Aventail's SSL VPN Adds Security and Flexibility to Citrix Environments

Aventail

Fujitsu, Mount Sinai NYU Health and many other organizations have enhanced their Citrix MetaFrame implementations with Aventail appliances and services to gain increased security and flexibility, and to broaden their remote access options. Aventail's clientless SSL VPNs provide anywhere access and work transparently, consistently and securely with Citrix MetaFrame Access Suite, Citrix Independent Computing Architecture (ICA) clients, all other Citrix products, in addition to all other enterprise resources.

In Aventail/Citrix environments, Aventail's SSL VPNs provide the following benefits:

- **Protecting the enterprise network, including your Citrix MetaFrame server(s)** from hackers by providing a shielding security layer at the edge of the network that offers strong authentication, encryption, and access control, while enabling secure remote access for authorized users.
- **Enforcing desktop firewall policy** on your remote desktops, protecting your network from worms and viruses.
- **Supporting any enterprise resource**, including
  - Applications: old and new Citrix, Web, client/server, legacy, and desktop
  - Security products or services: firewalls, directories, authentication, intrusion detection, proxies, anti-virus
  - Network environments: Network Address Translation, wireless, broadband, dial-up, ISDN, IP
  - Desktop platforms: Windows, Pocket PC (Windows Mobile), Macintosh, Linux with most Web browsers
- **Enabling both connected and offline application usage**, most notably e-mail synchronization, enhancing user productivity.
- **Adapting to changes in the remote connection**, eliminating connectivity problems, user frustration, lost productivity, and expensive support calls.
- **Offering integrated high availability** with load balancing and stateful failover, ensuring that your users always have access to the information they need, wherever and whenever they need it.
- **Providing flexible access options to secured resources,** resulting in improved usability for end users and increased security for enterprises.

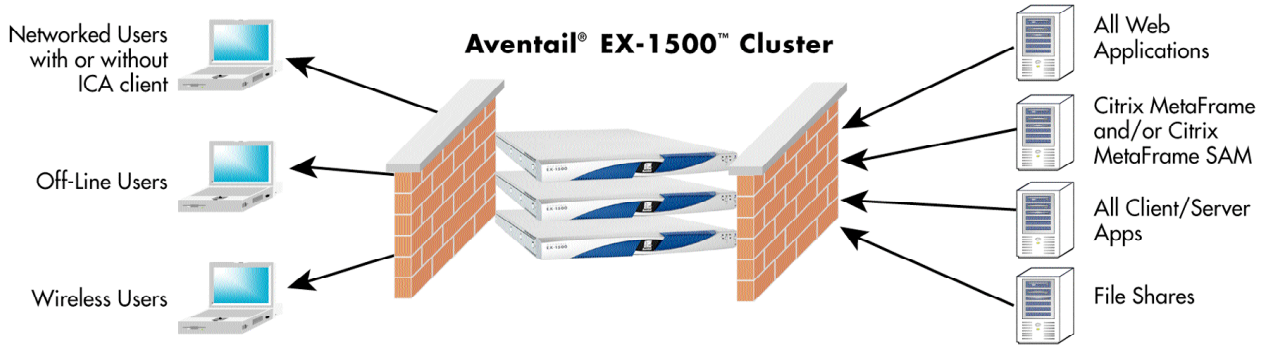
All of your wireless, remote, or traveling Citrix and non-Citrix users can benefit from Aventail's transparent, simple-to-use SSL VPN solution.

Aventail's SSL VPN adds stronger security to Citrix MetaFrame

Enhanced protection at the edge of your network

Aventail's SSL VPN is a hardened appliance designed to operate at the edge of the network, protecting access to less secure network resources. With more Windows vulnerabilities uncovered all the time, IT managers and industry analysts are now more cautious than ever about platforms they can deploy at the edge of the network. In a February 2004 report, the Gartner Group advised enterprises against using Windows Server 2003 in sensitive Internet-exposed applications. Enterprises should continue to heavily weigh the cost of continually patching Microsoft products when deciding which operating system to purchase.[1]

Citrix MetaFrame Access Suite is frequently deployed on Microsoft Windows operating system, making its platform



[1] "Prepare for Yet Another Critical Windows Vulnerability," Gartner Group, February 12, 2004.

vulnerable to many known Windows security problems. An easy and effective way to protect your Citrix MetaFrame environment from outside attacks is to move it behind the Aventail SSL VPN appliance onto your protected corporate network. You can reduce your integration and security concerns by deploying a hardened Aventail SSL VPN appliance at the edge of your network, in front of the Citrix MetaFrame Access Suite, instead of continuously patching Microsoft software at the edge of your network. As an added protection, Aventail has partnered with a number of vulnerability assessment vendors to proactively verify your network and application security, further helping you protect your sensitive information assets.

