March 2023

Azure AD elaborated story —
Why backup Azure AD?

What is Azure AD?

Have you thought about what happens to your organization if the system that holds your identity and access management information gets compromised? If Azure AD is unavailable, do you know if your users will be able to maintain access to apps like SharePoint, Exhange, OneDrive, Teams & Groups, or other important Microsoft 365 data?

Azure Active Directory, also referred to as 'Azure AD', is an identity and access management tool (IAM) used by organizations to help control identities and determine what users have permission to access data and resources through secure authentication. If you are new to Azure AD, you might ask yourself "what are identities and why should you protect them?"

Why identities need protection

The most novel ransomware techniques used by attackers rely on compromising your identities first. Why? Because it is the easiest, fastest, and most effective way for attackers to get a foothold into your environment, take your data hostage, cripple your organization, and force you to pay huge ransoms.

Using multifactor authentication is the most important thing companies can do to protect their identities and deflect dominant identity attacks. In fact, Microsoft deflects more than 1,000 password attacks per second in their systems, and more than 99.9 percent of accounts that are compromised don't have multifactor authentication enabled. Clearly, without multifactor authentication enabled it is easy for attackers to compromise identities. Why is that so? Because each individual identity represents a living and breathing human being that is prone to making mistakes.

Technically, an identity can be defined as a user (customers, partners, and employees) or a device that is used by a user (computers, smartphones, routers, servers, controllers, and sensors).

Humans are often the Achilles' heel of security because curiosity and feelings drive us to make mistakes and fall for malicious tricks. Some of the common mistakes include:

- Clicking on phishing e-mail links and filling in credentials on fake sign-in pages used to capture identity information and gain access to identity network.
- Using the same passwords multiple places, allowing attackers to use credential stuffing techniques to get access to the identity environment.
- Using common passwords such as *qwerty123* or *Summer2018!* that are easy for attackers to guess.
- Writing passwords down because they are too complex to remember (or a lack of SSO) that attackers can get a hold of.

So, what happens if attackers compromise an identity?

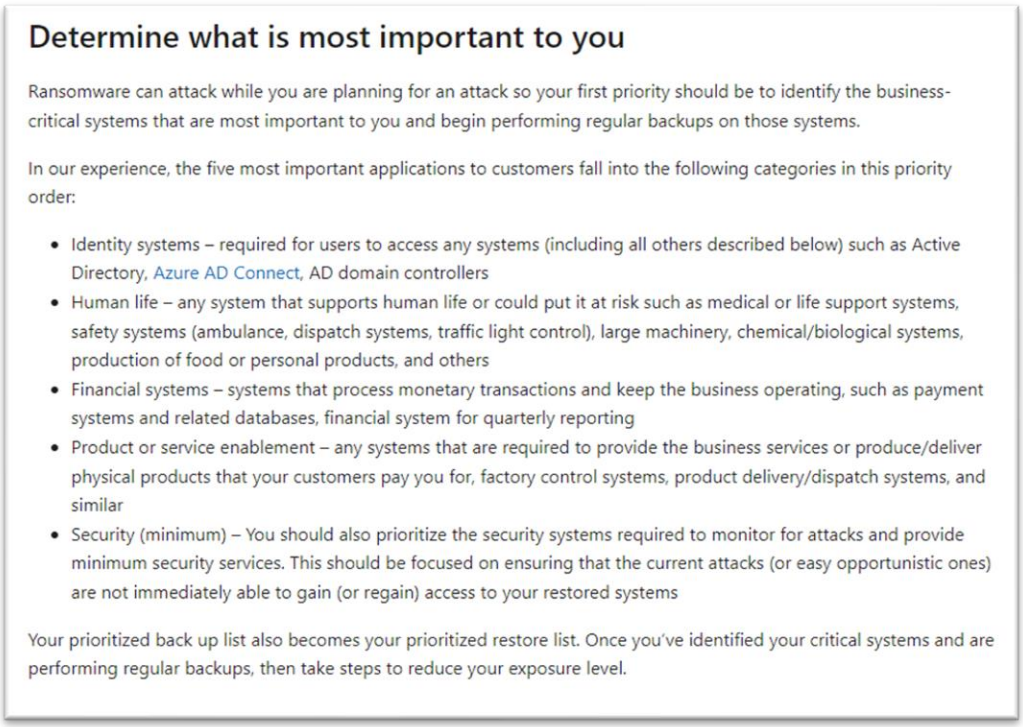
Each individual identity has a set of roles, permission, and access privileges that give the user or device special access

and control of important business applications.

Attackers that hack identities with administrative permission can use that control to create, modify, or delete identities and identity permissions in your environment with the aim of locking you out and keeping your business-critical data hostage.

If that happens, you are in a race against the attacker to secure your environment before further damage can be done.

According to Microsoft, protecting identity systems is the number one priority for any business—more important than protecting human life—as it ensures you and your users can maintain access to critical applications and systems such as Azure AD.



