ENABLE SEAMLESS, SECURE ACCESS WITH ADAPTIVE AUTHENTICATION AND AUTHORIZATION

TECHNICAL BRIEF

INTRODUCTION

Whether you're managing employee, partner or customer identities, adaptive control over user authentication and authorization has become a necessity. Given the risks and costs associated with an attack or breach, it's more important than ever to move beyond passwords to a more secure and flexible form of authentication.

No longer can a username and password alone be used to decide whether a user can be authenticated or given access to a resource. Adaptive authentication and authorization allow you to evaluate contextual, behavioral and correlated data to make a more informed decision and gain a higher level of assurance about a user's identity.

As attack vectors become more sophisticated, adaptive policies allow you to strengthen your security posture. Adaptive authentication and authorization controls can reduce your attack surface by automatically requiring a higher level of assurance for users authenticating from certain IP addresses or geolocations. They can also evaluate a number of criteria, like when a user last authenticated, before granting access to a resource.

Adaptive policies also allow you to deliver a better user experience by giving your users the convenience and ease of use they expect. While adaptive controls are ideal for keeping bad guys out, they also streamline and enable easier access for users who have safe and predictable patterns of use. For employee use cases, this translates to increased efficiency and productivity.

81%

of hacking-related breaches leverage either stolen and/or weak passwords

Source: Verizon 2017 Data Breach Investigations Report

To establish these critical controls and allow for modification as conditions change, modern IAM solutions must provide a rich set of administrative tools. The following guide provides an overview of recommended adaptive authentication and authorization capabilities, and illustrates how the Ping Identity Platform measures up.

DYNAMIC POLICY DECISION MAKING

Adaptive authentication is much more than ensuring that a user has the correct credentials. It uses dynamic policy decision making to attain a level of assurance that a user is who they claim to be. Then, it will only permit access to a resource if that level of assurance exceeds the level of risk associated with the context of the request.

The level of assurance is established by how and when the user authenticated. Did the user provide a username and password six hours ago? Or did they provide their username and password, plus authenticate with a fingerprint, just a few seconds ago? The latter clearly provides a higher level of assurance.

The level of risk can be determined using contextual, behavioral or correlated data associated with a user, as well as the risk associated with the resource they're trying to access. For example, if the user is logging in from a foreign country instead of their home city, this may pose a greater risk. Also, if they're requesting changes to their personal 401k account, this presents a greater risk than requesting access to public stock trading information.

A simple username and password can be compromised by phishing scams, brute force attacks or through credential reuse. Adaptive authentication uses policies to evaluate user contexts, behaviors and other correlated data to associate a level of assurance with the user's authentication. The result may be to deny access, silently authenticate the user, or require a higher level of assurance, such as multi-factor authentication (MFA).

Adaptive authentication policies might evaluate a combination of user identity attributes, geolocation, user activity, IP address or other details before deciding how to route the authentication request. That dynamic policy decision is what differentiates adaptive authentication from traditional authentication approaches.

Similarly, adaptive authorization is more than just a binary rule to determine if a user gets access to a resource or not. After initial access rights are confirmed, it uses policies to match the level of assurance attained during authentication to the level of risk associated with a resource. A policy may require the user to step-up authentication with MFA, or simply provide their username and password again if too much time has passed since they last authenticated.

Authorization becomes adaptive when a policy dynamically decides whether or not to require additional levels of assurance before granting access to a resource. Only after the appropriate level of assurance is achieved can access be granted.

AUTHENTICATION AND ACCESS POLICIES

The Ping Identity Platform—a unified, standards-based solution encompassing MFA, single sign-on, access security, directory and data governance—achieves adaptive authentication through policies that contain decision points, or selectors, for the routing of authentication requests. Requests are routed based on details about each authenticating user and/or their device.

Your enterprise likely has multiple resources and just as many types of users who need to access them. Authorization policies in the Ping Identity Platform are associated with one or more apps, APIs or URLs and define the criteria required to access specific resources. Authorization policies can evaluate some of the same criteria that authentication policies can, such as attributes of the user. The same policies may apply for several resources.

Both authentication and authorization must work in concert to provide seamless and secure access to resources. The Ping Identity Platform can evaluate a long list of criteria, which fall into the following categories: device, attribute, behavior, resource, network/browser and risk.

