

# RSA Authentication Manager 7.1 Proxy Server Configuration

## Introduction

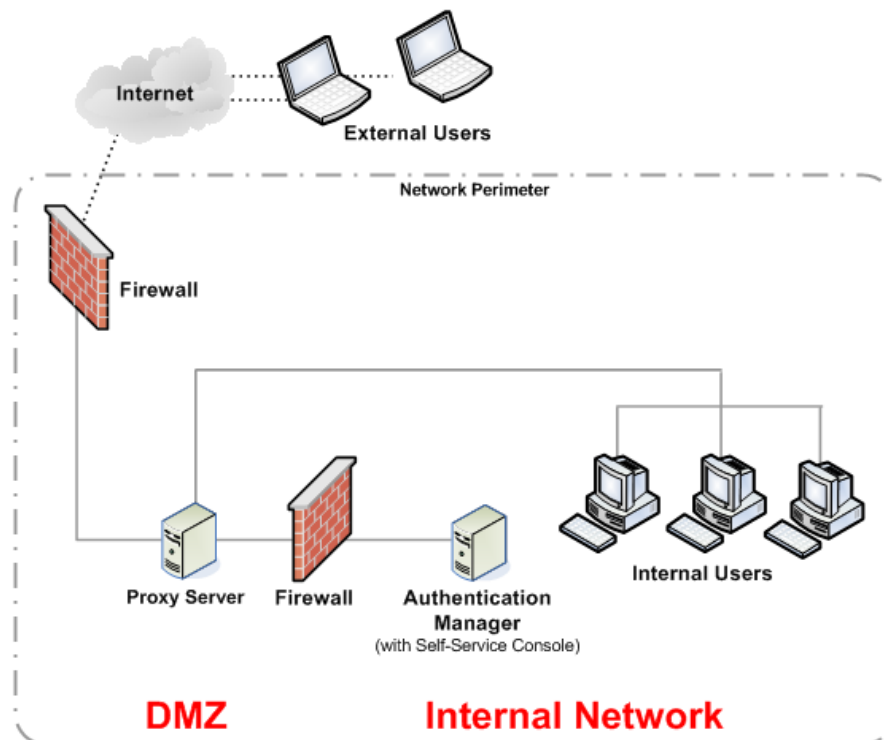
You may need to set up a proxy server for RSA Authentication Manager if:

- You are deploying software tokens using remote token-key generation (CT-KIP). You must configure a proxy server to connect to mobile devices through Secure Sockets Layer (SSL).
- You want to restrict users from directly accessing RSA Authentication Manager. You can configure a proxy server to accept RSA Self-Service Console requests and proxy to the Self-Service Console.

This document describes the process of setting up a proxy server in a Microsoft Windows environment. The instructions are based on a proxy server running Microsoft ISA Server 2006 Enterprise Edition.

**Note:** RSA does not provide support for third-party software. If you need further assistance to set up a proxy server, contact the product vendor.

The following figure shows a basic network setup with the Self-Service Console traffic directed through a proxy server.



---

## Prerequisites

To set up and test a proxy server, you must have at least three machines running Microsoft Windows:

**Internal Machine.** Runs RSA Authentication Manager.

**Proxy Machine.** Routes requests from the external network to the internal network. The proxy server must have two Network Interface Cards (NICs).

**External Machine.** Tests external access to the Self-Service Console.

---

**Important:** Test connectivity between these machines before beginning setup. When ISA Server is installed, the connectivity between the networks is lost.

---

---

## Configuring the Internal Machine

You must perform these steps in the following order to configure the internal machine to work with the proxy machine:

1. Install RSA Authentication Manager.
2. [Download the RSA Authentication Manager Server Certificate](#)
3. [Download the RSA Authentication Manager Root Certificate](#)

### Download the RSA Authentication Manager Server Certificate

You must download the RSA Authentication Manager Server Certificate so that you can copy it to the proxy machine later.

**To download the server certificate:**

1. In Internet Explorer, open the RSA Security Console.  
You are prompted to accept a certificate.
2. Accept and view the certificate.
3. Click the **Details** tab.
4. Click **Copy to File**.  
The Certificate Export Wizard opens.
5. Complete the Certificate Export Wizard screens.

