

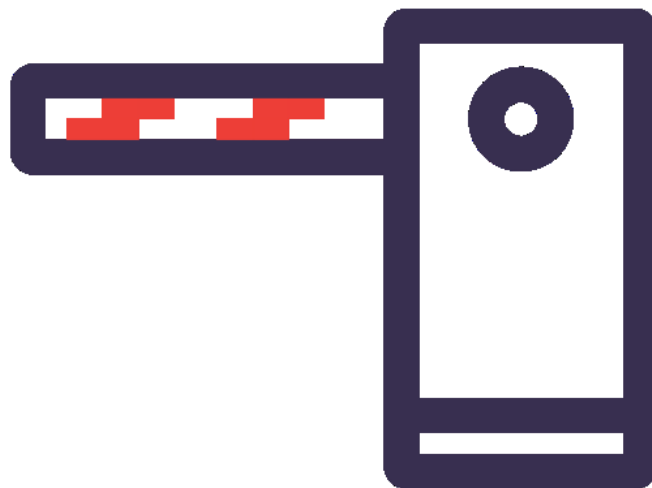


**CHECKMARX**  
choose what developers use

## Checkmarx Access Control (CxAC)

User Guide v1.5.x

---



July, 2018

---

---

# Contents

<b>OVERVIEW .....</b>	<b>4</b>
<b>SETTING UP CXAC .....</b>	<b>5</b>
SERVER HOST REQUIREMENTS .....	5
<i>Active Directory – LDAP SSO Configuration</i> .....	5
<b>HTTP.sys Configuration</b> .....	5
<b>LDAP SSO Configuration</b> .....	5
INSTALLATION.....	6
<b>CXAC USER ADMINISTRATION LOGIN .....</b>	<b>7</b>
<b>CHECKMARX LOGIN .....</b>	<b>8</b>
<b>GETTING TO KNOW THE ACCESS CONTROL WEB INTERFACE.....</b>	<b>10</b>
<b>ACCESS CONTROL – USERS TAB.....</b>	<b>11</b>
SEARCH FOR USERS.....	11
EXPORT USERS LIST (.CSV) .....	11
FILTER BY USER COLUMNS.....	11
<b>Examples of filtering options</b> .....	12
ADD A NEW USER .....	12
<i>Add New User – General Tab</i> .....	12
<i>Add LDAP User – General Tab</i> .....	14
<b>Import New LDAP Users from Directory</b> .....	14
<i>Deactivate / Activate a User</i> .....	15
<i>Add a New User – Teams Tab</i> .....	16
<b>Assign Teams to New Users</b> .....	16
<i>Add a New User – Roles Tab</i> .....	17
<b>Add Roles to New Users</b> .....	17
EDIT USER .....	18
<i>Edit an Existing User’s Details</i> .....	18
<b>Deactivate / Activate a User</b> .....	19
RESET PASSWORD .....	19
<i>Reset an Existing User Password</i> .....	19
DELETE USER.....	20
<b>ACCESS CONTROL – TEAMS TAB.....</b>	<b>21</b>
ADD, DELETE AND RENAME TEAMS .....	22
<i>Add a Team</i> .....	22
<i>Delete a Team</i> .....	22
<i>Rename a Team</i> .....	22
HIERARCHAL STRUCTURING OF TEAMS .....	23
ADD AND REMOVE TEAM MEMBERS.....	24
<i>Add Team Members</i> .....	24
<i>Remove Team Members</i> .....	25
LDAP GROUP MAPPING .....	26
<b>ACCESS CONTROL – SETTINGS TAB.....</b>	<b>28</b>
CONFIGURING SMTP SERVER SETTINGS (GENERAL PAGE) .....	29

CONFIGURING LDAP SERVER SETTINGS (LDAP PAGE) .....	30
<i>LDAP Settings – Server Settings</i> .....	31
<i>LDAP Settings – Directory Settings</i> .....	33
<i>LDAP Settings – Synchronization</i> .....	35

---

## Overview

Checkmarx Access Control Management (CxAC) is a user management solution for user administration managers. Using CxAC, administration managers are provided with a universal view of user access rights and a centralized management console to define unified access control management for all Checkmarx users.

In future releases the CxAC will be integrated into the CxPlatform, delivering a fully featured user interface for access control and user management across the entire Checkmarx product offering.

---

# Setting up CxAC

## Server Host Requirements

The following minimum prerequisites are recommended for the Server host:

- Windows 8 (or later)
- Windows 2008 R2 SP1 (or later)
- Ubuntu 16 (for Linux)
- RHEL\CentOS 7 (For Linux)
- 8GB RAM
- 4-core, 2.8 GHz

## Active Directory – LDAP SSO Configuration

### HTTP.sys Configuration

**NOTE:** HTTP.sys configuration is needed only for enabling Active Directory LDAP SSO.

To configure an HTTP.sys Web host implementation:

1. Add/Edit to appsettings.json

```
"Host": {  
  "Type" : "Http.Sys"  
}
```

2. Restart the application. The AC Windows service should run as a machine administrator.
3. Enable SSL for Http.Sys:
  - a. Create a X509 certificate.
  - b. Import the certificate to the local computer \ personal store
  - c. In a command prompt, as an administrator run the following command:  
> **netsh http add sslcert ipport=0.0.0.0:<port> certhash=<thumbprint> appid=<GUID value>**

```
netsh example
```

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=8137cffe8a40b123fd6b09cdf172a1db184f09c appid={00112233-4455-6677-8899-AABBCCDDEEFF}
```

### LDAP SSO Configuration

If the server is configured with LDAP SSO (only relevant for Active Directory), you can login to Access Control using Windows SSO (no user name / password needed).

To configure LDAP SSO:

1. Configure Access Control with HTTP.sys (see [HTTP.sys Configuration](#)) or host under IIS.

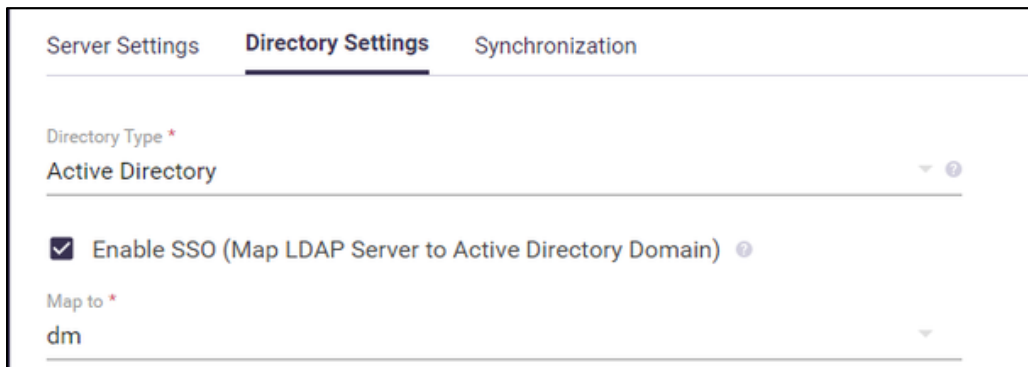
2. Add a domain to Access Control using the REST API (this can also be done via the built-in Swagger):

**NOTES:**

- The domain name can be determined by running "**echo %userdomain%**" in the command prompt
- The fully qualified domain name (FQDN) can be determined by running "**echo %userDNSdomain%**" in the command prompt