Determine what is most important to you

Ransomware can attack while you are planning for an attack so your first priority should be to identify the business-critical systems that are most important to you and begin performing regular backups on those systems.

In our experience, the five most important applications to customers fall into the following categories in this priority order:

- Identity systems – required for users to access any systems (including all others described below) such as Active Directory, Azure AD Connect, AD domain controllers
- Human life – any system that supports human life or could put it at risk such as medical or life support systems, safety systems (ambulance, dispatch systems, traffic light control), large machinery, chemical/biological systems, production of food or personal products, and others
- Financial systems – systems that process monetary transactions and keep the business operating, such as payment systems and related databases, financial system for quarterly reporting
- Product or service enablement – any systems that are required to provide the business services or produce/deliver physical products that your customers pay you for, factory control systems, product delivery/dispatch systems, and similar
- Security (minimum) – You should also prioritize the security systems required to monitor for attacks and provide minimum security services. This should be focused on ensuring that the current attacks (or easy opportunistic ones) are not immediately able to gain (or regain) access to your restored systems

Your prioritized back up list also becomes your prioritized restore list. Once you've identified your critical systems and are performing regular backups, then take steps to reduce your exposure level.

Whether you are an admin at a major company or launching a startup, protecting user identities is crucial. Knowing who is accessing your resources and for what purpose provides a foundation of security upon which all else rests.

Azure AD provides identity authentication and authorization for all the critical Microsoft 365 resources your organization depends upon every day, so it needs to be fully accounted for in your backup and recovery strategy. If you want to safeguard your entire Microsoft tenant, Azure AD needs to be a part of your backup and recovery strategy for Microsoft 365.

Let's explore the relationship between Azure AD and your Microsoft 365 cloud services.

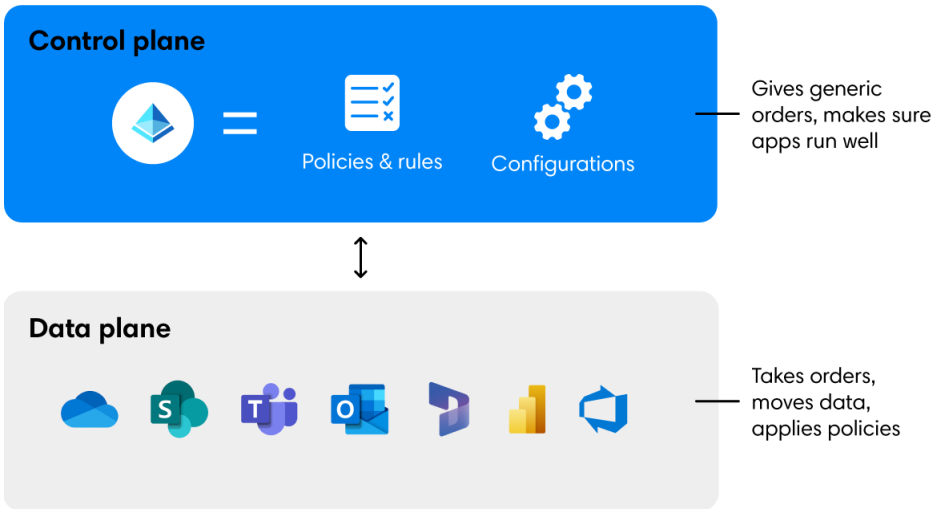
The relationship between Azure AD and Microsoft 365

In networking, a plane is an abstract conception of where certain processes take place. The two most commonly referenced planes in networking are *the control plane* and *the data plane*.

The control plane is the part of a network that controls how data packets are forwarded— meaning how data is sent from one place to another. In the context of identity and access management (IAM), Azure

AD is the control plane that manages the set of rules, policies, and other configurations to help define how the system works.

In contrast to the control plane, which determines how packets should be forwarded, the data plane actually forwards the packets. In the context of IAM, all applications connected to Azure AD for authentication represent the data plane. They take and execute orders from the control plane, move data, and apply policies:



Think of the control plane as being like the stoplights that operate at the intersections of a city. Meanwhile, the data plane is more like the cars that drive on the roads, stop at the intersections, and obey the stoplights.

Azure AD is the control plane used to manage user accounts and groups in Microsoft 365. Through SSO experience, Azure AD controls what users get access to the apps and what permissions they have.

