Microsoft

Power Platform and Dynamics 365 Apps

A Guide to Security and Compliance

Summary

The Microsoft Power Platform is a business application platform that helps support and extend Office 365, Dynamics 365 and Azure, as well as third-party services and applications.

Dynamics 365 is an online software service (SaaS, or Software as a Service) offering built as a Microsoft 1st-party application deployed to Power Platform utilizing Dataverse (formerly Common Data Service, CDS) to store data.

The Power Platform offers low-code automation and application development with Power Automate and Power Apps, business intelligence reporting with Power BI, and chatbot capabilities with Power Virtual Agents.

A Power Platform environment is a logical collection of optional components such as Dataverse, Power Automate (PA), Power Virtual Agent (PVA), and Connectors.

Dataverse is a heterogenous storage service that runs on Azure and is shared by Dynamics 365 Apps, Microsoft 365 and Power Platform with Common Data Model describing the entities and relationships.

Applies to: Dynamics 365 Apps and Power Platform environments

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Contents

Introduction

This document pulls together various information sources to provide an overview and underpinning details on aspects related to Compliance, Privacy, Security and Transparency.

It is worth noting that most complex implementations will use a mix of services from Microsoft. Dynamics 365, when subscribed to as Software as a Service (SaaS), has a well-defined security and compliance boundary. All aspects of the service that function within this boundary are governed by our compliance and security certifications, standards, and our Online Service Agreement with you.

For data flows extending outside the boundary to other Microsoft Services, customers' on-premises systems or other cloud services, you need to refer to the related documentation and contracts for those services.

You need to engage with all data flows leaving Dynamics 365 and Power Platform, and verify that your compliance, privacy, security and transparency requirements are met for the other services involved.

Microsoft offers an accelerator that can aid in analysis and automation of governance goals on the Power Platform, such as establishing Data Loss Prevention (DLP) policies. Refer to the Center of Excellence (CoE) Starter Kit documentation to understand the capabilities of this offering.

Compliance

Introduction

In a world where data breaches are daily occurrences and regulatory requirements for protecting data are increasing, it is essential for organizations to choose a cloud service provider which makes every effort to protect customer data. Microsoft is committed to the highest levels of trust, transparency, standards conformance, and regulatory compliance. Our broad suite of cloud products and services are all built from the ground up to address the most rigorous security and privacy demands of our customers.

Microsoft complies with data protection and privacy laws applicable to cloud services, and our compliance with world-class industry standards is verified by third parties.

Compliance

We will help you meet your specific compliance needs.

We offer a comprehensive framework to help you comply with your specific requirements. Microsoft Dynamics 365 meets many international and industry-specific compliance standards.

Microsoft cloud services have the largest compliance portfolio in the industry, including some of the most rigorous assessments in the world. These assessments range across global technical standards, industry-specific and region-specific requirements, and regulations.

A sample of Compliance and regulatory coverage:

Global

- ISO 27001
- ISO 27017
- ISO 27018
- SOC 1 Type 1
- SOC 1 (SSAE 18) Type 2
- SOC 2 Type 2
- PA-DSS
- CSA STAR Self-assessment

Government

- FedRAMP High
- FedRAMP Moderate
- ITAR
- DoD DISA SRG level 2
- CJIS (State criminal justice)
- NIST SP 800-171
- Section 508 VPATs
- FIPS 140-2
- CJIS
- IRS 1075

Regional

- Australia CCSL (IRAP)
- China GB GB18030
- China GBT 24589
- EU Model Clauses
- EU—US Privacy Shield
- GDPR
- New Zealand Gov CIO framework
- Singapore MTCS
- Spain ENS High
- Spain LOPD
- UK G- Cloud Framework

Industry

- HIPAA BAA (US)
- FDA CFR title 21 part 11
- FERPA
- FINMA (Switzerland, FSI)

Microsoft employs a risk-management model of shared responsibility with the customer:

Microsoft is responsible for the platform including services offered and seeks to provide a cloud service which can meet the security, privacy, and compliance needs of your organization. As a customer, you are responsible for management of the environment once the service has been provisioned. You must identify which controls apply to your business and understand how to implement and configure them to manage security and compliance with applicable regulatory requirements for your nation, region, and industry.

Audit Reports

To help your organization comply with national, regional, and industry-specific requirements governing the collection and use of customer data, Microsoft offers the most comprehensive set of compliance offerings of any cloud service provider.

Microsoft business cloud services operate with a cloud control framework, which aligns controls with multiple regulatory standards. We design and build our cloud services using a common set of controls, which streamlines compliance across a range of regulations not only for today, but for tomorrow as well. Then we engage independent auditors to perform in-depth audits of the implementation and effectiveness of these controls.

Learn how Microsoft cloud services have implemented security and privacy controls, and how third-party auditors have tested them:

SOC 1 Type 2 reports

- Azure + Dynamics 365 (Public & Government) SOC 1 Type 2 Report
- Microsoft 365 SOC 1 SSAE 16 Type II Audit Report

SOC 2 Type 2 reports

- Azure + Dynamics 365 (Public & Government) SOC 2 Type 2 Report
- Microsoft 365 SOC 2 AT 101 Type II Audit Report

ISO/IEC 27001 and ISO/IEC 27018 audit reports

- Microsoft Azure, Dynamics 365, and Other Online Services – ISO27001, 27018, 27701 Assessment Report
- Dynamics 365 (formerly Dynamics CRM) ISO 27001 Audit Assessment Report 2017
- Dynamics 365 ISO 27018 Audit Assessment Report
- Microsoft 365 – ISO 27001, ISO 27018, and ISO 27017 Audit Assessment Report

Security assessment reports

- Azure Security Assessment
- Dynamics 365 Security Assessment
- Microsoft 365 Security Assessment

Office 365 audit-related info

- Microsoft 365 Architecture and Audit Reports – Management Summary
- Microsoft 365 ISO 27001:2013 and ISO 27018:2014 Aligned FAQ

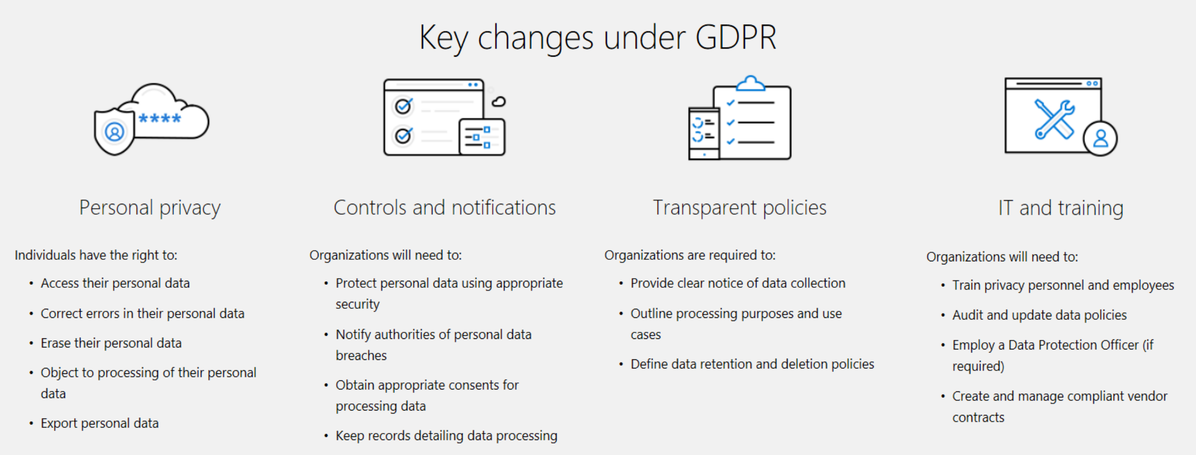
Other Audit Reports

In addition to the third-party audits referenced above, Microsoft meets a multitude of other standards and regulations; for a comprehensive list, see Other Audit Reports. This is a regularly maintained list of the reports related to the latest privacy, security, and compliance information about Microsoft's Cloud Services.

GDPR (EU) Compliance

Introduction

As of May 25, 2018, a European privacy law, the General Data Protection Regulation (GDPR), is in effect. The GDPR imposes new rules on companies, government agencies, non-profits, and other organizations which offer goods and services to people in the European Union (EU), or which collect and analyze data tied to EU residents. Microsoft applies GDPR requirements to all online services.



Key changes under GDPR

Personal privacy

Individuals have the right to:

- Access their personal data
- Correct errors in their personal data
- Erase their personal data
- Object to processing of their personal data
- Export personal data

Controls and notifications

Organizations will need to:

- Protect personal data using appropriate security
- Notify authorities of personal data breaches
- Obtain appropriate consents for processing data
- Keep records detailing data processing

Transparent policies

Organizations are required to:

- Provide clear notice of data collection
- Outline processing purposes and use cases
- Define data retention and deletion policies

IT and training

Organizations will need to:

- Train privacy personnel and employees
- Audit and update data policies
- Employ a Data Protection Officer (if required)
- Create and manage compliant vendor contracts

Microsoft has extensive expertise in protecting data, championing privacy, and complying with complex regulations, and currently complies with both EU-U.S. Privacy Shield and EU Model Clauses. We believe that the GDPR is an important step forward for clarifying and enabling individual privacy rights.

We are committed to GDPR compliance across our cloud services and provide GDPR-related assurances in our contractual commitments.

GDPR

Microsoft designed Dynamics 365 and Power Platform with industry-leading security measures and privacy policies to safeguard your data in the cloud, including the categories of personal data identified by the GDPR. Dynamics 365 can help you on your journey to reducing risks and achieving compliance with the GDPR.

Controlling who has access to personal data is a key to securing that data, and data security is a critical requirement of the GDPR. The platform enables you to manage and control access to your data in several ways:

- Role-based security allows you to group together a set of privileges that limits the tasks which can be performed by a given user. This is an important capability, especially when people change roles within an organization.
- Record-based security allows you to restrict access to specific records.
- Field-level security allows you to restrict access to specific high-impact fields, such as Personally Identifiable Information (PII).
- Azure Active Directory (Azure AD) helps you protect your environment from unauthorized access by simplifying the management of users and groups and allowing you to assign and revoke privileges easily. Azure AD includes tools such as Multi-Factor Authentication for highly-secure sign-in. Additionally, Azure AD

Privileged Identity Management helps you reduce risks associated with administrative privileges through access control, management, and reporting.

Another core requirement of the GDPR is to protect the personal data that you control or process. Power Platform is designed to optimize the security of your data:

- Security Development Lifecycle is a mandatory Microsoft process that embeds security requirements into every phase of the development process. Microsoft products, including Dynamics 365 are built using the Security Development Lifecycle.
- Encryption in transit between your users' devices and our data centers, as well as while at rest in Dataverse data storage, helps protect your data at all times.

Getting started with GDPR

Compliance is an on-going process and a shared responsibility. Microsoft offers a powerful set of tools and provides extensive documentation on how to use them to make the process easier. Microsoft is investing in additional features and functionality to help organizations with GDPR compliance.

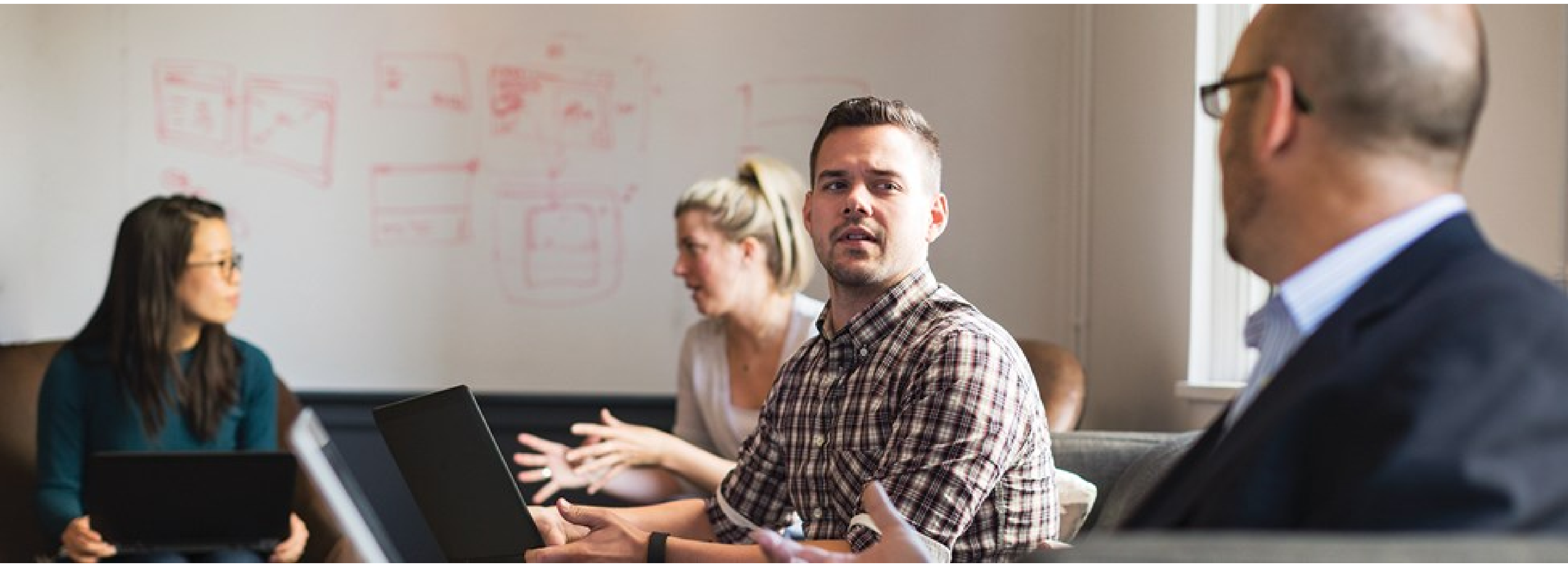
Whether you're a compliance officer, a decision-maker considering Dynamics 365 and Power Platform as a cloud solution, an administrator seeking help with a specific GDPR-compliant implementation, or an interested party looking for general information on how the GDPR relates to Dynamics 365 and cloud computing, the information here can provide you with a starting point to get what you need.

Every journey needs a roadmap. Your roadmap to GDPR compliance begins with focusing on four key steps, and Microsoft Dynamics 365 provides robust tools and solutions for tackling each step. Learn more about how Microsoft products and services can help you on the road to GDPR compliance.

Assess your organization	
Discover	The first step towards GDPR compliance is to assess whether the GDPR applies to your organization, and, if so, what data under your control is subject to the GDPR. This analysis includes understanding what data you have and where it resides. Adopting a classification scheme that applies throughout your organization helps you respond to data subject requests because it allows you to more quickly identify and process personal data requests. Microsoft Dynamics 365 and related tools help you discover and classify personal data. You can search for and identify personal data with: • Quick Find and Advanced Find • Relevance Search • Filters • Web API

Take advantage of tools	
Manage	The GDPR provides data subjects—individuals to whom data relates—with more control over how their personal data is captured and used. Managing access and controlling how data is used and accessed are fundamental to GDPR compliance. Dynamics 365 and Power Platform provides capabilities to authenticate users and govern access to personal data. Organizations can: • Display custom privacy notices and request and obtain consent for processing activities. • Rectify inaccurate or incomplete personal data using a variety of methods. • Decide if the delete request meets the GDPR requirements for deleting personal data. • Meet data subject portability requests by using data export capabilities. The organization may decide to use advanced-find capabilities to identify the data subject and their related data.

Discover built-in protection	
Protect	Microsoft services are developed using the Microsoft Secure Development Lifecycle which incorporates privacy-by-design and privacy-by-default methodologies. Dynamics 365 and related tools can help you comply with GDPR data protection requirements by providing ways to further secure/encrypt personal data at rest and in transit, detect and respond to data breaches, and facilitate regular testing of security measures. Dynamics 365 provides: • Transport Layer Security (TLS), SQL Server cell-level encryption, and Transparent Data Encryption (TDE) to protect personal data in transit and at rest. • Support for Azure Active Directory (Azure AD) to manage user identities. • The ability to grant and restrict user access to personal data via security roles and fields and hierarchy level security models. • Dynamics 365 auditing to help detect data breaches.



Tools to help keep detailed records	
Report	The GDPR sets new standards in transparency, accountability, and record-keeping. Organizations processing personal data will need to keep detailed records to be compliant. Microsoft provides capabilities to help meet data reporting requirements. With Microsoft Dynamics 365 and Dataverse environments, you can: • Track and record changes to personal data using the audit functionality. • Track and record processing activities relevant to a Data Protection Impact Assessment (DPIA) using audit capabilities. The GDPR sets requirements regarding the flows of personal data into and out of the EU and flows of personal data to third-party service providers. Exposure to unnecessary cross-border data transfer is reduced by Microsoft using a regional data center strategy. Microsoft offers contractual commitments for all its enterprise cloud services, including Dynamics 365. The commitments include detailed data protection terms, the EU Model Clauses, and compliance with the EU-US Privacy Shield Framework regarding the collection, use, and retention of personal information transferred from the European Union to the United States. Microsoft also maintains an inventory of third-party service providers who may have access to customer data, and limits access to customer data by third parties. Organizations that process personal data may be required to conduct Data Protection Impact Assessments (DPIAs). To help customers who are seeking information that may help them perform a DPIA addressing their use of Dynamics 365, Microsoft provides detailed information about its processing of customer data and the security measures used to protect that data.

GDPR Resources

See:

- GDPR Resources at Microsoft
- GDPR FAQ
- GDPR regulations
- Conduct a Data Privacy Impact Assessment
- Connect to the services you use with Power BI
- Get Started: Support for GDPR Accountability

How Microsoft Categorizes Data

Administrator data is the information about administrators supplied during signup, purchase, or administration of Microsoft services, such as names, phone numbers, and email addresses. It also includes aggregated usage information and data associated with your account, such as the controls you select. We use administrator data to provide services, complete transactions, service the account, and detect and prevent fraud.

Customer data is all data, including text, sound, video, or image files and software, that you provide to Microsoft or that is provided on your behalf through your use of Microsoft enterprise online services, excluding Microsoft Professional Services. For example, it includes data that you upload for storage or processing, as well as applications that you upload for distribution through a Microsoft enterprise cloud service.

