# RBAC vs. ABAC: What's the Difference?

October 31, 2019

In any company, network users must be both authenticated and authorized before they can access parts of the system capable of leading to security breaches. The process of gaining authorization is called access control. In this guide, I discuss the two main methods for managing access control for your systems—**role-based access control (RBAC)** and **attribute-based access control (ABAC)**—their differences, and the importance of **using an access rights management tool**. I also review SolarWinds® Access Rights Manager, which is my top choice for a comprehensive solution to help teams more easily monitor access control across their organization.



## Authentication and Authorization

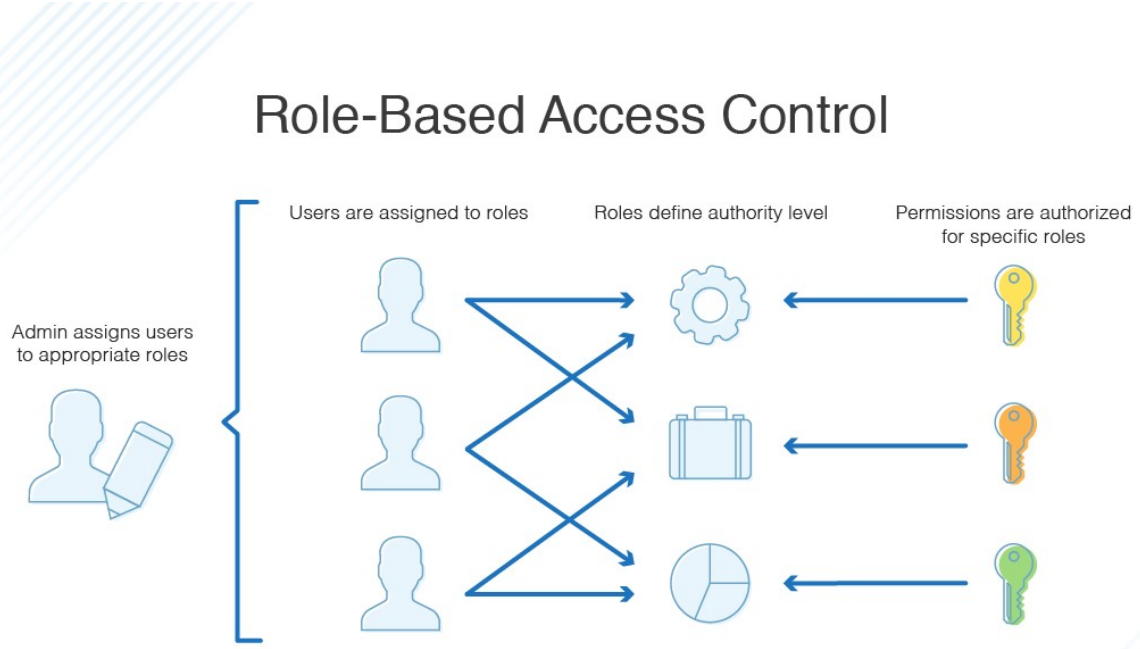
The two fundamental aspects of security are authentication and authorization. After you enter your credentials to log in to your computer or sign in to an app or software, the device or application undertakes authentication to determine your level of authorization. Authorization

may include what accounts you can use, what resources you have access to, and what functions you are permitted to carry out.

## Role-Based Access Control (RBAC) vs. Attribute-Based Access Control (ABAC)

Role-based access control (RBAC) and attribute-based access control (ABAC) **are two ways of controlling the authentication process and authorizing users**. The primary difference between RBAC and ABAC is RBAC provides access to resources or information based on user roles, while ABAC provides access rights based on user, environment, or resource attributes. Essentially, when considering RBAC vs. ABAC, RBAC controls broad access across an organization, while ABAC takes a fine-grain approach.

### What Is RBAC?




RBAC is role-based, so **depending on your role in the organization, you will have different access permissions**. This is determined by an administrator, who sets the parameters of what access a role should have, along with which users are assigned which roles. For instance, some users may be assigned to a role where they can write and edit particular files, whereas other users may be in a role restricted to reading files but not editing them.

