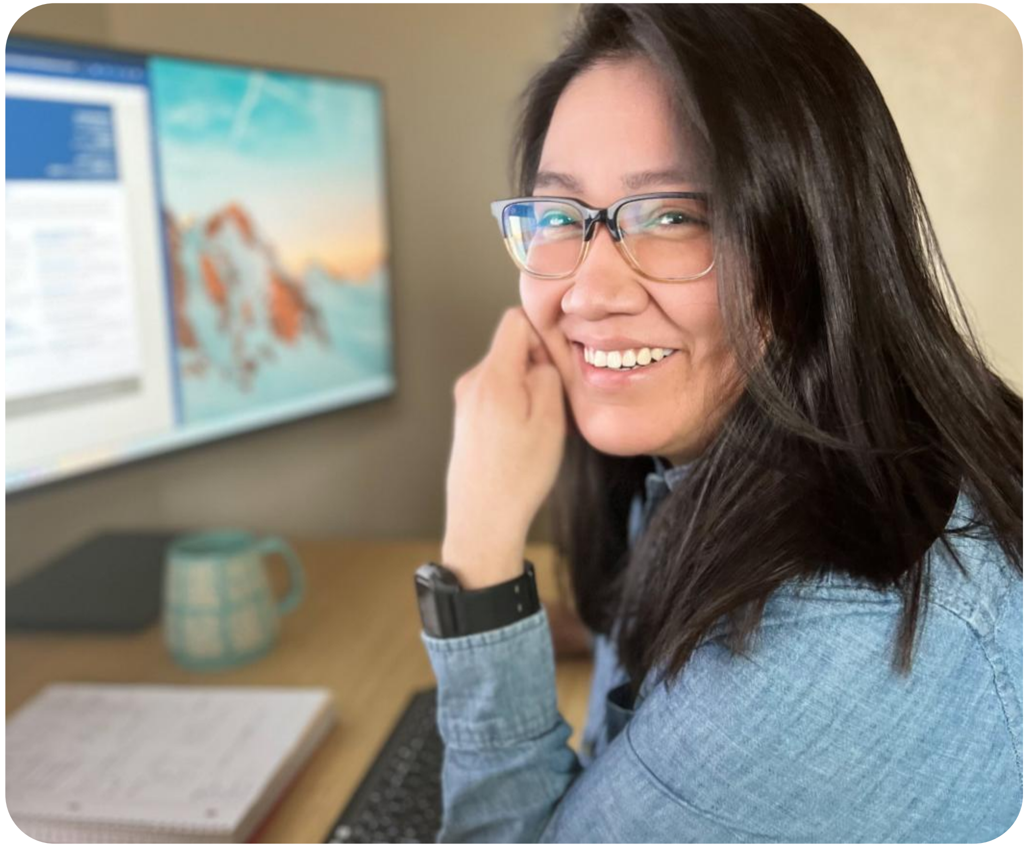
HOW TO SECURE

Microsoft 365 from Scratch

917SOLUTIONS
DELIVERING THE FUTURE

INTRODUCTION



- My name is Gerty Tsinnie
- Former Microsoft 365 Consultant to Fortune 500 and 1000 Companies
- After spending well over a decade leading corporate IT teams, I left the comfort of Corporate IT to start my business.
- Now CEO of 917 Solutions, AZ-based Cybersecurity Company started in 2022
- Delivered over 100 projects across 70 clients in the past 2 years and counting

Before we begin:

- Identify Your Primary Goals
- Understanding the Capabilities / Features of Your Licensing
- Pick Somewhere to Start
- Build a Framework for Managing What You’ve Turned On/Off
- Perform Technical Configuration Items

1. Identify Your Primary Goals

Why now? What's the reason behind the urgency and why is this important to your organization?

1. Identify Your Primary Goals

Are there Cyber insurance requirements that you need to meet?

- Multi-Factor Authentication (MFA)
- BitLocker Encryption
- Endpoint Detection and Response
- Vulnerability Management & Cybersecurity Training

Do you have Compliance requirements looming over your shoulder?

- HIPPA
- GDPR

Do you have Vendor Security Questionnaires that you’re not filling out correctly?

OR do you have a feeling that you could be managing Microsoft 365 more than you are right now?

2. Understand the Features of Your Licensing

Different licenses in Microsoft 365 unlock different features that are available to you and the capacity / context that they can be used in.

