



OSIRIUM PEM

Overview of Privileged Endpoint Management



Privileged Endpoint Management An Overview

The proliferation of administrator accounts on end-user's workstations and laptops or end-user accounts that have administrator rights is a major security risk. These accounts can be used by attackers to breach cyberdefences. Removing these rights is a common goal, but usually means an increased load for the IT Help Desk dealing with requests to install software or make configuration changes.

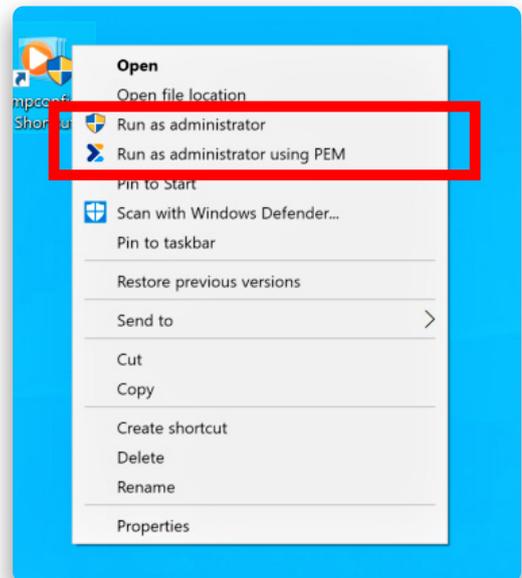
With Privileged Endpoint Management (PEM), IT can remove local administrator accounts and rights without increasing requests to the help desk.

Elevate Applications Not Users

PEM allows IT administrators to create policies, stored in Microsoft Active Directory as Group Policy Objects (GPOs), determining which applications can be run with elevated privileges.

For the end-user, they run the approved applications using the "Run as Administrator using PEM" option from the application's context menu, just as they would previously. The user is then presented with the Windows User Account Control (UAC) prompt where they enter their normal user credentials, assuming the policy IT established allows them to do so.

User context is maintained while privilege is elevated. As a result, any files created will be owned by the user's account and saved in their default locations. This produces a seamless experience for users to elevate privileges on demand.



Apove : Applications menu example

Building Approved Elevation Policies

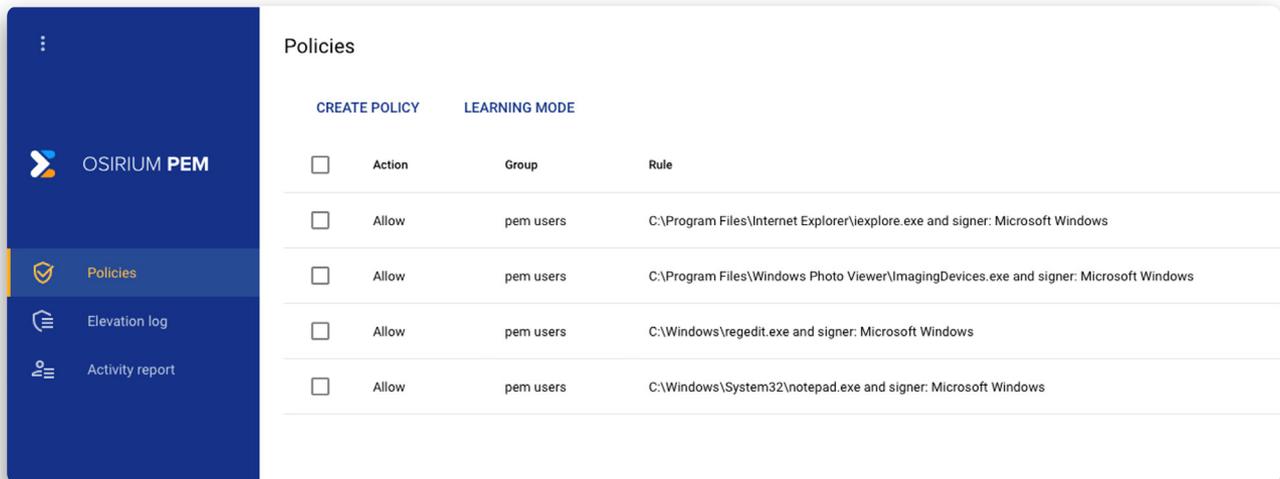
Automatic Policy Creation

The simplest method of deploying PEM is to run in "Learning Mode" to detect which applications users need without interrupting the user's work. PEM tracks the applications being run as administrator and IT can specify exactly which version is allowed to be run as administrator.

From that list, IT builds policies to permit elevated execution of approved applications. Learning Mode, ensures most applications that users will need will have been pre-approved reducing calls to the help desk when PEM is switched to "Enforce" mode.

Manual Policy Creation

Alternatively, Administrators can explicitly define the specific applications and versions that will be allowed through the PEM Administration console.



Above : PEM Administration console screen

Osirium Privileged Access Security

Privileged Endpoint Management is a component of Osirium's Privileged Access Security solution that also includes:

Privileged Access Management – PxM Platform

Modern, easy to deploy management of privileged access to shared devices, services and systems that includes session recording, behavioural analytics and rich audit controls.

Privileged Process Automation – PPA

IT Operations teams are overloaded with user requests, but traditional automation and RPA tools aren't appropriate. PPA securely automates IT processes to enable "shift-left" delegation of tasks.

Osirium PEM Benefits

With PEM, you can manage users' execution of applications that are run with elevated privileges.

Policies enable IT to fine-tune exactly which applications to either allow or deny privileged execution for specific AD users and groups.

Learning Mode ensures users can run their required privileged applications without contacting IT.

Enforce compliance and audit trails: ensure only verified applications are used and full audit trail of escalations is maintained.

About Osirium

Osirium is the UK's innovator in Privileged Access Management. Founded in 2008 and with its HQ in the UK, near Reading, Osirium's management team has been helping thousands of organisations over the past 25 years protect and transform their IT security services.

The Osirium team have intelligently combined the latest generation of Cyber-Security and Automation technology to create the world's first, built-for-purpose, Privileged Protection and Task Automation solution.

Tried and tested by some of the world's biggest brands and public-sector bodies, Osirium helps organisations drive down Business Risks, Operational Costs and meet IT Compliance.



OSIRIUM LTD.

Theale Court, 11-13 High Street, Theale, Reading, Berkshire, RG7 5AH
+44 (0) 118 324 2444, info@osirium.com, osirium.com