Outpost24

Vulnerability Management made easy

Manage Users

Quick Start Guide

Version: 2.1
2019-07-04

Table of Contents

About This Document

This document is meant to provide users a comprehensive overview of the feature Manage Users for OUTSCAN and HIAB. This document has been elaborated under the assumption the reader has access to the OUTSCAN /HIAB Account and Graphical User Interface.

For support information, visit https://www.outpost24.com/support.

Copyright

Trademark

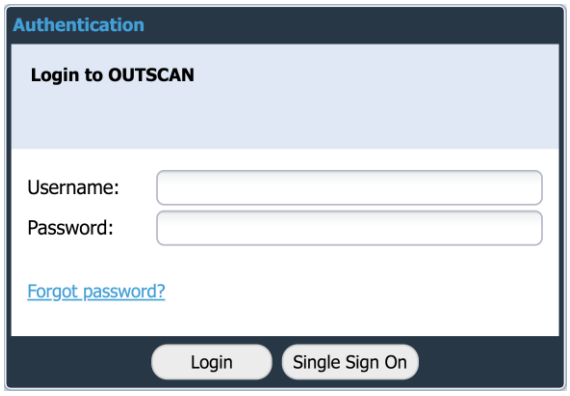
1 Getting Started

There are two ways of launching your applications.

- From OUTSCAN
- From a HIAB

1.1 OUTSCAN

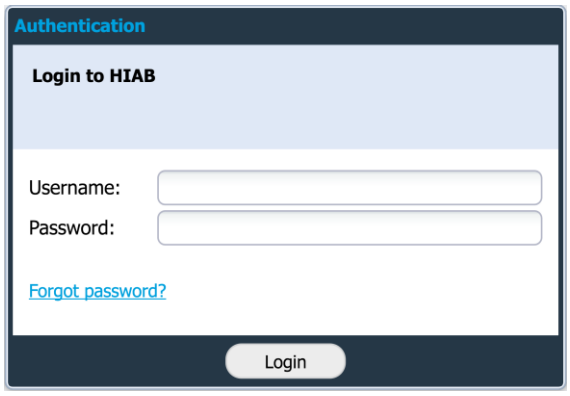
To launch the OUTSCAN application, navigate to https://outscan.outpost24.com.
***Note**: Use HTTPS protocol.*



Log in using your credentials.

1.2 HIAB

To connect to a HIAB, use the assigned network address.
***Note**: Use HTTPS protocol.*



Log in using your credentials.

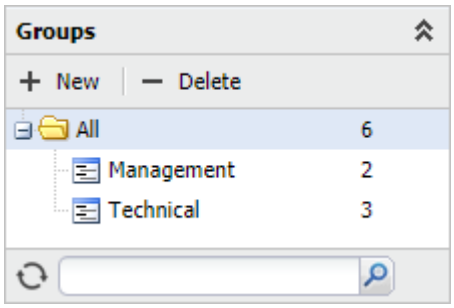
Go to **Main Menu → Settings → Manage Users** to access the *Manage Users* feature. This area allows for viewing and editing of all the users that you administer in the system.

2 Manage Users Accounts

The *Manage User Accounts* tab consists of the **Groups** tree and **Users** tree to the left, and a user grid to the right.

2.1 Groups

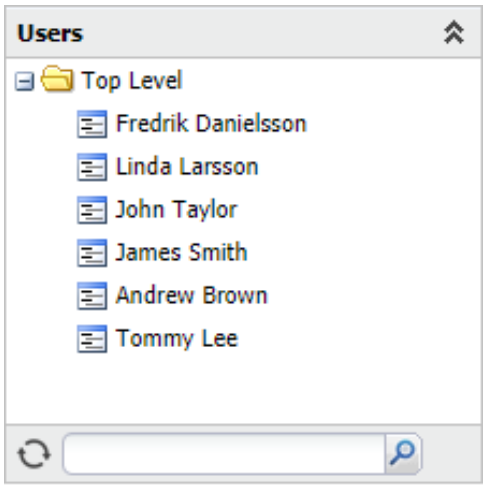
The *Groups* section shows a hierarchical structure of the defined user groups. The *Groups* section enable you to categorize users in different groups.
Clicking any group displays the users which are included in that specific group.



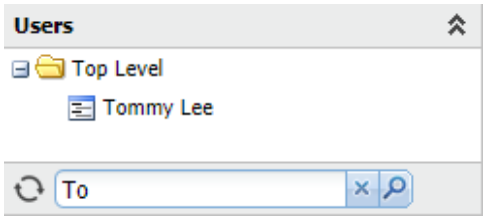
Filter: The Groups tree can be filtered by entering a partial or full name in the filter area at the bottom of the Groups tree section. This only show the groups that match the filtering string, and the parent accounts that are needed to show the hierarchy. Press the X-icon to clear the filter and show all groups again.

