

Evaluation Guide

bv-Control[®] for Windows[®]





bv-Control_® for Windows_® v8.00

Evaluation Guide

BindView Corporation · 5151 San Felipe, Suite 2500 · Houston, TX 77056

COPYRIGHT

Copyright © 2003, 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

bv-Control for Windows Evaluation Guide

Contents

Introduction .	
Account Mana	gement and Analysis10
Scenario 1	Stale or Unused Machine Accounts
Scenario 2	Audit User Privileges 13
Configuration	Management
Scenario 3	Share Configuration
Scenario 4	Service Configuration
Scenario 5	Flexible Registry and Event Log Reporting 23
Content and C	Capacity Management
Scenario 6	Disk Space Analysis and Management 26
Security of Se	nsitive Files and Directories
Scenario 7	Audit Users and Groups that Have Access toSensitive Files and Directories32
Active Directo	ry® Security Principle Analysis
Scenario 8	Assess Users and Groups that are able to Create, Delete, and Manage Active Directory Groups 37
Web Services	
Identifying Ch	anges to Virtual Files, Directories, and Shares
Scenario 9	Using MD5 Checksum Functionality to Show Variances in Data . 42
Using an IIS S	Server Lock Down Template
Scenario 10	Determine if Settings and Patches are Applied Correctly 46
Reviewing Per	missions to Web Site Home Directory
Scenario 11	Determine Users with Read Permissions to the Web Site Home Directory48
Identifying Un	authorized ISAPI Filters
Scenario 12	ISAPI Filter Properties and Settings
Conclusion	
Contacting Bir	ndView

8 *bv-Control for Windows Evaluation Guide*

Introduction

Securing and managing the Windows® environment is an ongoing process, not a point-in-time process. With bv-Control® for Windows®, administrators can audit and analyze data, notify and alert when issues are discovered, and quickly and easily remediate issues to keep their Windows environment maintained, secure, and available.

bv-Control for Windows focuses on automating the task of collecting and presenting information about the Windows environment in the areas of account and configuration management, content and capacity management, and performance. Using bv-Control for Windows, administrators are able to:

- Reduce security exposure Quickly audit and analyze the security of the Windows environment to identify security breaches and policy non-compliance. Using the account and configuration management features, administrators can identify and remove stale or unused accounts, determine who has excessive rights, assess share permissions, audit computers to ensure that only approved services are installed and properly configured, and perform detailed auditing and forensic analysis.
- Deliver fast security remediation Streamline and speed up the process of fixing security and administration problems with the closed-loop problem identification and resolution capability. Many problems can be fixed from within the numerous out-of-the-box or customized reports, thereby achieving security policy enforcement and eliminating security risk.
- Automate administrative tasks Simplify and accelerate daily tasks, such as monitoring systems for installed hotfixes and service packs, managing disk space utilization, and analyzing files to identify changes to Web content, virtual directories, files and permissions.
- Meet service level agreements (SLAs) Ensure system availability and adequate service levels. The IntelliPACS feature provides real-time monitoring and alerts, which empowers administrators to be proactive by highlighting past trends to determine potential trouble spots and avoid future pitfalls.
- Reduce business disruption and losses With the combination of security and administration capabilities, organizations can reduce business losses due to downtime by 30-70%, and reduce remediation, recovery time and associated costs by 20-50%.

About This Guide

This bv-Control for Windows Evaluation Guide is designed to guide you through an evaluation process that demonstrates key features of this product. After installing and configuring bv-Control for Windows, you can proceed through the scenarios that are intended to give you a brief, hands-on tour of specific functionality highlights.

Account Management and Analysis

A key area of system and security assessment is user account management. This includes ensuring that only users with valid identities have enabled accounts and that these accounts are properly provisioned. Two examples of how BindView addresses these issues are: locating stale or unused machine accounts, and analyzing detailed rights and group membership.

Note: These scenarios are given using only one Query Engine. If you scope to a domain with a large number of users, performance may be affected.

Scenario 1: Stale or Unused Machine Accounts

Organizations face constant change which places a significant burden on vulnerability management of the IT infrastructure. This includes adding, disabling, and deleting user accounts as employees or consultants are recruited and when they leave the organization. Although manually reviewing local computer and domain user accounts is a daunting task, it is vital that in this process you ensure that only accounts with valid identities are active in the environment. BindView not only allows administrators to automate this process, but also provides the ability to take direct action to disable or delete unused accounts. This exclusive closed-loop problem identification and remediation process can save a significant amount of time and effort.

- 1 From the **BindView RMS Risk Assessment and Control** folder, expand the **Pre-Defined** and **bv-Control for Windows** folders.
- 2 Expand the **Security Best Practices** folder.
- **3** Double-click the **User Security** folder.
- 4 Double-click Old User Accounts Still Enabled.

- m BindYiew [BindYiew RMS\Risk Assessment and Control\Pre-Defined\by-Control for Windows\Security Best Practices\User Security\Old Use - 🗆 × _ 8 × 🚡 Console <u>W</u>indow <u>H</u>elp Action View 🛛 🗢 🔿 🗈 🔃 🖻 🖆 😭 😰 🖉 🚺 🧱 🏀 😚 Old User Accounts Still Enabled Tree ۸ 🖻 쥷 Risk Assessment and Control * **Query Information** 🗄 💼 All User Items 🖻 💼 Pre-Defined Available Tasks E Dv-Control for Windows Old User Accounts Still Run And View As Grid Name: 🗄 🛅 Configuration Management Enabled 🗄 🧰 Documentation & Disaster Recovery 🟈 Modify Query Definition \Pre-Defined\by-Control for 🗄 🚞 Getting Started Windows\Security Best Location: 🗞 Create Schedule 🗄 💼 Historical Datasets and Internal Fields Practices\User Security 🗄 🚞 Patch Assessment Displays user accounts that 🎸 Modify Properties Short 🚊 🧰 Security Best Practices have not been used to Description: logon for 60 days or more 🔷 Save As HTML File 🗄 💼 Domain - Enterprise Security and have not been disabled 🗄 💼 Event Logs Security Default <Default> 🗄 💼 File System Security Action: 🗄 🧰 Machine Security 🗄 🧰 PWC Security Analysis Query Definition 🗄 🧰 SANS 🗄 💼 User Security Account Operators
 Administrator Accounts Not Renamed
 Backup Operators Product: by-Control for Windows Data Source: Users Fields: \otimes Backup Operators Filters: \otimes Detailed User Account Password Settin \otimes Disabled and Old User Accounts Scopes: Disabled User Accounts Effective Group Administrators Effective Group Historical Data Information History Enabled User Accounts - Never Logged 0 Count: Locked Out or Disabled User Accounts Locked None Locked Out User Accounts Dataset: Old User Accounts Still Enabled Old User Accounts Still Enabled - From Max History 50 Count:
- 5 In the Available Tasks section of the details pane, click Run And View As Grid.

This query allows you to see domain/workgroup name, user name, which users have or do not have disabled accounts, the date and time of last logon, as well as the container name in canonical format.

The results of this query can provide valuable information when trying to determine an accurate user count, or whether or not it is possible that a particular user accessed a sensitive file or directory at a given point in time.

Once you initiate the query, the **Task Status** dialog appears. This dialog shows the status of the query while it is being run.

Task 9	Status - ADELOSSA-TEST2				
Actions					
Job Ide	Name	Туре	Start 🔽	End	Details 🔺
01220	Old User Accounts Still Enabled	Query	7/8/2003 12:10:21 PM		Accepted : 0 Re
0 1201	Change Session Log : Untitled by-Control fo	Query	7/3/2003 12:42:30 PM	7/3/2003 12:42:31 PM	Records: 1/16
1200	Untitled by-Control for Windows Services Q	ActiveAdmin	7/3/2003 12:42:05 PM	7/3/2003 12:42:05 PM	Records: 1/1
1198	Change Session Log : Untitled by-Control fo	Query	7/3/2003 12:23:46 PM	7/3/2003 12:23:47 PM	Records: 1/15 🖵
1					
Error	📕 Partially Successful 🛛 🔵 Successful 🛛	Incomplete	🔷 Waiting 🛛 🔵 Runni	ng	

When the query is done generating, the dataset appears with the related fields included in the grid.

