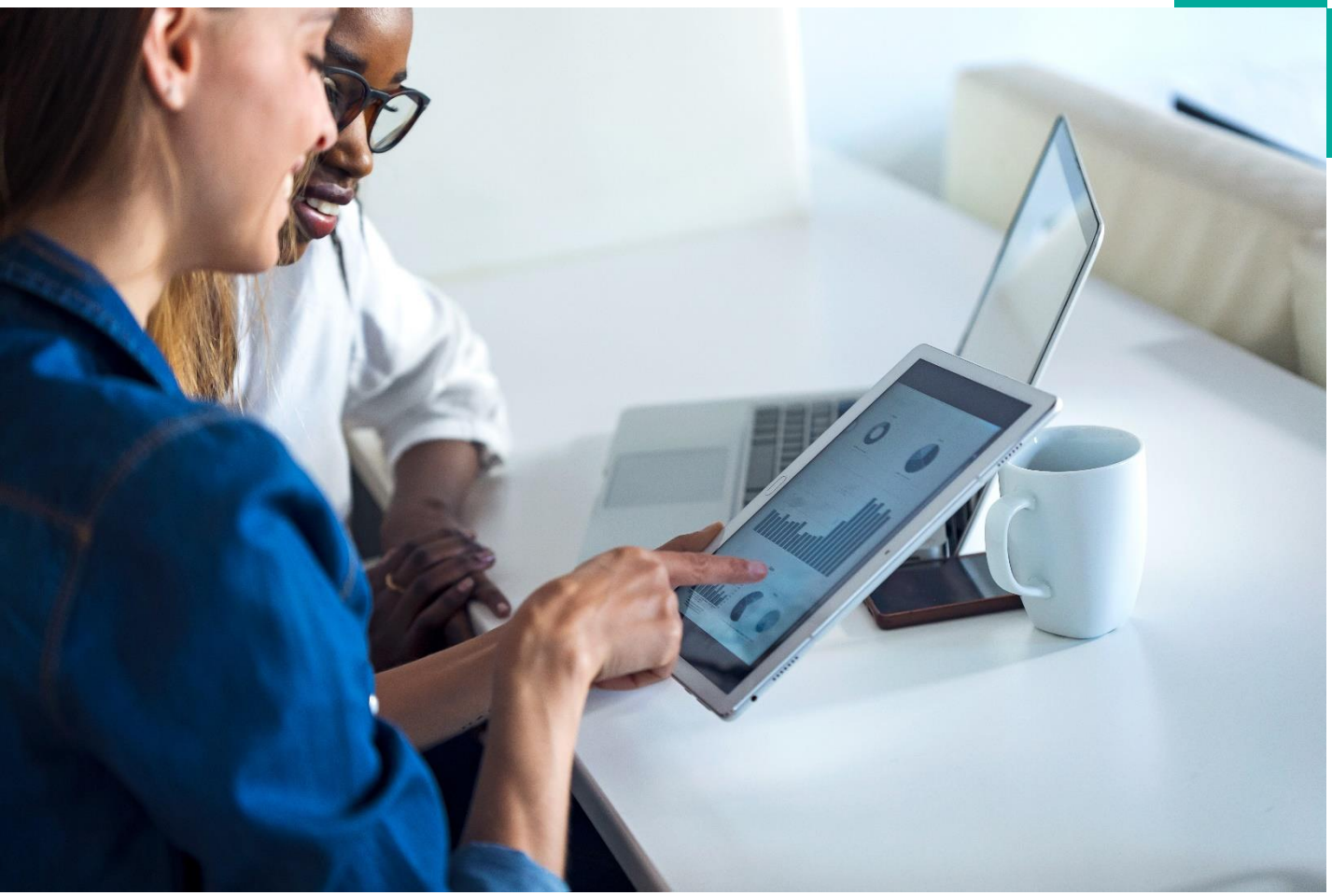


Self Service PIM

The Affordable Self Service Privileged Identity Management Solution

In any IT environment, **privileged accounts are everywhere**: IT administrators, privileged users, external vendors, and business applications all use them to access critical information systems in your network. They are **high value targets for cyber criminals** because the elevated permissions allow them to navigate through your environment undetected, to access highly confidential information and to make administrative-level changes to mission critical applications and systems. Furthermore, when IT admins don't know what employees are doing with their privileges, malicious insiders can abuse their position without anyone noticing. To win this battle, both inside and outside your organization, you need a solution that **protects**, **tracks**, and **manages** all your privileged accounts.
Reducing the amount of these overpowered accounts is the first step to redemption.
Making sure that privileged accounts are only valid for a restricted period is the next.
This is where **Self Service PIM** comes into play.

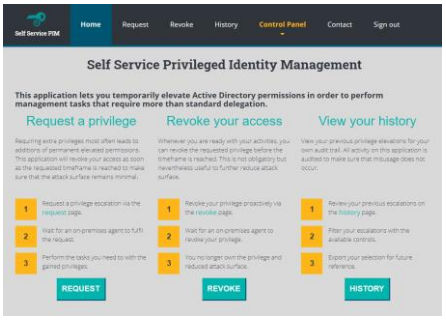
SSPIM (Self Service Privileged Identity Management) is a mechanism that will enable authorized users to elevate their permissions to a higher level. A higher level of permissions is obtained with the help of AD group memberships. SSPIM will for example enable users to obtain full control access over an Organizational Unit by adding those users to a group that was given these permissions (via delegate control for example).
SSPIM is available for both Active Directory and Entra ID and is based on group memberships. These environments can contain multiple forests, domains, and tenants.

Self-Service PIM
How does it work ?

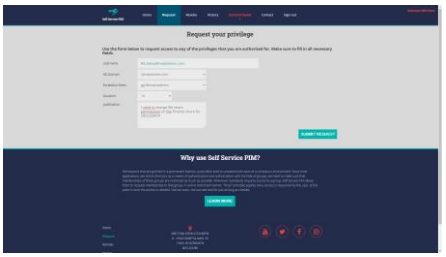
Positive flow Self Service PIM

Self-Service PIM is comprised of 3 main components:

- A cloud hosted Admin console to define which users can get what privileges for a given duration
