System Center Configuration Manager



TLS 1.2 Prerequisites Configuration Baseline

Prepared by

**Richard McIver**

Microsoft Premier Field Engineer

Richard.McIver@microsoft.com

Version 1.0

Contents

[1 Purpose 5](#_Toc535928076)

[2 Overview 5](#_Toc535928077)

[3 Instructions 5](#_Toc535928078)

[3.1 Import the TLS 1.2 Prerequisites.cab file 5](#_Toc535928079)

[3.2 Deploy the TLS 1.2 Prerequisites Configuration Baseline 6](#_Toc535928080)

[4 Configuration Baseline Detail 6](#_Toc535928081)

[4.1 Configuration Item Detail 7](#_Toc535928082)

[4.1.1 TLS 1.2 - .NET Framework Use Strong Cryptography (32-bit OS) 7](#_Toc535928083)

[4.1.2 TLS 1.2 - .NET Framework UseStrongCryptography (64-bit OS) 14](#_Toc535928084)

[4.1.3 TLS 1.2 - Internet Explorer 11 29](#_Toc535928085)

[4.1.4 TLS 1.2 - KB2898850 for .NET Framework 4.5.1 and 4.5.2 (32-bit OS) 31](#_Toc535928086)

[4.1.5 TLS 1.2 - KB2898850 for .NET Framework 4.5.1 and 4.5.2 (64-bit OS) 33](#_Toc535928087)

[4.1.6 TLS 1.2 - KB3140245 for WinHTTP Protocols 37](#_Toc535928088)

[4.1.7 TLS 1.2 - KB3154518 for .NET Framework 3.5.1 (32-bit OS) 39](#_Toc535928089)

[4.1.8 TLS 1.2 - KB3154518 for .NET Framework 3.5.1 (64-bit OS) 41](#_Toc535928090)

[4.1.9 TLS 1.2 - KB4019276 for Windows Server 2008 SP2 46](#_Toc535928091)

[4.1.10 TLS 1.2 - KB4022720 for WSUS (Windows Server 2012 R2) 47](#_Toc535928092)

[4.1.11 TLS 1.2 - KB4022721 for WSUS (Windows Server 2012) 50](#_Toc535928093)

[4.1.12 TLS 1.2 - Operating System (Server) 52](#_Toc535928094)

[4.1.13 TLS 1.2 - Operating System (Workstation) 54](#_Toc535928095)

[4.1.14 TLS 1.2 - SCHANNEL Protocol - DisabledByDefault 55](#_Toc535928096)

[4.1.15 TLS 1.2 - SCHANNEL Protocol - Enabled 59](#_Toc535928097)

[4.1.16 TLS 1.2 - SQL Server Native Client (32-bit OS) 62](#_Toc535928098)

[4.1.17 TLS 1.2 - SQL Server Native Client (64-bit OS) 68](#_Toc535928099)

[4.1.18 TLS 1.2 - WinHTTP Default Secure Protocols (32-bit OS) 80](#_Toc535928100)

[4.1.19 TLS 1.2 - WinHTTP Default Secure Protocols (64-bit OS) 82](#_Toc535928101)

[5 References 86](#_Toc535928102)

Revision and Signoff Sheet

Change Record

| Date | Author | Version | Change Reference |
| --- | --- | --- | --- |
| 01/22/2019 | Richard McIver | 1 | Initial version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Reviewers

| Name | Version Approved | Position | Date |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Purpose

The purpose of this document is to provide detailed information and instructions for the co-located TLS 1.2 Prerequisites Configuration Baseline for System Center Configuration Manager.

1. Overview

The TLS 1.2 Prerequisites Configuration Baseline checks the target system for documented settings, patches, and other minimum requirements to support the TLS 1.2 protocol for System Center Configuration Manager communication.

If all detected requirements are met, the baseline will report a status of “Compliant”. If one or more detected requirements are not met, the baseline will report a status on “Non-Compliant”. If non-compliant, each Configuration Item within the baseline will return a severity of either Critical or Warning, depending on the criticality of the finding.

A severity level of Critical indicates that a key component of the system requires action to ensure TLS 1.2 support with Configuration Manager. A severity of Warning indicates that action may be required depending on the environment.

If configured to do so within the baseline deployment, several of the included Configuration Items will take corrective action to remediate a non-compliant result. **Carefully review this document to understand what changes will be made to avoid adverse effects.**

1. Instructions
   1. Import the TLS 1.2 Prerequisites.cab file

|  |  |
| --- | --- |
| Step | Guidance |
| 1 | Download and save **TLS 1.2 Prerequisites.cab** to an accessible location |
| 2 | Open the Configuration Manager console |
| 3 | Select the **Assets and Compliance** node and expand **Compliance Settings** |
| 4 | Right-click on **Configuration Baselines** and select **Import Configuration Data** |
| 5 | In the **Import Configuration Data Wizard**, click the **Add** button. Browse to **TLS 1.2 Prerequisites.cab** and click **Open**. *NOTE: If you receive a warning that the publisher could not be verified, click Yes to proceed.* |
| 6 | Click **Next** |
| 7 | Click **Next** |
| 8 | Click **Close** to finish the import process |

* 1. Deploy the TLS 1.2 Prerequisites Configuration Baseline

|  |  |
| --- | --- |
| Step | Guidance |
| 1 | Open the Configuration Manager console |
| 2 | Browse to **Assets and Compliance\Configuration Settings\Configuration Baselines** |
| 3 | Right-click **TLS 1.2 Prerequisites** and select **Deploy** |
| 4 | Click the **Browse** button and select the desired collection to deploy the baseline |
| 5 | Customize the schedule as needed to determine how frequently the baseline will re-evaluate the targeted computers |
| 5 | If desired, configure the ***Remediate noncompliant rules when supported*** and ***Generate an alert*** options |
| 6 | Click **OK** |

1. Configuration Baseline Detail

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 Prerequisites |
| Description | Verifies that the system is configured to support TLS 1.2 communication with SCCM. See KB4040243 for more information. <https://support.microsoft.com/en-us/help/4040243/how-to-enable-tls-1-2-for-configuration-manager> |
| Evaluation Conditions | TLS 1.2 - .NET Framework UseStrongCryptography (32-bit OS)  TLS 1.2 - .NET Framework UseStrongCryptography (64-bit OS)  TLS 1.2 - Internet Explorer 11  TLS 1.2 - KB2898850 for .NET Framework 4.5.1 and 4.5.2 (32-bit OS)  TLS 1.2 - KB2898850 for .NET Framework 4.5.1 and 4.5.2 (64-bit OS)  TLS 1.2 - KB3140245 for WinHTTP Protocols  TLS 1.2 - KB3154518 for .NET Framework 3.5.1 (32-bit OS)  TLS 1.2 - KB3154518 for .NET Framework 3.5.1 (64-bit OS)  TLS 1.2 - KB4019276 for Windows Server 2008 SP2  TLS 1.2 - KB4022720 for WSUS (Windows Server 2012 R2)  TLS 1.2 - KB4022721 for WSUS (Windows Server 2012)  TLS 1.2 - Operating System (Server)  TLS 1.2 - Operating System (Workstation)  TLS 1.2 - SCHANNEL Protocol – DisabledByDefault  TLS 1.2 - SCHANNEL Protocol – Enabled  TLS 1.2 - SQL Server Native Client (32-bit OS)  TLS 1.2 - SQL Server Native Client (64-bit OS)  TLS 1.2 - WinHTTP Default Secure Protocols (32-bit OS)  TLS 1.2 - WinHTTP Default Secure Protocols (64-bit OS) |

* 1. Configuration Item Detail
     1. TLS 1.2 - .NET Framework Use Strong Cryptography (32-bit OS)

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 - .NET Framework Use Strong Cryptography (32-bit OS) |
| Description | See KB4040243 |
| Supported Platforms | All Windows Vista (32-bit)  All Windows 7 (32-bit)  All Windows 8 (32-bit)  All Windows 8.1 (32-bit)  All Windows 10 (32-bit)  All Windows Server 2008 (32-bit)  Windows Embedded 8.1 Industry (32-bit)  Windows Embedded 8 Industry (32-bit)  Windows Embedded 8 Standard (32-bit)  Embedded Windows 7 (32-bit) |
| Settings | .NET 3.0 UseStrongCryptography Enabled  SchUseStrongCrypto\_.NET 2.0.50727  SchUseStrongCrypto\_.NET 3.5  SchUseStrongCrypto\_.NET 4.6 and earlier |
| Compliance Rules | .NET 2.0.50727 UseStrongCryptography Enabled  .NET 3.0 Use Strong Cryptography Enabled  .NET 3.5 UseStrongCryptography Enabled  .NET 4.6 and earlier UseStrongCryptography Enabled |

