



# User Guide

## bv-Control<sup>®</sup> for Active Directory<sup>®</sup>





# **bv-Control<sup>®</sup>** ***for Active Directory<sup>®</sup> v8.00***

## User Guide



## **COPYRIGHT**

Copyright © 2002–2004 BindView Corporation. All rights reserved. BindView Corporation is a business name of BindView Development Corporation. Information in this document is subject to change and revision without notice. The software described herein may only be used and copied as outlined in the Software License Agreement. No part of this manual may be reproduced by any means, electronic or mechanical, for any purpose other than the purchaser's personal use, without prior written permission from BindView Corporation.

BINDVIEW CORPORATION PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL BINDVIEW CORPORATION BE LIABLE FOR ANY LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OR DATA, INTERRUPTION OF BUSINESS, OR FOR DAMAGES OF ANY KIND, EVEN IF BINDVIEW CORPORATION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES ARISING FROM ANY DEFECT OR ERROR IN THIS DOCUMENTATION.

BindView Corporation may revise this publication from time to time without notice. Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitations may not apply. BindView Corporation's liability for actual damages from any cause whatsoever, and regardless of the form of the action (whether in contract, tort (including negligence), product liability or otherwise) will be limited to \$50.00 U.S.

## **TRADEMARK NOTES**

BindView, the BindView logo, and the BindView product names used in this document are trademarks of BindView Corporation and may be registered in one or more jurisdictions.

The names of products of other companies mentioned in this document, if any, may be the registered or unregistered trademarks of the owners of the products.

**July 2004**



---

# Contents

<b>Information Resources</b> .....	<b>9</b>
About BindView Corporation .....	10
Online Documents .....	10
Using PDF Files .....	10
User Guides .....	10
Release Notes .....	11
Online Help .....	11
Typestyle Conventions .....	11
Alert Statements .....	11
Contacting BindView .....	12
<b>1 Overview</b> .....	<b>13</b>
BindView RMS Console .....	14
Understanding bv-Control for Active Directory .....	15
bv-Control for Active Directory Architecture .....	16
Client .....	16
Information Server .....	17
Key Features of bv-Control for Active Directory .....	17
<b>2 Setting Up the Product</b> .....	<b>19</b>
System Requirements .....	20
Pre-installation .....	20
Upgrading from a Previous Version .....	20
Installing	
bv-Control for Active Directory .....	21
Adding Product Licenses .....	26
Configuration Wizard .....	30
Credential Database .....	35
Credential Requirements .....	35
Assign a Credential Database to a User .....	39
Uninstalling	
bv-Control for Active Directory .....	42
<b>3 Using the Product</b> .....	<b>45</b>
Query-Related Features .....	46
Understanding a Query .....	46
Creating a Query .....	46
Query Building Process .....	46

Defining a Query . . . . .	46
Saving a Query Definition . . . . .	54
Multiple Forest Support . . . . .	55
Requirements . . . . .	55
Running a Query . . . . .	66
Task Status Monitoring . . . . .	66
Accessing a Previously Saved Query . . . . .	67
Displaying Query Results . . . . .	68
Grid . . . . .	68
Chart . . . . .	68
Report . . . . .	69
Baselining . . . . .	69
Creating a Baseline . . . . .	69
Task Lists . . . . .	70
Building Task Lists . . . . .	70
Generating a Field List . . . . .	71
Effective Trustees Functionality . . . . .	73
Available Permissions . . . . .	73
Credential Requirements . . . . .	74
Limitations . . . . .	75
Group Policy Objects (GPOs) Functionality . . . . .	75
Descriptor: <Available Fields to Group Policies> Dialog . . . . .	75
<b>4 Advanced Use Scenarios . . . . .</b>	<b>77</b>
Introduction . . . . .	78
Scenario 1: Reporting on Multiple Forests . . . . .	78
Scenario 2: Verifying Credentials Across Forests . . . . .	79
Scenario 3: Using Generic Scopes . . . . .	84
<b>Appendix A Troubleshooting . . . . .</b>	<b>87</b>
<b>Index . . . . .</b>	<b>99</b>



---

# Information Resources

---

## **In This Section**

About BindView Corporation .....	10
Online Documents .....	10
Typestyle Conventions .....	11
Alert Statements .....	11
Contacting BindView .....	12

---

---

## About BindView Corporation

BindView Corporation is a leading provider of proactive business policy, IT security and directory management software worldwide. BindView solutions and services enable customers to centralize and automate policy compliance, vulnerability management, directory administration and migration across the entire organization. With BindView insight at work™, customers benefit from reduced risk and improved operational efficiencies with a verifiable return on investment. More than 20 million licenses have shipped to 5,000 companies worldwide, spanning all major business segments and the public sector.

---

## Online Documents

Documentation is provided in the following electronic formats on the BindView product CD:

- Adobe® Acrobat® PDF files
- HTML Release Notes files
- Online help

---

## Using PDF Files

With Adobe Acrobat PDF files, you can navigate through a document quickly and perform full-text searches. In addition, the PDF files can be viewed online, distributed to multiple users electronically, or printed.

You must have Adobe® Reader® installed to read the PDF files.

To view PDF files, double-click PDF files to open them, and then move through the document by clicking topic headings in the left pane or **green** hypertext links in the text. To print copies, click **Print** from the **File** menu.

---

## Installing Adobe Reader

Adobe Reader installation programs for common operating systems are available for a free download from the Adobe Web site at [www.adobe.com](http://www.adobe.com).

---

## User Guides

The Docs directory on the BindView product CD contains copies of the user guides and other documentation in the PDF format.

The *bv-Control for Active Directory User Guide* contains information about bv-Control for Active Directory v8.0 and about the BindView RMS Console and Information Server v8.0. If you upgrade the BindView RMS Console and Information Server, the *BindView RMS Console and Information Server User Guide* included with the update will contain information about the new version of the Console.

---

## Release Notes

If the autorun function is enabled, a Readme HTML file for your BindView product is accessible under the Documentation menu of the BindView setup menu when you insert your CD. You also can select to view this file after the installation is completed, or by browsing to the Release Notes directory in the root directory for your program:

```
C:\Program Files\BindView\RMS\Release Notes\bv-Control  
for Active Directory
```

---

## Online Help

Comprehensive help is available from the Help menu on the BindView RMS Console and the BindView RMS Web Console. Additionally, you can access help by clicking the **Help** button in any dialog, by right-clicking an item and selecting **Help** from the action menu, or by pressing **F1** in any dialog.

---

## Typestyle Conventions

The following conventions are observed throughout this guide:

- **Bold** text is used to designate file and folder names, dialog titles, names of buttons, icons, and menus, and terms that are objects of a user selection.
- *Italic* text is used for word emphasis, defined terms, and manual titles.
- Monospace text (*Courier*) is used to show literal text as you would enter it, or as it would appear onscreen.

---

## Alert Statements

The alerting statements are Notes, Cautions, and Warnings. These statements are formatted in the following style:

---

**Note:** Information that is incidental to the main text flow, or to an important point or tip provided in addition to the previous statement or instruction.

---

---

**Caution:** Advises of machine or data error that could occur should the user fail to take or avoid a specified action.

---

---

**Warning:** Requires immediate action by the user to prevent actual loss of data or where an action is irreversible, or when physical damage to the machine or devices is possible.

---

---

## Contacting BindView

BindView has sales and support offices around the world. For information on contacting BindView, please refer to the information below or to the BindView Web site: **[www.bindview.com](http://www.bindview.com)**

For Technical Support: **[www.bindview.com/support](http://www.bindview.com/support)**

Technical Support is available Monday through Friday from 7:00 a.m. to 7:00 p.m. Central Time. Normal working hours for all other departments are 9:00 a.m. to 6:00 p.m.

---

### Phone

Sales and Customer Service	U.S. and Canada	800-813-5869
	Outside N. America	713-561-4000
Technical Support	U.S. and Canada	800-813-5867
	Outside N. America	713-561-4000
Training/Professional Service	U.S. and Canada	800-749-8439
	Outside N. America	713-561-4000

---

### Fax

All Areas 713-561-1000

---

### E-mail

Sales	<a href="mailto:sales@bindview.com">sales@bindview.com</a>
Training	<a href="mailto:edu@bindview.com">edu@bindview.com</a>
Documentation	<a href="mailto:docs@bindview.com">docs@bindview.com</a>

---

### Other

FTP Site	<a href="ftp://ftp.bindview.com">ftp://ftp.bindview.com</a>
Internet	<a href="http://www.bindview.com">www.bindview.com</a>
Postal Mail	BindView 5151 San Felipe, Suite 2500 Houston, TX 77056

---

---

# 1

# Overview

---

## In This Chapter

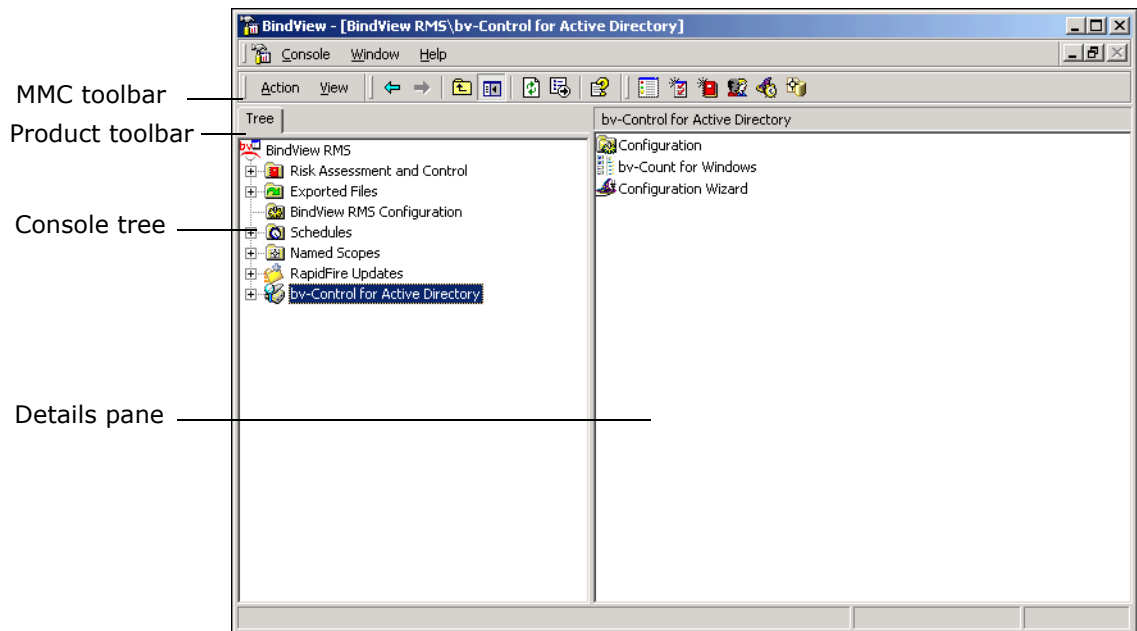
BindView RMS Console .....	14
Understanding bv-Control for Active Directory .....	15
bv-Control for Active Directory Architecture.....	16
Key Features of bv-Control for Active Directory .....	17

---

## BindView RMS Console

The BindView RMS® Console installs as a snap-in to the Microsoft Management Console (MMC). The MMC is a host application that provides a common user interface enabling you to navigate the BindView RMS Console application. The BindView RMS Console, along with bv-Control® for Active Directory®, is a powerful tool designed to help you manage your Microsoft® Windows® 2000 and Microsoft Windows Server™ 2003 environment. The BindView RMS Console serves as a host application to other BindView products, including bv-Control for Active Directory, bv-Control® IntelliPACS®, bv-Control for Microsoft Exchange, and other BindView products.

Figure 1 shows the BindView RMS Console and the major components of its user interface.



**Fig. 1** BindView RMS Console User Interface

The BindView RMS Console provides query-based data retrieval to gather information from your Active Directory service. When a query is processed, the BindView RMS Console queries Active Directory to gather information about the Active Directory objects and properties. Once the data is collected, it is returned to the BindView RMS Console and displayed as either a grid, chart, or a report. You can find more complete instructions on how to use the BindView RMS Console in the *BindView RMS Console and Information Server v8.0 User Guide*.

---

## Understanding bv-Control for Active Directory

The bv-Control for Active Directory snap-in is a BindView product that provides comprehensive administrative reporting capabilities for Active Directory service objects and properties. This product provides broad querying capabilities. The bv-Control for Active Directory product focuses on automating the task of collecting and reporting information about an Active Directory service relative to containers and OUs, domains, groups, group policies (GPO) and users. The bv-Control for Active Directory product can query information in multiple trees and domains across an enterprise, as well as specific objects in these trees and domains. Multi-forest support has been added in this release.

From BindView's centralized RMS Console, you can document and report on virtually every aspect of Active Directory and Group Policies. bv-Control for Active Directory provides IT personnel with key abilities to perform security checks across the enterprise for possible security or configuration breaches. bv-Control for Active Directory also provides hundreds of detailed fields for reporting on the configuration of Active Directory and Group Policies, saving administrators time and money over native or third-party tools. These key and unique capabilities of bv-Control for Active Directory allow administrators to communicate the current state of Active Directory, along with the ability to easily highlight configuration and security issues for immediate resolution.

bv-Control for Active Directory also allows for easy report modification and a vast amount of exporting venues for further analysis. This product leverages BindView's leadership in the vulnerability assessment market, which has allowed BindView to provide industry-leading technology for assessing, auditing, and administering Microsoft®, Novell®, and UNIX® enterprises.

bv-Control for Active Directory contains several new features contained in Windows Server 2003 such as:

- Reports on the new permissions and new delegated tasks offered by the Delegation Control Wizard.
- Reports on the new Group Policy settings for Terminal Services, Network Management, and Computer Management.
- Domain and Forest functional levels have been introduced in Windows Server 2003, which provide a way to enable features in a domain or forest throughout an organization. bv-Control for Active Directory reports on the different levels.
- Support for Forests Trusts – Effective Permissions, Effective Permissions Analysis, and Effective Trustees take into account the permissions obtained through security principals and memberships in groups across the forest.
- InetOrgPerson is a new object offered. This object is similar to the user object. bv-Control for Active Directory will report on this through the user's data source. This object is also a security principal. bv-Control for Active Directory also reports on the effective permissions and effective delegated tasks for this security principal.

- Reports on attributes available to Active Directory objects through Auxiliary classes.

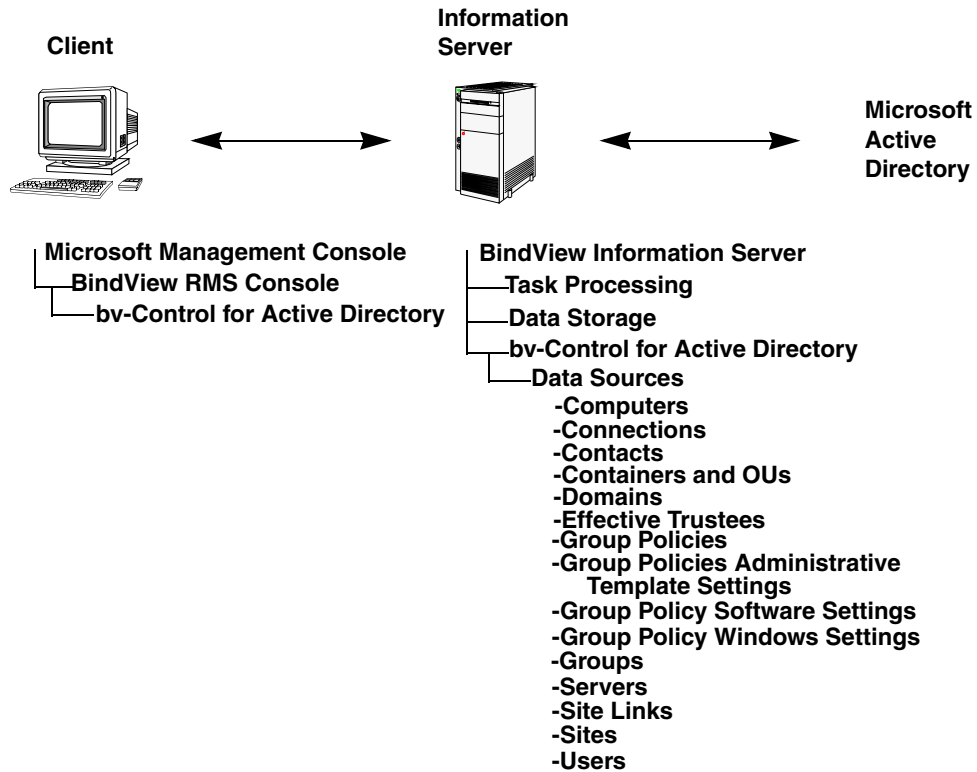
## bv-Control for Active Directory Architecture

bv-Control for Active Directory consists of two BindView RMS Console components:

- Client
- Information Server

The Information Server component provides the BindView RMS Console with a source of data for reporting, and the Client component provides the user interface extensions.

Figure 2 shows the architecture for bv-Control for Active Directory and how it interfaces with the Client and Server component.



**Fig. 2** bv-Control for Active Directory Architecture

### Client

The Client component provides the user interface extensions to the BindView RMS Console. This component enables you to configure the bv-Control for Active Directory product. It extends the BindView RMS Console shell to facilitate utilities that do not fit within the query model.



---

## Information Server

The Information Server is primarily used to perform the following services:

- Task processing
- Data storage

There are two types of Information Servers: local and remote. A local Information Server exists on the same machine as the Console you are using. A remote Information Server exists on a different machine than the one where your Console resides.

The Information Server component provides data collection facilities for the BindView RMS Console. This component exposes the user schema to the BindView RMS Console. The user schema constitutes the data sources and fields that the user may select for creating reports, and provides User Interface components, such as dialog pages that are specific to the data sources and fields of the bv-Control for Active Directory product. This component is responsible for combining information in a way that recognizes requests from the BindView RMS Console.

## Data Sources

Within bv-Control for Active Directory are categories of information called *data sources*. A data source is a collection of multiple related fields you select when defining a query, and is a key component of the product. By using bv-Control for Active Directory, administrators can analyze virtually every aspect of Active Directory. The first step in determining exactly what information you want to gather is to select a data source to query. For information on how to select a data source, refer to ["Defining a Query" on page 46](#).

---

## Key Features of bv-Control for Active Directory

System administrators who are responsible for administering and securing their Active Directory can rely on bv-Control for Active Directory for systems solutions.

The following key features of bv-Control for Active Directory will aid in administering and configuring Microsoft Active Directory. These key features are:

- Pre-defined Query Binder and Task List
- Full query-based interface to easily perform custom queries
- Advanced Report, Graph, and Export capability

## Pre-defined Query Binder and Task List

The bv-Control for Active Directory snap-in comes with hundreds of pre-defined Query Binders that identify key issues. With a simple point-and-click interface that can get the system up and running in a matter of minutes, bv-Control for Active Directory will allow you to quickly and proactively determine the state of Active Directory.

BindView periodically extends the number of pre-defined Query Binders and ships these additions with each future release.

***Custom Queries***

In addition to providing sample reports for out-of-the-box use, bv-Control for Active Directory also provides a full query-based interface allowing Active Directory administrators to easily build custom queries for information specific to their environment. Results from the queries can be saved for trend analysis and capability planning at a later time.

***Advanced Report, Graph, and Export Capability***

bv-Control for Active Directory provides flexible, comprehensive reporting and graphing that produces reports aimed at a variety of audiences. This allows an Active Directory administrator to quickly identify and document a specific problem. The ultimate in flexibility is achieved by advanced capabilities which allow report information to be graphed, compared to an established baseline, and exported into a variety of data formats such as Microsoft Excel, Microsoft Word, dBase, PDF, and Microsoft Access.

---

# 2

## Setting Up the Product

---

### In This Chapter

System Requirements .....	20
Pre-installation .....	20
Upgrading from a Previous Version.....	20
Installing bv-Control for Active Directory.....	21
Configuration Wizard.....	30
Credential Database.....	35
Uninstalling bv-Control for Active Directory .....	42

---

---

## System Requirements

For complete system requirements for the BindView RMS Console, please see the *BindView RMS Console and Information Server v8.00 User Guide*.

Before you install bv-Control for Active Directory, make sure that your workstation and network environment meet the following minimum bv-Control for Active Directory hardware and software requirements:

- 512 MB RAM in addition to Microsoft Windows 2000 minimum requirement
- 500 MB of free disk space
- Virtual memory size three times the size of RAM
- Microsoft XML parser v3.0 or higher
- Microsoft Windows Installer
- The RMS Console and Information Server requires one of the following OS versions:
  - Windows Server™ 2003 (Standard, Enterprise, Web Edition) or later
  - Windows® 2000 SP3 (Professional, Server, Advanced)
  - Windows XP® Professional SP1

Vast amounts of data can be gathered from Active Directory. This data is stored on the hard drive of the machine that the Information Server was installed on. Although 90 MB is sufficient storage space for the application, space is also needed for the data retrieved. The amount of space needed is dependent on multiple factors such as the size of your operational environment, the information you retrieve, and how often its data is refreshed and saved.

---

## Pre-installation

bv-Control for Active Directory is shipped on a CD. You must install the BindView RMS Console v8.0 CD *before* installing the bv-Control for Active Directory product. When you install bv-Control for Active Directory, it will either install into an existing BindView RMS Console, or it will install the BindView RMS Console if not already present. For more information on installing the BindView RMS Console, see the *BindView RMS Console and Information Server v8.00 User Guide*.

---

## Upgrading from a Previous Version

If your computer has a previously installed version of bv-Control for Active Directory, you do not need to perform any additional steps for an upgrade installation. It is a silent upgrade install.

## Installing bv-Control for Active Directory

After you have reviewed the pre-installation information, you can use the Install panel to install the bv-Control for Active Directory product. We recommend that you review the Release Notes files for the Console and Information Server and the bv-Control for Active Directory product.

