

RSA SecurID Wireless Authentication Solution Guide



Contact Information

See our web site for regional Customer Support telephone and fax numbers.

RSA Security Inc.
www.rsasecurity.com

RSA Security Ireland Limited
www.rsasecurity.ie

Trademarks

ACE/Agent, ACE/Server, Because Knowledge is Security, BSAFE, ClearTrust, Confidence Inspired, e-Titlement, IntelliAccess, Keon, RC2, RC4, RC5, RSA, the RSA logo, RSA Secured, the RSA Secured logo, RSA Security, SecurCare, SecurID, SecurWorld, Smart Rules, The Most Trusted Name in e-Security, Transaction Authority, and Virtual Business Units are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. All other goods and/or services mentioned are trademarks of their respective companies.

License agreement

This software and the associated documentation are proprietary and confidential to RSA Security, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright below. This software and any copies thereof may not be provided or otherwise made available to any other person.

Neither this software nor any copies thereof may be provided to or otherwise made available to any third party. No title to or ownership of the software or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA Security.

Note on encryption technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when exporting this product.

Distribution

Limit distribution of this document to trusted personnel.

RSA notice

The RC5™ Block Encryption Algorithm With Data-Dependent Rotations is protected by U.S. Patent #5,724,428 and #5,835,600.

Contents

Wireless Authentication Solution Guide	5
Supported Protocols and Methods	5
Choosing a Wireless Solution	6
Finding Supplemental Information	6
Deployment Steps for the RSA RADIUS Server Solution	7
RSA RADIUS Server With RSA EAP - Protected OTP	7
RSA RADIUS Server With PEAP	8
Deployment Steps for the Microsoft IAS RADIUS Server Solution.....	11
Microsoft IAS RADIUS Server With RSA EAP - Protected OTP.....	11
Microsoft IAS RADIUS Server With PEAP	12
Certificate Requirements.....	13
Requirements for the RSA RADIUS Solution	13
Requirements for the Microsoft Solution	14
Requirements for Remote RSA RADIUS Server Installation	15
Creation of a Node Secret for RSA RADIUS Servers.....	15
Refreshing the Node Secret on the RSA RADIUS Server.....	15
Refreshing the Node Secret Using a Command Line	16
Refreshing the Node Secret Using the RSA Security Center	16
Refreshing the Node Secret Using the Load Node Secret Utility.....	17
Authentication Environment Options	17

Wireless Authentication Solution Guide

This guide lists the steps for deploying the RSA SecurID for Microsoft Windows solution for wireless authentication. It also tells where to find detailed information about performing the steps.

Supported Protocols and Methods

RSA SecurID for Microsoft Windows supports the following network standards:

- IEEE 802.11i Security Enhancements
- IEEE 802.1x Authentication Protocol
- IETF RFC 3748 Extensible Authentication Protocol (EAP)
- Wi-Fi Alliance Wi-Fi Protected Access (WPA) specifications

RSA SecurID for Microsoft Windows supports the following protocols:

- 802.1x Authentication using EAP
- SecurID Authentication using the following EAP methods:
 - RSA EAP - Protected OTP
 - RSA Security EAP
- Generation of 128-bit encryption keys that can be used for 802.11i TKIP or AES data encryption
- Optional use of Protected EAP (PEAP) for additional security using PKI certificates
- RADIUS authentication servers that support the RSA EAP - Protected OTP and RSA Security EAP methods
- RSA EAP - Protected OTP support in the RSA Authentication Manager

RSA RADIUS Server supports other industry-standard EAP methods, such as TTLS.

Choosing a Wireless Solution

Wireless authentication requires users to provide valid RSA SecurID passcodes to establish wireless connections to protected networks. When a user attempts to establish a wireless connection, the RSA Authentication Agent prompts the user for RSA SecurID credentials. Authorized users establish connections easily, but unauthorized users are denied the connection.

