

Quest® IT Security Search 11.6.1

## User Guide



© 2025 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

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

Quest Software Inc.

Attn: LEGAL Dept  
20 Enterprise, Suite 100,

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.

IT Security Search User Guide

Updated - February 2025

Version - 11.6.1

# Contents

<b>Welcome to IT Security Search</b> .....	<b>7</b>
<b>Installing IT Security Search</b> .....	<b>8</b>
Compatibility .....	8
Software Requirements .....	8
Browser Compatibility .....	9
Hardware Requirements .....	9
Disk Space for Enterprise Reporter Data in Warehouse .....	9
Disk Space for Active Roles Event Data .....	10
Disk Space for InTrust and Change Auditor Data .....	11
Installing Microsoft SQL Server Express 2012 Service Pack 2 .....	11
Where to Install .....	11
Note for Windows Server 2022 installation .....	11
What Accounts to Use .....	12
<b>Security Details and Configuration</b> .....	<b>13</b>
Providing a CA-Signed Certificate .....	13
Providing a Self-Signed Certificate .....	14
Binding Your Certificate .....	15
Revoking a Certificate .....	15
.....	16
How IT Security Search Security Features Are Implemented .....	16
Enabling Secure Data Transfer for IT Security Search Warehouse .....	16
Running IT Security Search Services Under a Group Managed Service Account (gMSA) .....	17
<b>Who Can Do What in IT Security Search</b> .....	<b>19</b>
Setting the Scope of Responsibility for an Operator .....	19
Creating the List of OUs .....	20
Fine-Tuning the Scope with Queries .....	20
Auto-Lookup of Operator Data in a Query .....	21
Examples .....	21
Controlling Active Directory Recovery Privileges .....	22
<b>Where the Data Comes From</b> .....	<b>23</b>
Specifying Data Sources .....	23
Change Auditor Database .....	24
InTrust Repository .....	24
Enterprise Reporter .....	25
Setting Up Forwarding in Enterprise Reporter .....	25

Making All Data Cohesive with Enterprise Reporter .....	25
Ensuring Correct Object Counts for OUs .....	26
Recovery Manager for Active Directory Server .....	26
Active Roles .....	26
Management History Synchronization Specifics .....	27
Splunk .....	27
HTTPS API for Forwarded Change Auditor Events .....	28
Before You Begin .....	28
Getting Change Auditor Ready .....	28
Getting IT Security Search Ready .....	29
<b>Running Searches .....</b>	<b>30</b>
Viewing Data by Object Type .....	30
Specifying a Time Range for Events .....	30
Customizing the Event Grid Layout .....	31
Understanding the Event Timeline .....	31
Viewing Details of Search Results .....	31
Navigating Session History Using Breadcrumbs .....	31
Using Facets to Filter Results .....	32
Fine-Tuning Your Search Terms .....	32
Automating Complex Search Scenarios .....	32
Search Term Syntax .....	32
Single-Word Terms .....	33
Term Combinations .....	33
Searching in Specific Attributes .....	35
Specifying Quotation Marks .....	36
Filter Syntax .....	36
Normalized Attributes .....	37
Using Functions in Queries .....	38
Group Membership Resolution Functions .....	38
Permission Resolution Functions .....	39
Function Limitations .....	40
Making Multi-Stage Searches .....	40
Auto-Resolution of the Current User .....	41
Specifics of Recovery Manager for Active Directory Data .....	41
Searching by Distinguished Name .....	42
Searching for Deleted Objects .....	42
Searching Without Specifying Fields .....	42
Data Field Reference .....	42
Enterprise Reporter Data Fields .....	43
Computers .....	43
Files .....	44
Groups .....	46

OUs .....	48
Shares .....	49
Users .....	50
Other Object Types .....	54
InTrust Data Fields .....	54
Change Auditor for Active Directory Data Fields .....	56
Active Roles Data Fields .....	58
Events .....	59
Computers .....	62
Groups .....	63
OUs .....	64
Users .....	65
Recovery Manager for Active Directory Data Fields .....	66
Computers .....	67
Groups .....	68
OUs .....	69
Users .....	70
Saving Searches and Running Saved Searches .....	71
Saving Searches .....	71
Running a Saved Search .....	72
Making a Saved Search Public or Private .....	72
Deleting a Saved Search .....	72
Importing and Exporting Searches .....	72
Customizing Action Links .....	73
Defining Action Links .....	73
Importing and Resetting Custom Action Links .....	74
<b>Use Scenarios .....</b>	<b>76</b>
Finding and Examining a User .....	76
Understanding Who Did What .....	76
Getting Insights from the Who and Whom Fields .....	76
Exploring a User's Scope of Access .....	77
Tracking Permission Management .....	77
Exploring and Rolling Back Changes to Active Directory Objects .....	77
Detecting Preparations for Intrusion .....	77
Case Study: Investigating Tampering .....	78
Case Study: Making the Most of Multiple Connectors .....	79
Case Study: Active Roles Dynamic Group Membership Tracking .....	80
<b>Additional Utility Scripts .....</b>	<b>81</b>
<b>Providing Information to Support .....</b>	<b>82</b>
<b>About us .....</b>	<b>83</b>

Contacting Quest .....	83
Technical support resources .....	83
<b>Third-party contributions .....</b>	<b>84</b>
Licenses .....	88
Apache 2.0 .....	88
DotNetZip 1.13.3 .....	92
Eclipse Public License - v 1.0 .....	94
GPL (GNU General Public License) 2.0 .....	97
Microsoft Reciprocal License (MS-RL) .....	102
Microsoft Public License (Ms-PL) .....	103
New BSD License .....	104
RichText Builder (StringBuilder for RTF) License .....	104

# Welcome to IT Security Search

Quest IT Security Search provides IT administrators, IT managers and security teams with a way to navigate the expanse of information about the enterprise network. It helps you achieve the following:

- Examine what is going on
- Assess the efficiency of security practices
- Track security incidents
- Track incidents related to operations
- Have up-to-date information about users, computers, file server status and more at your fingertips
- Perform recovery operations if IT Security Search is connected to Recovery Manager for Active Directory

The search engine-like interface helps you pinpoint the data you need using only a few searches and clicks.

# Installing IT Security Search

To set up IT Security Search, run the **ITSearchSuite.exe** installation package present inside Components folder of IT Security Search package. You can customize the installation path and the port that will be used for getting data.

## Compatibility

The following versions of data-providing systems are supported in this version of IT Security Search:

- InTrust 11.6.1, 11.5.1, 11.5, 11.4.2, 11.4.1, 11.4, 11.3.2, 11.3.1, 11.3
- Change Auditor 7.4, 7.3, 7.2, 7.1, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0, 6.9.5, 6.9.4, 6.9.3, 6.9.2, 6.9.1, 6.9
- Enterprise Reporter 3.5.1, 3.2.2, 3.2.1, 3.2, 3.1
- Recovery Manager for Active Directory 10.3.1, 10.2.2, 10.2.1, 10.1.1, 10.1, 10.0.1, 10.0, 9.0.1, 9.0, 8.8.1
- Active Roles 8.1.5, 8.0, 7.5.3, 7.5.2, 7.4.1, 7.4, 7.3.2, 7.3.1, 7.2.1, 7.2, 7.1

**i** **NOTE:** The ARS installer is removed from the ITSS installer to adhere with the new AirGap compliance requirements.

## Software Requirements

- Operating system:
  - Microsoft Windows Server 2022
  - Microsoft Windows Server 2019
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows Server 2012
  - Microsoft Windows Server 2008 R2
- Additional software:
  - Microsoft .NET Framework 4.7.2 or later
  - Microsoft Windows PowerShell 3.0 or later
  - Microsoft SQL Server 2012 or later (all editions)  
This is a requirement of the IT Security Search Warehouse component, which needs it for internal configuration management.

- Additional requirements for the Recovery Manager for Active Directory connector:
  - Enable remote commands in Windows PowerShell. For details, see <https://technet.microsoft.com/en-us/magazine/ff700227.aspx>.
  - The PowerShell script operation policy must be set to **RemoteSigned**. Run the following cmdlet:  
`Set-ExecutionPolicy RemoteSigned`
- Additional requirements for the Active Roles connector:
  - Active Roles Management Tools
  - The PowerShell script operation policy must be set to **RemoteSigned**.

**i** | **NOTE:** Change Auditor components can be deployed on virtual machines running in Infrastructure as a Service (IaaS), such as Amazon Web Services and Microsoft Azure.

## Browser Compatibility

The IT Security Search Web interface works correctly with the following browsers:

- Microsoft Edge
- Microsoft Internet Explorer 11
- Google Chrome 72.0 or later
- Mozilla Firefox 65.0 or later

The minimum supported monitor resolution is 1024x768.

## Hardware Requirements

- CPU: 6 cores minimum; 16 cores recommended
- RAM: 8GB minimum; 16GB or more recommended
- Disk: 200GB (SSD recommended); disk space requirements are very dependent on the volume of Enterprise Reporter and Active Roles data being processed, because the index size varies proportionally; the indexes for Change Auditor, Recovery Manager for AD and InTrust data do not consume any disk space on the IT Security Search computer, because they are located in the data stores used by these systems
- If you deploy on a virtual machine, make sure the CPU and memory requirements above are met, and do not overload the virtual machine host

To find out the disk requirements for IT Security Search installation, consider the sections below. They describe how much disk space is used for indexing data provided by specific connectors.

## Disk Space for Enterprise Reporter Data in Warehouse

These are the average index entry sizes for each type of Enterprise Reporter object. Use them in calculating the required disk space for your particular on-premises or hybrid environment.

Note that there are generally multiple index entries per object, depending on how often objects are changed.

<b>Object type</b>	<b>Average size of an index entry, in kilobytes</b>
AD Permissions	2.1
AD Contacts	3.3
Computers	1.6
Groups	1.5
Files	1.5
OUs	2.3
Shares	2.1
Users	1.6
Azure Applications	1.6
Azure Contacts	1.6
Azure Devices	5
Azure Groups	1.4
Azure Network Security Groups	2.2
Azure Resource Groups	1.5
Azure Resource Subscriptions	5
Azure Resources	1.6
Azure Roles	1.4
Azure Service Principals	1.5
Azure Tenants	2.8
Azure Users	3.4
Azure Virtual Machines	2.5

## Disk Space for Active Roles Event Data

An index entry for a single Active Roles event in IT Security Search Warehouse takes 0.5KB on average. Estimate the event rate in your environment to calculate the required disk space.

## Disk Space for InTrust and Change Auditor Data

To display InTrust and Change Auditor events, IT Security Search uses the built-in indexes in InTrust and Change Auditor data stores, so no additional disk space is required.

## Installing Microsoft SQL Server Express 2012 Service Pack 2

Install SQL Server Express **SQLEXPR\_x64\_ENU** (present inside Redist folder of IT Security Search Setup) as a configuration store for the IT Security Search Warehouse server, which is an integrated component for audit data archival.

## Where to Install

It is recommended that you install IT Security Search in the same domain as the servers of your data-providing systems: InTrust, Enterprise Reporter, Change Auditor, Active Roles and Recovery Manager for Active Directory. Do not install IT Security Search on any of those systems' servers.



**NOTE:** IT Security Search 11.6.1 can be installed on a new machine directly or as a fresh installation after uninstalling the older version.



**CAUTION:**

- **When you specify the organization and configuration database for the Warehouse component during installation of a new instance of IT Security Search, do not select an existing InTrust or Warehouse organization or configuration database. If you do, that database can become corrupted. Always create a new organization and configuration database for each instance.**
- **Conversely, if you are upgrading IT Security Search, let setup reuse the existing configuration settings.**

## Note for Windows Server 2022 installation

Installing ITSS on Windows Server 2022 requires the users to perform the following steps, for removing the existing certificate and binding a new certificate, as described below:

1. Navigate to C:\Program Files\Quest\IT Security Search\Scripts\New-SslCertificate.ps1 and run following values:

```
[string]$FilePath = "C:\Temp\ITSearch.cer",  
[string]$Subject = "test-certificate",  
[string]$SubjectDnsAltNames = "test", #comma delimited  
[datetime]$Begin = [System.DateTime]::Today,  
[datetime]$End = (New-Object System.DateTime -ArgumentList @(2039,12,31)),  
[switch]$KeepExisting
```

2. Navigate to C:\Temp and copy the **ITSearch.cer** to installation certificate path (**C:\ProgramData\Quest\IT Security Search\ITSearch.cer**) and remove the existing certificate.
3. Get the new thumbprint of the certificate using below steps:
  - a. Double click the new certificate.
  - b. Navigate to **details** tab.
  - c. Fetch the value of thumbprint key.
4. Run **C:\Program Files\Quest\IT Security Search\Scripts\New-CertificateBinding.ps1**.
5. It will request for thumbprint value. Use the value which was fetch in the above step and press **Enter**.

## What Accounts to Use

In the course of IT Security Search setup, you create the Warehouse configuration database. Make sure you run setup under an account that has sufficient privileges to create databases on your SQL server.

Setup also prompts you to specify the accounts to use for the following:

- Warehouse server account configuration
- Warehouse API installation

For smooth IT Security Search operation, it is recommended that you specify a single account that is configured as follows:

1. Membership in the **Administrators** computer local group on the computer where you want to install IT Security Search.
2. DBO access to the Warehouse configuration database.
3. Full Control access to the network shares that you want to use as Warehouse stores.

You should create or appoint this account in advance. After IT Security Search installation, ensure that the account has the privileges listed above.

**i** | **IMPORTANT:** If you use SQL Server authentication for access to the Warehouse configuration database, the SQL Server account's password should be set to never expire.

# Security Details and Configuration

By default, IT Security Search uses a self-signed SSL certificate, which will cause security errors for IT Security Search users. You can provide a new certificate at any time. Your certificate can be either self-signed or issued by a certificate authority. Using a certificate generated by your organization and signed by a certificate authority is recommended.

## Providing a CA-Signed Certificate

If your company uses a registered SSL certificate, run the **New-CertificateBinding.ps1** PowerShell script described below to make IT Security Search use the certificate.

You can obtain a CA-signed certificate using Windows native tools and then bind it, as follows:

1. Log on to the IT Security Search server using an IT Security Search administrator account.
2. Run Microsoft Management Console (**mmc.exe**) and add the **Certificates** snap-in.
3. Select **Computer Account** and click **Next**.
4. Select **Local Computer**, and then **Finish**.
5. Click **OK** in the Add or Remove Snap-ins dialog box.
6. In the console, right-click **Certificates (Local Computer) | Personal | Certificates** and select **Request New Certificate** to start the Certificate Enrollment wizard.
7. Click **Next** and **Next** again to use the Active Directory Enrollment Policy.
8. Locate the Web Server certificate template and clear its check box. If you cannot see this template, make the check box to show all templates is selected. If you can see the template but don't have permission to enroll, contact your Certificate Authority administrator to be granted the **Enroll** permission for the account of the computer where IT Security Search is installed.
9. Click the **More information is required to enroll for this certificate** link.
10. On the **Subject** tab, from the drop-down menu under **Subject name** select Common Name and enter the NetBIOS name of the IT Security Search server. Click **Add**.
11. From the drop-down menu under **Alternative name**, select **DNS** and enter the NetBIOS of the IT Security Search server. Click **Add**.
12. From the drop-down menu under **Alternative name**, select **DNS** and enter the FQDN of the IT Security Search server. Click **Add**.
13. Change the drop-down menu to **IP address (v4)** and the IP address will be automatically supplied. Click **Add**.
14. Change the drop-down menu to **IP address (v6)**. If IPv6 is enabled, the IP address will also be automatically supplied. Click **Add**. If nothing is supplied, you can safely skip this step.
15. In the same section, if necessary, enter any predefined names that DNS records have been created for, such as "IT Security Search Console", so the certificate matches the name of the URL used for access to the page.

16. Go to the **General** tab and enter a **Friendly name**, for example **IT Security Search Certificate**. Optionally, add a description.
17. Go to the **Extensions** tab, expand **Extended Key Usage** and confirm that **Server Authentication** is available appears under **Selected options**.
18. Click **Apply**, then click **OK**, then click **Enroll**.
19. The new certificate should now appear in the **Certificates** folder, under **Personal**.
20. Export the certificate by right clicking it and selecting **All Tasks | Export**.
21. In the Certificate Export wizard, click **Next**.
22. On the next step, make sure the **No, do not export the private key** radio button is selected. Click **Next**.
23. Select the **DER encoded binary X.509 (.CER)** radio button and then click **Next**.
24. Click **Browse** to select where to save the certificate. For example, save it in **%ProgramFiles%\Quest\IT Security Search** and give the file a descriptive name.
25. Click **Next** and then click **Finish**. The certificate is saved at the specified location.
26. To make IT Security Search use this new certificate, run the **New-CertificateBinding.ps1** script as described below, supplying the file you saved on the previous step.

## Providing a Self-Signed Certificate

To create a new self-signed certificate, use the **New-SslCertificate.ps1** PowerShell cmdlet located in the **Scripts** subfolder of your IT Security Search installation folder. By default, the certificate is set to be in effect from the current date until December 31, 2039.

The cmdlet has the following parameters:

Parameter	Type	Description
-FilePath	string	The path to your certificate file.
-Subject	string	The subject of the certificate.
-SubjectDnsAltNames	string	Optional: a list of alternative names for the IT Security Search server (IP addresses, NetBIOS name and so on). If this parameter is omitted, the certificate will be generated for all possible alternative names of the specified host (IPv4 address, IPv6 address, FQDN, NetBIOS, but not for localhost or 127.0.0.1).
-Begin	datetime	Optional: the date from which the certificate is in effect; by default, from the current day.
-End	datetime	Optional: the date until which the certificate is in effect; by default, until December 31, 2039.
-KeepExisting	switch	Whether any existing file with the specified name should be kept instead of overwritten.

Example:

```
powershell -file "C:\Program Files\Quest\IT Security Search\Scripts\New-SslCertificate.ps1" -filepath "c:\temp\ITSearch.cer"
```

After you have generated the certificate (and ideally, had it signed by a CA), perform the procedure described in [Binding Your Certificate](#).

