

Microsoft Forefront Protection Server Script Kit

Version 1.0

Published: August 2010

For the latest information, please see   
microsoft.com/technet/**SolutionAccelerators**

Copyright © 2010 Microsoft Corporation. All rights reserved. Complying with the applicable copyright laws is your responsibility. By using or providing feedback on this documentation, you agree to the license agreement below.

This documentation is licensed to you under the Creative Commons Attribution License. To view a copy of this license, visit <http://creativecommons.org/licenses/by/3.0/us/> or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA. When using this documentation, provide the following attribution: The Microsoft Operations Framework 4.0 is provided with permission from Microsoft Corporation.

This documentation is provided to you for informational purposes only, and is provided to you entirely "AS IS". Your use of the documentation cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user’s particular environment. To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

Microsoft may have patents, patent applications, trademarks, or other intellectual property rights covering subject matter within this documentation. Except as provided in a separate agreement from Microsoft, your use of this document does not give you any license to these patents, trademarks or other intellectual property.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious.

Microsoft, Active Directory, Forefront, PowerShell, SharePoint, Windows, Windows 7, Windows Vista, Windows XP, Windows Server 2003, and Windows Server 2008 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

You have no obligation to give Microsoft any suggestions, comments or other feedback ("Feedback") relating to the documentation. However, if you do provide any Feedback to Microsoft then you provide to Microsoft, without charge, the right to use, share, and commercialize your Feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the Feedback. You will not give Feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your Feedback in them.

Contents

[**Overview of the Forefront Protection Server Script Kit** 1](#_Toc268005600)

[Who Should Read This Guidance 1](#_Toc268005601)

[Skills and Readiness 1](#_Toc268005602)

[What Is the Forefront Protection Server Script Kit? 2](#_Toc268005603)

[Requirements 2](#_Toc268005604)

[**Forefront Protection Server Script Kit Command Syntax** 3](#_Toc268005605)

[Compare 3](#_Toc268005606)

[Syntax 3](#_Toc268005607)

[Description 3](#_Toc268005608)

[Options 3](#_Toc268005609)

[Example 4](#_Toc268005610)

[Discover 5](#_Toc268005611)

[Syntax 5](#_Toc268005612)

[Description 5](#_Toc268005613)

[Options 5](#_Toc268005614)

[Example 5](#_Toc268005615)

[Export 5](#_Toc268005616)

[Syntax 5](#_Toc268005617)

[Description 5](#_Toc268005618)

[Options 6](#_Toc268005619)

[Example 7](#_Toc268005620)

[Import 7](#_Toc268005621)

[Syntax 7](#_Toc268005622)

[Description 7](#_Toc268005623)

[Options 7](#_Toc268005624)

[Example 8](#_Toc268005625)

[Report 8](#_Toc268005626)

[Syntax 8](#_Toc268005627)

[Description 8](#_Toc268005628)

[Options 9](#_Toc268005629)

[Example 9](#_Toc268005630)

[**Working with the Script Kit** 10](#_Toc268005631)

[Discovering Forefront Protection Servers 10](#_Toc268005632)

[Capturing a Baseline Server Configuration 10](#_Toc268005633)

[Applying a Baseline Configuration to Forefront Protection Servers 11](#_Toc268005634)

[Comparing Running Configurations to the Baseline Configuration 12](#_Toc268005635)

[Generating Server Reports 13](#_Toc268005636)

[**Advanced Script Kit Scenarios and Troubleshooting** 15](#_Toc268005637)

[Exporting Partial Forefront Protection Configurations 15](#_Toc268005638)

[Modifying the Scripts 15](#_Toc268005639)

[How the Script Kit Works 16](#_Toc268005640)

[Troubleshooting Connection Errors 17](#_Toc268005641)

[Troubleshooting Export and Import Failures on Microsoft Exchange Servers 18](#_Toc268005642)

[Resources 18](#_Toc268005643)

[**Feedback** 18](#_Toc268005644)

[**Acknowledgments** 19](#_Toc268005645)

[Development Team 19](#_Toc268005646)

[Contributors and Reviewers 19](#_Toc268005647)

# **Overview of the Forefront Protection Server Script Kit**

Welcome to the Microsoft® Forefront® Protection Server Script Kit. The guidance for this kit provides instructions on how to use the Forefront Protection Server Script Kit (FPSSK). This script kit includes a set of integrated Microsoft Windows® PowerShell™ scripts that enable you to manage from one console multiple Forefront Protection servers deployed across your environment. The functionality of the kit also provides you with basic compliance and reporting capabilities to detect configuration drift and monitor server statistics.

Microsoft Forefront® Protection 2010 for Exchange Server provides fast and effective protection against malware and spam by including multiple scanning engines from industry-leading security partners.

Microsoft Forefront® Protection 2010 for SharePoint® prevents users from uploading or downloading documents containing malware, prohibited content, or sensitive information to SharePoint libraries.

For more information about Forefront Protection 2010 for Microsoft Exchange Server, visit the [Forefront Protection 2010 for Exchange Server](http://go.microsoft.com/fwlink/?LinkId=191470) website. For more information about Forefront Protection 2010 for Microsoft SharePoint, visit the [Forefront Security for SharePoint](http://go.microsoft.com/fwlink/?LinkId=152269) website. For more information about all available accelerators, visit the [Solution Accelerators](http://go.microsoft.com/fwlink/?LinkId=108308) website.

