

What's New in Juniper's NetScreen IVE Platform Version 4.2

This application note describes the new features available in Version 4.2 of the NetScreen IVE platform for NetScreen Secure Access, Remote Access and Secure Meeting products. This document assumes familiarity with the Juniper's NetScreen IVE platform and the features of earlier releases including Versions 4.1 and 4.1.1.

Highlights of this Release

The enterprise integration features and dynamic capabilities of the 4.2 version of the IVE platform enables:

- **Increased ease of deployment**
 - **Adaptive Support for Proxy Settings**
 - **Enhanced Single-Sign On to Terminal Services and Citrix applications**
 - **Support for Multiple Credentials on the Sign-in Page**
 - **Native Citrix Win32 Integration**
 - **Enhanced ActiveX Re-writing**
 - **Support for multiple DNS/WINS IP Address settings**
 - **Enhanced PKI support**
 - **Secure Meeting Support for Outlook Integration**
 - **Secure Meeting LDAP Integration**
- **Extended ability to deploy secure access**
 - **Adaptive Delivery for Secure Application Manager, Network Connect and J.E.D.I.**
 - **Support for J.E.D.I. in restricted user privilege environments**
- **Enhanced ease of use, management and support**
 - **Dynamic Log Reporting**
 - **Support for RADIUS Accounting**
 - **SNMP MIB Enhancements**
 - **Dynamically Provisioned Bookmarks, Applications and Resource Policies**

- **Static IP Address Support for Network Connect Session**
- **Support for XML Export of Role Mapping Rules**
- **Enhanced Client Side Logging for Secure Application Manager**
- **Korean and Spanish Localization**
- **Secure Meeting Support for Annotation**
- **Selective Application of Web Compression**
- **Getting Started Task Guide**
- **Configurable End-User Help Link and Bookmarks**

Keys for Availability

- Any feature that is listed as an IVE platform feature applies to Secure Access, Secure Meeting and Remote Access products
- Any feature that requires the Network Connect license applies to Secure Access & Remote Access products
- Any feature that requires the Secure Application Manager license applies to Secure Access products only
- Any feature that requires the Central Manager license is applicable to Secure Access and Secure Meeting products
- Any feature that requires an Advanced Secure Meeting Upgrade is applicable to the Secure Access products only

I) Increased ease of deployment:

1. Adaptive Support for Proxy Settings: Network Connect adapts automatically to environments where web proxy servers are deployed

With this feature, Juniper Networks provides automated support for environments where proxy servers have been deployed. When Network Connect is launched, it automatically determines the proxy settings needed either to get to the IVE gateway or to be able to access internal applications.

Customer Benefits

- Enables administrators to seamlessly deploy Juniper's SSL VPN solutions in their existing infrastructure.
- Enhances end-user experience and reduces administrative support costs by minimizing need for end-user interaction in adapting to proxy environments.

Availability

- Network Connect License

2. Enhanced single-sign on to Microsoft Terminal Services and Citrix applications

User credentials processed at the time of initial Secure Access login can later be used for single-sign on to Microsoft Terminal Services or Citrix applications accessed during the SSL VPN session.

Customer Benefits

- Simplifies administration of terminal services applications secured through the Secure Access gateway

- Provides a seamless end user access experience by reducing keystrokes required for successful sign-on

Availability

- Secure Application Manager License

3. Support for Multiple Credentials on the Sign-in Page

With this feature, Juniper Networks allows users to enter multiple credentials on the sign-in page. Users enter these credentials once upon login and the process is automated from that point forward. The primary credential is required for the IVE platform authentication and then the primary or optional secondary credential can be used for authentication and/or Single Sign On (SSO). Following are some examples: (1) NTLM SSO for internal web sites that are protected by Windows Authentication; (2) Basic Authentication SSO for internal web sites in the intranet zone; (3) NTLM SSO for Internal Windows File Shares that are protected by Windows Authentication; (4) Web (Remote) SSO; and (5) Terminal Services SSO. The secondary credential will be validated only if the user's primary authentication succeeds.

