

Solution Brief

---

**Managing Token-  
Based Access to  
Wireless LANs**

---

Many enterprises elect to control access to their networks by deploying a two-factor user authentication system such as RSA Authentication Manager. These systems provide stronger security than that provided by static passwords alone.

While such token systems have most commonly been used to authenticate remote users to the enterprise networks, more and more security-conscious enterprises wish to use them to govern access to their WLANs as well.

Now you can, by using Juniper Network's WLAN security solutions Odyssey® and Steel-Belted Radius® in conjunction with RSA Authentication Manager. This joint solution lets you require strong two-factor authentication for some or all of your

WLAN access – so you can strictly govern who can connect to your WLAN, set up the security scheme that makes sense for your WLAN access, and, if pertinent, leverage your existing RSA deployment for WLAN security as well.

Plus, you'll be afforded all the benefits that a Juniper Networks WLAN security solution provides, including strong credential and data security on the wireless link to prevent wireless eavesdropping and other attacks; multi-platform, multi-vendor support to ensure compatibility in any network environment; and easy roll out of the WLAN access client across your entire network to significantly minimize deployment and support costs.

### **With the joint Juniper Networks/RSA WLAN security solution, you can:**

- Implement strong, two-factor authentication access control to your wireless LAN – no need to rely on static passwords that may be easily compromised
- Prevent unauthorized access to your WLAN – invalid SecurID tokens will be denied, and both credentials and corporate data are fully protected as they travel over the wireless link
- Leverage your existing token installation, and enforce the same high level of security for WLAN users as you require for remote users
- Enforce different security requirements for different areas of the network – SecurID authentication for those with the highest information privileges, and Windows, LDAP, or SQL for others
- Seamlessly integrate WLAN authentication and security into your existing network environment without upgrading or changing your authentication infrastructure
- Enable SecurID authentication from any wireless device, including Windows XP/2000/98/Me/Pocket PC
- Protect your investment against obsolescence, by implementing WLAN security based on the market-leading token system and the industry-standard 802.1X protocol.

Juniper Network's complete suite of 802.1X-based WLAN security solutions include:

- **Odyssey Access Client** – Juniper Network's 802.1X WLAN access client lets users securely connect to the WLAN. OAC supports EAP-TTLS, EAP-PEAP, EAP-TLS, and Cisco's EAP-FAST and LEAP, and runs on Windows XP/2000/98/Me/ Pocket PC. This multiprotocol, multi-platform support, plus advanced pre-configuration and usability features, make OAC ideally suited to enterprise-wide deployment.
- **Odyssey Access Server or SBR** – Market-leading RADIUS servers which communicate with WLAN access points to authenticate WLAN users against the RSA Authentication Manager (or other authentication method) and set up their secure connections. OAS and SBR support EAP-TTLS, EAP-PEAP, EAP-TLS, and Cisco's LEAP.

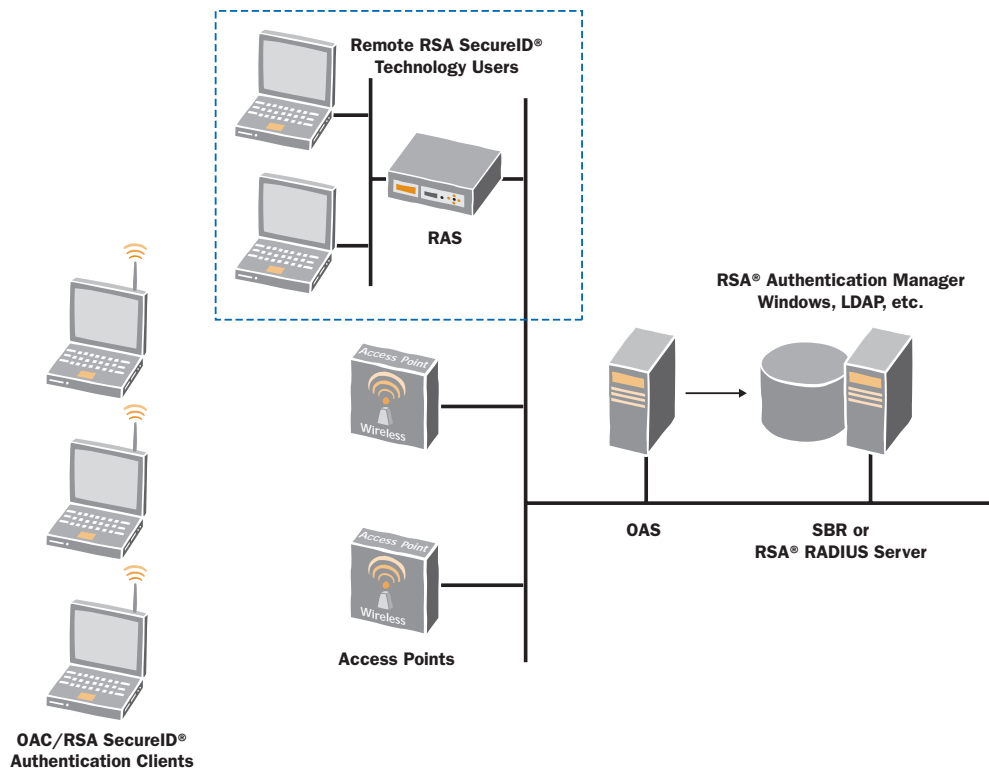
**SBR** can authenticate WLAN and remote access users against RSA Authentication Manager, Windows, Solaris, SQL, or LDAP.

**OAS** can authenticate WLAN users against Windows, or can forward authentication requests to SBR or other compatible RADIUS server for authentication against the RSA Authentication Manager or other non-Windows authentication method.

These solutions alone provide strong WLAN security, and protect your network in the following ways:

- Only authorized users can connect – if login credentials aren't valid, access to the network will be denied
- Users' login credentials are safe from attack as they travel over the wireless link if you are using EAP-TTLS or EAP-PEAP
- Data sent over the wireless connection is securely encrypted, using your choice of encryption protocols (WEP or Wi-Fi Protected Access)
- WLAN users cannot be duped into connecting to a bogus network

When used with RSA Authentication Manager, these solutions provide even stronger access control, relying on dynamic tokens to authenticate users to the network rather than static passwords. Users will connect as usual, except they are required to present their SecurID token (and next token, if required) for authentication by the RSA Authentication Manager.



Juniper Network's WLAN security solutions Odyssey and SBR allow wireless SecurID users to connect to the network and be authenticated against the RSA Authentication Manager.



CORPORATE HEADQUARTERS  
AND SALES HEADQUARTERS  
FOR NORTH AND SOUTH AMERICA

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
Phone: 888-JUNIPER (888-586-4737)  
or 408-745-2000  
Fax: 408-745-2100

[www.juniper.net](http://www.juniper.net)

EAST COAST OFFICE

Juniper Networks, Inc.  
10 Technology Park Drive  
Westford, MA 01886-3146 USA  
Phone: 978-589-5800  
Fax: 978-589-0800

ASIA PACIFIC REGIONAL  
SALES HEADQUARTERS

Juniper Networks (Hong Kong) Ltd.  
Suite 2507-11, Asia Pacific Finance Tower  
Citibank Plaza, 3 Garden Road  
Central, Hong Kong  
Phone: 852-2332-3636  
Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA  
REGIONAL SALES HEADQUARTERS

Juniper Networks (UK) Limited  
Juniper House  
Guildford Road  
Leatherhead  
Surrey, KT22 9JH, U. K.  
Phone: 44(0)-1372-385500  
Fax: 44(0)-1372-385501