

Juniper-SSL VPN FAQ

- What is the Juniper portal and how is it different from previous VPN solutions?
 - The Juniper portal does allow for a “full VPN” connection like our previous solutions, but it also replaces portals for Citrix and Outlook Web Access. This solution allows more flexibility and greater security for our remote connections. We can also offer more applications via the browser without needing a VPN connection to the network.
- What is an SSL VPN?
 - Traditional remote VPN connections use connection types that vary widely. Secure Sockets Layer (SSL) is the same technology used in your browser that encrypts your communication with web sites (HTTPS). Because the SSL VPN client uses the same port as secure web pages, it is more likely to be allowed through firewalls at remote locations.
- Will our old VPN connections continue to be available?
 - During the rollout of the Juniper solution the old VPN will be available, but there will be a cutoff date and this will be communicated to you by your local support team.
- Can I use my personal computer to connect to the Andritz network?
 - You will be able to use your personal computer to connect to basic portal services (Outlook Web Access, SPAM Quarantine, and other lower security resources). However, in order to use a full VPN (shown in the portal as Network Connect), your PC will be checked to see if its security software is installed, up-to-date and that the computer is a member of the Andritz group. If the connecting PC fails any of these checks it will not be allowed to use a full VPN connection.
 - It should be noted that this is in compliance with the published Andritz IT Security Policies. These policies are available on the Intranet. Contact your local support team if you have trouble locating them.
- What is Host Checker?
 - The checks mentioned in the question regarding personal computers connecting to the VPN are handled by a software component called Host Checker. This component checks your PC to determine if it meets the requirements to allow access to higher security resources.
- Can my mobile device connect with VPN?
 - Andritz IT understands many mobile devices offer convenience, but the Andritz security policies do restrict remote connectivity to the network to devices issued by the company. This is best handled with a company laptop.
 - Personal mobile devices **will not be allowed** to use full VPN connections.
- How do I install the Juniper software?
 - By connecting to one of the portals (<http://www.andritz.com/webaccess>) and logging in, the software will be automatically installed. In the case of Network Connect (full VPN), it will only be installed if the connecting PC passes the security checks.
- I already have Juniper software installed to allow connections to a customer/vendor, will I still be able to use it?
 - If their portal is using a different version of the software, they should still work independently and without conflict.
- What is “strong authentication” and why is it necessary?
 - Strong authentication (also called two-factor authentication) takes the traditional process of supplying a user name and password a step further by adding a one-time password to the authentication (login) process.
 - Using only a user name and password is a bad security practice because there are many ways for someone to acquire this information. Once they have it, they

would have easy access to the corporate network. Strong authentication helps to assure that the connecting party is actually who they say they are.

- I need to give an external contractor access to the network. Is this still possible?
 - It is, but you must contact your local support to make arrangements for access to the internal resources required for their task.
- Will I still have access to local network printers/servers while I am connected to the VPN?
 - The standard configuration will allow this by default.
- How long can I stay connected to the VPN?
 - The standard session limit is 24 hours. This is necessary because of limited concurrent use licenses on the gateways.
 - If you sign in via the portal page to Network Connect, the time left in your session is displayed at the top of the portal page.
- What do I do if the portal I use is unavailable?
 - All of the portals offer the same services, but the one that is geographically closest will have the best performance. If a portal you normally use is not working, select one of the others from <http://www.andritz.com/webaccess>.
- How many days out of date can the antivirus software be before I am denied access to Network Connect?
 - If your virus definitions are older than 8 days, you will not be able to use Network Connect. You will need to update the antivirus program to use Network Connect.
 - If you will be traveling, try to remember to run a manual update before leaving the office. Contact your local support for assistance/instructions for this. If you will be traveling for an extended period, assure that you run an update before disconnecting each day.
- How do I disconnect from the VPN?
 - You can either right click the Network Connect icon in the system tray and select "Sign Out" or click the Sign Out link in the portal page.