Customer Benefits

- Advanced SSO support improving user experience for access to internal applications.
- Seamless means for users to use SSO for applications that are integrated into the Windows domain authentication and other directories.
- Enhanced ability for users to authenticate easily to multiple applications that require different credentials (e.g. token, Active Directory, other LDAP directories) increasing interoperability in enterprise-level environments that require multi-step multi-protocol use for access.

Availability

- All Secure Access and Remote Access Products

4. Native Citrix Win32 integration

This feature enhances existing Citrix support for Java ICA and Windows ICA clients by providing native Win32 Citrix integration with adaptive delivery that would allow provisioning of Citrix Win32 clients directly from the Secure Access gateway to the end user connection device. Administrators and/or end users can setup bookmarks that launch a separate window from which users will have secure access to Citrix-based servers and/or applications without the need for a pre-installed Citrix client.

Customer Benefits

- Enables administrators to provide Win32 solution for secure access to Citrix-based applications without the cost of managing and delivering Citrix client software.
- Provides users with immediate access to Citrix-hosted applications without the need for a pre-installed Citrix ICA client or a Java Virtual Machine.

Availability

- Secure Application Manager License

5. Enhanced ActiveX Re-writing

With this feature, administrators can configure and manage a list of specific ActiveX ClassIDs and parameters that the Secure Access gateway will rewrite when delivered through the Content Intermediation Engine.

Customer Benefits

- Enables more flexible use of ActiveX controls in applications that need to be accessed through the Secure Access gateway, while retaining hostname obfuscation to end users.

Availability

- All Secure Access Products

6. Support for multiple DNS/WINS IP Address settings

Managed Service Providers need to manage an infrastructure environment that supports multiple DNS/WINS server settings. With this feature, managed service providers can create connection profiles that map a user not only to his roles but also to a configurable DNS and WINS IP address setting during a Network Connect session. This enables service providers to segregate traffic to the appropriate company's servers based on the user profile and thus manage a hosted environment more effectively.

Customer Benefits

- Enables seamless deployment of Juniper Networks SSL VPN solutions into existing managed hosting environments.
- Helps service providers manage their hosting networks more securely by deploying company specific access.

Availability

- Network Connect License

7. Enhanced PKI Support

The maximum supported size of the Certificate Revocation List has been increased from 7.5 MB to 15 MB.

Customer Benefits

- Ability for administrators to support diverse PKI deployments with greater flexibility.

Availability

- All Secure Access and Remote Access Products

8. Secure Meeting MS Outlook Integration

Secure Meeting now supports integration with the MS Outlook calendar item and Meeting Creators can schedule events and invite attendees through their Outlook client. The Secure Meeting information is stored on the appliance and displays within the calendar item in Outlook.

Customer Benefits

- Provides an integrated user experience and simplifies the ability for meeting organizers to leverage outlook contacts and availability to create and coordinate events within a single tool.

Availability

- All Secure Meeting Products and Advanced Secure Meeting Upgrade

9. Secure Meeting LDAP Integration

With this release support for LDAP for AAA and Role Mapping is extended within the Secure Meeting series and upgrades so that Meeting creators can view and search a corporate directory for Meeting Attendees. With enhanced LDAP integration, meeting creators can search for users by name, ID, email address, or other attributes. Administrators can setup one or more directory servers that a meeting creator can use to search the identity store and view results that include users, email addresses, and additional specified attributes before adding users to a meeting.

Customer Benefits

- Simplifies the user experience by eliminating the need for meeting creators to search for attendees by user ID or specify them by email address.
- Simplifies Meeting Policy Management by enabling administrators to leverage existing directory settings on the IVE platform to invite users to meetings.

