

Quest® InTrust 11.6.1

Special-Purpose Commands and Utilities



© 2024 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

4 Polaris Way

Aliso Viejo, CA 92656

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



Patents

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

Trademarks

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

Legend

-  **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.**

InTrust Special-Purpose Commands and Utilities

Updated - September 2024

Version - 11.6.1

Contents

Overview of Tools	4
	5
Cleanup of Temporary Tables	6
DBCleaner.exe Utility	6
SQL Scripts	7
Alert Severity Customization	8
Changing the Account Used by InTrust Services	9
Removing Unneeded InTrust Servers	10
Organization Parameter Editor	11
Tracking Real-Time Event Collection State	13
About us	15
Contacting Quest	15
Technical support resources	15

Overview of Tools

InTrust comes with a set of scripts and utilities that serve a variety of purposes. Using these tools, you can do the following:

- Automate InTrust installation by performing it in unattended mode.
The tools for InTrust installation are described in the [Deployment Guide](#).
- Provide the permissions and database tables required for InTrust installation and reporting.
The tools for database configuration are described in the [Deployment Guide](#).
- Manipulate repositories and their contents flexibly. For details about repository-related tools, see [Understanding InTrust Repositories](#) and [Repository Indexing for Advanced Search Capabilities](#).
- Clean up temporary database tables.
See [Cleanup of Temporary Tables](#).
- Customize the severity of real-time alerts.
See [Alert Severity Customization](#).
- Change the InTrust server account.
See [Changing the Account Used by InTrust Services](#).
- Cleanly remove the InTrust Server component from a computer.
See [Removing Unneeded InTrust Servers](#).
- Customize various operational parameters in InTrust.
See [Organization Parameter Editor](#).
- Estimate the health and efficiency of your real-time event collections.
See [Tracking Real-Time Event Collection State](#).

Cleanup of Temporary Tables

DBCleaner.exe Utility

Some reports may create temporary tables (which have prefixes such as **T_QCWP_TEMP_**, **TEMP_MACRO_** and **TEMP_**) in the data sources they work with. To avoid excessive database size growth, you can periodically remove temporary tables using the DBCleaner.exe command-line utility. This tool is located in the **InTrust\Tools\Database CleanUp** folder of your InTrust distribution.

When running the **DBCleaner.exe** utility, specify the following parameters:

1. Parameter to select tables by. Specify at least one of the following:
 - Table name prefix
 - Table owner

Also, you can use the **/from** and **/to** parameters to delete tables created in the specified time interval. The date format is YYYY-MM-DD hh:mm:ss.

2. Connection string. It must be typed in the following format and should be enclosed in double quotation marks:

```
"Provider=provider;Data Source=datasource;Initial Catalog=database;UID=username;PWD=password;"
```

-OR-

```
"Provider=provider;Data Source=datasource;Initial Catalog=database;Integrated Security='SSPI'"
```

where:

- Provider—OLEDB provider (for Microsoft SQL Server, it is "SQLOLEDB")
- Data Source—server name
- Initial Catalog—database name
- UID—user login name
- PWD—user password
- Integrated Security—specify this parameter if Windows authentication is in use

The format of the command line to run the utility should be like the following:

```
DBCleaner[.exe] /p[refix]:PREFIX /u[ser]:TABLE_OWNER [/from:DATE_FROM] [/to:DATE_TO] /c[onnection string]:CONNECTION_STRING
```

For example:

```
DBCleaner.exe /p:TEMP_ /u:DBO /from:2007-12-31 /to:2008-01-31 /c:"provider=SQLOLEDB; data source=DBServer; initial catalog=DBName; UID=UserName; PWD=test"
```

! **CAUTION:** Be careful when specifying the prefix. If no prefix is specified or the prefix is specified incorrectly, necessary tables can be deleted.

SQL Scripts

The **TempCleaner_2000.sql** and **TempCleaner_2005.sql** scripts are located in the same folder as the **DBCleaner.exe** command-line utility and have the same functionality.

To customize the parameters, edit them directly in the script code before running the scripts.

Alert Severity Customization

The **ITCustomAlertSeverity** utility allows you to define custom severity level for InTrust real-time alerts.

It is located in **<installation_folder>\Server\ADC\SupportTools\Win32**.