## Who Should Read This Guidance

The Forefront Protection Server Script Kit is for system administrators and other IT pros who manage Exchange Server and SharePoint server deployments that are secured by one of the Microsoft Forefront Server Protection 2010 products. This guidance for IT pros whose jobs may include one or more of the following roles:

* Security professional. Individuals in this role focus on how to provide security across computing platforms within an organization.
* IT operations, help desk, and deployment staff. Individuals in all of these roles troubleshoot security issues as well as application installation, configuration, usability, and manageability issues. They monitor these types of issues to define measurable security improvements with minimal impact on critical business applications. Individuals in IT operations focus on integrating security and controlling change in the deployment process, and deployment personnel focus on administering security updates quickly.
* Consultant. Individuals in this role are aware of security scenarios that span all the business levels of an organization. IT consultants from both Microsoft Services and partners take advantage of knowledge transfer tools for enterprise customers and partners.

## Skills and Readiness

The following skills are required to use the Forefront Protection Server Script Kit:

* Experience with Microsoft Windows PowerShell 2.0.
* Working knowledge of Forefront Protection Server 2010.

## What Is the Forefront Protection Server Script Kit?

The Forefront Protection Server Script Kit (FPSSK) is a set of interrelated Windows PowerShell scripts that you control from a single master script, the FPSSK.ps1 script file. These scripts enable you to manage the configuration of two Forefront Protection products: Forefront Protection 2010 for Microsoft Exchange Server and Forefront Protection 2010 for SharePoint.

The script kit enables you to capture the names of all computers running Forefront Protection 2010 in a an Active Directory domain, capture Forefront Protection 2010 configuration settings from specified computers, deploy those settings to specified computers, compare captured settings to those on specified running computers, and run basic computer status reports.

## Requirements

The Forefront Protection Server Script Kit requires Windows PowerShell 2.0 and Windows Remote Management (WinRM) 2.0. PowerShell 2.0 is pre-installed on Microsoft Windows 7® and Microsoft Windows Server® 2008 R2. You can also install PowerShell 2.0 and WinRM 2.0 on the following supported operating systems:

* Windows Server 2008 Service Pack 1 (SP1)
* Windows Server® 2003 SP2
* Windows Vista® SP1
* Windows® XP SP3

Windows PowerShell 2.0 also requires Microsoft .NET Framework 2.0 SP1.

In addition, you must confirm that your environment meets the following requirements to ensure that the script kit will work:

* Windows PowerShell remoting on the management computer and all servers that you intend to run script kit commands against must be enabled by running the Enable-PSRemoting cmdlet.
* The Windows PowerShell 2.0 session functionality must work properly on all computers in the environment that you manage with the script kit.
* You must modify the Windows PowerShell execution policy on each computer in your environment to **AllSigned** by running the following command:

set-executionpolicy –Scope LocalMachine   
–ExecutionPolicy AllSigned

**Note**   Though not a requirement for running the script kit, having all computers in your environment joined to an Active Directory® domain greatly simplifies using the script kit.

# **Forefront Protection Server Script Kit Command Syntax**

The Forefront Protection Server Script Kit uses specific commands, called *actions*, to enable you to manage the configuration of Forefront Protection 2010 for Microsoft Exchange Server and Forefront Protection 2010 for SharePoint.

The following is the syntax to use in the Windows PowerShell console:

FPSSK.ps1 [-action] [-option1] [-option2] … [-optionn]

There are five actions that you can use with the script kit, and each has one or more options that you can use to specify instructions for the action.

For more information about each action, see the following sections:

* [Compare](#_Compare)
* [Discover](#_Discover)
* [Export](#_Export)
* [Import](#_Import_1)
* [Report](#_Report_1)

For more information about using the actions in your environment, see the "[Working with the Script Kit](#_Working_with_the)" section in this script kit guidance.

**Note**For any script kit option that takes a file or directory path, you can use a period character (**.**) to specify the current directory.

## Compare

This section defines the syntax and options that you can use for the Compare action.

### Syntax

FPSSK.ps1 –Compare [-XmlPath] [-CsvPath] [-ComputerName]   
[-DiscoverCsv] [-Log]

### Description

This action compares the Forefront Protection 2010 configuration files obtained by using the Export action with the configuration settings on one or more servers running Forefront Protection 2010.

### Options

The following table includes the options and descriptions that you can use for the Compare action.

Table 1. Compare Options and Descriptions

| **Option** | **Description** |
| --- | --- |
| **XmlPath** | Required. Specifies a full file path to the Forefront Protection configuration setting .xml file to compare it to a configuration currently in use. |
| **CsvPath** | Specifies a full file path to the Forefront Protection configuration setting .csv file to compare to a running configuration. |
| **ComputerName** | Specifies an array of target computers to compare configuration settings to the Forefront Protection configuration settings files specified in the **XmlPath** and **CsvPath** options. The default is the local computer.  For this option, in the PowerShell console type the NetBIOS name, an IP address, or a fully-qualified domain name of one or more computers. To specify the local computer, type the computer name, "localhost", or a dot (.). When the computer is in a different domain than the management computer, the fully-qualified domain name is required. |
| **DiscoverCsv** | Specifies the full file path to the .csv file that was created using the [Discover](#_The_Discover_Action) action, which contains a list of computers running Forefront Protection 2010. |
| **Log** | Specifies the directory path to where the action writes log files. This option also tells the action to write the results to a log file. |

#### Remarks

In Windows Vista and later versions of Windows, to include the local computer in the *ComputerName* parameter, you must start Windows PowerShell using the **Run as** **administrator** option.