2.2 Users

In *Users* section, the *Top Level* represents your account and underneath a hierarchical structure of all the users that you can administrate is displayed. The usernames are shown in this tree. To select any user, click on the username. This changes the user account grid to show only that user. Re-click to deselect that user.



Filter: The **Users** tree can be filtered by entering a partial or full name in the search bar, located at the bottom of the *Users* section. This shows only the users that match the filtering string, and the parent accounts that are needed to show the hierarchy. Click on the **X** button, to clear the filter and show all users again.

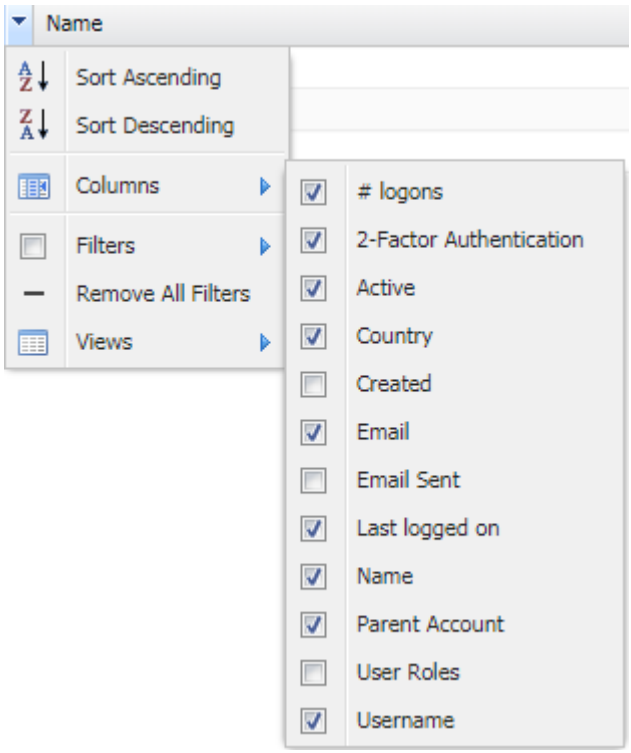


2.3 User Account Grid

The *User Accounts* grid shows detailed information about the users. It is possible to add or remove columns in this grid.

To add or remove columns:

1. Click on the arrow ▼ beside any column name to view the drop-down menu.
2. Choose **Columns** and select the columns that you wish to add.

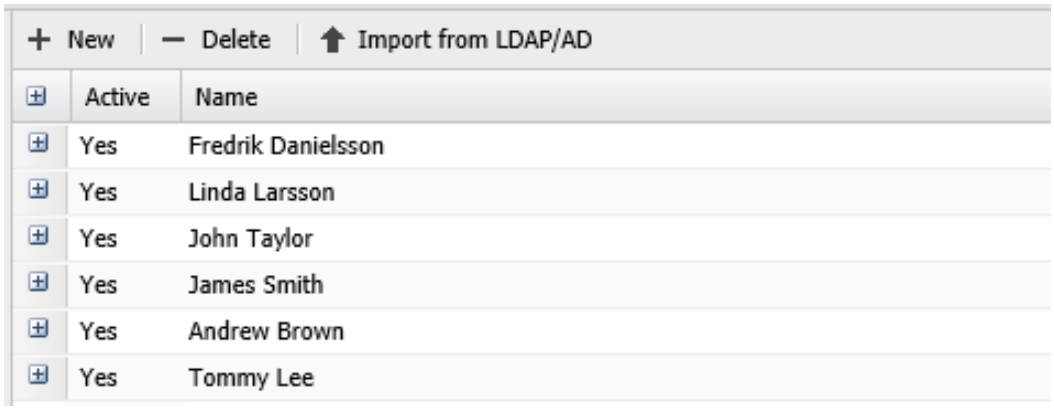


Below you find a list of the different columns available.

Option	Description
Logons	Displays how many times the user has logged into the system.
2-Factor Authentication	What sort of 2-factor authentication the user is using.
Active	If the account active or not.
Country	The users' country.
Created	The date and time when the account was created.
Email	The email address of the user.
Email Sent	The last time an information email or password recovery email was sent to the user.
Last logged on	When the user last logged into the system. If this entry is blank the user has still not logged into the system.
Name	The full name of the user.
Parent Account	The parent account of the user account. Top Level means that your account is the parent.
User roles	The type of user roles assigned to the user.
Username	The username that the user logs into the system with.

