semperis

What's New

Semperis Directory Services Protector and **Semperis Active Directory Forest Recovery**

Version 3.0 | June 2020

Semperis Directory Services Protector

Cyberattacks threaten the very existence of your organization, and it's your job to stop them. As the gatekeeper to sensitive credentials and data, Active Directory (AD) is the #1 target for attackers. Unwanted changes to AD can have significant security and operational consequences. But securing AD is difficult given its constant flux, sheer number of settings, and increasingly sophisticated threat landscape. Semperis® Directory Services Protector (DS Protector) stops cyberattacks in their tracks by continuously monitoring AD for indicators of exposure, detecting advanced attacks, and enabling rapid response.

DS Protector is known for providing uninterrupted tracking of AD modifications and immediate rollback of unwanted changes, without mounting backups or taking domain controllers (DCs) offline. It provides the capabilities you need to defend AD from cyberattacks, which routinely target AD and increasingly circumvent native Windows security event logging. It exposes hidden changes and alerts you to potential attacks in progress.

DS Protector 3.0 provides additional capabilities to monitor your Active Directory for vulnerabilities, intercept attacks in progress, and enable you to immediately close backdoors created by an attacker or rogue administrator, so critical systems stay secure and available. With this new version of DS Protector, you will notice a new, more modern user interface as well as the following new features and capabilities.

The following is a high-level description of the DS Protector 3.0 features. For more detailed information about DS Protector, please see Additional Resources.

Automatic remediation

DS Protector provides all the components needed for automated monitoring and remediation. The insights gathered by DS Protector can be used to trigger automated actions, including built-in rollback capabilities. The new **Auto Undo** option on the notification rule settings page allows you to undo critical security-related or operational changes without any user intervention. This enables you to undo suspicious changes, regain control, and circumvent further damage and security exposure.

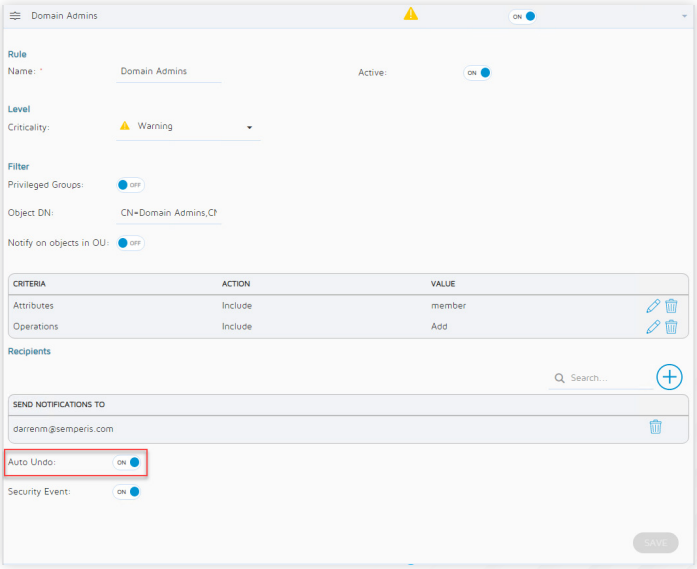

Figure 1: Notification Rule Settings – Auto Undo Option

Figure 2: Jobs > Auto Actions page showing auto-undo jobs

Security dashboard

DS Protector continuously scans Active Directory for risky configurations to identify weak links in your AD deployment. The new Security dashboard highlights the findings from performing Active Directory security posture checks against security indicators that point out misconfigurations.

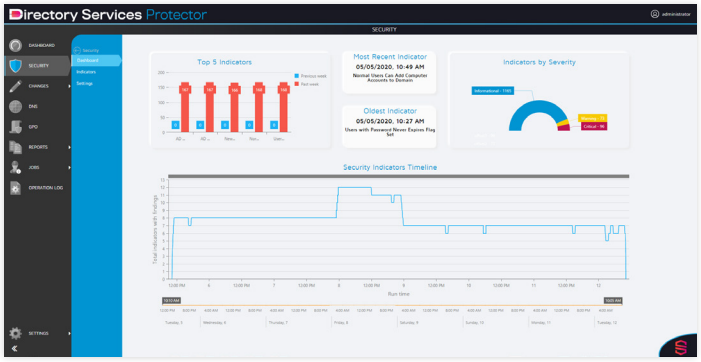

Figure 3: Security > Dashboard

Vulnerability assessment

By regularly assessing Active Directory for risky configurations, DS Protector provides a prioritized list of vulnerabilities and suggests corrective actions to reduce your Active Directory attack surface. This new functionality allows you to proactively address vulnerabilities in your AD configuration.

