cRSP
common Remote Service Platform

Technical Information

SIEMENS

common Remote Service Platform

The common Remote Service Platform (cRSP) provides a highly scalable and secure remote access infrastructure for fast, efficient and first-class remote service delivery. Predefined application templates ensure simple workflows for remote experts. After the initial setup, an authorized remote expert can establish a remote connection to the connected devices through secure VPN tunnel via a software client or IPsec router.

…but cRSP is more then just remote access!

The platform combines reactive remote service, Integrated M2M (proxy), file transfer, e-mail, SMS and file backup services. cRSP is ISO/IEC 27001 certified, complies with the latest security standards (IEC 62443, NIS 2) and focuses on remote access to IP-protocol-based industrial devices (Siemens and non-Siemens).

Security and Scalability are main Competences of cRSP

Key features of cRSP

Security Standards

- Privileged Access Management (PAM) as principle
- Data Centers ISO/IEC 27001 certified
- Development processes according to IEC 62443-4-1

Simple workflows

- Predefined application templates
- Various applications such as SSH, RDP, VNC,…
- Multiple file transfer mechanisms

Secure connection

- Software client-based VPN connectivity (SSL VPN)
- IPsec router-based VPN connectivity (IPsec VPN)
- Integration of customer's remote access VPN solutions

Highly scalable

- No limitations of number of users, systems & connections
- Remote connections to any type of IP-based devices
- Manufacturer independence

Centralized platform

- Centralized user and access management
- All connections are routed and terminated in cRSP DMZ (demilitarized zone)

Worldwide support

- cRSP Helpdesk is available 24/7/365
- Consulting & support during implementation and operation phase

SIEMENS

cRSP supports each of your use cases!

Remote Diagnosis
Diagnose problems or disruptions quickly and efficiently (assess system functionality, prepare error/problem correction)

Remote repair
Restore functionality, fix bugs,
adjust configurations, system reset

Maintenance support
Preparation of and support during maintenance, installation of updates and patches, health check

Remote commissioning
Remote support during installation and commissioning of systems, configuration adjustment, drawing of visualizations

Operational support
Support customers (or a technician on site) with system operation, panel mirroring, guided assistance

Data file transfer Northbound
System data and config backups, log files, application data for diagnostic and monitoring

Reporting
Integrated Data Warehouse and reporting portal with pre-defined on-demand reports for billing usage analytics. Multiple In-App reports for logs and events.

Date file transfer Southbound
Windows and Linux OS updates, Antivirus Software and patterns, firmware and config files

Automated data backup
Proxy solutions for system data backup to Intranet or Internet targets

System integration
REST interface for horizontal integration (e.g., iBase, Works), proxy solutions for integrations with backend applications (e.g., SPM, Navigator, GMA Manager)

Automated SW distribution
Multiple proxy solutions and managed device authorization groups for file distribution from targets in the Intranet or the Internet

Messaging
Integrated SMTP server for system event and status notifications (e.g., Apogee, Control Point), cRSP system notifications (e.g., lock state, connect, expiry dates), SMS for CWP MFA

SIEMENS

State-of-the-art industrial security

Of course, remote connectivity exposes customer networks, Siemens products and Siemens infrastructure to the internet and with that to multiple security risks. For this reason, cRSP manages security operations with the greatest of care. All core services are ISO27001 certified, risks are permanently monitored and evaluated, and frequent penetration testing is part of the protection concept of the platform.

common Remote Service Platform
Certified security

CERTIFICATE

TÜV AUSTRIA

Management system as per
ISO/IEC 27001:2017

In accordance with TÜV AUSTRIA procedures, it is hereby certified that

SIEMENS

Siemens AG
Smart Infrastructure - SI IT DIS IOT
Siemenspromenade 10
D-91058 Erlangen
Germany

applies a management system in line with the above standard for the following scope

Operations and product life cycle management (PLM) of the ‚common Remote Service Platform (cRSP)', including management of requirements, releases and deployment

Valid Statement of Applicability (SoA): V 1.5, 03.09.2018

Certificate Registration No. TA420233018237

Initial certification 2018-10-19
Valid until 2025-10-18

Certification Body
at TÜV AUSTRIA GMBH

Vienna, 2023-11-10

This certification was conducted in accordance with TÜV AUSTRIA auditing and certification procedures and is subject to regular surveillance audits.
TÜV AUSTRIA GMBH Deutschstraße 10 A-1230 Wien www.tuv.at

ZERTIFIKAT | CERTIFICATE | CERTIFICAT | CERTIFICADO | СЕРТИФИКАТ | شهادة | 证书 | 인증서

044671-23-1

ISO/IEC 27001
certified

cRSP

common Remote Service Platform

cRSP is ISO/IEC 27001 certified and complies with the latest security standards (IEC 62443, NIS 2). The web portal access is Zero trust approved for Identity Assurance Level 1 (IAL1).

Security by default using cRSP

- Compliant to Siemens security, Export Control & Customs (ECC), General Data Protection Regulation (GDPR) guidelines
- Periodical CERT (Computer Emergency Response Team) and Threat & Risk Assessment by Siemens
- Continuous security monitoring and regular penetration tests
- All connections are terminated and forwarded in the cRSP DMZ (demilitarized zone)
- Access only to devices defined (configured) in the backend
- Connections to devices are encrypted by using private networks (SSL VPN, IPsec VPN, Customer VPN)
- Comprehensive identity and access management (Privileged access management as principle)
- Strong role and privilege-based authentication, as well as authorization of users and cRSP Services for systems
- Multifactor authentication (MFA) for Siemens & non-Siemens user
- Strong logging and auditing mechanisms. Every access is recorded (Transparency for audit trail, analysis, reporting, etc.)
- Anti Virus Scanning , Data Integrity Protection and Monitoring of transferred files (file transfer client)

SIEMENS

cRSP Overview

common Remote Service Platform
cRSP Overview

cRSP

cRSP web portal

Connectivity options
- SSL VPN
- IPsec
- Customer VPN

VPN

Up to 3x redundant DMZs* with multi tenant capabilities
- Fürth (DE)
- Irving (US)
- Singapore (SG)

Connect industry devices worldwide

SIEMENS

common Remote Service Platform
cRSP is more then just remote access!

Comprehensive suite for remote service

- Available for Siemens Service, business partners or for own usage (Remote Platform SaaS)
- Clientless connect for remote access from smartphones and tablets
- Integrated cRSP Proxies, file transfer, e-mail, SMS, file backup services
- Update functionality for automatic roll-out of software updates to clients and gateways

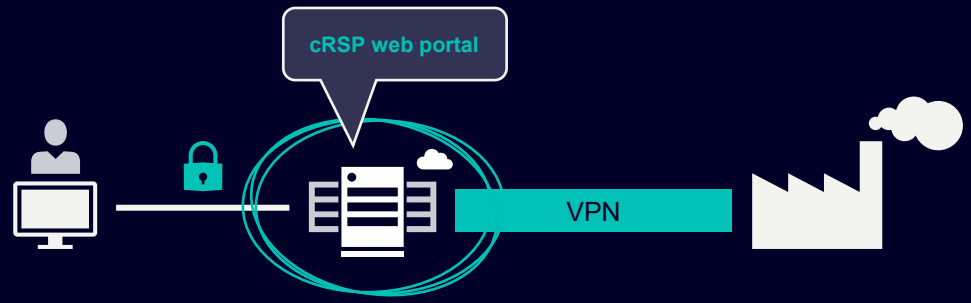
How does it work?

