Understanding the top cybersecurity threats to your organization

Néstor Díaz
Pre-sales Solutions Manager
Inova Solutions Puerto Rico

Top Breaches in 2022

Ransomware

- Malicious software that encrypts your data.
- Often requires a very large payment
- Payments are **never** guaranteed to result in release of your data

Use of Stolen Credentials

- Via Brute-force attacks
- Via Malware
- Reused passwords from other sites
- Social attacks (phishing and pretexting)

Phishing

- Emails asking for information or credentials to be used maliciously later on commonly disguised as:
  - Invoices
  - Business partners
  - Telephone calls
  - Criminal call centers
  - Social Engineering

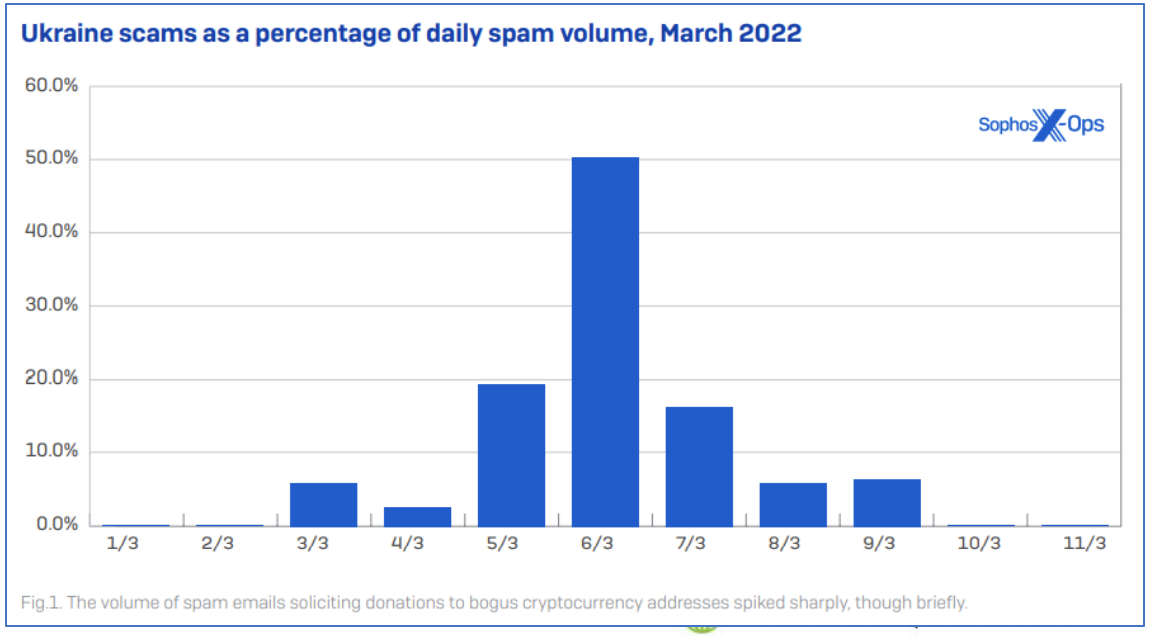
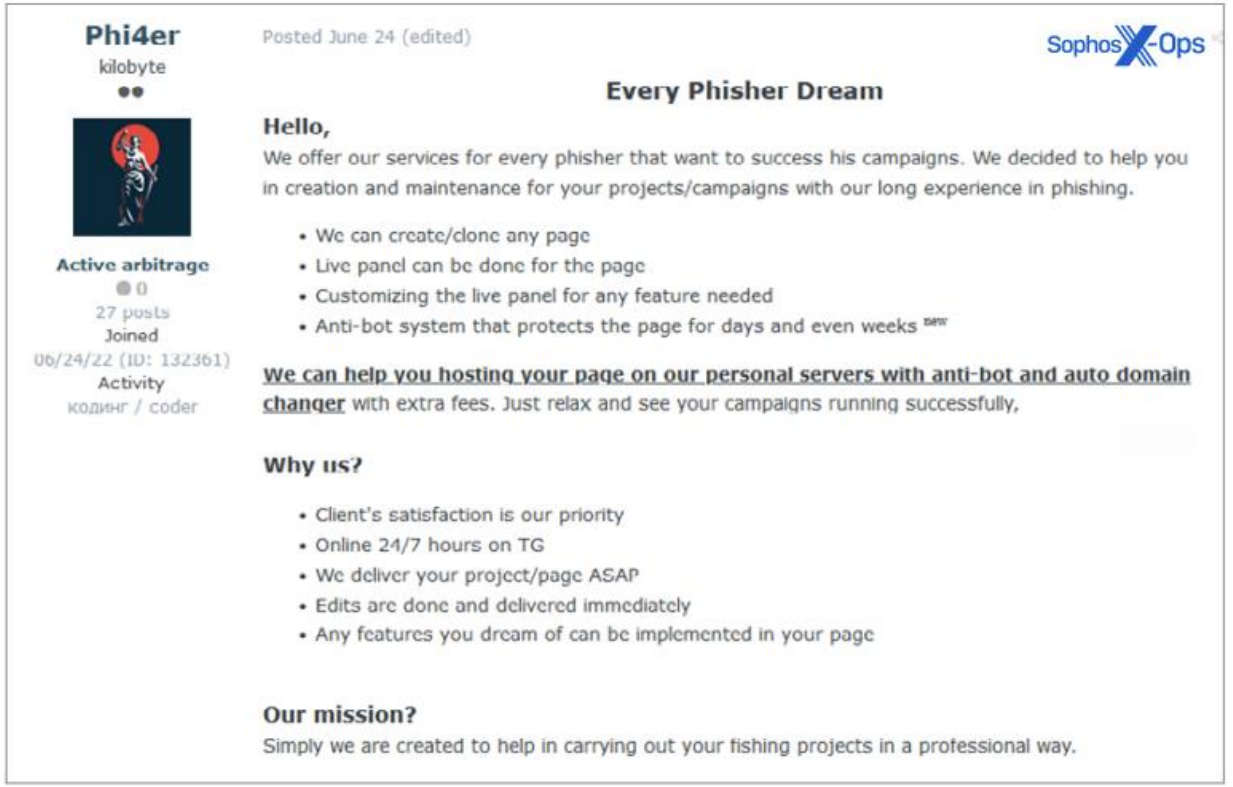


Fig.1. The volume of spam emails soliciting donations to bogus cryptocurrency addresses spiked sharply, though briefly.

Phishing (cont.)

- Guaranteed!
- 24/7 Service
- Expedited
- “Any features you dream”



Phi4er
kilobyte
●●

Active arbitrage
0
27 posts
Joined
06/24/22 (ID: 132361)
Activity
кодинг / coder

Posted June 24 (edited)

SophosX-Ops

Every Phisher Dream

Hello,
We offer our services for every phisher that want to success his campaigns. We decided to help you in creation and maintenance for your projects/campaigns with our long experience in phishing.

- We can create/clone any page
- Live panel can be done for the page
- Customizing the live panel for any feature needed
- Anti-bot system that protects the page for days and even weeks new

We can help you hosting your page on our personal servers with anti-bot and auto domain changer with extra fees. Just relax and see your campaigns running successfully,

Why us?

- Client's satisfaction is our priority
- Online 24/7 hours on TG
- We deliver your project/page ASAP
- Edits are done and delivered immediately
- Any features you dream of can be implemented in your page

Our mission?
Simply we are created to help in carrying out your fishing projects in a professional way.

Fig. 6. A suite of phishing services comes with customer-service guarantees.

Pretexting

- The “human version” of phishing
- Mostly Impersonating:
  - Partners
  - Bank employees
  - A superior in your own organization
- The main goals are:
  - Get banking information
  - Get a payment
  - Etc.

Misconfigurations

- Firewall Rules
- Unpatched Systems
- Antivirus without updates
- Windows / Linux OS Updates
- Mobile Device OS Updates
- Exposed to:
  - Trojans
  - Exploits

How do you know you're compromised

- Watch for anything out of the ordinary
  - Bank Statements
  - Phone Bills
  - Credit Card Statements
  - Email requests
  - Calls

How to avoid being a target

- **Use MFA**
- Do not reuse passwords
- Use complex password generators
- Do not click email links quickly
- Keep work and personal data/devices separate

How to avoid being a target

- Change default passwords
- Use endpoint protection
- Install software updates
- Keep backups

How to avoid being a target

- Configure the security tools at your disposal:
  - Identity management
  - Data classification and data loss prevention
  - Anti Spam, Anti Phishing, Anti Malware
  - Spoofing Protection
  - Mail tips
  - Device and app management

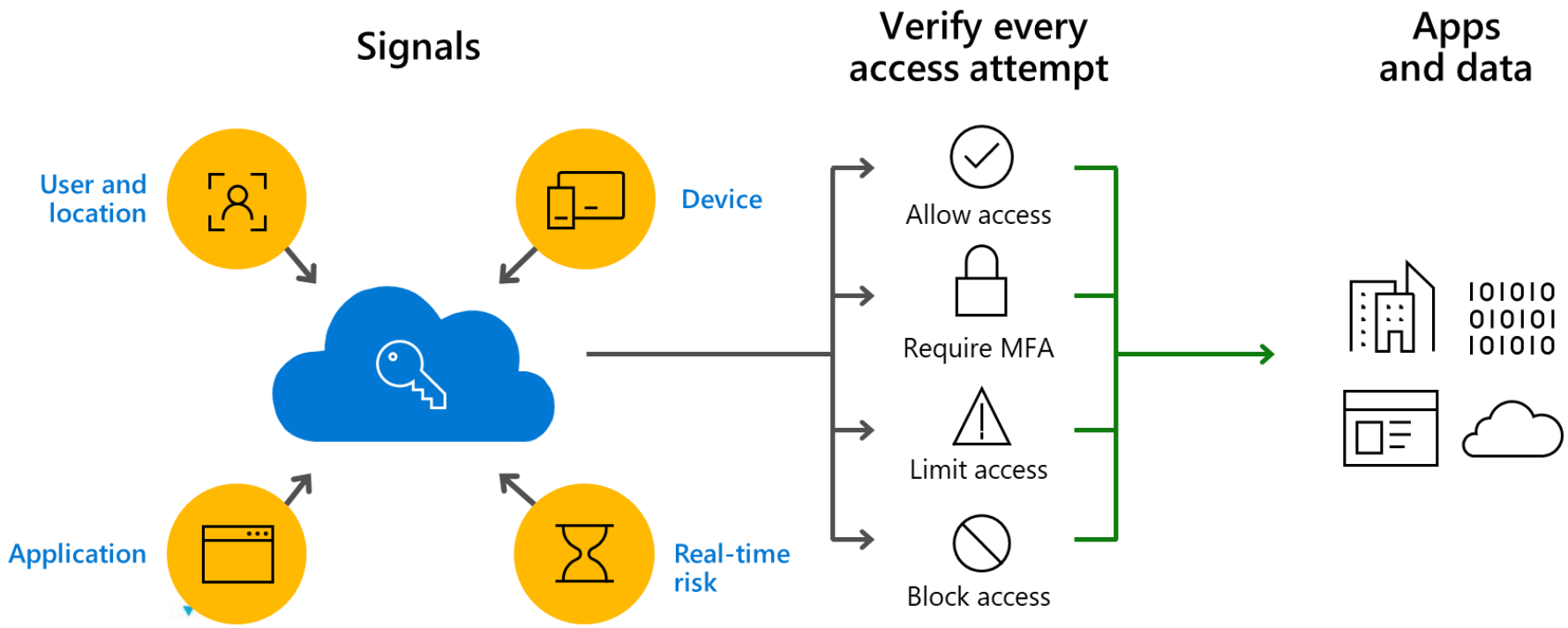
Security Quick Wins

- Configure MFA
- Perform Access Reviews

Security Quick Wins

- Configure MFA
- Perform Access Reviews
- Configure Security in Microsoft 365 / Azure (Not on by default)
  - Review Secure Score
  - Defender for Office 365
  - Conditional Access Policies (location)

Conditional Access Policies



Security Quick Wins

- Configure MFA
- Perform Access Reviews
- Configure Security in Microsoft 365 / Azure (Not on by default)
  - Review Secure Score
  - Defender for Office 365
  - Conditional Access Policies (location)

The Admin Experience
Data Classification

Home - Microsoft 365 security

https://security.microsoft.com/homepage

WOODGROVE | Microsoft 365 security

- Home
- Incidents
- Action center
- Reports
- Secure score
- Attack simulation training
- Hunting
- Classification
- Policies
- Permissions
- Settings
- More resources
- Customize navigation

Home

Office 365 Security & Compliance Center | What's new ? | Add cards

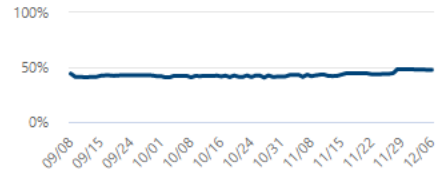
Microsoft Secure Score

Secure Score: 47.59%

411.64/865 points achieved

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Score last calculated 12/06



Identity	62.79%
Data	No data to show
Device	44.31%
Apps	86.67%
Infrastructure	No data to show

Improve your score | View history

Users at risk

104 users at risk

High Risk | Medium Risk | Low risk

View all users

Device compliance

20% noncompliant

Intune device compliance status

Compliant | Noncompliant | In grace period | Not evaluated

View details

Microsoft Security Intelligence feed

Tweets by @MsftSecIntel

Microsoft Security Intelligence @MsftSecIntel

Microsoft 365 Defender customers can take full advantage of signals & alerts from Microsoft Defender for Identity, combined w/ behavioral events & detections from Microsoft Defender for Endpoint, to detect Netlogon exploitation attempts, associated device process, file activity https://twitter.com/MSThreatProtect/status/1333544318858973184

Dec 1, 2020

Microsoft Security Intelligence @MsftSecIntel

New blog: The threat actor BISMUTH, which has been running increasingly complex targeted attacks, deployed coin miners in campaigns from July to August 2020. Learn how the group tried to stay under the radar using threats perceived

Embed | View on Twitter

Devices with active malware

No affected devices

Intune-managed devices with active, unresolved malware

Updated 11/28/2020

Active | No Active Malware

View details

Users with threat detections

Users with threat detections

User	Alerts
Oana Enache	2
Bob Smith	1
Guillaume Aubert	1
Tracy Yu	1
Audrina Clifton	1

Devices at risk

Privileged OAuth apps

Home - Microsoft 365 security

https://security.microsoft.com/homepage

WOODGROVE | Microsoft 365 security

- Home
- Incidents
- Action center
- Reports
- Secure score
- Attack simulation training
- Hunting
- Classification
  - Sensitivity labels
  - Retention labels
  - Sensitive info types
  - Label analytics
- Policies
- Permissions
- Settings
- More resources
- Customize navigation

Home

Office 365 Security & Compliance Center | What's new ? | Add cards

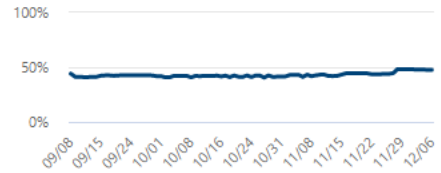
Microsoft Secure Score

Secure Score: 47.59%

411.64/865 points achieved

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Score last calculated 12/06



Identity	62.79%
Data	No data to show
Device	44.31%
Apps	86.67%
Infrastructure	No data to show

Improve your score | View history

Users at risk

104 users at risk

High Risk | Medium Risk | Low risk

View all users

Device compliance

20% noncompliant

Intune device compliance status

Compliant | Noncompliant | In grace period | Not evaluated

View details

Devices with active malware

No affected devices

Intune-managed devices with active, unresolved malware

Updated 11/28/2020

Active | No Active Malware

View details

Users with threat detections

Users with threat detections

User	Alerts
Oana Enache	2
Bob Smith	1
Guillaume Aubert	1
Tracy Yu	1
Audrina Clifton	1

Microsoft Security Intelligence feed

Tweets by @MsftSecIntel

Microsoft Security Intelligence @MsftSecIntel

Microsoft 365 Defender customers can take full advantage of signals & alerts from Microsoft Defender for Identity, combined w/ behavioral events & detections from Microsoft Defender for Endpoint, to detect Netlogon exploitation attempts, associated device process, file activity https://twitter.com/MSThreatProtect/status/1333544318858973184

Dec 1, 2020

Microsoft Security Intelligence @MsftSecIntel

New blog: The threat actor BISMUTH, which has been running increasingly complex targeted attacks, deployed coin miners in campaigns from July to August 2020. Learn how the group tried to stay under the radar using threats perceived

Embed | View on Twitter

Devices at risk

Privileged OAuth apps

Home
Incidents
Action center
Reports
Secure score
Attack simulation training
Hunting
Classification
Sensitivity labels
Retention labels
Sensitive info types
Label analytics
Policies
Permissions
Settings
More resources
Customize navigation

Sensitivity labels

Labels | Label policies | Auto-labeling

New feature in preview

Extend labeling to assets in Azure Purview

When you turn on labeling for Azure Purview, you'll be able to apply your Microsoft 365 sensitivity labels to assets such as SQL columns, files in Azure Blob Storage, and more. Learn more about labeling for Azure Purview

Turn on

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels

You can now create sensitivity labels with privacy and access control settings for Teams, SharePoint sites, and Microsoft 365 Groups. To do this, you must first complete these steps to enable the feature.

Create a label | Publish labels | Refresh

Name	Order	Scope	Created by	Last modified
General	0 - lowest	File, Email	Joey Cruz	11/20/2019
Confidential	1	File, Email	Joey Cruz	11/20/2019
All Employees	2	File, Email	Joey Cruz	6/26/2020
Anyone (not protected)	3	File, Email	Joey Cruz	6/26/2020
Highly Confidential	4	File, Email	Joey Cruz	6/26/2020
All Employees	5	File, Email	Joey Cruz	6/30/2020

Home
Incidents
Action center
Reports
Secure score
Attack simulation training
Hunting
Classification
Sensitivity labels
Retention labels
Sensitive info types
Label analytics
Policies
Permissions
Settings
More resources
Customize navigation

When you turn on labeling for Azure Purview, you'll be able to apply your Microsoft 365 sensitivity labels to assets such as SQL columns, files in Azure Blob Storage, and more. Learn more about labeling for Azure Purview

Turn on

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels

You can now create sensitivity labels with privacy and access control settings for Teams, SharePoint sites, and Microsoft 365 Groups. To do this, you must first complete these steps to enable the feature.

+ Create a label | Publish labels | Refresh

Name	Order	Scope	Created by	Last modified
General	0 - lowest	File, Email	Joey Cruz	11/20/2019
Confidential	1	File, Email	Joey Cruz	11/20/2019
All Employees	2	File, Email	Joey Cruz	6/26/2020
Anyone (not protected)	3	File, Email	Joey Cruz	6/26/2020
Highly Confidential	4	File, Email	Joey Cruz	6/26/2020
All Employees	5	File, Email	Joey Cruz	6/30/2020
Anyone (not protected)	6	File, Email	Joey Cruz	6/26/2020
Project TNT	7	File, Email	Joey Cruz	6/26/2020
Project DND	8 - highest	File, Email	Anna Smith	11/25/2020

0 items selected 9 items loaded

Home
Incidents
Action center
Reports
Secure score
Attack simulation training
Hunting
Classification
Sensitivity labels
Retention labels
Sensitive info types
Label analytics
Policies
Permissions
Settings
More resources
Customize navigation

Sensitivity labels

Labels | Label policies | Auto-labeling

New feature in preview

Extend labeling to assets in Azure Purview

When you turn on labeling for Azure Purview, you'll be able to apply your Microsoft 365 sensitivity labels to assets such as SQL columns, files in Azure Blob Storage, and more. Learn more about labeling for Azure Purview

Turn on

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels

You can now create sensitivity labels with privacy and access control settings for Teams, SharePoint sites, and Microsoft 365 Groups. To do this, you must first complete these steps to enable the feature.

Create a label | Publish labels | Refresh

Name	Order	Scope	Created by	Last modified
General	0 - lowest	File, Email	Joey Cruz	11/20/2019
Confidential	1	File, Email	Joey Cruz	11/20/2019
All Employees	2	File, Email	Joey Cruz	6/26/2020
Anyone (not protected)	3	File, Email	Joey Cruz	6/26/2020
Highly Confidential	4	File, Email	Joey Cruz	6/26/2020
All Employees	5	File, Email	Joey Cruz	6/30/2020

Home
Incidents
Action center
Reports
Secure score
Attack simulation training
Hunting
Classification
Sensitivity labels
Retention labels
Sensitive info types
Label analytics
Policies
Permissions
Settings
More resources
Customize navigation

Sensitivity labels

Labels | Label policies | Auto-labeling

Create sensitivity label policies to publish one or more labels to your users' Office apps (like Outlook and Word), SharePoint sites, and Office 365 groups. Once published, users can apply the labels to protect their content. Learn more about sensitivity label policies

Publish label | Refresh

2 items

Name	Created by	Last modified
Woodgrove_Compliance_General	Joey Cruz	2/24/2020
Project DND policy	Anna Smith	6/26/2020

Home
Incidents
Action center
Reports
Secure score
Attack simulation training
Hunting
Classification
Sensitivity labels
Retention labels
Sensitive info types
Label analytics
Policies
Permissions
Settings
More resources
Customize navigation

Sensitivity labels

Labels | Label policies | Auto-labeling

Create sensitivity label policies to publish one or more labels to your users' Office apps (like Outlook and Word), SharePoint sites, and Office 365 groups. Or
label policies

Publish label | Refresh

Name	Created by	Last modified
Woodgrove_Compliance_General	Joey Cruz	2/24/2020
Project DND policy	Anna Smith	6/26/2020

Woodgrove_Compliance_General

Edit policy | Delete policy

Name
Woodgrove_Compliance_General

Description
General Compliance

Published labels
Highly Confidential
All Employees/All Employees
All Employees/All Employees
Project TNT
Confidential
Anyone (not protected)/Anyone (not protected)
General
Anyone (not protected)/Anyone (not protected)

Published to
All

Policy settings
Label is mandatory
Users must provide justification to remove a label or lower its classification
Use custom URL to provide more information

Close

The Admin Experience
Identity and Device Management

Home
Incidents
Action center
Reports
Secure score
Attack simulator
Hunting
Classification
Policies
Settings
More resources
Customize navigation

Microsoft Secure Score

Score last calculated 11/02 ; 4:00 PM

Overview | Improvement actions | History | Metrics & trends

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

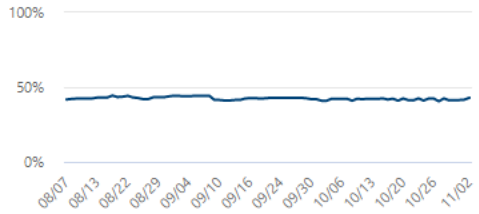
Applied filters: Filter

Your secure score

Include

Secure Score: 42.92%

360.92/841 points achieved



Breakdown points by: Category

Identity	56.82%
Data	No data to show
Device	39.65%
Apps	86.67%

Points achieved Opportunity

Actions to review

Regressed	To address	Planned	Risk accepted	Recently added	Recently updated
12	77	2	5	0	0

Top improvement actions

Improvement action	Score impact	Status	Category
Block credential stealing from the Windows local security authorit...	+1.07%	To address	Device
Use advanced protection against ransomware	+1.07%	To address	Device
Block Win32 API calls from Office macros	+1.07%	To address	Device
Block execution of potentially obfuscated scripts	+1.07%	To address	Device
Block Office applications from injecting code into other processes	+1.07%	To address	Device
Block executable content from email client and webmail	+1.07%	To address	Device
Block process creations originating from PSExec and WMI comma...	+1.07%	To address	Device
Block Office communication application from creating child proce...	+1.07%	To address	Device

View all

Comparison

Your score	42.92%
Organizations like yours	48.02%
Custom comparison	Not yet created

Manage comparisons

Resources

Read about Secure Score capabilities
Learn about the improvement actions and how to improve your score.