# Binding Your Certificate

To begin using your self-signed or CA-signed certificate, use the **New-CertificateBinding.ps1** cmdlet, which is located in the **Scripts** subfolder of your IT Security Search installation folder. The cmdlet has the following parameters:

Parameter	Type	Description
-FilePath	string	The path to your certificate file.
-Port	int	The port that IT Security Search uses. It is specified during setup, the default port is 443.
-Force	switch	If this switch is set, then any existing certificate will be unbound from the specified port. If the switch is not set, then the existing certificate will be kept instead of the specified one.
-FilePassword	SecureString	If your certificate is a password protected .PFX certificate, you need to provide this parameter.
-Thumbprint	string	The thumbprint of your certificate stored in Windows certificate store.

## Examples:

```
powershell -file "C:\Program Files\Quest\IT Security Search\Scripts\New-CertificateBinding.ps1" -filepath "c:\temp\ITSearch.cer" -port 443 -Force
```

```
powershell -file "C:\Program Files\Quest\IT Security Search\Scripts\New-CertificateBinding.ps1" -thumbprint 'AAFB5E587E91F0C81F6ED2FDD45F911AFF35C8E2D' -port 443 -Force
```

# Revoking a Certificate

To revoke a certificate that is currently in use by IT Security Search, run the **Delete-CertificateBinding.ps1** cmdlet located in the **Scripts** subfolder of your IT Security Search installation folder.

## Example:

```
powershell.exe -file "C:\Program Files\Quest\IT Security Search\Scripts\Delete-CertificateBinding.ps1" -Port 443
```

The **-Port** parameter specifies the port that the certificate is bound to.

**!** **CAUTION:** After you perform this operation, the IT Security Search service becomes unavailable until a new certificate is bound. Prepare the next certificate in advance to avoid downtime.

# How IT Security Search Security Features Are Implemented

IT Security Search security is based on the Windows Data Protection API (DPAPI). For details about its security features, see the "Windows Data Protection" MSDN article; at the time of this writing it is located at <https://msdn.microsoft.com/en-us/library/ms995355.aspx>.

## Enabling Secure Data Transfer for IT Security Search Warehouse

By default, IT Security Search Warehouse uses the insecure HTTP protocol. The steps below describe how to enable HTTPS for the Warehouse.

**CAUTION:** Before you begin, consider the following:

- **Functionality associated with IT Security Search Warehouse will be unavailable during the switch.**
- **The procedure should be performed at a time when Enterprise Reporter is not pushing data. Choose a time between discoveries, and confirm that all data from the latest discovery has been sent.**
- **We recommend stopping the Quest IT Security Search and Quest IT Security Search Active Roles Data Attendant services on the IT Security Search server for the duration of the switch to HTTPS.**

### To switch IT Security Search Warehouse to using HTTPS

1. (Conditional) Provide a CA-signed certificate, as described in [Providing a CA-Signed Certificate](#) above. If you have already installed such a certificate for use on port 443, you can skip this step.
2. In the **Scripts** subfolder of your IT Security Search Warehouse API installation folder, locate the **Enable-SecureEndpoint.ps1** script.
3. Run this script in PowerShell in Administrator mode. For the **-thumbprint** parameter, specify the thumbprint of your existing certificate in the certificate store. If you omit the **-port** parameter, the script makes the Warehouse share port 443 with IT Security Search.  
Example:  

```
powershell -file "C:\Program Files\Quest\IT Security Search Warehouse\Scripts\Enable-SecureEndpoint.ps1" -thumbprint 'AAFBE587E91F0C81F6ED2FDD45F911AFF35C8E2D' -port 443
```
4. Start or restart the Quest IT Security Search and Quest IT Security Search Active Roles Data Attendant services.

After you have completed these steps:

- Confirm that the Enterprise Reporter and Active Roles connectors are working. For that go to those connectors' settings and click **Test Connection**.
- If you use Enterprise Reporter data, open Enterprise Reporter Configuration Manager and enable secure connection to IT Search Warehouse. For more details, see Enterprise Reporter documentation.

# Running IT Security Search Services Under a Group Managed Service Account (gMSA)

To set up a gMSA to run IT Security Search services, you need to perform a few configuration procedures, as explained below.

## Make the gMSA a Server Administrator

Your gMSA must have local administrative rights on the computer where IT Security Search is installed. Make sure the gMSA is in the local **Administrators** group on the computer.

## Set Up Password Retrieval

You need to use PowerShell to allow your gMSA to retrieve the managed password from the domain controller. In the PowerShell prompt, run the following commands (assuming that the name of your gMSA is **my\_gmsa**):

```
Add-WindowsFeature RSAT-AD-PowerShell  
  
Install-ADServiceAccount -Identity my_gmsa
```

## Set the Service Account

The following steps need to be taken for each of the following services:

- ITSS.Server
- ITSS.DataAttendant.ActiveRoles
- ITSS.Warehouse

### *To set the gMSA for a service*

1. Open the properties of the service.
2. On the **Log On** tab, select **This account** and specify your gMSA in **domain\user\$** format. The dollar sign at the end is required. For example, if your gMSA is **my\_domain\my\_gmsa**, then type **my\_domain\my\_gmsa\$**. Leave the password fields empty.

**i** **NOTE:** When the service is configured, you may get a message that the account has been granted the “Log On As a Service” right.

3. Restart the service.

## Finalize Warehouse Reconfiguration

Finally, configure the InTrust Server service (**adcrpcs**) to use this gMSA, as described in [Minimal Rights and Permissions Required for InTrust Operations](#).

# Who Can Do What in IT Security Search

There are two roles that IT Security Search associates with users that access it: *operator* and *administrator*. Unless your user account is one of these, you do not have access to IT Security Search.

Each operator has a scope of responsibility, which defines which features the operator can use. To make an account an operator, include it in the IT Security Search access control list. This list is available on the IT Security Search **Settings** page, on the **Security** tab. You can supply individual users in **domain\user** format or security groups in **domain\group** format.

An administrator can do the following:

- Search everywhere
- Perform Active Directory recovery if the Recovery Manager data link is enabled
- Configure the connectors to the data-providing and operations management systems, as described in [Where the Data Comes From](#)
- Assign operator roles

To give a user account administrator privileges, make the account a member of the **IT Security Search Administrators** local group on the computer where IT Security Search is installed. You can assign the administrator role by specifying Active Directory groups or individual users. If an account is an administrator and an operator at once, the administrative privileges take precedence and the account's operator scope has no meaning. The user account that performs IT Security Search installation automatically becomes an administrator.

## Setting the Scope of Responsibility for an Operator

For each operator you add, specify the scope of objects visible to the operator by supplying a list of organizational units. In addition, you can further tweak the scope by specifying a search query. The resulting scope is the OR-based union of the results of the list and the query.

If you want to make everything visible to an operator, leave the list and query empty (for the OU list, specifying the asterisk wildcard \* also has the same effect). If you want to limit an operator's scope, follow the instructions below.

### ! CAUTION:

**If you use an asterisk for the OU list or leave it empty, InTrust events will not be affected by the scope delegation settings. All operators can see all InTrust events in this case.**

**If the OU list specifies OUs, InTrust events will be returned only if the Enterprise Reporter connector is enabled and configured.**

# Creating the List of OUs

To make the right decisions when specifying OUs, make sure you understand the relevance of these OUs to the results that the operator is going to get. The following table explains how the choice of OU affects the scope, depending on the type of object:

What type of object the operator looks for	The operator sees the object if...
Active Directory user, group or computer	It is in the OU (or any OU nested in it)
OU	It is the same OU or it is nested in the OU at any level
Computer that isn't in a domain	—
Computer local user or group	The computer is in the OU (or any OU nested in it)
File or network share	The hosting computer is in the OU (or any OU nested in it)
InTrust event	<p>If the OU list is empty or an asterisk, scope settings are irrelevant and the operator can see all InTrust events.</p> <p>If the Enterprise Reporter connector is enabled and the OU list specifies OUs:</p> <ul style="list-style-type: none"><li>• If the event has the <b>Whom</b> field, the operator sees it as long as the OU (or any OU nested in it) contains the object in <b>Whom</b></li><li>• Otherwise, the operator sees it as long as the OU (or any OU nested in it) contains the object in <b>Where</b></li></ul>
Non-InTrust event	<ul style="list-style-type: none"><li>• If the event has the <b>Whom</b> field, the operator sees it as long as the OU (or any OU nested in it) contains the object in <b>Whom</b></li><li>• Otherwise, the operator sees it as long as the OU (or any OU nested in it) contains the object in <b>Where</b></li></ul>

The OUs must be listed in canonical name format, one OU per line.

## Fine-Tuning the Scope with Queries

The queries you specify return not just OUs but any objects with the specified field values. You can supply any query that follows IT Security Search syntax conventions. For details, see [Search Term Syntax](#).

### **i** IMPORTANT:

- The results will contain objects that match the OU list, the query, or both. For example, if the query returns an object from an OU that isn't listed, the object is included in the results anyway.
- Functions such as **MemberOf** and **Members\_Deep** don't work in queries specified here.

Filtering by OU is not applicable to data from Azure, because Azure objects aren't organized into OUs. If you are interested in Azure objects, a good way to get them is to use a query that contains the **Tenant** field.

Use the **Test query** action link to make sure your query is valid and returns what you need. Note that the OU list doesn't affect the results of **Test query**.

## Auto-Lookup of Operator Data in a Query

To quickly supply the identifying details of an operator without looking them up in Active Directory, you can use the **{Context.CurrentUser}** variable as a field value. Alternatively, you can access specific identifying fields for the operator's account using syntax such as **{Context.CurrentUser.FullAccountName}** or **{Context.CurrentUser.AccountSid}**. For details about this technique, see the [Auto-Resolution of the Current User section of the Search Term Syntax topic](#).

If you specify a group (instead of a user) as an operator, then the resolution works for all members of the group (direct or indirect) when they use IT Security Search.

Queries containing the variable are stored as supplied, and the variables are resolved only when the queries are applied. Therefore, the resulting identifying data is always up to date.

## Examples

OU list	Query	Details
	FacilityName:AD AND What="user changed"	Searches by an operator with this scope will return all events of the "user changed" type from Active Directory.
OU1 OU2	"Tenant=T1 OR Tenant:T2"	Searches by an operator with this scope will return all objects related to OU1, all objects related to OU2, all objects where the <b>Tenant</b> field equals "T1" and all objects whose <b>Tenant</b> field contains "T2".
OU3	"Tenant=T3"	Searches by this operator will return all objects related to OU3 and all objects whose <b>Tenant</b> field equals "T3".  If the scope is defined for a group and the operator from the previous example is a member of that group, then that operator's scope is extended and becomes: all objects related to OU1, OU2 or OU3, all objects where the <b>Tenant</b> field equals "T1" or "T3" and all objects whose <b>Tenant</b> field contains "T2".
OU4	Eventid=4740	Searches by this operator will return all objects related to OU4 and all events (no matter if related to the listed OUs) with event ID 4740.

# Controlling Active Directory Recovery Privileges

In addition to visibility scope, you can configure which operators can restore Active Directory objects. For that, use the **Restore backups** option in the **Allowed Operations** column of the table. The actual recovery functionality is provided by the Recovery Manager for Active Directory connector. For details, see [Recovery Manager for Active Directory Server](#).

# Where the Data Comes From

IT Security Search relies on data provided by auditing and operations management systems. At this time, the following systems are supported:

- InTrust
- Change Auditor
- Enterprise Reporter
- Recovery Manager for Active Directory
- Active Roles
- Splunk

You can connect to any combination of these systems. However, to make the most of IT Security Search, you should establish links with all of them that are available to you. IT Security Search is designed to correlate the data they supply, sparing you the effort of trying to match disparate bits of information to build up a picture.

For example, an event captured by InTrust can prompt you to examine the initiator user account closely; user information is provided by Enterprise Reporter. Next, you might be interested in recent changes to the user account; this information comes from Change Auditor. With all three systems interconnected, these transitions from one piece of data to another are quick and seamless.

Support for Recovery Manager for Active Directory lets you perform recovery directly from the IT Security Search interface in addition to viewing a list of available backup states. For each of them, a link is provided that lets you restore that particular state. If the object was changed rather than deleted, you can select specific modified attributes to restore. If it was deleted, you can only restore it to a full state.

## Specifying Data Sources

To configure the connections between IT Security Search and any of the supported systems available in your environment, go to the IT Security Search settings page. To open this page, click **Settings** in the upper right corner. See the following topics for details about connection configuration for each of the systems:

- [InTrust](#)
- [Change Auditor](#)
- [Enterprise Reporter](#)
- [Recovery Manager for Active Directory](#)
- [Active Roles](#)
- [Splunk](#)

# Change Auditor Database

Change Auditor produces information about what is happening to critical resources such as Active Directory, Exchange or files on file servers, or in cloud environments such as Azure and Office 365. Generally, whenever you are looking for an answer to the question “What changed in the environment?” in IT Security Search, the data is likely provided by Change Auditor.

To start configuring the Change Auditor database data link, select the **Connector enabled** option. To set up connection to the Change Auditor database, configure the standard SQL Server database access settings:

- Server name
- Database name
- Authentication type  
The following options are available:
  - Windows authentication  
Make sure the Active Directory account you specify is granted **Read** and **Execute** permissions on the database.
  - SQL Server authentication  
Specifies that SQL Server-specific credentials are used.
- User name and password

To verify that your Change Auditor database access works, click the **Test Connection** link.

Finally, click **Apply**.

**! CAUTION:** To make Change Auditor generate the events you want to see in IT Security Search, configure monitoring of the Active Directory attributes you are interested in. For that, in the configuration of the Auditing task, in the AD Attribute Auditing page, go to Forest Attributes. Select the object class and enable monitoring for the necessary attributes.

For details about working with Change Auditor tasks, see the [Change Auditor User Guide](#).

# InTrust Repository

InTrust collects audit events from a wide range of logs on a variety of platforms. Generally, whenever you are looking for an answer to the question “What happened?” in IT Security Search, the data is provided by InTrust.

To start configuring the InTrust repository data link, select the **Connector enabled** option. To set up connection to one or more InTrust repositories with audit data, configure the following:

- InTrust server name and credentials  
This is an InTrust server in the InTrust organization where the repository is registered. There can be multiple servers in an InTrust organization, and any of them is accepted.  
Make sure access to repositories is configured for the account you supply:
  - The account must be a member of the computer local **AMS Readers** group on the InTrust server.
  - The account must have Read permissions on the network share that makes the repository available.
- The repository or repositories to connect to

## **i** NOTES:

- The page shows the date of the last gathered event across all of the included repositories.
- If there was recently a problem with a repository, indicated by an error icon, hover the mouse cursor over that repository, and a tooltip will show the error message.

To verify that your repository access works, click the **Test Connection** link.

Finally, click **Apply**.

# Enterprise Reporter

Enterprise Reporter retains information about the configuration of critical systems. Generally, whenever you are looking for an answer to the question “What settings are configured for this?” in IT Security Search, the data is provided by Enterprise Reporter.

IT Security Search receives and stores data that is forwarded from Enterprise Reporter. The Warehouse component is responsible for the capture and storage.

To start configuring the Enterprise Reporter data link, select the **Connector enabled** option. However, most of the configuration occurs on the pushing end.

## Setting Up Forwarding in Enterprise Reporter

1. In Enterprise Reporter Configuration Manager, under System in the left pane, click **Configuration**.
2. In the System Configuration view, click **IT Security Search**.
3. In the Add IT Security Search Configuration dialog box that opens, configure the connection to your IT Security Search server. The account that you supply must be an IT Security Search administrator, meaning a member of the computer local **IT Security Search Administrators** group on the IT Security Search server. For details about administrative privileges, see [Who Can Do What in IT Security Search](#).

The next push will occur after the next Enterprise Reporter discovery.

## Making All Data Cohesive with Enterprise Reporter

IT Security Search provides the **Who**, **Whom** and **Where** smart aliases for record fields in the data it analyzes. This ensures that you get associated data from unrelated sources using the same terms in your search queries.

The necessary field mapping is created from Enterprise Reporter data. For example, if the Enterprise Reporter connector is configured, you can proceed from the user details page directly to a list of events initiated by the user. Otherwise, the **Activity initiated by this user** link may not even be available in the details, or it may produce fewer results than it should.

To make sure Enterprise Reporter provides the data for the mapping, configure a recurring Active Directory discovery that includes users and computers in its scope. Set the frequency of the discovery according to the policies in your environment.

# Ensuring Correct Object Counts for OUs

By default, the **Do not collect object counts** option is enabled for Active Directory discoveries in Enterprise Reporter. If IT Security Search uses data obtained by such discoveries, it shows zeros for the number of users, groups and so on in the details of OUs. To make IT Security Search show the correct object counts, make sure the **Do not collect object counts** option is cleared for your Active Directory discoveries.

## Recovery Manager for Active Directory Server

Recovery Manager for Active Directory performs Active Directory recovery at any level: from individual objects and attributes to entire domains and, in the case of Recovery Manager for Active Directory Forest Edition, even Active Directory forests. IT Security Search lets you track recovery-related activity. Enabling the Recovery Manager for Active Directory data link makes it possible to list available backup states and restore objects to any of them.

**NOTE:** You cannot perform forest-level recovery from IT Security Search.

To start configuring the Recovery Manager for Active Directory data link, select the **Connector enabled** option. To set up connection to Recovery Manager for Active Directory, configure the following:

1. Recovery Manager connection settings  
Specify the Recovery Manager server to connect to and the credentials to use for running PowerShell cmdlets on that server. The account you supply must have local administrator privileges on the server.
2. Active Directory connection settings  
Specify the Active Directory domain or a particular domain controller and the credentials to use for working with backup data. The account you supply must be powerful enough to both read the backup configuration and perform recovery by applying backup states.

For up-to-date details about the permissions required for access to Recovery Manager for Active Directory, see the [Recovery Manager for Active Directory Deployment Guide](#).

To make sure that you have specified valid account or accounts, click the **Test connection** link. This verifies that the credentials are valid and suitable for running searches. However, it does not ensure that the Active Directory access account can perform recovery operations.

## Active Roles

Active Roles simplifies and streamlines creation and ongoing management of user accounts, groups and other objects in Active Directory. Generally, whenever you are looking for an answer to the question “What is known about this user or group?” in IT Security Search, the data can be provided by Active Roles.

