BEST PRACTICES GUIDE

SECUREAUTH

ADAPTIVE AUTHENTICATION
BEST PRACTICES GUIDE

TABLE OF CONTENTS

Introduction

Using adaptive authentication, SecureAuth IdP can provide multiple silent risk checks without the end user ever knowing, evaluating the risk of every access request. This enables you to allow access for low-risk requests without a multi-factor authentication (MFA) step, require MFA for medium risk, and deny or redirect for high risk, delivering the most user-friendly authentication experience while stopping attackers, even if they have stolen credentials and innovative ways to defeat some MFA methods.

This is a feature many users appreciate. When users are on-site, they go about their job and the device they are using is not prompted for credentials; however, if they take their devices off-site and out of network, they are automatically prompted for credentials. Another example is on initial log-on to the system, the user is prompted for second factor authentication (2FA). On subsequent log-ons, the user is not prompted because adaptive authentication recognizes the device or user and allows them to bypass second factor.

Every time prospective users attempt to sign on, they can be assessed on the basis of multiple risk checks, as depicted in Figure 1.

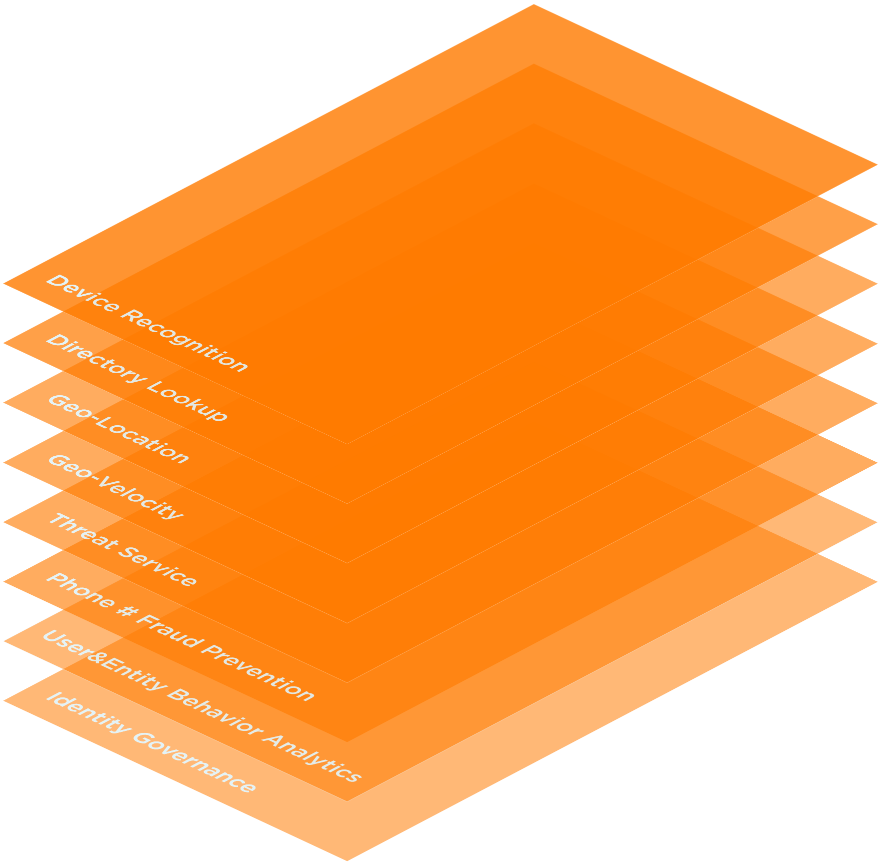


Figure 1. Adaptive Authentication Risk Checks

By layering security, you can reduce your level of risk and increase your level of security. Each of these risk checks represents another layer of scrutiny that can be used to make it increasingly more difficult for a suspect device or suspicious credential to gain access to the protected area.

The essential steps for configuring IdP for adaptive authentication are detailed in https:// docs.secureauth.com/x/0giLAg.

The specific adaptive authentication risk checks, the way they are implemented in SecureAuth IdP, and recommendations for configuring them are detailed in "Adaptive Authentication Risk Checks" starting on page 4.

Benefits

- Increase security without impacting users with pre-authentication risk analysis.
- Tailor the authentication process to different user types with flexible workflows.
- Maintain productivity and reduce help desk calls with user self-service password reset and account unlock.
- Improve user convenience and protect against password fatigue with single sign-on.
- Process secure access with flexibility and choice using more than 25 MFA methods.
- Optimize, rather than replace, existing security investments.
- Empower user to go passwordless with high identity confidence.
- Deploy enterprise-wide and eliminate the cost and complexity of multiple disparate security solutions.
- Correlate identity threats and data with SIEMs and other security systems for more holistic and orchestrated protection.

Adaptive Authentication Risk Checks

Each of the risk checks currently available for end-user post-authentication are explained in the following subsections.

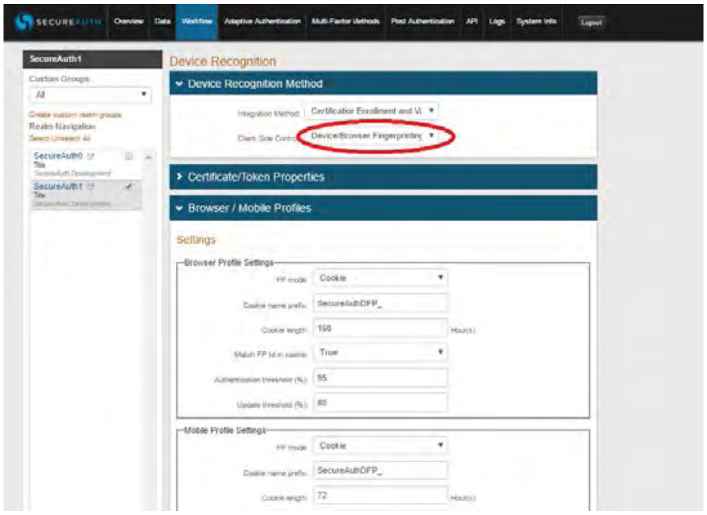
> **NOTE:** Adaptive authentication requires special SecureAuth IdP licenses to access and use. These are available through the SecureAuth Protect and Prevent packages. Contact SecureAuth Support for more information and upgrade information.

Device Recognition

SecureAuth analyzes the device being used to submit the log-in request. If the device profile deviates from accepted norms for the user (such as a previously unused computer), additional levels of authentication are added.

According to Verizon's 2015 Data Breach Investigation Report, the probability of a breach using a stolen device is 6%. SecureAuth Device Recognition can detect all such non-stolen (non-registered) devices. So, if we can stop all attacks without a stolen device, the probability of a breach getting through is 6%; that means that the rest of the attacks (94%) will be stopped by the Device Recognition detector, since it won't be registered as a previously verified device.

