

JUNOS PULSE SECURE ACCESS SERVICE FOR MAG SERIES JUNOS PULSE GATEWAYS

Product Overview

The Juniper Networks MAG Series Junos Pulse Gateways (MAG2600, MAG4610, MAG6610, MAG6611) are designed to address the challenges of connecting tomorrow’s workforce. Employees are more mobile than ever before; they carry multiple company issued and personal computing devices and smart mobile devices; and they want fast, easy yet secure connectivity that empowers them to do their jobs effectively and quickly. The MAG Series Junos Pulse Gateways enable companies to build an infrastructure that can provide this simple and secure role-based connectivity for their users while minimizing the costs. One of the key services delivered by the MAG Series is Junos Pulse Secure Access Service. Junos Pulse Secure Access Service provides secure, authenticated access via SSL VPN for remote and mobile users from any web-enabled device to corporate resources—anytime, anywhere.

Product Description

Enterprises and service providers have the difficult challenge of providing location- and device-independent network connectivity that is secure and capable of limiting resource access to authorized users. Breaches and threats continue to spiral out of control, and employees and users want to use their own personal smartphones, mobile and computing devices to access the enterprise network, applications, and corporate data, making this challenge even more difficult. Juniper Networks® Junos® Pulse Secure Access Service is a simple, intuitive service that provides secure, authenticated access for remote and mobile users from any web-enabled device to corporate resources—anytime, anywhere. Junos Pulse Secure Access Service uses SSL, the security protocol found in all standard Web browsers. The use of SSL eliminates the need for preinstalled client software, changes to internal servers, and costly ongoing maintenance and desktop support.

Junos Pulse Secure Access Service includes Juniper Networks Junos Pulse, a dynamic, integrated, multiservice network client for mobile and non-mobile devices. Junos Pulse enables optimized, accelerated anytime, anywhere access to corporate data. It enables secure SSL access from a wide range of mobile and non-mobile devices, including smartphones, netbooks, notebooks, Wi-Fi, or 3G-enabled devices. Junos Pulse delivers improved productivity and secure, ubiquitous access to corporate data and applications. For more details on Junos Pulse, please visit www.juniper.net/us/en/products-services/software/junos-platform/junos-pulse.

Architecture and Key Components

The Junos Pulse Secure Access Service can be enabled on the following MAG Series Junos Pulse Gateways to support the secure remote access needs of companies of all sizes:

- **MAG2600:** Fixed configuration appliance ideal for small and medium businesses, the MAG2600 can support up to 100 SSL VPN concurrent users.
- **MAG4610:** Fixed configuration appliance ideal for medium and large businesses. The MAG4610 can support up to 1,000 SSL VPN concurrent users.
- **MAG6610:** Chassis-based appliance ideal for scalable large businesses, the MAG6610 can support up to 20,000 SSL VPN concurrent users. Requires at least one service module to be ordered and installed (MAG-SM160 or MAG-SM360) to get SSL VPN functionality on the chassis. MAG6610 can support up to two service modules.

- **MAG6611:** Chassis-based appliance ideal to meet the highest scalability needs of large businesses, the MAG6611 can support up to 40,000 SSL VPN concurrent users. Requires at least one service module to be ordered and installed (MAG-SM160 or MAG-SM360) to get SSL VPN functionality on the chassis. MAG6611 can support up to four service modules.
- **MAG-SM160:** Service module for MAG6610 or MAG6611 that supports 1,000 SSL VPN users.
- **MAG-SM360:** Service module for MAG6610 or MAG6611 that supports 10,000 SSL VPN users.
- **MAG-CM060:** Optional management module for MAG6610 or MAG6611. Only orderable with at least one service module and a maximum of one management module can be ordered per chassis.

For more details on MAG Series hardware, including the specifications and ordering information of each model, please refer to the MAG Series Junos Pulse Gateways data sheet.

Features and Benefits

Junos Pulse

Junos Pulse is a simplified, integrated, multiservice network client enabling anytime, anywhere connectivity, security, and acceleration that requires minimal user interaction. Junos Pulse makes secure network and cloud access easy through virtually any device—mobile or non-mobile, Wi-Fi or 3G-enabled, managed or unmanaged—over a broad array of computing and mobile operating systems. The following table provides the key features and benefits of Junos Pulse working with MAG Series gateways.

