Outpost24

Vulnerability Management made easy

Integrations

A Quick Start Guide

Version: 2.2

2018-06-20

Table of Contents

About This Guide

The main purpose of this document is to provide users a comprehensive overview of how to setup and use Integrations module in OUTSCAN™ and HIAB™. This document has been elaborated under the assumption that the reader has access to the OUTSCAN /HIAB account and portal interface.

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

Copyright

Trademark

1 Overview

1.1 Integrations Overview

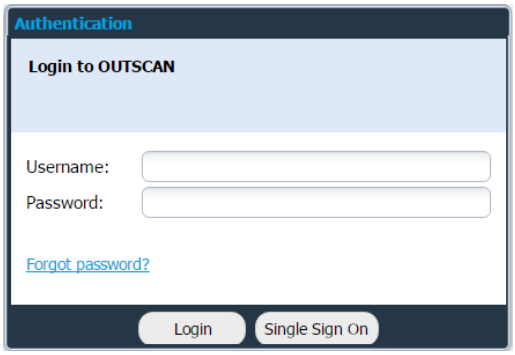
	DATA	OUTSCAN	HIAB
IDENTITY PROVIDER	Authentication <	✓	✓
SPLUNK	Events >	✓	✓
ATLASSIAN JIRA	Events >	✓	✓
SERVICENOW	Assets < Findings >	✓	✓
AMAZON	Assets <	✓	✓
CYBERARK	Credentials <	✓	✓
LDAP/AD	Users < Targets <		✓
SYSLOG/ SYSLOG TLS	Events >		✓
ARCSIGHT	Events >		✓
SNMP	Events >		✓
DATABASE CONNECTOR	Events > Findings >		✓

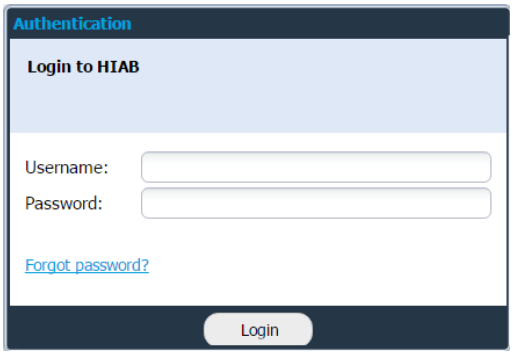
Note: *The arrows represent if our platform takes the data from the integrated system as an input or if it sends the data to the integrated system as an output.*

2 Getting Started

To launch the OUTSCAN application, navigate to https://outscan.outpost24.com.
Users who have HIAB, connect to your HIAB by using its assigned network address.

***Note**: Use HTTPS protocol.*





1. Log in as **Main User/Super User** using your credentials.
2. To access the Integrations module, go to **Main Menu → Settings → Integrations.**

3 Identity Provider

An Identity Provider (IDP) offers user authentication as a service. It is a trusted provider that allows the use of single sign-on (SSO) to access other application. SSO enhances usability by reducing password fatigue as passwords are maintained on your IDP.

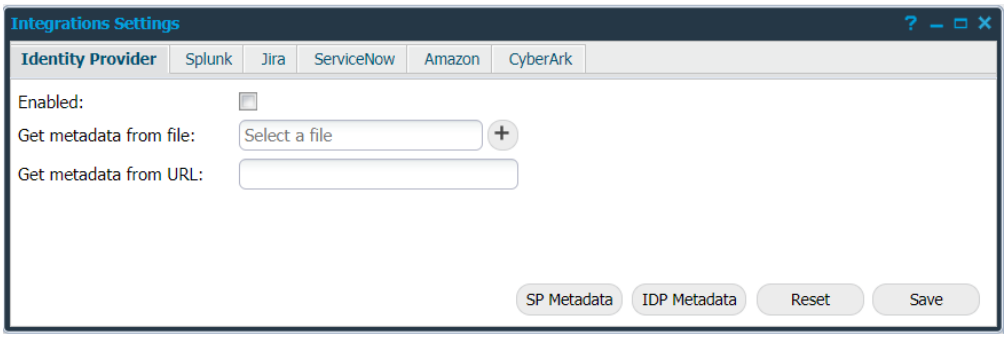
To enable SSO on HIAB/OUTSCAN you will have to import meta-data from your IDP into HIAB/OUTSCAN. You will also need to export the service provider's meta-data from HIAB/OUTSCAN and import it to your IDP.

***Note**: While reading the response from IDP during signing in to our portal, we accept signed assertions with parameters. The parameters list which your IDP is returning in response must include your user name in a parameter named UID.*

Set up Identity Provider Integration

To set up Identity Provider:

1. Go to **Main Menu → Settings → Integrations → Identity Provider**



2. Provide the below information to enable Identity Provider (IDP):

   - **Enabled:** Select the Enabled checkbox to enable the protocol for single sign-on trusting another source to login.

   Use one or both of the following option to provide metadata of IDP:

   - **Get metadata[1] from file:** Select Identity provider's metadata file by clicking the + symbol beside the field.
   - **Get metadata from URL:** Provide a URL from which the OUTSCAN or HIAB (Service Provider) should fetch metadata from IDP.

1 Metadata contains information such as how it works, what type of login is acceptable etc.,

After enabling the required settings:

1. Click **Save** to save the current settings.
2. Click **Reset** to fully remove the current settings. It will disable the integration and it doesn't have to be done after you've disabled it since you might want to use the same settings again.
   - **IDP Metadata**: This shows the currently uploaded metadata of the Identity Provider.
   - **SP Metadata**: Click on this button, to check service provider's metadata.

