Increase Productivity with Flexible, Secure Remote Access

As more mobile and remote workers use an increasing number of different devices to access corporate applications and data from many locations, your business benefits from more flexible and productive users. But securing applications, data, the network, and client devices from unauthorized access and attacks can quickly add management complexity and cost.

The FirePass® SSL VPN appliance and Virtual Edition (VE) provide secure remote access to enterprise applications and data for users over any device or network. FirePass ensures easy access to applications by delivering outstanding performance, scalability, availability, policy management, and endpoint security. The result is unified security enforcement and access control that increases the agility and productivity of your workforce.

**Key Benefits:**

**Increase worker productivity**
Provide fast and secure, always connected remote access from any location, from any device.

**Gain ultimate flexibility**
Quickly and easily deploy a virtual appliance to add remote access functionality to your existing virtual infrastructure.

**Decrease costs**
Reduce deployment and support costs with easy management, simple deployment, and secure application access.

**Increase security**
Deliver granular access control to intranet resources on a group basis, enhancing security.

**Reduce risk with endpoint security**
Verify the user quickly and easily with endpoint security to validate compliance with corporate policy.
Improved User Experience

FirePass helps ensure user productivity by minimizing the time and effort required to gain access to authorized files and applications.

“Always connected” remote access

Some access clients need constant reconnection throughout the day as users move locations or restart applications. The BIG-IP® Edge Client™ solution is a state-of-the-art, integrated client that provides location awareness and zone determination to deliver a remote access solution unlike any other. Cutting-edge roaming, domain detection, and automatic connection create a seamless transition as users move between locations. BIG-IP Edge Client helps ensure continued user productivity whether the user is at home on a wireless network, using an air card in transit, giving a presentation from corporate wireless, in a café on guest wireless, or docked on a LAN connection. BIG-IP Edge Client is supported in FirePass 6.1 and 7.0.

Seamless VPN access

When the user first enters credentials as part of the Windows logon process, BIG-IP Edge Client caches them and then automatically tries them in the first attempt to log onto the VPN. This streamlines the user experience to help improve productivity.
Network Access

FirePass provides LAN-type network access connectivity for all applications by supporting existing network infrastructure, identity management systems, and client-server operating systems.

FirePass Network Access for Microsoft Windows (Windows 7, Vista, XP), Mac, and Linux Systems

• Eliminates the need for special administrative privileges for FirePass client component updates with Windows Installer Service, lowering management costs.
• Provides secure remote access to the entire network for all IP-based (TCP, UDP) applications.
• Includes standard features across all desktop and laptop platforms, as well as split tunneling, compression, activity-based timeouts, and automatic application launching.
• Provides remote access—unlike IPSec VPNs—without requiring preinstalled client software and configuration of the remote device. Client- or server-side application changes are not required.
• Enables administrators to restrict and protect resources accessible through the connector by instituting rules that limit access to a specific network or port.
• Uses the standard HTTPS protocol with SSL as the transport, so the device works through all HTTP proxies including public access points, private LANs, and over networks and ISPs that don’t support IPSec VPNs.
• Utilizes GZIP compression to compress traffic before it is encrypted, reducing the amount of traffic that is sent across the Internet and improving performance.
• Supports the latest OSs and Browsers—FirePass 7.0 supports 32-bit versions of: Windows 7, Vista, and XP; Mac OS X Leopard and Snow Leopard; Internet Explorer 6, 7, and 8; Firefox 3.x; and Safari 4. It supports 64-bit versions of: Windows 7, Vista, and XP; Linux (contact F5 or Reseller for list), Internet Explorer 7 (except Win 7) and 8; and Firefox 3.0. Talk to an F5 sales representative or reseller to review compatibility for your environment.

Client Security

• Safe Split Tunneling—To protect against back-door attacks when accessing the network with split tunneling, FirePass provides a dynamic firewall that protects Windows, Mac, and Linux users when using the full network access feature. This prevents hackers from routing through the client to the corporate network or users from inadvertently sending traffic to the public network.
• Endpoint Client Checking—FirePass increases security by detecting the presence of required processes (for example, virus scans, anti-malware, personal firewalls, OS patch levels, registry settings, and more) and the absence of other processes (for example, key logger) on the Mac, Linux or Windows client before enabling full network access.
• Hardware Endpoint Inspectors—FirePass inspects client machine features such MAC address, CPU ID, and HDD ID to identify remote devices. FirePass authorizes machines without the complexity of deploying machine certificates.
Windows Network Access Features