Customer content is a subset of customer data and includes, for example, Exchange Online email and attachments, Power BI reports, SharePoint Online site content, or IM conversations.

Payment data is the information you provide when making online purchases with Microsoft. It may include a credit card number and security code, name and billing address, and other financial data. We use payment data to complete transactions, as well as to detect and prevent fraud.

Personal data means any information relating to an identified or identifiable natural person. In other words, personal data is any data that is associated with a specific person. Personal data provided by our customers through their use of the service, such as the names and contact information of customer end users, would also be customer data. But personal data could also include certain data that is not customer data, such as the user id our service assigns to each user; such personal data is considered pseudonymous because it alone cannot identify the individual.

Support and Consulting data means all data, including all text, sound, video, image files, or software, that are provided to Microsoft by, or on behalf of, Customer (or that Customer authorizes Microsoft to obtain from an Online Service) through an engagement with Microsoft to obtain Professional Services or Support. This may include information collected over phone, chat, e-mail, or web form. It may include description of problems, files transferred to Microsoft to resolve support issues, automated troubleshooters, or by accessing customer systems remotely with customer permission. It does not include administrator data or payment data.

Privacy

Introduction

Privacy

We will provide you with control over your data to help keep it private.

You are the owner of your data; we do not mine your data for advertising. If you ever choose to terminate the service, you can take your data with you.

Microsoft protects your data. We use your data only for purposes that are consistent with providing the services to which you subscribe.

If a government approaches us for access to your data, we redirect the inquiry to you, the customer, whenever possible. We have challenged in court, and will continue to challenge, any invalid legal demand which prohibits disclosure to our customer of a government request for their customer data. We will also refer all government requests for customer data to the legal authorities of the jurisdiction in which the customer data resides.

How we use your data

It is your data. You own the data you store and process with Microsoft 365 and Dynamics 365. We use your data only to provide the services you want.

We use your data for just what you pay us for: to maintain and provide Dynamics 365. It is our policy to not use your data for any other purposes. While some data may be stored or processed on systems used for both consumer and business services, our business services are designed and operated separately from Microsoft consumer services. Microsoft does not scan emails or documents for advertising purposes.

Customer Data is all the data, including all text, sound, software or image files that you provide, or are provided on your behalf, to us through your use of the services. Customer Data does not include Administrator Data, Payment Data or operational information about the services. See the Microsoft Online Services Privacy Statement for additional details.

Content is a subset of Customer Data. Content is generally considered confidential information, and in normal service operation, is not sent over the Internet without encryption. Content includes; for example, Exchange Online e-mail body and attachments, SharePoint Online site content (not URL) and file body, instant messaging conversation body and voice conversation, and CRM files containing data about your end-customer interactions.

Database metadata is information about database configuration and schema, including the names of database tables and columns. It does not include the contents of database rows of user tables. We use database metadata to provide services and compatible purposes and may store and process it in the United States or elsewhere. You should not include personal data in database metadata.

How does Dynamics 365 use my data?

The following table explains how Microsoft uses your Dynamics 365 Data:

Use of Dynamics 365 Customer Data	Customer Data (excluding Content)	Content	Database Metadata
Operating and Troubleshooting the Services	Yes	Yes	Yes
Security, Spam and Malware Prevention	Yes	Yes	Yes
Services Communications	Yes	No	Yes
Advertising	No	No	No
Voluntary Disclosure to Law Enforcement	No	No	No
Direct Marketing	No	No	No

Privacy FAQ

Question: How does Dynamics 365 use my data to maintain the service?

Answer: Customer Data will be used only to provide the service, including purposes compatible with providing the service, except as you direct.

In addition to day-to-day operations, such purposes can include using Customer Data for the following:

- Troubleshooting aimed at preventing, detecting and repairing problems affecting the operation of services.
- Ongoing improvement of features such as those that involve the detection of, and protection against, emerging and evolving threats to the services or Customer Data (such as malware or spam).
- Providing personalized or inference-based service features.

Question: Does Dynamics 365 share data with any advertiser-supported services? Does Dynamics 365 data-mine Customer Data for its advertisers?

Answer: No. Dynamics 365 does not share data with any advertiser-supported services. There is no data mining of customer data except as part of analysis services expressly used by customers, e.g., Power BI.

Question: Can Dynamics 365 use or disclose my data without my permission?

Answer: In a limited number of circumstances, Microsoft may need to disclose Customer Data without your prior consent, including as needed to satisfy legal requirements.

Question: What is Dynamics 365 process if law enforcement requests my data? What does Microsoft do when subpoenaed or legally mandated to produce customers' information?

Answer: Dynamics 365 believes that their customers should control their own information to the extent possible.

Accordingly, if a governmental entity approaches Microsoft directly for information hosted on behalf of our Dynamics 365 customers, Microsoft will try in the first instance to redirect the entity to the customer to afford the customer the opportunity to determine how to respond. If we are nonetheless required to respond to the demand, Microsoft will only provide information belonging to Dynamics 365 customers when it is legally required to do so, will limit the production to only that information which it is required to disclose and will use reasonable

efforts to notify the enterprise customer in advance of any production unless legally prohibited. Our notice will typically be delivered by email to one or more of the administrator(s) the customer has listed in the online services portal. It is the customer's responsibility to ensure contact information remains
up to date.

Question: What is usage data, and how does Microsoft use usage data?

Answer: Usage data are used to provide the service.

Usage data could refer to any number of data points related to Dynamics 365. "Usage data" could refer to the average number of emails an end user receives each day, the number of licenses in a customer's subscription, or the amount of electricity Microsoft needs to power Dynamics 365.

We understand our customers are most concerned about how we treat personally identifiable information about end users' interactions with the services. Such data may be used for day-to-day operations and maintenance of the services (as described above) and for services communications to administrators, including emails about end users' use or access to the services. For example, an administrator may receive a notification from Microsoft that an end user is near usage or storage limits.

Question: What are the services communications an administrator will receive?

Answer: Administrators may receive various types of communications from Microsoft related to use of the services. The administrator may also receive the following types of communications: communications about services operations, including scheduled maintenance and new features or functionalities of the services.

Privacy Controls

- Privacy controls help you configure who in your organization has access to the service and what they can access.
- We provision you with your own logically isolated data repository to help maximize the security and integrity of your data and to prevent mingling of your data with that of other organizations.

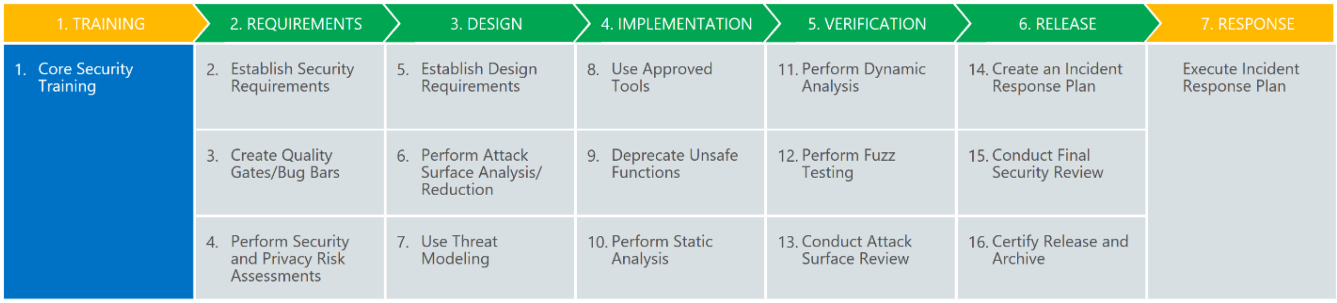
Security

Security

We will implement strong security measures to safeguard your data.

Security Development Life Cycle

The Security Development Lifecycle (SDL) is a software development process that helps developers build more secure software and address security compliance requirements while reducing development cost, and consists of the following phases:



1. TRAINING	2. REQUIREMENTS	3. DESIGN	4. IMPLEMENTATION	5. VERIFICATION	6. RELEASE	7. RESPONSE
1. Core Security Training	2. Establish Security Requirements	5. Establish Design Requirements	8. Use Approved Tools	11. Perform Dynamic Analysis	14. Create an Incident Response Plan	Execute Incident Response Plan
	3. Create Quality Gates/Bug Bars	6. Perform Attack Surface Analysis/ Reduction	9. Deprecate Unsafe Functions	12. Perform Fuzz Testing	15. Conduct Final Security Review	
	4. Perform Security and Privacy Risk Assessments	7. Use Threat Modeling	10. Perform Static Analysis	13. Conduct Attack Surface Review	16. Certify Release and Archive	

Data Center Security

Microsoft data centers employ controls at the perimeter, building, and computer room with increasing security at each level, utilizing a combination of technology and traditional physical measures.

- Security starts at the perimeter with camera monitoring, security officers, physical barriers and fencing.
- At the building, seismic bracing and extensive environmental protections protect the physical structure and integrated alarms, cameras, and access controls (including two-factor authentication via biometrics and smart cards) govern access. The systems are monitored 24x7 from the operations center.
- Similar access controls are used at the computer room, which also has redundant power.

DDoS Defense System

There are more distributed denial-of-services (DDoS) attacks than ever before, and they vary widely; they can be highly targeted or generic, long in duration or short. And they mutate; there's a new breed of DDoS attacks that use Web servers as payload-carrying bots, which makes them even more deadly because of exponential performance increases. And then there are application attacks, which are often targeted towards financial systems, which can bring a company to its knees.

- Azure has a defense system against DDoS attacks on Azure platform services. It uses standard detection and mitigation techniques such as SYN cookies, rate limiting, and connection limits. Azure's DDoS defense system is designed to withstand attacks generated from outside and inside the platform.
- Azure's DDoS defense system is designed not only to withstand attacks from the outside, but also from within.
- Azure monitors and detects internally initiated DDoS attacks and removes offending virtual machines (VMs) from the network.

- Azure's DDoS protection also benefits applications. However, it is still possible for applications to be targeted individually. As a result, customers should actively monitor their Internet-exposed and Windows Azure applications.

Supported DDOS Attack Profiles:

- TCP SYN
- UDP/ICMP/TCP Flood

Detection Process

- Traffic to a given /32 VIP Inbound or Outbound is tracked, recorded, and analyzed in real time to determine attack behavior

Mitigation Process

- Traffic is re-routed to scrubbers via dynamic routing updates
- Traffic is SYN auth. and rate limited

Data Segregation

Logical isolation segregates each customer's data from that of others. Azure is a multi-tenant service, meaning that multiple customers' deployments and virtual machines are stored on the same physical hardware. Azure uses logical isolation to segregate each customer's data from that of others. This provides the scale and economic benefits of multitenant services while rigorously preventing customers from accessing one another's data.

Encryption

At-Rest Data Protection

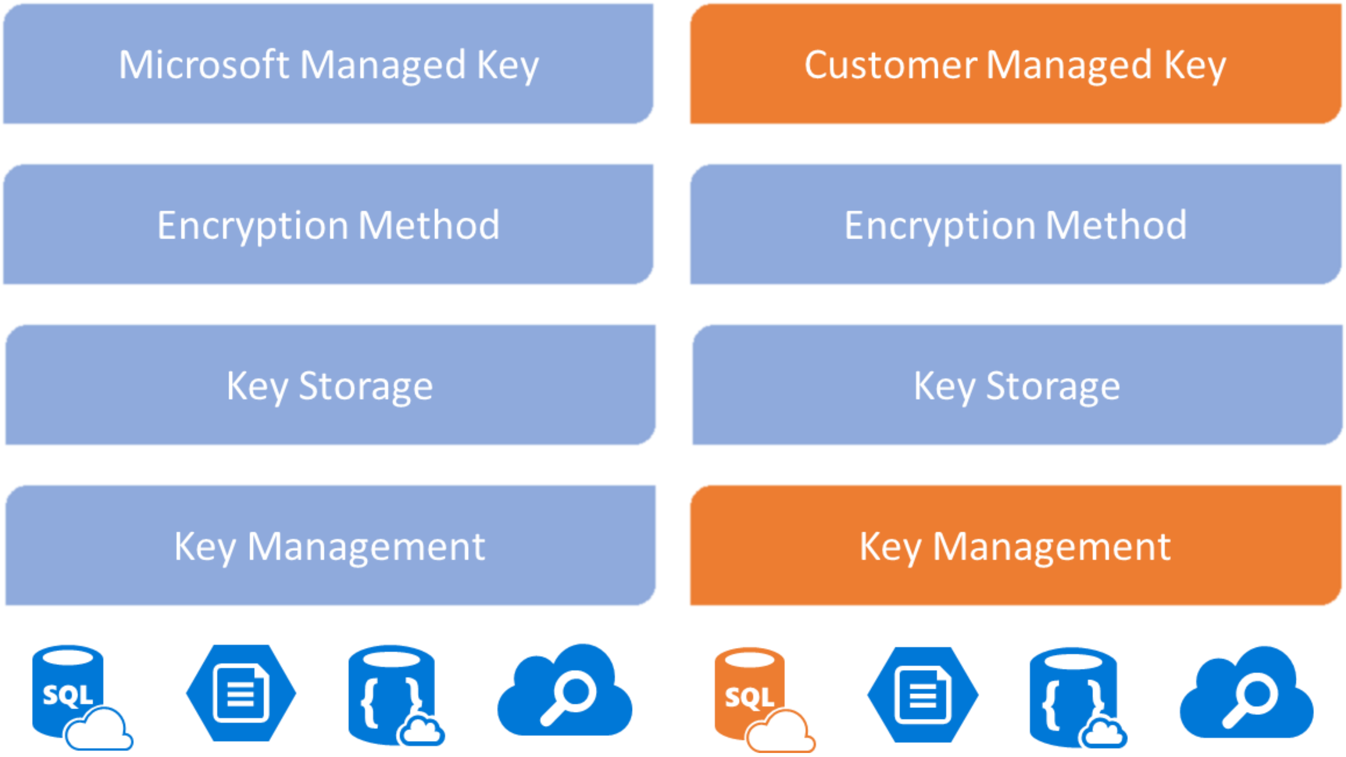
Data is an organization's most valuable and irreplaceable asset, and encryption serves as the last and strongest line of defence in a multi-layered data security strategy. Microsoft business cloud services and products use encryption to safeguard customer data and help you maintain control over it. Encrypting your information renders it unreadable to unauthorized persons, even if they break through your firewalls, infiltrate your network, get physical access to your devices, or bypass the permissions on your local machine. Encryption transforms data so that only someone with the decryption key can access it.

Dynamics 365 uses heterogenous storage (Dataverse) to store the data. The data is distributed across different storage types:

- Azure SQL Database for relational data
- Azure Blob storage for binary data, such as images and documents
- Azure Search for search indexing
- Microsoft 365 Activity Log and Azure Cosmos DB for audit data

Dataverse databases are using SQL TDE (Transparent Data Encryption, compliant with FIPS 140-2) to provide real-time I/O encryption and decryption of the data and log files for data encryption at-rest. Azure Storage Encryption is used for data at rest stored in the Azure Blob Storage. These are encrypted and decrypted transparently using 256-bit AES encryption compliant with FIPS 140-2.

By default, Microsoft stores and manages the database encryption key for your Dynamics 365 environments. As of now, given the heterogenous storage, the customer managed key feature is available only for the Azure SQL database that stores transactional data. The File/Document (blob storage) and Azure Data Lake encryption by customer managed key is in the roadmap for future releases. The manage keys feature in the Power Platform admin center gives administrators the ability to self-manage the database encryption key that is associated with the tenant. Given the heterogenous type of storage, Customer Managed Keys are limited to encrypt the Azure SQL Database storing transactional data only. File, Log and Search encryption will remain managed by Microsoft.



Administrators can provide their own encryption key using their own key generator hardware (HSM) or use our administrator tool to generate an encryption key. The key management feature supports both PFX and BYOK encryption files.

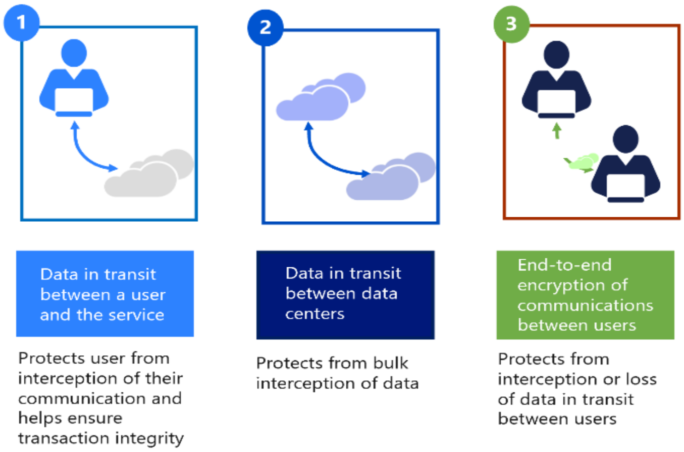
The key management feature takes the complexity out of encryption key management by using Azure Key Vault to securely store encryption keys. Azure Key Vault helps safeguard cryptographic keys and secrets used by cloud applications and services. The key management feature doesn't require that you have an Azure Key Vault subscription and for most situations there is no need to access encryption keys used for Dynamics 365 (Dataverse) within the vault. Encryption keys must meet the following Azure Key Vault requirements:

1. Key file format of PFX or BYOK,
2. 2048-bit RSA or RSA-HSM key type, and
3. PFX encryption key are password protected.

Administrators also can revert the encryption key back to a Microsoft managed key at any time.

In-Transit Data Protection

Azure protects data in transit to or from outside components, as well as data in transit internally, such as between two virtual networks. Azure uses industry standard transport protocols such as TLS between user devices and Microsoft data centers, and within data centers themselves. To protect your data even more, internal communication between Microsoft services is using Microsoft backbone network and therefore is not exposed to the public internet.