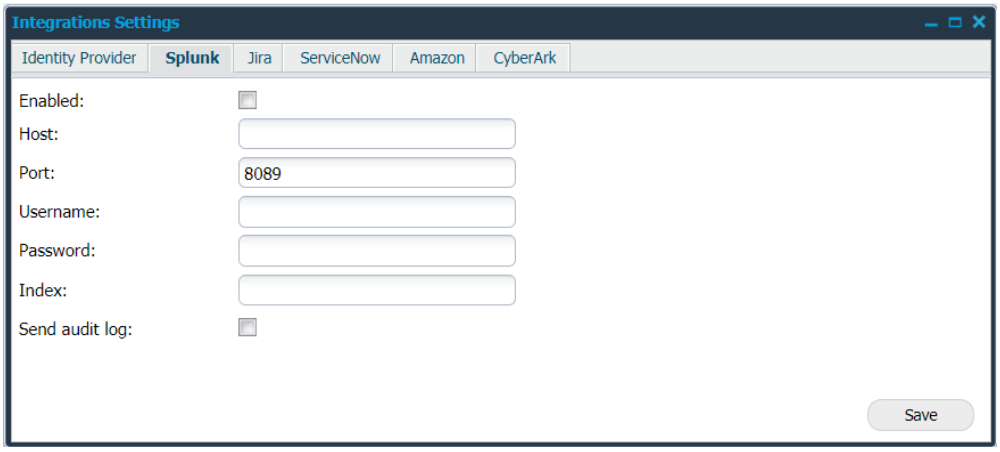
4 Splunk

Splunk is a software for searching, monitoring, and analyzing machine-generated big data. Splunk captures, indexes, and correlates real-time data in a searchable repository from which it can generate graphs, reports, alerts, dashboards, and visualizations.
A trial version of Splunk can be downloaded from the official Splunk website.
It is implemented in both OUTSCAN and HIAB and is mostly used in Event Notification system and Audit Log.

Set up Splunk Integration

To set up Splunk:

1. Go to **Main Menu → Settings → Integrations → Splunk**



2. Provide the below information to use Splunk:

Option	Description
Enabled	Click on this field to enable the Splunk feature.
Host	Provide your Splunk server name.
Port	Provide the management port that Splunk is using to communicate.
Username	Provide username to authenticate against Splunk server.
Password	Provide password to authenticate against Splunk server.
Index	If the user enters an index that does not exists, it will create a new one. All events will be prefixed with the index name
Send audit log	Check this box to send audit log entries to Splunk.
Save	Click on this button to save your current settings.

5 JIRA

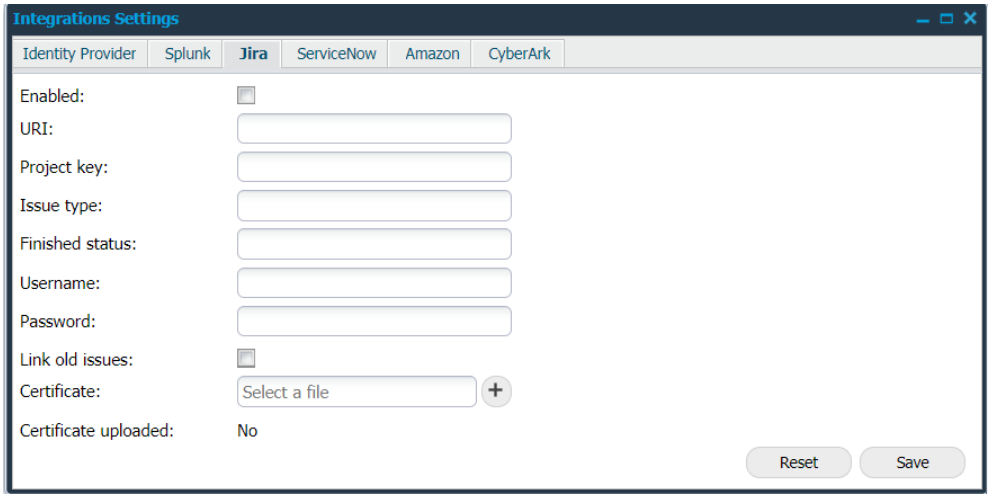
JIRA is a ticketing system which is implemented in both OUTSCAN and HIAB. It can be used in many ways and has different projects to organize the various usages. Tickets (issues) can be created with an assignee who is responsible for getting it done and a reporter who created it. When JIRA is enabled, it will be visible as a ticket system, both in **Assign Task** and **Event Notifications**.

***Note**: A linked issue can be created between projects or sub-tasks if it is a bigger task. The Jira instance must be running HTTPS.*

Set up JIRA Integration

To set up JIRA:

1. Download the HTTPS certificate from your JIRA server.
2. Go to **Main Menu → Settings → Integrations → JIRA**



3. Follow the below procedures to create a JIRA ticket:

Option	Description
Enabled	Select the **Enable** checkbox to enable JIRA.
URI	Provide the URI of JIRA server (only https protocol is supported).
Project Key	Provide the project key from the JIRA instance to use.
Issue Type	JIRA can be used to track different types of issue. The common Issue types used are Bug, Epic and Story.
Finished Status	Mention the status of the JIRA issue.
Username	Provide the username to authenticate against JIRA server.
Password	Provide the password to authenticate against JIRA server.
Link old issues	Enable this feature if you want to link old issues. It is useful when you regenerate tickets for similar issue.
Certificate	Upload the SSL certificate of the JIRA instance.
Certificate uploaded	Displays **Yes** if a certificate has been uploaded and **No** if there is no certificate available.
Reset	Click **Reset** to fully remove the current settings. It will disable the integration and it doesn't have to be done after you've disabled it since you might want to use the same settings again.
Save	Click on this button to save your current settings.