Device Recognition appears in the Workflow section of the Web Admin for a specific realm after you have selected the Device / Browser Fingerprinting option from the Client Side Control drop-down field.



Integration Method: Certification Enrollment and V

Client Side Control: Device/Browser Fingerprinting

Browser Profile Settings

FP mode: Cookie

Cookie name prefix: SecureAuthDFP_

Cookie length: 168 Hour(s)

Match FP Id in cookie: True

Authentication threshold (%): 95

Update threshold (%): 80

Mobile Profile Settings

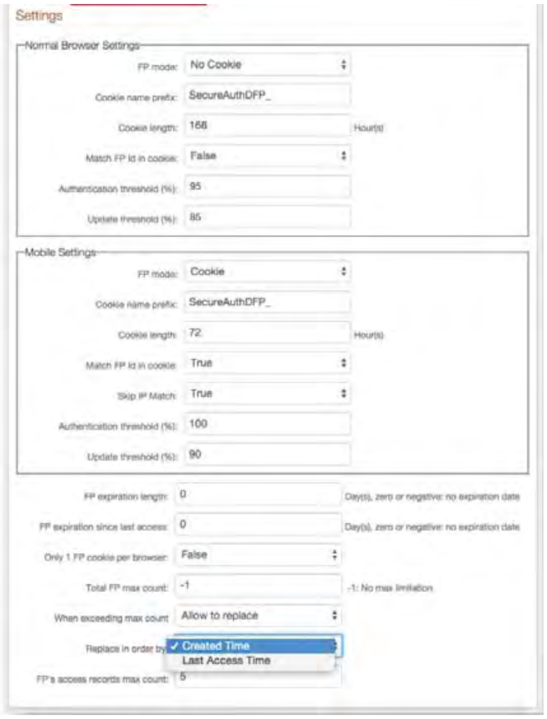
FP mode: Cookie

Cookie name prefix: SecureAuthDFP_

Cookie length: 72 Hour(s)

Figure 2. Device/Browser Fingerprinting Option

Scroll down to the Settings section which looks like the example in Figure 3.



Settings

Normal Browser Settings

FP mode: No Cookie

Cookie name prefix: SecureAuthDFP_

Cookie length: 168 Hour(s)

Match FP Id in cookie: False

Authentication threshold (%): 95

Update threshold (%): 85

Mobile Settings

FP mode: Cookie

Cookie name prefix: SecureAuthDFP_

Cookie length: 72 Hour(s)

Match FP Id in cookie: True

Skip IP Match: True

Authentication threshold (%): 100

Update threshold (%): 90

FP expiration length: 0 Day(s), zero or negative: no expiration date

FP expiration since last access: 0 Day(s), zero or negative: no expiration date

Only 1 FP cookie per browser: False

Total FP max count: -1 -1: No max limitation

When exceeding max count: Allow to replace

Replace in order by: ✓ Created Time

FP's access records max count: 5

Figure 3. FP Settings

The Settings section appears, including fields to configure for both browser and device settings. The Browser page defines the characteristics this realm is expecting to find for the browser seeking to log in. The Device page defines the characteristics deemed most important to identify the device being used to log in. The administrator is asked to weigh the importance of each profile component, by using a slider. Since the required maximum is 100%, an administrator is prompted when he/she has exceeded or underrated the components.

Select options or enter information for the following fields:

Field	Description/Recommendations
Normal Browser Settings	
FP Mode	Select **Cookie** from the drop-down field to enable SecureAuth IdP to deliver a cookie to the browser after authentication. If this option is selected, the Cookie name prefix and Cookie length are activated. Recommended setting is **Cookie**.
Cookie name prefix	If the **Cookie** option is selected in FP Mode, either enter a desired prefix or keep the default value. The cookie name format appears as Cookie Name Prefix + company name + hashed value of user ID.

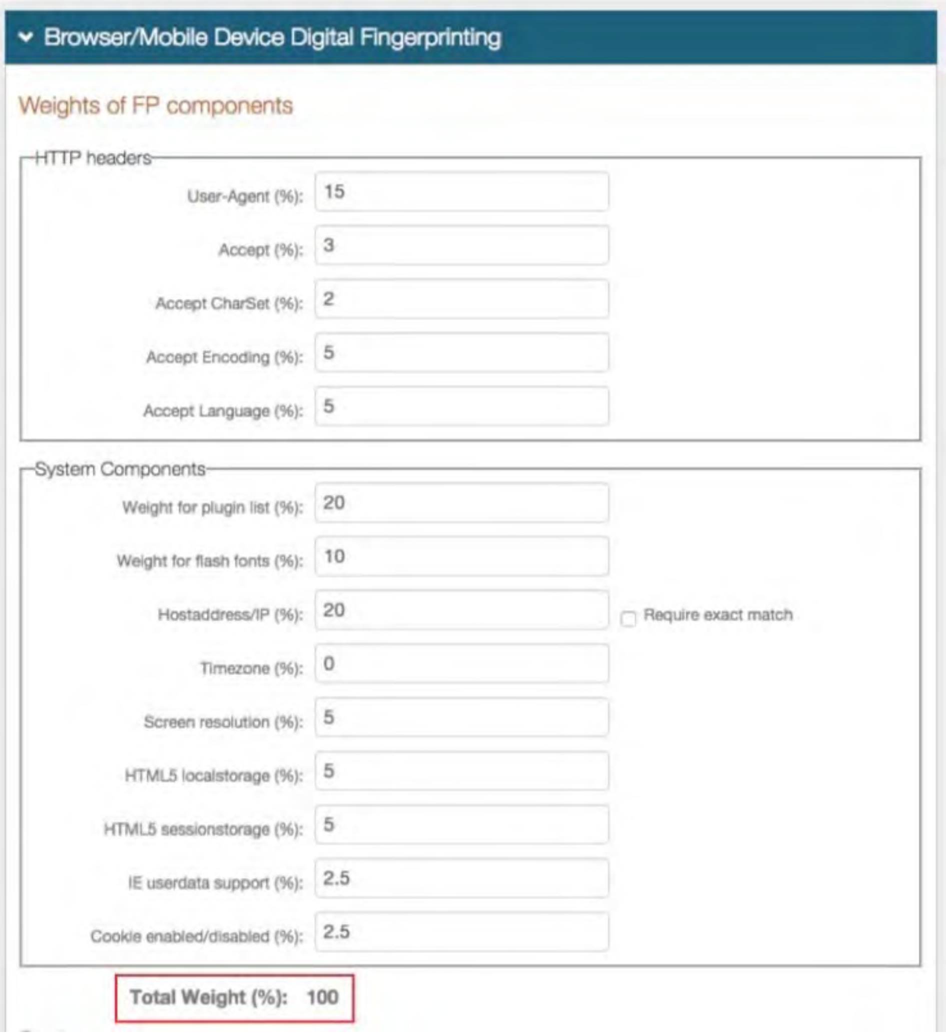
Field	Description/Recommendations
Cookie length	If the **Cookie** option is selected in FP Mode, specify how many hours the cookie is valid, such as 168 hours.
Match FP in cookie	Select **True** to require the digital fingerprint ID to be presented and then matched to a digital fingerprint ID in the directory, with an acceptable Authentication Threshold score. Select **False** to not require ID matching between the cookie and the stored digital fingerprint.
Authentication Threshold	Determines whether additional 2FA is required (OTP). Set in the range 90-100% based on preference. This value must be greater than the Update Threshold value. For example, if the Authentication Threshold is set to 95 and the Update Threshold is set to 85, then the following evaluation would be done on subsequent authentications: + <FP-Score> represents the score of the presented digital fingerprint + If <FP-Score> > 95, then no additional 2FA is required + If <FP-Score> < 95, but > 85, then additional 2FA is required and the + existing digital fingerprint is updated with the presented fingerprint + information + If <FP-Score> < 85, then additional 2FA is required, and a new digital + fingerprint will be created Recommended setting is 95.
Update Threshold	Determines whether an existing digital fingerprint is to be updated with new information from the presented digital fingerprint, or if a new digital fingerprint must be created. Set to the range 80-90% based on preference. This value must be less than the Authentication Threshold value. Recommended setting is 80.
Mobile Settings	
FP Mode	Select Cookie to deliver a cookie to the mobile device. The Cookie name prefix, Cookie Length, and Match FP ID to cookie fields are activated. Select App Mode to utilize the DR App for further device recognition. The App Mode option requires the SecureAuth Device Recognition (DR) App for iOS and Android.
Cookie name prefix	If the Cookie option is selected in FP Mode, leave as the default or set it to a preferred name. The cookie name format appears as Cookie Name Prefix + company name + hashed value of user ID.
Cookie Length	If the Cookie option is selected in FP Mode, set to the number of hours during which the cookie is valid, such as 72 hours.

