

cobweb

Tenant Review

for Company 456



Contents

Your Office 365 Tenant	3
The Tenant Review Process.....	4
Your Microsoft 365 Tenant Information	5
Identity & Access Management	6
Directory Synchronisation	7
What is Directory Synchronisation?.....	7
Directory Synchronisation Report.....	8
Password Protection	12
What is Entra ID Password Protection?	12
Entra ID Password Protection Report	13
Self Service Password Reset	15
What is Self Service Password Reset?.....	15
Self Service Password Reset Report.....	16
Modern Authentication	18
What is Modern Authentication?.....	18
Modern Authentication Report	18
Conditional Access	19
What is Conditional Access?.....	19
Conditional Access Report	21
Legacy Authentication	24
What is Legacy Authentication?	24
Legacy Authentication Report	24
Multi-Factor Authentication (MFA)	26
What is MFA?	26
Multi-Factor Authentication Report.....	26
Entra Privileged Identity Management (PIM).....	28
What is PIM?	28
Entra privileged Identity Management Report.....	29
Entra ID Guest Access	31
Entra ID Guest Access Report	31
Entra ID Users.....	33
Entra ID Users Report.....	33
Entra ID Gallery & Enterprise Applications Report.....	37
Entra ID Group Expiration Report.....	38
Entra ID Group Naming Policies Report.....	39
Entra ID Devices.....	40
Entra ID Devices Report.....	40
Threat Protection	42
Defender for Office 365	43
What is Defender for Office?.....	43
Defender for Office 365 Report.....	44

Defender for Endpoint	47	Defender for Cloud Apps (MCAS)	73
What is Defender for Endpoint?	47	What is Defender for Cloud Apps?	73
Defender for Endpoint Report	48	Microsoft Secure Score	74
Defender for identity	51	What is Microsoft Secure Score?	74
What is Defender for Identity?	51	75
Defender for Identity Report	53	Customer Name – Your Secure Score	75
Information Protection	55	Your Key Secure Score Improvements.....	76
Microsoft Information Protection (MIP)	56	Cloud Apps and Productivity	77
What is Information Protection?	56	SharePoint Online and OneDrive for Business	78
Information Protection Report	57	SharePoint Online and OneDrive for Business – Sharing Policies Report.....	78
Data Loss Prevention	58	SharePoint Online and OneDrive for Business – Access Control Report.....	80
What is Data Loss Prevention?	58	Exchange Online	81
Data Loss Prevention Report	60	Exchange Online Report	81
Retention Policies	61	Microsoft Teams	83
What are Retention Policies?.....	61	Microsoft Teams – Users/Guest Admission Report.....	83
Office 365 Message Encryption	63	Microsoft Teams – Guest Activity Report.....	84
What is Office 365 Message Encryption?	63	Microsoft Teams – Third-party Storage Providers Report.....	86
Security Management	64	Next Steps	87
Microsoft Intune	65		
What is Microsoft Intune?	65		
Microsoft Intune Report	68		

Your Office 365 Tenant

The Tenant Review Process

This Microsoft 365 tenant review report is provided to you based on recommendations that Cobweb believe will provide core value and security benefits to Company 456 under Microsoft 365. Your Microsoft 365 Tenant review has been broken down into five core areas:






- 1. Identity and Access Management** - which incorporates conditional access, directory synchronisation, password protection, self-service password reset and the use of biometrics to enhance multi factor authentication capabilities including going password-less.
- 2. Threat Protection** - incorporating Microsoft Defender for Office 365, Microsoft Defender for Endpoint and Microsoft Defender for Identity.
- 3. Information Protection** - which covers Microsoft Purview Information Protection with sensitivity labels, as well as labels for retention; and Data Loss Prevention (DLP) and Office 365 Message Encryption to protect, or appropriately protect, leakage of information.
- 4. Security Management** - which consists of Microsoft Intune, Defender for Cloud Apps (MCAS) and Secure Score.
- 5. Cloud Apps and Productivity** - which focuses on the configuration of cloud applications such as Exchange Online, Microsoft Teams and SharePoint Online



