

Risky sign-ins report in the Azure Active Directory portal

To view contributors to this article access the link below

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risky-sign-ins>

In this article

1. [Who can access the risky sign-ins report?](#)
2. [What Azure AD license do you need to access a security report?](#)
3. [Risky sign-ins report for Azure AD free edition](#)
4. [Risky sign-ins report for Azure AD premium editions](#)

Azure Active Directory (Azure AD) detects suspicious actions that are related to your user accounts. For each detected action, a record called a **risk detection** is created. For more details, see [Azure AD risk detections](#).

You can access the security reports from the [Azure portal](#) by selecting the **Azure Active Directory** blade and then navigating to the **Security** section.

There are two different security reports that are calculated based on the risk detections:

- **Risky sign-ins** - A risky sign-in is an indicator for a sign-in attempt that might have been performed by someone who is not the legitimate owner of a user account.
- **Users flagged for risk** - A risky user is an indicator for a user account that might have been compromised.



To learn how to configure the policies that trigger these risk detections, see [How to configure the user risk policy](#).

Who can access the risky sign-ins report?

The risky sign-ins reports are available to users in the following roles:

- Security Administrator

- Global Administrator
- Security Reader

To learn how to assign administrative roles to a user in Azure Active Directory, see [View and assign administrator roles in Azure Active Directory](#).

What Azure AD license do you need to access a security report?






All editions of Azure AD provide you with risky sign-ins reports. However, the level of report granularity varies between the editions:

- In the **Azure Active Directory Free edition**, you get a list of risky sign-ins.
- In addition, the **Azure Active Directory Premium 1** edition allows you to examine some of the underlying risk detections that have been detected for each report.
- The **Azure Active Directory Premium 2** edition provides you with the most detailed information about all underlying risk detections and it also enables you to configure security policies that automatically respond to configured risk levels.

Risky sign-ins report for Azure AD free edition






The Azure AD free edition provide you with a list of risky sign-ins that have been detected for your users. Each record contains the following attributes:

- **User** - The name of the user that was used during the sign-in operation.
- **IP** - The IP address of the device that was used to connect to Azure Active Directory.
- **Location** - The location used to connect to Azure Active Directory. This is a best effort approximation based on traces, registry data, reverse look ups and other information.
- **Sign-in time** - The time when the sign-in was performed
- **Status** - The status of the sign-in

	USER	IP	LOCATION	SIGN-IN TIME (UTC)	STATUS
	John Nash	193.90.12.87	Oslo, Oslo, NO	11/21/2016 01:03	Active
	John Nash	193.90.12.87	Oslo, Oslo, NO	11/20/2016 01:04	Active
	John Nash	193.90.12.87	Oslo, Oslo, NO	11/19/2016 01:04	Active
	John Nash			11/19/2016 01:03	Active
	John Nash			11/18/2016 01:03	Active

Based on your investigation of the risky sign-in, you can provide feedback to Azure AD by taking the following actions:

- Resolve
- Mark as false positive
- Ignore
- Reactivate


	USER	IP	LOCATION	SIGN-IN TIME (UTC)	STATUS
	John Nash			11/23/2016 01:02	Active
	John Nash	193.90.12.87	Oslo, Oslo, NO	11/23/2016 00:51	Active
	John Nash			11/22/2016 01:01	Active
	John Nash	193.90.12.87	Oslo, Oslo, NO	11/22/2016 00:57	Active
	John Nash	193.90.12.87	Oslo, Oslo, NO	11/21/2016 01:03	Active

This report also provides you with an option to:


- Search resources
- Download the report data


Microsoft Azure


rlfreetesttenant - Risky sign-ins




rlfreetesttenant - Risky sign-ins
Azure Active Directory



 Azure AD Connect





Risky sign-ins report for Azure AD premium editions

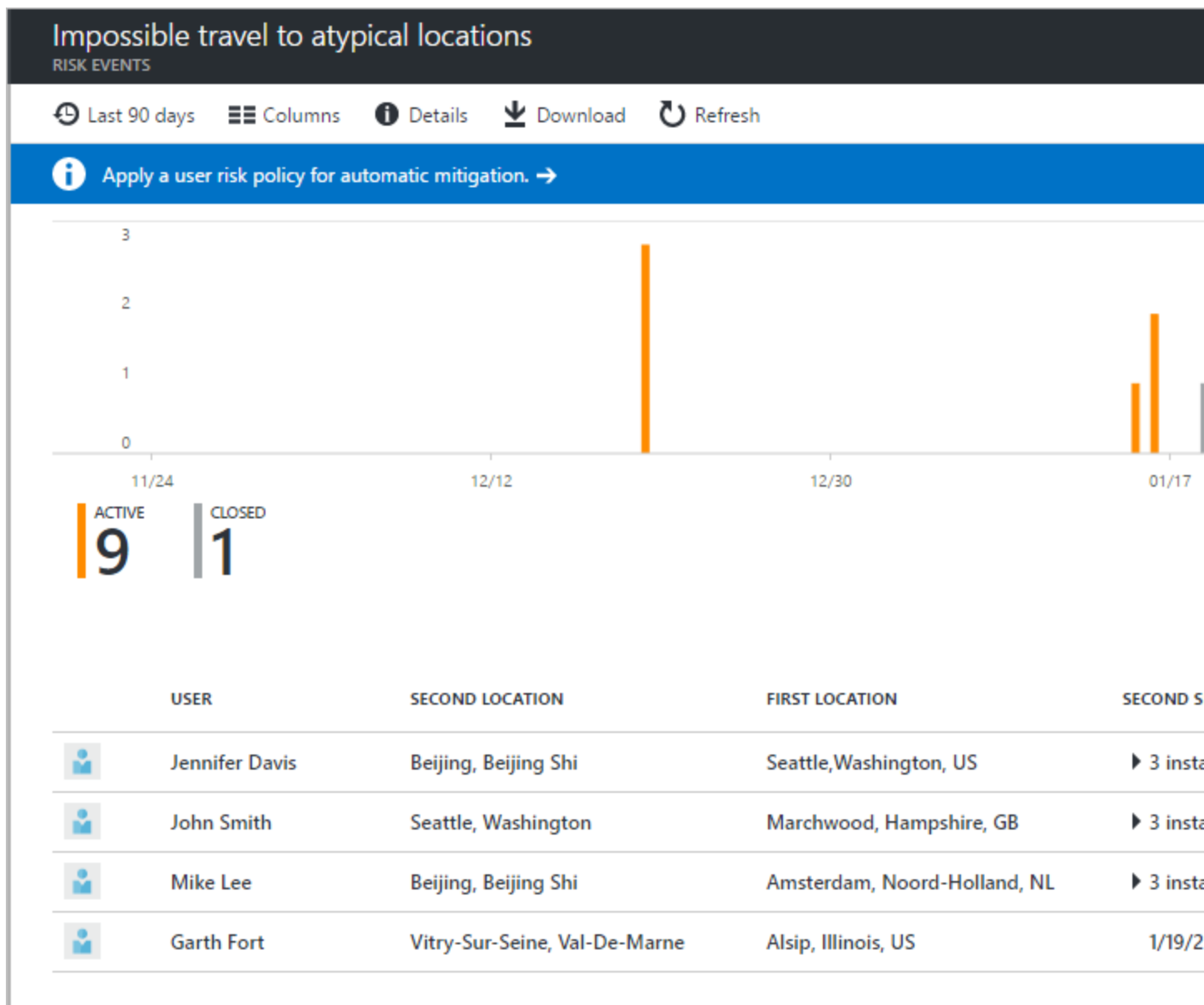
The risky sign-ins report in the Azure AD premium editions provides you with:

- Aggregated information about the [risk detection types](#) that have been detected. With the **Azure AD Premium P1 edition**, detections that are not covered by your license appear as the risk detection **Sign-in with additional risk detected**. With the **Azure AD Premium P2 edition**, you get the most detailed information about all underlying detections.
- An option to download the report

Contoso Cloud - Risky Sign-ins		
Azure Active Directory		
<div> <input type="text" value="Search (Ctrl+)/"/> </div> <div> <div>MANAGE</div> <div> <div>Users and groups</div> <div>Enterprise applications</div> <div>App registrations</div> <div>Application Proxy</div> <div>Azure AD Connect</div> <div>Domain names</div> </div> </div>		
<div> <div>Last 90 days</div> <div>Download</div> <div>Refresh</div> </div>		
RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE
High	Offline	Users with leaked credentials ⓘ
Medium	Real-time	Sign-ins from anonymous IP addresses ⓘ
Medium	Offline	Impossible travels to atypical locations ⓘ
Medium	Real-time	Sign-ins from unfamiliar locations ⓘ
Low	Offline	Sign-ins from infected devices ⓘ

When you select a risk detection, you get a detailed report view for this risk detection that enables you to:

- An option to configure a [user risk remediation policy](#)
- Review the detection timeline for the risk detection
- Review a list of users for which this risk detection has been detected
- Manually close risk detections.