1
2
3
Data in transit between a user and the service
Protects user from interception of their communication and helps ensure transaction integrity
Data in transit between data centers
Protects from bulk interception of data
End-to-end encryption of communications between users
Protects from interception or loss of data in transit between users

Microsoft uses multiple encryption methods, protocols, and algorithms across its products and services to help provide a secure path for data to travel through the infrastructure, and to help protect the confidentiality of data that is stored within the infrastructure. Microsoft uses some of the strongest, most secure encryption protocols in the industry to provide a barrier against unauthorized access to your data. Proper key management is an essential element in encryption best practices, and Microsoft helps ensure that encryption keys are properly secured.

Protocols and technologies examples include:

- **Transport Layer Security/Secure Sockets Layer** (TLS/SSL), which uses symmetric cryptography based on a shared secret to encrypt communications as they travel over the network.
- **Internet Protocol Security** (IPsec), an industry-standard set of protocols used to provide authentication, integrity, and confidentiality of data at the IP packet level as it's transferred across the network.
- **Advanced Encryption Standard** (AES)-256, the National Institute of Standards and Technology (NIST) specification for a symmetric key data encryption that was adopted by the US government to replace Data Encryption Standard (DES) and RSA 2048 public key encryption technology.

Data Residency

As a customer of Microsoft business services, you know where your data is stored.

It is particularly important for customers who operate in highly regulated industries, or in countries with data protection laws, to know the geographic location of the data that they have entrusted to a Microsoft cloud service. Microsoft also understands that some customers must maintain their data in a specific geographic location, such as within the European Union (EU). To that end, Microsoft maintains an ever-expanding network of data centers around the globe and verifies that each data center meets stringent security requirements.

- Customer data may be replicated within a selected geographic area for enhanced data durability in case of a major data center disaster. See the following section 5.1 Data Location and Access, and Dynamics 365 and Power Platform international Availability document – section Data Location, for specific details.
- Microsoft also complies with international data protection laws regarding transfers of customer data across borders. For example:
  - To allow for the continuous flow of information required by international business (including the cross-border transfer of personal data), many Microsoft business cloud services offer customers EU Standard Contractual Clauses that provide additional contractual guarantees around transfers of personal data for

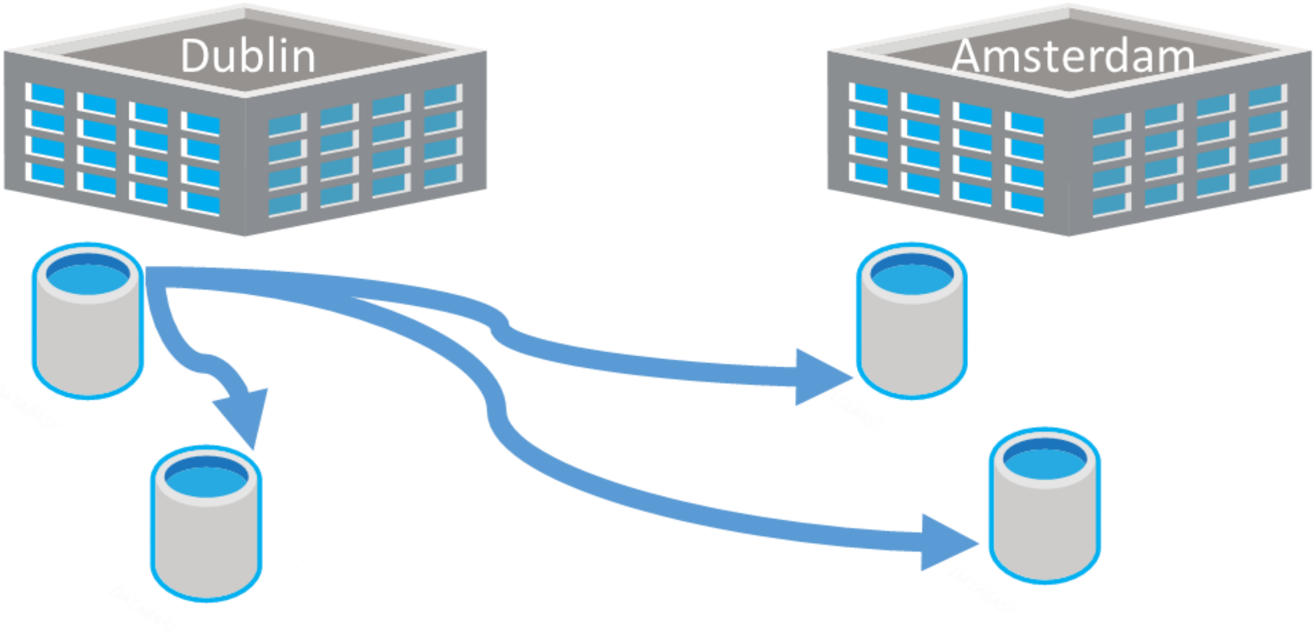
in-scope cloud services. Our implementation of the EU Model Clauses has been validated by EU data protection authorities as being in line with the rigorous privacy standards that regulate international data transfers by companies operating in its member states.

- In addition to our commitments under the Standard Contractual Clauses and other model contracts, Microsoft is certified to the EU-U.S. Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information transferred from the EU to the United States. Microsoft participation in the Privacy Shield applies to all personal data that is subject to the Microsoft Privacy Statement and is received from the EU, European Economic Area, and Switzerland. Microsoft also abides by Swiss data protection law regarding the processing of personal data from the European Economic Area and Switzerland.
- Microsoft will not transfer to any third party (not even for storage purposes) data that you provide to Microsoft through the use of our business cloud services that are covered under the Microsoft Online Services Terms.

Note that no matter where customer data is stored, Microsoft does not control or limit the locations from which customers or their end users may access their data.

Data Redundancy – Dynamics 365 and Dataverse Environments

Dynamics 365 and Power Platform data is replicated, the original copy and a real-time replica are kept on the primary data center site. Two additional near real-time replicas are located in a secondary data center site within the same
geo-region.



Data Redundancy

Microsoft ensures data is protected in the event of a cyberattack or physical damage to a data center. Data may be replicated within a selected geographic area for redundancy but will not be transmitted outside it.

- Locally redundant storage (LRS). Locally redundant storage maintains three copies of your data. LRS is replicated three times within a single facility in a single region. LRS protects your data from normal hardware failures, but not from the failure of a single facility.
- Zone-redundant storage (ZRS). Zone-redundant storage maintains three copies of your data. ZRS is replicated three times across two to three facilities, either within a single region or across two regions, providing higher durability than LRS. ZRS ensures that your data is durable within a single region.
- Geo-redundant storage (GRS). Geo-redundant storage is enabled for your storage account by default when you create it. GRS maintains six copies of your data. With GRS, your data is replicated three times within the primary region, and is also replicated three times in a secondary region hundreds of miles away from the primary region, providing the highest level of durability. In the event of a failure at the primary region, Azure Storage will failover to the secondary region. GRS ensures that your data is durable in two separate regions.

Disaster Recovery - Dynamics 365 and Dataverse environments

Disaster recovery is a feature of Power Platform to recover from a planned or unplanned service interruption. An example of a planned service interruption is regular and periodic data center system maintenance. An example of an unplanned service interruption is a failure of a key computer system or network component in a data center. For either case, you temporarily lose access to your organization's data and services.

Planned service interruptions are preceded by a public notice in the application and Microsoft Dynamics 365 Message center identifying the date and time of the service maintenance so that businesses can plan for the interruption in accessing their organization's data. Unplanned service interruptions result in a notice that the organization is currently undergoing unplanned maintenance.

When a failure or a disaster occurs, well-defined processes are applied by the administrators of the data center to recover from a service interruption. The processes and software to recover from these service interruptions is known as ***disaster recovery failover***. Your main data center maintains a duplicate and synchronized (alternate) copy of your organization's data on a different scale group set. Should a disaster occur in the data center where you no longer have access to your data, the administrators monitoring the data center can switch access from your primary organization to this replica, thereby minimizing the service interruption. When the failure has been corrected, service access to your primary organization can be restored.

This recovery happens in the data center and is handled transparently to you. To avoid any data loss due to unavailability of the environment, it is important to implement queueing and retry mechanisms into any custom code.

Microsoft does not contractually commit to specific Recovery Point Objective (RPO) or Recovery Time Objective (RTO). For our core platform, the RPO is 10 minutes (a direct measure of how frequently backups occur). However, we do maintain a continuous copy across the DR region for org databases, and therefore, in practice, the RPO is much less. For example, just as a data point, in production today, the lag of a continuous Disaster Recovery (DR) copy in Azure SQL DB across data centers is only about 5 seconds. For High Availability scenarios, RTO is about 30 seconds – for Disaster Recovery it depends on the nature of the disaster plus the time needed to re-route the DNS servers.

Data Destruction

When customers delete data or leave the Power Platform and Dynamics 365, Microsoft follows strict standards for overwriting storage resources before reuse, as well physical destruction of decommissioned hardware. Microsoft executes a complete deletion of data on customer request and on contract termination.

Aspects of Online Security

Introduction

Microsoft believes that security does not end in the public cloud. Security needs to be engineered into a system end to end, from the public cloud all the way to the desktop. From the very beginning, we architected our cloud services platform with multiple levels of security that are virtually and physically isolated. Your data is protected by hardened operating systems and backed by a defense-in-depth strategy that helps protect our cloud services.

In addition, we have continuous, proactive, and reactive threat monitoring and analytics. We also encrypt customer data at rest and in transit and encrypt customer data that passes between our data centers. Every data center is constructed, managed, and monitored to protect data from unauthorized access. We also do not engineer backdoors into our services.

Our platform and services offer an exceptional depth of security-intelligence that we use to help our customers detect threats and respond to them more quickly. The depth of our security-intelligence comes from running multiple large services at a global scale:

- 60 million monthly active Microsoft 365 commercial customers, with 50,000 small business customers added each month
- 49 million Xbox Live monthly active users
- 10 million seats for Dynamics 365
- Over 400 million active Outlook users
- Azure runs on a worldwide network of Microsoft-managed data centers across 30 regions—more countries and regions than Amazon Web Services and Google Cloud combined.

Because we handle both consumer and commercial customers at such a large scale, we have a unique perspective on what's happening in the public cloud. We use the expertise we have gained to identify attack vectors and define the best ways to respond to them. We also use machine learning and behavioral analytics to look for malicious characteristics, such as executable code or requests for elevated privileges. We build threat intelligence technology into the core of our products to help secure our customers' data. Additionally, we use the insights we gain to drive innovation in cybersecurity—to proactively develop new technologies and practices to help us secure our cloud services.

Defense-in-Depth

While security has always been a focus for Microsoft, we recognize that the digital world requires continuous evolution in to how we Protect, Detect, and Respond to security threats.

Defense-in-depth is a best practice across the industry and it's the approach we take to protect our valuable customer and corporate assets.

Defense-in-Depth ensures that:

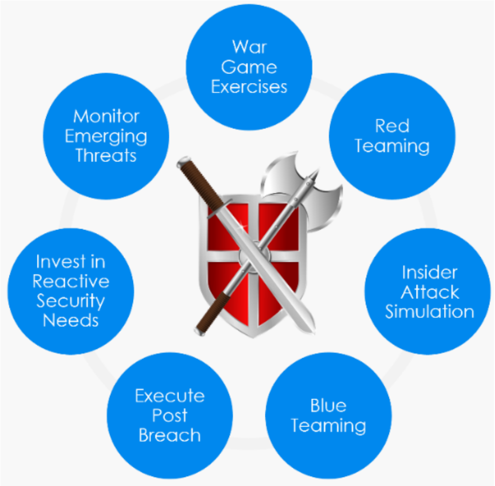
- We maintain proper hygiene through up-to-date anti-malware software and adhere to strict patching and configuration management.
- We have extensive monitoring and controls over the physical environment of our global data centers.
- We use Multifactor Authentication, ensure proper Identity and Access management and configuration, and ensure that vulnerability scanning remains effective across the entire stack.
- We also rely on a Just-In-Time (JIT) administrator policy, which eliminates persistent administrator rights. Elevated access is limited to a pre-determined duration of time and automates the removal of domain users and service accounts, and the removal from security groups.
- For applications, we utilize the Security Development Lifecycle and routinely validate it through penetration testing and vulnerability scanning.
- And finally, we classify data according to its sensitivity and take appropriate measures to protect it, including strong authentication, encryption in transit and at rest, and enforce least privilege access principles.

Our security teams know that we must:

- Move faster to detect threats using the scale and intelligence of our cloud, with machine learning and behavioral monitoring.
- Respond more quickly and comprehensively and share insights with customers that are actionable and holistic.

Assume Breach Strategy - Policies, Processes and Approach we use in the Cyber Defense Operations Center

The Assume Breach strategy requires the ability to automatically identify unexpected activity, analyze its cause, and address security gaps if any are found to exist. Microsoft baselines normal system behavior by collecting anonymized data on a massive scale and analyzing attack patterns. The system uses this information to proactively detect suspicious conditions and respond quickly and automatically. Microsoft has developed a highly effective system of automated patch deployment that generates and deploys solutions to problems identified by the monitoring systems—all without human intervention. This greatly enhances the security and agility of the service.



See “Anatomy of a Breach” here

Secure Admin Workstations (SAWs)	• Hardened and admiratively locked down systems required for Production Access • Separated from standard business activities such as Mail, Web-Browsing, etc
Just-in-Time Access / Zero Persistent Admins	• Administrative access is provisioned temporarily, and on-demand, backed with tickets trails and approval gates
Pattern analysis of attacks (e.g., APTs)	• Large scale data analytics to look for indications of compromise

Regular practice of incident response	• Reoccurring Cops-Robbers simulation with pen testers acting like rogue insiders who already have access • Continuous improvement on playbooks, containment, eviction
AppLocker Enforcement	• Whitelisted enforcement of apps execution
Auditing All Access to the Service	• PowerShell, Logins, Actions taken, Elevations, Account creations

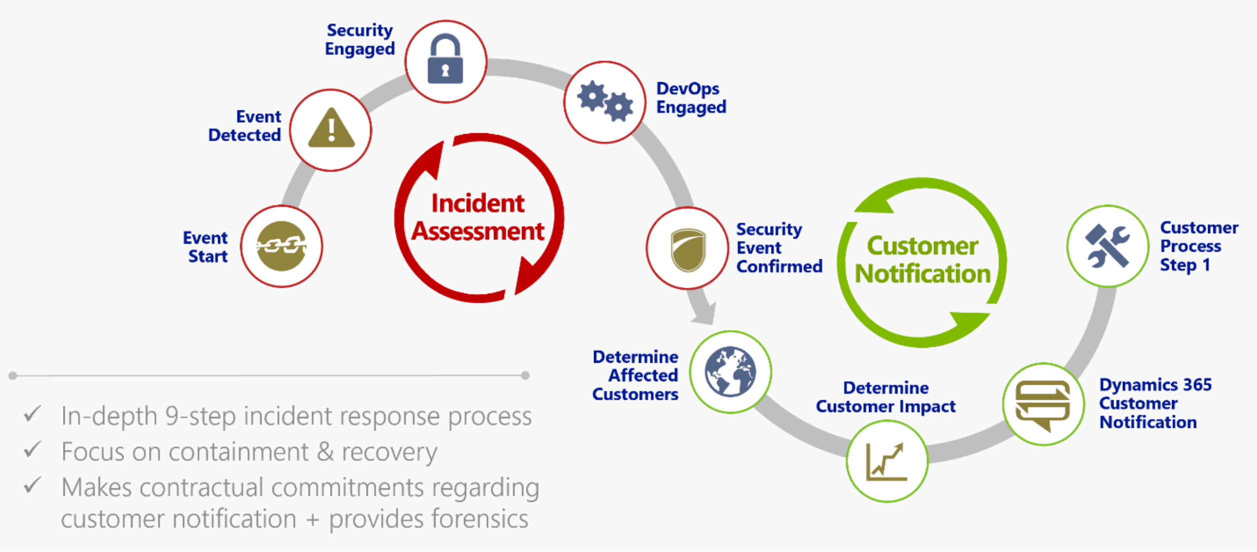
Assume breach also involves penetration tests and continuous improvement of incident response procedures.

Microsoft accomplishes this through a “War Games” approach in which a “Red Team” of Microsoft security experts tries to breach Microsoft 365, Dynamics 365 and Azure using emerging attack methodologies, and then attempts to escape and evade ensuing defences. An opposing “Blue Team” works to thwart the attack and is measured on “Mean Time To Detection” (the average time taken to detect that a security breach is imminent or has occurred) and “Mean Time To Recover” (the average time taken to recover from a security breach). The Blue Team works to create a methodical, repeatable, and optimized stepwise response process.

The War Games approach accurately simulates real-world attacks, trains the response team, identifies areas of investment, and helps create effective strategies for slowing attacks and speeding recovery

Security Incident Response

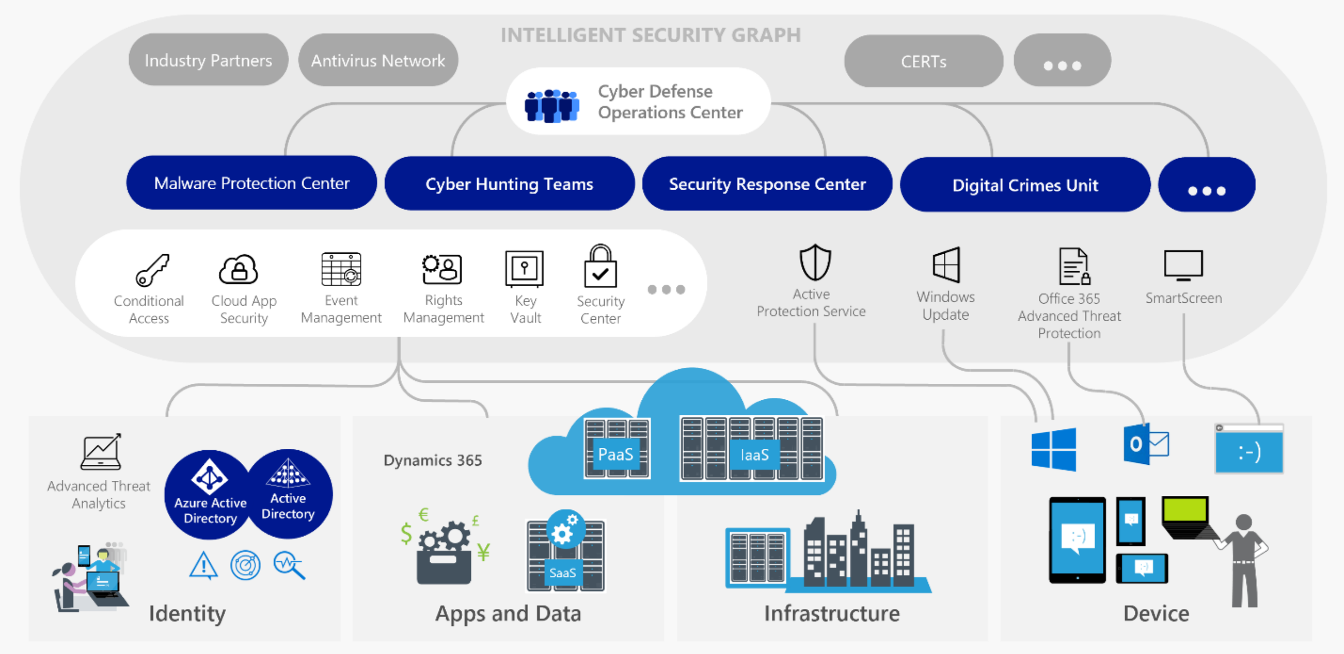
The security controls and risk management processes Microsoft has in place to secure the cloud infrastructure reduce the risk of security incidents, but in the event an incident occurs, the Security Incident Management (SIM) team within the Microsoft Online Security Services & Compliance (OSSC) team is ready 24 hours a day, every day to respond. SIM’s mission is to quickly and accurately assess and mitigate computer security incidents involving Microsoft's Online Services, while managing the necessary internal and customer communications.


