

Predict | Protect | Prevent

**ARCON|PAM**  
New Features for U16 SP1

# Table of Contents

1 Web Portal .....	4
2 Connectors .....	5
3 General .....	6

This section describes new features that were introduced in ARCON PAM U16 SP1.

## 1 Web Portal

New Features that are added in ARCON PAM Web Portal are as below.

### Multiple IP search functionality

Users can now search more than one IP with one after the other comma-separated (no spaces).

1. Login to ACMO
2. Select Report
3. Search Device Detailed report.
4. Enter IPs comma-separated and it will fetch details accordingly.

### Service connect via AGW

The following features have been added when a service is connected via AGW.

1. The remote session resizes based on the window size of the browser tab.
2. Reconnect button option
3. Disconnect button option.
4. Keyboard- Text typed is sent to the remote session.
5. Clipboard- This allows to copy-paste text from or into remote sessions.
6. File Transfer- Allows to upload/download files to/from a particular folder.

## 2 Connectors

New connectors added in ARCON PAM are as below.

ARCON PAM now supports the following connectors as well:

- **Sonicwall RAP**
- **Vmware Horizon:** Field 4 tags: <url> - For adding url field
- **Sonicwall NetExtender**

### Integration of SSH MySQL deployed on RDS

Integration of SSH MySQL has been deployed on RDS. You can now create a service for SSHMySQL with input 50 and above characters in hostname or domain.

## 3 General

New general features are as below.

### **Administrative Console on web**

The administrative console which includes creation, deletion, modification and assignment of LOB, User Group, Users, Server Group, Services has been moved to the web from the previous Server Manager.

### **ARCON|CLIProxy**

This module allows the end user to take a SSH connection from any third party client like MobaXterm, SecureCRT, etc and still be controlled. The user need not use the ARCON|PAM web portal to login but alternatively use these applications directly to login to the CLI Proxy using the PAM userid and password. IT is very useful for integration with bots and other automation tools to take a server session programatically.

### **Offline Vault**

The offline vault feature is unique to ARCON | PAM and allows users to connect to target devices even when they are not in the core orgnaization network. This is generally the scenario with organizations with distributed architectures like telecom industry, power industry, oil and gas companies, etc. Such organizations generally have a lot of connectivity touch points like BTS devices for telcom companies which are not always connected to the core network. These touchpoints generally pose a security threat as they are generally placed across a large geography and are huge in number. Hence, organizations end up having the same passwords for privilege ids across these systems. Also, field engineers are used to connecting directly to these devices through the console and hence their access is not monitored or recorded and hence cannot be audited. ARCON | PAM has come up with the capability to allow the end user to check out access to such devices. The password for these are checked out by the user from pam and stored in a thick client provided by ARCON on their respective laptops. This thick client allows a user to take a connection to the target device by using the checked out password(inaccessible to the user, stored in an encrypted manner). This allows the user to access the device without knowing the password and also store video logs of the entire activity performed by the user on the target device. These logs can be synced to the PAM system once the user connects to pam or is connected to the core network. PAM also has the capability to restrict access of the user if a certain threshold is attained, like he has accessed more than 25 sessions on target devices without syncing information back.

### **Mobile applications for approvals**

ARCON|PAM has launched its on application for android phones for different workflow(service access request, password request, user creation, service creation, user-service mapping, etc) approvers to be able to approve requests on the go. Previously, they needed to login to the ARCON|PAM portal to be able to approve requests.

### **Cloud Governance**

In a multi-cloud context, ARCON | Cloud Governance can find entities, resources, and their permissions. With a consolidated dashboard, key measures and suggestions are available on a single screen across multi cloud environments. The dashboard displays the total risk score for the whole cloud environment of the organization. It gives you a clear picture of the riskiest cloud entities as well as recently added IAM entities across several workspaces. It assists the administrator in monitoring the high-level resource distribution of VMs, Databases, Containers, Storage accounts, and Virtual Networks across workspaces, and it drills down to platform-specific services and their region-by-region distribution.

Privileged Access Management Suite



No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means such as electronic, mechanical, photocopying, recording, or otherwise without permission.