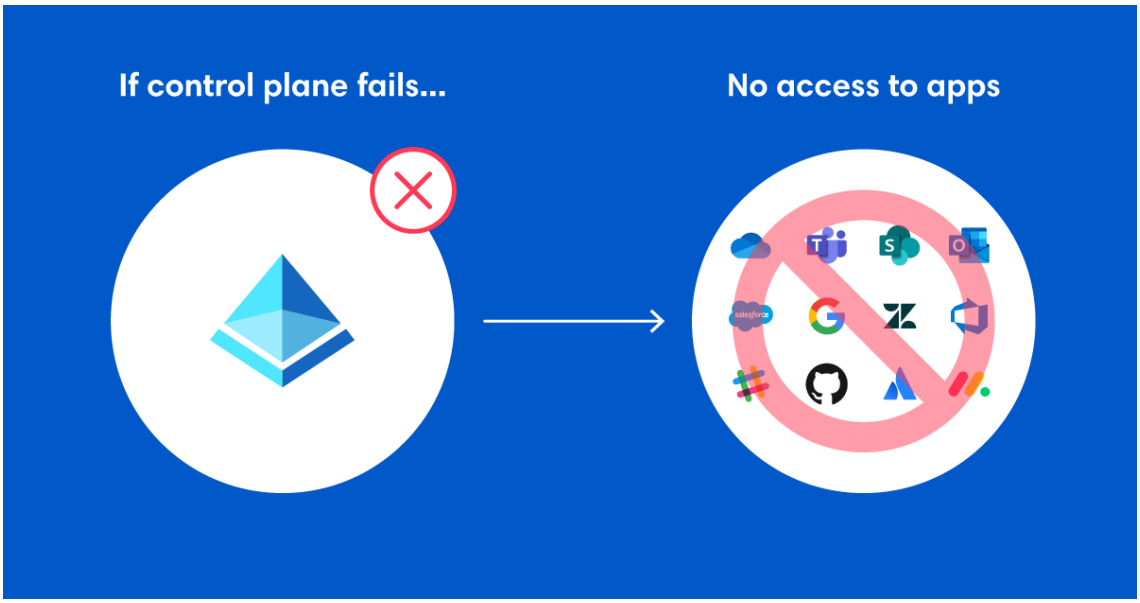
If your organization has a paid subscription to Microsoft 365, you have a free subscription to Azure AD — and that's why all Microsoft Cloud services use Azure AD for authentication. In the data plane, Microsoft 365 applications take authentication orders from Azure AD and execute them.

What happens if Azure AD is compromised?

To put it simply: Without Azure AD protection, you won't have access to your Microsoft 365 data.

Why? As all Microsoft cloud services are connected to Azure AD for authentication, users will not be able to sign in to their account or access their resources if Azure AD is unavailable. That's because all control plane data lives in the cloud.

In other words, if the control plane fails, the data plane does not know what to do or who to give access to the network.



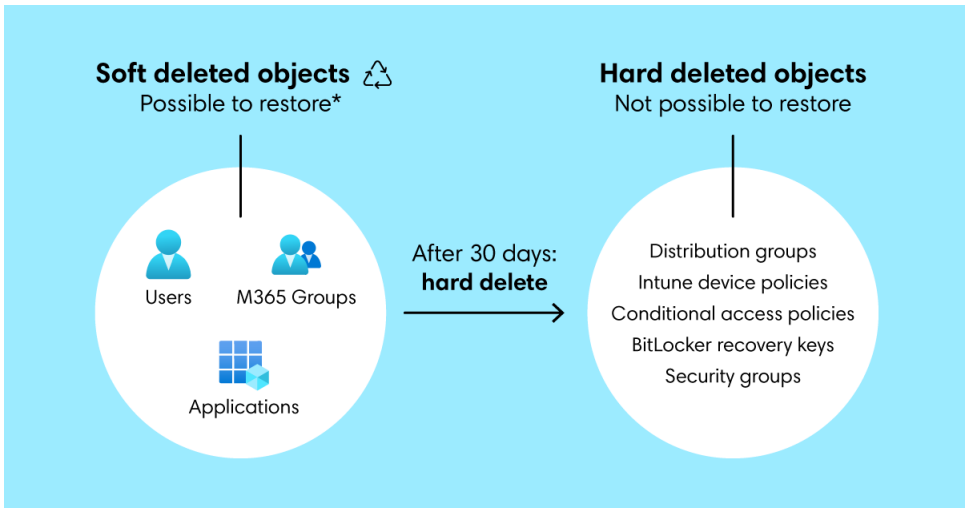
In those situations, Microsoft does offer some options for backing up and recovering data natively. However, recoverability is a shared responsibility between Microsoft and your organization. That's why it's important to understand exactly what objects you are responsible for protecting—and verify whether the Recycle Bin can sufficiently cover your needs:

	Customer	Microsoft
Preparation	Business continuity and disaster planning	Identity and access management functionality
	Documentation of known good states	Tools for documentation
	Monitoring and data retention	Log availability and consistency
	Operational security	Platform security
Recovery	Restoring soft-deleted resources	Availability of soft-deleted resources (time-limited)
	Restoring prior configurations	Availability of APIs

As Microsoft's shared responsibility table above shows, you are responsible for restoring soft-deleted resources as well as restoring prior configurations. So how do you verify if you have sufficient recovery capabilities? Let's look at what's covered by the Azure AD Recycle Bin.

