# PingOne Risk - Getting started

[**PingOne Risk - Getting started 1**](#_82lztyu17yyu)

[**The basics of PingOne Risk 3**](#_5rvrwma9vrl)

[**How PingOne Risk works 4**](#_lbm3ynw5m2d1)

[**Get started with PingOne Risk 5**](#_ivshrdjkd0px)

[**Try PingOne Risk with a sample app 5**](#_sabqk9qmh76t)

[**Getting up and running 7**](#_nhebc1o0n93)

[Getting started overview 7](#_xixqrasm8oni)

[Adding the PingOne Risk service to your environment 7](#_ee376k7pe5e7)

[Integrating PingOne Risk with authentication 8](#_vqpchxvcpkn2)

[Using the PingOne Risk Integration Kit with PingFederate 9](#_lrt3inwsm96i)

[Building a custom flow with PingOne DaVinci 9](#_rqlhjnsefilb)

[Using the PingOne API 11](#_k7r0849fia2d)

[Getting input from the PingOne Risk SDK 12](#_dvyv88f8evfm)

[Adding the required Risk SDK code to your applications 12](#_emmb05k2j8v7)

[Including the information from the Risk SDK in your flows 12](#_78ve69czehhx)

[**Running, analyzing, and adjusting your risk policy 13**](#_y8c7rpl2jgh1)

[**The default risk policy 14**](#_vbdlfriiqrvz)

[**Risk dashboard 14**](#_xlykjhbt971p)

[**Risk predictor types 14**](#_t79t3wn9va9j)

[User and entity behavior analytics 15](#_y7xa6vawi64)

[User risk behavior (organization-wide) 15](#_fo8ada2vjyh4)

[User-based risk behavior (individual user) 16](#_lx9lym9awn25)

[Velocity 16](#_4t2oandg8hm8)

[User velocity 16](#_8xoszrj8kt0p)

[IP velocity 17](#_et9uuxdsrkbn)

[Anonymous network detection 17](#_lxcurvspx7i8)

[IP reputation 17](#_5uqfpv6fuqih)

[Geovelocity anomaly 18](#_tik53es1rvbb)

[User location anomaly 18](#_s8crsyhfnpwz)

[New device 18](#_yjq0hemro4fs)

[**Testing risk predictors 19**](#_au3renqmsvp7)

[**Advanced - customizing risk policies 20**](#_9euiaw1f3sc8)

[**Advanced - staging policies 20**](#_jby0arjj4f7n)

[Tutorial: Evaluating staging policy risk data 20](#_n5bmhjgws2o8)

[**Advanced - customizing risk predictors 22**](#_vrgzvd958ber)

[Fine-tune out-of-the-box predictors 23](#_z2tol41cug7z)

[Create a composite predictor 24](#_yi9wzsd1g64m)

[Create a custom predictor 25](#_ygzdjc9ly0h0)

[**Advanced - using the PingOne API for risk evaluations 25**](#_4cjcexsi1bh8)

[**Troubleshooting 26**](#_3097hdd69um6)

[**Error codes 26**](#_rl8wl3wtfake)

[PingOne Risk/Protect start up guide skeleton 27](#_ptor4d4l37tj)

# 

# 

# The basics of PingOne Risk

PingOne Risk analyzes a variety of security risk factors in order to achieve two goals simultaneously:

* Prevent the “bad guys” from accessing your systems.
* Make it easier for your employees and customers to access the items they require.  
    
  The requirement of a second factor during authentication has resulted in “MFA fatigue” as people find themselves entering one-time passcodes or receiving push notifications many times throughout their day. PingOne Risk eliminates this frustration by recognizing legitimate users and lowering the friction they encounter.

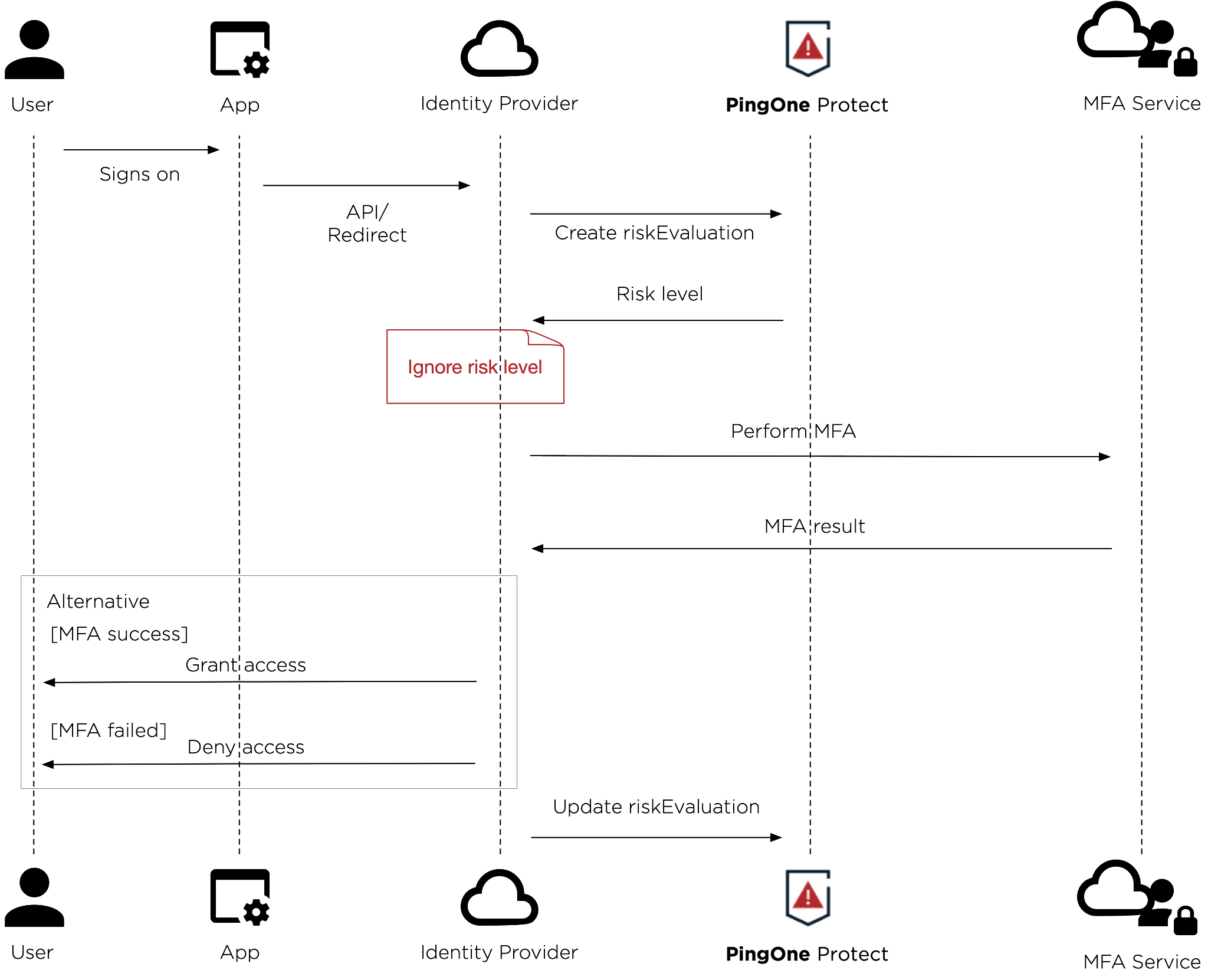
The two basic elements used in the risk analysis process are “risk predictors” and “risk policies”:

* A risk predictor looks at a single factor, for example, whether or not a user is trying to authenticate from an anonymous network. Each predictor yields an estimated risk level. For some predictors, the levels are Low and High. For other predictors, the levels are Low, Medium, and High.
* A risk policy combines a number of individual risk predictors. The policy looks at the risk level estimated for each of the predictors and then yields an overall risk level of Low, Medium, or High. When you define an authentication flow with one of the tools provided by Ping Identity, you decide which of your defined risk policies you would like to associate with that flow. For some situations, you may want to use a stricter risk policy, while for others, you may decide to use a more lenient risk policy.

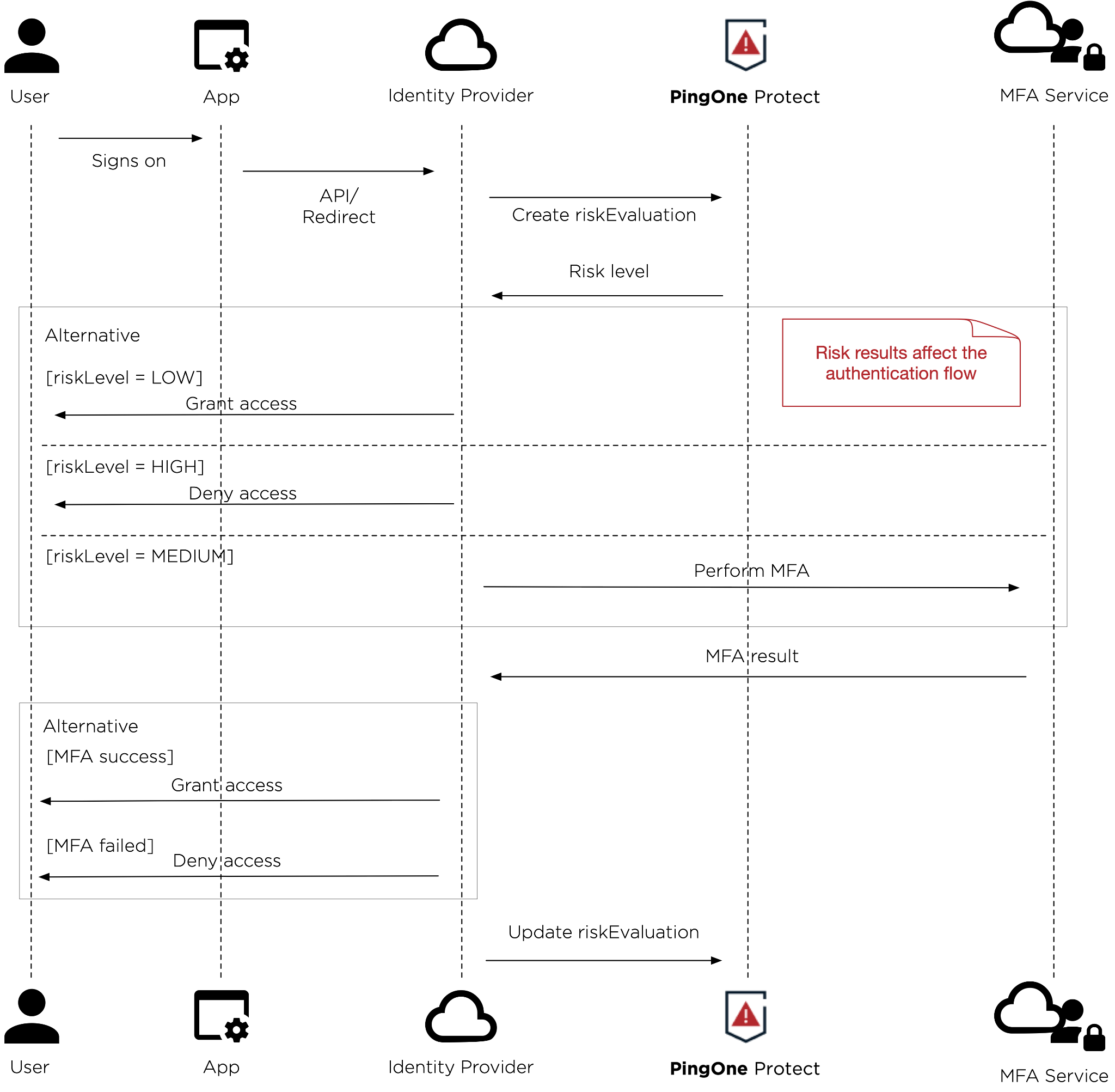
# 

# How PingOne Risk works

The following diagram shows a high-level overview of how PingOne Risk works. The diagram shows PingOne Risk integrated in silent mode into an example authentication flow.



The diagram below shows PingOne Risk integrated into an authentication flow with risk levels affecting the flow.



# Get started with PingOne Risk

To get started and familiarize yourself with PingOne Risk, you have two options:

* To try PingOne Risk with trial and sample application, see [Try PingOne Risk with a sample app](#_sabqk9qmh76t).
* To try PingOne Risk in your existing PingOne authentication flow, see [Getting up and running](#_nhebc1o0n93).

# Try PingOne Risk with a sample app

Signing up for a PingOne trial is a great way to experience the functionality of PingOne Risk with an automatically generated sample application. This sample app is a Ping-maintained application that allows you to design registration and sign-on experiences for your customers and test them in the app.

With your PingOne trial, you can try PingOne Risk, and quickly and easily simulate risk events with the sample app to test how risk predictors work. The sample app allows you to test the capabilities of PingOne Risk in addition to other PingOne services, such as PingOne MFA and PingOne SSO, and can be tailored to your industry.