Table 1. Key Features of Junos Pulse working with MAG Series Junos Pulse Gateways

FEATURE	FEATURE DESCRIPTION
Layer 3 SSL VPN (Network Connect)	<ul style="list-style-type: none"> • Layer 3 VPN connectivity with granular access control. • SSL mode only; no Encapsulating Security Payload (ESP) mode.
Location awareness	<ul style="list-style-type: none"> • Seamless roaming from remote access to local LAN access. • Junos Pulse can be preconfigured by administrators to automatically prompt end users for credentials to authenticate to the MAG Series gateways when they are remote.
Endpoint security	<ul style="list-style-type: none"> • Full Host Checker capability to check endpoint security. • Enhanced Endpoint Security (EES) delivers on-the-fly malware protection, pre-connection scanning policies, and real-time protection supported by both SSL VPN and network access control (NAC) capability on the MAG Series Junos Pulse Gateways.
Split tunneling options (enable or disable with overriding route capability and route monitoring)	<ul style="list-style-type: none"> • Key split tunneling options of Network Connect (NC) supported. • Enforces secure, granular access control.
Flexible launch options (standalone client, browser-based launch)	<ul style="list-style-type: none"> • Users can easily launch Junos Pulse via the Web from the SSL VPN landing page. • Remote users can simply launch Junos Pulse from their desktop.
Pre-configuration options (preconfigured installer to contain list of MAG Series appliances)	<ul style="list-style-type: none"> • Administrators can preconfigure a Junos Pulse deployment with a list of corporate MAG Series appliances for end users to choose from.
Connectivity options (max/idle session timeouts, automatic reconnect, logging)	<ul style="list-style-type: none"> • Administrators can set up flexible connectivity options for remote users
Authentication options (hardware token, smart cards, or soft token)	<ul style="list-style-type: none"> • Administrators can deploy Junos Pulse for remote user authentication using a hardware token or smart cards. • Junos Pulse supports integration with RSA SoftID, allowing automatic access to the user's RSA pass codes using the PIN entered by the user.

For more details on Junos Pulse, please visit www.juniper.net/us/en/products-services/software/junos-platform/junos-pulse/.

Table 2. End-to-End Layered Security Features and Benefits (continued)

End-to-End Layered Security

Junos Pulse Secure Access Service for the MAG Series Junos Pulse Gateways provides complete end-to-end layered security, including endpoint client, device, data, and server layered security controls.

Table 2. End-to-End Layered Security Features and Benefits

FEATURE	FEATURE DESCRIPTION	BENEFITS
Anti-malware support with Enhanced Endpoint Security (EES)	Dynamically download Webroot's market-leading anti-malware software to enforce endpoint security on devices which may not be corporate assigned computers being used for network access.	Protects endpoints from infection in real time from anti-malware, and thereby protects corporate resources from harm during network access. Enables dynamic enforcement of anti-malware protection on unmanaged assets such as the PCs of external partners, customers, or suppliers.
Endpoint auto-remediation	Automatically remediates noncompliant endpoints by updating software applications that do not comply to corporate security policies. Does not require Microsoft's Short Message Service (SMS) protocol for remediation and covers patches for Microsoft and other vendors such as Adobe, Firefox, Apache, Real Player, and others. Directly downloads missing patches from vendor's website without going through Juniper Networks MAG Series gateways.	Improves productivity of remote users who will gain immediate access to the corporate network without having to wait for periodic updates of software applications, and ensures compliance with corporate security policies.
Host Checker	Client computers can be checked both prior to and during a session to verify an acceptable device security posture requiring installed/running endpoint security applications (antivirus, firewall, other). Also supports custom-built checks such as verifying ports opened/closed, checking files/processes and validating their authenticity with Message Digest 5 (MD5) hash checksums, verifying registry settings, machine certificates, and more. Includes cache cleaner that erases all proxy downloads and temp files at logout.	Verifies/ensures that endpoint devices meet corporate security policy requirements before granting access, remediating devices, and quarantining users when necessary. Also, ensures that no potentially sensitive data is left behind on the endpoint device.
Host Checker API	Created in partnership with best-in-class endpoint security vendors. Enables enterprises to enforce an endpoint trust policy for managed PCs that have personal firewall, antivirus clients, or other installed security clients, and quarantine noncompliant devices.	Uses current security policies with remote users and devices; easier management.
Trusted Network Connect (TNC) support on Host Checker	Allows interoperability with diverse endpoint security solutions from antivirus to patch management to compliance management solutions.	Enables customers to leverage existing investments in endpoint security solutions from third-party vendors.
Policy-based enforcement	Allows the enterprise to establish trustworthiness of non-API compliant hosts without writing custom API implementations or locking out external users such as customers or partners running other security clients.	Enables access to extranet endpoint devices like PCs from partners who may run different security clients than that of the enterprise.
Security services with kernel-level packet filtering and safe routing	Undesirable traffic is dropped before it is processed by the TCP stack.	Ensures that unauthenticated connection attempts such as malformed packets or denial of service (DoS) attacks are filtered out.
Secure virtual workspace	A secure and separate environment for remote sessions encrypts all data and controls I/O access (printers, drives).	Ensures that all corporate data is securely deleted from unsecure kiosks after a session.

Ease of Administration

In addition to enterprise-class security benefits, Junos Pulse Secure Access Service for the MAG Series has a wealth of features that make it easy for the administrator to deploy and manage.

