FORSCHUNGSZENTRUM JÜLICH GmbH

Jülich Supercomputing Centre
D-52425 Jülich, Tel. (02461) 61-6402

Network Service Desk, Tel. (02461) 61-6440

Technical Information

FZJ-JSC-TKI-0418
Dr. F. Mohr, JSC

07.07.2025

Necessary measures for operating systems in end-of-support status

Information for system administrators

1. Introduction

As of January 14, 2020, Microsoft discontinued technical support and software updates for Windows 7, ending the product life cycle of this operating system [(1)]

This far-reaching change in the range of available operating systems serves as an occasion to point out the general handling of operating systems that have reached the end of their product maintenance (end-of-support). The respective platform (Windows, Linux, Mac OS etc.) is irrelevant, the considerations correspond.

In accordance with IT basic protection rule H3[(2)(3)], operating systems with the end-of-support status may not be operated on the JuNet, since necessary security-relevant updates are no longer available. Explicitly, this applies to the usage in virtual machines and in NAT (Network Address Translation) or PAT (Port and Address Translation) environments, also.

All administrators of systems in JuNet with outdated operating systems should immediately upgrade to a new supported version. If there are compelling reasons against such a changeover, the systems concerned must be notified to the IT security officer via the responsible IT officer, immediately.

2. Migration to current operating systems - feasible or not?

If there are no compelling reasons to continue using outdated software and/or hardware in such a way that otherwise relevant functionalities were lost, the migration to an up-to-date version of the operating system must be carried out. Obstacles could be experimental environments for which no software updates are available. Outdated hardware alone is no reason to continue operating, as long as the required applications are also available under supported versions of newer hard- and software.

If the continued operation of outdated operating systems is absolutely necessary, JSC will take measures to design solutions to protect these systems and other JuNet participants, as stipulated in the IT security guideline[4]. These measures are described below.

3. Continued operation of systems in the end-of-support status

3.1. The JuRassic network

Operating systems with end-of-support status may only be operated with a connection to the JuNet after they have been moved by JSC to a highly restricted *JuRassic* network set up for this purpose. The following communication rules apply to this network:

- JuRassic ➔ public network: Not possible.
- Public network ➔ JuRassic: Not possible.
- JuRassic ➔ JuNet: Only DHCP, DNS, NTP, SMTP to the central mail relay and SSL communication to the central enterprise anti-virus software operated by JSC possible.
- JuNet ➔ JuRassic: Possible with the exception of the SMB protocol, see below.

According to this, JuRassic systems cannot access the JuNet, only the services DHCP, DNS, NTP and SMTP as well as anti-virus updates are provided. However, JuNet participants can access JuRassic systems, for example to set up VNC sessions or initiate FTP transmissions. Data transfers via SMB protocol (Server Message Block, e.g. NetBIOS or Samba shares) are generally not possible.

A private IP address according to RFC 1918 is assigned to the system for further operation in JuRassic; the previous host ID and all DNS aliases are retained in order to facilitate the assignment of the institute.

3.2. Requirements for participation in JuRassic

As already described in the introduction, end devices for the JuRassic network must be reported to the IT security officer via the IT officer. Devices to be moved to JuRassic must meet two requirements:

1) Migration to an operating system that is still supported is not possible, see section 2.
2) The system does NOT share the network connection with other participants who are to remain in their previous network (e.g. via desktop switches).

If condition 1) is violated, an upgrade to a current operating system must be carried out or the end device replaced. If you have any questions, please contact your IT officer or PC service provider.

If condition 2) is not met, the system can only be moved to JuRassic for technical reasons as soon as the conflict e.g. was remedied by a re-wiring measure. If you have any questions in this

area, contact the network Service Desk at JSC (Tel. 6440). After placing a cabling order[5] the actual cabling of the end device into JuRassic will be carried out at short notice.

Since the systems in JuRassic are still potentially vulnerable, a firewall is urgently recommended; operating a current virus scanner is also mandatory in JuRassic.

3.3. Configuration of the JuRassic participants

As administrator of an end device in the JuRassic network, please adapt your system configuration to the communication relationships described in section **3.1**. At this point, as experiences have shown, some settings should be mentioned as examples, which often lead to problems or unnecessary data traffic and should therefore be improved:

• *WINS*: The JSC WINS server (134.94.80.84) cannot be reached by JuRassic participants. Therefore, remove it from the IP configuration.

• *DNS server*: The correct DNS servers are 134.94.32.3, 134.94.32.4 and 134.94.32.5. Remove all other DNS servers (both internal and external) from the IP configuration.

• *Public network*: The Internet is generally not accessible from JuRassic. You should therefore prevent all communication on ports 80 and 443.

• *Windows Update*: Since the public network is not accessible, Windows Update cannot access the corresponding Microsoft servers. Any Microsoft updates (MS Office etc.) must be applied in another way, so deactivate the Windows Update service.

• *Anti-virus*: Only the central anti-virus servers in JuNet can be reached from JuRassic, no http servers in the public network are reachable.

• *TeamViewer*: Please note that participants in the JuRassic network cannot establish TeamViewer connections to other networks.

With these adjustments, you make a noticeable contribution to relieving the data traffic in the JuRassic network, the JuNet administration therefore asks for attention.

4. Closing word

In the event that devices with an operating system that is no longer supported continue to operate outside of JuRassic, JSC reserves the right to block them immediately in order to maintain basic protection in JuNet for all participants. It is also not permitted to operate other interfaces in other networks on systems in JuRassic.

Systems without any network connection are not considered by this document. There is no objection to their continued operation as long as they are not connected to the JuNet or to the global Internet.

5. Documents

(1) End of support for various Windows versions:
https://support.microsoft.com/en-us/windows/what-does-it-mean-if-windows-isn-t-supported-08f3b92d-7539-671e-1452-2e71cdad18b5

(2) IT security rules for baseline protection:
go.fzj.de/grundschutz_englisch

(3) Collective internal framework agreement I+C Systems:
go.fzj.de/iuk_englisch

(4) IT Security Directive of Forschungszentrum Jülich:
go.fzj.de/sicherheitsrichtlinie_englisch

(5) JSC cabling order system [german]:
go.fzj.de/kabelauftrag