Field	Description/Recommendations
Match FP ID in cookie	If the Cookie option is selected in FP Mode, select True to require the digital fingerprint ID to be presented and then matched to a digital fingerprint ID in the directory, with an acceptable Authentication Threshold score. Select True to require ID matching between the cookie and the stored digital fingerprint.
Skip IP Match	Select True if an exact IP Address match for device recognition comparison is not required. Select False to require an exact match for device recognition comparison. Recommended setting is True.
Authentication Threshold	Determines whether additional 2FA is required (OTP). Set in the range 90-100% based on preference. The Authentication Threshold value must be greater than the Update Threshold. For example, if the Authentication Threshold is set to 95 and the Update Threshold is set to 85, then the following evaluation would be done on subsequent authentications: + <FP-Score> represents the score of the presented digital fingerprint + If <FP-Score> > 95, then no additional 2FA is required + If <FP-Score> < 95, but > 85, then additional 2FA is required and the existing fingerprint is updated with the presented digital fingerprint information + If <FP-Score> < 85, then additional 2FA is required, and a new digital fingerprint will be created Recommended setting is 100.
Update Threshold	Determines whether an existing digital fingerprint is to be updated with new information from the presented digital fingerprint, or if a new digital fingerprint must be created. Set in the range 80-90% based on preference. The Update Threshold value must be less than the Authentication Threshold.
FP expiration length	Set to the number of days the digital fingerprint is valid. Set to 0 for no expiration. For example, if this field is set to 10 days, then the user's fingerprint expires in 10 days, no matter how often it is used.
FP expiration since last access	Set to the number of days the digital fingerprint is valid since the last usage. Set to 0 for no expiration. For example, if this field is set to 10 days, then the user's digital fingerprint expires if it is not used during the 10 days since it was last employed.

Field	Description/Recommendations
Total FP max count	Set to the maximum number of digital fingerprints that can be stored at a given time. Set to -1 for no maximum entries. If a maximum is to be set, a typical configuration would limit digital fingerprint storage to 3-8.
When exceeding max count	If a maximum value is specified in Total FP max count, select Allow to replace to enable the replacement of an existing digital fingerprint with a new one, or select Not allow to replace if the digital fingerprints cannot be automatically replaced. If Not allow to replace is selected, the user or administrator must manually remove stored fingerprints from the user profile on the Self- Service Account Update Page or Account Management (Help Desk) Page.
Replace in order by	If a maximum is specified in Total FP max count and Allow to replace is selected above, select Created Time to enable the replacement of the oldest stored digital fingerprint with the new one; or select Last Access Time to enable the replacement of the least recently used digital fingerprint with the new one. Recommended setting is Created Time.
FP's access records max count	Set to the number of access history entries per digital fingerprint stored in the profile. SecureAuth recommends set this value to 5.

To create unique digital fingerprints for a device or browser, you must specify the number of components on which the profile is based and how each component is weighed.

The Weights for FP Profiles are configured on the Workflow page under the Weights of FP Components section as shown in the following example.



Browser/Mobile Device Digital Fingerprinting

Weights of FP components

HTTP headers

User-Agent (%): 15

Accept (%): 3

Accept CharSet (%): 2

Accept Encoding (%): 5

Accept Language (%): 5

System Components

Weight for plugin list (%): 20

Weight for flash fonts (%): 10

Hostaddress/IP (%): 20 □ Require exact match

Timezone (%): 0

Screen resolution (%): 5

HTML5 localstorage (%): 5

HTML5 sessionstorage (%): 5

IE userdata support (%): 2.5

Cookie enabled/disabled (%): 2.5

Total Weight (%): 100

Figure 4. Weights of FP Components

The total values designated in these fourteen fields must add up to 100%. It is the way in which these values are prioritized that determines how SecureAuth treats them during the detection process and how the program algorithm computes the score that determines the profile assigned. This section provides you with recommendations on what weights are best assigned to each component.

