Configuring Security
Copyright

Copyright © 2007 Business Objects. All rights reserved. Business Objects owns the following U.S. patents, which may cover products that are offered and licensed by Business Objects: 5,555,403; 6,247,008; 6,289,352; 6,490,593; 6,578,027; 6,768,986; 6,772,409; 6,831,668; 6,882,998; 7,139,766; 7,181,435; 7,181,440 and 7,194,465. Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Xcelsius, Crystal Decisions, Intelligent Question, Desktop Intelligence, Crystal Enterprise, Crystal Analysis, Web Intelligence, RapidMarts, and BusinessQuery are trademarks or registered trademarks of Business Objects in the United States and/or other countries. All other names mentioned herein may be trademarks of their respective owners.

Third-party contributors

Business Objects products in this release may contain redistributions of software licensed from third-party contributors. Some of these individual components may also be available under alternative licenses. A partial listing of third-party contributors that have requested or permitted acknowledgments, as well as required notices, can be found at: http://www.businessobjects.com/thirdparty
# Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1</td>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Conventions used in this guide</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>About BusinessObjects Planning</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Related documentation</td>
<td>8</td>
</tr>
<tr>
<td>Chapter 2</td>
<td>About Security</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Integrated Windows authentication</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Non-Windows authentication</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>About BusinessObjects Planning security components</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>BusinessObjects Planning Login Server</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>BusinessObjects Planning Security Configuration tool</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>BusinessObjects Planning ISAPI filter</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>Authorization</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>Object-level security</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Database security</td>
<td>18</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>Configuring Shared Folder Access</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Shared folder access</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>Configuring basic access</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>Overriding the bootstrap account</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Configuring group access</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Basic file-level permissions</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Extended file-level permissions</td>
<td>24</td>
</tr>
<tr>
<td>Chapter 4</td>
<td>Configuring Windows Server 2003</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>Configuring the Application Server environment</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>Assigning user rights for service logon</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>Configuring the Application Server service logon</td>
<td>31</td>
</tr>
</tbody>
</table>
Contents

<table>
<thead>
<tr>
<th>Chapter 7</th>
<th>Installing and Configuring the BusinessObjects Planning ISAPI Filter 87</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Installing the BusinessObjects Planning ISAPI filter .......................... 89</td>
</tr>
<tr>
<td></td>
<td>Configuring the BusinessObjects Planning ISAPI filter ............................ 89</td>
</tr>
<tr>
<td></td>
<td>Configuring the BusinessObjects Planning ISAPI extension ........................ 91</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 8</th>
<th>Configuring Security-Related INI Settings 93</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configuring INI settings .................................. 95</td>
</tr>
</tbody>
</table>

Index 97
Introduction
This guide contains information about configuring security for your BusinessObjects Planning site. This guide is intended for administrators who are configuring authentication and other security policies for their BusinessObjects Planning site.

This section discusses the following topics:

• “Conventions used in this guide” on page 7
• “About BusinessObjects Planning” on page 7
• “Related documentation” on page 8
Conventions used in this guide

The following table describes the conventions used in this guide.

<table>
<thead>
<tr>
<th>When you see...</th>
<th>It indicates...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold text</strong></td>
<td>A name of a user interface item that you should select. For example, “Right-click a report and select Properties.”</td>
</tr>
<tr>
<td><strong>Courier text</strong></td>
<td>Information you need to type into a data entry field. For example, when you see “Type AuthorizationServers”, you should type each individual letter key to make up the word AuthorizationServers.</td>
</tr>
<tr>
<td><strong>BOLD SMALL CAPS</strong></td>
<td>Specific keys you need to press. For example, when you see “Press ENTER”, you should press the ENTER key on your keyboard.</td>
</tr>
</tbody>
</table>

About BusinessObjects Planning

The BusinessObjects Planning product suite provides Web-enabled, vertical industry-targeted enterprise analytics software that helps companies measure, analyze, and predict business performance and profitability. Organizations leverage the suite for real-time business planning and forecasting, accelerating mergers and acquisitions, understanding business performance by customer segment, product, channel and business line, and delivering performance management information across the enterprise.

BusinessObjects Planning is the only suite that is selectively packaged into a series of applications, each one tailored to support a different segment of the user community. Moreover, every user leverages a common information infrastructure. All user applications are driven by the same set of data, business rules, user rights, and report templates, and any changes are automatically synchronized across the enterprise.

The product suite includes the following applications:

**BusinessObjects Planning Administrator**

BusinessObjects Planning Administrator allows nontechnical users to rapidly and easily configure, deploy, and administer BusinessObjects Planning applications across multiple sites. From a central site—and leveraging intuitive graphical interface, drag-and-drop function, and advanced automation capabilities—users can install and synchronize geographically dispersed sites, assign user access rights, and build and manage multiple business models.
BusinessObjects Planning Analyst Pro
BusinessObjects Planning Analyst Pro is designed for nontechnical users who have sophisticated information requirements. A comprehensive range of formatting features, and drag-and-drop functions allow users to easily create and maintain reports. In addition, users can quickly build, manage, and execute scripts that automate complex tasks such as scheduled report production and distribution.

BusinessObjects Planning Analyst
BusinessObjects Planning Analyst provides secure remote access to real-time report information anywhere, anytime, through a Web browser. Intelligent graphic indicators, drill-down toolbars, built-in annotation capabilities, forecasting tools, and a sophisticated charting interface allow users to easily view, enter, and edit report data.

BusinessObjects Planning Excel Analyst
The BusinessObjects Planning Excel Analyst allows users to leverage advanced analytics, superior performance, and automated information synchronization and distribution capabilities, all from within a familiar Microsoft® Excel environment.

Related documentation
For information about installing and using BusinessObjects Planning, please refer to the following documentation:

Installing BusinessObjects Planning Sites
This guide describes how to install a BusinessObjects Planning site that uses either a Microsoft SQL Server or Oracle® database.

Installing BusinessObjects Planning Server Components
This guide describes how to install the BusinessObjects Planning Server components to allow Internet-based use of BusinessObjects Planning. It provides installation and configuration instructions for the BusinessObjects Planning Analyst site, the BusinessObjects Planning Gateway, BusinessObjects Planning Server, and BusinessObjects Planning Scheduler.

Installing BusinessObjects Planning Workstation Applications
This guide describes how to install and configure BusinessObjects Planning Administrator, BusinessObjects Planning Analyst Pro, and BusinessObjects Planning Excel Analyst on user workstations.
**BusinessObjects Planning Server Components Administration Guide**

This guide, designed for administrators, describes how to configure and manage BusinessObjects Planning Servers and BusinessObjects Planning Gateways. It provides information about: using the BusinessObjects Planning Site Monitor tool to manage the BusinessObjects Planning enterprise, the Planning.ini configuration file, load balancing, and other configurable properties.

**Customizing BusinessObjects Planning Installations**

This guide describes how to modify configurable properties in BusinessObjects Planning configuration files or executables to create customized installations.

**Using the BusinessObjects Planning Configuration Assistant**

This guide describes how to use the BusinessObjects Planning Configuration Assistant to configure client applications, create or modify connections to BusinessObjects Planning sites, or create configuration reports to aid in troubleshooting.

**Administrator’s Guide**

This guide describes how to configure, customize, and maintain BusinessObjects Planning applications on behalf of other users. This guide includes conceptual and background information on the features and functions of the applications. It also gives examples of how to use BusinessObjects Planning Administrator and BusinessObjects Planning Analyst Pro.

**BusinessObjects Planning Reporting Guide**

This guide describes how to create, use, and format reports using BusinessObjects Planning Administrator and BusinessObjects Planning Analyst Pro. This guide explains reporting-related concepts and provides step-by-step instructions.

**BusinessObjects Planning Analyst User guide**

This guide describes how to use BusinessObjects Planning Analyst to access, view, and analyze BusinessObjects Planning reports in a World Wide Web environment.

**BusinessObjects Planning Excel Analyst User Guide**

This guide serves two purposes. It describes how to use the BusinessObjects Planning Excel Analyst to access, view, and analyze BusinessObjects Planning reports in an Excel environment. It also describes how to use the BusinessObjects Planning Excel Analyst to create ad hoc reports that query
business rules and data in your BusinessObjects Planning environment. This guide explains reporting-related concepts and provides step-by-step instructions.

