pikered

ZAIUX® Evo – User Guide

Version: 2.15.6 | February 2026

pikered

Table of Contents

Adversarial Exposure Validation, made simple

ZAIUX® Evo is a SaaS solution that automates Command and Control (C2) attack activities, generating false positive-free reports featuring Remediation Plans.
ZAIUX® Evo delivers advanced Breach and Attack Simulations (BAS) to IT infrastructures. It employes Artificial Intelligence to allocate resources through mathematical optimization, executing automated ethical hacking processes to concretely test security holes in the target network.
Unlike other attack simulations, ZAIUX® Evo autonomously emulates a realistic malware infection. This means that the whole defense chain is validated against a targeted attack coming from the outside, which brings out all vulnerabilities both in Privilege Escalation prevention within the domain and in data exfiltration protection.

What sets ZAIUX® Evo apart

ZAIUX® Evo makes it possible to perform a complete and realistic simulation of an intrusion in a MS Active Directory & Entra ID environment with an intelligent solution, exploiting a regularly updated range of the most modern and advanced hacking techniques, run in stealth mode to emulate a human approach.
Automation is managed by our proprietary engine, leveraging Machine Learning algorithms specially crafted by our team of experts, to emulate human intelligence, overcoming time and cost barriers of a manual execution.
Through Artificial Intelligence, the adaptive algorithms shape the system's response according to the attack surfaces emerging from the scans, all in a fully automated way.
ZAIUX® Evo generates, for each assessment, an isolated sandbox associated with a unique initialization package, which can be directly executed from any endpoint within the target network, without installing any agent.

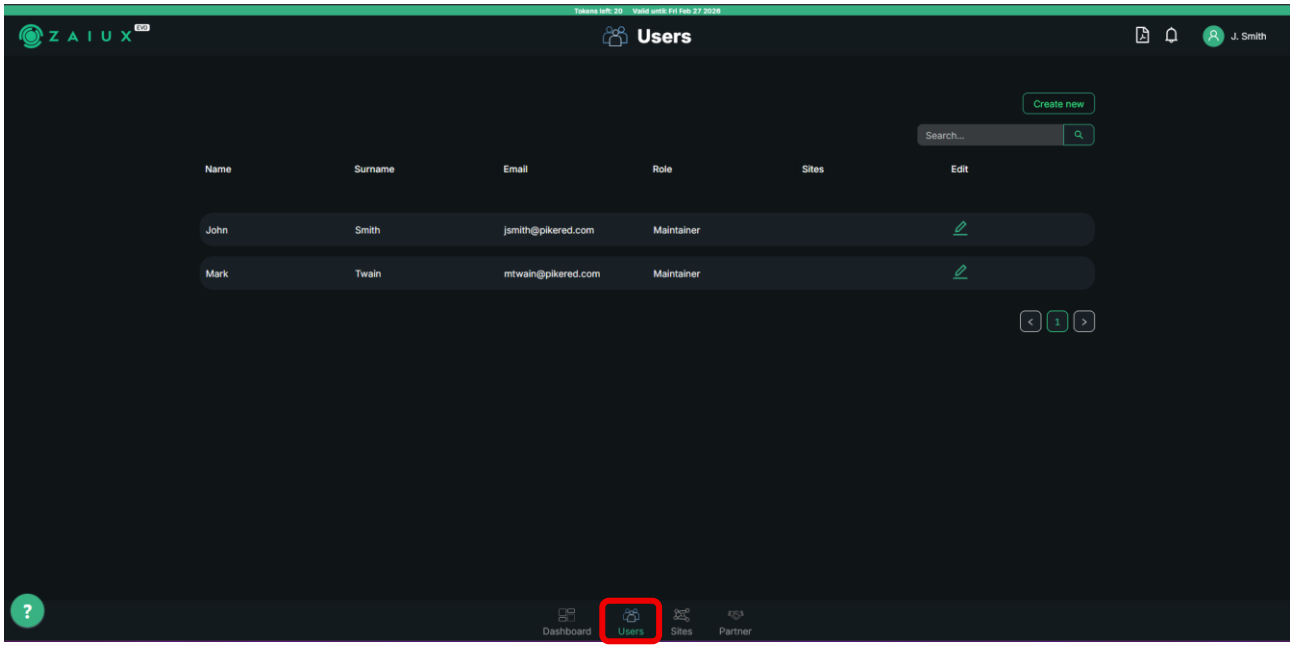
Key Benefits

Enhanced visibility of Crown Jewels and critical assets	Clear view of misconfigurations and realistic attack paths
Flexible partitioning of the BAS attack surface	Optimization of IR playbooks and defense tools

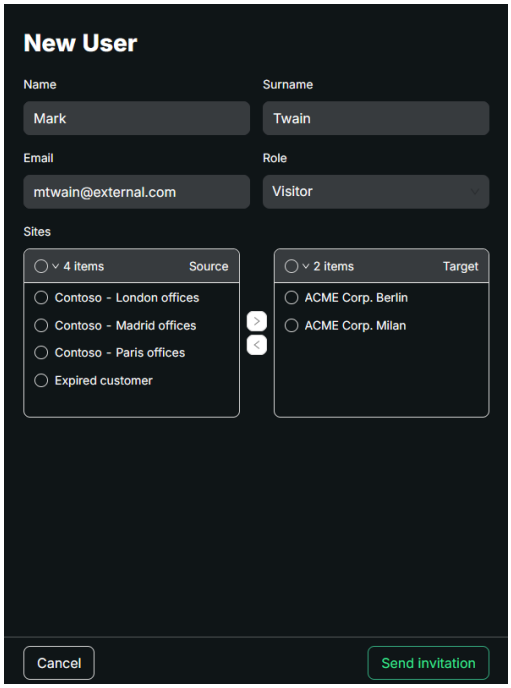
Getting started with ZAIUX® Evo

Upon completing the purchase process, the specified users will be invited to create the first administrator account for the tenant. Follow the video guide here to create your first account before proceeding with the user guide.

Types of users



Apart from the first user assigned during the purchase process, additional users with different access levels can be created. Clicking **"Create New"** opens a sub view on the right side of the page, allowing the creation of a new user.



- **Maintainer**: Full access to the tenant.
- **Regular**: Cannot edit or add sites, nor create or edit users.
- **Visitor**: External user granted read-only access to a selected site; cannot access any other pages . (e.g., an MSP customer who wants to monitor their network).
- **Sales**: For registered partners; provides access only to the partner program area to take certifications, download the Sales Kit, request pre-sale support, or create white-labeled reports by uploading a custom logo.

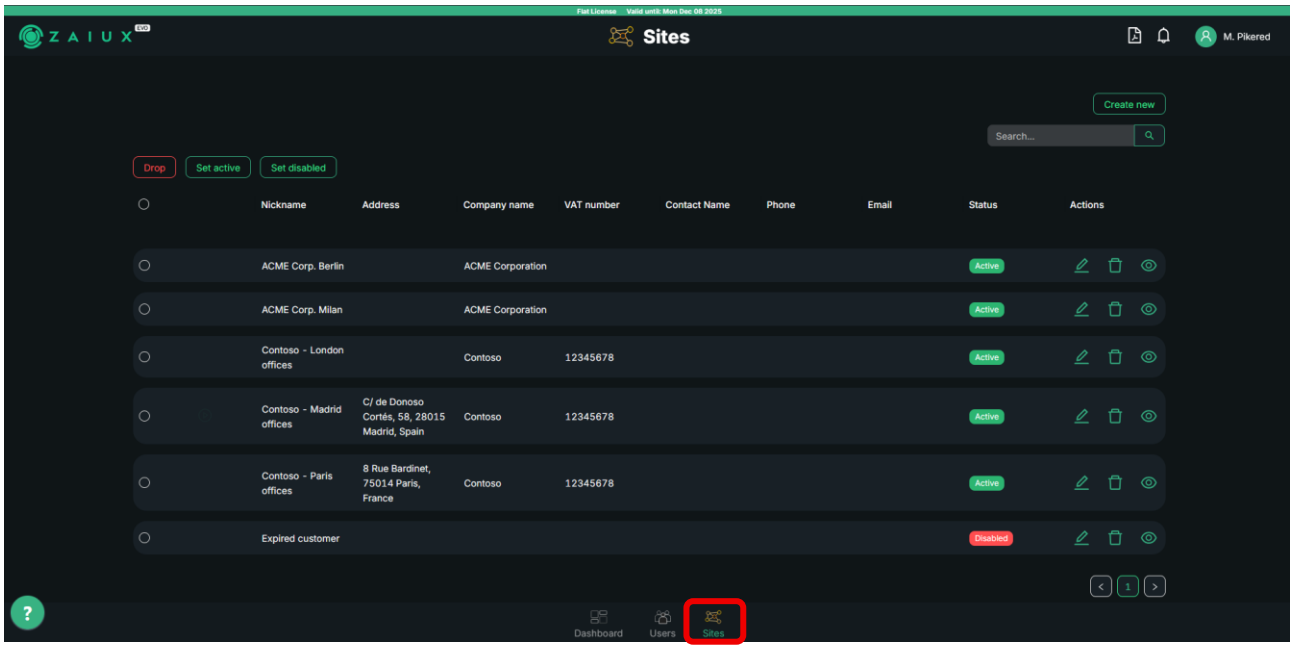
Clicking Send Invitation will send a registration email to the specified address.

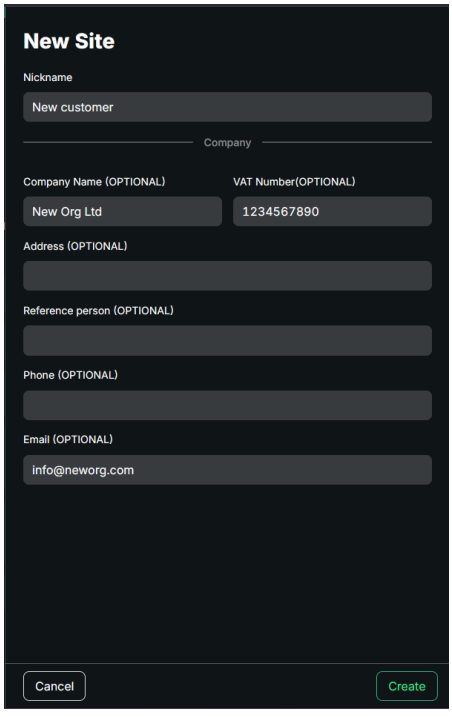
Creating a site

What is a site in ZAIUX® Evo?

- A single Active Directory domain to be tested (best use case for MSPs)
- A logical breakdown of a complex infrastructure with multiple domains (one site per domain to test)
- A logical breakdown of a complex infrastructure with one domain but different Organizational Units or VLANs that must be tested individually.

The list of sites can be accessed by clicking the "**Sites**" tab in the bottom-bar menu.





Clicking "Create new" opens a sub view on the right side of the page, allowing the creation of a new site.

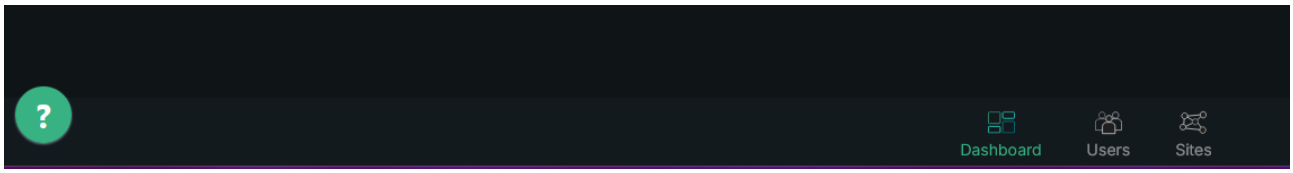
All fields are optional except Nickname, which should identify the customer (for MSPs) or the owned site (for end customers).

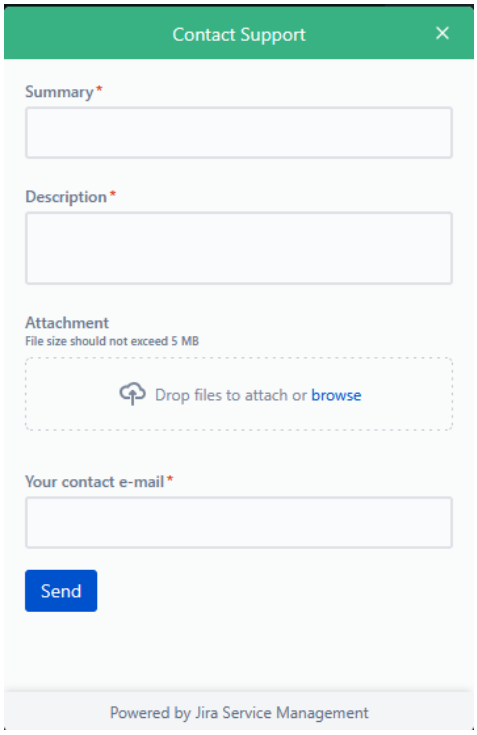
Click Create to add the new site to the list.

Anagraphic information can be edited later, and the site can be disabled or permanently deleted.

Opening a support request

Every page, including the login page, has the possibility to open a support request to pikered by clicking the "**?**" button on the bottom-left:





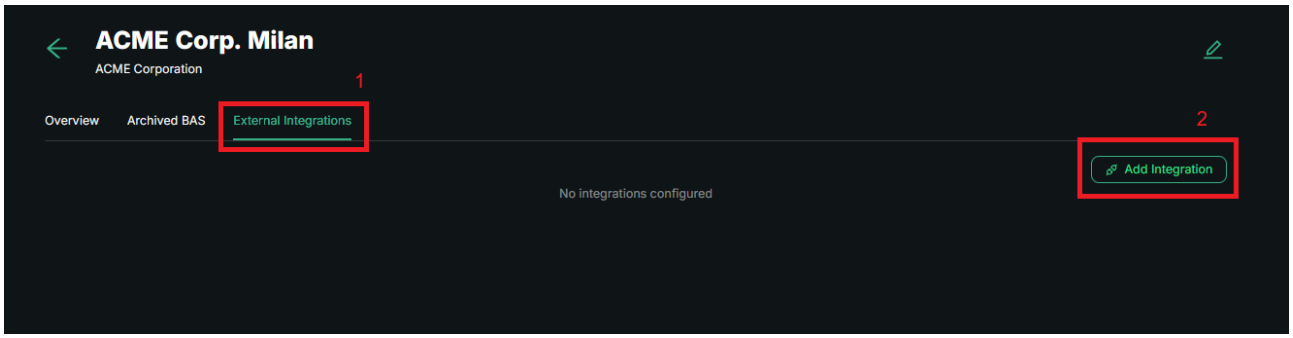
When contacting support, include as many details as possible and provide evidence of the issue, such as outputs and screenshot to help the analysts to assist you in the best way possible.

Fill in the contact email field, and the support team will respond as soon as possible, also depending on your contract type.

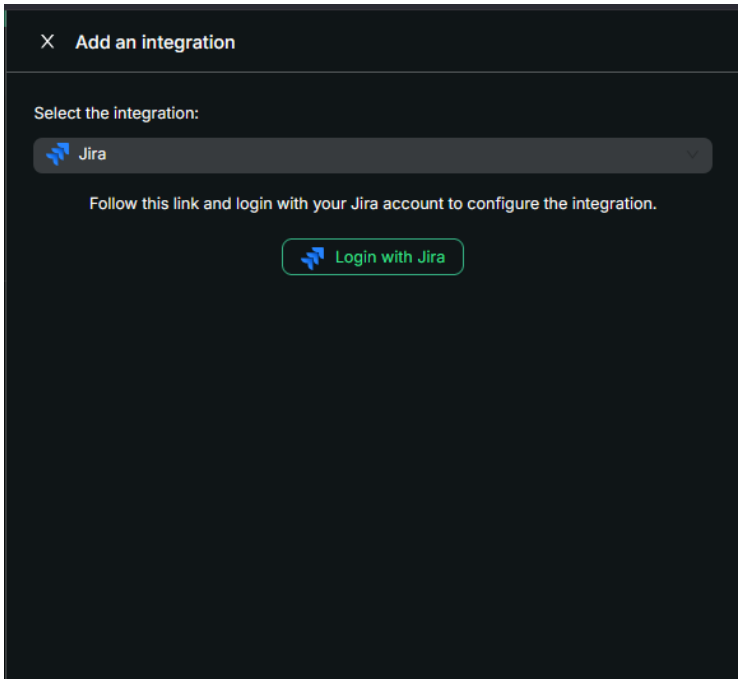
Support is delivered via Jira Service Management and handled exclusively by Pikered employees: no third-party technicians are involved.