```
{  
  "name": "<your domain name for logging in>",  
  "fullyQualifiedDomainName": "<FQDN domain name>"  
}
```

3. Go to (or create) an Active Directory LDAP server (select the checkbox to **Enable SSO** – see [LDAP Settings – Directory Settings](#))



4. Logout, then login again using the **Windows SSO** button.

## Installation

CxAC Installation is performed automatically as part of the Checkmarx installation.

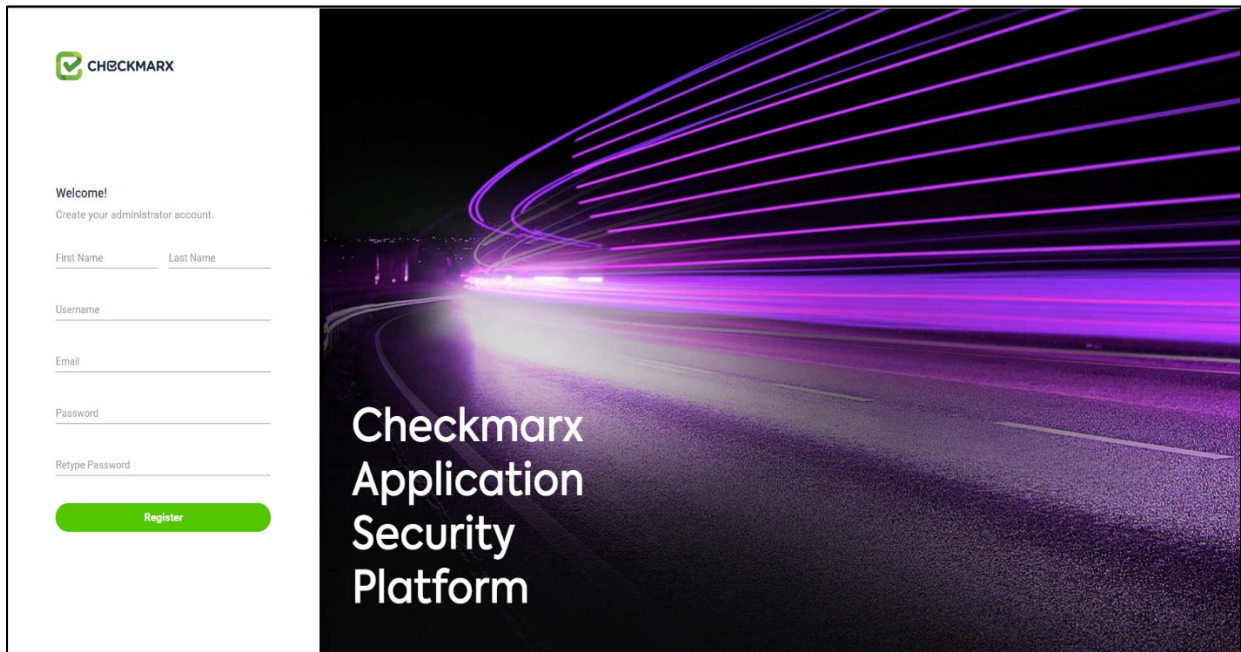
---

## CxAC User Administration Login

To access the CxAC user administration login:

Point your browser to `http://<IAST server>:<port>` where the Access Control port is as defined in the installation.

Upon a successful clean installation, you will be required to create your first administrator user account.



The screenshot shows the registration interface for the Checkmarx Application Security Platform. On the left, there is a white registration form with the Checkmarx logo at the top. The form includes a 'Welcome!' message and a prompt to 'Create your administrator account.' Below this are input fields for 'First Name', 'Last Name', 'Username', 'Email', 'Password', and 'Retype Password'. A green 'Register' button is at the bottom of the form. The right side of the image features a dark background with purple light trails and the text 'Checkmarx Application Security Platform' in white.

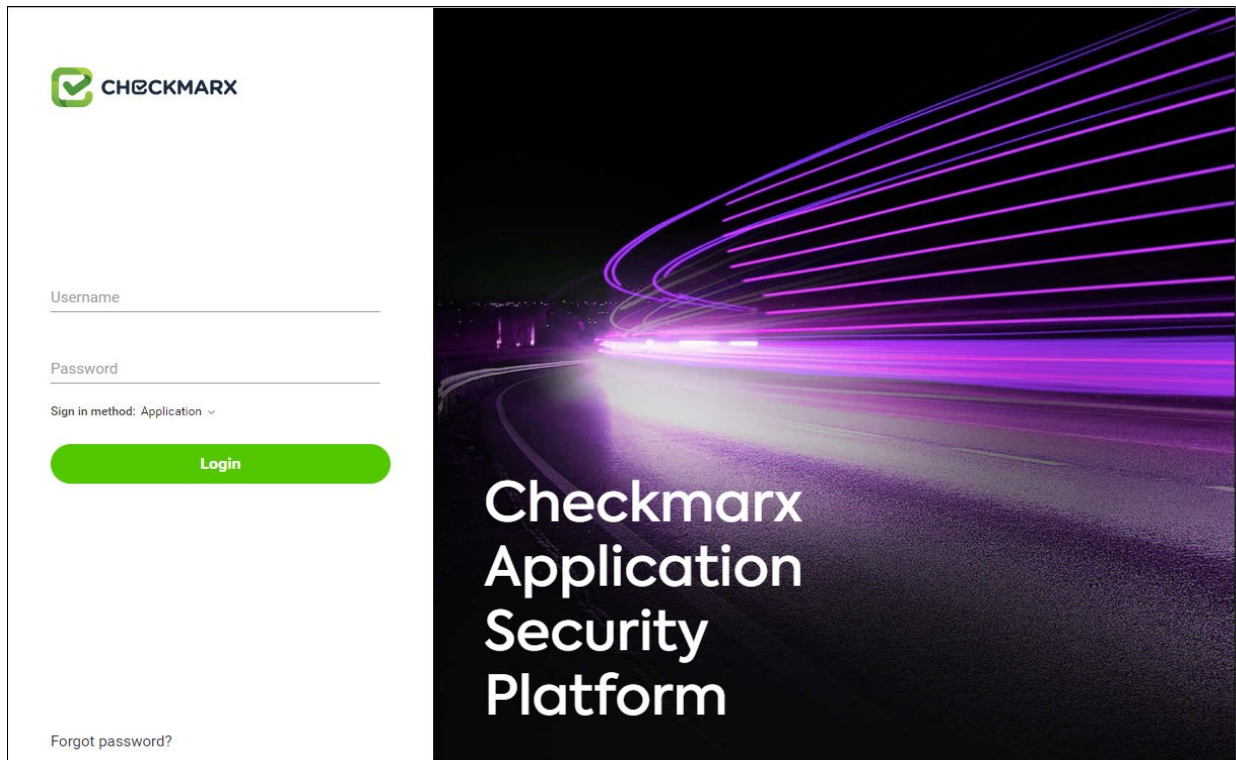
Enter the required administrator user account information:

Field	Description
First & Last Name	Full name for the administrator user
Username	User name for the administrator user as defined for login
Email	Email address for the administrator user
Password	Unique password as defined for the administrator user login. The same Password must be retyped to confirm.

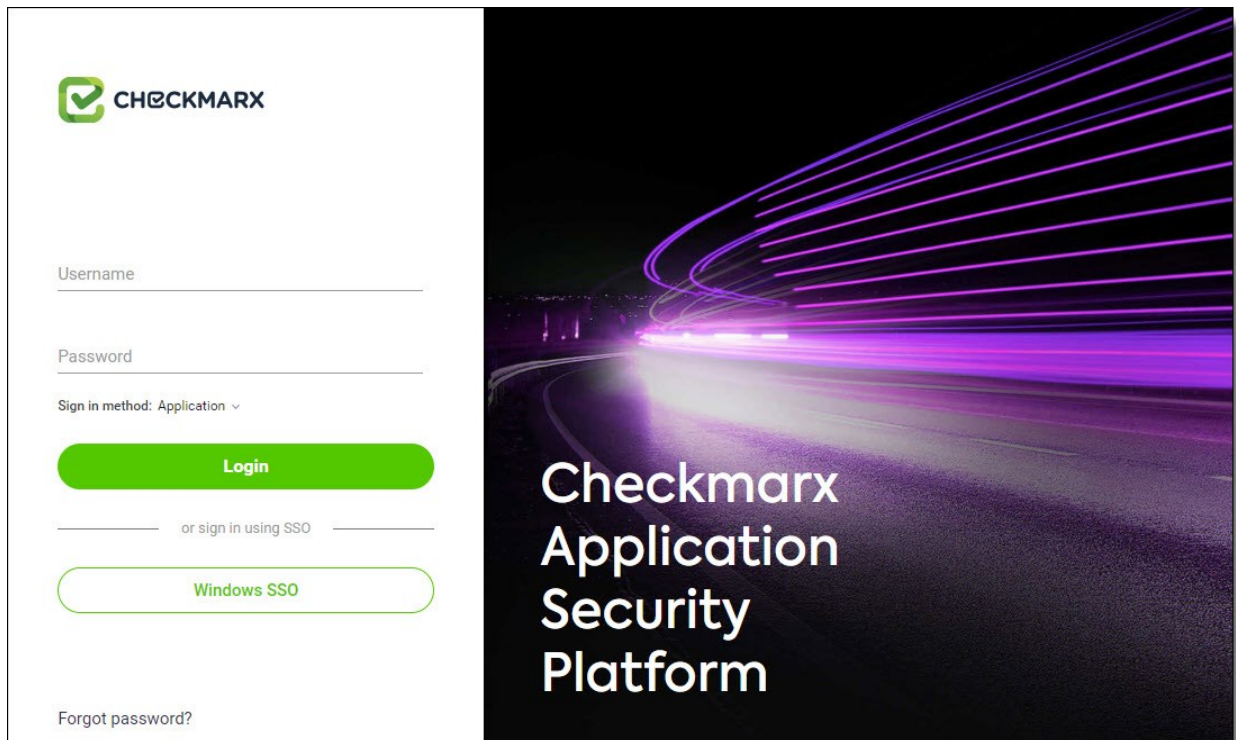
Click **Register**. You will now be taken directly to the Checkmarx Login.

## Checkmarx Login

The login page enables signing in to Access Control with Application or an LDAP account:



If the server has LDAP SSO configured, a login using Windows SSO is provided:





Field	Description
User name	User name, as defined for administrator user login
Password	Unique password as defined for the user login. Same password must be retyped to confirm.
Sign in method	Select a sign in method: Application, or the name of any configured LDAP server(s)
Login	After selecting the sign in method, click Login
Windows SSO	If the server has <b>LDAP SSO</b> configured, you can login using Windows SSO (no user name / password needed).

Once the Checkmarx Login window is displayed, enter the user login credentials and select a sign in method, then click Login (or sign in using Windows SSO).

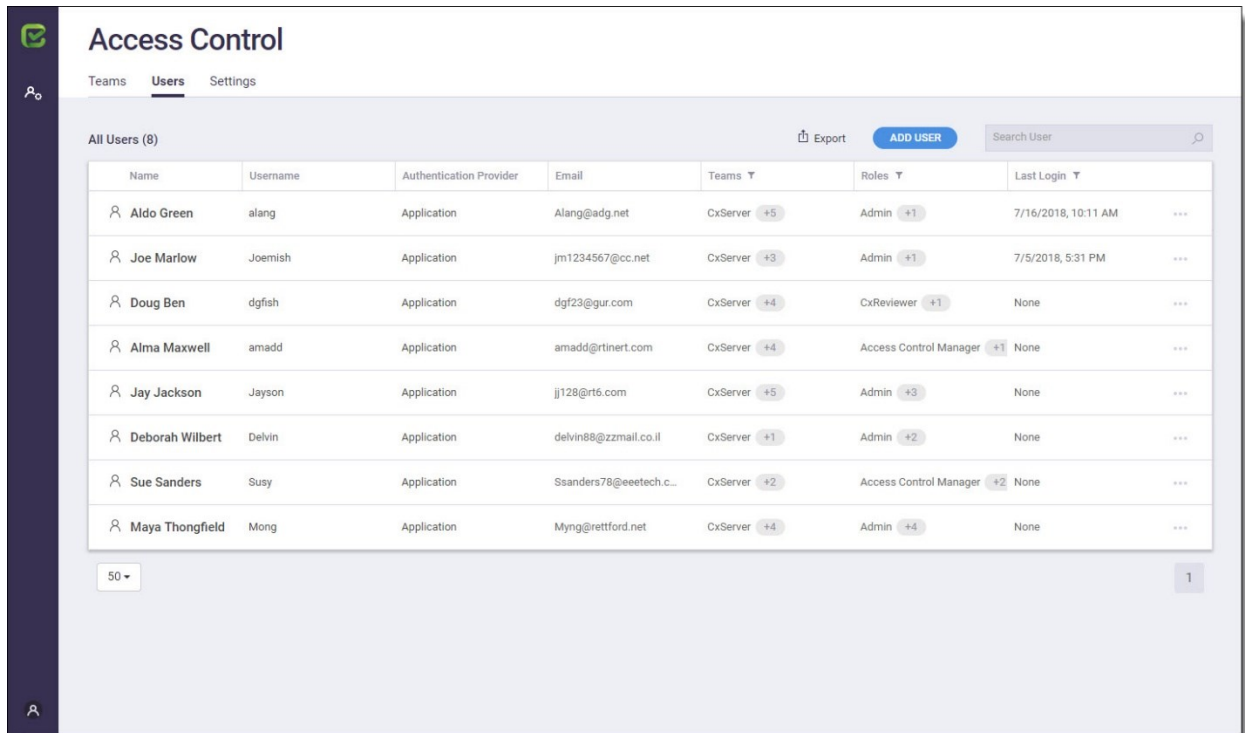
If you forgot your password, simply click 'Forgot password' on the login screen and CxAC will send you a temporary password.

**NOTE:** The 'Forgot Password' option is only relevant if an SMTP server is already configured in the system, as an email with a 'reset password' link will be sent to the registered account.

## Getting to Know the Access Control Web Interface

Once you have logged in to CxAC, the Access Control page is displayed.

The Access Control page provide user management and access control settings. This page is divided into three areas of attention (**Teams**, **Users** and **Settings**), each with its own navigation tab.



The screenshot displays the 'Access Control' web interface. At the top, there are navigation tabs for 'Teams', 'Users', and 'Settings'. The 'Users' tab is active. Below the tabs, there is a header area with 'All Users (8)', an 'Export' button, an 'ADD USER' button, and a search bar labeled 'Search User'. The main content is a table listing users with columns for Name, Username, Authentication Provider, Email, Teams, Roles, and Last Login. The table contains 8 rows of user data. At the bottom left, there is a dropdown menu set to '50', and at the bottom right, there is a page number '1'.



Name	Username	Authentication Provider	Email	Teams	Roles	Last Login
Aldo Green	alang	Application	Alang@adg.net	CxServer +5	Admin +1	7/16/2018, 10:11 AM
Joe Marlow	Joemish	Application	jfm1234567@cc.net	CxServer +3	Admin +1	7/5/2018, 5:31 PM
Doug Ben	dgfish	Application	dgf23@gur.com	CxServer +4	CxReviewer +1	None
Alma Maxwell	amadd	Application	amadd@rtinert.com	CxServer +4	Access Control Manager +1	None
Jay Jackson	Jayson	Application	jj128@rt6.com	CxServer +5	Admin +3	None
Deborah Wilbert	Delvin	Application	delvin88@zzmail.co.il	CxServer +1	Admin +2	None
Sue Sanders	Susy	Application	Ssanders78@eeetech.c...	CxServer +2	Access Control Manager +2	None
Maya Thongfield	Mong	Application	Myng@rettford.net	CxServer +4	Admin +4	None

To logout from CxAC, click the User Management icon  and select **Logout**.

---

## Access Control – Users Tab

The Users tab provides the following information columns/options:

Column	Description
<b>Name</b>	Users full name
<b>User name</b>	User name as defined for login credentials
<b>Authentication Provider</b>	The method used for authentication: <b>Application</b> , <b>LDAP server</b> (name of configured LDAP server)
<b>Email</b>	Users email address
<b>Teams</b>	This team(s) assigned to the user (at least one team per user). Multiple teams can be defined. You can also filter the users displayed in this list by teams (see <i>Filter by User Column</i> , below). <b>NOTE:</b> If multiple teams are assigned, a multiple team indicator  is displayed in the Team column for the user. Hover the mouse over this indicator to display the assigned teams.
<b>Role</b>	Lists the role(s) given to each user. You can also filter the users displayed in this list by roles (see <i>Filter by User Column</i> , below). <b>NOTE:</b> If multiple roles are assigned a multiple role indicator  is displayed in the Role column for the user. Hover the mouse over this indicator to display the assigned roles.
<b>Last Login</b>	This represents the last time the user logged into CxAC. You can filter the users displayed in this list by last login timeframes (see <i>Filter by User Column</i> below).