Two options are available to define remote servers in this operation:

* **ComputerName**. Use this option to specify an array of computer names in the PowerShell console.
* **DiscoverCsv**. Use this option to specify the .csv file that the script kit created when you ran the Discover action. This .csv file contains the full list of servers on a domain running Forefront Protection Server 2010. You can edit the file to contain only Microsoft Exchange Server computers or SharePoint Server computers.

The configuration files of Forefront Protection 2010 for Microsoft Exchange Server are different from those of Forefront Protection 2010 for SharePoint. When you compare the two, there will be a large number of differences that the script kit displays to the console.

### Example

This example uses the **XmlPath** option to specify the FPSSK-Export.xml file in the current directory as the Forefront Protection XML configuration file to compare against. It then uses the **DiscoverCsv** option to specify the FPSSK-Discover.csv file in the local directory as the list of servers against which to compare the baseline configuration files.

C:\PS>.\FPSSK.ps1 -Compare -XmlPath .\FPSSK-Export.xml  
-DiscoverCsv .\FPSSK-Discover.csv

#### See Also

The "[Comparing Running Configurations to the Baseline Configuration](#_Comparing_Running_Configurations)" section in this script kit guidance.

## Discover

This section defines the syntax and options that you can use for the Discover action.

### Syntax

FPSSK.ps1 –Discover [-Domain] [-ExportCsv]

### Description

This action identifies all Forefront Protection 2010 servers in the specified Active Directory domain.

### Options

The following table includes the options and descriptions for the Discover action.

Table 2. Discover Options and Descriptions

| **Option** | **Description** |
| --- | --- |
| **Domain** | Specifies the fully qualified name of an Active Directory domain. |
| **ExportCsv** | Specifies the path to the directory in which to write the .csv file that contains the names of all of the servers running Forefront Protection 2010 in the specified domain. |

#### Remarks

By default, the Discover action writes the results to the Windows PowerShell console. If you define a path using the **ExportCsv** option, the action creates a .csv file in the directory you specify and writes the results to it.

### Example

This example uses the Discover action to find all servers running the Forefront Protection product in the Contoso domain. The **ExportCsv** option tells the script kit that it should create a .csv file in the current directory, C:\PS, and then write the results to it.

C:\PS>.\FPSSK.ps1 -Discover -Domain Contoso.com –ExportCsv .

#### See Also

The "[Discovering Forefront Protection Servers](#_Discovering_Forefront_Protection)" section in this script kit guidance.

## Export

This section defines the syntax and options that you can use for the Export action.

### Syntax

FPSSK.ps1 –Export [-Path] [-ComputerName] [-Element]  
[-DiscoverCsv] [-Log]

### Description

This action captures the Forefront Protection 2010 configuration settings from the specified array of computers and then stores the settings to an .xml file and a .csv file on the local computer.

### Options

The following table includes the options and descriptions for the Export action.

Table 3. Export Options and Descriptions

| **Option** | **Description** |
| --- | --- |
| **Path** | Required. Specifies the path to the directory in which to write the .xml file and .csv file that contain the Forefront Protection 2010 configuration settings. |
| **ComputerName** | Specifies an array of target computers from which to capture the Forefront Protection configuration settings. The default is the local computer.  For this option, in the PowerShell console type the NetBIOS name, an IP address, or a fully-qualified domain name of one or more computers. To specify the local computer, type the computer name, "localhost", or a dot (.). When the computer is in a different domain than the management computer, the fully-qualified domain name is required. |
| **Element** | Specifies the configuration sections to capture. If you do not specify this option, the Export action captures all Forefront Protection 2010 configuration settings. For more information, see the "[Exporting Partial Forefront Protection Configurations](#_Exporting_Partial_Forefront)" section. |
| **DiscoverCsv** | Specifies the full file path to the .csv file that was created using the [Discover](#_The_Discover_Action) action, which contains a list of computers running Forefront Protection 2010. |
| **Log** | Specifies the directory path where the action writes log files. This option also tells the action to write the results to a log file. |

#### Remarks

You can select specific configuration sections to capture by using the **Element** option and specifying one or more configuration section names as a list of comma-separated strings.

**Note**   This is an advanced scenario and does not back up the full Forefront Protection 2010 configuration.

Two options are available to define remote servers in this operation:

* **ComputerName**. Use this option to specify an array of computer names in the PowerShell console.
* **DiscoverCsv**. Use this option to specify the .csv file that the; script kit created when you ran the Discover action. This .csv file contains the full list of all servers on a domain running Forefront Protection Server 2010. You can edit the file to contain only Microsoft Exchange Server computers or SharePoint Server computers.

**Important**   On computers running Microsoft Exchange Server, we recommend to not use the **Import** or **Export** options unless the Forefront Protection 2010 for Microsoft Exchange Server **ExchangeManagementAvailable** variable is set to **true**. For more information, see the "[Troubleshooting Export and Import Failures on Microsoft Exchange Servers](#_Troubleshooting_Export_and)" section.

### Example

This example uses the Export action to capture the configuration settings of two servers on the domain, one named server1.contoso.com and the other named server2.contoso.com. The command uses the **Path** option to write the resultant configuration files to the same directory from which the Export action is run, the C:\PS directory.

