Pulse Secure

MAG Series Pulse Gateways

Data Sheet

Published Date **July 2015**

Product Overview

The challenge for today's agile business is to deploy an infrastructure that enables fast and secure access to the corporate network, as well as cloud applications and resources for all workers—telecommuters, mobile workers, office workers, contractors, guests, partners and others—while minimizing costs. The Pulse Secure MAG Series Pulse Gateways deliver SSL VPN connectivity and/or network access control through a single converged gateway. Pulse Secure Pulse and the MAG Series gateways address the needs of today's users, regardless if they are mobile, remote, or local, delivering performance and security while keeping costs low.

Product Description

Your ideas. Connected.™

The Pulse Secure® MAG Series Pulse® Pulse Gateways work in concert with Pulse Secure's Pulse and its services to meet the secure remote and LAN access needs for small and medium-sized businesses (SMBs), government agencies, and large, multinational enterprises. The MAG Series gateways deliver secure connectivity and/or access control, offering a significant reduction in OpEx and CapEx costs, increased deployment density, extensive scalability, and easily reconfigurable "personality" changes between secure mobile and remote access control and network access control (NAC) modes. The combination of extensible, purpose-built gateways working hand-in-hand with Pulse and its associated services—including the Pulse Secure Access Service and Pulse Access Control Service—delivers secure mobile, remote, and LAN-based access control for users of mobile devices, laptops, and desktops in a way that is specifically designed to change the economics of enterprise security and the access infrastructure.

Architecture and Key Components

The MAG Series Pulse Gateways are offered in four models to meet the access needs of enterprises and organizations of all types and sizes.

The Pulse Secure MAG2600 Pulse Gateway meets the SSL VPN or Unified Access Control (UAC) requirements of small and medium-sized enterprises. With its quiet operation and tabletop form factor, the MAG2600 provides the ultimate flexibility in deployment. The MAG2600 comes with a single application engine in a fixed hardware configuration and supports up to 100 concurrent SSL VPN or 250 concurrent UAC users. Alternatively, the MAG2600 may be licensed for Enterprise Guest Access, supporting up to 200 concurrent guest users. The MAG2600's compact size (4 x 7 in) in a 1 U form factor allows it to be mounted in a rack or even placed on a desk.

The MAG4610 Pulse Gateway is designed to meet the secure network and application access control needs of medium to large-sized enterprises. The MAG4610 supports either SSL VPN or UAC functionality in a fixed hardware configuration design. The MAG4610 is 1 U high and one-half rack wide, and may be deployed side-by-side in a 1 U space. The MAG4610 supports up to 1,000 concurrent SSL VPN or 5,000 concurrent UAC users.

The MAG6610 Pulse Gateway provides scalable SSL VPN and/or UAC capability for large enterprises through service modules which can be mixed and matched in its two available service module slots. The MAG6610 requires at least one service module to be ordered and installed (MAG-SM160 or MAG-SM360 for SSL VPN or UAC functionality). The MAG6610 gateway includes chassis management single sign-on (SSO) functionality, which allows a network administrator to configure and manage all service modules from one central console. The MAG6610 gateway supports up to 20,000 concurrent SSL VPN users or up to 30,000 concurrent UAC users in a 1 U high form factor.

The MAG6611 Pulse Gateway provides SSL VPN and/or UAC capability that meets the most demanding access needs of larger enterprises. With the MAG6611's support for up to four service modules, the enterprise has flexibility to mix and match the gateway configuration to suit its access requirements. The MAG6611 requires at least one service module to be ordered and installed (MAG-SM160 or MAG-SM360 for SSL VPN or UAC functionality). The MAG6611 gateway, through the Chassis Management Module option, offers chassis management SSO functionality which allows the network administrator to configure and manage all application service modules from one central console. The MAG6611 gateway supports up to 40,000 concurrent SSL VPN users or up to 60,000 concurrent UAC users in a 2 U high form factor.