**BusinessObjects Planning Workflow Guide**

This guide is intended for BusinessObjects Planning users who deal with their organization's Workflow plans and who are responsible for administering, submitting, and approving Workflow scenarios. It contains conceptual and background information on the elements of Workflow in BusinessObjects Planning and gives examples of how to apply Workflow to an organization's planning and forecasting process. As Workflow functions are not specific to one application in BusinessObjects Planning, this guide includes Workflow-related information for BusinessObjects Planning Administrator, BusinessObjects Planning Analyst Pro, BusinessObjects Planning Analyst, and Workflow Console.

**Configuring Security Guide**

This guide, designed for administrators, describes how to configure and manage authentication and security for a BusinessObjects Planning site.

**Online help**

The online help provides step-by-step instructions for using BusinessObjects Planning applications. The online help also provides reference and conceptual information. To access online help in BusinessObjects Planning Administrator or BusinessObjects Planning Analyst Pro, select Help from the Help menu on the Organizer toolbar, or press **F1**. To access online help in BusinessObjects Planning Analyst, BusinessObjects Planning Excel Analyst, or Workflow Console, click the Help button on the application toolbar.
About Security
This chapter provides information about security within BusinessObjects Planning, and covers the following areas:

- “Authentication” on page 13
- “About BusinessObjects Planning security components” on page 14
- “Authorization” on page 16
- “Object-level security” on page 17
- “Database security” on page 18
Authentication

Authentication is the key to the perimeter of any system. It asks the question: “Are you who you say you are?” BusinessObjects Planning does not maintain a separate set of passwords, since your enterprise already has a strong, well-understood, and well-resourced catalog of users and passwords, with a carefully thought-out set of policies. Instead, BusinessObjects Planning integrates with it, ensuring consistency of user IDs, password policies, and password strengths. BusinessObjects Planning supports both integrated Windows® authentication and non-Windows authentication, and supplies a utility to configure the authentication mechanisms for your site.

Integrated Windows authentication

For enterprises using Microsoft Active Directory®, BusinessObjects Planning applications can take advantage of the single sign-on Windows features and obtain the user’s credentials directly from the operating system. BusinessObjects Planning never needs to handle the password. This applies to the desktop applications as well as Internet Explorer-based clients.

Non-Windows authentication

For enterprises that do not have Windows security and user management throughout their organization, BusinessObjects Planning supports plug-in authentication mechanisms. BusinessObjects Planning applications prompt users for credentials, and route them to an enterprise authentication server for validation. BusinessObjects Planning supports the following non-Windows authentication methods:

• Novell®
• LDAP
• Third-party ISAPI authentication filters (for example, DAF, AuthentiX)
• Custom ISAPI filters (documentation, sample code, and assistance are available from BusinessObjects Planning Consulting)
About BusinessObjects Planning security components

BusinessObjects Planning security components allow you to configure security on your site, as well as to set up non-Windows authentication sources. BusinessObjects Planning provides the following security components:

- BusinessObjects Planning Login Server
- BusinessObjects Planning Security Configuration tool
- BusinessObjects Planning ISAPI filter

**BusinessObjects Planning Login Server**

The BusinessObjects Planning Login Server is a Windows NT® service that handles user authentication against a variety of authentication sources. The BusinessObjects Planning Login Server can communicate with the following authentication sources:

- Windows domain authentication
- Novell NDS® trees
- HTTP server authentication

For more information on the BusinessObjects Planning Login Server, see "Installing and Configuring BusinessObjects Planning Login Server" on page 57.

**Note:** If you are only using Windows domain authentication for your site, you do not need to install a BusinessObjects Planning Login Server.

**BusinessObjects Planning Security Configuration tool**

The BusinessObjects Planning Security Configuration tool allows you to configure multiple aspects of security for your BusinessObjects Planning site. The tool allows you to perform the following actions:

- Edit the database access parameters—This feature allows you to modify the Planning.ini file to point to a new database if the BusinessObjects Planning site’s database has changed.
- Configure the shared folder access account—By default, BusinessObjects Planning uses Windows authentication to authenticate its users. However, there may be some BusinessObjects Planning users...
who are not working from a Windows domain. This feature lets you specify a dedicated Windows domain account for all unauthenticated users to use.

- Configure login account types—By default, BusinessObjects Planning uses Windows authentication. This feature allows you to use other forms of authentication to authenticate your users.
- Configure login confirmation—This feature allows you to specify whether users must always enter their username and password when trying to gain access to BusinessObjects Planning.
- Configure user auto-creation—This feature allows you to specify whether user IDs are automatically created in BusinessObjects Planning upon successful login.
- Configure external authentication servers—This feature allows you to specify which BusinessObjects Planning Login Servers are used to authenticate user logins.

For more information on the BusinessObjects Planning Security Configuration tool, see “Using the Security Configuration Tool” on page 67.

**BusinessObjects Planning ISAPI filter**

The BusinessObjects Planning ISAPI filter is a configurable filter that can be installed on your BusinessObjects Planning web site to handle user authentication against a variety of authentication sources. The BusinessObjects Planning ISAPI filter can communicate with the following authentication sources:

- Windows domain authentication
- Novell NDS trees
- LDAP repositories

For more information on the BusinessObjects Planning ISAPI filter, see “Installing and Configuring the BusinessObjects Planning ISAPI Filter” on page 87.

**Note:** If you are only using Windows domain authentication for your site, you do not need to install a BusinessObjects Planning Login Server.

The following diagram displays a sample site that uses both BusinessObjects Planning Login Server and BusinessObjects Planning ISAPI filter with LDAP authentication to authenticate its users. For web clients, the login request is sent from the BusinessObjects Planning ISAPI filter to the LDAP repository. If the login is successful, the request then proceeds to the BusinessObjects Planning Application Server and ultimately to the BusinessObjects Planning...
Authorization asks the question: “What are you allowed to see or do?” All BusinessObjects Planning objects and high-level operations are subject to authorization controls that limit which users may view, execute, modify, annotate, create, or delete objects.

To simplify administration, privileges may be granted to object hierarchies that are inherited by all members of the hierarchies. Also, administrators may define user groups and grant privileges to groups rather than to individual users.

BusinessObjects Planning supports controls to the granting of privileges. Users may only grant privileges that they have, and have been entitled to grant.
User impersonation is also supported. Users who are entitled to grant impersonation rights may allow other users to impersonate them. During impersonation, the user has the same access rights as the user being impersonated, but the audit trail shows both the real user and the user being impersonated.

When a BusinessObjects Planning site is installed, the login domain and name of the Core user must be supplied. This user has full privileges to the BusinessObjects Planning site. The site installation also defines the system user group, Site Administrators, with a single member, the Core user. Site Administrators and the Core user have virtually the same, universal access. Site Administrators have less control only on areas concerning remote sites. Beyond these two system-defined roles, BusinessObjects Planning roles are fully user-defined. The Core user grants selective privileges and delegation privileges to other users or user groups.

The Core user login may be disabled after the initial configuration and delegation. Impersonation privileges for the Core user may be selectively granted if desired.

BusinessObjects Planning supports user-defined groups of users and nested groups. There are also system-defined groups such as Everyone, Users at Site <x>, and groups built for specific functions, such as report creators. These groups may also be included in user-defined groups. A user can be part of multiple groups as required.

For information on creating groups, refer to the Administrator’s Guide.

Object-level security

Security rights are assigned by granting access rights to view and to modify data for certain business model components. Assigning user rights to scenarios makes it very easy and flexible to control the data a user can view and/or modify. For example, a user can be granted rights to view only the scenarios that contain official actuals for a given year while granting other users rights to view and modify scenarios that contain versions of the business plan.

Access to reports can be assigned on an individual basis or to a group of reports, by granting rights on reporting folders. If rights are assigned on a folder, all reports in that folder inherit the same rights.

Within BusinessObjects Planning security, the following objects can be administered with the following rights:

- Data Sets (such as, Plan but not Actuals, read/write, consolidate, and so forth)
About Security

Database security

- Reports (control, modify, run)
- Business Models (view, control, modify)
- Scripts (control, modify, run)
- Spreadsheets (control, modify)
- Rates (modify, view)
- Business Unit Dimensions (view, control, modify)

For information on assigning object-level rights, refer to the Administrator’s Guide.

