

What's New in Juniper's IVE Platform Version 5.3

This application note describes the new features available in Version 5.3 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 5.2.

Highlights of this Release

I. Configuration, Administration and Supportability Enhancements

- **Resource Profiles**
- **Basic Configuration and Endpoint Security Task Guides**
- **Pre-Defined Host Checker Policies**
- **High Availability External and Internal Port Pairs**

II. Enhanced End-User Access

- **Enhanced Sharepoint Support**
- **Start and Stop scripts support with Network Connect**

III. Security Enhancements

- **Coordinated Threat Control with Juniper's Secure Access SSL VPN and Intrusion Detection and Prevention Products**
- **Network Connect GINA and End Point Security Integration**

IV. Virtual System Enhancements

- **Path Based URLs for Instant Virtual Systems (IVS)**
- **Centralized DHCP support for Instant Virtual Systems (IVS)**

I. Configuration, Administration and Supportability Enhancements

- **Resource Profiles**

Resource Profiles are a new concept in the IVE that enables optimized configuration of resources and represents a more application-centric approach to configuring resources for secure access. A Resource Profile is a logical representation of all the resource policies and end-user bookmarks required to provide secure access to an Administrator defined resource. Resource profiles do not make any changes to the concept of resources policies, such as access policies, or bookmarks. Rather, a resource profile is simply a new, easier way to create and organize resource policies and bookmarks that allows administrators to map resources to which they want to provide access to a single set of configurations in the UI.

- **Customer Benefits**

- Eases configuration of resources by providing a single guided configuration flow and reducing the number of configuration steps.

- Improves administration by minimizing configuration changes due to changes in resources and by allowing administrators to manage resource related configurations in a single location in the UI.

Availability

- All Secure Access Products with Core Clientless Access

- **Resource Profile Templates**

Resource profile templates are customized configuration pages created specifically for selected commonly utilized applications. In the 5.3 release, we have created a Citrix web resource profile template that enables an admin to configure Citrix deployed via Web Interface/nFuse and/or the Java ICA client. The Citrix template allows users to configure all the necessary policies to provide secure access to Citrix and in addition simplifies configuration of single sign-on (SSO) by providing typical SSO settings.

Customer Benefits

- Eases configuration and administration of common applications.
- Makes it easier to configure advanced policies such as Single Sign-on.

Availability

- All Secure Access Products with Core Clientless Access

- **Basic Configuration and Endpoint Security Task Guides**

Task Guides are quick and easy procedures that guide administrators through common configuration tasks. Task Guides make configuration tasks easier by providing links to relevant screens in the administration console and to the help system. In 5.3, we provide task guides for a Basic configuration that guides a user through creation of Authentication Servers, Roles, Realms, Sign-in Policies and Resources, and for an Endpoint Defense configuration.

Customer Benefits

- Makes basic configuration of system easier.
- Utilizes a flexible approach that doesn't restrict administrators to a set configuration flow.
- Teaches administrators locations in UI while walking them through key Task Guide steps.

Availability

- All Secure Access Products

- **Pre-Defined Host Checker Policies**

In IVE v5.2, Juniper introduced the pre-defined Host Checker policy feature, which enables point-and-click configuration of endpoint security policies. With IVE v5.3, Juniper has extended that functionality by offering support for a wider range of pre-defined checks for antivirus, firewall or spyware applications to easily ensure that the selected applications are installed and running before granting access to users needing corporate access.

Customer Benefits

- Enables customers to easily configure Host Checker policies for third party endpoint applications.
- Removes requirement for administrators to independently determine how to set up checks for these applications.

Availability

- All Secure Access Products

- **Across Role Configuration Views**

Across role configuration views allows administrators to view configured settings related to selected or all roles. In this release, we have created the ability to allow administrators to view bookmarks and role restrictions for all or for selected roles.

Customer Benefits

- Improves ability for administrators to understand and audit current configuration settings from a role perspective.

