Unify Remote Service Platform

Remote Service Platform v2 Security White Paper

Issue 2.8

Trusted Partner for your **Digital Journey**

Atos

1. Introduction

1.1 Remote Services – Motivation and Objectives

Remote services will become increasingly important in the future as companies try to offset rising cost pressures and availability of telecommunication becomes more and more crucial. Remote monitoring of conditions and diagnosis can detect developing faults in an early stage, allowing maintenance to take place when needed, rather than at fixed intervals. With more than thirty years of experience in remote service, Unify is very much aware of the importance of security when offering remote service to its customers. Furthermore, the ongoing networking of telecommunication products and IT solutions, as well as advanced communication technology significantly drives new effective remote service offerings. Because of the convergence of traditional telecommunication and IT equipment, security issues and data privacy become even more important for remote services.

1.2 Perspective of Remote Services

The possibility of using remote services is not new to Unify and our customers, but the technology improved and made it possible that we can offer state of the art secure broadband transmission today.

The Remote Service Platform (RSP) provides support for the huge number of existing analogue and ISDN dial up connections as well as RSP.servicelink (based on OpenVPN) and Site-to-Site VPN (based on IP-Sec VPN).

All new products will offer broadband remote connectivity only. New versions of existing products will be prepared to support RSP only (Site-to-Site VPN and RSP.servicelink).

2. General operational concept

2.1 Purpose and usage of this document

This security concept describes the measures we at Unify undertake to protect data, application programs and IT- systems when performing remote services. Our security concept is divided into two main parts. Starting with a general operational part, we explain the basic concept of our Remote Service, our service processes, and the technical capabilities of our products. The first part is aimed at product users, technical managers, and everyone who is interested in obtaining a basic understanding of how Remote Service works. The second part, the technical concept, is aimed at IT specialists and data security experts who need to know in detail what technical and organizational security measures we are taking to achieve a high level of security and privacy of data. The Remote Service Platform offered by Unify is described in general where possible. If some topics will be handled differently for different connectivity types, it will be described separately. This part explains how a connection to this Remote Service is established, what our security infrastructure looks like, and what we do to prevent malicious attacks.

2.2 Data security as the fundamental prerequisite

The customer’s needs for information security and safety of his systems must be carefully evaluated. Only this way the customer considers remote service as trustworthy and grants the access rights necessary. Furthermore, it is important for Unify to understand and consider particular demands for information security to safeguard the business.

Depending on the customer’s business, the technical infrastructure, particular security issues, national regulations, etc., security measures may have to be realized, which are beyond the standard features of a product.

Before establishing a connection to a customer site, these demands must be clarified.

The typical customer requirements are:

- Comprehensive Logging
  The customer and/ or national regulations may require comprehensive logging of session data.

- Audit Trail
  Regulations may require a recording of remote service sessions, such that the session is traceable in case of future reviews.

- On-line Monitoring
  The customer may want to observe a remote session in real time. When critical parts of the equipment are serviced, customers may want to supervise all actions. This function is not integral part of the RSP but possible via separate WebCollaboration session offered by the Unify technician.

- Selective Access
  Comprehensive administration of user rights and data access
  Customers may want to have a very fine graduation of user rights and access capabilities to systems and data. Unify products offer a distinct management of user rights on top of the remote access security.

- Protection of Data Privacy
  Certain industries or national regulation require measures to ensure data privacy. In any case it must be clarified before connecting remotely to a customer's system, how and on which basis data privacy protection issues are to be addressed.

2.3 Service and maintenance of technical equipment

Given the growing complexity of modern products and solutions, Unify has responded to the challenge by providing additional support to optimally service our customers. Furthermore, it is often simply more efficient and faster to first determine the causes of system problems via remote diagnosis and, where possible, correct the problem through remote repair. However, in those cases where remote repair is not possible, the information obtained via remote diagnosis can support the service engineer on site. But that's not all. With our proactive services, we act in a preventive manner, rather than reacting after an emergency occurs.

Our software independently monitors certain important parameters within the customer's system. If values exceed or fall below the previously defined limits, the system automatically sends a message to our Service Center. The incoming message is then analysed and, if necessary, preventive remote repair is initiated with minimum interference to product usage. Or, we will correct the problem indicated in the message on site and within the scope of the particular service agreement.

