Azure AD Premium

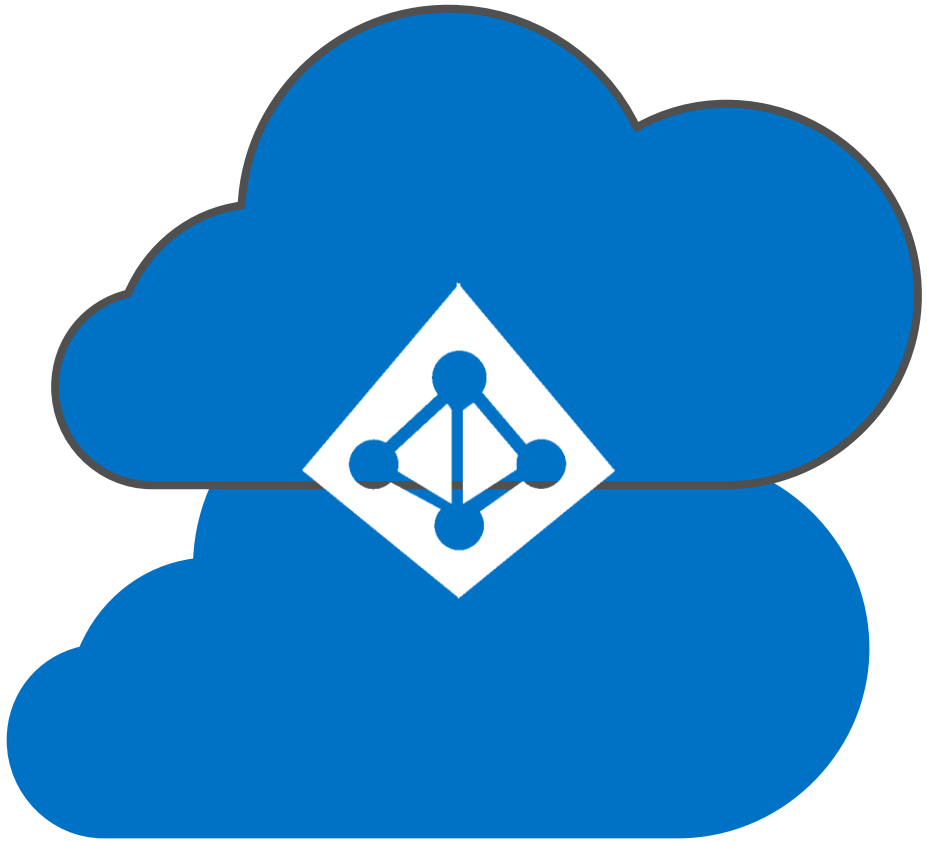
@directorcia

http://about.me/ciaops

Directory Comparison

Property	On premises	Azure
User identity and security	✓	✓
Windows 7 machine join	✓	✗
Windows 8 machine join	✓	✗
Windows 10 machine join	✓	✓
Group Policy	✓	✗
LDAP	✓	✗
DNS	✓	✗
Certificate server	✓	✗
Organisational units	✓	✗
Kerberos	✓	✗
Mobile device joins	✗	✓
Office 365 join	✗	✓

What is Azure Active Directory?



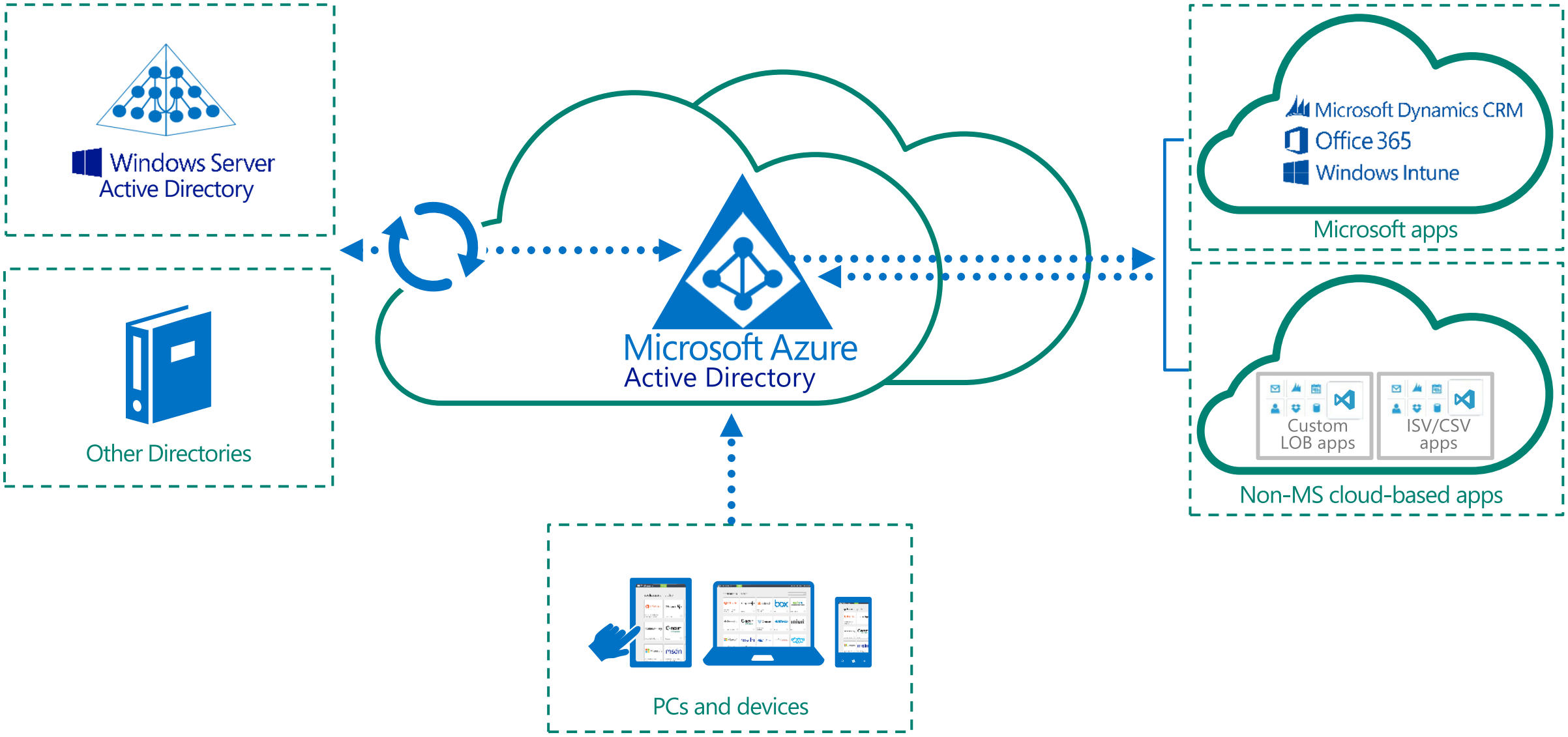
A comprehensive identity and access management cloud solution.

It combines directory services, advanced identity governance, application access management and a rich standards-based platform for developers.

Versions:

- Free
- Basic
- Premium

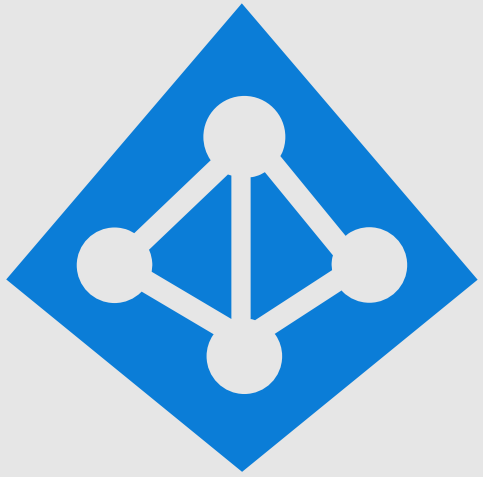
Azure AD as the control point



Azure Active Directory editions feature comparison + Office 365 IAM features

		Azure Active Directory Free	Azure Active Directory Basic	Azure Active Directory Premium	Office 365 apps only
Common Features	Directory as a Service	500,000 Object Limit	No Object Limit	No Object Limit	No Object limit for Office 365 user accounts
	User/Group Management (add/update/delete)	Yes	Yes	Yes	Yes
	SSO to pre-integrated SAAS Applications /Custom Apps	10 apps per user	10 apps per user	No Limit	10 apps per user
	User-Based access management/provisioning	Yes	Yes	Yes	Yes
	Self-Service Password Change for cloud users	Yes	Yes	Yes	Yes
	Connect (Sync engine that extends on-premises directories to Azure Active Directory)	Yes	Yes	Yes	Yes
	Security Reports/Audit	3 Basic Reports	3 Basic Reports	Advanced Security Reports	3 Basic Reports
Premium + Basic Features	Group-based access management/provisioning		Yes	Yes	
	Self-Service Password Reset for cloud users		Yes	Yes	Yes
	Company Branding (Logon Pages/Access Panel customization)		Yes	Yes	Yes
	Application Proxy		Yes	Yes	
	SLA		Yes	Yes	Yes
Premium Features	Self-Service Group Management			Yes	
	Self-Service Password Reset/Change with on-premises write-back			Yes	
	Advanced Usage Reporting			Yes	
	Multi-Factor Authentication (Cloud and On-premises (MFA Server))			Yes	Limited cloud only for Office 365 Apps
	MIM CAL + MIM Server			Yes	
	Administrative Units (in Preview)			Yes	
	Enterprise State Roaming			Yes	
	Conditional Access : MFA per application (in Preview)			Yes	
	Automated password roll-over (in Preview)			Yes	
	Connect health			Yes	

https://azure.microsoft.com/en-au/pricing/details/active-directory/



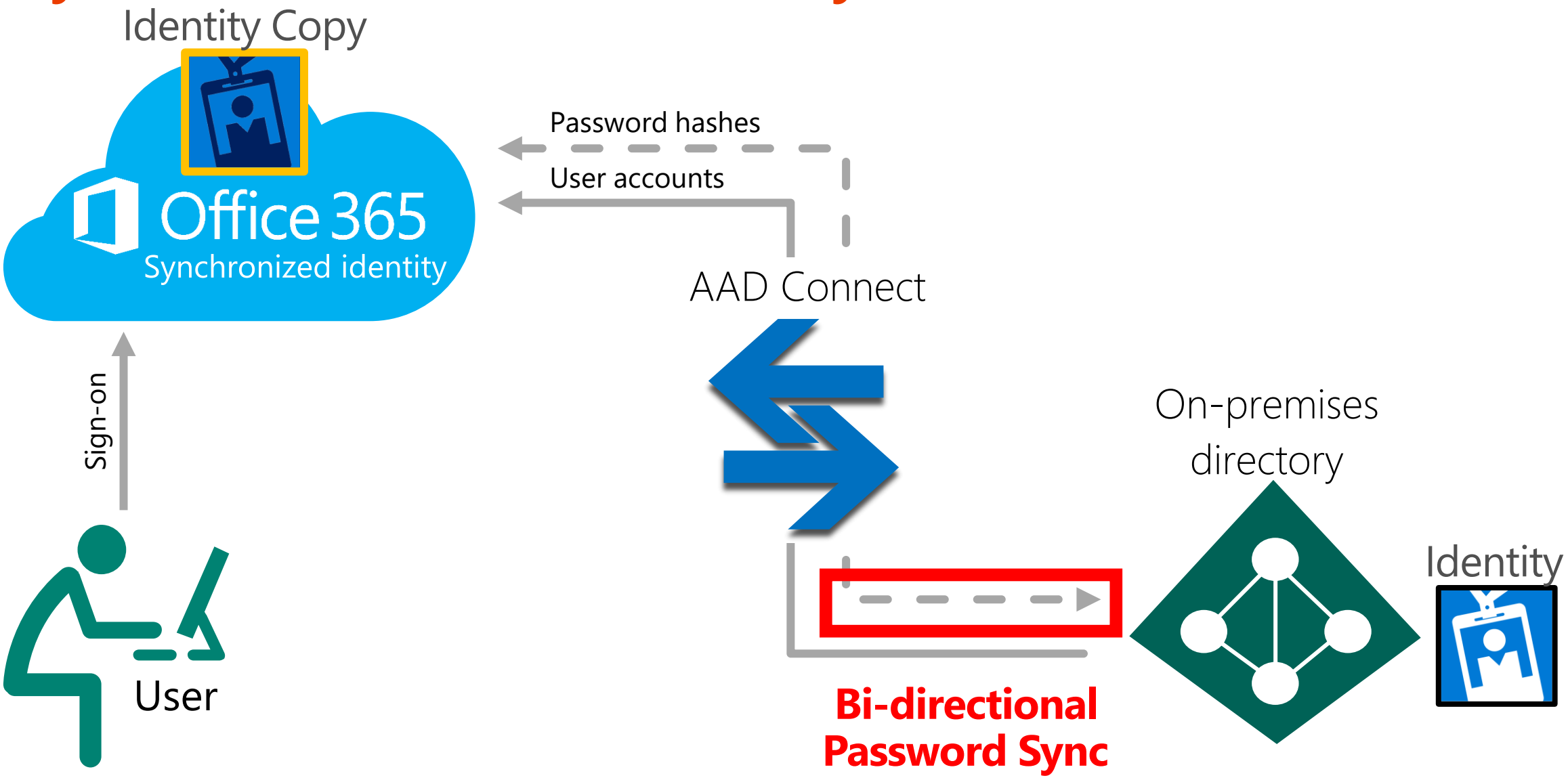
Azure Active Directory

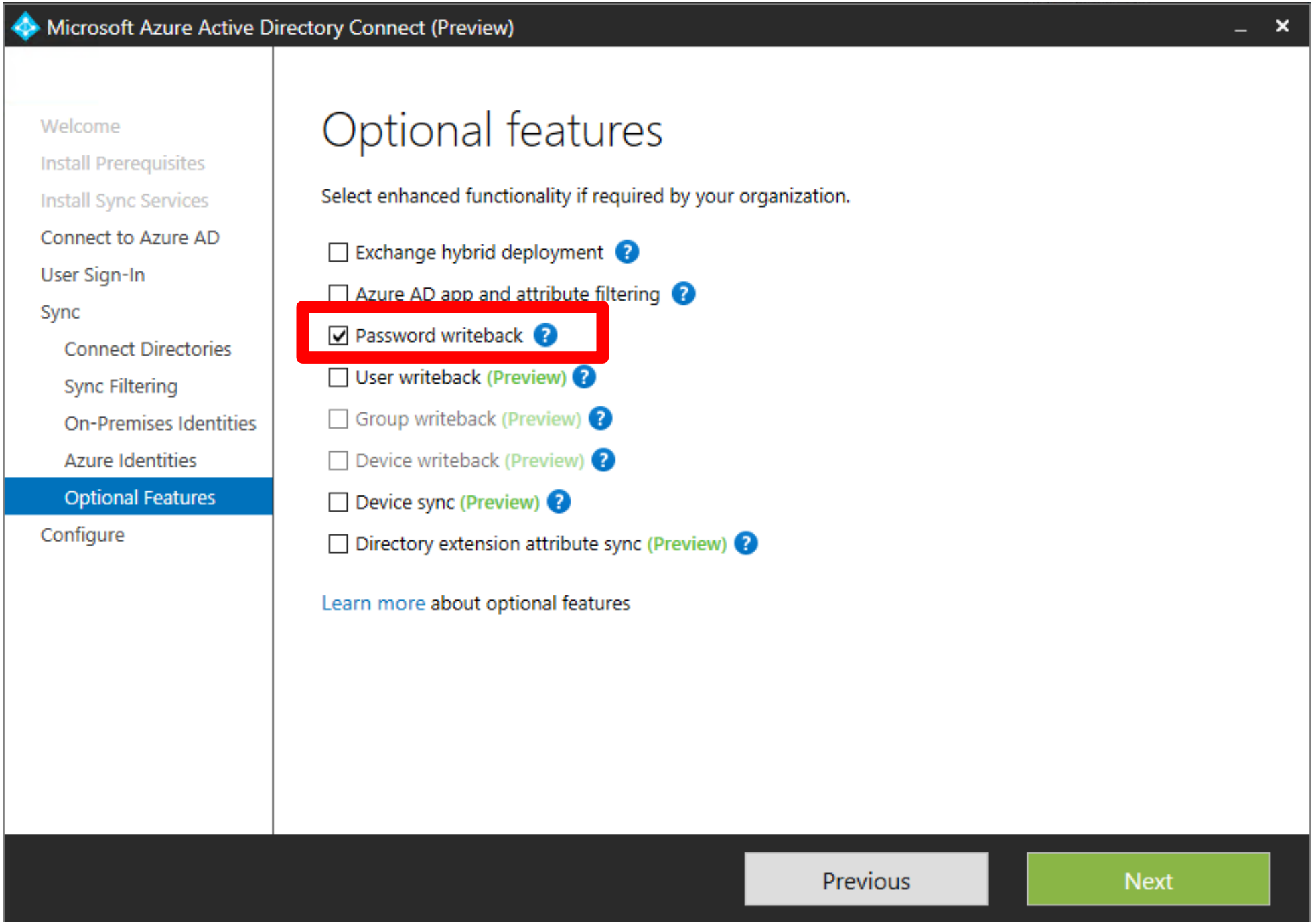
- Azure AD Connect
- B2B collaboration
- Provisioning-Deprovisioning
- Conditional Access
- SSO to SaaS
- Self-Service capabilities
- Connect Health
- Multi-Factor Authentication
- Addition of custom cloud apps
- Access Panel/MyApps
- Dynamic Groups
- Identity Protection
- Remote Access to on-premises apps
- Azure AD B2C
- Group-Based Licensing
- Privileged Identity Management
- Microsoft Authenticator - Password-less Access
- Azure AD Join
- MDM-auto enrollment / Enterprise State Roaming
- Security Reporting
- Azure AD DS
- Office 365 App Launcher
- HR App Integration
- Access Reviews

