Quest

Quest® InTrust 11.4.1

Searching for Events in Repository Viewer

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, **NOTE**, **TIP**, **MOBILE**, or **VIDEO**: An information icon indicates supporting information.

InTrust Searching for Events in Repository Viewer
Updated - December 2019
Version - 11.4.1

Contents

Searching for Events in Repository Viewer

To browse repositories, use the InTrust Repository Viewer application. This console provides tools for event viewing and on-the-spot audit data analysis. Repository Viewer lets you dispense with SSRS-based reporting if your intention is to examine audit data rather than submit formal reports or provide knowledge for regulations compliance.

The primary feature of Repository Viewer is event searching. Searching supports advanced filtering, grouping and sorting. For your searches to work fast, it is recommended that the repository be indexed. (For more information about indexing, see the Repository Indexing for Advanced Search Capabilities topic.)

You can do the following with the search results:

- Save search criteria as searches for future use
- Organize the results in a tree using multi-level grouping
- Apply view filters to further refine the scope of data
- Export the results to create an ad-hoc report

In addition, you can schedule a report to be built from an automatic search and have it delivered by email or saved in a network share.

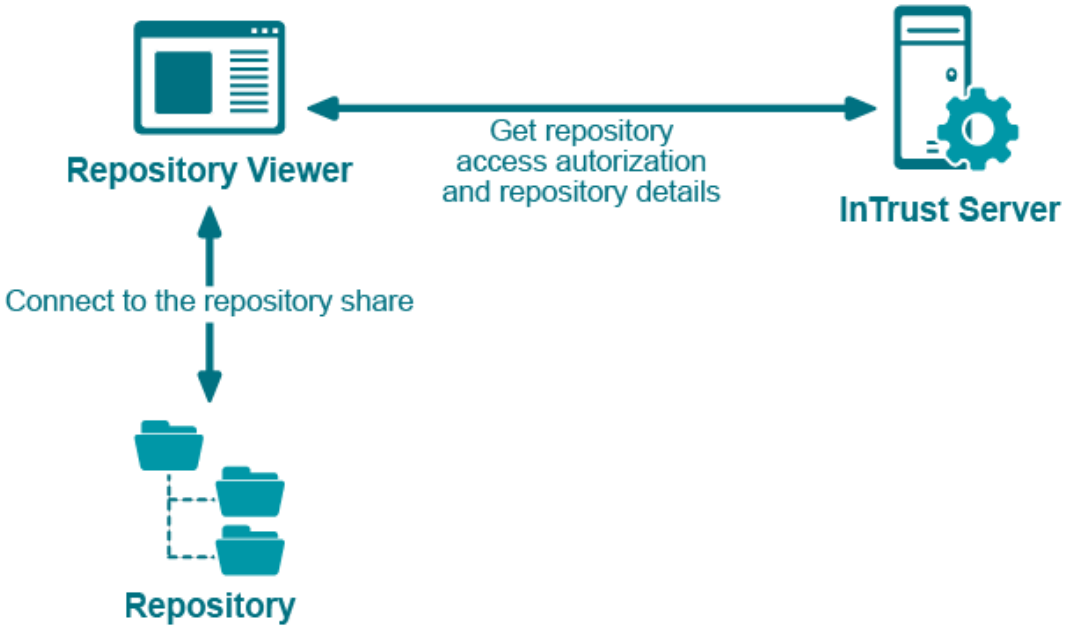
Where to Run Repository Viewer

Repository Viewer does not have complex InTrust component dependencies. However, in the primary use scenario it connects to the repository through an InTrust server, and it matters a lot how far apart the three components are: Repository Viewer, the InTrust server and the repository.

Working with Repository Viewer and InTrust Server

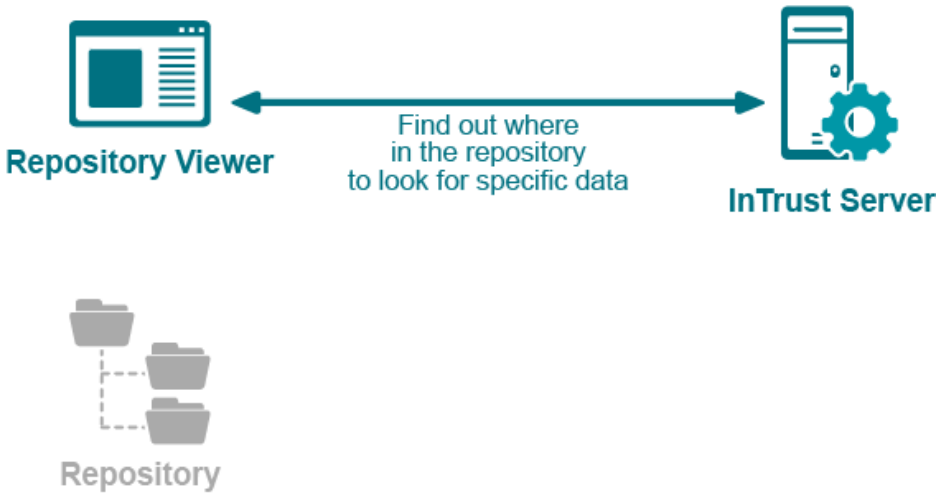
If Repository Viewer opens a repository through an InTrust server, it lets the server manage repository connections.

When Repository Viewer starts working with a repository, it connects to the InTrust server, gets authorization for access to the repository contents, and then connects to the repository.

