

# Configuring authentication and encryption

Updated: January 21, 2005

## Configuring authentication and encryption

### TLS authentication overview

Remote Desktop Protocol (RDP) provides data encryption, but it does not provide authentication to verify the identity of a terminal server. In Windows Server 2003 Service Pack 1 (SP1), you can enhance the security of Terminal Server by configuring Terminal Services connections to use Transport Layer Security (TLS) 1.0 for server authentication, and to encrypt terminal server communications. TLS is a standard protocol that is used to provide secure Web communications on the Internet or intranets. It enables clients to authenticate servers or, optionally, servers to authenticate clients. It also provides a secure channel by encrypting communications. TLS is the latest and most secure version of the Secure Sockets Layer (SSL) protocol. One important difference is that TLS 1.0 applies a Keyed-Hashing for Message Authentication Code (HMAC) algorithm, whereas SSL 3.0 applies the Message Authentication Code (MAC) algorithm. The HMAC produces an integrity check value as the MAC does, but with a hash function construction that makes the hash much harder to break.

The TLS and SSL protocols comprise two layers: the Handshake Protocol Layer and the Record Protocol Layer. For authentication purposes, the Handshake Protocol uses an X.509 certificate to provide strong evidence to a second party that helps prove the identity of the party that holds the certificate and the corresponding private key. A certificate is a digital form of identification that is usually issued by a certification authority (CA) and contains identification information, a validity period, a public key, a serial number, and the digital signature of the issuer. A CA is a mutually trusted third party that confirms the identity of a certificate requestor (usually a user or computer), and then issues the requestor a certificate. The certificate binds the requestor's identity to a public key. CAs also renew and revoke certificates as necessary. For example, if a client is presented with a server's certificate, the client computer might try to match the server's CA against the client's list of trusted CAs. If the issuing CA is trusted, the client will verify that the certificate is authentic and has not been tampered with. Finally, the client will accept the certificate as proof of identity of the server.

For more information about TLS, see [SSL/TLS in Windows Server 2003](#) [<http://go.microsoft.com/fwlink/?LinkId=19646>] (<http://go.microsoft.com/fwlink/?LinkId=19646>) and [RFC 2246, The TLS Protocol Version 1.0](#) [<http://go.microsoft.com/fwlink/?LinkId=40979>] (<http://go.microsoft.com/fwlink/?LinkId=40979>).

### Prerequisites for Configuring Server Authentication

By default, Terminal Server uses native RDP encryption and does not authenticate the server. For TLS to be used for server authentication and encryption of terminal server communications, the server and client must be correctly configured.

#### Server prerequisites

For TLS authentication to function correctly, terminal servers must meet the following prerequisites:

- Terminal servers must run Windows Server 2003 SP1.

- You must obtain a certificate for the terminal server. You can do this by doing any of the following:
  - [Use Windows Server 2003 Certificate Services Web Pages](http://technet2.microsoft.com/WindowsServer/en/library/26453270-45e5-4ffb-9a25-38a661b058241033.mspix) [http://technet2.microsoft.com/WindowsServer/en/library/26453270-45e5-4ffb-9a25-38a661b058241033.mspix] or [Use Windows 2000 Certificate Services Web Pages](http://technet2.microsoft.com/WindowsServer/en/library/871281d3-d9b4-4859-a7c6-9886e5f478f31033.mspix) [http://technet2.microsoft.com/WindowsServer/en/library/871281d3-d9b4-4859-a7c6-9886e5f478f31033.mspix] .
  - Use the Windows Server 2003 Certificate Request Wizard or Windows Server 2000 Certificate Request Wizard. For more information, see [Requesting certificates](http://technet2.microsoft.com/WindowsServer/en/library/590fcc3e-c54f-48b7-95f2-45ee2255fc111033.mspix) [http://technet2.microsoft.com/WindowsServer/en/library/590fcc3e-c54f-48b7-95f2-45ee2255fc111033.mspix] .
  - Purchase a certificate from a non-Microsoft vendor and install the certificate manually.

## Note

- If you plan to obtain a certificate by using the Certificate Web pages or Certificate Request Wizard, a public key infrastructure (PKI) must be configured correctly to issue SSL-compatible X.509 certificates to the terminal server. For information about PKI configuration, see [Public Key Infrastructure](http://technet2.microsoft.com/WindowsServer/en/library/32aacfe8-83af-4676-a45c-75483545a9781033.mspix) [http://technet2.microsoft.com/WindowsServer/en/library/32aacfe8-83af-4676-a45c-75483545a9781033.mspix] and [Deploying a Public Key Infrastructure](http://technet2.microsoft.com/WindowsServer/en/library/5028faa0-4ad7-44f7-b812-9a6f64304b771033.mspix) [http://technet2.microsoft.com/WindowsServer/en/library/5028faa0-4ad7-44f7-b812-9a6f64304b771033.mspix] .Each certificate must be configured as follows:
  - The certificate is a computer certificate.
  - The intended purpose of the certificate is server authentication.
  - The certificate has a corresponding private key.
  - The certificate has a cryptographic service provider (CSP) that can be used for the TLS protocols (for example, Microsoft RSA/SChannel Cryptographic Provider). For more information, see [Microsoft Cryptographic Service Providers](http://go.microsoft.com/fwlink/?LinkId=40983) [http://go.microsoft.com/fwlink/?LinkId=40983] (http://go.microsoft.com/fwlink/?LinkId=40983).
  - The certificate is stored in the terminal server's Personal store. You can view this store by using the Certificates snap-in. For more information, see [Certificate stores](http://technet2.microsoft.com/WindowsServer/en/library/1c4d3c02-e996-450a-bf4f-9a12d245a7eb1033.mspix) [http://technet2.microsoft.com/WindowsServer/en/library/1c4d3c02-e996-450a-bf4f-9a12d245a7eb1033.mspix] .