- A cloud hosted web application that allows users to request privilege escalation
- Onprem agent(s) that will fulfil escalation requests (only for Active Directory plan)



Home Page



Request a privilege escalation

The web application and administrator console are cloud-based SaaS applications, hence fully managed by Inetum-Realdolmen. The web application has no direct ties into the customer's physical infrastructure. The only notable integration with the customer's environment is integration with the Azure Active Directory tenant for authentication and authorization purposes.

All privilege escalations are audited, and auditing information can be queried dynamically using the Admin console. Admins can schedule audit information receival to their own likings.

Self Service PIM can be ordered via the Azure Marketplace.

What's the value of Self Service PIM for your business?

Decreases your attack surface	Easy to onboard	Easy to use	Affordable	Insights
Getting the number of privileged accounts under control dramatically reduces the opportunity for cyber attackers	Link with your Azure AD, install an agent on any member server (Active Directory plan only), and you're up and running	An intuitive GUI will let the Admin specify fine-grained privileges that users can get for a given duration. Claiming your privileges is as easy as browsing to the cloud hosted web application.	No fancy features: we choose to focus on the functionality you really need. This allows us to offer you an excellent PIM solution at an affordable price.	Get insights (again) on when users need extra privileges to perform their day-to-day work, and where you can improve even further with delegation of control.

WANT MORE INFORMATION?

Contact our experts with any questions, suggestions, or challenges. We are looking forward to informing you about other Azure or Identity services Inetum-Realdolmen can offer.

INFO.SSPIM@INETUM-REALDOLMEN.WORLD

Inetum-Realdolmen HQ – A. Vaucampslaan 42, 1654 Huizingen, Belgium | +32 2 801 55 55
info.sspim@inetum-realdolmen.world