ivanti

linuxac

Ivanti Application Control for Linux

Installation Guide

Version 2021.3

Copyright Notice

Contents

About Ivanti Application Control for Linux

Ivanti Application Control for Linux is a new addition to the powerful Ivanti User Workspace Manager solution. It enables Windows Administrators to create and deploy allow and deny lists to Linux machines in their environment.

Additional information is provided in the *Ivanti Application Control for Linux Utilization Guide* supplied with the software download media or available from the Ivanti Help web portal.

Target Audience

This guide is intended for existing administrators of Ivanti Application Control. It describes the process for the installation and essential configuration of the Linux environment.

Installation Overview

1. **Prerequisites**

   Administrators must ensure the essential prerequisites are in place before starting the installation process.

2. **Install Windows Server**

3. **Install Linux Endpoints**

4. **Uninstall**

   Should you need to interrupt the installation to start again, refresh an older installation, or remove unwanted files refer to Uninstall.

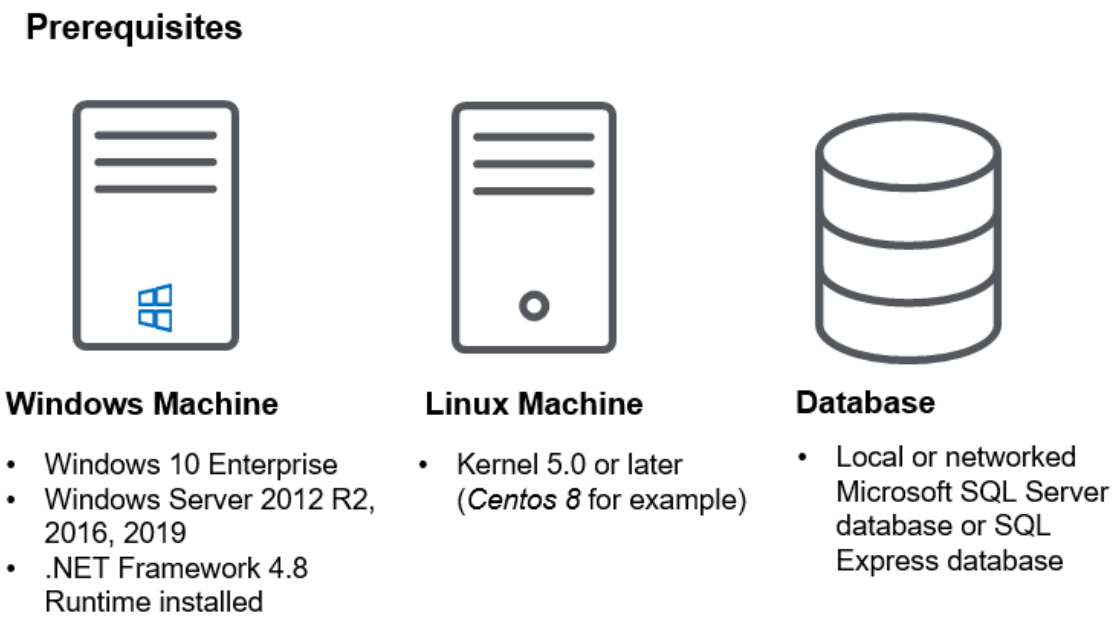
5. **Troubleshooting**

   For information on system upgrades and any known issues, refer to Troubleshooting.

Prerequisites

Essential prerequisites for the installation and configuration of Ivanti Application Control for Linux (2021.3 version) are described below.

Note, where a release version of third-party software is specified, this should be seen as a minimum.



Windows Server Machine

Operating System

- Windows 10 Enterprise edition
- Windows Server 2012 R2, Windows Server 2016, Windows Server 2019

Note, it is strongly recommended that a restore point is created in your Windows 10 Enterprise machine.

.NET Framework

- .NET Framework 4.8 Runtime must be available on the Windows server machine prior to the installation of Application Control for Linux.

Database

A local or networked SQL database must be available before the installation of Application Control for Linux:

- Microsoft® SQL Server® 2017 Express (or later), or a full license for SQL Server (2016, 2017 or 2019).