Azure AD P1 Features

Password Write Back

Synchronized Identity with Writeback

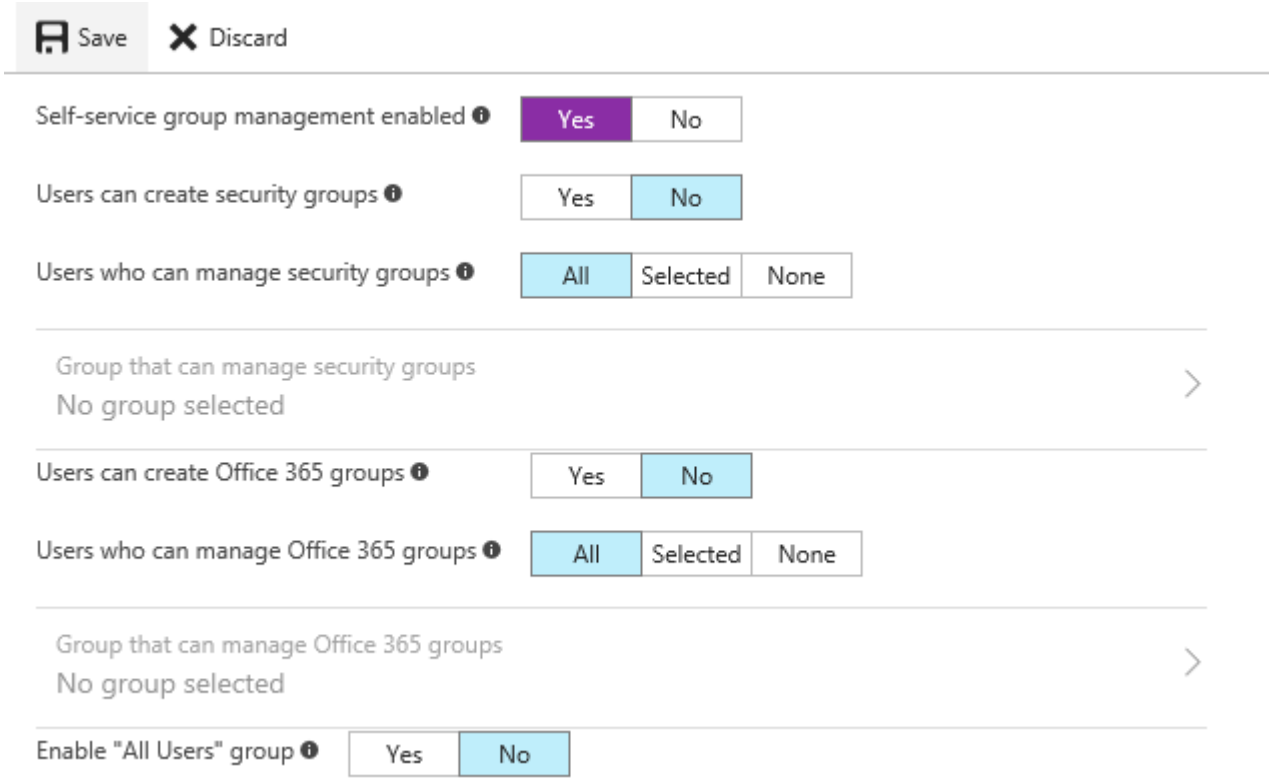



Microsoft Azure Active Directory Connect (Preview)
Welcome
Install Prerequisites
Install Sync Services
Connect to Azure AD
User Sign-In
Sync
Connect Directories
Sync Filtering
On-Premises Identities
Azure Identities
Optional Features
Configure
Optional features
Select enhanced functionality if required by your organization.
Exchange hybrid deployment
Azure AD app and attribute filtering
Password writeback
User writeback (Preview)
Group writeback (Preview)
Device writeback (Preview)
Device sync (Preview)
Directory extension attribute sync (Preview)
Learn more about optional features
Previous
Next

Group Management

Group Management: Configuration

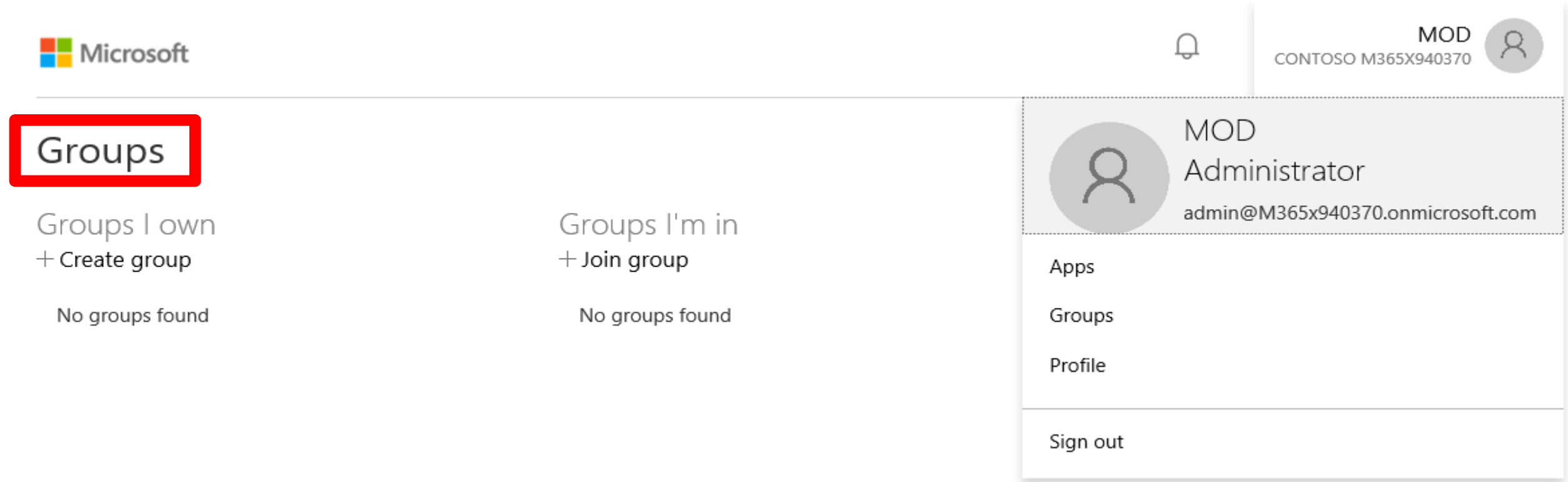
Azure Portal configuration



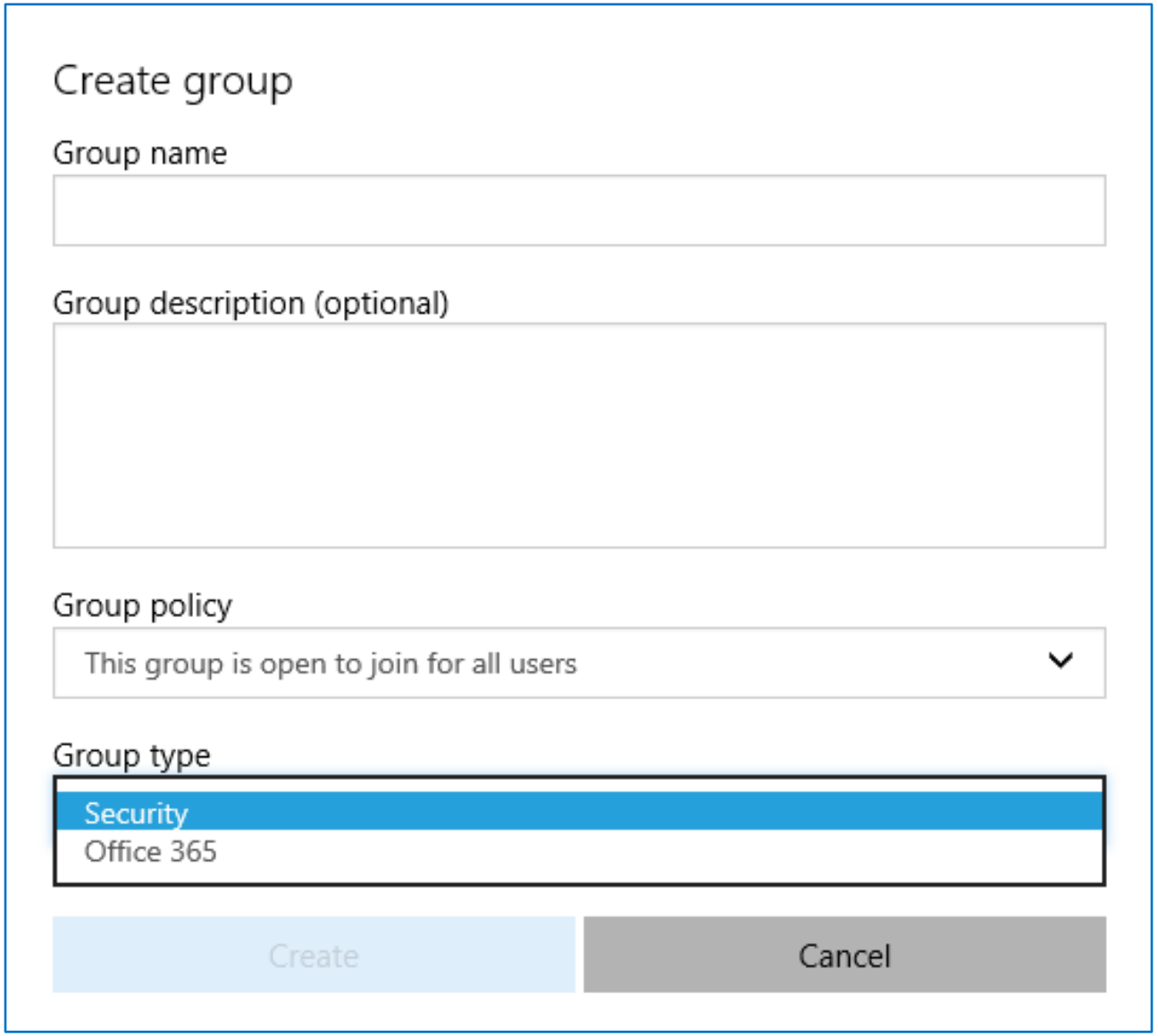
Admins can…

- Allow users to join existing groups, but not create
- Allow users to create their own groups
- Restrict feature availability to a specific group
- Report on group activity

Group Management



Group Management



Application Proxy

Remote Access as a Service

Easy to deploy and operate: minimal on-prem footprint

Secure remote access to business applications with zero DMZ on-prem infrastructure deployment and no network infrastructure change.

More secure to the business: pre-DMZ protection

All security verifications are outside of the organization premises done in cloud scale.

DDoS attacks will not influence your business.

Deep integration with Azure Active Directory

Richness of AAD capabilities and experiences: web access panel discovery and SSO, manage apps across SaaS and on-prem, machine learning traffic analysis, multifactor authentication, device registration, cloud ADFS proxy deployment.

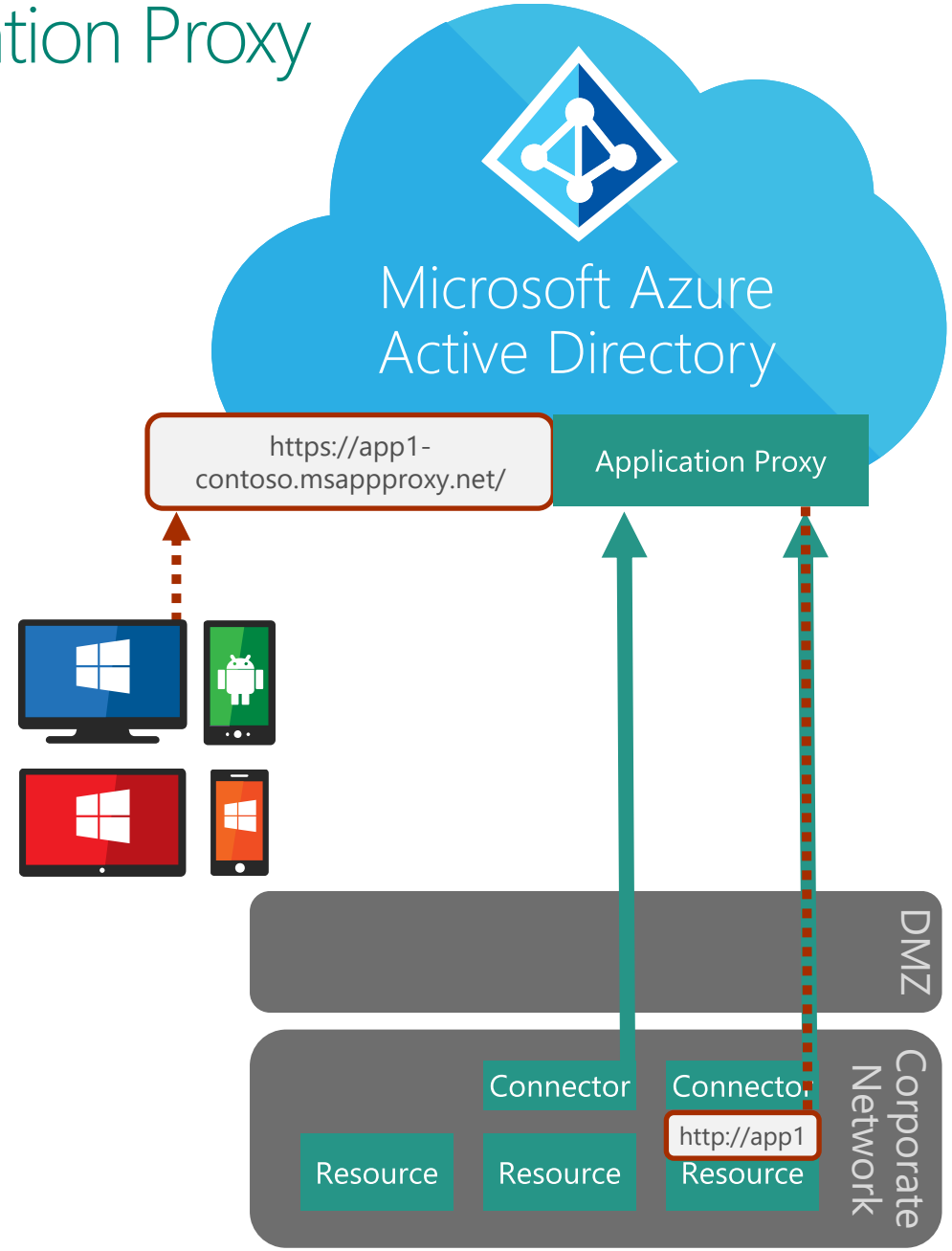
Azure Active Directory Application Proxy

A connector that auto connects to the cloud service

Multiple connectors can be deployed for redundancy, scale, multiple sites and different resources

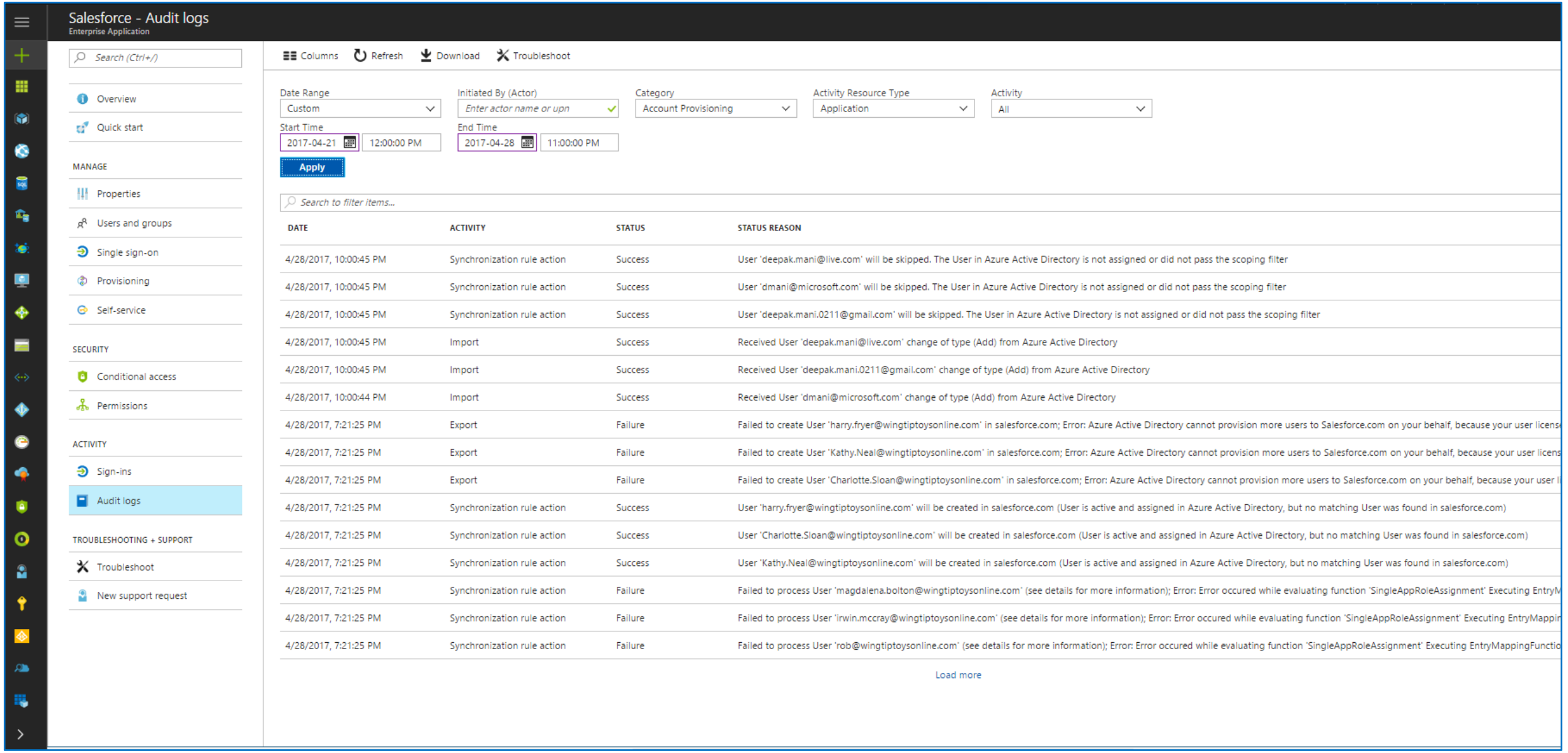
Connectors are deployed usually on the local network next to resources

Users connect to the cloud service that routes their traffic to the resources via the connectors

