Pulse Connect Secure

Product Overview

With the digital world, the secure access world has become complex, with the greatest impact from the consumerization of IT. BYOD and cloud has increased the need for anywhere access from devices, both personal productivity (laptop, smartphones, smartpads) or IP-enabled (printers, cameras, phones), to data or applications that reside in the traditional datacenter or cloud. Pulse Connect Secure is the key component to Pulse's Secure Access solution. Pulse Connect Secure provides a seamless, cost-effective, SSL VPN solution 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 controlling resource access for authorized users. Breaches and threats continue to spiral out of control, and increasing numbers of employees and users want to use their own personal productivity solutions from devices to cloud based applications. Making this challenge even more difficult. Pulse Secure Connect Secure provides secure, authenticated access for remote and mobile users from any web-enabled device to corporate resources—anytime, anywhere. Pulse Connect Secure is the most widely deployed SSL VPN for organizations of any size, across every major industry.

Pulse Connect Secure includes Pulse Secure Clients and the AppConnect SDK. Pulse Clients are dynamic, multiservice network client for mobile and personal computing devices. Pulse Clients are simply deployed, enabling users to quickly "click and connect" from any device, anywhere. Pulse Secure AppConnect SDK delivers per application SSL VPN connectivity for iOS and Android clients, enabling IT to create an even more transparent and secure mobile app experience for their users.

Architecture and Key Components

Pulse Connect Secure is available on a hardware-based (Pulse PSA or MAG Series) or as a virtual appliance as noted below.

- **PSA300 Pulse Secure Appliance:** Fixed configuration, compact appliance ideal for small and mid-size businesses, supporting up to 200 SSL VPN concurrent users. PSA300 is ideal for desktop deployments.
- **PSA3000 Pulse Secure Appliance:** Fixed configuration, rack-mount appliance ideal for small and mid-size businesses, supporting up to 200 SSL VPN concurrent users.
- **PSA5000 Pulse Secure Appliance:** Fixed configuration appliance ideal for scalable mid-size businesses, supporting up to 2,500 SSL VPN concurrent users.
- **PSA7000 Pulse Secure Appliance:** Fixed configuration appliance ideal for meeting the highest scalability needs of large businesses, supporting up to 25,000 SSL VPN concurrent users.
- **MAG2600 Pulse Secure Appliance:** Fixed configuration, compact appliance ideal for small and mid-size businesses, supporting up to 100 SSL VPN concurrent users.
- **MAG4610 Pulse Secure Appliance:** Fixed configuration appliance ideal for mid-size and large businesses, supporting up to 1,000 SSL VPN concurrent users.

- **MAG6610 Pulse Secure Appliance:** Chassis-based appliance ideal for scalable large businesses, supporting up to 20,000 SSL VPN concurrent users; it requires at least one service module (maximum of two) to be ordered and installed (MAG-SM160 or MAG-SM360).
- **MAG6611 Pulse Secure Appliance:** Chassis-based appliance ideal for meeting the highest scalability needs of large businesses, supporting up to 40,000 SSL VPN concurrent users; it requires at least one service module (maximum of four) to be ordered and installed (MAG-SM160 or MAG-SM360).
- **Virtual Appliance:** VMware, KVM, and Hyper-V virtual appliances for scalable elastic deployment of SSL VPN services.

For more details on PSA and MAG Series Appliance, including the specifications and ordering information of each model, please refer to the Pulse PSA or MAG Series Appliance datasheets.

Pulse Secure Clients

Pulse Clients securely connect users to networks, both datacenter and cloud. Wrapped in an extremely user-friendly package, Pulse Client dynamically enables the appropriate network and security services on users' endpoints. Users are not distracted from their work activities to figure out what network they are on or what service to enable. With Pulse Secure, the connection just works, helping to deliver the productivity promised by mobile devices. Pulse Client delivers dynamic access control, seamlessly switching between remote (SSL VPN) and local (NAC) access control services on Microsoft Windows devices. Pulse Client also enables comprehensive endpoint assessment for mobile and desktop computing devices, and quarantine and remediation, if necessary.