Partner experience updates
Learn about temporary incompatibility with Identity Secure Score and the Graph API.

History

Messages from Microsoft

Home
Incidents
Action center
Reports
Secure score
Attack simulator
Hunting
Classification
Policies
Settings
More resources
Customize navigation

Microsoft Secure Score

Score last calculated 11/02 ; 4:00 PM

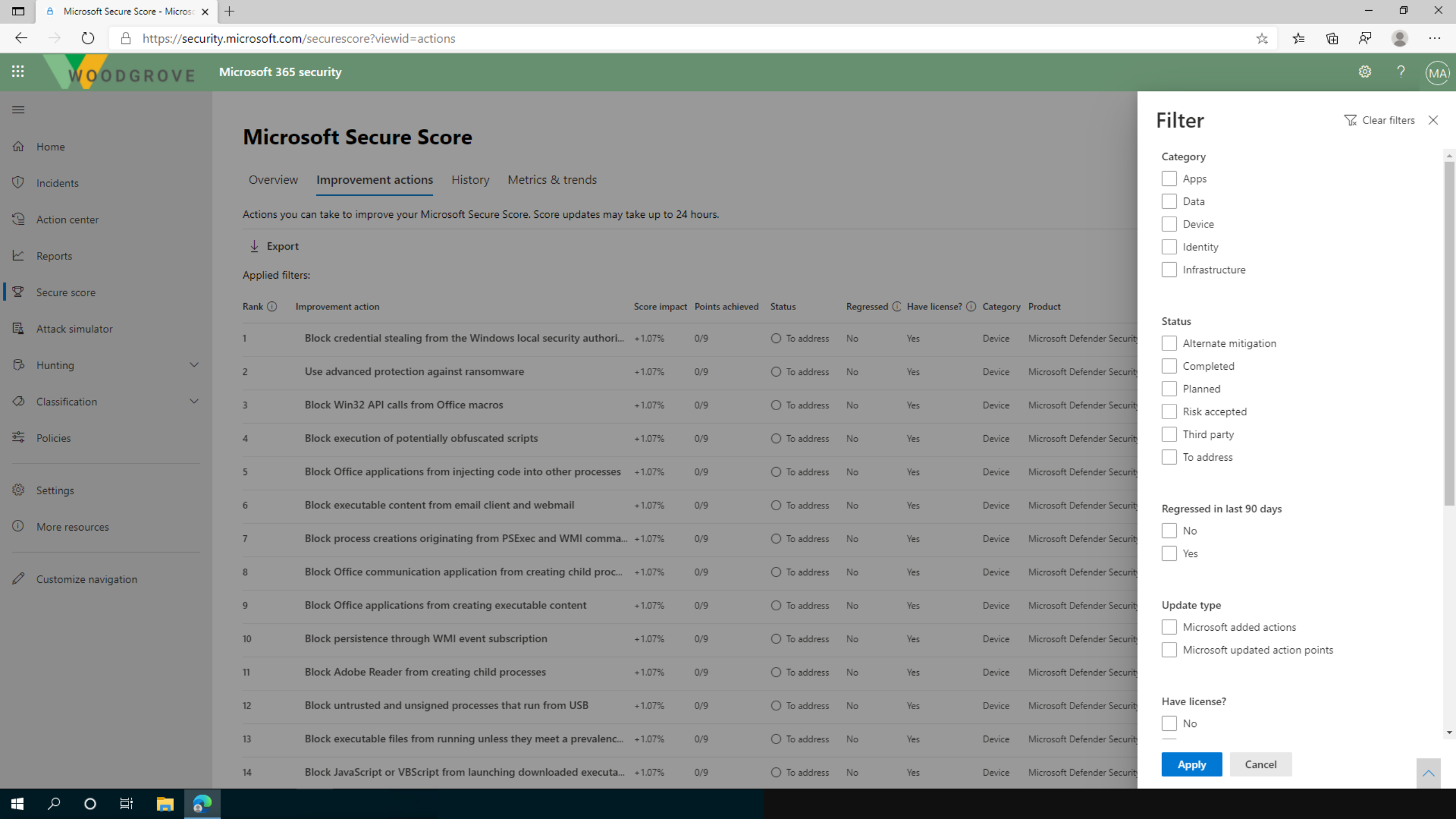
Overview | Improvement actions | History | Metrics & trends

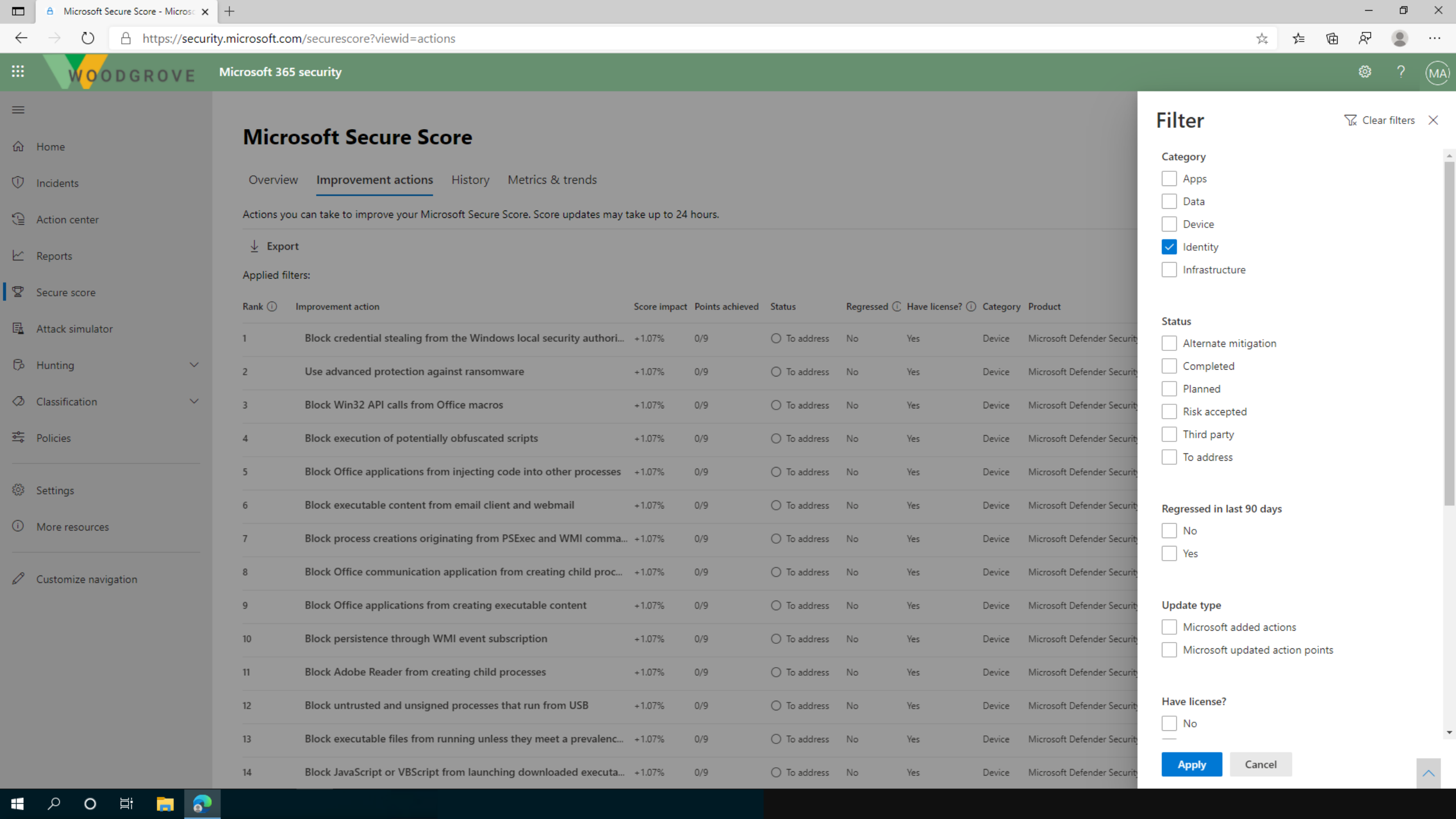
Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Export | 133 items | Search | Filter | Group by

Applied filters:

Rank	Improvement action	Score impact	Points achieved	Status	Regressed	Have license?	Category	Product	Last synced	Microsoft update	Notes
1	Block credential stealing from the Windows local security authori...	+1.07%	0/9	To address	No	Yes	Device	Microsoft Defender Security ...	11/4/2020	None	None
2	Use advanced protection against ransomware	+1.07%	0/9	To address	No	Yes	Device	Microsoft Defender Security ...	11/4/2020	None	None
3	Block Win32 API calls from Office macros	+1.07%	0/9	To address	No	Yes	Device	Microsoft Defender Security ...	11/4/2020	None	None
4	Block execution of potentially obfuscated scripts	+1.07%	0/9	To address	No	Yes	Device	Microsoft Defender Security ...	11/4/2020	None	None
5	Block Office applications from injecting code into other processes	+1.07%	0/9	To address	No	Yes	Device	Microsoft Defender Security ...	11/4/2020	None	None
6	Block executable content from email client and webmail	+1.07%	0/9	To address	No	Yes	Device	Microsoft Defender Security ...	11/4/2020	None	None
7	Block process creations originating from PSExec and WMI comma...	+1.07%	0/9	To address	No	Yes	Device	Microsoft Defender Security ...	11/4/2020	None	None
8	Block Office communication application from creating child proc...	+1.07%	0/9	To address	No	Yes	Device	Microsoft Defender Security ...	11/4/2020	None	None
9	Block Office applications from creating executable content	+1.07%	0/9	To address	No	Yes	Device	Microsoft Defender Security ...	11/4/2020	None	None
10	Block persistence through WMI event subscription	+1.07%	0/9	To address	No	Yes	Device	Microsoft Defender Security ...	11/4/2020	None	None
11	Block Adobe Reader from creating child processes	+1.07%	0/9	To address	No	Yes	Device	Microsoft Defender Security ...	11/4/2020	None	None
12	Block untrusted and unsigned processes that run from USB	+1.07%	0/9	To address	No	Yes	Device	Microsoft Defender Security ...	11/4/2020	None	None
13	Block executable files from running unless they meet a prevalenc...	+1.07%	0/9	To address	No	Yes	Device	Microsoft Defender Security ...	11/4/2020	None	None
14	Block JavaScript or VBScript from launching downloaded executa...	+1.07%	0/9	To address	No	Yes	Device	Microsoft Defender Security ...	11/4/2020	None	None


Microsoft Secure Score - Microsc
https://security.microsoft.com/securescore?viewid=actions
WOODGROVE
Microsoft 365 security
MA
Home
Incidents
Action center
Reports
Secure score
Attack simulator
Hunting
Classification
Policies
Settings
More resources
Customize navigation
Microsoft Secure Score
Overview
Improvement actions
History
Metrics & trends
Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.
Export
Applied filters:
Rank
Improvement action
Score impact
Points achieved
Status
Regressed
Have license?
Category
Product
1 Block credential stealing from the Windows local security authori... +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
2 Use advanced protection against ransomware +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
3 Block Win32 API calls from Office macros +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
4 Block execution of potentially obfuscated scripts +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
5 Block Office applications from injecting code into other processes +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
6 Block executable content from email client and webmail +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
7 Block process creations originating from PSExec and WMI comma... +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
8 Block Office communication application from creating child proc... +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
9 Block Office applications from creating executable content +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
10 Block persistence through WMI event subscription +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
11 Block Adobe Reader from creating child processes +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
12 Block untrusted and unsigned processes that run from USB +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
13 Block executable files from running unless they meet a prevalenc... +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
14 Block JavaScript or VBScript from launching downloaded executa... +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
Filter
Clear filters
Category
Apps
Data
Device
Identity
Infrastructure
Status
Alternate mitigation
Completed
Planned
Risk accepted
Third party
To address
Regressed in last 90 days
No
Yes
Update type
Microsoft added actions
Microsoft updated action points
Have license?
No
Apply
Cancel


Microsoft Secure Score - Microsc
https://security.microsoft.com/securescore?viewid=actions
WOODGROVE
Microsoft 365 security
Home
Incidents
Action center
Reports
Secure score
Attack simulator
Hunting
Classification
Policies
Settings
More resources
Customize navigation
Microsoft Secure Score
Overview
Improvement actions
History
Metrics & trends
Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.
Export
Applied filters:
Rank
Improvement action
Score impact
Points achieved
Status
Regressed
Have license?
Category
Product
1 Block credential stealing from the Windows local security authori... +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
2 Use advanced protection against ransomware +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
3 Block Win32 API calls from Office macros +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
4 Block execution of potentially obfuscated scripts +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
5 Block Office applications from injecting code into other processes +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
6 Block executable content from email client and webmail +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
7 Block process creations originating from PSExec and WMI comma... +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
8 Block Office communication application from creating child proc... +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
9 Block Office applications from creating executable content +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
10 Block persistence through WMI event subscription +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
11 Block Adobe Reader from creating child processes +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
12 Block untrusted and unsigned processes that run from USB +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
13 Block executable files from running unless they meet a prevalenc... +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
14 Block JavaScript or VBScript from launching downloaded executa... +1.07% 0/9 To address No Yes Device Microsoft Defender Securit
Filter
Clear filters
Category
Apps
Data
Device
Identity
Infrastructure
Status
Alternate mitigation
Completed
Planned
Risk accepted
Third party
To address
Regressed in last 90 days
No
Yes
Update type
Microsoft added actions
Microsoft updated action points
Have license?
No
Apply
Cancel

Home
Incidents
Action center
Reports
Secure score
Attack simulator
Hunting
Classification
Policies
Settings
More resources
Customize navigation

Microsoft Secure Score

Score last calculated 11/02 ; 4:00 PM

Overview | Improvement actions | History | Metrics & trends

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Export | 26 items | Search | Filter | Group by

Applied filters: Category: Identity

Rank	Improvement action	Score impact	Points achieved	Status	Regressed	Have license?	Category	Product	Last synced	Microsoft update	Notes
1	Turn on sign-in risk policy	+0.83%	0/7	To address	Yes	Yes	Identity	Azure Active Directory	11/3/2020	None	None
2	Turn on user risk policy	+0.83%	0/7	Planned	Yes	Yes	Identity	Azure Active Directory	11/3/2020	None	None
3	Resolve unsecure account attributes	+0.59%	0/5	To address	No	Yes	Identity	Azure ATP	11/3/2020	11/2/2020 04:00 PM	None
4	Disable Print spooler service on domain controllers	+0.59%	0/5	To address	No	Yes	Identity	Azure ATP	11/3/2020	11/2/2020 04:00 PM	None
5	Remove dormant accounts from sensitive groups	+0.59%	0/5	To address	No	Yes	Identity	Azure ATP	11/3/2020	11/2/2020 04:00 PM	None
6	Protect and manage local admin passwords with Microsoft LAPS	+0.59%	0/5	To address	No	Yes	Identity	Azure ATP	11/3/2020	11/2/2020 04:00 PM	None
7	Modify unsecure Kerberos delegations to prevent impersonation	+0.59%	0/5	To address	Yes	Yes	Identity	Azure ATP	11/3/2020	11/2/2020 04:00 PM	None
8	Ensure all users can complete multi-factor authentication for secu...	+1.07%	4.13/9	Risk accepted	No	Yes	Identity	Azure Active Directory	11/3/2020	None	
9	Enable policy to block legacy authentication	+0.95%	3.53/8	Planned	Yes	Yes	Identity	Azure Active Directory	11/3/2020	None	None
10	Require MFA for administrative roles	+1.19%	7.95/10	To address	Yes	Yes	Identity	Azure Active Directory	11/3/2020	None	None
11	Configure VPN integration	+0.12%	0/1	Risk accepted	No	Yes	Identity	Azure ATP	11/3/2020	None	None
12	Do not expire passwords	+0.95%	8/8	Completed	No	Yes	Identity	Azure Active Directory	11/3/2020	None	None
13	Enable Password Hash Sync if hybrid	+0.59%	5/5	Risk accepted	No	Yes	Identity	Azure Active Directory	11/3/2020	None	None
14	Reduce lateral movement path risk to sensitive entities	+0.59%	5/5	Completed	No	Yes	Identity	Azure ATP	11/3/2020	11/2/2020 04:00 PM	None

Requiring multi-factor authentication (MFA) for all administrative roles makes it harder for attackers to access accounts. Administrative roles have higher permissions than typical users. If any of those accounts are compromised, critical devices and data is open to attack.

Points achieved 7.95/10

History 8 events

Last synced 11/3/2020

Manage | Share | Save and close | Cancel

Action plan

Save is not available because you have read only permissions. Learn more

Update status for this improvement action. Note: some statuses are system generated and can't be updated.

- (○) Completed
- (◉) To address
- (○) Planned
- (○) Risk accepted
- (○) Resolved through third party
- (○) Resolved through alternate mitigation

Notes:

Write a note

Tags:

At a glance

Category: Identity

Protects against: Password Cracking, Account Breach, Elevation of Privilege

Product: Azure Active Directory

User impact

First, users with administrative roles need to register for MFA. After each admin is registered, your policies then determine when they're prompted for the additional authentication factors.

Users affected

All of your Microsoft 365 users with administrator roles

RA MD MR +32

Show all users

Implementation

Prerequisites

✓ You have Azure Active Directory Premium P2.

Next steps

Standard implementation: If your organization doesn't have complex security requirements, you can enable security defaults to block legacy authentication and require registration and enablement of MFA for all users. Learn more about how to turn on security defaults.

Custom implementation: Set up Azure Multi-Factor Authentication policies to protect devices and data that are accessible by your users with administrative roles: In the Azure AD Conditional Access portal

1. Select + **New Policy**
2. Go to Assignments > Users and groups > Include > choose **Select users and groups** > check **Directory roles**
3. At a minimum, select the following roles:

- Security administrator
- Exchange service administrator
- Global administrator
- Conditional Access administrator
- SharePoint administrator
- Helpdesk administrator
- Billing administrator
- User administrator
- Authentication administrator

4. Go to Cloud apps or actions > Cloud apps > Include > select **All cloud apps** (and don't exclude any apps)
5. Under Access controls > Grant > select **Grant access** > check **Require multi-factor**

Related reports None **Related tasks** None

Conditional Access | Policies

Azure Active Directory

Policies
Insights and reporting
Diagnose and solve problems

Manage

Named locations
Custom controls (Preview)
Terms of use
VPN connectivity
Classic policies

Troubleshooting + Support

New support request

New policy | What If | Refresh | Got feedback?

New Conditional Access policies now apply to all client app types when not configured, including legacy authentication and Exchange ActiveSync. →

Policy Name	State
RO - Block EAS and Legacy Auth	Report-only
CA01 - All Apps - Blocked Countries & Banned IPs - All Users	Off
RO - Require Hybrid Azure AD Join or MFA	Report-only
RO - Require compliant device or HAADJ to register security info	Report-only
CA02- Customer Data Apps - Compliant Device - Customer Data	On
CA03 - Security Registration - HAADJ OR Compliant Device	Off
CA04 - Block Sensitive Apps from High sign-in risk users	On
CA05 - MCAS Session Control - All Users	On
CA07 - AWS - Application Dev Restriction	On
CAX - TOU - All Woodgrove (and Guest) Users	On
CA00 - SPO/EXO - Limted access unmanged devices - All Users	On
CA08 - MFA - All Apps - All Users	On
CA09 - Admins - Block Legacy Auth	On
RO - Require MFA for guest users	Report-only
RO - Require MFA or Compliant Device to access Office 365	Report-only
CA10 - Require MFA for VPN Access	On
Vinayak-AADIPTest	On
CA11 - Require MFA for Forrester admin	On
CA50 Require MFA for Office 365 (Bsides)	On

Load more

Microsoft Secure Score - Micros

RO - Require MFA or Compliant

https://portal.azure.com/#blade/Microsoft_AAD_IAM/ConditionalAccessBlade/Policies

Microsoft Azure

Search resources, services, and docs (G+/)

admin@Woodgrove.ms
WOODGROVE

Home > Conditional Access >

RO - Require MFA or Compliant Device to access Office 365

Conditional access policy

Delete

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

RO - Require MFA or Compliant Device to ...

Assignments

Users and groups
All users included and specific use...

Cloud apps or actions
1 app included

Conditions
1 condition selected

Access controls

Grant
2 controls selected

Session
0 controls selected

Enable policy

Report-only | On | Off

https://aka.ms/capolicyhowto

Conditional Access | Policies

Azure Active Directory

Policies
Insights and reporting
Diagnose and solve problems

Manage

Named locations
Custom controls (Preview)
Terms of use
VPN connectivity
Classic policies

Troubleshooting + Support

New support request

New policy | What If | Refresh | Got feedback?

