WEBCONNECT

Browser based Remote Desktop White Paper

The future of remote workplaces

Content

1 Editorial

We bring the future to you. No matter where you are.

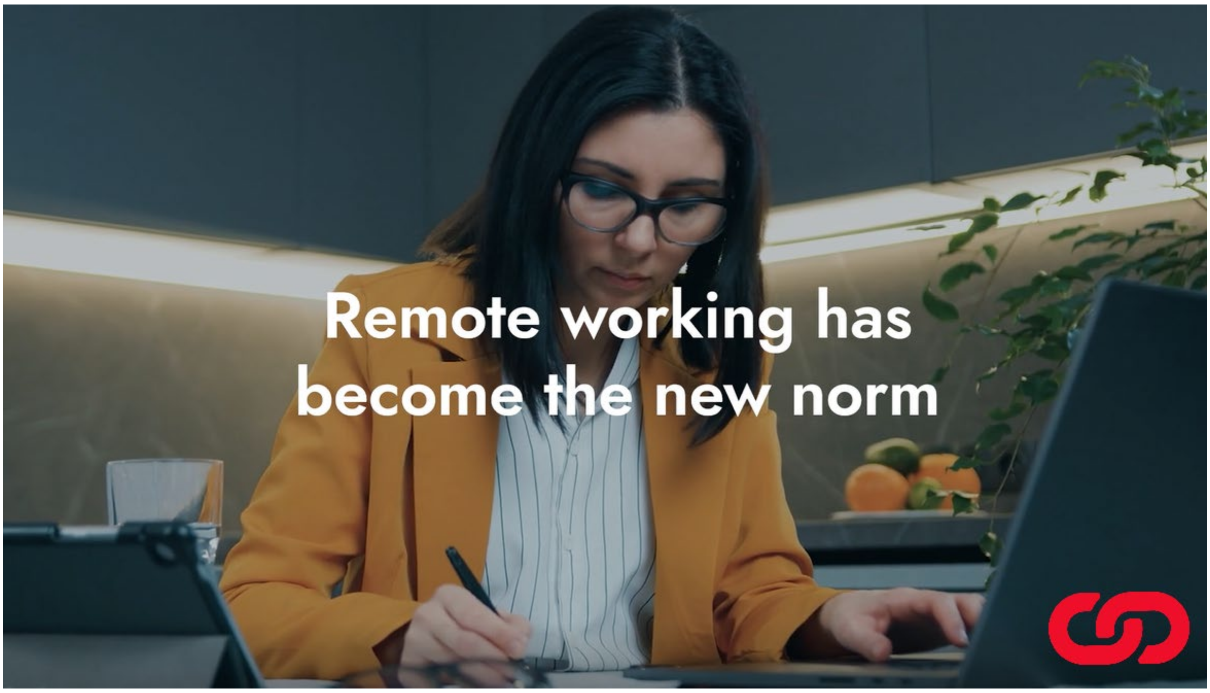
Ideas that revolutionise the world of work are born in the heart of Madrid. Founded by CEO Saber Maram, we specialise in privacy, security and communication. We develop our own products and advise clients on R&D.

"The true luxury in life is a short commute. We help people to improve their quality of life and companies to become more sustainable and flexible."

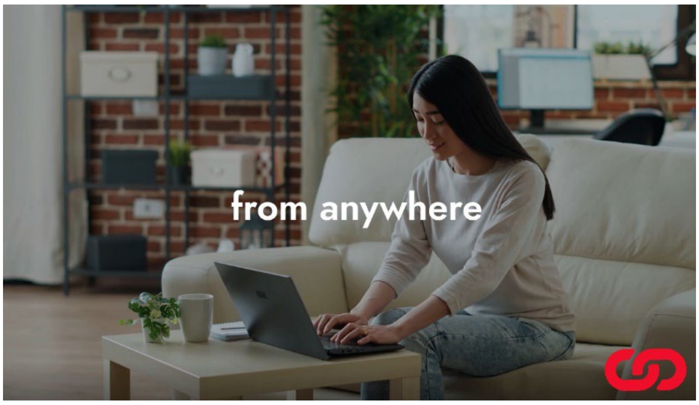
Saber Maram, CEO WebConnect World SL

2 Management summary

Home office and flexible remote working have become part of everyday life in companies. To ensure a secure connection to the company network, companies usually rely on an encrypted VPN tunnel (Virtual Private Network). But with a large workforce, the VPN quickly becomes overloaded and slows down business operations. In addition, the configuration and permanent monitoring of VPN connections in the company can be very time-consuming for administrators.

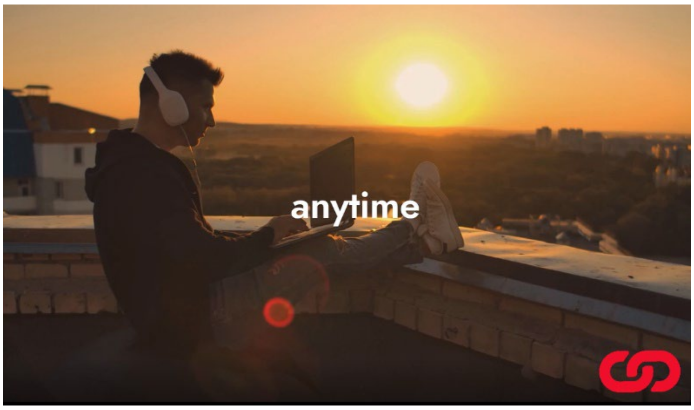


This is where WebConnect comes in with a novel concept for secure remote access to desktops and dialling into the company network. WebConnect does not use a VPN, but still achieves high security with high performance. For this purpose, WebConnect establishes all connections directly between client and remote device via the browser as a tunnel with https encryption. The solution uses one SSL certificate per device via https and Secure Websocket with encryption via TLS 1.3. A similar methodology is also used in banking.



Thanks to WebConnect, employees can even access any real or virtual PC in the office network as well as connected printers, scanners, card readers or webcams with their smartphone via the browser. Additional software installations and cumbersome VPN setup are now a thing of the past. WebConnect offers a wide range of settings with which companies can refine their security requirements as well as role-rights concepts and assign access rights individually or on a group basis.

WebConnect also offers functions such as Web Meet for optimised collaboration in video conferences (collaboration mode). Here, participants can share mouse and keyboard, edit documents and access the whiteboard during the RDP session. As host, WebConnect ensures the secure connection of the video conference and thus the necessary data protection.



A shared (Shared Drive) or personal (WebConnect Drive) private cloud directory for the secure storage of data as an alternative to external cloud storage is very useful - the latter now also with automated synchronisation via WebConnect with all devices used. WebConnect also allows documents stored on the remote PC to be printed directly on the local printer or documents to be sent from home to the office printer and printed there.

WebConnect is available in two variants: WebConnect Plug & Play and WebConnect Enterprise. WebConnect Plug & Play works via the already configured WebConnect Box (hardware), which is simply connected to the network, and is optimised for up to 20 simultaneous remote connections. WebConnect Enterprise is designed for more than 20 simultaneous connections and is therefore very suitable for large networks and cloud applications. With this version, the WebConnect software is installed in the network on a virtual machine (VM) with the Linux operating system.

WEBCONNECT
www.webconnect.pro
Working with remote desktop as if you were directly at the workplace

3 Work remotely

3.1 Home office and remote work - a challenge for security and administration

The Corona pandemic has put the world in a state of emergency and has also massively changed the way we work. Home office and flexible working are now part of normal business life. Before Corona, working from home was reserved for a small group of people or allowed in exceptional cases. But flexible working is not only important in times of crisis, but also in normal everyday business. Employees want to access company applications and data or participate in video conferences from home or on the move. Another requirement is a remote desktop connection with direct access to the computer located in the office - even from a smartphone. The goal is for every employee to be able to carry out his or her activities via the internet and thus independent of location.

What does this mean for the IT department? It has to provide network capacity for all employees and ensure security and data protection. The latter can be a major challenge. Because often the workstations set up in the home office are not secured to the same extent as the computers in the office. Due to the large number of digital applications, data accesses and end devices, there are also more sources of danger for security leaks. IT should therefore bring all devices together under a uniform management interface and use tools to manage the end devices, software and users, to encrypt the data or for secure backups.

In addition to pure technical security, it is important to define binding compliance and governance so that employees also adhere to the necessary rules and do not use data outside the secure environments. The zero-trust principle is recommended here according to the principle: "Do not trust any software and also no employee and only grant those rights that a solution and an employee need to complete their tasks.

To ensure a secure connection to the company network, companies usually rely on an encrypted VPN tunnel (Virtual Private Network). But with a large workforce, the VPN can quickly become overloaded and slow down business operations.

3.2 VPN - connection with weaknesses

In principle, the operation of a VPN is very simple. You use encryption to create a small network within a large network that is only accessible with the appropriate addresses and passwords. This means that only authorised users can communicate with each other. A VPN thus creates a kind of monitored private line within the internet. It connects computers or networks with each other by using other networks as a transport route. For this purpose, it is usually necessary to install and set up a VPN client on the computer.