Security Engaged
DevOps Engaged
Event Detected
Incident Assessment
Event Start
Security Event Confirmed
Customer Notification
Customer Process Step 1
Determine Affected Customers
Determine Customer Impact
Dynamics 365 Customer Notification
✓ In-depth 9-step incident response process
✓ Focus on containment & recovery
✓ Makes contractual commitments regarding customer notification + provides forensics

When events are detected, a 9-step process is kicked off that focuses first on containment and recovery. Customer notification is a key part of this process. Microsoft Azure provides coordination of forensic analysis, evaluation of logs, and VHD images in the event of platform-level incident. Azure also works with customers to provide log data to help them respond to threats.

Microsoft Protecting You

There are many components to the intelligent security graph:



- **Cyber Defense Operations Center (CDOC)** – The Microsoft Cyber Defense Operations Center is a 24x7 cybersecurity and defense facility that unites our security experts and data scientists in a centralized location. Advanced software tools and real-time analytics help us protect, detect, and respond to threats to Microsoft's cloud infrastructure, products and devices, and our internal resources.
- **Digital Crimes Unit (DCU)** – A team of legal and technical experts who work with law enforcement agencies—including Europol, the FBI, and Interpol—academia, global government agencies, and commercial customers.
- **Cyber Hunting Teams** – Microsoft's blue teams that are constantly hunting for adversaries on our enterprise and cloud services environments.
- **Microsoft Malware Protection Center (MMPC)** – Microsoft team responsible for the world's largest anti-virus and antimalware service who is committed to helping Microsoft customers keep their computers secure and quickly respond to malware outbreaks by continuously gathering and analyzing data and working with organizations inside and outside Microsoft.
- **Microsoft Security Response Center (MSRC)** – Microsoft team that identifies, monitors, responds to and resolves security incidents and vulnerabilities in Microsoft software, services and devices. Leads cross-company coordinated security response for highest severity events and partners with external organizations for coordinated cross-company and government response.

All of the learnings from these teams working together teaches us how to make our products more secure as well as to better protect customers in near real time.

Syrian Electronic Army (SEA) Story

As an illustration of how these come together, you may recall that the Syrian Electronic Army (SEA) attacked Microsoft a few years ago. During that attack, Microsoft leveraged intelligence from our internal investigation to find and remove attack emails from Microsoft mailboxes as well as those of our Microsoft 365 customers before customer users could click on them.

The assets you have to protect are broken down into 4 main categories:

- **Identities** – Critical element to security as all assurances are based on authentication and authorization provided by identity systems
- **Apps and Data** – The stores of business value whose confidentiality, integrity, and availability must be protected.
- **Infrastructure** – A critical security dependency for most apps and data that adversaries are exploiting to get at them
- **Devices** – the front line of the security battle that collectively protects access to all of your assets

Many of our capabilities directly leverage threat intelligence to protect you against threats including

- **SmartScreen** –Built into Edge and Internet explorer to provide cloud-powered protection against attack websites, downloaded applications, and malware hosted on legitimate websites.
- **Advanced Threat Protection** – Cloud-powered email filtering service for that helps protect against malware in email, it protects against links as they are clicked (versus just at time of sending) as well as detonating attachments in a VM to protect against well-hidden malware. https://technet.microsoft.com/en-us/library/exchange-online-advanced-threat-protection-service-description.aspx
- **Windows Update** – Updates Windows software and removes top malware threats from PCs each month
- **Active Protection Service (MAPS)** – Cloud powered malware detection built into Windows Defender that significantly increases detection of advanced malware

Additionally, Microsoft has many security capabilities to protect your data center and identity assets. Examples include:

- **Conditional Access** – Restrict access to data and applications using many factors including authentication strength, device health/security, and user role
- **Cloud App Security** – Address shadow IT issues by enabling you to discover corporate data stored on sanctioned and unsanctioned cloud services, then establishing, customizing, and enforcing policy
- **Event Management** – Get security and Operational Health insights into your on-premises and cloud hosted assets
- **Rights Management (RMS)** – Apply policy to documents and data, enforce using strong encryption, and enable users with simple integrated controls built into Office Apps, SharePoint, and Exchange (online and on-premises)
- **Key Vault** – Manage and Protect critical keys that your enterprise security depends on with strong hardware-rooted protection and convenience and availability of a cloud service.
- **Security Center (ASC)** – Get deep insight and detailed visibility into security hygiene for Azure hosted virtual machines (VMs)
- …and many more

Cybercrime / Cyber Defense Operations Center

Introduction

Cybercrime is a constantly evolving and ever-increasing challenge for all organizations. The combination of expanded access to the Internet, the explosive increase in connected devices, and the rapid expansion of innovative cloud-based services is creating tremendous economic and social opportunity for consumers, governments, and businesses. Unfortunately, it has also opened new avenues of attack for cybercriminals and other malicious actors.

Like all technical advances, the storage of data and applications in the cloud has attracted an entire criminal ecosystem, from individual hackers to highly organized groups that aim to take down entire networks. Cybercriminals, motivated by everything from profit to political gain, use the Internet to disrupt business activities and access sensitive personal and financial data. Because most companies rely on a third party to administer their cloud services, it is critical that companies which provide cloud services, like Microsoft, are committed to, and capable of, fighting cybercrime.

Unfortunately, cybercrime is not purely a technical problem—nor will it ever “go away.” Cloud service providers must continuously fight cybercrime at multiple levels using teams of specialists, from IT security experts to policy advocates. It takes a concerted effort as well as deep financial and operational investment to truly understand cybercrime and effectively fight it.

Microsoft knows that security and privacy are intrinsically connected—the data you entrust to Microsoft cloud services must be kept private. We work diligently to help protect your data from unauthorized access—both internally and externally. Microsoft has made significant investments in the security of its platform, which, when combined with high levels of security-intelligence and strategic partnerships, helps keep our cloud-based products and services more secure.

Microsoft has invested in multiple cybersecurity teams and related facilities to address threats to our customers and our technology ecosystem. The Microsoft Enterprise Cybersecurity Group is a team of world-class architects, consultants, and engineers that works with organizations to help move them to the cloud more securely, modernize their IT platforms, and avoid and mitigate breaches. The Microsoft Cybersecurity Policy Team partners with governments and policymakers around the world, blending technical acumen with legal and policy expertise. By identifying strategic issues, assessing the impacts of policies and regulations, leading by example, and driving ground-breaking research, the Cybersecurity Policy team helps promote a more secure online environment.

Defending against Cyberthreats

The Microsoft Cyber Defense Operations Center is a state-of-the-art facility that brings together security response experts from across the company to help protect, detect, and respond to cyberthreats in real-time—all day, every day.

Cyber Defense Operations Center
Providing world-class security protection, detection, and response
Microsoft

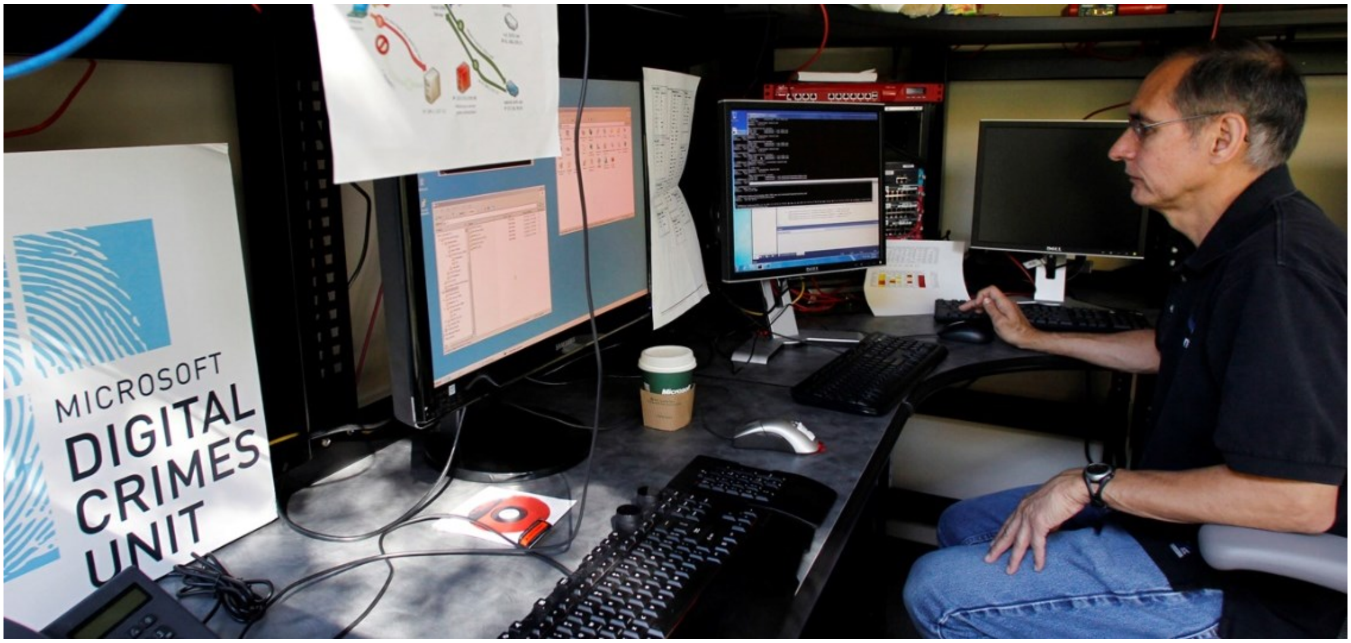
- 24 x 7 x 365 protection of Microsoft's cloud infrastructure, customer-facing cloud services, products and devices, and internal resources. Unite personnel, technology, and analytics
- Centralized hub for cybersecurity and defense
- World-class security protection, detection and response
- More than 50 Security Experts and Data Scientists
- Connected to >3500 Security Professionals across Microsoft
- Tight partnerships with Microsoft Research and the Security Development Lifecycle (SDL) team

The Digital Crimes Unit

Cybercrime is a constantly evolving and ever-increasing challenge for all organizations. The combination of expanded access to the Internet, the explosive increase in connected devices, and the rapid expansion of innovative cloud-based services is creating tremendous economic and social opportunity for consumers, governments, and businesses. Unfortunately, it has also opened new avenues of attack for cybercriminals and other malicious actors.

Like all technical advances, the storage of data and applications in the cloud has attracted an entire criminal ecosystem, from individual hackers to highly organized groups that aim to take down entire networks. Cybercriminals, motivated by everything from profit to political gain, use the Internet to disrupt business activities and access sensitive personal and financial data. Because most companies rely on a third party to administer their cloud services, it's critical that companies that provide cloud services, like Microsoft, are committed to, and capable of, fighting cybercrime.

Unfortunately, cybercrime is not purely a technical problem—nor will it ever "go away." Cloud service providers must continuously fight cybercrime at multiple levels using teams of specialists, from IT security experts to policy advocates. It takes a concerted effort as well as deep financial and operational investment to truly understand cybercrime and effectively fight it.



Microsoft knows that security and privacy are intrinsically connected—the data you entrust to Microsoft cloud services must be kept private. We work diligently to help protect your data from unauthorized access—both internally and externally. Microsoft has made significant investments in the security of its platform, which, when combined with high levels of security-intelligence and strategic partnerships, helps keep our cloud-based products and services more secure.

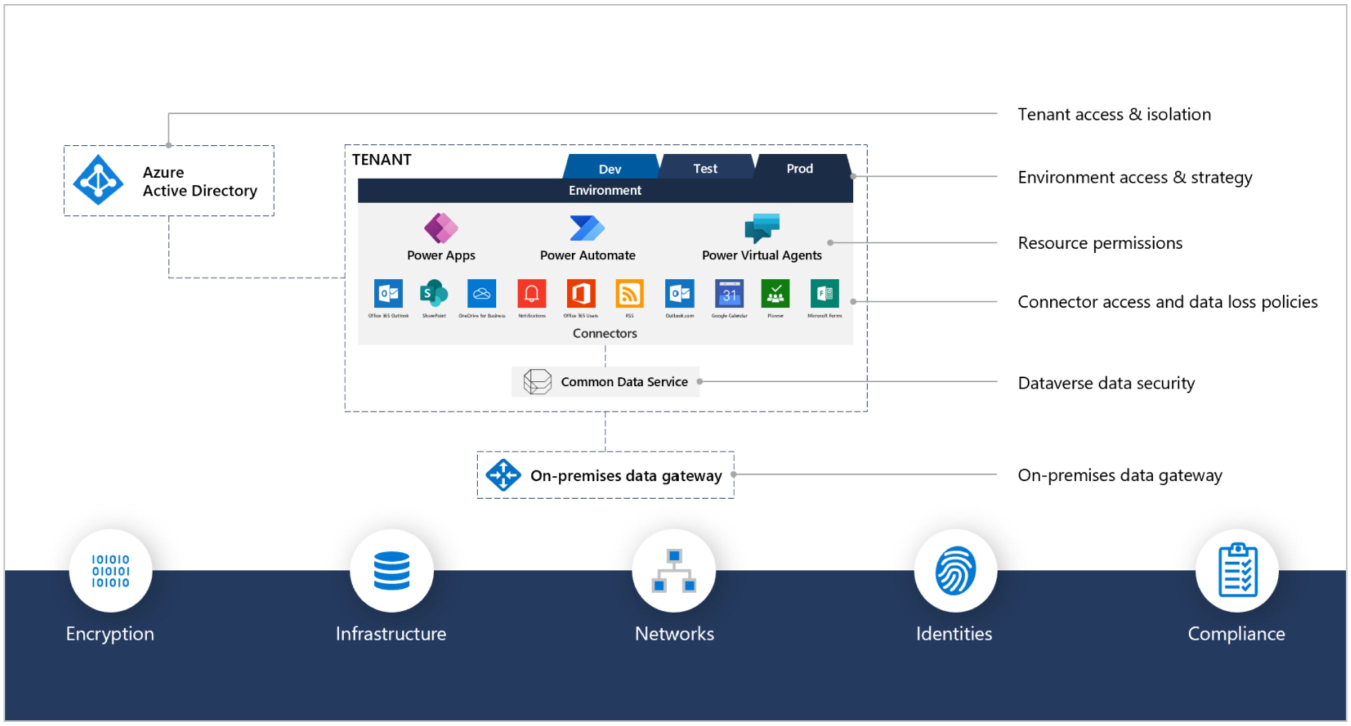
Microsoft's Digital Crimes Unit (DCU) combines big data analysis, cutting-edge forensics, partnerships and the law to keep customers and people safe online from cybercrime, relying on some of the brightest employees, some of the smartest scientists, and certainly some of the company's best partners in law enforcement, to disrupt and dismantle devious cybercriminals.

Secure Identity

Authentication – Users

Dynamics 365 and the Power Platform are exclusively authenticated via Azure Active Directory (AAD) helps you manage user identities and create intelligence-driven access policies to secure your resources. Azure AD centralizes identity and access management to enable deep security, productivity, and management across devices, data, apps, and infrastructure. Azure AD is built to work for apps in the cloud, on mobile, or on-premises, and you can layer security features such as ***conditional access*** to help protect users and your business.

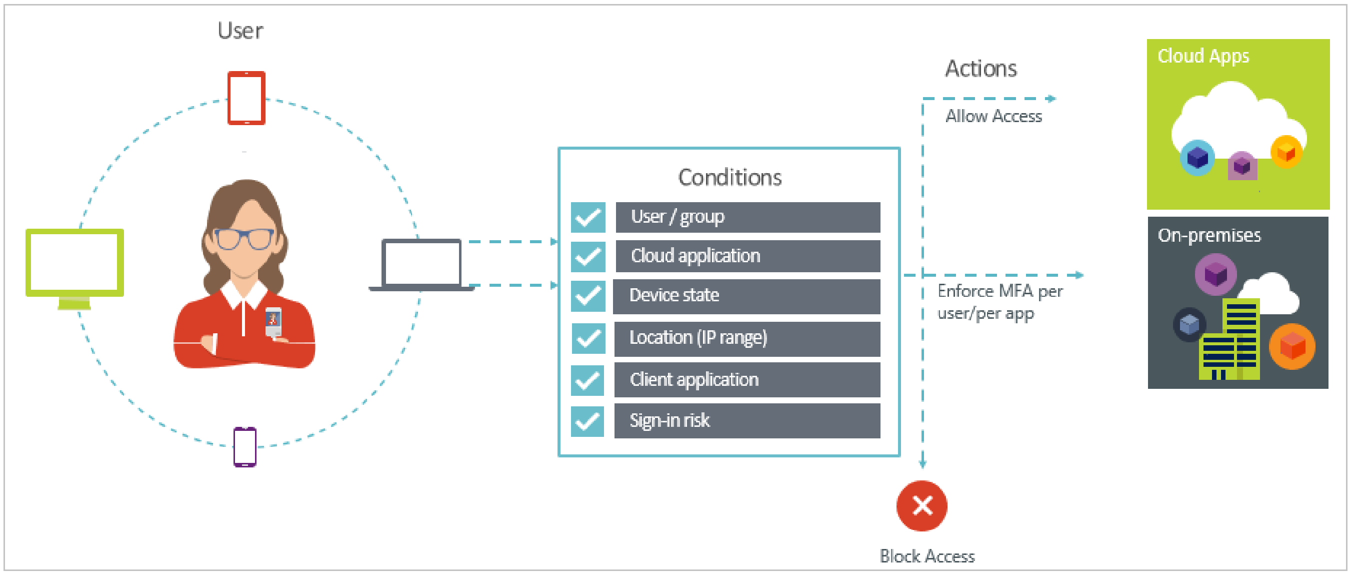
Azure AD provides full secured identity federation with Active Directory on premises – Federation with Azure AD enables users to authenticate using on-premises credentials and access all resources in cloud.



