Table of Contents

Preface ............................................................................................................................................................ 3

Product Description ...................................................................................................................................... 3

Prepare for Deployment ................................................................................................................................. 3

   Hardware/Software .................................................................................................................................... 3

   Performance Report .................................................................................................................................. 3

   Product Performance Improvement ....................................................................................................... 4

   PortalProtect 2.1 Configuration and Performance Impact ..................................................................... 4

Software ......................................................................................................................................................... 5

   Recommendations ...................................................................................................................................... 5

   System Requirements ............................................................................................................................. 5

   Database .................................................................................................................................................. 6

   Trend Micro Control Manager (TMCM) .................................................................................................. 7

Performance Tuning ....................................................................................................................................... 7

   PortalProtect Recommendations ........................................................................................................... 8

Installation ...................................................................................................................................................... 9

   Account Permission .................................................................................................................................... 9

   Installation Settings .................................................................................................................................... 9

   Fresh Installation ...................................................................................................................................... 10

   Upgrade .................................................................................................................................................... 11

   Post Installation ........................................................................................................................................ 12

Product Configuration .................................................................................................................................. 12

   GUI Configuration ..................................................................................................................................... 13
Preface

Welcome to Trend Micro PortalProtect for Microsoft SharePoint v2.1 Best Practices Guide. This document is designed to help customers develop a set of best practices when deploying and managing PortalProtect for Microsoft SharePoint. This document is also designed to be used only as a supplement to the Trend Micro PortalProtect for Microsoft SharePoint v2.1 Administrator’s Guide.

Product Description

Trend Micro™ PortalProtect™ for Microsoft™ SharePoint is an application designed to run on the existing Microsoft SharePoint Web Front End servers. Microsoft provides the VSAPI (Virus Application Programming Interface) to allow AV Vendors to scan contents uploading to or downloading from the SharePoint servers. Trend Micro PortalProtect is designed to use VSAPI, which is available for SharePoint 2007 and SharePoint 2010. Trend Micro PortalProtect will integrate tightly with both SharePoint 2007 and SharePoint 2010.

Once installed on SharePoint 2007 or 2010, PortalProtect for Microsoft SharePoint will protect the SharePoint Server against viruses, spyware, and other unwanted content. Additionally, it protects data from being leaked. PortalProtect for Microsoft SharePoint can also configure to scan all content stored in SharePoint content databases.

Prepare for Deployment

Hardware/Software

Since PortalProtect for Microsoft SharePoint is designed to run on the existing Microsoft SharePoint 2007/2010 servers, you should follow Microsoft’s recommendations for system requirements for SharePoint Servers. The following links contain information that can be used as a reference to deploy your SharePoint environments.

SharePoint Server 2007:

Windows SharePoint Services 3.0:

SharePoint Server 2010:

SharePoint Foundation 2010:

You can use the HP Sizing Tool below for additional resources:

Microsoft SharePoint Server 2007 at
http://g3w1656g-vip.houston.hp.com/SB/Installs/MOSS2007.zip

Microsoft SharePoint Server 2010 at
http://g3w1656g-vip.houston.hp.com/SB/Installs/SharePoint2010Sizer.zip

PortalProtect will have the least impact on your environment if you implement the information contained in the previously mentioned links to sizing articles and follow the recommendations in this document.

Performance Report

Note: This information should be used as a starting reference only. Actual performance will vary depending on features enabled, topology, hardware and software.
Trend Micro conducted a series of tests using an isolated network environment to measure the performance of PortalProtect 2.1 for Microsoft SharePoint. The objective of these tests was to obtain data about the performance of Trend Micro PortalProtect 2.1 for Microsoft SharePoint. These tests predominately focused on evaluating real-time and manual scanning options, its throughput and scanning performance.

## Product Performance Improvement

This testing compared the SharePoint 2010 baseline with PortalProtect 2.1 and FSSP 2010 running in a real-time anti-malware scans on a Web Front End server. The performance impact of these tests is illustrated in Table 1.

### Table 1. Real-time Anti-malware Scanning Results

<table>
<thead>
<tr>
<th>Baseline (SharePoint 2010 Only)</th>
<th>PortalProtect 2.1 Anti-Malware</th>
<th>FSSP 2010 Anti-Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor Utilization (%)</td>
<td>71.2%</td>
<td>73.3%</td>
</tr>
<tr>
<td>Throughput (Requests/s)</td>
<td>140</td>
<td>113</td>
</tr>
<tr>
<td>Throughput Difference (%)</td>
<td>19.2%</td>
<td>38.1%</td>
</tr>
</tbody>
</table>

**Observations:**

- Under similar CPU use circumstances, PortalProtect 2.1 with real-time anti-malware scanning reduced throughput performance by 19.2% compared to the baseline (SharePoint 2010 without anti-malware software installed).
- While this is measurable impact to throughput, it is much less than the impact of comparable anti-malware scanning by alternative products. FSSP 2010 real-time anti-malware scanning—using default settings with available engines—reduces performance by 38.6% compared to the baseline.

## PortalProtect 2.1 Configuration and Performance Impact

Different customers use different features based on their size, industry, overall security architecture, and even appetite for risk. Accordingly, we compare the most common filtering configurations of PortalProtect 2.1 with the baseline (SharePoint 2010 only) under similar situations. Table 2 shows the throughput and the processor utilization during the tests.

### Table 2. Impact of Different PortalProtect Real-Time Filters

<table>
<thead>
<tr>
<th>Baseline (SharePoint 2010 Only)</th>
<th>PortalProtect 2.1 Anti-Malware</th>
<th>PortalProtect 2.1 Anti-Malware+ Content Filtering</th>
<th>PortalProtect 2.1 All Filters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor Utilization (%)</td>
<td>71.2%</td>
<td>73.3%</td>
<td>70%</td>
</tr>
<tr>
<td>Throughput (Requests/s)</td>
<td>140</td>
<td>113</td>
<td>86.6</td>
</tr>
<tr>
<td>Throughput Difference (%)</td>
<td>19.2%</td>
<td>38.1%</td>
<td>45.9%</td>
</tr>
</tbody>
</table>

For complete performance results, please request the “Performance and Sizing Guide” from your TAM.
Software

This section discusses the best practices for using PortalProtect. It includes system requirements and operating recommendations to ensure the best performance and security.

