

Was this helpful?  

# Installation guide

## ON THIS PAGE

### ▸ Installation guide

About ForgeRock Identity Platform™ software

### ▸ Prepare for installation

Before you install

Download and unzip Java Agent

Preinstallation tasks

Configure communication with AM servers

Create agent profiles

Create agent administrators for a realm

### ▸ Install Java Agent

Install Tomcat Java Agent

Install JBoss Java Agent

Install Jetty Java Agent

Install WebLogic Java Agent

Install WebSphere Java Agent

### ▸ Post-installation tasks

Review directories for configuration, logs, and POST data.

Configure the agent filter for a web application

Configure the agent filter mode

Secure communication between the agent and AM

Upgrade Java Agent

### ▸ Remove Java Agent

Remove Tomcat Java Agent

Remove JBoss Java Agent

Remove Jetty Java Agent

Remove WebLogic Java Agent

Remove WebSphere Java Agent

▸ agentadmin command

--install

--forceInstall

--custom-install, --custom

--uninstall, -r

--version, -v

--uninstallAll

--listAgents, --list, -l

--agentInfo, --info

--encrypt

--getEncryptKey, --getKey

--key

--d, -d, --decryptAgent, --decrypt


--decryptPassword

## Installation guide

---

This guide describes how to install ForgeRock Access Management Java Agent.

### About ForgeRock Identity Platform™ software

ForgeRock Identity Platform serves as the basis for our simple and comprehensive Identity and Access Management solution. For more information, visit <https://www.pingidentity.com> .

## Prepare for installation

---

### Before you install

Consider the following points before you install:

- Install AM and Java Agent in different containers

- Install the container before you install the agent.
- Install only one Java Agent for each container, and configure as many agent instances as necessary.
- Install a supported version of the Java runtime environment, as described in the [Release notes](#). Set the `JAVA_HOME` environment variable accordingly. The agent installer requires Java.

```
$ echo $JAVA_HOME
/path/to/java
```

- For environments with load balancers or reverse proxies, consider the communication between the agent and the AM servers, and between the agent and the client. Configure both AM and the environment **before** you install the agent. For more information, see [Configure load balancers and reverse proxies](#).

## Download and unzip Java Agent

Go to the [ForgeRock BackStage download site](#) and download an agent based on your architecture, and operating system requirements. Verify the checksum of the downloaded file against the checksum posted on the download page.

Unzip the file in the directory where you plan to store the agent configuration and log files. The following directories are extracted:

| Directory      | Description  |
|----------------|--|
| bin            | The <b>agentadmin</b> installation and configuration program. For more information, see <a href="#">agentadmin command</a> . |
| config         | Configuration templates used by the <b>agentadmin</b> command during installation  |
| data           | Not used   |
| etc            | Configuration templates used during installation   |
| installer-logs | Location of log files written during installation  |
| legal-notice   | Licensing information including third-party licenses   |
| lib            | Shared libraries used by the agent   |
| locale         | Property files used by the installation program  |
| README         | README file containing platform and install information for the agent  |

## Preinstallation tasks

1. Create a text file for the agent password, and protect it. For example, use commands similar to these, changing the password value and path:

**Unix**

**Windows**

```
$ cat > /tmp/pwd.txt  
password  
CTRL+D  
  
$ chmod 400 /tmp/pwd.txt
```

### TIP

Although the agent accepts any password length and content, you are strongly encouraged to generate secure passwords. This can be achieved in various ways, for example using a password manager or by using the command line tool `agentadmin --key`.

2. In AM, add an agent profile, as described in [Create agent profiles](#):

The examples in this guide use an agent profile in the top-level realm, with the following values:

- **Agent ID:** java-agent
- **Agent URL:** `http://agent.example.com:80/app`
- **Server URL:** `http://openam.example.com:8080/openam`
- **Password:** password

3. In AM, add a policy set and policy, to protect resources with the agent, as described in [Configuring policies](#) in AM's *Authorization guide*.

The examples in this guide use a policy set and policy in the top-level realm, with the following values:

- Policy set:
  - **Name:** PEP
  - **Resource Types:** URL
- Policy:
  - **Name:** PEP-policy
  - **Resource Type:** URL

- **Resource pattern:** `*:/*:*/*`
- **Resource value:** `*:/*:*/*`
- **Actions tab:** Allow HTTP GET and POST
- **Subjects tab:** All Authenticated Users.

When you create your own policy set instead of using the default policy set, `iPlanetAMWebAgentService`, update the following properties in the agent profile:

- [Policy Set Map](#)
- [Policy Evaluation Realm Map](#)

4. When you exchange **signed** OpenID Connect JWTs between AM and the agent, set up a new key and secret as described in [Configure Communication With AM Servers](#). Do not use the default `test` key pair in a real environment.

## Configure communication with AM servers

AM communicates authentication and authorization information to Java Agent by using OpenID Connect (OIDC) JSON web tokens (JWT). To secure the JSON payload, AM and the agent support JWT signing with the RS256 algorithm. For more information, see [RFC 7518](#).

AM uses an HMAC signing key to protect requested ACR claims values between sending the user to the authentication endpoint, and returning from successful authentication.

By default, AM uses a demo key and an autogenerated secret for these purposes. For production environments, perform the steps in the following procedure to create new key aliases and configure them in AM.

### *Configure AM secret IDs for the agents' OAuth 2.0 provider*

By default, AM 6.5 and later versions are configured to:

- Sign JWTs with the secret mapped to the `am.global.services.oauth2.oidc.agent.idtoken.signing` secret ID. This secret ID defaults to the `rsajwt signingkey` key alias provided in AM's JCEKS keystore.
- Sign claims with the secret mapped to the `am.services.oauth2.jwt.authenticity.signing` secret ID. This secret ID defaults to the `hmacsigningtest` key alias available in AM's JCEKS keystore.

For more information about secret stores, see [Configuring secret stores](#) in AM's *Security guide*.

1. Create the following aliases in one of the secret stores configured in AM, for example, the default JCEKS keystore:
  - RSA key pair
  - HMAC secret
2. In the AM console, select **Configure** > **Secret Stores** > **Keystore Secret Store Name** > **Mappings**, and configure the following secret IDs:
  - The new RSA key alias in the `am.global.services.oauth2.oidc.agent.idtoken.signing` secret ID.
  - The new HMAC secret in the `am.services.oauth2.jwt.authenticity.signing` secret ID.

You might already have a secret configured for this secret ID, because it is also used for signing certain OpenID Connect ID tokens and remote consent requests. For more information, see [Secret ID default mappings](#) in AM's *Security guide*.

3. Save your changes.

## Create agent profiles

Java Agent requires a profile to connect to and communicate with AM, regardless of whether the agent is in [remote configuration mode](#) or [local configuration mode](#).

This section describes how to create an agent profile and inherit properties from a group. Alternatively, create agent profiles by using the `/realm-config/agents/WebAgent/{id}` endpoint in the REST API.

For more information, see [API Explorer](#) in your AM instance.

### Create an agent profile in the AM console

1. In the AM console, select **Realms** > **realm name** > **Applications** > **Agents** > **Java**, and add an agent using the following hints:

#### **Agent ID**

The ID of the agent profile. This ID resembles a username in AM, and is used during the agent installation. For example, `MyAgent`.

#### **TIP**

When AM is not available, the related error message contains the agent profile name. Consider this in your choice of agent profile name.

### **Agent URL**

The URL where the agent resides, for example, `http://agent.example.com:80/app`. When the agent is in remote configuration mode, the Agent URL is used to populate the agent profile for services, such as notifications.

### **Server URL**

The full URL to an AM instance. If AM is deployed in a site configuration (behind a load balancer), enter the site URL. When the agent is in remote configuration mode, the Server URL is used to populate the agent profile for use with as login, logout, naming, and cross-domain SSO.

### **Password**

The password the agent uses to authenticate to AM. Use this password when installing an agent.

#### **TIP**

Although the agent accepts any password length and content, you are strongly encouraged to generate secure passwords. This can be achieved in various ways, for example using a password manager or by using the command line tool `agentadmin --key`.

## **Create an agent profile with the `ssoadm` command line tool**

For information about how to use `ssoadm` and properties with multiple aliases, see [Property aliases](#).

For more information about `ssoadm`, see [ssoadm](#) in AM's *Reference*.