Table 3: Ease of Administration Features and Benefits

FEATURE	FEATURE DESCRIPTION	BENEFITS
Bridge Certificate Authority (CA) support	Supports federated public key infrastructure (PKI) deployments with client certificate authentication. Bridge CA is a PKI extension (as specified in RFC 5280) to cross-certify client certificates that are issued by different trust anchors (Root CAs). Also, enables the customer to configure policy extensions in the admin UI, to enforce during certificate validation. These policy extensions can be configured as per RFC 5280 guidelines.	Enables customers who use advanced PKI deployments to deploy the MAG Series Junos Pulse Gateways to perform strict standards-compliant certificate validation—before allowing data and applications to be shared between organizations and users.
Extensive directory integration and broad interoperability	Existing directories in customer networks can be leveraged for authentication and authorization, enabling granular secure access without recreating those policies.	Existing directory investments can be leveraged with no infrastructure changes and no APIs for directory integration, as they are all native/built-in.
Integration with strong authentication and identity and access management platforms	Ability to support SecurID, Security Assertion Markup Language (SAML) including standards-based SAML v2.0 support, and PKI/digital certificates.	Leverages existing corporate authentication methods to simplify administration.
Multiple hostname support	Ability to host different virtual extranet websites from a single appliance.	Saves the cost of incremental servers, eases management overhead, and provides a transparent user experience with differentiated entry URLs.
Customizable user interface	Creation of completely customized sign-on pages.	Provides an individualized look for specified roles, streamlining the user experience.
Juniper Networks Network and Security Manager	Intuitive centralized UI for configuring, updating, and monitoring MAG Series Junos Pulse Gateways within a single device/cluster or across a global cluster deployment.	Enables companies to conveniently manage, configure, and maintain MAG Series gateways and other Juniper devices from one central location.
Cross-platform support	Ability for any platform to gain access to resources such as Windows, Mac, Linux, or various mobile devices such as iPhone, WinMobile, Symbian, and Android.	Provides flexibility in allowing users to access corporate resources from any type of device using any type of operating system.
Enterprise licensing	Allows any organization with one or more devices to easily lease licenses from one appliance to another as required to adapt to changing organizational needs.	Provides administrators the ability to start with minimal licensing costs per device, and then incrementally upgrade to enterprise leased licensing capabilities as needed.

Rich Access Privilege Management Capabilities

Junos Pulse Secure Access Service for the MAG Series gateways provides dynamic access privilege management capabilities without infrastructure changes, custom development, or software deployment/maintenance. This facilitates the easy deployment and maintenance of secure remote access, as well as secure extranets and intranets. When users log into MAG Series, they pass through a pre-authentication assessment, and are then dynamically mapped to the session role that combines established network, device, identity, and session policy settings. Granular resource authorization policies further ensure exact compliance to security restrictions.

Table 4: Access Privilege Management Features and Benefits

FEATURE	FEATURE DESCRIPTION	BENEFITS
NAC-SSL VPN federation	Seamlessly provision SSL VPN user sessions into NAC sessions upon login, or the alternative (provisioning of NAC sessions into the SSL VPN sessions). Users need to authenticate only one time to get access in these types of environments.	Provides users, whether remote or local, seamless access with a single login to corporate resources that are protected by access control policies. Simplifies the end user experience.
Certificate authentication to backend servers	Enables customers to enforce client authentication on their secure backend servers, and allows the MAG Series gateways to present an admin-configured certificate to these servers for authentication.	Allows customers to mandate strict SSL policies on their backend servers by configuring client authentication.
Client certification authorization for ActiveSync	Any mobile device supporting ActiveSync along with client side certificates can now be challenged for a valid client certificate before being allowed access to the ActiveSync server.	Enables the administrator to enforce strict mobile authentication policies for ActiveSync access from mobile devices.
Multiple sessions per user	Allows remote users to launch multiple sessions to the MAG Series gateways.	Enables remote users to have multiple authenticated sessions open at the same time.
User record synchronization	Supports synchronization of user records such as user bookmarks across different non-clustered MAG Series gateways.	Ensures ease of experience for users who often travel from one region to another and therefore need to connect to different MAG Series Junos Pulse Gateways.
Virtual Desktop Infrastructure (VDI) support	Allows interoperability with VMware View Manager and Citrix XenDesktop to enable administrators to deploy virtual desktops with the MAG Series gateways.	Provides remote users seamless access to their virtual desktops hosted on VMware or Citrix servers. Provides dynamic delivery of the Citrix ICA client or the VMware View client, including dynamic client fallback options to allow users to easily connect to their virtual desktops.
ActiveSync feature	Provides secure access connectivity from mobile devices (such as Symbian, Windows Mobile, or iPhone) to the Exchange Server with no client software installation. Enables up to 5,000 simultaneous sessions.	Enables customers to allow a large number of users (including employees, contractors, and partners) to access corporate resources through mobile phones via ActiveSync.
Mobile-friendly SSL VPN login pages	Provides predefined HTML pages that are customized for mobile devices, including Apple iPhone and iPad, Google Android, and Nokia Symbian devices.	Provides mobile device users with a simplified and enhanced user experience with webpages customized for their device types.
Dynamic role mapping with custom expressions	Combines network, device, and session attributes to determine which types of access are allowed. A dynamic combination of attributes on a per-session basis can be used to make the role mapping decision.	Enables the administrator to provision by purpose for each unique session.
Resource authorization	Provides extremely granular access control to the URL, server, or file level for different roles of users.	Allows administrators to tailor security policies to specific groups, providing access only to essential data.
Granular auditing and logging	Can be configured to the per-user, per-resource, per-event level for security purposes as well as capacity planning.	Provides fine-grained auditing and logging capabilities in a clear, easy to understand format.

