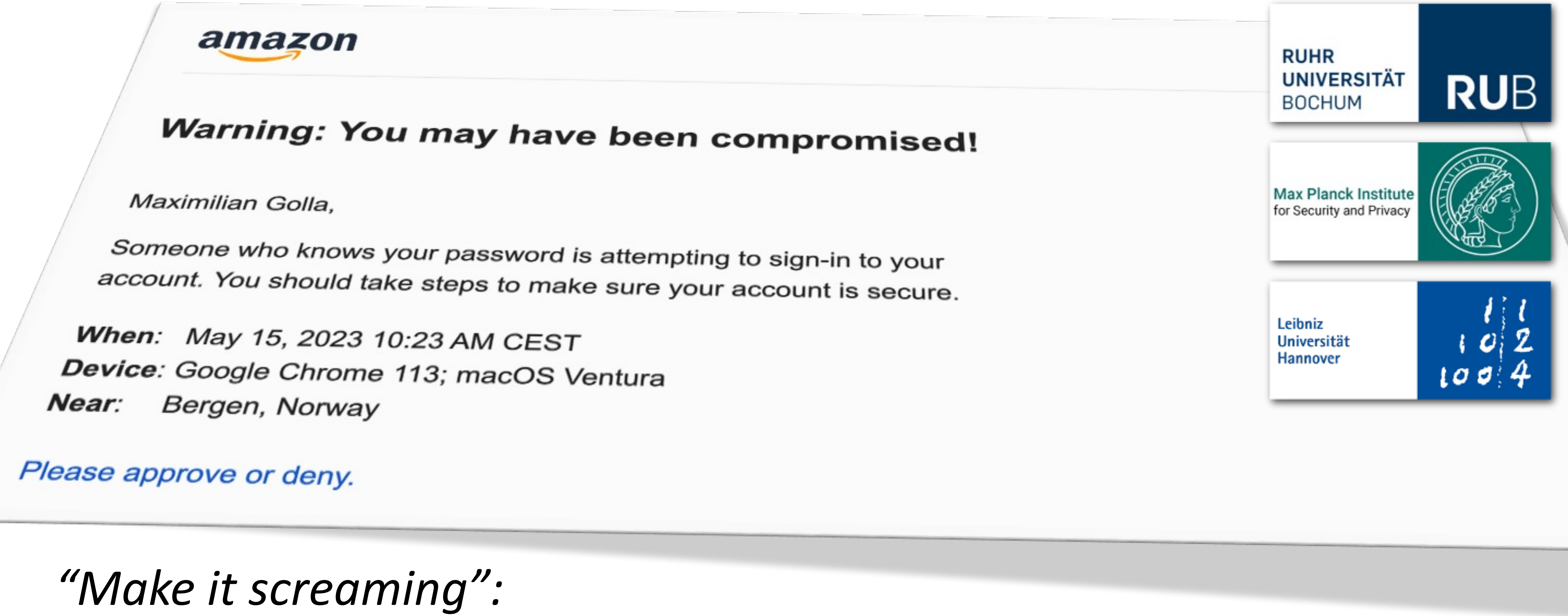


amazon

Warning: You may have been compromised!

Maximilian Golla,

Someone who knows your password is attempting to sign-in to your account. You should take steps to make sure your account is secure.

When: May 15, 2023 10:23 AM CEST
Device: Google Chrome 113; macOS Ventura
Near: Bergen, Norway

Please approve or deny.

RUHR UNIVERSITÄT BOCHUM RUB

Max Planck Institute for Security and Privacy

Leibniz Universität Hannover

“Make it screaming”: **How Administrators Configure Risk-based Authentication**

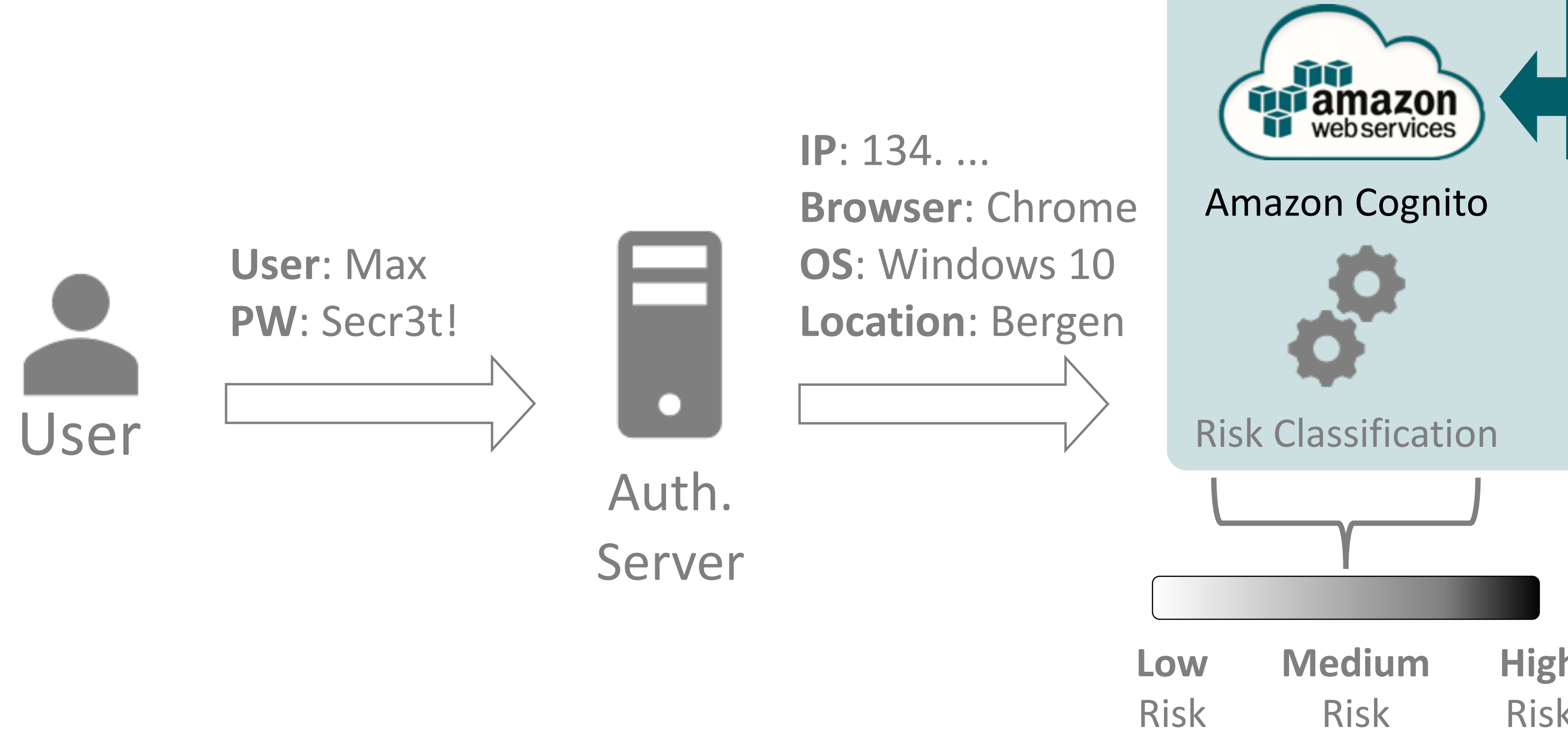
Philipp Markert, Theodor Schnitzler, Maximilian Golla, and Markus Dürmuth

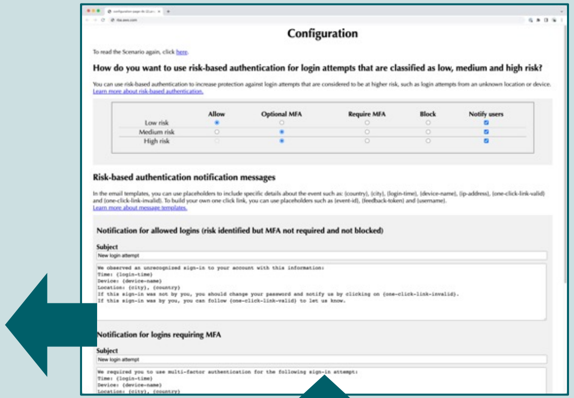
May 15—16, 2023 | PasswordsCon 2023 | Bergen, Norway

How Administrators Configure RBA

This Talk:

Configuration





Configuration

To read the Scenario again, click here.

How do you want to use risk-based authentication for login attempts that are classified as low, medium and high risk?

You can use risk-based authentication to increase protection against login attempts that are considered to be at higher risk, such as login attempts from an unknown location or device.
Learn more about risk-based authentication.

	Allow	Optional MFA	Require MFA	Block	Notify users
Low risk	●	○	○	○	☑
Medium risk	○	●	○	○	☑
High risk	○	●	○	○	☑

Risk-based authentication notification messages

In the email templates, you can use placeholders to include specific details about the event such as: {country}, {city}, {login-time}, {device-name}, {ip-address}, {one-click-link-valid} and {one-click-link-invalid}. To build your own one click link, you can use placeholders such as {event-id}, {feedback-token} and {username}.
Learn more about message templates.

