How We Handle Your Data

Data handling document regarding usage of Admin By Request

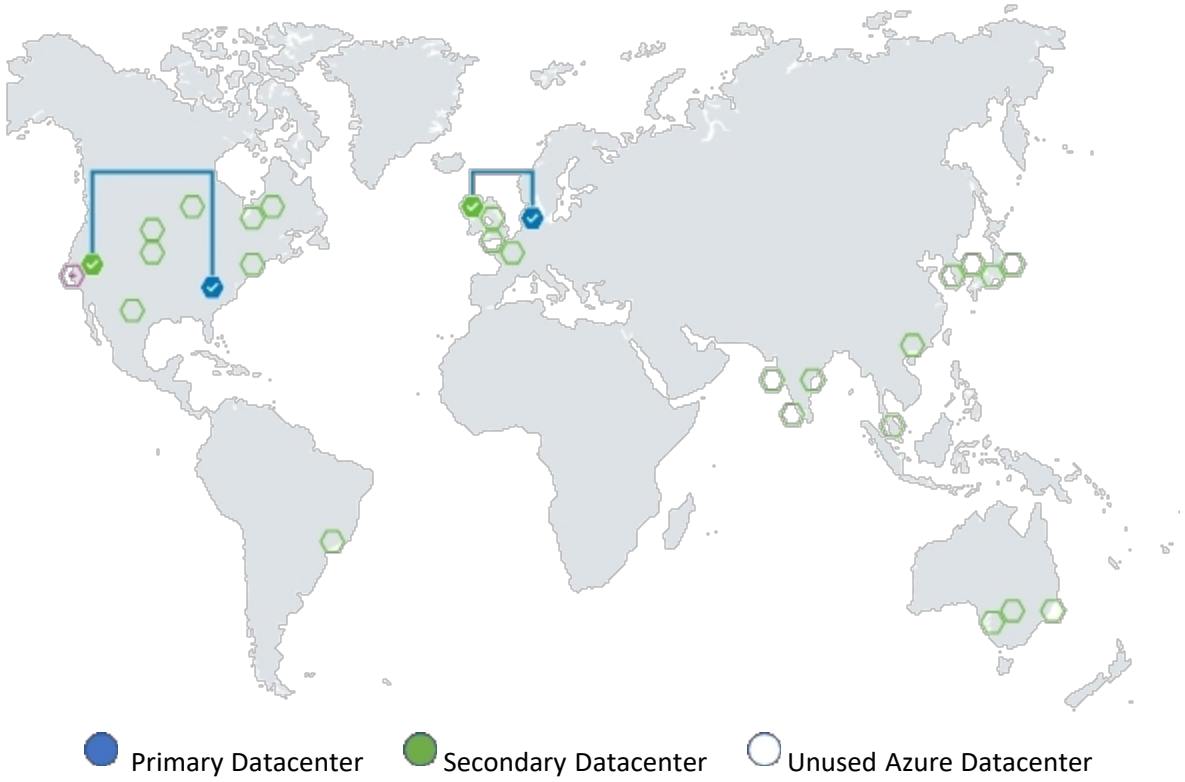
Version	1.3
Date of Version	20/03/2024
Created By	Jakob Bjørn Sørensen
Approved By	Lars Sneftrup Pedersen
Confidentiality Level	PUBLIC

Table of Contents

Data Storage

Where do we store your data?

We use Microsoft Azure SQL to store your data in two regions - USA and Europe. We use two locations in each region using SQL replication to make sure your service stays up and running in case of Microsoft Azure outages. If you are based anywhere outside Europe, your data is stored in the USA in the states of Virginia and Washington. If you are based in Europe, your data is stored in the Netherlands and Ireland. All our web servers are located in the same four locations for optimal performance for you. None of your data exists outside of these designated regions.



Can you choose where we store your data?

Yes. If you want us to store your data in the opposite region to where you are based, please let us know by the time you license.

How do we back up your data?

Data is real-time geo replicated between the two locations in your region to ensure backup, fail-over and disaster recovery. Microsoft backs up Azure SQL and guarantees an Azure SQL restore is possible from any minute of the day, within the last 30 days. We also do cold storage backup in case of a complete, irrecoverable Microsoft Azure failure on both locations in a region.

How long do we keep your data?

We keep your auditlog data for 12 months by default. You can change the data retention period in your settings from a minimum of 3 months to a maximum of 5 years.

Service Level Agreement

The service level agreement for Azure SQL is 99.99%. In case of a failure, geo replication will automatically fail-over to the secondary location.

