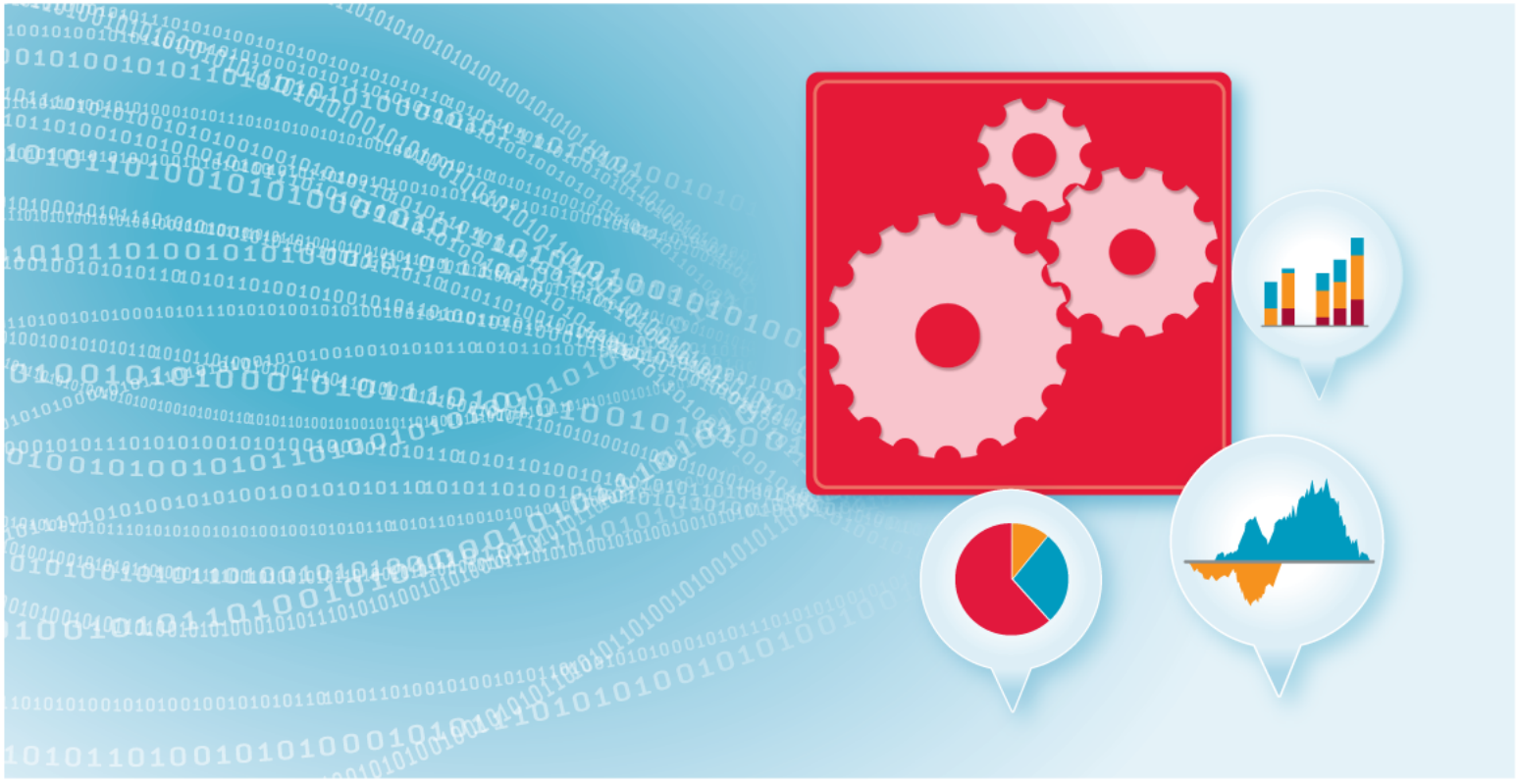


LAVASTORM analytics

Administration Guide

Lavastorm Analytics Engine 6.1.1

Legal notice

Copyright

Disclaimer

No representation, warranty or understanding is made or given by this document or the information contained within it and no representation is made that the information contained in this document is complete, up to date or accurate. In no event shall LAVASTORM ANALYTICS be liable for incidental or consequential damages in connection with, or arising from its use, whether LAVASTORM ANALYTICS was made aware of the probability of such loss arising or not.

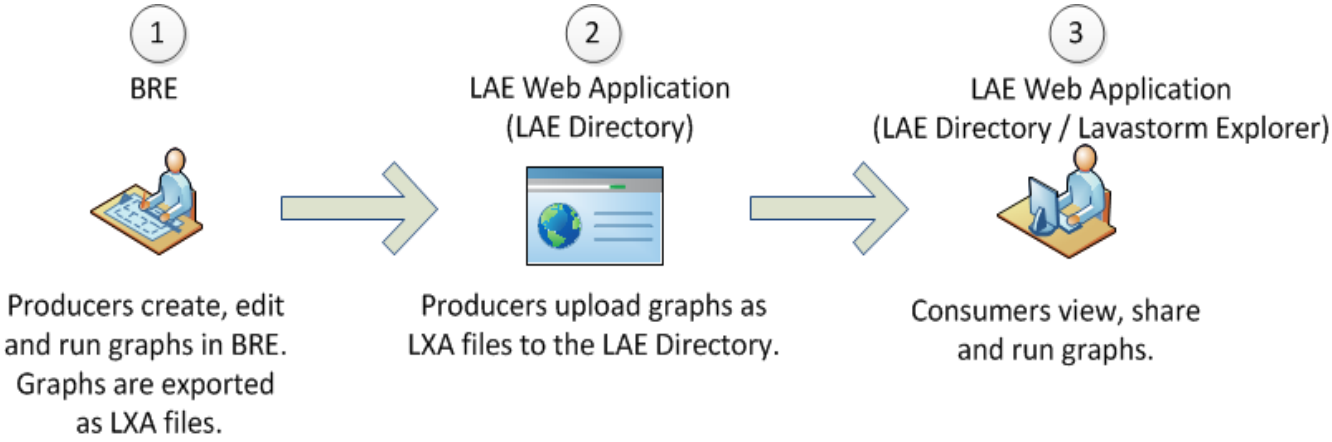
Legend

✓	Indicates a prerequisite.
•	Indicates an unordered list.
◊	Indicates a procedure with only one step.
1. 2.	Indicates a procedure with multiple steps.
»	Indicates the result of a procedure.
	Indicates a note. A note highlights important information.
	Indicates a tip. A tip gives you hints, for example, alternative methods for completing a task.
	Indicates a caution.
Bold text	Indicates user interface text.
`Code font`	Indicates code or system commands.
Menu > Menu item	Indicates navigation to a menu or sub menu item.
Link	Indicates a cross-reference to a section within the current document, or a link to an external document.
EXAMPLE	Indicates an example.
Image caption	Indicates an image caption.

Table of contents

Welcome to the LAE 6.1.1 administration guide

This document guides you through the main administrator user functions of Lavastorm Analytics Engine (LAE) 6.1.1, provided through the LAE Directory and Logistics Manager. The LAE Directory constitutes one part of the LAE Web Application.



Overview of the steps that enable users to view and run graphs in the LAE Web Application

LAE Directory

The first part of this document guides you through the administrator functions of the LAE Directory. As an administrator, you can perform the following functions in the LAE Directory:

- Upload libraries, see Uploading libraries to the LAE Directory on page 11.
- Import LDAP or Active Directory users and groups, see Importing LDAP/AD users and groups on page 15.
- Synchronize users and groups with LDAP or Active Directory, see Synchronizing LDAP/AD users and groups on page 21.
- Create local users, see Managing LAE Web Application users on page 22
- Create local groups, see Managing LAE Web Application groups on page 26.
- Edit or delete local users, see Viewing and editing users on page 23
- Edit or delete local groups, see Viewing and editing groups on page 27.

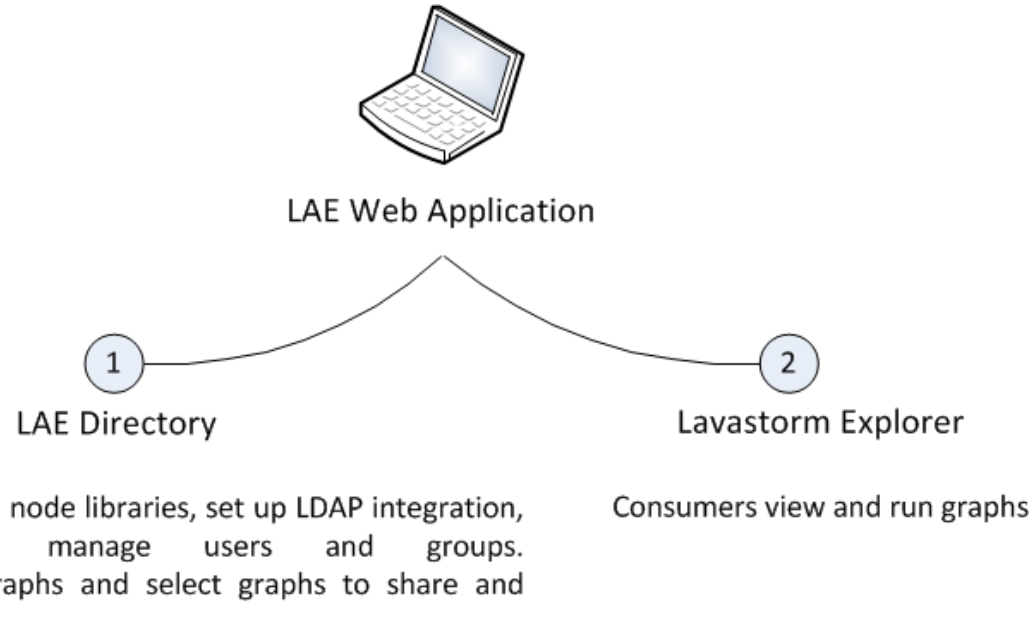
The "LAE configuration settings" chapter guides you through the LAE configuration settings that modify the behaviour of the LAE Directory for end users, including:

- Showing or hiding all documents on page 29
- Showing or hiding graph run data on page 30

- Editing the token refresh period on page 31.

  In this chapter, you can also find information on the following topics:

- Configuring LDAP/AD authentication settings on page 32.
- Administering the security store on page 34



Overview of the LAE Web Application which is composed of the LAE Directory and Lavastorm Explorer

Logistics Manager

The second part of this document guides you through the main functions of the Logistics Manager UI and API, including how to perform the following functions:

- Access Logistics Manager, see Scheduling graph runs on page 38.
- Upload Lavastorm Execution Archives (LXAs) to the web server, see Deploying an LXA file on page 40.
- Define parameter sets for a given LXA, see Defining parameter sets on page 41.
- Create an execution plan, see Creating an execution plan on page 43.
- Create run definitions for execution plans, see Creating run definitions on page 44.
- Enable execution plans, see Enabling an execution plan or a run definition on page 47.
- Examine the output of each run and access its logs, see Viewing run logs and output on page 48.
- Generate a link to view a graph in Lavastorm Explorer, see Generating a graph link on page 54.

1. LAE Directory overview

The LAE Web Application is comprised of the LAE Directory and Lavastorm Explorer. The LAE Directory is where users can select and import graphs ready for viewing in Lavastorm Explorer. As a user with the role of administrator, you can configure and manage LDAP/AD server integration and create and manage local users and groups in the LAE Directory.

After initial log in, the first steps to working with the LAE Directory are to change your password and then to upload node libraries, see Logging in to the LAE Directory below and Uploading libraries to the LAE Directory on page 11.

1.1 Logging in to the LAE Directory

Note: You must have browser cookies enabled in order to authenticate in the LAE Web Application.

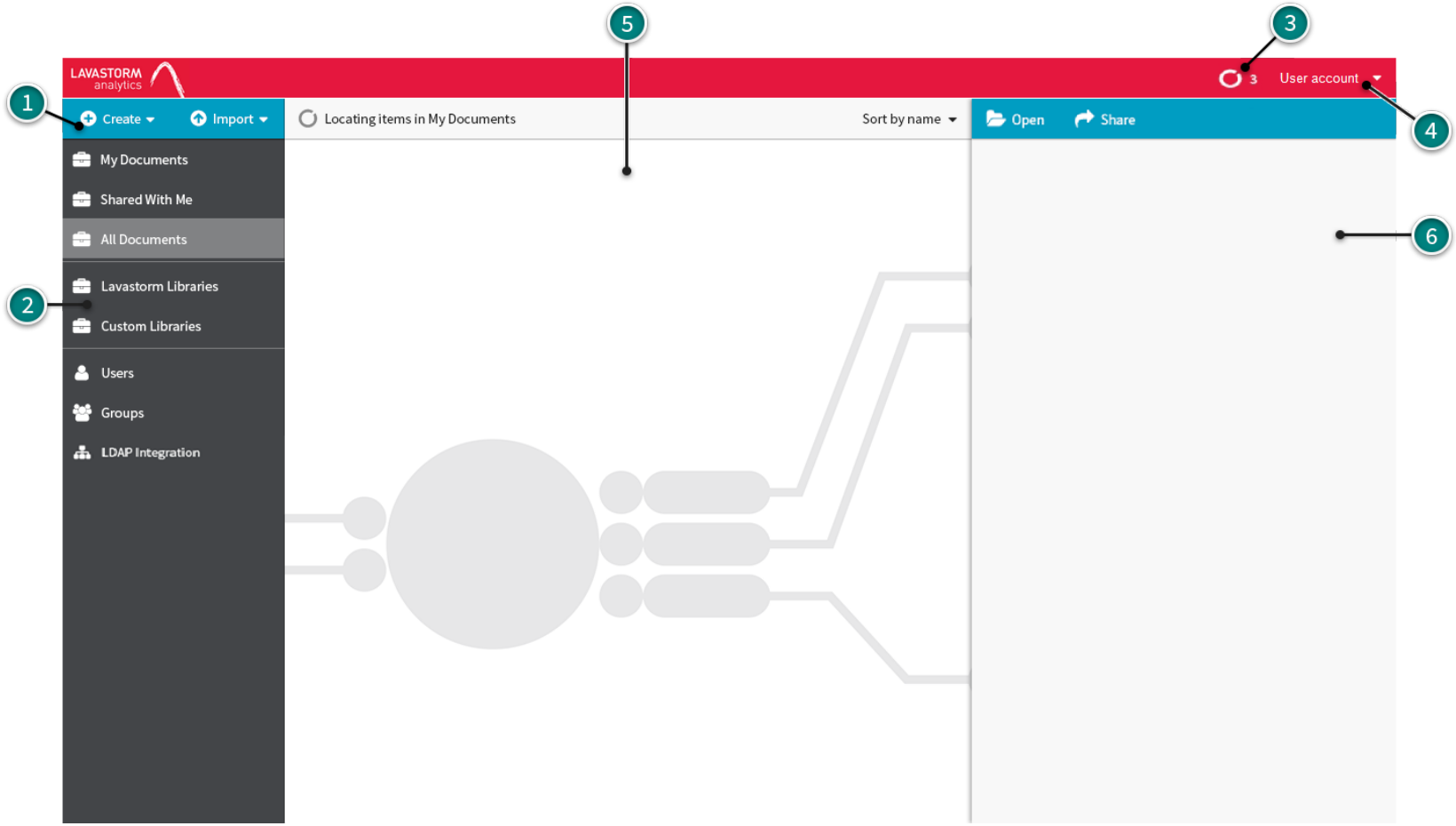
1. Navigate to the LAE Web Application.
2. Enter your username and password to log in to your Lavastorm Analytics Engine (LAE) account.
   » The LAE Directory opens.