Availability

- All Secure Access Products

- **Simplified configuration pages**

Going forward within configuration pages, we will separate less frequently used from more frequently used settings so as to reduce the complexity of the page and focus administrators on the required settings. In this release, we have simplified the New Authentication Realm page and the Role Web Options page.

Customer Benefits

- Reduces the complexity of configuration pages.
- Makes clearer to new administrators which settings are important for common configurations versus those that are not as common.

Availability

- All Secure Access Products

- **Customization of Administrative User Interface Views**

In 5.3, we have developed a configurable framework for customizing the appearance of pages or tabs in the web GUI. In this release, this framework has been enabled to customize the appearance of the Web Resource Policy pages/tabs. An administrator can show or hide pages by clicking on the "Customize view" button in the top right of every page in the Web Resource Policy section.

Customer Benefits

- Reduces complexity of Administrative UI by allowing administrators to only view the configuration pages that they require for their environment.

Availability

- All Secure Access Products

- **Configurable Viewing of Auto-Allow Options in UI**

Going forward, we encourage all administrators to use resource profiles as the primary way to configure bookmarks and resource policies. Resource profiles obviate the need to configure resources via creating bookmarks and selecting auto-allow. As a result, we have created the ability to hide the auto-allow options (located in web bookmarks, file bookmarks, SAM options, Telnet/SSH options, and Terminal Services options pages) in pages under the User Roles. Existing customers will find that auto-allow options are not hidden on upgrades. For fresh installs, however, auto-allow options will be hidden by default.

Customer Benefits

- Simplifies GUI by reducing number of ways customers can configure resources.

Availability

- All Secure Access Products

- **Disabling Accounts**

This functionality allows administrators to temporarily disable any authenticated user account and then easily enable that user later without having to recreate the account. When the account is disabled, the user will not be able to login to the SSL/VPN device and an error message will be displayed stating that the account was disabled by the administrator. If a user is logged in when the account is disabled, they will be forced out with the same error message. This feature is an enhancement of a 5.2 feature which enabled disabling accounts for locally authenticated users only.

Customer Benefits:

- Enhanced security – questionable accounts can be disabled
- Ease of use – reduces user account administration tasks.

Availability

- All Secure Access Products

- **LDAP Authentication Server Configuration Improvements**

In 5.3, we are making two improvements to the LDAP authentication server configuration. First, we will provide more default values for each LDAP server type. Second, we will provide more input validation by checking for the following: Server and Port, Admin credential, Base DN for Users, Base DN for Groups and providing warnings and/or errors in case of failures.

Customer Benefits

- Eases configuration of LDAP authentication servers.

Availability

- All Secure Access Products

- **Duplicate Realm**

Administrators now have the ability to duplicate a realm.

Customer Benefits

- Eases configuration of Realms.

Availability

- All Secure Access Products

- **Improvements to Navigation Bar**

In 5.3, we have restructured the navigation bar that appears on the left side of the Administrator web GUI in order to make it more intuitive and accommodate new features. For more details on changes, please see the document entitled "Introduction to IVE 5.3 Administrative UI Changes" on the support site.

Customer Benefits

- More intuitive names make it easier to learn how to navigate to necessary configuration pages.

Availability

- All Secure Access Products

- **Client Log Upload**

In 5.3, we have developed the ability to upload client logs for all client components including: Host Checker, Cache Cleaner, Meeting, Windows Secure Application Manager, Java Secure Application Manager and Applet Rewriting, Network Connect, and Terminal Services. Client logs are uploaded over HTTP allowing upload even when SAM, NC or Terminal Services are not working. Client log upload can be controlled on a per role basis.

Customer Benefits

- Enhances ability of IVE administrators and Juniper support to troubleshoot issues with clients.

Availability

- All Secure Access Products

- **Ethernet Port Statistics/Counters**

Now on the Network overview page of the Web Admin User Interface, the IVE provides the following Ethernet statistics: number of TX and RX packets, number of dropped packets, and number of errors.