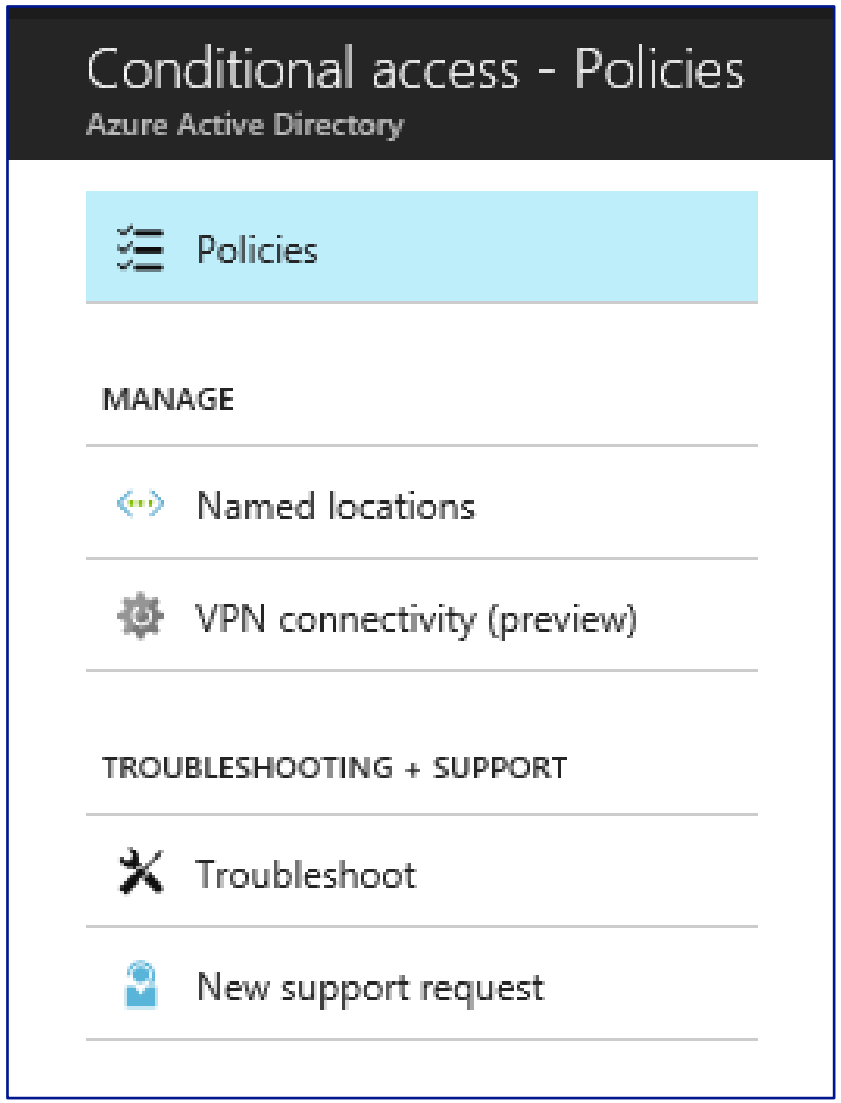


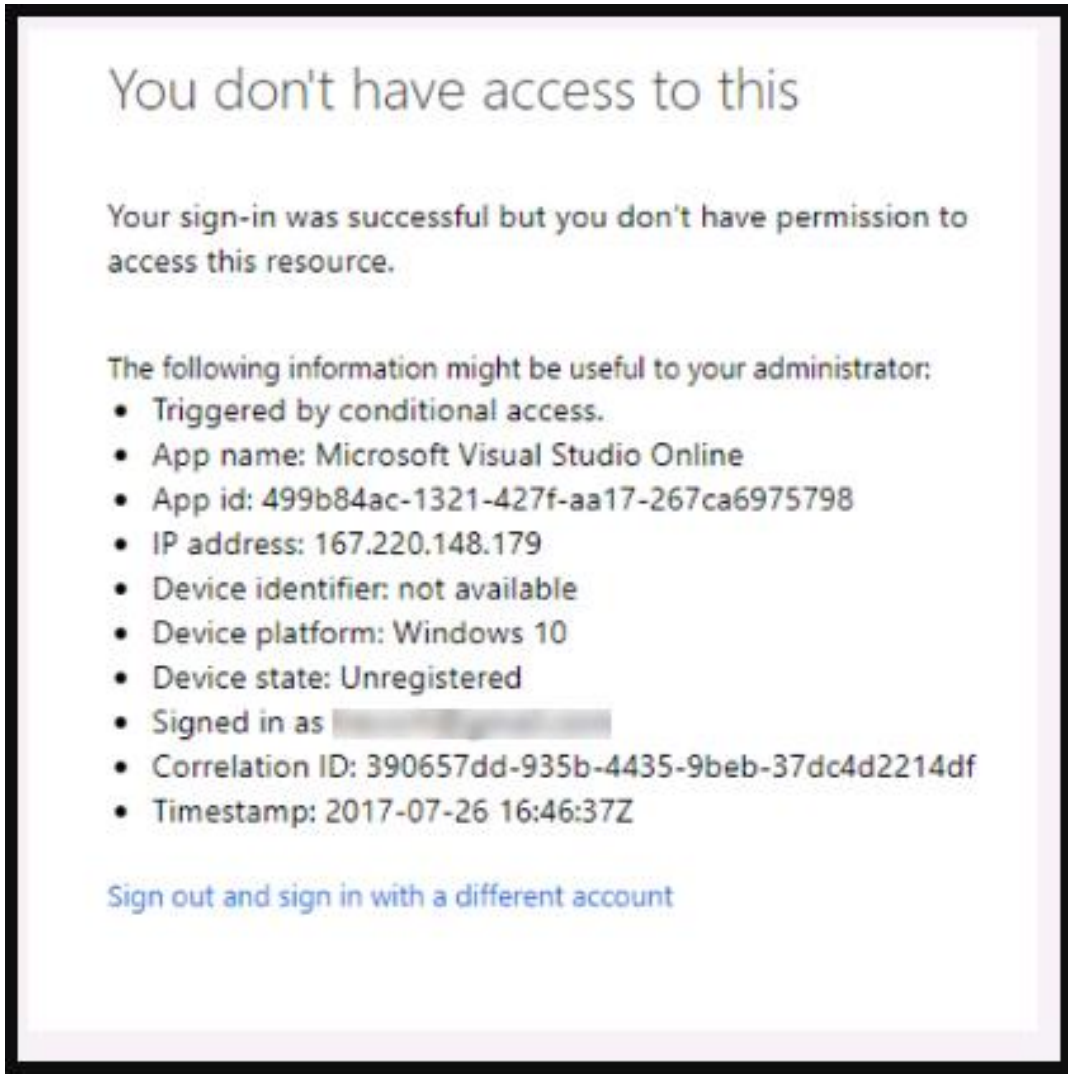
Advanced Reporting

Reports

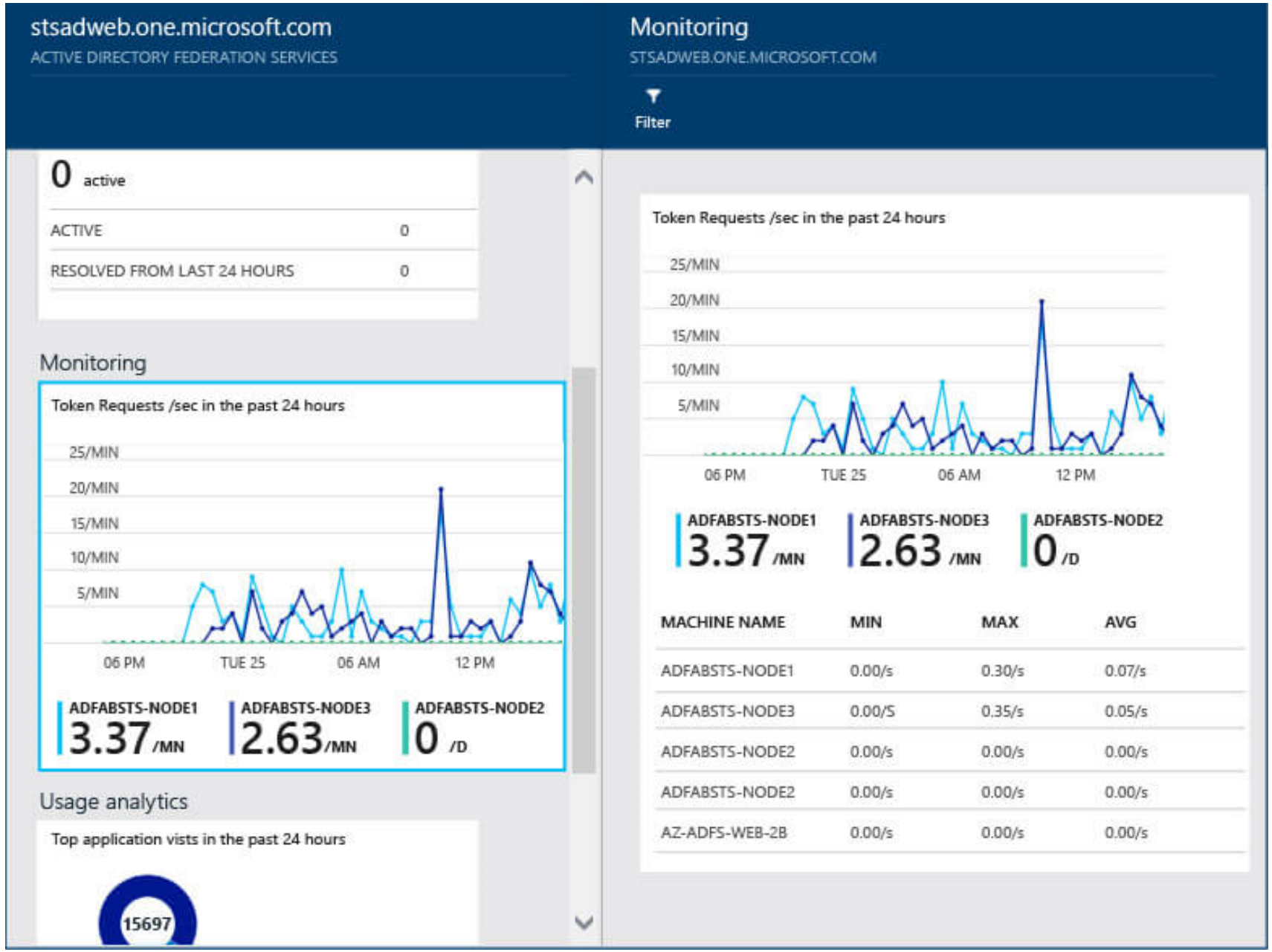

Salesforce - Audit logs
Enterprise Application
Search (Ctrl+/)
Overview
Quick start
MANAGE
Properties
Users and groups
Single sign-on
Provisioning
Self-service
SECURITY
Conditional access
Permissions
ACTIVITY
Sign-ins
Audit logs
TROUBLESHOOTING + SUPPORT
Troubleshoot
New support request
Columns
Refresh
Download
Troubleshoot
Date Range
Custom
Initiated By (Actor)
Enter actor name or upn
Category
Account Provisioning
Activity Resource Type
Application
Activity
All
Start Time
2017-04-21
12:00:00 PM
End Time
2017-04-28
11:00:00 PM
Apply
Search to filter items...
DATE
ACTIVITY
STATUS
STATUS REASON
4/28/2017, 10:00:45 PM
Synchronization rule action
Success
User 'deepak.mani@live.com' will be skipped. The User in Azure Active Directory is not assigned or did not pass the scoping filter
4/28/2017, 10:00:45 PM
Synchronization rule action
Success
User 'dmani@microsoft.com' will be skipped. The User in Azure Active Directory is not assigned or did not pass the scoping filter
4/28/2017, 10:00:45 PM
Synchronization rule action
Success
User 'deepak.mani.0211@gmail.com' will be skipped. The User in Azure Active Directory is not assigned or did not pass the scoping filter
4/28/2017, 10:00:45 PM
Import
Success
Received User 'deepak.mani@live.com' change of type (Add) from Azure Active Directory
4/28/2017, 10:00:45 PM
Import
Success
Received User 'deepak.mani.0211@gmail.com' change of type (Add) from Azure Active Directory
4/28/2017, 10:00:44 PM
Import
Success
Received User 'dmani@microsoft.com' change of type (Add) from Azure Active Directory
4/28/2017, 7:21:25 PM
Export
Failure
Failed to create User 'harry.fryer@wingtiptoysonline.com' in salesforce.com; Error: Azure Active Directory cannot provision more users to Salesforce.com on your behalf, because your user licens
4/28/2017, 7:21:25 PM
Export
Failure
Failed to create User 'Kathy.Neal@wingtiptoysonline.com' in salesforce.com; Error: Azure Active Directory cannot provision more users to Salesforce.com on your behalf, because your user licens
4/28/2017, 7:21:25 PM
Export
Failure
Failed to create User 'Charlotte.Sloan@wingtiptoysonline.com' in salesforce.com; Error: Azure Active Directory cannot provision more users to Salesforce.com on your behalf, because your user l
4/28/2017, 7:21:25 PM
Synchronization rule action
Success
User 'harry.fryer@wingtiptoysonline.com' will be created in salesforce.com (User is active and assigned in Azure Active Directory, but no matching User was found in salesforce.com)
4/28/2017, 7:21:25 PM
Synchronization rule action
Success
User 'Charlotte.Sloan@wingtiptoysonline.com' will be created in salesforce.com (User is active and assigned in Azure Active Directory, but no matching User was found in salesforce.com)
4/28/2017, 7:21:25 PM
Synchronization rule action
Success
User 'Kathy.Neal@wingtiptoysonline.com' will be created in salesforce.com (User is active and assigned in Azure Active Directory, but no matching User was found in salesforce.com)
4/28/2017, 7:21:25 PM
Synchronization rule action
Failure
Failed to process User 'magdalena.bolton@wingtiptoysonline.com' (see details for more information); Error: Error occured while evaluating function 'SingleAppRoleAssignment' Executing EntryM
4/28/2017, 7:21:25 PM
Synchronization rule action
Failure
Failed to process User 'irwin.mccray@wingtiptoysonline.com' (see details for more information); Error: Error occured while evaluating function 'SingleAppRoleAssignment' Executing EntryMappir
4/28/2017, 7:21:25 PM
Synchronization rule action
Failure
Failed to process User 'rob@wingtiptoysonline.com' (see details for more information); Error: Error occured while evaluating function 'SingleAppRoleAssignment' Executing EntryMappingFunctio
Load more

Conditional Access

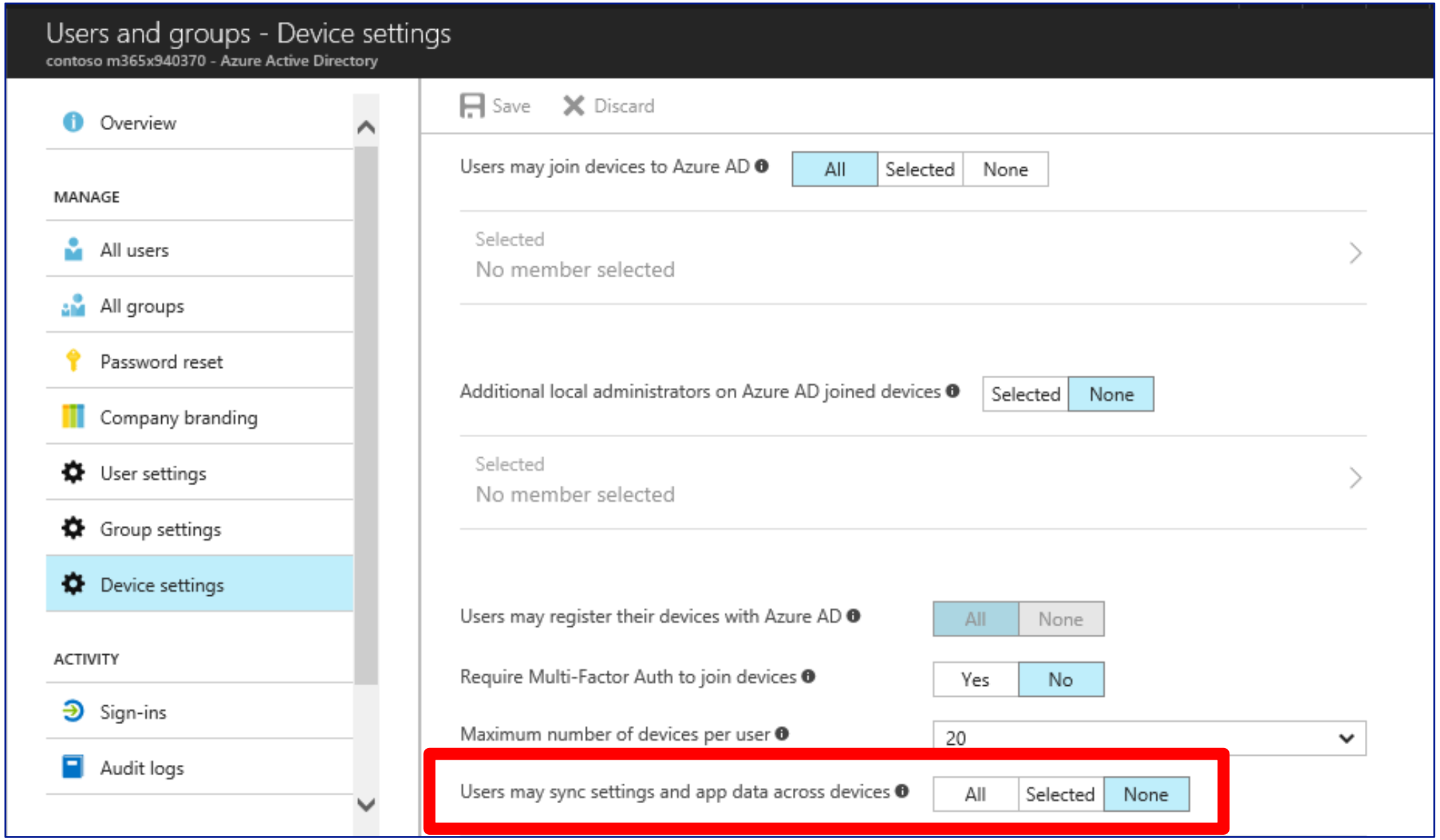

Conditional access - Policies
Azure Active Directory
Policies
MANAGE
Named locations
VPN connectivity (preview)
TROUBLESHOOTING + SUPPORT
Troubleshoot
New support request


You don't have access to this
Your sign-in was successful but you don't have permission to access this resource.
The following information might be useful to your administrator:
Triggered by conditional access.
App name: Microsoft Visual Studio Online
App id: 499b84ac-1321-427f-aa17-267ca6975798
IP address: 167.220.148.179
Device identifier: not available
Device platform: Windows 10
Device state: Unregistered
Signed in as
Correlation ID: 390657dd-935b-4435-9beb-37dc4d2214df
Timestamp: 2017-07-26 16:46:37Z
Sign out and sign in with a different account

Connection Health


stsadweb.one.microsoft.com
ACTIVE DIRECTORY FEDERATION SERVICES
Monitoring
STSADWEB.ONE.MICROSOFT.COM
Filter
0 active
ACTIVE 0
RESOLVED FROM LAST 24 HOURS 0
Monitoring
Token Requests /sec in the past 24 hours
25/MIN
20/MIN
15/MIN
10/MIN
5/MIN
06 PM
TUE 25
06 AM
12 PM
ADFABSTS-NODE1
3.37 /MN
ADFABSTS-NODE3
2.63 /MN
ADFABSTS-NODE2
0 /D
Usage analytics
Top application vists in the past 24 hours
15697
Token Requests /sec in the past 24 hours
25/MIN
20/MIN
15/MIN
10/MIN
5/MIN
06 PM
TUE 25
06 AM
12 PM
ADFABSTS-NODE1
3.37 /MN
ADFABSTS-NODE3
2.63 /MN
ADFABSTS-NODE2
0 /D
MACHINE NAME MIN MAX AVG
ADFABSTS-NODE1 0.00/s 0.30/s 0.07/s
ADFABSTS-NODE3 0.00/S 0.35/s 0.05/s
ADFABSTS-NODE2 0.00/s 0.00/s 0.00/s
ADFABSTS-NODE2 0.00/s 0.00/s 0.00/s
AZ-ADFS-WEB-2B 0.00/s 0.00/s 0.00/s

Enterprise State Roaming


Users and groups - Device settings
contoso m365x940370 - Azure Active Directory
Overview
MANAGE
All users
All groups
Password reset
Company branding
User settings
Group settings
Device settings
ACTIVITY
Sign-ins
Audit logs
Save
Discard
Users may join devices to Azure AD
All
Selected
None
Selected
No member selected
Additional local administrators on Azure AD joined devices
Selected
None
Selected
No member selected
Users may register their devices with Azure AD
All
None
Require Multi-Factor Auth to join devices
Yes
No
Maximum number of devices per user
20
Users may sync settings and app data across devices
All
Selected
None