All data and requests that the client sends to the Internet are first routed to the VPN server, encrypted and only then sent on to the web. The encryption takes place in real time and prevents external interference. The data that is sent back is also first received by the server, encrypted and then sent to the client. The VPN client then decrypts it again. This procedure is also called tunneling, as the data to be protected flows through a tunnel. Basically, the IP address of the client is disguised and that of the VPN server is displayed instead - the target servers can thus not track or log the true source of the request.

However, the use of VPN is not infrequently associated with undesirable side effects. The capacity of the VPN gateways in the companies is often limited and rarely designed to connect all employees, but only a part of the workforce. Due to the high load, access becomes slow, cumbersome or breaks down completely at times. Internet speed also depends, for example, on the type of encryption and the distance of the client from the VPN server. Let's face it: no employee wants to wait a long time for applications or websites to load. Another problem: If the VPN connection or the VPN service fails completely and a new dial-up is required, the encryption also fails for this period. This reveals the real IP address and the employee is no longer anonymous on the Internet.

In order to reduce VPN data traffic, some companies subsequently switch to split-tunnelling, for example. In this case, only those connections are routed through the VPN tunnel that have systems at the other end of the VPN tunnel as destinations. For all other connections, the VPN tunnel is ignored. This reduces the data volume at the central VPN endpoint in the company, but the security level decreases.

In addition, the configuration and permanent monitoring of VPN connections in the company can be very time-consuming for administrators. You must always keep an eye on the bandwidth used by the VPN as well as the integrity of your WAN and network. It's a matter of monitoring all VPN connections, identifying bandwidth problems and adding additional capacity as needed so that users don't experience any problems.

The users themselves are also challenged. They must secure their home network and their home office device with an endpoint protection solution. Because the best VPN is of no use if the end device at an employee's home is infected. The attacker then more or less already has access to the company network.

3.3 Secure solution: WebConnect

But there are good alternatives to VPN. One of them is WebConnect, a solution for secure remote access to desktops and dialling into the company network. The special feature: WebConnect establishes all connections directly between client and remote device as a tunnel with https encryption - all via the browser and without installation on the client. There are no third-party servers or nodes along the way. No device can be reached directly, the connection is established via user name and password. In addition, 2-factor authentication is standard with WebConnect. A user name and password must also be used on the target device. The solution thus ensures data protection and security.

WebConnect does not use a VPN, but still achieves high security with high performance. To achieve this, the solution uses one SSL certificate per device via https and Secure Websocket with encryption via TLS 1.3. A similar methodology is also used in banking. An SSL certificate is a small data file that digitally binds a cryptographic key to an organisation's details. When installed on a web server, it activates the security lock as well as the https protocol and enables secure connections from a web server to a browser. WebSocket, as an efficient, bidirectional transmission protocol, enables modern web applications to act much faster than traditional HTTP communication.

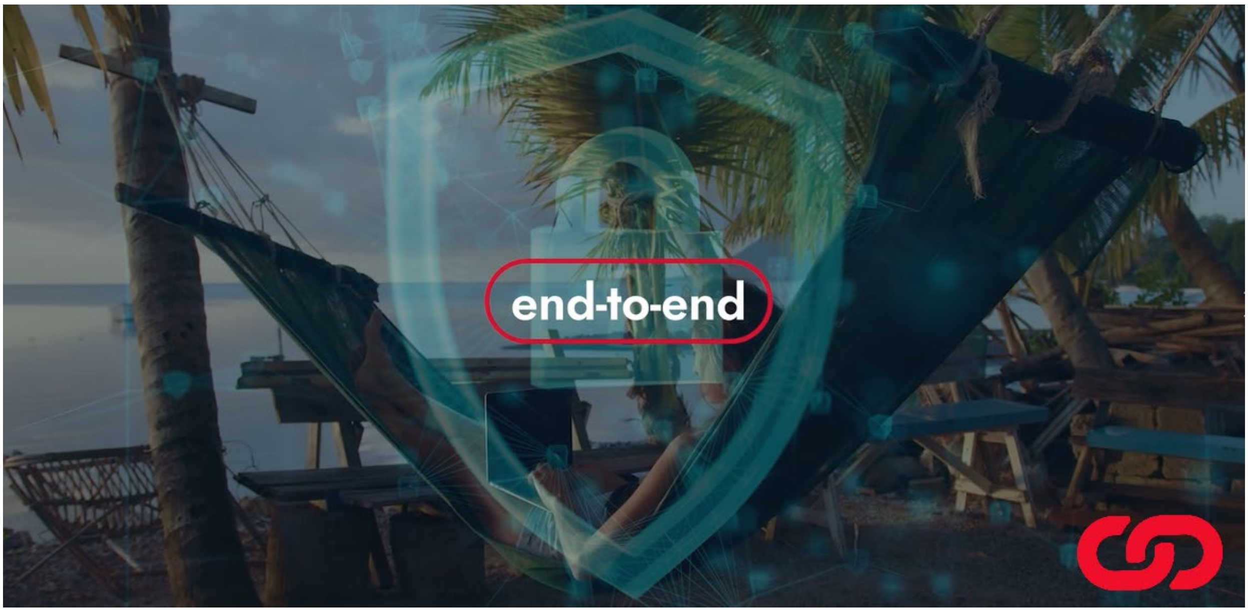
WebConnect offers a wide range of settings with which companies can individually refine their security requirements and role-rights concepts. Administrators are thus able to assign appropriate access rights or time restrictions to individual users, user groups and connection profiles on the same device, as well as adjust them at any time.

4 Why WebConnect?

4.1 For companies

As a **secure and simple alternative to VPN,** WebConnect is the ideal solution for freelancers as well as companies.

- With WebConnect any connection in the browser
- WebConnect works everywhere where internet is available



- WebConnect is fully compliant with the GDPR:
    - WebConnect has no central customer and device management
    - All access data is located exclusively within the respective installation
    - All data are the sole property of the client
- Productive user experience on any browser-enabled device
- Get started immediately without client installation
- No additional software for VPN or RDP management necessary
- Secure remote access without VPN (username and password, 2FA, direct tunnel between client and remote device, fail2ban)
- Flexibility: Work independent of time and place
- Shared RDP connections for simultaneous work on common projects
- RDP sessions with up to 60 FPS e.g. for video editing
- Private cloud directory in the WebConnect installation
- Advantages for administrators
    - Simple configuration and administration
    - Unlimited simultaneous connections
    - Simple assignment of access rights
- Lower costs due to reduced set-up and administration effort

4.2 For data centres and cloud providers

WebConnect offers a novel concept for remote working **- remote desktop in the browser**: Cloud service providers can provide their customers with RDP access - quickly and easily via the browser, accessible worldwide without VPN.

- WebConnect works in any cloud
- Encrypted: SSL certificate (HTTPS), Secure Websocket via HTTPS, additional protection by TLS 1.3
- MFA (multi-factor authentication): Access authentication with password and 2FA app
- The multifaceted role-rights concept supports a zero-trust security architecture
- Session time-out functionality in case of inactivity
- Fail-to-Ban
- Zero Knowledge - 100% Data Protection
- No third party server or node

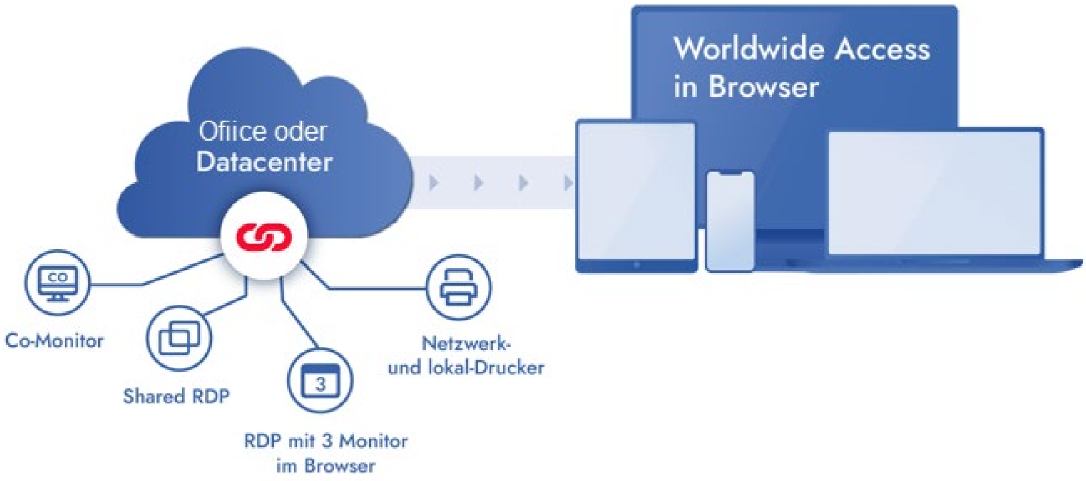
5 How WebConnect works

WebConnect is always installed in the customer's network. As a gateway solution, it establishes the connection between the user and the remote device. For security and privacy reasons, no user or connection data is stored on WebConnect servers. WebConnect is always an "**on-premise**" installation.