Service Modules for MAG6610 and MAG6611

The MAG-SM160 and MAG-SM360 service modules support up to 1,000 or 10,000 concurrent SSL VPN users, or up to 5,000 or 15,000 concurrent UAC users, respectively. The service module hard disk drive for MAG-SM360 is available as a field-replaceable unit.

The MAG-SM360-PROFILER service module supports Endpoint Profiler, a new license option for the MAG Series that interoperates with the Pulse Access Control Service (UAC). Endpoint Profiler discovers, locates and monitors unmanaged endpoints such as printers and VoIP phones, while Pulse Secure's UAC provides network access control for these devices, as well as PCs, laptops, smart devices, tablets and similar devices. Each Endpoint Profiler service module can support up to 15,000 unmanaged endpoints. More information on Endpoint Profiler is available in the Optional Licenses section of this document.

MAG-CM060 is the chassis manager module that is only orderable with at least one service module (MAG-SM160, MAGSM360, MAG-SM161, or MAG-SM361). The chassis manager module uses a dedicated reserved slot in the service module. Up to two MAG-CM060 chassis management modules can be installed in two service modules, but only one can be active.

	MAG2600	MAG4610	MAG6610	MAG6611
Fixed/modular design	Fixed	Fixed	Modular; up to two service modules	Modular; up to four service modules
Functionality supported	SSL VPN or UAC; both modes cannot be used at the same time	SSL VPN or UAC; both modes cannot be used at the same time	SSL VPN or UAC mode per service module	SSL VPN or UAC mode per service module
Service modules	None	None	MAG-SM160 MAG-SM360 MAG-SM360-PROFILER	MAG-SM160 MAG-SM360 MAG-SM360-PROFILER
Maximum capacity	Supports up to 100 SSL VPN concurrent users or 250 UAC concurrent users	Supports up to 1,000 SSL VPN concurrent users or 5,000 UAC concurrent users	Supports up to 20,000 concurrent SSL VPN users or 30,000 concurrent UAC users with two MAGSM360 modules.	Supports up to 40,000 SSL VPN concurrent users or 60,000 concurrent UAC users with four MAGSM360 modules.
Management module	None	None	MAG-CM060 chassis management module	MAG-CM060 chassis management module
Form Factor	1U, 4.31 x 1.65 x 7.73 in.	1U, 8.63 x 1.75 x 21.5 in.	1 U, 17.31 x 1.75 x 27.25 in.	1U, 17.31 x 3.5 x 27.25 in.

Features and Benefits

The MAG Series Pulse Gateways, in conjunction with Pulse, provide a single enabling user interface and single gateway solution which lowers OpEx and CapEx costs significantly by reducing the number of management and software installations and updates required on end user devices. In large environments, the MAG Series gateways replace multiple hardware devices with a single converged device, further lowering the overall cost.

The high density, modular design of the MAG6610 and MAG6611 allows service modules to be mixed and matched to suit changing enterprise requirements in a flexible form factor. The highly scalable MAG Series supports as few as 100 concurrent SSL VPN users, up to a large deployment of 40,000 concurrent SSL VPN users, or 250 concurrent UAC users, up to a large deployment of 60,000 concurrent UAC users. The simplified, integrated, multiservice Pulse works in concert with the MAG Series Pulse Gateways to enable optimized anytime, anywhere access to corporate networks and data from mobile and nonmobile devices alike.

Cross-platform SSL VPN capabilities allow users to access corporate resources from any type of device (i.e., desktop PCs, laptops, smartphones, tablets, other mobile devices) using nearly any type of operating system (Microsoft Windows, Apple Mac OS, Linux, Apple iOS, Google Android, Microsoft Windows Mobile, etc.). Existing backend data stores and directories such as Microsoft Active Directory or Lightweight Directory Access Protocol (LDAP) in customer networks can be leveraged for authentication and authorization, simplifying network administration and maintenance.