Caution: We recommend that you change your password the first time that you log in to the LAE Directory. To change your password, select your username from the list of users and click the **Change password** button, see Changing user passwords on page 24 for more information.

Note: Depending on the options taken during installation, you may be asked to enter the security store password after initializing the LAE Web Application (before you reach the login screen). If you chose to store the security store password during installation, then it will be stored as an encrypted value within both the web-conf/site.prop and the conf/site.prop configuration files under the `ls.lae.security.secureStorePassword` property, and you will not be asked to enter the security store password when the LAE Web Application initializes.

See Administering the security store on page 34.

The following screen shot gives an overview of the LAE Directory user interface for users with the role of administrator.



Overview of the LAE Directory user interface (administrator users)

(1) Create button: Create local users and/or groups

(2) Collections pane: Select an option to view related items in the Items pane

(3) Notifications indicator: Shows progress of background tasks

(4) Account menu: Click to log out

(5) Items pane: Displays a list of available items related to the option that is selected in the collections pane

(6) Details pane: Displays details of selected item

2. Uploading libraries to the LAE Directory

✓ You have logged in to the LAE Directory, see Logging in to the LAE Directory on page 9.

Before you begin working with the LAE Web Application, you must first upload the three Lavastorm node libraries (core, InFlow and LAL1). You should also import any custom libraries that you have created that are used by your graphs.

1. Click the **Import** button.

2. Select **Node Library**.

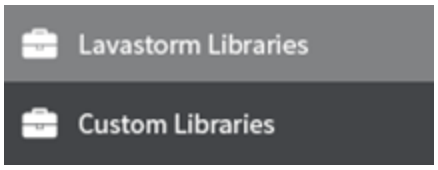
3. Select the .BRG files that you wish to import.

> **Note:** Node libraries can only be imported to the LAE Directory as .BRG files. The Lavastorm node libraries can be found in the following folder: *<LAE Server installation location>*/Lavastorm/LAE/lib/brain/brg, and must be imported in the following order:
> 1. Core
> 2. InFlow
> 3. LAL1

4. Select whether you want to save the library within the **Lavastorm Libraries** collection or the **Custom Libraries** collection.

> **Tip:** The **Lavastorm Libraries** and the **Custom Libraries** collections are shared workspaces. Nodes from these shared workspaces are available for all graphs.

5. When the import is complete, from the collections pane, click **Lavastorm Libraries** or **Custom Libraries** to view a list of available nodes.



3. Importing graphs into the LAE Directory

✓ You have logged in to the LAE Directory, see Logging in to the LAE Directory on page 9.

Note: It is only possible to import graphs in LXA (executable) file format.

1. From the left side of the screen, click the **Import** button.

2. Select **Graph**.
3. Navigate to the LXA ; file that you want to import and select it.
   » The graph is imported to the LAE Directory and is listed in your **My Documents** collection.

Tip: If you are the owner of a graph, you can import a new version at any time. To import a new version of your graph, follow the steps described above and select the new version of your graph.

Note: If your graph contains nodes from custom libraries, ensure that all custom libraries have been uploaded to the LAE Directory, see Uploading libraries to the LAE Directory on page 11. If a graph uses custom libraries that have not been uploaded to the LAE Directory, the graph import will fail.

4. LDAP/AD integration

To integrate LAE with your LDAP/AD source system, you must:

1. Setup LDAP/AD authentication.

   During installation, you may have configured LAE to authenticate your users via LDAP/AD. If you did not setup LDAP/AD authentication during installation, and you wish to setup or edit LDAP/AD authentication settings after installation, you can configure the relevant properties in the web-conf/site.prop configuration file, see Configuring LDAP/AD authentication settings on page 32.

2. Import LDAP/AD users to LAE.

   To complete the integration of LAE with your LDAP/AD source system, you must import users to LAE from the source LDAP/AD system, see Importing LDAP/AD users and groups on page 15. During the import, you have the option to:

   - Import LDAP/AD groups. For example, you may want to import an existing LDAP/AD group and assign specific rights to all members of that group, once the users have also been imported to LAE. See Importing LDAP/AD users and groups on page 15
   - Apply an advanced filter to limit the LDAP/AD import to specific users/groups, see Applying an advanced filter on page 18.
   - Import users and groups via a secure LDAPS connection, see Importing users and groups via a secure LDAPS connection on page 16
   - Set a paging limit to ensure that LAE is aligned with your LDAP/AD source system, see Setting a paging limit on page 16

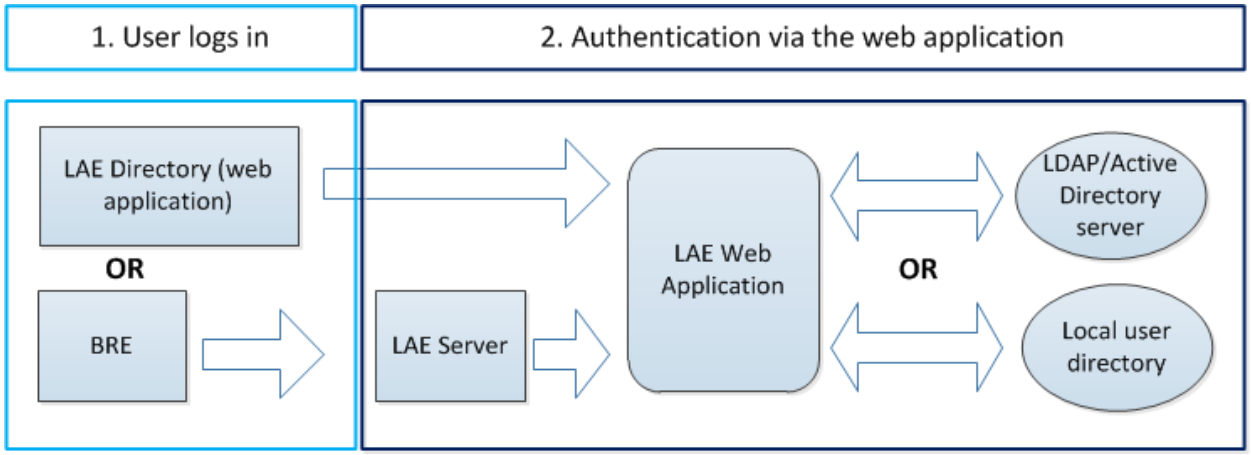
When you have completed the LDAP/AD integration setup (as per the steps above), you can run manual LDAP/AD synchronizations at any time after setup through the LAE Web Application to ensure that LAE has the latest user and group information. For example, once you have completed an initial LDAP/AD import, you may perform a synchronization task at a later date to add new LDAP/AD users to LAE if they have been added to the source system after the initial LDAP/AD import was performed. See Synchronizing LDAP/AD users and groups on page 21

Tip: Whilst it is not possible to automate synchronizations through the LAE Web Application, it is achievable through the use of Lavastorm APIs by using a graph to perform the synchronization and automating the process with Logistics Manager.

LAE authentication overview

LAE users can be either imported from an external LDAP or Active Directory (AD) system, or created manually in the web application by a user with the role of administrator.

User authentication is orchestrated by the web application, regardless of whether a user logs in to LAE from BRE, or if a user logs in via the LAE Directory page of the Web Application. For LDAP/AD imported users, authentication occurs via the LDAP/AD server. For manually created users, authentication occurs locally in the Web Application. When a user logs in via BRE, their credentials are transmitted from BRE to the LAE server, which then communicates with the LAE Web Application to perform user authentication through either the configured LDAP/AD server or through the local user directory.



Subsequent communications between the LAE Web Application server and the LAE server(s) is authenticated using host-based authentication, see the LAE Enterprise or Windows Server installation guides for more information.

4.1 Importing LDAP/AD users and groups

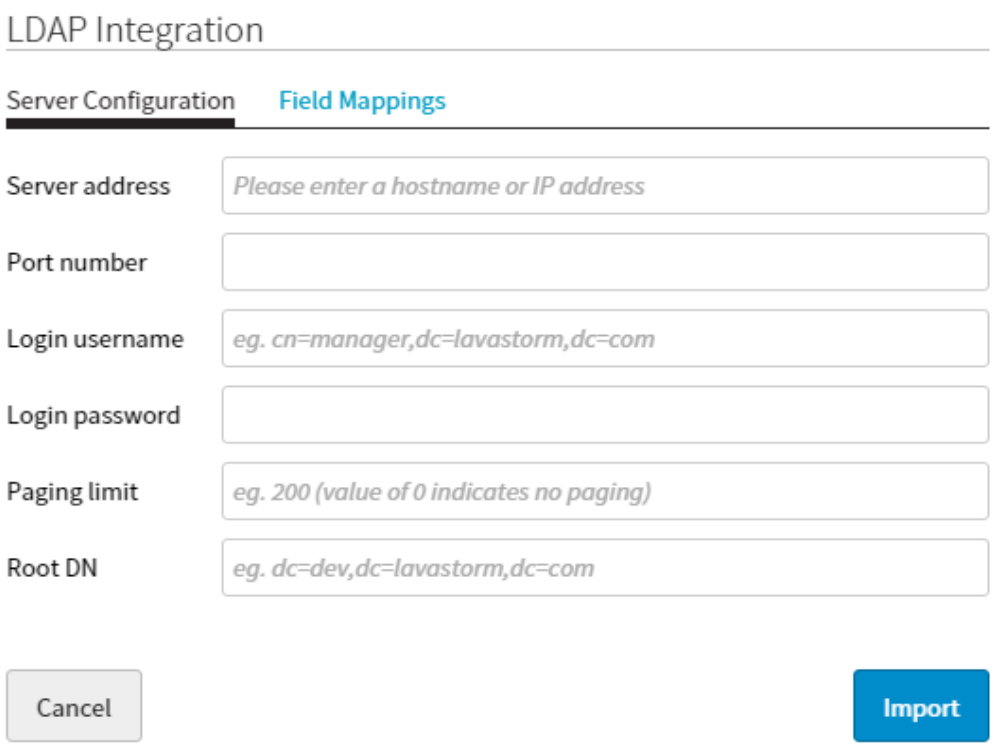
✓ You have logged in to the LAE Directory as an administrator, see Logging in to the LAE Directory on page 9.

This topic assumes that you have not yet imported any LDAP/AD users or groups. If you have already completed an import and wish to run an LDAP/AD synchronization, see Synchronizing LDAP/AD users and groups on page 21.

As an administrator, you can import users and groups from an LDAP or AD server to the LAE Directory. This allows users to log in to LAE with their existing LDAP/AD credentials.

1. From the collections pane, click **LDAP Integration**.

» The **LDAP Integration** dialog box opens.