- Intune (Mobile Device Management)
- Defender for Office 365 (Phishing Filter)
- Conditional Access Policies (MFA)
- Defender for Business (Anti-Virus / Endpoint Detection and Response, Vulnerability Management)
- Microsoft Teams (Webinars)
- SharePoint

Example: Business Standard vs. Business Basic

Business Basic ($6 user/month)

- Gives you access to use only the Online versions of Microsoft 365 (Word, Excel, PowerPoint and Teams)
- Offers 50 GBs of Email Storage + 50 GBs of Email Archiving
- Does not include Defender for Office 365 P1
- Does not include Entra ID Plan 1 license (Conditional access policies)
- No access to Intune
- Does not include ability to create/host Webinars

Business Standard ($12.50 user/month)

- Gives you access to use the Desktop versions of Microsoft 365 (Word, Excel, PowerPoint and Teams)
- Includes 50 GBs of Email Storage + 50 GBs of Email Archiving
- Does not include Defender for Office 365 P1
- Does not include Entra ID Plan 1 license (Conditional access policies)
- No access to Intune
- Includes ability to create/host Webinars

Look up your licenses to see what features you have access to:
https://m365maps.com/matrix.htm#0001110000000000000000

Our recommendation: Business Premium

Business Standard ($12.50 user/month)

- Gives you access to use the Desktop versions of Microsoft 365 (Word, Excel, PowerPoint and Teams)
- Includes 50 GBs of Email Storage + 50 GBs of Email Archiving
- Does not include Defender for Office 365 P1
- Does not include Entra ID Plan 1 license (Conditional access policies)
- No access to Intune
- Includes ability to create/host Webinars

Business Premium ($22 user/month)

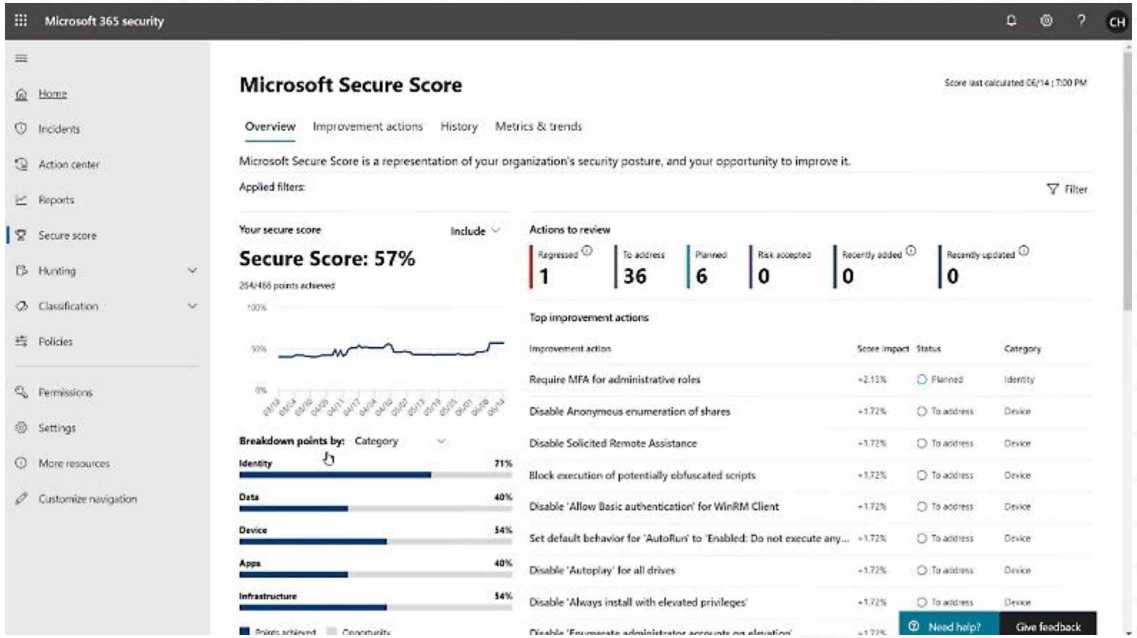
- Gives you access to use the Desktop versions of Microsoft 365 (Word, Excel, PowerPoint and Teams)
- Includes 150 GBs of Email Storage + 1.5TBs of Email Archiving
- Includes Defender for Office 365 P1
    - Phishing Filter
- Includes Entra ID Plan 1 license (Conditional access policies)
    - MFA and more policies
- Includes Intune
    - Encryption
    - Vulnerability Management
    - Enforce Security Controls
- Includes ability to create/host Webinars
- Includes Defender for Business
    - Anti-Virus / Endpoint Detection and Response

