

Features and customer value



Why protect Azure AD?



- Disaster recovery protection
 - Protect Users and Groups
 - Protect business-critical identity and application objects
 - Recover objects that Microsoft doesn't protect
 - Extended retention period
- Improve security
 - Protect policies (incl. Conditional Access), not just data
 - Full auditing and traceability of changes to access and device management policies
- Protect against day-to-day data loss
 - Rapid recovery of “oops” deletions or changes
- Improve IT efficiency
 - Selectively roll back changes
 - Speed up troubleshooting by allowing quick last-known-good restore



Microsoft's native recovery features—and its limitations

Microsoft has invested quite a bit of money in providing recovery (versioning, recycle bin, and preservation features), but one area where the native protection tools are weak is in the directory.

If your Azure AD account is deleted, you can recover it for 30 days—but can you really trust the native recovery features? What if an admin receives a request to restore Azure AD cloud objects on day 31?

And what about being able to roll back to a previous good state if everything has gone south?

Microsoft recycle bins are not alternatives to a backup, and were never intended to be an enterprise-level recovery solution.

What can/can't be recovered from the Recycle Bin

Not all objects go through the Recycle Bin when they are deleted.

Certain types of objects are “soft deleted,” which means they are put into the Recycle Bin, while other objects are “hard deleted”—they are not put into the Recycle Bin and therefore cannot be recovered.

Azure AD objects that are soft deleted include:

- [Users: 30 days retention period](#)
- [Groups: 30 days retention period](#)
- [Audit logs: 90 days retention period](#)
- [Sign-in logs: 90 days retention period](#)

Azure AD objects that are immediately hard deleted include:

- [Security groups](#)
- [Distribution groups](#)
- [Enterprise Apps/Service principals](#)
- [Conditional Access policies](#)
- [Device policies](#)

Many Azure AD objects have complex configurations or specific interactions with other systems. Those details are not captured by the Recycle Bin and cannot be restored from it.

Finally, the Recycle Bin is for deleted objects only. If an object has been changed rather than deleted, the Recycle Bin cannot help you restore the object to its previous state.



Conditional access policies

What's the customer value?

Feature

What's conditional access policies in Microsoft?
CA policies are if-then statements used to apply the right access controls when needed to keep the organization secure.

Example: If a payroll manager wants to access the payroll application, **then** it's required to do multi-factor authentication to access it.



What's conditional access policies in Keepit?
Keepit backs up all conditional access policies in the Azure AD tenant.

Advantage

CA policies backup and restore in Keepit
Keepit allows IT admins to make clear decisions on how they want to backup and restore CA policies:

- *select whether they want to backup CA policies*
- *back up all CA policies in the tenant*
- *selectively choose what CA policies to restore*
- *preview selected policies in a JSON format*
- *restore selected CA policies in-place*

Benefit

Control access to your environment
Backup is relevant for organizations that manages large numbers of CA policies. Admins face two significant problems when CA policies are not working:

- Users can't get into important applications to do their work
- Users can do things they shouldn't be able to do if a CA policy was deleted

There is no retention in the Azure portal if CA policies are deleted—they are immediately hard deleted and gone.

Admins want to be able to recover CA policies from the time they worked to avoid situations where users can't access apps or where users can do things they aren't supposed to.



App registrations

What's the customer value?

Feature

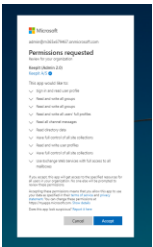
Advantage

Benefit

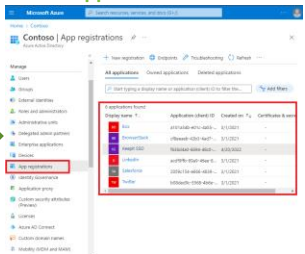
What is an app registration in Microsoft?

App registration is an identity configuration for an application that allows it to integrate with Azure AD (application object).

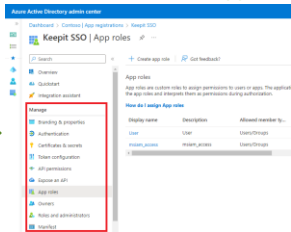
Register app in AAD



App registration of app created in AAD



Unique information about access to app



What is app registration in Keepit?

Keepit backs up application objects that have been registered in Azure AD.

App registration backup and restore in Keepit

Keepit's Azure AD backup allows IT admins to make clear decisions on how they want to backup and restore app registrations:

- select whether they want to backup app registrations
- backup all app registrations in the tenant
- decide whether to restore individual or all app registrations
- preview selected service principal in the object metadata previewer (the app name, application ID, object ID, and homepage URL)
- restore app registration in-place


Access important apps when needed

If an app registration is deleted (accidentally or on purpose) from Azure AD, employees can't use the application—that's annoying as they can't access important apps and work will not be done. Until the app registration has been recovered, no one can communicate with the app.

With Keepit, admins can roll back to a previous snapshot and restore the app registration back in place, so employees can quickly regain access to important apps.

Example:

If Paul Robichaux removes the Keepit app registration in our Azure AD, no one in Keepit would be able to access the Keepit platform—and that would mean trouble for sales!