Pulse Services for the MAG Series

Pulse Secure Access Service

Enterprises and service providers have the difficult challenge of providing device-independent, secure, mobile and remote network connectivity with the capability of controlling differentiated application and resource access for authorized users. Security breaches and threats continue to spiral out of control, and employees are seeking to use—or are even encouraged by their employers to use—their personal smartphones, tablets, and other mobile and computing devices to access the enterprise network, cloud, applications, and data, making this challenge even more difficult. Pulse Secure's Pulse Secure Access Service is a simple, intuitive service that provides secure, authenticated network and application access for remote and mobile users via SSL VPN from virtually any webenabled device.

Pulse Secure Access Service uses SSL, the security protocol supported by 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. Pulse Secure Access Service includes Pulse, a dynamic, integrated, multiservice network enabling user interface for mobile and nonmobile devices. Pulse enables optimized anytime, anywhere access to corporate networks, clouds, and data. It enables secure SSL VPN access from a wide range of mobile and nonmobile devices such as smartphones, tablets, laptops, desktop PCs, Wi-Fi, or 3G/4G/Long Term Evolution (LTE)-enabled devices. Pulse Secure Access Service also enhances users' remote access experience and productivity through seamless and transparent single sign-on (SSO) to thirdparty Web applications, including cloud-based Software-as-a- Service (SaaS) applications, while enforcing uniform device and user compliance before granting access. And, with the Pulse Collaboration feature license, users are able to participate in meetings and collaborate anytime, anywhere.

For more details on Pulse, please visit **https://www.pulsesecure.net/products/**. For further details about the features and license options of Pulse Secure Access Service, please view the Pulse Secure Access Service datasheet on the MAG Series webpage.

Pulse Access Control Service

Pulse Access Control Service enables NAC for any connected device, regardless if it is remote or local. It delivers Pulse Secure Unified Access Control services across the extended enterprise, providing a standards-based, comprehensive, network and application access control solution. The Pulse Access Control Service delivers identity-based, location- and device-aware, granular access control with robust endpoint security and integrity checks. When deployed with MAG Series gateways, Pulse, Pulse Access Control Service and Pulse Secure Access Service combine to deliver fast, secure network and application access, with the ability to automatically migrate from one access type (such as secure remote access) to another (local network and application access control) based on the user location, and through SSO. In addition, highly granular endpoint device assessment capabilities allow administrators to grant full or differentiated network and application access—or even deny access—based on a device's security state and status, i.e., if Google Android and Apple iOS mobile devices are jail-broken or rooted, compromised, infected, or running an unsecure OS version, or if Microsoft Windows and Apple Mac OS devices are running outdated antivirus, antimalware, endpoint firewall or patches, or custom checks.

Pulse and the Pulse Access Control Service combine to deliver identity-aware networking, complete with security and access control policies that follow users around the globe—regardless of how, from where, or from what device (smartphones, tablets, or similar mobile devices) they are attempting network and application access. All user session data is shared in MAG Series gateways and service modules via the Trusted Network

Connect (TNC) Interface for Metadata Access Point (IF-MAP) standard, enabling a seamless authentication and session data flow. For further details about the features and license options of Pulse Access Control Service, please view the Pulse Access Control Service datasheet on the MAG Series webpage.

Licensing

User License (Common Access License)

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

For administrative ease of use when it comes to license counts, each license enables as many users as specified, and the licenses 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 allow support for up to 200 concurrent users. See the Architecture and Key Components section of this datasheet for the maximum number of common access licenses for SSL VPN and UAC supported per MAG Series gateway and service module.

High Availability Clustering Capability (No Additional License Required)

With the MAG Series, 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 licenses ("-ADD") 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 1,000-user cluster is accomplished by bringing together two MAG Series gateways with 500 user licenses on each of the units.

Clustering features 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 or enterprise productivity, no need for users to log in again, and no downtime.

