Eliminate Administrator Rights Without Impacting Productivity
Windows Privilege Manager

Remove local admin rights on Windows servers and endpoints, elevate applications for standard users, whitelist trusted applications, enforce least privilege across the enterprise, and prevent malware propagation.

Enforce Least Privilege | Control Applications | Prevent Malware Propagation

Product Highlights

Inventory of Devices
Discover and create an inventory of endpoints and servers in your organization. Decide which devices require least privilege enforcement.

Applications Discovery
Automatically discover the applications that require administrator privileges across the enterprise. Consolidate and centrally track them.

Policy-based Management
Centrally manage least privileges through control policies. Allow processes to be elevated on specific endpoints, by specific users or groups.

Local Admin Analysis
Identify and track the list of users and groups that are part of the local admin group on computers in the domain.

Granular Application Control
Define and control which applications can be run by standard users. Whitelist trusted applications and prevent unapproved and malicious applications.

Offline Scenarios
Ensure least privilege and application controls even when the endpoint is offline or away from the network or when users are working from home.
The overall security posture of the product is very good, and above the industry standard.

Experts from Agile Infosec, London.

Validated by
3RD-PARTY SECURITY EXPERTS

"The overall security posture of the product is very good, and above the industry standard."
Experts from Agile Infosec, London.

Remove Admin Privilege
Remove local administrator rights from users on Windows endpoints. Enforce least privilege without impacting operational efficiency.

Elevate Applications On-Demand
Empower standard users to seamlessly run approved applications (that would normally require admin rights) whenever needed. Elevate applications, not users.

Temporary Administrator Access
Grant time-limited, fully controlled, and comprehensively audited temporary administrator access to standard users on need basis. Automatically revoke access.

Workflow Controls
Well-defined workflows with automation options to handle the lifecycle of all requests for approvals from end-users.

Application Elevation Trends
Track the trend of applications that are elevated by standard users over a period of time and detect unusual or suspicious activities.

Continuous Monitoring
Continuously monitor who all have administrator privileges. Detect if new local administrator accounts are added.

Recommended by a Windows Expert

"If you are struggling with local admin accounts on PCs and Servers, this product is definitely worth a look."

Mike Kanakos,
Seasoned Windows IT Professional and Active Directory Expert

www.securden.com
## Technical Specifications

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deployment Model</strong></td>
<td>On-prem, VMs (or) private cloud (AWS/Azure)</td>
</tr>
<tr>
<td><strong>Web-interface</strong></td>
<td>IE, Chrome, Safari, Edge, Firefox</td>
</tr>
<tr>
<td><strong>Backend Database</strong></td>
<td>PostgreSQL (bundled) or MS SQL server</td>
</tr>
<tr>
<td><strong>Primary Authentication</strong></td>
<td>Active Directory</td>
</tr>
<tr>
<td><strong>MFA</strong></td>
<td>Any TOTP authenticator (Google authenticator or Microsoft authentication), any RADIUS-based authentication mechanism (RSA SecurID, Digipass and others), Duo Security, Yubikey, Email to SMS gateway and OTP through email</td>
</tr>
<tr>
<td><strong>Data Encryption</strong></td>
<td>AES-256</td>
</tr>
<tr>
<td><strong>Data Transmission</strong></td>
<td>SSL over HTTPS</td>
</tr>
<tr>
<td><strong>Devices Discovery</strong></td>
<td>Agentless</td>
</tr>
<tr>
<td><strong>Admin Rights Removal</strong></td>
<td>Agentless</td>
</tr>
<tr>
<td><strong>Privilege Management, Application Control, and Temporary Admin Rights</strong></td>
<td>Through a light-weight agent.</td>
</tr>
<tr>
<td><strong>Integrations</strong></td>
<td>Active Directory, SIEM Solutions</td>
</tr>
<tr>
<td><strong>High Availability</strong></td>
<td>Redundant servers pointing to the same database. MS SQL clusters</td>
</tr>
<tr>
<td><strong>Disaster Recovery</strong></td>
<td>Periodic database backup and recovery</td>
</tr>
</tbody>
</table>

---

Securden - Datasheet

Securden, Inc.
2035 Sunset Lake Road, Suite B-2, Newark, Delaware, 19702

support@securden.com
www.securden.com