Designed for Companies with less than 300 licensed users

Look up your licenses to see what features you have access to:
https://m365maps.com/matrix.htm#000111000000000000000

3. Pick Somewhere to Start

1. Microsoft Secure Score
2. Microsoft Identity Score
3. Notifications from Microsoft 365 (Fast Track)
4. CIS Baseline Recommendations
5. Or you could use our Microsoft 365 SOPs as a reference guide



Microsoft Secure Score

Score last calculated 06/14 ; 7:00 PM

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

Applied filters:

Your secure score

Secure Score: 57%

264/466 points achieved

Breakdown points by: Category

Identity	71%
Data	40%
Device	54%
Apps	40%
Infrastructure	54%

■ Points achieved ■ Opportunity

Actions to review

Regressed	To address	Planned	Risk accepted	Recently added	Recently updated
1	36	6	0	0	0

Top improvement actions

Improvement action	Score impact	Status	Category
Require MFA for administrative roles	+2.15%	○ Planned	Identity
Disable Anonymous enumeration of shares	+1.72%	○ To address	Device
Disable Solicited Remote Assistance	+1.72%	○ To address	Device
Block execution of potentially obfuscated scripts	+1.72%	○ To address	Device
Disable 'Allow Basic authentication' for WinRM Client	+1.72%	○ To address	Device
Set default behavior for 'AutoRun' to 'Enabled: Do not execute any...	+1.72%	○ To address	Device
Disable 'Autoplay' for all drives	+1.72%	○ To address	Device
Disable 'Always install with elevated privileges'	+1.72%	○ To address	Device
Disable 'Enumerate administrator accounts on elevation'	+1.72%		

917SOLUTIONS
DELIVERING THE FUTURE

4. Build a Framework for Managing Your Settings

Microsoft Secure Score in Compliance Center

- Export the spreadsheet of recommendations and document the settings that you enable/disable as you're working through it.

Microsoft Identity Score in Entra ID

- Download the spreadsheet of recommendations and track the settings that you're modifying as you're working through it.

Notifications from Microsoft 365 (Fast Track)

- Work with the Microsoft Fast Track team to deploy Microsoft 365 at the pace that they pick for you.
- Free for business under 150 users

CIS Baseline Recommendations

- Download all applicable CIS baseline guides and start here.
- There are about 5-10 of these that you could use in total

Or you could use our Microsoft 365 SOPs as a reference guide

- We start from scratch and work through the configuration step-by-step

We're doing this one today

Performing Technical Configuration Items in Microsoft 365 🛠️

917SOLUTIONS
DELIVERING THE FUTURE

Pre-Requisites

To start, you will need at least Microsoft 365 Business Premium or Microsoft 365 E5 license. We also recommend that the user making the changes is a Global Administrator

Overview of Instructions

Why is this structured this way? We setup Microsoft 365 in the following order to make sure that we are:

1 Auditing any previous settings and documenting what changes we make

2 Catching any misconfigured settings and verifying that they are adjusted the right way

3 Each steps lends itself to another step in the process, preventing you from having to stop what you’re doing, go back, make a change, then go back to what you were doing

1 Create Security Groups

2 Entra ID Tenant and Microsoft 365 Tuning

3 Audit Users / Mailboxes / Service Accounts

4 Exchange Mailflow Rules

5 MFA Audit + Baselining

6 Conditional Access Policies + Reporting

7 Organization Customization

8 Defender for Office 365

9 Intune Deployment & Configuration

10 Microsoft Defender for Endpoint

1 Create Security Groups

- Devices Enrolled via Autopilot
- Devices Enrolled as Company Owned
- Devices Enrolled as BYOD Personal
- Devices Enrolled as Entra ID Joined
- Devices Enrolled as Hybrid Entra ID Joined
- Corporate Test Devices
- Corporate Pilot Devices
- Corporate Test Users
- Corporate Pilot Users
- Microsoft Defender for Endpoint Test Users
- Microsoft Defender for Endpoint Windows Enrolled Devices
- Microsoft Defender for Endpoint Windows Servers
- All Active Users
- All Active Unlicensed Users
- All Active Guests
- All Service Accounts
- Enforce MFA User Group
- Exclude from MFA User Group
- Exclude from Foreign Country Block
- Break Glass Administrators