Here are the clustering options for the MAG Series gateways:

1. MAG2600 gateways can be clustered in a pair.
2. MAG4610 gateways can be clustered in a pair.
3. For MAG6610 gateways, you may cluster two service modules in a pair (assuming any two MAG-SM160 or MAG-SM360 service modules are installed in the chassis).
4. For MAG6611 gateways, you may cluster two service modules in a pair, either using the MAG-SM160 or MAG-SM360. To cluster three or four service modules will require all MAGSM360 service modules in the chassis.

Please note that WAN clustering is not supported on the MAG Series. Multisite clustering is supported, however, provided the sites are on a campus network with LAN-like connectivity.

Enterprise Licensing

Enterprise licensing allows any organization with one or more MAG Series gateways to easily lease user licenses from one gateway to another, as required, to adapt to changing organizational needs. The centralized licenses can be either perpetual or subscription licenses. Perpetual licenses feature a one-time charge; however, maintenance is an additional cost and an additional license is required to allow each MAG Series gateway to participate in leasing. Please note that perpetual licenses also cannot be leased to a Pulse Secure SA Series SSL VPN Virtual Appliance or to a JunosV Policy Secure virtual UAC appliance.

Subscription licenses offer a more flexible and overall valuable option with one, two, or three-year terms. Subscription licenses can be leased to SA Series SSL VPN Virtual Appliances or JunosV Policy Secure virtual UAC appliance, and maintenance is included. Subscription licensing requires a licensing server, either dedicated or partially dedicated. (Please note that the licensing server does require a hardware maintenance contract.)

Optional Licenses

In addition to the Common Access licenses, the MAG Series Pulse Gateways also offer a number of optional licenses that can provide additional services and capabilities.

IT organizations are challenged to discover, locate and monitor unmanaged endpoints such as printers, VoIP phones and WLAN access points in order to successfully deploy network-based authentication and network access control. Once located, these devices must be provisioned with the appropriate level of network access and monitored to ensure they behave in an acceptable manner given their known identity. Endpoint Profiler, an OEM of Great Bay Software's Beacon discovers, locations and provisions these nonauthenticating endpoints. Endpoint Profiler works in conjunction with Pulse Access Control Service running on MAG Series Gateways to provide a comprehensive network access control and profiling solution for the enterprise.

The Pulse Secure ICE (In Case of Emergency) license option—in conjunction with the Pulse Secure Access Service—provides organizations with a quick resolution when the unexpected happens, delivering the ability to handle extreme peak demands and enabling a company to continue business operations when disaster strikes. Maintaining productivity, sustaining partnerships, and delivering continued services to customers, ICE enables government and other entities to meet business and compliance objectives for continuity of operations (COOP) in the event of a disaster or pandemic event. Two options are available: a full ICE option that allows use of the maximum capacity of the MAG Series hardware for a temporary period, or a 25 percent burst option, which allows bursting of up to 25 percent of the installed license count on a MAG Series gateway. More information on the ICE license option can be found on the MAG Series webpage

The Premier Java RDP (Remote Desktop Protocol) Applet option provides organizations with a platform-independent, Java-based solution for accessing Microsoft Windows Terminal Servers. It makes business critical data in Windows-based applications available to all remote users, regardless of the type of hardware or operating systems they are using. With the Premier Java RDP Applet option, central installation and administration are available through Java technology. When used in combination with the Premier Java RDP Applet, the Java Windows Terminal provides one of the most convenient terminal server access experiences. For additional information, please see the Premier Java RDP Applet Option License datasheet on the MAG Series webpage. The Enterprise Guest Access license, available for a wide range of MAG Series gateways allows organizations to secure their critical network resources from guests, partners, and others while providing them with secure clientless access to the Internet and limited network resource access, and performing full endpoint integrity and posture assessments and policy enforcement. The simple interface allows IT administrators to quickly provision guest users, or delegate the task to administrative or support staff. Enterprise Guest Access also allows organizations to effectively respond to regulatory or industry-mandated

compliance audits, and comply with regulatory and industry policies. The Enterprise Guest Access license supports up to 200 guest users.