Active Roles brings information about the following:

- Users
- Groups
- Computers
- OUs

- Active Directory change events as logged by Active Roles
- Active Roles-specific information:
  - Virtual attributes of objects
  - Dynamic groups and their membership rules
  - Management history
  - Managed units

To start configuring the Active Roles data link, select the **Connector enabled** option. To set up connection to the Active Roles server, configure the following settings:

- Server name
- User name and password  
The account you supply must be powerful enough to do the following:
  - Read Active Directory data
  - Run PowerShell cmdlets on the Active Roles server

To verify that your Active Roles server access works, click the **Test Connection** link.

Finally, click **Apply**.

**CAUTION:** For the connection to the Active Roles server to work, make sure that port 15172 is opened for both inbound and outbound traffic on that server.

## Management History Synchronization Specifics

Management history synchronization between IT Security Search and Active Roles does not happen directly. IT Security Search uses its own “warehouse” component as an intermediary data store. The first synchronization can take a long time, because all available history has to be processed. After that, synchronization involves only the most recent data.

## Splunk

The Splunk connector retrieves searchable data from Splunk.

The connector has the following minimal configuration options:

- Splunk server URI
- The user name and password of the account to use for access to Splunk

One additional setting that you may want to configure is the number of retrieved Splunk results. By default, Splunk returns 50,000 objects, whereas IT Security Search shows 100,000 per page. To make these limits consistent, take the following steps:

1. On the Splunk server, open (or create if necessary) the **%programfiles%\Splunk\etc\system\local\limits.conf** file (on Windows) or **/opt/splunk/etc/system/local/limits.conf** file (on Linux) in a text editor.

2. Add the following lines to the file:

```
[restapi]
maxresultrows = 100000
```

3. Restart Splunk.

A predefined Splunk-to-IT Security Search field mapping is provided out of the box. If you find that this mapping doesn't suit you, call Quest Support. This will help improve Splunk integration for you and everyone else.

# HTTPS API for Forwarded Change Auditor Events

IT Security Search 11.6.1 contains an early implementation of support for retrieval of forwarded Change Auditor data in the Warehouse connector. This feature preview is provided as-is, so that you can try it out, give us feedback and help us make it more useful in a future release.

## Before You Begin

First, make sure the **ITSS.Warehouse** service is running on your IT Security Search server. This is required for a successful Change Auditor subscription.

## Getting Change Auditor Ready

To make Change Auditor push audit data to Warehouse, run the **CreateCAITSSEventSubscription.ps1** PowerShell script, which is located in the **<Change Auditor installation folder>\Client\PowerShell Sample Scripts** folder on your Change Auditor coordinator. This will start a multi-step configuration procedure in the command prompt, where you will need to specify the settings for your particular environment.

The following are examples of values that you can supply for some of the prompts:

- Specify Change Auditor installation name  
**DEFAULT**
- Enter the number(s) of the subsystem events to be forwarded (separate multiple entries with commas)  
**1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18**
- Specify the destination URL and port for the ITSS warehouse instance  
**https://myitssserver:443/warehouse/changeauditor/events**

**i** **NOTES:** To find out which port is used, check the **HKEY\_LOCAL\_MACHINE\SOFTWARE\Quest\IT Security Search Warehouse API\ListenPort** registry value on the IT Security Search server. To see whether HTTPS is used instead of HTTP, check the **HKEY\_LOCAL\_MACHINE\SOFTWARE\Quest\IT Security Search Warehouse API\ListenScheme** registry value.

- Enter a coordinator DNS or NetBIOS name (or press enter to finish)  
**mycacoordinatorvm1,someothercacoordinatorvm9**

The following additional scripts are also provided to let you manage your IT Security Search subscriptions:

- GetCAITSSEventSubscriptions.ps1
- ModifyCAITSSEventSubscription.ps1
- RemoveCAITSSEventSubscription.ps1

## Getting IT Security Search Ready



### IMPORTANT:

- Using Change Auditor connector and the Warehouse connector to get data from the same Change Auditor coordinator at once is not recommended as it might result in duplicate events in your searches.

# Running Searches

To begin searching, enter what you are looking for in the search box. For example, start with a user name, a network share path, a computer name or a phrase to look for in event fields.

A search involves all available item types (events, users, files, computers and so on) at once, no matter which item type is currently highlighted. By default, the number of results returned is limited to 100,000. For Recovery Manager for Active Directory items, the limit is fixed at 5,000.

## Viewing Data by Object Type

IT Security Search groups the discovered data by object type:

- Computers
- Events
- Files
- Groups
- OUs
- Shares
- Users
- Various other object types for which only Enterprise Reporter provides data, such as those related to Exchange, Azure and Office 365.

You can restrict the view to these object types by clicking the corresponding tab at the top of the grid; for miscellaneous object types provided only by Enterprise Reporter, click the **More** tab. On this tab, you have the option to make a dedicated tab for any such object type. For that, locate its item in the **Object Type** list on the left and click the pin icon on that item; this pins a new tab for the object type next to the **More** tab. When you don't need the tab any more, you can close it; you can pin it again later at any time.

**i** **NOTE:** The number of items displayed on pinned tabs is limited to 100,000, as for predefined tabs. On the **More** tab, it is limited to 1000 items per object type.

The object type is also switched when you use links in the context of some object's details, such as **Activity initiated by this user** or **Who granted permissions to this file**.

## Specifying a Time Range for Events

To display events from only a specific time period, use the time range filter. For that, click the clock icon in the search box. If you choose not to specify a time range, the search will involve all available data.

# Customizing the Event Grid Layout

When you view events of a particular kind, you may want to see a specific set of fields, including fields unique to such events. You may also want to hide fields that don't matter to you. To make such changes to the event layout, use the tools in the Columns drop-down menu to the right of the grid.

To add a field as a column, type its name in the text box provided in the drop-down menu and click **Add**. You can specify any name. To look up the correct field names, use the details view for any relevant event.

To remove an existing column, click the trash can icon next to its name.

To restore the default set of fields, click **Reset to defaults**.

To reorder columns, drag their headings around in the grid.

Your custom layout settings are used when you export events to PDF or CVS (using the **Export to** drop-down menu).

# Understanding the Event Timeline

The event timeline is a bar graph representation of search results, where you can quickly spot event patterns. For example, it helps you find out the peak hours for the events you are interested in or easily track activity outside business hours.

# Viewing Details of Search Results

When you select an item from the result list, the right pane shows brief details about the item. To go to the full details view for this item, click **View Details**.

The details view also suggests links to related data which you might be interested in and which you might be trying to find in the first place. Clicking such a link starts a search in an automatically supplied context. For example, when you are viewing the details of a folder in a network share, the following links are ready for you:

- Who accessed this folder
- Who granted permissions to this folder
- Files and folders in this share

Information about users, groups, computers and organizational units can come from more than one source. At this time, the following systems provide data about them: Enterprise Reporter, Recovery Manager for Active Directory and Active Roles. When multiple sources have information about the same object, IT Security Search shows data from the source that submitted it first, so that the results can be displayed sooner. A warning is shown about additional data that may be available. If you want these results, click the **run a full scan** link in the warning text. This will cause IT Security Search to retrieve the data from the remaining sources and correlate it.

# Navigating Session History Using Breadcrumbs

As you work with the search results, your search path is saved as a breadcrumb sequence. This helps you go back to any previous step in your session without retracing the steps.

# Using Facets to Filter Results

Facets are quick view filters by property value. When you apply a facet, IT Security Search shows only matching items. You can apply multiple facets at once, progressively limiting the number of results; you can also remove any of the facets you have applied.

Facets are shown to the left of the result pane. To apply a facet, click an available value link. For example, if you are viewing the details of a deleted user account (where the value of **State** is **Deleted**) and want to focus on other deleted users, click the **Deleted** link.

Alternatively, you can use the item's properties to work with facets. The properties that support this have funnel icons next to them in the details pane. To apply a facet, click such a property.

# Fine-Tuning Your Search Terms

Simple searches produce results where the term you specify is contained anywhere in the discovered data. To make your searches less broad and more relevant, you can use hints—for example, by prefixing the field names to look in. For details, see [Search Term Syntax](#).

# Automating Complex Search Scenarios

Some search workflow ideas are best expressed as multi-stage search queries where data produced by a search is automatically streamed into the next search in a chain. The pipe operator (|) helps you achieve this, and field names in curly braces specify which fields to analyse in that data.

Example 1: Find the managers of all users who have created or deleted files on the **\\FILESRV1\Software** network share

```
"\\FILESRV1\Software" | Description:{SharePath} AND (What="File Created" OR What="File Deleted") | Who={Who} | DisplayName="{ManagedByDisplayName}"
```

Example 2: Find events by users from the Milwaukee office on computer FILESRV1

```
Office="Milwaukee" | Who:{SAMAccountName} AND Where:filesrv1
```

Example 3: Find computers where members of the **Accounting** group have logged in

```
"Accounting" | Who:{SAMAccountName} AND What:logon | Where={Where}
```

Example 4: Find all users from the same office as user **dshaw**

```
Who="dshaw" | Office="{Office}"
```

# Search Term Syntax

Use the following syntax for search terms in the search box. Searches are case-insensitive.

## i NOTES:

- Asterisk wildcards in an initial position are currently not supported for events provided by InTrust and Recovery Manager for Active Directory. This limitation does not apply to data provided by Change Auditor and Enterprise Reporter.
- If you specify file system paths (such as **C:\Windows**) or Active Directory distinguished names (such as **CN = Builtin, DC = k1test16, DC = test, DC = local**) as search terms, enclose them in quotation marks. This is necessary due to the way the search engine treats the backslash (as an escape character) and the equality sign (as an attribute indicator).

For details about the fields that you can use in your search queries, see [Data Field Reference](#).

## Single-Word Terms

This is known as full-text search. The search involves all available fields and uses the Contains operator.

Meaning	Syntax	Details
Look for a single-word term in any attribute	Word without spaces Example: <b>john</b>	<b>john</b> matches <b>John</b> or <b>john</b> in any attribute, but does not match <b>stjohn</b> in any attribute
Look for a single-word term with the specified beginning in any attribute	Word ending in an asterisk (*) without spaces Example: <b>john*</b>	<b>john*</b> matches <b>John</b> or <b>Johnson</b> in any attribute
Find attributes where a specific single-word term is not contained in any attributes	Word without spaces with a leading hyphen Example: <b>-john</b>	<b>-john</b> may match entries that contain <b>stjohn</b> , but does not match entries that contain <b>john</b> in any attribute
Find entries where a specific single-word term with the specified beginning is not contained in any attributes	Word ending in an asterisk (*) without spaces with a leading hyphen Example: <b>-john*</b>	<b>-john*</b> may match entries that contain <b>stjohn</b> , but does not match entries that contain <b>john</b> or <b>johnson</b> in any attribute

## Term Combinations

Meaning	Syntax	Details
Look for entries with specific single-word terms in any attributes	Words separated by spaces Example: <b>john glen*</b>	<b>john glen*</b> matches <b>john</b> and <b>glen</b> , or <b>john</b> and <b>glenda</b> , or <b>john</b> and <b>glen</b> and <b>glenda</b> , wherever they are found
Look for entries that do not contain specific single-word terms in any attribute	Word without spaces Examples: <ul style="list-style-type: none"><li>• <b>-john -glen</b></li><li>• <b>john -glen*</b></li></ul>	<ul style="list-style-type: none"><li>• <b>-john -glen</b> matches entries that do not contain <b>john</b> or <b>glen</b> anywhere</li><li>• <b>john -glen*</b> matches entries that contain <b>john</b> in any attribute and at the same time do not contain <b>glen</b> or <b>glenda</b> anywhere</li></ul>
Look for entries with a specific multiple-word	Phrase in quotation marks Example: <b>"Account Logon"</b>	<b>"Account Logon"</b> matches entries that contain the exact phrase <b>Account Logon</b> in any attribute

Meaning	Syntax	Details
phrase in any attribute		
Look for entries that do not contain a specific multiple-word phrase in any attribute	Phrase in quotation marks Example: <b>logon server01 - "Account Logon"</b>	<b>logon server01 -"Account Logon"</b> matches entries that contain the words <b>Logon</b> and <b>server01</b> anywhere but do not contain the exact phrase <b>Account Logon</b> in any attribute
Meet one of the specified terms (or sets of terms)	<p>Terms (single words or phrases) separated by the <b>OR</b> operator; this operator has the following specifics:</p> <ul style="list-style-type: none"> <li>• It is case-sensitive: it must always be specified as <b>OR</b></li> <li>• It denotes a choice between everything to the left of it and everything to the right of it</li> <li>• You can use multiple <b>OR</b> operators in a query; the boundary of an <b>OR</b> clause is the beginning of the query, the end of the query, or another <b>OR</b></li> </ul> <p>Examples:</p> <ul style="list-style-type: none"> <li>• <b>paul john OR thomas</b></li> <li>• <b>-"logon/logoff" server01 OR stjohn</b></li> </ul>	<ul style="list-style-type: none"> <li>• <b>paul john OR thomas</b> matches entries that contain either both <b>John</b> and <b>Paul</b>, or <b>Thomas</b> anywhere</li> <li>• <b>-"logon/logoff" server01 OR stjohn</b> matches either entries without the phrase <b>Logon/Logoff</b> that contain <b>server01</b>, or entries with <b>stjohn</b> (no matter whether they contain the phrase <b>Logon/Logoff</b>)</li> </ul>
Explicitly mark an AND operation for visual clarity	<p>Terms (single words or phrases) separated by the <b>AND</b> operator; this operator has the following specifics:</p> <ul style="list-style-type: none"> <li>• It is case-sensitive: it must always be specified as <b>AND</b></li> <li>• It can be omitted wherever it occurs</li> </ul> <p>Examples:</p> <ul style="list-style-type: none"> <li>• <b>paul AND john</b></li> <li>• <b>paul john</b></li> </ul>	<b>paul AND john</b> and <b>paul john</b> are identical in meaning: look for entries where both <b>paul</b> and <b>john</b> occur.
Group and nest terms for logical operations on them	<p>Parentheses enclosing the terms you want to group Example: <b>(homer marge) OR (peter lois)</b></p>	<b>(homer marge) OR (peter lois)</b> matches either entries with both <b>homer</b> and <b>marge</b> , or entries with both <b>peter</b> and <b>lois</b> . It does not match entries with both <b>peter</b> and <b>homer</b> that do not contain <b>lois</b> or <b>marge</b> .

## Searching in Specific Attributes

To apply your search term only to a particular attribute, prepend the name of the attribute with a colon (:) or equals sign (=) to your search term, as shown in the table below. If the attribute name is made up of multiple words, enclose it in brackets (as in **[log name]:security**). All the syntax conventions described above also apply.

The following distinction is important:

- Labels unambiguously mapped to entry attributes; for example, **Path:"Documents and Settings"** in file access entries  
In this case, the search involves the specified field and uses the Contains operator.
- Labels mapped to different attributes in different contexts (known as normalized attributes); for example, **Where:primrose** would mean the **primrose** domain for users or groups, the **primrose** computer for files or shares, and so on  
In this case, the search involves the associated fields as necessary and may even modify the search terms.

For details about the meanings of labels in particular contexts, see [Normalized Attributes](#) below.

**i** **NOTE:** When you look for permission information, you can use the Who, What and Owner attributes as follows:

- With regard to files, Who means the account that has permissions.
- Use What to specify the permission.
- Owner is not a real permission, but you can use it (as in **What:Owner**) to find the owner of a file.

Meaning	Syntax	Details
Attribute contains term	Examples: <ul style="list-style-type: none"> <li>• <b>user:stjohn</b></li> <li>• <b>description:"Special privileges assigned"</b></li> </ul>	<ul style="list-style-type: none"> <li>• <b>user:stjohn</b> matches entries where the <b>User</b> attribute contains the word <b>stjohn</b></li> <li>• <b>description:"Special privileges assigned"</b> matches entries where the <b>Description</b> attribute contains the exact phrase <b>Special privileges assigned</b></li> </ul>
Attribute does not contain term	Examples: <ul style="list-style-type: none"> <li>• <b>-user:john*</b></li> <li>• <b>-description:"Special privileges assigned"</b></li> <li>• <b>-[log name]:"Directory Service"</b></li> </ul>	<ul style="list-style-type: none"> <li>• <b>-user:john*</b> matches entries where the <b>User</b> attribute does not contain the words <b>john</b> or <b>johnson</b></li> <li>• <b>-description:"Special privileges assigned"</b> matches entries where the <b>Description</b> attribute does not contain the exact phrase <b>Special privileges assigned</b></li> <li>• <b>-[log name]:"Directory Service"</b> matches entries where the <b>Log Name</b> attribute does not contain the exact phrase <b>Directory Service</b></li> </ul>

Meaning	Syntax	Details
Attribute equals term	Examples: <ul style="list-style-type: none"> <li><b>computer=server01.example.com</b></li> <li><b>description="An account was successfully logged on."</b></li> </ul>	<ul style="list-style-type: none"> <li><b>computer=server01.example.com</b> matches entries where the contents of the <b>Computer</b> attribute are exactly <b>server01.example.com</b></li> <li><b>description="An account was successfully logged on."</b> matches entries where the contents of the <b>Description</b> attribute are exactly <b>An account was successfully logged on.</b></li> </ul>
Attribute does not equal term	Examples: <ul style="list-style-type: none"> <li><b>-computer=server01.example.com</b></li> <li><b>-description="An account was successfully logged on."</b></li> </ul>	<ul style="list-style-type: none"> <li><b>-computer=server01.example.com</b> matches entries where the contents of the <b>Computer</b> attribute are different from <b>server01.example.com</b></li> <li><b>-description="An account was successfully logged on."</b> matches entries where the contents of the <b>Description</b> attribute are different from <b>An account was successfully logged on.</b></li> </ul>

## Specifying Quotation Marks

If your search term must include double quotes ("), then for each double quote you need supply an additional double quote as an escape character. See the following examples:

### To find this string    Specify this term

the "Cancel" button    "the ""Cancel"" button"

computer "kltest16"    "computer ""kltest16"""

This requirement does not apply to apostrophes, which are frequently used as quotes. Single quotes of this kind do not need escaping and should be specified in a plain string, as in **"local 'Administrator' user"**.