The digital world continues to create workforce productivity beyond BYOD. More enterprises are combining apps and data that were traditionally delivered privately on premises with a variety of 3rd party, cloud hosted service offerings, whether it be cloud based storage, SaaS applications or IaaS platforms. This evolution of combining and managing private and public IT architectural worlds is Hybrid IT. Learn how to embrace Hybrid IT with Pulse Cloud Secure and have the capabilities to blend cloud and datacenter access into a seamless user experience for your next generation workforce. Additional details about Pulse Cloud Secure is available: https://www.pulsesecure.net/connect-secure/overview/

Features and Benefits

Table 1: Key Features of Pulse Connect Secure

Feature	Feature Description
Layer 3 SSL VPN	· Dual-transport (SSL + Encapsulating Security Payload) full Layer 3 VPN connectivity with granular access control. · 'Always ON VPN' & 'VPN Only Access' modes for Compliance.
Application VPN	· Client/server proxy application that tunnels traffic from specific applications to specific destinations (available for Windows devices only). · 'On Demand VPN' and 'Per App VPN', for Seamless & Secure end user experience.
Layer 7 Web single sign-on (SSO) via SAML	· Allows end users to authenticate to the network through a Layer 3 tunnel, while simultaneously enjoying SSO to Web applications accessed through their browser via SAML SSO support.
Optimized end-user experience	· Smooth roaming from remote access to local LAN access (Pulse Policy Secure). · SSO, via cloud secure feature, remote and onsite (via integration wit Policy Secure and available in Enterprise Edition of Secure Access Suites.
Endpoint integrity and assessment	· Assess and remediate end user devices prior to authentication with easy policy definition. Available on Windows, Mac OS X, Apple iOS, Android, and Windows Mobile 6.5 (capabilities vary by platform). Available pre-installed with Microsoft Windows 8.1 and RT.
Split tunneling options	· Full range of split tunneling options are configurable, including support for configuration at IP level, as well as FQDN level. · Includes enable and disable functionality with overriding route capability and route monitoring. · Pulse AppConnect enables IT to integrate per-application SSL VPN connectivity for maximum data security and user transparency.
Flexible launch options (standalone client, browser-based launch)	· Users can easily launch SSL VPN via their Web browser, or directly from their desktop. · Auto Connect-allows devices to automatically connect to VPN, either at the time when the machine starts or user logs on. · VPN on demand-leverages OS capabilities for auto triggering VPN, seamlessly in the background, when an approved application needs corporate access.
Supports Pulse Cloud Secure Solution	· Blend cloud and datacenter access into a seamless user experience for next generation workers. · Ability to add compliance rules for hybrid DC access.
Preconfiguration options (Windows and Mac only)	· Administrators can preconfigure a Pulse Secure deployment with a list of gateways for end users to choose from.
Authentication options	· Administrators can deploy Pulse Secure for remote user authentication using a wide array of authentication mechanisms, including hardware token, smart card, soft token, Google Authenticator, one-time passwords and certificate authentication. · SAML authentication, for delegating user authentication to an Identity Provider.

Feature	Feature Description
RDP/Telnet/SSH sessions using HTML5	· 100% clientless access using HTML5 browsers.
VMware Horizon and Citrix XenApp/ XenDesktop	· Supports VMware Horizon View 6.0.1, 6.1 & 6.2; 7.0 for VMware Horizon View, Citrix Xen 7.6, StoreFront 2.6 & 3.0.
Granular SSL Cipher Configuration	· Enables the administrator to select specific ciphers over those pre-configured for highly secure compliance.

End-to-End Layered Security

Pulse Connect Secure 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
Host Checker	· Endpoint devices can be checked prior to and during a remote access session to verify an acceptable device security posture requiring installed/running endpoint security applications (antivirus, personal firewall, etc.), as well as check for IT-required Operating System versions, patch level, browser type, and many other requirements. · Custom-built checks for specialized customer requirements are also supported. · Noncompliant endpoints can be quarantined, denied access, or granted access, depending on administrator defined policies. · Whenever possible, Host Checker automatically remediates noncompliant endpoints by updating software applications that do not comply to corporate security policies.	· Ensures that endpoint devices meet corporate security policy requirements before being granted network access. · Remediates devices and quarantines users, when necessary. · Can ensure that no potentially sensitive data is left behind on the endpoint device.
Trusted Network Connect (TNC) support in 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.
Always-On VPN	· Ensure all traffic from endpoints is sent over the tunnel which is set up automatically when an Internet connected is detected.	· Enables organizations to enforce security, compliance and visibility on all traffic from endpoints even when they are not on-prem.