- **Standalone Windows Client**—FirePass establishes a network connection after entering user credentials. Software can be automatically distributed to the client using Microsoft’s MSI installer technology.
- **Windows Logon/GINA Integration**—Enables implied, transparent user logon to the corporate network by integrating with the GINA (“Ctrl + Alt + Del” prompt) logon process.
- **Standalone VPN Client CLI**—Command-line interface support offers single sign-on support through integration with third-party applications (such as remote dialer software).
- **Windows VPN Dialer**—Provides a simplified user experience for those more comfortable with the dialup interface.
- **Automatic Drive Mapping**—Network drives can be automatically mapped to a user’s Windows PC.
- **Static IP Support**—Assigns a static IP based on the user when the user establishes a network access VPN connection, lowering administrative support costs.
- **Transparent Network Access**—Eliminates network access browser window pop-ups and prevents users from accidentally terminating the connection.

Mobile Device Support

- Enables secure application access from Windows Mobile and smartphones.
- Provides access to both client/server- and web-based applications.

**FirePass SSL VPN Value Proposition**
- Browser-based ubiquitous access
- Lower support and management costs
- Endpoint security
- Granular access control
- Group policy enforcement
Application Access—Secure Access to Specific Applications

FirePass enables administrators to grant certain users—for example, business partners using equipment not maintained by the company—access to specific extranet applications and sites. FirePass protects network resources by only permitting access to applications that are cleared by the system administrator.

Specific Client/Server Application Access

- Enables a native client-side application to communicate back to certain corporate application servers via a secure connection between the browser and the FirePass device.
- Requires no pre-installation or configuring of any software.
- Involves no additional network-side software to access the application servers.
- Accesses applications via standard protocols: HTTP and SSL/TLS. It works with all HTTP proxies, access points, and private LANs, and over networks and ISPs that do not support traditional IPSec VPNs.
- Includes supported applications such as Outlook to Exchange Clusters, Passive FTP, Citrix Nfuse, and network drive mapping.
- Supports custom CRM applications as well as applications that use static TCP ports.
- Supports auto-login to AppTunnels, Citrix, and WTS applications to simplify the user experience.
- Integrates with Citrix SmartAccess to deliver endpoint inspection results to Citrix applications and send SmartAccess filters to XenApp based on the results of endpoint scans.
- Supports the auto-launch of client-side applications to simplify user experience and lower support costs.
- Enables lock-down Java-based application tunnels for non-Windows and Windows systems to prevent the execution of ActiveX controls.
- Offers complete DHCP support for clients using network access, automating IP address assignment and dynamic DNS registration of addresses. DHCP support provides easier multi-unit deployments while remote-access IP address range can overlap with internal LAN.
- Delivers support for Microsoft Communicator via Portal Access, enhancing VoIP communications.
- Offers unique support for the compression of client/server application traffic over the WAN, enhancing performance.

Terminal Server Access

- Provides secure web-based access to Microsoft Terminal Servers, Citrix MetaFrame applications, Windows XP Remote Desktops, and VNC servers.
- Provides Terminal Services for VMware View web client to enable user access from virtual desktops.
- Supports group access options, user authentication, and automatic log-on capabilities for authorized users.
- Supports automatic downloading and installation of the correct Terminal Services or Citrix remote platform client component, if not currently installed on the remote device, saving time.
• Supports remote access to XP desktops for remote troubleshooting using RDP and non-XP desktops with the built-in VNC feature.
• Provides Java-based Terminal Services support for Citrix and Microsoft.

Dynamic App Tunnels
• Provides maximum support for accessing a wide variety of client/server- and web-based applications.
• Offers a better alternative to reverse proxies for accessing applications from Windows client devices.
• Eliminates the need for web application content interoperability testing.
• Requires only “power user” privileges for installation and no special privileges for execution.
• Provides added support for auto-launching web application tunnels, simplifying the user experience.

Host Access
• Enables secure web-based access to legacy VT100, VT320, Telnet, X-Term, and IBM 3270/5250 applications.
• Requires no modifications to the applications or application servers.
• Eliminates the need for third-party host access software, reducing total cost of ownership (TCO).

Portal Access—Proxy-Based Access to Web Applications, Files, and Email
FirePass Portal Access capability works on any client OS with a browser: Windows, Linux, Mac, smartphones, PDAs, and more.