## Client prerequisites

For TLS authentication to function correctly, clients must meet the following prerequisites:

- Clients must run Windows 2000 or Windows XP.
- Clients must be upgraded to use the RDP 5.2 (Windows Server 2003) client. You can install this client-side Remote Desktop Connection package by using the %systemdrive\system32\clients\tsclient\win32\msrdpcli.msi file. The msrdpcli.msi file is located on Windows Server 2003 terminal servers. Installing this file from the terminal server installs the 5.2 version of Remote Desktop Connection to the %systemdrive\Program files\Remote Desktop directory on the destination computer. For more information, see [Remote Desktop Connection for Windows Server 2003 \[5.2.3790\]](http://go.microsoft.com/fwlink/?LinkId=41068) [http://go.microsoft.com/fwlink/?LinkId=41068] (http://go.microsoft.com/fwlink/?LinkId=41068).
- Clients must trust the root of the server's certificate. That is, clients must have the certificate of the CA that issued the server certificate in their Trusted Root Certification Authorities store. You can view this store by using the Certificates snap-in.

## Tasks for Configuring Server Authentication

For TLS authentication to function correctly, you must complete the following configuration tasks on terminal servers and clients. The procedure links contain step-by-step instructions for completing these tasks.

### Server Configuration Tasks

1. [Request a computer certificate for server authentication](http://technet2.microsoft.com/WindowsServer/en/library/f9871e14-e923-47d3-a7ff-0c1a6cfc1f4d1033.mspx) [http://technet2.microsoft.com/WindowsServer/en/library/f9871e14-e923-47d3-a7ff-0c1a6cfc1f4d1033.mspx] , if you do not already have a certificate that meets the requirements described in "Server prerequisites," earlier in this topic.

If you have been granted the appropriate permissions, there are two primary ways to explicitly request certificates:

- You can explicitly request certificates by using the Windows Server 2003 or Windows 2000 Certificate Services Web pages.
- You can use the Windows Server 2003 or Windows 2000 Certificate Request Wizard.

Alternatively, you can buy a certificate from a non-Microsoft vendor.

2. [Configure authentication and encryption on the server](http://technet2.microsoft.com/WindowsServer/en/library/8be5bfb5-b652-49aa-8ac4-f6c2b01f35101033.mspx) [http://technet2.microsoft.com/WindowsServer/en/library/8be5bfb5-b652-49aa-8ac4-f6c2b01f35101033.mspx] . For TLS to function correctly, in Terminal Server Configuration, on the **General** tab of the **RDP-tcpProperties** dialog box, you must do the following:

- Select a certificate that meets the requirements described in "Server prerequisites" earlier in this topic.
- Set the **Security layer** to **Negotiate** or **SSL**.
- Set the **Encryption level** to **High**, or enable Federal Information Processing Standard (FIPS) compliant encryption. You can enable FIPS-compliant encryption by using Group Policy as well.
- You cannot enable TLS by using Group Policy.

## Note

If you enable TLS authentication in a session directory farm, in order for TLS authentication to remain enabled when a terminal server connection is redirected, you must configure all of the servers that are members of the session directory farm to use one of the following settings:

- Set the **Security layer** to **SSL**.
- Set the **Security layer** to **Negotiate**. If you use this configuration, TLS authentication is only enabled if the client supports it.

## Authentication and Encryption Settings

The following table summarizes the combinations of **Security layer** and **Encryption level** settings that are valid and invalid in Windows Server 2003 Service Pack 1, whether TLS authentication and encryption can be used, and the key strength provided by each encryption level.

SecurityLayers	Client Compatible	Encryption	Levels	FIPS-compliant
		Low RC4--56-bit	High RC4--128-bit	
<b>Negotiate</b>	Valid. The Maximum security layer and encryption level supported by the client are used. If TLS is supported for server authentication, TLS is used rather than RDP, and High or FIPS-compliant encryption level is used.	Valid	Valid	Valid

<b>SSL (TLS 1.0)</b>	Valid. TLS is required for server authentication. High or FIPS-compliant encryption level is used. If TLS is not supported, connections fail.	Not Valid. The encryption level defaults instead to Client Compatible. High or FIPS-compliant encryption level is used, if supported by client.	Valid	Valid
<b>RDP</b>	Valid. However, TLS cannot be used for server authentication. RDP encryption is used and the maximum encryption level supported by the client is used.	Valid	Valid	Valid

For more information about encryption options, see "Determining the level of encryption," later in this topic.

