"IN CASE OF EMERGENCY" (ICE) LICENSE OPTION

Enabling Business Continuity with Remote Access

Product Overview

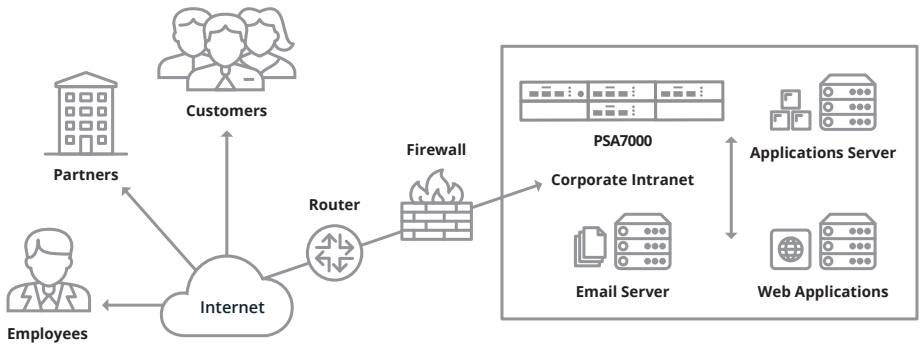
Pulse Secure ICE license option provides a quick resolution when the unexpected happens, delivering the ability to handle extreme peak demands and to support continued business operations. The ICE license option can be used in conjunction with the Pulse Secure PSA Series Appliance, MAG Series Appliances, or SA Series SSL VPN Appliances. ICE enables a company to maintain productivity, sustain partnerships and deliver continued services to customers, even when disaster strikes. ICE enables federal departments and agencies, state and local governments to meet compliance objectives for ensuring continuity of operations in the event of a disaster or pandemic event.

Product Description

SSL VPNs can help keep organizations and businesses functional by connecting people—even during the most unpredictable circumstances. When hurricanes, terrorist attacks, transportation strikes, pandemics, virus outbreaks or other potentially catastrophic events occur, they can result in the quarantine or isolation of entire regions or groups of people for an extended period of time. Effectively balancing risk and cost, Pulse Secure PSA Series Appliances, MAG Series Appliances, or SA Series SSL VPN Appliances with the ICE license option help ensure business continuity. Through the ICE license option, organizations can instantly address a dramatic peak in demand for remote access in cases of emergency by supporting additional users on a Pulse Secure PSA Series Appliances, MAG Series Appliances, or SA Series SSL VPN appliance.

The ICE license option is available in two forms:

1. Full ICE option (allows use of the maximum capacity of the underlying hardware for a temporary period) available on Pulse Secure PSA Series Appliances, MAG Series Appliances, or SA Series Appliance.
2. A 25% burst license option (allows bursting of up to 25% of the installed license count on a MAG Series Appliance or SA Series Appliance).



Unplanned events that could impact business continuity:
Hurricane, snowstorm, strike, virus outbreak, terrorist attack

Figure 1: Business continuity with ICE

With the full ICE option, for example, a customer with a Pulse Secure PSA5000 licensed for 100 concurrent users can add the PSA ICE license. When applied and enabled, ICE license will allow the customer to support up to 2,500 concurrent users on that device for up to 8 weeks. 2,500 users is the maximum user count supported on the PSA5000 .

With the 25% burst license option, if the customer has a MAG-SM360 service module (regardless of whether it is installed in a Pulse Secure MAG6610 Appliances or MAG6611 Appliances) with a 1,000 user license, the 25% burst license option will provide support for an additional 250 users during an unplanned event.

When ICE is applied but not enabled, the features cannot be used on that device unless the corresponding permanent feature license has been enabled on that device.

ICE can be employed for a limited time to:

- Maintain productivity by rapidly 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 securing and protecting resources
- Meet federal and government mandates for contingencies and continuity of operations (COOP) compliance

Architecture and Key Components

As shown in Figure 1, the ICE license option enables companies to instantly accommodate spikes in remote access demand for various audiences during unplanned events. For example, employees who would typically come to the office can work from home or from any location, and they don't need to worry if they've left their laptops in the office. They can use any web-enabled device such as their tablet or home PC to access the network and stay productive. This minimizes downtime and also assures employees' safety by not requiring them to work at the office during emergencies. In addition, during these events, additional partners and customers can be granted access to ensure that business continues unimpeded.

Features and Benefits

Productivity with Ubiquitous, Any Time Access

Security threats to the global Internet community of today are continuously challenging companies and organizations. Added to these challenges are environmental threats of pandemic or catastrophic events that can bring a business to a halt. Business continuity relies on a company having the ability to maintain their productivity, services and partnerships in the event of a disaster or pandemic. Pandemics, like the H1N1 virus, can impact a business by requiring a company to limit social interaction between employees, partners and customers to isolate further spread of the virus. This provides a compelling reason for the wider adoption of remote access, as employees are quarantined or recommended to work from home for an extended period of time.

To maintain productivity, innovative technologies like SSL VPN help workers to still remain connected, and enable many to work from anywhere, at any time and with any device including unmanaged PCs, smartphones, and tablets. The need for remote access capabilities in the event of a disaster can put a sudden strain on remote connectivity requirements as more employees suddenly create a burst of demand. ICE responds to that sudden peak in demand by providing the ability for a company to expand remote access connectivity whenever it is needed and in a cost effective manner.