1. Set up `ssoadm`, as described in AM's [Setting up administration tools](#) in AM's *Installation*.
2. Create a text file for the agent password, and protect it. For example, use commands similar to these, changing the password value and path:

**Unix**

**Windows**

```
$ cat > /tmp/pwd.txt
password
CTRL+D

$ chmod 400 /tmp/pwd.txt
```

Although the agent accepts any password length and content, you are strongly encouraged to generate secure passwords. This can be achieved in various ways, for example using a password manager or by using the command line tool `agentadmin --key`.

3. Run the `an ssoadm` command similar to this to create the agent:

```
./ssoadm create-agent \  
--agentname java-agent \  
--agenttype J2EEAgent \  
--password-file /tmp/pwd.txt \  
--realm / \  
--agenturl http://agent.example.com:80/app \  
--serverurl http://am.example.com:8080/am \  
--adminid uid=amadmin,ou=People,dc=am,dc=myorg,dc=org \  
--attributevalues userpassword=password
```

Agent configuration was created.

4. (Optional) Configure additional properties for the agent, by adding them to the `--attributevalues` option.

Add the following line to the above example to configure a value for Max Entries in Not-Enforced IP Cache:





```
--attributevalues  
com.sun.identity.agents.config.notenforced.ip.cache.size=2  
000
```

## Create an agent profile group and inherit settings

Use agent profile groups to set up multiple agents that inherit settings from the group.

1. In the AM console, select **Realms** > **realm name** > **Applications** > **Agents** > **Java**.
2. In the **Group** tab, add a group. Use the URL to the AM server in which to store the profile.
3. Edit the group configuration as necessary, and save the configuration.
4. Select **Realms** > **realm name** > **Applications** > **Agents** > **Java**, and select an agent you created previously.



5. In the **Global** tab, select **Group**, and add the agent to the group you created previously. The icon  appears next to some properties.
6. For each property where  appears, toggle the icon to set inheritance:
  -  Do not inherit the value from the group.
  -  Inherit the value from the group.

## Create agent administrators for a realm

To create agent profiles when installing Java Agent, you need the credentials of an AM user who can read and write agent profiles.

This section describes how to create an agent administrator for a specific realm. Use this procedure to reduce the scope given to users who create agent profiles.

1. In the AM console, select **Realms** > **realm name** > **Identities**.
2. In the **Groups** tab, add a group for agent administrators.
3. In the **Privileges** tab, enable **Log Read** and **Log Write**.
4. Return to **Realms** > **realm name** > **Identities**, add agent administrator identities.
5. For each identity, select the **Groups** tab, add the user to agent profile administrator group.
6. Provide each system administrator who installs agents with their agent administrator credentials.

When installing the agent with the `--custom-install` option, the system administrator can choose the option to create the profile during installation, and then provide the agent administrator user name and the path to a read-only file containing the agent administrator password. For silent installs, you can add the `--acceptLicense` option to auto-accept the software license agreement.

## Install Java Agent

### Install Tomcat Java Agent

Before you install, make sure that all Tomcat scripts are present in the `$CATALINA_HOME/bin` directory. The Tomcat Windows executable installer does not include the scripts. If the scripts are not present in your installation, copy the contents of

the bin directory from a .zip download of Tomcat of the same version as the one you installed.

## *Install Tomcat Java Agent interactively*

1. Review the information in [Before you install](#), and perform the steps in [Preinstallation tasks](#).
2. Shut down the Tomcat server where you plan to install the agent.
3. Make sure AM is running.
4. Run **agentadmin --install** to install the agent:

```
$ /path/to/java_agents/tomcat_agent/bin/agentadmin --install
```

You are prompted to read and accept the software license agreement for the agent installation. Use the [--acceptLicense](#) option to skip the prompt.

5. When prompted, enter information for your deployment.

### TIP

To cancel the installation at any time, press CTRL+C .

- a. Enter the complete path to the Tomcat configuration folder:

```
Enter the complete path to the directory which is used by Tomcat Server to store its configuration Files. This directory uniquely identifies the Tomcat Server instance that is secured by this Agent.
```

```
[ ? : Help, ! : Exit ]
```

```
Enter the Tomcat Server Config Directory Path
```

```
[ /opt/apache-tomcat/conf ]: /path/to/apache-tomcat/conf
```

- a. Enter the AM URL:

```
Enter the URL where the AM server is running. Please include the deployment URI also as shown below:
```

```
(http://openam.sample.com:58080/openam)
```

```
[ ? : Help, < : Back, ! : Exit ]
```

```
AM server URL: https://openam.example.com:8443/openam
```

To load balance connections between the agent and an AM site, enter the URL of the load balancer in front of the AM site.

If a reverse proxy is configured between AM and the agent, enter the proxy URL. For more information, see [Configure an Apache HTTP Server as a reverse proxy](#).

- b. Enter the `$CATALINA_HOME` environment variable, specifying the path to the root of the Tomcat server:

```
$CATALINA_HOME environment variable is the root of the
tomcat
installation.
[ ? : Help, < : Back, ! : Exit ]
Enter the $CATALINA_HOME environment variable:
/path/to/apache-tomcat
```

- c. Enter the agent URL:

```
Enter the Agent URL. Please include the deployment URI
also as shown below:
(http://agent1.sample.com:1234/agentapp)
[ ? : Help, < : Back, ! : Exit ]
Agent URL: \http://agent.example.com:80/app
```

- d. Enter the name of the agent profile created in AM:

```
Enter the Agent profile name
[ ? : Help, < : Back, ! : Exit ]
Enter the Agent Profile name: java-agent
```

- e. Enter the AM realm containing the agent profile. Realms are case-sensitive.

```
Enter the Agent profile realm
[ ? : Help, < : Back, ! : Exit, ^ : Accept Empty value
]
Enter the Agent Profile realm [/]:
```

- f. Enter the path to the password file you created during pre-installation:

```
Enter the path to a file that contains the password to
be used for identifying the Agent.
[ ? : Help, < : Back, ! : Exit ]
Enter the path to the password file: /tmp/pwd.txt
```

- g. Enter the path to a file that contains the agent pre-authentication cookie signing value

```
[ ? : Help, < : Back, ! : Exit ]
Enter the path to the signing file:
```

Provide a path to a file containing a randomly generated key that is at least 64 characters in length, but preferably about 80 characters.

To disable cookie signing, press return without providing a value.

Create arbitrary length keys with the `agentadmin --key` command.

6. Review a summary, and select how to continue:

```
-----
SUMMARY OF YOUR RESPONSES
-----
...
Verify your settings above and decide from the choices
below.
1. Continue with Installation
2. Back to the last interaction
3. Start Over
4. Exit
Please make your selection [1]: 1
...
```

After successful installation, the installer adds the agent configuration to the Tomcat configuration, and sets up configuration and log directories for the agent.

7. Test the installation by browsing to a resource that the agent protects. AM redirects you to authenticate. After authentication, AM redirects you back to the requested resource.

### *Install Tomcat Java Agent silently*

Use the **agentadmin --useResponse** command for silent installation. For information about the option, see [agentadmin command](#).

The following example uses a response file containing the same configuration as in *Install Tomcat Java Agent interactively*.

1. Review the information in [Before you install](#), and perform the steps in [Preinstallation tasks](#).
2. Shut down the Tomcat server where you plan to install the agent.

3. Make sure AM is running.
4. Create a response file with the following content, at `/path/to/response-file`:

```
# Response File
CONFIG_DIR= /path/to/apache-tomcat/conf
AM_SERVER_URL= https://am.example.com:8443/am
CATALINA_HOME= /path/to/apache-tomcat
AGENT_URL= \http://agent.example.com:80/app
AGENT_PROFILE_NAME= java-agent
AGENT_PROFILE_REALM= /
AGENT_PASSWORD_FILE= /tmp/pwd.txt
AGENT_SIGNING_FILE=/tmp/signing-key.txt
```

5. Run the **agentadmin** command with the `--useResponse` option:

```
$ agentadmin --install --acceptLicense --useResponse
/path/to/response-file
```

### *Install in a subrealm*

Other installation examples install the agent in the top-level realm. To install the agent in a subrealm during interactive or silent installation, use the subrealm during the installation or in the response file. For example, instead of:

```
AGENT_PROFILE_REALM = /
```

specify:

```
AGENT_PROFILE_REALM = /myrealm
```

Even though the agent is installed in a subrealm, the default login redirect requires users to log into the top-level realm. For information about how to change the login, see [Use the request domain to redirect login to a different realm](#).