Designed with security in mind, Aventail's SSL VPNs offer additional security options to protect your Citrix MetaFrame environment and the rest of your information assets.

Comprehensive authentication

Aventail products work with virtually any authentication system. They provide greater flexibility for large enterprises where diverse user credentials may be stored in multiple locations. For example, you may have employees using SecurID and authenticating against a RADIUS server, and customers using Username/Password and authenticating against an LDAP store. Multiple authentication services are supported, including Microsoft Active Directory, digital certificates, and other tokens.

Advanced encryption

Aventail's SSL VPN encryption settings help you specify acceptable ciphers, compression, server validation, and client certificate requirements for the SSL session. So, if the user's Web browser is only enabled for 56-bit encryption, you can restrict him from accessing highly sensitive information.

Scalable, granular access control

Aventail's flexible, object-based access policy and proxy technology eliminate direct network connections, providing transparent access to authorized users. Sheltering your internal network domain name system (DNS) and network topology reduces the risk of unauthorized access or attacks on your network resources. With granular access control, you can limit access based on parameters like:

- Source (IP Address or Host Name) and port
- Destination
- User identity and/or group affiliation
- Time, day, and/or date
- Application and/or service
- Authentication method and/or encryption algorithm
- URL level access

Aventail's flexible, object-based policy model accommodates complex, overlapping group structures and different access rules for the same resource. So, for example, for increased security, you can have a specific resource that a specific user can only access using a corporate computer, thereby preventing kiosk or home computer access.

Aventail End Point Control enforces security at the end user's PC

Vulnerabilities in Windows and the insecurity of shared networks make a PC connected to a public network easy to hack. Given recently exposed Windows vulnerabilities and the mass attacks that will result from attempts to exploit these vulnerabilities, the Gartner Group recommends that all organizations install personal firewalls on all PCs[2] to prevent malicious code from destroying corporate assets.

If, as recommended, you choose to deploy anti-virus or personal firewalls on your corporate desktops, Aventail's SSL VPN, which supports the Aventail® End Point Control™ initiative, can ensure that your personal firewall security policy is enforced for remote users. That's because one of the Aventail End Point Control features enforces activation and usage of a user's personal firewall software before allowing connectivity to the corporate network.

Today Aventail delivers End Point Control with our award-winning Aventail® Connect™ client, which offers automatic detection of desktop security applications, source-based access policy rules, control over split tunneling, strong authentication support, cache protection, AutoCompletion blocking, user authorization, and crypto-level access control. This allows Aventail to first detect the individual and their environment, then to secure that environment, and finally to deliver the right level of access to that user.

Using Aventail to manage access by environment and Aventail partners to make those environments safer, you can deliver secure access from virtually anywhere over any network. Aventail's End Point Control partners enforce policies for firewalls, intrusion detection, virus protection and other client-side security issues, while Aventail encrypts and authorizes access to all corporate resources with access control policies based on both the user's identity and the security of the user's environment.

[2] ibid.

Aventail's SSL VPNs increase remote access options for MetaFrame installations

Aventail's SSL VPNs offer more options for Citrix environments. They offer anywhere access to all old and new Citrix and non-Citrix enabled resources, including MetaFrame Presentation Server, Citrix Independent Computing Architecture (ICA) clients, Citrix Secure Gateway Server, and Citrix Nfuse.

Support for any enterprise resource

In addition to Citrix applications, Aventail's SSL VPNs also secure non-Citrix-enabled resources. They have been tested and deployed with hundreds of different technologies. These include different types of software, hardware, networking environments (dial-up, wireless, broadband, Ethernet), including access to client/server, legacy, Web, and desktop applications. Aventail's SSL VPNs also support a multitude of networking services (such as file and print), security services (including firewalls, authentication, access control, intrusion detection, and anti-virus), and XML-based Web Services.