### Search for Users


In the Users List, you can search for a specific user by any string contained within the user information. The list will be filtered as you type.

**NOTE:** All fields are searchable except for filtered fields (Teams, Roles and Last Login).

### Export Users List (.csv)

To export the full list of CxAC users to CSV format, click **Export**. The CxAC **users.csv** file is downloaded to your default download directory.

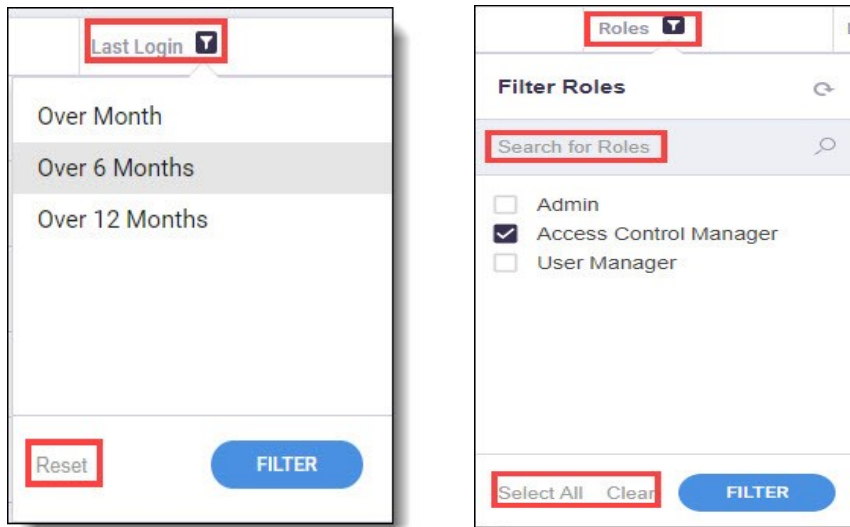
### Filter By User Columns

You can filter certain columns (**Teams**, **Roles** and **Last Login** only) in the Users tab. Simply click on the filter  icon, select the desired filtering option(s), and then click **Filter**. The results are displayed.

You can search for a specific filtering option by entering searchable text in the **Search For** field.

In addition, you can click **Select All** (selects all checkboxes), **Clear** (clears all checkboxes), or **Reset** (reverts back to the default “not-selected” state). Then click **Filter**.

### Examples of filtering options:



### Add a New User

The Add New User dialog enables inputting not just the user's personal details (manually, or by importing an existing user from an LDAP directory), but also respective user team(s) and role(s).

#### Add New User – General Tab

To add a new user to CxAC, click the **Add User** button. The **Add New User** window > **General** tab is displayed by default.

Fill in the required information for the General tab (see table below for details).

The screenshot shows a 'Add New User' dialog box with a close button (X) in the top right corner. The 'General' tab is selected, with 'Teams' and 'Roles' tabs also visible. An 'Import From Directory' button is located in the top right of the form area. The form contains the following fields:

- First Name \* (required)
- Last Name \* (required)
- Username \* (required)
- Email \* (required)
- Job Title
- Phone
- Mobile Phone
- Country (dropdown menu)
- Other
- Locale (dropdown menu)
- Password \* (required)
- Retype Password \* (required)
- Expiration Date: 7/9/2021
- Active User:

At the bottom right, there are 'CANCEL' and 'SAVE' buttons.

The **General** tab provides the following information fields for user data:

Field	Description
<b>First Name *</b>	User's first name
<b>Last Name *</b>	User's last name
<b>User Name *</b>	User's name as defined for login credentials. <b>NOTE:</b> LDAP users cannot edit the user name.
<b>Email *</b>	User's email address
<b>Job Title</b>	Responsibilities of the user's position or the level of the job
<b>Phone</b>	User's telephone number
<b>Mobile Phone</b>	User's mobile telephone number
<b>Country</b>	Country where the user is located
<b>Other</b>	Any other information
<b>Locale</b>	User's preferred language. <b>NOTE:</b> The only supported language in this version is English (United States).
<b>Password *</b>	User's unique password. Must be retyped to confirm. <b>NOTE:</b> An LDAP user's password cannot be reset by an administrator, as it is determined only by the LDAP Server.
<b>Retype Password</b>	Re-enter password
<b>Expiration Date</b>	Click in the field to set the date after which the user should be automatically deactivated. <b>NOTE:</b> For LDAP users there is no expiration date as the expiration is managed by the LDAP server, therefore the expiration date field is disabled.

Field	Description
<b>Activate User</b>	All new users are activated, by default. You can deactivate the user by using the toggle option (see <i>Deactivate a User</i> ).

\* indicates required field

## Add LDAP User – General Tab

For LDAP users only:


- An administrator cannot reset an LDAP user's password, as it is determined only by the LDAP Server.
- An LDAP user cannot use the "Forgot password" link
- An LDAP user cannot change the User name or Expiration Date fields

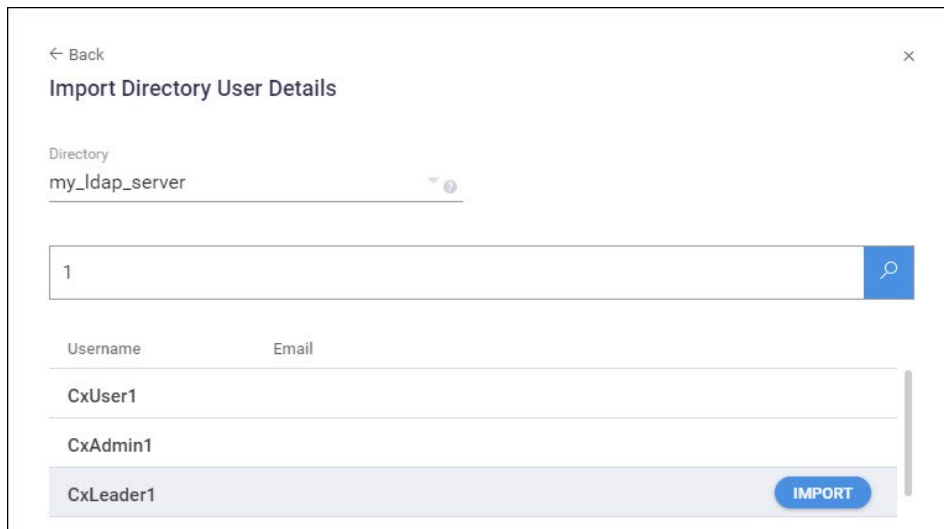
## Import New LDAP Users from Directory

The **Import from Directory** link appears only when there is at least one active LDAP server configured. When creating new LDAP users, this enables you to add (by importing from the directory) new user details manually – one user at a time, which populates the following user-detail fields in the **Add New User** window:

- **User name**
- **First name**
- **Last name**
- **Email address**

In the **Directory** field, click the arrow and then select a directory.

In the search field you can search the selected directory for the username by entering, for example, a **username**, a **part of a username** or uniquely-identifying **alphanumeric characters** (from which the user name is comprised), and then click  to display the results:



For each displayed result that you wish to import, hover the cursor over it and then click its **Import** button. The user's details now appear in its **Add New User** window. Scroll to each field making sure all required information is entered. See *Add New User*, above.

### Deactivate / Activate a User



All new users are activated by default. In the Add New User dialog use the toggle option to deactivate / activate the user as needed, and confirm the change by clicking **Save**.

On the list of users (User's tab), deactivated users are indicated with a red icon:



Users can also be deactivated via the LDAP Server settings, where a periodically-performed sync (if enabled) deactivates all deleted LDAP users (see [LDAP Settings – Synchronization](#))

**NOTE:** Deactivated users can be reactivated at any point.

### Saving Information in the General Tab

In the Add New User window, when finished with the General tab, click **Save**. A message will prompt you to go on to the next (**Teams**) tab to complete.

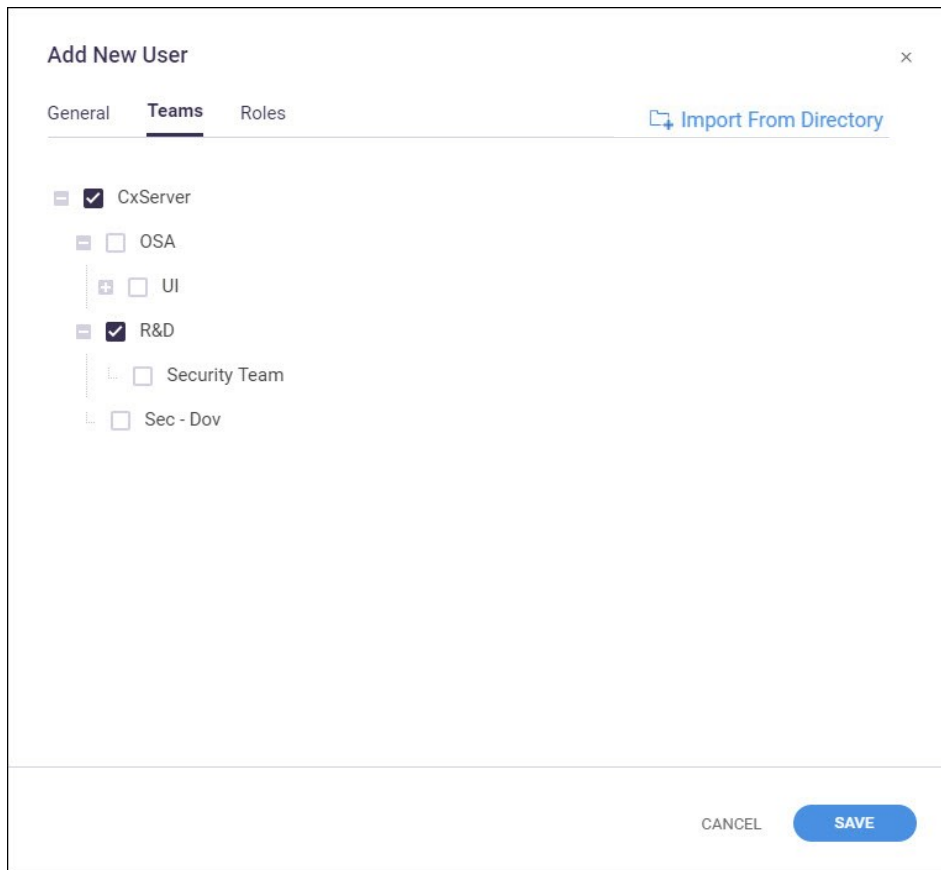
**NOTE:** In the Add New User window, both the **General** and **Teams** tabs are mandatory. The Roles tab is optional.

## Add a New User – Teams Tab

### Assign Teams to New Users

From the **Add New User – Teams** tab you assign team(s) to the new user by clicking the relevant checkboxes.