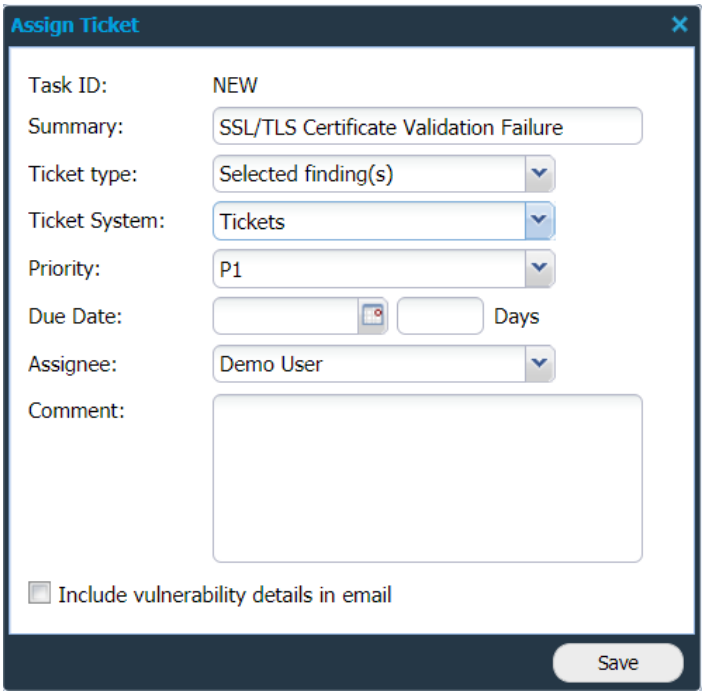
***Note**: The user should have permission to read issues and to create new issues.*

If you scan a lot of targets, it is recommended to have a separate JIRA project for these tickets, since they can easily reach high in numbers. Every new finding can create one or more new tickets in your JIRA server.
There is no maintenance needed except synchronizing configuration if you re-configure your JIRA in any way. Synchronization between JIRA and OUTSCAN/HIAB is periodic. This may cause some delay in the update.

After enabling JIRA, use any of the following ways to create a ticket:

Method 1:

1. Go to **Main Reporting Tools → Findings**.
2. Right click on any finding, select **Assign task**.



3. Select **JIRA** in the ticket system drop-down menu.
4. Click **Save** to create a ticket.

Method 2:

1. Go to PCI scanning → Reports.
2. Right click on a finding, select **Assign task**.
3. Select **JIRA** in the ticket system drop-down menu.
4. Click **Save** to create a ticket.

Method 3:

1. Go to Event Notifications
2. Click **+New**.
3. Select **JIRA** in the **Action** drop-down menu.
   ***Note**: This action is only available for Finding Information, Low Risk, Medium Risk and High Risk.*
4. Click **Save** to create tickets whenever a report is created with findings of the type of the event.

6 ServiceNow

ServiceNow is a cloud service that can handle many different needs within a company. Some of its features are:

- Ticket system
- CMDB
- Discovery server
- Security management

When ServiceNow is enabled, it will be visible as a ticket system in **Assign Task**, and **Event Notifications**. It also adds an option of importing targets from ServiceNow and activating events and tools for adding tickets. If you disable ServiceNow, the targets will no longer update or scan via ServiceNow until you enable it again.

Ticket system:

A ServiceNow ticket created for a finding will be added as an Incident with target and script information and solution to the finding will be added as Problem. Synchronization between ServiceNow and OUTSCAN/HIAB is periodic. This may cause some delay in the update. With the ticket system, we recommend using old scans to add tickets that you want to get started and then add the events you want for future scans.

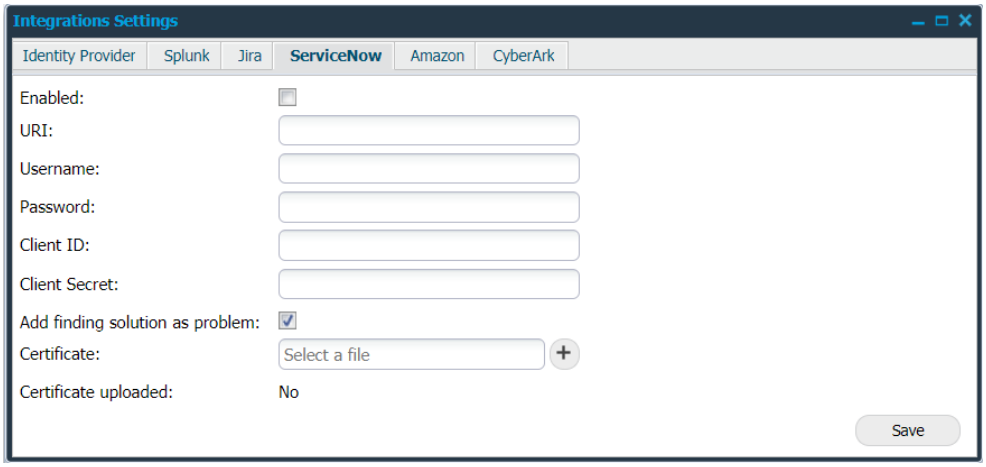
Set up ServiceNow Integration

The ServiceNow service requires an external OAuth Setup to be configured.
To set up:

1. Go to **System OAuth → Application Registry** in the Service Now service.
2. Click **New**.
3. On the interceptor page, click **Create an OAuth API endpoint for external clients**.
4. Fill in the fields.
5. Click **Submit**.

Once that has been done, fill in the Client ID and Client secret (if used) in the **Integrations** window.