Right clicking on a user brings up a context menu where specific actions on that user or view can be performed.

Option	Description
New	Opens the *Create new user* window.
Delete	Deletes the selected user.
Edit	Change details on the selected user.
Copy	Copies the selected users' base settings, and open a new user where the general information needs to be filled in. (First name, Last name, Email, Mobile number, Country, Username and Password).
Export	Export all user accounts as a CSV or HTML file.



By clicking on the expand icon ⊞ or double click on a user displays additional information about the user account.

3 Manage Users

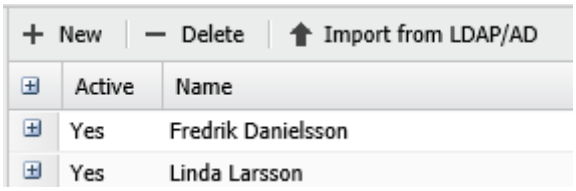
3.1 Prerequisites

User Roles need to be created before the user to be available for selection.
See *User Roles* for more information on how to create roles.

3.2 New User

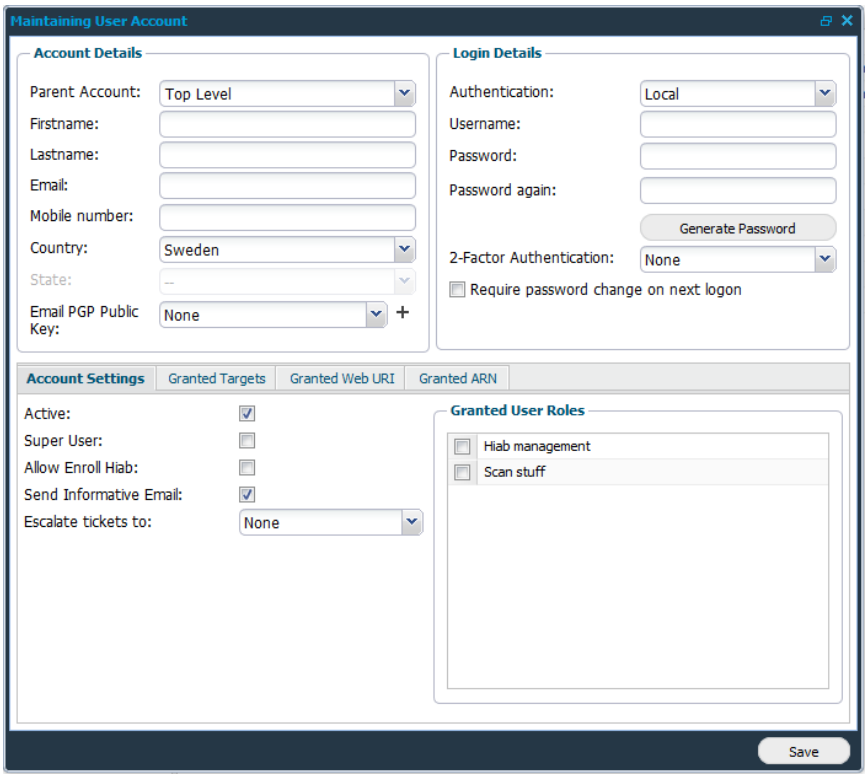
To create a user:

1. Click **Main Menu → Settings → Manage User**.
2. In the *Manage User Accounts* window select **User Accounts** tab. The buttons at the top center of the screen ids used to create, delete, or import users from LDAP/AD.



***Note**: The Import from LDAP/AD function is only available on HIAB. See LDAP/AD user guide for more information on setting up and mapping users in LDAP.*

3. Click **New** to create a new user.
4. In the *Maintaining User Account* window, fill in the *Account Details* and *Login Details*.



***Note**: In the grid on the lower half of Maintaining User Account window, the account access and rights can be further set up in the different tabs. Note that the tabs differ depending on your license*.

Account Details

Option	Description
Parent Account	Sets the parent account, could be used to create hierarchy structures.
First name	The first name of the user.
Last name	The last name of the user.
Email	The email address of the user.
Mobile number	The mobile number of the user.
Country	The country of the user.
State	The state of the user (Active if Country is United States).
Email PGP public key	Select PGP public key or click the **+** sign to upload a PGP key. ► None ► Unencrypted ► [uploaded keys]