* + - 1. Settings
         1. .NET 3.0 UseStrongCryptography Enabled

|  |  |
| --- | --- |
|  |  |
| Name | .NET 3.0 UseStrongCryptography Enabled |
| Description |  |
| Setting Type | Script |
| Data type | .Boolean |
| Run scripts by using the logged on user credentials | . |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Language | Windows PowerShell |
| Discovery Script |  |
| Remediation Script Language | Windows PowerShell |
| Remediation Script |  |
| Compliance Rules | .NET 3.0 Use Strong Cryptography Enabled |

* + - * 1. SchUseStrongCrypto\_.NET 2.0.50727

|  |  |
| --- | --- |
|  |  |
| Name | .SchUseStrongCrypto\_.NET 2.0.50727 |
| Description | See KB4040243 and Microsoft Security Advisory 296038. NET Framework 4.6.1 and earlier versions must be configured to support strong cryptography. |
| Setting Type | Script |
| Data type | .Boolean |
| Run scripts by using the logged on user credentials | . |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Language | Windows PowerShell |
| Discovery Script |  |
| Remediation Script Language | Windows PowerShell |
| Remediation Script |  |
| Compliance Rules | .NET 2.0.50727 UseStrongCryptography Enabled |

* + - * 1. SchUseStrongCrypto\_.NET 3.5

|  |  |
| --- | --- |
|  |  |
| Name | SchUseStrongCrypto\_.NET 3.5 |
| Description |  |
| Setting Type | Script |
| Data type | .Boolean |
| Run scripts by using the logged on user credentials | . |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Language | Windows PowerShell |
| Discovery Script |  |
| Remediation Script Language | Windows PowerShell |
| Remediation Script |  |
| Compliance Rules | .NET 3.5 UseStrongCryptography Enabled |

* + - * 1. SchUseStrongCrypto\_.NET 4.6 and earlier

|  |  |
| --- | --- |
|  |  |
| Name | SchUseStrongCrypto\_.NET 4.6 and earlier |
| Description |  |
| Setting Type | Script |
| Data type | .Boolean |
| Run scripts by using the logged on user credentials | . |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Language | Windows PowerShell |
| Discovery Script |  |
| Remediation Script Language | Windows PowerShell |
| Remediation Script |  |
| Compliance Rules | .NET 4.6 and earlier UseStrongCryptography Enabled |

* + - 1. Compliance Rules
         1. .NET 2.0.50727 UseStrongCryptography Enabled

|  |  |
| --- | --- |
|  |  |
| Name | .NET 2.0.50727 UseStrongCryptography Enabled |
| Description | See KB4040243 and Microsoft Security Advisory 296038. NET Framework 4.6.1 and earlier versions must be configured to support strong cryptography. |
| Selected setting | TLS 1.2 - .NET Framework Use Strong Cryptography (32-bit OS) \ SchUseStrongCrypto\_.NET 2.0.50727 |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Run the specified remediation script when this setting is noncompliant |  |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + - * 1. .NET 3.0 Use Strong Cryptography Enabled

|  |  |
| --- | --- |
|  |  |
| Name | .NET 3.0 Use Strong Cryptography Enabled |
| Description | See KB4040243 and Microsoft Security Advisory 296038. NET Framework 4.6.1 and earlier versions must be configured to support strong cryptography. |
| Selected setting | TLS 1.2 - .NET Framework Use Strong Cryptography (32-bit OS) \ .NET 3.0 UseStrongCryptography Enabled |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Run the specified remediation script when this setting is noncompliant |  |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + - * 1. .NET 3.5 UseStrongCryptography Enabled

|  |  |
| --- | --- |
|  |  |
| Name | .NET 3.5 UseStrongCryptography Enabled |
| Description | See KB4040243 and Microsoft Security Advisory 296038. NET Framework 4.6.1 and earlier versions must be configured to support strong cryptography. |
| Selected setting | TLS 1.2 - .NET Framework Use Strong Cryptography (32-bit OS) \ SchUseStrongCrypto\_.NET 3.5 |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Run the specified remediation script when this setting is noncompliant |  |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + - * 1. .NET 4.6 and earlier UseStrongCryptography Enabled

|  |  |
| --- | --- |
|  |  |
| Name | .NET 4.6 and earlier UseStrongCryptography Enabled |
| Description | See KB4040243 and Microsoft Security Advisory 296038. NET Framework 4.6.1 and earlier versions must be configured to support strong cryptography. |
| Selected setting | TLS 1.2 - .NET Framework Use Strong Cryptography (32-bit OS) \ SchUseStrongCrypto\_.NET 4.6 and earlier |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Run the specified remediation script when this setting is noncompliant |  |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + 1. TLS 1.2 - .NET Framework UseStrongCryptography (64-bit OS)

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 - .NET Framework Use Strong Cryptography (32-bit OS) |
| Description | See KB4040243 |
| Supported Platforms | All Windows Vista (64-bit)  All Windows 7 (64-bit)  All Windows 8 (64-bit)  All Windows 8.1 (64-bit)  All Windows 10 (64-bit)  All Windows Server 2008 (non-R2)(64-bit)  All Windows Server 2008 R2 (64-bit)  All Windows Server 2012 (64-bit)  All Windows Server 2012 R2 (64-bit)  All Windows Server 2016 and higher (64-bit)  Windows Embedded 8.1 Industry (64-bit)  Windows Embedded 8 Industry (64-bit)  Windows Embedded 8 Standard (64-bit)  Embedded Windows 7 (64-bit)  All Windows Server 2019 and higher (64-bit) |
| Settings | SchUseStrongCrypto\_.NET 2.0.50727 (x64)  SchUseStrongCrypto\_.NET 2.0.50727 (x86)  SchUseStrongCrypto\_.NET 3.0 (x64)  SchUseStrongCrypto\_.NET 3.0 (x86)  SchUseStrongCrypto\_.NET 3.5 (x64)  SchUseStrongCrypto\_.NET 3.5 (x86)  SchUseStrongCrypto\_.NET 4.6 and earlier (x64)  SchUseStrongCrypto\_.NET 4.6 and earlier (x86) |
| Compliance Rules | .NET 2.0.50727 SchUseStrongCrypto Enabled (x64)  .NET 2.0.50727 SchUseStrongCrypto Enabled (x86)  .NET 3.0 SchUseStrongCrypto Enabled (x64)  .NET 3.0 SchUseStrongCrypto Enabled (x86)  .NET 3.5 SchUseStrongCrypto Enabled (x64)  .NET 3.5 SchUseStrongCrypto Enabled (x86)  .NET 4.6 and earlier SchUseStrongCrypto Enabled (x64)  .NET 4.6 and earlier SchUseStrongCrypto Enabled (x86) |

* + - 1. Settings
         1. .NET 3.0 UseStrongCryptography Enabled (x64)

|  |  |
| --- | --- |
|  |  |
| Name | SchUseStrongCrypto\_.NET 2.0.50727 (x64) |
| Description |  |
| Setting Type | Script |
| Data type | Boolean |
| Run scripts by using the logged on user credentials | . |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Language | Windows PowerShell |
| Discovery Script |  |
| Remediation Script Language | Windows PowerShell |
| Remediation Script |  |
| Compliance Rules | .NET 2.0.50727 SchUseStrongCrypto Enabled (x64) |

* + - * 1. SchUseStrongCrypto\_.NET 2.0.50727 (x86)

|  |  |
| --- | --- |
|  |  |
| Name | SchUseStrongCrypto\_.NET 2.0.50727 (x86) |
| Description |  |
| Setting Type | Script |
| Data type | Boolean |
| Run scripts by using the logged on user credentials | . |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Language | Windows PowerShell |
| Discovery Script |  |
| Remediation Script Language | Windows PowerShell |
| Remediation Script |  |
| Compliance Rules | .NET 2.0.50727 SchUseStrongCrypto Enabled (x86) |

* + - * 1. SchUseStrongCrypto\_.NET 3.0 (x64)

|  |  |
| --- | --- |
|  |  |
| Name | SchUseStrongCrypto\_.NET 3.0 (x64) |
| Description |  |
| Setting Type | Script |
| Data type | .Boolean |
| Run scripts by using the logged on user credentials | . |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Language | Windows PowerShell |
| Discovery Script |  |
| Remediation Script Language | Windows PowerShell |
| Remediation Script |  |
| Compliance Rules | .NET 3.0 SchUseStrongCrypto Enabled (x64) |

* + - * 1. SchUseStrongCrypto\_.NET 3.0 (x86)

|  |  |
| --- | --- |
|  |  |
| Name | SchUseStrongCrypto\_.NET 3.0 (x86) |
| Description |  |
| Setting Type | Script |
| Data type | .Boolean |
| Run scripts by using the logged on user credentials | . |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Language | Windows PowerShell |
| Discovery Script |  |
| Remediation Script Language | Windows PowerShell |
| Remediation Script |  |
| Compliance Rules | .NET 3.0 SchUseStrongCrypto Enabled (x86) |

