



## What's New in Juniper's IVE Platform Version 5.5

The new release of Secure Access SSL VPN IVE 5.5 introduces support of Microsoft Vista. Version 5.5 of the IVE platform is applicable for all Secure Access SSL VPN products and supports Microsoft Vista 32 bit platform only. This document assumes familiarity with Juniper's IVE platform and the features of earlier releases up to version 5.4.

It is worth noting, from this IVE Software version 5.5 release and onwards, Windows 98 SE and Windows NT are no longer supported.

Firefox 2.0 is supported in IVE 5.5R1 and higher for Microsoft Vista.

**All Secure Access features are supported on Microsoft Vista IVE 5.5** with the following very minor exceptions:

- Secure Virtual Workspace is not supported for the Microsoft Vista platform only
- JSAM using modification of the host file and registry is not supported only on Microsoft Vista – This issue will be resolved in IVE platform version 6.0
- JSAM/Netbios is not supported for the Microsoft Vista platform only
- Adaptive delivery for Java is not supported for Microsoft Vista users on Internet Explorer 7. Java delivery is supported for non Microsoft Browsers, such as Firefox 2.0 (review the supported platform documentation for a complete list of browsers supported per component).
- To use Sharepoint 2003 through the rewriter on Microsoft Vista, users must add the IVE to the Trusted Sites zone on Internet Explorer 7 where Protected Mode is disabled. You must enable Persistent Session on the SA as well for Sharepoint Explorer View to work on Vista machine.
- With Microsoft Vista's strong host model enabled, when Network Connect client connects to IVE, current local area network traffic doesn't go through Network Connect tunnel even if split tunnel disabled is configured.

We recommend you to refer to the brief Knowledge Base article at the link below for updated list of minor exceptions: <http://kb.juniper.net/KB9678>

Other new features in IVE platform version 5.5

- Network Connect (NC) Connect at Log Off (Also known as NC double log on)
  - Enables end user to log into the Windows desktop using cached credentials and to establish a NC tunnel automatically to the domain controller. The user is automatically logged off while keeping the NC tunnel persistent such that the user can now log back in with their domain credentials. A user's log in script, domain single sign on, and file drive mapping can now be performed without requiring Microsoft GINA plug in

- Benefit: Enables network administrators to bypass Microsoft GINA but at the same time achieve the same on the LAN like experience for their end users that GINA provides (such as log in script execution, domain SSO, and file drive mapping)
  - Availability : SA 1000 and above with SAMNC license, SA 700
- Microsoft signed NC driver for Win 32 bit Win XP and Win Vista platforms
  - Enables network administrator to configure a policy to allow only Microsoft signed applications to be installed in the end user machines
  - Benefit: Tighter control on which applications or drivers get installed by the end users on company issued machines
  - Availability: SA 1000 and above with SAMNC license, SA 700