## Download the RSA Authentication Manager Root Certificate

You must download the RSA Authentication Manager Root Certificate so that you can copy it to the proxy machine later.

### To download the root certificate:

1. In Internet Explorer, open the RSA Security Console.  
You are prompted to accept a certificate.
2. Accept and view the certificate.
3. Click the **Certification Path** tab.
4. Select **Authentication Manager Root CA**, and click **View Certificate**.
5. Click the **Details** tab.
6. Click **Copy to File**.  
The Certificate Export Wizard opens.
7. Complete the Certificate Export Wizard screens.

---

## Configuring the Proxy Machine

You must perform these steps in the following order to configure the proxy machine to work with the internal machine:

1. Copy the RSA Authentication Manager server and root certificates from the internal machine.
2. [Import the RSA Authentication Manager Server Certificate](#)
3. [Import the RSA Authentication Manager Root Certificate](#)
4. [Install ISA Server 2006 Enterprise Edition](#)
5. [Create Network Rules](#)
6. [Generate a Server Certificate for the Published URL](#)
7. [Create a Secure Web Publishing Rule](#)

## Import the RSA Authentication Manager Server Certificate

You must import the Authentication Manager server certificate into the proxy machine so that the published URL is redirected correctly.

### To import the server certificate:

1. Click **Start > Run**.
2. Enter **mmc**, and click **OK**.
3. Click **File > Add/Remove Snap-in > Add**.
4. Select **Certificates**, and click **Add**.
5. Select **Computer Account**, and click **Next**.

6. Select **Local Computer**, and click **Finish**.
7. In the Add Standalone Snap-in dialog box, click **Close**.
8. In the Add/Remove Snap-in dialog box, click **OK**.
9. From the console tree, expand **Certificates**.
10. Right-click **Personal**, and click **All Tasks > Import**.  
The Certificate Import Wizard opens.
11. Click **Next**.
12. Browse to locate the server certificate that you copied from the internal machine, and click **Next**.
13. Review the settings, and click **Finish**.

### Import the RSA Authentication Manager Root Certificate

You must import the root certificate into the proxy machine so that the published URL is accessible over the internet.

#### To import the root certificate:

1. Click **Start > Run**.
2. Enter **mmc**, and click **OK**.
3. Click **File > Add/Remove Snap-in > Add**.
4. Select **Certificates**, and click **Add**.
5. Select **Computer Account**, and click **Next**.
6. Select **Local Computer**, and click **Finish**.
7. In the Add Standalone Snap-in dialog box, click **Close**.
8. In the Add/Remove Snap-in dialog box, click **OK**.
9. From the console tree, expand **Certificates**.
10. Right-click **Trusted Root Certification Authorities**, and click **All Tasks > Import**.  
The Certificate Import Wizard opens.
11. Click **Next**.
12. Browse to locate the root certificate that you copied from the internal machine, and click **Next**.
13. Review the settings, and click **Finish**.

## Install ISA Server 2006 Enterprise Edition

ISA Server 2006 Enterprise Edition is used to publish the URL to the external network.

Use the following configurations when installing ISA Server:

- On the Set up Scenarios screen, select **Install both Server services and Configuration storage server**.
- On the Internal network screen, give the IP range of internal network. For example, 172.16.130.1 to 172.16.130.254.

## Create Network Rules

You must create network rules to route traffic between the internal and external networks.

### To create a network rule from the external network to the internal network:

1. Open the ISA Server management console.
2. From the console tree, expand **Arrays**.
3. Expand the machine name.
4. Expand **Configuration**.
5. Right-click **Networks**, and click **New > Network Rule**.
6. In the **Network Rule** field, type **From External**, and click **Next**.
7. Click **Add**.
8. Expand **Networks**, select **External**, and click **Add**.
9. Click **Close**.
10. Click **Next > Add**.
11. Expand **Networks**, select **Internal**, and click **Add**.
12. Click **Close**.
13. Click **Next**.
14. Select **Route**, and click **Next**.
15. Click **Finish**.

### To create a network rule from the internal network to the external network:

1. From the console tree, expand **Arrays**.
2. Expand the machine name.
3. Expand **Configuration**.
4. Right-click **Networks**, and click **New > Network Rule**.
5. In the **Network Rule** field, type **From Internal**, and click **Next**.
6. Click **Add**.