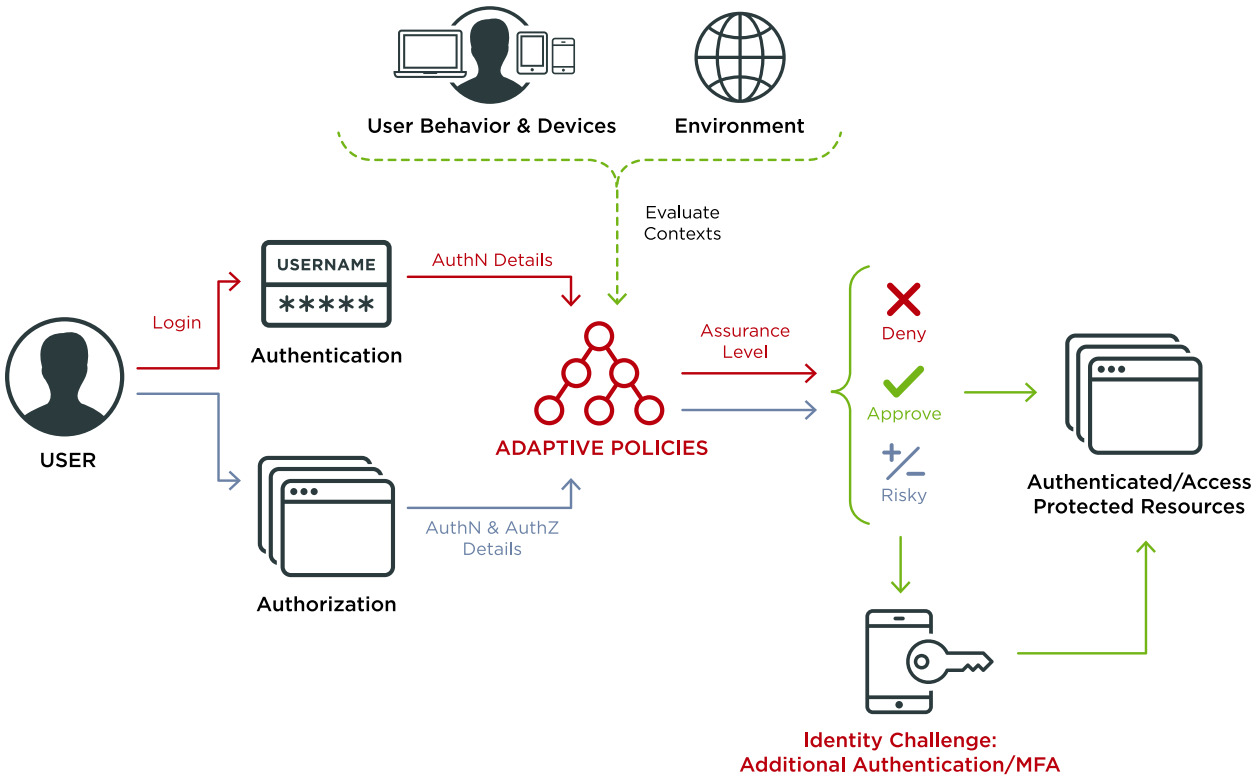
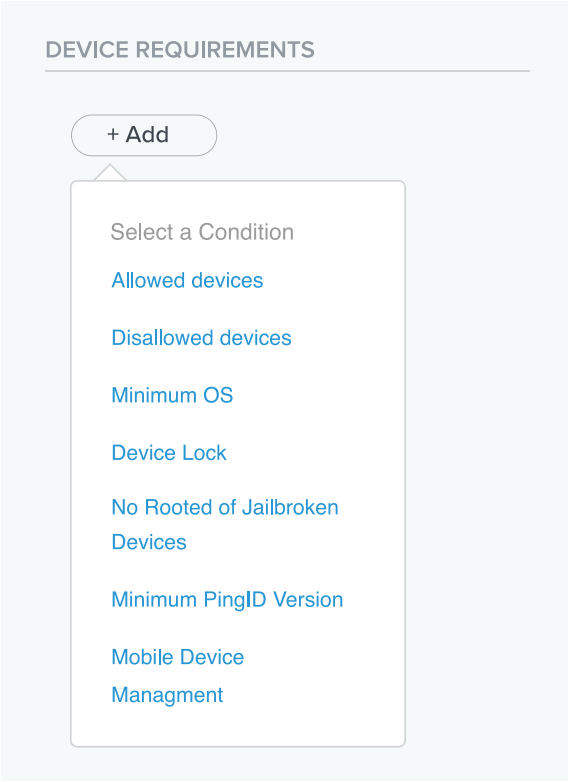


Figure 1: Adaptive policies can evaluate contextual risks and approve, deny or require additional authentication (MFA) for authentication and authorization requests.