Cleanup of any previously installed Application Control for Linux SQL Server instance is required. Ensure that any pre-release version of *AcDatabase* is manually deleted before starting a new installation.

Linux Endpoints

Operating System

- Supported distros with a Linux 5.x kernel
- Red Hat Enterprise Linux 8.x, Oracle Linux 8.x, CentOS 8.x

It is strongly recommended that backups of Linux endpoint machines are generated.

Install Windows Server

Ensure prerequisites are in place before you begin the installation

1. Run *IvantiAcServerMasterInstaller.exe* – this will install the Windows server solution and the Mosquitto MQTT broker on your machine.
2. At the SQL Database Connection Validation step, input your Connection String in the respective text box (some examples are provided by the installer itself).

   If the connection string is incorrect or incompletely formatted the system will not perform as expected. In some cases, you will be unable to continue with the installation.

   Example (note the use of required double semicolons):

   ```
   Data Source=<server_name>\<instance_name>;;Trusted_Connection=True
   ```

3. After the installer has finished, you will need to configure your active firewall to ensure it allows connections on some of the important, default-configured ports:
   - **8883** – MQTT over SSL communication (Mosquitto Broker).
   - **3123** – AFS over SSL communication (Application Control (AC) Server, Application Framework (AF) Server and AC Agent).
   - **5001** – Self-hosted user interface over SSL communication (AC for Linux Web Console).
4. The passphrase is used as a command parameter on your Linux endpoint and will be required to register the Application Control for Linux Engine securely with the Windows server.

Note: The installer automatically generates the security certificates required for Mosquitto Broker communication. Certificates are created with the predefined passphrase ***TestReg*** and this must be noted for use later.

The Linux endpoint command parameter is identified as <*your_certificates_passphrase*>. You will need to replace this value with `TestReg`.

For any troubleshooting of the Mosquitto installation refer to the relevant section in Troubleshooting.

Note, you will now have Ivanti AC Server and Ivanti AF Server as two separate shortcuts present in your Windows Start menu.

5. As an Administrator, run the *Ivanti AC Server* executable.

   - The console will start.
   - On first execution the database (AcDatabase) is created.
     Note that a clean install is recommended. If you do upgrade from a previous release the AcDatabase will automatically be updated to the latest schema.
   - If you encounter any exceptions or errors after starting up, refer to the relevant section in Troubleshooting.

6. As an Administrator, run the *Ivanti AF Server* executable.

   - The console will start.
   - If you encounter any exceptions or errors after starting up, refer to the relevant section in Troubleshooting.

7. In your browser, enter the following:

   ```
   https://<yourcomputername>:5001/home
   ```

   The self-hosted Application Control for Linux web console is displayed.

Install Linux Endpoint

Ensure prerequisites are in place before you begin the installation and that Linux endpoint machines are up-to-date.
Note, in Linux all file names are case-sensitive.

1. Transfer the generated security certificate CA.pem file from your Windows machine to your preferred directory on your Linux endpoint by performing a reverse SCP.

   On your Windows server, launch a new command prompt as an Administrator and execute the following commands:

   ```
   cd "C:\Program Files\Ivanti\ACServer\Certificates"
   scp CA.pem root@ip_of_your_linux_endpoint:<path_to_CA.pem>
   ```

2. The Linux installers need to be copied to the Linux device(s). To do this, copy the .tar files from the download media to the Windows server. Adapt the following commands to then copy these files to the Linux machine(s).

   ```
   scp ivanti-ac-agent.tar <root@ip_of_your_linux_endpoint>:/home/<users home folder>/
   scp ivanti-ac-engine.tar <root@ip_of_your_linux_endpoint>:/home/<users home folder>/
   ```

3. On your Linux endpoint, un-TAR (extract) the package files, using the following commands:

   ```
   sudo tar -xvf ivanti-ac-agent.tar
   sudo tar -xvf ivanti-ac-engine.tar
   ```

4. Install the extracted RPM packages.
   Adapt the following YUM commands with the required file and platform version:

   ```
   sudo yum install ivanti-ac-agent-<file_version&platforms>.rpm
   sudo yum install ivanti-ac-engine-<file_version&platforms>.rpm
   ```

5. Verify the relevant locations for each of the installed products:

   - AC for Linux Engine location (contains the engine executable):

   ```
   ls -la /opt/ivanti/ac/engines/ivanti-ac-engine-<distro_name>/bin
   ```

     where <distro_name> can be: "centos-8", or "oracle-8", or "redhat-8", quotes excluded.

