Application Server Administration Guide

Version 2020 R1

webMethods Insight
Powered by
Aurea Actional®

Notices

For details, see the following topics:

- Notices
- Third-party Acknowledgements

Notices

Third-party Acknowledgements

Please see the ‘notices.txt’ file for additional information on third-party components and copies of the applicable third-party licenses.

Table of Contents

Preface

For details, see the following topics:

Preface

This guide describes the use of the Insight Application Server, which is used when running the products on a Jetty platform.

The information in this chapter is specific to the Jetty application server provided by the installer. If you are using a platform other than Jetty, for example Oracle WebLogic or IBM WebSphere, refer to the product documentation for the application server you are using.

About this Documentation

This guide is part of the documentation set for Insight Ent. Edition Server 2020 R1.

Audience for this Guide

This guide is written for system administrators and others who are installing, configuring, and using the products on the Jetty platform.

Conventions

The documents use the following notes and icons to highlight additional aspects, notify you of situations in which special care is required, or to point you to additional sources of information.

Bold face is used to indicate user interface elements, such as names of menus, buttons, windows, and dialog boxes.

`monospace` is used for programming elements, such as code fragments, for system elements, such as file names, paths, and URLs, and for command-line commands.

Emphasis is used to indicate references to related documentation.

1

Introduction

For details, see the following topics:

- Configuring the Application Server

Configuring the Application Server

The information in this section is specific to the Jetty application server provided by the installer. If you are using the product on a platform other than Jetty, for example Oracle WebLogic or IBM WebSphere, refer to the product documentation for the application server you are using.

Using the Application Server Interface

The Administration Program lets you configure the Application Server that hosts that product.

To use the Administration Program:

1. Make sure your application is running.
2. Navigate to the application server's URL. By default this will be:

   `http://[server]:4040/lgserver` for Insight Server

2

Configuration

For details, see the following topics:

- Users and Roles
- Transport
- External Directories
- Certificates
- Global Settings

Users and Roles

The Users & Roles page of the application server console allows you to specify who can access the product, as well as to assign their roles.

To access the Users and Roles page:

By default when you first access the application server administrative interface the **Users & Roles** tab at the top of the page.

Creating Local Users

The Local Users section of the application server console allows you to create users for the application. Depending on the product you are using, the User Details page may appear slightly different, as tiered-administration roles vary for each. The application server administration interface for the Insight Server can be used to create two types of users: administrative users, who are assigned a role from the User Tiered-Admin Role section, and portal users who are assigned permissions from the User Portal Role section. The application server administration interface for CX Monitor Intermediary is used to create administrative users who are assigned a role from the Tiered-Admin Role section.

To create a local user:

1. Click the **Add** button in the **Local Users** section.
2. When the **Create User - User Details** page appears, enter a user name, password and an optional description in the **General Information** section of the page.

3. Select the user's role in the list displayed in the **Roles** section of the page.
4. Click **Finish** to continue.

Creating External Users

The External Users pane allows you to import users from an LDAP directory, as well as to define how those users are granted access to the user interface and to the SOAP APIs. From here, you can configure the LDAP directory that authenticates users, as well as how the LDAP users map to the user tiered-administration roles.

Use this option to authenticate users against an external user directory, to provide the source for the roles, and to map the external users to the predefined roles.

Note that to import users from an LDAP server you must first have at least one LDAP directory server configured. For more details see External Directories.

To configure an LDAP user:

Click **Edit** on the **Configure LDAP Users** section.

Authenticate Users Against LDAP

This feature allows you to enable or disable the feature that authenticates users against an external user directory.

To enable authentication:

1. Specify the LDAP directory to use to authenticate users.
2. Select the role source.
3. Optionally, specify the role overrides.
4. Click the **Enable** button. The authentication button turns green (Enabled).

Disabling Authentication

If the authentication of users against an external directory is enabled, the locally defined users will not be used. If the authentication feature is disabled, authentication returns to using the locally defined users.