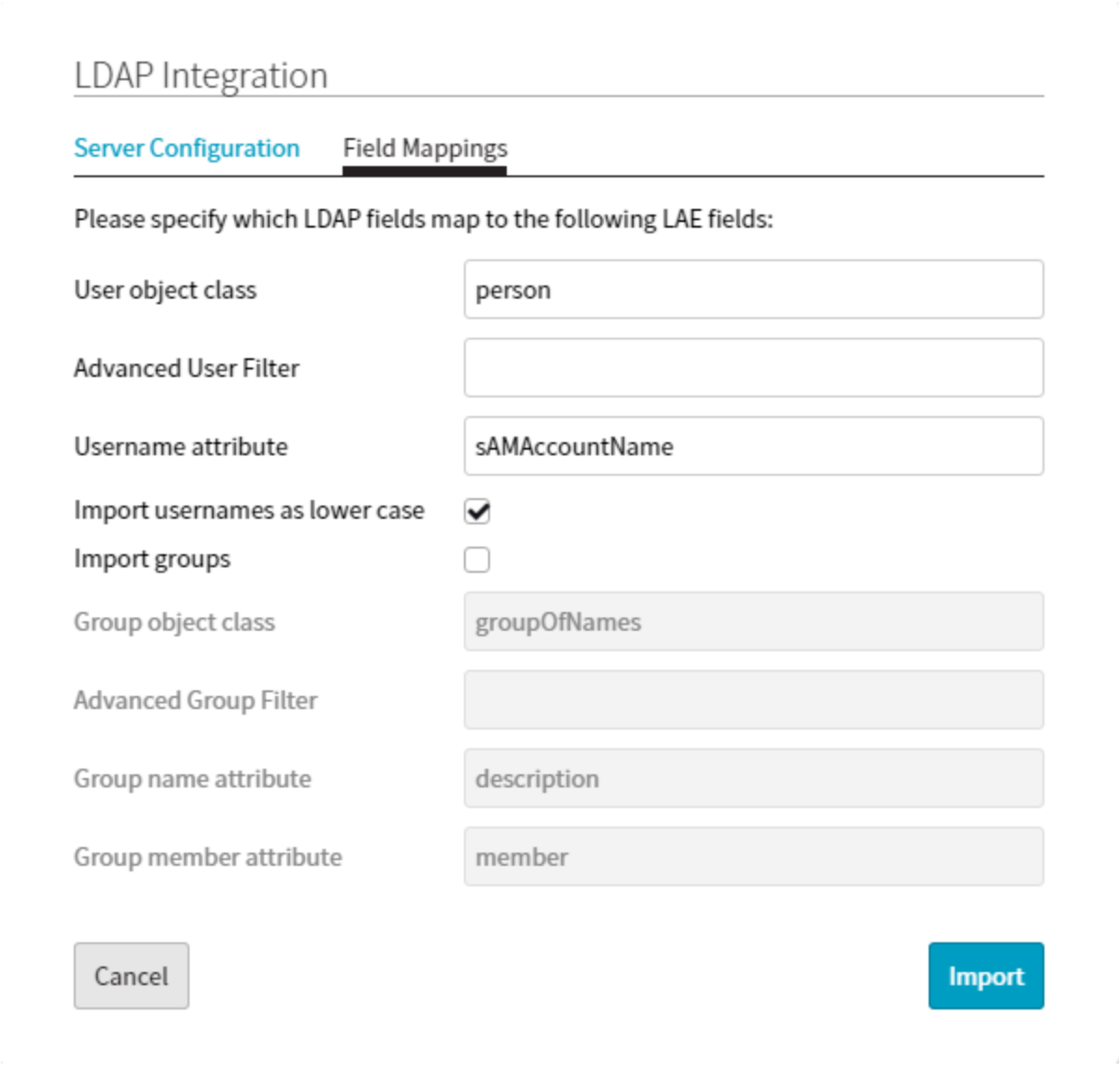


2. Enter the connection details for your LDAP/AD server, as per the examples in the following table.

Server Configuration value	Description
Server address	Enter your server address. **EXAMPLE:** lavastorm.com ### Importing users and groups via a secure LDAPS connection You can ensure that all import requests are performed over a secure connection by including the "`ldaps://`" protocol as a prefix in the server address field. **EXAMPLE:** ldaps://lavastorm.com You must also ensure that security certificates are installed on both your source LDAP/AD server and the LAE web server. Please refer to your vendor's documentation on how to install security certificates.
Port number	Enter your port number. If you have chosen to set up a secure LDAPS connection, you must ensure that the port number corresponds to the LDAPS port number on the LDAP server.
Login username	Enter the LDAP/AD binding username that you wish to use during the import. **EXAMPLE:** CN=User,DC=lavastorm,DC=com
Login password	Enter the password that corresponds to the username provided.
Paging limit	### Setting a paging limit To allow data to be handled in set sizes and thus avoid slowing down the LDAP/AD system when handling large data sets, paging limits are often set on LDAP/AD systems. You must align LAE with your source system by entering a paging limit that is the same or less than the paging limit that is set on your LDAP/AD source system. Please contact your LDAP/AD administrator regarding the paging limit that is set on your source system. **EXAMPLE:** If your source system specifies a paging limit of "5", and you set a paging limit of "0" (unlimited) in LAE, you would receive an error because this is greater than the paging limit of "5" that is specified on the source system. Similarly, if you specified a paging limit of "10" in LAE, you would receive an error stating that you have exceeded the page limit size that is set in the source system. By entering a paging limit of "5" or less in LAE, the import would complete successfully, as this corresponds to the paging limit that is set on the source system.

Server Configuration value	Description
Root DN	Enter the root DN of your source system from which you want to import users and groups. **EXAMPLE:** OU=Finance,DC=lavastorm,DC=com

3. Select the **Field Mappings** tab and enter the relevant values for your LDAP/AD implementation, as per the examples in the following table.



Field Mappings value	Description
User object class	The user object class identifies what a user is within the LDAP/AD system. Note that the **User object class** is ignored if the **Advanced User Filter** is set. **EXAMPLE:** If you enter a user object class of 'person', this will identify all objects in LDAP/AD as users if the objectClass attribute = 'person'.
Advanced User Filter / Advanced Group Filter	## Applying an advanced filter We recommend that you apply an advanced filter to limit the LDAP/AD import to specific users and/or groups by using standard LDAP query syntax to ensure that you only import users who require access to LAE. To apply a filter, type an LDAP query in the **Advanced User Filter** and **Advanced Group Filter** fields, as required. ### Filtering for multiple attributes **EXAMPLE:** `(&(objectClass=person)(memberOf=CN=LAE Users Group,dc=lavastorm,dc=com))` This query would import objects that have an objectClass attribute of "person" AND are member of the "LAE Users Group". ### Filtering to exclude an attribute **EXAMPLE:** `(&(!(|(ou:dn:=ResearchAndDevelopment)(ou:dn:=HumanResources)))(objectClass=person))` This query would import all objects that have an objectClass attribute of "person", and would exclude objects that have an Organizational Unit attribute of "HumanResources" OR "ResearchAndDevelopment". ### Using the wildcard operator **EXAMPLE:** `(objectClass=*)` This query would import all objects that have the objectClass attribute populated with a value. **Note:** Entering an **Advanced User Filter** will override the **User object class**. Similarly, entering an **Advanced Group Filter** will override the **Group object class**.
Username attribute	## Entering a valid "username attribute" If your source system is AD, you should enter either: • `userPrincipalName` - Or -

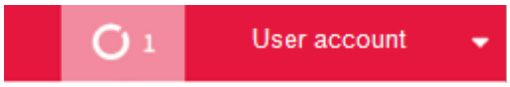
Field Mappings value	Description
	• `sAMAccountName` If you use `sAMAccountName`, then the "domain" property must be correctly set in the web-conf/site.prop file, such that the combination of the login username value, the '@' symbol, and the "domain" property match that of the `userPrincipalName` when looked up in Active Directory. See Configuring LDAP/AD authentication settings on page 32 If your LDAP/AD server is a non-AD system, such as OpenLDAP, you can enter any attribute against the user, for example: **EXAMPLE:** `uid` You must ensure that the **Username attribute** value that you enter matches the attribute used in the userSearchFilter property, see Configuring LDAP/AD authentication settings on page 32.
Import usernames as lower case	When integrating with an LDAP/AD system that performs case insensitive authentication, you may wish to import usernames as lower case. If you select this option, users will be able to enter their login username in lower case and still access the system. However, if you do not select this option, usernames will be imported in their original case. **EXAMPLE:** Username set to "aUser" on AD: • If **Import usernames as lower case** is not selected, users can only access LAE with the 'aUser' login name (case sensitive). • If **Import usernames as lower case** is selected, users can only access LAE with the 'auser' login name (lowercase only).
Import groups	Select **import groups** if you want to import groups as well as users.
Group object class	The group object class identifies what a group is within the LDAP/AD system. Note that the **Group object class** is ignored if the **Advanced Group Filter** is set. **EXAMPLE:** If you enter a group object class of 'groupOfNames', this will identify all objects in LDAP/AD as groups if the objectClass attribute = 'groupOfNames'.
Group name attribute	The value that you specify here will be used as the group name within LAE.

Field Mappings value	Description
Group member attribute	For each group that is found, the **Group member attribute** identifies members of the group.

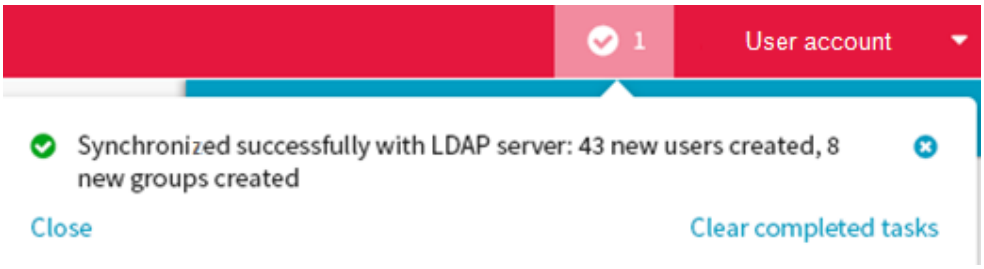
4. Click the **Import** button to import users and groups from your LDAP/AD server.

   Import

   » The notifications indicator shows that the LDAP integration task is in progress.

   » When the import is complete, the notification panel shows a summary of the import.

Tip: If the import task does not complete successfully, the notifications panel displays a summary of the errors. You can view the error details by clicking the **Show details** link.

After you have completed the initial LDAP import, you can synchronize LAE users and groups with your LDAP/AD server at any time, see Synchronizing LDAP/AD users and groups on the facing page.

Note: LDAP/AD authentication connection settings are managed separately to the LDAP import and synchronization settings and are configured in the web-conf/site.prop file, located at `<LAE Web Application Install Directory>/web-conf/site.prop`. See .

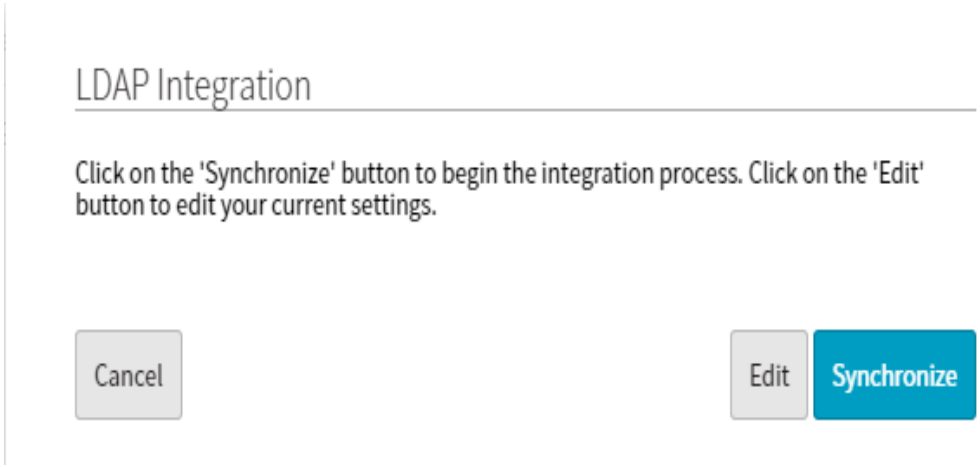
4.2 Synchronizing LDAP/AD users and groups

✓ You have imported users and groups from an LDAP/AD server see Importing LDAP/AD users and groups on page 15.

You can synchronize LAE users and groups with your LDAP/AD server at any time to ensure that the LAE Web Application has the latest user account information.

1. From the collections pane, click **LDAP Integration**.

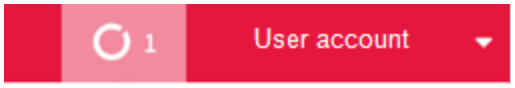
» The **LDAP Integration** dialog box opens.



Tip: You can edit your LDAP/AD server configuration by clicking the **Edit** button.

2. Click the **Synchronize** button.

» The notifications indicator shows that the LDAP/AD synchronization task is in progress.



» Imported users and groups are updated to align with the current LDAP/AD server settings. The notification panel shows a summary of the synchronization.

Caution: LAE assumes that a user who is being imported from LDAP/AD with the same username and DN as a previously imported user, who has since been deactivated in LAE, is the same user. Therefore, the deactivated LAE user will be re-instated, and they will regain access to their old LAE documents.

5. Managing LAE Web Application users

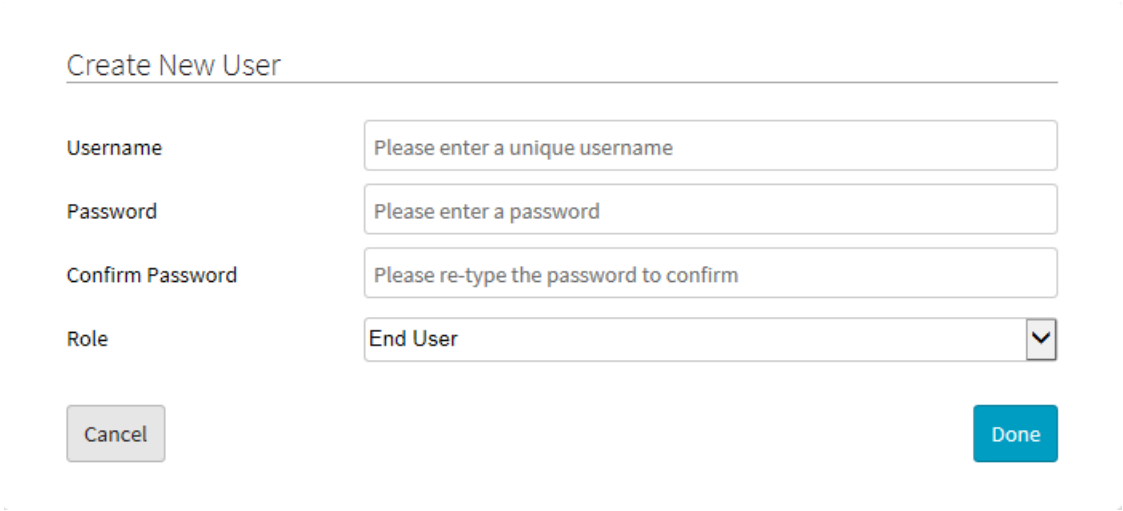
✓ You have logged in to the LAE Web Application as an administrator, see Logging in to the LAE Directory on page 9

Note: After installation, you are assigned the following default user credentials:
Username: admin
Password: welcome
When a user with the role of administrator has been created, (either locally or via LDAP) they can remove the default "admin" / "welcome" user from the system. In a situation where all users with the role of administrator have been removed, when the web server is re-started, then the "admin" / "welcome" user is re-created to ensure that the system always has an administrator.

5.1 Creating local users

1. Click the **Create** button.

2. Select **User**.
   » The **Create New User** dialog box opens.

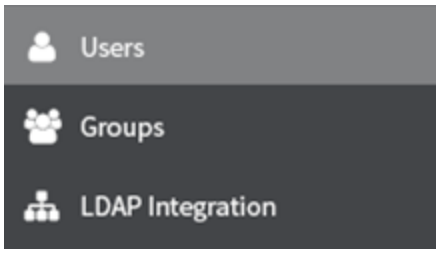


3. Complete the username and password details, and select a role for the new user.
4. Click **Done**.
   » The new user account is created.

