Microsoft Dynamics SL

Security Guidelines for Microsoft Dynamics SL

Release 2015

Disclaimer

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

Some examples are for illustration only and are fictitious. No real association is intended or inferred.

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

Sample Code Warranty disclaimer

Microsoft Corporation disclaims any warranty regarding the sample code contained in this documentation, including the warranties of merchantability and fitness for a particular purpose.

License agreement

Use of this software is covered by a license agreement provided with it. If you have any questions, please call the Customer Assistance Department at 800-456-0025 (in the United States or Canada) or +1-701-281-6500.

Copyright

Publication Date

September 2014

Contents

Introduction

Microsoft® Windows®, the foundation of Microsoft Dynamics® SL, provides sophisticated standards-based network security. In the broadest sense, security involves planning and considering trade-offs. For example, you could lock a computer in a vault and make it available to only one system administrator. This computer might be secure. However, it is not very usable because you cannot connect it to any other computer. You must consider how to make the network as secure as possible without sacrificing usability.

Most organizations plan for external attacks and construct firewalls. However, many companies do not consider how to lessen a security breach after a malicious user is inside the firewall. Security measures in your environment will work well if users are not required to perform too many procedures or too many steps in a single procedure in order to do their work in a secure manner. Implementing security policies should be as easy as possible for users, or they might seek less secure ways of doing their work.

Because the size of Microsoft Dynamics SL implementations can vary significantly, this guide tries to consider the needs of smaller sites while providing insight and guidance to larger sites. Each site must weigh the effectiveness of security against the costs involved. Use your best judgment to implement policies that help address security needs without creating a burden that can ultimately tempt managers to stop enforcing the policy.

The topic of computer security is both broad and deep. This guide is not a comprehensive security manual. Its purpose is to give you some strategies, considerations, and suggestions to help improve the level of computer security at your organization.

These guidelines will help acquaint the business decision maker, IT administrator, Microsoft Certified Partner, and accounting staff with ways of improving the security of computer networks generally and the Microsoft Dynamics SL application environment in particular. The document contains links to many articles and other resources to help you find security information that is relevant to your organization and your role.

Planning Security

Security Best Practices

For more information about how to help secure the network, see the following web topics:

- Security Guidance for Small Business
- Security TechCenter
- Securing SQL Server
- “SQL Server 2012 Security Best Practice Whitepaper”
- “Protect Your Data—Everything Else Is Just Plumbing”

General Administration

By following some general rules in administration, you can help improve the security of the Microsoft Dynamics SL environment:

- Because the system administrator has administrative credentials, other employees do not have administrative credentials over the domain. Administrator accounts should be restricted to those who have administrative responsibility for the domain users.
- Assuming that the business owner or manager has administrative credentials, users, such as accounts payable coordinators, cashiers, or sales representatives, do not have administrative credentials over the domain. These administrator accounts should be restricted to domain administrators.
- Users must not be members of the Microsoft® Windows® Guests group. Members of the Guests group who connect to Windows Server by using Remote Desktop Connection will not have access to Microsoft Dynamics SL. They will receive an abnormal program termination message and the software will not load.
- Do not reuse or share passwords across systems and domains. For example, an administrator responsible for two domains might create Domain Administrator accounts in each that use the same password, and even set local administrator passwords on domain computers that are the same across the domain. In such a case, a compromise of a single account or computer could lead to a compromise of the whole domain.
- If you use SQL Authentication, you should change the “master login” password after installation is complete and the Microsoft Dynamics SL databases are created or updated. Use *Database Administration* (98.270.00) to change the Master login password. Always keep this password confidential. It warrants the same protection you would give to the Microsoft SQL Server “sa” password if you used mixed mode authentication. All database access is funneled through the master login. This requires the highest level of protection. Only system and application administrators should know the “master login” password.
- Do not use domain administrator accounts as service accounts. Using domain administrator accounts as service accounts for common services poses a security risk because the password will be stored locally on every computer where the service resides. The compromise of one computer may compromise the whole domain.
- Although Microsoft Dynamics SL is supported on several operating systems, the newest versions of operating systems will have the most up-to-date security features. Also, operating system editions that are for business typically have additional security features. For example, BitLocker allows for encrypting of files and folders on a physical drive for added protection of sensitive data against theft or malicious users. BitLocker is included in Windows 7 Ultimate but is not available with Windows 7 Home Premium.

- Use Microsoft Update to apply the most current security updates for Windows, Office, SQL Server, and other Microsoft applications. Microsoft Update is the successor to Windows Update. For more information, see the Windows Update help page.
- Use the Windows Automatic Updates feature to keep your computers up to date with important updates. Automating the update management process by using Windows Server Update Services can help reduce IT costs and make sure of update compliance at sites that have many computers.
- For security about the application files, follow the principle of least-privilege. Give users only the minimum credentials required to access data and functionality.

  Examples of Microsoft Dynamics SL files that you should treat with this level of security are as follows:

  - General Ledger consolidation files
  - Payroll ACH files and scripts
  - Payroll tax tables
  - Transaction Import files, control macros, data files, and log files
  - EDI transaction files
  - Event logs
  - Executable files
  - Standard reports
  - \User reports directory
- When you use the *Access Rights* screen, assign rights to Microsoft Dynamics SL groups (roles), and then add users to the groups. This simplifies adding or removing employees.
- Have users log on to Microsoft Dynamics SL by using an integrated logon (Windows authentication). For more information, see “Adding Users” in the *Microsoft Dynamics SL System Manager* user’s guide (SystemManager.pdf). This can be installed when you install Microsoft Dynamics SL. A key benefit of using integrated logons is the ability to use the security features of your Windows Server® environment to help enforce strong password and password expiration policies with minimal intervention by administrators.
- If you decide not to use the recommended Microsoft Dynamics SL security authentication method, Windows authentication, then use a strong password methodology (see “Strong Passwords” on page 8 for guidelines). Implement a manual process that requires your employees to change their Microsoft Dynamics SL passwords at defined maximum intervals or define strong password policies on the server by using Group Policy objects (GPOs).
- The Application Server module can process requests based on email messages from remote employees. Malicious users could exploit this feature if they chose to send a destructive request through Application Server. We recommend that you:
  - Create a specific Exchange account for the application server to read from.
  - Make a list of employees that you will let use this feature and allow for the Application Server’s email account to process email messages only from those people. When you set up each of these users in Microsoft Dynamics SL, include their unique email addresses in the **EMail Address** box and then click to select the **Active Application Server User** check box to let Application Server accept email messages only from these specific accounts.
  - Create a Microsoft Dynamics SL user whose sole access rights are to the Application Server module. Log on as that user when you have to run Application Server.
- Focus on how to set the appropriate access rights for the following modules and applications:
  - Payroll module
  - System Manager module
  - Shared Information module
  - *Application Server* (96.010.00) – Application Server module
  - In Customization Manager:

    - *Code Window* (91.251.00)
    - *Export Customizations* (91.500.00)
    - *Import Customizations* (91.510.00)
    - *Customization Mode* (91.250.00)
  - *Project Transaction Transfer* (PA.PTT.00) – Project Controller module
  - *Password Maintenance* (PA.PWD.00) – Project Controller module
  - *Read Consolidation* (01.510.00) – General Ledger module

Physical Security

Physical security represents the best place to start preventing malicious attacks. Evaluate the following physical security issues:

- For larger deployments with dedicated IT departments, lock all server rooms and locations where software and manuals for an administrator audience are stored.
- Computers in the category would include the following:
  - The database server that is running Microsoft SQL Server
  - The file server where the Microsoft Dynamics SL executables reside
  - The file server that is used as the Application Server
  - The server(s) running IIS for Microsoft® SharePoint® and Web Services
  - The server that is running Microsoft Project Server and other server applications
- Install intrusion alarms or secure access to computer rooms and test labs.
- Store all backups of critical data offsite. Store all software in fireproof containers when not being used.
- If it is possible, deploy Microsoft Dynamics SL through a Remote Desktop Services/Terminal Services (http://technet.microsoft.com/en-us/library/dd640164(v=ws.10).aspx) implementation. Install Microsoft Dynamics SL onto a Terminal Server and have all users log on to the server to access Microsoft Dynamics SL. With this implementation, you install the Microsoft Dynamics SL files on only one computer. Therefore limiting the ability for an attacker to attack the Microsoft Dynamics SL binaries, and you have to maintain security on only one computer.
- If you have the Application Server module installed, lock the console of the computer that processes Application Server requests. Locking the console helps prevent unauthorized personnel from using the device to accessing your systems.

For the Employees

Always restrict administrative rights across all products and features. As a default, administrators should give users read-only access to system functions unless they require better access to perform their jobs. Follow the principle of least-privilege. Give users only the minimum credentials required to access data and functionality. For example, avoid requiring administrative rights as a default to run features.

Disgruntled and former employees are a threat to network security. When you evaluate security, consider implementing the following policies and procedures about employees:

- Conduct pre-employment background investigations.
- Expect “revenge” from disgruntled employees and former employees.
- When an employee leaves, immediately deactivate all associated Windows accounts and passwords. For reporting, do not delete users.
- Train users to be alert and to report suspicious activity.
- Do not grant permissions automatically. If users do not have to have access to particular computers, computer rooms, or sets of files, do not grant them access.

- Train supervisors to identify and respond to potential employee problems.
- Monitor system usage for unusual activity.
- Make sure that employees understand their roles in maintaining network security.
- Give a copy of the company policies to every employee.
- Consider restricting installation of all software on all computers to Administrators.

For the Administrator

We strongly recommend that system administrators keep up with the latest security fixes available from Microsoft. Malicious users are skilled at combining small bugs to enable large intrusions into a network. Administrators should first secure each computer as much as they can, and then add security updates. To that end, this guide contains many links and resources to help in finding valuable information and best practices.

Network complexity is another security consideration. The more complex the network, the more difficult it will be to help secure or fix it if an intruder successfully gains access. The administrator should maintain a document of the network topography.

Security is primarily concerned with risk management. Because software alone is not a cure-all, security requires a combination of technology and policy. How you use the technology ultimately determines the security level of a network. Microsoft delivers security-conscious technology and features, but only the administrator and the management can determine the best policies for each organization. Plan for security early in the implementation and deployment process. Understand what your organization wants to protect and what they are willing to do to protect it.

Finally, develop and document emergency contingency plans before they are needed. Thorough planning and solid technology will increase your level of security. For more information about general security, see the Microsoft Safety & Security Center (http://www.microsoft.com/security/default.aspx), the Security TechCenter (http://go.microsoft.com/fwlink/?linkid=151434), and *Secure Windows Server* (http://go.microsoft.com/fwlink/?linkid=191114). For information about security improvements in Windows Server 2008 R2 specifically, see *What's New in Security in Windows Server 2008 R2* at http://technet.microsoft.com/en-us/library/dd560640(WS.10).aspx. For Windows Server 2012 and 2012 R2, see the following article: http://technet.microsoft.com/en-us/library/dn250016.aspx.

Securing the Server Operating System

Although some smaller organizations do not have a server operating system, make sure that Microsoft Certified Partners understand and can communicate security best practices to larger organizations with more complex network environments. Many of the policies and practices throughout this section can easily be adapted by organizations with only client operating systems.

The concepts in this section apply to Windows Server® products. Windows Server offers a robust set of security features.

The *Windows Server 2012 Security Baseline* contains the security guide for this Windows Server product.

The *Windows Server 2008 Security Guide* provides specific recommendations about how to harden computers that run Windows Server® 2008 in the following distinct enterprise environments:

- Enterprise Client (EC) – In this environment, organizations seek to balance security and functionality. Typical security-conscious enterprises, government departments, and other organizations should start with the EC setting recommendations and customize them to meet their individual circumstances and requirements.
- Specialized Security - Limited Functionality (SSLF) – In this environment, organizations maintain very rigorous security standards. Concern for security is so great that a significant loss of functionality and manageability is acceptable. SSLF setting recommendations are designed for organizations and departments with national/regional security responsibilities or that handle highly classified information.

Warning The SSLF security settings are not intended for most organizations. The configuration for these settings is developed for organizations where security is a larger priority than functionality.

Guidance about how to harden computers is provided for a group of distinct server roles. The countermeasures described and the tools that are provided assume that each server will have a single role. If you have to combine roles for some servers in your environment, you can customize the security templates that are included in the downloadable version of the guide to create the appropriate combination of services and security options. The server roles that are referenced in this guide include the following:

- Domain controllers that also provide DNS services
- Infrastructure servers that provide WINS and DHCP services
- File servers
- Print servers
- Web servers that run Internet Information Services (IIS)
- Internet Authentication Service (IAS) servers
- Certificate Services servers
- Bastion hosts

A similar guide is available as part of a solution accelerator for Windows Server 2008, the *Microsoft Security Compliance Manager*. The solution accelerator also includes a utility that creates all the Group Policy objects (GPOs) you must have to deploy the security configuration that you select. For more information about the solution accelerator, such as a link to download the guide, see http://go.microsoft.com/fwlink/?linkid=113940. For more information about Group Policy settings in Windows Server 2008 R2, see the Group Policy page at http://technet.microsoft.com/en-us/library/cc726027(WS.10).aspx.

More information about security tools can be found at http://social.technet.microsoft.com/wiki/contents/articles/microsoft-security-compliance-manager-scm-baseline-download-help.aspx.

Authentication

Authentication is a fundamental aspect of system security. It confirms the identity of any user who is trying to log on to a domain or access network resources. The weak link in any authentication system is the user's password.

Passwords provide the first line of defense against unauthorized access to the domain and local computers. Implement the following password best practices where they are suitable for your organization.

Password Protection

- Always require strong passwords. For more information, see "Strong Passwords."
- If you must note passwords on a piece of paper, store the paper in a secure location and destroy it when you no longer need it.
- Never share passwords.
- Use different passwords for all user accounts.
- Change compromised passwords immediately.
- Be careful about saving passwords on computers. Some dialog boxes, such as those for remote access and other telephone connections, present an option to save or remember a password. Selecting this option poses a potential security threat because the password is stored in the system registry.
- Educate users about how best to protect their accounts from unauthorized attacks, especially if you cannot enforce password policies by using group policies on the server.

