ZAIUX EVO

User Guide

Breach & Attack Simulation and Adversarial Exposure Validation

Version 2.20.5 · October 2026

Produced by

pikered

www.pikered.com · info@pikered.com

How to read this guide

This guide covers the setup, execution, and interpretation of a Breach & Attack Simulation (BAS) with ZAIUX® Evo. Sections 1 to 3 describe the platform and its configuration, sections 4 to 6 walk through running and monitoring a simulation, and section 7 lists every attack vector the platform can execute.

The symbols and colours below are used throughout the document.

Platform icons

In the catalog of attack vectors, these icons mark the platforms a technique applies to.

	Microsoft Windows — the technique runs on, or targets, Windows hosts.
	Linux — the technique runs on, or targets, Linux hosts.
	Microsoft Entra ID and Azure — the technique targets cloud identities and resources.

Node colours in the BAS dashboard

Every host drawn on the dashboard and in the graph view is coloured according to how far the simulation reached it.

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

Technique icons on an asset

On the detail page of a compromised asset, each technique card carries one of these icons.

	Inbound. The technique targeted this node. It may be a local attack or one originating from an Implant on another node.
	Outbound. The Implant on this node targeted another machine in the network. This may involve enumeration or lateral-movement techniques.
	In progress. 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 running.

Callouts

Three kinds of panel interrupt the main text.

> **Note**
>
> Background information or a constraint worth keeping in mind. Nothing breaks if you skip it.

> **Recommended setting**
>
> A configuration Pikered advises for most environments.

> **Important**
>
> A condition that can block the simulation or change its results. Read before you proceed.

Typographic conventions

Bold	Labels, buttons, tabs, and fields exactly as they appear in the interface.
`mono`	File names, table names, registry keys, API permissions, and other literal values you type or copy.
link	An external reference. The target opens in your browser.

Table of contents

How to read this guide 2
Platform icons 2
Node colours in the BAS dashboard 2
Technique icons on an asset 2
Callouts 3
Typographic conventions 3
Adversarial Exposure Validation, made simple 6
What sets ZAIUX® Evo apart 6
Key benefits 6
Getting started with ZAIUX® Evo 7
Types of users 7
Creating a site 8
Opening a support request 9
External integrations 10
Integrating Jira Service Management 10
Integrating ServiceNow 12
Closing gaps in endpoint detection with Breach & Attack Simulation 17
Integrating SentinelOne AI SIEM 18
Integrating Microsoft Defender for Endpoint 20
Integrating Splunk for event collection 21
Integrating Elastic for event collection 24
How to create a BAS with ZAIUX® Evo 27
Note on defining exclusions 27
Deployment methods 29
If all deployment methods are blocked 31
Selecting the entry points 31
System requirements 31
Rollback and manual cleanup 31
How to plan a recurring BAS 33
Installing the service on the entry points 33
Creating a new planned BAS 36
Important considerations for planned BAS 39
Monitoring the BAS progress 40
Interface core components 40
Colour legend 42

Other navigation features 42
Leaked credentials 43
Graph view 43
Compromised asset details 44
Icon legend 44
Getting the results 45
Catalog of attack vectors 47
Process injection 47
Lateral movement 47
Domain-based attacks 48
Credential harvesting 50
Targeting Microsoft Entra ID 51
Privilege escalation 53
Enumeration and reconnaissance 54

Adversarial Exposure Validation, made simple

ZAIUX® Evo is a SaaS solution that automates Command and Control (C2) attack activities and generates false-positive-free reports that include remediation plans.

ZAIUX® Evo delivers advanced Breach and Attack Simulations (BAS) to IT infrastructures. It employs artificial intelligence to allocate resources through mathematical optimization, executing automated ethical hacking processes that concretely test security holes in the target network.

Unlike other attack simulations, ZAIUX® Evo autonomously emulates a realistic malware infection. The whole defense chain is therefore validated against a targeted attack coming from the outside, which brings out vulnerabilities both in privilege-escalation prevention within the domain and in data-exfiltration protection.

What sets ZAIUX® Evo apart

ZAIUX® Evo performs a complete and realistic simulation of an intrusion in a Microsoft Active Directory and Entra ID environment, exploiting a regularly updated range of modern hacking techniques that run in stealth mode to emulate a human approach.

Automation is handled by our proprietary engine. It uses machine-learning algorithms built by our team of experts to emulate human intelligence, which removes the time and cost barriers of a manual execution. The adaptive algorithms shape the system's response according to the attack surfaces that emerge from the scans, entirely automatically.

For each assessment, ZAIUX® Evo generates an isolated sandbox associated with a unique initialization package. That package runs directly from any endpoint inside the target network, with no agent to install.

Key benefits

Enhanced visibility of Crown Jewels and critical assets

Clear view of misconfigurations and realistic attack paths

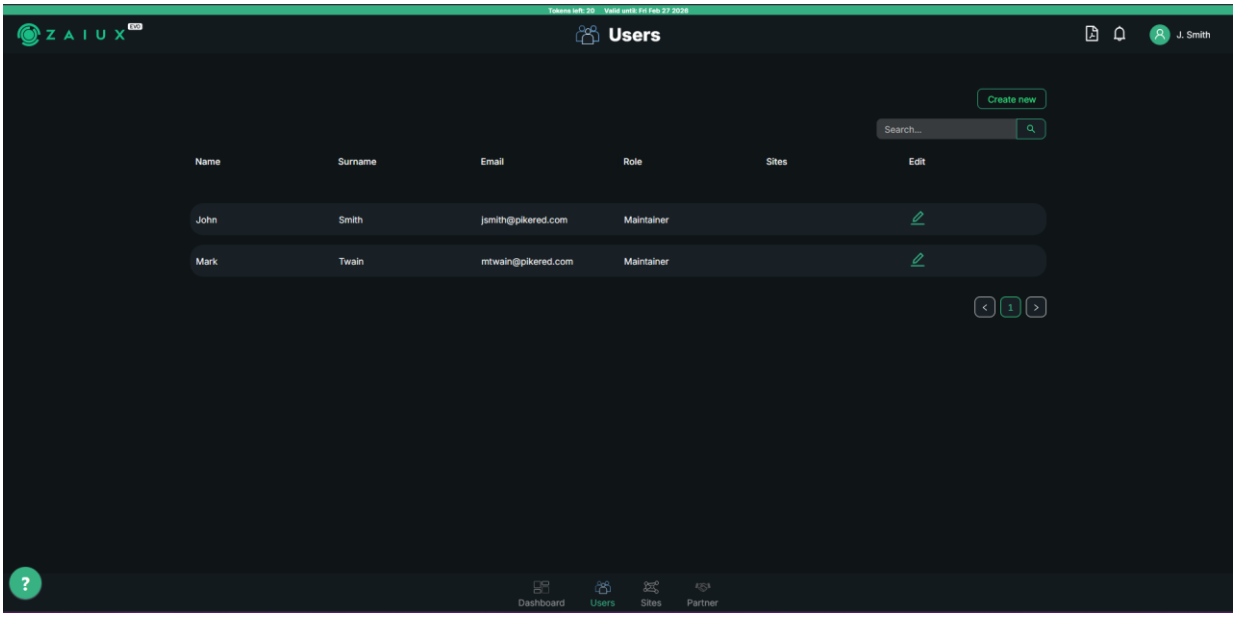
Flexible partitioning of the BAS attack surface

Optimization of IR playbooks and defense tools

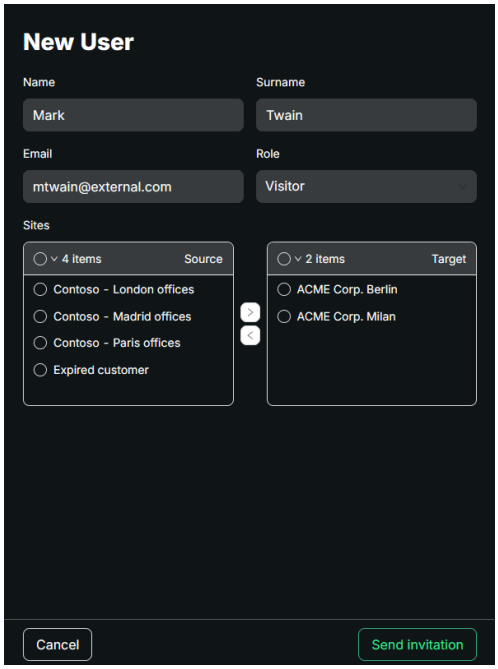
Getting started with ZAIUX® Evo

Once the purchase process is complete, the designated users are invited to create the first administrator account for the tenant. Follow the video guide here to create your first account before working through the rest of this guide.

Types of users



Beyond the first user assigned during the purchase process, you can create additional users with different access levels. Clicking **Create New** opens a sub view on the right side of the page, where the new user is defined.



- **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, with no access to any other page. For example, an MSP customer who wants to monitor their own network.
- **Sales**: for registered partners. Gives access only to the partner program area, where you can take certifications, download the Sales Kit, request pre-sale support, or create white-labeled reports by uploading a custom logo.

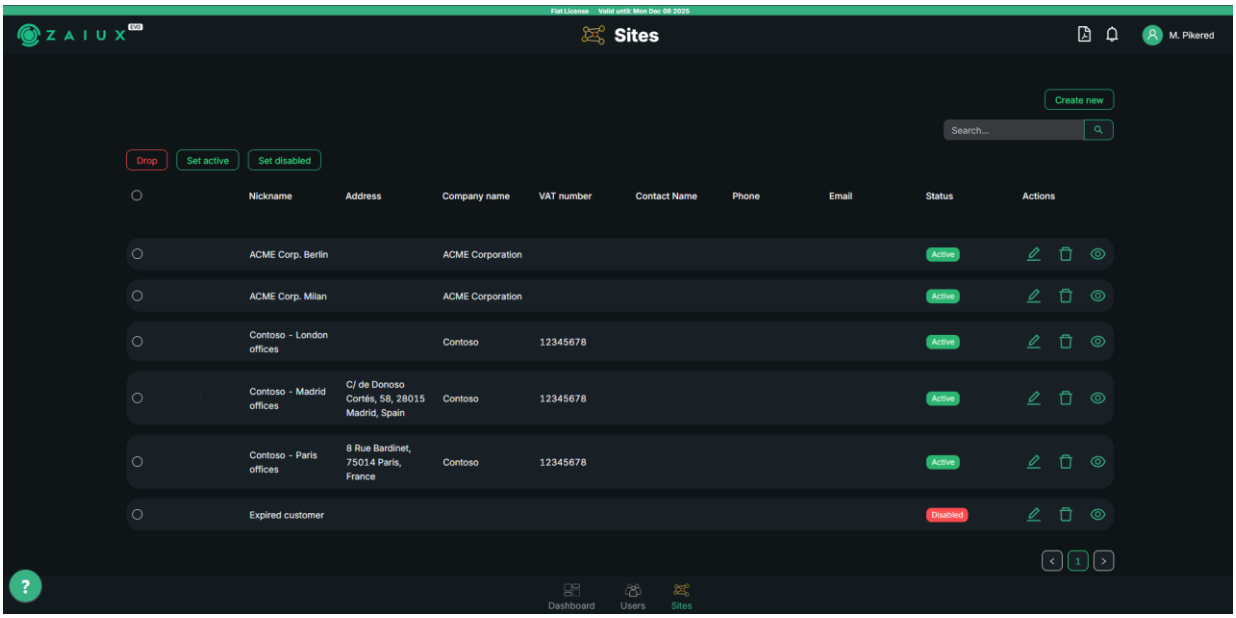
Clicking **Send Invitation** sends a registration email to the specified address.

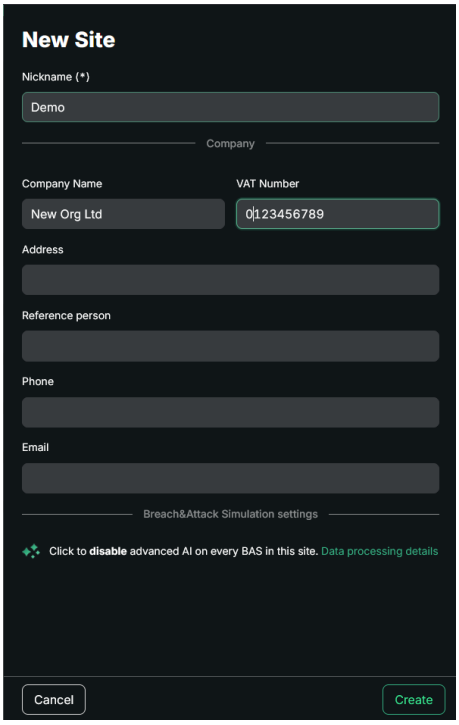
Creating a site

A site in ZAIUX® Evo is one of the following:

- A single Active Directory domain to be tested. This is the best use case for MSPs.
- A logical breakdown of a complex infrastructure with multiple domains, with 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 is available under the **Sites** tab in the bottom-bar menu.





Clicking **Create new** opens a sub view on the right side of the page, where the new site is defined.

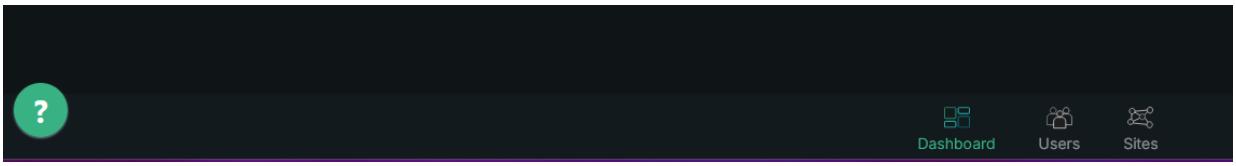
All fields are optional except **Nickname**, which should identify the customer (for MSPs) or the owned site (for end customers). Click **Create** to add the new site to the list.

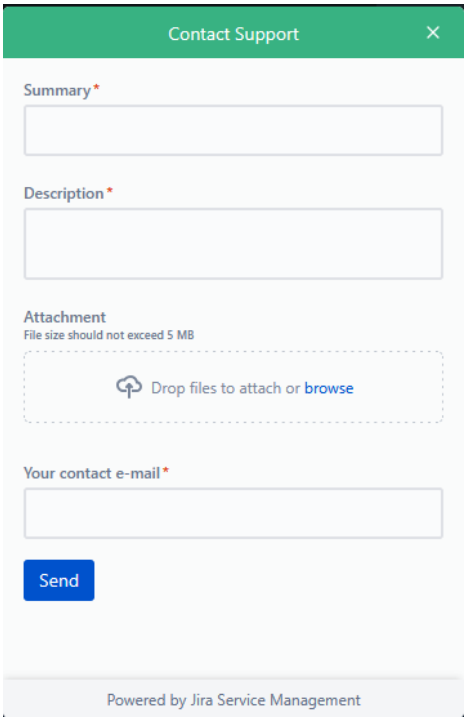
Site details can be edited later, and the site can be disabled or permanently deleted.

You can also enable **Advanced AI**. This lets the Breach & Attack Simulation platform correlate information gathered from the Dark Web with the analyzed corporate environment. It can also inspect the contents of files discovered on network shares to identify credentials and other valuable information that may support the continuation of the assessment.

Opening a support request

Every page, including the login page, can open a support request to Pikered through the **?** button at the bottom left.





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

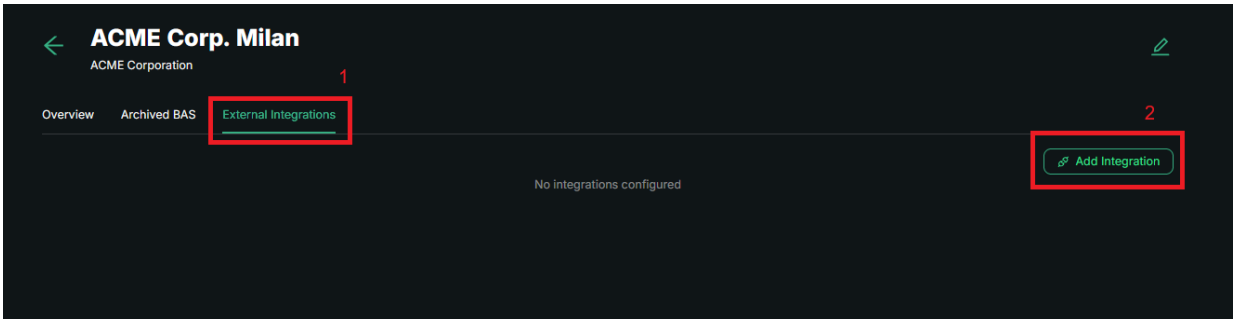
Fill in the contact email field and the support team will respond as soon as possible, depending also on your contract type.

Support is delivered through Jira Service Management and handled exclusively by Pikered employees. No third-party technicians are involved.

External integrations

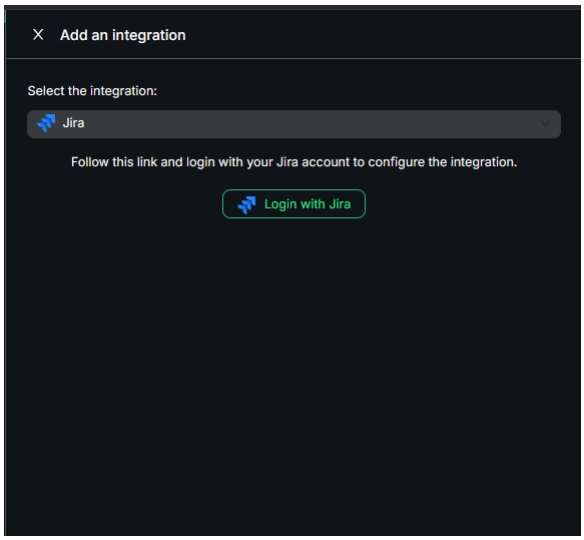
ZAIUX® Evo can be extended through external software and services, and new integrations are added to the platform continuously. Each integration is configured per site, which makes the platform interoperable with the tools system integrators and blue teams already use.

For each site, click **External Integrations**, then **Add Integration**, and choose one from the list.



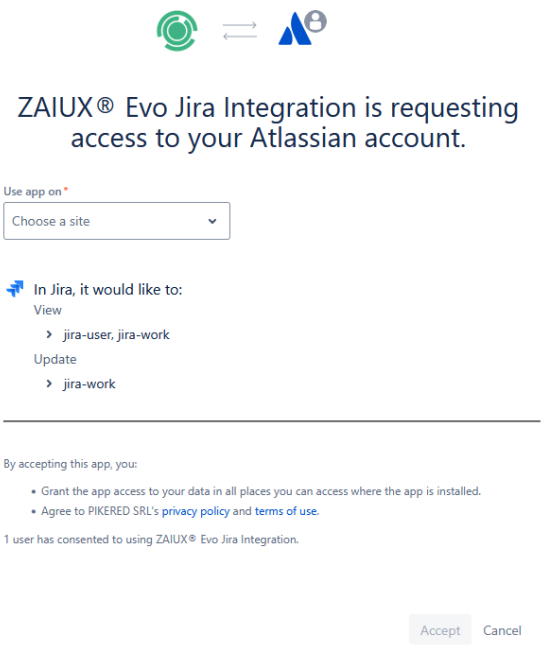
Integrating Jira Service Management

> **Note**
>
> ZAIUX® Evo is officially available on the Jira Marketplace.