5.2 Viewing and editing users

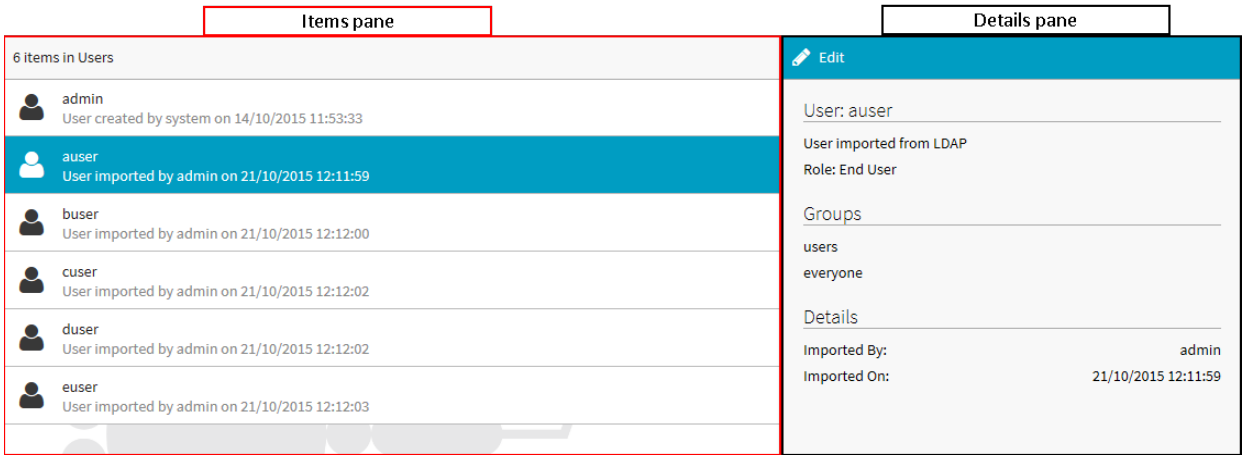
As an administrator, you can view and manage imported and local users in the LAE Directory.

1. From the collections pane, select **Users**.



   » A list of all users is displayed in the items pane in the center of the screen. The first user in the list is selected by default.

2. Select a user from the items pane.



   » User details are displayed in the details pane.

> **Tip:** If you select a user that has been imported from LDAP, **User imported from LDAP** is shown below the user name in the details pane. If the user is a local user, you can edit their user name and/or role. If the user has been imported from LDAP, you can only edit their role.

3. From the details pane, click the **Edit** button.

   » The **Edit User** dialog box opens.

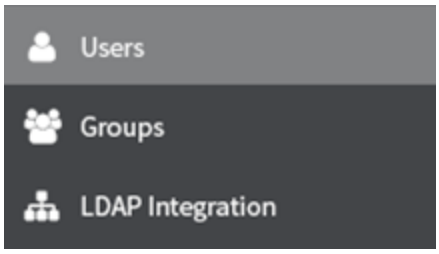
4. Edit the user details, as required.

> **Tip:** There are two user roles available; End User and Administrator.

5.3 Changing user passwords

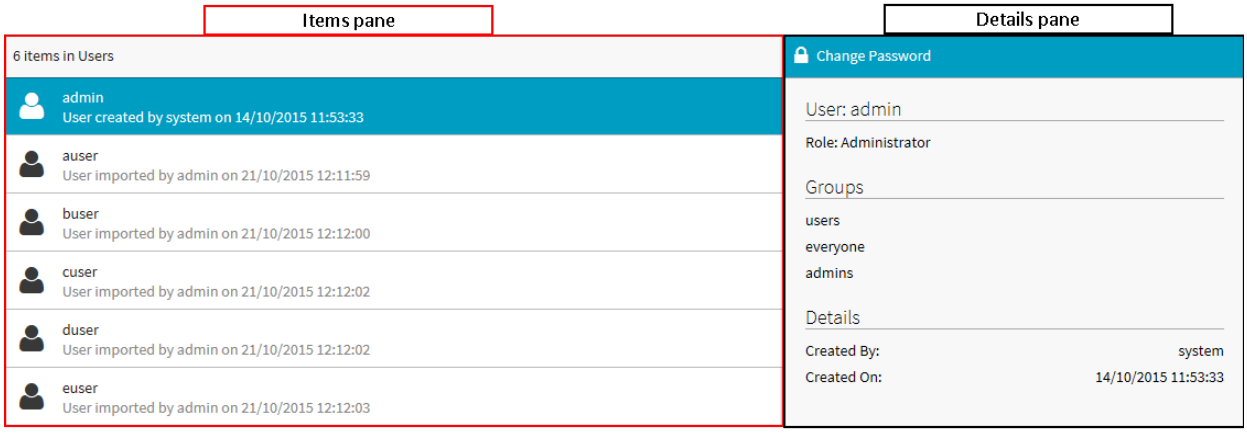
As an administrator, you can change the password of local users in the LAE Directory.

1. From the collections pane on the left side of the LAE Directory screen, select **Users**.



   » A list of all users is displayed in the items pane in the center of the screen. The first user in the list is selected by default.

2. Select a user from the items pane.



   » The user details are displayed in the details pane.

3. From the details pane, click the **Change password** button.

   » The **Change Password** dialog box opens.

> **Tip:** If you select a user that has been imported from LDAP, **User imported from LDAP** is shown below the user name in the details pane and the **Change password** button is not available.

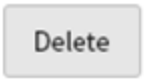
4. Enter a new password and click **Done**.

5.4 Deleting local users

1. From the items pane, select a user.
2. From the details pane, click the **Delete** button.

   » The **Delete User** dialog box opens.
3. Click **Delete** to confirm that you wish to delete the selected user.

Note: The delete option is not available for users that have been imported from LDAP.

Note: After installation, you are assigned the following default user credentials:
Username: admin
Password: welcome
When a user with the role of administrator has been created, (either locally or via LDAP) they can remove the default "admin" / "welcome" user from the system. In a situation where all users with the role of administrator have been removed, when the web server is re-started, then the "admin" / "welcome" user is re-created to ensure that the system always has an administrator.

6. Managing LAE Web Application groups

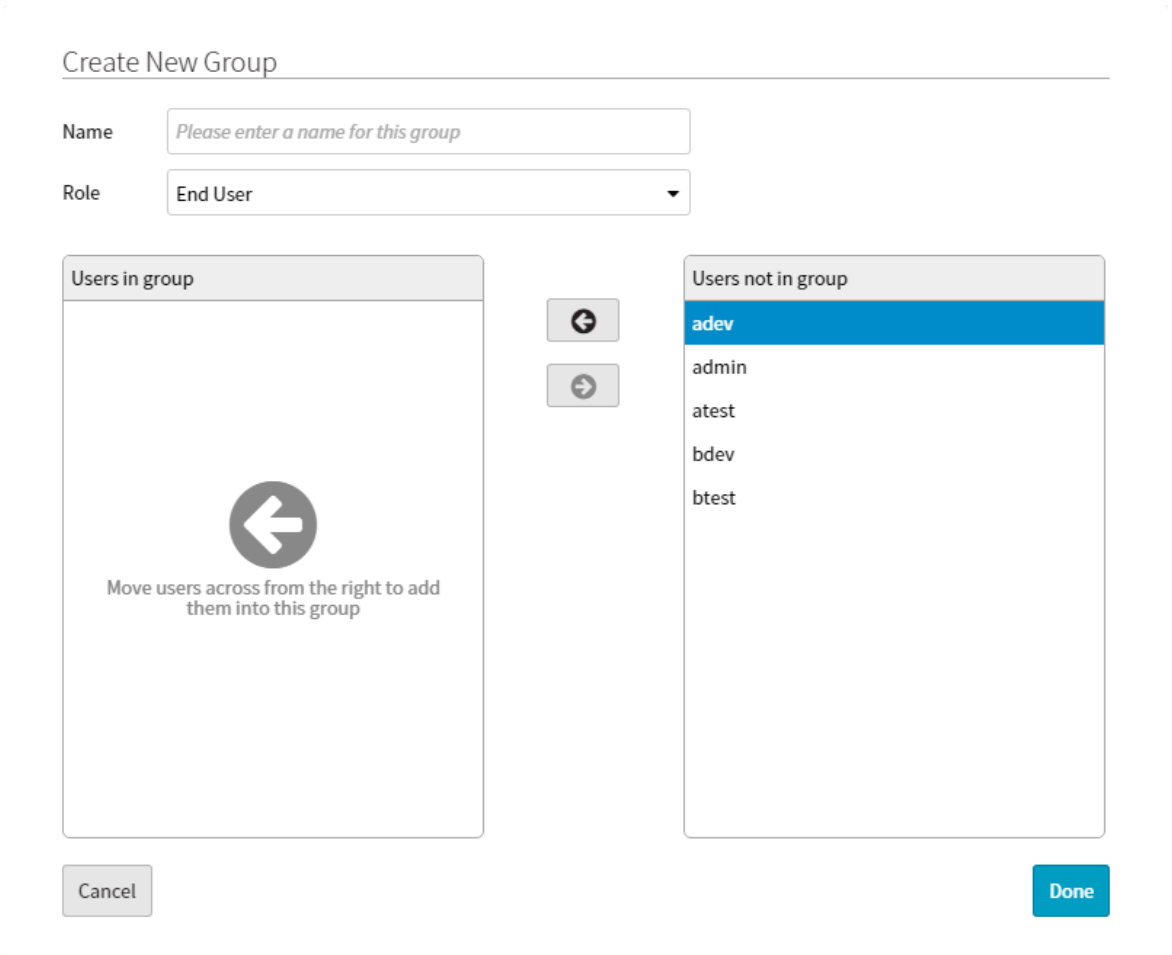
✓ You have logged in to the LAE Web Application as an administrator, see Logging in to the LAE Directory on page 9

Note: Changes to groups and group membership are not automatically updated in the LAE Server and BRE. For such changes to take effect, the LAE server must be restarted.

6.1 Creating local groups

1. Click the **Create** button.

2. Select **Group**.
   » The **Create New Group** dialog box opens.



3. Type a **Name** and select a **Role** for the group.

> **Note:** All users that belong to a group receive the feature access rights of both their user role and the group role.

> **Note:** To administer the LAE Server, for example to apply a new license or to shut down the LAE Server using the shutdown script, the administrator must be in the "admins" group in the LAE Web Application.

4. Select a user and click the left arrow button to add them to the group. Use the right arrow button to move users out of the group.

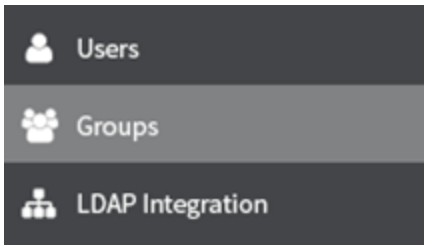
5. Click **Done**.
   » The new group is created.

> **Tip:** You can create a local group to easily combine imported and local users. For example, you may want to create a local group that combines two LDAP users, or you may want to create a local group that includes users from both LDAP and local groups.

6.2 Viewing and editing groups

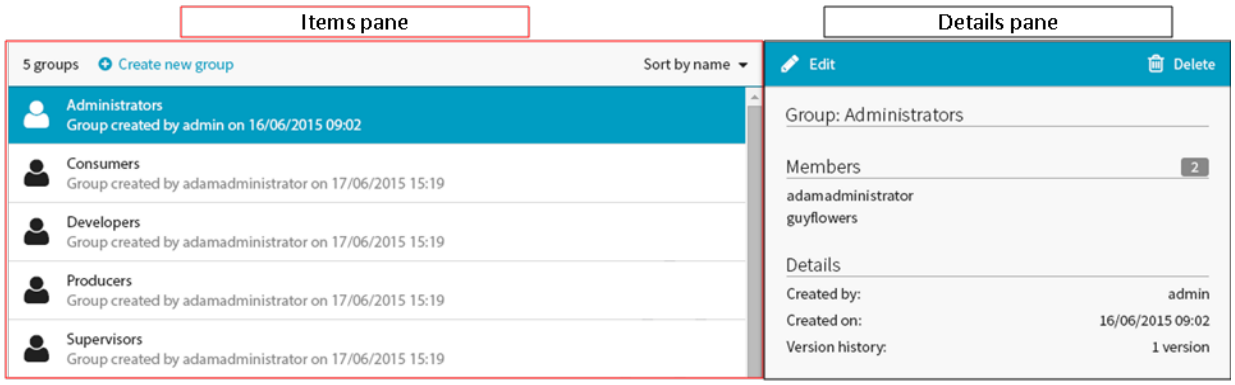
As an administrator, you can view and manage imported and local groups in the LAE Directory.

1. From the collections pane on the left side of the screen, select **Groups**.



   » A list of all groups is displayed in the items pane in the center of the screen. The first group in the list is selected by default.

2. Select a group from the items pane.



» The selected group details are displayed in the details pane on the right side of the screen.

Tip: If you select a group that has been imported from LDAP, **Imported from LDAP** is shown below the group name in the details pane.

3. From the details pane, click the **Edit** button.

» The **Edit Group** dialog box opens.

4. Edit the group details, as required.

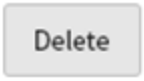
Note: The edit option is not available for groups that have been imported from LDAP.

6.3 Deleting local groups

1. From the items pane, select a user.
2. From the details pane, click the **Delete** button.

» The **Delete Group** dialog box opens.

3. Click **Delete** to confirm that you wish to delete the selected group.



Note: The delete option is not available for groups that have been imported from LDAP.

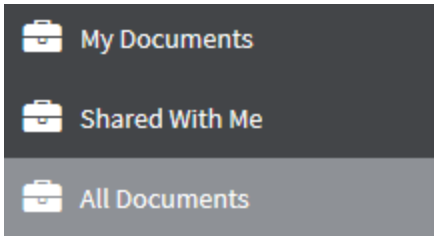
7. LAE configuration settings

Systems administrators can edit some LAE Directory settings in the web-conf/site.prop configuration file, located at: `<LAE Web Application Install Directory>/web-conf/site.prop`.

