

Quest® InTrust 11.3.2
Installing Agents Manually



Installing Agents Manually	4
Microsoft Windows Computers	4
Solaris Computers	5
Linux Computers	7
IBM AIX Computers	8
HP-UX Computers	10
Installing Agents Using Group Policy	11
Establishing a Connection with the Server	12
Finding Out the Servers that an Agent Responds to	13
Setting Up Authentication	14
Setting Up Encryption	15
Registering an Agent Alias on the Server	16
About us	17
Contacting Quest	17
Technical support resources	17

© 2018 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 Installing Agents Manually

Updated - June 2018

Version - 11.3.2

Installing Agents Manually

This topic describes the deployment of InTrust agents with native methods on supported platforms. For details about transparent automatic deployment, see [Getting Started with InTrust](#); for details about batch deployment on InTrust sites, see the [Deployment Guide](#).

Microsoft Windows Computers

Agents should be deployed manually under the following (or similar) circumstances:

- The InTrust server and the processed computers are connected by unreliable and slow links. Agent installation fails when the packet drop rate is higher than 5%.
- The processed computers are behind a firewall.

To install an agent manually, run the **ADC_AGENT.*.*.*.msi** installation package from the **DVD\Agent** folder on the InTrust DVD on the target computer.

i **NOTE:** If turned on, User Access Control (UAC) may prevent installation package from running properly. To avoid possible problems, the installation package should be run in an elevated context (use the **Run as Administrator** command).

If the DVD is unavailable, complete the following steps:

1. Log on to the target computer using a local administrator account.
2. Copy all files in the **<InTrust_Server_installation_folder>\Server\ADC\Agent\winnt_x86\redist** folder on the InTrust server to a local folder on the target computer. The agent will be installed to this folder.
3. In the command prompt on the target computer, `cd` to this folder and run the following command:
`adcscm.nt_intel -install`

The agent starts automatically after installation is complete.

To uninstall the agent, use the **Add/Remove Programs** facility. However, if the agent was installed through the command prompt, run the following command on the target computer:

```
adcscm.nt_intel -uninstall
```

i **NOTE:** Installing an agent does not make it usable by the server, but only prepares it (unpacks installation files, starts services, etc.). Please make sure that you establish a connection with the desired server (see [Establishing a Connection with the Server](#)).

Solaris Computers

Agents must always be deployed manually on these computers. To install an agent, complete the following steps:

1. Log in to the target computer under the **root** account. If you log in via telnet, log in using a normal account and then use the **su** command.
2. Copy one of the following agent installation files to a local folder on the target computer:
./adcscm_package.solaris_intel.pkg—for a computer running on the Intel platform
./adcscm_package.solaris_sparc.pkg—for a computer running on the Sparc platform
If you use a protocol with text and binary modes for copying (for example, FTP), make sure the mode is set to binary before the copying starts.
3. Run the following command to install the agent:

```
pkgadd -d Path
```

Replace *Path* with the full path to the agent installation file you copied in Step 2.
4. The system will prompt you for the package to install:
The following packages are available:
1 ADCAgent Quest InTrust Agent
(i386.i86pc) 1.0

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]: 1
Select the Quest InTrust Agent.
5. You will be prompted to supply the path to the directory where the agent will be installed:
Enter path to package base directory [?,q]
Enter the installation path.
6. Then the following prompt will be displayed:
This package contains scripts which will be executed with super-
user permission during the process of installing this package.
Do you want to continue with the installation of <ADCAgent> [y,n,?]
Enter **Y** to start the installation.
7. After the process is complete, the following message will be displayed:
Installation of <ADCAgent> was successful.

Make sure that you have enough disk space for the event cache, which is located in **/var/InTrust** by default. You can change the location by editing the **agent.ini** file located in the directory where you install the agent. If you want to make agent configuration changes, you must complete them before you establish a connection with the InTrust server.

i NOTES:

- Installing an agent does not make it usable by the server, but only prepares it (unpacks installation files, starts services etc.). Please make sure that you establish connection with the desired server (see [Establishing a Connection with the Server](#)).
- Uninstalling the agent does not automatically unregister it from InTrust servers.