All user access data and all connection data are encrypted and stored only in this installation. At no time does WebConnect itself gain knowledge of this data or have access to it.

The WebConnect Gateway is the only connection between the remote devices and the users who want to access these devices. A direct HTTPS connection is established between the WebConnect Gateway and the user. Only the WebConnect Gateway itself then establishes a connection to the remote device with the desired protocol (RDP, VNC, SSH, Telnet or Kubernetes).

Most remote providers work with central connection servers. Here they advertise end-to-end encryption, but the key holder is always the provider. WebConnect never owns the customer's keys. The HTTPS connection is established directly between the WebConnect gateway installed at the customer's and the user's browser. Only these two devices know the key. The connection does not run via WebConnect servers, but directly.



WebConnect enables services in the RDP connection that are otherwise only possible in a direct RDP connection. This enables functions such as direct printing, multiple monitors, shared RDP connections and video transmissions up to 60 FPS.

With WebConnect, no VPN is necessary. This makes it much easier for users to use. VPNs are often complex to administer and there are many use cases where VPN connections cannot be established because the necessary ports are blocked (hotels, conference rooms, etc.). Since WebConnect connects via HTTPS, only the corresponding HTTPS port is necessary, which is freely available almost everywhere.

Since no client installations are necessary for the basic functions of WebConnect, a public PC can also be used at any time for work that is necessary at short notice. The connection is also established from there in the browser and leaves no data behind. Nothing is saved on the local device, as work is done exclusively on the remote device.

With WebConnect, both distributed working from anywhere in the world and distributed working within modern office environments are possible. If the basic workstations are set up in the data centre of the office building, it is possible to work with any end device from any place in the office with the WebConnect installation.

Fixed workplaces are a thing of the past. Remote is now everywhere. Teams work together flexibly, whether in the conference room or in the open air - workplaces are where it is most effective for the users and the work.

With WebConnect, no applications and no data need to be stored locally. Everything remains exclusively and securely in the company. Work only takes place in the company, without the user having to be present on site. With WebConnect, the flexibilisation of the working world has arrived in the company.

All this without large investments in networks, in VPN, in infrastructure. WebConnect is simply connected to the internal network - and every device is automatically a flexible "remote workstation". With WebConnect, every company goes to the cloud without having to invest in cloud infrastructure. The branch office acts directly as a cloud and all data remains in the company.

6 WebConnect functionality

WebConnect is remote working in the browser. Everything takes place in the browser. This means that WebConnect can be used without client installation from any browser-capable end device, regardless of the operating system.

The extensive functions are listed in the appendix Function List. Here we show some features by way of example.

6.1 The most important functions of WebConnect

6.1.1 Protocols

WebConnect supports the following protocols directly in the browser:

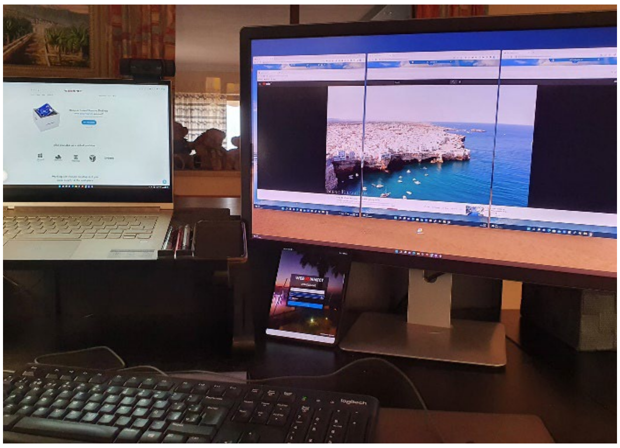
RDP, VNC, SSH, Telnet, Kubernetes.

6.1.2 Shared Monitor RDP with several participants

Simultaneous work on joint projects with any number of users and special attention to the protection of important data. Thanks to WebConnect, it is possible to share documents via shared RDP connections in one's own network without access to third-party systems. All participants can work equally on the screen and thus create and optimise documents together.

Shared Monitor also provides Llinks for guests who only have visitor rights. These guests can follow the RDP session but cannot interact themselves.

6.1.3 Multi-Monitor and Co-Monitor



WebConnect supports up to three monitors in browser tabs. Each monitor is in its own browser tab, which can be positioned and moved as desired. As with "real" monitors, elements can be moved from one tab to the next.

With Co-Monitor it is possible for users to log in with the same account on 2 devices. On the second device, a "Co-Monitor" button is offered for active connections. This button opens the RDP connection as an identical copy. This allows all applications to be operated equally on both devices. This function can be used, for example, to work on a PC or MacBook and to use a tablet for simple signing of documents.

6.1.4 Multi-connection

Up to 6 simultaneous connections can be opened in one browser. The connections are displayed as thumbnails in the footer area of the browser. By clicking on them, it is possible to conveniently switch between the connections. With this function, several devices can be easily and effectively controlled and monitored at the same time. This function is ideal for administrative work.

6.1.5 Shared drive with file manager

Shared-Drive is a common folder for all users of a WebConnect installation. It is located within the installation and can be accessed from any location as a logged-in user. Users can conveniently exchange data in the shared drive, as each user has equal access to these files. This means that public cloud directories are no longer necessary for the exchange of files. A modern file manager is available as a file manager.

6.1.6 Private drive with file manager

In addition to the shared drive, a private drive is also offered. Only the logged-in user has access to this directory. Administrators cannot view this directory either. Users can store data they need remotely in the private drive. The comfortable file manager is also available for administration in the private drive. The private drive is comparable to a private cloud directory, but unlike cloud services, it does not use third-party servers. All files always remain under the control and ownership of the user.

6.1.7 Print remotely

WebConnect allows you to print documents in PDF as standard. In addition, WebConnect has developed an add-on that makes it possible to directly address all local and network printers with all settings and to remotely print any document directly. This can be the shared printer in the hotel or at a conference, as well as the network printer in the office if you want to make printed documents available to colleagues.

The WebConnect add-on is available as a service for Windows and for MacOS.

6.1.8 Webcam and microphone

As WebConnect connects directly to the workplace, video calls can be made conveniently from home via the pre-installed company application. The solution supports webcams and microphones connected to the local device. There are no restrictions on specific webcam models or resolutions. The audio signal of the remote device is also transmitted without restriction.

6.1.9 SmartCard Forwarding

There is often a requirement to authenticate oneself for certain programmes or services via smart card. An example in Germany is the beA service as an electronic lawyer's mailbox. The WebConnect add-on, which also enables remote printing, also provides a function that allows SmartCard readers to be used on the local device and thus to verify oneself on the remote workstation. All data is transferred directly as if you were working on site.

6.1.10 Wake-on-LAN

Energy-efficient working is an important topic for reducing operating costs and being environmentally conscious. WebConnect supports Wake-on-LAN. This makes it possible to simply switch off remote devices or send them into power-saving mode when they are not needed. If the user now needs to access these devices to start certain programmes or to access data, Wake-on-LAN can be used to send a wake-up signal to the remote device.

6.1.11 Mobile apps

Of course, WebConnect also works in a mobile browser. However, in order to accommodate the limited screen size, WebConnect has developed apps for iOS and Android that dispense with disruptive browser elements. WebConnect mobile apps are optimised for mobile devices with iOS and Android operating systems.

6.1.12 Philips SpeechMike support

For employees who dictate a lot and use speech recognition software in their daily work, WebConnect enables limitless mobility. When they connect Philips SpeechMike to their local device, they can dictate from anywhere to their remote device. The files are then immediately available to the speech recognition software for further processing.

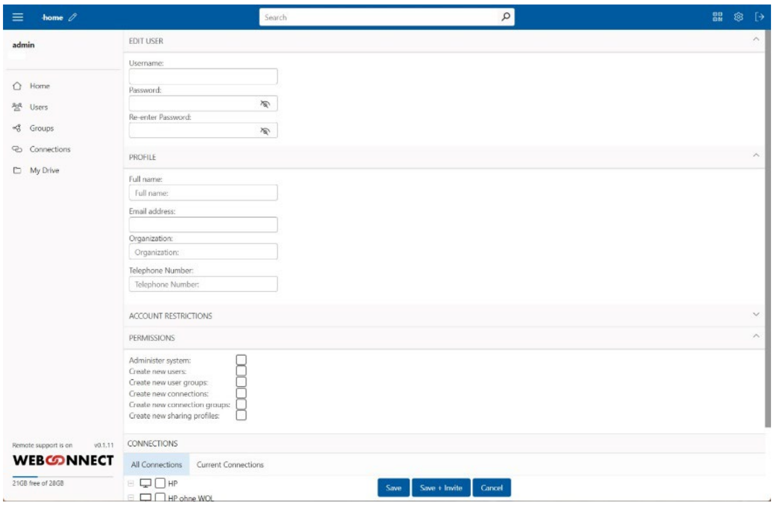
6.1.13 RDP sessions with video editing

With frame rates between 60 and (frames per second) with minimal delay, WebConnect sets new standards for streaming video files. This allows graphic designers, industrial designers and other employees to remotely access their high-performance process computers and the programmes installed on them and work together on their projects.

