HEIMDAL™
SECURITY

Heimdal™ Remote Desktop

Technical Paper

Author

Vladimir-Alexandru Unterfingher

Support your users anywhere in the world on both Desktops and mobiles *

- Support from dashboard-to-device and device-to-device
- Support Windows Servers, Windows Desktops, Android and MacOS *
- Secure connections with 2FA
- Content sharing
- Connect anytime and anywhere

'In-depth'

With our remote desktop product, which you can use stand alone or with any other Heimdal product component, as part of our UEM solution (Unified Endpoint Management) you can easily achieve remote support anytime, anywhere in the world by:

Features

- Supports connections from:
  - ☑ Dashboard-to-Heimdal Agent
  - ☑ Heimdal Agent-to- Heimdal agent
  - ☑ Dashboard-to-NO agent
- Support Windows Servers, Windows Desktops, Android and MacOS *
- Works via Application or via Web
- Secure connections with 2FA
- Attended / Unattended Access ie. End-user request or IT accessed
- Transfer Remote Session to other supporters **
- Invite other supporters to a session **
- Multiple sessions at once is supported
- Clipboard Sharing, Content Sharing and File Sharing supported
- Unlimited sessions **
- Locally-stored video session recordings

Security features

- RSA 2048/4096-bit public/private key exchange to negotiate a final symmetrical AES 256-bit end-to-end encryption

Cross-component features

- Works with our Privilege Access Management tool to raise elevations during sessions ***

Compliance

- Video Recording and Audit Log option

* Mobile support will be available in a later version
** Available in a later version
*** Needs force recording option. Available in a later version

Author
Vladimir-Alexandru Unterfingher

TABLE OF CONTENTS

1.

INTRODUCTION

1. Introduction

Heimdal™ Remote Desktop Technical Paper

The need for (secure) OTA, non-physical, server-mediated terminal operation has existed since the adoption of the T.120 point-to-multipoint communication protocol in the late '90s, replaced in 2006 by Microsoft's proprietary
Remote Desktop Protocol (RDP). With broad applicability, RPD services numerous industries (e.g. IT, education, business development, etc.), becoming the standard for OTA client support. Current historical conjectures, such as the COVID-19 pandemic have increased the users' dependency on remote assistance solutions. However, concomitantly, such circumstances have also compelled remote desktop service vendors and developers to quickly upscale the infrastructure in order to accommodate the ever-increasing demand for remote-based services. This sprint has left the existing RMD (i.e., remote desktop) framework vulnerable to any number of online cyber-aggressions. In an article published in August 2021, EC-Council has noted that in 2020 over.

Brute-force attacks, along with other initial access methods, have paved the way for ransomware and its metamorphic counterparts. Preventive measures may not be enough to counter these emergent threats. Considering the state of affairs, the complexity of malicious operations, and the pervasiveness of evil code, we require more application-level security measures to counter malware and malicious eavesdropping activities.

This paper represents a foray into Remote Desktop, application-level, security measures in the form of Heimdal™ Remote Desktop, a pay-per-use add-on developed by Heimdal™ Security. To fully comprehend the particularities of the Heimdal™ RMD (Remote Desktop) product, this paper has been divided into two major sections. The first will be dedicated to RDP best practices and communication protocol description, while the second will deal with the particularities of Heimdal™ RMD.

2.

REMOTE ACCESS COMMUNICATION.

INDUSTRY STANDARDS DIGEST.

2. Remote Access Communication.

Industry Standards digest.

Wherever remote access and control are concerned, RDP stands out, transforming into the verbatim synonym of OTA communication, collaboration, and control. Despite its time-honored merits, it is not the only way to establish a server-to-client remote collaboration session, and this preamble will highlight the various other RA (remote access) methodologies and specific communication protocols.

Irrefutably, Microsoft's RDP is the most cited RA approach. Popularized as an integrated, cost-free tool that enables real-time, Internet connection-dependent collaboration between a user and a supporter (i.e., the person who offers support to the end-user, either by request or as part of the company-enforced policy). Per the paper's introductory note, the Remote Desktop Protocol was adopted in the late '90s, having been built on top of the T.120 protocol. Furthermore, RDP is an extension of ITU-T T.128, the protocol that grants RPD its file-sharing capabilities. RDP has multiple channels and, in theory, can support up to 64,000 channels. Functionality-wise, Microsoft's proprietary RA approach facilitates the exchange of server output data, in the form of monitor display, and input data from the client (i.e. control peripherals such as mice, keyboards, graphic pads, etc.). By default, RPD data exchanges are secured by RSA's RC4 block cipher. In regards to the protocol's architecture, Microsoft's Remote Data Protocol is built on top of the Transmission Control Protocol (TCP), with four layers that mimic the vacillating OSI data transmission. The layers are ISO Transport Service (TPKT) with TLS and Encryption, TP-oriented X.224 with TPKT & FastMode DATA, T.125 Multipoint Communication Service with x.224, and, finally, encryption with T.125 Multipoint Communication Service.