Strong Passwords

The role that passwords play in securing an organization's network is frequently underestimated and overlooked. As mentioned, passwords provide the first line of defense against unauthorized access to your organization. The Windows Server family has a feature that checks the complexity of the password for the Administrator account during the setup of the operating system. If the password does not meet complexity requirements, the *Windows Setup* dialog box appears, warning of the dangers of not using a strong password for the Administrator account. In a workgroup environment, a user cannot access a computer over the network by using an account that has a blank password. Weak passwords provide an attacker with easy access to computers and the network, whereas strong passwords are significantly more difficult to compromise, even with the password-cracking tools available today.

Password-cracking tools continue to improve, and the computers that are used to reveal passwords are more powerful than ever. The software uses one of three approaches: intelligent guessing, dictionary attacks, and brute-force automated attacks that try every possible combination of characters. Given enough time, the automated method can discover any password. However, strong passwords are much more difficult to expose than weak passwords. A secure computer has strong passwords for all user accounts.

A weak password:

- Is no password at all.
- Contains the user's user name, real name, or company name.
- Contains a complete dictionary word. For example, the word *password* is a weak password.

A strong password:

- Is at least seven characters long.
- Does not contain the user's user name, real name, or company name.
- Has no personal information (employee ID, social security number, birth date, telephone number, and so on).
- Does not contain a complete dictionary word.

- Is significantly different from previous passwords. Passwords that increment (*Password1*, *Password2*, *Password3*, and so on) are not strong.
- Contains characters from each group that is listed in the following table.

Group	Examples
Uppercase letters	A B C D
Lowercase letters	a b c d
Numbers	0 1 2 3 4
Symbols	` ~ ! @ # $ % ^ & * ( ) _ + - { } | [ ] \ : “ ‘ < > ? , . /

Examples of strong passwords are *Pa$sw0rD* and *J*p2le04>F*.

A password can meet most of the criteria of a strong password but still be weak. For example, *Hello2U!* is a fairly weak password even though it meets most of the criteria for a strong password and most of the complexity requirements of the password policy. *H!elZl2o* is a strong password because the dictionary word is interspersed with symbols, numbers, and other letters. It is important to educate managers and users about the benefits of using strong passwords and to teach them how to create truly strong passwords.

Because strong passwords are frequently difficult to memorize, Microsoft has published an article to help users create strong passwords that are easier to remember. See “Create strong passwords” for more information.

Passwords can be created that contain characters from the extended ASCII character set. Using extended ASCII characters increases the number of characters from which users can select when they create a password. Therefore, it might take more time for password-cracking software to reveal passwords that contain these extended ASCII characters than it does to discover other passwords. Before you use extended ASCII characters in your password, test them thoroughly to make sure that passwords that contain extended ASCII characters are compatible with other applications that the organization uses. Be especially cautious when you use extended ASCII characters in passwords if the organization uses several different operating systems.

You can find extended ASCII characters in the Character Map. Some extended ASCII characters should not be used in passwords. Do not use a character if a keystroke is not defined for it in the lower-right corner of the *Character Map* dialog box. For more information about how to use *Character Map*, see Windows Server Online Help.

Examples of passwords that contain characters from the extended ASCII character set are *kUµ!¶0€㊽’ƒ†‡‰o* and *Wf©$0k#»g¤5ªrd*.

You can implement a password policy that enforces password complexity requirements. For more information about this policy, see “Creating a Strong Password Policy” on the Microsoft TechNet website.

Defining the Password Policy

When you define your password policy, create a policy that will require all user accounts to have strong passwords. The following Windows Server settings require strong passwords.

- Define the **Enforce password history** policy setting to remember several previous passwords. With this policy setting, users cannot use the same password when their password expires.
- Define the **Maximum password age** policy setting so that passwords expire as frequently as necessary for the environment, typically, every 30 to 90 days.
- Define the **Minimum password age** policy setting so that passwords cannot be changed until they are more than a certain number of days old. This policy setting works in combination with the **Enforce password history** policy setting. If you define a minimum password age, users cannot repeatedly change their passwords to avoid the **Enforce password history** policy setting and then use their original passwords. Users must wait the specified number of days to change their passwords.

- Define a **Minimum password length** policy setting so that passwords must consist of at least a specified number of characters. Long passwords (seven or more characters) are usually stronger than short passwords. With this policy setting, users cannot use blank passwords and they have to create passwords that are at least a certain number of characters long.
- Enable the **Password must meet complexity requirements** policy setting. This policy setting checks all new passwords to help ensure that they meet basic strong password requirements. For a full description of how to set these requirements, see "AD DS Fine-grained Password and Account Lockout Policy Step-by-Step Guide" on the Microsoft TechNet website.

Defining an Account Lockout Policy

Be careful when you define the account lockout policy. Although using an account lockout policy increases the probability of thwarting an unauthorized attack on your organization, you can also lock out authorized users unintentionally. This is also costly to resolve.

If you decide to apply the account lockout policy, set the **Account lockout threshold policy** setting to a high enough number that authorized users are not locked out of their user accounts because they mistype a password.

Authorized users can be locked out if they change their passwords on one computer, but not on another computer. The computer that is still using the old password will continuously try to authenticate the user who has the old password, and it will eventually lock out the user account. This might be a costly result of defining an account lockout policy, because the authorized users cannot access network resources until an administrator restores their accounts. This issue does not exist for organizations that use only domain controllers that are members of the Windows Server family.

For more information about account lockout policy, see "Account Policies" on the Microsoft TechNet website. For information about how to apply or change account lockout policy, see "Server Security Policy Management Tools," also on the Microsoft TechNet website.

Access Control

A Windows network and its resources (including Microsoft Dynamics SL files) can be secured by considering what rights users, groups of users, and other computers have on the network. You can secure a computer or multiple computers by granting users or groups specific user rights. You can secure an object, such as a file or a folder, through assigning permissions to let users or groups to perform specific actions on that object. Key concepts that make up access control include the following:

- Permissions
- Ownership of objects
- Inheritance of permissions
- User rights
- Object auditing

Permissions

Permissions define the kind of access granted to a user or group for an object or object property such as files, folders, and registry objects. You can apply permissions to any secured objects such as files or registry objects. You can also grant permissions to any user, group, or computer. It is a good practice to assign permissions to groups.

Ownership of Objects

An owner is assigned to an object when an object is created. Be aware that in Windows Server, when a member of the Administrators group creates an object, the Administrators group becomes the owner, instead of the individual account that created the object. You can change this behavior through the Local Security Settings Microsoft Management Console (MMC) snap-in, by using the setting **System objects: Default owner** for objects that are created by members of the Administrators group.

Regardless of what permissions are set on an object, the owner of the object can always change the object permissions. For more information, see "Managing Object Ownership" on the Microsoft TechNet website.

Inheritance of Permissions

Inheritance lets administrators assign and manage permissions easily. This feature automatically sets objects inside a container with the inheritable permissions from the container. Only permissions marked as inherited will be inherited.

User Rights

User rights grant specific permissions and logon rights to users and groups in your computing environment. For information about user rights, see "User Rights" on the Microsoft TechNet website.

Object Auditing

You can audit users' access to objects. View the security-related events in the Security log by using the Event Viewer. For more information, see "Global Object Access Auditing" on the Microsoft TechNet website.