Flexible Single Sign-On (SSO) Capabilities

Junos Pulse Secure Access Service for the MAG Series Junos Pulse Gateways offers comprehensive single sign-on features. These features increase end user productivity, greatly simplify administration of large diverse user resources, and significantly reduce the number of help desk calls.

Table 5: Flexible Single Sign-on Features and Benefits

FEATURE	FEATURE DESCRIPTION	BENEFITS
Kerberos Constrained Delegation	Support for Kerberos Constrained Delegation protocol. When a user logs into the MAG Series gateway with a credential that cannot be proxied through to the backend server, the gateway will retrieve a Kerberos ticket on behalf of the user from the Active Directory infrastructure. The ticket will be cached on the Junos Pulse Gateway throughout the session. When the user accesses Kerberos-protected applications, the Junos Pulse Gateway will use the cached Kerberos credentials to log the user into the application without prompting for a password.	Eliminates the need for companies to manage static passwords resulting in reduced administration time and costs.
Kerberos SSO and NT LAN Manager (NTLMv2) support	MAG Series Junos Pulse Gateways will automatically authenticate remote users via Kerberos or NTLMv2 using user credentials.	Simplifies user experience by avoiding having users enter credentials multiple times to access different applications.
Password management integration	Standards-based interface for extensive integration with password policies in directory stores (LDAP, Microsoft Active Directory, NT, and others).	Leverages existing servers to authenticate users; users can manage their passwords directly through the MAG Series gateway interface.
Web-based SSO basic authentication and NTLM	Allows users to access other applications or resources that are protected by another access management system without re-entering login credentials.	Alleviates the need for end users to enter and maintain multiple sets of credentials for web-based and Microsoft applications.
Web-based SSO forms-based, header variable-based, SAML-based	Ability to pass user name, credentials, and other customer-defined attributes to the authentication forms of other products and as header variables.	Enhances user productivity and provides a customized experience.

Provision by Purpose

Junos Pulse Secure Access Service for the MAG Series Junos Pulse Gateways includes different access methods. These different methods are selected as part of the user's role, so the administrator can enable the appropriate access on a per-session basis, taking into account user, device, and network attributes in combination with enterprise security policies.

Table 6: Provisioning Features and Benefits

FEATURE	FEATURE DESCRIPTION	BENEFITS
IPsec/Internet Key Exchange (IKEv2) support for mobile devices	Allows remote users to connect from devices such as PDAs, mobile devices, and smartphones which support IKEv2 VPN connectivity. Administrator can enable strict certificate authentication for access via IPsec/IKEv2. Administrator can also enable username/password authentication through Extensible Authentication Payload (EAP), whereby IKEv2 provides a "tunnel" mechanism for EAP authentication.	Extends Juniper's leading mobility and access control features to a broad range of devices and OS platforms that support IKEv2 VPN connectivity. Enables remote users to securely authenticate to the MAG Series Junos Pulse Gateways from platforms that support IKEv2 VPN connectivity.
Clientless core Web access	Access to web-based applications, including complex JavaScript, XML, or Flash-based apps and Java applets that require a socket connection, as well as standards-based email like Outlook Web Access (OWA), Windows and UNIX file share, telnet/SSH hosted applications, terminal emulation, SharePoint (including extensive SharePoint 2010 support), and others.	Provides the most easily accessible form of application and resource access from a variety of end user machines, including handheld devices; enables extremely granular security control options; completely clientless approach using only a Web browser.
Secure Application Manager (SAM)	A lightweight Java or Windows-based download enabling access to client/server applications.	Enables access to client/server applications using just a Web browser; also provides native access to terminal server applications without the need for a preinstalled client.
Network Connect (NC)	Provides complete network-layer connectivity via an automatically provisioned cross-platform download; Windows Logon/Graphical Identification and Authentication (GINA) integration for domain SSO; installer services to mitigate need for admin rights. Allows for split tunneling capability.	Users only need a Web browser. NC transparently selects between two possible transport methods to automatically deliver the highest performance possible for every network environment. When used with Juniper Networks Basic Installation services, no admin rights are needed to install, run, and upgrade NC; optional standalone installation is available as well. Split tunneling capability provides flexibility to specify which subnets or hosts to include or exclude from being tunneled.
Junos Pulse	Single, integrated, remote access client that can also provide LAN access control, WAN acceleration, and dynamic VPN features to remote users.	Pulse replaces the need to deploy and maintain multiple, separate clients for different functionalities such as VPN, LAN access control, and WAN acceleration. By seamlessly integrating all of these functionalities into one single, easy-to-use client, administrators can save on client management and deployment costs to end users.