Your Microsoft 365 Tenant Information

Tenant Name	Company 456
Tenant Microsoft Domain	Company456.onmicrosoft.com
Tenant Region	United Kingdom
Tenant Storage Locations	Exchange Online - European Union Exchange Online Protection - European Union Microsoft Teams - European Union OneDrive - United Kingdom SharePoint - United Kingdom Viva Connections - European Union
Core Licenses	Microsoft 365 Business Premium
Licensed User Count	238
Total Users	645
Total Groups	272

Total Applications	48
Total Devices	820
Entra ID Version	Entra ID Premium P1
Federated Domains	None

Key	
	Urgent action required
	Require improvements
	No action needed
	Not applicable
	Requires ongoing monitoring

Identity & Access Management

Example



Directory Synchronisation

What is Directory Synchronisation?

Entra Connect is the Microsoft tool designed to meet and accomplish your hybrid identity goals by synchronising your on-premises Active Directory to Entra ID. It provides the following features:

[Password hash synchronisation](#) - A sign-in method that synchronises a hash of users on-premises AD password with Entra ID.

- [Pass-through authentication](#) - A sign-in method that allows users to use the same password on-premises and in the cloud but doesn't require the additional infrastructure of a federated environment.
- [Federation integration](#) - Federation is an optional part of Entra Connect and can be used to configure a hybrid environment using an on-premises AD FS infrastructure. It also provides AD FS management capabilities such as certificate renewal and additional AD FS server deployments.
- [Synchronisation](#) - Responsible for creating users, groups, and other objects. As well as, making sure identity information for your on-premises users and groups is matching the cloud. This synchronisation also includes password hashes.
- [Health Monitoring](#) - Entra Connect Health can provide robust monitoring and provide a central location in the Entra ID portal to view this activity.

Directory synchronisation provides end user benefits of a single identity to access on-premises and cloud resources, allowing you to set secure and security conscious access without having to create these processes across a multitude of identities, or having varying degrees of security across each authentication provider.

Note for Company 456

Company 456 do have directory synchronisation enabled with Entra Connect.

Entra Connect 2.3.6 is in use and installed on Windows Server 2016. (Ext.Support until 2027). This machine was last restarted within 30 days.

Password Hash synchronisation is enabled for authentication with Password Writeback also enabled for Self-Service Password Reset (SSPR) from Microsoft Entra.

Seamless Sign-On is enabled with a Kerberos key creation date of 9/6/2021. Microsoft recommends the key is rotated every 30 days.

Directory Synchronisation Report

Configuration	Details/comments	Current Setting	Recommended Setting	Status
Entra Connect Synchronisation	If a Windows Server Active Directory environment is being used for user and device authentication it is recommended to deploy Entra Connect to synchronise these identities with Entra ID and Office 365. This allows for an improved user experience with a single sign-on and, when deployed with features such as Self-Service Password Reset and Password Writeback, can reduce the number of support calls being raised internally.	Enabled	Enabled	3
Password Hash Synchronisation	Password Hash Synchronisation is an optional authentication method when deploying Entra Connect. At least one authentication method must be chosen. Password Hash Synchronisation will synchronise hashed passwords to Entra ID and Office 365, meaning that when a user signs into Office 365 their authentication is still cloud based and carried out by Entra ID directly. The authentication request is not routed to the Windows Active Directory Environment. This can be seen as a positive thing from a management perspective as your users Office 365 sign-ins are not dependant on your Entra Connect Server or it's connectivity.	Enabled	Enabled	3


