Quest® InTrust 11.5.1

Installing Agents Manually

Contents

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 - November 2022
Version - 11.5.1

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.

We need to follow below steps for Manual Upgrade of Agent

1. Do not select "**Establish connection with InTrust Server**" during Agent MSI Installation.
2. After Agent upgrade, register server from the agent machine, by running the register command without password:
   - for Microsoft Windows computers - `adcscm.nt_intel -add ServerName Port`
   - for Unix computers - `./adcscm -add ServerName Port`

   It is recommended to uninstall all the old version of servers and agents for using the latest version to ensure successful authentication and communication between agents/servers.
   a. Do not select "Establish connection with InTrust Server" during Agent MSI Installation.
   b. After latest Agent installation, register server from the agent machine, by running the register command without password:
      a. for Microsoft Windows computers- adcscm.nt_intel-add ServerName Port
      b. for Unix computers- ./adcscm-add ServerName Port

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.

> **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
```

> **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).

Linux Computers

NOTE:

The agent is a 32-bit application. If you have a 64-bit system, make sure that 32-bit compatibility libraries are installed.

The required packages are **glibc.i686** and **libuuid.i686**. Debian and Ubuntu require **libc6:i386** and **libuuid1:i386**.

On Red Hat Enterprise Linux 8 and Oracle Linux 8, the **libnsl.i686** library must also be installed.

The way to enable support for the 32-bit architecture on Linux varies from distribution to distribution. For example, in Ubuntu this can be achieved with the following commands (as root):

```
dpkg --add-architecture i386
```

```
apt-get update
```

Finally, to install the libraries, you can use the following:

```
apt-get install libc6:i386 libuuid1:i386
```

Refer to your distribution's documentation if you need details.

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.

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
```

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 can be 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 Diffie-Hellman (DH) protocol. In addition to authenticating clients to the server securely, the DH 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.

NOTES:

- We have updated the Server and agents to use DH algorithm for the authentication in 11.5. Hence if we are adding 11.5 server in existing organization with agents and server with 11.4 or below, the communication and authentication cannot succeed. It is recommended to uninstall all the old servers and agents to use 11.5 for successful authentication and communication between agents/servers.
- As a workaround, the agent-server communication and authentication can be disabled so that the collection and communication can be continued between agent-server.
- In 11.5, first collection will take some time to communicate between agent and server.

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.

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

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