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

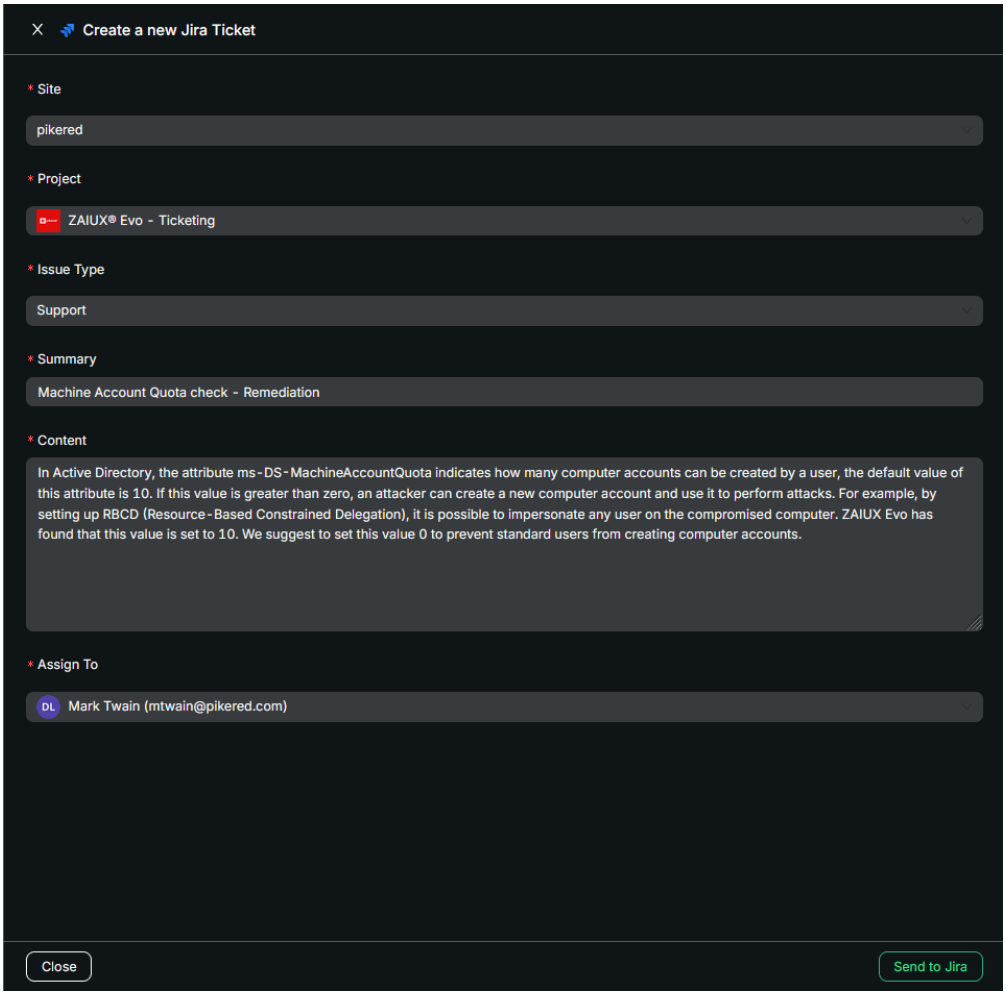
If your Jira session is already active, a Jira form is displayed.



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

Every attack frame in the timeline then offers the option to open a ticket directly in the Jira project.

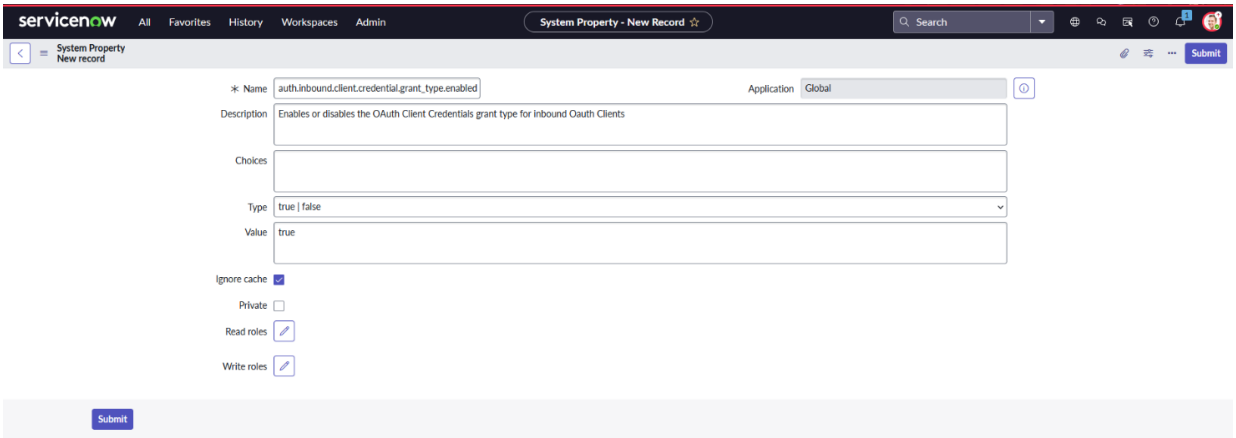
The **Summary** and **Content** fields are populated automatically with the description of the selected attack. You can choose the project, the issue type, and the ticket assignee; these values are retrieved through the Jira API. Once you click **Send to Jira**, the ticket appears on the ticketing platform.



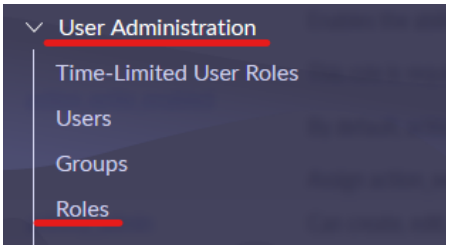
Integrating ServiceNow

Follow these steps to integrate ZAIUX® Evo with ServiceNow.

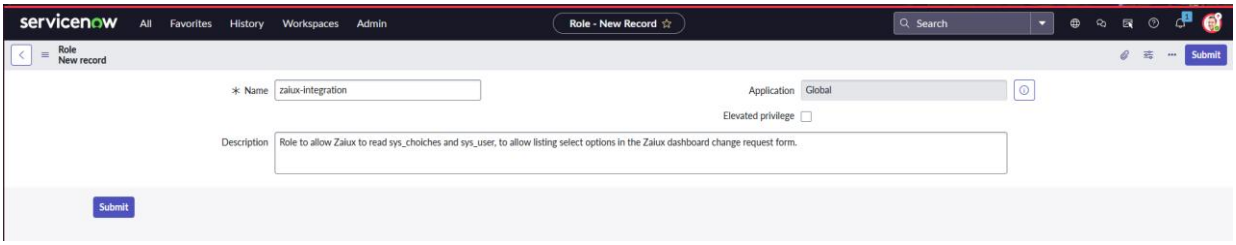
1. Enable the **client credentials** grant type by creating a new Boolean system property in the `sys_properties` table. Name it `glide.oauth.inbound.client.credential.grant_type.enabled` and set its value to `true`.



2. Create a new role that lets the ZAIUX® Evo integration read from the relevant tables. In the **User Administration** menu, open the **Roles** section.

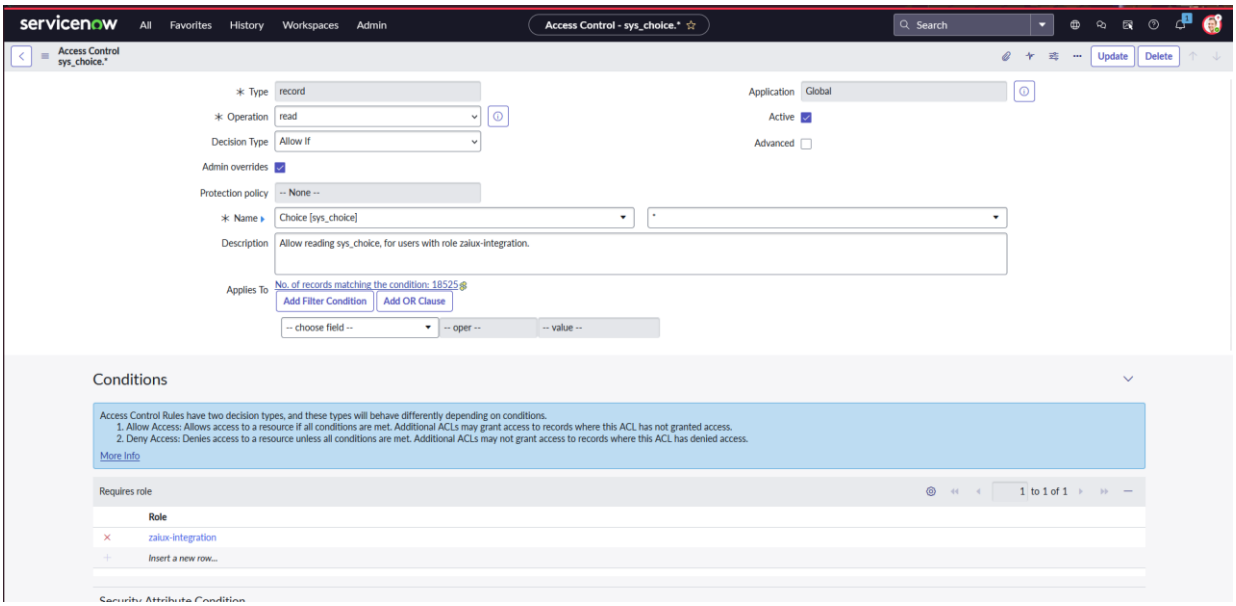


3. Create the role for the integration. The example below names it `zaiux-integration`.

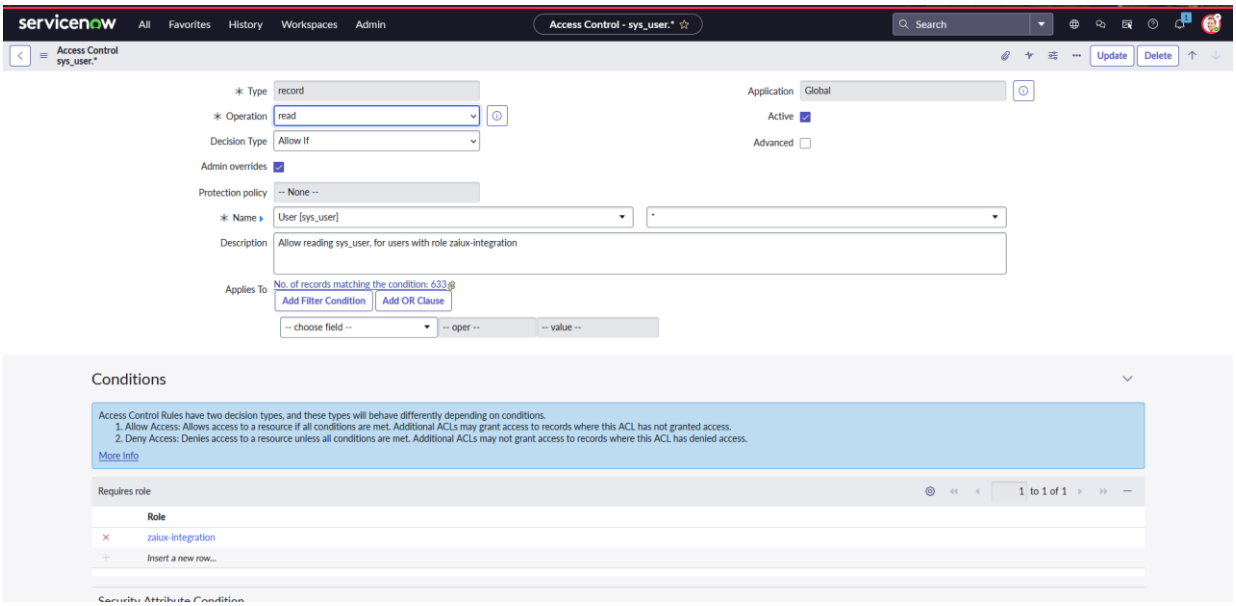


4. Create ACL rules that allow the new role to read from the `sys_user` and `sys_choice` tables. From **System Security**, open **Access Control (ACL)**.

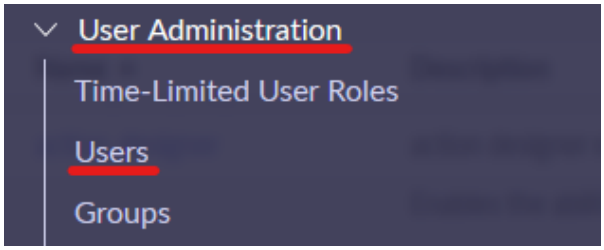
5. Create the first ACL rule, allowing the new role to read all fields in the `sys_choice` table.