### ► **To install bv-Control for Active Directory**

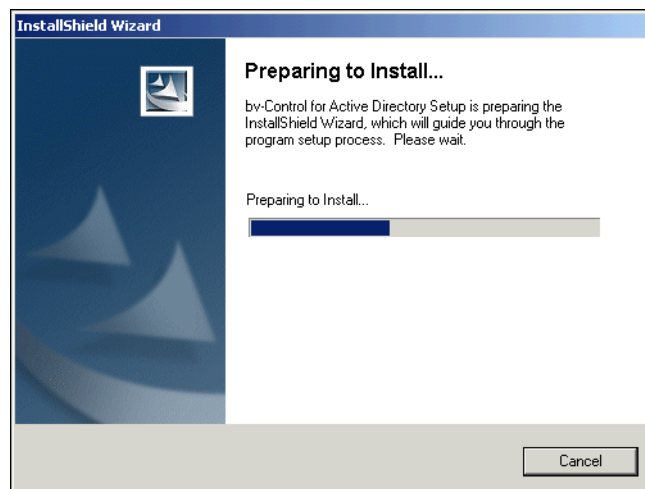
- 1 Insert your bv-Control for Active Directory v8.00 CD into the CD-ROM drive for your machine and the **Welcome Panel** appears.



**Fig. 3** Welcome Panel

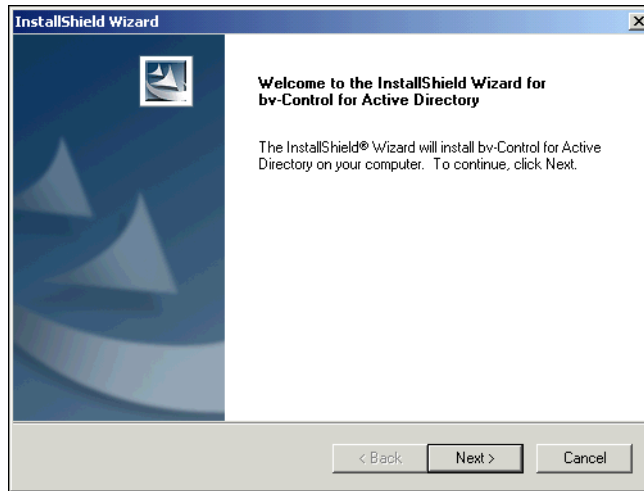
- 2 Select **Install** to install and configure bv-Control for Active Directory.

The **InstallShield Wizard – Preparing to Install** panel appears.



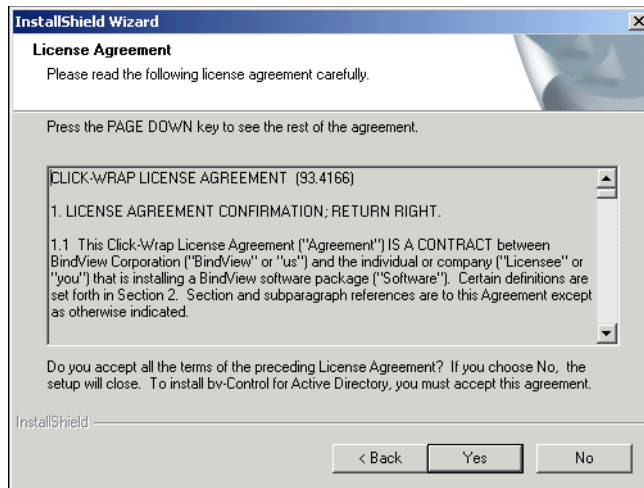
**Fig. 4** InstallShield Wizard – Preparing to Install Panel

The **InstallShield Wizard – Welcome panel** appears.



**Fig. 5** InstallShield Wizard – Welcome Panel

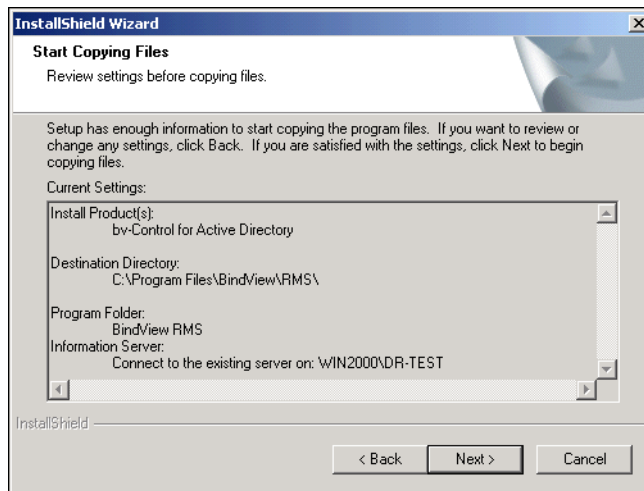
- 3 Read the information on the panel and click **Next**.  
The **Software License Agreement** panel appears.



**Fig. 6** License Agreement Panel

- 4 Read the license agreement and click **Yes** to accept the terms.

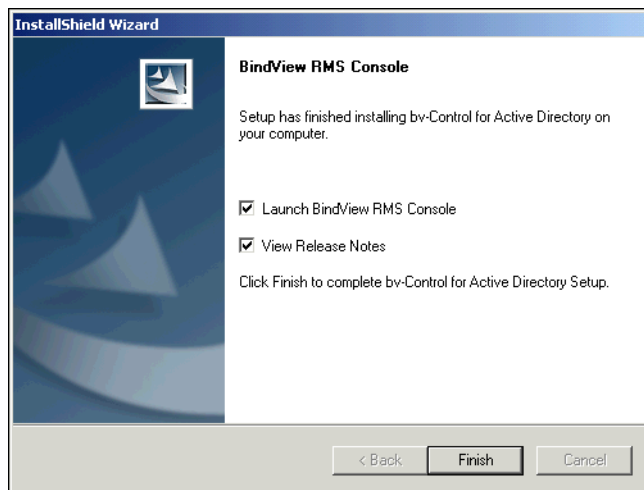
The **Start Copying Files** panel appears.



**Fig. 7** Start Copying Files Panel

- 5 Review the information in the Current Settings area and click **Next**.

The **InstallShield Wizard – Setup Complete** panel appears once the BindView RMS Console has been installed.



**Fig. 8** InstallShield Wizard – Setup Complete Panel

- 6 Select one or both options in the Setup Complete panel.

If you selected **Launch BindView RMS Console**, the BindView product installation screens appear while bv-Control for Active Directory is installed on your machine.

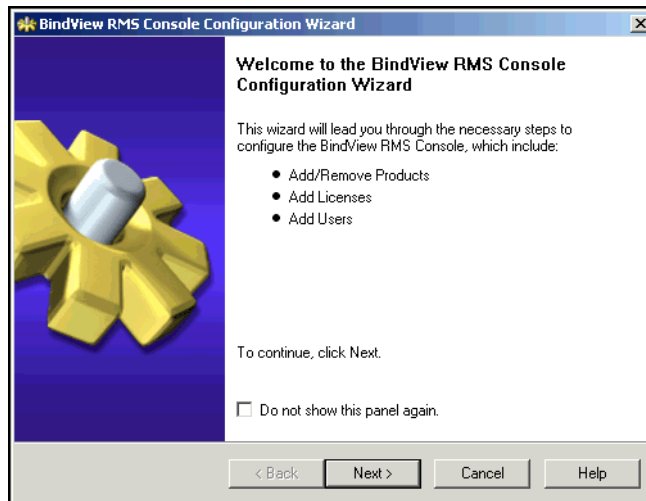
If you selected **View Release Notes**, the Release Notes for the bv-Control for Active Directory appears.

The Product Installation panel appears, showing which products have been installed.



**Fig. 9** Product Installation Panel

The **BindView RMS Console Configuration Wizard – Welcome** panel appears.

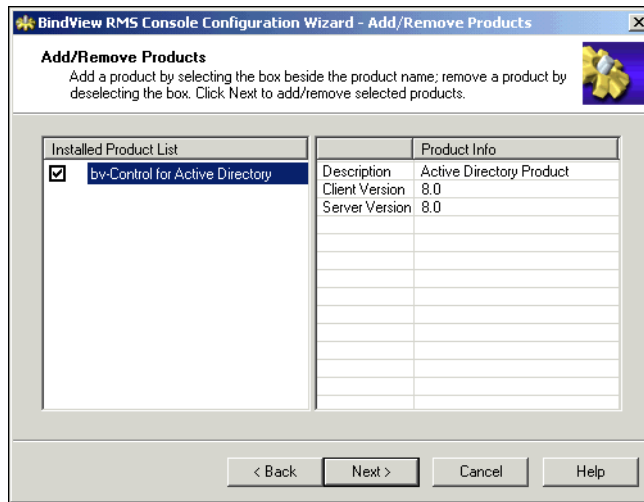


**Fig. 10** BindView RMS Console Configuration Wizard – Welcome Panel

**7** Click **Next** to continue.

This opens the **Add/Remove Products** panel.

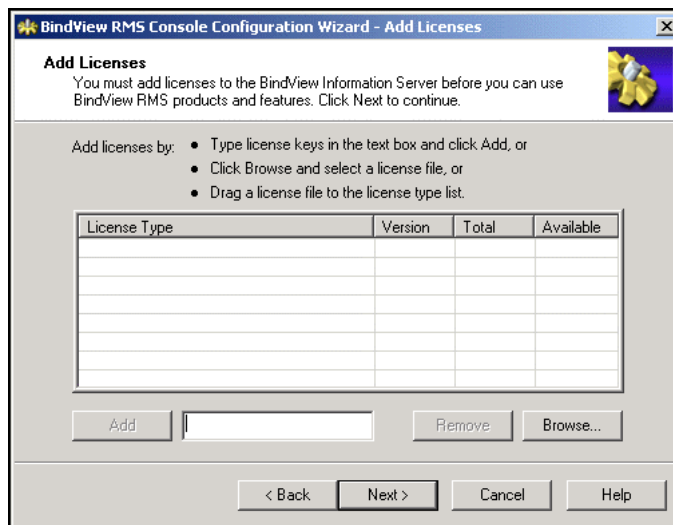




**Fig. 11** Add/Remove Products Panel

- 8** Check **bv-Control for Active Directory** to add to the BindView RMS Console and click **Next**.

The **Add Licenses** panel appears.



**Fig. 12** Adding Licenses

**License Type** - List of the type of licenses currently installed.

**Add** - Allows you to add a new license manually.

**Remove** - Displays the Delete License dialog.

**Browse** - Allows you to install licenses from a different location.

## Adding Product Licenses

To use the products, you must have the required licenses for both the Console and bv-Control for Active Directory.

► **To add licenses**

- 1 From the **Add Licenses** panel (Fig. 12), you can add license codes in the following ways:
  - Enter license keys in the text box and click **Add**.
  - Click **Browse** to browse to the location of the license file and select the file.
  - Drag a license file to the license type list.

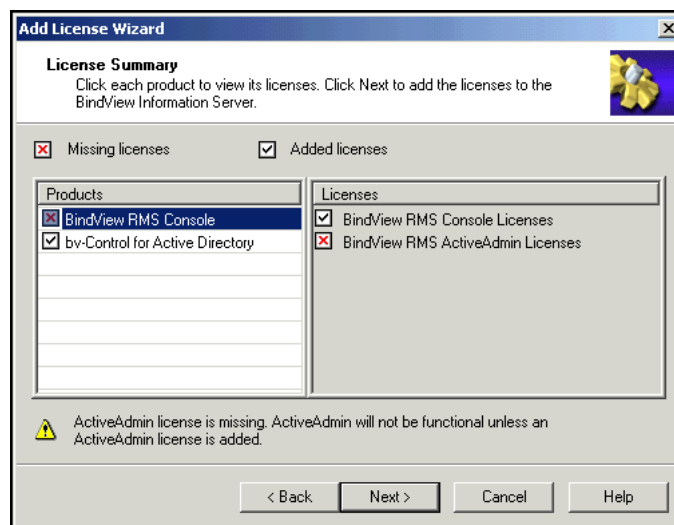
---

**Note:** A license.txt file can be dragged and dropped into the **Add Licenses** dialog.

---

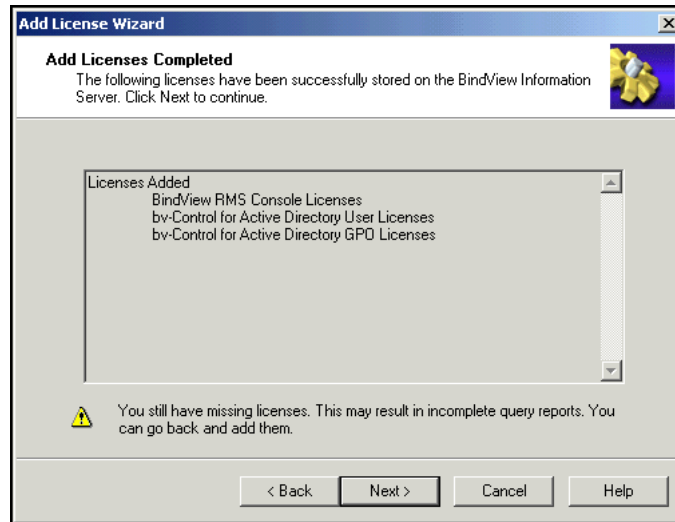
- 2 Repeat the process you choose until you have entered all your BindView product license codes and click **Next**.

The **License Summary** panel appears.



**Fig. 13** Add License Summary Panel

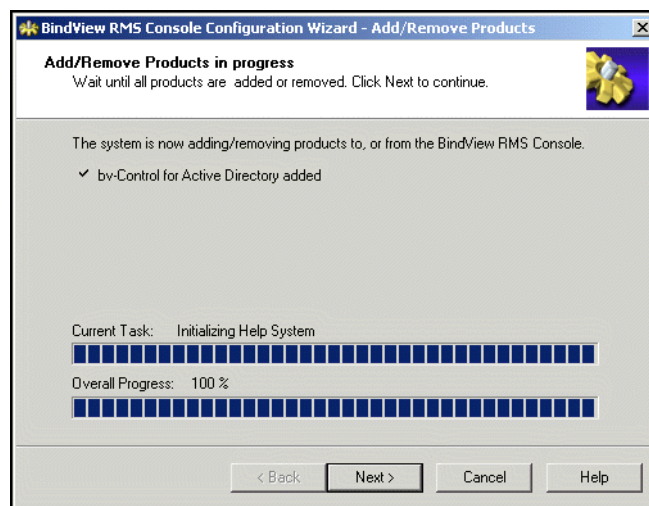
- 3 Click **Next**.  
This opens the **Add License Completed** panel.



**Fig. 14** Add Licenses Completed

**4** Click **Next** to continue.

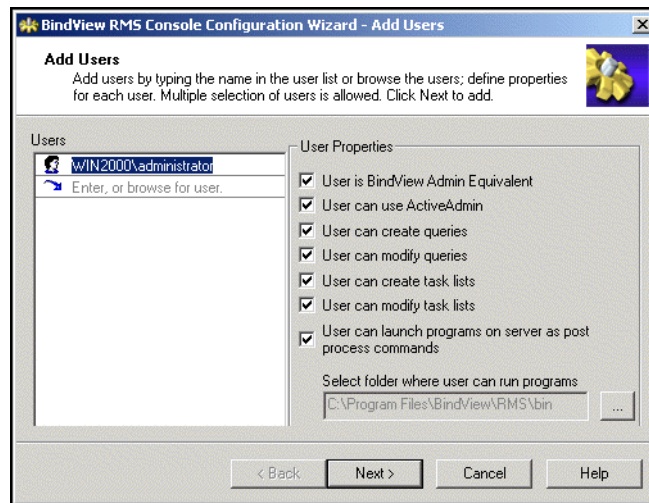
The **Add/Remove Products in progress** panel appears.



**Fig. 15** Add/Remove Products in Progress Panel

**5** When the process has finished, click **Next**.

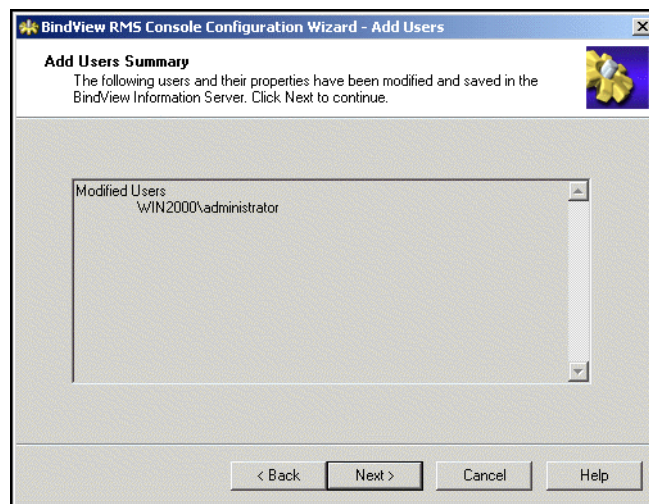
The **Add Users** panel opens.



**Fig. 16** Add Users Panel

- 6** Add users by typing their fully qualified path in the **Users** frame, or by using the browse (...) button to open a dialog for selecting the desired user.
- 7** Assign the desired user properties for each added user, click **Next**.

The **Add Users Summary** panel appears, displaying a summary of the users who were added.



**Fig. 17** Add Users Summary Panel

- 8** To continue, click **Next**.

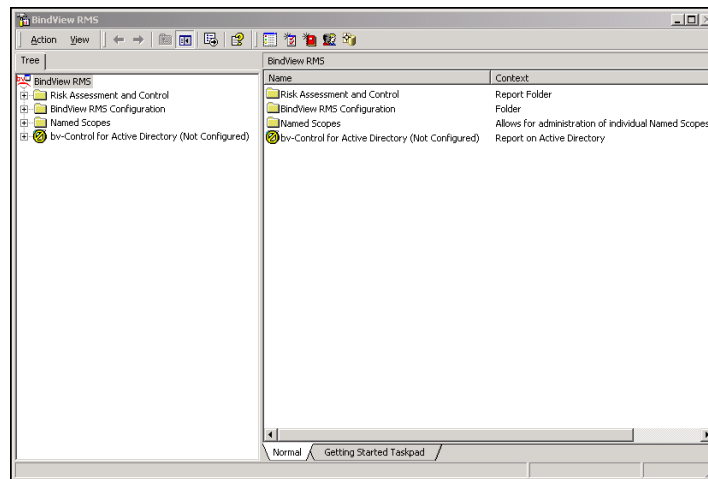
The **BindView RMS Console Configuration Wizard – Completed** panel appears.



**Fig. 18** BindView RMS Console Configuration Wizard – Completed Panel

- 9 Click **Finish** to close this panel.

After you have completed the installation process, the MMC console with the BindView RMS Console snap-in opens (Fig. 19).



**Fig. 19** BindView RMS Console

The first time the BindView RMS Console opens with bv-Control for Active Directory installed, the bv-Control for Active Directory product is not configured. Configuring the bv-Control for Active Directory is explained next.

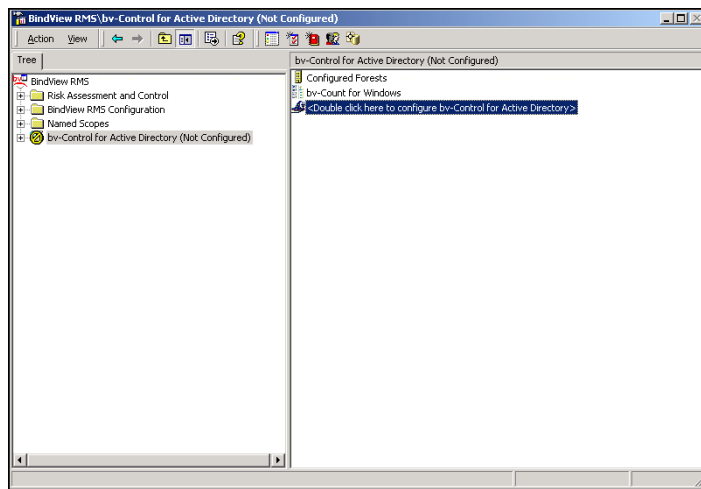
## Configuration Wizard

Prior to using bv-Control for Active Directory, you must configure the bv-Control for Active Directory product.

► **To configure bv-Control for Active Directory**

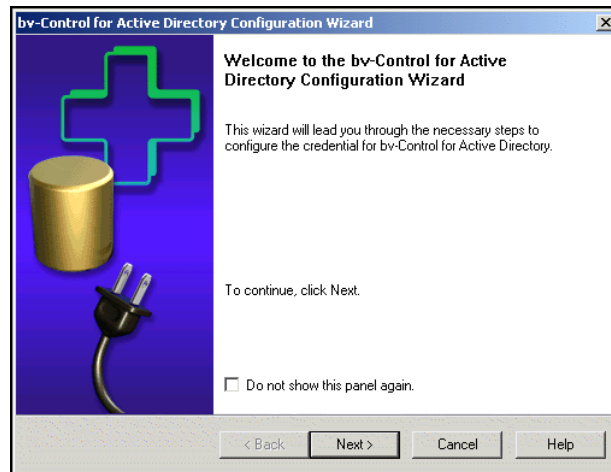
Once the BindView RMS Console and Information Server is installed, the bv-Control for Active Directory Configuration Wizard will guide you through the steps needed to configure the product.

- 1 Click the Not Configured  icon in the Console tree. This will display the Configuration Wizard  icon in the Details pane.