C:\PS>.\FPSSK.ps1 -Export -Path . -ComputerName server1.contoso.com, server2.contoso.com

#### See Also

The "[Capturing a Baseline Server Configuration](#_Capturing_a_Baseline)" section in this script kit guidance.

## Import

This section defines the syntax and options that you can use for the Import action.

### Syntax

FPSSK.ps1 –Import [-XmlPath] [-CsvPath] [-ComputerName]   
[-DiscoverCsv] [-Log] [-NoConfirm]

### Description

This action imports the configuration settings captured using the Export action to the specified array of target computers.

### Options

The following table includes the options and descriptions for the Import action.

Table 4. Import Options and Descriptions

| **Option** | **Description** |
| --- | --- |
| **XmlPath** | Required. Specifies a full file path to the Forefront Protection 2010 configuration settings .xml file to load on the specified servers. |
| **CsvPath** | Specifies a full file path to the Forefront Protection 2010 configuration setting .csv file to load to the specified servers. |
| **ComputerName** | Specifies an array of target computers on which to load the Forefront Protection 2010 configuration settings. The default is the local computer.  For this option, in the PowerShell console type the NetBIOS name, an IP address, or a fully-qualified domain name of one or more computers. To specify the local computer, type the computer name, "localhost", or a dot (.). When the computer is in a different domain than the local computer, the fully-qualified domain name is required. |
| **DiscoverCsv** | Specifies the full file path to the .csv file that was created using the [Discover](#_The_Discover_Action) action, which contains a list of computers running Forefront Protection 2010. |
| **Log** | Specifies the directory path where the action writes log files. This option also tells the action to write the results to a log file. |
| **NoConfirm** | Specifies that warnings do not prompt users. |

#### Remarks

Two options are available to define remote servers in this operation:

* **ComputerName**. Use this option to specify an array of computer names in the PowerShell console.
* **DiscoverCsv**. Use this option to specify the .csv file that the script kit created when you ran the Discover action. This .csv file contains the full list of servers on a domain running Forefront Protection Server 2010. You can edit the file to contain only Microsoft Exchange Server computers or SharePoint Server computers.

**Important**   On computers running Microsoft Exchange Server, the **Import** or **Export** options may display an error message if the Forefront Protection 2010 for Microsoft Exchange Server **ExchangeManagementAvailable** variable is set to **false**. For more information, see the "[Troubleshooting Export and Import Failures on Microsoft Exchange Servers](#_Troubleshooting_Export_and)" section.

### Example

This example calls the Import action. The command uses the **XmlPath** option to define the path to the FPSSK-Export.xml configuration file in the local directory. For the **ComputerName** option, the command defines two servers to configure, server01.contoso.com and server02.contoso.com. It also uses the **NoConfirm** option to suppress the overwrite warnings that otherwise would appear when you call the Import action.

C:\PS>.\FPSSK.ps1 -Import -XmlPath .\FPSSK-Export.xml

-ComputerName server01.contoso.com, server02.contoso.com

-NoConfirm

#### See Also

The "[Applying a Baseline Configuration to Forefront Protection Servers](#_Applying_a_Baseline)" section.

## Report

This section defines the syntax and options that you can use for the Report action.

### Syntax

FPSSK.ps1 –Report [-ComputerName] [-DiscoverCsv] [-Log]

### Description

This action generates a basic Forefront Protection Server status report for the specified computers.

### Options

The following table includes the options and descriptions for the Report action.

Table 5. Report Options and Descriptions

| **Option** | **Description** |
| --- | --- |
| **ComputerName** | Specifies an array of target computers on which to load the Forefront Protection 2010 configuration settings. The default is the local computer.  For this option, in the PowerShell console type the NetBIOS name, an IP address, or a fully-qualified domain name of one or more computers. To specify the local computer, type the computer name, "localhost", or a dot (.). When the computer is in a different domain than the local computer, the fully-qualified domain name is required. |
| **DiscoverCsv** | Specifies the full file path to the .csv file that was created using the [Discover](#_The_Discover_Action) action, which contains a list of computers running Forefront Protection 2010. |
| **Log** | Specifies the directory path where the action writes log files. This option also tells the action to write the results to a log file. |

#### Remarks

Two options are available to define remote servers in this operation:

* **ComputerName**. Use this option to specify an array of computer names in the PowerShell console.
* **DiscoverCsv**. Use this option to specify the .csv file that the script kit created when you ran the Discover action. This .csv file contains the full list of servers on a domain running Forefront Protection Server 2010. You can edit the file to contain only Microsoft Exchange Server computers or SharePoint Server computers.

### Example

This example uses the Report action to generate a report for server01.contoso.com and server02.contoso.com. It also generates a summary report that captures cumulative statistics of the two servers. The **Log** option instructs the script kit to write the resultant files to the same directory from which the Report action is run, the C:\PS directory.

C:\PS>.\FPSSK.ps1 -Report -ComputerName server01.contoso.com,  
server02.contoso.com -Log .

#### See Also

The "[Generating Server Reports](#_Generating_Server_Reports)" section in this script kit guidance.

# **Working with the Script Kit**

The Forefront Protection Server Script Kit enables you to automate configuration management tasks for Forefront Protection 2010 on Exchange Server or SharePoint.