Availability

- All Secure Meeting Products and Advanced Secure Meeting Upgrade

II) Extended ability to provide secure access

1. Adaptive Delivery for Network Connect, Secure Application Manager and J.E.D.I.

Adaptive delivery of Network Connect and Secure Application Manager (SAM) enables corporations to provide suppliers application and/or network level access from a broad array of potential connection environments, even including those where ActiveX has been disabled. Adaptive delivery of J.E.D.I. enables administrators to perform pre-authentication security policy checks and deploy best of breed end point security solutions from a broad array of connection points, even where the ActiveX settings have been disabled. Users who need higher levels of access from unmanaged devices can launch Secure Application Manager or Network Connect and gain appropriate access while J.E.D.I. automatically deploys in such environments to ensure that the end point complies with the security policies of the network.

Customer Benefits

- Extends the ability of administrators to provision secure remote access from a broader array of connection environments like remote kiosks and unmanaged devices.

Availability

- Adaptive delivery of Network Connect: Network Connect License
- Adaptive delivery of SAM: SAM License
- Adaptive delivery of J.E.D.I.: All Secure Access and Remote Access Products

2. Support for Juniper Endpoint Defense Initiative (J.E.D.I.) in restricted user privilege environments

With this feature, J.E.D.I. supports restricted user environments on the end-point device, when a user attempts to make a connection to the IVE platform. This enables system administrators to ensure that Host Checker and Cache Cleaner can be deployed on unmanaged devices with restricted user privileges, where endpoint defense and ensuring policy compliance before providing access are of paramount importance. Host Checker and Cache Cleaner will also support Windows 98 Operating System.

Customer Benefits

- Maximizes administrators' ability to provide secure access to employees, partners and suppliers.
- In conjunction with Adaptive Delivery of SAM, NC and J.E.D.I., this feature will enable system administrators to provide granular access, while ensuring that connection environments are compliant with the security needs of their networks.

Availability

- All Secure Access and Remote Access Products

III) Ease of Use, Management and Support

1. Dynamic Log Reporting

New dynamic capabilities have been added to the logging and reporting tools. Specifically, administrators can now filter existing logs without creating and then applying a new filter. They can do that by either defining the new filter in a simple textbox within the log page or by clicking on a specific variable from the existing log data.

Customer Benefits

- Flexible and dynamic log filtering and reporting.
- Enhanced manageability.

Availability

- Central Manager License

2. Support for RADIUS Accounting

With this feature, Juniper Networks supports standard RADIUS Accounting (RFC 2866) messages for user activity on the IVE platform. Specifically, upon user login and logout, the IVE platform sends Accounting Start and Stop messages respectively. RADIUS Accounting is the standard way to provide details on the end user activity through the NAS (Network Access Server) device in traditional remote access solutions.

Customer Benefits

- Enhanced interoperability with existing customer RADIUS accounting infrastructure enabling reporting and billing based on the information on the RADIUS accounting server.
- Enables actionable reporting on IVE user activity in environment with RADIUS servers.

Availability

- All Secure Access and Remote Access Products

3. SNMP MIB Enhancements

Simple Network Management Protocol (SNMP) support has been enhanced to include various new traps: (1) 'Log full' traps for each log file (event, user, admin); (2) Traps for IVE disk space; (3) Trap for every major or critical log message; (4) Trap for local user count (when in a cluster); and (5) Trap for cluster VIP failovers. and queryable objects: (1) Information on dashboard's swap memory utilization and (2) Information on local user count (when in a cluster)

Customer Benefits

- Advanced management and monitoring.

Availability

- All Secure Access and Remote Access products (where applicable)

4. Dynamically Provisioned Bookmarks, Applications and Resource Policies

With this feature, Juniper Networks allows administrators to dynamically define user bookmarks, applications, and/or resource policies using variables available in the user session context such as LDAP user attributes. Among others, this allows administrators to: (1) Configure automatic access to users' home directory on Windows File Shares; (2) Configure the list of servers (e.g. Exchange, Terminal servers) based on attributes available in the user record;

Customer Benefits

- Facilitates easy definition and configuration of complex and user-specific settings.