**Fig. 20** Starting the bv-Control for Active Directory Configuration Wizard

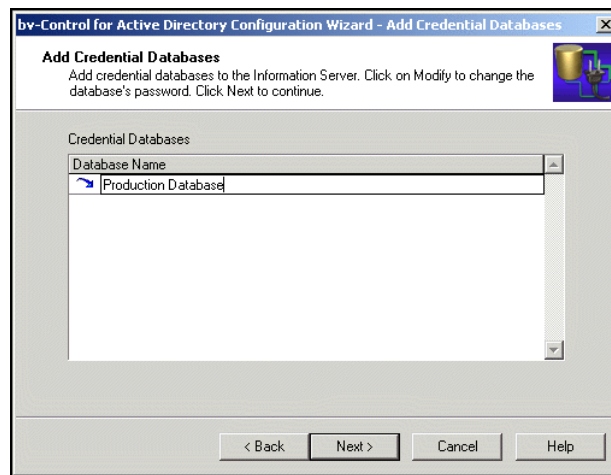
- 2 Double-click the Configuration Wizard icon.  
The bv-Control for Active Directory **Configuration Wizard** appears.



**Fig. 21** bv-Control for Active Directory Configuration Wizard –Welcome Panel

**3** Click **Next**.

The **Add Credential Databases** panel appears.



**Fig. 22** Add Credential Databases Panel

**4** Enter a Database Name.

**5** Click **Next**.

The **Create New Database** dialog appears.

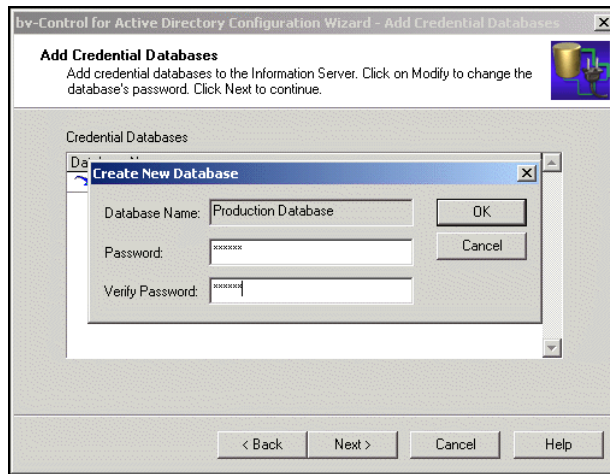


Fig. 23 Create New Database Dialog

► **To add a database**

- 6 Enter a password and verify this password for this database.
- 7 Click **OK** and then click **Next** to load the credentials.  
The **Select Credentials** panel appears.

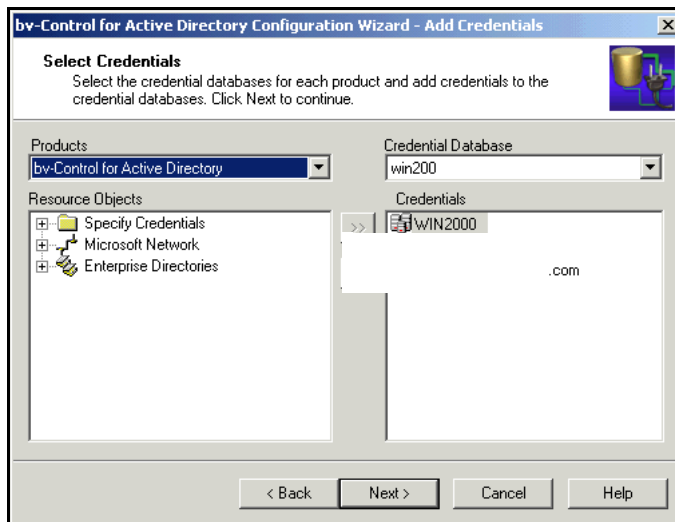
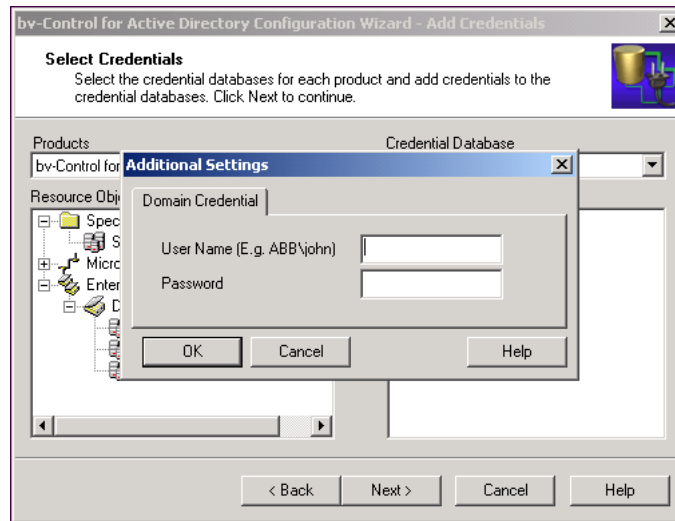


Fig. 24 Add Credentials

► **To add credentials and apply a credential database to a user**

- 1 Select a domain under Resource Objects to open the **Additional Settings** dialog.

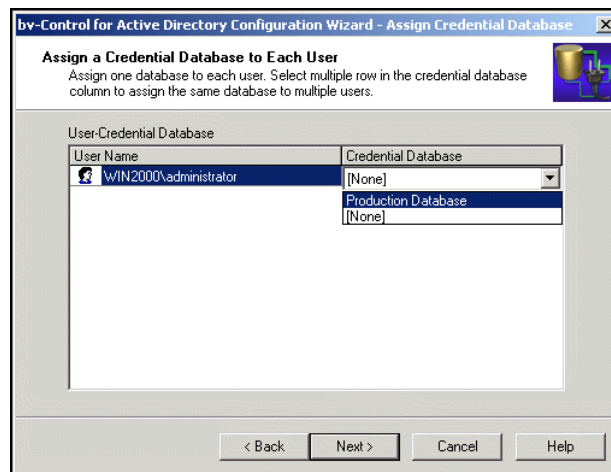




**Fig. 25** Additional Settings

**2** Click **OK**.

The bv-Control for Active Directory Configuration Wizard – Assign a Credential Database to Each User panel appears.

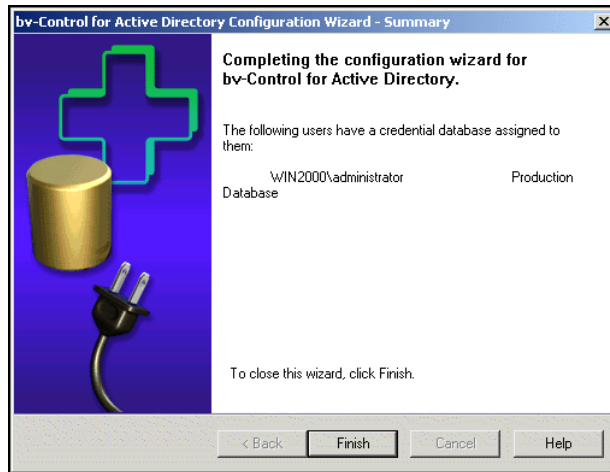


**Fig. 26** Assign a Credential Database to Each User Panel

**3** Click the drop-down list box and select a database.

**4** Click **Next**.

The bv-Control for Active Directory **Configuration Wizard – Summary** panel appears.



**Fig. 27** bv-Control for Active Directory Configuration Wizard – Summary Panel

- 5 Click **Finish** to close the wizard.

## Credential Database

The BindView RMS Console Job Processor is running as a local system account. Because the Job Processor is running locally, it has no network credentials. To collect information from the resource objects you are querying, the Information Server must have rights to those objects. A credential database provides the Information Server with the necessary credentials to authenticate the user of those resources. The Console uses the credential data so that the Information Server can logon to the resources during query processing and obtain information it needs to generate the results. Once a credential database is created, you must add that credential database to the user's account.

## Credential Requirements

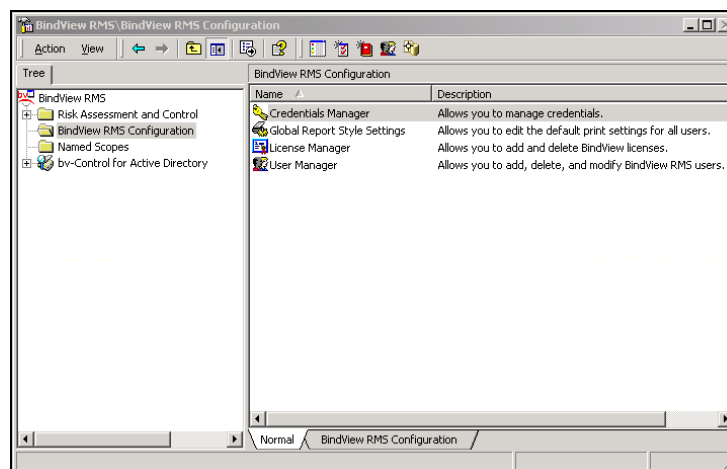
To configure the Console with the credential databases, you must perform the following tasks:

- Create a credential database
- Add a database
- Add credentials to the credential database
- Assign a credential database to a user

### ► **To create a credential database**

You can create and configure credential databases for each user to meet their requirements.

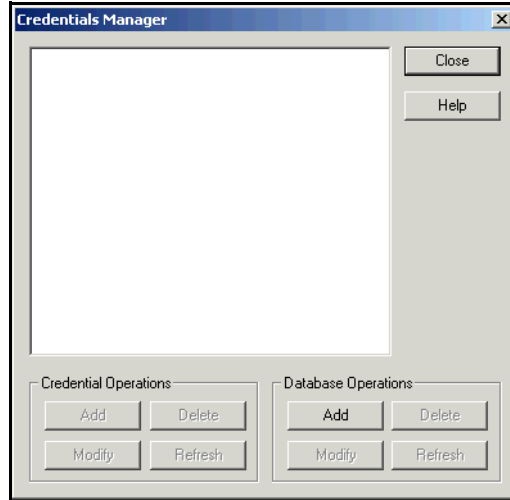
- 1 From the console, click the **BindView RMS Configuration** folder.



**Fig. 28** Console Setup

- 2 Double-click the **Credentials Manager**  icon in the details pane.

The **Credentials Manager** dialog appears for creating a credential database.



**Fig. 29** Credentials Manager Dialog

► **To add a database**

- 3 Click **Add** under **Database Operations**.

The **Create New Database** dialog appears for creating a credential database.



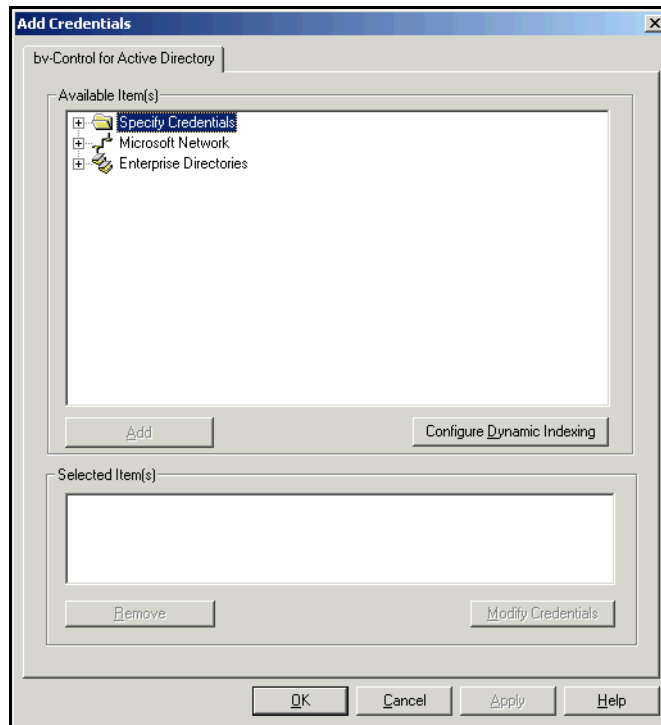
**Fig. 30** Create New Database Dialog

- 4 Enter a **Database Name**.
- 5 Enter a password and verify the password for this database.
- 6 Click **OK**.

► **To add credentials**

- 7 Click **Add** under **Credential Operations**.

The **Add Credentials** dialog appears (Fig. 31).



**Fig. 31** Add Credentials Dialog

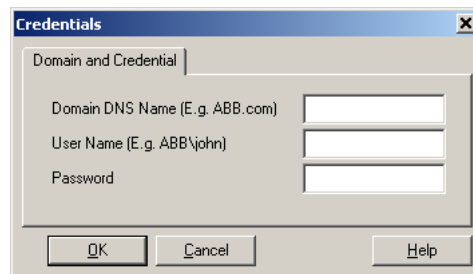
---

**Note:** For information on Available Item(s), which includes Specify Credentials, Microsoft Network, and Enterprise Directories see ["Multiple Forest Support"](#) on page 55.

---

- 8** Select the Domain Controller (DC) from the main forest you want to add credentials for and click **Add**.

The **Domain and Credential** tab appears.



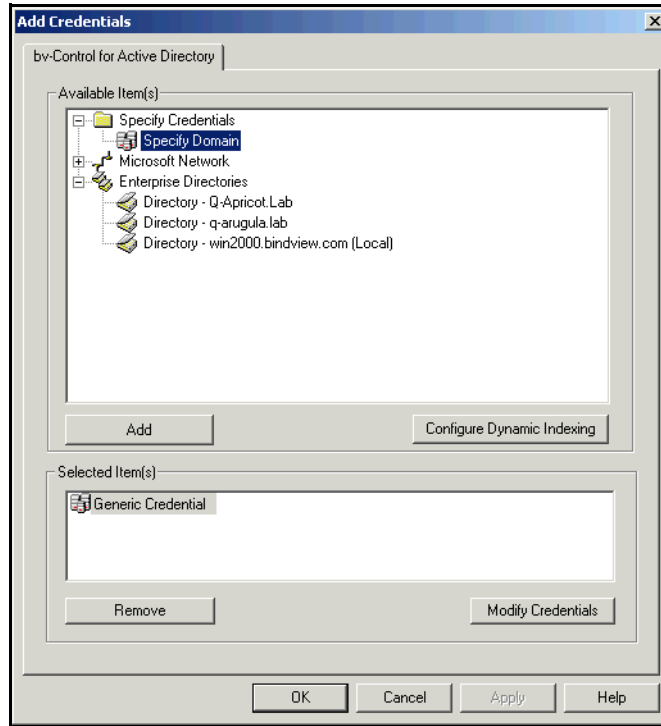
**Fig. 32** Domain and Credential Tab

- 9** On the Domain and Credential tab, enter the Domain Name\User Name and Password. Click **OK**.

The domain name\user name may be entered by either using a backslash \ to separate domain name and user name or by entering the user logon name. For example,

WIN2000\Administrator

- 10** The **Add Credentials** dialog reappears. The domain is listed under **Selected Item(s)**.



**Fig. 33** Adding Credentials

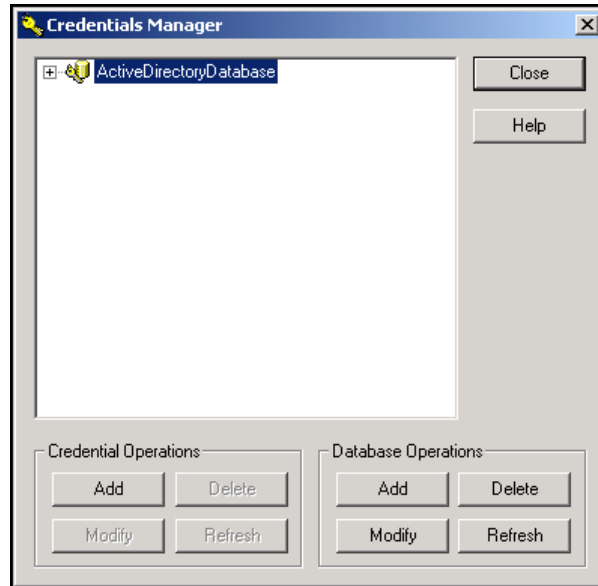
---

**Note:** "Local" refers to the Information Server being installed in this forest

---

- 11** To add credentials to multiple databases, repeat Steps 8 through 10.
- 12** Click **OK** only when all domains have been added.

The **Credentials Manager** dialog reappears showing the credential you added (Fig. 34).



**Fig. 34** Credentials Manager Dialog

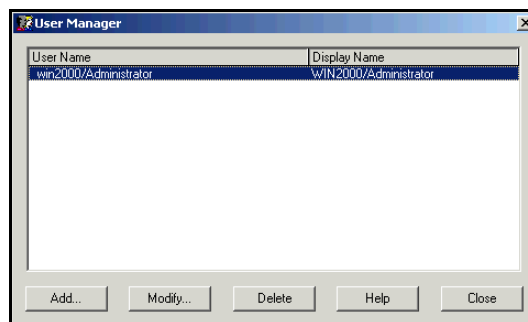
**13** Click **Close**.

## Assign a Credential Database to a User

Once a credential database is created, you must add the credential database to the user's account. You can attach users to the machine in the local domain where the currently selected Information Server is running or they can be attached to a domain trusted by the local domain.

### ► **To assign a credential database to a user**

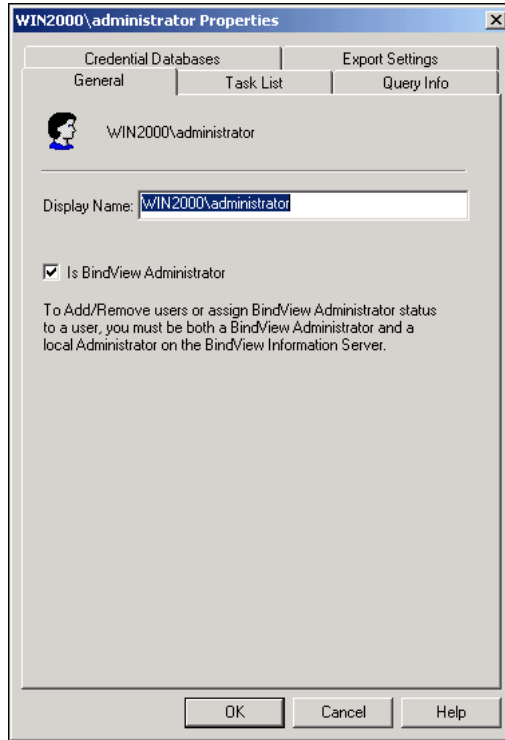
**1** Double-click the **User Manager**  icon in the details pane to show the **User Manager** dialog.



**Fig. 35** User Manager Dialog

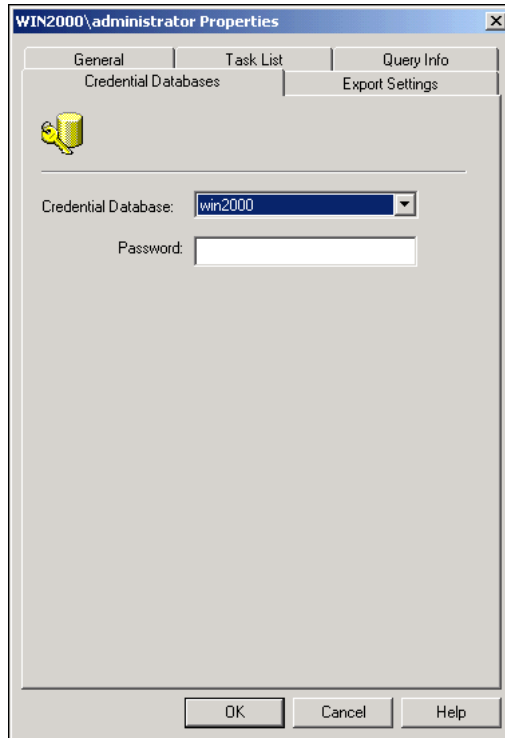
**2** Select a user name and click **Modify**.

The **<User> Properties** dialog appears (Fig. 36).



**Fig. 36** <User> Properties Dialog

**3** Select the **Credential Databases** tab.

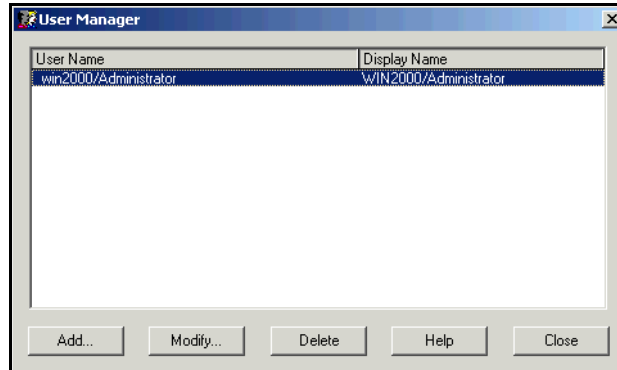


**Fig. 37** Credential Databases Tab



- 4 Select the database name from the **Credential Database** drop-down list.
- 5 Enter the password that is assigned to the database.
- 6 Click **OK** to return to the User Manager dialog.

The **User Manager** dialog reappears (Fig. 38).



**Fig. 38** User Manager Dialog

You can add, modify, or delete users by selecting the appropriate buttons. For more information on how to add or modify users, refer to the *BindView RMS Console and Information Server v8.00 User Guide*.

- 7 When you have completed this process, click **Close**.  
You have added the credential database to the user's account.

## Uninstalling bv-Control for Active Directory

Removing bv-Control for Active Directory can be accomplished in the following process:

- ▶ **To uninstall bv-Control for Active Directory**
  - 1 Close all applications running under Windows.
  - 2 Click **Start** from the task bar.
  - 3 Select **Settings**, and click **Control Panel**.
  - 4 From the **Control Panel**, double-click **Add/Remove Programs**.

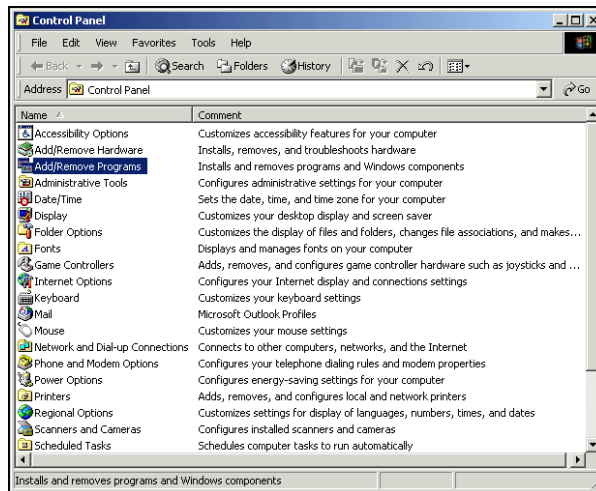


Fig. 39 Control Panel Window

- 5 From the **Add/Remove Programs** properties dialog, select bv-Control for Active Directory, and click **Change/Remove**.