Database security

BusinessObjects Planning users never need to know the database password to use the application. When a BusinessObjects Planning site is installed, the database administrator must provide the name and password of a user who owns the site’s database. This database user ID can already exist, or it can be created by the installation program. Once created, this database user ID is used by all BusinessObjects Planning applications to gain access to the database. The user’s name and encrypted password are stored in the shared Planning.ini file for all applications to retrieve, but because the password is encrypted in the file, it is not readable by your users.
Configuring Shared Folder Access
This chapter provides information about the BusinessObjects Planning shared folder and the possible types of access that can be granted to it. Specifically, this chapter provides information about:

- “Shared folder access” on page 21
- “Configuring basic access” on page 21
- “Configuring group access” on page 22
Shared folder access

The BusinessObjects Planning shared folder contains shared configuration files and files for BusinessObjects Planning objects such as business models, scripts, reports, and templates. All BusinessObjects Planning applications, beyond a few specialized Windows services and thin clients, require access to the BusinessObjects Planning shared folder at a site. BusinessObjects Planning allows for two models of shared folder authorization:

- Basic—Used for those sites where non-Windows authentication is in use.
- Group—Used for those sites where an administrator wants to specify individually which Windows users and user groups are allowed to see the contents of the shared folder and the shared Planning.ini file.

The mode of access that you choose for your site is dependent on the security policies within your organization.

The order in which BusinessObjects Planning authenticates users is as follows:

1. BusinessObjects Planning attempts to gain access to the config and public folders of the BusinessObjects Planning shared folder using the user’s account.
   
   If the user has valid credentials for any of the configured authentication types, BusinessObjects Planning validates the user. See “Configuring login account types” on page 75 for more information.

2. For those users who don’t have valid credentials, BusinessObjects Planning uses the shared account option to access the share.

Configuring basic access

Basic access is a simple way to limit access to the BusinessObjects Planning shared folder. In basic access, all BusinessObjects Planning applications use the same shared folder account to gain access to the site. When a request comes in from a BusinessObjects Planning application, the application attempts to read the shared folder using the credentials of the user. When this fails, the application defaults to the bootstrap account. This account reads the Planning.ini file to get the SharedDirectory account and password. Once the SharedDirectory account is known, this account is then used to view the contents of the BusinessObjects Planning shared folder.

Configuring basic access requires the following steps:

1. Remove all user and group rights from the BusinessObjects Planning shared folder.
2. Create an account on the shared folder machine. This account is used as the dedicated account by all BusinessObjects Planning applications when gaining access to the shared folder.

3. Grant view and modify rights to the shared folder for the shared account.

4. Create the bootstrap account on the shared folder machine. This account is a default account for initial shared file access. (Contact your BusinessObjects Planning Consultant for information about the default username and password for this account.)

5. Grant read access on the Planning.ini file to the bootstrap account.

6. Use the BusinessObjects Planning Security Configuration tool to configure the protected access to the shared folder and to set up the shared account. For information on how to do this, see “Configuring BusinessObjects Planning shared folder access” on page 74.

Overriding the bootstrap account

BusinessObjects Planning provides an option for a local override on the bootstrap account. This override may be either in the form of environment variables (which take precedence), or as a set of registry entries. The registry entries must appear in the same location as the existing BusinessObjects Planning settings.

Registry Settings:

BootstrapAccount="[domain name]\account name"
BootstrapPassword="<encrypted password>" - encrypted using standard BusinessObjects Planning encryption

Environment variables:

CTP_BootstrapAccount
CTP_BootstrapPassword

Warning: If you choose to override the bootstrap account, then all BusinessObjects Planning applications must have registry settings or environment variables that set the bootstrap account, otherwise the applications cannot open the Planning.ini file and connect to the site.

Configuring group access

Group access is a more detailed way to control access to the BusinessObjects Planning shared folder. With group access, an administrator defines user groups and assigns folder-level permissions to these user groups. This ensures that only those users who are assigned to the correct group have access to the shared folder.
Configuring group access to the BusinessObjects Planning shared folder requires the following steps:

1. Define the local groups that will have rights to access the shared folder.
2. Create the local groups and add users to the groups.
3. Share the BusinessObjects Planning folder so that it is visible over the network.
4. Grant file-level permissions to the shared folder’s subfolders.

Note: You must ensure that the shared folder is properly configured so that users and user groups can gain access to the shared folder over the network.

Note: Before a BusinessObjects Planning application can be installed on a client machine, you as the administrator must have rights to the shared installation folder. In addition, the primary user of the client machine you are installing on must be a member of one of the configured groups.

**Basic file-level permissions**

You can define any set of groups to access the shared folder, provided the access structure is created. The standard way to allow access to the BusinessObjects Planning shared folder is to create the following groups:

- PlanningFinance—For BusinessObjects Planning application users
- PlanningAdministrators—For BusinessObjects Planning application administrators

Note: The groups listed above are examples that show how to use basic file-level permissions for your organization. The actual groups and folder rights you use depend on the needs of your organization.

In this basic group environment, the following access rights should be granted:

<table>
<thead>
<tr>
<th>Shared Folder file or subfolder</th>
<th>Group Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PlanningFinance</td>
</tr>
<tr>
<td>&lt;root&gt;\a</td>
<td>Read, Write</td>
</tr>
<tr>
<td>\Config</td>
<td>Read</td>
</tr>
<tr>
<td>\Install&gt;</td>
<td>Read</td>
</tr>
<tr>
<td>Public</td>
<td>Write permissions for all users on all subfolders, since they contain publicly accessible objects such as business models, scripts, and reports</td>
</tr>
</tbody>
</table>

---

**Note:**

The groups listed above are examples that show how to use basic file-level permissions for your organization. The actual groups and folder rights you use depend on the needs of your organization.
Configuring Shared Folder Access

Configuring group access

a. All users need read and write access to the root of the shared folder in order to write to any log files in this folder.

Note: <root> is the root level of the BusinessObjects Planning site’s shared folder.

Note: <install> is the path to the folder that contains installation files for BusinessObjects Planning applications. It is recommended that you create this folder and copy the BusinessObjects Planning installation files from the CD to this central location.

Extended file-level permissions

You may prefer to apply more exclusive permissions to your shared folder and its subfolders. Instead of creating just the PlanningFinance and PlanningAdministrators groups, you could create four groups:

• PlanningFinance—Application users who only view information
• PlanningAnalysts—Analysts who create reports
• PlanningModellers—Model writers who create models or write scripts
• PlanningAdministrators—Administrators

Note: The groups listed above are examples that show how to use extended file-level permissions for your organization. The actual groups and folder rights you use depend on the needs of your organization.

In this extended group environment, the following access rights should be granted:

<table>
<thead>
<tr>
<th>Shared Folder file or subfolder</th>
<th>Planning Finance</th>
<th>Planning Analysts</th>
<th>Planning Modellers</th>
<th>Planning Administrators</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;root&gt;a</td>
<td>Read, Write</td>
<td>Read, Write</td>
<td>Read, Write</td>
<td>Read, Write</td>
</tr>
<tr>
<td>Logs</td>
<td>Read, Write</td>
<td>Read, Write</td>
<td>Read, Write</td>
<td>Read, Write</td>
</tr>
<tr>
<td>Config</td>
<td>Read</td>
<td>Read</td>
<td>Read</td>
<td>Read, Write</td>
</tr>
<tr>
<td>&lt;Install&gt;</td>
<td>Read</td>
<td>Read</td>
<td>Read</td>
<td>Read, Write</td>
</tr>
<tr>
<td>\Public\Reports</td>
<td>Read</td>
<td>Read, Write</td>
<td>Read, Write</td>
<td>Read, Write</td>
</tr>
<tr>
<td>\Public\Favorites</td>
<td>Read</td>
<td>Read, Write</td>
<td>Read, Write</td>
<td>Read, Write</td>
</tr>
<tr>
<td>\Public\Model</td>
<td>Read</td>
<td>Read, Write</td>
<td>Read, Write</td>
<td>Read, Write</td>
</tr>
<tr>
<td>\Public\Scripts</td>
<td>Read</td>
<td>Read, Write</td>
<td>Read, Write</td>
<td>Read, Write</td>
</tr>
</tbody>
</table>

a. All users need read and write access to the root of the shared folder in order to write to any log files in this folder.
Note: `<root>` is the root level of the BusinessObjects Planning site’s shared folder.

Note: `<install>` is the path to the folder that contains installation files for BusinessObjects Planning applications. It is recommended that you create this folder and copy the BusinessObjects Planning installation files from the CD to this central location.
Configuring Shared Folder Access
Configuring group access
Configuring Windows Server 2003

You should perform the configuration tasks outlined in this chapter after completing the installation of the server components. If you have installed different server components on separate machines, each machine must possess the proper security settings. For more information on installing BusinessObjects Planning server components, see the Installing Server Components guide.