2 Entra ID And Microsoft 365 Admin Tuning

Our checklist has 54 settings across Microsoft 365 and Entra ID Admin Centers that we adjust for security purposes. Here are the top settings that we would recommend adjusting at a bare minimum to improve your security:

1. ‘Microsoft 365 audit log search' is 'Enabled’
2. 'Users Can Register Applications' Is Set to 'No'
3. 'Restrict non-admin users from creating tenants' is set to 'Yes'
4. 'Restrict access to Microsoft Entra admin center' is Set to 'Yes'
5. 'Notify users on password resets?' is set to 'Yes'
6. 'Notify all admins when other admins reset their password?' is set to 'Yes'
7. 'Users can create security groups in Azure portals, API or PowerShell' is set to 'No'
8. 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No'
9. 'User consent for applications' is set to 'Do not allow user consent'
10. 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No'
11. Subscription leaving Microsoft Entra ID directory’ is set to No One

These settings alone help to prevent hackers from taking control of your environment via Phishing Links that get clicked by users within your environment.

3 Audit Users / Mailboxes / Service Accounts

The most common area of mismanagement in Microsoft 365 is user accounts.

When a user is terminated:

- Convert the mailbox to a Shared Mailbox to preserve its integrity.
- Block the user’s sign-in to prevent unauthorized access.
- Remove the license and reassign it to a new user or reduce the licensing count.

Common issues found:

- Mailboxes are not converted to Shared Mailboxes, leading to data loss.
- Terminated users' sign-ins remain active, allowing continued access to company resources.

To mitigate these issues:

- Perform steps to ensure proper management of users and service accounts.
- Avoid unnecessary licensing and prevent access where it is no longer authorized.

1. Audit and Verify Active Users and Service Accounts

- Active Licensed Users and Service Accounts
- Unlicensed Users and Service Accounts

2. Secure and Manage Shared Mailboxes

- Convert User Mailboxes to Shared Mailboxes
- Block Sign-In For Shared Mailboxes
- Block Shared Mailboxes in Microsoft 365 Admin Center

3. Audit Administrator Privileges

- Right-sizing Global Admin Roles
- Separate Admin Accounts
- Ensure that 2 Break Glass Admin accounts are created

4. Enforce Archiving Policies

- Implement Mailbox Archiving Policies

5. Audit and Secure Service Accounts

- Reset passwords and Rotate Keys for Service Accounts

6. Audit Sign-In Logs and Activity

- Review Sign-In Logs to identify suspicious behavior and flag incidents for response.

7. Disable Legacy Authentication

- Disable IMAP/POP across existing mailboxes
- Disable IMAP and POP for all future mailboxes

8. Set aside time to perform a Quarterly Audit

917SOLUTIONS
DELIVERING THE FUTURE

4 Exchange Mailflow Rules

Below are examples of Mailflow Rules we create to consolidate and make sense of existing rules in environments and prevent confusion.