DEVICE-BASED POLICY CONTROL

Device-based policies evaluate the context of the user's device. The context of the accessing device and/or the context of the authenticating device can be evaluated. These contexts can include the geolocation of the device and data about its security posture and operating system configuration. For example, you may want to define stricter authentication practices for older, more vulnerable OS versions on accessing devices. For authenticating devices, those that are rooted or don't meet minimum OS version requirements can be restricted from approving MFA requests (as shown in Figure 2).

Figure 2 (to the right): Policies can be established to evaluate the context of the user's device.



ATTRIBUTE-BASED POLICY CONTROL

Policies can also consider the attributes of a user. A common use case is evaluating a "group" attribute and defining which application/s that group's members can access (as shown in Figure 3). Beyond group membership evaluation, the options are limitless. Attributes such as age, premium member status or virtually any other criteria can be evaluated to approve or deny access, or to determine which authentication mechanisms are required to attain the appropriate level of assurance.

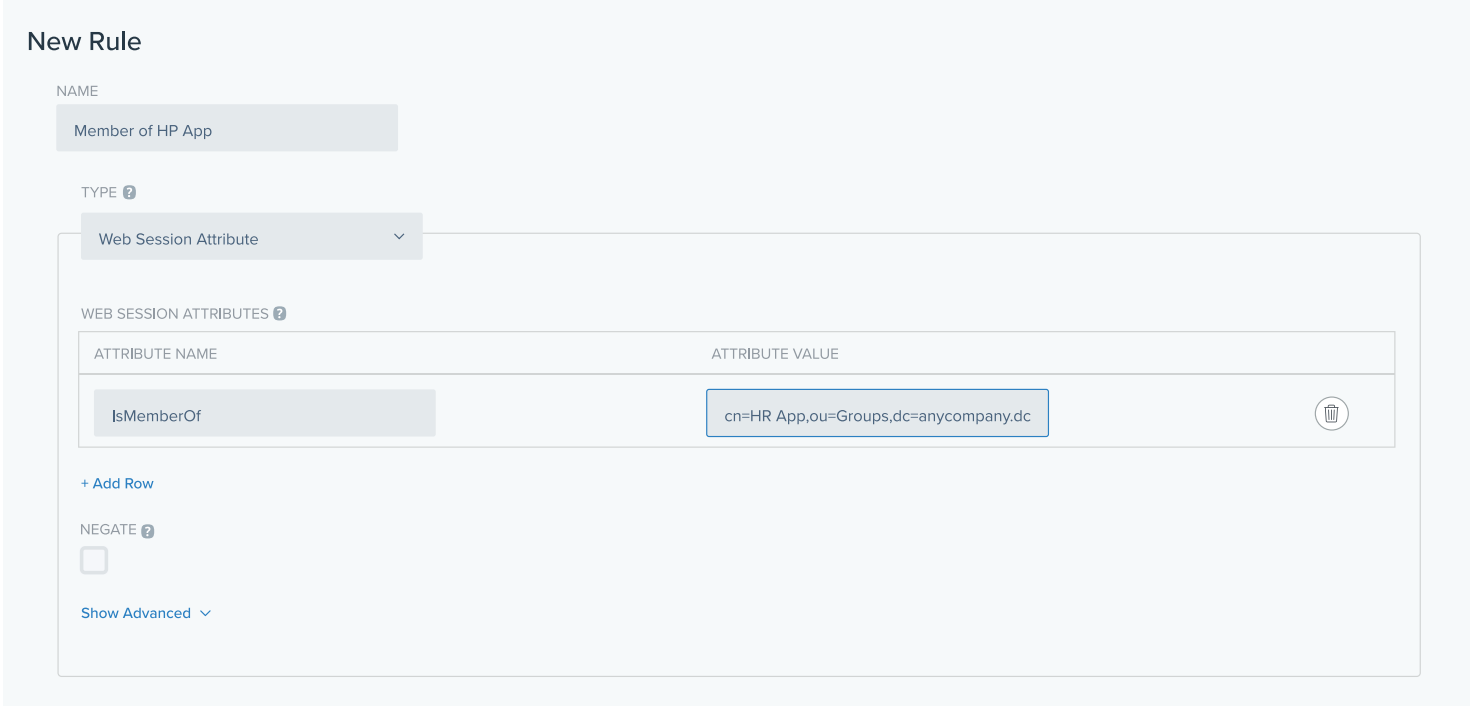
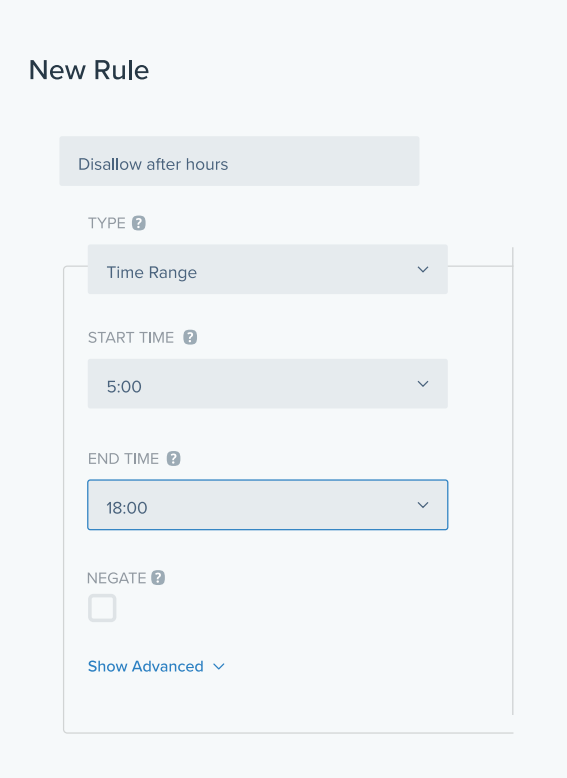