The UAC-SRX license enables application-aware firewall policies between the Pulse Access Control Service and the Juniper Networks SRX Series Services Gateways. Fully capable without the use of Common Access licenses, this feature provides a cost-effective solution to secure specific applications within the network—typically the data center—by enabling the Pulse Access Control Service to allow its identity-based list of user roles to be accessed by the SRX Series gateway. The end user benefits from a seamless experience, unaware that the Pulse Access Control Service service exists, thanks to the integrated Windows domain SSO functionality via Active Directory.

Pulse Secure is a strong supporter of open standards, including those of the Trusted Computing Group's TNC Work Group, which ensure interoperability with a host of network and security offerings. Through its support of the TNC standard Statement of Health (SOH) protocol, the Pulse Access Control Service interoperates with the Microsoft Windows SOH and embedded Microsoft Network Access Protection (NAP) Agents, enabling you to use your existing Microsoft Windows 7, Windows Vista, and/or Windows XP SP3 clients with MAG Series gateways. A separate SOH/NAP integration license is required. MAG Series gateways also support the TNC's open standard Interface for Metadata Access Point (IF-MAP), enabling integration with third-party network and security devices— including nearly any device that supports the IF-MAP standard and which collects information about the happenings on or status of your network. MAG Series gateways can leverage this data when formulating access control decisions (in conjunction with the Pulse Access Control Service), taking any necessary and appropriate actions. Pulse Access Control Service and Pulse Secure Access Service share session data via IF-MAP, enabling a location-aware experience for users with limited interaction required. An IF-MAP server license is required for this functionality.

The MAG Series Pulse Gateways may also be licensed as standalone RADIUS servers, and a separate license allows standalone Pulse Secure Odyssey Access Client customers to use OAC as the client/supplicant to Pulse Access Control Service running on MAG Series gateways. The Automatic Patch Remediation license combines the MAG Series secure access solutions—Pulse Secure Access Service or Pulse Access Control Service—with VMware's (formerly Shavlik) industry-leading asset discovery and broad update capabilities to provide an additional layer of security and control over unmanaged endpoints. The automatic patch management license enables MAG Series gateways to automatically scan Windows-based PCs and laptops for security threats, and perform remediation before granting users and their devices full access to the corporate network. It does not require Microsoft's System Management Server (SMS) or System Center Configuration Manager (SCCM) for remediation, and it addresses the latest operating system and software patches from Microsoft, as well as other vendors such as Adobe Systems, Mozilla Firefox, Apache, RealPlayer, and others. More information is available in the Automatic Patch Remediation License datasheet on the MAG Series webpage.

Specifications

	MAG2600	MAG4610	MAG6610	MAG6611
Dimensions and Power				
Dimensions (W x H x D)	4.31 x 1.65 x 7.73 in (10.95 x 4.2 x 19.64 cm)	8.63 x 1.75 x 21.50 in (21.92 x 4.45 x 54.61 cm)	17.31 x 1.75 x 27.25 in (43.97 x 4.45 x 69.22 cm)	17.31 x 3.5 x 27.25 in (43.97 x 8.89 x 69.22 cm)
Weight	1.98 lb (900 g)	11.5 lb (5.2 kg)	21 lb (9.5 kg)	31 lb (14.1 kg)
Rack mountable	Yes, with optional tray	Yes	Yes	Yes
A/C power supply	100-240 VAC, 1A 50-60 Hz, 30 W maximum	100-240 VAC, 1A 50-60 Hz, 70 W maximum	MAG-PS661 power supply: 100-240 VAC, 8A 50-60 Hz, 560 W maximum Optional DC power supply	MAG-PS662 power supply: 100-240 VAC, 10A 50-60 Hz, 750 W maximum Optional DC power supply
System battery	CR2032 3 V lithium coin cell	CR2032 3 V lithium coin cell	CR2032 3 V lithium coin cell	CR2032 3 V lithium coin cell
Efficiency	80% or greater at full load	80% or greater at full load	80% or greater at full load	80% or greater at full load
Material	Aluminum	Steel	Steel	Steel
Mean time between failure (MTBF)	212 khrs	142 khrs	707 khrs	428 khrs
LEDs	Power, HDD activity, hardware alert	Power, HDD activity, hardware alert	On MAG Service Module: Power, HDD activity, hardware alert	On MAG Service Module: Power, HDD activity, hardware alert
Interfaces	• RJ45 serial (console port) • Two RJ45 Ethernet 10/100/1000 (traffic) • USB	• RJ45 serial (console port) • Three RJ45 Ethernet 10/100/1000 (traffic) • USB	On MAG Series Service Module: • RJ45 serial (console port) • Three RJ45 Ethernet 10/100/1000 (traffic) • USB	On MAG Series Service Module: • RJ45 serial (console port) • Three RJ45 Ethernet 10/100/1000 (traffic) • USB