New Conditional Access policies now apply to all client app types when not configured, including legacy authentication and Exchange ActiveSync. →

Policy Name	State
RO - Block EAS and Legacy Auth	Report-only
CA01 - All Apps - Blocked Countries & Banned IPs - All Users	Off
RO - Require Hybrid Azure AD Join or MFA	Report-only
RO - Require compliant device or HAADJ to register security info	Report-only
CA02- Customer Data Apps - Compliant Device - Customer Data	On
CA03 - Security Registration - HAADJ OR Compliant Device	Off
CA04 - Block Sensitive Apps from High sign-in risk users	On
CA05 - MCAS Session Control - All Users	On
CA07 - AWS - Application Dev Restriction	On
CAX - TOU - All Woodgrove (and Guest) Users	On
CA00 - SPO/EXO - Limted access unmanged devices - All Users	On
CA08 - MFA - All Apps - All Users	On
CA09 - Admins - Block Legacy Auth	On
RO - Require MFA for guest users	Report-only
RO - Require MFA or Compliant Device to access Office 365	Report-only
CA10 - Require MFA for VPN Access	On
Vinayak-AADIPTest	On
CA11 - Require MFA for Forrester admin	On
CA50 Require MFA for Office 365 (Bsides)	On
Password Change Required for Risky Users	Report-only

Load more

Microsoft Secure Score - Micros

Password Change Required for R

https://portal.azure.com/#blade/Microsoft_AAD_IAM/ConditionalAccessBlade/Policies

Microsoft Azure

Search resources, services, and docs (G+/)

admin@Woodgrove.ms
WOODGROVE

Home > Conditional Access >

Password Change Required for Risky Users

Conditional access policy

Delete

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Password Change Required for Risky Users

Assignments

Users and groups
All users included and specific use...

Cloud apps or actions
All cloud apps

Conditions
1 condition selected

Access controls

Grant
1 control selected

Session
0 controls selected

Enable policy

Report-only | On | Off

Save

https://aka.ms/capolicyhowto

Microsoft Secure Score - Micros | Grant - Microsoft Azure

https://portal.azure.com/#blade/Microsoft_AAD_IAM/ConditionalAccessBlade/Policies

Microsoft Azure | Search resources, services, and docs (G+/) | admin@Woodgrove.ms WOODGROVE

Home > Conditional Access >

Password Change Required for Risky Users

Conditional access policy

Delete

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Password Change Required for Risky Users

Assignments

Users and groups
All users included and specific use...

Cloud apps or actions
All cloud apps

Conditions
1 condition selected

Access controls

Grant
1 control selected

Session
0 controls selected

Enable policy

Report-only | On | Off

Save

https://aka.ms/capolicyhowto

Grant

Control user access enforcement to block or grant access. Learn more

- Block access
- Grant access

- [x] Require multi-factor authentication
- [ ] Require device to be marked as compliant
- [ ] Require Hybrid Azure AD joined device
- [ ] Require approved client app
  See list of approved client apps
- [ ] Require app protection policy (Preview)
  See list of policy protected client apps
- [x] Require password change (Preview)

"Require password change" can only be used when policy is assigned to "All cloud apps"

- [ ] Duo Mfa
- [ ] Woodgrove - Sensitive App TOU
- [ ] Woodgrove - All Users TOU - English
- [ ] Woodgrove - All Users TOU - Spanish
- [ ] Hipstabank - All Users TOU

For multiple controls

- Require all the selected controls

Select

Microsoft Secure Score - Micros | Grant - Microsoft Azure

https://portal.azure.com/#blade/Microsoft_AAD_IAM/ConditionalAccessBlade/Policies

Microsoft Azure | Search resources, services, and docs (G+/) | admin@Woodgrove.ms WOODGROVE

Home > Conditional Access >

Password Change Required for Risky Users

Conditional access policy

Delete

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Password Change Required for Risky Users

Assignments

Users and groups
All users included and specific use...

Cloud apps or actions
All cloud apps

Conditions
1 condition selected

Access controls

Grant
1 control selected

Session
0 controls selected

Enable policy

Report-only | On | Off

Save

Grant

Control user access enforcement to block or grant access. Learn more

- Block access
- Grant access

- [ ] Require multi-factor authentication
- [ ] Require device to be marked as compliant
- [ ] Require Hybrid Azure AD joined device
- [ ] Require approved client app
  See list of approved client apps
- [ ] Require app protection policy (Preview)
  See list of policy protected client apps
- [x] Require password change (Preview)

"Require password change" can only be used when policy is assigned to "All cloud apps"

- [ ] Duo Mfa
- [ ] Woodgrove - Sensitive App TOU
- [ ] Woodgrove - All Users TOU - English
- [ ] Woodgrove - All Users TOU - Spanish
- [ ] Hipstabank - All Users TOU

For multiple controls

- Require all the selected controls

Select

Microsoft Secure Score - Micros | Grant - Microsoft Azure

https://portal.azure.com/#blade/Microsoft_AAD_IAM/ConditionalAccessBlade/Policies

Microsoft Azure | Search resources, services, and docs (G+/) | admin@Woodgrove.ms WOODGROVE

Home >

Conditional Access | Policies

Azure Active Directory

Updating Password Change Required for ... 9:47 AM
Updating Password Change Required for Risky Users

- Policies
- Insights and reporting
- Diagnose and solve problems

Manage

- Named locations
- Custom controls (Preview)
- Terms of use
- VPN connectivity
- Classic policies

Troubleshooting + Support

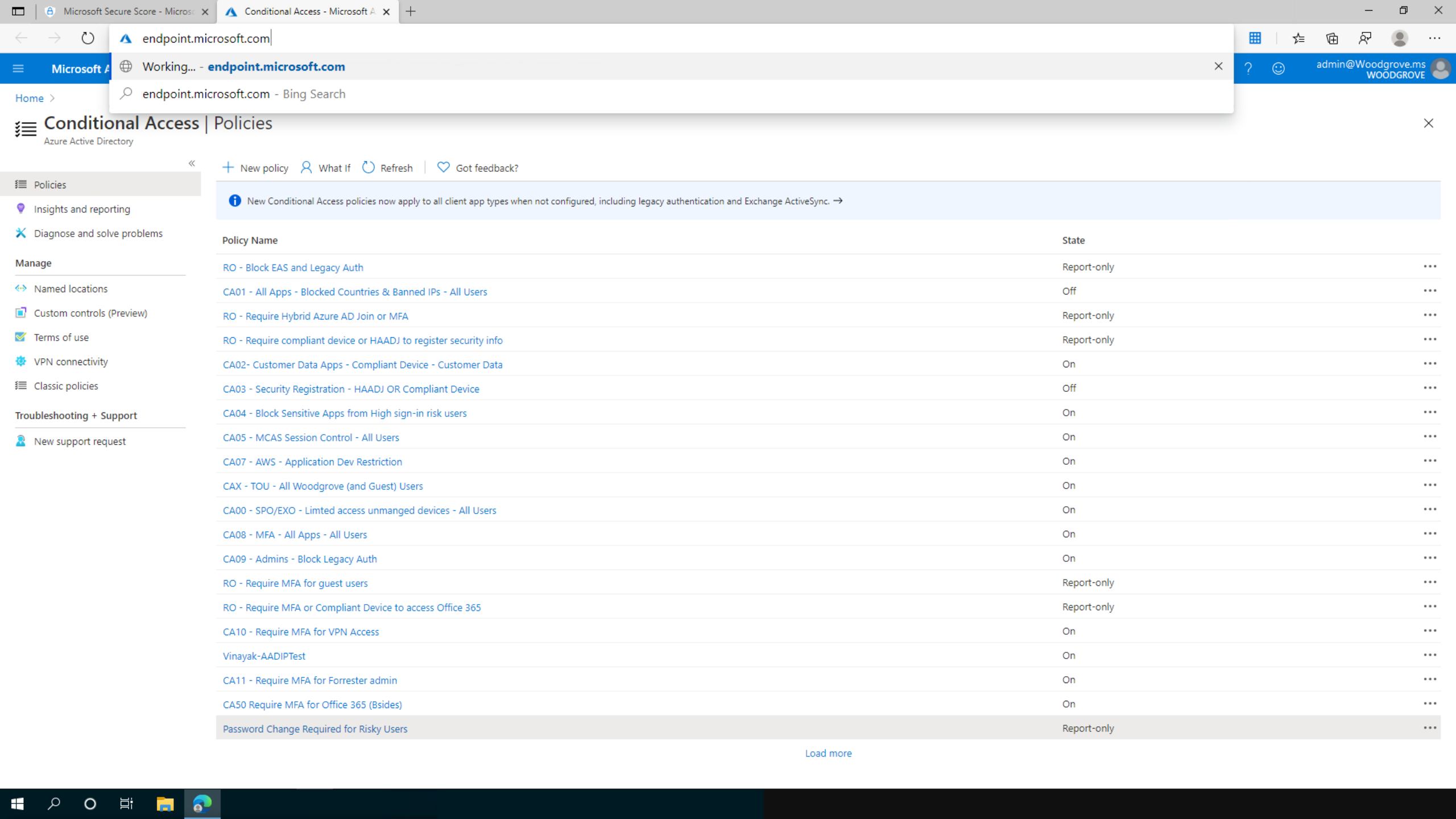
- New support request

New policy | What If | Refresh | Got feedback?

New Conditional Access policies now apply to all client app types when not configured, including legacy authentication and Exchange ActiveSync. →

Policy Name	State
RO - Block EAS and Legacy Auth	Report-only
CA01 - All Apps - Blocked Countries & Banned IPs - All Users	Off
RO - Require Hybrid Azure AD Join or MFA	Report-only
RO - Require compliant device or HAADJ to register security info	Report-only
CA02- Customer Data Apps - Compliant Device - Customer Data	On
CA03 - Security Registration - HAADJ OR Compliant Device	Off
CA04 - Block Sensitive Apps from High sign-in risk users	On
CA05 - MCAS Session Control - All Users	On
CA07 - AWS - Application Dev Restriction	On
CAX - TOU - All Woodgrove (and Guest) Users	On
CA00 - SPO/EXO - Limted access unmanged devices - All Users	On
CA08 - MFA - All Apps - All Users	On
CA09 - Admins - Block Legacy Auth	On
RO - Require MFA for guest users	Report-only
RO - Require MFA or Compliant Device to access Office 365	Report-only
CA10 - Require MFA for VPN Access	On
Vinayak-AADIPTest	On
CA11 - Require MFA for Forrester admin	On
CA50 Require MFA for Office 365 (Bsides)	On
Password Change Required for Risky Users	Report-only

Load more



Microsoft Secure Score - Microso | Conditional Access - Microsoft A

endpoint.microsoft.com

Working... - **endpoint.microsoft.com**

endpoint.microsoft.com - Bing Search

Microsoft A

admin@Woodgrove.ms
WOODGROVE

Home >

Conditional Access | Policies

Azure Active Directory

- Policies
- Insights and reporting
- Diagnose and solve problems

Manage

- Named locations
- Custom controls (Preview)
- Terms of use
- VPN connectivity
- Classic policies

Troubleshooting + Support

- New support request

+ New policy | What If | Refresh | Got feedback?

New Conditional Access policies now apply to all client app types when not configured, including legacy authentication and Exchange ActiveSync. →

Policy Name	State
RO - Block EAS and Legacy Auth	Report-only
CA01 - All Apps - Blocked Countries & Banned IPs - All Users	Off
RO - Require Hybrid Azure AD Join or MFA	Report-only
RO - Require compliant device or HAADJ to register security info	Report-only
CA02- Customer Data Apps - Compliant Device - Customer Data	On
CA03 - Security Registration - HAADJ OR Compliant Device	Off
CA04 - Block Sensitive Apps from High sign-in risk users	On
CA05 - MCAS Session Control - All Users	On
CA07 - AWS - Application Dev Restriction	On
CAX - TOU - All Woodgrove (and Guest) Users	On
CA00 - SPO/EXO - Limted access unmanged devices - All Users	On
CA08 - MFA - All Apps - All Users	On
CA09 - Admins - Block Legacy Auth	On
RO - Require MFA for guest users	Report-only
RO - Require MFA or Compliant Device to access Office 365	Report-only
CA10 - Require MFA for VPN Access	On
Vinayak-AADIPTest	On
CA11 - Require MFA for Forrester admin	On
CA50 Require MFA for Office 365 (Bsides)	On
Password Change Required for Risky Users	Report-only

Load more

Microsoft Secure Score - Micros | Woodgrove - Microsoft Endpoint

https://endpoint.microsoft.com/#home

Microsoft Endpoint Manager admin center

admin@Woodgrove.ms
WOODGROVE

- Home
- Dashboard
- All services
- FAVORITES
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Woodgrove

Home | Microsoft Managed Desktop

Status and alerts

Tenant status

Account status
Active

Service health
Healthy

Connector status
Healthy

Resource alerts

Device compliance
3 devices not in compliance

Device enrollment
No Intune enrollment failures

Device configuration
No configuration failures

Client apps
1 installation failure

Guided scenarios

Deploy Edge for mobile

Configure Edge for use at work and deploy it to the iOS and Android devices managed by your organization.

Start

Try out a cloud-managed PC

Quickly set up an example PC and user to experience the cloud managed modern desktop.

Start

News and support

Intune Customer Success blog

Intune certificate updates: Action may be required for continued connectivity

Microsoft Defender for Endpoint (preview) risk evaluation now included in device compliance on iOS

Intune Public Preview – Enroll Android Enterprise dedicated devices into Azure AD Shared device mode

See all >

What's happening in Intune

What's new in Microsoft Intune

Features in development

UI updates for Intune end-user apps

Home
Dashboard
All services
FAVORITES
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

Devices | Overview

Search (Ctrl+/)
Overview
All devices
Monitor
By platform
Windows
iOS/iPadOS
macOS
Android
Device enrollment
Enroll devices
Policy
Compliance policies
Conditional access
Configuration profiles
Scripts
Group Policy analytics (preview)
Windows 10 update rings
Windows 10 feature updates (...
Update policies for iOS/iPadOS
Enrollment restrictions
eSIM cellular profiles (Preview)
Policy sets
Other
Device clean-up rules

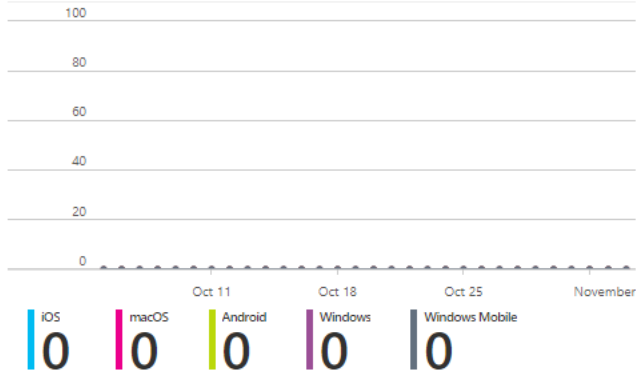
Enrollment status | Enrollment alerts | Compliance status | Configuration status | Software update status

Intune enrolled devices

LAST UPDATED 11/4/2020, 8:08:46 AM

Platform	Devices
Windows	22
Android	1
iOS/iPadOS	0
macOS	0
Windows Mobile	0
Total	23

Enrollment failures by OS



Top enrollment failures this week

No data to display

Home
Dashboard
All services
FAVORITES
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

iOS/iPadOS | iOS/iPadOS devices

Search (Ctrl+/)
iOS/iPadOS devices
iOS/iPadOS enrollment
iOS/iPadOS policies
Compliance policies
Configuration profiles
Update policies for iOS/iPadOS

Refresh | Filter | Columns | Export | Bulk Device Actions

Filters applied: OS

Search by IMEI, serial number, email, user principal name, device name, management name, phone number, model, or manufacturer

Showing 0 to 0 of 0 records

< Previous Page 0 of 0 Next >

Device name	Managed by	Ownership	Compliance	OS	OS version	Last check-in	Enrolled by user UPN
No results.							

Home
Dashboard
All services
FAVORITES
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

iOS/iPadOS | Compliance policies

Search (Ctrl+/)
iOS/iPadOS devices
iOS/iPadOS enrollment

iOS/iPadOS policies
Compliance policies
Configuration profiles
Update policies for iOS/iPadOS

Create Policy | Columns | Filter | Refresh | Export

Configured Windows compliance policies use the Machine Risk Score setting but do not have an active Microsoft Defender ATP connector.
Click here to setup a connector.

Search by name

Policy Name	Platform	Policy Type	Assigned	Last Modified
Enterprise Compliance Policy	iOS/iPadOS	iOS compliance policy	No	10/11/17, 1:23 PM
iOS_BYOD	iOS/iPadOS	iOS compliance policy	Yes	6/19/20, 2:28 PM

Home
Dashboard
All services
FAVORITES
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

iOS_BYOD

Device compliance policy

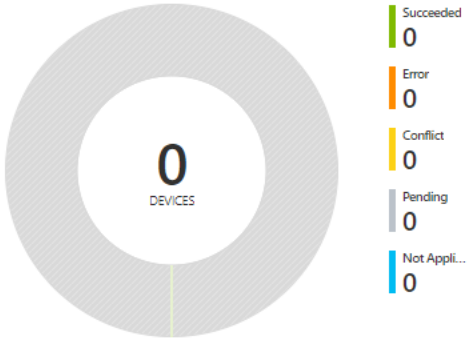
Search (Ctrl+/)
Overview
Manage
Properties
Monitor
Device status
User status
Per-setting status

Delete

Essentials

Profile type	: iOS compliance policy	Assigned	: Yes
Platform supported	: iOS/iPadOS	Groups assigned	: 1
Groups excluded	: 0		

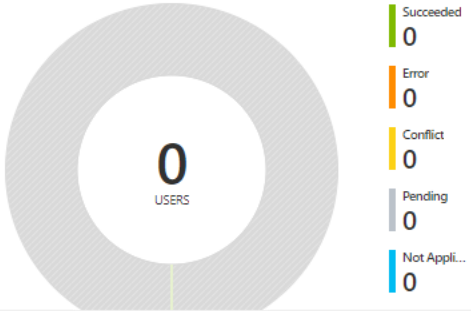
Policy assignment status — iOS/iPadOS devices



Assigned to non-iOS/iPadOS devices

0

Policy assignment status — iOS/iPadOS users



Home
Dashboard
All services
FAVORITES
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

iOS_BYOD | Properties

Device compliance policy

Search (Ctrl+/)
Overview
Manage
Properties
Monitor
Device status
User status
Per-setting status

Basics Edit

Name	iOS_BYOD
Description	--
Platform	iOS/iPadOS
Profile type	iOS compliance policy

Compliance settings Edit

Device Health

Jailbroken devices	Block
Require the device to be at or under the Device Threat Level	Medium

System Security

Require a password to unlock mobile devices	Require
Minimum password length	4
Required password type	Numeric
Number of non-alphanumeric characters in password	0
Maximum minutes after screen lock before password is required	4 hours
Maximum minutes of inactivity until screen locks	15 Minutes
Password expiration (days)	1000
Number of previous passwords to prevent reuse	1

Actions for noncompliance Edit

Action	Schedule	Message template	Additional recipients (via email)
Mark device noncompliant	Immediately		
Send push notification to end user	Immediately		

Home
Dashboard
All services
FAVORITES
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

Home >

Apps | Overview

Search (Ctrl+/)
Overview
All apps
Monitor

By platform
Windows
iOS/iPadOS
macOS
Android

Policy
App protection policies
App configuration policies
iOS app provisioning profiles
S mode supplemental policies
Policies for Office apps
Policy sets

Other
App selective wipe
App categories
E-books

Help and support
Help and support

Essentials

Tenant name : woodgrove.ms
Tenant location : North America 0101
MDM authority : Microsoft Intune
Account status : Active

Installation status | App protection policy status

Top installation failures by devices

Microsoft Authenticator	iOS	1

Apps with installation failures

1

Home
Dashboard
All services
FAVORITES
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

Apps | App protection policies

Search (Ctrl+/)
Overview
All apps
Monitor

By platform
Windows
iOS/iPadOS
macOS
Android

Policy
App protection policies
App configuration policies
iOS app provisioning profiles
S mode supplemental policies
Policies for Office apps
Policy sets

Other
App selective wipe
App categories
E-books

Help and support
Help and support

Create policy | Refresh | Columns | Export

Search by policy

Policy	Deployed	Updated	Platform	Management type	Apps
iOS - Outlook / OneDrive / Excel / P...	Yes	10/28/19, 1:54 PM	iOS/iPadOS	All app types	5
Woodgrove Interns Office365 MAM	Yes	6/19/20, 3:28 PM	iOS/iPadOS	All app types	2

Home
Dashboard
All services
FAVORITES
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

Intune App Protection

iOS - Outlook / OneDrive / Excel / Power BI

Search (Ctrl+/)
Overview
Manage
Properties
Help and support
Diagnose and solve problems

Delete policy

Essentials

Description : Sales Org - Device Access app protection
Platform : iOS/iPadOS
Apps : 5
Management type : All app types

User check-in per app

User check-in per app	CHECK-IN COUNT
Microsoft Outlook	0
Microsoft OneNote	0
Microsoft OneDrive	0
Microsoft Teams	0
Microsoft To-Do	0

Users checked in

0

Home
Dashboard
All services
FAVORITES
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support

Intune App Protection | Properties

iOS - Outlook / OneDrive / Excel / Power BI

Search (Ctrl+/)
Overview
Manage
Properties
Help and support
Diagnose and solve problems

