Secure WSUS with the Secure Sockets Layer Protocol

You can use the Secure Sockets Layer (SSL) protocol to help secure the WSUS deployment. WSUS uses SSL to authenticate client computers and downstream WSUS servers to the WSUS server. WSUS also uses SSL to encrypt update metadata.

WSUS uses SSL for metadata only, not for update files.

Configure SSL on the WSUS server

WSUS requires two ports for SSL: one port that uses HTTPS to send encrypted metadata, and one port that uses HTTP to send updates.

Limitations of WSUS SSL deployments

You must consider the following limitations when you use SSL to secure a WSUS deployment:

1. Using SSL increases the server workload. You should expect a 10 percent loss of performance because of the cost of encrypting all the metadata that is sent over the network.
2. If you use WSUS with a remote SQL Server database, the connection between the WSUS server and the database server is not secured by SSL. If the database connection must be secured, consider the following recommendations:

- Move the WSUS database to the WSUS server.
- Move the remote database server and the WSUS server to a private network.
- Deploy Internet Protocol security (IPsec) to help secure network traffic. For more information about IPsec, see Creating and Using IPsec Policies.

To configure SSL on the WSUS root server

1. Log on to the WSUS server by using an account that is a member of the WSUS Administrators group or the local Administrators group.
2. Go to **Start**, type **CMD**, right-click **Command Prompt**, and then click **Run as administrator**.
3. Navigate to the *%ProgramFiles%***Update Services****Tools**\ folder.
4. In the Command Prompt window, type the following command:

   Wsusutil configuressl *certificateName*

   where:

   certificateName is the DNS name of the WSUS server.

Configure SSL on client computers

When you configure SSL on client computers, you should consider the following issues:

- You must include a URL for a secure port on the WSUS server. Because you cannot require SSL on the server, the only way to make sure that client computers can use a security channel is by using a URL that specifies HTTPS. If you use any port other than 443 for SSL, you must include that port in the URL also.
- The certificate on a client computer must be imported into the Local Computer Trusted Root CA store or Automatic Update Service Trusted Root CA store. If the certificate is imported to the Local User's Trusted Root CA store only, Automatic Updates will fail server authentication.
- The client computers must trust the certificate that you bind to the WSUS server. Depending on the type of certificate that is used, you might have to set up a service to enable the client computers to trust the certificate that is bound to the WSUS server.

Configure SSL for downstream WSUS servers

The following instructions configure a downstream server to synchronize to an upstream server that uses SSL.

To synchronize a downstream server to an upstream server that uses SSL

1. Log on to the computer by using a user account that is a member of the local Administrators group or the WSUS Administrators group.
2. Click **Start**, click **All Programs**, click **Administrative Tools**, and then click **Windows Server Update Service**.
3. In the right pane, expand the server name.
4. Click **Options**, and then click **Update Source and Proxy Server**.
5. On the **Update Source** page, select **Synchronize from another Windows Server Update Services server**.
6. Type the name of the upstream server into the **Server name** text box. Type the port number that the server uses for SSL connections into the **Port number** text box.
7. Select the **Use SSL when synchronizing update information** check box, and then click **OK**.