Access Control Best Practices

- Assign permissions to groups instead of to users. Because it is inefficient to maintain user accounts directly, assigning permissions on a user basis should be the exception.
- Use Deny permissions for certain special cases. For example, you can use Deny permissions to exclude a subset of a group that has Allow permissions. Use Deny permissions to exclude a specific permission when you have already granted full control to a user or group.
- Never deny the Everyone group access to an object because that group includes administrators. A better solution would be to remove the Everyone group, as long as you give other users, groups, or computers permissions to that object.
- Assign permissions to an object as high on the tree as possible and then apply inheritance to propagate the security settings through the tree. You can quickly and effectively apply access control settings to all children or a subtree of a parent object. By doing this, you gain the greatest breadth of effect with the least effort. The permission settings that you establish should be sufficient for most users, groups, and computers.
- Explicit permissions can sometimes override inherited permissions. Inherited Deny permissions do not prevent access to an object if the object has an explicit Allow permission entry. Explicit permissions take precedence over inherited permissions, even inherited Deny permissions.
- For permissions on Active Directory® objects, make sure that you understand the best practices specific to Active Directory objects. For more information, see "View or Set Permissions on a Directory Object" on the Microsoft TechNet website.

Single Sign-on

A key feature of Windows Server family authentication is its support of single sign-on. Single sign-on lets a user to log on to the Windows domain one time, by using a single password, and authenticate to any computer in the Windows domain without having to re-enter that password.

A single sign-on provides two main security benefits for:

- Users — Use of a single password or smart card reduces confusion and improves work efficiency.
- Administrators — Administrative support that is required for domain users is reduced because the administrator has to manage only one account per user.

Authentication that includes single sign-on, is implemented as a two-part process: interactive logon and network authentication. Successful user authentication depends on both processes. For more information about how to configure the Windows single sign-on feature, see ”Windows Server 2012 AD FS Deployment Guide” on Microsoft TechNet.

External Security Firewall

A firewall is a piece of hardware or software that prevents data packets from either entering or leaving a specified network. To control the flow of traffic, numbered ports in the firewall are either opened or closed to information packets. The firewall examines several pieces of information in each arriving or departing packet: the protocol through which the packet is being delivered, the destination or sender of the packet, the kind of content that is contained in the packet, and the port number to which it is being sent. If the firewall is configured to accept the specified protocol through the targeted port, the packet is allowed through. Microsoft has released Forefront Threat Management Gateway ("Forefront TMG") 2010 as a successor to ISA Server 2006. In addition to the protection offered by a traditional firewall, Forefront TMG 2010 also provides new URL filtering, anti-malware, and intrusion-prevention technologies to help protect businesses against the latest Web-Based threats. Read more about Forefront TMG at Forefront Threat Management Gateway (TMG) 2010.

Securing the Database

By default, Microsoft SQL Server encrypts the pre-logon credential exchange. To run a secure Microsoft Dynamics SL environment, you must take steps to protect communications between the Microsoft Dynamics® SL client and Microsoft® SQL Server®.

When you can, use Secure Sockets Layer (SSL) to help secure the communication link between the Microsoft Dynamics SL client and Microsoft SQL Server. When you configure SQL Server to use SSL, all the data transmitted between client and server (and vice versa) can be encrypted to help ensure that data remains confidential while in transit between the client and SQL Server. If you currently do not use SSL certificates, you can issue your own certificates by using Microsoft Certificate Services. This is an optional feature of Windows Server®, or you can obtain certificates from a commercial certification authority.

For more information about how to configure certificates, see “Configuring Certificate for Use by SSL” at msdn.microsoft.com/en-us/library/ms186362.aspx.

Additional SQL Server Security Settings

Because Microsoft Dynamics SL relies intrinsically on SQL Server, make sure that you take measures to improve the security of the SQL Server installation. The following steps will help increase SQL Server security:

- Install the latest operating system and SQL Server service packs and updates. Check the Microsoft Safety & Security Center for the latest details.
- For file system-level security, install all SQL Server data and system files on NTFS partitions. You should make the files available only to administrative or system-level users through NTFS permissions. This helps safeguard against users who access those files when the MSSQLSERVER service is not running.
- Use a low-privilege domain account or the LocalSystem (recommended) account for SQL Server service (MSSQLSERVER). This account should have minimal rights in the domain and should help contain (but not stop) an attack to the server if there is a compromise. In other words, this account should have only local user-level permissions in the domain. If SQL Server is using a Domain Administrator account to run the services, a compromise of the server will lead to a compromise of the whole domain. Use SQL Server Management Studio to set permissions. The access control lists (ACLs) on files, the registry, and user rights will be changed automatically.

You can find SQL Server security information at the Microsoft SQL Server center.

Securing Microsoft Dynamics SL

Microsoft Dynamics SL provides several levels of security. This section provides an overview of the security features in Microsoft Dynamics SL. Please see also the System Manager Help or user's guide for more information about security and step-by-step instructions for creating users, groups, and access rights.

System Access

You select an authentication method—the process by which Microsoft Dynamics SL verifies a user's logon information--when you create or upgrade an application database. Windows authentication and SQL Server authentication are supported methods. However, some features, such as Microsoft Dynamics SL Web Apps, require Windows Authentication.

Windows Authentication

Windows Authentication is highly recommended for verifying users' credentials before they gain access to Microsoft Dynamics SL data. In this mode, each Microsoft Dynamics SL user must be associated with a Windows account.

A Microsoft Dynamics SL user is added in *User Import* (95.300.00) or *User Maintenance* (95.260.00). The user ID that is created is mapped to their Windows user account. When the user logs on to Microsoft Dynamics SL, they are authenticated by using their Windows user credentials

A Microsoft Dynamics SL user's credentials can be further secured in *User Maintenance* (95.260.00) by adding a strong password and entering a Windows user name to associate the Microsoft Dynamics SL user with the Windows user. This lets Microsoft Dynamics SL users who perform the same tasks or share roles the ability to log on with one Windows authenticated user name and password.

Using application roles prevents unauthorized access to Microsoft Dynamics SL data. When you add users in *User Import* (95.300.00) or *User Maintenance* (95.260.00), they become members of the MSDynamicsSL database role. Although this grants them access to the Microsoft Dynamics SL databases, they cannot run Microsoft SQL Server utilities such as SQL Server Management Studio to gain access to objects in the Microsoft Dynamics SL databases. Access to Microsoft Dynamics SL database objects is granted to the MSDSL application role. A user must access Microsoft Dynamics SL data through the Microsoft Dynamics SL applications unless they are a Microsoft Dynamics SL administrator, the role that has all rights to the Microsoft Dynamics SL databases and their objects.

Be aware that the SQL Server Administrator can differ from the Microsoft Dynamics SL Administrator when you use Windows Authentication. More information about how to configure security in this manner can be found in the System Manager Help or user's guide, in the *Maintaining Security* section. The specific instructions for the **Grant this user permission to create SQL Server logins and users** check box demonstrates this scenario.

MSDSL Application Role

Using application roles prevents unauthorized access to Microsoft Dynamics SL data. An application role limitation in Microsoft Dynamics SL requires you to use a secure SQL Server logon to gain access to the databases and perform certain procedures. When you add users in *User Import* (95.300.00) or *User Maintenance* (95.260.00), they become members of the MSDynamicsSL database role. Although this grants them access to data, they cannot run SQL Query Analyzer, SQL Management Studio, or any other utility to gain access to objects in the Microsoft Dynamics SL databases. Access to Microsoft Dynamics SL database objects is granted to the MSDSL application role. A user must access Microsoft Dynamics SL data through the applications, unless they are a Microsoft Dynamics SL administrator, the role that has all rights to the databases and their objects.

