

TLS Compliance Management Pack Guide

Version: 1.0.0.20

Microsoft Corporation

Published: 2020.07.06

Authored by: Sean Christie | Microsoft Services | Premier Field Engineering

sean.christie@microsoft.com

Copyright

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it.

Some examples depicted herein are provided for illustration only and are fictitious.  No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes.

© 2020 Microsoft Corporation. All rights reserved.

Microsoft, Windows, Windows Internet Explorer, Windows PowerShell, and Windows Server are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Table of Contents

[Introduction to the TLS Compliance Management Pack Guide 3](#_Toc45539724)

[Dependencies and Prerequisites 3](#_Toc45539725)

[Management packs this management pack depends on: 3](#_Toc45539726)

[Major Version History 4](#_Toc45539727)

[Supported Configurations 4](#_Toc45539728)

[Getting Started 4](#_Toc45539729)

[Importing the Management Pack 4](#_Toc45539730)

[Setup Overview: 4](#_Toc45539731)

[Security Considerations 5](#_Toc45539732)

[Classes 5](#_Toc45539733)

[Create a New Management Pack for Customizations 5](#_Toc45539734)

[Discoveries 6](#_Toc45539735)

[Security Protocol Discovery 6](#_Toc45539736)

[Security Protocol Provider Class Discovery 6](#_Toc45539737)

[Security Protocol Cipher Class Discovery 7](#_Toc45539738)

[Security Protocol Hash Class Discovery 8](#_Toc45539739)

[Security Protocol KeyEx Class Discovery 8](#_Toc45539740)

[Monitors 9](#_Toc45539741)

[TLS Compliance Monitor 9](#_Toc45539742)

[Cipher Compliance Monitor 9](#_Toc45539743)

[Hash Compliance Monitor 9](#_Toc45539744)

[Key Exchange Algorithm Compliance Monitor 10](#_Toc45539745)

[.Net Version Compliance Monitor 10](#_Toc45539746)

[Reporting 10](#_Toc45539747)

**Revision History**

|  |  |
| --- | --- |
| Release Date | Changes |
| **06/11/2020** | Initial release |
| 7/13/2020 | Added text for the .Net Monitor |
|  |  |

|  |  |
| --- | --- |
| Management Packs | Description |
| **TLS\_Compliance\_Pack.mp** | Main management pack |

# Introduction to the TLS Compliance Management Pack Guide

**NOTE:** The configurations for TLS 1.2 are complex and are not a one-size-fits all for each OS. So ensure you do your research and make sure all relevant OS versions, framework versions, and hotfixes are installed to support your compliance.

This MP gives you a quick and easy way to track your TLS compliance in your environment. The base monitor in this MP will evaluate your Security Protocol settings and ensure you are following recommended best practices for Security Protocol settings. Additionally you can enable additional monitors within this MP that track .Net Versions that are innately compatible with TLS registry settings(4.7+) and additionally you can enable monitors that will make sure you are using more secure ciphers suites, hashes, and key exchange algorithms.

Moving to TLS 1.2

<https://docs.microsoft.com/en-us/security/engineering/solving-tls1-problem>

.NetVersion interaction with respects to TLS 1.2

<https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls>

For Windows 7 and Server 2012 and below:

<https://support.microsoft.com/en-us/help/3140245/update-to-enable-tls-1-1-and-tls-1-2-as-default-secure-protocols-in-wi>

## 

## Dependencies and Prerequisites

This management pack requires a minimum version of Operations Manager 2012 or later (to my knowledge).

### Management packs this management pack depends on:

|  |  |
| --- | --- |
| Microsoft.SystemCenter.Internal | 7.0.8433.0 |
| Microsoft.SystemCenter.Library | 7.0.8433.0 |
| Microsoft.Windows.Library | 7.5.8501.0 |
| System.Health.Library | 7.0.8433.0 |
| System.Library | 7.5.8501.0 |
| System.Performance.Library | 7.5.8501.0 |

# Major Version History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Changes** | **Notes** |
| 06/11/2020 | 1.0.0.20 | Initial Release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Supported Configurations

|  |  |
| --- | --- |
| **Component** | **Supported Versions** |
| System Center Operations Manager | 2019, 2016, 2012 R2, 2012 Sp1 |
| Powershell | 3.0 or higher |
| Agent Managed Operating System | Windows 10, Windows server 2012 R2, Windows Server 2016, Windows Server 2019, **Windows 7\* Windows Server 2012\*** |

**\*Windows7 and Windows Server 2012 and below require updates for the data evaluated in this MP to be valid.**

<https://support.microsoft.com/en-us/help/3140245/update-to-enable-tls-1-1-and-tls-1-2-as-default-secure-protocols-in-wi>

# Getting Started

## Importing the Management Pack

Other than verifying the management pack dependencies are installed in the management group, there are no other prerequisites before importing.