1. Go to **Main Menu → Settings → Integrations → ServiceNow.**



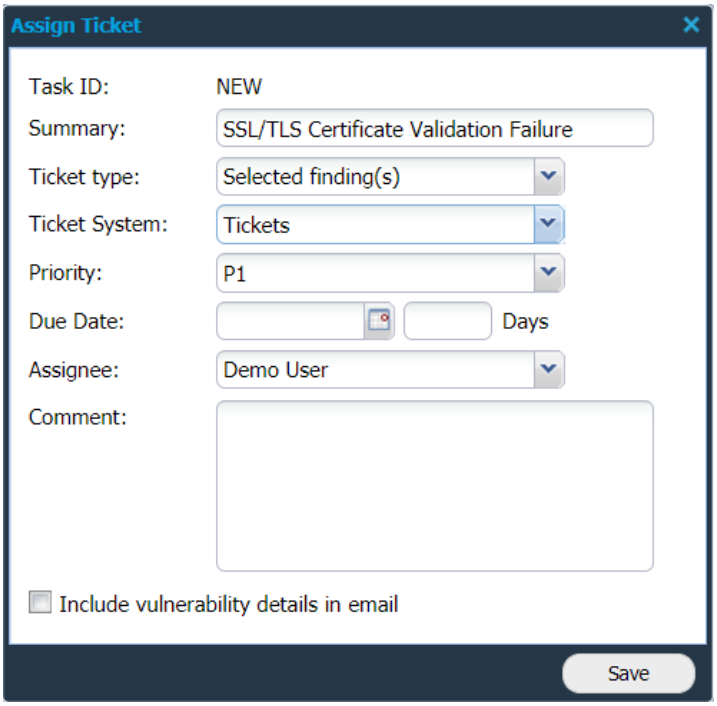
2. Follow the below procedure to enable ServiceNow:

Option	Description
Enabled	Click on this field to enable ServiceNow.
URI	Provide the URI of ServiceNow server (only https protocol is supported).
Username	Provide the username to authenticate against ServiceNow server
Password	Provide the password to authenticate against ServiceNow server
Client ID	(If used) Provide your client ID which is generated using OAuth module.
Client Secret	(If used) Provide your client password.
Certificate	Upload the SSL certificate of your ServiceNow instance.
Certificate uploaded	Displays Yes if a certificate has been uploaded and No if there is no certificate available.
Save	Click on this button to save your current settings.

After enabling ServiceNow, use any of the following ways to create a ticket:

Method 1:

1. Go to **Main Reporting Tools → Findings**.
2. Right click on any finding, select **Assign task**.



3. Select **ServiceNow** in the ticket system drop-down menu.
4. Click **Save** to create a ticket.

Method 2:

1. Go to PCI scanning → Reports
2. Right click on a finding, select **Assign task**.
3. Select **ServiceNow** in the ticket system drop-down menu.
4. Click **Save** to create a ticket.

Method 3:

1. Go to Event Notifications Click **+New**.
2. Select **ServiceNow** in the **Action** drop-down menu.

   ***Note**: This action is only available for Information, Low Risk, Medium Risk and High-Risk findings*

3. Click **Save** to create tickets whenever a report is created with findings of the type of the event.

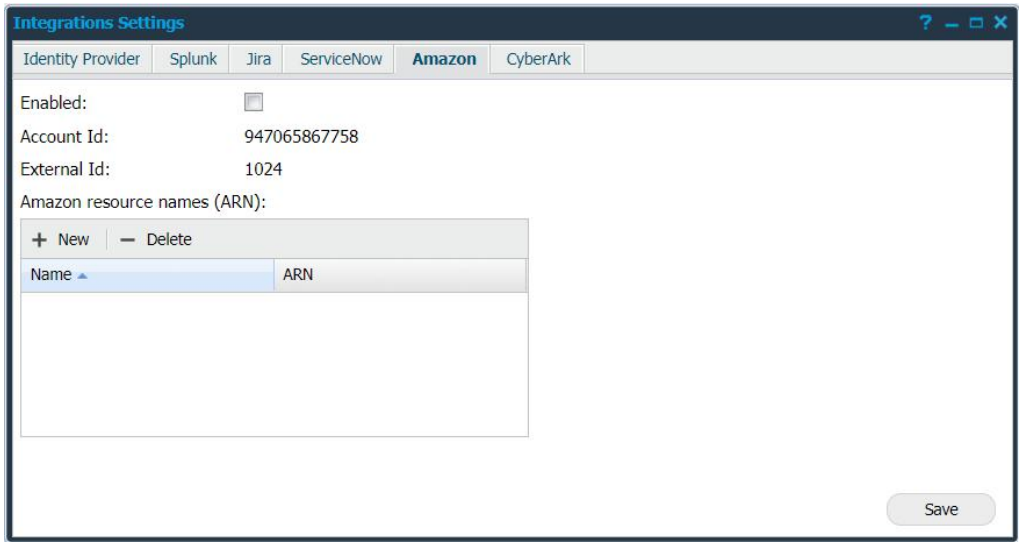
7 Amazon

Here you can set up to run scans against instances in the Amazon cloud. It will also enable the option to run discovery scans using ARNs added in this setup. Amazon service is implemented in both OUTSCAN and HIAB.

***Note**: Amazon targets can only be added to OUTSCAN/HIAB via discovery scans. Only OUTSCAN is Whitelisted by Amazon as an authorized scanner, and scanning from HIAB may require additional authorization from Amazon.*

Set up Amazon Integration

To setup Amazon, go to **Main Menu → Settings → Integrations → Amazon**



Follow the below procedure to scan instances:

1. Click on the **Enabled** field to enable this feature.
2. Create a new user role with the **Account Id** and **External Id** noted.