Akin to its many peers, some of which will be covered in this section, RDP must and should make available the following features:

- Bitmap color depth support (e.g. 8-bit, 16-bit, 24-bit, 32-bit);
- NLA (Network-Level Authentication);
- Data-in-transit encapsulation and encryption;
- Audio and video redirection;
- File-sharing capabilities;
- Port forwarding and redirection;
- Printer redirection;
- Clipboard sharing;
- Miscellaneous (e.g. logging, audio and video session recording, session transfer, support for non-agent users).

Virtual Network Computing (VNC) is an open-source alternative to RPD, built upon the open simple Remote Frame Buffer (RFB) protocol that supports user-supporter data exchange via a network-dependent GUI. Despite its readily available source code, VNC has remarked itself as a short and mid-term alternative to Microsoft's RDP, accommodating both Windows and non-Windows operating systems. VNC can support data exchange in both screen and 'headless mode (i.e. server is not connected to physical display) and basic I/O features. RFB has some limitations – pixel-based display means less efficiency in cases where screen scaling, sharing, or higher resolutions are required, clipboard encoding, and support for some types of peripherals (e.g. mice with macro functions).

In line with proprietary remote access engines, Microsoft's DirectAccess is a serviceable alternative to VNC's open-source engine, RDP. DirectAccess RA is founded on the 'always on' principle, thus dissociating itself from the Virtual Private Network (VPN) model, which entails user consensus for connection initiation and termination. In DirectAccess, the server-client connection is initiated as soon as the machine connects to the Internet. Until the adoption of the Forefront Unified Access Gateway (UAG) in 2010, DirectAccess RA required intranet IPv6 deployment. In essence, Microsoft's DirectAccess enables users to connect with intranet resources, DA server, or to another DA user by utilizing the IPv6 over IPv4 packet encapsulation – reaching the intranet over the world-wide-web.

3.

HEIMDAL™ REMOTE DESKTOP

PRESENTATION AND PROOF-OF-CONCEPT

3. Heimdal™ Remote Desktop

Presentation and Proof-of-Concept

Heimdal™ Remote Desktop (RD) is the latest addition to the company's lineup and is designed to accommodate all remote support necessities. RD's Proof-of-Concept (POC) is based on three remote support scenarios:

1. **Dashboard-to-Heimdal Agent.** Signifies a remote access session initiated by a dashboard-using claimant to an end-user with the solution deployed on the machine.

2. **Heimdal Agent-to-Heimdal Agent.** Signifies a remote access session initiated by an agent-using claimant to an end-user with the solution deployed on the machine.

3. **Dashboard-to-no Heimdal Agent.** Signifies a remote access session initiated by the dashboard-using claimant to an end-user who doesn't have the solution deployed on the machine or if the equipment does not support the agent and/or components.

Based on the client-supporter interaction schema highlighted above, we can define two roles:

a. **End-user.** The supported party. Can approve or deny supporter-initiated RA session via the deployed Heimdal™ agent. Alternatively, it can be the recipient of an unattended RA session, initiated by the supporter through the dashboard or the local agent.

b. **Supporter.** The person offering remote, technical support to the end-user, following end-user's approved request or during an unattended session. Supporter role assigned via a CLAIM – an ACL that defines supported access and control dimensions (e.g. modify license attributes, simulate customer, edit API key, generate email reports, view customers, edit customers, delete customers, assume full control over customers, etc.). CLAIM-assigned supporter roles are assigned when operating under the Dashboard-to-no Heimdal Agent. In dashboard-to-Heimdal Agent and Heimdal Agent-to-Heimdal Agent scenarios, supporters can be assigned from the dashboard's Standard View.

Heimdal™ RD supports two session types – attended and unattended. In an attended session, the supporter-initiated session can commence only on end-user approval. Accounts for most of the remote support sessions, since it's the default type of connection, once RD is enabled in the GP.