You can deploy wireless authentication in the following types of environments:

- RSA EAP - Protected OTP
- PEAP

Within these environments, you can deploy:

RSA RADIUS Server. Uses RSA RADIUS Server, which is shipped with RSA Authentication Manager. This solution does not use the RSA Security Center to configure remote authentication.

Microsoft IAS RADIUS Server. Uses Microsoft IAS RADIUS Server. This solution uses the RSA Security Center to configure remote authentication.

For information to help you decide which wireless solution to deploy, see the *RSA SecurID for Microsoft Windows Planning Guide 1.1*.

Finding Supplemental Information

This guide lists general deployment steps for the wireless solutions. For detailed information about the steps listed in this guide, you need the following documents:

RSA Authentication Manager Documentation Set

- *RSA Authentication Manager 6.1 Installation Guide* for your platform.
- *RSA Authentication Manager 6.1 Administrator's Guide*
- RSA Authentication Manager 6.1 for Windows Help
- *RSA RADIUS Server 6.1 Administrator's Guide*
- *RSA RADIUS Server 6.1 Reference Guide*

RSA Authentication Agent Documentation Set

- *RSA SecurID for Microsoft Windows Planning Guide 1.1*
- RSA Security Center Help
- *RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide*

Microsoft Documentation

Microsoft Knowledge Base article #295663 "How to Import Third-Party Certification Authority (CA) Certificates into the Enterprise NTAAuth Store."

Deployment Steps for the RSA RADIUS Server Solution

RSA RADIUS Server With RSA EAP - Protected OTP

Steps	Where to Find Information
1. Install RSA Authentication Manager 6.1 and make sure it is running. Important: The Authentication Manager must be running before you install the remote RSA RADIUS Server. A remote RSA RADIUS Server is one that is installed on a computer other than a computer that hosts a primary or replica RSA Authentication Manager. For more information, see “Requirements for Remote RSA RADIUS Server Installation” on page 15.	The chapter “Installing the RSA Authentication Manager” in the <i>RSA Authentication Manager 6.1 Installation Guide</i> for your platform.
2. Assign at least one authenticator or password to the Authentication Manager administrator (the administrator who installed RSA Authentication Manager). Important: If you do not assign an authenticator or password to the Authentication Manager administrator before you install the remote RSA RADIUS Server, a node secret will not be created. For more information about the node secret, see “Creation of a Node Secret for RSA RADIUS Servers” on page 15.	The section “Node Secret” in the chapter “About RSA RADIUS Server in the <i>RSA RADIUS Server 6.1 Administrator’s Guide</i>.”
3. Synchronize the clocks on the RSA RADIUS Server host and the Authentication Manager host so that they are no more than three minutes apart.	The chapter “Changing System Parameters” in the <i>RSA Authentication Manager 6.1 Administrator’s Guide</i>.
4. Install RSA RADIUS Server. You can install RSA RADIUS Server on the computer that hosts the Authentication Manager or on a separate computer. When you install RSA RADIUS Server, the RSA RADIUS Server host is automatically registered in the Authentication Manager database as an Agent Host, and a node secret is automatically created.	The chapter “Installing the RSA RADIUS Server” in the <i>RSA RADIUS Server 6.1 Administrator’s Guide</i>.
5. Configure authentication protocols on the RSA RADIUS Server.	• The chapter “EAP Configuration Files” in the <i>RSA RADIUS Server 6.1 Reference Guide</i>. • “Tunneled Accounting” in the chapter “About RSA RADIUS Server in the <i>RSA RADIUS Server 6.1 Administrator’s Guide</i>.”