Notification for allowed logins (risk identified but MFA not required and not blocked)

Subject
New login attempt

```
We observed an unrecognized sign-in to your account with this information:
Time: {login-time}
Device: {device-name}
Location: {city}, {country}
If this sign-in was not by you, you should change your password and notify us by clicking on {one-click-link-invalid}.
If this sign-in was by you, you can follow {one-click-link-valid} to let us know.
```

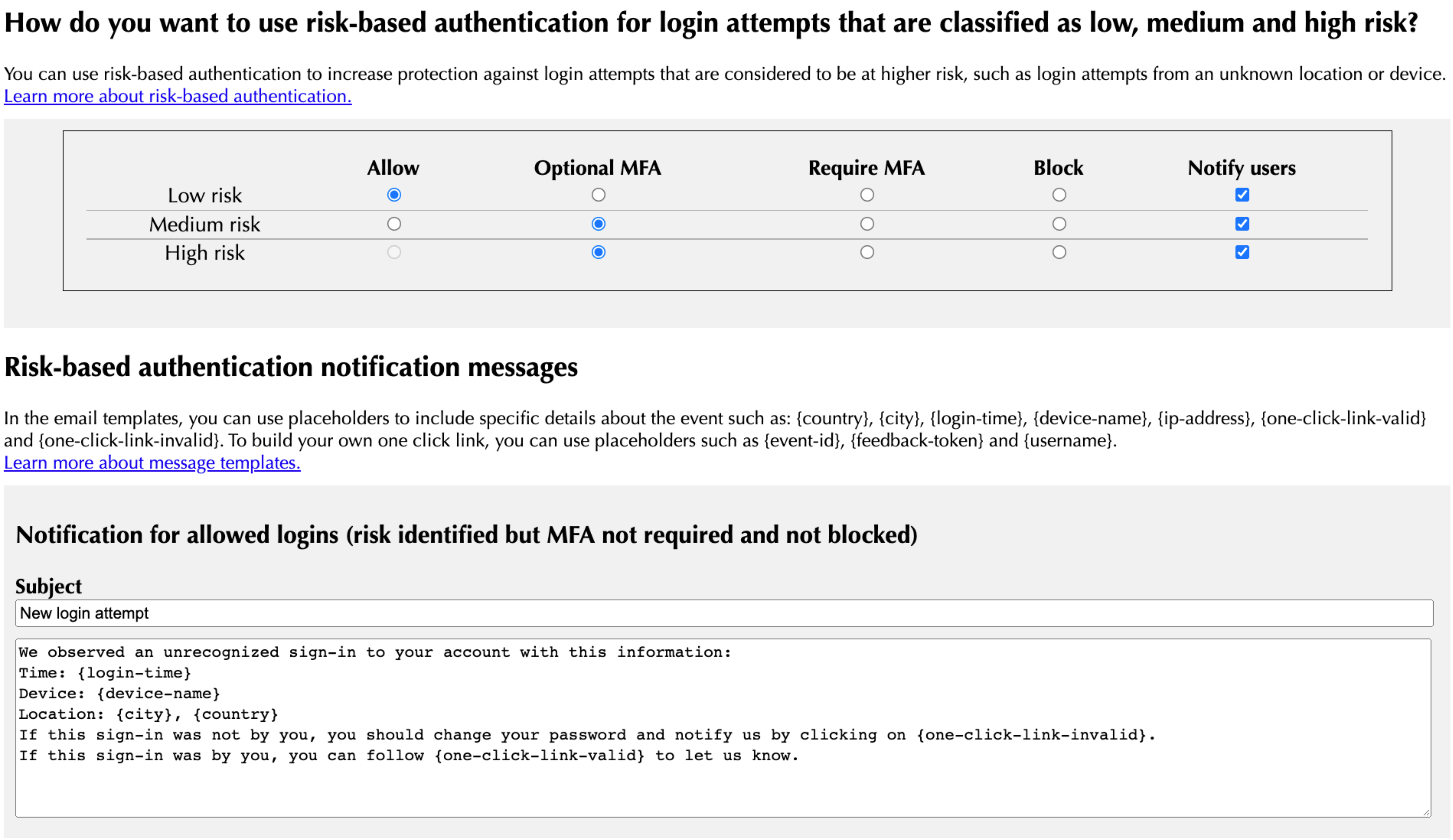
Notification for logins requiring MFA

Subject
New login attempt

```
We required you to use multi-factor authentication for the following sign-in attempt:
Time: {login-time}
Device: {device-name}
Location: {city}, {country}
```

Admin

Configuration



How do you want to use risk-based authentication for login attempts that are classified as low, medium and high risk?

You can use risk-based authentication to increase protection against login attempts that are considered to be at higher risk, such as login attempts from an unknown location or device.
Learn more about risk-based authentication.

	Allow	Optional MFA	Require MFA	Block	Notify users
Low risk	●	○	○	○	☑
Medium risk	○	●	○	○	☑
High risk	○	●	○	○	☑

Risk-based authentication notification messages

In the email templates, you can use placeholders to include specific details about the event such as: {country}, {city}, {login-time}, {device-name}, {ip-address}, {one-click-link-valid} and {one-click-link-invalid}. To build your own one click link, you can use placeholders such as {event-id}, {feedback-token} and {username}.
Learn more about message templates.

Notification for allowed logins (risk identified but MFA not required and not blocked)

Subject

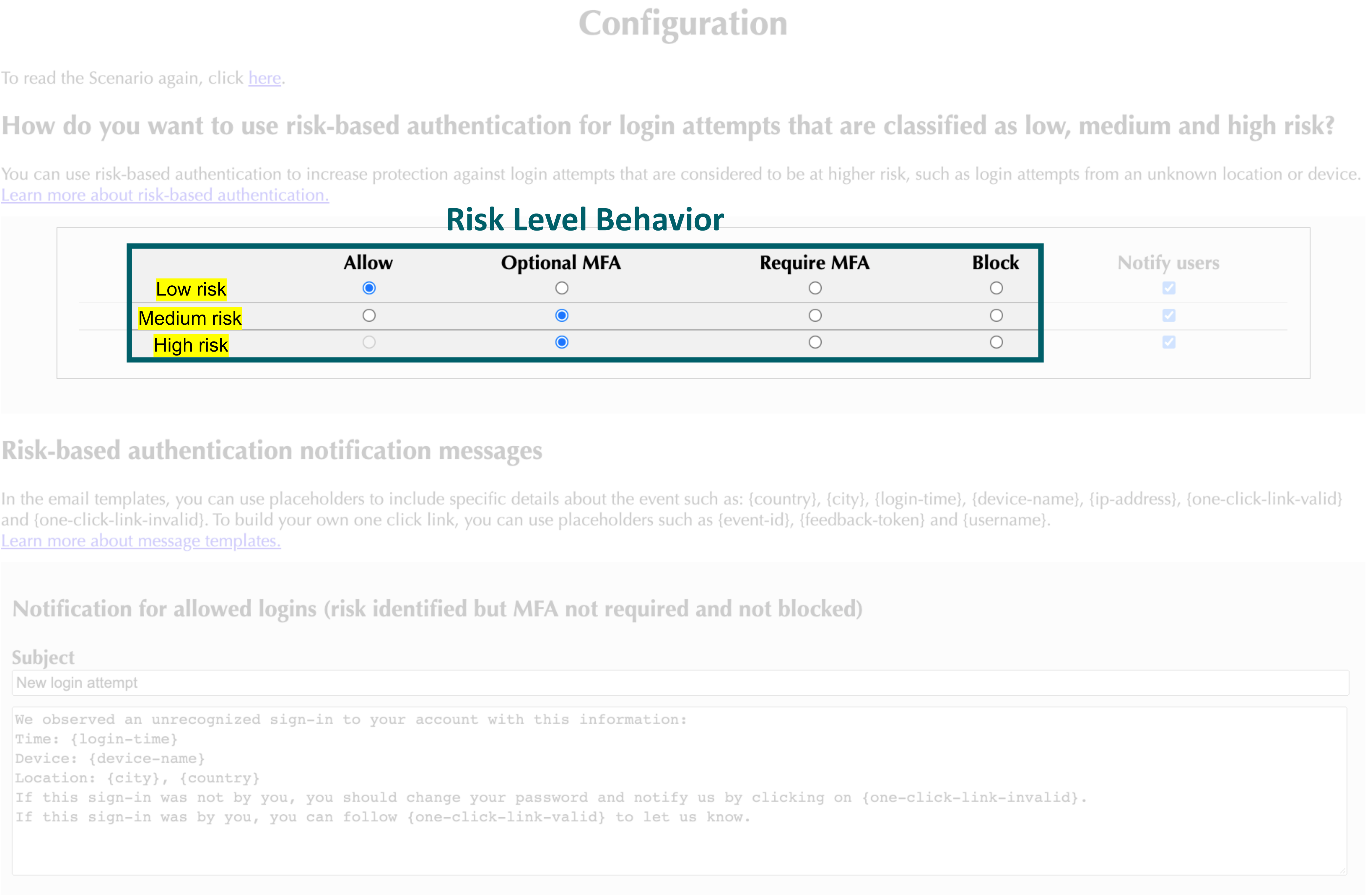
New login attempt

```
We observed an unrecognized sign-in to your account with this information:
Time: {login-time}
Device: {device-name}
Location: {city}, {country}
If this sign-in was not by you, you should change your password and notify us by clicking on {one-click-link-invalid}.
If this sign-in was by you, you can follow {one-click-link-valid} to let us know.
```

Risk Level Behavior

Risk Level Behavior

Risk	Allow	Block
Low	✓	
Medium	MFA	
High		✗



Configuration

To read the Scenario again, click here.

How do you want to use risk-based authentication for login attempts that are classified as low, medium and high risk?

You can use risk-based authentication to increase protection against login attempts that are considered to be at higher risk, such as login attempts from an unknown location or device.
Learn more about risk-based authentication.