Advanced Multi Factor

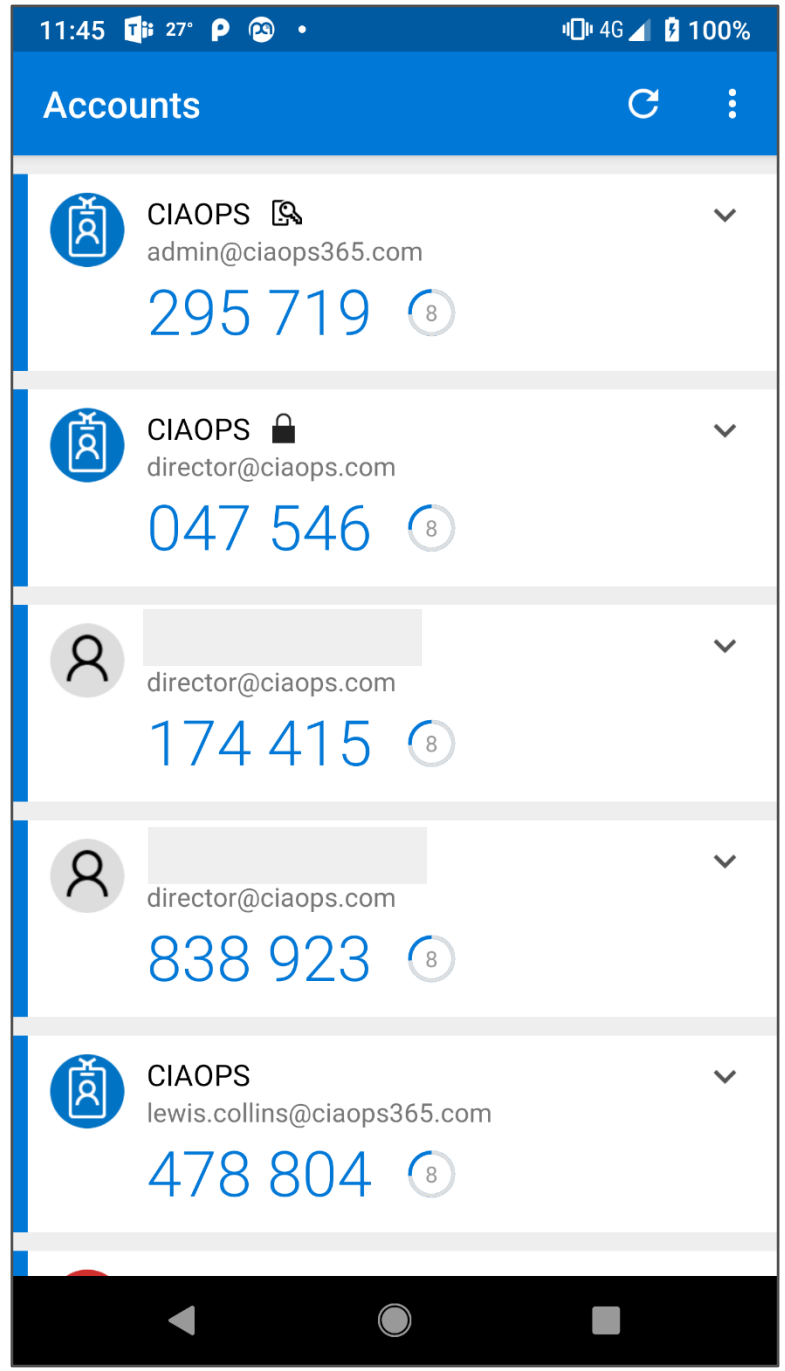
CLOUD-POWERED PROTECTION

How it works

Mobile apps

Phone calls

Text messages


11:45
27°
4G
100%
Accounts
CIAOPS
admin@ciaops365.com
295 719
8
CIAOPS
director@ciaops.com
047 546
8
director@ciaops.com
174 415
8
director@ciaops.com
838 923
8
CIAOPS
lewis.collins@ciaops365.com
478 804
8

Azure MFA vs MFA for Office 365

	MFA for Office 365/Azure Administrators	Azure Multi-Factor Authentication
Administrators can Enable/Enforce MFA to end-users	Yes	Yes
Use Mobile app (online and OTP) as second authentication factor	Yes	Yes
Use Phone call as second authentication factor	Yes	Yes
Use SMS as second authentication factor	Yes	Yes
Application passwords for non-browser clients (e.g. Outlook, Lync)	Yes	Yes
Default Microsoft greetings during authentication phone calls	Yes	Yes
Suspend MFA from known devices	Yes	Yes
Custom greetings during authentication phone calls		Yes
Fraud alert		Yes
MFA SDK		Yes
Security Reports		Yes
MFA for on-premises applications/ MFA Server.		Yes
One-Time Bypass		Yes
Block/Unblock Users		Yes
Customizable caller ID for authentication phone calls		Yes
Event Confirmation		Yes
Trusted IPs		Yes

MFA and Passwordless

Reasons for Azure AD P1

- Office 365 Group naming policy - https://support.office.com/en-us/article/office-365-groups-naming-policy-6ceca4d3-cad1-4532-9f0f-d469dfbbb552
- Office 365 Group Expiration Policy - https://support.office.com/en-us/article/Office-365-Group-Expiration-Policy-8d253fe5-0e09-4b3c-8b5e-f48def064733
- Azure AD Password write back - https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-get-started-custom#optional-features
- Enterprise state roaming with Windows 10 - https://docs.microsoft.com/en-us/azure/active-directory/active-directory-windows-enterprise-state-roaming-overview
- Conditional access in Azure AD - https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-azure-portal
- Control access from unmanaged AD devices - https://support.office.com/en-us/article/Control-access-from-unmanaged-devices-5ae550c4-bd20-4257-847b-5c20fb053622?ui=en-US&rs=en-US&ad=US
- Azure AD Connect Health - https://docs.microsoft.com/en-us/azure/active-directory/connect-health/active-directory-aadconnect-health
- Cloud App Discovery - https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/cloud-app-discovery

Reasons for Azure AD P1

- MDM auto-enrollment - https://docs.microsoft.com/en-us/windows/client-management/mdm/azure-ad-and-microsoft-intune-automatic-mdm-enrollment-in-the-new-portal
- Dynamic Group membership - https://docs.microsoft.com/en-us/azure/active-directory/active-directory-groups-dynamic-membership-azure-portal
- https://docs.microsoft.com/en-us/azure/active-directory/active-directory-reporting-security-risky-sign-ins
  - The risky sign-ins report in the Azure Active Directory premium editions provides you with:
  - Aggregated information about the risk event types that have been detected
  - An option to download the report
- Turn external sharing on or off for SharePoint Online - https://support.office.com/en-us/article/turn-external-sharing-on-or-off-for-sharepoint-online-6288296a-b6b7-4ea4-b4ed-c297bf833e30
- Azure AD Premium Password Protection - https://cloudblogs.microsoft.com/enterprisemobility/2018/06/19/azure-ad-password-protection-and-smart-lockout-are-now-in-public-preview/
- Multiple MFA tokens - Hardware OATH tokens in Azure MFA in the cloud now available - https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Hardware-OATH-tokens-in-Azure-MFA-in-the-cloud-are-now-available/ba-p/276466
- SharePoint and OneDrive limited access - https://docs.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices?redirectSourcePath=%252farticle%252f5ae550c4-bd20-4257-847b-5c20fb053622
- Terms of use - https://docs.microsoft.com/en-us/azure/active-directory/governance/active-directory-tou

Azure AD P2 Features

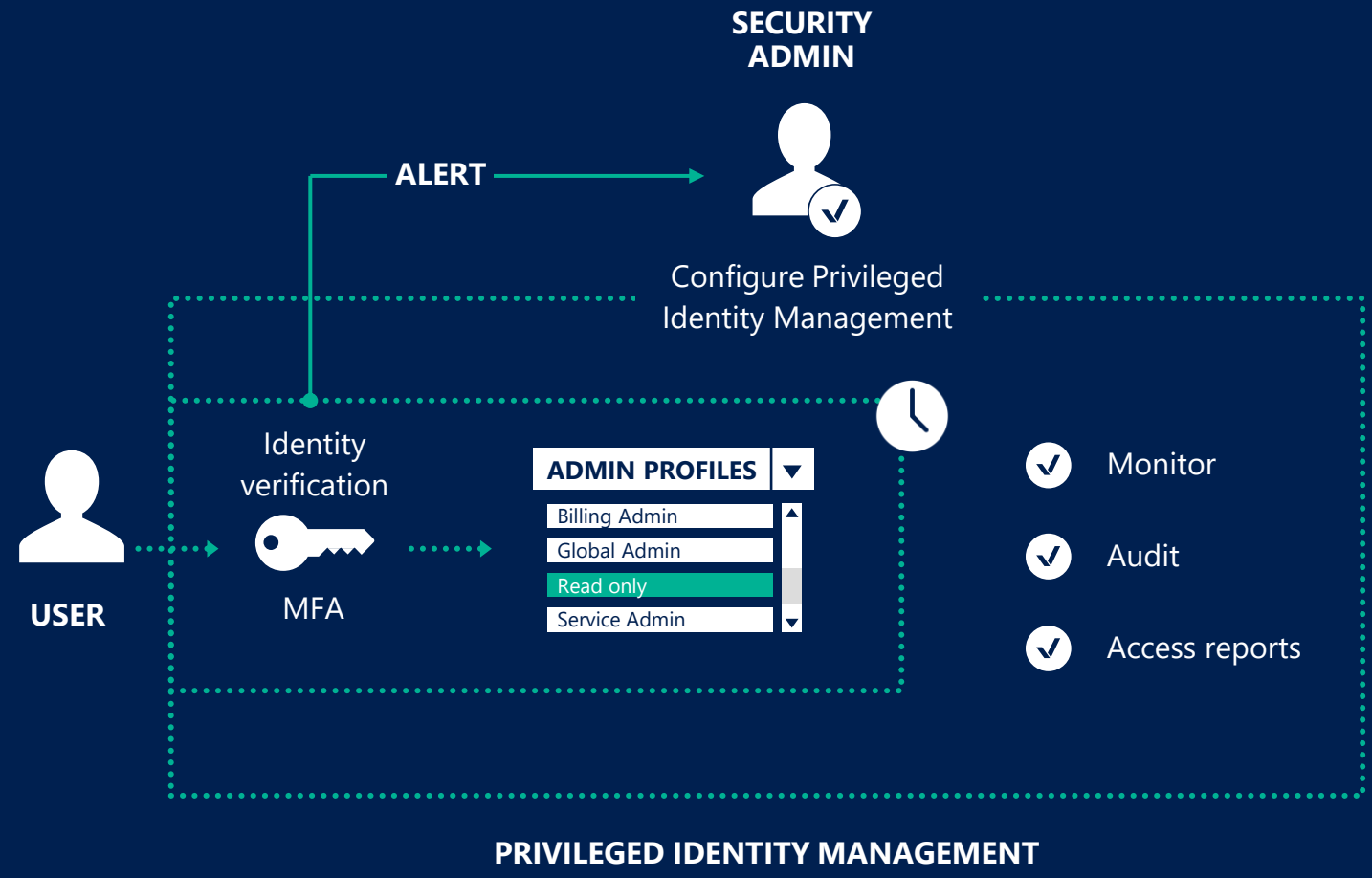
Privileged Identity Management (PIM)

CLOUD-POWERED PROTECTION

Privileged Identity Management

How time-limited activation of privileged roles works

- Users need to activate their privileges to perform a task
- MFA is enforced during the activation process
- Alerts inform administrators about out-of-band changes
- Users will retain their privileges for a pre-configured amount of time
- Security admins can discover all privileged identities, view audit reports and review everyone who has is eligible to activate via access reviews



Benefits: Privileged Identity Management

Reduces exposure to attacks targeting admins

- Removes unneeded permanent admin role assignments
- Limits the time a user has admin privileges
- Ensures MFA validation prior to admin role activation

Simplifies delegation

- Separates role administration from other tasks
- Adds roles for read-only views of reports and history
- Asks users to review and justify continued need for admin role

Increases visibility and finer-grained control

- Enables least privilege role assignments
- Alerts on users who haven't used their role assignments
- Simplifies reporting on admin activity

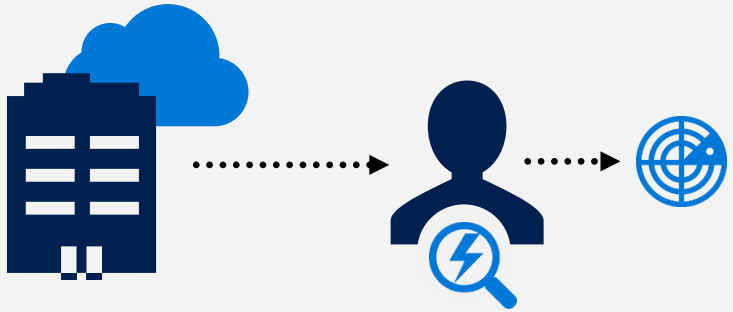
DETECT ATTACKS BEFORE THEY CAUSE DAMAGE

Microsoft Advanced Threat Analytics

An on-premises platform to identify advanced security attacks and insider threats ***before*** they cause damage

Behavioral Analytics + Detection of advanced attacks and security risks = Advanced Threat Detection

Microsoft Advanced Threat Analytics brings the behavioral analytics concept to IT and the organization's users.



What is Azure Multi-Factor Authentication?

A standalone Azure identity and access management service, also included in Azure Active Directory Premium

Prevents unauthorized access to both on-premises and cloud applications by providing an additional level of authentication

Trusted by thousands of enterprises to authenticate employee, customer, and partner access

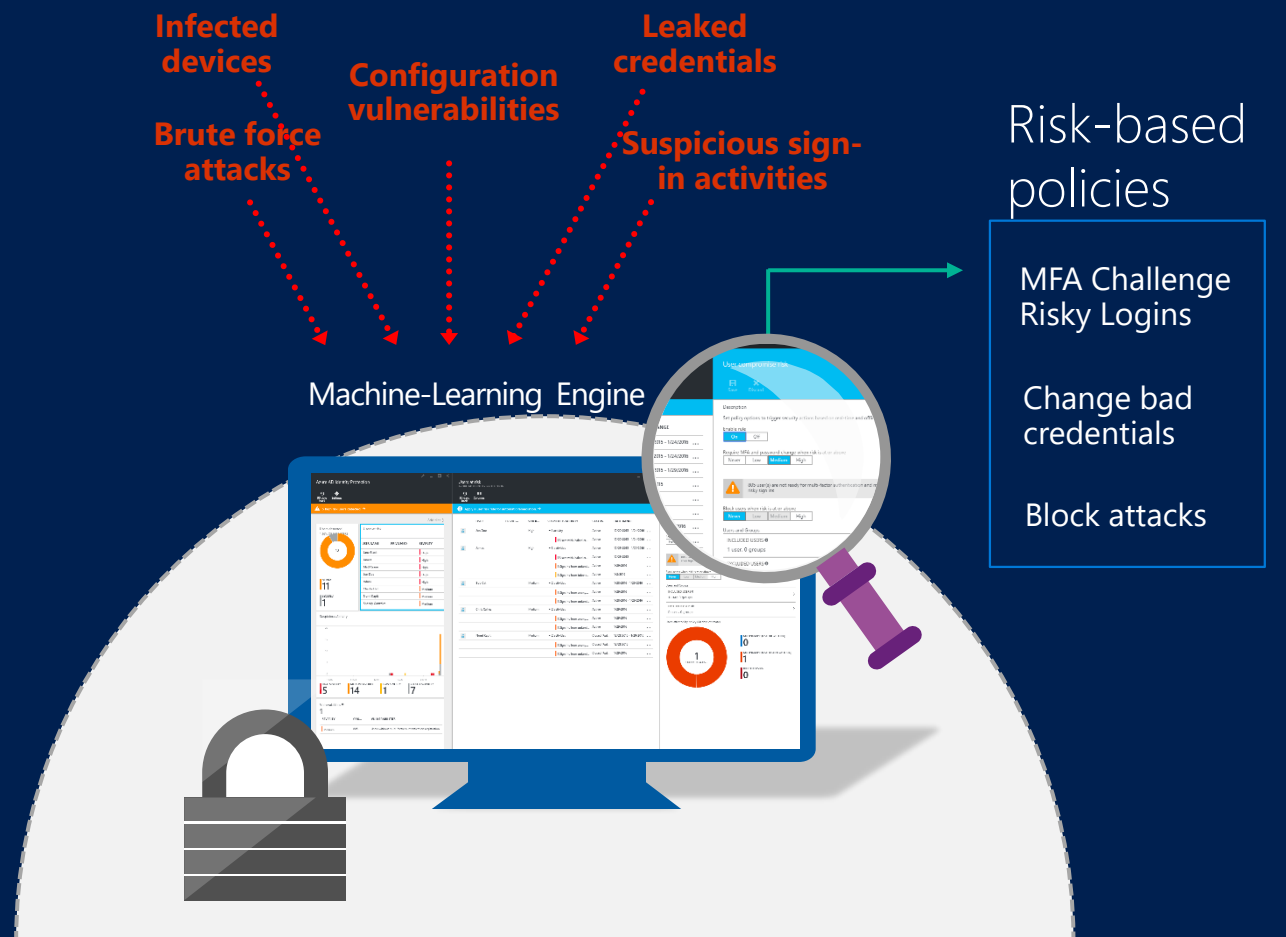
Identity Protection

CLOUD-POWERED PROTECTION

Azure Active Directory Identity Protection

Identity Protection at its best

- Gain insights from a consolidated view of machine learning based threat detection
- Remediation recommendations
- Risk severity calculation
- Risk-based conditional access automatically protects against suspicious logins and compromised credentials