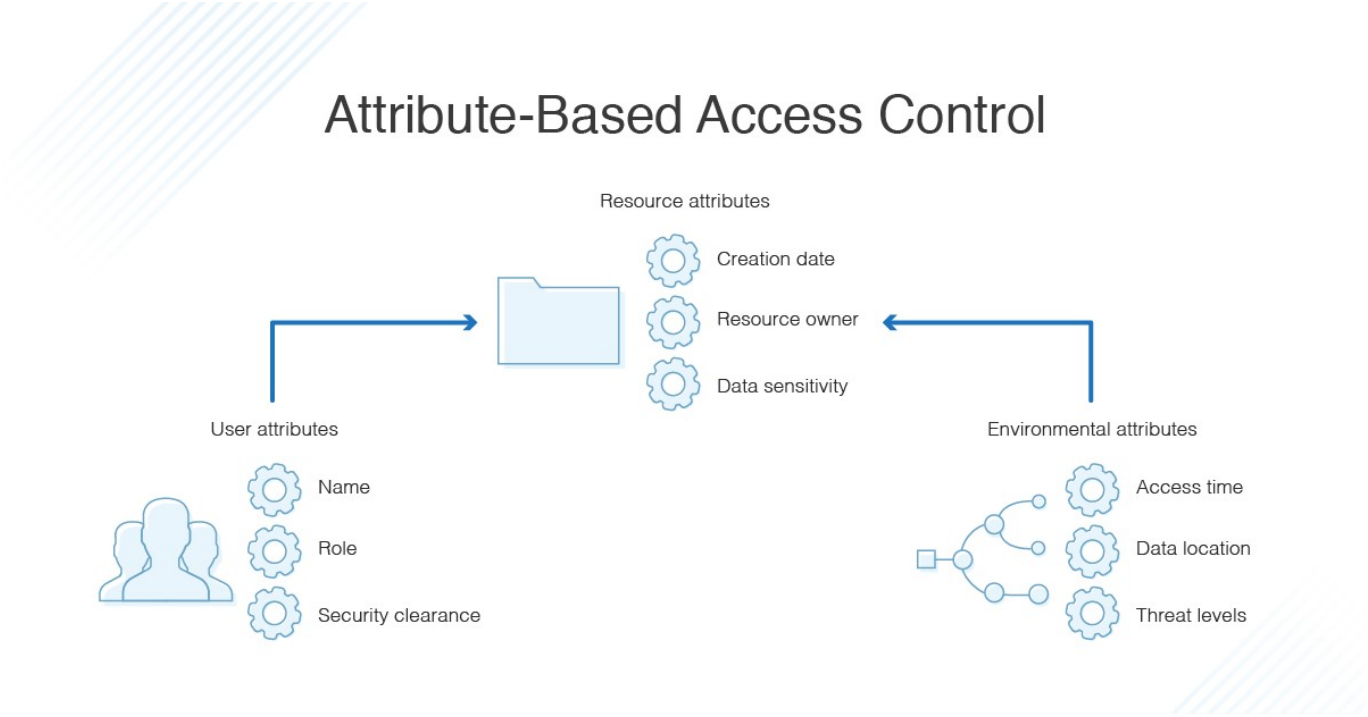
It's possible for one user to be assigned multiple roles, giving them access to numerous different files or abilities. Say there's a team of people working on a large project. The project

manager will have access to all the files and can edit and change things within the project. However, the development team might only be allowed access to the programming files and won't be able to see or edit the financial information or employee details for the project. On the flip side, the human resources or management team might have access to all the employee and financial information but has no use for the programming files.

An organization might use RBAC for projects like this because with RBAC, the policies don't need to be changed every time a person leaves the organization or changes jobs: they can simply be removed from the role group or allocated to a new role. This also means new employees can be granted access relatively quickly, depending on the organizational role they fulfill.

Back to top

## What Is ABAC?




Attribute-based access control draws on a set of characteristics called "attributes." This includes user attributes, environmental attributes, and resource attributes.

- **User attributes** include things like the user's name, role, organization, ID, and security clearance.
- **Environmental attributes** include the time of access, location of the data, and current organizational threat levels.

- **Resource attributes** include things like creation date, resource owner, file name, and data sensitivity.

Essentially, **ABAC has a much greater number of possible control variables than RBAC**. ABAC is implemented to **reduce risks** due to unauthorized access, as it can control security and access on a more fine-grained basis. For example, instead of people in the HR role always being able to access employee and payroll information, ABAC can place further limits on their access, such as only allowing it during certain times or for certain branch offices relevant to the employee in question. This can reduce security issues and can also help with auditing processes later.

### RBAC vs. ABAC

Generally, if RBAC will suffice, you should use it before setting up ABAC access control. Both these access control processes **are filters** with **ABAC being the more complex of the two, requiring more processing power and time**. There's no point in using this more powerful filter—and incurring the accompanying resource cost—if you don't need it.

Either way, it's important to use the minimum number of RBAC and ABAC filters to structure your access and security landscape. It **can help to carefully plan out your directory data and access approaches** to make sure you aren't using unnecessary filters or making things overly complex. In many cases, **RBAC and ABAC can be used together hierarchically, with broad access enforced by RBAC protocols and more complex access managed by ABAC**. This means the system would first use RBAC to determine who has access to a resource, followed by ABAC to determine what they can do with the resource and when they can access it.

Back to top

## Best Access Management Tools

Whether you use RBAC or ABAC, or a combination of the two, **I strongly suggest using an access rights management tool**. A good tool can streamline the setup and cut down on the administrative overhead involved in setting and managing filters. My pick is Access Rights Manager, a high-quality tool built to manage and audit access rights across your IT infrastructure.

Access Rights Manager includes a user management system **to monitor, analyze, and report on Active Directory and Group Policy**, and can show you what changes have been made, by

whom, and when, which helps you to minimize the likelihood of an insider threat. It **includes templates designed to help you enforce role-specific security and the provisioning and deprovisioning of user accounts**. You can smoothly delegate access to files, folders, or resources in a simple process to reduce administrative overhead.

## How to Choose an Access Control Solution

When it comes to security, it's crucial to plan and monitor your access control processes carefully. Use a robust access management tool to help you set up your access control, and regularly review your setup to make sure it still fits your organizational needs. Whether you invest in Access Rights Manager from SolarWinds or go another route, make sure the tool you choose can set up a protocol and mechanism to ensure users have the correct access to what they need to do their jobs, and nothing more.

---


### Related Posts

Best Active Directory Management Tools in 2020

Best NTFS Permissions Reporting Tools 2020

The Ultimate Guide to Active Directory Best Practices in 2020

Security

< The Best AWS Optimization and Monitoring Tools

> Top FREE Network Monitoring Tools


Search ...

## Most Popular Posts

Best Network Traffic Generator and Simulator Stress Test Tools

5 Best Free Help Desk Software and Ticketing Systems – DNSstuff

Best Wi-Fi Monitoring Tools

Spiceworks Help Desk vs. SolarWinds Web Help Desk Comparison

12 Best Log Monitoring Tools and Event Logging Software

## Categories

Cloud
Databases
General IT
Help Desk
Networking
Rezensionen zu Tools
Security
Systems
Tool Reviews