🔲 Old L	Old User Accounts Still Enabled							
Grid Ed	lit View Help							
] 🗟 🍯	📴 🥩 🏘 🤣 🛅 👯 🛄 📦 🗞 A 🧐 💵							
	Domain/Workgroup Name	User Name	Account	Logon: Last	Container Canonical Name			
			Disabled?	Date/Time				
1	SOUTHWESTERNCOL	IWAM_ANTONITO	No	[None]	southwesterncolorado.colorado.net/Users			
2	SOUTHWESTERNCOL	TsInternetUser	No	[None]	southwesterncolorado.colorado.net/Users			
3	SOUTHWESTERNCOL	IWAM_V-JBAKER-W2KAS	No	9/20/2001 8:05	southwesterncolorado.colorado.net/Users			
4	SOUTHWESTERNCOL	bvu_colorado	No	1/9/2003 14:20	southwesterncolorado.colorado.net/Users			
5	SOUTHWESTERNCOL	b∨u_larry	No	1/14/2003 8:20	southwesterncolorado.colorado.net/Users			
6	SOUTHWESTERNCOL	hien_qe02242003	No	2/24/2003 15:23	southwesterncolorado.colorado.net/Users			
7	SOUTHWESTERNCOL	IUSR_ANTONITO	No	5/28/2003 10:06	southwesterncolorado.colorado.net/Users			
8	SOUTHWESTERNCOL	IUSR_V-JBAKER-W2KAS	No	4/26/2004 7:51	southwesterncolorado.colorado.net/Users			
	Record 1 of 8 Messages: 0							

The grid displays all of the fields that are included in this particular pre-defined query. You can see that some column fields are blue. The blue fields on the grid are ActiveAdmin® fields. You can make changes to the contents of these fields by right-clicking on the value in the grid and editing it. The ActiveAdmin editor for the selected field is displayed so that you can make your changes.

To demonstrate this, we will attempt to move a machine account to an OU with no privileges that in turn will prevent the account from being used.

- 6 Right-click on one of the blue cells in the **Container Canonical Name** column.
- 7 Select **Edit** from the drop-down menu.

The Data Query Action dialog appears.

Data Query Action	2
Not all information needed wa	as found on the grid and will be queried.
Yes	No

8 Click Yes.

The ActiveAdmin editor Move Active Directory Object dialog appears.

Move Active Director	y Object	×
User: IWAM_ANTONI Domain: southweste Current Container: U	TO rncolorado.colorado.net sers	
Move To: Users	OK Cancel Help	Browse

Use this dialog to move a computer or user object to another container in the same domain. account.

9 Enter the complete path of the destination container in the **Move To:** field or click **Browse...** to browse for the destination container.

10 Click OK.

The **ActiveAdmin - Change Action** dialog appears.



11 Click Yes to proceed with the action.

The query will rerun and the Change Session Log will appear with the new value displayed in the grid.

🔲 Ch	ange Sessior	n Log : Old User Accoun	ts Still Enat	oled			_ _ ×
Grid	Edit View H	Help					
] 🔜) 🖾 🥩 🏕 🤣 🛅 🔛 🔟 🌒 🔂 🗛 🧐 📭						
	Job Identifier	Time Stamp	Result	Record Name	Console User	Comment	New Value
1	2,942	7/15/2004 1:48:54 PM	Success	"SOUTHWE:	QNT-CANA[🛛	[Form] 🕞	southwesterncolorado.colorado.net/Computers
1							
	Record 1	of 1 Mess	ages: 0				

Now that the machine account has been moved, you should determine whether or not the this account will be needed over the next couple of months. You can simply run the **Stale Users** pre-defined query located in the **Configuration Management** folder. This query will return all user accounts in the OU that are older than the time period allotted. You can then delete those accounts.

Scenario 2: Audit User Privileges

Rapid change in organizations creates a significant vulnerability management burden to ensure that users have the appropriate rights to applications, files, directories, and other assets. This includes not only reviewing what accounts have been given explicit access to assets, but what the effective access is to the assets. In this area, BindView provides the ability to thoroughly audit both direct and effective permissions and group membership.

- 1 From the **BindView RMS Risk Assessment and Control** folder, expand the **Pre-Defined** folder.
- 2 Expand the **Security Best Practices** folder.
- **3** Double-click the **User Security** folder in the tree pane.
- 4 Double-click User Accounts with Administrator Privilege Level to run the query.

5 In the Available Tasks section of the details pane, click Run And View As Grid.



This report is a crucial piece of information when assessing the security status of a network, ensuring that only those users with the proper authorization have the appropriate privileges.

The dataset appears with the full name, privilege level, last logon date and time, container name, and the effective group membership list for each account.

🔲 Use	User Accounts with Administrator Privilege Level							
Grid E	Grid Edit View Help							
] 🚉 🤇	📴 🥩 🏕 🤣 🛅 📰 🛄 📦 🗞 A 🧐 🗉							
	Fully Qualified Name	Full	Account	Logon: Last	Container Canonical Name	Effective Group		
		Name	Privilege Level	Date/Time		Memberships <list></list>		
1	SOUTHWESTERNCOL\Administrator	[None]	Administrator	2004 2:27:4 🛽	southwesterncolorado.colorado.net/Users	[List] 💽		
2	SOUTHWESTERNCOL\bvu_colorado	[None]	Administrator	:003 2:20:54 🛛	southwesterncolorado.colorado.net/Users	[List]		
3	SOUTHWESTERNCOL\bvu_larry	[None]	Administrator	2003 8:20:2 🛛	southwesterncolorado.colorado.net/Users	[List]		
4	SOUTHWESTERNCOL\hien_qe02242003	[None]	Administrator	2003 3:23:0 🛛	southwesterncolorado.colorado.net/Users	[List] 🛛 🗗		
5	SOUTHWESTERNCOL\maer-ddyn	[None]	Administrator	2004 9:48:1 🛛	southwesterncolorado.colorado.net/Users	[List]		
	Record 1 of 5 Messages: 0							

In addition to fields that are included in this query, you may also want to select other User Right fields to add to your queries. User Rights fields show whether or not the user has been granted a specific right. These fields also allow the user to determine which machine to analyze for the user right. Some of the user rights are: restoring files and directories, shutting down the system, synchronizing directory service data, and taking ownership of files or other objects.

Other fields of interest include the File and Directory Effective Permissions fields. These fields return the effective permissions that a user has to a specified file or directory while the user

is logged on locally or through Terminal Services, or accessing the object through a network share.

Configuration Management

A significant portion of vulnerability management activities are related to ensuring security best practices through configuration management of servers and workstations. This includes not only the basic OS and patch level review, but also the assessment of file share permissions, service configuration, and event logs. BindView enables administrators to efficiently assess and secure these and many other configuration management concerns.

Scenario 3: Share Configuration

Assessment of share configuration for servers and workstations is vital to ensure the availability of the server, the security of information within the share and security of the enterprise in general. For administrators to assess shares for servers manually would be a cumbersome and expensive task. For administrators to assess shares for workstations would be a nearly impossible task. BindView allows administrators to quickly and efficiently assess share permissions across even the largest enterprises and where necessary disable the share or alter the assigned permissions.

- 1 From the **BindView RMS Risk Assessment and Control** folder, expand the **Pre-Defined** folder.
- 2 Expand the **bv-Control for Windows** folder.
- 3 Expand the **Configuration Management** folder.
- 4 Double-click the Share Analysis folder.
- 5 Double-click Full Control for Everyone.
- 6 In the Available Tasks section of the details pane, click Run And View As Grid.



The result set displayed by the query can quickly identify which machines have shares, which domain or workgroup they are a part of, and what permissions are set for those shares. This information is necessary to know in order to maintain the proper share security within the enterprise.

The dataset appears with the Domain/Workgroup Name, Machine Name, Share Name, Share Path, Container Canonical Name, and Advanced Permissions fields displayed.

