Contacting SafeNet

We work closely with our reseller partners to offer the best worldwide technical support services. Your reseller is the first line of support when you have questions about products and services. However, if you require additional assistance you can contact the SafeNet technical support team help-desk which is available 24 hours a day, seven days a week:

<table>
<thead>
<tr>
<th>Country/Region</th>
<th>Telephone</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>+1-800-545-6608</td>
</tr>
<tr>
<td>International</td>
<td>+1-410-931-7520</td>
</tr>
</tbody>
</table>

For further assistance submit additional questions to the SafeNet technical support team at the following web page:

http://c3.safenet-inc.com/secure.asp

For assistance via email to SafeNet technical support send the request to the following address:

support@safenet-inc.com
# Table of Contents

**Introduction** ...................................................................................................................................................... 1  
Abstract.......................................................................................................................................................... 1  
SSTP-based VPN connection process ............................................................................................................ 2  
Basic test lab setup for SSTP remote access VPN connections ................................................................. 4

**Configuring DC** ........................................................................................................................................... 5

Configuring NPS ................................................................................................................................................ 6  
Define RRAS as RADIUS Client .................................................................................................................. 6  
Define MSCHAPv2 Authentication Protocol in NPS Policies ........................................................................ 9  
Create a Network Policy ................................................................................................................................ 11  
Configure SAM 8.0 ......................................................................................................................................... 15  
Configuring SafeNet IAS Plugin .................................................................................................................. 16  
IAS Plugin Settings ....................................................................................................................................... 16  
eToken-NG OTP enrollment ..................................................................................................................... 16

**Configuring RRAS** ................................................................................................................................... 18

Configure Routing and Remote Access ........................................................................................................ 18  
Configuring RRAS SSTP server Certificate ............................................................................................... 26  
Enable MSCHAPv2 authentication protocol ............................................................................................... 28

**Configuring SSTP Client** .......................................................................................................................... 31

Obtain a trusted root CA certificate ............................................................................................................. 31  
Export trusted root CA certificate to Local Machine Store ..................................................................... 33  
Configure and test an SSTP-based VPN connection .................................................................................. 35
Chapter 1
Introduction

Abstract

Secure Socket Tunneling Protocol (SSTP) is a new type of Virtual Private Network (VPN) tunnel enabling traffic to pass through firewalls that block PPTP and L2TP/IPsec traffic. SSTP provides a mechanism to encapsulate PPP traffic over the HTTPS protocol SSL channel. Using PPP enables support for strong authentication methods such as MSCHAPv2 carrying One Time Password (OTP) user credentials for enhanced security.

Using HTTPS transmits traffic through TCP port 443, a port commonly used for Web access. Secure Sockets Layer (SSL) provides transport-level security with enhanced key negotiation, encryption, and integrity checking.

This how-to guide provides basic details to create a test lab, and to configure and test VPN remote access with Windows Server 2008 R2 and Windows 7.
SSTP-based VPN connection process

For a computer running Windows Server 2008 or Windows 7 initiating an SSTP-based VPN connection, the SSTP client establishes a TCP connection with the SSTP server between a dynamically allocated TCP port on the SSTP client and TCP port 443 on the Routing and Remote Access Server (RRAS).

The following process illustrates the SSTP client connection process with the RRAS.

1. The SSTP client sends an SSL Client-Hello message to the SSTP server, indicating that the SSTP client wants to create an SSL session with the RRAS.
2. The SSTP server sends its computer certificate to the SSTP client.
3. The SSTP client validates the computer certificate, determines the encryption method for the SSL session, generates an SSL session key and encrypts it with the SSTP server’s certificate public key. The SSTP client then sends the encrypted form of the SSL session key to the RRAS.
4. The RRAS decrypts the encrypted SSL session key with the computer certificate’s private key. All future communication between the SSTP client and the RRAS is encrypted with the negotiated encryption method and SSL session key.
5. The SSTP client sends an HTTP over SSL request message to the RRAS to negotiate an SSTP tunnel.
6. The SSTP client negotiates an SSTP tunnel with the RRAS.
7. The SSTP client negotiates a PPP connection with the RRAS. This negotiation includes authenticating the user’s credentials with a PPP MSCHAPv2 authentication method and...
configuring settings for Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) traffic.

