

What's New in Juniper's IVE Platform Version 5.4

This application note describes the new features available in Version 5.4 of the IVE platform for all Secure Access SSL VPN products. This document assumes familiarity with the Juniper's IVE platform and the features of earlier releases up to version 5.3.

I. Configuration, Administration and Supportability Enhancements

- **Push Configuration to Multiple Targets**

The Push Configuration feature allows customers to push either a partial or a complete configuration from one SSL VPN gateway or cluster to any number of additional SSL VPN gateways or clusters. This feature provides an alternative to clustering, where changes are propagated automatically, so that the administrator can synchronize only those aspects of the configuration that should be shared amongst separate devices/clusters.

Customer Benefits

- Streamlines administration of multiple devices/clusters by allowing customers to share or partial configurations amongst many devices/clusters.

Availability

- All Secure Access Products 1000 and above with Advanced License

- **Resource Profile Templates for Outlook Web Access, iNotes & Sharepoint**

Resource profile templates are customized configuration pages created specifically for selected commonly utilized applications. In the 5.4 release, we have created resource profile templates for Outlook Web Access (OWA), iNotes and Sharepoint. The OWA and iNotes resource profiles will allow administrators to prevent the upload and download of attachments as well as easily control the amount of information that is cached on the end-user's endpoint. The Sharepoint resource profile template enables users to deploy certain Sharepoint features, such as editing in place, without requiring a permanent persistent session cookie. Instead, in order to use these features, administrators can now associate a timeout for the persistent cookie allowing for improved security. These templates join the Citrix Web Interface resource profile template that was introduced in v5.3.

Customer Benefits

- Eases configuration and administration of common applications.
- Makes it easier to configure advanced policies for OWA and iNotes such as prevention of attachment uploads and downloads and endpoint caching.
- Enables the use of certain Sharepoint features without requiring a persistent session cookie.

Availability

- All Secure Access Products with Core Clientless Access

- **Anti-Virus Signature File Version Monitoring**

This feature leverages a Juniper hosted web service which monitors many anti-virus vendors on a regular basis, continually polling them for the latest versions

of the signature files. This data can be regularly downloaded to Secure Access products (automatically), allowing administrators to enforce anti-virus protection policies that require the newest available AV definitions.

Customer Benefits

- Enables administrators to easily specify Host Checker policies that enforce "up-to-date" anti-virus protection.

Availability

- All Secure Access Products

- **Endpoint Security Assessment Plug-in Updates**

Since v5.2, Juniper has included pre-defined Host Checker policies for a wide range of anti-virus, personal firewall, anti-spyware, and anti-malware products. Recognizing that these vendors introduce new versions of their products on a regular basis and that customers do not always have the option to upgrade to newer versions of the Secure Access OS, Juniper has introduced the ability to update the pre-defined policies without upgrading to new versions of Secure Access. New versions of the plug-in are stored on the Juniper Support Center where customers can retrieve the files and update their SSL VPN as needed.

Customer Benefits

- Allows customers to support pre-defined policies for the newest available third-party endpoint security packages without requiring an upgrade to a newer Secure Access OS version.
- Allows customers to support new pre-defined policies more quickly, without waiting for new versions of the Secure Access OS to be released.

Availability

- All Secure Access Products

- **AD Configuration Validation**

In v5.4, we have added validation for Active Directory authentication server configurations. At the time of configuration, this feature tests various aspects of the configuration such as accessibility of AD domain controllers, verifies the existence of the AD domain, confirms whether AD administrator credentials have sufficient privileges, and whether specified authentication protocols (i.e. Kerberos) work successfully.

Customer Benefits

- Improves administrative usability by reducing configuration errors and aiding with troubleshooting.

Availability

- All Secure Access Products

II. Enhanced End-User Platform and Browser Support for Anytime, Anywhere Access

- **Win Mobile 5.0 Pocket PC PDAs and Phones Support**

Mobile device support is enhanced in IVE release 5.4 with the introduction of

support for the Core and WSAM access methods on Win Mobile 5.0 Pocket PC PDAs and phones. WSAM for Win Mobile 5.0 OS enables end users to access any TCP based client initiated corporate application securely from Win Mobile 5.0 Pocket PC PDAs or Phones. This includes support for Pocket Outlook, Pocket Terminal Services, and client initiated ActiveSync with corporate exchange server and other third party applications. The Core access method allows users to browse Intranets and access Web-based applications from Win Mobile 5.0 Pocket PC PDAs and phones.

Customer Benefits

- Granular application layer client/server and web-based application support on Win Mobile 5.0 Pocket PC PDAs and phones enables administrators to provision highly differentiated access to mobile users. Granular logging capabilities allow for detailed auditing of end-user application access.
- WSAM's application layer access is more resilient to the underlying wireless link fading (link up/down) than network layer access allowing mobile users to roam seamlessly across reduced strength wireless coverage and maintain the same authenticated SSL VPN session throughout the wireless data network session
- WSAM is a thin client application layer proxy for secure access to client/server applications from Win Mobile 5.0 devices and has a much smaller footprint than legacy network layer VPN clients, making it ideal for memory constrained mobile devices.
- Anytime, anywhere secure access to backend corporate applications using any standard web browser on Win Mobile 5.0 Pocket PC PDAs and phones.