Steps	Where to Find Information
6. Restart the RSA RADIUS Server.	The platform specific sections in the chapter “Installing the RSA RADIUS Server” in the <i>RSA RADIUS Server 6.1 Administrator’s Guide</i> .
7. Install and configure RADIUS authentication on the wireless access points.	Documentation provided by your network access server software vendors.
8. Add users to the Authentication Manager database, and assign tokens to the users.	The RSA Authentication Manager Help topic “Adding a User.”
9. In the Authentication Manager database, configure user access for the RSA RADIUS Server Agent Host. To control access, you can add RADIUS users to groups and activate the groups on the Agent Hosts of your RADIUS clients.	The RSA Authentication Manager Help topics: • “Agent Host Activations” • “Memberships” • “Editing User Access Times”
10. Configure RSA RADIUS Server profiles on the Authentication Manager and RSA RADIUS Server.	• The RSA Authentication Manager Help topic “Adding a Profile.” • “Setting Up Profiles” in the chapter “Administering Profiles” in the <i>RSA RADIUS Server 6.1 Administrator’s Guide</i>.
11. Choose a client model, and enable users on the corresponding Agent Host.	• “Authentication Environment Options” on page 17 in this guide.
12. Install the RSA EAP Client component on the client computers.	• The chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows” in the <i>RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide</i>.

RSA RADIUS Server With PEAP

Steps	Where to Find Information
1. Install RSA Authentication Manager 6.1 and make sure it is running. Important: The Authentication Manager must be running before you install the remote RSA RADIUS Server. A remote RSA RADIUS Server is one that is installed on a computer other than a computer that hosts a primary or replica RSA Authentication Manager. For more information, see “Requirements for Remote RSA RADIUS Server Installation” on page 15.	The chapter “Installing the RSA Authentication Manager” in the <i>RSA Authentication Manager 6.1 Installation Guide</i> for your platform.

Steps	Where to Find Information
2. Assign at least one authenticator or password to the Authentication Manager administrator (the administrator who installed RSA Authentication Manager). Important: If you do not assign an authenticator or password to the Authentication Manager administrator before you install the remote RSA RADIUS Server, a node secret will not be created. For more information about the node secret, see “Creation of a Node Secret for RSA RADIUS Servers” on page 15.	The section “Node Secret” in the chapter “About RSA RADIUS Server in the <i>RSA RADIUS Server 6.1 Administrator’s Guide</i>.
3. Synchronize the clocks on the RSA RADIUS Server host and the Authentication Manager host so that they are no more than three minutes apart.	The chapter “Changing System Parameters” in the <i>RSA Authentication Manager 6.1 Administrator’s Guide</i>.
4. Install RSA RADIUS Server. You can install RSA RADIUS Server on the computer that hosts the Authentication Manager or on a separate computer. When you install RSA RADIUS Server, the RSA RADIUS Server host is automatically registered in the Authentication Manager database as an Agent Host, and a node secret is automatically created.	The chapter “Installing the RSA RADIUS Server” in the <i>RSA RADIUS Server 6.1 Administrator’s Guide</i>.
5. Configure authentication protocols on the RSA RADIUS Server.	• The chapter “EAP Configuration Files” in the <i>RSA RADIUS Server 6.1 Reference Guide</i>. • “Tunneled Accounting” in the chapter “About RSA RADIUS Server in the <i>RSA RADIUS Server 6.1 Administrator’s Guide</i>.
6. Get a certificate from a trusted certificate authority and import it to the RSA RADIUS Server host.	• For certificate requirements, see the section “Certificate Requirements” on page 13 in this guide. • For information about importing certificates, see Microsoft Knowledge Base article #295663 “How to Import Third-Party Certification Authority (CA) Certificates into the Enterprise NTAAuth Store.”
7. Restart the RSA RADIUS Server.	The platform specific sections in the chapter “Installing the RSA RADIUS Server” in the <i>RSA RADIUS Server 6.1 Administrator’s Guide</i>.
8. Install and configure RADIUS authentication on the wireless access points.	Documentation provided by your network access server software vendors.
9. Add users to the Authentication Manager database, and assign tokens to the users.	The RSA Authentication Manager Help topic “Adding a User.”