The flexibility of the script kit enables you to design your own workflows. The following is a sample workflow for the script kit:

1. Discover all servers running Forefront Protection in a domain. For more information, see the "[Discovering Forefront Protection Servers](#_Discovering_Forefront_Protection)" section.
2. Capture a baseline Forefront Protection configuration from a specific server on the domain. For more information, see the "[Capturing a Baseline Server Configuration](#_Capturing_a_Baseline)" section.
3. Apply the baseline configuration to one or more servers running Forefront Protection 2010. For more information, see the "[Applying a Baseline Configuration to Forefront Protection Servers](#_Applying_a_Baseline)" section.
4. Compare the baseline configuration to the Forefront Protection configuration on the other servers running in your environment. For more information, see the "[Comparing Running Configurations to the Baseline Configuration](#_Comparing_Running_Configurations)" section.
5. Generate reports that contain Forefront Protection statistics. For more information, see the "[Generating Server Reports](#_Generating_Server_Reports)" section.

## Discovering Forefront Protection Servers

Determining which servers in your Exchange Server or SharePoint production environment are running Microsoft Forefront Protection is a key step in using the script kit. The Discover action enables you to quickly determine which Exchange servers and SharePoint servers in your Active Directory domain are running Forefront Protection.

The Discover action enables you to receive the results in two ways:

* Print the results to the Windows PowerShell screen.
* Use the **ExportCsv** option to pass the results to a .csv file in the directory that you specify. In most cases, we recommend this approach because the .csv file is then available for you to use with other script kit actions.

**Note**   In a large deployment, the Discover action can prove invaluable in identifying servers running Forefront Protection 2010.

The following example uses the Discover action to find all servers running the Forefront Protection product in the Contoso domain. It then sends the results to a Servers.csv file in the same directory from which the command is run, the C:\PS directory:

C:\PS>.\FPSSK.ps1 -Discover -Domain Contoso.com –ExportCsv .

For more information, see the "[Discover](#_The_Discover_Action)" section.

## Capturing a Baseline Server Configuration

After configuring a server with all the settings that you want to apply to all installations of Forefront Protection running on other servers in your environment, you can capture those settings by using the Export action. The Export action contacts the computers that you specify to obtain their configuration settings. After it obtains the configuration settings, this action writes the configuration settings of one or more target computer to the following two files on the local computer that you are using to run the script kit:

* An .xml file that contains the standard Forefront Protection configuration settings.
* A .csv file that contains advanced settings not typically set by an administrator.

You can specify where the action stores these files using the **Path** option.

You can choose to capture the configuration from a single remote server, an array of servers defined on the PowerShell command line or in a .csv file, or the local computer. By default, the Export action runs against the local computer.

Export captures the complete Forefront Protection configuration and is an excellent way not only to capture the baseline server configuration, but to perform periodic configuration backups as necessary.

**Important**   The configuration files for Forefront Protection 2010 for Microsoft Exchange Server and Forefront Protection 2010 for SharePoint are different. Be sure to capture a set of baseline configuration files for each server product if you run both of them in your environment.

The following example uses the Export action to capture the configuration settings for two servers on the domain, one named server1.contoso.com and the other named server2.contoso.com. The command writes the resultant configuration files to the same directory from which the Export action is run, the C:\PS directory.

C:\PS>.\FPSSK.ps1 -Export -Path . -ComputerName server1.contoso.com, server2.contoso.com

For more information, see the "[Export](#_Export)" section.

## Applying a Baseline Configuration to Forefront Protection Servers

After you run the Export action to create a baseline configuration files, you can import the configuration settings from those files into all servers running Forefront Protection in your domain. You use the Import action to perform this task, which enables you to replicate the baseline configuration across a deployment quickly and easily.

The Import action requires you to supply the .xml files and .csv files that you want to import to the remote servers by using the **XmlPath** and **CsvPath** options. You also use the **ComputerName** option to define the servers on which you want to import the configuration settings. You can perform this action on the local server, a single remote server, or an array of remote servers.

**Important**   If you do not specify a value for the **ComputerName** option, the default behavior of the script kit for this option is to import the configuration to the local computer.

If you specify an array of servers, the script kit performs the **Import** command on each remote server in a sequence that you specify. The script kit completes all of the import steps on the first remote server in the sequence before starting the import process on the next remote server.

The Import action performs the following steps on each remote computer:

1. Copies the baseline configuration .xml files and .csv files from the local computer on which you are running the script kit to the remote server.
2. Performs configuration import commands and overwrites the Forefront Protection configuration on the remote server.

If a failure results from any sequence of this action, by default the script kit logs the failure to the Windows PowerShell console. However, if you specify a large number of servers, the data on the console screen may become unreadable. In this case, we recommend using the **Log** option to write the errors to a file.

**Important**   The configuration files of Forefront Protection for Microsoft Exchange Server and Forefront Protection for SharePoint are different. Be sure that you import the correct baseline configuration files to your servers running Microsoft Exchange Server and those running SharePoint Server.

When you use the Import action, by default a warning message appears to indicate that you are about to overwrite the Forefront Protection configuration on the remote computer, and prompts you to confirm that you want to continue with this action. To automatically ignore these warnings, you can specify the **NoConfirm** option when you run the Import action.