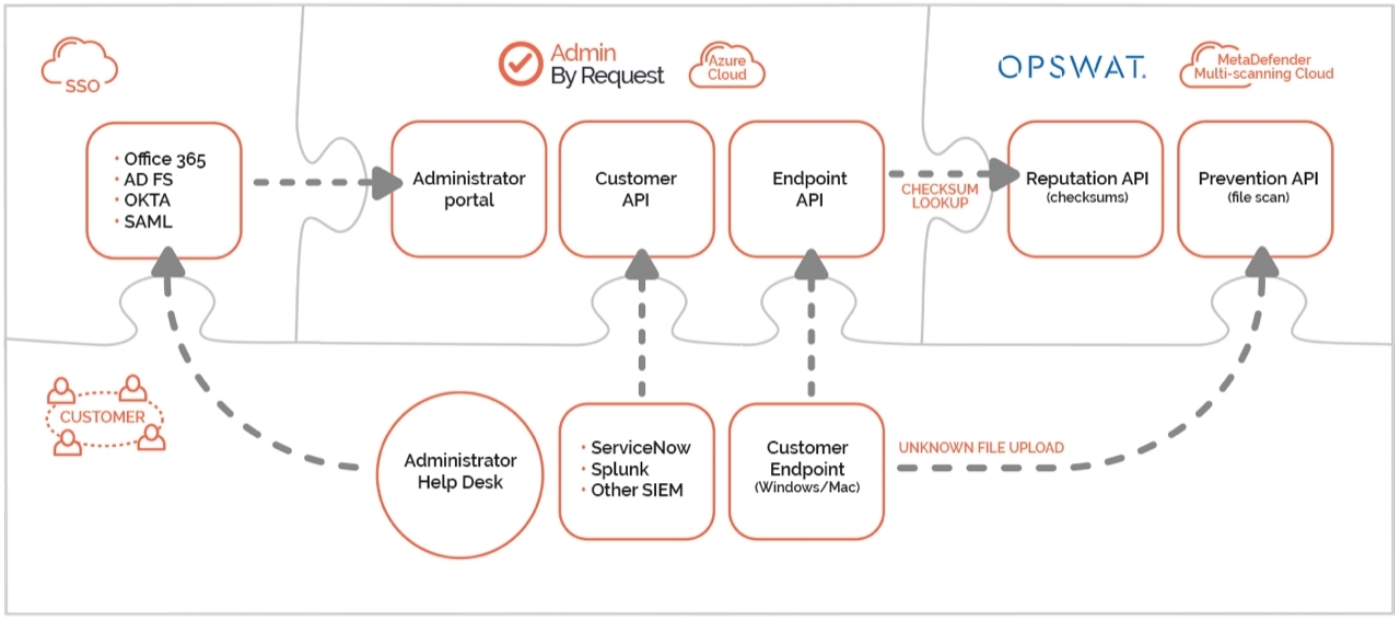
Service Level Agreement for Microsoft Azure SQL

Data Collection

What data flow in the system?

The following communications take place:

- The client software communicates with the cloud service
- Administrators and help desk personnel access the portal through single sign-on
- OPTIONAL: Files and checksums are sent to OPSWAT MetaDefender for multi-engine malware scan (enabled by default)
- OPTIONAL: Customer API can be used to consume data from your own systems (disabled by default)



Encryption at rest

We use Azure SQL transparent data encryption for all data at rest to ensure no unauthorized access to data is possible.

Encryption in transit

The data communication between the client software and our servers uses TLS 1.2 encryption. The load balancer IP depends on your region:

- 137.117.73.20 (if your data is located in the USA)
- 104.45.17.196 (if your data is located in Europe)

Furthermore, the raw data is also encrypted using a 256-bit encryption to protect against Man-in-the-middle attacks by a person who has physical access to a client.

What data does the inventory collect?

The inventory collects:

- Basic hardware inventory data, such as computer model, cpu, ram and operating system
- IP address
- User and computer domain and OU names
- User's phone number and email address (see note below)
- List of local administrator account names
- List of computer and user groups (AD Domain or Azure AD)
- List of installed software

NOTE: In case of GDPR concerns, you have the ability to disable the collection of user name, account name, email address and phone number in the Settings menu after login. You can also disable the entire inventory if you prefer.

What data is extracted from domain controllers?