Basics Edit

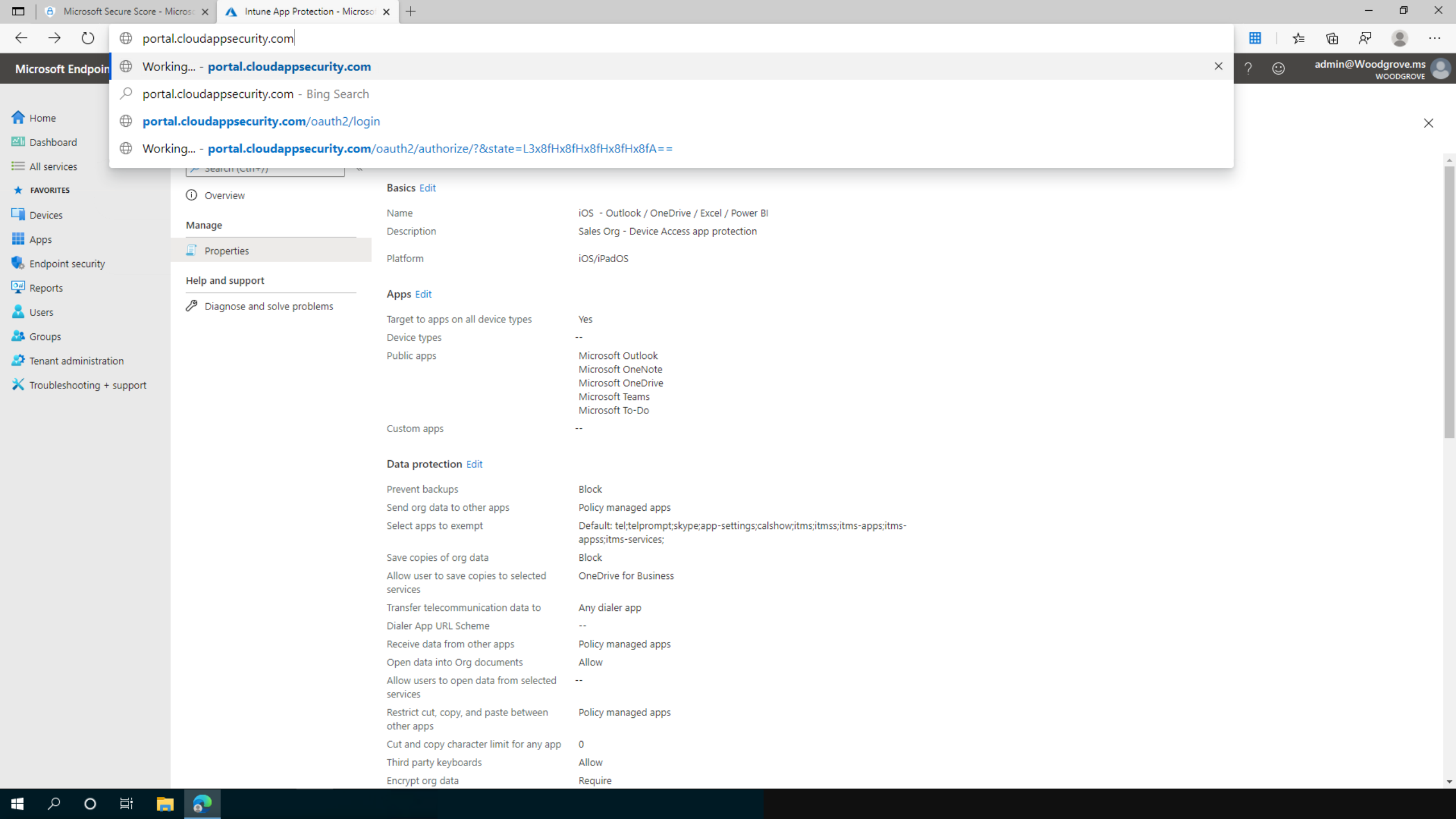
Name	iOS - Outlook / OneDrive / Excel / Power BI
Description	Sales Org - Device Access app protection
Platform	iOS/iPadOS

Apps Edit

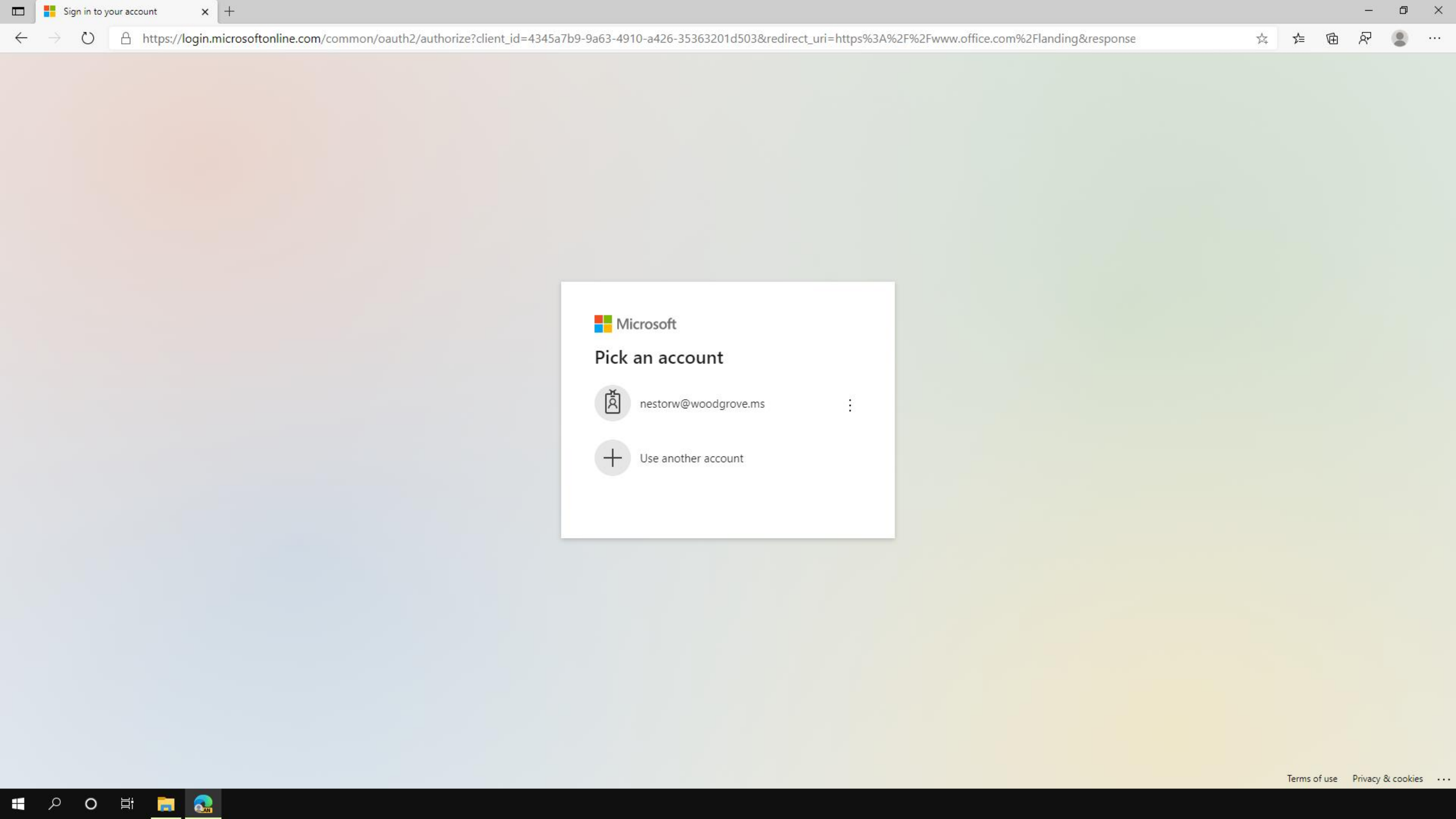
Target to apps on all device types	Yes
Device types	--
Public apps	Microsoft Outlook Microsoft OneNote Microsoft OneDrive Microsoft Teams Microsoft To-Do
Custom apps	--

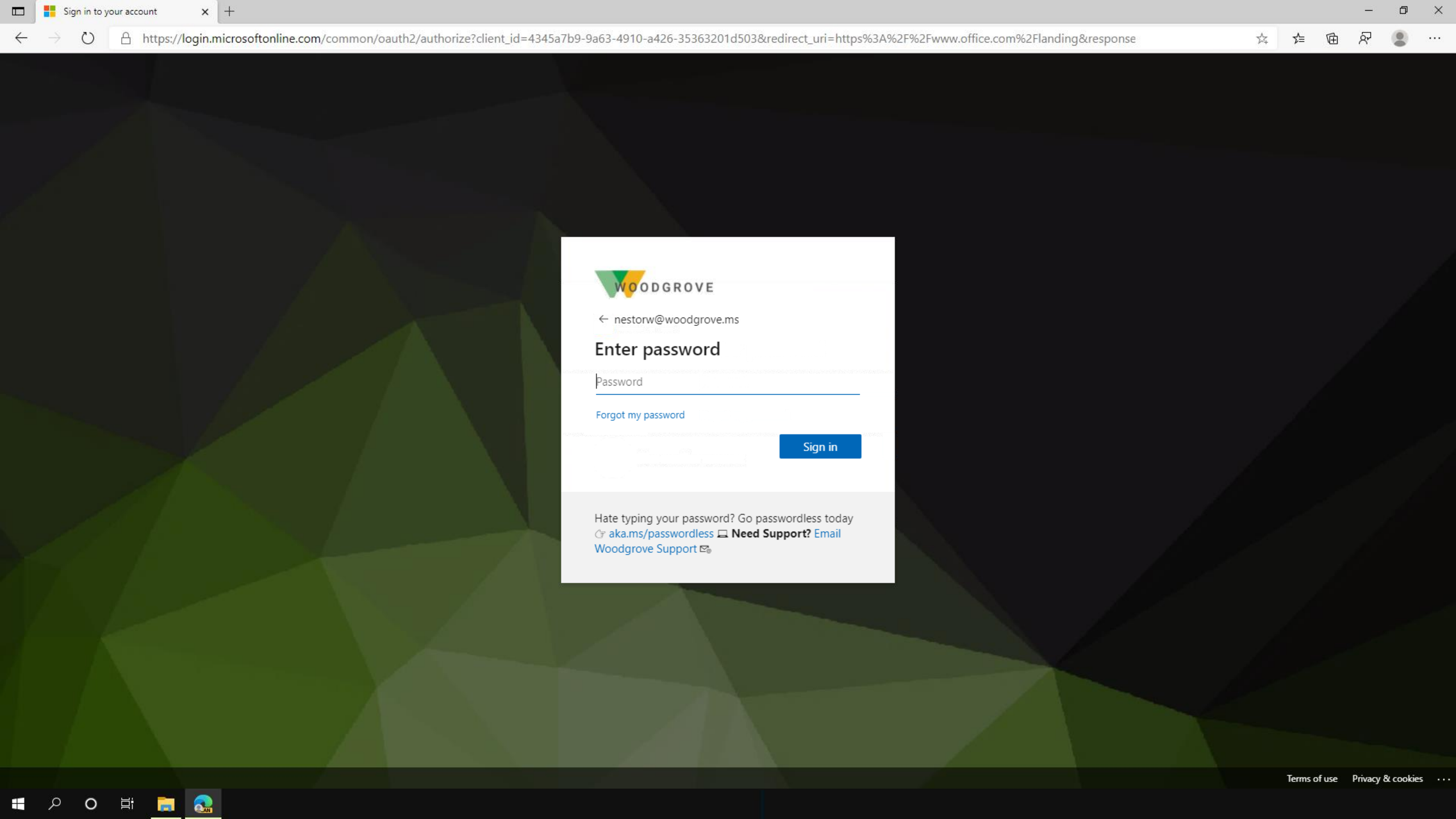
Data protection Edit

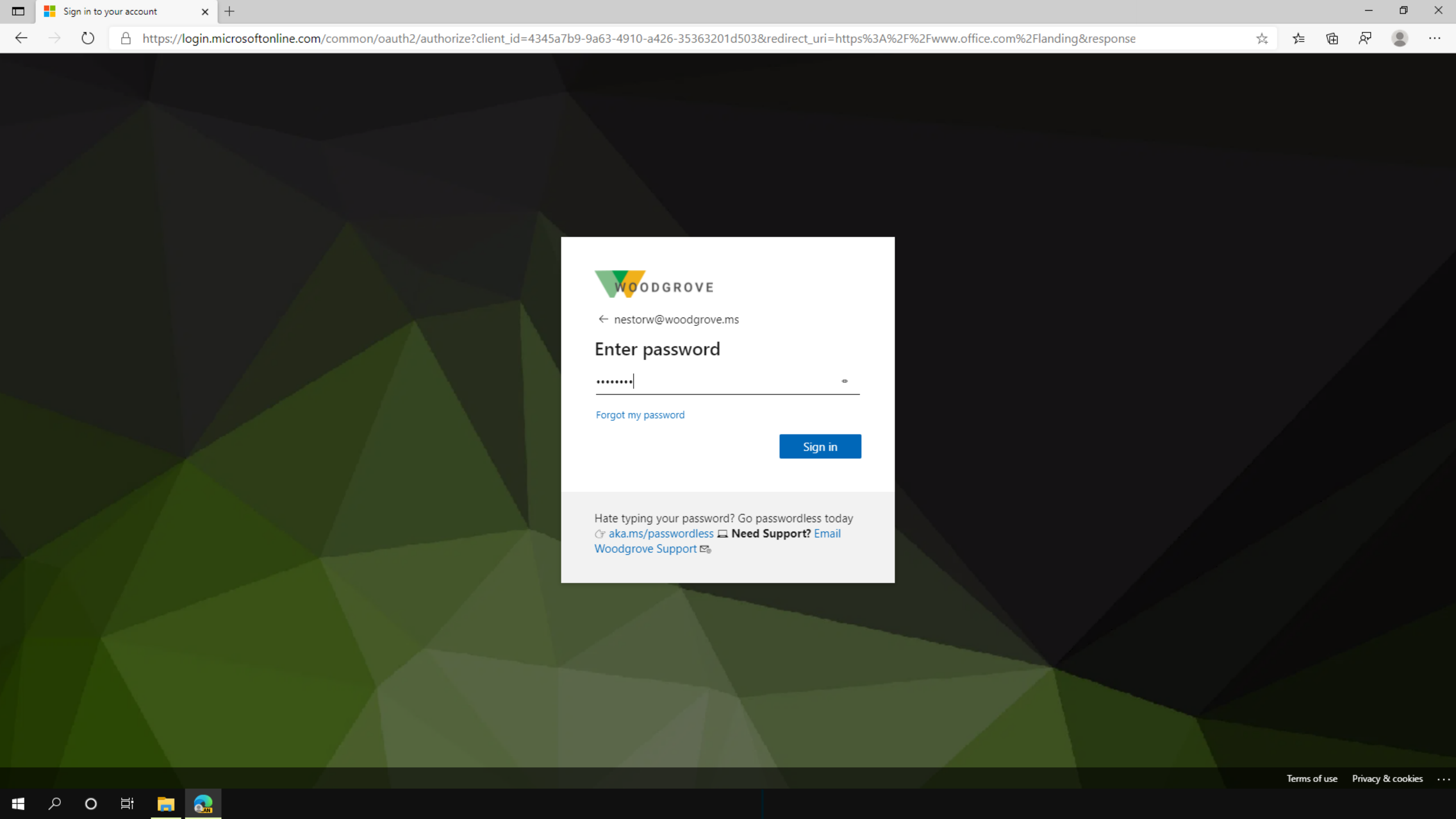
Prevent backups	Block
Send org data to other apps	Policy managed apps
Select apps to exempt	Default: tel;telprompt;skype;app-settings;calshow;itms;itmss;itms-apps;itms-appss;itms-services;
Save copies of org data	Block
Allow user to save copies to selected services	OneDrive for Business
Transfer telecommunication data to	Any dialer app
Dialer App URL Scheme	--
Receive data from other apps	Policy managed apps
Open data into Org documents	Allow
Allow users to open data from selected services	--
Restrict cut, copy, and paste between other apps	Policy managed apps
Cut and copy character limit for any app	0
Third party keyboards	Allow

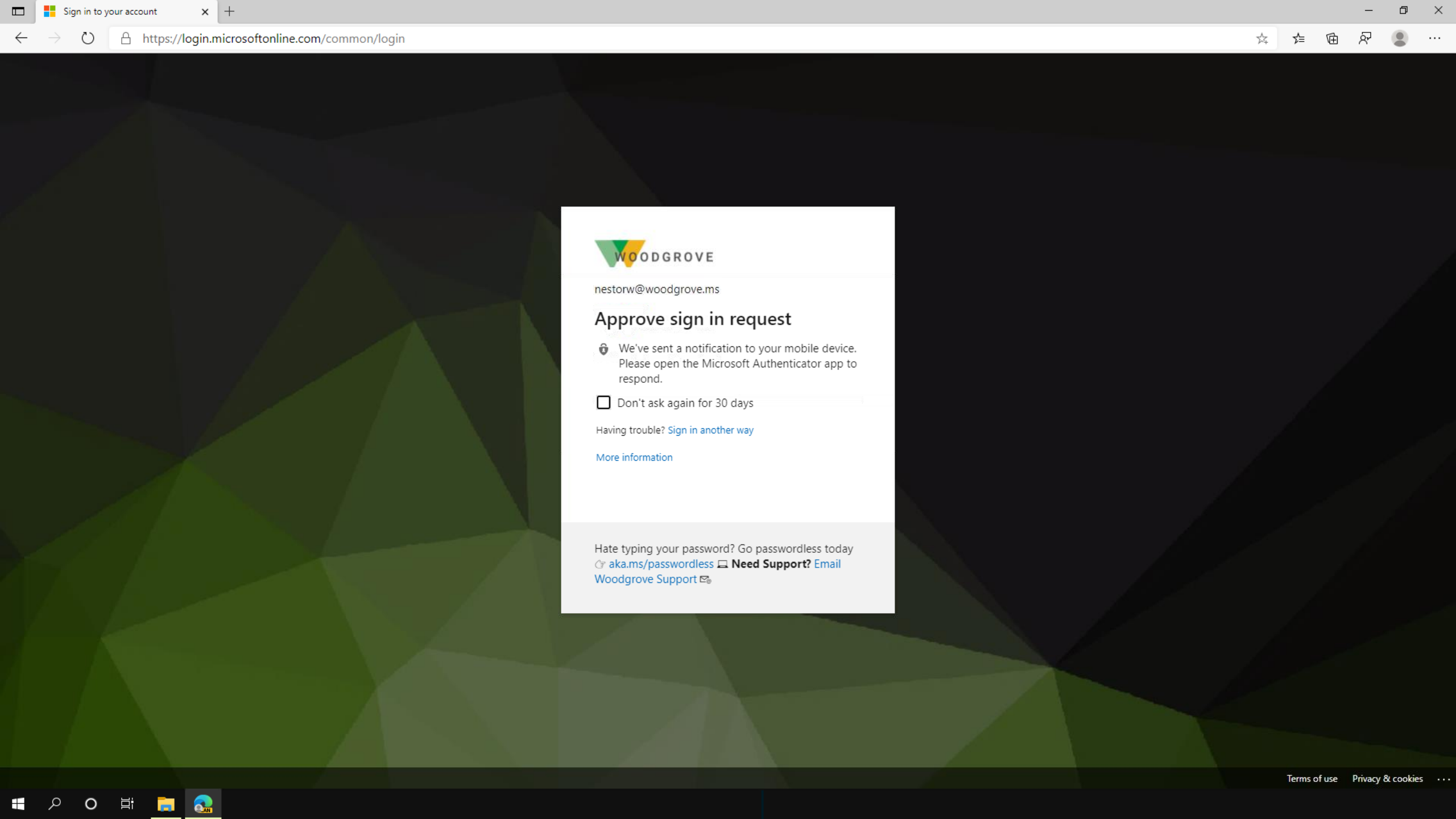

Microsoft Secure Score - Micros
Intune App Protection - Microso
portal.cloudappsecurity.com
Working... - portal.cloudappsecurity.com
portal.cloudappsecurity.com - Bing Search
portal.cloudappsecurity.com/oauth2/login
Working... - portal.cloudappsecurity.com/oauth2/authorize/?&state=L3x8fHx8fHx8fHx8fHx8fA==
Microsoft Endpoin
admin@Woodgrove.ms
WOODGROVE
Home
Dashboard
All services
FAVORITES
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Overview
Manage
Properties
Help and support
Diagnose and solve problems
Basics Edit
Name iOS - Outlook / OneDrive / Excel / Power BI
Description Sales Org - Device Access app protection
Platform iOS/iPadOS
Apps Edit
Target to apps on all device types Yes
Device types --
Public apps Microsoft Outlook
Microsoft OneNote
Microsoft OneDrive
Microsoft Teams
Microsoft To-Do
Custom apps --
Data protection Edit
Prevent backups Block
Send org data to other apps Policy managed apps
Select apps to exempt Default: tel;telprompt;skype;app-settings;calshow;itms;itmss;itms-apps;itms-appss;itms-services;
Save copies of org data Block
Allow user to save copies to selected services OneDrive for Business
Transfer telecommunication data to Any dialer app
Dialer App URL Scheme --
Receive data from other apps Policy managed apps
Open data into Org documents Allow
Allow users to open data from selected services --
Restrict cut, copy, and paste between other apps Policy managed apps
Cut and copy character limit for any app 0
Third party keyboards Allow
Encrypt org data Require

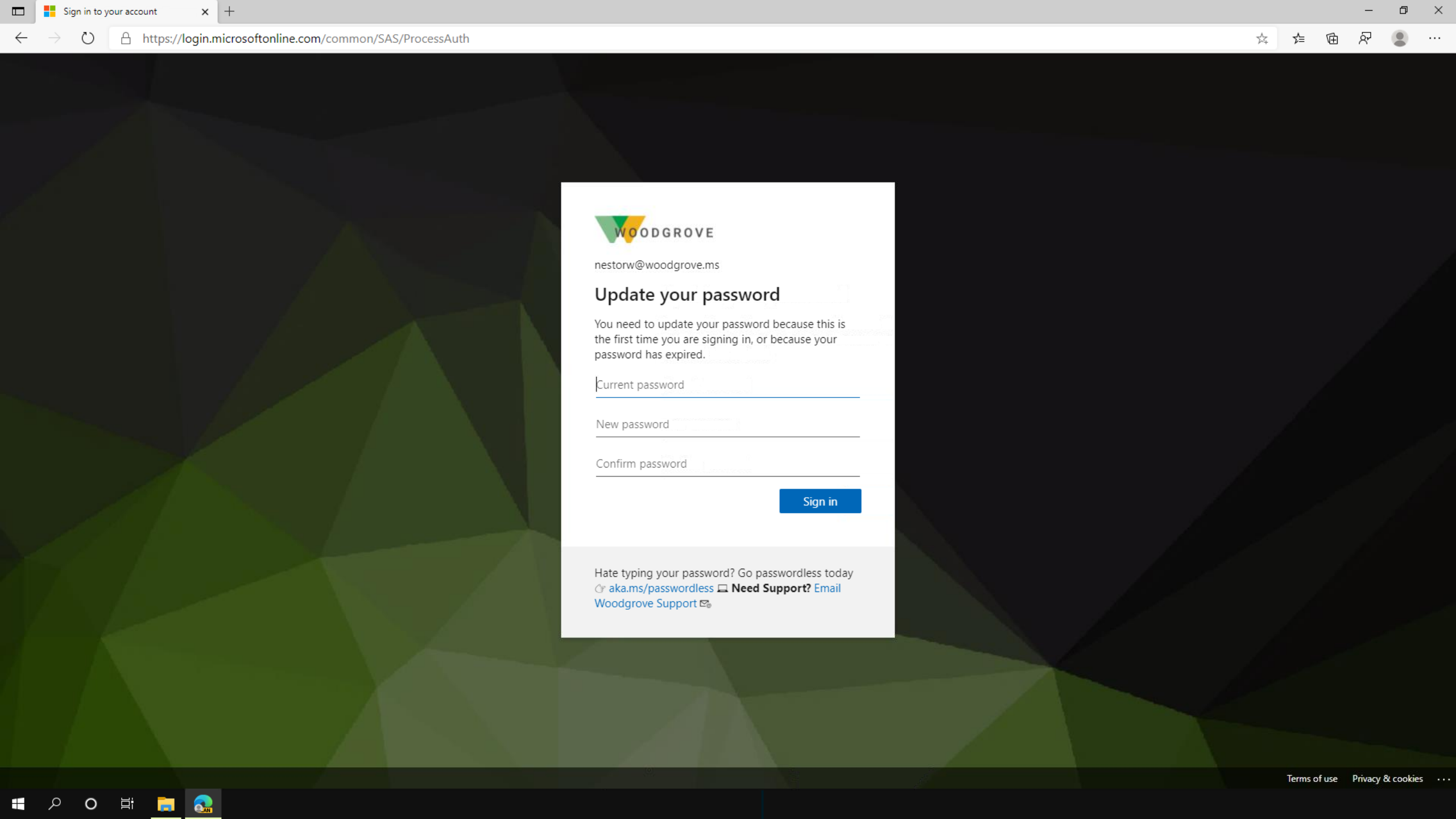
The End-User Experience
Compromised Identity

