SECURITY

Microsoft Dynamics GP

Planning for Security in Business Portal

White Paper

Date: May, 2007

http://www.microsoft.com/dynamics/gp/default.mspx

Microsoft Dynamics™

Table of Contents

Introduction

Business Portal extends Microsoft Dynamics™ GP, providing a browser interface to securely access back office data over an intranet or an extranet. This distributed computing model brings significant security challenges, with levels of integration between clients, servers, and services. This model requires that security be an integral part of every implementation.

Much of the information in this white paper is discussed in more detail in the Business Portal product documentation, namely, the Business Portal Administrator's Guide and the Business Portal Installation Guide. These documents are supplied on the product CD.

Portal architecture

Microsoft® .NET

At the core of the portal architecture is Microsoft .NET. A general purpose development tool, .NET is ideal for creating web-based applications. It contains the building blocks for creating security-enhanced, role-based applications, using a browser client along with an existing back office solution.

Microsoft Business Framework

The Microsoft Business Framework (MBF) controls access to data from Microsoft Dynamics GP in Business Portal. The Microsoft Business Framework was built using Microsoft .NET, and provides many of the building blocks used to create business applications.

Business Portal uses the security features provided by the business framework to ensure that data remains protected and available only to those who have been granted access. These security measures have been implemented in features such as role-based security and Query Web Service. These implementations are described in depth later in this document.

Web Services for Microsoft Dynamics GP

When Business Portal is installed on Microsoft Office SharePoint® Server 2007, Web Services for Microsoft Dynamics GP also is used to control access to back office data in Business Portal.

The foundation for web services on the Microsoft Windows Server® 2003 platform is Internet Information Services (IIS). ASP .NET adds the web service capabilities. With this foundation, Web Services for Microsoft Dynamics GP provides a standard web service interface that allows external applications to access data in Microsoft Dynamics GP.

For more information, see the Web Services Installation and Administration Guide.

Windows Server 2003 and IIS

In addition to Microsoft .NET, the Microsoft Business Framework, and Web Services for Microsoft Dynamics GP, Business Portal builds on the security features in underlying components such as Windows Server 2003 and Internet Information Services (IIS). Windows Server 2003 fully integrates the .NET Framework into the operating system and allows developers and system administrators to seamlessly use both Windows Server 2003 and .NET Framework security features in their applications.

Microsoft Internet Information Services (IIS) handles authentication for Windows® SharePoint Services or Office SharePoint Server, Web Services for Microsoft Dynamics GP, and Business Portal. To be authenticated, users need a local user account or a domain user account (if in a networked domain).

Windows SharePoint Services or Office SharePoint Server

Windows SharePoint Services provides the tools for sharing information in Business Portal. You must install Business Portal on either Windows SharePoint Services or Office SharePoint Server.

SharePoint user groups provide access to sites, pages, and content in Business Portal. SharePoint permission levels define the level of control users and groups have over securable items. For more information about how security is applied in Windows SharePoint Services or Office SharePoint Server, refer to the Windows SharePoint Services 3.0 Technical Library on Microsoft TechNet: http://technet2.microsoft.com/windowsserver/WSS/en/library/.

Securing the network

In a network environment such as Business Portal, where users access data over an intranet connection, maintaining security is critical. Security becomes especially important if you deploy Business Portal in an extranet environment, where you will allow external users access to your network. You should have an in-depth understanding of all the technologies and tools involved in securing your network prior to deployment.

TCP/IP

TCP/IP must be running on the network that is used to access Business Portal. Organizations should use some type of name resolution to identify each computer, by having a server act as a domain name server, or by putting a hosts file on each client and server.

Domains

Domain controllers provide a convenient, secure way to log on to Business Portal. When users log on to a domain, Business Portal can easily retrieve and verify those credentials. Business Portal requires that the web servers, back office server, Terminal Services server, and client workstations all belong to a domain.

External connections to Business Portal

If you are allowing intranet access to remote employees, we require that you configure a VPN server to provide access and a proxy server or firewall to secure it. A VPN encrypts all the traffic that travels over the Internet between two predetermined end-points—the client's web browser and the Business Portal application server. VPNs are an ideal solution when limited access to an intranet is required.