To disable authentication:

1. Click the **Disable** button
2. The authentication button turns red (Disabled).

LDAP Directory

Insight Server used the LDAP configuration to authenticate users and to retrieve user role information. You must already have configured a user directory on the External Directories tab. See External Directories for more information.

Role Source

Use the Edit button in the Role Source page to determine the user role. Available options are:

- **Local**: User's roles are defined locally. Mappings must be created from the LDAP User to the predefined roles using the LDAP User to Role Mapping pane
- **Groups**: User's roles are obtained through the LDAP users' groups. The external LDAP groups can be overridden using the Role Override pane
- **Attribute**: User's roles are obtained from the specified User Entity attribute

To define the role mapping for an external user:

1. Click **Edit** in the **Role Source** pane.
2. In the **External User - Role Mapping** pane, select the option button to define how you want to map this user (locally, by group, or by attribute).
3. When you select the mapping option, the external user is thus mapped.

Role Override

Use the Edit option in the Role Override pane to specify the external LDAP groups that will be mapped to the predefined roles. For example, if all users belonging to the external directory group “Group_A” are to be granted the Admin role when accessing this product, the predefined Admin role is overridden with “Group_A.”

If necessary you can map multiple LDAP groups to a single role by entering a comma-separated list of the applicable groups in the text field.

Configure LDAP User to Role Mapping

The Configure LDAP User to Role Mapping pane allows you to specify the user tiered-administration roles to which LDAP users will map. The users configured in this list are only used when the authentication of users against LDAP is enabled and the user-to-role mapping is done locally.

Use the Role Mapping page to specify the role to which a given LDAP user will map.

Note: Multiple users cannot be defined with the same name. This includes, collectively, the local users created in the Define Local Users pane and the users created in the LDAP User to Role Mapping pane.

To define role mapping for an LDAP user

1. Click **Edit** in the **Configure LDAP User to Role Mapping** pane.
2. Click the **Add** button, and enter the name of the LDAP user and its description.
3. Select the user tiered-administration role to which the user is mapped.

Defining Roles

When a new role is created in an instance of CX Monitor Intermediary, Insight Agent or Insight Server running in standalone mode, that role must be added to Jetty's list of defined roles before it can be used.

To add a role to Jetty:

1. Log in to the application server.
2. If necessary click on the **Users & Roles** tab at the top of the page.
3. In the **Roles** section click on the **Add** button.
4. In the **Roles - Administration** page enter a name and description for the new role. The name must match the name you entered when defining the role at the application level. Click on the **Finish** button to confirm the new role.
5. When the **Users & Roles** page reappears you will see the new role listed in Jetty's list of defined roles; you can now start using the newly-created role within your application.

Transport

Use the Transport tab to view, add or modify listeners. Listeners are HTTP or HTTPS connections belonging to the application server.

To view the existing listeners, click on the Transport tab. You will see at least one HTTP listener, the one you are using to connect to the application server. It was defined when you ran the Initial Configuration Wizard for the product you have installed.

You can have as many listeners defined for the application server as you have port numbers available.

Note: The Jetty class involved with these parameters is org.mortbay.http.SocketListener.

To add a listener:

1. Click **Add** in the **Listeners** pane. The **Create HTTP/S Listener - Protocol Wizard** appears.
2. Select the protocol for the new listener and click **Next**.
3. Enter a **Name** and **Description** for your new protocol.
4. Provide values for the following parameters:

Parameter	Description
Host	This setting lets you determine a specific IP address or host name to associate the current listener with. If this is not specified, the listener will be active on all active interfaces. You can use this setting to limit access to the listener from certain machines only; for example, setting this parameter to “localhost” will cause the listener to only accept calls from the local machine and ignore calls coming from other network interfaces.
Port	The port number used by the listener.
Maximum Idle Time	The maximum time (in milliseconds) indicating how long a thread can be idle after its task has been completed or cancelled and before it is destroyed. If Maximum Idle Time value is increased, then the Maximum Number of Threads value should be increased also, especially in a high-concurrency environment.
Minimum Number of Threads	The minimum number of threads available to Jetty application server. Default value is 5 and should never be less than that.
Maximum Number of Threads	The maximum number of threads available to Jetty application server. Default value is 10. If your server is of high capacity, the Maximum Number of Threads can be increased. However, more threads may result in a decrease in server performance.
Select a Server Certificate (required)	HTTPS listeners only. When you create a new HTTPS listener, that listener needs to use an SSL certificate which must be previously registered with the server (see Key Server Certificates for more information). A list of available server certificates will then be available for you to choose from.
Require a Client Certificate	HTTPS listeners only. Select this checkbox to require that clients of the new listener submit a client certificate with each request.