Customer Benefits

- Enhances ability of IVE administrators and Juniper support to troubleshoot network issues.

Availability

- All Secure Access Products

- **Administrator Specified Active Directory Computer Names**

By default, when an Active Directory (AD) authentication server is created, the IVE will create a hard-coded computer object in the trusted AD domain and join the domain using that computer object. This feature allows the Administrator to change that computer object to a name of their choosing so that it remains consistent with their internal AD naming scheme. This name must be unique across all units in a cluster.

Customer Benefits

- Improved manageability by allowing administrators to conform to company-specific AD naming schemes.

Availability

- All Secure Access Products

- **Active Directory Authentication Protocol Selection**

Juniper's Active Directory authentication server implementation supports three authentication protocols: Kerberos, NTLMv1 and NTLMv2. This enhancement allows the administrator to independently configure whether each protocol will be used or ignored.

Customer Benefits

- Improves usability by avoiding authentication attempts through protocols that are not supported by the customer's AD implementation. Attempts using unsupported protocols count against the failed login count policy in AD.

Availability

- All Secure Access Products

- **High Availability External and Internal Port Pairs**

This feature enables two additional mini-GBIC (Small Form Factor Pluggable - SFP) ports on SA 6000 and SA 6000 SP in high availability external and internal port pair configuration. Administrator can dual home the IVE to two upstream and/or downstream nodes in their network to ensure no single point of failure. Without this feature, all the nodes in an IVE cluster are connected to only one upstream and/or downstream node and if that node fails, all nodes in the IVE cluster become unreachable creating a single point of failure in the network. The SFP based additional Ethernet ports on SA 6000 / 6000 SP can be Fiber SX or LX or Copper 1000 interfaces.

Customer Benefits

- Allows for fully meshed / redundant configuration of IVE with multiple load balancers for optimized uptime
- Provides distance flexibility with Fiber SX or LX connections

Availability

- Secure Access 6000 and Secure Access 6000 SP

- **Delete Configuration Command**

In this release, we have created the ability to delete the system configuration. This feature will delete all system configuration information but will retain the code version that is installed on system. This feature is accessed as a command in the console interface.

Customer Benefits

- Enables users to easily re-configure the product.

Availability

- All Secure Access Products

II. Enhanced End-User Access

- **Enhanced Sharepoint Support**

With this release, Juniper Networks has enhanced their support for Sharepoint. Juniper continues to support Sharepoint through Pass-Through Proxy rewriting mode, Secure Application Manager and Network Connect. In this release, we also provide qualified support for Sharepoint through the IVE's Content Intermediation Engine or rewriter.

Customer Benefits

- Allows customers to support Sharepoint deployments through the Content Intermediation Engine enabling truly clientless support, single sign-on, and granular access control and logging.

Availability

- All Secure Access Products with Core Clientless Access

- **PDF Rewriting**

With this release, rewriting of absolute URLs in PDF documents is now supported. PDF rewriting can be controlled on per role basis under Role > Web > Options.

Customer Benefits

- End-user can now utilize hyperlinks to absolute URLs in PDF documents during IVE sessions.

Availability

- All Secure Access Products with Core Clientless Access

- **Start and Stop scripts support with Network Connect**

This feature enables Network Connect to launch Windows Start script once the tunnel is established and to launch Windows Stop scripts once the tunnel is terminated. Scripts can be local or remote to the client.

Customer Benefits

- Enables administrators to run and execute certain tasks and/or commands automatically with Network Connect.

Availability

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

- **Upload Java Applet Enhancements**

The Java Applet upload functionality now supports the uploading of file types other than jar and cab. This enables administrators to upload configuration, text, gif or html files to which an applet may refer that are necessary for the applet to work seamlessly. Administrators upload these files via a zip file that can contain multiple files in a hierarchical or a flat organization as well as the Java applet.