Integrating Jira Service Management

ZAIUX® Evo can be extended through external software and services that are now being continuously integrated into the platform.
Each integration can be configured per Site, enabling seamless interoperability with tools commonly used by system integrators and blue teams, and improving overall quality of life.
For each site, click "**External Integrations**", followed by "**Add Integration**", to choose a new one:

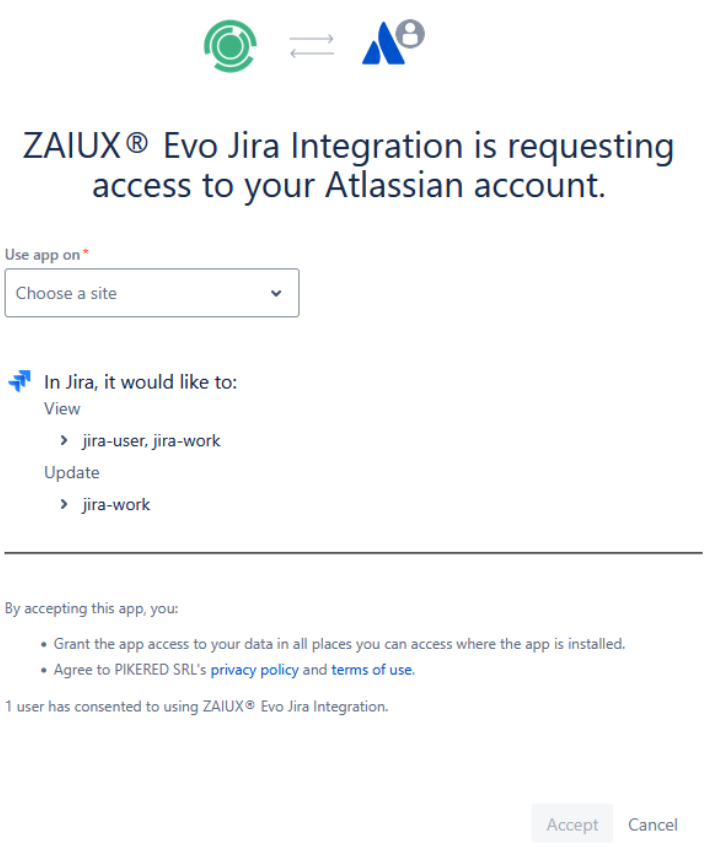


ZAIUX® Evo is now officially available on the [Jira Marketplace]



To integrate ZAIUX® Evo with Jira Service Management, simply select **"Jira"** from the list of integrations and click **"Login with Jira."**

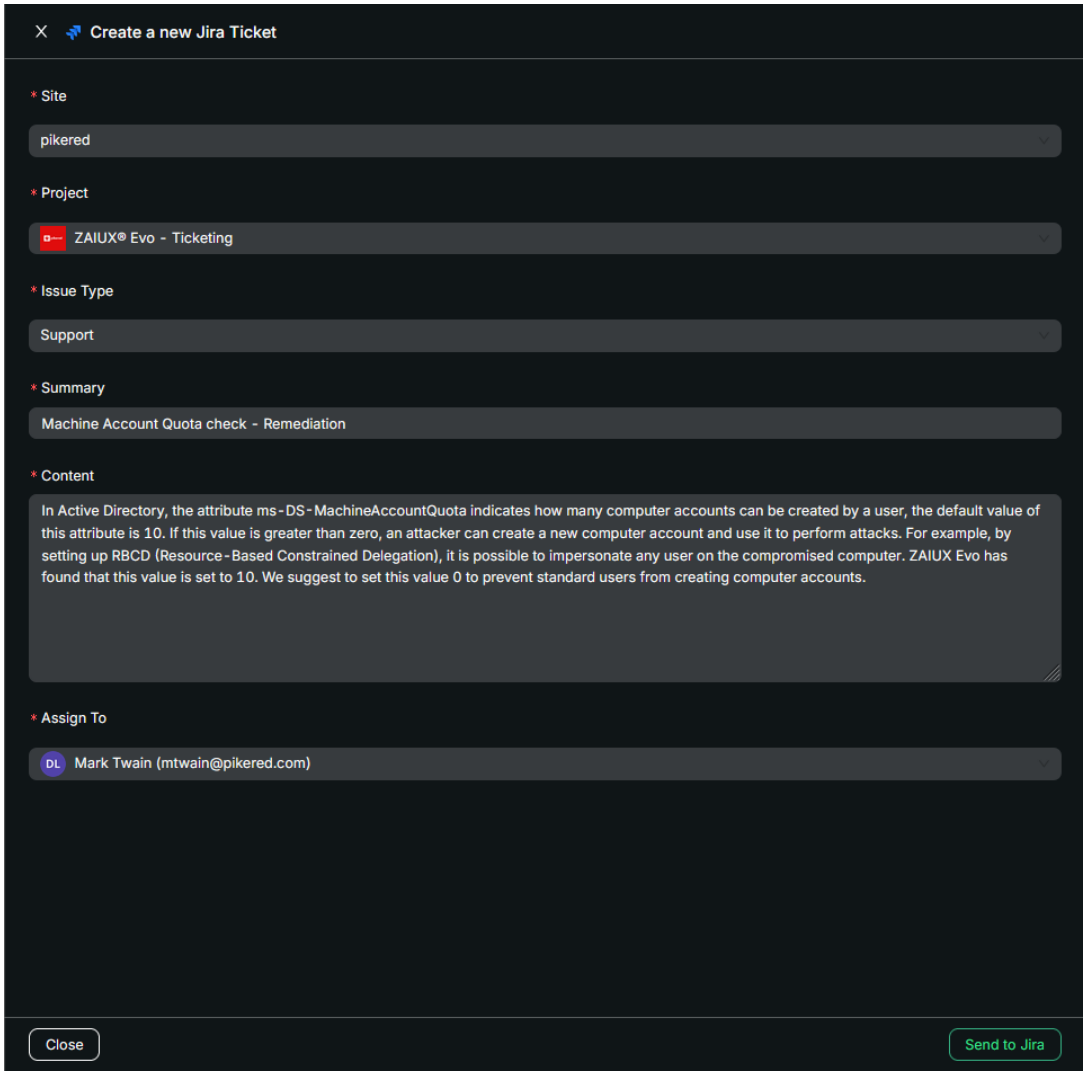
If your Jira session is already active, a Jira form will be displayed.



After selecting the desired sites where the new tickets will be created, simply click **"Accept."** Within a few seconds, the integration will be established, and the Jira widget will appear on the **External Integrations** page.

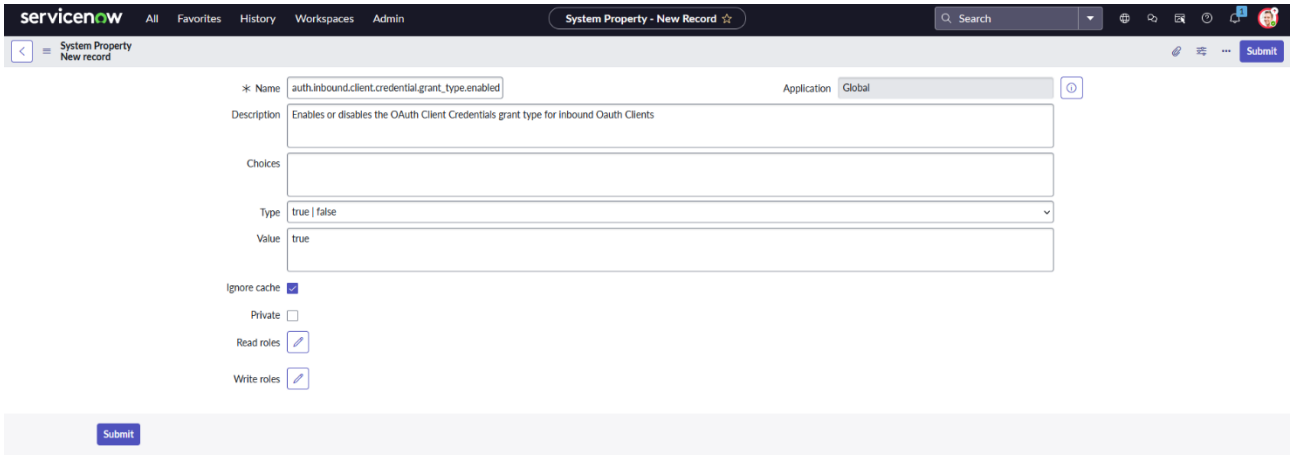
Each attack frame in the timeline is now enabled with the option to open a ticket directly in the Jira project:

The **"Summary"** and **"Content"** fields are automatically populated with the description of the selected attack. You can choose the project, issue type, and ticket assignee (these fields are retrieved through the Jira API). Once you click **"Send to Jira,"** the ticket will automatically appear on the ticketing platform.

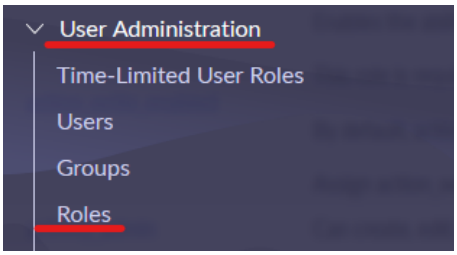


Follow these steps to integrate ZAIUX® Evo with ServiceNow:

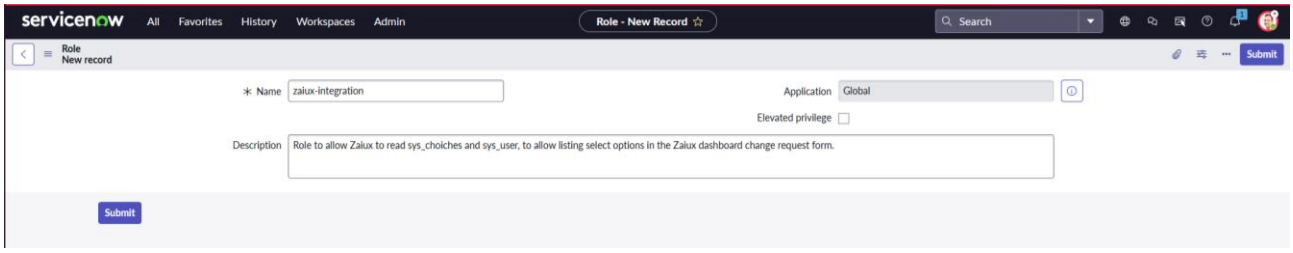
1. Enable the "**client credentials**" grant type, by creating a new Boolean system property inside the "**sys_properties**" table. The name should be "glide.oauth.inbound.client.credential.grant_type.enabled", and the value "**true**".



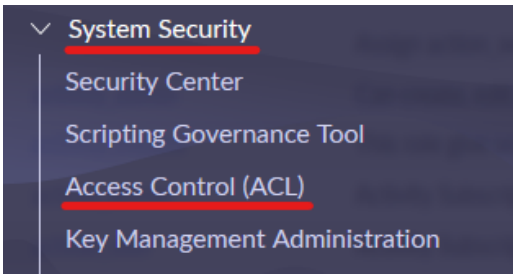
2. Create a new role to allow the Zaiux® EVO integration to read from the specific tables. In the "User Administration" menu, go into the "Roles" section.



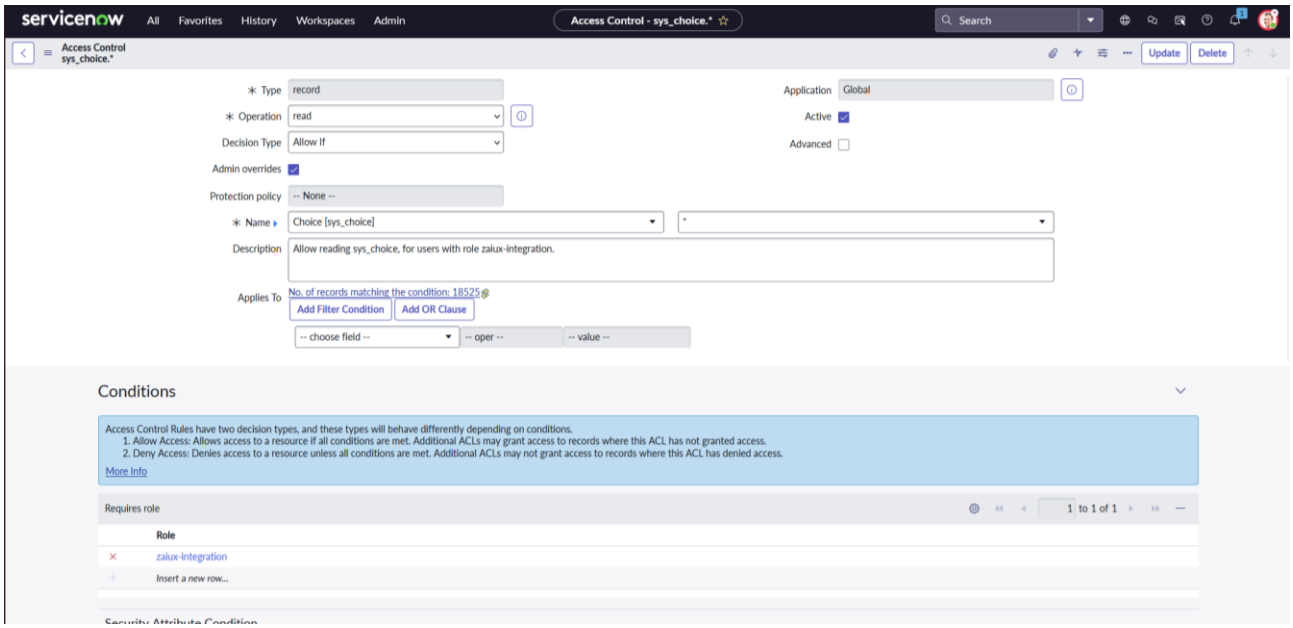
Now, create a new role for the integration. In this example we named it "zaiux-integration"



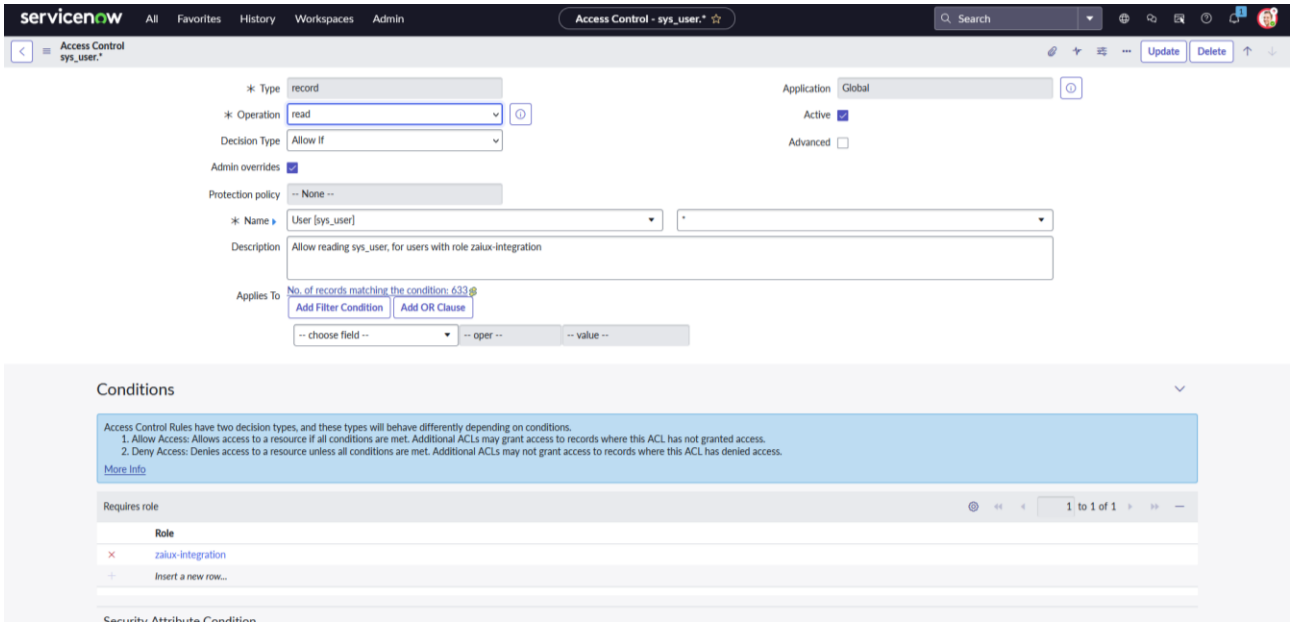
3. Create ACLs rules to allow the newly created role to read from the table "**sys_user**" and "**sys_choice**". From the "**System Security**", open the "**Access Control (ACL)**".



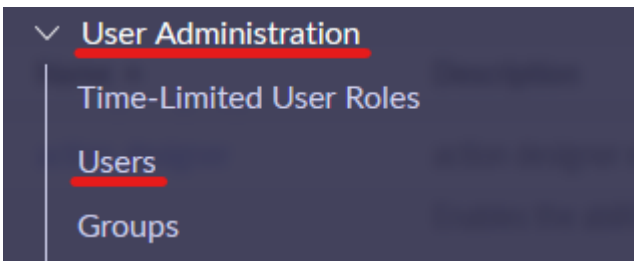
Create the first ACL rule to allow the newly created role to read all the fields in the "**sys_choice**" table:

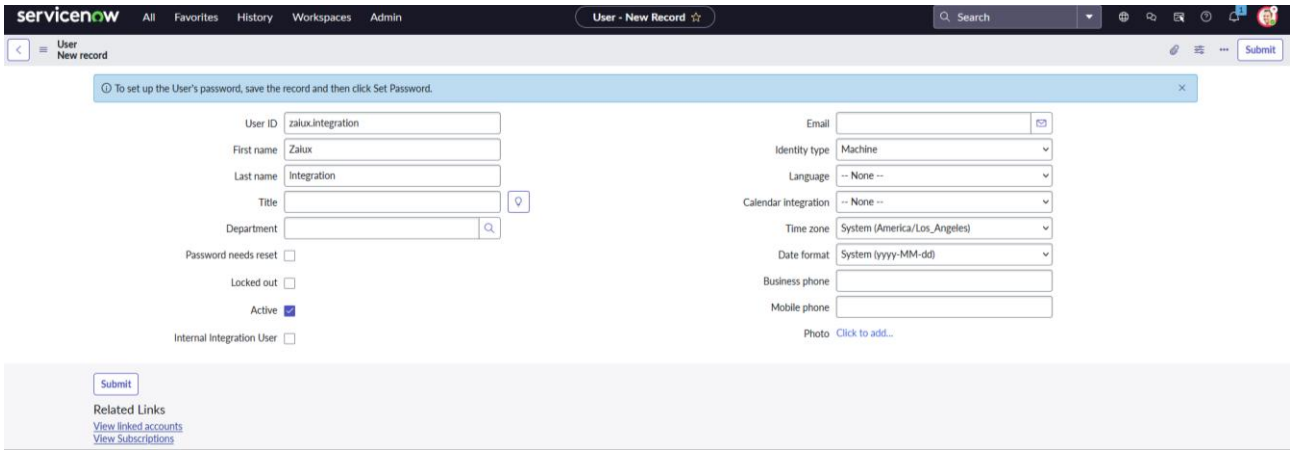


And the second one to allow reading from the "**sys_users**" table:

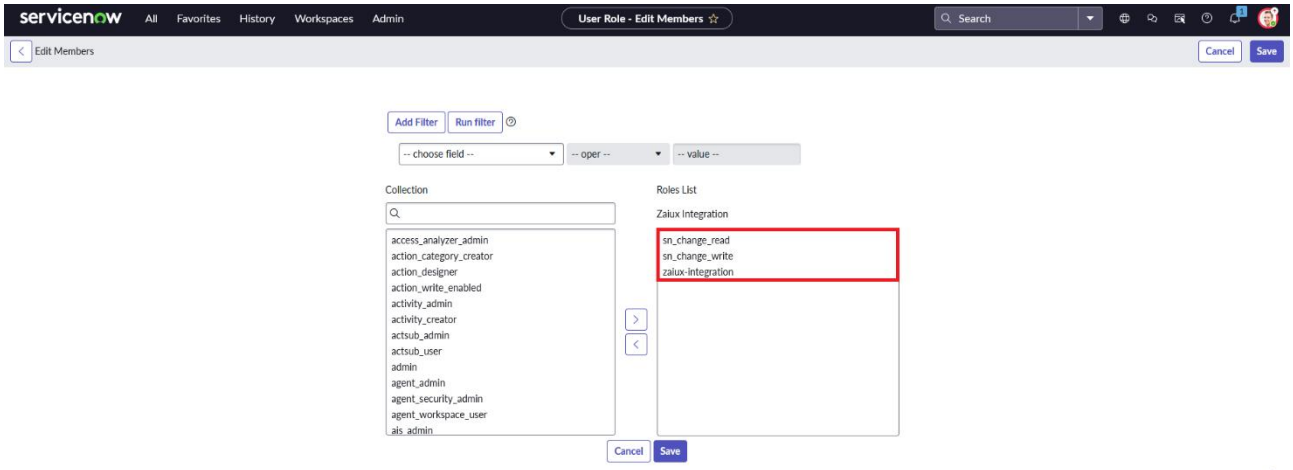


4. Create a new user for the integration to use. Open the "**User Administration**" menu and into the "**Users**" section.