What can and can't be recovered with Microsoft's native recovery features?

When talking about the native recovery provided by Microsoft, it's important to note that not all objects go through the Recycle Bin when they are deleted.



Some objects are “soft deleted” and get put into the Recycle Bin. They include:

- Microsoft 365 groups
- Azure AD applications
- User and guest accounts

It is also worth noting that soft deleted objects only stay in the Recycle Bin for 30 days. After that, they are permanently and irreversibly deleted and cannot be recovered.

All other objects are “hard deleted”, which means they never go to the Recycle Bin and thus can't be recovered natively. Microsoft shares that “hard-deleted items must be re-created and reconfigured. It is best to avoid unwanted hard deletions”. Immediately hard deleted objects include:

- Distribution groups
- Enterprise applications / Service principals
- Intune device policies
- Conditional access policies
- BitLocker recovery keys
- Security groups

Furthermore, many Azure AD objects have complex configurations or specific interactions with other systems that aren’t captured by the Recycle Bin. That means they can’t be recovered if deleted or changed.

Lastly, the Recycle Bin is for deleted objects only. If changes are made to an object, the Recycle Bin cannot recover the object to its previous state.

Why Azure AD needs to be part of your backup and recovery strategy for Microsoft 365?

Let us consider a couple of examples of how relying on just the Azure AD Recycle Bin in combination with your on-prem solution can cause significant problems for your users and your ability to resume business functions in a timely manner.

Conditional Access (CA) policies

Conditional Access policies help organizations provide additional control over access to their cloud applications and network by enforcing restrictions or requiring MFA under certain conditions. Common CA policy use cases include:

- Restricting unapproved devices from accessing resources
- Prohibiting users from accessing resources from untrustworthy networks (public Wi-Fi)
- Improving the user experience by reducing friction in secure environments (home Wi-Fi)
- Streamlining the experience for specific users and groups (i.e., executives require access via their phone)

If you are using CA policies to ensure only verified users outside the corporate network can access an application (or to block access entirely from certain IP addresses), then you might want to consider additional backup.

Why? The Recycle Bin offers no help, as it doesn't store improper modifications to objects—the Recycle Bin is for deleted objects only. In that case, if a CA policy has been changed, you're out of luck without a separate third-party backup. Trying to restore a CA policy manually requires complete and current documentation of all your Azure AD objects, which is practically impossible to maintain manually.

If a CA policy is accidentally or maliciously deleted, there is no retention in the Recycle Bin, as they are immediately hard deleted and gone.

A deleted or changed CA policy leaves admins with two significant problems:

- Users can't get into the app to do their work: A deleted, or faulty CA policy can lock out all users from an app. Want to know how that happens? Here's a real-life example how a faulty CA policy locked out all admins of all their Microsoft services—without the ability to register a support ticket for the issue, as they were unable to log into the Microsoft portal, where tickets are raised.
- Users can do things they shouldn't be able to do:
  Say you are using a CA policy to block access from certain IP addresses. Losing that type of policy exposes the associated application, as users that were previously blocked due to their IP addresses, now can gain access and do things they shouldn't be able to do.

Losing one policy is inconvenient but might not be a big deal. However, losing multiple CA policies can have disastrous consequences for your Microsoft 365 applications, your users, and business continuity. Most companies have many policies in place and continue to add user, geo, or function specific policies over time. The more policies you have, the more complex it becomes if you need to manually recover them.

Intune device compliance and configuration policies

Intune device compliance policies and configuration profiles help companies protect their organizational data by requiring users and devices to meet certain requirements. Let's look at each in isolation:

1) Intune device compliance policies

Intune device compliance policies are a set of custom rules that are set by the organization to make sure that users do not connect risky or unsafe devices to the network. Organizations can define what 'being compliant' means to their business and set up policies to verify whether a device is compliant. Examples of rules include requiring devices run a minimum OS version, not using a jail-broken device, requiring devices to have encryption activated, or requiring a certain password complexity, and a whole bunch of other rules.

Common device compliance policy use cases include:

- Restricting unapproved devices from accessing resources by applying certain actions to devices that don't meet your compliances rules i.e. an action could include being remotely locked or sending a device user an email about the device status, so they can fix the issue.
- Ensure compliance reporting by deploying device compliance policies to users in user groups and devices in device groups.
- If your organization uses Conditional Access, your CA policies can use your device compliance results to block access to data from non-compliant devices.

In short, if a device is non-compliant with a compliance policy, Conditional Access policy will block the user's access to Microsoft 365 if using this non-compliant device.

Device compliance policies depend on the platform type you select when creating a policy, as different platforms support different settings. Each platform requires a separate policy. That's why most companies would have quite a lot of different compliance policies set up.