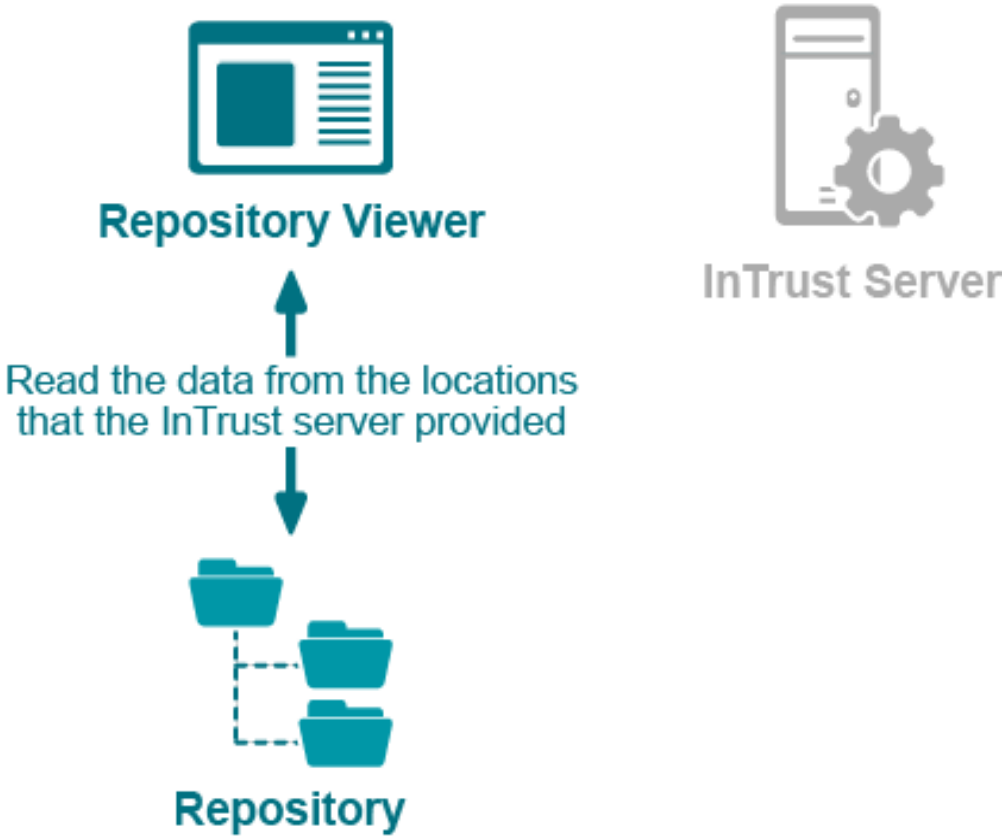


As Repository Viewer continues to work with the repository, it repeats the following steps:

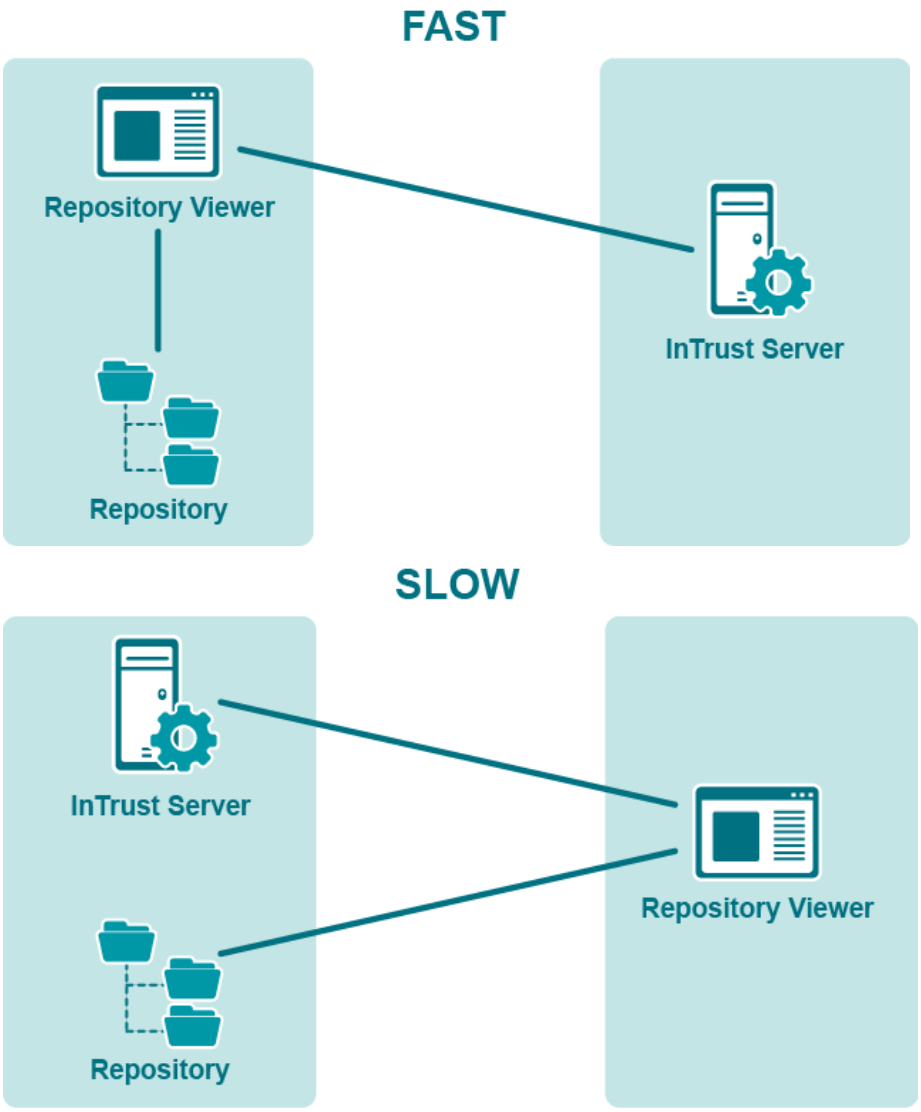
1. Ask the InTrust server for the exact locations of the requested data in the repository structure.



2. After this negotiation, read the data directly from the repository, using the information from the server.



The actual reading of repository data is the most traffic-intensive part of the process. Therefore, you should try to run Repository Viewer as close as possible to the repository share, especially in geographically-dispersed networks. Ideally, they should be on the same computer, but if that is not possible, you should run Repository Viewer on a computer or virtual machine located in the part of the network that is nearest the repository share location. How close Repository Viewer is to the InTrust server is far less important, because the amount of data they exchange is insignificant.



Working with Repository Viewer without an InTrust Server

You can use this option to analyze data from an idle repository; for example, a backup copy of a production repository with historical data.

Getting Started with Repository Viewer

NOTES:

- When you launch Repository Viewer for the first time, the console asks you to specify the repository to look in.
- Repository Viewer remembers the most recently used repository and opens it automatically on startup.

To open a repository, click **Repositories | Open** in the main menu. You are prompted to select what kind of repository to connect to: idle repository or production repository. These options mean the following:

- **Production repository**
  This ensures that the InTrust server you specify handles the communication between Repository Viewer and the repository. Always use this option if the repository you need is managed by an InTrust server and is available for gathering, consolidation and other operations. This method does not lock down the repository index, and multiple instances of Repository Viewer can use its index simultaneously.
- **Idle repository**
  This makes Repository Viewer read data directly from the repository without any intermediary components. Use this option only when the repository you need is not attached to any InTrust server. For example, it can be a backup copy of a production repository or an idle repository with historical data. Note that using direct connection locks the index of a repository so that only the first-connected instance of Repository Viewer can use the advantages of indexing.

