP anti-virus agent installed.

| **Step** | **Action** |
| --- | --- |
| 1 | The central manager is configured to pull the latest virus definitions twice per day from the vendor’s FTP site. |
| 2 | The agent is configured to pull the latest virus definition from the central manager once per day. |

# Associated Controls/Audit Mechanisms

The following table lists the controls and the audit mechanisms that are associated with this document.

| **Associated Control** | **Audit Mechanism** |
| --- | --- |
| Anti-virus software is configured to monitor virus activity on Windows-based systems in order to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the anti-virus software.  Exchange/SMTP anti-virus software is configured to monitor mail related traffic to detect and prevent the transmission of data or files via E-mail that contain certain virus signatures recognized by the anti-virus software. | Will review the logs for all virus events and will look for a corresponding SR for the details behind the event and the steps taken to resolve the issue. |
| Email anti-virus software is updated once per shift with current virus signatures. | For specified period, provide all production schedules to show anti-virus software was checked to confirm the systems were updated with current virus signatures. |
| Windows anti-virus software is updated with current virus signatures. | For specified period, provide all production schedules to show anti-virus software was checked to confirm the systems were updated with current virus signatures. |