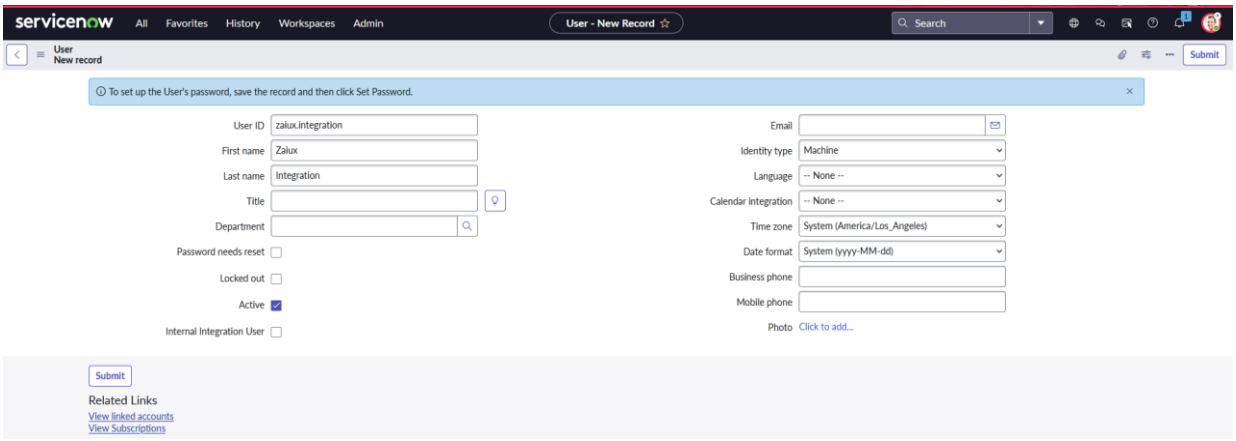


6. Create the second rule, allowing reads from the `sys_user` table.

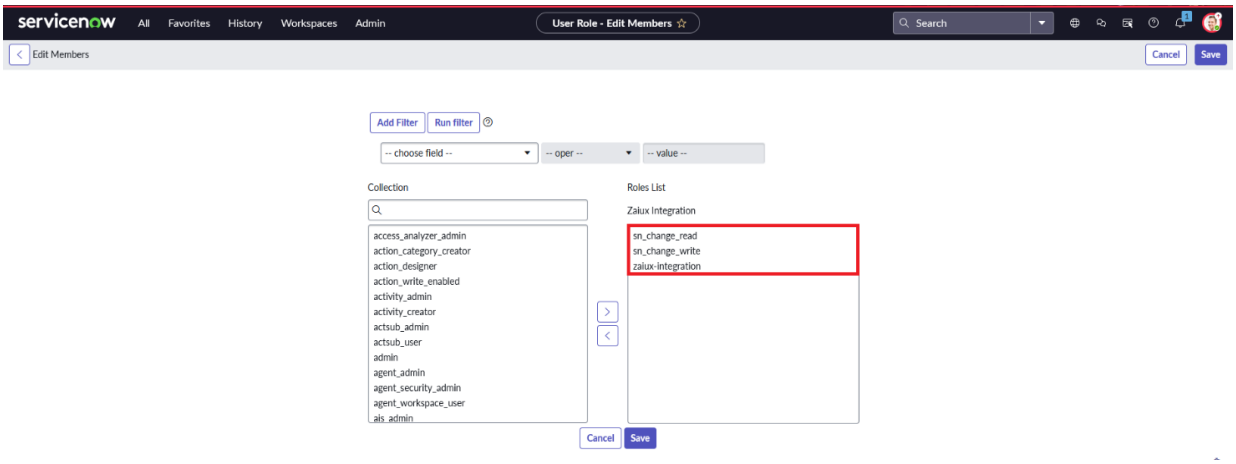


7. Create a user for the integration to use. Open the **User Administration** menu and go to the **Users** section.

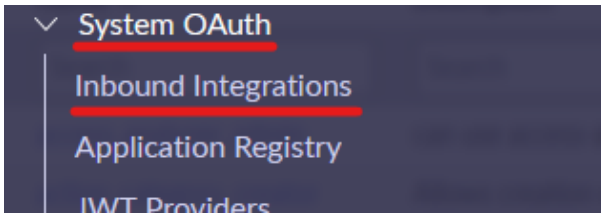


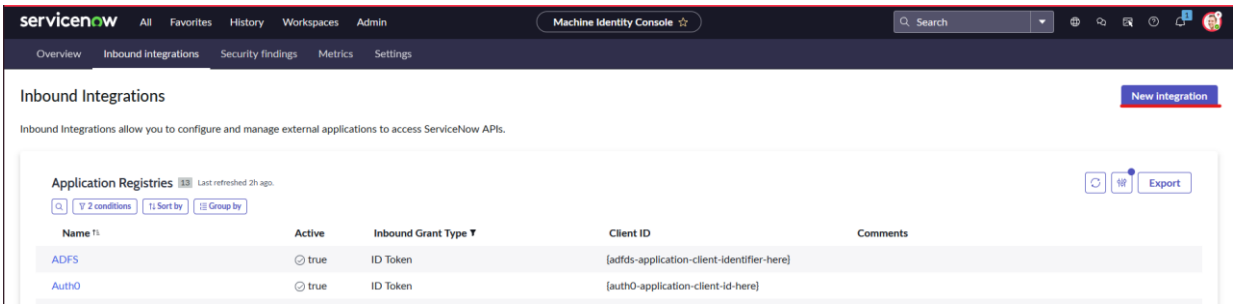


8. Associate the role you created with the new user, then add `sn_change_read` and `sn_change_write` to the roles list.

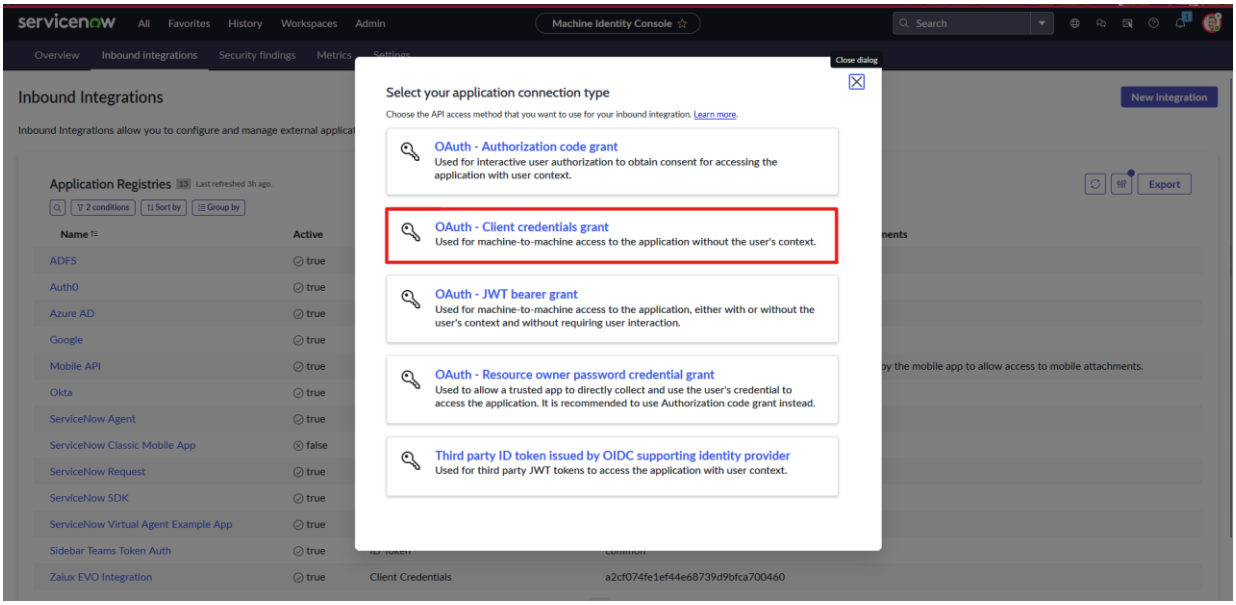


9. Create a new OAuth integration. Open the **System OAuth** menu and go to the **Inbound Integrations** section.

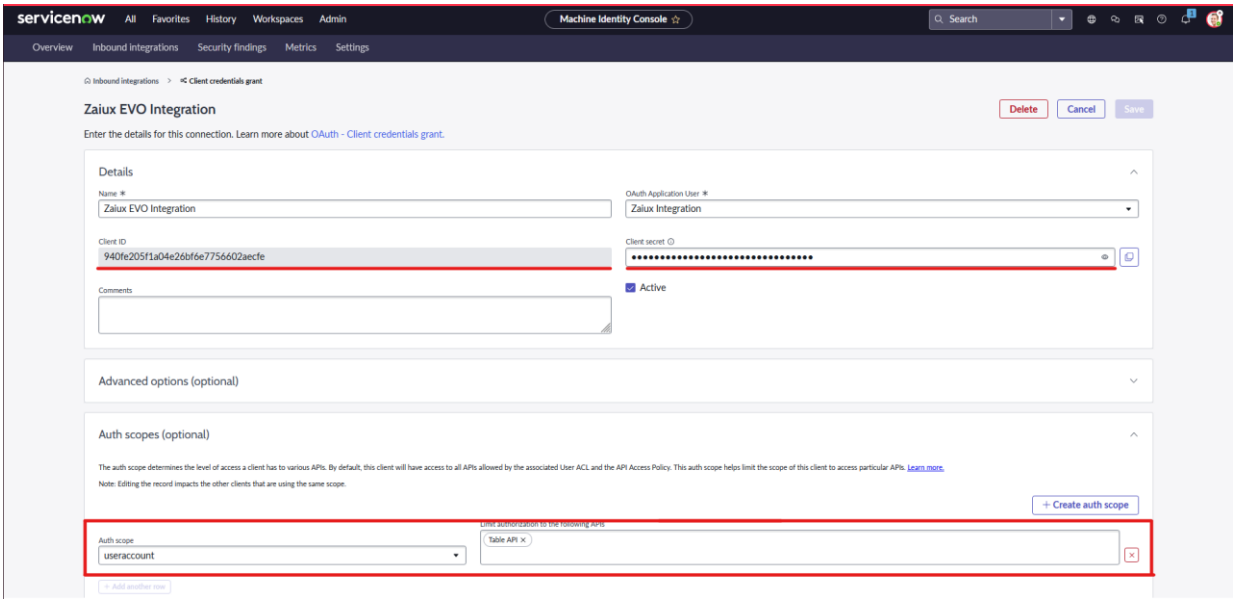


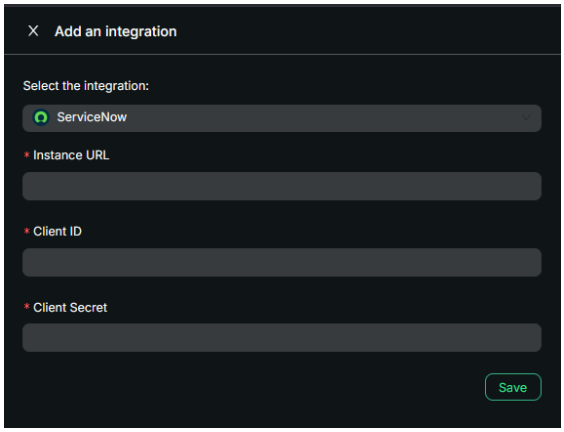


10. Choose **OAuth – Client Credentials grant**.



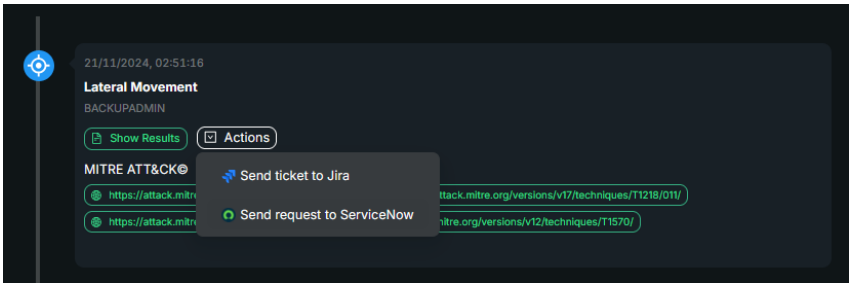
11. When creating the credential, associate the ZAIUX® Evo integration account with it using the **OAuth application user** field. Create a new **Auth Scope** named `useraccount` and limit its access to the Table API.



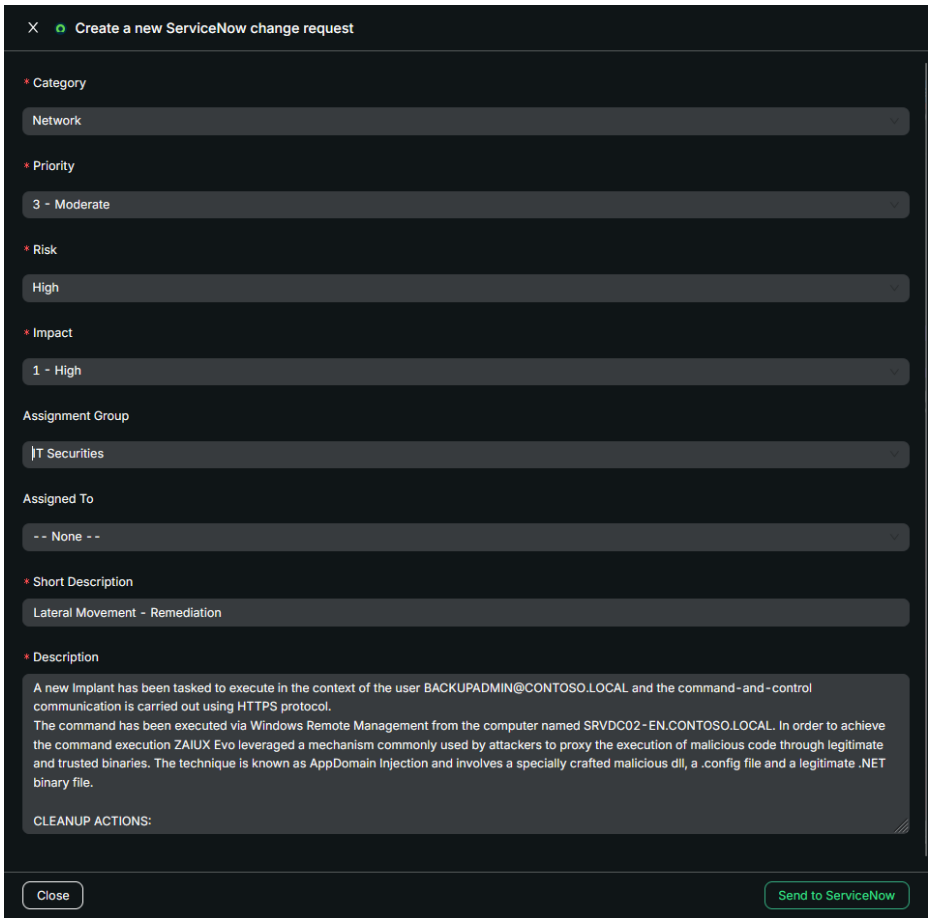


12. Take note of the **Client ID** and **Client Secret**; both are needed to configure the integration in the ZAIUX® Evo dashboard.

Once this step is complete, you can open a request in ServiceNow for every piece of evidence the Breach & Attack Simulation highlights.



As with the Jira integration, you can select several parameters to streamline the risk-management process and cut the communication time between teams.

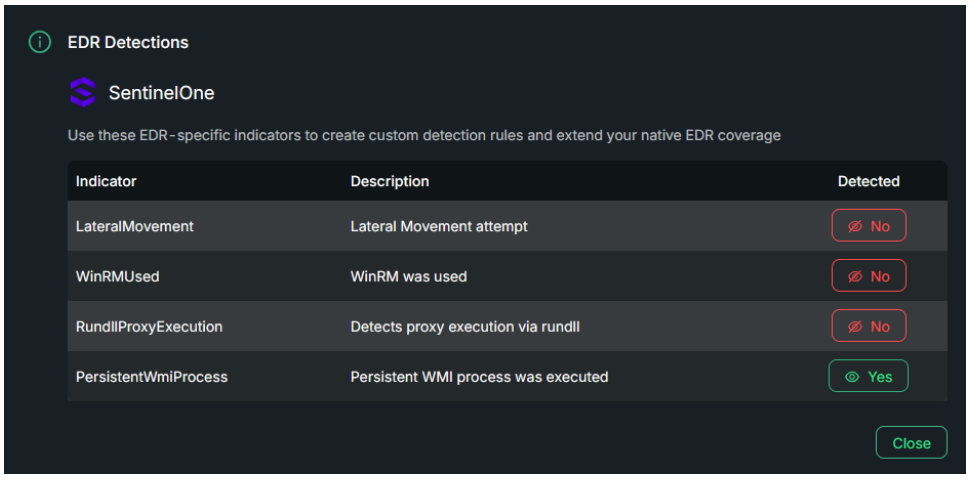


Closing gaps in endpoint detection with Breach & Attack Simulation

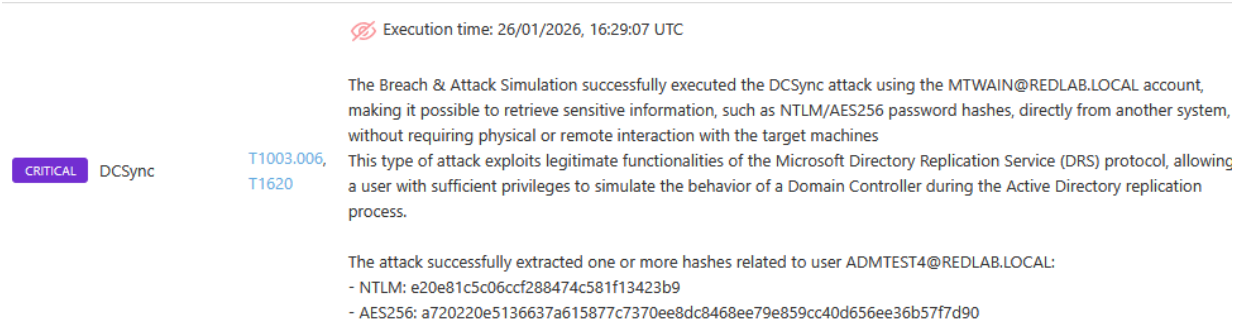
When an EDR is configured, ZAIUX® Evo fetches the events and alerts your endpoint security console generated during BAS activity. It then correlates them with the actions the Breach & Attack Simulation performed, so you can evaluate EDR/XDR coverage against modern attacks. The result is available in the web interface and in the generated reports.

In the example below, the lateral movement is marked **Detected**.

Clicking the button shows which detectors fired and which did not. Analysing the individual indicators makes it possible to detect and block attempts to exploit the same attack path with slightly different techniques that might otherwise bypass detection.



The report states whether each technique was detected or went unseen. The example below shows an undetected DcSync.

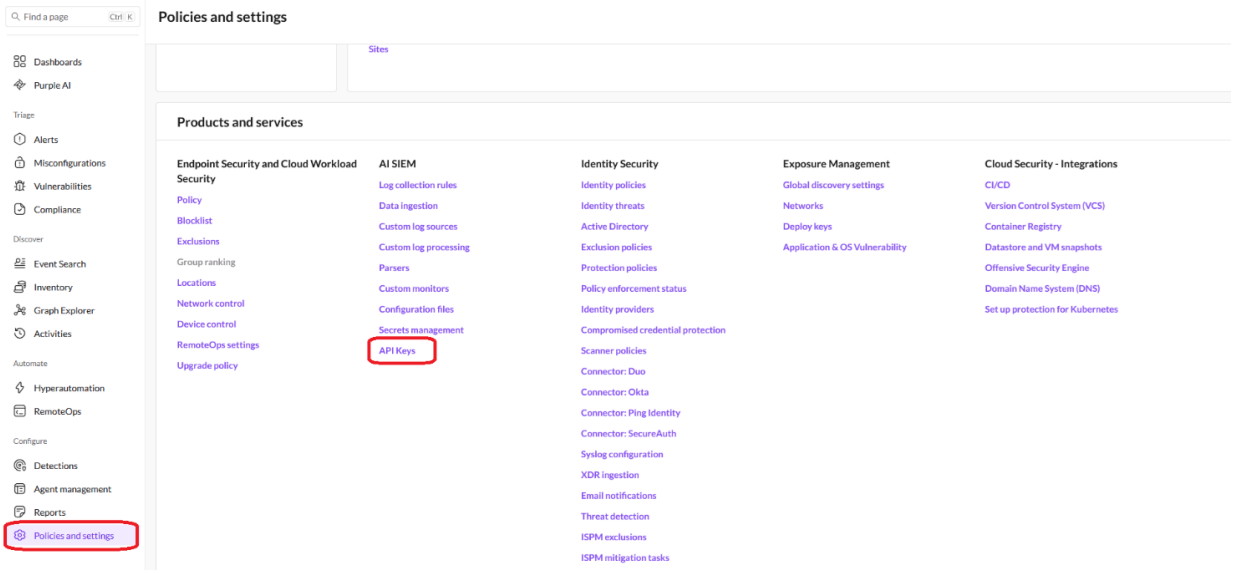


Integrating SentinelOne AI SIEM

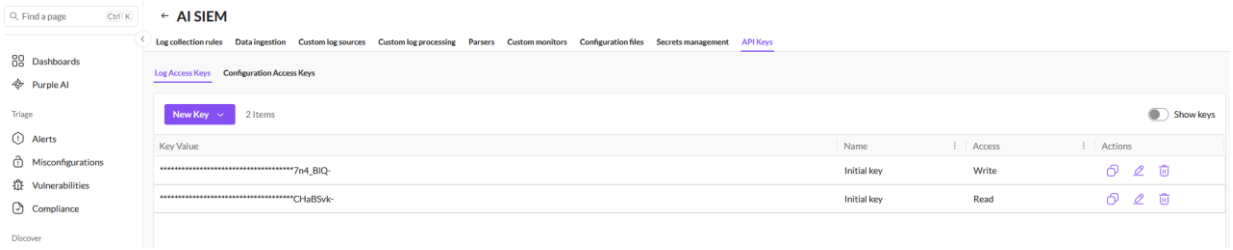
ZAIUX® Evo integrates with SentinelOne AI SIEM to bring the Breach & Attack Simulation and your defensive technologies closer together. The integration gives deeper visibility into simulated attack activity, which lets you extend the native EDR coverage and write custom detection rules.

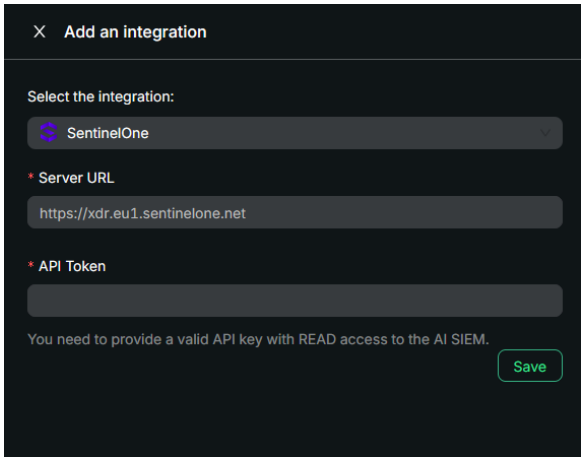
Follow the steps below to connect ZAIUX® Evo to your SentinelOne console.

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, open the **Integrations** section for the site you want and enter the SentinelOne server address and API key.

4. Click **Save**. The system validates the information automatically. If the check succeeds, the SentinelOne widget appears on the Integrations page.

Integrating Microsoft Defender for Endpoint

ZAIUX® Evo integrates with Microsoft Defender for Endpoint to bring the Breach & Attack Simulation and your defensive technologies closer together. The integration gives deeper visibility into simulated attack activity, which lets you extend the native EDR coverage and write custom detection rules.

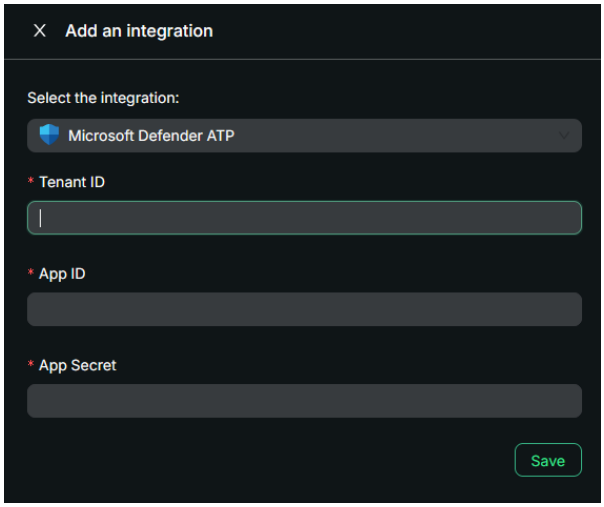
Follow the steps below to connect ZAIUX® Evo to your Microsoft Defender for Endpoint console.