If you have a large number of Exchange Server or SharePoint Server computers in your deployment, you can quickly configure them to match the baseline configuration. For example, if you created 50 antispam rules for Exchange Server on one server, you could use the Export action to capture the configuration for those rules. These configurations could be Allow/Block lists, Sender Block Lists, or Block Recipient Lists as examples. You could then use the **Import** action to deploy these configured rules to all of the Exchange Server computers in your environment.

The following example calls the Import action. This action first uses the **XmlPath** to define the path to the FPSSK-Export.xml configuration file. Then the example uses the **ComputerName** option to define two servers to configure, in this case server01.contoso.com and server02.contoso.com. This example also use the **NoConfirm** option to suppress the overwrite warnings that appear when you call the Import action.

C:\PS>.\FPSSK.ps1 -Import -XmlPath .\FPSSK-Export.xml

-ComputerName server01.contoso.com, server02.contoso.com

-NoConfirm

For more information, see the "[Import](#_Import_1)" section.

## Comparing Running Configurations to the Baseline Configuration

After configuring a number of servers and running Forefront Protection 2010 on them, the next important task is to compare the baseline configuration you captured to configurations on the servers. You can do this periodically to determine if the configuration on any of the servers has changed over time. Configuration changes can occur for many reasons, such as multiple administrators working in parallel to update different software components on a server or a modification of the organization's change-tracking process that occurred after the baseline configuration was applied to the servers in the deployment.

You perform this task using the Compare action.

The Compare action uses the .xml files and .csv files that you created using the Export action to compare them to the configuration of the remote servers that you specify. The results of this action display in the Windows PowerShell console. The console displays the differences in two color-coded sections:

* **Remote**. This section displays all configuration sections that exist on the remote server but do not exist in the baseline configuration files.
* **Local**. This section displays all configuration sections that exist in the baseline configuration files but do not exist in the remote server configuration.

**Note**   The configuration files for Forefront Protection for Microsoft Exchange Server and Forefront Protection for SharePoint are different. When you compare the two, there will be a large number of differences that the script kit displays to the console.

Use one of the following options to define the remote servers that you want to use in the operation:

* **ComputerName**. Use this option to specify an array of computer names in the PowerShell console.
* **DiscoverCsv**. Use this option to specify the .csv file that the script kit created when you ran the Discover action. This .csv file contains the full list of all servers on a domain running Forefront Protection Server 2010. You can edit the file to contain only Microsoft Exchange Server computers or SharePoint Server computers.

The Compare action does not perform any updates to configuration files. If there are differences between the baseline configuration files and the configuration on a running server, it is up to you to decide what actions to perform to resolve them.

This example uses the **XmlPath** option to specify the FPSSK-Export.xml file in the current directory as the Forefront Protection XML configuration file to compare against. It then uses the **DiscoverCsv** option to specify the FPSSK-Discover.csv file in the local directory as the list of servers against which to compare the baseline configuration files.

C:\PS>.\FPSSK.ps1 -Compare -XmlPath .\FPSSK-Export.xml   
-DiscoverCsv .\FPSSK-Discover.csv

For more information, see the "[Compare](#_Compare)" section.

## Generating Server Reports

The script kit also supports a task to generate reports that display data about Forefront Protection 2010 statistics, including some basic server health information. You can run reports by using the Report action. This action provides basic health status of Forefront Protection Server components and writes them to a text file.

By default, the Report action gathers statistics from the local computer and then writes them to the Windows PowerShell console. You can use the **ComputerName** option to define an array of server names from which to gather statistics, or the **DiscoverCsv** option to use a .csv file to define the servers from which to gather statistics. The **Log** option instructs the script kit to write the report to a text file located in a path that you define.

The server-specific reports contain the following sections:

* **Information about the server**. This includes the computer name, operating system, Forefront Protection 2010 product, and information about the Exchange Server or SharePoint Server.
* **Health Status**. This enumerates the status of each Forefront Protection 2010 Health Point, which defines the time and date of the last update.
* **Malware Detection**. This includes the number of files scanned, the number of files that contained malware, and other statistics on malware that Forefront Protection discovered on the server.
* **Spam Messages** (for Exchange Server only). This includes statistics on the number of spam messages received by the server and statistics on the possible Forefront Protection responses to each piece of spam.
* **Incidents**. This includes statistics on the types of protection incidents that Forefront Protection performed.
* **Quarantine Events**. This includes statistics on the types of security incidents that resulted in Forefront Protection performing a quarantine action.
* **Signature Updates**. This includes statistics on each scanning engine installed with Forefront Protection 2010, when the last signature update was performed, and the version number of the current scanning engine.

The summary report contains the following sections:

* Current Malware report
* Spam messages (for Exchange Server only)
* Incidents
* Quarantine events

When you generate a report, there are two parts of each section: the latest statistics and statistics since you installed Forefront Protection on the server. The latest statistics of the Malware Detection section are stored in a buffer that you must clear to get statistics since the last time you ran the Report action. You can do this on the remote server by running the **Clear-FseReport** cmdlet on computers running Forefront Protection 2010 for Microsoft Exchange Server or the **Clear-FsspReport** cmdlet on computers running Forefront Protection 2010 for SharePoint.

The following example uses the Report action to generate a report for server01.contoso.com and server02.contoso.com. The action generates a summary report that captures cumulative statics for the two servers. The **Log** option then instructs the script kit to write the resultant files to the same directory from which the Report action is run, the C:\PS directory.