Ease of Administration

In addition to enterprise-class security benefits, Pulse Connect Secure 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
Mobile Device Management (MDM) integration (available with Pulse Workspace, Microsoft Intune, AirWatch, MobileIron)	· Enables consolidated reporting and dashboards for simplified management. · Leverages MDM attributes for more intelligent and centralized policy creation. · Facilitates transparent "no touch" MDM-based deployment of Pulse Clients to iOS and Android devices.	· Extend MDM investments to gain comprehensive endpoint visibility and support additional mobile use cases.
Secure Browser	· A mobile browser for securely accessing corporate web applications, without the need of installing / managing / launching a VPN client.	· IT does not have to worry about deploying and managing VPN on mobile devices. End user does not have to worry about launching VPN. Seamless end user experience where a user launches browser and accesses his resources, as he would normally expect to.
Secure Access for SAP Applications	· Embeds Pulse Secure Per-App VPN SDK into SAP's Fiori mobile applications.	· Provides transparent, secure data center connectivity for SAP services through the existing Pulse Secure VPN appliance. Additional details are available: https://www.pulsesecure.net/solutions/sap/
Integration with strong authentication and identity and access management (IAM) platforms	· Ability to support SecurID, Security Assertion Markup Language (SAML) including standards-based SAML v2.0 support, and public key infrastructure (PKI)/digital certificates.	· Leverages existing corporate authentication methods to simplify administration.
Bridge Certification Authority (BCA) support	· Supports federated 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 customers to configure policy extensions in the admin UI, to be enforced during certificate validation.	· Enables customers who use advanced PKI deployments to deploy the Pulse Secure Appliances to perform strict standards-compliant certificate validation—before allowing data and applications to be shared between organizations and users.
Multiple hostname support	· Ability to host different virtual extranet websites from a single appliance.	· Saves the cost of incremental servers. · Eases management overhead. · Provides a transparent user experience with differentiated entry URLs.
Intuitive Dashboard Design	· View and control enterprise access to the data center and cloud from one console. (Reference Diagram 1)	· Quick access to dynamic information and reports. · Customizable layouts via drag and drop functionality.
Customizable user interface	· Creation of completely customized sign-on pages.	· Provides an individualized look for specified roles, streamlining the user experience.
Pulse One Compatible	· With Pulse One, configuring, updating, and monitoring PSA or MAG Series Appliances under a centralized management console with the capabilities of a single device/cluster or across a global cluster deployment.	· Enables companies to conveniently manage, configure, and maintain PSA or MAG Series Appliances along with Pulse Workspace from one central location.
Pulse Application Launcher (PAL)	· Enhanced support for non-JAVA based browsers.	· Support for latest generation browsers (Apple, Microsoft, Google, Firefox, etc) that do not support Java and Active X.

Diagram 1 - Dynamic UI for Pulse Connect Secure, Version 8.2

Rich Access Privilege Management Capabilities

Pulse Connect Secure provides dynamic access management capabilities. When users log into Pulse Connect Secure, 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. Users have access only to those resources that are deemed necessary for that session, according to administrator-defined policies.