6.1.14 User administration

WebConnect comes with a user and group administration for assigning different rights. Here, it can be defined which user is allowed to access which devices or is allowed to see them at all. Usage times can be defined to support working time models, and authorisations can be assigned to create new connections or manage other users.

All user data is stored exclusively in the local application. There is no central WebConnect user database. This decentralised user management of all WebConnect installations increases security for customers, as there are no centralised opportunities for attack.



EDIT USER

Username:

Password:

Re-enter Password:

PROFILE

Full name:

Email address:

Organization:

Telephone Number:

ACCOUNT RESTRICTIONS

PERMISSIONS

Administer system: □
Create new users: □
Create new user groups: □
Create new connections: □
Create new connection groups: □
Create new sharing profiles: □

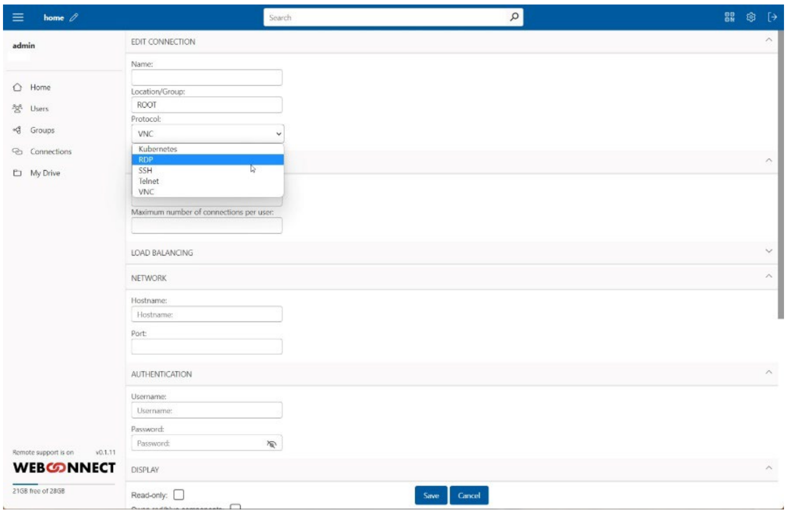
CONNECTIONS

All Connections | Current Connections

□ HP
□ HP ohne WOL

6.1.15 Connection management

All units are created in the WebConnect connection management. Different profiles can also be created for the same devices in order to adjust the settings for special usage situations. It is already possible to store the access data for the device in the connection profiles. However, it is safer to request these only during the connection, as this establishes another security level that is supported by WebConnect.



EDIT CONNECTION

Name:

Location/Group: ROOT

Protocol: VNC

Maximum number of connections per user:

LOAD BALANCING

NETWORK

Hostname:

Port:

AUTHENTICATION

Username:

Password:

DISPLAY

Read-only: □

6.2 Functions planned for Q4 2022

6.2.1 Shared Drive with online/offline synchronisation

Dropbox, Microsoft One Drive or Google Drive, everyone knows these and other services and uses them privately or professionally. All these services are located on the providers' servers and it is not clear what happens to the data. As a rule, the user does not even know the geographical storage location. Accounts can be arbitrarily blocked from one day to the next, data can be accessed without authorisation. The AI of large companies analyses the data for possible violations of the terms and conditions. In addition, there is the danger of targeted hacker attacks against these providers.

WebConnect's new online/offline synchronisation moves the cloud to the user's own network. Data is held offline on user-approved devices and synchronised when the respective devices are online on the network. All data is stored in a DVSGO-compliant manner and can be managed securely under the user's own control according to the strict requirements of some professional groups, such as doctors, lawyers or tax consultants.

The new WebConnect shared drive will be the secure storage space of the future, where users regain sovereignty over their data.

6.2.2 WebMeet video meeting with whiteboard and chat

WebMeet is a separate video meeting server in the WebConnect installation. Since all video connections, chats and whiteboard work take place exclusively peer2peer, there are no servers in the middle that manage or process data. The video meetings are therefore DSGVO-compliant.

WebMeet is optimised for up to 6 participants in one conversation. All users of the WebConnect installation can communicate with each other.

With WebMeet, invitation links can be sent to external participants (customers, patients, clients, etc.), who then also communicate in a secure direct connection.

With WebMeet and a shared RDP connection, effective and professional collaboration is possible in an absolutely secure environment. The technologies used prevent eavesdropping and recording by unauthorised persons.

In text chat, it is possible to exchange texts in the group or between individual participants during collaboration.

6.2.3 USB forwarding in the RDP session in the browser

WebConnect forwards all USB devices from the local workstation to the remote RDP session. Already printers, WebCams and SmardCard readers are supported by WebConnect in the remote RDP session. With the upcoming general USB forwarding, the USB connection will be completely forwarded into the work session. This means that the connected device no longer plays a role.

7 WebConnect: Function overview

7.1 The most important functions at a glance

- **Everything in the browser**: Access from any browser-enabled device - get started immediately without client installation
- **Wake-on-LAN**: Activate switched-off desktops remotely
- **Video optimised**: Transfer rate 60 frames per second (FPS)
- **Remote USB**: Use all USB devices from anywhere
- **Protocols**: RDP, VNC, SSH, Telnet, Kubernetes
- **Security**: 2-factor authentication & https encryption
- **Shared RDP connections**: Team work on one screen
- **Shared Drive**: The alternative to external cloud storage
- **Online / offline synchronisation (**4th quarter 2022)
- **WebMeet (**4th quarter 2022)
- **Optimised for mobile devices**: Apps for Android & iOS

7.2 The protocols supported in the browser

- RDP
- VNC
- SSH
- TelNet
- Kubernetes

7.3 Security and data protection

- Zero Trust Policy
- No central database (zero knowledge - no data with the operator)
- All user data encrypted in the customer installation
- Login directly in the installation
- Username and password
- 2FA (optional)
- Fail to Ban
- Additional login in the connection
    - Depending on the unit configuration:
    - Username and password
    - SmartCard (optional)
    - 2FA (optional)
- Peer to Peer (direct connection to the installation without third-party providers)
- Encryption: Secure websocket on https, TLS 1.3
- Secure remote access: secure unattended access

7.4 User and connection management

- Create unlimited user accounts
- Number of simultaneous users depending on the selected tariff
- Data avoidance through a minimum of necessary data for the operation of WebConnect
- Creation of user groups with defined users and devices
- Access rights to manage different levels of access
- Assign devices to specific users.
- Access restrictions with date and time
- Make 2FA mandatory for all users
- Define in the connection that users must also legitimise themselves there by user name and password.
- Create unlimited connections
- Password expired: Function to force user to set a new password
- Backup: Export and import of users, groups, connections and other settings
- E-mail invitation for new users (optional)
- Notes page for administrators
- Connection history
- Storage space adjustment in VM installations
- Ethernet port detection in VM installations

7.5 Properties

- Everything in the browser (no installation of transmitter or receiver software)
- Streaming up to 60FPS with RDP in the browser
- Cross Platform Access
- Wake On Lan (waking up, restarting devices)
- Up to 6 simultaneous connections in the browser with easy switching via tiles
- Shared drive incl. file manager
- Special keyboard shortcuts for applications in Windows RDP from MacOS or Windows
- Private Drive (Networkdrive with WebDAV)
- Settings for Keyboard Setup
- Remote audio
- USB forwarding in the RDP session in the browser (4th quarter 2022)

7.6 View

- Fullscreen mode in every connection
- Screen resize: screen automatically adjusts to the browser size
- Multi-monitor in RDP with up to 3 simultaneous screens in browser tabs
- Dark and Light Theme
- Individual wallpaper
- CO monitor

7.7 Cooperation

- Shared RDP connections with equal cooperation
- Read-only mode in shared RDP connections
- Shared drive incl. file manager
- Shared Drive with online/offline synchronisation (4th quarter 2022)
- WebMeet video meeting up to 6 people in one session (4th quarter 2022)
- WebMeet text chat (4th quarter 2022)
- WebMeet whiteboard (4th quarter 2022)

7.8 Periphery

- Printer redirect in browser RDP for local and network printers
- SmartCard redirect in browser RDP (e.g. for remote login to the electronic lawyer's mailbox bEA)
- Support for Philip- Speechmike in the browser RDP
- Redirecting WebCam and Audio in Browser RDP

7.9 Mobile app

- Optional iOS and Android Apps
- QR code in WebConnect for easy setup of the iOS and Android app