When finished with the Teams tab, click **Save**. A message will prompt you to go on to the next (optional) **Roles** tab to complete.



The screenshot shows a dialog box titled "Add New User" with a close button (X) in the top right corner. The dialog has three tabs: "General", "Teams", and "Roles". The "Teams" tab is currently selected. In the top right corner of the dialog, there is a link that says "Import From Directory" with a small icon to its left. Below the tabs, there is a list of teams with checkboxes next to them. The teams listed are: CxServer (checked), OSA (unchecked), UI (unchecked), R&D (checked), Security Team (unchecked), and Sec - Dov (unchecked). At the bottom right of the dialog, there are two buttons: "CANCEL" and "SAVE". The "SAVE" button is highlighted in blue.

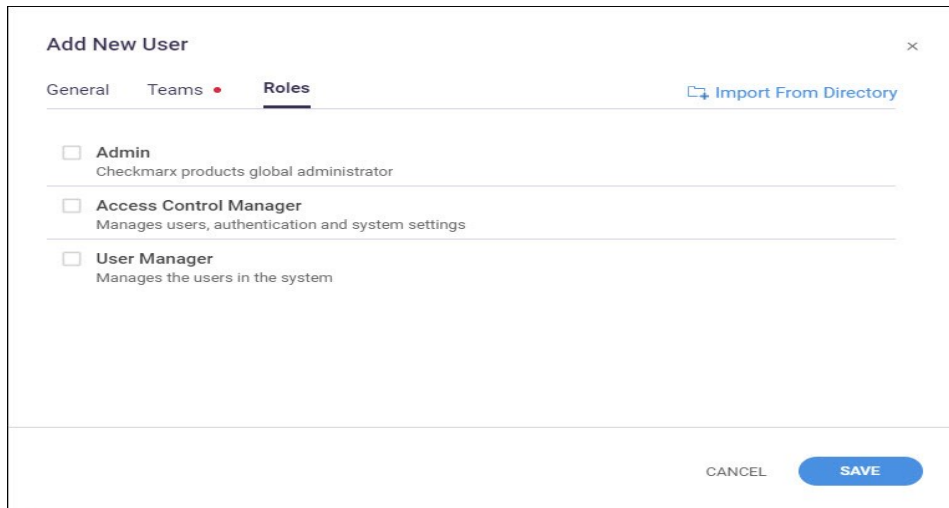


## Add a New User – Roles Tab

### Add Roles to New Users

From the **Add New User > Roles tab**, assign role(s) to a user by clicking the relevant checkboxes.

When finished with the Roles tab, click **Save**. If you have already completed the required **General** and **Teams** tabs, the newly created user will appear in the **Access Control > Users** list.



The screenshot shows a modal window titled "Add New User" with a close button (X) in the top right corner. Below the title bar, there are three tabs: "General", "Teams", and "Roles". The "Roles" tab is currently selected and highlighted with a red dot. To the right of the tabs is a link that says "Import From Directory" with a small icon. Below the tabs, there is a list of three roles, each with an unchecked checkbox and a description:

- Admin**  
Checkmarx products global administrator
- Access Control Manager**  
Manages users, authentication and system settings
- User Manager**  
Manages the users in the system

At the bottom right of the dialog, there are two buttons: "CANCEL" and "SAVE".


The **Add New User > Roles** tab provides default roles.

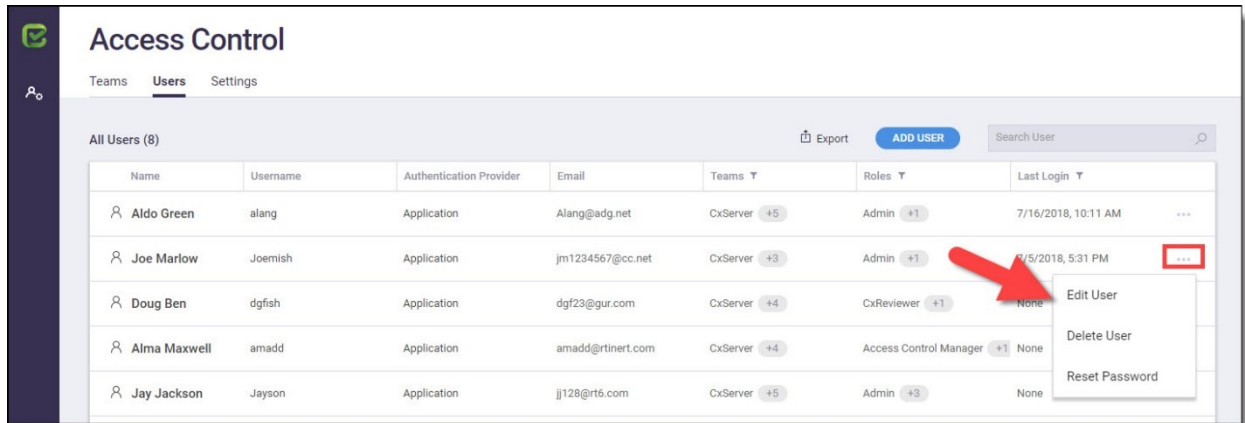
**NOTE:** The default roles displaying will differ according to the Checkmarx product.

Field	Type	Description
<b>Admin</b>	Access Control	Checkmarx products global administrator
<b>Access Control Manager</b>	Access Control	Manages users, authentication and system settings
<b>User Manager</b>	Access Control	Manages the users in the system
<b>CxIAST Reviewer</b>	CxIAST	Limited permissions on selected applications
<b>CxIAST Auditor</b>	CxIAST	Editing permissions for the Query languages
<b>CxIAST Admin</b>	CxIAST	Full account access
<b>CxIAST Power Reviewer</b>	CxIAST	Full permissions on selected applications

## Edit User

### Edit an Existing User's Details

From the **Access Control > Users tab**, to edit an existing user's details, click the user's  icon and then select **Edit User**.



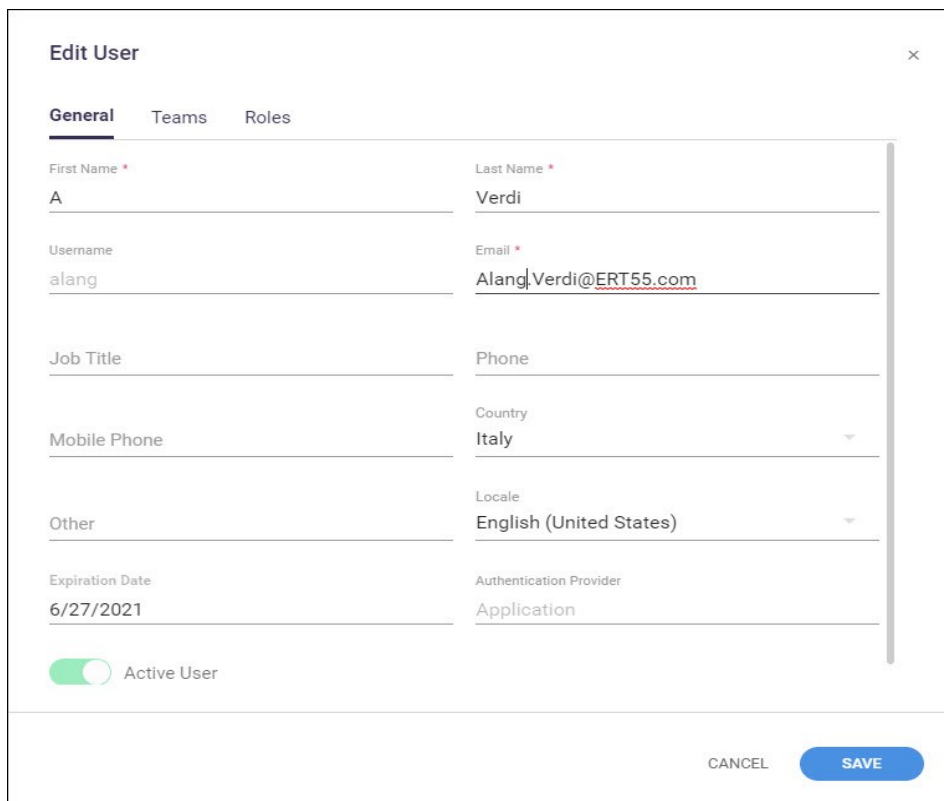
The screenshot shows the 'Access Control' interface with the 'Users' tab selected. A table lists users with columns for Name, Username, Authentication Provider, Email, Teams, Roles, and Last Login. A red arrow points to the 'More options' icon (three dots) for Joe Marlow, which has opened a dropdown menu with options: Edit User, Delete User, and Reset Password.

Name	Username	Authentication Provider	Email	Teams	Roles	Last Login	
Aldo Green	alang	Application	Alang@adg.net	CxServer +5	Admin +1	7/16/2018, 10:11 AM	...
Joe Marlow	Joemish	Application	jm1234567@cc.net	CxServer +3	Admin +1	7/5/2018, 5:31 PM	...
Doug Ben	dgfish	Application	dgf23@gur.com	CxServer +4	CxReviewer +1	None	...
Alma Maxwell	amadd	Application	amadd@rtinert.com	CxServer +4	Access Control Manager +1	None	...
Jay Jackson	Jayson	Application	jj128@rt6.com	CxServer +5	Admin +3	None	...

From the **Edit User** dialog that is displayed, make your changes on each of the 3 tabs (**General, Teams, Roles**) as needed.

**NOTE:** The General and Team tabs are mandatory, while the Roles tab is optional.

Click **Save** on the last tab edited (this will save changes on all tabs edited). The user's details are saved and any new changes are displayed on the Users List page.

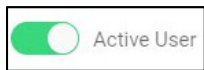


The 'Edit User' dialog box is shown with the 'General' tab selected. It contains the following fields:

- First Name: A
- Last Name: Verdi
- Username: alang
- Email: Alang.Verdi@ERT55.com
- Job Title: (empty)
- Phone: (empty)
- Mobile Phone: (empty)
- Country: Italy
- Other: (empty)
- Locale: English (United States)
- Expiration Date: 6/27/2021
- Authentication Provider: Application

At the bottom, there is a toggle for 'Active User' (which is turned on) and two buttons: 'CANCEL' and 'SAVE'.

## Deactivate / Activate a User



All new users are activated by default. In the Edit User dialog use the toggle option to deactivate / activate the user as needed, and confirm the change by clicking **Save**.

On the list of users (User's tab), deactivated users are indicated with a red icon:



Users can also be deactivated via the LDAP Server settings, where a periodically-performed sync (if enabled) deactivates all deleted LDAP users (see [LDAP Settings – Synchronization](#)).


**NOTE:** Deactivated users can be reactivated at any point.

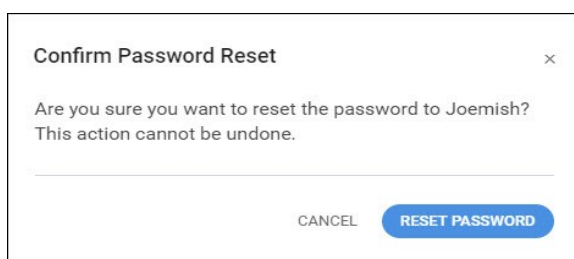
## Reset Password

### Reset an Existing User Password

**NOTE:** In order to reset an existing user's password, the SMTP server must be configured in the system. If not, the user must contact the system-responsible person (such as a Cx Administrator or User Manager) who will provide the user with a temporary password, which is changeable after signing in with it the first time.

**NOTE:** Once you reset a password, it cannot be undone.

To reset an existing user's password, click the user's  icon and select **Reset Password** from the dropdown menu. The Confirm Password Reset dialog is displayed.



Click **Reset Password** on the Confirm Password Reset dialog. A message notifies you that *"A new temporary password has been generated"* and you are provided a temporary new password for logging in (you will be asked to change this temporary password upon first login).

