TECH BRIEF

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

SailPoint IdentityIQ Integration with the BeyondInsight Platform

Providing Complete Visibility and Auditing of Identities

Table of Contents

Executive Summary

Identity and access management (IAM) is a combination of business process, policies and technologies to more effectively manage and control digital identities. SailPoint's IdentityIQ is an IAM technology designed to work across heterogeneous environments to provision and de-provision identities using a consistent process to ensure that that access privileges are granted according to business policy.

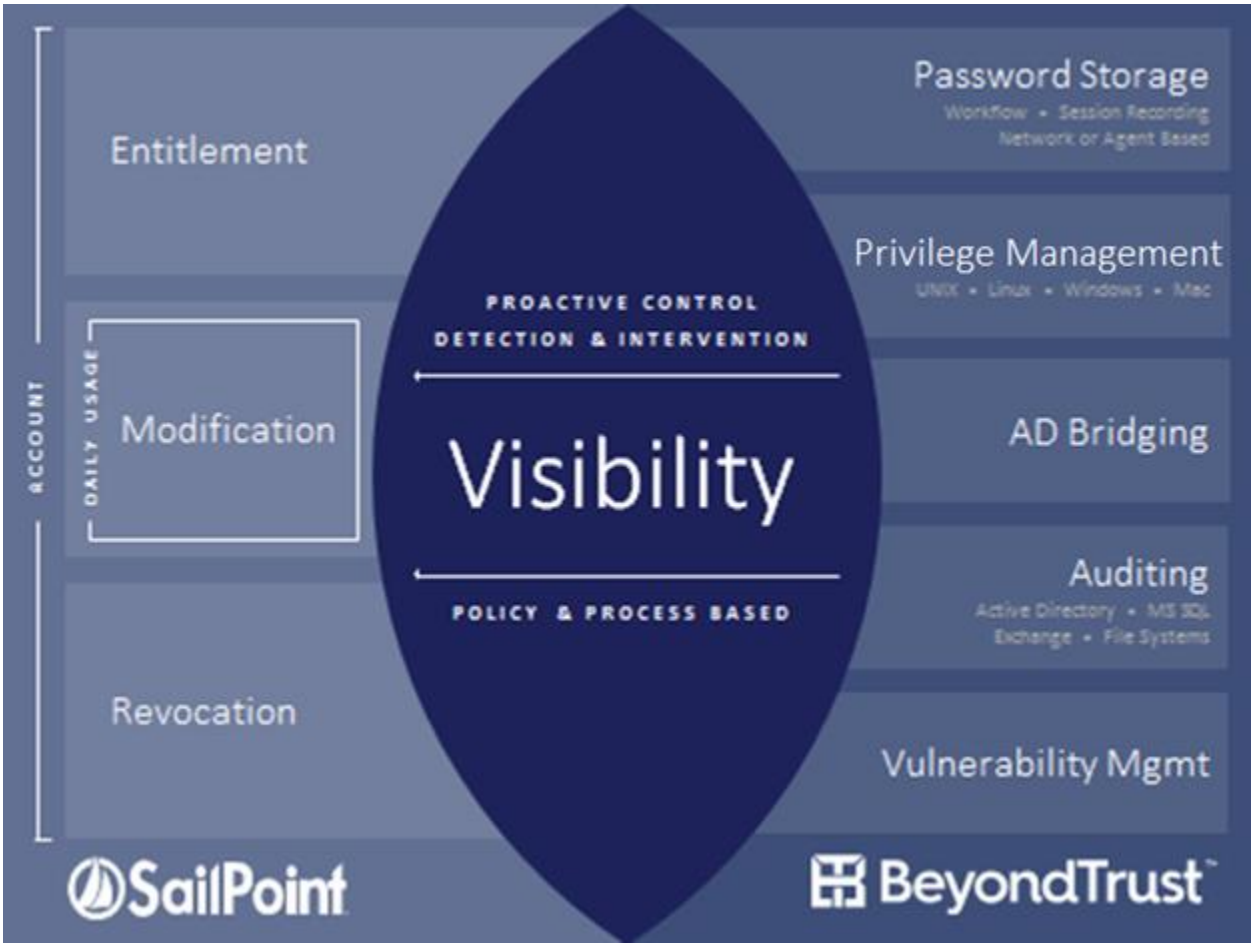
Most organizations that implement privileged access management (PAM) and identity and access management (IAM) have done them independently but are missing some key values that could come from their integration. Getting control over user access, permissions and rights to address a security, compliance or IT efficiency challenge tends to be the driver in adopting an IAM solution. PAM solutions take security and compliance a step further by helping IT teams get control over privileged users and accounts, and provide granular visibility on how identities are actually being used.

BeyondTrust privileged access management (PAM) solutions are designed to provide privileged and least privilege access to systems and applications. Where IdentityIQ identity and access management solutions focus on all digital identities, privilege access management targets the special requirements for any account managed by an enterprise.

When it comes to user access – whether it's privileged or non-privileged – every organization has to answer three questions:

1. Who has access to what?
2. Is that access appropriate? and
3. Is that access being used appropriately?

IAM solutions can tell you who has access to what, and whether that access appropriate. With BeyondTrust, SailPoint customers can also answer whether that access is being used appropriately. This gives you a more unified view for visibility and control of all users – privileged or non-privileged.