## Setup Overview:

1) **Import Management Pack**

# Security Considerations

This management pack uses script execution to simply read the values of some registry keys and evaluate them. Ensure the action account used on the agent has this level or permissions.

# Classes

The following table describes the available classes:

|  |  |
| --- | --- |
| **Available Classes** | **Description** |
| Security.Protocol.Class | Seed class |
| Security.Protocol.Provider.Class | Class for Security Protocols (TLS/SSL) |
| Security.Protocol.Cipher.Class | Class for Cipher Suites |
| Security.Protocol.Hash.Class | Class for Hashes |
| Security.Protocol.KeyEx.Class | Class for Key Exchange Algorithms |

## Create a New Management Pack for Customizations

Most vendor management packs are sealed so that you cannot change any of the original settings in the management pack file. However, you can create customizations, such as overrides or new monitoring objects, and save them to a different management pack. By default, Operations Manager 2007 saves all customizations to the default management pack. As a best practice, you should instead create a separate management pack for each sealed management pack you want to customize.

Creating a new management pack for storing overrides has the following advantages:

• It simplifies the process of exporting customizations that were created in your test and pre-production environments to your production environment. For example, instead of exporting a default management pack that contains customizations from multiple management packs, you can export just the management pack that contains customizations of a single management pack.

• It allows you to delete the original management pack without first needing to delete the default management pack. A management pack that contains customizations is dependent on the original management pack. This dependency requires you to delete the management pack with customizations before you can delete the original management pack. If all of your customizations are saved to the default management pack, you must delete the default management pack before you can delete an original management pack.

• It is easier to track and update customizations to individual management packs.

For more information about sealed and unsealed management packs, see Management Pack Formats (<http://go.microsoft.com/fwlink/?LinkId=108355>). For more information about management pack customizations and the default management pack, see About Management Packs in Operations Manager 2007 (<http://go.microsoft.com/fwlink/?LinkId=108356>).

# Discoveries

## Security Protocol Discovery

This discovery looks for the existence of this key registry key on the system, prepends the computer name, and is stored as the key property for all its sub classes

HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\

Instance Properties

KeyPath = “ComputerName+ HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\”

## Security Protocol Provider Class Discovery

This discovery discovers all protocols in the seed class registry hive and collects their settings. It also looks for registry values that indicate whether applications are allowed to use the default OS settings for security protocols, collects information on .Net version, collects SSL function data, and lastly collects registry settings for whether strong cryptography is enabled.

**Key Values Collected:**

HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

HKLM:\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full\

HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319

HKLM:\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319

HKLM:\SOFTWARE\Microsoft\.NETFramework\v2.0.50727

HKLM:\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v2.0.50727

Instance Properties

CYPTO = Strong Cryptography Settings.

DEFTLS = Setting for App ability to use OS Defaults.

DOTNET = .Net Version

FUNC = SSL Fucntion strings

SSL\_2.0cl = client key for SSL 2.0 Settings

SSL\_2.0sv = server key for SSL 2.0 Settings.

SSL\_3.0cl = client key for SSL 3.0 Settings

SSL\_3.0sv = server key for SSL 3.0 Settings.

TLS\_1.0cl = client key for TLS 1.0 Settings

TLS\_1.0sv = server key for TLS 1.0 Settings.

TLS\_1.1cl = client key for TLS 1.1 Settings

TLS\_1.1sv = server key for TLS 1.1 Settings

TLS\_1.2cl = client key for TLS 1.2 Settings

TLS\_1.2sv = server key for TLS 1.2 Settings.

## Security Protocol Cipher Class Discovery

This discovery discovers all Cipher suites in the registry.