Production repositories can be grouped together to form *repository groups*. A repository group acts as a single unit: you can run searches on it and create reports as if it were a regular repository. For details about repository group membership, see Managing Repository Groups.

NOTE: Repository Viewer works with repository groups concurrently, but multi-repository searching is not completely overhead-free.

Repository groups are stored in InTrust configuration, and they are available to every instance of Repository Viewer connected to the InTrust organization.

To open a production repository or repository group

1. Select whether you want to connect by specifying an InTrust organization or a specific InTrust server.
2. Select the organization or server.
3. Select whether you want to open individual repositories or a repository group.
   The following happens for individual repositories:
   - If you select a single repository, it will open in a temporary group. If there is still one repository in the group by the time you finish the session, the group is not saved in InTrust configuration.
   - If you select multiple individual repositories or repository groups, a new group will be created for them, and the group will open. It will include all members in your selection.

   If you select a repository group, that group will open.

You should always use the index if it is available and up to date. The index makes Repository Viewer operation interactive.

NOTES:

- For access to a production repository, Repository Viewer must be running under any of the following:
  - An account that is listed as an organization administrator.
  - An account which has at least **Read** permissions on the repository and index and is a member of the computer local **AMS Readers** group on the InTrust server that manages the repository (or repositories) and on the InTrust server that Repository Viewer connects to (these may be two different servers).
- Make sure all InTrust servers in the organization have the agent communication port (900 by default) and InTrust Server management port (8340 by default) open for inbound traffic.
- If Repository Viewer connects from a remote computer, inbound TCP ports 1024 to 65535 must be open on that computer for communication with the InTrust server.
- After you have opened a repository or repository group from some InTrust organization, there is a quick way to open other repositories from the same organization. For that, click **Repositories | Change**.

To open an idle repository

1. Specify the local or network path to the repository root folder.
2. To use the index of the repository, in the **Index location** group of options select **Repository folder** or supply a path in the **This location** text box. To continue without an index, select **No index**.

NOTE: For access to an idle repository, Repository Viewer must be running under an account with at least **Read** permissions on the share that contains the repository.

Once you have opened a repository or repository group, the left pane shows the following:

- A navigation tree with the repository structure
  The tree represents the repository structure using multiple levels, such as environment (Microsoft Windows or Unix), domain (for Windows only) and computer.
- Predefined searches with search condition presets
  These are essentially built-in interactive reports. For details, see Predefined Searches.
- Custom searches
  These are searches that you create yourself, either based on existing ones or from scratch. For details, see Custom Searches.

The right pane contains search tools.

NOTE: Any tab can be detached and docked freely in the right pane. To detach a tab, drag it away from where it is docked. To dock a pane, drag it onto any of the areas of the view compass that appears. To make it a tab again, right-click its caption and select **Tabbed Document**.

Running Searches

To run a search, click **Go**. The context of your search depends on the following:

1. Where in the navigation tree you are
   Selecting a node in the navigation tree means that your searches will include only the events available at that node's level. For example, to look in the entire repository group, select the repository group node; to get events only from a particular repository or computer, select that repository or computer's node.
2. Whether you are using any parameter filters
   Running the search without any parameters will show you all events at your current navigation tree level. If you add any filters, they are applied during the search. If you have selected any search in the left pane, you are already using the filter set configured for that search.

By default, the number of search results that can be displayed at once is capped at 5000. If you reach this limit, consider specifying better filtering conditions. You can also change the search result limit on the **Search Filter** tab.

NOTES:

- The higher the search limit, the more memory is used by Repository Viewer. If you want to increase the search result limit beyond 5000, do it with caution.
- Use filtering by date whenever the date range is known. This speeds up searches considerably.

Predefined Searches

Repository Viewer provides an extensive set of preconfigured searches out of the box. They will likely cover most of your event analysis needs; consider trying these searches before you begin creating your own. To view and use the searches included by default, expand the **Predefined Search Folders** node. Predefined searches are available only when you are working with production repositories.

NOTES:

- Predefined searches are stored in the InTrust configuration database.
- Predefined searches are updated from one InTrust version to another. This can cause upgraded Repository Viewer to fail to find events that the old version was able to find. For details, see Changes to Event Fields. Events gathered to the repository after the InTrust upgrade are fully compatible with the updated predefined searches.

You can freely modify these searches in the **Search Filter** tab (see Filter Parameters for details). However, any changes you make are applied only for the current session. The next time you open Repository Viewer, predefined searches will be in their default state. If you want to save your changes permanently, make a copy of the modified search using the **Copy To** button in the toolbar of the **Search Filter** tab . A predefined search can be a convenient starting point for creating your own search.

NOTE: The **Copy To** button is available only when an existing search is selected. When the filter parameters are configured from scratch, the button is labeled **Save As**.

In addition to the search filter configuration, the saved search includes the event list layout. If you have configured grouping and sorting for the search (see Configuring the Result Layout for details), these settings are preserved.

After you have saved your own search, all subsequent changes to it are applied immediately and permanently. See also the Custom Searches topic.

Changes to Event Fields

The set of fields in events stored in the InTrust repository has been expanded from version to version. Predefined searches in Repository Viewer have kept up with those changes and incorporated the newly-added fields. As a result, predefined searches may not always work as expected on event data that was collected by older versions of InTrust. This topic lists the added fields by InTrust version.

If your search unexpectedly turns up too little old data, you may want to modify the search to exclude recently implemented fields.

Added in Version 11.4.1 Update 1

New fields for rule match event (event ID 17408) in InTrust Server log:

Field Name	Field Display Name
Alert	Alert
Alert_Code	Alert Code
Alert_Generation_Time_Local	Alert Generation Time Local
Alert_Generation_Time_UTC	Alert Generation Time UTC
Alert_Severity	Alert Severity
Rule_ID	Rule ID
Severity_Code	Severity Code

Added in Version 11.4.1

New fields for Security log events that have Active Directory attributes in their descriptions:

Field Name	Field Display Name
DNS_Host_Name	DNS Host Name
Domain_Behavior_Version	Domain Behavior Version
Force_Logoff	Force Logoff
Lockout_Duration	Lockout Duration
Lockout_Observation_Window	Lockout Observation Window
Lockout_Threshold	Lockout Threshold
Machine_Account_Quota	Machine Account Quota

