

Understand the Requirements for AnyConnect Roaming Module for Versions Earlier than 4.8 MR2 and AD Connector

Contents

[Introduction](#)

[Background Information](#)

[AnyConnect Roaming Module](#)

[Windows Roaming Client or AnyConnect Module](#)

[Technical Details](#)

[Option A: schusestrongcrypto](#)

[Option B: SystemDefaultTlsVersions](#)

[Active Directory Connector](#)

Introduction

This document describes the requirements for using AnyConnect roaming module earlier than version 4.8 MR2 and AD Connector.

Background Information

As of January 27th, 2021, all clients must use TLS 1.2+ to connect to the Umbrella cloud for sync, registration, and updates. Clients with earlier versions need to make manual adjustments in order to continue to use the Umbrella clients without updating.

AnyConnect Roaming Module

Windows Roaming Client or AnyConnect Module

Endpoint Agent Version: Standalone Umbrella roaming clients only support the current version. Older versions are not supported. This version supports TLS 1.2 natively with .NET 4.6.2+.

Both of these requirements must be met:

1. A: Client Version
 - Cisco AnyConnect with Umbrella roaming module: Version 4.8.02042+ ([link](#))
or
 - Cisco AnyConnect 4.3 MR4+ plus configure TLS 1.2 use with changes to the Windows Registry to expand TLS support to include TLS 1.2:
2. B: .NET Framework Version
 - Microsoft .NET Framework Version: .NET 4.6.2
or
 - older .NET versions in accordance with registry key requirements

Windows Version: 7, 8, 8.1, 10



Note: For MacOS Roaming Client or AnyConnect Module, there is no change in system requirements for TLS 1.2 support.

For those that do not meet these requirements, please continue reading.

Technical Details

Verify if any older .NET versions are installed, and apply the registry keys as per the Microsoft article.

Steps required for older client versions earlier than AnyConnect 4.8 MR2 from 2):

Option A: schusestrongcrypto

This solution explicitly sets the supported secure protocols to the set of TLS 1.0, TLS 1.1, and TLS 1.2 rather than rely on .NET call defaults.

Here is a step-by-step guide:

1. Verify which [.NET Framework version](#) is installed on the Windows machine.

2. If only .NET version 4.6.2 (or later) is installed, the latest .NET Framework requires you to toggle **with stronger cipher**. Use these registry keys:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
"SchUseStrongCrypto"=dword:00000001
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319]
"SchUseStrongCrypto"=dword:00000001
```

A PowerShell script is provided as an example for making these changes via SCCM/CLI. This script is provided as is.

```
# set strong cryptography on 64 bit .Net Framework (version 4 and above)
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319' -Name 'SchUseStrongCrypto' -Value 1
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319' -Name 'SystemDefaultTlsVersions' -Value 1

# set strong cryptography on 32 bit .Net Framework (version 4 and above)
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\.NetFramework\v4.0.30319' -Name 'SchUseStrongCrypto' -Value 1
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\.NetFramework\v4.0.30319' -Name 'SystemDefaultTlsVersions' -Value 1
```

Option B: SystemDefaultTlsVersions

For older .NET versions, this option is required for older clients. For .NET 4.6.2+, this is an equivalent alternative to schusestrongcrypto; both solutions are required.

This solution defers TLS version choice to the OS rather than determining it within .NET. Allows legacy calls to use system supported versions. In most cases, this includes TLS 1.2.

1. .NET 4.5.1, 4.5.2: Requires <https://support.microsoft.com/kb/3156421>
2. .NET 3.5 SP1 on Windows 7: Requires <https://support.microsoft.com/kb/3154518>
3. .NET 3.5 SP1 on Windows 8.1: Requires <https://support.microsoft.com/kb/3154520>
4. .NET 4.6.2+: No additional requirements

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v2.0.50727]
"SystemDefaultTlsVersions"=dword:00000001
```