📰 Full (Control for Everyone					_ 🗆 ×
Grid Ed	dit View Help					
] 🗟 🧃	ð i 🍻 🛷 i 🛅 🕵	🔟 🗯 🏀	A 🧐 🔲			
	Machine Name	Share Name	Share Path	Container Canonical Name	Permissions (Advanced	d) <form> 🔺</form>
1	ANTONITO	ADMIN\$	C:\WINNT	southwesterncolorado.colorado.net/E 🗗	[Form]	Þ
2	ANTONITO	BVECSDS\$	C:\Program Files\B 🛛	southwesterncolorado.colorado.net/E 🖪	[Form]	Þ
3	ANTONITO	BVNTLLS\$	C:\Program Files\B 🛛	southwesterncolorado.colorado.net/E 🗗	[Form]	Þ
4	ANTONITO	BVQECDS\$	C:\Program Files\B 🛛	southwesterncolorado.colorado.net/E 🛛	[Form]	Þ
5	ANTONITO	BVQEDS\$	C:\Program Files\B 🛛	southwesterncolorado.colorado.net/E 🗗	[Form]	Þ
6	ANTONITO	BVQEMDS\$	C:\Program Files\B 🛛	southwesterncolorado.colorado.net/E 🗗	[Form]	Þ
7	ANTONITO	C\$	C:\	southwesterncolorado.colorado.net/E 🛛	[Form]	Þ
8	ANTONITO	IPC\$	[N/A]	southwesterncolorado.colorado.net/E 🗗	[Form]	Þ
9	ANTONITO	NETLOGON	C:\WINNT\SYSVO D	southwesterncolorado.colorado.net/E 🗗	[Form]	Þ
10	ANTONITO	SYSVOL	C:\WINNT\SYSVO D	southwesterncolorado.colorado.net/E 🗗	[Form]	Þ
11	CORTEZ	ADMIN\$	C:\WINNT	southwesterncolorado.colorado.net/E 🗗	[Form]	•
12	CORTEZ	BVECSDS\$	C:\Program Files\B 🛛	southwesterncolorado.colorado.net/E 🛛	[Form]	Þ
13	CORTEZ	BVNTLLS\$	C:\Program Files\B 🛛	southwesterncolorado.colorado.net/E 🗗	[Form]	Þ
14	CORTEZ	C\$	C:\	southwesterncolorado.colorado.net/E 🖪	[Form]	Þ
15	CORTEZ	IPC\$	[N/A]	southwesterncolorado.colorado.net/E 🖪	[Form]	Þ
16	CORTEZ	NETLOGON	C:\WINNT\SYSVO	southwesterncolorado.colorado.net/E 🖪	[Form]	Þ
17	CORTEZ	SYSVOL	C:\WINNT\SYSVO D	southwesterncolorado.colorado.net/E 🗗	[Form]	Þ
18	LEADVILLE	ADMIN\$	C:\WINDOWS	southwesterncolorado.colorado.net/C 🕞	[Form]	Þ
19	LEADVILLE	BVQECDS\$	C:\Program Files\B 🗗	southwesterncolorado.colorado.net/C 🗗	[Form]	Þ
20	LEADVILLE	BVQEDS\$	C:\Program Files\B 🖪	southwesterncolorado.colorado.net/C 🖪	[Form]	Þ
21		BVOEMDS\$	C:\Program Files\B	southwesterncolorado.colorado.net/C 🖪	[Form]	<u> </u>
						<u> </u>
	Record 1 of 37	Messag	ges: 3			Messages

Use BindView's ActiveAdmin feature to make the share more secure by editing the permissions for the share.

- **1** Right-click on a field in the **Permissions Advanced <FORM>** column.
- 2 Select **Edit** from the drop-down menu. The ActiveAdmin Editor appears.

Permissions Advanced Permissions		
Name	Remove	
Permissions: Full Control	Allow Deny	
Change Read		

18 bv-Control for Windows Evaluation Guide

You can use the ActiveAdmin dialog to change permissions for the share by choosing to deny specific permissions. For example, you can take away full control of the share, deny change rights, as well as deny read rights. You can even remove permissions from Everyone and add a specific user.

\\FORT-MORGAN\c				×
Permissions Advanced Permissions				
Name		Add Remove]	
Permissions:	Allow	Deny		
Full Control				
Change Bead				
	OK		Cancel	Help

In addition, you can use ActiveAdmin to edit the **Share Path**.

- **1** Right-click on a field in the **Share Path** column of the grid.
- 2 Select **Edit** from the drop-down menu. The ActiveAdmin editor dialog appears.

C:\	C:\Program Files Sharing Properties							
Γ	⊂ Donotsl —	nare this folder s folder	٦					
	Share name:	adriana						
	Comment:							
	User limit:	Maximum allowed Allow Users						
		Remove Share New Share						
		OK Cancel Help						

This dialog is similar to the Native Windows dialog. Use this dialog to disable, add a new share, or alter the permissions.

Scenario 4: Service Configuration

Auditing computers to ensure that only approved services are installed and are properly configured is a critical component of vulnerability management. For instance, how do you review your enterprise to locate unapproved installations of IIS? When these rogue instances are found how do you remediate the violation? Another example is related to the significant investment that organizations maintain in virus software. How do you ensure that this software is installed and running? BindView not only enables administrators to assess their environment for service configuration, but it also allows administrators to operatively remediate violations.

- 1 From the **BindView RMS Risk Assessment and Control** folder, expand the **Pre-Defined** folder.
- 2 Expand the Configuration Management folder.
- 3 Expand the **Services** folder.
- 4 Double-click Services Documentation.
- 5 In the Available Tasks section of the details pane, click Run And View As Grid.



The dataset appears with the Services information displayed. The information in the grid tells you the internal type of the service process (Service Type), the name of the user account used by the service process to logon to the system (Startup Account), the method by which the service is started (Startup Type), as well as machine name, display name, and the status.

This information will help you identify if the Service is authorized and can tell you the startup account and its owner.

Ser	Services Documentation							
	Domain/Workgroup Name	Machine Name	Display Name	Status	Service Type	Start Account	Startup Type	-
1	SOUTHWESTERNCOL	ANTONITO	Alerter	Started	Win32 Sharı 🗗	LocalSystem	Automatic	
2	SOUTHWESTERNCOL	ANTONITO	Application Manage 🛛	Stopped	Win32 Sharı 🗗	LocalSystem	Manual	
3	SOUTHWESTERNCOL	ANTONITO	Automatic Updates	Started	Win32 Sharı 🗗	LocalSystem	Automatic	
4	SOUTHWESTERNCOL	ANTONITO	Background Intellige 🛛	Started	Win32 Sharı 🛛	LocalSystem	Manual	
5	SOUTHWESTERNCOL	ANTONITO	BindView Enterprise 🗗	Stopped	Win32 Own 🛽	LocalSystem	Automatic	
6	SOUTHWESTERNCOL	ANTONITO	BindView Query Enc 🖪	Started	Win32 Own 🛽	SOUTHWEST D	Automatic	
7	SOUTHWESTERNCOL	ANTONITO	BindView Support Sip	Started	Win32 Own 🛽	LocalSystem	Automatic	
8	SOUTHWESTERNCOL	ANTONITO	ClipBook	Stopped	Win32 Own 🛽	LocalSystem	Manual	
9	SOUTHWESTERNCOL	ANTONITO	COM+ Event System	Started	Win32 Sharı 🖪	LocalSystem	Manual	
10	SOUTHWESTERNCOL	ANTONITO	Computer Browser	Started	Win32 Sharı 🛛	LocalSystem	Automatic	
11	SOUTHWESTERNCOL	ANTONITO	DHCP Client	Started	Win32 Sharı 🛛	LocalSystem	Automatic	
12	SOUTHWESTERNCOL	ANTONITO	Distributed File Syst 🖪	Started	Win32 Own 🛽	LocalSystem	Automatic	
13	SOUTHWESTERNCOL	ANTONITO	Distributed Link Trac 🗗	Started	Win32 Sharı 🛛	LocalSystem	Automatic	
14	SOUTHWESTERNCOL	ANTONITO	Distributed Link Trac 🖪	Started	Win32 Sharı 🛛	LocalSystem	Automatic	
15	SOUTHWESTERNCOL	ANTONITO	Distributed Transact 🛛	Started	Win32 Own 🛽	LocalSystem	Automatic	
16	SOUTHWESTERNCOL	ANTONITO	DNS Client	Started	Win32 Sharı 🗗	LocalSystem	Automatic	
17	SOUTHWESTERNCOL	ANTONITO	Event Log	Started	Win32 Sharı 🗗	LocalSystem	Automatic	
18	SOUTHWESTERNCOL	ANTONITO	Fax Service	Stopped	Win32 Own 🛽	LocalSystem	Manual	
19	SOUTHWESTERNCOL	ANTONITO	File Replication Ser 🖪	Started	Win32 Own 🛽	LocalSystem	Automatic	
20	SOUTHWESTERNCOL	ANTONITO	IIS Admin Service	Started	Win32 Sharı 🖪	LocalSystem	Automatic	
21	SOUTHWESTERNCOL	ANTONITO	Indexing Service	Stopped	Win32 Sharı 🛛	LocalSystem	Manual	
22	SOLITHWESTERNOOL		Internet Connection S 🗖	Stonned	Win32 Shan 🗖	LocalSystem	Manual	-
	Record 1 of 373 M	essages: 2					Messages	

You can modify the scope of this query to include a particular domain or organizational unit (OU). If you choose to scope to an OU, you can add the Container Canonical Name field to display the container in canonical name format.

If the services reported do not match policies or best practices used by your organization, you can use the **ActiveAdmin** feature to make changes. You can make changes to the contents of these fields by right-clicking on the value in the grid and editing it. For example, you can change how the service starts, how the service logs on to machines and the permissions it has, and whether the service will be able to make changes to the current Windows desktop environment.

- **1** Right-click on a blue field in the grid. A drop-down menu appears.
- 2 Select Edit from the drop-down menu. The Startup Properties dialog appears. The Startup Properties dialog is an ActiveAdmin editing dialog that allows you to change the value associated with the selected field. Use the Startup Properties dialog to change the startup properties of the service that is running. You can change the name of the selected service, choose how the selected service starts up, and control how the selected service starts up.