**Note:** To try PingOne Risk in your existing PingOne authentication flow instead of with a trial, see [Getting up and running](#_nhebc1o0n93).

**Before you begin:** Sign up for a PingOne trial. For more information, see [Starting a PingOne trial](https://docs.pingidentity.com/r/en-us/pingone/p1_start_a_pingone_trial?tocId=dTAKOHd57wlzNWVfCX6Myw).

To try PingOne Risk with a sample app:

1. In your PingOne account, click **Add Environment**.
2. Choose **Customer solution**, and click **Next**.

**Note:** When you choose to create a **Customer solution**, your new environment automatically includes the PingOne Risk service.

1. Click **Next** again to create the environment.
2. Enter the details for your environment, select the checkbox for ​​**Include a solution designer to easily design and test experiences**, and click **Finish**.

**Result:** Your new PingOne environment is created and automatically opens.

1. Choose if you want to tailor your experience for your industry, or click **Skip**.

**Result:** PingOne creates a sample app based on your selection. You can click **Get Started** to view the tour or close the tour pop-up window.

1. [Test the risk predictors](#_au3renqmsvp7).

**Note:** The PingOne Risk capabilities are available in the **Authentication** flow of the sample app.

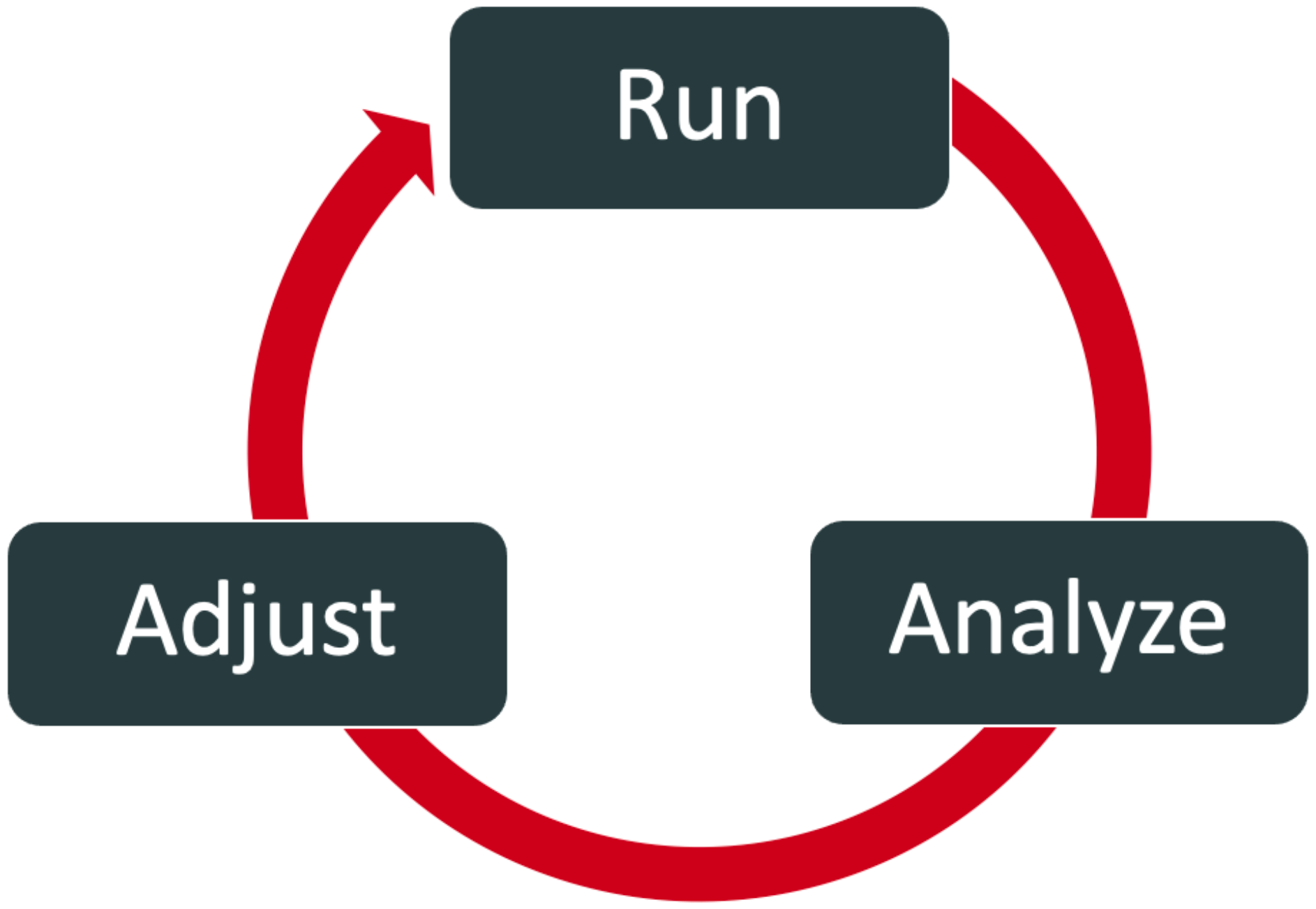
# Getting up and running

While PingOne Risk provides many ways to customize risk predictors and to combine predictors in a risk policy, it also provides out-of-the-box risk predictors, and a default risk policy that combines these predictors. When you first start with PingOne Risk, the best approach is to use the default risk policy that is provided. Once you’ve seen how this default policy affects the authentication experience for your users, you can go back and fine-tune it by customizing individual predictors or creating multiple risk policies.

Because you’ll use the default risk policy, the “heavy lifting” at the beginning is just the integration of PingOne Risk with your authentication process.

## Getting started overview

The main steps required to start using PingOne Risk are:

1. [Integrate PingOne Risk into an authentication flow](#_vqpchxvcpkn2).
2. [Configure the PingOne Risk (Signals) SDK](#_dvyv88f8evfm).
3. [Run and analyze your risk predictors](#_y8c7rpl2jgh1):
   1. Run PingOne Risk to train the risk predictor models.
   2. Use the Risk dashboard to analyze the results.
   3. Adjust the scores for the risk predictors in the risk policy.
4. Repeat step 3 as needed.

## Adding the PingOne Risk service to your environment

To get started, add the PingOne Risk service to your PingOne environment.