Login Details

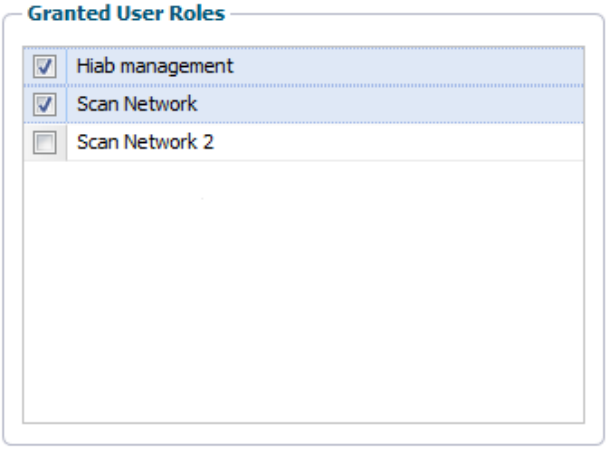
Option	Description
Authentication (HIAB Only)	Choose if the user credentials should be verified against the local database or the defined LDAP or Active Directory server.
Username	Enter a username.
Password	Enter a password, or generate a password using the password button. Passwords are generated according to the password policy located in the **Security Policy** tab under **Main Menu → Settings → Account**. See section *Password Policy* in *Account Settings* document for information on how to set password policies.
Password again	Confirm the password by re-typing in this field.
Require password change on next logon	If enabled, forces the user to change his/her password the next time they log in to the system.

Option	Description
2-Factor Authentication	If enabled, you may set up the mode of authentication from here. **Mobile Security Code** or **Google Authenticator** can be used for authentication. The method used for authentication can be limited, depending on the options configured for two factor authentications in the security policy. When Google authentication is selected, you will be asked to enter the credential ID which is used to set up the account.

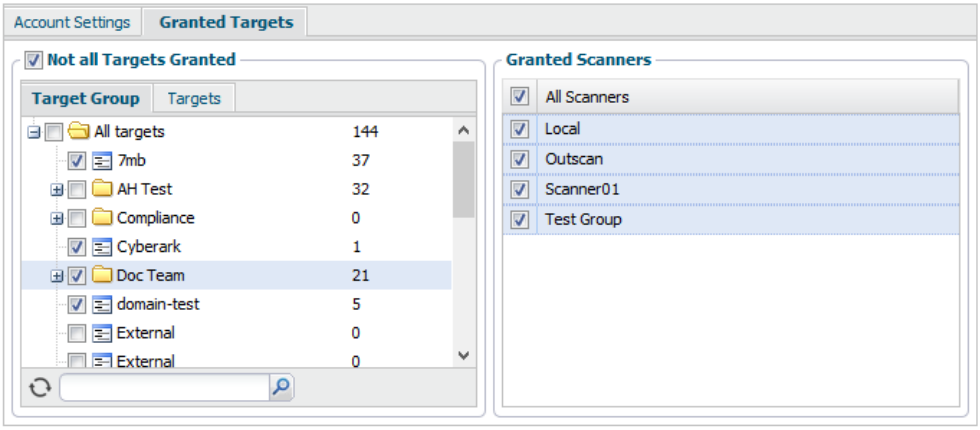
5. In **Account Settings** tab you can deactivate an account and set the users notification.

Option	Description
Active	Activate or deactivate account.
Super User	A user with **Super User** enabled will have the same rights as the main account (which is unrestricted).
Receive System Notifications	When **Super User** is active, the user can receive system notifications, or have it deactivated.
Allow Enroll Hiab	Allow the user to enroll HIABs.
Send Informative Email	If **Send Informative Email** is activated, then the system will send an email to the sub user when their account has been changed.
Escalate tickets to	The **Escalate tickets to** drop down menu allow you to define who should receive any tickets which has not been resolved prior to its due date (which were assigned to this specific user).

6. Assign the user with one or more **Granted User Roles** otherwise the user will not be allowed to perform any actions in the system.
   For more information on how to create user roles, see *User Roles.*



7. In the **Granted Targets** tab, you can define which targets and scanners (if enabled) the user should have access to.



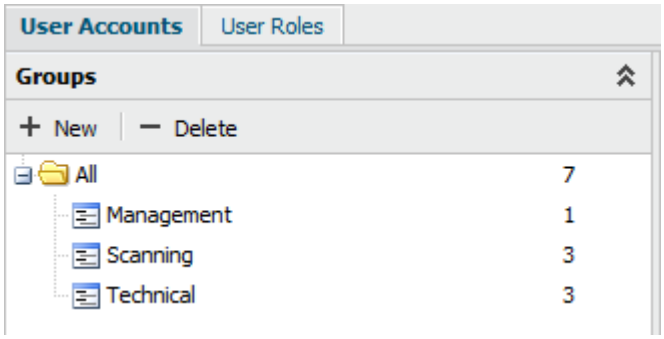
Not all Targets Granted limits the target groups and targets a user can see and administrate. The target list feature should be used sparsely since it creates an overhead when it comes to administrative task in the long run. The only time you should use this feature is when you would like to grant access to a whole IP range without having to define all targets within the system.