CLOUD-POWERED PROTECTION

Azure Active Directory Identity Protection

Use the power of Identity Protection in PowerBI, SIEM and other monitoring tools

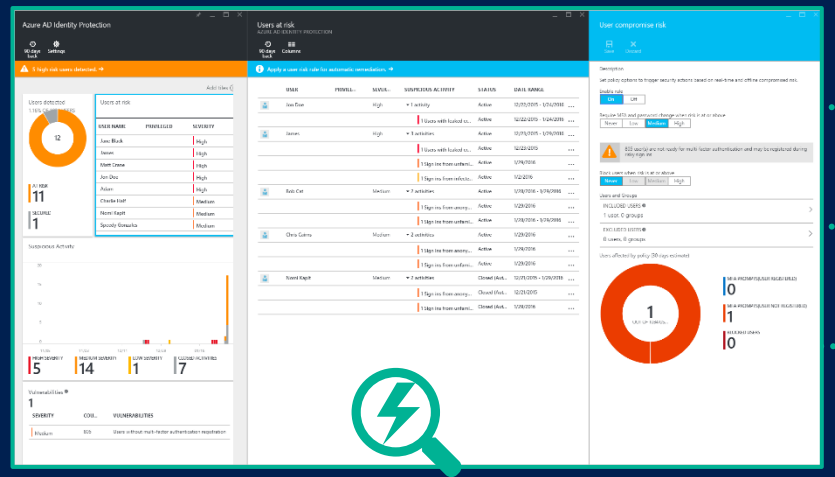
Infected devices

Brute force attacks

Configuration vulnerabilities

Leaked credentials

Suspicious sign-in activities



Microsoft machine - learning engine

Notifications

Data Extracts/Downloads

Reporting APIs

Security/Monitoring/Reporting Solutions

Power BI

SIEM

Monitor Tools

Apply Microsoft learnings to your existing security tools

Microsoft

Azure Active Directory

Your Azure AD Identity Protection Weekly Digest

July 25 to August 1 for Piper Alderman

Security snapshot

Users at risk

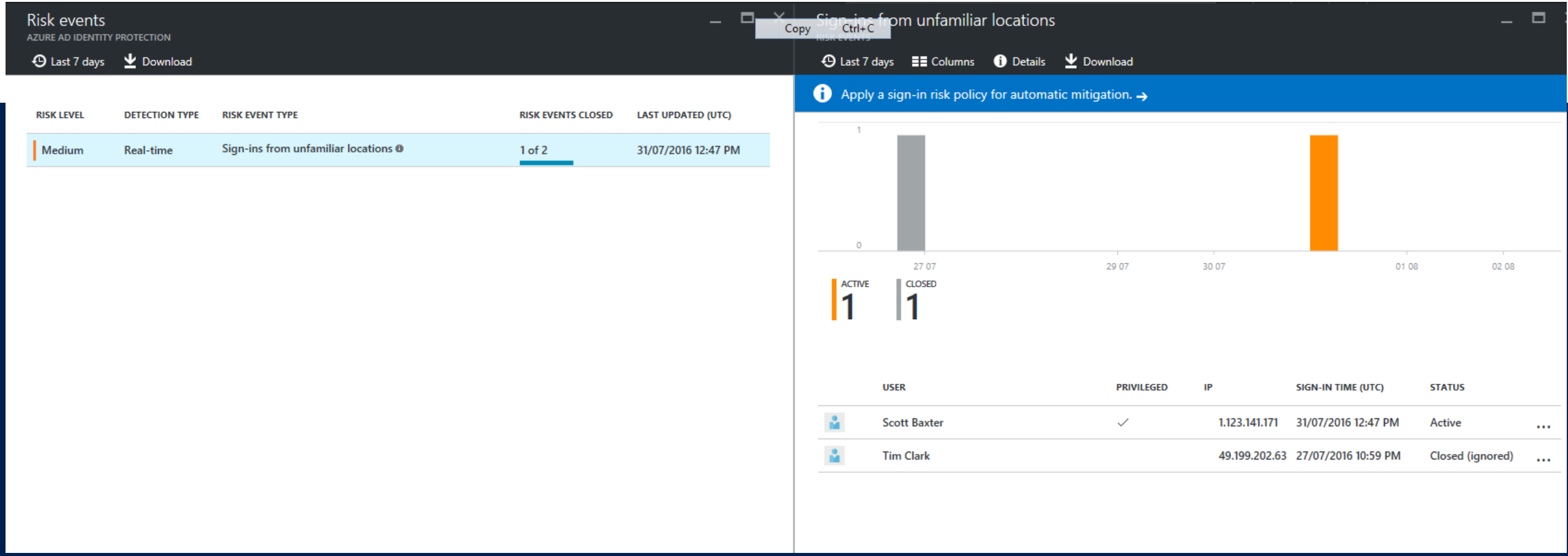
3

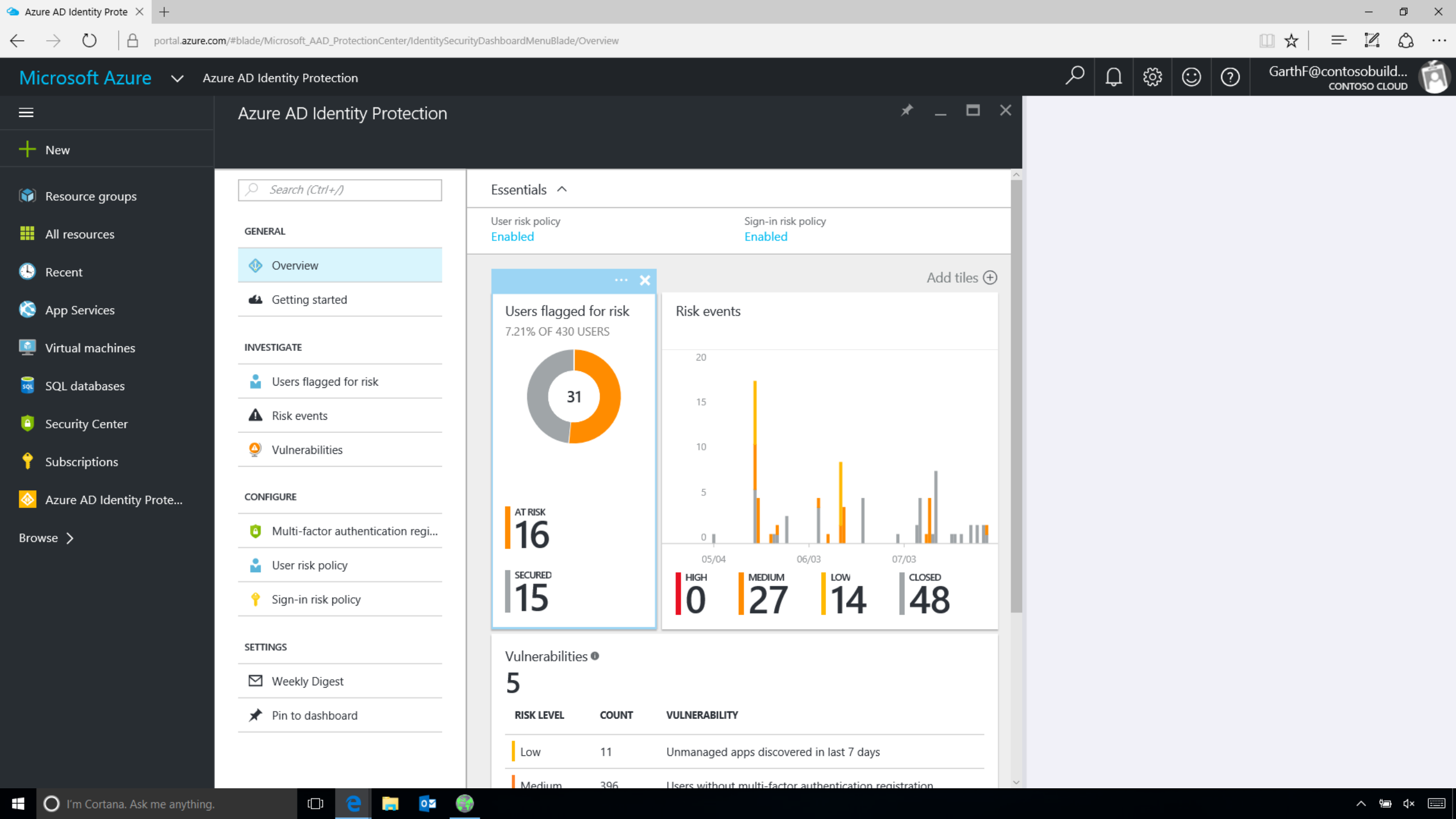
Risk events

3

Vulnerabilities

1


Risk events
AZURE AD IDENTITY PROTECTION
Last 7 days
Download
RISK LEVEL
DETECTION TYPE
RISK EVENT TYPE
RISK EVENTS CLOSED
LAST UPDATED (UTC)
Medium
Real-time
Sign-ins from unfamiliar locations
1 of 2
31/07/2016 12:47 PM
Copy Ctrl+C
Sign-ins from unfamiliar locations
RISK EVENTS
Last 7 days
Columns
Details
Download
Apply a sign-in risk policy for automatic mitigation.
1
0
27 07
29 07
30 07
01 08
02 08
ACTIVE
1
CLOSED
1
USER
PRIVILEGED
IP
SIGN-IN TIME (UTC)
STATUS
Scott Baxter
1.123.141.171
31/07/2016 12:47 PM
Active
Tim Clark
49.199.202.63
27/07/2016 10:59 PM
Closed (ignored)


Azure AD Identity Prote
portal.azure.com/#blade/Microsoft_AAD_ProtectionCenter/IdentitySecurityDashboardMenuBlade/Overview
Microsoft Azure
Azure AD Identity Protection
GarthF@contosobuild...
CONTOSO CLOUD
New
Resource groups
All resources
Recent
App Services
Virtual machines
SQL databases
Security Center
Subscriptions
Azure AD Identity Prote...
Browse
Azure AD Identity Protection
Search (Ctrl+/)
GENERAL
Overview
Getting started
INVESTIGATE
Users flagged for risk
Risk events
Vulnerabilities
CONFIGURE
Multi-factor authentication regi...
User risk policy
Sign-in risk policy
SETTINGS
Weekly Digest
Pin to dashboard
Essentials
User risk policy
Enabled
Sign-in risk policy
Enabled
Add tiles
Users flagged for risk
7.21% OF 430 USERS
31
AT RISK
16
SECURED
15
Risk events
20
15
10
5
0
05/04
06/03
07/03
HIGH
0
MEDIUM
27
LOW
14
CLOSED
48
Vulnerabilities
5
RISK LEVEL
COUNT
VULNERABILITY
Low
11
Unmanaged apps discovered in last 7 days
Medium
396
Users without multi-factor authentication registration
I'm Cortana. Ask me anything.

New
Resource groups
All resources
Recent
App Services
Virtual machines
SQL databases
Security Center
Subscriptions
Azure AD Identity Prote...
Browse

Azure AD Identity Protection

Search (Ctrl+/)

GENERAL
Overview
Getting started

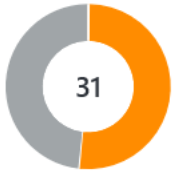
INVESTIGATE
Users flagged for risk
Risk events
Vulnerabilities

CONFIGURE
Multi-factor authentication regi...
User risk policy
Sign-in risk policy

SETTINGS
Weekly Digest
Pin to dashboard

Users flagged for risk

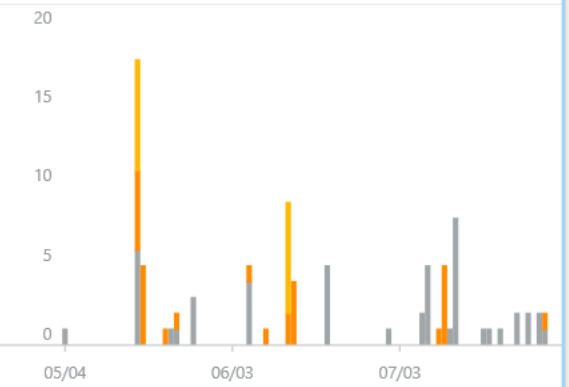
7.21% OF 430 USERS



AT RISK **16**

SECURED **15**

Risk events

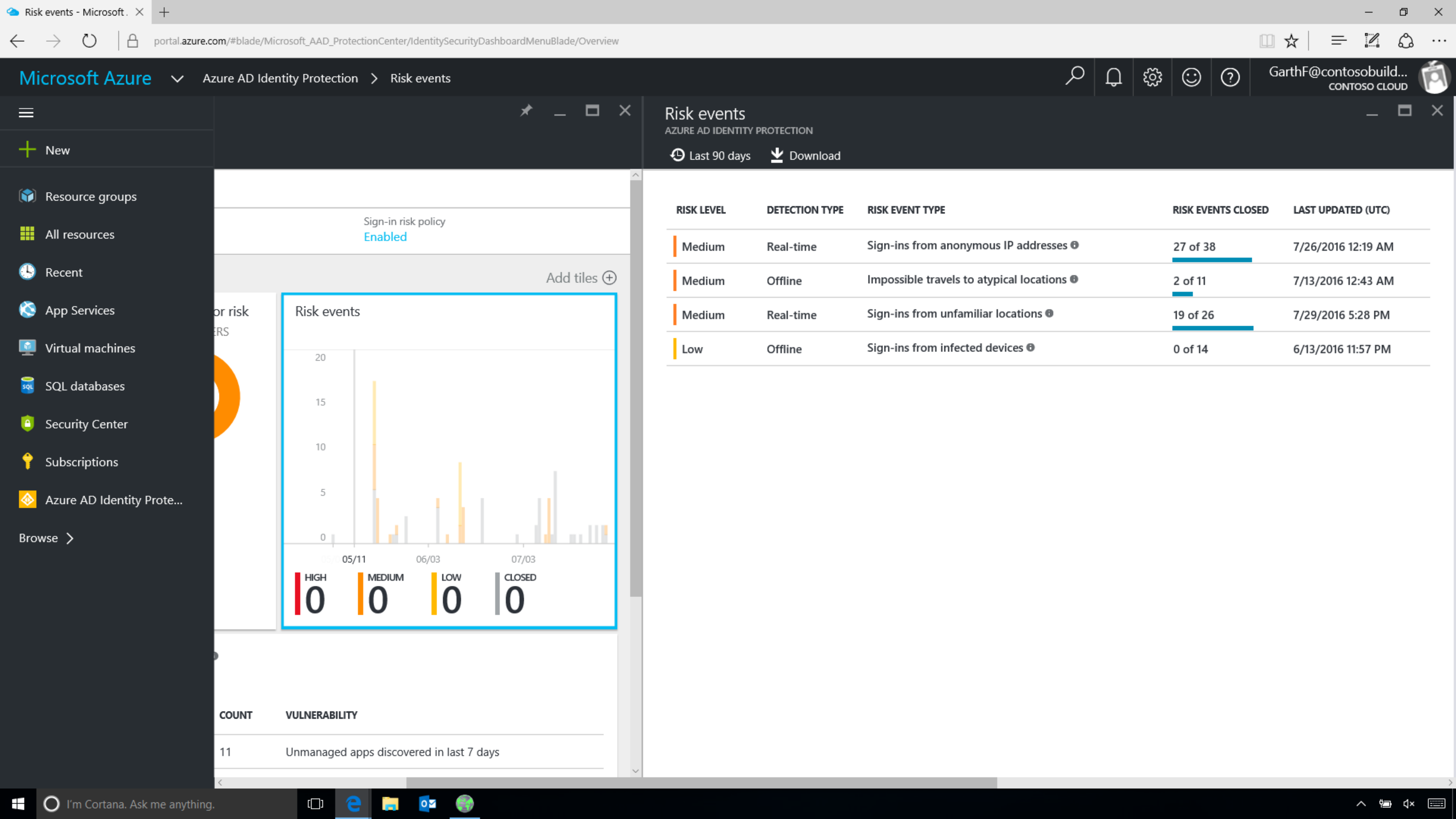


HIGH **0** | MEDIUM **27** | LOW **14** | CLOSED **48**

Vulnerabilities

5

RISK LEVEL	COUNT	VULNERABILITY
Low	11	Unmanaged apps discovered in last 7 days
Medium	396	Users without multi-factor authentication registration
Low	8	Administrators aren't using their privileged roles
Medium	13	Roles don't require multi-factor authentication for activation
Low	29	There are too many global administrators



Risk events - Microsoft
portal.azure.com/#blade/Microsoft_AAD_ProtectionCenter/IdentitySecurityDashboardMenuBlade/Overview
Microsoft Azure
Azure AD Identity Protection > Risk events
GarthF@contosobuild...
CONTOSO CLOUD
New
Resource groups
All resources
Recent
App Services
Virtual machines
SQL databases
Security Center
Subscriptions
Azure AD Identity Prote...
Browse >
Sign-in risk policy
Enabled
Add tiles
Risk events
20
15
10
5
0
05/11
06/03
07/03
HIGH 0
MEDIUM 0
LOW 0
CLOSED 0
COUNT
VULNERABILITY
11
Unmanaged apps discovered in last 7 days
Risk events
AZURE AD IDENTITY PROTECTION
Last 90 days
Download
RISK LEVEL
DETECTION TYPE
RISK EVENT TYPE
RISK EVENTS CLOSED
LAST UPDATED (UTC)
Medium Real-time Sign-ins from anonymous IP addresses 27 of 38 7/26/2016 12:19 AM
Medium Offline Impossible travels to atypical locations 2 of 11 7/13/2016 12:43 AM
Medium Real-time Sign-ins from unfamiliar locations 19 of 26 7/29/2016 5:28 PM
Low Offline Sign-ins from infected devices 0 of 14 6/13/2016 11:57 PM
I'm Cortana. Ask me anything.

Impossible travel to aty

portal.azure.com/#blade/Microsoft_AAD_ProtectionCenter/IdentitySecurityDashboardMenuBlade/Overview

Microsoft Azure | Azure AD Identity Protection > Risk events > Impossible travel to atypical locations

GarthF@contosobuild... CONTOSO CLOUD

New

Resource groups

All resources

Recent

App Services

Virtual machines

SQL databases

Security Center

Subscriptions

Azure AD Identity Prote...

Browse

LAST UPDATED (UTC)

7/26/2016 12:19 AM

7/13/2016 12:43 AM

7/29/2016 5:28 PM

6/13/2016 11:57 PM

Impossible travel to atypical locations

RISK EVENTS

Last 90 days | Columns | Details | Download

Apply a user risk policy for automatic mitigation. →

ACTIVE 9

CLOSED 2

USER	PRIVILEGED	SECOND LOCATION	FIRST LOCATION	SECOND SIGN-IN TIM...	FIRST SIGN-IN TIME (...	STATUS
Douglas Fife	✓	Bratislava, Bratislavsky	Toronto, Ontario, CA	7/13/2016 12:43 AM	7/13/2016 12:41 AM	Closed (password...
Douglas Fife	✓	Amsterdam, Noord-Holland	Toronto, Ontario, CA	7/13/2016 12:40 AM	7/13/2016 12:34 AM	Closed (password...
Jennifer Davis		Beijing, Beijing Shi	Seattle,Washington, US	▸ 3 instances		Active
John Smith		Seattle, Washington	Marchwood, Hampshire, GB	▸ 3 instances		Active
Mike Lee		Beijing, Beijing Shi	Amsterdam, Noord-Holland,...	▸ 3 instances		Active

I'm Cortana. Ask me anything.

New
Resource groups
All resources
Recent
App Services
Virtual machines
SQL databases
Security Center
Subscriptions
Azure AD Identity Prote...
Browse >

Impossible travel to atypical locations

RISK EVENTS

Last 90 days | Columns | Details | Download

Apply a user risk policy for automatic mitigation. →

LAST UPDATED (UTC)
7/26/2016 12:19 AM
7/13/2016 12:43 AM
7/29/2016 5:28 PM
6/13/2016 11:57 PM

ACTIVE 9 CLOSED 2

	USER	PRIVILEGED	SECOND LOCATION	FIRST LOCATION	SECOND SIGN-IN TIM...	FIRST SIGN-IN TIME (...	STATUS
	Douglas Fife	✓	Bratislava, Bratislavsky	Toronto, Ontario, CA	7/13/2016 12:43 AM	7/13/2016 12:41 AM	Closed (password...
	Douglas Fife	✓	Amsterdam, Noord-Holland	Toronto, Ontario, CA	7/13/2016 12:40 AM	7/13/2016 12:34 AM	Closed (password...
	Jennifer Davis		Beijing, Beijing Shi	Seattle,Washington, US	▼ 3 instances		Active
					6/14/2016 12:21 ...	6/13/2016 8:11 PM	Active
					5/17/2016 11:42 P...	5/17/2016 7:32 PM	Active
					7/11/2016 1:02 AM	7/10/2016 8:52 PM	Active
	John Smith		Seattle, Washington	Marchwood, Hampshire, GB	▶ 3 instances		Active
	Mike Lee		Beijing, Beijing Shi	Amsterdam, Noord-Holland,...	▶ 3 instances		Active

Jennifer Davis - Microsc

portal.azure.com/#blade/Microsoft_AAD_ProtectionCenter/IdentitySecurityDashboardMenuBlade/Risk events

Microsoft Azure | Impossible travel to atypical locations > Jennifer Davis | Search resources | GarthF@contosobuild... CONTOSO CLOUD

- New
- Resource groups
- All resources
- Recent
- App Services
- Virtual machines
- SQL databases
- Security Center
- Subscriptions
- Azure AD Identity Prote...
- Browse

	FIRST LOCATION	SECOND SIGN-IN TIM...	FIRST SIGN-IN TIME (...	STATUS
...vsky	Toronto, Ontario, CA	7/13/2016 12:43 AM	7/13/2016 12:41 AM	Closed (password...
...d-Holland	Toronto, Ontario, CA	7/13/2016 12:40 AM	7/13/2016 12:34 AM	Closed (password...
...i	Seattle,Washington, US	4 instances		Active
...on	Marchwood, Hampshire, GB	4 instances		Active
...i	Amsterdam, Noord-Holland,...	4 instances		Active

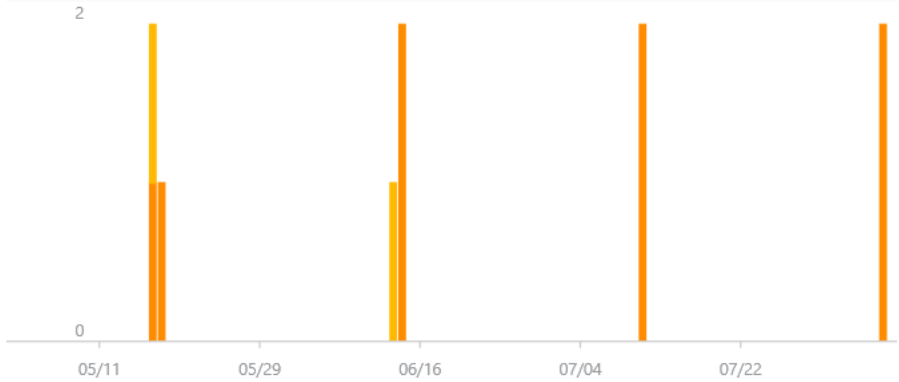
Jennifer Davis

All sign-ins | Reset password | Enable MFA | Dismiss all eve...