Weighted Field	Description/Recommendations
HTTP Headers	
User Agent	The user agent string (identification) of the user agent. This field is a highly important value, indicating the identity of the device to a high degree, and should be assigned up to 30% of the total.
Accept	The Content-Types that are acceptable for the response. This field is one of the least important values you will assign. Recommended value for this is 2-3%.
Accept Charset	The character sets that are acceptable. The weight you assign to this field depends on the importance you place on the character sets that this device utilizes. For the most part, this cannot be used as an important indication of identity. In general, we recommend assigning this field between 0-2%.
Accept Encoding	The list of acceptable encodings. This field cannot normally be used as a fair judge of identity. Normally, this field can only be weighted to 0-2%.
Accept Language	The list of acceptable human languages for response. Most devices use an unvarying assortment of languages. Therefore, this is field can be reliably assigned a value of 0-2%.
System Components	
Weight for Plugin list	The list of plug-ins on the user's browser. This value might change frequently on a person's browser since plug- ins are frequently added, so it is not a particularly good indication of identity. We recommend setting this to 5%.
Weight for flash font	The fonts inside of a flash application. This value can change frequently, depending on the flash application being used, so this is not a sensitive detector of identity. We recommend setting this to 5%.
Hostaddress/IP	The Host address or IP address for this device. This is a very important factor in detecting identity. We recommend setting this weight to 35-40%.
Require exact match	Click to check this box to require an exact match of the address. If enabled, the user will have to perform a different 2FA without an exact match, even if the Authentication Threshold percentage is met. In general, we do not require that this component be checked.
Timezone	The time zone of the user's browser. Recommended setting is 10%.

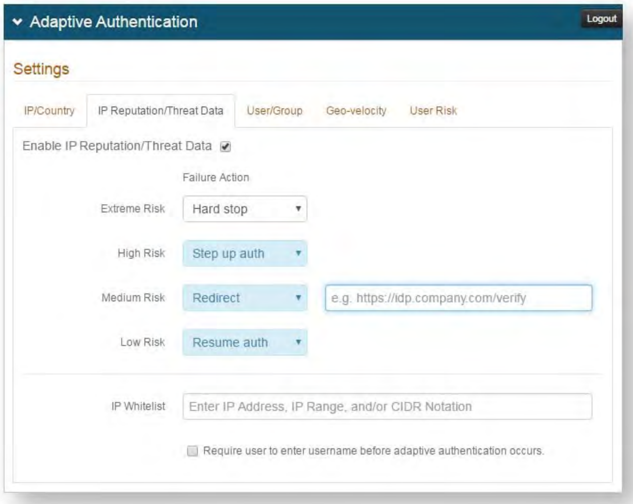
Weighted Field	Description/Recommendations
Screen resolution	The screen resolution of the device/browser. If only one screen is used, this can be an important component in determining identity; however, when a double or multiple monitor setup is used for a device, this component becomes problematic since multiple monitors are rarely of the same sort or resolution. In general, we recommend setting this weight to 5%.
HTML localstorage	The HTML5 local storage. This component should not change greatly and should be assigned some weight: normally, we recommend 5%.
HTML sessionstorage	The HTML5 session storage. This component should not change greatly and should be assigned some weight: normally, we recommend 5%.
IE userdata support	The Internet Explorer (IE) user data support. While some devices always use IE, there are many that use other browsers, such as Google or Firefox, or use a variety of browsers during a single session, so this is generally not a reliable indication of identity. For this reason, we recommend assigning a weight of 5%.
Cookie enabled/ disabled	Based on the user's settings, whether cookies are enabled or disabled. Cookies can be enabled or disabled indiscriminately, and often in the background. Therefore, this does not indicate a good evaluator of identity. For this reason, we recommend assigning a weight of 5%.

Threat Services

The SecureAuth Threat Services can detect authentication attempts from command and control (C2) servers and botnets. Sixteen percent of breaches are orchestrated by attackers logging in from known C2 Servers. According to the 2015 Verizon Data Breach Report, 84.13% of crimeware/malware uses C2 infrastructure – 15.87% of ALL attacks involved C2. SecureAuth's Threat Service monitors C2 communications and blocks suspicious queries.

What percentage of hackers are using proxy networks, through browsers such as Tor, or are repeat offenders? A SecureAuth study last year of our top customers revealed that 8,251 out of 8,723, or 94.59%, of all attacks came from the dark web. We know from Tor itself that there are currently about 2 million Tor users, and it is highly likely that 100% of those hitting a corporate network are nefarious. SecureAuth can detect and mitigate proxy networks and Tor encounters through our threat service. We also can check the IP address for historical malicious activity. With the probability of a breach coming from the dark web being 94.59%, if we only stop all attacks from the dark web, the probability of a breach is down to 5.41%.

Threat services are configured through the IP Reputation/Threat Data tab page on the Workflow page's Adaptive Authentication section.



Enable IP Reputation/Threat Data ☑

Failure Action

Extreme Risk: Hard stop

High Risk: Step up auth

Medium Risk: Redirect — e.g. https://idp.company.com/verify

Low Risk: Resume auth

IP Whitelist: Enter IP Address, IP Range, and/or CIDR Notation

☐ Require user to enter username before adaptive authentication occurs.

Figure 5. IP Reputation/Threat Data Page

Once you have checked the Enable IP Reputation/Threat Data box, the threat analysis is activated.

The available threat types are:

Threat Type	Score	SA IdP Risk Category	Definition
Anonymous Proxy	100	Extreme	Authentication is coming from a server that is designed to hide or anonymize the actual source IP Address Recommended setting: Hard Stop
Attacker	99	Extreme	Indicators confirmed to host malicious content, has functioned as a command-and-control (C2) server, and/or has otherwise acted as a source of malicious activity Recommended setting: Hard Stop
Compromised	98	Extreme	Indicators confirmed to host malicious content due to compromise or abuse – the exact time and length of compromise is unknown unless disclosed within the report Recommended setting: Hard Stop

Threat Type	Score	SA IdP Risk Category	Definition
Related	88	Extreme	Indicators likely related to an attack, but potentially only partially confirmed – detailed by one or more methods, like passive DNS, geo-location, and connectivity detection Recommended setting: Hard Stop
Victim	89	High	Indicators representing an entity that has been confirmed to have been victimized by malicious activity, where actors have attempted or succeeded compromise Recommended setting: Step-up
Uncategorized	80	High	Uncategorized threat Recommended setting: Step-up
No Threat Found	0	Low	Not found in threat aggregation platform Recommended setting: Resume Auth

Select the appropriate action to take when an end-user falls into a specific risk threshold from the following failure actions:

Field(s)	Description and Recommendations
Extreme Risk	+ Disable: No action. This is not an acceptable option for this risk level. + Hard Stop: Workflow is stopped immediately. One of the best options for this risk level. + Redirect: A text field appears to the right. Enter a URL to which the action is directed (e.g. another SecureAuth IdP realm). Another acceptable option for this risk level, particularly if the realm leads to hard vetting and a device detection mechanism. This can be set up as a 'honey pot' for any end-users deemed suspicious. + Step up auth: Additional authentication is required. For this risk level, this may be acceptable but only if authentication is rigorous. + Step down auth: End-user is taken to the next workflow step, bypass- ing additional analysis and any 2FA steps. Never an acceptable option. + Resume auth: The next step in adaptive authentication is performed, or, if all adaptive authentication steps are complete, the end-user is taken through any additional configured workflow steps. + Post auth: End-user is taken to the post-authentication target (such as IdM page or application.), bypassing additional analysis and config- ured workflow steps. Never acceptable for this risk level.