Product Options

Junos Pulse Secure Access Service currently includes several license options for enablement on the MAG Series Junos Pulse Gateways.

User License (Common Access License)

With the MAG Series Junos Pulse Gateways, common access licenses are available as user licenses. With common access licensing, the licenses can either be used for SSL VPN user sessions or NAC user sessions. Please see the Ordering Information section for licensing details.

The common access user licenses provide the functionality that allows users to access the network. They fully meet the needs of both basic and complex deployments with diverse audiences and use cases, and they require little or no client software, server changes, DMZ buildouts, or software agent deployments. For administrative ease of user license counts, each license only enables as many users as specified in the license and they are additive. For example, if a 100 user license was originally purchased and the concurrent user count grows over the next year

to exceed that amount, simply adding another 100 user license to the system will now allow for up to 200 concurrent users.

Key features enabled by this license include:

- Junos Pulse, Secure Application Manager (SAM), and NC provide cross-platform support for client/server applications using SAM, as well as full network-layer access using the SSL transport mode of Junos Pulse and the adaptive dual transport methods of Network Connect. The combination of SAM, Junos Pulse, and NC with core clientless access provides secure access to virtually any audience, from remote/mobile workers to partners or customers, using a wide range of devices from any network.
- Provision by purpose goes beyond role-based access controls and allows administrators to properly, accurately, and dynamically balance security concerns with access requirements.
- Advanced PKI support includes the ability to import multiple root and intermediate certificate authorities (CAs), Online Certificate Status Protocol (OCSP), and multiple server certificates.

- User self-service provides the ability for users to create their own favorite bookmarks, including accessing their own workstation from a remote location, and even changing their password when it is set to expire.
- Multiple hostname support (for example, <https://employees.company.com>, <https://partners.company.com>, and <https://employees.company.com/engineering>) can all be made to look as though users are the only ones using the system, complete with separate logon pages and customized views that uniquely target the needs and desires of that audience.
- User interfaces are customizable for users and delegated administrative roles.
- Advanced endpoint security controls such as Host Checker, cache cleaner, and secure virtual workspace work to ensure that users are dynamically provisioned to access systems and resources only to the degree that their remote systems are compliant with the organization's security policy, after which remnant data is scrubbed from the hard drive so that nothing is left behind.

High Availability Clustering Capability (No Additional License Required)

Customers have the ability to build clusters without buying any additional licenses. The clustering method can be explained in two simple steps:

1. Simply place an equal number of user (“-ADD”) licenses on each box.
2. When they are joined together to form a cluster, all of the user licenses add up so that the cluster can now support all of the licensed users. For example, building a cluster of 1,000 users is done by bringing together two boxes with 500 user licenses in each of the two units.

Clustering allows you to share licenses from one MAG Series gateway with one or more additional MAG Series gateways. These are not additive to the concurrent user licenses. For example, if a customer has a 100 user license for the MAG4610 and then purchases another MAG4610, this provides a total of 100 users that are shared across both appliances, not per appliance.

Clustering supports stateful peering and failover across the LAN, so in the unlikely event that one unit fails, system configurations (such as authentication server, authorization groups, and bookmarks), user profile settings (such as user defined bookmarks and cookies), and user sessions are preserved. Failover is seamless, so there is no interruption to user/enterprise productivity, no need for users to log in again, and no downtime.

Secure Meeting License (Optional)

The Juniper Networks Secure Meeting optional license extends the capabilities of the MAG Series by providing secure anytime, anywhere, cost-effective online Web conferencing and remote control PC access. Secure Meeting enables real-time application sharing so that authorized employees and partners can easily schedule online meetings or activate instant meetings through an intuitive Web interface that requires no training or special deployments. Help desk staff or customer service representatives can provide remote assistance to users and customers by remotely controlling their PCs without requiring the user to install any software. Best-in-class authentication, authorization, and accounting (AAA) capabilities enable companies to easily integrate Secure Meeting with their existing internal authentication infrastructure and policies.