Whether on site or remotely: Many problems can be detected and corrected based on technical data from the system. Should access to data sets or images containing sensitive data become necessary, we safeguard the compliance to the regulations and guidelines on data privacy protection. In the case of product classes where this is technically impossible, or where the task prohibits it (e.g., when accessing databases), we offer options for the customer to limit access to this data to the extent necessary and implement specialized technical and organizational security measures.

Basics of on-line support

Remote access to customer systems for on-line support (e.g., for user questions regarding operation) is additionally provided through remote desktop managing tools. They provide a 1:1 display of the customer's monitor at the Service Center, as well as enable remote control by the service engineer. However, this is only possible from a technical point of view if the customer has explicitly granted access. This authorization is required for each individual session. Additionally, in such cases, the customer can track

the course of the online support and, if necessary, terminate the access provided to the Service Center (located in Germany).

2.4 Proactive and value-added service activities

As part of our product related services, your devices can proactively send predefined system data to the Service Center. This includes technical data such as system logs, statistical data (e.g., number of restarts, scans, etc.), or system reliability data. In addition, remote monitoring as part of selected system parameters enables new attractive services in the managed service portfolio for our customers to further optimize product utilization and life cycle costs.

2.5 Using a standard solution

A growing number of manufacturers offer remote services for their products in various configurations. This results in an increasing number and variety of remote connections between the customer and product manufacturers, as well as increased administrative costs for the customer. However, added administrative complexity can also increase the probability of security gaps. We want to avoid this situation by building on a standards compliant and certified solution.

3. Technical and organizational security concept

3.1 Overview

3.1.1 Establishing the connection

As a general policy, the degree to which access is granted to a system is determined entirely by the customer. Usually the connection is established and stays in that state. If the customer does not want to keep a remote connection he has options to turn it off.

- For RSP.servicelink the RSP.servicelink router or the LAN cable can be unplugged

- For embedded RSP.servicelink Plug-ins an Activate/ Deactivate option is available in the product GUI

- For Site-to-Site VPN (IPSec) connection type the firewall settings are used to prevent permanent remote connectivity

- For Modem based RSP connection types the modem can be put out of service

3.1.2 Access Control

As a prerequisite for every service activity, the customer must expressly (within customer service contract) grant access to our Remote Service and controls who is permitted access to the system. Access is only granted to identify or correct errors or perform requested MACs.

3.1.3 Remote access logging

We record every access to the customer system and apply a time stamp. In addition, the service engineer or optionally a certified service partner who accesses the system is uniquely assigned a user identification which is also recorded in this log. As a result, we can inform the customer within an appropriate period of time, that a service engineer had access to data, when, and what communication activities were performed on each system. We retain these log reports for at least one year or according to the local data protection laws.

3.1.4 Privacy along the transmission route

We utilize the most modern encryption methods to protect customer data from unauthorized access during transmission. This is especially a prerequisite for any communications via the internet. For additional information, refer to section 3.2.

3.1.5 Organizational measures

Our service engineers are aware of the need for data privacy and IT security and understand the severe consequences of not abiding by the applicable requirements. Only service engineers who have been trained in and are committed to data privacy and security issues are authorized to perform remote services. As outlined in the next section, our currently used Remote Service Platform (RSP) contains a secured data set of these selected service employees, as well as their corresponding access rights. All statements within this document are valid for the Unify Remote Service Platform if not restricted to one of its components.

3.2 Overview of Unify Remote Access

3.2.1 Security infrastructure of RSP

Within this section more detailed technical information is provided concerning the following topics:

- Security certification of RSP
- Authentication and authorization of service engineers using RSP (Ch.3.3.1),
- The RSP - DMZ, the „demilitarized zone" between the Unify intranet and the Internet or public lines (Ch.3.3.3),
- Security measures for accessing the customer network (Ch. 3.4.1)), and
- Protocols and services supported by RSP (Ch.3.4.3.)

3.3 Security infrastructure details

3.3.1 Authentication and authorization of Unify service personal

A multi-level service domain concept defines which users of the Unify remote service platform are permitted to access which systems. This means that our service engineers only access those customer systems for which they are expressly authorized.

The central maintenance and dial-in database of RSP is located secured from the Unify intranet and cannot be accessed externally. Access to RSP is available only through the RSP terminal servers and requires a valid RSP user ID and password.

All RSP connectivity's terminate in the same Unify data center and use selected servers of the certified RSP platform for user administration and terminal sessions. External access for certified technicians to RSP is possible only via double authentication, one is over the Intranet and second is with own RSP login. Different user ID and password is used.