   - AC for Linux Engine Policy location (contains the latest policy deployed):

```
ls -la /opt/ivanti/ac/engines/ivanti-ac-engine-<distro_name>/policy/policy.xml
```

where <distro_name> can be: "centos-8", or "oracle-8", or "redhat-8", quotes excluded.

- AC for Linux Engine Logs location (contains all the engine business logs):

```
ls -la /opt/ivanti/ac/engines/ivanti-ac-engine-<distro_name>/logs
```

where <distro_name> can be: "centos-8", or "oracle-8", or "redhat-8", quotes excluded.

- AC for Linux Agent location (contains all the agent executables)

```
ls -la /opt/ivanti/ac/bin
```

6. The command below will open the "hosts" file for editing:

```
sudo nano /etc/hosts
```

Ensure the short name of your Windows server is present in your Linux endpoint "hosts" file - not the FQDN (Fully Qualified Domain Name).

In the hosts file ensure you have a line at the end of the file with the IP address and short name of the Windows server.
For example:

```
10.192.14.32 WIN-2018-325-UK
```

Having saved the "hosts" file you can then ping the device name of your Windows server to ensure the update has been successful.

7. Register the Linux endpoint agent with the Windows server.
Note that your security certificate passphrase is required for this step, refer to Install Windows Server for further information.

```
sudo ./stagentctl register --host <windows_server_hostname> --port 3123 --passphrase <your_certificates_passphrase> --selected-policy AcPolicy --issuer-certificate <path_to_CA.pem>
```

8. Verify Linux endpoint agent daemon status using the following command:

```
sudo systemctl status ivanti-ac-agent
```

9. Enable the Linux Endpoint engine daemon using the following command:

```
sudo systemctl enable ivanti-ac-engine
```

10. Start the Linux Endpoint engine daemon using the following command:

```
sudo systemctl start ivanti-ac-engine
```

11. Verify Linux Endpoint engine daemon status using the following command:

```
sudo systemctl status ivanti-ac-engine
```

12. Open the Ivanti Application Control for Linux web console on the Windows server. Navigate to the Devices menu item, and refresh the page to ensure that the Linux device(s) appear in the list.

Uninstall

This section describes how to uninstall and cleanup your files.

Windows Server

1. Uninstall the Ivanti Application Control for Linux Server from your Windows server. This removes Ivanti Application Control for Linux files and the security certificates automatically generated and configured on your Windows server by the installer.
2. If you have installed any pre-release version of Application Control for Linux you must cleanup your SQL Server instance by manually deleting the *AcDatabase*.
3. Optional step - manually uninstall Eclipse Mosquitto from your Windows server. It is recommended you also check your Program Files directory for any remaining Mosquitto folders and delete them as required.

Before uninstalling any files ensure the Mosquitto MQTT Broker Windows service is stopped, and the Services window is closed.
An Eclipse Mosquitto bug exists and requires this as a workaround.

Linux Endpoint

1. Find the package names on your Linux endpoint. The following command will return the names required

   ```
   rpm -qa | grep -i "ivanti*"
   ```

   Example output:

   ```
   ivanti-ac-engine-0.1-1.x86_64
   ivanti-ac-agent-1.1-1.x86_64
   ```

2. Remove found packages.
   Adapt the following commands with the package name values identified:

   ```
   sudo yum remove -y <ivanti-ac-agent_package_name>
   ```

   Example package_name: `"ivanti-ac-agent-1.1-1.x86_64"`, quotes excluded.

Optional: if your Linux system cannot resolve Agent to Engine dependency, and does not automatically offer Engine removal, also perform this step:

```
sudo yum remove -y <ivanti-ac-engine_package_name>
```

Example package_name: "`ivanti-ac-engine-0.1-1.x86_64`", quotes excluded.