## Install JBoss Java Agent

The examples in this section assume that you are using JBoss, but the procedures are the same for WildFly. Agent binaries for JBoss and WildFly are the same.

### *Install JBoss Java Agent interactively*

1. Review the information in [Before you install](#), and perform the steps in [Preinstallation tasks](#).
2. Shut down the JBoss server where you plan to install the agent.
3. Make sure AM is running.
4. Run **agentadmin --install** to install the agent:

```
$ /path/to/java_agents/jboss_agent/bin/agentadmin --install
```

You are prompted to read and accept the software license agreement for the agent installation. Use the [--acceptLicense](#) option to skip the prompt.

5. Enter the absolute path to the JBoss installation directory:

```
Enter the complete path to the home directory of the JBoss instance.  
[ ? : Help, ! : Exit ]  
Enter the path to the JBoss installation: /path/to/jboss
```

6. Enter the name of the deployment mode for the JBoss installation:

- **standalone** : Manage a single JBoss instance

In standalone mode, the agent installer uses an auto-deployment feature provided by the JBoss deployment scanner so that you do not have to deploy the `agentapp.war` manually.

- **domain** : Manage multiple server instances from a single control point.

In this mode, at the end of the procedure, you must manually deploy the `java_agents/jboss_agent/etc/agentapp.war` file to JBoss.

7. Enter the name of the profile to use in **standalone** or **domain** mode:

- **standalone** : Default.
- **full** : Supports Java EE 6 Full Profile, and subsystems that are not required for high-availability.
- **ha** : Enables all default subsystems, and adds the clustering capabilities.
- **full-ha** : Enables all default subsystems, including those required for high-availability, and adds clustering capabilities.

8. Choose whether to deploy the agent as a global JBoss module.

```
Enter true if you'd like to deploy the policy agent as a global JBoss module.
```

```
[ ? : Help, < : Back, ! : Exit ]  
Install agent as global module? [true]: true
```

To include specific modules for a web application, enter `false`, and complete the additional steps at the end of this procedure.

9. Enter the AM URL:

```
Enter the URL where the AM server is running. Please  
include the deployment URI also as shown below:  
(http://am.sample.com:58080/am)  
[ ? : Help, < : Back, ! : Exit ]  
AM server URL: https://am.example.com:8443/am
```

To load balance connections between the agent and an AM site, enter the URL of the load balancer in front of the AM site.

If a reverse proxy is configured between AM and the agent, enter the proxy URL. For more information, see [Configure an Apache HTTP Server as a reverse proxy](#).

10. Enter the agent URL:

```
Enter the Agent URL. Please include the deployment URI  
also as shown below:  
(http://agent1.sample.com:1234/agentapp)  
[ ? : Help, < : Back, ! : Exit ]  
Agent URL: http://agent.example.com:80/app
```

11. Enter the agent profile name created in AM as part of the pre-installation procedure:

```
Enter the Agent profile name  
[ ? : Help, < : Back, ! : Exit ]  
Enter the Agent Profile name: JBossAgent
```

12. Enter the realm in which the specified agent profile exists.

Press  to accept the default value of `/` for the top-level realm. If you specify the () : Accept Empty value option, the top-level realm is used.

```
Enter the Agent profile realm  
[ ? : Help, < : Back, ! : Exit, ^ : Accept Empty value ]  
Enter the Agent Profile realm [/]:
```

13. Enter the path to the password file you created as part of the pre-installation procedure:

```
Enter the path to a file that contains the password to be
used for identifying the Agent.
[ ? : Help, < : Back, ! : Exit ]
Enter the path to the password file: /tmp/pwd.txt
```

- a. Enter the path to a file that contains the agent pre-authentication cookie signing value

```
[ ? : Help, < : Back, ! : Exit ]
Enter the path to the signing file:
```

Provide a path to a file containing a randomly generated key that is at least 64 characters in length, but preferably about 80 characters.

To disable cookie signing, press return without providing a value.

Create arbitrary length keys with the `agentadmin --key` command.

14. Review a summary of your responses and select how to continue:

```
-----
SUMMARY OF YOUR RESPONSES
-----
```

```
...
```

```
Verify your settings above and decide from the choices
below.
```

- ```
1. Continue with Installation
2. Back to the last interaction
3. Start Over
4. Exit
```

```
Please make your selection [1]: 1
```

```
...
```

After successful completion, the installer updates the JBoss configuration, adds the agent web application under `JBOSS_HOME/server/standalone/deployments`, and sets up configuration and log directories for the agent.

15. Follow these steps if you responded `false` to the question `Deploy the policy agent as a global JBoss module` during the installation:

- a. Add the following line to the web application file  
`/path/to/protected/app/META-INF/MANIFEST.MF`:



```
Dependencies: org.forgerock.openam.agent
```

- b. Create a file at `/path/to/protected/app/WEB-INF/jboss-deployment-structure.xml` with the following content:

```
<?xml version="1.0"?>
  <jboss-deployment-structure
xmlns="urn:jboss:deployment-structure:1.2"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <deployment>
        <dependencies>
            <module name="org.forgerock.openam.agent" >
                <imports>
                    <include path="META-INF"/>
                    <include path="org"/>
                </imports>
            </module>
        </dependencies>
    </deployment>
</jboss-deployment-structure>
```

16. If you chose `domain` as the deployment mode, manually deploy the `java_agents/jboss_agent/etc/agentapp.war` file to JBoss.
17. Test the installation by browsing to a resource that the agent protects. AM redirects you to authenticate. After authentication, AM redirects you back to the requested resource.

## *Install JBoss Java Agent Silently*

To install the Java Agent silently, create a response file containing the installation parameters, and then provide it to the **agentadmin** command.

The following is an example response file to install the agent when JBoss is configured in standalone mode:

```
# Agent User Response File
HOME_DIR= /path/to/jboss
INSTANCE_NAME= standalone
GLOBAL_MODULE= true
INSTALL_PROFILE_NAME=
AM_SERVER_URL= https://am.example.com:8443/am
AGENT_URL= http://www.example.com:8080/agentapp
AGENT_PROFILE_NAME= JBossAgent
AGENT_PROFILE_REALM= /
```

```
AGENT_PASSWORD_FILE= /tmp/pwd.txt
AGENT_SIGNING_FILE=/tmp/signing-key.txt
```

The `INSTALL_PROFILE_NAME` variable is used only when the `INSTANCE_NAME` is set to `domain`. It specifies the name of the JBoss domain profile.

To load balance connections between the agent and an AM site, set `AM_SERVER_URL` to the URL of the load balancer in front of the AM site.

If a reverse proxy is configured between AM and the agent, set `AM_SERVER_URL` to the proxy URL. For more information, see [Configure an Apache HTTP Server as a reverse proxy](#).

1. Review the information in [Before you install](#), and perform the steps in [Preinstallation tasks](#).
2. Make sure that the response file for the installation is ready, or create a response file, for example:

```
$ agentadmin --install --saveResponse response-file
```

3. Shut down the JBoss server where you plan to install the agent.
4. Make sure AM is running.
5. Run the **agentadmin** command with the `--useResponse` option:

```
$ agentadmin --install --acceptLicense --useResponse
/path/to/response-file
```

6. If you configured the `GLOBAL_MODULE` variable as `false` in the response file, add the following line to the `META-INF/MANIFEST.MF` file of the web application:

```
Dependencies: org.forgerock.openam.agent
```

7. If you configured the `INSTANCE_NAME` variable as `domain` in the response file, manually deploy the `java_agents/jboss_agent/etc/agentapp.war` file to JBoss.

## *Install in a subrealm*

Other installation examples install the agent in the top-level realm. To install the agent in a subrealm during interactive or silent installation, use the subrealm during the installation or in the response file. For example, instead of:

```
AGENT_PROFILE_REALM = /
```

specify:

```
AGENT_PROFILE_REALM = /myrealm
```

Even though the agent is installed in a subrealm, the default login redirect requires users to log into the top-level realm. For information about how to change the login, see [Use the request domain to redirect login to a different realm](#).