Recommendations

System Requirements

<table>
<thead>
<tr>
<th>Hardware/Software</th>
<th>Requirement</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Server with processor speed of 2.5-GHz (32-bit or 64-bit)</td>
<td>Dual processor, 3-GHz or greater (32-bit or 64-bit)</td>
</tr>
<tr>
<td>Memory</td>
<td>2-GB RAM</td>
<td>4-GB RAM</td>
</tr>
<tr>
<td>Disk Space</td>
<td>2-GB free disk space</td>
<td>5-GB free disk space</td>
</tr>
</tbody>
</table>

Windows Server

- Windows Server 2003, Standard Edition X86/X64
- Windows Server 2003, Enterprise Edition X86/X64
- Windows Server 2003 R2, Standard Edition X86/X64
- Windows Server 2003 R2, Enterprise Edition X86/X64
- Windows Server 2008 Standard Edition X86/X64
- Windows Server 2008 Enterprise Edition X86/X64
- Windows Server 2008 R2 Enterprise Edition X64
- Windows Server 2008 R2 Standard Edition X64
- Microsoft Windows Server 2008 Datacenter X64
- Microsoft Windows Web Server 2008 X64
- Microsoft Windows Server 2008 HPC X64

SharePoint Service / Server

- Windows SharePoint Service 3.0 X86/X64
- Microsoft Office SharePoint Server 2007 Standard /Enterprise X32/X64
- Windows SharePoint Service 4.0 X64
- Microsoft Office SharePoint Server 2010 Standard /Enterprise X64

Web Server

- Microsoft Internet Information Services (IIS) 6.0
- Microsoft Internet Information Services (IIS) 7.0

Browser

- Microsoft Internet Explorer 6.0 or above
- Mozilla Firefox 3.0 or above
Database

Introduction

PortalProtect creates the following databases:

<table>
<thead>
<tr>
<th>Database</th>
<th>Used</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPCentralConfig</td>
<td>Central configuration</td>
<td>There will be only one central configuration database in the farm.</td>
</tr>
<tr>
<td></td>
<td>Central quarantine information</td>
<td></td>
</tr>
<tr>
<td>PPConf</td>
<td>Configuration for each PortalProtect in the farm</td>
<td>Each PortalProtect contains three databases in the farm.</td>
</tr>
<tr>
<td>PPLog</td>
<td>Log for each PortalProtect in the farm</td>
<td></td>
</tr>
<tr>
<td>PPREport</td>
<td>Report for each PortalProtect in the farm</td>
<td></td>
</tr>
</tbody>
</table>

PortalProtect 2.1 will not help to install SQL server, but provide supports using SharePoint or user-defined SQL server to create PortalProtect databases. These databases are located on the SQL server under:
- `<Program Files>\Microsoft SQL Server\MSSQL*.\MSSQL\Data`

The file names begin with:
- `PPConf_[ServerName], PPLog_[ServerName], PPREport_[ServerName], PPCentralConfig_[SharePoint_Config_DB_Name]`

Log and quarantine database maintenance runs at 2:30 AM every day by default. The administrator can change this time by adding the following registry key:
- `HKLM\SoftWare\TrendMicro\PortalProtect\CurrentVersion\StorageMaintenanceStartTime (REG_DWORD)`

You can change the time if the maintenance window conflicts with your existing maintenance window. It is recommended that you keep the default maintenance value of 30 days. All data older than 30 days will be deleted according to the previously mentioned maintenance times.

For report maintenance, the default report maintenance value is 180 days. This value may be changed using the registry key:
- `HKLM\SoftWare\TrendMicro\PortalProtect\CurrentVersion\ReportDataKeepDays (REG_DWORD)`

If you plan to setup a remote SQL server for your PortalProtect installation, make sure the SQL server is configured for high availability. If the remote SQL server is down, PortalProtect will not work. If you are using the remote SQL server, be sure to monitor the application event log for any logs related to the connections to the SQL server. By default, if the database is not available, PortalProtect will log an error in the application event log and stop main service. To ensure that PortalProtect is working as expected, a remote SQL server/connection must be operational. After that, PortalProtect will recover automatically.

**Note:** PortalProtect does not support SQL mirroring currently. Database Mirroring is not transparent to the application. Application needs to do some extra work to connect to a mirror database. This scenario was not considered in the current product development.

Privilege

PortalProtect must have access to the following SQL Server database sources:
- PortalProtect Configuration Database
- SharePoint Databases

To access these databases, PortalProtect requires the following database access accounts:
• PortalProtect Configuration Database Access Account
• SharePoint Database Access Account

These database access accounts must support either Windows Authentication or SQL Server Authentication. It is highly recommended that you use Windows Authentication. Windows Authentication provides a more stable environment and does not require you to save your password in any form. Besides authentication, these access accounts also require database permissions.

• PortalProtect will fetch or modify data in the SharePoint database. You need specify a database access account with relevant permissions. The following is a list of the required database permissions:
  - SharePoint Configuration Database: access account must have at least database role `db_datareader` and `WSS_Content_Application_Pools`
  - SharePoint Content Database: access account must have a database role of `db_owner`

• If you are using user-defined SQL server, it’s recommended to create a new account with `DBcreator` role in the instance where you want to install PortalProtect. See Figure 1.

![Figure 1. Login Properties - sqltest](image)

**Trend Micro Control Manager (TMCM)**

If you use Trend Micro Control Manager (TMCM) to manage your PortalProtect 2.1 servers, make sure the following minimum builds:

- Control Manager 5.0 GM (Build: 1467) + Patch7+ hotfix 2092
- Control Manager 5.5 GM (Build: 1250) + Service pack1

The above are the minimum builds but we recommended that you use the latest patch/hot fixes available for Control Manager.

**Note:** The Data Protection log and Data Protection report are available only with Control Manager 5.5 service pack 1. Other versions of Control Manager include the Content Filtering log and report, which contain Data Protection logs.

**Performance Tuning**

PortalProtect integrates tightly with Microsoft SharePoint. For PortalProtect to perform optimally, it is recommended that you follow and implement the recommendations from Microsoft’s Best Practice Analyzer Tool. Trend Micro worked closely with Microsoft to include the recommended settings for SharePoint in this tool. Make sure all the settings for both SharePoint and PortalProtect are implemented to allow both products to perform optimally.
PortalProtect Recommendations

1. The following files and directories should be excluded from the file-based anti-virus scanner running in the SharePoint servers:
   - Backup folder (Default folder: \PortalProtect\storage\backup)
   - Temp folder (Default folder: \PortalProtect\Temp)
   - SharedResPool folder (Default folder: \PortalProtect\SharedResPool)

2. Move the following directories to the fastest drive available:
   - SharedResPool directory may be customized with the following registry key:
     HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PortalProtect\CurrentVersion\SharedResPool
   - TempDir directory may be customized with the following registry key:
     HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PortalProtect\CurrentVersion\TempDir
     If the key does not exist, PortalProtect will use the default \PortalProtect\temp directory.