Figure 3: Policies can be established based on user attributes, including "group" attributes.

BEHAVIOR-BASED POLICY CONTROL

User behaviors can also be considered during authentication and authorization flows. For example, you can set controls based on the user's original authentication, the last time they were authenticated from their current device, or the time of day (as shown in Figure 4). Additionally, you can change the course of a flow if a large number of authentication requests come through in a short period of time, which can help defend against brute force attacks.

Figure 4 (to the right): Policies can be established based on user behaviors, including the time of day.



RESOURCE-BASED POLICY CONTROL

The resource being accessed, from the application down to the specific URL or API, can be evaluated alongside other user and device contexts during authorization. These authorization policy rules can be built around one or more resources. They can allow only specific groups to access certain applications (as shown in Figure 5), or require MFA for high-value resources.

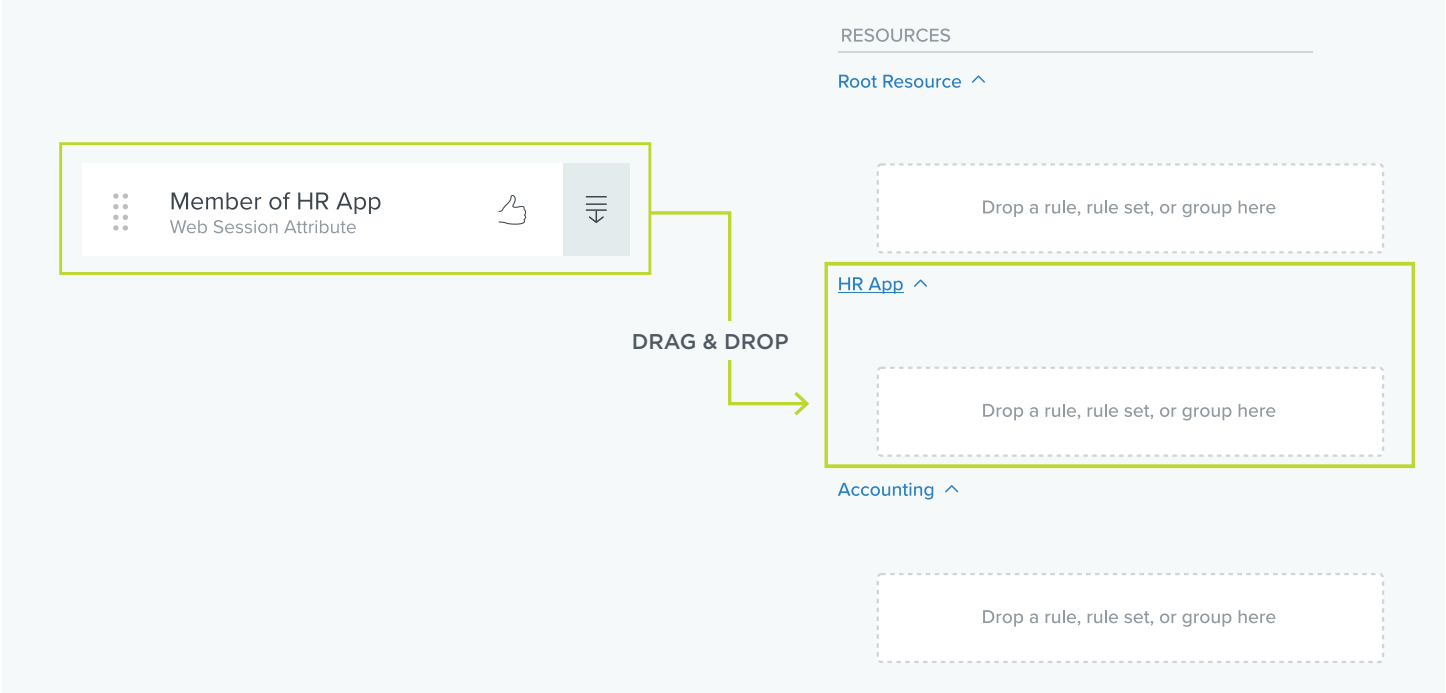


Figure 5: Policies can be established that allow only certain users access to resources.

NETWORK AND BROWSER-BASED POLICY CONTROL

A wide variety of network and browser details can be evaluated. These include IP address ranges, requested OAuth scopes, HTTP header data, predefined origin servers and more. These technical details can be used to ensure that a user is authenticating from a known office location's network, or that certain HTTP request parameters exist. Similarly, they can be used to deny access from certain countries (as shown in Figure 6).

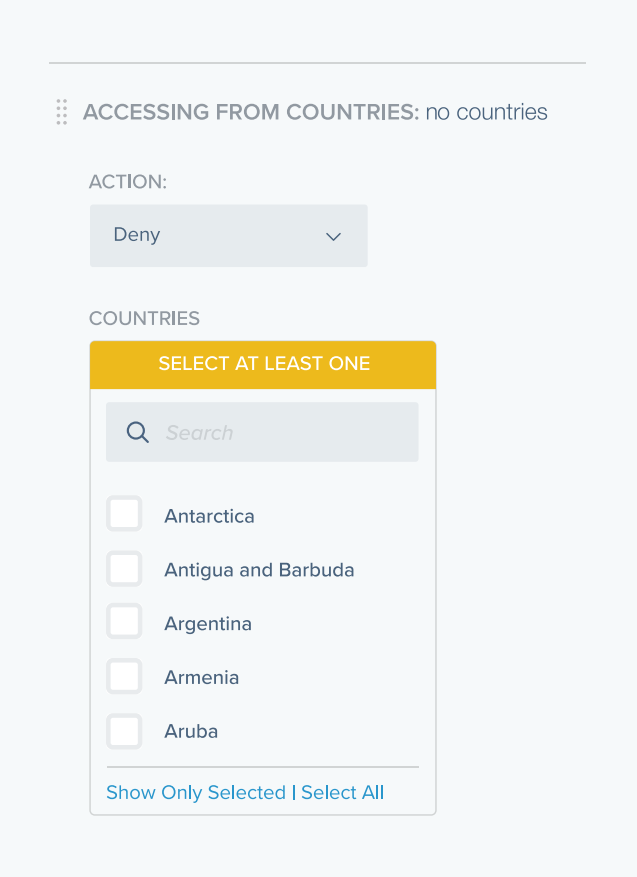


Figure 6: Policies can be established based on network and browser details, including geolocation.