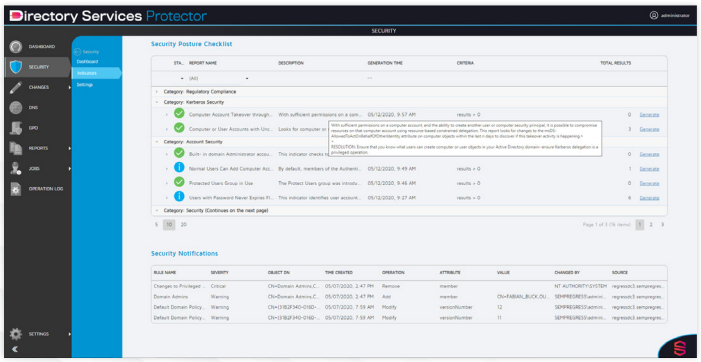

Figure 4: Security > Indicators page showing vulnerabilities and suggested resolution

As additional threat research is performed, Semperis can dynamically add security indicators to address new threat scenarios and attack techniques. In addition, you can adjust security indicators to meet the requirements specific to your environment.

Integrated Changes view

The new user interface provides a more integrated view of Active Directory changes that allows you to more easily filter by change types and by Active Directory partition. The new Changes page provides a single, consolidated view for monitoring and managing changed items, deleted items, and Configuration partition changes, which were separate views in the past.

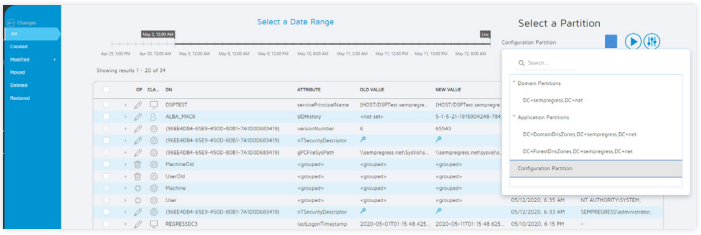

Figure 5: Consolidated Changes page – Partition Selector

New Report Authoring Tool

In addition to new built-in reports, DS Protector 3.0 includes a new Report Authoring Tool that allows you to query LDAP as well as the DS Protector database to create custom report templates. This new reporting capability allows you to create new report templates and Semperis to publish new report templates on a continuous release cycle, independent of the major product release cycle.

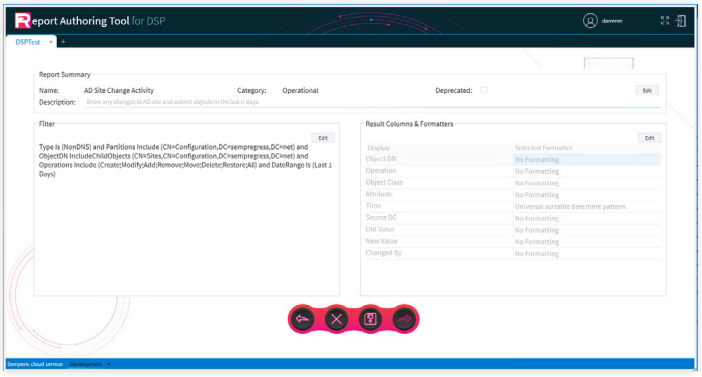

Figure 6: Report Authoring Tool

Enhanced event logging

Audit notifications are now included in a custom Windows event log, which enables you to collect and send alerts using your enterprise monitoring system. By integrating natively with your SIEM system, you can speed up forensic analysis and troubleshooting.

Semperis Active Directory Forest Recovery

Considering that cyber disasters now strike more frequently and inflict more business damage than natural disasters, it's time to think about "cyber-first" disaster recovery. Recovery playbooks must be updated to address this reality. Defenders need to be able to:

- Recover Active Directory (AD) cleanly without re-introducing malware.
- Recover AD to alternate hardware, virtual or physical.
- Automate AD recovery to reduce downtime and the impact of cyberattacks.

Semperis® Active Directory Forest Recovery (AD Forest Recovery) is a fully-automated system that enables you to recover AD even if domain controllers are infected or wiped out. It performs all the heavy lifting for you – backs up everything you need to recover AD and performs all the necessary steps and clean-up during recovery. Semperis AD Forest Recovery is the preferred solution of Active Directory experts who understand the complexities of Active Directory recovery and the need for a fully automated solution.