Customer Benefits

- Enables the generic Java applet upload functionality to work with Java applets that refer to other files.

Availability

- All Secure Access Products with Core Clientless Access

- **HTTP 1.1 Compatibility**

The IVE is now compatible with HTTP 1.1 servers. In this release, HTTP 1.1 protocol support is not enabled by default. Administrators can enable HTTP 1.1 by writing a web resource protocol policy.

Customer Benefits

- Enables IVE to utilize HTTP 1.1 with backend servers.

Availability

- All Secure Access Products with Core Clientless Access

- **Custom Error Messages**

In 5.3, administrators now have the ability to customize IVE end-user web browsing error messages. Customizable error messages include: (1) Access Blocked when user tries to access a site with a denied resource policy, (2) Form Post Blocked when Remote SSO post was performed earlier and cached and admin has turned off SSO for this resource, and (3) Invalid SSL Site Disabled when browsing to SSL sites has been disabled. Administrators can customize the error messages for each locale the IVE supports (Chinese simplified, Chinese traditional, French, German, Japanese, Korean, and Spanish). Error messages are customized on a system wide basis under Role Default Options > Custom Messages.

Customer Benefits

- Enable administrators to have greater control over end-user messages and interactions allowing them to customize the messages to their IT environment.

Availability

- All Secure Access Products with Core Clientless Access

- **Session Timeout Extension**

This administrator configurable option will allow end-users to extend their sessions by re-authenticating as they reach the session timeout limit. If authentication is successful, the timer will restart and the user's session will be extended, regardless of access method (Core, SAM, NC).

Customer Benefits

- End users can continue sessions without interruptions or loss of connectivity to remote resources that could result in loss of unsaved data

Availability

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

- **Support for Japanese eZweb and Vodafone Phones**

In this release we provide support for basic html/chtml rewriting for Japanese eZweb and Vodafone mobile phone, which utilize the Openwave Mobile browser.

Customer Benefits

- Enables users of eZweb and Vodafone phones in Japan to access web applications through the IVE

Availability

- All Secure Access Products with Core Clientless Access

III. Security Enhancements

Coordinated Threat Control with Juniper's Secure Access SSL VPN and Intrusion Detection and Prevention Products

Coordinated Threat Control technology enables Juniper's Secure Access SSL VPN and IDP appliances to tie the session identity of the SSL VPN with the threat detection capabilities of IDP to effectively identify, stop, and remediate both network and application-level threats within remote access traffic. With this technology, when IDP detects a threat or any traffic that breaks an administrator configured rule, it can, in addition to blocking that threat, signal Secure Access. Secure Access uses the information from IDP to identify the user session that is the source of undesired traffic and can take actions on the endpoint including: terminating the user session, disabling the user's account or mapping the user into a quarantine role. Administrators can configure the quarantine role so that they can provide users with a lower level of access to resources and inform the user of why they have been quarantined and what they should do in order to

remove themselves from the quarantined role. Secure Access allows Administrators to take action on user sessions either manually by selecting an active user session and executing the desired action, or automatically by creating policies that will execute the desired actions as soon as a signal that matches the policy criteria is received from IDP.

Juniper's coordinated threat control solution with SA and IDP products is easy to deploy and utilizes a simplified "self-registration" process to set up the signaling connection. The solution could be deployed in two ways. First, Secure Access will work seamlessly with an IDP deployment designed for total perimeter security, not just remote access security, requiring virtually no changes on configuration changes on IDP and minimal configuration on SA. Second, a dedicated IDP working in combination with SA can also be deployed solely for remote access security purposes.