Essentials

Risk level: Medium
Status: At risk
Role: User
Contact: JenDavis@contosobuild.com
Location: N/A
MFA registered: No
Department: N/A

Risk events



HIGH 0 | MEDIUM 8 | LOW 2 | CLOSED 0

TIME (UTC)	IP ADDRESS	RISK EVENT TYPE	RISK LEVEL
8/7/2016 4:40 ...	77.109.41.30	Sign-in from anonymous IP address	Medium

I'm Cortana. Ask me anything.

New
Resource groups
All resources
Recent
App Services
Virtual machines
SQL databases
Security Center
Subscriptions
Azure AD Identity Prote...
Browse

Azure AD Identity Protection

Search (Ctrl+/)

GENERAL
Overview
Getting started

INVESTIGATE
Users flagged for risk
Risk events
Vulnerabilities

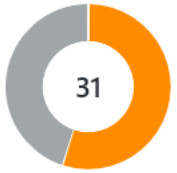
CONFIGURE
Multi-factor authentication regi...
User risk policy
Sign-in risk policy

SETTINGS
Weekly Digest
Pin to dashboard

Add tiles

Users flagged for risk

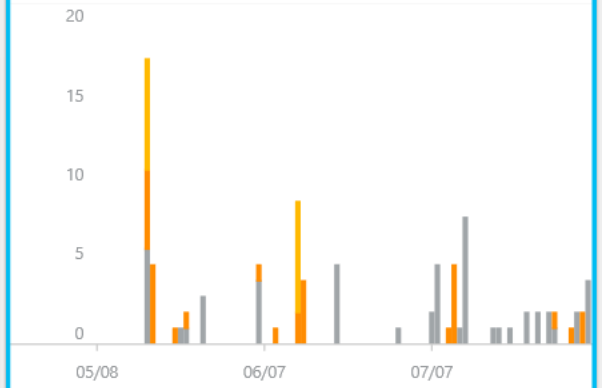
7.21% OF 430 USERS



AT RISK **17**

SECURED **14**

Risk events



HIGH **0** MEDIUM **30** LOW **14** CLOSED **53**

Vulnerabilities

5

RISK LEVEL	COUNT	VULNERABILITY
Low	13	Unmanaged apps discovered in last 7 days
Medium	396	Users without multi-factor authentication registration
Low	8	Administrators aren't using their privileged roles
Medium	13	Roles don't require multi-factor authentication for activation

Risk events

AZURE AD IDENTITY PROTECTION

Last 90 days Download

RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE
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

New
Resource groups
All resources
Recent
App Services
Virtual machines
SQL databases
Security Center
Subscriptions
Azure AD Identity Prote...
Browse

Risk events

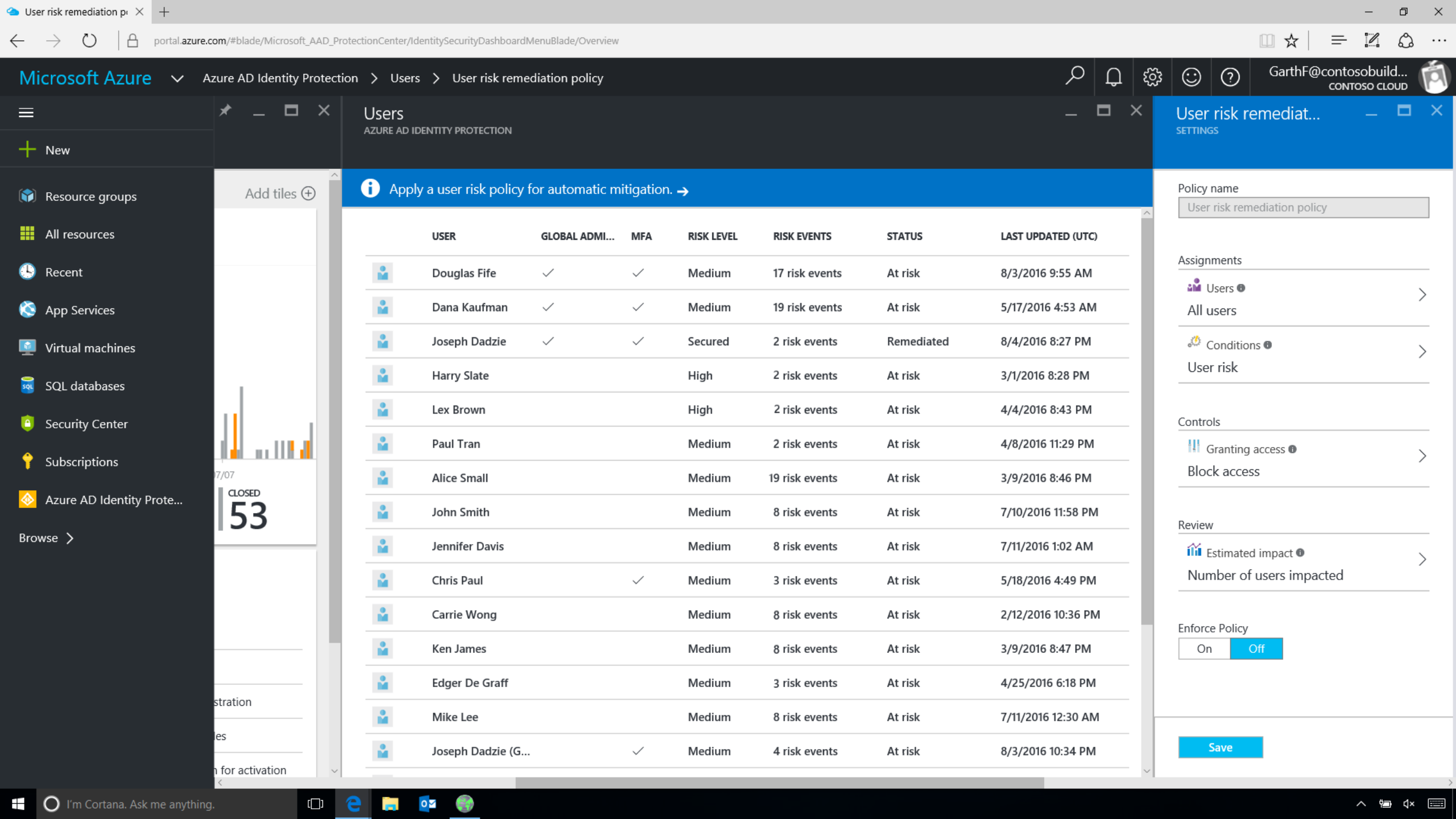
COUNT	VULNERABILITY
13	Unmanaged apps discovered in last 7 days
396	Users without multi-factor authentication registration
8	Administrators aren't using their privileged roles
13	Roles don't require multi-factor authentication for activation

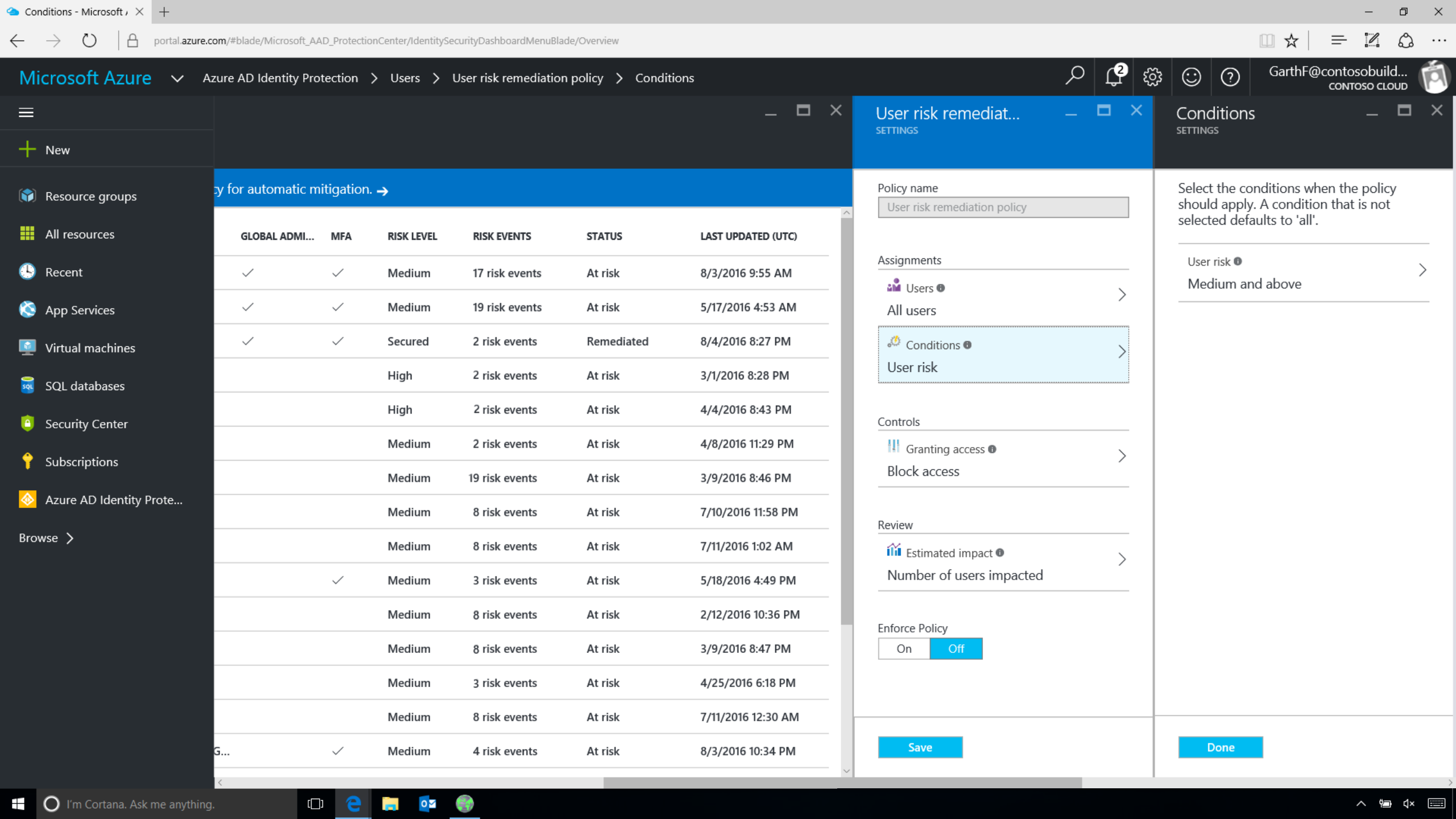
Users

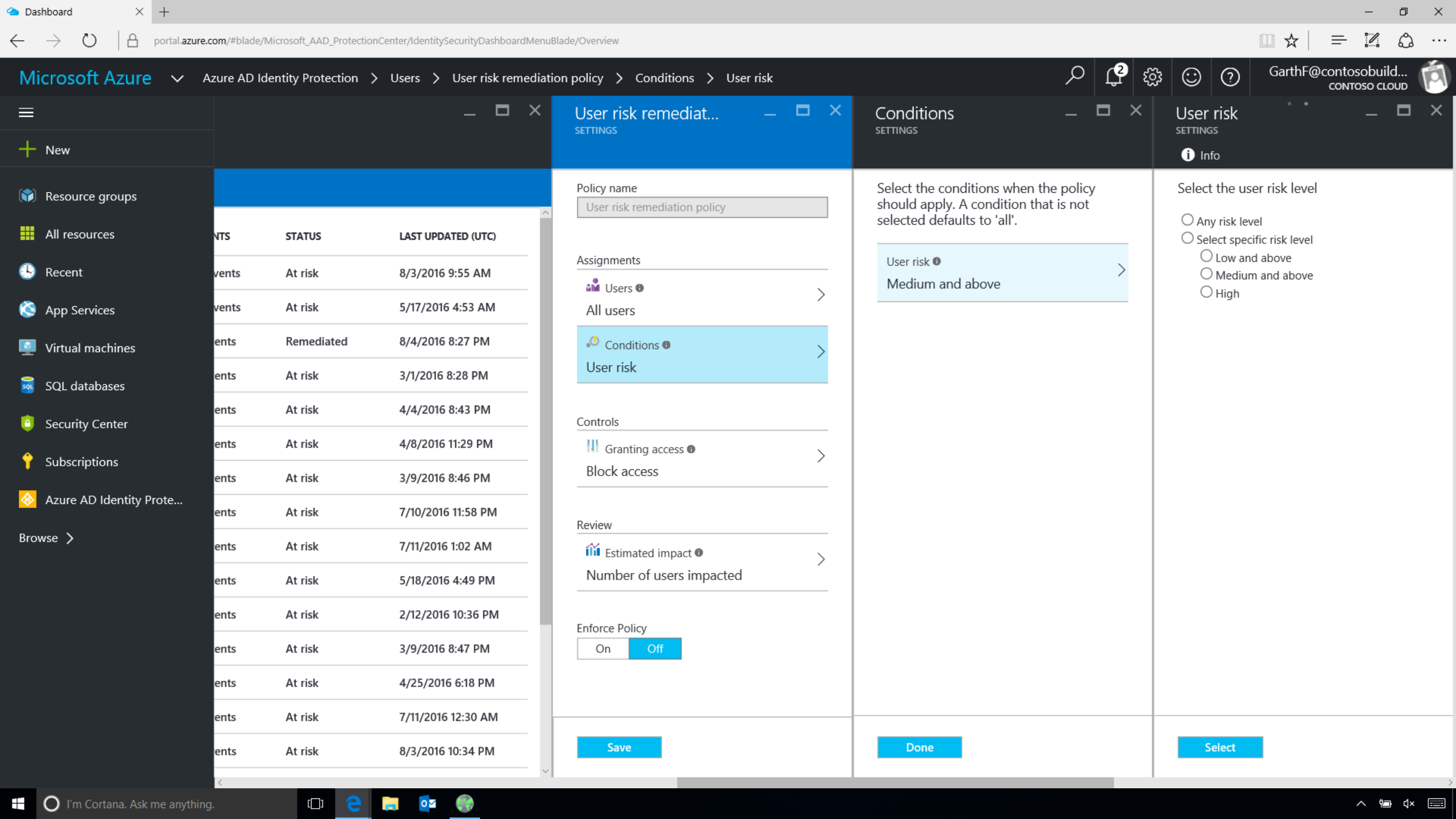
AZURE AD IDENTITY PROTECTION

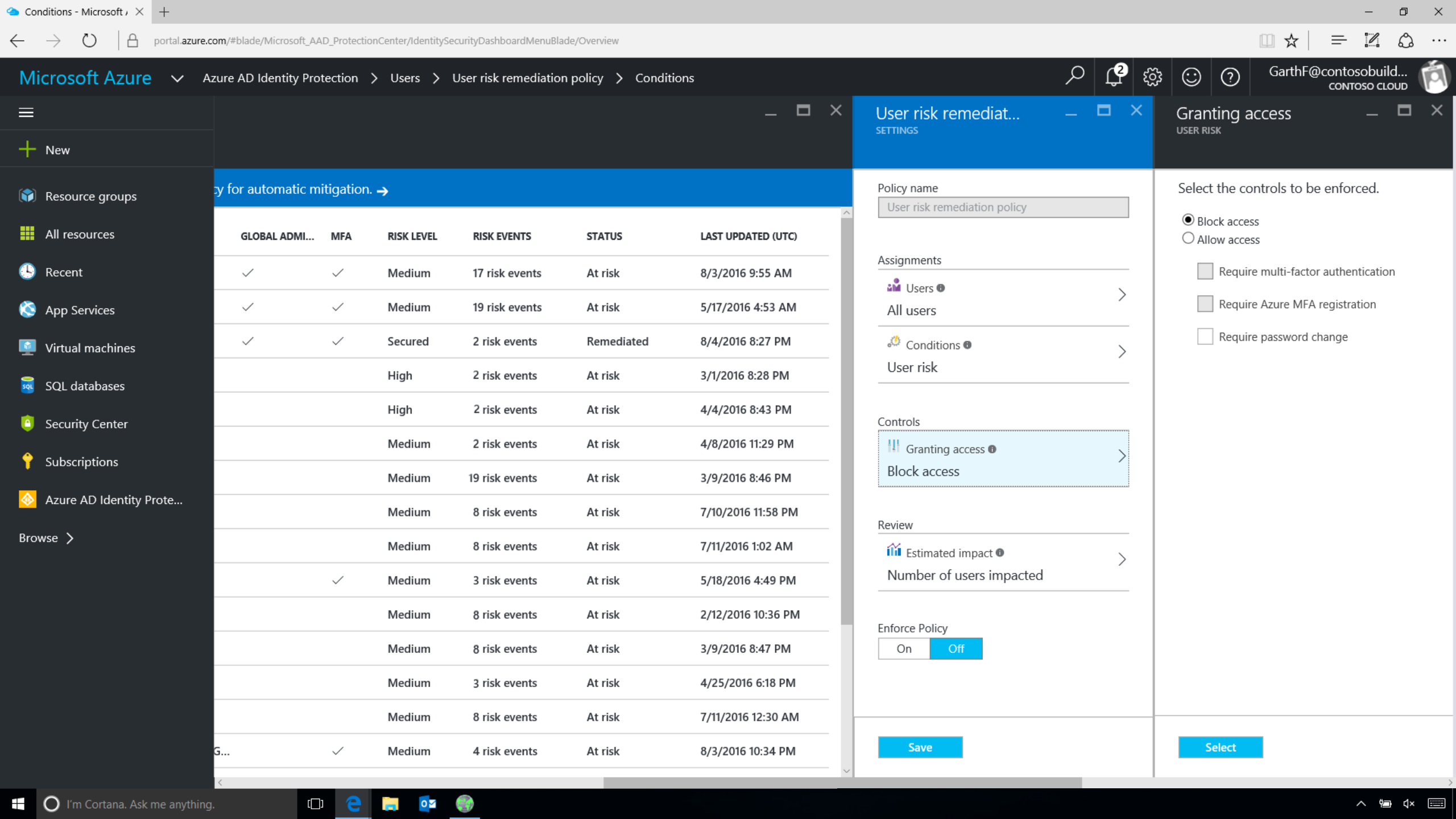
Apply a user risk policy for automatic mitigation. →