**Before you begin**

* If you don’t have a PingOne account yet, [start a PingOne trial](https://docs.pingidentity.com/r/0ue6NPmZLPN667l6iXUjRg/dTAKOHd57wlzNWVfCX6Myw).
* Make sure you can [sign on to the PingOne admin console](https://docs.pingidentity.com/r/0ue6NPmZLPN667l6iXUjRg/UOWvaYidxf5N2H9ToOhcSQ).
* [Add an environment](https://docs.pingidentity.com/r/0ue6NPmZLPN667l6iXUjRg/1_cCChOyWO~Bu3kmBe3w0g) to organize your services.
* Make sure you have the Environment Admin and Identity Data Admin roles in your PingOne environment. For more information, see [Assigning a user role](https://docs.pingidentity.com/r/0ue6NPmZLPN667l6iXUjRg/ksbju5W7WU9hTmQSw_dAQw).

To add PingOne Risk to your environment:

1. In your PingOne environment, go to **Overview**.
2. Next to **Services**, click the **+** icon.
3. Click **+ Add** to add the **PingOne Risk** service.
4. In the **Add a Service** window, click **Finish**.

**Result:** PingOne Risk is displayed in the left navigation pane.

## Integrating PingOne Risk with authentication

After you add PingOne Risk to your environment, integrate PingOne Risk into an authentication flow.

There are three ways to integrate your risk policy into an authentication flow:

* Using the PingOne Risk Integration Kit to integrate with PingFederate single sign-on (SSO)
* Building a custom authentication flow with PingOne DaVinci
* Using the PingOne API to associate a risk policy with an authentication flow

Below are the steps you must carry out for each of these approaches to integration.

**Before you begin**

You’ll need a PingOne account with at least one environment that includes the PingOne Risk service. For information, see [Creating an organization and environment in PingOne](https://docs.pingidentity.com/bundle/pingfederate-pingone-risk-ik/page/wkg1605199603294.html).

Regardless of the approach you use, the high-level steps are the same:

1. Integrate into an authentication flow.
2. Add risk evaluation to your authentication flow.
3. Send transaction feedback.
4. Configure a risk policy.

The simplest approach is to start off by using the default risk policy. You can also edit the default risk policy.

### Using the PingOne Risk Integration Kit with PingFederate

**Before you begin**

Before proceeding, make sure that PingFederate has been installed. For instructions on installing PingFederate, see [Installing PingFederate](https://docs.pingidentity.com/csh?Product=pf-latest&context=pf_installing_pf).

**Note:** The PingOne Protect Integration Kit 1.0 works with PingFederate 11.3 and above. The PingOne Risk Integration Kit will continue to support PingFederate versions 10.2 and above.

To get started with the PingOne Risk Integration Kit:

1. [Deploy the integration files](https://docs.pingidentity.com/bundle/pingfederate-pingone-risk-ik/page/lqi1608069506793.html).
2. [Create a connection between PingOne and PingFederate](https://docs.pingidentity.com/access/sources/dita/topic?category=Integration&resourceid=connecting_pingfederate_to_pingone).
3. Optionally, [integrate device profiling](https://docs.pingidentity.com/csh?context=pingfederate_pingone_risk_ik_integrating_device_profiling).
4. [Configure an adapter instance](https://docs.pingidentity.com/csh?context=pingfederate_pingone_risk_ik_configuring_an_adapter_instance).
5. [Add risk evaluation to your authentication flow](https://docs.pingidentity.com/csh?context=pingfederate_pingone_risk_ik_adding_risk_level_results_to_your_authentication_policy).  
   The response returns a final risk evaluation result: High, Medium, or Low.  
   Risk evaluation feedback is a crucial part of a flow that uses risk evaluation. This step is included after authentication has been completed, and it consists of sending an update with the final state of the transaction, such as success or failed. This step is essential for improving the accuracy of the machine learning models. When you use PingOne Risk in conjunction with PingFederate, risk evaluation feedback is included automatically.
6. [Configure PingFederate to forward IP addresses.](https://docs.pingidentity.com/csh?context=pingfederate_pingone_risk_ik_configuring_pingfederate_to_forward_ip_addresses)

### Building a custom flow with PingOne DaVinci

PingOne Davinci is the graphic orchestration tool used for designing flows such as user authentication flows. You can find general information on using PingOne Davinci [here](https://docs.pingidentity.com/r/en-us/davinci/davinci_landing_page).

You can use the PingOne Risk connector to define different paths in an authentication flow, based on the result of a risk evaluation.

For example, you can use a risk evaluation connector before an MFA step, and then define different paths based on the risk score calculated: skip the MFA challenge if low risk, use a specific authentication method if user behavior data suggests medium risk, and block access completely in a high risk situation, such as the detection of impossible user travel.

For examples of use of the PingOne Risk connector in different types of flows, see the following templates in the [Flow Library](https://docs.pingidentity.com/access/sources/dita/topic?resourceid=davinci_importing_a_flow_from_the_flow_library):

* PingOne - Sign On and Adaptive MFA
* PingID - MFA flow + Risk
* PingID - FIDO2 Passwordless + Risk

**Before you begin**

Add PingOne DaVinci to your PingOne environment. For more information, see [Creating an environment](https://docs.pingidentity.com/r/en-us/pingone/pingone_tutorial_passwordless_create_environment?tocId=obPrwmBIefGVsmFhwvoJrQ).

To use risk connectors in a flow:

1. After you have added DaVinci to your PingOne environment, any risk connectors you add to your flows already have been configured with the correct information for environment ID, client ID, and client secret. However, if you import a flow from a different PingOne environment, you must go to the settings for the risk connector and update this information to reflect the environment where you are adding the flow.
2. Add two different risk connectors to your flow by following the documentation for the [PingOne Risk Connector](https://docs.pingidentity.com/bundle/davinci-pingone-risk-connector/page/enk1642800997036.html).
   1. Add a risk connector with the **Create risk evaluation** capability.  
      The response returns a final risk evaluation result - High, Medium, or Low.  
      The risk connector with the Create Risk Evaluation capability should be added at a point in the flow where you would like to base the next action on the risk score assigned, for example, show an MFA prompt for Medium or High, but automatically grant access if the risk is deemed Low.
   2. Add risk evaluation feedback to the flow by adding a risk connector with the Update risk evaluation capability. This step is included after authentication has been completed, and it consists of sending an update with the final state of the transaction, such as SUCCESS or FAIL. The **Update risk evaluation** capability represents the system's ability to learn over time in order to improve results. You should always include an update connector in your flow because this step is essential for improving the accuracy of the machine learning models.

**Note:** Flows may take users on different paths. Make sure to include a risk connector with the **Update risk evaluation** capability at the end of each possible path.