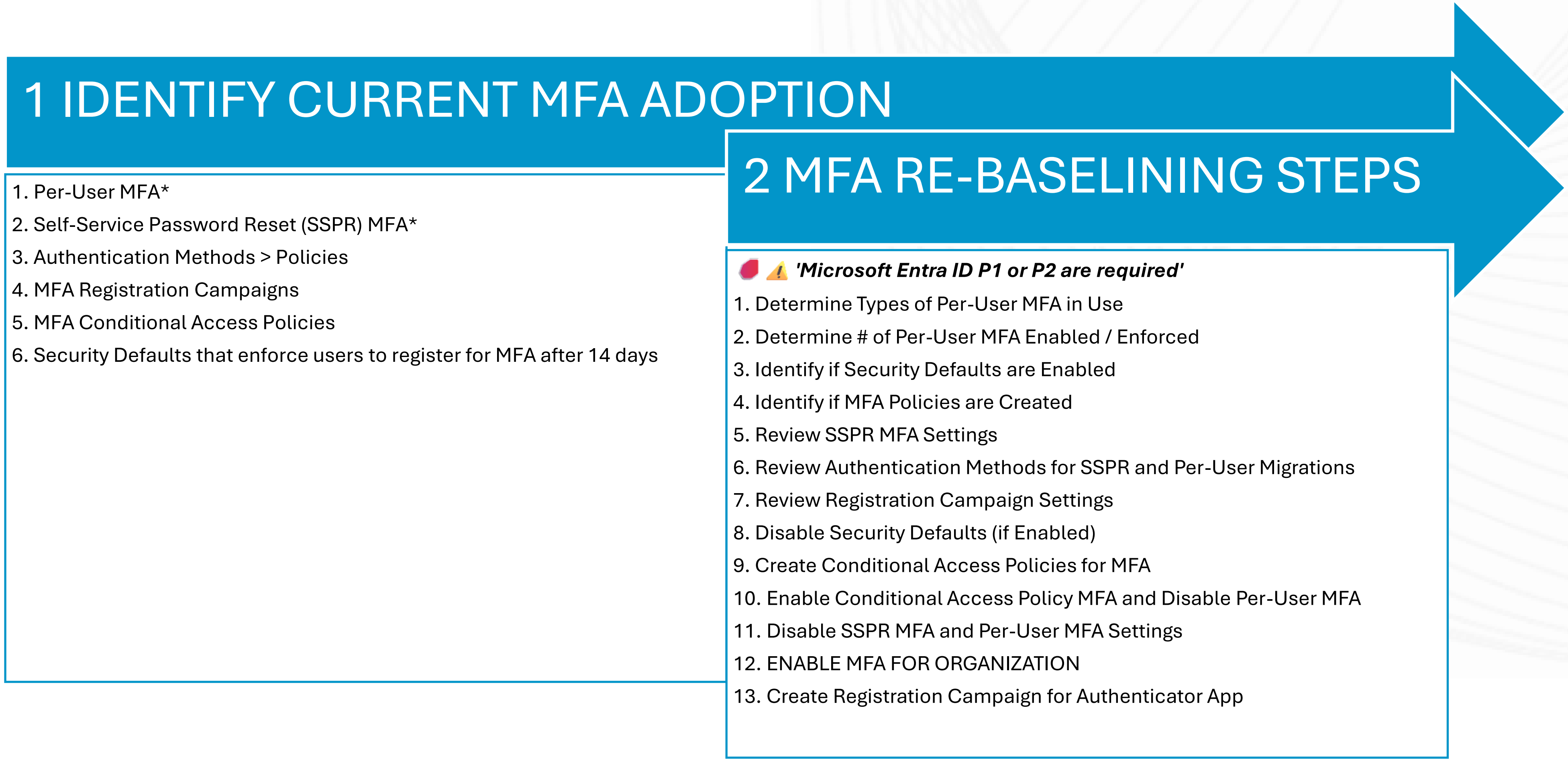
1. ⚠️ 🛑 Approved Domains
2. ⚠️ 🛑 Approved Senders
3. ⚠️ 🛑 Approved IPs
4. ⚠️ Blocked Domains
5. ⚠️ Blocked Senders
6. Append Confidentiality Disclaimer
7. External Sending Warning
8. ⚠️ 🛑 Quarantine Domain Impersonation Attempts
9. Encryption Apply (Internal)
10. Encryption Apply (External) | Enable
11. Configure Alerting Policies within Exchange Admin Center

For organizations that have the Defender for Office 365 P1 license as part of their plan – Use the Anti-Spam Policy to Allow and Block Senders.

For organizations who only have Exchange Online Protection, you may find that creating Mailflow Rules is what you need to manage email filtering in your environment.

NOTE: *For Allowing and Blocking Domains, Senders and IP addresses Microsoft recommends that you utilize the Anti-Spam Policy within Defender for Office 365 to ensure that emails are scanned utilizing Microsoft's Advanced Threat Protection Features*

5 MFA Audit + Baselining



1 IDENTIFY CURRENT MFA ADOPTION

1. Per-User MFA*
2. Self-Service Password Reset (SSPR) MFA*
3. Authentication Methods > Policies
4. MFA Registration Campaigns
5. MFA Conditional Access Policies
6. Security Defaults that enforce users to register for MFA after 14 days

2 MFA RE-BASELINING STEPS

🛑 ⚠️ ***'Microsoft Entra ID P1 or P2 are required'***

1. Determine Types of Per-User MFA in Use
2. Determine # of Per-User MFA Enabled / Enforced
3. Identify if Security Defaults are Enabled
4. Identify if MFA Policies are Created
5. Review SSPR MFA Settings
6. Review Authentication Methods for SSPR and Per-User Migrations
7. Review Registration Campaign Settings
8. Disable Security Defaults (if Enabled)
9. Create Conditional Access Policies for MFA
10. Enable Conditional Access Policy MFA and Disable Per-User MFA
11. Disable SSPR MFA and Per-User MFA Settings
12. ENABLE MFA FOR ORGANIZATION
13. Create Registration Campaign for Authenticator App

6 Conditional Access Policies

Conditional Access Policies are essential for organizations aiming to adopt a Zero Trust environment.