For the MAG Series, Secure Meeting is licensed through a concurrent user model. Secure Meeting supports four license options on the MAG Series. Up to 25, 50, 100, or 250 concurrent meeting user options are offered. Please note that the meeting user count is separate from the concurrent SSL VPN user count on the MAG Series. Also, there is a limit to the maximum number of licenses that can be supported on certain MAG Series models:

- A single MAG2600 will support up to 50 concurrent meeting users.
- A single MAG4610 will support up to 100 concurrent meeting users.
- The MAG-SM160 service module will support up to 100 concurrent meeting users.
- The MAG-SM360 service module will support up to 250 concurrent meeting users.

The Secure Meeting licenses are additive up to the maximum limit supported on a given platform. For example, on a single MAG2600, the customer can start with a 25 user license and then add another 25 users to support up to 50 concurrent meeting users (maximum limit) on that platform.

ICE License (Optional)

SSL VPNs can help keep organizations and businesses functioning by connecting people even during the most unpredictable circumstances—hurricanes, terrorist attacks, transportation strikes, pandemics, or virus outbreaks—the result of which could mean the quarantine or isolation of entire regions or groups of people for an extended period of time. With the right balance of risk and cost, the ICE offering delivers a timely solution for addressing a dramatic peak in demand for remote access to ensure business continuity whenever a disastrous event strikes. ICE provides licenses for a large number of additional users on a MAG Series gateway for a limited time.

With ICE, businesses can do the following:

- Maintain productivity by enabling ubiquitous access to applications and information for employees from anywhere, at any time, and on any device
- Sustain partnerships with around-the-clock, real-time access to applications and services while knowing resources are secured and protected
- Continue to deliver exceptional service to customers and partners with online collaboration
- Meet federal and government mandates for contingencies and continuity of operations (COOP) compliance
- Balance risk and scalability with cost and ease of deployment

For the MAG Series, the ICE licenses come in two forms: full ICE (following the same design as prior releases such as the SA Series ICE license option), and a new 25% burst license (which allows bursting of up to 25% of the installed license count on any given MAG Series gateway.) For example, if the customer has a MAG6610 with a 1,000 user license, the 25% burst license option will support an additional 250 users during an unplanned event.

Anti-Malware Support with Enhanced Endpoint Security (EES) (Optional)

The number of newly discovered malicious programs that can harm endpoint devices such as PCs continues to grow and replicate at an alarming rate. Malware is known to cost enterprises an increasing amount of money every year in terms of efforts involved to quarantine and remediate appropriate endpoints.

In order to prevent endpoints—either on the LAN or WAN—from being infected with malware, Juniper Networks offers the Enhanced Endpoint Security license option. This license is a full featured, dynamically deployable anti-malware module that is an OEM of Webroot's industry-leading Spy Sweeper product. This

dynamic anti-malware download capability is also available with Juniper Networks Unified Access Control. With this new capability, organizations can ensure that unmanaged and managed Microsoft Windows endpoint devices conform to corporate security policies before they are allowed access to the network, applications, and resources. For example, potentially harmful keyloggers can be found and removed from an endpoint device before users enter sensitive information such as their user credentials. The Enhanced Endpoint Security license protects endpoints from infection in real time and ensures that only clean endpoints are granted access to the network. Enhanced Endpoint Security licenses are available as 1-year, 2-year, and 3-year subscription options (see the Ordering Information section for more details).

Premier Java RDP Applet (Optional)

With the Premier Java RDP Applet option, users can remotely access centralized Windows applications independent of the client platform (Mac, Linux, Windows, and so on) through Java-based technology.

As a platform-independent solution, the Premier Java RDP Applet lets you use the entire range of Windows applications running on the Windows Terminal Server, regardless of how the client computer is equipped. By centrally installing and managing all Windows applications, you can significantly reduce your total cost of ownership. The Premier Java RDP Applet is an OEM of the HOblink JWT (Java Windows Terminal) product created by HOB Inc., a leading European software company specializing in Java programming.

Specifications

For specification details on the MAG Series, please refer to the MAG Series Junos Pulse Gateways datasheet.

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services and support, which are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to bring revenue-generating capabilities online faster so you can realize bigger productivity gains and faster rollouts of new business models and ventures. At the same time, Juniper Networks ensures operational excellence by optimizing your network to maintain required levels of performance, reliability, and availability. For more details, please visit www.juniper.net/us/en/products-services.

Ordering Information

MODEL NUMBER	DESCRIPTION
Service Module for MAG6610 or MAG6611	
MAG2600	MAG2600 Junos Pulse Gateway for SSL VPN and Guest Access.
MAG4610	MAG4610 fixed configuration Junos Pulse Gateway for SSL VPN users or NAC users.
MAG6610	MAG6610 Junos Pulse Gateway for SSL VPN or NAC users; includes MAG-PS661 560 W AC power supply. Must order at least one service module (MAG-SM160 or MAG-SM360).
MAG6611	MAG6611 chassis Junos Pulse Gateway for SSL VPN or NAC users; includes MAG-PS662 750 W AC power supply. Must order at least one service module (MAG-SM160 or MAG-SM360).
MAG-SM160	MAG-SM160 service module for MAG6610 and MAG6611 gateways. Supports 1,000 SSL VPN or 5,000 UAC users.
MAG-SM360	MAG-SM360 service module for MAG6610 and MAG6611 gateways. Supports 10,000 SSL VPN or 15,000 UAC users.
MAG-CM060	MAG-CM060 management module for MAG6610 or MAG6611 gateways. Only orderable with at least one service module, and a maximum of one management module can be ordered per chassis.