Startup Properties		X
Service: Alerter		
Startup Type		
C Automatic	Manual	C Disabled
Log On As-		
C Local System acco	unt	
Allow service to	interact with desktop	
This account:	NT AUTHORITY\LocalSer	vice Browse
Password:	*******	
Confirm password:	*****	
🔽 Grant log on as	service right	
🗖 Restart/Start se	ervice after change	
ОК	Cancel	Help

- **3** Make your changes and click **OK** to close the dialog.
- **4** You will be prompted to verify that you want to proceed with the change to the object attribute. Click **OK** to close the dialog.

The **Change Session Log** will appear with the change you made displayed in the grid.

For certain fields, you can also make changes to the item without using an ActiveAdmin editor. These changes affect entire classes of items rather than properties of those items. In terms of the grid, they affect a row rather than a column. For example, you can start and stop, pause, resume and restart services, as well as delete home directories. These changes are called **ActiveAdmin Record Operations**. To make ActiveAdmin Record Operations changes, right-click any ActiveAdmin field, or on any row containing an ActiveAdmin field and choose the **Row** item that appears on the context menu. A submenu appears with the relevant ActiveAdmin operations. Choose the action you want to take from the menu and the action happens immediately.

- **1** From the grid, right-click on an item.
- 2 Select **Row** and **ActiveAdmin** from the drop-down menu.

The ActiveAdmin menu displays.



- **3** Choose a record operation from the menu.
- **4** Verify your change by clicking **OK** on the **Change Action** dialog. The **Change Session Log** will appear with the change displayed in the grid.

Scenario 5: Flexible Registry and Event Log Reporting

Although there are general best practices, each IT enterprise exists to meet the business needs of the organization. As a result, each IT environment will have special cases whether it is proprietary software, a specific distribution of servers and server roles, and/or any number of other factors that make the environment unique. This creates a need for administrators to go beyond prepackaged queries and create queries that answer the questions relevant to their organization. The BindView bv-Control products offer unmatched flexibility in customizing queries. Two significant examples are the registry and event log reporting capabilities of the product.

- 1 From the **BindView RMS Risk Assessment and Control** folder, expand the **Pre-Defined** folder.
- 2 Expand the **bv-Control for Windows** folder.
- 3 Expand the Security Best Practices folder.
- 4 Expand the Event Logs Security folder.

The **Event Logs Security** folder contains several reports that will help you analyze application, security, and system log entries on your Windows servers and workstations.

- 5 Double-click the Logon Failures within the last 7 days.
- 6 In the Available Tasks section of the details pane, click Run And View As Grid.



The dataset appears with the name of the user account that caused the event, the machine name of the computer on which the event occurred, the time and date the event occurred, the event's numeric code (this code is defined by the process that generated the event), and a detailed description of what caused the event.

This query can be especially useful for forensic purposes, when a security event has occurred. The data extracted is presented in a way that gives the user information that can help determine the root cause of the issue and the identity of the machine. Thus, the query helps assist in identifying if the issue has been caused by accident or malice.

🔳 Logq	Logon Failures within the Last 7 days						
<u>G</u> rid <u>E</u> r	dit <u>V</u> iew <u>H</u> elp)					
🚉 🍯	3 😽 🛷 🚺	🎽 📰 🛄 📦 🛼	A 🤋 🔲				
	User Name	Machine Name	Event Date/Time	Event ID	Event Description	_	
324	SYSTEM	GENERIC	8/1/2003 1:00	529	Logon Failure:	Þ	
325	SYSTEM	GENERIC	8/1/2003 1:00	529	Logon Failure:	Þ	
326	SYSTEM	GENERIC	8/1/2003 1:00	529	Logon Failure:	Þ	
327	SYSTEM	GENERIC	8/1/2003 2:06	529	Logon Failure:	Þ	
328	SYSTEM	GENERIC	8/1/2003 10:43	529	Logon Failure:	Þ	
329	SYSTEM	GENERIC	8/1/2003 10:43	529	Logon Failure:	Þ	
330	SYSTEM	GENERIC	8/1/2003 10:43	529	Logon Failure:	Þ	
331	SYSTEM	GENERIC	8/1/2003 10:43	529	Logon Failure:	Þ	
332	SYSTEM	GENERIC	8/1/2003 10:43	529	Logon Failure:	Þ	
333	SYSTEM	GENERIC	8/1/2003 10:43	529	Logon Failure:	Þ	
334	SYSTEM	GENERIC	8/1/2003 10:43	529	Logon Failure:	Þ	
335	SYSTEM	GENERIC	8/1/2003 10:43	529	Logon Failure:	Þ	
336	SYSTEM	GENERIC	8/1/2003 10:43	529	Logon Failure:	Đ	
337	SYSTEM	GENERIC	8/1/2003 10:43	529	Logon Failure:	Đ	
338	SYSTEM	GENERIC	8/1/2003 10:43	529	Logon Failure:	E	
339	SYSTEM	GENERIC	8/1/2003 10:43	529	Logon Failure:	Þ	
340	SYSTEM	TKL-VM5-W2K-SRV	7/25/2003 11:19	529	Logon Failure:	Þ	
341	SYSTEM	TKL-VM5-W2K-SRV	7/25/2003 11:19	529	Logon Failure:	Þ	
342	SYSTEM	TKL-VM5-W2K-SRV	7/25/2003 17:28	529	Logon Failure:	Þ	
343	SYSTEM	TKL-VM5-W2K-SRV	7/25/2003 17:28	529	Logon Failure:	Þ	
344	SYSTEM	TKL-VM5-W2K-SRV	7/25/2003 17:28	529	Logon Failure:	Þ	
345	SYSTEM	TKL-VM5-W2K-SRV	7/25/2003 17:28	529	Logon Failure:	Þ	
346	SYSTEM	TKL-VM5-W2K-SRV	7/25/2003 17:28	529	Logon Failure:	Þ	
347	SYSTEM	TKL-VM5-W2K-SRV	7/25/2003 17:28	529	Logon Failure:	•	
348	SYSTEM	TKL-VM5-W2K-SRV	7/25/2003 17:28	529	Logon Failure:	Þ	
349	SYSTEM	TKL-VM5-W2K-SRV	7/25/2003 17:28	529	Logon Failure:	Þ	
350	SYSTEM	TKL-VM5-W2K-SRV	7/25/2003 17:28	529	Logon Failure:	Þ	
351	SYSTEM	TKL-VM5-W2K-SRV	7/25/2003 17:28	529	Logon Failure:	Þ	
352	SYSTEM	TKL-VM5-W2K-SRV	7/25/2003 17:28	529	Logon Failure:	Þ	
353	SYSTEM	TKL-VM5-W2K-SRV	7/25/2003 17:28	529	Logon Failure:	Þ	
354	SYSTEM	TKL-VM5-W2K-SRV	7/25/2003 22:03	529	Logon Failure:	Þ	
355	SYSTEM	TKL-VM5-W2K-SRV	7/25/2003 22:03	529	Logon Failure:	p 💌	
F	Record 1 of 42	22 Message	es: 31			Messages	

- 1 Click the **Modify Query** button on the grid toolbar.
- 2 The Query Builder appears with the grid fields in the Selected Fields box.



3 On the Query Builder, click the **Filter Specification** tab.

Note the expression at the lower part of the dialog, "Event ID is equal to 529." This is a numeric code that is defined by the process that generates the event.

Query Builder - Logon Failures within the Last 7 days	X
Field Specification Filter Specification Sort Specification Scope	
Filter Field Names: Apply	Fieldlafe
	Add
Operator Expression	Modify
AND Event Date/Time Days Before Today Greater or Equal To 7	Remove
	Remove All
	Descriptor
	AND/08
Add () Remove ()	
OK Cancel	Help

1 You can modify this expression by double-clicking on the field or selecting the field and clicking the **Modify...** button.

The Filter Term Definition dialog appears.

Filter Term Definition			X
Specific Value	C Another Field	C Prompt User	ОК
Event ID			Cancel
Equal To]		Help
Specify a value:			
529			

- **2** Modify the Event ID then specify a value.
- **3** Click **OK** to close the dialog.

The second half of the previous expression can also be modified.

1 Double-click on the field or click the **Modify...** button.

The **Filter Term Definition** dialog for the expression appears.

Filter Term Definition				X
Specific Value	C Special Value	C Another Field	C Prompt User	OK
Size (Bytes)				Cancel
Greater Than	•			Help
Specify a value:				
,				

- **2** Modify the Event Date/Time by selecting when you want the event to take place, then specify the value.
- **3** Click **OK** to close the dialog.

Content and Capacity Management

Another area of concern in rapidly changing IT organizations is assessing capacity. This includes both reviewing available capacity and determining how well the capacity usage fits with the business needs of the organization. BindView provides the administrator with the ability to not only identify these cases, but to directly remediate them.

Scenario 6: Disk Space Analysis and Management

Organizations maintain a significant investment in storage space in the form of servers, disarrays or SANs, backup systems, and man-hours. Locating servers that are running low on disk space and/or locating inappropriate or wasteful disk space allows the administrator to reduce the need to add new disk space and can shorten backup cycles.