Granted Scanners limits which scanners the user has access to within the system. If **All Scanners** is selected, then the user will also automatically have access to scanners which are added afterwards.

8. Once the user has been set up, click **Save**.

4 Groups

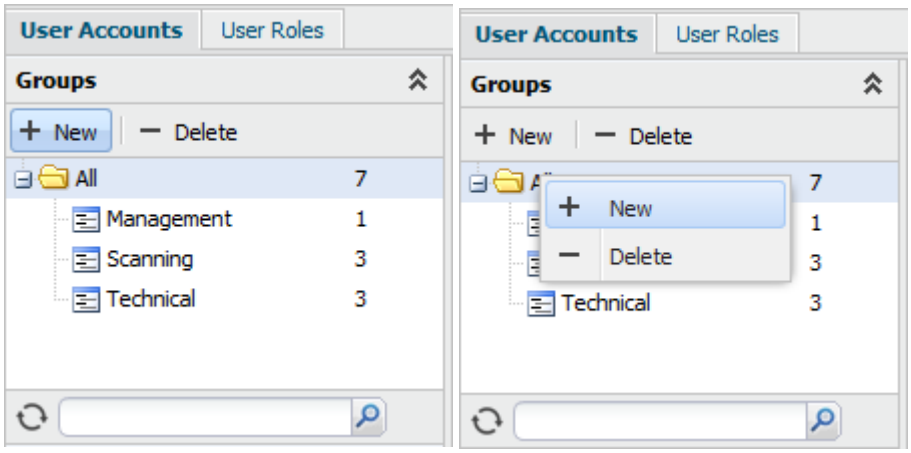
The Groups function enable you to bundle users together into simple groups to be presented in the group grid.



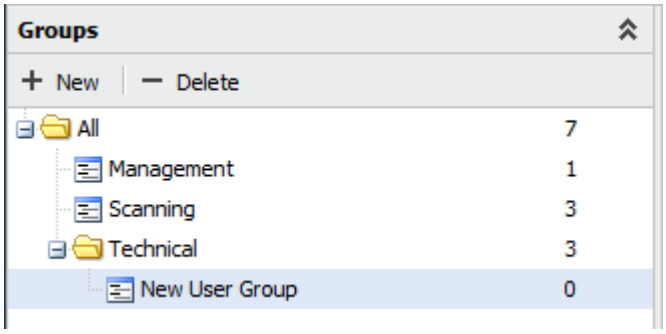
***Note**: Roles cannot be applied to groups, roles can only be applied on a user level.*

4.1 Create Groups

To create a new group, click the **+ New** option, or right click and **All** folder in the *Groups* tree and choose **New**.



To create a new subgroup, select a main group and click the **+ New** option, or right click the group name and select **New** in the menu.



4.2 Populate Groups

Once a group is created, it can be populated with users.
To populate a group:

1. Select the users by pressing **Ctrl + Left click** on each user in the *User Account* grid and drag them to the designated group.

***Note**: A user can only be part of one group.*

4.3 Moving Users Between Groups

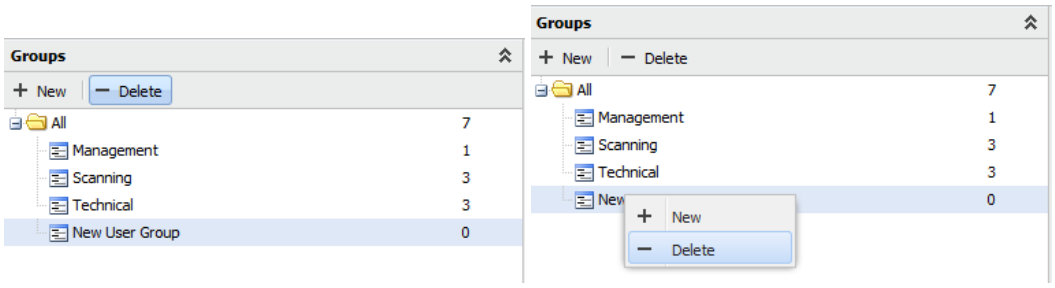
Users can be moved freely between groups.
To move users to another group:

1. Click the group where the user resides in to list the group content in the User Account grid.
2. Select the users by pressing **Ctrl + Left click** on each user you want to move. Then drag the user/users into the new group.

***Note**: Users connect to a top-level user will not be moved together with the top-level user. Each user needs to be moved individually or as a selected group.*

4.4 Delete Groups

To delete a group, select the group in the Groups section, and click **– Delete** option, or right click the group and select **Delete** in the menu.



