Odyssey® Client

Secure, Low-Overhead 802.1X Access Client

Key Benefits

- **Secure, easily managed WLAN and wired 802.1X access for the enterprise**
- **Low-overhead solution; easily deployed and managed enterprise-wide**
- **Enforce enterprise security policies, for the strongest protection of your network**
- **Supports multiple strong WLAN security protocols, including EAP-TTLS, which provide credential and data security, plus mutual authentication of client and server**
- **Supports Wi-Fi Protected Access (WPA) and WPA2 for strongest data security**
- **Safely authenticate WLAN and 802.1X wired users against any back-end authentication database, for administrative simplicity**
- **Simple user experience ensures rapid adoption, low support costs**
- **Multi-vendor, multiplatform support ensures compatibility in your network environment**
- **Used with Odyssey Server, Steel-Belted Radius,® or any other RADIUS server which supports WLAN security protocols**

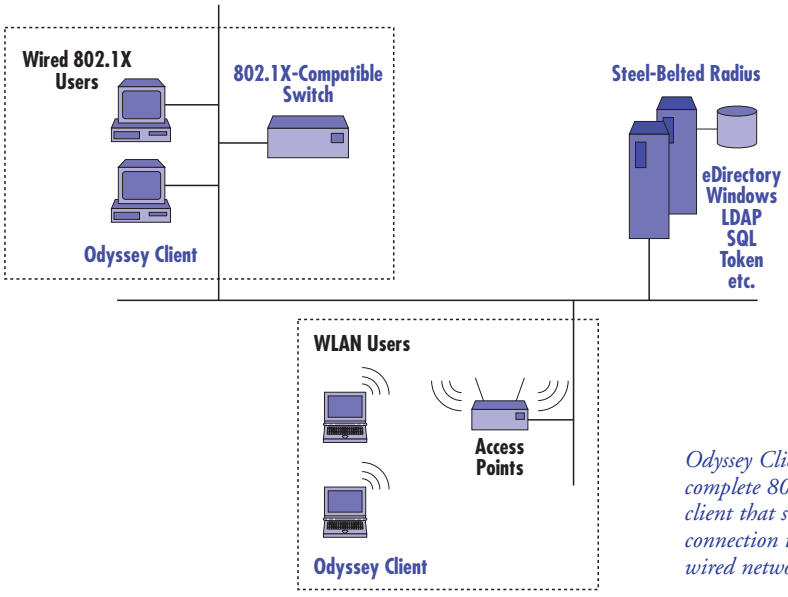
Odyssey Client is an enterprise-class 802.1X access client that provides state-of-the-art security to protect your network, is easily deployed across all your desktop and handheld devices for the lowest overhead, and gives you a fine level of control over how users can connect to the network – so you can mandate compliance with your company's security policies.

Based on the IEEE security standard 802.1X and with full support for advanced WLAN security protocols, Odyssey Client provides the strong security you require for wireless access to your LAN. Together with an 802.1X-compatible RADIUS server such as Funk Software's Odyssey Server or Steel-Belted Radius®, Odyssey Client secures the authentication and connection of WLAN users, ensuring that only authorized users can connect, that login credentials will not be compromised, and that data privacy will be maintained over the wireless link.

In addition to its strong security, Odyssey Client carries an exceptionally low total cost of ownership. With its combination of auto-configuration tools, client update capabilities, and unsurpassed multi-platform, multi-vendor compatibility, it is easily deployed enterprise-wide, whether you are installing it on 50 or 5,000 devices.

And, Odyssey Client provides a simple, straightforward user experience, whether a user is connecting to the enterprise network or to a public WLAN at an airport, coffee shop, or other hotspot. Its intuitive operation and numerous usability conveniences allow users to easily connect wherever they are – minimizing the demands placed on your support and training organizations.

What's more, Odyssey Client lets you control how your users connect to the network. Its Client lockdown capabilities let you prevent end users from changing their configurations, and integration with endpoint integrity solutions such as those from Check Point let you mandate and enforce your company's security policies, and provide strong protection for your network.



Odyssey Client is a complete 802.1X access client that supports secure connection to wireless or wired networks.

Preliminary

Odyssey Client

Finally, Odyssey Client is an ideal client for enterprises that are deploying identity-based (wired 802.1X) networking. Odyssey Client fully supports wired 802.1X connections, and saves time and effort by permitting one-time deployment of wireless and wired 802.1X access. The use of a single interface for both functions also simplifies user experience and reduces costs associated with user training.

With its emphasis on secure network access, easily implemented, Odyssey Client can be deployed with confidence in any organization.

Enterprise-Level Security

Odyssey Client runs on Windows XP, 2000, 98, Me, and Windows Mobile 2003 for Pocket PC and lets a user securely connect to a wireless or wired 802.1X network. It is compatible with Odyssey Server, Steel-Belted Radius, or any other EAP-compatible RADIUS server.

Odyssey Client supports a wide variety of WLAN security (EAP) authentication types, including EAP-TTLS, EAP-PEAP, EAP-TLS, Cisco's EAP-FAST and LEAP, EAP-SIM, and EAP-MD5.