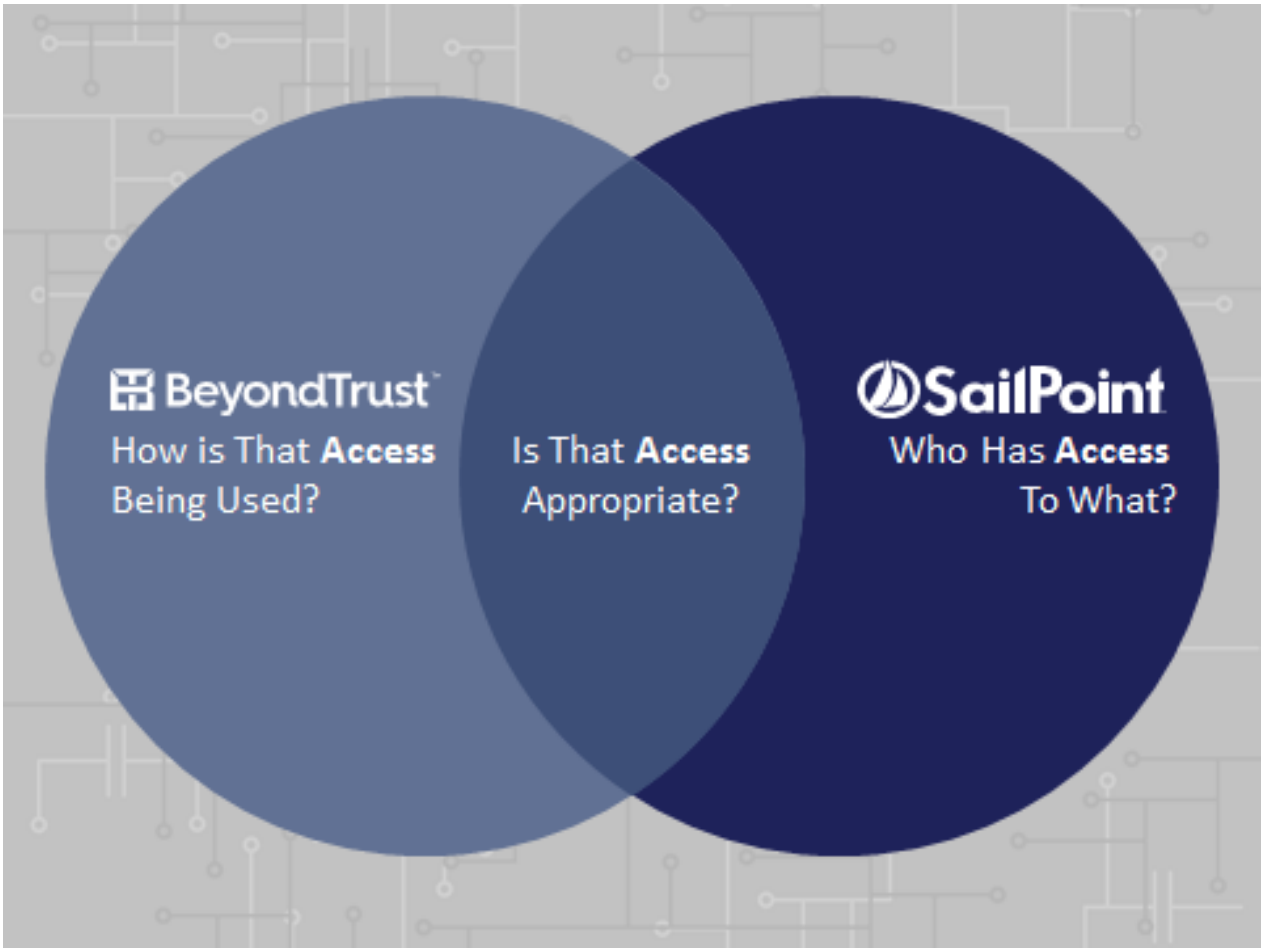


This document reviews the technical steps required to integrate an IdentityIQ solution with BeyondTrust's BeyondInsight platform for a seamless and automated approach to privileged access management and identity and access management.

Identity and Access Management

One common use case for an IAM solution is to provision identities into Active Directory. The typical provisioning process includes, but is not limited to, populating attributes and adding provisioned accounts to AD group policy. Once an identity is provisioned based on an IAM policy, BeyondTrust PowerBroker solutions will seamlessly leverage those identities for privileged password and session access in addition to enabling least privileged controls.

Below are some examples of how BeyondTrust can integrate with IdentityIQ.



BeyondTrust Solutions

Controlling and monitoring privileged access is extremely important to mitigating the risks posed by insider threats, preventing data breaches, and meeting compliance requirements. But security leaders have to walk a fine line between protecting access to the organization's critical data to ensure business continuity, and enabling users and administrators to be productive. Why? Disparate, disjointed tools deployed and managed in silos leaving gaps in coverage over privileged access. This legacy model is expensive, difficult to manage, and requires too much time to show any meaningful risk reduction.

The BeyondTrust PowerBroker Privileged Access Management Platform is a modular, integrated solution to provide control and visibility over all privileged accounts and users. By uniting capabilities that many alternative providers offer as disjointed tools, the PowerBroker platform simplifies deployments, reduces costs, improves system security and reduces privilege risks.

When BeyondTrust's privilege access management solutions are used within the IdentityIQ framework, your visibility into privileged accounts and privilege account activity will dramatically increase. As a core portion of the technology, BeyondTrust also provides detailed monitoring and auditing coupled with an advanced reporting and analytics capability to increase visibility, knowledge, and perform actions against potential threats.

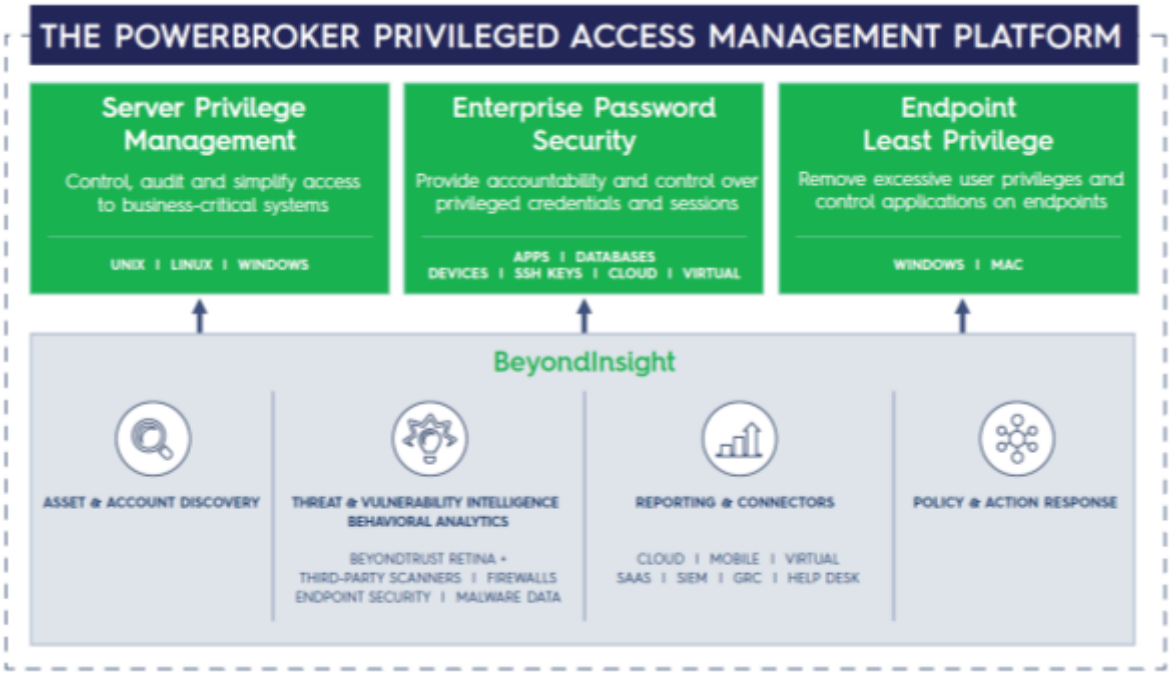
Below are the BeyondTrust solutions covered in this brief:

SOLUTION	DESCRIPTION
BeyondInsight IT Risk Management Platform (BI) *Central platform for management, reporting, policy and analytics*	BeyondInsight provides the unique capability of seeing both vulnerability and privilege in a single pane and can be deployed to meet operational requirements or merged for a consolidated view of all security and operational data. With BeyondInsight organizations have centralized reporting, auditing, session playback, and monitoring over users and administrators throughout disparate and heterogeneous infrastructures. Additionally, data can integrated into 3rd party tools including IAM, GRC, SIEM, and helpdesk solutions.
PowerBroker Password Safe (PBPS) *Privileged password*	PowerBroker Password Safe utilizes BeyondInsight for automated privileged password and session management solution across an organization's dynamic IT infrastructure. It can be configured as software, physical or virtual appliance, with no difference in functionality. Password Safe provides automated management of

and session management	highly privileged accounts, such as shared administrative accounts, application accounts, and local administrative accounts, across nearly all IP enabled devices. Furthermore, request, approval, and retrieval workflow functionality is included for end-user access of managed privileged accounts. It comes complete with audit-ready logging and reporting capabilities, application to application API, workflow, and session monitoring.
PowerBroker for Windows (PBW) *Least privilege and application control for Windows servers and desktops*	PowerBroker for Windows provides fine-grained policy based privileged delegation for the Windows environment. PowerBroker for Windows allows organizations to remove local admin rights from end users without hampering productivity. PowerBroker selectively elevates privileges for applications, software installs, system tasks, scripts, control panel applets, and other operations. Additionally, PowerBroker for Windows provides session monitoring and file integrity monitoring capabilities for granular tracking of privileged user activity across the Windows environment.
PowerBroker Identity Services AD Bridge (PBIS) *Integrate Unix, Linux and Mac into Active Directory*	PowerBroker Identity Services "AD Bridge" enables organizations to authenticate to Linux, Unix, and Mac machines using Active Directory (AD) credentials. It automatically maps UIDs and GIDs to users and groups defined in Active Directory by importing Linux, Unix, and Mac OS password and group files. Plus it provides centralized configuration management using AD Group Policy. PowerBroker Identity Services also provides compliance reporting and auditing capability.
PowerBroker for Unix & Linux (PBUL) *Least privilege delegation and command elevation for Unix and Linux*	PowerBroker for Unix & Linux is a user space network-based solution for fine-grained privileged delegation and auditing in Unix/Linux environments. PowerBroker for Unix & Linux enables granular policy control over privileged account user behavior after an identity has been provisioned. It is an inherently secure and centralized solution for both policy enforcement and auditing of user activity down to the keystroke level. The two main tasks that PowerBroker Unix & Linux performs are policy-based task delegation and auditing.
Retina *Enterprise vulnerability management*	Retina delivers large-scale, cross-platform vulnerability assessment and remediation, with available configuration compliance, patch management and compliance reporting. Retina's results-oriented architecture works with users to proactively identify security exposures, analyze business impact, and plan and conduct

	remediation across disparate and heterogeneous infrastructure.

This diagram below illustrates how all of BeyondTrust solutions integrate together for a complete privilege access management framework.



PowerBroker Password Safe Integration

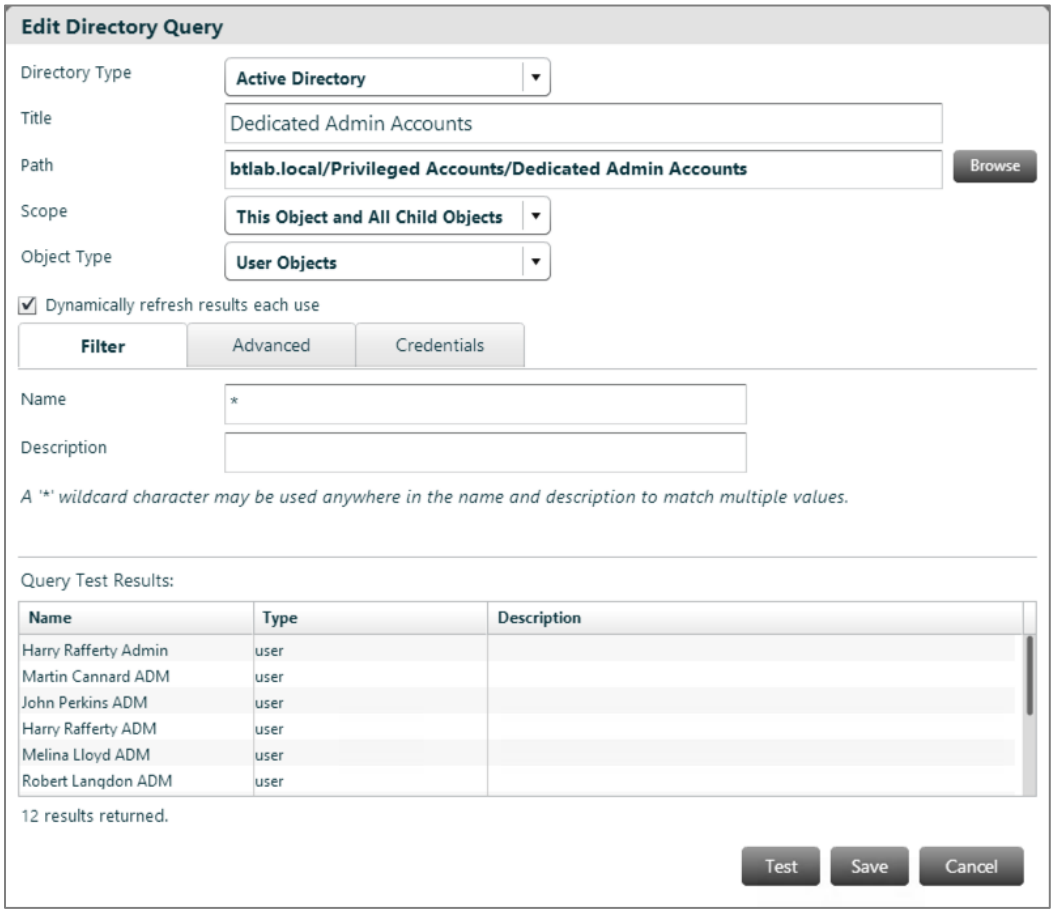
The ability to automatically discover, onboard and manage Active Directory or LDAP accounts is simple. By combining an LDAP query with our smart rule engine you can begin managing identities.