- 1 From the **BindView RMS Risk Assessment and Control** folder, expand the **Pre-Defined** folder.
- 2 Expand the **bv-Control for Windows** folder.
- 3 Expand the Storage Analysis folder.
- 4 Double-click the Server Disk Space folder.
- 5 Double-click Disk Space on Domain Controllers to run the query.
- 6 In the Available Tasks section of the details pane, click Run And View As Grid.



The dataset appears with the disk space summary, free disk space, disk space usage, and disk space totals.

🛄 Disk	Disk Space on Domain Controllers								
Grid Ed	Grid Edit View Help								
] 🗟 🍯	ð 🗞 🧳 🛅 👯 🛄 🎕	😼 🗛 🧐 🛙]						
	Domain/Workgroup Name	Machine Name	Machine Is PDC? (Browser)	Machine Is BDC? (Browser)	Disk Space Summary	Disk Space Free (KB)	Disk Space In Use (KB)	Disk Space Total (KB)	
1	SOUTHWESTERNCOL	ANTONITO	No	Yes	[Form] 🛛 🗗	688,542	1,355,650	2,044,192	
2	SOUTHWESTERNCOL	CORTEZ	Yes	No	[Form]	533,003	1,511,188	2,044,192	
	Record 1 of 2 M	essages: 0							

This report is beneficial especially when performing a compliance check concerning the presence of unauthorized filed types. Additionally, this report can be used when performing routine maintenance by determining which files have not been accessed in a certain amount of time.

You can also retrieve summary data on **Directories** and **Files**. Reports that specify directory size and amount of files in a directory are available in the **Storage Analysis** folder. In addition, in the same folder there are **File Detail** reports that specify common files, files greater than a specific size, and days since your files were last accessed

- 1 From the **BindView RMS Risk Assessment and Control** folder, expand the **Pre-Defined** folder.
- 2 Expand the **bv-Control for Windows** folder.
- 3 Expand the Storage Analysis folder.
- 4 Double-click the **File Details** folder.
- 5 Double-click Files Greater than 1MB and Not Accessed within 90 Days.
- 6 In the Available Tasks section of the details pane, click Run And View As Grid.



The dataset appears with the domain or workgroup membership of the machine containing the file, the file's parent machine name, the full path name of the file, whether the owner of

the file is a valid account, the date and time the file was last accessed, and the logical size of the file in bytes.

	Files Greater Than 1MB and Not Accessed within 90 Days									
Gri	Grid Edit View Help									
		Domain/Workgroup Name	Machine Name	File Name	Owner	Owner SID	Last Accessed	Size		
				(With Path)		is Valid?	Date/Time	(Bytes)		
	1	NORTHEASTCOLORA	CENTRAL-CITY	C:\Document n	NORTHEASTC N	Yes	2/12/2003 12:09	1.311.348	1	
	2	NORTHEASTCOLORA	CENTRAL-CITY	C:\Document	NORTHEASTC N	Yes	2/12/2003 12:09	1,908,815		
	3	NORTHEASTCOLORA	CENTRAL-CITY	C:\Document	NORTHEASTC N	Yes	2/12/2003 12:11	1,311,348		
	4	NORTHEASTCOLORA	CENTRAL-CITY	C:\Document	NORTHEASTC N	Yes	2/12/2003 12:11	1,908,815		
	5	NORTHEASTCOLORA	CENTRAL-CITY	C:\Document	NORTHEASTC N	Yes	2/12/2003 15:41	1,311,348		
	6	NORTHEASTCOLORA	CENTRAL-CITY	C:\Document 🛛	NORTHEASTC	Yes	2/12/2003 15:41	1,908,815		
	7	NORTHEASTCOLORA	CENTRAL-CITY	C:\Document 🛛	NORTHEASTC	Yes	2/12/2003 12:15	2,532,520		
	8	NORTHEASTCOLORA	CENTRAL-CITY	C:\Document 🖪	NORTHEASTC	Yes	2/12/2003 11:56	2,618,520		
	9	NORTHEASTCOLORA	CENTRAL-CITY	C:\Document 🖪	CENTRAL-CIT'	Yes	2/12/2003 8:44	1,129,040		
	10	NORTHEASTCOLORA	CENTRAL-CITY	C:\Document 🛛	CENTRAL-CIT'	Yes	3/28/2002 9:06	2,039,400		
	11	NORTHEASTCOLORA	CENTRAL-CITY	C:\Document 🗗	CENTRAL-CIT'	Yes	3/28/2002 9:06	1,611,880		
	12	NORTHEASTCOLORA	CENTRAL-CITY	C:\Document 🛛	CENTRAL-CIT'	Yes	3/28/2002 9:07	1,189,992		
	13	NORTHEASTCOLORA	CENTRAL-CITY	C:\Document 🗗	CENTRAL-CIT'	Yes	3/28/2002 9:06	2,931,304		
	14	NORTHEASTCOLORA	CENTRAL-CITY	C:\Document 🗗	CENTRAL-CIT'	Yes	3/28/2002 9:30	4,217,919		
	15	NORTHEASTCOLORA	CENTRAL-CITY	C:\Document 🗗	CENTRAL-CIT'	Yes	3/28/2002 9:08	3,424,344		
	16	NORTHEASTCOLORA	CENTRAL-CITY	C:\Document 🗗	CENTRAL-CIT'	Yes	3/28/2002 9:07	5,473,872		
	17	NORTHEASTCOLORA	CENTRAL-CITY	C:\Document 🖪	CENTRAL-CIT'	Yes	3/28/2002 9:05	2,513,264		
	18	NORTHEASTCOLORA	CENTRAL-CITY	C:\Document 🗗	CENTRAL-CIT'	Yes	3/28/2002 8:40	3,492,199		
·	19	NORTHEASTCOLORA	CENTRAL-CITY	C:\Program F 🗗	NORTHEASTC D	Yes	2/12/2003 11:54	2,756,663		
	20	NORTHEASTCOLORA	CENTRAL-CITY	C:\Program F 🛛	NORTHEASTC	Yes	2/12/2003 11:54	2,105,420	-	
	F	Record 1 of 581	Messages: 1]				Messages		

You can modify this query's scope to report on a single directory on all machines in a container.

- 1 Click the **Modify Query** button on the grid toolbar. The **Query Builder** appears.
- 2 Click the Scope Tab.
- **3** Expand the **Advanced Scopes** folder.

4 Double-click the Scope to a Directory on Machines in a Container folder.

Query Builder - Files Greater Than 1MB and Not Accessed within 90 Days	×				
Field Specification Filter Specification Scope Available Item(s) Image: Scope State Stat					
Scope to a File on Machines in a Container Scope to a Machine in a Domain Scope to a Directory on a Machine in a Domain Scope to a File on a Machine in a Domain Scope to a File on a Machine in a Workgroup Add Scope Configure Dynamic Indexing					
Selected Item(s)					
Remove Scope Save as Named Scope Additional Settings OK Cancel Help					

The **File Scoping Options** dialog appears. Use this dialog to limit the scope of the query to files in a specified directory or files on machines in the container.

Additional Settings
File Scoping Options - Directory
Container (EX: Corp.com/OU)
Container Level
 Files on machines in this container only
$\mathbf{C}_{\rm subcontainers}^{\rm Files}$ on machines in this container and all of its
Directory Path
File Level
 Files contained in this directory only
$\mathbf{C}_{\text{subdirectories}}^{\text{Files contained in this directory and its}}$
 All directories below this directory
C Limit levels below this directory
Levels 1
Files to include
OK Cancel Help

- 5 Click OK.
- 6 On the Query Builder, click the Filter Specification tab.

7 Change the filter from 1MB to 100MB by double-clicking the **Size (Bytes) Greater Than** 1000000 expression. The **Filter Term Definition** dialog appears.

ter Term Definition				<u>,</u>
Specific Value	C Special Value	C Another Field	C Prompt User	OK
iize (Bytes)				Cancel
Greater Than	•			Help
Specify a value:				
100				

- 8 In the **Specify a Value** field type in **100**. Click **OK**.
- 9 Click **OK** to rerun the query.

The **Query Options** dialog appears.

