



[UPDATE] Devolutions' PAM Platform for SMBs



AT DEVOLUTIONS, WE ARE ON A MISSION TO SOLVE THIS MAJOR PROBLEM FACED BY SMBs.

As you may have discovered, current Privileged Access Management (PAM) solutions in the marketplace are typically quite expensive, and therefore unaffordable for most small and midsize businesses (SMBs). Furthermore, it is difficult for many SMBs without in-house technical expertise to

understand the differences between core requirements and non-essential parts of a PAM solution.

At Devolutions, we are on a mission to solve this major problem faced by SMBs. To that end, we have worked closely with two well-known analyst firms, and **we are on target to deliver a robust Privileged Access Management (PAM) platform specifically designed for SMBs by November 2019.**

This platform will “democratize” PAM by making it affordable and accessible to SMBs everywhere. It will fulfill all core requirements, while reflecting Devolutions’ signature commitment to performance, usability, security and support.

Highlighting Core Requirements

One of the big challenges in the PAM marketplace is that different analysts and vendors use various non-standardized PAM terms, and they also rank and prioritize features according to their specific products and perspectives. Thankfully though, with the emergence of wide-reaching privacy and security regulations, there is a growing consensus regarding what constitutes the minimum requirements for a functional, robust and legitimate PAM platform.

With this in mind, we present the following series of tables. Here is how to interpret them:

The left column entitled "CORE" indicates with an asterisk whether there is a consensus in the market that the specified feature is a core requirement of a PAM platform. For example, in the Information Vault Table, the feature "Role Based Access Control" has an asterisk in the "CORE" column. This means that most experts see this as a fundamental feature rather than an optional feature.

The right column entitled "AVAILABLE" indicates which of our current and/or planned products meet these core requirements. There are five possible options for this column:

- ALL: the feature is available in all of our product offerings
- DPS: the feature is available with Devolutions Password Server
- DPS-PAM: the feature is available with the recently released DPS 2019.1
- DPS-PAM-Q2: the feature is planned for the end of Q2 in 2019
- DPS-PAM-Q3: the feature is planned for the end of Q3 in 2019

For example, in the Information Vault Table, the feature "Automated Credential" displays DPS-PAM in the "AVAILABLE" column. This means that the feature is available in DPS 2019.1.

Information Vault

At the heart of a PAM platform is the Information Vault, which is a secure storage system for credentials, along with many other kinds of sensitive data (e.g. alarm codes, software keys, corporate credit card numbers, etc.).

Feature	Core	Available
Role Based Access Control	*	ALL
Active Directory Integration	*	ALL
Secure Access to Privileged Credentials	*	ALL
Automated/Manual Credential Check In/Check Out	*	ALL
Automated Credential Rotation	*	DPS-PAM
One-Time Passwords (OTPs)		ALL
Approval and Emergency Access Workflows	*	DPS-PAM
Reporting on Privileged Credentials and Usage	*	DPS-PAM-Q2
Logging Information Protected from Tampering	*	DPS-PAM-Q3
Flexible Notification System	*	DPS-PAM-Q2
Syslog Notifications		DPS

Other notable features:

We are also looking into account provisioning workflows, as these are increasingly being viewed as essential components of a PAM Information Vault.

Discovery

Discovery focuses on tools to identify accounts and devices that are registered or found running within an infrastructure.

Feature	Core	Available
Active Directory Account Discovery	*	DPS-PAM
Active Directory Device Discovery		DPS-PAM-Q3
SSH Device Discovery		DPS-PAM-Q3

Session Management

Sessions are connections to a system/device that require remote access technology (RDP, SSH, web page, etc.). Session management also functions as an identification mechanism, which could be complex and/or composed of multiple factors.

Feature	Core	Available
Divulgence of Credentials to Manually Establish Sessions, Typically Followed by Triggered Password Rotation	*	ALL
Automatic Session Establishment Using Account Brokering (i.e. passwords are not exposed to users).	*	ALL

Other notable features:

We are also looking into Session Accompaniment and Termination (four-eyes principle) and are offering this with our Wayk Now proprietary remote access protocol.

Session Recording and Monitoring

Various analysts and vendors bundle Session Recording and Monitoring with Session Management. In our experience though, we have concluded that **all** SMBs would benefit greatly from using Session Management, whereas only a small percentage have the resources (material, financial, or human) to put the complex infrastructure in place required for Session Recording, and then to review the sessions in-house.

Additionally, we have discovered there are different rationales for recording activity. Analyst firms typically ignore these differences, as they are focused on large enterprises. However, since they matter to SMBs, we take them into consideration.

Justification	Description	Available
Individual self-protection	A contractor will record his or her activity in order to be able to prove the actions that were carried out during a session. This is shared with the customer (internal or external) only when a complaint is received. Recordings are not automatically protected from mishandling, as the contractor does this him or herself.	*
Organization protection	Recordings are required by the organization. Mishandling is only protected against malicious breaches by end users (not administrators).	DPS-PAM-Q2
Regulatory mandated	Recordings are needed by the organization in order to meet an external compliance requirement. Recordings are protected against tampering by end users and administrators.	DPS-PAM-Q3

Feature	Core	Available
SSH Session Activity Recording	*	ALL

Other notable features:

We are evaluating Keystroke Logging in Windows Sessions and the option to List Opened Windows in Windows Sessions, which we would offer through our Wayk Now products.

Application to Application Password Management

Just like large enterprises, SMBs need to ensure that passwords are not stored in scripts or transferred to applications using a mechanism that makes it possible for credentials to be divulged. Our DPS product offers a REST API paired with a Python SDK, plus we have enabled a limited Command Line Interface (CLI) for DevOps scenarios. Although the category is core, having one of the two is sufficient in order to be compliant.

Feature	Core	Available
REST API	*	DPS
CLI (full featured)	*	DPS-PAM-Q3

Looking Ahead

We are confident of meeting our November 2019 target for delivering a robust yet affordable PAM platform that gives SMBs the security, flexibility, and ease-of-use they need to protect privileged accounts and sensitive information, tools and networks. We will be sharing additional updates in the coming months, and we invite your feedback.