How to view and change the Windows Registry Settings for the SSL/TLS Protocols on a Windows Host

This article explains what plugins show the SSL/TLS Protocols may appear on a Windows Host. This also explains how to update the settings.

Dec 29, 2020 · How To

APPLIES TO
Nessus

OPERATING SYSTEM(S)
Windows 7/8/10;Windows Server 2008/2012/2016

ARTICLE NUMBER
000002733

TITLE
How to view and change the Windows Registry Settings for the SSL/TLS Protocols on a Windows Host

DESCRIPTION

Tenable scans may reveal what SSL/TLS settings are used on a particular host. These plugins include:

- Plugin 21643 (https://www.tenable.com/plugins/nessus/21643) SSL Cipher Suites Supported
- Plugin 131290 (https://www.tenable.com/plugins/nessus/131290) SSL/TLS Deprecated Ciphers
- Plugin 20007 (https://www.tenable.com/plugins/nessus/20007) SSL Version 2 and 3 Protocol Detection
- Plugin 56984 (https://www.tenable.com/plugins/nessus/56984) SSL / TLS Versions Supported
- Plugin 104743 (https://www.tenable.com/plugins/nessus/104743) TLS Version 1.0 Protocol Detection
- Plugin 121010 (https://www.tenable.com/plugins/nessus/121010) TLS Version 1.1 Protocol Detection
- Plugin 136318 (https://www.tenable.com/plugins/nessus/136318) TLS Version 1.2 Protocol Detection
- Plugin 138330 (https://www.tenable.com/plugins/nessus/138330) TLS Version 1.3 Protocol Detection

The following registry entry handles Microsoft Windows controlled SSL/TLS protocols:

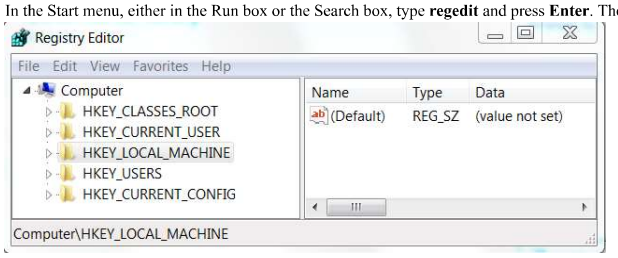
```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
```

Please consult your System Administrators prior to making any changes to the registry, and use caution when viewing or changing the Windows Registry Settings.

STEPS

How to identify if an SSL/TLS protocol is enabled/disabled

1. Click Start or press the **Windows** key.
2. In the Start menu, either in the Run box or the Search box, type **regedit** and press **Enter**. The **Registry Editor** window should open and look similar to the example shown below.



3. Navigate to follow the registry path:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
```

4. Check each SSL/TLS version for both server and client.
   - If the **DisabledByDefault** value is **0** or the value is missing, the protocol is **enabled**.
   - If the **DisabledByDefault** value is **1**, the protocol is **disabled**.

   WARNING: Before making any changes, create a backup of the registry.

Backing Up the Windows Registry Keys

1. In the Windows Registry Editor, locate and click the Protocols registry key or subkey that needs to be backed up.
2. Click **File**, then **Export**.

3. In the Export Registry File dialog box, select the filename and location of where to save the backup.
4. Click **Save**.

How to Disable Weak Protocols in the Windows Registry

The SSL/TLS Protocols are listed under the Protocols Key. If there are no SSL/TLS subkeys under the Protocols key, the system may be vulnerable to a weak protocol. The SSL/TLS Windows Registry Settings can be changed for the following Protocols:

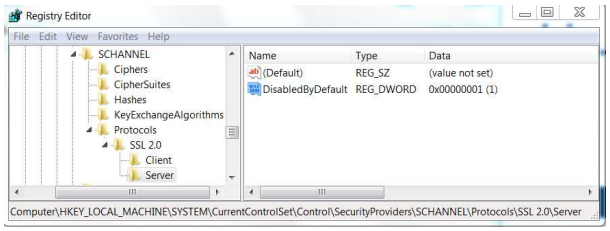
- PCT v1.0
- SSL v2.0
- SSL v3.0
- TLS v1.0
- TLS v1.1
- TLS v1.2

Note: This will not affect third-party applications that are installed unless the application was designed to adhere to this standard. This applies more for SMB and RDP which are built-in native protocols to Windows.
Note: PCT v1.0 is disabled by default on Windows Server Operating Systems. SSL v2.0 is disabled by default on Windows Server 2016 and later.

1. Navigate to follow the registry path:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
```