Uninstalling the Agent

To uninstall the agent

1. Run the following command on the target computer:

```
./pkgrm ADCAgent
```

2. The following message will be displayed:

```
The following package is currently installed:  
ADCAgent          Quest InTrust Agent  
(i386.i86pc) 1.0
```

```
Do you want to remove this package?
```

Enter **Y** to remove the agent.

3. The system will ask for confirmation:

```
Removing installed package instance <ADCAgent>  
This package contains scripts which will be executed with super-  
user permission during the process of removing this package.
```

```
Do you want to continue with the removal of this package [y,n,?,q]
```

Enter **Y** to confirm.

4. After the process is complete, the following message will be displayed:

```
Removal of <ADCAgent> was successful.
```

Linux Computers

i NOTE:

The agent is a 32-bit application. If you have a 64-bit system, make sure that 32-bit compatibility libraries are installed if you have one of the following 64-bit systems:

- Red Hat Enterprise Linux 7.4, 7.3, 7.2, 7.1, 7, 6.9, 6.8, 6.7, 6.6, 6.5, 6.4, 6.3
- Oracle Linux 7.4, 7.3, 7.2, 7.1, 7, 6.9, 6.8, 6.7, 6.6, 6.5, 6.4, 6.3
- Debian GNU/Linux 8

The required packages on these systems are **glibc.i686** and **libuuid.i686**. Debian requires **libc6:i386** and **libuuid1:i386**.

Agents must always be deployed manually on Linux computers. To install an agent, complete the following steps:

1. Log in to the target computer under the **root** account. If you log in via telnet, log in using a normal account and then use the **su** command.
2. Copy the **adcscm_package.linux_intel.sh** installation script to a local folder on the target computer. If you use a protocol with text and binary modes for copying (for example, FTP), make sure the mode is set to binary before the copying starts.
3. Start the script:

```
./adcscm_package.linux_intel.sh
```

You will be prompted to supply the path to the installation directory.

After the installation, the agent will be started automatically.

Make sure that you have enough disk space for the event cache, which is located in **/var/InTrust** by default. You can change the location by editing the **agent.ini** file located in the directory where you install the agent. If you want to make agent configuration changes, you must complete them before you establish a connection with the InTrust server.

i NOTES:

- Installing an agent does not make it usable by the server, but only prepares it (unpacks installation files, starts services etc.). Please make sure that you establish connection with the desired server (see [Establishing a Connection with the Server](#)).
- Uninstalling the agent does not automatically unregister it from InTrust servers.

Uninstalling the Agent

To uninstall the agent, run the following script from the agent's working directory:

```
./Uninstall.sh
```

IBM AIX Computers

Before you deploy the agent on an AIX host, make sure IBM C++ Runtime Environment Components for AIX (version 8.0 or later) are installed. For instructions on installing these components, see <http://www-1.ibm.com/support/docview.wss?uid=swg21215669>.

Installing an agent does not make it usable by the server, but only prepares it (unpacks installation files, starts services, etc.). Please make sure that you establish a connection with the desired server. When planning where to install the agent, consider that it requires at least 260 megabytes of disk space (280MB recommended).

In addition, make sure that you have enough disk space for the event cache, which is located in `/var/InTrust` by default. You can change the location by editing the `agent.ini` file located in the directory where you install the agent. If you want to make agent configuration changes, you must complete them before you establish a connection with the InTrust server.

i **NOTE:** To diagnose disk space usage, you can use the "Agent-side backup failure" and "Agent-side backup failure resolved" rules. Although these rules monitor all kinds of backup failures, the most common reason for a failure is lack of disk space.