If you are having issues with the PingOne Risk Connector, try the following:

* For each connector in the flow, make sure that all of the mandatory inputs have been provided.
* If you are using the *skrisk* component to include the data provided by the PingOne Risk SDK, make sure that you have carried out all of the necessary steps.
* Use the [Analytics feature](https://docs.pingidentity.com/r/en-us/davinci/davinci_best_practices_debugging_and_analytics) to see where the flow stopped.
* Select the Options icon, and turn on **Show Node ID**. This will make it easier to identify the source of inputs and outputs.

### Using the PingOne API

To integrate using the PingOne API:

1. Create a worker application and get an access token, as described in [Creating a worker application and getting an access token](https://docs.pingidentity.com/r/0ue6NPmZLPN667l6iXUjRg/yY8o650avhIGVkJMXNVWdw)
2. Add risk evaluation to your authentication flow. See the [section on risk evaluation](https://apidocs.pingidentity.com/pingone/platform/v1/api/#risk-evaluations) in the API reference.  
   The response returns a final risk evaluation result - High, Medium, or Low.
3. Add risk evaluation feedback to the flow. This step is included after authentication has been completed, and it consists of sending an update with the final state of the transaction, such as success or failed. This step is essential for improving the accuracy of the machine learning models. See [PUT UPDATE Risk Evaluation](https://apidocs.pingidentity.com/pingone/platform/v1/api/#put-update-risk-evaluation) in the API reference.
4. If you want to modify the default risk policy or create one of your own, see the documentation for [creating a risk policy set](https://apidocs.pingidentity.com/pingone/platform/v1/api/#post-create-risk-policy-set-scores) with the API.

# 

## Getting input from the PingOne Risk SDK

Certain risk predictors, such as the New Device predictor, rely on supplemental risk-related information that is supplied by the PingOne Risk (Signals) SDK.

The default risk policy that is provided includes predictors that are dependent upon this input So to get reliable risk evaluations right from the start, you’ll have to carry out the steps to include the required code in your applications and to include the information from the Risk SDK in your authentication flows.

### Adding the required Risk SDK code to your applications

You can integrate the Risk SDK into your web applications, Android applications, and iOS applications. For the necessary details, see:

* [PingOne Risk SDK for Web](https://apidocs.pingidentity.com/pingone/native-sdks/v1/api/#pingone-risk-sdk-for-web)
* [PingOne Risk SDK for Android](https://apidocs.pingidentity.com/pingone/native-sdks/v1/api/#pingone-risk-sdk-for-android)
* [PingOne Risk SDK for iOS](https://apidocs.pingidentity.com/pingone/native-sdks/v1/api/#pingone-risk-sdk-for-ios)

### Including the information from the Risk SDK in your flows

The information from the Risk SDK can be included through the PingOne Risk Integration Kit for PingFederate, through code that uses the PingOne Risk API, or as part of a flow designed with PingOne DaVinci.

For details on these three different methods, see:

* [Integrating device profiling](https://docs.pingidentity.com/csh?context=pingfederate_pingone_risk_ik_integrating_device_profiling) (PingFederate)
* [Creating risk evaluations](https://apidocs.pingidentity.com/pingone/platform/v1/api/#post-create-risk-evaluation) (Risk API)
* [PingOne Risk Connector](https://docs.pingidentity.com/csh?context=davinci_pingone_risk_connector) (DaVinci)

# 

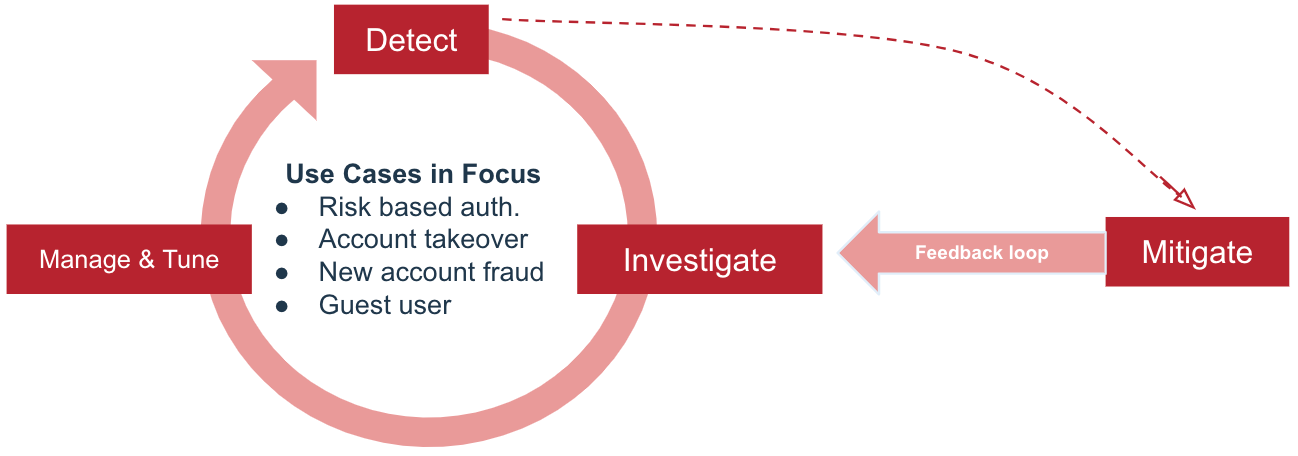
## Running, analyzing, and adjusting your risk policy

In order to make informed decisions about how to fine-tune risk predictors and policies, you’ll have to accumulate a certain amount of data on authentication attempts and how the risk evaluation impacts them.

It is recommended that you use the default risk policy for the initial period, before you start customizing the policy or defining multiple risk policies.

Fine-tuning your policy is an iterative process and should follow this approach:

1. Train the risk models with “production” data for 1-3 weeks for workforce usage or 2-4 weeks for CIAM usage. This should be done with the default policy.
2. Use the risk dashboards to analyze the results. Identify false positive results, meaning situations that are identified as High risk even though they are legitimate users. Check what is causing these false positives.
3. Adjust the scores for the different risk predictors in the risk policy to see if you can reduce the incidence of false positives.



# 

# The default risk policy

When you add the PingOne Risk service to a PingOne environment, it includes a default risk policy. This is the policy that we recommend for your initial testing of risk evaluations.

The default risk policy has the following characteristics:

* It uses the Scores approach, which gives you a higher degree of control than the Weights approach.
* It includes all of the out-of-the-box predictors, except User Risk Behavior (organization-wide behavior).
* It assigns a score of 50 for High risk for some of the predictors, and a score of 75 for High risk for the remaining predictors. This is based on the premise that the various IP-related predictors are less indicative of risky situations than the other predictors.