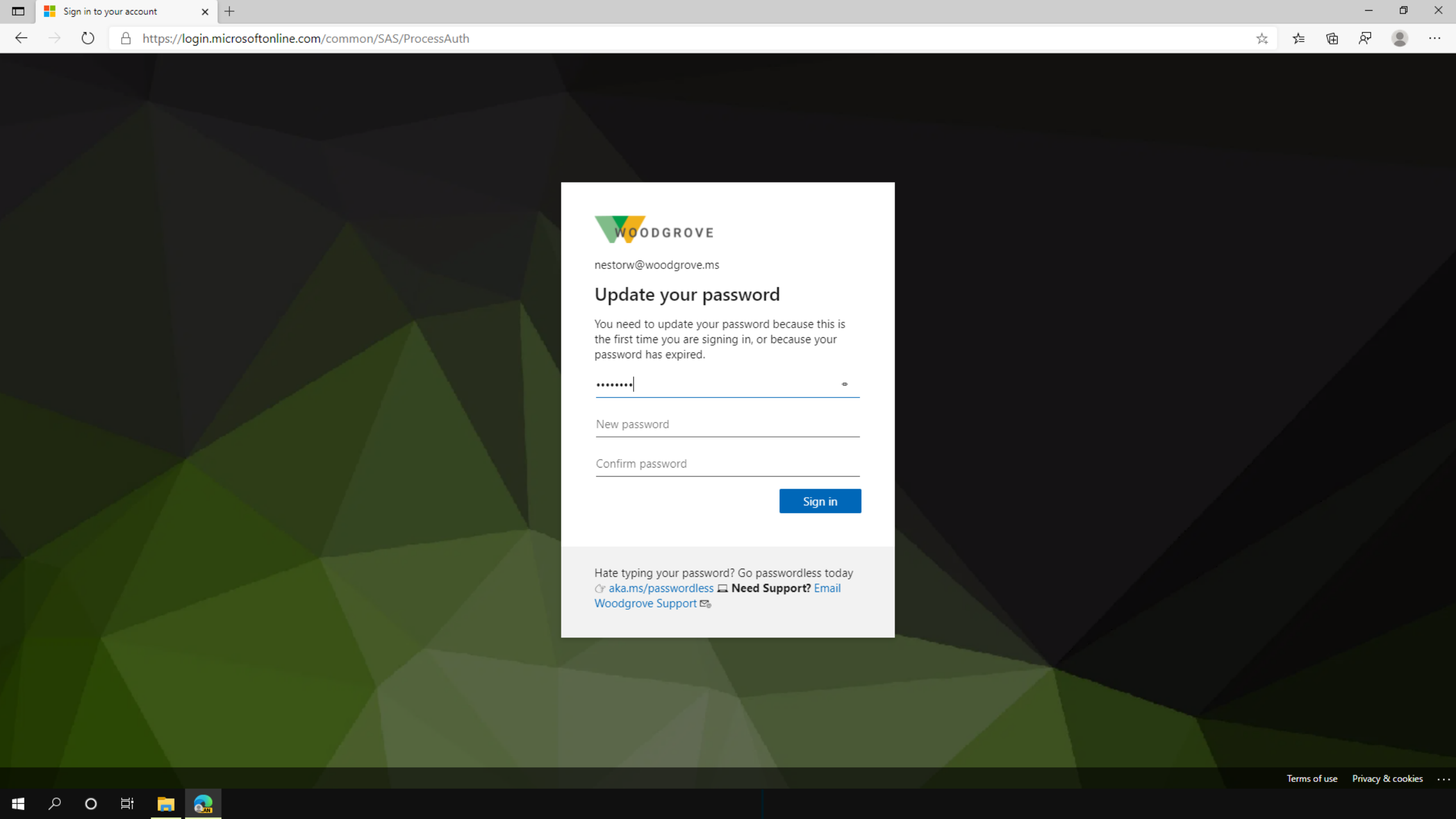

Sign in to your account
https://login.microsoftonline.com/common/oauth2/authorize?client_id=4345a7b9-9a63-4910-a426-35363201d503&redirect_uri=https%3A%2F%2Fwww.office.com%2Flanding&response
Microsoft
Pick an account
nestorw@woodgrove.ms
Use another account
Terms of use
Privacy & cookies

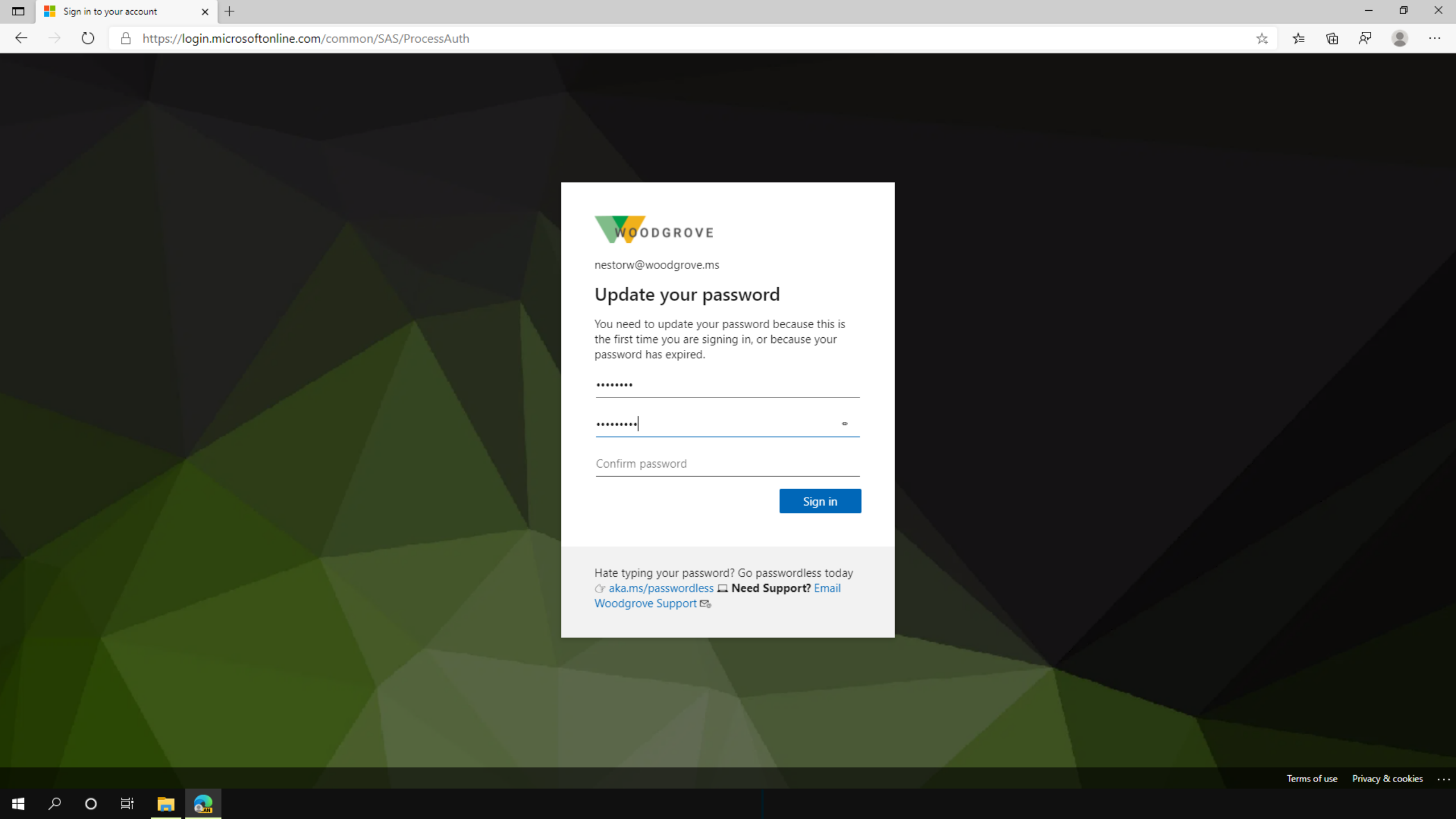

Sign in to your account
https://login.microsoftonline.com/common/oauth2/authorize?client_id=4345a7b9-9a63-4910-a426-35363201d503&redirect_uri=https%3A%2F%2Fwww.office.com%2Flanding&response
WOODGROVE
nestorw@woodgrove.ms
Enter password
Password
Forgot my password
Sign in
Hate typing your password? Go passwordless today
aka.ms/passwordless Need Support? Email Woodgrove Support
Terms of use
Privacy & cookies

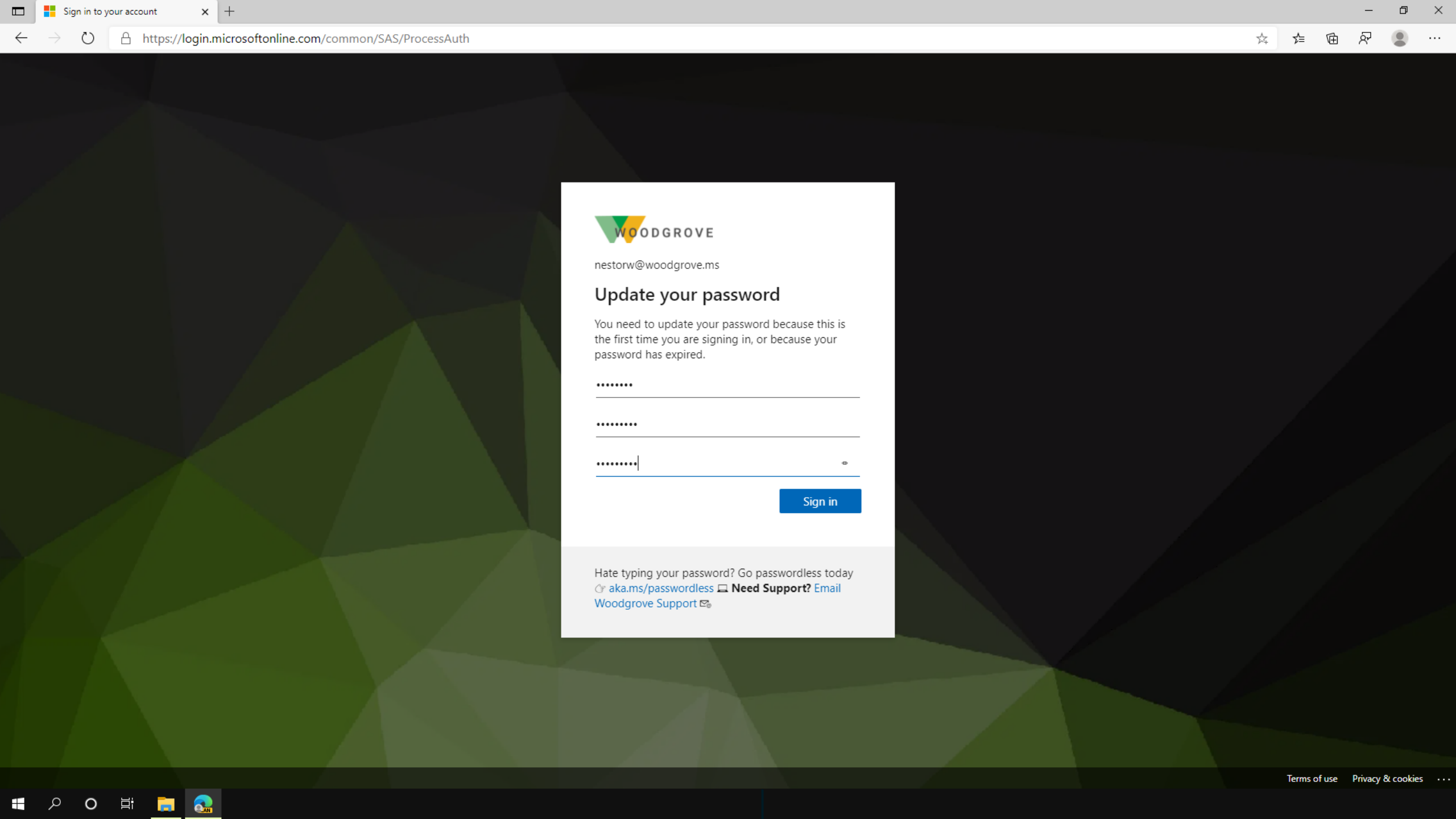

Sign in to your account
https://login.microsoftonline.com/common/oauth2/authorize?client_id=4345a7b9-9a63-4910-a426-35363201d503&redirect_uri=https%3A%2F%2Fwww.office.com%2Flanding&response
WOODGROVE
nestorw@woodgrove.ms
Enter password
Forgot my password
Sign in
Hate typing your password? Go passwordless today
aka.ms/passwordless
Need Support? Email Woodgrove Support
Terms of use
Privacy & cookies


Sign in to your account
https://login.microsoftonline.com/common/login
WOODGROVE
nestorw@woodgrove.ms
Approve sign in request
We've sent a notification to your mobile device. Please open the Microsoft Authenticator app to respond.
Don't ask again for 30 days
Having trouble? Sign in another way
More information
Hate typing your password? Go passwordless today
aka.ms/passwordless
Need Support? Email Woodgrove Support
Terms of use
Privacy & cookies


Sign in to your account
https://login.microsoftonline.com/common/SAS/ProcessAuth
WOODGROVE
nestorw@woodgrove.ms
Update your password
You need to update your password because this is the first time you are signing in, or because your password has expired.
Current password
New password
Confirm password
Sign in
Hate typing your password? Go passwordless today
aka.ms/passwordless
Need Support? Email Woodgrove Support
Terms of use
Privacy & cookies


Sign in to your account
https://login.microsoftonline.com/common/SAS/ProcessAuth
WOODGROVE
nestorw@woodgrove.ms
Update your password
You need to update your password because this is the first time you are signing in, or because your password has expired.
New password
Confirm password
Sign in
Hate typing your password? Go passwordless today
aka.ms/passwordless
Need Support? Email Woodgrove Support
Terms of use
Privacy & cookies


Sign in to your account
https://login.microsoftonline.com/common/SAS/ProcessAuth
WOODGROVE
nestorw@woodgrove.ms
Update your password
You need to update your password because this is the first time you are signing in, or because your password has expired.
Confirm password
Sign in
Hate typing your password? Go passwordless today
aka.ms/passwordless
Need Support? Email Woodgrove Support
Terms of use
Privacy & cookies


Sign in to your account
https://login.microsoftonline.com/common/SAS/ProcessAuth
WOODGROVE
nestorw@woodgrove.ms
Update your password
You need to update your password because this is the first time you are signing in, or because your password has expired.
Sign in
Hate typing your password? Go passwordless today
aka.ms/passwordless
Need Support? Email Woodgrove Support
Terms of use
Privacy & cookies

Microsoft Office Home

https://www.office.com/?auth=2

WOODGROVE Office 365

Search

NW

Good morning

Install Office

Recommended

You edited this
8m ago

Woodgrove Home Loan Applicatio...
m365x362046-my.sharepoin...

Recent | Pinned | Shared with me | Discover

Upload and open...

Woodgrove Home Loan Application - DB345 Nestor Wilke's OneDrive for Business » ... » Documents	6m ago	Only you