Web Applications
• Provides access to internal web servers, including Microsoft Outlook Web Access, Lotus iNotes, and Microsoft SharePoint Server as easily as from inside the corporate LAN.
• Delivers granular access control to intranet resources on a group policy basis. For example, employees can gain access to all intranet sites; partners can be restricted to a specific web host.
• Dynamically maps internal URLs to external URLs, so the internal network structure does not reveal them.
• Manages user cookies at the FirePass device level to avoid exposing sensitive information.
• Passes user credentials to web hosts to support automatic login and other user-specific access to applications. FirePass also integrates with existing identity management servers (for example, CA Netegrity) to enable single sign-on to applications.
• Proxies login requests from web hosts to avoid having users cache their passwords on client browsers.
• Enables or restricts access to specific parts of an application with granular access control list (ACL) for increased security and reduced business risks.
• Provides split-tunneling support for web applications, resulting in faster user performance when accessing public websites.

• Validates back-end certificate with rapid reverse-proxy to quickly authenticate the server’s certificate.

• Offers dynamic server-side and DNS caching for increased web application (reverse proxy) performance and faster page download times.

• Delivers out-of-the-box reverse proxy support for rewriting a wide variety of JavaScript content in web pages, saving time.

• Provides Java patch ACL support to limit client-initiated connections through FirePass using Portal Access.

• Enables NTLMv2 support for access to web applications.

• Delivers DNS relay proxy service, enabling client-side name resolution without requiring any special runtime rights (for example, modification of hosts). Also enables redirection of ports to more fully support applications such as Outlook and Windows drive mapping.

**File Server Access**

• Enables users to browse, upload, download, copy, move, or delete files on shared directories.

• Supports: SMB Shares; Windows Workgroups; NT 4.0 and Win2000 domains; Novell 5.1/6.0 with Native File System pack; and NFS servers.

**Email Access**

• Provides secure web-based access to POP/IMAP/SMTP email servers from standard and mobile device browsers.

• Enables users to send and receive messages, download attachments, and attach network files to emails.

**Mobile Device Support**

• Provides secure access from Apple iPhone, Windows Mobile, PDAs, smartphones, cell phones, WAP, and iMode phones to email and other web-based applications.

• Dynamically formats email from POP/IMAP/SMTP email servers to fit the smaller screens of mobile phones and PDAs.

• Supports the sending of network files as email attachments and the viewing of text and Word documents.

• Supports ActiveSync applications, enabling PDA synchronization of email and calendar on Exchange Server from a PDA device, without requiring the pre-installed VPN client component.
Portal Access—Comprehensive Security

FirePass delivers multiple layers of control for securing information access from public systems.

Client Security

- Protected Workspace—Users of the 32-bit version of Windows XP/Vista/7 or the 64-bit version of Windows Vista/7 can be automatically switched to a protected workspace for their remote access session. In a protected workspace mode, the user cannot write files to locations outside the protected workspace; the temporary folders and all of their contents are deleted at the end of the session.

- Cache Cleanup—The cache cleanup control removes—and empties from the recycle bin—the following data from the client PC: cookies, browser history, auto-complete information, browser cache, temp files, and all ActiveX controls installed during the remote access session.

- Secure Virtual Keyboard—For additional password security, FirePass offers the patent-pending Secure Virtual Keyboard which enables secure password entry from the mouse instead of the keyboard.

- Download Blocking—For systems unable to install a “cleanup” control, FirePass can be configured to block all file downloads to avoid the issue of inadvertently leaving behind temporary files, yet still enable access to applications.

- Automatic File Virtualization—In protected workspace mode, temporary files and registry settings are written to a virtual file system rather than to the local machine.

- Encrypted Saved Content—All temporary content saved on the remote system is encrypted in the event that the protected workspace doesn’t exit normally, such as in a power failure, rendering the content unreadable.

- Portal Support for Popular Mobile Clients—FirePass supports portal access with iPhone, BlackBerry, and Opera Mini browsers.

Content Inspection and Web Application Security

For users accessing web applications on the corporate network, FirePass enhances application security and prevents application-layer attacks (for example, cross-site scripting, invalid characters, SQL injection, buffer overflow) by scanning web application access for application layer attacks—then blocking user access when an attack is detected.

Integrated Virus Protection

FirePass can scan web and file uploads using either an integrated scanner or external scanner via ICAP API. Infected files are blocked at the gateway and not allowed onto email or file servers on the network, for increased protection.