The client software collects this information from a domain controller for domain computers:

- User and computer OU names
- User's phone number and email address
- List of computer and user groups

The traffic is marginal and only refreshed every 4 hours. You can monitor the traffic on an endpoint by running the ADInsight SysInternals tool.

What session data do we collect?

When a user has completed an App Elevation or an Admin Session, the client collects: ·

Computer name

- Duration
- Installed and uninstalled software
- UAC elevated programs
- Reason for administrator need (if configured)
- User's account name and full name (if configured)

If the Reason screen is used, email address and phone number are also collected, as entered by the user in the pop-up window. You can disable collection of user name, email address and phone number in the Privacy menu in Settings in the portal.

What data does diagnostics collect?

In a support situation, one of our support engineers might ask the end user to invoke the About screen, click the Connectivity tab and ask the end user to click the "Submit diagnostics data" link. This will send trivial system data to us to understand the history of the endpoint software. If the end user clicks the link and confirms, the client submits:

- Current configuration state (downloaded settings)
- Data in queue to be uploaded

- When the endpoint software was installed or upgraded
- When the services of the endpoint software were started or stopped
- Events from the local event log related to Admin By Request

This data cannot be extracted by us without the user clicking the link and is kept for up to a week. Note that an end user cannot create a support ticket, only portal administrators can.

What data is cached on the client?

The client software for domain joined computers works exactly the same off of your LAN as it does on your LAN. This is possible because the clients cache an encrypted copy of domain groups' names and OU name of the computer and the logged-on user, to be able to determine sub settings both online and offline. If your computers are Azure AD joined, a similar group's cache is kept for performance reasons. If your computers are stand-alone, no data is cached.

Data Security

Who has access to the production environment?

Only the appointed Risk Owner and/or Asset Owner has access to the production environment (maximum 2 persons). Please refer to our GDPR Data Processing Agreement for more information.

How do we handle internal security?

We have strict security policies in place for all our employees. Please contact us to receive a copy of our internal Information Security Policy.

How can you be sure your updates are free of malware?

Because we use VirusTotal Monitor (VT monitor). VirusTotal (www.virustotal.com) is owned by Google and offers scanning of files from 70 AntiVirus vendors including CrowdStrike, Sophos, McAfee, MalwareBytes, BitDefender, Symantec, TrendMicro, Kasparsky, F-Secure, FireEye, Microsoft, Webroot, Avast, Fortinet and Acronis. Our files can simply not be deployed without passing the scan of all 70 engines.

When we release updates, the binary files are uploaded to our VT monitor account and we thereby have confirmation that the files are clean before we put them into production for you to download. Should any files be flagged as false positives by a vendor, this vendor is automatically notified and we will await resolution before releasing the code. Proactively, we also keep the last three releases in our VT monitor account. All files are then scanned every day by all 70 engines. We are notified, if any false positives arises and will make sure the vendor in question will whitelist the file in question.

More about VirusTotal monitor

Compliance

Terms & Conditions

Please review our Terms & Conditions for using Admin By Request. Terms & Conditions along with the GDPR Data Processing Agreement are the two agreements in effect between you and us for you to be able to use Admin By Request.

Admin By Request Terms & Conditions

GDPR

Admin By Request is a European company, and we must therefore abide to the EU General Data Protection Regulation - GDPR in short. To comply with Article 28 in the General Data Protection Regulation, any European company must provide a Data Processing Agreement (DPA) between themselves and any European customer. The agreement applies to all customers around the world, which means all customers reap the benefits of the GDPR requirements observed by us. The overall purpose of Article 28 to describe internal procedures relating to security, availability and privacy when managing customer data, with the main objective being customer transparency. Click the link to see the agreement.

Admin By Request Data Processing Agreement

ISO 27001

ISO/IEC 27001 is an information security standard - part of the ISO/IEC 27000 family of standards. It is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee. ISO/IEC 27001 specifies a management system that outlines requirements and is intended to bring information security under management control. Organizations that meet the requirements may be certified by an accredited certification body following successful completion of an audit. Admin By Request is ISO 27001 certified. The documentation can be found in the Trust Center. ISO 27001 (iso.org)

SOC 2

Service Organization Control 2, known as SOC 2, is developed by the American Institute of CPAs (AICPA) and defines the criteria for managing customer data based on five "trust service principles": Security, Availability, Processing integrity, Confidentiality & Privacy. SOC 2 and GDPR Data Processing Agreements are very similar and they both address the same procedures. The key difference is that a GDPR Data Processing Agreement is based on the right to audit by the customer, whereas SOC 2 is a certification by a trusted third party.
The SOC 2 Type 2 report issued for Admin By Request by the C3PAO, A-LIGN, can be downloaded in the Trust Center.

www.aicpa.org

Cyber Essentials

Cyber Essentials is the UK Government's answer to a safer internet space for organisations of all sizes, across all sectors. Developed and operated by the National Cyber Security Centre (NCSC), Cyber Essentials is considered the best first step to a more secure network, protecting you from 80% of the most basic cyber security breaches. Admin By Request is fully certified to UK Cyber Essentials. Please refer to the Trust Center for certificate of proof.

