Outpost24

Vulnerability Management made easy

Account Settings

User Guide

Version: 1.4

2019-02-14

Table of Contents

About This Guide

This document provides users with a comprehensive overview of the account settings for OUTSCAN and HIAB. This document has been elaborated under the assumption the reader has access to the OUTSCAN/HIAB Account and Portal Interface.

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

Copyright

Trademark

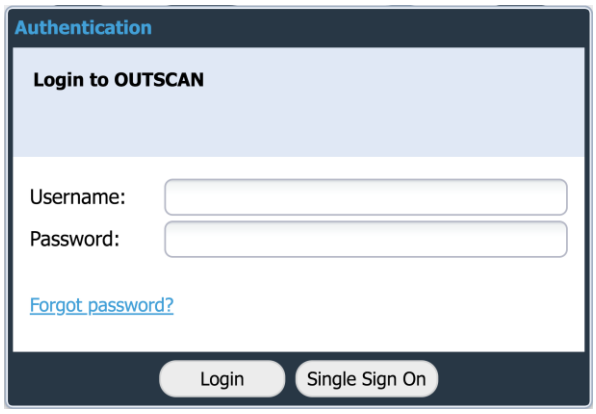
1 Getting Started

There are two ways of launching your applications.

- From OUTSCAN
- From a HIAB

1.1 OUTSCAN

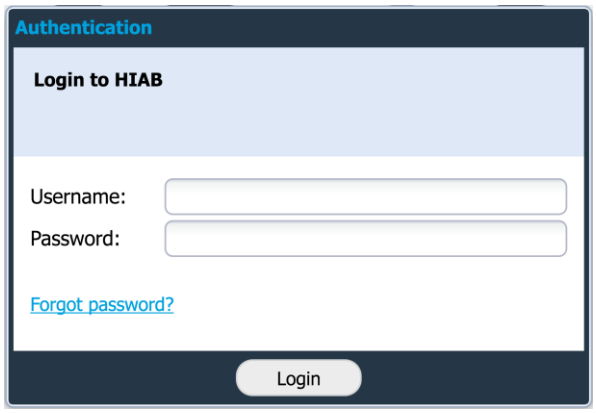
To launch the OUTSCAN application, navigate to https://outscan.outpost24.com.
***Note**: Use HTTPS protocol.*



Log in using your credentials.

1.2 HIAB

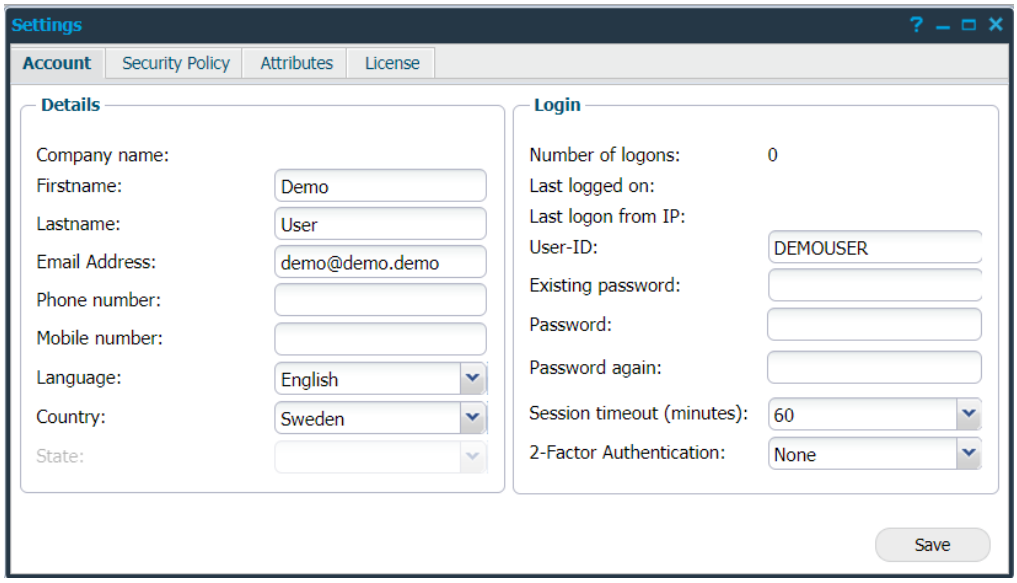
To connect to a HIAB, use the assigned network address.
***Note**: Use HTTPS protocol.*



Log in using your credentials.
To access the Account Settings module, go to **Main Menu > Settings > Account**.