Click **Copy** to copy the temporary password to the clipboard, and then close the dialog.

Logout of CxAC, and then enter (or paste) your login credentials using the copied temporary password. The Change Temporary Password window is displayed.


The screenshot shows a web interface for changing a temporary password. At the top left is the CHECKMARX logo. The main heading is 'Change temporary password'. Below this are three input fields: 'Temporary Password', 'New Password', and 'Confirm new password'. The 'New Password' field has a small eye icon to its right. At the bottom center is a green button labeled 'Update Password'.

Change the temporary password: minimum 6 characters that includes at least 1 in uppercase, at least 1 non-alphanumeric character, and at least 1 digit.

Click **Update Password**. You are now back in Access Control.

## Delete User

**NOTE:** When a user is deleted, it cannot be undone.

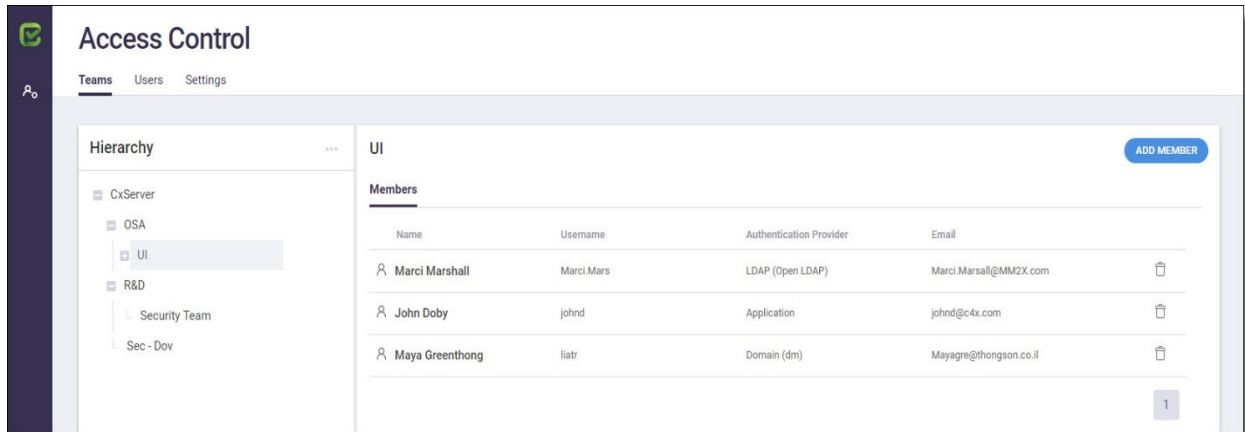
To delete a user (other than yourself), click the user's  icon and then select **Delete User**.

Confirm that you want to continue with the user deletion by clicking **Delete**. The user is deleted from the CxAC and is no longer displayed in the Users List page.

The dialog box is titled 'Delete User?' and has a close button (X) in the top right corner. The main text asks, 'Are you sure you want to delete user "Joemish"?' Below the text is a horizontal line. At the bottom, there are two buttons: 'CANCEL' and 'DELETE'.

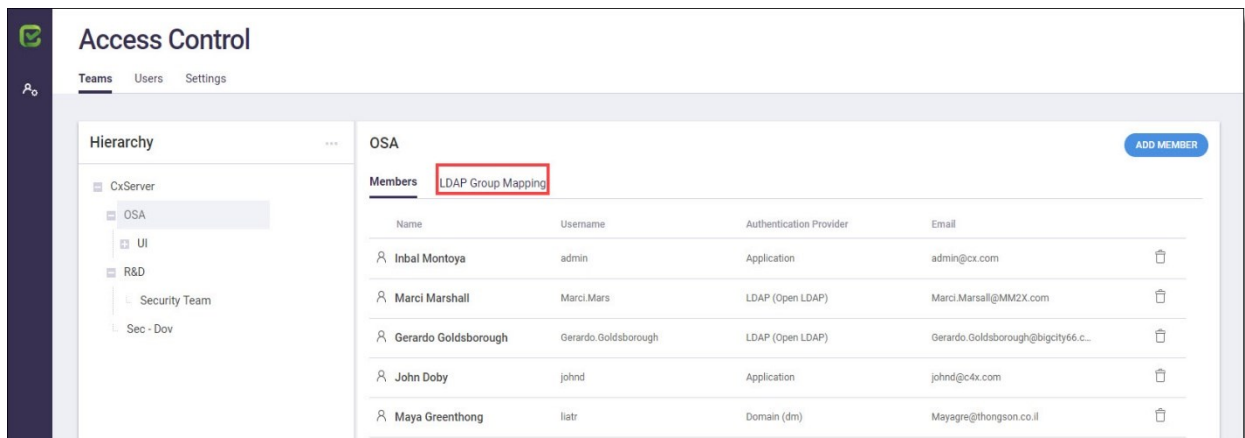
## Access Control – Teams Tab

The Teams tab enables you to add/delete, rename and structure your organization's teams, and assign users to those teams.



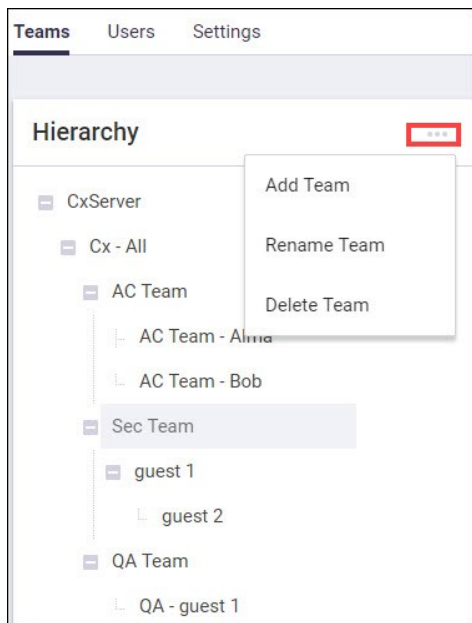
In addition, on the Teams tab you can also perform **LDAP Group Mapping**, where you search (using group name) to map group(s) to an LDAP directory.

**NOTE:** This feature is available only if specific configuration criteria are met (see [LDAP Group Mapping](#) for details).



## Add, Delete and Rename Teams

In the **Teams tab > Hierarchy pane**, you can add/delete or rename teams.



### Add a Team

In the hierarchal tree structure, click on the level that will be the “parent” level to the team you are creating (the level directly above what you wish to create), then click **☰** and select **Add Team**.

Enter a team name in the dialog box using any character except backslash (\), and then click **Add Team**. The newly added team name now appears in the tree.

### Delete a Team

In the hierarchal tree structure, click on the team to delete, then click **☰** and select **Delete Team**. The Delete Team? Dialog is displayed informing that if deleted, all LDAP group mappings for the team will be removed.

Click **Delete** on the dialog box to delete the team. A message informs that the team is deleted, and it no longer appears on the tree structure.

### Rename a Team

In the hierarchal tree structure, click on the team to delete, then click **☰** and select **Rename Team**.

Enter (type over) a team name in the dialog box using any character except backslash (\), and then click **Save**. The renamed team name now appears in the tree.

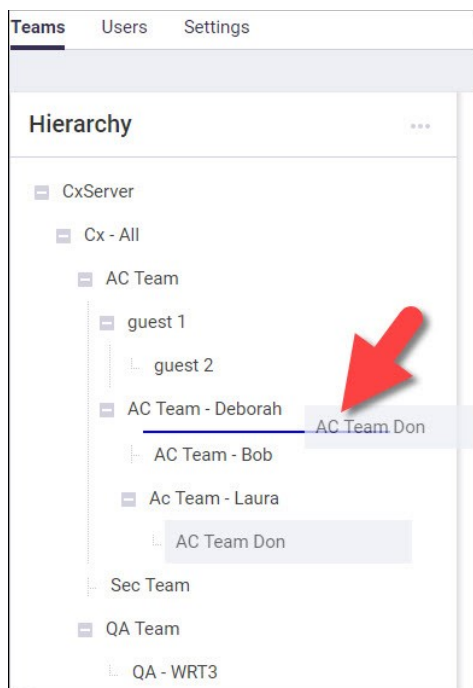
## Hierarchal Structuring of Teams

In the **Teams tab > Hierarchy pane**, you can also change the hierarchal nesting structure of the teams in the tree.

**NOTE:** Moving a higher-level ('parent-level') team in the tree will also move any respective teams that are nested under it ('children-level' teams), preserving the same parent–child nesting structure relationship of those teams.

To move a team, while you left-click on it, drag it to its new position (under another team). When dragging it, you may need to position it a bit to the right until you see a blue line, marking the position where you are repositioning the team. A confirmation prompt informs you where the team will be moved to. Click **Move** on the confirmation prompt.

In this example, the 'AC Team Don' is being moved from under 'AC Team Laura' to a higher level (under 'AC Team Deborah') – where it now will be the same level as the 'AC Team Laura':



## Add and Remove Team Members

In **Teams tab > Members**, you can add/delete members for any existing **team** (the user, however, will not be deleted).

### Add Team Members

In the Hierarchy tree, click on the team that you want to assign member(s) to.

Click **Add Member**. Existing members of the team are displayed in the **Add Team Member** window.

Search by name using the Search Users field, or scroll through the list and select the checkboxes of members to add to the team.

**Add Team Member** ×

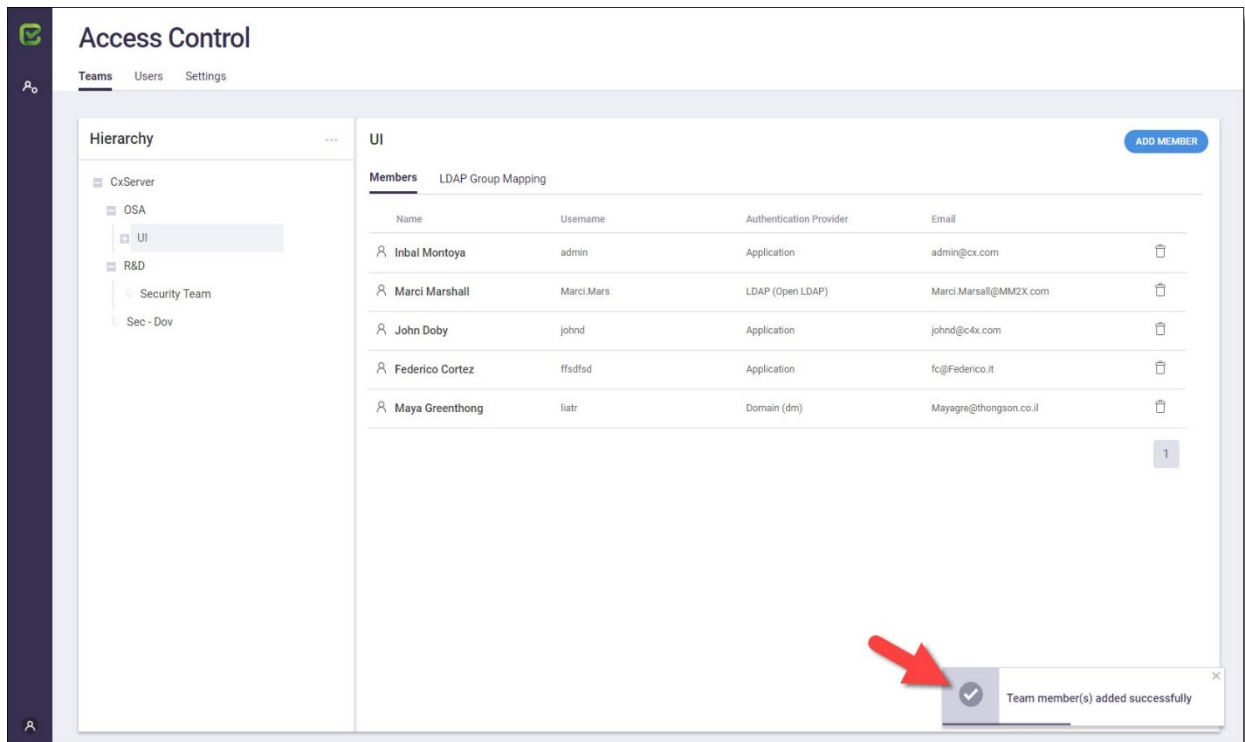
Search Users 🔍

Name	Username	Authentication Provider
<input checked="" type="checkbox"/> Inbal Montoya	admin	Application
<input type="checkbox"/> Aldo Campoverdi	a	Application
<input type="checkbox"/> Gerardo Goldsborough	Gerardo.Goldsborough	LDAP (Open LDAP)
<input type="checkbox"/> Joel Gersh	yoelG	LDAP (my_ldap_server)
<input checked="" type="checkbox"/> Federico Cortez	ffsdfsd	Application
<input type="checkbox"/> Elena Dleif	notusermng	Application
<input type="checkbox"/> Marjorie Buttersworth	dfgdfgdfg	Application
<input type="checkbox"/> Igor Zimmer	user	Application
<input type="checkbox"/> Peter Stinson	petert	LDAP (mv ldap server)

CANCEL **ADD MEMBERS (2)**




Click **Add Members**. The member(s) are added to the team:



## Remove Team Members

In the Hierarchy tree, click on the team from which you want to remove a member. All current members for the team are displayed.

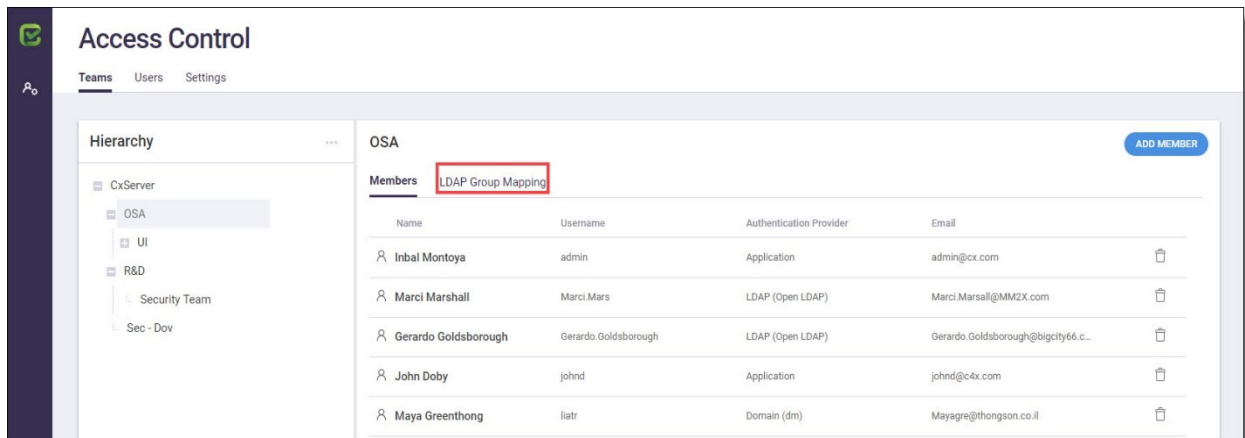
In the Members window, click the Remove Member icon (  ) of a member you want to remove from the team.

On the *Remove member from team* confirmation message, click **Remove**. A message confirms the removal.

## LDAP Group Mapping

From the Teams tab you can perform **LDAP Group Mapping**, where you search (using group name) to map group(s) to an LDAP directory. This feature is available only if all of the following apply:

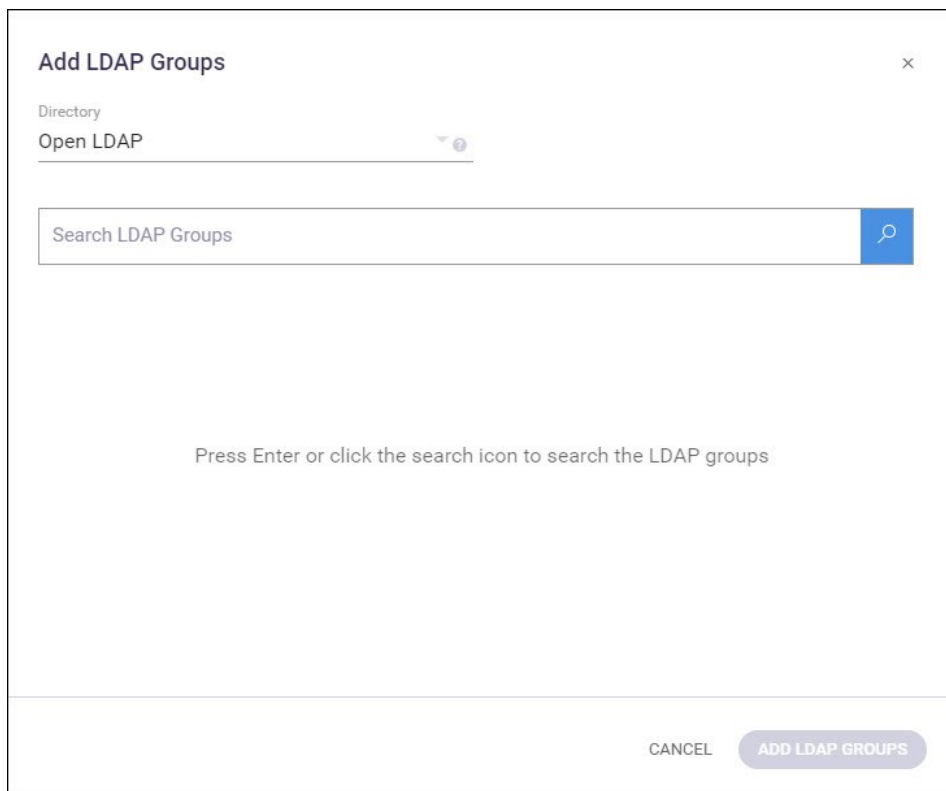
- At least 1 configured LDAP server is active
- Synchronization is enabled (see [Settings tab > LDAP > Synchronization](#))
- Advanced Team & Role Mapping is enabled (see [Settings tab > LDAP > Synchronization](#))
- User has *Manage Authentication Providers* permissions



The screenshot shows the 'Access Control' interface. On the left, a 'Hierarchy' tree shows 'CxServer' > 'OSA' selected. The main area is titled 'OSA' and has a sub-tab 'LDAP Group Mapping' highlighted with a red box. Below this is a table of team members:


Name	Username	Authentication Provider	Email	
Inbal Montoya	admin	Application	admin@cx.com	
Marci Marshall	Marci.Mars	LDAP (Open LDAP)	Marci.Marsall@MM2X.com	
Gerardo Goldsborough	Gerardo.Goldsborough	LDAP (Open LDAP)	Gerardo.Goldsborough@bigcity66.c...	
John Doby	johnd	Application	johnd@c4x.com	
Maya Greenthong	liatr	Domain (dm)	Mayagre@thongson.co.il	

From **Teams tab > LDAP Group Mapping tab**, click **Add LDAP Group Mapping**. The Add LDAP Groups window is displayed.



The 'Add LDAP Groups' dialog window is shown. It has a title bar with a close button (X). Below the title, it says 'Directory' and 'Open LDAP'. There is a search input field with the placeholder text 'Search LDAP Groups' and a search icon (magnifying glass) on the right. Below the search field, there is a message: 'Press Enter or click the search icon to search the LDAP groups'. At the bottom of the dialog, there are two buttons: 'CANCEL' and 'ADD LDAP GROUPS'.

In the **Directory** field, click the arrow and select the directory that you will map the group(s) to.

In the **Search LDAP Groups** field, search for an LDAP group name by entering searchable text/characters, and then click  or press **Enter** to display the results.

**NOTE:** All characters are permitted in the search field, except for the backslash (\).

If an LDAP group name has already been mapped to the same directory, in the search result list it will appear as non-selectable (greyed) and labeled 'mapped':

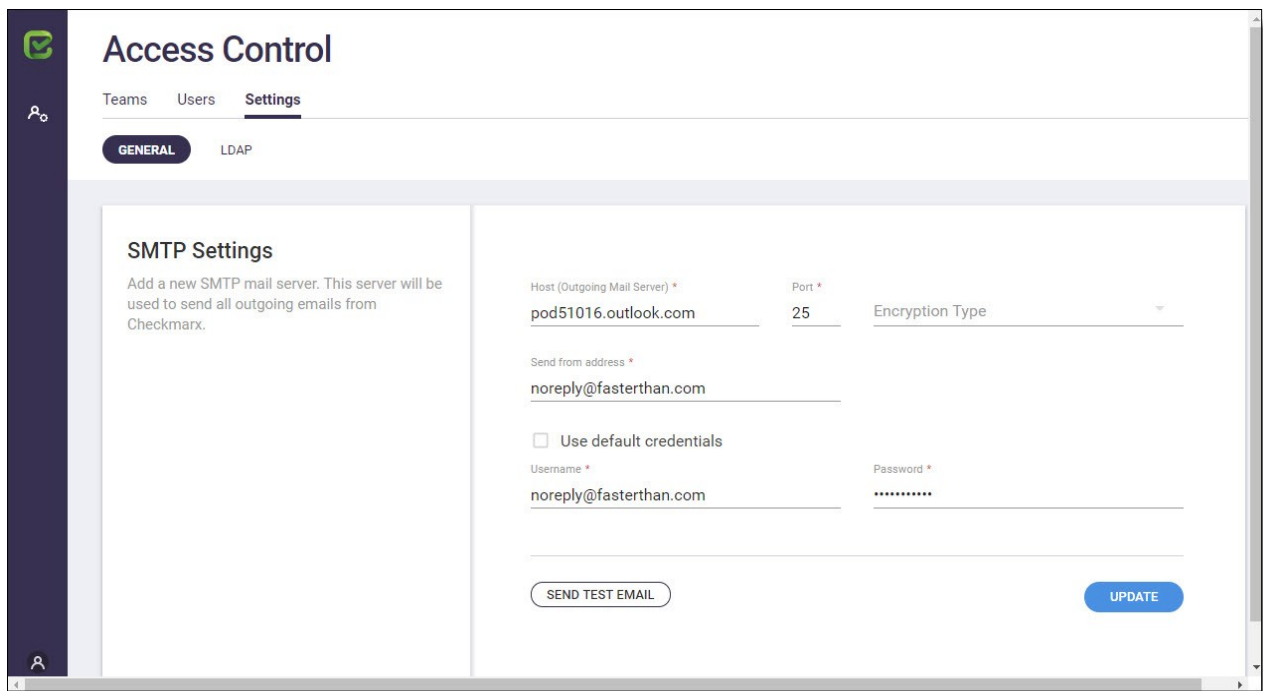


On the results list, select the LDAP group(s) to map to the directory, and then click the **Add LDAP Groups** button. The LDAP groups are mapped, and are displayed in the LDAP Group Mapping list.

## Access Control – Settings Tab

The Access Control Settings provides the CxAC Admin user with the possibility to setup and change global settings for the CxAC, pertaining to settings for the SMTP mail server and settings for the LDAP server(s).

To enter the Access Control Settings page, click the Access Control Settings icon from the menu and select the Settings tab. The **Settings tab > General (SMTP Settings) page** is displayed.



The screenshot shows the 'Access Control' settings page. The 'Settings' tab is selected, and the 'GENERAL' sub-tab is active. The page is titled 'SMTP Settings' and includes a description: 'Add a new SMTP mail server. This server will be used to send all outgoing emails from Checkmarx.' The form contains the following fields and controls:

- Host (Outgoing Mail Server) \***: pod51016.outlook.com
- Port \***: 25
- Encryption Type**: (Dropdown menu)
- Send from address \***: noreply@fasterthan.com
- Use default credentials
- Username \***: noreply@fasterthan.com
- Password \***: (Masked with dots)

At the bottom of the form, there are two buttons: 'SEND TEST EMAIL' and 'UPDATE'.

## Configuring SMTP Server Settings (General Page)

The CxIAST Server can email administrators about access control changes and alerts. First, however, you need to configure the SMTP settings that the server uses to send these emails.

**NOTE:** Users cannot reset their own password using the 'Forgot Password' option if SMTP server is not configured.

The SMTP Settings page provides the following information fields/options.

Field	Description
<b>Host (Outgoing Mail Server) *</b>	Enter the name or IP address of the outgoing mail server.
<b>Port *</b>	If you are not using the default SMTP port 25 (if encryption is not used), you can change the SMTP port value.
<b>Encryption Type</b>	<b>SSL</b> – Enable SSL to ensure that the connection to your mail server is encrypted and secure. <b>TLS</b> – Enable TLS for a more advanced and secure version of SSL. <b>None</b> – to connect to your mail server without encryption
<b>Send from address *</b>	Enter the address that will send the email (e.g. noreply@checkmarx.com).
<b>User default credentials</b>	Check to use the default credentials.
<b>User Name and Password</b>	Optionally, enter the SMTP user name and password for your pre-configured SMTP server account.
<b>Send Test Email</b>	Once the settings are defined, use this option to validate the connection. Validation is performed by sending and receiving a test email.

\* indicates required field

Enter all the required information, and then click **Send a Test Email** to ensure SMTP connectivity. A message informs you of the test status.

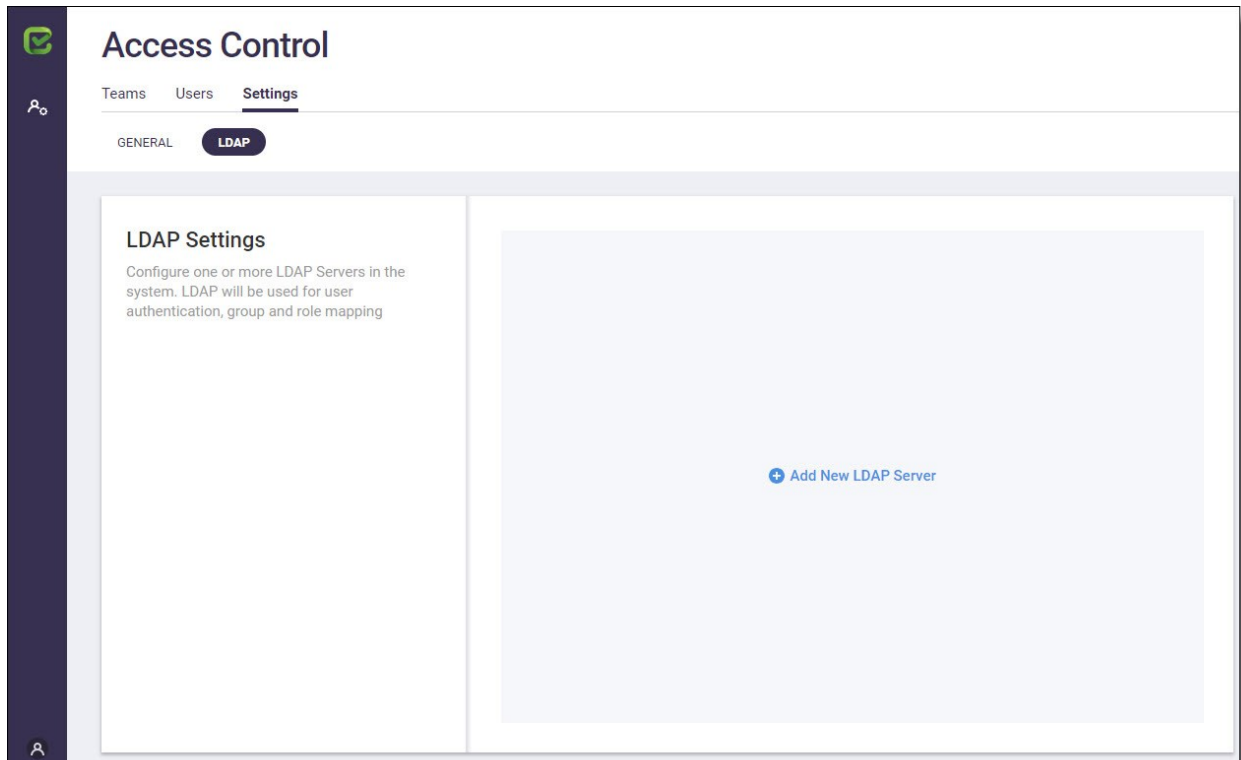
Upon notification of a successful email test, click **Update** to save the settings.



## Configuring LDAP Server Settings (LDAP Page)

Configure one or more LDAP servers in the system. LDAP will be used for user authentication, authorization, group and role mapping.

To configure an LDAP server, go to the **Settings tab > LDAP (LDAP Settings)** page.



Click **Add New LDAP Server**. The **LDAP Servers > Server Settings** tab is displayed.

**NOTE:** Three tabs can be configured for the LDAP server: **Server Settings**, **Directory Settings** (required) and **Synchronization** (optional, disabled by default). Each tab displays the default (but changeable) attributes in its respective fields – according to the directory type selected.

## LDAP Settings – Server Settings

The first of three tabs to configure on the LDAP Servers page is **Server Settings**, where you configure the LDAP server connection settings.