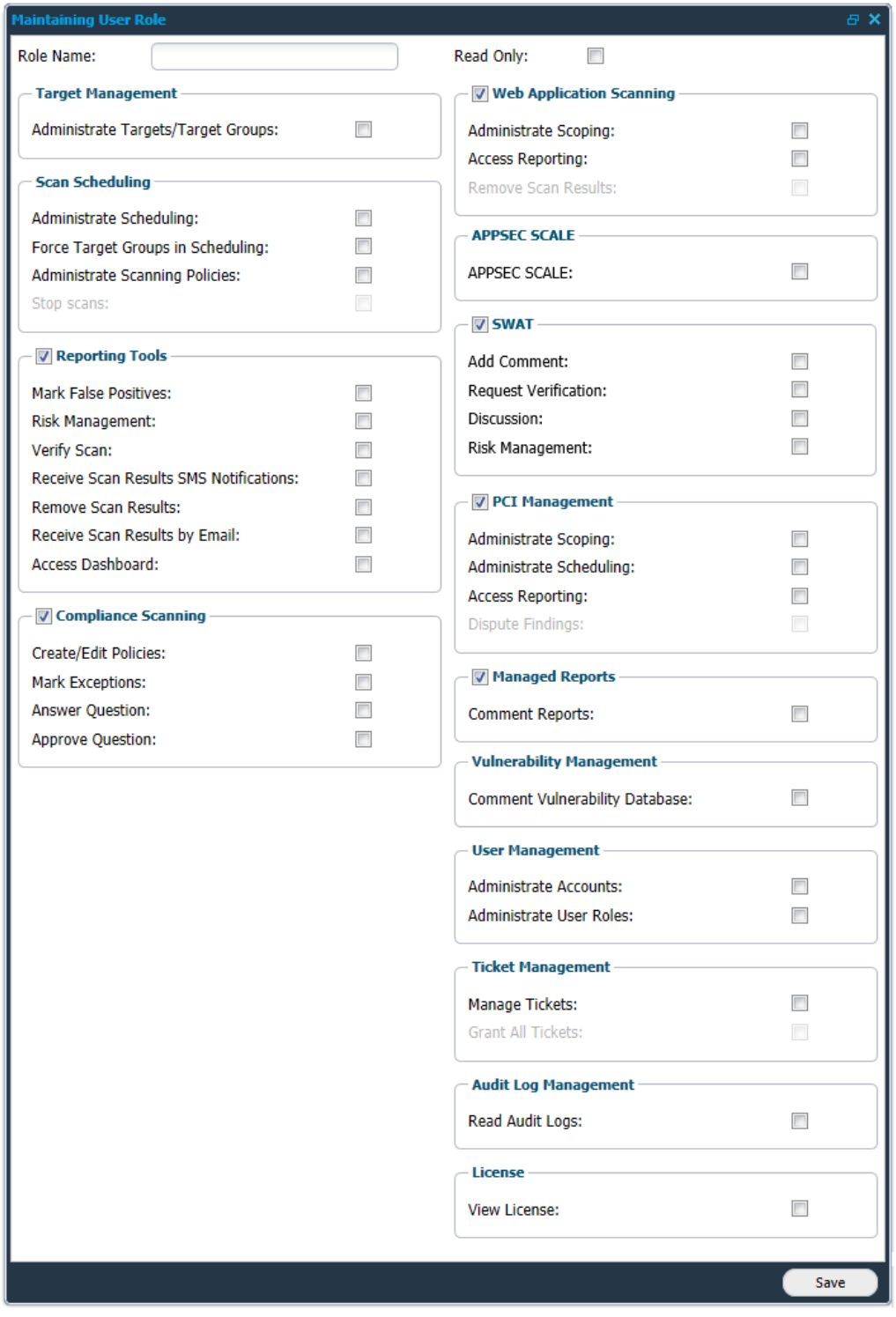
***Note**: Deleting a group do not delete the users within the group. They go back to **All** folder*.

5 User Roles

5.1 Create Roles

To create a user role:

1. Click **Main Menu → Settings → Manage User**.
2. In the *Manage User Accounts* window select **User Roles** tab and click **+ New**.
3. In the *Maintaining User Role* window, enter a *Role Name*.