Unattended sessions (i.e. based on a GP selection – enabling the corresponding tick box) are pre-approved (i.e., user not interrogated on session initiation) and mostly employed to force-push GPs, modify server-side configurations, uninstall unstable software on the end-user-side, or other jobs that do not necessarily require the user's approval.

RD Engine Presentation and Session Mock

Heimdal™ Remoted Desktop does not employ Microsoft's RDP remote access communication pathway by default. RMD digests RA requests and responses through a proprietary API via HTTP. This enables a 4-way communication lane for XML, POST/GET, and JSON(P). Fielding allows for country-centric settings, language, and default communication encoding.

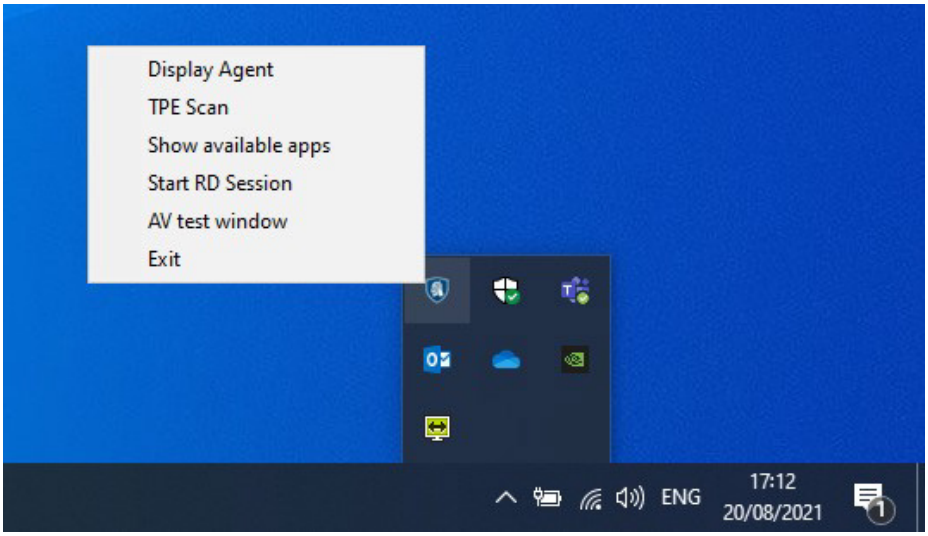
Furthermore, the API-mediated tunneling approach enables supporters to remote access a designated host who does not have the RMD agent installed on the machine. API-mediation is the most functional approach, serving multiple purposes: operating system interlacing (i.e., communication support between mobile and Microsoft devices, mobile-to-mobile, Microsoft-to-Mac, Mac-to-mobile), bandwidth load balancer, and asynchronous signal synchronization (PC-to-mobile). RMD's core is 'diatomic' – an endpoint-enabled service and a downloadable service.

The former is automatically installed on the end-user's machine on RD startup, while the latter can be deployed through the API whenever a dash board-to-no Heimdal Agent remote session takes place. The endpoint enabled service is required by RD to request a connection to the GP host and establish the session's authentication parameters (i.e., session uniquely generated password, name of target host, and session UID). The downloadable service is automatically downloaded and installed on the end-users machine after the supported generates a session.

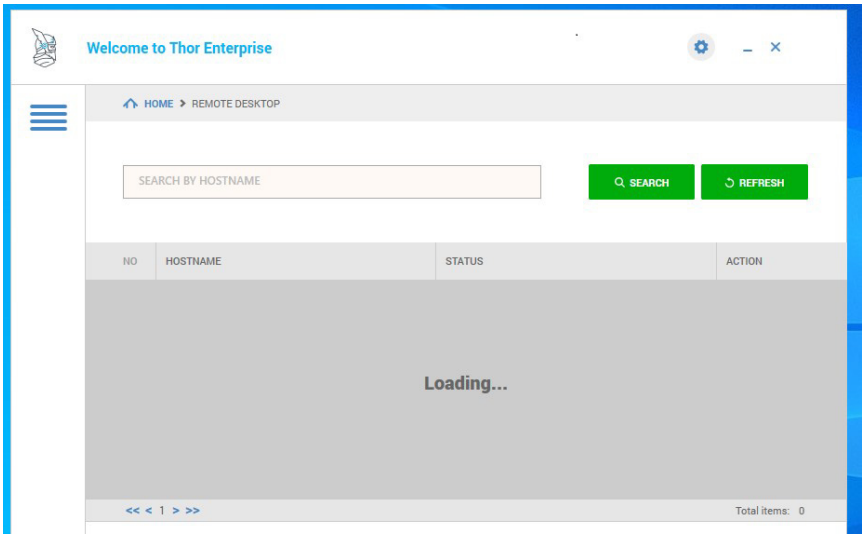
RD Sessions

This section shall describe, at length, the two types of RMD session generators: agent and dashboard.