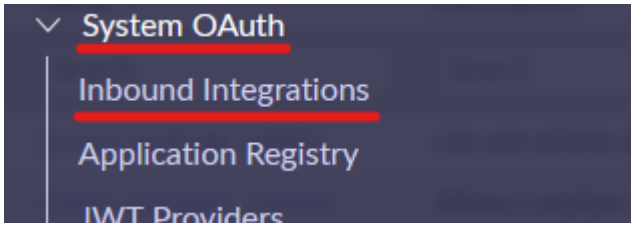


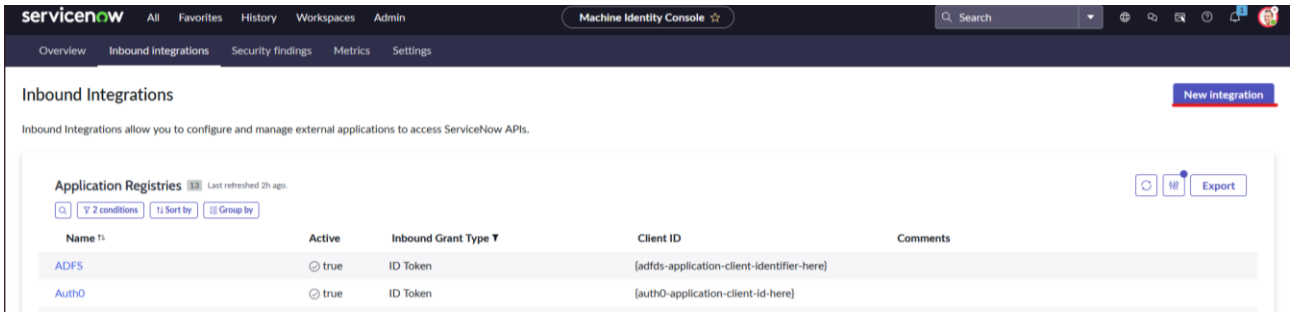


5. Associate the previously created role with the new user. Finally, add "**sn_change_read**" and "**sn_change_write**" to the roles list.

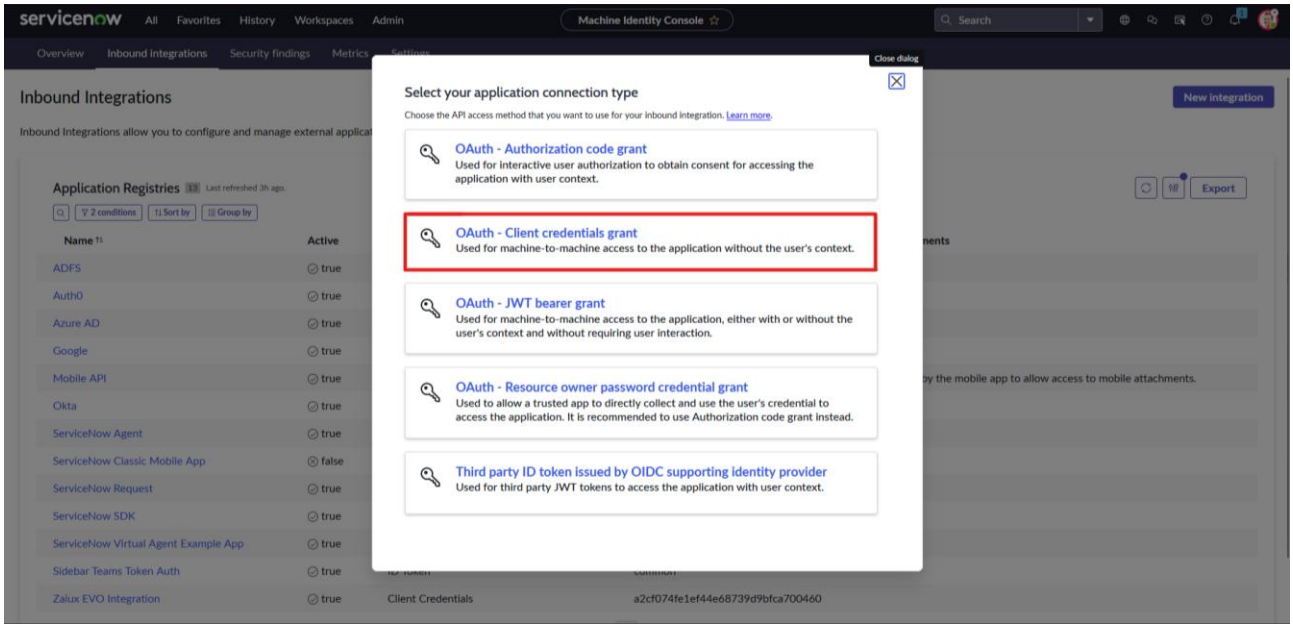


6. Create a new OAuth integration. Open the "**System OAuth**" menu and go into the "**Inbound Integrations**" section.

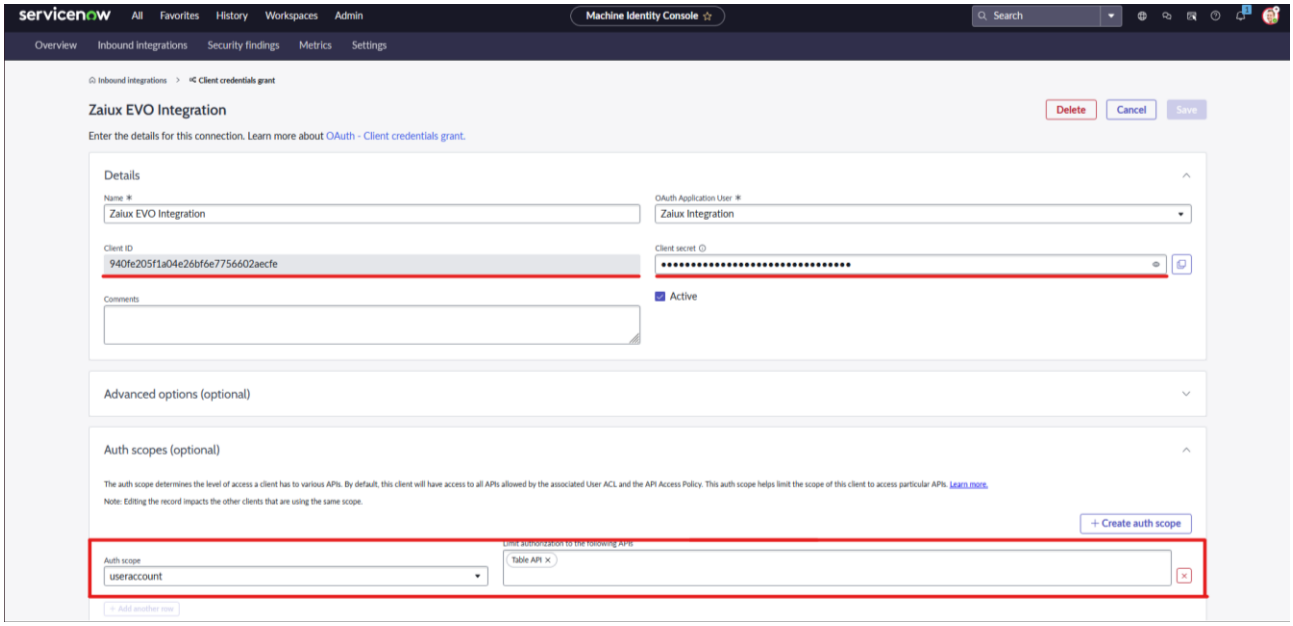


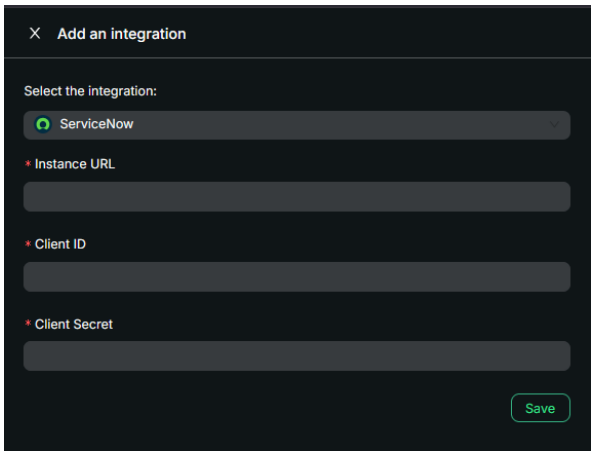


Choose "**OAuth – Client Credentials grant**":



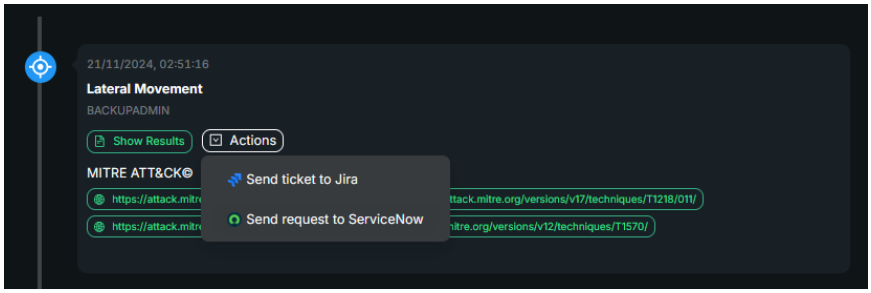
When creating the new credential, associate the ZAIUX® Evo integration account to the credential using the "**OAuth application user**" field.
Be sure to create a new "**Auth Scope**" named "**useraccount**" and limit the access to the "**Table API**".



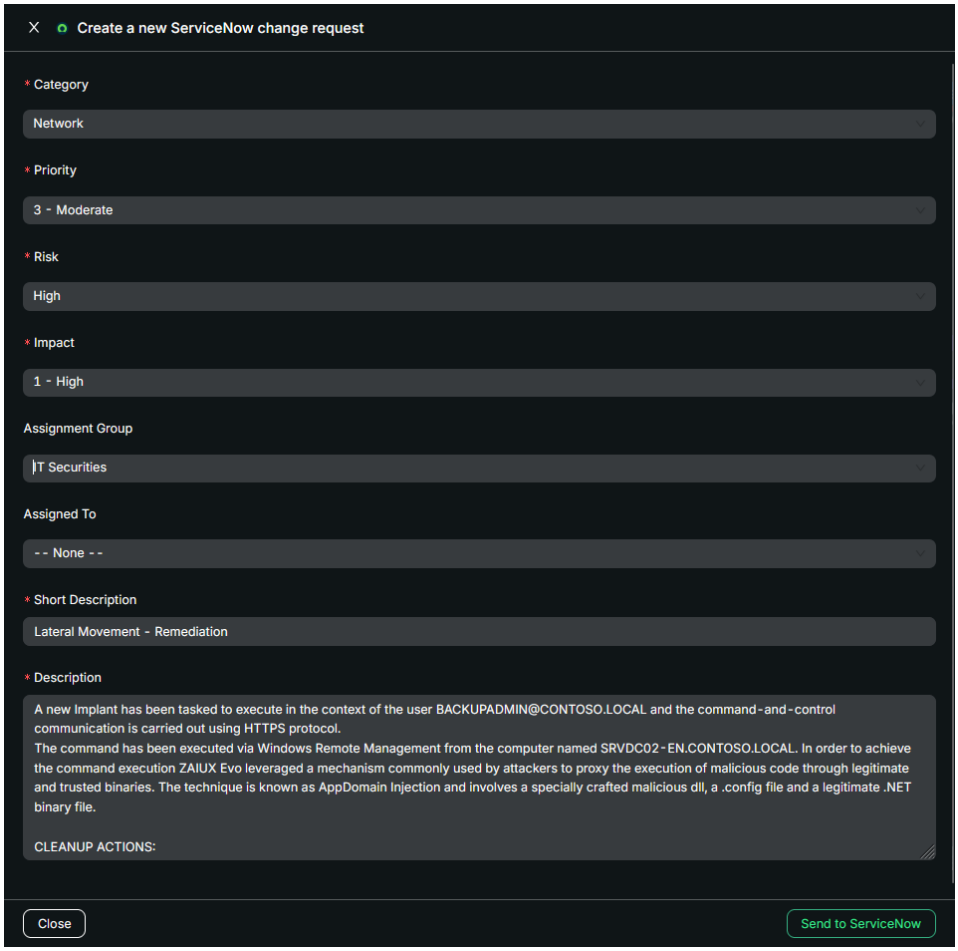


Finally, take note of the **Client ID** and **Client Secret** to configure the integration in the ZAIUX® Evo dashboard.

Once this step is completed, you will be able to open a request in ServiceNow for each evidence highlighted by the Breach & Attack Simulation.



As shown in the Jira integration, the user can select multiple parameters to streamline the risk management process and reduce communication time between teams.



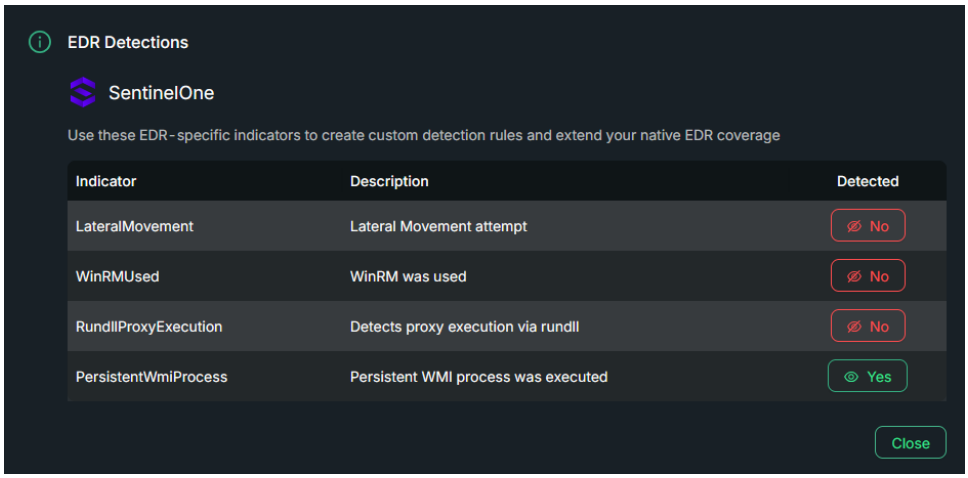
Closing Gaps in Endpoint Detection with Breach & Attack Simulation

When an EDR is configured, ZAIUX® Evo can fetch events and alerts generated by BAS activity from your endpoint security console. It then correlates these events with the actions performed by the Breach & Attack Simulation, enabling evaluation of the EDR/XDR coverage against modern attacks. This information is available to users through both the web interface and generated reports.

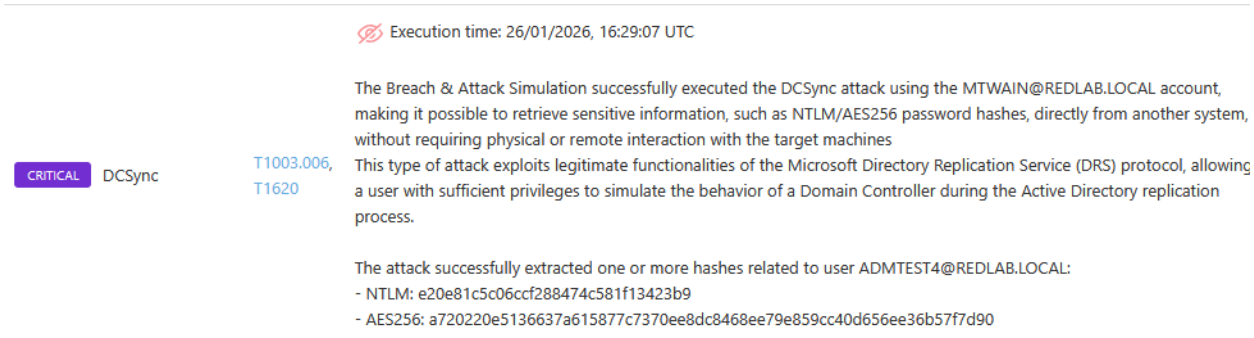
Example:

The **Lateral Movement** has been marked as "*Detected*".

Upon clicking the button, more information is provided about which detectors were triggered and which were not. By analyzing the specific indicators, it becomes possible to detect and block attempts to exploit the same attack path using slightly different techniques that might bypass normal detection.



The report indicates whether each technique was detected or went unseen. In the example below, an Undetected DcSync is shown:

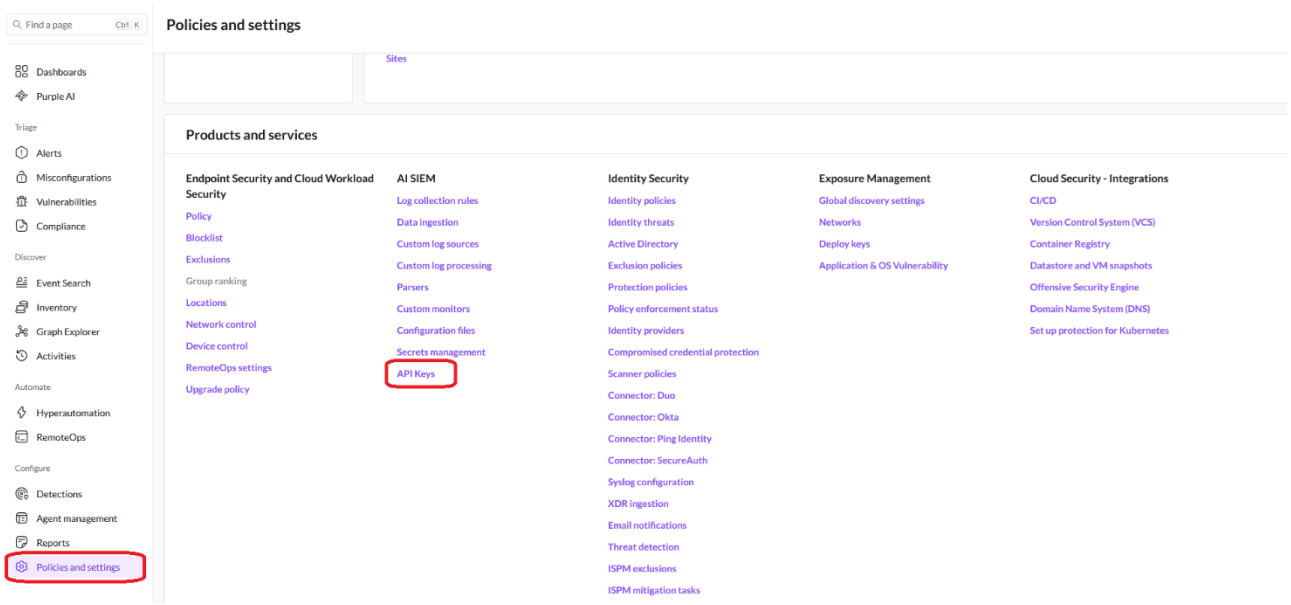


Integrating SentinelOne AI SIEM

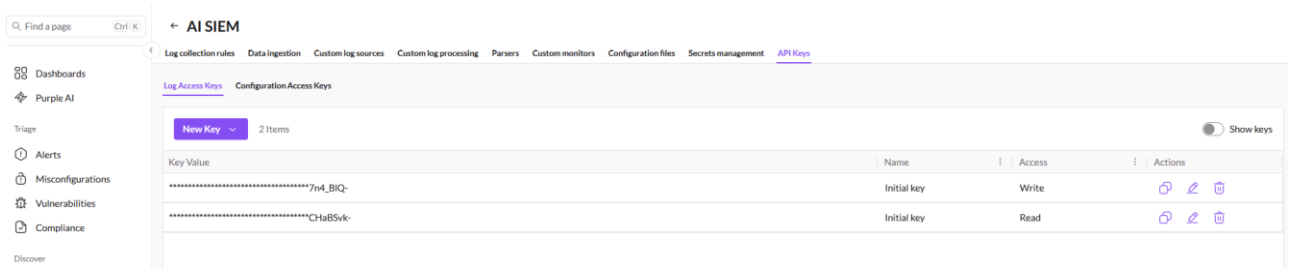
ZAIUX® Evo integrates with SentinelOne AI SIEM to enable tighter collaboration between Breach & Attack Simulation and defensive technologies. This integration provides deeper visibility into simulated attack activity, making it possible to extend the native EDR coverage and create custom detection rules that enhance endpoint protection.