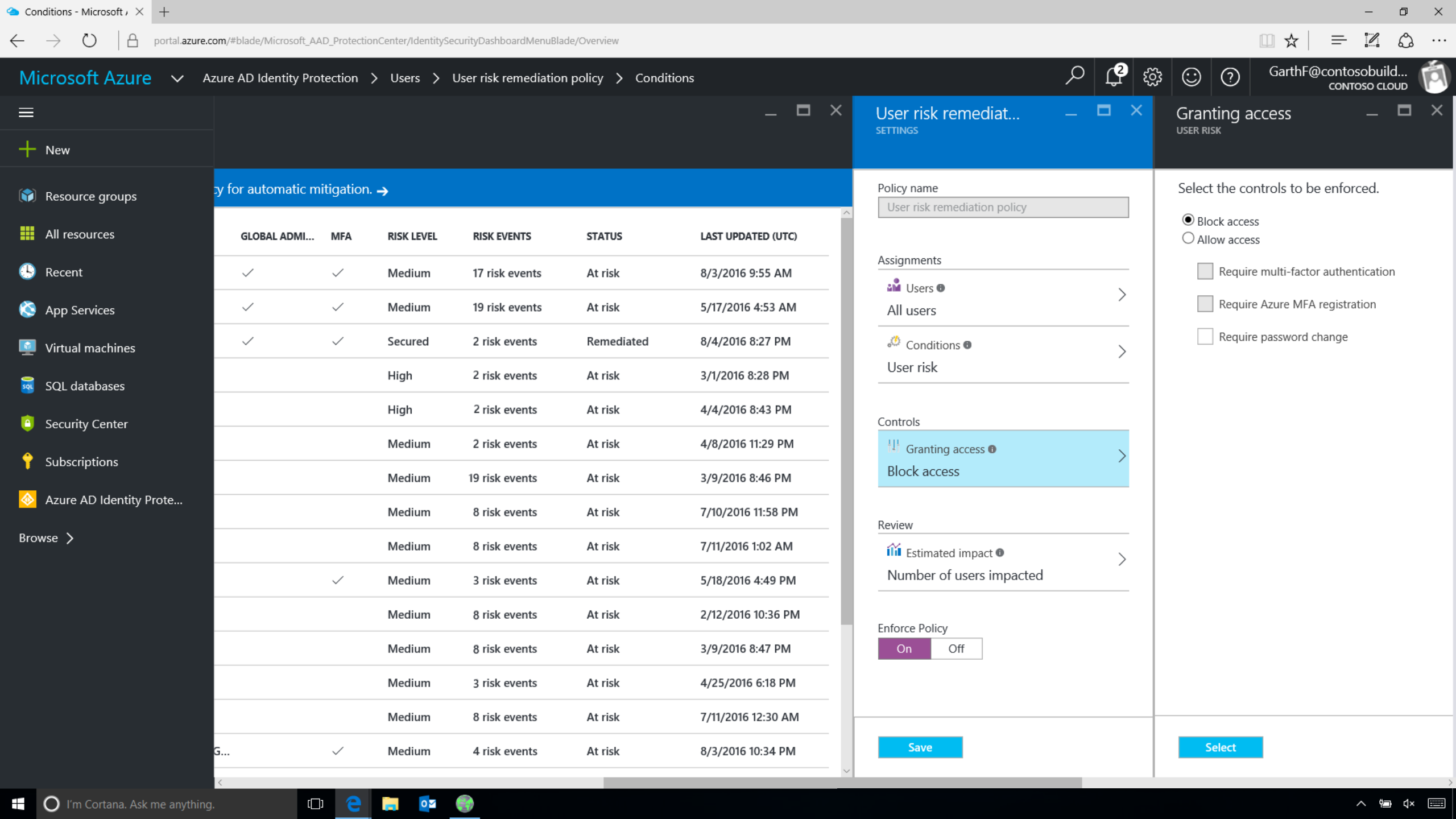
USER	GLOBAL ADMI...	MFA	RISK LEVEL	RISK EVENTS	STATUS	LAST UPDATED (UTC)
Douglas Fife	✓	✓	Medium	17 risk events	At risk	8/3/2016 9:55 AM
Dana Kaufman	✓	✓	Medium	19 risk events	At risk	5/17/2016 4:53 AM
Joseph Dadzie	✓	✓	Secured	2 risk events	Remediated	8/4/2016 8:27 PM
Harry Slate			High	2 risk events	At risk	3/1/2016 8:28 PM
Lex Brown			High	2 risk events	At risk	4/4/2016 8:43 PM
Paul Tran			Medium	2 risk events	At risk	4/8/2016 11:29 PM
Alice Small			Medium	19 risk events	At risk	3/9/2016 8:46 PM
John Smith			Medium	8 risk events	At risk	7/10/2016 11:58 PM
Jennifer Davis			Medium	8 risk events	At risk	7/11/2016 1:02 AM
Chris Paul		✓	Medium	3 risk events	At risk	5/18/2016 4:49 PM
Carrie Wong			Medium	8 risk events	At risk	2/12/2016 10:36 PM
Ken James			Medium	8 risk events	At risk	3/9/2016 8:47 PM
Edger De Graff			Medium	3 risk events	At risk	4/25/2016 6:18 PM
Mike Lee			Medium	8 risk events	At risk	7/11/2016 12:30 AM
Joseph Dadzie (G...		✓	Medium	4 risk events	At risk	8/3/2016 10:34 PM

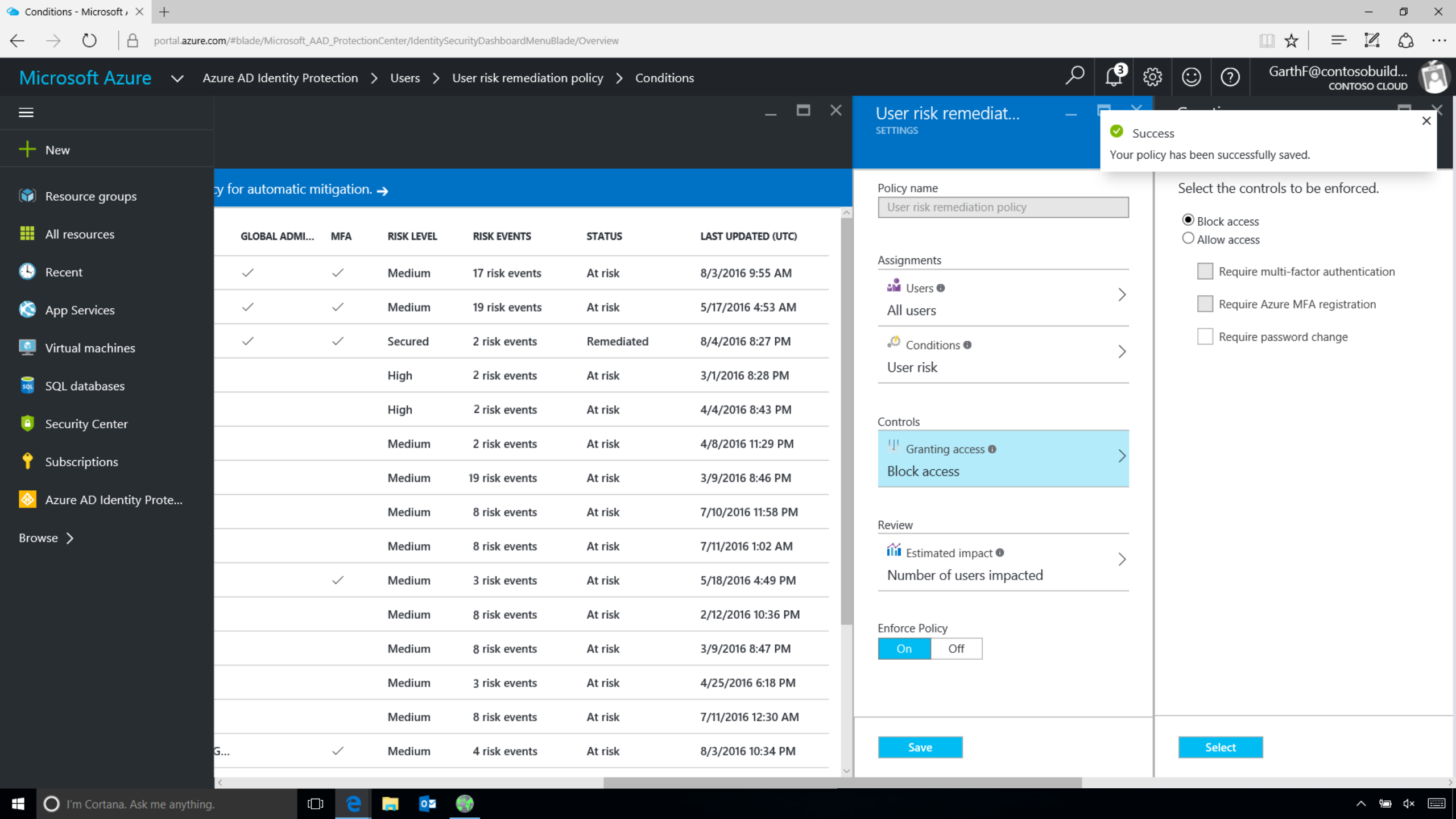

User risk remediation p
portal.azure.com/#blade/Microsoft_AAD_ProtectionCenter/IdentitySecurityDashboardMenuBlade/Overview
Microsoft Azure
Azure AD Identity Protection
Users
User risk remediation policy
GarthF@contosobuild...
CONTOSO CLOUD
New
Resource groups
All resources
Recent
App Services
Virtual machines
SQL databases
Security Center
Subscriptions
Azure AD Identity Prote...
Browse
Add tiles
CLOSED
53
Users
AZURE AD IDENTITY PROTECTION
Apply a user risk policy for automatic mitigation.
USER
GLOBAL ADMI...
MFA
RISK LEVEL
RISK EVENTS
STATUS
LAST UPDATED (UTC)
Douglas Fife ✓ ✓ Medium 17 risk events At risk 8/3/2016 9:55 AM
Dana Kaufman ✓ ✓ Medium 19 risk events At risk 5/17/2016 4:53 AM
Joseph Dadzie ✓ ✓ Secured 2 risk events Remediated 8/4/2016 8:27 PM
Harry Slate High 2 risk events At risk 3/1/2016 8:28 PM
Lex Brown High 2 risk events At risk 4/4/2016 8:43 PM
Paul Tran Medium 2 risk events At risk 4/8/2016 11:29 PM
Alice Small Medium 19 risk events At risk 3/9/2016 8:46 PM
John Smith Medium 8 risk events At risk 7/10/2016 11:58 PM
Jennifer Davis Medium 8 risk events At risk 7/11/2016 1:02 AM
Chris Paul ✓ Medium 3 risk events At risk 5/18/2016 4:49 PM
Carrie Wong Medium 8 risk events At risk 2/12/2016 10:36 PM
Ken James Medium 8 risk events At risk 3/9/2016 8:47 PM
Edger De Graff Medium 3 risk events At risk 4/25/2016 6:18 PM
Mike Lee Medium 8 risk events At risk 7/11/2016 12:30 AM
Joseph Dadzie (G... ✓ Medium 4 risk events At risk 8/3/2016 10:34 PM
User risk remediat...
SETTINGS
Policy name
User risk remediation policy
Assignments
Users
All users
Conditions
User risk
Controls
Granting access
Block access
Review
Estimated impact
Number of users impacted
Enforce Policy
On
Off
Save
I'm Cortana. Ask me anything.

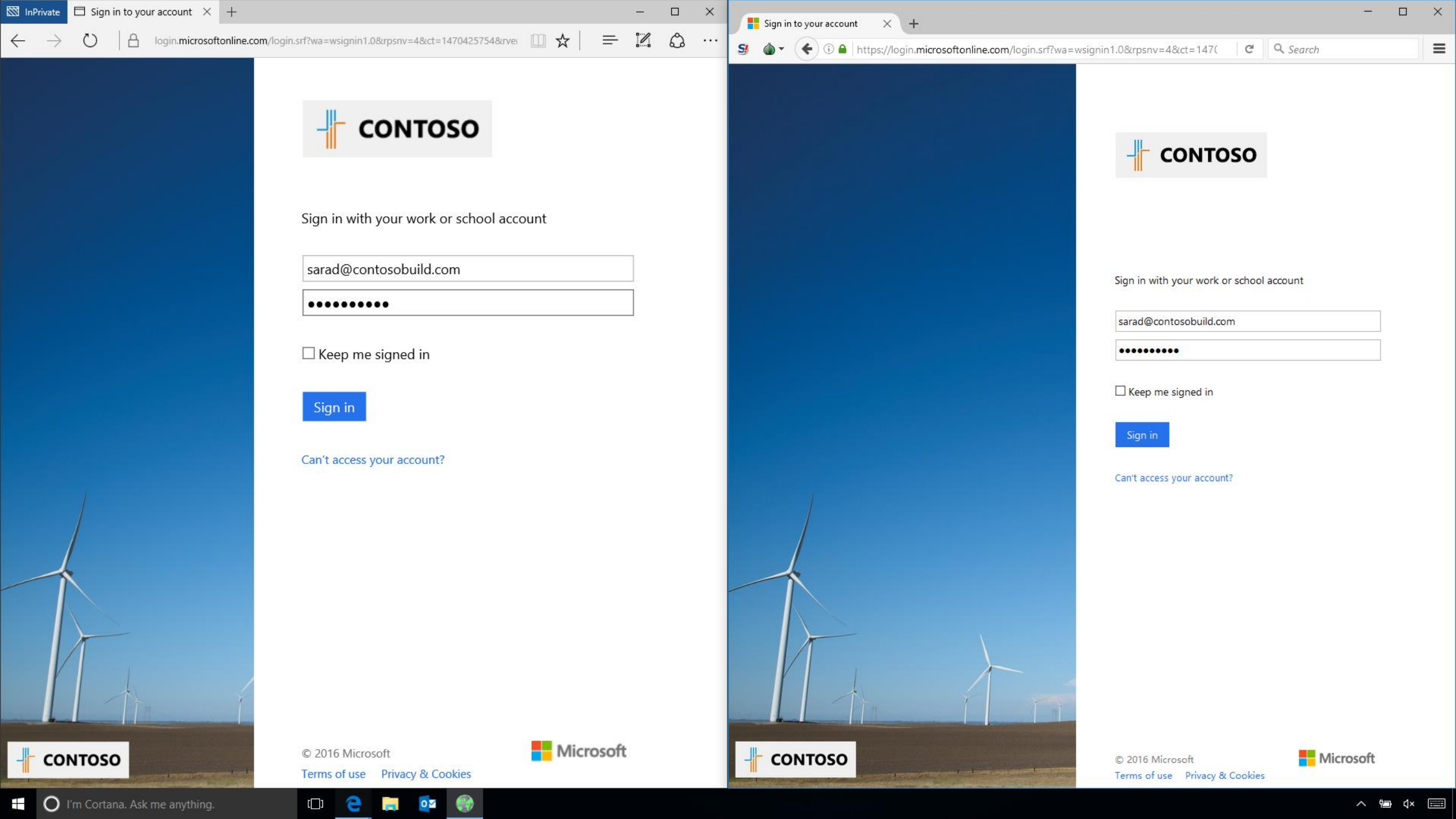

Conditions - Microsoft
portal.azure.com/#blade/Microsoft_AAD_ProtectionCenter/IdentitySecurityDashboardMenuBlade/Overview
Microsoft Azure
Azure AD Identity Protection
Users
User risk remediation policy
Conditions
GarthF@contosobuild...
CONTOSO CLOUD
New
Resource groups
All resources
Recent
App Services
Virtual machines
SQL databases
Security Center
Subscriptions
Azure AD Identity Prote...
Browse
for automatic mitigation.
GLOBAL ADMI...
MFA
RISK LEVEL
RISK EVENTS
STATUS
LAST UPDATED (UTC)
Medium 17 risk events At risk 8/3/2016 9:55 AM
Medium 19 risk events At risk 5/17/2016 4:53 AM
Secured 2 risk events Remediated 8/4/2016 8:27 PM
High 2 risk events At risk 3/1/2016 8:28 PM
High 2 risk events At risk 4/4/2016 8:43 PM
Medium 2 risk events At risk 4/8/2016 11:29 PM
Medium 19 risk events At risk 3/9/2016 8:46 PM
Medium 8 risk events At risk 7/10/2016 11:58 PM
Medium 8 risk events At risk 7/11/2016 1:02 AM
Medium 3 risk events At risk 5/18/2016 4:49 PM
Medium 8 risk events At risk 2/12/2016 10:36 PM
Medium 8 risk events At risk 3/9/2016 8:47 PM
Medium 3 risk events At risk 4/25/2016 6:18 PM
Medium 8 risk events At risk 7/11/2016 12:30 AM
Medium 4 risk events At risk 8/3/2016 10:34 PM
User risk remediat...
SETTINGS
Policy name
User risk remediation policy
Assignments
Users
All users
Conditions
User risk
Controls
Granting access
Block access
Review
Estimated impact
Number of users impacted
Enforce Policy
On
Off
Save
Conditions
SETTINGS
Select the conditions when the policy should apply. A condition that is not selected defaults to 'all'.
User risk
Medium and above
Done
I'm Cortana. Ask me anything.

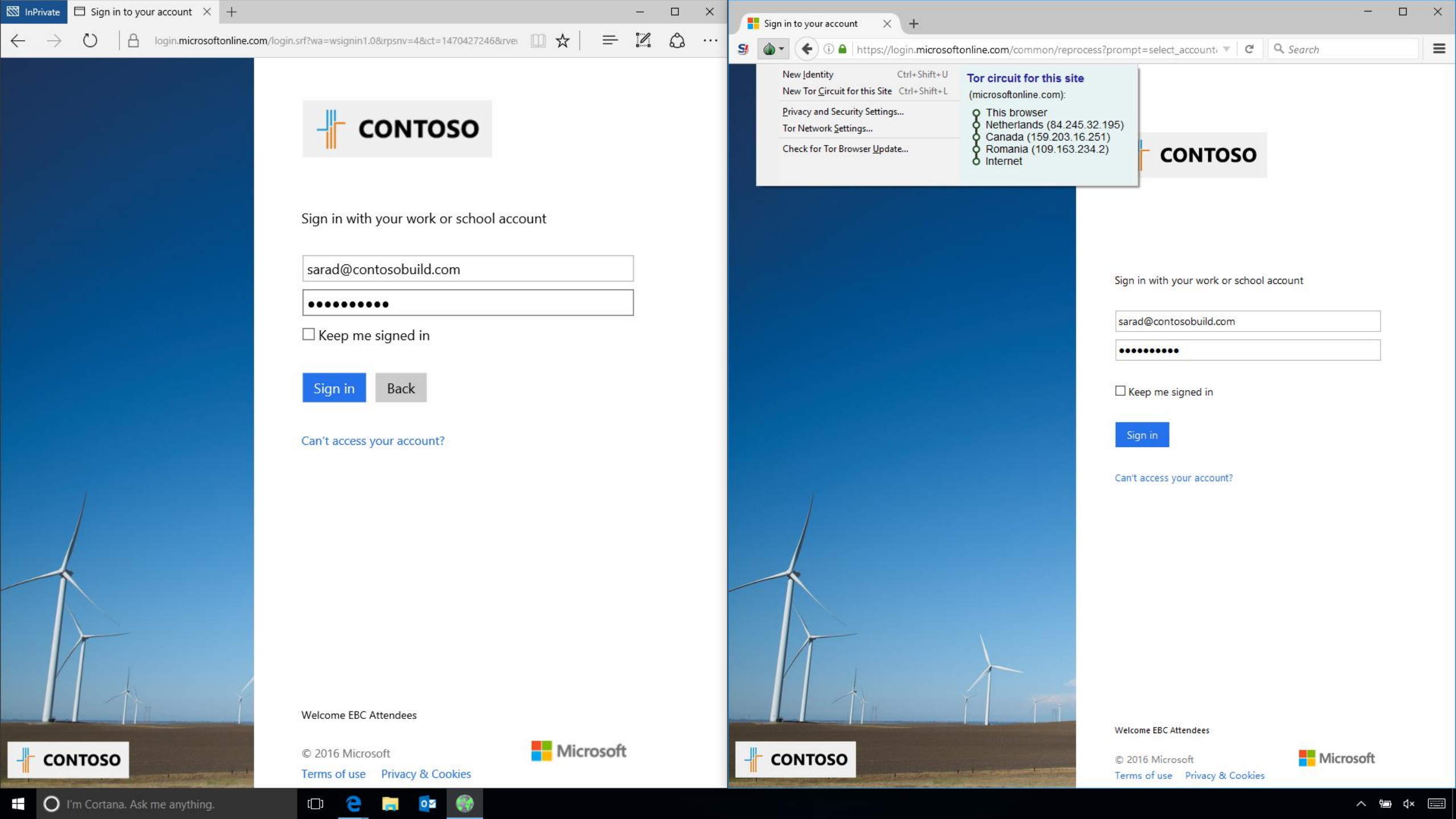

Dashboard
portal.azure.com/#blade/Microsoft_AAD_ProtectionCenter/IdentitySecurityDashboardMenuBlade/Overview
Microsoft Azure
Azure AD Identity Protection
Users
User risk remediation policy
Conditions
User risk
GarthF@contosobuild...
CONTOSO CLOUD
New
Resource groups
All resources
Recent
App Services
Virtual machines
SQL databases
Security Center
Subscriptions
Azure AD Identity Prote...
Browse
NTS
STATUS
LAST UPDATED (UTC)
vents At risk 8/3/2016 9:55 AM
vents At risk 5/17/2016 4:53 AM
ents Remediated 8/4/2016 8:27 PM
ents At risk 3/1/2016 8:28 PM
ents At risk 4/4/2016 8:43 PM
ents At risk 4/8/2016 11:29 PM
ents At risk 3/9/2016 8:46 PM
ents At risk 7/10/2016 11:58 PM
ents At risk 7/11/2016 1:02 AM
ents At risk 5/18/2016 4:49 PM
ents At risk 2/12/2016 10:36 PM
ents At risk 3/9/2016 8:47 PM
ents At risk 4/25/2016 6:18 PM
ents At risk 7/11/2016 12:30 AM
ents At risk 8/3/2016 10:34 PM
User risk remediat...
SETTINGS
Policy name
User risk remediation policy
Assignments
Users
All users
Conditions
User risk
Controls
Granting access
Block access
Review
Estimated impact
Number of users impacted
Enforce Policy
On
Off
Save
Conditions
SETTINGS
Select the conditions when the policy should apply. A condition that is not selected defaults to 'all'.
User risk
Medium and above
Done
User risk
SETTINGS
Info
Select the user risk level
Any risk level
Select specific risk level
Low and above
Medium and above
High
Select
I'm Cortana. Ask me anything.