## Filter Syntax

Select one of the operators (explained in the following table), and enter your filter terms.

Operator	Syntax	Example	Meaning
Contains	[FieldName]:<Value>	Name:Paul	The attribute contains all of the specified terms at once in any combination
Does not contain	-[FieldName]:<Value>	-Name:John	The attribute contains none of the specified terms anywhere

Operator	Syntax	Example	Meaning
Equals	[FieldName]=<Value>	Name="John Paul"	The attribute contents are identical to the specified phrase; do not enclose the phrase in quotation marks for this operator
Does not equal	-[FieldName]=<Value>	-SamAccountName=jpaul	The attribute contents are not identical to the specified phrase; do not enclose the phrase in quotation marks for this operator

The following search syntax rules described above also apply to filter terms:

- Terms are case-insensitive.
- The term can be a single word, multiple words, or a phrase in quotation marks.
- In single-word terms, a trailing asterisk is treated as a wildcard character.
- In exact phrases, an asterisk is treated as a regular character.

**i** **NOTE:** Asterisk wildcards in an initial position are currently not supported for events provided by InTrust and Recovery Manager for Active Directory. This limitation does not apply to data provided by Change Auditor and Enterprise Reporter.

## Normalized Attributes

The following table shows what attributes are involved in searches that use the Who, What and Where labels. Active Directory attributes are **bolded**. Information about events is not included, because Who, What and Where are mapped directly to the same-name fields in InTrust and Change Auditor events.

Label → Context ↓	Who	What	Where
Users	<b>SAMAccountName</b> <b>DisplayName</b> <b>AccountSid</b> <b>DistinguishedName</b> <b>LogonName</b>	N/A	<b>DomainName</b>
Groups	User information User account information <b>ManagedByFullName</b> <b>ManagedByDisplayName</b>	N/A	<b>DomainName</b>
Computers	<b>ManagedByFullName</b> <b>ManagedByDisplayName</b>	N/A	<b>ComputerName</b> <b>NetBiosName</b>

Label → Context ↓	Who	What	Where
Shares	User information	N/A	<b>ComputerName</b>
Files	Permission information	Permission information	<b>ComputerName</b>

## Using Functions in Queries

Functions are a way to transform the results of a query to other objects inside a larger query. IT Security Search functions take a query as their single argument and return a collection of objects. Function names are case-insensitive.

## Group Membership Resolution Functions

Function	Details	Examples
Members	Returns the direct members of all groups that the argument query returned.	<code>Members ([Managed By]:"marty stu")</code>
Members_Deep	Returns both direct and indirect members of all groups that the argument query returned.	<code>Members_Deep (name="DL.IT")</code>
MemberOf	Returns all groups that directly contain the accounts returned by the argument query.	<code>MemberOf (FullName="DL.Accounting")</code>
MemberOf_Deep	Returns all groups that directly or indirectly contain the accounts returned by the argument query.	<code>MemberOf_Deep (Name="DL.Facilities")</code>

If the argument query returns objects that a function cannot be applied to, the function skips these objects. For example, the **Members** function doesn't do anything about user account objects.

### Example

Suppose you want to get events from all computers where user **martystu** is an administrator. Use the following query:

```
MemberOf_Deep (Who=martystu) AccountSID="S-1-5-32-544" | Where="{DomainName}"
Who=martystu
```

This query takes advantage of the well-known SID of the built-in **Administrators** group. First it finds all aliases of this user account, then it gets all local **Administrators** groups where those accounts are members, no matter whether direct or indirect (membership information is discovered by Enterprise Reporter). Then the query pipes the results through a sub-query to find all events by these users on computers where they are administrators. For details about search-in-search capabilities, see [Making Multi-Stage Searches](#).

# Permission Resolution Functions

These functions support a syntax extension that lets you fine-tune their behavior by specifying attributes. A function call with attributes looks like this:

```
[FunctionName:attribute1,attribute2,..., attributeN](<search query>)
```

For example, to list objects that are explicitly denied access to a specific file, use the **ObjectPermissions** function as follows:

```
[ObjectPermissions:deny,explicit]("c:\sensitive\off_limits.txt")
```

By default, it is assumed that you request data about all "allow" permissions.

Function	Supported Attributes	Details	Examples
ObjectPermissions	allow deny inherited explicit	Returns users and groups that have direct (explicitly assigned and inherited) permissions on the discovered file, folder or network share.	<ul style="list-style-type: none"> <li>Get a list of users and groups that are directly granted "allow" permissions on the specified file: ObjectPermissions ("c:\boring\interesting.txt")</li> <li>Get objects that are directly granted "allow" and "deny" permissions on the specified folder: [ObjectPermissions:allow,deny] ("c:\outrageous")</li> </ul>
ObjectPermissions_Effective	allow deny inherited explicit direct indirect	Returns users and groups that have direct (explicitly assigned and inherited) and indirect (obtained through group membership) permissions on the discovered file, folder or network share.	<ul style="list-style-type: none"> <li>Get a list of users and groups that have "allow" permissions on the specified network share: ObjectPermissions_Effective ("\\prodfiles1\Department Documents")</li> <li>Get a list of users and groups that have access to the specified network share due to group membership: [ObjectPermissions_Effective:indirect] ("\\prodfiles1\Department Documents")</li> </ul>
AccountPermissions	allow deny inherited explicit	Returns files, folders and network shares where the specified user or group is directly granted permissions.	<ul style="list-style-type: none"> <li>Get a list of all files, folders and network shares where users from the Toronto office have direct "allow" permissions: AccountPermissions (Office="Toronto")</li> </ul>

Function	Supported Attributes	Details	Examples
AccountPermissions_Effective	allow deny inherited explicit direct indirect	Returns files, folders and network shares where the specified user or group is directly or indirectly granted permissions.	<ul style="list-style-type: none"> <li>Get a list of all files, folders and network shares to which users from the specified group are denied access explicitly or through permission inheritance:  <pre>[AccountPermissions:deny] ( name=dl.rd.backend)</pre> </li> <li>Get a list of all files, folders and network shares where users reporting to the specified manager have "allow" permissions:  <pre>AccountPermissions_Effective (Manager="Marty Stu")</pre> </li> <li>Get a list of all files, folders and network shares where users reporting to the specified manager have indirect access due to group membership:  <pre>[AccountPermissions_ Effective:indirect] (Manager="Mary Sue")</pre> </li> </ul>

Calling the default parameter-free variants of these functions is equivalent to calling them with all supported parameters except **deny**. For example, the following two calls are synonymous:

```
ObjectPermissions_Effective(Where:server1)
[ObjectPermissions:allow,inherited,explicit,direct,indirect](Where:server1)
```

## Function Limitations

Functions have the following limitations:

- Multi-stage searches** cannot be function arguments. Incorrect: `Members(ManagedBy:"mary sue" | name="{FullName}")`
- Functions are not supported in operator scope queries described in [Who Can Do What in IT Security Search](#).
- AND-based conjunction of function calls is disallowed. Incorrect: `Members(name="group1") AND Members(name="group2")`
- Negation of function calls is disallowed. Incorrect: `-MemberOf(name="group3")`
- A function cannot have a function call as an argument.
- The functions work only on Enterprise Reporter data. For all other data, they return nothing.

## Making Multi-Stage Searches

You have the option to run a search on the results of another search. It is a way to automate your established search practices, and it may provide a clearer and more convenient representation of your intentions.

This is similar to how the output of a command is redirected into another command as its input in PowerShell and Unix shell languages. Accordingly, search result redirection is provided by the familiar pipe (|) operator.

To indicate a field whose value should be carried over from the left query to the right through the pipe, enclose the field name in curly braces, as in **{Where}** or **{EventID}**.

Example:

```
"rd.itsearch" | What:Logon AND Who:"{SAMAccountName}" | Name="{Where}"
```

In this three-stage search, the initial results are refined twice. First, it finds all users that are members of the **rd.itsearch** group. For these users, it finds such events that the users' SAM account names are in the **Who** field, and the **What** field contains "Logon". From the resulting events, pick only those that have any of the discovered computer names in the **Where** field.

## Auto-Resolution of the Current User

If you specify the **{Context.CurrentUser}** variable in your query, it is automatically resolved to information that identifies the user who is running the query. The following information is extracted (where available): account name in domain\user format, SAM account name, display name and SID.

For example, if user Alan Smithee supplies a query containing **Who="{Context.CurrentUser}"**, the resulting substituted information can be something like this:

```
Who=production\asmithee OR Who=ASmithee OR Who="Alan Smithee" OR Who="S-1-5-21-2591644-1571856274-80062049-1617"
```

If you want a particular identifying field instead of a set of fields, use the following accessors:

- {Context.CurrentUser.FullAccountName}
- {Context.CurrentUser.SamAccountName}
- {Context.CurrentUser.DisplayName}
- {Context.CurrentUser.AccountSid}

Examples:

- **Description:"Computer of {Context.CurrentUser.DisplayName}"** becomes **Description:"Computer of Alan Smithee"**
- **onpremisessecurityidentifier="{Context.CurrentUser.AccountSid}"** becomes **onpremisessecurityidentifier="S-1-5-21-2591644-1571856274-80062049-1617"**

**i** | **NOTE:** Resolution of this variable does not require that the Enterprise Reporter connector be enabled.

## Specifics of Recovery Manager for Active Directory Data

Recovery Manager for Active Directory provides data about users, groups, computers and organizational units, including those that have been deleted. Searching within that data should be approached in special ways.

One drawback is that full-text search does not work in Recovery Manager for Active Directory. Generally, it is recommended that you complement this data with results from Enterprise Reporter, if possible.

## Searching by Distinguished Name

In all attributes that contain distinguished names, such as **distinguishedName** or **manager**, only the "equals" operator is used, meaning that the value must match exactly. For example, if the **manager** attribute of a user is "CN=David Shore,OU=Employees,DC=it,DC=example,DC=corp", then the following happens:

- These queries match the user:  
Manager:"CN=David Shore,OU=Employees,DC=it,DC=example,DC=corp"  
Manager="CN=David Shore,OU=Employees,DC=it,DC=example,DC=corp"
- These queries do not match the user:  
Manager:"CN=David Shore"  
Manager="CN=David Shore"

## Searching for Deleted Objects

When Active Directory objects are deleted, they are really moved to the **Deleted Objects** container; some of their attributes are cleared and some are changed, including the name. These tips will help you compose queries that produce the expected results for deleted objects:

- The **name** attribute undergoes the following change: **<object\_name>** becomes **<object\_name>\0ADEL<object\_GUID>**. If you are aware of this pattern, you can look for deleted objects specifically.
- The **samAccountName** attribute remains unchanged in deleted users, computers and groups.
- In computers, the **dnsHostName** attribute also remains unchanged.

## Searching Without Specifying Fields

When you supply a search term without prefixing a field name, IT Security Search adds the field name for you, as follows:

Object Type	Field	Examples
User or group	aNR	<b>"Alan Smithee"</b> becomes <b>aNR:"Alan Smithee"</b> <b>"Alan Smithee*"</b> becomes <b>aNR:"Alan Smithee"</b> (wildcards are not supported by Recovery Manager for Active Directory)
Computer or OU	name	<b>primrose.domain.local</b> becomes <b>name:primrose.domain.local</b> <b>Directors*</b> becomes <b>name:Directors</b> (wildcards are not supported by Recovery Manager for Active Directory)

It is recommended that you specify the target fields explicitly and use the fields suggested in [Searching for Deleted Objects](#) above.

## Data Field Reference

The following topics provide details about fields that you can use in search queries, organized by supported system:

- [Enterprise Reporter Data Fields](#)
- [InTrust Data Fields](#)
- [Change Auditor for Active Directory Data Fields](#)
- [Active Roles Data Fields](#)
- [Recovery Manager for Active Directory Data Fields](#)

## Enterprise Reporter Data Fields

The following are lists of fields that occur in Enterprise Reporter data, organized by type of returned object.

**i** **NOTE:** The **In UI** column indicates if the field is available in the IT Security Search web UI as a clickable element. Whether or not you can click it in the UI, you can type any of these fields in your search queries.

### Computers

Field Name	In UI	Example Value	Details
AccountFullName	No	MAIN\HOUDEVW04\$	SAMAccountDomain\SAMAccountName of the relevant computer account
AccountSid	No	S-1-5-21-636461855-2365528612-2953867313-5163	Security identifier (SID) of the computer account
ComputerName	Yes	achtung.main.mycompany.corp	Short or NetBIOS name for the computer
Description	Yes	Serial , AOPEN_, AWRDACPI, 1002MHz, 1002MHz, 3072MB RAM	Description for the computer
DistinguishedName	No	CN=HOUITW09, OU=Houston, OU=AMER, OU=Production Computers, DC=main, DC=mycompany, DC=corp	Distinguished name for domain computer
Domain	Yes		Same as DomainName
DomainName	No	main.mycompany.corp	Fully qualified domain name
Groups	No	Pre-Windows 2000 Compatible Access;Cert Publishers	List of groups (in common name format) where the computer account is a member explicitly
HasGroups	No	True	True if this computer account is a member of any group
IsHidden	No	False	True if the server is visible to other computers in the same network; otherwise, false

Field Name	In UI	Example Value	Details
Location	Yes	US/Houston	Location of domain computer
ManagedByDisplayName	No	Patricia Lum	The display name of account by which the domain computer is managed
ManagedByType	No	Users	Type of account by which the domain computer is managed; Users or Groups
Name	Yes	achtung	NetBIOS name of the computer
NetBiosName	No	IRVWEBW05	NetBIOS name for domain computer
NumLogons	No	291	Number of times the domain computer was logged into
OSName	No	Windows Server 2003	Full name of the computer's operating system
OSServicePack	No	Service Pack 1	Service pack name for the computer's operating system
OSVersion	No	5.2 (3790)	Operating system version number for the computer
OU_CanonicalName	No	main.mycompany.corp/Production Computers/US/Houston/R&D Test Computers	Canonical name for organizational unit
OU_DistinguishedName	No	OU=Cary, OU=AMER, OU=Production Computers, DC=main, DC=mycompany, DC=corp	Distinguished name for organizational unit
RelatedOU	No		Same as OU_CanonicalName
Scope	Yes	Active Directory	Active Directory or Workgroup
Source	Yes	Enterprise Reporter	Enterprise Reporter (data source)
State	Yes	Current	Current or Deleted
Where	No		Same as ComputerName, NetBiosName
Who	No		Same as ManagedByFullName, ManagedByDisplayName

## Files

Field Name	In UI	Example Value	Details
Computer	Yes		Same as ComputerName

Field Name	In UI	Example Value	Details
ComputerName	No	WST9240.main.mycompany.corp	Short or NetBIOS name for the computer
DomainName	Yes	MAIN	NetBIOS name for domain
Extension	Yes	.exe	Extension of the file
File	Yes	TestConsol.exe	File or folder name
FullAccountName	Yes	WST9240\Administrators	SAMAccountDomain\SAMAccountName of owner account
OU_CanonicalName	Yes	main.mycompany.corp/Production Computers/US/Houston/R&D Test Computers	Canonical name for organizational unit (for domain users only)
Owner	Yes		Same as FullAccountName, OwnerSid
Owner Domain	No		Same as SAMOwnerDomain
OwnerSid	No	S-1-5-32-544	Security identifier (SID) of the owner account
OwnerType	No	Groups	Owner account type: Users or Groups
Path	Yes	D:\Images\59491\	Full path of the folder or file; based on the collection options, the value could be in the format c:\folder or \\computer\shared\Folder
Permission	No		Same as PermissionsText
PermissionsText	No	WST9240\Remote Desktop Users: Allow List folder/read data, Create files/Write data, Create folders/append data, Read extended attributes, Write extended attributes, Traverse folder/run file, Read attributes, Write attributes, Read permissions Inherit	Semicolon-delimited list of <i>permission/Account: access_type</i> [Allow Deny] <i>inheritance</i> [Inherited Explicit]
RelatedOU	No		Same as OU_CanonicalName
SAMOwnerDomain	No	WST9240	SAM account name of owner account's domain
SAMOwnerName	No	Administrators	SAM account name of owner account
Size	Yes	31335914	Size in bytes of the NTFS object
Source	Yes	Enterprise Reporter	Enterprise Reporter (data source)
Type	Yes	File	File or Folder; Folder if the NTFS object is a folder; otherwise, File
What	No		Same as PermissionsText

Field Name	In UI	Example Value	Details
Where	No		Same as ComputerName
Who	No		Same as PermissionsText

## Groups

Field Name	In UI	Example Value	Details
AccountSid	No	S-1-5-21-636461855-2365528612-2953867313-107634	Security identifier (SID) of the account
AdminDisplayName	No	Administrator	Admin display name for the domain group; name is displayed on admin screens
CanonicalName	No	main.mycompany.corp/Groups/RD/MCDL.RD.CRDHub.APAC.AU	The name of the domain group in canonical format
CommonName	No	Development Users	Common name for domain group
Description	Yes	Owner: CLIVE_HERRY	Description of the group
DisplayName	No	AA_Accounting	Display or common name for the group
DistinguishedName	No	CN=MCDL.RD.CRDHub.APAC.AU,OU=RD,OU=Groups,DC=main,DC=mycompany,DC=corp	Distinguished name for domain group or SAM account name for a local user (computer/username)
Domain	Yes		Same as DomainName
DomainName	Yes	main.mycompany.corp	Fully qualified domain name for domain accounts or computer's NetBios Name for local
E-mail	Yes		Same as EmailAddress
EmailAddress	No	BC5796F842DD49CD8F4@sales.mycompany.com	Email address for the group
Friendly Name	Yes		Same as FriendlyName
FriendlyName	No	AA_Accounting (MAIN\FB430EAC2D2E4)	Friendly name for the group
FullAccountName	No	MAIN\Office.AMER.US.Boston	domain\group; group is a SAM account name, domain is the SAM account name of a domain or NetBIOS name of a computer
FullName	No	Development Users	Full name for domain group
Groups	No	MCDL.PreSales.NAC.DatabasePerf; MCDL.Sales.DBPerformance.SR.NA	Common or SAM account names of groups (semicolon-separated) that are explicitly