With this release of AD Forest Recovery, you will notice a new, more modern user interface that provides improved navigation as well as the following new features and capabilities that help you streamline your AD recovery process.

The following is a high-level description of the AD Forest Recovery 3.0 features. For more detailed information about AD Forest Recovery, please see Additional Resources.

Multi-forest support

AD Forest Recovery 3.0 allows you to consolidate your Semperis AD Forest Recovery deployments to manage multiple Active Directory forests using a single management server and web portal. This also simplifies the administration of backups by allowing you to use a single interface to easily switch between multiple forests.

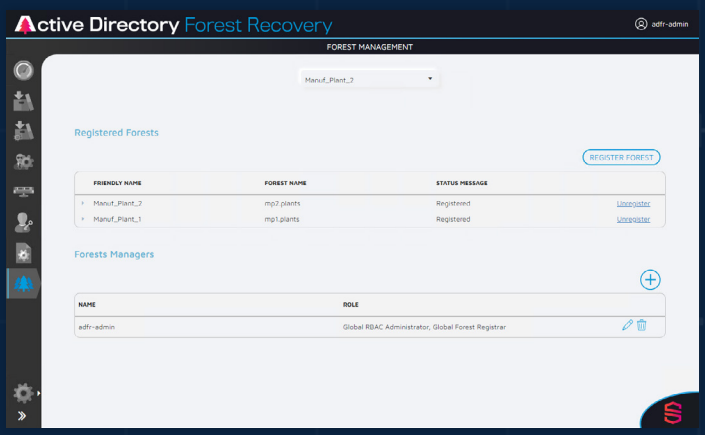

Figure 7: Forest Management page used to register forests and specify forest managers

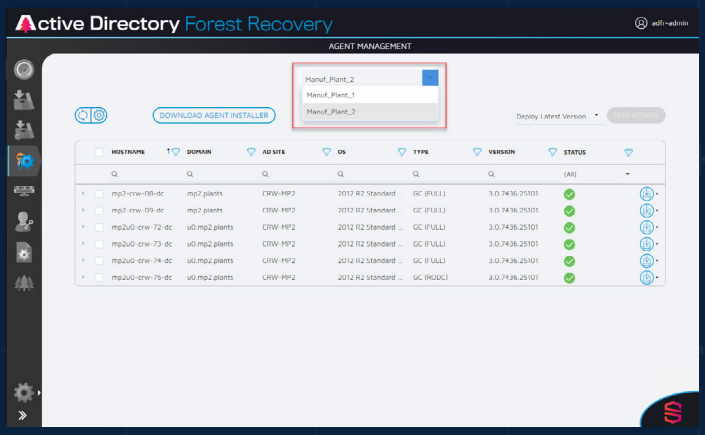

Figure 8: Selecting a forest in the web portal

Enhanced event logging

Agent, backup, and recovery events are now logged in a custom Windows event log, which enables you to collect and send alerts using your enterprise monitoring system. This allows you to easily integrate these events into your SIEM system for visibility into the status of your AD forest backup and recovery.

PowerShell support

AD Forest Recovery 3.0 includes additional PowerShell commands for automating the management of Semperis ADFR. This provides easier management of backup groups, backup rules, agents, and distribution points.

Additional Resources

For more detailed information about DS Protector and AD Forest Recovery, the current published documents can be downloaded from the Semperis website:

- https://www.semperis.com/downloads/docs/3.0/dsp documentation.zip
- https://www.semperis.com/downloads/docs/3.0/adfr documentation.zip

About Semperis

Semperis is the pioneer of identity-driven cyber resilience for cross-cloud and hybrid environments. The company provides cyber preparedness, incident response, and disaster recovery solutions for enterprise directory services—the keys to the kingdom. Semperis' patented technology for Microsoft Active Directory protects over 40 million identities from cyberattacks, data breaches, and operational errors. Semperis is headquartered in New York City and operates internationally, with its research and development team distributed between San Francisco and Tel Aviv.

Semperis hosts the award-winning Hybrid Identity Protection conference. The company has received the highest level of industry accolades; most recently being named Best Business Continuity / Disaster Recovery Solution by SC Magazine's 2020 Trust Awards. Semperis is accredited by Microsoft and recognized by Gartner.

Contacting Semperis

Thank you for your interest in Semperis and our directory recovery solutions. We are here to answer any questions you may have.

For technical support
contact support@semperis.com

For licensing issues
contact sales@semperis.com

For product inquiries or feature requests
contact info@semperis.com