Flexible Remote Access

FirePass Virtual Edition (VE) makes it easy to quickly deploy a virtual appliance to add SSL VPN functionality to an existing virtual infrastructure. This offers greater flexibility in disaster recovery scenarios or during a surge in remote access demand. Virtual editions of FirePass and BIG-IP Local Traffic Manager can be combined to provide industry-leading application delivery and remote access in the same environment.
Dynamic Policy Engine—Total Administrative Control

The FirePass policy engine enables administrators to easily manage user authentication and authorization privileges.

**Dynamic Policy-Based Access**

Administrators have quick and granular control over their network resources. Through policy management support, they can authorize access to applications based on the user and device. Administrators can easily implement existing policies with import and export of pre-logon policies.

**Visual Policy Editor**

The Visual Policy Editor creates a flow-chart style graphical view of your access policies, giving you point-and-click ease in profiling and managing groups, users, devices, or any combination of the three. This simplifies the definition and management of endpoint policies, lowers administrative costs, and increases the ability to quickly ensure the protection of company resources.
User Authentication

Users can be authenticated against an internal FirePass database, using passwords. FirePass can also be easily configured to work with RADIUS, Active Directory, RSA 2-Factor, LDAP authentication methods, basic and form-based HTTP authentication, identity management servers (for example, Netegrity), and Windows domain servers. With Active Directory, users can change current or expired passwords and receive warnings when passwords are set to expire. Support for nested Active Directory configurations enables the use of a more complex, hierarchical directory structure.

Two-Factor Authentication

Many organizations use “two-factor” authentication (such as tokens or SmartCards) that require more than just a user ID and password. FirePass supports two-factor authentication including RSA SecurID® Native ACE authentication.

Challenge Response Test

Administrators can implement CAPTCHA, an easy challenge response test for humans that protects the organization from DoS and script-based brute force attacks.

Client-side and Machine Certificates/PKI Support

FirePass integrates seamlessly with the existing PKI infrastructure and enables the administrator to restrict or permit access based on the device being used to access FirePass. FirePass can check for the presence of a client-side digital certificate or Windows machine certificate during user login. Based on the presence of a valid certificate, FirePass can support access to a broader range of applications. FirePass can also use client-side or machine certificates as a form of two-factor authentication and prohibit all network access for users without a valid certificate.

Group Management

Access privileges can be granted to individuals or to groups of users (for example: sales, partners, or IT). This enables FirePass to restrict individuals and groups to particular resources.

Group Policy Enforcement

Group policy provides an exclusive mechanism to apply and enforce policies on client systems not part of the network domain. You can use the Visual Policy Editor to design group policies, in the form of templates, that restrict user authority and access while enforcing compliance with PCI, HIPAA, and GLBA. (Note: Group Policy Objects are only available on Active Directory.)
Dynamic Group Mapping

FirePass dynamically maps users to FirePass groups using various dynamic group mapping mechanisms such as Active Directory, RADIUS, LDAP, client certificates, landing URI, and virtual host name as well as pre-logon session variables.

Single Sign-On (SSO) Support

SSO configuration uses authentication session variables to extract SSO information from certificates and authentication information from username and password settings. Advanced session variables help system administrators extend and customize FirePass, enabling them to manipulate and create new session variables for custom deployments. They also can collect and capture RADIUS attributes plus LDAP, Active Directory, and certificate field values.

SessionTimeouts and Limits

Administrators can configure inactivity and session timeouts to protect against a hacker attempting to take over a session from a user who forgets to logoff at a kiosk.

Role-Based Administration

Organizations have the flexibility to provide some administrative functions (enrolling new users, terminating sessions, re-setting passwords) to some administrator-users, without exposing all functions to them (for example, shutting down the server or deleting a certificate).

Logging and Reporting

FirePass delivers built-in logging support for logging user, administrator, session, application, and system events. Additionally, FirePass provides logs in silo format for integration with an external syslog server. The administration console offers a wide range of audit reports to help comply with security audits. Summary reports aggregate usage by day of the week, time of day, accessing OS, features used, websites accessed, session duration, session termination type, and other information for a user-specified time interval. A single URL is used to retrieve summary/group reports in either HTML or spreadsheet format.

Customization

FirePass provides advanced customization features, enabling the administrator to design a unique GUI or existing corporate website portal to best reflect corporate and user requirements.

Localized User GUI

FirePass enables all fields on the user web page to be localized, including the names of the feature (for example, web applications). This helps companies localize the user’s GUI, not just user favorites—increasing business value and lowering TCO.