Report Logon

A separate SQL Server login with read-only permissions is created for use in Database Maintenance for all reporting and possible values lists. Crystal Reports, SSRS Reports, and Management Reporter access data in Microsoft Dynamics SL by using this login.

SQL Server Authentication

Access to the system and application databases is granted by using SQL Server logon credentials that are protected with a password. Each Microsoft Dynamics SL user must log on with a user name and a strong password (see "Strong Passwords" on page 8 for guidelines).

Company and Application Access

Microsoft Dynamics SL security controls access to system-wide configuration and run-time information by restricting these kinds of actions to Microsoft Dynamics SL administrators. Microsoft Dynamics SL administrators are those users who are members of the Microsoft Dynamics SL Administrators group.

A user can log on to any company. However, their access rights, or the rights of the group they are assigned to, must be granted before they can run applications for that company, See the System Manager Help or user's guide for information about specific access rights and setup steps.

Product Deployment Security

Microsoft Dynamics SL can be deployed in many ways. This includes Client Only, Client/File Server, and Terminal Services/Remote Desktop installations.

Terminal Services Installations (more secure)

Terminal Services uses the Remote Desktop Protocol (RDP) to communicate between client and server. After you deploy an application on a terminal server, clients can connect over a remote access connection, local area network (LAN), wide area network (WAN), or the Internet. From a security perspective, there are several benefits to running the Microsoft Dynamics SL client on a Terminal Services:

- Only keyboard strokes and images of information that is displayed on the Terminal Services server are transmitted over the network. Microsoft Dynamics SL data is not transmitted over the network to client computers. This reduces the threat of a malicious user obtaining data that was stored on a user's client computer.
- No data is processed, cached, or stored on a user's local computer. All data processing, caching, and storage occur on the server that is running Microsoft Dynamics SL
- If a user's client computer is misappropriated or lost, a malicious user would not have access to Microsoft Dynamics SL data on that computer. If a security update were issued for Microsoft Dynamics SL, that update would only have to be applied to the Terminal Services computers. This means that the overall Microsoft Dynamics SL attack surface is minimized.

Client Installations and Client/File Server Installations

There are several reasons why it is less secure to deploy the Microsoft Dynamics SL client on users' computers than it is to deploy the Microsoft Dynamics SL client on a Terminal Services deployment, as discussed earlier in this section.

- Microsoft Dynamics SL data sent between the client and SQL Server is at more risk of being intercepted by a malicious user because there is more data being sent over the network.
- Data that is stored on individual computers is at more risk of being accessed by a malicious user if users are not diligent about securing their computers, or if a computer is lost or stolen.
- If users have access to the Internet, there is a more risk of virus attacks or problems with malicious software on the client computer.
- Your computing environment is at more risk if your business or organization does not enforce a policy that requires users to download and install security updates as soon as they are available.

To help reduce the security risk in these deployment methods, you should consider the following checklist:

- ✓ Always specify least-privileges when you set up and configure Microsoft Dynamics SL user security features.
- ✓ Educate users about how to use strong passwords and define password policies.
- ✓ Enable Windows Firewall or another firewall device on each computer.
- ✓ Enable a virus scanner on each computer.
- ✓ Deploy smart cards in your business or organization.

Upload to SharePoint and Attachments

Upload to SharePoint and Attachments features can be secured on SharePoint with same methods as described for Doc Share except for creating new sites or document libraries permissions.

You may want to separate the SharePoint user groups for each feature. This would mean that you would have the three SharePoint user groups for Doc Share and in addition have two groups for Upload to SharePoint and two for Attachments.

1. Create two SharePoint user groups representing the Attachments actions a user can perform. For clarity, give the groups names such as *AttachmentUpload*, and *AttachmentView*.
2. Create two SharePoint user groups representing the Upload to SharePoint actions a user can perform. For clarity, give the groups names such as *ROIUpload*, and *ROIView*.
3. In SharePoint, create two new permission levels, *Attachment Contribute* and *ROI Upload Contribute*. See "*Doc Share Security Considerations*" in the System Manager Help or user's guide for more information about how to create permission levels.
4. Assign the Attachment Contribute permission level to the AttachmentUpload group and the ROI Upload Contribute permission level to the ROIUpload group.
5. Associate the AttachmentView group and the ROIView group with the Visitors group in SharePoint.

Additional Microsoft Dynamics SL areas to help secure

- SharePoint Web Service Security – see page 21
- Web Services Security – see page 27
- Web Apps Security - see page 29
- Securing Business Analyzer and Report Server for use with Microsoft Dynamics SL – see page 23

SharePoint Web Service Security

This section provides information to help you configure the SharePoint Web Service to run on a server that has strong Internet Information Services (IIS), SharePoint, and Windows security settings. The steps describe a *recommended* security setup for the integration with SharePoint features such as Doc Share. This particular setup may not be appropriate for all businesses. Carefully consider your business needs when you select a security setup that must also limit access to the SharePoint Web Service.

Note: The Web Service itself does not expose any security settings.

Three kinds of users will access documents sent to a SharePoint site by using Doc Share:

- Your employees who use the Doc Share and Report Upload to SharePoint features from the Microsoft Dynamics SL applications
- Employees who access the SharePoint site directly
- External users, such as your company's customers, who may view content on the SharePoint site through an extranet

The instructions in this section apply to security for employees who use Microsoft Dynamics SL. The SharePoint administrator (a user who has SharePoint site administration credentials) can secure access for external users on a case-by-case basis. For example, the SharePoint administrator may create a new Windows user account for each external user, granting the account access to a single SharePoint site or document library.

Employees who use the SharePoint Web Service can perform three kinds of actions:

- Create new sites or document libraries
- Upload documents to sites or document libraries
- View SharePoint content

To set up SharePoint Web Service security:

1. Deny unauthenticated users access to the IIS-related file, DocShareService.asmx. This step prevents unwanted manipulation of SharePoint sites through the SharePoint Web Service.

Note: Integrated Windows authentication through IIS is the only supported authentication scheme for the SharePoint Web Service.

2. Create three SharePoint user groups representing the three Doc Share actions a user can perform. For clarity, give the groups names such as *DocShareCreate*, *DocShareUpload*, and *DocShareView*.
3. In SharePoint, create two new permission levels, *Doc Share Create* and *Doc Share Contribute*. See "Doc Share Security Considerations" in the System Manager Help or user's guide for more information about how to create permission levels.
4. Assign the Doc Share Create permission level to the DocShareCreate group and the Doc Share Contribute permission level to the DocShareUpload group.
5. Associate the DocShareView group with the Visitors group in SharePoint.

Note: These steps give users in the SharePoint groups that you created access to all the subsites under the root Doc Share sites configured in *SharePoint Site Configuration* (98.360.00). To help make your system more secure, you should consider creating a SharePoint subsite for each of your customer, vendor, and project entities. Then you can customize permission levels that offer the best protection for each subsite.

6. Use IIS to grant access to the DocShareService.asmx file for each employee’s Windows user account. Deny access to everyone else.
7. Add each employee’s Windows user account to the appropriate new SharePoint group.

