Outpost24

Vulnerability Management made easy

Manage Users

Quick Start Guide

Last update:
9 February 2017

Outpost24

Table of Contents

About This Guide

1. Executive Summary

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.

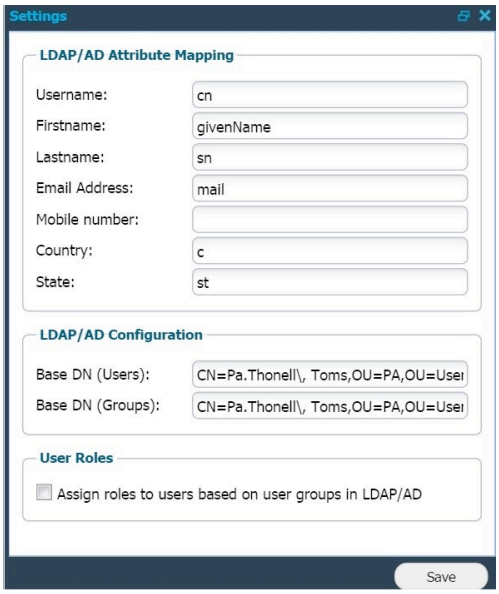
2. Manage Users Section

Navigate to "Main Menu -> Settings -> Manage Users" to access the feature. This area allows for viewing and editing of all the users that you are allowed to administrate in the system.

2.1. Settings

The settings option can be found in the top right corner: the button with the symbol of a small cogwheel. The settings option is only available if you've already setup LDAP/AD in "Main Menu -> Settings -> Server -> LDAP/AD (tab)".

In the LDAP/AD Attribute Mapping you may define the mapping between the HIAB and the LDAP/AD fields.

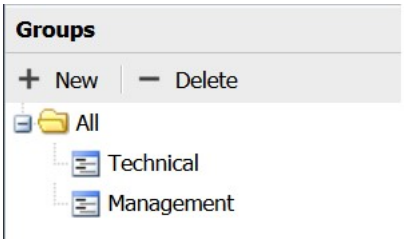


Enter the field that maps to the following fields:

- **Username** - The user name of the user to import
- **First name** - The first name of the user to import
- **Last name** - The last name of the user to import
- **Email Address** - The email address of the user to import
- **Mobile number** - The mobile number of the user to import
- **Country** - The country of the user to import.
- **State** - The state of the user to import

Base DN - use this specific Domain Name instead of the one defined for the server (Base DN override). If the box "Assign roles to users based on groups in LDAP/AD" within the User Roles section is checked, you will be allowed to define a static group reference on your already defined user roles. These are called "LDAP/AD Group" (under "Maintain User Role"), within the User Roles Tab. If a user belongs to any of these groups, then they will automatically be assigned that role.

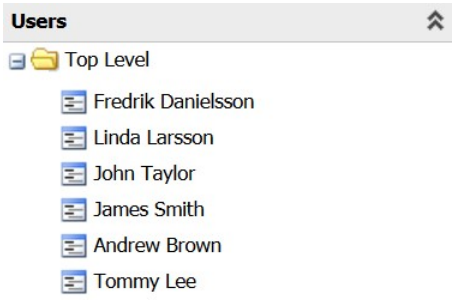
2.2. Manage Groups Tree



Shows a hierarchical structure of your defined User groups. The groups' names are shown in the tree. Clicking any group will display the users which are included in that specific group. To create a new group,

either use the "New" option, or right click and group and choose "New". This will create a new sub group for that group.

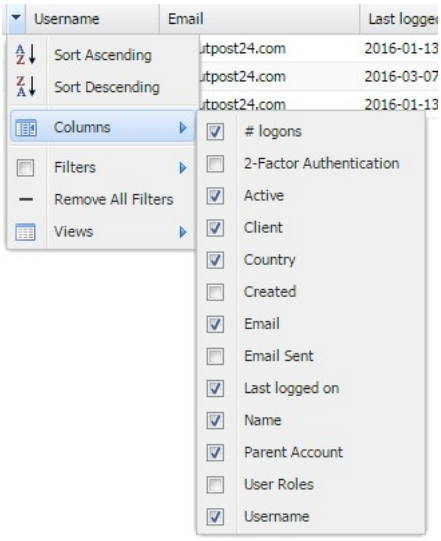
2.3. Manage Users Tree



The Top Level represents your account and underneath this you will be able to see a hierarchical structure of all the users that you can administrate. The user's names are shown in this tree. You may select any user by clicking on it. This will change the user account grid to only show that user. You deselect the user by clicking on it once more.

Filter: You may filter the user tree by entering a partial or full name in the filter area. This will only show the users that match the filtering string, and possibly some parent accounts that are needed to show the hierarchy. Press the clear icon to clear the filter and show all users again. The filter can be found at the bottom of the manage users tree section.

2.4. User Account Grid



The user account grid shows more detailed information about the users. It is possible to add or remove columns in this grid to better suit your needs. To add or remove columns; click the down pointing arrow that will appear when you hover your mouse pointer over the column. Choose 'columns', and check the checkboxes for the columns that you wish to add. Below you will find a list of the different columns available.