2 Account

In the **Account** tab the account *Details* and *Login* for a user can be edited.



2.1 Details

The **Details** area contains your personal information such as name, email address, phone number, language and location information.

Option	Description
Company name	Displays your company name.
First name	Provide your first name.
Last name	Provide your last name.
Email address	The Email address that you wish to bind to your account. This email address will receive notifications, recovered passwords, and update notes.
Phone number	Provide the phone number you wish to bind to your account.
Mobile number	Provide the mobile number you wish to bind to your account.
Language	The language that you would like the user interface to use.
Country	Your country location.
State	Select your state if applicable.
Email PGP Public Key	The email can be encrypted with a PGP public key.

Option	Description
	Default options: None, Unencrypted To add a public key file: 1. Click on + sign located beside the field. 2. This opens a new window (Maintaining Files) where files can be added or deleted. 3. Click Save followed by Close after uploading the file. 4. Select a public key file from the drop-down menu with which to encrypt the email.

2.2 Login

The **Login** area contains account statistics, including the number of times that the account has logged in. It also allows you to change the password, and the User-ID, which is used to log in to the service.

The main user can also set the **Session timeout** interval. If the timeout is specified, a session will timeout if the user is inactive for the specified number of minutes. This include the main user.

Two-factor authentication can be enabled, and the mode of authentication is selected from here. Either **Mobile Security Code** or **Google Authenticator** can be used for authentication. The means used for authentication can be limited, depending on the options configured for two factor authentications under **Security Policy** tab.

When Google Authentication is selected, you are asked to enter the credential ID which is used to set up the account.

Option	Description
Number of logons	Displays the total number of logons.
Last logged on	Displays the date of your last logon.
Last logon from IP	Displays the IP of your last logon.
USER-ID	Displays your user ID.
Existing Password	If you wish to reset your password, you must provide the current password for the account in this field.
Password	The password that you wish to use for this account.
Password Again	Type the password that you wish to use once again.
Session Timeout (minutes)	For how long the system is allowed to be idle before your session times out and you are logged out.
2-Factor-Authentication	Choose between the following in the dropdown menu: ► **None**: No authentication other than specifying USER-ID and Password is needed. ► Mobile **Security Code**: Upon login a six-digit security code will be sent to a specified mobile number of your choice, which can be used for additional authentication when logging in. ***Note**: Some network providers do not process incoming text messages where the sender information is set, this is a known issue with some larger providers in Turkey and Malaysia but may occur in other countries as well.*