Risk Level Behavior

	Allow	Optional MFA	Require MFA	Block	Notify users
Low risk	●	○	○	○	☑
Medium risk	○	●	○	○	☑
High risk	○	●	○	○	☑

Risk-based authentication notification messages

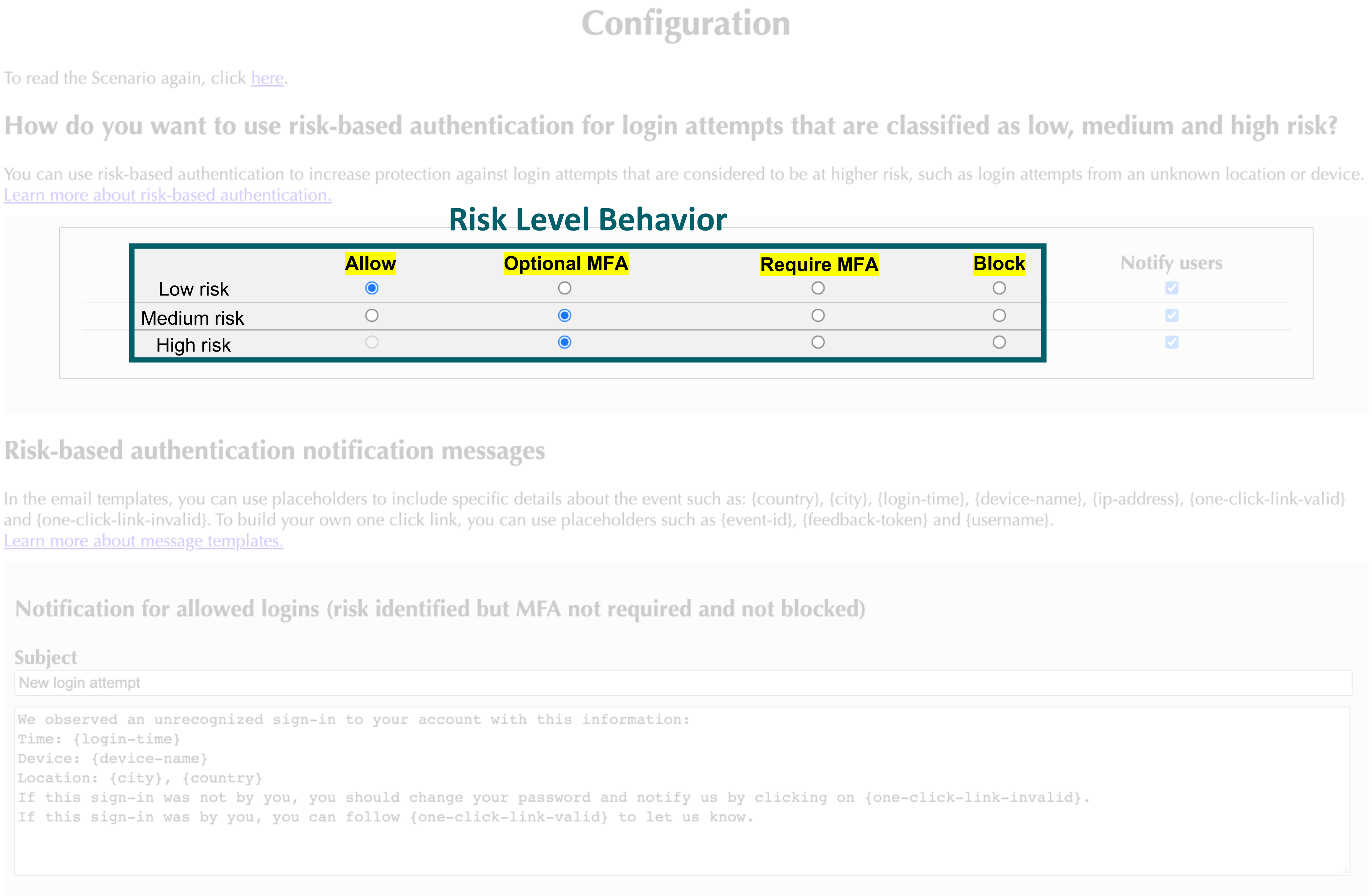
In the email templates, you can use placeholders to include specific details about the event such as: {country}, {city}, {login-time}, {device-name}, {ip-address}, {one-click-link-valid} and {one-click-link-invalid}. To build your own one click link, you can use placeholders such as {event-id}, {feedback-token} and {username}.
Learn more about message templates.

Notification for allowed logins (risk identified but MFA not required and not blocked)

Subject

New login attempt

```
We observed an unrecognized sign-in to your account with this information:
Time: {login-time}
Device: {device-name}
Location: {city}, {country}
If this sign-in was not by you, you should change your password and notify us by clicking on {one-click-link-invalid}.
If this sign-in was by you, you can follow {one-click-link-valid} to let us know.
```



Configuration

To read the Scenario again, click here.

How do you want to use risk-based authentication for login attempts that are classified as low, medium and high risk?

You can use risk-based authentication to increase protection against login attempts that are considered to be at higher risk, such as login attempts from an unknown location or device.
Learn more about risk-based authentication.

Risk Level Behavior

	Allow	Optional MFA	Require MFA	Block	Notify users
Low risk	●	○	○	○	☑
Medium risk	○	●	○	○	☑
High risk	○	●	○	○	☑

Risk-based authentication notification messages

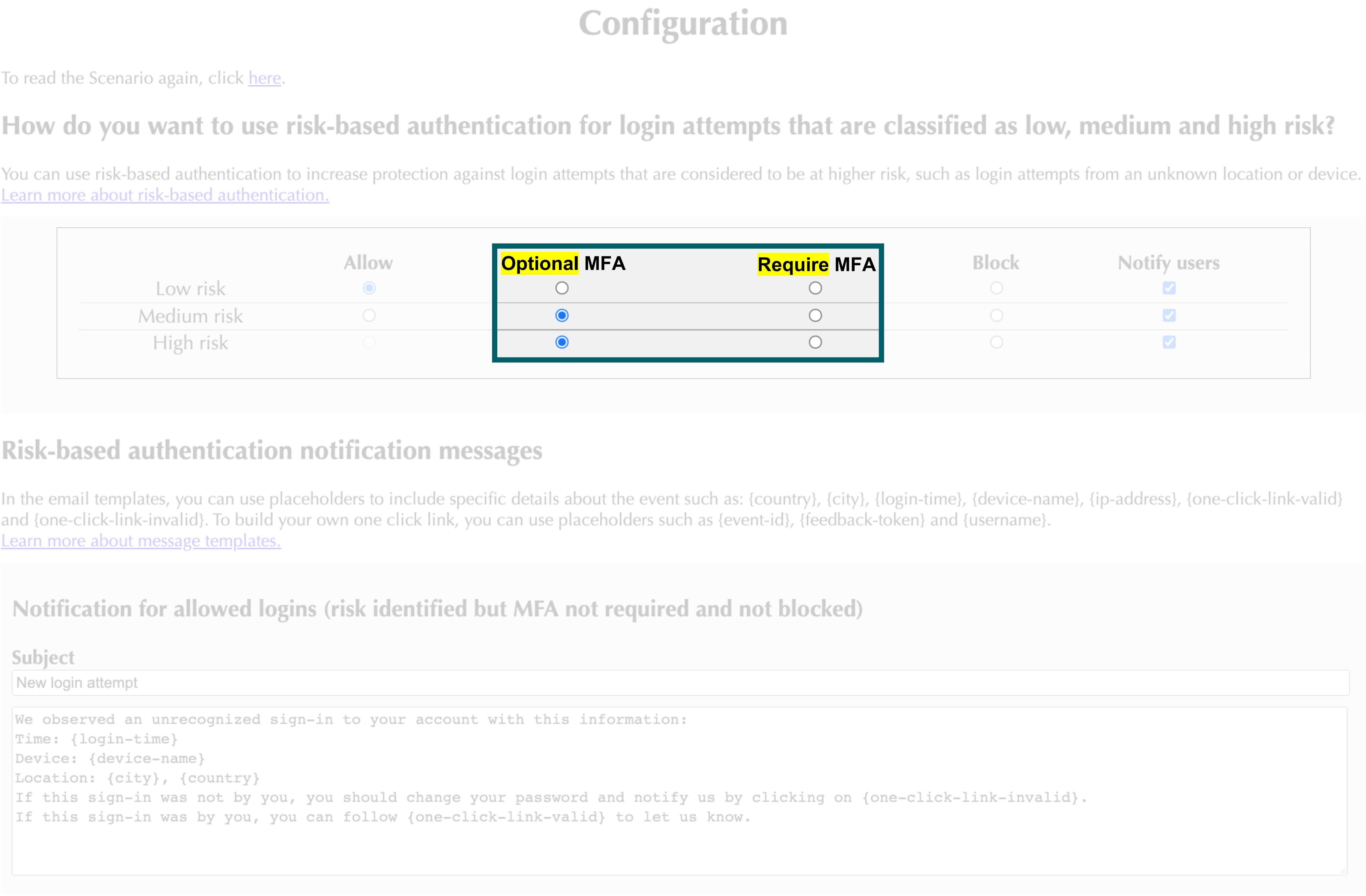
In the email templates, you can use placeholders to include specific details about the event such as: {country}, {city}, {login-time}, {device-name}, {ip-address}, {one-click-link-valid} and {one-click-link-invalid}. To build your own one click link, you can use placeholders such as {event-id}, {feedback-token} and {username}.
Learn more about message templates.

Notification for allowed logins (risk identified but MFA not required and not blocked)

Subject

New login attempt

```
We observed an unrecognized sign-in to your account with this information:
Time: {login-time}
Device: {device-name}
Location: {city}, {country}
If this sign-in was not by you, you should change your password and notify us by clicking on {one-click-link-invalid}.
If this sign-in was by you, you can follow {one-click-link-valid} to let us know.
```



Configuration

To read the Scenario again, click here.