Table 4: Access Privilege Management Features and Benefits

Feature	Feature Description	Benefits
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.
SSL VPN federation with NAC (Pulse Policy Secure)	• Seamlessly provision SSL VPN user sessions into NAC sessions upon login. • Since session data is shared between the Pulse Secure Appliances for SSL VPN and NAC, 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.
Support for RSA Authentication Manager	• RSA Authentications Manager 8.1 enables Risk Based Authentication.	• Offer another authentication layer option via email account.
Support for Google Authenticator	• Enables multi-factor authentication using smartphones	• Leverage ubiquitous smart phones to roll out a cost-effective and self-serve two-factor authentication mechanism, where one time passcodes are generated by a mobile app
Multiple sessions per user	• Allows remote users to launch multiple remote access sessions.	• Enables remote users to have multiple authenticated sessions open at the same time, such as when accessing VPN from a laptop and from a smartphone simultaneously.
User record synchronization	• Supports synchronization of user records such as user bookmarks across different Pulse Secure Appliances.	• Ensures a consistent experience for users who often travel from one region to another and therefore need to connect to different Pulse Secure Appliances running Pulse Connect Secure.
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 and webpages customized for their device types.

Flexible Single Sign-On (SSO) Capabilities

Pulse Connect Secure offers comprehensive single sign-on (SSO) 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 SSO Features and Benefits

Feature	Feature Description	Benefits
SAML single sign-on for cloud and Web applications access	· SAML 2.0-based SSO to a variety of Web applications, including many of today's most popular Software as a Service (SaaS) applications such as salesforce.com and Google Apps. · Includes SSO functionality, even when connecting via a Pulse Connect Secure Layer 3 VPN tunnel, which is unique in the industry. · Pulse Connect Secure supports deployments as both an SAML Identity Provider (IdP) and as a SAML Service Provider (SP).	· Single sign-on to a user's Web and cloud-based applications, simplifying the user's connectivity experience.
Kerberos Constrained Delegation	· Support for Kerberos Constrained Delegation protocol. · When a user logs into Pulse Connect Secure 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 Pulse Connect Secure throughout the session. · When the user accesses Kerberos-protected applications, the Appliance 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	· Pulse Connect Secure will automatically authenticate remote users via Kerberos or NTLMv2 using user credentials.	· Simplifies the user experience by eliminating users entering credentials multiple times to access different applications.
Password management integration	· Standards-based interface for extensive integration with password policies in directory stores (LDAP, AD, and others).	· Leverages existing servers to authenticate users. · Users can manage their passwords directly through the Pulse Connect Secure 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 reentering login credentials.	· Alleviates the need for 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

Pulse Connect Secure 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
Pulse Secure Client	• Single, integrated, remote access client that can also provide LAN access control, and dynamic VPN features to remote users.	• Pulse Client replaces the need to deploy and maintain multiple, separate clients for different functionalities such as VPN and LAN access control. • The end user simply "clicks and connects."
Clientless core Web access	• Secure access to many different types of web-based applications, including many of today's most common Web applications such as Outlook Web Access, SharePoint, and many others. • Remote Desktop Protocol (RDP) access in Pulse Connect Secure can be delivered over HTML5, via third-party RDP, through a WebSockets translator such as Ericom (www.ericom.com).	• Provides the most easily accessible form of application and resource access from a variety of end user devices with extremely granular security control options. • Completely clientless approach using only a web browser.
IPsec/IKEv2 support for mobile devices	• Allows remote users to connect from any mobile device that supports Internet Key Exchange (IKEv2) VPN connectivity. • Administrator can enable strict certificate or username/password authentication for access via IPsec/IKEv2.	• Full L3 VPN support for new devices that support IKEv2 but for which a Pulse Secure client is not yet available.
Virtual Desktop Infrastructure (VDI) support	• Allows interoperability with VMware View Manager to enable administrators to deploy virtual desktops with Pulse Connect Secure.	• Provides remote users seamless access to their virtual desktops hosted on VMware servers. • Provides dynamic delivery of the VMware View client, including dynamic client fallback options, to allow users to easily connect to their virtual desktops.
ActiveSync Proxy	• Provides secure access connectivity (strong encryption + certificate authentication) from mobile devices (such as iOS or Android devices) to the Exchange Server via proxy, 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.
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.

Product Options

Pulse Connect Secure currently includes several license options for enablement on the PSA or MAG Series Appliances.

User License (Connect Secure - 'CONSEC')

Pulse Connect Secure (CONSEC) licenses are per concurrent session licenses. (Please see the *Ordering Information* section below for licensing details.)

