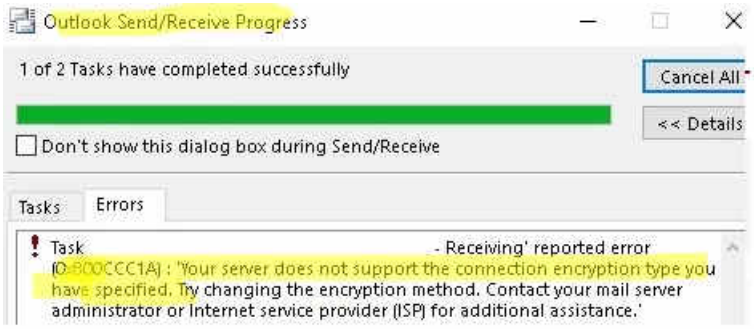
Outlook: Your Server Does Not Support the Connection Encryption Type

https://woshub.com/outlook-server-not-support-connection-encryption-type/

In legacy Windows versions (Windows 7/XP or Windows Server 2008R2/2003) with Outlook 2010/2013/2016/2019, you may see the following error when trying to connect to a mail server:

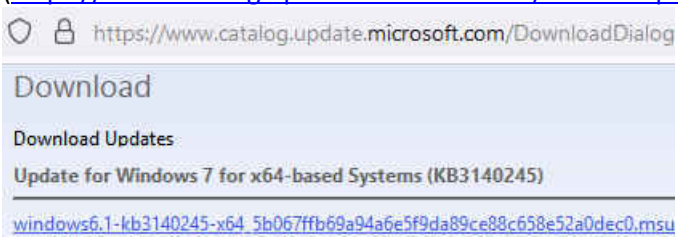
0x800CCC1A - Your server does not support the connection encryption type you have specified. Try changing encryption method. Contact your mail server administrator or Internet service provider (ISP).



The error occurs when an Outlook client tries to connect to a mail server using a non-supported encryption protocol.

Most often, this problem occurs if your mail server supports only TLS 1.2 and 1.3 protocols. For example, Windows 7 only supports the legacy TLS 1.0 and 1.1 protocols by default, which are no longer used by public mail servers.
The Outlook client uses the WINHTTP transport to send or receive data over TLS. If TLS 1.2 is not supported or is disabled on the winhttp level, Outlook won't be able to connect to a server due to an unsupported encryption type.
To fix this problem, you need to enable the TLS 1.2 protocol on Windows 7. Windows 7 supports TLS 1.2, but it is not enabled by default (unlike newer OS versions – Windows 8, 10, and 11).

In order to **enable TLS 1.2 on Windows 7**:

1. Make sure that Windows 7 SP1 is installed;
2. Manually download and install the update **KB3140245** from Microsoft Update Catalog (https://www.catalog.update.microsoft.com/search.aspx?q=kb3140245);
   

3. Download and install **MicrosoftEasyFix51044.msi** patch (https://download.microsoft.com/download/0/6/5/0658B1A7-6D2E-474F-BC2C-D69E5B9E9A68/MicrosoftEasyFix51044.msi);
   This fix is described in the article **Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows**. The fix adds TLS 1.1 and TLS 1.2 support options to the registry on Windows Server 2012, Windows 7 SP1, and Windows Server 2008 R2 SP1 (described below).
4. Restart your computer.

The patch mentioned above adds the following options to the registry:

A **DefaultSecureProtocols** parameter with the value **0x00000a00** in **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp.**

In a 64-bit Windows version, you have to create this setting under HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp.

The **0x0A0** parameter leaves SSL 3.0 and TLS 1.0 enabled for WinHTTP, and enables TLS 1.1 and TLS 1.2 as well. If you want to allow a client to use only TLS 1.1 or TLS 1.2, change the value to **0xA00**.

Create new subkeys TLS 1.2 and TLS 1.1 under HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\.