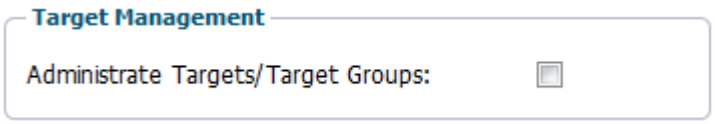


4. Select the various boxes to match the role being created.
5. Click **Save**.

Maintaining User Role

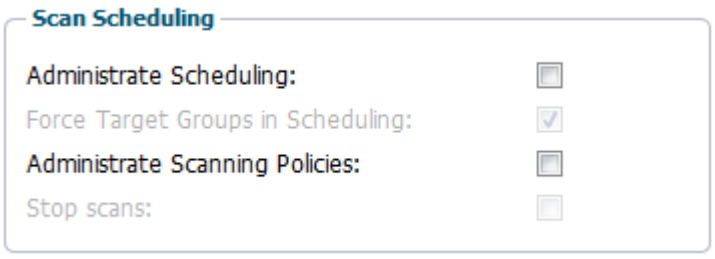
Option	Description
Role name	Every user role needs to have a given name to identify the role.
Read Only	User will not be permitted to do any changes or new creations when this option is enabled.
LDAP/AD Group (HIAB Only)	The LDAP/AD Group field is available if LDAP/AD is enabled on the HIAB. This user role is mapped to the defined role in LDAP/AD when the user login.

Target Management



Option	Description
Administrate Targets/Target Groups	This will allow the user to administrate targets and groups in the *Manage Targets* view.

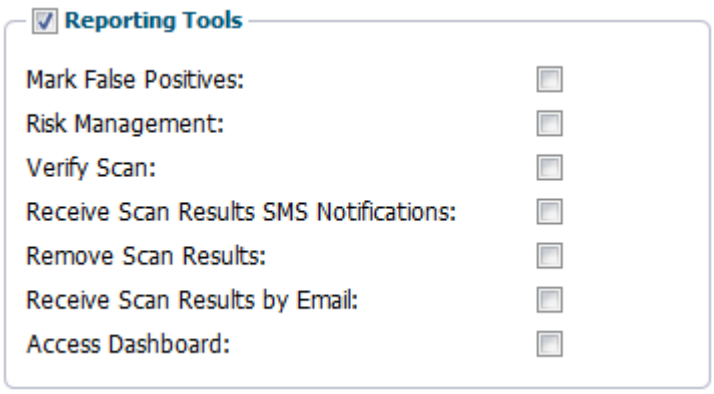
Scan Scheduling



Option	Description
Administrate Scheduling	Determines if the user can define and set up new scan schedules.
Force Target Group in Scheduling	Will enforce the user only to use the already defined groups in the scheduling section. No manual targets can be entered in the targets tab. This option will be checked and disabled if you have already set it in Scan Scheduling settings.
Administrate Scanning Policies	Determines if the user can create, modify and remove scanning policies within the system.

Option	Description
Stop scans	If the user can administrate scan scheduling, he/she will also be allowed to stop scans if this setting is enabled.

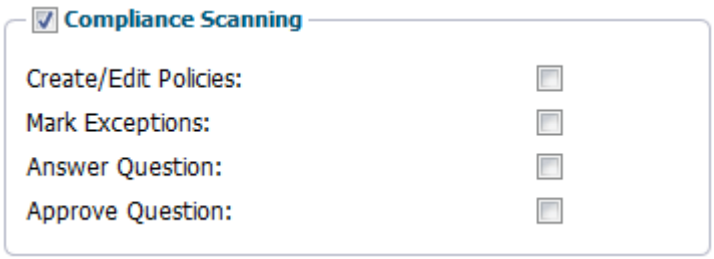
Reporting Tools



Reporting Tools field gives a user, permission to view the reporting tools. If not enabled, reporting tools is not shown to the user.

Option	Description
Mark False Positives	Allows a user to mark a finding as a false positive.
Risk Management	The user will be allowed to mark vulnerabilities as accepted risks and/or change the risk level for a finding.
Verify scan	The user will be allowed to perform verification scans. No scans will be deducted from the license when using this feature.
Remove Scan Result	The user will be allowed to remove reports.
Receive Scan Results by Email	The user will be able to receive reports by email.
Access Dashboard	The user will be able to see the Dashboard.

Compliance Scanning

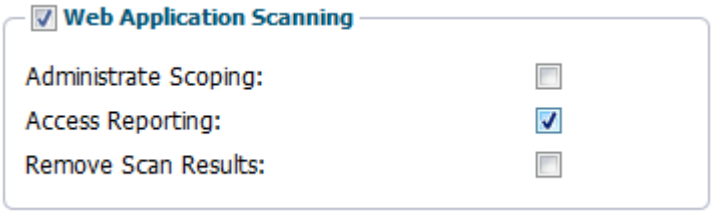


Note: *Compliance Scanning is only visible if it is included in your license.*

Compliance Scan field gives a user, permission to view the Compliance scanning module. If not enabled, it will not be shown to the user.