This section provides information on the following topics:

• “Configuring the Application Server environment” on page 28
• “Configuring the Web Server environment” on page 36

Configuring the Application Server environment

If you installed the BusinessObjects Planning Application Server on the Windows Sever 2003 platform, you should perform the following configuration tasks on the machine that is hosting the Application Server:

• “Assigning user rights for service logon” on page 28
• “Configuring the Application Server service logon” on page 31
• “Configuring Distributed COM” on page 32

Assigning user rights for service logon

The BusinessObjects Planning Application Server runs as a Windows service. You must ensure that the user account under which the Application Server service will run is a registered BusinessObjects Planning user account and has the appropriate rights to register Windows services.

To assign user rights for service logon:

1. Click the Start button and select Run from the menu.
2. In the Run dialog box, type secpol.msc and click OK.
3. In the left pane of the Local Security Settings manager, expand the Local Policies folder and select User Rights Assignment.
4. In the right pane, double-click the **Log on as a service** policy.

<table>
<thead>
<tr>
<th>Local Security Settings</th>
<th>Policy Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log on as a service</td>
<td>NETWORK SERVICE, ASP.NET, IIS_ADMIN, IIS_APPPOOL_ADMIN</td>
</tr>
<tr>
<td>Log on as a service</td>
<td>NETWORK SERVICE, ASP.NET, IIS_ADMIN, IIS_APPPOOL_ADMIN</td>
</tr>
<tr>
<td>Log on as a service</td>
<td>NETWORK SERVICE, ASP.NET, IIS_ADMIN, IIS_APPPOOL_ADMIN</td>
</tr>
<tr>
<td>Log on as a service</td>
<td>NETWORK SERVICE, ASP.NET, IIS_ADMIN, IIS_APPPOOL_ADMIN</td>
</tr>
<tr>
<td>Log on as a service</td>
<td>NETWORK SERVICE, ASP.NET, IIS_ADMIN, IIS_APPPOOL_ADMIN</td>
</tr>
<tr>
<td>Log on as a service</td>
<td>NETWORK SERVICE, ASP.NET, IIS_ADMIN, IIS_APPPOOL_ADMIN</td>
</tr>
<tr>
<td>Log on as a service</td>
<td>NETWORK SERVICE, ASP.NET, IIS_ADMIN, IIS_APPPOOL_ADMIN</td>
</tr>
</tbody>
</table>

5. On the Local Security Setting page, ensure that the user account under which the Application Server service will run appears in the display box. If this user account appears, go directly to step 9. If it does not, continue to step 6.
4 Configuring Windows Server 2003
Configuring the Application Server environment

Note: The user account under which the Application Server service will run must be a registered BusinessObjects Planning user account.

6. Click **Add User or Group**.
7. In the Enter the object names to select text box, type the user account under which the Application Server service will run. (You can click **Check Names** to validate the account information that you have entered.)

8. Click **OK**.
9. In the Log on as a service Properties dialog box, click **OK**.
Configuring the Application Server service logon

When the BusinessObjects Planning Application Server service is started, it logs on to a registered BusinessObjects Planning user account to access all the necessary resources and objects on the operating system. You must ensure that the service logs on using the proper user account. This user account is the same account that you identified in "Assigning user rights for service logon" on page 28.

- To configure the Application Server service logon:
  1. From the Windows Administrative Tools menu, select Services.
  2. In the Services manager, right-click BusinessObjects Planning Server and select Properties from the menu.
  3. In the BusinessObjects Planning Server Properties (Local Computer) dialog box, select the Log On tab.
  4. On the Log On page, select the This account option and enter the logon information of the user account under which the Application Server service will run.
Note: The user account under which the Application Server service will run must be a registered BusinessObjects Planning user account.

5. Click OK.

Configuring Distributed COM

You must customize the security settings for Distributed COM so that the BusinessObjects Planning Application Server can properly communicate with the BusinessObjects Planning Gateway.

To configure Distributed COM:
1. From the Windows Administrative Tools menu, select Component Services.
2. In the left pane of the Component Services manager, expand Component Services and Computers.
3. Right-click **My Computer** and select **Properties** from the menu.

4. In the My Computer Properties dialog box, select the **Default Properties** tab.
5. Ensure that the Enable Distributed COM on this computer check box is selected.

6. Ensure that the Default Authentication Level is set to Connect.
   
   **Note:** If you installed the BusinessObjects Planning Application Server and the BusinessObjects Planning Web server components on a single machine, you should set the Default Authentication Level to None.

7. Ensure that the Default Impersonation Level is set to Identify.

8. Select the COM Security tab.


10. In the Access Permission dialog box, click Add.

11. In the Enter the object names to select text box, type Anonymous Logon. (You can click Check Names to validate the account information that you have entered.)

12. Click OK.

13. Under Permissions for ANONYMOUS LOGON, grant the following rights:
   
   - Allow Local Access
14. Repeat steps 10 to 13 for the following objects:
   • The Everyone group
   • The user account under which the CtpWebGate DCOM object will run (for more information about the CtpWebGate DCOM object, see “Configuring the BusinessObjects Planning Gateway” on page 43).

15. Click OK.
17. In the Launch Permission dialog box, click Add.
18. In the Enter the object names to select text box, type Everyone. (You can click Check Names to validate the account information that you have entered.)
19. Click OK.
20. Under Permissions for Everyone, grant the following rights:
   • Allow Local Launch
   • Allow Remote Launch
   • Allow Local Activation
21. Repeat steps 17 to 20 for the following objects:
   • The machine’s Administrators group
   • The user account under which the CtpWebGate DCOM object will run (for more information about the CtpWebGate DCOM object, see “Configuring the BusinessObjects Planning Gateway” on page 43).

22. In the Launch Permission dialog box, click OK.

23. In the My Computer Properties dialog box, click OK.

Configuring the Web Server environment

If you installed the BusinessObjects Planning Gateway or BusinessObjects Planning Web site on the Windows Server 2003 platform, you should perform the following configuration tasks on the machine(s) hosting these server components:

• “Configuring Distributed COM” on page 37
• “Configuring the BusinessObjects Planning Analyst IIS COM+ application” on page 40
• “Configuring the BusinessObjects Planning Gateway” on page 43
• “Configuring DCOM machine launch restrictions” on page 50
• “Granting necessary folder access rights” on page 52
• “Configuring Internet Information Services (IIS)” on page 54

Note: After making any configuration changes to the BusinessObjects Planning Web site or BusinessObjects Planning Gateway, you should restart IIS.

Configuring Distributed COM

You must customize the security settings for Distributed COM on the machine acting as the Web Server so it can properly communicate with the BusinessObjects Planning Application Server.

To configure Distributed COM:

1. From the Windows Administrative Tools menu, select Component Services.
2. In the left pane of the Component Services manager, expand Component Services and Computers.
3. Right-click My Computer and select Properties from the menu.
4. In the My Computer Properties dialog box, select the **Default Properties** tab.

5. Ensure that the **Enable Distributed COM on this computer** check box is selected.

6. Ensure that the Default Authentication Level is set to **None**.

7. Ensure that the Default Impersonation Level is set to **Identify**.

8. Select the **COM Security** tab.


10. In the Access Permission dialog box, ensure that SELF and SYSTEM are present in the Group or user names list and that they are granted the following rights:
    - Allow Local Access
11. Click **OK**.


13. In the Launch Permission dialog box, ensure that the machine's Administrators group, INTERACTIVE, and SYSTEM are present in the Group or user names list and that they are granted the following rights:
   - Allow Local Launch
   - Allow Remote Launch
   - Allow Local Activation
14. In the Launch Permission dialog box, click OK.

15. In the My Computer Properties dialog box, click OK.

### Configuring the BusinessObjects Planning Analyst IIS COM+ application

You must configure the security settings of the COM+ application that was installed for the BusinessObjects Planning Analyst site.

- **To configure the BusinessObjects Planning Analyst IIS COM+ application:**
  1. From the Windows Administrative Tools menu, select Component Services.
  2. In the left pane of the Component Services manager, expand Component Services and Computers.
  3. Expand My Computer and COM+ Applications.
4. Right-click the IIS entry for the BusinessObjects Planning Analyst site (typically IIS-\(\text{Default Web Site/Root/BusinessObjectsPlanningWeb}\)) and select Properties from the menu.

