Microsoft Dynamics AX 2012 Security Guide

Microsoft Corporation

August 2013

Microsoft Dynamics is a line of integrated, adaptable business management solutions that enables you and your people to make business decisions with greater confidence. Microsoft Dynamics works like and with familiar Microsoft software, automating and streamlining financial, customer relationship and supply chain processes in a way that helps you drive business success.

U.S. and Canada Toll Free 1-888-477-7989

Worldwide +1-701-281-6500

www.microsoft.com/dynamics

Contents

About this guide

The *Microsoft Dynamics AX 2012 Security Guide* provides security guidance to system implementers planning an AX deployment and to system administrators protecting AX and its environment from external and internal threats. The guide applies to all versions of Microsoft Dynamics AX 2012 released as of this writing.

The guide does not directly address security at the level of software development. However, the technical reference at the end provides links to security-related developer resources from Microsoft.

Planning security for Microsoft Dynamics AX

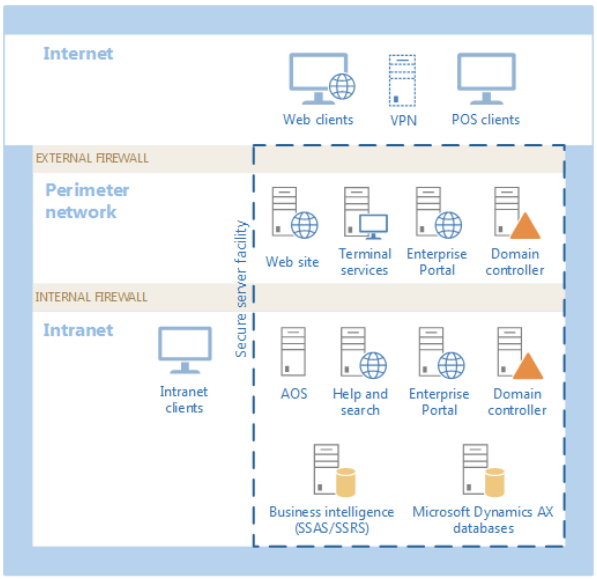
Security planning for a Microsoft Dynamics AX 2012 system starts before deployment and continues throughout the life cycle of Microsoft Dynamics AX. It requires an understanding of potential security threats and of the industry best practices for confronting each type of threat. This topic outlines an approach to planning that matches threats with defenses in each level of your computer infrastructure, placing the greatest levels of protection around your organization's most valuable assets.

Assess your threats

An organization's computer security strategy starts with an assessment of its most valuable assets and operational capabilities – that is, its core business processes or provided services. These assets and capabilities will include the following, in descending order of importance:

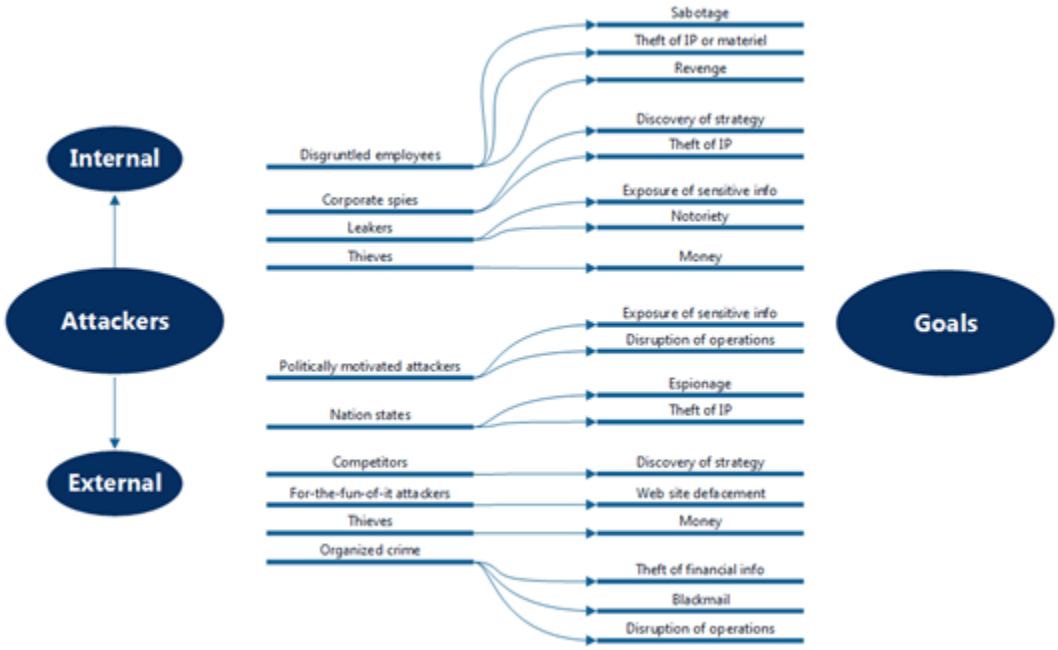
- Business, customer, and financial data
- Continuity of business operations
- Computer code and other intellectual property (IP)
- Network connectivity
- Integrity of public-facing websites
- Physical infrastructure

In a typical Microsoft Dynamics AX deployment, these assets and capabilities will be associated with computers that are distributed across public and private networks, and that have varying degrees of security. The following diagram illustrates the network topology and physical arrangement of a simple Microsoft Dynamics AX deployment, with the unsecured Internet at the top and increasingly secured enterprise environments as you move down.



The components of this Microsoft Dynamics AX system extend across several distinct security domains, including the public Internet (top), a perimeter network (also known as a DMZ, demilitarized zone, and screened subnet; middle), and an intranet (bottom). Users access public-facing business services from across the Internet by means of web browsers, point-of-sale terminals, or virtual private network (VPN) clients. An external firewall (located in a secured server facility along with the organization's other server and network equipment) filters and directs incoming network traffic based on the packet protocol and destination port. Protected by this firewall, the organization's perimeter network contains the public-facing servers – Terminal Services, Enterprise Portal for Microsoft Dynamics AX, DNS, and so on – that handle access from external clients. Separating the perimeter network from the organization's intranet is a second firewall that directs and filters traffic based on the source, port, and application. Behind this firewall, the intranet contains computers running the rich client or Enterprise Portal, Application Object Server (AOS), the Help server, the internal Enterprise Portal server, the databases, and other servers.

Next, develop a threat model that lists possible attackers, goals, exploits, and targets. Details will vary depending on the nature of your organization, but a general model of enterprise-level adversaries might resemble the following.



After this threat model is mapped to potential targets in your organization, you will have a framework for identifying threats, recognizing vulnerabilities, prioritizing by return on investment (ROI), and planning countermeasures. In the following table, some sample goals of potential attackers are juxtaposed with the assets and operations that would be threatened, and with the priority of the resulting threat.

Goal	Targets	Priority
Theft of IP	Databases	High
Theft of financial info	Databases, network, Microsoft Dynamics AX access	High
Disruption of operations	Network, server computers	High

Goal	Targets	Priority
Exposure of sensitive info	Network, office computers	Medium
Website defacement	Public web server	Low

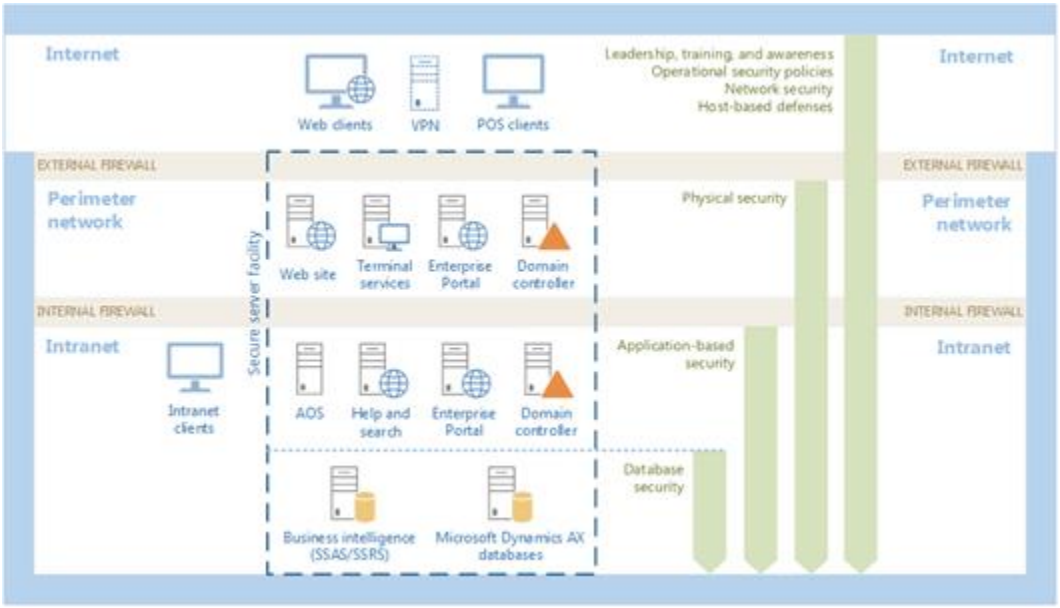
Based on the potential cost to the organization, greater resources should be devoted to protecting the databases than the public-facing web server. The protection of financial data requires that multiple attack vectors be taken into account: network intruders attacking the databases from outside the organization, and also insiders with access to Microsoft Dynamics AX client computers and other intranet resources.

Plan your countermeasures

To confront potential threats, Microsoft follows industry standards in recommending a layered, heavily redundant approach to security known as defense in depth. Defense in depth is based on the insight that any defensive measure can be defeated by a sufficiently determined adversary. Rather than trusting a single defense, such as a firewall that sits in front of otherwise vulnerable targets, defense in depth relies on multiple defenses that are understood primarily as delaying tactics. An effective implementation of defense in depth buys the defender time to respond to an attack before irretrievable losses are suffered.

After you have prioritized your organizational assets and operations, identified your potential attackers, and established what assets could be targeted, the next step of planning is to select appropriate countermeasures for each component of your system.

The following diagram matches the Microsoft Dynamics AX system topology that was already described with a layered defense that applies the most resources to the most valuable assets.



Moving from the Internet (at the top of the diagram) downward through levels within the enterprise, the security policy accrues deepening layers of protection and monitoring, as represented by the vertical bars on the right. Note that the most valuable business assets are afforded the most protections. The first four types of security measure apply to all assets across the organization:

- Leadership, training, and awareness
- Operational security policies
- Network security
- Host-based defenses

The next three are specific to on-premises hardware and software:

- Physical security
- Application-based security
- Database security

The rest of this section describes each of these categories and explains how they fit together into a comprehensive security plan.

Security categories

Leadership, training, and awareness

Management commitment to security is crucial to the success of a security plan. Applying security measures requires human and financial resources, and the enforcement of consistent policies throughout the organization. Ideally, an executive-level security chief should be responsible for the planning, implementation, and ongoing supervision of the security policy, and for serving as the single point of contact.

Employees also need to be engaged with the planning process, thoroughly trained in the security issues and best practices appropriate for their roles, and aware that the welfare of the organization depends on their awareness and loyalty.

Operational security policies

Operational security policies are open-ended and vary from one organization to another. These policies regulate the interactions of outsiders and employees with business assets.

- **Principle of least privilege** – Users (and personnel generally) should be given the minimum security privileges that they require to carry out their approved tasks. This principle can be applied equally well to computer and application access, network access, and physical access. Exceptions, if truly needed, should be cross-checked using segregation of duties.
- **Segregation of duties** – No organizational process should be under the control of a single employee. Instead, sign-offs by multiple employees should be required at each stage in any process. This policy protects against both fraud and errors. For example, an inside attacker attempting to obtain bulk financial information should face barriers created by Microsoft Dynamics AX role-based security. In addition, honest employees should be prevented by their roles from seeing or exposing sensitive data such as credit card numbers.
- **Logging computer access** – Access to restricted servers and software applications should be logged electronically, and the logs should be regularly audited. The information retained should include the identity of the user, and the time and duration of the user session. Access that deviates from an

employee's normal or expected pattern, including higher than normal computer processing workloads, should be investigated.

- **Domain-controlled password strength and expiration policies (including service accounts)** – Policies enforcing password strength and expiration can help minimize damage in the case of stolen or inadvertently leaked passwords. Consider using service account passwords that expire to prevent server assets from being exposed to attacks from insiders.
- **Domain-controlled computer access policies** – Domain policies offer a centralized way of designing and controlling access based on the principle of least privilege. Restrictions might be based on the user, host, time, location, or application.
- **Software installation policies** – Unauthorized software installed by employees inside the intranet might create a security hazard. Aside from the possibility of introducing actual malware, employees who do this might deliberately or inadvertently circumvent network and host-based security measures, or interfere with the operation of authorized software. Domain restrictions can reduce these threats, but employee training and awareness should be regarded as the first line of defense.
- **Encrypted internal and external data exchange** – The organization's internal and external electronic data exchanges (email, telephone, business records and data, and so on) should be protected by strong encryption. Reliable encryption means encryption performed by on-premises computers. Information encrypted by third parties or on remote server hosts (such as cloud storage) should not be considered safe. Furthermore, the protection of message content by encryption should not be confused with the use of secure channels provided by VPNs or HTTPS – for maximum security, these measures should be used in tandem. We strongly recommend hiring a reputable security consultant when planning and implementing an encryption policy.
- **External access over HTTPS or VPN** – Remote access to the organization's servers should only be allowed over HTTPS (for connecting via Enterprise Portal) or over a VPN (for connecting via Terminal Services to a rich client). Both methods provide a secure tunnel for communications between the user's remote client computer and the on-premises Microsoft Dynamics AX services. However, unless the content itself is encrypted, it will be available as clear text at both ends of the secure connection. For information about securing Enterprise Portal access, see Configure Enterprise Portal to use Secure Sockets Layer.
- **Restrictions on devices** – Unless the security impact of an employee-owned device is validated by your IT department and the device is approved for workplace use, it might be a security hazard. In environments demanding very high data security, the presence of portable storage media (USB thumb drives, portable disk drives, optical media, and so on) might not be acceptable. Domain controls on the types of devices that can connect to on your intranet might be advisable (especially if there is wireless support).

Network security

1. **Firewalls** – Firewalls filter network access based on rules. They are broadly divided into network and application firewalls, depending on the level of the OSI stack they work on. Any aspect of network communications, including sources, destinations, packet types, and timing, can be controlled. Dynamic firewalls can adjust rules automatically in response to hostile network traffic such as distributed denial of service (DDOS) attacks. Though generally deployed as dedicated network appliances, firewalls can also be implemented in software as a host-based defense. For information

about using host-based firewalls with Microsoft Dynamics AX, see Firewall settings for Microsoft Dynamics AX components.

2. **Forward and reverse proxies**– Proxy servers, located in the perimeter network, insert mediating services between two computers, enabling the transaction to be filtered, altered, or logged. A forward proxy passes packets from the intranet to the Internet, whereas a reverse proxy passes them from the Internet to the intranet. Most perimeter-hosted services play the role of a reverse proxy. A forward proxy lets administrators control services that users can connect to from the intranet. In this way, for example, sites known to be spreading malware can be blocked.
3. **Perimeter network (DMZ)** – A perimeter network contains servers that communicate directly with the Internet, and that have limited access to internal assets such as databases. In a Microsoft Dynamics AX deployment, the services provided might include HTTP/HTTPS, Terminal Services, and public-facing Enterprise Portal services. External connections are filtered by a firewall and forwarded to one of the perimeter network servers rather than to an intranet computer. The perimeter server processes the packets delivered to it and communicates with back-end services, but there is no communication between the Internet and the back end. The internal firewall accepts packets only from designated hosts in the perimeter and passes them to the intranet only if they meet security rules.
4. **Isolated sub-networks** – The principle of least privilege can be applied to the architecture of the organization's local area network (LAN). You can segregate groups or duties by placing their computer resources on mutually non-routable subnets.

For detailed information about all of these considerations, see Network Security (http://technet.microsoft.com/en-us/library/cc716269.aspx) on TechNet.

Host-based defenses

- **Local software firewall** – Client-side software firewalls can provide some of the same protection from network attacks as dedicated hardware firewalls. An example that comes with Microsoft Windows–based consumer computers is Windows Firewall, which uses application-based rules to block both incoming and outgoing communication that is unexpected or prohibited. Numerous third-party vendors also provide firewall software, much of it free, intended for use on consumer computers.
- **Intrusion detection system (IDS) and file integrity monitoring (FIM)** – IDS and FIM software alerts administrators to irregularities in network access and file integrity, respectively. A rule-based IDS can immediately give notice when a system comes under attack. A FIM package can spot changes to system or application files that might be a tip-off to the activities of an intruder.
- **Antivirus software** – Up-to-date antivirus software should be installed on all organization computers, whether on-premises or off-premises.
- **Logging** – Although intruders might erase signs of their presence in a computer's logs, it is good policy to inspect the system logs periodically to ensure that no anomalies have been detected.
- **Software updates** – Regular software updates, particularly security updates, should be applied as a part of domain policy.
- **Full-disk encryption** – Where practical, full-disk encryption can prevent data from falling into the wrong hands if the physical security of a computer is compromised. This is especially useful for laptops and other client computers used off-premises.

Physical security

Strong locks, reinforced doors, and other measures to prevent unauthorized physical access to computer hardware are fundamental security measures. Layers of physical security should include:

- Restricted access to buildings where servers are housed, possibly enforced by security personal, logging of persons entering and leaving, video surveillance, smart cards, biometric authentication, motion sensors and alarms, and so on. The value of the assets being protected should guide decisions about the measures required.
- Highly restricted access to rooms where servers are actually situated.
- Video surveillance inside server rooms.
- Locking enclosures on computer equipment to prevent theft or easy access to internal components.
- Banning or disabling uncontrolled means of inserting or extracting data (optical drives, USB ports, and so on).
- Use of BIOS passwords.
- Secure, off-premises storage of computer event logs that can be compared with local logs to look for irregularities and discrepancies.
- Case locks and biometric or smart-card logons for workstations.
- Secure storage of portable devices.

Application-based security

Microsoft Dynamics AX 2012 provides a role-based security framework to assign and restrict user permissions inside Microsoft Dynamics AX. For full documentation about the configuration and use of role-based security, see Set up user security in Microsoft Dynamics AX.

Database security

For information about Microsoft Dynamics AX 2012 database security, see Data security in Microsoft Dynamics AX.

Resources

Microsoft security resources on TechNet

Security Tech Center (http://technet.microsoft.com/en-US/security/)

Microsoft Security Blog (http://blogs.technet.com/b/security/)

Security Guidance (http://technet.microsoft.com/en-us/library/cc184906.aspx)

Microsoft Security Bulletins (http://technet.microsoft.com/en-us/security/bulletin)

Other security resources

[NIST] Computer security Division / Computer Security Resource Center (http://csrc.nist.gov/)

[NSA] Security Configuration Guides
(http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/index.shtml)

[NSA] Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environment (http://www.nsa.gov/ia/_files/support/defenseindepth.pdf) (PDF)

[NSA] The 60 Minute Network Security Guide (First Steps Towards a Secure Network Environment)
(http://www.nsa.gov/ia/_files/support/I33-011R-2006.pdf) (PDF)

Hardening Microsoft Dynamics AX components against security threats

Client security and protection

This topic describes important considerations and best practices for the security of Microsoft Dynamics AX 2012 client computers. One of the most important security considerations is how you deploy the client. Attention must be given to security when the Microsoft Dynamics AX client is deployed. Otherwise, malicious users may gain access to Microsoft Dynamics AX data, or users in your business or organization may unintentionally gain access to sensitive data. Regardless of whether your business or organization runs only a few Microsoft Dynamics AX clients or dozens of clients, we recommend that you deploy the client in the way that is described in this topic. By following these recommendations, you can help protect your data and reduce the overall attack surface of your computing environment. This topic includes the following information:

- Terminal Services deployment (more secure)
- Individual deployments (less secure)
- Encrypt communications between the client and Application Object Server (AOS)
- Best practices for secure client deployments

Terminal Services deployment (more secure)

Terminal Services, which is a feature of the Windows Server 2008 operating system, uses the Remote Desktop Protocol (RDP) to communicate between clients and servers. After you deploy an application on a Terminal Services server, clients can connect over a remote access connection, a local area network (LAN), a wide area network (WAN), or the Internet.

When a user accesses an application such as Microsoft Dynamics AX on a Terminal Services server, the application runs on the server. Only information from the keyboard, mouse, and display is transmitted over the network. Users can view only their own sessions. Each session is managed transparently by the server's operating system, and each session is independent of every other client session.

From a security perspective, there are several benefits to running the Microsoft Dynamics AX client on a Terminal Services cluster:

- Only keyboard strokes, mouse actions, and images of the information that is displayed on the Terminal Services server are transmitted over the network. Because Microsoft Dynamics AX data is not transmitted over the network to client computers, the threat that a malicious user may acquire data that is stored on a user's local client computer is reduced.
- No data is processed, cached, or stored on a user's local computer. All data processing, caching, and storage occur on the Windows Server computer that is running the Microsoft Dynamics AX client. Therefore, if a user's local client computer is stolen or lost, a malicious user cannot access Microsoft Dynamics AX data on that computer.

- If a security update is issued for Microsoft Dynamics AX, that update must be applied only to the computers in the Terminal Services cluster. Therefore, the overall attack surface of Microsoft Dynamics AX is minimized.

Figure 1 shows an example of an architecture in which Microsoft Dynamics AX runs on a Terminal Services cluster.