Drag a file here to upload and open

More in OneDrive

OneDrive

Recent folders

Documents Nestor Wilke's OneDrive for Business » ... » ..._...	6m ago

Go to OneDrive

SharePoint

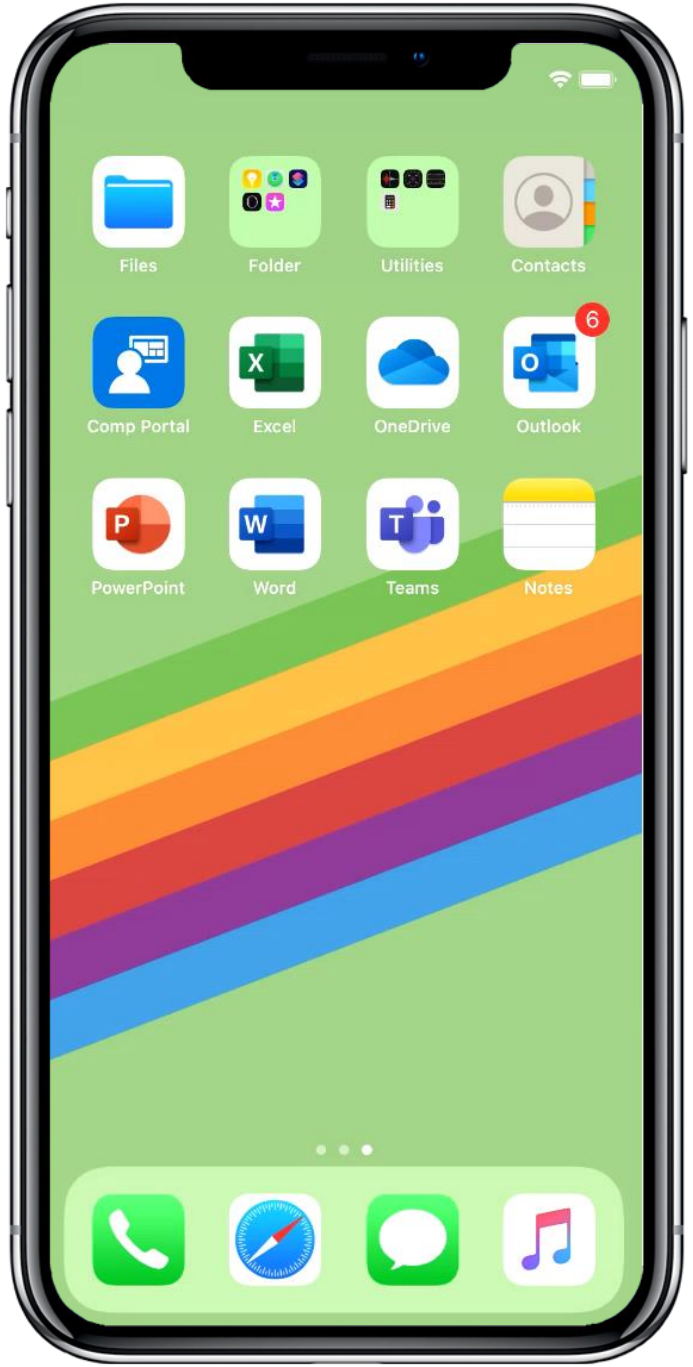
Frequent sites

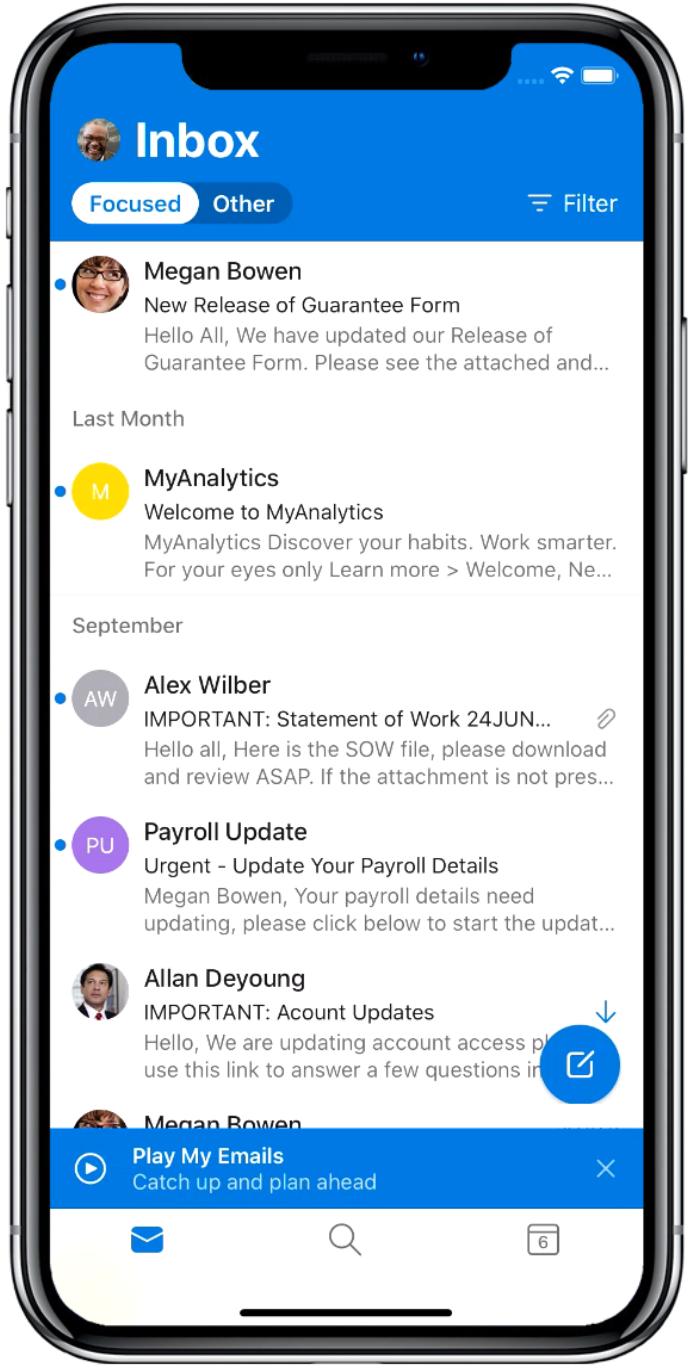
- B Benefits
- TL The Landing

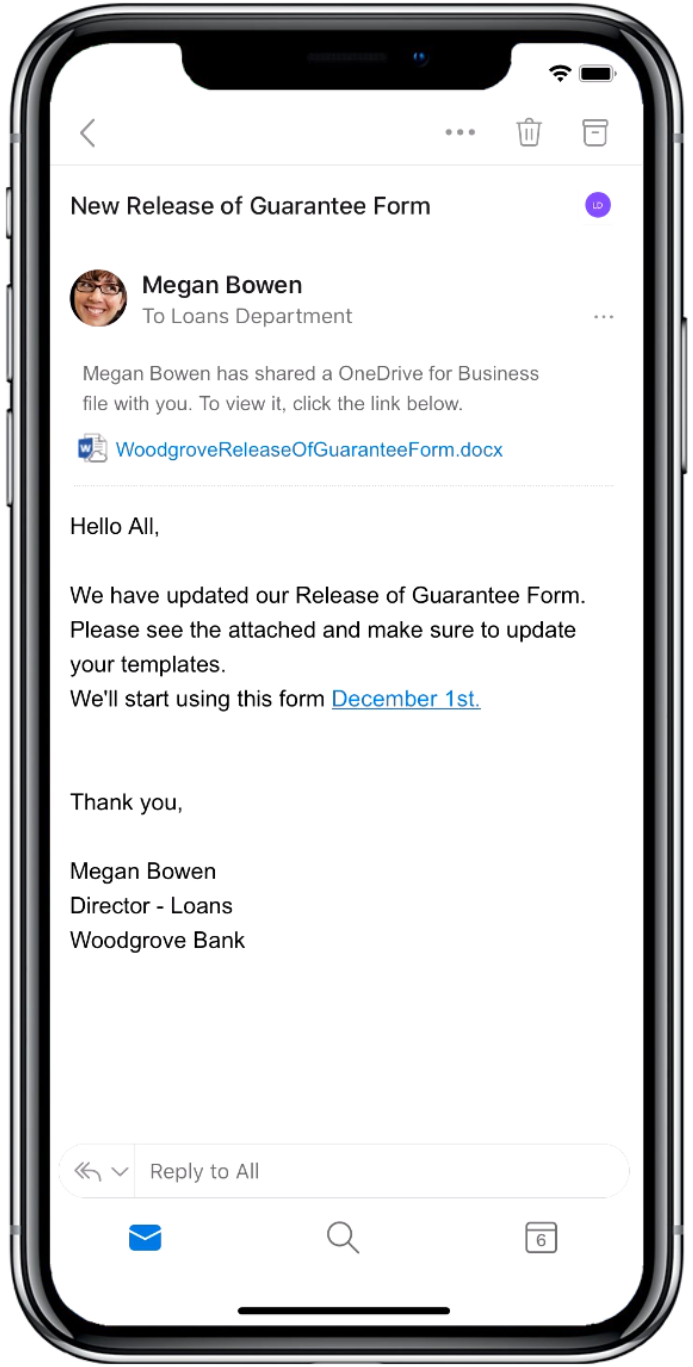
Go to SharePoint

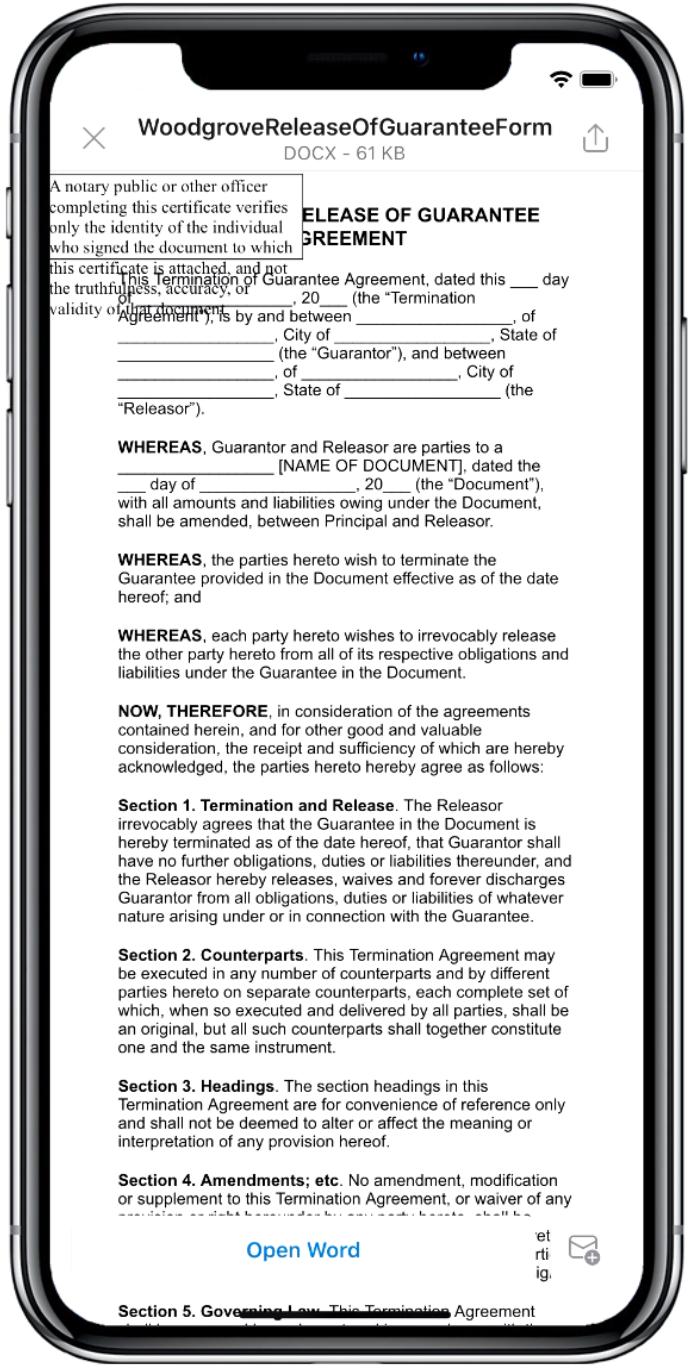
Feedback | Need help?

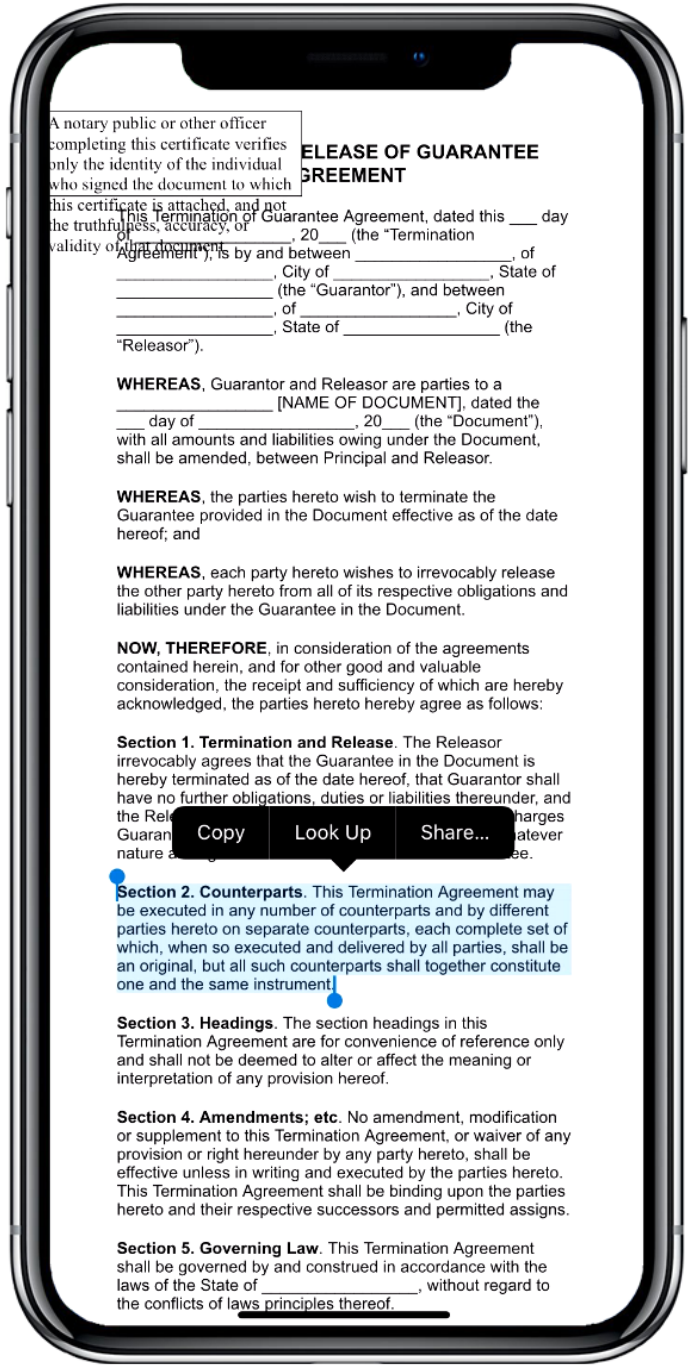
The End-User Experience
Devices and Apps


Files
Folder
Utilities
Contacts
Comp Portal
Excel
OneDrive
6
Outlook
PowerPoint
Word
Teams
Notes


Inbox
Focused
Other
Filter
Megan Bowen
New Release of Guarantee Form
Hello All, We have updated our Release of Guarantee Form. Please see the attached and...
Last Month
MyAnalytics
Welcome to MyAnalytics
MyAnalytics Discover your habits. Work smarter. For your eyes only Learn more > Welcome, Ne...
September
Alex Wilber
IMPORTANT: Statement of Work 24JUN...
Hello all, Here is the SOW file, please download and review ASAP. If the attachment is not pres...
Payroll Update
Urgent - Update Your Payroll Details
Megan Bowen, Your payroll details need updating, please click below to start the updat...
Allan Deyoung
IMPORTANT: Acount Updates
Hello, We are updating account access p
use this link to answer a few questions in
Play My Emails
Catch up and plan ahead


New Release of Guarantee Form
Megan Bowen
To Loans Department
Megan Bowen has shared a OneDrive for Business file with you. To view it, click the link below.
WoodgroveReleaseOfGuaranteeForm.docx
Hello All,
We have updated our Release of Guarantee Form. Please see the attached and make sure to update your templates.
We'll start using this form December 1st.
Thank you,
Megan Bowen
Director - Loans
Woodgrove Bank
Reply to All


WoodgroveReleaseOfGuaranteeForm
DOCX - 61 KB
A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.
ELEASE OF GUARANTEE
GREEMENT
This Termination of Guarantee Agreement, dated this ___ day of _____, 20___ (the "Termination Agreement"), is by and between _____, of _____, City of _____, State of _____ (the "Guarantor"), and between _____, of _____, City of _____, State of _____ (the "Releasor").
WHEREAS, Guarantor and Releasor are parties to a _____ [NAME OF DOCUMENT], dated the ___ day of _____, 20___ (the "Document"), with all amounts and liabilities owing under the Document, shall be amended, between Principal and Releasor.
WHEREAS, the parties hereto wish to terminate the Guarantee provided in the Document effective as of the date hereof; and
WHEREAS, each party hereto wishes to irrevocably release the other party hereto from all of its respective obligations and liabilities under the Guarantee in the Document.
NOW, THEREFORE, in consideration of the agreements contained herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereto hereby agree as follows:
Section 1. Termination and Release. The Releasor irrevocably agrees that the Guarantee in the Document is hereby terminated as of the date hereof, that Guarantor shall have no further obligations, duties or liabilities thereunder, and the Releasor hereby releases, waives and forever discharges Guarantor from all obligations, duties or liabilities of whatever nature arising under or in connection with the Guarantee.
Section 2. Counterparts. This Termination Agreement may be executed in any number of counterparts and by different parties hereto on separate counterparts, each complete set of which, when so executed and delivered by all parties, shall be an original, but all such counterparts shall together constitute one and the same instrument.
Section 3. Headings. The section headings in this Termination Agreement are for convenience of reference only and shall not be deemed to alter or affect the meaning or interpretation of any provision hereof.
Section 4. Amendments; etc. No amendment, modification or supplement to this Termination Agreement, or waiver of any
Open Word
Section 5. Governing Law. This Termination Agreement



A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

ELEASE OF GUARANTEE
GREEMENT

This Termination of Guarantee Agreement, dated this ___ day of _____, 20___ (the "Termination Agreement"), is by and between _____, of _____, City of _____, State of _____ (the "Guarantor"), and between _____, of _____, City of _____, State of _____ (the "Releasor").

WHEREAS, Guarantor and Releasor are parties to a _____ [NAME OF DOCUMENT], dated the ___ day of _____, 20___ (the "Document"), with all amounts and liabilities owing under the Document, shall be amended, between Principal and Releasor.

WHEREAS, the parties hereto wish to terminate the Guarantee provided in the Document effective as of the date hereof; and

WHEREAS, each party hereto wishes to irrevocably release the other party hereto from all of its respective obligations and liabilities under the Guarantee in the Document.

NOW, THEREFORE, in consideration of the agreements contained herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereto hereby agree as follows:

Section 1. Termination and Release. The Releasor irrevocably agrees that the Guarantee in the Document is hereby terminated as of the date hereof, that Guarantor shall have no further obligations, duties or liabilities thereunder, and the Rel harges Guaran atever nature a ee.

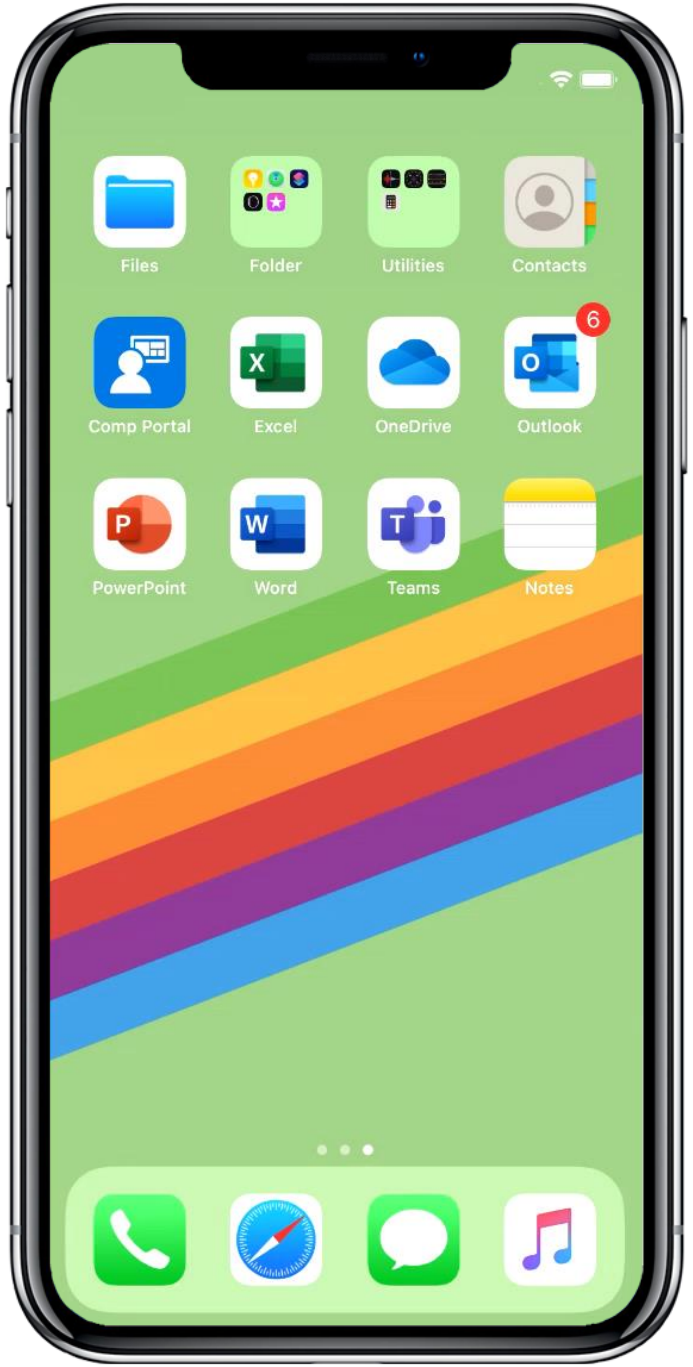
Copy | Look Up | Share...

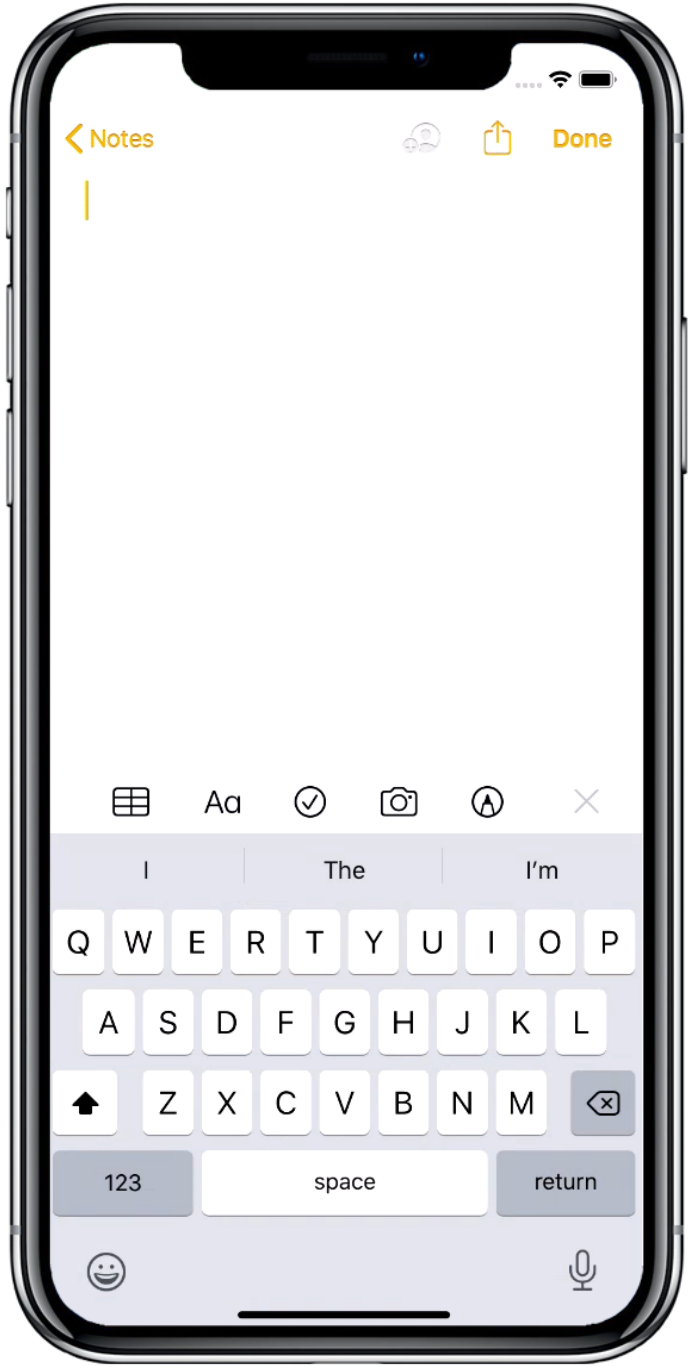
Section 2. Counterparts. This Termination Agreement may be executed in any number of counterparts and by different parties hereto on separate counterparts, each complete set of which, when so executed and delivered by all parties, shall be an original, but all such counterparts shall together constitute one and the same instrument.

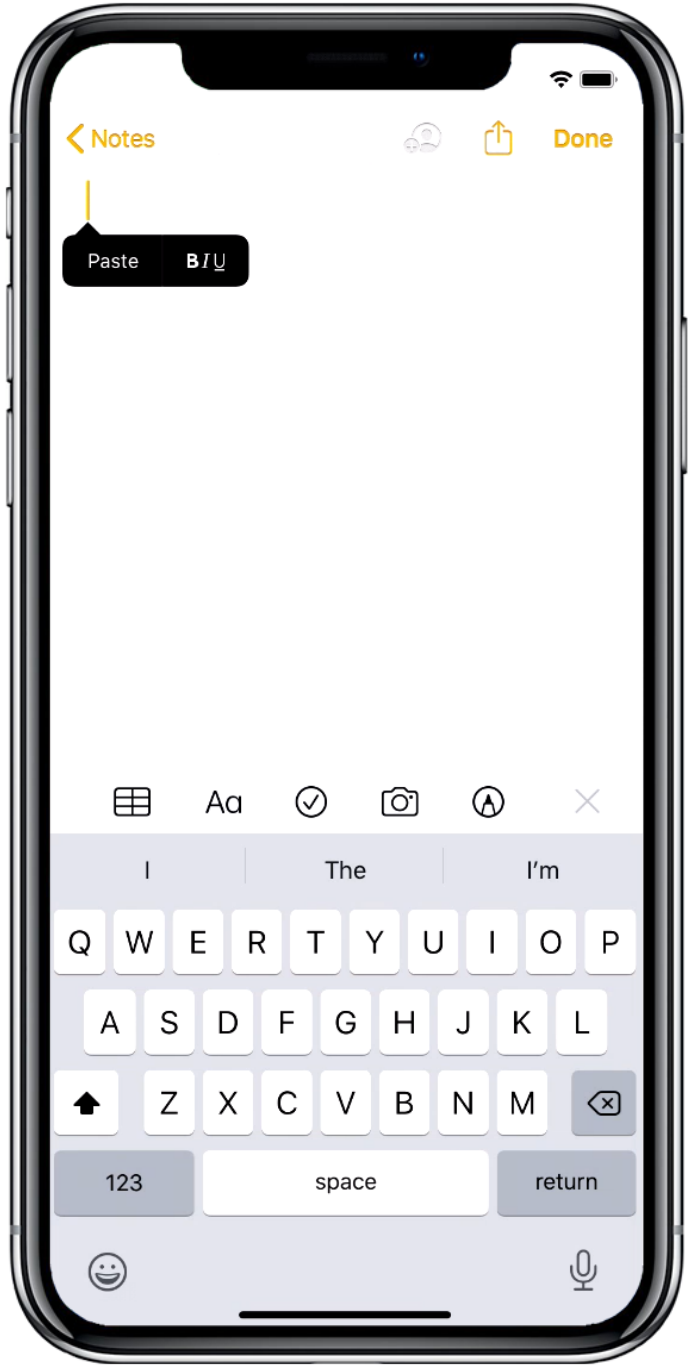
Section 3. Headings. The section headings in this Termination Agreement are for convenience of reference only and shall not be deemed to alter or affect the meaning or interpretation of any provision hereof.

