Versions-Information

Version - Datum	Kapitel	Beschreibung	Name / Abt..
11– 06.04.04		Adoption provider change WebEx	Oelsner/ RD
12 - 08.04.04		Comments B.Fritzsche/ viruses...	Oelsner/Fritzsche
13 - 26.04.04		Access for service technicians acc. Sec.council	Oelsner/RD

Content

1 Remote Access - HEIDELBERG's interactive remote service approach

HEIDELBERG provides a global web-based Remote Service approach that allows remote access to the customer's installation using the Internet as a carrier. Security is a vital concern for all remote service systems. HEIDELBERG recognizes this concern, and addresses it by the following:

- Enabling state-of-the-art secure remote access technology
- Security-trained service personnel and enforced security policies with strong commitment to our customer's privacy
- Continuous tracking of all security issues and established security processes by the HEIDELBERG Security Council to keep the highest level of confidence in HEIDELBERG's web based Remote Service on a permanent basis.

The following White Paper describes the security approach and addresses the Frequently Asked Questions (FAQ). The document is subject of change according the newest state of security technology and will be updated by Heidelberger Druckmaschinen AG without explicit notice to customers. The current version is published at Heidelberg's web site.

HEIDELBERG's commitment

HEIDELBERG believes that security and privacy are of the highest importance to our customers. HEIDELBERG's web based Remote Service will deliver trust by providing the highest level of security and protect customer's assets and IT in an efficient way.

2 How HEIDELBERG's remote service approach works

HEIDELBERG provides a web-based Remote Service. Any customer can request Remote Service, if his installation is capable to access the Internet. A company's Internet access is typically protected by a firewall and use application security provided by the operation of proxy servers. Nevertheless, in almost all cases HEIDELBERG's Remote Service connections are possible without any reconfiguration, so customers security policies accessing the Internet will be enforced.

Service technician's strong authentication: Login at Remote Service portal

First, HEIDELBERG's support representative must login to HEIDELBERG's Remote Service communication server successfully to get access to the customer base. The login process is restrictive, controlled and under supervision according the AAA approach, that is described in detail in chapter 3. This approach ensures, that no unauthorized technician can get access to the customer. After login the support representative can create a Remote Service session request to a specific customer. This request is pending and no interactive access is possible until the customer establishes the session.

Customer's control: Establish an interactive web-based Remote Service session

In general, any single, interactive, web-based Remote Service session must be granted from the customer site. The customer has to have physical access to the device, where he wants to get a remote service session started. The customer submits his session allowance to HEIDELBERG's Remote Service communication server using an unique identifier key (assigned per session or per device - depending on the implementation of the access protocol) The allowance will be transferred from the device to the Remote Service portal in real time on HTTPS (the secure version of the common Web server protocol). During the first visit a secure plug-in will be downloaded to the customer's Internet browser to implement the remote service tools and access points. To protect the data integrity and privacy during the transmission through the public Internet - any communication will use a strongly encrypted data tunnel.

Customer must grant any transaction: Remote Service Toolset

If the interactive web-based Remote Service session starts, the customer will get a personal identification text from the service technician to avoid anonymous counterparts. To fix the problem in an efficient way HEIDELBERG's service technician has a rich set of Remote Service tools available. In addition to device-specific tools the following standard set is available as a common platform:

- Access desktop of remote device without/with keyboard/mouse control
- Annotation tool for drawing on desktop by service technician and customer
- File browsing and bi-directional file transfer

The service representative select an appropriate tool. The customer has to grant the execution of the selected tool. (e.g. sent files have to be accepted by the customer for download) Web based Remote Service for Prepress devices is equipped in addition with a chat and video tool, that can be used from the service technician without extra grants since this tools have no impact to the device control at all.

Since the PC of the service representative and customer's device run synchronous tools, any activity of HEIDELBERG service representative is visible to the customer immediately.

Multi-Point Sessions and Over-The-Shoulder support

Web-based Remote Service expands the point-to-point capabilities of former remote approaches to a real-time support conference.

In case of a sophisticated workflow problem the customer can join the Remote Service session with more than one device to give the service representative the chance to track the problem not limited to device boundaries.
HEIDELBERG introduces the Global Expert Network - a virtual, global expert team, that can join existing Remote Service sessions on invitation of the regional service representative and on approval of customer to fix the problem.

Ensuring quality

Both sides, the customer and the service representative can end the session at any time. A regular close of a service request will send the customer a feedback sheet. The customer can rate the support session and provides feedback on the service experience. This data helps HEIDELBERG to monitor and improve the quality of our customer support.