## Install Jetty Java Agent

Command-line examples in this chapter show Jetty accessed remotely. If follow the examples and have issues accessing Jetty remotely, consider changing filter settings in the deployment descriptor file, `/path/to/jetty/webapps/test/WEB-INF/web.xml`, as shown in the following example:

```
<filter>
<filter-name>TestFilter</filter-name>
<filter-class>com.acme.TestFilter</filter-class>
<init-param>
  <param-name>remote</param-name>
  <param-value>true</param-value> <!-- default: false -->
</init-param>
</filter>
```

### *Install Jetty Java Agent interactively*

1. Review the information in [Before you install](#), and perform the steps in [Preinstallation tasks](#).
2. Shut down the Jetty server where you plan to install the agent.
3. Make sure AM is running.
4. Run **agentadmin --install** to install the agent:

```
$ /path/to/java_agents/jetty_agent/bin/agentadmin --
install
```

You are prompted to read and accept the software license agreement for the agent installation. Use the `--acceptLicense` option to skip the prompt.

5. Enter the absolute path to the root of the Jetty installation:

```
This is the home of the Jetty installation (directory
containing start.jar)
[ ? : Help, ! : Exit ]
Enter the Jetty home directory [/opt/jetty]:
/path/to/jetty/home
```

This is the equivalent of the JETTY\_HOME environment variable for Jetty.

6. Enter the absolute path to the Jetty configuration directory:

```
Enter the absolute path of the Jetty etc directory.
[ ? : Help, < : Back, ! : Exit ]
Enter the absolute path of the Jetty etc directory:
/path/to/jetty/etc
```

7. Enter the absolute path to the Jetty base directory:

```
This is the base of the Jetty installation (directory
containing the webapps subdirectory)
[ ? : Help, < : Back, ! : Exit ]
Enter the Jetty base directory [/usr/local/jetty]:
/path/to/jetty/base
```

This is the equivalent of the JETTY\_BASE environment variable for Jetty.

This path may be the same as the one specified as the root of the Jetty installation.

8. Enter the AM URL:

```
Enter the URL where the AM server is running. Please
include the deployment URI also as shown below:
(http://am.sample.com:58080/am)
[ ? : Help, < : Back, ! : Exit ]
AM server URL: https://am.example.com:8443/am
```

To load balance connections between the agent and an AM site, enter the URL of the load balancer in front of the AM site.

If a reverse proxy is configured between AM and the agent, enter the proxy URL. For more information, see [Configure an Apache HTTP Server as a reverse proxy](#).

9. Enter the agent URL:

```
Enter the Agent URL. Please include the deployment URI
also as shown below:
(http://agent1.sample.com:1234/agentapp)
[ ? : Help, < : Back, ! : Exit ]
Agent URL: \http://agent.example.com:80/app
```

10. Enter the agent profile name created in AM as part of the pre-installation procedure:

```
Enter the Agent profile name
[ ? : Help, &lt; : Back, ! : Exit ]
Enter the Agent Profile name: JettyAgent
```

11. Enter the realm in which the specified agent profile exists.

Press  to accept the default value of / for the top-level realm. If you specify the () : Accept Empty value option, the top-level realm is used.

```
Enter the Agent profile realm
[ ? : Help, < : Back, ! : Exit, ^ : Accept Empty value ]
Enter the Agent Profile realm [/]:
```

12. Enter the path to the password file you created as part of the pre-installation procedure:

```
Enter the path to a file that contains the password to be
used for identifying the Agent.
[ ? : Help, < : Back, ! : Exit ]
Enter the path to the password file: /tmp/pwd.txt
```

- a. Enter the path to a file that contains the agent pre-authentication cookie signing value

```
[ ? : Help, < : Back, ! : Exit ]
Enter the path to the signing file:
```

Provide a path to a file containing a randomly generated key that is at least 64 characters in length, but preferably about 80 characters.

To disable cookie signing, press return without providing a value.

Create arbitrary length keys with the `agentadmin --key` command.

13. Review a summary of your responses and select how to continue:

-----  
SUMMARY OF YOUR RESPONSES  
-----

...

Verify your settings above and decide from the choices below.

1. Continue with Installation
2. Back to the last interaction
3. Start Over
4. Exit

Please make your selection [1]: 1

...

After successful completion, the installer updates Jetty's `start.jar` to reference the agent, sets up the agent web application, and sets up configuration and log directories for the agent.

14. Test the installation by browsing to a resource that the agent protects. AM redirects you to authenticate. After authentication, AM redirects you back to the requested resource.

### *Install Jetty Java Agent silently*

To install the Java Agent silently, create a response file containing the installation parameters, and then provide it to the **agentadmin** command. The following is an example response file:

```
# Agent User Response File
CONFIG_DIR= /path/to/jetty/etc
JETTY_HOME= /path/to/jetty/home
JETTY_BASE= /path/to/jetty/base
AM_SERVER_URL= https://am.example.com:8443/am
AGENT_URL= http://www.example.com:8080/agentapp
AGENT_PROFILE_NAME= JettyAgent
AGENT_PROFILE_REALM= /
AGENT_PASSWORD_FILE= /tmp/pwd.txt
AGENT_SIGNING_FILE=/tmp/signing-key.txt
```

To load balance connections between the agent and an AM site, set `AM_SERVER_URL` to the URL of the load balancer in front of the AM site.

If a reverse proxy is configured between AM and the agent, set `AM_SERVER_URL` to the proxy URL. For more information, see [Configure an Apache HTTP Server as a reverse proxy](#).

1. Review the information in [Before you install](#), and perform the steps in [Preinstallation tasks](#).
2. Shut down the Jetty server where you plan to install the agent.
3. Make sure that AM is running.
4. Run the **agentadmin** command with the `--useResponse` option:

```
$ agentadmin --install --acceptLicense --useResponse  
/path/to/response-file
```

### *Install in a subrealm*

Other installation examples install the agent in the top-level realm. To install the agent in a subrealm during interactive or silent installation, use the subrealm during the installation or in the response file. For example, instead of:

```
AGENT_PROFILE_REALM = /
```

specify:

```
AGENT_PROFILE_REALM = /myrealm
```

Even though the agent is installed in a subrealm, the default login redirect requires users to log into the top-level realm. For information about how to change the login, see [Use the request domain to redirect login to a different realm](#).

## Install WebLogic Java Agent

### *Install WebLogic Java Agent interactively*

1. Review the information in [Before you install](#), and perform the steps in [Preinstallation tasks](#).
2. Shut down the WebLogic server where you plan to install the agent.
3. Make sure AM is running.
4. Run **agentadmin --install** to install the agent:

```
$ /path/to/java_agents/weblogic_agent/bin/agentadmin --  
install
```

You are prompted to read and accept the software license agreement for the agent installation. Use the `--acceptLicense` option to skip the prompt.

5. Enter the path to the `startWebLogic.sh` file of the WebLogic domain where you want to install the agent:

```
Enter the path to the location of the script used to start
the WebLogic domain.
Please ensure that the agent is first installed on the
admin server instance
before installing on any managed server instance.
[ ? : Help, ! : Exit ]
Enter the Startup script location
[/usr/local/bean/user_projects/domains/base_domain/startWeb
Logic.sh]:
/path/to/Oracle_Home/user_projects/domains/base_domain/sta
rtWebLogic.sh
```

6. Enter the path to the WebLogic installation directory:

```
Enter the WebLogic home directory
[ ? : Help, < : Back, ! : Exit ]
Enter the WebLogic home directory
[/usr/local/bean/wlserver_10.0]:
/path/to/weblogic
```

7. Enter the AM URL:

```
Enter the URL where the AM server is running. Please
include the deployment URI also as shown below:
(http://am.sample.com:58080/am)
[ ? : Help, < : Back, ! : Exit ]
AM server URL: https://am.example.com:8443/am
```

To load balance connections between the agent and an AM site, enter the URL of the load balancer in front of the AM site.

If a reverse proxy is configured between AM and the agent, enter the proxy URL. For more information, see [Configure an Apache HTTP Server as a reverse proxy](#).

8. Enter the agent URL:

```
Enter the Agent URL. Please include the deployment URI
also as shown below:
(http://agent1.sample.com:1234/agentapp)
```



```
[ ? : Help, < : Back, ! : Exit ]
Agent URL: \http://agent.example.com:80/app
```

9. Enter the agent profile name created in AM as part of the pre-installation procedure:

```
Enter the Agent profile name
[ ? : Help, < : Back, ! : Exit ]
Enter the Agent Profile name: WebLogicAgent
```

10. Enter the realm in which the specified agent profile exists.

Press  to accept the default value of / for the top-level realm. If you specify the () : Accept Empty value option, the top-level realm is used.

```
Enter the Agent profile realm
[ ? : Help, < : Back, ! : Exit, ^ : Accept Empty value ]
Enter the Agent Profile realm [/]:
```

11. Enter the path to the password file you created as part of the pre-installation procedure:

```
Enter the path to a file that contains the password to be
used for identifying the Agent.
[ ? : Help, < : Back, ! : Exit ]
Enter the path to the password file: /tmp/pwd.txt
```

- a. Enter the path to a file that contains the agent pre-authentication cookie signing value

```
[ ? : Help, < : Back, ! : Exit ]
Enter the path to the signing file:
```

Provide a path to a file containing a randomly generated key that is at least 64 characters in length, but preferably about 80 characters.