# Risk dashboard

To help you assess how risk evaluations are impacting user authentication, PingOne includes a Risk dashboard. This dashboard displays top-level information, and includes a number of charts that you can use to drill-down and get detailed information on specific aspects of the data. For example, the main dashboard shows a bar graph of how many risk evaluations yielded Low, Medium, and High risk. When you click the Risk Event chart, you can also view details for each of the events, for example, the country where the user was located and what IP was used.

Controls are provided to allow you to restrict the data displayed to a specific time frame.

# Risk predictor types

PingOne Risk leverages the following risk predictors to learn user behavior and detect anomalies:

* User and entity behavior analytics
  + User risk behavior (organization-wide)
  + User-based risk behavior (individual user)
* Velocity
  + User velocity
  + IP velocity
* Anonymous network detection
* IP reputation
* Geovelocity anomaly
* User location anomaly
* New device

The risk level for each predictor type is calculated separately. Most predictor types require training and learn from successful events. You can also configure a fallback value for most predictor types to use if there is insufficient information to calculate a risk level. Risk predictors are configured per PingOne environment, and you can have up to 15 of each predictor type per environment.

You can also create custom predictors that leverage external or processed data. See [Advanced - customizing risk predictors](#_vrgzvd958ber).

## User and entity behavior analytics

There are two types of user and entity behavior analytics predictors:

* User risk behavior (organization-wide)
* User-based risk behavior (individual user)

### User risk behavior (organization-wide)

To understand the behavior patterns of workforce users within an organization, PingOne Risk leverages user risk behavior and machine learning.

For example, if an organization’s workforce users primarily work on Mac operating system, but a user accesses an application on Windows operating system, the user risk behavior predictor detects an anomaly.

PingOne Risk continuously learns the behaviors of users inside an organization by analyzing many data points, including:

* Operating system
* Browser type and version
* Activity time frame
* IP range
* Geolocation (country)
* IP reputation
* Application being accessed

Using these data points, the machine-learning model characterizes abnormal activity as low, medium, or high risk and prompts the user for the appropriate authentication action. This organization-based risk predictor works at the PingOne environment level and only uses data from one PingOne environment.

You can configure a fallback value for this predictor type to use if there is insufficient information to calculate a risk level.

### User-based risk behavior (individual user)

Unlike the user risk behavior model, which compares a transaction with typical behavior within an organization, the user-based risk behavior model compares a transaction with the typical behavior of that specific user.

For example, if a user accesses an application that they rarely use but is frequently used within the organization, user-based risk behavior detects an anomaly, but user risk behavior doesn't.

User-based risk behavior is a machine-learning model that continuously updates and requires only one transaction for immediate training and learning. The model learns each user's behavior from various data points, including:

* Operating system
* Browser type and version
* Activity time frame
* Geolocation (country)
* Application being accessed
* Device settings and characteristics

The machine-learning model characterizes abnormal activity as Low, Medium, or High risk. Thresholds for this predictor are dynamic and may change between different users. You can configure a fallback value for this predictor type to use if there is insufficient information to calculate a risk level.

**Note:** The PingOne Risk SDK is required for the user-based risk behavior predictor type.

## Velocity

### User velocity

Stolen user accounts are becoming more common. A malicious user can have multiple sets of credentials originating from the same IP address. PingOne Risk detects the number of users originating from the same IP address and alerts on anomalies. For example, if a workforce organization has 50 users who typically work from the same IP address at their office location but 100 users attempt to authenticate from this IP address, the user velocity model alerts on this anomaly. Thresholds for this predictor are changed dynamically.

### IP velocity

Compromised accounts can be associated with many different IP addresses. PingOne Risk detects the number of IP addresses a user is leveraging and alerts on anomalies. This predictor learns user behavior and dynamically adjusts the thresholds for each user. For example, if a user attempts to access their account from 6 different IP addresses within a short time frame, the IP velocity model detects an anomaly.

## Anonymous network detection

Malicious actors typically use anonymous networks, such as unknown VPNs, Tor, and proxies, to mask their IP address. PingOne Risk analyzes IP address data from a user’s device to determine if the address is originating from any type of anonymous network and returns a High or Low risk score. If an anonymous network is detected, the user can be prompted for step-up authentication or denied access.

You can configure a fallback value for this predictor type to use if there is insufficient information to calculate a risk level. PingOne Risk also supports creating an allow list of networks, ensuring that legitimate VPN users can access authorized resources.

## IP reputation

IP addresses that have been involved in malicious activities, such as distributed denial-of-service (DDoS) attacks or spam activity, are considered risky. The more frequently an IP address is used for malicious activities, the higher its risk score. If a user attempts to access an application from an IP address previously involved with suspicious activity, the probability of potentially risky behavior increases. PingOne Risk analyzes data from different intelligence sources to determine the probability an IP address is associated with malicious activity and to request stronger authentication to verify the user’s identity.

You can configure a fallback value for this predictor type to use if there is insufficient information to calculate a risk level. You can customize an IP reputation predictor by creating an allow list of IP addresses for which the IP reputation score should be ignored.

## Geovelocity anomaly

Users frequently sign on to the same application from multiple locations throughout the day. However, a time lapse between two sign-on locations that is shorter than the time it would take to travel between the two points could indicate suspicious activity. PingOne Risk analyzes location data to calculate if travel time between two session locations is physically possible. If the elapsed time is calculated to be impossible, the user can be prompted with step-up authentication or denied access.

For example, if a user signs on to an application from the U.S. and then attempts to sign on again 2 hours later from Japan, the geovelocity anomaly predictor alerts on this anomaly.

You can configure a fallback value for this predictor type to use if there is insufficient information to calculate a risk level. You can customize a geovelocity anomaly predictor by creating an allow list of IP addresses for which these time and distance calculations should be ignored.

## User location anomaly

User location anomaly predictors allow you to define a radius around the location of the previous successful sign-on attempts. Sign-on attempts outside the defined radius result in a risk score of High. This information can be used in authentication policies to reduce the risk of unintentional push notification approval and account takeover (ATO) attacks.

You can configure a fallback value for this predictor type to use if there is insufficient information to calculate a risk level. You must also set a distance for the radius. The minimum radius distance is 10 miles (16 kilometers), and the maximum radius distance is 100 miles (160 kilometers).

## New device

New device predictors allow your risk policy to take into account the risk associated with users trying to access applications from unknown devices or devices that have not been used in the past 90 days.

You can configure a fallback value for this predictor type to use if there is insufficient information to calculate a risk level. You can also set an activation date for the model to restart the learning process.

This predictor requires that you include the input from the PingOne Risk SDK or provide a persistent cookie. It is recommended that you use the data from the SDK. If the SDK payload has been successfully sent to the risk evaluation, you will see a *deviceID* field in the response to the Create Risk Evaluation API request.