RISK-BASED AUTHENTICATION (RBA)

Ping partners and integrates with several third-party risk-based authentication providers. Through these integrations, the Ping Identity Platform can leverage sophisticated risk analysis as one of many steps in an authentication flow. These algorithms can detect device rooting cloaking techniques, as well as utilize anonymized digital identity intelligence from some of the world's largest e-commerce, payment and financial brands. RBA can be leveraged alongside other attribute, activity and resource-based criteria to ensure an extremely high level of assurance about a user's identity.

COMMON USE CASES

The number and combinations of attributes and criteria that you can utilize to structure adaptive policy controls is virtually limitless. Here are several common use cases that demonstrate how you might structure your own policies to ensure secure and seamless access for users.

REQUIRE MFA FOR REMOTE ACCESS

Enterprises may choose to require multi-factor authentication for employees that aren't in the office. As shown in Figure 7, the first step is to evaluate the IP address of the accessing device to determine whether it's inside the office's IP network range. If the device is in the network, Integrated Windows Authentication (IWA)/Kerberos authentication can be required. If the user's trusted authenticating device is also inside a geofence around the office, access will be granted immediately. If it isn't, MFA will be required. If a user's accessing device isn't authenticating from an office IP address, MFA will always be required. This allows for faster authentications for users who fall within standard, safe usage patterns, while requiring higher levels of assurance for more risky scenarios.