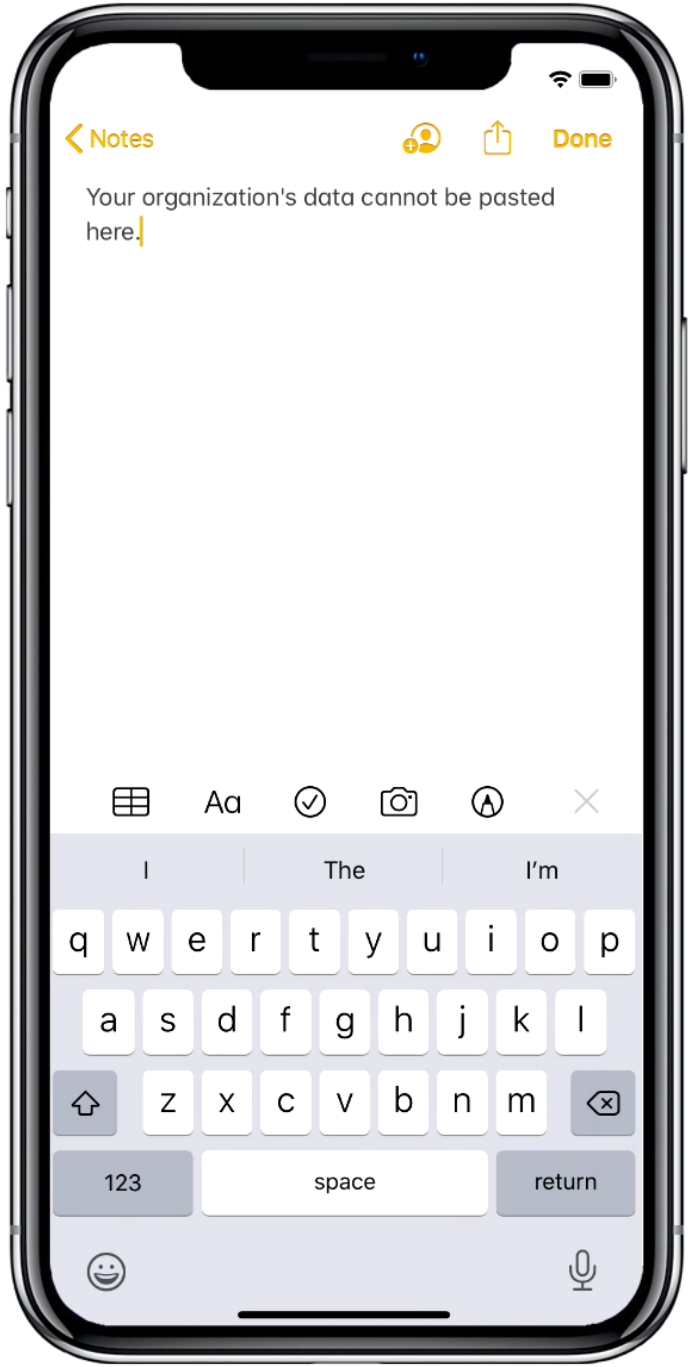
Section 4. Amendments; etc. No amendment, modification or supplement to this Termination Agreement, or waiver of any provision or right hereunder by any party hereto, shall be effective unless in writing and executed by the parties hereto. This Termination Agreement shall be binding upon the parties hereto and their respective successors and permitted assigns.

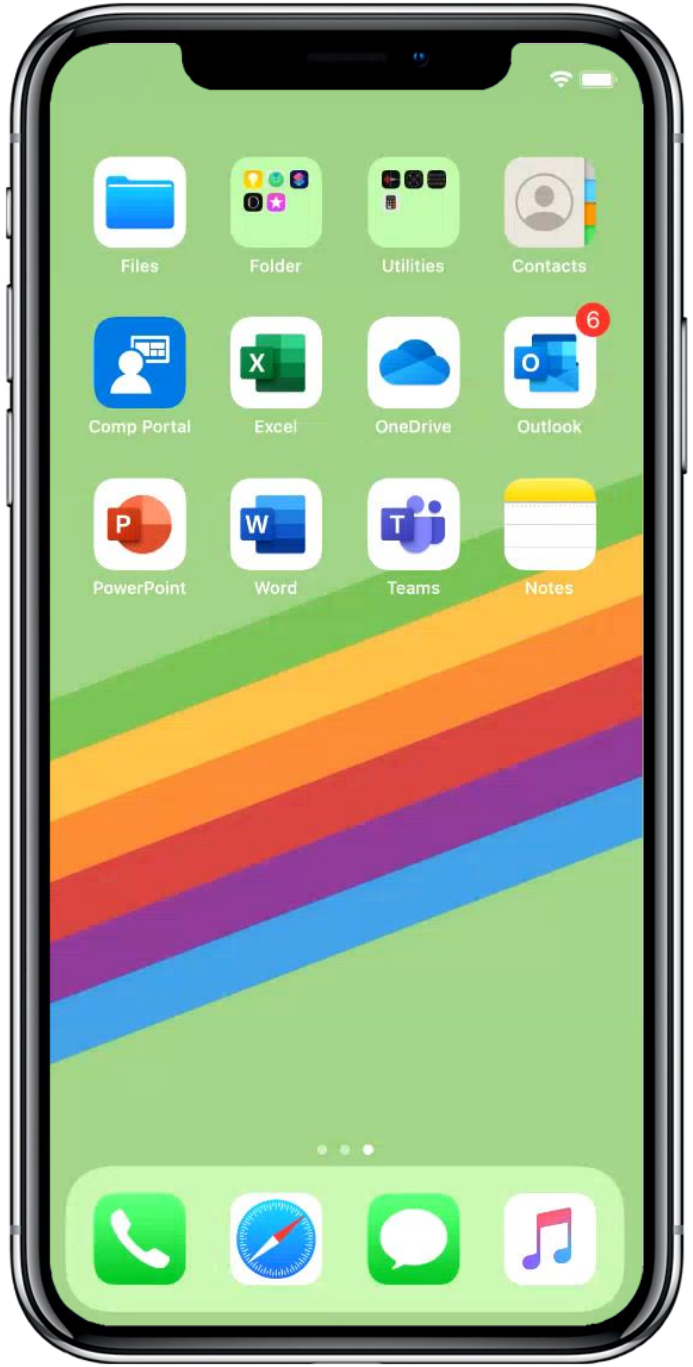
Section 5. Governing Law. This Termination Agreement shall be governed by and construed in accordance with the laws of the State of _____, without regard to the conflicts of laws principles thereof.

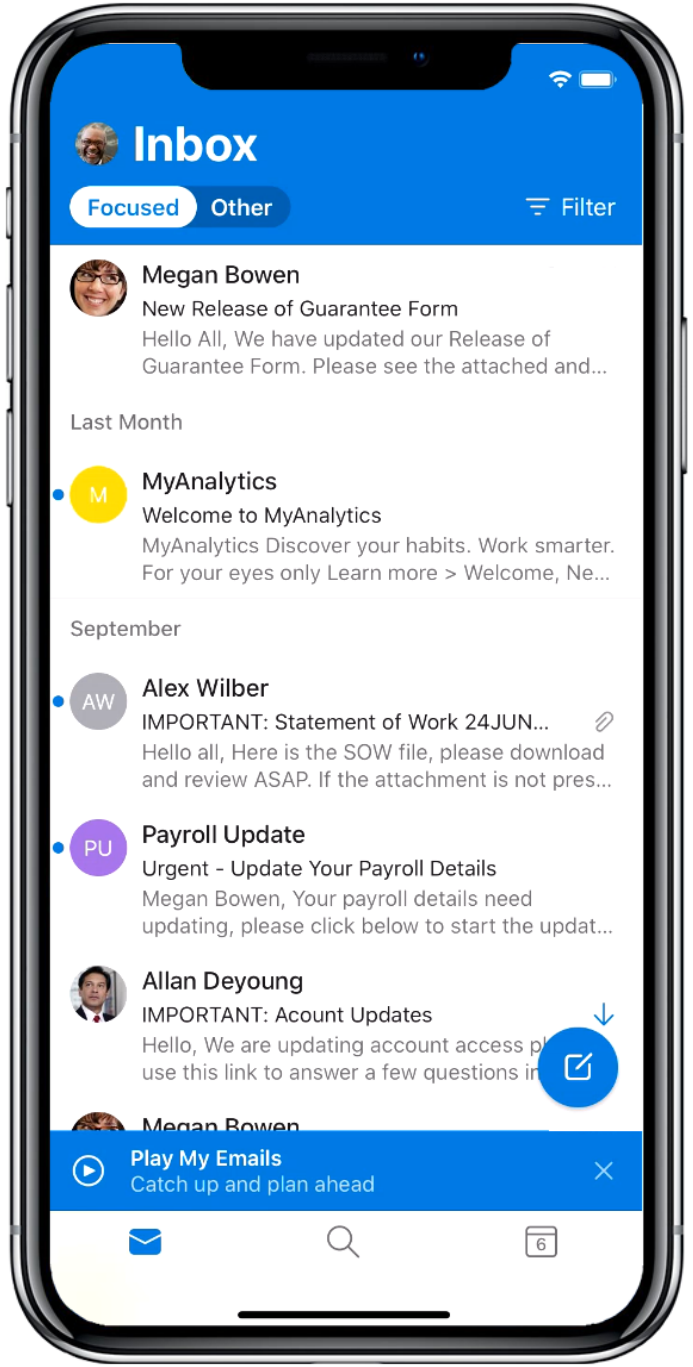

Files
Folder
Utilities
Contacts
Comp Portal
Excel
OneDrive
6
Outlook
PowerPoint
Word
Teams
Notes


Notes
Done
Aa
I
The
I'm
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123
space
return

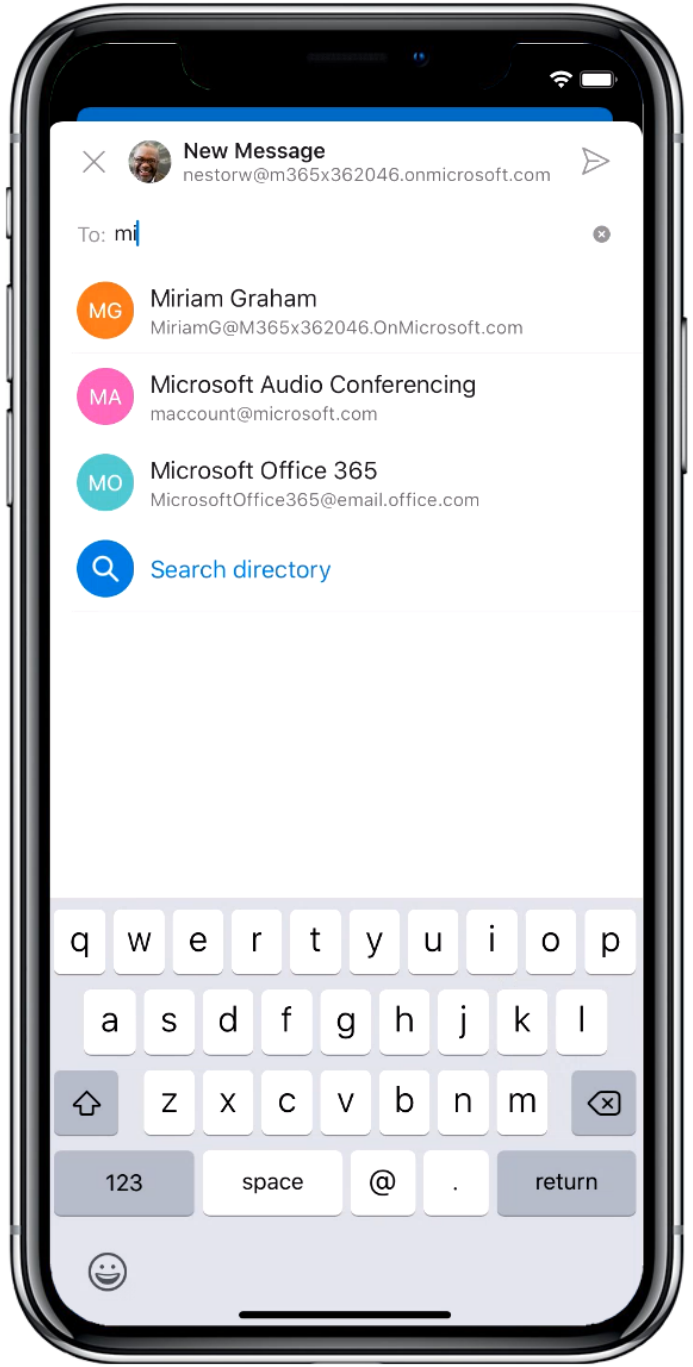

Notes
Done
Paste
B I U
Aa
I
The
I'm
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123
space
return


Notes
Done
Your organization's data cannot be pasted here.
Aa
I
The
I'm
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
return

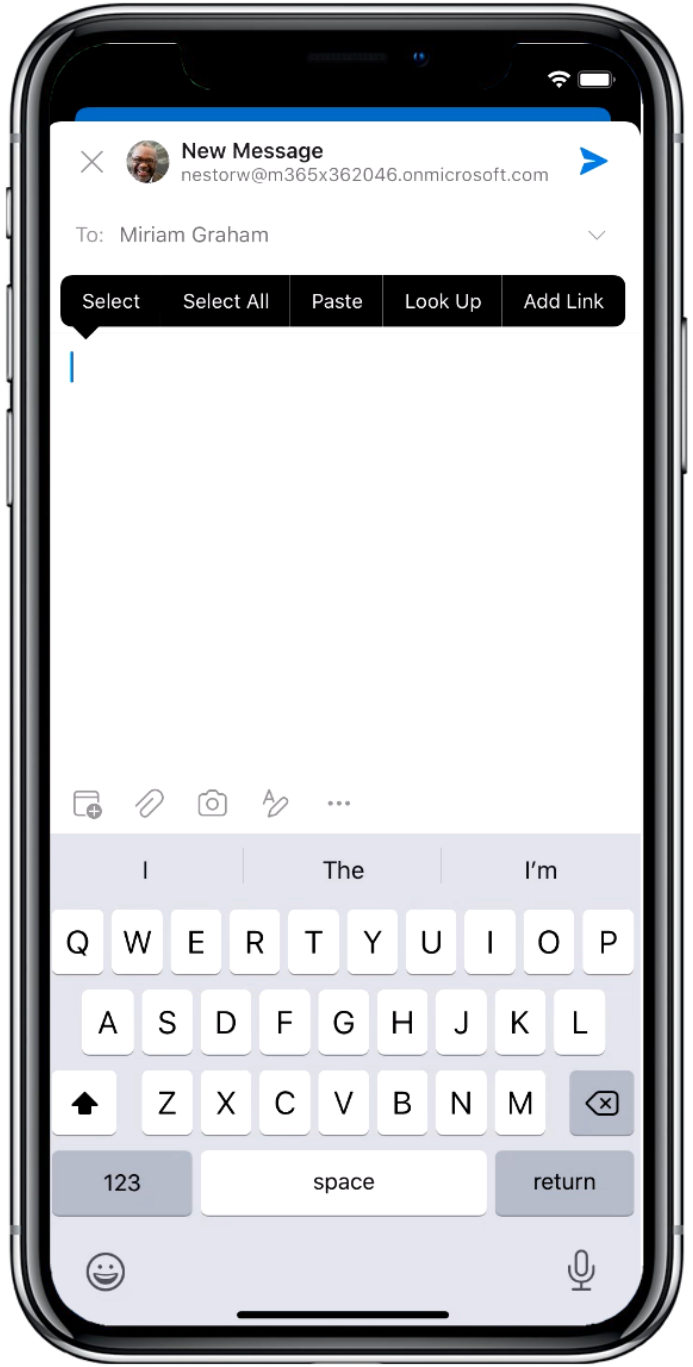

Files
Folder
Utilities
Contacts
Comp Portal
Excel
OneDrive
6
Outlook
PowerPoint
Word
Teams
Notes

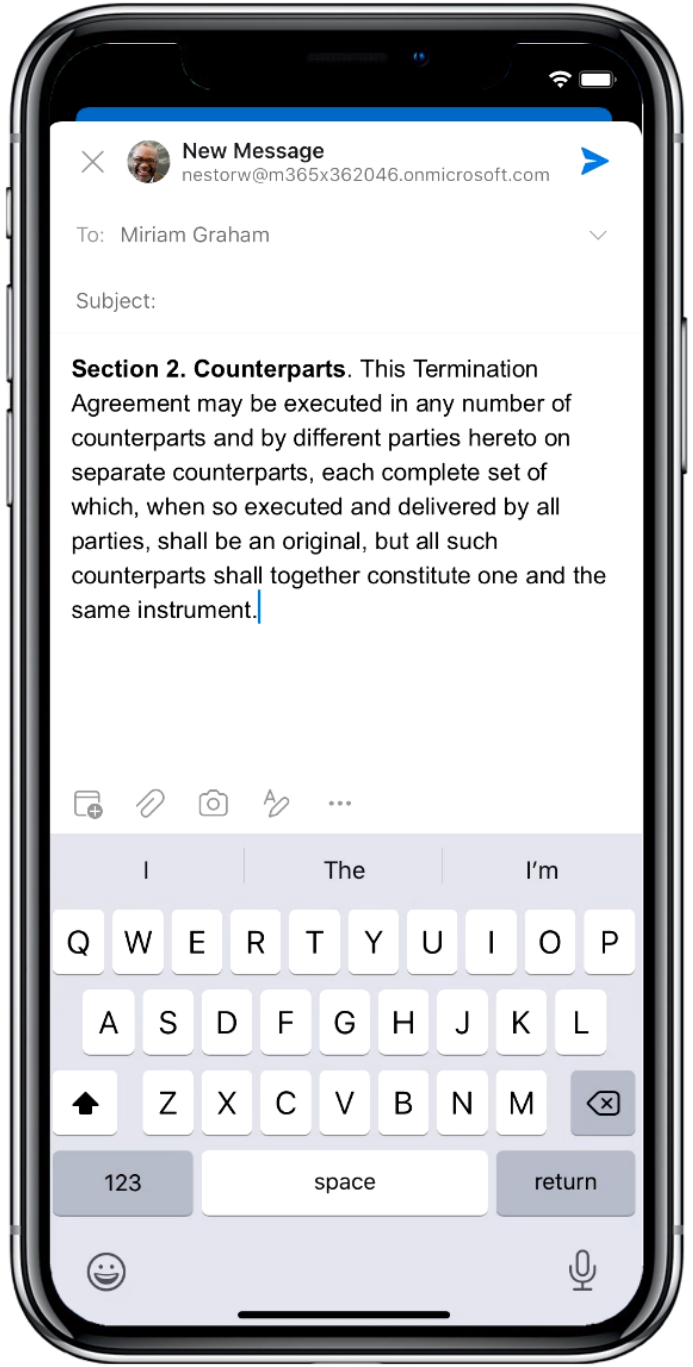

Inbox
Focused
Other
Filter
Megan Bowen
New Release of Guarantee Form
Hello All, We have updated our Release of Guarantee Form. Please see the attached and...
Last Month
M
MyAnalytics
Welcome to MyAnalytics
MyAnalytics Discover your habits. Work smarter. For your eyes only Learn more > Welcome, Ne...
September
AW
Alex Wilber
IMPORTANT: Statement of Work 24JUN...
Hello all, Here is the SOW file, please download and review ASAP. If the attachment is not pres...
PU
Payroll Update
Urgent - Update Your Payroll Details
Megan Bowen, Your payroll details need updating, please click below to start the updat...
Allan Deyoung
IMPORTANT: Acount Updates
Hello, We are updating account access pl
use this link to answer a few questions in
Play My Emails
Catch up and plan ahead
6

New Message
nestorw@m365x362046.onmicrosoft.com
To:
Subject:
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
@
.
return


New Message
nestorw@m365x362046.onmicrosoft.com
To: mi
MG
Miriam Graham
MiriamG@M365x362046.OnMicrosoft.com
MA
Microsoft Audio Conferencing
maccount@microsoft.com
MO
Microsoft Office 365
MicrosoftOffice365@email.office.com
Search directory
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
@
.
return

New Message
nestorw@m365x362046.onmicrosoft.com
To: Miriam Graham
Subject:
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
@
.
return


New Message
nestorw@m365x362046.onmicrosoft.com
To: Miriam Graham
Select
Select All
Paste
Look Up
Add Link
I
The
I'm
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123
space
return


New Message
nestorw@m365x362046.onmicrosoft.com
To: Miriam Graham
Subject:
Section 2. Counterparts. This Termination Agreement may be executed in any number of counterparts and by different parties hereto on separate counterparts, each complete set of which, when so executed and delivered by all parties, shall be an original, but all such counterparts shall together constitute one and the same instrument.
I
The
I'm
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123
space
return

Nestor Wilke

My files
Recent
Shared
Recycle bin

Shared libraries

Benefits
The Landing

Create shared library

My files

Name	Modified	Modified By	File size	Sharing
My Stuff	September 10	Nestor Wilke	2 items	Private
Audit of Small Business Sales August.xlsx	September 10	Nestor Wilke	13.8 KB	Shared
BI Improvement.docx	September 10	Nestor Wilke	22.5 KB	Shared
CSATData.xlsx	September 10	Nestor Wilke	30.9 KB	Private
CSATGoals Q2-Q3.docx	September 10	Nestor Wilke	1.24 MB	Private
Employee Engagement Plan.docx	September 10	Nestor Wilke	731 KB	Private
IR Handbook.pptx	September 10	Nestor Wilke	66.0 KB	Private
Over Budget Areas.xlsx	September 10	Nestor Wilke	15.5 KB	Private
Proposed_agenda_topics.docx	September 10	Nestor Wilke	691 KB	Private
Q3 Asia Shipping Budget Review.pptx	September 10	Nestor Wilke	76.2 KB	Shared
RD Projects KPIs.pptx	September 10	Nestor Wilke	343 KB	Shared
Trey Research Integration Plan.pptx	September 10	Nestor Wilke	1.58 MB	Private
Woodgrove Bank Annual Food Drive.pdf	4 hours ago	Nestor Wilke	590 KB	Private
Woodgrove Home Loan Application - DB...	4 hours ago	Nestor Wilke	32.5 KB	Private
Woodgrove Purchasing Data - Q1.xlsx	4 hours ago	Nestor Wilke	21.5 KB	Private

Get the OneDrive apps

Return to classic OneDrive

My files - OneDrive

https://m365x362046-my.sharepoint.com/personal/nestorw_m365x362046_onmicrosoft_com/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Fnestorw_m365x362046_onmicrosoft_com%2FDocuments%2F...