They safeguard user sign-ins against malicious activity.

Enable enforcement of granular security policies at scale to enhance organizational security.

Here are some examples of policies that we create by default for organizations that we work with.

As incredible as these policies are, they are also **INCREDIBLY DANGEROUS**.

Pay attention to the ⚠️ 🛑 as enabling these settings without understanding the impact to your organization could result in your end-users revolting against you.

For any Conditional Access policies that you are creating, make sure you are excluding your Break Glass Admin Accounts.

1. ⚠️ BLOCK - All users access to Windows Azure Service Manager API | CIS
2. BLOCK - Authenticator Transfer
3. BLOCK - Device Code Flow
4. ⚠️ BLOCK - High-Risk Sign-Ins
5. ⚠️ BLOCK - High-Risk Users
6. ⚠️ BLOCK - Legacy Authentication
7. 🛑 BLOCK - Logins from Foreign Countries
8. 🛑 BLOCK - Registration from Untrusted Locations
9. ⚠️ BLOCK - Unmanaged Access to Desktop Apps
10. ⚠️ BLOCK - Unmanaged Downloads from Desktop Apps
11. ⚠️ BLOCK - Unsupported Device Platforms
12. 🛑 BLOCK - Untrusted Locations
13. GRANT - MFA for All Active Users | CIS
14. GRANT - MFA for All Admins | CIS
15. GRANT - MFA for All Active Guests
16. ⚠️ GRANT - MFA for Device Register or Join
17. GRANT - MFA for Windows Azure Service Manager API
18. ⚠️ GRANT - Medium-Risk Sign-ins
19. ⚠️ GRANT - Medium-Risk Users
20. 🛑 GRANT - Require Compliant Mobile Devices
21. 🛑 GRANT - Require Compliant Windows Devices
22. 🛑 GRANT - Security Info Registration from Trusted Locations
23. GRANT - Terms of Use
24. 🛑 SESSION - Periodic reauthentication on Unmanaged devices

7 Organization Customization

- **Collect Organization Logos**
  - Favicon size requirement: 32x32px
  - Background image size requirement: 1920x1080px
  - Banner Logo: 245x36px
  - Square logo (for light and dark themes): 240x240px
- **Collect Organization Colors**
  - Hexcode Colors
- **Apply Organization Logos and Colors to Microsoft 365 Sign-In**

Why not make your Organization uniquely YOURS?

Some providers may downplay the importance of branding, claiming that attacks can spoof it anyway. However, the real concern is your users' experience, which is critical to maintain trust and engagement

8 Defender for Office 365

Most Commonly Missed Configuration Settings

1. Configure Quarantine Policy
2. Update Quarantine Policy Global Settings
3. **Add Email to Alert Policy in Microsoft Defender**
4. **Configure Incident Notification Rule**
5. Enable User Reported Add-ins in Admin Center
6. Create Shared Mailbox for User Reported Emails
7. Configure User Reported Settings
8. Add the Shared Mailbox to Advanced delivery settings

1 ANTI-PHISHING

- Office365 AntiPhish Default (Default)

2 ANTI-SPAM

- Anti-spam inbound policy (Default)
- Allowed and blocked senders and domains
- Connection filter policy (Default)
- Anti-spam outbound policy (Default)

3 ANTI-MALWARE

- Default (Default)

4 SAFE ATTACHMENTS

- Safe Attachments Policy

5 SAFE LINKS

- Safe Links policy

6 EMAIL NOTIFICATIONS FOR DEFENDER FOR OFFICE 365

- Incident Notification Rule

7 MAINTAINING DEFENDER FOR OFFICE 365

- Incidents & Alerts
- Actions & Submissions

9 Intune (Windows)

I build Intune in sections:

1. Core – App Protection Policies (Optional for some)
2. Core – Compliance Policies
3. Core – Enrollment Profiles
4. Custom – Device Configuration
5. Custom – Settings Catalog
6. Essential – Notifications
7. Essential – Scripts

When you're rolling out Intune, you need to understand the Why.