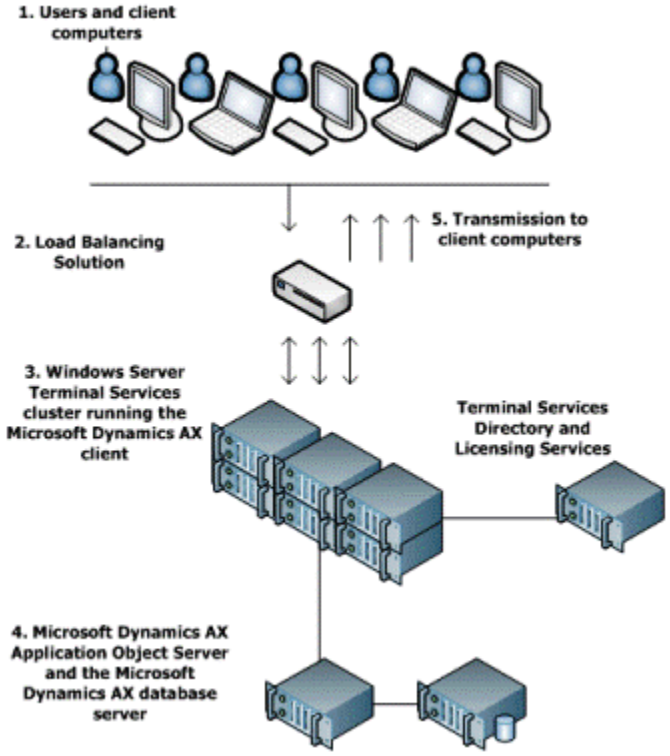


Figure 1: Microsoft Dynamics AX deployed on a Terminal Services cluster

1. Users log on to their client computers. The users then open either a remote desktop connection or, if they connect by using the HTTP service, a remote desktop Web connection. Alternatively, users can double-click the Microsoft Dynamics AX client icon on their computers and run the application as a Terminal Services session. This capability is a feature of Windows Server 2008 that is named RemoteApp.
2. The load balancing solution routes traffic to the Terminal Services cluster based on server availability and load.
3. Terminal Services receives the session request. Terminal Services then communicates with the Terminal Services Directory and Licensing Services to manage sessions, and to verify that a license is available. If a license is available, Terminal Services starts a unique session for each user. Depending on the configuration of Terminal Services, users may see a Windows desktop. These users can then access the Microsoft Dynamics AX client from the **All Programs** menu. Alternatively, if users are using Terminal Services RemoteApp, the Microsoft Dynamics AX client opens and appears to the users as an application that runs on their client computer.

4. The Microsoft Dynamics AX clients that run on the Terminal Services cluster communicate with the Microsoft Dynamics AX AOS and database server through ordinary channels.
5. The Terminal Services cluster transmits images of the information that is displayed on the Terminal Services server over the network to client computers. No data is transmitted over the network. Therefore, no Microsoft Dynamics AX data resides on any user's client computer.

Deployment considerations

- By default, Terminal Services enables only two client sessions at the same time. Before you can deploy a Terminal Services cluster, business decision makers in your business or organization must assess the cost of purchasing additional Terminal Services licenses. We highly recommend the investment, because a Terminal Services cluster reduces administrative overhead. Additionally, a Terminal Services cluster reduces the attack surface for security threats against Microsoft Dynamics AX and any other line-of-business applications that run on the cluster.
- Every user who connects to the Microsoft Dynamics AX client on the Terminal Services cluster must be a member of the Remote Desktop Users group in **Microsoft Windows Users and Groups**.
- To enhance the security of your computing environment, deploy Group Policy and Encrypting File System on all computers. If your business or organization uses Windows Server 2008, Windows 7, or Windows Vista, deploy Windows BitLocker Drive Encryption. Group Policy and Encrypting File System are described in more detail in the next section.

For more information about Terminal Services, see the Terminal Services in Windows Server 2008 (http://go.microsoft.com/fwlink/?LinkId=118304).

Individual deployments (less secure)

The Microsoft Dynamics AX client can be deployed on users' local computers. However, for the following reasons, this kind of deployment is less secure than a deployment of the Microsoft Dynamics AX client on a Terminal Services server.

- Because more data is transmitted over the network, there is more risk that a malicious user may intercept Microsoft Dynamics AX data that is sent between the client and AOS.
- If users do not diligently help secure their computers, or if a computer is lost or stolen, there is more risk that a malicious user may access data that is stored on individual computers.
- If users have access to the Internet, there is more risk of virus attacks or problems with malicious software.
- If your business or organization does not enforce a policy that requires that users download and install security updates as soon as they are available, your computing environment is at more risk.

You can reduce some of these security risks by deploying the Windows security features that are described in the following sections.

Deployment considerations

If you deploy the Microsoft Dynamics AX client on individual computers, we recommend that you use the deployment practices that are described in this section. By following these recommendations, you can improve security and reduce some of the risks that were described earlier in this topic.

Deploy Group Policy

If you intend to deploy the Microsoft Dynamics AX client on individual computers in your business or organization, we recommend that you first implement Group Policy, and then deploy Microsoft Dynamics AX. Group Policy is a feature of Windows Server 2008. Group Policy provides an infrastructure for delivering and applying configurations or policy settings to users and computers in an Active Directory environment. By using Group Policy you can perform the following tasks:

- Manage user settings and computers from a central location.
- Implement security settings across an enterprise.
- Implement standard computing environments for groups of users.
- Centrally manage software installations, updates, repairs, and upgrades, and software removal.
- Centrally deploy, recover, restore, and replace users' data, software, and personal settings.
- Centrally configure and customize users' computers to provide a consistent computing environment and consistent system settings.
- Centrally manage and control power settings for computers.
- Control device installation and access to devices such as USB drives, CD-RW drives, DVD-RW drives, and other removable media.
- Manage Group policy settings for your firewall and Internet Protocol security (IPsec) at the same time. This feature provides more security when you must help secure server-to-server communications over the Internet, limit access to domain resources based on trust relationships or the health of a computer, and protect data communication to a specific server to meet regulatory requirements for data privacy and security.
- Open and edit Group Policy settings for Internet Explorer. This feature reduces the risk that you may unintentionally change the state of the policy settings based on the configuration of the administrative computer.
- Assign printers based on either a location in the business or organization or a geographic location. You can also enable Group Policy settings that allow users to install printer drivers.

For more information, see Group Policy in Windows Server 2008.

Use the client configuration utility securely

This section describes recommended practices for using the Microsoft Dynamics AX 2012 Configuration utility in a secure manner.

- Do not install the Microsoft Dynamics AX 2012 Configuration utility on the client computers in a production environment. Instead, create a client configuration file, and store the file in a network shared folder. To install Microsoft Dynamics AX clients that do not include the Microsoft Dynamics AX 2012 Configuration utility, you must perform a silent installation. For more information, see Mass deployment of the Microsoft Dynamics AX Windows client.
- Configure the network shared folder that contains the client configuration file so that all Microsoft Dynamics AX users who are not system administrators have read-only permission. By storing the configuration file in a network shared folder that is configured for read-only permission, you can help prevent accidental changes to the configuration file.

Deploy Encrypting File System

Encrypting File System (EFS) is a component of the NTFS file system on Windows operating systems. EFS is used to encrypt files and folders on client computers and remote servers. When EFS is used, users can help protect their data from unauthorized access by other users or malicious users. Any individual or application that does not have the appropriate cryptographic key cannot read the encrypted data.

By deploying EFS on the computers where you install the Microsoft Dynamics AX client, you add another level of security for any data or files that users may store locally.

For more information, see Encrypting File System (http://go.microsoft.com/fwlink/?LinkId=118685).

Deploy Windows BitLocker Drive Encryption

Windows BitLocker Drive Encryption, or BitLocker, is a feature that is available in the Windows Server 2008, Windows 7, and Windows Vista operating systems. This feature can help protect data that is stored on client computers, especially mobile client computers.

BitLocker performs two functions:

- BitLocker encrypts all data that is stored on the Windows operating system volume and any data volumes that are configured. This data includes the Windows operating system, hibernation and paging files, applications, and data that is used by applications.
- BitLocker is configured to use a Trusted Platform Module (TPM) to help guarantee the integrity of components that are used in the early stages of the startup process. Any volumes that are protected by BitLocker are "locked." Therefore, these volumes remain protected, even if the computer is tampered with when the operating system is not running.

If a volume is protected by BitLocker, all data that is written to the volume is encrypted. This includes the operating system itself, and all applications and data. In this way, BitLocker helps protect data from unauthorized access. Although the physical security of servers remains important, BitLocker can help also protect data if a computer is stolen or shipped from one location to another, or if the computer is otherwise out of a user's physical control.

By encrypting the disk, BitLocker helps prevent offline attacks. For example, a malicious user may try to bypass Windows security provisions, such as permissions that are enforced by access control lists (ACLs) in NTFS, by removing a disk drive from one computer and installing it in another computer.

For more information, see Windows BitLocker Drive Encryption (http://go.microsoft.com/fwlink/?LinkId=118687).

Special considerations for client computers that are used in development environments

Client computers that are used for Microsoft Dynamics AX development must be isolated from the clients, AOS instances, and database computers that are used in the production environment. Otherwise, if the environments are not correctly isolated, the process of testing or developing customizations may unintentionally affect the production environment.

To help maintain the security of the production environment, we recommend that you not grant developers access to the Microsoft Dynamics AX production database. Instead, make sure that client

computers that are used for development have their own AOS instance and database, and that the development environment has its own data set. To help maintain security and privacy, do not use production data in a development environment.

Encrypt communications between the client and AOS

Microsoft Dynamics AX AOS performs business logic and data processing for all incoming and outgoing requests from client computers. If a malicious user intercepts requests between a client computer and AOS, that user may gain access to data or information. By using encryption, you can reduce the risk that a malicious user may intercept requests between client computers and AOS.

Remote procedure call encryption

By default, Microsoft Dynamics AX is configured to encrypt all credentials and data that are transmitted over the network between clients and AOS, and between AOS and the database. Microsoft Dynamics AX uses the remote procedure call (RPC) to perform the encryption.

We recommend that you not disable the RPC security feature. You can verify that RPC encryption is enabled by using the Microsoft Dynamics AX 2012 Configuration utility. The configuration utility is automatically installed when you install the Microsoft Dynamics AX client. If you suspect that users or administrators have disabled RPC encryption, verify the encryption setting on each Microsoft Dynamics AX client computer in your business or organization.

1. Click **Start** > **Control Panel** > **Administrative Tools** > **Microsoft Dynamics AX 2012 Configuration**.
2. Click the **Connection** tab.
3. Verify that **Encrypt client to server communications** is selected. If this option is not selected, select it, and then click **OK**.

Role Center encryption

Role Centers provide overview information for Microsoft Dynamics AX users. This information includes work lists, activities, common links, and key information about business intelligence. Role Centers use the framework for Enterprise Portal for Microsoft Dynamics AX to display information either on an Enterprise Portal Web site or on a Role Center home page in the Microsoft Dynamics AX client.

If your business or organization uses Role Centers, and if the administrator installed Enterprise Portal without Secure Sockets Layer (SSL) encryption, all communications between Role Centers in the Microsoft Dynamics AX client and AOS are sent in clear text. As a result, if a malicious user intercepts communications between a client computer that is using Role Centers and AOS, that user can see data from those communications.

If your business or organization uses Role Centers, you must make sure that Enterprise Portal is configured to use SSL encryption. SSL encryption is a feature of Internet Information Services (IIS), which is the Web server software that hosts the Enterprise Portal framework. For more information about how to configure SSL encryption, see Secure Sockets Layer encryption in IIS 7.0 (http://go.microsoft.com/fwlink/?LinkId=118362).

Best practices for secure client deployments

The following table describes the best practices that apply to all deployments of the Microsoft Dynamics AX client.

Recommendation	Description
Always assign the least permissions when you set up and configure the user security features in Microsoft Dynamics AX.	Before you set up and configure the least permissions in Microsoft Dynamics AX, consider the following recommendations: • By default, and by design, only Microsoft Dynamics AX system administrators have access to the Application Object Tree (AOT). Do not grant users access to the AOT, unless the users are members of a development role who must access the AOT as part of their job requirements. If you grant regular users access to the AOT, the users may intentionally or unintentionally compile the application, synchronize the application, change license files, or change module configurations. All of these actions can cause problems in your business or organization. • Do not make users members of the **System administrators** role, or grant these users access to **System administration** in Microsoft Dynamics AX, unless the users are responsible for setting up and configuring Microsoft Dynamics AX in your business or organization. If you grant regular users access to this group and module, the users may intentionally or unintentionally cause problems in the Microsoft Dynamics AX application. • Do not assign users to the Windows **Administrators** group or **Power Users** group on their local computers, unless the users are explicitly required to perform the job functions of an administrator or power user. Members of these groups can add applications to their local computers and remove applications from their local computers, and these actions can introduce security risks. Instead, assign users to the Windows **User** group. Click **Start** > **Administrative Tools** > **Server Manager** > **Local Users and Groups**.
Educate users about how to use strong passwords, and define password policies.	Strong passwords and password policies in your domain help maintain a secure computing environment. We highly recommend that you implement password best practices in your business or organization. For more

Recommendation	Description
	information, see Password Best Practices (http://go.microsoft.com/fwlink/?LinkId=118273).
Enable Windows Firewall or another firewall device on each computer.	A firewall drops incoming traffic that has not been sent in response to a request of the computer. Traffic that is sent in response to a request is named solicited traffic. The firewall also drops unsolicited traffic that has not been specified as allowed. Traffic that is unsolicited but allowed is named excepted traffic. A firewall adds a level of protection against malicious users and applications that rely on unsolicited incoming traffic to attack computers. We recommend that you enable Windows Firewall or another firewall device on every computer in your business or organization. Windows Firewall is a Control Panel feature that is used to set restrictions on the traffic that can enter your network from the Internet. For more information, see Windows Firewall (http://go.microsoft.com/fwlink/?LinkId=118283).
Enable a virus scanner on each computer.	The threat of virus attacks is ongoing and always changes. We recommend that you deploy a virus scanner on every computer in your business or organization, and that you configure the scanners to scan computers and update virus signatures regularly.
Deploy smart cards in your business or organization.	We recommend that you deploy smart cards in your business or organization. A smart card contains a small computer chip that is used to store security keys or other types of personal information. Smart cards use cryptographic technology to store the information. Some businesses or organizations deploy smart card readers on every laptop and desktop computer, and require that employees insert their smart card into the reader to connect to the corporate network. By deploying smart cards in this manner, the business or organization adds another physical layer of security to its computing environment, because every user who connects to the corporate network must have a valid password and a smart card. For more information, see the Smart Card Reference (http://go.microsoft.com/fwlink/?LinkId=118292).

Application Object Server security and protection

Application Object Server (AOS) processes client requests for data and performs Microsoft Dynamics AX business logic. If a malicious user gains access to AOS, that user may gain access to sensitive data, such as financial information and trade secrets. Therefore, we recommend that you follow the guidelines in this topic when you deploy AOS. By following these guidelines, you can help protect the data in your business or organization, and reduce the overall attack surface of this core component of Microsoft Dynamics AX.

Configure AOS to use a domain account

When you install AOS by using Setup, you can configure the service to use either a domain account, a managed service account, or the Network Service account. By default, a domain account is used. The Network Service account is less secure than a domain account, provided that you set up and configure the domain account correctly. The Network Service account is less secure, because it is available to other applications that are installed on the same server. Additionally, the Network Service account is translated into a computer account if the service must communicate with a different server. For example, you deploy four AOS instances that use the Network Service account, and these servers communicate with a separate instance of Microsoft SQL Server. As a result, four different computer accounts are created in SQL Server. Therefore, in this scenario, you have four accounts that a malicious user may be able to use to gain access to AOS or the database. By using a domain account, there is only one account that you must help secure. Therefore, the attack surface of your computing environment is reduced.

Work with your domain administrator to create a new managed service account or domain account in Active Directory. Managed service accounts are managed domain accounts that provide automatic password management and simplified service principal name (SPN) management. SPN management includes delegation of management to other administrators. For information about managed service accounts, see Service Accounts Step-by-Step Guide (http://go.microsoft.com/fwlink/?LinkID=218113).

If you use a standard domain account, the account must not be used for any other services or back office operations. The account must be a dedicated account. You must make sure that the permissions for the new account are as low, or restrictive, as possible, to help reduce the risk of processes that can harm the server. Verify with the domain administrator that the account has the following configuration:

- The password for the domain user account is a strong password.
- The domain user account does not have interactive logon rights.
- The domain user account can log on as a service.
- The domain user account is not listed as a member of any Active Directory groups that are added to Microsoft Dynamics AX. Otherwise, the account automatically becomes a Microsoft Dynamics AX user.
- The domain user account is not listed as a user or member of any groups in **Windows Users and Groups** on AOS.

For more information about Microsoft Dynamics AX service accounts, see Create service accounts (http://technet.microsoft.com/en-us/library/dd362055.aspx).

Change the default port that is used by AOS

By default, when you install Microsoft Dynamics AX, AOS is configured to listen on port 2712 for TCP/IP communications, port 8101 for WSDL communications, and port 8201 for NET-TCP communications. If

you install other AOS services on the same computer, the port numbers are incremented by 1 for each service.

If a malicious user who knows the default port numbers learns about a vulnerability in Microsoft Dynamics AX, that user may attempt to gain access to data by using a port number. You can reduce the attack surface by changing the default port numbers. For more information, see Change AOS ports (http://technet.microsoft.com/en-us/library/aa569616.aspx).

You must also specify the new port number on each client that connects to the AOS. You can change the port number by using the **Microsoft Dynamics 2012 Configuration** utility.

1. On a client computer, click **Start** > **Administrative Tools** > **Microsoft Dynamics AX 2012 Configuration**.
2. In the **Configuration target** drop-down list, select **Local client**.
3. Click **Manage** > **Create configuration**.
4. Enter a name, and then select **Copy from Active configuration**.
5. On the **Connection tab**, select the appropriate instance in the text box, and then click **Edit**.
6. Enter the new port number, and then click **OK**.

To expedite the process of configuring multiple client computers, you can export this configuration to a file and then import the configuration to all other client computers. For more information, see Manage a client configuration (http://technet.microsoft.com/en-us/library/aa569651.aspx).

Use Windows features to reduce the attack surface

Microsoft Windows operating systems include security features that can help you reduce the attack surface of your computing environment. We recommend that you implement and use the following features on AOS.

Internet Protocol Security (IPsec)

IPsec is a feature of Microsoft Windows Server 2008 that helps protect networks from active and passive attacks by using packet filtering, cryptographic security services, and trusted communications.

IPsec helps provide in-depth defense against the following kinds of attacks:

- Network-based attacks from unknown computers
- Denial-of-service attacks
- Data corruption
- Data theft
- User credential theft

For more information, see IPsec (http://go.microsoft.com/fwlink/?LinkId=119801).

Windows Firewall

Windows Firewall is a Control Panel feature that is used to set restrictions on the traffic that can enter the network from the Internet. Windows Firewall is included in Windows Server 2008.

For more information, see Windows Firewall (http://go.microsoft.com/fwlink/?LinkId=118283).

The Microsoft Security Configuration Wizard

The Microsoft Security Configuration Wizard reduces the attack surface of the Microsoft Windows Server 2008 operating system. The wizard determines the minimum set of features that is required for a server's role or roles, and then disables all features that are not required.

The Security Configuration Wizard performs the following tasks:

- Disable nonessential services
- Block unused ports
- Enable additional address or security restrictions for ports that are left open
- Prohibit unnecessary Web extensions for Internet Information Services (IIS)
- Reduce protocol exposure to server message block (SMB), LanMan, and Lightweight Directory Access Protocol (LDAP)
- Define a high signal-to-noise audit policy

To open the Security Configuration Wizard, click **Start** > **Administrative Tools** > **Security Configuration Wizard**. We recommend that you read the Help for the wizard before you change the system. For more information about services, ports, and protocols on the Windows Server 2008 operating system, see Service overview and network port requirements for the Windows Server system (http://go.microsoft.com/fwlink/?LinkId=119804).

Microsoft Security Baseline Analyzer

The Microsoft Baseline Security Analyzer scans your computer to detect non-secure configurations and identify any security updates that are missing. The analyzer then recommends changes and updates that can help improve the security of the computer.

For more information, see Microsoft Security Baseline Analyzer (http://go.microsoft.com/fwlink/?LinkId=119802).

Data security in Microsoft Dynamics AX

Database security best practices

If a malicious user were to gain access to the Microsoft Dynamics AX database, that user might gain access to data, including sensitive data such as credit card numbers, bank account numbers, and personal identification numbers. You should deploy the database as described in this section to protect data in your business or organization and reduce the overall attack surface of this core Microsoft Dynamics AX component.

We recommend that you do the following:

- Follow SQL Server security recommended practices.
- Use the table permissions framework.
- Secure the database logs.