Installation Troubleshooting

Basic troubleshooting help is provided in this section. Additional information is provided in the *Ivanti Application Control for Linux Utilization Guide* supplied with the software download media or available from the Ivanti Help web portal.

Windows Server

If you encounter issues and need to reinstall the Windows server solution it is strongly recommended you do this with logging explicitly activated, in case the original installation provided no default logs.

1. Edit the command example below with the required path for your log files and run the Windows server installer:

   ```
   IvantiAcServerMasterInstaller.exe -l "<path to where you want the log file.txt>"
   ```

2. Refer also to the Maintenance section of the *Ivanti Application Control for Linux Utilization Guide*.

Mosquitto – Extra Steps

In addition to the guidance suggested here, you may wish to refer to Mosquitto.org documentation.

1. The Mosquitto broker currently installed with Application Control for Linux requires Visual C++ Redistributable Packages for Visual Studio 2015. The package can be downloaded from Microsoft .com.

   Note that if your Windows machine is not up-to-date, this dependency may fail requiring a reinstall of the AcServerBundle.exe onto an updated machine.

2. To ensure the Mosquitto broker is running currectly, you can use an external tool to verify this such as *MQTT.fx* .
   Note that older versions of this software are freely available from the original developer's website, or refer to www.softblade.de for licensing and free trial downloads.

   - Install MQTT.fx, open it, and establish a connection to your local Mosquitto profile.
   - You can now test publishing and subscribing to data on your local Mosquitto broker installation.

3. As a debug option, you can also verify the Mosquitto configuration file is correctly setup, make changes if required, and then restart Mosquitto using the modified version.
   The action requires the following steps:

   - Stop any running Mosquitto broker.
   - View the content of the Mosquitto configuration file. If required, edit the file to match the following:

```
#
# Logging Settings
#
log_dest file C:\Program Files\mosquitto\mosquitto.log
log_type all
log_timestamp true
log_timestamp_format %Y-%m-%dT%H:%M:%S
connection_messages true
#
# TLS Settings
#
#NOTE port 8883 is for TLS
port 8883
capath C:\Program Files\mosquitto\
certfile C:\Program Files\mosquitto\server.crt
keyfile C:\Program Files\mosquitto\server.key
#tls_version tlsv1.1
#
# Authentication Settings
#
auth_plugin C:\Program Files\mosquitto\MosquittoAuth.dll
auth_opt_StsUri https://BDARROW19:3123/st/console/token
auth_opt_StsReloadPeriod 30
allow_anonymous true
```

- Start the Mosquitto Broker using the modified configuration file.
  From a command prompt session with Administrator privileges, enter:

```
mosquitto -c mosquitto.conf -v
```

4. If *MosquittoAuth.dll* fails to install correctly in the Mosquitto broker installation folder the installation must be uninstalled, cleanup performed and the process restarted.
   The default location for the MosquittoAuth.dll is C:\Program Files\Mosquitto.
   Refer to Uninstall for further information.

Linux Endpoint

Refer also to the Maintenance section of the *Ivanti Application Control for Linux Utilization Guide*.

Prerequisites – Upgrade from Kernel 4 to Kernel 5

The steps below summarize how to upgrade a Linux kernel from 4.x to 5 and apply to CentOS 8. Depending upon your current version of Linux and your specific upgrade path you may have to resolve system and other application dependencies. For more detailed upgrade specific information refer to your Linux provider's website.

- From a Command Prompt session with Administrator privileges enter the following commands:

```
:~$ su
:~# sudo rpm --import https://www.elrepo.org/RPM-GPG-KEY-elrepo.org
```

- Add the repository by installing an RPM package:

```
:~# sudo dnf install https://www.elrepo.org/elrepo-release-8.0-2.el8.elrepo.noarch.rpm
```

- Check the repository was successfully added:

```
:~# sudo dnf repolist
```

- Check the installed version is as expected:

```
:~# sudo uname -r
```

- Install the new kernel:

```
:~# sudo dnf --enablerepo=elrepo-kernel install kernel-ml
```

- Reboot the Linux machine - ensure you boot on Kernel 5.xxx:

```
:~# sudo uname -r
```

The current Linux kernel is displayed.