Query Options	×
View As-	Run
Grid	Modify
Chart Chart Settings	Save
C Report	Help
	Cancel

10 Click Run.

11 The dataset appears with the updated information displayed.

	🗐 Files Greater Than 1MB and Not Accessed within 90 Days								
Grid	l Ed	lit View Help							
	1 爹	ð 🍻 🛷 🛅 🚼	🛄 📦 🎭 🖌	\$					
		Domain/Workgroup Name	Machine Name	File Name (With Path)	Owner	Owner SID is Valid?	Last Accessed Date/Time	Size (Bytes)	•
	1	NORTHEASTCOL D	CENTRAL-CI 🖪	C:\Docume 🕨	NORTHEASTCOLORAV 🖪	Yes	2/12/2003 16:09	32,768	
	2	NORTHEASTCOL D	CENTRAL-CI	C:\Docume 🗗	NORTHEASTCOLORAV 🖪	Yes	2/12/2003 11:51	141	
	3	NORTHEASTCOL 🛛	CENTRAL-CI	C:\Docume 🗗	NORTHEASTCOLORAV	Yes	2/12/2003 11:51	10,405	
	4	NORTHEASTCOL 🛛	CENTRAL-CI	C:\Docume 🗗	NORTHEASTCOLORAV	Yes	2/12/2003 11:50	2,570	
	5	NORTHEASTCOL	CENTRAL-CI	C:\Docume 🗗	NORTHEASTCOLORAV	Yes	2/12/2003 11:51	160	
	6	NORTHEASTCOL	CENTRAL-CI	C:\Docume 🗗	NORTHEASTCOLORAV	Yes	2/12/2003 11:51	737	
	7	NORTHEASTCOL 🛛	CENTRAL-CI	C:\Docume 🗗	NORTHEASTCOLORAV	Yes	2/12/2003 11:50	804	
	3	NORTHEASTCOL 🛛	CENTRAL-CI	C:\Docume 🗗	NORTHEASTCOLORAV	Yes	3/19/2003 14:31	48,138	
1	3	NORTHEASTCOL 🛛	CENTRAL-CI	C:\Docume 🗗	NORTHEASTCOLORAV	Yes	2/12/2003 16:17	5,640	1
1	0	NORTHEASTCOL 🛛	CENTRAL-CI	C:\Docume 🗗	NORTHEASTCOLORAV	Yes	2/12/2003 12:59	101	
1	1	NORTHEASTCOL 🛛	CENTRAL-CI	C:\Docume 🗗	NORTHEASTCOLORAV	Yes	2/12/2003 14:34	127	1
1	2	NORTHEASTCOL 🛛	CENTRAL-CI	C:\Docume 🗗	NORTHEASTCOLORAV	Yes	2/12/2003 14:34	163	1
1	3	NORTHEASTCOL 🛛	CENTRAL-CI	C:\Docume 🗗	NORTHEASTCOLORAV	Yes	2/12/2003 11:51	119	
1	4	NORTHEASTCOL 🛛	CENTRAL-CI	C:\Docume 🖪	NORTHEASTCOLORAV	Yes	2/12/2003 11:51	113	-
	Re	cord 1 of 10714	Message	s: 1				Messages	

Security of Sensitive Files and Directories

Due to privacy regulations mandated by HIPAA, GLBA, and California SB 1386, it is necessary to audit which users and groups have access to sensitive corporate files and directories, such as human resources files. An audit report of this nature requires expert knowledge of Microsoft Windows and Active Directory security, and can take days or even weeks to complete for a small set of directories. An accurate analysis of this type of entitlement information should take into account whether access is local or through a file share as well as the effective group membership. The bv-Control for Windows product automates this analysis to allow the users to quickly produce an audit report detailing all users and/or groups with effective access to sensitive files and directories, what level of access is granted, and evidence of how it was obtained.

Scenario 7: Audit Users and Groups that Have Access to Sensitive Files and Directories

- 1 From the **BindView RMS Risk Assessment and Control** folder, expand the **Pre-Defined** folder.
- 2 Expand the bv-Control for Windows folder.
- 3 Expand the Security and Best Practices folder.
- 4 Double-click the File System Security folder.
- 5 Double-click UserEntitlement Users with Full Control of sensitive files and directories.
- 6 In the Available Tasks section of the details pane, click Run And View As Grid.



The ability to filter on specific permissions can be particularly useful when there is a need for granularity in determining whether a User or Group has appropriately assigned privileges down to a specific file.

Modify this query to include a specific file or server into the scope. In addition, you will add a filter to the query to add specific levels of access by filtering on any of the permission fields.

7 From the **Available Tasks** section of the details pane, click **Modify Query Definition**.

The Query Builder appears.



- 8 Click the Scope Tab.
- **9** Expand the **Active Directory** folder to display files that you want to include into the scope.
- 10 In this case we will navigate down to the **Documents and Settings** container. Click the **Add Scope** button on the Query Builder.

The Additional Settings dialog appears.

Additional Settings
File System Scoping Options - Directory
Search Level Search this directory only Search this directory and its subdirectories This directory and every directory below it Limit levels below this directory Levels
Object types to include Directories in specified level Files in specified level Names to include
OK Cancel Help

Use this dialog to specify how far down in the file's directory structure that you want to query.

- **11** Select from the available file scoping options and click **OK** to close the dialog.
- **12** On the Query Builder, select the **Filter Specification** tab.
- 13 Expand the All Fields folder.
- **14** Select the **Permission (Basic) Full Control** field. This field will return all records of users that have full control access of the selected file or directory.



15 Click Add.

34 bv-Control for Windows Evaluation Guide

The Filter Term Definition dialog appears.

Filter Term Definition			×
Specific Value	C Another Field	C Prompt User	OK
Permission (Basic): Full Control			Cancel
Equal To	Yes	•	Help

Ensure that **Equal To** and **Yes** are selected in the drop-down lists.

- 16 Click **OK** to close the dialog.
- **17** Click **OK** to close the Query Builder.

The **Query Options** dialog appears.

Query Options		×
View As		Run
Grid		Modify
C Chart	Chart Settings	Save
C Report		Halp
		Lancel

18 Click Run.

The query will rerun. The fields you selected will display in the grid.

📃 Us	erEntitlement ·	- Users with Ful	l Control of sens	itive files and directories	;		_	
Grid	Edit View Hel	p						
	🎯 🍓 🛷 I	🛅 📴 📕	🏟 🐞 🗛 🧐					
	Domain	Machine	Object Name	Account Name	Account Type	Effective Permissior	ns Evidence	
	Name	Name		(Qualified)		Summary <list></list>	<form></form>	
1	SOUTHV 🕨	LEADVILLE	C:\Documen 🗗	COLORADO\Admini 🛛	Global User	[List]	[Form]	Þ
2	SOUTHV 🛛	LEADVILLE	C:\Documen 🗗	COLORADO\bvu_q_ 🛛	Global User	[List]	[Form]	Þ
3	SOUTHV 🛛	LEADVILLE	C:\Documen 🗗	COLORADO\maer-c 🛛	Global User	[List]	[Form]	Þ
4	SOUTHV 🛛	LEADVILLE	C:\Documen 🗗	LEADVILLE (Adminis 🛛	Local User	[List]	[Form]	Þ
5	SOUTHV 🛛	LEADVILLE	C:\Documen 🗗	LEADVILLE\Adminis 🗗	Built-in Group	[List]	[Form]	Þ
6	SOUTHV 🛛	LEADVILLE	C:\Documen 🗗	SOUTHWESTERN	Global User	[List]	[Form]	Þ
7	SOUTHV 🛛	LEADVILLE	C:\Documen 🗗	SOUTHWESTERN	Global User	[List]	[Form]	Þ
8	SOUTHV 🛛	LEADVILLE	C:\Documen 🗗	SOUTHWESTERN	Global User	[List]	[Form]	Þ
9	SOUTHV 🛛	LEADVILLE	C:\Documen 🗗	SOUTHWESTERN	Global Group	[List]	[Form]	Þ
10	SOUTHV 🛛	LEADVILLE	C:\Documen 🗗	SOUTHWESTERN	Global User	[List]	[Form]	Þ
11	SOUTHV 🛛	LEADVILLE	C:\Documen 🛛	SOUTHWESTERN	Global User	[List]	[Form]	Þ
12	SOUTHV 🛛	LEADVILLE	C:\Documen 🛛	SYSTEM	Well Known Grc 🛛	[List]	[Form]	Þ
13	SOUTHV 🛛	LEADVILLE	C:\Documen 🗗	COLORADO\Admini 🖪	Global User	[List]	[Form]	Þ
14	SOUTHV 🛛	LEADVILLE	C:\Documen 🗗	COLORADO\bvu_q_ 🛛	Global User	[List]	[Form]	Þ
15	SOUTHV 🛛	LEADVILLE	C:\Documen 🗗	COLORADO\maer-c 🛛	Global User	[List]	[Form]	Þ
16	SOUTHV 🛛	LEADVILLE	C:\Documen 🗗	LEADVILLE\Adminis 🛛	Local User	[List]	[Form]	Þ
17	SOUTHV 🛛	LEADVILLE	C:\Documen 🛛	LEADVILLE\Adminis 🛛	Built-in Group	[List]	[Form]	Þ
18	SOUTHV	LEADVILLE	C:\Documen 🛛	SOUTHWESTERN	Global User	[List]	Form]	Þ
19	SOUTHV	LEADVILLE	C:\Documen	SOUTHWESTERN	Global User	[List]	[Form]	Þ
20	SOUTHV	LEADVILLE	C:\Documen 🛛	SOUTHWESTERN	Global User	[List]	[Form]	•
	Record 1 of 4	103	Messages: 8				Message:	s

Security of Sensitive Files and Directories 35

© 2003, 2004 BindView Corporation. All rights reserved.