Parameter	Description
Idle Connection Low Resource Timeout	HTTPS listeners only. The amount of time after which idle connections can be dropped when the application server is in a low-resource situation, for example when experiencing a high volume of incoming calls.
Enabled Cipher Suites	Type a comma or line feed separated list of the SSL cipher suites you want to enable and list them in order of preference from most preferred to least. This list will overwrite the default list of supported cipher suites, which will allow you to enable cipher suites that are not enabled by the JSSE provider and disable cipher suites that are enabled by the JSSE provider. For a list of the available supported cipher suites that can be used, see the JSSE provider's documentation. If you want to use the defaults provided by the JVM, leave the list empty.
Excluded SSL Protocols	Comma or line feed-separated list of SSL protocols to be excluded. Leave the list empty to use the default list of SSL protocols.

5. Click **Finish**.

Editing an Existing Listener

To edit an existing listener:

1. Click on the **Transport** tab.
2. Click on the listener you want to edit. The listener details page will be displayed.
3. To edit a setting, click on the **Edit** button at the top right of the **General Information** or **Configuration** sections.

External Directories

The External Directories tab allows you to add an external directory or to edit an existing one.

Adding an External Directory

The following procedures allow you to configure external directories.

To add an external directory:

1. Click Add in the External Directories pane.
2. Specify the type of user directory.
3. Provide a name and description for the user directory.
4. Provide credentials for the user directory.

Select External User Directory

The External User Directory page allows you to identify an external directory to use for your database. To use another directory you must select an external user directory type and then define the directory's connection parameters.