Because there are so many features available in Intune – I like to run teams through my Pre-Requisite Discovery Questionnaire.

Based on the answers to the questionnaire, I can point you to which settings you can import into your environment at scale.

9 Intune (Windows) Cont'd – Discovery Questions

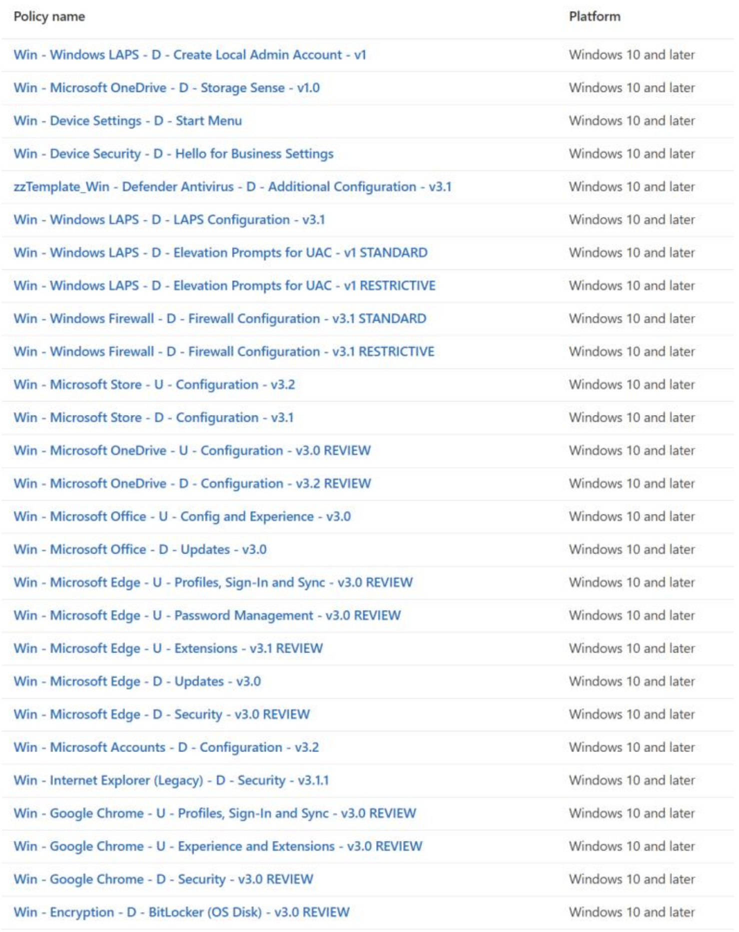
1. **Are users able to install their own software? Yes/No**
   1. Do they use their own account or a specific account on machine? Yes/No
   2. Does the team want to revoke admin privileges? Yes/No
   3. Document current admins on machines.
2. **Is BitLocker currently deployed in the environment? Yes/No**
   1. Encrypt OS Drives Yes/No
   2. Encrypt Fixed Drives Yes/No
   3. Encrypt Removable USB drives Yes/No
3. **Is there a defined Onboarding / Offboarding Process? Yes/No**
4. **Will updates be managed through Intune or another 3rd party tool?**
5. **Will apps be pushed through Intune or another 3rd party tool?**
6. **Is the org currently using Windows Hello for Business? Yes/No**
7. **How are vulnerabilities currently being managed?**
8. **Is there an Anti-virus currently installed within the Organization?**
   1. If there is an AV in place, you can still deploy Defender for Endpoint in passive mode - where the current AV and Defender can run concurrently. Is this desired?

Here are some sample discovery questions that you can ask yourself.

I like to ask these before I start an engagement with a customer to gauge what they need so I know what to build inside of their environment.