2) Intune device configuration profiles

While Intune device compliance policies are merely checking whether a device is compliant with the policy, Intune device configurations profiles enforce a set of standards onto devices. IT admins use it to maintain granular control over device settings by enforcing a set of standard policies onto devices. That way all devices meet a certain level of security before being allowed to enter the network.

Some common Intune device configuration profile examples include:

- Allowing or preventing access to Bluetooth on the device
- Creating a WiFi or VPN profile that gives different devices access to your corporate network
- Managing software updates, including when they are installed
- Running an Android device as dedicated kiosk device that can run one app, or run many apps

These settings are added to "configuration profiles" in the Azure Portal and Intune is used to assign the profile to the devices.

There are many different configuration profiles available in Intune. To manage all settings, companies often need to make use of many different configuration profiles or use custom profiles to maintain granular control over device settings. As a result, organizations have many different configuration profiles in place.

If you're using Intune device compliance policies and/or configuration profiles to ensure only 'good and secure' devices can access your network, you might want to consider additional backup.
The reason: There is no retention for Intune device compliance policies or configuration profiles in the Azure AD Recycle Bin, as they are immediately sent to hard deletion. Additionally, if you accidentally make a change to an Intune device compliance policy or configuration profile object, you won't be able to get it back with the native recovery features in Azure AD, as the Recycle Bin doesn't store modified objects.

A deleted or changed Intune device compliance policy or configuration profile leaves admins with serious problems: If a device compliance policy or configuration profile changes (accidentally or on purpose), the network might be exposed, and admins would want to put the policy back immediately to close the security gap

Losing a single device policy or profile is unfavorable but doesn't have to be disastrous. But losing access to many device policies and profiles at the same time can have fatal consequences for your Microsoft

365 data as well as the ability to continue business as usual. Without backup, it will be time-consuming to identify and rebuild lost device compliance and configuration policies.

Protecting BitLocker recovery keys

BitLocker is a security feature used by organizations to mitigate unauthorized data access to lost or stolen computers by encrypting all files on a device.

BitLocker forces encryption on the whole disc drive on a computer. When it is turned on, it encrypts every bit of the computer drive. The security key used to encrypt the computer is very long (unique 48-digit numerical password), making it impossible to crack with brute force.

If a BitLocker password is lost, you cannot decrypt the disc drive on the device. So, what do you do? When BitLocker generated its encryption key, it also stored an additional key in Azure AD called a *protector*. The machine can be unlocked by putting the protector into the BitLocker boot console.

Some examples of cases that would require using the BitLocker protection key:

- **Forget to decrypt device:** An employee leaves the organization and hands in their device. If this device has BitLocker turned on, the next new hire who gets the device cannot get into the machine. In that case, the IT Admin would have to find the BitLocker protector in Azure AD for that device to unlock it.
- **Lost password:** If an employee loses their BitLocker password, the machine is now turned into lawn furniture. There is no way to unlock the device, unless you can retrieve the BitLocker protector in Azure AD. Without the protector, the IT Admin will have to wipe the device and start over, which is unfortunate if the device holds valuable data.
- **Malicious insider attack:** A disgruntled employee starts a malicious attack from his BitLocker encrypted device before leaving the organization. In this case, if the IT Admin does not have the BitLocker protector to unlock the machine, it will be impossible to access the device to make a forensic analysis and better understand the attack (and remediate it).
- **Modified BitLocker protector:** An IT Admin (accidentally or maliciously) modifies a Bitlocker protector from ‘12345’ to ‘789123’. Now, no one is able to unlock the device, as Azure AD holds the wrong protector.

As with CA policies and Intune device compliance policies, and device configuration profiles, there is no retention for BitLocker protectors in the Azure AD Recycle Bin. They are hard-deleted and cannot be recovered without third-party backup. Modifications are also not covered by the Recycle Bin, so if a BitLocker protector is changed, there is no way to get it back natively.

The value of protecting the BitLocker protector in Azure AD is that the organization can always access the protector—and even go back in the history of the protector to make sure they have access to the right protector to unlock the device.

An encrypted BitLocker device can cause a lot of pain, so it is worth protecting. Without backup, it can take up to 4 hours just to reset one device—and days to reset all devices in an organization after an attack. A reset like this could include creating a new Azure AD environment and potentially rescripting everything. Now try to imagine translating this kind of downtime to hundreds or thousands of devices across an organization. Not fun.

Protecting Enterprise Applications / Service Principals

Applications and service principals define how non-Microsoft 365 applications interact with Azure AD. Companies use them to grant external applications access to Azure AD and to provide single sign-on (SSO) authentication with multiple applications.

Relationship between app registrations and enterprise apps

When registering an application with Azure AD, you're creating an identity configuration for your application that allows it to integrate with Azure AD. When an application is registered, it will automatically create an application object **and** a service principal in your home tenant.