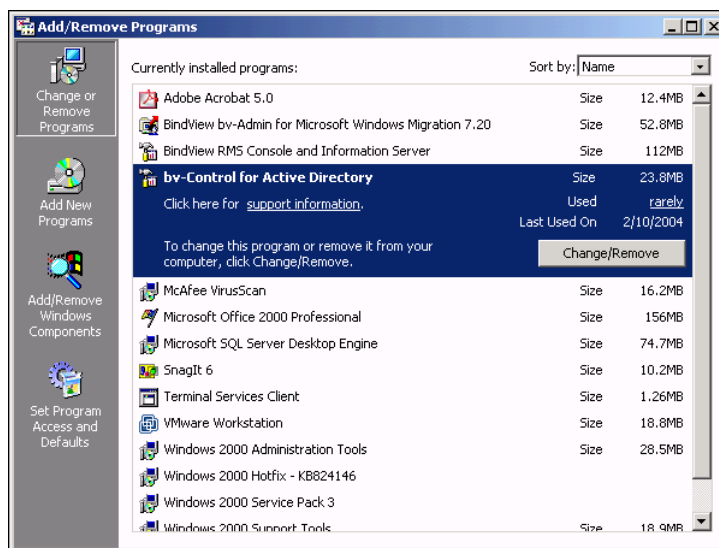
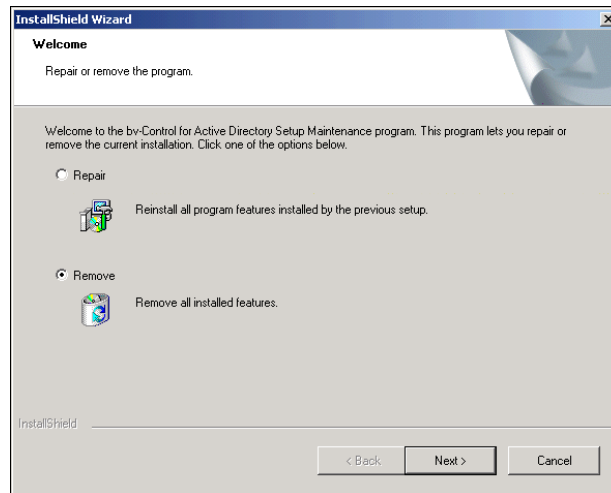


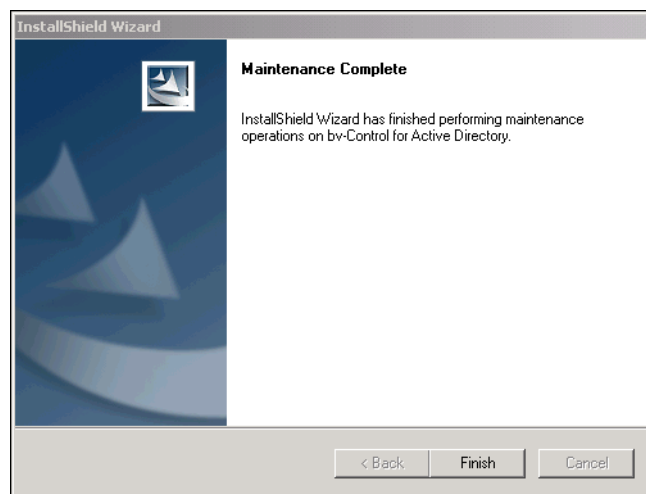
Fig. 40 Add/Remove Programs Dialog

The InstallShield Wizard appears and will guide you through the steps for repair or removal of programs.



**Fig. 41** InstallShield Wizard – Repair or Remove the Program

- 6 To remove bv-Control for Active Directory, select **Remove** and click **Next**. You will be prompted to confirm that you wish to remove the product.
- 7 Click **OK** to completely remove bv-Control for Active Directory. The InstallShield Wizard appears with the **Maintenance Complete** panel.



**Fig. 42** Maintenance Complete Panel

- 8 Click **Finish** to close the wizard.

---

**Note:** For information on how to uninstall the BindView RMS Console and Information Server, refer to the *BindView RMS Console and Information Server v8.00 User Guide*.

---



---

# 3

# Using the Product

---

## In This Chapter

Query-Related Features .....	46
Query Building Process .....	46
Multiple Forest Support .....	55
Running a Query .....	66
Displaying Query Results .....	68
Baselining.....	69
Task Lists .....	70
Effective Trustees Functionality.....	73
Group Policy Objects (GPOs) Functionality.....	75

---

---

## Query-Related Features

bv-Control for Active Directory provides the following features to help administrators gather and manage their Active Directory environment:

- Building a query
- Saving a query
- Running a query
- Displaying query results
- Baselining
- Building a task list

---

## Understanding a Query

A query is a series of structured questions posed to obtain specific information about the Active Directory structure. The query results are returned in the form of a Grid, Chart, or Report that can be viewed on-screen or printed.

---

## Creating a Query

System administrators use various administrative tools, such as Active Directory Users and Computers, to monitor system, security and application issues. This task can be a difficult process depending on how much data you have to query.

By querying with bv-Control for Active Directory, administrators can centrally view objects without having to manually scan through Active Directory. Using the Query Builder process, administrators can create a report that is specific to the data sources and fields of the query.

---

## Query Building Process

Query Building is a tool used to create a query. To create a new query, you must select the appropriate data source, field specification, filter specification, sort specification, and the scope of the query. Once the specifications have been made, you can run the query. To accomplish this process, selections must be made from two dialogs: the Data Source dialog and the Query Builder dialog.

For more information on the Query Building process, refer to the *BindView RMS Console and Information Server v8.0 User Guide*.


---

## Defining a Query

The first step in defining a query is determining what information you want to gather about your Active Directory environment. When defining a query, you use the **Data Source** dialog and **Query Builder** dialog to specify the information you want and the manner in which you want it collected. The dialogs used to create a new

query are accessed from the **New Query**  icon on the BindView product toolbar.

► **To create a query**

- 1 From the BindView RMS Console, click the **New Query**  icon on the BindView product toolbar.

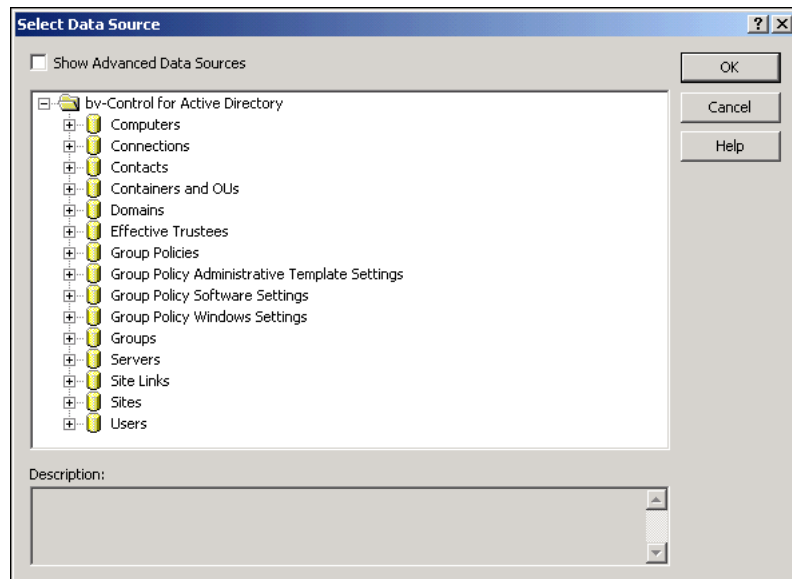
The **Select Data Source** dialog appears (Fig. 43).

---

**Note:** To view the Internal Data Source module, you must check the **Show Advanced Data Sources** option.

---

- 2 Click the plus (+) sign to expand the list of available data sources.

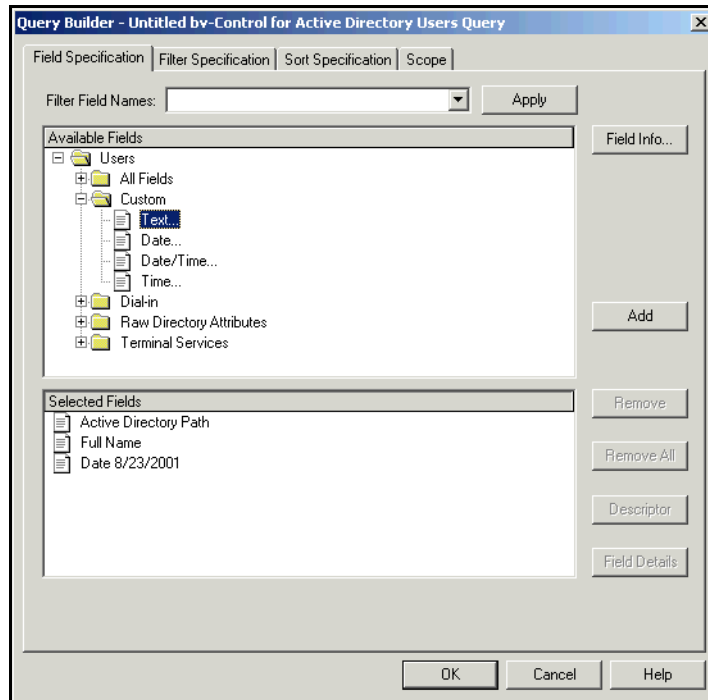


**Fig. 43** Select Data Source Dialog

- 3 Select the data source to be queried, and click **OK**.  
The **Query Builder** dialog appears (Fig. 44).

**Field Specification Tab**

The Query Builder dialog allows you to select the specific information you need to generate a query. By adding fields to a query, you define which fields of information bv-Control for Active Directory will collect when a query is executed.



**Fig. 44** Query Builder Dialog – Field Specification Tab

► **To add a field to a query**

- 4 On the **Field Specification** tab of the **Query Builder** dialog, select the desired field from the **Available Fields** list. Click **Add** or double-click the field.

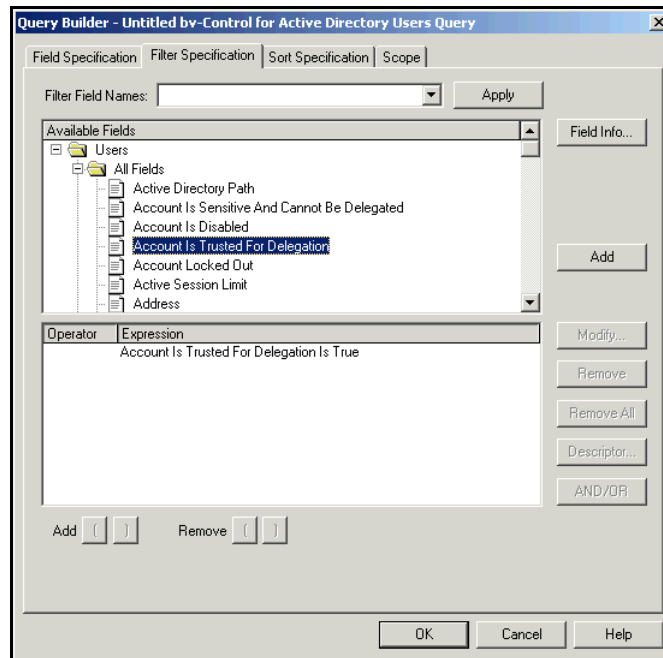
The fields you select will appear in the **Selected Fields** box. Fields appear in the dataset in the order they appear in the **Selected Fields** list. You change the field order by dragging fields to the desired position. You can also select multiple fields by pressing the Ctrl key and clicking on each field you want to select.



**Filter Specification Tab**

When defining a query to include a specific field or fields, bv-Control for Active Directory will examine every available occurrence of that field or fields. However, you can define a filter to instruct bv-Control for Active Directory not to display all occurrences. You can filter the fields by using the **Filter Specification** tab. Multiple filters can be grouped using the **Add** or **Remove** buttons, and further grouped through the use of parentheses.

For more information on filters, refer to the *BindView RMS Console and Information Server v8.00 User Guide*.

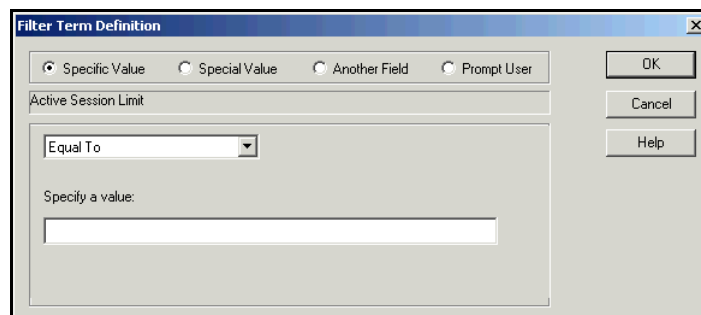


**Fig. 45** Filter Specification Tab

► **To define a filter**

- 5** Use the **Available Fields** list to select the field where you want to apply a filter.
- 6** Click **Add**.

The **Filter Term Definition** dialog appears.



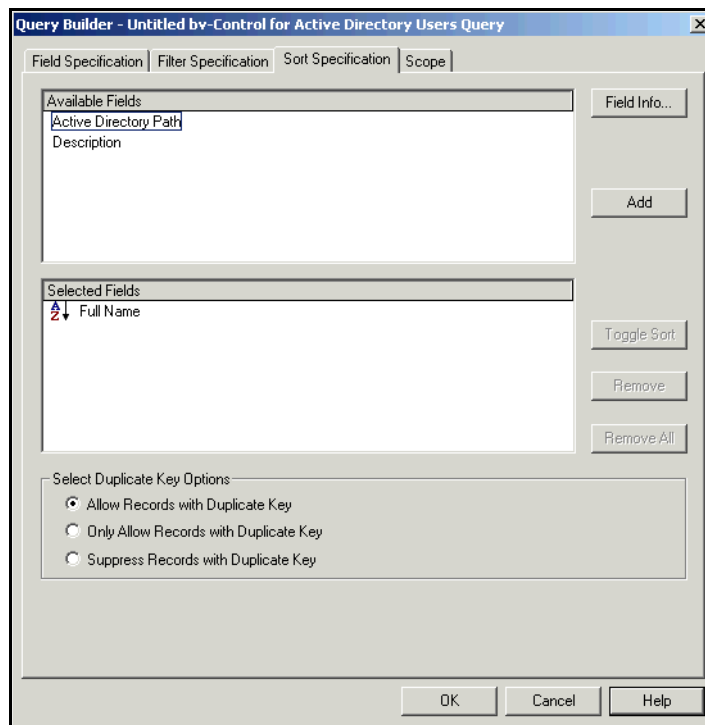
**Fig. 46** Filter Term Definition Dialog

- 7 Select the desired filter option. For more information on filter options, refer to the *BindView RMS Console and Information Server v8.00 User Guide*.
- 8 In the **Specify a value** text box, enter a specific value for the filter and click **OK**.

The **Query Builder** dialog reappears showing the filter that was just added, as shown in [Fig. 45 on page 49](#).

### **Sort Specification Tab**

The Sort Specification tab allows you to change the way information is sorted. Using the **Toggle Sort** button, a sort can be set to either ascending or descending order. Another feature is the ability to determine how the product will handle records with duplicate sort keys, by selecting an option button from the **Select Duplicate Key Options**.



**Fig. 47** Sort Specification Tab

- 9 From the **Sort Specification** tab, use the **Available Fields** list to apply a sort specification.
- 10 Highlight and **Add** the field to the **Selected Fields** list.
- 11 Click **OK** to save the order.

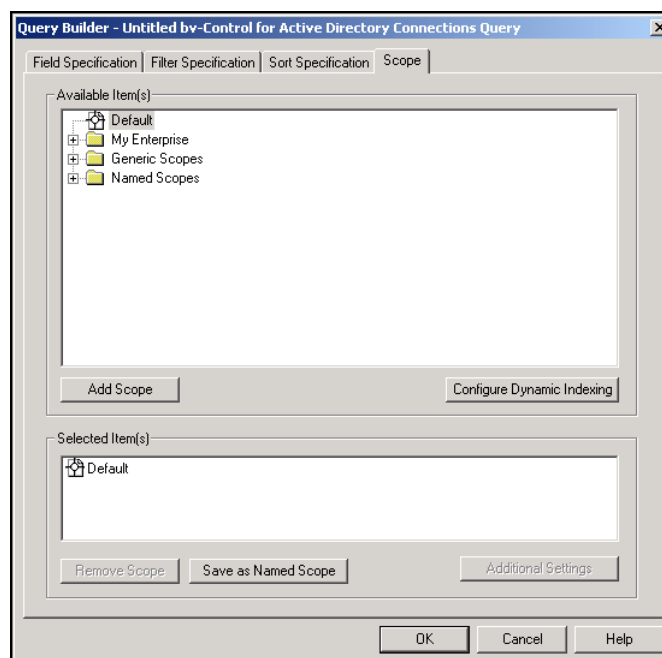
## Scope Tab

The last component of a query is Scope. Using the **Scope** tab, you can select the items you want to query, and limit the area of the report. This will reduce the amount of time it takes to receive query results.

A scope consists of user-selected scope items. Since the Information Server only queries the resource objects indicated by the scope, you can use scopes to significantly reduce the time it takes to retrieve a dataset.

The **Add Scope** button adds the resource object selected in the **Available Item(s)** box to the **Selected Item(s)** box and to the scope.

Using **Configure Dynamic Indexing** reduces the display time of the scope items on the Scope tab and quickly finds selected scope items.



**Fig. 48** Scope Tab

---

**Note:** The default scope is the contents of the current credential database.

---

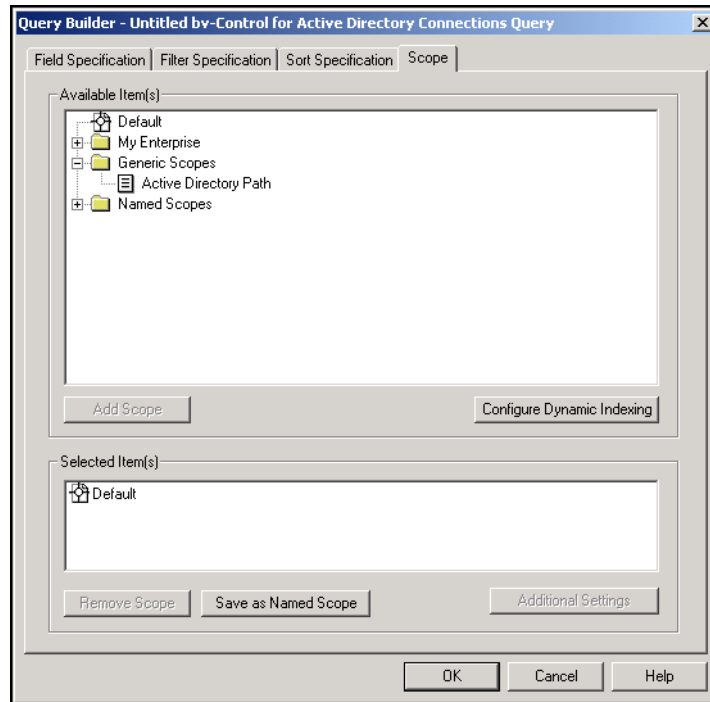
The **Scope** tab requires you to select a Named Scope. The Named Scope determines which files, folders, or servers the Query Builder will use to obtain information. You have a choice to either define and save a Named Scope or select from a previously saved Named Scope to query.

To select from a previously saved and existing Named Scope, see ["To select an existing Named Scope" on page 53](#).

► **To define a Named Scope**

- 1 On the Scope tab of the Query Builder dialog, expand the folders in the the **Available Item(s)** box to the area where

you want the query to begin its search and select the appropriate items.



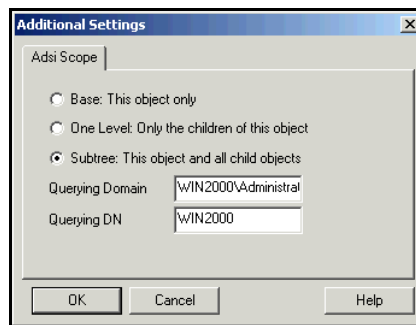
**Fig. 49** Scope Tab – Defining the Scope Area

- 2 Click **Add Scope**.

The **Additional Settings** dialog appears (Fig. 50).

### **Additional Settings**

Depending on which data source you selected, the **Additional Settings** dialog is displayed to give you additional advanced scope filter options.



**Fig. 50** Additional Settings Dialog – Adsi Scope Tab

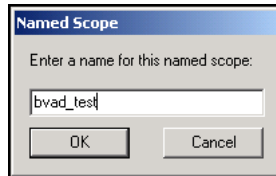
- 3 Select a level you would like to scope.
  - **Base** applies scoping to a selected folder.
  - **One Level** Only applies scoping to a selected folder and the contents of the selected folder.
  - **Subtree** applies scoping to a selected folder, sub-folders, and all items contained in the folders.

- 4 Click **OK**. The Query Builder dialog of the Scope tab reappears (Fig. 49). The Named Scope you added appears in the **Selected Item(s)** box.

► **To save the Named Scope**

- 5 From the **Selected Item(s)** box, select the Named Scope you want to save.
- 6 Click the **Save as Named Scope** button.