Field Name	In UI	Example Value	Details
			members
GroupScope	Yes	Universal	One of the following: <ul style="list-style-type: none"> <li>• Builtin local</li> <li>• Global</li> <li>• Domain local</li> <li>• Local</li> <li>• Universal</li> <li>• SQL Login</li> <li>• Well Known</li> <li>• Unknown</li> </ul>
GroupType	Yes		Same as IsSecurityEnabled
HasGroups	No	False	True if this group has members of type "group"
HasUsers	No	True	True if this group has members of type "user"
HomePage	No	http://homepage	Primary home page for domain group
Info	No	Created as part of the ChangeBase Mail migration by Charles Arrot	Informational notes on the domain group
IsSecurityEnabled	No	Security	Security or Distribution
Managed By	No		Same as ManagedByDisplayName, ManagedByFullName
ManagedByDisplayName	No	Owen Range	Display name or Common name of account by which the domain group is managed
ManagedByFullName	No	CN=Sarah Quash,OU=Employees,DC=main,DC=mycompany,DC=corp	Account (distinguished name) by which the domain group is managed
ManagedByType	No	Users	Type of account by which the domain group is managed; Users or Groups
Name	Yes		Same as DisplayName
Nested Groups	No		Same as Groups
Organizational Unit	Yes		Same as OU_CanonicalName
OU_CanonicalName	No	main.mycompany.corp/Groups/Sales	Canonical name for organizational unit
OU_DistinguishedName	No	OU=Sales,OU=Groups,DC=main,DC=mycompany,DC=corp	Distinguished name for organizational unit

Field Name	In UI	Example Value	Details
RelatedOU	No		Same as OU_CanonicalName
SAMAccountDomain	No	MAIN	SAM account name for the account's domain for domain's groups or NetBIOS name of the computer for computer's groups
SAMAccountName	No	MCDL.RD.CRDHub.APAC.AU	SAM account name for the account
SIDHistory	No	S-1-5-21-329068152-688789844-839522115-10863	List of previous security identifiers (SID) used if the domain group was moved from other domains
Source	Yes	Enterprise Reporter	Enterprise Reporter (data source)
State	Yes	Current	Current or Deleted
Url	No	http://group	URL addresses of websites for the domain group
Users	No	Zoe Ucchini;Peter Omelo	Common or SAM account names of users (semicolon-separated) that are explicitly members
Where	No		Same as DomainName
Who	No		Same as Users, UsersAccounts, ManagedByFullName, ManagedByDisplayName

## OUs

Field Name	In UI	Example Value	Details
AppliesTo	No		Same as PermissionsText
CanonicalName	Yes	main.mycompany.corp/Builtin	Canonical name for organizational unit
ContainerType	No	Container	Type of container: Container or Organizational Unit
Description	Yes	Default container for upgraded computer accounts	
DistinguishedName	No	Description for organizational unit	Distinguished name for organizational unit
Domain	Yes		Same as DomainName
DomainName	No	main.mycompany.corp	Fully qualified domain name
HasPermissions	No	True	True or False; True if PermissionsText is not empty
Managed By	Yes		Same as ManagedByFullName, ManagedByDisplayName

Field Name	In UI	Example Value	Details
ManagedByDisplayName	No	MCDL.RD.ITSearch	Display or common name of management account
ManagedByFullName	No	CN=MCDL.RD.ITSearch,OU=RD,OU=Groups,DC=main,DC=mycompany,DC=corp	The account (distinguished name) by which the organizational unit is managed
ManagedByType	No	Groups	Management account type; Users or Groups
Name	Yes	Computers	Common short name for organizational unit
NumberOfComputers	No	4	Number of domain computers in organizational unit
NumberOfContacts	No	5	Number of contacts in organizational unit
NumberOfGroups	No	3	Number of domain groups in organizational unit
NumberOfOtherObjects	No	6	Number of other domain objects in organizational unit
NumberOfUsers	No	2	
Permission	No		Same as PermissionsText
PermissionsText	No	NT AUTHORITY\SELF: Allow Read Property, Write Property for location [Descendant computer objects] Inherited;NT AUTHORITY\SELF: Allow Read Property, Write Property for defender-tokenData [Descendant defender-tokenLicenseClass objects] Inherited	Semicolon-separated list of <i>permission/ account: access_type</i> [Allow Deny] <i>inheritance</i> [Inherited Explicit]
RelatedOU	No		Same as CanonicalName
Source	Yes	Enterprise Reporter	Enterprise Reporter (data source)
State	Yes	Current	Current or Deleted
What	No		Same as PermissionsText
Where	No		Same as DomainName
Who	No		Same as ManagedByFullName,PermissionsText

## Shares

Field Name	In UI	Example Value	Details
Comment	Yes	Docs share	Comment for the share
Computer	Yes		Same as ComputerName
ComputerName	No	WST9240.main.mycompany.corp	NetBIOS name of the computer

Field Name	In UI	Example Value	Details
FullOwnerName	No	WST9240\Administrators	SAMAccountDomain\SAMAccountName of owner account
Local Path	Yes		Same as SharePath
Name	Yes		Same as ShareName
Owner	Yes		Same as FullOwnerName
OwnerDomain	No	WST9240	SAM account name of owner account's domain
OwnerName	No	Administrators	SAM account name of owner account
OwnerType	No	Groups	Owner account type; Users or Groups
PermissionsText	No	WST9240\Remote Desktop Users: Allow List folder/read data, Create files/Write data, Create folders/append data, Read extended attributes, Write extended attributes, Traverse folder/run file, Read attributes, Write attributes, Read permissions Inherit	Semicolon-delimited list of permission/Account: access type [Allow Deny] Inheritance[Inherited Explicit]
RelatedOU	No	main.mycompany.corp/Production Computers/US/Houston/R&D Test Computers	Canonical name for organizational unit (for domain users only)
ShareName	No	C\$	Name of the share
SharePath	No	D:\Custom Utilites	Local path of share
ShareType	No	Administrative Shared Folder	Type of resource being shared
Source	Yes	Enterprise Reporter	Enterprise Reporter (data source)
What	No		Same as PermissionsText
Where	No		Same as ComputerName
Who	No		Same as PermissionsText

## Users

Field Name	In UI	Example Value	Details
Account SID	Yes		Same as AccountSid
AccountIsDisabled	No	True	True if domain(computer) user account is disabled; otherwise, False
AccountIsLocked	No	False	True if domain(local) user account is locked; otherwise, False
AccountSid	No	S-1-5-21-636461855-	Security identifier (SID) of the account

Field Name	In UI	Example Value	Details
		2365528612- 2953867313-71684	
Assistant	No	CN=Pamela Ear, OU=Employees, DC=main, DC=mycompany, DC=corp	The distinguished name of the domain user's administrative assistant
CannotChangePassword	Yes	False	True if the local user cannot change the password; otherwise, false
City	No	Shanghai	City of domain user account
Company	Yes	My Company Inc.	Company of the user account
Country	Yes	Canada	Country or region of the user account
Department	Yes	R&D - Development	Name of the user's department
Description	No	Build account for Archive Manager Offline Client	Description of the user
DirectReports	No	CN=Philip Arsley, OU=Employees, DC=main, DC=mycompany, DC=corp; CN=Gwen Arlic, OU=Employees, DC=main, DC=mycompany, DC=corp; CN=Greg Inger, OU=Employees, DC=main, DC=mycompany, DC=corp	List of domain users that directly report to the domain user
DisplayName	No	Caroline Abbage	Display name or SAMAccount name for the user
DistinguishedName	No	CN=Caroline Abbage, OU=Employees, DC=main, DC=mycompany, DC=corp	Distinguished name for domain user or computer\user for local users
Division	No	Reporting division	Division for domain user
Domain	Yes	main.mycompany.corp	Fully qualified domain name for domain's

Field Name	In UI	Example Value	Details
			users or NetBIOS name of the computer for computer's users
E-mail	Yes		Same as EmailAddress
EmailAddress	No	Patricia.Lum@support.mycompany.com	Email address for the user
EmployeeID	No	69267	Employee ID for domain user
FaxNumber	No	0123456789	Facsimile number for domain user
FirstName	No	Paul	Given name (first name) of domain user
FullAccountName	No	MAIN\jcdenton	domain\user; user is a SAM account name, domain is the SAM account name of a domain or NetBIOS name of a computer
Groups	No	WST8766VM1\Administrators; Office.US.Houston	List of groups. CommonName or Computer\groupName (explicit membership)
HasDirectReports	No	True	True or False; True if DirectReports is not empty
HasGroups	No	True	True if this user is member of any group
HasPhoto	No	True	True if this user has a photo
HomeDirSize	No	0	Size of the home directory for the domain user
HomePhoneNumber	No	+7-123-4567890	Phone number for the domain user
HomePostalAddress	No	Main street	Mailing address for the domain user
Info	No	Account used for Patchlink & Symantec scanning of domain systems	Informational notes on the domain user
Initials	No	M	Initials for the domain user
IpPhone	No	+44 1234 567890 x12345	IP telephone number or address for the domain user
LastName	No	Epper	Last name of domain user
LogonHours	No	FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF	Hex-coded hours that the domain/local user is allowed to log on to the domain
Logon Name	No		Same as LogonName
LogonName	No	SVC-Scanner@main.mycompany.corp	Logon name for the domain user

Field Name	In UI	Example Value	Details
ManagedBy	No	CN=Christina Hilli, OU=Employees, DC=main, DC=mycompany, DC=corp	The account (distinguished name) by which the domain user is managed
Manager	Yes		Same as ManagedBy,ManagedByDisplayName
MiddleName	No	N	Middle name for the domain user
Mobile	Yes	+7-123-4567890	Mobile number for the user
Name	Yes		Same as DisplayName
NumLogons	No	3910	Number of times the domain/local user has successfully logged on
Office	Yes	Castlegar	Office location for the user
Organizational Unit	Yes		Same as OU_CanonicalName
OtherIpPhone	No	Conference 84030	List of alternate TCP/IP addresses for the phone for the domain user (Telephony)
OtherMailbox	No	other_mailbox@hotmail.com	Additional email addresses for the domain user
OtherMobile	No	+55 11 12345 6789	List of alternate mobile phone numbers for the domain user
OtherTelephone	No	+1 123 456 7890	List of alternate telephone numbers for the domain user
OU_CanonicalName	No	main.mycompany.corp/IS/SVC-Accounts/MailboxEnabled	Canonical name for organizational unit (for domain users only)
OU_DistinguishedName	No	OU=Enabled SVC-Accounts, OU=SVC-Accounts, OU=IS, DC=main, DC=mycompany, DC=corp	Distinguished name for organizational unit (for domain users only)
PasswordIsExpired	No	True	True if domain user's password is expired; otherwise, false
PasswordNeverExpires	No	True	True if the domain/local user's password never expires; otherwise, false
PersonalTitle	No	Mr.	Personal title for the domain user

Field Name	In UI	Example Value	Details
PostalCode	No	411016	Postal or zip code for the domain user
RelatedOU	No		Same as OU_CanonicalName
SAM Account Domain	Yes		Same as SAMAccountDomain
SAM Account Name	Yes		Same as SAMAccountName
SAMAccountDomain	No	MAIN	SAM account name for the account's domain for domain's users or NetBIOS name of the computer for computer's users
SAMAccountName	No	jcdenton	SAM account name for the account
Scope	Yes	Active Directory	Active Directory or Computer
Source	Yes	Enterprise Reporter	Enterprise Reporter (data source)
State	Yes	Current	Current or Deleted
StateOrProvince	No	AZ	State or province for the domain user
StreetAddress	No	1042 Bluesky Blvd., Bldg. 1 Flagstaff AZ	Street address for the domain user
TelephoneNumber	No	+1 123 456 7890 x45678	Telephone number for the domain user
Title	Yes	Software Developer 3	Title for the user
UserPrivilegeLevel	No	Normal	Flag for user privilege level: Normal or Unknown
UserWorkstations	No	ALVMISW02,ALVSANW01,ALVPATW01,ALVPATW02	NetBIOS or DNS names of the computers running Windows?NT Workstation or Windows?2000 Professional to which the domain user can log on
Where	No		Same as DomainName
Who	No		Same as SAMAccountName, DisplayName, AccountSid, DistinguishedName

## Other Object Types

In addition to the object types listed above, Enterprise Reporter can provide field data for various other objects. To see the kinds of objects available in your environment, click the **More** tab in the search result grid. For a list of supported fields of a particular object type, see the details of such an object.

## InTrust Data Fields

The following are lists of fields that occur in InTrust events, organized by type of returned object.

**i** | **NOTE:** The **In UI** column indicates if the field is available in the IT Security Search web UI as a clickable element. Whether or not you can click it in the UI, you can type any of these fields in your search queries.

Field Name	In UI	Example Value	Details
Category	No	Sensitive Privilege Use	Event category
Computer	No	Y1202.seldom.mycompany	Computer where the event occurred
ComputerType	No	69635	Mask for computer type
DataSourceType	No	{A9E5C7A2-5C01-41B7-9D36-E562DFDDEFA9}	GUID of InTrust data source type
Description	No	An operation was attempted on a privileged object.	Event description
Environment	No	9E442BEE-EAC2-4D79-9013-053FB225CFD0	Environment GUID
EventID	No	4674	Event ID
Type	No	16	Event Type ID numeric
SourceComputer	No	Y1202	Name of gathering computer
SourceDomain	No	SELDOM	Name of gathering computer's domain
Log	No	Security	Log name
PlatformID	No	500	Platform ID (500 means Windows)
Source	No	Security	Event source
UserDomain	No	WST9983	Domain of the user that initiated this event
UserName	No	Administrator	Name of the user that initiated this event
VersionMajor	No	6	OS version major
VersionMinor	No	2	OS version minor
InsertionString*	Yes	NT AUTHORITY	InsertionString1, InsertionString2 etc.
Workstation	No	WST9983	Computer where the operation was initiated
Where_From	No	WST9983	Same as Workstation
WhoDomain	No	SALES	Same as UserDomain
Who	No	Administrator	Same as UserName
Object_DN	No	CN=HealthMailbox, CN=Users, DC=seldom,	DN of the object that was changed/deleted/created

Field Name	In UI	Example Value	Details
		DC=mycompany	
Object_ID	Yes	DE442BEE-EAC2-4D79-9013-053FB225CFD0	ID of the object that was changed/deleted/created
WhomId	No	CN=Admin, CN=Users, DC=seldom, DC=spb, DC=qsft	Object_DN of the object that was changed/deleted/created, if available; otherwise Object_ID of the object
Whom_ObjectClass	No	user	Class of the object that was changed/deleted /created
ComputerName	No	COMP1	Same as Computer
What	No	NTLM Authentication	Event literal
Log name	No	Security	Same as Log
SourceName	No	Security	Same as Source
RelatedOU	No	sales.mycompany.corp/Production Computers	By Enterprise Reporter: OU associated with the computer
Whom_ObjectClass	No	user	By Enterprise Reporter: Object class of Whom

## Change Auditor for Active Directory Data Fields

The following are lists of fields that occur in Change Auditor for Active Directory events, organized by type of returned object. All of these fields are available in the IT Security Search web UI as clickable elements. You can also type any of these fields in your search queries.

Field Name	Example Value	Details
AAD_City	"Halifax", "New York City"	Azure sign-in city
AAD_Country	"Canada", "US"	Azure sign-in country
AAD_ActivityStatusReason	User successfully reset password	Reason for activity status
AAD_OnPremisesTarget	RHSOFTWARE\AD_Admin	Azure AD on premises target name
AAD_OnPremisesUserName	RHSOFTWARE\AD_Admin	Azure AD on premises user name
AAD_State	"Nova Scotia", "New York"	Azure sign-in state
AAD_TargetDisplayName	AD_Admin@RHSoftware.Net	Azure AD Target object display name
AAD_	QAMyProduct.onmicrosoft.com	Azure AD tenant default domain name

Field Name	Example Value	Details
TenantDefaultDomain		
AAD_TenantDisplayName	QA QAMyProduct.onmicrosoft.com My Product	Azure AD tenant display name
ActionName	Modify Attribute	Name of action
Activity Details	User successfully reset password	Same as AAD_ActivityStatusReason
After	E:\NewName.txt	Same as ValueNew
Azure - Activity Name	Set Company Information	Same as O365_Operation
Before	E:\OldName.txt	Same as ValueOld
Description	User AD Admin in the directory had their password reset	Event's description
DomainName	PROD	Domain where operation was performed
FacilityName	Local User Monitoring	Name of Facility
LDAP - Attributes	canonicalName, co, company, department, displayName	Attributes that were queried
LDAP - Elapsed	8094	How long the AD query took to run, in milliseconds; zero (0) indicates that it took less than a millisecond to complete
LDAP - Filter	(&(objectClass=user)(!(objectClass=computer)))	Filter string used in the AD query
LDAP - Occurrences	1	Number of times the AD query occurred during the specified interval
LDAP - Results	52	Number of results returned for the query
LDAP - Scope	This object and all children	Scope of coverage: (This object only, This object and all children)
LDAP - Since	2018-01-15T09:42:01.3672010Z	Date and time when the AD query was first initiated
Log	ChangeAuditor	Name of event log
Log name	ChangeAuditor	Same as Log
O365_Operation	Set Company Information	Office 365 operation
O365_SiteUrl	https://qa.sharepoint.com/sites/Certification/	URL of Office 365 site
Office 365 Site URL	https://qa.sharepoint.com/sites/Certification/	Same as O365_SiteUrl
On premises target	RHSOFTWARE\AD_Admin	Same as AAD_OnPremisesTarget
On premises user name	RHSOFTWARE\AD_Admin	Same as AAD_OnPremisesUserName

Field Name	Example Value	Details
RelatedOU	RHSoftware.Net/AzureAD Accounts	Same as RelatedOUWhom
RelatedOUWhere	OU=Domain Controllers,DC=RHSoftware,DC=Net	Ou where operation was performed
RelatedOUWhom	RHSoftware.Net/AzureAD Accounts	OU of target object
Result	None	Operation result
SiteName	EMEA-SPB	Site where operation was performed
Target display name	AD_Admin@RHSoftware.Net	Same as AAD_TargetDisplayName
Tenant	QAMyProduct.onmicrosoft.com	Same as AAD_TenantDisplayName
Tenant initial domain	QAMyProduct.onmicrosoft.com	Same as AAD_TenantDefaultDomain
UserName	SPB9983\Administrator	Event initiator
ValueNew	E:\NewName.txt	new value of changed attribute
ValueOld	E:\OldName.txt	old value of changed attribute
What	Local user logged on	Event class name
When	2016-11-12T06:00:00.0460000Z	When the operation was performed
Where	wst9983	Where the operation was performed
Where_From	wst9943.sales.mycompany.com	Same as Workstation
Who	Administrator	Display name or name of initiator
Whold	S-1-5-21-1763487455-1171009733- 2095814533-500	SID of initiator
Whom	WST9983\TestUser	Target object of operation
Whom_ObjectClass	Users	Target object's class
Workstation	wst9983.sales.mycompany.com	Workstationn from that operation was initiated

## Active Roles Data Fields

The following are lists of fields that occur in Active Roles data, organized by type of returned object. All of these fields are available in the IT Security Search web UI as clickable elements. You can also type any of these fields in your search queries.