C:\PS>.\FPSSK.ps1 -Report -ComputerName server01.contoso.com,  
server02.contoso.com -Log .

For more information, see the "[Report](#_Report_1)" section.

# **Advanced Script Kit Scenarios and Troubleshooting**

This section of the Forefront Protection Server Script Kit guidance provides information about advanced techniques that you can use with the script kit, such as modifying the scripts to run them in your environment. It also provides troubleshooting information that you can use to address instances when the script kit does not work as expected.

## Exporting Partial Forefront Protection Configurations

The script kit Export action enables you to only capture the Forefront Protection 2010 configuration settings that you select by providing the **Element** option. Specify the configuration settings that you want to capture in the XML configuration output as a series of comma-separated values.

The following example uses the Element option of the Export action to capture the **ExcahngeAntiSpamPS** and **FSSEHPolicy** configuration settings from the server1.contoso.com computer, which in this case runs Microsoft Exchange Server. The command writes the resultant configuration files to the same directory from which the Export action is run, the C:\PS directory.

C:\PS>.\FPSSK.ps1 -Export -Path . -ComputerName server1.contoso.com –Element ExchangeAntiSpamPS, FSSEHSPolicy

## Modifying the Scripts

As mentioned earlier, the script kit is a set of interrelated script files. The seven script files that the script kit contains can be broken into the following categories:

* The central command script file, FPSSK.ps1, which calls all the other script files. It is responsible for parsing the command arguments and calling the appropriate action script file based on those arguments.
* The FPSSK-Common.ps1 file, which provides common functions to all scripts in the script kit.
* A script file for each of the actions provided by the script kit. These include the FPSSK-Compare.ps1, FPSSK-Discover.ps1, FPSSK-Export.ps1, FPSSK-Import.ps1, and FPSSK-Report.ps1 script files.

You can choose to use one or more of the script files associated with the actions outside of the script kit, or you can modify any of the script kit code for your environment. To understand how the script kit works to make informed decisions about how to modify the scripts, see the "[How the Script Kit Works](#_How_the_Script)" section.

The scripts in the script kit are signed by Microsoft. When you modify the scripts in any way, they are no longer recognized as signed. You must perform the following two tasks to enable the modified scripts to work across all of the servers in your environment:

1. Sign the modified scripts. Work with a certificate authority to sign the modified scripts. For more information about this topic, see [Using PowerShell to Sign Scripts with Digital Certificates](http://go.microsoft.com/fwlink/?LinkId=160357) and [Set-AuthenticodeSignature](http://go.microsoft.com/fwlink/?LinkId=113391).
2. Ensure that the PowerShell remote execution level is set to **AllSigned** on all computers. You can do this in one of two ways. First, you can do it manually on each computer in your environment by using the set-executionpolicy cmdlet as in the following example:

set-executionpolicy –Scope LocalMachine   
–ExecutionPolicy AllSigned

You can also create a Group Policy object (GPO) that sets the execution policy to AllSigned, and then deploy the object across all of the servers in your environment.

**Note**   You can download the [Windows PowerShell Administrative Templates](http://go.microsoft.com/fwlink/?LinkId=93675) to create a GPO that sets the execution policy to AllSigned for all the required servers.

For more information, see [Set-ExecutionPolicy](http://go.microsoft.com/fwlink/?LinkId=113394). For more background on PowerShell execution policies, see [Stop Malicious Code in Windows PowerShell with Execution Policies](http://go.microsoft.com/fwlink/?LinkId=192747).

### How the Script Kit Works

When you call the script kit from the Windows PowerShell console, you call the FPSSK.ps1, which starts the process of running the action you specified. The script kit performs the following steps:

1. The FPSSK.ps1 file parses all of the arguments and determines whether all of the arguments are valid.
2. If the FPSSK.ps1 file finds any errors in the arguments, it prints an error message to the Windows PowerShell console and terminates execution of the action. It does this before it attempts to connect to any remote servers.
3. If you specified the Discover action, the script contacts the Active Directory domain controller for the domain specified in the command. It then retrieves a list of all servers with Forefront Protection 2010 installed on them.
4. If you specified any of the other actions, the FPSSK.ps1 performs the following substeps:
5. The script kit iterates through the array of servers you specified, and attempts to connect to each server in the array sequentially.
6. If the script kit cannot connect to a server, it writes an error message to the PowerShell console and attempts to connect to the next server in the array.
7. When the script kit connects to a server, it creates a remote PowerShell 2.0 session and starts executing the specified action.
8. On session startup, the script kit loads the required FPSSK cmdlet to the remote machine.
9. The script kit loads and runs the action provided by the loaded cmdlet.
10. The script kit performs any required cleanup steps on the remote server.
11. The script kit prints reports to the PowerShell console on the local computer or to a log file at the specified directory location.
12. The script kit moves to the next server in the array until it finishes processing the action for all specified servers.

The script kit was designed to use the PowerShell 2.0 session feature on each remote server that it connects to by using the **New-PSSession** cmdlet. This enables the script kit to be authenticated once to perform all of the steps each action requires on the remote server. This authentication method reduces the amount of latency required simply to authenticate the request for each operation involved in executing the action.