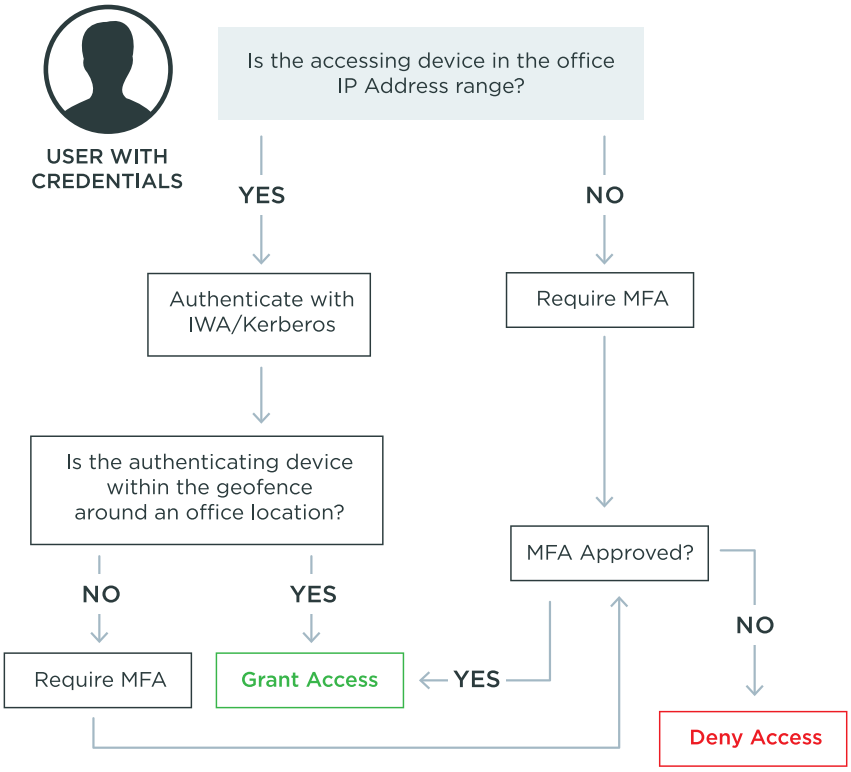


Figure 7: This workflow illustrates a policy that requires multi-factor authentication for those authenticating from outside an office.

LIMIT ACCESS USING GROUP MEMBERSHIP

Authorizing users to access applications based on an attribute that defines their group membership is another common use case. This makes granting access to new applications or provisioning new employees much easier. Policies can be modified to include new applications or new employee profiles based on a specific group attribute. Figure 8 illustrates a common scenario involving access to HR applications. As shown, you first determine whether a user trying to access an HR application is a member of the HR group. If so, you can establish policies based on the resource being accessed, like a payroll application. Because it contains sensitive data, it requires a higher level of assurance than other HR applications.