Follow SQL Server security recommended practices

We assume that you have followed the recommended transactional SQL Server security best practices described in the article Securing SQL Server (http://msdn.microsoft.com/en-us/library/bb283235.aspx). These best practices include:

- Platform and network security, including physical, operating system, and file security
- Principals and database object security

We also assume that security best practices are in place for all functions of SQL Server throughout the environment:

- Security and protection (SSRS) (http://msdn.microsoft.com/en-us/library/bb522728.aspx)
- Security and protection for analytics (http://msdn.microsoft.com/en-us/library/ee910037.aspx)
- Security planning for SharePoint 2013 farms (http://technet.microsoft.com/en-us/library/hh377941.aspx)

Encrypt sensitive data

We recommend that you implement database encryption to enhance the security of data, including sensitive data such as credit card numbers, bank account numbers, and personal identification numbers. If your business or organization processes and stores credit card information, we recommend that you adhere to the standards set by the PCI Security Standards Council (http://go.microsoft.com/fwlink/?LinkId=119942) for securing cardholder data. The PCI Data Security Standard (http://go.microsoft.com/fwlink/?LinkId=119943) requires the following:

Security standard	Requirement
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect stored cardholder data. 4. Encrypt the transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	5. Use and regularly update antivirus software. 6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	7. Restrict access to cardholder data. 8. Assign a unique ID to each user with computer access. 9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security.

Enabling database encryption directly addresses the requirement to protect stored cardholder data. SQL Server includes an encryption feature called Transparent Data Encryption (TDE). TDE is designed to provide protection for the entire database while it is at rest, without affecting existing applications. Implementing encryption in a database traditionally involves complicated application changes, such as modifying table schemas, removing functionality, and significant performance degradations. Custom schemes are often used to resolve equality searches, and ranged searches often cannot be used at all. Even basic database elements, such as creating an index or using foreign keys often do not work with cell-level or column-level encryption schemes, because the use of these features inherently leaks information. TDE solves these problems by encrypting everything, including all data types, keys, and indexes. For more information, see Database Encryption in SQL Server 2008 Enterprise Edition (http://go.microsoft.com/fwlink/?LinkId=119936).

Secure the database logs

Database logs can contain sensitive data. By default, any database log that is created can be queried by any user who has access to the database. Users can query the log by using .NET Business Connector, X++, alerts, or direct access to the database. To protect data, restrict the permissions on the sysdatabaselog table. For detailed information, see Table Properties (http://msdn.microsoft.com/en-us/library/aa871620.aspx).

Manage record level security

Record-level security builds on the restrictions enforced by role-based security. By using role-based security, you restrict the menus, forms, and reports that role members can access. By using record level security to set restrictions on specific records or tables in the database, you can restrict the data that is shown in reports and on forms.

Note:
The record-level security feature will be removed in a future release. If you previously set up record-level security filters, they will continue to function. If you are setting up new filters, we recommend that you create data security policies using the extensible data security framework. For more information about data security policies, see Overview of Security Policies for Table Records (http://msdn.microsoft.com/en-us/library/hh272123.aspx).

The following examples demonstrate how you can use record-level security.

- Allow members of a Sales role to see only the accounts they manage.
- Prohibit financial data from appearing on forms or reports for a specific role.
- Prohibit account details or account IDs from appearing on forms and reports for a specific role.
- Restrict form and report data according to location or country/region.

When a record-level security policy and a data security policy filter the same data, they may not work together as expected. For example, if the constrained table in the data security policy differs from the primary table in the record-level security filter, the existing record-level security policy is not added to the data security policy query. To achieve the desired behavior, you must add the ranges from the record-level security policy to the data security policy query.

Before you set up record-level security

The process of setting record-level security involves selecting a database table in the Record Level Security Wizard. Tables store the data shown in reports and on forms. You might find it helpful to work with a developer who has knowledge of the database tables when configuring record-level security. The developer can help you select the table that directly corresponds to the report or form elements to which you want to restrict access.

Also, verify the following before you begin:

- Determine whether the role that will be assigned record-level security already exists. For information about how to create a new role, see Create or modify a security role.
- Determine whether the role has permission to the report or form. If, for example, the Project accountant role does not have access to the General ledger module, then it does not make sense to assign record level security to tables in that module. For information about role permissions, see Create or modify a security role.

Set up record-level security

Setting up record-level security is a two-part process. First, you must select a role and a database table by using the Record Level Security Wizard. Next, you must create a query that specifies the fields to filter on and the criteria to be applied.

Use the Record Level Security Wizard

1. Click **System administration** > **Setup** > **Security** > **Record level security**.
2. Press CTRL + N to open the **Record level security** wizard.
3. Select the role for which you want to create a filter, and then click **Next >**.
4. Select the table to filter. By default, the main database tables are shown. Click **Show all tables** to expand the selection.

   Important:
   You cannot use record-level security filters on the tables in an inheritance hierarchy. For example, the DirPerson and DirOrganizationBase tables inherit from the DirPartyTable table. Record-level security filters cannot be used on any one of these tables.

   Click **Next >**.
5. Click **Finish**.

Create a query

1. In the **Record level security** dialog box, select the role and table association that you just created and then click **Query**. The **Inquiry** dialog box is displayed.
2. Select the first item listed on the **Range** tab. If no item is listed, press CTRL + N.
3. In the **Field** list, select the field that you want to filter on.
4. In the **Criteria** field, enter or select the filter criteria for the designated field.
5. As necessary, press CTRL + N to add fields and criteria.
6. Click **OK**.

7. Inform members of the selected role that they must close their current client sessions and start a new session. If it is necessary, end active sessions from the **Online users** form. For information about how to end active sessions, see Monitor users.
8. Verify that record-level security is enforced on the report or form by logging on to Microsoft Dynamics AX as a member of the specified role. You should see only the information specified in the query for the designated criteria. If you see additional information, troubleshoot the query.

Range filters on surrogate foreign keys

If you must specify a range filter on a column that is a surrogate foreign key, we recommend that you use data security policies instead of record-level security. For more information about data security policies, see Overview of Security Policies for Table Records (http://msdn.microsoft.com/en-us/library/hh272123.aspx). A surrogate foreign key is a column in one table that retrieves its values from, or is joined to, a column in another table. Because it is a surrogate key, its value has no meaning to people and is used only to identify a record in the table. A large number generated by the system, such as RecId, could be a surrogate key.

In the **Advanced Filter** form, a range filter on a surrogate foreign key is applied to the table that is referenced by the foreign key. However, in record-level security, a range filter must be applied to the current table. This means that record-level security will treat a range filter on a surrogate foreign key as an invalid range.

Manage data access by using the Table Permissions Framework

The Table Permissions Framework (TPF) enables administrators to add an additional level of security to tables that store sensitive data.

When the Application Object Server (AOS) attempts to perform an operation on a table that is authorized by TPF, the AOS verifies that members of the user's role have permission to perform the operation. If members of the role do not have the appropriate permissions, the AOS does not complete the operation.

Note:
TPF can be enabled on any table in the Microsoft Dynamics AX database. However, for the sake of time and efficiency, administrators assign TPF to tables that are considered to be sensitive or to be of critical business value. For information about tables where TPF is enabled by default, see the Table Permissions Framework reference.

Example

TPF adds table-level security that verifies user rights regardless of the origin of the request. For example, consider the following scenario:

1. Contoso Corporation implemented Microsoft Dynamics AX. Users access data by using the Microsoft Dynamics AX client, Enterprise Portal, the Application Integration Framework, and a third-party application that connects to Microsoft Dynamics AX by using the .NET Business Connector.
2. The administrator configured a security role called Senior Leadership, and members of this role have access to sensitive data about financial information and trade secrets. One of the database tables that stores this sensitive information is called FinancialResults. This table was added as part of a customization done by a partner after Microsoft Dynamics AX was installed.

3. In the Application Object Tree (AOT), the administrator configures the FinancialResults table so that the Application Object Server (AOS) must authorize all operations for that table.
4. Soon thereafter, a malicious user discovers a vulnerability in Contoso's third-party application that connects to Microsoft Dynamics AX by using the .NET Business Connector. The malicious user connects to the database as a member of the Sales Representative security role and attempts to read the data in the FinancialResults table.
5. Before allowing the read operation, the AOS verifies that the user is a member of the Senior Leadership security role and that members of the role have permission to read the data. The malicious user is not a member of the Senior Leadership security role. Therefore, the AOS denies the read operation.

Set authorization requirements on database tables by using the Table Permissions Framework

To enable TPF, the administrator specifies a value for the **AOSAuthorization** property on a specific table in the AOT. By default, this value is set to **None**.

The **AOSAuthorization** property can be used to authorize Create, Read, Update, and Delete operations. For some tables, you might specify a subset of operations, such as Create, Update, and Delete. If you specify a subset, the AOS authorizes the Create, Update, and Delete operations, but allows any Microsoft Dynamics AX users to perform View operations. For other tables, you should authorize all operations because the data is sensitive.

When the **AOSAuthorization** property is set for a table, table methods that cause the AOS to verify permissions are invoked on each affected table row. For more information, see AOSAuthorization Property on Tables (http://msdn.microsoft.com/en-us/library/bb278259.asp).

Use the following procedure to enable TPF on database table.

1. In the AOT, expand **Data Dictionary** > **Tables**.
2. Select a table. The properties for the table are displayed in the right pane.
3. Click the **AOSAuthorization** property and select a new value by using the drop-down list.
4. Click **Save All**.

Ensure that security roles can access data in a TPF-protected table

If you enabled TPF for a table, you might have to specify or expand permissions for roles that require access to the table.

If a table uses TPF, and the security role does not have explicit access to the table, the user may see the following message: "User <UserName> is not authorized to update a record in table <TableName>. Request denied. Access Denied: You do not have sufficient authorization to modify data in database."

Use the following procedure to determine which roles require access to the table.

1. In the AOT, expand **Data Dictionary** > **Tables**.
2. Right-click a table, and then click **Add-ins** > **Security tools** > **View related security roles**. The **Roles related to table** form is displayed. This form shows all security roles that access the selected table and the privileges that the table is included in.

Use the **Override permissions** form to grant the role access to the TPF-protected table. For more information, see Create or modify a security role.

Enterprise Portal and Role Centers security and protection

In Enterprise Portal for Microsoft Dynamics AX, security is enforced by using a combination of features and services. This topic includes checklists that can help you configure security in Enterprise Portal.

Checklists for configuring Enterprise Portal security

By default, only the administrator who installed Enterprise Portal can access the site. Therefore, Enterprise Portal is effectively locked after it is installed. The configuration of security in Enterprise Portal involves verifying roles, enabling security features, and granting users access to the site. Information in the following tables can help you configure Enterprise Portal security.

Table 1: Security tasks for the server and operating system

Task	More information
Verify security settings for Internet Information Services (IIS) and SharePoint.	See the product documentation on Microsoft TechNet and MSDN.
Encrypt Enterprise Portal client-server communications by using Secure Sockets Layer (SSL).	How to Setup SSL on IIS 7 (http://go.microsoft.com/fwlink/?LinkId=223135)

Table 2: Security tasks for extranet deployments

Task	More information
Enhance Enterprise Portal security in extranet deployments by using two domain controllers and two firewalls. This deployment model is called a traditional perimeter network. **Tip:** If you prefer not to deploy Enterprise Portal with multiple domain controllers, you can authenticate Enterprise Portal users by using claims-mode authentication. For more information, see the next item in this checklist.	Install Enterprise Portal in a traditional perimeter network (http://technet.microsoft.com/en-us/library/dd361998.aspx)

Task	More information
Deploy an Enterprise Portal site that uses the claims mode authentication that is provided by SharePoint. In the context of Microsoft Dynamics AX, this claims mode authentication is called Flexible authentication. Flexible authentication enables businesses and organizations to authenticate Enterprise Portal users without having to store user accounts in Active Directory Domain Services.	Deploy an Enterprise Portal site that uses forms-based authentication (http://technet.microsoft.com/en-us/library/hh575253.aspx)

Table 3: Security tasks to enable user access

Task	More information
Verify that the Enterprise Portal site is registered in Microsoft Dynamics AX.	Click **System administration** > **Setup** > **Enterprise Portal** > **Web sites**.
Verify that Microsoft Dynamics AX role-based security is configured. At a minimum, users and groups must be members of the **System user** role.	Set up user and data security in Microsoft Dynamics AX Set up user security in Microsoft Dynamics AX
Grant users and groups permission to view the site in SharePoint.	Enable users to access Enterprise Portal sites (http://technet.microsoft.com/en-us/library/dd309631.aspx)
Specify user relations. User relations trim data based on a user's designated role and account. User relations are required for extranet deployments and for an employee self-service portal. Employees who only access an employee self-service portal must be assigned a **Worker** relation in the **User relations** form.	Specify user relations (http://technet.microsoft.com/en-us/library/dd309687.aspx)
Grant users and groups access to Microsoft SQL Server Reporting Services (SSRS) reports. Users and groups must have this access to view SSRS reports in Enterprise Portal and Role Centers.	Grant users access to reports (http://technet.microsoft.com/en-us/library/aa496432.aspx)
Grant users and groups access to Microsoft SQL Server Analysis Services (SSAS) cubes. Users and groups must have this access to view SSAS reports in Enterprise Portal and Role Centers.	Grant users access to cubes
Configure Enterprise Portal for data partitions.	Configure Enterprise Portal to access data in a partition (http://technet.microsoft.com/en-us/library/jj670113.aspx)

Configure Enterprise Portal to use Secure Sockets Layer

Secure Sockets Layer (SSL) enables web servers and clients to communicate more securely by using encryption. When SSL is not used, data that is sent between the client and server is vulnerable to observation by anyone who has physical access to the network. We recommend that you implement SSL for all Enterprise Portal and Role Center sites. If you are concerned about SSL and site performance, at a minimum, you should implement SSL on all public-facing sites.

Implement SSL

To implement SSL, you must install a certificate and a private encryption key on the web server by using Internet Information Services (IIS) manager. For more information, see How to Setup SSL on IIS 7 (http://go.microsoft.com/fwlink/?LinkId=223135).

Enterprise Search security and protection

This topic describes how Microsoft Dynamics AX restricts access to data, metadata, and documents in Enterprise Search results. If Search is installed by using Setup, users can search in the Microsoft Dynamics AX client or Enterprise Portal. After you install Search, the search box is available in the Microsoft Dynamics AX client. The data that is returned by Search is determined by queries that are listed in the Application Object Tree (AOT) and design features that trim data in Search results.

Note:
In this topic, Search results that include data, metadata, and documents are referred to as *data*.

Application Object Tree queries

Data can only be crawled and indexed for Search if the database table is included in an AOT query in Microsoft Dynamics AX. After the table is specified in a query, the query must be configured for Search. You configure a query for Search by setting the **Searchable** property to **True** in the AOT. By default, only the following queries are configured for Search. These queries are automatically published and indexed after you install Enterprise Search:

- BdcDocuRef
- CustTableListPage
- EcoResProductPerCompanySearch
- HcmWorkerListPage
- SecurityRoleAllTasks
- smmBusinessRelations_NoFilter
- VendorEnterpriseSearch

If you configure queries for Search, you must publish the queries to the SharePoint Business Data Connectivity Service, so that the tables can be crawled and indexed for Microsoft Dynamics AX Enterprise Search. For information about how to publish Microsoft Dynamics AX queries for Search, see Configure Enterprise Search by using the Search Configuration wizard (http://technet.microsoft.com/en-us/library/gg732177.aspx).

Design features that trim data in Search results

The following design features of Microsoft Dynamics AX Enterprise Search help trim data in Search results.

Role-based security

Microsoft Dynamics AX restricts the data that is returned in Search results, based on each user's role in Microsoft Dynamics AX. Role-based security trims data at the level of database tables, records, and fields.

- **Tables** – When a user performs a search, Microsoft Dynamics AX verifies that members of the user's role can view the tables that are listed in the AOT query. If the role does not have permission to view data from a table, Search trims the results. For example, an AOT query includes Table 1 and Table 2, but a user's role only has permission to view data from Table 1. In this case, Search returns data from Table 1 but trims all data from Table 2.
- **Records** – When a user performs a search, Microsoft Dynamics AX verifies that members of the user's role can view the records that are contained in the tables in the AOT query. If the role does not have permission to view one or more records in a table, Search trims the results. For example, an AOT query includes Table 1, a user's role has permission to view data from Table 1, but Table 1 has a record that the user's role is not permitted to view. In this case, Search returns data from Table 1 but trims the data for the restricted record.
- **Variable field access** – Microsoft Dynamics AX excludes a field from Search results if the field has different access permissions for different roles. For example, a record includes a field that is named **Employee Performance Score**. Role 1 can view the field, but Role 2 cannot view the field. In this case, the data in the field is excluded from all Search results. Therefore, **Employee Performance Score** is not displayed in the Search results, regardless of the user who performed the search, because the field is not indexed by Search. Fields that have variable access are not indexed and are therefore not discoverable in Search.

Form references

Tables in the AOT include a **FormRef** property. This property specifies the form that is used in the Microsoft Dynamics AX client to enter data for a specific table. Tables also include a **SearchLinkRefName** property. This property specifies the form that is used in Enterprise Portal to enter data for a specific table. If either of these properties is empty, Search excludes results for form metadata for the corresponding client, the Microsoft Dynamics AX client or Enterprise Portal. For example, an AOT query includes Table 1, and the **FormRef** property is empty for Table 1. In this case, Search results do not include metadata links to the form.

Security and protection for reporting

Security Considerations Creating a Report

This topic describes security considerations for creating Reporting Services reports using the Microsoft Dynamics AX reporting tools.

Data Access

1. When accessing data from the Microsoft Dynamics AX database, it is recommended that you use the predefined Microsoft Dynamics AX data sources to ensure that appropriate security is enforced. For more information about the predefined Dynamics AX data source, see Report Data Overview (http://technet.microsoft.com/en-us/library/cc596629.aspx). When you use the query and report data provider data source types, all data access requests go through the Role and Task security system. When you use an external SQL or OLAP data source, security settings from the Role and Task security system are not applied when accessing data. In this case, you can use the role-based security features that are available from Microsoft SQL Server to secure the data. For more information about the security features from Microsoft SQL Server, see Securing Reports and Resources (http://go.microsoft.com/fwlink/?LinkId=110169) and Securing Reporting Services (http://go.microsoft.com/fwlink/?LinkId=110170) in SQL Server 2008 Books Online.

Extensible Data Security

The extensible data security framework enables you to secure data in shared tables such that users have access to only the part of the table that is allowed by the enforced policy. Extensible data security policies, when deployed, are enforced on Microsoft Dynamics AX reports. For more information, see the Extensible Data Security (http://go.microsoft.com/fwlink/?LinkId=230460) white paper.

Note:
When you bind a report to a report data provider class that writes data to a temp table, apply the XDS policy to the table that contains the source data for the report, not the temp table.

Projects and Build

- When building from the command line, Microsoft Dynamics AX reporting tools does not perform any checks for unsafe entries in the project file. The project file entries are not analyzed by Microsoft Dynamics AX reporting tools from a security perspective. Therefore, it is strongly recommended that you do not build third-party reporting projects from the command line. Build from the command line only in trusted scenarios.
- Microsoft Visual Studio, with the help of MSBuild, analyzes unsafe entries in a project file when it is loaded and warns you about them. An example of an unsafe entry is the redirection of the project output path to a system folder. For example, the output path could be redirected to C:\Windows, which could overwrite a system file. Or, the output path could be redirected so as to overwrite a default MSBuild property for Microsoft Dynamics AX reporting tools projects. When attempting to open a reporting project that contains unsafe entries, a dialog box displays that prompts you not to open the project. If you experience this, you should inspect the unsafe entries as you decide whether to open the project.
- Project files, model files, code files, and referenced assemblies should always be placed in a safe location whether it is a local folder, network share, or source code control database. The default project location for Microsoft Visual Studio projects is \My Documents\Visual Studio 2010\Projects, which is protected by the administrator and current user access control lists.
- Threat detection in a business logic project is limited to the functionality provided by standard C# and Visual Basic project systems in Microsoft Visual Studio. The current implementation of the C# and

Visual Basic project systems displays only the first detected threat in the project file. Therefore, if you skip the threat and load the project file, all other threats that exist in the project file will be skipped.

- The build cache file has an internal binary structure. The first violation of this structure that is discovered will force the compilation to regenerate the file. If the file is modified without violating the structure, the issue will not be mitigated, but you can invoke a clean build to regenerate the build cache file to eliminate the threat.

Assembly Access on a Report Server

- If an administrator grants an assembly access to the SessionManager API (which wraps .NET Business Connector), then the assembly must be given the AxSessionPermissionSet in the rssrvpolicy.config file on the report server.

Note:
This is the recommended setting for business logic assemblies (depending on the main report project name length, either .BusinessLogic.dll or .BL.dll), and it is added by default for the business logic assemblies that are created for a deployed reporting project. This includes the business logic assemblies from referenced reporting projects.

- Giving a custom assembly full trust in the report server security policy file allows the assembly to directly access .NET Business Connector running under the Business Connector proxy account. This is an account that has elevated privileges that allows for access to the LogonAs functionality. In this case, the assembly could impersonate any user and access their records.
- Granting a custom assembly ReflectionPermission with MemberAccess could allow the assembly to retrieve cached sessions from the session cache. Those sessions are logged in for a specific user, and the custom assembly could have access to that user's data.
- The following code must be present in the custom code section of the RDL file if the report is expected to make use of the SessionManager API:

```
Protected Overrides Sub OnInit()
Microsoft.Dynamics.Framework.Reports.SessionManager.BeginRequest(Rep
ort)
End Sub
```

- Entries in the security policy file will not be created for any assemblies referenced by business logic assemblies.

