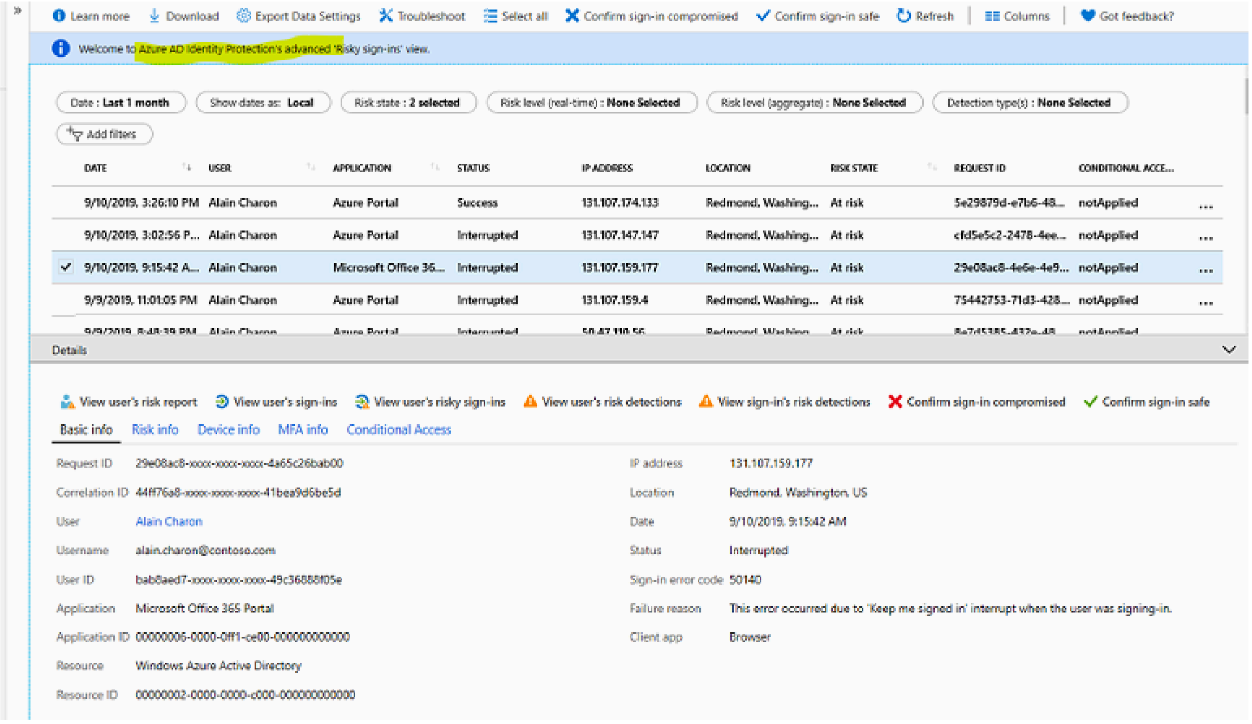
Microsoft Defender for Identity

By: Ryan Stewart



Welcome to Azure AD Identity Protection's advanced 'Risky sign-ins' view.

Date : **Last 1 month** | Show dates as: **Local** | Risk state : **2 selected** | Risk level (real-time) : **None Selected** | Risk level (aggregate) : **None Selected** | Detection type(s) : **None Selected**

	DATE	USER	APPLICATION	STATUS	IP ADDRESS	LOCATION	RISK STATE	REQUEST ID	CONDITIONAL ACCE...	
	9/10/2019, 3:26:10 PM	Alain Charon	Azure Portal	Success	131.107.174.133	Redmond, Washing...	At risk	5e29879d-e7b6-48...	notApplied	...
	9/10/2019, 3:02:56 P...	Alain Charon	Azure Portal	Interrupted	131.107.147.147	Redmond, Washing...	At risk	cfd5e5c2-2478-4ee...	notApplied	...
✓	9/10/2019, 9:15:42 A...	Alain Charon	Microsoft Office 36...	Interrupted	131.107.159.177	Redmond, Washing...	At risk	29e08ac8-4e6e-4e9...	notApplied	...
	9/9/2019, 11:01:05 PM	Alain Charon	Azure Portal	Interrupted	131.107.159.4	Redmond, Washing...	At risk	75442753-71d3-428...	notApplied	...
	9/9/2019, 8:48:39 PM	Alain Charon	Azure Portal	Interrupted	50.47.110.56	Redmond, Washing...	At risk	8e7d5385-437e-48	notApplied	

Request ID	29e08ac8-xxxx-xxxx-xxxx-4a65c26bab00	IP address	131.107.159.177
Correlation ID	44ff76a8-xxxx-xxxx-xxxx-41bea9d6be5d	Location	Redmond, Washington, US
User	Alain Charon	Date	9/10/2019, 9:15:42 AM
Username	alain.charon@contoso.com	Status	Interrupted
User ID	bab8aed7-xxxx-xxxx-xxxx-49c36888f05e	Sign-in error code	50140
Application	Microsoft Office 365 Portal	Failure reason	This error occurred due to 'Keep me signed in' interrupt when the user was signing-in.
Application ID	00000006-0000-0ff1-ce00-000000000000	Client app	Browser
Resource	Windows Azure Active Directory		
Resource ID	00000002-0000-0000-c000-000000000000		