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

2. When creating the application, grant the following API permissions: `Alert.Read.All` and `Machine.Read.All`.

3. Generate an application secret and take note of its value, as it is required later.

4. Take note of the **Tenant ID** and **Application (Client) ID**, both visible on the application Overview page. These values are required to configure the integration on the ZAIUX® Evo side.



5. In ZAIUX® Evo, open the **Integrations** section for the site you want and enter your Tenant ID, App ID, and App Secret.

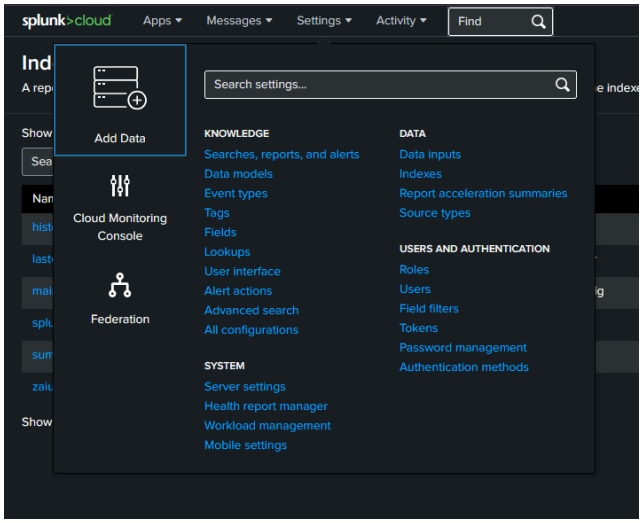
6. Click **Save**. The system validates the information automatically. If the check succeeds, the Microsoft Defender for Endpoint widget appears on the Integrations page.

Integrating Splunk for event collection

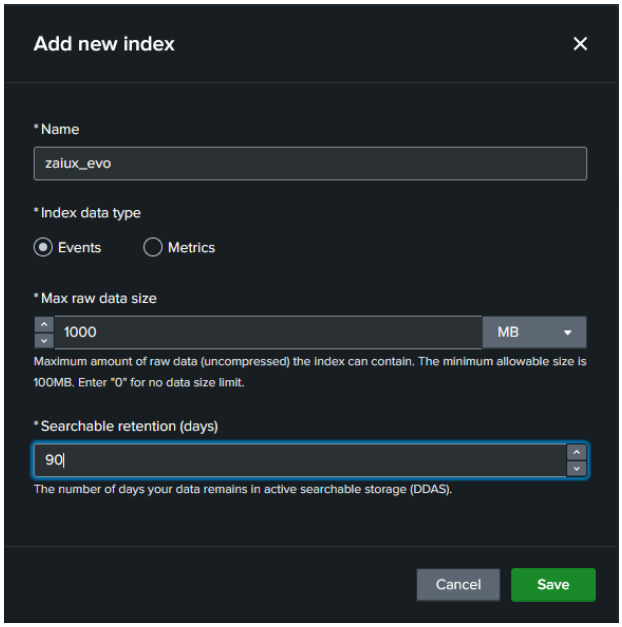
ZAIUX® Evo integrates with Splunk through a dedicated forwarding plugin that streams all Breach & Attack Simulation data directly into a dedicated Splunk index.

Security teams can therefore centralize BAS telemetry inside their existing Splunk environment, where it can be searched, correlated, and analyzed alongside logs from endpoints, network devices, and other data sources. The plugin forwards detailed execution data continuously, including techniques, timestamps, TTPs, and other contextual metadata, which improves visibility into validation activities and detection coverage.

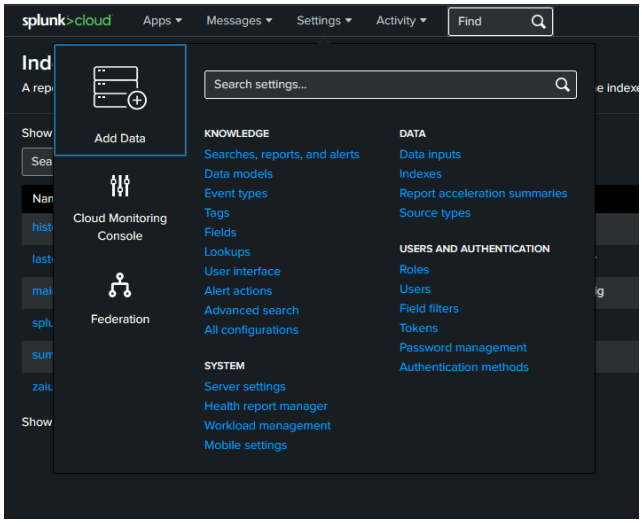
Follow the steps below to connect ZAIUX® Evo to your Splunk console.



1. From the navigation menu, go to **Settings** and select **Indexes**. This section manages data storage and is where you create a dedicated index for the events the Breach & Attack Simulation generates.



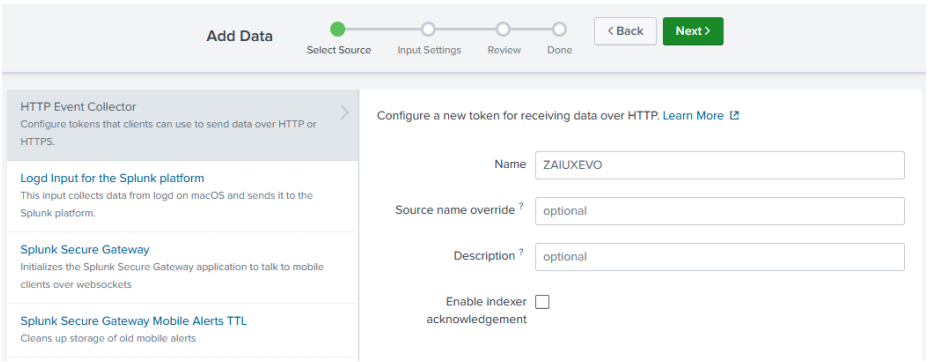
2. Click **New Index** and define a name for the index that will store BAS events. Configure the maximum data size and the retention period according to your requirements.



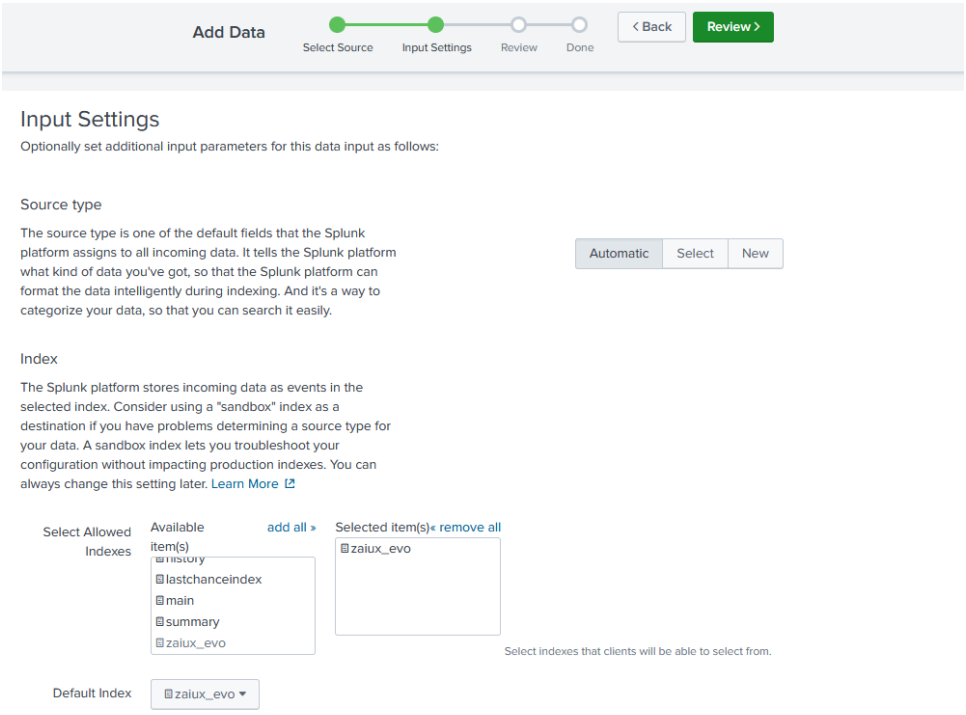
3. From the navigation menu, go to **Settings** and select **Data Inputs**.

As a final step, create a new HTTP Event Collector (HEC). This component lets ZAIUX® Evo stream BAS event data securely into the index you just created.

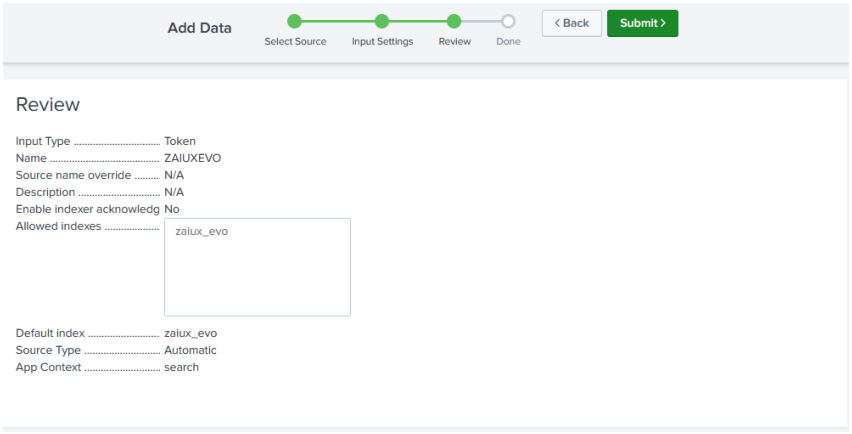
4. Choose a name for the HTTP Event Collector and move to the next step.



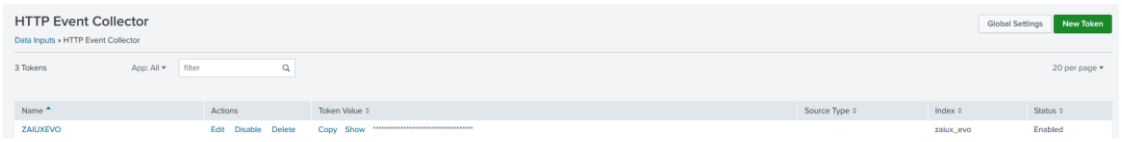
5. Select the index you created to store the incoming data.

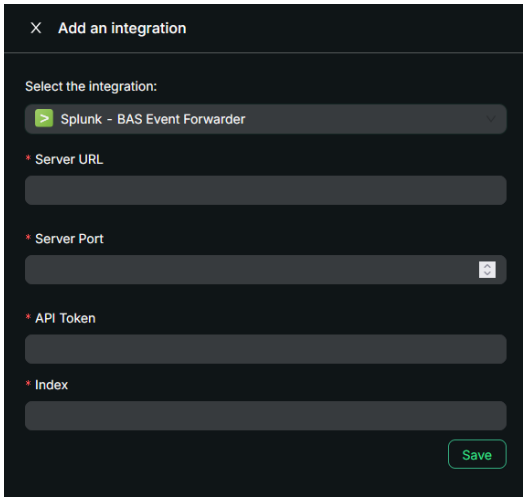


6. Review the new data input configuration and submit it.



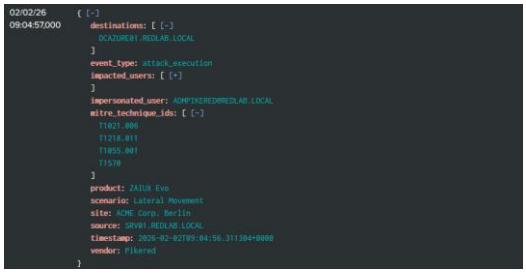
7. Copy the generated **Token** value to use in the ZAIUX® Evo interface.





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

- Server URL
- Server port (the default HEC port is 8088)
- API token
- The index name created in the previous steps



9. Once configured, every action from the next Breach & Attack Simulation run on this site is forwarded to the Splunk server, giving detailed context for each technique ZAIUX® Evo executes.

Integrating Elastic for event collection

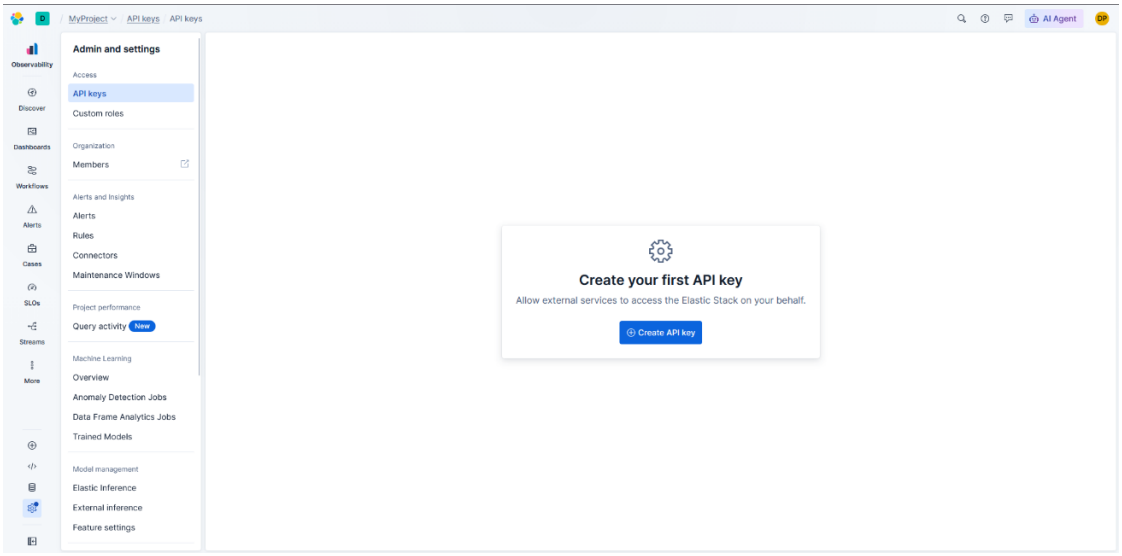
ZAIUX® Evo integrates with Elastic through a dedicated forwarding plugin that streams all Breach & Attack Simulation data directly into a dedicated Elastic index.

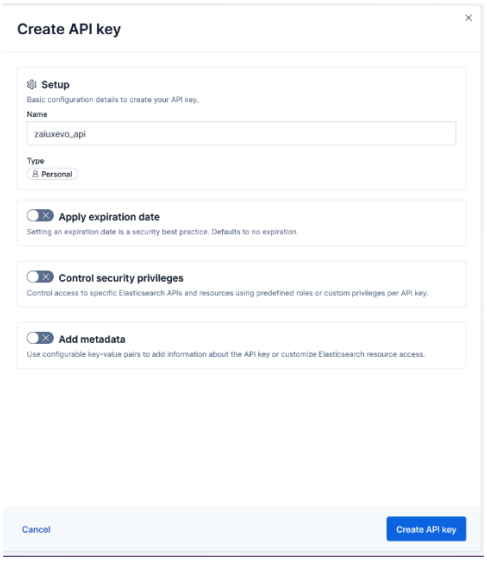
Security teams can therefore centralize BAS telemetry inside their existing Elastic environment, where it can be searched, correlated, and analyzed alongside logs from endpoints, network devices, and other data sources. The plugin forwards detailed execution data continuously, including techniques, timestamps, TTPs, and other contextual metadata, which improves visibility into validation activities and detection coverage.

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

1. Retrieve your Cloud ID by following the official Elastic documentation at https://www.elastic.co/search-labs/tutorials/install-elasticsearch/find-cloud-id-create-api-keys.

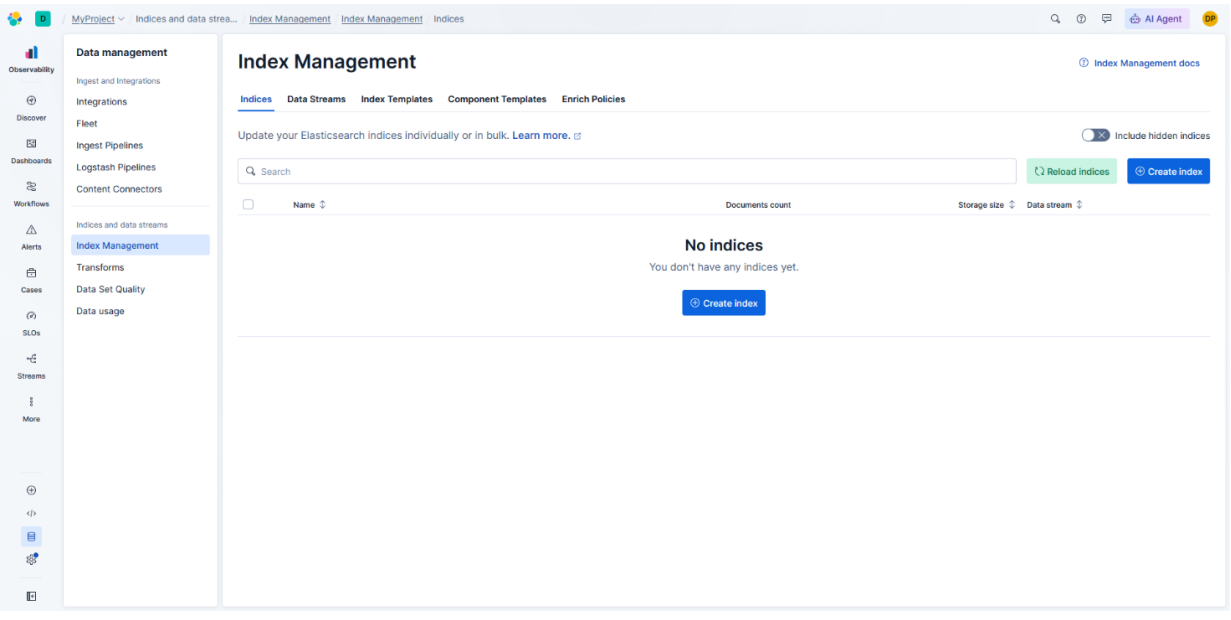
2. Create a new API key from the **Admin and settings** page of your Elastic project.

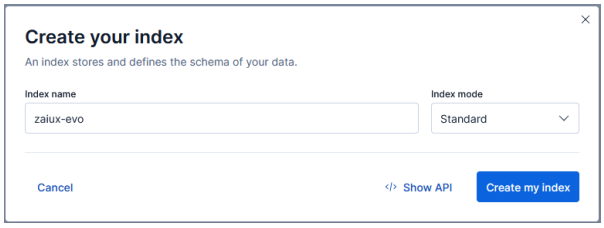




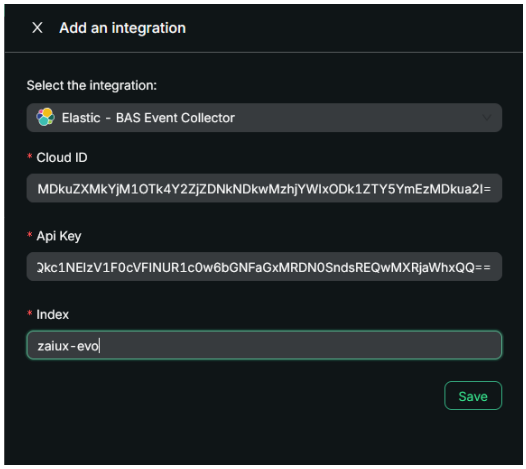
3. Give the API key a name and configure any additional options according to your requirements, leaving optional fields empty if they are not needed. Once the key is created, copy and store it securely: it is required in the next steps.