8. On the RRAS, the user clicks the button on the either an eToken NG-OTP or eTokenPASS, generating an OTP Passcode number. The RRAS then provides the SSTP client the following logon credentials for authentication:
   ♦ User name
   ♦ OTP Passcode
   ♦ Domain name

9. The RRAS forwards the request to the Network Policies service (NPS) using MSCHAPv2 authentication protocol.

10. NPS uses an installed eToken OTP Plugin extension to check the user credentials validity with the backend SafeNet SAM. The installed eToken OTP authentication plug-in on the RADIUS server validates the request via web services (SOAP over HTTPS) to the TMS validation service.

11. Based on the OTP value calculation results and the NPS Remote access policies authorization, the SSTP server sends a Radius Access Accept/Reject response to the SSTP server.

12. Based on the response received from the NPS server, the SSTP server authorizes or denies network entry.

13. The SSTP client begins sending IPv4 or IPv6 traffic over the PPP link.
Basic test lab setup for SSTP remote access VPN connections

The infrastructure for the VPN test lab network consists of three computers, performing the following services:

- A server computer running Windows Server 2008 R2 operating as a domain controller, with Active Directory Certificate Services, Domain Name System (DNS) server, NPS server, SAM 8.0 server and eToken OTP Plugin.

- A server computer running Windows Server 2008 R2 configured with Routing and Remote Access and operating as a VPN SSTP server. This server has two network adapters installed.

- A client computer running Windows 7 operating as a VPN SSTP client on a public (Internet) network.

The following diagram illustrates the VPN test lab configuration.
Chapter 2
Configuring DC

The DC is a computer running Windows Server 2008 R2 providing the following services:

- A domain controller for the Active Directory domain.
- A DNS server for the domain.
- An Active Directory Certificate Service to issue the computer certificate required for an SSTP-based VPN connection.
- An NPS server.
- A SAM server with NPS plugin.

The DC configuration requires the following steps:

**Step 1:** Install Active Directory, DNS, CA and NPS roles.

**Step 2:** Install SAM 8.0 and SafeNet NPS plugin.

**Step 3:** Create a user account with remote access permission.

**Step 4:** Enroll an OTP profile on eToken NG-OTP or eTokenPASS.
Configuring NPS

To configure NPS perform the following:

- Define RRAS as a RADIUS client
- Define MSCHAPv2 Authentication Protocol in NPS policies
- Create a Network Policy
- Configure SAM 8.0

Define RRAS as RADIUS Client

To identify the RRAS as RADIUS client:

1. Open the Network Policy Server.
2. In the left tree view expand **RADIUS Clients and Servers**.
3. Right-click **RADIUS Clients**. On the shortcut menu select **New RADIUS Client**.
The *New RADIUS Client* dialog box opens.

4. In the *New RADIUS Client* dialog box, complete the following fields:
   - **Enable this RADIUS client**—Select this option.
   - **Friendly name**—Enter the RRAS name.
   - **Address (IP or DNS)**—Enter the RRAS IP address.
   - **Select an existing Shared Secret template**—From the drop-down list select None.
   - **Select RADIUS Standard** from the Vendor name list box.

5. In the *Shared Secret* workspace select Manual. The *Shared Secret* and Confirm shared secret fields are enabled.

6. Complete the following fields.
   - **Shared Secret**—Enter a Shared secret for the RRAS.
   - **Confirm shared secret**—Enter the exact same secret as entered in Shared Secret. The secret is case sensitive.

7. Click **OK**. The RRAS is defined as a RADIUS Client
The next step is to create a connection request policy. This is performed by defining MSCHAPv2 Authentication Protocol in NPS Policies.
Define MSCHAPv2 Authentication Protocol in NPS Policies

To create a connection request policy:

1. In the Network Policy Server left tree view, expand Policies.

3. In the New Connection Request Policy dialog box, enter a Policy name and leave Type of network access server set to Unspecified.

4. Click Next. The Specify Conditions dialog box opens.

5. In the Specify Conditions box, select the conditions to help identify which connection types can be authenticated (for example, NAS Identifier).

6. Click Add.

7. In the next dialog box, enter additional information on the conditions selected in the previous step.

8. Click OK.

The Specify Connection Request Forwarding dialog box opens.
9. In the Specify Connection Request Forwarding dialog box, select **Authenticate requests on this server**.