Note: After editing the site.prop file, you must restart the web server for the changes to take effect.

7.1 Showing or hiding all documents

By default, the **All Documents** menu option is not displayed for end users. You can configure the site.prop file to enable the display of the **All Documents** menu option and allow users to view all documents that are available on the system.



1. Navigate to the site.prop file.
2. Locate the following property:
   `ls.lae.enableAllDocumentsView=false`
   A value of `false` is the default setting and means that the **All Documents** menu option is only available for users with the role of administrator.
3. Change the property value from `false` to `true`:
   `ls.lae.enableAllDocumentsView=true`
   A value of `true` means that the **All Documents** menu option is available for all users.
4. Restart the LAE Server for the changes to take effect.

7.2 Showing or hiding graph run data

By default, all users can view graph run data, even if the graph run was completed by another user.

This setting can be changed by editing the site.prop file to restrict the view of graph run data to the person who runs the graph.

1. Navigate to the site.prop file.
2. Locate the following property:
   `ls.lae.disableRunDataSharing=false`
   A value of `false` is the default setting and means that all users can view all graph run data.
3. Change the property value from `false` to `true`:
   `ls.lae.disableRunDataSharing=true`
   A value of `true` means that only the user who runs a graph can view the graph run data.
4. Restart the LAE Server for the changes to take effect.

7.3 Editing the token refresh period

Additions and deletions of users that are made in the LAE Web Application are automatically updated in the LAE Server and BRE, however, changes to groups and group membership are not. For such changes to take effect, the LAE Server must be restarted.

When the LAE Web Application is restarted, the LAE Server will not be able to communicate with the Web Application until its token is refreshed. The period of time that the LAE Server waits before refreshing its token is known as the token refresh period. The default token refresh period is five minutes.

You can change the token refresh period by editing the site.prop file.

1. Navigate to the site.prop file.
2. Add the following property:
   `ls.brain.webapp.tokenRefreshPeriodMinutes`
   This property specifies the amount of time (in minutes) that the LAE Server waits before refreshing its token. Note that if you do not add this property, the default token refresh period of five minutes is automatically set.
3. Edit the token refresh period by specifying the number of minutes, shown in red and italics in the following example:
   `ls.brain.webapp.tokenRefreshPeriodMinutes=`*`5`*
4. Restart the LAE Server for the changes to take effect.

7.4 Configuring LDAP/AD authentication settings

During installation, you may have configured LAE to authenticate your users via LDAP/AD. If you did not setup LDAP/AD authentication during installation, and you wish to setup or edit LDAP/AD authentication settings after installation, you can configure the relevant properties in the web-conf/site.prop configuration file, located at `<LAE Web Application Install Directory>/web-conf/site.prop`.

Both AD and LDAP

Configure the following two properties for both LDAP and Active Directory implementations:

- URL - `ls.lae.auth.url=`

  Configure this property to set or edit the server which hosts the LDAP/AD source system. After the server name, you must append the port number, in the following format:
  `<protocol>.<server>:<port number>/<rootDN>`.
  The root Distinguished Name (root DN) defines the entry point in the LDAP/AD structure from which an authentication search will take place. It is recommended that the root DN is set to the lowest possible point in the LDAP/AD structure.

  EXAMPLE:
  `ls.lae.auth.url=ldap://server.lavastorm.com:389/ou=someOrgUnit,dc=lavastorm,dc=com`

  If you wish to use a secure protocol, you must include the "`ldaps://`" protocol as a prefix when you enter your LDAP/AD server information.

  EXAMPLE:
  `ls.lae.auth.url=ldaps://server.lavastorm.com:389/ou=someOrgUnit,dc=lavastorm,dc=com`

- Directory provider - `ls.lae.auth.provider=`

  Set this property to be either ldap, ad, or none according to your external source system.

  EXAMPLE: `ls.lae.auth.provider=ad`

Active Directory only

If your source system is Active Directory, you must also configure the following property:

- Domain - `ls.lae.auth.ad.domain=`

  Configure this property to set or edit the AD domain. This domain is passed to AD during authentication to identify users on the source system.

  EXAMPLE: `ls.lae.auth.ad.domain=lavastorm.com`

  When importing users to AD from LAE, if you enter `sAMAccountName` as the **Username attribute**, the domain property must be correctly set such that the combination of the login username value, the '@' symbol, and the 'domain' setting match that of the `userPrincipalName` when looked up in Active Directory.

EXAMPLE: A user in Active Directory has the following attributes set:

- `userPrincipalName = aUser@lavastorm.com`
- `sAMAccountName = aUser`

In this example, if you enter a **Username attribute** of `sAMAccountName`, the "domain" property must be configured as follows: `ls.lae.auth.ad.domain= lavastorm.com`. See Entering a valid "username attribute" on page 18

LDAP only

If your directory provider is LDAP, you must also configure the following two properties (these properties are configured by default for AD):

- User search base - `ls.lae.auth.ldap.userSearchBase=`

  The user search base is used to further drill into specific organization units (OU) within the source directory from the specified root DN, which indicates where to look when attempting to authenticate users. In a scenario where users are spread across multiple OUs below the root DN, then the user search base property can be left blank, as follows: `ls.lae.auth.ldap.userSearchBase=`

  EXAMPLE: `ls.lae.auth.ldap.userSearchBase=OU=users` In this example, all users are stored in a "users" OU directly below the root DN.

- User search filter - `ls.lae.auth.ldap.userSearchFilter=`

  The user search filter is used to identify the attribute that is used to search for a user, and to pass the **Login username** to the source system.

  If your source system is not Active Directory, for example if you are using OpenLDAP, you must ensure that the **Username attribute** that is entered during an LDAP/AD import is also set here.

  EXAMPLE: If you enter "uid" as the **Username attribute** in the **LDAP Integration** dialog box during an LDAP/AD import, then the userSearchFilter property should be set as follows:

  `ls.lae.auth.ldap.userSearchFilter=uid={0}`

  where {0} represents the **Login username** value entered in the **LDAP Integration** dialog box. See Importing LDAP/AD users and groups on page 15

7.5 Administering the security store

When you perform an LDAP/AD import, the binding user password is saved securely in a security store. You can then perform any subsequent LDAP/AD synchronization tasks without re-entering the password. The security store is setup during installation, and is password protected.

> **Note:** Depending on the options taken during installation, you may be asked to enter the security store password after initializing the LAE Web Application (before you reach the login screen). If you chose to store the security store password during installation, then it will be stored as an encrypted value within both the web-conf/site.prop and the conf/site.prop configuration files under the `ls.lae.security.secureStorePassword` property, and you will not be asked to enter the security store password when the LAE Web Application initializes.

You can administer the security store after installation by using the following laeConfig utility command:

```
laeConfig secureStore
```

By using this laeConfig command, you can perform the following actions:

- Create a security store.
- Update an existing security store to change its password. This command will return the encrypted version of the updated password; if during installation you opted to store the password, the updated password can then be stored within both the web-conf/site.prop and the conf/site.prop configuration files.
- Create, read, update, and delete entries in the security store.

All access to the security store via laeConfig requires access to the security store password either:

- Specified within the command.

  - Or -

- If not specified within the command, the encrypted password must be available in the `ls.lae.security.secureStorePassword` property of the web-conf/site.prop configuration file.

You can view the full help for this command by running the following help command:

```
laeConfig help secureStore
```

For more information on the laeConfig utility, see the Enterprise Installation Guide or the Windows Server Installation Guide.

8. Logistics Manager overview

Logistics Manager enables you to remotely schedule LAE graphs to run on-demand or at predetermined times and intervals, with multiple graphs in series or in parallel, and with different graph-level parameter sets.

The feature makes use of Lavastorm Execution Archive (LXA) files, executable versions of the graph and data that you create in the Business Rules Editor (BRE).

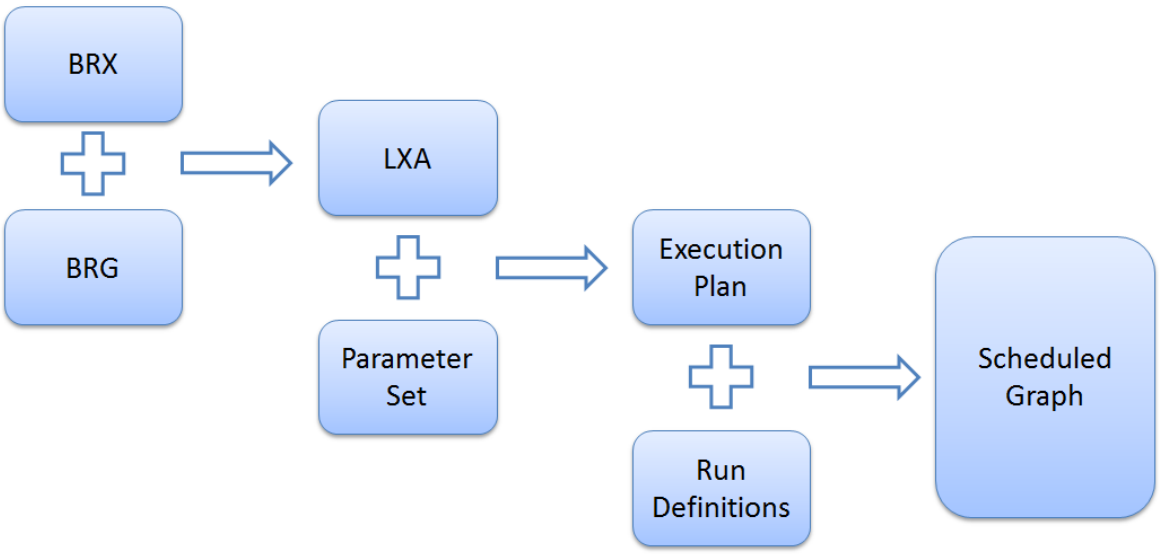
From within BRE, a Business Rules Graph (BRG) and Business Rules Executable (BRX) can be exported as a single LXA for use with Logistics Manager.

> **Tip:** You can save a graph as an LXA in BRE by selecting **Save As Executable** from the **File** menu. For more information, see the BRE Help.

A parameter set created with Logistics Manager allows you to set graph-level parameters for the graph contained within an LXA.

With an LXA and an associated parameter set, you can then create an execution plan and schedule it to run at a desired time.

Within the execution plan, you can create individual run definitions and select LXAs, parameter sets and introduce additional run-specific, graph-level parameters.



8.1 System information

When Logistics Manager is first installed, HTTPS is not enabled by default. If you would like to configure SSL on your installation, please refer to the Jetty documentation, which can be found here: https://wiki.eclipse.org/Jetty/Howto/Configure_SSL.

You may wish to disable unused HTTP methods for security reasons. Logistics Manager only uses the GET and POST methods, and the LAE Directory / Lavastorm Explorer use the PUT and DELETE HTTP methods; all other methods can be disabled without affecting functionality.

8.2 Web UI

The Logistics Manager web UI allows you to upload LXAs. Once you deploy an LXA through the web UI, you can create and edit execution plans and parameter sets and schedule graphs to run on a predetermined schedule or manually.

8.3 REST API

The Logistics Manager API makes use of a representational state transfer (REST) architecture style, where communication between the client and server is accomplished through simple HTTP requests. You can call LAE from other applications and perform all of the logistics management operations of the web UI.

The API works with the four following object types:

- Parameter sets
- Lavastorm execution archives
- Run definitions
- Execution plans

Note: To view additional API information, navigate to `http://localhost:8080/api-viewer`, where *localhost:8080* is replaced with your *LAE web server address*.

8.4 Character restrictions for object names

Due to various operating system requirements, a number of characters are not permitted in the names of objects created in Logistics Manager. This includes LXAs, execution plans, parameter sets and run definitions.

The Logistics Manager UI will not allow you to enter an invalid name, but it is important for API users to be aware of the restricted characters.

The following characters are not allowed:

- /, ", ', @, !, #, $, %, \, ^, +, &, *, ~, `, ;, :, |, <, >, (,),{, }, [,], ,, ., ?

9. Scheduling graph runs

9.1 Access Logistics Manager

The Logistics Manager web UI is located by default at your <*LAE web server address*>/automation. Check with your IT department to confirm the location and URL of the web server. The example URL to access the web UI in this guide is:

```
http://localhost:8080/automation/
```

The URL prefix for calls and queries made to the Logistics Manager API in this guide is:

```
http://localhost:8080/schedule/rest/automation/
```

Calls and queries to the Logistics Manager API take the following two forms, where `ltk` is your authentication token:

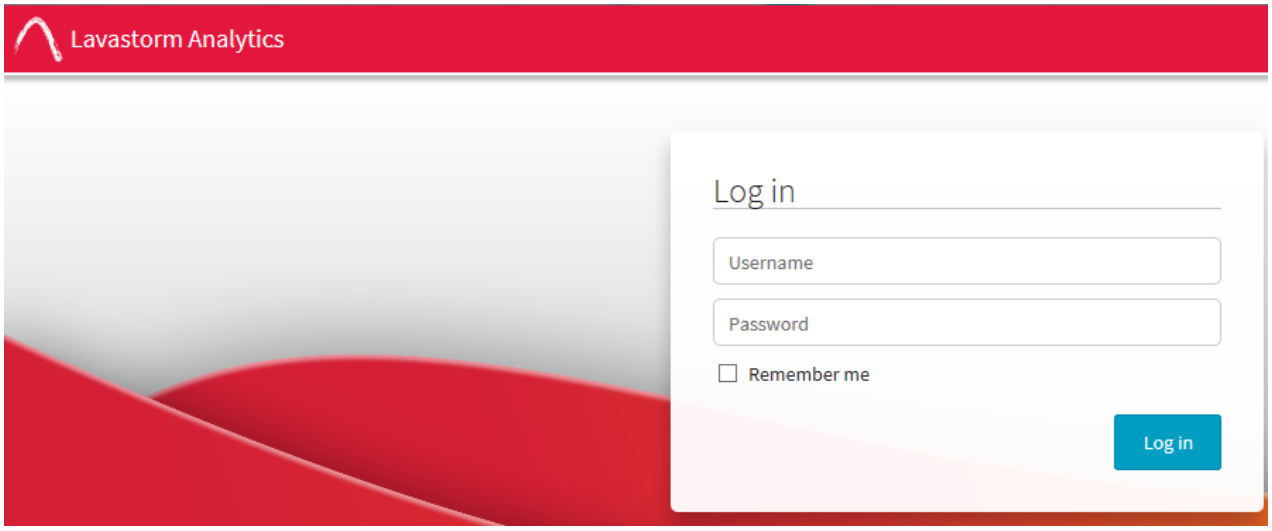
```
urlPrefix + call + ltk
```

EXAMPLE:

```
http://localhost:8080/schedule/rest/automation/put-
object?ltk=cRvxnEPjYuz965cnv9jQ2bayGg6tkqQodg6Qf3EfFWI%3D
```

Logging in from the web UI

1. Navigate to Logistics Manager in your web browser.
2. In the **Log in** dialog box, enter your username and password.
3. Click **Log in**.