Security settings for reports

To grant users access to reports, you must configure security settings in Microsoft Dynamics AX, Microsoft SQL Server Reporting Services or Microsoft SharePoint, and Microsoft SQL Server Analysis Services. This topic describes the tasks that you must complete in each product.

Configure security settings in Microsoft Dynamics AX

To configure security settings in Microsoft Dynamics AX, complete the following tasks:

- Verify that each Microsoft Dynamics AX role is assigned the correct duties and privileges, so that users (who are assigned to the roles) can access the appropriate reports. For more information, see Create or modify a security role.
- Assign users to Microsoft Dynamics AX roles. For more information, see Assign users to security roles.
- Help secure the data that is displayed on reports. For more information, see Data security in Microsoft Dynamics AX.

Configure security settings in Reporting Services

If you are running Reporting Services in native mode, complete the following tasks to configure security settings in Reporting Services.

Assign users and groups to the DynamicsAXBrowser role

Follow these steps to assign users and groups to the DynamicsAXBrowser role on the Report Manager website.

1. Open the Report Manager website for the Reporting Services instance. By default, the URL is http://[SSRSServerName]:80/Reports_[SSRSInstanceName].
2. Click the **DynamicsAX** folder.
3. Click **Folder Settings**.
4. Click **Security**.
5. Click **New Role Assignment**.
6. Enter the Active Directory user name or group to assign to the DynamicsAXBrowser role.
7. Select the **DynamicsAXBrowser** role.
8. Click **OK**.

Restrict access to report folders and reports

We recommend that you use the security features and tools that are included in Reporting Services to help control access to report folders and published reports. For detailed conceptual information and step-by-step tutorials that can help you administer security in Reporting Services, see the SQL Server documentation.

Configure security settings in SharePoint

If you are running Reporting Services in SharePoint integrated mode, you must grant users permission to view reports in SharePoint. To grant this permission, grant users **Read** permission to the document library that stores the reports. Alternatively, if the document library inherits permissions from the site, you can grant users **Read** permission to the site. The following procedure describes how to grant users **Read** permission to the site.

Important:
If the SharePoint site is configured for claims-based authentication, you must also grant the following accounts **Read** permission to the document library or site:

The account that is used as the Business Connector proxy

The account that is used to run the Microsoft Dynamics AX Application Object Server (AOS) service.

1. Open your browser and navigate to the SharePoint site that contains the document library that stores the reports.
2. Click **Site Actions** > **Site Permissions**.
3. Click **Grant Permissions**. The **Grant Permissions** window is displayed.
4. In the **Users/Groups** field, enter the Active Directory names of the users or groups that you want to view reports.
5. In the **Grant Permissions** area, select the **Grant users permission directly** option.
6. Select the **Read** check box.

   Note:
   If you want Enterprise Portal users to be able to filter reports using a custom parameter value, select the **Design** check box. For more information about the permissions required to use Enterprise Portal, see Enable users to access Enterprise Portal (http://technet.microsoft.com/en-us/library/dd309631.aspx).
7. Click **OK**.

Configure security settings in Analysis Services

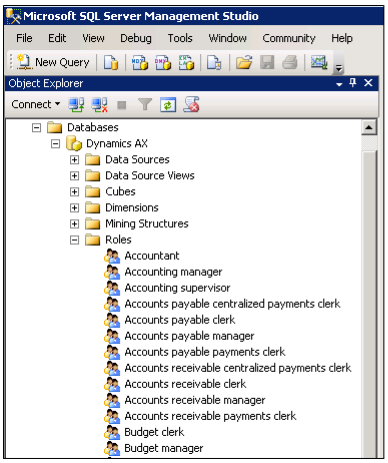
Some reports use Analysis Services cubes to access data. Before users can view data on these reports, you must assign the users to roles in Analysis Services. For more information, see Grant users access to cubes.

Security and protection for analytics

The default security model

Security for analysis cubes is set up independently from security for Microsoft Dynamics AX. To grant users access to cubes, you must assign the users to database roles in Microsoft SQL Server Analysis Services.

When you deploy the cubes that are included with Microsoft Dynamics AX, default roles are created in the database where you deploy the cubes. The following image shows some of these default roles.



To set up security for the cubes, follow these steps:

1. Review Default Analysis Services roles to learn more about the roles that are created in Analysis Services when you deploy the cubes that are included with Microsoft Dynamics AX.
2. Assign users to the Analysis Services roles. For instructions, see Grant users access to cubes.

   Keep in mind that the members of a role have permission to view all data in the cubes that the role has access to. For example, if you assign a user to the **Project supervisor** role, the user has access to all data in the Project accounting cube.

Customizing security for cubes

The members of an Analysis Services role have permission to view all data in the cubes that the role has access to. To help restrict a role's access to specific dimensions and cells in a cube, you can perform customizations. The following topics describe customizations that can help secure Microsoft Dynamics AX cubes:

- Scenario: Help prevent employees of one company from viewing cube data for another company
- Scenario: Help secure cube data so that managers see only the data for their own team
- Scenario: Mapping security in Microsoft Dynamics AX to Analysis Services

The documentation for SQL Server also provides the following topics that explain how to help restrict a role's access to specific dimensions and cells in a cube:

- Granting Dimension Access (http://technet.microsoft.com/en-us/library/ms175421.aspx) explains how to help restrict access to dimensions.
- Granting Custom Access to Dimension Data (http://technet.microsoft.com/en-us/library/ms175366.aspx) explains how to help restrict access to dimension attribute members.
- Granting Custom Access to Cell Data (http://technet.microsoft.com/en-us/library/ms174847.aspx) explains how to help restrict access to cell data.

Caution:
If you modify a default Analysis Services role that is provided by Microsoft Dynamics AX, you may accidentally prevent some members of the role from viewing reports and key performance indicators (KPIs) that those members were intended to view. For more information about the default roles that are included with Microsoft Dynamics AX and the cubes that the roles have access to, see Default Analysis Services roles.

Default Analysis Services roles

Security for analysis cubes is set up independently from security for Microsoft Dynamics AX. To grant users access to cubes, you must assign the users to database roles in Microsoft SQL Server Analysis Services.

When you deploy the cubes that are included with Microsoft Dynamics AX, default roles are created in the database where you deploy the cubes. This topic lists the default roles that are created. Notice that these roles correspond to security roles in Microsoft Dynamics AX. For example, if you assign a user to the **Accountant** role in Microsoft Dynamics AX, you should assign that same user to the **Accountant** role in Analysis Services.

Important:

Keep the following information in mind when assigning users to roles in Analysis Services:

Role members have permission to view all data in the cubes that the role has access to. For example, if you assign a user to the **Project supervisor** role, that user will have access to all data in the Project accounting cube.

The default roles that are created in Analysis Services are not synchronized with the security roles in Microsoft Dynamics AX. For example, if you modify the permissions of the **Accountant** role in Microsoft Dynamics AX, you do not affect the **Accountant** role in Analysis Services.

Analysis Services roles that are created when you deploy the Microsoft Dynamics AX 2012 R2 cubes

When you deploy the cubes that are included with Microsoft Dynamics AX 2012 R2, the following roles are created in the Analysis Services database where you deploy the cubes.

Analysis Services role	Cubes that the role has access to
Accountant	Accounts payable cube Accounts receivable cube General ledger cube Profit tax totals cube Purchase cube Workflow cube
Accounting manager	Accounts payable cube Accounts receivable cube Budget control cube Budget plan cube General ledger cube Profit tax totals cube Purchase cube Retail cube Sales cube Workflow cube
Accounting supervisor	Accounts payable cube Accounts receivable cube Budget control cube Budget plan cube General ledger cube Profit tax totals cube Purchase cube Workflow cube

Analysis Services role	Cubes that the role has access to
Accounts payable centralized payments clerk	Accounts payable cube General ledger cube Purchase cube
Accounts payable clerk	Accounts payable cube Expense management cube General ledger cube Purchase cube
Accounts payable manager	Accounts payable cube Accounts receivable cube Expense management cube General ledger cube Purchase cube Workflow cube
Accounts payable payments clerk	Accounts payable cube General ledger cube
Accounts receivable centralized payments clerk	Accounts receivable cube General ledger cube
Accounts receivable clerk	Accounts receivable cube General ledger cube
Accounts receivable manager	Accounts payable cube Accounts receivable cube General ledger cube Retail cube Sales cube
Accounts receivable payments clerk	Accounts receivable cube General ledger cube
Budget clerk	General ledger cube
Budget manager	Budget control cube Budget plan cube General ledger cube Workflow cube
Buying agent	Purchase cube

Analysis Services role	Cubes that the role has access to
Chief executive officer	Accounts payable cube Accounts receivable cube Budget control cube Budget plan cube Environmental sustainability cube Expense management cube General ledger cube Inventory value cube Production cube Project accounting cube Purchase cube Retail cube Sales and marketing cube Sales cube Workflow cube
Chief financial officer	Accounts payable cube Accounts receivable cube Budget control cube Budget plan cube Expense management cube General ledger cube Inventory value cube Project accounting cube Purchase cube Retail cube Sales cube Workflow cube
Collections agent	Accounts receivable cube General ledger cube
Collections manager	Accounts receivable cube General ledger cube
Compensation and benefits manager	Workflow cube

Analysis Services role	Cubes that the role has access to
Compliance manager	Accounts payable cube Accounts receivable cube Budget control cube Budget plan cube General ledger cube Purchase cube Retail cube Sales cube Workflow cube
Cost accountant	Inventory value cube
Cost clerk	Inventory value cube
Customer service representative	Workflow cube
Environmental manager	Environmental sustainability cube
Field service technician	Workflow cube
Financial controller	Accounts payable cube Accounts receivable cube Budget control cube Budget plan cube Expense management cube General ledger cube Purchase cube Retail cube Sales cube Workflow cube
Human resource assistant	Workflow cube
Human resource manager	Workflow cube
Information technology manager	Workflow cube
Marketing coordinator	Sales and marketing cube
Marketing manager	Sales and marketing cube
Materials manager	Inventory value cube
Product designer	Workflow cube
Production manager	Production cube

Analysis Services role	Cubes that the role has access to
Project accountant	Workflow cube
Project manager	Expense management cube Project accounting cube Purchase cube Workflow cube
Project supervisor	Project accounting cube
Purchasing manager	Accounts payable cube Purchase cube Workflow cube
Receiving clerk	Workflow cube
Retail merchandising manager	Retail cube Sales cube
Retail operations manager	Retail cube Sales cube
Retail store manager	Retail cube Sales cube
Sales manager	Retail cube Sales and marketing cube Sales cube Workflow cube
Sales representative	Sales and marketing cube
Treasurer	Accounts payable cube General ledger cube Workflow cube
Vendor account manager	Workflow cube
Warehouse manager	Inventory value cube Retail cube Sales cube

Analysis Services roles that are created when you deploy the Microsoft Dynamics AX 2012 Feature Pack cubes

When you deploy the cubes that are included with Microsoft Dynamics AX 2012 Feature Pack, the following roles are created in the Analysis Services database where you deploy the cubes.

Analysis Services role	Cubes that the role has access to
Accountant	Accounts payable cube Accounts receivable cube General ledger cube Purchase cube Workflow cube
Accounting manager	Accounts payable cube Accounts receivable cube General ledger cube Purchase cube Sales cube Workflow cube
Accounting supervisor	Accounts payable cube Accounts receivable cube General ledger cube Purchase cube Workflow cube
Accounts payable centralized payments clerk	Accounts payable cube General ledger cube Purchase cube
Accounts payable clerk	Accounts payable cube Expense management cube General ledger cube Purchase cube
Accounts payable manager	Accounts payable cube Accounts receivable cube Expense management cube General ledger cube Purchase cube Workflow cube
Accounts payable payments clerk	Accounts payable cube General ledger cube
Accounts receivable centralized payments clerk	Accounts receivable cube General ledger cube

Analysis Services role	Cubes that the role has access to
Accounts receivable clerk	Accounts receivable cube General ledger cube
Accounts receivable manager	Accounts payable cube Accounts receivable cube General ledger cube Sales cube
Accounts receivable payments clerk	Accounts receivable cube General ledger cube
Budget clerk	General ledger cube
Budget manager	General ledger cube Workflow cube
Buying agent	Purchase cube
Chief executive officer	Accounts payable cube Accounts receivable cube Customer relationship management cube Environmental sustainability cube Expense management cube General ledger cube Production cube Project accounting cube Purchase cube Sales cube Workflow cube
Chief financial officer	Accounts payable cube Accounts receivable cube Expense management cube General ledger cube Project accounting cube Purchase cube Sales cube Workflow cube
Collections agent	Accounts receivable cube General ledger cube

Analysis Services role	Cubes that the role has access to
Collections manager	Accounts receivable cube General ledger cube
Compensation and benefits manager	Workflow cube
Compliance manager	Accounts payable cube Accounts receivable cube General ledger cube Purchase cube Sales cube Workflow cube
Customer service representative	Workflow cube
Environmental manager	Environmental sustainability cube
Field service technician	Workflow cube
Financial controller	Accounts payable cube Accounts receivable cube Expense management cube General ledger cube Purchase cube Sales cube Workflow cube
Human resource assistant	Workflow cube
Human resource manager	Workflow cube
Information technology manager	Workflow cube
Marketing coordinator	Customer relationship management cube
Marketing manager	Customer relationship management cube
Product designer	Workflow cube
Production manager	Production cube
Project accountant	Workflow cube
Project manager	Expense management cube Project accounting cube Purchase cube Workflow cube
Project supervisor	Project accounting cube

Analysis Services role	Cubes that the role has access to
Purchasing manager	Accounts payable cube Purchase cube Workflow cube
Receiving clerk	Workflow cube
Retail merchandising manager	Sales cube
Retail operations manager	Sales cube
Retail store manager	Sales cube
Sales manager	Customer relationship management cube Sales cube Workflow cube
Sales representative	Customer relationship management cube
Treasurer	Accounts payable cube General ledger cube Workflow cube
Vendor account manager	Workflow cube

Analysis Services roles that are created when you deploy the Microsoft Dynamics AX 2012 cubes

When you deploy the cubes that are included with the initial release of Microsoft Dynamics AX 2012, the following roles are created in the Analysis Services database where you deploy the cubes.

Analysis Services role	Cubes that the role has access to
Accountant	Accounts payable cube Accounts receivable cube General ledger cube Purchase cube Workflow cube
Accounting manager	Accounts payable cube Accounts receivable cube General ledger cube Purchase cube Sales cube Workflow cube

Analysis Services role	Cubes that the role has access to
Accounting supervisor	Accounts payable cube Accounts receivable cube General ledger cube Purchase cube Workflow cube
Accounts payable centralized payments clerk	Accounts payable cube General ledger cube Purchase cube
Accounts payable clerk	Accounts payable cube Expense management cube General ledger cube Purchase cube
Accounts payable manager	Accounts payable cube Accounts receivable cube Expense management cube General ledger cube Purchase cube Workflow cube
Accounts payable payments clerk	Accounts payable cube General ledger cube
Accounts receivable centralized payments clerk	Accounts receivable cube General ledger cube
Accounts receivable clerk	Accounts receivable cube General ledger cube
Accounts receivable manager	Accounts payable cube Accounts receivable cube General ledger cube Sales cube
Accounts receivable payments clerk	Accounts receivable cube General ledger cube
Budget clerk	General ledger cube
Budget manager	General ledger cube Workflow cube

Analysis Services role	Cubes that the role has access to
Buying agent	Purchase cube
Chief executive officer	Accounts payable cube Accounts receivable cube Customer relationship management cube Environmental sustainability cube Expense management cube General ledger cube Production cube Project accounting cube Purchase cube Sales cube Workflow cube
Chief financial officer	Accounts payable cube Accounts receivable cube Expense management cube General ledger cube Project accounting cube Purchase cube Sales cube Workflow cube
Collections agent	Accounts receivable cube General ledger cube
Collections manager	Accounts receivable cube General ledger cube
Compensation and benefits manager	Workflow cube
Compliance manager	Accounts payable cube Accounts receivable cube General ledger cube Purchase cube Sales cube Workflow cube
Customer service representative	Workflow cube
Environmental manager	Environmental sustainability cube
Field service technician	Workflow cube

Analysis Services role	Cubes that the role has access to
Financial controller	Accounts payable cube Accounts receivable cube Expense management cube General ledger cube Purchase cube Sales cube Workflow cube
Human resource assistant	Workflow cube
Human resource manager	Workflow cube
Information technology manager	Workflow cube
Marketing coordinator	Customer relationship management cube
Marketing manager	Customer relationship management cube
Product designer	Workflow cube
Production manager	Production cube
Project accountant	Workflow cube
Project manager	Expense management cube Project accounting cube Purchase cube Workflow cube
Project supervisor	Project accounting cube
Purchasing manager	Accounts payable cube Purchase cube Workflow cube
Receiving clerk	Workflow cube
Sales manager	Customer relationship management cube Sales cube Workflow cube
Sales representative	Customer relationship management cube
Treasurer	Accounts payable cube General ledger cube Workflow cube
Vendor account manager	Workflow cube

Grant users access to cubes

Security for analysis cubes is set up independently from security for Microsoft Dynamics AX. To grant users access to cubes, you must assign the users to database roles in Microsoft SQL Server Analysis Services.

When you deploy the cubes that are included with Microsoft Dynamics AX, default roles are created in the database where you deploy the cubes. The following procedures explain how you can assign users to these default roles.

Important:
Keep the following information in mind when assigning users to roles in Analysis Services:

Role members have permission to view all data in the cubes that the role has access to. For example, if you assign a user to the **Project supervisor** role, that user will have access to all data in the Project accounting cube.

The default roles that are created in Analysis Services are not synchronized with the security roles in Microsoft Dynamics AX. For example, if you modify the permissions of the **Accountant** role in Microsoft Dynamics AX, it does not affect the **Accountant** role in Analysis Services.

Assign users to a database role

Complete the following procedure to assign users to a database role.

1. In SQL Server Management Studio, connect to your Analysis Services instance.
2. In the tree view, expand the **Databases** > **[Database Name]** > **Roles** node.
3. Right-click the appropriate role, and then click **Properties**. The **Edit Role – [Role Name]** form is displayed.
4. In the **Select a page** area, click **Membership**.
5. Click **Add**. The **Select Users or Groups** form is displayed.
6. Add the appropriate Active Directory users or user groups to this role.
   - To add an Active Directory user to the role, enter the user's name in the following format: [DomainName]\[UserName]. Click **OK**.
   - To add an Active Directory group to the role, complete the following steps:
     i. Click **Object Types**.
     ii. In the **Object Types** form, select the **Groups** check box. Click **OK**.
     iii. The **Select Users or Groups** form is redisplayed. Enter the name of the user group in the following format: [DomainName]\[UserGroupName]. Click **OK**.

Notes:
Analysis Services supports Windows authentication only. Users who do not have Active Directory accounts will not be able to access cube data. This means that users who access Enterprise Portal for Microsoft Dynamics AX using claims-based authentication will not be able to view cube data in reports and web parts.

If you configure Enterprise Portal to use claims-based authentication, you should remove the reports and web parts that were designed to display cube data. For more information about

using claims-based authentication with Enterprise Portal, see Flexible Authentication in Microsoft Dynamics AX 2012 (http://technet.microsoft.com/en-us/library/jj860379.aspx).

Specify which cubes a database role has access to

Complete the following procedure to specify which cubes a database role has access to. To see a list of the cubes each role has access to by default, see Default Analysis Services roles.

1. In SQL Server Management Studio, connect to your Analysis Services instance.
2. In the tree view, expand the **Databases** > **[Database Name]** > **Roles** node.
3. Right-click the appropriate role, and then click **Properties**. The **Edit Role – [Role Name]** form is displayed.
4. In the **Select a page** area, click **Cubes**. A list of the cubes that are contained in the database is displayed.
5. In the **Access** column, specify the type of access that you want the selected role to have for each cube. You can select **None**, **Read**, or **Read/Write**.
6. Click **OK**.

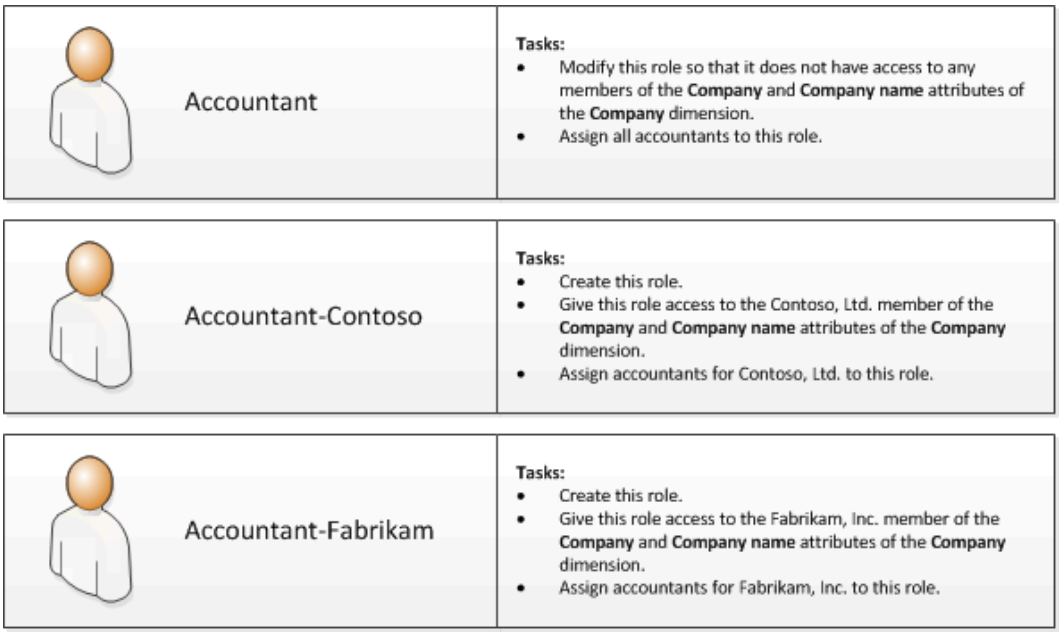
Scenarios regarding cube security

The following topics describe customization options that can help secure Microsoft Dynamics AX cubes.