The same scenario can be used for identifying groups with effective access to files and directories. Simply run the **GroupEntitlement - Groups with Full Control of sensitive files and directories** pre-defined query.

Active Directory® Security Principle Analysis

Configuration best practices, patch management, and change control processes are all necessary, but these and other measures cannot ensure the security and availability of critical IT assets if users are granted excessive and inappropriate privileges. Therefore, it is vital that routine assessments are performed to determine who has the ability to manage objects in Active Directory to ensure privileges are only granted to users with an appropriate business need. The bv-Control for Active Directory product automates this analysis allowing administrators to proactively identify and address cases where excessive privileges have been granted.

Scenario 8: Assess Users and Groups that are able to Create, Delete, and Manage Active Directory Groups

This analysis allows a security professional to audit users and groups that have a particular privilege to a security principle.

Run a query that identifies trustees that have been assigned as an administrator on the domain or organizational unit.

- 1 From the **BindView RMS Risk Assessment and Control** folder, expand the **Pre-Defined** folder.
- 2 Expand the bv-Control for Active Directory folder.
- 3 Expand the Security and Best Practices folder.
- 4 Double-click the **Users** folder.
- 5 Double-click Active Directory Security Principle Analysis.
- 6 In the Available Tasks section of the details pane, click Run and View as Grid.



The grid appears with the fields that included in the query.

Active Directory® Security Principle Analysis 37

- 7 Select the **Modify Query** button on the toolbar. The Query Builder appears.
- 8 Select the Field Specification Tab.
- 9 Expand the **All Fields** folder.
- 10 Select the Is Effective Trustee?... field and click Add.
- **11** The Descriptor dialog appears. Click **Change Descriptor**.

Is Effective Trustee?			×
Descriptor Va	lue C P	rompt Value	OK
			Cancel
			Help
Descriptor:			
	Change Des	criptor	
			J

The **Descriptor: Is Effective Trustee?** dialog appears. Use this dialog to choose the object whose trustees are to be retrieved.

criptor: Is Effective Trustee?	
Select the object whose Trustees are to be retrieved Wy Enterprise Grand ant-america lab Builtin Computers Domain Controllers ForeignSecurityPrincipals ForeignSecurityPrincipals Foreign Data System System Selected Object Selected Object	Select
gnt-canada.gnt-america.lab/Users Select the permissions the security principals should have on the object OK	Permissions Help

12 Browse to the object and click **Select**. The object will display in the **Selected Object** box.

13 Click the **Permissions...** button. The **Select Permissions** dialog appears.



Use this dialog to select the permissions to be used for querying on a specific user, group, or computer and determine whether the security principal account is an effective trustee on the Active Directory object selected in the descriptor dialog.

- **14** Click on the **Create, delete, and manage groups** permission and click **Select**. The permission will be added to the Selected Permissions box.
- 15 Click OK to close the Select Permissions dialog.
- 16 Click OK to close the Descriptor dialog.
- 17 Click **OK** to close the next dialog.
- The Filter Term Definition dialog appears.

Filter Term Definition		×
Specific Value	C Prompt User	ОК
Is Effective Trustee?		Cancel
Is Yes		Help

- 18 Ensure that the Is Yes value is selected in the drop-down list. Click OK to close the dialog.
- 19 On the Query Builder, click the Scope tab.
- 20 Scope to a user OU and click Add Scope.

The **Additional Settings - Scope Level Options** dialog appears. Use this dialog to determine the depth of the level that will be queried in the scope.



- **21** Make your selection and click **OK** to close the dialog and return to the Query Builder.
- **22** The **Query Options** dialog appears. Click **Run** to generate the query.
- 23 The Query Completion Wizard appears. Click Next to complete the query.

The query wizard will guide you through the same procedure explained above. The dataset will appear with the value in the **Effective Trustee?... field** as **Yes**.

🔲 Activ	ve Directory Security Principle Analysis - modified1				_ 🗆 🗙
<u>G</u> rid <u>E</u>	dit <u>V</u> iew <u>H</u> elp				
] 🗟 🧃	2 😹 A 🕼 🛄 😫 🔂 🗛 🗩				
	Active Directory Path	Security Principal Name	Security Principal Account Type	Is Effective Trustee? For fpanda.qfe/Users - Permissions: [Create, delete, and manage groups]	
1	LDAP://fpanda.qfe/CN=Robert M. Tanner3,CN=Users,DC=fpanda,DC=qfe	Robert M. Tanner3	User	Yes	
2	LDAP://fpanda.qfe/CN=Administrator,CN=Users,DC=fpanda,DC=qfe	Administrator	User	Yes	
3	LDAP://fpanda.qfe/CN=Enterprise Admins,CN=Users,DC=fpanda,DC=qfe	Enterprise Admins	Group	Yes	
4	LDAP://fpanda.qfe/CN=Robert M. Tanner,CN=Users,DC=fpanda,DC=qfe	Robert M. Tanner	User	Yes	
5	LDAP://fpanda.qfe/CN=Robert M. Tanner2,CN=Users,DC=fpanda,DC=qfe	Robert M. Tanner2	User	Yes	
	Record 1 of 5 Messages: 0		•		

Web Services

The recent publication of serious vulnerabilities in Microsoft-IIS means that a majority of Internet sites can be remotely exploited if not patched. Daily tasks such as keeping up with patch-level versions, identifying the machines with IIS installed, and troubleshooting accesscontrol problems on the website are further complicated because there is no central console for multiple machines, configuration settings drift over time, and there is no efficient way to manage Web services remotely-maintenance is very "hands-on."

Web Services, Microsoft-based platforms, helps Web administrators and information security groups manage Web services configuration settings, diagnose website problems, and enforce security policies.

Web Services can:

- Report patch levels and versions
- Identify changes to virtual files, directories, and shares
- Provide IIS server lock down templates based on guidelines from the National Security Agency (NSA)
- Drill-down to details regarding NTFS permissions-specific access rights
- Identify unauthorized ISAPI filters, default samples installed, and unnecessary default services

Identifying Changes to Virtual Files, Directories, and Shares

Web Services provides the ability to use MD5 Checksum encryption to determine changes to virtual files, directories, and shares. Encryption technology is one of the most accurate methods to use in determining changes to Web content.

Every morning, the Web administrator schedules a baseline report to run on all virtual files, directories, and shares to identify what files have changed in the last 24 hours. Knowing what has changed in the virtual environment is valuable information when running daily maintenance routines, responding to an intrusion-detection alert, or troubleshooting a technical problem with the Web site.

Scenario 9: Using MD5 Checksum Functionality to Show Variances in Data

Generate a baseline report by creating a query on a data sample from the virtual files, directories, and shares. Use the MD5 checksum functionality to show variances in the data.

1 On the BindView RMS Console toolbar, click the **New Query 2** icon.

The Select Data Source dialog displays.



2 Select the IIS Virtual Directories data source, and click OK.

The **Query Builder** dialog displays.

Query Builder - Untitled by-Control for Windows IIS Virtual Directories Query	X
Field Specification Filter Specification Sort Specification Scope	
Filter Field Names: Apply	
Available Fields IIS Vitual Directories ASP.NET Web.Config IIS vitual Directories AIF Fields Application Options Image: Application Settings Image: Authentication Image: Custom Image: Home Directory	Field Info
IP Address and Domain Restrictions Log File Options Ratings	Add
Selected Fields	Remove
Domain/Workgroup Name Machine Name Diplot Type ADSI Path	Remove All
Dbject Name	
OK Cancel	Help

3 Expand the **All Fields** folder to display all available fields.

The **All Fields** container opens and displays all available fields.

Query Builder - Untitled by-Control for Windows IIS Virtual Directories Query	×
Field Specification Filter Specification Sort Specification Scope	
Filter Field Names: Apply	
Available Fields	Field Info
	Add
Selected Fields	Remove
Uomain/Workgroup Name Machine Name Diject Type	Remove All
Dbject Name	Descriptor
	Field Details
OK Cancel	Help

4 Select the **MD5 Checksum** field and click **Add**.

The MD5 Checksum field is added to the **Selected Fields** box.

5 Select the **Scope** tab.

The **Query Builder - Scope Tab** dialog displays.

Query Builder - Untitled by-Control for Windows IIS	5 Virtual Directories Query
Field Specification Filter Specification Sort Specification	n Scope
Available Item(s)	
Pefault Scope	
Microsoft Windows Network	
Active Directory	
Advanced Scopes	
Add Scope	Configure Dynamic Indexing
Selected Item(s)	
Default	
Remove Scope Save as Named Scope	Additional Settings
P	OK Cancel Help

6 Expand the **Advanced Scopes** container.

The Advanced Scopes container opens and displays the available Advanced Scopes for the selected data source.