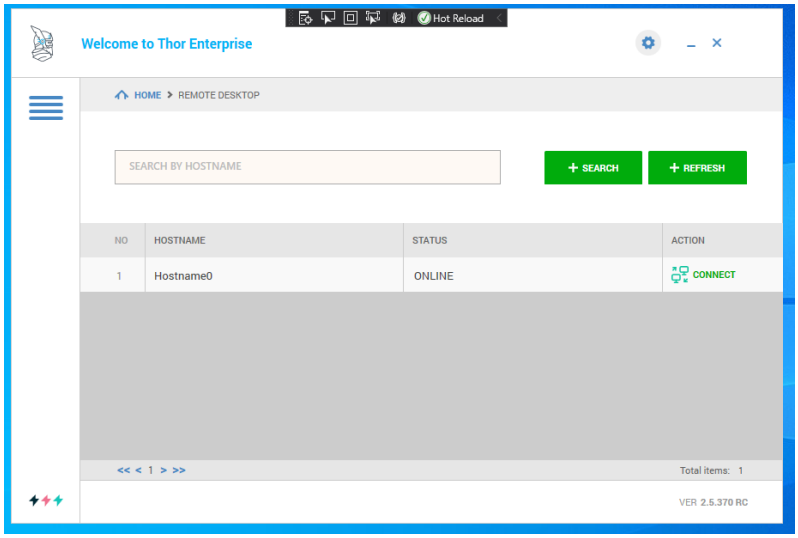
Agent remote sessions can be initiated from the Heimdal™ agent's context menu. From the remote desktop window, the user who, in our case, is a supporter, can select the hostname(s) from the group policy to which he claimed the supporter role.



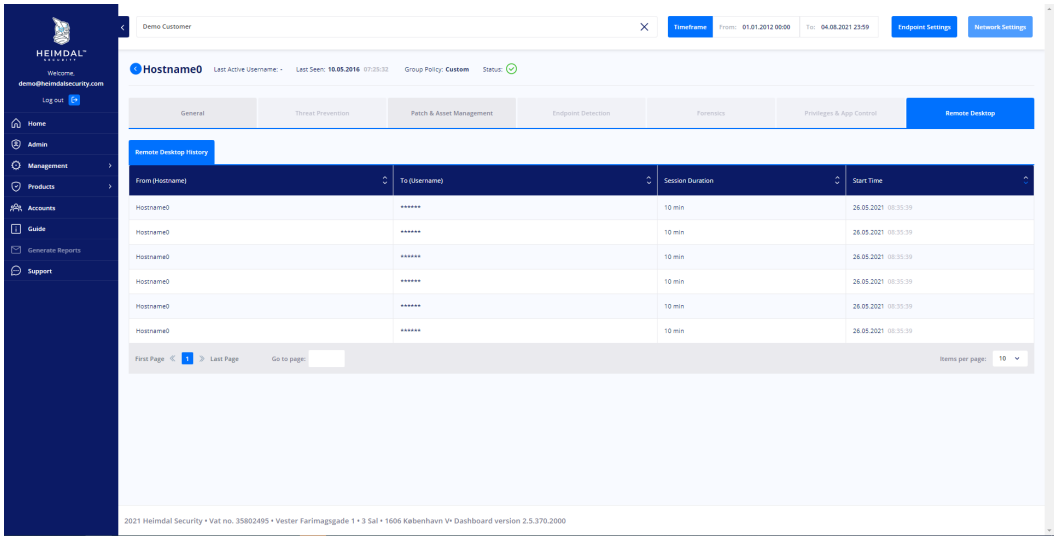
The supporter can search by hostname or refresh the list if it's not populated. Hostname machines that have been offline for the past 7 days will not appear on the hostname lists.