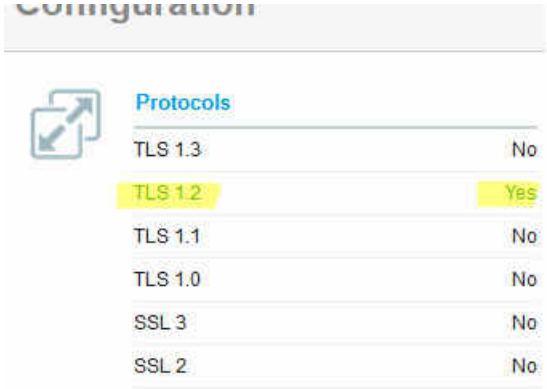
Create a **Client** key in each registry section. Then open each Client key and create a DWORD parameter **DisabledByDefault** with the value **0x00000000**.

To create these registry parameters, you may use the following PowerShell script:

```
$reg32bWinHttp = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp"
$reg64bWinHttp = "HKLM:\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet
Settings\WinHttp"
$regWinHttpDefault = "DefaultSecureProtocols"
$regWinHttpValue = "0x00000a00"
$regTLS11 = "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.1\Client"
$regTLS12 = "HKLM:SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.2\Client"
$regTLSDefault = "DisabledByDefault"
$regTLSValue = "0x00000000"
# For Windows x86
New-ItemProperty -Path $reg32bWinHttp -Name $regWinHttpDefault -Value $regWinHttpValue -
PropertyType DWORD
# For Windows x64
New-ItemProperty -Path $reg64bWinHttp -Name $regWinHttpDefault -Value $regWinHttpValue -
PropertyType DWORD
New-Item -Path $regTLS11
New-ItemProperty -Path $regTLS11 -Name $regTLSDefault -Value $regTLSValue -PropertyType DWORD
New-Item -Path $regTLS12
New-ItemProperty -Path $regTLS12 -Name $regTLSDefault -Value $regTLSValue -PropertyType DWORD
```

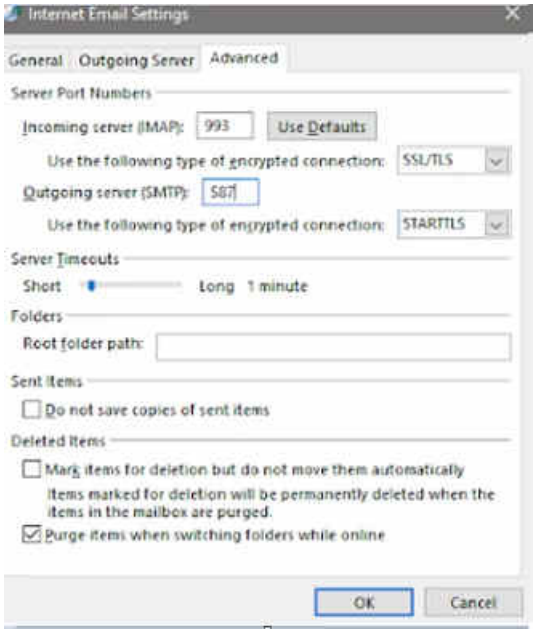
Learn more about how to disable legacy TLS versions on Windows.

You can check the TLS protocol versions supported by your mail server using an online service SSL Labs (https://www.ssllabs.com/ssltest/analyze.html?d=mail.woshub.com)



In Microsoft 365 (Office 365), TLS 1.0 and TLS 1.1 protocols are not yet disabled by default.

In the Outlook settings, make sure that **STARTTLS** (available in all modern Outlook versions) or SSL/TLS are used to connect to the mail server. Make sure that the option "**This server requires an encrypted connection (SSL/TLS)**" is enabled. Check the IMAP/POP/SMTP port numbers.



Also, note that some antiviruses have the SSL/TLS inspection (filtering) option enabled by default. Try to disable this option in your antivirus software settings and check the connection to a mail server in Outlook.