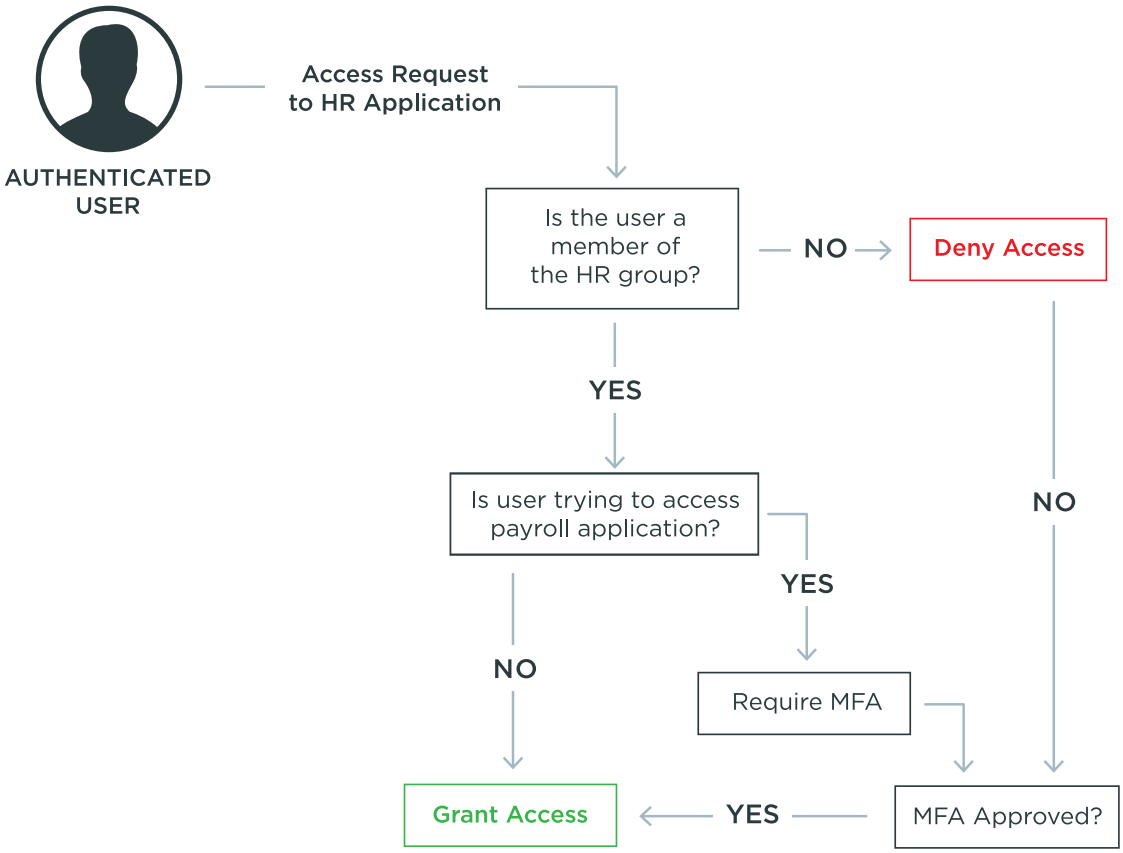


Figure 8: This workflow illustrates a policy that limits access to a sensitive HR resource based on group attributes.

REQUIRE MFA BASED ON USER BEHAVIOR

Let's assume an HR user has just proceeded through the flow in Figure 8 and was able to access the payroll application by providing MFA. A few minutes later, this same user tries to access a specific URL within the payroll app to see information about employee salaries and other sensitive data (as shown in Figure 9). Since the user just provided MFA to access the payroll app from the same accessing device, you may choose not to require the user to authenticate again for a page within the same app. However, if the same user is still authenticated but has been idle for a long period of time, you may want to require MFA again before granting access to a high-value page within the app. The length of time can be set to any number of minutes, hours or even days based on your security team's preferences.

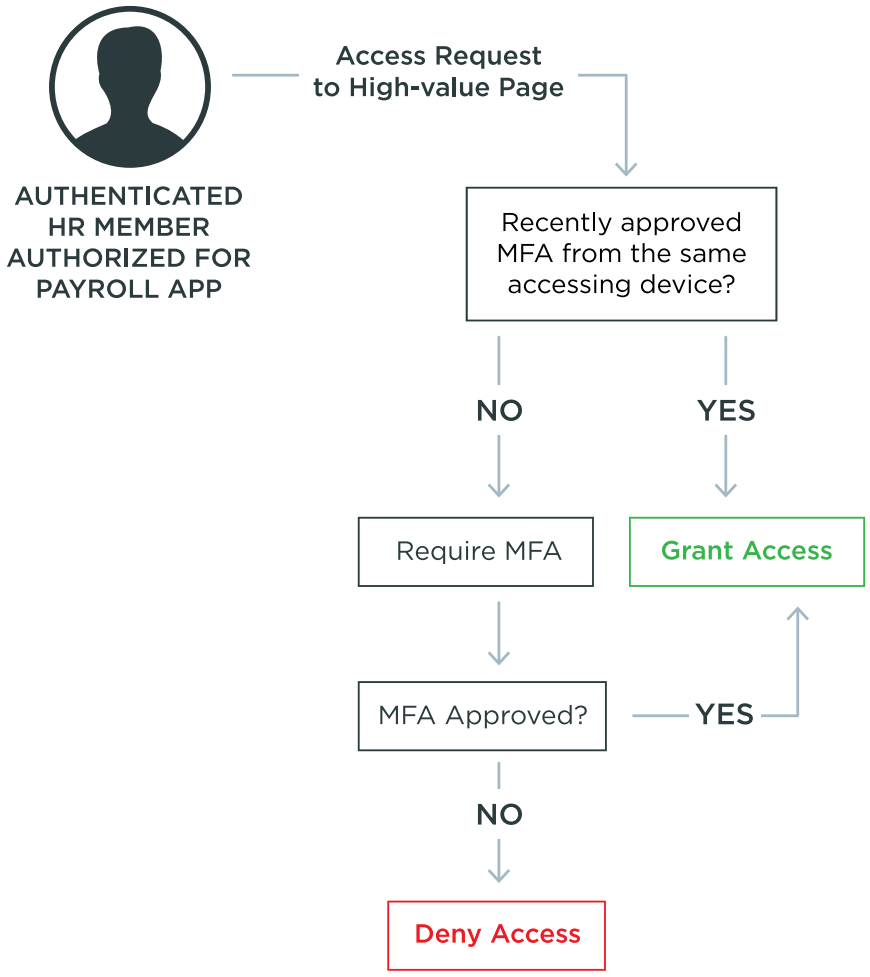


Figure 9: This workflow illustrates a policy that limits access to sensitive resources based on the accessing device and amount of time since the last authentication.