3 Security starts with AAA (Authentication, Authorization, Accounting)

HEIDELBERG's approach to confidentiality builds on the strong foundation provided by AAA - authentication, authorization and accounting.

Authentication

Authentication verifies the identity of every party, from the Remote Service communication server to the service representative client and the customer's computer.

Authentication for service representatives
Any remote service representative has a personal named account. This name will be displayed during the access to a customer's device. The customer will never be faced to an anonymous counterpart. Any access by a service representative requires a successful login to the communication server by a secure connection in advance.

Any remote service representative will be trained for security issues and has signed the "HEIDELBERG Acceptable Use Policy". This document contains the responsibilities of our remote service personnel and management.

Named accounts will be managed by the HEIDELBERG Remote Service Administration Team and the accountant list will be kept up to date on a daily basis. Even with a policy-based withdrawal process - there is always a slight chance of dead accounts, that increase the security risk. So, HEIDELBERG accounts will be assigned for a maximum period of 12 months. Without renewal any account will be closed at this period.

Authentication for customers
A customer is authenticated by the use of an unique identifier key. Depending on the Remote Service approach this key is:
- generated per session and valid only for one specific session. In this case the session key will be hand over from the service representative to the customer. Using a 9-digit random number, the chance for guessing the number is extremely low. -OR-
- build in the HEIDELBERG device internally and stored in a protected unit. (in case of embedded systems)

Authorization

Authentication will be combined with access controls ensuring only authorized activities.

Authorized access as a service representative

Access to the customer network is strictly controlled at multiple points. As described only authorized and authenticated service representatives can get access to the web-based Remote Service portal. Hereby HEIDELBERG's Security policy is enforced.

Transaction-oriented authorization by the customer required
The authorization of the web-based Remote Service portal allows HEIDELBERG's service representatives to access to the customer's device, that establishes the service session. First step of authorization is the establishment of the Remote Service session. In this stage the authorized service representative can use tools like chat and video only to push information to customer's screen. For any further Remote Service transaction the tool usage must be granted by the customer case by case.

Common understanding
HEIDELBERG service representatives are restricted by "HEIDELBERG Statement of Acceptance" from accessing any system or network device on the customer's network without the customer's expressed authorization.

Accounting

The first part of accounting is the permanent overview of all ongoing activities for the communication participants. HEIDELBERG's Remote Service ensures a permanent update of all partners (list of customer's devices and service representatives (regional+ global experts)). By enforcing the authentication approach no anonymous participation is possible. Nevertheless - even in the unexpected case of number guessing - any joining of a remote service session will be signaled to all participants. No hidden spoofing is impossible.

HEIDELBERG tracks all connections made by service representatives and maintain session logs for security audit.

Session information listing
The HEIDELBERG administrator can create listing of sessions for any given day, including those that are still active. Each session records the service representative's name initiating the session, the session start and stop time, the session duration and all information from the pre-session form like customer's name, company, email, system, operational system.
HEIDELBERG generates reports that cover any range of dates and which sum users, sessions and session time and calculate the average session duration.
These standard reports can be analyzed to spot unusual access patterns, including exceptionally long sessions and unexpected client activities. They also serve as audit trails, making it possible to check who accessed a particular computer at a particular time.
(See also chapter 4)

Suspending or Canceling Accounts
The session information listing can also be used to check the activation status for individuals and groups. Controls are available to temporarily suspend or permanently cancel any user's account.

Optional session recording
Starting after the pilot phase, any session can be logged as a video-like stream. This stream is encrypted to protect the data privacy, but will be stored for a detailed session replay. So any display, keystroke and mouse-click can be recorded and replayed for analysis of a dedicated session. To protect customer's privacy and in conformance to regional data protection laws, the customer will be ask for allowance per session for this recording.

4 Protecting Customer Privacy

HEIDELBERG understands that privacy is a major concern for any remote service approach. HEIDELBERG has a strong privacy policy that prohibits unauthorized access and disclosure of personal or corporate information. Only information that is relevant to the service request will be accessed.

Published Privacy Policy
Heidelberg Information Security Policy is included in every service agreement. This policy identifies information gathered, how it is used, with whom it is shared and the customer's control over dissemination.

Disclosure of Customer Information
In order to deliver remote service, HEIDELBERG must collect certain user and machine information, including machine ids or serial numbers. Unless expressly authorized by the customer, HEIDELBERG will not disclose this and any other confidential information of the customer to any third party and will use this information only in manners that are directly related to the customer or the agreed upon services.