3. If you enable global smart scan for Web Reputation, PortalProtect 2.1 default rating server is tmpp20-en.url.trendmicro.com. Make sure your firewall/proxy allows connection to tmpp20-en.url.trendmicro.com. Otherwise, there will be a delay while PortalProtect connects to the rating server to check URL scores. By default, if unable to connect to the rating server, timeout will occur in ten-seconds for both connect and query. You can decrease the timeout by creating the following:
   - Path: HKLM\SOFTWARE\TrendMicro\PortalProtect\CurrentVersion
   - Key: TmufeConnectTimeout
   - Type: REG_DWORD
   - Data value: 10 (default)

   - Path: HKLM\SOFTWARE\TrendMicro\PortalProtect\CurrentVersion
   - Key: TmufeRSQueryTimeout
   - Type: REG_DWORD
   - Data value: 10 (default)

   If you enable local smart scan for Web Reputation, make sure that you are connected to the local smart scan server. Otherwise, there will be a delay while PortalProtect connects to the rating server to check the score for URLs.

4. Make sure all debug logging parameters are disabled unless working with Trend Micro support engineers to troubleshoot an issue. Check the management console under Administration > Trend Support/Debugger to see whether debugging is enabled on any of the modules. Continual debugging may affect performance.

5. Scheduled/Manual Scanning. It is not recommended to invoke manual or scheduled scanning during business hours. Invoking manual or scheduled scanning will consume significant resources in your SharePoint environment. Manual scanning should only be invoked during business hours if there is a suspected virus outbreak. Otherwise, schedule all scans during off-hours or weekends. When scheduling a scan, it is recommended that you do not pick all the SharePoint sites at once. Instead, try to schedule each task separately.

   Do not schedule multiple scheduled scans too closely together. Multiple scheduled scans that occur at the same time will be queued and only start once the previous scan task is complete.

   Manual and scheduled scans may use different settings than those of real-time scans. If you invoke manual/schedule scans, be sure to verify the settings to make sure that they are as you wanted. To speed up scheduled scanning, only select the scanning type you want to run. Enabling all scanning types will take longer to process and is not necessary.

   When configuring the manual/scheduled scan, consider using incremental scanning:
Configure incremental scanning to scan only the new content that appears since your last scheduled/manual scan.

6. Configure one PortalProtect server to download all the components from ActiveUpdate, and then set the other PortalProtect servers within the same location to get updates from the primary PortalProtect resource server. This provides a much faster deployment and saves Internet bandwidth. To enable this option for other PortalProtect servers, do the following:

- Ensure either “Trend Micro’s ActiveUpdate Server” or “Other Update Source” is selected and also select “Allow other servers to download updates from this server”.
- Invoke the manual/schedule update as usual so that the source PortalProtect server can pull down all update components.
- Configure the other PortalProtect servers to use:
  `http://[ServerName:16372]/PortalProtect/Activeupdate`

7. Use Control Manager to push out the updates. If you have Control Manager, configure it to push out updates to the PortalProtect servers. However, you should have multiple sources of update in case the TMCM update fails to deploy. Accomplish this by using the Trend Micro ActiveUpdate server, Intranet or Other Update Source option.

## Installation

It is recommended to install PortalProtect on servers that are running the Web application servers (services), also called the Web front-end servers.

### Account Permission

- It is recommended that if SharePoint is deployed without AD, which is not typical, that the account be set to local administrator.
- It is recommended that if SharePoint deployed with AD, that the account be local admin + domain user.

## Installation Settings

<table>
<thead>
<tr>
<th>Item Checklist</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Installation</td>
<td>NetBIOS (445, 137,138,139) with File and Printer Sharing for Microsoft Networks Enabled</td>
</tr>
<tr>
<td>Ports</td>
<td>16372 for HTTP and 16373 for HTTPS</td>
</tr>
<tr>
<td>IIS</td>
<td>CGI role service is added</td>
</tr>
<tr>
<td>SSL</td>
<td>Enabled</td>
</tr>
<tr>
<td>Other</td>
<td>System partition of the target host is administratively shared (C$)</td>
</tr>
</tbody>
</table>
Fresh Installation

The following is a list of the main points to consider when installing PortalProtect 2.1:

- Make sure that you have reviewed the previous sections and have all the recommended/requirements.
- You do not need to manually stop any SharePoint/Windows services. PortalProtect does not need to stop/start any SharePoint/Windows services during a fresh installation. However, ensure your server is working normally before installing PortalProtect.
- Select an action to install PortalProtect according to your actual environment. During installation, you will be presented with the dialog shown in Figure 3:

![Figure 3. Installation Select an Action](image)

- Select an SQL server to store PortalProtect configuration and related data. During installation, you will be presented with the dialog shown in Figure 4. It is recommended that you select an SQL server with high availability, because PortalProtect will stop working and notify the administrator if its database cannot be accessed. The user must have the required privileges needed to access the SQL server.
- It is not recommended to use the same PortalProtect configuration database instance when installing PortalProtect to different SharePoint farms. It is strongly recommended that each SharePoint farm use its own PortalProtect configuration database instance.

![Figure 4. Specify PortalProtect Configuration Database](image)

- Select an authentication method to access the SharePoint configuration database if you installed PortalProtect on a SharePoint farm environment. During installation, you will be presented with the dialog shown in Figure 5. It is highly recommended that you specify the same authentication method as the one used to deploy SharePoint.
It is recommended you create an AD group for PortalProtect to enable users to log on the PortalProtect Web management console. During installation, you will be presented with the dialog shown in Figure 6.

It is recommended that you stipulate proxy settings if you need a proxy to connect to the TrendMicro ActiveUpdate server.

It is also recommended that you select “Update the pattern when installation is complete” to apply the latest antivirus patterns to protect your SharePoint.

### Upgrade

The following is a list of the main points you should know when upgrading to PortalProtect 2.1:

- PortalProtect 2.1 supports upgrade from PortalProtect 2.0 using the GM build or any patch/hotfix builds.
- For PortalProtect 1.7 or PortalProtect 1.8, it is recommended that you uninstall the previous version and install PortalProtect 2.1.
- Before upgrading, check the size of your log database. If the log database is very large, it is recommended that you run maintenance using your current version before you upgrade. This will greatly reduce the amount of time required for upgrade.
• Before upgrading, check your quarantined files. If there are several quarantined files, it is recommended that you delete or restore quarantined files during off-hours. This will greatly improve the upgrading performance.