Aventail works well with virtually any technology. Aventail and its customers have successfully deployed Aventail's SSL VPNs in Healthcare, Manufacturing, Professional Services, Financial Services, Government, High Technology, Retail, Telecommunications, and Education.

Support for applications in online and offline modes

Certain applications, most notably e-mail, are designed to work in both connected (online) and disconnected (offline) modes, where the e-mail client and the mail server are periodically synchronized automatically whenever the connection is available. Historically, disconnected mode of e-mail applications have not been supported by Citrix MetaFrame, limiting user flexibility. Aventail's SSL VPNs work transparently with both connected and disconnected applications.

Aventail's SSL VPNs: Deep support for healthcare applications

- Cerner
- Epic
- McKesson
- SMS
- IDX
- Misys
- Meditech
- GE Medical

When first connected over an Aventail SSL VPN, e-mail users can securely synchronize their desktop clients with their mail servers. Once synchronized—meaning they now have new messages loaded on their e-mail clients— users can disconnect from the network to read and reply to their messages offline. The next time secure connection is available, e-mail clients seamlessly send and receives new messages to the mail servers over the Aventail-protected connection. This capability is very helpful for people working in transit, without consistent network connectivity or for budget-conscious travelers who want to minimize telephone charges at hotel rooms and on mobile phones. With support for both connected and disconnected modes, Aventail's SSL VPNs can provide your users with increased flexibility and productivity, while reducing your telecommunications costs.

Adapts to changes in the remote connection

Aventail's SSL VPNs connect to the enterprise, traversing all network boundaries—including firewalls, Network Address

Customers frequently use Aventail's SSL VPNs with applications from companies including:

- BEA (Tuxedo, WebLogic)
- Cisco
- Check Point
- HP (HP-UX, OpenView, VMS)
- IBM (AIX, AS/400, DB2, Lotus Notes, Tivoli, WebSphere)
- ISS
- Lucent
- Microsoft (Exchange, Office, Outlook, SharePoint, Windows)
- Network Associates
- Nortel
- Oracle (databases, applications and tools)
- Peoplesoft
- Red Hat
- RSA Security
- SAP R/3
- Siebel
- Sun (Solaris, iPlanet)
- Symantec

Translations (NAT), and proxy services. This prevents configuration conflicts common with other remote access products. Aventail's SSL VPNs provide trouble-free and consistent access, without requiring client or server changes, in the following environments:

- A wired connection with NAT, behind a firewall at a hotel room
- A wireless hotspot at a coffee shop
- A dial-up hookup at the airport
- A broadband connection behind a personal firewall at a home office
- An Ethernet connection on a partner's corporate network behind multiple firewalls and proxy servers

With trouble-free access to Citrix MetaFrame and all other authorized applications, Aventail's SSL VPN improves remote workforce productivity and reduces your support costs.

> "Aventail technology gives us the ability to use a local Internet service provider from anywhere in the world. Plus it integrates seamlessly with existing network and security infrastructures."
>
> — Kevin Bregartner,
> CIO, Fujitsu Consulting

Fault tolerance and high availability

Fault tolerance and high availability are particularly important when protecting high-end Citrix MetaFrame presentation server farms that support thousands of connected users. Aventail is the first SSL VPN provider to offer integrated load balancing with stateful failover for enhanced fault tolerance and high availability. Aventail's SSL VPNs ensure that all of your users always have access to the information they need, wherever and whenever they need it.

Flexible access options to secured resources

Aventail offers a full range of clientless access options plus the award-winning Aventail Connect Windows SSL VPN client, giving users secure access from un-trusted, semi-trusted, and trusted Internet-enabled devices—everything from kiosks to PDAs to corporate-managed computers. The Aventail SSL VPN is flexible enough to work well in just about any remote access situation.

Aventail provides three access options:

- **Browser-based access for Web applications** and file shares
- **Aventail® OnDemand™**, a Web-delivered Java SSL VPN agent for secure client/server application access
- **Aventail® Connect™**, a cost-effective Windows SSL VPN client for full secure access to network resources from corporate laptops

With its broad access methods and the granularity it allows in managing policy, Aventail enables companies to extend secure remote access from more places and to more resources at a low total cost of ownership. Aventail's client/server access options—Aventail Connect and Aventail OnDemand —are tested and ideal solutions for remote usage of Citrix products.