- **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 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 will bring up a context menu where you can perform specific actions on that user or on the view.

- **New** - Will open the "Create new user" window
- **Delete** - Will delete the selected user
- **Edit** - Will allow you to perform changes on the selected user
- **Copy** - Will copy 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** - Will export the all user accounts as a CSV or HTML file

By clicking on the plus icon or double click on a user you will display additional information about the user account

2.5. Creating and Maintaining Users

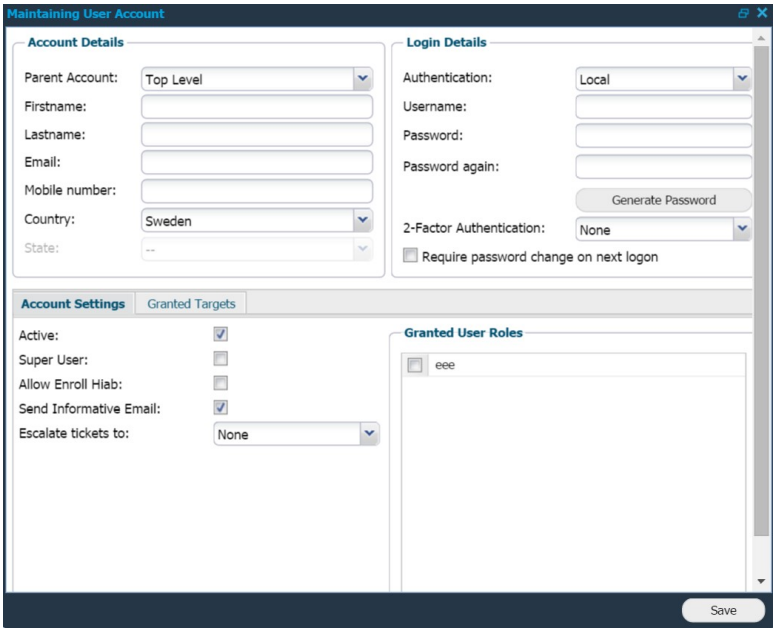
The buttons at the top center of the screen allows you to:

New: Will allow you to create a new user

Delete: Will allow you to remove an existing user

Import from LDAP/AD: Will allow you to import users from your server if you have configured the server settings mentioned under chapter 3.1 Settings.

When creating a new user you will be prompted with the window shown below. Populate all the following fields with the credentials and information of the person for whom you are creating an account for.



- **First name, Last name, Email, Mobile number, country, username** and **password** for the user
- **Parent Account -** Sets the parent account, could be used to create hierarchy structures
- **Authentication** - Will allow you to define if the user credentials should be verified against the local database or the defined LDAP or Active Directory server
- **Require password change on next logon** - Will force the user to change his/her password the next time they log in to the system
- **Two factor authentication** – If enabled, you may set up the mode of authentication from here. Mobile Security Code and Google Authenticator can be used for authentication. The method used for authentication can be limited, depending on the options configured for two factor authentication 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

2.5.1. Account Settings

- **Active** – Determine if a user account should be active or not
- **Super User** - Define if the user should have the same privileges as the main account (which is unrestricted)
- **Allow Enroll Hiab** - Defines if the user should be able to enroll additional HIABs. This may be useful if a distributed environment is used
- **Send Informative Email** – If activated, the user will receive an email notification with the credentials details defined for the account.
- **Escalate tickets to** – Prompts you with a drop down menu that allows you to define who is to receive any ticket that hasn't been resolved prior to its due date (only tickets that were assigned to this specific user)

Unless the user is a Super User, you must assign the user with one or more Granted User Roles, otherwise the user will not be allowed to perform any actions in the system.

2.5.2. Granted Targets

Under the Granted targets tab you will be able to define which targets and scanners (if enabled) the user will have access to.

- **Not all Targets Granted** - Limit the target groups and targets a user is allowed to see and administrate. This option has two tabs:
    - **Target Group -** Will show a small tree of which target groups the HIAB already has defined. Check the checkbox for the group the user should be able to administrate
    - **Targets** - Should be used sparsely since it will create 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** - Limit which scanners the user has access to within the system. If the All Scanners box is checked then the user will also automatically have access to all scanners that are added in the future