Field Name	Field Display Name
Max_Password_Age	Max Password Age
Min_Password_Age	Min Password Age
Min_Password_Length	Min Password Length
Mixed_Domain_Mode	Mixed Domain Mode
OEM_Information	OEM Information
Password_History_Length	Password History Length
Password_Properties	Password Properties
Service_Principal_Names	Service Principal Names

New fields for InTrust Server log events:

Field Name	Field Display Name
Alert_Code	Alert Code
Alert_Severity	Alert Severity
Port	Port
License	License
Data_Source_Type	Data Source Type
Server	Server
Timezone	Timezone
UTC_offset	UTC offset
Permission	Permission

Removed in Version 11.4.1

These fields were never used and have been superseded:

Field Name	Field Display Name
DS_Name	DS Name
DS_Type	DS Type

Added in Version 11.4

New fields for InTrust Self-Audit log events:

Field Name	Field Display Name
Audit_Level	Audit Level
Extension	Extension
Interface	Interface
Interface_ID	Interface ID
UTC	UTC
Log_Name	Log_Name
End_Date	End Date
Job	Job

New fields for PowerShell log events:

Field Name	Field Display Name
Context	Context
User_Data	User Data
Payload	Payload
Scriptblock	Scriptblock
Scriptblock_ID	Scriptblock ID

New fields for Windows Security log event 4738:

Field Name	Field Display Name
Account_Expires	Account Expires
AllowedToDelegateTo	Allowed To Delegate To
Home_Directory	Home Directory
Home_Drive	Home Drive
Logon_Hours	Logon Hours
Password_Last_Set	Password Last Set
Primary_Group_ID	Primary Group ID
Profile_Path	Profile Path
Script_Path	Script Path

Field Name	Field Display Name
SID_History	SID History
User_Account_Control	User Account Control
User_Parameters	User Parameters
User_Workstations	User Workstations

Added and Changed in Version 11.3.2

New field for Windows Security log events:

Field Name	Field Display Name
Failure_Code	Failure Code

Repurposed field for Windows Security log events, changed to contain textual descriptions instead of failure codes:

Field Name	Field Display Name
Failure_Reason	Failure Reason

New fields for the Agent Management and Real-Time Service sources in InTrust Sever log events:

Field Name	Field Display Name
Agent	Agent
AgentID	Agent ID
Data_Source	Data Source
Data_Source_ID	Data Source ID
Error_Text	Error Text
Not_Responding_Minutes	Not Responding Minutes
Not_Responding_Seconds	Not Responding Seconds
Percent	Percent
Repository	Repository
Rule	Rule
Size	Size

Added and Changed in Version 11.3.1

Field Name	Field Display Name
DS_Name	DS Name
DS_Type	DS Type
Property	Property
Schema	Schema
Status	Status
Value	Value

Added and Changed in Version 11.3

These changes mostly concern the ARS log and also, to a minor extent, Windows Security log.

Field Name	Field Display Name
Access_Mask	Access Mask
Accesses	Accesses
Account_Domain	Account Domain
Activity	Activity
Activity_Operation_GUID	Activity Operation GUID
Activity_Operation_ID	Activity Operation ID
Activity_Type	Activity Type
Admin_Account	Service Account
Advanced_Options	Advanced Options
Approver	Approver
Assembly	Assembly
Attachment_file_name	Attachment file name
Attestor	Attestor
Attribute	Attribute
Attribute_name	Attribute name
Authentication_Package	Authentication Package

Field Name	Field Display Name
Body	Body
Branch	Branch
CAP	CAP
CAPs_Added	CAPs Added
CAPs_Deleted	CAPs Deleted
CAPs_Modified	CAPs Modified
Certificate_Issuer_Name	Certificate Issuer Name
Certificate_Serial_Number	Certificate Serial Number
Certificate_Thumbprint	Certificate Thumbprint
Class_ID	Class ID
Class_Name	Class Name
Collection	Collection
Command	Command
Compatible_IDs	Compatible IDs
Configuration	Configuration
Configuration_Group	Configuration Group
Configured_Names	Configured Names
Container	Container
Database	Database
DC	DC
Destination	Destination
Details	Details
Details2	Details 2
Details3	Details 3
Device_Claims	Device Claims
Device_ID	Device ID
Device_Name	Device Name

Field Name	Field Display Name
Direction	Direction
Disable_Integrity_Checks	Disable Integrity Checks
Disabled_Privileges	Disabled Privileges
Enabled_Privileges	Enabled Privileges
EncapMethod	EncapMethod
Error_Code	Error Code
EtherType	EtherType
Event_in_Sequence	Event in Sequence
Expiration	Expiration
Failed	Failed
File_Name	File Name
Filter	Filter
Filter_ID	Filter ID
Flight_Signing	Flight Signing
Forest	Forest
Function	Function
GC	GC
GC_Site	GC Site
Group_Membership	Group Membership
Group_Type	Group Type
Handle_ID	Handle ID
Handler	Handler
Hardware	Hardware
Header	Header
HyperVisor_Debugging	HyperVisor Debugging
HyperVisor_Launch_Type	HyperVisor Launch Type
HyperVisor_Load_Options	HyperVisor Load Options

Field Name	Field Display Name
Instance	Instance
Interval	Interval
IP_Address	IP Address
Kernel_Debugging	Kernel Debugging
Layer_ID	Layer ID
Layer_Name	Layer Name
Load_Options	Load Options
Location	Location
Logon_ID	Logon ID
Master	Master
Maximum_Allowed	Maximum Allowed
Module	Module
Module_GUID	Module GUID
Nested_Group	Nested Group
New_Accesses	New Accesses
New_MaxUsers	New MaxUsers
New_Name	New Name
New_Remark	New Remark
New_SD	New SD
New_Share_Flags	New Share Flags
Object_ID	Object ID
Old_MaxUsers	Old MaxUsers
Old_Remark	Old Remark
Old_Share_Flags	Old Share Flags
Operation	Operation
Operation_GUID	Operation GUID
Operation_ID	Operation ID

Field Name	Field Display Name
Ownership_Type	Ownership Type
Packets_Discarded	Packets Discarded
Parameters	Parameters
Partition	Partition
Policy_Category	Policy Category
Policy_Change	Policy Change
Policy_ID	Policy ID
Policy_Subcategory	Policy Subcategory
Pre_Authentication_Type	Pre-Authentication Type
Process_ID	Process ID
Protocol	Protocol
Reason	Reason
Result	Result
Result_Code	Result Code
Run_As	Run As
Schema_Builtin_Version	Schema Builtin Version
Schema_Info	Schema Info
Schema_Virtual_Version	Schema Virtual Version
SCP	SCP
SD	SD
Sequence_Length	Sequence Length
Server_Name	Server Name
Service_ID	Service ID
Service_Name	Service Name
Shadow	Shadow
Share_Name	Share Name
Share_Path	Share Path