How do you want to use risk-based authentication for login attempts that are classified as low, medium and high risk?

You can use risk-based authentication to increase protection against login attempts that are considered to be at higher risk, such as login attempts from an unknown location or device.
Learn more about risk-based authentication.

	Allow	Optional MFA	Require MFA	Block	Notify users
Low risk	●	○	○	○	☑
Medium risk	○	●	○	○	☑
High risk	○	●	○	○	☑

Risk-based authentication notification messages

In the email templates, you can use placeholders to include specific details about the event such as: {country}, {city}, {login-time}, {device-name}, {ip-address}, {one-click-link-valid} and {one-click-link-invalid}. To build your own one click link, you can use placeholders such as {event-id}, {feedback-token} and {username}.
Learn more about message templates.

Notification for allowed logins (risk identified but MFA not required and not blocked)

Subject

New login attempt

```
We observed an unrecognized sign-in to your account with this information:
Time: {login-time}
Device: {device-name}
Location: {city}, {country}
If this sign-in was not by you, you should change your password and notify us by clicking on {one-click-link-invalid}.
If this sign-in was by you, you can follow {one-click-link-valid} to let us know.
```

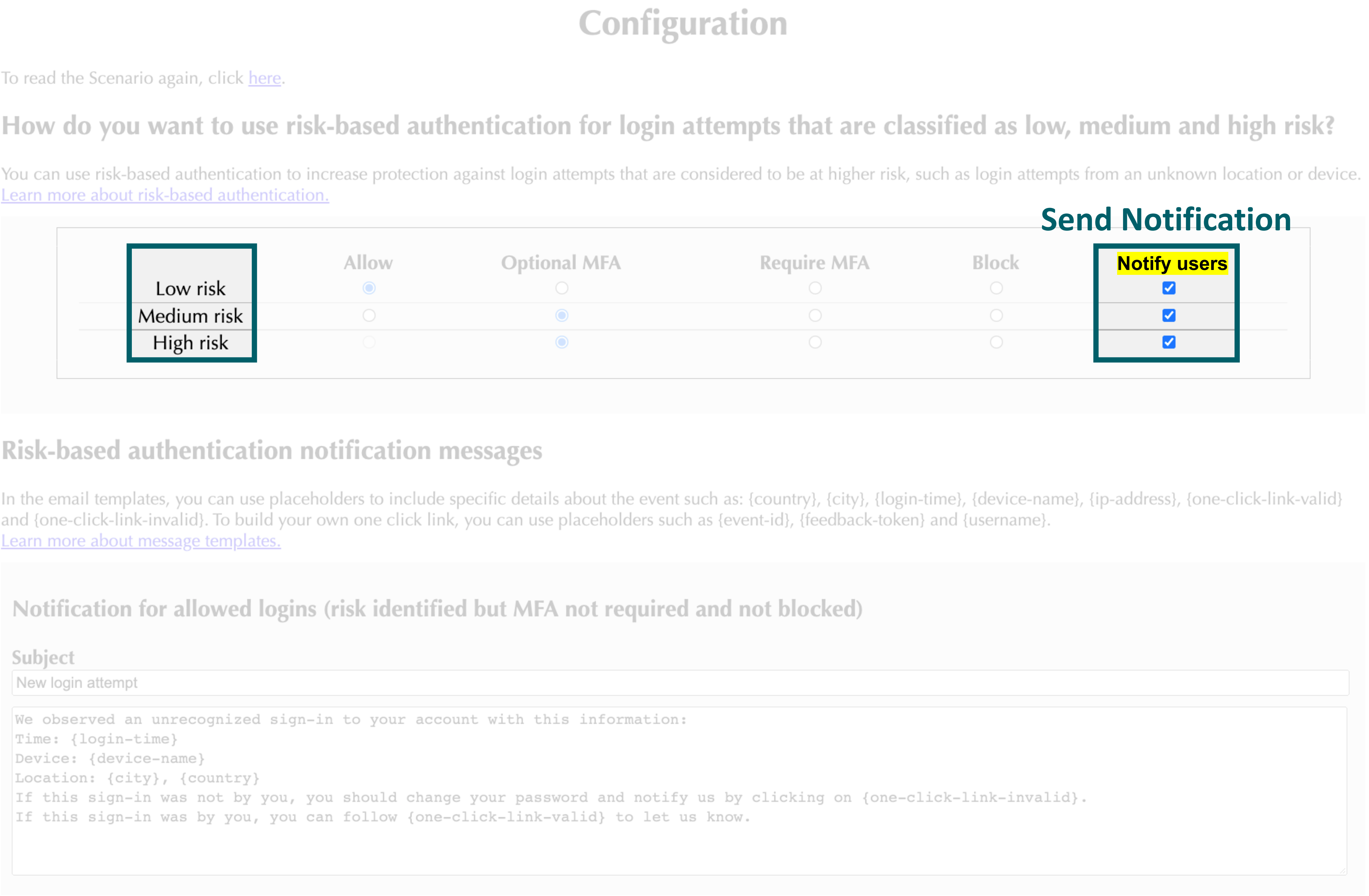
Send Notification

Risk Level Behavior

Send Notification

Risk	Allow	Block
Low	✓	
Medium	MFA	
High		✗

Notify	Yes	No
Low		✗
Medium	✓	
High	✓	



Configuration

To read the Scenario again, click here.

How do you want to use risk-based authentication for login attempts that are classified as low, medium and high risk?

You can use risk-based authentication to increase protection against login attempts that are considered to be at higher risk, such as login attempts from an unknown location or device.
Learn more about risk-based authentication.

Send Notification

	Allow	Optional MFA	Require MFA	Block	Notify users
Low risk	●	○	○	○	☑
Medium risk	○	●	○	○	☑
High risk	○	●	○	○	☑

Risk-based authentication notification messages

In the email templates, you can use placeholders to include specific details about the event such as: {country}, {city}, {login-time}, {device-name}, {ip-address}, {one-click-link-valid} and {one-click-link-invalid}. To build your own one click link, you can use placeholders such as {event-id}, {feedback-token} and {username}.
Learn more about message templates.

Notification for allowed logins (risk identified but MFA not required and not blocked)

Subject

New login attempt

```
We observed an unrecognized sign-in to your account with this information:
Time: {login-time}
Device: {device-name}
Location: {city}, {country}
If this sign-in was not by you, you should change your password and notify us by clicking on {one-click-link-invalid}.
If this sign-in was by you, you can follow {one-click-link-valid} to let us know.
```

Notification Text

Risk Level Behavior

Send Notification

Notification Text

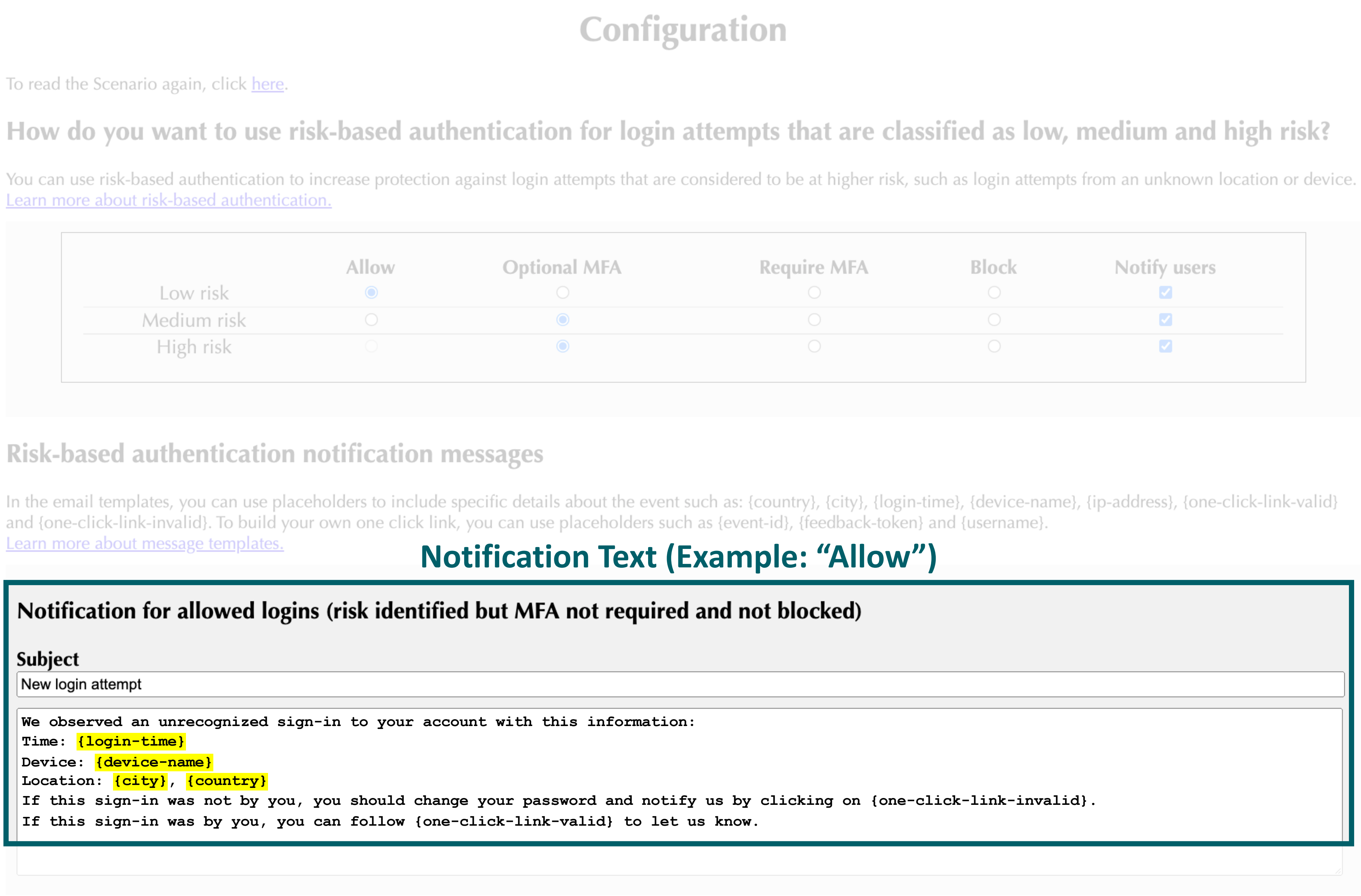
Risk	Allow	Block
Low	✓	
Medium	MFA	
High		✗

Notify	Yes	No
Low		✗
Medium	✓	
High	✓	

Hey, was that you?