Environment

Operating temperature

- 41° through 104° F (5° through 40° C)

Storage temperature

- -40° through 158° F (-40° through 70° C)

Relative humidity (operating)

- 8% - 90% (non condensing)

Relative humidity (storage)

- 5% - 95% (non condensing)

Altitude (operating)

- 10,000 ft maximum

Altitude (storage)

- 40,000 ft maximum

Certifications

Safety certifications

- EN 60950-1; CAN/CSA-C22.2 No. 60950-1; UL 60950-1; IEC 60950-1 Emissions certifications
- EN 55022 (CISPR 22); Australian Communications and Media Authority (ACMA) AS/NZS CISPR 22; VCCI V-3/2011.04 and V-4/2011.04, R-3064, G-254, C-3969, and T-1049; ETSI EN 300 386 V1.5.1; EN 55024; FCC Part 15, Class A, Industry Canada ICES-003 Issue 4 (MAG2600 only: FCC Part 15, Class B, Industry Canada ICES-003 Issue 4)

Warranty

- 90 days (Can be extended with support contract)

Pulse Secure Services and Support

Pulse Secure is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Pulse Secure ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit **https://www.pulsesecure.net/products/.**

Ordering Information

Model Number	Description
MAG Base Systems	
MAG2600 Base System	MAG2600 Pulse Gateway for SSL VPN, NAC, or guest access

Model Number	Description
MAG4610 Base System	MAG4610 fixed configuration Pulse Gateway for SSL VPN users or NAC
MAG6610 Base System	MAG6610 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 Base System	MAG6611 chassis 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 Base Systems	
MAG-SM160	Service module for MAG6610 or MAG6611 that supports 1,000 SSL VPN or 5,000 NAC users
MAG-SM360	Service module for MAG6610 or MAG6611 that supports 10,000 SSL VPN or 15,000 NAC users
MAG-SM360- PROFILER	MAG SM-360 HW Blade for Endpoint Profiler
MAG-CM060	Management module for MAG6610 or MAG6611; only orderable with at least one service module. A maximum of one management module can be ordered per chassis
MAG Series Accessories	
MAG-PS260	Spare/replacement external “brick” power supply for MAG2600
MAG-PS661	Spare 560 W AC power supply module for MAG6610
MAG-PS664	Spare 560 W DC power supply module for MAG6610
MAG-PS662	Spare/additional 750 W AC power supply module for MAG6611
MAG-PS663	Spare 750 W DC power supply module for MAG6611
MAG-HD060	Field-replaceable spare HDD for MAG-SM360 service module
MAG-HD361	Field-replaceable spare HDD for MAG-SM361 service module
MAG-FT060	Spare fan tray for MAG6610 or MAG6611
MAG-RK1U4	Rack kit to place four MAG2600 gateways side-by-side in a rack
MAG-RK1U2	Rack kit to mount two MAG46XX units side-by-side in a rack or when included rack kit is lost or damaged
MAG-RK1U	Replacement rack kit for MAG6610
MAG-RK2U	Replacement rack kit for MAG6611