Logging in from API

1. Make a login call to the API, as in the following example request.
2. If your login is authenticated, the API will return a message containing your token.
3. Use the token for the value of `ltk` in all of your subsequent calls.

> **Note:** The authorization token that you receive is only valid for 24 hours. After that, you must re-authenticate to receive a new token for the following 24 hours.

EXAMPLE:

Request URL: `http://localhost:8080/login/rest`

Request Method: `POST`

Request Payload:

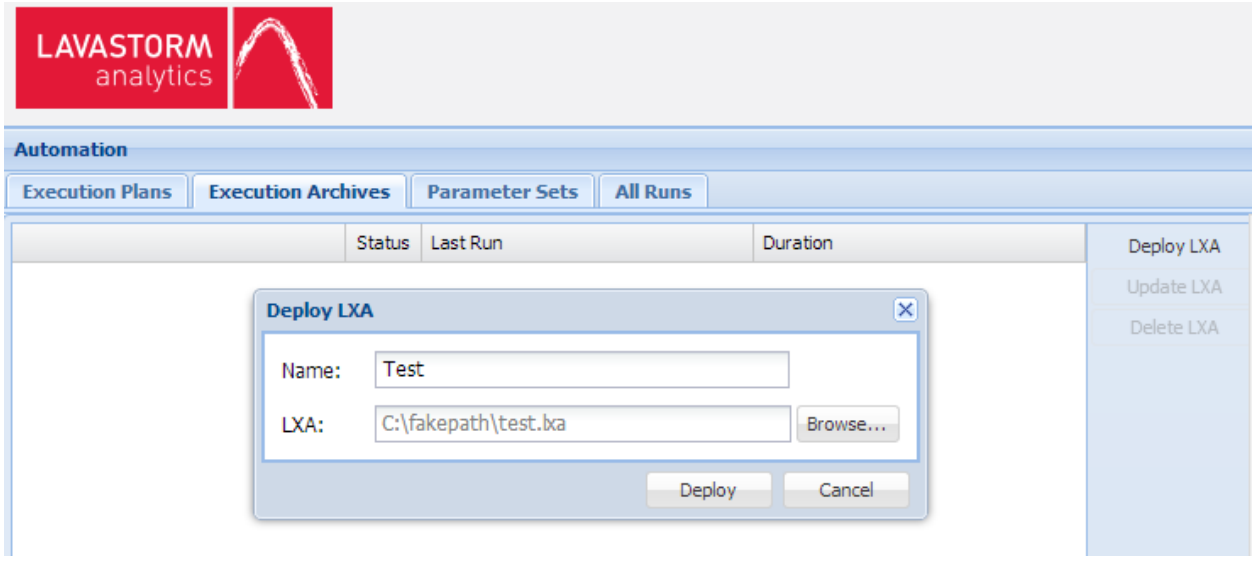
```
{"username":"(your username)","password":"(your password)"}
```

9.2 Deploying an LXA file

From the web UI

1. Select the **Execution Archives** tab.
2. Click **Deploy LXA**.
3. Type a **Name** for the execution archive.
4. Click **Browse** and select the desired LXA file from your computer.
5. Click **Deploy**.

> **Note:** All of the names entered for LXAs and other file types must be unique. Once entered into Logistics Manager, file names can never be edited.



From API

1. Encode the desired LXA in Base64.
2. Insert the Base64-encoded file into the example request payload (see following example).
3. Make a `put-object` call to the API with the LXA in the request payload.

EXAMPLE:

Request URL: `http://localhost:8080/schedule/rest/automation/put-object?ltk=(your login token)`

Request Method: `POST`

Request Payload:

```
{"token":null,"repositoryVO":
    {"@type":"ro","version":-1,
    "id":null,"path":"deploy/lxa/Test","object":
        {"lxa":"(Base64-encoded file)",
        "@type":"Lxa","name":"Test"}
        }
        }
```

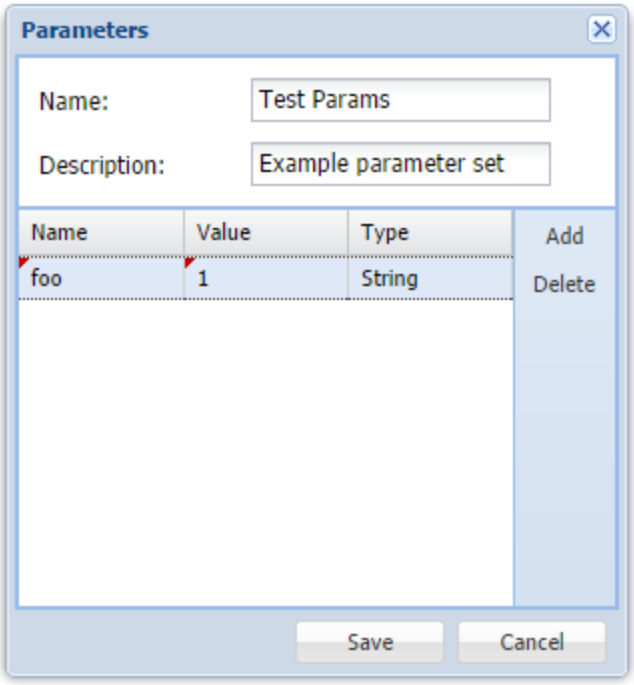
9.3 Defining parameter sets

Note: All execution plans require a parameter set.

From web UI

1. Click the **Parameter Sets** tab.
2. Click **Add**.
3. In the dialog box, type a **Name** and a **Description** for the parameter set.
4. Click **Add** to insert a new, blank parameter.
5. Select **String** or **Password Type** for the parameter.

   Note: Password parameters appear obfuscated in the user interface.
6. Enter a **Name** and a **Value** for the parameter.
7. Repeat steps 4, 5 and 6 until the desired number of parameters have been added.
8. Click **Save**.



From API

- Make a `put-object` call to the API with the new parameter set defined in the request payload.

Request URL: `http://localhost:8080/schedule/rest/automation/put-object?ltk=(your login token)`

Request Method: `POST`

Request Payload:

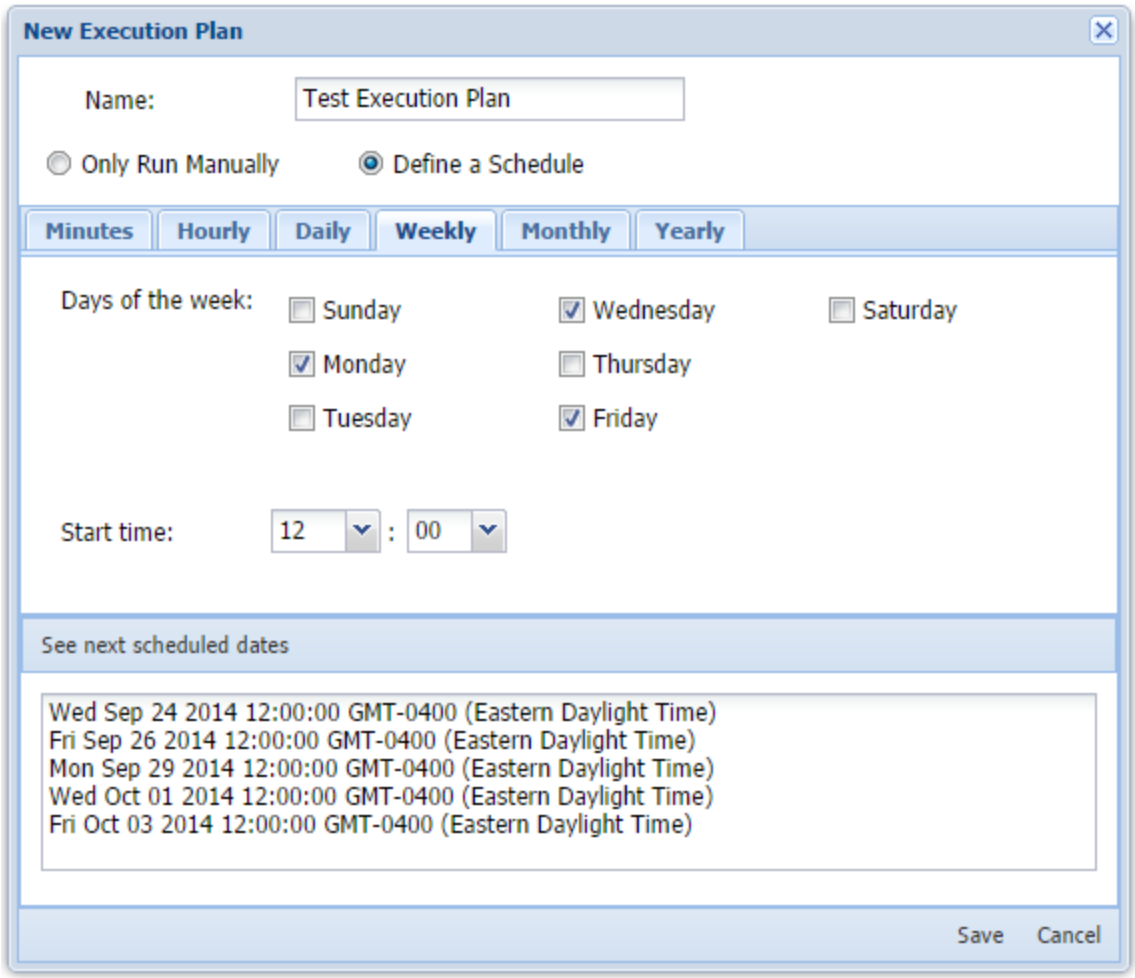
```
{"token":null,"repositoryVO":
    {"@type":"ro","version":-
    1,"id":null,"path":"deploy/parameterSet/Test Params",
    "object":
        {"type":"S","value":"<parameters>\n<param><param encrypted="FALSE"
        type="STRING"><name>foo</name><value>1</value></param>\n</parameter
        s>\n","description":"Example parameter set",
        "@type":"Parameter","name":"Test Params"
        }
    }
}
```

For a parameter of password type, use: `<param encrypted="TRUE" type="PASSWORD">`

9.4 Creating an execution plan

From web UI

1. Click the **Execution Plans** tab.
2. Click **New Execution Plan**.
3. In the dialog box, type a **Name** for the execution plan.
4. To set your run schedule, select **Only Run Manually** or **Define a Schedule**.
5. If you choose to run manually, your configuration is complete; click **Save**.
6. If you choose to define a schedule, select the tab for the desired interval (**Minutes**, **Hourly**, **Daily**, **Weekly**, **Monthly** or **Yearly**) and specify the corresponding details.
7. You can click **See next scheduled dates** to preview the next 5 run times. Click **Save**.



From API

1. Make a `put-object` call to the API with the execution plan in the request payload.
2. To define a schedule for the execution plan, include the `cronExpression` for the desired interval in the request payload.

   - Or -

   For a manual execution plan, leave the `cronExpression` blank.

Request URL: `http://localhost:8080/schedule/rest/automation/put-object?ltk=(your login token)`

Request Method:`POST`

Request Payload:

```
{"token":null,"repositoryVO":
    {"@type":"ro","version":-1,"id":null,"path":"deploy/executionPlan/Test Execution Plan","object":
        {"cronExpression":"0 0 12 ? * MON,WED,FRI *",
        "status":"N","@type":"ExecutionPlan","enabled":false "name":"Test Execution Plan"
        },
    }
}
```

9.5 Creating run definitions

In LAE 6.0, 6.1 and 6.1.1, child run definitions have the option of running only when their parent or predecessor succeeds, or running only when their parent or predecessor fails. This is accomplished via the `runIfPredecessorFailed` parameter, see From API.

The following graph states are available:

Run Definition Name	Status
Run1	
Run2	
Run3	

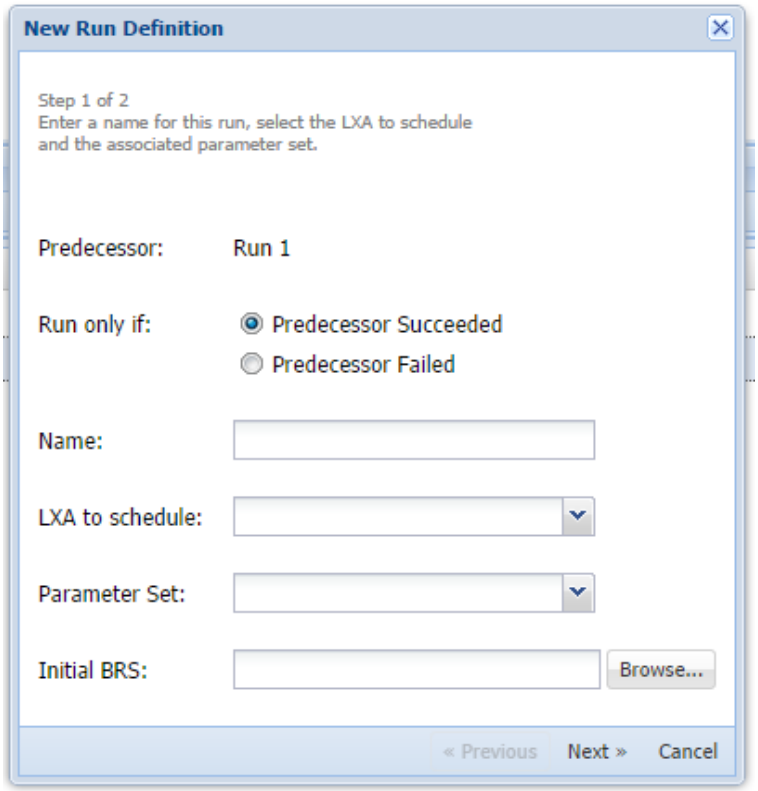
This graph completed successfully.