Hey Maximilian,
We noticed an usual login:

Date: May 15, 2023 10:29:42 CEST
Location: Bergen, Norway
Device: Safari on iOS 16



Configuration

To read the Scenario again, click here.

How do you want to use risk-based authentication for login attempts that are classified as low, medium and high risk?

You can use risk-based authentication to increase protection against login attempts that are considered to be at higher risk, such as login attempts from an unknown location or device.
Learn more about risk-based authentication.

	Allow	Optional MFA	Require MFA	Block	Notify users
Low risk	●	○	○	○	☑
Medium risk	○	●	○	○	☑
High risk	○	●	○	○	☑

Risk-based authentication notification messages

In the email templates, you can use placeholders to include specific details about the event such as: {country}, {city}, {login-time}, {device-name}, {ip-address}, {one-click-link-valid} and {one-click-link-invalid}. To build your own one click link, you can use placeholders such as {event-id}, {feedback-token} and {username}.
Learn more about message templates.

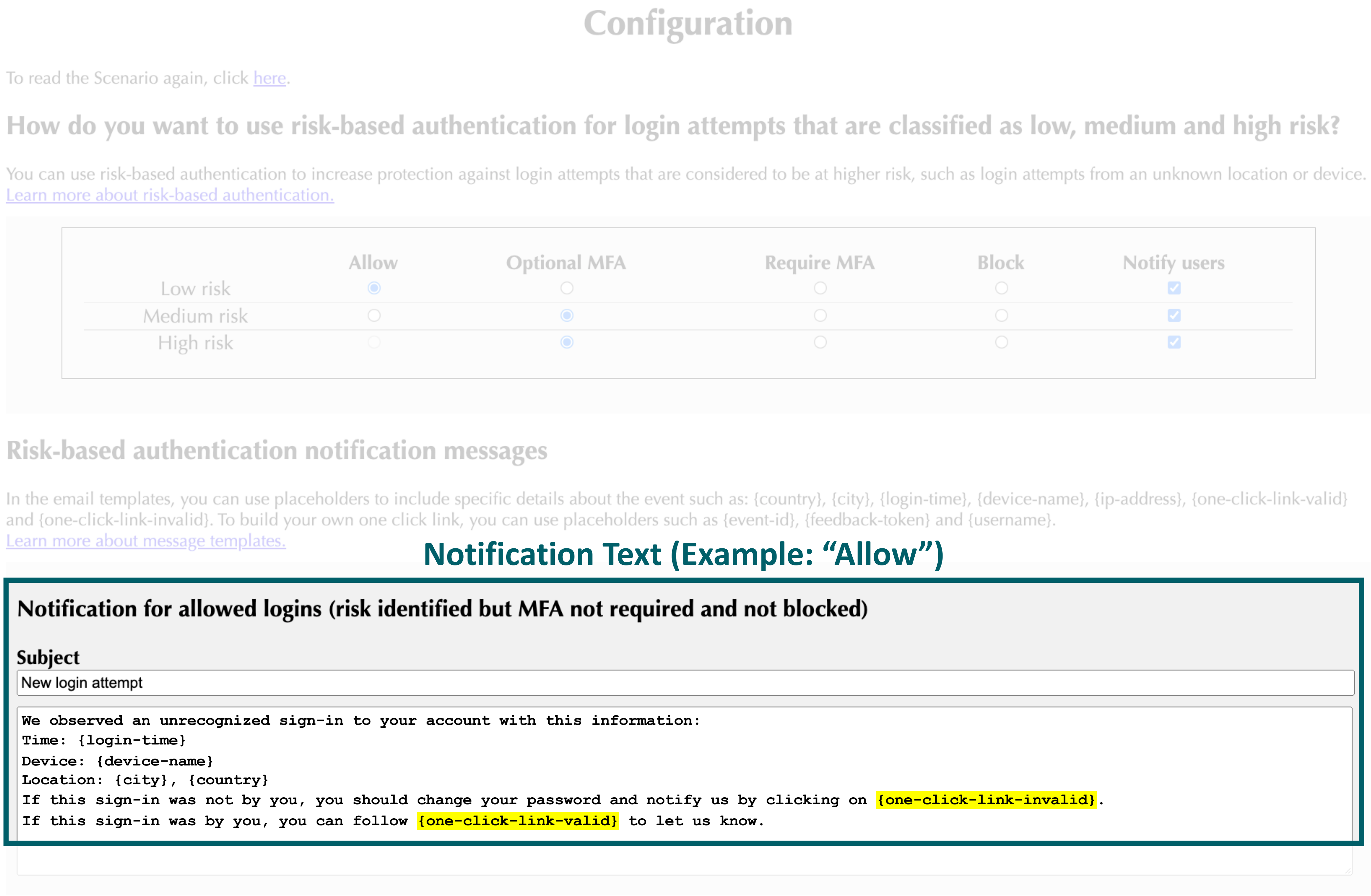
Notification Text (Example: “Allow”)

Notification for allowed logins (risk identified but MFA not required and not blocked)

Subject

New login attempt

```
We observed an unrecognized sign-in to your account with this information:
Time: {login-time}
Device: {device-name}
Location: {city}, {country}
If this sign-in was not by you, you should change your password and notify us by clicking on {one-click-link-invalid}.
If this sign-in was by you, you can follow {one-click-link-valid} to let us know.
```



Configuration

To read the Scenario again, click here.

How do you want to use risk-based authentication for login attempts that are classified as low, medium and high risk?

You can use risk-based authentication to increase protection against login attempts that are considered to be at higher risk, such as login attempts from an unknown location or device. Learn more about risk-based authentication.

	Allow	Optional MFA	Require MFA	Block	Notify users
Low risk	●	○	○	○	☑
Medium risk	○	●	○	○	☑
High risk	○	●	○	○	☑

Risk-based authentication notification messages

In the email templates, you can use placeholders to include specific details about the event such as: {country}, {city}, {login-time}, {device-name}, {ip-address}, {one-click-link-valid} and {one-click-link-invalid}. To build your own one click link, you can use placeholders such as {event-id}, {feedback-token} and {username}.
Learn more about message templates.

Notification Text (Example: “Allow”)

Notification for allowed logins (risk identified but MFA not required and not blocked)

Subject

New login attempt

```
We observed an unrecognized sign-in to your account with this information:
Time: {login-time}
Device: {device-name}
Location: {city}, {country}
If this sign-in was not by you, you should change your password and notify us by clicking on {one-click-link-invalid}.
If this sign-in was by you, you can follow {one-click-link-valid} to let us know.
```

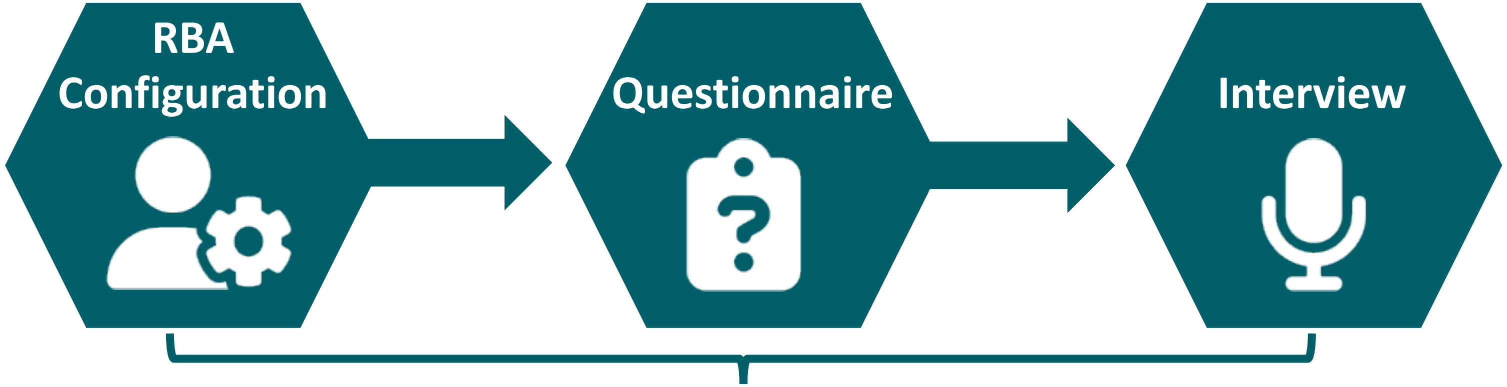
User Study + Interviews

Scenario:

“You are the system administrator of the MediaShop Corporation, where you administrate the online shop dresscode.com.”