7 Select the type of Advanced Scope you want to add to the query and click **Add Scope**.

The **Additional Settings** dialog for that scope displays. The contents of the dialog will differ depending on which Advanced Scope type you choose. In this example, we selected Scope to a Machine in a Domain.

Additional Settings
Virtual Directory Scoping Options - Machine
Virtual Directory Level
 Virtual Directories Only
O Virtual Directories and Folders
C Virtual Directories, Folders and Files
Machine Name
OK Cancel Help

8 Enter the relevant information for the Advanced Scope and click **OK**.

The Advanced Scope item is added to the current scope as shown in the **Scope Tab** - **Selected Item** dialog.

Query Builder - Untitled by-Control for Windows IIS Virtual Directories Query	x
Field Specification Filter Specification Sort Specification Scope	
- Available Item(s)	
Active Directory Advanced Scopes Advanced Scopes Scope to a Domain Scope to a Web Site on Machines in a Container Scope to a Virtual Directory on Machines in a Container Scope to a Web Site on a Machine in a Domain Scope to a Web Site on a Machine in a Domain Scope to a Web Site on a Machine in a Domain Scope to a Machine in a Workgroup Scope to a Wirtuel Directory on a Machine in a Morkgroup	
Scope to a Virtual Directory on a Machine in a Workgroup	
Add Scope Configure Dynamic Indexing	
Selected Item(s)	
Remove Scope Save as Named Scope Additional Settings	
OK Cancel Help	

9 Click OK.

The Query Options dialog displays.

Run
Modify
Save
Help
Cancel

10 click Run to generate and view the report.

Run this report daily and compare the baseline values to determine if any changes have occurred in the MD5 Checksum field. Any changes in the field value may indicate problems that have been caused by content changes on the Web site.

Using an IIS Server Lock Down Template

Web Services provides valuable security knowledge and experience to the Web administrator in the form of pre-defined queries for locking down an IIS server. The BindView elite security team, RAZOR, has created a template of reports to lock down an IIS server based on best practices issued by the National Security Agency (NSA).

A new IIS server needs to be moved online or an existing IIS server has been brought down for maintenance. Before placing the new or rebuilt IIS server online, the Web administrator can run an audit on the server (in the test environment) to ensure that all default settings have been removed and patches have been properly applied.

Scenario 10: Determine if Settings and Patches are Applied Correctly

Run a pre-defined NSA IIS5 report to determine if all of the default settings have been removed from the server and that all patches have been applied correctly.

- 1 From the BindView RMS Console, navigate to the **Security Best Practices NSA IIS5** folder.
- 2 Expand the **Web Services Checks** folder.

The available pre-defined query reports are displayed.



- **3** Select the query report that you want to run and right-click.
- 4 On the shortcut menu select **Run**, **And View As Grid**.

The query building process starts. The **Task Status** dialog is displayed.

Task St	atus - ADELOSSA-TEST2			
Actions				
Job Ide	Name	Туре	Start 💎	End 🔺
2621	Administration web site configured to allow	Query	7/7/2004 2:52:46 PM	
2537	Detailed Machine Configuration	Query	7/1/2004 2:57:20 PM	7/1/2004 2:59:15 PM
2536	Detailed Machine Configuration	Query	7/1/2004 2:57:18 PM	7/1/2004 2:59:15 PN 🖵
1				
🕘 Error	🧧 Partially Successful 🛛 🔵 Successful	🕗 Incomplete	🔷 Waiting 🛛 🔵 Runnir	ng

If you selected View as Grid, your report will be displayed when completed. If you selected View as Chart, when your report is complete, the Chart Builder Wizard will be launched. Use the Wizard to create the look of your chart.

Reviewing Permissions to Web Site Home Directory

In a Web administration team environment, managing rights and permissions to the Web Site home directory is essential. Web Services provides a centralized, granular view of NTFS permissions, and specific access rights.

The Web administrator discovers that several virtual folders have been deleted in error. To identify the point of failure, an audit is needed to identify user accounts that have more than Read permissions to the Web Site home directory.

Scenario 11: Determine Users with Read Permissions to the Web Site Home Directory

- 1 From the BindView RMS Console, navigate to the **Security Best Practices NSA IIS5** folder.
- 2 Expand the Web Services Checks folder.

The available pre-defined query reports are displayed.



The available pre-defined query reports are displayed.

3 From the list of reports, select the **Web site Home directory allows more than Read permission** and right-click.

Image: Second Secon	🏽 BindView - [BindView RM5\Risk Assessment and Control\Pre-Defined\by-Control for Windows\Web Services\Security Be 💶 🗖 🗙						
Action View Image: Constraint of the second s	Console Window Help						
Tree Web Services Checks Content of "\Pre-Defined\bv-Control for Windows\Web Service BindView RMS Name Image: Service Checks Name Image: Service Checks Configured to include server port Image: Service Checks Name Image: Service Checks<	Action View ← → € 🖬 🖻 🗗 🕄 🕞 😤 🗊 🦉 🍓 🕱 🅎						
Wame Image: Second se	Tree	eb Services Checks – Content of	"\Pre-Defined\bv-Control fo	r Windows\Web Services\Se			
Image: Patch Management Image: Patch Management Image: Patch Management Imagement	Bindview RM5 Risk Assessment and Control All User Items Pre-Defined by-Control for Windows Configuration Management Documentation & Disaster Recovery Getting Started Historical Datasets and Internal Fields Patch Management Security Best Practices Web Services Web Services Getting Started Getting Started	ame Web site extended logging not o Web site has parent paths enab Web site site site site site site Web site site site site site site site site	onfigured to include server onfigured to include time onfigured to include time to onfigured to include URI st onfigured to include URI st onfigured to include user n led And View As Grid And View As Grid And View As Chart And Print And Export And Export	port aken uery em ame esn't log authoring actions esn't manage permissions m			
Security Best Practices - NSA IISS Security Best Practices - NSA IISS Web Services Checks	Security Best Practices - NSA IIS5 Security Best Practices - NSA IIS5 Web Services Checks Windows Checks	W Schedule W Create Shortcut	s remote authoring and we	lesn't require SSL for authori eb site can inherit security se			
Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared Image: Shared <t< td=""><td>Shared Shared Definition Shared Definition Shared Definition Shared Definition Shared Definition</td><td>W Export Definition To W Copy Refresh</td><td>y default documents y enabled in the WWW Se</td><td>ervice Master Properties</td></t<>	Shared Shared Definition Shared Definition Shared Definition Shared Definition Shared Definition	W Export Definition To W Copy Refresh	y default documents y enabled in the WWW Se	ervice Master Properties			

4 Select Run, And View as Grid from the shortcut menus.

The query building process starts. Your report will be displayed when completed.

Identifying Unauthorized ISAPI Filters

Effective ISAPI filter management is required to maintain a secure and properly functioning Web service. Web Services enables proactive ISAPI filter management by delivering a centralized, granular view of ISAPI filter settings and properties.

An unauthorized ISAPI filter, if executed, can cause hours of corrective work. An ISAPI filter executed in the wrong order can cause the Web server to not function properly.

Scenario 12: ISAPI Filter Properties and Settings

1 From the BindView RMS Console, navigate to the **Getting Started** folder.



The available pre-defined query reports are displayed.

2 From the list of reports, select the Web Site ISAPI Filters and right-click.



3 Select **Run**, **And View as Grid** from the shortcut menus.

The query building process starts. Your report will be displayed when completed.

51

Conclusion

The information provided in this Evaluation Guide covers only a few of the features of bv-Control for Windows. However, the scenarios give you an idea of how bv-Control for Windows can help you audit, secure, and manage your Windows environment. As part of the BindView Vulnerability Management solutions family, bv-Control for Windows can assist your organization in properly configuring and protecting your Windows environment, avoid unplanned downtime, and realizing a desired return on IT investments.

Because bv-Control for Windows has a distributed architecture, multiple query engines, and an agent-less architecture, the product can help any size organization maintain control across complex IT environments.

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**

For Technical Support: 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	U.S. and Canada	800-813-5869	
Service	Outside N. America	713-561-4000	
Technical Support	U.S. and Canada	800-813-5867	
	Outside N. America	713-561-4000	
Training/Professional	U.S. and Canada	800-749-8439	
Service	Outside N. America	713-561-4000	
Fax	All Areas	713-561-1000	
E-mail			
Sales	sales@bindview.com		
Training	edu@bindview.com		
Documentation	docs@bindview.com		
Other			
FTP Site	ftp://ftp.bindview.com		
Internet	www.bindview.com		
Postal Mail	BindView 5151 San Felipe, Suite 2500 Houston, TX 77056		

Contacting BindView