Option	Description
Create/Edit Policies	Allow the user to Create/Edit policies.
Mark Exceptions	Allow the user to mark exceptions.
Answer Question	Allow the user to answer questions.
Approve Question	Allow the user to approve questions.

Web Application Scanning (WAS)



Note*: Web Application Scanning is only visible if it is included in your license.*

Option	Description
Administrate Scoping	Allows the user to create, modify or remove any scopes.
Access Reporting	Allows the user to view WAS reports.
Remove Scan Results	Allows the user to delete WAS reports.

Appsec Scale

***Note**: This section is only visible if you have an Appsec license.*

Option	Description
Appsec Scale	Grants access to the APPSEC SCALE module for the sub user.

SWAT

***Note**: This section is only visible if you have a SWAT license.*

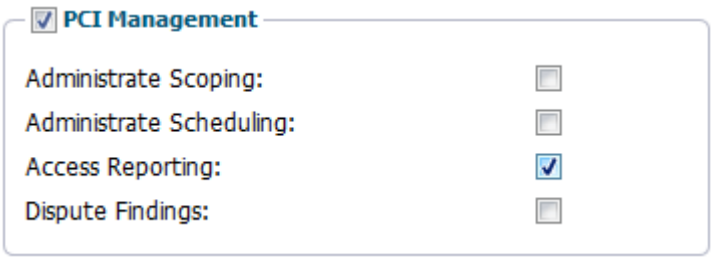
Option	Description
Add Comment	Allows the user to add comments to vulnerabilities in this module.
Request Verification	Allows the user to request more information regarding the existence of vulnerability in this module.
Discussion	Allows the user to start a discussion with Outpost24 support.
Risk Management	Allows the user to accept risks in the report.

Scoping

***Note**: OUTSCAN only*

Option	Description
Submit scoping request	Allows the user role to submit Appsec scoping requests.

PCI Management



***Note**: PCI Management is only visible if PCI Compliance scan is included in your license.*

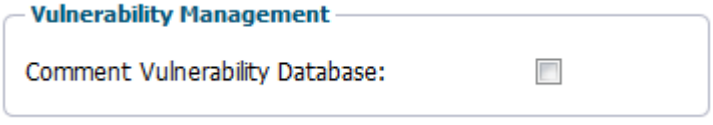
Option	Description
Administrate Scoping	Allows the user to create, modify, or remove any scopes in this module.
Administrate Scheduling	Allows the user to start and stop PCI scans.
Access Reporting	Allows the user to view PCI reports.
Dispute Findings	If the user has *Access Reporting* this option will allow the user to dispute findings from the report.

Managed Reports

***Note**: This section is only visible if you have a Managed Reports license.*

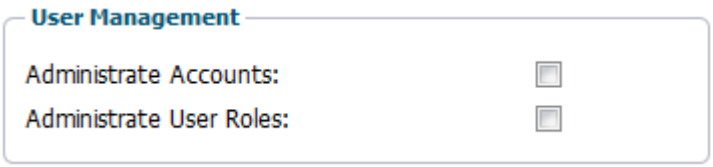
Option	Description
Comment Reports	Allows users to add comments to reports.

Vulnerability Management



Option	Description
Comment Vulnerability Database	Allows the user to create and edit comments in the vulnerability database.

User Management



Option	Description
Administrate Accounts	Allows the user to administrate accounts.
Administrate User Roles	Allows the user to administrate user roles.

Ticket Management

Option	Description
Manage Tickets	Allows the user to administrate tickets.
Grant All Tickets	Gives access to all internal tickets. (If **Manage Tickets** is selected).

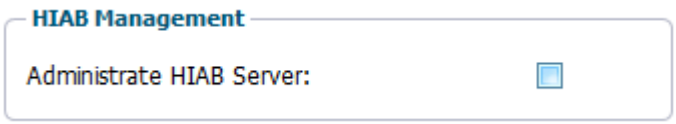
Audit Log Management

Option	Description
Read Audit Logs	The user can read the auditing log.

License

Option	Description
View License	Allows the user to view the **License** tab in **Main Menu → Settings → Account**.

HIAB Management (HIAB only)



***Note**: HIAB Management only visible if it is included in your license.*

Option	Description
Administrate HIAB Server	Allows the user to restart the HIAB and setup HIAB settings like backup and networking.

6 Attributes

The Attributes tab is available only if they are set to active. See Attributes section in Account Settings document for information on how to set attributes.

***Note**: The tabs in the lower half of the window varies depending on your license.*