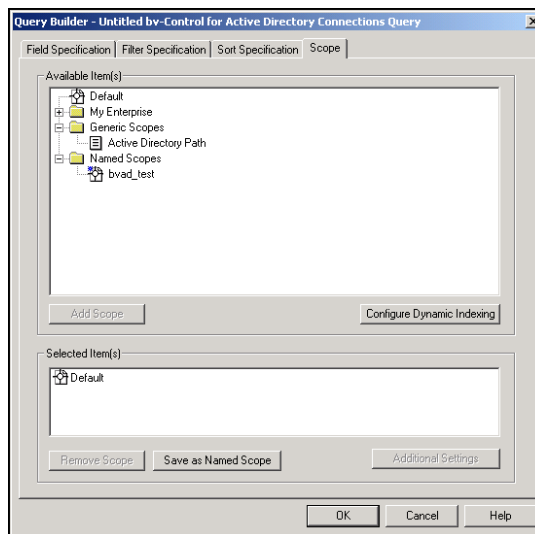
The **Named Scope** dialog appears.



**Fig. 51** Named Scope Dialog

- 7 Enter a name for the Named Scope.
- 8 Click **OK**.

The Named Scope is saved in the **Named Scopes** folder.



**Fig. 52** Named Scopes Folder

► **To select an existing Named Scope**

- 1 From the **Named Scopes** folder (Fig. 52), select the Named Scope you want to query.

The Named Scope you selected appears in the **Selected Item(s)** box.

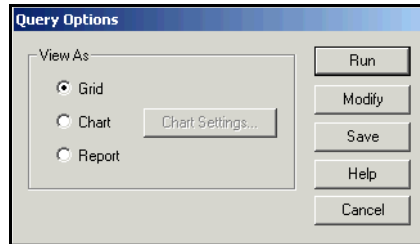
- 2 Click **OK**.

## Saving a Query Definition

A query's definition is referred to as the Query Binder by the BindView RMS Console. By default, the Query Binder file will be saved in the **My Items** folder, a subfolder found in the **Risk Assessment and Control** folder of the BindView RMS Console. If you wish to save your Query Binder in a different location, you may do so by browsing for the location and selecting it.

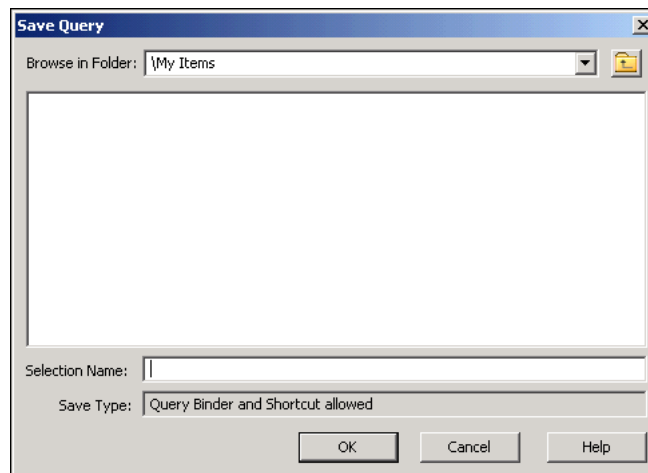
► **To save a New or Modified Query**

- 1 Choose the **Save** option when the **Query Options** dialog appears. Then click the **Save** button.



**Fig. 53** Query Options Dialog – Selecting a View As Option

The **Save Query** dialog appears (Fig. 54).



**Fig. 54** Save Query Dialog

- 2 Enter the name of your Query Binder in the **Selection Name** field and click **Save**.

The **Query Options** dialog reappears. Select a **View As** type option to run, modify, or save another query, or click **Cancel** to close this dialog.

## Multiple Forest Support

This feature allows you to report on different Windows® 2000 and Windows Server™ 2003 forests. You can install your BindView Information Server in one forest and report on that forest and other forests on your network without physically installing the BindView Information Server in other forests. You can also install the BindView Information Server on a Windows 2000 or Windows Server 2003 machine within an NT4 domain and report on other Windows 2000 and Windows Server 2003 forests on your network.

## Requirements

Multiple forest support relies on your DNS configuration. The DNS must be configured properly and the BindView Information Server must be installed on the machine where the DNS name resolution is working properly. The Global Catalog server and at least one Domain Controller in the domain must be reachable from the BindView Information Server.


Three options for using the multi-forest feature are:

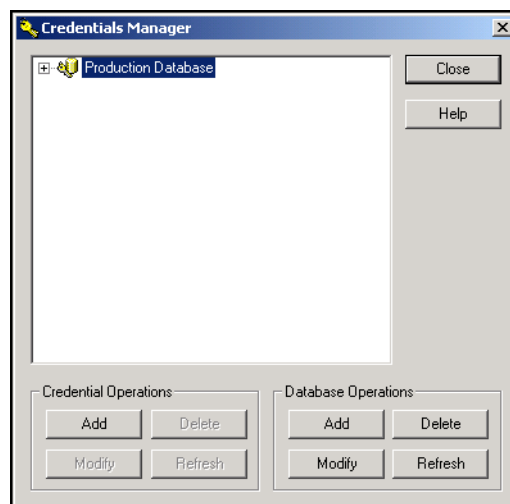
- Specify Credentials
- Microsoft Network
- Enterprise Directories

The option you choose depends on your network configuration.

### ► **Using Specify Credentials**

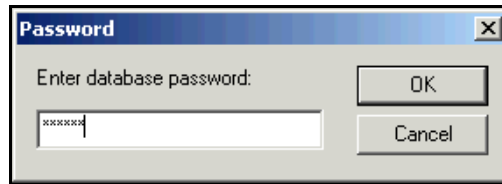
This feature allows you to enter credentials for the domains that are not seen in the Microsoft Network folder. The Specify Credentials option assumes that the domain can be reached from your BindView Information Server. This feature requires the DNS name of the domain that you want to use.

- 1 In the BindView RMS Configuration folder, open the **Credentials Manager**  icon in the details pane.



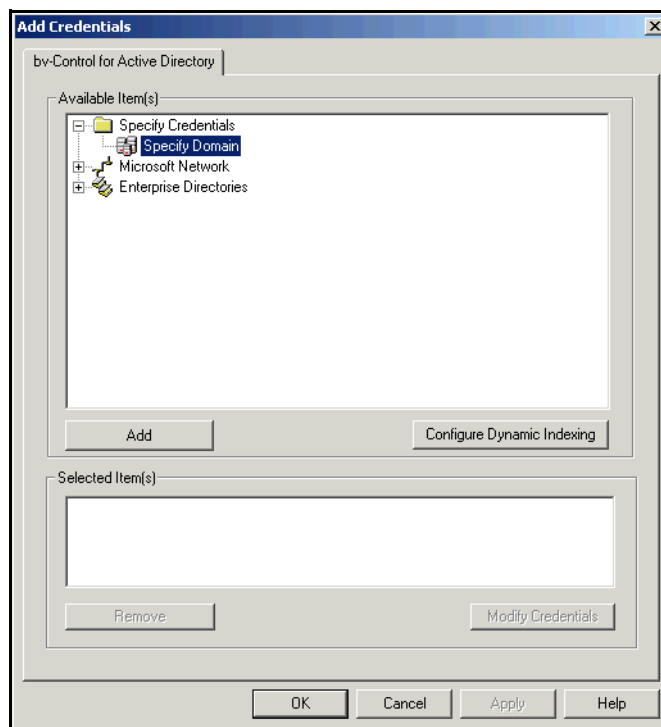
**Fig. 55** Credentials Manager Dialog

- 2 Click **Add** under Credential Operations.  
The password prompt appears.



**Fig. 56** Password Dialog

- 3 Enter the database password and click **OK**.  
The **Add Credentials** dialog appears.

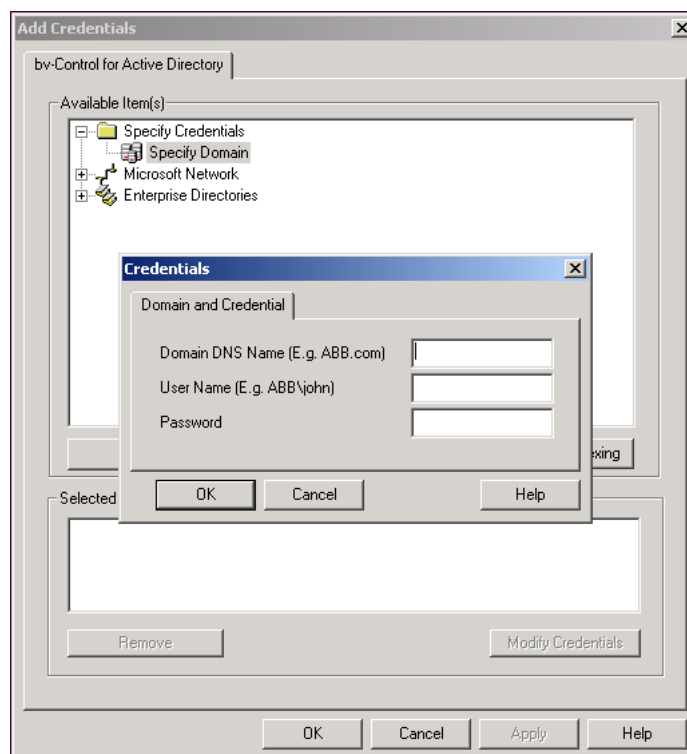


**Fig. 57** Add Credentials Dialog

- 4 Double-click **Specify Credentials** or click the **Add** button to open the Specify Domain.



- 5 Double-click Specify Domain. The **Domain and Credential** tab will open in the Credentials dialog.



**Fig. 58** Domain and Credential Tab Dialog

- 6 Enter the Domain DNS Name, Domain Name\User Name, and Password.

The domain name\user name may be entered by either using a backslash \ to separate domain name and user name. For example,

WIN2000\Administrator

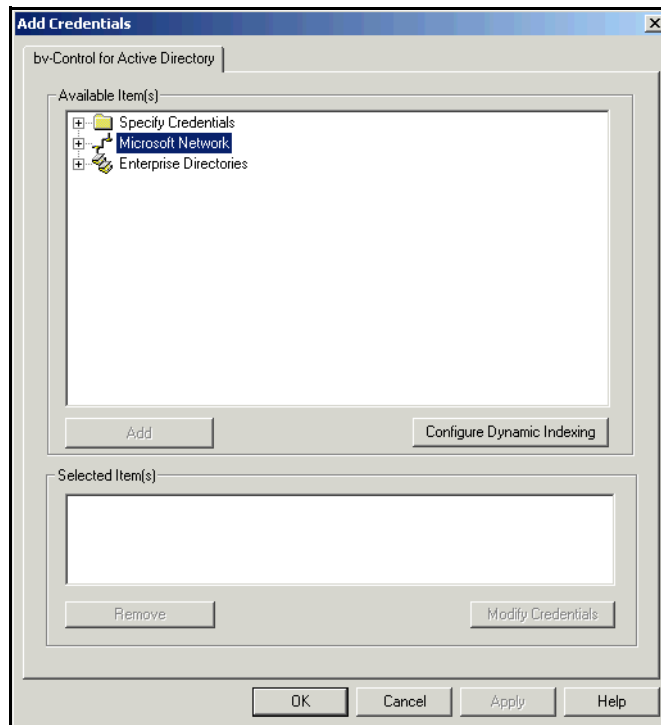
- 7 Click **OK**.

The added credential will be listed as a Generic Credential under Selected Item(s).

► **Using Microsoft Network**

Use this option to select available domains listed in your Microsoft Windows network or Network Neighborhood. This typically is the list of domains seen by your network browser.

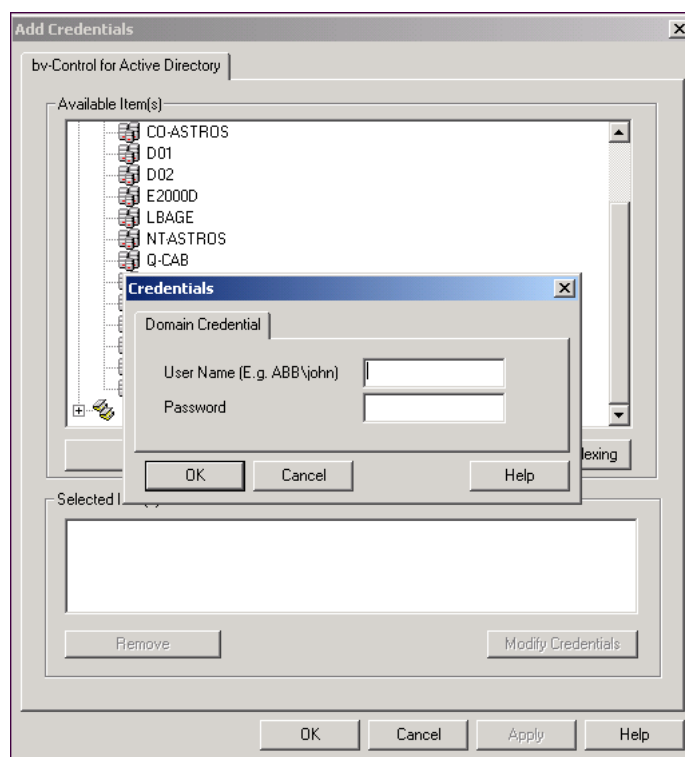
- 1 Follow steps 1 through 3 in “Using Specify Credentials” on page 55.
- 2 Double-click Microsoft Network when the Add Credentials dialog is open.



**Fig. 59** Add Credentials Dialog With Microsoft Network Selected

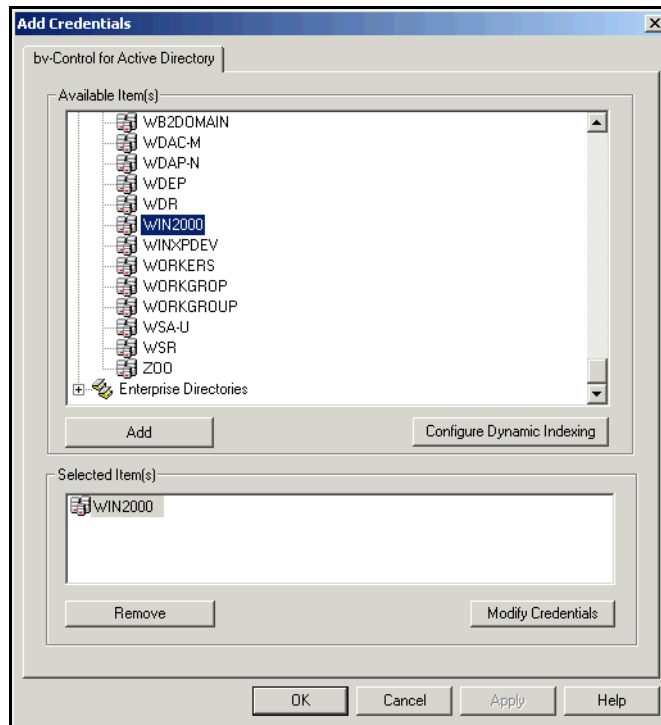
The list of available domains within the Microsoft Network appear in the Available Item(s) panel.

- 3 Double-click on a domain from the Available Item(s) to open the Credentials dialog.



**Fig. 60** Domain Credential Dialog

- 4 Enter the Domain Name\User Name and Password.  
The domain name\user name may be entered by either using a backslash \ to separate domain name and user name. For example,  
`WIN2000\Administrator`
- 5 Click **OK** in the Credentials dialog. The credential is added under Selected Item(s).



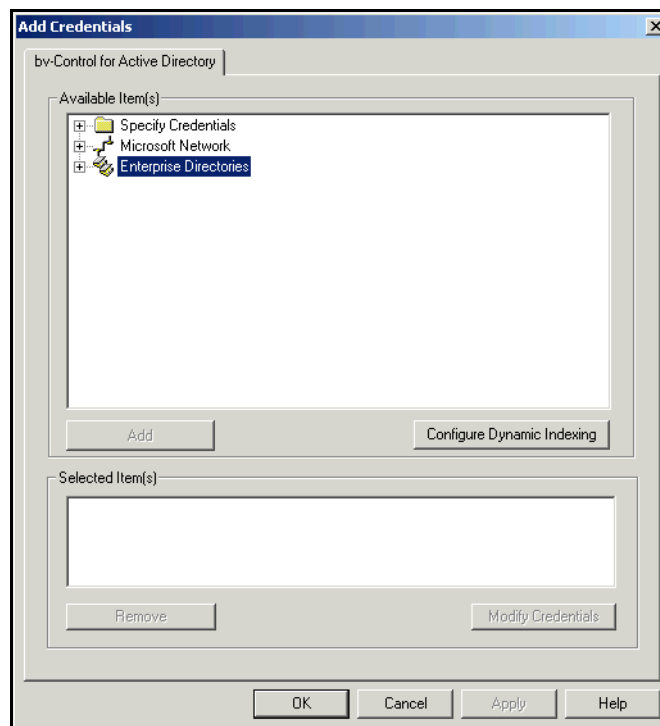
**Fig. 61** Add Credentials Dialog – Complete

- 6 Click **OK** to close this dialog.

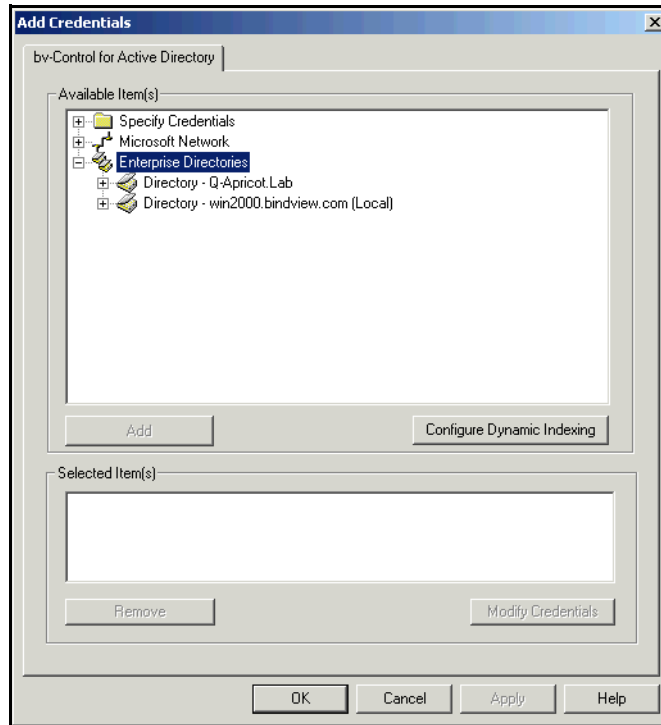
► **Using Enterprise Directories**

This feature allows you to select a domain from your forest domain tree. This tree is created using the information entered in the credential database. It does not automatically browse your network to find all the forests. By default, your local or native forest will be seen. If you added another domain that resides in a different forest, the additional forest will be seen.

- 1 Follow steps 1 through 3 in ["Using Specify Credentials" on page 55](#).
- 2 Double-click on Enterprise Directories to open the available directories from the Available Item(s).

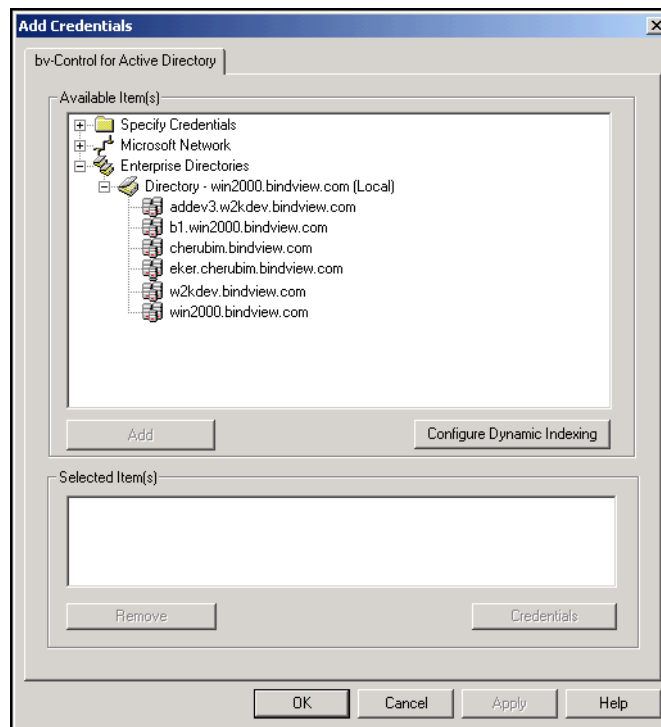


**Fig. 62** Add Credentials Dialog With Enterprise Directories



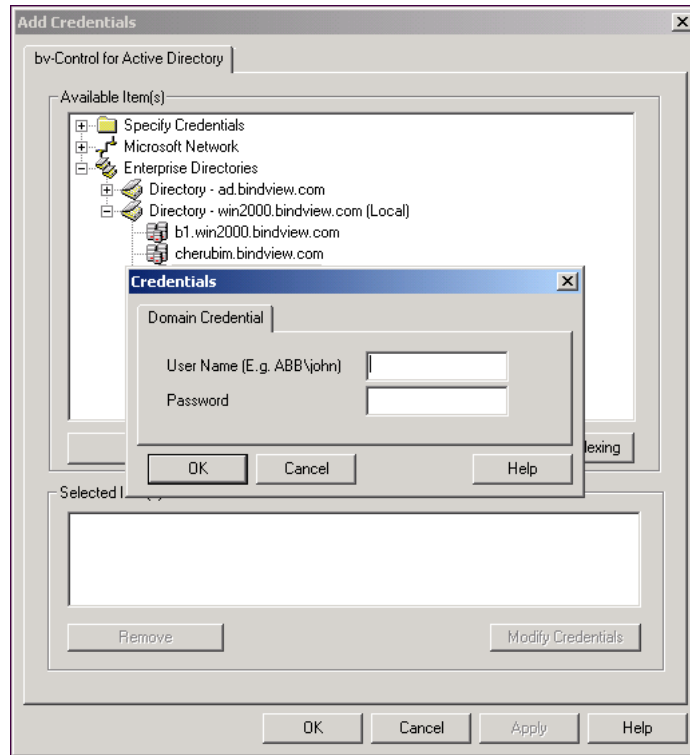
**Fig. 63** Add Credentials Dialog – Directories

- 3 Double-click on a directory to open the available domains (Fig. 64).