External User Directory Definition

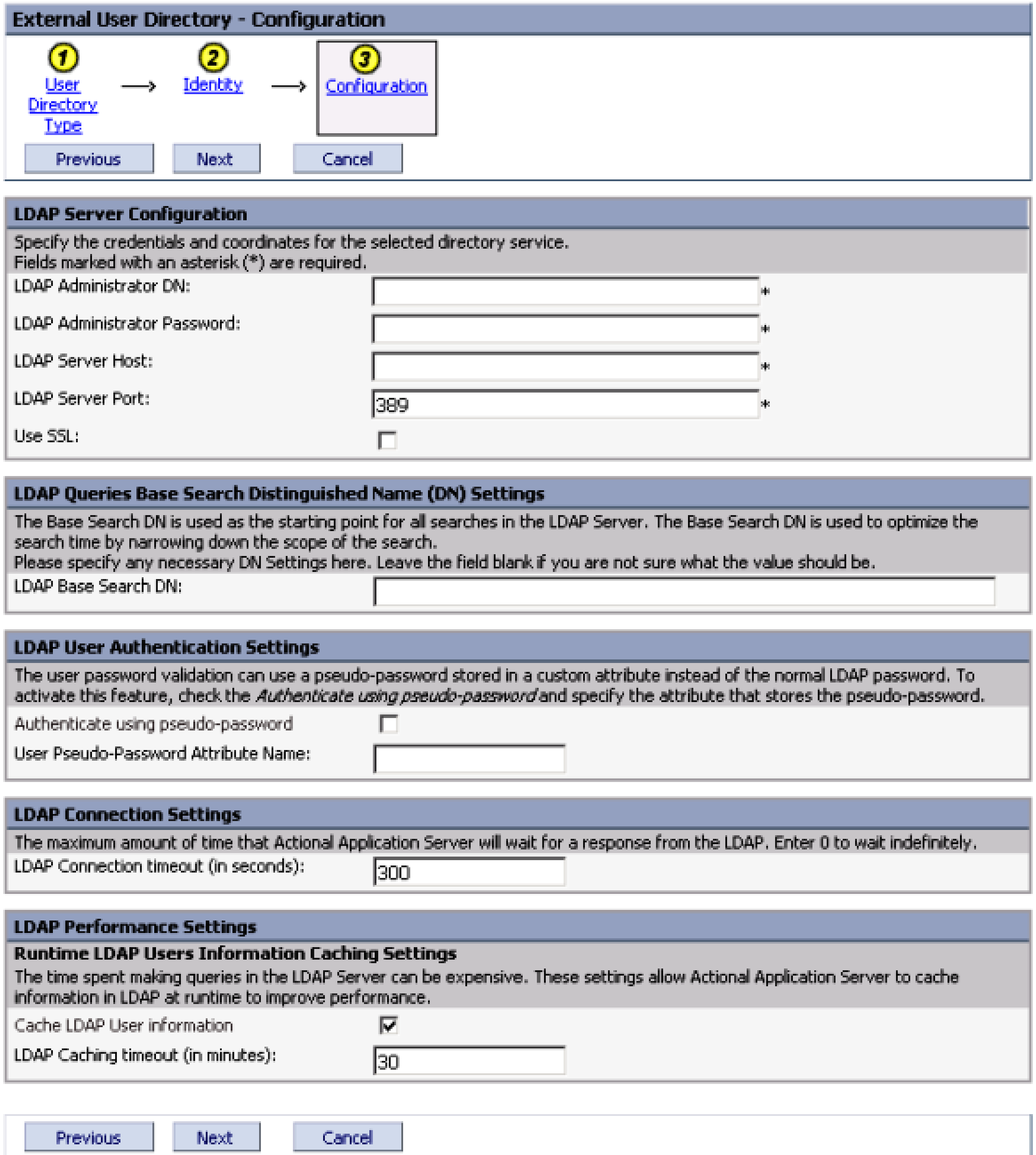
You must provide a database name and, optionally, a description for each external directory.

To identify the external directory:

1. In the **Name** field, assign a name to the external directory.
2. In the **Description** field, enter any additional free-form information about the directory to help you identify it later.
3. Click **Next**.

Credentials and Configuration

Specify the credentials and coordinates for the selected directory service.



Certificates

Key Server Certificates

The Key Certificates page displays a list of certificates that have been imported into the product. The list provides information on the certificates and provides a means for you to import, delete, or export certificates.

Importing a Key Server Certificate

To import a Key Server Certificate:

1. Click Import Certificate in the Key Server Certificate area to activate the wizard.
2. Enter the following information in the appropriate fields:
   - **File for Import**: Enter, or browse to, a certificate file to import.
   - **Certificate Password**: Enter the certificate's password.
3. Complete the wizard.

Exporting a Key Server Certificate

To export a Key Server Certificate:

1. In the **Key Server Certificate** page, click the **Export** link associated with the certificate you wish to export..
2. Type in the **Certificate Password** for the certificate, confirm the password and click **Next**.
3. Click the **DownLoad Key Certificate** link to specify the location for the certificate, and click **Finish**.

Certificate Signing Requests

The Certificate Signing Requests page allows you to create CSRs and import their replies.

Create Certificate Signing Requests

To create a Certificate Signing Request:

1. Click the **Certificate Signing Requests** tab.
2. Click the **Create CSR** button.
3. Complete the fields to specify the set of attributes for the certificate singing request.

   Refer to your own Certificate Authority (CA) as to the manner in which these fields are to be filled. The first and last name should match the Web site or the hostname for some tools, for example, Internet Explorer, to verify the certificate.
4. In the **Key Size** list, click the key length for the generated CSR.
5. Complete the CSR credentials to define the CSR password.
   - Type in an **Alias**, for example, `productCA`.
   - Type in the **Certificate Password**.

- Retype the certificate's password to confirm the password.