In addition to the manual login RSP offers the automatic login to customer devices for active RSP users. In the RSP there is the option to store user credentials of customer devices (user/password). RSP is the central storage for user credentials. This allows Single Sign On (SSO) from RSP to customer devices. The user credentials (user/password) of these SSO connections can only be created and changed by an RSP data administrator.

3.3.2 Authentication and authorization of Unify service partner and customer personal

Sometimes comprehensive services for our customers require the involvement of service- and engineering partners. To ensure the same level of security in that cases, our service partner services is available as an optional extension to our Unify remote service security infrastructure.

Service partners using RSP will authenticate themselves at the then get access to the Unify RSP. Besides our high security standards, a seamless logging of all Unify remote service activities is guaranteed. User management is part of Unify Support Portal.

3.3.3 Demilitarized Zone - DMZ

To protect the Unify intranet and that of the customer from reciprocal problems and attacks, we have secured our remote service servers in demilitarized zones (DMZ). Connections from the Unify service engineer to the customer system, and vice versa, are not "put through directly." They terminate in the RSP servers using a reverse proxy function.

This means for RSP that a connection established from the Unify intranet is terminated in the RSP terminal servers. This server then establishes the connection to the customer's system via a proxy server and mirrors the communication coming from the customer back to the terminal servers which are separated from the Intranet. No matter which of our connectivity options is behind the communication path the possibility of a communication between the Unify intranet and the customer's network over not explicitly authorized protocols is thereby prevented.

This architecture is designed to prevent:

- Unauthorized access from one network to the other (e.g., hackers)
- Access from a third-party network (e.g., the Internet)
- Prevent fraudulent use of secure passwords, access data, etc.
- Transmission of viruses or similar harmful programs from one network to the other

In addition, we do separate critical data with at least two different firewalls from insecure zones like the Internet.

Within our managed services, messages and data are frequently sent by the monitored product. Also this communication is established only after successful authorization of the system requesting the connection.

3.3.4 Securing the transmission route

The actual Unify remote service is strongly focused on offering an up to date level of security with increased performance. The remote service for all new products has been committed to be the secure broadband (RSP.servicelink and Site-to-Site VPN (IPSec). For all customers who have to keep their existing ISDN dial up connections we still offer remote access via RSP.

Virtual Private Network (VPN) via the Internet

We recommend establishing a broadband, secure connection via the Internet which offers you the following advantages: highest possible level of security, best data transfer quality and availability, as well as access to all services. Based on current technology, this is implemented preferably via

Unify's preferred connectivity option is RSP.servicelink, which allows protocol tunneling over https (known from internet banking), as well as a Virtual Private Network (VPN) secured with IPSec VPN (Internet Protocol Security) between the Unify DMZ and your network portal. Unify can assist and provide you with the prerequisites to use our Remote Service.

RSP.servicelink based on OpenVPN uses AES 256 bit CBC encryption. A 2048-bit X509v3 server certificate is used to ensure that the RSP.servicelink Plug-Ins on the customer products or the RSP.servicelink router can only connect to the central RSP server.

Additionally, client certificates are used on customer site to ensure that only certified clients can connect to Unify's central server. A Client Certificate will be created for every single RSP.servicelink Plug-In or RSP.servicelink router on customer site which ensures recognizability of devices to raise data quality.

Site-to-Site VPN (IPSec) has been Unify's standard broadband connectivity with pre shared secrets for encrypted and authenticated data transmission. Pre shared secrets comprise a minimum length (according to the customer agreement) of characters selected randomly. The Internet Security Association and Key Management Protocol (ISAKMP) based IKE mechanism is used to exchange encryption key information. The use of an Authentication Header (AH) provides the integrity of data with the Hash method HMAC-SHA1. Encrypted Secure Payload (ESP) provides the confidentiality of data by encrypting with algorithm 3DES. The session keys for encrypting and authenticating the IPSec connection are derived from a Diffie-Hellmann key exchange.