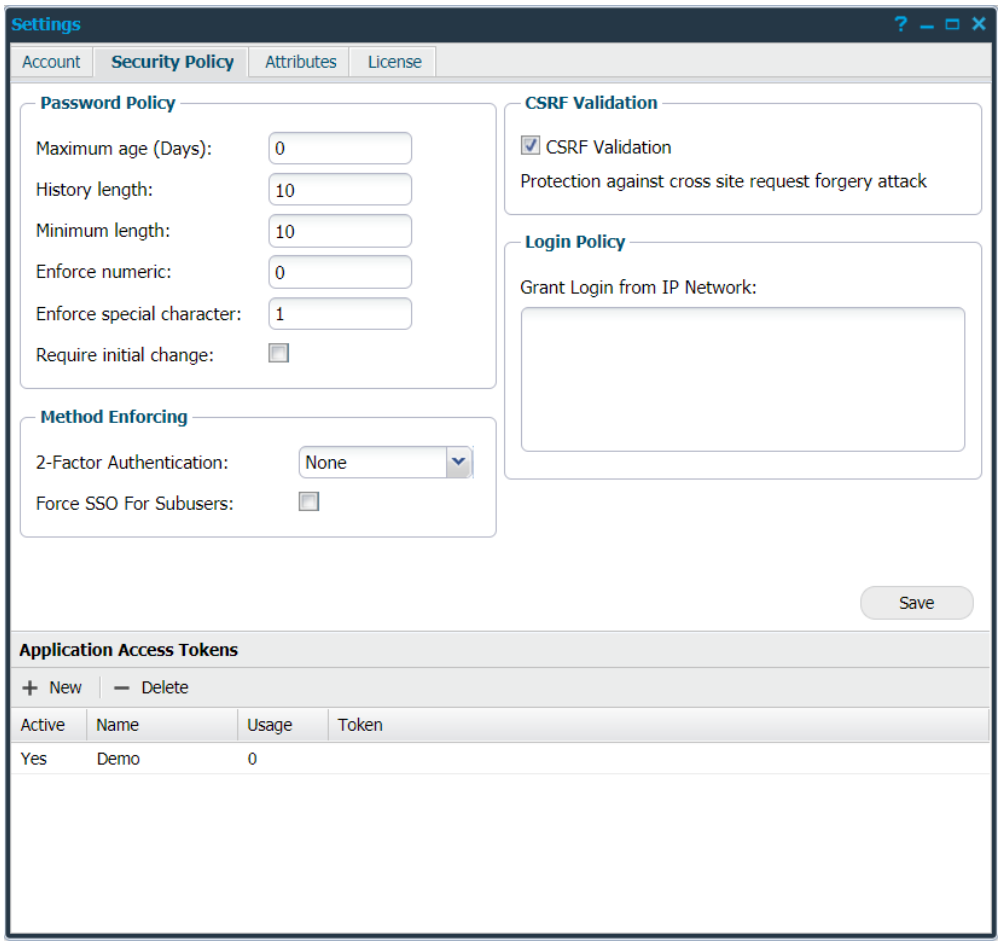
Option	Description
	In those cases, the best option is to use the Google Authenticator. *The feature is provided as an enhancement option.* ► **Google Authenticator**: A mobile application that produces a random six-digit number which can be used for additional authentication when logging in.

3 Security Policy

In the **Security Policy** tab several security policies can be edited such as:

- Password Policy
- Method Enforcing
- CSRF Validation
- Login Policy

Application Access Tokens can also be managed.



3.1 Password Policy

The **Password Policy** area is used to setup a policy regarding password complexity. Following fields are available to use to increase or decrease password security:

Option	Description
Maximum Age	Used to set for how long a set password is valid before it expires and the user has to set a new password.
History Length	Determines how many entries the system will save to confirm that the entered password has not been used before.
Minimum Length	Set the minimum length of the password.
Enforce Numeric	Determines the number of digits that the password must contain.
Enforce Special Character	Determines the number of special characters a password must contain. The special characters are `~!@#$%^&*()-_=+[{]}\\|;:'\",<.>/?.
Require initial change	Force the newly created user to change the password upon the first login to the system.

When changing the password policy, the existing passwords that do not match the new policy will not be subject to change, the only change that affects all existing passwords is the **Maximum Age**.

The new setting of the **Maximum Age** will therefore be applied even for existing passwords.

3.2 Method Enforcing

The **Method Enforcing** area determines the type of method used for authentication.

Option	Description
2-Factor Authentication	The available options are: ► **None**: *Two-factor authentication* is not enforced; however, each user can still use a two-factor authentication on his/her account. ► **Any**: This option enforces users to choose between the two authentication methods mentioned above. ► **Mobile Security Code**: When this option is selected, a *Mobile Security* code is enforced as default on all users. ► **Google Authenticator**: When this option is selected, *Google Authenticator* is enforced as default on all users.
Force SSO For Subusers	Force the subuser to use *Single Sign On*. *Default Value:* Enable

3.3 CSRF Validation

If enabled your account will have protection against cross site request forgery attacks. The reason for why this can be disabled is due to older integrations which do not have support for protection against cross site request forgery attacks.

***Note**: Do not disable this if not necessary.*

Option	Description
CSRF Validation	Protects against *Cross Site Request Forgery* attacks. Only disable for older integrations which do not have support for protection against cross site request forgery attacks. Default Value: Enable

3.4 Login Policy

The **Login Policy** area is used to grant login access from a specific network range. Here you can define multiple network ranges from which the users will be allowed to log in. If a user supplies the correct credentials but isn't located within the granted range, their access will be denied.