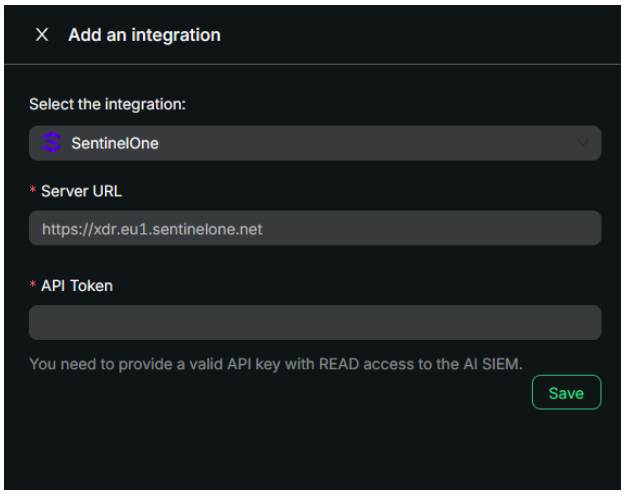
Follow the steps below to connect ZAIUX® Evo to your SentinelOne console.

1. From the navigation menu, select **Policies and settings**, then click **API Keys** under the **AI SIEM** section.



2) Create a new API key with **READ** privileges or copy the pre-generated key.





3. In ZAIUX® Evo, navigate to the **Integrations** section for the desired **Site** and enter the SentinelOne server address and API key.

4. Click **Save**. The system will automatically validate the information provided. If the verification is successful, the SentinelOne integration widget will appear on the **Integrations** page.

Integrating Microsoft Defender for Endpoint

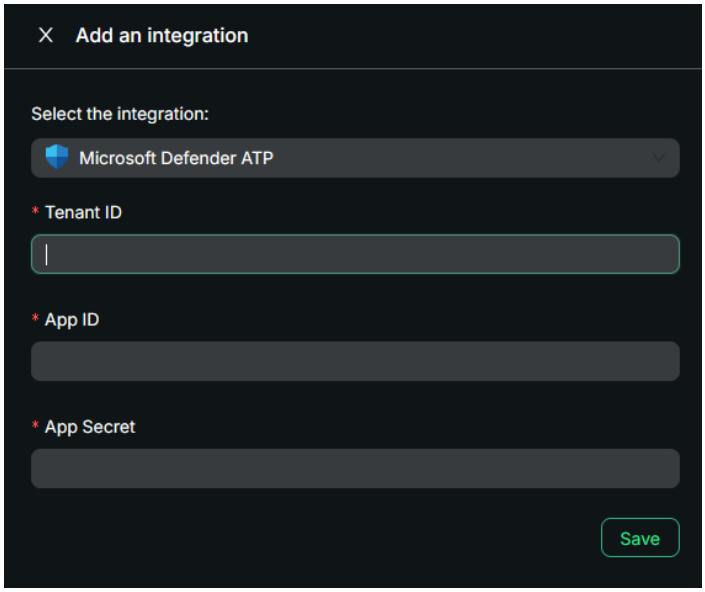
ZAIUX® Evo integrates with Microsoft Defender for Endpoint to enable tighter collaboration between Breach & Attack Simulation and defensive technologies. This integration provides deeper visibility into simulated attack activity, making it possible to extend the native EDR coverage and create custom detection rules that enhance endpoint protection.

Follow the steps below to connect ZAIUX® Evo to your Microsoft Defender for Endpoint console.

1. Register a new Application in your ENTRA ID Tenant. If you are unsure how to create one, follow the instructions provided here: https://learn.microsoft.com/en-us/defender-endpoint/api/exposed-apis-create-app-nativeapp

When creating the application, grant the following API permissions: **Alert.Read.All, Machine.Read.All** take note of your APP Secret.

3. Generate an application secret and take note of its value, as it will be required later. Take note of the Tenant ID and Application (Client) ID, which are visible in the application Overview page. These values are required to configure the integration on the ZAIUX® Evo side.



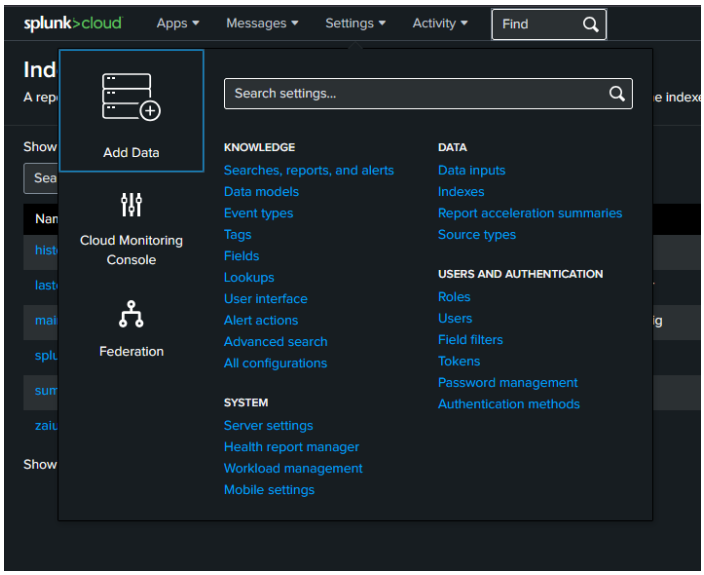
3. In ZAIUX® Evo, navigate to the **Integrations** section for the desired **Site** and enter your Tenant ID, App ID and App Secret..

4. Click **Save**. The system will automatically validate the information provided. If the verification is successful, the Microsoft Defender for Endpoint integration widget will appear on the **Integrations** page.

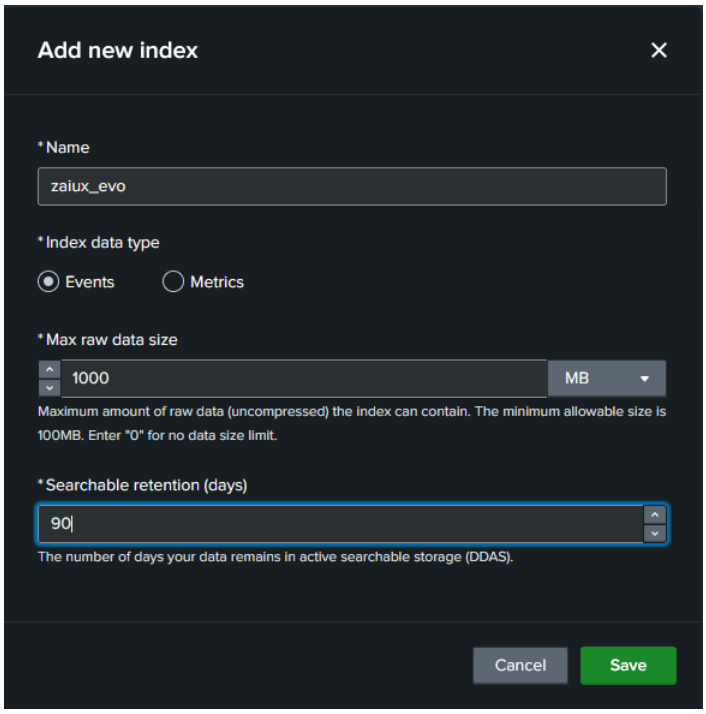
Integrating Splunk for event forwarding

ZAIUX® Evo integrates with Splunk through a dedicated forwarding plugin that streams all Breach & Attack Simulation (BAS) data directly into a dedicated Splunk index.
This integration enables security teams to centralize BAS telemetry within their existing Splunk environment, where it can be searched, correlated, and analyzed alongside logs from endpoints, network devices, and other data sources. By continuously forwarding detailed execution data, including techniques, timestamps, TTPs, and other contextual metadata, ZAIUX® Evo enhances visibility into validation activities and detection coverage.

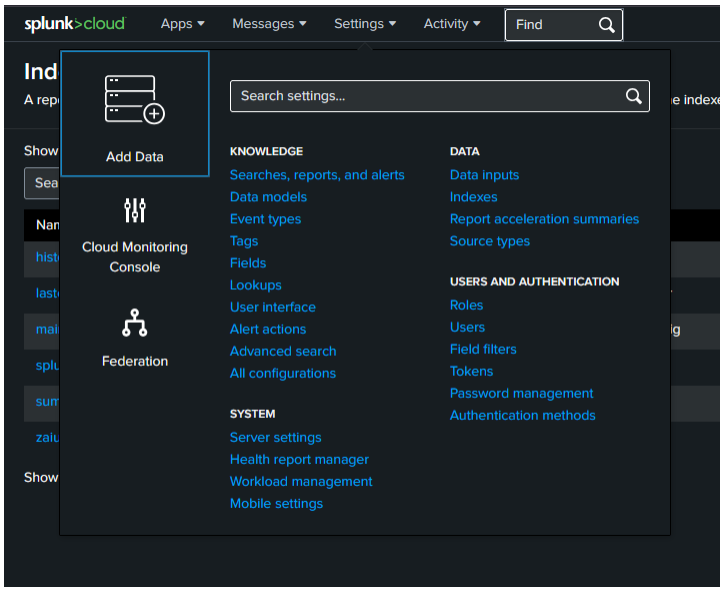
Follow the steps below to connect ZAIUX® Evo to your Splunk console.



1. From the navigation menu, go to **Settings** and select **Indexes**. This section allows you to manage data storage and create a dedicated index for the events generated by the Breach & Attack Simulation.

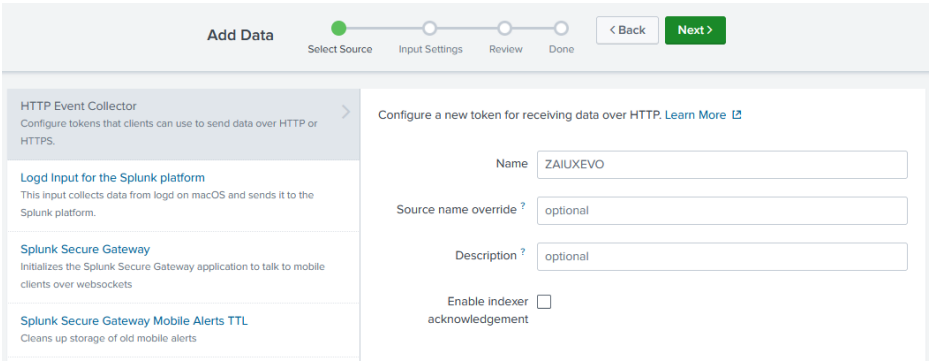


2. Click **New Index** and define a name for the index that will store BAS events. Configure the maximum data size and data retention period according to your requirements.

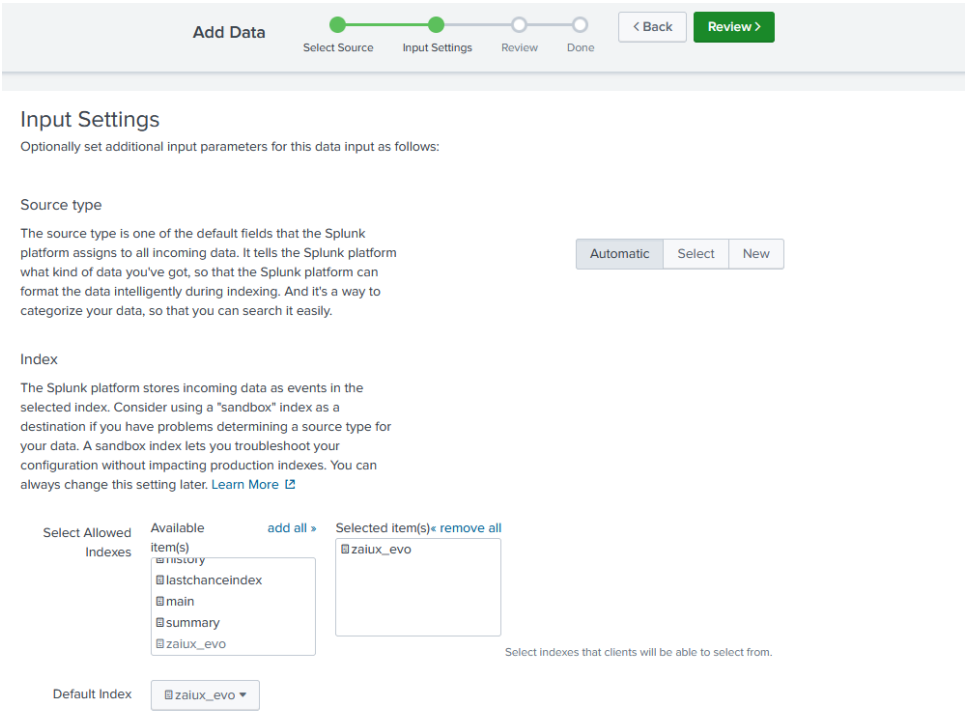


3. From the navigation menu, go to **Settings** and select **Data Inputs**. As a final step, create a new **HTTP Event Collector** (**HEC**). This component enables ZAIUX® Evo to securely stream BAS event data directly into the previously created Splunk index.

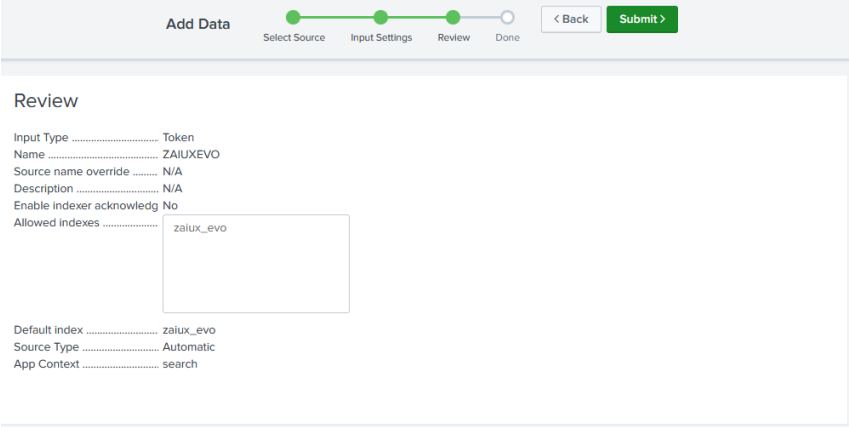
4. Select a name for the HTTP Event Collector (HEC) and go to the next step:



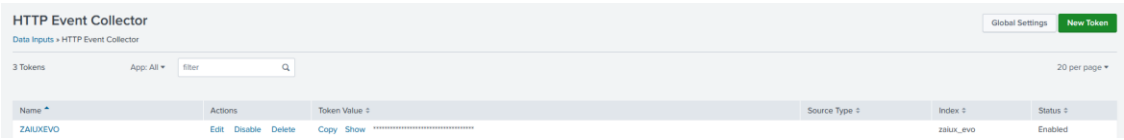
5. Select the previously created index to store the incoming data:

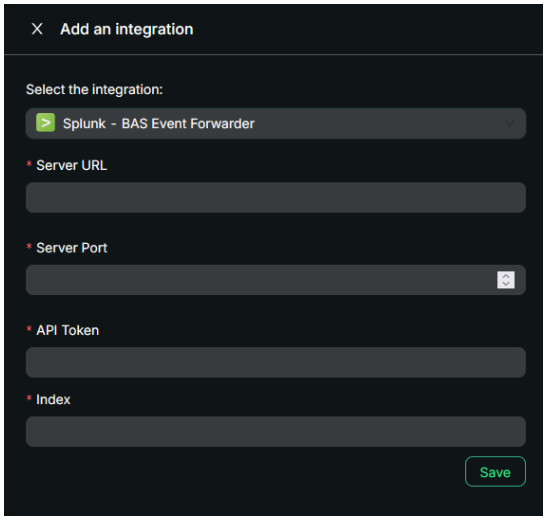


6. Review the new Data Input configuration and submit it:



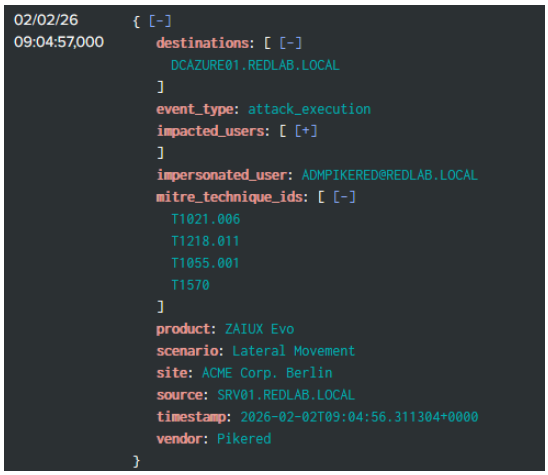
7. Copy the generated Token value to use in the ZAIUX® Evo interface:





8. In the ZAIUX® Evo plugin, provide the following information:

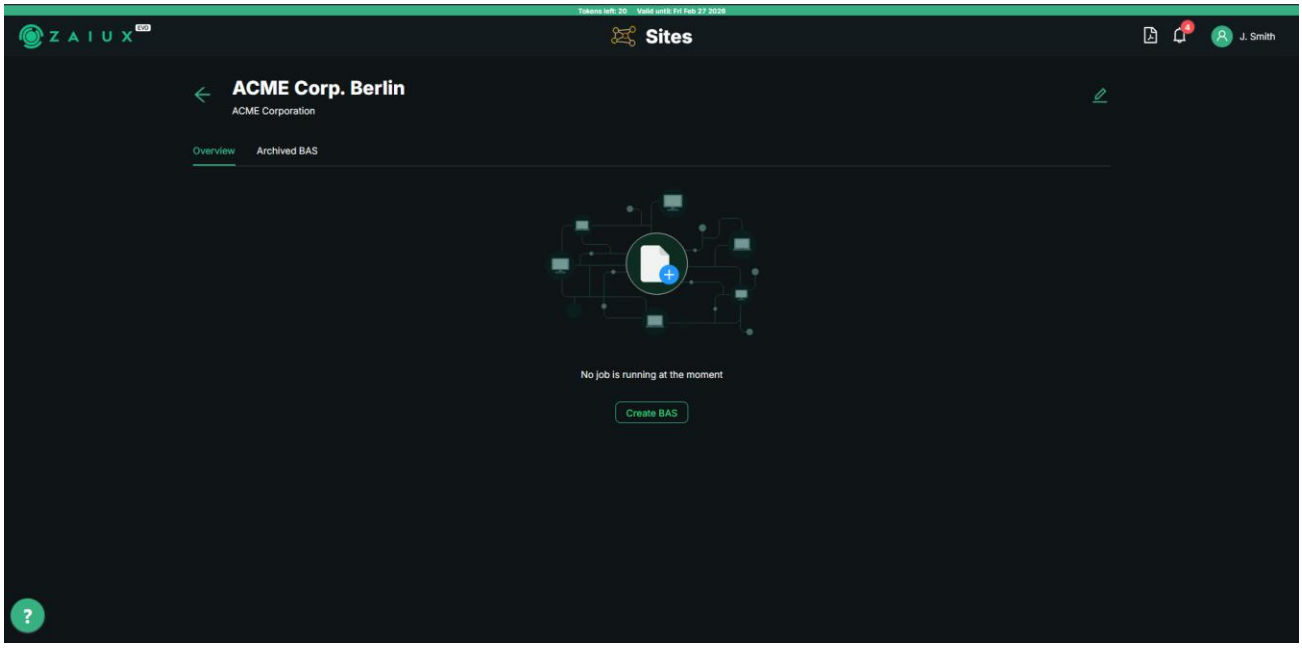
- Server URL
- Server Port (default HEC port: 8088)
- API Token
- Index name created in the previous steps



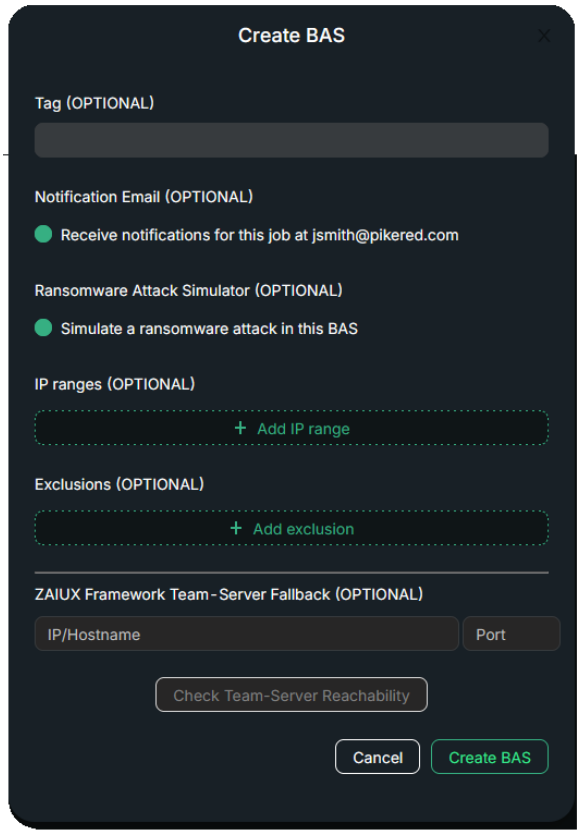
9. Once configured, all actions from the next Breach & Attack Simulation run on this site will be forwarded to the Splunk server, providing detailed context for each technique executed by ZAIUX® Evo.

How to create a BAS with ZAIUX® Evo

After creating a site, it can be opened, presenting the user with a page similar to the following:



The **Create BAS** button opens the window shown below. As all fields are optional the user can click **Create BAS** immediately. Below is a brief description of each field:



- Optional label to assign to this BAS for future reference.
- **Notification Email:** ZAIUX® Evo will notify the BAS creator about completion, fatal errors, or additional guidance during the simulation.
- **Ransomware Attack Simulation:** Option to disable the ransomware simulation. More details are available in the related section.
- **IP Ranges (*):** Define internal IP ranges to limit the scope of the Breach & Attack Simulation.
- **Exclusions (*):** Exclude specific IP addresses from the simulation.
- **ZAIUX Framework Team-Server Fallback**: If a valid ZAIUX Framework license is purchased, the two solutions can be integrated to combine automated testing with human expertise for optimal results.

(*) Domain Controllers are always included in the scope, even if manually excluded.

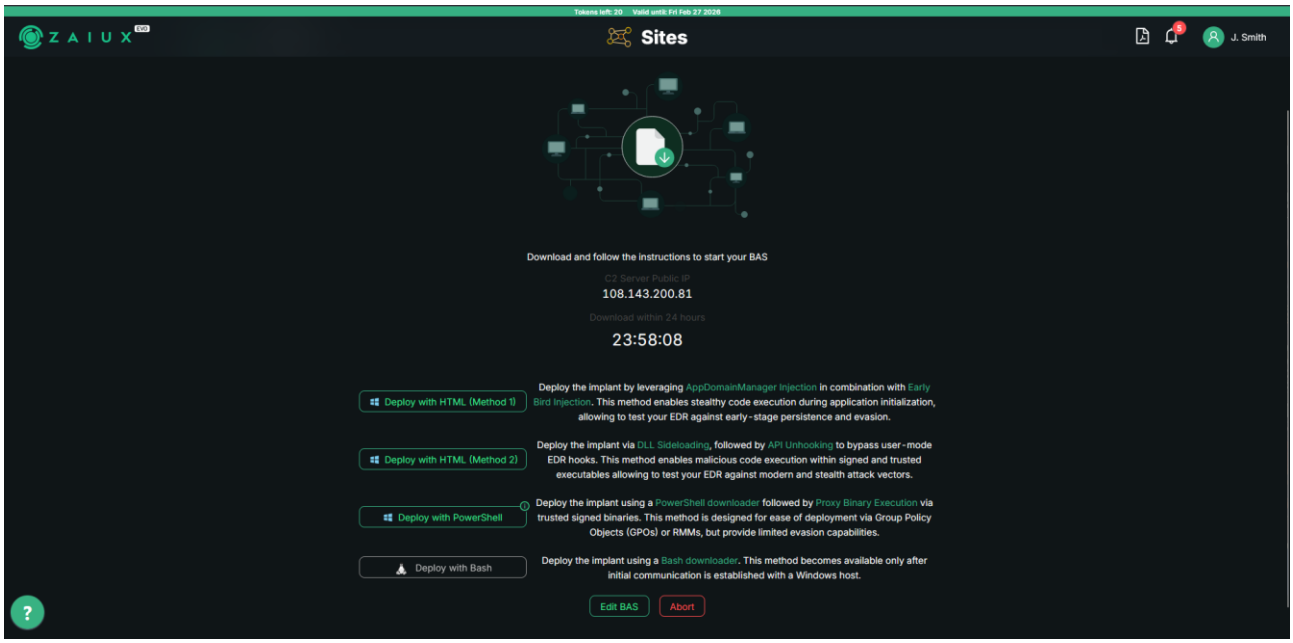
Once the user confirms the BAS configuration, they can click **Create BAS**. A few moments are required to deploy the Breach & Attack Simulation environment, which runs in a secure and isolated sandbox. From this point, the user has 24 hours to launch the simulation. Refer to the next section for instructions about how to properly start the simulation. Clicking **Abort** at this stage results in token reassignment.

Note on defining exclusions

Although these fields are available, we recommend minimizing the use of exclusions. ZAIUX® Evo does not target legacy or end-of-life operating systems, and all techniques are designed to avoid disruption or service crashes. Limiting the assessment scope may reduce the quality and completeness of the outcomes.

Deployment methods

ZAIUX® Evo offers users three distinct methods for deploying the **Implant** on Windows operating systems and a dedicated method for Linux-based operating systems.
What is an **Implant**? The *"Implant"* is a piece of executable code, technically known as shellcode, developed by PIKERED, that emulates real malwares to deliver sophisticated and realistic cyber-attacks, without causing service disruption, network bottlenecks, or business impact.



1. **HTML (Method 1)**: T1574.014 and T1055.004 are chained to enable stealthy application initialization. A temporary sacrificial process is spawned to establish a connection with the ZAIUX® Evo command-and-control (C2) server. This method is intended for testing endpoint detection and response (EDR) solutions against remote process-injection techniques.
2. **HTML (Method 2)**: T1574.001and T1562.001 are chained to enable a stealthy application initialization. The starting process itself establishes a connection with the ZAIUX® Evo command-and-control (C2) server. This method is intended for testing endpoint detection and response (EDR) solutions against DLL side-loading and API-unhooking techniques.

Before you open the HTML (1 and 2)

- After downloading and moving the HTML file to the chosen entry point(s), open it in a web browser. An .ISO will be downloaded to the default Downloads folder. Mount the ISO (double-click or right-click > Mount); a mapped drive will be created and its folder opened. Launch the BAS by double-clicking **Start_x64.exe**.
- Refer to the instructions inside the HTML file for the complete procedure as the ISO file might be flagged by MOTW (Mark-of-the-Web) and therefore being blocked.
- Prefer delivering the HTML file to Entry-Point using a remote assistance system. Avoid e-mail attachments which could be marked as suspicious by an anti-phishing system.
- These are the most suitable deployment methodologies, as in most cases they guarantee greater stealthiness.
- A video demonstration is available here.

3. **PowerShell command:** a dynamic-link library (DLL) is downloaded to C:\Temp (the folder is created if it doesn't exist) and executed via the built-in rundll32.exe. This method is intended for use with remote management (RMM) tools on selected hosts, or at scale, if necessary, to silently deploy ZAIUX® Evo.
4. **Bash Command**: designed for deploying the implant on Linux systems using a sequence of concatenated Bash commands. The technique leverages the shell to perform a fast, automated deployment and includes an automatic cleanup step to minimize persistent traces.
   Note: the first implant must be executed on a Windows host; consequently, the Linux deployment option is initially disabled in the user interface.

If all deployment methods are blocked

While realism is a core goal of ZAIUX® Evo, we recognize that evading every EDR or defensive control isn't always possible. For this reason, we recommend starting with **Fail-Closed testing** (all protections active). Only after a documented, reproducible block that prevents the test objectives should a defensive control be disabled. Before doing so, verify both Deployment Method 1 and Method 2.

Selecting the entry point(s)

There is no limit to the number of entry-points you can select for a Breach & Attack Simulation of ZAIUX Evo®, provided they all belong to the same Active Directory domain. We recommend a **Least-Privilege First** approach: start with one or more nodes using standard user accounts (for example, receptionist, front-desk, or back-office users). Only, if necessary, should you add higher-privileged entry-points later, such as public-facing servers that expose services on the internet and are more likely to be targeted by cyber-criminals.

System Requirements

The ZAIUX® Evo Implant is available for both Windows and Linux operating systems. Detailed platform requirements are listed below:

- Windows (64-bit): Server 2016, Server 2019, Server 2022, Server 2025, Windows 10, Windows 11
- Linux (64-bit): Compatible with a wide range of distributions; officially supported on Ubuntu, Debian, RedHat, SUSE, Fedora, CentOS.
- Hardware Requirements: No specific minimum resources are required for RAM, CPU or storage, as the implant has a very low footprint.

Note: ZAIUX® Evo can still target outdated operating systems for enumeration purposes without deploying any Implant on them. If you want to prevent ZAIUX® Evo from interacting in any way with outdated systems, you should use the scope limitation features available during the BAS creation.

Rollback and manual-cleanup

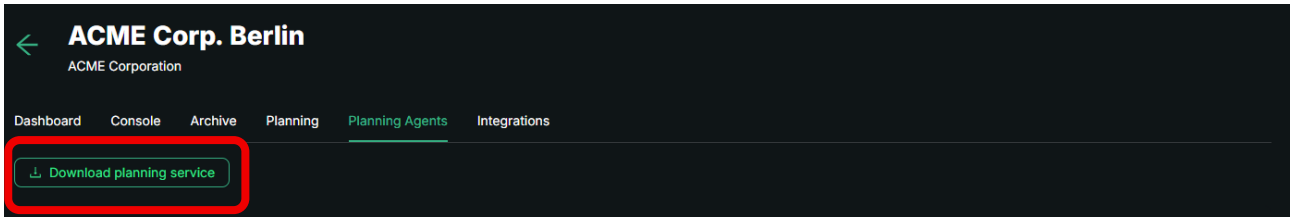
ZAIUX® Evo can revert all configuration changes and remove artifacts left on disk. However, in some cases, automatic rollback may be incomplete, and manual cleanup may be required by system administrators. The final report highlights the steps needed to remove any remaining artifacts or traces. In all cases, these leftovers pose no risk or harm to the system.
Note: After the activity is complete, remove all files used during the trigger phase (HTML, ISO, DLL) from the designated entry points.

How to plan a recurring BAS

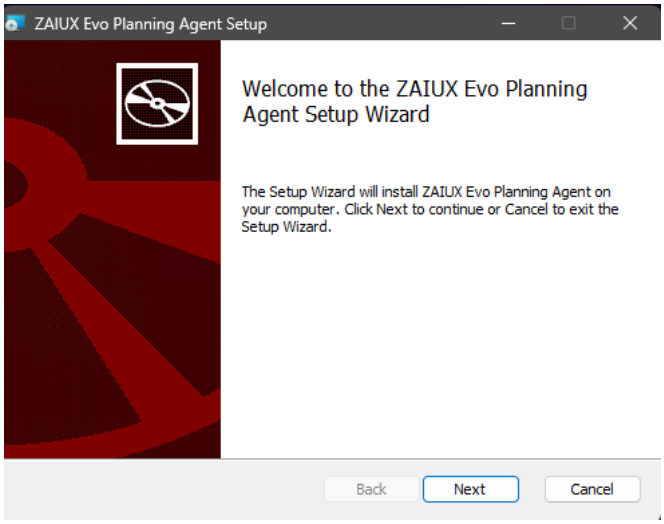
If your license includes the BAS Planner feature, you have the possibility to run recurring and fully autonomous BAS with ZAIUX® Evo. The platform allows you to plan weekly and monthly executions, at the chosen dates and times, using user-defined Windows computers in the target Site as entry points.
Performing planned BAS enables an approach oriented to continuous exposure monitoring, as opposed to ad-hoc, manually configured simulations, taking advantage of the Site Dashboard as an early warning to detect any deviation in the response to the simulated attack.

Installing the service on the entry points

From the **Planning Agents** tab, you can download the Connector by clicking the "**Download planning service**" button, as shown below:

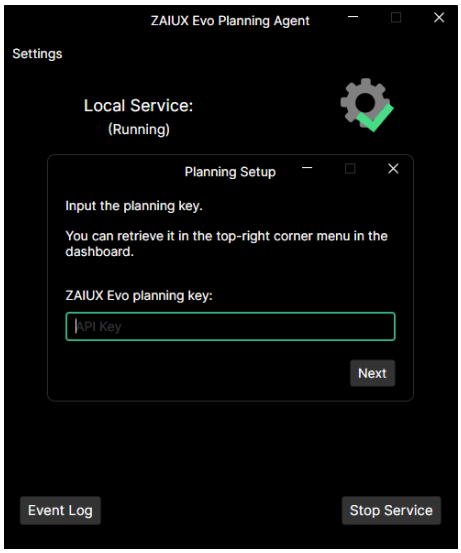


Installing the Connector requires administrative privileges on the target machines, as a new Windows Service will be installed and configured to start automatically at system boot.
The service is distributed as an MSI package and is therefore compatible with deployment via SCCM.

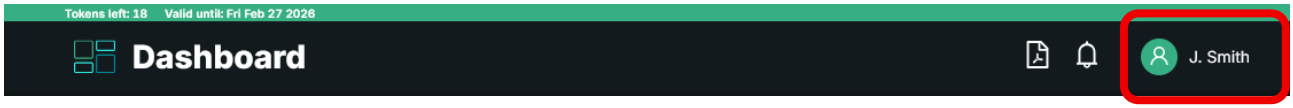


After the installation completes, a new application named "**ZAIUX Evo Planning Agent**" will appear in the Windows Start menu. This application is used to interact with the background service running on the system.

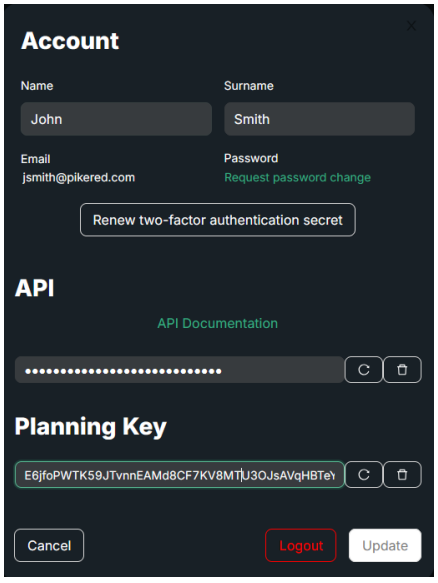
The first required step is to configure a valid planning key to establish the initial connection between the on-premises service and your tenant.



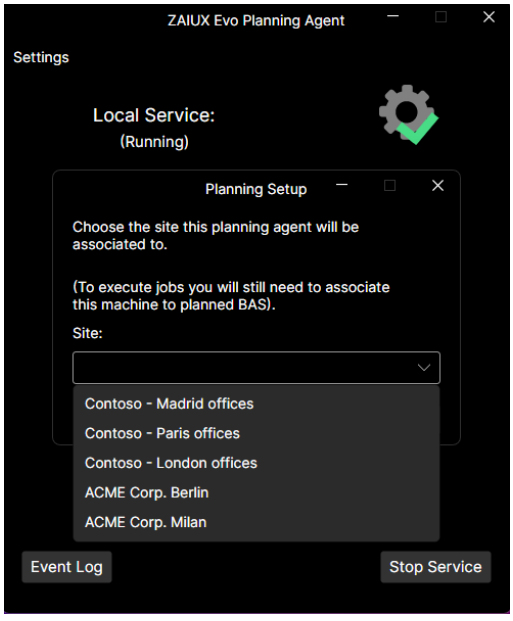
The planning key can be found in your account details, located in the top-right corner of the interface:



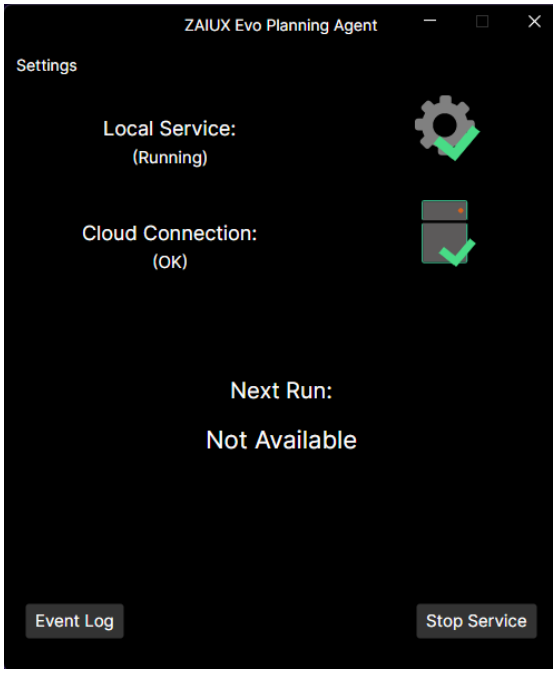
Step 1: Copy the planning key from your account page. The planning key is tenant-specific, and all users within the same tenant share the same key. A new key can be generated if required.