• Before upgrading, record the SQL server information that contains the PortalProtect configuration database, log database, report database, and central configuration database. You can get the information from the following registry key:
  - Path: HKLM\SOFTWARE\TrendMicro\PortalProtect\CurrentVersion
  - Key: PPConfDatabaseInstance
  - Type: REG_SZ

  - Path: HKLM\SOFTWARE\TrendMicro\PortalProtect\CurrentVersion
  - Key: PPConfDatabaseAuthentication
  - Type: REG_SZ

Note: This SQL information will need to be used to upgrade PortalProtect 2.0.

• It is recommended that you use a new activation code (AC) that supports the Data Protection function.

Note: Before performing this installation, be sure to read the PortalProtect 2.1 Installation Guide completely as it contains detailed information. You can request a copy of this guide from your TAM.

Post Installation

After installing PortalProtect, configure the antivirus settings in the SharePoint Central Administration and Web content scan settings from the PortalProtect management console. This will enable PortalProtect to protect your SharePoint environment. Make sure the Windows SharePoint Services Administration service is running, which regularly checks for PortalProtect status updates for virus scanning and virus signature.

Product Configuration

You can change the PortalProtect configuration via the GUI. Any changes made in the GUI are stored in the database. It is not recommended that you change the settings directly via the database or .ini file unless instructed by a support professional handling your case. You should always use the GUI to make changes to PortalProtect. Some settings are required to add/edit/modify the registry to take effect.

This section provides recommendations and important notes on key settings that will help you understand and make necessary configuration changes based on your security requirements. Additional information is also included for some items to assist you in configuring PortalProtect according to best practices. The following information is presented in the same order as it appears in the management console:
GUI Configuration

<table>
<thead>
<tr>
<th>Summary</th>
<th>Notes and Recommendations</th>
</tr>
</thead>
</table>
| **System**  
  **Scan Services** | It is highly recommended that you enable “Scan documents on upload”, and “Attempt to clean infected documents” to scan new documents.
You can enable “Scan documents on download” after the fresh installation to scan old documents in the current environment. However, after PortalProtect manually scans all content in your environment, it is suggested that you disable this option.
It is recommended that you configure **Scan Web content** to run during off-hours. The time it takes effect will depend on the number of lists in the current farm as it needs to go through all lists.
After you enable **Scan Web Content**, PortalProtect will periodically check newly created lists and add Web content; the default duration is 12 hours.
If you want to change the duration, you can add the following registry key:
• Path: HKLM\SOFTWARE\TrendMicro\PortalProtect\CurrentVersion
• Key: WCHookDeployIntervalInMinutes
• Type: REG_DWORD
• Data value: 720 (default)

  **Note:** The minimum value is one (1) minute; the maximum value is 30-days

It is highly recommended that you not set the duration to a value less than the default value.

<table>
<thead>
<tr>
<th>Security Risk Scan</th>
<th>Notes and Recommendations</th>
</tr>
</thead>
</table>
| **Security Risk Scan**  
  **Enable real-time security risk scan** | It is highly recommended you enable this option to protect documents from security risks.
| **Default Scanning**  
  **All scannable files** | This is the most secure setting since all files will be scanned including .txt files. It is recommended that you enable this feature if security is preferred over performance
| **Intelliscan: uses “true file type” identification** | This setting is recommended if you would like to improve system performance. With this option enabled, PortalProtect will analyze the file header using “true file type” to determine if the file is able to carry viruses. If it is a text file (which do not carry viruses), PortalProtect will simply skip them. However if an .exe file was renamed to a .txt extension, PortalProtect will be able to detect any infection because of this true-file-type analysis feature.
| **Specified file type** | This option is typically not recommended and must be used with extreme caution and a good understanding of your environment. It is not the best choice since you might leave other files types out that can potentially carry the viruses. It is recommended to use either the All scannable files or Intelliscan option unless you know for sure what you want to scan in your environment.
| **IntelliTrap**  
  **Enable IntelliTrap** | IntelliTrap detects potentially malicious code in real-time compressed executable files.
| **Spyware/Grayware Scan**  
  **Spyware** | Spyware is computer software that collects personal information about users without their consent. It is recommended to filter these malware
<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Adware</strong></td>
<td>Adware is any software application in which advertising is displayed while the program is running. The authors of these applications include additional code that delivers the ads, which can be viewed through pop-up windows or through a bar that appears on a computer screen and sometimes through text links or in integrated search results. Adware may or may not track personal information. It may also gather information anonymously or in aggregate only. Users should check the EULA and Privacy policy to ensure if the adware on their machines conforms to their standards.</td>
</tr>
<tr>
<td><strong>Dialers</strong></td>
<td>A program that can secretly change your dialup connection setting so that instead of calling your local Internet provider, your PC calls are routed to an expensive 0900 or international phone number. It is recommended to filter these programs.</td>
</tr>
<tr>
<td><strong>Joke Programs</strong></td>
<td>A computer prank is a prank related to either the software or the hardware of computers. Some are intended to humiliate, while others are comical, but not humiliating. Some pranks are &quot;screamers,&quot; which are described by their name. Others involve loss of control of the computer software.</td>
</tr>
<tr>
<td><strong>Hacking Tools</strong></td>
<td>Hacker tools are programs written to access a computer system using known software vulnerability. Most of these programs have been written and are freely distributed from &quot;Hacker&quot; websites. Some of these programs were written for legitimate uses and are abused as a hacking tool. It is recommended to filter these programs.</td>
</tr>
<tr>
<td><strong>Remote Access Tools</strong></td>
<td>A tool that is intended to be used by network administrators to remotely control a PC on the network, usually for support or inventory purposes. Due to the nature of the program, the possibility exists to be exploited for spying purposes</td>
</tr>
<tr>
<td><strong>Password Cracking Applications</strong></td>
<td>Software designed to allow users to decrypt or recover lost or unknown passwords. In the hands of security administrators these may be legitimate tools; however password crackers can be a security and privacy threat when used maliciously by unauthorized users.</td>
</tr>
<tr>
<td><strong>Other</strong></td>
<td>Spyware applications that are in this category usually fit multiple categories and are grouped into a miscellaneous category</td>
</tr>
</tbody>
</table>

**Note:** The Spyware/Grayware Scan is divided into the previously mentioned eight sub-categories. If you enable any of these additional threats, the action taken is found under "Spyware/Grayware Scan". This Spyware/Grayware Scan is available for use and can be enabled according to your security needs.