Open | Share | Copy link | Print | Download | Delete | Copy to | Version history

Previous 13 of 15 Next

Woodgrove Bank Annual Food Drive!!

- When: Saturday November 21st-Sunday November 22nd
- Times: 8am – 6pm
- Where: Redmond location
- What to bring: Canned, dried, non-perishable food stuffs, monetary donations are also welcome
- Extra: Donations will be used to create as many "Thanksgiving in a box" as possible to hand out at the local food banks. Margarineball has donated 50 turkeys and has given us a reduced rate to purchase more.

1 of 1

My files - OneDrive

https://m365x362046-my.sharepoint.com/personal/nestorw_m365x362046_onmicrosoft_com/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Fnestorw_m365x362046_onmicrosoft_com%2FDocuments%2F...

Open | Share | Copy link | Print | Download | Delete | Copy to | Version history

Previous 13 of 15 Next

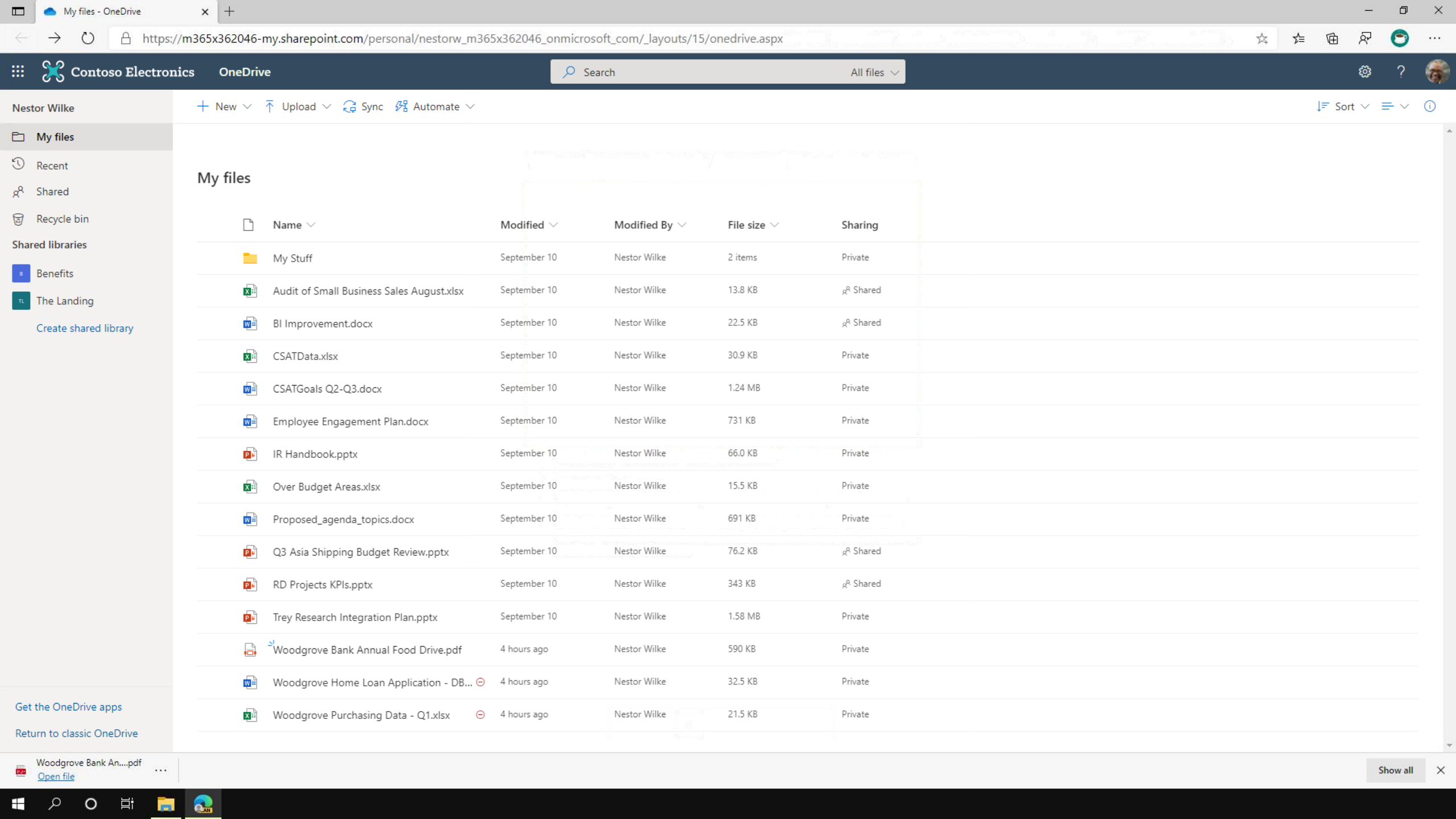
Woodgrove Bank Annual Food Drive!!

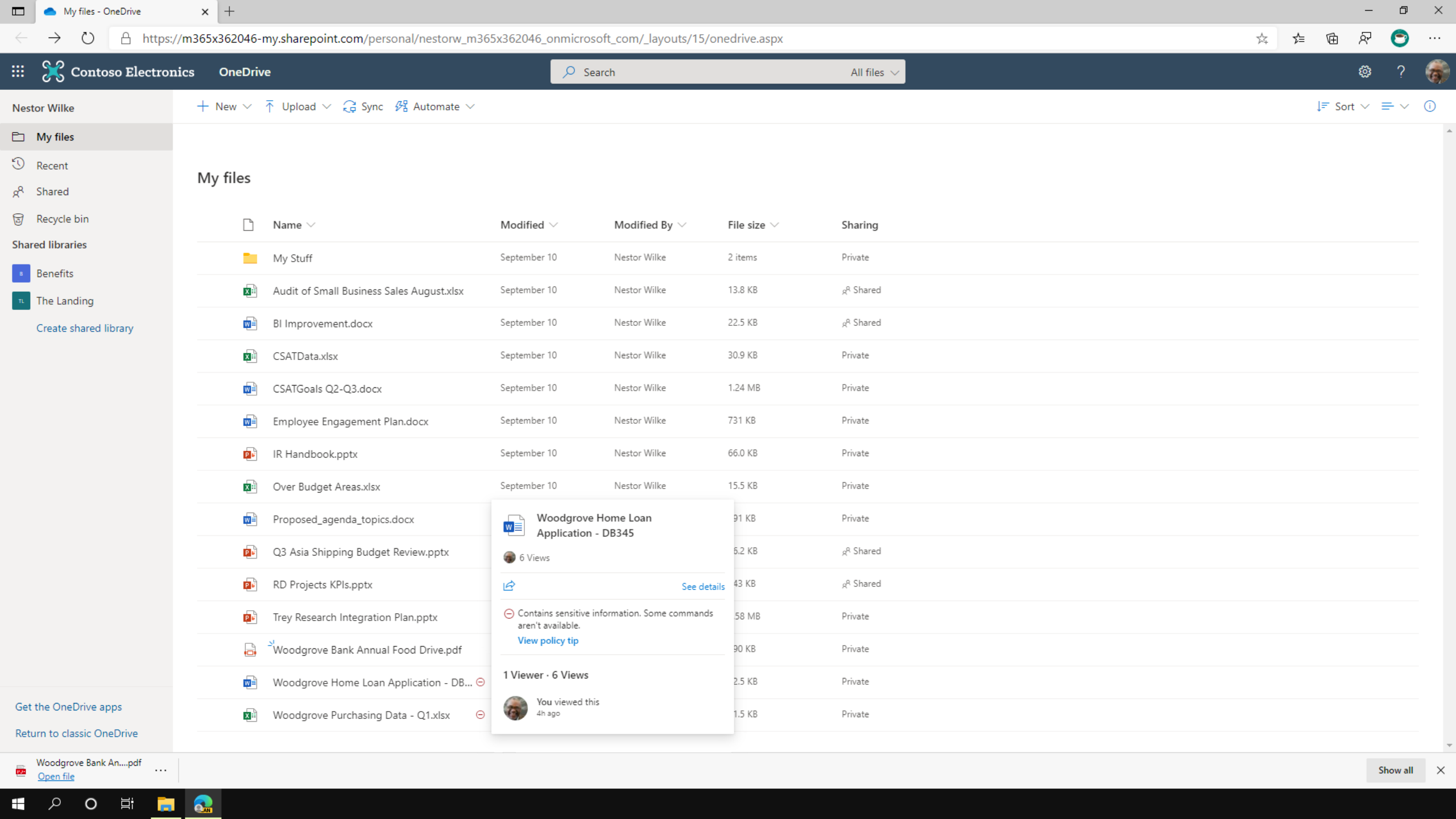
- When: Saturday November 21st-Sunday November 22nd
- Times: 8am – 6pm
- Where: Redmond location
- What to bring: Canned, dried, non-perishable food stuffs, monetary donations are also welcome
- Extra: Donations will be used to create as many "Thanksgiving in a box" as possible to hand out at the local food banks. Margarineball has donated 50 turkeys and has given us a reduced rate to purchase more.

1 of 1

Woodgrove Bank An....pdf
Open file

Show all


My files - OneDrive
https://m365x362046-my.sharepoint.com/personal/nestorw_m365x362046_onmicrosoft_com/_layouts/15/onedrive.aspx
Contoso Electronics
OneDrive
Search
All files
Nestor Wilke
My files
Recent
Shared
Recycle bin
Shared libraries
Benefits
The Landing
Create shared library
Get the OneDrive apps
Return to classic OneDrive
New
Upload
Sync
Automate
Sort
My files
Name
Modified
Modified By
File size
Sharing
My Stuff
September 10
Nestor Wilke
2 items
Private
Audit of Small Business Sales August.xlsx
September 10
Nestor Wilke
13.8 KB
Shared
BI Improvement.docx
September 10
Nestor Wilke
22.5 KB
Shared
CSATData.xlsx
September 10
Nestor Wilke
30.9 KB
Private
CSATGoals Q2-Q3.docx
September 10
Nestor Wilke
1.24 MB
Private
Employee Engagement Plan.docx
September 10
Nestor Wilke
731 KB
Private
IR Handbook.pptx
September 10
Nestor Wilke
66.0 KB
Private
Over Budget Areas.xlsx
September 10
Nestor Wilke
15.5 KB
Private
Proposed_agenda_topics.docx
September 10
Nestor Wilke
691 KB
Private
Q3 Asia Shipping Budget Review.pptx
September 10
Nestor Wilke
76.2 KB
Shared
RD Projects KPIs.pptx
September 10
Nestor Wilke
343 KB
Shared
Trey Research Integration Plan.pptx
September 10
Nestor Wilke
1.58 MB
Private
Woodgrove Bank Annual Food Drive.pdf
4 hours ago
Nestor Wilke
590 KB
Private
Woodgrove Home Loan Application - DB...
4 hours ago
Nestor Wilke
32.5 KB
Private
Woodgrove Purchasing Data - Q1.xlsx
4 hours ago
Nestor Wilke
21.5 KB
Private
Woodgrove Bank An....pdf
Open file
Show all


My files - OneDrive
https://m365x362046-my.sharepoint.com/personal/nestorw_m365x362046_onmicrosoft_com/_layouts/15/onedrive.aspx
Contoso Electronics
OneDrive
Search
All files
Nestor Wilke
My files
Recent
Shared
Recycle bin
Shared libraries
Benefits
The Landing
Create shared library
Get the OneDrive apps
Return to classic OneDrive
New
Upload
Sync
Automate
Sort
My files
Name
Modified
Modified By
File size
Sharing
My Stuff
September 10
Nestor Wilke
2 items
Private
Audit of Small Business Sales August.xlsx
September 10
Nestor Wilke
13.8 KB
Shared
BI Improvement.docx
September 10
Nestor Wilke
22.5 KB
Shared
CSATData.xlsx
September 10
Nestor Wilke
30.9 KB
Private
CSATGoals Q2-Q3.docx
September 10
Nestor Wilke
1.24 MB
Private
Employee Engagement Plan.docx
September 10
Nestor Wilke
731 KB
Private
IR Handbook.pptx
September 10
Nestor Wilke
66.0 KB
Private
Over Budget Areas.xlsx
September 10
Nestor Wilke
15.5 KB
Private
Proposed_agenda_topics.docx
91 KB
Private
Q3 Asia Shipping Budget Review.pptx
6.2 KB
Shared
RD Projects KPIs.pptx
43 KB
Shared
Trey Research Integration Plan.pptx
58 MB
Private
Woodgrove Bank Annual Food Drive.pdf
90 KB
Private
Woodgrove Home Loan Application - DB...
2.5 KB
Private
Woodgrove Purchasing Data - Q1.xlsx
1.5 KB
Private
Woodgrove Home Loan Application - DB345
6 Views
See details
Contains sensitive information. Some commands aren't available.
View policy tip
1 Viewer · 6 Views
You viewed this
4h ago
Woodgrove Bank An....pdf
Open file
Show all

Nestor Wilke

Open Share Copy link Download Delete Rename Automate ... Sort 1 selected

My files
Recent
Shared
Recycle bin
Shared libraries
Benefits
The Landing
Create shared library

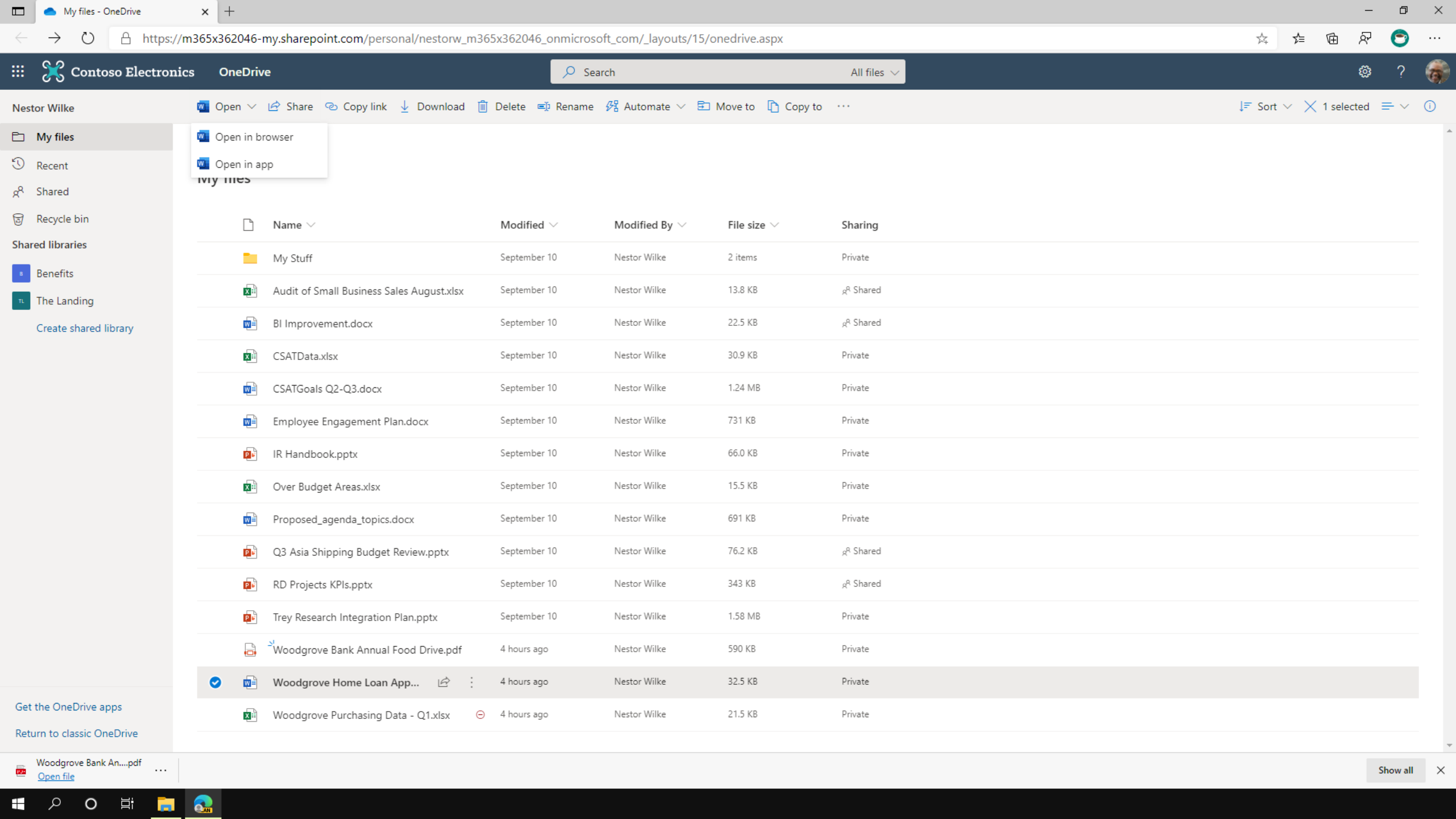
My files

Name	Modified	Modified By	File size	Sharing
My Stuff	September 10	Nestor Wilke	2 items	Private
Audit of Small Business Sales August.xlsx	September 10	Nestor Wilke	13.8 KB	Shared
BI Improvement.docx	September 10	Nestor Wilke	22.5 KB	Shared
CSATData.xlsx	September 10	Nestor Wilke	30.9 KB	Private
CSATGoals Q2-Q3.docx	September 10	Nestor Wilke	1.24 MB	Private
Employee Engagement Plan.docx	September 10	Nestor Wilke	731 KB	Private
IR Handbook.pptx	September 10	Nestor Wilke	66.0 KB	Private
Over Budget Areas.xlsx	September 10	Nestor Wilke	15.5 KB	Private
Proposed_agenda_topics.docx	September 10	Nestor Wilke	691 KB	Private
Q3 Asia Shipping Budget Review.pptx	September 10	Nestor Wilke	76.2 KB	Shared
RD Projects KPIs.pptx	September 10	Nestor Wilke	343 KB	Shared
Trey Research Integration Plan.pptx	September 10	Nestor Wilke	1.58 MB	Private
Woodgrove Bank Annual Food Drive.pdf	4 hours ago	Nestor Wilke	590 KB	Private
Woodgrove Home Loan App...	4 hours ago	Nestor Wilke	32.5 KB	Private
Woodgrove Purchasing Data - Q1.xlsx	4 hours ago	Nestor Wilke	21.5 KB	Private

Get the OneDrive apps
Return to classic OneDrive

Woodgrove Bank An....pdf
Open file

Show all


My files - OneDrive
https://m365x362046-my.sharepoint.com/personal/nestorw_m365x362046_onmicrosoft_com/_layouts/15/onedrive.aspx
Contoso Electronics
OneDrive
Search
All files
Nestor Wilke
Open
Share
Copy link
Download
Delete
Rename
Automate
Move to
Copy to
Sort
1 selected
Open in browser
Open in app
My files
Recent
Shared
Recycle bin
Shared libraries
Benefits
The Landing
Create shared library
Get the OneDrive apps
Return to classic OneDrive
Name
Modified
Modified By
File size
Sharing
My Stuff
September 10
Nestor Wilke
2 items
Private
Audit of Small Business Sales August.xlsx
September 10
Nestor Wilke
13.8 KB
Shared
BI Improvement.docx
September 10
Nestor Wilke
22.5 KB
Shared
CSATData.xlsx
September 10
Nestor Wilke
30.9 KB
Private
CSATGoals Q2-Q3.docx
September 10
Nestor Wilke
1.24 MB
Private
Employee Engagement Plan.docx
September 10
Nestor Wilke
731 KB
Private
IR Handbook.pptx
September 10
Nestor Wilke
66.0 KB
Private
Over Budget Areas.xlsx
September 10
Nestor Wilke
15.5 KB
Private
Proposed_agenda_topics.docx
September 10
Nestor Wilke
691 KB
Private
Q3 Asia Shipping Budget Review.pptx
September 10
Nestor Wilke
76.2 KB
Shared
RD Projects KPIs.pptx
September 10
Nestor Wilke
343 KB
Shared
Trey Research Integration Plan.pptx
September 10
Nestor Wilke
1.58 MB
Private
Woodgrove Bank Annual Food Drive.pdf
4 hours ago
Nestor Wilke
590 KB
Private
Woodgrove Home Loan App...
4 hours ago
Nestor Wilke
32.5 KB
Private
Woodgrove Purchasing Data - Q1.xlsx
4 hours ago
Nestor Wilke
21.5 KB
Private
Woodgrove Bank An....pdf
Open file
Show all

Customer ID: 234234234

Loan Application

Name of Applicant Megan

Surname of Applicant Bowen

Address Old Natchez Trace Rd, Mathiston, MS, 39752

Contact Number 327-322-733245

Identify provided Driver's license

Type of Loan Home

Loan Amount $600,000

Employment Details Employed

Name of Employer Microsoft

No of Years with Employer 8

Position Manager

Net Salary $120,000

Other Loan Details

Loan 1 Personal

Amount $30,000

CONFIDENTIAL

How can Inova Solutions help?

Guardian 360

- Adaptive Security & Monitoring
- Automatic Remediation
- Audits and reports

Guardian 360

- Security baselines based on CIS best practices
- Establish custom baselines based on your orgs needs

CIS Center for Internet Security®
Creating Confidence in the Connected World.

Thank you

- Any questions?