This graph did not run due to the condition of its predecessor.

This graph completed with errors.

From web UI

1. Ensure that the execution plan that you would like to create a run definition for is selected, and click **New Run Definition**.
   » The **New Run Definition** dialog box opens.



2. In the dialog box, type a **Name** for the run definition.
3. From the **LXA to schedule** menu, select an LXA to schedule.
4. From the **Parameter Set** menu, select a parameter set.
5. If you would like to upload an initial BRS file, click **Browse** and navigate to the desired file.
6. Click **Next** to define run parameters, which will override the parameters in the selected parameter set.
7. Click **Add** to insert a new blank parameter.
8. Type a **Name** and **Value** for the parameter.
9. Repeat steps 6 and 7 until the desired number of run parameters have been added.
10. Click **Finish**.

Each execution plan can schedule multiple graph runs, both in parallel and in series.

- To chain runs together, click **New Run Definition** when the run you wish to follow is selected and repeat the steps above.

Note: Graphs can be viewed and run in Lavastorm Explorer, see Generating a graph link on page 54. If the graph run parameters are edited in Lavastorm Explorer, this also edits the corresponding parameters in Logistics Manager. Therefore, always confirm that the run parameters are set according to your preferences before running a graph in Logistics Manager.

From API

1. Make a `put-object` call to the API to create a new parameter set for the run parameters with the following Request Payload:

```
{"token":null,"repositoryVO":

 {"@type":"ro","version":-
 1,"id":null,"path":"deploy/parameterSet/Trial Run - Execution
 Parameters", "object":

     {"type":"E",
     "value":"<parameters>\n<param><name>foo</name><value>2</value></
     param>\n</parameters>\n",
     "description":"Execution Parameter",
     "@type":"Parameter","name":"Trial Run - Execution Parameters"
     }

 }
}
```

2. Make a second `put-object` call to create the run definition with the following request payload:

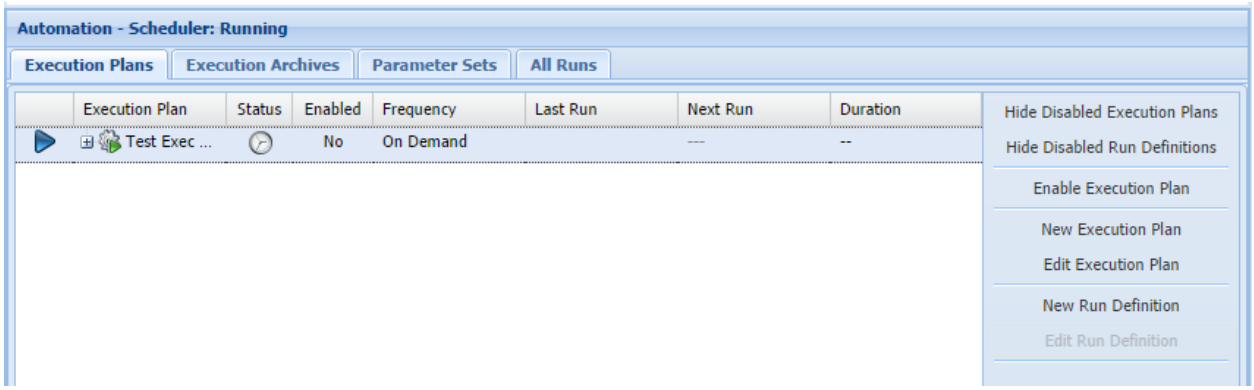
```
{"token":null,"repositoryVO":

 {"@type":"ro","version":-
 1,"id":null,"path":"deploy/runDefinition/Trial Run", "object":

     {"savedParameters":["deploy/parameterSet/Test Params"],
     "executionParameters":["deploy/parameterSet/Trial Run - Execution
     Parameters"], "lxa":"deploy/lxa/Test",
     "executionPlan":"deploy/executionPlan/Test Execution Plan",
     "parentRunDef":null, "runIfPredecessorFailed":
     "Y","@type":"RunDefinition","name":"Trial Run"
     }

 }
}
```

9.6 Enabling an execution plan or a run definition

An execution plan will not run until it has been enabled. Run definitions can be enabled or disabled using the same calls.

From web UI

1. Select the **Execution Plans** tab.
2. Select the desired execution plan.
3. Click **Enable Execution Plan**.
4. For a manual execution plan, click the blue **Play** button next to the name of the execution plan to start the run.



From API

1. Make an `enable-disable-execution-plan` call to the API with the path of the desired execution plan in the request payload.

   Request URL: `http://localhost:8080/schedule/rest/automation/enable-disable-execution-plan?ltk=(your login token)`

   Request Method: `POST`

   Request Payload: `{"path":"deploy/executionPlan/Test Execution Plan"}`

   To enable or disable a run definition, follow the same syntax as above and replace the request payload with the path for the run definition. For example: deploy/runDef/

2. To run a manual execution plan, make a `start-stop-run` call to the API with the path of the desired execution plan in the request payload.

Request URL: `http://localhost:8080/schedule/rest/automation/start-stop-run?ltk=(your login token)`

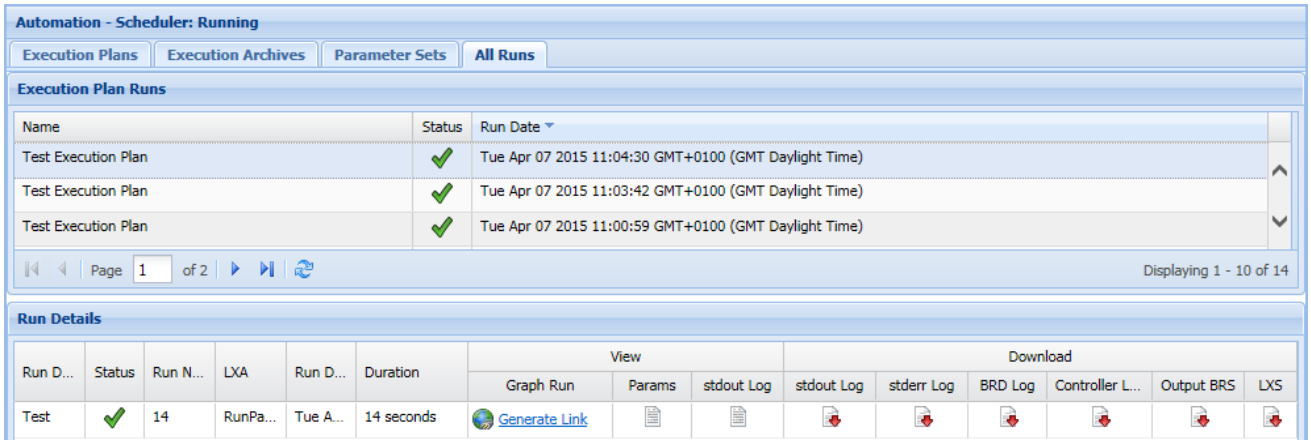
Request Method: `POST`

Request Payload: `{"path":"deploy/executionPlan/Test Execution Plan"}`

9.7 Viewing run logs and output

From web UI

1. Select the **All Runs** tab.
2. In the **Execution Plan Runs** pane, click a run.
   » The corresponding **Run Details** are displayed in the bottom pane.
3. Click to download the desired logs or output files.



From the **Run Details** pane, you can also generate a link to share a graph with others for viewing in Lavastorm Explorer. See Generating a graph link on page 54.

From API

To download a run's logs and output files using the API, request the link to the desired file's location in the following format:

```
http://localhost:8080/schedule/rest/automation/download-file?ltk=(your login token)&path=deploy/runDefinition/(run definition name)/run/(run name id)/(file type)
```

1. Query for all of the execution plan runs for the desired execution plan:

   Request URL:
   ```
   http://localhost:8080/schedule/rest/automation/query-for-object?ltk=(your login token)&sql=select l.id, l.executionPlan.name, l.runDate, l.status from SimpleExecutionPlanRuns l where l.executionPlan.name = 'Test Execution Plan'
   ```

   Request Method: `GET`

2. Use the ID that is returned to query all the individual runs within the execution plan run:

Request URL: `http://localhost:8080/schedule/rest/automation/query-for-object?ltk=(your login token)&sql= select l.id, l.status, l.startTime, l.duration, l.name, l.runDefinition.lxa.name, l.runDefinition.name from SimpleRun l where l.executionPlanRuns.id = '(id)'`

Request Method: `GET`

> **Note:** Different application servers return IDs in different formats that may include both upper- and lowercase letters as well as dashes. However, the internal representation of the ID is all uppercase without dashes. When inputting an ID as part of a query or other GET request, be sure to strip all dashes ("-") and convert all characters in the ID to uppercase before making your API call.

3. Make a `GET` request of the link to the desired output file from the desired run using its run name ID:

   Standard Output Log:

   `http://localhost:8080/schedule/rest/automation/download-file?ltk=(your login token)&path=deploy/runDefinition/Trial Run/run/1/stdoutlog`

   BRD Log:

   `http://localhost:8080/schedule/rest/automation/download-file?ltk=(your login token)&path=deploy/runDefinition/Trial Run/run/1/brdlog`

   Output BRS:

   `http://localhost:8080/schedule/rest/automation/download-file?ltk=(your login token)&path=deploy/runDefinition/Trial Run/run/1/outputbrs`

   LXS:

   `http://localhost:8080/schedule/rest/automation/download-file?ltk=(your login token)&path=deploy/runDefinition/Trial Run/run/1/lxs`

9.8 Updating and editing elements

From web UI

To update an execution plan, run definition or parameter set from the web UI:

1. Navigate to the corresponding tab.
2. Select the desired element.
3. Click the edit button located on the right side of the window.
4. For **Execution Archives**, click **Update LXA** to load a new file.

From API

1. Make a `get-object` call for the object that you wish to update or edit.

   Request URL: `http://localhost:8080/schedule/rest/automation/get-object?ltk=(your login token)`

   Request Method: `POST`

   Request Payload: `{"path":"deploy/runDefinition/Trial Run"}`

2. Make a `put-object` call for the object with the desired updated attributes, but be certain to use the same version number for the object as the one returned from the API in your previous `get-object` call.

   Request URL: `http://localhost:8080/schedule/rest/automation/put-object?ltk=(your login token)`

   Request Method: `POST`

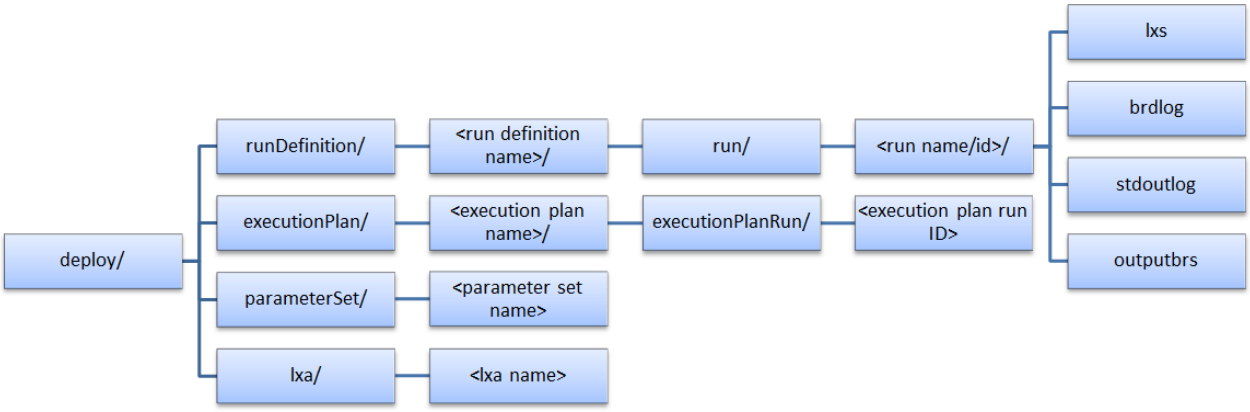
   Request Payload:

```
{"token" : "76f08bbb-173b-4bf4-a026-8e2888c7e0c0",
 "repositoryVO" : {"@type" : "ro","version" : 0,
  "id" : "ce5af2aa-7c49-44ba-957b-2392766a2feb",
   "path" : "deploy/runDefinition/Trial Run",
  "object" : {
"@type" : "RunDefinition", "enabled" : null,
"name" : "Test Run",
      "savedParameters" : [ "PAR/Example Params" ],
      "executionParameters" : [ "deploy/parameterSet/Trial
Run - Execution Parameters" ],
      "lastRun" : "RUN/4", "lxa" : "deploy/lxa/Test",
      "executionPlan" : "deploy/executionPlan/Test Execution Plan",
      "parentRunDef" : null,"initialState" : null,
```

```
    }
  }
}
```

9.9 File path structure

Files for Logistics Manager follow the path structure illustrated below:



9.10 API queries

The API can be queried using the Hibernate Query Language, the documentation for which can be found at:

http://docs.jboss.org/hibernate/orm/3.3/reference/en-US/html/queryhql.html

Request URL: `http://localhost:8080/schedule/rest/automation/query-for-object?ltk=(your login token)&(your HQL query)`

Request Method: `GET`

The following objects can be queried:

Objects	Attributes

SimpleExecutionPlan	`private String name;`
	`private Boolean enabled;`
	`private String path;`
	`private String cronExpression;`
	`private String status;`
	`private Timestamp lastExecution;`
	`private Set<SimpleExecutionPlanNode> executionPlanNodes;`

SimpleExecutionPlanNode	`private SimpleRunDefinition runDefinition;`
	`private SimpleExecutionPlan executionPlan;`
	`private SimpleExecutionPlanNode parentNode;`
	`protected UUID parentId;`