1. **Initial one-time setup of VPN tunnel**
   Connect customer sites and systems to cRSP
2. **User identification and authorization**
   Grant privilege-based access with the help of e.g., roles and user groups
3. **Tunnel is available for usage**
   cRSP remote features can be used through secure VPN tunnel

cRSP Web Portal

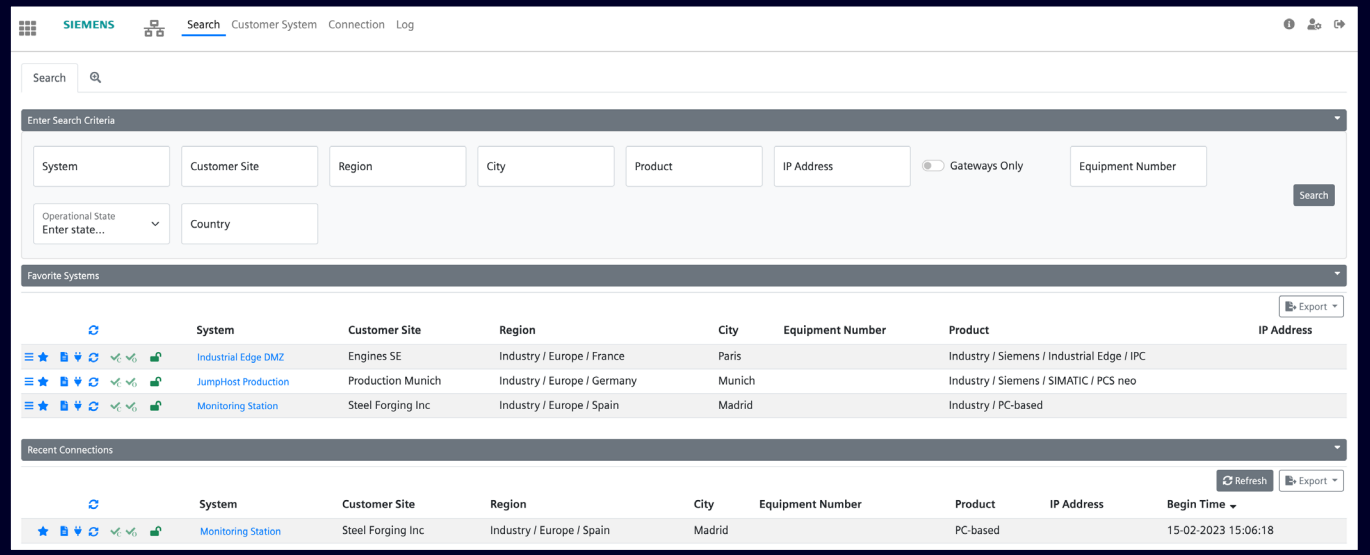
Efficient operation, transparency, and controls

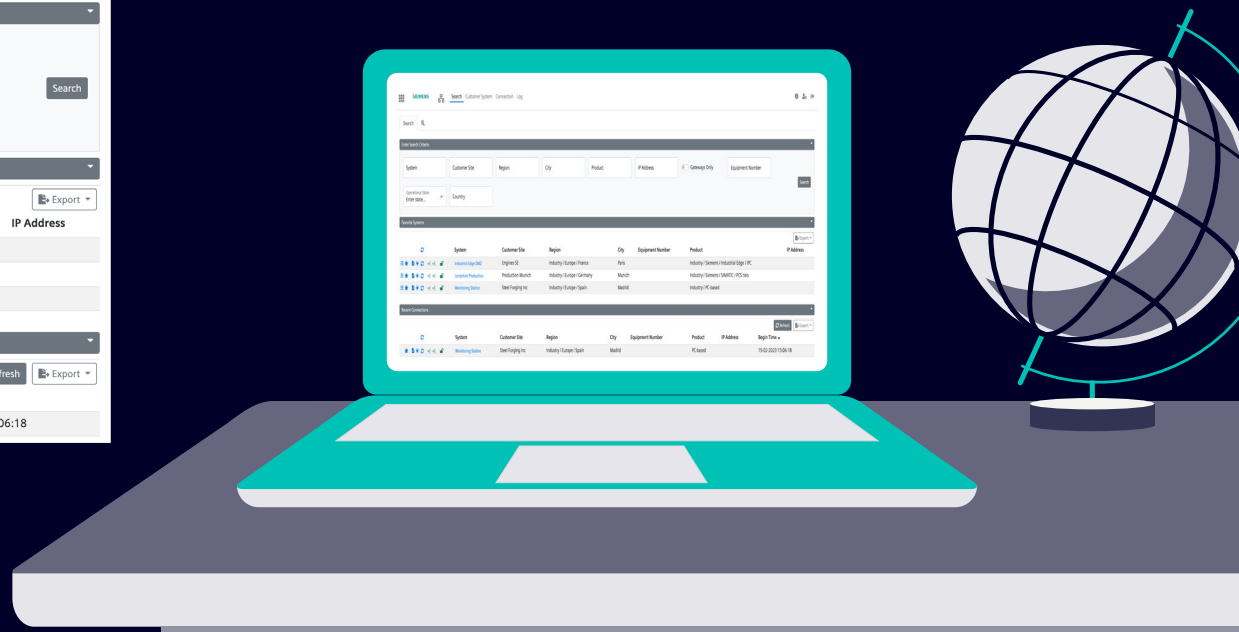
The heart of cRSP is the intuitive, workflow-oriented User Interface which cuts down operation times for users by a factor of 2-3 and allows for quick connects, multi-threading, user customizations, reports, templates, bulk operations, and many other workflow optimizations.