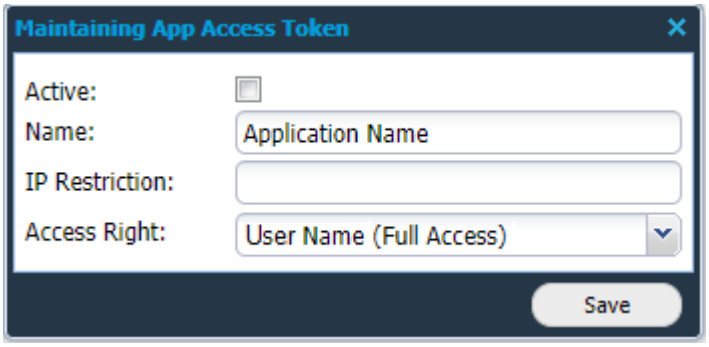
Option	Description
Grant Login from IP network	Multiple entries separated by a new line can be entered in the following formats: ▶ CIDR notation ▶ Network range ▶ Single IP numbers.

3.5 Application Access Tokens

The **Application Access Tokens** are keys that are generated and can be used instead of username/password. The key can be copied and sent into the request as the parameter `APPTOKEN` using the API.

The **Application Access Tokens** area lists the applications using access tokens.

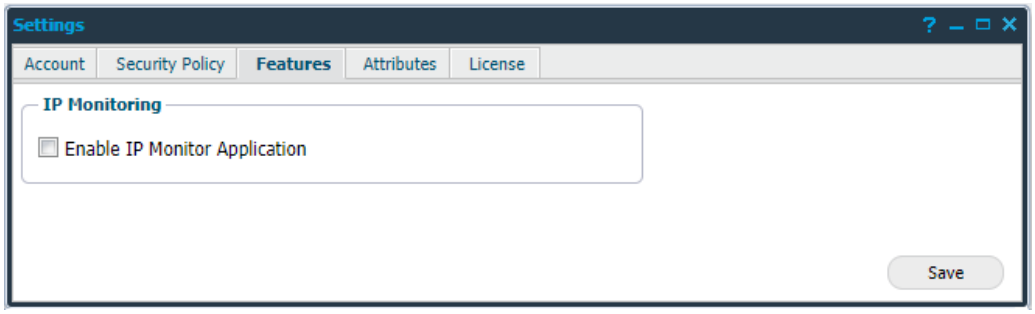
Clicking on the **+ New** button will display the **Maintaining App Access Token** window



Option	Description
Active	Checking this box will mark the token active.
Name	Indicates the name of the Application.
IP Restriction	Restricting the IP address used by the application.
Access Right	Indicates the type of access right.

4 Features (HIAB only)

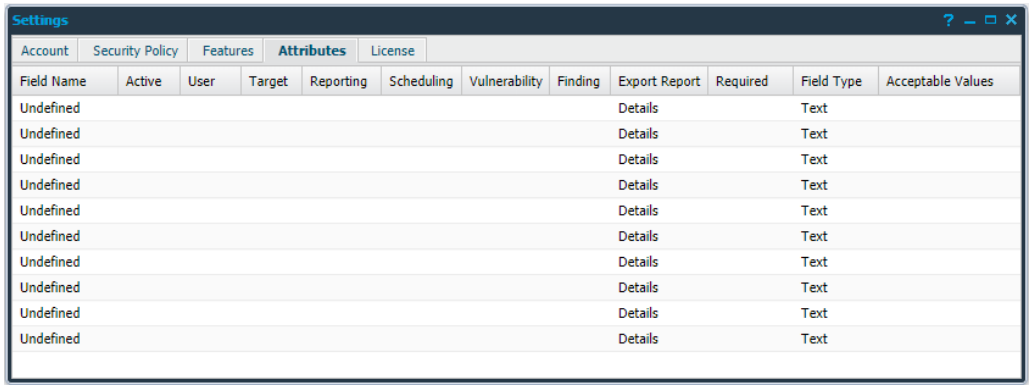
When the **Enable IP Monitor Application** is selected, an application is available in the menu which can be used to determine if a target goes online or offline.



Option	Description
Enable IP Monitor Application	Check this box if you want to enable *IP Monitor Application*. Default value: Disabled

5 Attributes

In the Attributes tab, you can define up to ten custom attributes which can be used throughout the system. They can also be configured to only allow predefined values.