CONSEC licenses provide SSL VPN 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 managing license counts, each user license enables as many concurrent sessions as specified in the license and they are additive. For example, if a 100 user license was originally purchased and the concurrent user session 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 sessions.

Key features enabled by this license include:

- The combination of core clientless access, SAM, Pulse Client/Network Connect provides secure access to virtually any audience, from remote and 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 workstations from a remote location, and even changing their passwords when they are 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 each individual user community is the only ones using the system, complete with separate logon pages and customized views that uniquely reflect 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, and, cache cleaner, 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 policies, after which remnant data is scrubbed from the user's device 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 (CONSEC) licenses on each PSA or MAG Series Appliance.
2. When the PSA or MAG Series Appliances 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.

If either box fails, the remaining box inherits the full 1,000 user licenses.

Clustering supports stateful peering and failover across LAN connection, 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.

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

ICE (In Case of Emergency) 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 license 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 additional users on a PSA or MAG Series Appliance running Pulse Connect Secure for a limited time.

With ICE licenses, 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
- 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 Appliances, the ICE licenses are available in two forms: full ICE (which allows bursting to the full capacity of the MAG Series Appliances); and a 25% burst license (which allows bursting of up to 25% of the installed license count on any given MAG Series Appliances). 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. Likewise, for the Pulse PSA Series Appliances, only the full ICE licenses are available.

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 OS, 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.

PSA Series Ordering Information

Model Number	Description*
PSA Series Appliances	
PSA300	PSA300 Appliance for SSL VPN users or NAC users. Supports up to 200 SSL VPN or 500 NAC concurrent user sessions.
PSA3000	PSA3000 Appliance for SSL VPN users or NAC users. Supports up to 200 SSL VPN or 500 NAC concurrent user sessions.
PSA5000	PSA5000 Appliance for SSL VPN or NAC users Supports up to 2,500 SSL VPN or 10,000 NAC concurrent user sessions.
PSA7000	PSA7000 Appliance for SSL VPN or NAC users Supports up to 25,000 SSL VPN or 50,000 NAC concurrent user sessions.

PSA Series Accessories**

SKU	Description
PSA-SFP-10GE-SR-3M	4xSFP+ Transceiver modules + 4xCable (3m, SR,10G, up to 300m).
PSA-SFP-10GE-DAC-3M	4xDirect Attach SFP+ to SFP+ copper cable (3m).

PSA Series Licensing Options

Ordering Number	Description
Connect Secure Licenses* **	
CONSEC-xU(-zYR)	Add x simultaneous PCS users to Pulse PSA Appliance (x options: 10, 25, 50, 100, 250, 500, 1000, 2000, 2500, 5000, 7500, 10K, 15K, 20K, or 25K concurrent sessions) Subscription Licenses (z options: 1, 2, or 3 year).
CONSEC-ADD-yU	Add y simultaneous PCS users to Pulse PSA Appliance (y options: 10, 25, 50, 100, 250, 500, 1000, 2000, 2500, 5000, 7500, 10K, 15K, 20K, or 25K concurrent sessions) Perpetual for hardware platform where activated.
Leased Licensing Licenses	
ACCESS-LICENSE-SVR	Enables enterprise access appliance as a license server.
PSA-LICENSE-MBR	Allows PSA appliance to participate in leased licensing.
Secure Meeting License Options	
PSA-MTG-xU	Add x simultaneous Secure Meeting users to Pulse PSA Appliance (x options: 25, 50, 100, 250, 500).
ICE (In Case of Emergency) License Options	
PSA-ICE	In Case of Emergency (ICE) license for PSA Series 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, 1,000, 2,000, 2,500, 5000, 7500, or 10K simultaneous users. RDP user license count cannot exceed the number of user licenses) (z options: 1, 2, or 3 year subscription).

*With Pulse Connect Secure 8.2 & Pulse Policy Secure 5.3, all PSA hard disks are encrypted with AES128 using a random generated key, unique to each appliance.