You can also provide extranet access to Business Portal. An extranet, or perimeter network, is an extension of your company's intranet that provides secure access to authorized users who are not signed on to your corporate network. If you will have extranet users, we recommend using Microsoft Internet Security and Acceleration Server (ISA Server) to create a perimeter network. ISA Server performs many of the same functions as a firewall in determining who should have access to certain pieces of information. If your company has an existing perimeter network that doesn't use ISA Server, we recommend that you use hardware and software with similar functionality. In addition, you should set up the same communication rules and policies as recommended for ISA Server.

Securing the web server

Regardless of your organization's environment, server security should be treated with great thought and planning. A properly implemented security strategy can help to improve the availability and performance of your servers.

Windows Server 2003

Computers running Windows Server 2003 should be secured to the highest possible level, while maintaining usability for clients and access to other applications in the environment. Carefully follow the guidelines for web servers in the Windows Server 2003 Security Guide when setting up your portal environment.

Windows Server 2003 Security Guide:
http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx

SQL authentication

Business Portal uses SQL authentication to connect to your Microsoft SQL Server™ databases, so SQL Server must be using mixed-mode authentication. Mixed-mode authentication allows you to use either Windows Authentication or SQL Authentication to access the SQL Server.

When you install Business Portal, you'll create a Business Portal login ID, which is the login account Business Portal uses to access Microsoft Dynamics GP data in SQL Server. This user shouldn't be used for any other purpose, and the password should be held securely.

Business Portal and IIS

IIS provides services for web applications like Business Portal. During Business Portal installation, a virtual directory called "BusinessPortal" is created in IIS. This directory folder maps to a folder on the server's hard disk that contains the portal web pages. This redirection is a security mechanism that prohibits people from identifying the location of portal page files on the web server. We recommend using integrated Windows authentication for the Business Portal virtual directory.

To make your IIS servers as secure as possible, we recommend that you use only the services that are required to run Business Portal. The following services or subcomponents must be enabled for Business Portal:

SMTP Service If you plan to send e-mail messages from Business Portal, such as notifications for document approvals, you need to enable this subcomponent.

ASP.NET This component provides support for ASP.NET applications. It is required for both Windows SharePoint Services and Business Portal to be installed and to operate accurately.

Use the following recommendations regarding IIS to further secure the server:

- In the Machine.config and Web.config files, determine whether debugging is enabled, and also whether detailed error messages are sent to the client. Make sure that debugging is disabled on all production servers, and that a generic error message is sent to the client in the event of a problem. This avoids unnecessary information about the web server configuration being sent to the client.
- Make sure that the IIS web root is installed on a non-system NTFS partition for file system-level security. A non-system partition is one other than the partition containing the operating system files (for example, C:\Winnt).
- Make sure that the latest operating system and IIS service packs and hotfixes are applied. Check the Microsoft Security & Privacy web site (www.microsoft.com/security/default.asp) for the latest details.

Business Portal and Windows SharePoint Services or Office SharePoint Server

To protect the security of your portal application, install Windows SharePoint Services or Office SharePoint Server and Business Portal on a server that has unnecessary server computer and server site privileges disabled.

Using Secure Sockets Layer (SSL)

We recommend you use SSL to secure the Business Portal web site. If the Business Portal web site is deployed externally, you must use SSL to help protect sensitive data.

SSL secures the exchange of data between clients and servers through an encrypted data stream. IIS 6.0 has a fast and manageable SSL implementation, allowing administrators to easily use SSL certificates on all their web servers as well as take advantage of third-party cryptographic service providers.

Certificates are issued by non-Microsoft organizations called certification authorities (CAs). The server certificate is typically associated with the Business Portal web server where you plan to configure SSL. You must generate a request for a certificate, send the request to the CA, and then install the certificate to the default web directories, including Business Portal.

If administrators implement SSL after Business Portal has been installed, changes must be made to the Business Portal configuration to accommodate SSL. For more information, refer to the Business Portal Administrator's Guide.

Changing the port number

Some web applications and databases that were configured to use default port numbers have been prone to security issues. For example, a worm that searches for vulnerable database servers on the Internet might examine only TCP Port 1433. By default, SQL Server uses this port number. One way to protect Business Portal from automated attacks (such as viruses and worms) is to change the default port numbers that the application and database servers use for communications.

Securing sites, pages, and content through SharePoint

Windows SharePoint Services user groups and permission levels are used to secure sites, pages, and other content in Business Portal that does not come from Microsoft Dynamics GP.