* + - * 1. SchUseStrongCrypto\_.NET 3.0 (x64)

|  |  |
| --- | --- |
|  |  |
| Name | SchUseStrongCrypto\_.NET 3.0 (x64) |
| Description |  |
| Setting Type | Script |
| Data type | Boolean |
| Run scripts by using the logged on user credentials | . |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Language | Windows PowerShell |
| Discovery Script |  |
| Remediation Script Language | Windows PowerShell |
| Remediation Script |  |
| Compliance Rules | .NET 3.5 SchUseStrongCrypto Enabled (x64) |

* + - * 1. SchUseStrongCrypto\_.NET 3.5 (x86)

|  |  |
| --- | --- |
|  |  |
| Name | SchUseStrongCrypto\_.NET 3.5 (x86) |
| Description |  |
| Setting Type | Script |
| Data type | .Boolean |
| Run scripts by using the logged on user credentials | . |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Language | Windows PowerShell |
| Discovery Script |  |
| Remediation Script Language | Windows PowerShell |
| Remediation Script |  |
| Compliance Rules | .NET 3.5 SchUseStrongCrypto Enabled (x86) |

* + - * 1. SchUseStrongCrypto\_.NET 4.6 and earlier (x64)

|  |  |
| --- | --- |
|  |  |
| Name | SchUseStrongCrypto\_.NET 4.6 and earlier (x64) |
| Description |  |
| Setting Type | Script |
| Data type | Boolean |
| Run scripts by using the logged on user credentials | . |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Language | Windows PowerShell |
| Discovery Script |  |
| Remediation Script Language | Windows PowerShell |
| Remediation Script |  |
| Compliance Rules | .NET 4.6 and earlier SchUseStrongCrypto Enabled (x64) |

* + - * 1. SchUseStrongCrypto\_.NET 4.6 and earlier (x86)

|  |  |
| --- | --- |
|  |  |
| Name | SchUseStrongCrypto\_.NET 4.6 and earlier (x86) |
| Description |  |
| Setting Type | Script |
| Data type | Boolean |
| Run scripts by using the logged on user credentials | . |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Language | Windows PowerShell |
| Discovery Script |  |
| Remediation Script Language | Windows PowerShell |
| Remediation Script |  |
| Compliance Rules | .NET 4.6 and earlier SchUseStrongCrypto Enabled (x86) |

* + - 1. Compliance Rules
         1. .NET 2.0.50727 SchUseStrongCrypto Enabled (x64)

|  |  |
| --- | --- |
|  |  |
| Name | .NET 2.0.50727 SchUseStrongCrypto Enabled (x64) |
| Description | See KB4040243 and Microsoft Security Advisory 296038. NET Framework 4.6.1 and earlier versions must be configured to support strong cryptography. |
| Selected setting | TLS 1.2 - .NET Framework UseStrongCryptography (64-bit OS) \ SchUseStrongCrypto\_.NET 2.0.50727 (x64) |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Run the specified remediation script when this setting is noncompliant |  |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + - * 1. .NET 2.0.50727 SchUseStrongCrypto Enabled (x86)

|  |  |
| --- | --- |
|  |  |
| Name | .NET 2.0.50727 SchUseStrongCrypto Enabled (x86) |
| Description | See KB4040243 and Microsoft Security Advisory 296038. NET Framework 4.6.1 and earlier versions must be configured to support strong cryptography. |
| Selected setting | TLS 1.2 - .NET Framework UseStrongCryptography (64-bit OS) \ SchUseStrongCrypto\_.NET 2.0.50727 (x86) |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Run the specified remediation script when this setting is noncompliant |  |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + - * 1. .NET 3.0 SchUseStrongCrypto Enabled (x64)

|  |  |
| --- | --- |
|  |  |
| Name | .NET 3.0 SchUseStrongCrypto Enabled (x64) |
| Description | See KB4040243 and Microsoft Security Advisory 296038. NET Framework 4.6.1 and earlier versions must be configured to support strong cryptography. |
| Selected setting | TLS 1.2 - .NET Framework UseStrongCryptography (64-bit OS) \ SchUseStrongCrypto\_.NET 3.0 (x64) |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Run the specified remediation script when this setting is noncompliant |  |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + - * 1. .NET 3.0 SchUseStrongCrypto Enabled (x86)

|  |  |
| --- | --- |
|  |  |
| Name | .NET 3.0 SchUseStrongCrypto Enabled (x86) |
| Description | See KB4040243 and Microsoft Security Advisory 296038. NET Framework 4.6.1 and earlier versions must be configured to support strong cryptography. |
| Selected setting | TLS 1.2 - .NET Framework UseStrongCryptography (64-bit OS) \ SchUseStrongCrypto\_.NET 3.0 (x86) |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Run the specified remediation script when this setting is noncompliant |  |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + - * 1. .NET 3.5 SchUseStrongCrypto Enabled (x64)

|  |  |
| --- | --- |
|  |  |
| Name | .NET 3.5 SchUseStrongCrypto Enabled (x64) |
| Description | See KB4040243 and Microsoft Security Advisory 296038. NET Framework 4.6.1 and earlier versions must be configured to support strong cryptography. |
| Selected setting | TLS 1.2 - .NET Framework UseStrongCryptography (64-bit OS) \ SchUseStrongCrypto\_.NET 3.5 (x64) |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Run the specified remediation script when this setting is noncompliant |  |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + - * 1. .NET 3.5 SchUseStrongCrypto Enabled (x86)

|  |  |
| --- | --- |
|  |  |
| Name | .NET 3.5 SchUseStrongCrypto Enabled (x86) |
| Description | See KB4040243 and Microsoft Security Advisory 296038. NET Framework 4.6.1 and earlier versions must be configured to support strong cryptography. |
| Selected setting | TLS 1.2 - .NET Framework UseStrongCryptography (64-bit OS) \ SchUseStrongCrypto\_.NET 3.5 (x86) |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Run the specified remediation script when this setting is noncompliant |  |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + - * 1. .NET 4.6 and earlier SchUseStrongCrypto Enabled (x64)

|  |  |
| --- | --- |
|  |  |
| Name | . .NET 4.6 and earlier SchUseStrongCrypto Enabled (x64) |
| Description | See KB4040243 and Microsoft Security Advisory 296038. NET Framework 4.6.1 and earlier versions must be configured to support strong cryptography. |
| Selected setting | TLS 1.2 - .NET Framework UseStrongCryptography (64-bit OS) \ SchUseStrongCrypto\_.NET 4.6 and earlier (x64) |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Run the specified remediation script when this setting is noncompliant |  |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + - * 1. .NET 4.6 and earlier SchUseStrongCrypto Enabled (x86)

|  |  |
| --- | --- |
|  |  |
| Name | .NET 4.6 and earlier SchUseStrongCrypto Enabled (x86) |
| Description | See KB4040243 and Microsoft Security Advisory 296038. NET Framework 4.6.1 and earlier versions must be configured to support strong cryptography. |
| Selected setting | TLS 1.2 - .NET Framework UseStrongCryptography (64-bit OS) \ SchUseStrongCrypto\_.NET 4.6 and earlier (x86) |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Run the specified remediation script when this setting is noncompliant |  |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + 1. TLS 1.2 - Internet Explorer 11

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 - .NET Framework Use Strong Cryptography (32-bit OS) |
| Description | See KB4040243 |
| Supported Platforms | All Windows Vista  All Windows 7  All Windows 8  All Windows 8.1  All Windows 10  All Windows Server 2008  All Windows Server 2008 R2  All Windows Server 2012  All Windows Server 2012 R2  All Windows Server 2016  Windows Embedded 8.1 Industry  Windows Embedded 8 Industry  Windows Embedded 8 Standard  Embedded Windows 7  All Windows Server 2019 |
| Settings | Internet Explorer Version |
| Compliance Rules | IE Version |

* + - 1. Settings
         1. Internet Explorer Version

|  |  |
| --- | --- |
|  |  |
| Name | Internet Explorer Version |
| Description |  |
| Setting Type | Registry value |
| Hive Name | HKEY\_LOCAL\_MACHINE |
| Key Name | . SOFTWARE\Microsoft\Internet Explorer |
| Value Name | svcVersion |
| Discovery Script Language | Windows PowerShell |
| This registry value is associated with a 64-bit application |  |
| Compliance Rules | IE Version |

* + - 1. Compliance Rules
         1. IE Version

|  |  |
| --- | --- |
|  |  |
| Name | IE Version |
| Description | TLS 1.2 is enabled by default in Internet Explorer 11. See: <https://blogs.msdn.microsoft.com/ie/2013/11/12/ie11-automatically-makes-over-40-of-the-web-more-secure-while-making-sure-sites-continue-to-work/> |
| Selected setting | TLS 1.2 - Internet Explorer 11 \ Internet Explorer Version |
| Rule type | Value |
| The setting must comply with the following rule | Internet Explorer Version: **Begins with**  The following values: **11** |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + 1. TLS 1.2 - KB2898850 for .NET Framework 4.5.1 and 4.5.2 (32-bit OS)

