

Juniper Networks Odyssey Access Server

Juniper Networks Odyssey Access Server (OAS) is a RADIUS server customized to handle wireless LAN (WLAN) access control and security. Based on the IEEE security standard 802.1X, and with full support for tunneled EAP methods, OAS provides the strong WLAN security you need to protect your network against the known hazards of wireless

computing. With OAS, you can centralize the authentication and security of all WLAN users on your network. You'll be able to ensure that only authorized wireless users can connect to your network, and that their connections are securely configured.

Juniper's OAS is a good fit in a variety of different deployments. In small-to-medium sized deployments, OAS lets you authenticate WLAN users directly against your Windows Active Directory database. Users simply log in with their Windows credentials to securely access the WLAN. If you're in a larger enterprise, you can distribute OAS to autonomous networks to handle large traffic loads and improve user response time. In a distributed scenario, OAS can authenticate users locally against Active Directory, or forward authentication requests to Steel-Belted Radius or other compatible RADIUS server for centralized authentication against non-Windows systems such as an LDAP directory or token system.

OAS also provides unsurpassed multi-vendor compatibility. It works with any wireless equipment that is 802.1X-compatible, and can handle connection requests from any 802.1X supplicant, including Juniper Network's Odyssey Access Client. OAS reflects the reliability, high-performance operation, and interoperability that are the hallmarks of Juniper Networks market-leading Steel-Belted Radius RADIUS/AAA server. With its simple setup and support for strong WLAN security protocols, OAS puts secure WLAN access within any organization's reach.

Secure Wireless Access to Enterprise Resources

OAS is based on the 802.1X IEEE standards and supports a wide variety of 802.1X security methods, including EAP-TTLS, EAP-PEAP, EAP-TLS, and Cisco's LEAP.

Windows Authentication

OAS can safely authenticate WLAN users directly against your existing Windows Domain or Active Directory database, and it includes full support for user and group designations.

Distributed Enterprise WLAN Authentication

OAS can communicate with Juniper Networks SBR or other 802.1X-compatible RADIUS server to authenticate WLAN users in branch offices or distributed departments against a central security infrastructure that is not based on Windows. This includes popular methods such as SQL/LDAP databases and two-factor authentication systems such as RSA Security's Authentication Manager.

Proven and Trusted Interoperability

OAS supports all 802.1X-capable access equipment—for ensured compatibility in your network environment.

System Requirements

OAS runs in Windows XP, 2000.