Customer Benefits

- Deploying Juniper's SSL VPN and IDP products provides unmatched, multi-protocol threat control capabilities for extended enterprise access deployments including detecting and protecting against sophisticated application layer threats (host and application vulnerabilities, worms, Trojan horses, and others), and providing deep visibility into application layer traffic.
- Correlated threat information allows administrators to instantly identify users and correlate user and traffic information to provide critical information to mitigate security incidents.
- Coordinated threat response gives administrators the ability to react to threats by not only blocking attacks before they reach their targets, but also by taking action against the remote access device and/or user that is the source of the attack.
- The combination of SA and IDP also provides unprecedented visibility and granular control over application usage enabling administrators to provision and monitor access to networks and applications in a way that dramatically reduces a company's security exposure when providing extended enterprise access.

Availability

- All Secure Access Products 1000 and above with Advanced license
- All IDP appliances with IDP 3.2R2 software

- **Network Connect GINA and End Point Security Integration**

Juniper's Network Connect GINA feature is further enhanced in IVE 5.3 by integrating it with Juniper's End Point Defense Initiative (J.E.D.I). Network Connect GINA enables end users to establish a secure VPN tunnel to the IVE prior to Windows logon. Having a secure connection to a corporate Windows infrastructure prior to Windows logon allows scripts to establish network drive mappings, update client's Group Policy store, and run any software updates/patches as part of a software delivery mechanism, such as SMS. Integrating Network Connect GINA with end point security functionality allows administrators to conduct pre-authentication or post authentication end point security checks on the user's machine using Juniper's Host Checker functionality before the network layer tunnel is established. If the end user machine is

determined to be compliant as part of these end point security checks, Network Connect GINA proceeds to establishing the network layer tunnel.

Customer Benefits

- Increases administrators' ability to enforce security policies for devices using Network Connect with GINA integration.

Availability

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

- **Ability to Disable Windows Terminal Services Drive and Printer Access**

In IVE OS 5.3, the Administrators will have the option of disabling access to local printers and drives for user created Windows Terminal Services bookmarks.

Customer Benefits

- Enables administrators to control the security settings of Terminal Services and reduce the risk of lost intellectual property through printing to local printers or saving information to local drives.

Availability

- All Secure Access Products 1000 and above with SAMNC license

- **Out-of-Band Management Ethernet Port**

With IVE v5.3, Juniper Networks has added an out-of-band management Ethernet port, enabling administrators to have always-on management (configuration, monitoring, etc) access to the SA appliance through a dedicated port. Once the Out-of-Band management port is enabled, all management traffic transfer such as admin log in, syslog, FTP, NTP, SCP, archiving, etc, is directed through management port only, resulting in complete separation of management and user traffic through the IVE.

Customer Benefits

- Allow for always-on management access.
- Enables seamless integration into dedicated management networks.

Availability

- Secure Access 6000 and Secure Access 6000 SP

IV. Virtual System Enhancements

- **Path Based URLs for Instant Virtual Systems (IVS)**

With IVE v5.3, the sign-in URL for an IVS can be path based in addition to being host name based. For example, using this feature, a service provider can define a sign-in URL for a customer / IVS to be www.serviceprovider.com/customer1. This feature enables multiple IVS's on a single or clustered IVE to be accessed via a single IP address. As a result, only one server certificate and one DNS entry will be required across all IVS's provisioned on an IVE.

Customer Benefits

- Enables service providers to provision sign-in URL's for each customer / IVS without requiring a specific server certificate for that URL.

Availability

- Secure Access 3000 and above with Instant Virtual System (IVS) license

- **Centralized DHCP support for Instant Virtual Systems (IVS)**

This feature enables Network Connect (NC) users across multiple IVS's to receive their IP addresses from a centralized DHCP server located in service provider network. The DHCP server maintains separate IP address pools for each customer / IVS. DHCP requests issued by an IVS are marked with identifying information, thereby allowing the server to issue an IP address from the pool specific to that particular customer / IVS.

Customer Benefits

- Enables service providers to seamlessly provision and manage NC IP addresses for multiple customers using a single central DHCP server.

Availability

- Secure Access 3000 and above with Instant Virtual System (IVS) license