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 - KB2898850 for .NET Framework 4.5.1 and 4.5.2 (32-bit OS) |
| Description |  |
| Supported Platforms | All Windows Vista (32-bit)  All Windows 7 (32-bit)  All Windows 8 (32-bit)  All Windows 8.1 (32-bit)  All Windows 10 (32-bit)  All Windows Server 2008 (32-bit)  Windows Embedded 8.1 Industry (32-bit)  Windows Embedded 8 Industry (32-bit)  Windows Embedded 8 Standard (32-bit)  Embedded Windows 7 (32-bit) |
| Settings | KB2898850 Installed for .NET 4.5.1 or 4.5.2 |
| Compliance Rules | KB2898850 Installed for .NET Framework 4.5.1 and 4.5.2 |

* + - 1. Settings
         1. KB2898850 Installed for .NET 4.5.1 or 4.5.2

|  |  |
| --- | --- |
|  |  |
| Name | KB2898850 Installed for .NET 4.5.1 or 4.5.2 |
| Description | KB2898850 is required to enable TLS 1.2 support for .NET Framework 4.5.1 and 4.5.2. Download link: <https://www.microsoft.com/en-us/download/details.aspx?id=42883> |
| Setting Type | Script |
| Data type | .Boolean |
| Run scripts by using the logged on user credentials | . |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Language | Windows PowerShell |
| Discovery Script |  |
| Remediation Script | None |
| Compliance Rules | KB2898850 Installed for .NET Framework 4.5.1 and 4.5.2 |

* + - 1. Compliance Rules
         1. KB2898850 Installed (32-bit OS)

|  |  |
| --- | --- |
|  |  |
| Name | KB2898850 Installed (32-bit OS) |
| Description | KB2898850 is required to enable TLS 1.2 support for .NET Framework 4.5.1 and 4.5.2. Download link: https://www.microsoft.com/en-us/download/details.aspx?id=42883 |
| Selected setting | TLS 1.2 - KB2898850 for .NET Framework 4.5.1 and 4.5.2 (32-bit OS) \ KB2898850 Installed for .NET 4.5.1 or 4.5.2 |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + 1. TLS 1.2 - KB2898850 for .NET Framework 4.5.1 and 4.5.2 (64-bit OS)

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 - KB2898850 for .NET Framework 4.5.1 and 4.5.2 (64-bit OS) |
| Description |  |
| Supported Platforms | All Windows Vista (64-bit)  All Windows 7 (64-bit)  All Windows 8 (64-bit)  All Windows 8.1 (64-bit)  All Windows 10 (64-bit)  All Windows Server 2008 (non-R2)(64-bit)  All Windows Server 2008 R2 (64-bit)  All Windows Server 2012 (64-bit)  All Windows Server 2012 R2 (64-bit)  All Windows Server 2016 and higher (64-bit)  Windows Embedded 8.1 Industry (64-bit)  Windows Embedded 8 Industry (64-bit)  Windows Embedded 8 Standard (64-bit)  Embedded Windows 7 (64-bit)  All Windows Server 2019 and higher (64-bit) |
| Settings | KB2898850 Installed for .NET 4.5.1 or 4.5.2 (x64)  KB2898850 Installed for .NET 4.5.1 or 4.5.2 (x86) |
| Compliance Rules | KB2898850 Installed (x64) |

* + - 1. Settings
         1. KB2898850 Installed for .NET 4.5.1 or 4.5.2 (x64)

|  |  |
| --- | --- |
|  |  |
| Name | KB2898850 Installed for .NET 4.5.1 or 4.5.2 (x64) |
| Description |  |
| Setting Type | Script |
| Data type | .Boolean |
| Run scripts by using the logged on user credentials | . |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Language | Windows PowerShell |
| Discovery Script |  |
| Remediation Script | None |
| Compliance Rules | KB2898850 Installed (x64) |

* + - * 1. KB2898850 Installed for .NET 4.5.1 or 4.5.2 (x86)

|  |  |
| --- | --- |
|  |  |
| Name | KB2898850 Installed for .NET 4.5.1 or 4.5.2 (x86) |
| Description |  |
| Setting Type | Script |
| Data type | .Boolean |
| Run scripts by using the logged on user credentials | . |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Language | Windows PowerShell |
| Discovery Script |  |
| Remediation Script | None |
| Compliance Rules | KB2898850 Installed (x86) |

* + - 1. Compliance Rules
         1. KB2898850 Installed (x64)

|  |  |
| --- | --- |
|  |  |
| Name | KB2898850 Installed (x64) |
| Description | KB2898850 is required to enable TLS 1.2 support for .NET Framework 4.5.1 and 4.5.2. Download link: https://www.microsoft.com/en-us/download/details.aspx?id=42883 |
| Selected setting | TLS 1.2 - KB2898850 for .NET Framework 4.5.1 and 4.5.2 (64-bit OS) \ KB2898850 Installed for .NET 4.5.1 or 4.5.2 (x64) |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + - * 1. KB2898850 Installed (x86)

|  |  |
| --- | --- |
|  |  |
| Name | KB2898850 Installed (x86) |
| Description | KB2898850 is required to enable TLS 1.2 support for .NET Framework 4.5.1 and 4.5.2. Download link: https://www.microsoft.com/en-us/download/details.aspx?id=42883 |
| Selected setting | TLS 1.2 - KB2898850 for .NET Framework 4.5.1 and 4.5.2 (64-bit OS) \ KB2898850 Installed for .NET 4.5.1 or 4.5.2 (x86) |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + 1. TLS 1.2 - KB3140245 for WinHTTP Protocols

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 - KB3140245 for WinHTTP Protocols |
| Description | KB3140245 is required to enable TLS 1.1 and TLS 1.2 as default secure protocols for WinHTTP in Windows Server 2012, 2008 R2, and Windows 7 |
| Supported Platforms | All Windows 7 (32-bit)  All Windows 7 (64-bit)  All Windows Server 2008 R2 (64-bit)  All Windows Server 2012 (64-bit)  Embedded Windows 7 (32-bit)  Embedded Windows 7 (64-bit) |
| Settings | KB3140245 Installed |
| Compliance Rules | KB3140245 Installed |

* + - 1. Settings
         1. KB3140245 Installed

|  |  |
| --- | --- |
|  |  |
| Name | KB3140245 Installed |
| Description | KB3140245 is required to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows Server 2012, 2008 R2, and Windows 7 |
| Setting Type | Script |
| Data type | Boolean |
| Run scripts by using the logged on user credentials | . |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Language | Windows PowerShell |
| Discovery Script |  |
| Remediation Script | None |
| Compliance Rules | KB3140245 Installed |

* + - 1. Compliance Rules
         1. KB3140245 Installed

|  |  |
| --- | --- |
|  |  |
| Name | KB3140245 Installed |
| Description | KB3140245 is required to enable TLS 1.1 and TLS 1.2 as default secure protocols for WinHTTP in Windows Server 2012, 2008 R2, and Windows 7. See: <https://support.microsoft.com/en-us/help/3140245/update-to-enable-tls-1-1-and-tls-1-2-as-default-secure-protocols-in-wi> |
| Selected setting | TLS 1.2 - KB3140245 for WinHTTP Protocols \ KB3140245 Installed |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Critical |

* + 1. TLS 1.2 - KB3154518 for .NET Framework 3.5.1 (32-bit OS)

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 - KB3154518 for .NET Framework 3.5.1 (32-bit OS) |
| Description |  |
| Supported Platforms | All Windows 7 (32-bit)  Embedded Windows 7 (32-bit) |
| Settings | KB3154518 Installed for .NET Framework 3.5.1 |
| Compliance Rules | KB3154518 Installed |

* + - 1. Settings
         1. KB3154518 Installed for .NET Framework 3.5.1

|  |  |
| --- | --- |
|  |  |
| Name | KB3154518 Installed for .NET Framework 3.5.1 |
| Description |  |
| Setting Type | Script |
| Data type | Boolean |
| Run scripts by using the logged on user credentials | . |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Language | Windows PowerShell |
| Discovery Script |  |
| Remediation Script | None |
| Compliance Rules | KB3154518 Installed |

* + - 1. Compliance Rules
         1. KB3154518 Installed

|  |  |
| --- | --- |
|  |  |
| Name | KB3154518 Installed |
| Description | KB3154518 is required to enabled TLS 1.2 support for .NET Framework 3.5.1: <https://support.microsoft.com/en-us/help/3154518/support-for-tls-system-default-versions-included-in-the-net-framework> |
| Selected setting | TLS 1.2 - KB3154518 for .NET Framework 3.5.1 (32-bit OS) \ KB3154518 Installed for .NET Framework 3.5.1 |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + 1. TLS 1.2 - KB3154518 for .NET Framework 3.5.1 (64-bit OS)