4. Open the **Data management** section, go to **Index Management**, and create a new index.





5. Enter a name for the index and select **Standard** as the index mode, then click **Create my index**.



6. In the ZAIUX® Evo plugin, provide the information collected in the previous steps:

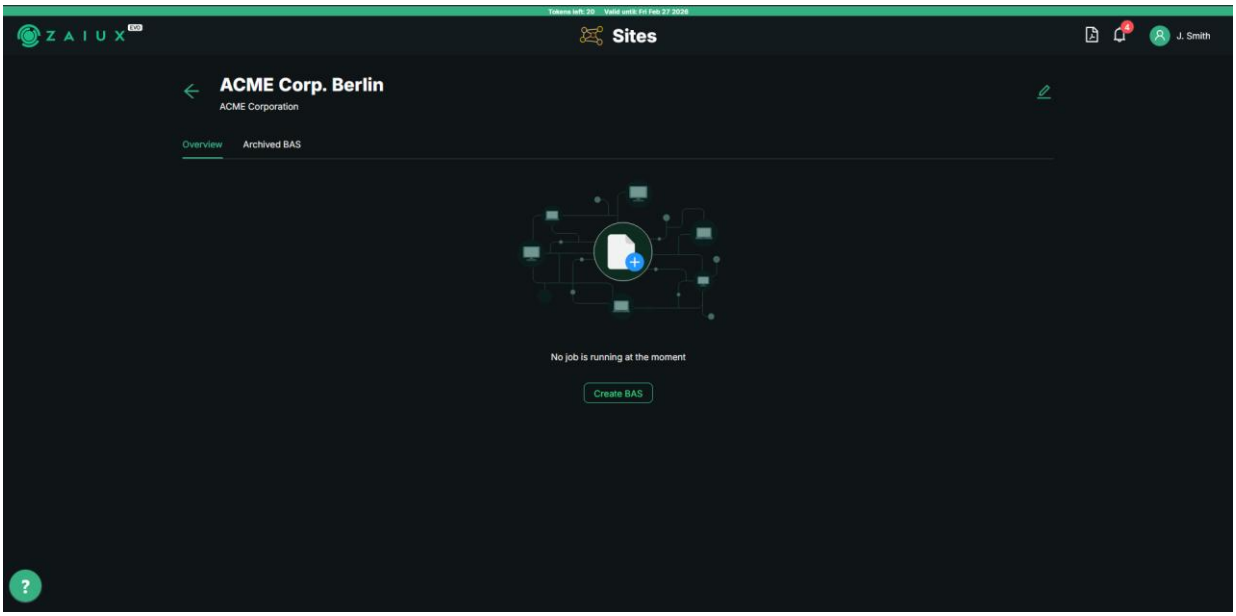
- Cloud ID
- API key
- Index

7. Click **Save** to validate the configuration. If the information is correct, a test event is generated and forwarded to your Elastic console.

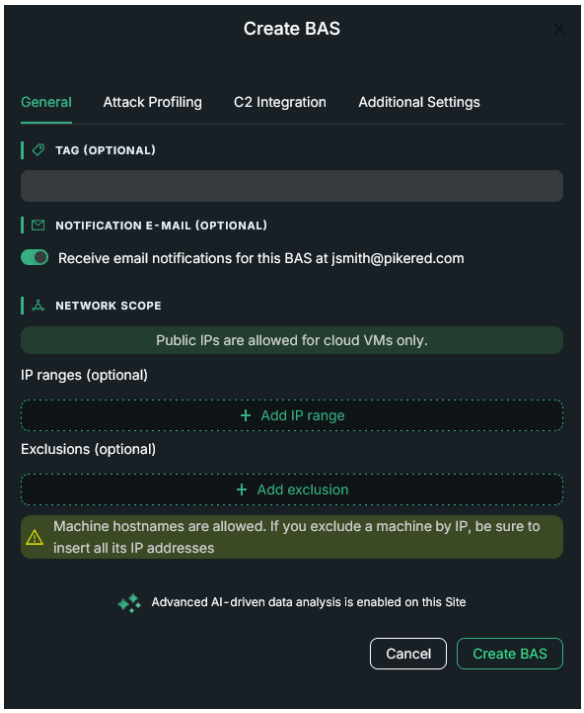
Once configured, every action from the next Breach & Attack Simulation run on this site is forwarded to the Elastic server, giving detailed context for each technique ZAIUX® Evo executes.

How to create a BAS with ZAIUX® Evo

Once a site is created it can be opened, which presents a page similar to the one below.



The **Create BAS** button opens the window shown below. All fields are optional, so you can click **Create BAS** straight away. Each field is described here.

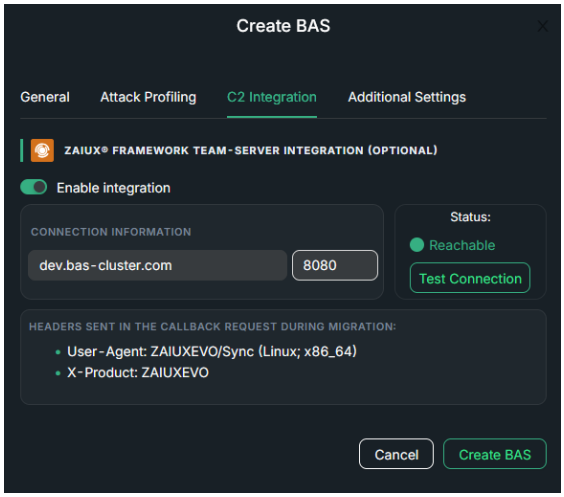


- **Label**: optional label to assign to this BAS for future reference.
- **Notification Email**: ZAIUX® Evo notifies the BAS creator about completion, fatal errors, or additional guidance during the simulation.
- **Attack profile**: disable specific attack vectors, or enable Stealth, which is available only when ransomware is disabled.
- **IP Ranges** (*): define internal IP ranges to limit the scope of the Breach & Attack Simulation.
- **Exclusions** (*): exclude specific IP addresses from the simulation.

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

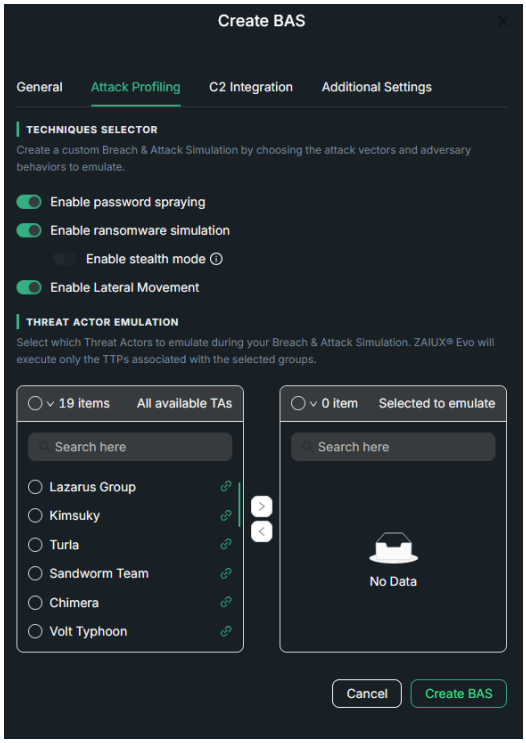
Note on defining exclusions

Although these fields are available, we recommend keeping exclusions to a minimum. 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.



C2 Integration: with a valid ZAIUX® Framework license, the two solutions can be integrated so that automated testing runs alongside hands-on operator activity.

Enter the Team Server details. The port must match the defined callback port, then click **Test Connection**. If the connection succeeds and the license information is validated, **Status** displays the label **Reachable**.



Attack Profiling: you can disable specific techniques that may lock out user accounts, such as password spraying, or cause endpoints to be isolated, such as the ransomware simulation. Stealth mode emulates a stealthier attacker, but it reduces the number of techniques available during the Breach & Attack Simulation.

Some organizations prefer not to allow automatic lateral movement inside the network, so this behavior can always be deactivated.

Finally, the **Threat Actor Emulation** feature emulates specific APT groups. Select one or more groups and ZAIUX® Evo uses only the techniques attributed to them.

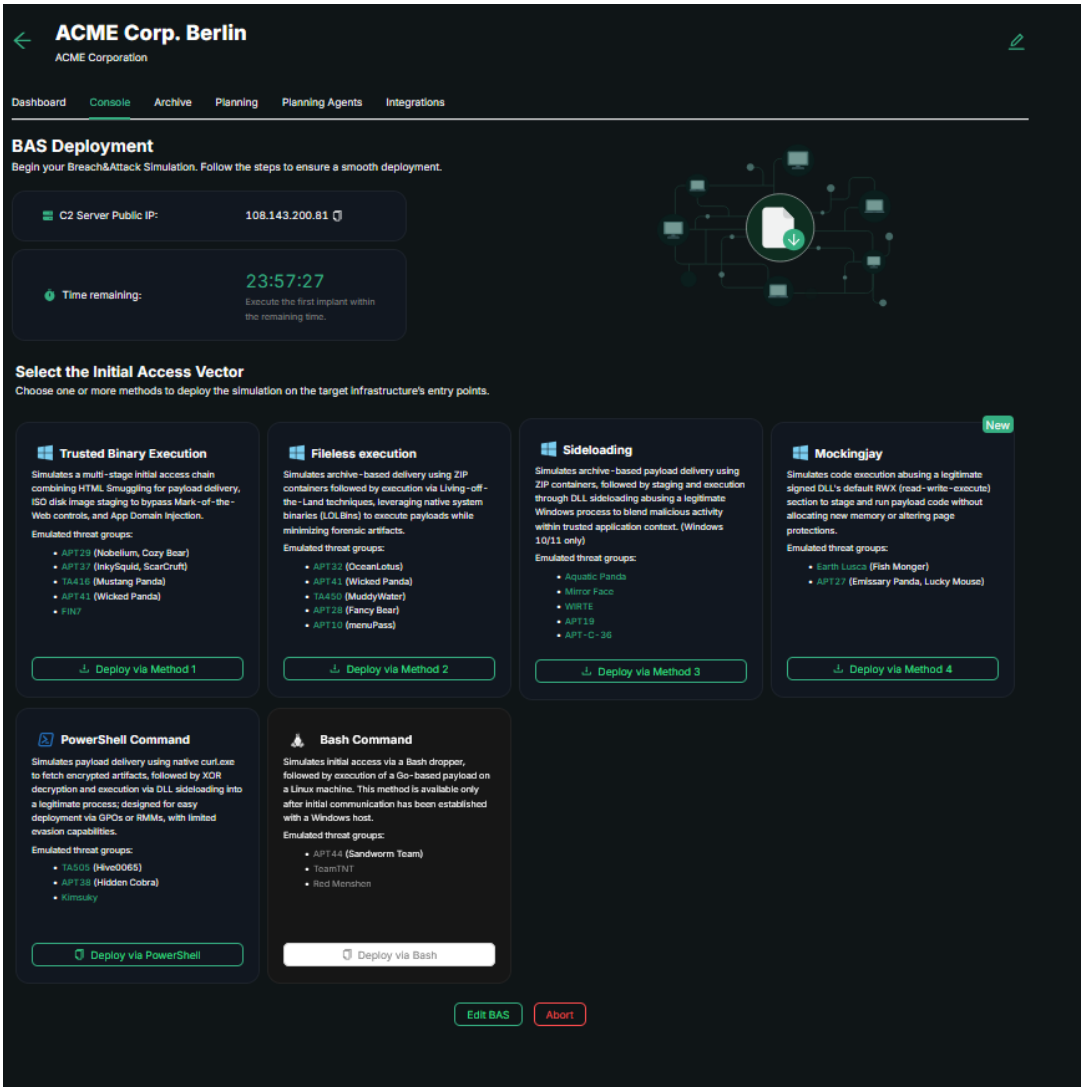
> **Recommended setting**
>
> If no group is selected, all techniques are included in the scope by default. This is the recommended configuration. Select threat actors only when the goal is to emulate those specific groups.

Once the configuration is confirmed, click **Create BAS**. Deploying the Breach & Attack Simulation environment, which runs in a secure and isolated sandbox, takes a few moments. From that point you have 24 hours to launch the simulation; the next section explains how to start it properly. Clicking **Abort** at this stage results in token reassignment.

Deployment methods

ZAIUX® Evo offers four deployment methods plus a PowerShell command for 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. It emulates real malware to deliver sophisticated and realistic cyber-attacks without causing service disruption, network bottlenecks, or business impact.



Method 1: simulates a multi-stage initial access chain combining HTML Smuggling for payload delivery, ISO disk image staging to bypass Mark-of-the-Web controls, and App Domain Injection.

Emulated threat groups: APT29 (Nobelium, Cozy Bear), APT37 (InkySquid, ScarCruft), TA416 (Mustang Panda), APT41 (Wicked Panda), FIN7

> **Before you open the HTML (Method 1)**
>
> - After downloading and moving the HTML file to the chosen entry points, open it in a web browser. An `.ISO` file is downloaded to the default Downloads folder. Mount the ISO by double-clicking it or right-

clicking and choosing **Mount**; a mapped drive is created and its folder opens. Launch the BAS by double-clicking `RunSimulation.exe`.

- Refer to the instructions inside the HTML file for the complete procedure, because the ISO file might be flagged and blocked by Mark-of-the-Web.
- Prefer delivering the HTML file to the entry point through a remote assistance system. Avoid email attachments, which an anti-phishing system may mark as suspicious.
- Methods 1 and 2 are the most suitable deployment methodologies, as in most cases they guarantee greater stealthiness.
- A video demonstration is available here.

Method 2: simulates archive-based delivery using ZIP containers, followed by execution through Living-off-the-Land techniques that leverage native system binaries (LOLBins) to run payloads while minimizing forensic artifacts.

The ZIP archive contains two files that can start the Breach & Attack Simulation. Each one replicates an execution technique commonly observed in real-world attacks, so you can choose whichever fits the simulation objectives.

- `Setup.bat`: simulates direct command execution through a batch script. This is the simpler technique, where commands are invoked directly from a script or command line.
- `SetupV2.vbs`: simulates indirect command execution through a COM object. This mimics how attackers abuse trusted Windows components to proxy execution and reduce visibility.

Emulated threat groups: APT32 (OceanLotus), APT41 (Wicked Panda), TA450 (MuddyWater), APT28 (Fancy Bear), APT10 (menuPass)

Method 3: simulates archive-based payload delivery using ZIP containers, followed by staging and execution through DLL sideloading, which abuses a legitimate Windows process so the activity blends into a trusted application context. Windows 10 and 11 only.

Emulated threat groups: Aquatic Panda, Mirror Face, WRITE, APT19, APT-C-36

Method 4: simulates code execution that abuses the default RWX (read-write-execute) section of a legitimate signed DLL to stage and run payload code without allocating new memory or altering page protections.

Emulated threat groups: Earth Lusca (Fish Monger), APT27 (Emissary Panda, Lucky Mouse)

PowerShell command: simulates payload delivery using native curl.exe to fetch encrypted artifacts, followed by XOR decryption and execution through DLL sideloading into a legitimate process. It is designed for easy deployment through GPOs or RMMs and has limited evasion capabilities.

Emulated threat groups: TA505 (Hive0065), APT38 (Hidden Cobra), Kimsuky

Bash command: deploys the Implant on Linux systems using a sequence of concatenated Bash commands. The technique uses the shell for a fast, automated deployment and includes an automatic cleanup step that minimizes persistent traces.

Emulated threat groups: APT44 (Sandworm Team), TeamTNT, Red Menshen

Running the first Implant outside a domain

The first Implant no longer has to run on a domain-joined host. It can be executed on a system that belongs to a workgroup or on a fully Microsoft Entra joined host, on Windows or on Linux.

The scope of the simulation still targets Active Directory. When the Implant starts from a system that is not joined to an Active Directory domain, ZAIUX® Evo performs a network scan to identify the other hosts on the network and, if one exists, an Active Directory domain. The actions that follow then attempt to move from the workgroup or Entra joined system to a domain-joined system.

If no Active Directory is present at all, the execution targets the other standalone systems on the network and, where present, the Entra ID and Office 365 tenant.

If all deployment methods are blocked

Realism is a core goal of ZAIUX® Evo, but evading every EDR or defensive control is not always possible. We therefore recommend starting with fail-closed testing, with all protections active. Disable a defensive control only after a documented, reproducible block that prevents the test objectives, and verify both Deployment Method 1 and Method 2 before you do.

Selecting the entry points

There is no limit to the number of entry points you can select for a Breach & Attack Simulation, 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, such as receptionist, front-desk, or back-office users. Add higher-privileged entry points later only if necessary, 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. 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, and CentOS.
- **Hardware**: no specific minimum 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 an Implant on them. To prevent ZAIUX® Evo from interacting with outdated systems in any way, use the scope-limitation features available during BAS creation.

Rollback and manual cleanup

ZAIUX® Evo reverts all configuration changes and removes the artifacts it left on disk. In some cases the automatic rollback may be incomplete and system administrators need to clean up manually. The final report lists the steps required 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.

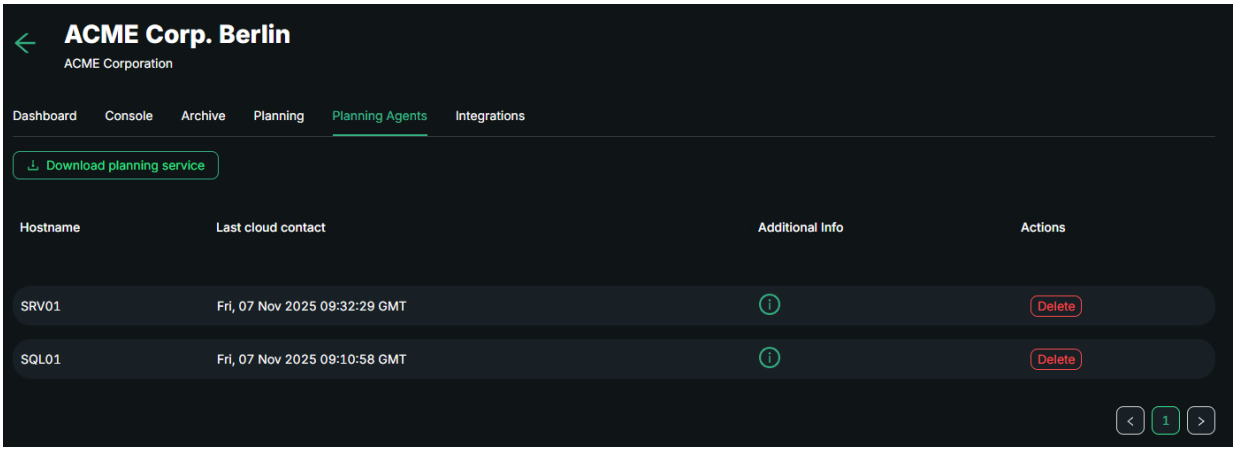
How to plan a recurring BAS

If your license includes the **BAS Planner** feature, you can run recurring and fully autonomous simulations. The platform schedules weekly and monthly executions at the dates and times you choose, using user-defined Windows computers in the target site as entry points.