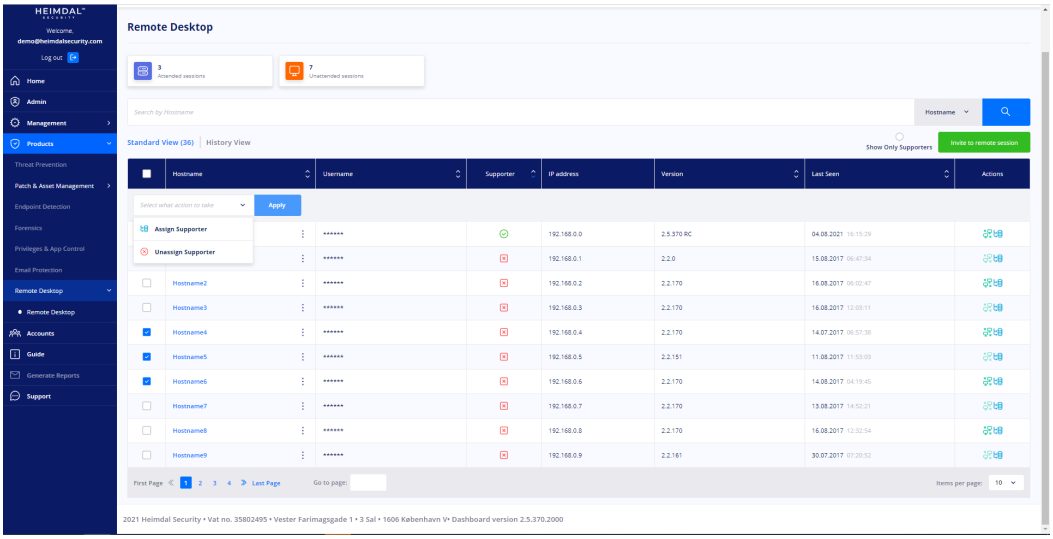
From the same menu, the supporter can connect to the end-user by clicking on the "Action" button located in the "Action" section/column. Agent-based remote sessions can only be initiated if the host has the agent installed on the machine or device.



Dashboard mode is employed when the supporter's machine does not have the Heimdal agent or the supporter prefers opening a session from the dashboard.

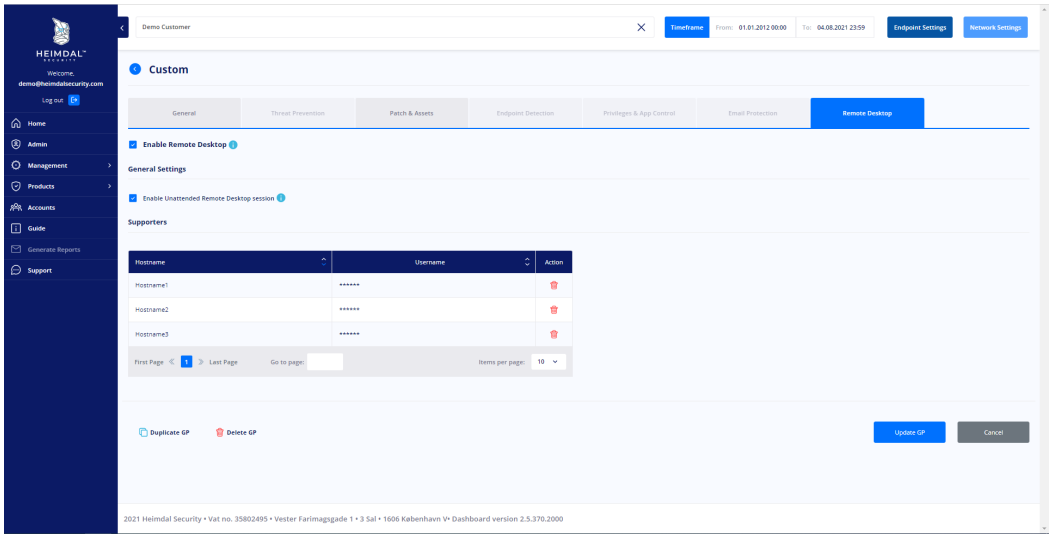


The supporter's dashboard contains information about curated host machines, hashed passwords, last session duration, and the associated timestamp(s). The client's history view aggregates info regarding the supporter's activity on the host or group policy since the supporter's association with the target end-user.