8 Comparison matrix

	Webconnect	Anydesk	Teamviewer	Microsoft Browser RDP	Microsoft RDP with VPN
Performance / Price					
Frame rate	up to 60 fps	up to 60 fps	up to 60 fps	up to 60 fps	up to 60 fps
Price	10 EUR p.m.	from 9.90 EUR p.m.	from 298.80 EUR p.a.	-	-
Browser-based Remote Desktop	Yes	No	No	Yes	No
Features					
Activity Dashboard	Yes	No	No	No	No
API	Yes	Yes	Yes	No	No
App	Yes	Yes	Yes	No	Yes, requires two apps
Share Screen / Shared Screen	Yes	Yes	Yes	No	No
Requires client software	No	Yes	Yes	No	Yes, requires two apps
Drag & Drop	Yes	No	Yes	No	Yes
File sharing (direct)	Yes	Yes	Yes	No	Yes
File sharing (offline/online sync aka OneDrive)	Yes	No	No	No	Yes
Generic USB redirection	Yes	No	No	No	Yes
Integration Active Directory (LDAP)	Yes	No	No	Yes	Yes
No third-party server / "man in the middle	Yes	No	No	No	Yes
Local user database	Yes	No	No	No	Yes
Comments/Notes	Yes	No	No	No	No
Customised branding	Yes	Yes	Yes	No	No
Live chat	Yes	No	Yes	No	No
MFA (Multi Factor Authentication)	Yes	No	Yes	No	No
Mobile access	Yes	Yes	Yes	Yes	Yes
User management	Yes	No	No	Yes	Yes
Personalisation	Yes	No	Yes	No	No
Presentation streaming	Yes	No	Yes	No	No
Remote printer as PDF	Yes	Yes	Yes	No	Yes
Remote printing on local printer	Yes	No	No	No	Yes
Remote access/control	Yes	Yes	Yes	Yes	Yes
Secure login	Yes	No	No	Yes	Yes
Unattended access	Yes	Yes	Yes	Yes	Yes
Video conferencing	Yes	No	Yes	No	No
Switching between multiple monitors	Yes	Yes	Yes	No	Yes
Simultaneous access to multiple monitors	Yes	No	No	No	Yes
Access controls / permissions	Yes	Yes	Yes	Yes	Yes
Wake on Lan	Yes (direct)	Yes (2t device required)	Yes (2t device required)	No	No
Multiple sessions in one session	Yes	Yes	Yes	No	No
Fail-to-Ban	Yes	No	No	No	Yes
Group management	Yes	No	No	No	Yes
Live Display Update Resize	Yes	No	No	Yes	No
Real RDP (Native Remote Desktop)	Yes	No	No	Yes	Yes
Smart Card Redirection	Yes	No	No	No	Yes
Phillips Speech Mike Redirection	Yes	No	No	No	Yes
Self Administered	Yes	Yes	Yes	No	No

9 Security

Secure and simple alternative to VPN: WebConnect offers a novel concept for remote working **-** a similar methodology to banking.

9.1 Connection & Encryption

- No third party server or node
- WebConnect functions as an application gateway
- Secure HTTPS encryption (tap-proof protocol that transmits encrypted data between browser and WebConnect in both directions)
- SSL Certificate (HTTPS) / Secure Web Socket over HTTPS
- Key length SSL: RSA 2048
- Additional protection through TLS 1.3 (Transport Layer Security)

9.2 Authentication

- MFA (Multi-Factor Authentication): Access authentication with password and 2FA app
- Authentication at the target device with username and password
- All user data is stored exclusively and encrypted in the WebConnect installation (no central access database on WebConnect servers)
- Lock with staggered time intervals in case of multiple false logins (Fail to Ban)

9.3 Data Protection & Compliance

- Zero knowledge / 100% data protection: no data at the manufacturer, all data in the possession of the customer
- Product installed at the customer
- Security by Design
- DSGVO-compliant, as all user data is stored exclusively with the user.

9.4 Network security

- Hiding access through port forwarding. Only WebConnect is accessible with the public IP of the network.
- Higher availability than with VPN. WebConnect uses port 443 (HTTPS) to establish the connection, which is the only port open in many networks (e.g. airports, conference centres).
- No need to open additional firewall ports other than 443 or port forwarding.
- The multifaceted role-rights concept supports a zero-trust security architecture
- Session time-out functionality in case of inactivity

10 Webconnect: Licensing

WebConnect is available in two variants: WebConnect Plug & Play and WebConnect Enterprise.

10.1 WebConnect Plug&Play

The plug-and-play solution works via the already configured WebConnect co-router (hardware), which is simply connected to the network. All companies need to access their desktops is a web browser and the WebConnect co-router in the network. All that is usually required for operation is port forwarding of port 443 (HTTPS) to the WebConnect co-router on the network. WebConnect automatically controls all security rules. With the WebConnect co-router, it is not necessary to set up a complex VPN to reach devices from outside.

This is because only the WebConnect co-router is accessible with the public IP of the network, all other network devices are further hidden behind internal IP addresses and are not directly accessible. As a kind of gateway, the WebConnect co-router allows simple and secure access from outside, regardless of the operating system and device. Even mobile devices, which are usually difficult to integrate into the VPN, are standard with WebConnect.

WebConnect Plug&Play is optimised for up to 20 simultaneous remote connections.

10.2 WebConnect Enterprise

The enterprise solution is designed for more than 20 simultaneous connections and is therefore very suitable for large networks and cloud applications. With this version, the WebConnect software is installed in the network on a virtual machine (VM) with the Linux operating system (VM). The VM is set up within the remote network and is therefore - like the WebConnect co-router - the only device visible via a public IP address. All other remote devices with internal IP addresses remain invisible for access without WebConnect. WebConnect Enterprise can be installed within a local network as a VM, for example on an existing NAS (e.g. Synology). In the cloud in the data centre, companies should select a small VM for this.

The installation of the Enterprise solution is somewhat more complex than that of the Plug&Play solution, but significantly easier than setting up a VPN with all its problems. The Enterprise solution has the same range of functions as the Plug&Play version, but is also designed for large teams accessing the remote network simultaneously.

11 Resources

Website: https://webconnect.pro

Brand Guidelines: https://webconnect.pro/wp-content/uploads/2022/08/Brand_Guidelines_V3.pdf

Help centre: https://webconnect.pro/de/hilfezentrum/

12 About WebConnect

WebConnect World SL, based in Madrid, specialises in data protection, security and communication. The company develops its own products and advises customers in the area of research & development. The central product is WebConnect for flexible and secure working from anywhere in the world. The solution offers a novel concept for secure remote access to desktops and dial-in to the company network - as a secure and simple alternative to VPN. WebConnect is distributed through resellers and various partner programmes. For more information, please visit https://webconnect.pro/de/.

Attachments

WebConnect brings data centre to Azure level

WebConnect RDP in the browser or RDP with VPN

Switching on external devices with Wake-on-LAN

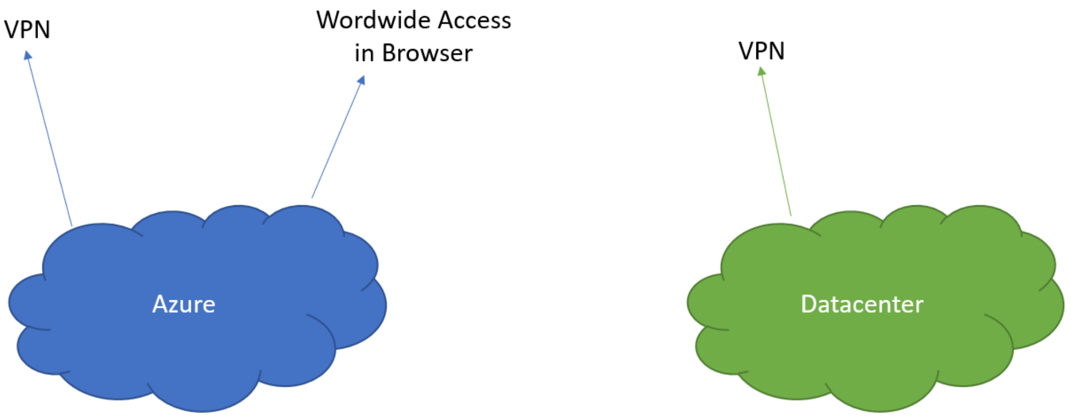
Manage remote access securely

WebConnect and / or other IT solutions

WebConnect brings data centre to Azure level

Working remotely from anywhere is the challenge of today. Data centres have faced up to this situation and are offering ever more comprehensive office solutions in the cloud. This also includes Microsoft's entire office software portfolio. Microsoft has therefore also recognised the potential of this market and is now competing with other data centre providers for customers.

Why does Microsoft Azure have an advantage here?



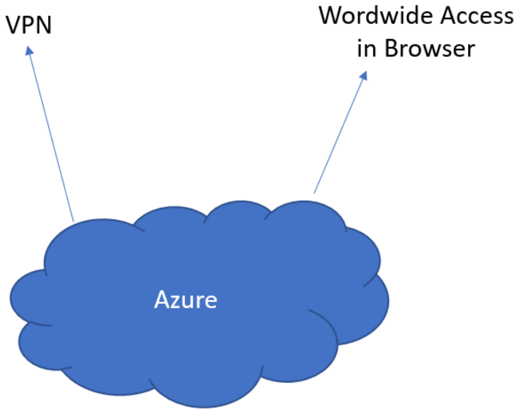
The difference is in the last mile, in the way applications are accessed to create the best working environment for the user. Data centres can offer Office, Teams, SharePoints and other solutions just like Microsoft, but Microsoft does not license the simple comfortable browser access to the RDP of the remote computer. Microsoft markets this exclusively in the Azure Cloud and thus creates the decisive market advantage for itself.