10. Click **Next**.

   The Specify Authentication Methods and Configure Settings dialog boxes opens.

11. In the Specify Authentication Methods and Configure Settings dialog boxes, accept the defaults by clicking **Next**.

12. Click **Finish**.

The next step is to create a network policy.

**Create a Network Policy**

**To create a network policy:**

1. In the Network Policy Server left tree view, expand **Policies**.
2. In the Network Policy Server, right-click **Network Policies**. On the shortcut menu select **New**.

   The New Network Policy dialog box opens.
3. In the **New Network Policy** dialog box, enter a **Policy name** such as MSCHAPv2 and leave **Type of network access server** set to **Unspecified**.

4. Click **Next**.

5. In the next dialog box, click **Add** to select one or more conditions. The specified condition(s) determine whether the created policy is evaluated for connection requests. The **Specify Conditions** dialog box opens.

6. In the **Specify Conditions** dialog box, select the required conditions.

7. Click **Add**.

8. In the next dialog box, enter additional information on the conditions selected in the previous step.

9. Click **OK**. The **Specify Access Permission** dialog box opens.

10. In the **Specify Access Permission** dialog box, select **Access granted**.

11. Click **Next**.

12. For the connection request select the **MSCHAPv2 authentication** method.

13. Click **Next**.

   The **Configure Constraints and Configure Settings** dialog boxes open.

14. In the **Configure Constraints and Configure Settings** dialog boxes, click **Next**.
15. Click **Finish**.
Configure SAM 8.0

To configure SAM 8.0

1. Install SAM 8.0 in the domain environment and enable the OTP connector.

2. Define OTP Parameters according to the domain policy restrictions.
Configuring SafeNet IAS Plugin

The configure SafeNet IAS Plugin perform the following:

- IAS Plugin Settings
- eToken-NG OTP Enrollment

IAS Plugin Settings

To install IAS plugin settings:

1. Install the eToken OTP Authentication installation file on the IAS server.
2. Configure IAS to use it for authentication. The configuration settings are saved in an XML file.

![Example XML configuration]

eToken-NG OTP enrollment

To enroll an eToken-NG OTP:

1. From SAMservice or SAMmanage enroll an eToken NG-OTP profile for domain users.
RRAS SSTP server is a computer running Windows Server 2008R2 providing the following roles:

- Network Policy and Access Services providing support for VPN connections through Remote Access Service.
- Web Server (IIS).

**Note:** Routing and Remote Access does not require IIS because it listens to HTTPS connections directly over HTTP.SYS.

RRAS SSTP configuration consists of the following steps:

**Step 1:** Configure RRAS SSTP.

**Step 2:** Configure the RRAS SSTP Server Authentication certificate.

**Step 3:** Enable MSCHAPv2 authentication protocol.

### Configure Routing and Remote Access

Configure the server to be a VPN server providing remote access for Internet-based VPN clients.

**To configure the RRAS to be a VPN server**

1. On the server, click **Start**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
The *Routing and Remote Access* dialog box opens.

2. In the *Routing and Remote Access* dialog box console tree, right-click *Local Server*, and then click *Configure and Enable Routing and Remote Access*. 
The *Routing and Remote Access Server Setup Wizard* page opens in the details workspace.

![Routing and Remote Access Server Setup Wizard](image)

3. In the *Welcome to the Routing and Remote Access Server Setup Wizard* page click **Next**. The *Configuration* page opens.

![Configuration page](image)

4. In the *Configuration* page, select **Remote access (dial-up or VPN)**.
5. Click **Next**.

   The *Remote Access* page opens.

6. In the *Remote Access* page, select **VPN**.

7. Click **Next**.
The **VPN Connection** page opens.

8. In the **VPN Connection** page, in the **Network interfaces** workspace, click **Public**. This is the interface connecting RRAS to the Internet.

9. Clear the **Enable security on the selected interface by setting up static packet filters** option, and then click **Next**.
The *IP Address Assignment* page opens.

10. In the *IP Address Assignment* page, select **From a specified range of addresses** and define a range.

11. Click **Next**.
12. In the Managing Multiple Remote Access Servers page select **Yes, set up this server to work with a RADIUS server**.