ESTABLISHING YOUR POLICIES

The Ping Identity Platform can support a wide range of enterprise use cases as shown in the following two tables. The first table shows which criteria can be evaluated by policies within each authentication and authorization solution. The second describes how each solution's policies can route requests.

PING IDENTITY PLATFORM:
Evaluation of Criteria by Capability

POLICY EVALUATION CRITERIA	SINGLE SIGN-ON controls token minting	ACCESS controls access to resources	MFA bypass or require MFA	POLICY CATEGORY
USER ATTRIBUTES *Does the user have specific attributes?*	✓ *(From AuthN Sources)*	✓ *(From Token)*	✓ *(From Token)*	Attribute
GEOFENCING *Is the device within a certain geofence?*			✓	Device
DEVICE POSTURE *Is the device rooted, MDMed or lock enabled? What is the OS version?*			✓	Device
NETWORK RANGE *Does the IP address fall within a certain range?*	✓	✓	✓	Network/Browser
FROM COUNTRY *Is the IP address from a certain country?*			✓	Network/Browser
RECENT AUTHENTICATION FROM DEVICE *Did the user perform MFA already in the last X minutes, hours, days on this device?*			✓	Behavioral
RECENT AUTHENTICATION FROM LOCATION *Was authenticating device within a known geofence recently and is the accessing device the same?*			✓	Behavioral
OAUTH SCOPE *Is there a match in requested and configured OAuth scopes?*	✓	✓		Network/Browser

PING IDENTITY PLATFORM: EVALUATION OF CRITERIA BY CAPABILITY (CONT.)

POLICY EVALUATION CRITERIA	**SINGLE SIGN-ON** controls token minting	**ACCESS** controls access to resources	**MFA** bypass or require MFA	POLICY CATEGORY
HTTP REQUEST PARAMETERS *Does a certain HTTP query parameter exist?*	✓	✓		Network/Browser
APPLICATIONS *Which application or federation partner is the user trying to access?*	✓	✓	✓	Resource
API/URL *Which API or URL is the user trying to access?*		✓		Resource
TIME OF DAY *What time of day was the request received?*		✓		Behavioral
RATE LIMITING *Are authentication requests being sent too frequently?*		✓		Behavioral
PINGFEDERATE CLUSTER NODE *Which PingFederate cluster node is servicing the request?*	✓			Network/Browser
SERVICE PROVIDER CONNECTION *Is there a match between the target SP connection and SP connections configured in PingFederate?*	✓			Network/Browser
HTTP HEADER *Is there a match for a specific HTTP header?*	✓	✓		Network/Browser
AUTHENTICATION CONTEXT *How was the user originally authenticated?*	✓	✓		Behavioral
CORS (CROSS-ORIGIN RESOURCE SHARING) *Evaluates predefined origin servers.*		✓		Network/Browser
NEW DEVICE *Is the device attempting web access requesting PingID authentication for the first time?*			✓	Network/Browser & Behavioral
RBA *Leverages sophisticated risk analysis techniques.*	✓			RBA

PING IDENTITY PLATFORM:
Routing of Authentication and Authorization Requests

REQUEST ROUTING OPTIONS	**SINGLE SIGN-ON** controls token minting	**ACCESS** controls access to resources	**MFA** bypass or require MFA
Send to authentication source **Includes MFA*	✓ *(Any third party IDP)*	✓ *(Through PingFederate Adapter)*	
Require swipe, SMS, email, hard token or other second factor			✓
Silently authenticate or prompt user for MFA approval			✓
Approve or deny authentication requests	✓		✓
Approve or deny access to resources **Denials routed back to PingFederate or Azure AD in Microsoft use cases*		✓	

CONCLUSION

The adaptive authentication and authorization capabilities of the Ping Identity Platform can help you mitigate security threats, while increasing convenience for your customers, partners and employees. Supporting a wide range of adaptive use cases, the Ping Identity Platform allows you to define authentication and authorization policies based on any number and type criteria, including the context of users, devices, web browsers, networks and more.

To learn more and see a demo of Ping's adaptive authentication and authorization capabilities, visit www.pingidentity.com.

#3271 | 08.17