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.

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Allow</th>
<th>Optional MFA</th>
<th>Require MFA</th>
<th>Block</th>
<th>Notify users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low risk</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Medium risk</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>High risk</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
</tbody>
</table>

“As soon as it’s a risk, I want to require MFA”: How Administrators Configure Risk-based Authentication

Philipp Markert, Theodor Schnitzler, Maximilian Golla, and Markus Dürmuth
Risk-based Authentication (RBA)

During the login of a user, calculate a risk based on contextual factors like the device and location.
Risk-based Authentication (RBA)

During the login of a user, calculate a risk based on contextual factors like the device and location.
Risk-based Authentication (RBA)

During the login of a user, calculate a risk based on contextual factors like the device and location.
Configuration of RBA

**Behavior**
- **Allow**
- **Optional MFA**
- **Required MFA**
- **Block**

**Notify User**
- **Notify**
- **Don’t Notify**

**Change Notification**
- **Change**
- **Don’t Change**
Research Questions

How do administrators configure RBA?

Which obstacles and misunderstandings do they encounter?

What is the impact of previous exposure to other RBA systems and how do different requirements influence administrators?
Method

Conducted with n=28 participants who work as administrators

10 participants 11–15 years of experience
9 participants >15 years of experience

"You are the system administrator of the MediaShop Corporation, where you administrate the online shop dresscode.com"
RQ1: How Do Administrators Configure RBA?

Behavior:

- ** Allow
- ? Optional MFA
- ! Required MFA
- Block

Low Risk: 9
Medium Risk: 13
High Risk: 6

“As soon as it’s a risk, I want to require MFA.”
RQ1: How Do Administrators Configure RBA?

Behavior:  
- **Allow**
- **Optional MFA**
- **Required MFA**
- **Block**

**Low Risk**
- Allow: 9
- Optional MFA: 13
- Required MFA: 6

**Medium Risk**
- Allow: 25
- Optional MFA: 3

**High Risk**
- Allow: 1
- Optional MFA: 17
- Required MFA: 10

"It is dresscode.com, had it been my bank, maybe block would be more prudent."

"As soon as it's a risk, I want to require MFA": How Administrators Configure Risk-based Authentication
Philipp Markert, Theodor Schnitzler, Maximilian Golla, and Markus Dürmuth
### RQ1: How Do Administrators Configure RBA?

<table>
<thead>
<tr>
<th>Behavior:</th>
<th>Allow</th>
<th>Optional MFA</th>
<th>Required MFA</th>
<th>Block</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification:</td>
<td>Notify</td>
<td>Do Not Notify</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low Risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Allow:** 9
- **Optional MFA:** 13
- **Required MFA:** 6
- **Block:** 21

- **Total:** 71

| Medium Risk | | | | |

- **Allow:** 25
- **Optional MFA:** 3
- **Required MFA:** 3
- **Block:** 25

- **Total:** 88

| High Risk | | | | |

- **Allow:** 1
- **Optional MFA:** 17
- **Required MFA:** 10
- **Block:**

- **Total:** 19

"If you get bombarded with login notifications, you get annoyed."

"As soon as it's a risk, I want to require MFA": How Administrators Configure Risk-based Authentication
Philipp Markert, Theodor Schnitzler, Maximilian Golla, and Markus Dürmuth
RQ1: How Do Administrators Configure RBA?

<table>
<thead>
<tr>
<th>Behavior:</th>
<th>Allow</th>
<th>Optional MFA</th>
<th>Required MFA</th>
<th>Block</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification:</td>
<td>Notify</td>
<td>Do Not Notify</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Low Risk:
- Allow: 9
- Optional MFA: 13
- Required MFA: 6
- Block: 21
- Notify: 7

Medium Risk:
- Allow: 25
- Optional MFA: 3
- Required MFA: 2
- Block: 26
- Notify: 2

High Risk:
- Allow: 1
- Optional MFA: 17
- Required MFA: 10
- Block: 27
- Notify: 1
RQ2: Which Obstacles and Misunderstandings Do Administrators Encounter?

Understanding Of Risk Level Calculation

“If I don't know exactly what ‘low’, ‘medium’, or ‘high risk’ means, then there is no reason for me to distinguish between them.”

Consequence: User Burdening

“If I don't know exactly what ‘low’, ‘medium’, or ‘high risk’ means, then there is no reason for me to distinguish between them.”

Consequence: Reduced Sales

Understanding Of Crucial Terms

Optional MFA

“For users it's convenient to just skip it.”

Block

“How long will the block last for? Is this an indefinite block? Is this just a slowdown of the login attempts?”

Awareness About All Risk Levels

- High Risk
- Medium Risk
- Low Risk
- No Risk

Consequence: User Burdening

“If I don't know exactly what ‘low’, ‘medium’, or ‘high risk’ means, then there is no reason for me to distinguish between them.”

Consequence: Reduced Sales

Philipp Markert, Theodor Schnitzler, Maximilian Golla, and Markus Dürmuth
"As soon as it’s a risk, I want to require MFA": How Administrators Configure Risk-based Authentication

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

Risk-based Authentication

Risk Levels

Behavior

Notify User

Method

Risk Levels

Optional MFA

Block

Findings

Spicing up Defaults

Clarity About the System

Understanding of Crucial Terms

“what classifies ‘low’, ‘medium’, and ‘high’”

n=28 administrators

19 participants with >10 years of experience

“you’re responsible for the web shop dresscode.com”