Field(s)	Description and Recommendations
High Risk	+ Disable: No action. This is not an acceptable option for this risk level. + Hard Stop: Workflow is stopped immediately. One of the best options for this risk level. + Redirect: A text field appears to the right. Enter a URL to which the action is directed (e.g. another SecureAuth IdP realm). Perhaps the best acceptable option for this risk level, particularly if the realm leads to hard vetting and a device detection mechanism. This can be set up as a 'honey pot' for any end-users deemed suspicious. + Step up auth: Additional authentication is required. For this risk level, this is acceptable; MFA is highly recommended. + Step down auth: End-user is taken to the next workflow step, bypass- ing additional analysis and any 2FA steps. Given this risk level, this is rarely an acceptable option. + Resume auth: The next step in adaptive authentication is performed, or, if all adaptive authentication steps are complete, the end-user is taken through any additional configured workflow steps. + Post auth: End-user is taken to the post-authentication target (IdM page, application, etc.), bypassing additional analysis and configured workflow steps. Never acceptable for this risk level.
Low Risk	+ Disable: No action. This can be an acceptable option for this risk level. + Hard Stop: Workflow is stopped immediately. Rarely required for this risk level. + Redirect: A text field appears to the right. Enter a URL to which the action is directed (e.g. another SecureAuth IdP realm). Almost never required for this risk level. + Step up auth: Additional authentication is required. To eliminate any possibility of attack, use this option. + Step down auth: End-user is taken to the next workflow step, bypass- ing additional analysis and any 2FA steps. Given this risk level, this can be an acceptable option, though use with caution. + Resume auth: The next step in adaptive authentication is performed, or, if all adaptive authentication steps are complete, the end-user is taken through any additional configured workflow steps. + Post auth: End-user is taken to the post-authentication target (IdM page, application, etc.), bypassing additional analysis and configured workflow steps. Given the risk level, this is an acceptable option.

Field(s)	Description and Recommendations
High Risk	+ Disable: No action. This is not an acceptable option for this risk level. + Hard Stop: Workflow is stopped immediately. One of the best options for this risk level. + Redirect: A text field appears to the right. Enter a URL to which the action is directed (e.g. another SecureAuth IdP realm). Perhaps the best acceptable option for this risk level, particularly if the realm leads to hard vetting and a device detection mechanism. This can be set up as a 'honey pot' for any end-users deemed suspicious. + Step up auth: Additional authentication is required. For this risk level, this is acceptable; MFA is highly recommended. + Step down auth: End-user is taken to the next workflow step, bypass- ing additional analysis and any 2FA steps. Given this risk level, this is rarely an acceptable option. + Resume auth: The next step in adaptive authentication is performed, or, if all adaptive authentication steps are complete, the end-user is taken through any additional configured workflow steps. + Post auth: End-user is taken to the post-authentication target (IdM page, application, etc.), bypassing additional analysis and configured workflow steps. Never acceptable for this risk level.
Low Risk	+ Disable: No action. This can be an acceptable option for this risk level. + Hard Stop: Workflow is stopped immediately. Rarely required for this risk level. + Redirect: A text field appears to the right. Enter a URL to which the action is directed (e.g. another SecureAuth IdP realm). Almost never required for this risk level. + Step up auth: Additional authentication is required. To eliminate any possibility of attack, use this option. + Step down auth: End-user is taken to the next workflow step, bypass- ing additional analysis and any 2FA steps. Given this risk level, this can be an acceptable option, though use with caution. + Resume auth: The next step in adaptive authentication is performed, or, if all adaptive authentication steps are complete, the end-user is taken through any additional configured workflow steps. + Post auth: End-user is taken to the post-authentication target (IdM page, application, etc.), bypassing additional analysis and configured workflow steps. Given the risk level, this is an acceptable option.

Field(s)	Description and Recommendations
IP Whitelist	Enter the IP addresses (comma-separated) that are automatically allowed. IP addresses in a field can be entered in any of the following formats, separated by comma: Specific IP address: e.g. 72.32.245.182 CIDR Notation: e.g. 72.32.245.0/24 IP range: e.g. 72.32.245.1-72.32.245.254 Different formats can be used in the same field. For example, the following example entry is valid: 72.32.245.182,72.32.245.0/24,72.32.245.1-72.32.245.254 Highly recommended to eliminate unnecessary investigation of qualified devices.
Require user to enter username before adaptive authentication occurs	Check this box if end users are required to provide a username before conducting the IP Reputation/Threat Data analysis.

Identity Governance

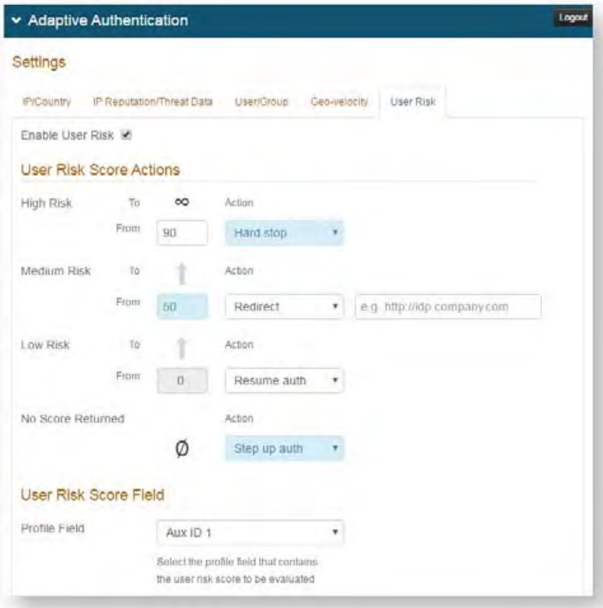
Identity Governance ensures that the correct people have the correct access to the correct applications and data.

According to the 2016 Verizon Data Breach Report, privilege misuse accounted for over fifteen percent of all incidents, second only to “miscellaneous errors.” When it came to full-scale breaches, privilege misuse accounted for the cause of almost ten percent. And according to Forrester Research’s Q3 2016 Wave report on Privileged Access Management, 80% of security breaches involved privileged credentials. SecureAuth can limit that through 2FA alone, but we provide nearly unlimited choices for how to accomplish that. So, if we only stop all attacks that involve a misuse of privileged accounts, the probability of a breach is 85%.

In SecureAuth IdP this is performed through integration with SailPoint. When a new user or device requests entry, IdP makes a call to SailPoint for an assessment of the risk involved; SailPoint returns a report on the available risk. Based upon that score, entry is either granted or denied.