5. In the IIS Properties dialog box, select the Security tab.
6. On the Security page, ensure that the **Enforce access checks for this application** check box is cleared.

7. Ensure that the **Perform access checks only at the process level** option is selected.

8. Ensure that the Authentication Level for Calls is set to **Packet**.

9. Ensure that the Impersonation Level is set to **Impersonate**.

10. Select the **Identify** tab.
11. On the Identify page, ensure that the **This user** option is selected and that the IWAM (Internet Web Application Manager) user account information is displayed. The IWAM account must be the account under which this COM+ application will run.

![Image](https://example.com/image.png)

12. Click **OK**.

### Configuring the BusinessObjects Planning Gateway

The BusinessObjects Planning Gateway is configured through the CtpWebGate DCOM object. You must configure the CtpWebGate DCOM object of the machine on which the BusinessObjects Planning Gateway was installed.

- **To configure the BusinessObjects Planning Gateway:**
  1. From the Windows Administrative Tools menu, select **Component Services**.
  2. In the left pane of the Component Services manager, expand **Component Services** and **Computers**.
  3. Expand **My Computer** and **DCOM Config**.
4. Right-click **CtpWebGate** and select **Properties** from the menu.
5. On the General page of the CtpWebGate Properties dialog box, select **None** from the Authentication Level list.

6. Select the **Location** tab.
7. Ensure that the **Run application on this computer** check box is selected and all other check boxes are cleared.

![Image of Configuration Settings](image)

8. Select the **Security** tab.

9. Under Launch and Activation Permissions, select the **Customize** option and click **Edit**.

10. In the Launch Permission dialog box, click **Add**.

11. In the **Enter the object names to select** text box, type **Everyone**. (You can click **Check Names** to validate the account information that you have entered.)

12. Click **OK**.

13. Under Permissions for Everyone, grant the following rights:
   - Allow Local Launch
   - Allow Remote Launch
   - Allow Local Activation
14. Click OK.
15. Under Access Permissions, select the Customize option and click Edit.
16. In the Access Permission dialog box, ensure that SELF and SYSTEM are present in the Group or user names list and that they are granted the following rights:
   • Allow Local Access
• Allow Remote Access

17. Click **OK**.

18. Under Configuration Permissions, select the **Customize** option and click **Edit**.

19. In the Change Configuration Permission dialog box, ensure that the machine’s Administrators group, Power Users group, and Users group, as well as CREATOR OWNER and SYSTEM, are present in the Group or user names list and that they are granted the following rights:

- Allow Full Control
- Allow Read
20. Click **OK**.

21. Select the **Identify** tab.
22. On the Identify page, select the **This user** option and enter the account information of the user under which the BusinessObjects Planning Gateway will run. This user account is the same account that you identified in “Configuring Distributed COM” on page 32.

![Identify page screenshot](image)

23. Click **OK**.

**Configuring DCOM machine launch restrictions**

To allow for successful authentication between machines with different domains, you must change the DCOM launch permissions on the machine(s) hosting the BusinessObjects Planning Gateway and BusinessObjects Planning Web site to include the ANONYMOUS LOGIN object.

1. To configure DCOM machine launch restrictions:

   1. Click the **Start** button and select **Run** from the menu.
   2. In the Run dialog box, type `secpol.msc` and click **OK**.
   3. In the left pane of the Local Security Settings manager, expand the **Local Policies** folder and select **Security Options**.
4. In the right pane, double-click the **DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax** policy.


6. In the Launch Permission dialog box, click **Add**.

7. In the Enter the object names to select text box, type **ANONYMOUS LOGON**. (You can click **Check Names** to validate the account information that you have entered.)

8. Click **OK**.

9. Under Permissions for ANONYMOUS LOGON, grant the following rights:
   - Allow Local Launch
   - Allow Remote Launch
   - Allow Local Activation
• Allow Remote Activation

![Launch Permissions](image)

10. Click **OK**.
11. On the Template Security Policy Setting page, click **OK**.

**Granting necessary folder access rights**

The worker account that performs all requests for BusinessObjects Planning is the IWAM_MachineName user. For the BusinessObjects Planning Gateway to function properly, the IWAM user must have full rights to the following folders:

- The directory where the BusinessObjects Planning Gateway was installed (default installation is `c:\BusinessObjects\Planning\Programs\WebServer`)
- `c:\Windows\system32`
To grant necessary folder access rights:

1. In Windows Explorer, right-click on the **WebServers** folder and select **Sharing and Security** from the menu.

2. In the WebServer Properties dialog box, select the **Security** tab.

3. On the Security page, click **Add**.

4. In the Enter the object names to select text box, enter the IWAM_MachineName account name. This IWAM account is the same account that you identified in “Configuring the BusinessObjects Planning Analyst IIS COM+ application” on page 40. (You can click **Check Names** to validate the account information that you have entered.)

5. Click **OK**.
6. Under Permissions, grant the Allow Full Control right.

7. Click **OK**.

8. Repeat steps 1-7 for the c:\Windows\system32 folder.

**Configuring Internet Information Services (IIS)**

By default, IIS recycles worker processes every 120 minutes. This action causes the BusinessObjects Planning Gateway service to restart after 120 minutes of idle time. It is highly recommended that you disable this default setting. It is also recommended that you disable the idle timeout setting.

- **To configure Internet Information Services:**
  1. From the Windows Administrative Tools menu, select **Internet Information Services (IIS) Manager**.
  2. In the Internet Information Services (IIS) Manager, expand the **Applications Pools** folder.
3. Right-click **DefaultAppPool** and select **Properties** from the menu.

4. In the DefaultAppPool Properties dialog box, in the **Recycling** tab, clear the **Recycle worker processes (in minutes)** checkbox.
5. In the **Performance** tab, clear the **Idle timeout** checkbox.

6. Click **OK**.
Chapter 5

Installing and Configuring BusinessObjects Planning Login Server
The BusinessObjects Planning Login Server is a Windows NT service that handles user authentication against a variety of authentication sources. The BusinessObjects Planning Login Server can communicate with the following authentication sources:

- Windows domain authentication
- Novell NDS trees
- HTTP server authentication

This chapter provides the information necessary to install and configure BusinessObjects Planning Login Server. Specifically, this chapter provides information about:

- “Hardware requirements” on page 59
- “Installing BusinessObjects Planning Login Server” on page 59
- “Configuring BusinessObjects Planning Login Server” on page 61
- “Starting the Login Server” on page 64
- “Adding BusinessObjects Planning Login Server to your authentication scheme” on page 65
- “Error reporting” on page 65
Hardware requirements

The following table lists the minimum hardware requirements for BusinessObjects Planning Login Server.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Recommended minimum</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Pentium® III - 1.0 GHz</td>
</tr>
<tr>
<td>RAM</td>
<td>256 MB</td>
</tr>
<tr>
<td>Available hard drive space</td>
<td>100 MB</td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows 2000 Workstation or Server</td>
</tr>
<tr>
<td></td>
<td>Windows Server™ 2003</td>
</tr>
<tr>
<td>Network Bandwidth</td>
<td>Server to server 100 MB/sec</td>
</tr>
<tr>
<td>Other</td>
<td>A dedicated local user account on the BusinessObjects Planning Login Server machine. This account is used to start the BusinessObjects Planning Login Server service. If you are using Novell authentication, you must have a Novell client installed on the BusinessObjects Planning Login Server machine.</td>
</tr>
</tbody>
</table>

Installing BusinessObjects Planning Login Server

BusinessObjects Planning Login Server is implemented as a simple Windows service that runs using the local system account and does not have any shared file or database access. This section explains how to install BusinessObjects Planning Login Server.

To install BusinessObjects Planning Login Server:
1. Expand the LoginServer folder on the installation CD or network share and run BusinessObjectsPlanningLoginServer.msi.
2. In the BusinessObjects Planning Installation Wizard welcome dialog box, click Next.
3. In the Destination Folder dialog box, accept the default installation path, or click Change to specify the path to where you want the BusinessObjects Planning Login Server to be installed.
Note: You cannot change the installation path if you already have a BusinessObjects Planning application installed on the machine.

4. Click **Next**.

5. In the **Ready to Install the Program** dialog box, click **Install**.

6. In the **Folder locations** dialog box, in the **Path to the local folder** text box, type the path to your local folder or click **Browse** to select a location.