<table>
<thead>
<tr>
<th>Advanced Options (Scan Restriction Criteria)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File Size exceeds</strong></td>
<td>The default value is 30MB. You can decrease the value based on your security needs.</td>
</tr>
<tr>
<td><strong>Decompressed file count exceeds</strong></td>
<td>The default value is 9999. You can decrease / increase the value based on your security needs. When the amount of decompressed files within the compressed file exceeds this number, then PortalProtect only scans files up to the limit set by this option.</td>
</tr>
<tr>
<td><strong>Size of decompressed file exceeds</strong></td>
<td>The default value is 100MB. You can decrease / increase the value based on your security needs. PortalProtect only scans compressed files that are smaller or equal to this size after decompression.</td>
</tr>
<tr>
<td><strong>Number of layers of compression exceeds</strong></td>
<td>The default value is five (5). You should not change this default value. Increasing this value will slow the processing time to extract each layer and scan it. PortalProtect only scans compressed files that have less than or equal to the specified layers of compression. For example, if you set the limit to five (5) layers of compression, then PortalProtect will scan the first five (5) layers of compressed files, but not scan files compressed to six (6) or more layers.</td>
</tr>
<tr>
<td><strong>Size of decompressed file is &quot;x&quot; times the size of compressed file</strong></td>
<td>The default value is 1000. PortalProtect only scans compressed files when the ratio of the size of the decompressed file compared to the size of the compressed file is less than or equal to this number.</td>
</tr>
</tbody>
</table>
Note: PortalProtect will not scan/process any content matching the previously listed restrictions. PortalProtect will take the action specified under Action > Unscannable Files > Files exceeding specified scanning restrictions. It is not recommended to set these values too large since it may degrade performance.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customized action for detected threats</td>
<td>You can customize actions if the pre-defined options in ActiveAction do not meet requirements. You can also choose whether or not to send notifications for each of the threat. It is recommended that you enable notifications for virus events so that you can take action / investigate when there are many viruses detected within a short period of time.</td>
</tr>
<tr>
<td>Backup infected file before performing action</td>
<td>Enabling this function will use more disk space for storage as it leaves a copy of the infected files on your system. This is generally not recommended except on specific environments with high requirements on preserving data. Also, make sure that the file based antivirus application running in the SharePoint server is configured to exclude the backup directory of PortalProtect as stated in the best practice section.</td>
</tr>
<tr>
<td>Do not clean infected compressed files to optimize performance</td>
<td>By default, this option is enabled to improve performance. Only disable this option if company policy requires it. Disabling this option will use more CPU resources as the compressed files need to be extracted, scanned, cleaned, and eventually recompressed.</td>
</tr>
</tbody>
</table>

### Advanced Options

#### Macros
- Enable advanced macro scan
- Delete all macros detected by advanced macro scan

#### Unscannable Files
- Encrypted or password protected files
- Files exceeding specified scanning restrictions

### Backup Settings

- Backup directory

### Notification

- Notify administrator
- SMTP notification contains the following three settings:
  1. Send consolidated notification every X hours - This option is recommended so that you will not get too many notifications. This option consolidates all the notifications into one email and sends it every x-number of hours as defined.
  2. Send consolidated notification every X occurrences - This option will consolidate all the notification into one email and send the notification if x-number of occurrences are met.
  3. Send individual notifications - If you enable this option, PortalProtect will send individual notifications per event. Options one (1) and two (2) are recommended for most installations.

### Advanced notification

Besides SMTP notification, you also can configure to send notification to SNMP tool or Windows event log.
### Policy Management

<table>
<thead>
<tr>
<th>Notes and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note: PortalProtect 2.1 contains policies for some scanning filters which include file blocking on SharePoint 2010, content filtering on SharePoint 2010, and data protection on SharePoint 2010.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Global Approved List</th>
<th>AD users or AD groups in this list will be used as a white list for this scanning filter. If you want to skip scanning content posted by some users, you can add their accounts or groups in this list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: Specify Rules (Target)</td>
<td>Different filters will have different options, which will be covered later in this best practice.</td>
</tr>
<tr>
<td>Step 2: Exceptions Site exceptions Accounts exceptions</td>
<td>This exception will be used as white list for this policy. This policy will skip scanning content posted to the site (site exceptions) by the account (account exceptions). You can add AD users, AD groups, SharePoint users, SharePoint groups to this account exceptions list. One policy can contain more than one exception.</td>
</tr>
<tr>
<td>Step 3: Specify Action</td>
<td>You can decide which action will be taken for this policy. The available actions for real-time scan include: Block, Pass.</td>
</tr>
<tr>
<td>Step 4: Specify Notification</td>
<td>You can set notification for this policy; some detailed information can refer to notification for Security Risk Scan.</td>
</tr>
</tbody>
</table>

**Add**
- If you want to add a new rule, click “Add” and then follow the directions as displayed by the wizard.

**Delete**
- If you want to delete a rule, select the checkbox next to it and click “Delete.” Consider disabling a rule instead of deleting so you can later reuse them.

**Reorder**
- If you want to reorder specific rules, select them and click “Reorder”. Type the numbers for the new order in the dialog box. It is recommended that you move the rules that are of higher priority to the top using “Reorder”.

**Enable/Disable**
- Rules must be enabled to take effect. A check icon 🗝️ indicates that the rule is enabled. An X icon ✗ indicates it is disabled.

### File Blocking

<table>
<thead>
<tr>
<th>Notes and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable real-time file blocking</td>
</tr>
<tr>
<td>Target</td>
</tr>
<tr>
<td>Specific files File types</td>
</tr>
<tr>
<td>Block file types or names within compressed files</td>
</tr>
<tr>
<td>Action</td>
</tr>
</tbody>
</table>

### Content Filtering

<table>
<thead>
<tr>
<th>Notes and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable real-time content filtering for document</td>
</tr>
<tr>
<td>Enable real-time content filtering for Web content</td>
</tr>
</tbody>
</table>
### Policy/Target

**Match "Any specified keyword" / Match "All keyword"**

Match any specified keyword is recommended, which will take action if any keyword defined in this rule is matched; "Match all keywords" means action is taken when all keywords defined in this rule is matched.

**Keyword**

Keywords support operators, wildcard, and regular expressions:
1. Wildcard support only "*". "?" does not support.
2. By default, keywords are exact match. Users must input .REG. for regular expressions.

When creating the content filtering rules, make sure that they do exactly what you need. You can use regular expressions to accomplish this with fewer keywords as possible. Creating plenty of complex rules may degrade the performance of PortalProtect so keep them at a minimum as possible.