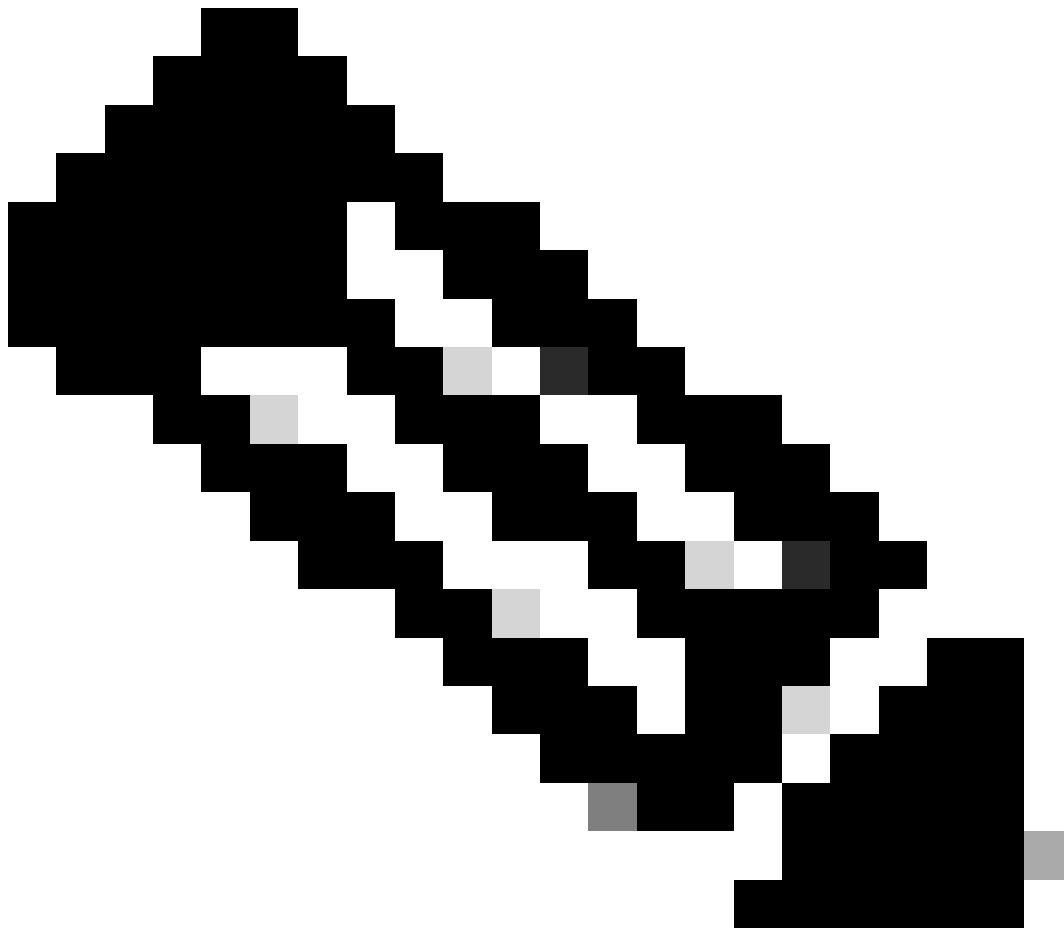
```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727]
"SystemDefaultTlsVersions"=dword:00000001
```

Active Directory Connector

Platforms supported: Windows Server 2012 and later.

If your Connector runs on Windows Server 2012 or later and runs .NET version 4.x, the Connector must use

TLS 1.2 by default when communicating with Umbrella.



Note: Support for connectors running Windows Server 2008 and 2008 R2 has been discontinued, since Microsoft has announced End of support for these versions in Jan 2020. You need to upgrade to a supported Windows Server version to continue running the Connector. If you cannot upgrade the Windows Server version, ensure to install .NET version 4.5 on this system in order to enable the connector to use TLS 1.2 to communicate with Umbrella.
