



RSA SecurID Ready Implementation Guide

Last Modified: 10/24/2003

1. Partner Information

Partner Name	Apple Computer, Inc.
Web Site	www.apple.com
Product Name	Mac OS X Server
Version & Platform	v. 10.3
Product Description	MAC OS X Server provides a Virtual Private Network (VPN) service allowing users to access their corporate network over the Internet. The VPN service currently supports L2TP/IPSec and PPTP protocols
Product Category	Perimeter Defense

2. Contact Information

	Sales Contact	Support Contact
E-mail	sales@apple.com	support@apple.com
Phone		
Web	www.apple.com/sales	www.apple.com/support

3. Solution Summary

Feature	Details
Authentication Methods Supported	EAP with ACE
ACE/Agent Library Version	Version #5.1
ACE 5 Locking	Yes
Replica ACE/Server Support	Full Replica Support
Secondary RADIUS/TACACS+ Server Support	No
Location of Node Secret on Client	/var/ace
ACE/Server Agent Host Type	UNIX
SecurID User Specification	All users
SecurID Protection of Administrators	No

4. Product Requirements

- *Hardware requirements*

Mac OS X Server v. 10.3 is supported on the following hardware machines:

- Xserve
- Macintosh Server G3 or G4
- iMac or eMac

A minimum of 128MB of RAM.

A minimum of 8GB of available disk space.

- *Software requirements*

The Apple Virtual Private Networking (VPN) software is included with Mac OS X Server v10.3 & Mac OS X v10.3 (client). Client operating systems that support EAP-SecurID with L2TP over IPsec or PPTP can connect to Mac OS X Server v10.3. These clients include Mac OSX 10.3.x and Windows.

5. Partner ACE/Agent configuration

The Apple VPN software is installed by default with Mac OS X Server v10.3. Configuration of standard VPN services is done via the Server Admin application.

Using SecurID VPN Authentication

It is not possible to choose your authentication method using Server Admin. To use RSA Security's SecurID authentication, you will need to change the VPN configuration manually. Make sure VPN Service is disabled before configuring the authentication method.

To manually configure Mac OS X Server to use RSA Security's SecurID authentication:

1. Create the directory `/var/ace` on your Mac OS X Server.

```
cd/
```

```
sudo mkdir var/ace
```

2. Copy the SecurID configuration file `sdconf.rec` from your SecurID server to the `/var/ace` directory.
3. Enable EAP-SecurID authentication. Type the following commands in the Terminal, one at a time:

```
serveradmin settings vpn:Servers:com.apple.ppp.l2tp:PPP:AuthenticatorEAPPlugins:_array_index:0="EAPRSA"
```

```
serveradmin settings vpn:Servers:com.apple.ppp.l2tp:PPP:AuthenticatorProtocol:_array_index:0="EAP"
```

Once SecurID has been manually configured, continue to configure VPN service using Server Admin.

Enabling and Configuring the L2TP Transport Protocol

Use Server Admin to enable the L2TP transport protocol. When enabling this protocol, you must also configure the connection settings. You must designate an IPsec shared secret, the IP address allocation range to be assigned to your clients, and groups to be allowed VPN privileges (if desired).

To enable L2TP:

1. In Server Admin, choose the VPN Service from the Computers & Services list.
2. Click Settings.
3. Select the General tab.
4. Select L2TP.
5. Enter the shared secret.
6. Set the beginning IP address of the allocation range.
7. Set the ending IP address of the allocation range.
8. Enter the group that has access to VPN login.

You can use the Users & Groups button to browse for a group. If you leave this blank, all workgroups will have access to VPN login.

Enabling and Configuring the PPTP Transport Protocol

Use Server Admin to enable the PPTP transport protocol. When enabling this protocol, you must also configure the connection settings. You should designate an encryption key length (40-bit in addition to 128-bit), the IP address allocation range to be assigned to your clients, and groups to be allowed VPN privileges (if desired).

To enable PPTP:

1. In Server Admin, choose the VPN Service from the Computers & Services list.
2. Click Settings.
3. Select the General tab.
4. Select PPTP.
5. If desired, check “Allow 40-bit encryption keys” to allow such keys to be used in addition to 128-bit keys.

Warning: Allowing 40-bit encryption is less secure, but may be necessary for some VPN client applications.