common Remote Service Platform
cRSP web portal

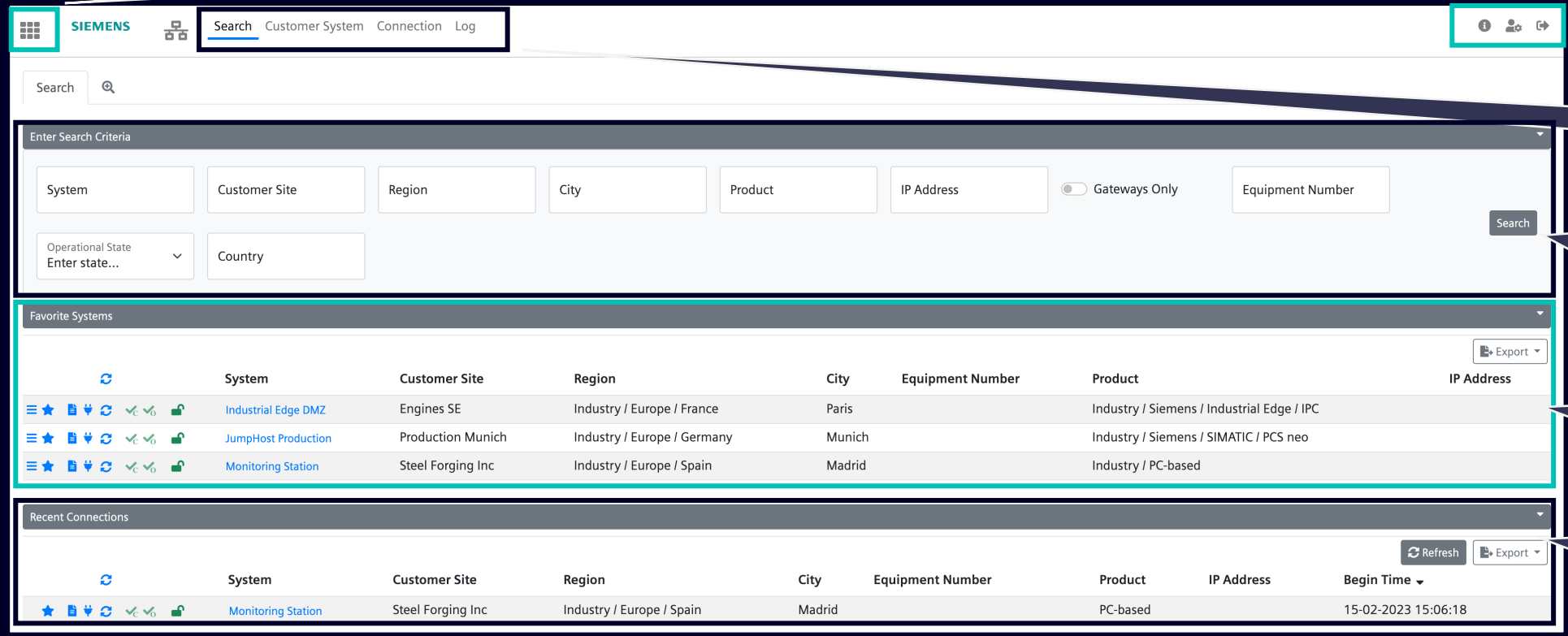
cRSP landing page





common Remote Service Platform
cRSP web portal

Navigation within the web portal



Burger menu
Here you can switch between the different user and admin modules of the cRSP

User area
In this area you can find support information and the settings of your account

Navigation area
In this area you can navigate between the different views

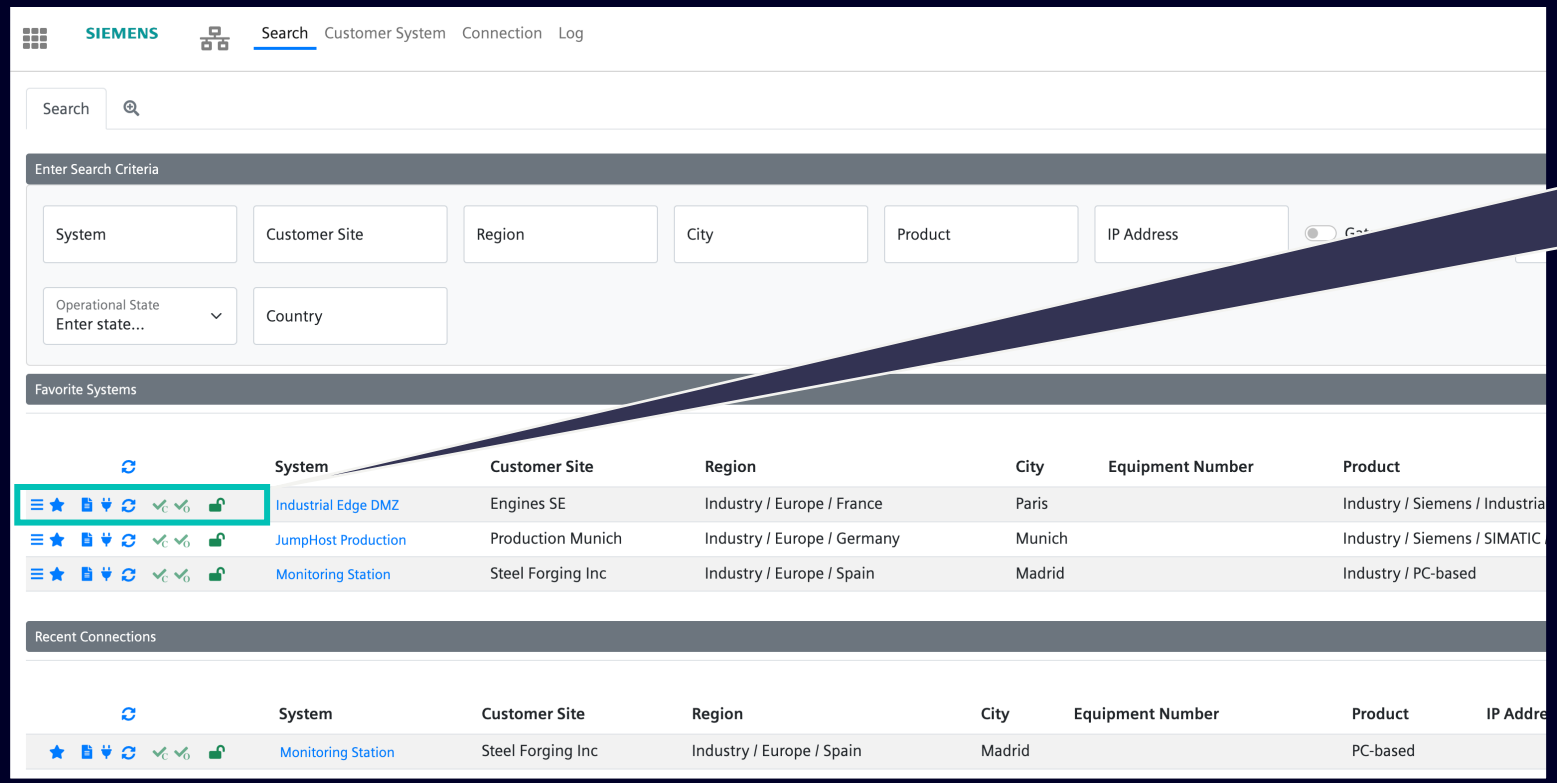
Search
You can search for an existing system using the available search criteria, which can be customized in the search settings.

Favorite Systems
Here you can find a list with all systems that were marked as favorite (star icon).

Recent Connections
This list contain recent connections ordered from latest to oldest.

common Remote Service Platform
cRSP web portal

Start a remote connection

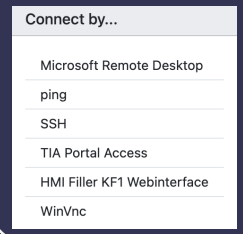


Quick start icons

With this icons you can start a remote connection or get mor information (e.g. tunnel status, log information,…) about your system.

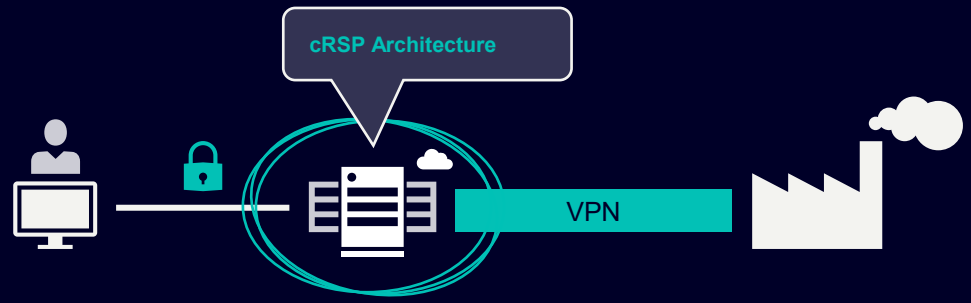
Start a remote connection

If you click on the “Start connection” icon on the system’s list, the list of available applications for that system will show. From there, you can simply choose the desired application and start a remote connection.