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 - KB3154518 for .NET Framework 3.5.1 (64-bit OS) |
| Description |  |
| Supported Platforms | All Windows 7 (64-bit)  All Windows Server 2008 R2 (64-bit)  Embedded Windows 7 (64-bit) |
| Settings | KB3154518 Installed for .NET Framework 3.5.1 (x64)  KB3154518 Installed for .NET Framework 3.5.1 (x86) |
| Compliance Rules | KB3154518 Installed (x64)  KB3154518 Installed (x86) |

* + - 1. Settings
         1. KB3154518 Installed for .NET Framework 3.5.1 (x64)

|  |  |
| --- | --- |
|  |  |
| Name | KB3154518 Installed for .NET Framework 3.5.1 (x64) |
| Description |  |
| Setting Type | Script |
| Data type | Boolean |
| Run scripts by using the logged on user credentials | . |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Language | Windows PowerShell |
| Discovery Script |  |
| Remediation Script | None |
| Compliance Rules | KB3154518 Installed (x64) |

* + - * 1. KB3154518 Installed for .NET Framework 3.5.1 (x86)

|  |  |
| --- | --- |
|  |  |
| Name | KB3154518 Installed for .NET Framework 3.5.1 (x64) |
| Description |  |
| Setting Type | Script |
| Data type | Boolean |
| Run scripts by using the logged on user credentials | . |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Language | Windows PowerShell |
| Discovery Script |  |
| Remediation Script | None |
| Compliance Rules | KB3154518 Installed (x86) |

* + - 1. Compliance Rules
         1. KB3154518 Installed (x64)

|  |  |
| --- | --- |
|  |  |
| Name | KB3154518 Installed (x64) |
| Description | KB3154518 is required to enabled TLS 1.2 support for .NET Framework 3.5.1: <https://support.microsoft.com/en-us/help/3154518/support-for-tls-system-default-versions-included-in-the-net-framework> |
| Selected setting | TLS 1.2 - KB3154518 for .NET Framework 3.5.1 (64-bit OS) \ KB3154518 Installed for .NET Framework 3.5.1 (x64) |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + - * 1. KB3154518 Installed (x86)

|  |  |
| --- | --- |
|  |  |
| Name | KB3154518 Installed (x86) |
| Description | KB3154518 is required to enabled TLS 1.2 support for .NET Framework 3.5.1: <https://support.microsoft.com/en-us/help/3154518/support-for-tls-system-default-versions-included-in-the-net-framework> |
| Selected setting | TLS 1.2 - KB3154518 for .NET Framework 3.5.1 (64-bit OS) \ KB3154518 Installed for .NET Framework 3.5.1 (x86) |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + 1. TLS 1.2 - KB4019276 for Windows Server 2008 SP2

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 - KB4019276 for Windows Server 2008 SP2 |
| Description | KB4019276 is required to enable TLS 1.2 support in Windows Server 2008 SP2 |
| Supported Platforms | All Windows Server 2008 (Non-R2) (64-bit)  All Windows Server 2008 (32-bit) |
| Settings | KB4018276 Installed |
| Compliance Rules | KB4019276 Is Installed |

* + - 1. Settings
         1. KB4018276 Installed

|  |  |
| --- | --- |
|  |  |
| Name | KB4018276 Installed |
| Description | https://support.microsoft.com/en-us/help/4019276/update-to-add-support-for-tls-1-1-and-tls-1-2-in-windows |
| Setting Type | Script |
| Data type | Boolean |
| Run scripts by using the logged on user credentials | . |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Language | Windows PowerShell |
| Discovery Script |  |
| Remediation Script | None |
| Compliance Rules | KB4019276 Is Installed |

* + - 1. Compliance Rules
         1. KB4019276 Is Installed

|  |  |
| --- | --- |
|  |  |
| Name | KB4019276 Is Installed |
| Description | KB4019276 is required to enable TLS 1.2 support on Windows Server 2008 SP2. See: <https://support.microsoft.com/en-us/help/4019276/update-to-add-support-for-tls-1-1-and-tls-1-2-in-windows> |
| Selected setting | TLS 1.2 - KB4019276 for Windows Server 2008 SP2 \ KB4018276 Installed |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Critical |

* + 1. TLS 1.2 - KB4022720 for WSUS (Windows Server 2012 R2)

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 - KB4022720 for WSUS (Windows Server 2012 R2) |
| Description | Verifies KB4022720 or later has been installed to add TLS 1.2 support for WSUS. |
| Supported Platforms | All Windows Server 2012 R2 (64-bit) |
| Settings | WSUS Updated for TLS 1.2 Support |
| Compliance Rules | WSUS Updated to Support TLS 1.2 |

* + - 1. Settings
         1. WSUS Updated for TLS 1.2 Support

|  |  |
| --- | --- |
|  |  |
| Name | WSUS Updated for TLS 1.2 Support |
| Description |  |
| Setting Type | Script |
| Data type | Boolean |
| Run scripts by using the logged on user credentials | . |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Language | Windows PowerShell |
| Discovery Script |  |
| Remediation Script | None |
| Compliance Rules | WSUS Updated to Support TLS 1.2 |

* + - 1. Compliance Rules
         1. WSUS Updated to Support TLS 1.2

|  |  |
| --- | --- |
|  |  |
| Name | WSUS Updated to Support TLS 1.2 |
| Description | KB4022720 or later cumulative updates must be installed to enable TLS 1.2 support in WSUS on Windows Server 2012 R2. See KB4040243. |
| Selected setting | TLS 1.2 - KB4022720 for WSUS (Windows Server 2012 R2) \ WSUS Updated for TLS 1.2 Support |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Critical |

* + 1. TLS 1.2 - KB4022721 for WSUS (Windows Server 2012)

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 - KB4022721 for WSUS (Windows Server 2012) |
| Description | Verifies KB4022721 or later has been installed to add TLS 1.2 support for WSUS. |
| Supported Platforms | All Windows Server 2012 (64-bit) |
| Settings | WSUS Updated for TLS 1.2 Support |
| Compliance Rules | WSUS Updated to Support TLS 1.2 |

* + - 1. Settings
         1. WSUS Updated for TLS 1.2 Support

|  |  |
| --- | --- |
|  |  |
| Name | WSUS Updated for TLS 1.2 Support |
| Description |  |
| Setting Type | Script |
| Data type | Boolean |
| Run scripts by using the logged on user credentials | . |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Language | Windows PowerShell |
| Discovery Script |  |
| Remediation Script | None |
| Compliance Rules | WSUS Updated to Support TLS 1.2 |

* + - 1. Compliance Rules
         1. WSUS Updated to Support TLS 1.2

|  |  |
| --- | --- |
|  |  |
| Name | WSUS Updated to Support TLS 1.2 |
| Description | KB4022721 or later cumulative updates must be installed to enable TLS 1.2 support in WSUS on Windows Server 2012. See KB4040243. |
| Selected setting | TLS 1.2 - KB4022721 for WSUS (Windows Server 2012) \ WSUS Updated for TLS 1.2 Support |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Critical |

* + 1. TLS 1.2 - Operating System (Server)

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 - Operating System (Server) |
| Description |  |
| Supported Platforms | All Windows Server 2003  All Windows Server 2008  All Windows Server 2008 R2  All Windows Server 2012  All Windows Server 2012 R2  All Windows Server 2016  All Windows Server 2019 |
| Settings | BuildNumber |
| Compliance Rules | BuildNumber |

* + - 1. Settings
         1. BuildNumber

|  |  |
| --- | --- |
|  |  |
| Name | BuildNumber |
| Description | TLS 1.2 support is included in Windows Server 2008 and later server operating systems. Windows 7 and later workstation operating systems. See the whitepaper referenced in the TLS 1.2 support at Microsoft blog post: https://cloudblogs.microsoft.com/microsoftsecure/2017/06/20/tls-1-2-support-at-microsoft/ |
| Setting Type | WQL query |
| Data type | Integer |
| Namespace | root\cimv2 |
| Class | Win32\_OperatingSystem |
| Property | BuildNumber |
| WQL query WHERE clause |  |

* + - 1. Compliance Rules
         1. BuildNumber

|  |  |
| --- | --- |
|  |  |
| Name | BuildNumber |
| Description | TLS 1.2 support is included in Windows Server 2008 and later server operating systems. See the whitepaper referenced in the TLS 1.2 support at Microsoft blog post: https://cloudblogs.microsoft.com/microsoftsecure/2017/06/20/tls-1-2-support-at-microsoft/ |
| Selected setting | TLS 1.2 - Operating System (Server) \ BuildNumber |
| Rule type | Value |
| The setting must comply with the following rule | BuildNumber: **Greater than or equal to**  The following values: **6002** |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Critical |

* + 1. TLS 1.2 - Operating System (Workstation)

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 - Operating System (Server) |
| Description |  |
| Supported Platforms | All Windows XP  All Windows Vista  All Windows 7  All Windows 8  All Windows 8.1  All Windows 10  All Windows Embedded |
| Settings | BuildNumber |
| Compliance Rules | BuildNumber |