SailPoint analyzes user risk based on the level of access a user has, and can detect when a user's access controls may be violating policy or configured improperly to provide excessive access. SailPoint then quantifies this information into a user reputation risk score. For example, an HR manager's user account would naturally be assigned a high user risk score since that account has access to confidential data and systems, while an intern's user account with limited network access would have a low user risk score. However, if the intern's user account was inadvertently given access to the HR database, the software would assign a high user risk score, alerting information managers to a potential misconfiguration and security risk.

To specify what constitutes each risk level, you must set the parameters in the User Risk tab page.



Enable User Risk ☑

User Risk Score Actions

High Risk To ∞ Action
From 90 Hard stop

Medium Risk To ↑ Action
From 50 Redirect e.g. http://idp.company.com

Low Risk To ↑ Action
From 0 Resume auth

No Score Returned Action
Ø Step up auth

User Risk Score Field

Profile Field Aux ID 1
Select the profile field that contains the user risk score to be evaluated

Figure 6. User Risk Tab Page

Threat analysis is mediated by database and analytics from FireEye, Neustar, and other sources.

For more on this topic, refer to IP reputation and threat assessment.

For more on deploying SailPoint, refer to https://docs.secureauth.com/display/90docs/Connecting+Sailpoint+to+SecureAuth+IdP.

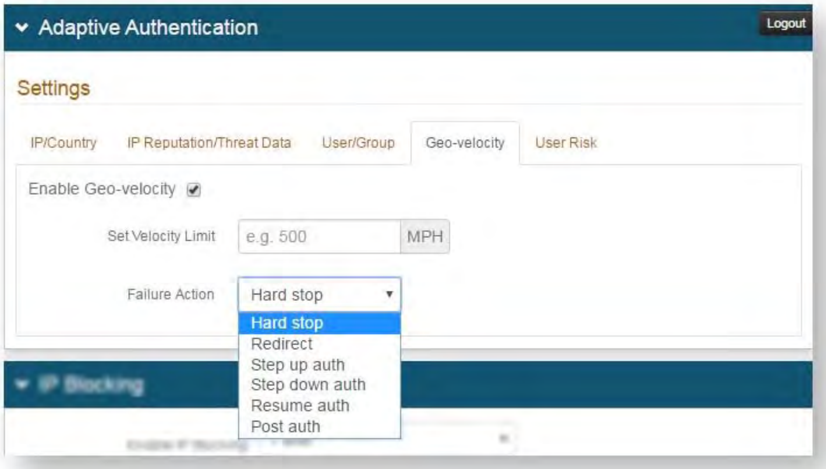
Geographic Restrictions

How many of your employees travel or telecommute? If you know where your employees should be, what is the percentage of attacks you can stop? We decrease or eliminate risk by checking for location, improbable travel events, and location blocking. 25% of breaches originate from an undesirable geographic location. 37% of people telecommute as an industry average.

Geo-Velocity

SecureAuth attempts to determine the user's current velocity. If that velocity deviates from the norm, an additional level of authentication is added.

To use this feature, open the Geo-velocity tab page of the Adaptive Authentication Settings section.



Enable Geo-velocity ☑

Set Velocity Limit e.g. 500 MPH

Failure Action Hard stop ▾

Figure 7. Geo-velocity Tab Page

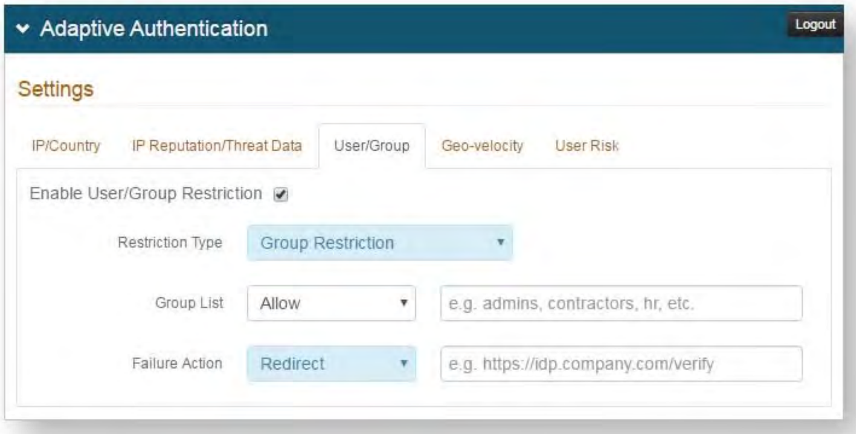
The fields on this page are explained below, with some recommendations for best use.

Field(s)	Meaning and Recommendations
Enable Geo-velocity	Check to enable this feature.
Set Velocity Limit	Enter the miles per hour an end-user is allowed to travel without activating the Failure Action. Recommended setting is 500.
Failure Action	From the drop-down list, select the action to be taken for end-users whose current location is not possible to reach based on the value set in the Set Velocity Limit, the last access time, and the previous location. These actions can include: + Hard Stop: Workflow is stopped immediately. Not recommended. + Redirect: A text field appears to the right. Enter a URL to which the action is directed (e.g. another SecureAuth IdP realm). Not recommended. + Step up auth: Additional authentication is required. Recom- mended. + Step down auth: End-user is taken to the next workflow step, bypassing additional analysis and any 2FA steps. Not recom- mended. + Resume auth: The next step in adaptive authentication is per- formed, or, if all adaptive authentication steps are complete, the end-user is taken through any additional configured workflow steps. Not recommended. + Post auth: End-user is taken to the post-authentication target (IdM page, application, etc.), bypassing additional analysis and configured workflow steps. Not recommended.

Directory Lookup

Directory lookup is used to make decisions on what flow the user gets – allow/deny, step down, step up, or redirect. It provides for flexible workflows. SecureAuth can perform an analysis of the data to determine this and respond with the appropriate remedy.

SecureAuth IdP configures for this method using the User/Group tab in the Adaptive Authentications Settings section.



Enable User/Group Restriction ☑

Restriction Type: Group Restriction

Group List: Allow | e.g. admins, contractors, hr, etc.

Failure Action: Redirect | e.g. https://idp.company.com/verify

Figure 8. User/Group Tab Page

The fields on this page determine how users and groups are included in adaptive authentication.

Field(s)	Meaning and Recommendations
Enable User/Group Restriction	Check to enable this feature.
Restriction Type	Select User Restriction option to restrict access by end-users or select Group Restriction to restrict access by user groups.
User/Group List	Select Allow to create a list of users or groups that can access the realm. Select Deny to create a list of users or groups that cannot access the realm.
User/Group text field	Enter a list of User/Groups that are allowed or denied access to the realm. Each user or group is separated by a comma.