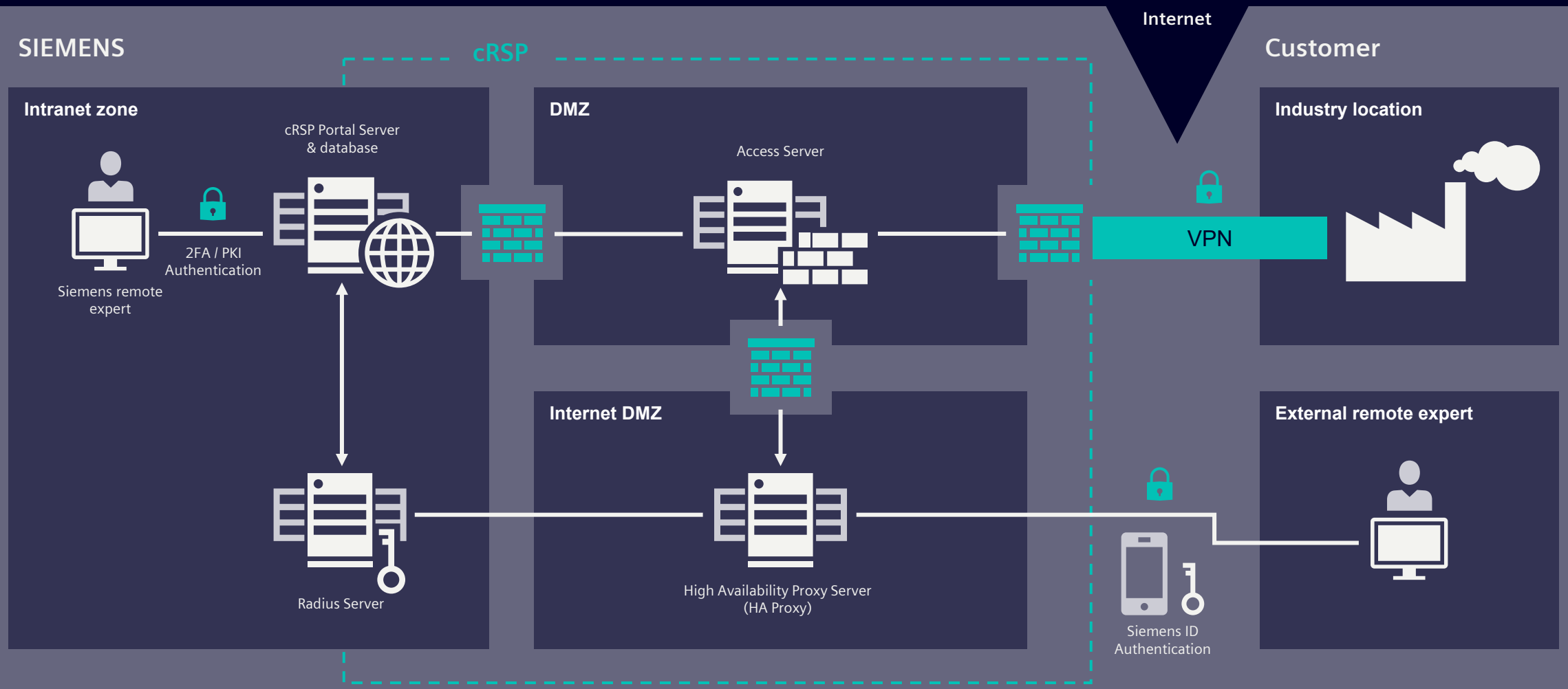


SIEMENS

cRSP Architecture



common Remote Service Platform
cRSP architecture in detail



common Remote Service Platform
cRSP architecture - components

Intranet zone

The Intranet Zone is a separately secured internal network area that is only accessible to Siemens employees. Siemens employees must be on our corporate VPN (or logged in directly to our domain by hard wire or WiFi from a Siemens location).

INTRA

cRSP Portal Server & database

The cRSP Portal Server is the central frontend of the cRSP and provides the web GUI which is connected to the cRSP database. One advantage of cRSP is its multi-client capability. This allows to provide a separate database schema for each tenant and ensures a maximum level of data security.

Access Server

The Access Server provides connectivity services for a secure tunnel connection between the cRSP DMZ and the local network of the industry location.

DMZ / Internet DMZ

To protect customer networks, Siemens has secured the cRSP infrastructure in DMZs. Remote Experts do not set up end-to-end connections to customer systems or vice versa. Instead, the connections end in the DMZ, which is secured on both sides by firewalls.

Radius Server

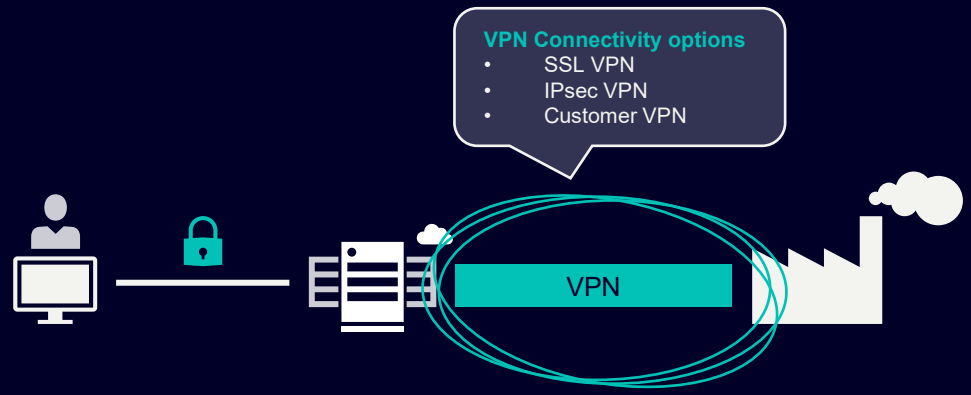
The Radius Server is the authentication server of the cRSP. Access rights of a Siemens employee are verified based on the PKI, a strong authentication technique using a smart card. External users log in via Siemens ID which provides secure access to Siemens applications and services with one digital identity via multi-factor authentication.

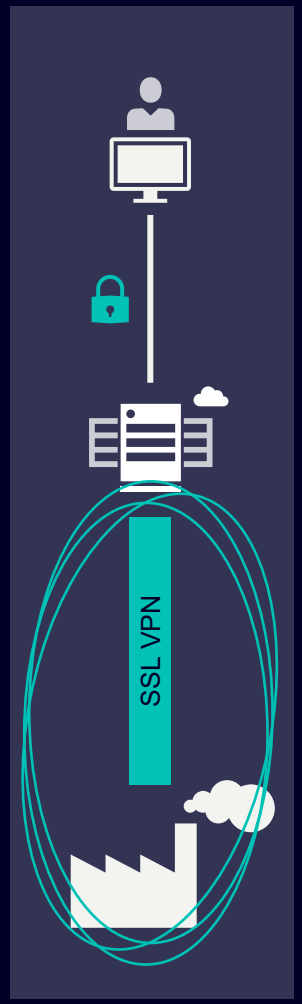
HA Proxy Server

The High Availability Proxy (HA Proxy) Server is a security appliance that provides secure access to the DMZ for customers and other external users.