The application object describes three aspects of an application:

- How the service can issue tokens in order to access the application
- The resources that the application might need to access
- The actions that the application can take

The service principal object defines:

- What the application can do in the specific tenant
- Who can access the application
- What resources the application can access

Simply put, the application describes whether the application exists and how to talk to it, while the service principal explains who is allowed to access and manage the app.

Applications and service principals are one of the things that can be a little confusing. Part of that is because of the different terminology used. While the technical terms are *applications* and *service principals,* the Azure AD portal uses the terms *app registrations* and *enterprise applications.* Confusing, right? Let's demystify the terminology:

- Service principals are an instance of an application—a specific aspect of an application in your tenant. In the Azure AD portal, service principals are defined as *enterprise applications*. In short, they are the same thing, but have different names.

- Most companies will have a long list of service principals in the Azure AD portal. Each of these service principals has its own object ID that refers back to an application ID. The application ID refers to the application's home tenant (the tenant where it was registered). The application is seen as the template the service principal is generated from. That is because the application defines a lot of the pieces of a service principal. In the Azure AD portal, those applications are defined as *app registrations.*

One important thing to keep in mind is that applications can either be specifically defined to your tenant, or they can be defined in someone else's tenant. That impacts the way the application is configured in Azure AD.

What do service principals do and why are they important?

Service principals do various different things. One very common use case is to publish SSO on non-Microsoft applications into the Azure portal. For simplicity, let's make it tangible and look at a real life example using an app most of us know—the Salesforce application.

Many organizations use Salesforce to manage their sales pipeline. The Salesforce application is often used primarily by the sales division. Thus, the data that lives in there is invaluable for the sales team to

do their jobs. If they cannot access Salesforce, then their work comes to a complete halt. Morale of the story: It is important to protect Salesforce from unauthorized access.

Salesforce is an application that needs to be defined specifically for your tenant. This is where service principals come in handy, because they can be used to provision the Salesforce application with SSO. Once SSO method is configured, the service principal also define what groups and users can access the Salesforce application. Additionally, the same service pricincipal might also have conditional access policies associated, which means that users will be required to have multifactor authentication enabled to be able to access Salesforce.

What happens if a service principal is changed or goes missing?
Any changes that you make to your application object are also reflected in its service principal object in the application's home tenant only (the tenant where it was registered). This means that deleting an application object will also delete its home tenant service principal object.

However, restoring that application object through the app registrations UI in the Azure AD portal will not restore its corresponding service principal. In that situation, the app registration says "use service principal 0x12345 to log in", but if that service principal no longer exist the application cannot log in—and users will not be able to access the app to get their work done.

As service principals can be used for a lot of Azure objects besides just applications, admins need to be able to quickly put service principals back, because they may have granted specific permissions to that application to read or write certain data or to go to certain parts of the network.

Microsoft offers 30 days retention for app registration objects, but if a service principal is changed or deleted the Azure AD Recycle Bin does not offer any help, as service principals are immediately hard deleted.

Without third-party backup, restoring service principals and their associated permissions can be complex, time-consuming, and close to impossible to restore manually.

Recovering Azure AD and avoiding disruption to business continuity

Knowing that some cloud objects in Azure AD are unrecoverable if changed or deleted, let’s look at what you can do to protect Azure AD from losing data.

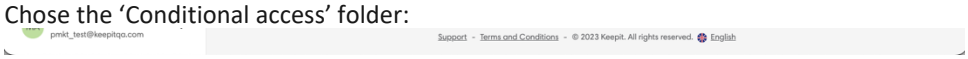
Recovering Conditional Access policies

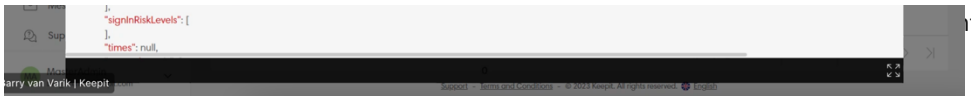
If you didn’t plan for it, you will need to trawl through the audit logs and recreate each CA policy by hand, which is both extremely time-consuming and potentially very costly—especially if you have many CA policies in your tenant. What if you can’t recreate the policies? Or what if it takes too long to get the data back to a previous state? What’s the cost of users not being able to access their data, and how long can you afford to be down?

This is where Keepit comes in handy. We back up your Azure AD CA policies and restore deleted objects or changed attributes instantly with just a single click.

Simply go to your Azure AD backup and click on ‘Policies’:

Chose the ‘Conditional access’ folder:





t of the CA

From this view, you can see the current CA policy. If you want to compare it to a previous point in time, you can download a JSON file to identify when and how the CA policy changed.

Once you have identified the file and version you wish to restore, click the 'Restore' button:

Your CA policy will be restored back into your Azure AD portal instantly, so you can get back on track fast. That's how easy it is to get your CA policies back.

Recovering Intune device compliance policies and configuration profiles

What are your options if you can't restore compliance policies and configuration profiles using the Azure AD Recycle Bin? What's the consequence of users being locked out of their critical business apps? And what is the cost of letting unauthorized users into your network? How long can your business afford to be down?