Directory Synchronisation Report

Configuration	Details/comments	Current Setting	Recommended Setting	Status
Pass-through Authentication	Pass-through Authentication is an optional authentication method when deploying Entra Connect. At least one authentication method must be chosen. Pass-through Authentication does not synchronise any hashed passwords to Entra ID and Office 365. Instead, when a user signs into Office 365 their authentication request is send from Entra ID to Authentication Agents installed in the Active Directory, the password they enter is hashed and compared with the password stored in Windows Active Directory. This can be seen as a positive as it means that the sign-in will honour disabled states and office hours configured in Windows Active Directory.	Disabled	Optional	3
Seamless Single Sign-On	Entra ID Seamless Single Sign-On (Entra ID Seamless SSO) automatically signs users in when they are on their corporate devices connected to your corporate network. When enabled, users don't need to type in their passwords to sign in to Entra ID. This feature provides users easy access to cloud-based applications without needing additional on-premises components. This feature can be rolled out to some or all users via Group Policy and works with Password Hash Synchronisation or Pass-Through Authentication.	Enabled Key Creation Date - 9/6/2021	Enabled Rotate Key in line with Microsoft guidance	2

Directory Synchronisation Report

Configuration	Details/comments	Current Setting	Recommended Setting	Status
Password Writeback	Enabling Password Writeback in conjunction with Self-Service Password Reset will allow your administrators and users to reset their Windows Active Directory passwords from Office 365. This process is protected by Multi-Factor Authentication and can reduce the number of support ticket raised internally, particularly if users are working remotely over VPN and only access the VPN occasionally for certain resources.	Enabled	Enabled	3
Hybrid AD Join	Organisations with existing Active Directory implementations can benefit from some of the functionality provided by Entra ID by implementing hybrid Entra ID joined devices. These devices are joined to your on-premises Active Directory and registered with Entra ID. This allows for SSO to both cloud and on-premises resources, Conditional Access through Domain join or through Intune if co-managed and Self-service Password Reset and Windows Hello PIN reset on lock screen. Hybrid AD Join is also required to leverage Windows 10 E3 or E5 CSP subscription activation licenses with Windows 10 devices that are joined to a Windows Active Directory.	Disabled	Enabled - If Windows devices are joined to the Windows Server Active Directory	2
Entra Connect Version	It is recommended to be on the latest version of Entra Connect available with a minimum recommendation of having moved to the new 2.0 version of Entra Connect. This enforces the use of TLS 1.2 communication between Entra Connect and Entra ID.	2.3.6	2.x	3

Directory Synchronisation Report

Configuration	Details/comments	Current Setting	Recommended Setting	Status
Total numbers of synchronisation errors 	You must stay on top of your synchronisation and ensure no errors are present	0	0	3

Password Protection

What is Entra ID Password Protection?

Industry leaders tell you not to use the same password in multiple places, to make it complex, and to not make it simple like “Password123”. How can organisations guarantee that their users are following best-practice guidance? How can they make sure users aren't using weak passwords, or even variations on weak passwords?

The initial step in having stronger passwords is to provide guidance to your users. Microsoft's current guidance on this topic can be found at the following link: [Microsoft Password Guidance](#)

Having good guidance is important, but even with that we know that many users will still end up choosing weak passwords. Entra ID Password Protection protects your organisation by detecting and blocking known weak passwords and their variants, as well as optionally blocking additional weak terms that are specific to your organisation. Entra ID password protection enhances password policies in an organisation by taking advantage of Microsoft sign-in analytics across the entirety of Office 365. If Microsoft detects that it has seen the password a user is

entering too many times – across the entirety of Office, or if the password is deemed weak; then it will disallow the use of the password. This is in addition to any traditional passwords policies you currently have.

Deployments of password protection also support the inclusion of custom banned-password lists that are stored in Entra ID. It performs the same checks for on-premises Active Directory, when configured, as Entra ID does for cloud-based changes. These checks are performed, audited and/or enforced during password changes and password reset scenarios.

Note for Company 456

Company 456 are enabled for Password Protection. The configuration has been left as default which is generally acceptable. Cobweb would recommend implementing a Custom banned password list and populating this with organisation information and industry terms that should not be used in passwords.