Authentication – Conditional Access

Security is a top concern for organizations using the cloud. A key aspect of cloud security is identity and access when it comes to managing your cloud resources. In a mobile-first, cloud-first world, users can access your organization's resources using a variety of devices and apps from anywhere. As a result of this, just focusing on who can access a resource is not sufficient anymore. To master the balance between security and productivity, you also need to factor how a resource is accessed into an access control decision. With Azure AD conditional access, you can address this requirement. Conditional access is a capability of Azure Active Directory.

With conditional access, you can implement automated access control decisions for accessing your cloud apps that are based on conditions.



In a mobile-first, cloud-first world, Azure Active Directory enables single sign-on to devices, apps, and services from anywhere. With the proliferation of devices (including BYOD), work off corporate networks, and third-party SaaS apps, you are faced with two opposing goals:

- Empower users to be productive wherever and whenever
- Protect the corporate assets at any time

By using conditional access policies, you can apply the right access controls under the required conditions. Azure AD conditional access provides you with added security when needed and stays out of your user's way when it isn't.

Following are some common access concerns that conditional access can help you with:

- **Sign-in risk:** Azure AD Identity Protection detects sign-in risks. How do you restrict access if a detected sign-in risk indicates a bad actor? What if you would like to get stronger evidence that a sign-in was performed by the legitimate user? What if your doubts are strong enough to even block specific users from accessing an app?
- **Network location:** Azure AD is accessible from anywhere. What if an access attempt is performed from a network location that is not under the control of your IT department? Using a username and password combination might be good enough as proof of identity for access attempts to your resources from your corporate network. What if you demand a stronger proof of identity for access attempts that are initiated from unexpected countries or regions of the world? What if you even want to block access attempts from certain locations?
- **Device management:** In Azure AD, users can access cloud apps from a broad range of devices including mobile and personal devices. What if you demand that access attempts should only be performed using devices that are managed by your IT department? What if you even want to block certain device types from accessing cloud apps in your environment?
- **Client application:** Today, you can access many cloud apps using different app types such as web-based apps, mobile apps, or desktop apps. What if an access attempt is performed using a client app type that causes known issues? What if you require a device that is managed by your IT department for certain app types?

These questions and the related answers represent common access scenarios for Azure AD conditional access. Conditional access is a capability of Azure Active Directory that enables you to handle access scenarios using a policy-based approach.

A conditional access policy is a definition of an access scenario using the following pattern:

When this happens
Then do this

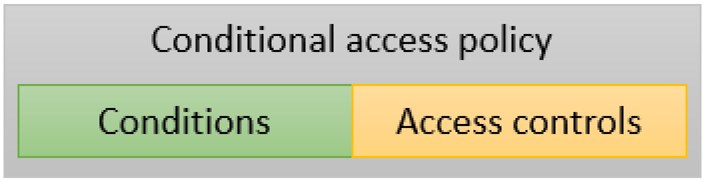
When this happens defines the reason for triggering your policy. This reason is characterized by a group of conditions that have been satisfied. In Azure AD conditional access, the two assignment conditions play a special role:

- **Users:** The users performing an access attempt (**Who**).
- **Cloud apps:** The targets of an access attempt (**What**).

These two conditions are mandatory in a conditional access policy. In addition to the two mandatory conditions, you can also include additional conditions that describe how the access attempt is performed. Common examples are using mobile devices or locations that are outside your corporate network. For more information, see Conditions in Azure Active Directory conditional access.

Then do this defines the response of your policy. It is important to note that the objective of a conditional access policy is not to grant access to a cloud app, it is to control how access may be granted. In Azure AD, granting access to cloud apps is subject of user assignments. With a conditional access policy, you control how authorized users (users that have been granted access to a cloud app) can access cloud apps under specific conditions. In your response, you enforce additional requirements such as multi-factor authentication, use of a managed device, and others. In the context of Azure AD conditional access, the requirements your policy enforces are called access controls. In the most restrictive form, your policy can block access. For more information, see Access controls in Azure Active Directory conditional access.

The combination of conditions with your access controls represents a conditional access policy.



With Azure AD conditional access, you can control how authorized users can access your cloud apps. The objective of a conditional access policy is to enforce additional access controls on an access attempt to a cloud app that is driven by how an access attempt is performed.

One benefit of using a policy-based approach to protect access to your cloud apps is that you can start drafting the policy requirements for your environment using the structure outlined in this article without worrying about the technical implementation.

Authentication – Server to Server (S2S)

There are two scenarios where you may want to connect external Apps with Dynamics 365/Dataverse:

Scenario	Description
Multi-Tenant	This is the most common scenario and the one which is used for apps distributed using Microsoft AppSource. Each Dataverse tenant is associated with an Azure AD tenant. Your web application or service is registered with your Azure AD tenant. In this scenario any Dataverse tenant can potentially use your multi-tenant application after they grant consent for the application to access data in their tenant.
Single-Tenant	This scenario typically applies to Dataverse environments that want to develop apps for their own tenant and don't intend to distribute them to other Dataverse environments. An enterprise can create a web application or service to connect to all the environments for their tenant. In this scenario, your web application or service will only be able to connect to environment using the same Azure AD tenant.

Use server-to-server (S2S) authentication to securely and seamlessly communicate with Dataverse with your web applications and services. S2S authentication is the common way that apps registered on Microsoft AppSource use to access the Dataverse data of their subscribers.

S2S authentication means you don't need to use a paid user license when you connect to Dataverse environments. There is no license fee for the special ***application user*** account you will use with S2S authentication. With S2S authentication a special unlicensed application user account is created and includes information about your application registered with Azure Active Directory (Azure AD). Rather than user credentials, the application is authenticated based on a service principal identified by an Azure AD Object ID value which is stored in the application user record. The application user is associated with a custom security role which controls the kinds of data and operations the application is allowed to perform.

All operations performed by your application or service using S2S will be performed as the application user you provide rather than as the user who is accessing your application. If you want your application to perform data operations on behalf of a specific user, such as the one who is interacting with your application, you can apply impersonation when the custom security role applied to your application service principal has the privileges required. More information: Impersonate another user

A web application or service which uses S2S authentication is responsible for controlling access to the data that it has access to. This is typically done using an OpenID Connect provider. More information: http://openid.net/connect/.

Authorization

Introduction

Authorization refers to the mechanisms available inside Power Platform that allows you to control the functionality and data accessible to the users in your environment. You use the security model to protect the data integrity and privacy in Dataverse environment. The security model also promotes efficient data access and collaboration. The goals of the model are as follows:

- Provide a multi-tiered licensing model for users.
- Grant users access that allows only the levels of information required to do their jobs.
- Categorize users and teams by security role and restrict access based on those roles.
- Support data sharing so that users can be granted access to objects they do not own for a one-time collaborative effort.
- Prevent access to objects a user does not own or share.
- You combine business units, role-based security, record-based security, and field-based security to define the overall access to information that users have in your Microsoft Dynamics 365 organization.

Role-based security for simplified administration

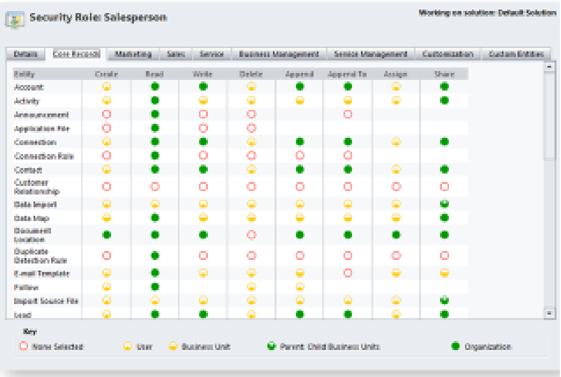
User or team level record ownership

Record sharing for collaboration

Field-level security for sensitive data

Business Unit Access

Management Hierarchy



Security Role: Salesperson

Working on solution: Default Solution

Entity	Create	Read	Write	Delete	Append	Append To	Assign	Share
Account	◔	●	●	◔	●	●	◔	●
Activity	◔	●	◑	◔	◑	◑	◔	●
Announcement	○	●	○	○		○		
Application File	○	●	○	○				
Connection	◔	●	●	◔	●	●	◔	●
Connection Role	○	●	○	○	○	○		
Contact	◔	●	●	◔	●	●	◔	●
Customer Relationship	○	○	○	○	○	○	○	○
Data Import	◔	◔	◔	◔	◔	◔	◔	◕
Data Map	◑	●	◑	◑	◑	◑	◑	●
Document Location	●	●	●	○	●	●	●	●
Duplicate Detection Rule	○	●	○	○	○	○	○	○
E-mail Template	◔	●	◔	◔	◑	○	◑	◑
Follow	◔	●		◔	◔			
Import Source File	◔	◔	◔	◔	◔	◔	◔	◕
Lead	◔	●	●	◔	●	●	◔	●

Key

○ None Selected ◔ User ◑ Business Unit ◕ Parent: Child Business Units ● Organization

Role-Based Security

The fundamental concept in role-based security is that a role contains privileges that define a set of actions that can be performed within the organization. For example, the salesperson role is assigned a set of privileges that are relevant to the tasks defined for that role. All users must be assigned to one or more predefined or custom roles. In an environment, roles can also be assigned to teams. When a user or team is assigned to one of these roles, the person or team members are assigned the set of privileges associated with that role. A user must be assigned to at least one role.

A privilege authorizes the user to perform a specific action on a specific entity type. Privileges apply to an entire class of objects, rather than individual instances of objects. For example, if a user does not have the privilege to read accounts, any attempt by that user to read an account will fail. A privilege contains an access level that determines the levels within the organization to which a privilege applies. Each privilege can have up to four access levels: Basic, Local, Deep, and Global.

Dynamics 365 includes fourteen predefined roles that reflect common user roles with access levels defined to match the security best-practice goal of providing access to the minimum amount of business data required for the job. With these roles you can quickly deploy a Dynamics 365 system without having to define your own roles. However, you can create custom roles using the predefined roles as a template, or you can define a new set of roles. For a list, see List of Predefined Security Roles.

Each role is associated with a set of privileges that determines the user or team's access to information within the company.

You can create, modify or remove custom roles to fit your business needs. The roles you create for your business unit are inherited by all the business units in the hierarchy.

You can assign one or more roles to a user or to a team. For example, a user can have the Sales Manager role in addition to being a Customer Service Representative, in which case that user has all the privileges of both roles.

You cannot modify privileges at the user level, but you can create a new role with the desired privileges. For example, John is given a Salesperson role, which requires him to accept all leads assigned to him. However, the administrator wants John to be able to reassign leads assigned to him. As a result, the administrator needs either modify the Salesperson role to allow this or create a new role that incorporates this specific privilege and add John to this role. Creating a new role is the recommended option unless you think it necessary that all users who are assigned the Salesperson role now have this additional privilege.

Privileges

There are over 580 privileges that are predefined system-wide during environment setup. A privilege is a permission to perform an action in an environment. Some privileges apply in general and some to a specific entity type.

Power Platform uses privileges as the core of the underlying security check. Privileges are "built in" to the product and are used throughout the application and platform layers. You cannot add or remove privileges or change how privileges are used to grant access to certain functionality, but you can construct new roles from the existing privilege set.

Each role defines a set of privileges that determines the user or team's access to information within the company. The platform checks for the privilege and rejects the operation if the user does not have the necessary privilege. A privilege is combined with a depth or access level.

For example, the Salesperson role could contain the privileges `Read Account` with `Basic` access and `Write Account` with `Basic` access, whereas the Sales Manager role might contain privileges like `Read Account` with `Local` access and `Assign Contact` with `Local` access.

Most entities have a set of possible privileges that can be added to a role that correspond to the various actions you can take on the records of that entity time.

Each action in the system, and each message described in the SDK documentation, requires one or more privileges to be present for the action to be performed.

Access Levels

The access level or privilege depth for a privilege determines, for a given entity type, at which levels within the organization hierarchy a user can act on that type of entity.

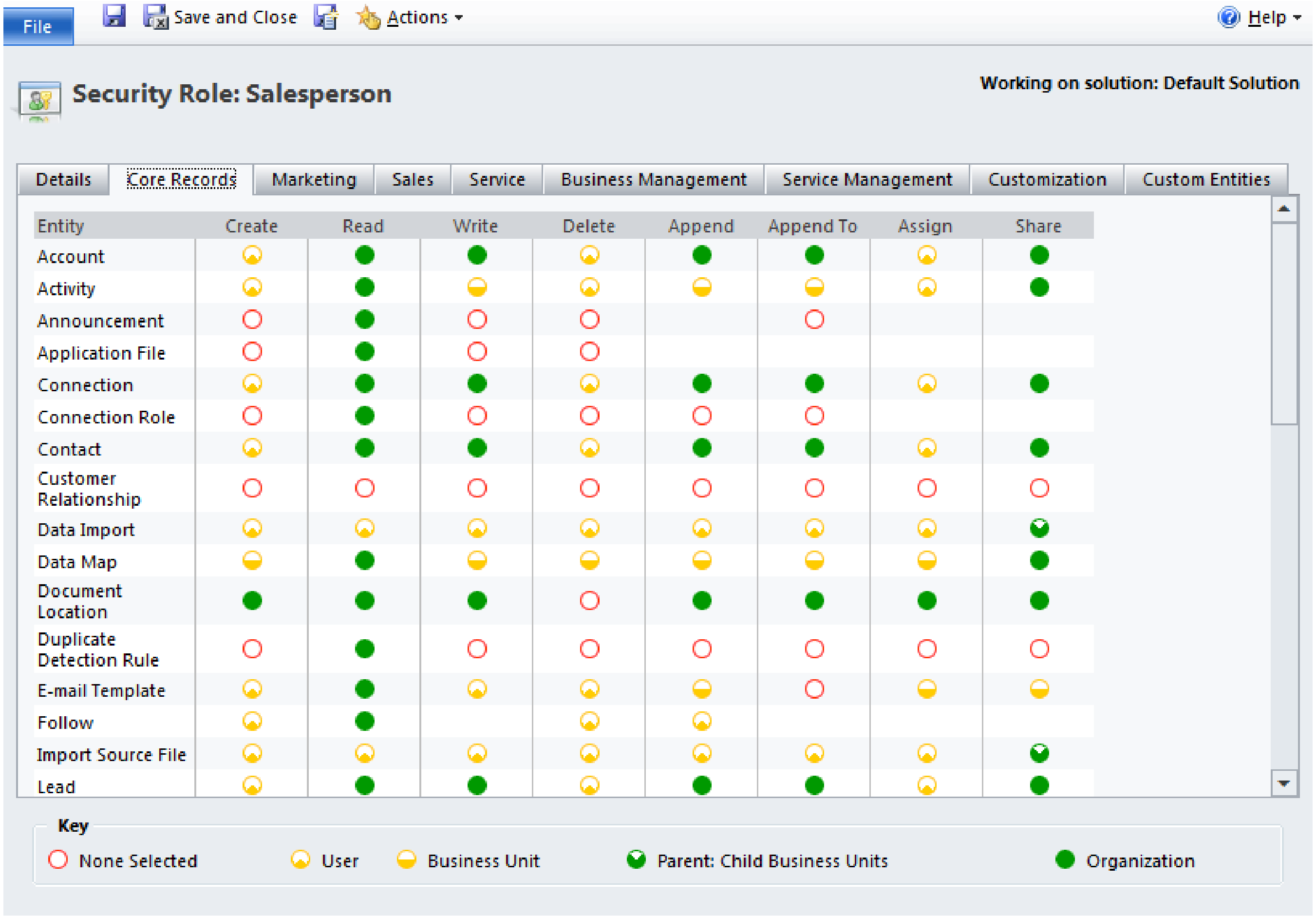
The following table lists the levels of access in Dynamics 365, starting with the most access. The icon is shown in the security role editor in the Web application.

●	**Global**. This access level gives a user access to all records within the organization, regardless of the business unit hierarchical level to which the instance or the user belongs. Users who have Global access automatically have Deep, Local, and Basic access, also. Because this access level gives access to information throughout the organization, it should be restricted to match the organization's data security plan. This level of access is usually reserved for managers with authority over the organization. The application refers to this access level as **Organization**.
◕	Deep. This access level gives a user access to records in the user's business unit and all business units subordinate to the user's business unit. Users who have Deep access automatically have Local and Basic access, also. Because this access level gives access to information throughout the business unit and subordinate business units, it should be restricted to match the organization's data security plan. This level of access is usually reserved for managers with authority over the business units. The application refers to this access level as **Parent: Child Business Units**.

◒	**Local**. This access level gives a user access to records in the user's business unit. Users who have Local access automatically have Basic access, also. Because this access level gives access to information throughout the business unit, it should be restricted to match the organization's data security plan. This level of access is usually reserved for managers with authority over the business unit. The application refers to this access level as **Business Unit**.
◔	**Basic**. This access level gives a user access to records he or she owns, objects that are shared with the user, and objects that are shared with a team of which the user is a member. This is the typical level of access for sales and service representatives. The application refers to this access level as **User**.
○	**None**. No access is allowed.