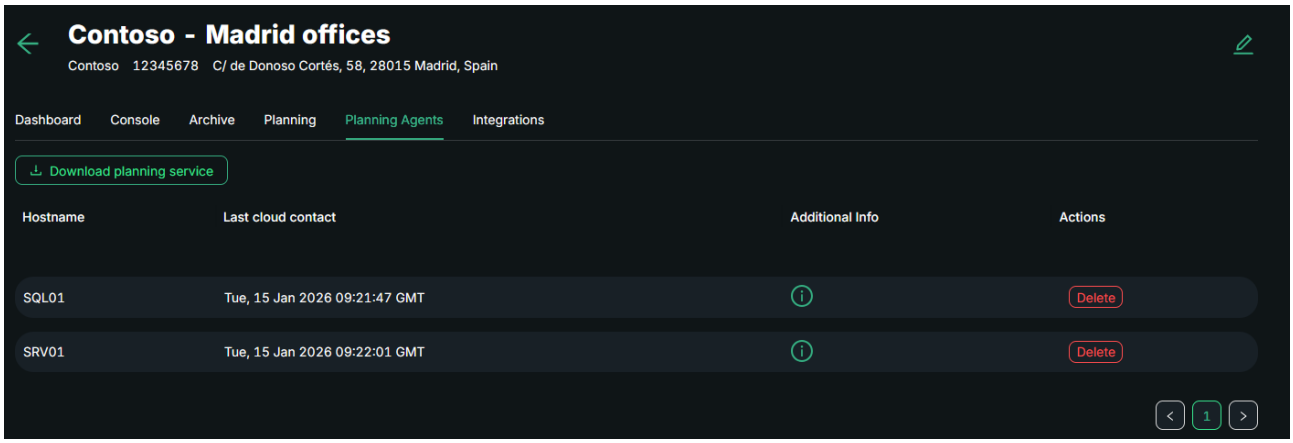
Step 2: Enter the planning key and select one of the available sites according to your requirements.



If the connection is established successfully, the application will appear as shown below:



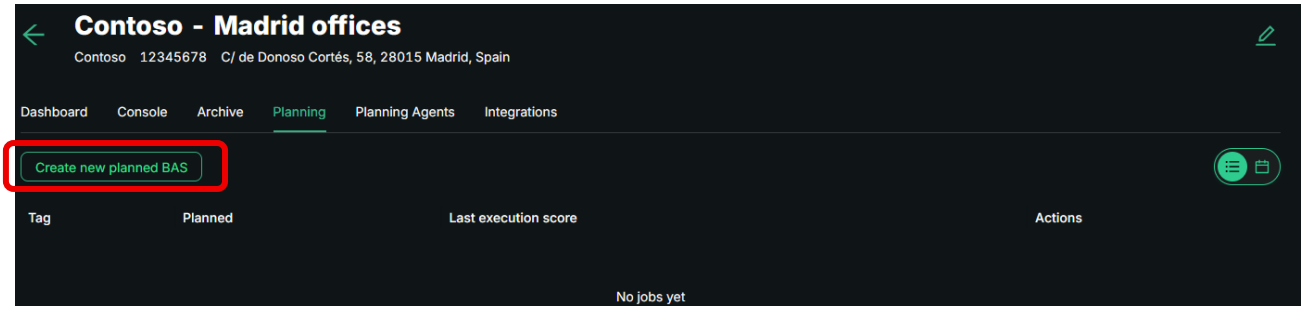
Connected services are listed in the ZAIUX® Evo user interface under the **Planning Agents** tab:

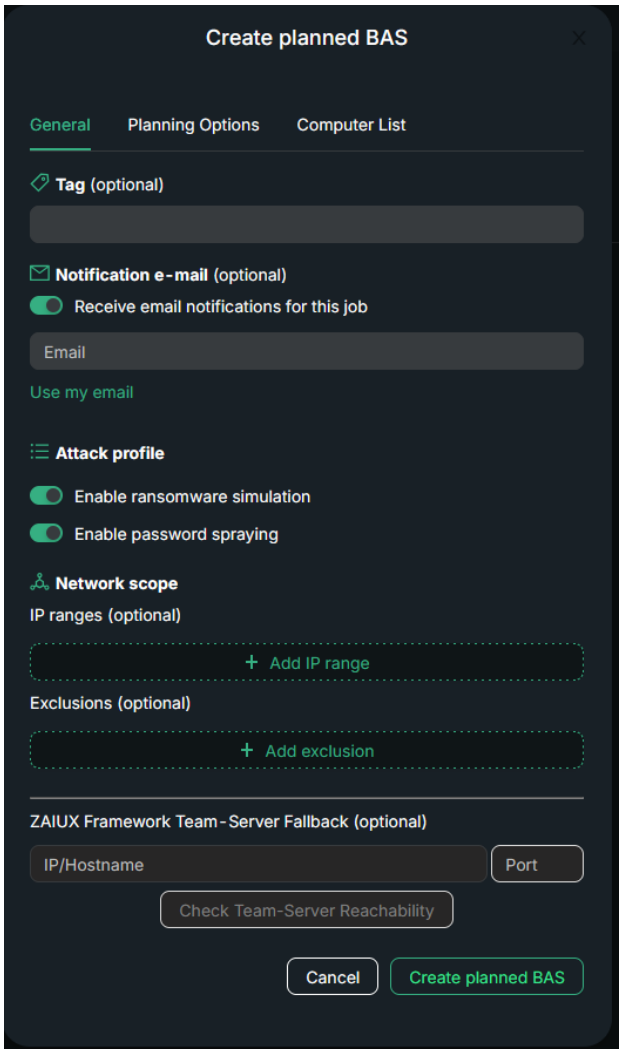


Once all required entry points have been successfully installed, the next step is to configure one or more recurring BAS scenarios.

Creating a new planned BAS

Navigate to the **Planning** tab and click **Create new planned BAS**:





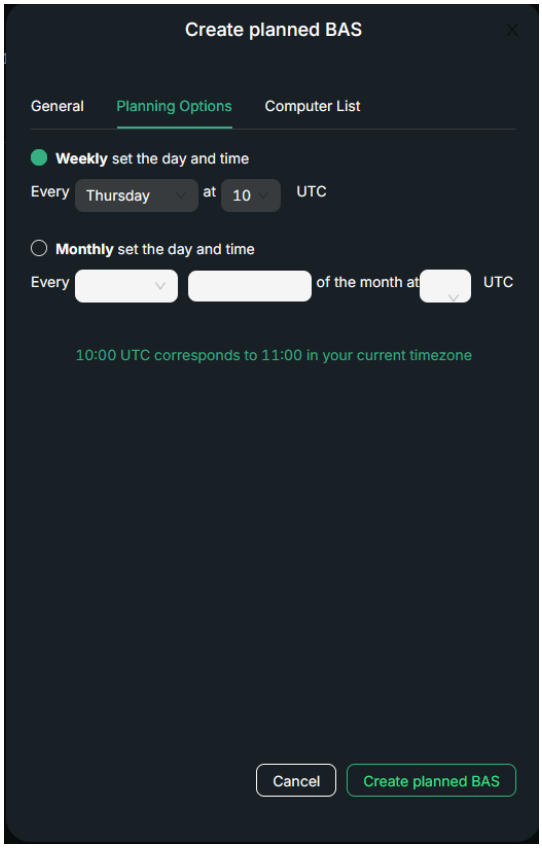
The only difference between the **General** tab and the configuration of a standard BAS is the possibility to designate a different e-mail address for notifications

Two additional tabs are available:

Planning Options: Allows you to define the schedule for the planned BAS on a weekly or monthly basis.

Computer List: Allows you to select the computers, connected through the previously installed service, from which the activity will start. Multiple computers can be defined as entry points to expand the attack surface or to test different virtual LANs simultaneously.

(Both **Planning Options** and **Computer List** will be explained in more detail on the next page.)

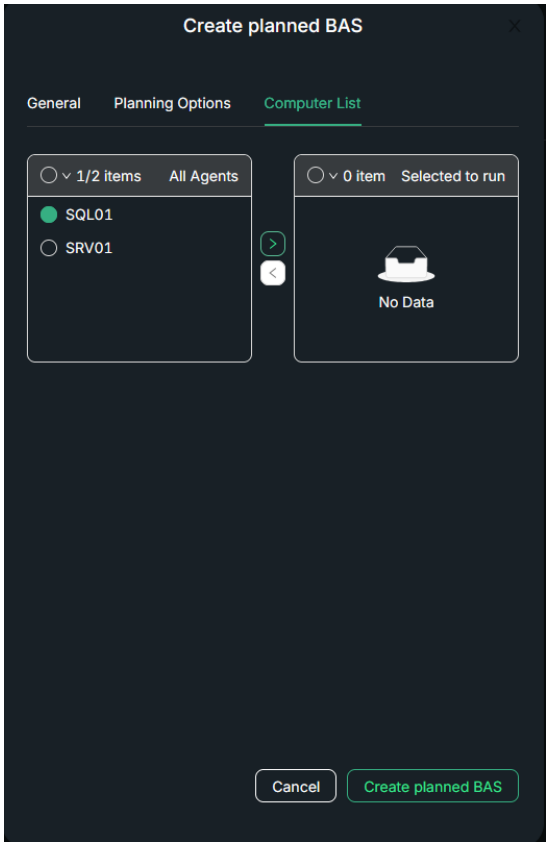


The **Planning Options** tab allows you to select a mandatory scheduling basis: weekly or monthly.

The **Weekly** option allows you to select a day (from Monday to Sunday) and a specific start time.

The **Monthly** option allows you to choose the first, second, third, or fourth occurrence of a specific day (from Monday to Sunday) within the month, along with a specific start time.

The green label at the end displays the corresponding UTC time based on your current time zone.

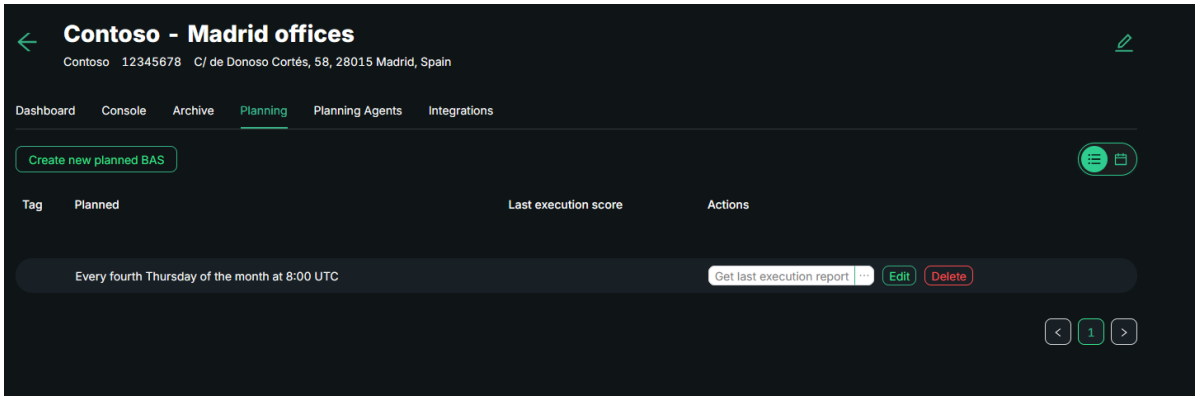


From this tab, you can select the computer from which the BAS will start.

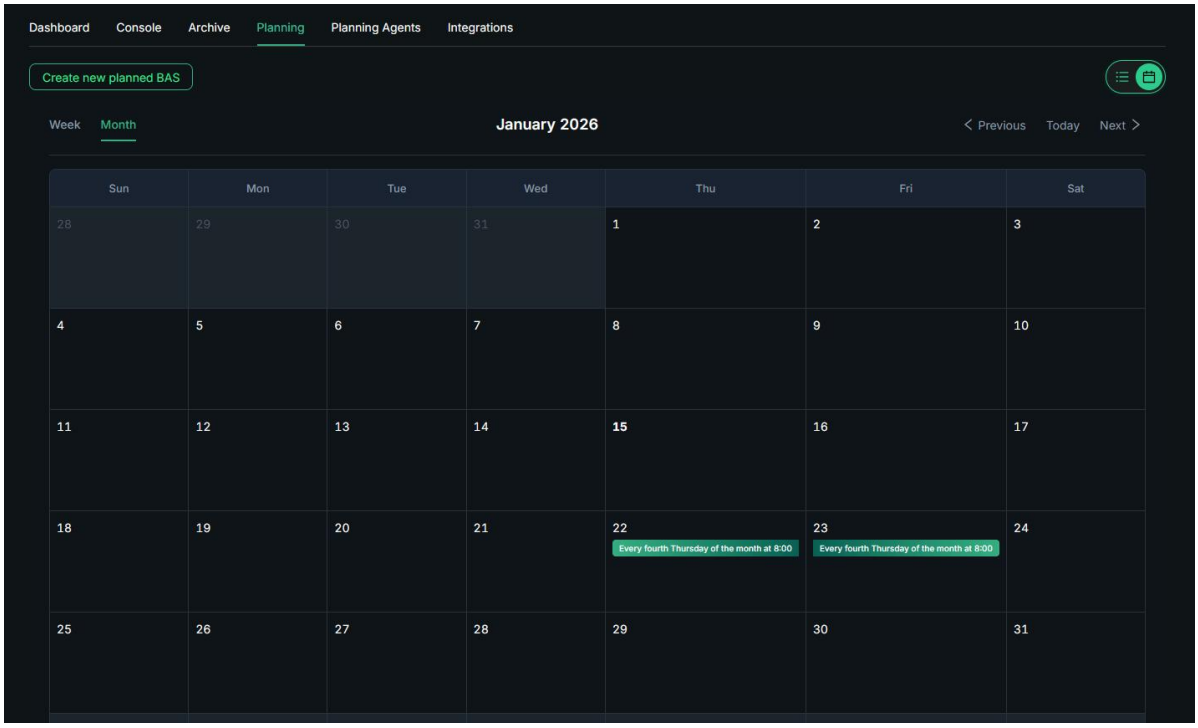
The selected computers must have the ZAIUX® Evo Planning Service installed, running, and the system must be powered on.

By selecting one or more computers and moving them to the right-hand table using the green arrow button, those computers will be enabled to execute the implant at the time specified in the **Planning Options** tab.

When everything is ready, click **Create Planned BAS** to create the schedule.



The green selector in the top-right corner allows you to switch between the tabular view and the calendar view, which displays the start and end times of all BAS schedules for the selected site (weekly or monthly view):



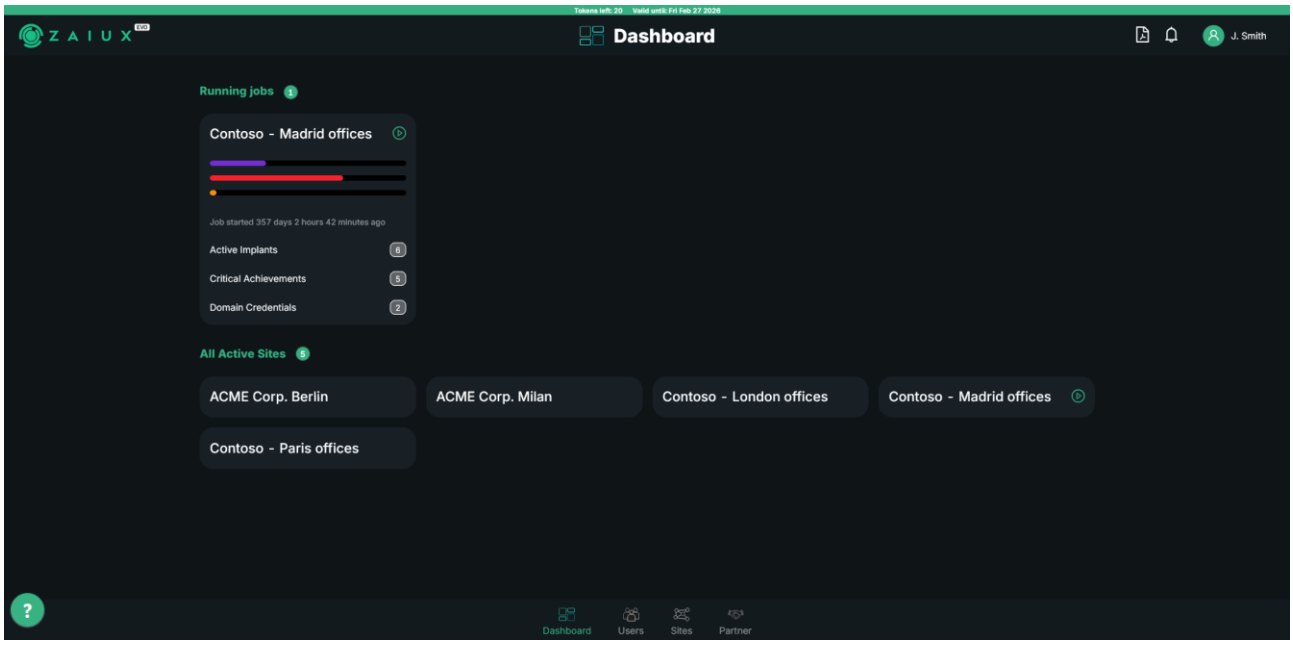
The scheduled BAS will now run automatically according to your configuration.

Important considerations for planned BAS

Only one BAS can run at a time on the same Site. If an on-demand BAS is running when a planned BAS is scheduled, the planned BAS will be postponed to the next scheduled execution.
Multiple BAS can run simultaneously on different Sites, but for FLAT licenses the total number of concurrent BAS cannot exceed the number of Domains specified during the purchase process.