Below are the examples of command line syntax that should be used when running the utility:

```
ITCustomAlertSeverity -add <name> <severity_value> <color> <icon_file>
```

```
ITCustomAlertSeverity -remove <name>
```

```
ITCustomAlertSeverity -list
```

```
ITCustomAlertSeverity -export-icon <name> <icon_file>
```

The options are as follows:

Option	Description
-ADD	Adds a custom alert severity level to the configuration; the following arguments must be specified: <ul style="list-style-type: none">• NAME—Display name of the severity level• SEVERITY_VALUE— Decimal, hexadecimal or octal number that stands for the severity level• COLOR—Decimal, hexadecimal or octal number that sets the RGB color to mark the alert record that appears in Monitoring Console• ICON_FILE—Name of the alert icon file; 16x16 GIF image is the recommended format (BMP, JPG and ICO also supported)
-REMOVE	Removes the severity level (not the alerts!) specified by the <name> argument from configuration.
-LIST	List all currently defined severity levels.
-EXPORT-ICON	Export the icon associated with a severity level to an image file; the following arguments must be specified: <ul style="list-style-type: none">• NAME—Display name of the severity level• ICON_FILE—Name of the alert icon file

Changing the Account Used by InTrust Services

Use the **adcsrvacc** command-line utility to change the account of the Quest InTrust Server and Quest InTrust Real-Time Monitoring Server services. The **adcsrvacc** utility also lets you create a Service Connection Point (SCP) container and change its permissions and properties after starting the InTrust Server service.

This utility is located in **<InTrust_installation_folder>Server\ADC\SupportTools**.

To provide automatic creation of SCP or changing its permissions and properties by InTrust means, you should perform one of the following procedures before running **adcsrvacc**:

- Open the ADSI Edit snap-in and specify the following rights for **CN=System, DC=<Domain>** in the Active Directory configuration partition for the account under which you will run the **adcsrvacc** utility: **Create All Child Objects, Read Permissions, Modify Permissions, Read All Properties, Write All Properties**. These permissions must be applied to the **This object and all child objects** scope for this container.
- Open the ADSI Edit snap-in and create the **CN=Quest InTrust, CN=System, DC=<Domain>** in the Active Directory configuration partition. Assign the following rights for this container for the account under which you will run the **adcsrvacc** utility: **Create All Child Objects, Read Permissions, Modify Permissions**.

Run the utility with the following parameters:

```
adcsrvacc.exe -user <user> [-password <password>] [-restart] [-nocheck]
```

Here, **<user>** is the name of the user account (in the **DomainName\UserName** format) you want the services to use from now on; **<password>** is an optional parameter specifying the password of this account. If the password is not supplied, you will be asked to specify it in a secure prompt.

The optional **-restart** parameter automatically restarts the services after the account change.

The optional **-nocheck** parameter makes the utility skip the step where it checks whether the new account has the necessary privileges for access to the InTrust configuration database.

For information about the privileges required by the InTrust Server account, see [System Requirements](#).

Removing Unneeded InTrust Servers

If an InTrust server is no longer needed in an InTrust organization, it is best to remove it from the configuration database. This helps avoid possible problems during InTrust upgrade and other configuration-related operations.

To check for out-of-use InTrust servers

1. Use the SQL Server management tool to open the ADCServer table in the InTrust configuration database.
2. Review the values in the LastServerPing and Status fields to identify InTrust servers that are not in use any more.

When you have determined which servers are not in use any more, uninstall InTrust Server from those computers using the Add or Remove Programs facility.

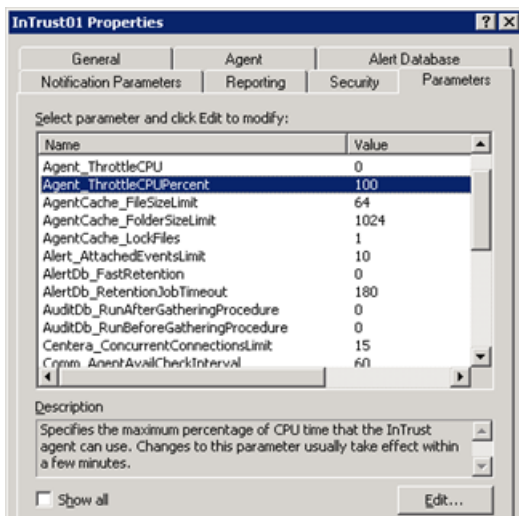
If this fails for some reason (for example, due to a corrupted InTrust Server installation), use the **adremoveserver.exe** command-line utility to clear all configuration data for the out-of-use servers. For that, run the **adremoveserver.exe** utility on an InTrust server different from the ones you are going to remove. The utility is located in the **<InTrust installation folder>\ADC\SupportTools folder**. The syntax is as follows:

```
adremoveserver.exe <server_name>
```