**i** **NOTE:** The **In UI** column indicates if the field is available in the IT Security Search web UI as a clickable element. Whether or not you can click it in the UI, you can type any of these fields in your search queries. For events, all fields are displayed.

# Events

Field Name	Example Value	Details
AR_ClientComputerName	ITSEARCHTEST3	Host with Active Roles client software
AR_ClientVersion_Build	2	Version build number of Active Roles client software
AR_ClientVersion_Major	7	Version major number of Active Roles client software
AR_ClientVersion_Minor	1	Version minor number of Active Roles client software
AR_ClientVersion_Revision	3406	Revision of Active Roles client software
AR_Server	arsit	Active Roles Server host
Attribute_*	New description1	New value of attribute
ChangedAttributes	description,streetAddress	List of attributes
Completed	2017-05-04T07:18:57.9741631Z	Timestamp of operation when that was completed
Control_OperationReason	Reason for modification	Reason of operation
Description	Modified attributes: groupType: -2147483646 objectClass: group sAMAccountName: ArsTestTemporalGroupSam_CB79 objectSid: AQUAAAAAAAAUVAAAA+mvC8lvUdNjWHCAbGGkBAA==	Description of event
ID	1-107540	ID of operation
Initiated	2017-05-04T07:18:57.9116595Z	Timestamp of operation when that was initiated
Initiator_DN	CN=Zakhar Shkonda, OU=zs, OU=TestUsers, DC=it, DC=sales, DC=mycompany	DN of initiator
Initiator_Guid	b58c2906-ad0b-4682- bab3-0ae56503eeb5	GUID of initiator
Initiator_Host	ARSIT.it.sales.mycompany	Host of Initiator
Initiator_IsDSAdmin	True	True if initiator is DS administrator

Field Name	Example Value	Details
Initiator_NTAccountName	IT\zs	NT Account name of initiator
Initiator_ObjectClass	user	Class of initiator
Initiator_Sid	S-1-5-21-4039273466-3631535243-455089366-91270	SID of initiator
Initiator_Site	Default-First-Site-Name	Site of initiator
Log	Active Roles	Log name
Logon_Site	Default-First-Site-Name	Same as Initiator_Site
Operation_GUID	9b3c5524-065d-418a-9511-3043ab1a5bd7	GUID of operation
Operation_Type	Delete	Type of operation
Operation_TypeID	1	Type ID of operation
Reason	Reason for modification	Same as Control_OperationReason
RelatedOU	it.sales.mycompany/AutotestOU/ARS/FIT2711055222_0E7C	Same as TargetObject_OUCanonical
Result	Completed	Same as Status
Status	Completed	Operation status
StatusID	1	Operation status ID
TargetObject_DN	CN=ArsCHUser1_0E7C, OU=FIT2711055222_0E7C, OU=ARS, OU=AutotestOU, DC=it, DC=sales, DC=mycompany	DN of target object
TargetObject_Guid	b6a8b5d0-e003-4421-a7a4-e6fc11f3075a	GUID of target object
TargetObject_NTAccountName	IT\ArsCHUser1_0E7C	NT Account name of target object
TargetObject_ObjectClass	user	Class of target object
TargetObject_OUCanonical	it.mycompany.com/AutotestOU/ARS/FIT2711055222_0E7C	Canonical name of object's OU
TargetObject_Sid	S-1-5-21-4039273466-3631535243-455089366-91270	SID of target object

Field Name	Example Value	Details
TargetObject_SimpleName	ArsCHUser1_0E7C	Name of target object
What	Delete	Same as Operation_Type
When	2017-05-10T08:38:58.000000Z	Same as Completed
Where	dc2.it.sales.mycompany	Host where this operation was performed
Who	IT\zs	Same as Initiator_NTAccountName
Who_DN	CN=Caroline Abbage, OU=mgmt, OU=TestUsers, DC=it, DC=sales, DC=mycompany	Same as Initiator_DN
Who_Guid	b58c2906-ad0b-4682- bab3-0ae56503eeb5	Same as Initiator_Guid
Who_IsDSAdmin	True	Initiator_IsDSAdmin
Who_ObjectClass	user	Same as Initiator_ObjectClass
Who_Sid	S-1-5-21-4039273466- 3631535243-455089366-1131	Same as Initiator_Sid
Whold	S-1-5-21-4039273466- 3631535243-455089366-1131	Same as Initiator_Sid
Whom	ArsTestDynamicGroup_CB79	Same as TargetObject_SimpleName
Whom_DN	CN=ArsTestTemporalGroup_CB79, OU=FIT1010370592_CB79, OU=ARS, OU=AutotestOU, DC=it, DC=sales, DC=mycompany	Same as TargetObject_DN
Whom_Guid	eff86e4b-7800-44ce- af3c-ecf198ccadd5	Same as TargetObject_Guid
Whom_NTAccountName	IT\ArsCHUser1_0E7C	Same as TargetObject_NTAccountName
Whom_ObjectClass	Groups	Same as TargetObject_ObjectClass
Whom_Sid	S-1-5-21-4039273466- 3631535243-455089366-92446	Same as TargetObject_Sid
WhomId	CN=ArsTestDynamicGroup_CB79,	Same as TargetObject_DN

Field Name	Example Value	Details
	CN=ArsTestContainer2_C829, OU=FIT1012125742_C829, OU=ARS, OU=AutotestOU, DC=it, DC=sales, DC=mycompany	
WhomSimple	ArsTestDynamicGroup_CB79	Same as TargetObject_SimpleName
Workstation	ARSIT.it.sales.mycompany	Same as Initiator_Host

## Computers

Field Name	In UI	Example Value	Details
AccountSid	Yes	S-1-5-21-4039273466- 3631535243-455089366- 89812	Computer account SID
Description	Yes	Storage Server	Description of computer
DistinguishedName	No	CD=DC1, CN=Domain Controllers, DC=it, DC=sales, DC=mycompany	Computer account distinguished name; search by full value only
DNSHostName	Yes	DC1.it.sales.mycompany	DNS host name
Location	Yes	Houston	Location of computer
ManagedBy	No	CN=Caroline Abbage, OU=Employees, DC=it, DC=sales, DC=mycompany	Same as ManagedByFullName
ManagedByFullName	No	CN=Caroline Abbage, OU=Employees, DC=it, DC=sales, DC=mycompany	Distinguished name of manager of the computer account; search by full value only
Name	Yes	DC1	Same as NetBiosName
NetBiosName	Yes	DC1	NetBIOS name of computer
NumLogons	Yes	12656	Logon count

Field Name	In UI	Example Value	Details
ObjectCategory	Yes	computer	Object class = computer
ObjectGUID	No	ddd94ab4-5de6-4696-a93c-433cf9827c28	Object GUID of computer account
OSName	Yes	Windows Server 2008 R2 Enterprise	OS name
OSServicePack	Yes	Service Pack 1	OS service pack
OSVersion	Yes	6.1 (7601)	OS version
Where	Yes	DC1	Same as NetBiosName
Who	Yes	CN=Caroline Abbage, OU=Employees, DC=it, DC=sales, DC=mycompany	Same as ManagedByFullName

## Groups

Field Name	In UI	Example Value	Details
CN	Yes	Users	Common name of group
Description	Yes	Houston internal group for notification	Description of group
DisplayName	Yes	Users	Display name of group
DistinguishedName	No	CN=MCDL.RD.Notification, OU=RD, OU=Groups, DC=it, DC=sales, DC=mycompany	Distinguished name of group;. search by full value only
Email	Yes	MCDL.RD.Notification@it.sales.mycompany	Email address of group
GroupType	No	-2147483640	Integer value of bitmask that contains information about group type and scope; search by full value only (more details at <a href="https://msdn.microsoft.com/en-us/library/ms675935.aspx">https://msdn.microsoft.com/en-us/library/ms675935.aspx</a> )
HomePage	Yes	http://homepage	Home page of group
Info	Yes	Some info	Additional information about group
ManagedBy	No	CN=Caroline Abbage,	Same as ManagedByFullName

Field Name	In UI	Example Value	Details
		OU=Employees, DC=it, DC=sales, DC=mycompany	
ManagedByFullName	Yes	CN=Caroline Abbage, OU=Employees, DC=it, DC=sales, DC=mycompany	Distinguished name of manager of the group; search by full value only
Name	Yes	Users	Name of group
ObjectCategory	Yes	group	Object class = group
ObjectGUID	No	80b090a2-968f-42e6- bc76-6e2505f43759	GUID of group object
SAMAccountName	Yes	Users	SAMAccount name of group
Url	Yes	http://groupname	URL of group
Who	Yes	CN=Caroline Abbage, OU=Employees, DC=it, DC=sales, DC=mycompany	Same as ManagedByFullName

## OUs

Field Name	In UI	Example Value	Details
Description	Yes	Default container for Defender objects	Description of OU
DistinguishedName	No	OU=BestEmployees, DC=it, DC=sales, DC=mycompany	Distinguished name of group; search by full value only
ManagedBy	No	CN=Clive Herry, OU=mgmt, OU=TestUsers, DC=it, DC=sales,	Same as ManagedByFullName

Field Name	In UI	Example Value	Details
		DC=mycompany	
ManagedByFullName	Yes	CN=Clive Herry, OU=mgmt, OU=TestUsers, DC=it, DC=sales, DC=mycompany	Distinguished name of manager of the OU; search by full value only
Name	Yes	Users	Name of OU
ObjectCategory	Yes	organizationalUnit	Object class = organizationalUnit or container
ObjectGUID	No	675205fb-4d29-44b6-9284-69e867689f38	GUID of OU
USNChanged	No	9296605	USN-Changed attribute of OU; search by full value only

## Users

Field Name	In UI	Example Value	Details
AccountSid	No	S-1-5-21-4039273466-3631535243-455089366-26350	User SID; search by full value only
Company	Yes	MyCompany	Company name
Country	Yes	United States	Country name
Department	Yes	Sales	Department name
DisplayName	No	Caroline Abbage	User display name
DistinguishedName	No	CN=Caroline Abbage, OU=Employees, DC=it, DC=sales, DC=mycompany	User distinguished name; search by full value only
EmailAddress	Yes	Caroline.Abbage@sales.mycompany.com	Email address
HomePhoneNumber	Yes	+1 410 531 0638	Home telephone number
Logon Name	Yes		Same as LogonName
LogonName	No	SVC-Scanner@main.mycompany.corp	Logon name for the domain user
ManagedBy	No	CN=Caroline Abbage,	Same as ManagedByFullName

Field Name	In UI	Example Value	Details
		OU=Employees, DC=it, DC=sales, DC=mycompany	
ManagedByFullName	No	CN=Caroline Abbage, OU=Employees, DC=it, DC=sales, DC=mycompany	Distinguished name of manager of user; search by full value only
Mobile	Yes	+ 911 9 769 8889	Mobile phone number
Name	Yes	Caroline Abbage	User name
ObjectCategory	Yes	user	Object class = user
ObjectGUID	No	861205fb-4d29-44b6-9284-69e867689f38	User object GUID; search by full value only
Office	Yes	Ludlow st. 80, suite 200	Physical delivery office name
SAMAccountName	Yes	jc Denton	SAMAccountName of user
StreetAddress	Yes	Ludlow st. 80	Street address
TelephoneNumber	Yes	+ 123 4 567 8900	Telephone number
Title	Yes	Mgr, Sales	User job title
USNChanged	No	9296605	USN-Changed attribute of user; search by full value only
Who	No	Administrator	Search in the following attributes: SAMAccountName, DisplayName, AccountSid, DistinguishedName

## Recovery Manager for Active Directory Data Fields

The following are lists of fields that occur in Recovery Manager for Active Directory data, organized by type of returned object.

**i** **NOTE:** The **In UI** column indicates if the field is available in the IT Security Search web UI as a clickable element. Whether or not you can click it in the UI, you can type any of these fields in your search queries.

# Computers

Field Name	In UI	Example Value	Details
AccountSid	Yes	S-1-5-21-4039273466-3631535243-455089366-89812	Computer account SID
Description	Yes	Storage Server	Description of computer
DistinguishedName	No	CD=DC1, CN=Domain Controllers, DC=it, DC=sales, DC=mycompany	Computer account distinguished name; search by full value only
DNSHostName	Yes	DC1.it.sales.mycompany	DNS host name
Location	Yes	Houston	Location of computer
ManagedBy	No	CN=Caroline Abbage, OU=Employees, DC=it, DC=sales, DC=mycompany	Same as ManagedByFullName
ManagedByFullName	No	CN=Caroline Abbage, OU=Employees, DC=it, DC=sales, DC=mycompany	Distinguished name of manager of the computer account; search by full value only
Name	Yes	DC1	Same as NetBiosName
NetBiosName	Yes	DC1	NetBIOS name of computer
NumLogons	Yes	12656	Logon count
ObjectCategory	Yes	computer	Object class = computer
ObjectGUID	No	ddd94ab4-5de6-4696-a93c-433cf9827c28	Object GUID of computer account
OSName	Yes	Windows Server 2008 R2 Enterprise	OS name
OSServicePack	Yes	Service Pack 1	OS service pack
OSVersion	Yes	6.1 (7601)	OS version
Where	Yes	DC1	Same as NetBiosName
Who	Yes	CN=Caroline Abbage,	Same as ManagedByFullName

Field Name	In UI	Example Value	Details
		OU=Employees, DC=it, DC=sales, DC=mycompany	

## Groups

Field Name	In UI	Example Value	Details
CN	Yes	Users	Common name of group
Description	Yes	Houston internal group for notification	Description of group
DisplayName	Yes	Users	Display name of group
DistinguishedName	No	CN=MCDL.RD.Notification, OU=RD, OU=Groups, DC=it, DC=sales, DC=mycompany	Distinguished name of group;. search by full value only
Email	Yes	MCDL.RD.Notification@it.sales.mycompany	Email address of group
GroupType	No	-2147483640	Integer value of bitmask that contains information about group type and scope; search by full value only (more details at <a href="https://msdn.microsoft.com/en-us/library/ms675935.aspx">https://msdn.microsoft.com/en-us/library/ms675935.aspx</a> )
HomePage	Yes	http://homepage	Home page of group
Info	Yes	Some info	Additional information about group
ManagedBy	No	CN=Caroline Abbage, OU=Employees, DC=it, DC=sales, DC=mycompany	Same as ManagedByFullName
ManagedByFullName	Yes	CN=Caroline Abbage, OU=Employees, DC=it, DC=sales, DC=mycompany	Distinguished name of manager of the group; search by full value only
Name	Yes	Users	Name of group

Field Name	In UI	Example Value	Details
ObjectCategory	Yes	group	Object class = group
ObjectGUID	No	80b090a2-968f-42e6- bc76-6e2505f43759	GUID of group object
SAMAccountName	Yes	Users	SAMAccount name of group
Url	Yes	http://groupname	URL of group
Who	Yes	CN=Caroline Abbage, OU=Employees, DC=it, DC=sales, DC=mycompany	Same as ManagedByFullName

## OUs

Field Name	In UI	Example Value	Details
Description	Yes	Default container for Defender objects	Description of OU
DistinguishedName	No	OU=BestEmployees, DC=it, DC=sales, DC=mycompany	Distinguished name of group; search by full value only
ManagedBy	No	CN=Clive Herry, OU=mgmt, OU=TestUsers, DC=it, DC=sales, DC=mycompany	Same as ManagedByFullName
ManagedByFullName	Yes	CN=Clive Herry, OU=mgmt, OU=TestUsers, DC=it, DC=sales, DC=mycompany	Distinguished name of manager of the OU; search by full value only
Name	Yes	Users	Name of OU
ObjectCategory	Yes	organizationalUnit	Object class = organizationalUnit or container
ObjectGUID	No	675205fb-4d29-44b6-	GUID of OU

Field Name	In UI	Example Value	Details
		9284-69e867689f38	
USNChanged	No	9296605	USN-Changed attribute of OU; search by full value only

## Users

Field Name	In UI	Example Value	Details
AccountSid	No	S-1-5-21-4039273466-3631535243-455089366-26350	User SID; search by full value only
Company	Yes	MyCompany	Company name
Country	Yes	United States	Country name
Department	Yes	Sales	Department name
DisplayName	No	Caroline Abbage	User display name
DistinguishedName	No	CN=Caroline Abbage, OU=Employees, DC=it, DC=sales, DC=mycompany	User distinguished name; search by full value only
EmailAddress	Yes	Caroline.Abbage@sales.mycompany.com	Email address
HomePhoneNumber	Yes	+1 410 531 0638	Home telephone number
Logon Name	No		Same as LogonName
LogonName	No	SVC-Scanner@main.mycompany.corp	Logon name for the domain user
ManagedBy	No	CN=Caroline Abbage, OU=Employees, DC=it, DC=sales, DC=mycompany	Same as ManagedByFullName
ManagedByFullName	No	CN=Caroline Abbage, OU=Employees, DC=it, DC=sales, DC=mycompany	Distinguished name of manager of user; search by full value only
Mobile	Yes	+ 911 9 769 8889	Mobile phone number

Field Name	In UI	Example Value	Details
Name	Yes	Caroline Abbage	User name
ObjectCategory	Yes	user	Object class = user
ObjectGUID	No	861205fb-4d29-44b6-9284-69e867689f38	User object GUID; search by full value only
Office	Yes	Ludlow st. 80, suite 200	Physical delivery office name
SAMAccountName	Yes	jcdenton	SAMAccountName of user
StreetAddress	Yes	Ludlow st. 80	Street address
TelephoneNumber	Yes	+ 123 4 567 8900	Telephone number
Title	Yes	Mgr, Sales	User job title
USNChanged	No	9296605	USN-Changed attribute of user; search by full value only
Who	No	Administrator	Search in the following attributes: SAMAccountName, DisplayName, AccountSid, DistinguishedName

# Saving Searches and Running Saved Searches

You can save any search for later reuse. Any IT Security Search operator or administrator can save searches and run saved searches, but only administrators can make them public for shared use.