To disable cookie signing, press return without providing a value.

Create arbitrary length keys with the `agentadmin --key` command.

12. Review a summary of your responses and select how to continue:

```
$ /path/to/java_agents/weblogic_agent/bin/agentadmin --
install --acceptLicense
-----
SUMMARY OF YOUR RESPONSES
```

```

-----
...
Verify your settings above and decide from the choices
below.
1. Continue with Installation
2. Back to the last interaction
3. Start Over
4. Exit
Please make your selection [1]: 1
...

```

13. Source the agent in one of the following ways:

- Manually source the file containing the agent environment settings for WebLogic before starting the container.

```
$ . /path/to/setAgentEnv_AdminServer.sh
```

- Add the `setAgentEnv_AdminServer.sh` line to the shown location [path] in the `startWebLogic.sh` script. Note that the file can be overwritten:

```

$ cat /path/to/startWebLogic.sh
...
# Any changes to this script may be lost when adding
extensions to this
# configuration.
DOMAIN_HOME="/opt/Oracle/Middleware/user_projects/domai
ns/base_domain"
. /path/to/setAgentEnv_AdminServer.sh
${DOMAIN_HOME}/bin/startWebLogic.sh $*

```

If the sourcing is not set properly, the following message appears:

```

<Error> <HTTP> <cent.example.com>
<AdminServer> <[STANDBY] ExecuteThread: '5' for queue:
weblogic.kernel.
Default (self-tuning) '> <<WLS Kernel>>
<BEA-101165> <Could not load user defined filter in
web.xml:
ServletContext@1761850405[app:agentapp
module:agentapp.war path:null
spec-version:null]
com.sun.identity.agents.filter.AmAgentFilter.
java.lang.ClassNotFoundException:
com.sun.identity.agents.filter.AmAgentFilter

```

14. Start the WebLogic server.
15. Deploy the `/path/to/java_agents/weblogic_agent/etc/agentapp.war` agent web application in WebLogic.
16. Test the installation by browsing to a resource that the agent protects. AM redirects you to authenticate. After authentication, AM redirects you back to the requested resource.

### *Install WebLogic Java Agent silently*

To install the Java Agent silently, create a response file containing the installation parameters, and then provide it to the **agentadmin** command. The following is an example response file:

```
# Agent User Response File
STARTUP_SCRIPT=
/path/to/Oracle_Home/user_projects/domains/base_domain/startWebLogic.sh
SERVER_NAME= AdminServer
WEBLOGIC_HOME_DIR= /path/to/weblogic
AM_SERVER_URL= https://am.example.com:8443/am
AGENT_URL= http://www.example.com:8080/agentapp
AGENT_PROFILE_NAME= WebLogicAgent
AGENT_PROFILE_REALM= /
AGENT_PASSWORD_FILE= /tmp/pwd.txt
AGENT_SIGNING_FILE=/tmp/signing-key.txt
```

To load balance connections between the agent and an AM site, set `AM_SERVER_URL` to the URL of the load balancer in front of the AM site.

If a reverse proxy is configured between AM and the agent, set `AM_SERVER_URL` to the proxy URL. For more information, see [Configure an Apache HTTP Server as a reverse proxy](#).

1. Review the information in [Before you install](#), and perform the steps in [Preinstallation tasks](#).
2. Make sure that the response file for the installation is ready, or create a response file, for example:

```
$ agentadmin --install --saveResponse response-file
```

3. Shut down the WebLogic server where you plan to install the agent.
4. Make sure AM is running.

5. Run the **agentadmin** command with the **--useResponse** option:

```
$ agentadmin --install --acceptLicense --useResponse  
/path/to/response-file
```

6. Source the agent in one of the following ways:

- Manually source the file containing the agent environment settings for WebLogic before starting the container.

```
$ . /path/to/setAgentEnv_AdminServer.sh
```

- Add the `setAgentEnv_AdminServer.sh` line to the shown location [path] in the `startWebLogic.sh` script. Note that the file can be overwritten:

```
$ cat /path/to/startWebLogic.sh  
...  
# Any changes to this script may be lost when adding  
extensions to this  
# configuration.  
DOMAIN_HOME="/opt/Oracle/Middleware/user_projects/domai  
ns/base_domain"  
. /path/to/setAgentEnv_AdminServer.sh  
${DOMAIN_HOME}/bin/startWebLogic.sh $*
```

If the sourcing is not set properly, the following message appears:

```
<Error> <HTTP> <cent.example.com>  
<AdminServer> <[STANDBY] ExecuteThread: '5' for queue:  
weblogic.kernel.  
Default (self-tuning)'> <<WLS Kernel>>  
<BEA-101165> <Could not load user defined filter in  
web.xml:  
ServletContext@1761850405[app:agentapp  
module:agentapp.war path:null  
spec-version:null]  
com.sun.identity.agents.filter.AmAgentFilter.  
java.lang.ClassNotFoundException:  
com.sun.identity.agents.filter.AmAgentFilter
```

7. Start the WebLogic Server.

8. Deploy the `/path/to/java_agents/weblogic_agent/etc/agentapp.war` agent web application in WebLogic.

## *Install WebLogic Java Agent in multi-server domains*

In many WebLogic domains, the administration server provides a central point for controlling and managing the configuration of the managed servers that host protected web applications.

If WebLogic-managed servers run on different hosts, you must create separate agent profiles and perform separate installations for each so that AM can send notifications to the appropriate addresses.

### *Install WebLogic Java Agent on administration and managed servers*

1. If servers are on different hosts, create agent profiles for each server where you plan to install the agent. For more information, see [Installing the WebLogic Java Agent](#).
2. Prepare your protected web applications by adding the agent filter configuration as described in [Configure the agent filter for a web application](#).
3. Use the **agentadmin** command to install the agent either interactively, or silently on each server in the domain:
  - For interactive installation, follow the instructions in [To install the WebLogic Java Agent](#).
  - For silent installation, follow the instructions in [Installing the WebLogic Java Agent silently](#).
4. On each managed server in the domain, update the classpath to include agent .jar files.

In WebLogic Node Manager console, navigate to Environment > Servers > **server** > **Server Start** > **Class Path**, and then edit the classpath as in the following example, but all on a single line:

```
/path/to/java_agents/weblogic_agent/lib/agent.jar:  
/path/to/java_agents/weblogic_agent/lib/opensocclientsdk.j  
ar:  
...  
/path/to/java_agents/weblogic_agent/locale:  
/path/to/java_agents/weblogic_agent/Agent_001/config:  
$CLASSPATH
```

Replace the paths in the example with the actual paths for your domain.

5. Restart the managed servers.

# Install WebSphere Java Agent

If you are using IBM Java, perform the procedure in [Install WebSphere with IBM Java](#)

## *Install WebSphere Java Agent interactively*

1. Review the information in [Before you install](#), and perform the steps in [Preinstallation tasks](#).
2. Shut down the WebSphere server where you plan to install the agent.
3. Make sure AM is running.
4. Run **agentadmin --install** to install the agent:

```
$ /path/to/java_agents/websphere_agent/bin/agentadmin --install
```

You are prompted to read and accept the software license agreement for the agent installation. Use the [--acceptLicense](#) option to skip the prompt.

5. Enter the path to the configuration directory of the server instance for the WebSphere node:

```
Enter the fully qualified path to the configuration
directory of the Server
Instance for the WebSphere node.
[ ? : Help, ! : Exit ]
Enter the Instance Config Directory
[/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/config/cel
ls/<hostname>Node01Cell/nodes/<hostname>Node01/servers/ser
ver1]:
**/path/to/WebSphere/AppServer/profiles/AppSrv01/config/c
ells/DefaultCell01/nodes/DefaultNode01/servers/server1**
```

6. Enter the name of the server instance where the agent will be installed:

```
Enter the Server Instance name.
[ ? : Help, < : Back, ! : Exit ]
Enter the Server Instance name [server1]: **server1**
```

7. Enter the path to the WebSphere install directory:

```
Enter the WebSphere Install Root directory.
[ ? : Help, < : Back, ! : Exit ]
```

```
Enter the WebSphere Install Root directory
[/opt/IBM/WebSphere/AppServer]:
**/path/to/WebSphere/AppServer**
```

8. Enter the AM URL:

```
Enter the URL where the AM server is running. Please
include the deployment URI also as shown below:
(http://am.sample.com:58080/am)
[ ? : Help, < : Back, ! : Exit ]
AM server URL: https://am.example.com:8443/am
```

To load balance connections between the agent and an AM site, enter the URL of the load balancer in front of the AM site.