3.3.5 Upgrade your remote connection

If you have dial-up capabilities and want to upgrade your remote connection possibilities while reducing your costs, please contact your local Unify representative to coordinate the precise configuration changes required for new connectivity types. He can advise you in setting up the right infrastructure or if you prefer Unify to provide such equipment contact your local representative to coordinate this provision. Unify offers protection for the transmission route via internet as well as via dial up connection. All passwords follow the strict Unify password policy which requires upper and lower case alphanumeric as well as special characters in combination with a required number of characters. Even the passwords randomly generated for the Challenge Handshake Protocol (CHAP) meet these requirements. The RSP does not allow usage of passwords which do not meet Unify password policy. For dial up connections there are optional functions available like Caller authentication via the ISDN function CLIP.

3.4 Security measures in the customer network

3.4.1 Access to the customer network

External access to the customer network requires - due to the security issues involved, specific attention and measures. The key security features depend on the specific concept and configuration of the SPoA (Single Point of Access) concept.

Access enabled by customer

A general security measure can be, to block any external access when not explicitly authorized or initiated by a component within the customer network. This security measure is, of course, supported by RSP, but has some considerable limitations, especially if no on-site personal is available. Access using RSP.servicelink Plug-in can be easily switched off by deactivating the appropriate service on customer site. For RSP.servicelink router the power supply or the LAN cable has to be unplugged to deactivate the remote access.

Customer supplied Access

If the customer already has an existing remote access solution in place, in most cases this system can be configured to work securely with our remote infrastructure. This can be one of our possible options from RSP.servicelink, Site-to-Site VPN (IPSec) down to Dial-up (ISDN or analogue Modem),.

To clarify the required configuration and measures, please contact your local Unify service representative.

Unify supplied Access

As the connection types developed from ISDN dial up over the usage of leased lines for IPSec-VPN to modern secure broadband connections like the preferred SSL-VPN (RSP.servicelink). Today's solution, due to cost, performance and security benefits, is our specified RSP.servicelink access without the need to change the customers firewall concept.

This solution can support high performance remote service solutions at low communication costs and enables future value-added services. Specific customer demands for additional security measures of certain applications, network segments etc.

or requested on-site firewall features can be provided easily based on this access solution.

3.4.2 System access

When remote access to your system is set up (either manually by user/administrator or automatic based on system configuration), the Unify service engineer has to be authenticated at the system before being able to perform any service operations.

3.4.3 Protocols

Depending on the capabilities of the software of your systems, the protocols http or preferably https as well as any standard service protocols like MS terminal server, ssh can be used to service your system.

Different connectivity's offer a tunnel which makes it even possible to use plain http because the tunnel is a comparable measure. RSP offers direct connection via RSP.servicelink, Site-to-Site VPN (IPSec) tunnel or Modems.

3.4.4 Data Transmission from customer systems

Diagnostic data is sent from your system to the Unify Remote Access servers for some of our proactive services, either automatically (based on your system configuration), or at the explicit request of the Unify service engineer. In such cases, only technical data are transmitted.

Depending on the capabilities of the software, the following services are used:

- sftp (Secure File Transfer Protocol)
- scp (Secure Copy)
- AFR (Open Scape 400 only)
- Syslog
- SNMP (via ZENOSS)

Different connectivity's offer a tunnel which makes it even possible to use plain ftp because the tunnel is a comparable measure. RSP offers direct connection via RSP.servicelink, Site-to-Site VPN (IPSec) tunnel or Modems.

3.5 Protection against malicious attacks

3.5.1 Protected Platform Servers

The servers in the Unify remote service platform are protected using state-of-the-art technology. Therefore infection by worms, viruses, Trojan horses, or other attacks are extremely unlikely and has not occurred to date.

3.5.2 Protecting customer systems

No direct threat from Unify servers

A virus infection to your system from our servers, or distribution of viruses in the direction of your system, is unlikely due to local virus checks performed continuously on our servers.

Threat due to Internet connection

Systems connected to the corresponding Unify remote platform servers via the Internet are – as with any connection via the Internet – exposed to a certain level of threat. If you use Internet access only for Unify Remote Service purposes, infection by viruses is unlikely due to our security infrastructure. Should you, however, use your Internet connection for other purposes, we advise you to take appropriate precautions to protect your system.

4 Contacts and information

For further contacts and information concerning Unify Remote Access please contact your local Unify representative.

About Atos

Atos is a global leader in digital transformation with 110,000 employees in 73 countries and annual revenue of € 12 billion. European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos|Syntel, and Unify. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more
about us atos.net
atos.net/career

Let’s start a discussion together

For more information: rsp@atos.net

Atos, the Atos logo, Atos|Syntel, and Unify are registered trademarks of the Atos group. April 2020. © 2020 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.