## Saving Searches

To save a search, click the drop-down icon at the left edge of the search box and click **Save Current Search**. Proceed to configure your search in the popup that appears:

- Give the search a meaningful name.
- Add tags so that users can easily find the search by category.
- Select which parameters you want to make customizable, if necessary.  
All field names that occur in your search string are listed. Select the check boxes next to the ones that you want to make customizable. Whenever this saved search is used in the future, it will prompt for the values of all of the fields you select.

**i** **NOTE:** The field selection controls in the popup are really only a graphical way to include special syntax in your search string. The syntax for a customizable attribute is a string (usually, the field name) enclosed in double curly braces, in the place of a value substring.

For example, **Domain:{{Domain}}** will make IT Security Search prompt you for the value of the Domain field, labeled "Domain"; **Domain:{{Active Directory Domain}}** will also prompt you for the value of Domain, but the label will be "Active Directory Domain".

You can manually construct search strings that include this syntax, without using the field selector. This helps you provide descriptive labels for parameters.

- Specify the time period that the search must cover.  
For that, select one of the options at the right edge of the search box. These times are relative to the moment the saved search is run.

When you have configured these options, click **Save**.

## Running a Saved Search

To run an existing saved search, click the drop-down icon at the left edge of the search box; the available saved searches are listed at the bottom of the popup that appears. You can filter the list by clicking tag buttons in the **Saved Search Categories** drop-down.

## Making a Saved Search Public or Private

You can publish a search to make it available to all operators only if you are an IT Security Search administrator.

In the saved search list, the items have a lock icon showing their state. A private search has a closed lock icon; click the icon to make it public. A public search has an open lock icon; click the icon to make it private.

## Deleting a Saved Search

To delete a saved search, highlight it in the saved search list and click the cross icon.

## Importing and Exporting Searches

Saved search import and export capabilities help you back up and restore your IT data analysis knowledge and share it with other IT Security Search users.

To use the **Import** and **Export** actions, click the drop-down icon at the left edge of the search box; these actions are available at the top of the drop-down menu.

When you click **Export**, you are prompted to save a **\*.yaml** file. The resulting file will contain all saved searches created under your account plus any saved searches made public by administrators.

**i** **NOTE:** This action saves not only searches but also any custom action links defined in your IT Security Search deployment. For details about making custom action links, see [Customizing Action Links](#).

When you click **Import**, you are prompted to select a previously exported **\*.yaml** file. If the file includes any searches with the same names as your existing searches, you have the option to collectively skip, overwrite or automatically rename such searches.

**i** | **IMPORTANT:** Overwriting administrator-created public saved searches is disallowed for IT Security Search operators, but not for administrators; in this situation, if you are an operator, the search in the source file is silently skipped instead.

## Customizing Action Links

An action link is a clickable search link displayed to the left of a details page for an object. Action links are a way to enhance the cohesion of data that is linked in any way and enrich the context for the data you discover.

IT Security Search provides a number of action links out of the box. For example, you get the **Files and folders owned by this user** link when you view the details of a user and the **Who changed permissions on this file** link for a file. In addition to such bundled action links, you can define your own and bring them into your IT Security Search deployment using an import operation.

## Defining Action Links

To define an action link, you need to create a valid YAML file that specifies the details of that link. A single YAML file can contain definitions of multiple action links along with definitions of saved searches. If action links and saved searches are in the same YAML file, that doesn't mean they are associated with one another in any way. Each one is defined individually, and you can group them into files however you like.

The following is an example of two YAML-formatted action link definitions specified after saved search definitions in a single file. If you need additional information about the valid format, see the documentation at <https://yaml.org>.

```
SavedSearches:
...
ActionLinks:
- Name: Logons by this user
  Query: 'Who:"{LogonName}" AND (What:authentication OR What:logon) '
  Source: Users
  Target: Events
  Condition: '-Department:Management'
  Tags:
  - My company's action link kit
  - OnPremise
- Name: Applications for this tenant
  Query: 'objecttype="Azure Applications" AND Tenant:"{name}" '
  Source: Azure Tenants
  Target: Azure Applications
  Tags:
```

```
- My company's action link kit
- Cloud
- Name: Find this event in Event-o-pedia
  Query: 'http://eventopedia.cloudapp.net/?EventID={EventID}'
  Source: Events
  External: true
```

The following fields are required in an action link definition (mandatory fields are **bolded**):

- **Name**  
The display name of the link as it should appear in the left pane of the object details page; make sure this name is unique across your entire IT Security Search deployment.
- **Query**  
The search query that is run when the action link is clicked; the query can contain references to the field values of the current object, enclosed in curly braces.
- **Source**  
The type of object for which the action link is available.
- **Target**  
The search will run for all object types, but this tab will be opened. This field is ignored if the External field is set to **true**.
- **Condition**  
A valid IT Security Search query that specify particular properties that an object must have to provide this action link. If the condition isn't met, then the action link remains hidden. The query can contain references to the field values of the current object.
- **External**  
If set to **true**, the link is treated as the URL of an external resource instead of an IT Security Search query. If you want to insert field values in any part of the URL, use field names enclosed in curly braces. This helps automate the use of search engines and similar resources directly from IT Security Search details pages.
- **Tags**  
Arbitrary tags with arbitrary values. Currently, this field is unused and treated as a user comment. Consider giving your custom action links unified tags for your own convenience.

## Importing and Resetting Custom Action Links

Only IT Security Search administrators can import and reset actions links. To import action links, click the drop-down icon at the left edge of the search box and select **Import**. Note that both action links and saved searches are imported by this action. If you want strictly action links, don't include any saved searches in the **\*.yaml** file intended for import.

### **i** NOTES:

- Unlike saved searches, action links cannot be made private. All imported action links become available to everyone.
- In the event of a name clash during import, you are prompted to choose if you want to overwrite, rename or skip the links, or cancel the import.

To remove all custom action links and restore the default set, click the **Reset Actions** button, which is at the top of the Actions section in object details. Note that the button removes all custom action links for all object types and leaves only the default set.

# Use Scenarios

The following examples explain how IT Security Search tools can be applied in practice to real-life situations.

## Finding and Examining a User

To find events where a particular user is somehow involved (as the doer or as a subject), run a search for any of the variety of names that identify the user in the environment. You can supply the first name, last name, full name, logon name and so on.

The results of your search put the most relevant matching users at the top of the list. If there are too many matches, refine the results using facets.

From a different perspective, if you need to find a user whose name you are not sure about but whose manager's name you remember, try searching for the manager's name, then opening the details of the manager's user account and finding the user you are looking for among the manager's direct reports.

## Understanding Who Did What

A typical use case is tracking the activity that involved a particular object, such as a file, folder, group or user account. You begin by finding this object; this provides a starting point and a context for your session. The next step is to use the links in the object's details view. This is the easiest way to create a context and filter out irrelevant data.

Another option is to start with events directly, especially if you expect to find specific events within a specific period of time. To specify the period, use the date range filter. The graphical timeline in the result grid can help you quickly locate peaks of activity that need closer examination.

For example, suppose you have discovered an unknown application called **testaadapp** in your Azure environment, and you want to know how it got there. To find the relevant events, run a search like the following:

```
testaadapp AND description:"add"
```

In the events that you find, use the **Who** link to discover who added the application.

## Getting Insights from the Who and Whom Fields

You can learn a lot about a security incident just by looking at the initiator of an event and the account or object affected by the event. For this common pattern, the **Who** and **Whom** fields are defined for a variety of events. This gives you a consistent analysis tool, no matter what event fields the relevant data is actually stored in.

The technique is especially useful when you are looking at the account management activity of a particular user with administrative privileges.

## Exploring a User's Scope of Access

IT Security Search provides quick access to information about files and folders owned by a user and all permissions assigned to the user; for that, use the **Files and folders owned by this user**, **Files and folders where this user has direct permissions** and **Files and folders where this user has permissions (both direct and indirect)** links in the details view for the user you are interested in.

Conversely, if you start with a particular file or folder, its details contain a table of permissions, which can prompt your further steps.

## Tracking Permission Management

You can easily follow permission assignment activity using the **Who changed permissions on this file** and **Who changed permissions on this folder** links in the details view of a file or folder, respectively.

## Exploring and Rolling Back Changes to Active Directory Objects

Object change history is available only if the Recovery Manager for Active Directory connector is enabled. For information about changes to an object and recovery tools, go to the **History** tab on the object's details page. This tab has two modes: Changes and Backups.

In Backups mode, the most recent backup states (three by default) of the object are shown, with details about how their attribute values differ from the current state. You can fully restore any of these states by clicking the **Restore from backup** link for that state.

In Changes mode, you have more fine-grained control and can view and roll back individual attribute changes. All changes recorded in the most recent backups are shown, including the "before" and "after" values, and you can sort them by attribute name or by date. To roll back individual changes, select their check boxes in the table and click the **Revert to the previous attribute state** link.

**i** **NOTE:** In Changes mode, the date shown for a particular change is the date of the backup that contains information about that change. The date can be empty, meaning that the change is recent and has not been recorded in any backup state.

## Detecting Preparations for Intrusion

You can track attempts to probe Active Directory prior to intrusion. One symptom of such activity is a trail of LDAP queries from unlikely workstations or by suspicious accounts. It may mean an effort to find vulnerable Active Directory accounts with administrative privileges. The following types of LDAP query in quick succession are telltale signs of this:

- Looking for information about account passwords and statuses
- Listing groups
- Querying administrative group membership

In IT Security Search, you can track such queries by running the following search:

```
What:"AD Query Performed"
```

In the search results, examine the **LDAP - Attributes** and **LDAP - Filter** fields.

In the following examples, **trustedworkstation1** and **trustedworkstation2** are computers where you don't consider running LDAP queries suspicious; with all other workstations, it's best to take a closer look.

- Someone is looking for information about user accounts:  

```
Source="ChangeAuditor" What="AD Query Performed" [LDAP - Attributes]:"*password*" [LDAP - Filter]:"*user*" - Workstation=trustedworkstation1 -Workstation=trustedworkstation2
```
- Someone is exploring administrative group membership:  

```
Source="ChangeAuditor" What="AD Query Performed" [LDAP - Attributes]:"*member*" [LDAP - Filter]:"*admin*" [LDAP - Filter]:"*group*" - Workstation=trustedworkstation1 -Workstation=trustedworkstation2
```

Similar suspicious behavior often precedes pass-the-hash attacks that rely on stored password hashes. In this case, it can be accompanied by series of remote logon attempts to computers in the network. To capture such activity, you should also search for logon events that occurred around the same time as the LDAP queries you found.

## Case Study: Investigating Tampering

Suppose a critical file (such as a project roadmap or payroll file) is showing signs of tampering. You want to use IT Security Search to look into this.

### What you will need

To make the investigation as efficient as possible, make sure that data from the following sources is available:

- For security events, including user session events: InTrust
- For file change information: Change Auditor
- For user information: Enterprise Reporter

### Where to start

You are about to examine the circumstances of file modifications, so it makes sense to start by finding the affected file. This will provide clues about where to go next and also mark a point (as a breadcrumb) that you can always fall back to, even if your next steps take you too far.

### How to proceed

When you have found the file, open its full details and use the **Who accessed this file** link provided in that view. In the list of events that are found, find a "File changed" event and use the **What** facet to filter out other types of events. Try to spot any unlikely users in the list of file change events.

Suppose you find an event by a user who is not meant to have access to the file. Note the time of the event, and then open the details of the event and click the user name. In the the user details view that opens, click the **Files and folder where this user has permissions** link. If the file in question is not listed, that means the permissions have been rolled back by now—likely a piece of incriminating data.

You can also view the entire history of permission management for the file. Use the breadcrumbs to go back to the file details view, and click the **Who granted permissions to this file** link.

Use the breadcrumbs to go back to the user details view, and click the **Activity initiated by this user** link. Use the time range filter to restrict the results to a period around the time of the suspicious file modification. The results may reveal noteworthy details about the situation. Consider examining InTrust-specific user session events for the following clues:

- Logon session time and duration
- Whether the session was interactive or Terminal Services-based

In addition, check if there were any attempts to clear security logs.

## Case Study: Making the Most of Multiple Connectors

Suppose a user complains about being unable to log in through VPN. Use IT Security Search to investigate and resolve the situation.

### What you will need

For best results, enable the following connectors:

- For security events: InTrust and Change Auditor
- For Active Directory object modification and recovery: Recovery Manager for Active Directory
- For user information: Enterprise Reporter

### Where to start

You should start by searching for the **David Shore** user account, which is having problems. To get results quickly, use the **Whom:"David Shore"** query. This will take you directly to the events that affected the account.

### How to proceed

Suppose the search results include group membership change events from InTrust and Change Auditor indicating that the user was removed from one or more groups. Examine these events and find the one about the group used for providing VPN access. Note that the timestamp of the event is later than the last Active Directory backup. Also note the other event details such as who did this.

In the breadcrumbs line, click the user name to open the user details, and go to the **History** tab. In the change history view on the Backups tab, locate the state before the VPN-related group membership change, and click the corresponding **Restore from backup** link.

VPN access for **David Shore** is restored now, and you know who interfered with his group membership.

# Case Study: Active Roles Dynamic Group Membership Tracking

Suppose a new user is not getting the expected permissions to open a network share. You want to use IT Security Search to look into this.

## What you will need

To make the investigation as efficient as possible, make sure that data from the following sources is available:

- For network share and user information: Enterprise Reporter
- For dynamic group membership information: Active Roles

## Where to start

You are about to examine share access, so it makes sense to start by looking at share permissions.

## How to proceed

Search for the share path. Click the share you need in the list of results and open its details. In the permissions table, you find the **Marketing** group, which is used for controlling access to the share. Apparently the user is supposed to be a member of this group, but is not.

Do a search for the **Marketing** group; click the group in the results and go to the details view for the it. It turns out to be an Active Roles dynamic group. Click the **Membership Rules** tab in the details table to see how the group is populated. In the Rule Details column, you find the following rule: "[User] department Is (exactly) Marketing".

The user's department information is probably wrong, making the user unfit for membership in the **Marketing** dynamic group. See if this guess is correct: search for the user name, locate the user in the results and open the user's details.

You find that the value of the Department attribute has a typo: "Markering" instead of "Marketing", and you notify security administrator about this issue.

When you get a response from the administrator saying that the problem has been resolved, you do another search for the **Marketing** group to confirm that the user is now a member.

# Additional Utility Scripts

IT Security Search comes with additional PowerShell scripts that help automate configuration. These scripts are available in the **Scripts** subfolder of your IT Security Search installation folder. At this time, the following scripts are shipped:

Scripts	Details
New-SslCertificate.ps1 New-CertificateBinding.ps1 Delete-CertificateBinding.ps1	These scripts help configure the SSL certificate used by IT Security Search. For details, see <a href="#">Security Details and Configuration</a> .
Set-ItssConnectorSettings.ps1	Updates the settings of an IT Security Search connector. For details, see the script's help output.
ITSS-ExportFields.psm1	Customizes the layout of search results exported to a file: rearranges and resizes the columns for the object types that you specify. The script applies the layout configuration you provide directly; it doesn't use the column set configured in the IT Security Search UI. For details, see the script's help output.

# Providing Information to Support

If you need to contact Support, you should provide various technical details for a speedy response. IT Security Search includes a utility that automatically gathers all the information that support engineers may need and stores it in a single ZIP file.

To create such a file, open the About box in the IT Security Search UI, select the Contact tab and click **Save Information for Support**. The file is not transferred to Support automatically. To submit it, open a service request at <https://support.quest.com/contact-support>.

Quest needs your consent for gathering the data, because some information in the resulting file may be considered sensitive. Quest ensures that storage and processing of this information are duly protected to safeguard your privacy.

The following information is gathered:

- Settings of connected products (InTrust, Change Auditor and others); passwords are encrypted
- Security settings
- IT Security Search log files, which contain queries, counts of found objects and IT Security Search users' names
- IT Security Search configuration files
- Information about IT Security Search files: path, last write time, version
- Status of IT Security Search stores: path, counts of collected items, sizes
- The user-agent string of the browser
- Products installed on the server: name, version, publisher, install date, PSChildName
- Services installed on the server and the list of running services
- List of running processes and their details
- Server configuration: name, description, OS, amount of available memory, country code, current time zone, local time, encryption level, number of users, organization, OS language, DNS host name, domain, domain role, number of processors
- Logical drive details: caption, description, drive type, size, free space, path, file system

IT Security Search uses PowerShell to collect the data.

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit [www.quest.com](http://www.quest.com).

## Contacting Quest

For sales or other inquiries, visit [www.quest.com/contact](http://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

# Third-party contributions

This product contains the following third-party components. For third-party license information, go to <http://www.quest.com/legal/license-agreements.aspx>. Source code for components marked with an asterisk (\*) is available at <https://opensource.quest.com>.