SharePoint groups

A number of predefined SharePoint groups are created when you install Business Portal. SharePoint groups are used to provide access to sites, pages, and SharePoint content. For example, the default Sales Manager group automatically has access to pages on the Sales Center site.

Permission levels

SharePoint permission levels define the level of control users and groups have over securable items. Default SharePoint permission levels include Full Control, Design, Contribute, Read, and Limited Access.

To protect the security of your portal application, only give essential users Full Control, Design, Contribute, and BP Administration permission levels on the Business Portal site. Most Business Portal groups need only Read access to pages and other content.

Note: SharePoint permission levels do not affect data entry on Business Portal pages. For example, users with Read access to the page where requisitions are entered can still enter requisitions. The ability to enter requisitions is controlled by the user's MBF role assignments. The Read permission level applies only to modifying the page itself and any SharePoint content on the page.

The Business Data Catalog

If Business Portal is installed on Office SharePoint Server, the Business Data Catalog is available. When you install Business Portal, the Microsoft Dynamics GP web service is registered with the Business Data Catalog, allowing Microsoft Dynamics GP data to be displayed in Office SharePoint Server business data web parts.

Because the Microsoft Dynamics GP web service is used to retrieve data for the Business Data Catalog, web service security is used to secure the data displayed in these web parts.

Search

If Business Portal is installed on Office SharePoint Server, the Search feature can be used to locate Microsoft Dynamics GP data along with data stored in Windows SharePoint Services. Summary information is displayed with each Microsoft Dynamics GP search result. Selecting a result opens the detailed business data profile for that record.

Detailed information is protected by web service security; however, all users can view the summary information on the Search results page. To help make your data more secure, we recommend the following.

- If you plan to deploy Office SharePoint Server for all of your employees, but you want to allow only a certain group of employees to use Search, use SharePoint groups to secure the Search Center site.
- If you plan to deploy Office SharePoint Server for all of your employees and you want to allow all employees to use Search, set permissions on individual business entities to limit the Microsoft Dynamics GP data that can be searched by certain employees.

For more information about securing Search data, refer to the Business Portal Administrator's Guide.

Securing data through the Microsoft Business Framework

Just because two users are from the same department doesn't automatically mean they should have the same permissions. The Microsoft Business Framework (MBF) uses a security model based on user roles and data permissions, providing users with the least amount of system privileges they need to do their jobs.

For additional information about Microsoft Business Framework security, see the Business Portal Administrator's Guide.

Microsoft Business Framework roles

With MBF roles, businesses can pinpoint the types of information and processes they offer individual employees. Salespeople can review quotas and query customer data; and executives can review reports online or look up critical business information. Advanced MBF roles further tailor the information presented to employees by associating an MBF user with an ID from Microsoft Dynamics GP.

MBF roles An MBF role is used to grant a group of users access to the same data. Business Portal ships with several MBF roles that represent typical job functions, such as Sales Manager or Employee.

Advanced MBF roles A user can be assigned to an advanced MBF role to provide more granular data access. With an advanced role, a user is mapped to a back office ID, which provides the user with information that is specific only to that ID. For example, you can assign a user to the Employee advanced MBF role, which allows you to associate the user with a specific Microsoft Dynamics GP employee ID. The user can then access information such as pay stubs and available time off. The user will have access to his information, but not any other employee's information.

Data permissions

The Microsoft Business Framework uses data permissions to control the Microsoft Dynamics GP data that users can view. In order to access data through a particular data permission, the user must belong to an MBF role that has access to that data permission.

A data permission is a column-level restriction, which controls access to entity properties. Some data permissions can be refined to provide access to specific rows of data. A row-level restriction, in effect, specifies which rows from the Microsoft Dynamics GP SQL table will be displayed.

Row-level restrictions are applied to all default data permissions assigned to the Customer role. The Customer ID associated with a user determines which data is displayed.

Row-level restriction policies for the Salesperson Summary, Salesperson Period Summary, Receivables Commission, and Receivables Commission History entities are available by default, but data permissions using these restrictions are not. To make this information available, create new data permissions using the row-level restriction policies. When you use your new data permissions, the Salesperson ID associated with a user determines which data is displayed.

Only users in the MBF Administrator role can create data permissions. Typical Business Portal users can't create their own data permissions.