Field Name	Field Display Name
Silo_Name	Silo Name
Site	Site
SnapControl	SnapControl
SnapOui	SnapOui
Source_Details	Source Details
Source_Network_Address	Source Address
SPN_Name	SPN Name
Start_Date	Start Date
Succeed	Succeed
System_Event_Logging	System Event Logging
Target_Address	Target Address
Target_Port	Target Port
Task	Task
Test_Signing	Test Signing
TGT_Lifetime	TGT Lifetime
Ticket_Encryption_Type	Ticket Encryption Type
Ticket_Options	Ticket Options
Total	Total
TPAM_Failed	TPAM: Failed
TPAM_Operation	TPAM: Operation
TPAM_Role	TPAM: Role
TPAM_Target	TPAM: Target
Transited_Services	Transited Services
UNIX_Result	UNIX: Result
User_Claims	User Claims
User_Name	User_Name
VlanTag	VlanTag

Field Name	Field Display Name
VSM_Launch_Type	VSM Launch Type
vSwitch_ID	vSwitch ID
Workflow	Workflow
Workflow_GUID	Workflow GUID

Added in Version 11.1

Field Name	Field Display Name
Facility	Facility
Object_New_DN	Object New DN
Object_Old_DN	Object Old DN
Severity	Severity

Added in Version 11.0

Field Name	Field Display Name
UNIX_AUDIT_NAME	Audit Event
UNIX_AUDIT_CLASS	Audit Class
UNIX_AUDIT_CALL	Audit Call
UNIX_AUDIT_TRAIL	Audit Trail
UNIX_AUDIT_COMMAND	Audit Command

Added in Version 10.7

Field Name	Field Display Name
Filer	Filer
New_path	New path
Scope	Scope
Number_of_results	Number of results
Query_filter	Query filter
Attribute_name	Attribute name

Field Name	Field Display Name
Elapsed	Elapsed
Query_type	Query type
TPAM_Operation	Operation
TPAM_Role	Role
TPAM_Target	Target
TPAM_Failed	Failed
UNIX_Result	Result
UNIX_OS	OS
QPMU_Service	Service
QPMU_Master_host	Master host
QPMU_Submit_host	Submit host
QPMU_Submit_user	Submit user
QPMU_Run_host	Run host
QPMU_Run_user	Run user
QPMU_Command_line	Command line
Permissions_Changed	Permissions Changed
Original_Owner	Original Owner
New_Owner	New Owner
Data_Written	Data Written
Permission_level_name	Permission level name
Permission_level_allow_mask	Permission level allow mask
Permission_level_deny_mask	Permission level deny mask
Site_URL	Site URL
List_URL	List URL
List_relative_URL	List relative URL
User_Logon_Name	User Logon Name

Field Name	Field Display Name
Applied_to	Applied to
Inherited_from	Inherited from
Version	Version
Grantee_user_name	Grantee user name
Grantee_group_name	Grantee group name
Field_Name	Field Name
Old_value	Old value
New_value	New value
Attachment_file_name	Attachment file name

Added in Version 10.6

Field Name	Field Display Name
Affected_Group	Affected Group

Custom Searches

If the predefined Repository Viewer searches do not cover your specific needs, use custom searches: either based on the predefined ones or created from scratch.

IMPORTANT:
To create custom searches, you need to make sure your account is an InTrust organization administrator. To view and edit the list of organization administrators, do one of the following:

- In InTrust Deployment Manager, click **Manage | Configure Access**.
- In InTrust Manager, open the properties of the root node.

The default organization administrators are the accounts used for installing InTrust and for running InTrust services.

Ad-Hoc Searches

To run an ad-hoc search with parameters, use the **Search Filter** tab, which is under the event list in the default layout. The **Add or Remove Parameters** button lets you customize your search, as follows:

1. Click **Add or Remove Parameters**.
2. In the Select Filter Parameters tool bar that opens, select the parameters that you want to define for the filter. See Filter Parameters for details.

3. When you have added the necessary parameters, close the Select Filter Parameters tool bar, and specify the values you want to filter by and the operators to use for value matching.
4. Click **Go**.

If you expect to use the same set of parameters in the future, you can save it as a custom search. For details, see Custom Searches below.

Custom Searches

Any search filter configuration can be saved as a search. You can make custom searches:

1. By modifying predefined searches and saving your changes, as described in the Predefined Searches topic. This method can save you a great deal of time and effort.
2. By building a set of filters from scratch when only a node in the navigation tree is selected, and saving this.

To create a search based on your current filter configuration and place in the navigation tree, click **Save As** in the **Search Filter** tab when it shows your filter settings, and specify the name of the new search in the dialog box that appears.

NOTE: The **Save As** button is available only when the filter parameters are configured from scratch. When an existing search is selected, the button is labeled **Copy To**.

Mind that the node currently selected in the navigation tree can affect the set of parameters defined for the search. For example, if a particular computer is selected, an additional parameter will be automatically added to show events only from this computer. If you want to avoid this, create searches while the root folder of the repository is selected.

NOTE: Each user's custom searches are saved in the InTrust configuration database. They are available to all InTrust organization administrators (for reading and writing) and members of the **AMS Readers** local group on the repository-managing InTrust server (for reading).

Organizing Searches

To logically nest searches, organize them into folders:

- To create folders for your searches in advance, right-click **Custom Search Folders** in the left pane and select **Create Folder**.
- To create a folder while saving the search, click the folder icon in the **Save As** dialog box.

Best Practice: Search Across Event Fields

If you want to find specific information no matter which event field it is in, use the **Any Field** parameter for your search term. This is especially helpful if you are not familiar with the information layout in the events you are working with.

To find this parameter in the Select Filter Parameters dialog box, select the **Primary** option in the drop-down list. **Any Field** is the first item in the list.

Generally, this is a good starting point for refining a search: it let you exclude the fields where you don't want the term to occur instead of trying to include all the fields where it might occur.

Managing Repository Groups

After you have opened a repository group in Repository Viewer, you can manage its membership as follows:

- Using the **Remove** command in the member repository shortcut menu
- Using the **Add Repository** command in the group shortcut menu

The shortcut menu for a repository group also contains the **Rename Repository Group** and **Delete Repository Group** commands. The **Delete Repository Group** command erases the group from InTrust configuration. The other place where you can delete a repository group is in the Open Repositories wizard; all existing repository groups in the InTrust organization are listed there.