2. Create or edit the **DWORD DisabledByDefault** Value data to 1**.** Verify the **Base** is set to **Hexadecimal** for the following registry keys under the Protocols key for both **Client** and **Server** subkeys.
   - SCHANNEL\Protocols\SSL 2.0\Client
   - SCHANNEL\Protocols\SSL 2.0\Server
   - SCHANNEL\Protocols\TLS 1.0\Client
   - SCHANNEL\Protocols\TLS 1.0\Server



3. Restart the host to ensure the new settings take effect on the services.

ADDITIONAL RESOURCES

Tenable.sc (/s/topic/0TOf2000000HPDaGAO/ten…) | Nessus (/s/topic/0TOf2000000HPDVGA4/nes…) | Tenable.io (/s/topic/0TOf2000000HPDXGA4/ten…) | Configuration (/s/topic/0TOf2000000HPDIGA4/conf…) | Tenable.ot (/s/topic/0TO3a000000EGIVGA4/tena…) | Lumin (/s/topic/0TO3a000000EGIQGA4/lumin)

Helpful?

Yes | Somewhat | No

How can we improve it?

Submit

This is a survey preview. Responses will not be saved.

We're having trouble saving. You can continue taking this survey but remember to submit your answers at the end.

Not finding your answer?
Ask our community of users and experts.

ASK A QUESTION

RELATED ARTICLES

How to check the SSL/TLS Cipher Suites in Linux and Windows (/s/article/How-to-check-the-SSL-TLS-Cipher-Suites-in-Linux-and-Windows) 122.58K

About SSL/TLS alerts in the System Event Log on Windows targets (/s/article/About-SSL-TLS-alerts-in-the-System-Event-Log-on-Windows-targets) 15.75K

How to verify if the Target is using a particular SSL/TLS protocol (/s/article/How-to-verify-if-the-Target-is-using-a-particular-SSL-TLS-protocol) 11.97K

Troubleshooting Credential scanning on Windows (/s/article/Troubleshooting-Credential-scanning-on-Windows) 180.78K

Export a Windows Certificate with the Private Key (/s/article/Export-a-Windows-Certificate-with-the-Private-Key) 104.28K

All Topics

ASSET SCANNING & MONITORING (/S/TOPIC/0TOF2000000HPDGGA4/ASSET-SCANNING-MONITORING)
AUDIT & COMPLIANCE (/S/TOPIC/0TOF2000000HPDHGA4/AUDIT-COMPLIANCE)
CONFIGURATION (/S/TOPIC/0TOF2000000HPDIGA4/CONFIGURATION)
INSTALL & ORCHESTRATION (/S/TOPIC/0TOF2000000HPDJGA4/INSTALL-ORCHESTRATION)
INTEGRATION (/S/TOPIC/0TOF2000000HPDKGA4/INTEGRATION)
LICENSING (/S/TOPIC/0TOF2000000HPDLGA4/LICENSING)
PLUGINS (/S/TOPIC/0TOF2000000HPDMGA4/PLUGINS)
REPORTS, DASHBOARDS & TEMPLATES (/S/TOPIC/0TOF2000000HPDNGA4/REPORTS-DASHBOARDS-TEMPLATES)
Q&A (/S/TOPIC/0TOF2000000HPFBGAO/QA)

TRENDING ARTICLES

How to check the SSL/TLS Cipher Suites in Linux and Windows
(/s/article/How-to-check-the-SSL-TLS-Cipher-Suites-in-Linux-and-Windows)

Troubleshooting Credential scanning on Windows
(/s/article/Troubleshooting-Credential-scanning-on-Windows)

Plugins associated with CVE-2021-44228 (Log4Shell)
(/s/article/Plugins-associated-with-CVE-2021-44228-Log4Shell)

Useful plugins to troubleshoot credential scans
(/s/article/Useful-plugins-to-troubleshoot-credential-scans)

What ports are required for Tenable products?
(/s/article/What-ports-are-required-for-Tenable-products)

Phone
Toll Free US : +1-855-267-7044
US Direct : +1-443-545-2104
UK : +44-800-098-8086
Australia : 1800-875-306 (+61-18-0087-5306)
Japan : 0120 963 622 (+81-120-963-622)