The screenshot displays the 'Access Control' interface with the 'LDAP' tab selected. The main content area is titled 'LDAP Settings' and contains a sub-section 'Server Settings' with three tabs: 'Server Settings' (active), 'Directory Settings', and 'Synchronization'. The 'Server Settings' tab is configured as follows:

- Enable LDAP Server:** A toggle switch is turned on.
- Server Name:** A text input field containing 'Open LDAP'.
- Host Name:** A text input field containing '10.0.1.1'.
- Port:** A text input field containing '389'.
- Username:** A text input field containing 'cn=admin,dc=example,dc=com'.
- Password:** A password input field with masked characters (dots).
- Use SSL:** An unchecked checkbox.
- Buttons:** A 'TEST CONNECTION' button is located below the form fields. At the bottom right, there are 'CANCEL', 'BACK', and 'CONTINUE' buttons.

The **LDAP Settings > Server Settings** page provides the following information fields/options.

Field	Description
<b>Enable LDAP Server</b>	Toggle to enable/disable the LDAP server. <b>NOTE:</b> Disabling the LDAP server will prevent the users of this LDAP server from logging into the system. It will still be possible to manually add users and map LDAP groups to roles.
<b>Server name *</b>	Enter the name of the LDAP server. <b>NOTE:</b> This name that will also be used in the login page.
<b>Host name *</b>	Enter the LDAP server hostname <b>For example:</b> ldap.company.com
<b>Port *</b>	Enter the LDAP server port <b>For example:</b> 389, 636 (for SSL)
<b>User name &amp; Password *</b>	Enter the credentials of the <b>binding user</b> (LDAP bind username and bind password). <b>NOTE:</b> User needs at least <b>read</b> permissions to the LDAP directory. The username can be in the following formats: <domain\username> or <username@domain> or <full user DN> <b>For example:</b> user@domain.name or cn=user,dc=domain,dc=name
<b>Use SSL</b>	Check this to connect to the LDAP server using SSL encryption
<b>Verify SSL certificate</b>	Check this to verify the SSL certificate. <b>NOTE:</b> If you are using an untrusted certificate, you can cancel the verification of certificate to make the connection pass. SSL will still be used and the network will be encrypted.

\* indicates required field

After all information is entered, click **Test Connection** to validate the LDAP connectivity. A message informs you of the test status.

Upon a successful connectivity test, click **Save**, and then configure in **Directory Settings**.



## LDAP Settings – Directory Settings

The second tab to configure on the LDAP Servers page is **Directory Settings**.

Example of Directory Settings page, for the directory type *Active Directory*:

The screenshot shows the 'Directory Settings' tab for an 'Active Directory' server. The interface includes three tabs: 'Server Settings', 'Directory Settings', and 'Synchronization'. The 'Active Directory' type is selected. There is an unchecked checkbox for 'Enable SSO (Map LDAP Server to Active Directory Domain)'. The 'Map to' dropdown is set to 'Select a domain'. Under 'LDAP Schema', the 'Base DN' is 'ou=testing,dc=example,dc=com' and the 'Additional User DN' is 'ou=people'. Under 'User Schema Settings', the 'User Object Class' is 'user' and the 'User Object Filter' is '(&(objectCategory=Person)(sAMAccountName=\*))'. The 'Username Attribute' is 'sAMAccountName', 'User First Name Attribute' is 'givenName', 'User Last Name Attribute' is 'sn', and 'User Email Attribute' is 'mail'. A 'TEST USER SCHEMA' button is located at the bottom left. At the bottom right, there are 'CANCEL', 'BACK', and 'SAVE & CONTINUE' buttons.

Example of Directory Settings page, for the directory type *Open LDAP*:

The screenshot shows the 'Directory Settings' tab for an 'Open LDAP' server. The interface includes three tabs: 'Server Settings', 'Directory Settings', and 'Synchronization'. The 'Open LDAP' type is selected. There is an unchecked checkbox for 'Enable SSO (Map LDAP Server to Active Directory Domain)'. The 'Map to' dropdown is set to 'Select a domain'. Under 'LDAP Schema', the 'Base DN' is 'ou=testing,dc=example,dc=com' and the 'Additional User DN' is 'ou=people'. Under 'User Schema Settings', the 'User Object Class' is 'inetorgperson' and the 'User Object Filter' is '(objectclass=inetorgperson)'. The 'Username Attribute' is 'uid', 'User First Name Attribute' is 'givenName', 'User Last Name Attribute' is 'sn', and 'User Email Attribute' is 'mail'. A 'TEST USER SCHEMA' button is located at the bottom left. At the bottom right, there are 'CANCEL', 'BACK', and 'SAVE & CONTINUE' buttons.

The **LDAP Settings > Directory Settings** page provides the following information fields/options.

Field	Description
<b>Directory Type *</b>	Select from the options: <b>Active Directory, Open LDAP, Custom LDAP Server</b> . Server attributes are automatically populated according to default settings.
<b>Enable SSO</b>	<b>NOTES:</b> <ul style="list-style-type: none"> <li>• Only enabled for the 'Active Directory' directory type</li> <li>• User login with Windows SSO does not require entering login credentials</li> <li>• See <a href="#">Configuring LDAP SSO</a></li> </ul>
<b>Domain *</b>	Select a Windows domain to map the LDAP server to. <b>NOTES:</b> <ul style="list-style-type: none"> <li>• It is only possible to map domains which are not already mapped to an LDAP server</li> <li>• Users not in this domain cannot login through Windows SSO (even though they are part of the LDAP server settings). They will be able to login with their LDAP username and password though.</li> </ul>
<b>Base DN *</b>	The LDAP root node for searching users.
<b>Additional User DN</b>	Limits user search to specific DN (in order to optimize the search time). The additional user DN is appended to the base DN. <b>NOTE:</b> Do not repeat the base DN in this field.
<b>User Object Class *</b>	The LDAP user object class type to use when loading users.
<b>User Object Filter *</b>	The filter expression to use when searching user objects.
<b>Username Attribute *</b>	The attribute field to use on the user object