13. Click Next.
14. In the *Radius Server Selection* page complete the following fields:
   - **Primary RADIUS Server**—Enter the NPS IP address.
   - **Shared Secret**—Enter the shared secret.

15. Click **Next**.

The *Completing the Routing and Remote Access Server Setup Wizard* opens.
16. In the *Completing the Routing and Remote Access Server Setup Wizard* page review the setup configuration. If the setup is correct click **Finish**.

**Configuring RRAS SSTP server Certificate**

Install a computer certificate on the RRAS SSTP server.

This certificate must have the same subject name (CN) as the host name to which the VPN clients connect. This is required for SSL negotiation to succeed.
Currently the SSTP by default picks up a certificate available in the cert store and uses it to perform SSL binding. The same information is cached to do crypto binding for the inbound connection.

To enable viewing the certificate selection UI:

1. Open the `rrasmgmt.msc`, and right click the targeted server.
2. Select the Properties option. The Properties dialog box opens.
3. Select the Security Tab.

    The Security tab opens.
3. In the Security tab, in the SSL Certificate Binding workspace, from the Certificate drop-down list, select one of the valid certificates for SSL binding. The RRAS UI picks up and displays valid certificates in the Certificate drop-down list from the Local Machine personal cert store. Users can check currently provisioned certificates using certificate snap-in the Windows2008 R2. Once a user configures a certificate, the RRAS UI prompts a Remote Access Service (including SSTP service) restart. During the remote service restart the SSL (SSTP service) binds to the selected certificate.

Enable MSCHAPv2 authentication protocol

In RRAS it is required to enable MSCHAPv2 authentication.

To enable MSCHAPv2:

1. Open the rrasmgmt.msc and right click the targeted server.
2. Select the Properties option. The Properties dialog box opens.
3. Select the Security Tab.
Deploying SSTP using OTP How-To Guide

Configuring RRAS

The Security tab opens.

![Security tab](image)

4. In the Security tab, click **Authentication Methods**.
5. Select **Microsoft encrypted authentication version 2 (MSCHAPv2)**.

6. Click **OK**.
Chapter 4
Configuring SSTP Client

The SSTP Client is a computer running Windows 7 functioning as a remote access VPN client for the domain.

A VPN client using an SSTP connection must install the root CA certificate of the VPN server's computer certificate. During the SSL authentication phase, the VPN client validates the Server Authentication certificate using the certificate installed on the client.

Obtain a trusted root CA certificate

For clients joined to an Active Directory domain, or through Web enrollment from the CA's certificate-issuing Web site, the root certificate can be obtained through auto-enrollment. In this scenario, the client obtains the root CA certificate from DC by using Web enrollment.

To obtain a computer certificate from DC:
1. On the client machine, click Start, and then click Internet Explorer. The Internet Explorer window opens.
2. In Internet Explorer, clear the URL and enter http://DC/certsrv, and then press ENTER.
3. If a phishing filter alert opens, click Turn off automatic Phishing Filter, and then click OK. The DC Welcome page opens.
4. On the DC Welcome page, under Select a task, click Download a CA certificate, certificate chain, or CRL.
5. If an Information Bar alert opens, click Close.
6. Click Download CA certificate. The File Download dialog box opens. The File Download dialog box is to download the security certificate.
7. In the File Download dialog box navigate to the folder containing the CA certificate download file.
8. Select the CA certificate download file and click Open. The Security Alert dialog box opens.
9. In the Security Alert dialog box, click Allow. The Install Certificate button is enabled.
12. To accept the default automatic store location, in the Certificate Store dialog box click Next. The TBD dialog box opens.
13. In the TBD dialog box click Finish. The DC certificate is imported. The Import Confirmation dialog box opens.
14. In the Import Confirmation dialog box, click **OK**.

15. To close the Import Certificate dialog box click **OK**.
Export trusted root CA certificate to Local Machine Store

Now that the computer certificate has been installed, it must be moved to the correct store. The default automatic location for the installed certificate is in the Current User, Intermediate Certification Authority store. The certificate must be moved to the Local Computer, which is the Trusted Root Certification Authority store on your machine. Begin by configuring a Microsoft Management Console (MMC) with user and computer certificate snap-ins.