* + - 1. Settings
         1. BuildNumber

|  |  |
| --- | --- |
|  |  |
| Name | BuildNumber |
| Description | TLS 1.2 support is included in Windows Server 2008 and later server operating systems. Windows 7 and later workstation operating systems. See the whitepaper referenced in the TLS 1.2 support at Microsoft blog post: <https://cloudblogs.microsoft.com/microsoftsecure/2017/06/20/tls-1-2-support-at-microsoft/> |
| Setting Type | WQL query |
| Data type | Integer |
| Namespace | root\cimv2 |
| Class | Win32\_OperatingSystem |
| Property | BuildNumber |
| WQL query WHERE clause |  |

* + - 1. Compliance Rules
         1. BuildNumber

|  |  |
| --- | --- |
|  |  |
| Name | BuildNumber |
| Description | TLS 1.2 support is included in Windows Server 2008 and later server operating systems. See the whitepaper referenced in the TLS 1.2 support at Microsoft blog post: https://cloudblogs.microsoft.com/microsoftsecure/2017/06/20/tls-1-2-support-at-microsoft/ |
| Selected setting | TLS 1.2 - Operating System (Server) \ BuildNumber |
| Rule type | Value |
| The setting must comply with the following rule | BuildNumber: **Greater than or equal to**  The following values: **7600** |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Critical |

* + 1. TLS 1.2 - SCHANNEL Protocol - DisabledByDefault

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 - SCHANNEL Protocol - DisabledByDefault |
| Description |  |
| Supported Platforms | All Windows 7 (32-bit)  All Windows 7 (64-bit)  All Windows Server 2008 (Non-R2) (64-bit)  All Windows Server 2008 R2 (64-bit)  All Windows Server 2008 (32-bit)  All Embedded Windows 7 (64-bit)  All Embedded Windows 7 )32-bit) |
| Settings | Client\_DisabledByDefault  Server\_DisabledByDefault |
| Compliance Rules | TLS 1.2 Client – DisabledByDefault  TLS 1.2 Server - DisabledByDefault |

* + - 1. Settings
         1. Client\_DisabledByDefault

|  |  |
| --- | --- |
|  |  |
| Name | Client\_DisabledByDefault |
| Description |  |
| Setting Type | Registry value |
| Data type | Integer |
| Hive Name | HKEY\_LOCAL\_MACHINE |
| Key Name | SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client |
| Value Name | DisabledByDefault |
| The registry value is associated with a 64-bit application |  |
| Create the registry value as a REG\_DWORD data type if remediate for noncompliant rules |  |

* + - * 1. Server\_DisabledByDefault

|  |  |
| --- | --- |
|  |  |
| Name | Server\_DisabledByDefault |
| Description |  |
| Setting Type | Registry value |
| Data type | Integer |
| Hive Name | HKEY\_LOCAL\_MACHINE |
| Key Name | SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server |
| Value Name | DisabledByDefault |
| The registry value is associated with a 64-bit application |  |
| Create the registry value as a REG\_DWORD data type if remediate for noncompliant rules |  |

* + - 1. Compliance Rules
         1. TLS 1.2 Client – DisabledByDefault

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 Client - DisabledByDefault |
| Description | The DisbabledByDefault registry key must exist and be set to 0 to enable TLS 1.2 Server support on Windows Server 2008 R2 and Windows 7. See: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn786418(v=ws.11)#BKMK\_SchannelTR\_TLS12 |
| Selected setting | TLS 1.2 - SCHANNEL Protocol - DisabledByDefault \ Server\_DisabledByDefault |
| Rule type | Value |
| The setting must comply with the following rule | Client\_DisabledByDefault: **Equals**  The following values: **0** |
| Remediate noncompliant rules when supported |  |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + - * 1. TLS 1.2 Server - DisabledByDefault

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 Server - DisabledByDefault |
| Description | The DisbabledByDefault registry key must exist and be set to 0 to enable TLS 1.2 Server support on Windows Server 2008 R2 and Windows 7. See: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn786418(v=ws.11)#BKMK\_SchannelTR\_TLS12 |
| Selected setting | TLS 1.2 - SCHANNEL Protocol - DisabledByDefault \ Server\_DisabledByDefault |
| Rule type | Value |
| The setting must comply with the following rule | Server\_DisabledByDefault: **Equals**  The following values: **0** |
| Remediate noncompliant rules when supported |  |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Critical |

* + 1. TLS 1.2 - SCHANNEL Protocol - Enabled

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 - SCHANNEL Protocol - Enabled |
| Description |  |
| Supported Platforms | All Windows Vista (32-bit)  All Windows Vista (64-bit)  All Windows 7 (32-bit)  All Windows 7 (64-bit)  All Windows 8 (32-bit)  All Windows 8 (64-bit)  All Windows 8.1 (32-bit)  All Windows 8.1 (64-bit)  All Windows Server 2008 (Non-R2) (64-bit)  All Windows Server 2008 R2 (64-bit)  All Windows Server 2008 (32-bit)  All Windows Server 2012 (64-bit)  All Windows Server 2012 R2 (64-bit)  Windows Embedded 8.1 Industry (32-bit)  Windows Embedded 8.1 Industry (64-bit)  Windows Embedded 8 Industry (32-bit)  Windows Embedded 8 Industry (64-bit)  Windows Embedded 8 Standard (32-bit)  Windows Embedded 8 Standard (64-bit)  Embedded Windows 7 (64-bit)  Embedded Windows 7 (32-bit) |
| Settings | Client\_Enabled  Server\_Enabled |
| Compliance Rules | TLS 1.2 Client – Enabled  TLS 1.2 Server - Enabled |

* + - 1. Settings
         1. Client\_Enabled

|  |  |
| --- | --- |
|  |  |
| Name | Client\_Enabled |
| Description |  |
| Setting Type | Registry value |
| Data type | Integer |
| Hive Name | HKEY\_LOCAL\_MACHINE |
| Key Name | SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client |
| Value Name | Enabled |
| The registry value is associated with a 64-bit application |  |
| Create the registry value as a REG\_DWORD data type if remediate for noncompliant rules |  |

* + - * 1. Server\_Enabled

|  |  |
| --- | --- |
|  |  |
| Name | Server\_Enabled |
| Description |  |
| Setting Type | Registry value |
| Data type | Integer |
| Hive Name | HKEY\_LOCAL\_MACHINE |
| Key Name | SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server |
| Value Name | Enabled |
| The registry value is associated with a 64-bit application |  |
| Create the registry value as a REG\_DWORD data type if remediate for noncompliant rules |  |

* + - 1. Compliance Rules
         1. TLS 1.2 Client - Enabled

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 Client - Enabled |
| Description | This registry key must exist and be set to1 to enable TLS 1.2 Client support. See: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn786418(v=ws.11)#BKMK\_SchannelTR\_TLS12 |
| Selected setting | TLS 1.2 - SCHANNEL Protocol - Enabled \ Client\_Enabled |
| Rule type | Value |
| The setting must comply with the following rule | Server\_Enabled: **Equals**  The following values: **1** |
| Remediate noncompliant rules when supported |  |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + - * 1. TLS 1.2 Server - Enabled

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 Server - Enabled |
| Description | This registry key must exist and be set to1 to enable TLS 1.2 Server support. See: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn786418(v=ws.11)#BKMK\_SchannelTR\_TLS12 |
| Selected setting | TLS 1.2 - SCHANNEL Protocol - Enabled \ Server\_Enabled |
| Rule type | Value |
| The setting must comply with the following rule | Server\_Enabled: **Equals**  The following values: **1** |
| Remediate noncompliant rules when supported |  |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Critical |

* + 1. TLS 1.2 - SQL Server Native Client (32-bit OS)

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 - SQL Server Native Client (32-bit OS) |
| Description |  |
| Supported Platforms | All Windows Vista (32-bit)  All Windows 7 (32-bit)  All Windows 8 (32-bit)  All Windows 8.1 (32-bit)  All Windows Server 2008 (32-bit)  Windows Embedded 8.1 Industry (32-bit)  Windows Embedded 8 Industry (32-bit)  Windows Embedded 8 Standard (32-bit)  Embedded Windows 7 (32-bit) |
| Settings | Client\_Enabled  Server\_Enabled |
| Compliance Rules | TLS 1.2 Client – Enabled  TLS 1.2 Server - Enabled |

* + - 1. Settings
         1. SQL Server 2008 Native Client

|  |  |
| --- | --- |
|  |  |
| Name | SQL Server 2008 Native Client |
| Description |  |
| Setting Type | Script |
| Data type | Boolean |
| Run scripts by using the logged on user credentials |  |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Type | Windows PowerShell |
| Discovery Script |  |
| Remediation Script | None |
| Compliance Rules | SQL Server 2008 Native Client Updated |