Securing Business Analyzer and Report Server for use with Microsoft Dynamics SL

The resources on the Report Server that you have to help secure include reports, data sources, and data sets. After you deploy the reports to a report server, several Data Source and Data Sets are created on the Report Server. The Data Sets use the Data Sources to obtain data and have no special security considerations. A Report Server Data Source defines the credentials needed to access the Microsoft Dynamics SL databases. The Data Sources use the “Report User” credentials to access the data. This same access method is used when you print reports in Microsoft Dynamics SL.

Additionally, Windows Accounts that require the ability to change the reports while they are stored on the Report Server need additional setup. The Users would use the Report Builder Utility to change the report. However, the Report Builder link does not appear on the item menu until the Windows Account is set up as a System User on the Report Server, by using the “Site Settings” menu. SQL Reporting Services, not Microsoft Dynamics SL, dictates this stipulation.

SSRS in Native Mode

When you install Reporting Services in native mode, these resources are secured by using Reporting Services Security Roles. The *Microsoft Dynamics SL Report Server Configuration Console* creates the following roles:

SQL Security Role	**Microsoft Dynamics SL permissions**	**Purpose**
Dynamics Folder	The user has no access rights for any Report Server reports.	A Windows account that has this permission can see what reports exist in the folders on the Server but cannot run the report
Dynamics Browser	The user has View rights to one or more Report Server reports.	A windows account that has this permission can run the given report and browse the data rendered in the report
Dynamics Publisher	The user has Update rights to one or more Report Server reports.	A Windows account that has this permission can see what reports exist in the folders, run the report and load the report into the Report Builder application and change the report
Dynamics Deploy	The user has rights to the RS.DEP.LO screen.	A windows account that has this permission can add new reports to the server and change the security setting of the Data Sources, Reports, and Data Sets

Windows User Accounts are granted rights to the Report items hosted on a SQL Server Report Server based on data in *Access Rights Maintenance* (95.270.00). Each report file that is hosted on a Report Server for use with Business Analyzer is assigned a screen number in Microsoft Dynamics SL. When the report is deployed to a Report Server Site, the appropriate permissions are applied to the report. If a Microsoft Dynamics SL user has View rights to the report, they are granted the Dynamics Browser permission. If the user has no rights to the Microsoft Dynamics SL screen number, they will be granted the Dynamics Folder permission. Update rights to the screen will give the user the Dynamics Publisher Permission. If the Microsoft Dynamics SL user is a member of the Administrators group in Microsoft Dynamics SL, their Windows Account is granted the Content Manager permission. Finally, if the Microsoft Dynamics SL user is granted rights to the RS.DEP.LO screen they are additionally given the Dynamics Deploy permission.

SSRS in SharePoint Integrated Mode

When you install Reporting Services in SharePoint Integrated mode, these resources are secured by using SharePoint permissions. The *Microsoft Dynamics SL Report Server Configuration Console* creates the following permissions:

SharePoint Security Permission	**Microsoft Dynamics SL permissions**	**Purpose**
Dynamics Folder	The user has no access rights for any Report Server reports.	A Windows account that has this permission can see what reports exist in the folders on the Server but cannot run the report
Dynamics Browser	The user has View rights to one or more Report Server reports.	A windows account that has this permission can run the given report and browse the data rendered in the report
Dynamics Publisher	The user has Update rights to one or more Report Server reports.	A Windows account that has this permission can see what reports exist in the folders, run the report and load the report into the Report Builder application and change the report
Dynamics Deploy	The user has rights to the RS.DEP.LO screen.	A windows account that has this permission can add new reports to the server and change the security setting of the Data Sources, Reports, and Data Sets

Windows User Accounts are granted rights to the Report items hosted on a SQL Server Report Server based on data in *Access Rights Maintenance* (95.270.00). Each report file that is hosted on a Report Server for use with Business Analyzer is assigned a screen number in Microsoft Dynamics SL. When the report is deployed to a Report Server Site, the appropriate permissions are applied to the report. If a Microsoft Dynamics SL user has View rights to the report, they are granted the Dynamics Browser permission. If the user has no rights to the Microsoft Dynamics SL screen number, they are granted the Dynamics Folder permission in addition to the SharePoint permission of “Limited Access.” Update rights to the screen grant the user the Dynamics Publisher permission. If the Microsoft Dynamics SL user is a member of the Administrators group in Microsoft Dynamics SL, their Windows Account is granted the SharePoint permission of “Full Control.” Finally, if the Microsoft Dynamics SL user is granted rights to the RS.DEP.LO screen they are also granted the Dynamics Deploy permission.

Web Services Security

This section discusses run-time security for Microsoft Dynamics SL Web Services, instead of administration. Web Services administration is performed through screens in the client. For more information about how to administer Web Services, see the System Manager Help or user's guide. Please see also Web Services user's guide for more information about how to write consumers.

Web Services runs on Windows Communication Foundation (WCF). WCF security techniques and best practices are beyond the scope of this document.

Authentication

Consumer-to-Service Authentication

Microsoft Dynamics SL Web Services supports Windows Authentication exclusively. IIS Applications used to host Web Services should always be configured to use Windows Authentication and no other kind of authentication.

Exposing a web service outside the domain is not supported. To access a web service remotely, configure a virtual private network (VPN). This lets remote users securely log on to the domain. VPN setup and configuration is beyond the scope of this document.

Service-to-Database Authentication

Microsoft Dynamics SL Web Services supports Windows Authentication exclusively. The instance of SQL Server hosting the Microsoft Dynamics SL databases must enable Windows Authentication for Web Services to function.

Web servers that host Microsoft Dynamics SL Web Services should be located on a trusted subnet with the instance of SQL Server that hosts the Microsoft Dynamics SL databases, to improve performance and simplify security. Avoid putting firewalls or other security layers between your web servers and your SQL Server as a best practice. Instead, put emphasis on protecting the subnet.

For a web service to authenticate with SQL Server, the IIS application pool account running the web service must be a member of the TrustedWebService role in SQL Server, a role that the web service installation process creates. Membership in this group is maintained through System Manager's *Trusted Web Service Account Maintenance* (95.261.00). For more information, see the System Manager Help or user's guide.

As a best practice, each account in the TrustedWebService role should be a least-privileged, noninteractive domain user account. It is very important to follow the best practices listed earlier in this document to protect the credentials of each TrustedWebService account against unauthorized use. Anyone with access to an account in the TrustedWebService role also has access to the Microsoft Dynamics SL databases.

Authorization

After a user is successfully authenticated by using IIS, they must be authorized to access Web Services. The LoginWindows and LoginForms web services are used to conduct authorization. You do not have to run both login web services. To determine which login web service best fits the needs of your organization, see the Web Services Help or user's guide.

It is a best practice that authorization to access each IIS application that hosts web services be granted to a Windows group that contains all Microsoft Dynamics SL users in the domain. Then, you can grant or revoke permissions for individual users in System Manager's *Access Rights Maintenance* (95.270.00), without changing IIS settings. By default, all Microsoft Dynamics SL users (including SYSADMIN) are denied permissions to all web services.

To avoid potential security weaknesses around authorization, avoid using impersonation in any IIS application that hosts Web Services. Anonymous users should always be denied access to an IIS application that hosts a web service.

Channel Security

Because web services transmit and receive sensitive, sometimes personally-identifiable information, it is required that Web Services only be exposed on secure channels. Every IIS application that hosts a web service must be configured to use SSL/TLS. This is enforced for the LoginForms web service because it transmits passwords over the network.