User Licenses (Common Access Licenses)

ACCESSX600-ADD-10U	Add 10 simultaneous users to Junos Pulse Gateway X600 Series Appliances
ACCESSX600-ADD-25U	Add 25 simultaneous users to Junos Pulse Gateway X600 Series Appliances
ACCESSX600-ADD-50U	Add 50 simultaneous users to Junos Pulse Gateway X600 Series Appliances
ACCESSX600-ADD-100U	Add 100 simultaneous users to Junos Pulse Gateway X600 Series Appliances
ACCESSX600-ADD-250U	Add 250 simultaneous users to Junos Pulse Gateway X600 Series Appliances
ACCESSX600-ADD-500U	Add 500 simultaneous users to Junos Pulse Gateway X600 Series Appliances
ACCESSX600-ADD-1000U	Add 1,000 simultaneous users to Junos Pulse Gateway X600 Series Appliances
ACCESSX600-ADD-2000U	Add 2,000 simultaneous users to Junos Pulse Gateway X600 Series Appliances

MODEL NUMBER	DESCRIPTION
ACCESSX600-ADD-2500U	Add 2,500 simultaneous users to Junos Pulse Gateway X600 Series Appliances
ACCESSX600-ADD-5000U	Add 5,000 simultaneous users to Junos Pulse Gateway X600 Series Appliances
ACCESSX600-ADD-7500U	Add 7,500 simultaneous users to Junos Pulse Gateway X600 Series Appliances
ACCESSX600-ADD-10KU	Add 10,000 simultaneous users to Junos Pulse Gateway X600 Series Appliances
ACCESSX600-ADD-15KU	Add 15,000 simultaneous users to Junos Pulse Gateway X600 Series Appliances
ACCESSX600-ADD-20KU	Add 20,000 simultaneous users to Junos Pulse Gateway X600 Series Appliances
ACCESSX600-ADD-25KU	Add 25,000 simultaneous users to Junos Pulse Gateway X600 Series Appliances

Secure Meeting Licenses

ACCESSX600-MTG-25U	Add 25 simultaneous Secure Meeting users to X600 Series Appliances
ACCESSX600-MTG-50U	Add 50 simultaneous Secure Meeting users to X600 Series Appliances
ACCESSX600-MTG-100U	Add 100 simultaneous Secure Meeting users to X600 Series Appliances
ACCESSX600-MTG-250U	Add 250 simultaneous Secure Meeting users to X600 Series Appliances

ICE Licenses

ACCESS-ICE-25PC	In Case of Emergency (ICE) 25%: Burst to 25% of installed license count on X500 or X600 Series Appliances
MAGX600-ICE	In Case of Emergency (ICE) License for X600 Appliances

Enhanced Endpoint Security Licenses

ACCESS-EES-50U-1YR	Enhanced Endpoint Security subscription, 50 concurrent users, 1-year
ACCESS-EES-100U-1YR	Enhanced Endpoint Security subscription, 100 concurrent users, 1-year
ACCESS-EES-250U-1YR	Enhanced Endpoint Security subscription, 250 concurrent users, 1-year
ACCESS-EES-500U-1YR	Enhanced Endpoint Security subscription, 500 concurrent users, 1-year
ACCESS-EES-1000U-1YR	Enhanced Endpoint Security subscription, 1,000 concurrent users, 1-year
ACCESS-EES-2500U-1YR	Enhanced Endpoint Security subscription, 2,500 concurrent users, 1-year
ACCESS-EES-5000U-1YR	Enhanced Endpoint Security subscription, 5,000 concurrent users, 1-year
ACCESS-EES-7500U-1YR	Enhanced Endpoint Security subscription, 7,500 concurrent users, 1-year
ACCESS-EES-50U-2YR	Enhanced Endpoint Security subscription, 50 concurrent users, 2-years
ACCESS-EES-100U-2YR	Enhanced Endpoint Security subscription, 100 concurrent users, 2-years
ACCESS-EES-250U-2YR	Enhanced Endpoint Security subscription, 250 concurrent users, 2-years
ACCESS-EES-500U-2YR	Enhanced Endpoint Security subscription, 500 concurrent users, 2-years
ACCESS-EES-1000U-2YR	Enhanced Endpoint Security subscription, 1,000 concurrent users, 2-years
ACCESS-EES-2500U-2YR	Enhanced Endpoint Security subscription, 2,500 concurrent users, 2-years