* + - * 1. SQL Server 2008 R2 Native Client

|  |  |
| --- | --- |
|  |  |
| Name | SQL Server 2008 R2 Native Client |
| Description |  |
| Setting Type | Script |
| Data type | Boolean |
| Run scripts by using the logged on user credentials |  |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Type | Windows PowerShell |
| Discovery Script |  |
| Remediation script | None |
| Compliance Rules | SQL Server 2008 R2 Native Client Updated |

* + - * 1. SQL Server 2012 Native Client

|  |  |
| --- | --- |
|  |  |
| Name | SQL Server 2012 Native Client |
| Description |  |
| Setting Type | File system |
| Type | File |
| Path | C:\Windows\System32 |
| File or folder name | sqlncli11.dll |
| Include subfolders |  |
| This file or folder is associated with a 64-bit application |  |
| Compliance Rules | sqlncli11.dll File Version |

* + - 1. Compliance Rules
         1. SQL Server 2008 Native Client Updated

|  |  |
| --- | --- |
|  |  |
| Name | SQL Server 2008 Native Client Updated |
| Description | The SQL Server 2008 Native Client must be updated to support TLS 1.2. See: https://support.microsoft.com/en-us/help/3135244/tls-1.2-support-for-microsoft-sql-server |
| Selected setting | TLS 1.2 - SQL Server Native Client (32-bit OS) \ SQL Server 2008 Native Client |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Critical |

* + - * 1. SQL Server 2008 R2 Native Client Updated

|  |  |
| --- | --- |
|  |  |
| Name | SQL Server 2008 R2 Native Client Updated |
| Description | The SQL Server 2008 R2 Native Client must be updated to support TLS 1.2. See: https://support.microsoft.com/en-us/help/3135244/tls-1.2-support-for-microsoft-sql-server |
| Selected setting | TLS 1.2 - SQL Server Native Client (32-bit OS) \ SQL Server 2008 R2 Native Client |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Critical |

* + - * 1. sqlncli11.dll File Version

|  |  |
| --- | --- |
|  |  |
| Name | sqlncli11.dll File Version |
| Description | The SQL Server 2012 Native Client must be updated to support TLS 1.2. See: https://support.microsoft.com/en-us/help/3135244/tls-1.2-support-for-microsoft-sql-server |
| Selected setting | TLS 1.2 - SQL Server Native Client (32-bit OS) \ SQL Server 2012 Native Client |
| Rule type | Value |
| Property | File Version |
| The setting must comply with the following rule | SQL Server 2012 Native Client: **Greater than or equal to**  The following values: **2011.110.7000.00** |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Critical |

* + 1. TLS 1.2 - SQL Server Native Client (64-bit OS)

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 - SQL Server Native Client (64-bit OS) |
| Description |  |
| Supported Platforms | All Windows Vista (64-bit)  All Windows 7 (64-bit)  All Windows 8 (64-bit)  All Windows 8.1 (64-bit)  All Windows Server 2008 (Non-R2) (64-bit)  All Windows Server 2008 R2 (64-bit)  All Windows Server 2012 (64-bit)  All Windows Server 2012 R2 (64-bit)  All Windows Server 2016 and higher (64-bit)  All Windows Server 2019 and higher (64-bit)  Windows Embedded 8.1 Industry (64-bit)  Windows Embedded 8 Industry (64-bit)  Windows Embedded 8 Standard (64-bit)  Embedded Windows 7 (64-bit) |
| Settings | SQL Server 2008 Native Client (x64)  SQL Server 2008 Native Client (x86)  SQL Server 2008 R2 Native Client (x64)  SQL Server 2008 R2 Native Client (x86)  SQL Server 2012 Native Client (x64)  SQL Server 2012 Native Client (x86) |
| Compliance Rules | SQL Server 2008 Native Client Updated (x64)  SQL Server 2008 Native Client Updated (x86)  SQL Server Native Client 2008 R2 Updated (x64)  SQL Server Native Client 2008 R2 Updated (x86)  sqlncli11.dll (x64)  sqlncli11.dll (x86) |

* + - 1. Settings
         1. SQL Server 2008 Native Client (x64)

|  |  |
| --- | --- |
|  |  |
| Name | SQL Server 2008 Native Client (x64) |
| Description |  |
| Setting Type | Script |
| Data type | Boolean |
| Run scripts by using the logged on user credentials |  |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Type | Windows PowerShell |
| Discovery Script |  |
| Remediation Script | None |
| Compliance Rules | SQL Server 2008 Native Client Updated (x64) |

* + - * 1. SQL Server 2008 Native Client (x86)

|  |  |
| --- | --- |
|  |  |
| Name | SQL Server 2008 Native Client (x86) |
| Description |  |
| Setting Type | Script |
| Data type | Boolean |
| Run scripts by using the logged on user credentials |  |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Type | Windows PowerShell |
| Discovery Script |  |
| Remediation Script | None |
| Compliance Rules | SQL Server 2008 Native Client Updated (x64) |

* + - * 1. SQL Server 2008 R2 Native Client (x64)

|  |  |
| --- | --- |
|  |  |
| Name | SQL Server 2008 R2 Native Client (x64) |
| Description |  |
| Setting Type | Script |
| Data type | Boolean |
| Run scripts by using the logged on user credentials |  |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Type | Windows PowerShell |
| Discovery Script |  |
| Remediation script | None |
| Compliance Rules | SQL Server Native Client 2008 R2 Updated (x64) |

* + - * 1. SQL Server 2008 R2 Native Client (x86)

|  |  |
| --- | --- |
|  |  |
| Name | SQL Server 2008 R2 Native Client (x86) |
| Description |  |
| Setting Type | Script |
| Data type | Boolean |
| Run scripts by using the logged on user credentials |  |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Type | Windows PowerShell |
| Discovery Script |  |
| Remediation script | None |
| Compliance Rules | SQL Server Native Client 2008 R2 Updated (x86) |

* + - * 1. SQL Server 2012 Native Client (x64)

|  |  |
| --- | --- |
|  |  |
| Name | SQL Server 2012 Native Client (x64) |
| Description |  |
| Setting Type | File system |
| Type | File |
| Path | C:\Windows\System32 |
| File or folder name | sqlncli11.dll |
| Include subfolders |  |
| This file or folder is associated with a 64-bit application |  |
| Compliance Rules | sqlncli11.dll (x64) |

* + - * 1. SQL Server 2012 Native Client (x86)

|  |  |
| --- | --- |
|  |  |
| Name | SQL Server 2012 Native Client (x86) |
| Description |  |
| Setting Type | File system |
| Type | File |
| Path | C:\Windows\System32 |
| File or folder name | sqlncli11.dll |
| Include subfolders |  |
| This file or folder is associated with a 64-bit application |  |
| Compliance Rules | sqlncli11.dll (x86) |

* + - 1. Compliance Rules
         1. SQL Server 2008 Native Client Updated (x64)

|  |  |
| --- | --- |
|  |  |
| Name | SQL Server 2008 Native Client Updated (x64) |
| Description | The SQL Server 2008 Native Client must be updated to support TLS 1.2. See: https://support.microsoft.com/en-us/help/3135244/tls-1.2-support-for-microsoft-sql-server |
| Selected setting | TLS 1.2 - SQL Server Native Client (64-bit OS) \ SQL Server 2008 Native Client (x64) |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Critical |

* + - * 1. SQL Server 2008 Native Client Updated (x86)

|  |  |
| --- | --- |
|  |  |
| Name | SQL Server 2008 Native Client Updated (x86) |
| Description | The SQL Server 2008 Native Client must be updated to support TLS 1.2. See: https://support.microsoft.com/en-us/help/3135244/tls-1.2-support-for-microsoft-sql-server |
| Selected setting | TLS 1.2 - SQL Server Native Client (64-bit OS) \ SQL Server 2008 Native Client (x86) |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Critical |

* + - * 1. SQL Server Native Client 2008 R2 Updated (x64)

|  |  |
| --- | --- |
|  |  |
| Name | SQL Server Native Client 2008 R2 Updated (x64) |
| Description | The SQL Server 2008 R2 Native Client must be updated to support TLS 1.2. See: https://support.microsoft.com/en-us/help/3135244/tls-1.2-support-for-microsoft-sql-server |
| Selected setting | TLS 1.2 - SQL Server Native Client (64-bit OS) \ SQL Server 2008 R2 Native Client (x64) |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Critical |

* + - * 1. SQL Server Native Client 2008 R2 Updated (x86)

|  |  |
| --- | --- |
|  |  |
| Name | SQL Server Native Client 2008 R2 Updated (x86) |
| Description | The SQL Server 2008 R2 Native Client must be updated to support TLS 1.2. See: https://support.microsoft.com/en-us/help/3135244/tls-1.2-support-for-microsoft-sql-server |
| Selected setting | TLS 1.2 - SQL Server Native Client (64-bit OS) \ SQL Server 2008 R2 Native Client (x86) |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Critical |