Putting it all together

- If a user has the `Deep Read Account` privilege, this user can read all accounts in his or her business unit, and all accounts in any child business unit of that business unit.
- If a user has `Local Read Account` privileges, this user can read all accounts in the local business unit.
- If a user is assigned the `Basic Read Account` privilege, this user can read only the accounts that he or she owns or the accounts that are shared with him or her.
- A customer service representative with the `Basic Read Account` privilege can view accounts that he or she owns and any accounts another user has shared with this user. This makes it possible for the representative to read the account data that is relevant to a service request, but not to change the data.
- A data analyst with the `Local Read Account` privilege can view account data and run account-related reports for all accounts in his or her business unit.
- A finance officer for the company with the `Deep Read Account` privilege can view account data and run account-related reports for all accounts in his or her business unit and accounts in any child business unit.



Security Role: Salesperson

Working on solution: Default Solution

Entity	Create	Read	Write	Delete	Append	Append To	Assign	Share
Account	◔	●	●	◔	●	●	◔	●
Activity	◔	●	◒	◔	◒	◒	◔	●
Announcement	○	●	○	○		○		
Application File	○	●	○	○				
Connection	◔	●	●	◔	●	●	◔	●
Connection Role	○	●	○	○	○	○		
Contact	◔	●	●	◔	●	●	◔	●
Customer Relationship	○	○	○	○	○	○	○	○
Data Import	◔	◔	◔	◔	◔	◔	◔	◕
Data Map	◒	●	◒	◒	◒	◒	◒	●
Document Location	●	●	●	○	●	●	●	●
Duplicate Detection Rule	○	●	○	○	○	○	○	○
E-mail Template	◔	●	◔	◔	◒	○	◒	◒
Follow	◔	●		◔	◔			
Import Source File	◔	◔	◔	◔	◔	◔	◔	◕
Lead	◔	●	●	◔	●	●	◔	●

Key

○ None Selected ◔ User ◒ Business Unit ◕ Parent: Child Business Units ● Organization

Use Record-Based Security to Control Access to Records

Record-based security applies to individual records. It is provided by using access rights.

The relationship between an access right and a privilege is that access rights apply only after privileges have taken effect. For example, if a user does not have the *privilege* to read accounts, that user is unable to read any account, regardless of the *access rights* another user might grant to a specific record through sharing.

An access right is granted to a user for a particular record. The following table lists the descriptions for these access rights.

Access right	Description
Read	Controls whether the user can read a record.
Write	Controls whether the user can update a record.
Assign	Controls whether the user can assign a record to another user.
Append	Controls whether the user can attach another record to the specified record. The Append and Append To access rights work in combination. Every time that a user attaches one record to another, the user must have both rights. For example, when you attach a note to a case, you must have the Append To Access right on the note and the Append access right on the case for the operation to work.

Append To	Controls whether the user can append the record in question to another record. The Append and Append To access rights work in combination. For more information, see the description for Append.
Share	Controls whether the user can share a record with another user or team. Sharing gives another user access to a record. For more information, see Sharing Records.
Delete	Controls whether the user can delete a record.

The right to create a record for an entity type is not included in the previous table because this right does not apply to an individual record, but instead to a class of entities. Create is handled as a privilege instead of as an access right. The user who creates a record has all rights on that record, unless his or her other privileges forbid a specific right.

Sharing records

Sharing lets users give other users or teams access to specific customer information. This is useful for sharing information with users in roles that have only the Basic access level. For example, in an organization that gives salespeople Basic read and write access to accounts, a salesperson can share an opportunity with another salesperson so that they can both track the progress of an important sale.

For security reasons, develop the practice of sharing only the necessary records with the smallest set of users possible. Only grant the minimum access required for users to do their jobs.

Dynamics 365 provides the following sharing capabilities:

- **Share**. Any user who has share privileges on a given entity type can share records of that type with any other user or team in Dynamics 365. To share a record, use GrantAccessRequest.
- When you share a record with another user, indicate what access rights (Read, Write, Delete, Append, Assign, and Share) you want to grant to the other user. Access rights on a shared record can be different for each user with whom the record is shared. However, you cannot give a user any rights that he or she would not have for that type of entity, based on the role assigned to that user. For example, if a user does not have Read privileges on accounts and you share an account with that user, the user will be unable to see that account.
- **Modify share**. You can modify the rights granted to a shared record after it has been shared. To modify sharing for a record, use the ModifyAccessRequest.
- **Remove share**. If you share a record with another user or team, you can stop sharing the record. After you remove sharing for a record, the other user or team loses access rights to the record. To remove sharing for a record, use the RevokeAccessRequest.

A user might have access to the same record in more than one context. For example, a user might share a record directly with specific access rights, and he or she might also be on a team in which the same record is shared with different access rights. In this case, the access rights that this user has on the record are the union of all the rights.

For a list of entities that support sharing, see the GrantAccessRequest.

Sharing and Inheritance

If a record is created and the parent record has certain sharing properties, the new record inherits those properties. For example, Joe and Mike are working on a high priority lead. Joe creates a new lead and two activities, shares the lead with Mike, and selects cascade sharing. Mike makes a telephone call and sends an email regarding the new lead. Joe sees that Mike has contacted the company two times, so he does not make another call.

Sharing is maintained on individual records. A record inherits the sharing properties from its parent and also maintains its own sharing properties. Therefore, a record can have two sets of sharing properties—one that it has on its own and one that it inherits from its parent.

Removing the share of a parent record removes the sharing properties of objects (records) that it inherited from the parent. That is, all users who previously had visibility into this record no longer have visibility. Child objects still could be shared to some of these users if they were shared individually, not from the parent record.

Assigning Records

Anyone with Assign privileges on a record can assign that record to another user. When a record is assigned, the new user or team becomes the owner of the record and its related records. The original user or team loses ownership of the record, but automatically shares it with the new owner.

In Dynamics 365, the system administrator can decide for an organization whether records should be shared with previous owners or not after the assign operation. If **Share with previous owner** is selected, then the previous owner shares the record with all access rights after the assign operation. Otherwise, the previous owner does not share the record and may not have access to the record, depending on his or her privileges. The `Organization.ShareRoPreviousOwnerOnAssign` attribute controls this setting.

For a list of entities that support Assign, see the AssignRequest.

Dependencies between access rights

Sometimes, security dependencies exist because it is necessary to have more than one access right to perform a given action. For example, if you have the **create** access right for accounts, you can create a record of the account entity type. However, unless you also have **read** access for accounts, you cannot create an account record and be the owner of that new record. The following table lists the access right dependencies for the actions specified.

Action	Access rights required
To **Create** a record and be the record owner	CREATE READ
To **Share** a record	SHARE. This right is required by the person doing the share operation. READ. This right is required by the person doing the share operation and also by the person with whom the record is being shared.
To **Assign** a record	ASSIGN WRITE READ
To **Append To** a record	READ APPENDTO
To **Append** a record	READ APPEND

Another type of dependency exists when objects are subordinate to another object. For example, the opportunity object cannot exist on its own. Each opportunity is always attached to an account or contact. To create an opportunity, you must have the access right **appendto** on accounts and the access right **append** on opportunities.

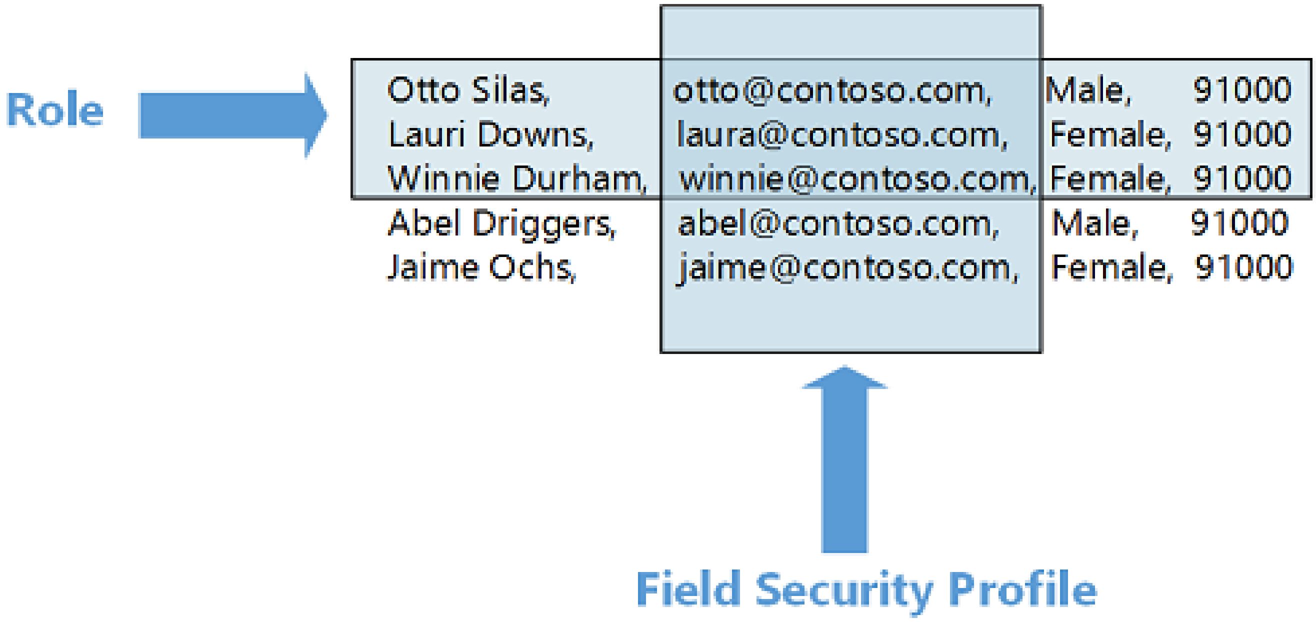
Use Field Security to Control Access to Field Values

You can use field-level security to restrict access to high business impact fields to specific users and teams. For example, you use this to enable only certain users to read or update the credit score for a customer. For this release, field-level security can be applied to both custom fields and many out-of-box (OOB) fields.

The following steps describe how to restrict access to a field:

1. Enable field-level security for an attribute
2. Create a field-level security profile
3. Associate users or teams with the profile
4. Add specific field permissions, such as Create, Update or Read for a specific attribute to the profile

The following diagram shows the interaction between role-based security, record-based security, and field-level security.



Otto Silas,	otto@contoso.com,	Male,	91000
Lauri Downs,	laura@contoso.com,	Female,	91000
Winnie Durham,	winnie@contoso.com,	Female,	91000
Abel Driggers,	abel@contoso.com,	Male,	91000
Jaime Ochs,	jaime@contoso.com,	Female,	91000

Role-based security lets you see a specific entity type, record-based security lets you see individual records, and field-level security lets you see specific fields.

Hierarchical Security

Hierarchy security offers a more granular access to records for an organization and helps to bring the maintenance costs down. For example, in complex scenarios, you can start with creating several business units and then add the hierarchy security. This will achieve a more granular access to data with far less maintenance costs that a large number of business units may require. The hierarchy security model is an extension to the earlier security models that use business units, security roles, sharing, and teams. It can be used in conjunction with all other existing security models.

Previously, implementing this kind of security often required developers to mimic this behavior using custom plug-ins. Now, with the hierarchy security model, that type of security is built into the product. This removes the need to create and update custom plug-ins.

Two security models can be used for hierarchies, the Manager hierarchy and the Position hierarchy. With the Manager hierarchy, a manager must be within the same business unit as the report, or in the parent business unit of the report's business unit, to have access to the report's data. The Position hierarchy allows data access across business units. If you are a financial organization, you may prefer the Manager hierarchy model, to prevent managers' accessing data outside of their business units. However, if you are a part of a customer service organization and want the managers to access service cases handled in different business units, the Position hierarchy may work better for you.

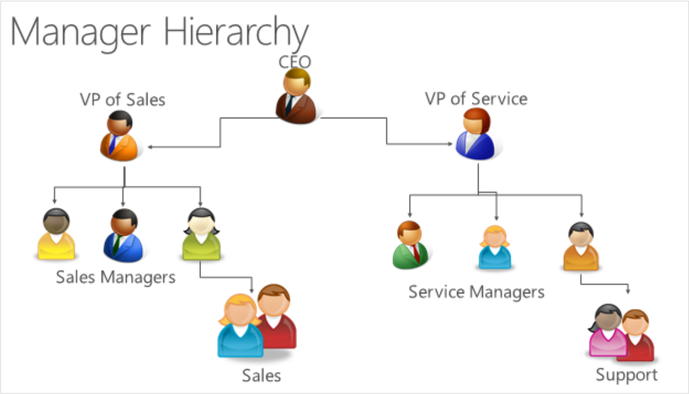
Manager Hierarchy

The Manager hierarchy security model is based on the management chain or direct reporting structure, where the manager's and the report's relationship are established by using the Manager field on the system user entity. With this security model, the managers are able to access the data that their reports have access to. They are able to perform work on behalf of their direct reports or access information that needs approval.

With the Manager hierarchy security model, a manager has access to the records owned by the user or by the team that a user is a member of, and to the records that are directly shared with the user or the team that a user is a member of.

In addition to the Manager hierarchy security model, a manager must have at least the user level Read privilege on an entity, to see the reports' data. For example, if a manager doesn't have the Read access to the Case entity, the manager won't be able to see the cases that their reports have access to.

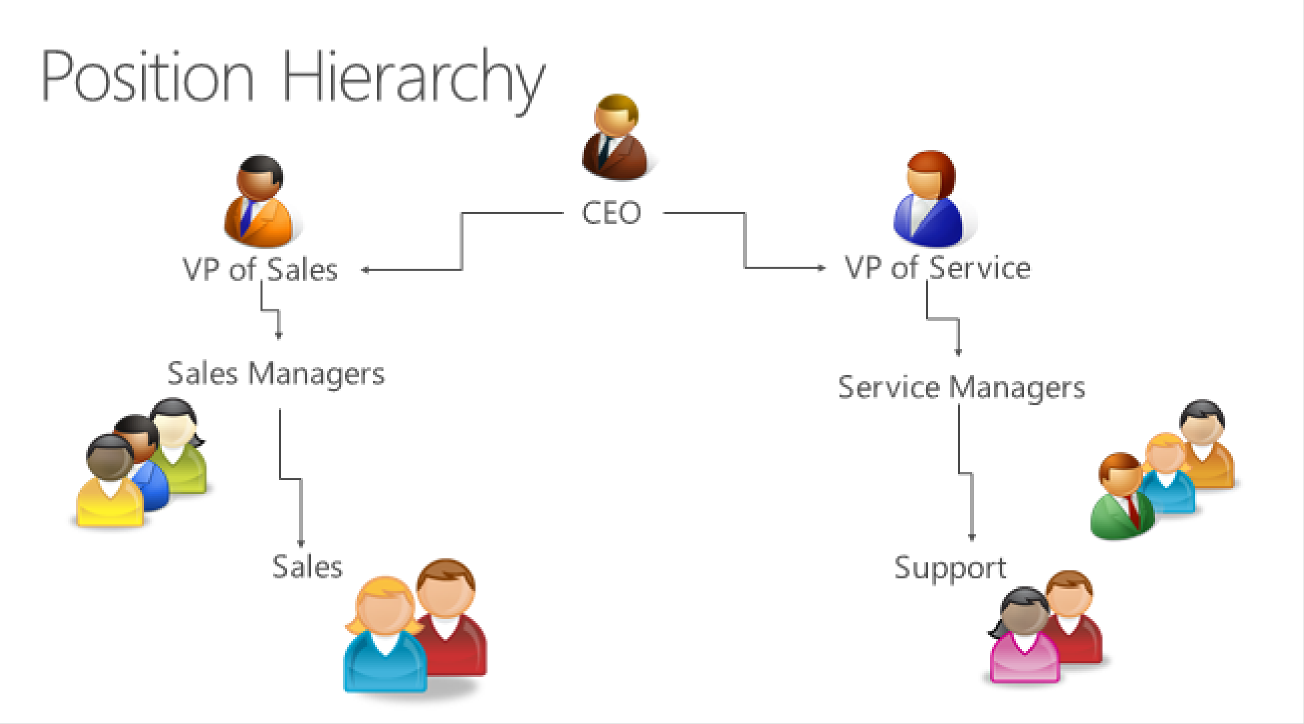
For a non-direct report, a manager has the Read-only access to the report's data. For a direct report, the manager has the Read, Write, Update, Append, AppendTo access to the report's data. To illustrate the Manager hierarchy security model, let's take a look at the diagram below. The CEO can read or update the VP of Sales data and the VP of Service data. However, the CEO can only read the Sales Manager data and the Service Manager data, as well as the Sales and Support data. You can further limit the amount of data accessible by a manager with "Depth". Depth is used to limit how many levels deep a manager has Read-only access to the data of their reports. For example, if the depth is set to 2, the CEO can see the data of the VP of Sales, VP of Service and Sales and Service Managers. However, the CEO doesn't see the Sales data or the Support data.



Position Hierarchy

The Position hierarchy is not based on the direct reporting structure, like the Manager hierarchy. A user doesn't have to be an actual manager of another user to access user's data. As an administrator, you will define various job positions in the organization and arrange them in the Position hierarchy. Then, you add users to any given position, or, as we also say, "tag" a user with a particular position. A user can be tagged only with one position in a given hierarchy, however, a position can be used for multiple users. Users at the higher positions in the hierarchy have access to the data of the users at the lower positions, in the direct ancestor path. The direct higher positions have Read, Write, Update, Append, AppendTo access to the lower positions' data in the direct ancestor path. The non-direct higher positions, have Read-only access to the lower positions' data in the direct ancestor path.

To illustrate the concept of the direct ancestor path, let's look at the diagram below. The Sales Manager position has access to the Sales data, however, it doesn't have access to the Support data, which is in the different ancestor path. The same is true for the Service Manager position. It doesn't have access to the Sales data, which is in the Sales path. Like in the Manager hierarchy, you can limit the amount of data accessible by higher positions with "Depth". The depth will limit how many levels deep a higher position has a Read-only access, to the data of the lower positions in the direct ancestor path. For example, if the depth is set to 3, the CEO position can see the data all the way down from the VP of Sales and VP of Service positions, to the Sales and Support positions.



