PowerBroker Auditing & Security Suite Version 5.3

New and Updated Features

BeyondTrust PowerBroker Auditing & Security Suite centralizes real-time change auditing for Active Directory, File Systems, Exchange, SQL and NetApp, restores Active Directory objects or attributes, and helps to establish and enforce entitlements across AD and file systems. Through simpler administration, IT organizations can mitigate the risks of unwanted changes and better understand user activity to meet compliance requirements.

With PowerBroker Auditing & Security Suite, customers can:

- Audit the who, what, where and when of changes in Active Directory, Group Policy, Exchange, File Systems and SQL, and alert to those changes, providing real-time visibility to address potential compliance concerns
- Provide rollback and restore of any Active Directory changes or deletions, and backup and restore of Group Policy, protecting the business from downtime
- Deliver entitlement reporting, ensuring that users have access to the resources – and only those resources – they need to do their jobs
- Centralize distributed audit data across the Microsoft infrastructure, providing more capabilities than native tools and a unified view of changes across the environment

PowerBroker Auditing & Security Suite includes modules for the following systems:

Auditing	Recovery	Entitlement Reporting
• PowerBroker Auditor for Active Directory • PowerBroker Auditor for File Systems • PowerBroker Auditor for Exchange • PowerBroker Auditor for SQL	PowerBroker Recovery for Active Directory	PowerBroker Privilege Explorer for Active Directory and File Systems

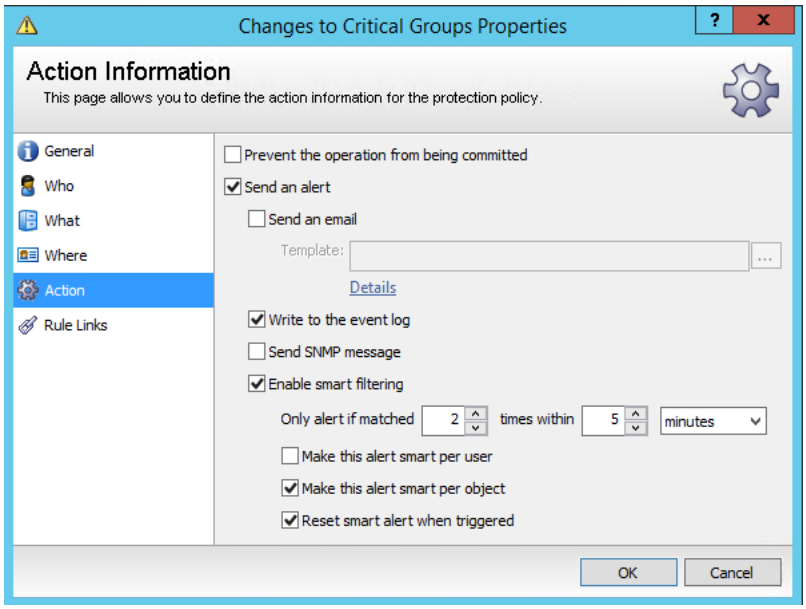
PowerBroker Auditing & Security Suite version 5.3 adds several capabilities that further enhance simplicity and usability. Please read below for a summary of new features.

New Features Highlights

Smart Alerts Streamline Notifications

Email notification of alerts can be overwhelming due to volume. Often, administrators don't need notification the first time an event occurs, rather only if it occurs multiple times. What admins want is the ability to specify that an alert be delivered if it occurs *x* number of times over *n* period of time.

With version 5.3, PowerBroker Auditor introduces a new feature called Smart Alerts. The filter in this feature enables admins to raise an alert if an event happens multiple times over a specific duration of time, with the number of occurrences and time duration configurable. Additionally, the alert can be configured by the type of change, the user making the change or the object impacted by the change. Once an alert is raised, the rule can clear the trigger so the time and occurrence can begin again. For a representation of this new feature, please see the screenshot below.



This new capability helps administrators by preventing cluttering of their inbox, enabling them to focus on the most important changes.