Consumer Security

Web Services offers HTML-encoding for string-based data for web service consumers that request it. This functionality is made easier by the Anti-XSS Library 4.0. HTML-encoding helps protect web-based consumers from cross-site scripting attacks. For more information, see the Web Services Help or user's guide.

Windows Communication Foundation (WCF) Configuration

When Web Services is installed on an IIS application, the installer automatically inserts content into the IIS application's web.config file. Similarly, the uninstall process removes content from the web.config file. It is a best practice to create a backup of the web.config file before you install or uninstalling Web Services.

By default, a WCF custom binding named "basicHttpsBinding" is used to expose web services. This is the only supported binding for exposing a web service endpoint and should not be changed except as described in the Web Services Help or user's guide. Although you may be able to successfully expose a web service by using another binding without losing any functionality, you do this at your own risk.

URLs used to expose a web service may be changed from the default settings while maintaining a supported configuration. Similarly, by default service metadata is exposed, although it does not have to be exposed to remain supported.

WCF settings not mentioned here or in the Web Services Help or user's guide can be changed if you want, but configurations that conflict with guidance in these documents are unsupported.

Web Apps Security

This section discusses security for Microsoft Dynamics SL Web Apps.

Use *Trusted Web Service Account Maintenance* (95.261.00) to control membership in the TrustedWebService role in SQL Server. Specify one of these users as the Identity user when you deploy Web Apps.

As a best practice, each account in the TrustedWebService role should be a least-privileged, noninteractive domain user account. It is very important to follow the best practices listed earlier in this document to protect the credentials of each TrustedWebService account against unauthorized use. Anyone with access to an account in the TrustedWebService role also has access to the Microsoft Dynamics SL databases.

Use *Access Rights Maintenance* (95.270.00) to secure Web Apps. See the steps in the “Deploy Microsoft Dynamics SL Web Apps” topic, the “Securing Microsoft Dynamics SL Web Services” topic, and the “Access Rights” topic in the Microsoft Dynamics SL Web Apps Deployment Guide.

Configure timeouts by using IIS and web.config settings. See the “Setting Timeouts” topic in the Microsoft Dynamics SL Web Apps Deployment Guide.

Virus and Malware Protection

A computer virus is an example of an executable file that replicates itself, erases or corrupts data files and programs, and avoids detection. In fact, viruses are frequently rewritten and adjusted to avoid detection. Viruses are frequently sent as email message attachments. Antivirus programs must be updated regularly to look for new and changed viruses. Viruses are the number one method of computer vandalism.

Antivirus software is designed specifically for the detection and prevention of virus programs. Because new virus programs are created constantly, many makers of antivirus products offer anti-malware protection against multiple kinds of malicious software. We strongly recommend implementing antivirus/anti-malware software in your environment.

Virus software is usually installed on all user workstations, servers, and the network where email messages come into (and in some cases, leave) the organization.

The constantly-evolving nature of malware makes documenting current mitigation efforts difficult. Threats that are known at the time of this writing may become superseded by new threats quickly. We recommend that you review information on the latest threats periodically. The Microsoft Security Center is a good place to start.

Virus Prevention Best Practices

You can help prevent the spread of a computer virus. Consider implementing the following:

- Install a virus protection solution that scans incoming messages from the Internet for viruses before the messages pass the router. This helps ensure that email messages are scanned for known viruses.
- Know the source of incoming documents. Users should not open documents unless they are from someone the user feels is trustworthy.
- If users are at all unsure whether a document is safe, they should contact the person who created the document.
- Use the Microsoft Office macro virus protection. In Office, the applications warn the user if a document contains macros. This feature lets the user either enable or disable the macros before they open the document. You can also configure Office applications to prevent all macros from running.
- Use virus-scanning software to detect and remove macro viruses. Virus-scanning software can detect and frequently remove macro viruses from documents. We recommend that you use antivirus software that is certified by the International Computer Security Association (ICSA).

For more information about viruses and computer security generally, see the following Microsoft security websites:

- Microsoft Safety & Security Center
- Microsoft TechNet Security TechCenter

Network Security Strategies

Network architecture is constantly evolving in functionality, security, and complexity. The addition of virtualization technology increases complexity.

Because the design and deployment of an Internet Protocol (IP) Internetworking environment requires balancing private and public network concerns, the firewall has become a key ingredient in safeguarding network integrity. A firewall is not a single component. The National Computer Security Association (NCSA) defines a firewall as “a system or combination of systems that enforces a boundary between two or more networks.” Although different terms are used, that boundary is frequently known as a perimeter network. The perimeter network protects your intranet or enterprise local area network (LAN) from intrusion by controlling access from the Internet or other networks.

The following illustration shows a perimeter network bounded by firewalls and positioned between a private network and the Internet in order to help secure the private network:

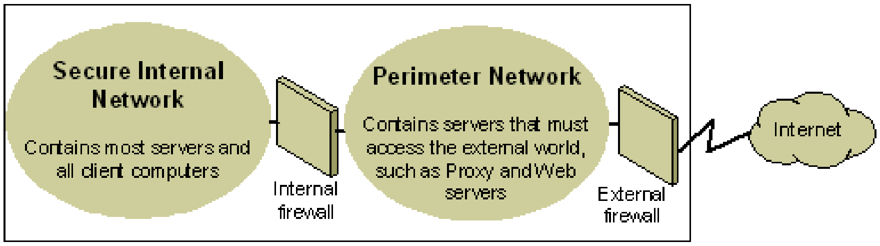
Secure Internal Network
Contains most servers and all client computers
Internal firewall
Perimeter Network
Contains servers that must access the external world, such as Proxy and Web servers
External firewall
Internet

Figure 1: Basic Perimeter Network

Organizations vary in their approach to using firewalls for providing security. IP packet filtering offers weak security, is cumbersome to manage, and can easily be defeated. Application gateways are more secure than packet filters and easier to manage because they pertain only to some specific applications, such as a particular email system. Circuit gateways are most effective when the user of a network application is of more concern than the data being passed by that application. The proxy server is a comprehensive security tool that includes an application gateway, safe access for anonymous users, and other services. Here is some information about these different options:

- **IP Packet Filtering** — IP packet filtering was the earliest implementation of firewall technology. Packet headers are examined for source and destination addresses, Transmission Control Protocol (TCP), User Datagram Protocol (UDP) port numbers, and other information. Packet filtering is a limited technology that works best in clear security environments where, for example, everything outside the perimeter network is not allowed and everything inside is. In recent years, various vendors have improved on the packet filtering method by adding intelligent decision-making features to the packet-filtering core. Therefore creating a new form of packet filtering called *stateful protocol inspection*. You can configure packet filtering to either accept specific kinds of packets and deny all other kinds, or deny specific kinds of packets and accept all other kinds.
- **Application Gateways** — Application gateways are useful when the actual content of an application is of greatest concern. That they are application-specific is both their strength and their limitation, because they do not adapt easily to changes in technology.
- **Circuit Gateways** — Circuit gateways are tunnels built through a firewall connecting specific processes or systems on one side with specific processes or systems on the other. Circuit gateways are best employed when the person who uses an application is potentially a bigger risk than the information carried by the application. The circuit gateway differs from a packet filter in its ability to connect to an out-of-band application scheme that can add more information.