Access Teams and Owner Teams

With *owner* teams or *access* teams, you can easily share business objects and collaborate with the users across business units in Dynamics 365. A team belongs to one business unit, but it can include users from other business units. A user can be associated with more than one team.

An owner team owns records and has security roles assigned to the team. The team's privileges are defined by these security roles. In addition to privileges provided by the team, team members have the privileges defined by their individual security roles and by the roles from other teams in which they are members. A team has full access rights on the records that the team owns.

While teams provide access to a group of users, you must still associate individual users with security roles that grant the privileges they need to create, update, or delete user-owned records. These privileges cannot be applied by assigning security roles to a team and then adding the user to that team.

An access team doesn't own records and doesn't have security roles assigned to the team. The team members have privileges defined by their individual security roles and by roles from the teams in which they are members. The records are shared with an access team and the team is granted access rights on the records, such as Read, Write or Append.

Owner team or access team?

Choosing the type of the team may depend on the goals, nature of the project, and even the size of your organization. There are a few guidelines that you can use when choosing the team type.

When to use owner teams	• Owning records by entities other than users is required by your company's business policies. • The number of teams is known at the design time of your Dynamics 365 system. • Daily reporting on progress by owning teams is required.
When to use access teams	• The teams are dynamically formed and dissolved. This typically happens if the clear criteria for defining the teams, such as established territory, product, or volume aren't provided. • The number of teams isn't known at the design time of your Dynamics 365 system. • The team members require different access rights on the records. You can share a record with several access teams, each team providing different access rights on the record. For example, one team is granted the Read access right on the account and another team, the Read, Write and Share access rights on the same account. • A unique set of users requires access to a single record without having an ownership of the record.

Service Administrator roles

There are two dedicated administrative roles present in Azure Active Directory – Dynamics 365 Service Admin and Power Platform Service Admin. These roles are meant to be assigned to administrators that are taking care of environment administration, including backup/restore, turning on the Release Previews as well as handling and logging support tickets.

The Dynamics 365 Service Administrator can sign in to and manage multiple environments. If an environment uses a security group, a service admin would need to be added to the security group to manage that environment. Not assigning to an in-place security group essentially locks these admins out of any admin management.

Users with the Power Platform service admin role can sign in to and manage multiple environments. Power Platform admins are not limited by security group membership and can manage environments even if not added to an environment's security group.

Assigning these roles to users grants System Administrator role in the environment itself, so they have full access to all the organizational data. For this reason, it is recommended to use the Administrative roles with care and only on need to basis.

	Power Platform Service admin	Dynamics 365 Service admin[1]
POWER PLATFORM		
Environments		
Full access	✓	✓
Create	✓	✓
Backup and restore	✓	✓
Copy	✓	✓
Ability to exclude access from selected environments	✗	✓
Analytics		
Capacity	✓	✓
Capacity allocation	✓	✓
Dataverse	✓	✓
Power Automate	✓	✓
Power Apps	✓	✓
Help + support	✓	
Create and access support requests	✓	✓

Data integration		
Create new project and connection set	✓	✓
Data gateways		
View gateways	✓	✓
Data policies		
View and manage tenant policies	✓	✓
View and manage environment policies	✓	✓
POWER BI		
Manage the Power BI tenant	✓	✗
Acquire and assign Power BI licenses	✗	✗
MICROSOFT 365		
Create users	✗	✗
Add security roles	✗	✗
Add licenses	✗	✗

[1] If a security group is assigned to the environment and the user with this role belongs to this security group

Source: https://docs.microsoft.com/en-us/power-platform/admin/use-service-admin-role-manage-tenant

Database access for Customer support and troubleshooting issues

In an event that an engineering or support staff needs access to customer data for support purpose, secured and just-in-time (JIT) access is granted to the staff member. Access to customer data is restricted:

- No one in Microsoft has standing access to any customer data.
- Only if customer provides explicit consent Microsoft Support can access data
- Access to customer data by Microsoft support will be:
  - Time restricted – environment expires 7 days after creation or after resolution of the problem1
  - Limited to authorized support personnel
  - Performed from a secure admin workstation
  - Audited
  - Subject to further internal Microsoft approval if access is required to the database

When Microsoft investigate a ticket raised by customer, it may need access to a copy of the environment in order to investigate. Such as copy is called a 'support environment'. There are two types of support environments:

1. A minimal copy – this is a copy of the application (metadata) only and does not contain customer data
2. A full copy – this is a copy of the application including all customer data. Requests for a full copy requested only if the actual data is needed for troubleshooting

Access control to the support *full and minimal copy* environments is based on the following principles:

a) Customer controls the creation *and* deletion of the full environment copy

b) All support environments are created in the customer's tenant

c) Only authorized Microsoft Support personnel have access to the support environment (by default only through the User Interface) as System Administrator

d) Microsoft Support can request access to the support environment database

   – It is subject to approval within Microsoft, and is restricted to those within an elevated support security group

   – Access to the database can be gained from a Secure Admin Workstation (SAW) only

Where remediation of the issue requires executive action, this can be applied by Microsoft Support based on the following principles:

a) The fix can be applied only from a Secure Admin Workstation

b) The executive action needs to be approved within the Microsoft support organization

c) The executive action must be selected from pre-approved and validated actions

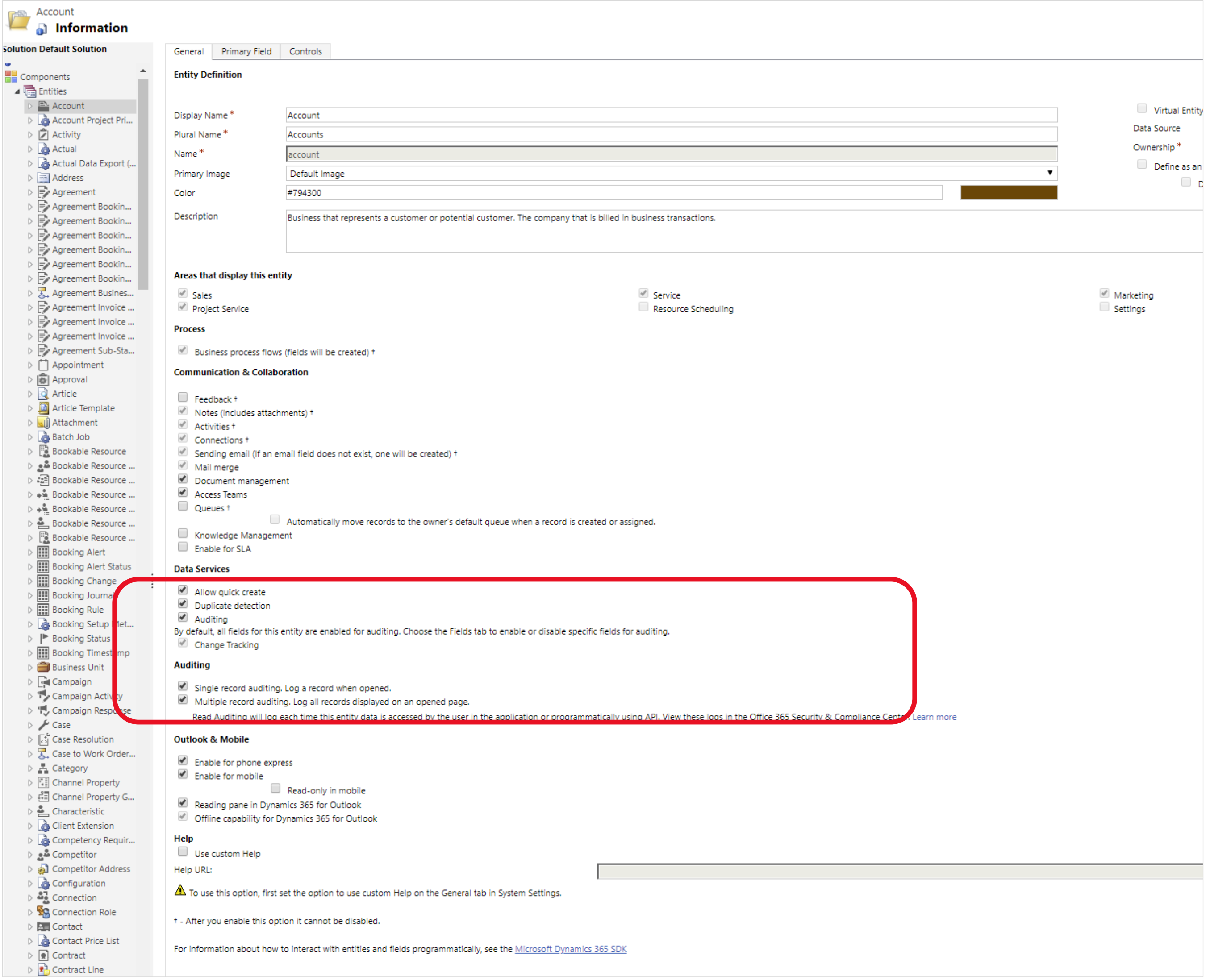
d) Performing the executive action does not expose customer data

e) All actions from the Secure Admin Workstations are recorded

Where Microsoft Support is not able to remediate the issue and this requires escalation to the Engineering or D365 Operations Centre the same principles as above apply however authorized product group personnel can eventually access the production database if needed.

Audit logs

Audit logs are provided to ensure the data integrity of the system. Audit logs are also available to meet certain security and compliance requirements. Administrators can enable auditing at an entity level.



Account
Information

Solution Default Solution

- Components
  - Entities
    - Account
    - Account Project Pri...
    - Activity
    - Actual
    - Actual Data Export (...
    - Address
    - Agreement
    - Agreement Bookin...
    - Agreement Bookin...
    - Agreement Bookin...
    - Agreement Bookin...
    - Agreement Bookin...
    - Agreement Bookin...
    - Agreement Busines...
    - Agreement Invoice ...
    - Agreement Invoice ...
    - Agreement Invoice ...
    - Agreement Sub-Sta...
    - Appointment
    - Approval
    - Article
    - Article Template
    - Attachment
    - Batch Job
    - Bookable Resource
    - Bookable Resource ...
    - Bookable Resource ...
    - Bookable Resource ...
    - Bookable Resource ...
    - Bookable Resource ...
    - Bookable Resource ...
    - Booking Alert
    - Booking Alert Status
    - Booking Change
    - Booking Journa
    - Booking Rule
    - Booking Setup let...
    - Booking Status
    - Booking Timest mp
    - Business Unit
    - Campaign
    - Campaign Acti y
    - Campaign Resp se
    - Case
    - Case Resolution
    - Case to Work Order...
    - Category
    - Channel Property
    - Channel Property G...
    - Characteristic
    - Client Extension
    - Competency Requir...
    - Competitor
    - Competitor Address
    - Configuration
    - Connection
    - Connection Role
    - Contact
    - Contact Price List
    - Contract
    - Contract Line

Entity Definition

Display Name *	Account	□ Virtual Entity
Plural Name *	Accounts	Data Source
Name *	account	Ownership *
Primary Image	Default Image ▾	□ Define as an
Color	#794300 ▇	□ D
Description	Business that represents a customer or potential customer. The company that is billed in business transactions.	

Areas that display this entity

☑ Sales
☑ Project Service
☑ Service
□ Resource Scheduling
☑ Marketing
□ Settings

Process

☑ Business process flows (fields will be created) †

Communication & Collaboration

□ Feedback †
☑ Notes (includes attachments) †
☑ Activities †
☑ Connections †
☑ Sending email (If an email field does not exist, one will be created) †
☑ Mail merge
☑ Document management
☑ Access Teams
□ Queues †
□ Automatically move records to the owner's default queue when a record is created or assigned.
□ Knowledge Management
□ Enable for SLA

Data Services

☑ Allow quick create
☑ Duplicate detection
☑ Auditing
By default, all fields for this entity are enabled for auditing. Choose the Fields tab to enable or disable specific fields for auditing.
☑ Change Tracking

Auditing

☑ Single record auditing. Log a record when opened.
☑ Multiple record auditing. Log all records displayed on an opened page.
Read Auditing will log each time this entity data is accessed by the user in the application or programmatically using API. View these logs in the Office 365 Security & Compliance Cent . Learn more

Outlook & Mobile

☑ Enable for phone express
☑ Enable for mobile
□ Read-only in mobile
☑ Reading pane in Dynamics 365 for Outlook
☑ Offline capability for Dynamics 365 for Outlook

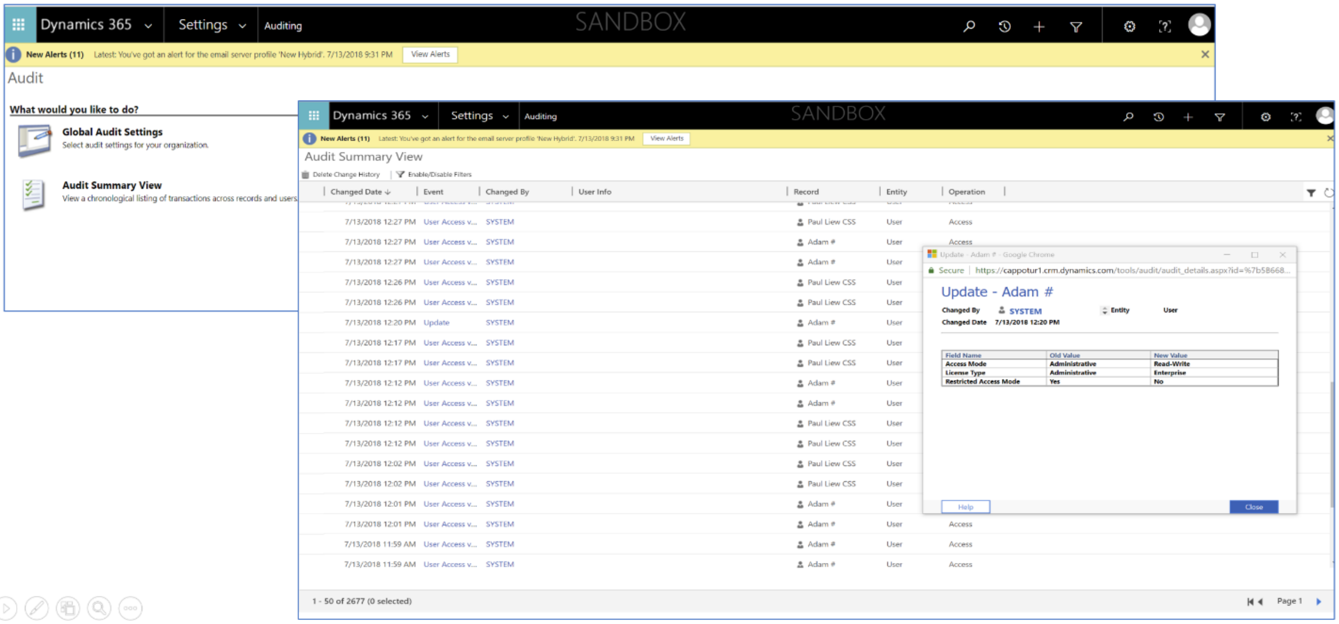
Help

□ Use custom Help
Help URL:
⚠ To use this option, first set the option to use custom Help on the General tab in System Settings.

† - After you enable this option it cannot be disabled.

For information about how to interact with entities and fields programmatically, see the Microsoft Dynamics 365 SDK

Audit logs can be accessed via the Web client in Dynamics 365.



Dynamics 365 | Settings | Auditing | SANDBOX

New Alerts (11) Latest: You've got an alert for the email server profile 'New Hybrid'. 7/13/2018 9:31 PM View Alerts

Audit

What would you like to do?

Global Audit Settings
Select audit settings for your organization.

Audit Summary View
View a chronological listing of transactions across records and users

Audit Summary View

Delete Change History | Enable/Disable Filters

Changed Date ↓	Event	Changed By	User Info	Record	Entity	Operation
7/13/2018 12:27 PM	User Access v...	SYSTEM		Paul Liew CSS	User	Access
7/13/2018 12:27 PM	User Access v...	SYSTEM		Adam #	User	Access
7/13/2018 12:27 PM	User Access v...	SYSTEM		Adam #	User	
7/13/2018 12:26 PM	User Access v...	SYSTEM		Paul Liew CSS	User	
7/13/2018 12:26 PM	User Access v...	SYSTEM		Paul Liew CSS	User	
7/13/2018 12:20 PM	Update	SYSTEM		Adam #	User	
7/13/2018 12:17 PM	User Access v...	SYSTEM		Paul Liew CSS	User	
7/13/2018 12:17 PM	User Access v...	SYSTEM		Paul Liew CSS	User	
7/13/2018 12:12 PM	User Access v...	SYSTEM		Adam #	User	
7/13/2018 12:12 PM	User Access v...	SYSTEM		Adam #	User	
7/13/2018 12:12 PM	User Access v...	SYSTEM		Paul Liew CSS	User	
7/13/2018 12:12 PM	User Access v...	SYSTEM		Paul Liew CSS	User	
7/13/2018 12:02 PM	User Access v...	SYSTEM		Paul Liew CSS	User	
7/13/2018 12:02 PM	User Access v...	SYSTEM		Paul Liew CSS	User	
7/13/2018 12:01 PM	User Access v...	SYSTEM		Adam #	User	
7/13/2018 12:01 PM	User Access v...	SYSTEM		Adam #	User	Access
7/13/2018 11:59 AM	User Access v...	SYSTEM		Adam #	User	Access
7/13/2018 11:59 AM	User Access v...	SYSTEM		Adam #	User	Access

1 - 50 of 2677 (0 selected) Page 1

Update - Adam # - Google Chrome

Secure | https://cappotur1.crm.dynamics.com/tools/audit/audit_details.aspx?id=%7b58668...