**Fig. 64** Add Credentials Dialog – Available Domains

- 4 Double-click on a domain, or select a domain and click **Add** to open the Domain Credential tab of the Credentials dialog.



**Fig. 65** Credentials Dialog

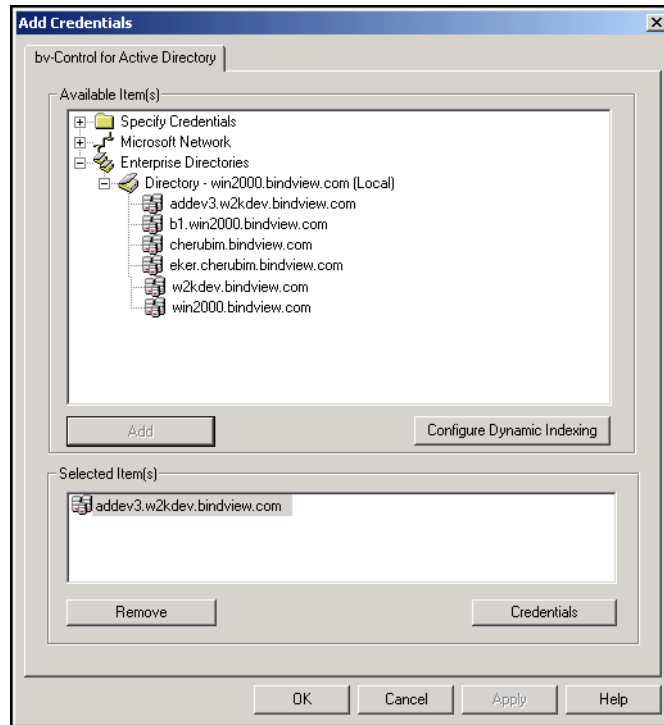
- 5 Enter the Domain Name\User Name and Password. The user name is "sAMAccountName", which is the user logon name format.

---

**Note:** The sAMAccountName property is a single-valued property that is the logon name used to support clients and servers from a previous version of Windows (such as Windows NT 4.0 and earlier, Windows 95, Windows 98, and LAN Manager).

---

- 6 Click **OK** in the Credentials dialog.  
The credential is added under Selected Item(s).



**Fig. 66** Add Credentials Dialog – Complete

7 Click **OK** to close this dialog.

### ► **Using Configured Forests**

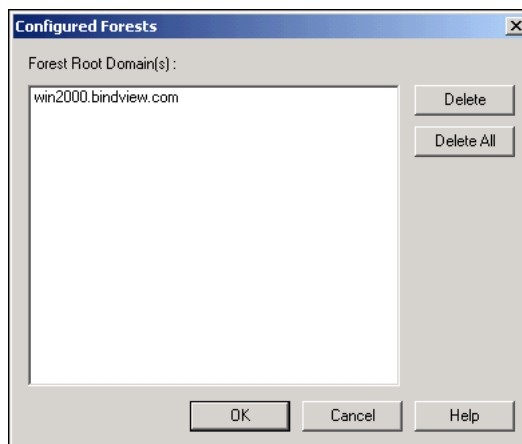
This is the list of forests that bv-Control for Active Directory will display in the **Enterprise Directories** folder in the **Credential Manager** dialog. This list is generated as you continue entering the credentials for different domains in your credential database. Every new domain added to the credential database is verified and its forest information is recorded in **Configured Forests**. This domain need not always be the root of your forest. Any child domain will also cause the forest information to be entered in this folder.

Removing the credentials from the credential database does not remove the recorded forest information and it will continue to appear in the Enterprise Directories.

To stop a forest from being displayed in the Enterprise Directories, you must delete it from the Configured Forests folder.

- 1 In the details pane of the bv-Control for Active Directory Configuration folder in the BindView RMS Console, open the **Configured Forests** folder.





**Fig. 67** Configured Forests


- 2 Select the forest you want to delete and click **Delete**. If you wish to delete all forests, click **Delete All**.
- 3 To complete the delete process, click **OK**. The selected forest is deleted and the **Configured Forests** dialog closes.


If you wish to cancel the delete process, click **Cancel**. The **Configured Forests** dialog closes but when it is reopened, the forest you previously selected to delete remains in the list.

### **Credential Verification**

After you enter the credentials, bv-Control for Active Directory verifies the credentials before they can be used to run a query. This verification process does not verify the account password. It only verifies that the account name exists in the domain.

The **Refresh** button in the **Credentials Manager** dialog can be used to update the account properties if the user is moved between domains in a forest. The bv-Control for Active Directory product indicates the verification results by displaying the appropriate icon

for that credential. A credential with a question mark  icon indicates that the account could not be verified. The bv-Control for Active Directory product can use this credential to run a query on objects in the specified domain. A credential with a red line across


the  icon indicates that the account is invalid and that the bv-Control for Active Directory product will not use this account to run a query. A credential without any such overlays indicates that the account was verified and can be tracked.

---

**Note:** The credential verification process does not use the password entered in the credentials. This process uses the BindView Information Server security context.

---

If your remote domain or forest does not grant anonymous access rights to the domain object, the credential verification will not

succeed. You will see a question mark  icon in the credential entry. This means that there is no certainty of the accuracy of the account name entered.

---

## Running a Query

When you run a query, the settings you defined in your query definition are polled for the information you requested. The results are returned in the selected view type: Grid, Chart, or Report.

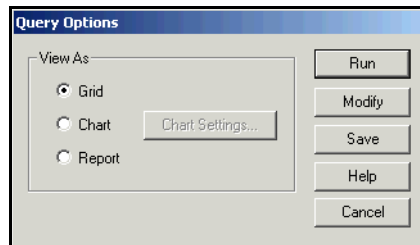
Queries can be launched from two places:

- A new **Query Options** dialog
- An existing Query Binder

The **Query Options** dialog appears after you click **OK** on the **Query Builder** dialog. The following is an example of a query being run from the **Query Options** dialog. For detailed information on how to run a query from an existing Query Binder, refer to the *BindView RMS Console and Information Server v8.0 User Guide*.

► **To run a query**

- 1 In the **View As** option box of the **Query Options** dialog, select the view type you want for the query results.



**Fig. 68** Query Options Dialog


- 2 Click **Run** to execute the query.

The results of the query will be displayed in the view type you selected: Grid, Chart, or Report.

---

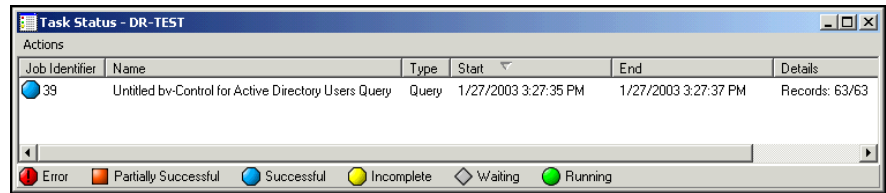
## Task Status Monitoring

The **Task Status** message, shown in [Fig. 69](#), offers you a quick and easy way to monitor and manage your tasks while they are running. The **Task Status** message displays the status of Error, Successful, Incomplete, Waiting, or Running.

The **Task Status** message can be accessed by clicking on the **Task Status**  icon.

For example, while waiting for your query results, you may want to open the **Task Status** message to view the status of your query.

The message will tell you if the query is still processing, or if it did not process due to an error (see Fig. 69).



**Fig. 69** Task Status Message

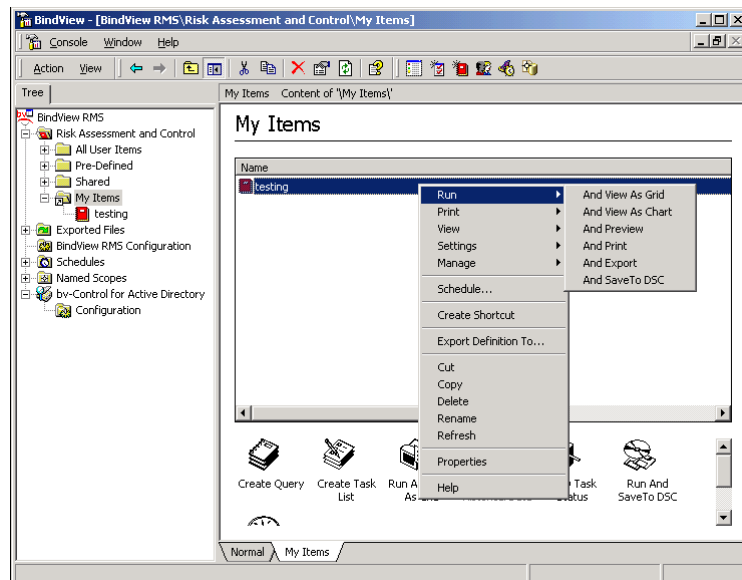
The lower end of the **Task Status** message displays an example of each task status symbol and its meaning.

### Accessing a Previously Saved Query

bv-Control for Active Directory provides a comprehensive reporting capability, which allows the administrator to view a previously saved query for purposes such as trend analysis and capacity planning. During the query definition process, you have the option to create and save a Query Binder. A Query Binder contains the query's definition. By default, the Query Binder files are saved in the BindView RMS under the Risk Assessment and Control folder. Click the **My Items** subfolder to locate queries that have been saved.

► **To access a previously saved query**

- 1 From the BindView RMS Console container, open the **Risk Assessment and Control** folder.



**Fig. 70** MMC User Interface – Accessing the Query Binder

- 2 To view all previously saved queries, open the **My Items** subfolder.

- 3 Highlight and right-click on the query you want to access.
- 4 From the **Run** option list, select the **And View as** type option to run the query. You can choose to view the results in the Grid or Chart format.

## Displaying Query Results

The results obtained from the query will be displayed in the format that you selected as the **View As** option. These formats are Grid, Chart, or Report. An example of the results displayed in a Grid format is shown in [Fig. 71](#).

	Domain Name	Active Directory Path
1	qad-england	LDAP://qad-england.lab/DC=qad-england,DC=lab
2	qad-france	LDAP://qad-france.qad-england.lab/DC=qad-france,DC=qad-england,DC=lab
3	qad-germany	LDAP://qad-germany.qad-england.lab/DC=qad-germany,DC=qad-england,DC=lab
4	qad-portugal	LDAP://qad-portugal.qad-england.lab/DC=qad-portugal,DC=qad-england,DC=lab
5	qad-spain	LDAP://qad-spain.qad-england.lab/DC=qad-spain,DC=qad-england,DC=lab

**Fig. 71** Grid Results

**Note:** After running a query, always check for messages that have been returned with the query results. Click the Messages button at the lower right side of the results window. View any messages in this window.

### Grid

A grid is a tool used to analyze and display information about resources in your Active Directory environment, displayed in the form of a spreadsheet interface. The grid toolbar ([Fig. 71](#)), also includes options to create charts and print reports of your query results.

### Chart

A chart displays the results of a query in a graphic format (column, pie, or histogram). Charts are created and modified using the Chart Builder Wizard. The wizard guides you through the process of building a custom chart for your query. During the building process, you will have the option to determine the type of chart you want to build, and how you want your chart to be labeled.

For complete instructions on how to build a chart using the Chart Building Wizard, refer to the *BindView RMS Console and Information Server v8.00 User Guide*.

There are two basic types of chart style:

- Series Chart, which displays the relative values for each record depicted on the chart, using column or pie style.
- Histogram Chart, which displays the record frequencies for a single field in a dataset.

For more complete information on how to create the different chart styles, refer to the *BindView RMS Console and Information Server v8.00 User Guide*.

---

## Report

The reporting feature allows you to create a variety of customized reports for your query results, and to print a report of the data results from your query. The appearance of your report is dictated by the print settings defined on the **Print Setup** dialog.

The BindView RMS Console is installed with default settings. If you wish to customize the default settings, you can do so from the Global Print Setup item in the Console Setup folder.

For more information about the print settings, refer to the *BindView RMS Console and Information Server v8.00 User Guide*.

---

## Baselining

Another key feature that bv-Control for Active Directory provides to assist administrators is *baselining*. Baselining is a comparison of two historical datasets from the Query Binder. Baselining can help administrators perform risk management by allowing them to view exceptions and monitor changes in the Active Directory environment. Administrators can then analyze the differences to determine how the Active Directory environment has changed over a particular time period.

You can baseline any two historical datasets in a query binder. You can also select the type of records that you want compared between the two historical datasets.

---

## Creating a Baseline

Before running a baseline, you must select any two historical datasets for a selected query binder to compare.

- ▶ **To create a baseline**
  - 1 Select the query binder that contains the historical datasets you want to baseline.
  - 2 Right-click on the query binder to display the shortcut menu.
  - 3 From the **Manage** option select **Historical Data** options.  
The **Manage Historical Data** dialog appears.
  - 4 Select two historical datasets you want to baseline from the list. Click the **Run Baseline** button.  
The **Baseline Options** dialog appears.
  - 5 Select the record types to be included in the baseline.

- 6 Click **OK** to run the baseline.

For more complete information on the functionality of baselining, refer to the *BindView RMS Console and Information Server v8.00 User Guide*.

---

## Task Lists

bv-Control for Active Directory provides a task list capability to help you administer your Active Directory environment by allowing you to organize and run multiple tasks as a single task unit. When you run the task list file, all of the queries and baselines defined in the file will automatically run.

A task list is an organized collection of individual tasks which can be managed and run as a single unit. A task list file can contain the following items:

- Query tasks
- Baseline tasks
- Post process commands for added tasks
- Summary file commands


For detailed information on each individual item listed above, refer to the *BindView RMS Console and Information Server v8.00 User Guide*.

---

## Building Task Lists

Task Lists are created from the **Task List** dialog. The following steps explain how to create and run a task list.

► **To create a new task list**

- 1 From the product toolbar, click on the **New Task List**  icon.  
The **Task List** message will appear.
- 2 Click **Add**.  
The **Select a Task Type** message will appear.
- 3 Select the baseline or query you want to add to the task list.

For detailed steps on how to add a baseline or query to a task list, refer to the *BindView RMS Console and Information Server v8.00 User Guide*.

- 4 Click **Add**.  
The **Task List** message reappears after you have created the task list.

► **To run a new task list**

- 5 From the **Task List** message, click **Run Task List**.
- 6 Close the **Task List** message.

To monitor the progress of the task list as it runs, open the **Task Status** dialog.

For more complete information on how to create or modify a task list, refer to the *BindView RMS Console and Information Server v8.00 User Guide*.

## Generating a Field List

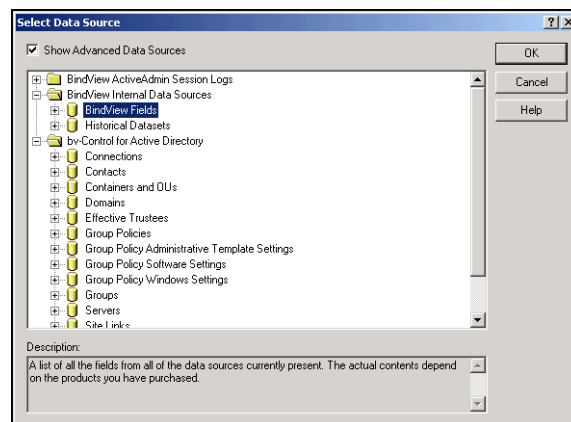
The first requirement for reporting on a specific area in your Active Directory is to know what fields are available to filter when running a query. bv-Control for Active Directory offers a quick way to gather a list of all available fields.

### ► To generate a field list

- 1 From the BindView RMS Console toolbar, click the **New Query**



- 2 Select the **Show Advanced Data Sources** option.

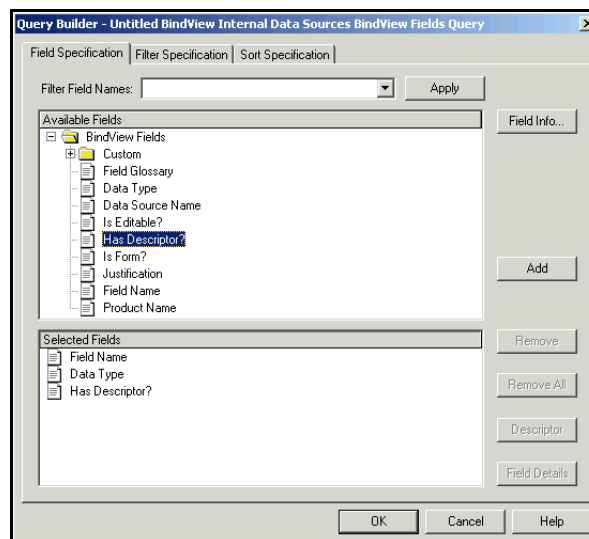


**Fig. 72** Show Advanced Data Sources Option

- 3 Double-click the **BindView Internal Data Sources** folder.

- 4 Highlight the **BindView Fields** data source, and click **OK**.

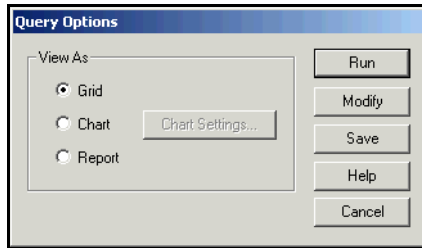
The **Query Builder** dialog appears, as shown in [Fig. 73](#).



**Fig. 73** BindView Fields List

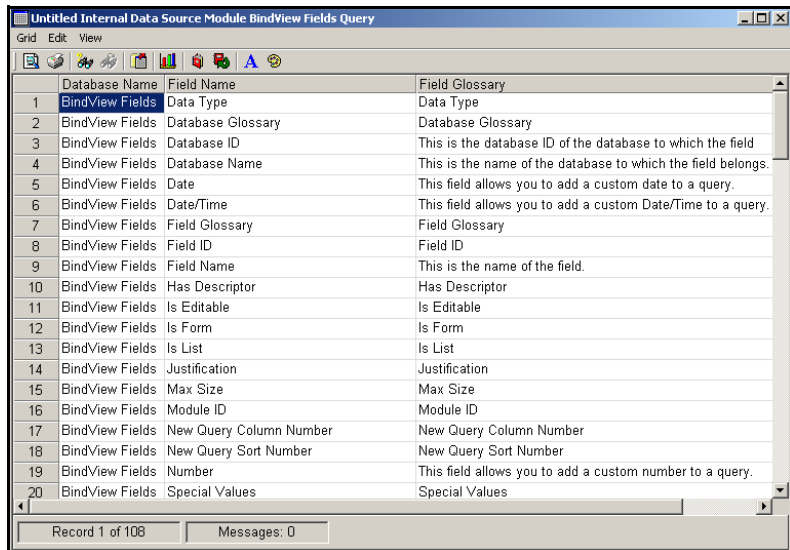
- 5 Double-click on a field from the **Available Fields** box to cause the field to appear in the **Selected Fields** box (Fig. 73).
- 6 Click **OK**.

The **Query Options** dialog appears.



**Fig. 74** Query Options Dialog

- 7 Select the type of view (grid, chart, or report) and click **Run** to launch the query.



**Fig. 75** Results of a Generated Field List

- **Database Name** - Displays the name of the Data Source in the query.
- **Field Name** - Displays the fields associated with the data source.
- **Field Glossary** - Displays the definition of that particular field.



## Effective Trustees Functionality

The Effective Trustee field indicates whether a security principal gains the specified permissions on the specified Active Directory object. The permissions and the Active Directory object should be specified in the descriptor of this field. The security principal(s) should be specified through the scope. The 'Default' scope of this query will scan all the security principals in the domains available in the credential database.

### Available Permissions

The following permissions are supported in the descriptor.

- **Create, delete, and manage user accounts** - Same as the permissions delegated by the task "Create, delete and manage user accounts" on an OU object through the Delegation of Control wizard of the Active Directory Users and Computers snap-in. This is the permission to create, delete, and manage user accounts in the specified object and all of its container child objects.
- **Reset user passwords and force password change at next logon (Windows 2003)** - Same as the permissions delegated by the task "Reset user passwords" on an OU object through the Delegation of Control wizard of the Active Directory Users and Computers snap-in. This is the permission to reset passwords and force password change on next logon of user accounts in the specified object and all of its container child objects.
- **Read All User Information** - Same as the permissions delegated by the task "Reset All User Information" on an OU object through the Delegation of Control wizard of the Active Directory Users and Computers snap-in. This is the permission to read all information of user accounts in the specified object and all of its container child objects.
- **Create, Delete and Manage groups** - Same as the permissions delegated by the task "Create, delete and manage group accounts" on an OU object through the Delegation of Control wizard of the Active Directory Users and Computers snap-in. This is the permission to create, delete, and manage group accounts in the specified object and all of its container child objects.
- **Modify the membership of a group** - Same as the permissions delegated by the task "Modify the membership of a group" on an OU object through the Delegation of Control wizard of the Active Directory Users and Computers snap-in. This is the permission to modify the membership of group accounts in the specified object and all of its container child objects.
- **Manage Group Policy Links** - Same as the permissions delegated by the task "Manage Group Policy Links" on an OU object through the Delegation of Control wizard of the Active Directory Users and Computers snap-in. This is the permission to manage group policy links of container, OUs and sites in the specified object and all of its container child objects.
- **Generate Resultant Set of Policy (Planning) (Windows 2003)** - Same as the permissions delegated by the task "Generate Resultant Set of Policy (Planning)" on an OU object through the Delegation of Control wizard of the Active Directory

Users and Computers snap-in. This is the permission to manage group policy links of container, OUs and sites in the specified object and all of its container child objects.