* + - * 1. sqlncli11.dll (x64)

|  |  |
| --- | --- |
|  |  |
| Name | sqlncli11.dll (x64) |
| Description | The SQL Server 2012 Native Client must be updated to support TLS 1.2. See: https://support.microsoft.com/en-us/help/3135244/tls-1.2-support-for-microsoft-sql-server |
| Selected setting | TLS 1.2 - SQL Server Native Client (64-bit OS) \ SQL Server 2012 Native Client (x64) |
| Rule type | Value |
| Property | File Version |
| The setting must comply with the following rule | SQL Server 2012 Native Client: **Greater than or equal to**  The following values: **2011.110.7000.00** |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Critical |

* + - * 1. sqlncli11.dll (x86)

|  |  |
| --- | --- |
|  |  |
| Name | sqlncli11.dll (x86) |
| Description | The SQL Server 2012 Native Client must be updated to support TLS 1.2. See: https://support.microsoft.com/en-us/help/3135244/tls-1.2-support-for-microsoft-sql-server |
| Selected setting | TLS 1.2 - SQL Server Native Client (64-bit OS) \ SQL Server 2012 Native Client (x86) |
| Rule type | Value |
| Property | File Version |
| The setting must comply with the following rule | SQL Server 2012 Native Client: **Greater than or equal to**  The following values: **2011.110.7000.00** |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Critical |

* + 1. TLS 1.2 - WinHTTP Default Secure Protocols (32-bit OS)

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 - WinHTTP Default Secure Protocols (32-bit OS) |
| Description | See KB3140245 |
| Supported Platforms | All Windows 7 (32-bit)  All Windows 8 (32-bit)  All Windows 8.1 (32-bit)  Embedded Windows 7 (32-bit) |
| Settings | WinHTTP DefaultSecurityProtocol |
| Compliance Rules | WinHTTP DefaultSecureProtocols Includes TLS 1.2 |

* + - 1. Settings
         1. WinHTTP DefaultSecurityProtocol

|  |  |
| --- | --- |
|  |  |
| Name | WinHTTP DefaultSecurityProtocol |
| Description |  |
| Setting Type | Script |
| Data type | Boolean |
| Run scripts by using the logged on user credentials |  |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Type | Windows PowerShell |
| Discovery Script |  |
| Remediation Script Language | Windows PowerShell |
| Remediation Script |  |
| Compliance Rules | WinHTTP DefaultSecureProtocols Includes TLS 1.2 |

* + - 1. Compliance Rules
         1. WinHTTP DefaultSecureProtocols Includes TLS 1.2

|  |  |
| --- | --- |
|  |  |
| Name | WinHTTP DefaultSecureProtocols Includes TLS 1.2 |
| Description | See KB3140245. Dword values of 2048 or later include the TLS 1.2 protocol. The remediation script sets the value to 2688, which enables TLS 1.0, TLS 1.1, and TLS 1.2 by default for compatibility. |
| Selected setting | TLS 1.2 - WinHTTP Default Secure Protocols (32-bit OS) \ WinHTTP DefaultSecurityProtocol |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Run the specified remediation script when this setting is noncompliant |  |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + 1. TLS 1.2 - WinHTTP Default Secure Protocols (64-bit OS)

|  |  |
| --- | --- |
|  |  |
| Name | TLS 1.2 - WinHTTP Default Secure Protocols (64-bit OS) |
| Description | See KB3140245 |
| Supported Platforms | All Windows 7 (64-bit)  All Windows 8 (64-bit)  All Windows 8.1 (64-bit)  All Windows Server 2008 R2 (64-bit)  All Windows Server 2012 (64-bit)  All Windows Server 2012 R2 (64-bit)  Embedded Windows 7 (64-bit) |
| Settings | WinHTTP DefaultSecureProtocols (x64)  WinHTTP DefaultSecureProtocols (x86) |
| Compliance Rules | WinHTTP DefaultSecureProtocol Includes TLS 1.2 (x64)  WinHTTP DefaultSecureProtocols Includes TLS 1.2 (x86) |

* + - 1. Settings
         1. WinHTTP DefaultSecureProtocols (x64)

|  |  |
| --- | --- |
|  |  |
| Name | WinHTTP DefaultSecureProtocols (x64) |
| Description |  |
| Setting Type | Script |
| Data type | Boolean |
| Run scripts by using the logged on user credentials |  |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Type | Windows PowerShell |
| Discovery Script |  |
| Remediation Script Language | Windows PowerShell |
| Remediation Script |  |
| Compliance Rules | WinHTTP DefaultSecureProtocol Includes TLS 1.2 (x64) |

* + - * 1. WinHTTP DefaultSecureProtocols (x86)

|  |  |
| --- | --- |
|  |  |
| Name | WinHTTP DefaultSecureProtocols (x86) |
| Description |  |
| Setting Type | Script |
| Data type | Boolean |
| Run scripts by using the logged on user credentials |  |
| Run scripts by using the 32-bit scripting host on 64-bit devices |  |
| Discovery Script Type | Windows PowerShell |
| Discovery Script |  |
| Remediation Script Language | Windows PowerShell |
| Remediation Script |  |
| Compliance Rules | WinHTTP DefaultSecureProtocols Includes TLS 1.2 (x86) |

* + - 1. Compliance Rules
         1. WinHTTP DefaultSecureProtocol Includes TLS 1.2 (x64)

|  |  |
| --- | --- |
|  |  |
| Name | WinHTTP DefaultSecureProtocol Includes TLS 1.2 (x64) |
| Description | See KB3140245. Dword values of 2048 or later include the TLS 1.2 protocol. The remediation script sets the value to 2688, which enables TLS 1.0, TLS 1.1, and TLS 1.2 by default for compatibility. |
| Selected setting | TLS 1.2 - WinHTTP Default Secure Protocols (64-bit OS) \ WinHTTP DefaultSecureProtocols (x64) |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Run the specified remediation script when this setting is noncompliant |  |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

* + - * 1. WinHTTP DefaultSecureProtocols Includes TLS 1.2 (x86)

|  |  |
| --- | --- |
|  |  |
| Name | WinHTTP DefaultSecureProtocols Includes TLS 1.2 (x86) |
| Description | See KB3140245. Dword values of 2048 or later include the TLS 1.2 protocol. The remediation script sets the value to 2688, which enables TLS 1.0, TLS 1.1, and TLS 1.2 by default for compatibility. |
| Selected setting | TLS 1.2 - WinHTTP Default Secure Protocols (64-bit OS) \ WinHTTP DefaultSecureProtocols (x86) |
| Rule type | Value |
| The setting must comply with the following rule | The value returned by the specified script: **Equals**  The following values: **True** |
| Run the specified remediation script when this setting is noncompliant |  |
| Report noncompliance if this setting instance is not found |  |
| Noncompliance severity for reports | Warning |

1. References

|  |
| --- |
|  |
| [How to enable TLS 1.2 for Configuration Manager](https://support.microsoft.com/en-us/help/4040243/how-to-enable-tls-1-2-for-configuration-manager) |
| [TLS 1.2 support for Microsoft SQL Server](https://support.microsoft.com/en-us/help/3135244/tls-1-2-support-for-microsoft-sql-server) |
| [Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows](https://support.microsoft.com/en-us/help/3140245/update-to-enable-tls-1-1-and-tls-1-2-as-default-secure-protocols-in-wi) |
| [TLS/SSL Settings](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn786418(v=ws.11)#tls-12) |
| [TLS 1.2 support at Microsoft](https://cloudblogs.microsoft.com/microsoftsecure/2017/06/20/tls-1-2-support-at-microsoft/) |
| [KB4019276: Update to add support for TLS 1.1 and TLS 1.2 in Windows Server 2008 SP1, Windows Embedded POSReady 2009, and Windows Embedded Standard 2009](https://support.microsoft.com/en-us/help/4019276/update-to-add-support-for-tls-1-1-and-tls-1-2-in-windows) |
| [KB3154518: Support for TLS System Default Versions included in the .NET Framework 3.5.1 on Windows 7 SP1 and Server 2008 R2 SP1](https://support.microsoft.com/en-us/help/3154518/support-for-tls-system-default-versions-included-in-the-net-framework) |
| [KB3140245: Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows](https://support.microsoft.com/en-us/help/3140245/update-to-enable-tls-1-1-and-tls-1-2-as-default-secure-protocols-in-wi) |
| [KB2898850: Description of the security update for the .NET Framework 4.5.1 and the .NET Framework 4.5.2 on Windows 8.1, Windows RT 8.2, and Windows Server 2012 R2](https://support.microsoft.com/en-us/help/2898850/description-of-the-security-update-for-the-net-framework-4-5-1-and-the) |
| [IE11 Automatically Males Over 40% of the Web More Secure While Making Sure Sites Continue to Work](https://blogs.msdn.microsoft.com/ie/2013/11/12/ie11-automatically-makes-over-40-of-the-web-more-secure-while-making-sure-sites-continue-to-work/) |