At a high level, the process is represented by the following steps:

1. A query is executed on a schedule to identify new accounts to be on-boarded based on identifies add or removed by IdentityIQ.
2. New accounts are provisioned and managed in Password Safe automatically.
3. Managed accounts are automatically linked to resources based on pre-defined roles.

Creating the AD Query

The first step is to create an Active Directory query which represents the user objects you wish to onboard from AD and managed by IdentityIQ. This could be a simple enumeration of items in an organizational unit or a complex query that evaluates a number of criteria.



Once the query is tested, it's added to a Smart Rule to automatically on-board the accounts.

Onboarding Smart Rule

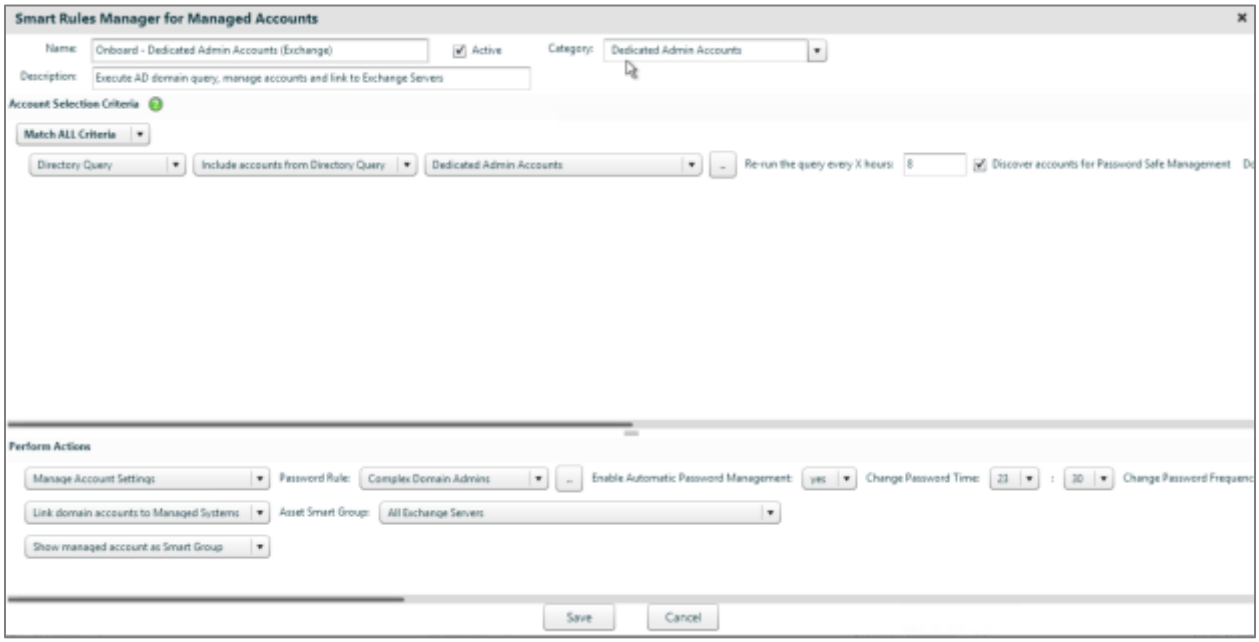
Smart Rules are not limited to performing single actions. They can dynamically link accounts to systems, bring accounts under management, set policies for accounts under management, trigger alerts, and much more.

When the AD query is referenced as a trigger criteria and the frequency the query should be evaluated is defined, it is represented in the top section of the Smart Rule pictured below.

When accounts are discovered, the Actions section (at the bottom) are invoked. There are two primary actions in this example.

1. Provision and manage the account using parameters defined in the Managed Account Setting Action.

2. Link the managed accounts to specific resources. In the example below, we are linking the domain admin accounts to Exchange servers.



The process is easy to set up and provides a reliable mechanism to automatically on-board, manage, and link managed Active Directory accounts to roles.

When roles are linked to Active Directory groups, IdentityIQ can control access to the roles by adding and removing users from the groups.