7. Select **Skip the verification of directories** if you don’t want the installer to verify that these folder exist.
Warning: If these folders don’t exist, the installer will not create them for you.

8. Click Next.
9. Click Finish.

Configuring BusinessObjects Planning Login Server

BusinessObjects Planning Login Server requires that a minimal set of user credentials be passed to it in order to verify a user. The minimal set of user credentials is a user name and password. User domain (for Windows authentication) or context and tree (Novell authentication) are optional for different authentication methods. The credentials are encrypted before being sent to the server. BusinessObjects Planning Login Server does not cache the credentials and removes them from memory when the authentication process is complete.

After installing the BusinessObjects Planning Login Server, you must configure settings in the [Login] section in the local Planning.ini file to define the authentication sources you want to use. BusinessObjects Planning Login Server supports the following types of authentication:

- Windows authentication—BusinessObjects Planning Login Server is able to verify Windows user credentials against:
  - Windows domains with which the machine can communicate. The authentication request is redirected to the corresponding domain controller.
  - Its own local machine domain.
- Novell authentication—BusinessObjects Planning Login Server verifies Novell user credentials against those NDS trees that are accessible from the machine.
- HTTP-based authentication—BusinessObjects Planning Login Server communicates with an HTTP server using the URL and HTTP method specified in the local configuration file. The authentication request follows standard HTTP protocol and it is up to the HTTP server how to handle it.

When configuring BusinessObjects Planning Login Server, you must set the following parameters:

- ActiveAuthenticationModules

If you are using HTTP authentication, you must also set the following parameters:
Configuring Security Guide

- HTTPPath
- HTTPLoginNamePattern
- HTTPRequestTimeout
- HTTPMethod

**Warning:** All changes to the configuration file require a restart of the BusinessObjects Planning Login Server service for the changes to take effect.

**ActiveAuthenticationModules**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Specifies a comma-separated list of names of authentication modules in the order that they should be queried to verify a user’s credentials. If any module succeeds in verifying the credentials, the user is verified and the remaining modules are not queried.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range of Values</td>
<td>The supported authentication modules are:</td>
</tr>
<tr>
<td></td>
<td>• NT – authentication against the local machine and Windows domains (default)</td>
</tr>
<tr>
<td></td>
<td>• NDS – authentication against Novell eDirectory (NDS)</td>
</tr>
<tr>
<td></td>
<td>• HTTP – authentication against an HTTP server</td>
</tr>
</tbody>
</table>

**HTTPPath**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Specifies the URL to use to authenticate BusinessObjects Planning users. There is no default value. The setting must be defined and have a valid value if the HTTP module is listed as one of the active authentication modules.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
<td>HTTPPath=<a href="http://authServer1">http://authServer1</a></td>
</tr>
</tbody>
</table>
### HTTPLoginNamePattern

**Purpose**  
Specifies the pattern that a user’s credentials (name and optional domain) should follow when sent to the HTTP server. The pattern should satisfy the requirements of the specific HTTP server configuration. The default value is user@domain. However, most IIS installations and configurations may require that information be sent as domain\user. If you are using the BusinessObjects Planning ISAPI filter to provide your HTTP authentication, this pattern must be the same as the UserNamePattern used to configure the ISAPI filter. For more information on this setting, see “Configuring the BusinessObjects Planning ISAPI filter” on page 89.  
Example: HTTPLoginNamePattern=user@domain

### HTTPRequestTimeout

**Purpose**  
Defines how long (in seconds) the Login Server waits for a response from the HTTP server. If the server does not respond within the time defined by the setting, the request is considered expired and user authentication failed.  
Example: HTTPRequestTimeout=420

<table>
<thead>
<tr>
<th>Range of Values</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>60 – 1 minute</td>
<td>420 - 7 minutes</td>
</tr>
<tr>
<td>600 – 10 minutes</td>
<td></td>
</tr>
</tbody>
</table>

### HTTPMethod

**Purpose**  
Specifies which HTTP method the BusinessObjects Planning Login Server uses when sending the authentication request to the HTTP server.  
Example: HTTPMethod=GET

<table>
<thead>
<tr>
<th>Range of Values</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td>GET</td>
</tr>
<tr>
<td>POST</td>
<td></td>
</tr>
</tbody>
</table>
Starting the Login Server

If you configured BusinessObjects Planning Login Server for automatic startup when you installed it, the server starts automatically when you start your system. If you configured it for manual startup, you must manually start the server using Windows Services.

To start the server manually using Windows Services, you must be a member of the Windows Administrator group.

To start the BusinessObjects Planning Login Server:
1. From the Start menu, select Settings and Control Panel.
2. In the Control Panel, double-click Administrative Tools.
3. In the Administrative Tool dialog box, double-click Services.
4. In the Services dialog box, right-click BusinessObjects Planning Login Server and select Start from the menu.

A message is displayed indicating that the Service is attempting to start the BusinessObjects Planning Login Server.

Note: If the service does not start, or an error message is displayed, ensure your Windows password is correct. To do this, right-click BusinessObjects Planning Login Server and select Properties. In the BusinessObjects Planning Site Login Service Properties dialog box, click the Log On tab. Re-enter and re-confirm your password, click OK, and repeat step 3.
Adding BusinessObjects Planning Login Server to your authentication scheme

After BusinessObjects Planning Login Server has been installed and configured, it must be added to your authentication scheme so that BusinessObjects Planning directs any authentication requests through BusinessObjects Planning Login Server and to whatever authentication source has been configured. Adding BusinessObjects Planning Login Server to your authentication scheme requires the following steps:

1. Launch the BusinessObjects Planning Security Configuration tool. See “Starting the Security configuration tool” on page 69 for information on how to do this.
2. Configure those applications that require authentication. See “Configuring the applications that require identity confirmation” on page 77 for information on how to do this.
3. Add the BusinessObjects Planning Login Server to your list of external authentication servers. For information on adding BusinessObjects Planning Login Server to your list of authentication servers, see “Configuring external authentication servers” on page 83.
4. Close the tool.

Error reporting

Since BusinessObjects Planning Login Server runs under a local system account, the BusinessObjects Planning shared folder is inaccessible to the application. Therefore, Login Server does not log any messages into files located on shared network resources, including the BusinessObjects Planning shared folder. Instead, BusinessObjects Planning Login Server logs internal errors, user authentication failures and successes, and any diagnostics messages using the local machine’s Windows Event Log.
Installing and Configuring BusinessObjects Planning Login Server

Error reporting
Using the Security Configuration Tool
The BusinessObjects Planning Security Configuration tool configures BusinessObjects Planning data repository access, BusinessObjects Planning shared folder access, and user creation and authentication when gaining access to BusinessObjects Planning.

This section provides information about:

- “Starting the Security configuration tool” on page 69
- “Editing database access parameters” on page 70
- “Configuring BusinessObjects Planning shared folder access” on page 74
- “Configuring login account types” on page 75
- “Configuring login confirmation” on page 76
- “Configuring user auto-creation” on page 79
- “Configuring external authentication servers” on page 83
Starting the Security configuration tool

BusinessObjects Planning Site Administrators can use the BusinessObjects Planning Security Configuration tool to configure their site security settings.

**Warning:** This tool should be used by BusinessObjects Planning site administrators only. Before launching this tool, you must know the BusinessObjects Planning site database password and you must have write access to the BusinessObjects Planning configuration file, Planning.ini.

**To start the Security Configuration tool:**
1. Expand the **Site** and **Tools** folder on the installation CD or network share and run **CtpSecConfig.exe**.

2. In the BusinessObjects Planning Site Shared Folder dialog box, in the Folder text box, type the path to the BusinessObjects Planning site’s shared folder, or click **Browse** to specify a location.

   **Note:** This dialog box is not shown if your registry settings already point to a valid shared folder.

3. In the Password text box, type the password to the BusinessObjects Planning data repository. This is the same password that was created during the installation of the BusinessObjects Planning site.

4. Click **OK**.
Editing database access parameters

If the BusinessObjects Planning site's database or database server has been moved or renamed, the corresponding site configuration settings must be updated.

With the Security Configuration tool, you can edit the following database access parameters:

- Database attributes
- Database account
- Database password

**Note:** Depending on how your database has been configured, you may be required to have appropriate rights and privileges to perform these actions.

To edit the database access parameters, on the Database page, click **Change**.
Editing the database attributes

The database attributes specify the database server name, the database name, and the data source name to be used in ODBC connections.