Service principals / Enterprise apps

What's the customer value?

Feature

What's a service principal in Microsoft?

When an app registration is created, a corresponding service principal is created in the Azure AD tenant. Simply put, the app registration describes whether the app exists and how to talk to it, while the service principal explains who is allowed to access and manage the app:



What's a service principal in Keepit?

Keepit backs up service principals registered in the Azure AD tenant along with its assigned permissions

Advantage

Service principals backup and restore in Keepit

Keepit allows IT admins to make clear decisions on how they want to backup and restore service principals:

- select whether they want to backup service principals
- backup all service principals in the tenant
- decide whether to restore individual or all service principals
- preview selected service principal in the object metadata previewer (service principal name, service principal ID, and object ID)
- restore service principals in-place

Benefit

Bring back permissions seamlessly

If a service principal is deleted, the app registration will still be there, but all the access policies and permissions for the application will be gone.

Service principals can be used for a lot of Azure objects besides just applications. Multiple permissions might be tied to a single service principal—e.g. application X is allowed to trigger a runbook in Azure automation, create a new Azure VM, etc.

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. Without backup, these permissions can be complex and time-consuming to restore manually.



Intune device compliance policies

What's the customer value?

Feature

What's Intune device compliance in Microsoft?

Intune device compliance policies are a set of custom rules that are set by the organization to make sure that users don't connect risky or unsafe devices to the network—only compliant devices are allowed in.

Organizations can define what 'being compliant' means to their business and set up policies to verify whether a device is compliant.



What's Intune device compliance in Keepit?

Keepit helps organizations backup and recover their Intune device compliance policies in Azure AD

Advantage

Device compliance backup and restore in Keepit

Keepit allows IT admins to make clear decisions on how they want to backup and restore Intune device compliance policies:

- *select whether or not they want to back up Intune compliance policies*
- *backup all device compliance policies in the tenant*
- *selectively choose what device compliance policies to restore*
- *preview selected policies in a JSON format*
- *the policy will be restored as a complete unit*

Benefit

Keep your network safe

Intune device compliance policies are playing an important part in keeping insecure and unsafe stuff like malware out of your network.

If a device compliance policy 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.

Without backup, it will be time-consuming to identify and rebuild deleted/lost device compliance policies



Intune device configuration profiles

What's the customer value?

Feature

What's Intune device configuration in Microsoft?

With Intune device configurations, IT admins can enforce a set of standard policies onto devices to ensure all devices meet a certain level of security before being allowed to enter the network.



Example: For every Windows device that belongs to a user in the Sales AD group, we enforce them to have an 8-digit PIN and encryption turned on. If they change it, we will automatically change it back.

What's Intune device configuration in Keepit?

Keepit helps organizations backup and recover their Intune device configuration policies in Azure AD.

Advantage

Device configuration backup and recovery in Keepit

Keepit allows IT admins to make clear decisions on how they want to backup and restore Intune device configuration policies:

- *select whether or not they want to back up Intune device configuration profiles*
- *backup all device configuration profiles in the tenant*
- *selectively choose what device configuration profiles to restore*
- *preview selected profiles in a JSON format*
- *restore selected device configuration profiles in-place*

Benefit

Enforce your security boundaries

Intune device configuration profiles are put in place by IT admins to automatically enforce certain configurations of devices.

The profiles are how admins define and enforce the organization's security boundary.

If a device configuration profile has been changed or deleted, admins want to be able to see exactly what changed, so they can restore the profile back to a point-in-time where everything was working.

Without a backup, admins risk having gaps in their security posture, which could let bad stuff into the network



Bitlocker recovery keys

What's the customer value?

Feature

What's Bitlocker recovery key in Microsoft?

Bitlocker is a security feature used to protect data on a device. Bitlocker forces encryption on the whole disc drive on a computer. When it's turned on it encrypts every bit of the computer drive.

The security key used to encrypt the computer is very long, making it impossible to crack. When Bitlocker generates its encryption key, it can store an additional key in Azure AD called a *protector*. If a Bitlocker password is lost, the machine can be unlocked with the protector.

What's Bitlocker recovery key in Keepit?

Keepit backs up and shows the Bitlocker recovery keys stored as attributes of device accounts in Azure AD

Advantage

Bitlocker recovery key backup and recovery in Keepit

Keepit allows IT admins to make clear decisions on how they want to backup and restore Bitlocker recovery keys:

- *select whether or not they want to back up Bitlocker recovery keys*
- *backup for all devices in the connector scope*
- *selectively choose what devices to restore Bitlocker recovery keys for*
- *preview selected devices*

Benefit

Instant access to the right Bitlocker protector

Losing access to Bitlocker recovery keys causes problems if you want to unlock an encrypted computer. Without the right key, the computer device is locked, and the only option is to wipe it and start over.

That's problematic if the computer holds valuable data. It's even worse if an insider started an attack from the device and then left the company. Now, the admin can't do forensic analysis on the machine to determine how to remediate the attack.

Keepit gives admins a way to go back and look at the history of the Bitlocker protector and get access to the right protector to unlock an encrypted computer drive.