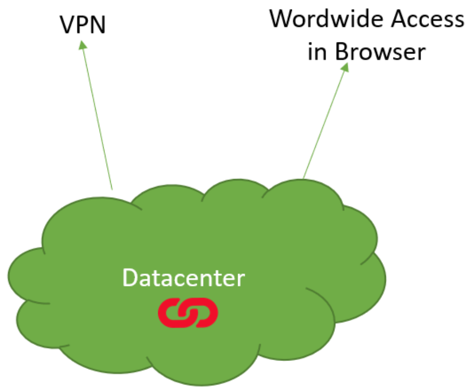
	Datacenter	Azure
Office, Teams, SharePoint	✓	✓
VPN	✓	✓
RDP in the browser	X	✓

Customers want it to be simple. They want to access the company network from anywhere and with any device, and they want a perfect screen experience when working. Data centres can't offer that. They have to set up access via VPN. However, this is support-prone and always requires administrators to set it up and manage it. Microsoft Azure offers access via browser from anywhere with any device.

Turn any data centre into an Azure competitor with WebConnect

This is where WebConnect comes in. WebConnect offers data centres exactly this missing last mile with features that make the data centre more powerful than Azure.





WebConnect is installed as software in the customer's cloud and forms the gateway between the customer and the cloud. The customer can operate his cloud computers via browser. The connection is established via HTTPS directly between the customer and the cloud (peer-to-peer), the RDP connection is established via WebConnect.

	Datacenter	Azure
Office, Teams, SharePoint	✓	✓
VPN	✓	✓
RDP in the browser	✓	✓

WebConnect supports every workstation with a browser and offers mobile apps with optimised screens for smartphones and tablets. Simple device management and extensive customer and rights management round off the product.

Lifting the data centre from Azure with WebConnect

With WebConnect, all access data is stored exclusively in the local customer installation; with Azure, it is stored in the central Microsoft database.

All of the customer's data and applications reside in the data centre they trust, whereas with Azure, the data is all in the hands of a multinational company based in the US.

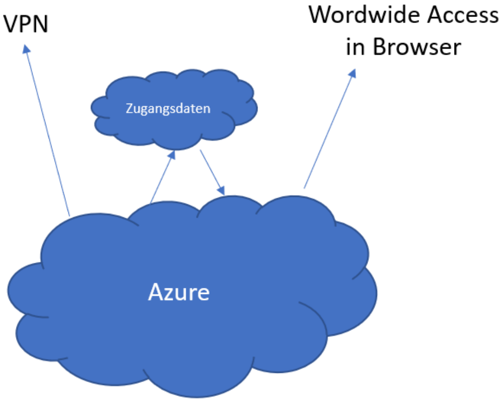
While WebConnect with multiple installations stores and backs up access and device data decentrally, with Azure the access data is always in the central Microsoft database.

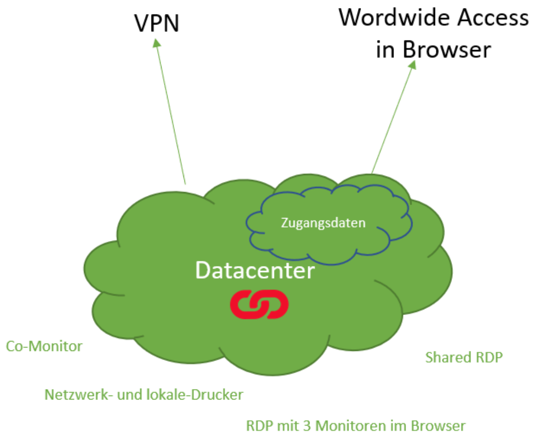
With WebConnect, access is secured with username and password, with 2FA and with Fail to Ban. Zero trust is the basic principle for all users.

With WebConnect, any RDP connection can be extended to up to 3 monitors in browser tabs.

WebConnect directly controls all local and network printers and takes over all existing printer settings.

With WebConnect, the user can display and operate his RDP connection on a second device (co-monitor), for example for digital signatures via tablet while editing documents on the PC.




VPN
Wordwide Access in Browser
Zugangsdaten
Datacenter
Co-Monitor
Shared RDP
Netzwerk- und lokale-Drucker
RDP mit 3 Monitoren im Browser

With WebConnect, the user can invite other users to his RDP session (Shared-RDP) and all users can work together on the RDP screen in the browser

With WebConnect, the user can invite other users into his RDP session as mere spectators and show them presentations or just let them watch the work.

	Datacenter	Azure
Access data.	Local	Cloud
Customer data and applications	Local	Cloud
Access data in decentralised installations	Decentralised	Cloud
Username, Password, 2FA, Fail to Ban	✓✓✓✓	✓✓✓ X
RDP with 3 monitors in browser tabs	✓	X
Network and local printers in the browser RDP	✓	X
Co-Monitor - RDP on 2nd device	✓	X
Shared-RDP - RDP with multiple users	✓	X
Share RDP in the browser as a view with users	✓	X

WebConnect and Datacenter - the real alternative to Microsoft Azuree

WebConnect World SL

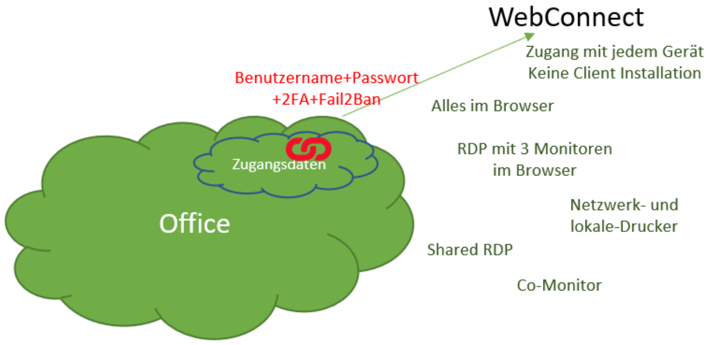
WebConnect World SL, based in Madrid, specialises in data protection, security and communication. The company develops its own products and advises customers in the area of research & development. The central product is WebConnect for flexible and secure working from anywhere in the world. The solution offers a novel concept for secure remote access to desktops and dial-in to the company network - as a secure and simple alternative to VPN. WebConnect is distributed through resellers and various partner programmes. For more information, please visit https://webconnect.pro/de/.

WebConnect RDP in the browser or RDP with VPN

- What is the difference between the two solutions?
- How should you decide as a company?
- What are the advantages for the employees?
- Are both solutions safe?

WebConnect RDP in the browser

WebConnect offers RDP in the browser on any end device. The connection is made directly via HTTPS and TLS 1.3 from the remote workstation to the WebConnect installation. Port 443 (HTTPS) is required for this. Depending on the network configuration, port forwarding to port 443 of the WebConnect installation must be set up on the router.



WebConnect does not require client software.

Since the remote workstation does not become part of the remote network, it is easier to secure it against malware and unwanted access.

WebConnect always adjusts the RDP desktop to the browser window. There is no need to manually set screen sizes, regardless of whether work is to be done on the tablet or a 4K monitor.

WebConnect does not require a physical monitor at the remote workstation. It automatically creates up to 3 simultaneous virtual monitors that are displayed simultaneously in 3 browser tabs for working. Elements can be moved between the screens.

With WebConnect, the employee is completely location-independent, as he or she can work via browser and HTTPS wherever the internet is available.

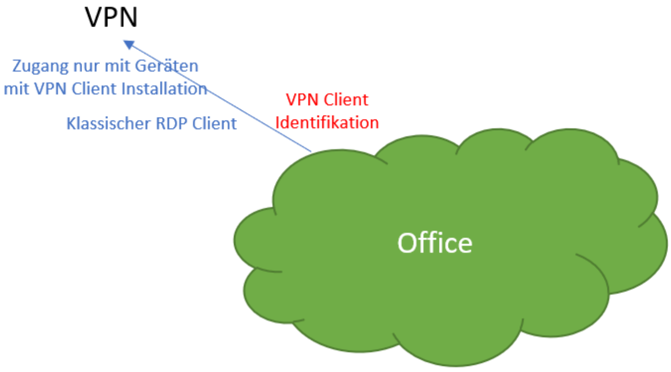
WebConnect is easy to administer.

RDP with VPN

VPN requires a VPN installation on the client and in the company, which establishes a tunnel between the devices for each connection.

With VPN, RDP is established via the classic RDP client.

The remote workplace becomes an integral part of the company network with all the risks that arise on the remote workplace (viruses, malware, etc.).