The choice of EAP authentication method for your 802.1X deployment is critical: your network's security depends on it. We recommend that you use an EAP method which provides the strongest security, such as EAP-TTLS, EAP-PEAP, or EAP-TLS. These methods protect your network in three key ways:

- First, they fully protect your users' credentials against attack on the wireless link, preventing stolen passwords.
- Second, they provide for distribution of encryption keys to users and access points, and for re-keying during a WLAN session to protect data privacy and guard against wireless eavesdropping.
- Third, they provide "mutual authentication" of client and server, to ensure that users are connecting to a legal network, preventing man- in-the-middle attacks and other forms of hacking.

Each of these security capabilities is described below.

- **Credential Security:** EAP-TTLS and EAP-PEAP use TLS (Transport Layer Security, the successor to SSL) as the underlying strong cryptography. With both protocols, the user is authenticated to the network using ordinary password-based credentials, whose use is made proof against active and passive attack by enclosing it in the TLS security wrapper.

  EAP-TLS also relies on TLS as the underlying strong cryptography; it requires the use of client-side certificates for authentication.

- **Data Privacy:** With all three protocols, as a result of user authentication, session keys are distributed to encrypt the wireless connection and enable data privacy between client and access point.

  For the strongest over-the-air encryption of wireless data, Odyssey Client supports the advanced encryption protocols Wi-Fi Protected Access (WPA) and WPA2 across all platforms. WPA uses the Temporal Key Integrity Protocol (TKIP); WPA2 is based on the encryption algorithm AES.

- **Mutual authentication of client and server:** Finally, all three protocols ensure that WLAN users can only connect to legal networks. In particular, clients will only be able to connect to access points that are associated with a RADIUS server which presents a trusted certificate; access points only communicate with RADIUS servers they've been configured to know about; the RADIUS server only trusts an access point it's been configured to know about and with which it shares a secret password; access points only trust RADIUS server responses which have been signed.

Selecting the right EAP method is not just about security, however. These protocols differ in how easy they are to manage, and in the range of authentication databases they support.

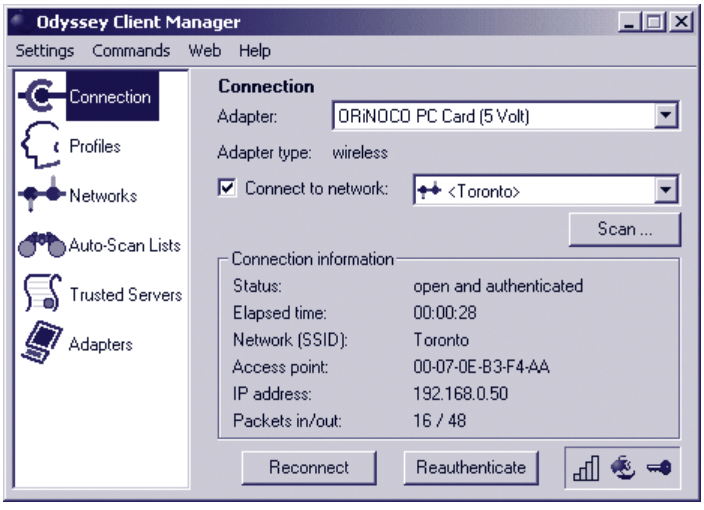
For example, EAP-TLS relies on the use of client-side certificates to authenticate WLAN users. For this reason, it is generally most appropriate for enterprises which have already deployed or committed to a PKI infrastructure.

EAP-TTLS supports the widest range of password protocols and authentication databases, simplifying deployment by permitting the use of any existing authentication system for WLAN user authentication, including Active Directory, token systems, LDAP, and SQL databases.

Low-Overhead Solution

Odyssey Client is easily deployed and maintained across all your client devices. With Odyssey Client, you can rapidly deploy secure WLAN and wired 802.1X access to all your users – saving time on both on the initial deployment and on any subsequent configuration updates you need to distribute. These capabilities substantially reduce the amount of time it takes you to deploy secure WLAN and wired 802.1X access, and slash the costs associated with user support.

- **Pre-configuration capabilities** let you create a template configuration which includes all network and security settings, and deploy this configuration to your WLAN users. You can deploy it via a software installation program such as SMS, or silently via a network login script.
- **Client update capabilities** let you easily distribute new client configuration settings, so changes to network settings, security requirements, or other configuration settings are easily accommodated. You'll be able to easily add or delete networks from users' settings, roll out a stronger security policy (for example, a move from LEAP to EAP-PEAP), and make any other necessary updates on a global or group basis.
- **Multi-platform, multi-vendor compatibility** ensures that Odyssey Client will run in your network environment today, without requiring time-consuming platform upgrades or equipment changes.



Network managers can use the Odyssey Client Manager to create a template configuration, for easy deployment of secure WLAN access across the enterprise.

Enforce Enterprise Security Policies

Odyssey Client also includes powerful capabilities that allow you to mandate compliance with your organization's security policies, providing the strongest protection possible for your network.