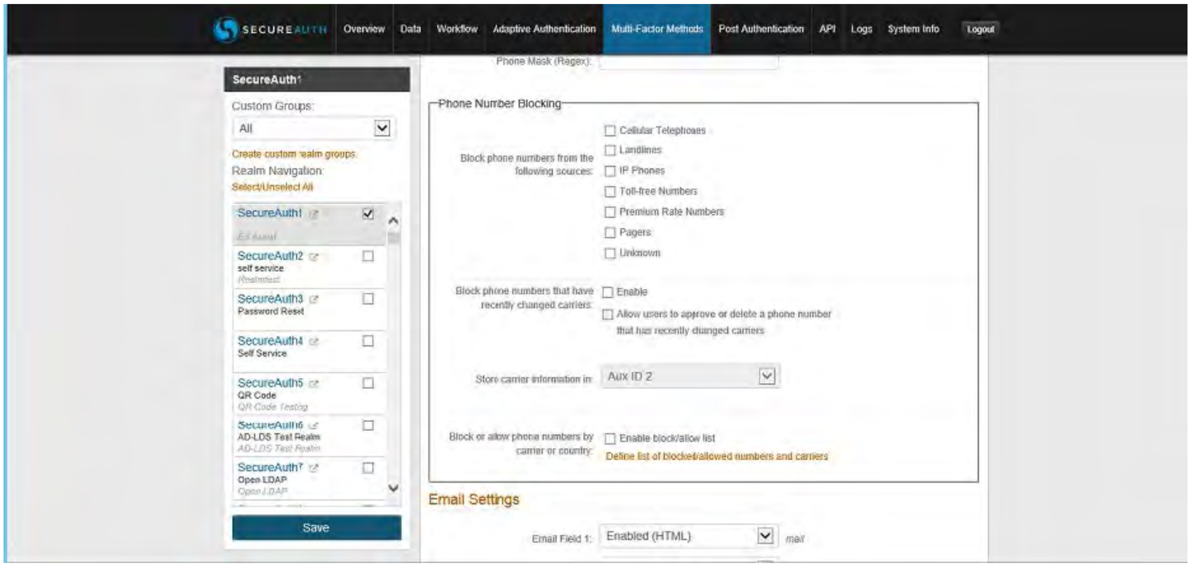
Field(s)	Meaning and Recommendations
Failure Action	From the drop-down list, select the action to be taken for end-users who are restricted from accessing the realm. These actions can include: + Hard Stop: Workflow is stopped immediately. Not normally an acceptable option for this risk. + Redirect: A text field appears to the right. Enter a URL to which the action is directed (e.g. another SecureAuth IdP realm). This can be set to redirect users from specific groups to a different realm. + Step up auth: Additional authentication is required. This can be useful when certain groups are always required to do second fac- tor. + Step down auth: End-user is taken to the next workflow step, bypassing additional analysis and any 2FA steps. This can be use- ful when certain groups should never be required to do second factor. + Resume auth: End-user is taken through any additional configured workflow steps (2-Factor Authentication), bypassing remaining analysis steps. If the user or group meets the criteria, the log-on process progresses to the next step in the adaptive authentication engine. + Post auth: End-user is taken to the post-authentication target (IdM page, application, etc.), bypassing additional analysis and configured workflow steps. This can be useful when certain groups should never be required to do second factor.

Phone Number Fraud Prevention

These risk checks enables the system to block an end-user trying to log in whose phone number is suspicious. Factors that can be considered in determining whether a phone number is fraudulent are:

- Restricted or bogus carrier
- Type of phone or phone method that is restricted (e.g. VoIP phone)
- Past porting status (recent carrier change)

SecureAuth IdP handles this prevention tactic through Phone Number Blocking located in the Phone Settings section of the Multi-Factor Methods tab page shown in Figure 9, “Phone Number Blocking,” on page 22.



Custom Groups: All

Realm Navigation:

Phone Mask (Regex):

Phone Number Blocking

Block phone numbers from the following sources: □ Cellular Telephones □ Landlines □ IP Phones □ Toll-free Numbers □ Premium Rate Numbers □ Pagers □ Unknown

Block phone numbers that have recently changed carriers: □ Enable □ Allow users to approve or delete a phone number that has recently changed carriers

Store carrier information in: Aux ID 2

Block or allow phone numbers by carrier or country: □ Enable block/allow list

Email Settings

Email Field 1: Enabled (HTML)

Figure 9. Phone Number Blocking

The restrictions available for this method include the following fields.

Field(s)	Meaning and Recommendations
Block phone number from the following sources	Check the box of each type you want blocked: + Cellular Phones: any access requested from a cell phone + Landlines: any access requested from a landline + IP Phones: virtual phone numbers, also known as DID or access numbers, without a directly associated phone line, such as Skype – such a source can be easily spoofed or anonymized + Toll-free Numbers: phone numbers with the following area codes: 800, 888, 877, 866, 855 or 844 – frequently and deservedly restricted + Premium Rate Numbers: phone numbers or phone calls in which certain services are provided and part of the charges are paid to the service provider – almost always restricted + Pagers: phone numbers of call devices that can only receive mes- sages – normally a good source of bad actors + Unknown: phone number of an anonymous classification – almost always restricted

Field(s)	Meaning and Recommendations
Block phone numbers that have recently changed carriers	Check Enable to prevent newly ported phone numbers from receiving Voice OTPs or SMS / Text OTPs. Check Allow users to approve or delete a phone number that has recently changed carriers to enable end-users to accept or remove a newly ported phone number from the multi-factor methods page during authentication.
Store carrier information in	From the drop-down list, select an option in which to store the carrier information – such as Aux ID 2. Select the option mapped to the appropriate data store previously defined in the Data Profile fields. If using the Authentication API, this is the call that stores the original Carrier information
Block or allow phone numbers by carrier or country	Select Enable block / allow list to deny or permit Voice OTPs or SMS/ Text OTPs to be received by phone numbers from carriers/countries specified on the activated blacklist/ whitelist. Click the Define list of blocked / allowed numbers and carriers link to configure the blacklist/ whitelist.
Block or Allow Countries/ Carriers	Indicate whether to Block or Allow numbers of specified countries or carriers. Based on the radio button selection, the heading toggles between Blocked Countries/ Carriers and Allowed Countries/Carriers – only one of these two options can be applied Click Add country/carrier to add to the available list of country/ carrier that is either blocked or allowed.

For more information on configuring phone blocking, refer to https://docs.secureauth.com/ display/90docs/ Phone+Number+Profiling+Service+Configuration+Guide.