Availability

- All Secure Access Products 1000 and above with SAMNC license
- **Intel based Macintosh Support**
Support for Intel based Mac end user machines has been introduced in IVE release 5.4 enabling end users to connect to SSL VPN gateways using Core, JSAM and NC access methods. The PowerPC based Macintosh platforms have been supported since IVE v5.0.

Customer Benefits

- Anytime anywhere secure access to back end corporate resources using Intel based Macintoshes.
- Allows administrators to enable secure access to applications from a wide variety of end user platforms

Availability

- All Secure Access Products 1000 and above, SAMNC license required for JSAM and NC access methods
- SA 700 product, Core license required for Core access method
- **Extended Platform Support: Firefox, Suse Linux, Fedora & Windows 2003**
In this release, Juniper has supplemented its browser support to include Firefox 2.0 and has added support for Suse Linux 10, Fedora Core 5 and Windows 2003 Server operating systems. For more details, please see the Secure Access Supported Platforms document for release 5.4R1 in the SSL VPN Technical Resources section in Juniper's Customer Support Center.

Customer Benefits

- Enables users to securely access applications from a greater range of platforms improving end-user usability and productivity.

Availability

- All Secure Access Products

- **SAML POST Profile Support**

In version 5.2 of the Secure Access software, Juniper introduced the ability for the SSL VPN to act as a SAML authentication consumer via the artifact profile method. Release 5.4 extends that support to now include the POST profile method, in which a SAML assertion is pushed directly to the relying party.

Customer Benefits

- Improves usability by allowing the Secure Access products to interoperate directly with a wider variety of existing SAML deployments.

Availability

- All Secure Access Products 1000 and above with Advanced License

III. Enhanced End-User Access

- **Network Connect (NC) Command Line Launcher**

With IVE release 5.4, Network Connect can be auto launched and terminated as part of a script or from a third party application using the NC command line launcher (similar to SAM Launcher) feature. This feature is available for all Windows based end user machines on which NC is supported. For more details on NC supported machines, please see the Secure Access Supported Platforms document for release 5.4R1 in the SSL VPN Technical Resources section in Juniper's Customer Support Center.

Customer Benefits

- Enables seamless user experience by automatically authenticating the user and establishing the NC tunnel in the background.
- Enables machine to machine communication using a script or third party applications to schedule a periodic file upload / download in an automated and secure fashion

Availability

- All Secure Access Products 1000 and above with SAMNC license
- Secure Access 700 products

- **NC GINA Chaining**

NC GINA chaining enables the Juniper NC GINA thin client to be installed on Windows based end-user machines with existing third party GINA clients and for chaining to work seamlessly across multiple GINA clients.

Customer Benefits

- Seamless interoperability with third party GINA clients when using the NC GINA feature

Availability

- All Secure Access Products 1000 and above with SAMNC license
- Secure Access 700 products

Support Meeting

Support Meeting is new type of Secure Meeting designed to meet the need for web conferencing during support calls. Specifically, with a Support Meeting, a support representative is automatically given remote control over the end-users' device. In addition, Support Meeting features a significantly simpler user interface.

Customer Benefits

- Eases use of Secure Meeting for support calls

Availability

- All Secure Access Products with Secure Meeting license

Single Simultaneous Secure Meeting in Advanced License

Starting with v5.4, the Advanced license will include the Secure Meeting functionality and allow the use of one simultaneous meeting with a maximum of three simultaneous users. This feature will enable administrators to easily evaluate the Secure Meeting functionality for further use. In order to support more than one simultaneous meeting and three simultaneous users, administrators will need to purchase the Secure Meeting license.

Customer Benefits

- Enables administrators to easily evaluate Secure Meeting functionality

Availability

- All Secure Access Products 1000 and above with Advanced license

IV. In Case Of Emergency (ICE) Licensing

• In Case of Emergency (ICE) License for Enabling Business Continuity with SSL VPN

ICE is a new SSL VPN-based solution allowing customers to achieve immediate response for any potential dramatic increase for secure remote employee and partner access. Examples include Pandemic (Avian Flu, SARS, ...), natural disasters (Hurricanes, earthquakes, snow storms ...), terror attacks, power or Water outages and transportation strikes. The common theme to all of these is the increase in the need for secure remote access given the geographical isolation and sometimes quarantining. SSL VPN provides secure remote access for big user communities coming from managed and unmanaged PCs and requiring various levels of granular access. Juniper's ICE allows customers to achieve that in a cost-effective manner - ICE provides licenses for a large number of additional users on a Secure Access SSL VPN appliance for a limited time (total of 8 weeks that can be activated and deactivated as needed - allowing for testing and fire drills, emergency use, and buffer to process a new purchase order if the need becomes permanent).

Customer Benefits

- Immediate response for any potential dramatic increase for secure remote employee and partner access.
 - Maintain productivity by enabling anywhere, anytime, and any device secure remote access
 - Sustain partnerships with real-time access to applications and services
 - Continue to deliver exceptional service to customers and partners with online collaboration
 - Meet government mandates for DR and compliance
- Flexible deployment - ability to test the solution initially and periodically and deploying it as a warm or cold backup.

Availability

- Secure Access 3000 and above with In Case of Emergency (ICE) license