7. Expand **Networks**, select **Internal**, and click **Add**.
8. Click **Close**.
9. Click **Next > Add**.
10. Expand **Networks**, select **External**, and click **Add**.
11. Click **Close**.
12. Click **Next**.
13. Select **Route**, and click **Next**.
14. Click **Finish**.

### Generate a Server Certificate for the Published URL

The server certificate contains information about how the web site is published to the external network.

---

**Important:** Complete this procedure only if you need the proxy server to accept SSL connections.

---

#### To generate a server certificate for the published URL:

1. Generate a server certificate request for the published URL.  
For example, if you want users to access the Self-Service Console at the URL `https://cm.example.com`, request `cm.example.com`.

---

**Note:** You can use Microsoft IIS to generate a server certificate request. If you do so, and your ISA Server uses default ports (80 and 443), be sure to disable IIS when you have completed this procedure. IIS interferes with ISA if both applications use the same ports.

---

2. Upload the request file to a Certificate Authority (CA).

---

**Note:** If the certificate needs to be trusted by mobile devices, purchase a certificate from a well-known trusted CA.

---

3. Download the certificate from the CA.
4. Import the certificate into the proxy server.

### Create a Secure Web Publishing Rule

ISA Server uses web publishing rules to publish web sites to the internet without compromising internal network security.

#### To create a secure web publishing rule:

1. From the console tree, expand **Arrays**.
2. Expand the machine name.
3. Right-click **Firewall Policy**, and click **New > Web Site Publishing Rule**.

4. Enter a name for the web publishing rule, and click **Next**.
5. Select **Allow**, and click **Next**.
6. Select **Publish a single Web site or load balancer**, and click **Next**.
7. Select **Use SSL to connect to the published Web server or server farm**, and click **Next**.
8. Enter the name of the web server.
9. Select **Use a computer name or IP address to connect to the published server**.
10. Enter the computer name or IP address of the internal machine.
11. Click **Next**.
12. Optional. Type /\* in the **Path** field, and click **Next**.
13. Complete the public name details using the URL you created, and click **Next**.
14. Click **New**.  
The New Web Listener Wizard opens.
15. Enter a web listener name, and click **Next**.
16. Do one of the following:
  - If you want to accept SSL connection requests from the clients:
    - Select **Require SSL secured connections with clients**.
    - Select **External**, and click **Next**.
    - Select **Use a single certificate for this Web Listener**, and click **Select Certificate**.
    - Select the appropriate server certificate, and click **Select > Next**.
  - If you do not want to accept SSL connection requests from the clients:
    - Select **Do not require SSL secured connections with clients**.
    - Select **External**, and click **Next**.
17. Select **No Authentication** from the drop-down box, and click **Next > Next**.
18. Review the settings, and click **Finish**.
19. Click **Next**.
20. Select **No Delegation, and client cannot authenticate directly**, and click **Next**.
21. Accept the defaults, and click **Next**.
22. Click **Finish**.

23. In the Firewall Policy Rules section, right-click the rule you just created, and click **Properties**.
24. Edit the following details:
  - On the **Bridging** tab, enter 7004 for the SSL port.
  - On the **Paths** tab, remove the default entry, and add the following entries:
 

```
/console-selfservice/*
                    /console-troubleshoot/*
                    /IMS-AA-IDP/*
                    /ctkip/*
```

---

**Note:** Select **Same as published folder** as the External Path for each entry.

---
25. Click **Apply**.

---

## Configuring External Machines

Make sure that the published URL domain name resolves to the proxy server external IP address. RSA recommends that you do this through the Domain Name System (DNS).

---

## Customizing E-mail Templates for Proxy Servers

If you set up a proxy server in your network DMZ to protect Authentication Manager, you must customize the e-mail notifications by replacing the URL for the authentication server with the information for the proxy server.

---

**Note:** When you set up secure web publishing, you create a server certificate on the application machine that contains a server certificate common name. Be sure to use the server certificate common name in the proxy server replacement tags.

---

Replace the default tags for the authentication server with the tags for the proxy server replacement listed in the following table.