Scenario: Help prevent employees of one company from viewing cube data for another company

Your organization may consist of several companies. To help prevent employees of one company from viewing the data for another company by using cubes, we recommend that you create a role for each company in Microsoft SQL Server Analysis Services.

For example, assume that your organization consists of two companies: Contoso, Ltd. and Fabrikam, Inc. You want to prevent accountants in one company from viewing the data for the other company. Therefore, you should modify the default Accountant role and create a new role for each company. The following illustration provides an overview of the tasks that you need to complete.



The following sections describe the procedures that you must complete for each role in this scenario.

Accountant role

The Accountant role was automatically created in the Analysis Services database that you deployed the Microsoft Dynamics AX cubes to. By default, the Accountant role has access to data for all companies. Follow these steps to prevent users who are assigned to the Accountant role from accessing company-specific data.

1. In SQL Server Management Studio, connect to your instance of Analysis Services.
2. In the tree view, expand the **Databases** > **[Database Name]** > **Roles** node.
3. Right-click the **Accountant** role, and then click **Properties**. The **Edit Role – Accountant** form is displayed.
4. In the **Select a page** area, click **Dimension Data**.
5. In the **Dimension** list, select **Company**.
6. In the **Attribute Hierarchy** list, select **Company**.
7. Click **Deselect all members**.
8. In the **Attribute Hierarchy** list, select **Company name**.
9. Click **Deselect all members**.
10. Click **OK**.
11. Assign all your accountants to the Accountant role. For instructions about how to assign users to this role, see Grant users access to cubes.

Accountant-Contoso role

Follow these steps to create a new role that is named Accountant-Contoso. This role has access to data for the Contoso, Ltd. company only.

1. Create the Accountant-Contoso role in Analysis Services.

   For information about how to create the role, see the SQL Server documentation on TechNet or MSDN.
2. Give the role access to the Contoso, Ltd. company by following these steps:
   a. Right-click the **Accountant-Contoso** role, and then click **Properties**. The **Edit Role – Accountant-Contoso** form is displayed.
   b. In the **Select a page** area, click **Dimension Data**.
   c. In the **Dimension** list, select **Company**.
   d. In the **Attribute Hierarchy** list, select **Company**.
   e. Select the check box for Contoso, Ltd. Then clear all other check boxes.
   f. In the **Attribute Hierarchy** list, select **Company name**.
   g. Select the check box for Contoso, Ltd. Then clear all other check boxes.
   h. Click **OK**.
3. Assign the accountants for Contoso, Ltd. to the Accountant-Contoso role.

Accountant-Fabrikam role

Follow these steps to create a new role that is named Accountant-Fabrikam. This role has access to data for the Fabrikam, Inc. company only.

1. Create the Accountant-Fabrikam role in Analysis Services.

   For information about how to create the role, see the SQL Server documentation on TechNet or MSDN.
2. Give the role access to the Fabrikam, Inc. company by following these steps:
   a. Right-click the **Accountant-Fabrikam** role, and then click **Properties**. The **Edit Role – Accountant-Fabrikam** form is displayed.
   b. In the **Select a page** area, click **Dimension Data**.
   c. In the **Dimension** list, select **Company**.
   d. In the **Attribute Hierarchy** list, select **Company**.
   e. Select the check box for Fabrikam, Inc. Then clear all other check boxes.
   f. In the **Attribute Hierarchy** list, select **Company name**.
   g. Select the check box for Fabrikam, Inc. Then clear all other check boxes.
   h. Click **OK**.
3. Assign the accountants for Fabrikam, Inc. to the Accountant-Fabrikam role.

See Also

Granting Dimension Access (http://technet.microsoft.com/en-us/library/ms175421.aspx)

Granting Custom Access to Dimension Data (http://technet.microsoft.com/en-us/library/ms175366.aspx)

Scenario: Help secure cube data so that managers see only the data for their own team

Some managers in your organization may want to use cube data to track and analyze data for their teams. The following sections provide options for implementing security in this scenario.

Option: Use dynamic security

To implement security so that a manager has access only to the data for his or her own team, use dynamic security practices. For an example of these practices, see the Dynamic Security in SSAS cube (http://blogs.msdn.com/b/azazr/archive/2008/08/15/dynamic-security-in-ssas-cube.aspx) blog post.

Option: Create a new role for a specific manager

Some managers in your organization may want to use cube data to track and analyze expenses for their teams. For example, suppose that Ann is a manager in your organization, and she wants to create pivot tables to analyze expenses for her team. The following procedure explains how to create a manager role for Ann in Microsoft SQL Server Analysis Services. The procedure explains how to create the role, grant the role access to the Expense management cube, and restrict the role to the data for Ann's team.

1. In SQL Server Management Studio, connect to your instance of Analysis Services.
2. In the tree view, expand the **Databases** > **[Database Name]** > **Roles** node.
3. Right-click the **Roles** node, and then click **New Role**. The **Create Role** window is displayed.
4. In the left pane, click **General**. Then follow these steps:
    a. Enter a name for the role. For this example, enter **Manager-Ann**.
    b. Enter a description of the role.
    c. Select the **Read definition** check box.
5. In the left pane, click **Membership**. Then follow these steps:
    a. Click **Add**. The **Select Users or Groups** form is displayed.
    b. Enter Ann's name in the following format: [DomainName]\[UserName]. Click **OK**.
6. In the left pane, click **Cubes**. To give Ann access to expense information, follow these steps:
    a. In the **Expense management cube** row, select the **Access** cell.
    b. In the list, select **Read**.
7. In the left pane, click **Dimension Data**. To give Ann access to expense information only for the employees on her team, follow these steps:
    a. In the **Dimension** list, select **Worker**.
    b. In the **Attribute Hierarchy** list, select **Personnel number**. Then select the personnel numbers that are associated with the employees on Ann's team.
    c. In the **Attribute Hierarchy** list, select **Worker - Name**. Then select the names of the employees on Ann's team.
    d. In the **Attribute Hierarchy** list, select **Worker**. Then select the names of the employees on Ann's team.

Ann can now create pivot tables to analyze expenses for her team. For more information about how to create pivot table reports, see Create a report by using the Excel data connection wizard to connect to a cube (http://technet.microsoft.com/en-us/library/gg243095.aspx).

Scenario: Mapping security in Microsoft Dynamics AX to Analysis Services

Security for analysis cubes is set up independently of security for Microsoft Dynamics AX. This topic describes methods that you can use to map the security that you implemented in Microsoft Dynamics AX to security in Microsoft SQL Server Analysis Services.

Mapping Microsoft Dynamics AX roles to Analysis Services roles

When you deploy the cubes that are included with Microsoft Dynamics AX, default roles are created in the Analysis Services database where you deploy the cubes. These roles correspond to roles in Microsoft Dynamics AX. If you assign a user to a specific role in Microsoft Dynamics AX, you should assign that user to the corresponding role in Analysis Services. For example, if you assign a user to the **Accountant** role in Microsoft Dynamics AX, assign that user to the **Accountant** role in Analysis Services. For a list of the default roles that are created in Analysis Services, see Default Analysis Services roles.

Determining which Microsoft Dynamics AX roles have access to privileges and duties

Microsoft Dynamics AX has a role-based security model. The security model is hierarchical, and each element in the hierarchy represents a different level of detail. Permissions represent access to individual securable objects, such as menu items and tables. *Privileges* are composed of permissions and represent access to tasks, such as viewing a report. *Duties* are composed of privileges and represent parts of a business process, such as maintaining bank transactions. Both duties and privileges can be assigned to roles to grant access to Microsoft Dynamics AX. For more information about the security model for Microsoft Dynamics AX, see Role-based security in Microsoft Dynamics AX.

For example, assume that you have created or modified privileges and duties in Microsoft Dynamics AX. The following procedures explain how to determine which Microsoft Dynamics AX roles have been assigned to specific privileges and duties. You can then assign users to corresponding roles in Analysis Services.

Determine which roles have access to a privilege

Follow these steps to determine which roles in Microsoft Dynamics AX have access to a privilege.

1. Open Microsoft Dynamics AX.
2. Click the **Windows** icon, which is located in the upper-right corner. Then click **New Development Workspace**. The Application Object Tree (AOT) is displayed.
3. Expand the **Security** > **Privileges** node.
4. Right-click a privilege, and then click **Add-Ins** > **Security tools** > **View related security roles**.

   The **Roles** form is displayed. This form lists the Microsoft Dynamics AX roles that have access to the privilege.
5. Assign the users in those Microsoft Dynamics AX roles to corresponding roles in Analysis Services. For information about how to assign users to roles in Analysis Services, see Grant users access to cubes.

Determine which roles have access to a duty

Follow these steps to determine which roles in Microsoft Dynamics AX have access to a duty.

1. Open Microsoft Dynamics AX.
2. Click the **Windows** icon, which is located in the upper-right corner. Then click **New Development Workspace**. The AOT is displayed.
3. Expand the **Security** > **Duties** node.
4. Right-click a duty, and then click **Add-Ins** > **Security tools** > **View related security roles**.

The **Roles** form is displayed. This form lists the Microsoft Dynamics AX roles that have access to the duty.

5. Assign the users in those Microsoft Dynamics AX roles to corresponding roles in Analysis Services. For information about how to assign users to roles in Analysis Services, see Grant users access to cubes.

Services and AIF security and protection

The topics in this section provide information about security for Microsoft Dynamics AX services and Application Integration Framework (AIF).

About role-based security in services and AIF

Security for Microsoft Dynamics AX services and Application Integration Framework (AIF) is based on the role-based security that is used in Microsoft Dynamics AX. For an overview of role-based security in Microsoft Dynamics AX, see Role-based security in Microsoft Dynamics AX. This topic describes how services and AIF help enforce security requirements through users, roles, duties, and privileges.

AIF users

The following types of user can work with services and AIF.

Submitting user

The submitting user submits the message to Microsoft Dynamics AX. The submitting user must be an authenticated Microsoft Dynamics AX user.

The following table explains the process that AIF uses to determine the submitting user.

Data exchange method	Submitting user
File system adapter	The submitting user is the owner of the message request file as returned by the Windows GetFileSecurity (OWNER_SECURITY_INFORMATION) function. You can specify a default message owner that AIF uses when file ownership cannot be resolved deterministically. See Configure addresses for enhanced integration ports (http://technet.microsoft.com/en-us/library/hh202051.aspx).
MSMQ adapter	The submitting user is the sender of the message as set on the SenderId property of the message.
Web services	The submitting user is the Windows identity of the caller.

Authorized port user

When you configure an integration port, you can restrict access to the port to a list of authorized users. For information about how to restrict users to authorized users, see Configure security for integration ports (http://technet.microsoft.com/en-us/library/hh202131.aspx).

Claims user

A claims user is a type of Microsoft Dynamics AX user. Claims users are authenticated by an external system, not by Application Object Server (AOS). To gain authorization to access services, a claims user must be authenticated, and then impersonated by a trusted intermediary user. See the next section.

Trusted intermediary user

Trusted intermediaries are typically used for business-to-business data exchanges. A trusted intermediary is a type of submitting user that can act on behalf of another user, such as a claims user. A trusted intermediary is not a type of Microsoft Dynamics AX user. Instead, trusted intermediaries are typically middleware applications, such as Microsoft BizTalk Server or Electronic Data Interchange (EDI) services. These applications are represented by Microsoft Dynamics AX users or user groups that are authorized to submit inbound requests to an integration port. By using trusted intermediaries, you can delegate authentication to a trusted source, whereas authorization continues to be managed by Microsoft Dynamics AX through the role-based security framework.

Trusted intermediaries are associated with integration ports. You can define custom intermediaries when you configure an integration port. For information about how to configure integration ports to use trusted intermediaries, see Configure security for integration ports (http://technet.microsoft.com/en-us/library/hh202131.aspx).

A trusted intermediary must always be an Active Directory user, never a claims user. A trusted intermediary can impersonate any other Microsoft Dynamics AX user, even a claims user. When the submitting user is a trusted intermediary, AIF provides authorization to the user that is defined in the message header by the `<LogonAsUser>` element. Otherwise, this element is ignored.

Important:
When you use a trusted intermediary, make sure that the trusted intermediary represents a known, valid partner or a trusted system.

Proxy user

If a proxy is used, .NET Business Connector can connect on behalf of Microsoft Dynamics AX users when authentication is performed by an AOS instance. For more information, see Specify the .NET Business Connector proxy account (http://technet.microsoft.com/en-us/library/aa496652.aspx).

Roles, duties, and privileges

Users who have the roles that are described in the following table can configure integration port settings for services and AIF.

Role	AOT name	Description
Information technology manager	**SysServerITManager**	This role has the following two duties that are related to services and AIF: • **AifIntegrationMaintain**, which provides the privileges that are required for typical AIF tasks, such as configuring integration ports, viewing the message queue, and reviewing history information. • **AifSyncConfigure**, which provides the privileges that are required to configure document filters.
System administrator	**-SYSADMIN-**	A user who has this role is a super user, and therefore has full permission for every operation in Microsoft Dynamics AX.

Every service operation is associated with an entry point privilege. This privilege provides permissions for the tables that the service reads or modifies. For example, the **SalesSalesOrderServiceCreate** service operation is associated with the **SalesSalesOrderServiceCreate** privilege. The **ServiceOperation** duty provides privileges for all service operations. Other duties provide privileges for specific service operations, depending on the responsibilities of the duty and its associated roles. For example, among the privileges that the **DOCommerceOnlineSalesOrderMaintain** duty provides is the **SalesSalesOrderServiceCreate** privilege.

To understand the relationships between roles, duties, privileges, and permissions, see the **Security** node of the Application Object Tree (AOT).

Security best practices for services and AIF

It is very important that you maintain data security when you use services and Application Integration Framework (AIF) to exchange data with other systems. Follow the security-related recommendations in this topic when you configure AIF. For more information about security and web services in AIF, see Security architecture for Web services.

Security best practices

- When configuring your system to accept data by using the file system adapter, make sure that only trusted users authorized by the system administrator have the right to take ownership of the files containing inbound messages.

  For asynchronous requests that use the file system adapter, AIF uses the file owner as the submitting user to process the request. The service is executed in the context of the submitting user if a separate logon user is not specified on the **Inbound ports** form. Windows Server 2008 allows a user with sufficient user rights to change the owner of a file to some other user. The service request will then be executed as the other user.

To prevent this elevation of privilege, you should not grant the user right of **Take ownership of files or other objects** and **Restore files and directories** to non-administrator users in your production environment.

Note:
You can avoid any change in file ownership by using a Uniform Naming Convention (UNC) path to specify the location of the file adapter. Ownership of files cannot be changed if you use a UNC path.

For more information, see Configure addresses for enhanced integration ports (http://technet.microsoft.com/en-us/library/hh202051.aspx) and Managing Object Ownership (http://technet.microsoft.com/en-us/library/cc732983).

- Make sure that data that is sent to and from AIF integration ports is encrypted and can be accessed only by authenticated and authorized users. All data transmissions must be secured, so that no one can read or modify the data during transmission. Authentication and encryption are especially important for business-to-business scenarios in which data is transmitted over the public Internet. For HTTP ports, you can add HTTPS settings through Internet Information Services (IIS).
- When you transmit messages by using the file system adapter or the MSMQ adapter, make sure that the file shares and queues themselves are secured and can be accessed only by authorized users. You can help secure the file shares and queues by using specialized security software that encrypts data and guarantees that only authorized users can access a file location.
- The Microsoft Dynamics AX system administrator must restrict access to AIF by assigning users only to the roles that those users require. See About role-based security in services and AIF.
- Be aware that all actions in Microsoft Dynamics AX that involve inbound documents are performed in the context of a valid Microsoft Dynamics AX user. For information about how AIF determines the submitting user, see About role-based security in services and AIF.
- Be sure to help secure the location on the file system to which you export messages from the **Queue manager** form. These messages may contain confidential information.
- Restrict the use of integration ports to authorized users and companies. In this way, an integration port can send or receive data only for specific customers, vendors, or warehouses, and you can avoid spoofing attacks. Trusted intermediary users can submit AIF requests on behalf of authorized port users. See Configure security for integration ports (http://technet.microsoft.com/en-us/library/hh202131.aspx).

In Microsoft Dynamics AX 2012 R2, you must restrict an inbound port to a partition before you can restrict the port to a company. Each company in Microsoft Dynamics AX 2012 R2 exists in one data partition, although one data partition can contain more than one company. For more information about data partitions, see Data partitioning architecture (http://technet.microsoft.com/EN-US/library/jj728665.aspx).

- To restrict the data fields that can be read or modified through an integration port, use data policies. For information about how to configure data policies, see Customize service contracts (http://technet.microsoft.com/en-us/library/hh202119.aspx).
- Add external components only from a trusted and reliable source, such as a Microsoft Partner or an independent software vendor (ISV). External components include document classes, adapter classes, and pipeline components. Pipeline components are X++ classes that are called during processing of the AIF pipeline.

- Before you add an Extensible Stylesheet Language Transformation (XSLT) as part of pipeline processing, make sure that the XSLT is secured. Also make sure that the XSLT can handle documents that contain incorrect or malicious data. Thoroughly test any transformations to make sure that they do not contain code that can run and cause exploitable errors on the system.
- By default, scripting is disabled on the component that is used for XSLT transforms, to help protect the system against scripting attacks. For information about how to enable scripting, see Configure processing options (http://msdn.microsoft.com/en-us/library/hh202050.aspx).

Security best practices for web services

Follow these additional security-related recommendations when you configure AIF web services:

- By default, AIF web services implement the basicHttpBinding binding. This binding is configured to use the message-level security that is offered through Windows Communication Foundation (WCF). We recommend that administrators follow the standard WCF configuration in IIS. For more information about security in WCF, see Securing Services (http://go.microsoft.com/fwlink/?LinkId=102986).
- Restrict access to the files for AIF web services. When AIF web services are installed, Setup creates a network share to the content directory where the files for AIF web services are located. We recommend that you restrict access to this network share.
    a. Open the Computer Management application. Click **Start** > **Administrative Tools** > **Computer Management**.
    b. Under **Local Users and Groups**, click the **Groups** folder.
    c. Right-click the **Microsoft Dynamics AX Web Service Administrators** local group, and then select **Properties**.
    d. In the **Members** field, verify that only accounts for Application Object Server (AOS) are members of the group.
    e. If you are using the default permissions in Windows Server 2008, all domain users have Read and Execute permissions for the content directory where the web services are installed. For more information, see the Default local groups (http://go.microsoft.com/fwlink/?LinkId=227787) article on TechNet. If you are not using default permissions, you may have to grant access to the share by using one of the following methods:
- Create a local Windows group that has access to the directory, and then add users of AIF web services to this group.
- Add users of AIF web services to the local **Users** group of the computer.
- All data that is exchanged with external web services must be exchanged over secure channels to prevent tampering, spoofing, and so on. Data is exchanged with external web services when, for example, an external web service is consumed from X++. We recommend that confidential and business-critical information be exchanged with external web services only through communication channels that provide secure authentication, message confidentiality, and integrity.
- Never consume unknown or untrusted external web services. When you consume a web service, always make sure that the service that is consumed is the correct service. To verify the identity of web services that you consume, use a secure identification and authentication mechanism.

Security architecture for Web services

Application Integration Framework (AIF) supports Web services for Windows Communication Foundation (WCF). In AIF, each document is represented by a service that can be exposed from an integration port. To consume services over the Internet, you must host services on Internet Information Services (IIS). AIF uses standard WCF processing to receive and process SOAP requests. For information about how to install Web services on IIS, see Install web services on IIS (http://technet.microsoft.com/en-us/library/gg731848.aspx).

Security architecture for Web services

Security in AIF is enforced through a combination of WCF, IIS, Active Directory, and role-based security in Microsoft Dynamics AX.

1. The client calls a service method, such as the Customer.read method, and passes the entity key of the requested customer in a SOAP message.
2. The request is received by the IIS where the AIF services are hosted. IIS retrieves the user credentials, depending on the authentication mechanism that is specified in the service configuration. IIS then tries to map the security credentials to a valid domain user. By default, Microsoft Dynamics AX configures WCF to use the basicHttpBinding binding and message security, so that the user credentials are contained in the message's SOAP header. IIS authenticates the user as a valid user in Active Directory.
3. The request is passed to AIF, which performs additional authentication by verifying that the user meets the following criteria:
   - The user is a valid Microsoft Dynamics AX user.
   - The user has the appropriate permissions, through role-based security, to start the operation.
4. After AIF determines that the user has access to the service, the message is processed. At run time, standard AIF security guarantees that the user has access to the data that is exposed by the service.