6. Click **Finish** to create the CSR. A private/public key pair is created under the alias named lgserver and wraps the public key in a self-signed X.509 certificate.
7. Click the **Download CSR** link to specify the location for the CSR.
8. Select a location to save the generated CSR.
9. Click **OK** to have the new CSR appear in the list.

Export a CSR

After the CSR has been created, you have to export the CSR. Otherwise, the pending request will be removed and you will have to delete the existing key.

To export a CSR:

1. In the **Status** window, select the **Download CSR** link to export the request.
2. Click the **DownLoad CSR** link to specify the location for the request.

Trusted Certificate Authorities

To import, export, or delete trusted certificate authorities for use in Looking Glass, select the Trusted Certificate Authorities tab.

You can review the details of the Trusted CA by clicking on the Issued To: link. The details page appears. To return to the list, click Done.

The Trusted Certicate Authorities page displays the following information:

Column	Description
Issued To	The name or the DN of the Certificate Authority that this certificate identifies.
Issued By	The name or the DN of the Certificate Authority that signed this certificate.
Expiry Date	The date the Trusted CA authorization expires.
Export	Link provided to download the Trusted CA certificate to another location.

Import a Trusted CA

To import a Trusted CA:

1. Click **Import** to activate the Import Trusted CA wizard.
2. Specify, or **Browse** to, the Trusted CA file to import. More than one certificate can be stored in a single file in the following formats:
   - X.509DER encoded binary (.CER)
   - X.509 Base-64 encoded ASCII (.CER)
   - Cryptographic Message Syntax Standard - PKCS#7 Certificates (.P7B)
3. Click **Next** to view the trusted CA's contents.
4. Click **Finish** for the new certificate appears in the list.

Export a Trusted CA

You can export a Trusted CA and then import it to another location.

To export a Trusted CA:

1. Click the **Export** link associated with the Trusted CA to export.
2. Click the **DownLoad Trusted CA Certificate** link to specify the location for the certificate.
3. Select what you would like done with the new certificate and click **Finish**. You can now import the certificate to a different product using the instructions in Import a Trusted CA.
4. Click **Finish**.

Delete a Trusted CA

If you are no longer using a Trusted CA, you should update this list of Trusted CAs.

To delete a Trusted CA:

1. Select the option box for the Trusted CA to delete.
2. Click **Delete** to remove the Trusted CA from the list.

Certificate Revocation List

The Certificate Revocation List (CRL) is a list of subscribers paired with a digital certificate status. This list allows clients and servers to verify whether the entity they are accessing has a valid certificate. The CRL is a binary file and contains the following information:

- A list of revoked certificates along with the reason(s) for revocation
- The dates of certificate issue and the CRL issue,
- Proposed date when the next version of the CRL will be published
- The validity status of the CRL

Upon receiving a TLS connection, and if a client certificate is required, the application server verifies if the CRLs have expired. If an expired CRL was originally uploaded from a URL, it will attempt to reload it. If the reloading fails, it logs an error, but does not throw an exception. It will not attempt to reload an expired CRL again until at least 5 minutes have elapsed since a previous failure occurred.

To import a Certificate Revocation List:

1. Click the **Certificate Revocation List** tab.
2. Cick **Import**.
3. Do one of the following:
   - In the **CRL URL** box, type the endpoint URL for the CRL.
   - In the **File for Import** box, type the file name and path to the CRL file or click **Browse** to select the file.
4. Click **Next**.

   You can then view the CRL's contents.
5. Click **Finish**.

Delete a Certificate Revocation List

If you are no longer using a CRL, you should update this list.

To delete a CRL:

1. Select the option box for the CRL to delete.
2. Click **Delete**. The CRL is removed from the list.

Global Settings

Use the Global Settings tab to access the default SSL protocol using the application server user interface.

Note: Changing the default SSL Protocol requires a restart for the SSL change to take effect.

To edit a protocol on the application server:

1. Log in to the application server.
2. Click on the **Global Settings** tab at the top-right of the page.
3. Click **Edit** to change the default SSL Protocol for outbound communication such as SSL over LDAP to a valid SSL protocol supported by the JVM.