Implementing Business Portal in an Extranet Environment
**Table of contents**

Introduction ........................................................................................................... 1

What is extranet access? ......................................................................................... 1

Why deploy Business Portal in an extranet? .......................................................... 1
  Order Management .................................................................................................. 1
  Project Time and Expense .................................................................................... 2

Business Portal 3.0 Enhancements ................................................................................. 2
  Extranet Deployment ............................................................................................... 2
  Customer Data Access Policy .................................................................................. 2
  Restricted Access for External Users ...................................................................... 2
  Home Page for External Users ............................................................................... 3

Implementation ...................................................................................................... 3
  Network Topologies ............................................................................................... 3
  Optional Configurations ........................................................................................ 5
  Business Portal Installation and Setup Considerations ............................................ 5

Summary .................................................................................................................. 5
Introduction

This white paper provides information you can use in planning the deployment of Microsoft Dynamics™ GP Business Portal 3.0 in an extranet environment. In this paper, you will find information about:

- The benefits of deploying Business Portal in an extranet
- Changes made in Business Portal 3.0 to support extranet access
- Tested and supported network topologies for secure extranet access
- Implementation guidance

What is extranet access?

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.

For example, Microsoft® Outlook® Web Access (OWA) provides extranet access to corporate e-mail accounts in Microsoft Outlook. Users can access OWA from any computer connected to the Internet; they don’t have to be signed on to the corporate intranet.

Why deploy Business Portal in an extranet?

In the past, Business Portal access was limited to users on your local intranet. By adding support for extranet access, Business Portal now provides the applications and deployment support to extend Business Portal to your broader business community. This community can now include employees or business partners on your corporate intranet and those on other networks, such as customers, vendors, and offsite employees.

Using an extranet is an easy way for traveling staff, vendors, clients, and telecommuting employees to stay in touch and work from anywhere. Your company can save on travel, shipping, communications, and staffing costs simply by giving pertinent people access to your extranet. Plus, you can significantly decrease the hours your staff spends looking up information for customers and vendors by training everyone to use Business Portal.

Order Management and Project Time and Expense are Business Portal applications that can provide needed extranet functionality.

Order Management

Deploying Business Portal in an extranet enables you to provide self-service order functionality to empower your customers and salespeople.

The Business Portal Order Management application provides the ability to enter and view sales orders via a web browser. Both business partners and remote employees can access Order Management by using any computer that is Internet accessible. The end result is that your users have access to their order information at any time, from anywhere. Rather than calling your staff after hours...
with questions, extranet users can review their information through Business Portal. In addition, traveling salespeople can use any Internet connection to access the customer and order information necessary to support their accounts.

**Project Time and Expense**

The Business Portal Project Time and Expense application allows employees to enter and approve timesheets and expense reports via a web browser.

Typical Project Time and Expense users are consultants on the go. They often work away from the corporate office, and can’t always connect to the corporate intranet. In order to keep project information up-to-date, these users often need to enter their time and expense information from a hotel room or a customer’s office. Deploying Project Time and Expense in an extranet provides that flexibility and convenience by allowing access from any computer connected to the Internet.

**Business Portal 3.0 Enhancements**

We made a number of enhancements to Business Portal to help you deliver secure access to your employees and customers via the Internet.

**Extranet Deployment**

For Business Portal Release 3.0, we fully tested Business Portal in an extranet environment using standard perimeter network topologies. After Business Portal had been tested in each topology, we documented how to set up Business Portal in each environment.

An overview of the tested topologies is provided later in this paper. Detailed information, including network rules and policies required to run Business Portal in each topology, are included in the Business Portal Installation Guide.

**Customer Data Access Policy**

If you give your company’s customers access to Business Portal, you need a way to restrict their access to data. Each customer should have access to only their own records. To help you accomplish this, we’ve provided default data permissions with row-level restrictions for customer-related data in Business Portal.

Where data permissions limit the columns of data displayed to a user, row-level restrictions limit the rows of data. For example, a data permission could be used to allow access to the Order Number property. A row-level restriction can limit access so that users see only their own order numbers.

**Restricted Access for External Users**

Beginning with Business Portal Release 3.0, roles are classified as either internal or external. Internal roles should be assigned to employees of your company. External roles should be assigned to users outside of your organization, such as your customers and vendors. Users in both types of roles can access Business Portal through an extranet. However, users in external roles have access to only a Home page by default; you control what else is made available to them.
Home Page for External Users

A separate Home page is provided for external users. You can use this page to provide news, announcements, and links geared toward your customers.

The home page is an ideal place to communicate with your customers and include a marketing message that is geared specifically for them. It’s also a great way to reinforce your company’s existing branding efforts.

Implementation

There are many different ways to design and build an extranet network topology. A discussion about all of the factors involved is outside the scope of this paper. However, this paper will discuss two network topologies that Business Portal was tested in: the tri-homed perimeter network and the back-to-back perimeter network.

Both scenarios have benefits; you must choose the approach that will work best for your company. Read more below about other important deployment factors to consider.

Network Topologies

A perimeter network separates a trusted network (the intranet) from a network that is not trusted (the Internet). Perimeter networks are typically, but not always, physical networks.

All of the configurations in this paper use Microsoft Internet Security and Acceleration Server (ISA Server) 2004 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. For more information about ISA Server 2004, refer to the ISA Server home page on Microsoft’s web site.
**Tri-homed perimeter network**

In this scenario, a single ISA Server computer is used to control communication between your intranet and the Internet. This configuration also is known as a single-screened subnet. The following illustration shows a tri-homed perimeter network configuration:

![Tri-homed perimeter network diagram](image)

The primary risk with a single ISA server configuration is that it constitutes a single point of failure. If the ISA server is compromised, an intruder could gain access to your intranet.

**Back-to-back perimeter network**

In this scenario, back-to-back ISA Server computers are used to control communication between your intranet and the Internet. This configuration is also known as a dual-screened subnet. The following illustration shows a back-to-back perimeter network configuration:

![Back-to-back perimeter network diagram](image)

This scenario is typically considered more secure than the single ISA server scenario. If the external ISA server were compromised, the internal ISA server...
would still help protect your intranet. However, a higher cost is associated with this scenario because additional servers are needed. There is also additional setup complexity.

Optional Configurations
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.

Business Portal Installation and Setup Considerations
The Business Portal installation is the same whether you’re installing in a perimeter network or in your intranet. However, there are security considerations to keep in mind when you implement Business Portal in an extranet environment. Use the following guidelines to help provide secure access to Business Portal.

Secure Sockets Layer (SSL)
To help protect your data, you must use Secure Sockets Layer (SSL) for your Business Portal web site if it is deployed externally.

Setting up domain accounts for external users
All Business Portal users—both internal and external—must have valid Windows® domain accounts; Business Portal does not support anonymous users.
Use caution when assigning external users to domain accounts or groups. Access rights associated with the account or group apply to all users, internal or external, that are assigned to the account or group. Give external users the least amount of access that is necessary.

Assigning roles to external users
External roles should be assigned to users outside of your organization, such as your customers and vendors.

Summary
This white paper provided information to use in planning the deployment of Microsoft Dynamics GP Business Portal in an extranet environment. In particular, it provided information about:

- The benefits of deploying Business Portal in an extranet
- Changes made in Business Portal 3.0 to support extranet access
- Tested and supported network topologies for secure extranet access
- Implementation guidance

To learn more about using the Business Portal extranet to increase efficiency and improve communications with your customers and vendors, please contact your Microsoft Dynamics GP Partner.