VPN
Zugang nur mit Geräten mit VPN Client Installation
Klassischer RDP Client
VPN Client Identifikation
Office

The classic RDP client does not automatically adjust to the screen of the remote workstation when the size changes.

Setting up a VPN in the company and on the client devices is time-consuming and requires constant control and maintenance.

VPN only works where the corresponding outgoing ports are freely available. This is not the case in many hotels, airports, train stations, conference centres and many other places, or it has to be requested and set up separately.

WebConnect World SL

WebConnect World SL, based in Madrid, specialises in data protection, security and communication. The company develops its own products and advises customers in the area of research & development. The central product is WebConnect for flexible and secure working from anywhere in the world. The solution offers a novel concept for secure remote access to desktops and dial-in to the company network - as a secure and simple alternative to VPN. WebConnect is distributed through resellers and various partner programmes. For more information, please visit https://webconnect.pro/de/.

Switch on external devices with Wake-on-LAN

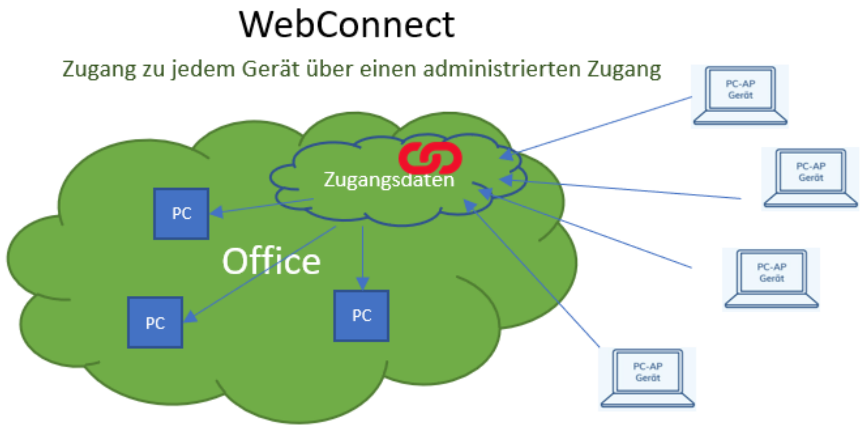
The challenge for organisations with remote workplaces today is to be as energy-efficient as possible and, for example, to switch off unused resources.

There are solutions for this in the IT network, such as Wake-on-LAN. With Wake-on-LAN it is possible to switch on switched-off devices within a network. To do this, it is necessary for these devices to receive a so-called magic packet from another device, which is sent directly to the network card and, if configured accordingly, starts the device.

The advantage of such a configuration: devices only consume energy when they are actually in use. There is no longer any reason to leave devices switched on around the clock in order to reach them occasionally from outside.

Wake-on-LAN with WebConnect

WebConnect is optimally prepared for Wake-on-LAN as it offers the sending of the Magic Packet directly in the connection. When WebConnect is installed in the network, it is the only device that must be accessible online. With a consumption of only 8 watts, it is the most efficient device in the network.

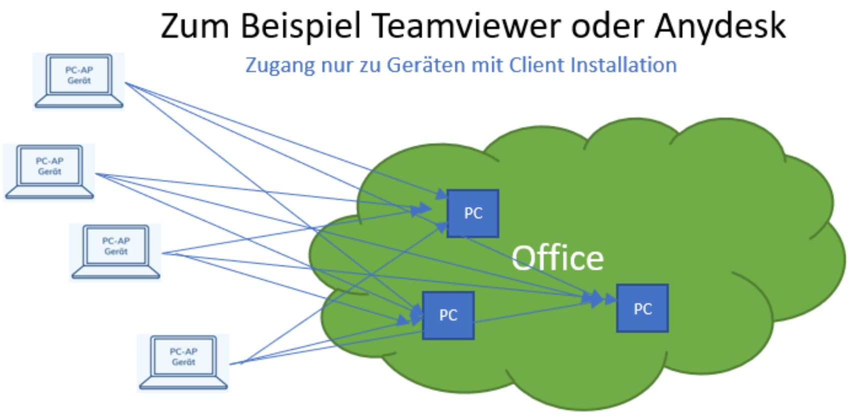


All workstations can be in power-saving mode or switched off. With WebConnect, the user always connects to the local installation, which switches on a workstation directly when the connection is started. Once the user has finished his or her work, the device is simply switched off again.

Since WebConnect does not require any installations on the sending or receiving device, there are also no dependencies here. The user only needs usage rights to the devices he is allowed to use.

Wake-on-LAN with Teamviewer, Anydesk and other solutions

With solutions of this type, there is no central unit within the organisation's IT network. One installation is required on the local and one on the remote workstation. Since Magic Packets can only be sent within the network, it is necessary that at least one device with an installation is active and accessible in the network.


Zum Beispiel Teamviewer oder Anydesk
Zugang nur zu Geräten mit Client Installation
PC-AP Gerät
PC-AP Gerät
PC-AP Gerät
PC-AP Gerät
PC
PC
PC
Office

These applications must then send the signal to the desired workstation. The whole thing must therefore be set up in such a way that the installation first finds an active device, gives it the command to send the signal and then establishes the connection to the desired device.

There is a lot to be considered here in terms of configuration and rights management.

If not a single device remains switched on, the entire network cannot be reached.

WebConnect World SL

WebConnect World SL, based in Madrid, specialises in data protection, security and communication. The company develops its own products and advises customers in the area of research & development. The central product is WebConnect for flexible and secure working from anywhere in the world. The solution offers a novel concept for secure remote access to desktops and dial-in to the company network - as a secure and simple alternative to VPN. WebConnect is distributed through resellers and various partner programmes. For more information, please visit https://webconnect.pro/de/.

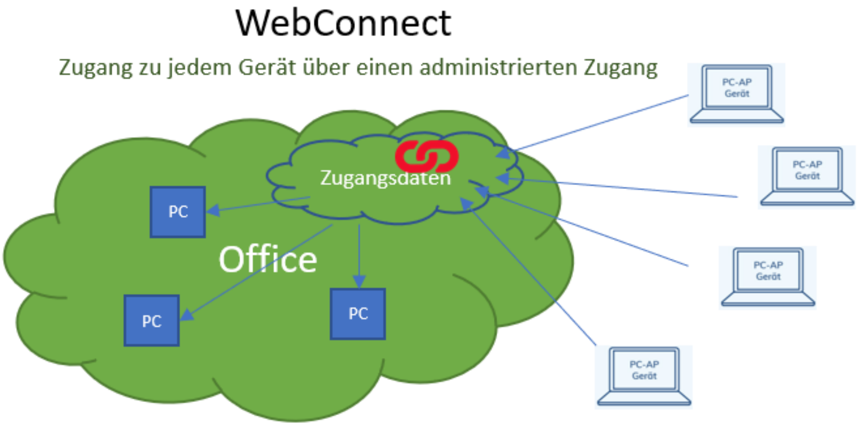
Manage remote access securely

Even in the internal network, it is necessary to bind the rights of users to services and devices. With the expansion of the organisation from the physical premises into the remote working world, the challenges for administration increase further.

The systems and data of an organisation are a valuable and sensitive asset. It is necessary to protect them as best as possible from unauthorised access.

Manage remote access with WebConnect

WebConnect runs as a central access system for all accesses from outside and inside who want to use the remote browser sessions. WebConnect offers a comprehensive user and connection administration in which each user is set up with his or her rights and in which each user is assigned exactly the connections he or she is allowed to use.

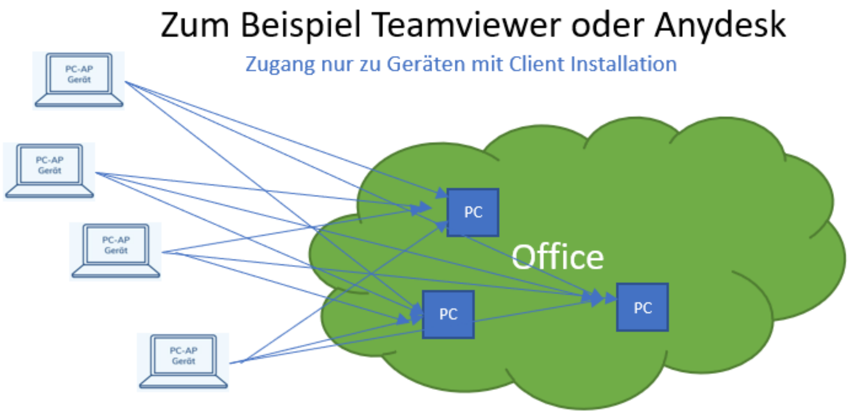


Every user must first log on to the WebConnect installation before he can access his devices on the network. They must also log on to their device (depending on the configuration). There are thus sufficient hurdles before a device can be accessed. Important: All these settings are under the constant control of the administrators, who can change or remove any authorisation at any time. In addition, the administrators can see who is and was currently connected where.

No user outside the network can see any internal device without logging into WebConnect. These are hidden behind WebConnect and never public.