IMPORTANT: Whenever a repository is added to a group or removed from it, the change is immediately applied in all instanced of Repository Viewer connected to an InTrust organization. In addition, removing a repository group also deletes all scheduled reports that use the repository group. These changes should be made responsibly.

Filter Parameters in Repository Viewer

Repository Viewer provides a variety of fields to look in. To list all of them, select **All** in the drop-down list in the Select Filter Parameters toolbar. By default, only the normalized fields (such as Who, When or What) are shown.

The parameters include:

1. Regular event fields (available in the Primary set and under All)
2. Additional parameters:
    - The **Insertion strings** set
      These are the unnamed insertion strings that events use for storing various information. You can use these fields if you know precisely what they are used for in the events you are working with.
    - The **Resolved insertion strings** set
      These are regular insertion strings that have been processed to resolve any GUIDs and SIDs that occur in them. Note that the resolution works only for events that were gathered using InTrust agents.
    - The **Named insertion strings** set
      These are friendly labels for regular insertion strings. Note that different types of events use identically-numbered insertion strings for different kinds of data, so you should make sure the meaning is right if you use a named insertion string in your search. Named insertion strings are intended for improving presentation, especially if you are preparing custom searches for someone else to use.
    - The **Normalized event fields** set
      See Normalized Event Fields (Who, What, When and Others) for details.
    - The **Any Field** parameter
      See the *Best Practice: Search Across Event Fields* section in Custom Searches for details.
    - The **Custom** parameter
      See Advanced Expression-Based Filters for details.

Configuring Parameters

When you have added a parameter to the **Search Filter** tab, specify the following:

1. The operator to apply
   Use the leftmost button in the operator block. The operators are "Equals", "Contains", "Ends with" and so on.

2. The parameter value
   This is a combo box where in addition to an explicit value, this can be one of the following options:
   - **Blanks**
     Matches if the field is empty.
   - **NonBlanks**
     Matches if the field is not empty.
   - **Custom**
     Lets you build a logical condition tree that works within this particular parameter; see below for details.

NOTE: In the current version of Repository Viewer, the following issues are known to exist in search filters:

- The value used for the Any Field parameter matches only the beginnings of words.
- The "Contains" operator matches only the beginnings of words.

All the parameters you include in the filter are combined using logical AND—they must all match for the filter as a whole to match. For details about using OR operations, see Advanced Expression-Based Filters.

CAUTION: For some search filter operators, there is no search speedup if the repository is indexed. The following operators cannot take advantage of the index:

- **Not equals**
- **Does not contain**
- **Not like (wildcards)**
- **Does not start with**
- **Ends with**
- **Does not end with**

Custom Logic for Parameters

Selecting **Custom** in the parameter value combo box opens a dialog box that lets you set up multiple matching conditions and manage their flow with the AND and OR operators.

- To change the list, use the **Add Condition** and **Remove Condition(s)** buttons.
- To select conditions, use the leftmost column: you can Ctrl-click, Shift-click and drag-select items.
- To apply the AND operator (meaning, match all of them) to selected conditions, click the 'And' Group button. The grouping will be visualized as a blue line that spans the operators.
- To apply the OR operator (meaning, match any of them) to selected conditions, click the 'Or' Group button. The grouping will be visualized as an orange line that spans the operators.
- To change a group's operator from OR to AND or the other way around, click the line that marks the grouping, or select a member of the group and click the Toggle button.
- To remove one or more conditions from a group, select them and click the **Ungroup** button.

Note that this logic is processed for values of a single parameter. If you want to analyze multiple parameters, see Advanced Expression-Based Filters for details.

Normalized Event Fields (Who, What, When and Others)

These fields are not present in the original events; they are filled in by InTrust based on knowledge about the contents of regular fields in various types of events. Normalized fields make it easier to retrieve the most important information from the event; you do not have to know which particular original fields contain which kind of information.

The current set of supported normalized fields is as follows:

FIELD	MEANING
What	A brief description of what the event is about. It is related to such fields as **Description** and **Category**. Example: For all events that have to do with logging on, the **What** field says **Logon**, regardless of the event category, platform where it occurred, or nature of the logon.
When	When the event was generated. The time is automatically converted to the local time on the computer where Repository Viewer is running.
Where	The computer where the event happened (had effect).
Where From	The name or IP address of the computer from which the activity (such as a logon, or a configuration change) was performed. This is not necessarily the same computer as the one where the activity had effect.
Who	Plain user name of the account that caused the event. Example: Using this field helps you track user activity across platforms: Windows, Unix, VMware and so on.
WhoDomain	The Active Directory domain of the account that caused the event, where applicable.
Whom	The user account that was affected by the event, where applicable. Example: In password change events, this field shows whose password was changed.

NOTE: Use Event-o-Pedia (http://eventopedia.cloudapp.net/) to learn more about the events you can audit. This Web site is a knowledge base that helps you find out the meaning, structure and importance of the events you encounter.

Advanced Expression-Based Filters

The **Custom** filter parameter lets you specify expressions for very specific filtering needs that cannot be covered by the built-in options (for example, complex time ranges). The parameter accepts expressions in the REL expression language, which is used for event analysis throughout InTrust. The language is described in the InTrust Customization Kit document.

The immediate and intuitive advantage of custom expressions is the ability to use logical OR across multiple fields to branch your matching conditions. Effectively, this lets you combine multiple searches.

The default catch-all expression is **true**. In real-world use, you need to provide a REL expression that evaluates to **true** only if your specific conditions are met.

Examples of expression-based filters:

What you want to find	Expression
Events where the **Computer** field is "SRV01" or the **User Name** field is "DOMAIN1\jdoe", but not necessarily both at once.	`(Computer = "SRV01") or (UserName = "DOMAIN1\\jdoe")`
Events where the **Who** field is an account that is a member of the **Domain Admins** group.	`member_of( Who, 'Domain Admins', true)` **Important:** This expression works only for global and universal groups, not for domain local groups. It is suitable in this case, because **Domain Admins** is a global group.

For more advanced expression techniques, refer to the REL-specific topics in the InTrust Customization Kit.