- **Generate Resultant Set of Policy (Logging) (Windows 2003)** - Same as the permissions delegated by the task "Generate Resultant Set of Policy (Logging)" on an OU object through the Delegation of Control wizard of the Active Directory Users and Computers snap-in. This is the permission to create, delete, and manage user accounts in the specified object and all of its container child objects.
- **Create, delete and manage inetOrgPerson accounts (Windows 2003)** - Same as the permissions delegated by the task "Create, delete and manage inetOrgPerson accounts" on an OU object through the Delegation of Control wizard of the Active Directory Users and Computers snap-in. This is the permission to create, delete, and manage inetOrgPerson accounts in the specified object and all of its container child objects.
- **Reset inetOrgPerson passwords and force password change at next logon (Windows 2003)** - Same as the permissions delegated by the task "Reset inetOrgPerson passwords and force password change at next logon" on an OU object through the Delegation of Control wizard of the Active Directory Users and Computers snap-in. This is the permission to reset passwords and force password change on next logon of inetOrgPerson accounts in the specified object and all of its container child objects.
- **Read All inetOrgPerson Information (Windows 2003)** - Same as the permissions delegated by the task "Reset All inetOrgPerson Information" on an OU object through the Delegation of Control wizard of the Active Directory Users and Computers snap-in. This is the permission to read all information of inetOrgPerson accounts in the specified object and all of its container child objects.

---

## Credential Requirements

The accuracy of the result of the 'Is Effective Trustee?' field depends on the availability of credentials for the domains of the security principals or of the members of the groups that have been assigned permissions on the selected Active Directory object. If credentials are not available for a security principal's domains, then that security principal will not be considered while calculating the effective trustees.

- The credential database should have credentials for searching the Global Catalog of the forest hosting the selected object.
- If the object DACL includes ACEs that grant or deny the permissions for security principal(s) in any trusted domains in a different forest then credentials for all such domains must be entered in the credential database.
- If the object DACL includes ACEs that grant or deny the permissions to the security principals which have been migrated to other domain(s) and if such domains are trusted by the domain

hosting the object, then the credentials for all such domains are required to calculate the effective trustees.

The responsiveness of the 'Is Effective Trustee?' field is dependent on the complexity of the permissions assigned on the specified Active Directory object and the nesting and hierarchy of the members of the group(s) that have been assigned these permissions. Since all possible combinations of the assigned permissions and the assigned trustees are considered for calculating the effective trustees, the query with the 'Is Effective Trustee?' field is time intensive.

---

## Limitations

- Only domain, OU, or container objects can be selected for reporting the effective trustees.
- Memberships of the Logon-related, well-known pseudo groups such as Everyone, Network, etc., are not considered. You can include these well-known security principals in the scope and the query will include them in the final result.
- Windows NT 4.0 or earlier system domains are not supported.

---

## Group Policy Objects (GPOs) Functionality

A Group Policy Object (GPO) is a collection of policies that are included within an Active Directory container, domain, group, organizational unit (OU), or user. In Active Directory, GPOs define user and computer settings for groups of user and computers in a domain, site or organizational unit (OU).

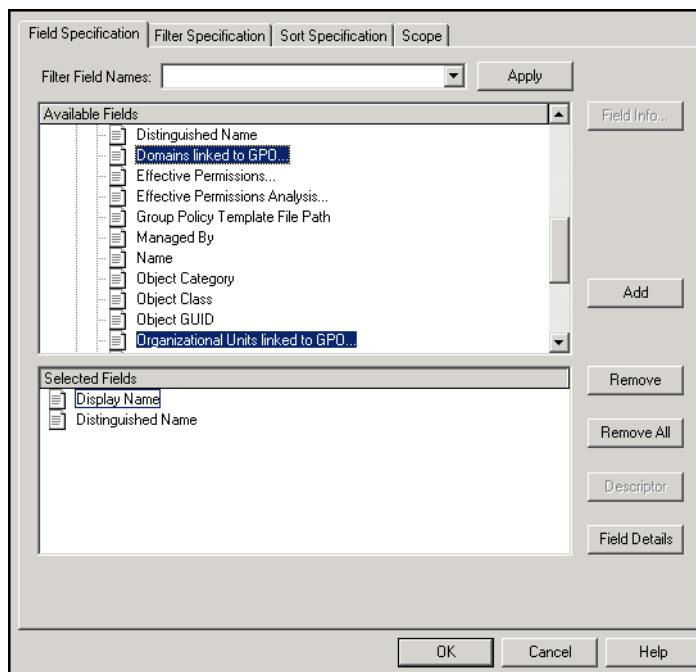
Group Policies define the various components of the user's environment that system administrators need to manage, and include software settings, application deployment options, scripts, user desktop and document folder settings, and security settings. Group Policy includes registry-based policies found in Windows NT Server 4.0, as well as policies enabled by Directory Services to store various types of policy data.

A Policy is applied when the computer starts up and the user logs on. When a user starts up the computer, the system applies the computer policy. When a user logs on interactively, the system loads the user's profile, then applies the user policy. The Policy can be optionally reapplied on a periodic basis.

---

## Descriptor: <Available Fields to Group Policies> Dialog

In the Group Policies data source in the All Fields folder there are three Available Fields where you can change the descriptor by clicking the Change Descriptor button.



**Fig. 76** Field Specification Tab for Group Policies

The three Available Fields are:

- Domains linked to GPO - Returns a list of domains to which the group policy object is applied.
- Organizational Units linked to GPO - Returns a list of organizational units to which the group policy object is applied.
- Sites linked to GPO - Returns a list of sites to which the group policy object is applied.

The above three fields are used to select a credential for the Sites, Domains, or Organization Units to which the Group Policy object is applied. All unique user names in a currently assigned credential database will appear in the Available Item(s) list.

---

# 4

## Advanced Use Scenarios

---

### In This Chapter

Introduction.....	78
Scenario 1: Reporting on Multiple Forests .....	78
Scenario 2: Verifying Credentials Across Forests .....	79
Scenario 3: Using Generic Scopes .....	84

---

## Introduction

This chapter contains different scenarios for advanced usage of the bv-Control for Active Directory product in the following circumstances:


- Reporting on multiple forests
- Verifying credentials across forests
- Using generic scopes

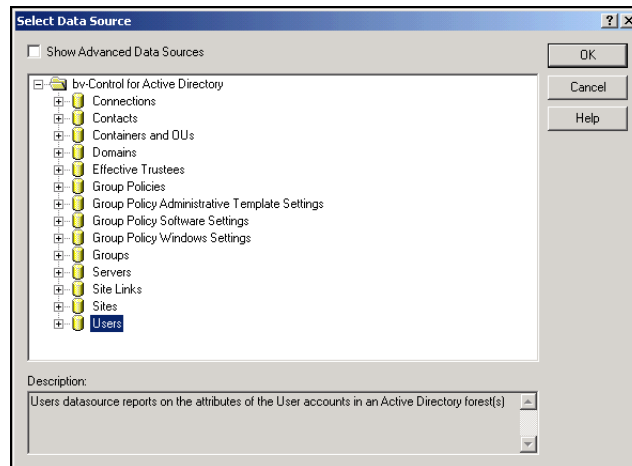
## Scenario 1: Reporting on Multiple Forests

With bv-Control for Active Directory you can report on multiple forests. You don't need a BindView Information Server in every forest and you don't need any trusts between the forests. You can also install the BindView Information Server on a Windows 2000 machine within an NT4 domain and report on other Windows 2000 forests on your network.

Multiple forests support relies on your Domain Naming Service (DNS) configuration. The DNS must be configured properly and the BindView Information Server must be installed on the machine where the DNS name resolution is working properly.

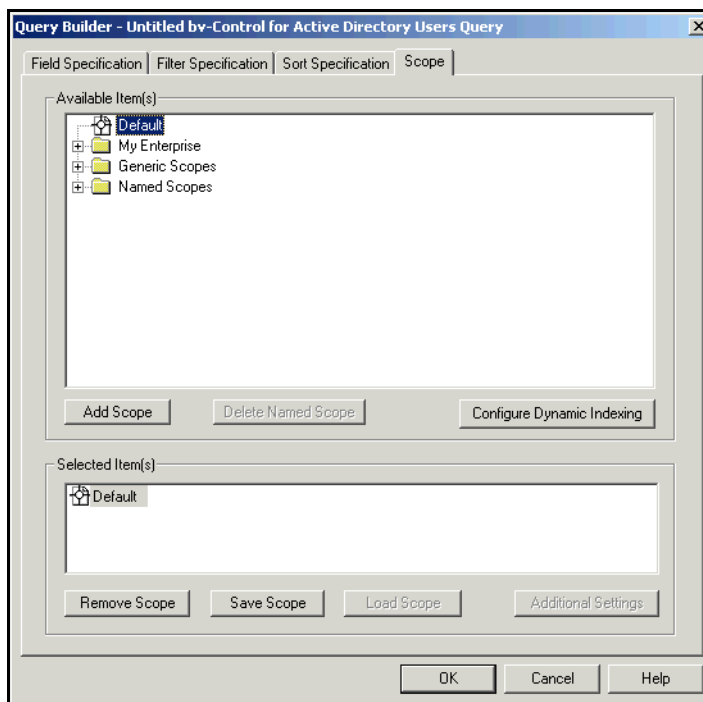
Enter the credentials for the Windows domain that you want to report on.

- 1 From the BindView RMS Console, click the **New Query**  icon on the BindView product toolbar. The **Select Data Source** dialog appears.



**Fig. 77** Select Data Source Dialog

- 2 Double-click on a data source.  
The Query Builder dialog appears.



**Fig. 78** Query Builder Dialog – Scope Tab

**3** Click the Scope tab.

The default scope of a query includes all the domains listed in your credentials database. You can expand the domains to see a list of Containers and OUs in the domain and select an item to scope. See ["Running a Query" on page 66](#) for more information.

You can also use pre-defined reports with multiple forests. Right-click a report and select Settings. Change the scope to use required domains or Containers/OUs.


## Scenario 2: Verifying Credentials Across Forests

The BindView RMS Console and bv-Control for Active Directory validate credentials as they are entered into the credential database. This feature allows you to synchronize the changes in the user accounts, such as user rename, user move, and other processes. This verification may not work if you are entering the credentials for a domain that is not a part of your current forest. Within the bv-Control for Active Directory product, queries are executed on the BindView Information Server machine. For internal operations the product uses the security context of BindView Job Processor. By default, this process runs under the Local System account.

If you have entered the credentials for a domain that is not a part of the forest in which your BindView Information Server is installed, then it may not always be possible to validate the account name entered in the credentials. The security settings on the remote

domain/forest (outside of your current forest) determine the success of this validation.

These queries running under the Local System account and that access any domain that does not have trust with the current domain are seen as Anonymous queries by the remote domain. By default, Active Directory grants anonymous access permissions on the domain/forest and verification will succeed. If these are turned off, the query to that domain/forest does not succeed. The credential is

still accepted but is flagged as an unknown credential  icon.

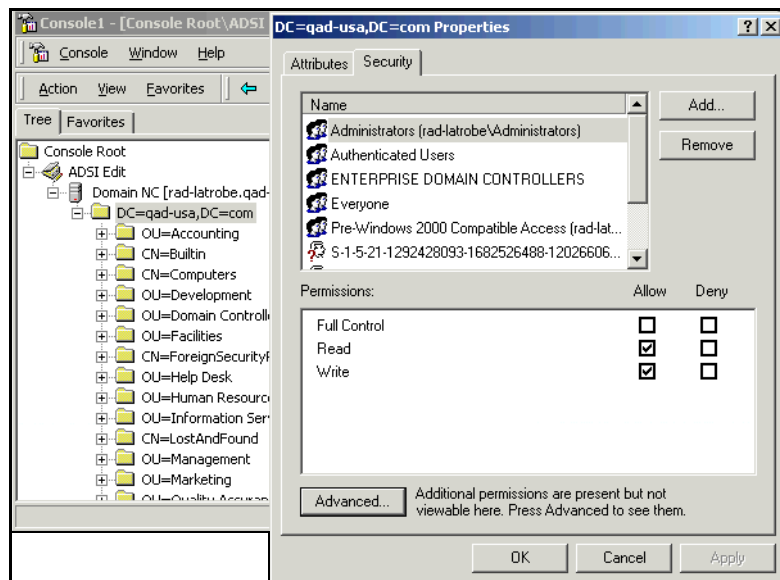
If you want the credential to be verified you have to make changes to the security settings of the remote domain/forest.

► **Using ADSI Edit**

You can use ADSI Edit or the Active Directory Users and Computers snap-in.

Grant the Read All properties right to the domain object.

- 1 Select the Domain.
- 2 Right-click and select Properties.
- 3 Select the Security tab.

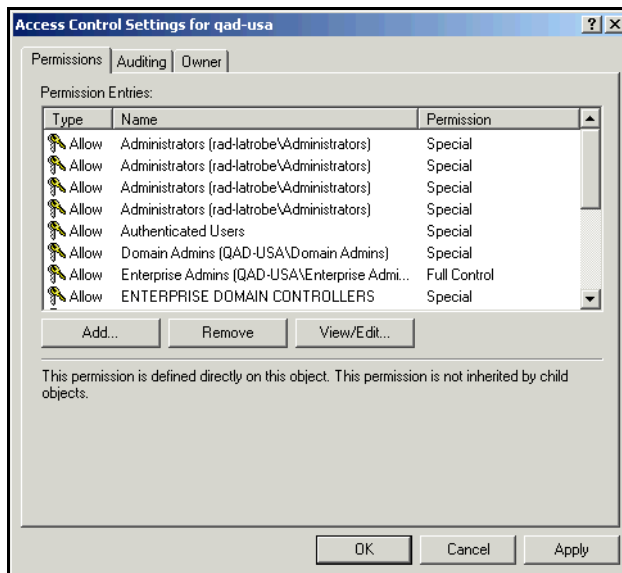


**Fig. 79** Credentials in a Domain Data Source

- 4 Click the **Advanced** button.

This opens the Access Control Settings dialog for your computer.



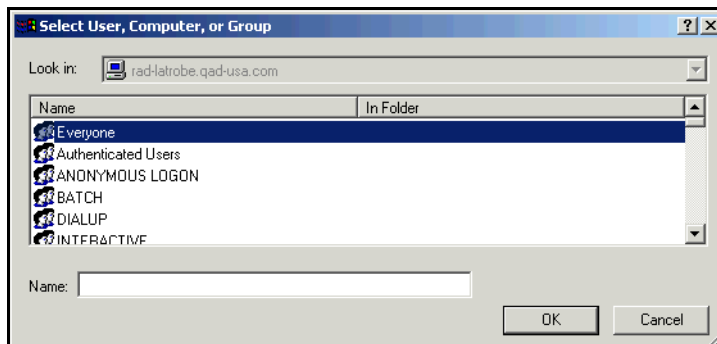


**Fig. 80** Access Control Settings Dialog

5 Click the **Add** button.

6 Click **OK**.

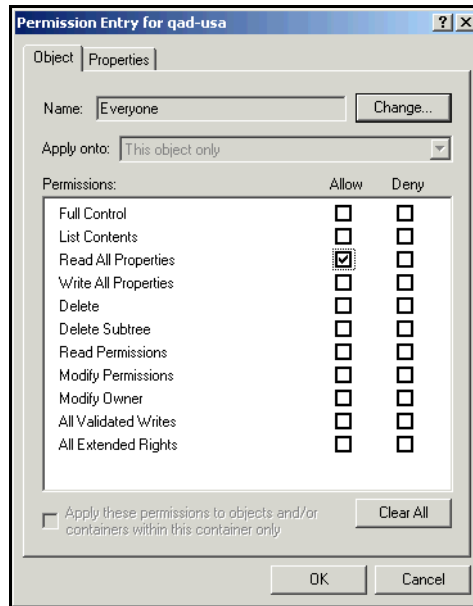
This opens the **Select User, Computer, or Group** dialog.



**Fig. 81** Select User, Computer, or Group Dialog

7 Select **Everyone** or enter in the **Name** text box.

8 Click **OK** to accept selection.

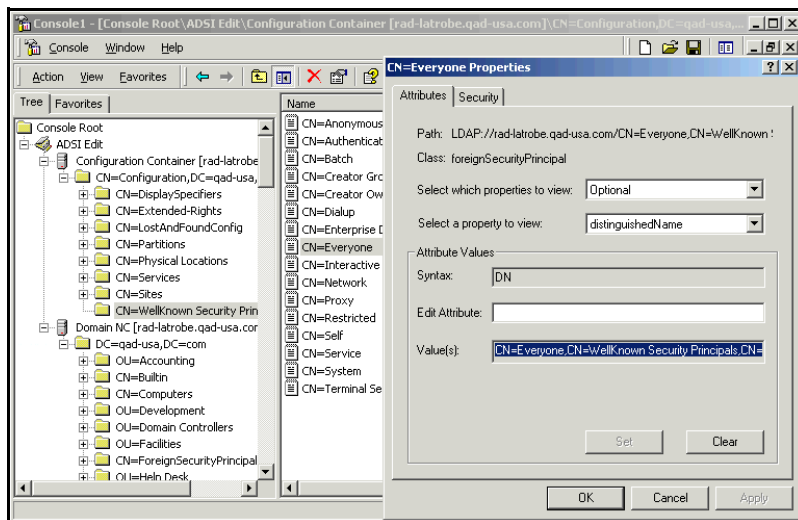


**Fig. 82** Permission Entry Dialog

- 9 Using the Permission Entry dialog, set the **Apply onto** setting to **This object only**. In the Permissions section, check in the **Allow** column for Read All Properties permission.
- 10 Click **OK** to close this dialog.

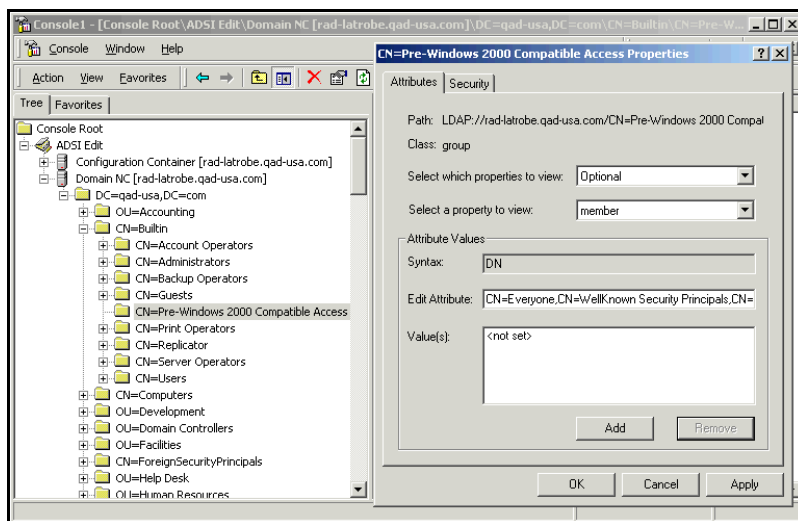
► **Changing the membership of Pre-Windows 2000 compatible access**

- 1 Select the group from the built-in container. Use ADSI Edit to modify this group.
- 2 Connect to the domain using Domain NC and Configuration Container.
- 3 Go to Configuration Container \ CN=Configuration, DC=<your domain controller name>\ CN=WellKnown Security Principals.
- 4 Select CN=Everyone.  
This opens the CN=Everyone Properties dialog (Fig. 83).
- 5 Copy the **distinguishedName** attribute to the clipboard in the Select a property to view list box.
- 6 Click **OK** in the CN=Everyone Properties dialog.



**Fig. 83** Verifying Credentials Pre-Windows 2000

This opens the CN=Pre-Windows 2000 Compatible Access Properties dialog (Fig. 84).



**Fig. 84** CN=Pre-Windows 2000 Compatible Access Properties Dialog

- 7 Go to Domain NC \ CN=Builtin.
  - 8 Select CN=Pre-Windows 2000 Compatible Access.
  - 9 Select **member** attribute of this object in the Select a property to view list box.
  - 10 In the Edit Attribute text box, paste the DN that was copied in [Step 5](#), page 82.
  - 11 Click the **Add** button.
- The added selections are listed in the Value(s) section.
- 12 Click **OK** to close this dialog.

---

## Scenario 3: Using Generic Scopes

With *bv-Control* for Active Directory v8.00 you can scope to an object by specifying the Distinguished Name (DN) of an object. Use the Generic Scope option on the Query Binder scope page. The objects searched are determined by the data source selected in the Query Binder.

The Generic Scope option allows you to enter any arbitrary path in the directory to start your search. You can use this option to start your search at object paths not listed in the standard scope pages.

To use this facility you need to specify the DNS name of the domain and the distinguished name (DN) of the object path where you want to start your search.

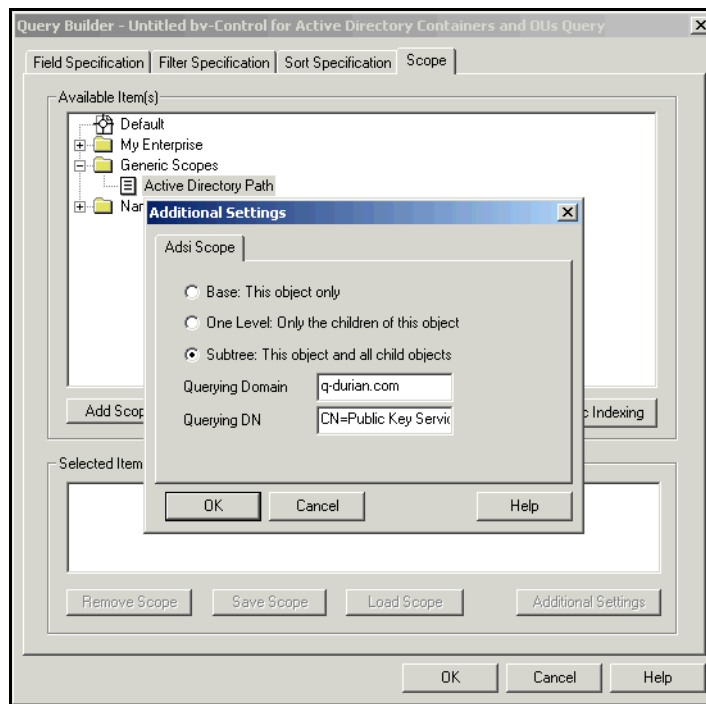
Typically this facility is used to search through the portions of Active Directory that are not directly accessible from the standard scope UI.