SIEMENS

cRSP VPN Connectivity





SSL VPN connection

The cRSP SSL VPN software client is our standard when connecting systems to cRSP. Before using it for the first time, the client must be installed on the target device and initially registered.

The software client is available for installation on Windows or Linux-based customer systems and as well for industrial edge devices. In addition, it can be implemented in hardware or software-based gateways (e.g., Docker container) where a decoupled solution is required. With an optional addon installation the SSL VPN Software Client can be used as a gateway. It is therefore also possible to reach devices that are connected behind the tunnel endpoint. The initial registration of the client is done with a one-time password (OTP). This OTP is generated in the cRSP uniquely for each individual target device and is only valid for the registration process. After initial registration, the SSL VPN tunnel is established from the customer's system to the cRSP and can now be used by an authorized remote service expert via cRSP.

The SSL tunnel, which uses state-of-the-art Transport Layer Security (TLS) protocol, provides communication privacy over the Internet to prevent man-in-the-middle eavesdropping, tampering, or message forgery between the client and the server. In addition, the communication between the cRSP SSL VPN client and the cRSP access service is secured by using server certificates signed by an internal Siemens certificate authority. This ensures that only that specific device can communicate with the cRSP servers. An additional hardware-based hash ensures that no unauthorized device can connect to the cRSP (system cloning).

How does it work?

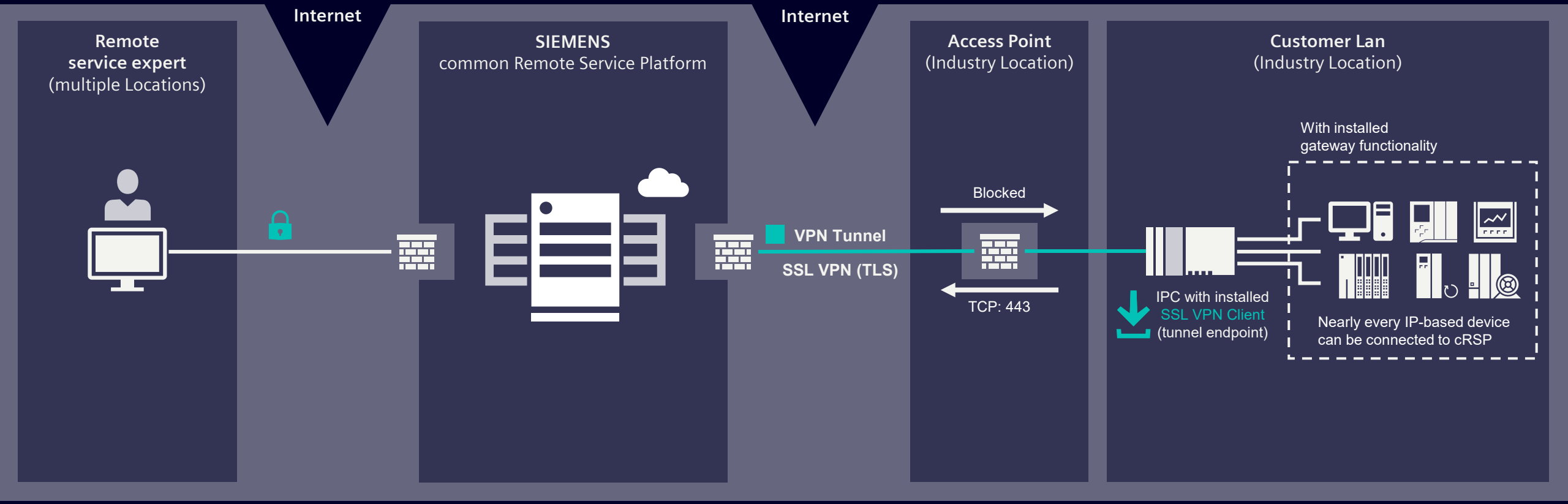
1. Installation of the cRSP SSL VPN software client
2. Registration of the client by using One-time password (OTP)
3. VPN tunnel is established and ready to use
4. Remote service expert can start a remote connection via cRSP

SSL VPN client
Available for:

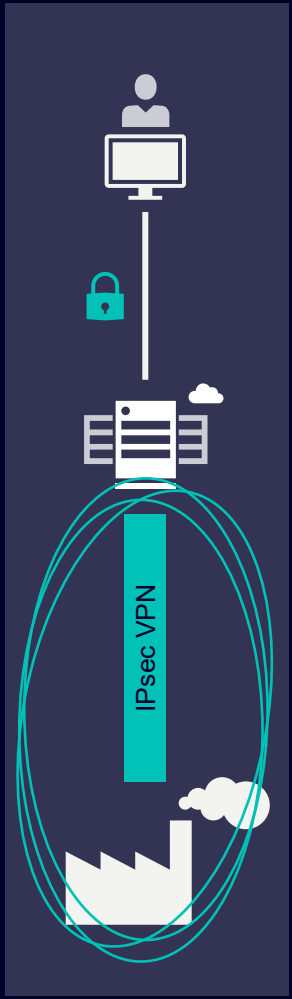
Windows & Linux
(download)

Industrial Edge
(download)

common Remote Service Platform
SSL VPN connection



common Remote Service Platform
IPsec VPN connection



IPsec VPN

As an alternative to SSL VPN, Siemens uses the established standard Internet Protocol Security (IPsec) with preshared secrets for encrypted and authenticated data transmission. To use the remote connection via IPsec, the corresponding parameters must be configured both in the cRSP and on the target IPsec endpoint (e.g. IPsec router).

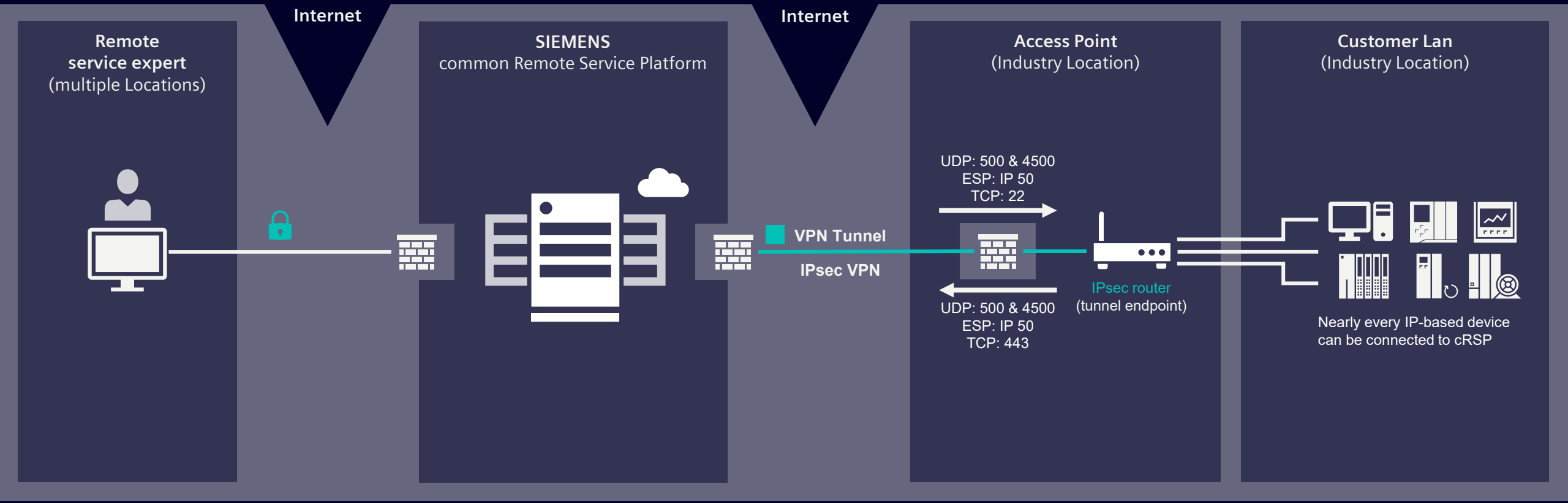
Preshared secrets consist of an arbitrary string with a minimum of 12 random characters. The Internet Security Association and Key Mananagement Protocol (ISAKMP) is used to securely exchange session keys. Encrypted secure payload (ESP) ensures data confidentiality through an AES-256 encryption while the SHA2 hash method offers integrity and authenticity protection of your data. Diffie Hellman key exchange with a key size of 4096 bit (group 16) is used for key exchange security and Perfect Forward Secrecy (PFS).