# Testing risk predictors

To test risk predictors, you can simulate risk events with a sample application in PingOne. Simulations allow you to deepen your understanding of how PingOne Risk detects different types of risk events.

For more information on risk predictors, see [Risk predictor types](#_t79t3wn9va9j).

**Before you begin**

You’ll need:

* You’ll need a PingOne account and an environment with the PingOne Risk service. You can use an existing account or start a PingOne trial. For more information, see [Starting a PingOne trial](https://docs.pingidentity.com/r/en-us/pingone/p1_start_a_pingone_trial?tocId=dTAKOHd57wlzNWVfCX6Myw) and [Adding the PingOne Risk service to your environment](#_ee376k7pe5e7).
* You can optionally use a sample app to test the risk predictors. To learn how to configure an environment with a sample app, see [Try PingOne Risk with a sample app](#_sabqk9qmh76t).

To test common risk predictors:

* **Geovelocity anomaly**: Sign on to your account, and then sign on again with a Remote Desktop Protocol (RDP) in a server from a remote datacenter. You can alternatively have a colleague based in a different location sign on to the sample app with the same user.
* **New device**: Sign on from one device, and then sign on again from another device.
* **Anonymous network detection**: Use a public VPN/server or browser extension that hides your IP address, and sign on.
* **User-based risk behavior (individual user)**: Train the predictor by creating risk evaluations (such as signing on with the same user account several times and authenticating successfully each time), and then create a new risk evaluation (such as signing on again from a different browser or a different operating system if possible).

To learn more about testing risk predictors, see [Simulating risk events](https://support.pingidentity.com/s/article/simulating-risk-events). To get access to this support information, contact Ping Identity Sales at [www.pingidentity.com/en/company/contact-sales.html](http://www.pingidentity.com/en/company/contact-sales.html).

# Advanced - customizing risk policies

Once you’ve accumulated sufficient authentication data and analyzed it, you can use the **Risk Policies** page in PingOne to modify the default risk policy or create additional risk policies of your own.

When you create a policy, there are four decisions you are making:

* Which risk predictors you want to include in the overall risk calculation
* The degree to which each included predictor should be taken into account when calculating the overall risk score.
* What the cutoffs should be for categorizing an overall risk score as Low, Medium, or High risk
* Whether there are factors that should override the generated risk score. For example, you may decide that if the authentication attempt is coming from an unrecognized device, the overall risk evaluation should be High risk, regardless of the total risk score that was calculated.

# Advanced - staging policies

To test risk policy changes before actually putting them into production, you can create a staging policy that is associated with the risk policy that you are currently using.

When an evaluation event occurs for the production risk policy, the incoming risk data is also passed through the associated staging policy, creating two sets of risk evaluation data: one for the production policy and one for its associated staging policy.

A staging policy allows you to fine tune and test risk policy changes before releasing changes to your production policy, and does not affect your end users until you decide to do so by promoting a staging policy to production.

For more information on creating and managing staging policies, see [Risk policies](https://docs.pingidentity.com/r/en-us/pingone/pingone_p1risk_risk_policies).

## Tutorial: Evaluating staging policy risk data

Learn how to analyze and evaluate risk data from a staging policy displayed in the Risk dashboard.

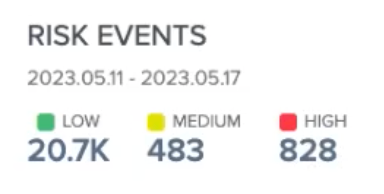
**Before you begin**

Create a staging policy. For more information, see [Risk policies](https://docs.pingidentity.com/r/en-us/pingone/pingone_p1risk_risk_policies).

After creating your staging policy, you can view the risk data to determine how your policy changes affect end users.

To view risk data from a staging policy in the Risk dashboard:

1. Go to **Dashboards** → **Risk**.
2. Click the **Risk Events** graph.
3. Review the total counts above the default graph, which shows only production event types.



1. Click the **Event Types** dropdown, and select both the **Production** and **Staging** checkboxes.

**Result**: The graph refreshes to display risk event data from both production and staging risk policies.

1. Review the updated total counts to see how your staging policy affects each risk level.



1. Next, review the data in the drill-down table.

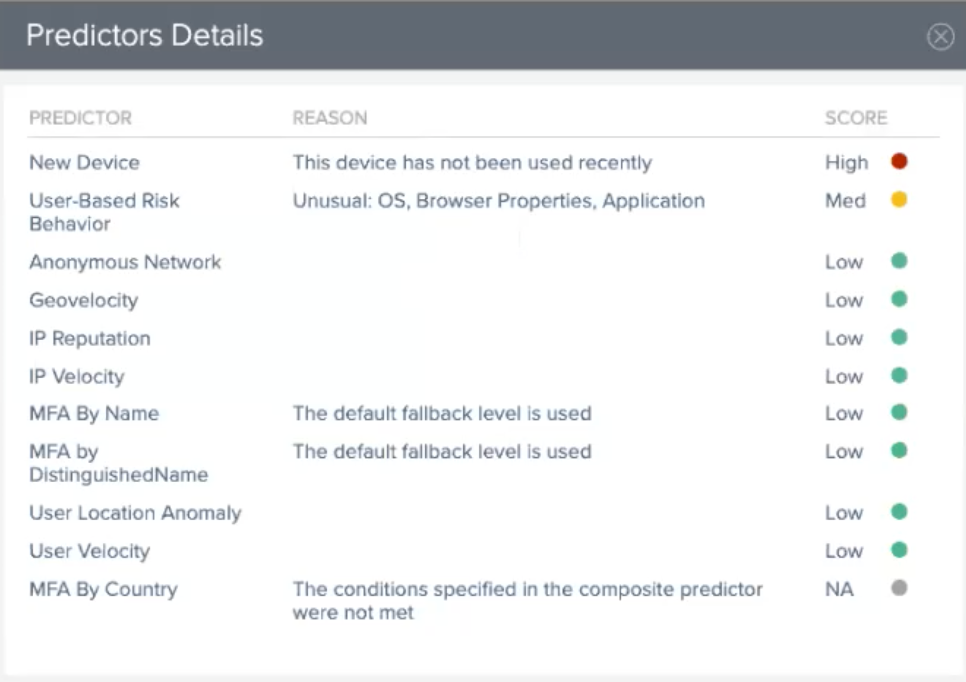
**Note:** Only events that have triggered a specific risk predictor, such as geovelocity anomaly, or have an aggregated risk score of HIGH are shown.

