Orange
Cyberdefense

Flexible Applications Access
Remote working, simply and securely

With secure remote access your office can be anywhere!

Working outside of the company

Access the Information System (IS) securely, from home or while traveling, with any device

Keep working in a crisis situation

Temporary open remote access to the IS, to deal with travel restrictions, natural disasters, etc.

Collaborate with partners

Allow them safe access to the resources they require for remote maintenance or application development
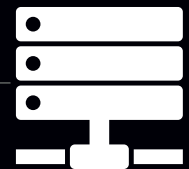
Simple secure access to your Information Systems

Remote workers & partners

Orange Cyberdefense

Flexible Applications Access

On-site

Network Data Storage

Cloud

- Flexible Applications Access is an SSL VPN gateway that allows easy and secure remote access to the information system.
- Users are authenticated, and access only authorized data with their computer, tablet or smartphone.

Benefits

Ease of use
Users access with their AD credentials, and use their usual office software

Real-time online management
Updates of user access rights, add and remove users as needed, usage statistics

No restrictions
Independent of your intranet and internet providers, works with any type of internet connection: 5G, 4G, Wi-Fi, etc.

Security
Encrypted transactions and access limited to authorized data and users

Customized to your needs
Virtual Machine or physical deployment in your public cloud, in our data centers, or on premises, customized access rights, etc.

Two user experiences

Flexible Applications Access allows either full access to the information system as if the user were at the office, or restricted access to certain resources through a web portal.

Full access

This access requires a VPN connection software on the user's equipment, which creates an encrypted SSL VPN tunnel between the user and Flexible Applications Access. The user logs in with their credentials and accesses their work environment as if they were in the office.

The user's equipment can be checked: OS version, presence of up-to-date anti-virus, etc. Access to the information system is then authorized or denied depending on the result of the check.

A Split Tunneling feature is also offered, allowing traffic to transit according to its destination. Normally any traffic is automatically redirected to the SSL VPN tunnel. Thanks to this functionality, it will or will not be redirected to the tunnel depending on its criticality. For example, traffic to the Internet will not go through the SSL VPN tunnel, but traffic to business applications or the intranet will go through it.

Restricted access

This access does not require any prior software installation on the user's equipment. The user connects to the web portal with their credentials and accesses the applications to which they are entitled. The transaction between Flexible Applications Access and the user is encrypted in https.

This access allows restricted access to resources according to the user's profile. In particular, it is via this web portal that partners can access only the applications intended for them.