Steps	Where to Find Information
10. In the Authentication Manager database, configure user access for the RSA RADIUS Server Agent Host. To control access, you can add RADIUS users to groups and activate the groups on the Agent Hosts of your RADIUS clients.	The RSA Authentication Manager Help topics: • “Agent Host Activations” • “Memberships” • “Editing User Access Times”
11. Configure RSA RADIUS Server profiles on the Authentication Manager and RSA RADIUS Server.	• The RSA Authentication Manager Help topic “Adding a Profile.” • “Setting Up Profiles” in the chapter “Administering Profiles” in the <i>RSA RADIUS Server 6.1 Administrator’s Guide</i>.
12. Choose a client model, and enable users on the corresponding Agent Host.	• “Authentication Environment Options” on page 17 in this guide
13. Install the RSA EAP Client component on the client computers.	• The chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows” in the <i>RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide</i>.
14. Get a certificate from a trusted certificate authority and import it to the client computers.	• For certificate requirements, see the section “Certificate Requirements” on page 13 in this guide. • For information about importing certificates, see Microsoft Knowledge Base article #295663 “How to Import Third-Party Certification Authority (CA) Certificates into the Enterprise NTAAuth Store.”

Deployment Steps for the Microsoft IAS RADIUS Server Solution

Microsoft IAS RADIUS Server With RSA EAP - Protected OTP

Steps	Where to Find Information
1. Install RSA Authentication Manager 6.1.	The chapter “Installing the RSA Authentication Manager” in the <i>RSA Authentication Manager 6.1 Installation Guide</i> for your platform.
2. Install the RSA Authentication Agent Remote Authentication Server component on the Microsoft IAS Server host.	The chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows” in the <i>RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide</i> .
3. Add the Microsoft IAS Server host to the Authentication Manager database as a third-party RADIUS server Agent Host.	The RSA Authentication Manager Help topic “Configuring RADIUS Parameters.”
4. Create a node secret by performing a test authentication from the RSA Security Center on the Microsoft IAS Server host.	RSA Security Center Help topic “Testing Authentication.”
5. Configure authentication protocols on the RSA Authentication Agent Remote Authentication Server component host.	The chapter “Configuring Remote Authentication” in the <i>RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide</i> .
6. Restart the Microsoft IAS Server.	
7. Install and configure RADIUS authentication on the wireless network access points.	Documentation provided by your network access server software vendors.
8. Add users to the Authentication Manager database, and assign tokens to the users.	The RSA Authentication Manager Help topic “Adding a User”
9. In the Authentication Manager database, configure user access for the Microsoft IAS Server Agent Host. To control access, you can add RADIUS users to groups and activate the groups on the Agent Hosts of your RADIUS clients.	The RSA Authentication Manager Help topics: • “Agent Host Activations” • “Memberships” • “Editing User Access Times”
10. Choose a client model, and enable users on the corresponding Agent Host.	• “Authentication Environment Options” on page 17 in this guide
11. Install the RSA EAP Client component on the client computers.	• The chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows” in the <i>RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide</i>.