**Note these accessories pertain to the Pulse PSA7000 Appliance.

***Total number of licenses cannot exceed the maximum supported per PSA Series Appliance.

MAG Series Ordering Information

Model Number	Description
MAG Series Appliances	
MAG2600	MAG2600 Appliance for SSL VPN users or NAC users. Supports up to 100 SSL VPN or 250 NAC concurrent user sessions.
MAG4610	MAG4610 fixed configuration appliance for SSL VPN users or NAC users. Supports up to 1,000 SSL VPN or 5,000 NAC concurrent user sessions.
MAG6610	MAG6610 Appliance 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 appliance 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).
Service Modules for MAG6610 or MAG6611	
MAG-SM160	MAG-SM160 service module for MAG6610 and MAG6611 appliances. Supports 1,000 SSL VPN or 5,000 NAC concurrent user sessions.
MAG-SM360	MAG-SM360 service module for MAG6610 and MAG6611 appliances. Supports 10,000 SSL VPN or 15,000 NAC concurrent user sessions.
MAG-CM060	MAG-CM060 management module for MAG6610 or MAG6611 Appliances. Only orderable with at least one service module, and a maximum of one management module can be ordered per chassis.

MAG Series Accessories

SKU	Description
MAG-RK1U	Replacement rack kit for MAG6610
MAG-RK2U	Replacement rack kit for MAG6611

MAG Series Licensing Options

Ordering Number	Description
ACCESSX600-ADD-yU	Add y simultaneous users to Pulse MAG Series Appliance, where y = 10 ,25, 50, 100, 250, 500, 1000, 2000, 2500, 5000, 7500, 10k, 15k, 20k, 25k. Perpetual for the hardware platform where activated.
ACCESSX600-yU-zYR	Add y simultaneous users to Pulse MAG Series Appliance, where y = 10 ,25, 50, 100, 250, 500, 1000, 2000, 2500, 5000, 7500, 10k, 15k, 20k, 25k; where subscription licenses are z = 1, 2, or 3 year licenses are available
CONSEC-yU	Add y simultaneous users to Pulse MAG Series Appliance, where y = 10, 25, 50, 100, 250, 500, 1000, 2000, 2500, 5000, 7500, 10k, 15k, 20k, or 25k. Perpetual for the hardware platform where activated.
CONSEC-ADD-yU(-zYR)	Add y simultaneous users to Pulse MAG Series Appliances, where y = 10, 25, 50, 100, 250, 500, 1000, 2000, 2500, 5000, 7500, 10k, 15k, 20k, or 25k; where subscription licenses are z = 1, 2, or 3 year licenses are available
Leased Licensing Licenses	
ACCESS-LICENSE-SVR	Enables enterprise access appliance as a license server
MAG-LICENSE-MBR	Allows Pulse MAG Series Appliances to participate in leased licensing
Secure Meeting License Options	
MAG-MTG-xU	Add x simultaneous Secure Meeting users to Pulse MAG Series Appliances (x options:25, 50, 100, 250, 500)
ICE Licenses	
ACCESS-ICE-25PC	In Case of Emergency (ICE) 25%: Burst to 25% of installed license count on Pulse MAG Series Appliances
MAGX600-ICE	In Case of Emergency (ICE) License for Pulse MAG Series Appliances
Premier RDP Applet Licenses	
ACCESS-RDP-yU-zYR	Java RDP Applet z-year subscription for y simultaneous users, where y= 50, 100, 250, 500, 1000, 2000, 2500, 5000, 7500, or 10k and z= 1, 2, or 3.

For additional details, please visit https://www.pulsesecure.net/support/eol/hardware/mag-series/

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.

About Pulse Secure, LLC

Pulse Secure, LLC is a leading provider of access and mobile security solutions to both enterprises and service providers. Enterprises from every vertical and of all sizes utilize the company's Pulse virtual private network (VPN), network access control and mobile security products to enable end user mobility securely and seamlessly in their organizations. Pulse Secure's mission is to enable open, integrated enterprise system solutions that empower business productivity through seamless mobility.

Corporate and Sales Headquarters
Pulse Secure LLC
2700 Zanker Rd. Suite 200
San Jose, CA 95134
www.pulsesecure.net

Pulse Connect Secure Datasheet 040317