917SOLUTIONS
DELIVERING THE FUTURE

9 Intune Cont’d



Policy name	Platform
Win - Windows LAPS - D - Create Local Admin Account - v1	Windows 10 and later
Win - Microsoft OneDrive - D - Storage Sense - v1.0	Windows 10 and later
Win - Device Settings - D - Start Menu	Windows 10 and later
Win - Device Security - D - Hello for Business Settings	Windows 10 and later
zzTemplate_Win - Defender Antivirus - D - Additional Configuration - v3.1	Windows 10 and later
Win - Windows LAPS - D - LAPS Configuration - v3.1	Windows 10 and later
Win - Windows LAPS - D - Elevation Prompts for UAC - v1 STANDARD	Windows 10 and later
Win - Windows LAPS - D - Elevation Prompts for UAC - v1 RESTRICTIVE	Windows 10 and later
Win - Windows Firewall - D - Firewall Configuration - v3.1 STANDARD	Windows 10 and later
Win - Windows Firewall - D - Firewall Configuration - v3.1 RESTRICTIVE	Windows 10 and later
Win - Microsoft Store - U - Configuration - v3.2	Windows 10 and later
Win - Microsoft Store - D - Configuration - v3.1	Windows 10 and later
Win - Microsoft OneDrive - U - Configuration - v3.0 REVIEW	Windows 10 and later
Win - Microsoft OneDrive - D - Configuration - v3.2 REVIEW	Windows 10 and later
Win - Microsoft Office - U - Config and Experience - v3.0	Windows 10 and later
Win - Microsoft Office - D - Updates - v3.0	Windows 10 and later
Win - Microsoft Edge - U - Profiles, Sign-In and Sync - v3.0 REVIEW	Windows 10 and later
Win - Microsoft Edge - U - Password Management - v3.0 REVIEW	Windows 10 and later
Win - Microsoft Edge - U - Extensions - v3.1 REVIEW	Windows 10 and later
Win - Microsoft Edge - D - Updates - v3.0	Windows 10 and later
Win - Microsoft Edge - D - Security - v3.0 REVIEW	Windows 10 and later
Win - Microsoft Accounts - D - Configuration - v3.2	Windows 10 and later
Win - Internet Explorer (Legacy) - D - Security - v3.1.1	Windows 10 and later
Win - Google Chrome - U - Profiles, Sign-In and Sync - v3.0 REVIEW	Windows 10 and later
Win - Google Chrome - U - Experience and Extensions - v3.0 REVIEW	Windows 10 and later
Win - Google Chrome - D - Security - v3.0 REVIEW	Windows 10 and later
Win - Encryption - D - BitLocker (OS Disk) - v3.0 REVIEW	Windows 10 and later

Over the years, I have collected policies that I have built to streamline deployments in Microsoft 365, specifically for Intune. We have 57 templates that we import by default that cover:

- OneDrive
- Edge
- Google Chrome
- Firewall
- Defender for Endpoint Settings
- Local Admin Policies and Configuration Rules

I have made these templates available along with our SOPs and these are what my team uses to deploy Microsoft 365 in bulk.

If you’re looking at building something comprehensive of your own, I would recommend checking out the following creators, I have adopted OIB’s naming convention for example – it makes looking for and assigning policies so simple.

10 Microsoft Defender for Endpoint (Business)

- Last but not least, Microsoft Defender for Endpoint (Business)
- This final step adds additional alerting to your environment.
- You would be surprised at what Defender picks up that other tools miss.

1. Create Connection from Defender to Intune
2. Create MDE Onboarding Profile
3. Defender Incident Alerts
4. Defender Vulnerability Management Alerts
5. Defender Threat Analytics Reports
6. Enforcement Scope for Devices (Do this last for your deployment)
7. Automated Tagging for Devices
8. Additional settings to configure for Defender for Endpoint

Q&A

917SOLUTIONS

DELIVERING THE FUTURE

Our Services at 917

Managed IT & Cybersecurity Services

We handle all of your IT and Cybersecurity for you.

Microsoft 365/Cloud Consulting
For organizations who need help navigating Microsoft licensing and deployment of Microsoft/Azure Tools.

Microsoft 365 SOPs
Step-by-step guide to deploy Microsoft 365 from scratch for DIY Teams and Service Providers.

Co-Managed Cyber Services

We help your IT team manage your Cybersecurity.

vCISO Services for AEC + Manufacturing
Strategic cybersecurity leadership, risk management, and compliance support to help businesses enhance their security posture.

Risk Assessments
For organizations seeking to understand where their biggest gaps in security are.

Follow us on our Social Media for More Updates

You can find 917 Solutions on LinkedIn, Facebook, and Instagram.

You can find me, Gerty Tsinnie on LinkedIn, Facebook, and Instagram as well.

Any questions or inquiries, email me at Gerty@917solutions.com

917SOLUTIONS
DELIVERING THE FUTURE