Retail PCI security compliance

Special security and compliance provisions apply to Retail deployments of Microsoft Dynamics AX 2012 that use credit or debit cards. For guidance in this area, consult the PCI Implementation Guide for Microsoft Dynamics AX 2012 R2 (http://www.microsoft.com/en-us/download/confirmation.aspx?id=36537), available for download as a PDF file.

Set up user security in Microsoft Dynamics AX

This section describes security concepts, and explains how to set up and maintain user security in Microsoft Dynamics AX. The following topics are included:

What's New: User security

This topic describes the enhancements to security in Microsoft Dynamics AX 2012.

Role-based security

In previous releases of Microsoft Dynamics AX, managing security could be a lengthy and difficult process. Microsoft Dynamics AX 2012 introduces role-based security, which makes security easier to manage by providing the following benefits:

- **Security that is aligned with your business**

  In previous releases, Microsoft Dynamics AX administrators had to create their own user groups and manually assign users to those groups. To grant a user group permission to perform a particular operation, the administrator had to identify the application objects, such as tables, fields, and menu items, that were required for the operation. Identifying these elements could be a difficult and lengthy process. When a person changed jobs, the administrator had to manually update that person's permissions in Microsoft Dynamics AX.

  In Microsoft Dynamics AX 2012, security is role-based, and many security roles are predefined to make security easier to set up. In role-based security, users are assigned to roles based on their responsibilities in the organization and their participation in business processes. The administrator no longer has to identify application objects and grant access to those objects. Instead, the administrator grants access to the duties that users in a role perform. Because rules can be set up for automatic role assignment, the administrator does not have to be involved every time that a user's responsibilities change. After security roles and rules have been set up, role assignments can be updated based on changes in business data.

- **Reusable permissions**

  In previous releases, user groups could not span multiple companies. If the same functional role was required in two companies, the administrator had to create two user groups. Therefore, the number of user groups could grow quickly. For example, in a business with 50 functional roles in 50 companies, the administrator had to create and manage 2500 user groups to appropriately assign permissions.

  In Microsoft Dynamics AX 2012, a single set of roles applies across all organizations. The administrator no longer has to create and maintain separate user groups for each organization.

  Although roles themselves are not specific to an organization, the administrator can still assign a user to a role in specific organizations.

- **Default and sample security definitions**

In previous releases, security was not defined by default. Administrators had to create their own user groups and grant those groups access to application objects. In Microsoft Dynamics AX 2012, permissions for all application objects have been grouped into task-based privileges and duties. For example, the administrator no longer has to grant access to the **Create sales order** form and all of the related application objects. Instead, the administrator can grant access to the **Maintain sales order** duty, which includes all of the permissions that are required to view, create, modify, and delete sales orders.

Sample security roles and duties also make security easier to set up. Roles and duties are provided for every area of Microsoft Dynamics AX, and relevant privileges are assigned to these roles and duties by default. You can use the sample security roles and duties as they are, modify them to fit the needs of your business, or create new security roles and duties.

Note:
By default, program access is defined for the default security roles. However, no data restrictions are applied by default.

- **Compliance and auditing**

  In previous releases, administrators had to manually audit for compliance. There were no built-in features to help prevent fraud and guarantee compliance.

  Role-based security in Microsoft Dynamics AX 2012 is easier to audit, because fewer security objects are assigned to fewer groups of users. In addition, because of the concept of roles and duties, you can audit for compliance based on business activities instead of program elements.

  In Microsoft Dynamics AX 2012, you can set up rules for the segregation of duties to guarantee that a user does not have access to conflicting duties. For example, you can set up a rule that specifies that one person cannot both acknowledge the receipt of goods and pay the vendor.

For more information, see Role-based security in Microsoft Dynamics AX and Set up segregation of duties.

Extensible data security framework

The extensible data security framework provides the following benefits to the system administrator who helps secure data in Microsoft Dynamics AX 2012:

- **Improved filters for data security**

  In previous releases, the record-level security feature was used to help secure the data. The filters that were used for record-level security could not be based on fields that were contained in a separate table from the data that was being filtered. For example, to filter sales lines, you could not use the customer location, because the customer location field is not contained in the sales line table. In addition, record-level security was enforced only through the client interface.

  In Microsoft Dynamics AX 2012, the extensible data security framework can be used to help secure the data. By using the new framework, you can create data security policies that are based on data that is contained in a different table. Data security policies are enforced at the server, regardless of the type of client that is used to access the data. In addition, policies can take security privileges into account. For example, the administrator can grant View access to one subset of sales orders and Edit access to another subset of sales orders.

Caution:
The record-level security feature is still available in Microsoft Dynamics AX 2012, but it will become obsolete in a future release. Filters that you previously set up for record-level security can still be used. If you set up new filters, we recommend that you create data security policies by using the extensible data security framework.

- **Data security that is based on effective dates**

  In Microsoft Dynamics AX 2012, you can specify whether the users in a role have access to past, present, or future records. A user can also have different levels of access based on effective dates. For example, a user can have access to view past records, and access to create and edit present records.

For more information, see Data security in Microsoft Dynamics AX.

Server enforcement of security

In previous releases, authorization was performed primarily on the client. Therefore, permissions could be validated differently by the Windows client, the Enterprise Portal for Microsoft Dynamics AX client, and other types of client.

The addition of the Table Permissions Framework (TPF) to some tables in Microsoft Dynamics AX 4.0 and Microsoft Dynamics AX 2009 shifted some authorization to the server. However, TPF permissions were applied at the table level, not at the field level. Therefore, TPF could be used to deny users access to whole records, but could not be used to deny access to specific fields that were associated with a record. To limit access to fields, the administrator could set up permissions to show or hide the fields in client forms. However, because all data was sent to the client, tables that were not protected by TPF could be freely accessed by code, regardless of the user's permissions.

In Microsoft Dynamics AX 2012, because TPF permissions can be applied at the field level, more authorization is performed on the server. Therefore, permissions on protected fields are consistently enforced, regardless of the type of client.

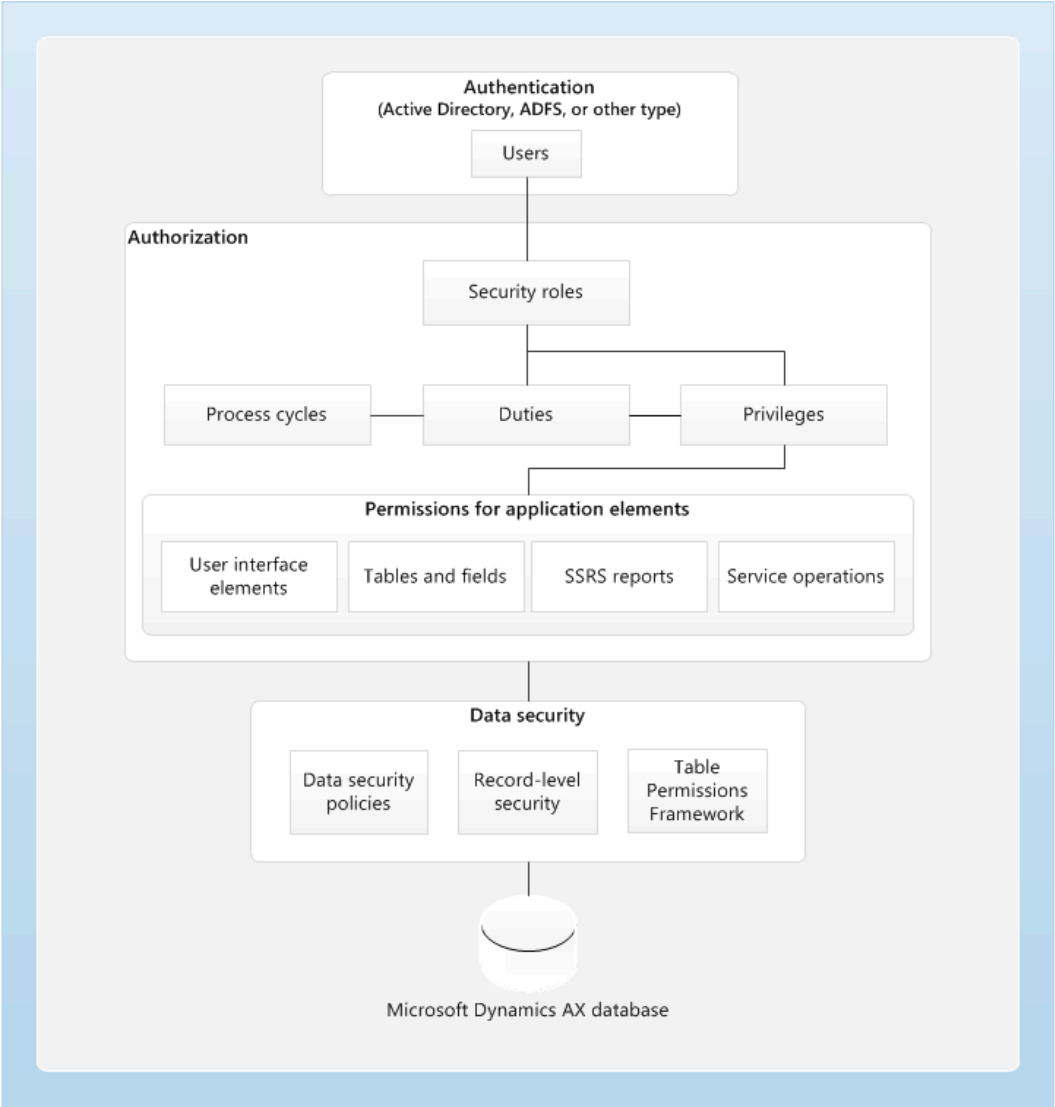
For more information, see Manage data access by using the Table Permissions Framework.

Flexible authentication

Since Microsoft Dynamics AX 4.0, user authentication has been based on Active Directory. All users have been required to be domain users. Even external users of Enterprise Portal have had to be domain users. To help secure other data on the network, the administrator had to set up group policies to prevent external users from accessing that data. In Microsoft Dynamics AX 2012, users can be authenticated by using methods other than Active Directory. Therefore, external users no longer require domain accounts to access Microsoft Dynamics AX. For more information, see Deploy an Enterprise Portal site that uses forms-based authentication (http://technet.microsoft.com/en-us/library/hh575253.aspx).

Security architecture of the Microsoft Dynamics AX application

When you understand the security architecture of Microsoft Dynamics AX, you can more easily customize security to fit the needs of your business. The following diagram provides a high-level overview of the security architecture of Microsoft Dynamics AX.



Authentication

By default, only authenticated users who have user rights in Microsoft Dynamics AX can establish a connection.

The Microsoft Dynamics AX client uses integrated Windows authentication to authenticate Active Directory users.

Enterprise Portal supports flexible authentication, which allows you to use authentication providers other than Active Directory. If you configure Enterprise Portal to use a different authentication provider, users are authenticated by that provider.

After a user connects to the client or Enterprise Portal, access is determined by the duties and privileges that are assigned to the security roles that the user belongs to.

Authorization

Authorization is the control of access to the Microsoft Dynamics AX application. Security permissions are used to control access to individual elements of the application: menus, menu items, action and command buttons, reports, service operations, web URL menu items, web controls, and fields in the Microsoft Dynamics AX client and Enterprise Portal for Microsoft Dynamics AX.

In Microsoft Dynamics AX, individual security permissions are combined into privileges, and privileges are combined into duties. The administrator grants security roles access to the application by assigning duties and privileges to the roles.

For more information about role-based security in Microsoft Dynamics AX, see Role-based security in Microsoft Dynamics AX.

Data security

Authorization is used to grant access to elements of the application. By contrast, data security is used to deny access to tables, fields, and rows in the database.

Use the extensible data security framework to control access to transactional data by assigning data security policies to security roles. Data security policies can restrict access to data, based on the effective date or based on user data, such as the sales territory or organization. For more information about how to use data security policies in Microsoft Dynamics AX, see Overview of Security Policies for Table Records (http://msdn.microsoft.com/en-us/library/hh272123.aspx).

In addition to the extensible data security framework, record-level security can be used to limit access to data that is based on a query. However, because the record-level security feature is becoming obsolete in a future release of Microsoft Dynamics AX, we recommend that you use data security policies, instead.

Additionally, the Table Permissions Framework helps protect some data. Data security for specific tables is enforced by Application Object Server (AOS). For more information about the Table Permissions Framework, see Manage data access by using the Table Permissions Framework.

Role-based security in Microsoft Dynamics AX

In role-based security, access is not granted to individual users, only to security roles. Users are assigned to roles. A user who is assigned to a security role has access to the set of privileges that is associated with that role. A user who is not assigned to any role has no privileges.

In Microsoft Dynamics AX, role-based security is aligned with the structure of the business. Users are assigned to security roles based on their responsibilities in the organization and their participation in business processes. The administrator grants access to the duties that users in a role perform, not to the program elements that users must use.

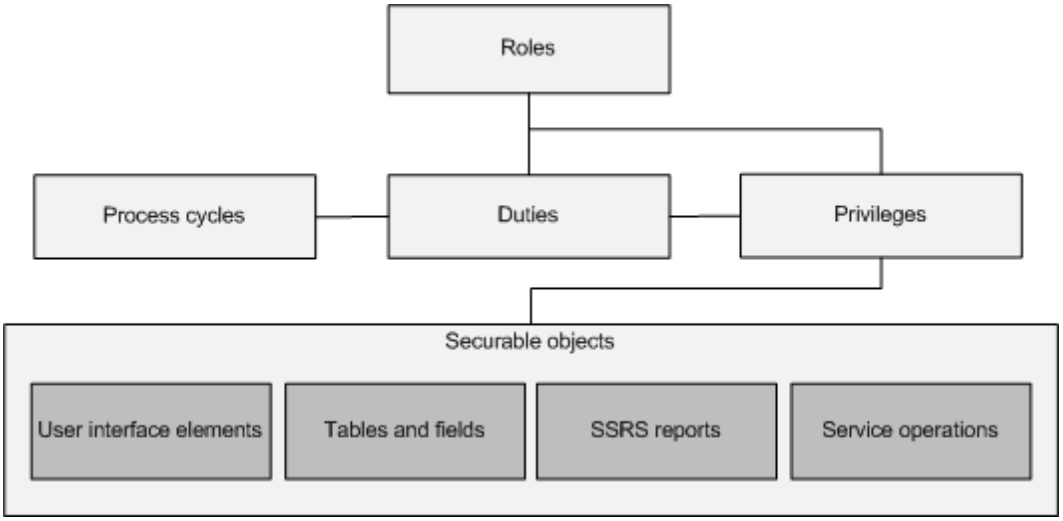
Because rules can be set up for automatic role assignment, the administrator does not have to be involved every time that a user's responsibilities change. After security roles and rules have been set up, business managers can control day-to-day user access based on business data.

Role-based security concepts

This section provides an overview of the elements of role-based security in Microsoft Dynamics AX. The security model is hierarchical, and each element in the hierarchy represents a different level of detail.

Permissions represent access to individual securable objects, such as menu items and tables. Privileges are composed of permissions and represent access to tasks, such as canceling payments and processing deposits. Duties are composed of privileges and represent parts of a business process, such as maintaining bank transactions. Both duties and privileges can be assigned to roles to grant access to Microsoft Dynamics AX.

The following illustration shows the elements of role-based security and their relationships.



The following sections explain the elements of the security model in more detail.

Security roles

All users must be assigned to at least one security role in order to have access to Microsoft Dynamics AX. The security roles that are assigned to a user determine the duties that the user can perform and the parts of the user interface that the user can view.

Administrators can apply data security policies to limit the data that the users in a role have access to. For example, a user in a role may have access to data only from a single organization. The administrator can also specify the level of access that the users in a role have to current, past, and future records. For example, users in a role can be assigned privileges that allow them to view records for all periods, but that allow them to modify records only for the current period.

By managing access through security roles, administrators save time because they do not have to manage access separately for each user. Security roles are defined one time for all organizations. In addition, users can be automatically assigned to roles based on business data. For example, the administrator can set up a rule that associates a Human resources position with a security role. Any time that users are assigned to that position, those users are automatically added to the appropriate security roles. Users can also be automatically added to or removed from roles based on the Active Directory groups that they belong to.

Security roles can be organized into a hierarchy. The role hierarchy allows the administrator to define a role based on another role. For example, the sales manager role could be defined as a parent role of the manager role and the salesperson role. A parent role automatically inherits the duties, privileges, and conditions that are assigned to its child roles. Therefore, a user who is assigned to the parent role can perform all of the tasks that users in the child roles can perform. A role can have one or more child roles or one or more parent roles.

By default, sample security roles are provided. All functionality in Microsoft Dynamics AX is associated with at least one of the sample security roles. The administrator can assign users to the sample security roles, modify the sample security roles to fit the needs of the business, or create new security roles. By default, the sample roles are not arranged in a hierarchy.

Note:
The sample security roles do not correspond to Role Centers.

For more information about how to work with security roles, see the following topics:

- Create or modify a security role
- Assign users to security roles
- Data security in Microsoft Dynamics AX

Process cycles

A business process is a coordinated set of activities in which one or more participants consume, produce, and use economic resources to achieve organizational goals.

To help the administrator locate the duties that must be assigned to roles, duties are organized by the business processes that they are part of. In the context of the security model, business processes are referred to as process cycles. For example, in the accounting process cycle, you may find the **Maintain ledgers** and **Maintain bank transactions** duties.

Process cycles are used for organization only. The process cycles themselves cannot be assigned to roles.

Duties

Duties correspond to parts of a business process. The administrator assigns duties to security roles. A duty can be assigned to more than one role.

In the security model for Microsoft Dynamics AX, duties contain privileges. For example, the **Maintain bank transactions** duty contains the **Generate deposit slips** and **Cancel payments** privileges. Although both duties and privileges can be assigned to security roles, we recommend that you use duties to grant access to Microsoft Dynamics AX.

You can assign related duties to separate roles. These duties are said to be segregated. By segregating duties, you can better comply with regulatory requirements, such as those from Sarbanes-Oxley (SOX), International Financial Reporting Standards (IFRS), and the United States Food and Drug Administration (FDA). In addition, segregation of duties helps reduce the risk of fraud, and helps you detect errors or irregularities.

Default duties are provided. The administrator can modify the privileges that are associated with a duty, or create new duties.

For more information about how to work with duties, see the following topics:

- Set up segregation of duties
- Create or modify a security privilege, duty, or process cycle

Privileges

In the security model for Microsoft Dynamics AX, a privilege specifies the level of access that is required to perform a job, solve a problem, or complete an assignment. Privileges can be assigned directly to roles. However, for easier maintenance, we recommend that you assign only duties to roles.

A privilege contains permissions to individual application objects, such as user interface elements and tables. For example, the **Cancel payments** privilege contains permissions to the menu items, fields, and tables that are required to cancel payments.

By default, privileges are provided for all features in Microsoft Dynamics AX. The administrator can modify the permissions that are associated with a privilege, or create new privileges.

Permissions

Each function in Microsoft Dynamics AX, such as a form or a service, is accessed through an entry point. Menu items, web content items, and service operations are referred to collectively as entry points.

In the security model for Microsoft Dynamics AX, permissions group the securable objects and access levels that are required to run a function. This includes any tables, fields, forms or server side methods that are accessed through the entry point.

Only developers can create or modify permissions. For more information about how to work with permissions, see the Microsoft Dynamics AX developer documentation. Be aware that modifying permissions may affect your licensing requirements. For more information about how licensing relates to security, see the Security roles and licensing white paper (http://go.microsoft.com/fwlink/?LinkID=228370) for Microsoft Dynamics AX 2012.

Important:
In the licensing model for Microsoft Dynamics AX, entry points are referred to as *menu items*.

Manage users

This section provides information about how to manage users of Microsoft Dynamics AX. The following topics are included:

Manage user groups

To use some features and functionality in Microsoft Dynamics AX, you may have to create user groups. For example, if users who are outside the organization hierarchy for budget planning must work with budget plans, you can assign budget plans to user groups. You can also set up restrictions for journal posting that are based on user groups.

The following procedure describes how to create a user group and add users to it.

1. Click **System administration** > **Common** > **Users** > **User groups**.
2. On the **Groups** tab, press CTRL+N to create a new group.
3. In the **Group** column, enter a short name for the group. A short name is required. For example, enter **Budget A** for a budgeting group or **Journals 1** for a journal posting group.
4. In the **User group name** column, enter a long name for the group. A long name is required. For example, enter **Budgeting group A** or **Journal posting group 1**.

   To avoid confusion, we recommend that you make the names of user groups as descriptive as you can.
5. Click the **Users** tab.

6. In the **Remaining users** list, select users. Then click the left arrow button (**<**) to move the selected users to the **Selected users** list. All users that you move to the **Selected users** list are added to the group.

Work with users from Active Directory

Before users can be made Microsoft Dynamics AX users, they must be defined in Active Directory Domain Services (AD DS).

AD DS is a Microsoft Windows–based directory service that catalogs information about all the objects on a network and distributes that information throughout the network. These objects include people, computers, and printers. Security is integrated with AD DS through logon authentication and access control. For more information about AD DS, see Active Directory Overview (http://go.microsoft.com/fwlink/?LinkId=47868).

Before you install or deploy Microsoft Dynamics AX, carefully plan the user topology of your AD DS directory service. The computers that run Microsoft Dynamics AX must have access to computers in the same domain on which AD DS runs in native mode.