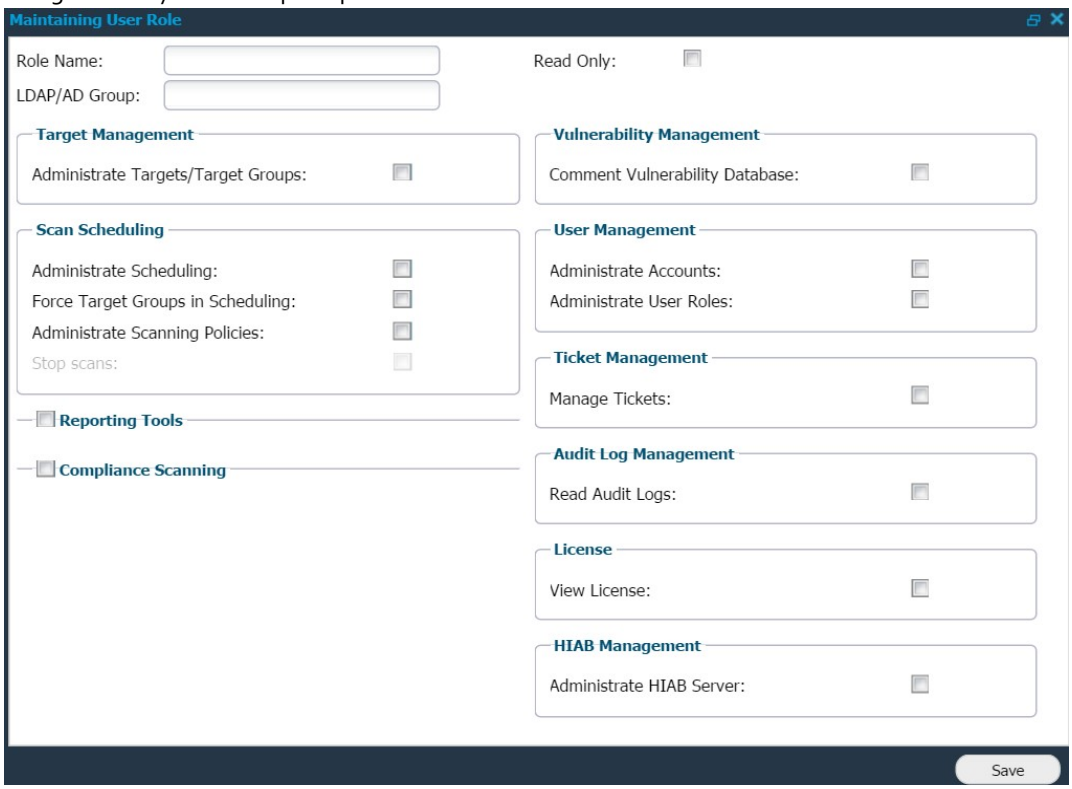
2.6. User Roles Tab

This area is used to administrate the user roles. Every user can be given one or several user roles which will determine what actions the user is allowed to perform. You are also able to assign multiple user roles to one user, which will give you the ability to customize the user permissions even further.

New - Creates a new user role

Delete - Removes a selected user role

When clicking on *New* you will be prompted with a new window as seen below.



The different options will be explained on the next page. If enabled, some checkboxes will reveal more options within the specific section.

Maintaining User Role

- **Role name** - Every user role needs to have a given name in order to identify the role
- **LDAP/AD Group** - If a LDAP/AD user have this attribute, then this user role will be assigned to that user after log in
- **Read Only** - User will not be permitted to do any changes or new creations when this option is enabled

Target management

- **Administrate Targets/Target Groups** - This will allow the user to administrate targets and groups in the 'Manage Targets' view

Scan Scheduling

Administrate Scheduling - Determines if the user is allowed to define and set up new scans

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

- **Administrate Scanning Policies** - Determines if the user is allowed to create, modify and remove scanning policies within the system
- **Stop scans** - If the user is allowed to administrate scan scheduling he/she will also be allowed to stop scans if this setting is enabled

Reporting Tools

- **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

- **Mark Exceptions** – This will allow the user to mark exceptions in the compliance module

Web Application Scanning

- **Administrate Scoping** - Allows the user to create, modify or remove any scopes in this module
- **Access Reporting** - Allows the user to view reports in this module
- **Remove Scan Results** - Allows the user to delete reports

PCI Management

This section is only visible if PCI is included in your Outscan License.

- **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

- **Comment Repots** – Outscan only. Allows users to add comments to reports

Vulnerability Management

- **Comment Vulnerability Database** – Allows the user to create and edit comments in the vulnerability database

User Management

- **Administrate Accounts** - Allows the user to administrate accounts
- **Administrate User Roles** - Allows the user to administrate user roles

Ticket Management

- **Manage Tickets** – Allows the user to administrate tickets

Audit Log Management

- **Read Audit Logs** – The user will be able to read the auditing log

License

- **View License** - Allows the user to view the license tab

HIAB Management

- **Administrate HIAB Server** - Allows the user to restart the HIAB and setup HIAB settings like backup and networking
- **Administrate Network Monitors** - Allows the user to administrate the Monitor Targets

3. Technical Support

Contact our 24/7 support team by email or telephone:

Email support@outpost24.com

Tel (from the UK): +44 20 7193 8410

Tel (from the US): +1 (800) 69 13 150

Tel (from Spain): +34 91 188 08 15

Tel (from Mexico): +52 55 8421 4503

Tel (from Hong Kong): +852 8175 8310

Tel (from Malaysia): +603 2035 5931

Tel (from Singapore): +65 3151 8310

Tel (from Thailand): +662 642 7258

Tel (all other countries): +46 455 612 310