If a reverse proxy is configured between AM and the agent, enter the proxy URL. For more information, see [Configure an Apache HTTP Server as a reverse proxy](#).

9. Enter the agent URL:

```
Enter the Agent URL. Please include the deployment URI
also as shown below:
(http://agent1.sample.com:1234/agentapp)
[ ? : Help, < : Back, ! : Exit ]
Agent URL: \http://agent.example.com:80/app
```

10. Enter the realm in which the specified agent profile exists.

Press  to accept the default value of / for the top-level realm. If you specify the () : Accept Empty value option, the top-level realm is used.

```
Enter the Agent profile realm
[ ? : Help, < : Back, ! : Exit, ^ : Accept Empty value ]
Enter the Agent Profile realm [/]:
```

11. Enter the path to the password file you created as part of the pre-installation procedure:

```
Enter the path to a file that contains the password to be
used for identifying the Agent.
[ ? : Help, < : Back, ! : Exit ]
Enter the path to the password file: /tmp/pwd.txt
```

- a. Enter the path to a file that contains the agent pre-authentication cookie signing value

```
[ ? : Help, < : Back, ! : Exit ]  
Enter the path to the signing file:
```

Provide a path to a file containing a randomly generated key that is at least 64 characters in length, but preferably about 80 characters.

To disable cookie signing, press return without providing a value.

Create arbitrary length keys with the `agentadmin --key` command.

12. Review a summary of your responses and select how to continue:

```
-----  
SUMMARY OF YOUR RESPONSES  
-----  
  
...  
Verify your settings above and decide from the choices  
below.  
1. Continue with Installation  
2. Back to the last interaction  
3. Start Over  
4. Exit  
Please make your selection [1]: 1  
...
```

After successful completion, the installer updates the WebSphere configuration,] copies the agent libraries to WebSphere's external library directory, and sets up configuration and log directories for the agent.

13. Restart the WebSphere server.

14. Deploy the `/path/to/java_agents/websphere_agent/etc/agentapp.war` agent web application in WebSphere.

15. Test the installation by browsing to a resource that the agent protects. AM redirects you to authenticate. After authentication, AM redirects you back to the requested resource.

## *Install WebSphere Java Agent silently*

To install the Java Agent silently, create a response file containing the installation parameters, and then provide it to the **agentadmin** command. The following is an example response file:

```
# Agent User Response File  
SERVER_INSTANCE_DIR=
```



```
/path/to/WebSphere/AppServer/profiles/AppSrv01/config/cells/DefaultCell01/nodes/DefaultNode01/servers/server1
SERVER_INSTANCE_NAME= server1
HOME_DIRECTORY= /path/to/WebSphere/AppServer
AM_SERVER_URL= https://am.example.com:8443/am
AGENT_URL= http://www.example.com:8080/agentapp
AGENT_PROFILE_NAME= WebSphereAgent
AGENT_PROFILE_REALM= /
AGENT_PASSWORD_FILE= /tmp/pwd.txt
AGENT_SIGNING_FILE=/tmp/signing-key.txt
```

To load balance connections between the agent and an AM site, set `AM_SERVER_URL` to the URL of the load balancer in front of the AM site.

If a reverse proxy is configured between AM and the agent, set `AM_SERVER_URL` to the proxy URL. For more information, see [Configure an Apache HTTP Server as a reverse proxy](#).

### *Install WebSphere Java Agent silently*

1. Review the information in [Before you install](#), and perform the steps in [Preinstallation tasks](#).
2. Make sure that the response file for the installation is ready, or create a response file, for example:

```
$ agentadmin --install --saveResponse response-file
```

3. Shut down the WebSphere server where you plan to install the agent.
4. Make sure AM is running.
5. Run the **agentadmin** command with the `--useResponse` option:

```
$ agentadmin --install --acceptLicense --useResponse
/path/to/response-file
```

6. Start the WebSphere server.
7. Deploy the `/path/to/java_agents/websphere_agent/etc/agentapp.war` agent web application in WebSphere.

### *Install WebSphere Java Agent with IBM Java*

The WebSphere Java Agent runs with IBM Java. To install the agent using IBM Java on platforms other than AIX, change the **agentadmin** script to use the IBM Java

Cryptography Extensions (JCE).

Line breaks and continuation marker ( \ ) characters have been added to the following examples to make them easier to understand. They are not required.

1. Open the file `bin/agentadmin` for editing.
2. Edit the line that calls the **AdminToolLauncher** jar file to move the `$AGENT_OPTS` environment variable before the classpath is set:

Before:

```
$JAVA_VM -classpath "$AGENT_CLASSPATH" $AGENT_OPTS \  
com.sun.identity.install.tools.launch.AdminToolLauncher $*
```

After:

```
$JAVA_VM $AGENT_OPTS -classpath "$AGENT_CLASSPATH" \  
com.sun.identity.install.tools.launch.AdminToolLauncher $*
```

3. Save the file.

You can now install the WebSphere Java Agent with IBM Java as described in [Install the WebSphere Java Agent](#).

## About WebSphere Network Deployment

When using WebSphere Application Server Network Deployment, you must install WebSphere Java Agents on the Deployment Manager, on each Node Agent, and on each Application Server. Installation requires that you stop and then restart the Deployment Manager, each Node Agent, and each Application Server in the Network Deployment.

Before installation, synchronize each server configuration with the profile saved by the Deployment Manager using the **syncNode** command. After agent installation, copy the server configuration for each node stored in `server.xml` to the corresponding Deployment Manager profile. After you have synchronized the configurations, you must restart the Deployment Manager for the Network Deployment.

## Post-installation tasks

## Review directories for configuration, logs, and POST data.

Each agent instance has a numbered directory, starting with `Agent_001` for the first instance. The following directories are created under `/path/to/java_agents/agent_type/Agent_n`:

- `config` : For information, see [Configuration files](#).
- `logs` : During agent startup, the location of the logs is based on the container which is being used. For example, bootstrap logs for Tomcat agents are written to `catalina.out`. The following log directories are created:
  - `logs/audit/` : Operational audit log directory, used only if remote logging to AM is disabled.
  - `logs/debug/` : The directory where the agent writes debug log files after startup.
- `pdp` : The directory to store POST data. The directory is created on installation, but used only when [Enable POST Data Preservation](#) and [POST Data Preservation in Files or Cache](#) are `true`.

## Configure the agent filter for a web application

After installation, configure an *agent filter* to intercept inbound client requests and give them access to resources. The agent filter class is `com.sun.identity.agents.filter.AmAgentFilter`. The agent filter gives access based on the value of [Agent Filter Mode Map](#).

Configure the agent filter in the web application's `web.xml` file. For information about configuration options, see the documentation for your web application. For example, see Oracle's [Developing Web Applications for WebLogic Server](#)<sup>☞</sup>.

Configure the agent filter first, before configuring other filters in `web.xml`. If several web applications run in the same container, configure an agent filter for each web application.

The following example protects every resource in the web application where it is configured:

```
<filter>
  <filter-name>Agent</filter-name>
  <display-name>AM Agent</display-name>
  <description>AM Agent Filter</description>
  <filter-
class>com.sun.identity.agents.filter.AmAgentFilter</filter-class>
</filter>
<filter-mapping>
```

```

<filter-name>Agent</filter-name>
<url-pattern>/*</url-pattern>
<dispatcher>REQUEST</dispatcher>
<dispatcher>INCLUDE</dispatcher>
<dispatcher>FORWARD</dispatcher>
<dispatcher>ERROR</dispatcher>
</filter-mapping>

```

The following example protects an application that processes requests asynchronously:

```

<filter>
  <filter-name>Agent</filter-name>
  <display-name>AM Agent</display-name>
  <description>AM Agent Filter</description>
  <filter-
class>com.sun.identity.agents.filter.AmAgentFilter</filter-class>
  <async-supported>true</async-supported>
</filter>

```

## Configure the agent filter mode

By default, the agent filter uses the filter mode `URL_POLICY`. After installation, you can change the filter mode with the property Agent Filter Mode Map, or in the AM console:

1. In the AM console, go to **Realms** > **realm name** > **Applications** > **Agents** > **Java**, and select your Java Agent.
2. On the **Global** tab, select **Agent Filter Mode Map**, and set the filter mode as follows:
  - To use `URL_POLICY` for all web applications in the web container, do not change the setting; this is the default.
  - To use `SSO_ONLY` for the `BankApp` web application, set these values:
3. (Optional) In **Agent Filter Mode**, override the global mode for a specific context path:
  - **Key:** `BankApp`.
  - **Value:** Enter the mode name, for example `URL_POLICY`.
4. Click **Add**, and save your changes.