Aventail's SSL VPNs offer support for multiple platforms, including Windows XP, Windows 98, Windows 95, Pocket PC, Macintosh, Linux, and any Java-enabled Web browser. Unlike Citrix MetaFrame Secure Access Manager that only supports Windows clients with Internet Explorer, Aventail's SSL VPN supports many of the same client platforms as Citrix ICA, providing enhanced convenience to your users with better security.

Aventail's SSL VPN with its flexible access control technology can enhance your Citrix implementation in several ways:

- **Network protection:** Deploy Aventail's SSL VPNs in front of all of your remote access points, to maximize protection of all of your enterprise resources, including Citrix access points.
- **Broader application protection:** Deploy new (e.g. Web and Client/Server) applications to all relevant users using Aventail's SSL VPN, while continuing to support your existing Citrix MetaFrame applications unchanged.
- **User access expansion:** Provide some of your users (e.g. power users, executives) with Aventail's SSL VPN-secured full network access, seamless connected and disconnected application support, and access to select technical resources, while maintaining other less demanding users on your Citrix infrastructure.
- **Organizational enablement:** Expand support for new types of users (e.g., customers, suppliers, partners) to select resources (e.g., Web applications, limited file shares) through Aventail's SSL VPN, independently of your Citrix environment.

For Citrix-enabled resources, Aventail lets you choose the user experience that best suits your organization. For instance, the

Citrix ICA client and Aventail OnDemand Java applet can be easily integrated to automatically launch with a single mouse-click, simplifying end user training and support.

For non-Citrix-enabled resources (any application and/or file and printer shares), Aventail's SSL VPN can either work with existing intranets, Web pages and enterprise portals or seamlessly plug into the Microsoft Windows user interface, transparently securing both the desktop and the connection. Aventail's SSL VPN can seamlessly interface with SAP Enterprise Portal, IBM WebSphere, BEA WebLogic, Microsoft SharePoint, or provide its own Aventail® ASAP™ WorkPlace portal.

Aventail's SSL VPN is substantially simpler to deploy and manage than traditional IPSec VPNs, since no software needs to be installed on the remote device. Citrix ICA users can automatically download Aventail OnDemand, a Java-based client, at the initiation of a secure connection. If you desire a stronger security option that protects the users' computer as well as the corporate network, your end users can install an optional Aventail Connect client, in a similar way to how they installed Citrix ICA. Users simply go to a designated URL and click the link for an automated installation of Aventail Connect.

Conclusion: Aventail's SSL VPNs are your best choice for remote access

Every day, thousands of organizations depend on proven Aventail's SSL VPN appliances to cost-effectively access protected network resources from remote locations using a wide variety of devices. Many of these companies have secured and expanded their Citrix MetaFrame environments with Aventail's SSL VPNs, offering secure access to both Citrix and non-Citrix enabled resources. Fujitsu, for example, has 5,000+ consultants in more than 100 countries using the combined solution. Mount Sinai NYU Health has 450 mobile doctors, in-home nurses, and administrators using the combined solution.

Working together with your Citrix infrastructure or independently of it, Aventail's SSL VPNs can protect any enterprise resource, strengthen your information security enforcement, adapt to changes in the remote connection, and offer flexible access options to secured resources. With Aventail technology, companies can extend secure remote access from more places and to more resources for increased productivity at a low total cost of ownership.

> "Aventail was able to build an infrastructure that supports current applications and gives us the flexibility to extend new applications out quickly to multiple audiences."
>
> — Fred Eisenberg,
> Director, Information Security,
> Mount Sinai NYU Health

Aventail is the leading SSL VPN product company.

The authority on clientless and client-based anywhere secure access, Aventail ensures enterprises can provide access to any application from the broadest range of devices of any SSL VPN, thereby increasing the productivity of end-users and IT professionals. Customers including Aetna, DuPont, Mount Sinai NYU Health, Office Depot, and Sanyo and leading service providers including AT&T, IBM Global Services, MCI, Sprint, and Bell Canada rely on Aventail technology. Aventail has been named a Gartner Magic Quadrant leader four times since 2002.

Aventail

WP-40675-0404/1

Corporate Headquarters
808 Howell Street
Seattle, WA 98101
Tel 206.215.1111
Fax 206.215.1120
americas@aventail.com
www.aventail.com

Aventail Europe Ltd
Tel +44 (0) 870.240.4499
emea@aventail.com

Aventail Asia-Pacific
Tel +65 6832.5947
asiapac@aventail.com