MODEL NUMBER	DESCRIPTION
Enhanced Endpoint Security Licenses	
ACCESS-EES-5000U-2YR	Enhanced Endpoint Security subscription, 5,000 concurrent users, 2-years
ACCESS-EES-7500U-2YR	Enhanced Endpoint Security subscription, 7,500 concurrent users, 2-years
ACCESS-EES-50U-3YR	Enhanced Endpoint Security subscription, 50 concurrent users, 3-years
ACCESS-EES-100U-3YR	Enhanced Endpoint Security subscription, 100 concurrent users, 3-years
ACCESS-EES-250U-3YR	Enhanced Endpoint Security subscription, 250 concurrent users, 3-years
ACCESS-EES-500U-3YR	Enhanced Endpoint Security subscription, 500 concurrent users, 3-years
ACCESS-EES-1000U-3YR	Enhanced Endpoint Security subscription, 1,000 concurrent users, 3-years
ACCESS-EES-2500U-3YR	Enhanced Endpoint Security subscription, 2,500 concurrent users, 3-years
ACCESS-EES-5000U-3YR	Enhanced Endpoint Security subscription, 5,000 concurrent users, 3-years
ACCESS-EES-7500U-3YR	Enhanced Endpoint Security subscription, 7,500 concurrent users, 3-years

Premier RDP Applet Licenses

ACCESS-RDP-50U-1YR	Java RDP Applet 1-year subscription for 50 simultaneous users
ACCESS-RDP-100U-1YR	Java RDP Applet 1-year subscription for 100 simultaneous users
ACCESS-RDP-250U-1YR	Java RDP Applet 1-year subscription for 250 simultaneous users
ACCESS-RDP-500U-1YR	Java RDP Applet 1-year subscription for 500 simultaneous users
ACCESS-RDP-1000U-1YR	Java RDP Applet 1-year subscription for 1,000 simultaneous users
ACCESS-RDP-2000U-1YR	Java RDP Applet 1-year subscription for 2,000 simultaneous users
ACCESS-RDP-2500U-1YR	Java RDP Applet 1-year subscription for 2,500 simultaneous users
ACCESS-RDP-5000U-1YR	Java RDP Applet 1-year subscription for 5,000 simultaneous users
ACCESS-RDP-7500U-1YR	Java RDP Applet 1-year subscription for 7,500 simultaneous users
ACCESS-RDP-10KU-1YR	Java RDP Applet 1-year subscription for 10,000 simultaneous users
ACCESS-RDP-50U-2YR	Java RDP Applet 2-year subscription for 50 simultaneous users
ACCESS-RDP-100U-2YR	Java RDP Applet 2-year subscription for 100 simultaneous users
ACCESS-RDP-250U-2YR	Java RDP Applet 2-year subscription for 250 simultaneous users
ACCESS-RDP-500U-2YR	Java RDP Applet 2-year subscription for 500 simultaneous users
ACCESS-RDP-1000U-2YR	Java RDP Applet 2-year subscription for 1,000 simultaneous users
ACCESS-RDP-2000U-2YR	Java RDP Applet 2-year subscription for 2,000 simultaneous users
ACCESS-RDP-2500U-2YR	Java RDP Applet 2-year subscription for 2,500 simultaneous users
ACCESS-RDP-5000U-2YR	Java RDP Applet 2-year subscription for 5,000 simultaneous users

MODEL NUMBER	DESCRIPTION
Premier RDP Applet Licenses (continued)	
ACCESS-RDP-7500U-2YR	Java RDP Applet 2-year subscription for 7,500 simultaneous users
ACCESS-RDP-10KU-2YR	Java RDP Applet 2-year subscription for 10,000 simultaneous users
ACCESS-RDP-50U-3YR	Java RDP Applet 3-year subscription for 50 simultaneous users
ACCESS-RDP-100U-3YR	Java RDP Applet 3-year subscription for 100 simultaneous users
ACCESS-RDP-250U-3YR	Java RDP Applet 3-year subscription for 250 simultaneous users
ACCESS-RDP-500U-3YR	Java RDP Applet 3-year subscription for 500 simultaneous users
ACCESS-RDP-1000U-3YR	Java RDP Applet 3-year subscription for 1,000 simultaneous users
ACCESS-RDP-2000U-3YR	Java RDP Applet 3-year subscription for 2,000 simultaneous users
ACCESS-RDP-2500U-3YR	Java RDP Applet 3-year subscription for 2,500 simultaneous users
ACCESS-RDP-5000U-3YR	Java RDP Applet 3-year subscription for 5,000 simultaneous users
ACCESS-RDP-7500U-3YR	Java RDP Applet 3-year subscription for 7,500 simultaneous users
ACCESS-RDP-10KU-3YR	Java RDP Applet 3-year subscription for 10,000 simultaneous users

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2011 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.