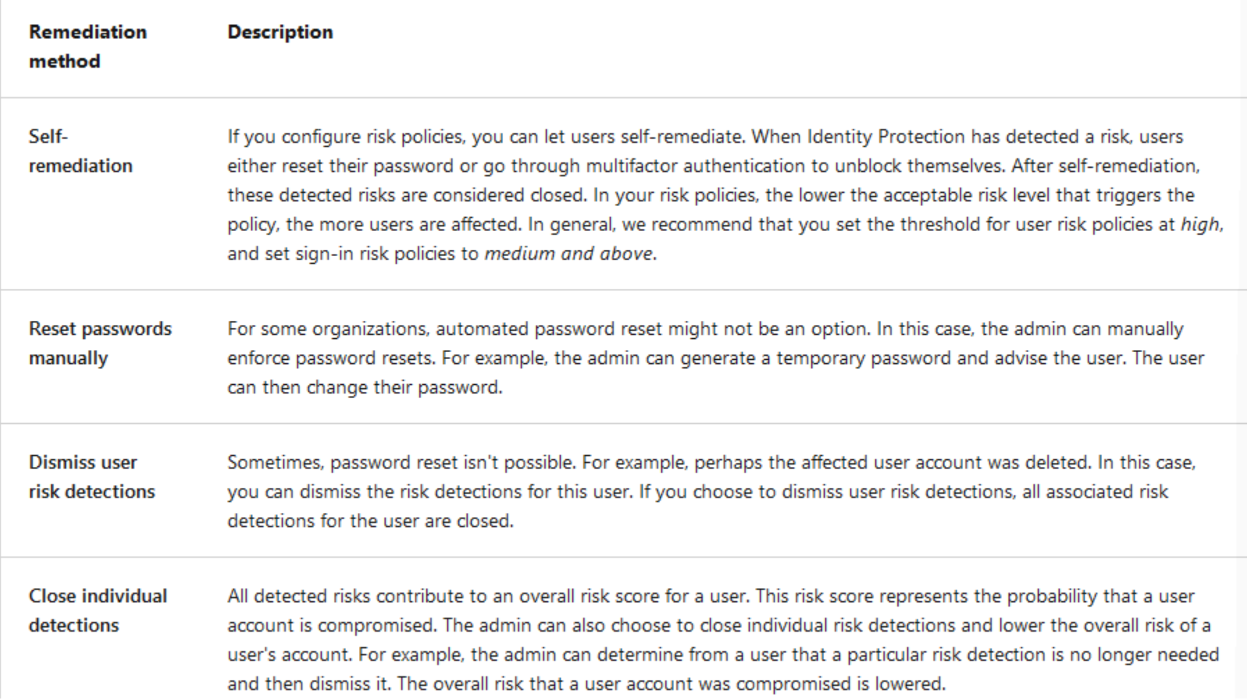
Investigate risks

Report	Information included	Actions the admin can take	Period covered
Risky sign-ins	Location details, device details, sign-ins confirmed as safe, or with dismissed or remediated risks.	Confirm that sign-ins are safe or confirm that they're compromised.	Last 30 days
Risky users	Lists of users at risk and users with dismissed or remediated risks. User history of risky sign-ins.	Reset user passwords, dismiss user risk, block user sign-ins, and confirm user accounts as compromised.	Not applicable

Remediate risks

When your investigation is complete, you want to remediate the risks if you're not already using risk policies to automatically deal with them. Always address detected risks quickly.

There are different ways to remediate risks. The methods you use depend on your organization's needs.



Remediation method	Description
Self-remediation	If you configure risk policies, you can let users self-remediate. When Identity Protection has detected a risk, users either reset their password or go through multifactor authentication to unblock themselves. After self-remediation, these detected risks are considered closed. In your risk policies, the lower the acceptable risk level that triggers the policy, the more users are affected. In general, we recommend that you set the threshold for user risk policies at *high*, and set sign-in risk policies to *medium and above*.
Reset passwords manually	For some organizations, automated password reset might not be an option. In this case, the admin can manually enforce password resets. For example, the admin can generate a temporary password and advise the user. The user can then change their password.
Dismiss user risk detections	Sometimes, password reset isn't possible. For example, perhaps the affected user account was deleted. In this case, you can dismiss the risk detections for this user. If you choose to dismiss user risk detections, all associated risk detections for the user are closed.
Close individual detections	All detected risks contribute to an overall risk score for a user. This risk score represents the probability that a user account is compromised. The admin can also choose to close individual risk detections and lower the overall risk of a user's account. For example, the admin can determine from a user that a particular risk detection is no longer needed and then dismiss it. The overall risk that a user account was compromised is lowered.

Summary

You were asked to prevent your company's identities from being compromised again and to ensure that identities are protected in the future. This problem is common for retail companies such as yours, which must guard their reputation for trustworthiness and conform with data protection legislation.

You used **Microsoft Entra ID** Protection to protect your organization's identities by detecting, investigating, and remediating risks.

Without Identity Protection, your organization's identities wouldn't be protected and could have been compromised again. Your company can now use Identity Protection to protect its identities and help prevent negative reputation and financial loss.