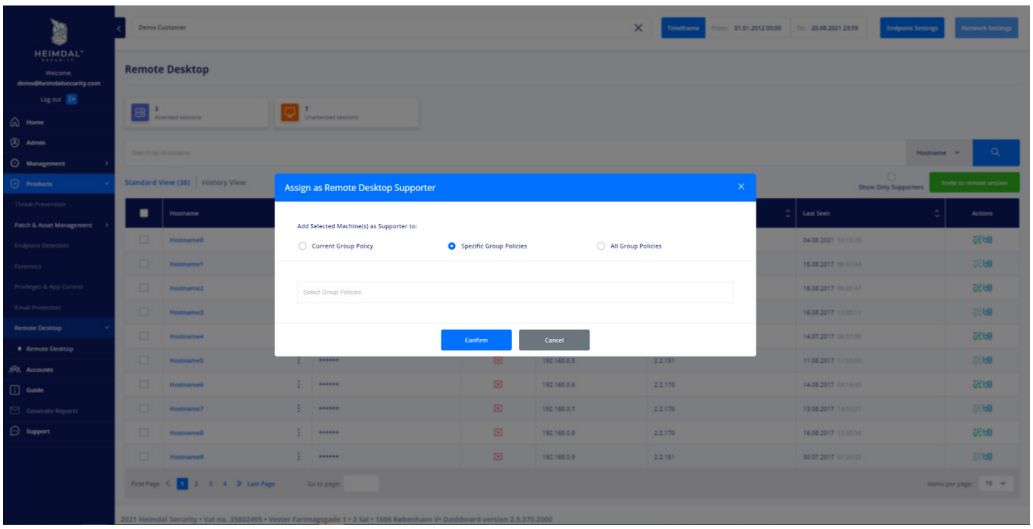


Additional controls are made available to the supporter – advanced sorting, hostname availability, filtering (i.e. after supporter or endpoints/ end-users), host's IP, software version, last seen timestamp, the "connect to hostname" or "manage a group for supporter/endpoint" buttons. Clicking on the connect button will start the remote session with the selected hostname. If it's an attended session, the end-user will need to consent to the RA request sent by the supporter.

This request will appear as a tooltip on the right-hand side of the screen or as a pop-up on mobile devices. If the supporter wants to initiate an unattended session with one or more hostnames from the serviced group policy, he must enable an unattended session from the dashboard and update the modified group policy.