Remote access with Teamviewer, Anydesk and similar solutions

With systems like Teamviewer, the system is structured differently. Each device requires software that assigns it a number and a password. The number always remains the same and is registered in the central server of the software provider with the corresponding target address. Anyone who knows this number can reach the internal target device without any registration or legitimisation. Only on the target device is a password entered, which is either set in the local software or by a random password that is passed on to the remote user by a user within the organisation. Alternatively, a user in the internal network can also click directly on "Allow access".



Zum Beispiel Teamviewer oder Anydesk

Zugang nur zu Geräten mit Client Installation

If software such as Teamviewer, Anydesk or similar is installed in the internal network, the administrator loses further control over this device and can no longer trace its actions in the network. He hands it over to the sovereignty of the respective employee, who can give any person access to this device and thus the network at any time.

Since the structure of the numbers is known, external parties can also try to reach devices and bypass the respective password. This opens doors that were previously laboriously closed with firewalls and the like.

WebConnect World SL

WebConnect World SL, based in Madrid, specialises in data protection, security and communication. The company develops its own products and advises customers in the area of research & development. The central product is WebConnect for flexible and secure working from anywhere in the world. The solution offers a novel concept for secure remote access to desktops and dial-in to the company network - as a secure and simple alternative to VPN. WebConnect is distributed through resellers and various partner programmes. For more information, please visit https://webconnect.pro/de/.

WebConnect and / or other IT solutions

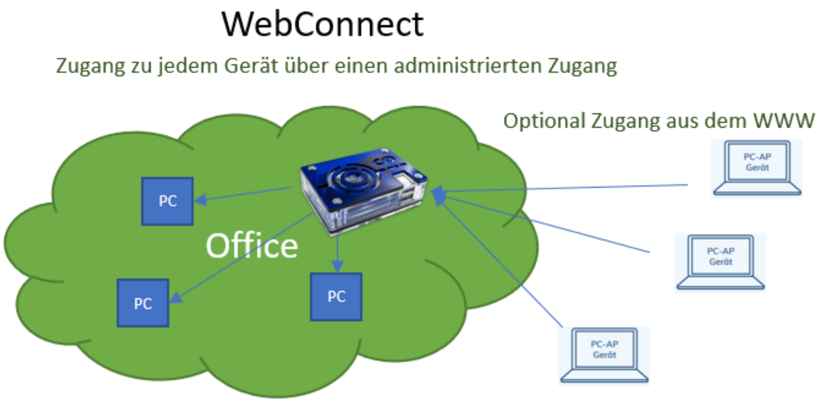
A fundamental decision that IT decision-makers often face in IT projects: Which project do we realise? Do we replace system A with system B? If we want to use B, however, we have to part with A. Wouldn't it be better to keep A and do without B?

WebConnect helps with this decision crossroads. Since the solution connects IT worlds, an **'or'** becomes an **'and'**. This allows companies to maintain existing investments and gently supplement resources with new investments.

WebConnect and internal network

Workplaces of the future are remote. But remote does not only mean outside the physical premises of an organisation. Remote simply means spatially flexible. Larger units today have a campus, smaller ones have always had a terrace. Work should take place where employees feel comfortable.

WebConnect not only works from outside via the internet, but also on the internal network. And if the organisation's IT policy requires it, WebConnect can even be restricted to purely internal use.


WebConnect
Zugang zu jedem Gerät über einen administrierten Zugang
Optional Zugang aus dem WWW
PC
Office
PC
PC
PC-AP Gerät
PC-AP Gerät
PC-AP Gerät

WebConnect is an add-on that makes workplaces mobile. The usual IT infrastructure in companies often consists of desktop PCs that are tied to a fixed workstation. However, most of these desktop PCs can also be set up so that they can be reached via RDP. However, most companies are reluctant to do this because setting up regulated and secure access options is very time-consuming.

WebConnect provides a remedy here. Installation in the internal network is simple and the solution is above all easy to manage. Each authorised user is given access with a user name, password and optionally 2FA. These users are then assigned exactly those workstations that they are also allowed to access in normal operation.

From this point on, the employee has maximum flexibility. They can simply go to their workplace via WebConnect in the browser with any device. This can be with a tablet from the terrace or the campus, with a Chromebook from the meeting room or with a laptop from the current location. It is even possible to bring your own workstation onto the screen of another desktop PC.

WebConnect turns static networks into flexible modern working environments without high investments in the conversion of the existing and proven IT infrastructure.

WebConnect and Cloud

Consultants often recommend migrating to the cloud for flexibility and remote working. But if all applications are moved to the cloud, the existing hardware is consigned to electronic waste. Cloud and internal network are often competitors that do not get along.

Alternative approaches are much more cost-effective. WebConnect transforms the internal network into a private cloud and conserves resources. WebConnect in the cloud extends this with attractive functions that standard cloud installations do not offer. Both can be combined in the working environment.

WebConnect and Citrix

Normally one would think: WebConnect or Citrix? However, WebConnect can also complement existing Citrix systems and expand them in a meaningful way.

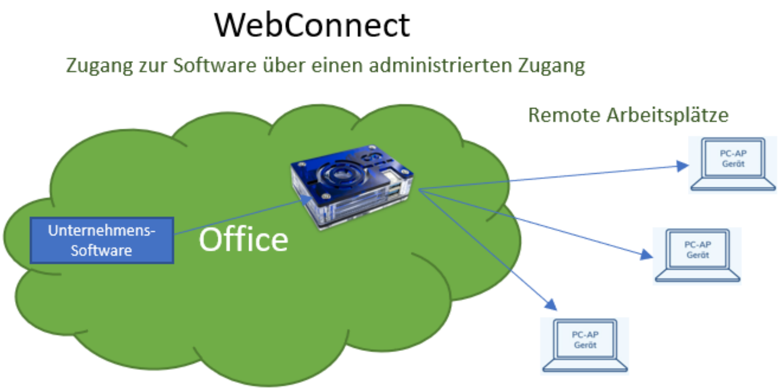
With WebConnect, additional devices can be used in the system within a Citrix infrastructure, which are then not subject to the Citrix licence module. This makes it possible to integrate temporary workstations in particular at low cost.

WebConnect and in-house software solutions

Many organisations have highly specialised enterprise software in place that has been developed and customised over many years. Unfortunately, most of these software solutions only run within a closed network. They cannot be used in the cloud or on the web. This poses challenges for IT managers when they want to offer remote workplaces.

With WebConnect, no changes to the existing solution are necessary. As WebConnect is installed in the internal IT system, it transforms the home system into a private and protected cloud accessible from anywhere in the world.

WebConnect forms the gateway between the World Wide Web and the house system and thus at the same time the secure boundary between indoors and outdoors.



External users only see the WebConnect gateway and connect with a browser with HTTPS and TLS 1.3 (banking standard). Here they legitimise themselves with user name, password and 2FA. Only the WebConnect gateway knows the devices that are to be accessible. Only between the gateway and the internal device is the remote connection established, which is then displayed and operated in the browser via HTTPS.

As the external devices do not become part of the internal network with WebConnect connections, it is better protected against viruses or malware. Another advantage is that users can use their own preferred hardware and do not have to be equipped with secure hardware from the organisation.

With WebConnect, any desktop application previously only available locally can be operated in the browser from anywhere in the world without the software itself running outside the organisation. The application always runs locally, only the screen is transmitted and operated in the browser with HTTPS.

WebConnect World SL

WebConnect World SL, based in Madrid, specialises in data protection, security and communication. The company develops its own products and advises customers in the area of research & development. The central product is WebConnect for flexible and secure working from anywhere in the world. The solution offers a novel concept for secure remote access to desktops and dial-in to the company network - as a secure and simple alternative to VPN. WebConnect is distributed through resellers and various partner programmes. For more information, please visit https://webconnect.pro/de/.

Licences and prices

WebConnect is offered as a plug&play version including hardware (co-router) and as a software image for installation on server hardware.

Installation price:

Plug&Play	
Co-Router (MiniPC optimised for up to 20 simultaneous users)	150 Euro
Purchase price for resellers 100 euros	
Installation help optional for end customers	50 Euro
Server installation: (Hyper-V, Proxmox, Virtualbox, VMware, Synology)	
Software download (image with installation file)	free of charge

The WebConnect licence model is based on simultaneously active users. The customer can freely choose the desired maximum number of simultaneous connections and adjust it at any time.

Licence price:

Per simultaneous user (connection) per month	10 Euro

Resellers receive a 50% discount on the licence price

Large customers such as data centres or organisations receive attractive graduated and flat-rate prices.

All prices plus VAT at the current rate.

WebConnect World SL

WebConnect World SL, based in Madrid, specialises in data protection, security and communication. The company develops its own products and advises customers in the area of research & development. The central product is WebConnect for flexible and secure working from anywhere in the world. The solution offers a novel concept for secure remote access to desktops and dial-in to the company network - as a secure and simple alternative to VPN. WebConnect is distributed through resellers and various partner programmes. For more information, please visit https://webconnect.pro/de/.