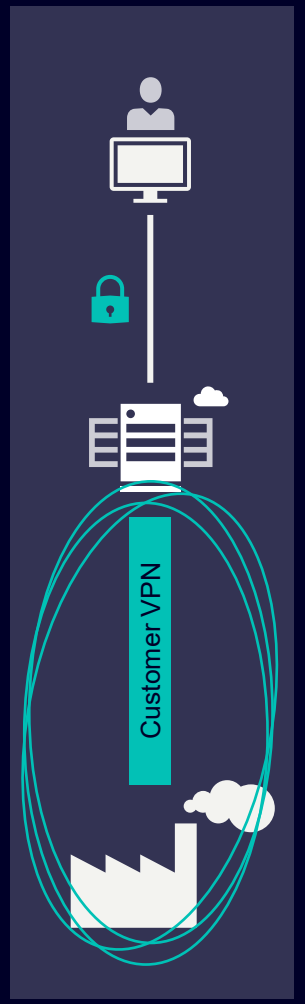
IPsec as well as SSL VPN is designed to provide communication privacy over the Internet to prevent man-in-the-middle eavesdropping, tampering, or message forgery between the client and the server.

How does it work?

1. IPsec configuration on suitable router / endpoint
2. VPN tunnel is established and ready to use
3. Remote service expert can start a remote connection via cRSP

common Remote Service Platform
IPsec VPN connection





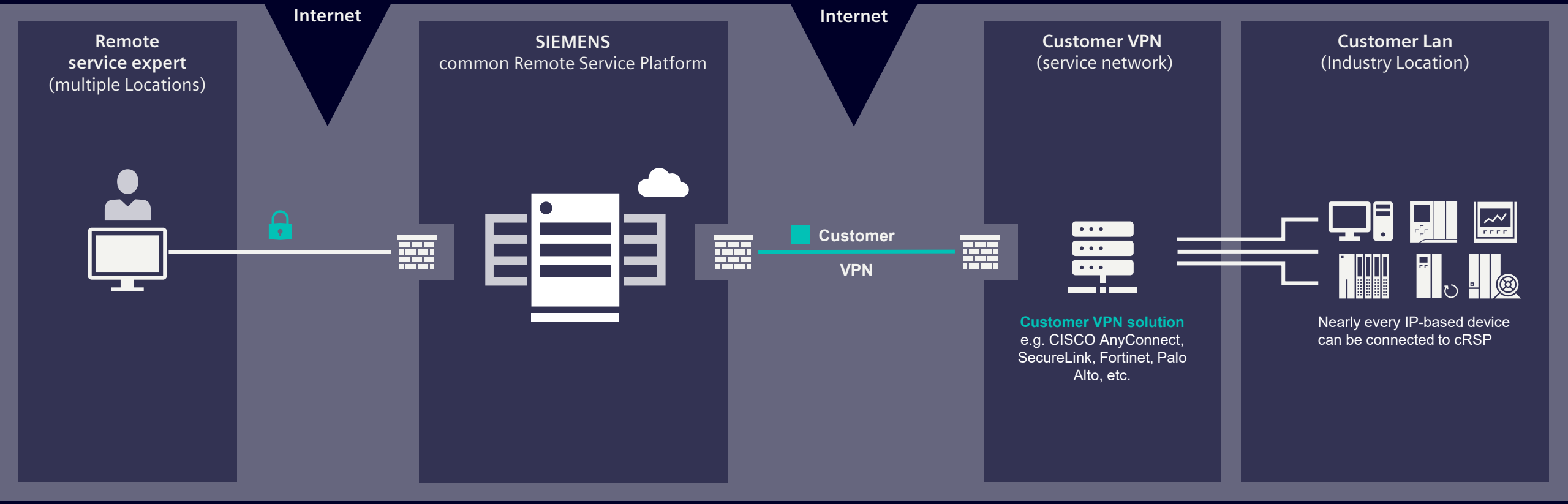
Customer VPN connection

Some customers do not allow direct access to their network but make available specific service networks. The reasons for this can be manifold, e.g. to create a bastion host between the own network and other providers, to have more control in the own network or to consolidate site access from outside into one customer VPN access, which is then linked to dozens of different sites (especially large customers with many sites). There are many different types of customer VPN (CVPN) solutions commercially available. cRSP is generally able to connect to a variety of customer VPNs (e.g. CISCO AnyConnect, SecureLink, Fortinet, Palo Alto, Checkpoint, Barracuda, OpenVPN and Wireguard) and new types are added step-by-step. Each VPN type works differently, even within the same vendor. There are a lot of different configurations and there is no one solution fitting all situations! If a specific service network is your preferred option to connect, your Siemens contact can assist in determining the best VPN solution. An extensive documentation would be a great help for the onboarding.

How does it work?

1. Identify the used customer VPN solution
2. Collect configuration parameters of the VPN solution & documentation
3. Get in touch with your Siemens contact
4. CVPN connection to cRSP is verified

common Remote Service Platform
Customer VPN connection



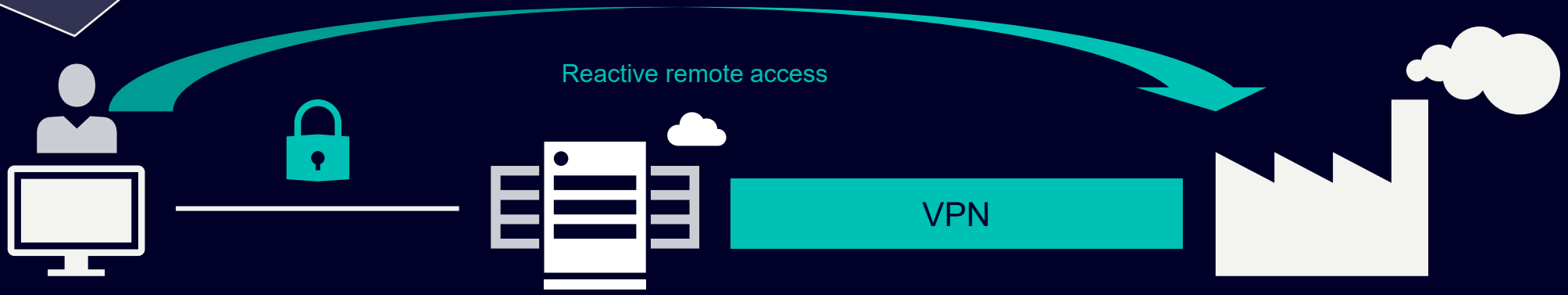
cRSP
Remote Features

Reactive remote access

common Remote Service Platform
Reactive remote access

Use of **cRSP web portal** for reactive remote access

1. Use of the clientless access for simple access use cases via browser
2. Use of the Operator Client to enable full potential of access