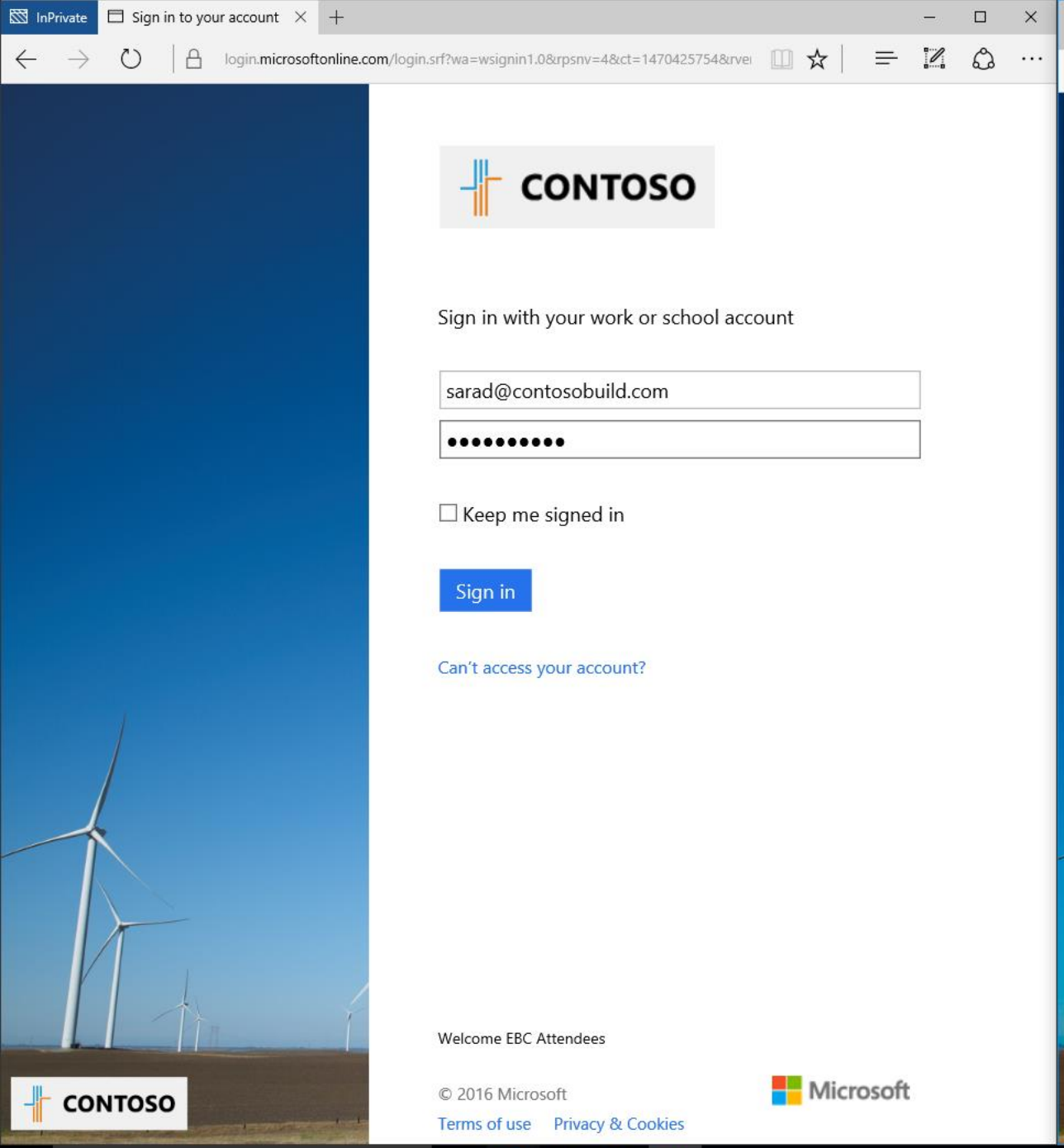

Conditions - Microsoft
portal.azure.com/#blade/Microsoft_AAD_ProtectionCenter/IdentitySecurityDashboardMenuBlade/Overview
Microsoft Azure
Azure AD Identity Protection
Users
User risk remediation policy
Conditions
GarthF@contosobuild...
CONTOSO CLOUD
New
Resource groups
All resources
Recent
App Services
Virtual machines
SQL databases
Security Center
Subscriptions
Azure AD Identity Prote...
Browse
for automatic mitigation.
GLOBAL ADMI...
MFA
RISK LEVEL
RISK EVENTS
STATUS
LAST UPDATED (UTC)
Medium 17 risk events At risk 8/3/2016 9:55 AM
Medium 19 risk events At risk 5/17/2016 4:53 AM
Secured 2 risk events Remediated 8/4/2016 8:27 PM
High 2 risk events At risk 3/1/2016 8:28 PM
High 2 risk events At risk 4/4/2016 8:43 PM
Medium 2 risk events At risk 4/8/2016 11:29 PM
Medium 19 risk events At risk 3/9/2016 8:46 PM
Medium 8 risk events At risk 7/10/2016 11:58 PM
Medium 8 risk events At risk 7/11/2016 1:02 AM
Medium 3 risk events At risk 5/18/2016 4:49 PM
Medium 8 risk events At risk 2/12/2016 10:36 PM
Medium 8 risk events At risk 3/9/2016 8:47 PM
Medium 3 risk events At risk 4/25/2016 6:18 PM
Medium 8 risk events At risk 7/11/2016 12:30 AM
Medium 4 risk events At risk 8/3/2016 10:34 PM
User risk remediat...
SETTINGS
Policy name
User risk remediation policy
Assignments
Users
All users
Conditions
User risk
Controls
Granting access
Block access
Review
Estimated impact
Number of users impacted
Enforce Policy
On
Off
Save
Granting access
USER RISK
Select the controls to be enforced.
Block access
Allow access
Require multi-factor authentication
Require Azure MFA registration
Require password change
Select
I'm Cortana. Ask me anything.

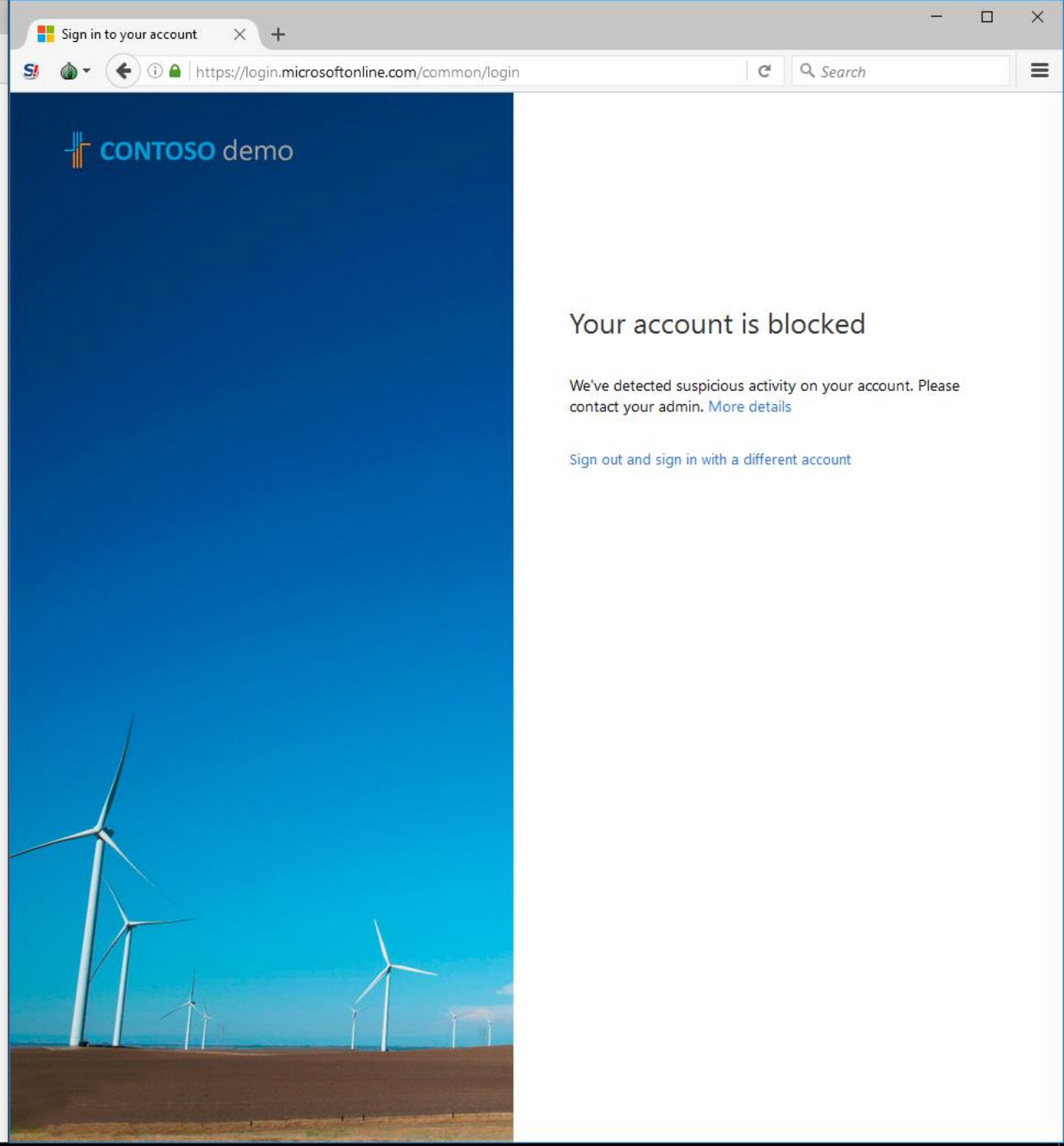

Conditions - Microsoft
portal.azure.com/#blade/Microsoft_AAD_ProtectionCenter/IdentitySecurityDashboardMenuBlade/Overview
Microsoft Azure
Azure AD Identity Protection
Users
User risk remediation policy
Conditions
GarthF@contosobuild...
CONTOSO CLOUD
New
Resource groups
All resources
Recent
App Services
Virtual machines
SQL databases
Security Center
Subscriptions
Azure AD Identity Prote...
Browse
y for automatic mitigation.
GLOBAL ADMI...
MFA
RISK LEVEL
RISK EVENTS
STATUS
LAST UPDATED (UTC)
Medium 17 risk events At risk 8/3/2016 9:55 AM
Medium 19 risk events At risk 5/17/2016 4:53 AM
Secured 2 risk events Remediated 8/4/2016 8:27 PM
High 2 risk events At risk 3/1/2016 8:28 PM
High 2 risk events At risk 4/4/2016 8:43 PM
Medium 2 risk events At risk 4/8/2016 11:29 PM
Medium 19 risk events At risk 3/9/2016 8:46 PM
Medium 8 risk events At risk 7/10/2016 11:58 PM
Medium 8 risk events At risk 7/11/2016 1:02 AM
Medium 3 risk events At risk 5/18/2016 4:49 PM
Medium 8 risk events At risk 2/12/2016 10:36 PM
Medium 8 risk events At risk 3/9/2016 8:47 PM
Medium 3 risk events At risk 4/25/2016 6:18 PM
Medium 8 risk events At risk 7/11/2016 12:30 AM
Medium 4 risk events At risk 8/3/2016 10:34 PM
User risk remediat...
SETTINGS
Policy name
User risk remediation policy
Assignments
Users
All users
Conditions
User risk
Controls
Granting access
Block access
Review
Estimated impact
Number of users impacted
Enforce Policy
On
Off
Save
Granting access
USER RISK
Select the controls to be enforced.
Block access
Allow access
Require multi-factor authentication
Require Azure MFA registration
Require password change
Select
I'm Cortana. Ask me anything.


Conditions - Microsoft
portal.azure.com/#blade/Microsoft_AAD_ProtectionCenter/IdentitySecurityDashboardMenuBlade/Overview
Microsoft Azure
Azure AD Identity Protection
Users
User risk remediation policy
Conditions
GarthF@contosobuild...
CONTOSO CLOUD
New
Resource groups
All resources
Recent
App Services
Virtual machines
SQL databases
Security Center
Subscriptions
Azure AD Identity Prote...
Browse
for automatic mitigation.
GLOBAL ADMI...
MFA
RISK LEVEL
RISK EVENTS
STATUS
LAST UPDATED (UTC)
Medium 17 risk events At risk 8/3/2016 9:55 AM
Medium 19 risk events At risk 5/17/2016 4:53 AM
Secured 2 risk events Remediated 8/4/2016 8:27 PM
High 2 risk events At risk 3/1/2016 8:28 PM
High 2 risk events At risk 4/4/2016 8:43 PM
Medium 2 risk events At risk 4/8/2016 11:29 PM
Medium 19 risk events At risk 3/9/2016 8:46 PM
Medium 8 risk events At risk 7/10/2016 11:58 PM
Medium 8 risk events At risk 7/11/2016 1:02 AM
Medium 3 risk events At risk 5/18/2016 4:49 PM
Medium 8 risk events At risk 2/12/2016 10:36 PM
Medium 8 risk events At risk 3/9/2016 8:47 PM
Medium 3 risk events At risk 4/25/2016 6:18 PM
Medium 8 risk events At risk 7/11/2016 12:30 AM
Medium 4 risk events At risk 8/3/2016 10:34 PM
User risk remediat...
SETTINGS
Policy name
User risk remediation policy
Assignments
Users
All users
Conditions
User risk
Controls
Granting access
Block access
Review
Estimated impact
Number of users impacted
Enforce Policy
On
Off
Save
Success
Your policy has been successfully saved.
Select the controls to be enforced.
Block access
Allow access
Require multi-factor authentication
Require Azure MFA registration
Require password change
Select
I'm Cortana. Ask me anything.


InPrivate
Sign in to your account
login.microsoftonline.com/login.srf?wa=wsignin1.0&rpsnv=4&ct=1470425754&rve
CONTOSO
Sign in with your work or school account
sarad@contosobuild.com
Keep me signed in
Sign in
Can't access your account?
© 2016 Microsoft
Terms of use
Privacy & Cookies
Microsoft
CONTOSO
Sign in to your account
https://login.microsoftonline.com/login.srf?wa=wsignin1.0&rpsnv=4&ct=147(
Search
CONTOSO
Sign in with your work or school account
sarad@contosobuild.com
Keep me signed in
Sign in
Can't access your account?
© 2016 Microsoft
Terms of use
Privacy & Cookies
Microsoft
CONTOSO
I'm Cortana. Ask me anything.


InPrivate
Sign in to your account
login.microsoftonline.com/login.srf?wa=wsignin1.0&rpsnv=4&ct=1470427246&rve
CONTOSO
Sign in with your work or school account
sarad@contosobuild.com
Keep me signed in
Sign in
Back
Can't access your account?
Welcome EBC Attendees
© 2016 Microsoft
Terms of use
Privacy & Cookies
Microsoft
CONTOSO
Sign in to your account
https://login.microsoftonline.com/common/reprocess?prompt=select_account
Search
New Identity Ctrl+Shift+U
New Tor Circuit for this Site Ctrl+Shift+L
Privacy and Security Settings...
Tor Network Settings...
Check for Tor Browser Update...
Tor circuit for this site
(microsoftonline.com):
This browser
Netherlands (84.245.32.195)
Canada (159.203.16.251)
Romania (109.163.234.2)
Internet
CONTOSO
Sign in with your work or school account
sarad@contosobuild.com
Keep me signed in
Sign in
Can't access your account?
Welcome EBC Attendees
© 2016 Microsoft
Terms of use
Privacy & Cookies
Microsoft
CONTOSO
I'm Cortana. Ask me anything.


InPrivate
Sign in to your account
login.microsoftonline.com/login.srf?wa=wsignin1.0&rpsnv=4&ct=1470425754&rve
CONTOSO
Sign in with your work or school account
sarad@contosobuild.com
Keep me signed in
Sign in
Can't access your account?
Welcome EBC Attendees
© 2016 Microsoft
Terms of use
Privacy & Cookies
Microsoft
CONTOSO
I'm Cortana. Ask me anything.


Sign in to your account
https://login.microsoftonline.com/common/login
Search
CONTOSO demo
Your account is blocked
We've detected suspicious activity on your account. Please contact your admin. More details
Sign out and sign in with a different account

InPrivate | Office Admin center pre

portal.office.com/AdminPortal/Home?switchtomoderndefault=true#/homepage

Admin center preview

Sara Davis

Home

Contoso Cloud

Search users, groups, settings or tasks

Go to the old admin center

Grow your business

Fill out your Bing places for business profile to help customers find yo

Edit profile

Users

- Add a user
- Delete a user
- Edit a user
- Reset a password

Billing

Total balance $0.00

- Change payment details
- View my bill

Office software

- Install my software
- Share the download link
- Software download settings
- Troubleshoot installation

Need help?

Feedback

Sign in to your account

https://login.microsoftonline.com/common/login

Search

CONTOSO demo

Your account is blocked

We've detected suspicious activity on your account. Please contact your admin. More details

Sign out and sign in with a different account

I'm Cortana. Ask me anything.

Reasons for Azure AD P2

- Privileged Identity Management - https://docs.microsoft.com/en-us/azure/active-directory/active-directory-privileged-identity-management-configure
- What is Azure AD Identity protection - https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview
- Azure AD Access reviews - https://docs.microsoft.com/en-us/azure/active-directory/active-directory-azure-ad-controls-manage-user-access-with-access-reviews
- Customizing of sharing emails - Administrators will be able to brand the outgoing sharing emails to recipients with their company logo. Note, this functionality will require Azure Active Directory Premium P2.