Complete Login and Webtop Customization

With FirePass, administrators can completely customize an entire login and webtop web page to best suit their existing corporate website portals. Administrators can use WebDAV capabilities to upload custom pages, for an enhanced user experience.
iControl SSL VPN Client API for Secure Application Access

As the only SSL VPN product with an open client API and SDK, FirePass enables automated, secure access from the Win32 client OS (XP, Vista, 7) by providing secure system-to-system or application-to-application communication. Applications can automatically start and stop network connections transparently without requiring users to log into the VPN. This enables faster, easier connections for users while reducing client application installation costs.

FirePass Product Details

The range of FirePass appliances and Virtual Edition address the concurrent user access needs of small to large enterprises.

**FirePass 1200**

The FirePass 1200 device is designed for small to medium enterprises and branch offices, and supports from 10 to 100 concurrent users.

**FirePass 4100**

The FirePass 4100 controller is designed for medium-size enterprises and, from a price/performance standpoint, is recommended for up to 500 concurrent users.

**FirePass 4300**

The FirePass 4300 appliance is designed for medium to large enterprises and service providers and supports up to 2000 concurrent users.

**FirePass Virtual Edition**

FirePass Virtual Edition runs in a VMware ESX 4.0 virtual environment and is designed for medium to large enterprises and service providers supporting up to 2000 concurrent users.

**Clustering**

The FirePass 4100 and 4300 appliances and Virtual Edition have built-in clustering support. They can be combined with F5 BIG-IP® Global Traffic Manager™ and BIG-IP® Local Traffic Manager™ to provide industry-leading scalability, performance, and availability.

**Failover**

FirePass appliances and Virtual Edition can also be configured for stateful failover between pairs of servers (an active server and a standby server) to avoid having to re-logon to another FirePass device or Virtual Edition in the unlikely event of a primary unit failure.

**SSL Accelerator Hardware Option**

FirePass 4100 offers a unique Hardware SSL Acceleration option to offload the SSL key exchange as well as the encryption and decryption of SSL traffic. This enables significant performance gains in large enterprise environments for processor-intensive ciphers such as 3DES and AES.
FIPS SSL Accelerator Hardware Option

FirePass is FIPS compliant* to meet the strong security needs of government, finance, healthcare, and other security-conscious organizations. FirePass 4100 and 4300 devices offer support for FIPS 140 Level-2 enabled tamper-proof storage of SSL keys, as well as FIPS-certified cipher support for encrypting and decrypting SSL traffic in hardware. FIPS SSL Accelerator is available as a factory install option to the base 4100 and 4300 platform.

* FIPS 140-2 meets the security criteria of CESG (UK’s National Technical Authority For Information Assurance) for use in private data traffic.
FirePass Specifications

The FirePass appliance is available in three models and as a Virtual Edition to address the concurrent user access needs of small to large enterprises.

---

Virtual Specifications

<table>
<thead>
<tr>
<th>Recommended Conc. Users:</th>
<th>Up to 2000*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clustering Support:</td>
<td>Yes – up to 10 virtual appliances</td>
</tr>
</tbody>
</table>

*Note: Actual performance varies depending on hardware platform, resources available, and configuration. Customer is responsible for performance testing and scaling of FirePass Virtual Edition.

---

Host System Requirements

It is highly recommended that the host system contain CPUs based on AMD-V or Intel-VT technology.

<table>
<thead>
<tr>
<th>Hypervisor:</th>
<th>VMware ESX 4.0 or ESXi 4.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VMware vSphere Client</td>
</tr>
<tr>
<td></td>
<td>VMware virtual hardware version 7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Processor:</th>
<th>1 CPU</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(4 CPUs or more are recommended for more than 500 concurrent users.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Memory:</th>
<th>2 GB RAM</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(8 GB or more are recommended for more than 500 concurrent users.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Adapters:</th>
<th>3 network interfaces</th>
</tr>
</thead>
</table>

| Disk Space:                 | 30 GB hard drive of thin provisioning |
## Physical Specifications

