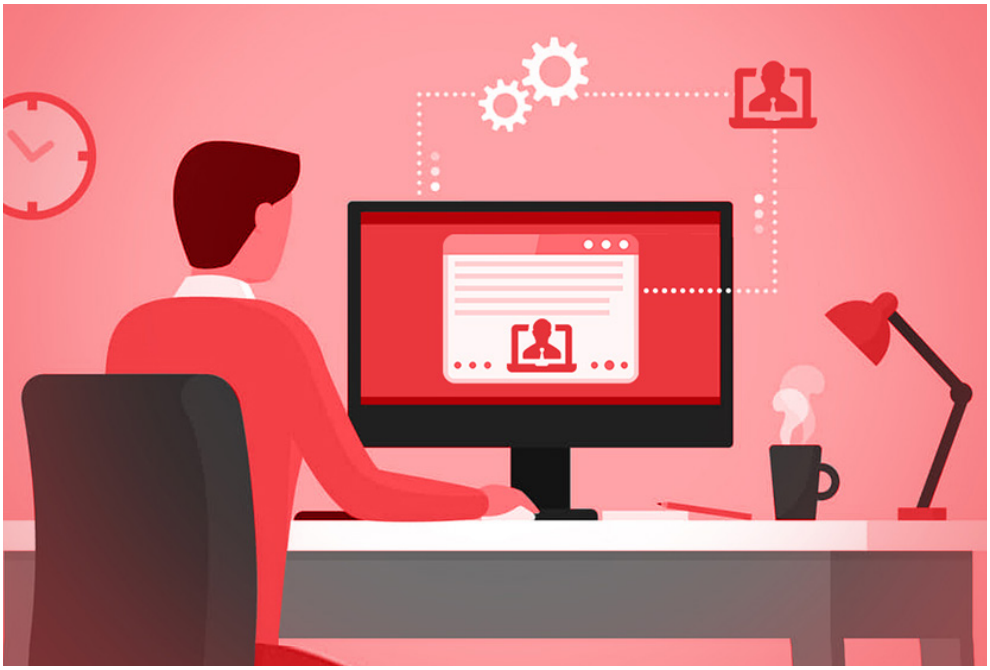
ARCON | Remote Assist



This paper discusses how the IT administrators can address a challenge: How to ensure seamless management of all the endpoints within and outside the enterprise network. ARCON | Remote Assist is a robust solution that helps the IT admins to effectively attend the end-users' request.

Table of content

1 Overview

2 The risks

3 What is ARCON Remote Assist?

4 Features

5 How Remote Assist works?

6 Conclusion

Overview

The IT administrators typically have a very busy day in the office. They have to administer day-to-day IT operational, administrative and datacentre tasks.

Furthermore, the IT admins have to address many problems encountered by the end-users. For example; troubleshooting a helpdesk request among other requirements associated with the desktop management. It's a challenge for the admins. Think about a situation in a typical large-scale enterprise set-up with lots of desktops. An admin will have to address problems from one desktop to another. This 'troubleshooting' approach will not only be time-consuming; hence, unproductive, but it can also result in process backlogs.

The major concern of the admins is indeed the lack of enough time. The admins have to take care of so many things apart from the end-user assistance that they hardly have enough time to attend every request, and thus they end up working for more hours and sometimes even over the weekend.

Moreover, in the wake of increasing work-for-home culture, today's enterprise requires a mechanism to ensure seamless desktop management in a remote environment.

To overcome this challenge, ARCON Remote Assist is an effective solution. The solution offers the admins seamless mechanism to administer all the endpoints; and attend end-users' requests, both within and outside the network. The solution offers combined capability of privilege elevation and delegation management within or outside the enterprise network as well.

The risks: When an IT admin has no remote assist solution

In addition to IT administrative delays, the absence of a remote assist tool can also increase security threats. Some of the risks can be as follows:

Credential's misuse:

Generally, the admin credentials of all desktops are the same. Hence, it poses a major security risk as if an end-user comes to know the admin credentials, then he can access any desktop in the organization.

Shared Passwords:

One Administrator ID is shared between multiple IT admins. Thus, if something malicious activity takes place, there is no accountability for the same.

No audit trail:

There is no record or logs maintained for any activities related to the support offered by the Admin to the end-user. This could lead to a greater insider threat arising from the lack of maintaining audit trails.

What is ARCON Remote Assist?

ARCON Remote Assist is an effective IT solution that enables the administrators to manage any on-boarded desktop either remotely or in the network. It enables the IT admins to troubleshoot any machine within and outside the network.

The solution enables the administrators to elevate admin rights, privileges, change passwords, access related tasks for the end-users in a controlled environment.

Thus, ARCON Remote Assist ensures a timely resolution of desktops' problems, no process backlogs, and productivity enhancements.

The solution offers superb and effective administrative controls to mitigate IT risks as well. By deploying ARCON Remote Assist, the enterprise will be able to:

By being on top of everything:

Ensure security updates and reduce downtime as the solution will offer complete maintenance to all the endpoint systems as well.

Auditing & record keeping:

Track and maintain records and logs in detail of all the processes and support offered throughout the day.

Key-Features of ARCON | Remote Assist

Single Interface

A single management platform is used to manage multiple systems and connections. It simplifies the tracking and reporting of the remote assistance activities performed on each and every system, thus implementing an efficient process in complying with security obligations.

Controlled Access

Application Restriction and Elevation can be implemented to have better access control on end users working in different remote locations. Furthermore, Dash boarding can assist in investigating anomalous behavior of the users in real-time.