**Key Values Collected:**

HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers

Instance Properties

AES128 = Settings for AES 128/128

AES256 = Settings for AES 256/256

DES56 = Settings for DES 56/56

NULL = Settings for NULL

RC2128 = Settings for RC2 128/128

RC240128 = Settings for RC2 40/128

RC256128 = Settings for RC2 56/128

RC4128 = Settings for RC4 128/128

RC440128 = Settings for RC4 40/128

RC456128 = Settings for RC4 56/128

RC464128 = Settings for RC4 64/128

TriDes168 = Settings for Triple DES 168

## Security Protocol Hash Class Discovery

This discovery discovers all Hashes in the registry.

**Key Values Collected:**

HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes

Instance Properties

MD5 = Settings for MD5

SHA = Settings for SHA

SHA256 = Settings for SHA256

SHA384 = Settings for SHA384

SHA512 = Settings for SHA512

## Security Protocol KeyEx Class Discovery

This discovery discovers all Key Exchange Algorithms in the registry.

**Key Values Collected:**

HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms

Instance Properties

DiffHel = Settings for Diffie-Hellman

ECDH = Settings for ECDH

PKCS = Settings for PKCS

# Monitors

## TLS Compliance Monitor

Default: Enabled.

This uses a Powershell script that will test registry values to ensure they meet best practice standards for TLS 1.2 compliance settings. The expected values below constitute a healthy value. Anything else will present in a warning state.

Strong Cryptography (CRYPTO) – Supported

Allow Apps to use OS Defaults (DEFTLS) – Using OS Defaults

TLS 1.2 Client OR Server OR Both – Enabled

Non-TLS 1.2 Protocols - Disabled

## Cipher Compliance Monitor

Default: Disabled.

This uses a Powershell script that will test registry values to ensure they meet best practice standards for secure Cipher Suite settings. The expected values below constitute a healthy value. Anything else will present in a warning state.

AES 128/128, AES 256/256 – Enabled

All other Cipher Suites - Disabled

## Hash Compliance Monitor

Default: Disabled.

This uses a Powershell script that will test registry values to ensure they meet best practice standards for secure Hash settings. The expected values below constitute a healthy value. Anything else will present in a warning state.

MD5 – Disabled

SHA – Disabled

SHA256, SHA384, SHA512 – Enabled

## Key Exchange Algorithm Compliance Monitor

Default: Disabled.

This uses a Powershell script that will test registry values to ensure they meet best practice standards for secure Key Exchange Algorithm settings. The expected values below constitute a healthy value. Anything else will present in a warning state.

Diffie-Hellman – Disabled

ECDH – Disabled

## .Net Version Compliance Monitor

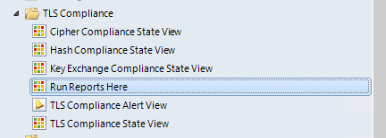
Default: Disabled.

If your .Net Version is above 4.6.2 making the recommended registry changes will work for most OS versions. So, I added this optional monitor to check for .NET versions to assist you in what I think is the easier approach to making sure you are compliant. AGAIN, understanding the subtle nuances to this are very important.

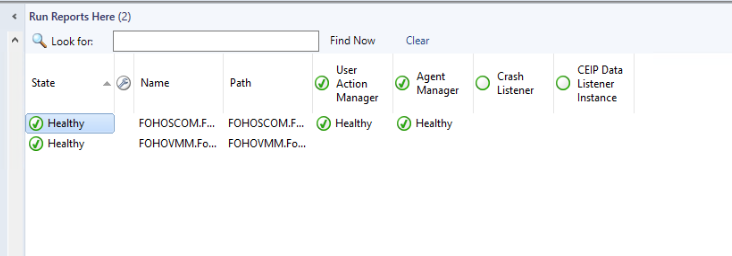
# Reporting

To export a report of all settings to CSV simply use the “Run reports Here” view.

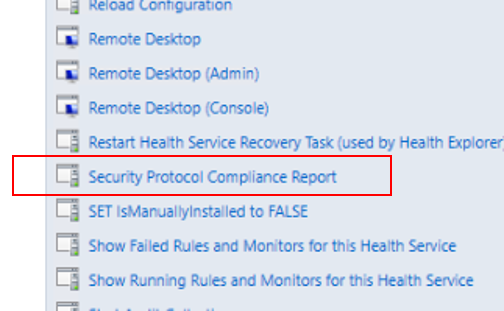
1. Under the TLS Compliance Folder locate the “Run Reports Here” State view.



1. Select a Management Server you want to run the reports on.



1. In the Task Pane select the “Security Protocol Compliance Report”



1. Run it
2. This will output all class discovery data to C:\TLSCompliance in a CSV Format.