<b>User First Name Attribute *</b>	The attribute field to use when loading the user's first name.
<b>User Last Name Attribute *</b>	The attribute field to use when loading the user's last name.
<b>User Email Attribute *</b>	The attribute field to use when loading the user's email

\* indicates required field


After all information is entered, click **Test User Schema** to check the connection to the LDAP server, and validate the user schema settings and attributes. A message informs of the test status.

Upon a successful user schema test, click **Save** and then configure in **Synchronization**.

## LDAP Settings – Synchronization

The third tab to configure on the LDAP Servers page is **Synchronization**.

Field	Description
<b>Synchronization enabled/disabled</b>	<p>If synchronization is disabled, users will need to be created manually (via <i>Import from Directory</i> only), as there is no information about role and team in order to create them.</p> <p>Enabling synchronization enables automatically creating new LDAP users who will be automatically assigned to roles and teams, according to their LDAP mapping.</p> <p><b>NOTE:</b> If synchronization is disabled, login can only be performed only using existing LDAP users. If synchronization is enabled, a user can easily login with only user name and password.</p>

Field	Description
<b>ROLE AND TEAM MAPPING</b>	Enables defining the default role(s) and team(s) to be assigned to newly-created LDAP-based users.
<b>Default Role &amp; Default Team *</b>	<p>Define the default role and team that will be assigned to newly-created, LDAP-based users.</p> <p><b>NOTE:</b> A default team (but not a default role) must be selected when synchronization is enabled.</p> <p>These defaults (for Role and Team) will be used in case no <i>Advanced Team and Role Mapping</i> were defined for a current user trying to login.</p>
<b>Automatically update user role and team upon login</b>	<p>If checked, a user's role and team will be automatically updated upon login, according to default or <i>Advanced Team and Role Mapping</i>.</p> <p><b>NOTE:</b> If this feature is not checked, a user's personal details will only be updated once – at the first login.</p>
<b>Periodically sync user availability</b>	<p>If checked, then every 24-hours all LDAP users (usernames) that were deleted from the LDAP server will be deactivated in Access Control (therefore freeing up those licenses).</p> <p>A red indicator next to a user's name (on the list of users – User's tab) indicates the user has been deactivated:</p> <div data-bbox="470 981 826 1061" style="border: 1px solid black; padding: 2px; display: inline-block;">  Marjorie Buttersworth </div> <p><b>NOTE:</b> If the connection to the LDAP server fails, the deleted users will not be deactivated in Access Control.</p>
<b>Advanced Team and Role Mapping</b>	<p>Enables mapping roles and teams to LDAP groups.</p> <p>Enables a user's role to be automatically set according to specific LDAP group DNs. Enables the user to automatically be assigned to a team according to LDAP mapping configuration (see <a href="#">LDAP Group Mapping</a>).</p>
<b>GROUP SCHEMA SETTINGS</b>	Enables defining the search of LDAP groups that can be mapped to teams (see <a href="#">LDAP Group Mapping</a> ).
<b>Additional Group DN</b>	<p><b>[Optional]:</b> The Additional Group DN (appended to the Base DN) reduces the search scope to a specific DN when searching for groups.</p> <p><b>NOTE:</b> Do not repeat the Base DN in this field.</p>
<b>Group Object Class</b>	<p>Used for team mapping, it defines the group object class, and limits group searching to a specific DN.</p> <p><b>NOTE:</b> Required if <i>Synchronization</i> and <i>Advanced Team and Role Mapping</i> are enabled.</p>
<b>Group Object Filter</b>	<p>Used for team mapping, Group Object Filter is an LDAP filter expression for use when searching groups.</p> <p><b>NOTE:</b> Required if <i>Synchronization</i> and <i>Advanced Team and Role Mapping</i> are enabled.</p>
<b>Group Name Attribute</b>	Used for team mapping, Group Name Attribute is an attribute in LDAP defining a group's name.

Field	Description
	<b>NOTE:</b> Required if <i>Synchronization</i> and <i>Advanced Team and Role Mapping</i> are enabled.
<b>MEMBERSHIP SCHEMA SETTINGS</b>	Enables defining the attributes that associate the LDAP users with their assigned teams.
<b>Group Members Attribute (member)</b>	An LDAP member attribute which is multi-value, it contains a list of unique names for users in the team (user DN's), as well as group and contact objects that are members of the group.  It is used to determine the logged in user groups, in order to perform the right mapping to roles and teams.  <b>NOTE:</b> Required if <i>Synchronization</i> and <i>Advanced Team and Role Mapping</i> are enabled.
<b>User Membership Attribute (memberOf)</b>	An LDAP memberOf attribute which is multi-value, it contains all the groups that the current user is a member of (group DN's).  If designated, this attribute replaces the Group Members Attribute for determining the logged in user groups (taking the groups the user belongs to straight from the user entry, instead of searching inside every group).
<b>ADVANCED ROLE MAPPING</b>	Define what role(s) the users in specific LDAP group(s) will be assigned (mapped) to. Multiple roles can be assigned to the same LDAP Group DN.  1. Click <b>Edit Advanced Role Mapping</b> . 2. Click the arrow in the Cx Role field and then select a role from the options. 3. In the LDAP Group DN field, use a semicolon to separate multiple group entries. <b>Examples:</b> cn=dev;ou=grp;dc=my;dc=org;cn=qa;ou=grp;dc=my;dc=org 4. Repeat this procedure for each LDAP group—role mapping. 5. Click <b>Update</b> .

\* indicates required field

After you have finished configuring synchronization settings (or if you have disabled synchronization), click **Test User & Group Schema** to check the connection to the LDAP server, validate the user schema settings and attributes, and validate the group. A message informs of the test status.

Click **Save**.