## Secure communication between the agent and AM

After installation, you can optionally configure secure communication between the agent and AM.

1. Configure AM to send cookies only when the communication channel is secure:
  - a. In the AM console, select **Realms** > **realm name** > **Applications** > **Agents** > **Java** > **agent name** > **SSO**.
  - b. Enable Transmit Cookies Securely.
2. Import a CA certificate in the JDK truststore, usually at `$JAVA_HOME/jre/lib/security/cacerts`. The certificate should be the one configured for HTTPS connections in the AM container, or signed with the same CA root certificate. For example:

```
$ keytool \  
-import \  
-trustcacerts \  
-alias agentcert \  
-file /path/to/cacert.pem \  
-keystore $JAVA_HOME/jre/lib/security/cacerts
```

Make sure that all containers where AM is installed trust the certificate stored in the JDK truststore, and that the JDK trusts the certificates stored on the containers where AM is installed.

3. Add the following properties to the `AgentBootstrap.properties` file:
  - `javax.net.ssl.trustStore`, to specify the full path to the JDK truststore.
  - `javax.net.ssl.trustStorePassword`, to specify the password of the truststore.

For example:

```
javax.net.ssl.trustStore=/Library/Java/JavaVirtualMachines/jdk1.8.0_101.jdk/Contents/Home/jre/lib/security/cacerts  
javax.net.ssl.trustStorePassword=changeit
```

For backward-compatibility, you can also provide the truststore and the password to the agent by specifying them as Java properties in the container's start-up sequence. For example, add them to Tomcat's `$CATALINA_OPTS` variable instead of specifying them in the `AgentBootstrap.properties` file:

```
$ export CATALINA_OPTS="$CATALINA_OPTS \  
-  
Djavax.net.ssl.trustStore=$JAVA_HOME/jre/lib/security/c  
acerts \  
-Djavax.net.ssl.trustStorePassword=changeit"
```

4. Restart the agent.

## Upgrade Java Agent

1. Read the [Release notes](#) for information about changes in Java Agent.
2. Back up the directories for the agent installation and the web application container configuration:

- In [local configuration mode](#):

```
$ cp -r /path/to/java_agents/agent_type /path/to/backup  
$ cp -r /path/to/tomcat/webapps/agentapp  
/path/to/backup
```

- In [remote configuration mode](#), back up as described in AM's [Maintenance guide](#).
3. Redirect client traffic away from the protected web application.
  4. Stop the web application container where the agent is installed.
  5. Remove the old Java Agent, as described in [Remove Java Agent](#).
  6. Install the new agent, as described in [Install Java Agent](#).

The installer creates new `AgentConfiguration.properties` and `AgentBootstrap.properties` files, containing properties for the agent version.

7. Review the agent configuration:

- In [local configuration mode](#), see the `AgentConfiguration.properties` file. Use the backed-up copy of the configuration file for guidance, the agent's [Release notes](#), and AM's [Release notes](#) to check for changes. Update the file manually to include properties for your environment.

The `AgentBootstrap.properties` file created by the installer contains bootstrap properties relevant to the new version of the agent.

- In [remote configuration mode](#), review the agent's [Release notes](#) and AM's [Release notes](#) to check for changes. If necessary, change the agent

configuration using the AM console.

8. Secure communication between AM and the agent with appropriate keys. For information, see [Configuring AM servers to communicate with Java Agents](#).
9. Start the web application container where the agent is installed.
10. Check that the agent is performing as expected. For example, navigate to a protected page on the website and confirm whether you can access it according to your configuration.
11. Allow client traffic to flow to the protected web application.

## Remove Java Agent

### Remove Tomcat Java Agent

1. Shut down the server where the agent is installed.
2. Run the **agentadmin** command with the `--listAgents` option list installed agent instances:

```
$ agentadmin --listAgents
The following agents are configured on this Application
Server.
...
The following are the details for agent Agent_001 :-
...
```

3. Note the configuration information of the agent instance you want to remove.
4. Run the **agentadmin** command with the `--uninstall` option.

```
$ agentadmin --uninstall
```

5. Enter the path of the Tomcat installation directory:

```
Enter the complete path to the directory which is used by
Tomcat Server to
store its configuration Files. This directory uniquely
identifies the
Tomcat Server instance that is secured by this Agent.
[ ? : Help, ! : Exit ]
```

```
Enter the Tomcat Server Config Directory Path
[/opt/apache-tomcat/conf]: /path/to/apache-tomcat/conf
```

6. Review a summary of your responses and select how to continue:

```
-----
SUMMARY OF YOUR RESPONSES
-----
```

```
...
```

```
Verify your settings above and decide from the choices
below.
```

```
1. Continue with Uninstallation
```

```
2. Back to the last interaction
```

```
3. Start Over
```

```
4. Exit
```

```
Please make your selection [1]: **1**
```

```
...
```

## Remove JBoss Java Agent

1. Shut down the server where the agent is installed.
2. Run the **agentadmin** command with the **--listAgents** option list installed agent instances:

```
$ agentadmin --listAgents
The following agents are configured on this Application
Server.
...
The following are the details for agent Agent_001 :-
...
```

3. Note the configuration information of the agent instance you want to remove.
4. Run the **agentadmin** command with the **--uninstall** option.

```
$ agentadmin --uninstall
```

5. Enter the path to the JBoss installation directory:

```
Enter the complete path to the home directory of the JBoss
instance.
```



```
[ ? : Help, ! : Exit ]
```

```
Enter the path to the JBoss installation: /path/to/jboss
```

6. Enter `domain` or `standalone`, for the deployment mode of the JBoss installation to uninstall:

```
Enter the name of the deployment mode of the JBoss
installation that you wish
to use with this agent. Supported values are: domain,
standalone.
```

```
[ ? : Help, < : Back, ! : Exit ]
```

```
Enter the deployment mode of JBoss [standalone]:
```

```
standalone
```

7. Review a summary of your responses and select how to continue:

```
-----
SUMMARY OF YOUR RESPONSES
-----
```

```
...
```

```
Verify your settings above and decide from the choices
below.
```

```
1. Continue with Uninstallation
```

```
2. Back to the last interaction
```

```
3. Start Over
```

```
4. Exit
```

```
Please make your selection [1]: **1**
```

```
...
```

## Remove Jetty Java Agent

1. Shut down the server where the agent is installed.
2. Run the **agentadmin** command with the `--listAgents` option list installed agent instances:

```
$ agentadmin --listAgents
```

```
The following agents are configured on this Application
Server.
```

```
...
```

```
The following are the details for agent Agent_001 :-
```

```
...
```

3. Note the configuration information of the agent instance you want to remove.
4. Run the **agentadmin** command with the `--uninstall` option.

```
$ agentadmin --uninstall
```

5. Enter the path of the Jetty configuration directory:

```
Enter the complete path to the directory which is used by
Jetty Server to store
its configuration Files. This directory uniquely
identifies the Jetty
Server instance that is secured by this Agent.
[ ? : Help, ! : Exit ]
Enter the Jetty Server Config Directory Path
[/opt/jetty/etc]: /path/to/jetty/etc
```

6. Review a summary of your responses and select how to continue:

```
-----
SUMMARY OF YOUR RESPONSES
-----
...
Verify your settings above and decide from the choices
below.
1. Continue with Uninstallation
2. Back to the last interaction
3. Start Over
4. Exit
Please make your selection [1]: 1
...
```

## Remove WebLogic Java Agent

1. Shut down the server where the agent is installed.
2. Run the **agentadmin** command with the `--listAgents` option list installed agent instances:

```
$ agentadmin --listAgents
The following agents are configured on this Application
Server.
...
```

The following are the details for agent Agent\_001 :-

...