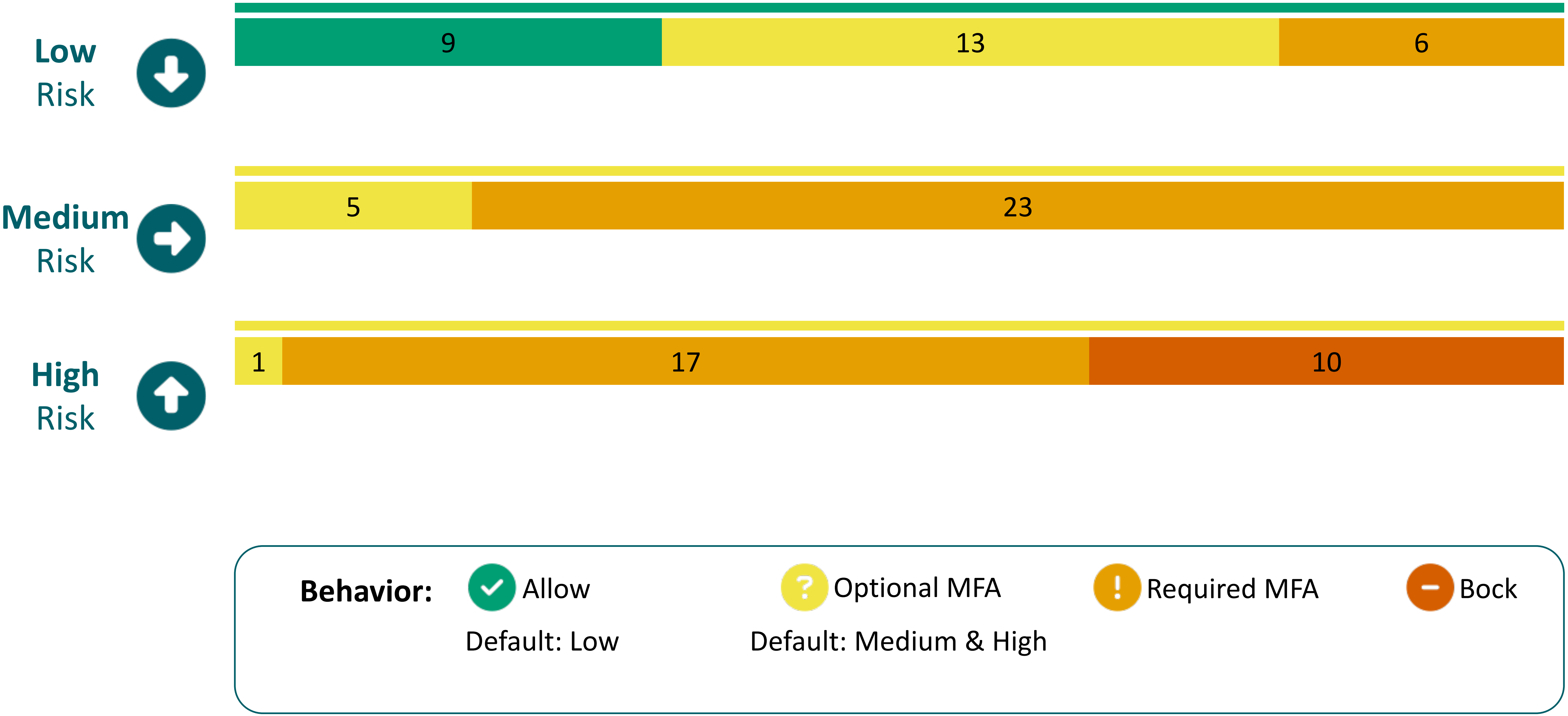
Task:

Configure a mock-up RBA system, modelled after Amazon Cognito.



~45 min; n=28 administrators
(9x < 10 years; 10x 10-15 years; 9x > 15 years)

Result: Risk Level Behavior



Reasoning

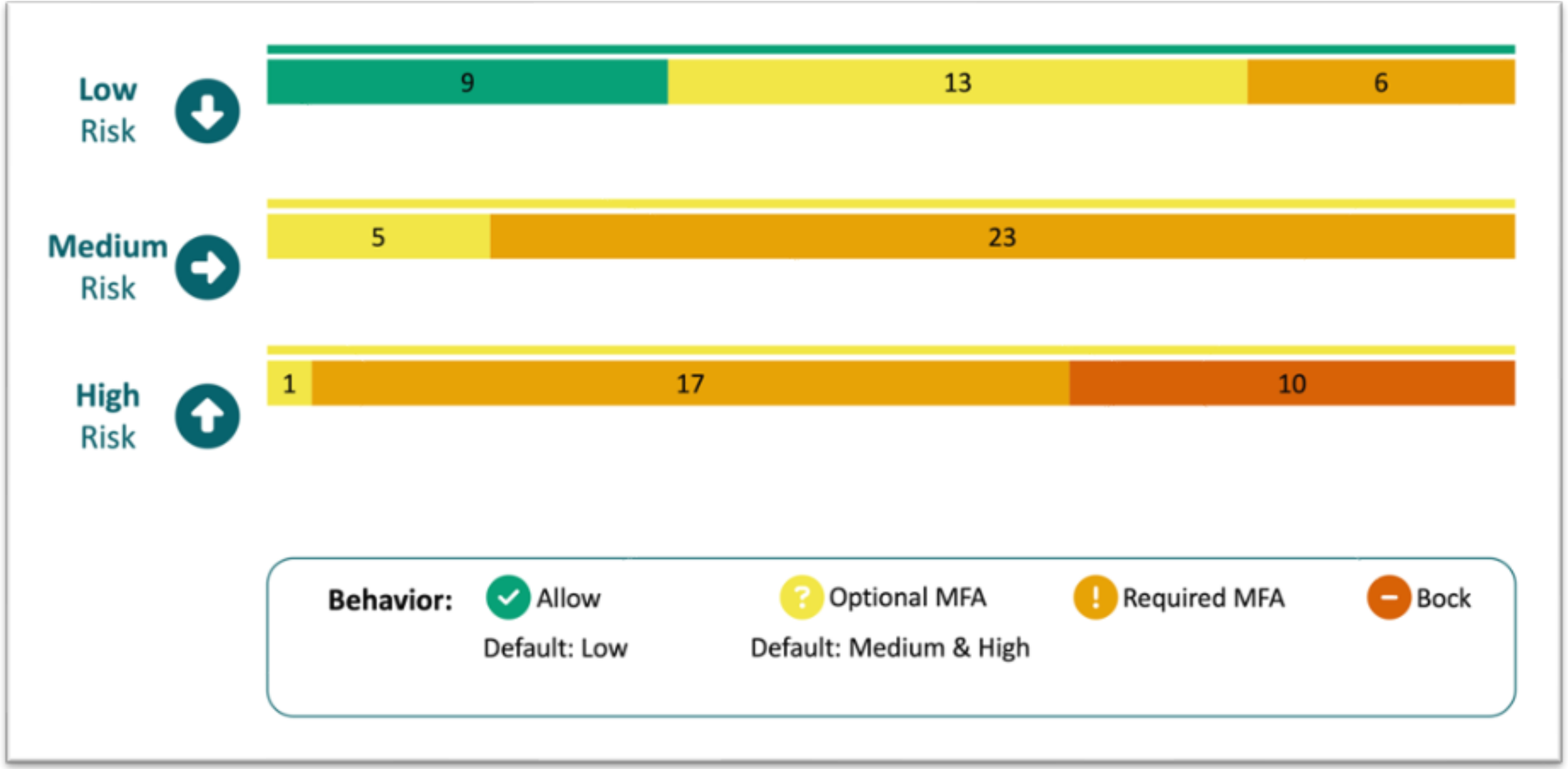
Theme:

- Spicing up the defaults

(19x Low, 23x Medium, 27x High)

Rationale:

- 14x MFA is easy
- 6x Prior experience
- 4x Focus on user



Quotes

MFA is Easy

“I chose to require MFA because from my experience, **users don’t find it that hard to use**, and it really increases the security.” (N-P5)

$$$ >> Security

“Blocking is of course invasive. I mean, **I would bounce our customers and we don’t want that**. Maybe they go to a competitor.” (N-P3)

Reasoning

Theme:

- Spicing up the defaults

(19x Low, 23x Medium, 27x High)

Rationale:

- 14x MFA is easy
  - 6x Prior experience
  - 4x Focus on user

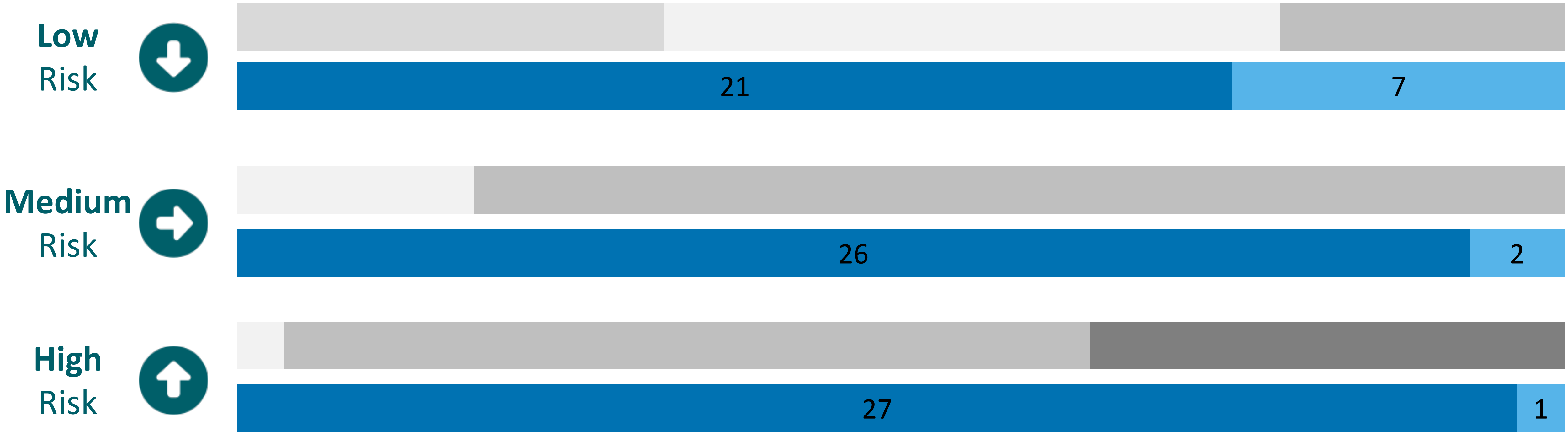
Obstacles:

- 8x Computation of risk levels
- 6x “Optional” MFA
- 4x Missing descriptions
- 4x Confusion around risk levels
- 3x Missing configuration options

Insights:

- 15x Clicked the help link
  - 2x Used Google/Wikipedia

Result: Send Notification



Behavior: ✓ Allow ? Optional MFA ! Required MFA − Bock

Notification: 🔔 Notify (Default) 🔕 Do not notify

Reasoning

🏴 **Theme**:

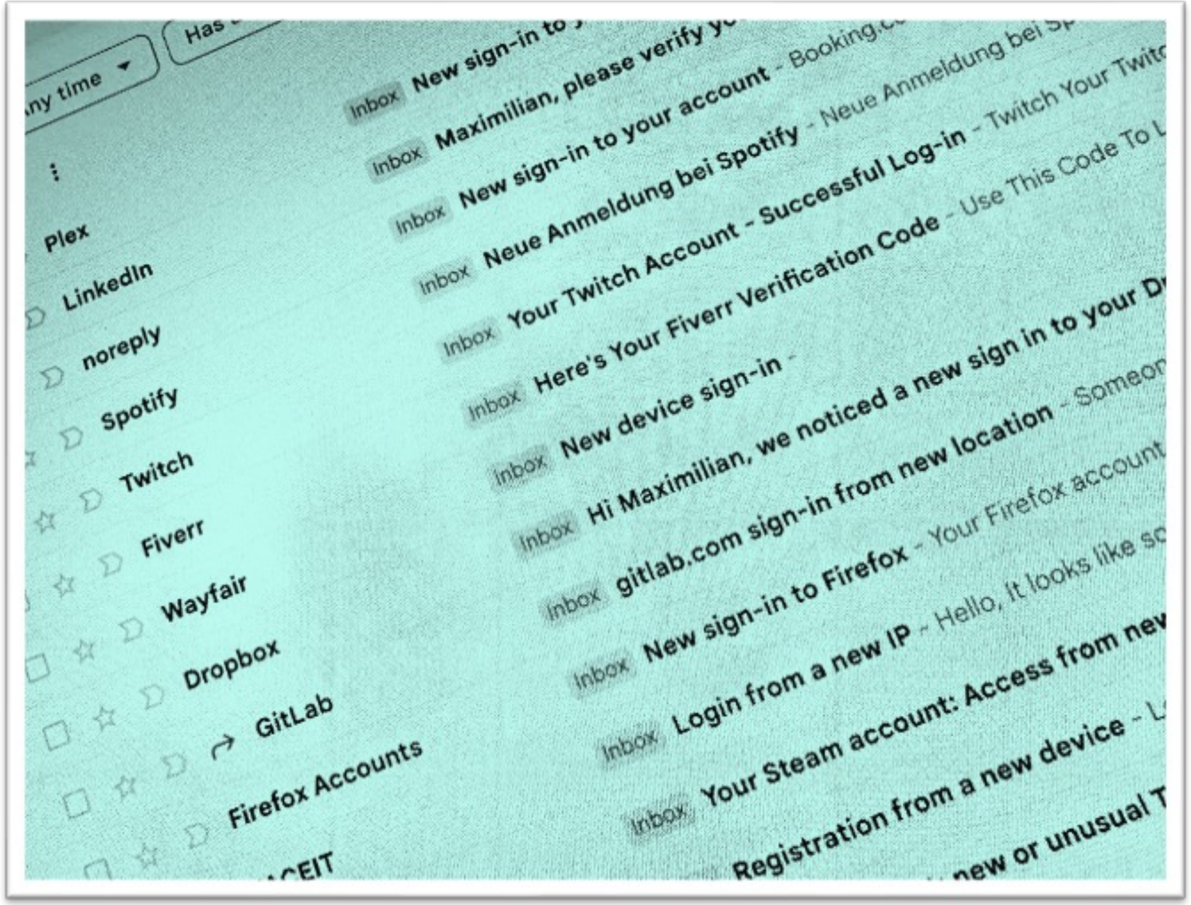
- Do not touch the defaults

(20x No change, 8x Change)

💬 **Rationale**:

- 7x Notification fatigue

- 1x Attacker could fool the system



ny time ▾ Has

Plex Inbox New sign-in to

LinkedIn Inbox Maximilian, please verify yo

noreply Inbox New sign-in to your account - Booking.c

Spotify Inbox Neue Anmeldung bei Spotify - Neue Anmeldung bei Sp

Twitch Inbox Your Twitch Account - Successful Log-in - Twitch Your Twit

Fiverr Inbox Here's Your Fiverr Verification Code - Use This Code To L

Wayfair Inbox New device sign-in -

Dropbox Inbox Hi Maximilian, we noticed a new sign in to your D

GitLab Inbox gitlab.com sign-in from new location - Someon

Firefox Accounts Inbox New sign-in to Firefox - Your Firefox account

Inbox Login from a new IP - Hello, It looks like so

Inbox Your Steam account: Access from new

CEIT Registration from a new device - L

new or unusual T

Quotes

Do Not Annoy Users

“If you get bombarded with login notifications, you get annoyed. […] why would you look at it unless you **make it screaming**?” (N-P1)

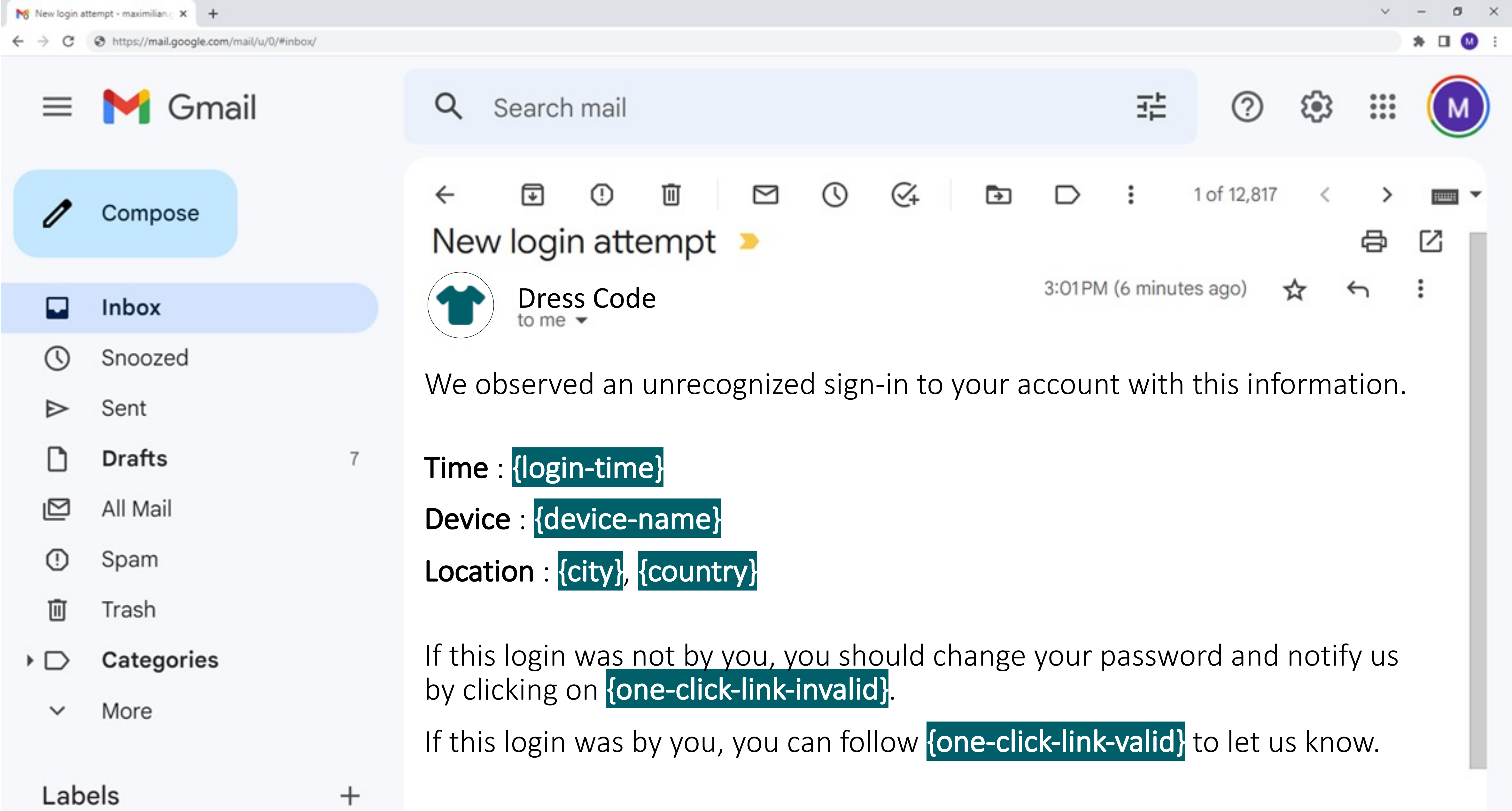
Attacker Could Fool the System

“I don’t know if I’m giving away information. If I have a hijacked account, and the **attacker can click—‘Yes, it’s really me.**’—How does it go then?” (U-P4)

At Google deleting the notification, cause an increase of the risk score.