Availability

- All Secure Access products and Remote Access products (where applicable)

5. Static IP Address Support for Network Connect Session

This feature provides the ability to specify a fixed IP address to a Network Connect connection based on the response returned in a RADIUS Access-Request.

Customer Benefits

- Enhances administrators' ability to manage by providing seamless interoperability with existing infrastructure like RADIUS servers.

Availability

- All Secure Access and Remote Access Products

6. Support for XML Export of Role Mapping Rules

Extending the existing XML import and export capabilities of the IVE, Juniper Networks has added the ability to export role mapping rules.

Customer Benefits:

- Increased ability to audit the user's association with roles defined in the IVE.

Availability

- All Secure Access and Remote Access Products

7. Enhanced Client Side Logging Capability for Secure Application Manager (SAM)

This feature provides an enhanced ability to support end-users with a friendly user interface that helps pinpoint problems quickly and thereby fix issues in a more timely fashion. The client interface has detailed diagnostics that help administrators and users trace a SAM session with the help of an event log that tracks the progress of each request, identify the precise nature of a failure and thereby troubleshoot problems more effectively during the session.

Customer Benefits

- Enhanced manageability and support.

Availability

- Secure Application Manager license

8. Support for Korean and Spanish Localization

Juniper Networks SSL VPNs are double-byte character set enabled. With this release, Juniper Networks supports Korean and Spanish localization. These languages will be supported across the entire end user interface including all access methods (Core, Secure Application Manager, Network Connect), J.E.D.I. native components: Host Checker and Cache Cleaner, etc.

Customer Benefits

- Extends corporations ability to deploy Juniper's SSL VPN solution on a more global scale.

Availability

- IVE Platform

9. Support for Annotation in Secure Meeting

This feature allows users to mark annotations on the screen so other users can see it. Annotation supports a set of drawing tools and highlighting tools, including a "laser pointer," circles and rectangles. "Annotation mode" enables presenters and attendees to markup meeting content as they would on a white board in a physical meeting.

Customer Benefits

- Enhances the meeting experience of the end user by creating an atmosphere that more closely mimics a "real world" meeting.

Availability

- All Secure Meeting Products

10. Selective Application of Web Compression

Administrators have the ability to determine whether to apply compression to particular traffic to a particular resource as part of web or file resource policy. Supported content types include: text/html, text/plain, text/css, text/javascript, text/rtf, application/pdf, application/msword, application/ms-powerpoint, and application/ms-excel.

Customer Benefit

- Allows administrators to better control performance and improve troubleshooting.

Availability

- Applies only to Secure Access 5000 products

11. Getting Started Task Guide

This Guide will provide customers with step-by-step instructions on how to initially set up the Secure Access, Remote Access and Secure Meeting products including setting system date and time, changing the administrator session timeout options, obtaining the latest IVE platform service package, entering the license key and creating a test user. The Remote Access Series Guide also includes steps for creating a Network Connect profile. Each instruction step includes a link to the relevant administrator page. The Task Guide also includes information on key concepts relevant to configuring the IVE. The Guide is activated on initial configuration as well as being available through the help link.

Customer Benefit

- Simplifies initial setup and reduces set-up time.

Availability

- IVE Platform

12. Configurable End-User Help Link

With this feature, administrators will be able to configure the end-user Help link on a per-role basis. Administrators can either enable the online help, point the help link to an administrator defined URL or disable online help.

Customer Benefit

- Allows administrators to better control their end-user experience by customizing the assistance information available to users on a role by role basis.

Availability

- IVE Platform

13. Configurable End-User Bookmarks

With this feature, Administrators can specify whether bookmarks on the end-user bookmark page should open in a new window.

Customer Benefit

- Improve end-user experience by allowing users to maintain their home page in a separate window as they navigate to specific bookmarks.

Availability

- IVE Platform