6. Set the beginning IP address of the allocation range.
7. Set the ending IP address of the allocation range.
8. Enter the group that has access to VPN login.
You can use the Users & Groups button to browse for a group. If you leave this blank, all workgroups will have access to VPN login.
9. Click Save.

Configuring Additional Network Settings for VPN Clients

When a user connects to your server through VPN, that user is given an IP address from your allocated range. The user will also be automatically given DNS addresses and search domains from the server’s configuration. If you wish to provide the client with a different set of DNS addresses or search domains, you will need to configure these settings. These settings include the DNS addresses, network masks, and search domains.

To configure addition network settings:

1. In Server Admin, choose the VPN Service from the Computers & Services list.
2. Click Settings.
3. Select the Client Information tab.
4. Enter the IP address of the DNS server.
5. Enter any search domains, as needed.
6. Click Save.

Configuring Network Routing Definitions

Network routing definitions allows you to specify routes be installed in the client to control what data is sent through the VPN tunnel. For example, you may want traffic that goes to your IP address range be routed through the tunnel to your LAN but all other traffic to be routed through the users normal, unsecured internet connection. This helps provide a finer control over what goes through the VPN tunnel. These definitions are unordered, and the network mask is used to determine how specific a route is. Packets will be routed using the most specific route.

To set routing definitions:

1. In Server Admin, choose the VPN Service from the Computers & Services list.
2. Click Settings.
3. Select the Client Information tab.
4. Click the Add button below the routing definition list.
5. Enter the routing address.
6. Enter the network mask for the route.
7. Select the routing destination from the popup menu
 - Private means to route it through the VPN tunnel.
 - Public means to use the normal interface with no tunnel.

Starting or Stopping VPN service

You use Server Admin to start and stop VPN service.

To start or stop VPN service:

1. In Server Admin, choose the VPN Service from the Computers & Services list.
2. Make sure at least one of the transport protocols is checked and configured.
3. Click Start Service or Stop Service.
 - When the service is turned on, the Stop Service button is available.

6. Certification Checklist

Date Tested: <09/12/2003>

Product	Tested Version
ACE/Server	5.0 for Windows NT and Windows 2000
Mac OS X Server	v.10.3

Test	ACE	RADIUS
1st time auth. (node secret creation)	<input type="text" value="P"/>	<input type="text" value="N/A"/>
New PIN mode:		
System-generated		
Non-PINPAD token	<input type="text" value="P"/>	<input type="text" value="N/A"/>
PINPAD token	<input type="text"/>	<input type="text" value="N/A"/>
User-defined (4-8 alphanumeric)		
Non-PINPAD token	<input type="text" value="P"/>	<input type="text" value="N/A"/>
Password	<input type="text"/>	<input type="text" value="N/A"/>
User-defined (5-7 numeric)		
Non-PINPAD token	<input type="text" value="P"/>	<input type="text" value="N/A"/>
PINPAD token	<input type="text"/>	<input type="text" value="N/A"/>
SoftID token	<input type="text"/>	<input type="text" value="N/A"/>
Deny 4 digit PIN	<input type="text" value="P"/>	<input type="text" value="N/A"/>
Deny Alphanumeric	<input type="text" value="P"/>	<input type="text" value="N/A"/>
User-selectable		
Non-PINPAD token	<input type="text" value="F"/>	<input type="text" value="N/A"/>
PINPAD token	<input type="text"/>	<input type="text" value="N/A"/>
PASSCODE		
16 Digit PASSCODE	<input type="text" value="P"/>	<input type="text" value="N/A"/>
4 Digit Password	<input type="text" value="P"/>	<input type="text" value="N/A"/>
Next Tokencode mode		
Non-PINPAD token	<input type="text" value="P"/>	<input type="text" value="N/A"/>
PINPAD token	<input type="text"/>	<input type="text" value="N/A"/>
Replica Servers	<input type="text" value="P"/>	<input type="text" value="N/A"/>
User Lock Test (ACE Lock Function)	<input type="text" value="P"/>	<input type="text" value="N/A"/>
No ACE/Server	<input type="text" value="P"/>	<input type="text" value="N/A"/>

JGS

Pass, Fail or N/A (N/A=Non-available function)

7. Known Issues

User-selectable mode has been implemented to always default to system-generated mode.