Access to Customer Information
HEIDELBERG's remote service representatives are the only individuals with access to communication servers. The session logs are used by HEIDELBERG to maintain quality of service and assist in performance analysis. (See chapter 3)

Ensuring Traffic Privacy
Any traffic is encrypted in a data tunnel, that means data will never be transmitted in a clear text (readable) format over public networks. Nobody spying on the Internet can decipher this traffic, because he does not possess the code used to generate encryption keys. (See also chapter 6)

5 Secure Customer Installation

HEIDELBERG's remote service software installation is designed in respect to customer's enterprise security on highest level.

Firewall Compatibility
HEIDELBERG's approach is firewall compatible* and support proxy servers. It generates only outgoing HTTPS traffic to ports 443. Because most firewalls are already configured to permit outgoing Web traffic, you don't have to bypass or compromise your corporate security/firewall to implement secure remote service.

*In most cases remote-service connections are possible without any firewall reconfiguration. HEIDELBERG requires access to outbound ports only. Occasionally, some firewalls may require port and IP adjustments to allow those accesses. For additional information related to firewall issues, please contact a HEIDELBERG sales representative.

If the customer establishes a Remote Service session an outgoing HTTPS request is sent to the HEIDELBERG's Remote Service communication server. This makes the HEIDELBERG approach completely compatible with application proxy firewalls, dynamic IP addresses, and network/port address translation (NAT/PAT). However, HEIDELBERG's customers can control traffic by simply filtering on HEIDELBERG's communication server IP addresses if required. Your HEIDELBERG sales representative will provide this addresses on demand. For security reasons this addresses will not be published in a broad range in advance.

Zero configuration
There are no security parameters to be configured by the customer for the remote service approach. This prevents misconfiguration, ensuring that company-specified secure remote access policies are always enforced.

Guarding Device Access
The customer must establish a Remote Service session to HEIDELBERG to grant their access to the dedicated computer within his network. To do so, a physical access is used to the device. Any remote service access needs to be established by the customer granting the HEIDELBERG service representative access to the extent desired by the customer. No unattended access is possible.
With HEIDELBERG's approach, the service representative has unprecedented access to the customer's computer to pinpoint and resolve technical issues more efficiently than ever before. Yet HEIDELBERG's approach leaves the ultimate control in the hands of the customer. The customer actively participates in the screen-sharing process and observes every step that is taken to resolve the technical issue. At anytime the customer can retake control of the mouse and keyboard or end the session altogether.

No "homeless" sessions - avoid inactivity
To compare the web-based HEIDELBERG approach to a "classical" dedicated modem line, the "plug" is always out! Only if the customer establishes a Remote Service session, the "modem" will powered on. The "modem" is kept on as long as the interactive service session takes place.

If a Remote Service session has lost the service representative the session will be closed immediately to avoid that broken communication could be hijacked by externals.

Access Notifications
Whenever a service representative arrives at customer's device by an interactive session, a welcome message is displayed on the customer's device screen. This notification ensures that the customer is always aware of the HEIDELBERG remote service session.

Ensure legitimate HEIDELBERG software by digitally signed software
During the first visit a secure plug-in will be downloaded to the customer's Internet browser to implement the remote service tools and access points.
All remote service executables are digitally signed. The software automatically keeps itself up-to-date. However, no component is ever installed or updated without checking signatures. This prevents "Trojan horses" from masquerading as legitimate HEIDELBERG software.

Virus checking
According to HEIDELBERG's Security policy every HEIDELBERG service PC is equipped with an up-to-date virus checker. If a service representative has to transfer any files from or to the customer site, those files will be checked by the virus software automatically. HEIDELBERG ensures that all technical measurements are done in order to prevent malicious software from spreading over the temporary switched path between HEIDELBERG and the customer's network. Nevertheless a local virus checker at any customer computer is highly recommended.

6 Protecting transmitted data

Strong Encryption
HEIDELBERG's remote service approach uses a highly compressed, encrypted stream to ensure data confidentiality without sacrificing performance. All traffic between the service representative PC and the customer's device, including screen images, file transfers, keyboard/mouse input and chat text, is protected with 128-bit SSL encryption. This type of encryption provides state-of-the-art security. (See glossary)
So the data is always protected during transmission.

Enforce encryption by unique session keys
Even a strong cipher is vulnerable if it does not use strong, confidential encryption keys. HEIDELBERG's service provider generates unique secret keys for each connection. The keys are valid only for one session.