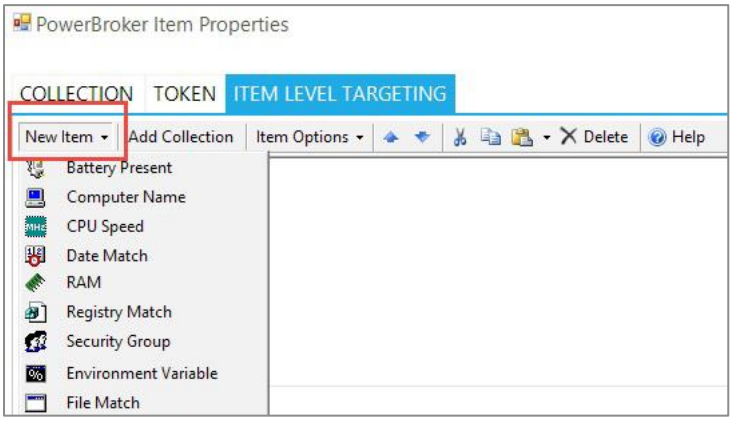
PowerBroker for Windows Integration

PowerBroker for Windows is designed to coincide with IdentityIQ workflow automation. By providing a set of filters to specify when and which policies should apply, companies can ensure consistency between IdentityIQ and PowerBroker for Windows. Auditing of policy can be tied back for further analysis within the BeyondInsight IT Risk Management Platform.

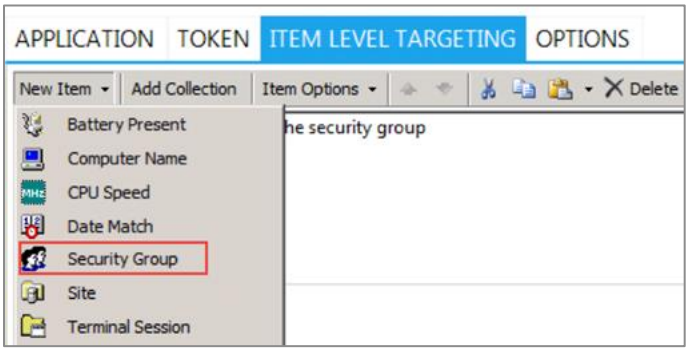
Policy enforcement can be configured via Item-Level Targeting, which is a property of a PowerBroker for Windows Rule or Collection. To configure these settings please see the following steps:

1. Create or Modify an existing Rule/Collection
2. Click the Item-Level Targeting Tab

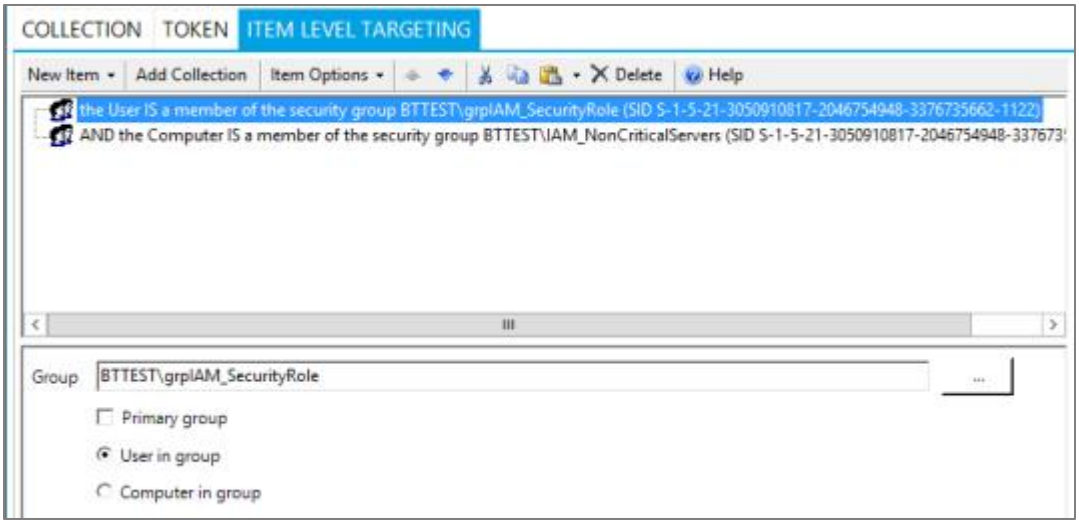
3. Click the 'New Item' option



4. Select 'Security Group'. You may select as many items as necessary. For instance, to ensure the Rule(s) apply to Users in a Security Group logged into Computers in a particular Security Group, create two Security Group targets. The results will look similar to this based on your AD groups:



5. Supply the appropriate information to sync your entitlement policies with PowerBroker for Windows enforcement. For instance, if a privilege identity elevation rule should only apply to users in a security role when logged into a non-critical server the information will look similar the image below.



6. Save your changes by clicking OK.

Policy auditing is centralized within the BeyondInsight IT Risk Management Platform as it is with other BeyondTrust privileged access management solutions. You can easily validate entitlements are being allowed for the appropriate roles and devices, but not for others.

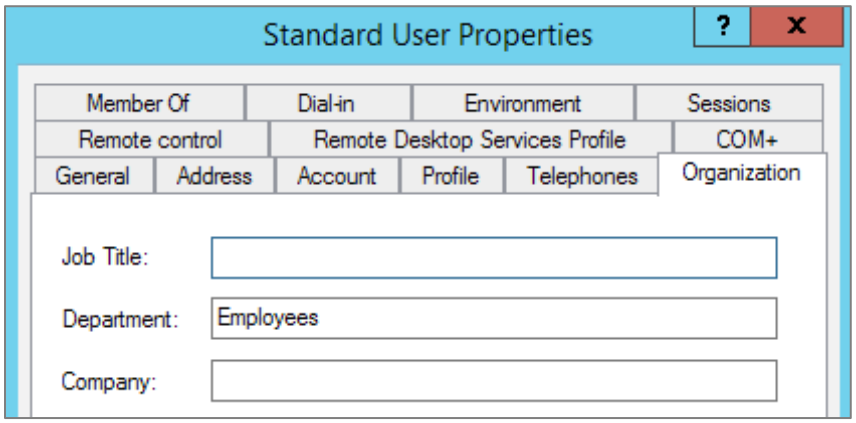
In the screenshot below, User "BTTEST\Standard" was entitled to several privilege elevations as part of their role, so long as they were logged into a machine in the appropriate security group, in this case Computer "WIN8-ONE".