USENIX Enigma 2018 - Anatomy of Account Takeover

Notification Text



New login attempt

Dress Code
to me

3:01 PM (6 minutes ago)

We observed an unrecognized sign-in to your account with this information.

Time : {login-time}

Device : {device-name}

Location : {city}, {country}

If this login was not by you, you should change your password and notify us by clicking on {one-click-link-invalid}.

If this login was by you, you can follow {one-click-link-valid} to let us know.

Results

Theme:

- The more details the better

(12x No change, 16x Change)

Rationale:

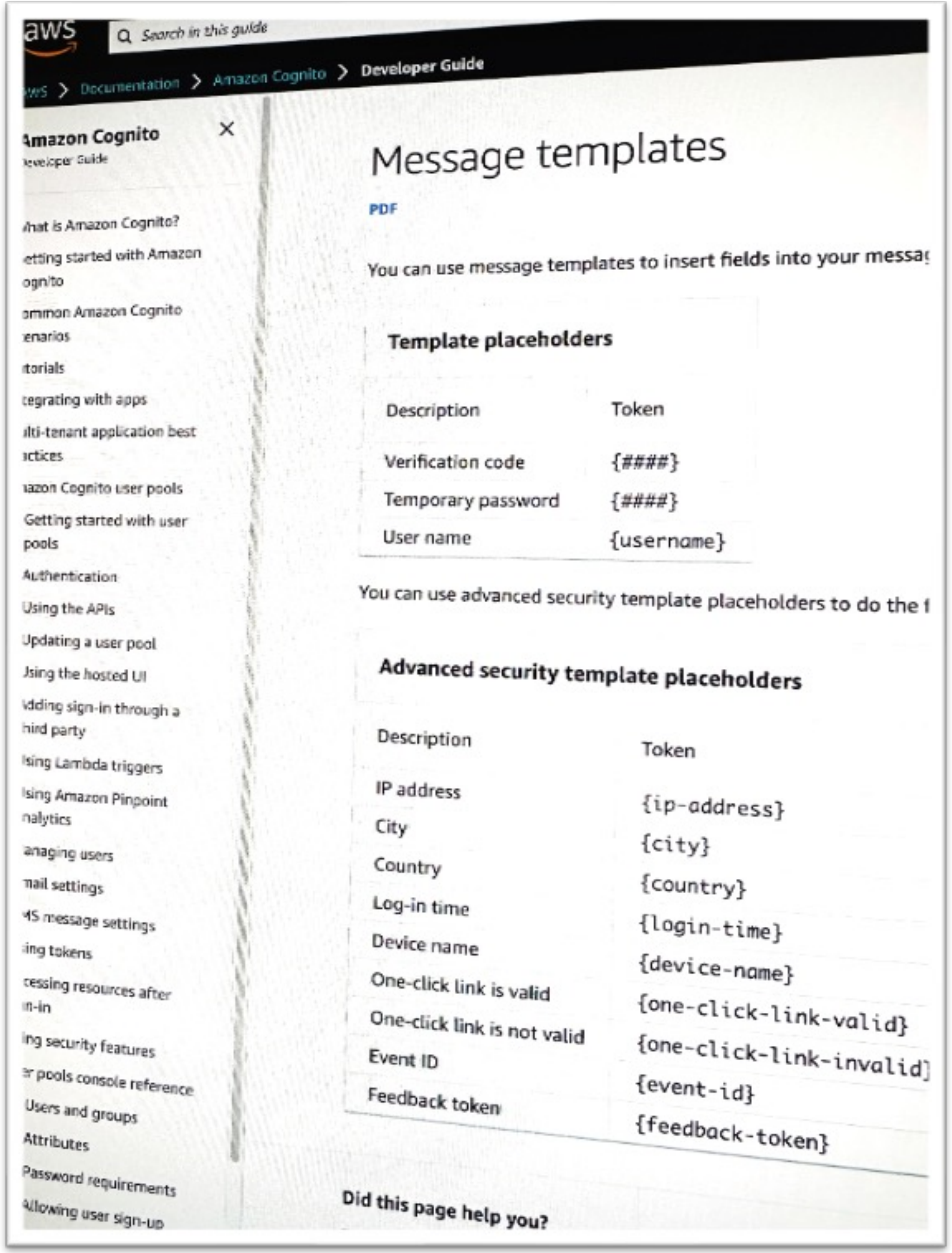
- 8x Add technical **details**

- 4x Change **wording**

- 3x Add more **context**

- 3x Prevent **phishing**

- 2x **Location distrust**



Amazon Cognito
eveloper Guide

hat is Amazon Cognito?
etting started with Amazon ognito
ommon Amazon Cognito enarios
torials
tegrating with apps
ilti-tenant application best actices
nazon Cognito user pools
Getting started with user pools
Authentication
Using the APIs
Updating a user pool
Jsing the hosted UI
dding sign-in through a hird party
sing Lambda triggers
sing Amazon Pinpoint nalytics
anaging users
nail settings
MS message settings
ing tokens
cessing resources after n-in
ing security features
r pools console reference
Users and groups
Attributes
Password requirements
Allowing user sign-up

Message templates

PDF

You can use message templates to insert fields into your messa

Template placeholders

Description	Token
Verification code	{####}
Temporary password	{####}
User name	{username}

You can use advanced security template placeholders to do the f

Advanced security template placeholders

Description	Token
IP address	{ip-address}
City	{city}
Country	{country}
Log-in time	{login-time}
Device name	{device-name}
One-click link is valid	{one-click-link-valid}
One-click link is not valid	{one-click-link-invalid}
Event ID	{event-id}
Feedback token	{feedback-token}

Did this page help you?

Quotes

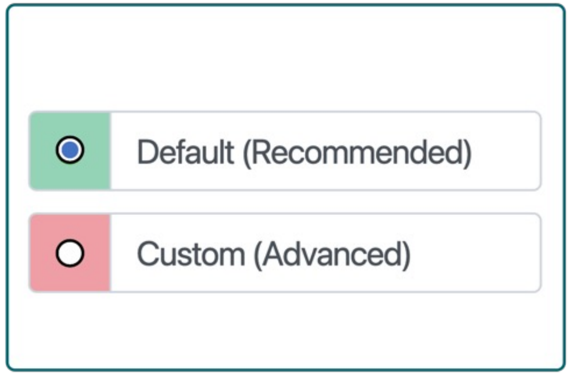
Help Users (aka Avoid Tickets)

“I’m trying to make it understandable, which can be a challenge, so in real life, I probably would have spent more time and also work with the communications people and tested it.” (N-P1)

Updates Will Break It

“I know that if you put software somewhere and tinker with it, it will break by the third update at the latest. [...] Especially when working with placeholders, things go wrong so easily.” (N-P4)

Recommendations



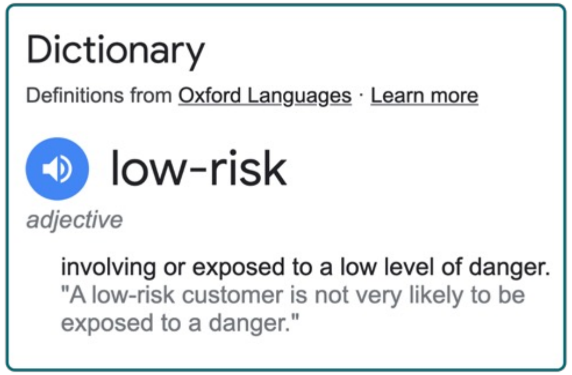
● Default (Recommended)

○ Custom (Advanced)

The Power of Defaults

Administrators struggle to decide which behavior is reasonable.

Have professionals predefine defaults for common scenarios, e.g., “online shopping.”



Dictionary

Definitions from Oxford Languages · Learn more

low-risk

adjective

involving or exposed to a low level of danger.
"A low-risk customer is not very likely to be exposed to a danger."

Define Important Terms

Certain terms are open to interpretation,

- “low risk”
- “optional MFA”
- “block”

explain them in meaningful ways and give examples.

Documentation & FAQ!

Time of Access
IP Restriction
123.201.0.5
213.201.1.1
Device Restriction
Location Resiction
first.last@example.com
Accept
Deny

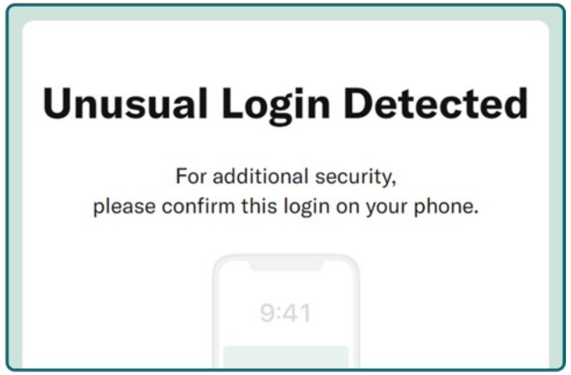
[1]

Urge to Understand

Provide descriptions of the risk levels and how many levels there are. (“no risk”)

Administrators want:

- insights into the calculation (crucial for decision).
- to better understand the implications of decisions.



Unusual Login Detected

For additional security,
please confirm this login on your phone.

9:41

Impact on Users

Offer a simulation that depicts the user’s perspective.

Enforce the use of an “audit mode.”

Lack of consensus when it comes to notification design.

[Img. 1]: miniOrange Security Software Pvt Ltd.: “What is RBA?”