Keepit's Azure AD backup and recovery gives you the confidence you need to be able to instantly get your policies and profiles back.

To recover your policies, go to your Azure AD backup and click on 'Policies':

From here you chose whether you are looking to restore a Compliance policy or a Configuration profile. Select the folder that is relevant to your use case:

he content:

This view allows you to see the details of the most recent compliance policy or configuration profile. You can use the 'versions' feature to go back in time to see what the details of the objects looked like. If you wish to compare your data side by side, you can easily download a JSON file to help identify when something changed and what was modified.

After identifying the object and version you wish to restore from, click the 'Restore' button:

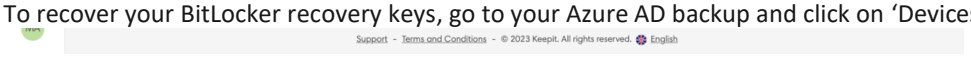
Your compliance policy or configuration profile will be restored back into your Azure AD portal instantly. And that's how easy it is to get your device policies and profiles back.

Recovering BitLocker recovery keys

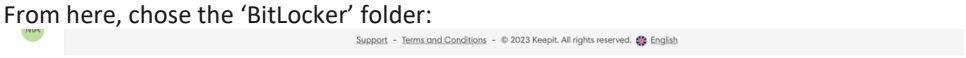
An encrypted BitLocker device can cause a lot of pain—especially when you can't recover the BitLocker recovery key through the Azure AD Recycle Bin. Without proper backup and recovery capabilities, it can easily take up to 4 hours just to reset one device—and days to reset all devices in an organization after an attack.

With Keepit you can avoid putting your organization in that situation. In a few simple steps, you can retrieve the right BitLocker recovery keys to unlock the device and save yourself a lot of time and resources.

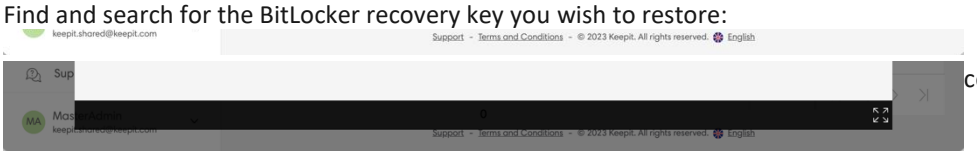
To recover your BitLocker recovery keys, go to your Azure AD backup and click on ‘Devices’:



From here, chose the ‘BitLocker’ folder:



Find and search for the BitLocker recovery key you wish to restore:

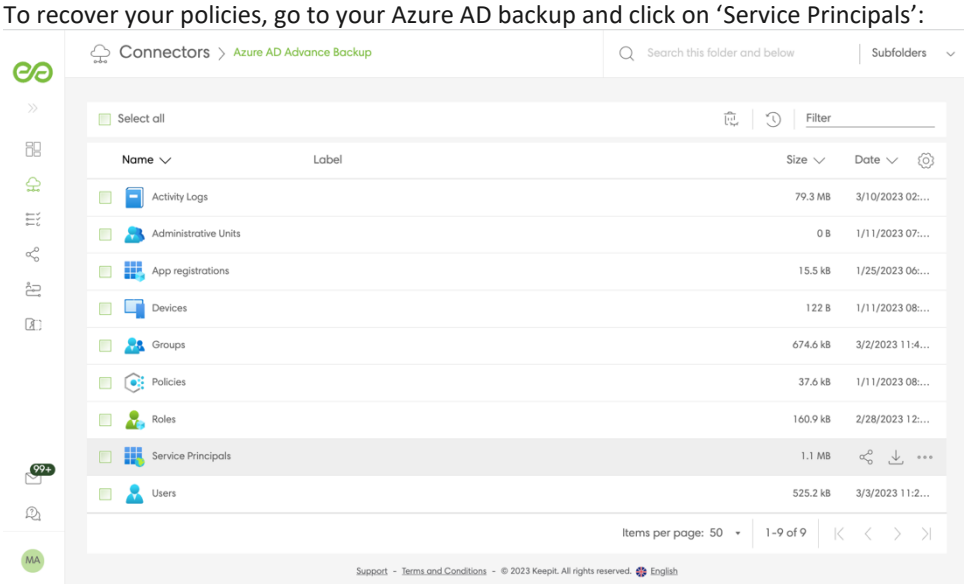


covery key. You can also use the ‘versions’ feature to go back in time to a previous backup to access previous versions of the BitLocker recovery key. That way you will always have instant access to the BitLocker recovery keys when needed.