**Table 1: List of Third-Party Contributions**

Component	License and/or Acknowledgement
Angular 9.0	MIT Copyright (c) 2010-2020 Google LLC. <a href="http://angular.io/license">http://angular.io/license</a>
Angular.js 1.8.0	MIT Copyright (c) 2010-2020 Google, Inc. <a href="http://angularjs.org">http://angularjs.org</a>
angular-file-upload 1.1.5	MIT Copyright (c) 2013 nerv. <a href="https://github.com/nervgh">https://github.com/nervgh</a>
angular-timer 1.1.9	MIT Copyright (c) 2013 Siddique Hameed
angular-translate 2.8.1	MIT Copyright (c) 2015 The angular-translate team, Pascal Precht
angular-ui-bootstrap 2.5.0	MIT Copyright (c) 2012-2017 the AngularUI Team, <a href="https://github.com/organizations/angular-ui/teams/291112">https://github.com/organizations/angular-ui/teams/291112</a>
angular-ui-utils 0.0.3	MIT Copyright (c) 2015 the AngularUI Team, <a href="http://angular-ui.github.com">http://angular-ui.github.com</a>
Bootstrap 3.1.1	MIT Copyright (c) 2011-2016 Twitter, Inc.
Castle.Core 4.3.1	Apache 2.0 Copyright 2004-2018 Castle Project - <a href="http://www.castleproject.org/">http://www.castleproject.org/</a>
CommandLineParser 2.3.0	MIT Copyright (c) 2005 - 2018 Giacomo Stelluti Scala & Contributors
Community MSI Extensions 1.4*	Eclipse Public License 1.0 Copyright (c) Application Security Inc. and Contributors The source code for this component is available at <a href="https://opensource.quest.com/releases/WixUserPrivilegesExtension.zip">https://opensource.quest.com/releases/WixUserPrivilegesExtension.zip</a>

<b>Component</b>	<b>License and/or Acknowledgement</b>
CsQuery 1.3.4	MIT Copyright (c) 2012 James Treworgy
CsvHelper 7.1.1	Dual licensing under Microsoft Public License (MS-PL) and Apache 2.0 Copyright 2009-2017 Josh Close and Contributors
daterangepicker 2.1.25	MIT Copyright (c) 2012-2017 Dan Grossman
DotNetZip 1.13.3	DotNetZip 1.13.3 Copyright (c) 2006 - 2011 Dino Chiesa Copyright (c) 2006, 2007, 2008, 2009 Dino Chiesa and Microsoft Corporation. Copyright (c) 2000,2001,2002,2003 ymnk, JCraft, Inc. Copyright (C) 1995-2004 Jean-loup Gailly and Mark Adler Copyright 2002-2014 The Apache Software Foundation
Elasticsearch.Net 2.5.8	Apache 2.0 Copyright (c) 2014-2018 by Elasticsearch BV
Google Open Sans 1.10	Apache 2.0 Digitized data copyright © 2010-2011, Google Corporation.
HighCharts 3.0.4	Highsoft Solutions AS OEM License Agreement 2.0 (c) 2009-2013 Torstein Hønsi
JetBrains.Annotations 2018.2.1	MIT Copyright (c) 2016 JetBrains <a href="http://www.jetbrains.com">http://www.jetbrains.com</a>
jQuery 3.3.1	MIT Copyright 2018 The jQuery Foundation
jquery.fileDownload 1.4.5	MIT Copyright (c) 2014 John Culviner
Kendo UI Web 2014.3.1411	Kendo UI Web Copyright 2013 Telerik AD. All rights reserved.
keycloak-js-bower 3.2	Apache 2.0 Copyright 2017 Red Hat
Linq2Rest 4.1.0	Microsoft Public License (Ms-PL) 1.0 Copyright © Reimers.dk 2014
Log4Net 2.0.12	Apache 2.0 Copyright 2004-2017 The Apache Software Foundation

<b>Component</b>	<b>License and/or Acknowledgement</b>
Lucene.Net 3.0.3	Apache 2.0 Copyright 2013 The Apache Software Foundation
Lucene.Net.Contrib 3.0.3	Apache 2.0 Copyright 2013 The Apache Software Foundation
Microsoft.Bcl 1.1.10	Microsoft .NET Library 1.0
Microsoft.Bcl.Build 1.0.21	Microsoft .NET Library 1.0
Microsoft.IdentityModel.JsonWebTokens 5.3.0	MIT Copyright (c) Microsoft Corporation. All rights reserved.
Microsoft.IdentityModel.Logging 5.3.0	MIT Copyright (c) Microsoft Corporation. All rights reserved.
Microsoft.IdentityModel.Protocols 5.3.0	MIT Copyright (c) Microsoft Corporation. All rights reserved.
Microsoft.IdentityModel.Protocols.OpenIdConnect 5.3.0	MIT Copyright (c) Microsoft Corporation. All rights reserved.
Microsoft.IdentityModel.Tokens 5.3.0	MIT Copyright (c) Microsoft Corporation. All rights reserved.
Microsoft.Owin 4.0	Microsoft .NET Library
Microsoft.Owin.Host.HttpListener 4.0	Microsoft .NET Library
Microsoft.Owin.Hosting 4.0	Microsoft .NET Library
Microsoft Unity 3.5	Apache 2.0 Copyright (c) Microsoft Corporation. All rights reserved.
Moment.js 2.29.2	MIT Copyright (c) JS Foundation and other contributors
Nancy 1.4.5	MIT Copyright (c) 2010 Andreas Håkansson, Steven Robbins and contributors
Nancy.Boostsrappers.Ninject 1.4.1	MIT Copyright (c) 2010 Andreas Håkansson, Steven Robbins and contributors
Nancy.Owin 1.4.1	MIT Copyright (c) 2010 Andreas Håkansson, Steven Robbins and contributors



Component	License and/or Acknowledgement
	<pre>// Project Item Name: IRTFCell.cs - Code // Purpose: Exposes an underlying RTFBuilderbase // ----- -----</pre>
SharpZipLib 1.1	MIT Copyright © 2000-2018 SharpZipLib Contributors
SmartFormat.NET 2.3.0	MIT Copyright 2011-2017 Scott Rippey, axuno gGmbH, Bernhard Millauer and other contributors.
Splunk.Client 2.2.9	Apache 2.0 Copyright © 2015 Splunk, Inc.
System.Collections.Immutable 1.1.37	Microsoft .NET Library 1.0
System.IdentityModel.Tokens.Jwt 5.3.0	MIT Copyright (c) Microsoft Corporation. All rights reserved.
System.Management.Automation.dll 10.0.10586.0	Microsoft .NET Library 1.0
System.Runtime.CompilerServices.Unsafe 4.5.2	MIT Copyright (c) Microsoft Corporation. All rights reserved.
System.Threading.Tasks.Extensions 4.5.1	MIT Copyright (c) Microsoft Corporation. All rights reserved.
Underscore.js 1.9.1	MIT Copyright (c) 2009-2018 Jeremy Ashkenas, DocumentCloud and Investigative Reporters & Editors
Windows Installer XML Toolset (aka WiX) 3.11.1	Microsoft Reciprocal License (MS-RL) Copyright (c) Outercurve Foundation The source code for this component is available at <a href="https://opensource.quest.com/releases/Wix_3.11.zip">https://opensource.quest.com/releases/Wix_3.11.zip</a>
ZetaLongPaths 1.0.0.25	MIT Copyright (c) 2009-2018 Zeta Software GmbH

## Licenses

### Apache 2.0

Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>

## TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

### 1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition,

"control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems,

and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution." "Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

- (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
- (b) You must cause any modified files to carry prominent notices stating that You changed the files; and
- (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
- (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained

within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions.

Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have performed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special,

incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

## DotNetZip 1.13.3

Software Licenses that apply to the DotNetZip library and tools

As DotNetZip includes work derived from other projects, you are required to comply with the terms and conditions for each of them. These licenses include BSD, Apache, and zlib.

To use the software, you must accept the licenses. If you do not accept the licenses, do not use the software.

Original intellectual property in DotNetZip is provided under the Ms-PL:

Copyright (c) 2006 - 2011 Dino Chiesa

Copyright (c) 2006, 2007, 2008, 2009 Dino Chiesa and Microsoft Corporation.

Microsoft Public License (Ms-PL)

This license governs use of the accompanying software, the DotNetZip library ("the software"). If you use the software, you accept this license. If you do not accept the license, do not use the software.

### 1. Definitions

The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.

A "contribution" is the original software, or any additions or changes to the software.

A "contributor" is any person that distributes its contribution under this license.

"Licensed patents" are a contributor's patent claims that read directly on its contribution.

### 2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

### 3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

-----  
The managed ZLIB code included in Ionic.Zlib.dll and Ionic.Zip.dll is derived from jzlib.

jzlib ( <https://github.com/yumnk/jzlib> ) is provided under a BSD-style (3 clause)

Copyright (c) 2000,2001,2002,2003 yumnk, JCraft, Inc.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL JCRAFT, INC. OR ANY CONTRIBUTORS TO THIS SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

-----  
The jzlib library, itself, is a re-implementation of ZLIB v1.1.3 in pure Java.

zlib is provided under the zlib license:

Copyright (C) 1995-2004 Jean-loup Gailly and Mark Adler

The ZLIB software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly [jloup@gzip.org](mailto:jloup@gzip.org) Mark Adler [madler@alumni.caltech.edu](mailto:madler@alumni.caltech.edu)

---

The managed BZIP2 code included in Ionic.BZip2.dll and Ionic.Zip.dll is modified code, based on Java code in the Apache commons compress library.

Apache Commons Compress ( <http://commons.apache.org/proper/commons-compress/> ) is provided under the Apache 2 license:

Apache Commons Compress

Copyright 2002-2014 The Apache Software Foundation

Licensed to the Apache Software Foundation (ASF) under one or more contributor license agreements. See the NOTICE file distributed with this work for additional information regarding copyright ownership. The ASF licenses this file to you under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Many thanks to Julian Seward for the original C implementation of BZip2 ( <http://www.bzip.org/> ).

## Eclipse Public License - v 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS ECLIPSE PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

### 1. DEFINITIONS

"Contribution" means:

- a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and
- b) in the case of each subsequent Contributor:

- i) changes to the Program, and
- ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

### 2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the

combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

### 3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

### 4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's

responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

#### 5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

#### 6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

#### 7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. The Eclipse Foundation is the initial Agreement Steward. The Eclipse Foundation may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

# GPL (GNU General Public License) 2.0

## GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

### Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free

program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all. The precise terms and conditions for copying, distribution and modification follow.

## GNU GENERAL PUBLIC LICENSE

### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an

announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or runnable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or runnable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an runnable work, complete source code means all the source code for all modules it contains, plus any

associated interface definition files, plus the scripts used to control compilation and installation of the runnable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the runnable runs, unless that component itself accompanies the runnable.

If distribution of runnable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then

the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

**NO WARRANTY**

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

As a special exception, you may use this file as part of a free software library without restriction. Specifically, if other files instantiate templates or use macros or inline functions from this file, or you compile this file and link it with other files to produce an runnable, this file does not by itself cause the resulting runnable to be covered by the GNU General Public License. This exception does not however invalidate any other reasons why the runnable file might be covered by the GNU General Public License.

END OF TERMS AND CONDITIONS

## Microsoft Reciprocal License (MS-RL)

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

### 1. Definitions

The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.

A "contribution" is the original software, or any additions or changes to the software.

A "contributor" is any person that distributes its contribution under this license.

"Licensed patents" are a contributor's patent claims that read directly on its contribution.

### 2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make,

have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

### 3. Conditions and Limitations

(A) Reciprocal Grants- For any file you distribute that contains code from the software (in source code or binary format), you must provide recipients the source code to that file along with a copy of this license, which license will govern that file. You may license other files that are entirely your own work and do not contain code from the software under any terms you choose.

(B) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(C) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(D) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(E) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(F) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

## Microsoft Public License (Ms-PL)

This license governs use of the accompanying software, the DotNetZip library ("the software"). If you use the software, you accept this license. If you do not accept the license, do not use the software.

### 1. Definitions

The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.

A "contribution" is the original software, or any additions or changes to the software.

A "contributor" is any person that distributes its contribution under this license.

"Licensed patents" are a contributor's patent claims that read directly on its contribution.

### 2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

### 3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

## New BSD License

Copyright (c) 2015-2017, App vNext

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

\* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

\* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

\* Neither the name of App vNext nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL <COPYRIGHT HOLDER> BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## RichText Builder (StringBuilder for RTF) License

License Text - Code Project Open License (CPOL) 1.02

Preamble

This License governs Your use of the Work. This License is intended to allow developers to use the Source Code and Executable Files provided as part of the Work in any application in any form.

The main points subject to the terms of the License are:

Source Code and Executable Files can be used in commercial applications;

Source Code and Executable Files can be redistributed; and

Source Code can be modified to create derivative works.

No claim of suitability, guarantee, or any warranty whatsoever is provided. The software is provided "as-is".

The Article(s) accompanying the Work may not be distributed or republished without the Author's consent

This License is entered between You, the individual or other entity reading or otherwise making use of the Work licensed pursuant to this License and the individual or other entity which offers the Work under the terms of this License ("Author").

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CODE PROJECT OPEN LICENSE ("LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HEREIN, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. THE AUTHOR GRANTS YOU THE RIGHTS CONTAINED HEREIN IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO ACCEPT AND BE BOUND BY THE TERMS OF THIS LICENSE, YOU CANNOT MAKE ANY USE OF THE WORK.

Definitions.

"Articles" means, collectively, all articles written by Author which describes how the Source Code and Executable Files for the Work may be used by a user.

"Author" means the individual or entity that offers the Work under the terms of this License.

"Derivative Work" means a work based upon the Work or upon the Work and other pre-existing works.

"Executable Files" refer to the runnables, binary files, configuration and any required data files included in the Work.

"Publisher" means the provider of the website, magazine, CD-ROM, DVD or other medium from or by which the Work is obtained by You.

"Source Code" refers to the collection of source code and configuration files used to create the Executable Files.

"Standard Version" refers to such a Work if it has not been modified, or has been modified in accordance with the consent of the Author, such consent being in the full discretion of the Author.

"Work" refers to the collection of files distributed by the Publisher, including the Source Code, Executable Files, binaries, data files, documentation, whitepapers and the Articles.

"You" is you, an individual or entity wishing to use the Work and exercise your rights under this License.

Fair Use/Fair Use Rights. Nothing in this License is intended to reduce, limit, or restrict any rights arising from fair use, fair dealing, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

License Grant. Subject to the terms and conditions of this License, the Author hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

You may use the standard version of the Source Code or Executable Files in Your own applications.

You may apply bug fixes, portability fixes and other modifications obtained from the Public Domain or from the Author. A Work modified in such a way shall still be considered the standard version and will be subject to this License.

You may otherwise modify Your copy of this Work (excluding the Articles) in any way to create a Derivative Work, provided that You insert a prominent notice in each changed file stating how, when and where You changed that file.

You may distribute the standard version of the Executable Files and Source Code or Derivative Work in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution.

The Articles discussing the Work published in any form by the author may not be distributed or republished without the Author's consent. The author retains copyright to any such Articles. You may use the Executable Files and Source Code pursuant to this License but you may not repost or republish or otherwise distribute or make available the Articles, without the prior written consent of the Author.

Any subroutines or modules supplied by You and linked into the Source Code or Executable Files this Work shall not be considered part of this Work and will not be subject to the terms of this License.

Patent License. Subject to the terms and conditions of this License, each Author hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, import, and otherwise transfer the Work.

Restrictions. The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

You agree not to remove any of the original copyright, patent, trademark, and attribution notices and associated disclaimers that may appear in the Source Code or Executable Files.

You agree not to advertise or in any way imply that this Work is a product of Your own.

The name of the Author may not be used to endorse or promote products derived from the Work without the prior written consent of the Author.

You agree not to sell, lease, or rent any part of the Work. This does not restrict you from including the Work or any part of the Work inside a larger software distribution that itself is being sold. The Work by itself, though, cannot be sold, leased or rented.

You may distribute the Executable Files and Source Code only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy of the Executable Files or Source Code You distribute and ensure that anyone receiving such Executable Files and Source Code agrees that the terms of this License apply to such Executable Files and/or Source Code. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute the Executable Files or Source Code with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License.

You agree not to use the Work for illegal, immoral or improper purposes, or on pages containing illegal, immoral or improper material. The Work is subject to applicable export laws. You agree to comply with all such laws and regulations that may apply to the Work after Your receipt of the Work.

Representations, Warranties and Disclaimer. THIS WORK IS PROVIDED "AS IS", "WHERE IS" AND "AS AVAILABLE", WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OR GUARANTEES. YOU, THE USER, ASSUME ALL RISK IN ITS USE, INCLUDING COPYRIGHT INFRINGEMENT, PATENT INFRINGEMENT, SUITABILITY, ETC. AUTHOR EXPRESSLY DISCLAIMS ALL EXPRESS, IMPLIED OR STATUTORY WARRANTIES OR CONDITIONS, INCLUDING WITHOUT LIMITATION, WARRANTIES OR CONDITIONS OF MERCHANTABILITY, MERCHANTABLE QUALITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTY OF TITLE OR NON-INFRINGEMENT, OR THAT THE WORK (OR ANY PORTION THEREOF) IS CORRECT, USEFUL, BUG-FREE OR FREE OF VIRUSES. YOU MUST PASS THIS DISCLAIMER ON WHENEVER YOU DISTRIBUTE THE WORK OR DERIVATIVE WORKS.

Indemnity. You agree to defend, indemnify and hold harmless the Author and the Publisher from and against any claims, suits, losses, damages, liabilities, costs, and expenses (including reasonable legal or attorneys' fees) resulting from or relating to any use of the Work by You.

Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL THE AUTHOR OR THE PUBLISHER BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK OR OTHERWISE, EVEN IF THE AUTHOR OR THE PUBLISHER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Termination.

This License and the rights granted hereunder will terminate automatically upon any breach by You of any term of this License. Individuals or entities who have received Derivative Works from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 6, 7, 8, 9, 10 and 11 will survive any termination of this License.

If You bring a copyright, trademark, patent or any other infringement claim against any contributor over infringements You claim are made by the Work, your License from such contributor to the Work ends automatically.

Subject to the above terms and conditions, this License is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, the Author reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

**Publisher.** The parties hereby confirm that the Publisher shall not, under any circumstances, be responsible for and shall not have any liability in respect of the subject matter of this License. The Publisher makes no warranty whatsoever in connection with the Work and shall not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation any general, special, incidental or consequential damages arising in connection to this license. The Publisher reserves the right to cease making the Work available to You at any time without notice

#### Miscellaneous

This License shall be governed by the laws of the location of the head office of the Author or if the Author is an individual, the laws of location of the principal place of residence of the Author.

If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this License, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

This License constitutes the entire agreement between the parties with respect to the Work licensed herein. There are no understandings, agreements or representations with respect to the Work not specified herein. The Author shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Author and You.