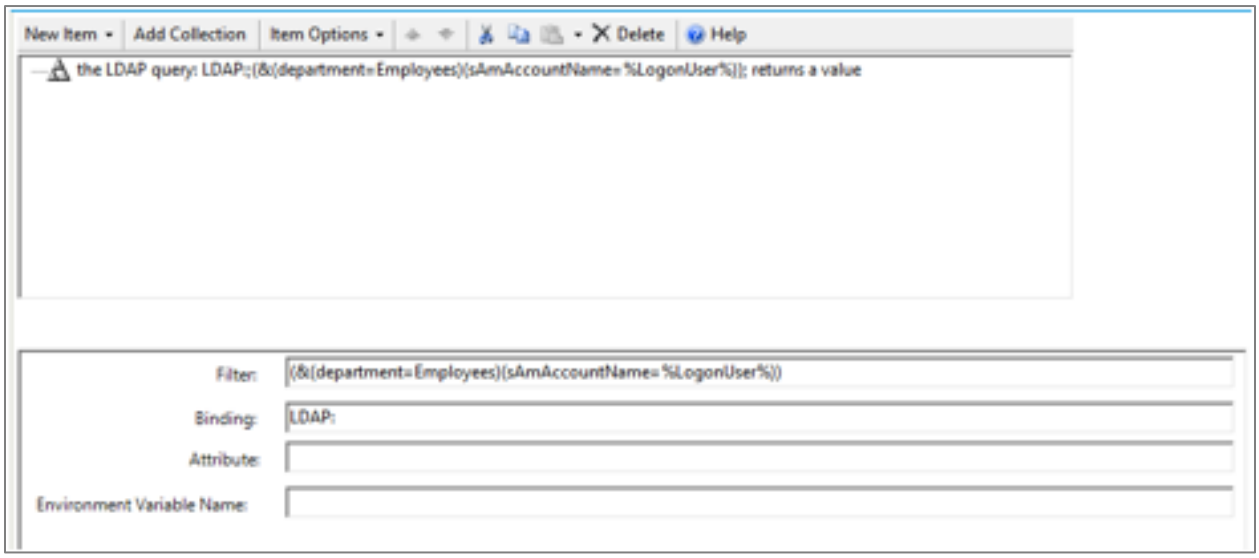
Event Id	Message	Product Name	Application	Arguments	User Name	Computer Name
1974	Custom Rule Applied	Microsoft® Windows® Operating...	OptionalFeatures.exe		BTTEST\Standard	WIN8-ONE
1973	Custom Rule Applied	Microsoft® Windows® Operating...	RunDll32.exe	c:\windows\system3...	BTTEST\Standard	WIN8-ONE
1972	Custom Rule Applied	Microsoft® Windows® Operating...	RunDll32.exe	c:\windows\system3...	BTTEST\Standard	WIN8-ONE
1971	Custom Rule Applied	Microsoft® Windows® Operating...	RunDll32.exe	sysdm.cpl,editenviro...	BTTEST\Standard	WIN8-ONE
1970	Custom Rule Applied	Microsoft® Windows® Operating...	RunDll32.exe	shell32.dll,control_ru...	BTTEST\Standard	WIN8-ONE

When this same user attempts the same activities on a machine not in the appropriate Security Group, the user was prevented from performing these same tasks.

Event Id	Message	Product Name	Application	Arguments	User Name	Computer Name
1985	UAC Prompt	Microsoft® Windows® Operating...	OptionalFeatures.exe		BTTEST\Standard	HR-WINDOWS10
1984	Denied Rule Applied	Microsoft® Windows® Operating...	rundll32.exe	c:\windows\system3...	BTTEST\Standard	HR-WINDOWS10
1983	Denied Rule Applied	Microsoft® Windows® Operating...	rundll32.exe	sysdm.cpl,editenviro...	BTTEST\Standard	HR-WINDOWS10
1982	Denied Rule Applied	Microsoft® Windows® Operating...	rundll32.exe	shell32.dll,control_ru...	BTTEST\Standard	HR-WINDOWS10

Additionally, in cases where group, site, or organization unit memberships are not the catalyst for role assignment within IdentityIQ, other attributes can be used instead. For instance, if you use AD Attributes rather than membership, PowerBroker for Windows can enforce policy in this manner as well. Follow the same steps to bring up Item-Level Targeting for a Rule or Collection and choose the LDAP Query Target. Below is an example of entitling/enforcing policy to users in the Employees Department:





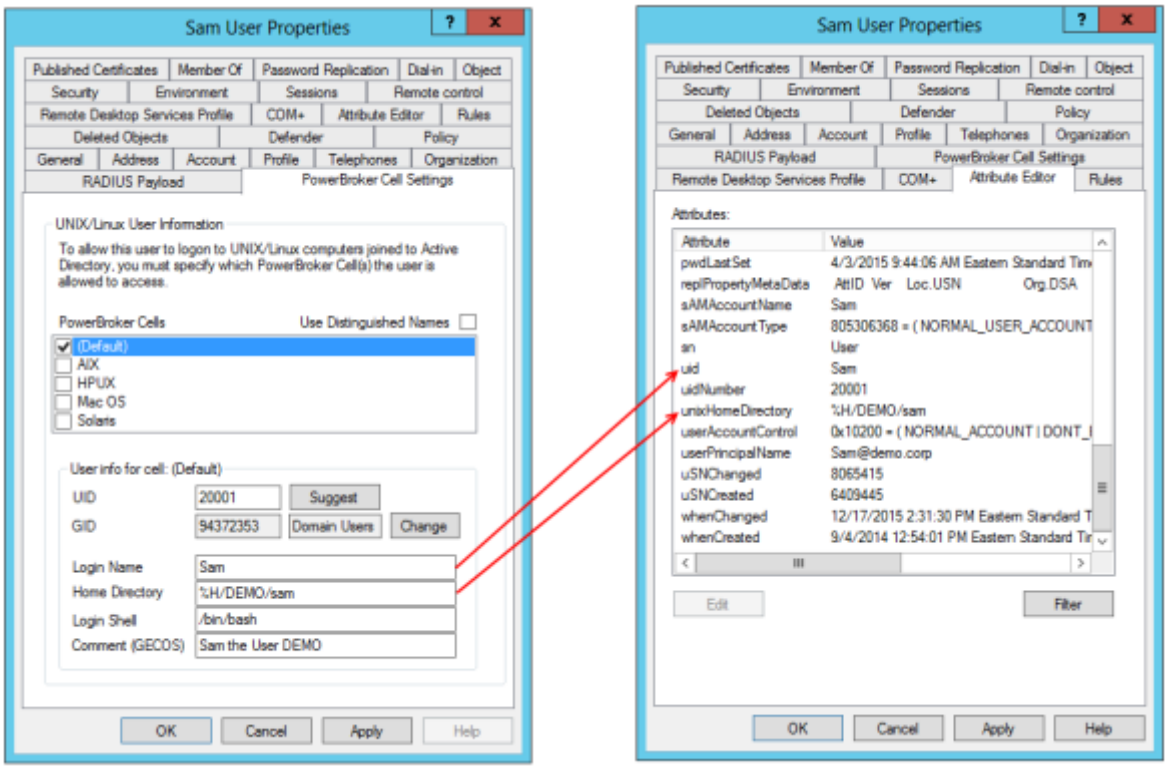
This allows for IdentityIQ to provision least privilege tasks on Windows by either Active Directory group membership or AD attributes. This can be applied to Microsoft Windows Desktops and Servers using the same procedure. In addition, when combined with PowerBroker Password Safe, access to the asset can be granted without the need for administrator privileges and individual tasks can be managed for administrator access.