* 1. Take note of the **Risk Policy** column to determine whether each risk event is associated with the production or staging policy. Check risk events specifically from the staging policy and review how the changes you made affect the data.



* 1. Scroll across to the **Predictors** column, and click **Details** in any risk event row to review the score for each configured predictor and the reason.

**Example:** If you added the **New Device** predictor in your staging policy and do not use this predictor in your production policy, a risk event is triggered only in the staging policy when a user signs on with a new device**.** In the **Predictors Details** for this risk event, the **New Device** predictor shows a **High** score because the device has not been used recently. This allows you to test how your changes to the staging policy might affect users with real-time risk data passed from the production policy.



**Next Steps:** Make any further adjustments to your staging policy if needed. After evaluating your staging policy, you can decide whether to [promote the staging policy to production](https://docs.pingidentity.com/r/en-us/pingone/pingone_p1risk_risk_policies).

# Advanced - customizing risk predictors

Risk predictors are the basic building blocks that form risk policies.

When you define your own risk policies, you may be satisfied just to use the out-of-the-box predictors provided, or a subset of them, and just adjust the degree to which each predictor is taken into account. If you want to further refine the process, you can customize the individual predictors.

There are three ways to customize the risk predictors that can be included in risk policies:

* Fine-tuning out-of-the box predictors
* Creating composite predictors
* Creating custom predictors, using risk variables that are not included in the out-of-the-box predictors

## Fine-tune out-of-the-box predictors

When you add the risk service to a PingOne environment, the environment includes one predictor of each basic type that is supported, for example, one Anonymous Network predictor and one IP Reputation predictor. The default name of the predictor is the name of the category.

You can customize the predictor by:

* Renaming the predictor
* Editing the settings contained in the predictor. For example, for the IP Reputation predictor, you can modify the fallback decision value or add a list of IPs that should always be considered low risk.

In addition to changing the settings of the default predictor in each category, you can create additional predictors of that type.

For example, you can create:

* A predictor of type User Location Anomaly called Strict User Location Anomaly and set the distance to 20 km and the fallback value to High risk.
* A second predictor of type User Location Anomaly called Lenient User Location Anomaly and set the distance to 50 km and the fallback value to Medium risk.

This will make it easy for you to include the strict predictor in a risk policy that you use for highly-sensitive applications, and include the more lenient predictor in a risk policy that you use for less-sensitive applications.

## Create a composite predictor

Each of the out-of-the-box risk predictors represents a single risk factor. In some cases, you may be interested in combining a number of risk predictors into a single predictor, such as when you're concerned about the use of an anonymous network only when a user location anomaly is also reported. This is where composite predictors come in.

In a composite predictor, you define conditions based on individual predictors, and you decide what level of risk should be assigned when the defined conditions are met. Composite predictors can include both the standard predictor types provided and any custom predictors that you have created.

In addition to taking into account the results of multiple individual risk predictors, you can include conditions that relate to the total number of predictors in a policy that were low risk, medium risk, or high risk.

For example, you can create a composite predictor that specifies that the predictor should get a result of high risk if any of the following conditions are true:

* IP reputation is high risk
* IP Velocity is high risk
* Any three predictors in the policy being evaluated are found to be high risk

In addition to standard and custom predictors, you can include the following risk factors as conditions in composite predictors:

* Country
* State
* IP range
* IP domain organization
* ISP
* target resource (application).

The result yielded by a composite predictor can be used in the same ways as the results of individual risk predictors:

* You can assign the predictor a score or weight to be used with the other predictors in your risk policy in order to calculate a final risk level.
* You can define an override in a policy that uses the composite predictor so that in cases where the predictor's conditions are met, you can directly assign a final risk level and ignore the other predictors in the risk policy.

For additional information on composite predictors, see [Composite predictors](https://docs.pingidentity.com/r/en-us/pingone/p1risk_add_composite_predictors).

## Create a custom predictor

In addition to including the out-of-the-box predictors in a risk policy, you can create custom predictors to include other sources of risk in your risk policies.

Custom predictors can include the following types of comparisons:

* Numerical comparisons, using ranges you have defined for Low, Medium, and High risk
* Checking if an IP falls into a range of IPs that you have defined
* String-matching

When defining a custom predictor, the Attribute Mapping field can take any of the following types of data:

* One of the fields included in the *details* object returned in the API response for risk evaluations, for example, *details.country*.
* One of the fields included in the *event* object included in the API request for risk evaluations, for example, *event.browser.userAgent.*
* Data that you include from an external source. This is done by including the data as a new field in the *event* object in the *Create risk evaluatio*n API request, for example, *event.externalAttribute*. You use the same name in the Attribute Mapping field in the UI when you define the custom predictor. For example, you can provide as input a risk score from a third-party.

For an idea of the types of information you can include as a custom predictor, see the fields in the *details* and *event* objects in the “Details data model” and “Event data model” tables in the [risk evaluation section](https://apidocs.pingidentity.com/pingone/platform/v1/api/#risk-evaluations) of the PingOne API documentation. See also the [sample response](https://apidocs.pingidentity.com/pingone/platform/v1/api/#post-create-risk-evaluation) for a *Create risk evaluatio*n API request.

When filling in the Attribute Mapping field, use this syntax: *${details.country}* or *$(event.browser.userAgent)*

# Advanced - using the PingOne API for risk evaluations

You can use the PingOne API to:

* Create and manage risk predictors.
* Create and manage risk policies.
* Create risk evaluations.
* Update the completion status of risk evaluations in order to help improve the accuracy of future risk evaluations.

For details, see the [risk section](https://apidocs.pingidentity.com/pingone/platform/v1/api/#pingone-risk) of the PingOne API documentation.

# Troubleshooting

# Error codes

=====

## PingOne Risk/Protect start up guide skeleton

**Introduction** Start with the value

* Example of use cases (registration , authentication) and how to integrate into these flows - avoid technical description)
* Fundamental steps to integrate PingOne Protect
* For developers - link to API documentation
* Architecture diagram (reuse from Ping’s web site)

**Try PingOne Protect in less than 5 minutes**

* Start a trial with our trial (CIAM or WF) - link to trials

**Getting Started**

* Short overview of use case (CIAM or WF)
* How POP sits in your flow (Registration, Authentication, Authorization, Access)
* Implementation order - best practices

**Risk Policies**How a policy works (focus on Scores), with examples

* Registration policy
* Mobile policy (TBD)
* How to tune the policy

**Predictors**

* Explain each predictor, what does it protect
* Explain Custom Predictors with two examples

Add interpretation of the API response (Can be post GA)

\*\*\* We must keep reference to PingOne Risk and documentation to PingOne Risk IK 1.3 and 1.3.1