File Transfer

Files can be transferred between the target system to host system. When a requestor initiates a file transfer, the service provider can accept or reject the file transfer process and vice versa. Once the transfer process is complete, the session can be disconnected.

Audit Trail

Video logs and reports are generated for each and every remote assist session. Video logs form a detailed audit trail and provide material for session analysis and training purposes.

Process Elevation

Administrators can elevate a particular process based on the customized requirements of the end-users. If a particular end-user needs access to an application, the Administrator can elevate that particular application for the specified user without entering the administrator password. Critical applications can be elevated when required. Administrators don't have to share privileged credentials with end users or the IT staff, thus helping to follow the basic principle of least privilege.

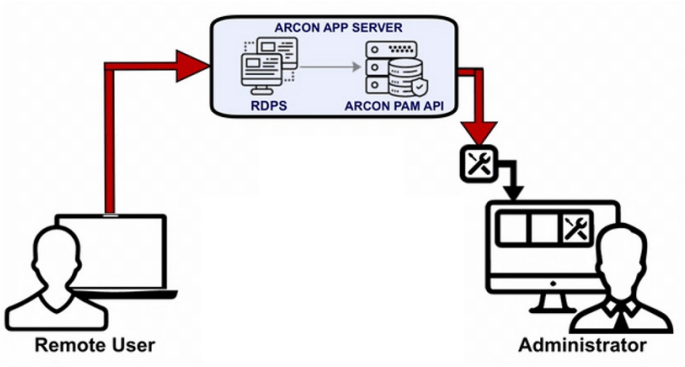
Password Rotation

Administrators can remotely enable password rotation on the end-user systems through remote assist. Password rotation on end-user systems can be ensured with one click and with least human intervention even as it keeps a check through password checkout flow.

How Remote Assist works?

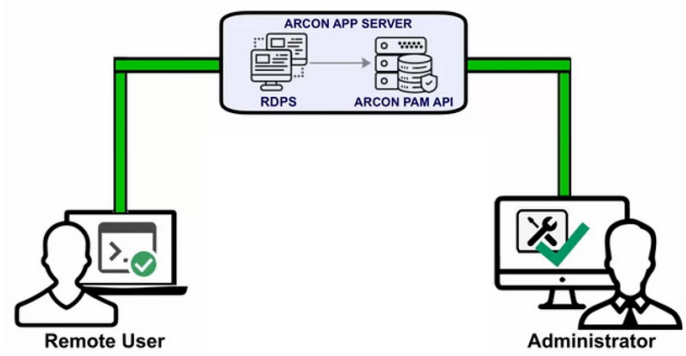
Step 1.

End-User Raises a Connection Request and the request is added to the Administrators' Queue



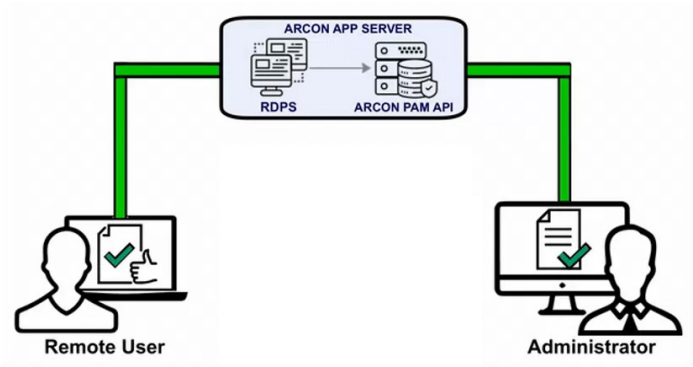
Step 2.

The Administrator Accepts and a Connection Request Prompt is sent to the User. Once accepted by the user, Connection is established



Step 3.

Admin can now control the users' screen with elevated rights.
Post Resolution, the session can be disconnected with a comment



Conclusion

For the IT administrators, to be omnipresent is not possible; yet, they have to be on the top of everything. ARCON Remote Assist ensures all end-users' requests are troubleshooted by the admins with ease.

Benefits include:

- The ADMINs and end-users stay productive and efficient in their day-to-day tasks
- Enterprise has a mechanism in place that would enhance remote desktop management in a controlled environment
- Privilege elevation on demand that helps both complying with the IT standards and enforcing the principle of least privilege

About ARCON

ARCON is a leading enterprise information risk control solution provider, specializing in Privileged Access Management (PAM) and continuous risk assessment solutions. Our mission is to help enterprises identify emerging technology risks and help mitigate them by robust solutions that predict, protect and prevent.

PAM: ARCON | **Privileged Access Management (PAM)** is a highly effective solution that helps in managing, controlling and monitoring privileged user activities. The solution provides IT security team with a centralized policy framework to authorize privileges based on roles and responsibilities ensuring rule-based restricted access to target systems.

UBA: ARCON | **User Behaviour Analytics (UBA)** is a highly effective risk predictive & analytics tool built for daily enterprise use cases. It breaks the traditional approach of 'restrictive' access and is capable of crunching large lakes of enterprise data, spot anomalous activity and trigger alerts in real-time.

SCM: ARCON | **Security Compliance Management (SCM)** allows an enterprise to prioritize security and compliance efforts based on risk level. The tool enables continuous risk assessment for critical technology platforms and ensuring desired compliance levels.

Connect with us

All rights reserved by ARCON
This document or any part of the document may not be reproduced, distributed or published in any form without the written consent of the copyright owner under any circumstances. Any kind of infringement in the owner's exclusive rights will be considered unlawful and might be subject to penalties. This document was made in good faith with all the available information at the time of publishing. For the latest updates, please get in touch with our sales team.