### Data Protection

<table>
<thead>
<tr>
<th>Notes and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable real-time data protection for document</td>
</tr>
<tr>
<td>Enable real-time data protection for Web content</td>
</tr>
</tbody>
</table>

### Target

**Compliance Rule**

Available compliance templates can be added into the compliance rule, which will take action if any selected templates defined in this rule are matched.

**Compliance Templates**

PortalProtect provides several default compliance templates, which include GLBA, HIPPA, PCI-DSS, SB-1386, US PII. These templates cannot be modified.

**Add**

If you want to add a new template, click "Add" and select expressions or keywords for your template. The suggested setting is "Occurrences" for expressions if you want to take action when the expression is matched several times.

**Import/Export**

Compliance templates can be exported or you can import compliance templates.

### Web Reputation

**Notes and Recommendations**

Enable real-time Web Reputation for documents Make sure that this option is selected and saved if you intend to use Web Reputation to rate the URL in posted documents by querying the Trend backend database or query the local smart scan server.

Enable real-time Web Reputation for Web content Make sure that this option is checked and saved if you intend to Leverage the Web Reputation to rate the URL in posted Web by query Trend backend database or query local smart scan server.

**Note:** Make sure PortalProtect can connect to the Trend Global Smart Protection Network if using Global Smart Protection Network; or connect to local smart scan server if using local Smart Protection Server.

### Target

A maximum of 1024 URLs can be included in the approved URLs list. Before including the URLs, you can use: http://reclassify.wrs.trendmicro.com to check the URL reputation ranking/score. You may enter the domain as yahoo.com, google.com and the entire Web site will be included, including subfolders and pages.

(Example: www.google.com/intl/zh-TW/about.html...)

**Action**

Take action on URLs that have not been assessed by Trend Micro

PortalProtect may encounter newly created URLs that have not been assessed by Trend Micro. If this option is enabled, PortalProtect will take action for these un-assessed URLs. It is not recommended to enable it if your action is "Block".
### Manual Scan

#### Database selection
- **All databases/ Specific databases**

If PortalProtect is freshly installed, it is recommended you scan all databases during the weekend or scan specific databases one by one during off-hours.

If PortalProtect is deployed in a farm that has several Web Front End servers, it is recommended to do manual/scheduled scans on only one server.

**Note:** Take note that a manual scan will require significant server resources. For this reason, make sure you understand the settings and target databases. It is highly recommended to run manual scans outside of regular business hours unless absolutely necessary.

#### Incremental Scan Options

To avoid scanning all content, it is recommended that the "Incremental Scan Options" be used only to scan content that has not been scanned or content that falls within the changed dates. Try to configure incremental scanning to scan only content since the last scheduled/manual scan occurred.

### Scheduled Scan

#### Add Scan Task
- **Schedule Daily**

It is not recommended to enable daily especially for environments with large content stored.

- **Weekly, every**

Weekly is recommended for scheduled scan task during office off-hours. It is also a good practice to perform a scan before backup to make sure all archived content is scanned with the latest virus definition files.

- **Monthly, on date**

You can also schedule a monthly scan by selecting this option.

#### Database selection
- **All databases/ Specific databases**

It is recommended that you schedule multiple schedule scans for each of your databases instead of doing one scheduled scan for all your databases. Depending on the size of each of your databases, you can schedule them 1-2 hours apart. If you have multiple scheduled scans configured, your scheduled scan will queue until the previous scheduled scan is finished.

**Note:** Keep in mind that the individual databases you pick for scheduled scan will not be replicated using either Server Management or CM Replication. This is normal behavior since the databases are different from servers to servers across one farm. However, the following registry key was created to replicate scheduled tasks via control manager replication:

- **Path:** HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PortalProtect\CurrentVersion
- **Key:** MoreCfgReplicationList
- **Type:** REG_SZ
- **Value:** SMEX_SUB_CFG_SS:TM_ScheduledScan

User can still change database settings by modifying the replicated scheduled task.

### Smart Protection

#### Scan Service Settings
- **Security Risk Scan**
- **Conventional Scan**

If local Smart Protection Server is not available in your environment, conventional scan is recommended for security risk scan which will use anti-malware and anti-spyware components stored locally. It is recommended updating these components timely using scheduled update.

**Smart Scan**

Smart scan is recommended for security risk scan if you want to get prompt security protection, because smart scan will use the local smart protection server to do security risk scan.
### Web Reputation

**Smart Protection Network**
Global smart protection network requires an Internet connection to query URL reputation from this infrastructure.

**Smart Protection Server**
Local smart protection server is recommended if content privacy is your main consideration. This will query URL reputation from this local infrastructure.

**Do not make external queries to Smart Protection Network**
If privacy is your main consideration, it is recommended you use the default setting.

**Local Sources Server List Priority**
It is recommended you set high priority to the local scan server with high performance and high stability.

**File Reputation Service**
The status of the file reputation service which is used for security risk scan.

**Web Reputation Service**
The status of the Web reputation service which is used for Web reputation scan.

**Console**
You can enable or disable the reputation service via the smart scan server console.

**Query order**
It is recommended you select “Order” to send requests to the local server with the highest priority. If you select “Random”, the request will send to a randomly selected local server.

**Add/Delete**
You can add or delete smart scan servers to PortalProtect. For file reputation service, you can select SSL connection; for Web reputation service, the default port is 5274.

**Import/Export**
You can export/import a server list from other machines.

**Note:** It is recommended you monitor the performance of Smart Scan server, and add extra servers if the performance is not acceptable.

### Updates

**Notes and Recommendations**

<table>
<thead>
<tr>
<th>Scheduled Update</th>
<th>It is recommended you enable this option to ensure components are updated in a timely manner.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Components to Update</td>
<td>It is strongly recommended that you select all the components for new updates.</td>
</tr>
<tr>
<td>Update Schedule</td>
<td>Hourly is the recommended option to choose for scheduled update.</td>
</tr>
<tr>
<td>Download Source</td>
<td>By default, this option should be enabled if you are getting updates directly from Trend Micro’s ActiveUpdate Server via the Internet.</td>
</tr>
<tr>
<td>Trend Micro ActiveUpdate server</td>
<td></td>
</tr>
</tbody>
</table>
Intranet location containing a copy of the current file

If you have multiple PortalProtect servers and you would like to conserve some bandwidth, you can setup one of your PortalProtect servers to pull the updates from Trend Micro’s ActiveUpdate server or TMCM with the option “Allow other servers to download updates from this server” and then configure the other PortalProtect servers to use the UNC path of this PortalProtect server along with the User name and Password.