For example, consider a search through the configuration of Active Directory in an Active Directory forest. The three parameters of the search are starting point (domain and the DN), object to search for (Data source), and the fields to retrieve (Field list). You have an option to select the fields from the standard list of fields or from the User Defined Fields as listed in the Query Binder. You can also mix these in a query.

For this example use a forest with an Exchange 2000 installation, which results in Active Directory Schema extension. We will search to find out the Public Key Services installed in the forest. This example assumes that the credential database has been configured and assigned to a user. The Windows 2000 Active Directory domain for this example is *q-durian.com*.

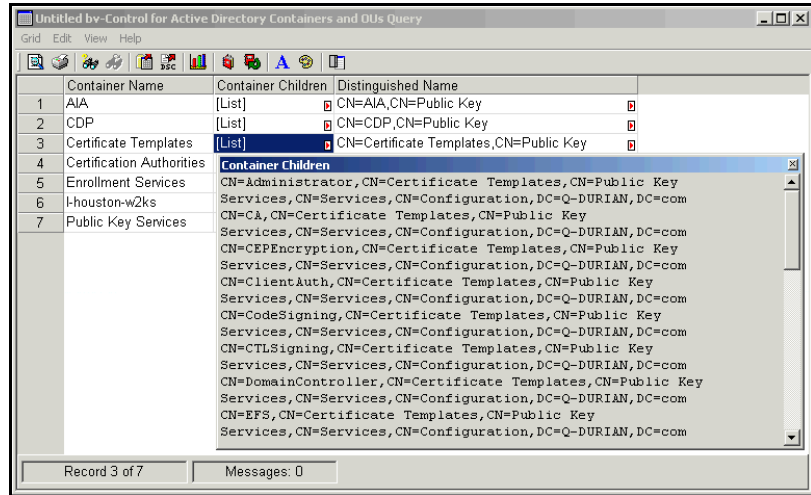
- 1 Select the Query Builder.
- 2 Remove the default fields and select Container name, Container children, and Distinguished Name from the list of available fields.
- 3 Go to the Scope tab.
- 4 Remove the default scope from the list of Selected Items.
- 5 Open Generic Scopes, select Active Directory Path and click the **Add Scope** button.

The Additional Settings with the **Adsi Scope** tab appears.



**Fig. 85** Query Builder and Additional Settings Dialog

- 1 In the Adsi Scope tab of the Additional Settings dialog:
  - Select Subtree search.
  - **Querying Domain** - Enter the DNS name of the domain that you want to search. For this example, `q-durian.com`
  - **Querying DN** - Enter the DN of the object path where you want to start your search. For this example, you can start searching in Configuration container (CN=Public Key Services,CN=Services,CN=Configuration,DC=Q-DURIAN,DC=com)
- 2 Click **OK** to close the Additional Settings dialog.
- 3 Click **OK** to close the Query Builder dialog.
- 4 Run this Query.



**Fig. 86** Query Results Panel

The results will list all the Public Key Services listed in the Active Directory.

---

# A

# Troubleshooting

---

<b>Problem</b>	<b>Solution</b>
Some field descriptors, such as 'Effective Permissions / Effective Permissions Analysis / Effective Trustees', may not show appropriate selections.	If the 'canonicalName' attribute is not accessible using the credentials available in the credentials database, then some field descriptors such as 'Effective Permissions / Effective Permissions Analysis / Effective Trustees', may not show appropriate selections. The typical result will be that the names added to the list of selected item will be blank. This is by design. No action is required.
Cannot Initialize ADSI search object. Incorrect function. You may see this error while adding credentials to the credential database or browsing through the scope pages. This is because the Global Catalog server was not available or could not be reached.	Check DNS setting on BindView Information Server machine. Make sure that GC server is running and can be reached from BindView Information Server machine.
When an object is moved in Active Directory, the scope in saved queries displays the old path of the object. As an example, if a query was scooping to an OU and the OU is then moved, the query still displays the old path of the OU. While running the query the server uses the correct path. This is a display refresh problem.	Modify the saved query. Remove the scope and add the new path.
When an object, such as an OU, is moved in Active Directory and a new OU with the same name is created at the same location, the saved queries use the moved path but the display still shows the old path. To reproduce this behavior, create a query and scope to an OU. Move the OU to some other OU/Domain and create a new OU with the same name. Now rerun the query. The query will return data from the moved OU but the query scope will still point to the old OU.	Modify the saved query. Remove the scope and add the new path.

---

<b>Problem</b>	<b>Solution</b>
<p>A query will fail with Unavailable scope, and search fields were not found. The bv-Control for Active Directory search engine is not able to get the data from FSR database. The error message is as follows:</p> <ol style="list-style-type: none"> <li>1. Unavailable Scope: (AdsiScope LDAP:ADS_SCOPE_SUBTREE)</li> <li>2. Search Fields were not found.</li> </ol>	<p>Install Windows 2000 SP1.</p>
<p>When new user credentials are added to the credentials database, the validation process may return an error message saying that the credentials are invalid. This typically happens when the domain hosting the account could not be reached.</p>	<ol style="list-style-type: none"> <li>1. Verify that your DNS server is available and can be reached.</li> <li>2. Verify that your DNS server can resolve the DNS name of the domain.</li> </ol>
<p>Queries running Users data source will use 100% CPU. If a query is running fields in the Users data source, the CPU utilization will stay at 100% for the duration of that query. This data source uses multiple threads to complete the search through the supplied scope. In large Active Directory installations this design practice improves the query performance. In version 8.00 of the product, only the Users data source is expected to return very large number of records. So only Users data source uses multiple threads. This can change in subsequent releases of the product.</p>	<p>This is by design. No action is required.</p>
<p>Uninformative System failure message. While a query is in progress, if the network gets disconnected, the query fails with the following message: Logon failure: unknown user name or bad password. The query uses the credentials supplied in the credentials database to bind to the Active Directory Object. The network problems prevent Active Directory Service Interfaces from logging on to the domain. The query returns the error returned by ADSI. This error message may change, depending on the point of failure.</p>	<p>This is by design. No action is required.</p>
<p>Containers query on a domain scope includes System container. A query that scopes to System container can return objects in the system container and its child containers. There are many hidden /unwanted records in the System container.</p>	<p>To avoid reporting System container objects, include the following filter in the query Active Directory Path Doesn't Contain CN=System</p>



Problem	Solution
<p>GPO data source reports 'Not Configured' value when the 'Customize???' option is unchecked for options in User Configuration\Windows Settings\Internet Explorer Maintenance\* *            Microsoft GPO snap-in will show the URL path details even when the 'Customize???' is unchecked. The value set in the policy file is Empty and the original value is saved in a separate variable. The Microsoft Group Policy snap-in shows the old value. This affects 7 settings under the mentioned folder hierarchy.</p>	<p>This behavior is by design. No action is required at this time. This may change in subsequent releases.</p>
<p>Containers and OUs data source.--            Container Children fields and Groups data source – Group member fields require more time than other fields.            These fields require nested computation and take longer than other fields The performance impact will be more if the network bandwidth is narrower between BindView Information Server and the connected DC/GC is small. The problem seems to occur largely on 10 MBPS connections between these two servers.</p>	<p>No action is required at this time. This may change in subsequent releases.</p>
<p>BindView Information Server memory utilization may increase before stabilizing a steady state.            BindView Information Server uses Access Database to save temporary data. Microsoft Jet Engine that is used to access this database caches some information locally. The buffers allocated to cache this information may not be released for the life of the process. This causes the memory utilization to go up and then stabilize.</p>	<p>Set the MaxBufferSize value to some reasonable number such as 1024. For more information on MaxBufferSize setting refer to Chapter 7-Optimizing Your Application in 'Microsoft Access 2000 – Building Applications with Forms and Reports. See, Adjusting Windows Registry Settings to Improve Performance.'</p>
<p>When the Active Directory credentials are removed from the credential database, the forest that they were used in is still listed in the configuration folder. The 'Enterprise Directories' folder in the 'Add Credentials' page lists these forests until they are removed.            The product does not automatically remove those configured forests.</p>	<p>Click the Configuration folder. Double click the Configured Forests item in the right pane. Select the forest and click Delete. Click OK to save the changes.</p>

<b>Problem</b>	<b>Solution</b>
<p>Adding credentials to the credential database using the 'Specify Domain' option does not accept the addition of more than one domain.</p> <p>Once you add the credential using Specify Domain option, the credential gets added to the 'Selected Items' list as 'Generic Credential'. If you try to add any more credentials without closing the 'Add Credentials' dialog, the new credentials are neither accepted nor is there any error message.</p>	<p>Close the Add Credential dialog before entering the second credential.</p>
<p>If the installation path is longer than 50 characters, the installation will fail. The pre-defined reports shipped with the product fail to install.</p>	<p>Choose the install path less than 50 characters.</p>
<p>Group Policy Windows Settings\Windows Settings\User Configuration\Folder Redirection fields return data that is inconsistent with Microsoft Group Policy snap-in.</p> <p>Run Microsoft Group Policy snap-in and select a policy. Go to User Configuration\Windows Settings\Folder Redirection. Select any setting and open the property page On the 'Target' page select the 'Advanced' setting. The contents of the 'Settings' tab are all disabled when the 'Security Group Membership' list on 'Target' page is empty. bv-Control for Active Directory v8.0 shows the previously set values By default this is set to "Leave the folder in its location".</p>	<p>No action is required at this time.</p>
<p>When first launching the BindView RMS Console, if you click "bv-Control for Active Directory (Checking Configuration)" in the Console tree before the RMS Console has finished opening, the RMS Console may lock up.</p>	<p>Close the BindView RMS Console and launch it again. Do not click on the snap-in product until the RMS Console has finished checking the configuration.</p>
<p>The Site Links, Domain Links, and OU Links fields in the Group Policies data source will have a descriptor page that asks for the credential to use to search for the Sites, Domains, and OUs linked to the Group Policies. The field will only return the sites, domains, and OUs on which the given credential has read rights.</p>	<p>To view complete results, the credential provided must at least have delegated rights to read the Group Policy link property of all sites, domains, or OUs in the forest.</p>

Problem	Solution
<p>Effective Permission Analysis field may not account for recent changes made group membership, in the subsequent runs of the query. This affects the effective permissions and the indirect permissions displayed in the form field. bv-Control for Active Directory caches the group memberships, which provides a better performance while calculating the effective permissions of security principals.</p>	<p>Close and relaunch the BindView RMS Console.</p>
<p>Windows Server 2003 has changed the behavior of "Additional restrictions for Anonymous Connections" (this appears in Query Builder under "Windows Settings\Computer\ Configuration\Security Settings\Local Policies\Security Options" of Group Policy Windows Settings datasource). This setting has been renamed in Windows 2003 as "Network Access: Do not allow enumeration of SAM accounts and shares". Though the title names are different, the registry key updated is the same. Also in 2000 this setting had a drop down box, while in 2003 this setting has a single Checkbox to define the setting.</p>	<p>bv-Control for Active Directory v8.00 has introduced a new field "Network Access: Do not allow enumeration of SAM accounts and shares" to report this setting in Windows Server 2003. This setting will correctly report only against Windows 2003. Using this field to report against Windows 2000 will give wrong results. Same is the case with "Additional restrictions for Anonymous Connections" i.e. it will report correctly for Windows 2000, but not against Windows Server 2003.</p>
<p>Querying for the attributes tokenGroups, tokenGroupsNoGCAcceptable, tokenGroupsGlobalAndUniversal, using the User Defined Field "String SID List Attribute", for Users, Groups, and Computers data source, returns no results. This happens when SubTree and One-Level scope level options are selected for the scopes.</p>	<p>Select the individual objects with base level scope option in the Scoping tab to query these attributes.</p>

Problem	Solution
<p>The settings listed in the table below have changed in Windows Server 2003. In Windows 2000 these fields had a check box setting. In order to configure these, apart from selecting the Configured option button, the user needed to check the box. In Windows Server 2003 the check box has been removed. Now the user needs to select only the Configured option button.</p>	<p>These are all settings of Group Policy Administrative Templates datasource.</p> <p><b>Setting</b> Always install with elevated privileges <a href="#">Location in Query builder</a> \Administrative Templates\Computer Configuration\Windows Components\Windows Installer</p> <p><b>Setting</b> Prohibit Rollback <a href="#">Location in Query builder</a> \Administrative Templates\Computer Configuration\Windows Components\Windows Installer</p> <p><b>Setting</b> Remove browse dialog box for new source <a href="#">Location in Query builder</a> \Administrative Templates\Computer Configuration\Windows Components\Windows Installer</p> <p><b>Setting</b> Prohibit patching <a href="#">Location in Query builder</a> \Administrative Templates\Computer Configuration\Windows Components\Windows Installer</p> <p><b>Setting</b> Disable IE security prompt for Windows Installer scripts <a href="#">Location in Query builder</a> \Administrative Templates\Computer Configuration\Windows Components\Windows Installer</p> <p><b>Setting</b> Enable user control over installs <a href="#">Location in Query builder</a> \Administrative Templates\Computer Configuration\Windows Components\Windows Installer</p> <p><b>Setting</b> Enable user to browse for source while elevated <a href="#">Location in Query builder</a> \Administrative Templates\Computer Configuration\Windows Components\Windows Installer</p> <p><b>Setting</b> Enable user to use media source while elevated <a href="#">Location in Query builder</a> \Administrative Templates\Computer Configuration\Windows Components\Windows Installer</p>

Problem	Solution
	<p><b>Setting</b>            Enable user to patch elevated products  <a href="#">Location in Query builder</a>            \Administrative Templates\Computer Configuration\Windows Components\Windows Installer</p> <p><b>Setting</b>            Allow admin to install from Terminal Services session  <a href="#">Location in Query builder</a>            \Administrative Templates\Computer Configuration\Windows Components\Windows Installer</p> <p><b>Setting</b>            Cache transforms in secure location on workstation  <a href="#">Location in Query builder</a>            \Administrative Templates\Computer Configuration\Windows Components\Windows Installer</p> <p>In bv-Control for Active Directory Active Directory v8.00 a new field has been added for each of the above settings. To distinguish the Windows 2000 field from the corresponding one for Windows Server 2003, each field is suffixed with "[Windows 2003]". Ex. corresponding field for "Always install with elevated privileges" of Windows 2000 is "Always install with elevated privileges [Windows 2003]" for Windows Server 2003. If a Windows 2000 field is used to report against Windows Server 2003, then the results will display "Not Configured". Same is the case for Windows 2000 fields reporting against Windows Server 2003.</p>

<b>Problem</b>	<b>Solution</b>
The fields for the new settings of Windows Server 2003 may report 'Not Configured' for configured settings, when 'Turn Of Automatic Updates of Adm Files' Group Policy setting is effective. This happens when the Information Server is on a Windows 2000/Windows XP machine and reporting against a Windows Server 2003 policy. When this setting is effective the Adms are not present in the Sysvol folder. Therefore the local Adms in the %windir%\Inf folder, on the Information Server are used and these are older then the ones shipped with Windows Server 2003.	Update the %windir%\Inf folder on the Information Server with the latest Adm files. <a href="#">Recommendations for Managing Group Policy Administrative Template (.adm) Files.</a>
The 'All Configured Settings' field of Group Policies datasource, reports default values for few settings, even if these are not configured. These GPO settings, though not configured, have default effective values. These default values get applied to the User when the policy is applied. Therefore these are reported in the 'All Configured Settings' field.	These are the settings that have default values: Please see Tables 1-7

Windows Settings\User Configuration\Internet Explorer Maintenance\URL\Channels

**Table 1**

<b>Setting</b>	<b>Default</b>
Turn on desktop Channel Bar by default	False

Windows Settings\User Configuration\Internet Explorer Maintenance\URLs\Important URLs

**Table 2**

<b>Setting</b>	<b>Default</b>
Customize Online support page URL	False
Customize Home Page URL	False
Customize Search bar URL	False

Windows Settings\User Configuration\Internet Explorer  
Maintenance\Browser User Interface

**Table 3**

<b>Sub category</b>	<b>Setting</b>	<b>Default</b>
Custom Logo	Customize the static logo bitmap	False
Browser Title	Customize Title Bars	False
	Customize Toolbar background bitmap	False

Windows Settings\User Configuration\Internet Explorer  
Maintenance\Connection\User Agent String

**Table 4**

<b>Setting</b>	<b>Default</b>
Turn on desktop Channel Bar by default	False

Windows Settings\User Configuration\Internet Explorer  
Maintenance\URLs\Favorites and Links

**Table 5**

<b>Setting</b>	<b>Default</b>
Only delete the favorites created by the administrator	False
Delete Existing Favorites and Links if Present	False
Favorites specified?	No
Links specified?	No

**Table 6**

<b>Sub category</b>	<b>Setting</b>	<b>Default</b>
Application Data	Grant the user exclusive rights to Application Data	False
	Move the contents of Application Data to the new location	False
	Application Data Policy Removal Option	None
	Application Data redirection option	No administrative policy specified
Desktop	Desktop redirection option	No administrative policy specified
	Grant the user exclusive rights to Desktop	False
	Move the contents of Desktop to the new location	False
	Desktop Policy Removal Option	None
My Documents	My Documents redirection option	No administrative policy specified
	Grant the user exclusive rights to My Documents	False
	Move the contents of My Documents to the new location	False
	My Pictures Preferences	Do not specify administrative policy for My Pictures
	My Documents Policy Removal Option	None
My Pictures	My Pictures redirection option	No administrative policy specified
	Grant the user exclusive rights to My Pictures	False
	Move the contents of My Pictures to the new location	False
	My Pictures Policy Removal Option	None
Start Menu	Start Menu redirection option	No administrative policy specified
	Grant the user exclusive rights to Start Menu	False
	Move the contents of Start Menu to the new location	False
	Start Menu Policy Removal Option	None



Windows Settings\User Configuration\Folder Redirection\

**Table 7**

<b>Sub category</b>	<b>Setting</b>	<b>Default</b>
Connection\User Agent String	Custom User Agent string	False
Connection\Proxy Settings	Do not use proxy server for local (intranet) addresses	False
Programs	Import the current Program Settings	False



# Index

## A

- Adding a database, 36
- Adding credentials, 36 – 39
- Advanced reporting, 17
- Advanced use scenarios, 77
  - Generic scopes, 84
  - Reporting, 78
  - Verifying credentials, 79
- Architecture, illustrated, 16

## B

- Baseline options, 69
- BindView RMS Console, 14
  - Components, 16
- Building queries, 46

## C

- Charts, 68
  - Histogram, 69
  - Series, 69
- Client, 16
- Configured forests, 64
- Console tree, illustrated, 14
- Creating a baseline, 69
- Credential database, 35 – 41
  - Adding credentials, 36
  - Adding databases, 36
  - Applying to a user, 39
  - Requirements, 35
- Credential verification, 65
- Custom queries, 17

## D

- Data sources, 17, 46
  - Showing, 71
- Data storage, 17
- Deleting files, 43
- Directories
  - enterprise, 61
- Displaying query results, 68
- Duplicate key options, 50

## E

- Effective Trustees, 73
- Enterprise Directories, 61
- Exporting, 17

## F

- Features
  - Advanced reporting, 18
  - Custom queries, 18

- Graphing, 18
- Pre-defined Query Binder, 17
- Field tab, 48
- Filter tab, 49
- Forests, 55, 64, 78, 79

## G

- Generic scopes, 84
- Global print setup, 69
- GPOs, Group Policies
  - see** Group Policy Objects
- Graphing, 17
- Grids, 68
- Group Policy Objects, 75
  - Defined, 75

## H

- Histogram charts, 69
- Historical data, 69

## I

- Information Servers, 16
  - Data sources, 17
  - Task processing, 17
- Installation wizard, 20

## K

- Key options, 50

## L

- Licenses
  - Adding, 26
  - Description, 26
  - Properties, 26

## M

- Microsoft Management Console, 14
- Microsoft Network, using, 58
- MMC **See** Microsoft Management Console, 14
- Monitoring task status, 66
- Multiple forests, 55
  - Reporting, 78
  - Requirements, 55
  - Verifying credentials, 79

## P

- Pre-defined Query Binders, 17
- Pre-installation, 20
- Print setup, 69
- Product licenses, 26

## Q

### Queries

- Accessing, 67
- Adding fields, 48
- Defining, 46
- Displaying results, 68
- Filters, 49
- Running, 66
- Saving, 54
- Scopes, 51

### Query, 46

### Query binder defined, 17

### Query Builder

- Field tab, 48
- Filter tab, 49
- Scope tab, 51
- Sort tab, 50

### Query features

- Baselining, 69
- Building process, 46
- Task lists, 70

### Query results, 68

## R

### Reports, 69

### Requirements

- Credential databases, 35
- Multiple forest support, 55
- System, 20

### Running a query, 66

## S

### Saving queries, 54

### Scope tab, 51

### Scopes, 51

- Generic, 84
- Named, 53
- Settings, 52

### Selecting

- Duplicate key options, 50
- Task types, 70

### Series charts, 69

### Sort tab, 50

### System requirements, 20

- Security checks, 15
- Snap-in defined, 15

## T

### Task Lists, 70

### Task processing, 17

### Task Status, 66

## U

### Upgrading from previous version, 20

## V

### Verifying

- Credentials, 65
- Credentials across forests, 79

### View types

- Charts, 68
- Grids, 68
- Reports, 69