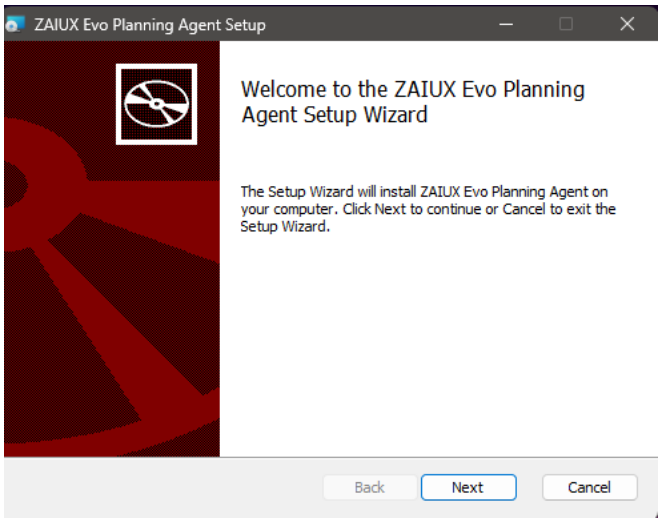
Planned simulations support an approach oriented to continuous exposure monitoring, as opposed to ad-hoc, manually configured runs. The site dashboard then works as an early warning that surfaces any deviation in the response to the simulated attack.

Installing the service on the entry points

From the **Planning Agents** tab, download the Connector with the **Download planning service** button, as shown below.

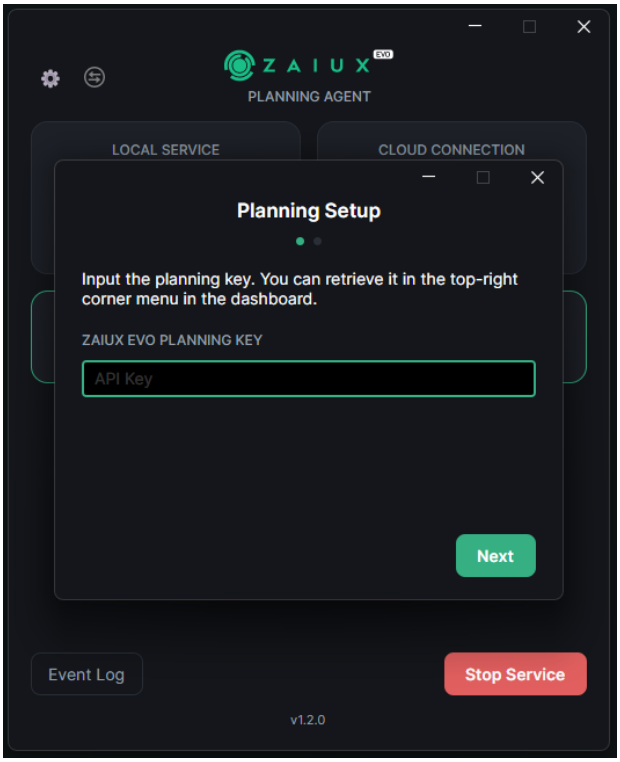


Installing the Connector requires administrative privileges on the target machines, because it installs a new Windows service configured to start automatically at system boot. The service ships as an MSI package, so it is compatible with deployment through SCCM.

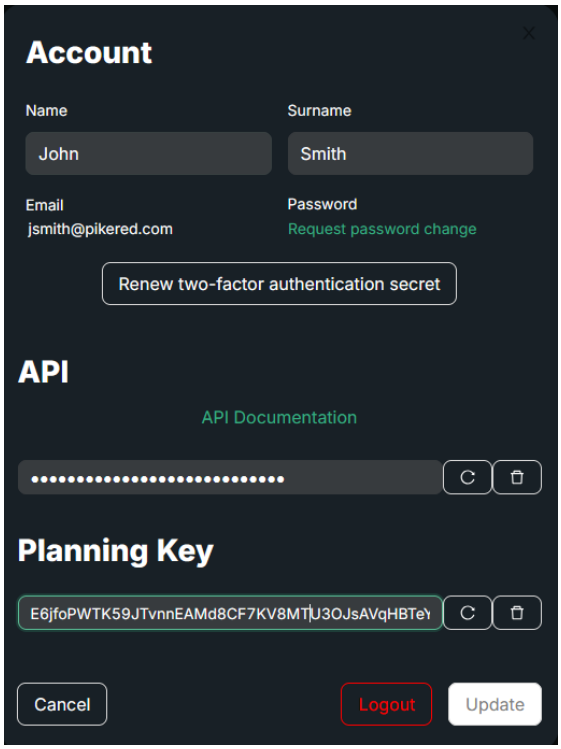


After the installation completes, a new application named **ZAIUX Evo Planning Agent** appears in the Windows Start menu. Use it to interact with the background service running on the system.

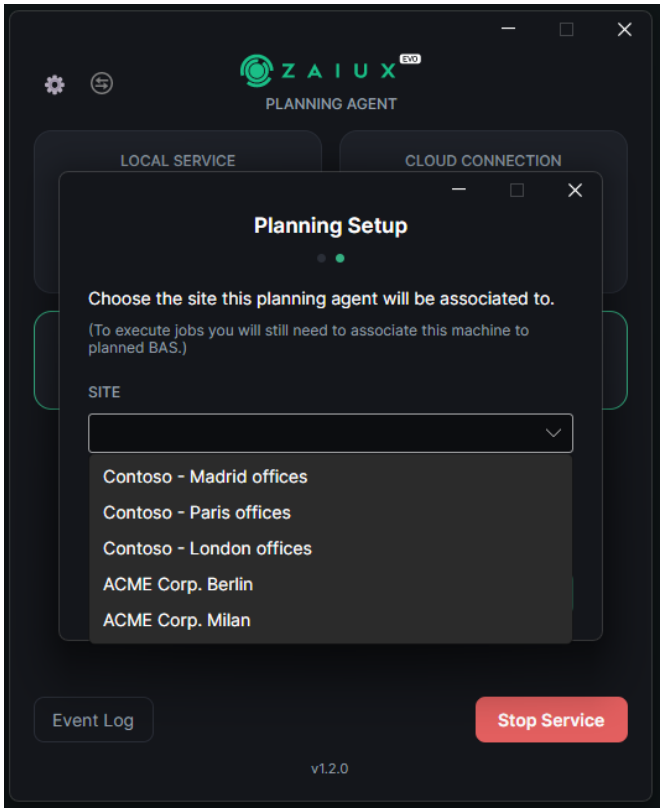
The first step is to configure a valid planning key, which establishes the initial connection between the on-premises service and your tenant.



The planning key is in your account details, in the top-right corner of the interface.

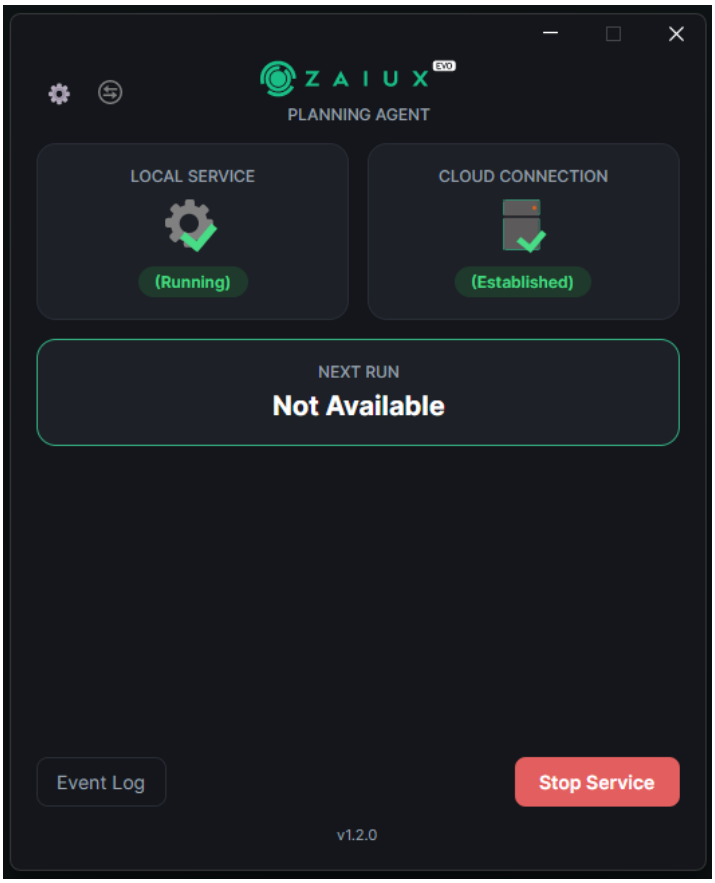


Step 1. Copy the planning key from your account page. The key is tenant-specific and all users within the same tenant share it. You can generate a new key if required.

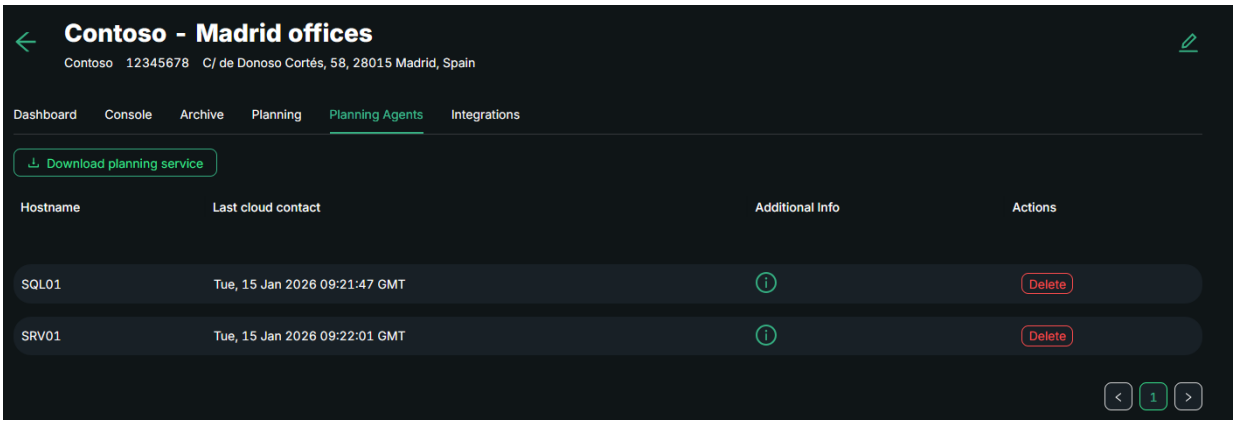


Step 2. Enter the planning key and select one of the available sites according to your requirements.

If the connection is established successfully, the application appears as shown below.



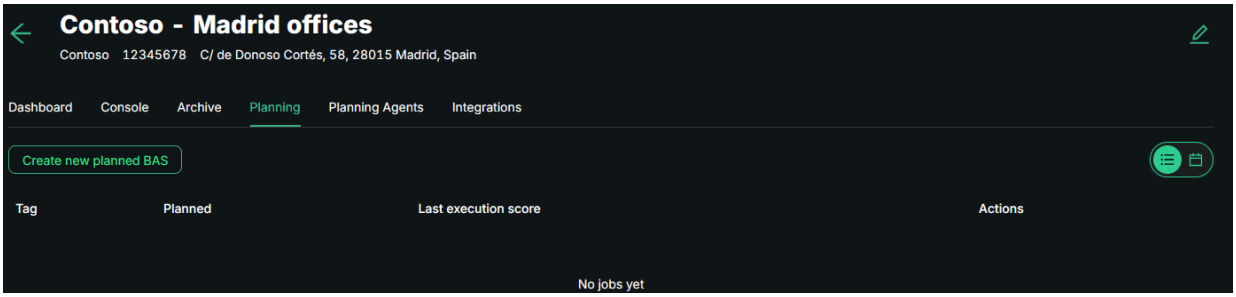
Connected services are listed in the ZAIUX® Evo user interface under the **Planning Agents** tab.

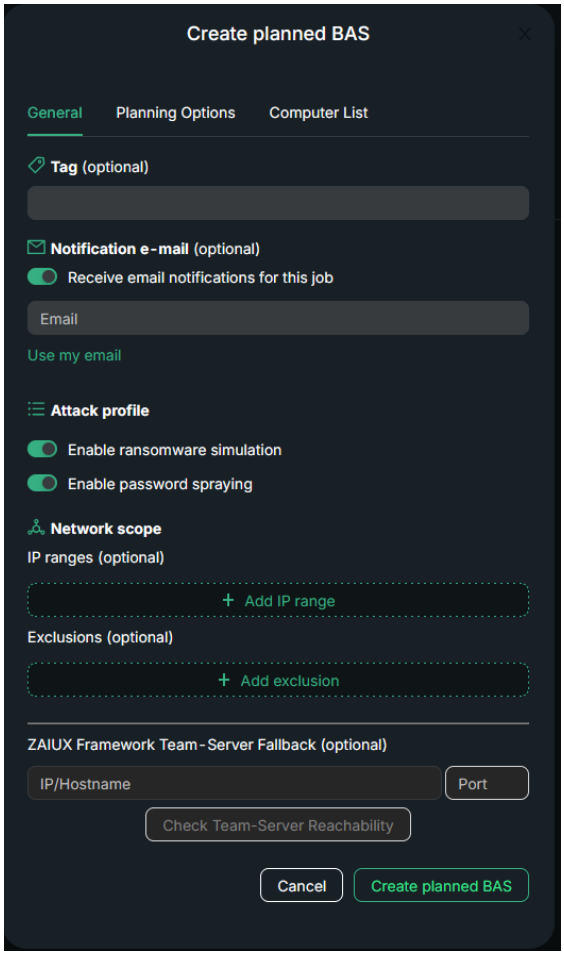


Once all required entry points are installed, the next step is to configure one or more recurring BAS scenarios.

Creating a new planned BAS

Go to the **Planning** tab and click **Create new planned BAS**.



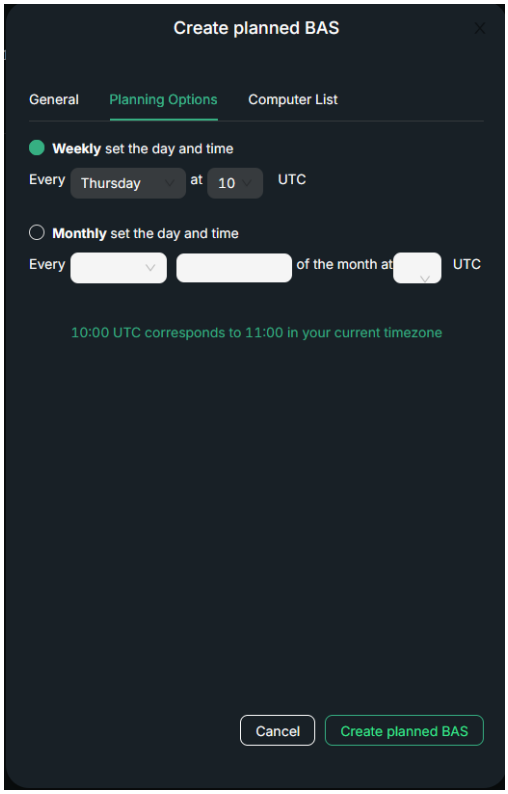


The only difference between the **General** tab and the configuration of a standard BAS is that you can designate a different email address for notifications.

Two additional tabs are available:

- **Planning Options**: defines the schedule for the planned BAS on a weekly or monthly basis.
- **Computer List**: selects the computers, connected through the service installed earlier, from which the activity starts. Several computers can be defined as entry points to expand the attack surface or to test different virtual LANs simultaneously.

Both tabs are described below.

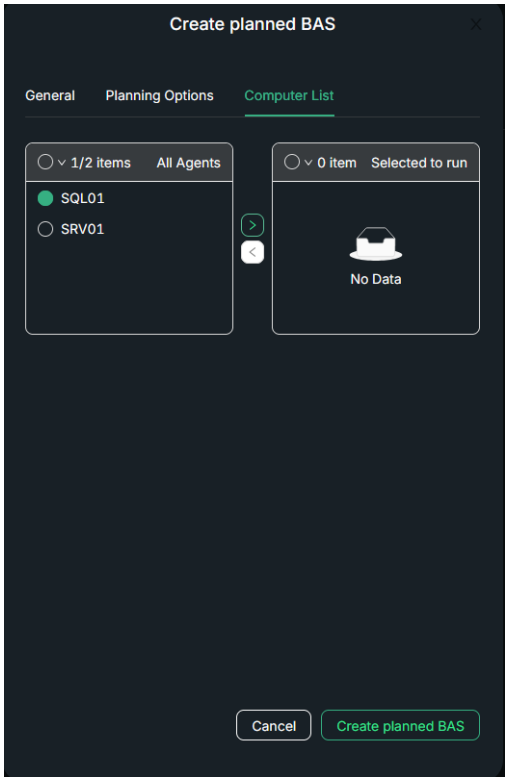


The **Planning Options** tab requires a scheduling basis: weekly or monthly.

Weekly lets you select a day from Monday to Sunday and a specific start time.

Monthly lets you choose the first, second, third, or fourth occurrence of a specific day 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.

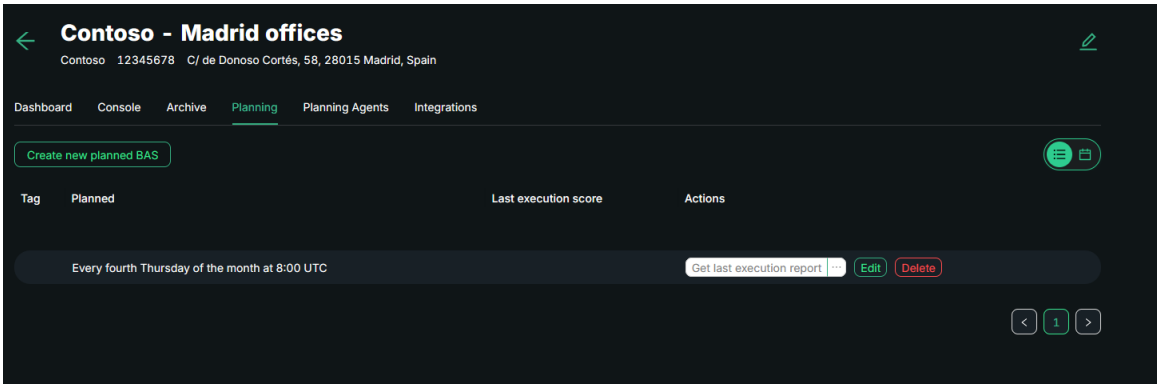


This tab selects the computer from which the BAS starts.