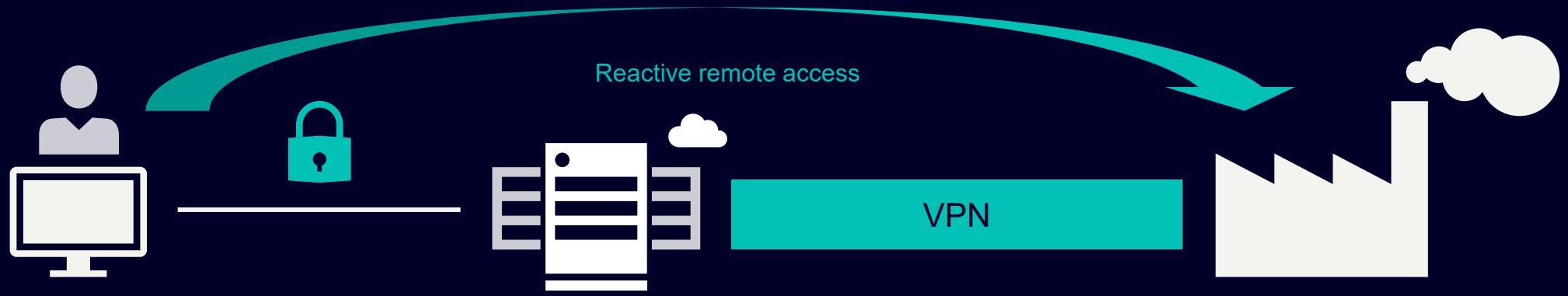


Important features for reactive remote access

e.g.:

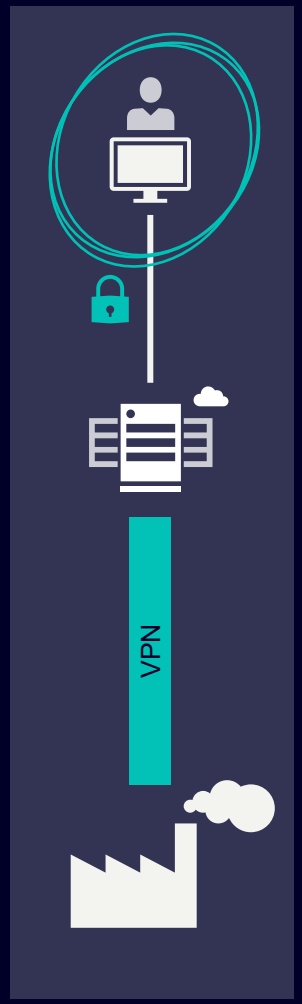
- >25 different supported application templates available
- Lock/unlock feature (sites/ systems) with timer
- Connect notifications (access, disconnect)
- Service call ID, annotations, tagging

common Remote Service Platform
Simple and secure remote access



Workflow

1. Login to the cRSP web portal
2. User grants will be checked
3. Selection of the target system
4. Start remote connection via pre-defined application templates
5. Access the target system



Remote access for remote service experts

The remote service expert can access cRSP via a secure https connection to the web portal (Web GUI). For this purpose, the remote service expert must log on to the portal using multifactor authentication. After logging on to the portal, the remote service expert has access to the connected systems according to his authorizations. To start a reactive connection, the remote service expert can use a wide range of pre-configured protocols and application templates. For simple use cases (e.g. desktop sharing) the cRSP offers clientless access to target systems by only using the browser. In case of advanced access use cases (e.g. configuring a PLC), where the expert needs to run local applications or use application templates provided by cRSP, the operator client is needed.

cRSP detects automatically if the operator client is necessary or not. In case the client is not installed yet, a download of the client is offered to the remote service expert. After installation, the operator client is started and opens a secure SSH encrypted tunnel for the used application to the cRSP access server. From the cRSP access server the secure connection is forwarded to the target system.

How does it work?

1. Login to cRSP Portal (Web GUI)
2. Selection of the target system
3. Starting the remote connection
4. Operator client is provided via download or is started if already installed
5. Operator client is running and connects the used application securely

Operator client
Download from cRSP is offered automatically when needed

All communication takes place via the secure VPN tunnel.
Selection of supported applications

http/https
Web-session

RDP
Microsoft remote desktop protocol/ Terminal server

VNC
Virtual network computing

Ping
Network utility

SSH
Secure shell

SFTP
Secure file transfer protocol

SCP
Secure copy file transfer

FTP
File transfer protocol

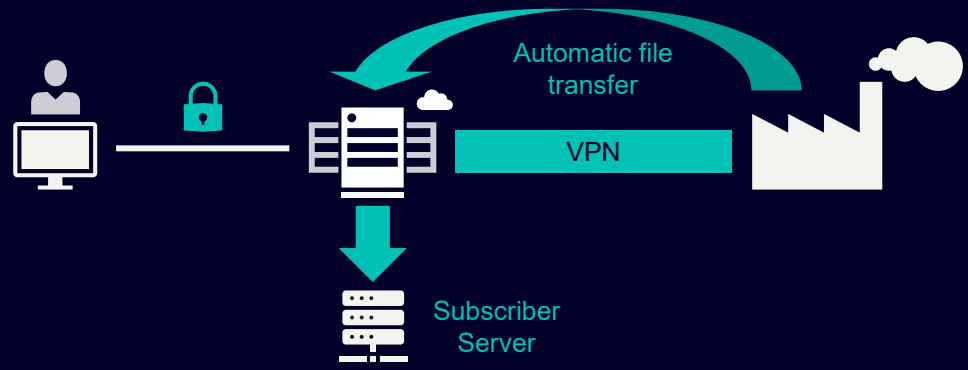
NetOp
NetOP remote control

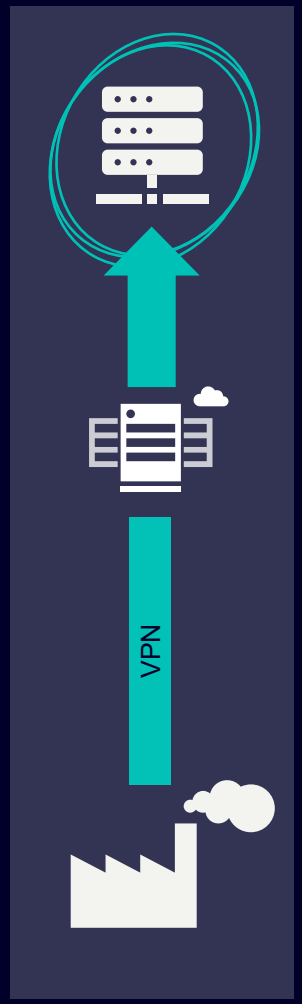
Transparent application tunnelling
Tunnel any TCP/UDP ports

Any other applications can be made accessible!