Microsoft IAS RADIUS Server With PEAP

Steps	Where to Find Information
1. Install RSA Authentication Manager 6.1.	The chapter “Installing the RSA Authentication Manager” in the <i>RSA Authentication Manager 6.1 Installation Guide</i> for your platform.
2. Install the RSA Authentication Agent Remote Authentication Server component on the Microsoft IAS Server host.	The chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows” in the <i>RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide</i> .
3. Add the Microsoft IAS Server host to the Authentication Manager database as a third-party RADIUS server Agent Host.	The RSA Authentication Manager Help topic “Configuring RADIUS Parameters.”
4. Create a node secret by performing a test authentication from the RSA Security Center on the Microsoft IAS Server host.	RSA Security Center Help topic “Testing Authentication.”
5. Configure authentication protocols on the RSA Authentication Agent Remote Authentication Server component host.	The chapter “Configuring Remote Authentication” in the <i>RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide</i> .
6. Get a certificate from a trusted certificate authority and import it to the Microsoft IAS Server host.	- For certificate requirements, see the following section “Certificate Requirements.” - For information about importing certificates, see Microsoft Knowledge Base article #295663 “How to Import Third-Party Certification Authority (CA) Certificates into the Enterprise NTAAuth Store.”
7. Restart the Microsoft IAS Server.	
8. Install and configure RADIUS authentication on the wireless network access points.	Documentation provided by your network access server software vendors.
9. Add users to the Authentication Manager database, and assign tokens to the users.	The RSA Authentication Manager Help topic “Adding a User.”
10. In the Authentication Manager database, configure user access for the Microsoft IAS Server Agent Host. To control access, you can add RADIUS users to groups and activate the groups on the Agent Hosts of your RADIUS clients.	The RSA Authentication Manager Help topics: “Agent Host Activations” “Memberships” “Editing User Access Times”
11. Choose a client model, and enable users on the corresponding Agent Host.	“Authentication Environment Options” on page 17 in this guide.
12. Install the RSA EAP Client component on the client computers.	The chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows” in the <i>RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide</i>.

Steps	Where to Find Information
13. Get a certificate from a trusted certificate authority and import it to the client computers.	- For certificate requirements, see the section “Certificate Requirements” on page 13. - For information about importing certificates, see Microsoft Knowledge Base article #295663 “How to Import Third-Party Certification Authority (CA) Certificates into the Enterprise NTAAuth Store.”

Certificate Requirements

When you use wireless authentication with Protected Extensible Authentication Protocol (PEAP) and Tunnelled Transport Layer Security (TTLS), both servers and clients use certificates to verify their identities to one another.

Requirements for the RSA RADIUS Solution

Server Certificates

Server certificates must meet the following requirements:

- The certificate must be in PKCS#12 .pfx file format with a private key and all of the certificates necessary to establish the chain to the issuing certificate authority (CA).
- The certificates cannot be self-signed.
- The **certinfo.ini** file in the **/RADIUS/service** directory on the RSA RADIUS Server host must point to the .pfx file.
- Key usage must be set in one of the following ways:
 - Key usage unspecified.
 - digitalSignature** or **keyEncipherment** is set with either no extended key usage or **serverAuth**, **msSGC** or **nsSGC**.

Client Certificates

Client certificates must meet the following requirements:

- Key usage must be set in one of the following ways:
 - Key usage unspecified.
 - digitalSignature** is set with either no extended key usage or **clientAuth** is specified.
- If the certificate is a Netscape certificate, the client bit must be set. If the certificate is a CA certificate only, select only extended key usage.

Requirements for the Microsoft Solution

All certificates must meet the following minimum requirements:

- X.509 format
- Secure Sockets Layer (SSL) encryption
- Transport Layer Security (TLS) encryption

Additionally, all certificates must be configured with at least one purpose object identifier. For example, a certificate that is used to authenticate from a client to a server must be configured with the Client Authentication purpose. The purpose is recorded in the certificate's Extended Key Usage (EKU) extension. During authentication, the authenticator examines the certificate to verify that its purpose object identifier matches the way the certificate is being used.

Server Certificates

Server certificates must meet the following requirements:

- The certificate must chain to one of the following:
 - A trusted Microsoft root CA.
 - A Microsoft standalone root or third-part root certificate authority in an Active Directory domain. The Active Directory domain must have an NTAuthCertificates store that contains the published root certificate.
- If the certificate is a Netscape certificate, the client bit must be set. If the certificate is a CA certificate only, extended key usage must be selected.
- The certificate must be configured with the Server Authentication purpose.
- The certificate must pass the checks that are performed by the CryptoAPI certificate store, and must pass all of the requirements in the remote access policy.
- The name in the subject line of the certificate must match the name that is configured for the connection on the client.
- The Subject Alternative Name (SubjectAltName) extension contains the fully qualified domain name of the server.