Cyber Essentials.

Tenancy

The service we provide to you uses a multitenancy model. Multitenancy is the norm for SaaS solutions and is the model used by all major SaaS solutions, such as SalesForce or Google Apps – and also your bank. Your bank does not have a separate system for you as a customer, instead your bank uses multitenancy, which means that a set of pooled computing resources is shared among multiple customers (tenants) using application level isolation. A tenant (e.g. your company as a customer in your bank) is a group of users who share a common access with specific privileges to the software instance. With a multitenant architecture, the software application is designed to provide every tenant a dedicated share of the instance - including its data, configuration, user management and individual functionality. Please refer to the Microsoft tenancy design pattern page below for more deeper explanation of SaaS and Multitenancy.

Multitenancy on Microsoft.com

Portal

Access

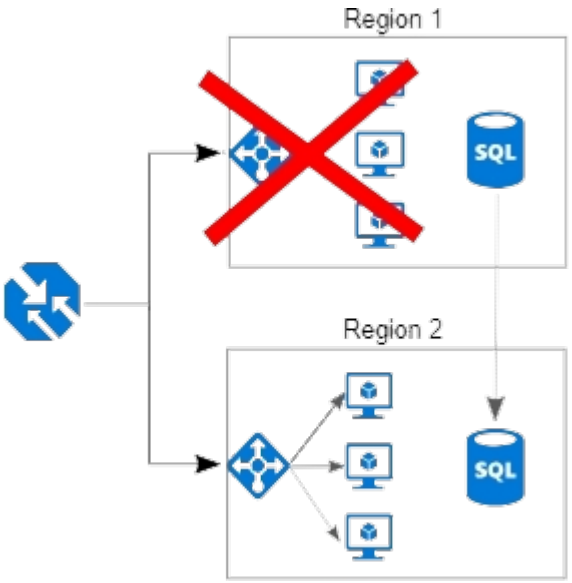
At the time of licensing, you will receive a main login. With this login, you can create multiple logins with limited access, such as access for an auditor or a manager. A login also grants rights to see the same data in the mobile app. For all users, you can enable two factor authentication and single sign-on. If you received an NFR license for a proof-of-concept project, and you later choose to license, this tenant instance will automatically roll on to become your commercially licensed tenant.

Single sign-on

We support single sign-on (SSO) for Office 365, Azure AD, ADFS, Okta and any SAML 2.0 identity provider. We recommend that you set up single sign-on because this ensures that you terminate access to the portal when employees leave the company. Refer to this page for technical setup of SSO.

Availability

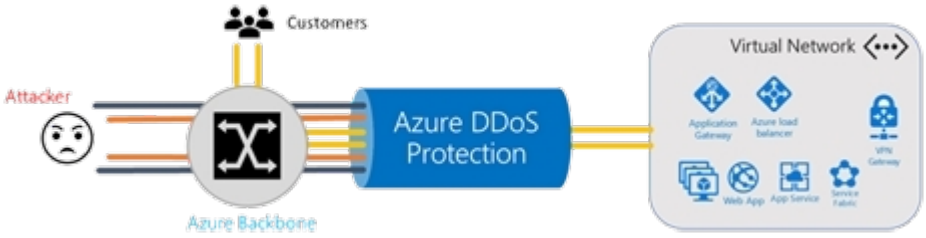
We use Azure web servers in multiple continents in order to make sure we provide great performance anywhere in the world and that the portal is always up and running.



Denial of Service Protection

The portal is protected from Distributed Denial of Service by Azure DDos protection. Refer to the document below for more information:

Azure DDos Standard overview



Service Level Agreement

Our web servers are located in the same Azure Availability Set in each continent. An Azure Availability Set is a guarantee that Microsoft will not take web servers down for maintenance at the same time. Microsoft guarantees a

99.95% up time in each continent in this set up:

Service Level Agreement for Microsoft Azure Virtual Machines