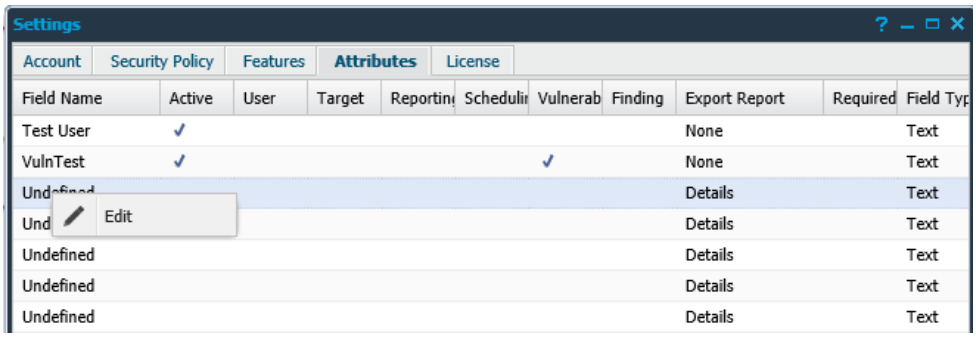
These attributes become available in the following sections depending on their configuration:

- Users
- Target
- Reports
- Scheduling
- Discovery

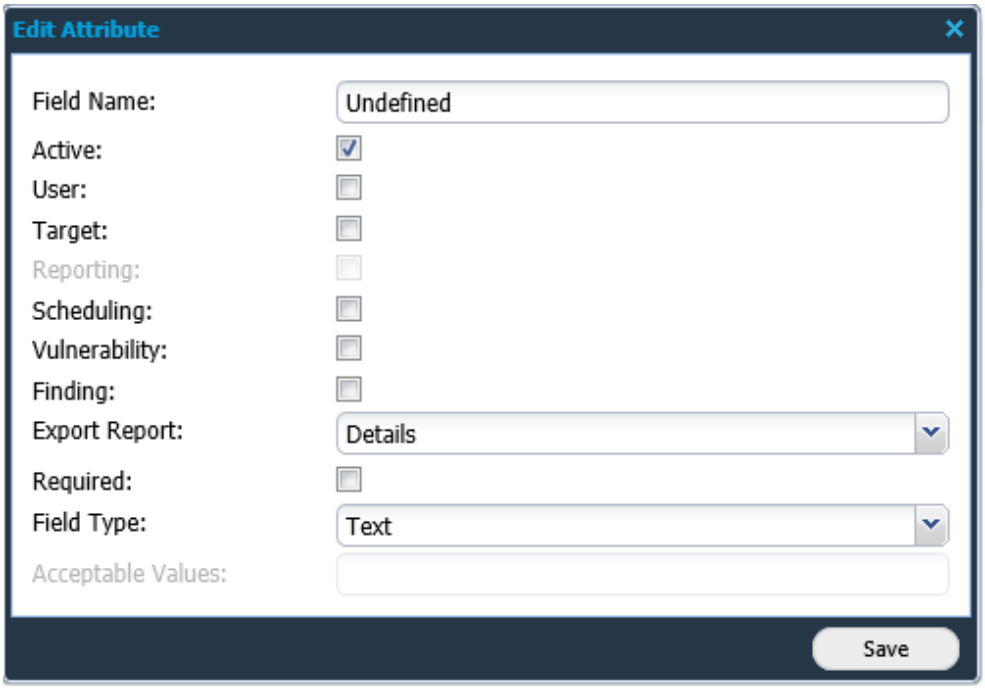
5.1 Configure Attributes

To configure a custom attribute,

1. Go to **Main Menu > Settings > Account**.
2. Select **Attributes** tab.
3. Right click on any undefined fields and click **Edit** to open the *Edit Attribute* window.