Organization Parameter Editor

The organization parameter editor is a tool for viewing and editing settings directly in the InTrust configuration database. The editor is meant for advanced parameters that are not changed often.

The available settings relate to agents, jobs and so on. They vary in where and how soon they take effect. For details, see the descriptions of individual settings.



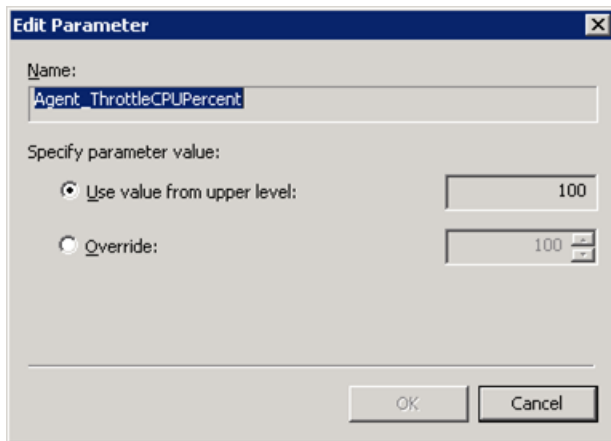
Only some of the parameters have descriptions; when the **Show all** option is disabled, these are the only parameters displayed. With the **Show all** option enabled, undocumented parameters are exposed for troubleshooting purposes; they should be changed only on recommendation from product support.

The organization parameter editor is available in the following locations in InTrust Manager:

Location	Scope of effect
Properties of the root node in InTrust Manager, Parameters tab	All servers and agents in the organization, unless overridden on individual servers and agents
Properties of an InTrust server, Parameters tab	The selected server and all of its agents, unless overridden on individual agents
Properties of an InTrust agent, Parameters tab	The selected agent

Parameter settings defined at the InTrust organization level are inherited by servers and further by agents. However, you can override these settings on the server and agent level.

To edit a parameter, select it in the list and click Edit and use the Edit Parameter dialog box that appears. On the server and agent level, this dialog box lets you override inherited parameter settings.



Tracking Real-Time Event Collection State

The **InTrust\Tools\DumpInTrustConfiguration2csv** folder in your InTrust distribution contains the **RealTimeCollectionStatus.ps1** PowerShell script, which writes out a CSV file with information about the current state of real-time event collection. Analyzing this information can be useful for troubleshooting or optimization of your gathering process. Each environment is unique, so there are no clear-cut interpretations of the data you find in such CSV files. It's up to you what tools you use to analyze the resulting tables, how you make sense of the data and what measures you decide to take.

The script is intended to be run on any of the InTrust servers in the InTrust organization under an account which has at least Read permissions in the InTrust organization.

The following columns are written in default mode:

- CurrentTimeLocal
- ServerName
- ServerVersion
- AgentName
- AgentDomain
- AgentStatus
- AgentVersion
- AgentType
- CollectionName
- RepositoryName
- DataSourceName
- DataSourceStatus
- LastEventTimeGMT

The script supports an optional **-Verbose** parameter, which includes additional columns in the output. The following columns are added in **-Verbose** mode:

- AgentStatusCode
- AgentStatusError
- AgentTypeCode
- AgentID
- RTAgentID
- RepositoryID
- DataSourceID
- DataSourceStatusCode
- DataSourceError

For the full list of available parameters and usage details, see the header of the script in a text editor.

Examples

```
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -NoProfile -NonInteractive  
-file .\RealTimeCollectionStatus.ps1
```

```
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -NoProfile -NonInteractive  
-file .\RealTimeCollectionStatus.ps1 -Verbose
```

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.

Contacting Quest

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

Technical support resources

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

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

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