If a client is configured to trust a specific server certificate by name, users are prompted to decide whether to trust certificates with different names. If a user rejects a certificate, authentication fails. If the user accepts the certificate, the certificate is added to the trusted root store on the user's computer.

Client Certificates

Client certificates must meet the following requirements:

- The certificate must be issued by an enterprise CA or must map to a user account or computer account in Active Directory.
- The user or the computer certificate on the client must chain to a trusted root CA.
- The certificate must include the Client Authentication purpose.
- The certificate must pass the checks that are performed by the CryptoAPI certificate store, and must pass all of the requirements in the remote access policy.

- The certificate must pass the certificate object identifier checks that are specified in the Internet Authentication Service (IAS) remote access policy.
- The certificate must not be a registry-based smart card certificate or a certificate that is protected with a password.
- The Subject Alternative Name (Subject AltName) extension in the certificate must contain the user principal name (UPN) of the user.

Requirements for Remote RSA RADIUS Server Installation

A remote RSA RADIUS Server is one that is installed on a computer other than a primary or replica RSA Authentication Manager host. The RSA RADIUS Server installation process adds an Agent Host record for the RADIUS Server to the Authentication Manager database, and generates a node secret and delivers it to the RADIUS Server. For this process to occur, before you install RSA RADIUS Server:

- The RSA Authentication Manager must be running.
- The clocks on the RSA RADIUS Server host and the Authentication Manager host must be synchronized so that they are no more than three minutes apart.
- One or more authenticators or a password must be assigned to the Authentication Manager administrator.

Creation of a Node Secret for RSA RADIUS Servers

The node secret is a symmetric encryption key used by RSA Authentication Manager and RSA Authentication Agent to encrypt and decrypt packets of data as they travel across the network.

Ordinarily, the node secret is created during initial authentication. However, RSA RADIUS Servers use a protocol that prevents a node secret from being created during authentication. Therefore, node secrets for RSA RADIUS Servers are automatically created when the RSA RADIUS Server is installed. For creation of the node secret to occur, before you install a remote RSA RADIUS Server, the RSA Authentication Manager must be running, and one or more authenticators or a password must be assigned to the Authentication Manager administrator.

Refreshing the Node Secret on the RSA RADIUS Server

You can refresh the node secret on the RSA RADIUS Server using one of the following methods:

- Use a command line to reregister the RSA RADIUS Server as an Agent Host in the Authentication Manager database.
- Install the Local Authentication Client component on the computer that hosts the RSA RADIUS Server, and use the RSA Security Center to update the node secret.
- Manually generate a new node secret and deliver it to the RSA RADIUS Agent Host.

Refreshing the Node Secret Using a Command Line

To reregister the RSA RADIUS Server in the Authentication Manager using a command line:

1. Stop the RSA RADIUS service on the RSA RADIUS Server host.
2. Log on to the RSA RADIUS Server as an administrator.
3. On the RADIUS Server host, navigate to the `\service` directory.
For Windows, by default, the full path to this directory is `C:\Program Files\RSA Security\RSA RADIUS\radius\service` directory.
For UNIX, by default, the full path to this directory is `/opt/rsa/radius`.
4. At a command line, do one of the following:
 - Regenerate the node secret for a Primary RADIUS Server by entering the following command:

```
# rsainstalltool -identity PRIMARY
```
 - Regenerate the node secret for a Replica RADIUS Server by entering the following command:

```
# rsainstalltool -identity REPLICA
```
5. Restart the RSA RADIUS service.

Refreshing the Node Secret Using the RSA Security Center

Remote authentication with RSA RADIUS Server does not require an Authentication Agent component on the RSA RADIUS Server host, and does not use the RSA Security Center to configure remote authentication. However, you may want to install (but not configure) the Local Authentication Client component on the computer that hosts RSA RADIUS Server to provide a way to easily manage the node secret.