## Client configuration tasks

1. [Request a certification authority certificate for the client](http://technet2.microsoft.com/WindowsServer/en/library/cbbfd6c6-0c3a-4f76-b120-c71ecb16a6471033.mspix) [http://technet2.microsoft.com/WindowsServer/en/library/cbbfd6c6-0c3a-4f76-b120-c71ecb16a6471033.mspix] .

Use this procedure to request a certificate chain from a Windows Server 2003 CA. A certificate chain contains the chain of certificates that can be traced back to the root CA. The certificate that you retrieve by using this procedure is stored in the Trusted Root Certification Authorities store.

2. [Configure authentication on the client by using Remote Desktop Connection](http://technet2.microsoft.com/WindowsServer/en/library/cdfe9f76-fb54-46fe-84c0-7cf637dc65be1033.mspix) [http://technet2.microsoft.com/WindowsServer/en/library/cdfe9f76-fb54-46fe-84c0-7cf637dc65be1033.mspix] or [Configure authentication on the client by using an .rdp file](http://technet2.microsoft.com/WindowsServer/en/library/926dd6ae-1fa5-481a-bcc6-112a7b1da7581033.mspix) [http://technet2.microsoft.com/WindowsServer/en/library/926dd6ae-1fa5-481a-bcc6-112a7b1da7581033.mspix] .

Keep in mind that clients must run Windows 2000 or Windows XP and that they must use the RDP 5.2 (Windows Server 2003) client.

## Determining the level of encryption

For Terminal Services connections, data encryption can protect your data by encrypting it on the communications link between the client and the server. Encryption protects against the risk of unauthorized transmission interception on the link between server and client.

By default, Terminal Services connections are encrypted at the highest level of security available (128-bit). However, some older versions of the Terminal Services client do not support this high level of encryption. If your network contains such legacy clients, you can set the encryption level of the connection to send and receive data at the highest encryption level supported by the client. In order for clients to be able to connect to a terminal server that uses FIPS-compliant encryption, you must upgrade these clients to use the RDP 5.2 (Windows Server 2003) client. For more information, see [Remote Desktop Connection for Windows Server 2003 \[5.2.3790\]](http://go.microsoft.com/fwlink/?LinkId=41068) [http://go.microsoft.com/fwlink/?LinkId=41068] (http://go.microsoft.com/fwlink/?LinkId=41068).

There are four levels of encryption available:

Level of encryption	Description
FIPS-compliant	<p>This level encrypts and decrypts data sent from client to server and from server to client with the Federal Information Processing Standard (FIPS) encryption algorithms using the Microsoft cryptographic modules. You can enable FIPS-compliant encryption by using Group Policy or Terminal Services Configuration. For more information, see <a href="http://go.microsoft.com/fwlink/?LinkId=36329">FIPS 140 Evaluation</a> [http://go.microsoft.com/fwlink/?LinkId=36329] (http://go.microsoft.com/fwlink/?LinkId=36329).</p> <p><b>Important</b></p> <ul style="list-style-type: none"> <li>Any encryption level settings that you configure in Group Policy override the configuration that you set by using the Terminal Services Configuration tool. Also, if you enable the <a href="http://technet2.microsoft.com/WindowsServer/en/library/6ff574cb-30c4-4ad9-8d5e-ae697c65b9b1033.mspix">System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing</a> [http://technet2.microsoft.com/WindowsServer/en/library/6ff574cb-30c4-4ad9-8d5e-ae697c65b9b1033.mspix] Group Policy setting, this setting overrides the <b>Set client connection encryption level</b> Group Policy setting.</li> </ul>

	<ul style="list-style-type: none"> <li>You must enable FIPS-compliant encryption or set the encryption level to <b>High</b> if you plan to use TLS for server authentication.</li> </ul>
High	<p>This level encrypts data sent from client to server and from server to client by using strong 128-bit encryption. Use this level when the terminal server is running in an environment containing 128-bit clients only (such as Remote Desktop Connection clients). Clients that do not support this level of encryption will not be able to connect.</p> <p><b>Important</b></p> <ul style="list-style-type: none"> <li>You must enable FIPS-compliant encryption or set the encryption level to <b>High</b> if you plan to use TLS for server authentication.</li> </ul>
Client Compatible	<p>This level encrypts data sent between the client and the server at the maximum key strength supported by the client. Use this level when the terminal server is running in an environment containing mixed or legacy clients.</p>
Low	<p>This level encrypts data sent from the client to the server using 56-bit encryption.</p> <p><b>Important</b></p> <ul style="list-style-type: none"> <li>Data sent from the server to the client is not encrypted.</li> </ul>

[↑Top of page](#)

#### Related Links

- [Working with MMC console files](#)
- [Request a computer certificate for server authentication](#)
- [Configure authentication and encryption on the server](#)
- [Request a certification authority certificate for the client](#)
- [Configure authentication on the client by using Remote Desktop Connection](#)
- [Configuring Terminal Services with Group Policy](#)

[Manage Your Profile](#)