

# “IN CASE OF EMERGENCY” (ICE) LICENSE OPTION

## Enabling Business Continuity with Remote Access

### Product Overview

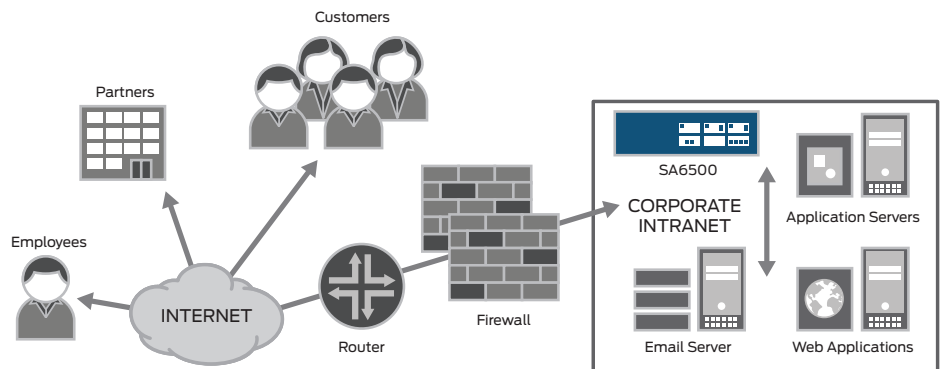
Juniper Networks ICE license option provides companies with a quick resolution when the unexpected happens, delivering the ability to handle extreme peak demands and to support the overall success of the business. The ICE license option can be used in conjunction with either the new MAG Series Junos Pulse Gateways or the legacy SA Series SSL VPN Appliances. ICE enables a company to continue business operations when disaster strikes, maintaining productivity, sustaining partnerships and delivering continued services to customers. 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. The ICE license option offers flexibility and scalability to help organizations effectively balance the costs and the risks inherent in preparing for and coping with “cases of emergency.”

### 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, Juniper Networks® MAG Series Junos® Pulse Gateways or SA Series SSL VPN Appliances with the ICE license option ensures business continuity by helping organizations instantly address a dramatic peak in demand for remote access in cases of emergency by using ICE licenses for a large number of additional users on a MAG Series Junos Pulse Gateway 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)
- 2) A new 25% burst license option (allows bursting of up to 25% of the installed license count on a MAG Series gateway 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 Juniper Networks MAG4610 Junos Pulse Gateway licensed for 100 concurrent users can add the MAGX600-ICE license. When applied and enabled, that ICE license will allow the customer to use 1,000 concurrent users on that device for up to 8 weeks. 1,000 users is the maximum user count supported on the MAG4610.

With the 25% burst license option, for example, if the customer has a MAG-SM360 service module (regardless of whether it is installed in a Juniper Networks MAG6610 Junos Pulse Gateway or MAG6611 Junos Pulse Gateway), with a 1,000 user license, the 25% burst license option will provide an additional 250 users support during an unplanned event. See the MAG Series Junos Pulse Gateways website for more details on the hardware ([www.juniper.net/us/en/products-services/security/mag-series](http://www.juniper.net/us/en/products-services/security/mag-series)).

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 tablets or home PCs 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 from 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 us 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 delivers on 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 with the best-in-class endpoint security features of Juniper Networks MAG Series Junos Pulse Gateways 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 cost-effective, fixed, site-to-site network connectivity; however, in many ways they were still too expensive for mobile users and for business partners or customers, they were extremely difficult to deploy. 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.

The original design of the IPsec VPN protocol was to connect one private network to another with the assumption that both networks were secure using the same security policies. However, network viruses and worms can propagate rapidly and widely through a geographically extended VPN. This is especially pertinent when users are partners connecting from their office PCs and remote devices which are not a part of a company's controlled network. SSL VPNs have more sophisticated controls for protecting the network. 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 can be scanned to make sure that it meets corporate security requirements. Based on knowledge about who the user is and which computer 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 being 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 Government Compliance for Contingencies and Continuity of Operations (COOP)**

In preparation for and response to the threat of Avian and influenza pandemics, the U.S. federal government has prepared an implementation plan for the National Strategy for Pandemic Influenza. This Implementation Plan provides clear direction to federal departments and agencies, state and local governments, communities and the private sector on the actions that must be taken to prepare for a possible pandemic, including contingencies and continuity of operations (COOP) planning. Each agency is responsible for ensuring, in the context of contingencies and COOP situations, the continued availability of its mission essential and national security/emergency preparedness telecommunications services.

The plan includes establishing policies for preventing influenza spread at the workplace. And the plan specifically states enhancing communications and information technology infrastructure, as needed, to support employee telecommuting and remote customer access. Juniper Networks MAG Series Junos Pulse Gateways 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 purpose-built 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 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, Juniper Networks MAG Series Junos Pulse Gateways 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.

### **Juniper Networks Services and Support**

Juniper Networks 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. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit [www.juniper.net/us/en/products-services](http://www.juniper.net/us/en/products-services).

## Ordering Information

The ICE license is available for use with any of the new MAG Series Junos Pulse Gateway models (MAG2600, 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 MAG Series Junos Pulse Gateway 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
MAGX600-ICE	In Case of Emergency (ICE) license for MAG Series Junos Pulse Gateways
ACCESS-ICE-25PC	ICE 25%: Burst to 25% of installed license count on MAG Series Junos 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 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](http://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](http://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.