3. Apply IAM policy given below for the role on Amazon cloud to grant access to the targets.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "Stmt1400711494000",
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeInstances",
            "ec2:DescribeRegions",
            "elasticloadbalancing:DescribeLoadBalancers",
            "elasticloadbalancing:DescribeTargetGroups",
            "elasticloadbalancing:DescribeTargetHealth"
        ],
        "Resource": ["*"]
    }]
}
```

***Note**: Any role which gives you read-only access to the required Actions listed in the policy will work.*

4. Enter the Amazon Resource Name (ARN) for the newly created role in the table using **+ New** button.
5. Click **Save** to save the current settings.

8 CyberArk

CyberArk provides a privileged account security solution and password vault. It is required to have the CyberArk AIM suite to use the integration.

Note: *CyberArk is supported in HIAB and OUTSCAN for both internal and external IP addresses.*

Manually Define Application

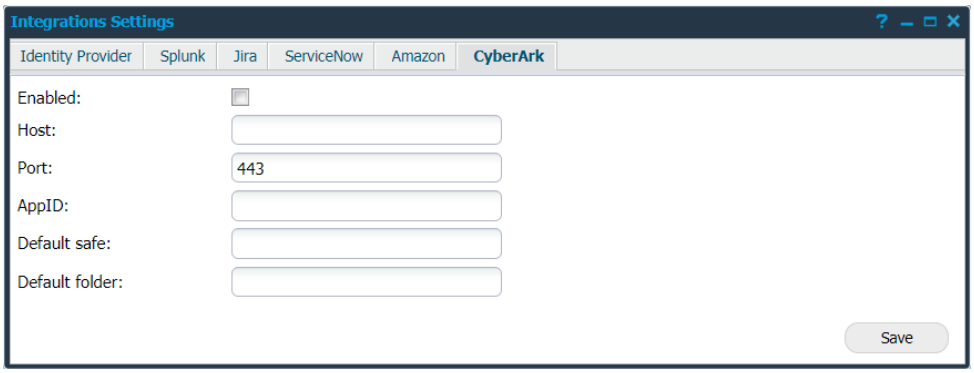
To define the Application manually via CyberArk's PVWA (Password Vault Web Access) Interface:

1. Log in as user allowed to managed applications (it requires Manage Users authorization)
2. Go to **Applications** tab, click **Add Application**; the Add Application page is displayed.
3. Fill with the pre-defined APPID the customer should use, specified in the **Name** field.

Set up CyberArk Integration

To set up CyberArk in OUTSCAN or HIAB:

1. Go to **Main Menu → Settings → Integrations → CyberArk**

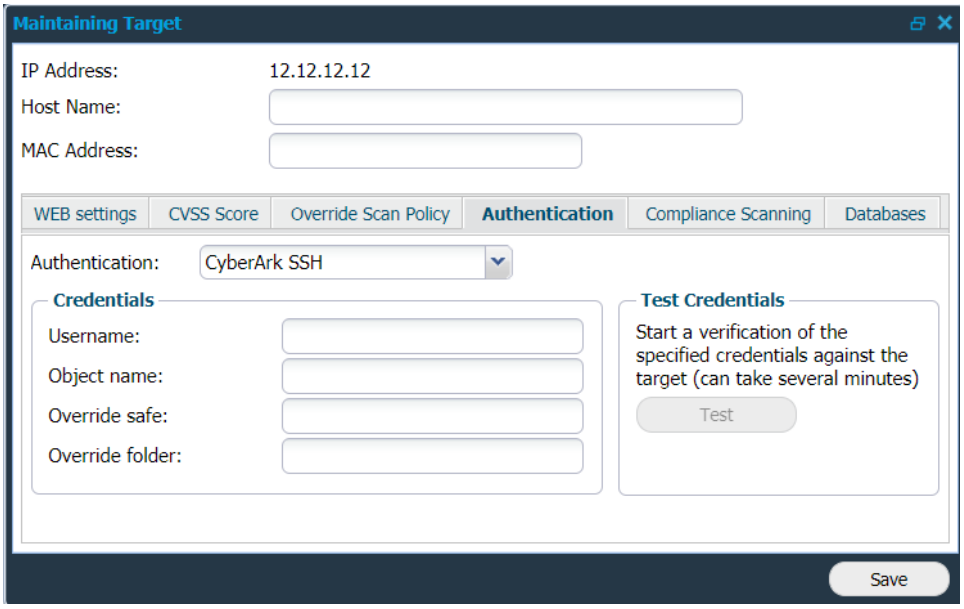


2. Provide the below information to use CyberArk:

Option	Description
Enabled	Click on this field to enable CyberArk.
Host	Provide the hostname of the CyberArk server.
Port	Provide the port number.
AppID	Enter the application ID.
Default safe	Provide a safe name in which you would like to store the password.
Default folder	Folder is usually root by default.
Save	Click on this button to save your current settings.

After enabling CyberArk,

1. Go to Manage targets.
2. **Edit** a target to setup the **Authentication**. **CyberArk SSH** and **CyberArk SMB** is now visible as new options.
3. Click on any of the options to use the respective authentication.



4. Provide your **Credentials**:

Option	Description
Username	Provide your username to authenticate against CyberArk Server.
Object name	Check your CyberArk Vault administrator and provide the object name.
Override safe	Provide a different safe name in case you wish to override the existing safe name.
Override folder	Provide a different folder name in case you wish to override the existing folder names.

5. Click **Test** to start a verification.
6. Click **Save** to enable the current settings.

9 LDAP/AD (HIAB only)

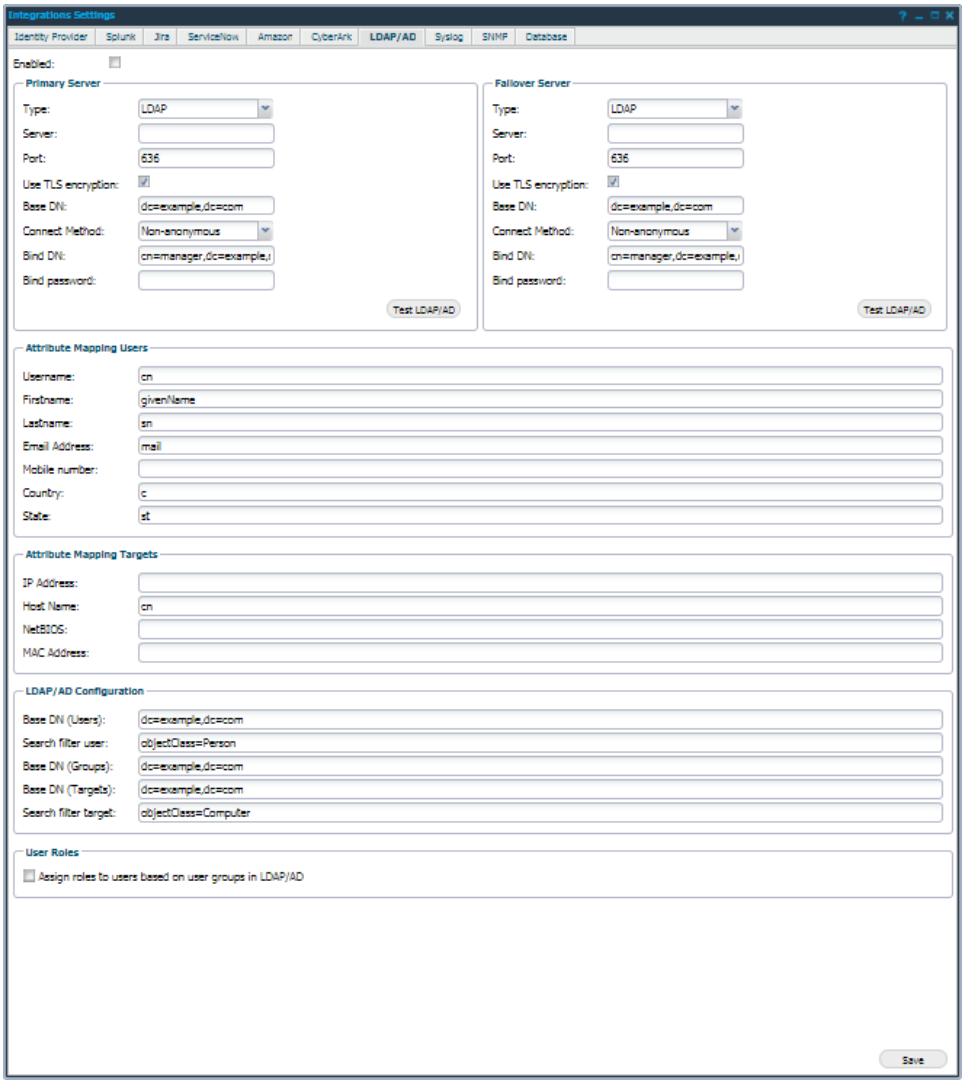
The Active Directory/LDAP integration is used for several purposes, such as:

- Authentication against the system with the purpose of user management, allowing organizational memberships or attributes from the AD dictate access in the HIAB.
- Discovery scanning, implying that devices added in the active directory can be added as devices to the HIAB for scanning purposes.