Default E-mail Tag	Proxy Server Replacement Tag
<b>Request Approval E-mail Template - Hardware Token</b>	
Replace the CT-KIP URL and service address. (You do not need to delete the <code>#{MailComposer.CtkipURL}</code> tag in the e-mail template.)	To replace the CT-KIP URL and service address: <ol style="list-style-type: none"> <li>1. Click <b>Setup &gt; Component Configuration &gt; Authentication Manager &gt; Basic Settings</b>.</li> <li>2. Under CT-KIP Generation, replace the content of the <b>Token Key Generation URL</b> field with:  <code>https://&lt;server certificate common name&gt;/ctkip/trigger.jsp?dest url=http://www.rsasecurity.com</code></li> <li>3. Under CT-KIP Generation, replace the content of the <b>Service Address</b> field with:  <code>https://&lt;server certificate common name&gt;/ctkip/services/CtkipService</code></li> </ol>
<code>#{MailComposer.EnablementURL}</code>	<code>https://&lt;server certificate common name&gt;/console-selfservice/EnableToken.do?action=nvEnableToken</code>
<code>#{MailComposer.SelfserviceConsoleURL}</code>	<code>https://&lt;server certificate common name&gt;/console-selfservice</code>
<b>Request Approval E-mail Template - Software Token</b>	
Replace the CT-KIP URL and service address. (You do not need to delete the <code>#{MailComposer.CtkipURL}</code> tag in the e-mail template.)	To replace the CT-KIP URL and service address: <ol style="list-style-type: none"> <li>1. Click <b>Setup &gt; Component Configuration &gt; Authentication Manager &gt; Basic Settings</b>.</li> <li>2. Under <b>CT-KIP Generation</b>, replace the content of the <b>Token Key Generation URL</b> field with:  <code>https://&lt;server certificate common name&gt;/ctkip/trigger.jsp?dest url=http://www.rsasecurity.com</code></li> <li>3. Under CT-KIP Generation, replace the content of the <b>Service Address</b> field with:  <code>https://&lt;server certificate common name&gt;/ctkip/services/CtkipService</code></li> </ol>
<code>#{MailComposer.EnablementURL}</code>	<code>https://&lt;server certificate common name&gt;/console-selfservice/EnableToken.do?action=nvEnableToken</code>
<code>#{MailComposer.DownloadURL}</code>	Specify a link to the location where users can download the software token application.



---

Default E-mail Tag	Proxy Server Replacement Tag
<code>\${MailComposer.HelpLink}</code>	Add a link to the Help that describes how to use the software token application.
<code>\${MailComposer.SelfserviceConsoleURL}</code>	<code>https://&lt;server certificate common name&gt;/console-selfservice</code>
<b>Request Approval E-mail Template - On-Demand Tokencode Service</b>	
<code>\${MailComposer.SMSOttURL}</code>	<code>https://&lt;server certificate common name&gt;/console-self-service/OnDemandOTTLogin.do?action-nvPreEdit</code>
<b>Request Available E-mail Template</b>	
<code>\${MailComposer.WorkflowParticipantConsoleURL}</code>	<code>https://&lt;server certificate common name&gt;/console-ucm</code>
<b>Request Approval E-mail Template - Non-token</b>	
<code>\${MailComposer.SelfserviceConsoleURL}</code>	<code>https://&lt;server certificate common name&gt;/console-selfservice</code>

---

## Configuring a Proxy Server for RSA Authentication Manager Failover

In the case of failover, the administrator must immediately change the IP address associated with the server certificate to the new primary instance. This allows users to use the same URL when a primary instance is removed from a deployment and a replica is promoted. If this change is not made, the proxy server continues to try to access the original primary server, causing downtime for users.

© 2008 RSA Security Inc. All rights reserved.  
May 2008

### Trademarks

RSA and the RSA logo are registered trademarks of RSA Security Inc. in the United States and/or other countries. For the most up-to-date listing of RSA trademarks, go to [www.rsa.com/legal/trademarks\\_list.pdf](http://www.rsa.com/legal/trademarks_list.pdf). EMC is a registered trademark of EMC Corporation. All other goods and/or services mentioned are trademarks of their respective companies.