For information about how to configure AD DS, see one of the following resources:

- Deploy Active Directory Domain Services (AD DS) in Your Enterprise (Windows Server 2012) (http://technet.microsoft.com/en-us/library/hh472160.aspx)
- Deployment guide for Active Directory Domain Services on Windows Server 2008 (http://go.microsoft.com/fwlink/?LinkID=164995)
- Deployment guide for Active Directory Domain Services on Windows Server 2003 (http://go.microsoft.com/fwlink/?LinkID=164994)

Existing structures in AD DS do not require modification to support Microsoft Dynamics AX users. If you have AD DS domains, and all the domains in the forest are set up to have two-way trust, Microsoft Dynamics AX recognizes all the users in the domains. Work with the system administrator to understand the existing structures in AD DS.

Create service accounts for required functionality

You must create the dedicated domain accounts that are required by various components of Microsoft Dynamics AX. For more information, see Create service accounts (http://technet.microsoft.com/en-us/library/dd362055.aspx).

Import users from AD DS

After a user is listed in AD DS, you can manually add that user to Microsoft Dynamics AX. If you use the Active Directory Import Wizard, you can also import users from AD DS by specifying various search criteria.

For more information about how to add users, see Create new users in Microsoft Dynamics AX.

Administrator permissions

The Microsoft Dynamics AX administrator does not have to be a domain administrator to import users from AD DS. However, a Microsoft Dynamics AX administrator who is also a domain administrator can see all users in AD DS and import those users into Microsoft Dynamics AX. Because of security functionality in the Group Policy objects (GPOs) for AD DS, a Microsoft Dynamics AX administrator who is not a domain administrator can see only a subset of the users in AD DS.

To see the complete list of users in AD DS during import, a Microsoft Dynamics AX administrator who is not a domain administrator must be a member of the **Authenticated users** security group on the domain. Use the following procedure to add a member to the **Authenticated users** security group.

1. In **Active Directory Users and Computers**, on the **View** menu, make sure that **Advanced Features** is selected.
2. Right-click a user that you cannot see when you run the import wizard, and then select **Properties**.
3. Click the **Member Of** tab. Confirm that the user is listed as a member of the **Domain Users** group.
4. Click the **Security** tab. Select the **Authenticated Users** group, and then make sure that **Read** is set to **Allow**.

If you want all authenticated users to see the complete list of users in AD DS during import, grant the **Authenticated Users** security group **Read** permissions to all objects.

1. In **Active Directory Users and Computers**, on the **View** menu, make sure that **Advanced Features** is selected.
2. Click the **Users** organizational unit. The **User Properties** dialog box appears.
3. Click the **Security** tab, and select the **Authenticated Users** group.
4. Click the **Advanced** tab. Select **Authenticated Users Name**, and then click **Edit**.
5. Make sure that **Read all properties** is selected. Then, in the **Apply to** box, select **This object and all descendant objects**.

Duplicate alias IDs

When you import users from AD DS into Microsoft Dynamics AX, the import wizard tries to create Microsoft Dynamics AX user IDs from the AD DS aliases. However, a Microsoft Dynamics AX user ID is limited to five characters, whereas an AD DS alias can have up to 255 characters. If the first five characters of the AD DS alias are the same for more than one user, the wizard generates alternative Microsoft Dynamics AX user IDs for these users.

When alternative user IDs are generated, if the alias has more than five characters, the first four characters of the first name and a single character from the last name are used. If there are still duplicates, the first three characters of the first name and two characters from the last name are used.

You can't change user IDs while running the wizard. However, you can change user IDs later to make them more meaningful. For more information, see Create new users in Microsoft Dynamics AX.

Assign an AD DS group to a role

You can assign AD DS groups to roles in Microsoft Dynamics AX. When an AD DS group is assigned to a role, membership in the role corresponds to membership in the group.

Warning:
When an AD DS group is assigned to a security role, Microsoft Dynamics AX is unable to calculate conflicts in segregation of duties for individual users who are part of the AD DS group.

Create new users in Microsoft Dynamics AX

Microsoft Dynamics AX users are internal employees of your organization, or external customers and vendors, who require access to Microsoft Dynamics AX to perform their jobs. Any individual who must access Microsoft Dynamics AX must be added to the list of Microsoft Dynamics AX users in the **Users** form.

For users and groups that are in AD DS, you can use the **Active Directory Import Wizard** to import the users into Microsoft Dynamics AX.

Add a new user

To add a single new user to Microsoft Dynamics AX, complete the following procedure. Use this procedure to add a user from AD DS or a user that is authenticated by a claims-based authentication provider. For more information about claims-based authentication in Microsoft Dynamics AX, see Deploy an Enterprise Portal site that uses forms-based authentication (http://technet.microsoft.com/en-us/library/hh575253.aspx).

1. Click **System administration** > **Common** > **Users** > **Users**.
2. Click **User**.
3. In the **User ID** field, enter a unique identifier for the user. A user ID is required. The user ID can contain a maximum of eight characters.

   You can't change the information in the **User ID** field after the user record has been saved. For information about how to change a user ID, see Change a user ID.
4. Optional: In the **User name** field, enter the user or group's name.
5. In the **Network domain** field, enter the user or group's Active Directory Domain Services (AD DS) domain, if the user or group is authenticated by AD DS. If the user is authenticated by a claims-based authentication provider, this field displays the name of the trusted identity provider in SharePoint that authenticates the user.
6. In the **Alias** field, enter a network alias if the user or group is in AD DS. If the user is not in AD DS, enter an e-mail address.
7. In the **Account type** field, select whether the user or group is authenticated by AD DS or by a claims-based authentication provider.

   Caution:
   You must select the correct account type for the user or group to be validated. For example, an AD DS group is not recognized if **Active Directory user** is selected in the **Account type** field.
8. In the **Default company** list, select the company that the user logs on to by default. If you do not select a company, Microsoft Dynamics AX uses the current company that the administrator is logged on to.
9. To grant the user access to Microsoft Dynamics AX, select **Enabled**.

   Note:
   The **External** option is automatically selected when a user is designated as a web user.
10. Click **Assign roles** to select the security roles that are assigned to the user. If you must assign the user to a role in a particular organization, select a role, and then click **Assign organizations**.

    For more information about how to assign users to roles manually or automatically, see Assign users to security roles.

    Many users, especially external users, access Microsoft Dynamics AX by using Enterprise Portal for Microsoft Dynamics AX. For more information about how to grant access to Enterprise Portal, see Enable users to access Enterprise Portal (http://technet.microsoft.com/en-us/library/dd309631.aspx).

Import users from Active Directory

If you must create multiple new users, and those users are listed in AD DS, use the **Active Directory Import Wizard** to import the users into Microsoft Dynamics AX. For more information, see Work with users from Active Directory.

1. Click **System administration** > **Common** > **Users** > **Users**. Then click **Import**.
2. The **Welcome to Active Directory Import Wizard** page is displayed. Click **Next >**.
3. The **Select Users to import from Active Directory** page is displayed. Select the AD DS domain to import users from, and then enter search criteria for the AD DS users or groups that you want to import.

   Note:
   You cannot search for users by using only the **Title** field. To search on the **Title** field, you must also include at least one other field in the search criteria.

   Click **Next >**.
4. The **Select users** page is displayed. This page shows the results of the AD DS search that was performed in the previous step. Select the check boxes next to the users to add to Microsoft Dynamics AX, and then click **Next >**.
5. Verify the users to be imported into Microsoft Dynamics AX.

   The wizard creates user IDs of up to five characters for the new Microsoft Dynamics AX users. The user ID is the first five characters of the AD DS alias.

   When multiple users in the group have the same first five characters in their AD DS aliases, the wizard automatically generates Microsoft Dynamics AX user IDs that consist of the first four characters of the AD DS alias, followed by a digit.

   You can't change user IDs while you are running the wizard. For information about how to change a user ID, see Change a user ID.

   Click **Next >**.
6. The **Select roles** page is displayed. Use this page to assign security roles to the list of users. The roles that you select will be assigned to all the users that you are importing. If the users must be assigned to different roles, you can skip this page and assign roles to individual users after the users are imported.

   When you assign a user to a role by using this wizard, you cannot assign the user to a role in a specific organization. The user is assigned to the role in all organizations. To modify an individual user's settings after you import users, use the **User** form.

   Click **Next >**.
7. The **Select profile** page is displayed. Use this page to assign profiles to the list of users. A user profile determines the content that is displayed on the Role Center page for the users who are assigned to that profile.

   Click **Next >**.
8. The **Completing the Active Directory Import Wizard** page is displayed. Click **Finish** to close the wizard.

Change a user ID

When you import users from AD DS, user IDs are generated automatically. You can't change user IDs while you are running the wizard, and you can't change a user ID by using the **User ID** field in the **Users** form. To change a user ID, you must rename the key in the database. When you change a user ID by using this procedure, all related user settings are modified to use the new user ID. For example, the usage information in the SysLastValue table is updated to reference the new user ID.

Note:
The user ID is the primary key of the user information table. Renaming the primary key can take some time, because all references to the key are also updated in the database.

1. Click **System administration** > **Common** > **Users** > **Users**.
2. Right-click a user in the list and select **Record info**.
3. Click **Rename**.
4. Enter a new value for the user ID, and then click **OK**. You must enter a unique value.
5. Click **Yes** to confirm.

Monitor users

Microsoft Dynamics AX includes several features to help you monitor which users are currently logged on to Microsoft Dynamics AX, how frequently a particular user has logged on, and the length of time that a user has been logged on. The procedures in this topic explain how complete the following actions:

- View which users are currently logged on.
- Disconnect one or more connected users.
- View logon statistics for a specified user.

View which users are currently logged on

Click **System administration** > **Common** > **Users** > **Online users**.

Disconnect one or more connected users

You can end one or more user sessions from the **Online users** form. Before you disconnect a user, warn that user of the impending disconnection so that you do not disrupt an important operation such as a posting.

1. Click **System administration** > **Common** > **Users** > **Online users**.
2. Select the user who you want to disconnect. Press and hold the CTRL key to select multiple users.
3. Click **End sessions**.

Important:
If you disconnect a user because you changed permissions for a role, restart the Microsoft Dynamics AX server after you make this change. If you do not restart the server, members of the role might keep their former permissions until the next restart.

View logon statistics for a specified user

1. Click **System administration** > **Common** > **Users** > **Users**..
2. Select the user for whom you want to view logon statistics.

3. Click **User log**.
    - By default, the **Overview** tab lists every time that the user logged on during the last 100 days. You can change the time period by clicking the **Clean up** button and selecting a new duration.
    - The **General** tab includes information about the user's computer ID, client type, and more.
    - The **Statistics** tab includes details about the user's session, such as the duration.

Manage roles

This section provides information about how to manage roles in Microsoft Dynamics AX.

Create or modify a security role

If the security roles that are provided with Microsoft Dynamics AX do not meet the needs of your business, you can create new roles. You can create a custom role that is based on an existing role, or you can build a completely new role.

Work with managers who oversee the different groups in your business to determine the appropriate permission levels for roles. For example, work with a manager in the Finance department to determine permission levels for Finance roles.

Only the Microsoft Dynamics AX administrator can create or modify a role.

Important:
Be aware that modifying roles may affect your licensing requirements. For more information about how licensing relates to security, see the Security roles and licensing white paper (http://go.microsoft.com/fwlink/?LinkID=228370) for Microsoft Dynamics AX 2012.

1. Click **System administration** > **Setup** > **Security** > **Security roles**.
2. To create a new role, click **New**. To modify an existing role, select the role.
3. If you are creating a new role, enter the name that you want to appear for the role in the Application Object Tree (AOT).

    Note:
    AOT names must contain only alphanumeric or underscore characters. AOT names cannot begin with a number, and they cannot contain special characters or spaces.
4. Enter or modify the display name of the role.
5. Enter or modify the description of the role.
6. To add security privileges to the selected role, click **Add...** to open the **Add privileges to role** form.

    Find the security privileges that you want to add. You can sort and view the privileges by role, process cycle, or duty/privilege. You can also enter a privilege name or keywords in the **Find** field.

    Tip:
    Security is organized hierarchically. Permissions on specific application elements are combined into privileges, privileges are combined into duties, and duties are grouped into process cycles. You can assign either duties or privileges to roles. For more information about the security hierarchy, see Security architecture of the Microsoft Dynamics AX application.

To include all of the permissions from another role, open the **Security roles** form, and drag the role that has the permissions that you want to the role that you are modifying. By dragging one role to another, you create a hierarchical relationship, where the main role contains all of the permissions of the sub-role. If you change the permissions of a sub-role, the changes also apply to the main role.

A role cannot contain duties that conflict according to the rules for the segregation of duties. For more information, see Set up segregation of duties.

To remove a duty, privilege, or sub-role from the role, select the duty, privilege, or sub-role, and then click **Remove**.

7. To change the role's permission level on securable objects such as controls, tables, fields, and server methods, right-click the role, and then click **Override permissions**.

   Note:
   Overrides for securable objects are not associated with specific duties or privileges. If you apply an override, the access level for the securable object is set for the role, regardless of access levels specified by the duties and privileges assigned to that role.

8. To limit access to rows, or records, in the database based on a query, you can use record-level security. To apply filters for record-level security, right-click the role, and then click **Record-level security**. For more information, see Manage record level security.

   Important:
   The record-level security feature will become obsolete in a future release. If you are setting up new filters, we recommend that you create data security policies by using the extensible data security framework.

9. When you have finished modifying the role, click **Close** in the **Security roles** form.

Assign users to security roles

To access Microsoft Dynamics AX, users must be assigned to security roles. You can assign users to roles automatically, based on business data, or you can assign users to roles manually. We recommend that you assign roles automatically most of the time.

Important:
Users must exist in Microsoft Dynamics AX before they can be assigned to roles. Even if you use automatic role assignment, users are not automatically added to Microsoft Dynamics AX. For more information about how to add users, see Create new users in Microsoft Dynamics AX.

You can assign individual users or Active Directory groups to a role.

Users can be assigned to multiple roles. If a user is assigned to multiple roles that grant different levels of access to the same item, the user has the highest level of access that the various roles grant. For example, if the user is a member of both role A, which has View access to sales orders, and role B, which has Create access to sales orders, the user has Create access to sales orders.

Automatically assign users to roles

Set up rules for automatic role assignment to guarantee that role membership is based on current business data. If you use automatic role assignment, permissions are automatically updated when people change jobs in an organization.

Rules for automatic role assignment run at a fixed interval by using the batch framework. The batch job for role assignment belongs to the default, or blank, batch group.

Tip:
If automatic role assignment is not working as expected, make sure that the batch job is enabled. Additionally, make sure that the default batch group is assigned to a batch server, and that batch servers are currently processing batches. Upgrades and other non-interactive processes can disable the batch job, and batch servers may be configured to run only at certain times of the day.

If a rule for automatic role assignment encounters a conflict that is related to the segregation of duties, the user who has the conflict cannot be automatically assigned to the role. Instead, the user is marked as excluded from the role. The user is also listed in the **Segregation of duties unresolved conflicts** form. (Click **System administration** > **Setup** > **Security** > **Segregation of duties** > **Segregation of duties unresolved conflicts**.) For more information, see Set up segregation of duties.

1. Click **System administration** > **Setup** > **Security** > **Assign users to roles**.
2. Select a role. The users who are currently assigned to the role are displayed.
3. In the **Rules for dynamically assigning users to role** pane, click **Add rule** to open a list of queries that can be used for automatic role assignment. Queries in the list use the UserInfo table as the primary data source, and the User field is included in the list of fields.

   Important:
   By default, the **Security administrator** role has access to only a subset of tables and fields in Microsoft Dynamics AX. If the **Security administrator** role is required to use other tables in a query, the permissions for the role must be modified to grant access to those tables. For more information, see Override permissions (form) (http://technet.microsoft.com/en-us/library/425b809d-947a-4c56-ba20-40811e2b4d93).
4. Select a query in the list.

   To modify a query, select it, and then click **Edit query**. In the **Inquiry** form, use the **Range** tab to add or remove fields. Click **OK** to save the query. When you save a query, it runs immediately.
5. The rule is assigned a default name. If necessary, you can modify the name or add a description by typing in the list.

Exclude users from automatic role assignment

Users who are automatically assigned to roles cannot be removed from those roles by the administrator. However, the administrator can exclude users from roles. When you exclude a user from a role, the user's role assignment is no longer controlled automatically. When the rules for automatic role assignment run, or when an Active Directory group is assigned to a role, excluded users are listed in the role membership, but they are marked as excluded. The excluded users are not granted the access that is associated with the role. Excluded users cannot be assigned to the role until the administrator removes the exclusion.

1. Click **System administration** > **Setup** > **Security** > **Assign users to roles**.
2. Select a role. The users who are currently assigned to the role are displayed.
3. In the **Users assigned to role** pane, click **Manually assign / exclude users** to open the **Assign users to or exclude users from role** form.
4. Select the users who you want to exclude from the role. To select multiple users, hold down the **CTRL** key, and then click each user that you want to exclude.

Click **Exclude from role** to exclude the users from the role.

To remove exclusions, select the users who you want to remove exclusions for, and then click **Reset status**.

When you remove an exclusion by resetting the user's status, the user's role is again assigned automatically. However, the user is not immediately assigned to the role or excluded from the role when you reset the status. Instead, the user is either assigned to the role or removed from the role the next time that the rules for automatic role assignment run.

5. When you have finished making changes, close the **Assign users to or exclude users from role** form.

Manually assign users to roles

Manually assign users to roles when role membership cannot be based on data in Microsoft Dynamics AX. For example, you can manually assign roles if an employee goes on vacation, and another employee must temporarily perform that employee's duties. Users who are manually assigned to security roles must also be manually removed by the administrator. These users are not removed from roles by rules for automatic role assignment.

1. Click **System administration** > **Setup** > **Security** > **Assign users to roles**.
2. Select a role. The users who are currently assigned to the role are displayed.
3. In the **Users assigned to role** pane, click **Manually assign / exclude users** to open the **Assign users to or exclude users from role** form.
4. Select the users who you want to add to the role. To select multiple users, hold down the **CTRL** key, and then click each user that you want to add.
5. Click **Assign to role** to add the users to the role.

   Do not assign users to roles that contain duties that conflict according to the rules for the segregation of duties. If you attempt to assign a user to a role, and the duties of that role conflict with the duties of a role that was previously assigned to the user, a message is displayed. The user is not assigned to the new role. For more information, see Set up segregation of duties.

   Warning:
   When an Active Directory Domain Services group is assigned to a security role, Microsoft Dynamics AX is unable to calculate conflicts in segregation of duties for individual users who are part of the Active Directory Domain Services group.
6. When you have finished making changes, close the **Assign users to or exclude users from role** form.

Create or modify a security privilege, duty, or process cycle

If the security privileges, duties, and process cycles that are provided with Microsoft Dynamics AX do not meet the requirements of your business, you can create new privileges, duties, and process cycles.

Tip:
Security is organized hierarchically. Permissions on specific application elements are combined into privileges, privileges are combined into duties, and duties are grouped into process cycles. You can assign either duties or privileges to roles. For more information about the security hierarchy, see Security architecture of the Microsoft Dynamics AX application.

Only the Microsoft Dynamics AX administrator can create or modify a security privilege, duty, or process cycle.

For information about how privileges, duties, and process cycles are used in the security model for Microsoft Dynamics AX, see Role-based security in Microsoft Dynamics AX.

Create or modify a security privilege or duty

1. Click **System administration** > **Setup** > **Security** > **Security privileges**.
2. To create a new privilege, select the duty that the privilege must belong to, and then click **New**.

   To create a new duty, select the process cycle that the duty must belong to, and then click **New**.

   To modify an existing privilege or duty, select the privilege or duty.
3. If you are creating a new privilege or duty, enter the name that appears for the privilege or duty in the Application Object Tree (AOT).

   Note:
   AOT names can contain only alphanumeric characters and underscore characters (_). AOT names cannot begin with a number, and they cannot contain special characters or spaces.
4. Enter or modify the display name of the privilege or duty.
5. Enter or modify the description of the privilege or duty.
6. Add or modify the content of the privilege or duty.
   - To add an existing privilege to a duty, right-click the privilege in the left pane, and then click **Copy**. Right-click the duty, and then click **Paste**.
   - To remove a privilege from a duty, right-click the privilege in the left pane, and then click **Delete**. To remove a permission from a duty or privilege, select the permission in the central pane, and then click **Remove**.
   - To add permissions to a duty or privilege, click **Add...** to open the **Add permissions to privilege** form. Find the security permissions to add. You can sort the permissions by the location of the entry points on the main menu or by process cycle. If you sort by process cycle, you can also enter the permission name or keywords in the **Find** field.
7. When you have finished modifying the privilege or duty, click **Close** in the **Security privileges** form.

Create or modify a process cycle

1. Click **System administration** > **Setup** > **Security** > **Security privileges**.
2. To create a new process cycle, select the **Process cycles** node in the left pane, and then click **New**.

   To modify an existing process cycle, select the process cycle.
3. If you are creating a new process cycle, enter the name that appears for the process cycle in the AOT.

   Note:
   AOT names can contain only alphanumeric characters and underscore characters (_). AOT names cannot begin with a number, and they cannot contain special characters or spaces.
4. Enter or modify the display name of the process cycle.
5. Enter or modify the description of the process cycle.
6. Add or modify the content of the process cycle.

- To add an existing duty or privilege to a process cycle, right-click the duty or privilege in the left pane, and then click **Copy**. Right-click the process cycle, and then click **Paste**.
- To remove a duty or privilege from a process cycle, right-click the duty or privilege in the left pane, and then click **Delete**.