Query Web Service

Query Web Service (QWS) enforces security through the use of data permissions. Query Web Service is a component service of the Microsoft Business Framework. Business Portal uses the service to locate and display information from the back office in result viewer web parts and on query pages.

QWS listens for messages from Business Portal (requests for data) and passes back the requested information. Messages are sent between the Business Portal and the web service using Extensible Markup Language (XML) and using standard HTTP protocol.

Business Portal ships with a number of predefined query pages and queries that are used to perform searches and retrieve data in Business Portal. In addition, pre-built queries are also shipped for use with the various web parts.

Securing data through Web Services for Microsoft Dynamics GP

Security for the Dynamics GP web service is controlled by the Dynamics Security web service. Through this web service, the web service administrator configures which users and groups are able to execute the web methods (operations) provided by the Dynamics GP web service. If an application attempts to run a web method for which the current user doesn't have access, a security exception will be raised and the action will be prevented. Security is controlled through the Dynamics Security Administration console, which is a snap-in for Microsoft Management Console (MMC).

Securing Microsoft Dynamics GP reports displayed in Business Portal

In addition to securing real-time data, it is important to secure the Microsoft Dynamics GP reports that are displayed in Business Portal.

Report permissions on Windows SharePoint Services

If Business Portal is installed on Windows SharePoint Services only, the Reports Catalog is available. The Reports Catalog is a folder on a server that contains back office reports that can be viewed through Business Portal. A "Top 5 Reports" web part appears on each center site home page, and contains links to back office reports that are stored in the folder. Users can also access Reports pages from each center site in Business Portal.

The Reports folder is a shared folder on the network. Only users who routinely print reports to the folder should be given write access. The "Everyone" and "Anonymous User" groups should not have access to the shared reports folder. Business Portal administrators assign permissions to view reports in Reports Catalog by assigning MBF roles to the reports.

Report permissions on Office SharePoint Server

If Business Portal is installed on Office SharePoint Server, the Report Center site is available. The Report Center site serves as a central location to manage business-critical information sources, such as reports, spreadsheets, and SQL Reporting Services data connections.

When you install Business Portal, report libraries for Microsoft Dynamics GP reports are created on the Report Center site. Business Portal report libraries on the Report Center site are automatically set up to enable you to secure reports by company.

Within each report library, a folder is automatically created for each company in Microsoft Dynamics GP. For each company-specific folder in a report library, a corresponding SharePoint group is created that permits read-only access to that folder. For example, the BP Executive Reports – Fabrikam group automatically has access to the Executive Reports – Fabrikam report folder.

The Microsoft Dynamics Security Synchronization Utility

Because Business Portal users must be given access to back office data and SharePoint content separately, you may want to use the Microsoft Dynamics Security Synchronization Utility.

The Security Synchronization Utility is a Microsoft Management Console snap-in that enables you to synchronize role membership between applications with different security infrastructures and different administration experiences. The following applications can be synchronized:

- Microsoft Dynamics GP
- Web Services for Microsoft Dynamics GP
- Business Portal (MBF roles)
- Windows SharePoint Services

You can synchronize from any supported application to any other supported application. For example, you can synchronize members of an MBF role with members of a SharePoint group, or vice versa.

You must have administrative permissions to the source and destination applications in order to perform the synchronization. You can run the synchronization manually, or you can set up a Windows scheduled task to run on a regular basis.

The Security Synchronization Utility is available as a download on CustomerSource (https://mbs.microsoft.com/customersource). For more information, refer to the documentation provided with the utility.

Terminal Services

A Terminal Services server can be used in conjunction with Business Portal to provide access to Microsoft Dynamics GP windows from Business Portal. Users must have a back office user ID in order to view back office windows.

A Terminal Services connection is commonly called "thin client" access. Once Business Portal connects to Microsoft Dynamics GP, windows from Microsoft Dynamics GP can be displayed in the client browser. All system functions run on the Terminal Services server.

In order to preserve back office performance and security, Terminal Services must be implemented on a server separate from both the Business Portal and SQL servers.

For more information about deploying Terminal Services with Microsoft Dynamics GP, see Microsoft Knowledge Base article #872242.

Summary

The distributed computing model of Business Portal brings significant security challenges, with levels of integration between clients, servers, and services. This model requires that security be an integral part of every implementation. This document was designed to make you aware of actions that you can complete to help make the Microsoft Dynamics GP data displayed in Business Portal as secure as possible.

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

Microsoft