For more information about running remote commands on a computer running PowerShell 2.0, In the Windows PowerShell About Help Topics, see [about\_Remote](http://go.microsoft.com/fwlink/?LinkId=135182), [about\_Remote\_FAQ](http://go.microsoft.com/fwlink/?LinkId=135183), [about\_Remote\_Requirements](http://go.microsoft.com/fwlink/?LinkId=135187), and [about\_Remote\_Troubleshooting](http://go.microsoft.com/fwlink/?LinkId=135188). For more information about PowerShell sessions, see [about\_PSSessions](http://go.microsoft.com/fwlink/?LinkId=135181).

## Troubleshooting Connection Errors

Connection errors to the remote computer are the most prevalent issues encountered when using the script kit. These issues make it impossible to start the remote PowerShell session.

When the script kit cannot connect to a remote computer, regardless of the reason, it writes an error message to the PowerShell console.

The following example displays the command, the status message, and the error message that the script kit returns when the attempt to connect to a server names server1.contoso.com fails.

PS C:\PS> .\FPSSK.ps1 -report -computername server1.contoso.com

Connecting to server1.contoso.com

**Error: Failed to connect to server1.contoso.com**

**Note**   The script kit formats the error message text as red when it writes it to the PowerShell console.

Use the following steps to troubleshoot connection problems:

1. Attempt to establish a session to the remote computer manually. You can do this by using the **New-PSSession** cmdlet and the **ComputerName** parameter to specify the remote computer on which to establish the session. The following is an example of how to establish a remote session manually, and run a series of commands in that session.

$s = New-PSSession –ComputerName Server1.contoso.com

Invoke-command –session $s –ScriptBlock {$p = Get-Process}

1. Check to ensure that the WinRM service on the remote computer has started and is configured to allow remote management. For more information, see [Installation and Configuration for Windows Remote Management](http://go.microsoft.com/fwlink/?LinkId=171111).
2. Check to ensure that the firewall on the remote computer is not blocking the WinRM service. For more information, see [Installation and Configuration for Windows Remote Management](http://go.microsoft.com/fwlink/?LinkId=171111).

The inability to establish a remote session can also be caused by a corrupt Windows PowerShell plug-in on the remote server. If the remote computer is experiencing this problem, it will send the following error message when you run the **New-PSSession** cmdlet during troubleshooting:

The WS-Management service cannot process the request. The resource URI (<http://schemas.microsoft.com/powershell/Microsoft.Powershell>) was not found in the WS-Management catalog. The catalog contains the metadata that describes the resources, or logical endpoints.

If you receive this error message, perform the following steps:

1. On the remote server, log on as a local administrator and run the following cmdlet:

Remove-Item   
HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\  
WSMAN\Plugin\Microsoft.PowerShell

1. On the remote server, run the **Enable-PSRemoting** cmdlet.

**Note**   The Enable-PSRemoting cmdlet performs all of the required configuration for the WinRM service.

You should now be able to establish a connection and a remote session with the target server.

## Troubleshooting Export and Import Failures on Microsoft Exchange Servers

When you install Forefront Protection 2010 for Microsoft Exchange Server on a computer running Microsoft Exchange Server, a delay can occur between the completion of the installation and when the server is available for monitoring by Forefront Protection Server. This is because Exchange Server stores its configuration settings in Active Directory and requires some time to synchronize the new settings from the Exchange Server to the Active Directory domain controller.

Forefront Protection 2010 captures this information in the **ExchangeManagementAvailable** variable, which is set to either **True** or **False**. If this variable is set to **False**, the script kit Export and Import actions may not work correctly, and they may return an error message. You can determine the value of the **ExchangeManagementAvailable** variable by using the **Get-FseExchangeManagementStatus** cmdlet from the Forefront Management Shell on the computer that you are using to attempt to export configuration information from or import configuration information to.

For more information about how to troubleshoot this problem, see [Troubleshooting integration with Exchange Server 2010 Active Directory Components](http://technet.microsoft.com/en-us/library/ee358879.aspx).

In most cases, the **ExchangeManagementAvailable** variable will be set to **False** for a very short time. If this condition persists, it may indicate other problems with the server that you may need to investigate.

# Resources

The following resources provide more information about Microsoft products closely related to this script kit:

* [Microsoft Forefront Protection 2010 for Microsoft Exchange Server](http://go.microsoft.com/fwlink/?LinkId=182950).
* [Microsoft Forefront Protection 2010 for SharePoint](http://go.microsoft.com/fwlink/?LinkId=152269).
* [Windows PowerShell](http://go.microsoft.com/fwlink/?LinkId=107116).

# **Feedback**

Please send comments and feedback to [secwish@microsoft.com](mailto:secwish@microsoft.com?subject=Microsoft%20Forefront%20Protection%20Server%20Script%20Kit%20feedback). To keep current with the latest releases and beta review programs, please subscribe to our news feed on [Security Solution Accelerators](http://go.microsoft.com/fwlink/?LinkId=168796) website.

# **Acknowledgments**

The Microsoft Forefront Protection Server Script Kit team acknowledges and thanks the people who participated in the development of this guide.

## Development Team

Author

Benjamin Curry, *Content Master Ltd.*

Editor

John Cobb, *Wadeware LLC*

Product Manager

Mike Chan, *Microsoft*

Michelle Arney*, Microsoft*

Program Manager

Jeffrey Sigman, *Microsoft*

Ken Toole, *Microsoft*

Test Manager

Sumit Parikh, *Microsoft*

Testers

Raxit Gajjar, *Infosys Technologies Ltd*

## Contributors and Reviewers

Ryan McGrath, *Microsoft*