Do the following to make this Intranet option work for the other PortalProtect servers:

1. Select either “Trend Micro’s ActiveUpdate Server” or “Other Update Source”. Also, ensure you have selected “Allow other servers to download updates from this server”.
2. Invoke the manual/scheduled update as usual so that this PortalProtect server can pull down all the components necessary for other PortalProtect servers to update.
3. Once all the components are downloaded successfully, go to the following directory:
   \Program Files\Trend Micro\PortalProtect\web\activeupdate
   and share the ActiveUpdate folder.
4. Test from another PortalProtect server to ensure you can access this share by going to:
   Start > Run and type \\[servername]
   If the ActiveUpdate folder appears, then you were successful.
5. Configure the other PortalProtect servers to use \\
   Specify the username and password if needed and save the changes.

Other update source

This option may be used in the following three ways:

1. Using the PortalProtect URL from one of the PortalProtect server that has the “Allow other servers to download updates from this server” enabled. Then on the PortalProtect servers, specify the URL of the source PortalProtect server like:
   http://[source-PortalProtect-servername]:16372/PortalProtect/ActiveUpdate
2. Specify the URL of the TMCM (if you have Control Manager) like:
   http://[tmcm-servername]:80/TVCSDownload/ActiveUpdate
3. If you are given another URL to the update.

Allow other servers to download updates from this server

This option must be enabled if you are planning to make the target server an update source for other PortalProtect installations.

Alerts

### System Events

**PortalProtect Services**

It is recommended that you enable some of these alerts to help you take a proactive approach in maintaining PortalProtect.

**PortalProtect service did not start successfully**

This alert is recommended to be enabled. An email notification with write to application event log is also recommended. Click this setting to define the notification options. If PortalProtect service is unable to start successfully, then your SharePoint server is not protected. This alert will help you monitor your SharePoint environment.

**PortalProtect service is unavailable**

This alert is recommended to be enabled. An email notification with write to application event log is also recommended. Click this setting to define the notification options. If PortalProtect service unexpectedly becomes unavailable, then your SharePoint server is not protected. This alert will help you monitor your SharePoint environment.

### PortalProtect Events

**Smart Protection Server - Each time File Reputation service was [Unavailable / Recover]**

It is recommended to enable this alert when Smart Protection server – File Reputation service was Unavailable. If Smart Protection Server was unavailable, PortalProtect will switch to scan files with local components, which need to be the latest version. This alert will help you monitor status of Smart scan.
| **Smart Protection Server** - Each time Web Reputation service was [Unavailable / Recover] | It is recommended to enable this alert when Smart Protection server – Web Reputation service was Unavailable. If Smart Protection Server was unavailable, PortalProtect may switch to scan URLs with TrendMicro global Smart Protection Network which need Internet access. This alert will help you monitor status of Smart scan. |
| **Update - Each time update was [Unsuccessful/Successful]** | It is recommended to enable this option if PortalProtect scans files with local components rather than using the Smart Protection server. |
| **Update - Last update time is older than** | You might want to enable this alert to check if the last update time is older than two (2) days. Trend Micro might not release a daily update, but there should be a release at least once a week. For this reason, if you are getting these alerts, you should verify the latest pattern/engine PortalProtect is using to make sure they are the latest. |
| **Manual/Scheduled scan tasks were [Unsuccessful/Successful]** | By default, this alert is enabled and is very useful to make sure that your manual/scheduled scans are successful. |
| **Manual/Scheduled scan time exceeds** | You might want to enable this alert especially if you have a large content database. If you configure the scheduled/manual scan over the weekend (off-hours) as recommended, you might want to specify the time before business day starts so you can take action to stop the task if still running before business day starts. |
| **The disk space on the local drive (volume) of the backup directory is less than** | This alert is recommended to be enabled so that you get notified when disk space is low. |
| **The log database size exceeds** | This alert is recommended to be enabled so that you get notified when the size of the database exceeds the defined threshold. |
| **The size of quarantined files exceeds** | This alert is recommended to be enabled so that you get notified when the size of the quarantined files exceeds the defined threshold. It is recommended to maintain quarantine files regularly. |
| **Outbreak Alert** | There are three alerts related with outbreak: viruses detected, Un-cleanable viruses, Blocked files. You can select some options to get notified when an outbreak occurs. |

### Reports

| **Notes and Recommendations** |
| **One-time Reports** | Most of the content of this report is useful, therefore it is recommended to select all types when generating a report. |
| **Scheduled Reports** | You can also schedule reports to be sent via email: Daily, Weekly, or Monthly. |
| **Report Maintenance** | This is the number of reports that you would like PortalProtect to generate and keep. |

#### One-time reports

| **Scheduled reports saved in each template** | This is the number of reports in each scheduled report template that you would like PortalProtect to generate and keep. |
| **Report templates** | Number of scheduled report templates that you can generate and keep. When a user chooses the maximum setting of Report templates and clicks "Save", the report module will check the Maintenance setting and delete the older ones. |

**Note:** The default for keeping reports is 180 days. If the Report database size increases too fast, use the following registry key to reduce report keeping days:

Path: HKLM\SOFTWARE\TrendMicro\PortalProtect\CurrentVersion
Key: ReportDataKeepDays
Type: REG_DWORD
Data value: the default value is 180
<table>
<thead>
<tr>
<th>Logs</th>
<th>Notes and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Query</td>
<td>You can query the log for Security risk scan, File blocking, Content filtering, Web Reputation, Data Protection, Updates, Scan Events, Backup for security risk, Unscanable files and Event tracking. You can narrow down the search by providing the violator, site, file name information.</td>
</tr>
<tr>
<td>Log Maintenance</td>
<td>This option allows you to manually delete all the logs or selected logs within the specified days.</td>
</tr>
<tr>
<td>Manual</td>
<td>By default, all the logs that are older than 30 days will be deleted automatically. If you do not want this default option, you can change it based on your security settings.</td>
</tr>
<tr>
<td>Automatic</td>
<td></td>
</tr>
<tr>
<td>Quarantine</td>
<td>You can query quarantined files so you can restore them if needed. Just enter the search criteria, and then click the Search button.</td>
</tr>
<tr>
<td>Restore</td>
<td>If there are results that match criteria and you would like to restore the files back to the location, then, select the check box next to your result and then click &quot;Restore&quot;. You can select multiple results to restore or you can select individual results. It is recommended you check quarantined files periodically.</td>
</tr>
<tr>
<td>Delete</td>
<td>It is not recommended that you delete the query result. However, if you feel there is a need, this option is available. To use, select the result(s) you would like to delete and the &quot;Delete&quot; option will be available. PortalProtect has an automatic delete feature that will delete the old quarantined files that are older than 30 days.</td>
</tr>
<tr>
<td>Quarantine Maintenance</td>
<td>PortalProtect provides manual maintenance or automatic maintenance. By default, automatic maintenance will delete the old quarantined files that are older than 30 days. If you received quarantined files excessive size alert, it is recommended that you use manual maintenance to delete old quarantined files.</td>
</tr>
<tr>
<td>Administration</td>
<td>You can query the log for Security risk scan, File blocking, Content filtering, Web Reputation, Data Protection, Updates, Scan Events, Backup for security risk, Unscanable files and Event tracking. You can narrow down the search by providing the violator, site, file name information.</td>
</tr>
<tr>
<td>Proxy</td>
<td>If your environment requires a Proxy to access the Internet, enter the information on Proxy settings. If you do not enter this required information, updates will be unsuccessful.</td>
</tr>
<tr>
<td>Notification Settings</td>
<td>You can enter multiple addresses separated by a semicolon (;). This will save you time to modify each individual notification for different administrators.</td>
</tr>
<tr>
<td>Email account settings</td>
<td>You can set SMTP server information that will send email notification for PortalProtect.</td>
</tr>
<tr>
<td>SNMP</td>
<td>You can set SNMP server and apply this setting to all SNMP options used by PortalProtect.</td>
</tr>
<tr>
<td>Access Control</td>
<td>The administrator will have full access rights of the entire PortalProtect console and configuration. During installation, you can create an AD group to be administrator of PortalProtect. After installation, you can add new AD groups or AD users to be administrator via access control.</td>
</tr>
<tr>
<td>Operator</td>
<td>The operator will typically only handle routine maintenance tasks, report generation, and so on. It is recommended that you configure Access Control to limit the users from making changes to the configurations of PortalProtect.</td>
</tr>
<tr>
<td>Product License</td>
<td>The product license section allows you to update your existing Activation Code or activate a new Activation Code. When activating new Activation Code, no Internet connection is required. However, if you need to update an existing Activation Code, you must have access to the following URL: <a href="http://licenseupdate.trendmicro.com/ollu/">http://licenseupdate.trendmicro.com/ollu/</a> If you receive an error while trying to update your existing Activation Code, verify that you can access the URL from your SharePoint server.</td>
</tr>
</tbody>
</table>
### World Virus Tracking
If you would like to participate in the World Virus Tracking Program, you can enable this option. The results are available at: http://www.trendmicro.com/map/
By default, it will send the logs every day, 03:00 AM. This time cannot be configured.

### Control Manager Settings
<table>
<thead>
<tr>
<th>Enable communication between the PortalProtect MCP agent and Control Manager</th>
</tr>
</thead>
</table>
If you are using Control Manager (TMCM) to manage your PortalProtect, you must enable this option to register PortalProtect to Control Manager. When registering to Control Manager, it is best practice to keep the entity display name consistent using the default naming convention of [ServerName]_PortalProtect.

### Control Manager Server Settings
It is also best practice to use the FQDN when registering with Control Manager and also using HTTPS for secure communications between PortalProtect and Control Manager. If your IIS server required authentication, make sure you provided the valid username/password for IIS to authenticate.

### MCP Proxy Settings
If your environment uses the Proxy, make sure that you provide the correct Proxy settings and check "Use a proxy server for communication with the Control manager server."

### Two Way Communication Port Forwarding
![Diagram of two-way communication port forwarding](image)
This setting is designed for environment that uses NAT as illustrated in the diagram. If your environment uses NAT, make sure you "Enable two-way communication port forwarding" and provide the appropriate IP Address and Port.

### Trend Support/System Debugger
PortalProtect has built-in debugging capabilities that can be enabled for troubleshooting purposes. If you have any issues with PortalProtect, you should enable these debug modules before reproducing the issue. The debug files are located in \PortalProtect\debug folder.

The following describes the different events when you should enable specific module debugging. When in doubt on which debug module to enable, you can enable them all.

- **PortalProtect Master Service**– This is the main scanning process. Debugging this process must be enabled for all issues.
- **PortalProtect System Watcher**– This module is for the Alerts of PortalProtect services. If you have any issue with the Alert, this module is also needed.
- **SharePoint Virus Scan API Hooking**– This module is about scanning hook for file and Web content. If you have any issue with the real-time scanning, this module is also needed.
- **Manual/Scheduled Scan Process**– This module is for the manual/schedule scan module. If you have any issues with the manual/scheduled scanning, this module is needed.
- **Common Gateway Interface (CGI)**– This module should be enabled if you have any issue with the PortalProtect console.
### Server Management

<table>
<thead>
<tr>
<th>Notes and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Query</strong>&lt;br&gt;Server management will show PortalProtect servers in one farm. You can select to query &quot;Pattern and engine version&quot;, &quot;Scanning status&quot;, &quot;Scanning result&quot;, &quot;Last replication&quot; for all servers in the farm.</td>
</tr>
<tr>
<td><strong>Replication</strong>&lt;br&gt;To replicate settings to other servers, you must select the target servers here. If you wish to select all the servers, select &quot;all servers&quot;. You can also specify servers to do configuration replication. Make sure you have the correct source server from which to replicate settings.</td>
</tr>
<tr>
<td><strong>Select target server</strong>&lt;br&gt;After you have selected the servers to replicate to, you can select which settings you would like to replicate.&lt;br&gt;&quot;Overwrite server-dependent settings (such as backup directories)&quot; should not be selected unless you want the target servers to use the same path as the source for the backup directories.</td>
</tr>
<tr>
<td><strong>Automatic Replication</strong>&lt;br&gt;It is recommended you select this option, which will automatically replicate changed settings to other PortalProtect servers in this farm. You can use one PortalProtect console to configure all servers in one farm.</td>
</tr>
<tr>
<td><strong>Real-time Monitor</strong>&lt;br&gt;Real-time Monitor is useful for reviewing a server’s scanning status in real-time. You can observe the monitor window to verify that PortalProtect is scanning files or Web contents accordingly.&lt;br&gt;Also, take note that if you open the Real-time Monitor window, PortalProtect's management console will not timeout. By default, the management console times-out after 30 minutes or as defined by: &quot;UISessionPeriod&quot; key under [HKEY_LOCAL_MACHINE \ SOFTWARE \ TrendMicro \ ScanMail for Exchange \ CurrentVersion] &lt;br&gt;Make sure you close the Real-time Monitor window once you have completed reviewing the information. It is not recommended to leave this open when you are away from the computer.</td>
</tr>
</tbody>
</table>

---

*PortalProtect 2.1 Best Practices Guide*