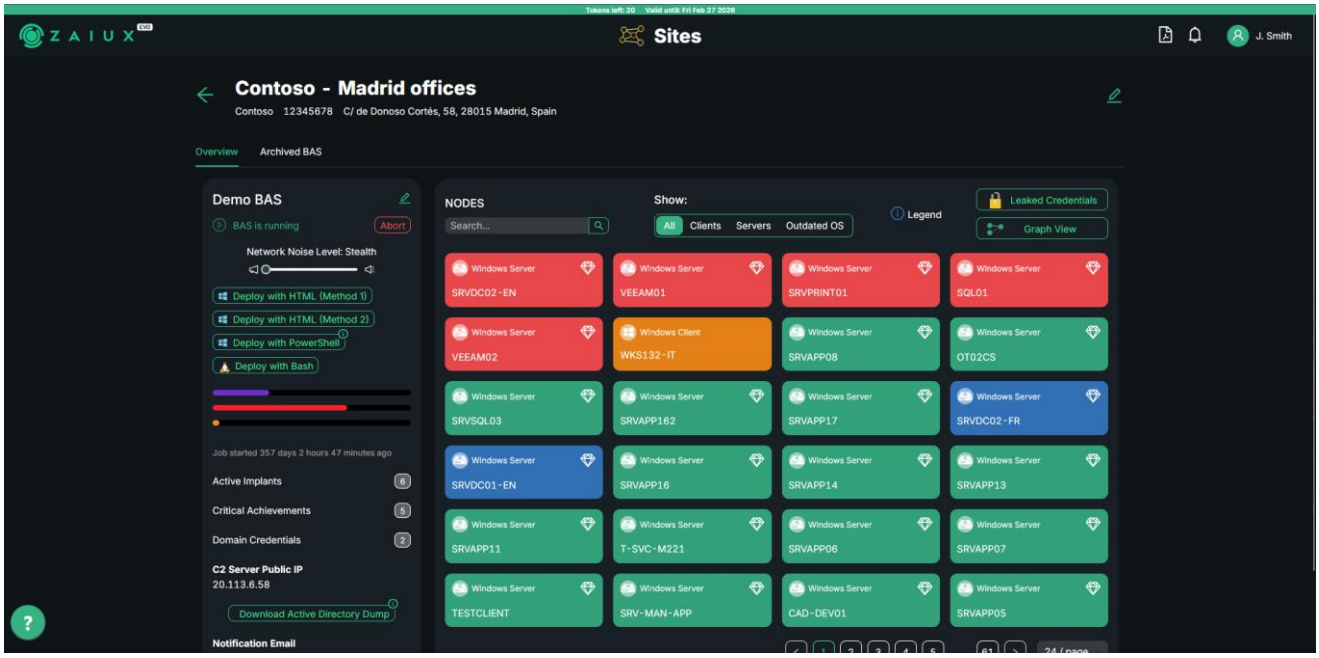
Monitoring the BAS progress

Running Breach & Attack simulations will appear in the top section of the Dashboard, under "**Running Jobs**".



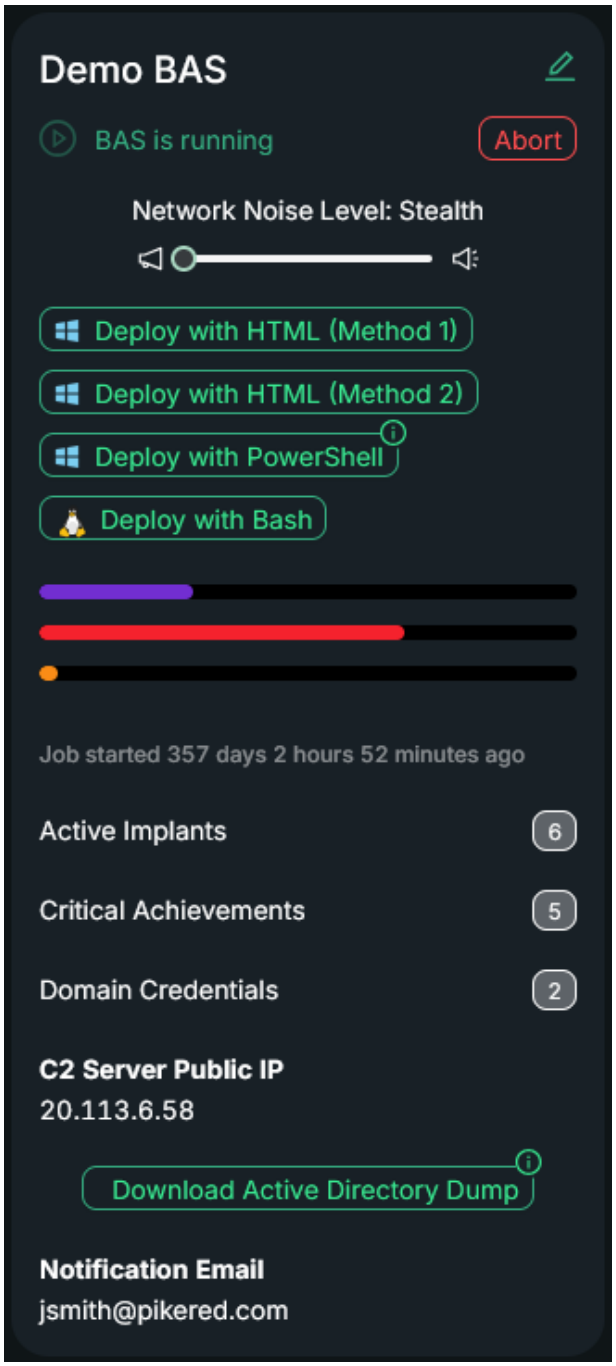
Running Breach & Attack simulations will appear in the top section of the Dashboard, under "**Running Jobs** By clicking the widget, the user can open the simulation and navigate through the findings.

<u>Here's how the BAS dashboard appears once the Active Directory enumeration phase is completed. Until that point, only the entry points are visible:</u>



Interface core components

The interface can be broken down into the following components:

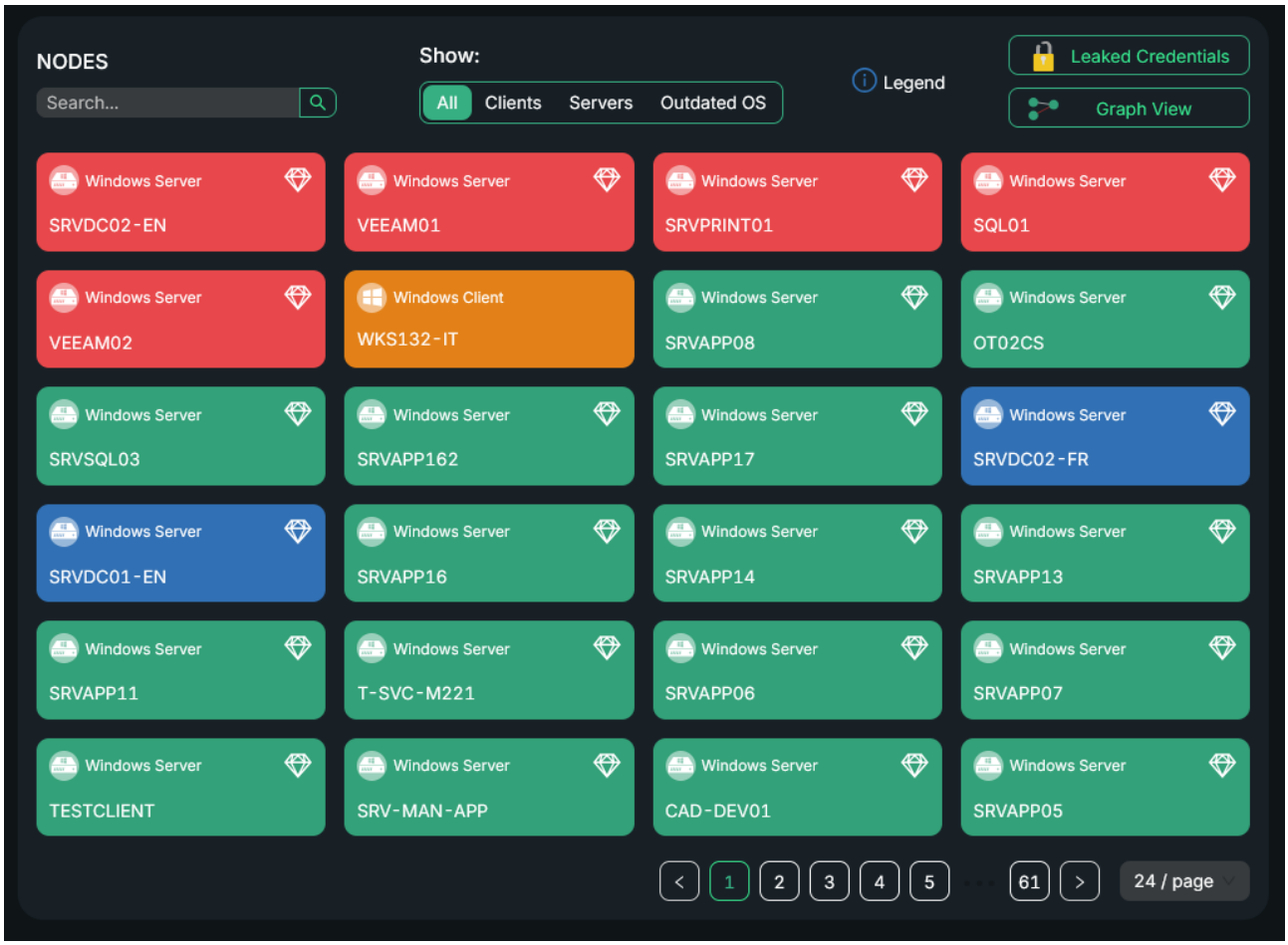


On the left are the available controls for the running BAS. The user can:

- **Abort:** Stop the BAS and retrieve results immediately without waiting for natural completion. The token will not be reassigned because the BAS is considered properly started.
- **Change Network Noise Level:** Slide the widget right to increase the Implant's C2 communication frequency to **Normal** or **Noisy**, raising the chance of detection by SOC/EDR/NDR. This setting can be adjusted multiple times during the same BAS.
- **Add more entry points:** Download the deployment methods again to select additional entry points during execution.
- **View results:** See total techniques executed (with severity), number of active implants, compromised servers, obtained credentials, and the public IP of the C2 server.
- **Download AD dump:** While the BAS is running, download the Active Directory dump for offline/manual analysis. (The dump is compatible with BloodHound)
- **Notification email:** The email address configured for notifications is displayed.

Further insights into C2 communication and how to detect such activity are available here:

- https://www.elastic.co/security-labs/identifying-beaconing-malware-using-elastic
- https://attack.mitre.org/tactics/TA0011/
- https://attack.mitre.org/techniques/T1102/002/



Color legend:

- Host detected, but neither compromised nor targeted.
- Host targeted by enumeration attacks.
- Compromised host.
- Compromised host with administrative privileges.

Other navigation features:

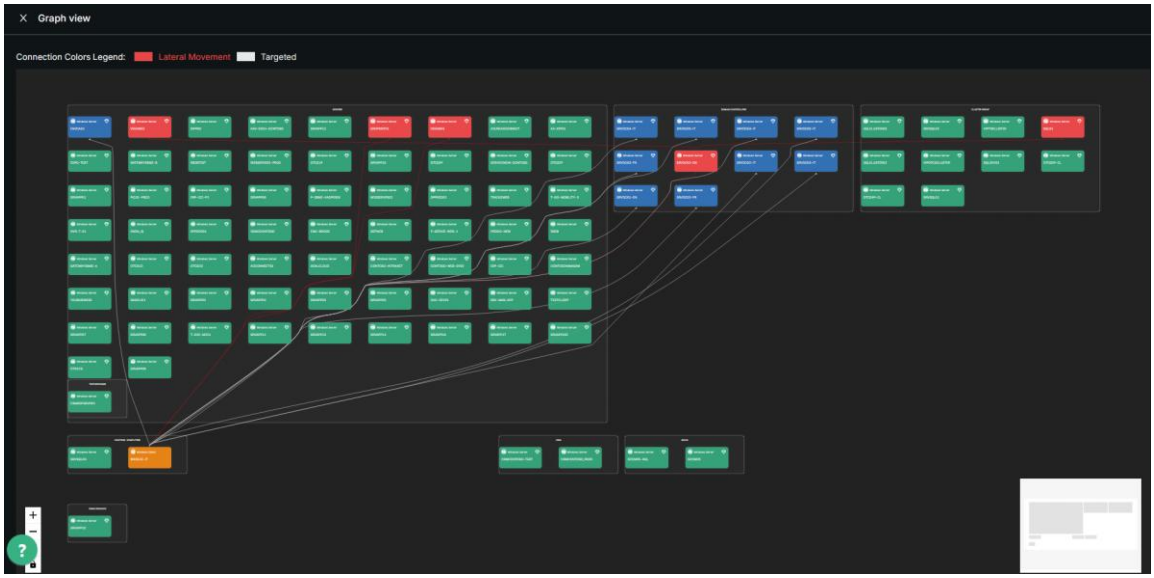
- Search bar (top-left): Find a specific node by hostname or node type.
- Filter: Display only clients, servers, or outdated operating systems.
- Pagination (bottom-right): Navigate through pages to view all hosts or adjust the number of nodes shown per page.

Leaked Credentials

ZAIUX® Evo automatically identifies the public domain associated with the organization's Entra ID tenant and queries credential-leak databases for matches. Found credentials (filtered to the target domain) are shown on this dashboard, including leak source and number of exposed credentials by year. The view is limited to the top 100 entries; click **Download as CSV** to retrieve the full list.

This feature goes further: ZAIUX® Evo evaluates the results and, using controlled password-spraying, determines whether those credentials are still valid within the organization's Active Directory.

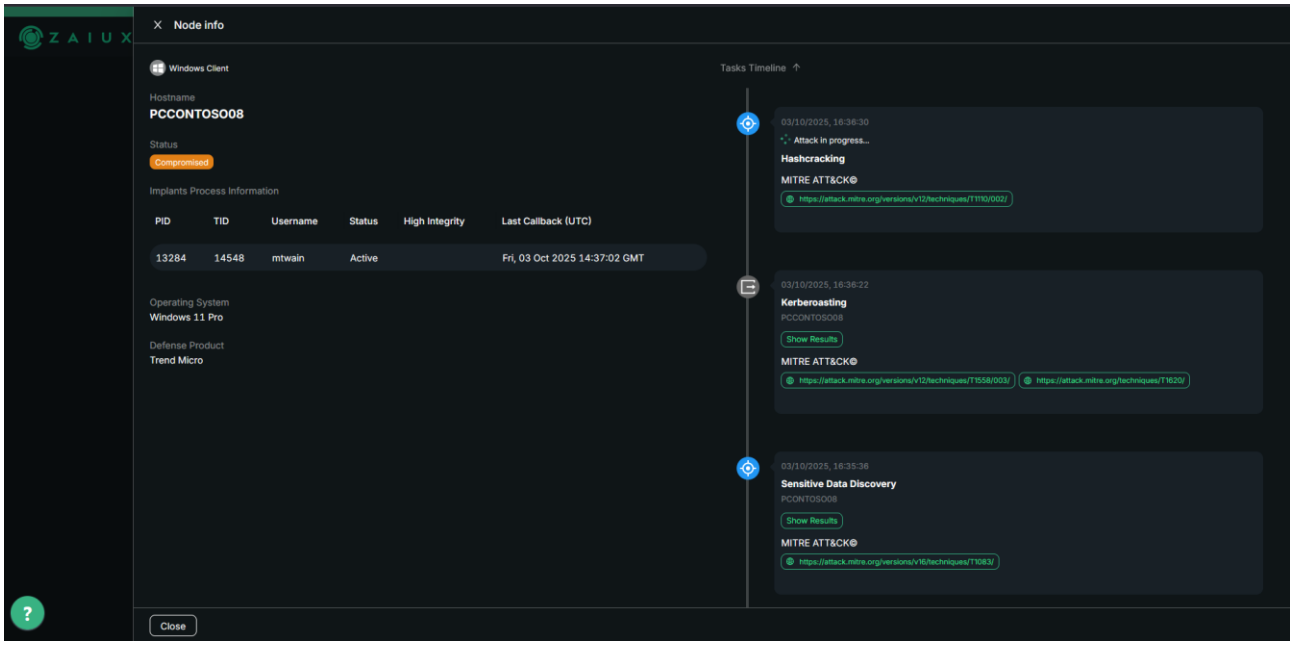
Graph view



The graph view shows all attacks executed by ZAIUX® Evo. It includes enumeration links (grey) and lateral-movement links (red), helping the user visualize how an adversary could propagate across the network, and which hops lead to critical assets.

Compromised Asset details

By clicking on a node, the user can access the view below:



On the left, information about the implant and the compromised asset is displayed. **PID** and **TID** indicate the Process ID and Thread ID where the implants are running. The status of each implant (Active or Inactive) its integrity, and the last callback from the C2 are also shown. The PID can be used to verify whether an Implant is still running or to correlate alarms triggered by defensive solutions such as EDRs.
If all implants on a host are inactive and their PIDs no longer exist, the user may choose to deploy new implants to the same entry point. ZAIUX® Evo maintains a history for each node and avoids repeating operations on the same targets.

On the right, the successful attacks carried out by Implants on this node are listed in chronological order, with the most recent at the top.

Icons legend:

The technique targeted this node. It may be a local attack or originating from an Implant on another node.

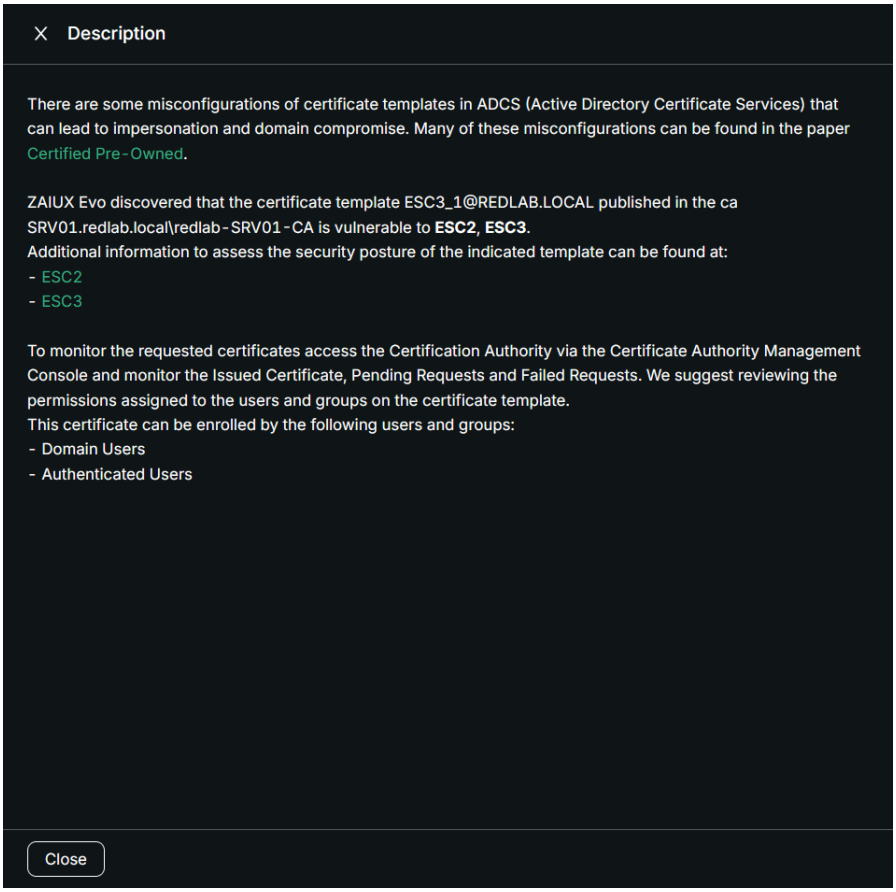
The implant on this node targeted another machine in the network. This may involve enumeration or lateral-movement techniques.

Animated icons indicate ongoing activity. An animation on a node means an action is being executed there; an animation on a technique means it is currently in progress.

The results of each action can be viewed by clicking **Show Results** on the card associated with the technique.