To refresh the node secret on the RSA RADIUS Server host using the RSA Security Center:

1. Install the Local Authentication Client component on the computer that hosts RSA RADIUS Server.
2. To open the RSA Security Center, click **Start > Programs > RSA Security > RSA Security Center**.
3. In the left pane of the RSA Security Center, click **Advanced Settings**.
4. On the Advanced Settings page, under **Node Secret**, click **Clear**.
5. Click **OK**.
6. Clear the node secret for this Authentication Agent Host from the RSA Authentication Manager database.
7. Restart the computer.

8. In the left pane of the RSA Security Center, click **Configuration > Authentication Test**.
9. On the Authentication Test page, under **Direct Authentication Test**, click **Test**. Testing authentication replaces the node secret in the Authentication Manager database.

Refreshing the Node Secret Using the Load Node Secret Utility

The Load Node Secret utility (**agent_nsload**) is stored in the **ACEPROG** directory on the RSA Authentication Manager host.

Using this procedure, you create the node secret from the RSA Authentication Manager and load it to the RSA RADIUS Server host.

To refresh the node secret using the Load Node Secret utility:

1. To create a node secret for the RSA RADIUS Server, on the RSA Authentication Manager main menu, click **Agent Host > Add (or edit) Agent Host > Create Node Secret**.
2. Copy the Windows version of **agent_nsload** from the **ACEPROG** directory on the Authentication Manager host to the RSA RADIUS Server host.

RSA Security provides four platform-specific versions of the utility:

- Windows
- Solaris
- HP-UX
- IBM AIX
- LINUX

3. From a command line on the RSA RADIUS Server host, run the Load Node Secret utility by typing the following command:

```
agent_nsload -f path -p directory
```

where:

- *path* is the directory location and name of the node secret file
- *password* is the password used to protect the node secret file

Authentication Environment Options

You can set up your environment so that authentication works in one of the following ways:

- Authentication occurs on the RSA RADIUS Server or Microsoft IAS Server on behalf of network access devices such as a Remote Access Server (RAS), a Network Access Server (NAS), or a wireless access point.
- Authentication occurs only on the RSA RADIUS Server or Microsoft IAS Server themselves.

The following table describes the differences between these setups:

Method	Configuration Requirements	Benefits
Authentication occurs on behalf of the network access devices.	Register the following components as Agent Hosts in the RSA Authentication Manager database: • Each network access device • RSA RADIUS Server	• Access control per device. For example, you can specify the network access device through which users or groups of users can access the network. • Authentication events recorded in the Authentication Manager are specific to each network access device.
Authentication occurs only the server itself.	Register the server as an Agent Host in the RSA Authentication Manager database. When you install RSA RADIUS Server, registration occurs automatically. However, you must register Microsoft IAS Server manually.	Less administrative burden.

By default, the environment is configured so that authentication occurs on behalf of network access devices. You can change the default so that authentication occurs only on the Microsoft IAS Server or RSA RADIUS Server itself.

To change the default setup on the RSA RADIUS Server:

1. On the RSA RADIUS Server host, use a text editor to open the **securid.ini** file. This file is located, by default, in the **C:\Radius\Service** directory. However, the RSA Authentication Manager installation enables you to put this file in another location.
2. Edit the file so that the **CheckUserAllowedByClient** line appears as follows:


```
CheckUserAllowedByClient = 0
```

 Changing the value to 0 configures the environment so that authentication occurs only on the RSA RADIUS Server itself.
3. Restart RSA RADIUS Server for the changes to take effect.

To change the default setup on the Microsoft IAS Server:

1. On the Microsoft IAS Server host, open RSA Security Center.
2. On the **Configuration** tab, click **Remote > EAP**.
3. On the EAP Configuration page, under **Authentication Settings**, click **Settings**.
4. On the Authentication Settings page, clear **Enable RADIUS client check**.
Clearing **Enable RADIUS client check** configures the environment so that authentication occurs only on the Microsoft IAS Server itself.