PowerBroker Identity Services Integration

PowerBroker Identity Services uses standard Active Directory attributes to store POSIX information (Unix/Linux User and Group details). Plus, IdentityIQ is capable of managing Active Directory attributes can also manage PowerBroker Identity Services user and group object settings.

PowerBroker Identity Services can leverage up to six attributes for a user and up to three attributes for a group. An example of a user and group with their associated attribute names and sample values are listed below:

When PowerBroker Identity Services is installed, an optional MMC snap-in is provided to set and manage these attributes for both users and groups. A new tab is shown within the standard management console called 'PowerBroker Cell Settings' and allows for a simplified way to manage object attributes. Below you can see the direct correlation of two user attributes from the MMC snap-in to actual attributes on the user object:



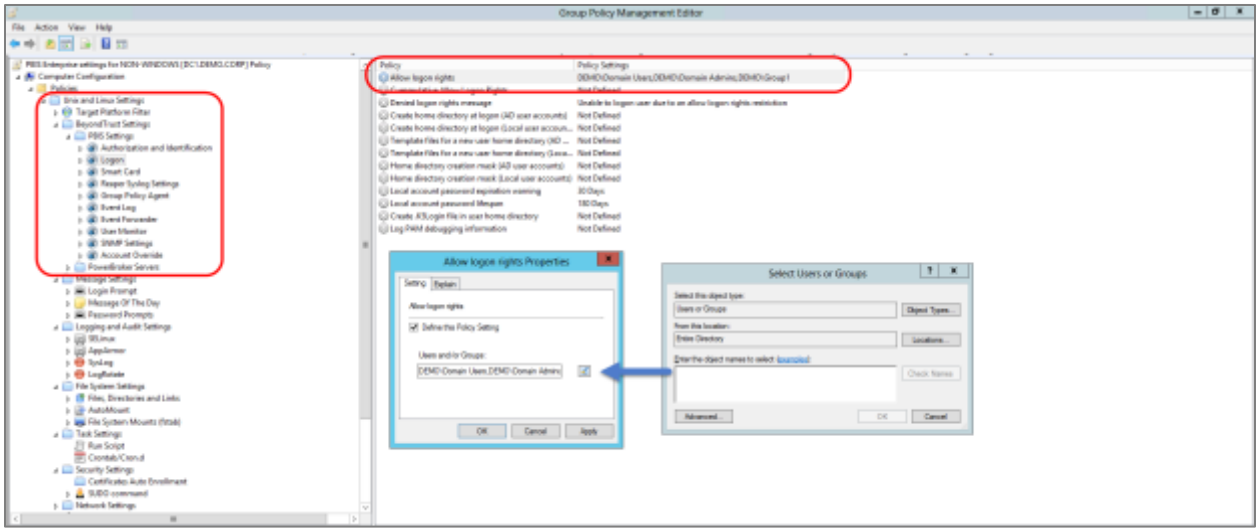
PowerBroker Identity Services Login Rights

PowerBroker Identity Services grants administrators out of the box integration with IdentityIQ by leveraging a user's Active Directory group membership settings to control who is allowed to logon to which servers.

PowerBroker Identity Services allows the logon right settings to be configured using the Microsoft Group Policy tool or any tool capable of manipulating group policy settings used by Active Directory. The logon rights settings may also be configured directly on the target host using the products 'config' command line utility. This also allows for batch updates and scripted updates.

The Allow Logon setting, regardless of where or how it is configured, allows Users, Groups, or a combination of Users and Groups to be specified. When set via group policy, the configured Users and/or Groups will be set on the target hosts controlled by the policy and that host will then limit logon rights on that host to only those AD users explicitly defined or defined by way of their group membership.

Allow Logon Rights configured via Group Policy:



Allow Logon Rights configured via the command line configuration utility:

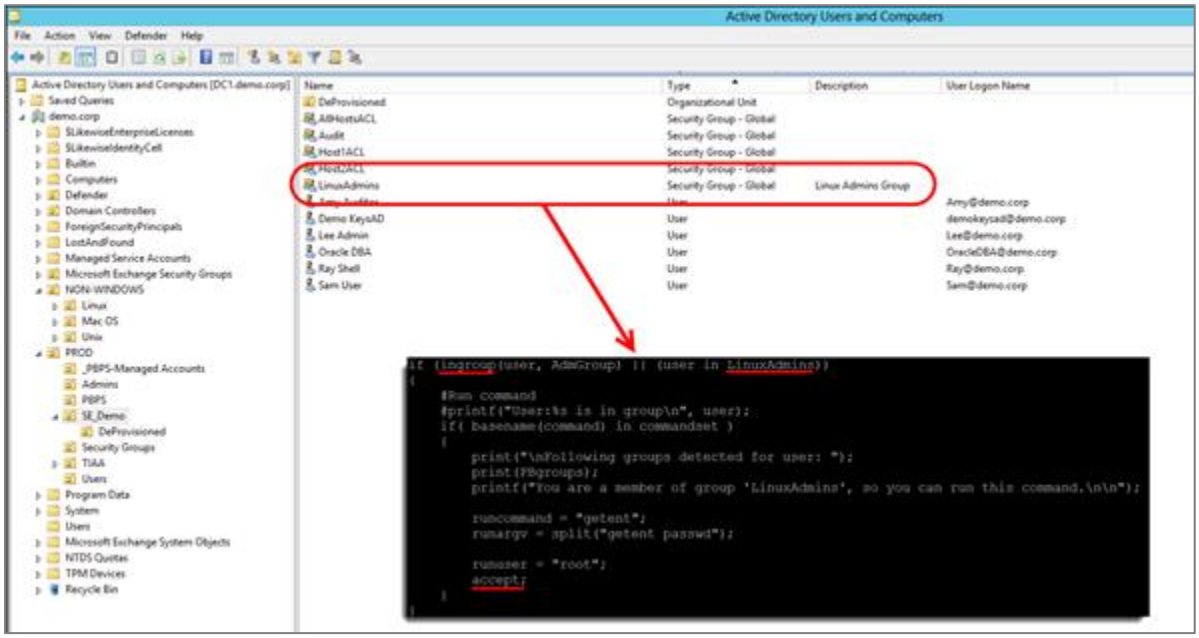
PowerBroker for Unix & Linux Integration