To install an agent

1. Log in to the target computer.
2. Copy the `adcscm_package.aix_ppc.sh` installation script to a local folder on the target computer. This script is located in `<InTrust_installation_folder>/InTrust/Server/ADC/Agent/aix_ppc` on the InTrust server, where it is put during IBM AIX 5L Knowledge Pack setup. If you use a protocol with text and binary modes for copying (for example, FTP), make sure the mode is set to binary before the copying starts.
3. Start the script:

```
./adcscm_package.aix_ppc.sh
```

You will be prompted to supply the path to the installation directory.
4. The script prompts you whether you want to configure system audit so that the InTrust agent can capture Audit log events. If you answer **y**, the following changes will be made to the `/etc/security/audit/config` file:
 - In the **start** stanza of the file, the **streammode** option will be set to **on**.
 - In the **stream** stanza, the **cmds** option will be set to the `<agent_installation_directory>/InTrustStreamCmds` file.A backup copy of the original `/etc/security/audit/config` file will be saved to the `/etc/security/audit/config_intrust_backup` file.
5. Restart system audit.

After the installation, the agent will be started automatically.

i **NOTE:** There is another way to specify the path to an installation directory. Supply the location right in the command line. For example:

```
./adcscm_package.aix_ppc.sh /opt/InTrustAgent
```

In this case the agent will be installed in `/opt/InTrustAgent`.

Uninstalling the Agent

To uninstall an agent from the AIX computer

1. Run the following script from the agent's working directory:
`./Uninstall.sh`
2. Restore the settings in the **start** and **stream** stanzas of the `/etc/security/audit/config` file to the state they were in before the InTrust agent installation. For that, use the backup stored in the `/etc/security/audit/config_intrust_backup` file.
3. Restart system audit.

Uninstalling the agent does not automatically unregister it from InTrust servers. So, you should manually disconnect the agent from each InTrust server it communicates with.

HP-UX Computers

When planning where to install the agent, consider that it requires at least 260 megabytes of disk space (280MB recommended).

In addition, make sure that you have enough disk space for the event cache, which is located in **/var/InTrust** by default. You can change the location by editing the **agent.ini** file located in the directory where you install the agent. If you want to make agent configuration changes, you must complete them before you establish a connection with the InTrust server.

To install the agent, complete the following steps:

1. Log in to the target computer.
2. Copy the **adcscm_package.hpux_parisc.depot** package to a local folder on the target computer. This file is located in **<InTrust_installation_folder>\InTrust\Server\ADC\Agent\hpux_parisc** on the InTrust server, where it is put during HP-UX Knowledge Pack setup. If you use a protocol with text and binary modes for copying (for example, FTP), make sure the mode is set to binary before the copying starts.
3. Start SAM, and use the **Software Management | Install Software to Local Host** item to set up the agent.

The default installation directory is **/usr/local/ADC**.

After the installation, the agent will be started automatically.

Uninstalling the Agent

To uninstall the agent from the HP-UX computer, use the **Software Management | Remove Local Host Software item in SAM**. The name of the package is **ADCAgent**.

i NOTES:

- Installing an agent does not make it usable by the server, but only prepares it (unpacks installation files, starts services etc.). Please make sure that you establish connection with the desired server (see [Establishing a Connection with the Server](#)).
- Uninstalling the agent does not automatically unregister it from InTrust servers.
- To diagnose disk space usage, you can use the "Agent-side backup failure" and "Agent-side backup failure resolved" rules. Although these rules monitor all kinds of backup failures, the most common reason for a failure is lack of disk space.

Installing Agents Using Group Policy

You can automate the installation of agents using Group Policy settings. InTrust is shipped with a Windows Installer file containing the agent package.

To automatically install agents on specific computers, take the following steps:

1. Copy the agent package from the **Agent** folder in the InTrust distribution to a share available to all those computers.
2. In the Active Directory Users and Computers MMC snap-in, create an OU that includes all of the required computers and add a Group Policy object for this OU.
3. Using the Group Policy Object Editor MMC snap-in, in Computer Settings, assign the agent package to the Group Policy object you added earlier.
4. To make InTrust process these computers with agents, make sure the computers are included in InTrust sites.