► To edit the database attributes:
1. On the Database And Account page, select the Change database attributes check box.
2. In the Database server text box, type the name of the new database server.
3. In the Database name text box, type the name of the database.
4. In the Data source name text box, type the name of the data source. This name will be used to create ODBC connections to the database.

5. Click OK.

Editing the database account

The database account specifies the account name to be used to connect to the database.

To edit the database account:
1. On the Database And Account page, select the Account check box.
2. In the Account text box, type the name of the new account.
Using the Security Configuration Tool

Editing database access parameters

Note: This account must exist in the database and have rights to access the BusinessObjects Planning database, otherwise client applications cannot connect.

3. Click OK.

Note: This change causes the connection to the database to close. You must restart the Security Configuration tool to continue working with it.

Editing the database password

The database password specifies the password to be used to connect to the database.

To edit the database password:

1. On the Database And Account page, select the Password check box.
2. In the Password text box, type the new password.
3. In the Type it again text box, retype the new password.
4. Select the Update also in the database check box to update the password in the database if the password has not been updated there yet.
5. Click OK.

Note: This change causes the connection to the database to close. You must restart the Security Configuration tool to continue working with it.
By default, BusinessObjects Planning uses Windows authentication to authenticate its users. However, there may be some BusinessObjects Planning users who are not working from a Windows domain. The Security Configuration tool allows an administrator to redirect all unauthenticated accounts to use a dedicated Windows domain account.

The shared folder configuration settings are saved in the [Planning] section of the shared Planning.ini file.

### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SharedDirectoryAccount</td>
<td>The account to use.</td>
</tr>
<tr>
<td>SharedDirectoryPassword</td>
<td>The encrypted password for the account.</td>
</tr>
</tbody>
</table>

**Note:** A dedicated account must be created before default user access can be configured. This account must be granted full rights (read, write, modify, control) on the BusinessObjects Planning shared folder.

To configure shared folder access:

1. Click the Protection tab.
2. On the Protection page, click Change.
3. In the User name text box, type the domain and name of the dedicated account.
4. In the Password text box, type the password for the account.
5. In the Confirm password text box, retype the password for the account.
6. Click OK.
Configuring login account types

By default, BusinessObjects Planning uses Windows authentication to authenticate its users. Using the Security Configuration tool, you can enable your site authentication through other pre-configured types of user accounts.

To configure the login account types:
1. Click the Accounts tab. The types of accounts are listed in the order that they are checked when a user logs in.

2. To add a type of user account to BusinessObjects Planning authentication, click Add.

3. Select the type of account to add from the account list.

4. Click OK.
5. Select the **Remember the last login and use it next time** check box if you want the last used type of account to be remembered for each user. When the user logs in again, the last used type of account is used first to authenticate that user.

6. To remove an account, select the account you want to remove from the Type of account list and click **Remove**.

7. To change the order in which accounts are checked, select an account from the Type of account list and click **Up** or **Down**.

8. Click **Apply**.

### Configuring login confirmation

Depending on the level of security your organization requires, you can configure BusinessObjects Planning applications to force users to confirm their identity every time they launch a BusinessObjects Planning application. The security configuration tool allows you to perform the following actions when configuring login confirmation:

- Enable identity confirmation
- Configure the applications that require identity confirmation
- Edit application properties

### Enabling identity confirmation

When identity confirmation is enabled, users must type in their username and password every time they login to BusinessObjects Planning.

- **To enable identity confirmation**:
  1. Click the **Confirmation** tab.
Using the Security Configuration Tool

Configuring login confirmation

2. Select the **Identity confirmation is required** check box.

3. Select when a user must confirm their identity. The options are:
   - **Mandatory for every user**—Every time a user logs in they must enter their username and password
   - **For not yet registered users only**—Unregistered users must enter their username and password the first time they use BusinessObjects Planning
   - **Optional for pre-authenticated users**—The username and password text boxes are pre-filled for pre-authenticated users. A different username and password can be entered if the user wants to log in as a different user.

4. Click **Apply**.

**Configuring the applications that require identity confirmation**

Once identity confirmation is enabled, you can specify which BusinessObjects Planning applications require identity confirmation.
To configure which applications require identity confirmation:

1. On the Confirmation page, in the Application list, view the list of BusinessObjects Planning applications that require identity confirmation.
2. To add an application, click **Add**.
3. Select the application to add from the application list.
4. Select the **User may edit identity attributes** check box if you want to allow users to log into BusinessObjects Planning with an account different from the one they are currently using on their workstation.
5. Click **OK**.
6. To remove an application, select the BusinessObjects Planning application from the Application list and click **Remove**.
7. Click **Apply**.

**Editing application properties**

You can configure whether users are allowed to log into BusinessObjects Planning with an account that is different from the one they are currently using on their workstation.

To edit an application’s properties:

1. Select the application from the Application list and click **Properties**.
2. Select the **User may edit identity attributes** check box if you want to allow users to log into BusinessObjects Planning with an account different from the one they are currently using on their workstation.

OR

Clear the **User may edit identity attributes** check box if you want to force users to log into BusinessObjects Planning with the account they are currently using on their workstation.
Configuring user auto-creation

When a new user attempts to gain access to BusinessObjects Planning, you can configure whether to register them with BusinessObjects Planning automatically. Specifically, you can:

• Enable automatic user registration
• Configure account types for automatic registration
• Configure applications that register users automatically

Enabling automatic user registration

When automatic user registration is enabled, new users are automatically registered in BusinessObjects Planning upon successful login, provided that:

• The user's account type is configured to allow auto-registration
• The BusinessObjects Planning application that the user launched is configured to allow auto-registration

To enable automatic user registration:
1. Click the Auto-creation tab.
Using the Security Configuration Tool
Configuring user auto-creation

2. Select the **Register a new BusinessObjects Planning user automatically** check box.

3. Click **Apply**.

**Configuring login account types for user registration**

Once automatic user registration is enabled, you can configure the type of user accounts that are allowed to register user accounts in BusinessObjects Planning automatically.

- **To configure login account types:**
  1. On the Auto-creation page, in the Type of account list, view the list of accounts that are allowed to register users automatically.
  2. To add an account type, click **Add**.
  3. Select the account type to add from the account list.

4. Click **OK**.
5. To remove an account type, select the account type from the Type of account list and click Remove.

6. Click Apply.

### Configuring applications that automatically register users

You can specify which BusinessObjects Planning applications can or cannot register users automatically. The Security Configuration tool allows only one of the two options to be chosen; therefore you must decide whether you will specify which applications will register users automatically, or which applications will not register users automatically.

➤ **To configure which applications can automatically register users:**

1. On the Auto-creation page, select the **These applications should not register accounts automatically** option if you want to specify which applications will not register accounts automatically. Any application not listed will be able to register accounts automatically.

OR
Select the **Only these applications may register accounts automatically** option if you want to specify which applications can register accounts automatically. Any application not listed will not be able to register accounts automatically.

2. In the Application list, view the list of BusinessObjects Planning applications.

3. To add an application to the list, click **Add**.

4. Select the application to add from the application list.

**Note:** It is not recommended to enable automatic user registration from BusinessObjects Planning Application Servers (ApplicationServer).

5. Click **OK**.
6. To remove an application, select the application from the Application list and click **Remove**.

7. Click **Apply**.

### Configuring external authentication servers

If user identity confirmation is required (as configured on the Confirmation page), then the verification of a user’s credentials can be performed either locally or on an external BusinessObjects Planning Login Server. (For information on installing the BusinessObjects Planning Login Server, see “Installing and Configuring BusinessObjects Planning Login Server” on page 57.)

Windows domain accounts and Novell (NDS®) accounts can be verified locally as long as the workstation is a member of the appropriate Windows domain, or Novell Client software is installed and the machine is connected to the appropriate eDirectory server. If neither of these options are applicable, the BusinessObjects Planning application delegates the verification of a user’s credentials to a BusinessObjects Planning Login Server.

Using the Security Configuration tool, you can:

- Enable external authentication
- Configure the server order
- Remove servers
- Test server connection
- Edit the properties of a server

### Enabling external authentication

When external authentication is enabled, users who cannot be authenticated by their local workstation can be authenticated by an external authentication server.

- **To enable external authentication:**
  1. Click the **Servers** tab.
  2. Select the **Redirect user authentication to external servers** check box.
3. Select the **Only if local authentication fails** check box if you want external authentication servers to be used only when local authentication fails.