Set up LDAP/AD Integration

To set up a connection to a LDAP/Active Directory server follow the below instructions:

1. Go to **Main Menu → Settings → Integrations → LDAP/AD**



2. Enable the use of LDAP/AD in the system by select the **Enabled** checkbox.

Primary Server and Failover Server

The system allows you to define both **Primary Server** and a **Failover Server**.
The F**ailover Server** will be accessed if the **Primary Server** is unavailable when required. The following options are available for both **Primary** and **Failover** Server.

Option	Description
Type	Select if you want to use a LDAP or an Active directory server to authenticate user against, importing targets, users into HIAB.
Server	The Server and Port settings are where you define the network location of the LDAP or Active directory server.
Port	
Use TLS Encryption	Must be checked if the server utilizes TLS (Transport Layer Security) during the connection phase.
Base DN	Enter the base domain name, ex: "dc=ad,dc=local" ***Note**: If you have an Active Directory server, then you should also provide the Domain in a simple form like "ad.local". This will be used when we supply the user name in the authentication process against the active directory server.*
Connected Method	Define if the connection should be Anonymous or Non-anonymous. If the connection method is not anonymous, then you need to supply both Bind DN and a Bind password which will authenticate the connection to the server. ***Note**: Base DN is the domain where AD is located and Bind DN is the* *account which the HIAB should use to access the AD.*
Bind DN	
Bind Password	
Test LDAP/AD	Once all the required settings are supplied, you can check the configuration by pressing Test LDAP/AD button for respective section.

Import and specific mapping settings for the user and target integration are located under respective settings sections.

Attribute Mapping Users

Provide the attribute names on the LDAP server that corresponds to the user fields mentioned below.

Option	Description
Username	Attribute name on the LDAP server that maps to your username
Firstname	Attribute name on the LDAP server that maps to your first name.
Lastname	Attribute name on the LDAP server that maps to your last name.
Email Address	Attribute name on the LDAP server that maps to your email address.
Mobile number	Attribute name on the LDAP server that maps to your mobile number.
Country	Attribute name on the LDAP server that maps to your country name.
State	Attribute name on the LDAP server that maps to your state name.

Attribute Mapping Targets

Provide the attribute names on the LDAP server that corresponds to the target fields mentioned below.

Option	Description
IP Address	Enter the attribute name on the LDAP server that maps to IP address of the target.
Host name	Enter the attribute name on the LDAP server that maps to hostname.
NetBIOS	Enter the attribute name on the LDAP server that maps to NetBIOS name.
MAC Address	Enter the attribute name on the LDAP server that maps to MAC address.

LDAP/AD Configuration

Option	Description
Base DN (Users)	Enter the base domain name.