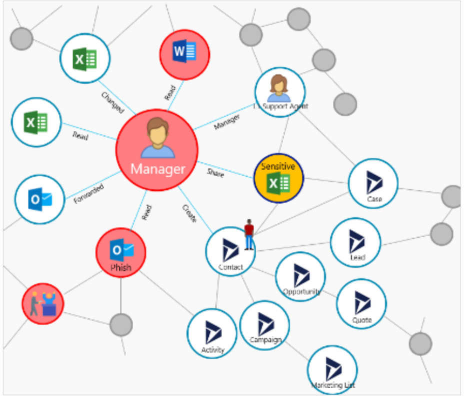
Update - Adam #

Changed By SYSTEM Entity User
Changed Date 7/13/2018 12:20 PM

Field Name	Old Value	New Value
Access Mode	Administrative	Read-Write
License Type	Administrative	Enterprise
Restricted Access Mode	Yes	No

Help Close

Activity Logging



Activity Logging logs user and admin activities across Dynamics 365 and Power Platform:

- **Management in a central location on the portal:** Administrators can now manage settings and activity reporting for all environments within the "Security & Compliance Center" Previously, Audit Logging was set up separately within each environment.
- **All data in the system is now logged:** All data transactions including plugin operations, entity operations, bulk operations, user login/out sessions, and even Microsoft Support Personnel operations are logged by this new functionality.
- **Configurable Alert Policies:** The system can now be set up to notify administrators or Compliance Officers of certain events, according to configurable settings.
- **Audit Log Search capability:** Administrators can now easily query audit logs via predefined or custom filters.
- **Analyze suspicious behavior with Security Information and Event Management (SIEM):** Functioning in near real-time, the SIEM will work to analyze and alert administrators of possible suspicious behavior within the system and provide actions to address these events.
- **SIEM Vendor Integration:** Dynamics 365 now provides out-of-box integration with multiple SIEM vendors such as ArcLight, Microsoft OMS, Okta, SumoLogic, BetterCloud, and standard CEF format integration for many others.
- **Minimized impact to system performance:** This new Activity Logging Management functionality has a smaller footprint on system resources compared to the previous Audit Log functionality.

When audit log search in the Office 365 Security and Compliance Center is turned on, user and admin activity from your organization is recorded in the audit log and retained for 90 days. However, your organization might not want to record and retain audit log data. Or you might be using a third-party security information and event management (SIEM) application to access your auditing data. In those cases, a global admin can turn off audit log search in Office 365.

The following is a partial extract of admin and user events you can audit.

Admin-related events

Event	Description
Publishing customizations	An admin publishes a new customization which overrides a change done by the previous one. The action requires auditing for analysis.
Attribute deletes	Admin accidentally deletes an attribute. This action also deletes the data.
Team, user management	Who was added, who was deleted, what access rights a user/team had is important for analyzing impact.
Configure instance	Adding solutions to an instance.
Backup and restore	Backup and restore actions at the tenant.
Manage applications	New instance added, existing instance deleted, trials converted to paid, etc.

User and support-related events

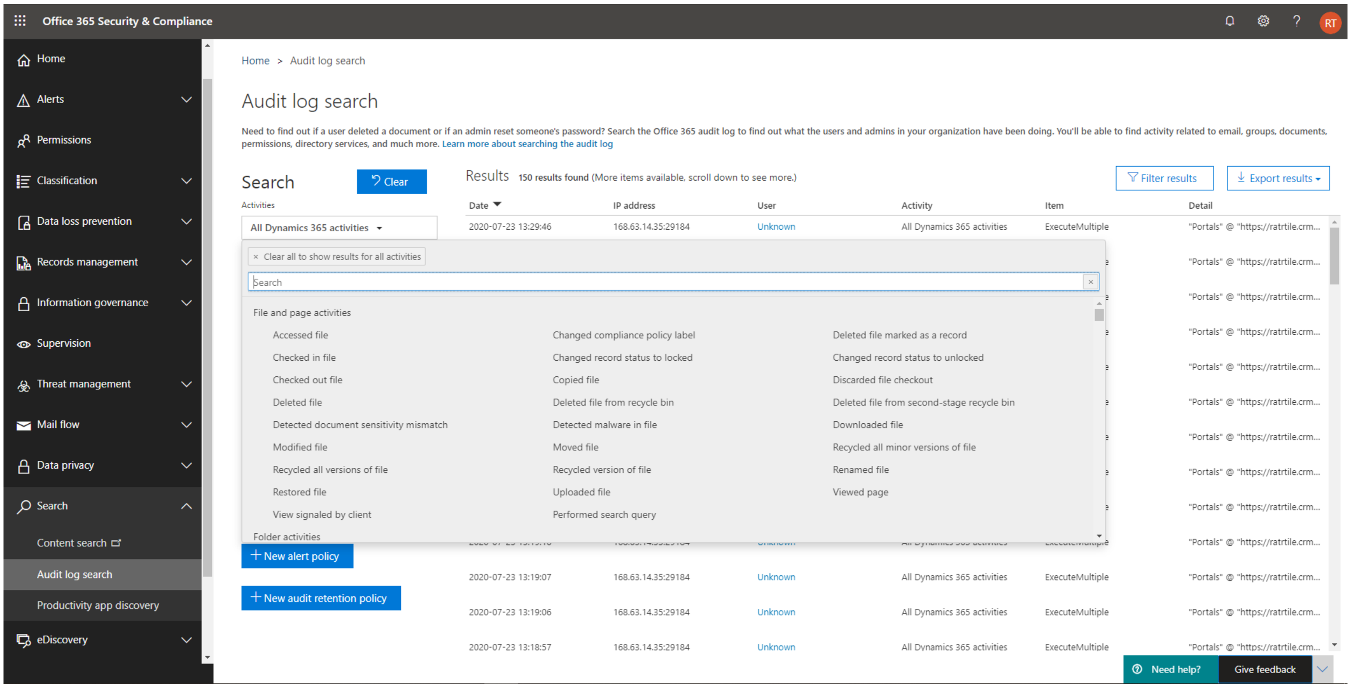
Event	Description
Create, read, update, delete (CRUD)	Logging all CRUD activities essential for understanding the impact of a problem and being compliant with data protection impact assessments (DPIA).
Multiple record view	Users of Dynamics view information in bulk, like grid views, Advanced Find search, etc. Critical customer content information is part of these views.
Export to Excel	Exporting data to Excel moves the data outside of the secure environment and is vulnerable to threats.
SDK calls via surround or custom apps	Actions taken via the core platform or surround apps calling into the SDK to perform an action needs to be logged.
All support CRUD activities	Microsoft support engineer activities on customer environment.
Admin activities	Admin activities on customer tenant.
Backend commands	Microsoft support engineer activities on customer tenant and environment.
Report Viewed	Logging when a report is viewed. Critical customer content information might be displayed on the report.
Report Viewer Export	Exporting a report to different formats moves the data outside of the secure environment and is vulnerable to threats.
Report Viewer Render Image	Logging multimedia assets that are shown when a report is displayed. They might contain critical customer information.

For a list of what's logged with Activity Logging, see Microsoft.Crm.Sdk.Messages Namespace.

We log all Dynamics 365 SDK messages except the following:

- WhoAmI
- RetrieveFilteredForms
- TriggerServiceEndpointCheck
- QueryExpressionToFetchXml
- FetchXmlToQueryExpression
- FireNotificationEvent
- RetrieveMetadataChanges
- RetrieveEntityChanges
- RetrieveProvisionedLanguagePackVersion
- RetrieveInstalledLanguagePackVersion
- RetrieveProvisionedLanguages
- RetrieveAvailableLanguages
- RetrieveDeprovisionedLanguages
- RetrieveInstalledLanguagePacks
- GetAllTimeZonesWithDisplayName
- GetTimeZoneCodeByLocalizedName
- IsReportingDataConnectorInstalled
- LocalTimeFromUtcTime
- IsBackOfficeInstalled
- FormatAddress
- IsSupportUserRole
- IsComponentCustomizable
- ConfigureReportingDataConnector
- CheckClientCompatibility
- RetrieveAttribute

Activity logs can be filtered by different services; e.g., Dynamics 365:



Audit log search

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. Learn more about searching the audit log

Search

Activities: All Dynamics 365 activities

× Clear all to show results for all activities

Search

File and page activities

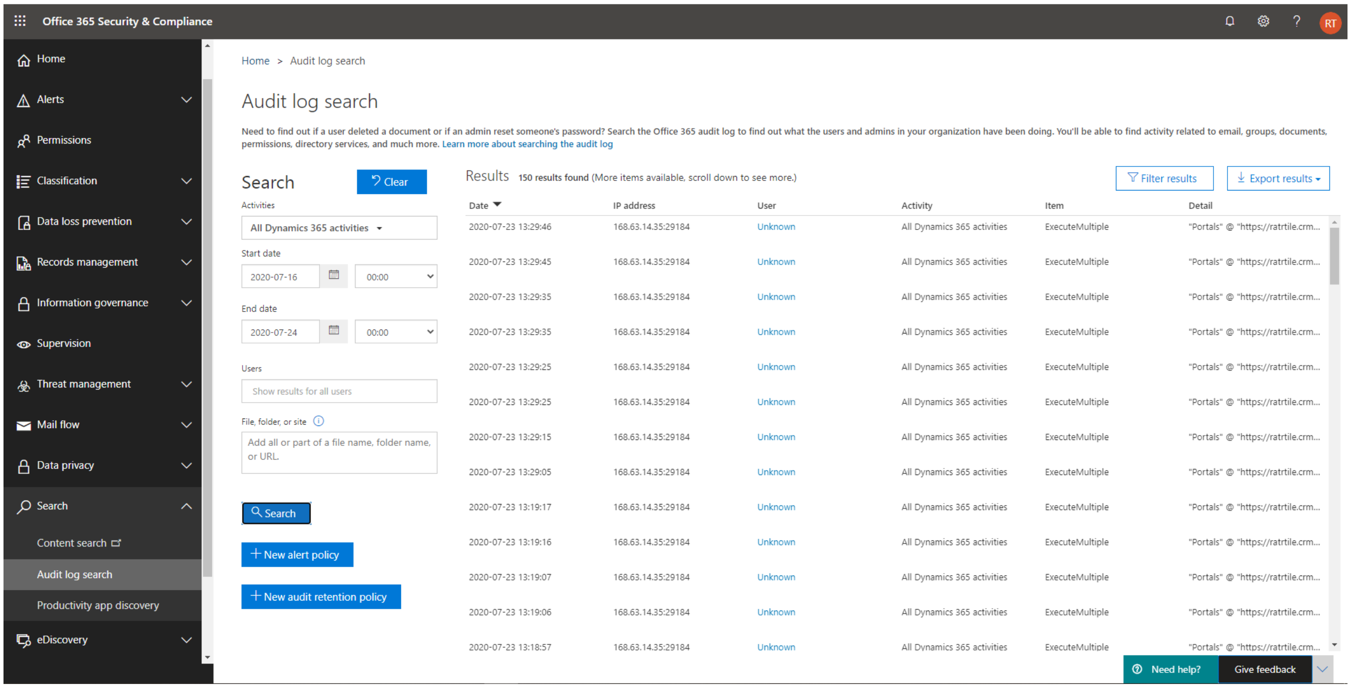
Accessed file	Changed compliance policy label	Deleted file marked as a record
Checked in file	Changed record status to locked	Changed record status to unlocked
Checked out file	Copied file	Discarded file checkout
Deleted file	Deleted file from recycle bin	Deleted file from second-stage recycle bin
Detected document sensitivity mismatch	Detected malware in file	Downloaded file
Modified file	Moved file	Recycled all minor versions of file
Recycled all versions of file	Recycled version of file	Renamed file
Restored file	Uploaded file	Viewed page
View signaled by client	Performed search query	

Folder activities

Results 150 results found (More items available, scroll down to see more.)

Date	IP address	User	Activity	Item	Detail
2020-07-23 13:29:46	168.63.14.35:29184	Unknown	All Dynamics 365 activities	ExecuteMultiple	"Portals" @ "https://ratrtile.crm...
					"Portals" @ "https://ratrtile.crm...
					"Portals" @ "https://ratrtile.crm...
					"Portals" @ "https://ratrtile.crm...
					"Portals" @ "https://ratrtile.crm...
					"Portals" @ "https://ratrtile.crm...
					"Portals" @ "https://ratrtile.crm...
					"Portals" @ "https://ratrtile.crm...
					"Portals" @ "https://ratrtile.crm...
					"Portals" @ "https://ratrtile.crm...
2020-07-23 13:19:07	168.63.14.35:29184	Unknown	All Dynamics 365 activities	ExecuteMultiple	"Portals" @ "https://ratrtile.crm...
2020-07-23 13:19:06	168.63.14.35:29184	Unknown	All Dynamics 365 activities	ExecuteMultiple	"Portals" @ "https://ratrtile.crm...
2020-07-23 13:18:57	168.63.14.35:29184	Unknown	All Dynamics 365 activities	ExecuteMultiple	"Portals" @ "https://ratrtile.crm...

Audit log includes user login and administrator actions and more:



Audit log search

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. Learn more about searching the audit log

Search

Activities: All Dynamics 365 activities

Start date: 2020-07-16 00:00

End date: 2020-07-24 00:00

Users: Show results for all users

File, folder, or site: Add all or part of a file name, folder name, or URL.

Results 150 results found (More items available, scroll down to see more.)

Date	IP address	User	Activity	Item	Detail
2020-07-23 13:29:46	168.63.14.35:29184	Unknown	All Dynamics 365 activities	ExecuteMultiple	"Portals" @ "https://ratrtile.crm...
2020-07-23 13:29:45	168.63.14.35:29184	Unknown	All Dynamics 365 activities	ExecuteMultiple	"Portals" @ "https://ratrtile.crm...
2020-07-23 13:29:35	168.63.14.35:29184	Unknown	All Dynamics 365 activities	ExecuteMultiple	"Portals" @ "https://ratrtile.crm...
2020-07-23 13:29:35	168.63.14.35:29184	Unknown	All Dynamics 365 activities	ExecuteMultiple	"Portals" @ "https://ratrtile.crm...
2020-07-23 13:29:25	168.63.14.35:29184	Unknown	All Dynamics 365 activities	ExecuteMultiple	"Portals" @ "https://ratrtile.crm...
2020-07-23 13:29:25	168.63.14.35:29184	Unknown	All Dynamics 365 activities	ExecuteMultiple	"Portals" @ "https://ratrtile.crm...
2020-07-23 13:29:15	168.63.14.35:29184	Unknown	All Dynamics 365 activities	ExecuteMultiple	"Portals" @ "https://ratrtile.crm...
2020-07-23 13:29:05	168.63.14.35:29184	Unknown	All Dynamics 365 activities	ExecuteMultiple	"Portals" @ "https://ratrtile.crm...
2020-07-23 13:19:17	168.63.14.35:29184	Unknown	All Dynamics 365 activities	ExecuteMultiple	"Portals" @ "https://ratrtile.crm...
2020-07-23 13:19:16	168.63.14.35:29184	Unknown	All Dynamics 365 activities	ExecuteMultiple	"Portals" @ "https://ratrtile.crm...
2020-07-23 13:19:07	168.63.14.35:29184	Unknown	All Dynamics 365 activities	ExecuteMultiple	"Portals" @ "https://ratrtile.crm...
2020-07-23 13:19:06	168.63.14.35:29184	Unknown	All Dynamics 365 activities	ExecuteMultiple	"Portals" @ "https://ratrtile.crm...
2020-07-23 13:18:57	168.63.14.35:29184	Unknown	All Dynamics 365 activities	ExecuteMultiple	"Portals" @ "https://ratrtile.crm...

Transparency

Data Location and Access

Transparency & Control

We will explain what we do with your data in clear plain language.

You know where your data is stored, who can access it, and under what conditions. Dynamics 365 and Dataverse environments, customers can specify the region where their customer data will be stored. Microsoft may replicate customer data to other regions available within the same geography for data durability, except as specified below.

No matter where customer data is stored, Microsoft does not control or limit the locations from which customers, or their end users may access customer data. The most up-to-date interactive report is available here.

Microsoft will not transfer customer data outside the selected Azure geographic location (geo) except when:

- It is necessary for Microsoft to provide customer support, troubleshoot the service, or comply with legal requirements.
- Customers use services that are designed to operate globally, including the following:
  - Home page, which stores application names, descriptions, and logos globally for performance.
  - Azure Active Directory, which may store Active Directory data globally. You can find more information here;
  - Azure Multi-Factor Authentication, which may store Multi-Factor Authentication data globally. You can find more information here;
  - Customer data collected during the onboarding process by the Admin Center. You can find more information here;
  - Services that provide global routing functions and do not process or store customer data. This includes Azure DNS, which provides domain name services that route to different regions; or
  - Preview, beta, or other pre-release services, which typically store customer data in the United States but may store it globally.
  - Additionally, certain types of customer data (specifically the application name, application description, and application logo) will be stored globally, rather than in the primary storage geo.
- Customers configure external services to extend their environment, such customer configurations may cause customer data to be transferred outside of the selected geo. Examples of customer configurable external services include:
  - **Machine Learning Cognitive Services:** If features that use cognitive services are activated, customer data for domains such as product recommendations and demand forecasting can be synchronized outside of the configured region. Use of these features is optional. You can find more information here.
  - **Data integration:** Configuration of Dynamics 365 data management features that work with external services (whether provided by Microsoft or a third party) may result in the transfer of core customer data outside of the region configured for the production environment to a geographic location that customers designate. You can find more information here.

- **Microsoft Power BI, Microsoft Power Apps, and Microsoft Power Automate:** Customers who connect their Power BI, PowerApps, or Flow deployment to Dynamics 365 may send customer data outside of the designated region to the geographic area where their Power BI, Power Apps, or Power Automate is deployed. You can find more details here.
- **Azure DevOps and Visual Studio Team Services:** Customers can choose where to store custom code, metadata, and data assets that support their implementation. You can find more information about the availability of Azure DevOps Service (Previously Visual Studio Team Services) here.

We are Accountable to You

If you have requested notifications, we will notify you about changes in our service operations. As an administrator, you will receive security, privacy, and audit information, as well as service and compliance notifications regarding data center location changes.

Resources

Trust Center
Dynamics 365 and Power Platform trust Platform trust