- Proxy Servers — Proxy servers are comprehensive security tools that include firewall and application gateway functionality. These tools manage Internet traffic to and from a LAN. Proxy servers also provide document caching and access control. A proxy server can improve performance by caching and directly supplying frequently requested data, such as a popular Webpage. A proxy server can also filter and discard requests that the owner does not consider appropriate, such as requests for unauthorized access to proprietary files.

Take advantage of those firewall security features that can best help your organization. Position a perimeter network in the network topography at a point where all traffic from outside the corporate network must pass through the perimeter maintained by the external firewall. You can fine-tune access control for the firewall to meet specific needs and can configure firewalls to report all attempts at unauthorized access.

To reduce the number of ports that you must open on the inner firewall, you can use an application layer firewall.

For more information about TCP/IP and other protocols, see the Windows Server 2008 R2 Core Network Guide. Or, see the Windows Server® 2012 and 2012 R2 Core Network Guide.

Network Security Scenarios

The level of network security that your organization requires will depend on several factors. It usually comes down to a compromise between budget and the need to keep the corporate data safe. A small or mid-sized company can provide a very complex security structure that will provide the highest level of network security possible. But a small company may be unable to afford that level of security. In this section, we will examine four scenarios and make recommendations in each that will provide varying levels of security at a relative cost.

No Firewall

If your organization has a connection to the Internet but no firewall, some measure of network security must be implemented. There are simple network firewall appliances, as described in the next section that may provide enough security to deter would-be malicious users.

One Simple Firewall

The minimum level of security recommended is a single firewall between the Internet and your data. This firewall may not provide any level of advanced security and is not very secure. However, it is better than no firewall.

A more secure solution will better protect your corporate data. One such solution is Forefront Threat Management Gateway (“Forefront TMG”) 2010. The increased cost of this additional server provides a good deal more security than consumer firewalls, because they typically only provide network address translation (NAT) and packet filtering. A Forefront TMG single firewall solution is more secure than an entry-level firewall appliance and provides Windows-specific security services.

One Existing Firewall

If you have an existing firewall that separates your intranet from the Internet, you may want to consider an additional firewall that provides multiple ways to configure internal resources to the Internet.

One such method is web publishing with Forefront TMG deployed in front of an organization’s web server that is providing access to Internet users. With incoming web requests, Forefront TMG can impersonate a web server to the outside world, fulfilling client requests for web content from its cache. Forefront TMG forwards requests to the web server only when the requests cannot be serviced from its cache.

Another method is server publishing. Forefront TMG allows for publishing internal servers to the Internet without compromising the security of the internal network. You can configure web publishing and server publishing rules that determine which requests should be sent to a server on the local network. This provides an increased layer of security for the internal servers.

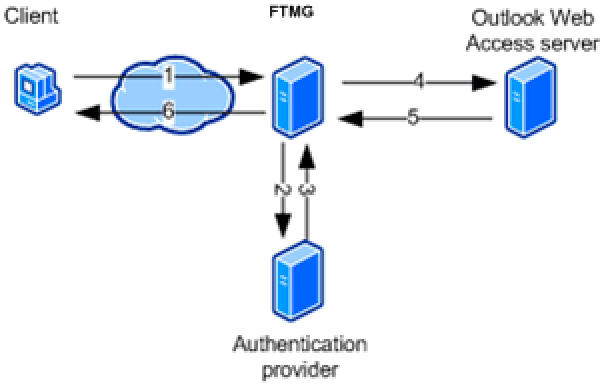

Figure 2: Existing Firewall with Forefront TMG Added

Two Existing Firewalls

The next scenario is where the organization has two firewalls with an established perimeter network. One or more of these servers is providing reverse proxy services so that Internet clients are not accessing servers on the intranet directly. Instead, one of the firewalls, ideally the internal firewall, is intercepting network requests for internal servers, inspecting those packets, and then forwarding them on behalf of the Internet host.

This scenario resembles the previous scenario after the second firewall is added. The only difference is that the internal firewall that supports reverse proxy is not running Forefront TMG. In this scenario, you should work closely with the managers of each firewall to define server publishing rules that correspond to the security policy.

Forefront Threat Management Gateway (TMG) 2010

Forefront Threat Management Gateway (TMG) 2010 is an integrated edge security gateway that helps protect IT environments from Internet-based threats while providing users fast and secure remote access to applications and data. Forefront TMG is available in two versions: standard edition and enterprise edition (view comparison).

Forefront TMG provides value to IT managers, network administrators, and information security professionals who are concerned about the security, performance, manageability, or reduced cost of network operations. Forefront TMG can help you:

- Securely Publish Content for Remote Access. Forefront TMG helps streamline the implementation providing security for corporate applications that are accessed over the Internet.
- Connect and Secure Branch Offices. Forefront TMG provides a robust way to securely expand corporate networks reducing network costs by using existing network connections.
- Defend Against External and Internal Web-Based Threats. Forefront TMG was engineered to deliver stronger security to manage and protect your networks.

Wireless Networks

By default, wireless networks are frequently configured in a manner that does not prevent eavesdropping on the wireless signals. They can be vulnerable to a malicious outsider gaining access because of the default settings on some wireless hardware, the accessibility that wireless networks offer, and encryption methods. There are configuration options and tools that can protect against eavesdropping but be aware that they do not protect the computers from malicious users and viruses that try to enter through the Internet connection. Therefore, make sure that you include a firewall to protect the computers from unwanted intruders on the Internet.

For more information about how to protect a wireless network, see “Choosing a Strategy for Wireless LAN Security.”

Note: Microsoft Dynamics SL is currently not supported in a wireless environment.

Security Update Management

Operating systems and applications are immensely complex. They can consist of millions of lines of code, written by many programmers. The software must work reliably and not compromise the security or stability of the IT environment. To minimize problems, programs should be tested thoroughly before release. However, an attacker continually strives to find weaknesses in software so that predicting all future attacks is not possible.

Whatever the nature and size of the organization, it is very important to have a good update management strategy. Most successful attacks against computer systems occur to those systems that do not have security updates installed.

Security updates present a specific challenge to most organizations. Frequently when a weakness in software is discovered, an attacker spreads information about it quickly throughout the malicious user community. When a weakness occurs in its software, Microsoft strives to release a security update as soon as possible. But until you install the update, the security that you depend on will not be optimal.

In the Microsoft Dynamics SL environment, you should have the most recent security updates applied throughout your system. Consider using the Microsoft technologies in this section:

- **Microsoft Security Notification Service –** The Security Notification Service is an email message list that distributes notices when an update becomes available. These notices serve as a valuable piece of a proactive security strategy. They are also available at the Microsoft Technical Security Notifications website.
- **Microsoft Automatic updates –** Windows can automatically apply security updates to your computers. For information about how to configure automatic updates, see “How to configure automatic updates by using Group Policy or registry settings.”
- **Microsoft Security Bulletin Search –** The security bulletin search tool is available on the Microsoft Security Bulletin search page of the TechNet website. You can determine which updates that you must have based on the operating system, applications, and service packs that you are currently running.
- **Microsoft Security Tools** – The Security TechCenter includes a page that lists various security tools.

Talk to an IT professionals about each of these tools and encourage their use. It is very important to address security issues as quickly as possible, while maintaining the stability of the environment.

Index