3. Note the configuration information of the agent instance you want to remove.
4. Run the **agentadmin** command with the **--uninstall** option.

```
$ agentadmin --uninstall
```

5. Enter the path to the **startWebLogic.sh** file of the WebLogic domain where you want to install the agent:

Enter the path to the location of the script used to start the WebLogic domain.

Please ensure that the agent is first installed on the admin server instance

before installing on any managed server instance.

[ ? : Help, ! : Exit ]

Enter the Startup script location

[/usr/**local**/bea/user\_projects/domains/base\_domain/startWebLogic.sh]:

**/Oracle\_Home/user\_projects/domains/base\_domain/startWebLogic.sh**

6. Enter the name of the WebLogic instance:

Enter the name of the WebLogic Server instance secured by the agent.

[ ? : Help, < : Back, ! : Exit ]

Enter the WebLogic Server instance name [AdminServer]:

**AdminServer**

7. Review a summary of your responses and select how to continue:

-----  
SUMMARY OF YOUR RESPONSES  
-----

...

Verify your settings above and decide from the choices below.

1. Continue with Uninstallation
2. Back to the last interaction
3. Start Over
4. Exit

```
Please make your selection [1]: 1
```

```
...
```

## Remove WebSphere Java Agent

1. Shut down the server where the agent is installed.
2. Run the **agentadmin** command with the **--listAgents** option list installed agent instances:

```
$ agentadmin --listAgents
The following agents are configured on this Application
Server.
...
The following are the details for agent Agent_001 :-
...
```

3. Note the configuration information of the agent instance you want to remove.
4. Run the **agentadmin** command with the **--uninstall** option.

```
$ agentadmin --uninstall
```

5. Enter the path to the configuration directory of the server instance for the WebSphere node:

```
Enter the fully qualified path to the configuration
directory of the Server
Instance for the WebSphere node.
[ ? : Help, ! : Exit ]
Enter the Instance Config Directory
[/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/config/cel
ls/<hostname>Node01Cell/nodes/<hostname>Node01/servers/ser
ver1]:
/path/to/WebSphere/AppServer/profiles/AppSrv01/config/cel
ls/DefaultCell01/nodes/DefaultNode01/servers/server1
```

6. Enter the name of the server instance where the agent will be removed. For example, **server1**.

```
Enter the Server Instance name.
[ ? : Help, < : Back, ! : Exit ]
Enter the Server Instance name [server1]: server1
```

7. Enter the path to the WebSphere install directory:

```
Enter the WebSphere Install Root directory.  
[ ? : Help, < : Back, ! : Exit ]  
Enter the WebSphere Install Root directory  
[/opt/IBM/WebSphere/AppServer]:  
/path/to/WebSphere/AppServer
```

8. Review a summary of your responses and select how to continue:

```
-----  
SUMMARY OF YOUR RESPONSES  
-----  
  
...  
Verify your settings above and decide from the choices  
below.  
1. Continue with Uninstallation  
2. Back to the last interaction  
3. Start Over  
4. Exit  
Please make your selection [1]: 1  
  
...
```

## agentadmin command

The **agentadmin** command manages Java Agent installation. It requires a Java runtime environment. The command supports the following options:

### --install

Installs a new agent instance.

Usage: **agentadmin --install [--useResponse | --saveResponse *file-name*] [-acceptLicence]**

Before installation, shut down the agent container. If a service on an agent URL is responding, the installer stops with an error.

When the command is used without options, the installation process prompts for the following information:

- Confirmation that you have read and accepted the software license agreement.
- Information about the container installation.

- The URL of the AM instance. The agent confirms that it can log in to AM by using the profile name and password provided during installation. If unsuccessful, the installation stops with an error.
- The URL of the agent instance. The agent confirms that it can access the host and port of the URL. If the port is busy, it prompts the user to stop the container.
- The agent profile name in AM.
- The AM realm containing the agent profile.
- The path to the file containing the agent password.

#### ***--useResponse***

Run in silent mode by specifying all the responses in the **file-name** file. When this option is used, **agentadmin** runs in non-interactive mode.

#### ***--saveResponse***

Save all the supplied responses in a response file specified by **file-name**.

#### ***--acceptLicense***

Suppress the license agreement prompt. Specifying this option indicates that you have read and accepted the terms stated in the license.

View the license agreement at `/path/to/java_agents/agent_type/legal-notices/Forgerock_License.txt`.

## ***--forceInstall***

Installs a new agent instance, without checking the AM URL or agent URL.

Use this option in deployments with load balancers or reverse proxies, where the URL of the agent and AM can be concealed.

Usage: **agentadmin --forceInstall [--useResponse | --saveResponse *file-name*] [--acceptLicence]**

Before installation, shut down the agent container. If a service on an agent URL is responding, the installer stops with an error.

When the command is used without options, the installation process prompts for the following information:

- Confirmation that you have read and accepted the software license agreement.
- Information about the container installation.
- The URL of the AM instance. The agent confirms that it can log in to AM by using the profile name and password provided during installation. If unsuccessful, the installation stops with an error.

- The URL of the agent instance. The agent confirms that it can access the host and port of the URL. If the port is busy, it prompts the user to stop the container.
- The agent profile name in AM.
- The AM realm containing the agent profile.
- The path to the file containing the agent password.

#### ***--useResponse***

Run in silent mode by specifying all the responses in the **file-name** file. When this option is used, **agentadmin** runs in non-interactive mode.

#### ***--saveResponse***

Save all the supplied responses in a response file specified by **file-name**.

#### ***--acceptLicense***

Suppress the license agreement prompt. Specifying this option indicates that you have read and accepted the terms stated in the license.

View the license agreement at `/path/to/java_agents/agent_type/legal-notices/Forgerock_License.txt`.

### ***--custom-install, --custom***

Installs a new agent instance, specifying advanced configuration options.

Usage: **agentadmin --custom-install [--useResponse | --saveResponse *file-name*] [--acceptLicence]**

#### ***--useResponse***

Run in silent mode by specifying all the responses in the **file-name** file. When this option is used, **agentadmin** runs in non-interactive mode.

#### ***--saveResponse***

Save all the supplied responses in a response file specified by **file-name**.

#### ***--acceptLicense***

Suppress the license agreement prompt. Specifying this option indicates that you have read and accepted the terms stated in the license.

View the license agreement at `/path/to/java_agents/agent_type/legal-notices/Forgerock_License.txt`.

### ***--uninstall, -r***

Uninstalls an existing agent instance.

Usage: **agentadmin --uninstall [--useResponse | --saveResponse *file-name*]**

### **--useResponse**

Run in silent mode by specifying all the responses in the **file-name** file. When this option is used, **agentadmin** runs in non-interactive mode.

### **--saveResponse**

Save all the supplied responses in a response file specified by **file-name**.

### **--version, -v**

Displays the agent version.

Usage: **agentadmin --version**

### **--uninstallAll**

Uninstalls all agent instances.

Usage: **agentadmin --uninstallAll**

### **--listAgents, --list, -l**

Displays information about all configured agents.

Usage: **agentadmin --listAgents**

### **--agentInfo, --info**

Displays information about the agent corresponding to the specified **agent-id**.

Usage: **agentadmin --agentInfo agent-id**

Example: **agentadmin --agentInfo agent\_001**

### **--encrypt**

Encrypts a given string.

Usage: **agentadmin --encrypt agent-instance password-file**

#### **agent-instance**

Agent instance identifier. The encryption functionality requires the use of agent instance specific encryption key present in its configuration file.

#### **password-file**

File containing the password to encrypt.



## `--getEncryptKey, --getKey`

Generates an agent encryption key of 40 characters in length.

Usage: **agentadmin --getEncryptKey**

## `--key`

Generates an agent encryption key of the specified length. For security, generate keys that are about 80 characters long.

Usage: **agentadmin --key *key-length***

## `--d, -d, --decryptAgent, --decrypt`

Reveals the agent password in clear text, for the agent corresponding to the specified **agent-id**.

Usage: **agentadmin --d [*agent-id*]**

Example: **agentadmin --d Agent\_001**

### ***agent-id***

The agent instance. Default: Agent\_001 .

## `--decryptPassword`

Decrypts the agent password, for the agent corresponding to the specified **agent-id**.

Usage: **agentadmin --decryptPassword *encrypted-password encryption-key***

### ***encrypted-password***

Encrypted agent password.

### ***encryption-key***

Key used to encrypt the agent password.

Was this helpful?  