Password Expiration Notifications Minimize Productivity Disruptions

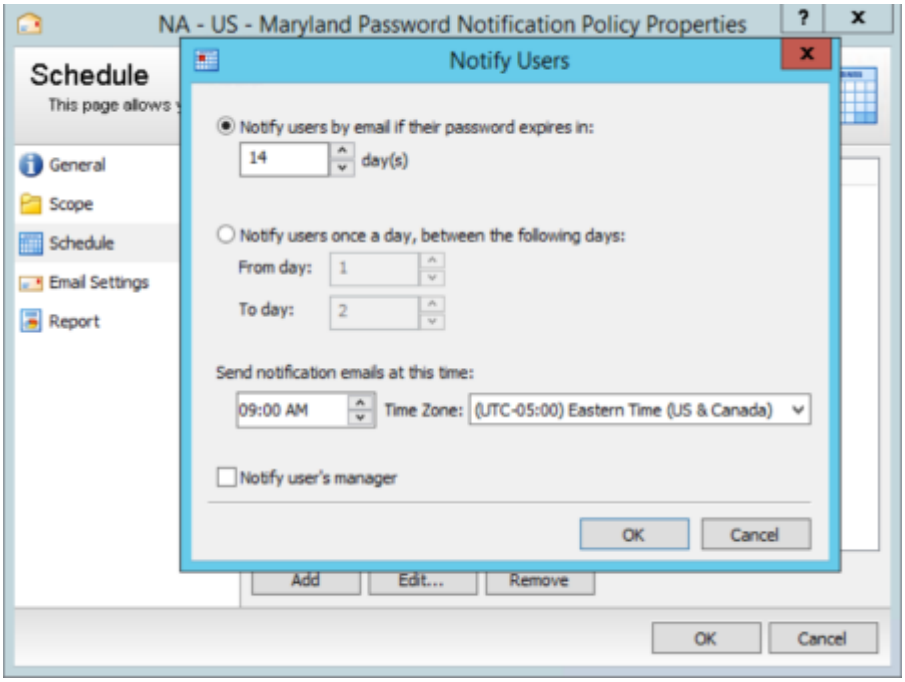
For security and best practices reasons organizations require users to have long passwords and to change them frequently. Commonly, users will miss the notification at logon that tells them they need to change their password. Organizations need an automated process to identify

accounts that will expire within a given time range, then send out an email notification proactively with instructions on how to reset their password.

In PowerBroker Auditor version 5.3, password expiration notification emails have been enhanced to identify which user's accounts will expire within a specified time, and send out notifications to:

- The users whose password is set to expire
- The managers of the users whose password is set to expire
- The administrators who desire a summary report of all accounts with passwords set to expire

For a representation of the notification schedule, please see the screenshot below.



The benefit of this enhancement is that end users will avoid any unexpected password expirations – or productivity disruptions.

Nested Group Auditing Provides Greater Depth

When the membership of a group is changed, it is considered a single direct event. What cannot be seen, however, is the effective change that has occurred due to group nesting. While it is possible to monitor for changes to critical groups like Domain Admins if changes are made

to a group that is a member of Domain Admins, native auditing does not alert on nested changes, leaving admins blind to the change. When a group membership is changed, there should be an audit event generated for all the effective changes. The risk is that users could effectively be added to sensitive groups without security and compliance teams being aware of the change.

In version 5.3, PowerBroker Auditor for AD now notifies on nested group changes regardless of the number of nested layers. When a group gets modified it looks at the resulting changes and sends a notification for any nested group events that would be impacted by adding or removing of a member.

For a representation of this capability, please see the screenshot below.

This new capability allows an administrator to create an alert when a sensitive group is modified directly or via a nested membership change, providing greater depth of auditing and securing against unwanted changes.

Additional Enhancements

- PowerBroker Auditing & Security Suite solutions now feature the Auto Update engine for automatic upgrades for available updates and installs.
- All agents now support Windows Server 2016.
- Domain Controller Add / Remove Events. When a domain controller is promoted an even will be generated for the addition or removal of domain controllers.
- Global Catalog Add / Remove. When a server is set to be a Global Catalog server an event is generated for the addition or removal of a global catalog.
- General Web Console enhancements.

About BeyondTrust

BeyondTrust® is a global security company that believes preventing data breaches requires the right visibility to enable control over internal and external risks.

We give you the visibility to confidently reduce risks and the control to take proactive, informed action against data breach threats. And because threats can come from anywhere, we built a platform that unifies the most effective technologies for addressing both internal and external risk: Privileged Account Management and Vulnerability Management. Our solutions grow with your needs, making sure you maintain control no matter where your organization goes.

BeyondTrust's security solutions are trusted by over 4,000 customers worldwide, including over half of the Fortune 100. To learn more about BeyondTrust, please visit www.beyondtrust.com.