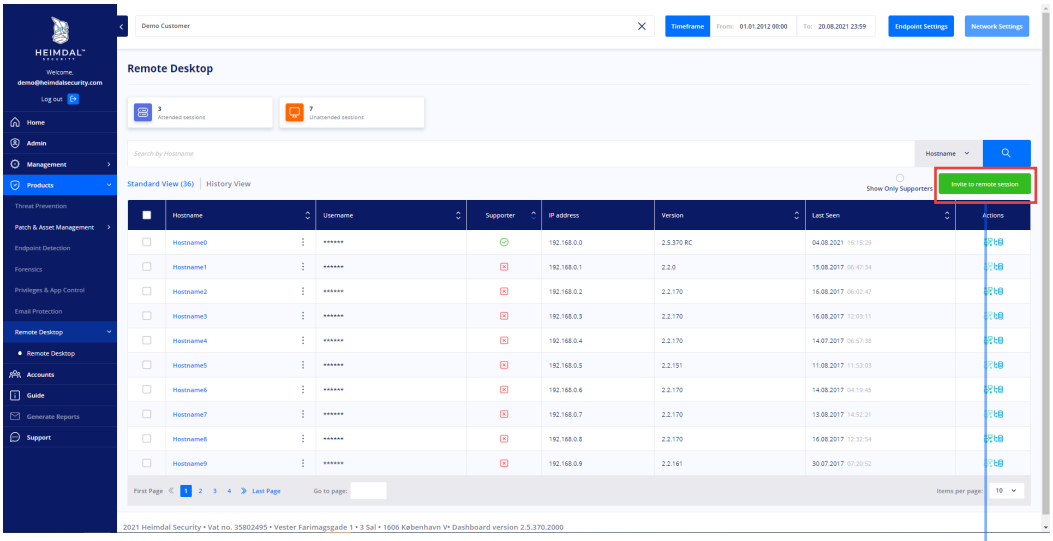


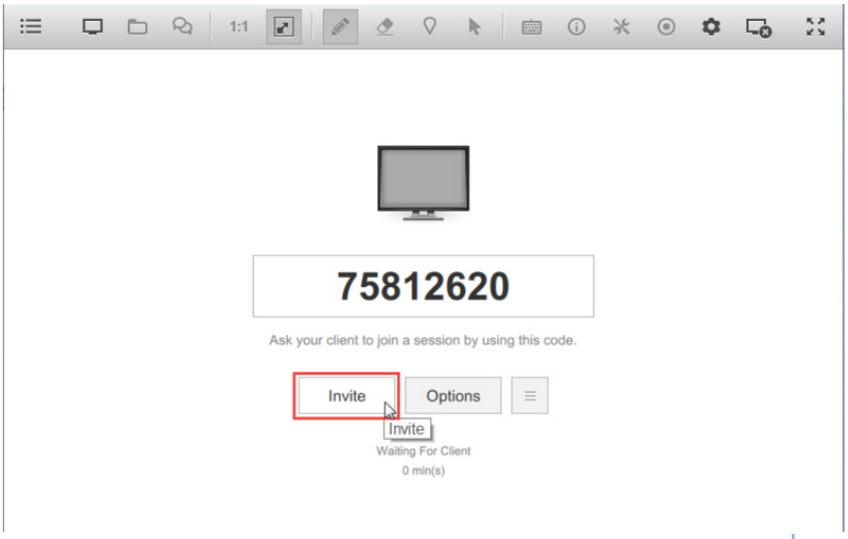
Supporters can be assigned to the group policy to which he belongs, to a specific group policy, or all group policies generated within the active customer.

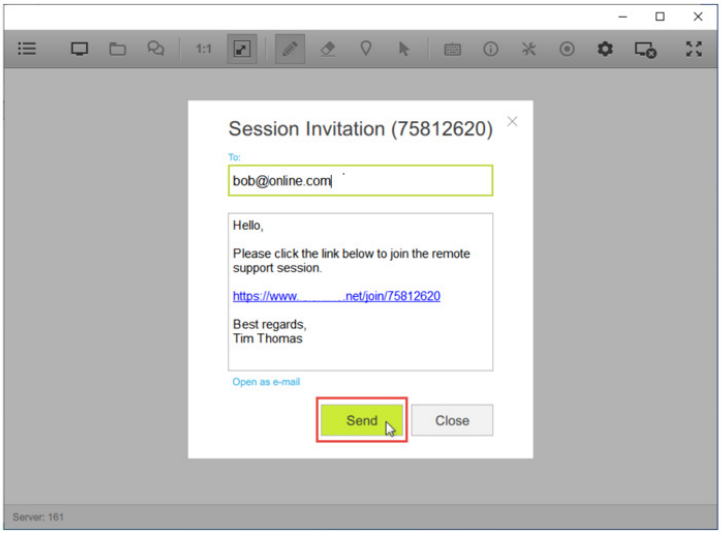


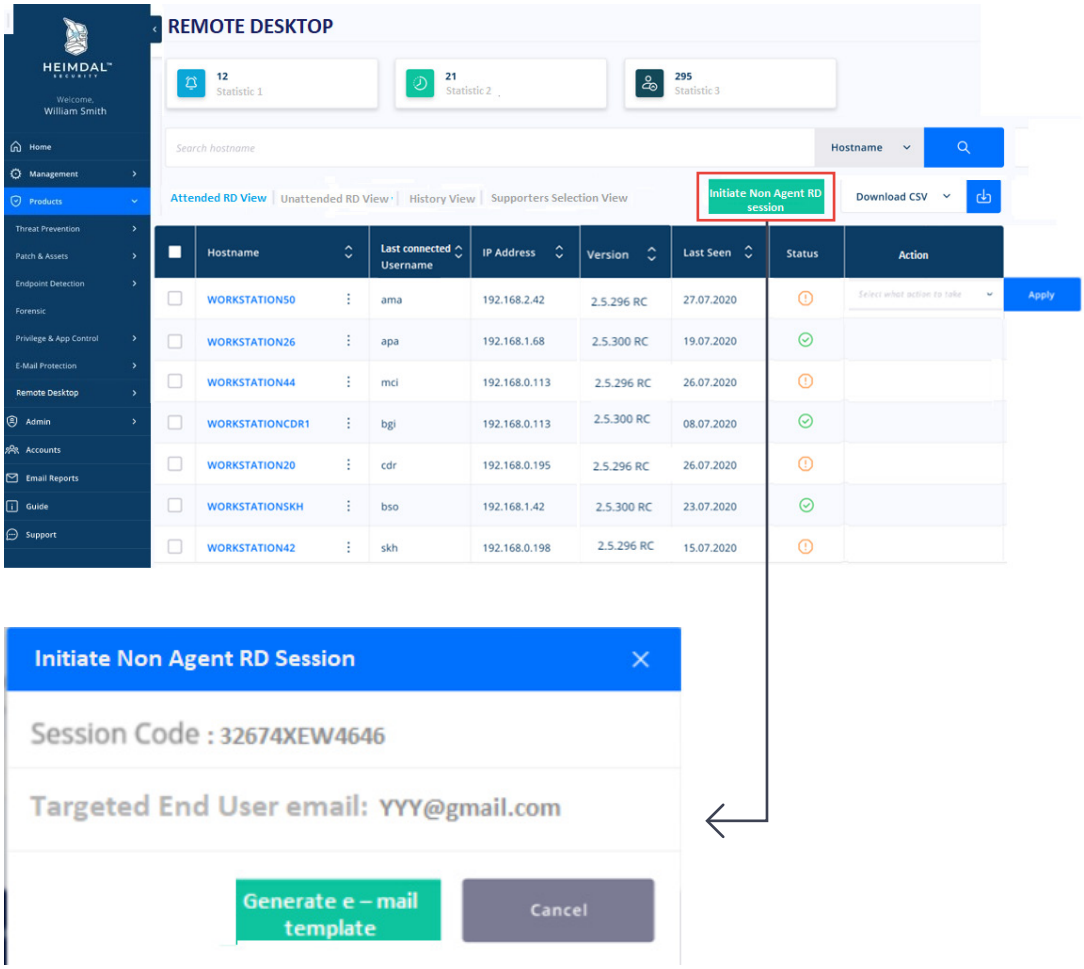
IT admins can revert one or more supporters to end-users by using the unassign supporte(s) command. However, it should be considered that this function removes supporters from all group policies, not just a specific one.

