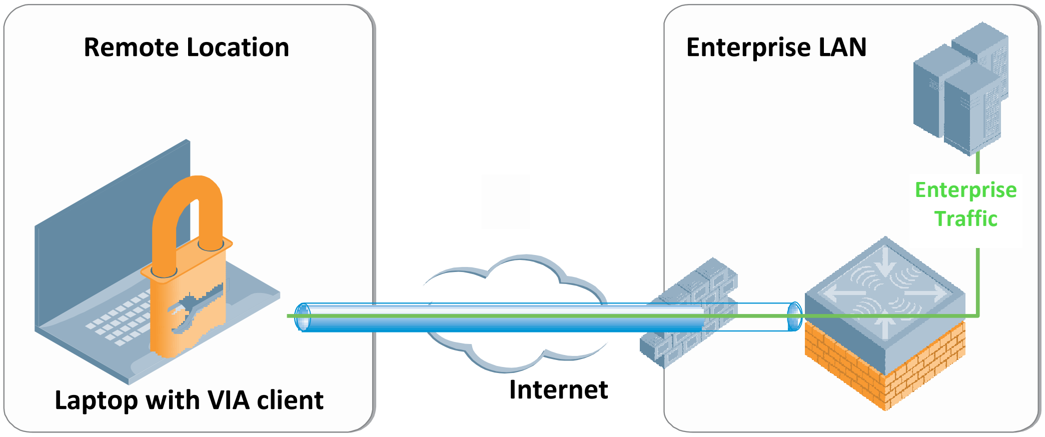
Alcatel·Lucent

Alcatel-Lucent OmniAccess Virtual Intranet Access Agent

SECURE REMOTE CONNECTIVITY

The Alcatel-Lucent OmniAccess Virtual Intranet Access™ (VIA™) agent provides secure remote network connectivity for Windows and Apple MacBook laptops. A key component of the Alcatel-Lucent Virtual Branch Network™ (VBN™) solution, VIA is available as a licensed option with Alcatel-Lucent WLAN Switch/Controller.

VIA is a hybrid IPsec/SSL VPN solution that scans network connections and automatically selects the best connection back to the corporate network whenever needed. Unlike traditional VPN software, VIA offers a zero-touch experience for the end user and can even configure the WLAN settings on laptops.



FEATURES	BENEFITS
Automatic IPsec Connection	Auto-Detection of non-corporate network to initiate IPsec connection
SSL fallback	Detect IPsec blockage by firewall and automatically wraps IPsec in SSL for un-interrupted connectivity
Single sign on	Can leverage Windows credential for authentication to provide seamless user experience.
Troubleshooting support	Built-in in diagnostic and troubleshooting capabilities to speed up resolution time and simplifies administrative process.
Windows ZERO configuration	Ability to WLAN setting using Windows Zero configuration which allows configuration to be dynamically pushed to clients.

Integrated Solution

Orderable through the Alcatel-Lucent Policy Enforcement Firewall (PEF) license, VIA can be downloaded directly from the WLAN Switch/Controller, or pushed out from an existing software management platform. VIA connects to and receives both software and configuration updates directly from the WLAN Switch/Controller with no additional hardware required.

Automatic IPSec Connection

Frequent business travelers often connect from hotels, airports, coffee shops and 3G cellular networks, which require secure links to access internal corporate resources. Legacy VPNs often require users to start additional software and undergo a complicated login process.

However, VIA automatically detects the network connection and determines if it is inside the corporate network. If not, VIA initiates an IPsec connection to the data center, making network access seamless to users, no matter where they work.

IPsec with SSL Fallback Encapsulation

VIA uses the standard IPsec protocol suite to secure communications between VIA-enabled devices and an OmniAccess WLAN Switch/Controller in the data center. This ensures the fastest connections possible where clients can connect via native IPsec. If a firewall blocks direct IPsec connections, VIA can wrap IPsec packets in an SSL header to allow secure connectivity through corporate firewalls.

Leveraging Single Sign-On

The same Windows credentials that authenticate users to wireless LANs (WLANs) can also be used to authenticate VIA users. Leveraging these credentials, VIA automatically connects users in the background without prompting them for a username and password.

When coupled with the automatic connection capability, users experience a consistent connection and authentication experience without changing their work habits. Organizations that require additional authentication methods can employ traditional username and password or token schemes.

User Role Support

The VIA agent leverages the same role-based and stateful firewall policies for local and remote network access to ensure a consistent end-user experience, regardless of location. It can also be configured to allow separate access roles and policies on the same end point, depending on where the user logs into the network.

Extensive Troubleshooting Support

VIA's built-in logging and diagnostics capabilities enable remote troubleshooting of connectivity issues without requiring users to navigate through a complex set of tools. This speeds up the time to resolution and simplifies administrative and end user repair processes.

If required, client logs can be emailed to support teams for more detailed troubleshooting. The diagnostic tools include connection logs, system information, detected WLAN networks, and detailed connectivity tests.

Windows Zero Configuration Support

Optionally, VIA has the ability to configure WLAN settings using the Windows Zero Configuration (WZC) supplicant. This allows network administrators to dynamically push preferred WLAN settings to clients without touching their machines or managing additional tools.

Corporate, Home Office and Road Access

VIA is licensed as part of the AOS-W OS and available on OmniAccess 4306 series, 4504 series, 4604 series, 4704 series and 6000 WLAN switch/Controllers. No additional VPN head-end servers or appliances are needed.

With VIA, users have the same experience as when they connect to the headquarters or branch office network, creating a seamless end-user experience whether accessing resources locally or remotely.

VIA Agent Features

Security Protocols Supported

- Encryption: AES-GCM-128, AES-GCM-256, AES256, AES192, AES128, 3DES, DES
- Hash: SHA-256, SHA-384, SHA, MD5
- Authentication: Preshared key, RSA, RSA and ECDSA, Smart card
- Diffie-Hellman Group: Group 1, Group 2, ECDH Group 19, ECDH Group 20
- IPsec IKEv2

Authentication Options

- Username/password and certificate multifactor authentication
- Smart card

Forwarding Modes

- Tunnel mode
- Split-tunnel mode

Supported Client Operating Systems

- Windows® 7 (32 bit and 64 bit)
- Windows Vista (32 bit and 64 bit)
- Windows XP, Service Pack 2 or greater
- Mac OS X* *(from R6.1)*
- Provides for the optional configuration of Windows WLAN client configuration

Supported OmniAccess WLAN Switch/Controllers

- 4306 series WLAN Switch/Controller
- 4504 series WLAN Switch/Controller
- 4604 series WLAN Switch/Controller
- 4704 series WLAN Switch/Controller
- 6000 series WLAN Switch/Controller with Supervisor Card III

Ordering Information

Part Number	Description
OAW-4306-PEFV	Policy Enforcement Firewall Module for the OAW-4306 (VIA/VPN termination point)
OAW-4306G-PEFV	Policy Enforcement Firewall Module for the OAW-4306G (VIA/VPN termination point)
OAW-4306GW-PEFV	Policy Enforcement Firewall Module for the OAW-4306GW (VIA/VPN termination point)
OAW-4504-PEFV	Policy Enforcement Firewall Module for the OAW-4504 (VIA/VPN termination point)
OAW-4604-PEFV	Policy Enforcement Firewall Module for the OAW-4604 (VIA/VPN termination point)
OAW-4704-PEFV	Policy Enforcement Firewall Module for the OAW-4704 (VIA/VPN termination point)
OAW-S3-PEFV	Policy Enforcement Firewall Module for the Supervisor 3 (VIA/VPN termination point)