7 Security from the Ground Up

Secure application provider
HEIDELBERG selected an Internet application service provider (ASP) to fulfill the communication services. This application service provider accepts the security policy and implements security at same or a higher level.

Secure Facilities
The communication services are provided through points of presence in various geographic locations. All facilities have on duty personnel, 24 hours a day and seven days a week. To gain access to any facility, one must be on the approved access list and then be authenticated by additional security controls.

Secure Network and platform
HEIDELBERG's application service provider's access routers are configured to watch for Denial of Service (DoS) attacks and to log denied connections. The security of the network architecture has been confirmed by penetration tests and vulnerability assessments. Servers have been penetration tested and system logs are continuously audited for suspicious activity.

8 Certified security

To ensure the highest level of security HEIDELBERG's solution provider has passed an external security audit and has been awarded a WebTrust seal of accreditation.

WebTrust is a seal awarded to web sites that consistently adhere to certain business standards established by the Canadian Institute of Chartered Accountants (CICA.ca) and the American Institute of Chartered Public Accountants (AICPA). Now globally recognized, these standards can be in the areas of privacy, security, business practices/transaction integrity, availability, confidentiality or non-repudiation.

The WebTrust Security Principle sets out an overall objective for the security of data transmitted over the Internet and stored on an e-commerce system. In the course of a WebTrust audit, the practitioner uses the WebTrust Criteria as the basis for assessing whether the Principle has been achieved.

9 Glossary

HTTP
The Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web . Relative to the TCP/IP suite of protocols (which are the basis for information exchange on the Internet), HTTP is an application protocol.

IP
Internet Protocol. The protocol used for transmitting IP datagrams within and between subnetworks in a (packet oriented) IP network environment.

Packet
A data packet consists of a sequence of bits and is used to carry information over a network. Every data packet has a well defined format, consisting of a set of bits in the beginning and end of the packet (source and target address, packet type, etc.). This information controls the transfer of the packet. A data stream is transformed into a sequence of packets on the transmitting side (fragmented). The packet sequence is then transformed back into a data stream on the receiving side (de-fragmented).

Protocol
In network terminology, a protocol is the formal description of the method and exchanged control information contained in the data exchange between two or more systems (for example IP, TCP, UDP, ARP, ICMP etc.).

Proxy Server
A Proxy server acts as a gateway between a computer in a local network and the Internet and is an application running on a computer that sits between a Web browser in a local network and a Web server in the internet. It can speed up the loading of commonly requested pages, since it can store (cache) a copy of them for retrieval. Proxy servers can also be used when security is a factor, such as from behind a firewall. (Firewalls are gateways that control traffic into and out of an organization's network.). In this case the proxy server acts as a gateway, allowing you to use the Internet, but not allowing unauthorized access to a private network.

TCP
Transmission Control Protocol. TCP is one of the core protocols in the Internet protocol family and provides a flow- and point-to-point controlled, connection-oriented, full duplex data transfer service. TCP sends its data packets via the IP Internet protocol.

Router
A system (computer) that uses a defined method to determine which path data packets should follow to get from the source to the target in an Internet environment. A router connects two subnets in the OSI network layer and forwards data packets between sub-networks.

Server
A station that makes available certain services (e.g. file service or print service) to other stations in an network.

10 FAQs

My print shop is already connected to the Internet. Do I have to implement any additional security measures before using HEIDELBERG remote service?

No. As described HEIDELBERG Remote Service uses state-of-the-art technology to provide a convenient and secure way to get service via the Internet. Nevertheless it is expected and recommended that the print shop uses the Internet by it's own security measures:

- Access restricted by a firewall
- Virus checking at the Internet gateway and at any computer
- Current security patches* installed in your network concerning OS and applications

*Patches will be checked in parallel by HEIDELBERG's application center for compatibility with HEIDELBERG products. If there are any problems, please contact your sales representative.

My workstations have no direct access to the Internet. We use a proxy server to control all traffic to the Internet. Do you support this configuration?

Yes. Using a HTTPS tunneling protocol our configuration supports typical proxy configurations.

I am afraid, that the support session could be used by hackers as a trapdoor to get access to my network. What can I do to increase my local security?

HEIDELBERG sees the risk, but is addressing it by a lot of security measures as described above to ensure, that only authorized HEIDELBERG service representatives use this approach. You could install a specific firewall rule to allow and trace all traffic between the HEIDELBERG service communication server and your devices in addition. This approach would log any activity twice, once at HEIDELBERG site, once on your site.