Attended remote sessions initiated by a dashboard-using, CLAIM-type supporter to the no Heimdal agent user can be initiated from the supporter's dashboard. To commence this session, the supporter is required to send the session's UID to the end-user by inputting the user's address in the "targeted end-user email" field. The mechanism is described in picture series below.


Remote Desktop
Invite to remote session
Standard View (36)
History View


75812620
Ask your client to join a session by using this code.
Invite
Options
Invite
Waiting For Client
0 min(s)


Session Invitation (75812620)
To:
bob@online.com
Hello,
Please click the link below to join the remote support session.
https://www. net/join/75812620
Best regards,
Tim Thomas
Open as e-mail
Send
Close



The supporter will be redirected to the user invite API page where he will be able to send the invitation code or adjust the remote-control session parameters. The session invitation will require additional personalization (i.e. target's email address and an invitation template). The end-user will be able to join the remote session upon accessing the link in the received email. At the same time, the API will silently download and install the light service on the target's machine or device so the tunneling operation can be completed.

4.

SECURITY AND FEATURES

4. Security and features

OTA transmission for RMD is supported by RSA 2048/4096-bit public key exchange. Pre-ignition is built on the Diffie-Hellman exchange to safeguard confidentiality and non-repudiation. The initial public key exchange will later be used to negotiate a symmetrical AES 256-bit session key. Furthermore, a validated supporter can enforce additional safe communication countermeasures such as multi-factor authentication (MFA) via mobile app or email.

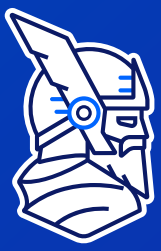
Features supported by Heimdal™ Remote Desktop:

- Multi-sessions. A supporter can initiate two or more remote sessions from the dashboard or agent.
- Transfer remote session. A supporter can transfer the remote session to another supporter. The second supporter must be validated and appointed supporter in the same GP as the first supporter. (please insert footnote: “available in a later version”)
- Invite additional supporters. A session can support more than one supporter. Only a supporter can invite additional supporters. (please insert footnote: “available in a later version”)
- Screen sharing. In-session screen-sharing options include keyboard and mouse control and tweaking the streaming quality.
- File and content sharing. A record of the transferred files will be available Video Recording.
- Enforce video recording for active sessions.
- Audit log. At session end, a backlog is made available.

5. Conclusion

Heimdal™’s Remote Desktop is an integrative approach to remote support and access technologies. Over the web or from the agent, the solution can be utilized to resolve various IT support needs. Privileged Access Management (PAM) integrations enable the supporter to assume full control over the session, without having to circumvent company-enforced policies.

RMD’s security features ensure data integrity, making the connection impervious to malicious eavesdropping, packet capture, hash reverse-engineering, or Man-in-the-Middle attacks. AC and PAM features can also be added to Remote Desktop, for extra security and logging. The product may be associated with digital forensics tools, IDS, or IPS systems.



HEIMDAL™
SECURITY

Leading the fight against cybercrime.

Vat No. 35802495, Vester
Farimagsgade 1, 2 Sal, 1606 København V