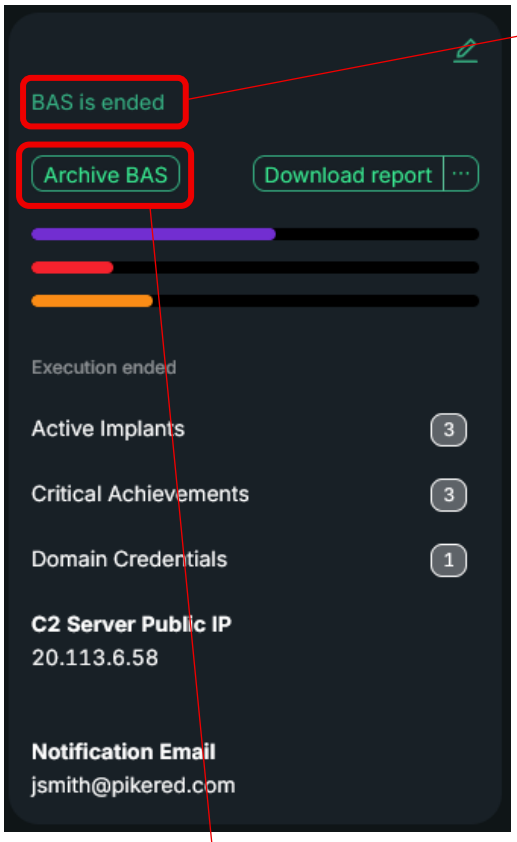
Each finding includes evidence of the misconfiguration, affected entities, and a link for further information (highlighted in green).

The example on the right shows a server vulnerable to a privilege-escalation path due to a weak template in the Certification Authority.



Getting the results

Upon completion of the Breach & Attack Simulation, the report can be downloaded in two formats: **HTML** for a user-friendly view of the results, and **JSON** for structured data to import into other reporting tools. Click **Download report** to retrieve the final document.

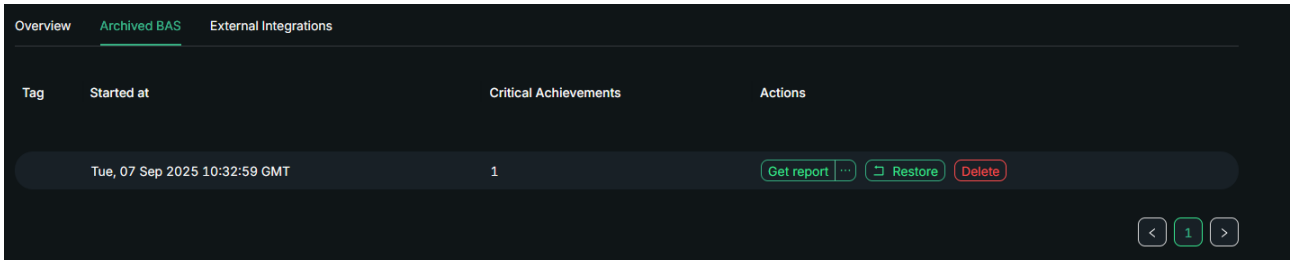


There are different possible ending messages depending on the final status of the Breach & Attack Simulation:

- **BAS is ended**: The BAS terminated normally, either because the threshold limit was reached or the goal achieved.
- **BAS was stopped**: The user manually terminated the BAS before its natural conclusion.
- **Error**: A fatal error occurred that prevented the BAS from continuing execution.

Clicking on "**Archive BAS**" will clean up the dashboard for the selected site, and the BAS will be stored in the site's "**Archived BAS**" tab. From there, the user can:

1. Download the reports again.
2. Unarchive a previous BAS to make it visible in the dashboard (only if no other BAS is running on that site).
3. Permanently delete a previous BAS history, including the report.



Catalog of attack vectors

Below is a comprehensive view of the attack vectors executed by ZAIUX® Evo. Some techniques may be omitted because they run as under-the-hood jobs to enable full-chain attacks.

Process injection

OS	Name	Description
	Thread Execution Hijacking (https://attack.mitre.org/techniques/T1055/003/)	In some real-world scenarios attackers deploy multiple malware binaries on the same host to hide execution chains or provide fallbacks. ZAIUX® Evo emulates this by creating a sacrificial process, hijacking its main thread, and executing an additional Implant to test EDR effectiveness. This specific scenario is validated with deploy method HTML (1).
	Dynamic-link Library Injection (https://attack.mitre.org/techniques/T1055/001/)	Adversaries may inject malicious libraries inside trusted and well-known processes in order to remain stealthy and hide their intentions. Testing EDR effectiveness against such threats is essential to prevent data-breaches. This specific scenario is validated with deploy method HTML (2).

Lateral Movement

OS	Name	Description
	Windows Remote Management	Abusing legitimate protocols is a common technique used by attackers to gain remote code execution. ZAIUX Evo®, leverages WinRM to execute arbitrary code on remote systems to execute new Implants and spread across the network.
	SMB Pivoting	When systems are isolated from the public network it's possible to leverage Named Pipes and establish a pivoting mechanism between the isolated system and an already compromised machine. This technique is often abused by attackers to stay under-the-radar. ZAIUX Evo® detects and exploits these pivoting opportunities.
	Remote Desktop Protocol	If clear-text credentials are recovered, they may allow an attacker to authenticate via RDP. ZAIUX® Evo emulates this scenario by opening an RDP

		session and executing a PowerShell script in the session to deploy a new Implant.
	Abuse SQL Stored Procedure	Existing SQL Server instances can be abused—if an attacker has sufficient privileges—to execute C# code via stored procedures, enabling a fileless attack that can launch an Implant on a remote host.
	SSH Unprotected Key Abuse	ZAIUX® Evo detects unprotected SSH keys and can exploit them to authenticate to remote Linux hosts and perform lateral movement.
	Plaintext SSH Credentials Abuse	Using tools like WinSCP without protecting the credential vault with a master password can expose stored credentials. ZAIUX® Evo can extract unprotected credentials and use them to execute code on remote Linux systems.
	Kerberos ticket abuse	ZAIUX® Evo can detect, and hijack existing Kerberos tickets stored on Linux hosts, enabling lateral movement that may extend to Windows systems.
	SSH Forward Agent abuse	ZAIUX® Evo can detect and hijack active ssh agent forwarding to spread across other Linux machines.

Domain based attacks

OS	Name	Description
	Kerberoasting	ZAIUX® Evo detects Service Principal Names (SPNs) associated with services (for example IIS, SQL Server, Exchange) and requests service tickets for those SPNs. ZAIUX® Evo can then attempt offline hashcracking with the goal of recovering clear-text passwords.
	AS-Rep Roasting	ZAIUX® Evo detects users with the flag "Do not require kerberos preauthentication" enabled. This flag exposes the accounts as their hashes may be requested by other users inside the domain. ZAIUX® Evo can then attempt offline hashcracking with the goal of recovering clear-text passwords.
	Unconstrained Delegation	ZAIUX® Evo identifies machines configured for Unconstrained Delegation and can coerce a Domain Controller to authenticate to them, enabling extraction of Kerberos tickets and impersonation of higher-privilege users and services.
	S4u2Self Abuse	Adversaries may abuse Kerberos Constrained Delegation to force a service to obtain a ticket itself on a user's behalf. This technique allows ZAIUX® Evo to impersonate different user categories on compromised machines.

	Overpass-the-Hash / Pass-the-Ticket	As an alternative to the traditional, commonly detected Pass-The-Hash technique, adversaries now use less-detectable methods such as Overpass-the-Hash and Pass-the-Ticket. It is crucial to assess the effectiveness of defensive solutions against these impersonation attacks.
	Make Token	ZAIUX® Evo can impersonate a user context when a clear-text password is recovered. Adversaries commonly use this technique for lateral movement.
	Password Spraying	Accounts identified as critical or relevant to the simulation are subjected to password-spraying using thresholds that avoid account lockouts, aiming to find weak or easily guessed passwords.
	ESC1	ZAIUX® Evo can exploit vulnerable certificate templates in the Active Directory Certificate Services to attempt privilege escalation. More information about the attack can be found at this link.
	ESC2	ZAIUX® Evo can exploit vulnerable certificate templates in the Active Directory Certificate Services to attempt privilege escalation. More info regarding the attack can be found at this link.
	ESC3	ZAIUX® Evo can exploit vulnerable certificate templates in the Active Directory Certificate Services to attempt privilege escalation. More information about the attack can be found at this link.
	ESC4	ZAIUX® Evo can exploit vulnerable certificate templates in the Active Directory Certificate Services to attempt privilege escalation. More information about the attack can be found at this link.
	ESC15	ZAIUX® Evo can exploit vulnerable certificate templates in the Active Directory Certificate Services to attempt privilege escalation. More information about the attack can be found at this link.
	Abuse *GenericAll* and *GenericWrite* group permission	ZAIUX® Evo detects weak permissions on critical security groups and attempts privilege escalation by adding a controlled user to those groups.
	Clear-Text Password property	In some environments where Unix systems are joined to Active Directory, the *unixUserPassword* attribute may expose clear-text passwords. ZAIUX® Evo detects this attribute and evaluates potential privilege-escalation actions.
	SQL User Impersonation	ZAIUX® Evo identifies whether it can leverage weak permissions and impersonate high-privilege users by exploiting Microsoft SQL Server instances discovered during the enumeration phase.
	BadSuccessor	ZAIUX® Evo detects unpatched Windows Server 2025 instances and can attempt to compromise privileged

		Active Directory accounts by exploiting delegated Managed Service Accounts. More information here.
	GPP Credential	Legacy Group Policy Preferences may expose plaintext credentials usable for local privilege escalation.
	LAPS Abuse	If LAPS has not been properly configure, it can be exploited by attackers to read local admins' credentials and escalate privileges.
	Resource Based Constrained Delegation	Exploiting the WebClient service can enable an NTLM relay, which may result in code execution under the *NT AUTHORITY\SYSTEM* account.

Credential Harvesting

OS	Name	Description
	LSASS Memory Dump	Dumping lsass.exe memory remains a common adversary technique for harvesting privileged credentials. When prerequisites are met, ZAIUX® Evo can perform an LSASS memory dump and transfer the dump for offline analysis to validate exfiltration-prevention controls.
	Browser Credential Dump	ZAIUX® Evo can extract saved credentials from common browsers (Google Chrome, Firefox, Microsoft Edge) and validate recovered credentials against Active Directory.
	Backup Credential Dump	Backup tools in organizational environments are prime targets for attackers seeking full network control. ZAIUX® Evo can detect running instances of popular backup software (e.g., Veeam) and assess their security posture against credential-exfiltration risks.
	Steal Token	When processes run in a different security context they can be targeted for privilege escalation. When conditions permit, ZAIUX® Evo can extract access tokens from other processes and impersonate those users.
	RDP Credential	ZAIUX® Evo monitors processes on compromised hosts and detects execution of remote-desktop clients; it parses those processes' memory and extracts the credentials used for the connection.
	Credential Vault	This module uses OS-specific APIs to verify whether plaintext credentials stored in the Windows Vault can be extracted. These credentials may include SMB share login passwords, mailbox access credentials, or other service credentials.

	Kerberos Ticket Enumeration	When the conditions are met, ZAIUX® Evo attempts to read cashed Kerberos tickets on the compromised assets. These tickets can be used in attacks such as Pass-The-Ticket or S4u2self.
	Linked SQL Server Credential Discovery	ZAIUX® Evo determines whether credentials can be extracted from Linked Servers on SQL instances discovered during enumeration.
	Sensitive Data Discovery	Legitimate Windows APIs such as FindFirstFileA, FindNextFileA, and CreateFileA can be abused to enumerate the filesystem and locate sensitive files (command histories, configuration files, etc.). ZAIUX® Evo simulates this behavior and flags files that may pose a risk.
	Credential Phishing	Attackers may abuse GUI components to display prompts that trick users into entering credentials.
	DcSync	ZAIUX® Evo can perform a full DCSync attack when conditions permit. Validating protection against such attacks is crucial, as a successful DCSync can lead to full network compromise.
	Exposed IIS Configuration File	Administrators may leave backup, test, or legacy IIS configuration files exposed. ZAIUX® Evo determines whether these files can be accessed remotely and attempts to extract credentials that could enable lateral movement or privilege escalation.
	Hashcracking	To avoid consuming RAM and CPU on compromised hosts, hashes are exfiltrated to our cloud for scalable offline hash-cracking. The cracking process combines dictionary attacks, permutations, key-walking, and context-based candidate generation. Recovered passwords are shown masked in the report and may be used by ZAIUX® Evo for subsequent operations (for example, Lateral Movement or Privilege Escalation).
	SAM Credential Extraction from Shadow Copies	ZAIUX® Evo may attempt to dump the SAM database from Shadow Copies and extract local credentials to reuse in Credential Stuffing attacks.

Targeting Microsoft ENTRA ID

OS	Name	Description
	Steal Application Access Token	Access tokens can be recovered by parsing the memory of processes that hold them (for example, OUTLOOK.EXE or MS-TEAMS.EXE). ZAIUX® Evo exploits these tokens to access resources within the Entra ID tenant.
	E-mail Collection	ZAIUX® Evo may use obtained access tokens to read user mailboxes. This simulates an external mailbox compromise (e.g., BEC) to validate detection and response.
	Steal Primary Refresh Token cookie	A Primary Refresh Token (PRT) is present on devices when an Entra ID user signs into a hybrid-joined asset. ZAIUX® Evo can extract the PRT from lsass.exe memory and use it to authenticate to Entra ID, bypassing MFA.
	Access Token Acquisition via Browser request	This technique abuses saved login in browser to initiate an authentication flow as the user, obtaining a new access token valid for ENTRA ID.
	Access Token Acquisition via Refresh Token	The OAuth authentication model allows obtaining new access tokens for additional resources by leveraging a previously obtained refresh token. ZAIUX® Evo leverages this behavior to gather further information about the target cloud infrastructure.
	Data from Cloud Storage	ZAIUX® Evo may attempt to read files from cloud storage (for example, OneDrive). Adversaries commonly target these repositories to retrieve credentials and other sensitive data.
	Blob Storage Access	After impersonating a user, ZAIUX® Evo attempts to access Storage Accounts to identify overly broad read permissions.
	Azure Key Vault Secrets	After impersonating a user, ZAIUX® Evo attempts to access Key Vault Secrets to identify overly broad read permissions.
	Cloud Infrastructure Discovery	ZAIUX® Evo uses ARM access tokens to enumerate Azure resources and role assignments visible to the token's associated user. This simulates an adversary exploring the tenant to identify privilege and configuration weaknesses.
	Azure VM Lateral Movement	Weak permissions may allow ZAIUX® Evo to perform lateral movement to Azure virtual machines, effectively escalating from on-premises infrastructure to the cloud.
	Azure VM Command Execution	Weak permissions may allow ZAIUX® Evo to execute commands on an Azure virtual machine, effectively

		escalating from on-premises infrastructure to the cloud.
	Windows Hello Abuse	If a device is not equipped with a Trusted Platform Module (TPM), the Windows Hello PIN may be extracted. If biometric authentication is enabled, a privileged actor may request a new Primary Refresh Token (PRT) for an ENTRA ID user.
	Access Token from File	ZAIUX® may attempt to decrypt cached cloud access tokens stored in local paths.

Privilege Escalation

OS	Name	Description
	UAC Bypass – Fodhelper	If the current user is a member of the "Local Administrators" group, it is possible to execute arbitrary code in a High-Integrity context by manipulating the windows registry and invoking fodhelper.exe (a windows binary that allows auto-elevation)
	UAC Bypass – SSPI Datagram Context	If the current user is a member of the "Local Administrators" group, it is possible to execute arbitrary code in a High-Integrity context by invoking the SSPI functions.
	UAC Bypass – CMSTPLUA	If the current user is a member of the "Local Administrators" group, it is possible to execute arbitrary code in a High-Integrity by exploiting the CMSTPLUA COM Interface.
	AlwaysInstallElevated Abuse	If this attribute is enabled in the Windows Registry, every user is allowed to install MSI packages with administrative privileges. It is possible to abuse this functionality by executing arbitrary code in a High-Integrity context.
	Unquoted Service Path	If a service path with spaces is not properly wrapped in double quotes, an attacker may be able to exploit the misconfiguration to escalate privileges.
	PrintNightmare	Misconfigurations in the Print Spooler and related registry settings (for example, *RestrictDriverInstallationToAdministrators* and *NoWarningNoElevationOnInstall*) can be abused to achieve arbitrary code execution with elevated privileges.
	Abuse Leaked Token Handle	Leaked user token handles can be hijacked to impersonate a more-privileged user and execute code in that context, enabling privilege escalation and potential lateral movement.
	Sudo programs abuse	If a user can run commands or binaries with *sudo* without a password (due to */etc/sudoers*

		misconfigurations), those privileges can be abused to obtain root-level access. Commonly installed system programs may be misconfigured to allow arbitrary command execution as root.
	Cron Task Privilege Escalation	If a user has "*Write*" permissions to files or directories referenced by cron jobs that run with elevated privileges (for example, as *root*), those permissions can lead to privilege escalation. Since modifying scheduled jobs can disrupt critical services and may not be reliably reversible, ZAIUX® Evo restricts its activity to discovery: it identifies risky cron configurations but does not modify them.

Enumeration and Reconnaissance

OS	Name	Description
	Portscan	Although ZAIUX® Evo does not generate significant network traffic, in certain situations it performs limited port discovery to identify services exposed by a target host. Typical targets include IIS and SQL Server to enumerate reachable services.
	Active Directory Enumeration	Initial stage of every BAS launched with ZAIUX® Evo: a series of LDAP queries that enumerate computers, users, groups, group memberships, access rights, and other domain data. Enumeration is performed by the initial entry point, which loads a C# toolkit into memory to collect the information and exfiltrate it to the external command-and-control (C2) server.
	Stealth LDAP queries	When Active Directory enumeration fails, ZAIUX® Evo switches to a fallback strategy that makes use of targeted, low-volume LDAP queries instead of flooding the Domain Controllers. This approach reduces noise and helps the traffic appear more legitimate.
	Process List	Attackers may enumerate running processes on compromised hosts to identify ones that could contain sensitive data such as passwords or hashed credentials.
	PPL check	Process Protect Light (PPL) helps defend the system critical components against unauthorized access. Before delivering attacks that target protected processes (for example, dumping the memory of lsass.exe), ZAIUX® Evo checks whether PPL is enabled and reports its status.
	Spooler Service check	The Print Spooler Service should be disabled on Domain Controllers when not required, as it introduces potential privilege escalation risks. ZAIUX Evo® checks whether this service is running and reports its status.

	Machine Account Quota check	ZAIUX Evo® performs a check of the *ms-DS-MachineAccountQuota* attribute to determine how many computer-accounts each user can create within the domain. Setting this value to 0 (zero) is a best-practice, as it helps mitigate several attack scenarios.
	LDAP Enforcement check	Enabling LDAP channel binding and signing is crucial to increase the security for communications between the LDAP clients and Domain Controllers. ZAIUX Evo® performs a check of these attributes and reports their status.
	Network Share Discovery	ZAIUX® Evo can explore network shares to locate exposed sensitive information, including credentials and configuration files.