To configure an MMC:

1. On client machine, click Start, click All Programs, click Accessories, and then click Run. The Run dialog box opens.
2. In Open, enter mmc, and then click OK. The User Account Control dialog box opens.
3. In the User Account Control dialog box, click Continue. The Console1 Snap-in window opens.
4. On the File menu, and click Add/Remove Snap-in. The Add or Remove Snap-ins dialog box opens.
5. In the Available snap-ins workspace, click Certificates, and then click Add. The Certificate snap-in dialog box opens.
6. To accept the default settings select My user account and click Finish. The Certificates – Current user is displayed in the Selected snap-ins workspace.
8. To accept the Local computer default settings select Local Computer, and then click Finish. The Computer Manager (Local) is displayed in the Selected snap-ins workspace.
9. Click OK.

Export the installed certificate from the default store location. Because the certificate does not involve private key binding, copy and paste the certificate to the new certificate store.

To Export the certificate:

1. On client machine open the newly created MMC.
2. In the Console Tree pane, expand Certificates (Current User), expand Intermediate Certification Authorities, and then click Certificates. The certificates are displayed in the pane on the right side.
3. In the right pane, right-click the CA certificate, and then click Copy.
4. In the Console Tree pane, expand Certificates (Local Computer), expand Trusted Root Certification Authorities, and then click Certificates. The certificates are displayed in the pane on the right side.
5. Right click in the right pane and click **Paste**.

6. Refresh the view to verify that the certificate is added to this store.
Configure and test an SSTP-based VPN connection

Now that the root CA certificate of the RRAS SSTP server computer certificate is in the Trusted Root Certification Authorities certificate store on the SSTP client box, configure and test an SSTP connection.

To configure and test an SSTP connection:

1. On the Client, open Network and Sharing Center, click Manage network connections.
2. Double-click VPN Connection, and then click Properties. The VPN Connection Properties dialog box opens.
3. Select the General tab.
   The General tab opens.

4. In Host name or IP address of destination enter the RRAS Fully Qualified Domain Name (FQDN).
5. Select the Networking tab.
   The Networking tab opens.
6. From the **Type of VPN** drop-down list, select **Secure Socket Tunneling Protocol (SSTP)**.

7. Select the **Security** tab. The **Security** tab opens.

8. Click **Advanced**.

   The **Advanced Security Settings** dialog box opens.
9. Select **Allow these protocols**, and select **Microsoft CHAP Version 2 (MS-CHAP v2)**.

10. Click **OK**. The Advanced Security Setting dialog box closes.

11. Click **OK**. The VPN Connection Properties dialog box closes.

12. On an **eToken NG-OTP** or **eTokenPASS** click the button to generate the OTP Passcode number.

13. Initiate a VPN connection.

   The VPN Connection dialog box *Connect SSTP* opens.
14. Enter the following logon credentials for authentication:

- **User name**—Provided by the System Administrator.
- **Password**—The OTP Passcode generated by the *eToken NG-OTP* or *eTokenPASS*.
- **Domain**—The domain name provided by the System Administrator.

15. Click **Connect**.

The **Connecting to SSTP** dialog box opens.

After connection the **Applying** dialog box opens.

16. Verify that the corporate file server can be accessed from a remote location.

17. Close the VPN Connection.

On DC hosting NPS, the user connection authorization and authentication type can be examined using an extension CALLED the eToken OTP Plugin extension dll.
Network Policy Server granted full access to a user because the host met the defined health policy.

<table>
<thead>
<tr>
<th>User</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Security ID</td>
<td>2008DEV\Administrator</td>
</tr>
<tr>
<td>Account Name</td>
<td>2008DEV.COM\administrator</td>
</tr>
<tr>
<td>Account Domain</td>
<td>2008DEV</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RADIUS Client</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Friendly Name</td>
<td>UTP2008R2</td>
</tr>
<tr>
<td>Client IP Address</td>
<td>172.10.10.1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authentication Details</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Request Policy Name</td>
<td>Microsoft Routing and Remote Access Service</td>
</tr>
<tr>
<td>Network Policy Name</td>
<td>Connections to Microsoft Routing and Remote Access Service</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access server</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Provider</td>
<td>Windows</td>
</tr>
<tr>
<td>Authentication Server</td>
<td>utp2008r2.2008dev.com</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Extension</td>
</tr>
</tbody>
</table>