Model Number	Description
User Licenses (Common Access Licenses)*	
ACCESSX600- ADD-xU	Add x simultaneous users to MAGX600 Pulse Gateway Appliances (x options: 10, 25, 50, 100, 250, 500, 1000, 2000, 2500, 5000, 7500, 10K, or 15K concurrent users)
High Scale Licenses**	
ACCESSX600- ADD-xU	Add x simultaneous users to Pulse Gateway X600 Series Appliances (x options: 20K or 25K simultaneous users)
Endpoint Profiler	
ACCESSX600-PF-SC-xD	Endpoint Profiler - Server and Collector functionality for x devices (x options: 1,000, 2,500, 5,000 or 10K devices)
ACCESSX600-PF-CO-xD	Endpoint Profiler - Collector (only) functionality for x devices (x options: 1,000, 2,500, 5,000 or 10K devices)
ACCESSX600-PF-SO-15KD	Endpoint Profiler - Server (only) functionality for 15,000 devices
SRX Series Role-Based Firewall Licenses	
MAGX600-UAC-SRX-xU	Role-based firewall licenses for 25 users (basic features) (x options: 25, 250, 5K or 15K users)
Server and Miscellaneous Licenses	
MAGX600-IFMAP	License for IF-MAP server on standalone UAC (hardware purchased separately)
MAGX600- RADIUS-SERVER	Add RADIUS Server Feature to the MAG X600
MAGX600-SOH	Adds Microsoft SOH/NAP Agent integration capabilities to the Pulse Gateway X600
MAGX600-OAC-ADD-UAC	Allows EE edition OAC clients to be converted to the UE edition OAC clients and used with Pulse Gateway X600
Leased Licensing Licenses	
ACCESS-LICENSE-SVR	Enables enterprise access appliance as a license server
MAG2600- LICENSE-MBR	Allows Pulse Gateway 2600 appliance to participate in leased licensing
MAG4610- LICENSE-MBR	Allows Pulse Gateway 4610 appliance-blade to participate in leased licensing

Model Number	Description
SM160-LICENSE-MBR	Allows Pulse Gateway SM160 appliance-blade to participate in leased licensing
SM360-LICENSE-MBR	Allows Pulse Gateway SM360 SA/ IC appliance-blade to participate in leased licensing
ICE (In Case of Emergency) License Options	
MAGX600-ICE	In Case of Emergency (ICE) license for MAG Series Pulse Gateways
ACCESS-ICE-25PC	ICE 25%: Burst to 25% of installed license count on MAG Series Pulse Gateway or SA Series SSL VPN Appliance
Java RDP (Remote Desktop Protocol) Applet License Options	
ACCESS-RDP-xU-zYR	Java RDP Applet z-Year subscription for x simultaneous users (x options: 50, 100, 250, 500, 1000, 2000, 2500, 5000, 7500, or 10K simultaneous users. RDP user license count cannot exceed the number of user licenses/common access licenses) (z options: 1, 2, or 3 year subscription)
Enterprise Guest Access License Options	
MAGX600-GUEST-ACCESS	Enterprise Guest Access License
Automatic Patch Remediation License Options	
ACCESS-PRM-xU-zYR	Patch Remediation Management (PRM), z-year subscription for x simultaneous users (x options: 50, 100, 250, 500, 1000, 2000, 2500, 5000, 7500, 10K, 20K or 25K simultaneous users. PRM user license count cannot exceed the number of user licenses/ common access licenses) (z options: 1, 2 or 3 year subscription)

*Total number of licenses cannot exceed the maximum supported per MAG Series gateway. See the Architecture and Key Components section of this document for the maximum number of licenses supported per system model.

**High Scale licenses allow stackable MAG Series licenses beyond the license capacity of single MAG Series gateways.

About Pulse Secure

Pulse Secure is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Pulse Secure 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.pulsesecure.net.**

Pulse Secure, LLC
2700 Zanker Road, Suite 200
San Jose, CA 95134