Transparent application tunneling forwards existing service applications through the secure cRSP VPN tunnel so that users can benefit from all the advantages of the common remote service platform (such as authenti-cation and authorization) without having to leave their familiar application environment.

cRSP
Remote Features
Automatic File Transfer



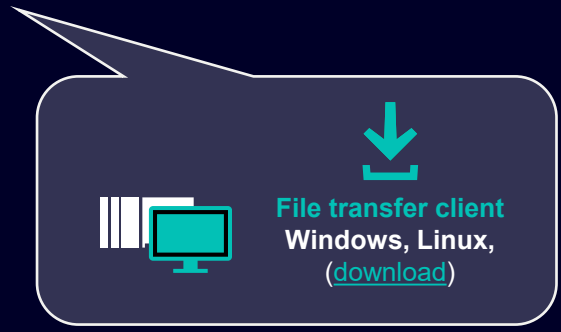


Automatic file transfer

cRSP is able to automatically transfer files or entire folders from a target system through the secure VPN tunnel of the cRSP.
The data transfer must be set up so that the remote system can transfer files or folders. For this purpose, the File Transfer Client must be installed and configured on a suitable remote system from which the data is to be retrieved and sent. The cRSP determines where the data sent by the File Transfer Client is to be made available.
It is possible to transfer files to one or more file subscription endpoints. The data can be transferred in various ways, e.g. FTP, SCP or by e-mail.

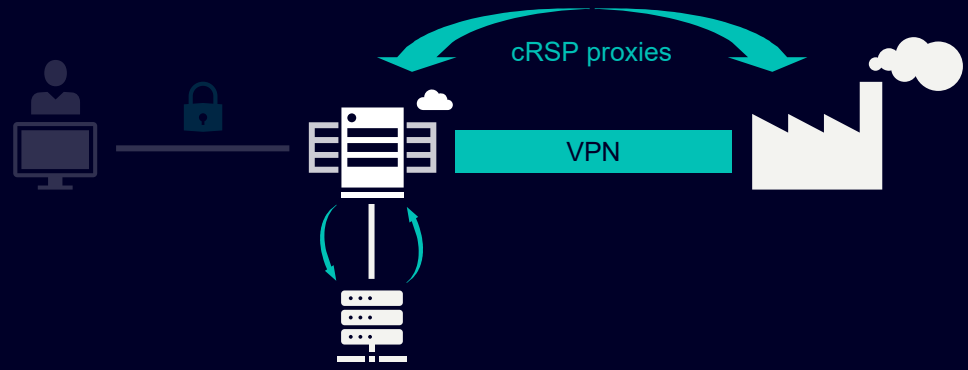
How does it work?

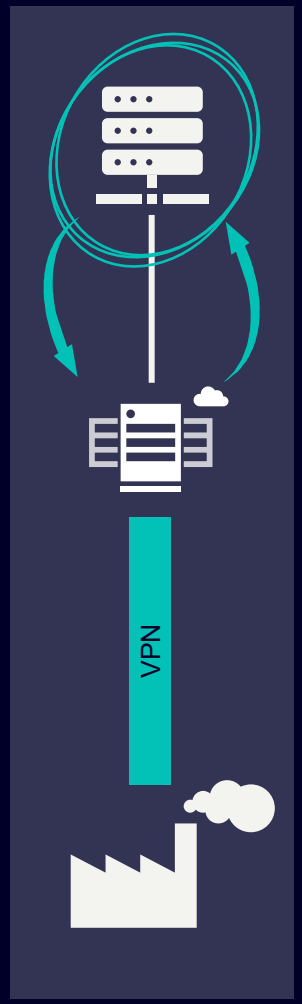
1. Target device is connected to cRSP
2. Installation of the cRSP file transfer client on the target system
3. Configuration of the file transfer client
4. Configuration of the subscription server in cRSP
5. Files can be automatically transferred through secured VPN tunnel



cRSP Remote Features

cRSP Proxies





cRSP Proxies

cRSP proxies enable secure communication between a customer device connected to the cRSP and any endpoint on the internet. The proxy functionality can also be used if the customer system itself is not proxy-capable.
To be able to use the proxy functionalities, a cRSP administrator must define which endpoint can be reached by the customer device (connected to cRSP). The customer device can then send its requests according to the configuration. cRSP checks the request and establishes a connection to the endpoint on the Internet. Endpoints can be different systems, for example servers that provide important updates for a customer system.
The security advantage over direct M2M communication is that cRSP acts as a rendezvous server and the customer device remains invisible to the connected endpoint.

How does it work?

1. Connect customer system to cRSP
2. Configure Proxy for connected customer system in cRSP
3. Customer system send request to cRSP
4. cRSP establish the requested connection as configured

Facts, Figures & Benefits

The cRSP is an Industry Standard for many Customers

Facts & figures of the cRSP

High availability

Three redundant data centers in Germany, USA and Singapore

Approx. 35k registered users	Approx. 700k connected systems	Approx. 5TB daily data transfer	Approx. 10MM Daily connections	Approx. 20k permanent parallel connections

Multivendor-capability

Support for systems of various vendors

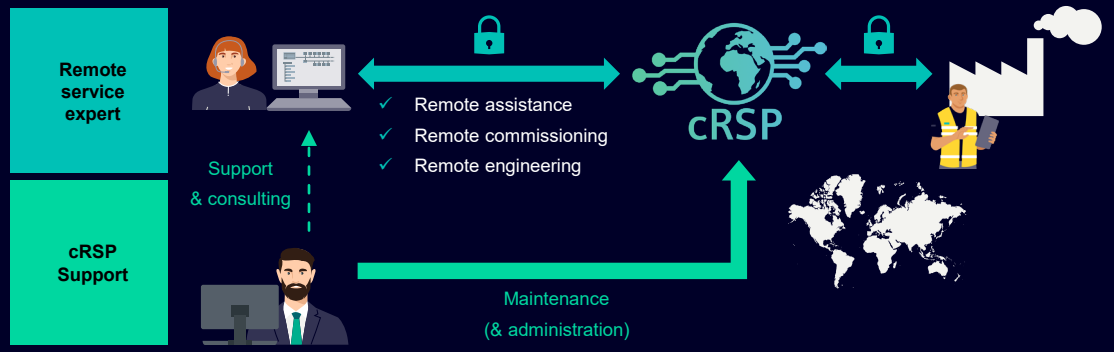
SIEMENS

Remote Collaboration with cRSP
Wrap Up

Remote Collaboration with cRSP

With the common Remote Service Platform (cRSP), we have a trusted and worldwide established system.

- >700k configured systems and >35k registered users
- >10MM daily connections and 5TB data volume per day
- Fits into all remote service use cases



Combine the benefits of

Remote Service

Remote Service enables fast & effective support and contributes to sustainability.

- Cost reduction due to higher time-to-fix rate
- Improves service efficiency
- Contributes to sustainability

cRSP

cRSP enables secure and direct remote access to industry devices.

- State-of-the-art industrial security
- Highly performant and scalable
- Siemens proven and worldwide available

SIEMENS

Disclaimer

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

SIEMENS

Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g., firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/cybersecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under https://www.siemens.com/cybersecurity.

SIEMENS