4. Provide a name for the column to be added.

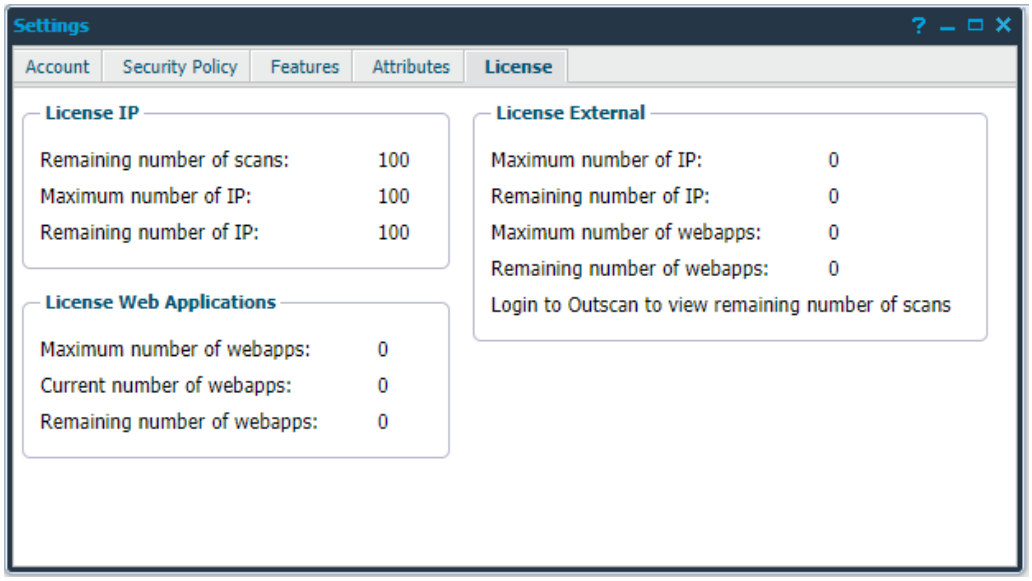


5. Enable **Active** field.
6. Configure the attribute according to options described in the *Attribute Options* table below.
7. Click **Save**.

Option	Description
Field Name	Specifies the name of the custom attribute.
Active	If checked the attribute will be active in the system.
User	Creates a column in Manage Users, which is set when creating or editing a user.
Target	Creates a column in *Manage Targets*, which is set when editing a target or labeling a target group.
Reporting	Creates a column in *Manage Targets* and the **Findings** tab in *Reporting Tools*, which can be set when editing a target or labeling a target group. Only usable if target is selected.
Scheduling	Creates a column in the **Scan Schedules** tab in *Scan Scheduling*, which can be set when creating or editing a scan schedule.
Vulnerability	Creates a column in the *Vulnerability Database*, and in the **Findings** tab in *Reporting Tools*. This attribute can be set by editing an entry in the *Vulnerability Database* by right clicking the entry to edit and choose **Edit Attributes**.
Finding	Creates a column in the **Findings** tab in *Reporting Tools*, which can be set by editing an entry in the **Findings** tab by right clicking and select **Edit Attributes**.

Option	Description
Export report	Choose in what section of an exported report the attributes will be presented in. *User*, *Target*, and *Scheduling* are not presented in the exported reports. ► **None**: The attribute will not be included in any reports. ► **Details**: The attribute will be included in both PDF and XML reports. ► **Host Summary**: The attribute will be included in both Excel and XML reports. ► **All**: The attribute will be included in PDF, Excel and XML reports.
Required	If an attribute field exists for an entity, the attribute field requires a value.
Field Type	This will select a specific type of input that can be used in the attribute. ► **Text**: Input of strings. ► **Combo**: Toggle a dropdown menu with values specified in **Accepted Values**. ► **Checkbox**: Creates a checkbox for the attribute which allow the attribute to be checked or not checked. ► **Number**: Only allows numbers to be entered in the attribute, ranges can be specified in **Accepted Values.** ► **Date**: Allow the attribute to select a date through a calendar.
Acceptable Values	Accepted values for the Combo and Number attributes. ► **Combo**: Specify values that is shown in the combo attribute, to separate values use the pipe | symbol, e.g. Mr|Mrs|Miss|Dr etc. ► **Number**: Specify an allowed range that can be entered in the attribute, e.g. 35-70. ***Note**: Acceptable Values is only visible if Combo or Number has been selected in Field Type.*

6 License



In the **License** tab, the remaining number of scans on the account can be seen, together with the maximum number of targets that can be maintained in the system.