<table>
<thead>
<tr>
<th></th>
<th>4300</th>
<th>4100</th>
<th>1200</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recommended Conc. Users:</strong></td>
<td>2000</td>
<td>500</td>
<td>100</td>
</tr>
<tr>
<td><strong>Max. Conc. Users per Appliance:</strong></td>
<td>2000</td>
<td>2000</td>
<td>100</td>
</tr>
<tr>
<td><strong>Interfaces:</strong></td>
<td>4 (10/100/1000) LAN ports</td>
<td>4 (10/100/1000) LAN ports</td>
<td>2 (10/100) LAN ports</td>
</tr>
<tr>
<td><strong>Dimensions:</strong></td>
<td>3.5” H x 17.5” W x 23.5” D</td>
<td>3.5” H x 17.5” W x 23.5” D</td>
<td>1.7” H x 16.7” W x 11” D</td>
</tr>
<tr>
<td><strong>Weight:</strong></td>
<td>43 lbs</td>
<td>40 lbs</td>
<td>10 lbs</td>
</tr>
<tr>
<td><strong>Processors:</strong></td>
<td>Two Opteron 2.2 GHz - dual core</td>
<td>Two Opteron 2.0 GHz - single core</td>
<td>Intel Celeron 2.0 GHz - single core</td>
</tr>
<tr>
<td><strong>Power Supply:</strong></td>
<td>Dual 475 W 90/240 +/- 10% VAC auto switching</td>
<td>425 W 90/240 +/- 10% VAC auto switching</td>
<td>Single full-range 250 W</td>
</tr>
<tr>
<td><strong>Typical Power Consumption:</strong></td>
<td>275 W</td>
<td>275 W</td>
<td>180 W</td>
</tr>
<tr>
<td><strong>Maximum Heat Output:</strong></td>
<td>939 BTU/hr</td>
<td>939 BTU/hr</td>
<td>785 BTU/hr</td>
</tr>
<tr>
<td><strong>Device Redundancy:</strong></td>
<td>Watchdog timer, failsafe cable (primary and secondary)</td>
<td>Watchdog timer, failsafe cable (primary and secondary)</td>
<td>Watchdog timer, failsafe cable (primary and secondary)</td>
</tr>
<tr>
<td><strong>Clustering support:</strong></td>
<td>Yes – up to 10 appliances</td>
<td>Yes – up to 10 appliances</td>
<td>No</td>
</tr>
<tr>
<td><strong>FIPS SSL Accelerator Card Option:</strong></td>
<td>Yes – factory only</td>
<td>Yes – factory only</td>
<td>No</td>
</tr>
<tr>
<td><strong>Hard Drive Capacity:</strong></td>
<td>160 GB</td>
<td>160 GB</td>
<td>40 GB</td>
</tr>
<tr>
<td><strong>RAM:</strong></td>
<td>8 GB standard</td>
<td>4 GB standard</td>
<td>512 MB</td>
</tr>
<tr>
<td><strong>Temperature (operating):</strong></td>
<td>41° F to 104° F (5° C to 40° C)</td>
<td>41° F to 104° F (5° C to 40° C)</td>
<td>41° F to 104° F (5° C to 40° C)</td>
</tr>
<tr>
<td><strong>Non-Operating Ambient Temperature Range:</strong></td>
<td>-40° F to 149° F (-40° C to 65° C)</td>
<td>-40° F to 149° F (-40° C to 65° C)</td>
<td>-40° F to 149° F (-40° C to 65° C)</td>
</tr>
<tr>
<td><strong>Humidity (relative):</strong></td>
<td>20% to 90% at 40° C</td>
<td>20% to 90% at 40° C</td>
<td>20% to 90% at 40° C</td>
</tr>
<tr>
<td><strong>Safety Agency Approval:</strong></td>
<td>UL 60950 (UL 1950-3), CSA-C22.2 No 60950-00 (Bi-national standard with UL 60950) CB test certification to IEC 950, EN 60950</td>
<td>UL 60950 (UL 1950-3), CSA-C22.2 No 60950-00 (Bi-national standard with UL 60950) CB test certification to IEC 950, EN 60950</td>
<td>UL 60950 (UL 1950-3), CSA-C22.2 No 60950-00 (Bi-national standard with UL 60950) CB test certification to IEC 950, EN 60950</td>
</tr>
</tbody>
</table>
More Information

Visit these resources on F5.com to learn more about FirePass.

White papers
F5 FirePass Endpoint Security
Get to Know GPO

Podcast
Secure Remote Access for Disaster Recovery

Case study
City of Diamond Bar Deploys FirePass

Deployment guides
F5 FirePass controller with BIG-IP LTM and GTM
(FirePass v6.x, LTM, and GTM 9.4.2), Deployment Guide
FirePass and VMware View Deployment Guide