Search filter user	Provide any phrase to filter further.
Base DN (Groups)	Enter the base domain name.
Base DN (Targets)	Enter the base domain name.
Search filter target	Provide a phrase to filter further.

User Roles

1. Select the **User Roles** checkbox to assign roles to the users based on user groups in LDAP/AD.
2. Click **Save** to save the current settings.

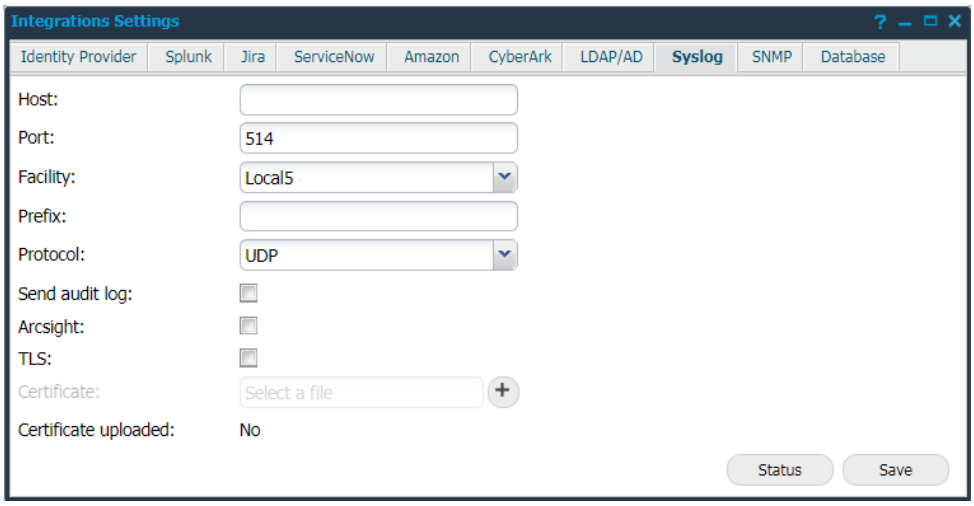
10 Syslog (HIAB only)

HIAB can pass logs and findings via Syslog events, which work with virtually any other security solution in the market, custom implementation of this with a wide range of SIEMs and event correlations systems among our existing MSSPs and partners already.
For example: ArcSight.

Set up Syslog Integration

To set up Syslog:

1. Go to **Main Menu → Settings → Integrations → Syslog**



2. Provide the below information to use Syslog:

Option	Description
Host	Provide the hostname.
Port	Provide the port that Syslog is using to communicate.
Facility	Choose a facility code from the drop-down menu. ***Note**: Facility code is used to specify the type of program that is logging the message.*
Prefix	Enter any word that you want to add as a prefix for each line.
Protocol	Select one of the protocols from the drop-down menu.
Send audit log	Check this box to receive audit log.
Arcsight	Click on this field to use the ArcSight format.
TLS	Click on this field to encrypt data. Use secure transport layer.
Certificate	Upload the certificate for the syslog server. Only needed if TLS is enabled.
Certificate uploaded	Displays if any certificate has been uploaded.
Status	Click on this button to check the network connectivity.
Save	Click on this button to save your current settings.

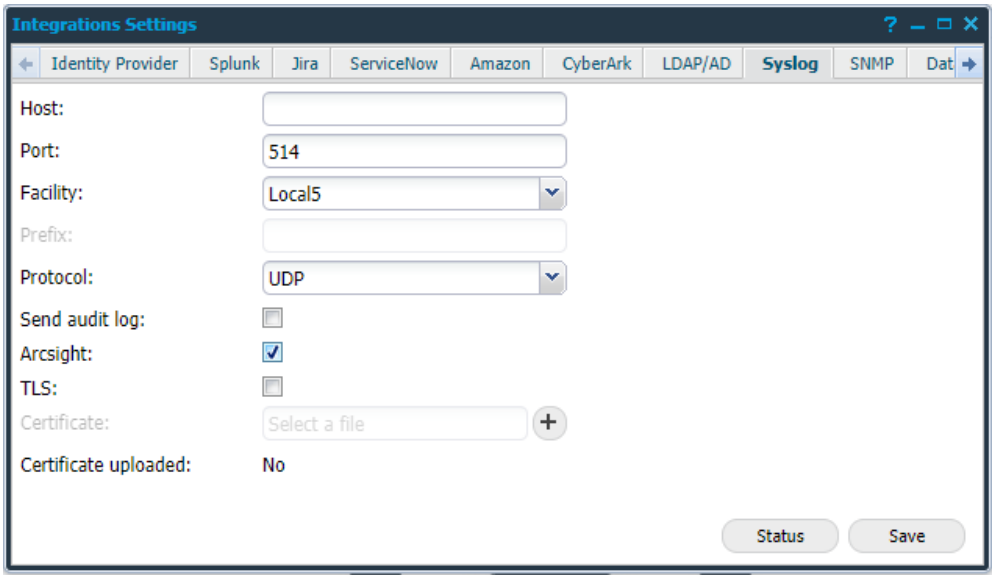
11 ArcSight (HIAB only)

ArcSight is a Syslog service developed by HP and is available at the systems which offer the Syslog feature. To date that is only HIAB.
Before enabling ArcSight in the HIAB, the ArcSight server need to be set up and configured.

Set up ArcSight Integration

To enable ArcSight:

1. Log in to the HIAB with the Main User/Super User.
2. Go to **Main Menu → Settings → Integrations → Syslog**.
3. Check the **Arcsight:** checkbox as shown in the figure.



4. Click **Save**.

When ArcSight is enabled, the Syslog message is built differently to fit into the ArcSight protocol.

11.1 Using ArcSight

When a Syslog event is activated, an ArcSight message will be built instead of the ordinary Syslog message.
The Syslog message will be sent to the ArcSight logger or the connector. When the logger shows the message, it is divided into columns that is easier to work with than the raw data.

***Note**: No ArcSight specific errors should occur. If the ArcSight server has errors it is due to the Syslog implementation, not the ArcSight implementation.*

It is recommended that the customer uses ArcSight together with TLS. If the logger cannot work with the TLS messages, a connector is recommended to be able to do so. There is no maintenance needed for ArcSight, but the logger or the Syslog settings must be updated if IP numbers or other information are switched.

Examples:

A Syslog message