Changing the Business Hours and Non-Business Hours Parameters

The **Business Hours** and **Non-Business Hours** parameters define fixed time patterns, and no user interface is provided for editing these patterns. If you need to adjust the hours for a particular search, you can do so using native SQL Server tools, as follows:

1. Run an SQL query on the InTrust configuration database to find the search you need. For example:
   `select [Guid], [Query] from [dbo].[SearchItem] where [name] = '<search_name>'`
   This returns the GUID of the search and the query that it uses. Here is a sample search query:

```
<SearchQuery>
  <SimpleCriterias>
    <SimpleCriteria>
      <name>When</name>
      <condition>
        <GroupOperator>And</GroupOperator>
        <Items>
          <DateTimeComparisonCondition_BusinessHours>
            <start_time>8</start_time>
            <end_time>19</end_time>
            <start_dow>1</start_dow>
            <end_dow>5</end_dow>
          </DateTimeComparisonCondition_BusinessHours>
        </Items>
      </condition>
    </SimpleCriteria>
  </SimpleCriterias>
  <FullTextSearchCriteriaItem>
    <FTS/>
  </FullTextSearchCriteriaItem>
</SearchQuery>
```

2. Edit the search query so that it meets your requirements. You need to make changes to the contents of the **DateTimeComparisonCondition_BusinessHours** or **DateTimeComparisonCondition_NonBusinessHours** node. In particular, you need to modify the integer values of the following:

    - **start_time**
      What time the business or non-business hours start
    - **end_time**
      What time the business or non-business hours end
    - **start_dow**
      The first work day in the case of business hours; the first day off in the case of non-business hours (0 through 6 is Sunday through Saturday)
    - **end_dow**
      The last work day in the case of business hours; the last day off in the case of non-business hours (0 through 6 is Sunday through Saturday)

NOTE: It is assumed that the times you specify are in the time zones of the computers where the events were logged. If you want these original timestamps to appear in Repository Viewer and scheduled reports, make sure the **Local Time** column is displayed in the grid. This column is hidden by default. For details about changing the grid, see Configuring the Result Layout.

3. Overwrite the original search query with your modified version in the configuration database, using the previously extracted GUID to identify the search. For that, use an SQL query like the following:
   `update [dbo].[SearchItem] set [Query] = '<modified_search_query_string>' where [Guid] = '<search_GUID>'`

Examining Event Details

To view the details of a selected event, use the **Event Details** tab. Double-click the event to open this tab.

In addition to displaying event details, this view provides some useful functionality. Click anywhere in the **Event Details** tab to open the shortcut menu with the additional options:

- **Copy to Clipboard**
  You can paste the copied event details in a spreadsheet, word processor, plain text file and so on. The result should be correctly formatted for any of these destinations.
- **View Details in Eventopedia**
  Eventopedia (http://eventopedia.cloudapp.net) is an encyclopedia of known audit log events that explains their meanings and uses.
- **Investigate in IT Security Search** and **Set Up IT Security Search Link**
  See Drilling Down with IT Security Search below for details.
- **Email Event Details**
  This action composes an email message from the event details in Microsoft Outlook. An installed copy of Outlook is required.

Drilling Down with IT Security Search

You can use the event whose details you are viewing as a starting point for an event analysis session in IT Security Search.

Before you can use this functionality, you need to configure the link between Repository Viewer and IT Security Search. Repository Viewer needs to know the URL where IT Security Search is available in your environment and which event fields to use for generating search queries. Click **Set Up IT Security Search Link** in the shortcut menu to specify these settings.

After you have configured the link, you can use the **Investigate in IT Security Search** action with any event currently opened in the **Event Details** tab.

For details about using IT Security Search, see the IT Security Search User Guide.

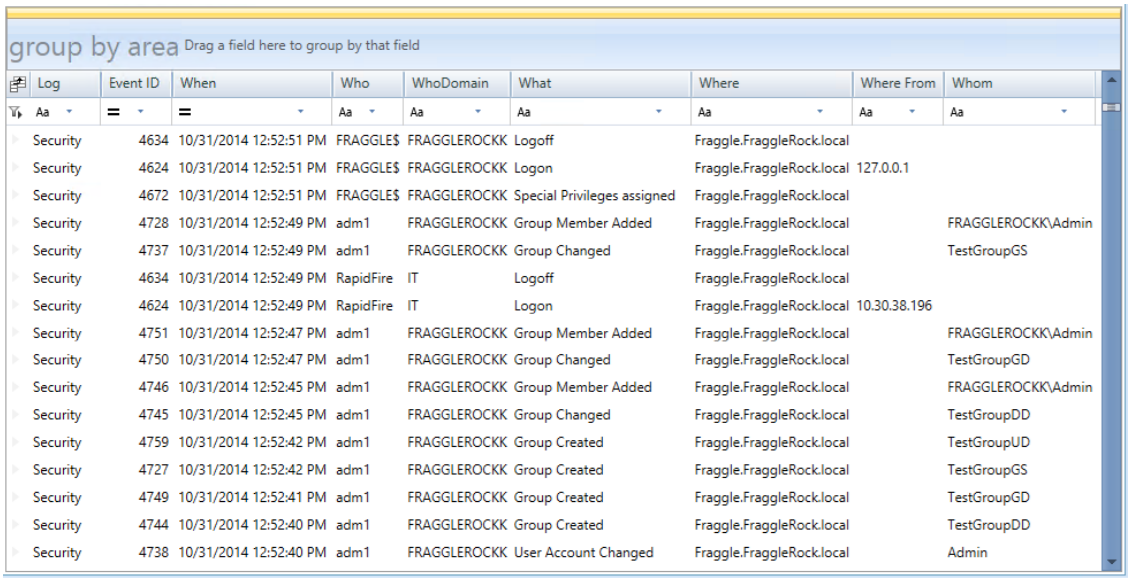
Configuring the Result Layout

You can set up event display in the right pane exactly the way you want your search results to be presented, using sorting and grouping.

Organizing the Grid

The default event view in Repository Viewer is a grid, and the default grid layout is a table, where the columns are named after event fields.

You can snap the column names together like building blocks, vertically as well as horizontally, to make compact layouts instead of using a plain table. The grid will use your block layout for every event it displays.