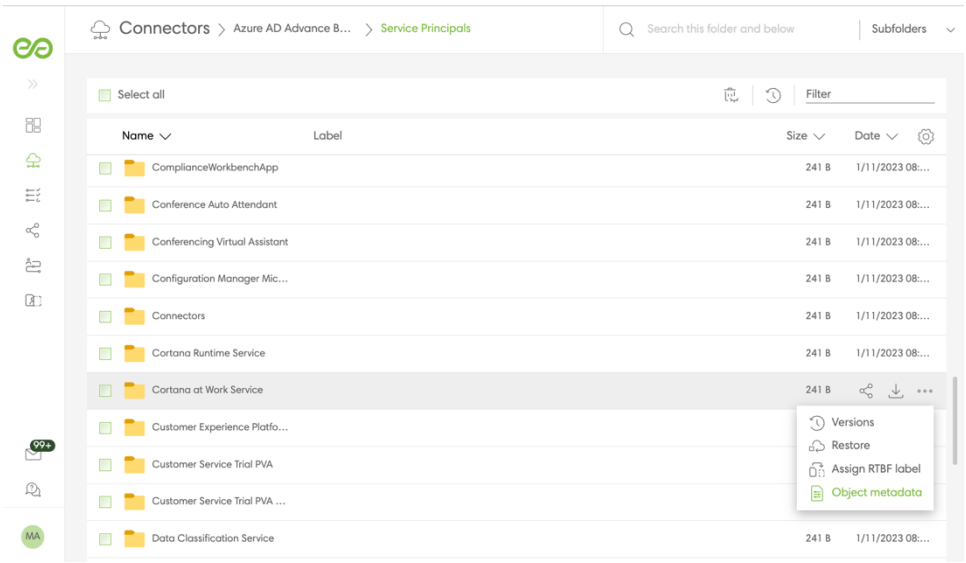
Recovering service principals

You made a change that deleted an application object and now the service principal object in the home tenant is gone. Users can’t log in to the app to do their job. What do you do? How are you going to restore a service principal fast? The Azure AD Recycle Bin doens’t offer any help as service principals are hard deleted. With Keepit, you can get your service principals back in an instant.

To recover your policies, go to your Azure AD backup and click on ‘Service Principals’:

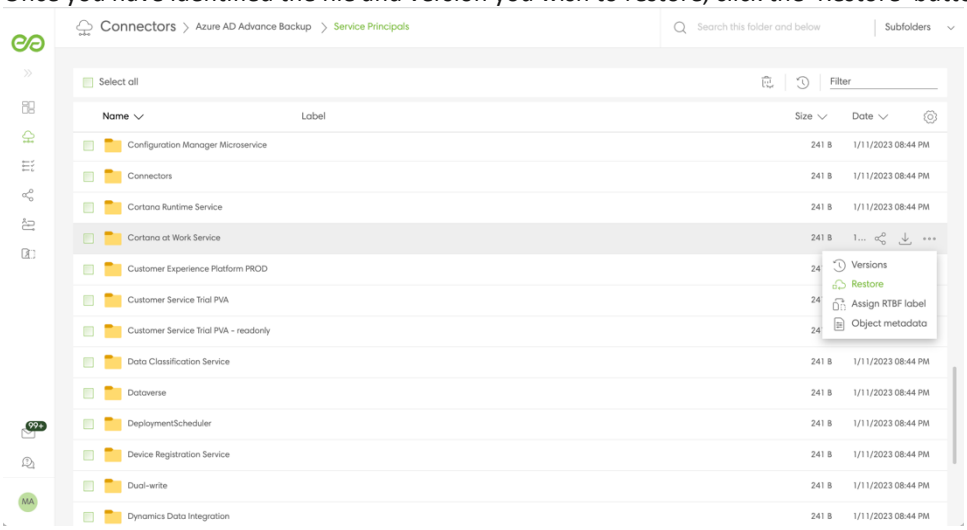


Find and search for the service principal you wish to recover. To see the object metadata, simply click on the ‘...’ symbol and choose ‘object metadata’ to preview the content:



To identity what changed, you can use the 'Difference' feature that helps compare object metadata across backup versions:

Once you have identified the file and version you wish to restore, click the 'Restore' button:



Your service principal will now be restored instantly and will sync with your Azure AD tenant.

Summing it all up

Azure AD is the authentication and authorization system for Microsoft 365. In other words, Azure AD is like a brain that controls the rest of the entire body. If the brain does not work, the body stops working too.

Protecting Azure AD and Microsoft 365 are not separate problems. Thinking about them as separate problems is like wearing half a helmet to protect your head. Both the brain and the body need protection to ensure the entire Microsoft tenant is fully safeguarded.

Microsoft offers several strategies for backing up and recovering data that might be changed or lost, however, as we learned in this paper, not all cloud critical cloud objects are covered by the Azure AD

Recycle Bin. That's why you should consider getting Keepit's free Azure AD protection to protect the core of your business.

Keepit also offers advanced coverage for Azure AD with all the comprehensive recovery capabilities you need to ensure productivity and business continuity.