7. When you have finished modifying the process cycle, click **Close** in the **Security privileges** form.

Set up segregation of duties

Security or policies may require that specific tasks be performed by different users. For example, you might not want the same person both to acknowledge the receipt of goods and to process payment to the vendor. This concept is named *segregation of duties*.

Segregation of duties helps you reduce the risk of fraud, and it also helps you detect errors or irregularities. You can also use segregation of duties to enforce internal control policies.

In Microsoft Dynamics AX, when two duties in the same role conflict, or when a user is assigned to two roles that contain conflicting duties, the conflict is logged. The security administrator must approve or reject each assignment that causes a conflict.

For duties that are typically separated, separate sample roles and default duties are included with Microsoft Dynamics AX. By default, no rules are set up for segregation of duties.

Compliance with the rules for segregation of duties is not verified when you create rules. Therefore, you can create a rule that causes existing user role assignments to conflict. You can also create a rule that causes an existing role definition to have a conflict. You must validate compliance manually after you create new rules. For more information about how to identify and resolve conflicts, see Identify and resolve conflicts in segregation of duties.

Use the following procedure to set up a rule for segregation of duties.

1. Click **System administration** > **Setup** > **Security** > **Segregation of duties** > **Segregation of duties rules**.
2. Click **New**.
3. Enter a name for the rule.
4. Select the first duty that is controlled by the rule.
5. Select the second duty that is controlled by the rule.
6. Select the severity of the risk that occurs when the same user or role performs both duties.
7. Enter a description of the security risk.
8. Enter a description of the actions that you take to mitigate the security risk. For example, you can mitigate the risk by conducting more detailed reviews of the process, by conducting a monthly managerial review, or by sharing resources with other departments.

Identify and resolve conflicts in segregation of duties

In Microsoft Dynamics AX, you can set up rules to separate tasks that must be performed by different users. This concept is named *segregation of duties*. When the definition of a security role or the role assignments of a user violate the rules, the conflict is logged. All conflicts must be resolved by the administrator.

Use the procedures in this topic to identify and resolve conflicts that involve segregation of duties.

Verify whether user role assignments comply with new rules for segregation of duties

When you assign users to roles, the rules for segregation of duties are automatically enforced. If you try to assign a user to roles that contain conflicting duties, you receive an error message. You must then resolve the conflict either by denying the role assignment or by overriding the conflict.

However, compliance is not verified when you create the rules for segregation of duties. Therefore, it is possible to create a rule that causes existing user role assignments to conflict. This means that you must validate compliance after you create new rules.

Use the **Verify compliance of user-role assignments with rules for segregation of duties** form to verify whether existing role memberships comply with the rules. You can run the verification process on demand or as a regularly scheduled batch job.

Warning:
When an Active Directory Domain Services group is assigned to a security role, Microsoft Dynamics AX is unable to calculate conflicts in segregation of duties for individual users who are part of the Active Directory Domain Services group.

1. Click **System administration** > **Setup** > **Security** > **Segregation of duties** > **Verify compliance of user-role assignments**.
2. Follow one of these steps:
   - To run the verification process immediately, click **OK**. The **Infolog** form displays the results of the validation. If there is a conflict, you can double-click the message to open the **Users** form and change the user's role assignments. Conflicts are also logged in the **Segregation of duties conflicts** form.
   - To run the verification process as a batch job, select **Batch processing**, and then set the other batch parameters. After the batch job runs, you can review the conflicts in the **Segregation of duties conflicts** form.

View and resolve conflicting user role assignments

Use the **Segregation of duties conflicts** form to allow or deny role assignments that cause a conflict.

This form lists conflicts that are identified by the batch job that is run from the **Verify compliance of user-role assignments with rules for segregation of duties** form. This form also lists conflicts that occur when rules for automatic role assignment try to assign a user to two roles that contain conflicting duties.

1. Click **System administration** > **Setup** > **Security** > **Segregation of duties** > **Segregation of duties conflicts**.

   –or–

   Click **System administration** > **Setup** > **Security** > **Segregation of duties** > **Segregation of duties unresolved conflicts**.
2. Select a conflict, and then click one of the following buttons:
   - **Deny assignment** – Deny the assignment of the user to the additional security role. If you deny an automatic role assignment, the user is marked as excluded from the role. The excluded user is not granted the access that is associated with the role, and the user cannot be assigned to the role until the administrator removes the exclusion.

- **Allow assignment** – Override the conflict, and allow the user to be assigned to both security roles. If you override a conflict, you must enter a reason in the **Reason for override** field.

Verify whether existing roles comply with new rules for segregation of duties

When you create or modify a role, the rules for segregation of duties are automatically enforced. You cannot assign conflicting duties to a role.

However, compliance is not verified when you create the rules for segregation of duties. Therefore, it is possible to create a rule that causes an existing role definition to have a conflict. This means that you must validate compliance manually after you create new rules.

1. Click **System administration** > **Setup** > **Security** > **Segregation of duties** > **Segregation of duties rules**.
2. Select a rule, and then click **Validate duties and roles**.

   The **Infolog** form is displayed.

   - If any existing roles violate the selected rule, a message is displayed that contains the name of the role and the names of the conflicting duties. The administrator must either indicate the mitigation for the security risk or modify the role so that it does not violate the rules for segregation of duties.
   - If no roles violate the selected rule, a message indicates that all roles are in compliance.

Security technical reference

Firewall settings for Microsoft Dynamics AX components

If you use Windows Firewall to help protect your computers, Microsoft Dynamics AX components require the settings in the following table. For more information about Windows Firewall, see the Windows documentation.

Component	Computer	Firewall setting	Notes
Setup	Any	Allow outbound HTTP connections.	To access the documentation that is available from the Setup wizard, you must be able to connect to the Internet from the computer where you are running Setup.
Databases	Database server	Exclude the port that is used by Microsoft SQL Server. By default, SQL Server uses port 1433.	For more information, see the SQL Server documentation.

Component	Computer	Firewall setting	Notes
Application Object Server (AOS)	AOS server	• Exclude the TCP/IP port that is used by the AOS instance. By default, AOS uses port 2712. Setup automatically creates the inbound rule "Dynamics AX 6.0 – MicrosoftDynamicsAX (RPC)" for the TCP/IP port. • Exclude the services WSDL port that is used by the AOS instance. By default, AOS uses port 8101. Setup automatically creates the inbound rule "Dynamics AX 6.0 – MicrosoftDynamicsAX (WSDL)" for the WSDL port. • Exclude the services endpoint port that is used by the AOS instance. By default, AOS uses port 8201. Setup automatically creates the inbound rule "Dynamics AX 6.0 – MicrosoftDynamicsAX (NetTCP)" for the services endpoint port.	Windows Firewall must be enabled on the computer. Each AOS instance must use a different port number. **Note:** By default, every time that you install an additional AOS instance on a computer, the TCP/IP port number and the services endpoint port numbers are incremented by 1. For example, by default, the second AOS instance on a computer is assigned to TCP/IP port 2713.
Client	Client workstation	Exclude Ax32.exe.	The client uses a TCP port to connect to the AOS instance.
Microsoft SQL Server Reporting Services extensions	Report server	Exclude the port that is used by Reporting Services virtual directories, if Reporting Services uses a port other than port 80.	If you are installing Reporting Services extensions in a perimeter network, you may need to add a firewall policy that enables you to connect to the Microsoft Dynamics AX database. For example, if you are using Forefront Threat Management Gateway (TMG), you must add a **Non-Web Server Protocol Rule**. For more information, see Configuring SQL Server publishing (http://technet.microsoft.com/en-us/library/cc441596.aspx) in the Forefront TMG documentation.

Component	Computer	Firewall setting	Notes
Microsoft SQL Server Analysis Services integration	Analysis server	• Exclude the port that is used by Analysis Services. By default, Analysis Services uses port 2383. • If you are using SQL Server Browser, you must also exclude port 2382.	For more information about how to configure access to Analysis Services through Windows Firewall, see the SQL Server documentation on MSDN.
Debugger	Developer workstation	Exclude AxDebug.exe and its target programs, such as Ax32.exe and AxServ32.exe.	The debugger uses a dynamically allocated TCP port.
Enterprise Portal for Microsoft Dynamics AX	Web server	• Enable the Web Server (HTTP). • Exclude the port that is used by the Enterprise Portal website, if the site uses a port other than port 80.	If you do not enable the Web Server in Windows Firewall, you can view the site only from the local server.
Help Server	Web server	Exclude the port that is used by the Help Server web site, if the site uses a port other than port 80.	
Enterprise Search	Web server	Exclude the port that is used by the Search web site, if the site uses a port other than port 80.	
Web services	Web server	Exclude the port that is used by the services web site, if the site uses a port other than port 80.	External programs use this port to consume the Microsoft Dynamics AX web services that are based on Internet Information Services (IIS).
Management utilities	Remotely managed computer	Enable Remote Administration.	You must enable Remote Administration on computers that are administered remotely by using Windows PowerShell. For example, enable Remote Administration on a computer if you deploy reports to that computer from another computer where Windows PowerShell is installed.

Component	Computer	Firewall setting	Notes
Synch Service	Head-office communications server	• Exclude the port that is used by Microsoft SQL Server. By default, SQL Server uses port 1433. • Exclude the port that is used by Synch Service. By default, Synch Service uses port 16750. • Exclude the port that is used by Real-time Service. By default, Real-time Service uses port 1239.	For instructions, see the PCI Implementation Guide for Microsoft Dynamics AX 2012 Feature Pack (http://go.microsoft.com/fwlink/?LinkId=237283).
Synch Service	Store communications server	• Enable Internet Protocol security (IPsec). • Exclude the port that is used by Microsoft SQL Server. By default, SQL Server uses port 1433. • Exclude the port that is used by Synch Service. By default, Synch Service uses port 16750.	For more information, see the PCI Implementation Guide for Microsoft Dynamics AX 2012 Feature Pack (http://go.microsoft.com/fwlink/?LinkId=237283).
Real-time Service		Exclude the port that is used by Real-time Service, if the site uses a port other than port 80.	For more information, see the PCI Implementation Guide for Microsoft Dynamics AX 2012 Feature Pack (http://go.microsoft.com/fwlink/?LinkId=237283).
Retail POS	Store communications server	Exclude the port that is used by Microsoft SQL Server. By default, SQL Server uses port 1433. Exclude the port that is used by Synch Service. By default, Synch Service uses port 16750.	For more information, see the PCI Implementation Guide for Microsoft Dynamics AX 2012 Feature Pack (http://go.microsoft.com/fwlink/?LinkId=237283).
Retail POS	Store database server	Exclude the port that is used by Microsoft SQL Server. By default, SQL Server uses port 1433. On a register that has its own local database, you only need to open the firewall to SQL Server if Synch Service is on a computer other than the register.	For more information, see the PCI Implementation Guide for Microsoft Dynamics AX 2012 Feature Pack (http://go.microsoft.com/fwlink/?LinkId=237283).

Component	Computer	Firewall setting	Notes
Microsoft Dynamics ERP RapidStart Connector	Microsoft Dynamics ERP RapidStart Services host machine	• Exclude the executable file for the Microsoft Dynamics ERP RapidStart Connector service. By default, the file is installed in this location: %SystemDrive%\Program Files\Microsoft Dynamics AX\60\RapidStartConnectorService\Microsoft.Dynamics.AX.AppConfig.ConnectorLoaderService.exe • Exclude the endpoint port that is used by the Microsoft Dynamics ERP RapidStart Connector service. By default, the service communicates with the Windows Azure Service Bus on ports 9350-9354, 80, and 443. • Exclude the Windows Azure Cloud Services Protocols.	

Table Permissions Framework reference

The Table Permissions Framework (TPF) enables administrators to set restrictions on tables that store data, including sensitive data. To enable TPF, an administrator specifies a value for the AOSAuthorizationProperty on a specific table in the Application Object Tree (AOT). The AOSAuthorizationProperty can be used to authorize Create, Read, Update, and Delete operations.

For more information, see Manage data access by using the Table Permissions Framework.

Tables

This section lists all database tables that are TPF-enabled by default in Microsoft Dynamics AX and the authorization requirements for those tables.

Important:
These tables store sensitive data. We recommend that you do not adjust these authorization requirements, especially in a production environment. Test your changes in a test environment so that you can study the impact on user-role permissions and make adjustments as necessary.

Table name	Authorization required for
AifChannel	Create, Update, Delete
AifSqlCdcEnabledTables	Create, Read, Update, Delete
AifValueSubstitutionComponentConfig	Create, Read, Update, Delete

Table name	Authorization required for
BankAccountTable	Create, Read, Update, Delete
BankBillOfExchangeTmp	Create, Read, Update, Delete
BankIBSLog_BE	Create, Read, Update, Delete
BatchGroup	Create, Update, Delete
BatchServerConfig	Create, Update, Delete
BatchServerGroup	Create, Update, Delete
BIAnalysisServer	Create, Read, Update, Delete
BIConfiguration	Create, Read, Update, Delete
BIPerspectives	Create, Read, Update, Delete
BIUdmTranslations	Create, Read, Update, Delete
CompanyInfo	Create, Read, Update, Delete
CreditCardCust	Create, Read, Update, Delete
CreditCardCustNumber	Create, Read, Update, Delete
CreditCardMicrosoftSetup	Create, Read, Update, Delete
CreditCardProcessorsSecurity	Create, Read, Update, Delete
CustBankAccount	Create, Read, Update, Delete
CustVendOutTmp	Create, Read, Update, Delete
EPDocuParameters	Create, Update, Delete
EPGlobalParameters	Create, Update, Delete
EPWebSiteParameters	Create, Update, Delete
ExpressionTable	Create, Update, Delete
GeneralJournalAccountEntry	Create, Read, Update, Delete
HcmPersonIdentificationNumber	Create, Read, Update, Delete
HcmWorkerBankAccount	Create, Read, Update, Delete
LedgerActivityZakatTmp_SA	Create, Read, Update, Delete
LedgerClosingSheet	Create, Read, Update, Delete
LedgerMainZakatTmp_SA	Create, Read, Update, Delete
LedgerOpeningSheet_ES	Create, Read, Update, Delete
LedgerProvisionsTmp_SA	Create, Read, Update, Delete

Table name	Authorization required for
LedgerRevenueActivityTmp_S	Create, Read, Update, Delete
LedgerZakatHeaderTmp_SA	Create, Read, Update, Delete
NumberSequenceDatatype	Create, Update, Delete
NumberSequenceScope	Create, Update, Delete
OMUserRoleOrganization	Create, Update, Delete
OMUserRoleOrganizationTmp	Create, Update, Delete
RetailSetupLog	Create, Update, Delete
ShipCarrierSQLRoleUser	Create, Read, Update, Delete
SIGCertificateUsage	Update, Delete
SIGParameters	Update, Delete
SIGProcSetup	Create, Update, Delete
SIGProcSetupField	Create, Update, Delete
SIGProdStatusChange	Update, Delete
SIGReasonCode	Create, Update, Delete
SIGReportFinished	Update, Delete
SIGSignatureDelegation	Create, Update, Delete
SIGSignatureFailure	Update, Delete
SIGSignatureLog	Update, Delete
SRSAnalysisEnums	Create, Read, Update, Delete
SRSEnabledLanguages	Create, Read, Update, Delete
SRSModelEntityCache	Create, Read, Update, Delete
SRSModelFieldCache	Create, Read, Update, Delete
SRSModelFieldRoleSortCache	Create, Read, Update, Delete
SRSModelForeignKeyCache	Create, Read, Update, Delete
SRSModelIndexCache	Create, Read, Update, Delete
SRSModelPerspectiveCache	Create, Read, Update, Delete
SRSModelPerspectiveEntityCache	Create, Read, Update, Delete
SRSModelPerspectiveFieldCache	Create, Read, Update, Delete
SRSModelPerspectiveForeignKeyCache	Create, Read, Update, Delete

Table name	Authorization required for
SRSModelPerspectiveRoleCache	Create, Read, Update, Delete
SRSModelRoleCache	Create, Read, Update, Delete
SRSModelRoleGroupsCache	Create, Read, Update, Delete
SRSReportDeploymentSettings	Create, Update, Delete
SRSServers	Create, Read, Update, Delete
SRSUpdateOptions	Create, Read, Update, Delete
SRSUserConfiguration	Create, Read, Update, Delete
SysClusterConfig	Create, Update, Delete
SysCompileILTable	Create, Read, Update, Delete
SysDataBaseLog	Update, Delete
SysExpImpField	Create, Update, Delete
SysExpImpTable	Create, Update, Delete
SysFileStore	Create, Update, Delete
SysFileStoreFile	Create, Update, Delete
SysMapParameters	Create, Read, Update, Delete
SysPerimeterNetworkParams	Create, Update, Delete
SysRecordTemplateSystemTable	Create, Update, Delete
SysRemoveConfig	Create, Read, Update, Delete
SysRemoveFields	Create, Read, Update, Delete
SysRemoveLicense	Create, Read, Update, Delete
SysRemoveTables	Create, Read, Update, Delete
SysSecurityFormControlTable	Create, Update, Delete
SysSecurityFormTable	Create, Update, Delete
SysServerConfig	Create, Update, Delete
SysSetupCompanyLog	Create, Update, Delete
SysSetupLog	Create, Update, Delete
SysSignatureSetup	Create, Update, Delete
SysSortOrder	Create, Update, Delete
SysUserInfo	Create, Delete

Table name	Authorization required for
SysWorkflowElementTable	Update, Delete
SysWorkflowFaultTable	Update, Delete
SysWorkflowInstanceTable	Update, Delete
SysWorkflowTable	Update, Delete
SysWorkflowTrackingEntry	Update, Delete
SysXppAssembly	Create, Read, Update, Delete
Tax1099BoxDetailHistory	Create, Read, Update, Delete
Tax1099IRSPayerRec	Create, Read, Update, Delete
Tax1099TransmitterParameters	Create, Read, Update, Delete
TmpBankBillofExchangePrintout	Create, Read, Update, Delete
TmpBankPromissoryNotePrintout	Create, Read, Update, Delete
TmpChequePrintout	Create, Read, Update, Delete
TrvCreditCards	Create, Read, Update, Delete
VendBankAccount	Create, Read, Update, Delete
VendCoverPageSignature	Create, Read, Update, Delete
VendRequestProspectiveProfile	Create, Read, Update, Delete
VendSubcontractorZakatTmp_SA	Create, Read, Update, Delete
VendTable	Create, Read, Update, Delete
WorkflowActionTable	Create, Update, Delete
WorkflowAssignmentTable	Create, Update, Delete
WorkflowAssociation	Create, Update, Delete
WorkflowElementLinkTable	Create, Update, Delete
WorkflowElementNotificationTable	Create, Update, Delete
WorkflowElementOutcomeTable	Create, Update, Delete
WorkflowElementTable	Create, Update, Delete
WorkflowEscalationPathTable	Create, Update, Delete
WorkflowEscalationTable	Create, Update, Delete
WorkflowMaxRuntimeTable	Create, Update, Delete
WorkflowMessageText	Create, Update, Delete

Table name	Authorization required for
WorkflowParallelBranchTable	Create, Update, Delete
WorkflowStepTable	Create, Update, Delete
WorkflowSubWorkflow	Create, Update, Delete
WorkflowSubWorkflowItem	Create, Update, Delete
WorkflowSubWorkflowTable	Create, Update, Delete
WorkflowTable	Create, Update, Delete
WorkflowTimeSpanTable	Create, Update, Delete
WorkflowVersionNotificationTable	Create, Update, Delete
WorkflowVersionTable	Create, Update, Delete
WorkflowVersionTableNotes	Create, Update, Delete
xRefNames	Create, Read, Update, Delete
xRefPaths	Create, Read, Update, Delete
xRefReferences	Create, Read, Update, Delete
xRefTableRelation	Create, Read, Update, Delete
xRefTmpReferences	Create, Read, Update, Delete

Security resources for software developers

This topic provides links to programming best practices related to security and to discussions of security in the context of individual Microsoft Dynamics AX components.

What's New: Security for Developers in Microsoft Dynamics AX 2012 (http://msdn.microsoft.com/en-us/library/gg843512.aspx)

Security for Microsoft Dynamics AX (http://msdn.microsoft.com/en-us/library/aa653742.aspx)

Best Practices: Avoiding Potential Security Issues (http://msdn.microsoft.com/en-us/library/aa625308.aspx)

AOS Security (http://msdn.microsoft.com/en-us/library/cc551159.aspx)

Security in Enterprise Portal (http://msdn.microsoft.com/en-us/library/hh608234.aspx)

Security and protection for reporting (http://msdn.microsoft.com/en-us/library/ee873253.aspx)

Security and protection for analytics (http://msdn.microsoft.com/en-us/library/ee910037.aspx)

Record level security and outbound documents (http://msdn.microsoft.com/en-us/library/aa630391.aspx)

Walkthrough: Creating a Simple Default Security Policy (http://msdn.microsoft.com/en-us/library/hh272121.aspx)

Workflow Security (http://msdn.microsoft.com/en-us/library/cc641033.aspx)

Security and .NET Business Connector Applications (http://msdn.microsoft.com/en-us/library/bb986589.aspx)

Using the MorphX Security System (http://msdn.microsoft.com/en-us/library/aa887523.aspx)

See the collection of coding recommended coding practices/Patterns white papers/whatever – ask Margo (), many of which deal with security best practices.