![Security Configuration Tool](image1)

4. Click **Add** to add an authentication server to the list of authentication servers.

5. In the Computer text box, type the name of the BusinessObjects Planning Login Server machine.

![Add new server](image2)

6. Click **OK**.

7. Click **Apply**.

**Configuring server order**

Using the Security Configuration tool, you can manage the order in which external authentication servers are contacted.
To configure the server order:
1. On the Servers page, in the List of authentication servers, view the order of the external authentication servers.
2. To change the order in which an external server is contacted, select the server from the List of authentication servers and click Up or Down.
3. Click Apply.

Removing servers
Using the Security Configuration tool, you can remove a server from the list of external authentication servers.

To remove a server:
1. On the Servers page, in the List of authentication servers, view the names of the available external authentication servers.
2. Select the server you want to remove from the List of authentication servers and click Remove.
3. Click Apply.

Testing the server connection
Using the Security Configuration tool, you can test the connection to an external authentication servers.

To test the connection to a server:
1. On the Servers page, in the List of authentication servers, view the names of the available external authentication servers.
2. Select the server whose connection you want to test from the List of authentication servers and click Test.
3. In the User name text box, type a valid account username.
4. In the Password text box, type the password for the account.
5. In the Domain text box, type the domain for the account.
6. Click OK.

Editing the properties of a server
This feature is reserved for future use.
Using the Security Configuration Tool
Configuring external authentication servers
Installing and Configuring the BusinessObjects Planning ISAPI Filter
This section provides the information necessary to install and configure the BusinessObjects Planning ISAPI filter. This filter can authenticate users against the following authentication sources:

- Windows domains
- Novell NDS trees
- Active Directory

This section assumes that you have knowledge of Microsoft IIS and the authentication source you are using to authenticate your users.

Specifically, this section provides information about:

- “Installing the BusinessObjects Planning ISAPI filter” on page 89
- “Configuring the BusinessObjects Planning ISAPI filter” on page 89
- “Configuring the BusinessObjects Planning ISAPI extension” on page 91
Installing the BusinessObjects Planning ISAPI filter

The BusinessObjects Planning ISAPI filter must be installed on all web servers.

To install BusinessObjects Planning ISAPI filter:
1. Expand the Filters folder on the installation CD or network share.
2. Copy the following files to the <web_install>/bin folder, where <web_install> is the folder where you have installed the BusinessObjects Planning Analyst site. (For most installations, this is the C:\BusinessObjects\Planning\Programs\WebServer\Web folder.)
   • ServiceSetup.dll
   • std-2.1-vc5.0-mt.dll
   • DirectoryServiceAuthFilter.dll
3. Open Internet Services Manager and add the DirectoryServiceAuthFilter.dll file to your list of ISAPI filters.

Configuring the BusinessObjects Planning ISAPI filter

After installing the BusinessObjects Planning ISAPI filter, you must create the configuration file for the filter and add the necessary settings to configure the authentication sources.

To configure the ISAPI filter:
1. In the <web_install>/bin folder, create a file called CtpWebConfig.ini.
2. Type the following section heading in this file:
   [DirectoryServiceAuthentication]
3. Save the file and add the following parameters to the listed section:
   • Provider
   • DirectoryName
   • UserNamePattern
   • ProtectedResource

Warning: All changes to the configuration file require a restart of the BusinessObjects Planning Web Server for the changes to take effect.
## Provider

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Specifies the authentication module to use to provide authentication.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range of Values</td>
<td>The supported authentication modules are:</td>
</tr>
<tr>
<td></td>
<td>• WINNT – authentication against the local machine and Windows domains (default)</td>
</tr>
<tr>
<td></td>
<td>• NDS – authentication against Novell eDirectory (NDS)</td>
</tr>
<tr>
<td></td>
<td>• LDAP – authentication against an LDAP repository</td>
</tr>
<tr>
<td>Example</td>
<td>Provider=LDAP</td>
</tr>
</tbody>
</table>

### DirectoryName

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Specifies the name and path to the authentication module.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
<td>DirectoryName=LDAP://CORENW_WIN</td>
</tr>
</tbody>
</table>

### UserNamePattern

<table>
<thead>
<tr>
<th>Purpose</th>
<th>When a user logs in, they can enter their username and domain combination in one of the following ways:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• domain/username</td>
</tr>
<tr>
<td></td>
<td>• domain\username</td>
</tr>
<tr>
<td></td>
<td>• username@domain</td>
</tr>
<tr>
<td></td>
<td>• username</td>
</tr>
<tr>
<td>The ISAPI filter parses the user’s name from the text and passes the username to the authentication module.</td>
<td></td>
</tr>
<tr>
<td>The UserNamePattern specifies, according to the specifications of the authentication module, how to pass the parsed user name to the authentication module. Each UserNamePattern must include the &lt;user&gt; value. This value is a placeholder for the username that is parsed from the user’s credentials on the login screen.</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>UserNamePattern=cn=&lt;user&gt;,ou=user,o=employee</td>
</tr>
</tbody>
</table>

| Range of Values | There is no set range of values as each authentication module can have its own specific pattern. |
| Section | DirectoryServiceAuthentication |
After configuring the BusinessObjects Planning ISAPI filter, you must add the necessary settings to configure the ISAPI extension.

To configure the ISAPI extension:
1. Open the CtpWebConfig.ini file in an editor.
2. Type the following section headings in this file:
   [CtpWebExtension]
   [CtpWebISAPI]
3. Save the file and add the following parameters to the listed sections:
   - DefaultDomainName
   - ThreadPoolMaxSize

ProtectedResource

Purpose Identifies the local BusinessObjects Planning web site. This must be specified using the local Windows path.
Example: ProtectedResource= c:\BusinessObjects\programs\webserver\web.

DirectoryServiceAuthentication

Purpose Specifies the domain name to use when connecting to BusinessObjects Planning. BusinessObjects Planning requires that all usernames consist of a user name and a domain. If your authentication module does not require users to enter a domain when being authenticated, this setting can be used to pass a domain to BusinessObjects Planning.

Range of Values Any valid domain name. The default value is ‘none’.
Example: DefaultDomainName=domainName

Section CtpWebExtension

Configuring the BusinessObjects Planning ISAPI extension
**ThreadPoolMaxSize**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Specifies the maximum number of operating system threads that can process BusinessObjects Planning SOAP requests.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range of Values</td>
<td><strong>40 - infinite.</strong> The default value is 40. Example:ThreadPoolMaxSize=40</td>
</tr>
<tr>
<td>Section</td>
<td>CtpWebISAPI</td>
</tr>
</tbody>
</table>
Configuring Security-Related INI Settings
This chapter provides information about security-specific INI settings in BusinessObjects Planning. Specifically, this chapter provides information about:

- "Configuring INI settings" on page 95
Configuring INI settings

The following settings in the [Planning] section of the Planning.ini file are used to configure security:

- ApplicationTimeout

To configure the security-related INI settings:

1. Expand the `<BusinessObjects_Planning_shared_folder>` and `config` folders.
2. Open the `Planning.ini` file in an editor.
3. Change the parameters to the necessary values.
4. Save and close the file.

**ApplicationTimeout**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Specifies the time in minutes to wait for a user’s session to end before they can open another application session on a different machine. Regardless of this setting’s value, a user is always allowed to open multiple application sessions from the same machine.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range of Values</td>
<td>Any integer &gt;=0.</td>
</tr>
<tr>
<td>Example: ApplicationTimeout=0</td>
<td></td>
</tr>
<tr>
<td>Default Value</td>
<td>0 - Allow multiple sessions for the same user from multiple machines.</td>
</tr>
</tbody>
</table>
Configuring Security-Related INI Settings

Configuring INI settings
Index

B
BusinessObjects Planning Login Server
  hardware requirements 59
  installing 59, 89, 95
BusinessObjects Planning Server
  starting on Windows 2000 64

H
hardware requirements
  BusinessObjects Planning Login Server 59

I
INEAFinance.ini settings
  ServerRating parameter 62, 62, 63, 63
  installing
    BusinessObjects Planning Login
      Server 59, 89, 95

P
Planning.ini settings
  ServerRating parameter 91

R
RPCTransport section of INEAFinance.ini
  ServerRating parameter 62, 62, 63, 63
RPCTransport section of Planning.ini
  ServerRating parameter 91

S
ServerRating parameter 62, 62, 63, 63, 91
  starting
    BusinessObjects Planning Server (Windows 2000) 64