PowerBroker for Unix & Linux supports a number of different policy modes. All modes allow for Data Driven Polices and can use external data such as Active Directory group membership information, or the results of a SQL query against a corporate database in order to process the elevation (or rejection) of a command.

The benefit is that IdentityIQ can manipulate a user's group membership in any repository, can then be queried by a PowerBroker for Unix & Linux policy as part of the decision making process. With the externalization of the data used to drive privilege elevation request

processing, the policy does not need to change in order grant or deny access to individual users or groups of users. Any data from any source that is managed by IdentityIQ can also be leveraged, such as the requesting user's office location, time zone information, job title, etc.

Below is an example of a simple policy snippet in code form that will check a user's group membership before elevating and processing a command based on the user belonging to the LinuxAdmins group located in Active Directory:

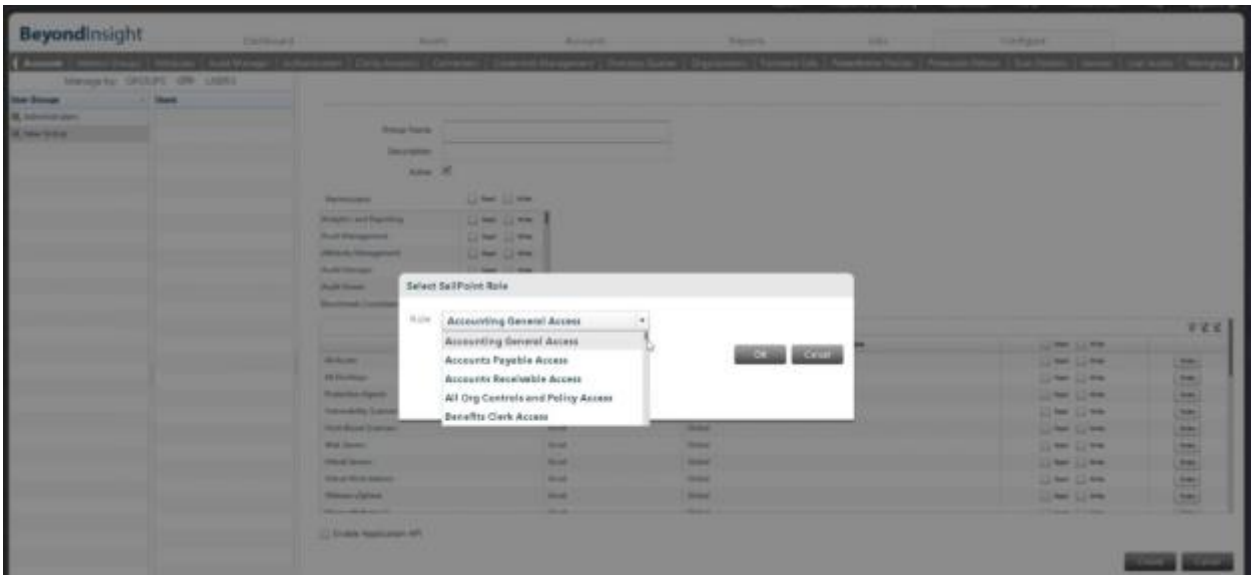


Retina Integration

Managing Retina CS users can be handled in a number of different ways. You can manually create local accounts within BeyondInsight, you can integrate with Active Directory and now you can also integrate with SailPoint.

The benefit of the SailPoint integration is best seen in organizations with a mature Vulnerability Management program. These organizations will have defined roles/groups for those that run scans, review results, perform auditing and finally for those in charge of patching systems. Instead of manually creating and maintaining these groups in BeyondInsight you can automatically and dynamically manage them as SailPoint Roles.

As Sailpoint Roles, Retina CS can import then, permissions are assigned to each Role. Any changes to the members of those Roles is then automatically synced with Retina CS. This enables Retina CS and SailPoint visibility into reporting and Role assignment to control Vulnerability Management identities. See the screenshot below.



Conclusion: Why SailPoint and BeyondTrust

Identity and access management (IAM) solutions provide a framework for business processes that simplify the management of electronic identities, users, and accounts. These technologies are designed to work across platforms, applications, and virtually any system within an environment to provision and de-provision identities. This ensures that access privileges are granted according to a unified interpretation of business policy and all personnel and services are properly delegated and permissioned. Privileged access management solutions are designed to provide privileged access management and least privileged access to systems and applications.

In the context of identity and access management, BeyondTrust's BeyondInsight platform feeds entitlement data on users, accounts and applications into IdentityIQ so that the provisioning of an identity by IdentityIQ and performing PAM on the account can be unified to provide a seamless approach within an environment.

BeyondTrust provides SailPoint customers with:

- Complete privileged access and vulnerability management integration
- Bi-directional role reporting
- Complete visibility reporting

BeyondTrust and SailPoint provide unified visibility and control over privileged and non-privileged users and accounts. www.beyondtrust.com/solutions/identity-access-management/.

About BeyondTrust

BeyondTrust® is a global cyber 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 Access 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.