SimpleExecutionPlanRuns	`private Timestamp runDate;`
	`private Set<SimpleRun> runs;`
	`private String status;`

SimpleLxa	`private String name;`
	`private Date creationDate;`
	`private String path;`
	`private Timestamp lastExecution;`
	`private byte[] lxa;`

SimpleParameters	`private String name;`

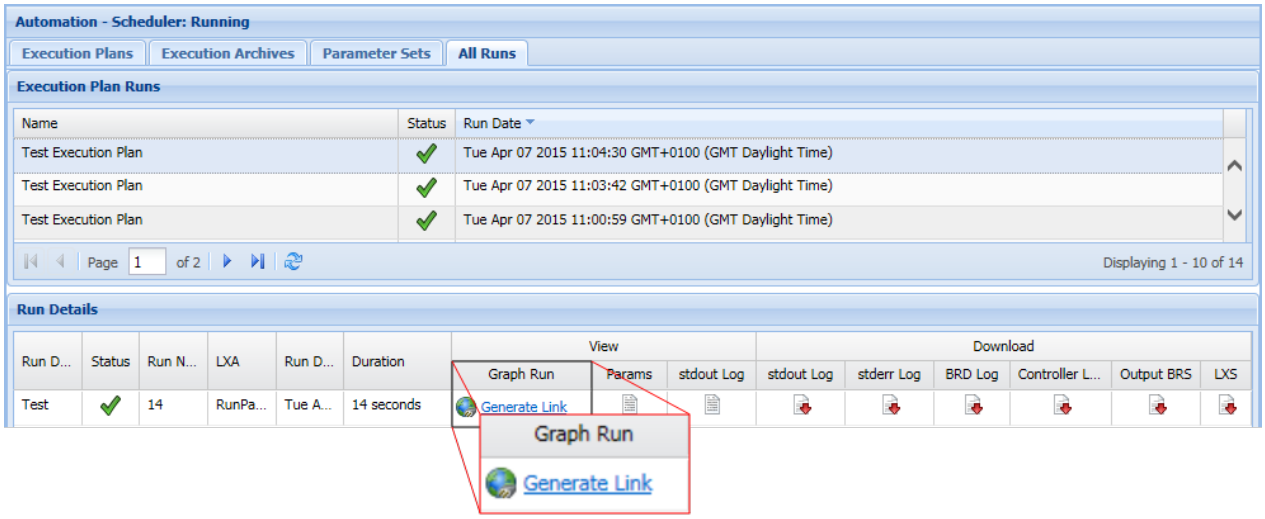
Objects	Attributes
	private String value; private String type; private String path; private String description;
SimpleRun	private String controllerId; private String status; private Timestamp startTime; private Timestamp endTime; private String path; private int duration; private String controllerHost; private SimpleRunDefinition runDefinition; private Set<SimpleRunParameters> runParameters; private String name; private Long runNumber; private SimpleExecutionPlanRuns executionPlanRuns;
SimpleRunDefinition	private byte[] initialState; private String path; private String schedule; private SimpleExecutionPlanNode executionPlanNode; private SimpleLxa lxa; private Set<SimpleParameters> parameters; private String name; private Date lastRun;

10. Generating a graph link

You can generate a link in Logistics Manager to share a graph with others for viewing in Lavastorm Explorer.

- You have imported an LXA graph file into Logistics Manager.
- The graph has been run in Logistics Manager (either on a schedule or manually).

1. Select the **All Runs** tab.
2. In the **Execution Plan Runs** pane, click a run.
   » The corresponding **Run Details** are displayed in the bottom pane.
3. In the **View** section of the **Run Details** pane, click **Generate Link**.



» The **Generating Link** dialog box opens.

> **Note:** For large graphs, it may take longer than usual for the link to be generated; ensure that you keep the **Generating Link** dialog box open until the link has been generated.

> **Note:** Each time you click **Generate Link**, the link is regenerated.

4. Click the graph link to open the graph in the same browser window.

- Or -

Copy the link and click **Close** to close the **Generating Link** dialog box.

5. Paste the link into a browser window or send the link to a consumer to view the graph.
   » The graph opens in Lavastorm Explorer. For more information, see the Lavastorm Analytics Engine User Guide.

Note: By default, a link is valid for 30 days. After that, you must generate a new link for the following 30 days. Links are automatically deleted from the system at 0200h on the day that they expire. You can edit graph link expiry settings, see Editing graph link expiry settings on the next page.

Caution: Graphs that have been uploaded to Logistics Manager and opened in Lavastorm Explorer can only be run if the execution plan that is set in Logistics Manager contains only one run definition and is set to run manually. Graphs that have been uploaded to the LAE Directory can always be run in Lavastorm Explorer.

10.1 Editing graph link expiry settings

You can configure the period for which a link is valid and you can configure the system clean up time by editing the web-conf/site.prop file. The web-conf/site.prop file is located at: <*LAE Web Application installation location*>web-conf/site.prop.

1. Navigate to the site.prop file.
2. To configure the period for which a link is valid, edit the following site.prop file property, replacing the default expiry time (shown in italics in this example) as needed:
   `ls.lae.repository.expiredHours=`*`720`*
   For the `expiredHours` property, the unit is hours; the default is 720 hours (30 days).
3. To configure the time that links are automatically deleted from the system, edit the following site.prop file property, replacing the default time (shown in italics in this example) as needed:
   `ls.lae.repository.cleanupSchedule=`*`0 0 2 * * *`*
   For the `cleanupSchedule` property, the values must be in cron syntax; the default is 2:00 a.m.

For more information on editing the site.prop file, see the Windows Server Installation Guide or the Enterprise Installation Guide.

11. Frequently asked questions

11.1 LDAP/AD integration

How do I ensure that only specific users from LDAP/AD can access LAE?

You can apply an advanced filter to limit an LDAP/AD import to specific users or groups by using standard LDAP query syntax. The filter is applied during an import in the **LDAP Integration** dialog box; only users that have been imported will be allowed access to LAE. See Applying an advanced filter on page 18.

How can I edit my LDAP/AD authentication settings after installation?

You can edit LDAP/AD authentication properties after installation in the web-conf/site.prop file, located at `<LAE Web Application Install Directory>/web-conf/site.prop`. See Configuring LDAP/AD authentication settings on page 32.

How can I improve slow log in times when integrated to LDAP/AD?

Larger and more complex LDAP/AD repositories have the potential to increase log in times. It is recommended that the root DN is set to the lowest possible point in the LDAP/AD structure when configuring LDAP/AD authentication settings. See Configuring LDAP/AD authentication settings on page 32.

How do I ensure that all users on LAE are authenticated via the LDAP/AD source system?

LAE ships with a seed admin user. You can use this user to setup and run an import of users and groups from LDAP/AD. Assuming that you have imported a group containing administrator users, then you can assign this group the 'administrator' role within LAE, thus granting administrator rights to any imported users who belong in that group. You can then log in to LAE with one of these LDAP/AD administrator users and delete the original seed admin user. Once the seed admin user has been deleted, all users are now imported users and thus authenticate against the external LDAP/AD system.

All admin users have been removed, how do I log in again as an administrator to rectify this?

If you find yourself in a situation where there are no admin users in LAE, for example if you performed an LDAP/AD import and all admin users were moved out of the admin group, then you need to restart the web server. When the web application restarts, the original seed admin user is re-created. You can then log in as the seed admin user and perform a new synchronization.

I configured LDAP/AD authentication, but my LDAP/AD users are still not able to log in to LAE.

Once you have configured LDAP/AD authentication, you must then import users to LAE. Only users that have been imported can log in to LAE with their LDAP/AD user credentials.

What do I need to do to ensure a successful import when using a secure protocol?

If you are using a secure protocol, ensure that you have correctly installed security certificates on both your LDAP/AD server and the LAE web server. Please refer to your vendor's documentation for how to install security certificates.

Why am I asked to enter a "secure store" password when I try to access LAE?

The secure store, or security store, is setup during installation and is password protected. During installation, you can choose to store the security store password as an encrypted value in both the web-conf/site.prop and the conf/site.prop configuration files. For increased security, you can choose not to store the security store password. In this case, you will be asked to enter the security store password when the LAE Web Application is started, before you reach the login screen. See Administering the security store on page 34.

11.2 LAE Server administration

Why am I not able to apply a new license?

To apply a new license, you must be a member of the "admins" group in the LAE Web Application. Changes to groups and group membership are not automatically reflected in the LAE Server and BRE; for such changes to take effect, the LAE Server must be restarted.

How do I start/stop the server on Windows?

Note: Before installation, you must first run the .profile.lavastorm script, see the Windows Server Installation Guide or the Enterprise Installation Guide for more information.

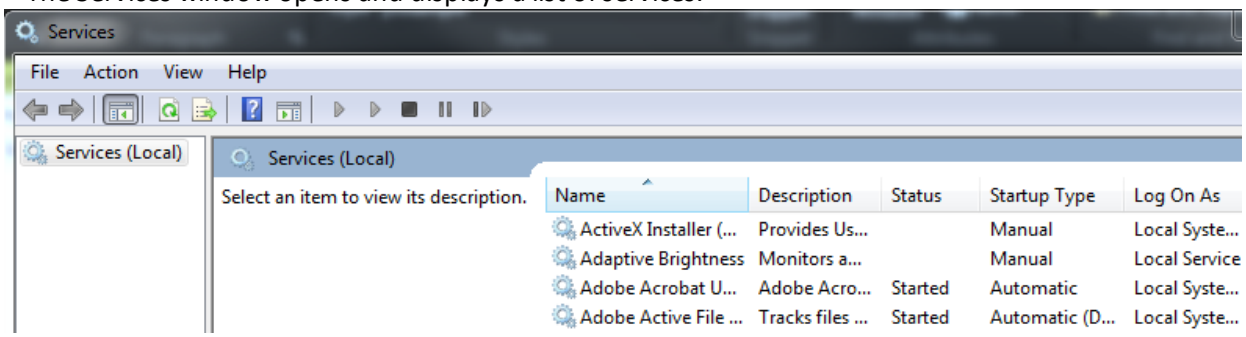
✓ You have installed the LAE Server, see the LAE Windows Server Installation Guide for more information.

As part of the installation, the LavastormLAEServer service is created. Depending on the specific settings of your installation, the LavastormH2Database and the LavastormJettyServer services are also created on your machine. You can start, stop or configure the LAE services by using the Windows Control Panel.

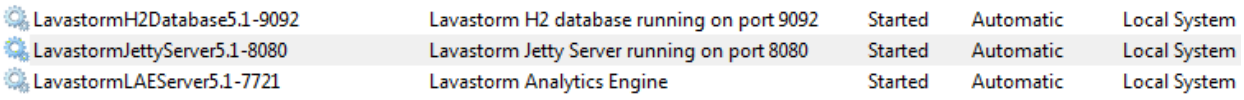
Caution: The LAE server authenticates against the LAE Web Application, therefore the Web Application must be running prior to starting the LAE server. Similarly, if the shutdownServer scripts are to be used, the Web Application must be running.

1. From the Windows Start menu, click **Control Panel**.
2. Click **System and Security**.
3. Click **Administrative Tools**.
4. Double-click **Services**.

» The Services window opens and displays a list of services.



EXAMPLE: The following example shows (from left to right) the LAE Servers, their Description, Status, Startup Type and Log On As information. The port numbers are those that are set during installation.



5. Right-click a service to display the context menu.
6. From the context menu, you can choose to **Start**, **Stop** or **Restart** the server. You can also select **Properties** to configure the server settings. For example, you can select a Manual or Automatic Startup Type. By default, the server Status is set to Started and the Startup Type is set to Automatic.

How do I start/stop the server in Linux?

In order to start the LAE server, you must be in a properly configured LAE environment. This means that you must have executed one of the LAE environment resource scripts:

- For *sh* or *bash*: source .profile.lavastorm

To invoke the LAE Server, type the following command:

sh, bash:

```
<installation-directory>/bin/laeServer >
<lae-log-directory>/laeServer.log 2>&1 &
```

Note: The default port used by the LAE Server is 7721. Ensure that your administrator has configured the server so that the LAE Server port is not blocked.

To start the LAE Web Application, you must start both the H2 database and the Jetty server.

1. Start the H2 database with the following command:
   `<installation-dir>/bin/startDatabase &`
2. Start the Jetty server with the following command:
   `<installation-dir>/bin/startLavastormJettyServer &`

Note: The H2 database must be started before the Jetty server.

Note: The default port used by the LAE Web Application is 8080 and the default port used by the database is 8089. Ensure that you have configured the server so that the LAE Web Application port and database port are not blocked.

To stop the LAE Web Application, you must stop both the Jetty server and the H2 database.

1. Stop the Jetty server with the following command:
   `<installation-dir>/bin/stopLavastormJettyServer &`
2. Stop the H2 database with the following command:
   `<installation-dir>/bin/stopDatabase &`
3. Stop the LAE Server with the following command:
   `<installation-dir>/bin/shutdownServer`

Why am I unable to start/stop the LAE Server in Linux?

After installation, you are assigned the following default user credentials:
Username: admin
Password: welcome
When another user with the role of administrator has been created, (either locally or via LDAP), they can remove the default "admin" / "welcome" user from the system. In this scenario, to start/stop the LAE Server, the new administrator must be a member of the "admins" group in the LAE Web Application. However, changes to groups and group membership are not automatically reflected in the LAE Server and BRE; for such changes to take effect, the LAE Server must be restarted.

If the default "admin"/"welcome" user has been deleted, and your new administrator has been added to the "admins" group since the LAE Server was last restarted, the server will not recognize any admin user with permission to restart the server. In this case, you would need to force the LAE Server to shutdown by using unix commands to kill the process. When the LAE Server is restarted, the changes to the "admins" group membership will be reflected, and the `shutdownServer` command can be used with additional options to specify the admin user and their password, for example, `./shutdownServer -u admin2 -p password`.

Index

I

L

M

N

O

P

R

S

U

Website: www.lavastorm.com
Support Email: Support@lavastorm.com

Document ID: LAE-6.1.1-ADM-1
Date of Publication: 01 December 2015