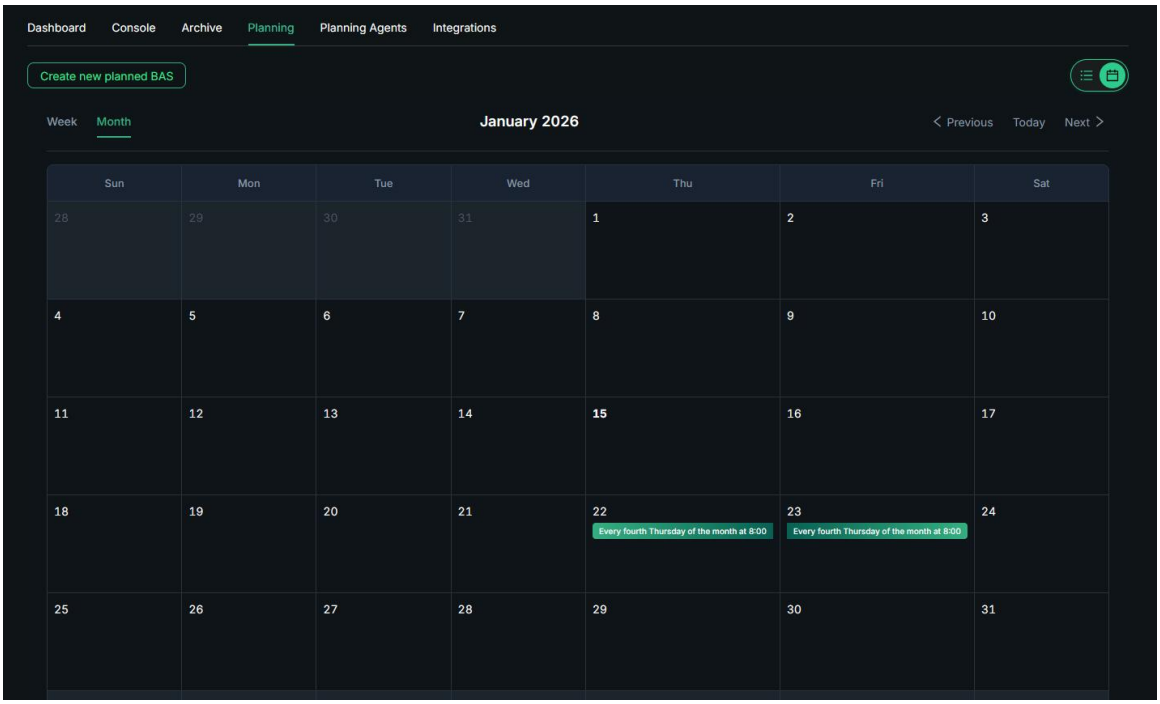
The selected computers must have the ZAIUX® Evo Planning Service installed and running, and the system must be powered on.

Select one or more computers and move them to the right-hand table with the green arrow button. Those computers are then 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 switches between the tabular view and the calendar view, which displays the start and end times of all BAS schedules for the selected site in a weekly or monthly layout.



The scheduled BAS then runs automatically according to your configuration.

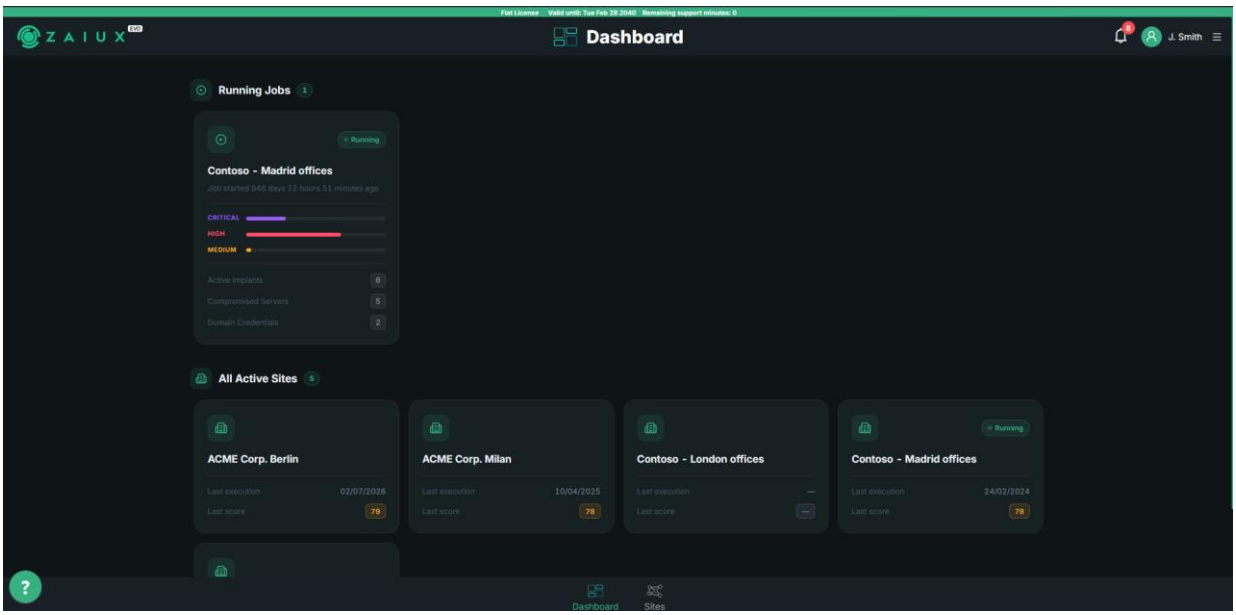
Important considerations for planned BAS

Only one BAS can run at a time on the same site. If an on-demand BAS is running when a planned BAS is due, the planned BAS is postponed to the next scheduled execution.

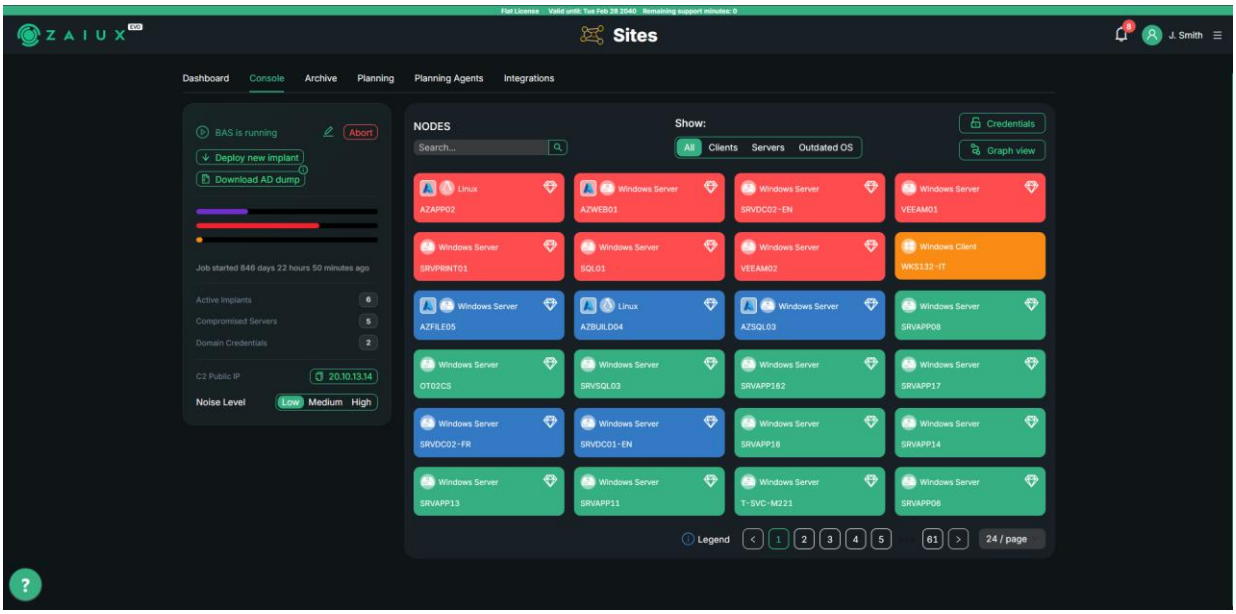
Multiple simulations can run simultaneously on different sites, but for FLAT licenses the total number of concurrent BAS cannot exceed the number of domains specified during the purchase process.

Monitoring the BAS progress

Running Breach & Attack Simulations appear in the top section of the dashboard, under **Running Jobs**. Clicking the widget opens the simulation so you can navigate through the findings.

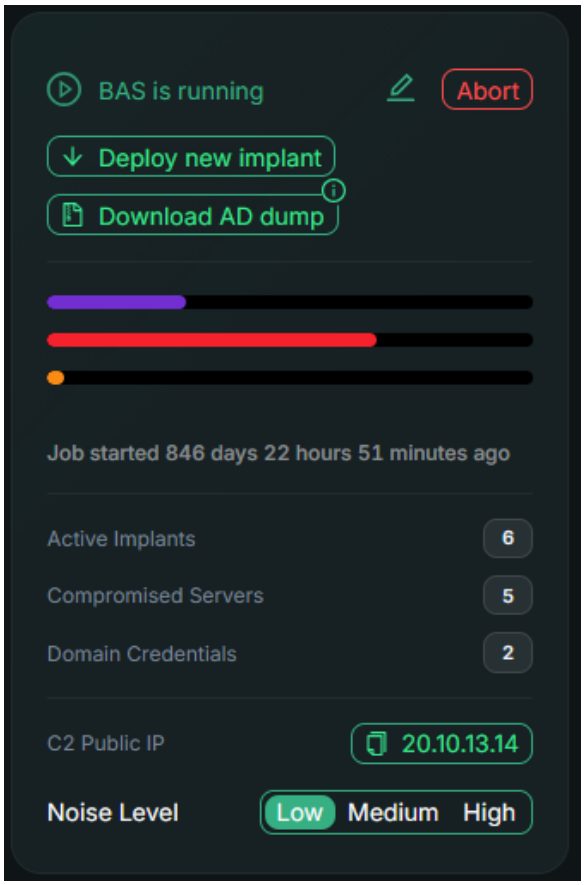


The BAS dashboard looks like this once the Active Directory enumeration phase is complete. Until that point, only the entry points are visible.



Interface core components

The interface breaks down into the following components.

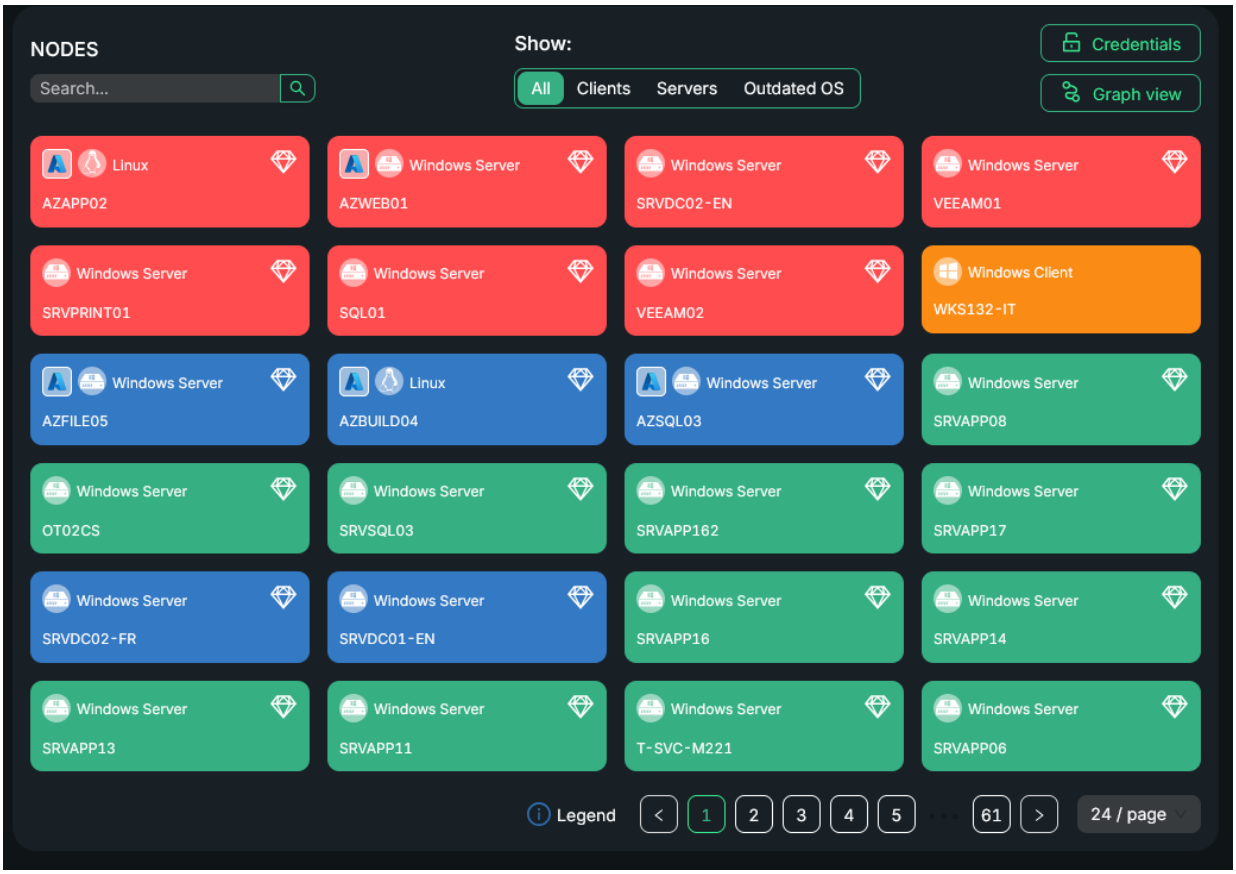


On the left are the available controls for the running BAS:

- **Abort**: stop the BAS and retrieve results immediately, without waiting for natural completion. The token is not reassigned, because the BAS is considered properly started.
- **Change Network Noise Level**: increase the Implant's C2 communication frequency to Medium or High, raising the chance of detection by SOC, EDR, or NDR. This setting can be adjusted several times during the same BAS.
- **Add more entry points**: download the deployment methods again to select additional entry points during execution.
- **View results**: see the total techniques executed with their severity, the 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 or manual analysis. The dump is compatible with BloodHound.
- **Edit BAS configuration**: enable or disable specific attack vectors in real time.

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/



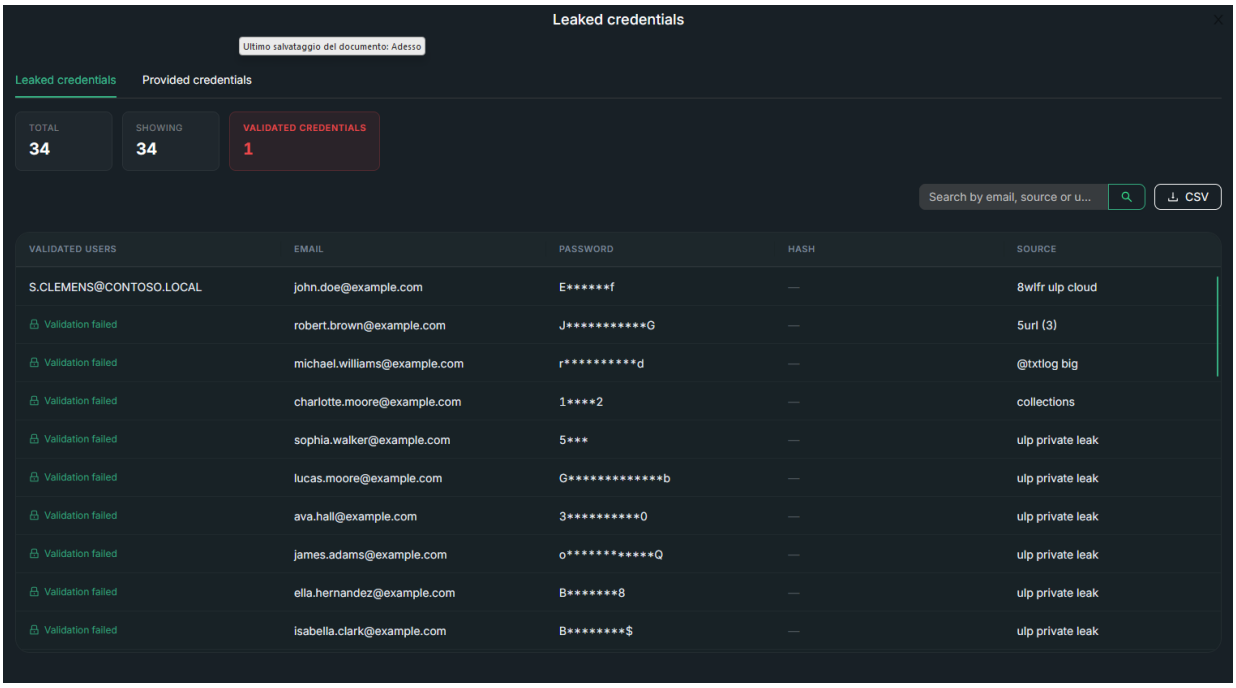
Colour legend

■	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): move through pages to view all hosts, or adjust the number of nodes shown per page.

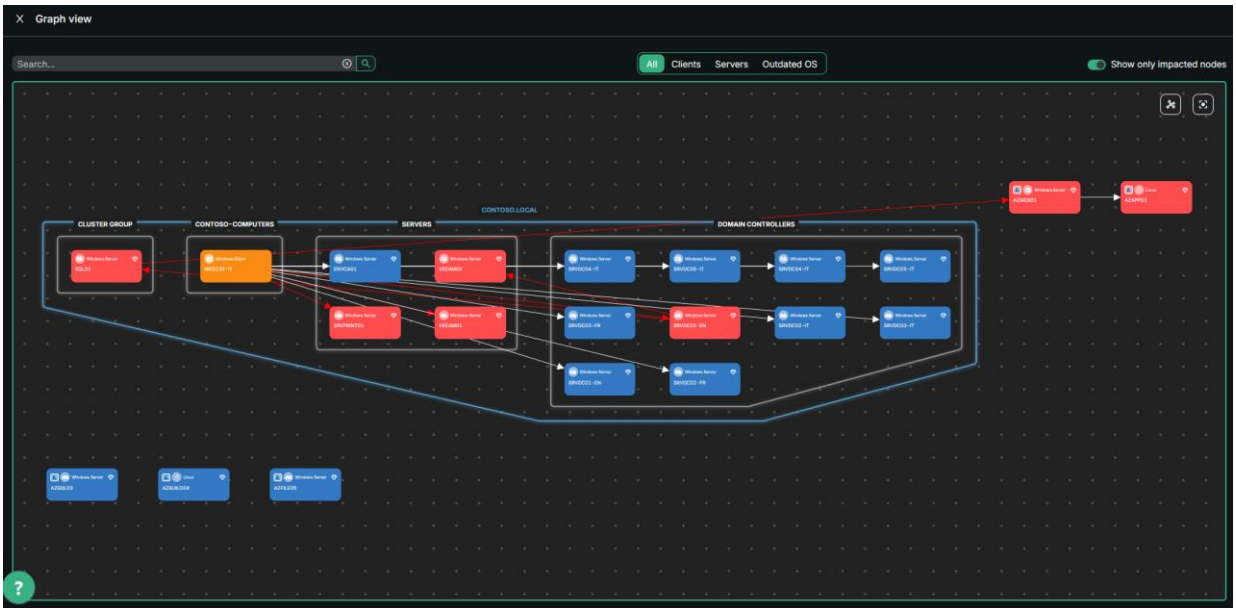
Leaked credentials



ZAIUX® Evo automatically identifies the public domain associated with the organization's Entra ID tenant and queries credential-leak databases for matches. Credentials found for the target domain are shown on this dashboard, together with the leak source. The view is limited to the top 100 entries; click **Download as CSV** to retrieve the full list.