User & Entity Behavior Analytics (UEBA)

This adaptive authentication risk check concentrates on the detection of any sort of malicious behavior that might arise from any devices, applications, servers, data, or anything with an IP address. UEBA solutions look at patterns of human behavior by using special algorithms to detect insider threats.

UEBA assesses the behaviors of organizations' insiders (employees), outsiders connected to their networks (such as third-party contractors), and flags security vulnerabilities across organizations' assets that hold sensitive data. In addition to analyzing user behavior, UEBA also vets an organization's entities – meaning endpoints (such as laptop computers) and applications – and identifies any unusual behavior coming from those entities. Finally, UEBA connects the dots – combining the data collected from users and entities to uncover security risks that criminals may exploit.

To provide this risk check, SecureAuth teams with Exabeam, one of the leaders in the UEBA field.

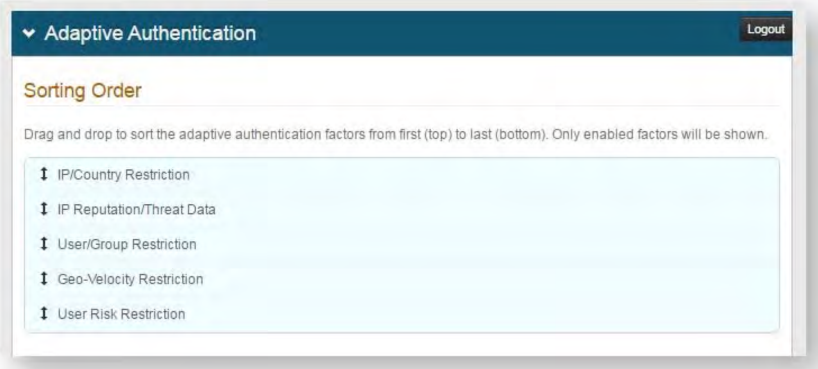
When integrated with IdP, Exabeam provides analytical assessments to IdP on a received risk, culminating in a risk score that help IdP determine the type of response to that risk. This response is configured through the User Risk section on the Adaptive Authentication page. For more on judging and configuring risk, refer to "Threat Services" starting on page 10.

For detailed information on deploying and configuring SecureAuth IdP with Exabeam, refer to https://docs.secureauth.com/display/90docs/Connecting+Exabeam+to+SecureAuth+IdP.

Sorting Order

SecureAuth IdP enables you to specify the order in which each risk check is used in the adaptive authentication process. Sorting Order organizes the Adaptive Authentication risk checks to create a completely customized workflow.

Each enabled method appears in the Sorting Order table. The Sorting Order table appears on the Adaptive Authentication tab page as shown in the example in Figure 10.



Sorting Order

Drag and drop to sort the adaptive authentication factors from first (top) to last (bottom). Only enabled factors will be shown.

- IP/Country Restriction
- IP Reputation/Threat Data
- User/Group Restriction
- Geo-Velocity Restriction
- User Risk Restriction

Figure 10. Sorting Order Section

A qualified administrator can then drag and drop these risk checks to reorder the sequence in which they are processed.

Since each adaptive authentication risk check will initiate a distinct workflow (some of which are time-consuming), try to sort these risk checks in a way that will minimize the workflow for most users requesting entry. After all, the majority of users to your site do not need to be detoured and asked to wait while the authentication process churns through options

The following table provides a description of each risk check and recommendations for sorting.

Field(s)	Meaning and Recommendations
IP/Country Restriction	IP and country restrictions are explained in “Geographic Restrictions” starting on page 18. These geographic methods are particularly useful for restricting users to approved countries and IPs. If your website
IP Reputation/Threat Data	This method is outlined in “Threat Services” starting on page 12. Threat assessment can be placed first or second on any sort list, since it is frequently the most determinative.
User/Group Restriction	This method is explained in “Directory Lookup” starting on page 20. Restricting by user or group is frequently placed in the middle of any sorting list.
Geo-Velocity Restricting	This method is explained in “Geo-Velocity” starting on page 19. A method that can be safely placed near the bottom of any sort list.
User Risk Restriction	This method is explained in “Identity Governance” starting on page 17 and “User & Entity Behavior Analytics (UEBA)” starting on page 23. Since this technique frequently requires time-consuming queries to databases provided by either SailPoint and/or Exabeam, this method should be placed near the end of any sort list

Use Cases

In this section we present use case scenarios for several institutions illustrating how each would benefit from adaptive authentication.

1. Healthcare insurance company using B2C, where
   - Customers check health records on public website
   - Self-registration is allowed
   - All customers are residents of the USA
2. Hospital with multiple campuses that physicians must travel between, where
   - All clinical and office staff remotely access EHR, financial, and other resources via NetScaler
   - Many apps are accessed via XenApp or XenDesktop
   - SSO is provided to a number of apps both internal and external
   - When in the office, the users are on a domain-joined machines accessing the same resources
3. State government tax dispersal entity where
   - Downloading of documents is allowed from public website is allowed
   - Customers can check the progress of their returns on a public website
   - Customers can register requests and contact a help desk
4. State university admissions department where
   - Applicants can download some forms from website
   - Applicants can submit forms and essays to website
   - Anyone using the site can consult or download the syllabus
   - Interviewers can upload their confidential reviews of applicants
   - Applicants can email a help desk
5. International bank with global branches

The adaptive authentication recommendations for each use case are shown in the table below.

Adaptive/Risk-Based Authentication	1	2	3	4	5
Device Recognition	✓	✓	✓	✓	✓
Threat Services (IP Threat)	✓	✓	✓	✓	✓
Identity Governance (SailPoint Score)		✓			✓
Geo-velocity		✓			✓
Geo-location (Country restriction)	✓	✓	✓		✓
Directory Lookup (User/Group restriction)		✓			✓
Phone Number Fraud Prevention	✓		✓	✓	
UEBA (Exabeam Score)		✓		✓	✓

The 2FA methods that might be implemented and acceptable for each use case are:

Second-Factor Method	1	2	3	4	5
x.509					✓
SMS OTP	✓	✓	✓	✓	
Telephony OTP	✓	✓	✓	✓	
Email OTP	✓		✓	✓	
Yubikey USB*		✓			✓
CAC/PIV					✓
Static PIN					✓
Help Desk	✓		✓	✓	
Integrated Windows Authentication / Kerberos		✓			✓
Mobile OATH token		✓			✓
Desktop OATH token					
Hard OATH token TOTPa		✓			✓
Push		✓	✓	✓	✓
KBA					
Symantec VIP					
Push2Accept		✓			✓
Google Authenticator	✓				
RSA SecureID / Other Hard Token*					✓

*: Hard tokens are not recommended because of administrative burden and user acceptance, but are often required for transitions or for limited high-security use cases.

SECUREAUTH