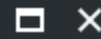
Important

Sometimes, you may find a risk detection without a corresponding sign-in entry in the [sign-ins report](#). This is because Identity Protection evaluates risk for both **interactive** and **non-interactive** sign-ins, whereas the sign-ins report shows only the interactive sign-ins.

When you select a user, you get a detailed report view for this user that enables you to:

- Open the All sign-ins view
- Reset the user's password
- Dismiss all events
- Investigate reported risk detections for the user.

Jennifer Davis



All sign-ins Reset password Dismiss all events

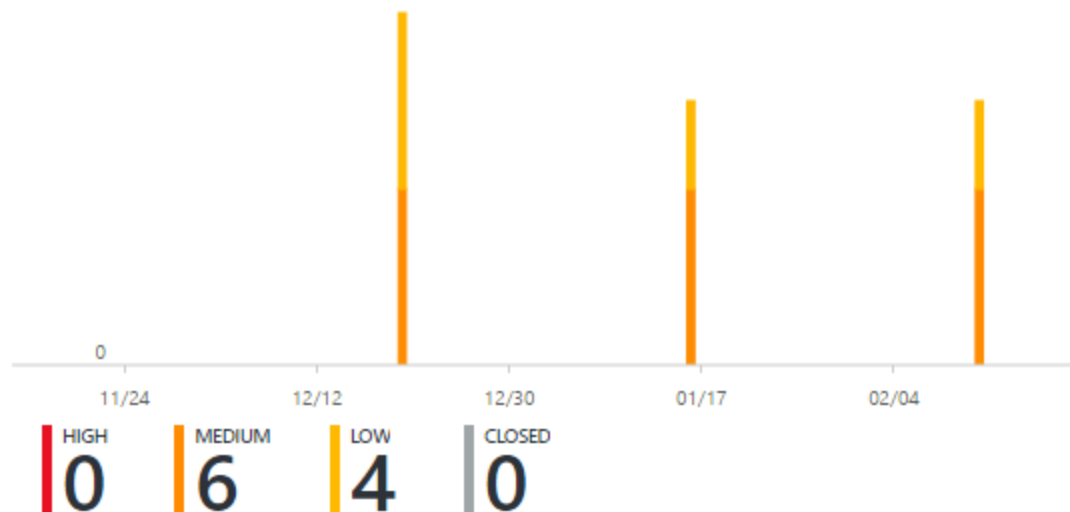
User has a high risk level

Essentials ^

Risk level	Status
High	At risk
Role	Contact
User	JenDavis@contosobuild.com
Location	MFA registered
N/A	No
Department	Object Id
N/A	c0de123c-ee1e-4c5a-b115-e11cf66aba92

Risk events

5



TIME (UTC)	IP ADDRESS	RISK EVENT TYPE	RISK LEVEL
2/12/2017 5:26 ...	77.109.41.30	Sign-in from anonymous IP address	Medium
2/12/2017 1:02 ...	125.37.113.28	Impossible travel to atypical location	Medium
2/12/2017 12:38...	81.25.53.98	Sign-in from infected device	Low
1/16/2017 5:15 A..	77.109.41.30	Sign-in from anonymous IP address	Medium

To investigate a risk detection, select one from the list.

This opens the **Details** blade for this risk detection. On the **Details** blade, you have the option to either manually close a risk detection or reactivate a manually closed risk detection.

Details

JENNIFER DAVIS

✓ Resolve

✓ Mark as false positive

✓ Ignore

↶ Reactivate

DESCRIPTION

Sign-ins from IP addresses that are anonymous, such as Tor IP addresses.

SECURITY IMPACT

This risk event may indicate that an attacker has compromised the user's credential and is exploiting it through an anonymous IP address.

IP

77.109.41.30

LOCATION

Kyiv, Kyiv Misto, UA

SIGN-IN TIME (UTC)

2/12/2017 5:26 AM

STATUS

Active