Employees can stay productive from anywhere knowing that their corporate devices will make their connection to applications and resources seamless, as if they were physically in the office. The use of SSL eliminates the need for client-side software deployment, changes to internal servers, and costly ongoing maintenance and desktop support. IT organizations have peace of mind knowing that corporate resources will not be compromised due to the best-in-class endpoint security features of Pulse Secure PSA Series, MAG Series or SA Series SSL VPN Appliances. This is especially pertinent when users connect from locations such as the home or public access terminals which are more vulnerable to network threats than the controlled office LAN environment.

Sustained Partnerships with Around-the-Clock, Real-Time Access to Applications and Services

In the early 1990s, there were only limited options to extend the availability of the enterprise's network beyond the boundaries of the corporate central site. These mainly consisted of extremely costly and inflexible private networks and leased lines. However, as the Internet grew, it spawned the concept of virtual private networks (VPNs) as an alternative. Most of these VPN solutions leveraged free/public long-haul IP transport services and the IPsec protocol. VPNs effectively addressed the requirements for costeffective, fixed, site-to-site network connectivity; however, in many ways they were still too expensive for mobile users and they were extremely difficult to deploy for business partners or customers. It is in this environment that SSL VPNs were introduced, providing remote/mobile users, business partners and customers easy, secure access to corporate resources through the Internet— without the need to pre-install a client.

SSL VPNs have sophisticated controls for protecting the network from viruses, worms and other network threats. Unlike IPsec VPNs, SSL VPNs offer control at the user, application and network level, with awareness of the security health status of connecting end nodes. For example, a connecting computer or mobile device can be scanned to ensure that it meets corporate security requirements. Based on knowledge about who the user is and which device he/she is using, the SSL VPN can grant appropriate access rights and audit at a granular level, showing the precise resources accessed. With all of these benefits, SSL VPN technology is seen as the best means to connect remote users, in addition to partners and customers.

ICE provides the scalability and continued security required to provide continued accessibility to partners in the event of a disaster, so that your company can remain productive while sustaining important relationships.

Federal and Other Government Compliance for Contingencies and Continuity of Operations (COOP)

National Security Presidential Directive-51/Homeland Security Presidential Directive-20 (NSPD-51/HSPD-20) requires the U.S. executive branch organizations to develop and maintain a comprehensive and effective continuity capability that includes Continuity of Operations in the event of disaster, pandemic or other catastrophic emergency. The guidelines issued by Homeland Security have been widely adopted by state, local, territorial and tribal governments as well. Under NSPD-51/HSPD-20, each agency is responsible for ensuring, in the context of contingencies and COOP situations, the continued availability of its primary mission-essential functions and national security/emergency preparedness telecommunications services.

Homeland Security guidelines specifically state that continuity programs must support full connectivity for leadership, critical customers, the public and others. Pulse Secure PSA Series Appliances, MAG Series Appliances, or SA Series SSL VPN Appliances with the ICE license option will aid all federal agencies, state and local governments, communities and enterprises in meeting the guidelines of this plan.

Balanced Risk and Scalability with Cost and Ease of Deployment

As an easy-to-deploy and highly secure solution that is purposebuilt for secure remote access, SSL VPN should be on the top of the list for companies drawing up their IT “in case of emergency” plans. ICE provides a cost-effective and scalable temporary approach for mitigating the risk of a disaster or epidemic at a fraction of the cost of implementing a permanent solution which might not otherwise be used.

From a best practices perspective, Pulse Secure PSA Series Appliances, MAG Series Appliances or SA Series SSL VPN Appliances with the ICE license option has all of the necessary features to enable testing before an unpredictable event occurs. For example, ICE can be activated and deactivated to test an appliance during emergency recovery drills. ICE also provides a seamless approach to automatically scaling a system should requirements change for deploying an increased number of remote users permanently, thereby providing investment protection.

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.

Ordering Information

The ICE license is available for use with Pulse Secure Appliance (PSA) models including PSA300, PSA3000, PSA5000, PSA7000c, and PSA7000f or MAG Series Appliance models including MAG4610, MAG6610, or MAG6611, or with certain SA Series models (SA4000, SA4000 FIPS, SA4500, SA4500 FIPS, SA6000, SA6000 SP, SA6000 FIPS, SA6500, and SA6500 FIPS Appliances).

Please note that third-party components such as the Enhanced Endpoint Security license are not included as part of the ICE license. ICE provides licenses for a large number of additional users on a Pulse Secure Appliance (PSA), MAG Series Appliance, or an SA Series SSL VPN Appliance for up to eight weeks for periodic testing and transitioning to permanent licenses, if necessary. ICE licenses can be purchased for products designated for business continuity requirements. Existing SSL VPN customers can also upgrade their SSL VPN appliances with ICE licenses.

Model Number	Permanent License Equivalent
PSA-ICE	In Case of Emergency (ICE) license for PSA
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
SA4500-ICE	ICE license for SA4500
SA4500-ICE-CL	ICE clustering license for SA4500
SA6500-ICE	ICE license for SA6500
SA6500-ICE-CL	ICE clustering license for SA6500

Note: There are specific ICE SKUs for the older EOL (end of life) SA4000 and SA6000 models. The SKUs are SA4000-ICE, SA4000-ICE-CL, SA6000-ICE, and SA6000-ICE-CL.

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

VERSION DS 040317