The 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.

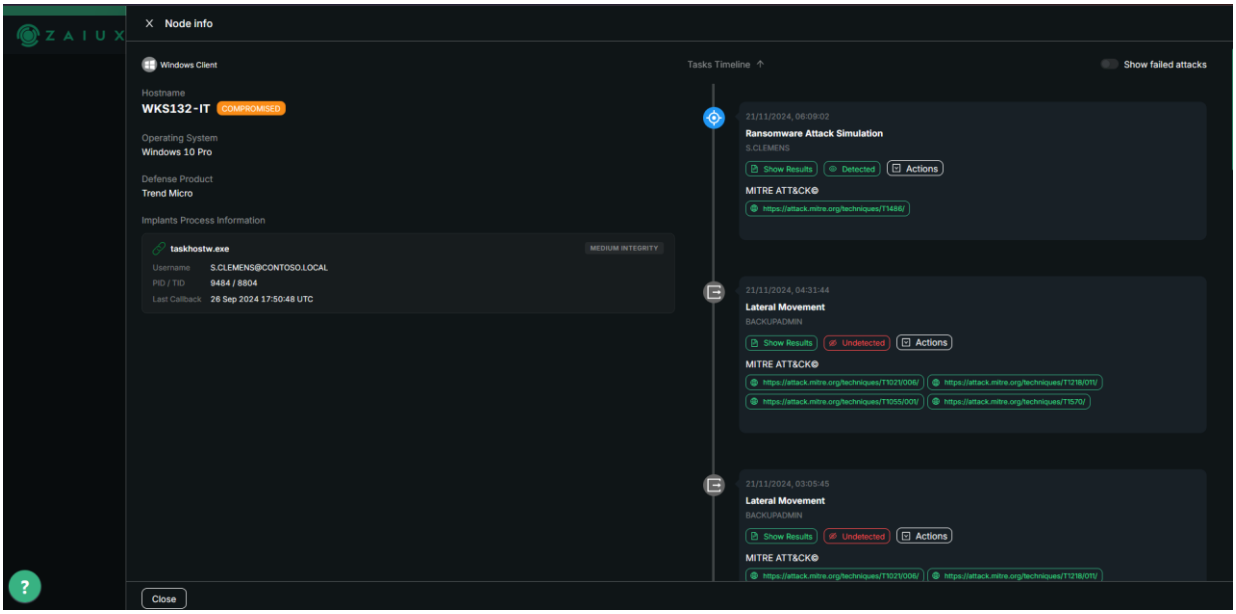
Graph view



The graph view shows all attacks ZAIUX® Evo executed. It includes enumeration links in grey and lateral-movement links in red, which helps you see how an adversary could propagate across the network and which hops lead to critical assets.

Compromised asset details

Clicking a node opens the view below.



On the left is information about the Implant and the compromised asset. PID and TID are 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. Use the PID 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, you may choose to deploy new Implants to the same entry point. ZAIUX® Evo keeps 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.

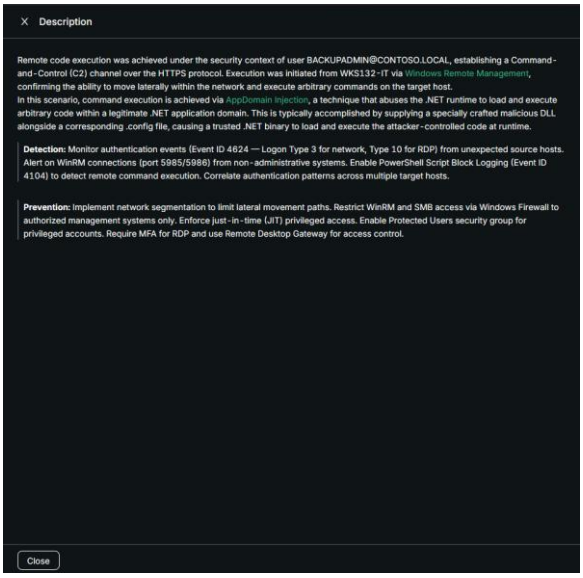
Icon legend

	The technique targeted this node. It may be a local attack or one 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 running.

The results of each action are available through **Show Results** on the card associated with the technique.

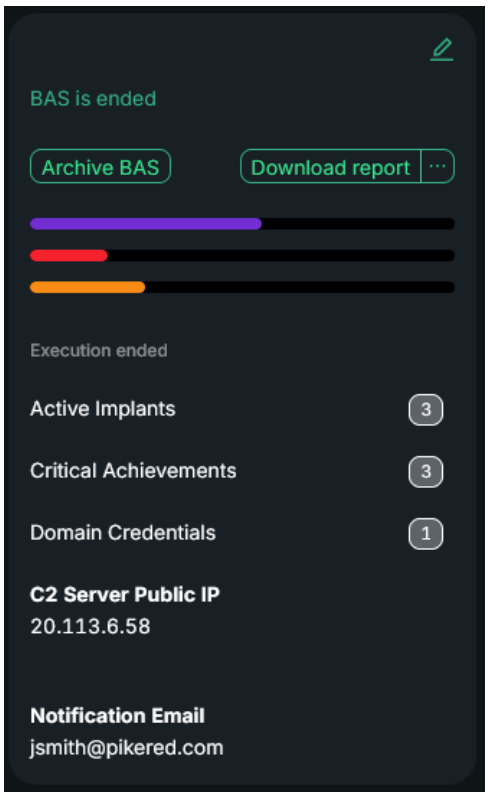
Each finding includes evidence of the misconfiguration, the affected entities, and a link for further information, highlighted in green.

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



Getting the results

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



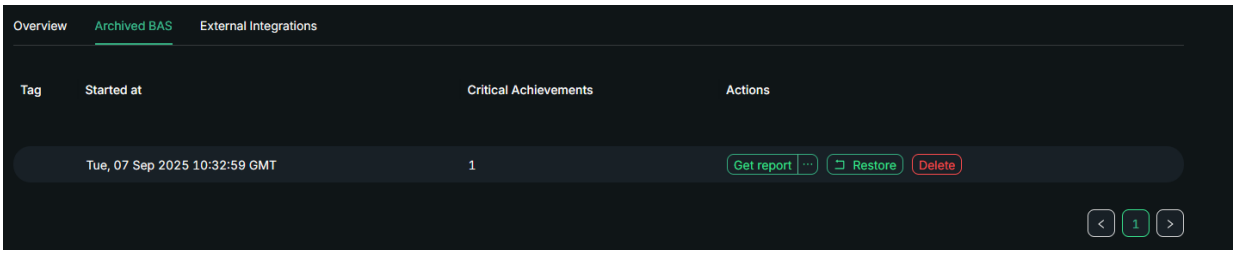
The closing message depends on the final status of the simulation:

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

Clicking **Archive BAS** cleans up the dashboard for the selected site and stores the BAS in the site's **Archived BAS** tab. From there you can:

- Download the reports again.

- Unarchive a previous BAS to make it visible in the dashboard, provided no other BAS is running on that site.
- Permanently delete a previous BAS history, including the report.



Catalog of attack vectors

Below is a comprehensive view of the attack vectors ZAIUX® Evo executes. Some techniques are omitted because they run as under-the-hood jobs that enable full-chain attacks.

> **Note**
>
> The platform icons in the OS column are explained in "How to read this guide" at the start of this document.
>
> Every technique applies to domain-joined systems. The Workgroup/Entra column states whether the technique also applies when no Active Directory domain is present, which covers both workgroup systems and fully Microsoft Entra joined hosts.

Process injection

OS	Workgroup/Entra	Technique	Description
	✓	**Thread Execution Hijacking** T1055.003	In some real-world scenarios attackers deploy several 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.
	✓	**Dynamic-link Library Injection** T1055.001	Adversaries may inject malicious libraries into trusted, well-known processes to stay stealthy and hide their intentions. Testing EDR effectiveness against such threats is essential to prevent data breaches.

Lateral movement

OS	Workgroup/Entra	Technique	Description
	✗	**Windows Remote Management**	Abusing legitimate protocols is a common way for attackers to gain remote code execution. ZAIUX® Evo leverages WinRM to execute arbitrary code on remote systems, launching new Implants and spreading across the network.
	✗	**SMB Pivoting**	When systems are isolated from the public network, Named Pipes can establish a pivoting mechanism between the isolated system and an already compromised machine. Attackers often abuse this technique 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 over RDP. ZAIUX® Evo emulates this scenario by opening an RDP session and

OS	Workgroup/Entra	Technique	Description
			running a PowerShell script inside it to deploy a new Implant.
	✓	**Abuse SQL Stored Procedure**	Existing SQL Server instances can be abused, when an attacker has sufficient privileges, to execute C# code through 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 such as WinSCP without protecting the credential vault with a master password can expose stored credentials. ZAIUX® Evo extracts unprotected credentials and uses them to execute code on remote Linux systems.
	✗	**Kerberos Ticket Abuse**	ZAIUX® Evo detects and hijacks existing Kerberos tickets stored on Linux hosts, enabling lateral movement that may extend to Windows systems.
	✓	**SSH Forward Agent Abuse**	ZAIUX® Evo detects and hijacks active SSH agent forwarding to spread across other Linux machines.

Domain-based attacks

OS	Workgroup/Entra	Technique	Description
	✗	**Kerberoasting**	ZAIUX® Evo detects Service Principal Names (SPNs) associated with services such as IIS, SQL Server, or Exchange, and requests service tickets for those SPNs. It then attempts offline hash cracking to recover clear-text passwords.
	✗	**AS-Rep Roasting**	ZAIUX® Evo detects users with the flag “Do not require Kerberos preauthentication” enabled. The flag exposes those accounts, because any user inside the domain can request their hashes. ZAIUX® Evo then attempts offline hash cracking to recover clear-text passwords.
	✗	**Unconstrained Delegation**	ZAIUX® Evo identifies machines configured for Unconstrained Delegation and can coerce a Domain Controller to authenticate to them, which allows 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 on a user’s behalf. The technique lets ZAIUX® Evo impersonate different user categories on compromised machines.

OS	Workgroup/Entra	Technique	Description
	✗	**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. Assessing how well defensive solutions handle these impersonation attacks is crucial.
	✗	**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, to find weak or easily guessed passwords.
	✗	**ESC1**	ZAIUX® Evo can exploit vulnerable certificate templates in Active Directory Certificate Services to attempt privilege escalation. More information about the attack is available at this link.
	✗	**ESC2**	ZAIUX® Evo can exploit vulnerable certificate templates in Active Directory Certificate Services to attempt privilege escalation. More information about the attack is available at this link.
	✗	**ESC3**	ZAIUX® Evo can exploit vulnerable certificate templates in Active Directory Certificate Services to attempt privilege escalation. More information about the attack is available at this link.
	✗	**ESC4**	ZAIUX® Evo can exploit vulnerable certificate templates in Active Directory Certificate Services to attempt privilege escalation. More information about the attack is available at this link.
	✗	**ESC15**	ZAIUX® Evo can exploit vulnerable certificate templates in Active Directory Certificate Services to attempt privilege escalation. More information about the attack is available 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 environments where Unix systems are joined to Active Directory, the unixUserPassword attribute may expose clear-text passwords. ZAIUX® Evo detects the attribute and evaluates potential privilege-escalation actions.
	✗	**SQL User Impersonation**	ZAIUX® Evo identifies whether it can leverage weak permissions to impersonate high-privilege users on Microsoft SQL Server instances discovered during enumeration.
	✗	**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.

OS	Workgroup/Entra	Technique	Description
	✗	**GPP Credential**	Legacy Group Policy Preferences may expose plaintext credentials usable for local privilege escalation.
	✗	**LAPS Abuse**	If LAPS has not been configured properly, attackers can exploit it to read local administrators' 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	Workgroup/Entra	Technique	Description
	✗	**LSASS Memory Dump**	Dumping `lsass.exe` memory remains a common adversary technique for harvesting privileged credentials. When the prerequisites are met, ZAIUX® Evo performs an LSASS memory dump and transfers it for offline analysis, which validates exfiltration-prevention controls.
	✓	**Browser Credential Dump**	ZAIUX® Evo can extract saved credentials from common browsers (Google Chrome, Firefox, Microsoft Edge) and validate the recovered credentials against Active Directory.
	✓	**Backup Credential Dump**	Backup tools are prime targets for attackers seeking full network control. ZAIUX® Evo detects running instances of popular backup software such as Veeam and assesses their security posture against credential-exfiltration risks.
	✓	**Steal Token**	Processes running in a different security context can be targeted for privilege escalation. Where conditions permit, ZAIUX® Evo extracts access tokens from other processes and impersonates those users.
	✓	**RDP Credential**	ZAIUX® Evo monitors processes on compromised hosts and detects the execution of remote-desktop clients. It parses the memory of those processes 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. They may include SMB share passwords, mailbox access credentials, or other service credentials.
	✗	**Kerberos Ticket Enumeration**	When conditions allow, ZAIUX® Evo reads cached Kerberos tickets on the compromised assets. These tickets can feed attacks such as Pass-the-Ticket or S4U2Self.

OS	Workgroup/Entra	Technique	Description
	✗	**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 such as command histories or configuration files. 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 their credentials.
	✗	**DcSync**	ZAIUX® Evo can perform a full DCSync attack when conditions permit. Validating protection against such attacks is crucial, because 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 cracking. The process combines dictionary attacks, permutations, key-walking, and context-based candidate generation. Recovered passwords are shown masked in the report and may be reused by ZAIUX® Evo for subsequent operations such as 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.
	✓	**Credentials in Files**	If Advanced AI is enabled on the current site, ZAIUX® Evo may use an LLM to improve detection accuracy, scanning shared folders to uncover credentials contained in documents, scripts, or configuration files.

Targeting Microsoft Entra ID

OS	Workgroup/Entra	Technique	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

OS	Workgroup/Entra	Technique	Description
			compromise such as 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 browser logins 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 new access tokens for additional resources to be obtained with a previously issued refresh token. ZAIUX® Evo uses 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 such as 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 move laterally to Azure virtual machines, 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, escalating from on-premises infrastructure to the cloud.
	✓	**Windows Hello Abuse**	If a device has no 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 for an Entra ID user.
	✓	**Access Token from File**	ZAIUX® Evo may attempt to decrypt cached cloud access tokens stored in local paths.
	✓	**Access Token via Azure IMDS**	ZAIUX® Evo may query the Azure Instance Metadata Service (IMDS) to obtain access tokens for the managed identity assigned to the compromised resource, which

OS	Workgroup/Entra	Technique	Description
			opens access to Azure Resource Manager and other cloud services.

Privilege escalation

OS	Workgroup/Entra	Technique	Description
	✓	**UAC Bypass – Fodhelper**	If the current user belongs to the Local Administrators group, arbitrary code can run 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 belongs to the Local Administrators group, arbitrary code can run in a high-integrity context by invoking the SSPI functions.
	✓	**UAC Bypass – CMSTPLUA**	If the current user belongs to the Local Administrators group, arbitrary code can run in a high-integrity context by exploiting the CMSTPLUA COM interface.
	✓	**AlwaysInstallElevated Abuse**	If this attribute is enabled in the Windows registry, every user can install MSI packages with administrative privileges. The functionality can be abused to execute arbitrary code in a high-integrity context.
	✓	**Unquoted Service Path**	If a service path containing spaces is not wrapped in double quotes, an attacker may 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, which enables privilege escalation and potential lateral movement.
	✓	**Sudo programs abuse**	If a user can run commands or binaries with sudo without a password, because of `/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 on files or directories referenced by cron jobs that run with elevated privileges, for example as root, those permissions can lead to privilege escalation. Because modifying scheduled jobs can disrupt critical services and may not be reliably reversible, ZAIUX® Evo restricts its activity to discovery:

OS	Workgroup/Entra	Technique	Description
			it identifies risky cron configurations but does not modify them.
	✓	**Copy-Fail (CVE-2026-31431)**	ZAIUX® Evo may attempt to exploit CVE-2026-31431 (Copy-Fail) in the Linux kernel's `algif_aead` module to escalate privileges from a low-privileged user to root through a crafted `AF_ALG` socket interaction.
	✓	**Abuse Docker for Privilege Escalation**	Users who belong to the `docker` group may be abused to escape container boundaries and gain root-level access to the host machine.

Enumeration and reconnaissance

OS	Workgroup/Entra	Technique	Description
	✓	**Portscan**	ZAIUX® Evo does not generate significant network traffic, but in certain situations it performs limited port discovery to identify services exposed by a target host. Typical targets include IIS and SQL Server.
	✗	**Active Directory Enumeration**	The 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 runs from the initial entry point, which loads a C# toolkit into memory to collect the information and exfiltrate it to the external command-and-control server.
	✗	**Stealth LDAP queries**	When Active Directory enumeration fails, ZAIUX® Evo switches to a fallback strategy of targeted, low-volume LDAP queries instead of flooding the Domain Controllers. This reduces noise and helps the traffic look 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**	Protected Process Light (PPL) defends critical system components against unauthorized access. Before delivering attacks that target protected processes, such as 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 it is not required, because it introduces privilege-escalation risks. ZAIUX® Evo checks whether the service is running and reports its status.
	✗	**Machine Account Quota check**	ZAIUX® Evo checks the ms-DS-MachineAccountQuota attribute to determine how many computer accounts each user can create within the domain. Setting this

OS	Workgroup/Entra	Technique	Description
			value to 0 is a best practice, as it mitigates several attack scenarios.
	✗	**LDAP Enforcement check**	LDAP channel binding and signing are crucial to the security of communications between LDAP clients and Domain Controllers. ZAIUX® Evo checks 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.
	✗	**Privileged SQL Server Access**	ZAIUX® Evo can enumerate SQL Server instances, identifying high-value targets for lateral movement or sensitive data theft.