Log	Event ID	When	Who	WhoDomain	What	Where	Where From	Whom
Security	4634	10/31/2014 12:52:51 PM	FRAGGLE$	FRAGGLEROCKK	Logoff	Fraggle.FraggleRock.local		
Security	4624	10/31/2014 12:52:51 PM	FRAGGLE$	FRAGGLEROCKK	Logon	Fraggle.FraggleRock.local	127.0.0.1	
Security	4672	10/31/2014 12:52:51 PM	FRAGGLE$	FRAGGLEROCKK	Special Privileges assigned	Fraggle.FraggleRock.local		
Security	4728	10/31/2014 12:52:49 PM	adm1	FRAGGLEROCKK	Group Member Added	Fraggle.FraggleRock.local		FRAGGLEROCKK\Admin
Security	4737	10/31/2014 12:52:49 PM	adm1	FRAGGLEROCKK	Group Changed	Fraggle.FraggleRock.local		TestGroupGS
Security	4634	10/31/2014 12:52:49 PM	RapidFire	IT	Logoff	Fraggle.FraggleRock.local		
Security	4624	10/31/2014 12:52:49 PM	RapidFire	IT	Logon	Fraggle.FraggleRock.local	10.30.38.196	
Security	4751	10/31/2014 12:52:47 PM	adm1	FRAGGLEROCKK	Group Member Added	Fraggle.FraggleRock.local		FRAGGLEROCKK\Admin
Security	4750	10/31/2014 12:52:47 PM	adm1	FRAGGLEROCKK	Group Changed	Fraggle.FraggleRock.local		TestGroupGD
Security	4746	10/31/2014 12:52:45 PM	adm1	FRAGGLEROCKK	Group Member Added	Fraggle.FraggleRock.local		FRAGGLEROCKK\Admin
Security	4745	10/31/2014 12:52:45 PM	adm1	FRAGGLEROCKK	Group Changed	Fraggle.FraggleRock.local		TestGroupDD
Security	4759	10/31/2014 12:52:42 PM	adm1	FRAGGLEROCKK	Group Created	Fraggle.FraggleRock.local		TestGroupUD
Security	4727	10/31/2014 12:52:42 PM	adm1	FRAGGLEROCKK	Group Created	Fraggle.FraggleRock.local		TestGroupGS
Security	4749	10/31/2014 12:52:41 PM	adm1	FRAGGLEROCKK	Group Created	Fraggle.FraggleRock.local		TestGroupGD
Security	4744	10/31/2014 12:52:40 PM	adm1	FRAGGLEROCKK	Group Created	Fraggle.FraggleRock.local		TestGroupDD
Security	4738	10/31/2014 12:52:40 PM	adm1	FRAGGLEROCKK	User Account Changed	Fraggle.FraggleRock.local		Admin

You may want to hide the fields you do not need or display the blocks that you want to work with. For that, click the icon next to the leftmost block name and change the selection in the **Field Chooser** toolbar. The following fields are available:

- Normalized event fields
- Regular event fields (available in the **Primary** set and under **All**)
- Insertion strings
- Named insertion strings
- Resolved insertion strings

For details about the fields, see Filter Parameters.

Grouping

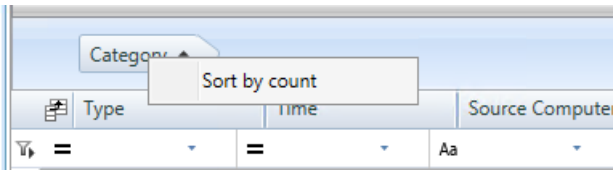
Repository Viewer supports multi-level grouping of events, so that you can organize the results in tree-like views using any criteria. For example, you can group events by log, then by event ID, and then by user.

To use multi-level grouping, In the **Events** pane, drag column names from the event list to the area above the event grid. The event list changes accordingly.

Sorting

To sort the results by a particular field, click that field's block in the grid. Clicking a block repeatedly toggles between ascending and descending order.

Items are sorted by name. However, for groups you also have the option of sorting items by count. To enable it, right-click the block you need in the grouping area and select **Sort by count**.



This option is set independently for each grouping level.

Hiding and Unhiding Events

Hiding and unhiding events is useful when you need to repeatedly locate specific events in the same pool of audit data. This does not change your list of search results, but only specifies which parts of it are shown. It is quicker than redefining search filters and redoing searches every time, and if you are using a custom search, it helps you avoid modifying it.

To configure a view filter, use the controls underneath the column names in the event view: click the operator icon to select the operator, and specify the value to filter by. For details about operators, see the Filter Parameters topic.

Using Pie Charts and Column Graphs

Pie charts and column graphs are graphical alternatives to the grid-based textual representation of search results.

An event list can use multi-level grouping, but pie charts and column graphs work only if single-level grouping is used. In addition, the charts are most informative when they have only a few elements to display. Otherwise, the visual clutter can make them useless.

To switch to a non-default event view, select the **Pie Chart** or **Column Graph** tab.

Saving the Results

In any event view, you can export the currently displayed events to a file. For that, click **Report | Save Report** button. In the save dialog box, you have the options of saving the current view "as is" or running a fresh search without an item limit and possibly with more recent results.

The **Report** drop-down menu also contains scheduling options. For details about scheduled reporting, see Reporting on Events Using Repository Viewer.

Case Study: Forensic Analysis of Active Directory Tampering

This example is based on an actual investigation, but the details have been changed. In the example environment, a business-critical server named **acc05** hosts the payroll in a network share. Access to the share is controlled through share permissions. Only the members of the **Finance and Accounting** Active Directory group have read and write access.

Jake, the investigator, has grounds to suspect that some of the payroll files have been tampered with, and needs to perform forensic analysis. Here is how he does it using InTrust-collected audit data from the Security log and Change Auditor File Access Audit event log:

1. 1. The starting point is the **acc05** computer where the breach supposedly happened. In Repository Viewer, Jake runs a search that shows events from the computer for the past 24 hours. The filter parameters are as follows:
    - Computer: “acc05”
    - When: “Last 1 day”
2. He groups the results by **Who** then by **What**, and checks who accessed the share. In the Where From field, he spots an IP address that needs looking into.
3. Jake checks what else was done from the same IP address. For that, he runs a new search with the **Any Field** parameter set to the suspicious IP address. He finds out that a logon to a domain controller from the suspicious IP address occurred under an administrator account. Jake notes the time of the logon.
4. He then finds out what the administrator account did after the logon to the domain controller. For that, he runs a new search with the **Who** parameter set to the administrator account name and the **When** parameter set to after the logon.
5. It turns out that the impersonator cleared the Security log in an attempt to cover the tracks. However, the events from the log were not lost, because the InTrust agent on the domain controllers was running with log backup enabled.
6. It also turns out that user **david_shore** was added to the **Finance and Accounting** Active Directory group and removed from it shortly afterwards. This is the apparent intruder. To confirm it, Jake checks if this account did anything to the payroll files.
7. He runs a new search with the following parameters:
    - Computer: “acc05”
    - When: “Last 1 day”
    - Who: “david_shore”
8. The search turns up changes to the payroll files. This is clear evidence of a breach, and the perpetrator is now known.

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product