```
Risk: Script Name: "Unencrypted Remote Authentication Available -
POP3" Script Id: "219784" Target: "192.168.202.6" Port: "110"
BugTraq: "No bugtraq" CVSS: "6.8" New: "0" CVE: "No CVE" Family:
"pop3" First Seen: "2016-11-21 11:08" Last Seen: "2016-11-24
18:06" Product: "Unencrypted Remote Authentication" Has Exploits:
"false" - Medium
```

An ArcSight message

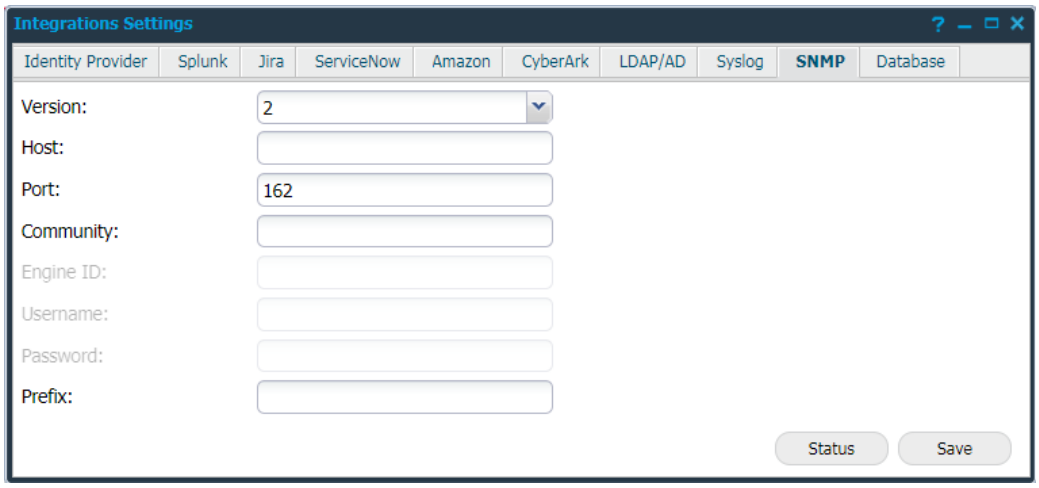
```
dvc=192.168.202.6 spt=110 cs1Label=Script Name cs1=Unencrypted
Remote Authentication Available - POP3 cs4Label=BugTraq cs4=No
bugtraq cs2Label=CVE cs2=No CVE deviceCustomDate1Label=First Seen
deviceCustomDate1=Nov 21 2016 11:08:00
deviceCustomDate2Label=Last Seen deviceCustomDate2=Nov 24 2016
18:08:00 msg=Script Id: 219784 New: 0 Family: pop3 Product:
Unencrypted Remote Authentication Has Exploits: false
```

12 SNMP (HIAB only)

HIABs can pass events via SNMP and integrate into SIEM/Log management solutions.

Set up SNMP Integration

To set up SNMP, go to **Main Menu → Settings → Integrations → SNMP**



Provide the below information to use SNMP:

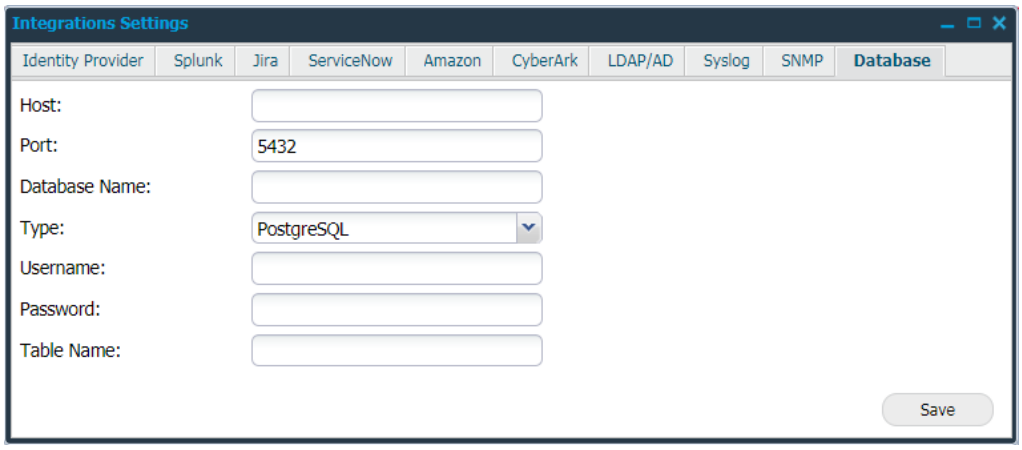
Option	Description
Version	Select either 2 or 3 depending on the SNMP version you are using.
Host	Provide the hostname.
Port	Provide the port number SNMP is using to communicate.
Community	Add a password that is shared by multiple SNMP agents.
Prefix	Enter any word that you want to add as a prefix for each line.
Status	Click on this button to check the network connectivity.
Save	Click on this button to save the current settings.

13 Database (HIAB only)

There are other products which may require Outpost24 data to be available in a database for selection. We do not grant access to the internal database used in HIAB because it is subject to restructuring for performance and optimization, and as a security measure.
However, HIAB can be configured to set up a database connector and export findings data to external databases using **Events** or **Report Schedules**. Then, you may run your analysis or integrate external products/solutions to the external database.
When connecting to the database, you must have permissions to create tables as well as updating data.

Supported External Databases:

- MS SQL
- MySQL
- PostgreSQL



Provide the below information to set up a Database connector:

Option	Description
Host	Provide your hostname of your external database server.
Port	Provide the port number database connector is using to communicate.
Database Name	Provide database name of external database server to which findings data should be exported.
Type	Select one of the types from the drop-down menu ► MS SQL ► MySQL ► PostgresSQL
Username	Provide the username to authenticate against external database server
Password	Provide the password to authenticate against external database server
Table Name	Provide a valid name for table in the database.
Save	Click on this button to save your current settings.