- **Client lockdown capabilities** let you prohibit a user from editing some or all of his WLAN or wired 802.1X connection settings. This allows you to require that users connect with a certain level of security, and according to the policies you've set up.
- **Interface with endpoint integrity solutions,** such as Check Point's Integrity, allow you to proactively address security problems – such as out-of-date anti-virus software – before a user is granted access to the network. You can automate problem resolution, and fully protect enterprise PCs against infection, providing the most secure defense for endpoint PCs and data.

Simple User Experience

Odyssey Client incorporates numerous conveniences which simplify how an end user connects to the network, speeding adoption time and reducing your support costs.

Odyssey Client lets you associate an ordered group of wireless networks with an auto-scan list, so that you can be connected to any of the networks available in the list. Users will be connected automatically to the network with the highest priority and strongest signal. These networks and auto-scan lists can be pre-configured by the network administrator.

Through its Auto-Scan capability, Odyssey Client provides significant usability benefits over other 802.1X clients:

• First and foremost, with Odyssey Client, an end user can move seamlessly between different networks, for example, home, office, and hotspot.

• Odyssey Client will automatically associate with the correct network upon PC startup, regardless of location. The user need not interact with Odyssey Client at all.

Funk Software, Inc.
222 Third Street
Cambridge, MA 02142
1-800-828-4146 (US & Canada)
1-617-497-6339
sales@funk.com
www.funk.com

Europe Office
H. Henneaulaan 103 - Third Floor
B-1930 Zaventem
Belgium
(32) 02 712 40 50
europe@funk.com

Asia Office
Suite E - 13 - 12, Block E
Plaza Mont'Kiara
No. 2, Jalan 1/70C
50480 Kuala Lumpur
Malaysia
+603 6201 9682
asia@funk.com

- Users can automatically connect to networks which have different security requirements – again, with no user interaction required. This lets users easily move between office and hotspot networks, for example.
- To connect to new networks, Odyssey Client will scan for available networks, and walk the user through setting the connection up correctly. If the new network will be visited regularly, it can easily be added to the auto-scan list.

(Odyssey Client does not support network auto-scan on Windows Mobile 2003 for Pocket PC.)

Sophisticated Network Logon Capabilities

In addition, Odyssey Client provides advanced network logon capabilities – including support for an advanced "GINA module" and machine connections – which significantly facilitate network connection and administration processes. The following logon capabilities are supported when either the Windows login client or the Novell Client for Windows is used:

- Simplified connection from new, wireless-only devices – to eliminate support calls associated with not being able to connect from devices which have never logged in to a domain controller.
- Automatic running of login scripts – so wireless devices can be centrally administered by IT staff in the same way wired devices commonly are.
- The use of a shared wireless device by several different users – for example on a factory floor or at a nurse's station – with each user being able to log in and access his network profile.
- Easy access to the wireless device by network managers when a user is not logged in – to silently perform such tasks as machine back-ups, virus scan updates, and the like, during off-hours.

Supports 802.1X Wired Connections

Odyssey Client supports both wireless and wired connections to a network. As you consider moving to 802.1X-based wired access for the enhanced security, lower IT costs, and user-based network access it provides, Odyssey Client will fully meet your requirements for an 802.1X client.

Odyssey Client can manage multiple adapter cards simultaneously, so your users won't have to change their configuration settings as they move, for example, from a wired office connection to a wireless conference room connection. This ensures a much simpler experience.

Designed for Compatibility

Odyssey Client's multi-platform, multi-protocol support ensures compatibility in any environment, whether on the secure enterprise WLAN or wired 802.1X network, or at a public WLAN hotspot.

Because it implements standard protocols and EAP methods, it is fully interoperable with solutions from other vendors which support these protocols. For example, an Odyssey Client user can easily be authenticated by a RADIUS server from Cisco or Microsoft.

SIM-Based Authentication

Odyssey Client optionally supports EAP-SIM, the WLAN protocol that allows GSM subscribers log on to a public WLAN and be authenticated against their provider's Subscriber Information Management (SIM)-based infrastructure.

Features at a Glance

- **Multi-platform 802.1X client runs on Windows XP, 2000, 98, ME, and Windows Mobile 2003 for Pocket PC**
- **Supports both 802.1X wireless and wired network access**
- **Great for enterprise and hotspot access**
- **Supports EAP-TTLS, EAP-PEAP, EAP-TLS, EAP-FAST, LEAP, EAP-SIM, and EAP-MD5**
- **Supports Wi-Fi Protected Access (WPA) and WPA2 for enhanced data security**
- **Pre-configure Odyssey Client settings for easy deployment across the enterprise**
- **Auto-scan network lists provides seamless connection to networks, and seamless movement between networks**
- **Sophisticated network logon capabilities, including support for GINA and the Novell Client for Windows and machine connections, facilitate connection and administration processes**
- **Client lockdown capabilities and endpoint integrity interface let you enforce any security policy**
- **Easily deploy new network settings or changes to your security policy**
- **Compatible with any RADIUS server that supports EAP**

WINNER The Fiercest 15 top WLAN startups of 2003 from The 802.11Report

Cisco Systems | AVVID Partner

Frost & Sullivan Market Engineering Award Recipient Market Leadership 2003

PartnerNet ISV PARTNER Novell

FUNK SOFTWARE