Establishing a Connection with the Server

To establish a connection between an agent and an InTrust server, you should log on to the computer where the agent is installed using an administrative account (Microsoft Windows computers) or the **root** account (Unix computers) and run one of the following commands:

```
adcscm.nt_intel -add ServerName Port [password]
```

for Microsoft Windows computers

```
./adcscm -add ServerName Port [password]
```

for Unix computers

where:

- **ServerName** specifies the InTrust Server to which you bind the agent. This may be either the NetBIOS name, FQDN, or IP address.
- **Port** specifies the port number at which the server listens to the requests coming from the agent (that is the same as the listening port you specified for InTrust server during setup); the default port number is 900.
- **Password** is the password for initial agent-server authentication; it is required if the **Use authentication** option is enabled on the InTrust server (see [Setting Up Authentication](#)). By default this password is the same as the organization password supplied during InTrust Server installation (you can change the agent installation password in InTrust server properties). If you want to use an empty password, supply empty quotation marks (""). If authentication is disabled on the InTrust server, do not specify any password.

To disconnect the agent from the InTrust server, on the target computer run:

```
adcscm.nt_intel -remove ServerName Port
```

for Microsoft Windows computers

```
./adcscm -remove ServerName Port
```

for Unix computers

Finding Out the Servers that an Agent Responds to

To find out which InTrust server or servers an agent responds to, log on to the computer where the agent is installed using an administrative account (Microsoft Windows computers) or the **root** account (Unix computers) and run one of the following commands:

```
adcscm.nt_intel -list
```

for Microsoft Windows computers

```
./adcscm -list
```

for Unix computers

The output should look similar to the following:

```
Name: 10.30.39.254
Port: 900
Name: s8050-w2k3.testorg.local
Port: 900
Name: gz.testorg.local
Port: 900
Name: 10.30.46.108
Port: 900
```

on Microsoft Windows computers

```
Name: 10.30.37.49
Port: 900
Name: 10.30.37.128
Port: 900
```

on Unix computers

Setting Up Authentication

The authentication process is two-sided (both server-side and agent-side) and based on the Secure Remote Password (SRP) protocol. In addition to authenticating clients to the server securely, the SRP exchanges a cryptographically-strong symmetric key as a byproduct of successful authentication, which enables the two parties to communicate steadily. After initial authentication is successfully performed, the authentication password will automatically be changed every week to secure communication between server and agents. The symmetric key is changed every hour.

For manually installed agents, you first have to specify the password on the server. By default, this is the organization password you specified during setup. The authentication mechanism will use this password only when establishing connection for the first time; then this password will be changed regularly.

If you want to use a password other than the default, take the following steps:

1. In **Quest InTrust Manager | Configuration | Servers**, right-click the server name and select **Properties**.
2. On the Agent tab, select **Use authentication** and supply a new password for initial authentication.
3. Now provide this password to the agent. For that, on the target computer, run:

```
adcscm.nt_intel -add ServerName Port Password
```

for Microsoft Windows computers

```
./adcscm -add ServerName Port Password
```

for Unix computers

Replace *Password* with the password that you specified in Step 2.

Setting Up Encryption

You can select to encrypt data communicated between the agent and the server (encryption uses 3DES with a 168-bit key). By default, encryption is enabled.

To enable or disable encryption manually

1. In **Quest InTrust Manager | Configuration | Servers**, right-click the server name and select **Properties**.
2. On the **Agent** tab, select or clear the **Use encryption** check box.
3. Click **Apply** and close the dialog box.

Registering an Agent Alias on the Server

After the connection is established, you can register the agent access name (alias) that the server will use to communicate with the agent. On the computer where the agent is installed, run:

```
adcscm.nt_intel -register ServerName Port Alias
```

for Microsoft Windows computers

```
./adcscm -register ServerName Port Alias
```

for Unix computers

Replace **Alias** with the agent name to be used by the server for communication with the agent.

i | **NOTE:** Agent names must be unique within the scope of an InTrust server.

If you want to change the alias, first run the following command on the computer where the agent resides:

```
adcscm.nt_intel -unregister ServerName Port Alias
```

for Microsoft Windows computers

```
./adcscm -unregister ServerName Port Alias
```

for Unix computers where **Alias** is the current agent name, and then register the new name as described above.

You can view agent names and aliases in an agent's properties dialog box in InTrust Manager.

About us

We are more than just a name

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

Our brand, our vision. Together.

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

Contacting Quest

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

Technical support resources

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

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

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